XenApp 和 XenDesktop 7.15 LTSR

Apr 18, 2018

XenApp 和 XenDesktop 的长期服务版本 (LTSR) 计划可为 XenApp/XenDesktop 的各版本提供稳定性和长期支持。

XenApp 和 XenDesktop LTSR 当前可用的版本为 7.6 和 7.15。累积更新 2 (CU2) 是 7.15 LTSR 的最新更新。如果您是 LTSR 程序的新用户，并且未部署最初的 7.6 或 7.15 LTSR 版本，则无需在此时安装。Citrix 建议您开始使用 7.15 LTSR CU2。

此外，Citrix 还建议您使用特定版本的 Citrix Receiver 及其他组件。升级到这些组件的推荐版本可确保进一步简化维护过程以及确保您的部署中最新修复的可用性，但这并非是 LTSR 合规性的必需条件。

有关自 7.6 LTSR 起增加的 7.15 LTSR 功能的概览，请参见 XenApp 和 XenDesktop 功能汇总比较表。

下载

7.15 LTSR XenApp 和 XenDesktop 累积更新 2

7.15 LTSR（XenApp 和 XenDesktop）

有用链接

- Citrix 支持包

  支持包是一组由 Citrix 工程师编写、用于帮助诊断和解决 XenDesktop/XenApp 产品故障的常用工具。这些工具按功能和组件编目，因此很方便查找和使用。该包的早期版本用作相应产品的基础...

- LTSR 常见问题解答 (FAQ)

  Citrix Windows 应用程序交付团队一直在快速发布针对 XenApp 和 XenDesktop 产品线的创新功能和增强功能。在 2015 年，每季度会提供新产品版本。这样的快速创新步伐增强了 XenApp 的用例和 ...

- XenApp 和 XenDesktop 服务选项

  灵活的服务选项能够实现可预测的支持功能。Citrix 经常为 XenApp 和 XenDesktop 提供新的特性和功能，使企业能够保持竞争力、简化 IT 运营、提高数据安全性，并确保员工可在任何地点访问其业务资源。...

- 产品生命周期日期

  请参阅此表了解产品生命周期日期。下方的产品列表提供了其产品生命周期受生命周期阶段限制的 Citrix 产品。产品生命周期里程碑中包括状态更改通知 (NSC)、销售结束 (EOS)、维护结束 (EOM) 和生命周期结束 (EOL)。...

- Receiver for Windows 的 LTSR 计划

  对于 Citrix Receiver for Windows、Citrix Receiver for Mac、Citrix Receiver for Linux、Citrix Receiver for HTML5、Citrix Receiver for Java 或 Citrix Receiver for WinCE 的每个主要版本（例如 v3.0），客户将收到最短 4 年的生命周期。生命周期由至少前三年的主要维护阶段后跟扩展维护阶段组成。

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

新增功能

Apr 18, 2018

关于此版本

关于累积更新 2 (CU2)

关于累积更新 1 (CU1)

关于 7.15 LTSR（初始版本）

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

Cumulative Update 2 (CU2)

Apr 18, 2018

关于此版本

XenApp 和 XenDesktop 7.15 LTSR 累积更新 2 (CU2) 修复了自发布 7.15 LTSR CU1 起报告的 150 多个问题。

7.15 LTSR（常规信息）

自 XenApp 和 XenDesktop 7.15 LTSR CU1 起已修复的问题

本版本中的已知问题

下载

下载 7.15 LTSR CU2

新建部署

如何从头开始部署 CU2？

您可以设置基于 CU2 的全新 XenApp/XenDesktop 环境（通过使用 CU2 Metainstaller）。在此之前，建议您熟悉产品：

请仔细阅读 XenApp 和 XenDesktop 7.15 LTSR（初始版本）部分，并特别注意技术概述、安装和配置以及安全部分，然后再开始规划您的部署。请确保您的设置满足所有组件的系统要求。

现有部署

如何更新？

CU2 提供 7.15 LTSR 的基础组件的更新。请记住：Citrix 建议您将您的部署中的所有 LTSR 组件更新到 CU2。例如：如果您的 LTSR 部署中包含 Provisioning Services，请将 Provisioning Services 组件更新到 CU2。如果 Provisioning Services 不属于您的部署的一部分，则不需要安装或更新该组件。

XenApp 和 XenDesktop 7.15 LTSR CU2 基础组件

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

7.15 LTSR Baseline Component	Version	Notes
VDA for Desktop OS	7.15.2000	
VDA for Server OS	7.15.2000	
Delivery Controller	7.15.2000	
Citrix Studio	7.15.2000	
Citrix Director	7.15.2000	
组策略管理体验	3.1.2000	
StoreFront	3.12.2000	
Provisioning Services	7.15.3	
通用打印服务器	7.15.2000	
会话录制	7.15.2000	仅限 Platinum Edition
Linux VDA	7.15.2000	有关受支持的平台，请参阅 Linux VDA 文档
Profile Management	7.15.2000	
联合身份验证服务	7.15.2000	

XenApp 和 XenDesktop 7.15 LTSR CU2 兼容组件

建议您在 7.15 LTSR 环境中使用以下组件。这些组件无权享有 LTSR 的优势（扩展的生命周期以及仅用于修复的累积更新）。Citrix 可能会要求您在 7.15 LTSR 环境中升级到这些组件的较新版本。

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

7.15 LTSR CU2 Compatible Components and Platforms	Version
App Layering	4.10.0
Citrix SCOM Management Pack for License Server	1.2
Citrix SCOM Management Pack for Provisioning Services	1.19
Citrix SCOM Management Pack for StoreFront	1.13
Citrix SCOM Management Pack for XenApp and XenDesktop	3.14
HDX RealTime Optimization Pack	2.4
许可证服务器	11.14.0.1 Build 23101
自助服务密码重置	1.1.10.0
工作区环境管理	4.6

Citrix Receiver 的兼容版本

为简化维护过程以及确保实现最佳性能，Citrix 建议您在最新版本的 Citrix Receiver 可用时随时升级到相应版本。可以从 https://www.citrix.com/downloads/citrix-receiver.html 下载最新版本。为方便起见，请考虑订阅 Citrix Receiver RSS 源以在新版本的 Citrix Receiver 可用时接收通知。

请注意，Citrix Receiver 无法享有 XenApp 和 XenDesktop LTSR 的优势（扩展的生命周期和仅用于修复的累积更新）。Citrix 可能会要求您在 7.15 LTSR 环境中升级到 Citrix Receiver 的较新版本。如果使用的是 Citrix Receiver for Windows，Citrix 已公布特殊的 LTSR 计划。可以从 Citrix Receiver 的生命周期里程碑页面获取有关该计划的详细信息。

特别需要指出的是，7.15 LTSR CU2 支持以下版本的 Citrix Receiver 以及之后的所有版本。

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

7.15 LTSR CU2 Compatible Version of Citrix Receiver	Version
Citrix Receiver for Android	3.13.5 或更高版本
Citrix Receiver for Chrome	2.6.5 或更高版本
Citrix Receiver for HTML5	2.6.5 或更高版本
Citrix Receiver for iOS	7.5.3 或更高版本
Citrix Receiver for Linux	13.9.1 或更高版本
Citrix Receiver for Mac	12.9 或更高版本
Citrix Receiver for UWP (通用 Windows 平台)	1.0.5 或更高版本
Citrix Receiver for Windows	4.9 或更高版本

XenApp 和 XenDesktop 7.15 LTSR 值得注意的排除项

以下功能、组件和平台无法享有 7.15 LTSR 的生命周期里程碑和优势。需要特别指出的是，累积更新和扩展生命周期优势被排除在外。可以通过常规的最新版本获取排除的功能和组件的更新。

Excluded Features
Framehawk
StoreFront Citrix Online 集成

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

Excluded Components
Personal vDisk： • Windows 10 计算机除外。 • 对于 Windows 7 计算机，提供有限的 LTSR 支持，直至 2020 年 1 月 14 日（适用 CU 要求）
AppDisk

Excluded Windows Platforms *
Windows 2008 32位（面向通用打印服务器）

* Citrix 保留根据第三方供应商的生命周期里程碑更新平台支持的权利。

安装和升级分析

当您使用完整产品安装程序部署或升级 XenApp 或 XenDesktop 组件时，将在安装/升级组件的计算机上收集和存储有关安装过程的匿名信息。这些数据用于帮助 Citrix 改善其客户的安装体验。有关详细信息，请参阅 http://more.citrix.com/XD-INSTALLER。

XenApp 6.5 迁移

XenApp 6.5 迁移过程有助于高效快速地从 XenApp 6.5 场过渡到运行 XenApp 7.15 LTSR CU2 的站点。这在部署中包含大量应用程序和 Citrix 组策略时很有用，可以降低手动将应用程序和 Citrix 组策略移至新 XenApp 站点时意外引入错误的风险。

安装 XenApp 7.15 LTSR CU2 核心组件并创建站点后，迁移过程按照以下顺序进行：

- 在每个 XenApp 6.5 工作进程上运行 XenApp 7.15 CU2 安装程序，将其自动升级到新 Virtual Delivery Agent for Server OS 以便在新站点中使用。
- 在 XenApp 6.5 Controller 上运行 PowerShell 导出 cmdlet，以将应用程序和 Citrix 策略设置导出至 XML 文件。
- 编辑 XML 文件（如果需要），以细化要导入到新站点的内容。通过自定义这些文件，可以将策略和应用程序设置分阶段导入到 XenApp 7.15 LTSR CU2 站点：即一些现在导入，其他稍后导入。
- 在新 XenApp 7.15 LTSR CU2 Controller 上运行 PowerShell 导入 cmdlet，以将 XML 文件中的设置导入新 XenApp 站点。

根据需要重新配置新站点，然后对其进行测试。

有关详细信息，请参阅迁移 XenApp 6.x。

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

已修复的问题

Apr 18, 2018

Citrix Director

- 按 DNS 名称过滤计算机时，Citrix Director 可能不显示任何计算机，或者显示重复的计算机条目。首次将计算机添加到监视数据库，但同时从两个不同的 Delivery Controller 中添加时，将出现此问题。因此，将创建两个计算机条目。[#LC4905]
- 您（即自定义管理员）无法从计算机目录中获取 Remote PC 设置时可能会出现异常。您有权管理计算机目录，但作用域不包含特定的目录时会出现此问题。[#LC8170]
- 在 Citrix Director 中导航到**过滤器** > **会话**并尝试调整浏览器大小时，整个表格可能会对齐不正确。[# LC8624]
- 从 Citrix Director 中导出数据时，CSV 文件可能会变得不可用。设置任何非英语版本的 Microsoft Windows 作为 Director 显示语言时可能会出现此问题，因为逗号可能会同时用作值和小数分隔符。[#LC8625]
- 启动 Citrix Director 时，**基础结构**选项卡中将显示以下错误消息：

  “无法检索数据。与 Web 服务器的连接断开。请检查您的网络连接并重试。”[#LC8752]
- 配置了多个站点时，Citrix Director 站点名称将被截断。[#LC9258]

Citrix 策略

- 打开组策略编辑器 (gpedit.msc) 的第二个实例时，“Citrix 策略”节点将不打开，并且可能会显示以下错误消息：

  “Unhandled exception in managed code.”（托管代码管理单元中出现未处理的异常。）[#LC7600]
- 通过组策略管理控制台 (GPMC) 应用 Citrix 策略时，这些策略可能不在 GPMC 策略设置下显示。但是，编辑组策略对象 (GPO) 时，您可以看到这些策略和设置处于启用状态。[#LC8282]
- 在 Active Directory 中使用 Citrix 组策略管理 3.1 向**用户策略**中添加**打印机分配**设置可能会导致出现窗口大小调整问题。窗口可能会在您将其打开后开始水平自动调整大小，直至扩展到屏幕的中心。因此，编辑策略会非常困难，因为您无法搜索所有列。[#LC8684]
- 本地策略缓存文件夹 (%ProgramData%/CitrixCseCache) 中的文件设置为“只读”时，可能无法成功应用策略设置。[#LC8750]
- 尝试在单用户管理模式下从 VDA 中启动 App-V 应用程序可能会失败。**ApplicationStartDetails** 注册表项的值为空时，或者如果该注册表项中缺少应用程序详细信息，则会出现此问题。[#LC8798]
- 尝试使用 NETBIOS 名称向交付组中添加计算机以实现用户关联可能会失败。相反，域名可能会显示。NETBIOS 名称使用错误的 URL 时会出现此问题。[#LC9393]

Citrix Studio

- 尝试手动从 Linux VDA 添加应用程序时，可能会显示以下错误消息：

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

"Value cannot be null while publishing the application."（发布应用程序时，值不能为空。）

但是，在出现的错误消息中单击"确定"时，会成功添加应用程序。[# LC7910]

- 当应用程序位于 Citrix Studio 中的**应用程序**节点的子文件夹中时，尝试从交付组中删除应用程序可能会失败。[#LC8705]
- 尝试使用 NETBIOS 名称向交付组中添加计算机以实现用户关联可能会失败。相反，域名可能会显示。NETBIOS 名称使用错误的 URL 时会出现此问题。[#LC9393]

Controller

- 日语操作系统中安装的某些 Citrix 服务的"Service Display Name"（服务显示名称）和"Service description"（服务说明）结尾处可能会出现无关字符。[#LC5208]
- 尝试从 Citrix Director 检索会话的数据时，监视数据库中出现空条目。因此，某些数据不会显示在 Citrix Director 中，并显示以下错误消息：

  "无法检索数据"[#LC6273]
- 尝试手动从 Linux VDA 添加应用程序时，可能会显示以下错误消息：

  "Value cannot be null while publishing the application."（发布应用程序时，值不能为空。）

  但是，在出现的错误消息中单击"确定"时，会成功添加应用程序。[# LC7910]
- Citrix Broker Service (Brokerservice.exe) 可能会意外退出。LicPolEng.dll 模块出错导致出现此问题。[#LC8638]
- 通过 Machine Creation Services 置备具有所需的最低 VMware 权限的虚拟机 (VM) 时，尝试删除 VM 可能会失败。即使具有最低的 VMware 授权，也可能会出现此故障。[#LC8868]
- 删除了分配有区域首选项的 Active Directory 用户时，尝试将 Broker 配置导入第二个 Broker 可能会失败。将 XenDesktop 升级到最新版本后，导入操作也可能会失败。[#LC9269]
- 尝试使用 NETBIOS 名称向交付组中添加计算机以实现用户关联可能会失败。相反，域名可能会显示。NETBIOS 名称使用错误的 URL 时会出现此问题。[#LC9393]

HDX MediaStream Flash 重定向

- 启用了 HDX MediaStream Flash 重定向时，当您通过 Qumu.com 重新连接 VDA 会话时，Flash 内容可能不在 Microsoft Internet Explorer 中加载。[#LC9193]

安装程序

- 尝试更改 Delivery Controller 中的安装目录路径可能不适用于 **XaXdProxy.msi**。[#LC8691]

Linux VDA

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

- 使用 Delivery Controller 注册 Linux VDA 可能会间歇性失败。[#LC7982]
- 在 Red Hat Enterprise Linux Server 7.3 中运行的 Citrix Director 7.13 可能不显示计算机的会话详细信息。此时将显示以下错误消息：

  “无法检索数据。”[#LC8204]
- 一段时间后，Linux VDA 可能会在 Delivery Controller 中注册并取消注册。[#LC8205]
- 用于检查 Linux VDA 的会话显示的某些第三方应用程序可能不会显示所有像素。[#LC8419]
- 存在多个 LDAP 服务器时，在更新了策略并且会话超时后，尝试在 Linux VDA 上启动应用程序可能会失败。[#LC8444]
- 将会话连接到 Linux VDA 时，ctxhdx 进程可能会意外退出并显示 segfault 错误。[#LC8611]
- 使用 Linux VDA 7.16 早期访问版本时，Broker 代理可能无法获取应用程序名称。此故障会导致 Director 显示错误**已请求代理**，之后将开始重新注册。[#LC9243]

Profile Management

- 重新启动 Profile Management 服务后，Citrix Director 可能不会显示用户登录和个性化信息。[#LC6942]

Provisioning Services

StoreFront

- 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]
- 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]
- 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 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]

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

VDA for Desktop OS

HDX 3D Pro

- 在 Microsoft Windows 10 中运行的 VDA 上启用了 HDX 3D Pro 和自定义分辨率后，登录时可能会间歇性出现灰屏。[#LC8417]

HDX MediaStream Flash 重定向

- 启用了 HDX MediaStream Flash 重定向时，当您通过 Qumu.com 重新连接 VDA 会话时，Flash 内容可能不在 Microsoft Internet Explorer 中加载。[#LC9193]

HDX MediaStream Windows Media 重定向

- 禁用了 HDX MediaStream Windows Media 重定向时，尝试通过 Windows Media Player 打开某些视频文件格式可能会导致正在播放的视频垂直翻转。[#LC9194]

HDX RealTime

- 安装 RealTime Connector。使用利用重定向的网络摄像机的应用程序时（例如 Skype for Business），可能会在初始会话启动过程中重定向和检测 VDA for Desktop OS 中安装的网络摄像机。但是，当您重新连接到用户会话时，将无法再检测到该网络摄像机。用户设备上未安装 RealTime Media Engine 时会出现此问题。[#LC8793]

键盘

- 在 Android 设备上启动应用程序时，如果您的光标在文本字段中，可能不会自动显示键盘。此外，必须始终触摸键盘按钮进行打开或关闭。[#LC8936]

打印

- 尝试使用 Microsoft Word 通过打印机设置在纸张双面打印可能会失败。[#LC7501]
- 尝试从 Microsoft Internet Explorer 的已发布实例打印文档可能会失败。[#LC8093]
- 如果法语是 VDA 上安装的显示语言，尝试打印文档可能会失败。[#LC8209]
- 在您重新连接到会话后，从用户设备重定向的打印机可能不会重定向。[#LC8762]
- 启动第一个会话过程中停止打印后台处理程序服务时，尝试重新启动 Citrix Print Manager 服务 (cpsvc.exe) 可能会失败。[#LC9192]

会话/连接

- 从已映射客户端驱动器读取文件时，如果在客户端会话之外更改了旧的缓存文件长度，则可能会返回该文件长度。此外，对于删除的任何字符，会插入空字符。

  要启用此修复，请将以下注册表值设置为“0”：

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters
  名称：CacheTimeout
  类型：REG_DWORD
  值：默认值为 60 秒。如果 CacheTimeOut 设置为“0”，则会立即重新加载文件长度，否则会在定义的超时之后进行加载。

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

[#LC6314]

- 使用旧图形模式时，VDA for Desktop OS 上运行的会话可能会变得无响应。出现此问题时，您可能无法更新 Desktop Viewer 上的任何内容，但 Desktop Viewer 不处于无响应状态。此外，30-60 分钟后，以前无响应的会话将恢复。[#LC7777]
- 在启用了会话延迟的情况下启动应用程序时，会话可能会在应用程序出现后注销。[# LC8245]
- 尝试启动 VDA for Desktop OS 时，桌面可能会启动，然后在几秒钟之后消失。[#LC8373]
- 在下列一种情况下，Windows 资源管理器可能会异常关闭：
  - 选择大量文件且文件名中包含的字符数超过 260，然后选择“发送至 > 传真收件人”选项。
  - 尝试打开第三方应用程序。
  - 尝试使用 Nitro PDF 合并文件。[#LC8423]
- 对视觉效果下的高级系统设置所做的更改应用于当前 VDA for Desktop OS 会话，但可能不会保留到后续会话中。要使此类更改持续存在，请设置以下注册表项：

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix
  名称：EnableVisualEffect
  类型：DWORD
  值：1 [#LC8049，#LC8658]

- 断开会话后，monitor1 可能会在下次本地登录时错误地显示为主监视器。当您在多监视器环境中本地登录到 Remote PC Access VDA 并将 monitor2 配置为主监视器，通过用户设备连接，然后使用 Desktop Viewer 断开会话时，可能会出现此行为。[#LC8675]
- 尝试启动 Microsoft Windows Server 2012 或 2016 中运行的已发布应用程序时，您可能会被锁定。[#LC8681]
- 在多监视器环境中启动应用程序时，可能会显示包含两个监视器的登录横幅。使用单个监视器时，登录横幅窗口将在全屏模式下显示。[#LC8741]
- 启用了本地应用程序访问的情况下，如果尝试在 Microsoft Windows 10 上运行的已发布桌面上打开应用程序，这些应用程序将无法最小化。[#LC8813]
- DLP 软件可能无法扫描包含 UNC 链接的文件。[#LC8893]
- 启动已发布的应用程序后，Num Lock 键不起作用。当 Num Lock 键的 LED 指示灯在用户设备上可见，但数字在用户会话中不起作用时，将出现此问题。在某些情况下，当客户端请求的 LED 更新的时间早于新创建的远程桌面初始化其 LED 状态的时间时，将出现此问题。出现这种情况时，WinsStation 可能不更新其 LED 状态，LED 状态在端点与 VDA 之间将不同步。[#LC8921]
- 尝试启动应用程序和桌面可能会失败。VDA for Server OS 变得无响应时将出现此问题。

  要启用此修复，请设置以下注册表项：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard
  名称：EnableSCardHookVcResponseTimeout
  类型：DWORD
  值：1 [#LC8969]

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

- 尝试打开 VM 托管应用程序可能会失败。[#LC9001]
- 尝试重新连接到会话可能会失败。[#LC9040]
- 在会话中使用 WFAPI SDK **WFQuerySessionInformation** 命令获取安装的 VDA 版本信息时，该命令可能不起作用。[#LC9041]
- 从版本 7.14 到 7.15 升级 XenApp 和 XenDesktop 后，尝试在已发布的应用程序的选项卡之间切换可能会导致应用程序变得无响应。此外，如果将无缝窗口的大小调整到较小的大小，然后展开窗口，则需要一段时间才能绘制该窗口内的所有元素。[#LC9078]
- 启动应用程序后，已发布的应用程序可能会立即间歇性关闭。[#LC9167]
- 重新连接到 Millennium 套件中屏幕分辨率与初始连接不同的无缝应用程序时，该应用程序可能会错误地调整大小。因此，该窗口可能会被截断。[#LC9214]
- 尝试通过用户设备连接到 Windows 10 版本 1709 的已发布桌面可能会导致显示灰色屏幕。尝试通过虚拟机管理程序的控制台连接到已发布的桌面时，将显示一个包含纺车状指示器的黑色屏幕。但是，通过 RDP 连接到已发布的桌面将成功运行。[#LC9215]
- 尝试从 Citrix Receiver for Mac 启动应用程序可能会失败。无法提取客户端许可证 (LicenseRequestClientLicense) 时会出现此问题。[#LC9286]
- 启用了 HDX 3D Pro 时，尝试启动 XenDesktop 可能会间歇性失败。GPU 出现故障时会出现此问题。[#LC9343]
- 平稳漫游时，从用户会话到非托管远程桌面会话的会话显示可能不正确。[#LC9471]

智能卡

- 使用智能卡时，某些第三方应用程序可能会变得无响应，而非显示 PIN 提示。[#LC8805]

系统异常

- 服务器上的 picadm.sys 可能发生致命异常，并显示蓝屏和错误检测代码 0x22。[#LC6177]
- 服务器上的 picadm.sys 可能发生致命异常，并显示蓝屏和错误检测代码 0x00000050 (PAGE_FAULT_IN_NONPAGED_AREA)。[#LC6985]
- 服务器上的 picadm.sys 可能发生致命异常，并显示蓝屏和错误检测代码 0x22。[#LC7574]
- 服务器上的 vdtw30.dll 可能会遇到致命异常，并显示蓝屏和停止代码 SYSTEM_SERVICE_EXCEPTION (3b)。[#LC8087]
- 服务器上的 pdcrypt2.sys 可能发生致命异常，并显示蓝屏和错误检测代码 0x3B。启动 VDA 时会出现此问题。[#LC8328]
- 在启用了 HDX 3D Pro 和 GPU 硬件编码的情况下使用 NVIDIA GPU 时，Citrix 软件图形进程 (Ctxgfx.exe) 可能会意外退出。使用高分辨率屏幕时会出现此问题。[#LC8435]
- VDA for Server OS 上的 TDICA.sys 可能会遇到致命异常，并显示蓝屏。[#LC8708]
- VDA 上的 picadm.sys 可能遇到致命异常，并显示蓝屏和错误检测代码 0x22。[#LC8749]
- 在重新启动 VDA 后首次登录时，可能会出现意外访问冲入异常。Citrix 软件图形进程 (Ctxgfx.exe) 将意外退出。因此，VDA 中显示的图像和文本的质量可能会非常模糊。[#LC9005]

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

- 在下列一种情况下，Windows 资源管理器可能会异常关闭：
  - 选择大量文件且文件名中包含的字符数超过 260，然后选择**发送至** > **传真收件人**选项时。
  - 尝试打开第三方应用程序。
  - 尝试使用 Nitro PDF 合并文件时。[#LC9076]

用户体验

- 复制客户端上运行的应用程序中的内容并将其粘贴到用户会话中时，该内容可能不会被粘贴。此外，**粘贴**按钮可能处于禁用状态。[#LC8516]
- 尝试登录以前锁定的会话之后，带登录提示的屏幕可能无法刷新。[#LC8774]

用户界面

- 即使将“桌面墙纸”策略设置为“禁止”，也会出现桌面墙纸。[# LC8398]
- 用于检查 Linux VDA 的会话显示的某些第三方应用程序可能不会显示所有像素。[#LC8419]

其他

- 此修复解决了 Enlightened Data Transport (EDT) 的次要性能和质量改进问题。[#LC9278]

VDA for Server OS

HDX MediaStream Windows Media 重定向

- 禁用了 HDX MediaStream Windows Media 重定向时，尝试通过 Windows Media Player 打开某些视频文件格式可能会导致正在播放的视频垂直翻转。[#LC9194]

HDX RealTime

- 安装 RealTime Connector。使用利用重定向的网络摄像机的应用程序时（例如 Skype for Business），可能会在初始会话启动过程中重定向和检测 VDA for Desktop OS 中安装的网络摄像机。但是，当您重新连接到用户会话时，将无法再检测到该网络摄像机。用户设备上未安装 RealTime Media Engine 时会出现此问题。[#LC8793]

键盘

- 在 Android 设备上启动应用程序时，如果您的光标在文本字段中，可能不会自动显示键盘。此外，必须始终触摸键盘按钮进行打开或关闭。[#LC8936]

打印

- 尝试使用 Microsoft Word 通过打印机设置在纸张双面打印可能会失败。[#LC7501]
- 尝试从 Microsoft Internet Explorer 的已发布实例打印文档可能会失败。[#LC8093]
- 如果法语是 VDA 上安装的显示语言，尝试打印文档可能会失败。[#LC8209]
- 启动第一个会话过程中停止打印后台处理程序服务时，尝试重新启动 Citrix Print Manager 服务 (cpsvc.exe) 可能会失败。[#LC9192]

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

服务器/站点管理

- 如果多个域中有两个或更多同名的组，当 VDA 检查用户的组成员身份时，Citrix Stack Control Service (SCService64.exe) 可能会意外退出。在 DS_DOMAIN_TRUSTSW 结构中字符串“DnsDomainName”为空时，会出现此问题。[# LC8484]

会话/连接

- 启动 XenApp 7.6 长期服务版本 Cumulative Update 2 VDA for Server OS 或早期版本时，以下警告消息可能会在系统事件日志中显示：

  “尝试连接 SemsService 失败，错误代码为 0x2。” [#LC6311]

- 从已映射客户端驱动器读取文件时，如果在客户端会话之外更改了旧的缓存文件长度，则可能会返回该文件长度。此外，对于删除的任何字符，会插入空字符。

  要启用此修复，请将以下注册表值设置为“0”：

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters
  名称：CacheTimeout
  类型：REG_DWORD
  值：默认值为 60 秒。如果 CacheTimeOut 设置为“0”，则会立即重新加载文件长度，否则会在定义的超时之后进行加载。
  [#LC6314]

- 在取消停靠便携式计算机后，会话共享可能会失败。在客户端自动重新连接期间触发无序通知时，VDA 向 Delivery Controller 重新注册，此时会出现此问题。[# LC7450]

- 使用旧图形模式时，VDA for Desktop OS 上运行的会话可能会变得无响应。出现此问题时，您可能无法更新 Desktop Viewer 上的任何内容，但 Desktop Viewer 不处于无响应状态。此外，30-60 分钟后，以前无响应的会话将恢复。
  [#LC7777]

- 关闭 VDA 上安装的 App-V 客户端中的已发布应用程序后，如果在会话中启用了配置设置“EnablePubilishingRefreshUI”和“会话延迟”，iOS 设备上的一个黑色窗口可能会保留在打开状态。会话处于主动延迟状态时会出现此问题。[#LC8080]

- 在启用了会话延迟的情况下启动应用程序时，会话可能会在应用程序出现后注销。[# LC8245]

- 服务器上的 RPM.dll 可能会变得无响应，并显示以下错误消息：

  “错误 ID 1009，picadm: 等待来自客户端的响应消息超时”[#LC8339]

- 在下列一种情况下，Windows 资源管理器可能会异常关闭：

  - 选择大量文件且文件名中包含的字符数超过 260，然后选择“发送至 > 传真收件人”选项。
  - 尝试打开第三方应用程序。
  - 尝试使用 Nitro PDF 合并文件。[#LC8423]
- Citrix Director 可能会遇到多个连接失败问题。每位用户都使用分配的用于控制应用程序的有限可见性的组的展开时会出现此问题。此展开过程需要很长时间才能完成，并且可以在包含许多跨多个域的组的网络中观察到。[#LC8652]

- COM 端口在版本为 7.15 的 VDA 上可能无法映射。[#LC8656]

- 尝试启动 Microsoft Windows Server 2012 或 2016 中运行的已发布应用程序时，您可能会被锁定。[#LC8681]

- 在多监视器环境中启动应用程序时，可能会显示包含两个监视器的登录横幅。使用单个监视器时，登录横幅窗口将在全屏模式下显示。[#LC8741]

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

- 启用了本地应用程序访问的情况下，如果尝试在 Microsoft Windows 10 上运行的已发布桌面上打开应用程序，这些应用程序将无法最小化。[#LC8813]
- 将用户设备连接到 VDA 时，桌面可能不会显示。相反，桌面上将显示一个灰色屏幕。[#LC8821]
- DLP 软件可能无法扫描包含 UNC 链接的文件。[#LC8893]
- 启动已发布的应用程序后，Num Lock 键不起作用。当 Num Lock 键的 LED 指示灯在用户设备上可见，但数字在用户会话中不起作用时，将出现此问题。在某些情况下，当客户端请求的 LED 更新的时间早于新创建的远程桌面初始化其 LED 状态的时间时，将出现此问题。出现这种情况时，WinsStation 可能不更新其 LED 状态，LED 状态在端点与 VDA 之间将不同步。[#LC8921]
- 尝试启动应用程序和桌面可能会失败。VDA for Server OS 变得无响应时将出现此问题。

  要启用此修复，请设置以下注册表项：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard
  名称：EnableSCardHookVcResponseTimeout
  类型：DWORD
  值：1 [#LC8969]
- 尝试打开 VM 托管应用程序可能会失败。[#LC9001]
- 在会话中使用 WFAPI SDK **WFQuerySessionInformation** 命令获取安装的 VDA 版本信息时，该命令可能不起作用。[#LC9041]
- 从版本 7.14 到 7.15 升级 XenApp 和 XenDesktop 后，尝试在已发布的应用程序的选项卡之间切换可能会导致应用程序变得无响应。此外，如果将无缝窗口的大小调整到较小的大小，然后展开窗口，则需要一段时间才能绘制该窗口内的所有元素。[#LC9078]
- 启动应用程序后，已发布的应用程序可能会立即间歇性关闭。[#LC9167]
- 重新连接到 Millennium 套件中屏幕分辨率与初始连接不同的无缝应用程序时，该应用程序可能会错误地调整大小。因此，该窗口可能会被截断。[#LC9214]
- 尝试从 Citrix Receiver for Mac 启动应用程序可能会失败。无法提取客户端许可证 (LicenseRequestClientLicense) 时会出现此问题。[#LC9286]

智能卡

- 使用智能卡时，某些第三方应用程序可能会变得无响应，而非显示 PIN 提示。[#LC8805]

系统异常

- 服务器上的 picadm.sys 可能发生致命异常，并显示蓝屏和错误检测代码 0x22。[#LC6177]
- 服务器上的 picadm.sys 可能发生致命异常，并显示蓝屏和错误检测代码 0x00000050 (PAGE_FAULT_IN_NONPAGED_AREA)。[#LC6985]
- 服务器上的 picadm.sys 可能发生致命异常，并显示蓝屏和错误检测代码 0x22。[#LC7574]
- 服务主机 (svchost.exe) 进程可能会遇到访问冲突并意外退出。icaendpoint.dll 模块出错导致出现此问题。[#LC7694]

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

- 服务器上的 vdtw30.dll 可能会遇到致命异常，并显示蓝屏和停止代码 SYSTEM_SERVICE_EXCEPTION (3b)。[#LC8087]
- 服务器上的 pdcrypt2.sys 可能发生致命异常，并显示蓝屏和错误检测代码 0x3B。启动 VDA 时会出现此问题。[#LC8328]
- 在启用了 HDX 3D Pro 和 GPU 硬件编码的情况下使用 NVIDIA GPU 时，Citrix 软件图形进程 (Ctxgfx.exe) 可能会意外退出。使用高分辨率屏幕时会出现此问题。[#LC8435]
- 服务器上的 icardd.dll 可能会遇到致命异常，并显示蓝屏和错误检测代码 0x0000003B。[#LC8492]
- VDA for Server OS 上的 TDICA.sys 可能会遇到致命异常，并显示蓝屏。[#LC8708]
- 服务器上的 icardd.dll 可能会遇到致命异常，并显示蓝屏和错误检测代码 0x0000003B。[#LC8732]
- VDA 上的 picadm.sys 可能遇到致命异常，并显示蓝屏和错误检测代码 0x22。[#LC8749]
- 在重新启动 VDA 后首次登录时，可能会出现意外访问冲入异常。Citrix 软件图形进程 (Ctxgfx.exe) 将意外退出。因此，VDA 中显示的图像和文本的质量可能会非常模糊。[#LC9005]
- 在下列一种情况下，Windows 资源管理器可能会异常关闭：
  - 选择大量文件且文件名中包含的字符数超过 260，然后选择**发送至** > **传真收件人**选项时。
  - 尝试打开第三方应用程序。
  - 尝试使用 Nitro PDF 合并文件时。[#LC9076]

用户体验

- 复制客户端上运行的应用程序中的内容并将其粘贴到用户会话中时，该内容可能不会被粘贴。此外，**粘贴**按钮可能处于禁用状态。[#LC8516]
- 在 VDA for Server OS 上，鼠标光标可能会从会话中消失。光标变为**文本选择**光标并且背景色与**文本选择**光标的颜色相同时会出现此问题。Microsoft Windows 中的可编辑区域的默认背景色为白色，而默认**文本选择**光标颜色也是白色。因此，光标可能不再可见。[#LC8807]
- 会话登录过程中，即使提交正确的凭据后，Microsoft Windows 也可能会继续保留可编辑的密码字段。[#LC9407]

用户界面

- 即使将“桌面墙纸”策略设置为“禁止”，也会出现桌面墙纸。[# LC8398]
- 用于检查 Linux VDA 的会话显示的某些第三方应用程序可能不会显示所有像素。[#LC8419]

其他

- 此修复解决了 Enlightened Data Transport (EDT) 的次要性能和质量改进问题。[#LC9278]

其他

禁用或停止了 Citrix Telemetry Service，并使用 metainstaller 将 XenApp 和 XenDesktop 7.15 LTSR 升级到累积更新 1 (CU1) 时，可能会显示以下警告消息：

我们无法启动使您能够在 Call Home 中注册的 Citrix 服务。有关指导，请参阅 CTX218094。[#LCM-3642]

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

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

Cumulative Update 1 (CU1)

Apr 18, 2018
发布日期：2017 年 12 月 5 日

关于此版本

XenApp 和 XenDesktop 7.15 LTSR 累积更新 1 (CU1) 修复了自 7.15 LTSR 的初始版本起报告的 80 多个问题。

7.15 LTSR（常规信息）

自 XenApp 和 XenDesktop 7.15 LTSR（初始版本）起已修复的问题

本版本中的已知问题

从 7.6 LTSR CU5 升级之前...

从 7.6 LTSR CU5 升级到 7.15 LTSR CU1 的主要优势是基础 7.15 LTSR 中包含比基础 7.6 LTSR 中更多的功能。但是，如果考虑执行此升级，则建议 7.6 LTSR CU5 中包含的一小部分修复不要存在于 7.15 LTSR CU1 中。这是因为 7.15 LTSR CU1 是在 7.6 LTSR CU5 之前发布的。有关适用于 7.15 但不包含在 7.15 LTSR CU1 中的修复列表，请参阅存在于 7.6 LTSR CU5 中但不存在于 7.15 LTSR CU1 中的修复列表。如果您的部署基于 7.6 LTSR CU5 中包含的特定修复，Citrix 建议您在升级之前核对此列表。

新建部署

如何从头开始部署 CU1？

您可以设置基于 CU1 的全新 XenApp/XenDesktop 环境（通过使用 CU1 Metainstaller）。在此之前，建议您熟悉产品：

请仔细阅读 XenApp 和 XenDesktop 7.15 LTSR（初始版本）部分，并特别注意技术概述、安装和配置以及安全部分，然后再开始规划您的部署。请确保您的设置满足所有组件的系统要求。

现有部署

如何更新？

CU1 提供 7.15 LTSR 的 13 个基础组件的更新。请记住：Citrix 建议您将您的部署中的所有 LTSR 组件更新到 CU1。例如：如果您的 LTSR 部署中包含 Provisioning Services，请将 Provisioning Services 组件更新到 CU1。如果 Provisioning Services 不属于您的部署的一部分，则不需要安装或更新该组件。

XenApp 和 XenDesktop 7.15 LTSR CU1 基础组件

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

7.15 LTSR CU1 Baseline Component	Version	Notes
VDA for Desktop OS	7.15.1000	
VDA for Server OS	7.15.1000	
Delivery Controller	7.15.1000	
Citrix Studio	7.15.1000	
Citrix Director	7.15.1000	
组策略管理体验	3.1.1000	
StoreFront	3.12.1000	
Provisioning Services	7.15.1	
通用打印服务器	7.15.1000	
会话录制	7.15.1000	仅限 Platinum Edition
Linux VDA	7.15.1000	有关受支持的平台，请参阅 Linux VDA 文档
Profile Management	7.15.1000	
联合身份验证服务	7.15.1000	

XenApp 和 XenDesktop 7.15 LTSR CU1 兼容组件

建议您在 7.15 LTSR CU1 环境中使用以下组件。这些组件无权享有 LTSR 的优势（扩展的生命周期以及仅用于修复的累积更新）。Citrix 可能会要求您在 7.15 LTSR CU1 环境中升级到这些组件的较新版本。

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

7.15 LTSR Compatible Components and Platforms	Version
AppDNA	7.16
Citrix SCOM Management Pack for License Server	1.2
Citrix SCOM Management Pack for Provisioning Services	1.19
Citrix SCOM Management Pack for StoreFront	1.13
Citrix SCOM Management Pack for XenApp and XenDesktop	3.14
HDX RealTime Optimization Pack	2.2.100
许可证服务器	11.14.0.1 Build 22103
工作区环境管理	4.4
App Layering	4.6
自助服务密码重置	1.1

Citrix Receiver 的兼容版本

为简化维护过程以及确保实现最佳性能，Citrix 建议您在最新版本的 Citrix Receiver 可用时随时升级到相应版本。可以从 https://www.citrix.com/downloads/citrix-receiver.html 下载最新版本。为方便起见，请考虑订阅 Citrix Receiver RSS 源以在新版本的 Citrix Receiver 可用时接收通知。

请注意，Citrix Receiver 无法享有 XenApp 和 XenDesktop LTSR 的优势（扩展的生命周期和仅用于修复的累积更新）。Citrix 可能会要求您在 7.15 LTSR CU1 环境中升级到 Citrix Receiver 的较新版本。如果使用的是 Citrix Receiver for Windows，Citrix 已公布特殊的 LTSR 计划。可以从 Citrix Receiver 的生命周期里程碑页面获取有关该计划的详细信息。

特别需要指出的是，7.15 LTSR CU1 支持以下版本的 Citrix Receiver 以及之后的所有版本。

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

LTSR Compatible Version of Citrix Receiver	Version
Citrix Receiver for Android	3.12.3 或更高版本
Citrix Receiver for Chrome	2.5.2 或更高版本
Citrix Receiver for HTML5	2.5.2 或更高版本
Citrix Receiver for iOS	7.3.1 或更高版本
Citrix Receiver for Linux	13.7 或更高版本
Citrix Receiver for Mac	12.7 或更高版本
Citrix Receiver for UWP (通用 Windows 平台)	1.0.5 或更高版本
Citrix Receiver for Windows	4.9 或更高版本

XenApp 和 XenDesktop 7.15 LTSR 值得注意的排除项

以下功能、组件和平台无法享有 7.15 LTSR 的生命周期里程碑和优势。需要特别指出的是，累积更新和扩展生命周期优势被排除在外。可以通过常规的最新版本获取扩展功能和组件的更新。

Excluded Features
Framehawk
StoreFront Citrix Online 集成

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

Excluded Components
Personal vDisk： • Windows 10 计算机除外。 • 对于 Windows 7 计算机，提供有限的 LTSR 支持，直至 2020 年 1 月 14 日（适用 CU 要求）
AppDisk

Excluded Windows Platforms *
Windows 2008 32位（面向通用打印服务器）

* Citrix 保留根据第三方供应商的生命周期里程碑更新平台支持的权利。

安装和升级分析

当您使用完整产品安装程序部署或升级 XenApp 或 XenDesktop 组件时，将在安装/升级组件的计算机上收集和存储有关安装过程的匿名信息。这些数据用于帮助 Citrix 改善其客户的安装体验。有关详细信息，请参阅 http://more.citrix.com/XD-INSTALLER。

XenApp 6.5 迁移

XenApp 6.5 迁移过程有助于高效快速地从 XenApp 6.5 场过渡到运行 XenApp 7.15 LTSR CU1 的站点。这在部署中包含大量应用程序和 Citrix 组策略时很有用，可以降低手动将应用程序和 Citrix 组策略移至新 XenApp 站点时意外引入错误的风险。

安装 XenApp 7.15 LTSR CU1 核心组件并创建站点后，迁移过程按照以下顺序进行：

- 在每个 XenApp 6.5 工作进程上运行 XenApp 7.15 CU1 安装程序，将其自动升级到新 Virtual Delivery Agent for Server OS 以便在新站点中使用。
- 在 XenApp 6.5 Controller 上运行 PowerShell 导出 cmdlet，以将应用程序和 Citrix 策略设置导出至 XML 文件。
- 编辑 XML 文件（如果需要），以细化要导入到新站点的内容。通过自定义这些文件，可以将策略和应用程序设置分阶段导入到 XenApp 7.15 LTSR CU1 站点：即一些现在导入，其他稍后导入。
- 在新 XenApp 7.15 LTSR CU1 Controller 上运行 PowerShell 导入 cmdlet，以将 XML 文件中的设置导入新 XenApp 站点。

根据需要重新配置新站点，然后对其进行测试。

有关详细信息，请参阅迁移 XenApp 6.x。

存在于 7.6 LTSR CU5 中但不存在于 7.15 LTSR CU1 中的修复列表

如果考虑从 7.6 LTSR CU5 升级到 7.15 LTSR CU1，则建议 7.6 LTSR CU5 中包含的一小部分修复不要存在于 7.15 LTSR CU1 中。如果您的部署基于 7.6 LTSR CU5 中包含的特定修复，Citrix 建议您在升级之前核对此列表。

LC6311

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

LC6985
LC7430
LC7450
LC7574
LC7600
LC7777
LC7911
LC8046
LC8080
LC8130
LC8170
LC8281
LC8339
LC8492
LC8732
LC8750
LC8774

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

已修复的问题

Apr 18, 2018

XenApp 和 XenDesktop 7.15 LTSR 累积更新 1 (CU1) 修复了自 7.15 LTSR 的初始版本起报告的 80 多个问题：

Citrix Director

- 打开 Director 控制台并首次搜索用户时，不显示加载条。在后续搜索中，加载条按预期显示。[# LC8190]

Citrix 策略

- 尝试向 Active Directory 中的用户策略添加新 USB 重定向规则可能会失败。滚动条不可用时会出现此问题。[#LC8112]
- 尝试管理“打印机分配”策略时，可能会出现以下问题：
  - 添加或编辑打印机分配策略时，出现异常“InvalidCastException”。
  - 添加新会话打印机时，出现异常“InvalidOperationException”。
  - 尝试从打印机分配策略中删除会话打印机失败。“删除”选项处于禁用状态时会出现此问题。
  - 在“打印机分配”策略的搜索框中停止键入时，搜索操作不会开始。
  - 会话打印机替代设置复选框（“PrintQuality”、“PaperSize”、“Scale”和“TrueTypeOption”）始终处于选中状态，即使您以前取消选中这些复选框亦如此。[#LC8146]

Citrix Studio

- 尝试向交付组中添加用户分配的计算机时，未分配的计算机可能会显示在“计算机分配”页面中。[#LC6755]
- 尝试访问 Citrix Studio 中的计算机目录会导致 Citrix Studio 意外退出并出现以下异常：

  “错误 ID: XDDS:ABB14FD9”[#LC7961]
- 在非英语版本的 Windows 操作系统中运行的“添加连接和资源”向导中的“使用虚拟机管理程序的本地存储”选项的文本可能会被截断。[#LC8041]
- 将 Citrix Studio 升级到版本 7.14.1 后，现有 App-V 软件包的“使用者”列（指使用应用程序的交付组）可能显示为空白。[# LC8075]
- 单击 Citrix Studio 中的交付组超链接时，可能会被重定向到选定的交付组节点。[#LC8095]
- 尝试管理“打印机分配”策略时，可能会出现以下问题：
  - 添加或编辑打印机分配策略时，出现异常“InvalidCastException”。
  - 添加新会话打印机时，出现异常“InvalidOperationException”。
  - 尝试从打印机分配策略中删除会话打印机失败。“删除”选项处于禁用状态时会出现此问题。
  - 在“打印机分配”策略的搜索框中停止键入时，搜索操作不会开始。
  - 会话打印机替代设置复选框（“PrintQuality”、“PaperSize”、“Scale”和“TrueTypeOption”）始终处于选中状态，即使您以

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

前取消选中这些复选框亦如此。[#LC8146]

- 将 Delivery Controller 升级到版本 7.15 后，尝试在 Delivery Controller 上启动 Citrix Studio 可能会失败，并显示以下错误消息：

  “MissingMandatoryParameter,Citrix.Licensing.Admin.SDK.Commands.GetLicAlertsCommand”
  [#LC8396]

- 在 Citrix Studio 中选择交付组节点，然后选择“应用程序”选项卡时，“应用程序”选项卡中的超链接可能不起作用。[#LC8555]

Controller

- 如果某个交付组包含多个处于维护模式的 VDA，您可能无法选择该交付组来启动已发布的应用程序。[#LC6943]
- 更新使用 Machine Creation Services (MCS) 创建的计算机目录后，在 vSAN 6 或更高版本上托管的虚拟机可能无法启动。VMware 控制台上显示以下错误消息：

  “A general system error occurred: PBM error occurred during PreProcessReconfigureSpec: pbm.fault.PBMFault; Error when trying to run pre-provision validation; Invalid entity.”（出现常规系统错误: 在执行 PreProcessReconfigureSpec 期间出现 PBM 错误: pbm.fault.PBMFault；尝试运行预置备验证时出现错误；实体无效。）[#LC7860]

- 尝试访问 Citrix Studio 中的计算机目录会导致 Citrix Studio 意外退出并出现以下异常：

  “错误 ID: XDDS:ABB14FD9”[#LC7961]

- Citrix Director 可能会在每小时的前几分钟显示不正确的断开连接会话数。[#LC8006]
- 面向服务器操作系统中的会话的“AllowRestart”策略不允许您从断开连接的会话中注销。重新启动断开连接的会话时，该会话将重新连接到以前的会话，而非启动新会话。[#LC8090]
- 尝试管理“打印机分配”策略时，可能会出现以下问题：
  - 添加或编辑打印机分配策略时，出现异常“InvalidCastException”。
  - 添加新会话打印机时，出现异常“InvalidOperationException”。
  - 尝试从打印机分配策略中删除会话打印机失败。“删除”选项处于禁用状态时会出现此问题。
  - 在“打印机分配”策略的搜索框中停止键入时，搜索操作不会开始。
  - 会话打印机替代设置复选框（“PrintQuality”、“PaperSize”、“Scale”和“TrueTypeOption”）始终处于选中状态，即使您以前取消选中这些复选框亦如此。[#LC8146]
- Monitoring Service 可能无法向监视数据库中插入新会话数据。[#LC8191]
- **Director** > **趋势** > **登录性能**下的“登录持续时间(按用户会话)”面板可能仅显示部分登录记录。[#LC8265]
- 将 Delivery Controller 升级到版本 7.15 后，尝试在 Delivery Controller 上启动 Citrix Studio 可能会失败，并显示以下错误消息：

  “MissingMandatoryParameter,Citrix.Licensing.Admin.SDK.Commands.GetLicAlertsCommand”
  [#LC8396]

- 在大型 XenApp 和 XenDesktop 环境中，如果监视数据库的大小非常大，监视数据库整理的存储过程将无法正确运行。[#LC8770]

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

HDX MediaStream Flash 重定向

- 在启用了 HDX MediaStream Flash 重定向的情况下，Flash 视频可能无法在 MSN.com 和 News.com 上播放。[#LC6823]

Linux VDA

- 一段时间后，Linux VDA 可能会在 Delivery Controller 中注册并取消注册。[#LC8205]
- 用于检查 Linux VDA 的会话显示的某些第三方应用程序可能不会显示所有像素。[#LC8419]
- 存在多个 LDAP 服务器时，在更新了策略并且会话超时后，尝试在 Linux VDA 上启动应用程序可能会失败。[#LC8444]

Profile Management

- 尝试启动 Microsoft Windows 10 会话时，Profile Management 会导致显示黑屏。应用此修复后，必须配置策略“要同步的目录”并添加文件夹 *AppData\Local\Microsoft\Windows\Caches*。 [#LC7596]
- 从 Microsoft Windows 10 上运行的 VDA 中注销时，ntuser.dat 文件可能正在使用中，不会被复制到 Profile Management 存储中。因此，对“HKEY_CURRENT_USER”注册表项所做的更改将丢失。[#LC8068]
- 启用了“注销时删除本地缓存的配置文件”策略，并且“删除缓存的配置文件之前的延迟”设置为 2 分钟时，尝试使用相同的帐户在 2 分钟内注销和登录会话可能会创建一个新的本地配置文件。[#LC8388]

Provisioning Services

StoreFront

- 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]
- 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

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

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]

- 在启用了套接字池的情况下，如果站点数据库连接不一致，则当您连续登录并注销时，StoreFront 中的套接字可能会用尽。[#LC8514]

VDA for Desktop OS

HDX MediaStream Flash 重定向

- 在启用了 HDX MediaStream Flash 重定向的情况下，Flash 视频可能无法在 MSN.com 和 News.com 上播放。[#LC6823]
- 尝试保存 Microsoft Office 文件（例如在启用了 HDX 无缝应用程序中运行的 Microsoft Excel 电子表格）会导致文件意外退出。[#LC8572]

HDX Plug and Play

- 为多个设备（例如 Syn-Tech ProKee V2）报告相同的序列号的 USB 设备可能不会被重定向到 VDA 会话。将显示以下 CDF 跟踪：

  “Failed to assign the instance ID, error 0xc000000d.”（无法分配实例 ID，错误 0xc000000d。）[#LC8264]

打印

- 已发布的应用程序等待 Citrix Print Manager Service (cpsvc.exe) 中的 mutex 对象时，尝试启动该应用程序可能会失败。[#LC6829]
- Citrix Print Manager Service (CpSvc.exe) 可能会间歇性退出。[#LC7535]
- 在客户端之间漫游会话时，无法删除会话打印机。例如，配置策略“打印机分配”时（打印机 A 分配给客户端 A，打印机 B 分配给客户端 B），如果从客户端 A 漫游到客户端 B，则可能无法删除打印机 A。[#LC8077]

服务器/站点管理

- 在 VDA 7.12 或更高版本中，尝试通过在注册表项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI 下将无缝标志设置为“0x00040000”（禁用语言栏代理）来禁止在无缝会话中显示语言栏时，语言不再隐藏。[#LC8349]

会话/连接

- 在启用了本地应用程序访问的情况下，使用交互登录免责声明策略可能会导致出现黑屏或灰屏并持续 45 秒。[#LC6518]
- 尝试重新连接到应用程序可能会失败。会话最初断开连接时，任何断开连接的应用程序会变得无响应，此时会出现此问题。[# LC6550]
- 使用 HDX 3D Pro 锁定双监视器会话时，仅锁定主监视器。[#LC7767]
- 建立 Skype for Business 视频通话时，与第三方应用程序的窗口相交后可能会显示一个蓝色的窗口边框。[#LC7773]
- 在启用了本地应用程序访问的情况下，使用交互式登录免责声明策略可能会导致出现黑屏或灰屏。[#LC7798]

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

- 最大化时，某些已发布的应用程序可能不会覆盖整个屏幕。[#LC7854]
- 在版本 7.9 VDA 上运行的两个 Microsoft Excel 2010 工作表之间执行插入操作时，Excel 窗口可能会变得无响应。[#LC7912]
- 在某些情况下，无缝应用程序可能不会在无缝模式下显示，或者某些功能可能不起作用。[#LC8030]
- 登录屏幕显示时，如果在 VDA 上启用了 HDX 3D Pro，并且启用了策略“Message text for users attempting to log on”（向尝试登录的用户显示的文本），尝试启动已发布的桌面可能会失败，并显示灰屏。

  要启用此修复，请设置以下注册表项：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\BitmapRemotingConfig
  名称：HKLM_DisableMontereyFBCOnInit
  值：DWORD
  类型：1（表示启用）[#LC8082]
- 在启用了本地应用程序访问的情况下，连接到 VDA 时，使用交互式登录免责声明策略会导致桌面查看器显示灰屏。[#LC8136]
- 使用利用重定向的网络摄像机的应用程序时（例如 Skype for Business 或 VLC 媒体播放器），可能会在初始会话启动的过程中重定向和检测该网络摄像机。但是，当您重新连接到用户会话时，将无法再检测到该网络摄像机。相反，将显示一个灰色屏幕，而非视频预览。[#LC8588]

智能卡

- 使用智能卡登录某个会话时，该会话可能会变得无响应，直至您断开并重新连接会话。[#LC8036]

系统异常

- wfshell.exe 进程可能会意外退出，指向任务栏分组模块。[#LC6968]
- 在启用了 USB 重定向策略的情况下，VDA 可能发生致命异常，并显示蓝屏和错误检测代码 SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)。[#LC7999]
- VDA 可能会遇到致命异常，显示蓝屏和错误检测代码 0x7E。将 VDA 会话保持空闲状态一段时间时会出现此问题。[#LC8045]
- 服务器上的 picavc.sys 可能发生致命异常，并显示蓝屏和错误检测代码 SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)。[#LC8063]

用户体验

- 重新连接到无缝应用程序会话时，应用程序窗口可能不会在客户端正确显示。相反，将在客户端上的一个小长方形中绘制会话图形。[#LC7857]
- Windows Media Player 可能会将 Microsoft AVI (.avi) 文件格式显示为垂直翻转。[#LC8308]
- 在第三个显示器上将已发布的应用程序最大化时，该应用程序可能不会覆盖整个屏幕。而是显示一个黑色边框。[#LC8472]
- 在移动应用程序窗口过程中，VDA 7.15 上托管的无缝应用程序可能会在后台显示一个灰色或黑色方框。[#LC8551]

用户界面

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

- 如果在 Excel 2010 中打开一个包含多个工作簿的电子表格，任务栏将仅显示最新的工作簿。[#LC7557]

VDA for Server OS

HDX MediaStream Flash 重定向

- 尝试保存 Microsoft Office 文件（例如在启用了 HDX 无缝应用程序中运行的 Microsoft Excel 电子表格）会导致文件意外退出。[#LC8572]

HDX Plug and Play

- 为多个设备（例如 Syn-Tech ProKee V2）报告相同的序列号的 USB 设备可能不会被重定向到 VDA 会话。将显示以下 CDF 跟踪：

  “Failed to assign the instance ID, error 0xc000000d.”（无法分配实例 ID，错误 0xc000000d。）[#LC8264]

打印

- 已发布的应用程序等待 Citrix Print Manager Service (cpsvc.exe) 中的 mutex 对象时，尝试启动该应用程序可能会失败。[#LC6829]
- Citrix Print Manager Service (CpSvc.exe) 可能会间歇性退出。[#LC7535]
- 在客户端之间漫游会话时，无法删除会话打印机。例如，配置策略“打印机分配”时（打印机 A 分配给客户端 A，打印机 B 分配给客户端 B），如果从客户端 A 漫游到客户端 B，则可能无法删除打印机 A。[#LC8077]

服务器/站点管理

- 在 VDA 7.12 或更高版本中，尝试通过在注册表项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI 下将无缝标志设置为“0x00040000”（禁用语言栏代理）来禁止在无缝会话中显示语言栏时，语言不再隐藏。[#LC8349]

会话/连接

- 尝试重新连接到应用程序可能会失败。会话最初断开连接时，任何断开连接的应用程序会变得无响应，此时会出现此问题。[# LC6550]
- 在会话启动的进度条上单击“取消”时，错误的会话信息可能会保留在 Delivery Controller 中。因此，将不在 VDA 上创建实际的会话，并且您可能无法启动新会话。[#LC6779]
- 即使在将“客户端麦克风重定向”策略之设置为“禁止”时，也可能会在用户会话中间歇性重定向麦克风。

  此修复解决了该问题。但是，如果您仍遇到该问题，请在配有麦克风的设备上应用以下注册表项：

  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ica-tcp\AudioConfig
    名称：MaxPolicyAge
    类型：DWORD
    值：允许上次策略评估时间与端点激活时间之间间隔的最长时间（秒）。默认值为 30 秒。
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ica-tcp\AudioConfig
    名称：PolicyTimeout
    类型：DWORD

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

值：确定策略非最新后系统等待策略的最长时间（单位为毫秒）。默认为 4,000 毫秒。出现超时时，系统将读取策略并继续进行初始化。将此值设置为 (0) 将跳过 Active Directory 策略检查并立即处理策略。[#LC7495]

- 建立 Skype for Business 视频通话时，与第三方应用程序的窗口相交后可能会显示一个蓝色的窗口边框。[#LC7773]
- 最大化时，某些已发布的应用程序可能不会覆盖整个屏幕。[#LC7854]
- 使用 vGPU 时升级到 VDA 版本 7.13、7.14 或 7.15 后，可能会在 Microsoft Windows Server 操作系统中运行的已发布应用程序或桌面上显示一个黑色区域。[#LC7875]
- 在版本 7.9 VDA 上运行的两个 Microsoft Excel 2010 工作表之间执行插入操作时，Excel 窗口可能会变得无响应。[#LC7912]
- 在某些情况下，无缝应用程序可能不会在无缝模式下显示，或者某些功能可能不起作用。[#LC8030]
- 在启用了本地应用程序访问的情况下，连接到 VDA 时，使用交互式登录免责声明策略会导致桌面查看器显示灰屏。[#LC8136]
- 向 Delivery Controller 发送无序通知时，VDA for Server OS 可能会间歇性重新注册。[#LC8228]
- 使用利用重定向的网络摄像机的应用程序时（例如 Skype for Business 或 VLC 媒体播放器），可能会在初始会话启动的过程中重定向和检测该网络摄像机。但是，当您重新连接到用户会话时，将无法再检测到该网络摄像机。相反，将显示一个灰色屏幕，而非视频预览。[#LC8588]

智能卡

- 使用智能卡登录某个会话时，该会话可能会变得无响应，直至您断开并重新连接会话。[#LC8036]

系统异常

- wfshell.exe 进程可能会意外退出，指向任务栏分组模块。[#LC6968]
- 单击任务栏上的音量控件时，Windows Shell Experience Host 可能会意外退出。[# LC7000]
- 服务主机 (svchost.exe) 进程可能会遇到访问冲突并意外退出。icaendpoint.dll 模块出错导致出现此问题。[#LC7900]
- 在启用了 USB 重定向策略的情况下，VDA 可能发生致命异常，并显示蓝屏和错误检测代码 SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)。[#LC7999]
- 服务器上的 picavc.sys 可能发生致命异常，并显示蓝屏和错误检测代码 SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)。[#LC8063]

用户体验

- 重新连接到无缝应用程序会话时，应用程序窗口可能不会在客户端正确显示。相反，将在客户端上的一个小长方形中绘制会话图形。[#LC7857]
- Windows Media Player 可能会将 Microsoft AVI (.avi) 文件格式显示为垂直翻转。[#LC8308]
- 在第三个显示器上将已发布的应用程序最大化时，该应用程序可能不会覆盖整个屏幕。而是显示一个黑色边框。[#LC8472]
- 在移动应用程序窗口过程中，VDA 7.15 上托管的无缝应用程序可能会在后台显示一个灰色或黑色方框。[#LC8551]

用户界面

- 存在未保存数据的情况下，使用连接中心从无缝会话注销，会显示黑色窗口和以下消息：

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

“Programs still need to close”（程序仍需关闭） - 包含两个选项 - “Force Logoff”（强制注销）或“Cancel”（取消）。“Cancel”（取消）选项不起作用。

安装此修复后，“Cancel”（取消）选项可按预期工作。[#LC6075]

- 如果在 Excel 2010 中打开一个包含多个工作簿的电子表格，任务栏将仅显示最新的工作簿。[#LC7557]
- 尝试从 Microsoft Windows Server 2008 R2 桌面会话中注销时，可能不会显示注销屏幕。您可能无法从会话中注销，但会话将显示为好像已意外断开连接。[#LC8016]

虚拟桌面组件 - 其他

- Citrix Director 可能会在每小时的前几分钟显示不正确的断开连接会话数。[#LC8006]
- Monitoring Service 可能无法向监视数据库中插入新会话数据。[#LC8191]
- **Director** > **趋势** > **登录性能**下的“登录持续时间(按用户会话)”面板可能仅显示部分登录记录。[# LC8265]
- 将 Microsoft Windows 10 从 Build 1511 升级到安装了 VDA 的 Build 1703 后，System Center Configuration Manager (SCCM) 客户端可能会意外退出。[#LC8632]
- 使用 Machine Creation Services (MCS) 时，Microsoft Office 2016 的重置可能会在 Microsoft Windows 10 中中断。[#LC8680]
- 在大型 XenApp 和 XenDesktop 环境中，如果监视数据库的大小非常大，监视数据库整理的存储过程将无法正确运行。[#LC8770]

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

7.15 LTSR（初始版本）

Apr 18, 2018

关于此版本

XenApp 和 XenDesktop 7.15 长期服务版本 (LTSR) 包括新版本的 Windows VDA 以及新版本的多个 XenApp 和 XenDesktop 核心组件。可以执行以下操作：

- **安装或升级 XenApp 或 XenDesktop 站点**

  在此版本中使用 ISO 安装或升级所有核心组件和 Virtual Delivery Agent。安装或升级到最新版本允许您使用所有最新功能。

- **在现有站点上安装或升级 VDA**

  如果您已部署 XenApp 或 XenDesktop，但尚未准备好升级核心组件，则仍可通过安装（或升级到）新的 VDA 来使用多个最新的 HDX 功能。如果要在非生产环境中测试增强功能，仅升级 VDA 通常会非常有用。

有关说明，请参阅准备安装或升级部署。

此版本的 XenApp 和 XenDesktop 下载页面还包括以下软件的更新版本。有关功能和安装说明的详细信息，请参阅相应组件的文档。

StoreFront

AppDNA

Citrix SCOM Management Pack for XenApp and XenDesktop

有关自 XenApp 和 XenDesktop 7.6 LTSR 版本起增加的功能的概览，请参阅 https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/xenapp-xendesktop-715-ltsr-feature-summary-comparison-to-76-ltsr.pdf。

本产品版本还包括自 XenApp 和 XenDesktop 7.14.1 起的以下新增功能、已修改的功能和增强功能。

未安装 Microsoft 媒体基础的计算机上的 VDA 安装

大多数受支持的 Windows 版本都已附带安装 Microsoft 媒体基础。如果要安装 VDA 的计算机上未安装媒体基础（例如 N 版本），多项多媒体功能将不安装并且无法运行。您可以在安装媒体基础后确认该限制，或者终止 VDA 安装并在以后重新启动。在图形界面中，此选项在消息中提供。在命令行中，可以使用 /no_mediafoundation_ack 选项确认该限制。

将 XenApp 6.5 工作进程升级到新 VDA

迁移 XenApp 6.5 场后，可以将 XenApp 6.5 工作进程升级到新 VDA。以前，在工作进程服务器上运行 XenApp 和 XenDesktop 安装程序会自动删除 XenApp 6.5 软件，然后安装新 VDA。现在，您将使用独立的进程先从服务器中删除 HRP7 和 XenApp 6.5 软件。然后，安装新 VDA。有关详细信息，请参阅将 XenApp 6.5 工作进程升级到新 VDA。

MCS 支持第 2 代 VM

使用 Microsoft System Center Virtual Machine Manager 提供 VM 时，您现在可以使用 Machine Creation Services (MCS) 置

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

备第 2 代 VM。

本地主机缓存

全新安装 XenApp 和 XenDesktop 的过程中，默认启用本地主机缓存。连接租用默认处于禁用状态。

升级后，本地主机缓存设置保持不变。例如，如果本地主机缓存在早期版本中处于启用状态，在升级后的版本中也会保持启用状态。如果本地主机缓存在早期版本中处于禁用状态（或不受支持），在升级后的版本中也会保持禁用状态。

Director

应用程序故障监视。Director 将“趋势”视图扩展为包括**应用程序故障**选项卡，以显示与已发布的应用程序关联的历史故障。可以查看选定时间段内启动或运行选定应用程序或进程时发生的故障和错误。此信息可帮助您理解应用程序特定的问题并对这些问题进行故障排除。有关详细信息，请参阅“对应用程序进行故障排除”中的历史应用程序故障监视。

默认监视服务器操作系统 VDA 上托管的应用程序故障。可以通过监视组策略修改监视设置：“启用应用程序故障的监视”、“在桌面操作系统 VDA 上启用应用程序故障的监视”以及“从故障监视中排除的应用程序列表”。有关详细信息，请参阅“监视策略设置”中的应用程序故障监视策略。

此功能要求 Delivery Controller 和 VDA 7.15 或更高版本。支持 Windows Vista 或更高版本上的桌面操作系统 VDA 以及 Windows Server 2008 或更高版本上的服务器操作系统 VDA。

Virtual Delivery Agent (VDA) 7.15

将 VDA 从版本 7.9、7.11、7.12、7.13 或 7.14 升级后，不需要更新计算机目录的功能级别。默认设置（7.9 (或更高版本)）保留当前功能级别。有关信息，请参阅 VDA 版本和功能级别。

Session Recording 7.15

适用于 Session Recording 的负载平衡：此实验性功能存在于 XenApp 和 XenDesktop 7.14 中，不包含在本版本中。

新建部署

如何从头开始部署 7.15 LTSR？

可以使用 7.15 LTSR 设置一个全新的 XenApp 或 XenDesktop 环境。* 开始执行该操作之前，我们建议您熟悉以下产品：

请仔细阅读 XenApp 和 XenDesktop 7.15 长期服务版本文档，并特别注意技术概述、安装和配置以及安全部分，然后再开始规划您的部署。请确保您的设置满足所有组件的系统要求。请按照安装和配置中的部署说明进行操作。

* 注意：Provisioning Services 和 Session Recording 作为单独的下载和安装程序提供。

现有部署

如何更新？

XenApp 和 XenDesktop 7.15 LTSR 提供 7.6 LTSR 的所有基础组件的更新。请记住：Citrix 建议您将您的部署中的所有 LTSR 组件更新到 7.15 LTSR。例如：如果您的 LTSR 部署中包含 Provisioning Services，请更新 Provisioning Services 组件。如果 Provisioning Services 不属于您的部署的一部分，则不需要安装或更新该组件。

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

自最初的 7.6 LTSR 版本起，添加了一个 metainstaller，允许您从单个统一界面中更新 LTSR 环境的现有组件。按照升级说明，使用 metainstaller 更新您的部署中的 LTSR 组件。

XenApp 和 XenDesktop 7.15 LTSR 基础组件

7.15 LTSR Baseline Component	Version	Notes
VDA for Desktop OS	7.15	
VDA for Server OS	7.15	
Delivery Controller	7.15	
Citrix Studio	7.15	
Citrix Director	7.15	
组策略管理体验	3.1	
StoreFront	3.12	
Provisioning Services	7.15	
通用打印服务器	7.15	
会话录制	7.15	仅限 Platinum Edition
Linux VDA	7.15	有关受支持的平台，请参阅 Linux VDA 文档
Profile Management	7.15	
联合身份验证服务	7.15	

XenApp 和 XenDesktop 7.15 LTSR 兼容组件

建议您在 7.15 LTSR 环境中使用以下组件。这些组件无权享有 LTSR 的优势（扩展的生命周期以及仅用于修复的累积更新）。Citrix 可能会要求您在 7.15 LTSR 环境中升级到这些组件的较新版本。

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

7.15 LTSR Compatible Components and Platforms	Version
AppDNA	7.15
Citrix SCOM Management Pack for License Server	1.2
Citrix SCOM Management Pack for Provisioning Services	1.19
Citrix SCOM Management Pack for StoreFront	1.12
Citrix SCOM Management Pack for XenApp and XenDesktop	3.13
HDX RealTime Optimization Pack	2.3
许可证服务器	11.14.0 Build 21103
工作区环境管理	4.4
App Layering	4.3
自助服务密码重置	1.1

Citrix Receiver 的兼容版本

为简化维护过程以及确保实现最佳性能，Citrix 建议您在最新版本的 Citrix Receiver 可用时随时升级到相应版本。可以从 https://www.citrix.com/downloads/citrix-receiver.html 下载最新版本。为方便起见，请考虑订阅 Citrix Receiver RSS 源以在新版本的 Citrix Receiver 可用时接收通知。

请注意，Citrix Receiver 无法享有 XenApp 和 XenDesktop LTSR 的优势（扩展的生命周期和仅用于修复的累积更新）。Citrix 可能会要求您在 7.15 LTSR 环境中升级到 Citrix Receiver 的较新版本。如果使用的是 Citrix Receiver for Windows，Citrix 已公布特殊的 LTSR 计划。可以从 Citrix Receiver 的生命周期里程碑页面获取有关该计划的详细信息。

特别需要指出的是，7.15 LTSR 支持以下版本的 Citrix Receiver 以及之后的所有版本。

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

LTSR Compatible Version of Citrix Receiver	Version
Citrix Receiver for Android	3.11.1 或更高版本
Citrix Receiver for Chrome	2.4 或更高版本
Citrix Receiver for HTML5	2.4 或更高版本
Citrix Receiver for iOS	7.2 或更高版本
Citrix Receiver for Linux	13.5 或更高版本
Citrix Receiver for Mac	12.5 或更高版本
Citrix Receiver for UWP (通用 Windows 平台)	1.0.5 或更高版本
Citrix Receiver for Windows	4.9 或更高版本

XenApp 和 XenDesktop 7.15 LTSR 值得注意的排除项

以下功能、组件和平台无法享有 7.15 LTSR 的生命周期里程碑和优势。需要特别指出的是，累积更新和扩展生命周期优势被排除在外。可以通过常规的最新版本获取扩展功能和组件的更新。

Excluded Features
Framehawk
StoreFront Citrix Online 集成

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

Excluded Components
Personal vDisk： • Windows 10 计算机除外。 • 对于 Windows 7 计算机，提供有限的 LTSR 支持，直至 2020 年 1 月 14 日（适用 CU 要求）
AppDisk

Excluded Windows Platforms *
Windows 2008 32位（面向通用打印服务器）

* Citrix 保留根据第三方供应商的生命周期里程碑更新平台支持的权利。

当您使用完整产品安装程序部署或升级 XenApp 或 XenDesktop 组件时，将在安装/升级组件的计算机上收集和存储有关安装过程的匿名信息。这些数据用于帮助 Citrix 改善其客户的安装体验。有关详细信息，请参阅 http://more.citrix.com/XD-INSTALLER。

XenApp 6.5 迁移

XenApp 6.5 迁移过程有助于高效快速地从 XenApp 6.5 场过渡到运行 XenApp 7.15 LTSR（或支持的更高版本）的站点。这在部署中包含大量应用程序和 Citrix 组策略时很有用，可以降低手动将应用程序和 Citrix 组策略移至新 XenApp 站点时意外引入错误的风险。

安装 XenApp 7.15 LTSR 核心组件并创建站点后，迁移过程按照以下顺序进行：

- 在每个 XenApp 6.5 工作进程上运行 XenApp 7.15 安装程序，将其自动升级到新 Virtual Delivery Agent for Server OS 以便在新站点中使用。
- 在 XenApp 6.5 Controller 上运行 PowerShell 导出 cmdlet，以将应用程序和 Citrix 策略设置导出至 XML 文件。
- 编辑 XML 文件（如果需要），以细化要导入到新站点的内容。通过自定义这些文件，可以将策略和应用程序设置分阶段导入到 XenApp 7.15 LTSR 站点：即一些现在导入，其他稍后导入。
- 在新 XenApp 7.15 Controller 上运行 PowerShell 导入 cmdlet，以将 XML 文件中的设置导入新 XenApp 站点。

根据需要重新配置新站点，然后对其进行测试。

有关详细信息，请参阅迁移 XenApp 6.x。

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

已修复的问题

Apr 18, 2018

以下问题自版本 7.14.1 起已修复：

与 7.14.1 相比已修复的问题

与 7.6 LTSR CU4 相比已修复的问题

与 7.14.1 相比已修复的问题

AppDNA

Citrix Director

- 在 Citrix Director 中导航到**趋势** > **故障** > **连接**选项卡时，可能会显示以下错误消息：

  “意外错误。请检查您的网络连接或查看 Director 服务器事件日志了解更多信息。”[#LC7755]

- 在 Citrix Director 中尝试查看某些会话的策略信息将失败，并显示以下错误消息：

  “无法检索数据”[#LC8207]

Citrix 策略

- 可能无法执行同时包含 Citrix 和 Microsoft 设置的组策略对象。列表中的扩展单元包含两个以上的 GUID 时会出现此问题。[#LC7533]

Citrix Studio

- 使用 GUI 模式来代替使用 PowerShell 命令时，尝试向新的或现有的计算机目录中添加计算机帐户可能会失败。查找 NetBIOS 名称过程中，目录搜索程序工具未绑定正确的对象时会出现此问题。

  例如，如果域名为 xyz.ad.airxyz.aa，NetBIOS 名称为 xyz-Ad，使用 GUI 模式时 NetBIOS 名称将以 xyz 格式（而非 xyz-Ad 格式）被接受。因此，不能同时为现有的和新的计算机帐户添加计算机帐户。[#LC6679]

- 将 Citrix Delivery Controller 升级到版本 7.12 后，在多域环境中尝试从 Citrix Provisioning Services (PVS) 向目录中添加计算机可能会失败。PVS 不返回域名以及设备名称时会出现此问题。Citrix Studio 搜索本地域中的帐户名称时，找不到帐户。[#LC6818]

- 尝试发布 App-V 应用程序可能会失败。[#LC7421]

- 管理员尝试从隔离组向交付组中添加 App-V 应用程序或者尝试创建隔离组时，Citrix Studio 中可能会显示以下错误消息：

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

“出现未知错误。”[#LC7594]

- 尝试为用户关联使用“NETBIOS”名称向交付组中添加计算机可能会失败。相反，域名可能会显示。NETBIOS 名称使用错误的 URL 时会出现此问题。[#LC7830]

Controller

- 将 Citrix Delivery Controller 升级到版本 7.12 后，在多域环境中尝试从 Citrix Provisioning Services (PVS) 向目录中添加计算机可能会失败。PVS 不返回域名以及设备名称时会出现此问题。Citrix Studio 搜索本地域中的帐户名称时，找不到帐户。[#LC6818]
- 对于可以选择以接受新计算机的多个存储，尝试向现有 Machine Creation Services 目录中添加计算机可能不会遵循轮询方法。[#LC7456]
- 自定义管理员尝试创建隔离组可能会失败，并显示以下错误消息：

  您没有完成此请求所需的权限。有关详细信息，请联系您的 XenDesktop 站点管理员。” [#LC7563]
- 管理员尝试从隔离组向交付组中添加 App-V 应用程序或者尝试创建隔离组时，Citrix Studio 中可能会显示以下错误消息：

  “出现未知错误。”[#LC7594]
- 尝试在 Citrix Delivery Controller 上禁用 TLSv1.0 会导致断开与 VMware vCenter 虚拟机管理程序的通信。[#LC7686]
- 尝试为用户关联使用“NETBIOS”名称向交付组中添加计算机可能会失败。相反，域名可能会显示。NETBIOS 名称使用错误的 URL 时会出现此问题。[#LC7830]

HDX RealTime Optimization Pack

Profile Management

- 在启用了 Profile Streaming 的情况下尝试打开配置文件中的文件时，当您登录后该文件可能会显示为空文件。[#LC6996]
- 服务器上的 picadm.sys 可能发生致命异常，并显示蓝屏和错误检测代码 0x135。[#LC7841]
- 登录 VDA 时，UserProfileManager.exe 可能会意外退出。[#LC7952]

StoreFront

- 在多站点聚合部署中，尝试重新连接到断开的会话可能会失败。因此，您可能会收到同一个资源的第二个实例。[#LC7453]
- 禁用了某个聚合应用程序的一部分源时，该应用程序可能会意外对最终用户隐藏。[#LC7675]
- 尝试在 StoreFront 中禁用“帐户自助服务”选项可能不会生效，即使该选项显示为已禁用亦如此。[#LC7744]
- 在 StoreFront 中，尝试从应用商店中删除共享身份验证可能会导致保存更改时显示以下错误消息：

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

保存您的更改时出错。[#LC7781]

通用打印服务器

客户端

- 打印后台处理程序服务可能无响应，从而导致通用打印无法正常工作。等待来自处理程序服务的事务响应时，如果达到超时时间，会出现该问题。[#LC5209]
- 使用 Profile Management 时，在一个服务器上的某个会话中对 Citrix 通用打印服务器打印机所做的更改（添加、删除和重命名）可能无法在另一个服务器上的后续会话中正确反映。[#LC7645]

服务器

- 尝试打印文档可能会失败并显示以下错误消息：

  “由于打印机的当前设置有问题，Windows 无法打印。”[#LC6825]

- 使用某些打印机时，Microsoft 记事本可能会显示消息“句柄无效”并且无法打印。如果在 Citrix 策略“通用打印驱动程序用法”中配置了“仅使用特定于打印机型号的驱动程序”，以及如果在 Citrix 策略“启用通用打印服务器”中配置了“启用但不回退到 Windows 的本机远程打印”，会出现此问题。[#LC7623]

VDA for Desktop OS

安装、卸载、升级

- 将 VDA 从版本 5.6.400 升级到版本 7.9 后，重新启动 VDA 会导致以前的版本安装的镜像驱动程序遗留下来。[#LC6295]
- 在非英语版本的 Microsoft Windows 操作系统中安装 7.12 或 7.13 版本的 VDA 后，某些 WMI 类可能会被重命名。[#LC7555]
- 在非英语版本的 Microsoft Windows 操作系统中安装 7.12 或 7.13 版本的 VDA 后，某些 WMI 类可能会被重命名。[#LC7587]

打印

- 新用户登录时，Citrix Print Manager 服务 (cpsvc.exe) 可能会变得无响应并意外退出。[#LC6933]
- 将 VDA 从版本 7.9 升级到版本 7.12 或更高版本后，尝试使用 Citrix 通用打印驱动程序从 Microsoft Internet Explorer 打印可能会仅打印到送纸器 1，而非打印到选定的送纸器。[#LC7463]

会话/连接

- 在 VDA for Desktop OS 上安装了同一型号的多个摄像头时，只有最新的摄像头可能会被会话识别并映射。[#LC5008]
- 在 VDA for Desktop OS 上，WFAPI SDK 可能不会返回可移除的客户端驱动器。[#LC6877]
- 重新连接到已发布的桌面会话并使用多个显示器时，可能不会保留窗口位置。[#LC7644]
- 在启用了旧图形模式且没有配置 Desktop Viewer 的情况下，在全屏模式下的多个显示器之间切换会话时，只有一台显示器可能显示正在运行会话。#LC7907]

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

智能卡

- 有时，删除智能卡读卡器可能不会触发用户会话被锁定，即使智能卡删除已配置为锁定用户会话也是如此。[#LC7411]

系统异常

- VDA 上的 vd3dk.sys 可能发生致命异常，并显示蓝屏和错误检测代码 0X00000050。[#LC6833]
- VDA 上的 picadm.sys 可能发生致命异常，并显示蓝屏和错误检测代码 0x7F，同时关闭会话。[#LC7545]
- 服务主机 (svchost.exe) 进程可能会遇到访问冲突并意外退出。scardhook64.dll 模块出错导致出现该问题。[#LC7580]
- 在 vdtw30.dll 上服务器可能会遇到致命异常，显示蓝屏和停止代码 0xc0000006。[#LC7608]
- 在 tdica.sys 上 VDA 可能会遇到致命异常，显示蓝屏和缺陷检查代码。[#LC7632]
- 此修复解决了会导致服务器意外退出的 wdica.sys 文件存在的内存问题。[#LC7666]

用户体验

- 此修复在使用高质量音频时改进了对播放一小段时间的声音的支持。

  注意：

  - 此修复在 Windows Server 2008 R2 上运行的会话中不生效。
  - 要使此修复生效，必须使用适用于 Windows 长期服务版本 (LTSR) CU5 或更高版本的 Citrix Receiver 4.4 以及 XenApp 和 XenDesktop 7.6 LTSR CU4 或更高版本的 VDA 版本。

  [#LC5842]

- 在版本 7.9 VDA 上运行的两个 Microsoft Excel 2010 工作表之间执行插入操作时，Excel 窗口可能会变得无响应。[#LC7481]
- 在多显示器环境中，将外部显示器定义为 Windows 的“主显示”，并在控制面板的显示设置中将其放置在辅助便携式计算机或平板电脑显示器右侧。启动在外部显示器上显示的已发布的应用程序，并将此应用程序移至连接至外部显示器的平板电脑显示器或便携式计算机时，打开或关闭平板电脑或便携式计算机的盖会导致已发布的应用程序变为黑色。

  要启用此项修复，必须在 VDA 上设置以下注册表项值：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\Thinwire
  名称：EnableDrvTw2NotifyMonitorOrigin
  类型：REG_DWORD
  值：1（启用）和 0（禁用；0 为默认值）。默认情况下，缺少注册表值。

  [#LC7760]

用户界面

- 使用经过触控优化的桌面时，URL 快捷方式图标可能显示为空白。[#LC6663]
- 如果在 Excel 2010 中打开一个包含多个工作簿的电子表格，任务栏将仅显示最新的工作簿。[#LC7557]

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

VDA for Server OS

安装、卸载、升级

- 在非英语版本的 Microsoft Windows 操作系统中安装 7.12 或 7.13 版本的 VDA 后，某些 WMI 类可能会被重命名。[#LC7555]
- 在非英语版本的 Microsoft Windows 操作系统中安装 7.12 或 7.13 版本的 VDA 后，某些 WMI 类可能会被重命名。[#LC7587]

打印

- 新用户登录时，Citrix Print Manager 服务 (cpsvc.exe) 可能会变得无响应并意外退出。[#LC6933]
- 将 VDA 从版本 7.9 升级到版本 7.12 或更高版本后，尝试使用 Citrix 通用打印驱动程序从 Microsoft Internet Explorer 打印可能会仅打印到送纸器 1，而非打印到选定的送纸器。[#LC7463]

服务器/站点管理

- 通过 Web Interface 或 StoreFront 启动应用程序时，可能会向子域用户显示以下错误消息：

  “未授予您访问此已发布的应用程序所需的权限。”[#LC7566]

会话/连接

- 在 VDA for Desktop OS 上安装了同一型号的多个摄像头时，只有最新的摄像头可能会被会话识别并映射。[#LC5008]
- 尝试重新连接到会话可能会间歇性失败，并导致 VDA for Server OS 进入“正在初始化”状态。在 Delivery Controller 中再次注册 VDA 时会出现此问题。

  [#LC6647]
- Delivery Controller 失去连接时，在 XenApp 服务器上，活动会话可能会被断开连接。VDA 无法跟踪从“预启动”正确变为“活动”状态的会话的状态时会出现该问题。因此，重新启动 Delivery Controller 时，它会尝试从 VDA 中清除资源，且处于预启动的会话会被断开连接或注销，虽然应用程序正在使用中。[#LC6819]
- 在 Microsoft Windows Server 2016 上启动已发布的应用程序时，可能会在应用程序可见之前显示几秒黑屏。[#LC7947]

系统异常

- VDA 上的 picadm.sys 可能发生致命异常，并显示蓝屏和错误检测代码 0x7F，同时关闭会话。[#LC7545]
- 服务主机 (svchost.exe) 进程可能会遇到访问冲突并意外退出。scardhook64.dll 模块出错导致出现该问题。[#LC7580]
- 在 vdtw30.dll 上服务器可能会遇到致命异常，显示蓝屏和停止代码 0xc0000006。[#LC7608]
- 在 tdica.sys 上 VDA 可能会遇到致命异常，显示蓝屏和缺陷检查代码。[#LC7632]
- 此修复解决了会导致服务器意外退出的 wdica.sys 文件存在的内存问题。[#LC7666]

用户体验

- 此修复在使用高质量音频时改进了对播放一小段时间的声音的支持。

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

注意：

- 此修复在 Windows Server 2008 R2 上运行的会话中不生效。
- 要使此修复生效，必须使用适用于 Windows 长期服务版本 (LTSR) CU5 或更高版本的 Citrix Receiver 4.4 以及 XenApp 和 XenDesktop 7.6 LTSR CU4 或更高版本的 VDA 版本。

[#LC5842]

- 在版本 7.9 VDA 上运行的两个 Microsoft Excel 2010 工作表之间执行插入操作时，Excel 窗口可能会变得无响应。[#LC7481]
- 在多显示器环境中，将外部显示器定义为 Windows 的“主显示”，并在控制面板的显示设置中将其放置在辅助便携式计算机或平板电脑显示器右侧。启动在外部显示器上显示的已发布的应用程序，并将此应用程序移至连接至外部显示器的平板电脑显示器或便携式计算机时，打开或关闭平板电脑或便携式计算机的盖会导致已发布的应用程序变为黑色。

  要启用此项修复，必须在 VDA 上设置以下注册表项值：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\Thinwire
  名称：EnableDrvTw2NotifyMonitorOrigin
  类型：REG_DWORD
  值：1（启用）和 0（禁用；0 为默认值）。默认情况下，缺少注册表值。

  [#LC7760]

用户界面

- 使用经过触控优化的桌面时，URL 快捷方式图标可能显示为空白。[#LC6663]
- 如果在 Excel 2010 中打开一个包含多个工作簿的电子表格，任务栏将仅显示最新的工作簿。[#LC7557]

虚拟桌面组件 - 其他

- 尝试发布 App-V 应用程序可能会失败。[#LC7421]
- 尝试在单管理员模式下启动 App-V 应用程序可能会失败。应用程序名称中包含特殊字符时会出现此问题。[#LC7897]

与 7.6 LTSR CU4 相比已修复的问题

Citrix Director

- 采用 Windows 集成身份验证 (WIA) 的 Citrix Director 可能无法与 Kerberos Constrained Delegation 设置协同工作。[#LC5196]
- 尝试登录 Citrix Director 后发生“系统不可用”错误。[#LC5385]
- Citrix Director 可能不会显示会话详细信息。使用已发布的内容作为应用程序类型时会出现此问题。[#LC6577]

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

Citrix 策略

- Citrix 策略处理可能停止响应，从而导致用户会话无响应。如果发生此问题，发送到 Receiver 和远程桌面 (RDP) 的连接请求将失败。[#LA4969]
- 在安装了修复 #LC1987（GPCSExt170W2K8R2X64006 或其替换选项）的系统中，可能无法执行同时包含 Citrix 和 Microsoft 设置的 Active Directory (AD) 策略。

  注意：此修复解决了您在安装此更新后创建的 AD 策略存在的问题。此外，此修复还解决了在 Citrix 设置先于 Microsoft 设置配置的*现有*策略存在的问题。在 Microsoft 设置*先于* Citrix 设置配置的现有 AD 策略中，此修复无法解决该问题。对于这些 AD 策略，必须打开受影响的策略并保存 Citrix 设置。[#LC2121]
- 有了此功能增强，Citrix Group Policy Engine 在处理 Citrix 策略时生成额外的事件日志消息。[#LC3664]
- 从 7.6 升级到 7.8 或 7.9 时，Citrix Studio 中某些颜色方案的显示可能会太暗，以致文本无法正确显示。[#LC5690]
- 安装 Citrix 联合身份验证服务后，尝试在 StoreFront 服务器上在**用户规则**下配置**安全访问控制列表**会导致“配置”窗口变得无响应。[#LC5788]
- 打开扩展名为 XLSM 并且带有宏的文件时，Microsoft Excel 的 CPU 和内存占用量可能会激增。因此，尝试打开该文件失败。[#LC6142]
- 可能无法执行同时包含 Citrix 和 Microsoft 设置的组策略对象。列表中的扩展单元包含两个以上的 GUID 时会出现此问题。[#LC7533]

Citrix Studio

- 如果多个用户在多个 Studio 会话中创建策略，则刷新 Citrix Studio 时，创建的最新策略会覆盖之前的策略。[#LA5533]
- Citrix Studio 可能无法识别 XenDesktop App Edition 许可证并显示以下错误消息：

  找不到有效的许可证
  无可用的合适许可证。请检查许可证服务器地址并核对产品版本和型号的正确性。” [#LC0822]
- 尝试将跨域用户添加到交付组中时，Citrix Studio 将他们的实际域解析为本地域帐户。[#LC1886]
- 尝试使用包含引号 (") 的命令行参数在 Citrix Studio 7.7 中发布应用程序时，可能会出现错误消息。[#LC4525]
- 即使未执行任何目录更新时，Citrix Studio 也可能会提供目录回滚选项。选择回滚会导致出现异常。[#LC4791]
- 从 Citrix Studio 向计算机目录添加计算机的尝试可能会失败，并会显示一条错误消息。当使用 XenDesktop 安装向导添加计算机时不会发生此问题。[#LC5030]
- 当两个应用程序具有相同的 ApplicationID 时，如果刷新 App-V 应用程序，可能导致 Citrix Studio 错误地设置 App-V 包名称。[#LC5261]

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

- Delivery Controller 脱机或以其他方式变为不可用时，Citrix Studio 可能运行缓慢。[#LC5335]
- 将 XenApp 或 XenDesktop 从 7.6 升级到 7.7 后，Citrix Studio 中可能偶尔会出现升级提示。[#LC5478]
- 当您关闭配置有包含多个软件包的 App-V 服务器的 Citrix Studio 7.9 版 的一个实例，然后再尝试重新打开该实例时，Studio 会保持展开状态且无法关闭。[#LC5643]
- 使用 Citrix Studio，只能向一个站点中添加一个 App-V 服务器。要向站点中添加额外的 App-V 服务器，必须使用 PowerShell。[#LC5767]
- 将 Citrix Studio 从 7.8 升级到 7.9 后，在升级后添加的应用程序显示时没有软件包名称和版本。[#LC5958]
- 在 Citrix Studio 中通过应用程序节点添加应用程序可能会导致应用程序未添加的错误。解决方法：请使用交付组节点添加应用程序。[#LC5975]
- 尝试通过 Citrix Studio 创建新 XenDesktop 站点并指向 SQL AlwaysOn 侦听器时，可能出现以下错误：

  无法访问副本服务器“”。请检查 SQL Server 上的数据库状态。请确保数据库服务器允许建立远程连接，并且防火墙不阻止连接。 [#LC6010]
- 如果从 Citrix Studio 删除现有的已发布 App-V 包，并尝试将具有相同名称和发布位置的相同 App-V 包的另一个版本添加到交付组，该包列出时可能会带有红色的感叹号，并显示以下错误消息：

  “加载应用程序“应用程序名称”的应用程序数据失败” [#LC6254]
- 尝试使用 Citrix Studio 中用于添加其他 Controller 的选项和 PowerShell 命令 Add-XDController 在镜像的数据库设置中添加 Delivery Controller 可能会失败。[#LC6563]
- 使用 GUI 模式来代替使用 PowerShell 命令时，尝试向新的或现有的计算机目录中添加计算机帐户可能会失败。查找 NetBIOS 名称过程中，目录搜索程序工具未绑定正确的对象时会出现此问题。

  例如，如果域名为 xyz.ad.airxyz.aa，NetBIOS 名称为 xyz-Ad，使用 GUI 模式时 NetBIOS 名称将以 xyz 格式（而非 xyz-Ad 格式）被接受。因此，不能同时为现有的和新的计算机帐户添加计算机帐户。[#LC6679]
- 将 Citrix Delivery Controller 升级到版本 7.12 后，在多域环境中尝试从 Citrix Provisioning Services (PVS) 向目录中添加计算机可能会失败。PVS 不返回域名以及设备名称时会出现此问题。Citrix Studio 搜索本地域中的帐户名称时，找不到帐户。[#LC6818]
- 升级 XenApp 站点时，许可模式可能会意外从 XenApp 变为 XenDesktop。[#LC6981]
- 在 PowerShell 5 中运行时，针对“Get-XDSite”和其他 XenDesktop 高级别管理 PoSH 命令的“Start-Transcript”命令可能会失败。[#LC7006]
- 管理员尝试从隔离组向交付组中添加 App-V 应用程序或者尝试创建隔离组时，Citrix Studio 中可能会显示以下错误消息：

  出现未知错误。 [#LC7594]
- 尝试为用户关联使用“NETBIOS”名称向交付组中添加计算机可能会失败。相反，域名可能会显示。NETBIOS 名称使用错误的 URL 时会出现此问题。[#LC7830]

Controller

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

- 在 Citrix Studio 中使用 Machine Creation Services 部署虚拟机失败，并显示以下错误消息：

  “错误 ID: XDDS:0F7CB924。”[#LC4930]

- 用户尝试删除在 XenServer 上创建的池目录，然后再运行目录更新时，基础磁盘未从存储中删除，并且基础磁盘数可能会增加。[#LC0577]

- 在使用 XenDesktop 5.6 Desktop Delivery Controller (DDC) 启动的 VDA 7.x 会话中，无法使用 Active Directory 组策略对象 (GPO) 或通过 Citrix Studio 禁用会话可靠性。 [#LC0878]

- 使用 Machine Creation Services 从具有自定义 VMX 和 nvram 设置的主映像创建新的池计算机时，这些设置不会复制到新虚拟机。[#LC0967]

- 在 XenDesktop 5.6 环境中使用时，Broker Service 执行的 PrepareSession 任务可能会超时，导致 StoreFront 无法运行。[#LC1055]

- 此修复解决了初始计算机创建过程中格式化 PvD 磁盘卷时虚拟机管理程序阻塞的情况下出现的计时问题。[#LC3275]

- 使用 VMware vSphere 6.0 和 vSAN 6 存储通过 Machine Creation Services 创建虚拟机可能会失败。[#LC4563]

- WaitForTask 响应导致 VimApi.MissingProperty 异常，其不允许更新计算机目录。[#LC4573]

- 从 Citrix Studio 向计算机目录添加计算机的尝试可能会失败，并会显示一条错误消息。当使用 XenDesktop 安装向导添加计算机时不会发生此问题。[#LC5030]

- 将 VDA 升级到版本 7.8 后，尝试执行更新清单操作可能会失败，并显示以下错误消息：

  “Update inventory failed with :An internal error occurred Error code 0x2.”（更新清单失败: 出现内部错误 错误代码 0x2。）[#LC5051]

- 日语操作系统上安装的某些 Citrix 服务的“Service Display Name”（服务显示名称）和“Service description”（服务说明）结尾处可能会出现无关字符。[#LC5208]

- 当两个应用程序具有相同的 ApplicationID 时，如果刷新 App-V 应用程序，可能导致 Citrix Studio 错误地设置 App-V 包名称。[#LC5261]

- 将 XenApp 或 XenDesktop 从 7.6 升级到 7.7 后，Citrix Studio 中可能偶尔会出现升级提示。[#LC5478]

- 应用程序标题中的和号 (&) 会导致 StoreFront XML 损坏，且不显示应用程序和图标。[#LC5505]

- 当您关闭配置有包含多个软件包的 App-V 服务器的 Citrix Studio 7.9 版 的一个实例，然后再尝试重新打开该实例时，Studio 会保持展开状态且无法关闭。[#LC5643]

- 升级到 XenDesktop 7.9 后，登录有时可能会因为 NetScaler Broker 未正确发送凭据而失败。[#LC5753]

- 使用 Citrix Studio，只能向一个站点中添加一个 App-V 服务器。要向站点中添加额外的 App-V 服务器，必须使用 PowerShell。[#LC5767]

- 安装 Citrix 联合身份验证服务后，尝试在 StoreFront 服务器上在**用户规则**下配置**安全访问控制列表**会导致“配置”窗口变得无响应。[#LC5788]

- 更改 Analytics、Broker、Log 等 Flexcast Management Architecture 服务的 SDK 端口会导致 Citrix Studio 无法正确连接。[#LC6005]

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

- 尝试通过 Citrix Studio 创建新 XenDesktop 站点并指向 SQL AlwaysOn 侦听器时，可能出现以下错误：

  无法访问副本服务器“”。请检查 SQL Server 上的数据库状态。请确保数据库服务器允许建立远程连接，并且防火墙不阻止连接。 [#LC6010]

- Citrix Director 可能会在控制板上显示大量未注册的计算机，这与“趋势”页面上的报告不一致。[#LC6184]

- 启用了“负载评估器指数”策略时，监视服务无法向监视数据库中插入新会话数据。这会导致 Citrix Director 不显示会话的最新数据，例如“登录时长”、“当前活动会话数量”等等。该问题在 Citrix Director 中显示时，是由 Delivery Controller 中的问题导致的。Controller 的当前版本解决了此问题。[#LC6241]

- 尝试删除托管单元会导致在任何其他托管单元上复制 AppDisk 失败。因此，交付组中包含 AppDisk 的计算机将无法启动。[#LC6433]

- 重新启动 Citrix Monitoring Service 或 Citrix Delivery Controller 后，可能会出现事件 ID 1013：

  “首次执行数据库常规事务失败，错误消息为: System.NullReferenceException: Object reference not set to an instance of an object（对象引用未设置为对象的实例）。”

  Citrix Monitor Service 停止时会出现此问题。[#LC6438]

- 尝试在 Citrix Delivery Controller 上使用某些第三方应用程序（例如 RayStation）可能会失败，并出现以下错误消息：

  “The communication object, System.ServiceModel.Channels.ServiceChannel, cannot be used for communication because it is in the Faulted state.”（由于通信对象 System.ServiceModel.Channels.ServiceChannel 处于“出错”状态，无法用于通信。） [#LC6552]

- 尝试使用 Citrix Studio 中用于添加其他 Controller 的选项和 PowerShell 命令 Add-XDController 在镜像的数据库设置中添加 Delivery Controller 可能会失败。[#LC6563]

- 尝试删除 VMware VSAN 上的 MCS 目录可能会失败。[#LC6691]

- Monitoring Service 的内存占用量会出现峰值，导致服务器无响应。[#LC6705]

- 从早期版本升级 Citrix Studio 后，或者全新安装 Citrix Studio 7.12 时，Delivery Controller 可能会导致 Citrix Studio 卡在强制升级循环中。[#LC6737]

- 使用 7.12 版本的 Machine Creation Services 创建 VM 时，无法安装 XenTools，这将阻止正常关闭 VM。[#LC6769]

- 将 Citrix Delivery Controller 升级到版本 7.12 后，在多域环境中尝试从 Citrix Provisioning Services (PVS) 向目录中添加计算机可能会失败。PVS 不返回域名以及设备名称时会出现此问题。Citrix Studio 搜索本地域中的帐户名称时，找不到帐户。[#LC6818]

- 对没有完全权限的管理员，可能会拒绝发布 App-V 包的权限，并出现以下异常：

  “Citrix.Console.Models.Exceptions.PermissionDeniedException: 您没有执行此操作所需的权限。” [#LC6897]

- HighAvailabilityService.exe 进程可能会占用高内存。[#LC6918]

- 升级 XenApp 站点时，许可模式可能会意外从 XenApp 变为 XenDesktop。[#LC6981]

- 在 PowerShell 5 中运行时，针对“Get-XDSite”和其他 XenDesktop 高级别管理 PoSH 命令的“Start-Transcript”命令可能会失败。[#LC7006]

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

- 此修复解决 Citrix Host Service 中的内存问题。[#LC7516]
- 自定义管理员尝试创建隔离组可能会失败，并显示以下错误消息：

  您没有完成此请求所需的权限。有关详细信息，请联系您的 XenDesktop 站点管理员。” [#LC7563]
- 管理员尝试从隔离组向交付组中添加 App-V 应用程序或者尝试创建隔离组时，Citrix Studio 中可能会显示以下错误消息：

  出现未知错误。 [#LC7594]
- 已安装 Microsoft 远程桌面会话主机角色服务时，尝试在 Microsoft Windows Server 上安装 VDA 可能会失败。[#LC7680]
- 尝试在 Citrix Delivery Controller 上禁用 TLSv1.0 会导致断开与 VMware vCenter 虚拟机管理程序的通信。[#LC7686]
- 尝试为用户关联使用“NETBIOS”名称向交付组中添加计算机可能会失败。相反，域名可能会显示。NETBIOS 名称使用错误的 URL 时会出现此问题。[#LC7830]

许可

- 许可证服务器可能会由于未设置“X-Frame-Options”标头类型而无法通过支付卡行业 (Payment Card Industry, PCI) 关于点击劫持的合规性扫描。[#LC1983]
- 尝试添加名称中包含超过 32 个字符的域组可能会失败。[#LC1986]
- 如果 NetBios 域名包含 & 符号，尝试打开 Studio 中的“许可”选项卡可能会失败，并显示以下错误消息：

  “Citrix 许可证服务器不可用”[#LC2728]

Profile Management

- 登录或注销过程中，某些第三方应用程序尝试重命名或移动文件可能会失败。例如，假设本地配置文件中有 file0、file1 和 file2 三个文件，如果 file2 已存在于挂起区域或用户存储中，则注销过程中尝试将 file2 重命名为 file3、将 file1 重命名为 file2 以及将 file0 重命名为 file1 可能会失败。[#LC0465]
- 用户注销时，Profile Management (UserProfileManager.exe) 服务有时会出现故障。[#LC0625]
- 性能监视器 (Perfmon) 计数器中的“登录持续时间”面板可能会记录不通过 Profile Management 管理的用户登录的数据。[#LC0779]
- 一段时间后，Profile Management 可能不会将文件与用户存储同步。[#LC1338]
- 启用以下登录选项后，日志文件中将不记录任何调试信息：
  - 策略：Active Directory 操作
  - 策略：登录和注销时的策略值
  - 策略：注销时的注册表差异

[#LC2003]

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

- 如果按 https://support.microsoft.com/zh-cn/kb/2890783 中所述启用了配置文件版本控制，Profile Management 可能会因以下原因而不迁移：
  - 创建的 Microsoft 漫游配置文件带有扩展名 V4
  - UPM 配置文件未迁移，并且是基于模板“默认用户”创建的。

[#LC2427]

- 重置 Desktop Director 中的用户配置文件后，文件夹重定向在用户首次登录时将不起作用。用户后续登录时，文件夹重定向不起作用。[#LC2602]
- Profile Management (UserProfileManager.exe) 服务可能会意外关闭。[#LC2979]
- 应用修复 #LC0625 后，Profile Management (UserProfileManager.exe) 服务可能会意外关闭。[#LC3058]
- 在 Windows 8.1 上，如果启用了增强保护模式，尝试使用 Internet Explorer 11 下载文件将失败。[#LC3464]
- 注销过程中 Profile Management 中会发生文件锁定，并显示以下错误消息：

  The process cannot access the file because it is being locked by another process.（此进程无法访问该文件，因为该文件正被另一个进程锁定。）

  尝试删除 Profile Management 锁定的文件可能会失败，直至锁定被释放。[#LC3532]
- 关闭用户设备过程中，Profile Management 会意外退出。[#LC3626]
- XenApp 服务器在场中可能会无响应，直至重新启动服务器。[#LC4318]
- 尝试使用 RDP 登录 XenApp 7.7 服务器时，该服务器可能会在欢迎屏幕上变得无响应。[#LC5169]
- 将 VDA 从版本 7.6.1000 或更早版本升级到版本 7.7 或更高版本后，尝试删除、修复或重新安装 VDA 可能会失败。[#LC5207]
- 注销时，Profile Management 有时会锁定服务器上的文件/文件夹，导致应用程序无法启动。本地缓存的配置文件也不会被删除。[#LC5266]
- Profile Management 有时会锁定用户配置文件中的文件。出现此问题时，尝试重新连接时用户会收到一个临时配置为文件，直至其配置文件上的锁定被释放。[#LC5278]
- 用户注销时，本地缓存的配置文件可能不删除。[#LC5470]
- 许可证服务器处于脱机状态时，服务器上使用用户重定向文件夹的文件将丢失。[#LC5595]
- 许可证试用期结束但未续订时，用户的文件将丢失。[#LC5775]
- Profile Management 可能会错误地引出“NetworkDetection”标志，指示网络可能已断开。此修复引入了额外的检查，以确保网络不可用，而非暂时不可用。[#LC5943]

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

- 在 Windows Server 2012 R2 上，用户登录屏幕偶尔会变得无响应。[#LC6149]
- 尝试将漫游配置文件迁移到 Profile Management 中可能会失败。向配置文件中添加了不正确的版本号时会出现此问题。[#LC6150]
- 尝试通过 WAN 连接复制 Profile Management 用户配置文件存储中的图标时，应用程序图标可能会显示为灰色。[#LC6152]
- 文件类型关联可能无法在 Microsoft Windows 10 和 Windows Server 2016 上运行的启用了 Profile Management 的会话中漫游。[#LC6736]
- 在 Microsoft Windows 10 或 Windows Server 2016 中启用了“注销时删除本地缓存”策略时，NTUSER.DAT 文件可能无法在注销时删除，导致下次登录时创建另一个本地配置文件。[#LC6765]
- 在 Microsoft Windows Server 2016 上使用 Profile Management 时，如果包括 usrclass.dat，“开始”菜单可能无法正常工作。[#LC6914]
- 在启用了 Profile Streaming 的情况下尝试打开配置文件中的文件时，当您登录后该文件可能会显示为空文件。[#LC6996]
- 尝试启动 Microsoft Windows 10 会话时，Profile Management 会导致显示黑屏。应用此修复后，必须配置策略“要同步的目录”并添加文件夹 *AppData\Local\Microsoft\Windows\Caches*。 [#LC7596]

Provisioning Services

控制台问题

- 应用此修复后，“Schedule the next vDisk update to occur on”（安排发生下一次虚拟磁盘更新的时间）选项和“Apply vDisk updates as soon as they are directed by the server”（服务器引导后立即应用虚拟磁盘更新）选项不再对 Provisioning Services 可用。[#LA4166]
- 在非英语 Microsoft System Center Virtual Machine Manager (SCVMM) 环境中，尝试通过 XenDesktop 设置向导创建虚拟机可能会失败。[#LC5451]
- 尝试使用 New-BootDeviceManager PowerShell 脚本创建 ISO 失败，并显示以下错误消息：ISOFileName must be called with the name of the new ISO file to create（ISOFileName 必须通过要创建的新 ISO 文件的名称进行调用）。[#LC5559]
- 使用群集卷存储时，流 VM 设置向导不遵从所做的卷选择，而是能够在随机卷中创建目标设备。[#LC5890]
- 运行 XenDesktop 设置向导或流 VM 设置向导后尝试关闭 Provisioning Services 控制台会导致出现异常。[#LC6048]
- 从版本 7.6 升级到 PVS 7.11 后，其他域中的用户可能无法登录控制台。[#LC6216]
- 服务器通信超时。在某些情况下，登录超时会变得过长（例如，超过 2 分钟）。这会导致 PVS 控制台与 SoapServer 服务器之间出现服务器超时问题。默认情况下，此类连接的超时值为 2 分钟。但是，您可以通过修改注册表值 HOTKEY_LOCAL_MACHINE\Software\Citrix\ProvisioningServices ConnectionTimeout=<超时值（分钟）> 来增加此值。如果登录时间大约超过 4 分钟，用户还会遇到来自包含 PVS 控制台的 Microsoft MMC 的超时（可以消除这些超时）。

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

此问题的一个原因是 Active Directory 中存在无法访问的域，在这些域中，每次尝试连接到无法访问的域都会应用 30 秒超时。如果存在多个无法访问的域，可以将超时值最大快速增加到几分钟。一般情况下，通过以下方法创建无法访问的域：向 Active Directory 中添加测试或实验性域，稍后再将其删除。虽然该域已消失，但枚举域或授权组时 Active Directory 仍会报告该域。

暂时关闭并断开网络连接的域控制器也会导致域无法访问，因此，不应将所有无法访问的域都列入黑名单。

确定是否存在无法访问的域的最佳方式是查看 CDF 跟踪中是否存在 PVS_DLL_ADSUPPORT 模块并检查“无法访问的域”和“服务器引用”错误。如果找到其中任何错误，请检查域以确保其不再使用，如果不再使用，请将域名添加到黑名单中。

黑名单是一个名为 %ProgramData\Citrix\Provisioning Services\blacklist.json 的 JSON 格式的文件。例如：
{

"Domains":

[

"sub.xs.local",

"sb.xs.local"

]

}

其中，两个域 **sub.xs.local** 和 **sb.xs.local** 将从域和组枚举中排除。更新文件后，必须重新启动 SoapServer 和任何正在运行的控制台以加载更新后的值。[#LC6249]

- 配置 Provisioning Services 控制台后，目标设备属性中可能会缺少标签名称。[#LC6864]

服务器问题

- 在 VMware ESX 环境中，XenDesktop 设置向导会引发异常，阻止用户正确地设置模板和计算机。[#LA2499]
- 两个 PVS 服务器可能看不到对方服务器上的虚拟磁盘的复制状态，但每个服务器都会正确地显示各自虚拟磁盘的状态。[#LC4317]
- Citrix PXE 服务可能会忽略 BOOTPTAB 文件中的条目。[#LC4600]
- 使用 BDM 分区时，如果列表中最上面的服务器无法访问，VMware 上运行的目标设备将不尝试登录列表中的所有服务器。[#LC4736]
- 在非英语 Microsoft System Center Virtual Machine Manager (SCVMM) 环境中，尝试通过 XenDesktop 设置向导创建虚拟机可能会失败。[#LC5451]
- 如果未克隆硬盘驱动器上的所有分区，正在克隆的最终分区可能会失败。[#LC5452]

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

- 在 PVS 控制台中运行两个 PVS 服务器的复制状态时，两个服务器的状态都显示不完整。[#LC5700]
- 使用群集卷存储时，流 VM 设置向导不遵从所做的卷选择，而是能够在随机卷中创建目标设备。[#LC5890]
- 从版本 7.6 升级到 PVS 7.11 后，其他域中的用户可能无法登录控制台。[#LC6216]
- 服务器通信超时。在某些情况下，登录超时会变得过长（例如，超过 2 分钟）。这会导致 PVS 控制台与 SoapServer 服务器之间出现服务器超时问题。默认情况下，此类连接的超时值为 2 分钟。但是，您可以通过修改注册表值 HOTKEY_LOCAL_MACHINE\Software\Citrix\ProvisioningServices ConnectionTimeout=<超时值（分钟）> 来增加此值。如果登录时间大约超过 4 分钟，用户还会遇到来自包含 PVS 控制台的 Microsoft MMC 的超时（可以消除这些超时）。

  此问题的一个原因是 Active Directory 中存在无法访问的域，在这些域中，每次尝试连接到无法访问的域都会应用 30 秒超时。如果存在多个无法访问的域，可以将超时值最大快速增加到几分钟。一般情况下，通过以下方法创建无法访问的域：向 Active Directory 中添加测试或实验性域，稍后再将其删除。虽然该域已消失，但枚举域或授权组时 Active Directory 仍会报告该域。

  暂时关闭并断开网络连接的域控制器也会导致域无法访问，因此，不应将所有无法访问的域都列入黑名单。

  确定是否存在无法访问的域的最佳方式是查看 CDF 跟踪中是否存在 PVS_DLL_ADSUPPORT 模块并检查“无法访问的域”和“服务器引用”错误。如果找到其中任何错误，请检查域以确保其不再使用，如果不再使用，请将域名添加到黑名单中。

  黑名单是一个名为 %ProgramData\Citrix\Provisioning Services\blacklist.json 的 JSON 格式的文件。例如：

  ```
  {
  "Domains":
  [
  "sub.xs.local",
  "sb.xs.local"
  ]
  }
  ```

  其中，两个域 **sub.xs.local** 和 **sb.xs.local** 将从域和组枚举中排除。更新文件后，必须重新启动 SoapServer 和任何正在运行的控制台以加载更新后的值。[#LC6249]

目标设备问题

- 如果更新不可用，Provisioning Services 目标设备的自动更新功能将在目标的事件查看器中生成以下应用程序错误消息（事件 ID：0）。
  “No update server found. Stopping client service.”（服务器找不到更新。正在停止客户端服务。）[#LC0450]

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

- 目标设备软件无法识别 AppDisk 驱动器，并且为写入缓存使用 AppDisk 驱动器，这会导致出现冲突。[#LC5409]
- 将虚拟磁盘配置为使用“在 RAM 上写入缓存”并将 RAM 缓存大小设置为 4096 MB 或 4097 MB 时，从 Hyper-V 第二代虚拟机启动会导致目标设备遇到致命异常，显示蓝屏。[#LC6707]

StoreFront

- 如果管理员更改了组策略设置 MaxPasswordAge，StoreFront 的默认域服务将不重新加载新值。在 StoreFront 中，系统可能会向用户显示不正确的“密码过期前的天数”。

  注意：此问题已修复，但可能需要长达一小时时间来加载新值。[#DNA-41380]
- 安装 StoreFront 3.5 后，目录视图中的文件夹颜色可能不再使用在 StoreFront 管理控制台中定义的自定义颜色。该颜色将还原到默认颜色。[#LC5001]
- 管理 Citrix Receiver for Web 站点时，StoreFront 可能会意外退出。为 Citrix Receiver for Web 自定义了 style.css 时会出现此问题。[#LC5589]
- 在 StoreFront 上启用联合身份验证服务可能会导致出现登录错误。[#LC5708]
- 即使在 Citrix StoreFront 中启用了 Citrix Receiver for HTML5，StoreFront 控制台可能也会显示“未使用”，而不显示 HTML 版本。[#LC6626]
- 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，并且可能会显示以下错误消息：

  “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。）[#LC6664]
- 如果从 StoreFront 控制台为某个特定的应用商店配置了自助服务密码重置 (SSPR)，该配置将应用到所有应用商店，而非仅应用到选定的特定应用商店。[#LC6987]
- 在多站点聚合部署中，尝试重新连接到断开的会话可能会失败。因此，您可能会收到同一个资源的第二个实例。[#LC7453]
- 禁用了某个聚合应用程序的任何源时，该应用程序可能会意外对最终用户隐藏。[#LC7675]
- 尝试在 StoreFront 中禁用“帐户自助服务”选项可能不会生效，即使该选项显示为已禁用亦如此。[#LC7744]
- 在 StoreFront 中，保存更改时尝试从应用商店中删除共享身份验证可能会导致显示以下错误消息：

  “保存您的更改时出错。”[[#LC7781]

通用打印服务器

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

客户端

- 使用 Profile Management 时，在一个服务器上的某个会话中对 Citrix 通用打印服务器打印机所做的更改（添加、删除和重命名）可能无法在另一个服务器上的后续会话中正确反映。[#LC7645]

服务器

- 使用 Citrix 通用打印驱动程序时，尝试从 Microsoft Internet Explorer 打印可能会失败，并提示以下错误消息：

  “There was an internal error and Internet Explorer is unable to print this document.”（存在内部错误，Internet Explorer 无法打印此文档。）[#LC4735]

- 尝试打印文档可能会失败，并显示以下错误消息：

  “Windows cannot print due to a problem with the current printer setup.”（由于当前打印机设置存在问题，Windows 无法打印。）[#LC6825]

- 使用某些打印机时，Microsoft 记事本可能会显示消息“句柄无效”并且无法打印。如果在 Citrix 策略“通用打印驱动程序用法”中配置了“仅使用特定于打印机型号的驱动程序”，以及如果在 Citrix 策略“启用通用打印服务器”中配置了“启用但不回退到 Windows 的本机远程打印”，会出现此问题。 [#LC7623]

VDA for Desktop OS

内容重定向

- 尝试使用 DirectShow 捕获图像失败，导致应用程序意外退出。[#LC6667]

HDX Broadcast

- HDX 音频设备在启动一个会话时可能会被随机禁用。[#LC5281]

安装、卸载、升级

- 将 VDA 从版本 5.6.400 升级到版本 7.9 后，重新启动 VDA 会导致以前的版本安装的镜像驱动程序遗留下来。[#LC6295]
- 将 VDA 从版本 5.6 升级到 7.x 时，可能会安装不正确的旧版视频驱动程序。[#LC6363]
- 使用 7.12 版本的 Machine Creation Services 创建 VM 时，无法安装 XenTools，这将阻止正常关闭 VM。[#LC6769]
- 在非英语版本的 Microsoft Windows 操作系统中安装 7.12 或 7.13 版本的 VDA 后，某些 WMI 类可能会被重命名。[#LC7555]
- 在非英语版本的 Microsoft Windows 操作系统中安装 7.12 或 7.13 版本的 VDA 后，某些 WMI 类可能会被重命名。[#LC7587]

键盘

- Citrix Receiver for Linux 可能不支持西班牙语 DNIe 身份证。[#LC6547]
- 在 VDA 中启用了 HDX 3D Pro 的情况下，键盘快捷方式“Alt+p”和“Alt+s”可能不起作用。[#LC6826]

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

打印

- 尝试将某个文档打印两份或两份以上时，可能只打印一份。如果在 Citrix 策略“通用打印驱动程序用法”中配置了“仅使用特定于打印机型号的驱动程序”，以及如果在 Citrix 策略“启用通用打印服务器”中配置了“启用但不回退到 Windows 的本机远程打印”，会出现此问题。 [#LC6023]
- 新用户登录时，Citrix Print Manager 服务 (cpsvc.exe) 可能会变得无响应并意外退出。[#LC6933]
- 将 VDA 从版本 7.9 升级到版本 7.12 或更高版本后，尝试使用 Citrix 通用打印驱动程序从 Microsoft Internet Explorer 打印可能会仅打印到送纸器 1，而非打印到选定的送纸器。[#LC7463]

服务器/站点管理

- 对“视觉效果”下的“高级系统设置”所做的更改应用于当前 VDA for Desktop OS 会话，但可能不会保留到后续会话中。要使此类更改持续存在，请设置以下注册表项：

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix
  名称：EnableVisualEffect
  类型：DWORD
  值：1

  [#LC8049]

会话/连接

- 客户端 USB 设备重定向规则策略可能无法应用。当用户在策略中输入的字符数超过 1002 时，会出现此问题。 [#LC1144]
- 在网络中断后重新连接到 VDA 会话的尝试可能会失败。将 VDA 升级到 7.8 版本后会出现此问题。 [#LC5040]
- 启用了 Framehawk 后，鼠标上的滚动按钮在 XenDesktop 7.8 VDA 会话中可能无法执行任何操作。XenDesktop 7.9 提供了相应的 VDA 端修复。 [#LC5302]
- VDA 可能会遇到类型为 0x50 (Page_Fault_In_NonPaged_Area) 的有关 Citrix 显示驱动程序 vdodk.sys 的严重异常。[#LC5074]
- 将 AppDisk 附加到非英语版本的 Microsoft Windows 操作系统上运行的虚拟机时，可能会显示“Restart Now or Restart Later”（立即重新启动或稍后重新启动）提示。应用此修复后，该提示将消失。[#LC5403]
- 在重新连接到一个已断开连接的多监视器会话后，显示屏会变黑，同时自定义设置会恢复为默认值。[#LC5556]
- 将 VDA 从版本 7.6.300 升级到版本 7.8 时，剪贴板同步可能会停止工作。[#LC5699]
- 启用了 Framehawk 后，鼠标上的滚动按钮在 XenDesktop 7.9 VDA 会话中可能无法执行任何操作。[#LC5779]
- 针对联合身份验证服务配置后，VDA 可能会停止接受连接并在“欢迎”屏幕上无法响应，直到重新启动。[#LC5978]
- 启动应用程序时，Citrix Receiver 在显示错误消息“Connection Established. Negotiate Capabilities”（已建立连接。协商功能）之后可能无法继续运行。[#LC6021]
- 对“视觉效果”下方的“高级系统设置”所做的更改应用于当前 VDA 会话，但可能不会保留到后续会话中。为了永久保持此类更改，必须设置以下注册表项：

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix

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

名称：EnableVisualEffect
类型：DWORD
值：0

[#LC6163]

- 尝试从启用了触控功能的设备上运行的 RemotePC 会话断开连接会导致出现无法恢复的黑屏。[#LC6384]
- Citrix Receiver for Linux 可能不支持西班牙语 DNIe 身份证。[#LC6547]
- 通过 Windows 10 上安装的 SecureDoc 锁定远程 PC 会话时，锁屏界面将显示长达两分钟的时间。在此期间，您将无法与该会话交互。[#LC6668]
- 如果在播放时多次断开 Citrix Receiver for Mac 会话连接并重新连接，音频可能无法工作。[#LC6678]
- 在 VDA for Desktop OS 上，WFAPI SDK 可能不会返回可移除的客户端驱动器。[#LC6877]
- 在 XenDesktop 7.13 Windows 7 VDA 上使用旧图形模式时，可能会出现灰屏。[#LC7477]
- 在启用了旧图形模式且没有配置 Desktop Viewer 的情况下，在全屏模式下的多个显示器之间切换会话时，只有一台显示器可能显示正在运行会话。[#LC7907]

系统异常

- VDA for Server OS 上的 TDICA.sys 可能会发生致命异常，并显示蓝屏。[#LC6898]
- 在 vdtw30.dll 上服务器可能会遇到致命异常，显示蓝屏和停止代码 0xc0000006。[#LC7608]
- 在 tdica.sys 上 VDA 可能会遇到致命异常，显示蓝屏和缺陷检查代码。[#LC7632]
- 此修复解决了会导致服务器意外退出的 wdica.sys 文件存在的内存问题。[#LC7666]

智能卡

- 在用户会话与 Microsoft 远程桌面会话之间切换时，会话中识别智能卡的应用程序（例如 Microsoft Outlook 和 Microsoft Word）可能无法使用智能卡。因此，可能会出现各种错误消息。此外，在命令窗口中使用“CertUtil /scinfo”测试会话中智能卡支持可能会导致出现以下错误消息：

  “Microsoft 智能卡资源管理器没有运行。”[#LC5839]

- 智能卡直通可能会间歇性失败。[#LC6147]

用户体验

- 如果在 Excel 2010 中打开一个带有多个工作簿的电子表格时，任务栏仅显示最新的工作簿。[#LC5370]
- 在 XenDesktop 7.11 Windows 7 VDA 上使用旧图形模式时，仅显示屏幕的左上角。[#LC6532]
- 在版本 7.9 VDA 上运行的两个 Microsoft Excel 2010 工作表之间执行插入操作时，Excel 窗口可能会变得无响应。[#LC7481]

用户界面

- 存在未保存数据的情况下，使用连接中心从无缝会话注销，会显示黑色窗口和以下消息：

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

“程序仍需要关闭”，并提供两个选项“强制注销”或“取消”。“Cancel”（取消）选项不起作用。

安装此修复后，“Cancel”（取消）选项可按预期工作。[#LC6075]

- “自动显示键盘”策略设置为启用且“启动触控优化桌面”策略设置为禁止的情况下，从 iPad 启动已发布的桌面会导致文档查看器以 80% 的比例显示。关闭桌面上的某些应用程序后，文档查看器会以 100% 的比例显示。 [#LC6460]
- 如果在 Excel 2010 中打开一个包含多个工作簿的电子表格，任务栏将仅显示最新的工作簿。[#LC7557]

VDA for Server OS

内容重定向

- 尝试使用 DirectShow 捕获图像失败，导致应用程序意外退出。[#LC6667]

安装、卸载、升级

- 从 VDA 7.11 for Desktop OS 升级到 VDA 7.12 for Desktop OS 后，启动某些应用程序时，可能会显示以下错误消息。

  “缺少 wfapi.dll”[#LC6874]

- 在非英语版本的 Microsoft Windows 操作系统中安装 7.12 或 7.13 版本的 VDA 后，某些 WMI 类可能会被重命名。[#LC7555]
- 在非英语版本的 Microsoft Windows 操作系统中安装 7.12 或 7.13 版本的 VDA 后，某些 WMI 类可能会被重命名。[#LC7587]

打印

- 尝试使用 CreateClientPrinter 命令映射网络打印机时，Citrix Print Manager 意外退出。[#LC4685]
- 尝试将某个文档打印两份或两份以上时，可能只打印一份。如果在 Citrix 策略“通用打印驱动程序用法”中配置了“仅使用特定于打印机型号的驱动程序”，以及如果在 Citrix 策略“启用通用打印服务器”中配置了“启用但不回退到 Windows 的本机远程打印”，会出现此问题。 [#LC6023]
- 新用户登录时，Citrix Print Manager 服务 (cpsvc.exe) 可能会变得无响应并意外退出。[#LC6933]
- 将 VDA 从版本 7.9 升级到版本 7.12 或更高版本后，尝试使用 Citrix 通用打印驱动程序从 Microsoft Internet Explorer 打印可能会仅打印到送纸器 1，而非打印到选定的送纸器。[#LC7463]

服务器/站点管理

- 如果用户在位于两个不同网络子网上的会话之间移动，打印机列表中将包含同时位于这两个子网中的打印机，而不是用户当前登录的子网中的打印机。[#LC2308]
- 通过 Web Interface 启动应用程序时，可能向子域用户显示以下错误消息：

  “未授予您访问此已发布的应用程序所需的权限。” [#LC7566]

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

- 对“视觉效果”下的“高级系统设置”所做的更改应用于当前 VDA for Desktop OS 会话，但可能不会保留到后续会话中。要使此类更改持续存在，请设置以下注册表项：

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix
  名称：EnableVisualEffect
  类型：DWORD
  值：1

  [#LC8049]

会话/连接

- 在含有修复程序 #LC2702（包括在修补程序汇总包 6 中）的系统中，应用程序可能无法在客户端映射的驱动器上保存，并会生成损坏的文件。[#LC3976]

- 在已安装 Streaming Profiler 或 Offline Plugin 插件的情况下，可能无法使用 WinDbg.exe 启动进程。之所以出现该问题，是因为 RadeAPHook 挂接 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<*processname*> 和 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<*processname*>。

  要启用此修复，请创建以下注册表项：

- *对于 32 位 Windows：*
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\StreamingHook
  名称：EnableReadImageFileExecOptionsExclusionList
  类型：Reg_SZ
  值：< *与“图像文件执行选项”设置有关、要从钩起中排除的可执行文件的列表，以逗号分隔，不包含空格。例如，windbg.exe,application_1.exe。*>

- *对于 64 位 Windows 上的 32 位应用程序：*
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StreamingHook
  名称：EnableReadImageFileExecOptionsExclusionList
  类型：Reg_SZ
  值：< *与“图像文件执行选项”设置有关、要从钩起中排除的可执行文件的列表，以逗号分隔，不包含空格。例如，windbg.exe,application_1.exe.*>

  [#LC4750]

- 启动新会话时，如果 Citrix Audio Redirection Service 尝试连接到包含无效信息的虚拟通道会话，可能会失败。[#LC5024]
- 启用了 Framehawk 后，鼠标上的滚动按钮在 XenDesktop 7.8 VDA 会话中可能无法执行任何操作。XenDesktop 7.9 提供了相应的 VDA 端修复。 [#LC5302]
- 将 VDA 从版本 7.6.300 升级到版本 7.8 时，剪贴板同步可能会停止工作。[#LC5699]
- 启用了 Framehawk 后，鼠标上的滚动按钮在 XenDesktop 7.9 VDA 会话中可能无法执行任何操作。[#LC5779]
- 针对联合身份验证服务配置后，VDA 可能会停止接受连接并在“欢迎”屏幕上无法响应，直到重新启动。[#LC5978]

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

- 对“视觉效果”下方的“高级系统设置”所做的更改应用于当前 VDA 会话，但可能不会保留到后续会话中。为了永久保持此类更改，必须设置以下注册表项：

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix
  名称：EnableVisualEffect
  类型：DWORD
  值：0

  [#LC6163]

- 启动 XenApp 7.6 长期服务版本 Cumulative Update 2 VDA for Server OS 或早期版本时，以下警告消息可能会在系统事件日志中显示：

  “尝试连接 SemsService 失败，错误代码为 0x2。” [#LC6311]

- 在 VDA for Server OS 上，远程桌面会话接管控制台会话时，可能会创建无法运行的 XenApp 会话。[#LC6617]
- 尝试重新连接到会话可能会间歇性失败，并导致 VDA for Server OS 进入“正在初始化”状态。在 Delivery Controller 中再次注册 VDA 时会出现此问题。[#LC6647]
- 通过 Windows 10 上安装的 SecureDoc 锁定远程 PC 会话时，锁屏界面将显示长达两分钟的时间。在此期间，您将无法与该会话交互。[#LC6668]
- 如果在播放时多次断开 Citrix Receiver for Mac 会话连接并重新连接，音频可能无法工作。[#LC6678]
- 在 Microsoft Windows Server 2016 上启动已发布的应用程序时，可能会在应用程序可见之前显示几秒黑屏。[#LC7947]

智能卡

- 在用户会话与 Microsoft 远程桌面会话之间切换时，会话中识别智能卡的应用程序（例如 Microsoft Outlook 和 Microsoft Word）可能无法使用智能卡。因此，可能会出现各种错误消息。此外，在命令窗口中使用“CertUtil /scinfo”测试会话中智能卡支持可能会导致出现以下错误消息：

  “Microsoft 智能卡资源管理器没有运行。”[#LC5839]

系统异常

- VDA for Server OS 上的 TDICA.sys 可能会发生致命异常，并显示蓝屏。[#LC6898]
- 在 vdtw30.dll 上服务器可能会遇到致命异常，显示蓝屏和停止代码 0xc0000006。[#LC7608]
- 在 tdica.sys 上 VDA 可能会遇到致命异常，显示蓝屏和缺陷检查代码。[#LC7632]
- 此修复解决了会导致服务器意外退出的 wdica.sys 文件存在的内存问题。[#LC7666]

用户体验

- 如果在 Excel 2010 中打开一个带有多个工作簿的电子表格时，任务栏仅显示最新的工作簿。[#LC5370]
- 在版本 7.9 VDA 上运行的两个 Microsoft Excel 2010 工作表之间执行插入操作时，Excel 窗口可能会变得无响应。[#LC7481]

用户界面

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

- 存在未保存数据的情况下，使用连接中心从无缝会话注销，会显示黑色窗口和以下消息：

  “程序仍需要关闭”，并提供两个选项“强制注销”或“取消”。“Cancel”（取消）选项不起作用。

  安装此修复后，“Cancel”（取消）选项可按预期工作。[#LC6075]

- “自动显示键盘”策略设置为启用且“启动触控优化桌面”策略设置为禁止的情况下，从 iPad 启动已发布的桌面会导致文档查看器以 80% 的比例显示。关闭桌面上的某些应用程序后，文档查看器会以 100% 的比例显示。 [#LC6460]

- 如果在 Excel 2010 中打开一个包含多个工作簿的电子表格，任务栏将仅显示最新的工作簿。[#LC7557]

虚拟桌面组件 - 其他

- 用户的“VM 托管应用程序会话”会话类型可能会意外地从“应用程序”更改为“桌面”。因此，尝试重新连接到应用程序失败。[#LC5461]

- 对使用与 XenDesktop 集成的 Microsoft App-V 5.0 基础结构的 App-V 软件包进行启动时，App-V 软件包可能会无法同步，并显示以下异常：

  “无法启动 ”[#LC5483]

- 尝试通过网络加载 App-V 应用程序时，可能导致出现以下错误消息：

  Index was out of range. Must be non-negative and less than the size of the collection.”（指数超出范围。必须为非负数，并且小于该集合的大小。） [#LC5828]

- 将 XenApp 从版本 7.7 升级到版本 7.8 后，尝试启动 App-V 应用程序可能失败。“TargetIn”布尔值设置为“0”而不是“1”时会发生该问题。此外，手动设置值可能没有任何效果。刷新应用程序时，它可能会还原。[#LC5861]

- 向 Citrix Studio 添加包含多个应用程序的 App-V 软件包并发布该软件包中的所有应用程序时，在用户会话中，可能只有第一个应用程序启动。[#LC5863]

- App-V 应用程序只能由单个用户启动。另一个用户尝试在同一台服务器上启动同一个应用程序可能会失败。[#LC6414]

- 即使实际的 App-V 包引用了 App-V 排序的应用程序 (InTarget=False)，这些应用程序可能也不会包含在该包中。因此，应用程序启动不适用于应用程序正常运行所需的任何相关连接组。[#LC6534]

- 从 XenApp/XenDesktop 7.11 升级到 7.12 后，可能不会遵守现有的交付组重新启动计划。[#LC6766]

- 从映射的驱动器尝试启动 App-V 应用程序可能会失败。[#LC6961]

- 尝试发布 App-V 应用程序可能会失败。

  [#LC7421]

- 在 VDA 主映像上安装了 Microsoft 消息队列时尝试创建计算机目录可能会失败， 并在 Citrix Studio 中显示以下错误消息：

  Image Preparation did not complete. 状态为“NotSet”[#LC7528]

- 尝试在单管理员模式下启动 App-V 应用程序可能会失败。应用程序名称中包含特殊字符时会出现此问题。[#LC7897]

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

其他已修复的问题

- 如果在将 Delivery Controller 从 7.11 升级到 7.14、从 7.12 升级到 7.14 或从 7.13 升级到 7.14 之前，在“Profile Management”>“注册表”>“默认排除项”下配置了 UPM - Software\Microsoft\Speech_OneCore 策略，Citrix Studio 中的组策略会缺失。 [#UPM-538]
- 在 Windows Server 2008 上尝试使用 XenApp 和 XenDesktop 完整产品安装程序安装或升级到 Session Recording 版本 7.14 失败，并显示以下错误消息“Microsoft 消息队列失败”。 [#SRT-1782]
- 升级 Controller 后， VDA 的电源状态可能指示“未知”。[#DNA-37756]

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

已知问题

Apr 18, 2018

本文的 7.15 基础组件和 CU1 部分中介绍的已知问题将继续在 CU2 中提供，除非其包含在已修复的问题列表中。

累积更新 2 中的已知问题

- 在 W2k16 VDA 上，使用智能卡登录的用户可能无法在登录时查看所有可用用户。此问题是登录窗口的默认大小导致的，默认大小为 600x520。有关详细信息和解决方法，请参阅知识中心文章 CTX204070。[LCM-3951]

- 有关 Windows 10 Redstone 4（Insider Preview 内部版本）中的已知问题的列表，请参阅知识中心文章 CTX231942。

累积更新 1 中的已知问题

- 从 StoreFront 3.12（XenApp 和 XenDesktop 7.15 LTSR）升级到 StoreFront 3.12.1000（XenApp 和 XenDesktop 7.15 LTSR CU1）后或在安装 StoreFront 3.12.1000 后，StoreFront 管理控制台不打开。StoreFront 管理控制台显示错误“MMC could not create the snap-in. The snap-in might not have been installed correctly.”（MMC 无法创建此管理单元。此管理单元可能未正确安装）。要解决此问题，请按照 CTX233206 中所述的步骤进行操作。[# LC8935]

- 在 Windows 7 或 Windows Server 2008 R2 计算机上安装通过 SHA-256 证书签名的驱动程序时，可能会显示 Microsoft WHQL（Windows 硬件质量实验室）消息。要解决此问题，请在计算机上安装下列 Microsoft 修补程序：
  - Windows 7（一个修补程序）：https://support.microsoft.com/en-us/help/2921916/the-untrusted-publisher-dialog-box-appears-when-you-install-a-driver-i
  - Windows Server 2008 R2（两个修补程序）：https://support.microsoft.com/en-us/help/2921916/the-untrusted-publisher-dialog-box-appears-when-you-install-a-driver-i 和 https://support.microsoft.com/en-us/help/2837108/you-cannot-import-a-windows-8-signed-driver-on-a-windows-server-2008-r [#LCM-2836]
- 禁用或停止了 Citrix Telemetry Service，并使用 metainstaller 将 XenApp 和 XenDesktop 7.15 LTSR 升级到累积更新 1 (CU1) 时，可能会显示以下警告消息：
  我们无法启动使您能够在 Call Home 中注册的 Citrix 服务。有关指导，请参阅 CTX218094。[#LCM-3642]

7.15 LTSR（初始版本）中的已知问题

XenApp 和 XenDesktop 7.15 LTSR 版本存在以下问题：

App-V

- 在 Studio 中，从应用程序节点或从选定交付组中删除一个或多个 App-V 应用程序时，显示消息“出现未知错误”。您可以放心地忽略该消息；应用程序会被删除。[#DNA-29702]

- 如果为该应用程序启动了一个子进程，但该子进程在应用程序关闭时无法关闭，您将无法从交付组中删除 App-V 应用程序。错误消息指示应用程序正在使用中。要确定进程名称，请运行 Get-AppVVirtualProcess.。然后通过任务管理器或 Stop-AppVClientPackage 终止该进程。[#DNA-23624]

- 从应用程序库中删除 App-V 软件包时，该软件包将从 Studio 显示屏幕中删除，但不从 VDA 中删除。解决方法：使用提升的

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

管理员权限从 VDA 运行以下 cmdlet：

```
Import-Module AppvClient
Get-AppVClientPackage -all
#确定要删除的软件包的软件包 ID 和版本 ID
Remove-AppVClientPackage -PackageId <packageid> -VersionId <versionid>
```

[#DNA-47379]

- 由于 Microsoft APP-V 的运行方式，使用单管理方法或双管理方法发布同一应用程序的多个排序的版本时，VDA 上的每个用户一次只能启动该应用程序的一个版本。无论用户首先启动哪个版本，都将决定随后为其运行的版本。即使不涉及 Citrix 组件，并且用户从指向不同路径的桌面快捷方式启动排序的版本时，也会出现相同的行为。到目前为止，我们 (Citrix) 已在 Mozilla Firefox 和 Google Chrome 浏览器的不同版本中发现过此问题。[#APPV-60]

安装和升级

- 将 VDA 7.14 升级到 VDA 7.15 时，在注册表项 HKEY_LOCAL_MACHINE\Software\Policies\Citrix 下使用**管理模板**为应用的 Citrix 策略设置创建的注册表项可能不会从 VDA 中删除。[#LCM-3876]

- 使用安装介质中的 AutoSelect 应用程序安装组件时，autorun.log 文件可能包含与权限不足有关的错误和异常。如果安装已成功完成，您可以忽略这些错误。但是，要避免出错，请使用**以管理员身份运行**启动 AutoSelect。[#DNA-45937]

- 将 XenDesktop 5.6 部署升级到 XenDesktop 7.15 LTSR 时，组策略将丢失。解决方法：先从 XenDesktop 5.6 升级到 XenDesktop 7.13。然后从 7.13 升级到 7.15 LTSR [#DNA-44818]

- 安装 Controller 时，如果安装向导的 **Smart Tools** 页面上选择**我想连接到 Smart Tools 和 Call Home**，Call Home 可能未启用。解决方法：使用 Citrix Scout 中的计划功能，或使用 PowerShell 启用 Call Home。[#CAM-9907]

- 在 Windows Server 2012 R2 或 Windows Server 2016 上安装 Delivery Controller 时，如果选择连接到 Smart Tools，且有多个组织与您的 Citrix Cloud 帐户链接，在您输入 Citrix Cloud 凭据后，登录过程可能无法完成。解决方法：完成以下操作之一：
  - 确保 Windows Server 和 Internet Explorer 具有最新的更新。
  - 清除 Internet Explore 浏览器选项：Internet 选项 > 安全 > 本地 Intranet > 站点 > 包括所有不使用代理服务器的站点。

  [#CAM-9816]

- 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]

- 从 7.13 之前的版本将 Delivery Controller 升级到 7.13 及更高版本时，如果在任意策略中配置了“客户端自动重新连接超时”设置，则会出现错误（异常）。如果“客户端自动重新连接超时”设置的值不在允许的范围（0 到 300）内，则会出现此错误（首先在 7.13 版中引入的）。要阻止出现此错误，请使用 Citrix 组策略 PowerShell 提供程序取消配置该设置，或者将其设置为指定范围内的值。有关示例，请参阅 CTX22947。[#DNA-52476]

- 选择计算机并将其添加到现有交付组时，Studio 允许您将不兼容计算机目录中的计算机添加到同一交付组。（如果先选择交付组并向其添加计算机，Studio 会正确阻止添加不兼容计算机目录中的计算机。） [#DNA-39589]

常规

- 使用联合身份验证服务会话中证书对 TLS 1.1（或早期版本）连接进行身份验证时，连接会失败。系统将记录事件 ID 305，指示不受支持的哈希 ID。联合身份验证服务不支持 SHAMD5 哈希。要解决此问题，请使用 TLS 1.2 连接。此问题影响 XenApp 和 XenDesktop 7.9 到此版本。[#DNA-47628]

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

- 策略设置不保存在“打印机驱动程序映射和兼容性”策略中。解决方法：使用 Citrix 组策略 PowerShell 提供程序编辑此设置。有关解决方法的详细信息，请参阅 CTX226589。[#DNA-47423]
- Windows 事件日志错误“Windows is unable to verify the image integrity of the file MfApHook64.dll”（Windows 无法验证文件 MfApHook64.dll 的图像完整性）。有关详细信息，请参阅 CTX226397。[HDX-9063]
- 从 StoreFront 启动应用程序时，该应用程序可能无法在前台启动，或者该应用程序在前台启动，但可能没有焦点。解决方法：单击任务栏中的图标将应用程序置于前面，或者单击应用程序屏幕中的图标将其置于焦点之下。[#HDX-10126]
- 从 Citrix Receiver 启动时，无法成功启动已发布的内容。通过 StoreFront Web 客户端（或 Web Interface）启动的内容将按预期启动。[#LC6316，#RFWIN-4957]
- 与 VMware VSAN 6.x 结合使用时，Machine Creation Services (MCS) 图像更新过程可能会失败，因为标识磁盘无法可靠地检索并附加回虚拟机。如果出现此问题，请手动删除并重新创建虚拟机，或者创建一个新目录用于映像更新。有关详细信息，请参阅 CTX219670。
- 删除 Azure Resource Manager 计算机目录时，关联的计算机和资源组将从 Azure 中删除，即使您指示应保留这些计算机和资源组亦如此。[#DNA-37964]
- 使用高于版本 4.6 的 Citrix Receiver for Windows 时，多播功能可能无法显示视频。音频仍可用。解决方法：在端点上添加以下注册表项：

  HKEY_CURRENT_USER\Software\Citrix\HdxMediaStream\
  名称：DisableVMRSupport
  类型：DWORD
  值：4

  [#HDX-10055]

打印

- 停止或重新启动 Citrix Print Manager Service 可能会将 CpSvc.exe 进程保留在无响应状态。解决方法：先停止 CpsSvc.exe 进程，然后再停止或重新启动“服务”管理单元中的服务，或者重新启动 VDA 以避免出现此问题。[#HDX-10071]
- 在虚拟桌面中选择的通用打印服务器打印机不会在 Windows“控制面板”的**设备和打印机**窗口中显示。但是，当用户在使用应用程序时，可以使用这些打印机进行打印。此问题仅出现在 Windows Server 2012、Windows 10 和 Windows 8 平台上。有关详细信息，请参阅知识中心文章 CTX213540。[#335153]

Profile Management

尝试启动 Microsoft Windows 10 会话时，Profile Management 会导致显示黑屏。应用此修复后，必须配置策略“要同步的目录”并添加文件夹 *AppData\Local\Microsoft\Windows\Caches*。有关其他信息和解决方法，请参阅知识中心文章 CTX234144。[#LC-9030]

会话录制

- 如果 Machine Creation Services (MCS) 或 Provisioning Services (PVS) 创建的多个 VDA 具有配置的主映像并安装了 Microsoft 消息队列 (MSMQ)，则在某些情况下，这些 VDA 可能具有相同的 QMId。这样可能会导致各种问题，例如：
  - 即使接受了录制协议，也可能无法录制会话。
  - Session Recording Server 可能收不到会话注销信号，从而导致会话可能始终处于活动状态。

  有关解决方法，请参阅 Session Recording 安装文章。[#528678]

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

第三方问题

- Citrix 和 Microsoft 已确定从运行 Windows Server 2016 的服务器 VDA 启动无缝应用程序时会出现问题。用户从此 VDA 启动已发布的应用程序时，Citrix Receiver 将显示一个覆盖监视器的工作区的黑屏几秒钟时间，然后再启动应用程序。有关详细信息，请参阅 https://support.citrix.com/article/CTX225819。

  警告：如果要使用 Azure Active Directory (AAD)，请不要按 CTX225819 中所述更改注册表。做出此更改可能会导致 AAD 用户的会话启动失败。[HDX-5000]

- 在压力测试环境中执行 20000 次登录，Microsoft Windows WinLogon.exe 间歇性崩溃的频率可能会小于 0.001%。 [#HDX-9938]

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

第三方声明

Apr 18, 2018

此版本的 XenApp 和 XenDesktop 可能包含根据以下文档定义的条款获得许可的第三方软件：

PDF XenApp 和 XenDesktop 第三方声明

PDF 适用于 FlexNet Publisher 2016 R1 (11.14.0.0) 的商业软件保密

PDF FLEXnet Publisher 文档补充：适用于 FlexNet Publisher 11.14.0 的开源软件许可证

PDF Session Recording 第三方声明

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

弃用

Apr 18, 2018

本文声明旨在提前通知您正在逐渐淘汰的平台、Citrix 产品和功能，以便您能够及时制定业务决策。Citrix 将监视客户使用情况和反馈以确定其退出时间。此列表在后续版本中会有更改，可能不会包括每个弃用的特性或功能。

以下平台、Citrix 产品和功能*已弃用*。这并不意味着会立即删除它们。Citrix 继续在此 XenApp 和 XenDesktop 7.15 长期服务版本 (LTSR) 向其提供支持。弃用项目将在此 LTSR 之后的当前版本中删除。如有可能，会提供建议的弃用项目的替代项目。

有关产品生命周期支持的详细信息，请参阅 Product Lifecycle Support Policy（产品生命周期支持策略）一文。

项目	宣布弃用的版本	替代项目
Citrix Receiver for Web 经典体验（“绿色气泡”用户界面）。	7.15 LTSR（和 StoreFront 3.12）	Citrix Receiver for Web 统一体验。
Windows 10 版本 1511 (Threshold 2) 及早期版本的 Windows 桌面操作系统版本（包括 Windows 8.x 和 Windows 7）上的 VDA。	7.15 LTSR（和 7.12）	在 Windows 10 版本 1607 (Redstone 1) 或更高版本的 Semi-Annual Channel 上安装桌面操作系统 VDA。如果使用的是 1607 LTSB，我们建议使用 7.15 VDA。
Windows Server 2008 R2 和 Windows Server 2012（包括 Service Pack）上的 VDA。	7.15 LTSR（和 7.12）	应在支持的版本（例如 Windows Server 2012 R2 或 Windows Server 2016）上安装服务器操作系统 VDA。
Windows Server 2012 和 2008 R2（包括 Service Pack）上的 Delivery Controller。	7.15 LTSR	在受支持的备用操作系统中安装 Delivery Controller。
Windows 7（包括 Service Pack）上的 Studio。	7.15 LTSR	在受支持的备用操作系统中安装 Studio。
Flash 重定向。	7.15 LTSR	使用 HTML5 视频。有关详细信息，请参阅 Flash 重定向生命周期结束备注。
DirectX Command Remoting (DCR)。	7.15 LTSR	使用 Thinwire。
与 StoreFront 的 Citrix Online 集成（Goto 产品）。	7.14 （和 StoreFront 3.11）	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。有关详细信息，请参阅将 Citrix Online 应用程序与应用商店集成。
StoreFront 2.0、2.1、2.5 和 2.5.2 中的原位升	7.13	从其中一个版本升级到受支持的更高版本，然后升

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

级。		级到 XenApp 和 XenDesktop 7.13。
XenDesktop 5.6 或 5.6 FP1 中的原位升级。	7.12	将 XenDesktop 5.6 或 5.6 FP1 部署迁移到当前 XenDesktop 版本。
Windows 8.1 和早期 Windows 桌面版本上的 VDA。	7.12	应在 Windows 10 上安装桌面操作系统 VDA。
Windows Server 2008 R2 上的 VDA。	7.12	应在支持的版本（例如 Windows Server 2012 R2 或 Windows Server 2016）上安装服务器操作系统 VDA。
Windows XP 上使用的 XenDesktop 5.6。将不支持 Windows XP 上安装的任何 VDA。	7.12	应在支持的 Windows 版本上安装 VDA。
CloudPlatform 连接。	7.12	应使用其他受支持的虚拟机管理程序或云服务。
Azure 经典（也称为 Azure 服务管理）连接。	7.12	应使用 Azure 资源管理器。
在 32 位计算机上安装核心组件（Studio 除外）：Delivery Controller、Director、StoreFront 和许可证服务器。	7.12	应使用 64 位计算机。
连接租用。	7.12	使用本地主机缓存。
旧 Thinwire 模式	7.12	使用 Thinwire。
HDX 桌面组合重定向 (DCR)	7.12	

AppDisk 和 Personal vDisk

XenApp 和 XenDesktop 提供的 AppDisk 和 Personal vDisk 功能现在已对当前版本禁用*。Citrix 正在将此功能替换为最近从 Unidesk 收购的技术（Citrix 应用分层）。在此转换期间，Citrix 会继续维护当前支持级别，如 XenApp and XenDesktop Servicing Options（XenApp 和 XenDesktop 服务方案）中所述。

* AppDisk 和 Personal vDisk 现在不包含在长期服务版本 (LTSR) 服务方案中。

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

Section 508 Voluntary Product Accessibility Template

Apr 18, 2018

- PDF Citrix XenApp 和 XenDesktop 7.15 Director VPAT
- PDF Citrix XenApp 和 XenDesktop 7.15 Installer VPAT
- PDF Citrix XenApp 和 XenDesktop 7.15 许可管理控制台 VPAT
- PDF Citrix XenApp 和 XenDesktop 7.15 Licensing Manager VPAT
- PDF Citrix XenApp 和 XenDesktop 7.15 Receiver for Web 经典经验 VPAT
- PDF Citrix XenApp 和 XenDesktop 7.15 Receiver for Web 统一体验 VPAT
- PDF Citrix XenApp 和 XenDesktop 7.15 StoreFront VPAT
- PDF Citrix XenApp 和 XenDesktop 7.15 Studio VPAT
- PDF Citrix Provisioning Services Boot Device Manager VPAT
- PDF Citrix Provisioning Services BOOTPTAB 编辑器 VPAT
- PDF Citrix Provisioning Services 客户端映像向导 VPAT
- PDF Citrix Provisioning Services 配置向导 VPAT
- PDF Citrix Provisioning Services 控制台 VPAT
- PDF Linux VDA VPAT
- PDF Citrix Scout VPAT
- PDF Citrix Session Recording Player VPAT
- PDF Citrix Session Recording Authorization 控制台 VPAT
- PDF Citrix Workspace Environment Management Administration 控制台 VPAT
- PDF Citrix Workspace Environment Management Infrastructure Service 配置 VPAT
- PDF Citrix Workspace Environment Management Agent Log Parser VPAT
- PDF Citrix Workspace Environment Management Installer VPAT
- PDF Citrix Workspace Environment Management Profile Cleanser VPAT
- PDF Citrix Workspace Environment Management Integrity Condition List Manager VPAT

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

PDF Citrix Workspace Environment Management 数据库管理实用程序 VPAT

PDF Citrix 自助服务密码重置 VPAT

PDF Citrix SCOM Management Pack VPAT

PDF Citrix Receiver for macOS VPAT

PDF Citrix Management Pack 配置 VPAT

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

系统要求

Apr 18, 2018

In this article:

- Introduction
- Delivery Controller
- Databases
- Citrix Studio
- Citrix Director
- Virtual Delivery Agent (VDA) for Desktop OS
- Virtual Delivery Agent (VDA) for Server OS
- Hosts / virtualization resources
- Active Directory functional levels
- HDX
- Session Recording
- Universal Print Server
- Other

Introduction

The system requirements in this document were valid when this product version released; updates are made periodically. System requirements components not covered here (such as StoreFront, host systems, Citrix Receivers and plug-ins, and Provisioning Services) are described in their respective documentation.

Important: Review the Prepare to install article before beginning an installation.

Unless otherwise noted, the component installer deploys software prerequisites automatically (such as .NET and C++ packages) if the required versions are not detected on the machine. The Citrix installation media also contains some of this prerequisite software.

The installation media contains several third-party components. Before using the Citrix software, check for security updates from the third party, and install them.

For globalization information, see CTX119253.

For XenApp and XenDesktop components and features that can be installed on Windows Servers, Server Core and Nano Server installations are not supported, unless specifically noted.

For components and features that can be used on Windows 10 machines, the following Windows 10 servicing options and editions are supported:

- Semi-annual Channel: Pro, Enterprise, Education, Mobile Enterprise (the IoT Core Pro Edition is supported only for Citrix Receiver).
- Long-term Servicing Channel (LTSC): Enterprise LTSB Edition

  For further details, see CTX224843.

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

Hardware requirements

RAM and disk space values are in addition to requirements for the product image, operating system, and other software on the machine. Your performance will vary, depending on your configuration. This includes the features you use, plus the number of users, and other factors. Using only the minimum can result in slow performance.

For example, the amount of disk space needed on the Controller for connection leasing (which is enabled by default) depends on the number of users, applications, and the mode: 100,000 RDS users with 100 recently-used applications require approximately 3 GB for connection leases; deployments with more applications may require more space. For dedicated VDI desktops, 40,000 desktops require at least 400-500 MB. In all cases, Citrix suggests providing several GBs of additional space.

The following table shows the minimum requirements for core components.

Component	**Minimum**
All core components on one server, for an evaluation only, not a production deployment	5 GB RAM
All core components on one server, for a test deployment or a small production environment	12 GB RAM
Delivery Controller (more disk space required if a high availability feature such as connection leasing is enabled)	5 GB RAM 800 MB hard disk Database: see the Sizing guidance article
Studio	1 GB RAM 100 MB hard disk
Director	2 GB RAM 200 MB hard disk
StoreFront	2 GB RAM See the StoreFront documentation for disk recommendations
License Server	2 GB RAM See the Licensing documentation for disk recommendations

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

Sizing of VMs that deliver desktops and applications

Specific recommendations cannot be provided because of the complex and dynamic nature of hardware offerings, and every XenApp and XenDesktop deployment has unique needs. Generally, sizing a XenApp VM is based on the hardware and not the user workloads (except for RAM; you'll need more RAM for applications that consume more). The Citrix VDI Handbook and Best Practices contains the latest guidance on VDA sizing.

Delivery Controller

Supported operating systems:

- Windows Server 2016, Standard and Datacenter Editions
- Windows Server 2012 R2, Standard and Datacenter Editions
- Windows Server 2012, Standard and Datacenter Editions
- Windows Server 2008 R2 SP1, Standard, Enterprise, and Datacenter Editions

Requirements:

- Microsoft .NET Framework 3.5.1 (Windows Server 2008 R2 only).
- Microsoft .NET Framework 4.5.2 (4.6 through 4.7 are also supported).
- Windows PowerShell 3.0 or later.
- Microsoft Visual C++ 2015 Runtime, 32- and 64-bit.

Databases

Supported Microsoft SQL Server versions for the Site Configuration, Configuration Logging, and Monitoring databases:

- SQL Server 2017, Express, Standard, and Enterprise Editions.
- SQL Server 2016 through SP1, Express, Standard, and Enterprise Editions.
- SQL Server 2014 through SP2, Express, Standard, and Enterprise Editions. By default, SQL Server 2014 SP2 Express is installed when installing the Controller, if an existing supported SQL Server installation is not detected.
- SQL Server 2012 through SP4, Express, Standard, and Enterprise Editions.
- SQL Server 2008 R2 SP2 and SP3, Express, Standard, Enterprise, and Datacenter Editions.

The following database high availability solutions are supported (except for SQL Server Express, which supports only standalone mode):

- SQL Server AlwaysOn Failover Cluster Instances
- SQL Server AlwaysOn Availability Groups (including Basic Availability Groups)
- SQL Server Database Mirroring

Windows authentication is required for connections between the Controller and the SQL Server Site database.

When installing a Controller, a SQL Server Express database is installed by default for use with the Local Host Cache feature. This installation is separate from the default SQL Server Express installation for the Site database.

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

For more information, see the following articles:

- Databases
- CTX114501
- Database sizing guidance
- Local Host Cache

Citrix Studio

Supported operating systems:

- Windows 10 (see edition support in the *Introduction* section)
- Windows 8.1, Professional and Enterprise Editions
- Windows 7 Professional, Enterprise, and Ultimate Editions
- Windows Server 2016, Standard and Datacenter Editions
- Windows Server 2012 R2, Standard and Datacenter Editions
- Windows Server 2012, Standard and Datacenter Editions
- Windows Server 2008 R2 SP1, Standard, Enterprise, and Datacenter Editions

Requirements:

- Microsoft .NET Framework 4.5.2 (4.6 through 4.7 are also supported)
- Microsoft .NET Framework 3.5 SP1 (Windows Server 2008 R2 and Windows 7 only)
- Microsoft Management Console 3.0 (included with all supported operating systems)
- Windows PowerShell 2.0

Citrix Director

Supported operating systems:

- Windows Server 2016, Standard and Datacenter Editions
- Windows Server 2012 R2, Standard and Datacenter Editions
- Windows Server 2012, Standard and Datacenter Editions
- Windows Server 2008 R2 SP1, Standard, Enterprise, and Datacenter Editions

Requirements:

- Microsoft .NET Framework 4.5.2 (4.6 through 4.7 are also supported).
- Microsoft .NET Framework 3.5 SP1 (Windows Server 2008 R2 only)
- Microsoft Internet Information Services (IIS) 7.0 and ASP.NET 2.0. Ensure that the IIS server role has the Static Content role service installed. If these are not already installed, you are prompted for the Windows Server installation media, then they are installed for you.

System Center Operations Manager (SCOM) integration requirements:

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager

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

Supported browsers for viewing Director:

- Internet Explorer 11. (You can use Internet Explorer 10 only on Windows Server 2012 R2 machines.) Compatibility mode is not supported for Internet Explorer. You must use the recommended browser settings to access Director. When you install Internet Explorer, accept the default to use the recommended security and compatibility settings. If you already installed the browser and chose not to use the recommended settings, go to Tools > Internet Options > Advanced > Reset and follow the instructions.
- Microsoft Edge.
- Firefox ESR (Extended Support Release).
- Chrome.

The recommended optimal screen resolution for viewing Director is 1366 x 1024.

Virtual Delivery Agent (VDA) for Desktop OS

Supported operating systems:

- Windows 10, (see edition support in the *Introduction* section. The following features are not supported on Windows 10: desktop composition redirection and legacy graphics mode.
- Windows 8.1, Professional and Enterprise Editions
- Windows 7 SP1, Professional, Enterprise, and Ultimate Editions

Requirements:

- Microsoft .NET Framework 4.5.2 (4.6 through 4.7 are also supported)
- Microsoft .NET Framework 3.5.1 (Windows 7 only)
- Microsoft Visual C++ 2013 and 2015 Runtimes, 32- and 64-bit

Remote PC Access uses this VDA, which you install on physical office PCs. This VDA supports Secure Boot for XenDesktop Remote PC Access on Windows 10.

Several multimedia acceleration features (such as HDX MediaStream Windows Media Redirection) require that Microsoft Media Foundation be installed on the machine on which you install the VDA. If the machine does not have Media Foundation installed, the multimedia acceleration features will not be installed and will not work. Do not remove Media Foundation from the machine after installing the Citrix software; otherwise, users will not be able to log on to the machine. On most supported Windows desktop OS editions, Media Foundation support is already installed and cannot be removed. However, N editions do not include certain media-related technologies; you can obtain that software from Microsoft or a third party. For more information, see Prepare to install.

During VDA installation, you can choose the HDX 3D Pro mode of the VDA for Windows Desktop OS. That mode is particularly suited for use with DirectX and OpenGL-driven applications and with rich media such as video. See the HDX 3D Pro section for additional support information.

For Linux VDA information, see the Linux Virtual Delivery Agent articles.

To use the Server VDI feature, you can use the command line interface to install a VDA for Windows Desktop OS on a supported server operating system. See Server VDI for guidance.

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

Virtual Delivery Agent (VDA) for Server OS

Supported operating systems:

- Windows Server 2016, Standard and Datacenter Editions
- Windows Server 2012 R2, Standard and Datacenter Editions
- Windows Server 2012, Standard and Datacenter Editions
- Windows Server 2008 R2 SP1, Standard, Enterprise, and Datacenter Editions

The installer automatically deploys the following requirements, which are also available on the Citrix installation media in the Support folders:

- Microsoft .NET Framework 4.5.2 (4.6 through 4.7 are also supported)
- Microsoft .NET Framework 3.5.1 (Windows Server 2008 R2 only)
- Microsoft Visual C++ 2013 and 2015 Runtimes, 32- and 64-bit

The installer automatically installs and enables Remote Desktop Services role services, if they are not already installed and enabled.

Several multimedia acceleration features (such as HDX MediaStream Windows Media Redirection) require that the Microsoft Media Foundation be installed on the machine on which you install the VDA. If the machine does not have Media Foundation installed, the multimedia acceleration features will not be installed and will not work. Do not remove Media Foundation from the machine after installing the Citrix software; otherwise, users will not be able to log on to the machine. On most Windows Server versions, the Media Foundation feature is installed through the Server Manager (for Windows Server 2012 and later: ServerMediaFoundation; for Windows Server 2008 R2: DesktopExperience). However, N editions do not include certain media-related technologies; you can obtain that software from Microsoft or a third party. For more information, see Prepare to install.

If Media Foundation is not present on the VDA, these multimedia features do not work:

- Flash Redirection
- Windows Media Redirection
- HTML5 Video Redirection
- HDX Realtime Webcam Redirection

For Linux VDA information, see the Linux Virtual Delivery Agent articles.

Hosts / virtualization resources

Some XenApp and XenDesktop features may not be supported on all host platforms or all platform versions. For example, AppDisks are supported with XenServer, VMware, and System Center Virtual Machine Manager hosts. See the feature documentation for details.

The Remote PC Access Wake on LAN feature requires Microsoft System Center Configuration Manager minimum 2012.

Supported host platforms and virtualization environments

IMPORTANT: The following *major.minor* versions are supported, including updates to those versions. CTX131239 contains

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

the most current hypervisor version information, plus links to known issues.

XenServer

- XenServer 7.4
- XenServer 7.3
- XenServer 7.2
- XenServer 7.1 LTSR
- XenServer 7.0
- XenServer 6.5 and SP1
- XenServer 6.2 SP1 plus hotfixes (you must apply SP1 to enable application of future hotfixes)
- XenServer 6.1

VMware vSphere (vCenter + ESXi). No support is provided for vSphere vCenter Linked Mode operation.

- VMware vSphere 6.5
- VMware vSphere 6.0
- VMware vSphere 5.5
- VMware vSphere 5.1
- VMware vSphere 5.0
- VMware vCenter 5.5, 6, and 6.5 appliance

System Center Virtual Machine Manager. Includes any version of Hyper-V that can register with the supported System Center Virtual Machine Manager versions.

- System Center Virtual Machine Manager 2016
- System Center Virtual Machine Manager 2012 R2
- System Center Virtual Machine Manager 2012 SP1
- System Center Virtual Machine Manager 2012

Nutanix Acropolis 4.5

Amazon Web Services (AWS)

- You can provision applications and desktops on supported Windows server operating systems.
- The Amazon Relational Database Service (RDS) is not supported.
- See Citrix XenDesktop on AWS for additional information.

CloudPlatform

- The minimum supported version is 4.2.1 with hotfixes 4.2.1-4.
- Deployments were tested using XenServer 6.2 (with Service Pack 1 and hotfix XS62ESP1003) and vSphere 5.1 hypervisors.
- CloudPlatform does not support Hyper-V hypervisors.
- CloudPlatform 4.3.0.1 supports VMware vSphere 5.5.
- See the CloudPlatform documentation (including the Release Notes for your CloudPlatform version) for more information.

Microsoft Azure

Microsoft Azure Resource Manager

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

Active Directory functional levels

The following functional levels for the Active Directory forest and domain are supported:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003
- Windows 2000 native (not supported for domain controllers)

HDX

UDP audio for Multi-Stream ICA is supported on Receiver for Windows and Citrix Receiver for Linux 13.

Echo cancellation is supported on Citrix Receiver for Windows.

See the specific HDX feature support and requirements below.

HDX Desktop Composition Redirection

The Windows user device or thin client must support or contain:

- DirectX 9
- Pixel Shader 2.0 (supported in hardware)
- 32 bits per pixel
- 1.5 GHz 32-bit or 64-bit processor
- 1 GB RAM
- 128 MB video memory on the graphic card or an integrated graphics processor

HDX queries the Windows device to verify that it has the required GPU capabilities, and then automatically reverts to server-side desktop composition if it does not. List the devices with the required GPU capabilities that do not meet the processor speed or RAM specifications in the GPO group for devices excluded from Desktop Composition Redirection.

The minimum available bandwidth is 1.5 Mbps; the recommended bandwidth is 5 Mbps. Those values incorporate end-to-end latency.

HDX Windows Media delivery

The following clients are supported for Windows Media client-side content fetching, Windows Media redirection, and realtime Windows Media multimedia transcoding: Citrix Receiver for Windows, Citrix Receiver for iOS, and Citrix Receiver for Linux.

To use Windows Media client-side content fetching on Windows 8 devices, set the Citrix Multimedia Redirector as a default program: in **Control Panel > Programs > Default Programs > Set your default programs**, select **Citrix Multimedia Redirector** and click either **Set this program as default** or **Choose defaults for this program**. GPU transcoding requires an NVIDIA CUDA-enabled GPU with Compute Capability 1.1 or higher; see http://developer.nvidia.com/cuda/cuda-gpus.

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

HDX Flash Redirection

The following clients and Adobe Flash Players are supported:

- Citrix Receiver for Windows (for second generation Flash Redirection features) - Second generation Flash Redirection features require Adobe Flash Player for Other Browsers, sometimes referred to as an NPAPI (Netscape Plugin Application Programming Interface) Flash Player.
- Citrix Receiver for Linux (for second generation Flash Redirection features) - Second generation Flash Redirection features require Adobe Flash Player for other Linux or Adobe Flash Player for Ubuntu.
- Citrix Online plug-in 12.1 (for legacy Flash Redirection features) - Legacy Flash Redirection features require Adobe Flash Player for Windows Internet Explorer (sometimes referred to as an ActiveX player).

The major version number of the Flash Player on the user device must be greater than or equal to the major version number of the Flash Player on the server. If an earlier version of the Flash Player is installed on the user device, or if the Flash Player cannot be installed on the user device, Flash content is rendered on the server.

The machines running VDAs require:

- Adobe Flash Player for Windows Internet Explorer (the ActiveX player)
- Internet Explorer 11 (in non-Modern UI mode). You can use Internet Explorer versions 7-10, but Microsoft supports (and Citrix recommends using) version 11. Flash redirection requires Internet Explorer on the server; with other browsers, Flash content is rendered on the server.
- Protected mode disabled in Internet Explorer (Tools > Internet Options > Security tab > Enable Protected Mode check box cleared). Restart Internet Explorer to effect the change.

HDX 3D Pro

When installing a VDA for Windows Desktop OS, you can choose to install the HDX 3D Pro version.

The physical or virtual machine hosting the application can use GPU Passthrough or Virtual GPU (vGPU):

- GPU Passthrough is available with: Citrix XenServer; Nutanix AHV, VMware vSphere and VMware ESX, where it is referred to as virtual Direct Graphics Acceleration (vDGA); and with Microsoft Hyper-V in Windows Server 2016 where it is referred to as Discrete Device Assignment (DDA).
- vGPU is available with Citrix XenServer, Nutanix AHV, and VMware vSphere; see https://www.citrix.com/products/xenapp-xendesktop/hdx-3d-pro.html.

Citrix recommends that the host computer have at least 4 GB of RAM and four virtual CPUs with a clock speed of 2.3 GHz or higher.

Graphical Processing Unit (GPU):

- For CPU-based compression (including lossless compression), HDX 3D Pro supports any display adapter on the host computer that is compatible with the application being delivered.
- For virtualized graphics acceleration using the NVIDIA GRID API, HDX 3D Pro can be used with supported NVIDIA GRID cards (see NVIDIA GRID). The NVIDIA GRID delivers a high frame rate, resulting in a highly interactive user experience.
- Virtualized graphics acceleration is supported on the Intel Xeon Processor E3 Family of data center graphics platform. For more information, see http://www.citrix.com/intel and http://www.intel.com/content/www/us/en/servers/data-center-graphics.html
- Virtualized graphics acceleration is supported with AMD RapidFire on the AMD FirePro S-series server cards (see AMD Virtualization Solution).

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

User device:

- HDX 3D Pro supports all monitor resolutions that are supported by the GPU on the host computer. However, for optimum performance with the minimum recommended user device and GPU specifications, Citrix recommends a maximum monitor resolution for user devices of 1920 x 1200 pixels for LAN connections, and 1280 x 1024 pixels for WAN connections.
- Citrix recommends that user devices have at least 1 GB of RAM and a CPU with a clock speed of 1.6 GHz or higher. Use of the default deep compression codec, which is required on low-bandwidth connections, requires a more powerful CPU unless the decoding is done in hardware. For optimum performance, Citrix recommends that user devices have at least 2 GB of RAM and a dual-core CPU with a clock speed of 3 GHz or higher.
- For multi-monitor access, Citrix recommends user devices with quad-core CPUs.
- User devices do not need a GPU to access desktops or applications delivered with HDX 3D Pro.
- Citrix Receiver must be installed.

For more information, see the HDX 3D Pro articles and www.citrix.com/xenapp/3d.

HDX video conferencing requirements for webcam video compression

Supported clients: Citrix Receiver for Windows, Citrix Receiver for Mac, and Citrix Receiver for Linux.

Supported video conferencing applications:

- Adobe Connect
- Cisco WebEx
- Citrix GoToMeeting HDFaces
- Google+ Hangouts
- IBM Sametime
- Media Foundation-based video applications on Windows 8.x, Windows Server 2012, and Windows Server 2012 R2
- Microsoft Lync 2010 and 2013
- Microsoft Office Communicator
- Microsoft Skype 6.7

To use Skype on a Windows client, edit the registry on the client and the server:

Client registry key HKEY_CURRENT_USER\Software\Citrix\HdxRealTime

Name: DefaultHeight , Type: REG_DWORD, Data: 240

Name: DefaultWidth, Type: REG_DWORD, Data: 320

Server registry key HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Vd3d\Compatibility

Name: skype.exe, Type: REG_DWORD, Data: Set to 0

Other user device requirements:

- Appropriate hardware to produce sound.
- DirectShow-compatible webcam (use the webcam default settings). Webcams that are hardware encoding capable reduces client-side CPU usage.
- Webcam drivers, obtained from the camera manufacturer if possible.

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

Session Recording

Session Recording administration components

You can install the Session Recording administration components (Session Recording Database, Session Recording Server, and Session Recording Policy Console) on a single server or on different servers.

Session Recording Database

Supported operating systems:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1

Supported Microsoft SQL Server versions:

- Microsoft SQL Server 2016 SP1 Enterprise, Express, and Standard editions
- Microsoft SQL Server 2014 SP2 Enterprise, Express, and Standard editions
- Microsoft SQL Server 2012 SP3 Enterprise, Express, and Standard editions
- Microsoft SQL Server 2008 R2 SP3 Enterprise, Express, and Standard editions

Requirement: .NET Framework 4.7, 4.6.2, or 4.5.2

Session Recording Server

Supported operating systems:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1

Other requirements:

- Internet Information Services (IIS) 10, 8.5, 8.0, or 7.5
- .NET Framework Version 4.7, 4.6.2, or 4.5.2
- If the Session Recording Server uses HTTPS as its communications protocol, add a valid certificate. Session Recording uses HTTPS by default, which Citrix recommends.
- Microsoft Message Queuing (MSMQ), with Active Directory integration disabled and MSMQ HTTP support enabled.
- For Administrator Logging: Latest version of Chrome, Firefox, or Internet Explorer 11

Session Recording Policy Console

Supported operating systems:

- Windows Server 2016
- Windows Server 2012 R2

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

- Windows Server 2012
- Windows Server 2008 R2 SP1

Requirement: .NET Framework 4.7, 4.6.2, or 4.5.2

Session Recording Agent

Install the Session Recording Agent on every XenApp and XenDesktop server on which you want to record sessions.

Supported operating systems:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1
- Windows 10
- Windows 8.1
- Windows 7 SP1

Requirements:

- XenApp/XenDesktop 7.15 with Platinum license
- XenApp/XenDesktop 7.6.4000 with Platinum license (VDA for Windows Server OS only; VDA for Windows Desktop OS not supported)
- .NET Framework 4.7, 4.6.2, or 4.5.2
- Microsoft Message Queuing (MSMQ), with Active Directory integration disabled and MSMQ HTTP support enabled

Session Recording Player

Supported operating systems:

- Windows 10
- Windows 8.1
- Windows 7 SP1

Requirement: .NET Framework 4.7, 4.6.2, or 4.5.2

For optimal results, install Session Recording Player on a workstation with:

- Screen resolution of 1024 x 768
- Color depth of at least 32-bit
- 2GB RAM minimum; additional RAM and CPU/GPU resources can improve performance when playing graphics-intensive recordings, especially when recordings contain many animations

The seek response time depends on the size of the recording and your machine's hardware specifications.

Universal Print Server

The Universal Print Server comprises client and server components. The UpsClient component is included in the VDA installation. You install the UpsServer component on each print server where shared printers reside that you want to

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

provision with the Citrix Universal Print Driver in user sessions.

The UpsServer component is supported on:

- Windows Server 2016
- Windows Server 2012 R2 and 2012
- Windows Server 2008 R2 SP1

Requirement: Microsoft Visual C++ 2013 Runtime, 32- and 64-bit

For VDAs for Windows Server OS, user authentication during printing operations requires the Universal Print Server to be joined to the same domain as the VDA.

Standalone client and server component packages are also available for download.

For more information, see Provision printers.

Other

StoreFront 3.12.2000 is the minimum supported version with this release. To use the zone preference feature, you must be using minimum StoreFront 3.12.2000 or later and NetScaler Gateway 11.0-65.x.

When using Provisioning Services with this release, the minimum supported Provisioning Services version is 7.15.3.

Only Citrix License Server 11.14 is supported.

The Microsoft Group Policy Management Console (GPMC) is required if you store Citrix policy information in Active Directory rather than the Site Configuration database. If you install CitrixGroupPolicyManagement_x64.msi separately (for example, on a machine that does not have a XenApp or XenDesktop core component installed), that machine must have Visual Studio 2015 runtime installed. For more information, see the Microsoft documentation.

Multiple network interface cards are supported.

By default, the Citrix Receiver for Windows is installed when you install a VDA. For more information, see the Citrix Receiver for Windows documentation.

See App-V for supported versions of Microsoft App-V.

See Local App Access for supported browser information for that feature.

See the Self-Service Password Reset documentation for support and requirements information.

Client folder redirection - Supported operating systems:

- Server: Windows Server 2008 R2 SP1, Windows Server 2012, and Windows Server 2012 R2
- Client (with latest Citrix Receiver for Windows): Windows 7, Windows 8, and Windows 8.1

Mixed DPIs with multi-monitors. The use of different DPIs between monitors is not supported in Citrix XenDesktop and XenApp environments. You can verify the DPI (% scaling) using Windows Control Panel > Display options. If using a Windows 8.1 or Windows 10 client device, enabling the **Let me choose one scaling level for all my displays option** in the Windows Control Panel > Display options will configure the monitors appropriately. For more information, see CTX201696.

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

This version of XenApp and XenDesktop is not compatible with AppDNA 7.8 and AppDNA 7.9. Citrix recommends using the current AppDNA release.

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

技术概述

Dec 05, 2017

在本文中：

- XenApp 和 XenDesktop 主要组件
- 典型部署的工作原理
- 用户连接的处理方式
- 数据访问的工作方式
- 交付桌面和应用程序：计算机目录、交付组和应用程序组

XenApp 和 XenDesktop 是虚拟化解决方案。利用这些方案，IT 可以在提供随时随地访问任何设备的同时，控制虚拟机、应用程序、许可和安全性。

XenApp 和 XenDesktop 允许：

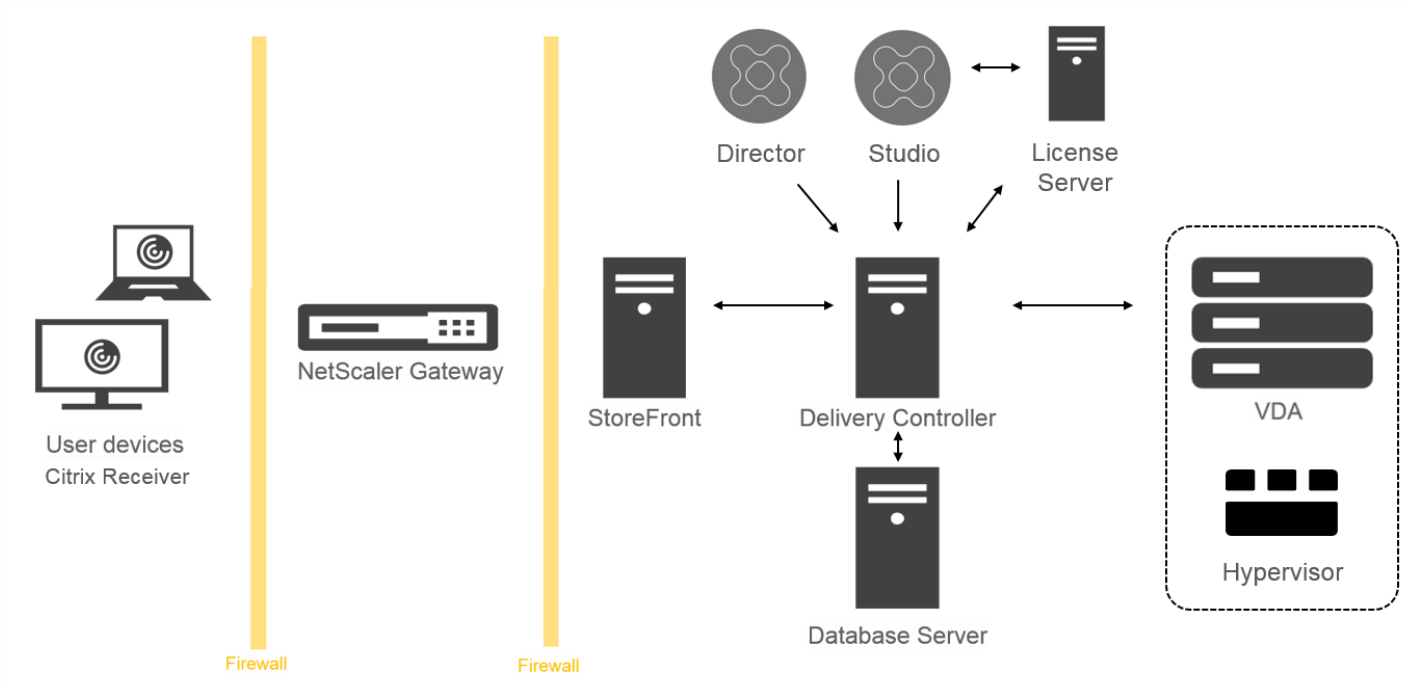
- 最终用户独立于设备的操作系统和界面运行应用程序和桌面。
- 管理员管理网络并控制来自选定设备或所有设备的访问。
- 管理员从单个数据中心管理整个网络。

XenApp 和 XenDesktop 共享统一的体系结构 FlexCast Management Architecture (FMA)。FMA 的主要功能是可以通过单个站点和集成置备运行多个版本的 XenApp 或 XenDesktop。

XenApp 和 XenDesktop 主要组件

提示：如果您不了解 XenApp 或 XenDesktop，本文非常有用。如果您当前拥有 6.x 或更低版本的 XenApp 场或者 XenDesktop 5.6 或更低版本的站点，还请查看 7.x 中的更改一文。

此图显示了典型的 XenApp 或 XenDesktop 部署（称为站点）中的主要组件。



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

Delivery Controller

Delivery Controller 是 XenApp 或 XenDesktop 站点的中心管理组件。每个站点有一个或多个 Delivery Controller。至少安装在数据中心内的一个服务器上。为实现站点可靠性和可用性，Controller 应安装在多个服务器上。如果您的部署中包含在虚拟机管理程序或云服务上托管的虚拟机，Controller 服务将与虚拟机管理程序进行通信，以分发应用程序和桌面、对用户进行身份验证并管理用户访问、代理用户与其虚拟桌面和应用程序之间的连接、优化使用连接并对这些连接进行负载平衡。

Controller 的 Broker Service 跟踪登录的用户和登录位置、用户拥有的会话资源以及用户是否需要重新连接到现有应用程序。Broker Service 执行 PowerShell cmdlet 并通过 TCP 端口 80 与 VDA 上的 Broker Agent 通信。它不可以使用 TCP 端口 443。

Monitor Service 收集历史数据并将其放置在监视数据库中。此服务使用 TCP 端口 80 或 443。

来自 Controller 服务的数据存储在站点数据库中。

Controller 管理桌面的状态，根据需要和管理配置启动和停止桌面。在某些版本中，Controller 允许您安装 Profile Management 以在虚拟化或物理 Windows 环境中管理用户个性化设置。

数据库

每个 XenApp 或 XenDesktop 站点至少需要一个 Microsoft SQL Server 数据库，用于存储配置和会话信息。此数据库存储组成 Controller 的服务所收集并管理的数据。在数据中心内安装此数据库，并确保此数据库与 Controller 建立持续型连接。站点还使用一个配置日志记录数据库和一个监视数据库。默认情况下，这些数据库与站点数据库安装在相同位置，但您可以更改它。

Virtual Delivery Agent (VDA)

VDA 安装在您将其提供给用户的站点中的每个物理机或虚拟机上；那些计算机可以交付应用程序或桌面。VDA 使计算机能够向 Controller 注册，Controller 进而允许向用户提供它所托管的计算机和资源。VDA 建立并管理计算机与用户设备之间的连接，确认 Citrix 许可证可供用户或会话使用，并应用已为会话配置的任何策略。

VDA 通过 VDA 中包含的 Broker Agent 将会话信息传递给 Controller 中的 Broker Service。托管多个插件并收集实时数据的 Broker 代理。它通过 TCP 端口 80 与 Controller 通信。

“VDA”一词通常用于指代理以及安装了它的计算机。

VDA 适用于 Windows 服务器和桌面操作系统。适用于 Windows 服务器操作系统的 VDA 允许多个用户同时连接到服务器。适用于 Windows 桌面操作系统的 VDA 每次仅允许一个用户连接到桌面。Linux VDA 也可用。

Citrix StoreFront

StoreFront 可对托管资源的站点的用户进行身份验证，并可管理用户访问的桌面和应用程序的存储。它可以托管企业应用商店，使用户可以自助访问您为其提供的桌面和应用程序。它还跟踪用户的应用程序订阅、快捷方式名称和其他数据，以确保用户在多个设备之间具有一致的体验。

Citrix Receiver

安装在用户设备和其他端点（如虚拟桌面）上，Citrix Receiver 可使用户能够快速安全地从任何用户设备（包括智能手机、平板电脑和 PC）自助访问文档、应用程序和桌面。通过 Citrix Receiver 可以对 Windows、Web 和软件即服务 (SaaS) 应用程序进行按需访问。对于无法安装 Citrix Receiver 软件的设备，Citrix Receiver for HTML5 通过与 HTML5 兼容的

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

Web 浏览器提供了一个连接。

Citrix Studio

Studio 是可用于配置和管理 XenApp 和 XenDesktop 部署的管理控制台，使用此控制台则不需要为管理应用程序和桌面的交付而配置单独的管理控制台。Studio 提供多种向导来引导您完成设置环境、创建用于托管应用程序和桌面的工作负载并将应用程序和桌面分配给用户的过程。还可以使用 Studio 为站点分配和跟踪 Citrix 许可证。

Studio 从 Controller 中的 Broker Service 获取所显示的信息，它通过 TCP 端口 80 通信。

Citrix Director

Director 是一款基于 Web 的工具，IT 支持团队和技术支持团队可以利用该工具监控环境和对问题进行故障排除，以避免这些问题危及系统，并可以为最终用户执行支持任务。可以使用一个 Director 部署连接和监视多个 XenApp 或 XenDesktop 站点。

Director 显示：

来自 Controller 中的 Broker Service 的实时会话数据，其中包括 Broker Service 从 VDA 中的 Broker Agent 获取的数据。

来自 Controller 中的 Monitor Service 的历史站点数据。

HDX Insight 从 NetScaler 捕获的有关 HDX 通信（也称为 ICA 通信）的数据，前提是部署中包含 NetScaler，并且 XenApp 或 XenDesktop 版本包含 HDX Insight。

还可以使用 Windows 远程协助通过 Director 查看用户会话并与之交互。

Citrix 许可证服务器

许可证服务器管理您的 Citrix 产品许可证。它与 Controller 通信以管理每个用户会话的许可，与 Studio 通信以分配许可证文件。必须至少创建一个许可证服务器来存储和管理许可证文件。

虚拟机管理程序或云服务

虚拟机管理程序或云服务托管站点中的虚拟机。这些虚拟机可以是用于托管应用程序和桌面的 VM，也可以是用于托管 XenApp 和 XenDesktop 组件的 VM。虚拟机管理程序安装在完全专用于运行虚拟机管理程序和托管虚拟机的主机计算机上。

XenApp 和 XenDesktop 支持多种虚拟机管理程序和云服务。

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

尽管许多 XenApp 和 XenDesktop 部署需要一个虚拟机管理程序，但您不需要使用虚拟机管理程序来提供 Remote PC Access，或者在使用 Provisioning Services（某些 XenApp 和 XenDesktop 版本附带）而非 Machine Creation Services (MCS) 来置备 VM 时不需要使用虚拟机管理程序。

详细信息：

- 端口，请参阅网络端口。
- 数据库，，请参阅数据库。
- XenApp 和 XenDesktop 组件中的 Windows 服务，请参阅配置用户权限。
- 支持的虚拟机管理程序和云服务，请参阅系统要求。

其他组件

以下其他组件（未显示在上面的图中）也可以包含在 XenApp 或 XenDesktop 部署中。有关详细信息，请参阅其文档。

Provisioning Services (PVS)

PVS 是 XenApp 和 XenDesktop 的可选组件，在有些版本中提供。它是 MCS 的备选方式，用于置备虚拟机。MCS 创建主映像的副本，PVS 采用流技术将主映像推送到用户设备。PVS 执行此操作时无需使用虚拟机管理程序，因此，您可以使用它来托管物理机。站点中包含 PVS 时，PVS 与 Controller 通信以向用户提供资源。

NetScaler Gateway

用户从公司防火墙外部连接时，XenApp 和 XenDesktop 可以使用 Citrix NetScaler Gateway（以前称为 Access Gateway）技术保护与 TLS 连接时的安全性。NetScaler Gateway 或 NetScaler VPX 虚拟设备是在隔离区域 (DMZ) 中部署的 SSL VPN 设备，用于通过公司防火墙提供单个安全访问点。

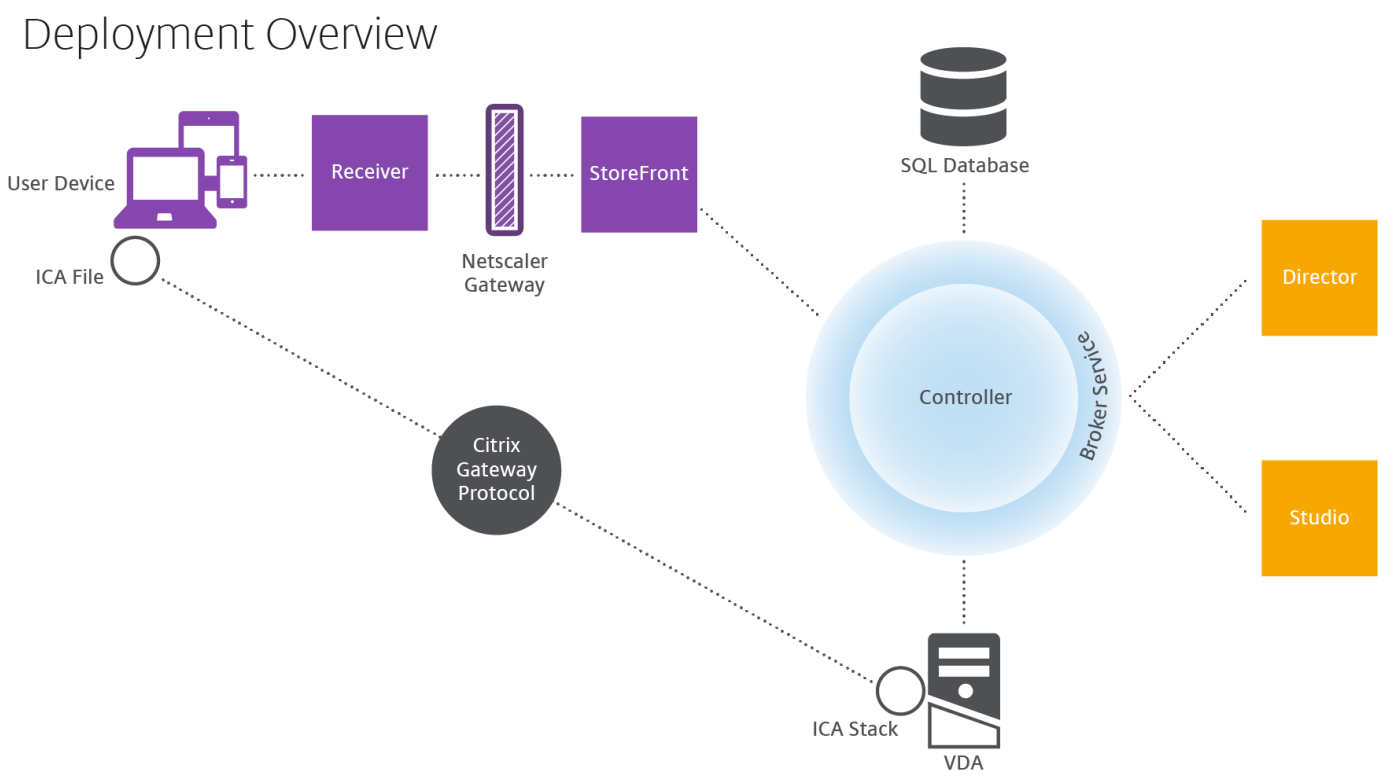
NetScaler SD-WAN

在向位于远程位置（如分支机构）的用户交付虚拟桌面的部署中，可以采用 Citrix NetScaler SD-WAN（以前称为 Citrix CloudBridge、Branch Repeater 或 WANScaler）技术来优化性能。Repeater 可提高整个广域网的性能，因此通过在网络中使用 Repeater，分支机构的用户将在 WAN 上体验到像 LAN 一般的性能。例如，NetScaler SD-WAN 可以设置用户体验不同部分的优先级，以便实现特定目的，例如，通过网络发送大型文件或打印作业时，位于分支机构的用户体验不会降低。HDX WAN 优化提供令牌索引化压缩和重复数据删除功能，极大地降低了带宽要求并改进了性能。

典型部署的工作原理

XenApp 和 XenDesktop 站点由具有专用角色的计算机组成，用于实现可扩展性、高可用性和故障转移，并提供采用安全设计的解决方案。XenApp 或 XenDesktop 站点包括安装 VDA 的服务器和桌面计算机，以及用于管理访问权限的 Delivery Controller。

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



VDA 使用户能够连接到桌面和应用程序。它安装在数据中心内的服务器或桌面计算机上以实现大多数交付方法，但是也可以安装在物理 PC 上以用于 Remote PC Access。

Controller 由独立的 Windows 服务组成，用于管理资源、应用程序和桌面，并优化和平衡用户连接。每个站点具有一个或多个 Controller，并且，由于会话依赖延迟、带宽和网络可靠性，在理想状态下，所有 Controller 应该位于相同 LAN 上。

用户绝对不能直接访问 Controller。VDA 充当用户和 Controller 之间的媒介。当用户使用 StoreFront 登录到站点时，其凭据被传递到 Controller 上的 Broker Service，Broker Service 根据为用户设置的策略获取其配置文件和可用资源。

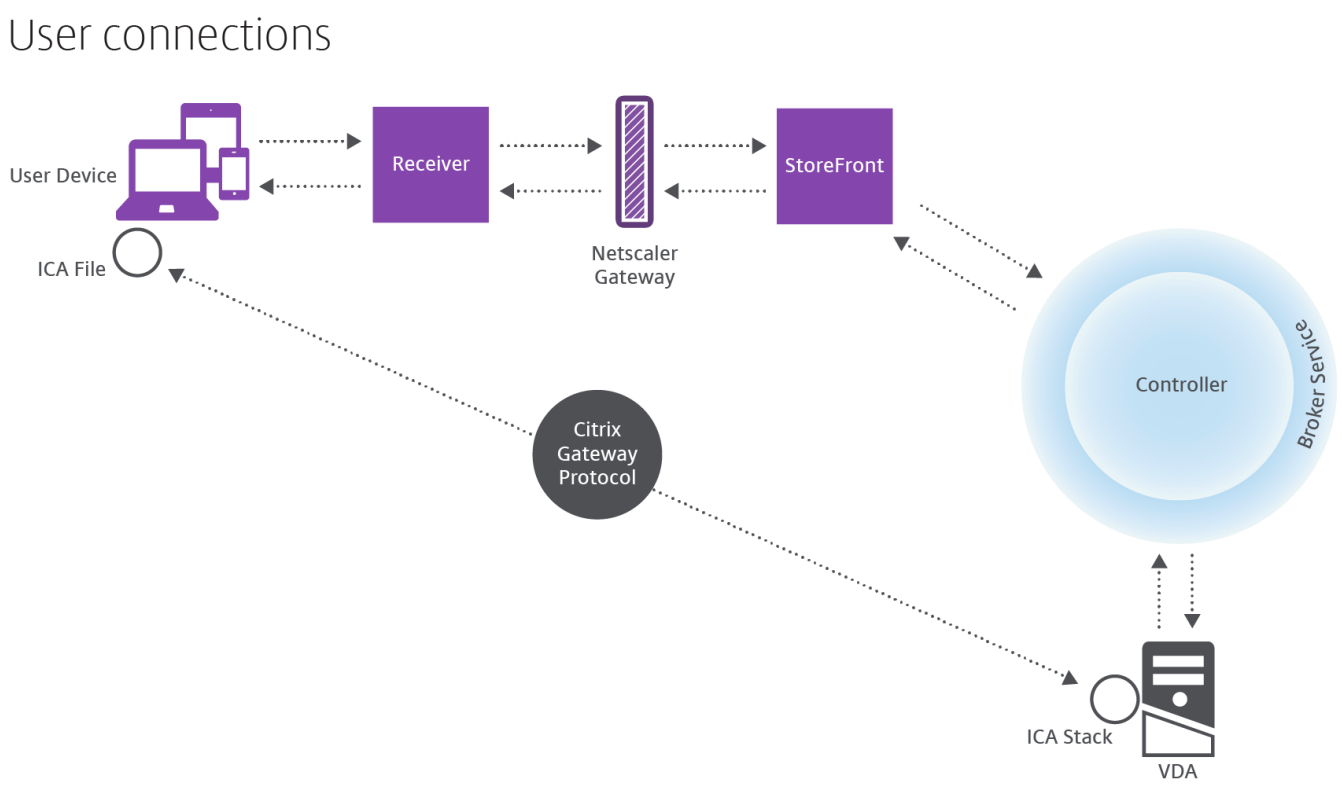
用户连接的处理方式

要启动 XenApp 或 XenDesktop 会话，用户通过 Citrix Receiver（安装在用户设备上）或 StoreFront Citrix Receiver for Web 站点进行连接。

用户选择所需的物理桌面、虚拟桌面或虚拟应用程序。

用户的凭据按照此路径进行传递以访问 Controller，Controller 通过与 Broker Service 通信确定所需的资源。Citrix 建议管理员在 StoreFront 上放置一个 SSL 证书以加密来自 Citrix Receiver 的凭据。

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



Broker Service 决定允许用户访问的桌面和应用程序。

验证凭据后，有关可用应用程序或桌面的信息通过 StoreFront-Citrix Receiver 路径发送给用户。用户选择此列表中的应用程序或桌面时，该信息按照相反路径返回到 Controller，Controller 决定托管特定应用程序或桌面的 VDA。

Controller 将用户的凭据通过消息发送给 VDA，然后将关于用户和连接的所有数据发送给 VDA。VDA 接受连接，并将该信息按相同路径返回给 Citrix Receiver。在 StoreFront 上收集一组必需参数。这些参数随后被发送到 Citrix Receiver，作为 Receiver-StoreFront 协议对话的一部分，或者转换为 Independent Computing Architecture (ICA) 文件并下载。只要站点经过正确设置，凭据在整个流程均保留加密状态。

ICA 文件被复制到用户设备上，并在设备与 VDA 上运行的 ICA 堆栈之间建立直接连接。此连接绕过管理基础结构（Citrix Receiver、StoreFront 和 Controller）。

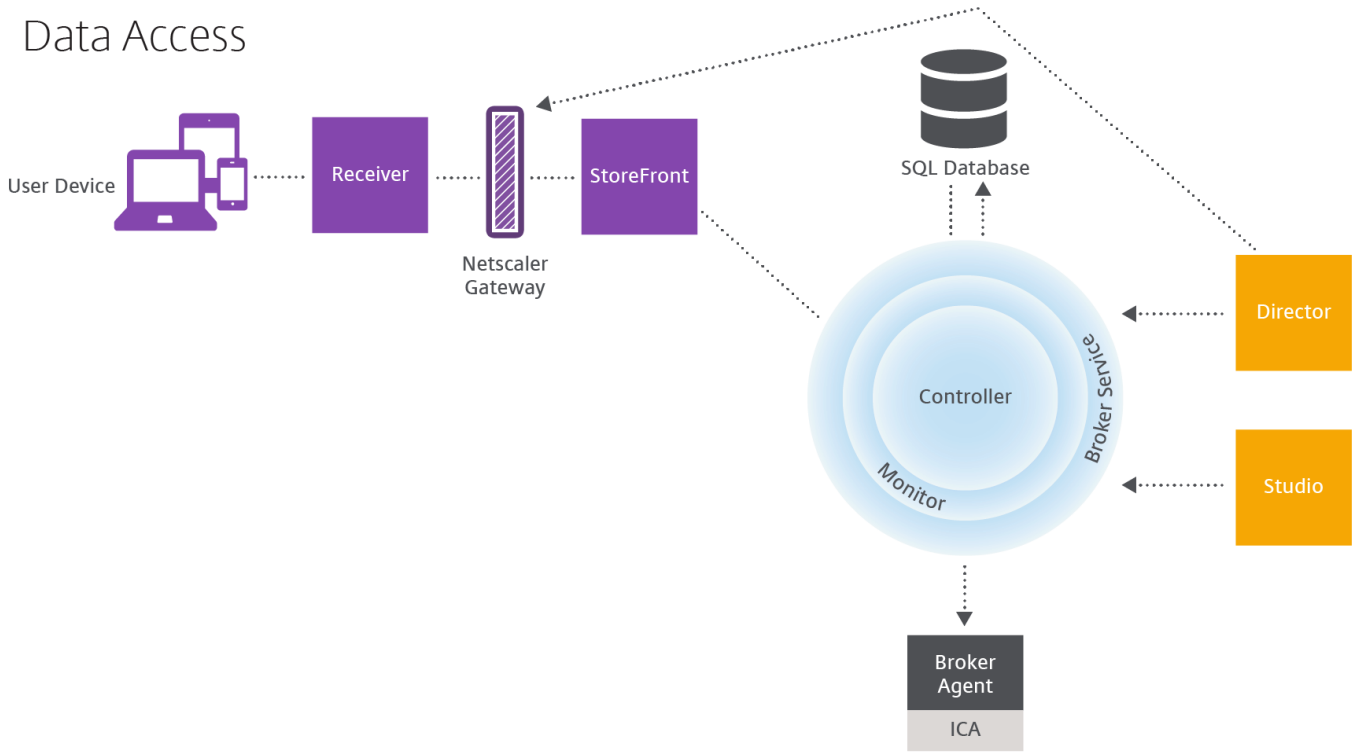
Citrix Receiver 和 VDA 之间的连接使用 Citrix Gateway Protocol (CGP)。如果连接丢失，通过会话可靠性功能，用户可以重新连接到 VDA，而无需通过管理基础结构重新启动。可以在 Citrix 策略中启用或禁用会话可靠性。

客户端连接到 VDA 后，VDA 会通知 Controller 用户已登录，Controller 将此信息发送到站点数据库，并开始在监视数据库中记录数据。

数据访问的工作方式

IT 可以通过 Studio 或 Director 访问每个 XenApp 或 XenDesktop 会话生成的数据。通过使用 Studio，管理员可以访问 Broker Agent 中的实时数据，以便更好地管理站点。Director 可以访问相同的实时数据、存储在监视数据库中的历史数据以及 NetScaler Gateway 中的 HDX 数据，用于提供技术支持和故障排除。

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



在 Controller 内部，Broker Service 报告计算机上的每个会话的会话数据，以提供实时数据。监视服务还跟踪实时数据并将其作为历史数据存储在监视数据库中。

Studio 只与 Broker Service 通信，因此也只访问实时数据。Director 可以与 Broker Service 通信（通过 Broker Agent 中的插件）以访问站点数据库。

Director 还可以访问 NetScaler Gateway 以获取 HDX 数据信息。

交付桌面和应用程序：计算机目录、交付组和应用程序组

为计算机目录设置将交付应用程序和桌面的计算机。然后，创建交付组，交付组指定将提供的应用程序和桌面（使用目录中一些或所有计算机）以及哪些用户可以访问它们。

计算机目录

计算机目录是作为单个实体进行管理的虚拟机或物理机集合。这些计算机及其中的应用程序或虚拟桌面是要提供给用户的资源。目录中的所有计算机安装相同的操作系统和相同的 VDA，并且，这些计算机上具有相同的应用程序或虚拟桌面。

通常，您创建一个主映像，然后使用此主映像在目录中创建完全相同的 VM。对于 VM，您可以为该目录中的计算机指定置备方法：Citrix 工具（PVS 或 MCS）或其他工具。也可以使用您自己的现有映像。在这种情况下，必须单独或统一使用第三方电子软件分发 (ESD) 工具管理目标设备。

有效的计算机类型包括：

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

- **服务器操作系统计算机**：基于服务器操作系统的虚拟机或物理计算机，用于交付 XenApp 发布的应用程序（也称为基于服务器的托管应用程序）和 XenApp 发布的桌面（也称为服务器托管的桌面）。这些计算机允许多个用户同时与其建立连接。
- **桌面操作系统计算机**：基于桌面操作系统的虚拟机或物理计算机，用于交付 VDI 桌面（运行桌面操作系统并且可以完全进行个性化设置的桌面，具体取决于您选择的选项）、VM 托管应用程序（来自桌面操作系统的应用程序）和托管的物理桌面。同一时间仅允许一个用户与其中的一台计算机建立连接。
- **Remote PC Access**：支持远程用户从任何运行 Citrix Receiver 的设备访问他们的办公室物理 PC。办公 PC 通过 XenDesktop 部署进行管理，同时要求在白名单中明确指定用户设备。

有关详细信息，请参阅创建计算机目录一文。

交付组

交付组指定哪些用户可以访问哪些计算机上的哪些应用程序和/或桌面。交付组包含计算机目录中的计算机和具有站点访问权限的 Active Directory 用户。由于 Active Directory 组和交付组均是将具有相似要求的用户分成一组，因此，通常可以按照用户所属的 Active Directory 组将其分配到交付组。

每个交付组可以包含多个计算机目录中的计算机，每个目录可以向多个交付组提供计算机，但是每个单独的计算机在同一时间只能属于一个交付组。

可以定义交付组中的用户可以访问的资源。例如，如果要向不同的用户交付不同的应用程序，一种方式是在一个计算机目录的主映像上安装要交付的所有应用程序，并在此目录中创建足够多的计算机以在多个交付组之间分发。然后，配置各个交付组，以交付计算机上安装的不同应用程序子集。

有关详细信息，请参阅创建交付组一文。

应用程序组

与使用多个交付组相比，应用程序组提供应用程序管理和资源控制优势：通过使用标记限制功能，可以使用现有计算机来完成多个发布任务，从而节省与部署和管理其他计算机有关的成本。标记限制可以视为对交付组中的计算机进行划分（或分区）。对交付组中的一部分计算机进行隔离和故障排除时，应用程序组也很有用。

有关详细信息，请参阅创建应用程序组一文。

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

Active Directory

Dec 05, 2017

进行身份验证和授权时需要使用 Active Directory。Active Directory 中的 Kerberos 基础结构用于保证与 Delivery Controller 通信的真实性和保密性。有关 Kerberos 的详细信息，请参阅 Microsoft 文档。

系统要求一文列出了支持的林和域功能级别。要使用策略建模，域控制器必须在 Windows Server 2003 到 Windows Server 2012 R2 上运行；这不会影响域功能级别。

本产品支持：

- 具有以下特征的部署：用户帐户和计算机帐户所在的域位于同一 Active Directory 林中。用户和计算机帐户可以存在于同一林中的任意域内。所有域功能级别和林功能级别在这种类型的部署中都得到支持。
- 具有以下特征的部署：用户帐户所在的 Active Directory 林不同于控制器和虚拟桌面的计算机帐户所在的 Active Directory 林。在此类部署中，包含控制器和虚拟桌面计算机帐户的域必须信任包含用户帐户的域。可以使用林信任和外部信任。所有域功能级别和林功能级别在这种类型的部署中都得到支持。
- 具有以下特征的部署：在该部署中，控制器的计算机帐户所在的 Active Directory 林不同于虚拟桌面的计算机帐户所在的一个或多个附加 Active Directory 林。在此类部署中，在控制器计算机帐户所在的域与虚拟桌面计算机帐户所在的所有域之间必须存在双向信任关系。在此类部署中，包含控制器或虚拟桌面计算机帐户的所有域都必须处于“Windows 2000 本机”功能级别或更高级别。所有林功能级别都得到支持。
- 可写域控制器。不支持只读域控制器。

或者，Virtual Delivery Agent (VDA) 可以使用在 Active Directory 中发布的信息来确定可以注册的控制器（发现）。支持此方法的目的主要是实现向后兼容，并且此方法仅在 VDA 与控制器位于相同的 Active Directory 林中时可用。有关此发现方法的信息，请参阅 Delivery Controller 一文和 CTX118976。

提示：请勿在配置站点后更改 Controller 的计算机名称或域成员关系。

在多林 Active Directory 环境中部署

注意：此信息适用的最低版本为 XenDesktop 7.1 和 XenApp 7.5，不适用于早期版本的 XenDesktop 或 XenApp。
在具有多个林的 Active Directory 环境中，如果已配置单向或双向信任，则可以使用 DNS 转发器执行名称查找和注册。要允许相应的 Active Directory 用户创建计算机帐户，请使用控制委派向导。有关此向导的详细信息，请参阅 Microsoft 文档。

如果已在两个林之间配置相应的 DNS 转发器，则不需要在 DNS 基础结构中配置反向 DNS 区域。

无论 Active Directory 和 NetBios 名称是否相同，如果 VDA 和 Controller 位于不同的林中，则需要创建 SupportMultipleForest 注册表项。只有 VDA 需要 SupportMultipleForest 注册表项。请使用以下信息添加注册表项：
小心：注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因“注册表编辑器”使用不当导致出现的问题能够得以解决。使用“注册表编辑器”需自担风险。在编辑注册表之前，请务必进行备份。

- HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest
  - 名称：SupportMultipleForest
  - 类型：REG_DWORD
  - 数据：0x00000001 (1)

如果 DNS 命名空间与 Active Directory 的命名空间不同，您可能需要反向 DNS 配置。

如果设置期间已配置外部信任，则需要创建 ListOfSIDs 注册表项。如果 Active Directory FQDN 与 DNS FQDN 不同，或者如果包含域控制器的域具有的 Netbios 名称与 Active Directory FQDN 不同，也需要创建 ListOfSIDs 注册表项。要添加此注册表项，请使用以下信息：

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

- 对于 32 位或 64 位 VDA，请找到注册表项 HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs
  - 名称：ListOfSIDs
  - 类型：REG_SZ
  - 数据：控制器的安全标识符 (SID)

如果具有现有外部信任，应对 VDA 做以下更改：

1. 找到文件 \Citrix\Virtual Desktop Agent\brokeragentconfig.exe.config。
2. 备份该文件。
3. 在文本编辑程序（例如记事本）中打开该文件。
4. 找到文本 allowNtlm="false"，并将其更改为 allowNtlm="true"。
5. 保存该文件。

在添加 ListOfSIDs 注册表项并编辑 brokeragent.exe.config 文件之后，重新启动 Citrix Desktop Service 以应用所做的更改。

下表列出了支持的信任类型：

信任类型	传递性	方向	此版本支持
父与子	可传递	双向	是
树根	可传递	双向	是
外部	不可传递	单向或双向	是
林	可传递	单向或双向	是
快捷方式	可传递	单向或双向	是
领域	可传递或非可传递	单向或双向	否

有关复杂 Active Directory 环境的详细信息，请参阅 CTX134971。

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

数据库

Dec 05, 2017

XenApp 或 XenDesktop 站点使用三个 SQL Server 数据库：

- **站点：**（也称为站点配置）存储正在运行的站点配置，以及当前会话状态和连接信息。
- **配置日志记录：**（也称为日志记录）存储有关站点配置更改和管理活动的信息。启用配置日志记录功能（默认情况下启用）时将使用此数据库。
- **监视：**存储 Director 使用的数据，如会话和连接信息。

每个 Delivery Controller 与站点数据库通信；Controller 与数据库之间需要进行 Windows 身份验证。拔出或关闭一个 Controller 不会对站点中的其他 Controller 产生影响。但这也意味着站点数据库会形成单点故障。如果数据库服务器出现故障，现有连接继续正常运行，直到用户注销或断开连接。有关站点数据库变得不可用时的连接行为的信息，请参阅本地主机缓存。

Citrix 建议您定期备份数据库，以便在数据库服务器出现故障时可以通过备份进行还原。各个数据库的备份策略可以有所不同。相关说明，请参阅 CTX135207。

如果站点包含多个区域，站点数据库应始终位于主要区域内。各区域内的 Controller 与该数据库通信。

高可用性

可以考虑采取几种高可用性解决方案以确保实现自动故障转移：

- **AlwaysOn 可用性组：**这是 SQL Server 2012 中引入的具有高可用性和灾难恢复能力的企业级解决方案，此方案可以使您最大程度地提高一个或多个数据库的可用性。AlwaysOn 可用性组要求 SQL Server 实例必须驻留在 Windows Server 故障转移群集 (WSFC) 节点上。有关详细信息，请参阅 http://msdn.microsoft.com/zh-cn/library/hh510230。
- **SQL Server 数据库镜像：**通过数据库镜像可以确保一旦与活动数据库服务器失去联系，可以在几秒钟内快速实现自动故障转移，因此用户通常不会受到影响。此方法比其他解决方案更为昂贵，因为在每台数据库服务器上必须使用完整的 SQL Server 许可证；在镜像环境中不能使用 SQL Server Express 版本。
- **SQL 群集化：**可以使用 Microsoft 的 SQL 群集化技术，允许一台服务器自动接管另一台故障服务器的任务和职责。但是，该解决方案的设置更为复杂，自动故障转移过程通常比其他备选方案（如 SQL 镜像）更慢。
- **使用虚拟机管理程序的高可用性功能：**通过此方法，可以将数据库作为虚拟机进行部署，并使用虚拟机管理程序的高可用性功能。此解决方案的成本比镜像方法要低，因为它使用的是现有虚拟机管理程序软件，您也可以使用 SQL Server Express 版本。但是，其自动故障转移过程比较慢，因为需要花时间为数据库启动新计算机，这样可能会导致为用户提供的服务中断。

注意：在 SQL 群集或 SQL 镜像安装中，不支持在节点上安装 Controller。

通过本地主机缓存功能，用户可以连接以及重新连接到应用程序和桌面，即使在站点数据库不可用时也能连接，补充了 SQL Server 高可用性最佳做法。有关详细信息，请参阅本地主机缓存一文。

如果站点中的所有 Controller 均出现故障，可以将 VDA 配置为在高可用性模式下运行，这样用户便可以继续访问并使用其桌面和应用程序。在高可用性模式下，VDA 将接受来自用户的直接 ICA 连接，而不是由 Controller 代理的连接。此功能仅在与所有 Controller 的通信都出现故障时使用，这种情况非常罕见；此功能不能代替其他高可用性解决方案。有关详细信息，请参阅 CTX 127564。

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

安装数据库软件

默认情况下，安装首个 Delivery Controller 时，如果在该服务器上未检测到另一个 SQL Server 实例，系统将安装 SQL Server Express 版本。通常情况下，此默认行为可满足概念验证或试验部署的要求；但是 SQL Server Express 不支持 Microsoft 高可用性功能。

默认安装程序使用默认 Windows 服务帐户和权限。请参阅 Microsoft 文档了解关于这些默认设置的详细信息，其中包括如何向 sysadmin 角色添加 Windows 服务帐户。Controller 使用此配置中的网络服务帐户。Controller 不需要使用任何其他 SQL Server 角色或权限。

如果需要，您可以为数据库实例选择**隐藏实例**。在 Studio 中配置数据库的地址时，请输入实例的静态端口号，而不是它的名称。请参阅 Microsoft 文档了解关于隐藏 SQL Server 数据库引擎实例的详细信息。

大多数生产部署以及任何使用 Microsoft 高可用性功能的部署都应该使用受支持的非 Express 版本的 SQL Server，且安装此数据库的计算机应不同于安装首个 Controller 的服务器。“系统要求”一文列出了受支持的 SQL Server 版本。数据库可以位于一台或多台计算机上。

请务必在创建站点之前安装 SQL Server 软件。无须创建数据库，但是，如果确实已创建数据库，此数据库必须为空。同时，建议配置 Microsoft 高可用性技术。

使用 Windows 更新保持 SQL Server 处于最新状态。

通过站点创建向导设置数据库

在站点创建向导中的**数据库**页面指定数据库名称和地址（位置）；请参阅下面的*数据库地址格式*。为避免 Director 查询 Monitor Service 时存在潜在错误，请勿在监视数据库的名称中使用空格。

数据库页面提供两个用于设置数据库的选项：自动或使用脚本。通常，如果您（Studio 用户和 Citrix 管理员）拥有所需的数据库权限，可以使用自动选项；请参阅下面的“设置数据所需的权限”部分。

可以在创建站点之后更改数据库的位置；请参阅下面的*更改数据库位置*。

要将站点配置为使用镜像数据库，请完成以下操作，然后继续执行自动设置过程或脚本设置过程。

1. 在两个服务器（A 和 B）上安装 SQL Server 软件。
2. 在服务器 A 上，创建要作为主体数据库的数据库。在服务器 A 上备份此数据库，然后将其复制到服务器 B。
3. 在服务器 B 上，还原备份文件。
4. 在服务器 A 上启动镜像。

提示：要在创建站点后验证镜像，请运行 PowerShell cmdlet **get-configdbconnection**，以确保已在连接字符串中将故障转移合作伙伴设置为镜像。

如果以后在镜像的数据库环境中添加、移动或删除 Delivery Controller，请参阅“Delivery Controller”一文。

自动设置

如果拥有所需的数据库权限，请在站点创建向导的**数据库**页面选择“在 Studio 中创建和设置数据库”选项，然后提供主体数据库的名称和地址。

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

如果指定的地址已存在数据库，此数据库必须为空。如果指定的地址没有数据库，系统会提示您未找到数据库，然后询问是否为您创建数据库。确认该操作后，Studio 将自动创建数据库，然后为主体数据库和复制数据库应用初始化脚本。

脚本设置

如果您没有所需的数据库权限，必须在具有这些权限的人员（如数据库管理员）的帮助下进行操作。以下是操作步骤：

1. 在站点创建向导中，选择**生成脚本**选项。此操作将生成六个脚本：三个数据库各具有两个脚本（一个用于对应的主体数据库，另一个用于对应的复制数据库）。可以指定存储这些脚本的位置。
2. 将这些脚本提供给数据库管理员。站点创建向导此时自动停止；稍后您返回继续创建站点时会收到提示。

然后，数据库管理员创建数据库。每个数据库应具有以下特征：

- 使用结尾为"_CI_AS_KS"的排序规则。Citrix 建议使用结尾为"_100_CI_AS_KS"的排序规则。
- 为获得最佳性能，请启用 SQL Server Read-Committed 快照。有关详细信息，请参阅 CTX 137161。
- 如果需要，应配置高可用性功能。
- 要配置镜像，请首先将数据库设置为使用完整恢复模式（默认情况下为简单模式）。将主体数据库备份到某个文件中，然后将其复制到镜像服务器。在镜像数据库上，将备份文件还原到镜像服务器。然后，在主体服务器上启动镜像。

数据库管理员使用 SQLCMD 命令行实用程序或采用 SQLCMD 模式的 SQL Server Management Studio 在高可用性 SQL Server 数据库实例（如果配置了高可用性）上运行每个 xxx_Replica.sql 脚本，然后在主体 SQL Server 数据库实例上运行每个 xxx_Principal.sql 脚本。有关 SQLCMD 的详细信息，请参阅 Microsoft 文档。

所有脚本成功完成后，数据库管理员向 Citrix 管理员提供三个主体数据库地址。

在 Studio 中，系统会提示您继续创建站点，并返回到**数据库**页面。输入地址。如果无法联系托管数据库的任何服务器，系统会显示错误消息。

设置数据库所需的权限

您必须是本地管理员或域用户才能创建和初始化数据库（或更改数据库位置）。您还必须具有某些 SQL Server 权限。以下权限可以显式配置或通过 Active Directory 组成员身份获取。如果您的 Studio 用户凭据不包括这些权限，系统会提示您使用 SQL Server 用户凭据。

操作	用途	服务器角色	数据库角色
创建数据库	创建合适的空数据库	dbcreator	
创建架构	创建所有服务特定的架构，并将第一个 Controller 添加到站点	securityadmin *	db_owner
添加 Controller	将 Controller（除第一个外）添加到站点	securityadmin *	db_owner
添加 Controller（镜像服务器）	将 Controller 登录信息添加到当前位于镜像数据库的镜像角色中的数据库服务器	securityadmin *	

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

更新架构	应用架构更新或修补程序		db_owner

* 虽然在技术层面上的限制更加严格，但实际上应将 securityadmin 服务器角色视为等同于 sysadmin 服务器角色。

使用 Studio 执行这些操作时，用户帐户必须属于 sysadmin 服务器角色的成员。

数据库地址格式

可以使用以下格式之一指定数据库地址：

- 服务器名称
- 服务器名称\实例名称
- 服务器名称,端口号

对于 AlwaysOn 可用性组，请在位置字段指定组的侦听器。

更改数据库位置

创建站点后，可以更改数据库的位置。更改数据库的位置时：

- 以前数据库中的数据不会导入到新数据库中。
- 检索日志时，不能合并来自两个数据库的日志。
- 新数据库中的第一条日志指示数据库发生更改，但不会标识以前的数据库。

可以在启用强制日志记录功能时更改配置日志记录数据库的位置。

要更改数据库的位置，请执行以下操作：

1. 确保您希望数据库所在的服务器上已安装受支持版本的 Microsoft SQL Server。根据需要设置高可用性功能。
2. 在 Studio 导航窗格中选择**配置**。
3. 选择要指定新位置的数据库，然后在“操作”窗格中选择**更改数据库**。
4. 指定新位置和数据库名称。
5. 如果希望 Studio 创建数据库，并且您具有相应的权限，请单击**确定**。出现提示时，请单击**确定**，然后 Studio 会自动创建数据库。Studio 会尝试使用您的凭据访问数据库；如果此操作失败，系统会提示您输入数据库用户的凭据。然后，Studio 会将数据库架构上载到数据库。凭据仅在数据库创建期间保留。
6. 如果不希望 Studio 创建数据库，或者您没有足够的权限，请单击**生成脚本**。生成的脚本中包括用于手动创建数据库和镜像数据库（如果需要）的指令。上载架构前，请确保数据库为空，且至少有一个用户有权访问和更改该数据库。

相关详细信息

高级概念部分中的文章包含 Citrix 团队提供的最具技术性深度的文章。例如：

- “设计集合”包含与数据库大小调整工具有关的文章。
- “实施和配置集合”包含使用 SQL Server 高可用性解决方案时调整站点数据库大小和配置连接字符串的指南。

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

交付方法

Dec 05, 2017

采用一种虚拟化部署满足每个用户的需要面临很多挑战。XenApp 和 XenDesktop 允许管理员采用各种方法（有时称为 FlexCast 模式）定制用户体验。

此 交付方法集合（其中的交付方法分别有其各自的优势和劣势）可在任何用例场景下提供 最佳用户体验。

使 Windows 应用程序具有能够在移动设备上使用的移动性

现在，触摸屏设备（如平板电脑和智能手机）在移动性方面已标准化。 这些设备在运行通常需要采用全屏并且需要依靠单击鼠标右键输入才能实现全部功能的基于 Windows 的应用程序时会出现问题。

采用 Citrix Receiver 的 XenApp 提供了安全的解决方案，允许移动设备用户访问其基于 Windows 的应用程序中的全部功能，无需针对本地移动平台重写这些应用程序。

XenApp 发布的应用程序交付方法利用 HDX 移动技术解决了与使 Windows 应用程序具有移动性相关的问题。 此方法允许重构 Windows 应用程序以实现触摸体验，同时维护多点触控手势、本机菜单控件、摄像头和 GPS 功能等诸多功能。 多种触控功能本身可在 XenApp 和 XenDesktop 中使用，无需更改任何应用程序源代码即可激活。

这些功能包括：

- 可编辑的字段获得焦点后自动显示键盘
- 更大的选取控件取代了 Windows 组合框控件
- 多点触控手势，如收缩和放大
- 可感知惯性的滚动功能
- 触控板或直接光标导航

降低 PC 刷新成本

升级物理计算机是一项艰巨的任务，很多企业每三到五年就要升级一次，尤其是当企业需要维护最新的操作系统和应用程序时。 不断成长的企业还面临着向其网络中添加新计算机所产生的巨大成本开销。

VDI Personal vDisk 交付方法向任何使用服务器资源的计算机或瘦客户端上的单个用户提供完全个性化的桌面操作系统。 管理员可以创建将其资源（如处理能力、内存和存储）存储在网络数据中心内的虚拟机。

这样可以延长旧计算机的使用时间、保持软件处于最新状态以及在升级期间尽可能降低停机时间。

确保承包商与合作伙伴可以安全访问虚拟应用程序和桌面

网络安全问题日益严重，在与需要访问公司应用程序和数据的承包商、合作伙伴和其他第三方临时工作人员合作时此情况尤为突出。工作人员可能还需要租用便携式计算机或其他设备，这可能会带来额外的成本忧虑。

数据、应用程序和桌面存储在采用 XenDesktop 和 XenApp 的安全网络的防火墙后面，这样一来，最终用户过渡时只需考虑用户设备输入和输出，例如按键、鼠标点击、音频和屏幕更新。通过在数据中心内维护这些资源，XenDesktop 和 XenApp 提供了比使用典型 SSL VPN 更加安全的远程访问解决方案。

通过具有个人虚拟磁盘的 VDI 部署，管理员可以在网络服务器上创建虚拟机并提供单用户桌面操作系统，从而利用瘦客户端或用户的个人设备。这使得 IT 部门无需购买昂贵的设备，即可维护与第三方工作人员合作时的安全性。

加速迁移

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

切换到新操作系统时，IT 可能会面临交付旧版不兼容应用程序的挑战。

利用虚拟机托管应用程序，用户可以通过 Citrix Receiver 在升级后的虚拟机上运行旧的应用程序，并且不会出现任何兼容性问题。 这样一来，IT 无需花费额外的时间来解决和测试应用程序兼容性问题，便于用户过渡，并使技术支持呼叫更加有效。

迁移期间使用 XenDesktop 的其他优势包括：

- 降低桌面复杂度
- 改善 IT 控制
- 在设备使用和工作区位置方面增强最终用户的灵活性

通过虚拟化专业的 3-D 图形应用程序支持设计师和工程师

许多设计公司和制造公司严重依赖专业的 3-D 图形应用程序。 要支持此类型的软件需要功能强大的硬件，由此产生的成本以及通过 FTP、电子邮件和类似的专门方法共享大型设计所带来的传输问题使得这些公司面临着财务压力。

XenDesktop 的托管物理桌面交付方法提供工作站和刀片式服务器的单个桌面映像，无需使用虚拟机管理程序在本地操作系统上运行图像密集型 3-D 应用程序。

所有文件保存在网络中的中央数据中心内，因此，在网络中向其他用户共享大型设计文件更快，更安全，因为无需再将文件从一个工作站传输到另一个工作站。

转换呼叫中心

维护足够的员工以应对高峰期，同时又不会在不忙时过度置备计算机，这种需求为需要大规模呼叫中心的企业带来了严峻挑战。

池 VDI 交付方法可在置备大量用户的情况下，以最低成本动态地向多个用户提供对标准化桌面的访问权限。 池计算机按照每个会话以先到先服务的原则进行分配。

由于在用户注销时会丢弃在会话期间执行的所有更改，因此，基本上无需每日对这些虚拟机进行管理。 这同样也增强了安全性。

XenApp 托管桌面交付方法是另一种转换呼叫中心的可行选项。 此方法在单个基于服务器的操作系统上托管多个用户桌面。

此方法比池 VDI 更具成本效益，但是使用 XenApp 托管桌面时，会限制用户安装应用程序、更改系统设置和重新启动服务器。

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

XenApp 发布的应用程序和桌面

Mar 21, 2018

使用服务器操作系统计算机交付 XenApp 发布的应用程序和发布的桌面。

用例

- 您希望使用基于服务器的经济实惠的交付，以便最大程度地减少向大量用户交付应用程序的成本，同时提供安全的高清晰度用户体验。
- 您的用户执行定义明确的任务且不需要个性化设置或应用程序脱机访问权限。用户可能包括任务型工作人员（如呼叫中心操作人员和零售工作人员）或共享工作站的用户。
- 应用程序类型：任何应用程序。

优势和注意事项

- 数据中心内可管理、可扩展的解决方案。
- 最经济的应用程序交付解决方案。
- 托管应用程序集中进行管理且用户无法修改应用程序，从而提供一致、安全、可靠的用户体验。
- 用户必须联机才能访问其应用程序。

用户体验

- 用户可通过 StoreFront、“开始”菜单或您为其提供的 URL 请求一个或多个应用程序。
- 应用程序以虚拟方式进行交付并在用户设备上高清晰度无缝显示。
- 根据配置文件设置，用户所做的更改会在用户的应用程序会话结束时进行保存。否则，这些更改将被删除。

处理、托管和交付应用程序

- 应用程序处理在托管计算机（而非用户设备）上执行。托管计算机可以是物理机，也可以是虚拟机。
- 应用程序和桌面驻留在服务器操作系统计算机上。
- 计算机通过计算机目录提供。
- 计算机目录中的计算机组织成可将相同的应用程序集交付给用户组的交付组。
- 服务器操作系统计算机支持托管桌面或应用程序或二者的交付组。

会话管理和分配

- 服务器操作系统计算机可从单台计算机运行多个会话，以便将多个应用程序和桌面交付给多个同时连接的用户。每个用户均需要可从中运行其所有托管应用程序的单个会话。

  例如，一个用户登录并请求某个应用程序。该计算机上的一个会话变为对其他用户不可用。另一个用户登录并请求该计算机托管的应用程序。同一台计算机上的另一个会话现在不可用。如果两个用户同时请求其他应用程序，则不需要任何其他会话，因为用户可以使用同一个会话运行多个应用程序。如果有另外两个用户登录并请求桌面且同一台计算机上存在两个可用会话，该计算机现在将使用四个会话托管四个不同的用户。

- 在分配有用户的交付组内，将选择负载最低的服务器上的计算机。具有可用会话的计算机将随机分配，用以在用户登录时向用户交付应用程序。

要交付 XenApp 发布的应用程序和桌面，请执行以下操作：

1. 在运行受支持的 Windows 服务器操作系统的主映像上安装要交付的应用程序。

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

2. 创建此主映像的计算机目录或使用主映像更新现有目录。
3. 创建交付组以向用户交付应用程序和桌面。如果要交付应用程序，请选择要交付的应用程序。

有关详细信息，请参阅安装和配置文章。

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

VM 托管应用程序

Dec 05, 2017

使用桌面操作系统计算机交付 VM 托管应用程序

用例

- 您希望使用基于客户端的安全应用程序交付解决方案，提供集中管理功能，并支持每台主机服务器（或虚拟机管理程序）具有大量用户，同时为用户提供以高清晰度无缝显示的应用程序。
- 您的用户是内外部承包商、第三方合作者及其他临时团队成员。您的用户不需要脱机访问托管应用程序。
- 应用程序类型：可能不会与其他应用程序完美配合使用或可能与操作系统进行交互的应用程序，例如 Microsoft .NET Framework。这些类型的应用程序最适合在虚拟机上进行托管。

优势和注意事项

- 可在数据中心内的计算机上安全管理、托管和运行主映像上的应用程序和桌面，从而提供一个更为经济的应用程序交付解决方案。
- 登录后，可以将用户随机分配给交付组内配置为托管相同应用程序的计算机。还可以静态分配单台计算机，以便在每次有单个用户登录时将应用程序交付给该用户。通过静态分配的计算机，用户可以在虚拟机上安装和管理自己的应用程序。
- 桌面操作系统计算机上不支持运行多个会话。因此，登录后，每个用户都将占用交付组内的单台计算机，且这些用户必须联机才能访问其应用程序。
- 此方法可能会增加用于处理应用程序的服务器资源量，同时增加用户的个人虚拟磁盘的存储量。

用户体验

与在服务器操作系统计算机上托管共享应用程序相同的无缝应用程序体验。

处理、托管和交付应用程序

与服务器操作系统计算机相同，但这些计算机属于虚拟桌面操作系统计算机。

会话管理和分配

- 桌面操作系统计算机可从单台计算机运行单个桌面会话。仅当访问应用程序时，单个用户才能使用多个应用程序（不限于单个应用程序），因为操作系统将每个应用程序视为一个新会话。
- 在交付组中，当用户登录时，可以访问静态分配的计算机（每次用户登录到相同的计算机时）或随机分配的计算机（根据会话可用性进行选择）。

要交付 VM 托管应用程序，请执行以下操作：

1. 在运行受支持的 Windows 桌面操作系统的主映像上安装要交付的应用程序。
2. 创建此主映像的计算机目录或使用主映像更新现有目录。
3. 定义计算机目录的桌面体验时，确定用户每次登录时是连接到新 VM 还是连接到相同的 VM。
4. 创建交付组以向用户交付应用程序。
5. 从安装的应用程序列表中，选择要交付的应用程序。

有关详细信息，请参阅安装和配置文章。

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

VDI 桌面

Dec 05, 2017

使用桌面操作系统 计算机交付 VDI 桌面。

VDI 桌面托管在虚拟机上，并向每个用户提供桌面操作系统。

VDI 桌面需要的资源 高于 XenApp 发布的桌面，但是不要求其上安装的 应用程序支持基于服务器的操作系统。此外， 根据您选择的 VDI 桌面类型，可以将这些桌面 分配给单个用户，并允许这些用户进行高度 个性化设置。

创建 VDI 桌面的计算机目录时，创建以下桌面类型之一：

- 随机非永久性桌面，也称为池 VDI 桌面。用户每次登录以使用其中一个桌面时，将连接到从基于单个主映像的桌面池中动态选择的桌面。计算机重新启动时，对桌面所做的更改将全部丢失。
- 静态非永久性桌面。用户首次登录以使用其中一个桌面时，将向此用户分配基于单个主映像的桌面池中的桌面。第一次使用后，用户每次登录以使用其中的桌面时，将连接到此用户第一次使用时向其分配的桌面。计算机重新启动时，对桌面所做的更改将全部丢失。
- 静态永久性桌面，也称为使用个人虚拟磁盘的 VDI。与其他 VDI 桌面类型不同，用户完全可以对这些桌面进行个性化设置。用户首次登录以使用其中一个桌面时，将向此用户分配基于单个主映像的桌面池中的桌面。该用户的后续登录会连接到首次使用时分配的相同桌面。计算机重新启动时，会保留对桌面所做的更改，因为这些更改存储在个人虚拟磁盘中。

要交付 VDI 桌面，请执行以下操作：

1. 创建运行受支持的 Windows 桌面操作系统的主映像。
2. 创建此主映像的计算机目录或使用主映像更新现有目录。定义计算机目录的桌面体验时，确定用户每次登录时是连接到新 VM 还是连接到相同的 VM。如果用户连接到相同的计算机，您可以指定如何保留对桌面所做的更改。
3. 创建交付组以向用户交付桌面。

有关详细信息，请参阅安装和配置文章。

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

网络端口

Mar 21, 2018

下表列出了 XenApp 和 XenDesktop Delivery Controller、Windows VDA、Director 和 Citrix 许可证服务器使用的默认网络端口。默认情况下，安装 Citrix 组件时，还会更新操作系统的主机防火墙，以与这些默认网络端口相匹配。

有关其他 Citrix 技术和组件中使用的通信端口的概览，请参阅 CTX101810。

在以下情况下您可能需要此端口信息：

- 满足法律合规性要求。
- 如果这些组件与其他 Citrix 产品或组件之间存在网络防火墙，则可以相应地配置该防火墙。
- 如果使用第三方主机防火墙（例如，反恶意软件安装包附带的防火墙），而非操作系统的主机防火墙。
- 如果更改这些组件上的主机防火墙配置（通常为 Windows 防火墙服务）。
- 如果将这些组件的任何功能重新配置为使用不同的端口或端口范围，然后希望禁用或阻止您的配置中未使用的端口。有关详细信息，请参阅组件的相关文档。

有关其他组件（例如 StoreFront 和 Provisioning Services）的端口信息，请参阅组件的最新“系统要求”一文。

下表仅列出了传入端口；传出端口通常由操作系统决定，并且使用不相关的编号。实现上述目的通常不需要传出端口信息。

其中某些端口已在 Internet 编号分配机构 (Internet Assigned Numbers Authority, IANA) 注册。http://www.iana.org/assignments/port-numbers 提供了有关这些分配的详细信息；但是，IANA 拥有的描述性信息并不总是反映现今的使用情况。

此外，VDA 和 Delivery Controller 上的操作系统需要传入端口以供自己使用。有关详细信息，请参阅 Microsoft Windows 文档。

组件	使用情况	协议	默认传入端口	注意
VDA	ICA/HDX	TCP、UDP	1494	EDT 协议要求为 UDP 开放 1494。 请参阅 ICA 策略设置。
VDA	ICA/HDX（启用了会话可靠性）	TCP、UDP	2598	EDT 协议要求为 UDP 开放 2598。 请参阅 ICA 策略设置。
VDA	ICA/HDX（通过 TLS）	TCP	443	所有 Citrix Receiver
VDA	ICA/HDX（通过 WebSocket）	TCP	8008	仅限 Citrix Receiver for HTML5、Citrix Receiver for Chrome 1.6 及更早版本
VDA	ICA/HDX 通过 UDP 实时传输	UDP	16500-16509	

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

	音频			
VDA	ICA/HDX Framehawk	UDP	3224-3324	
VDA	ICA/通用打印服务器	TCP	7229	由通用打印服务器打印数据流 CGP（通用网关协议）侦听器使用。
VDA	ICA/通用打印服务器	TCP	8080	由通用打印服务器侦听器使用，用于侦听传入的 HTTP/SOAP 请求。
VDA	局域网唤醒	UDP	9	Remote PC Access 电源管理
VDA	唤醒代理	TCP	135	Remote PC Access 电源管理
VDA	Delivery Controller	TCP	80	
Delivery Controller	VDA、StoreFront、Director、Studio	TCP	80	
Delivery Controller	StoreFront、Director、Studio（通过 TLS）	TCP	443	
Delivery Controller	Delivery Controller、VDA	TCP	89	本地主机缓存（在将来的版本中可能不再使用端口 89）。
Delivery Controller	调配	TCP	9095	调配
Director	Delivery Controller	TCP	80、443	

对于 Citrix Licensing：

组件	**使用情况**	**协议**	**默认传入端口**	注意
许可证服务器	许可证服务器	TCP	27000	
许可证服务器	Citrix 的许可证服务器（供应商守护程序）	TCP	7279	

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

许可证服务器	许可证管理控制台	TCP	8082	
许可证服务器	Web Services for Licensing	TCP	8083	

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

HDX

Dec 05, 2017

> **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。

Citrix HDX 融合了多种技术，可提供高清晰度用户体验。

在设备上

HDX 利用用户设备的计算能力来改善和优化用户体验。HDX 技术可确保用户在其虚拟桌面或应用程序中获得流畅、无缝的多媒体内容体验。工作区控制功能使用户能够暂停虚拟桌面和应用程序，然后在其他设备上从上次暂停的位置继续工作。

在网络上

HDX 集成了先进的优化和加速功能，可在任何网络（包括低带宽、高延迟的 WAN 连接）中交付最佳性能。

HDX 功能能够适应环境变化。这些功能将平衡性能和带宽。这些功能为每种用户场景应用最佳技术，而无论用户是在企业网络中本地访问桌面或应用程序，还是从公司防火墙外部远程访问桌面或应用程序。

在数据中心中

HDX 利用服务器的处理能力和可扩展性，交付高级图形性能，而无论客户端设备具备何种功能。

Citrix Director 提供的 HDX 通道监控功能可在用户设备上显示已连接 HDX 通道的状态。

HDX Insight 将 NetScaler Network Inspector 和性能管理器与 Director 相集成。它将捕获与 ICA 流量有关的数据，并提供实时详细信息和历史详细信息的控制板视图。此数据包括客户端和服务器端 ICA 会话延迟、ICA 通道的带宽使用情况以及每个会话的 ICA 往返时间值。

从虚拟桌面体验 HDX 功能：

- 了解 Flash 重定向（三个 HDX 多媒体重定向技术之一）如何加快 Adobe Flash 多媒体内容的交付：
  1. 请下载 Adobe Flash Player (http://get.adobe.com/flashplayer/)，然后将其安装在虚拟桌面和用户设备上。
  2. 在 Desktop Viewer 工具栏中，选择**首选项**。在 Desktop Viewer 首选项对话框中，选择 **Flash** 选项卡并选择**优化内容**。
  3. 要了解 Flash 重定向功能是如何向虚拟桌面快速交付 Flash 多媒体内容的，请在桌面上观看含有 Flash 视频的 Web 站点（例如 YouTube）上的视频。Flash 重定向采用无缝模式，因此用户察觉不到它在运行。您可以进行检查以确认是否正在使用 Flash 重定向。请寻找在 Flash 播放器启动前短暂显示的一个色块，或者右键单击视频并在菜单中查找“Flash 重定向”。

- 了解 HDX 如何交付高清晰度音频：
  1. 将 Citrix 客户端配置为采用最高音频质量；请参阅 Citrix Receiver 文档了解详细信息。
  2. 在桌面上使用数字音频播放器（如 iTunes）播放音乐文件。

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

默认情况下，HDX 为大多数用户提供卓越的图形和视频体验，无需执行任何配置。在大多数情况下提供最佳体验的 Citrix 策略设置默认处于启用状态。

- HDX 会根据客户端、平台、应用程序和网络带宽因素自动选择最佳的交付方法，然后基于不断变化的条件自行调整。
- HDX 可优化 2D 和 3D 图形和视频的性能。
- 借助 HDX，用户设备可以通过流技术直接从 Internet 或 Intranet 上的源提供程序推送多媒体文件，而非通过主机服务器推送。如果未满足此客户端内容提取的要求，媒体交付将回退到服务器端内容提取和多媒体重定向。通常情况下，不需要调整多媒体重定向功能策略。
- 在多媒体重定向不可用时，HDX 将服务器端呈现的丰富视频内容交付到虚拟桌面：在包含高清晰度视频的 Web 站点上观看视频，例如 http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/。

须知事项：

- 有关 HDX 功能的支持和要求信息，请参阅系统要求一文。除非另有说明，否则 HDX 功能适用于受支持的 Windows 服务器操作系统、Windows 桌面操作系统和 Remote PC Access 桌面。
- 本内容介绍如何进一步优化用户体验，提高服务器可扩展性或降低带宽要求。有关使用 Citrix 策略和策略设置的信息，请参阅适用于此版本的 Citrix 策略文档。
- 对于包括编辑注册表在内的说明，请谨慎操作：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。

限制

在会话内部使用 Windows Media Player 时，如果启用了“远程音频和视频扩展(RAVE)”，则当您右键单击视频内容并选择**始终在最上显示正在播放列表**，将显示黑屏。

客户端自动重新连接和会话可靠性

访问托管应用程序或桌面时，可能会出现网络中断问题。我们提供了客户端自动重新连接和会话可靠性功能，以使您能够体验更加顺畅的重新连接。在默认配置中，依次启动会话可靠性和客户端自动重新连接。

客户端自动重新连接

客户端自动重新连接将重新启动客户端引擎以重新连接到断开连接的会话。客户端自动重新连接将在设置中指定的时间之后关闭（或断开）用户会话。如果启用了客户端自动重新连接，系统将向用户发送应用程序和桌面网络中断通知，如下所示：

- **桌面。**会话窗口将变为灰色，并且倒计时器将显示重新连接发生之前的时间。
- **应用程序。**会话窗口将关闭并向用户显示一个对话框，其中包含一个显示尝试重新连接之前的剩余时间的倒计时器。

客户端自动重新连接过程中，会话将重新启动所需的网络连接。客户端自动重新连接过程中，用户不能与会话交互。

重新连接时，断开的会话将使用保存的连接信息重新连接。用户可以正常与应用程序和桌面交互。

默认客户端自动重新连接设置：

- 客户端自动重新连接超时：120 秒
- 客户端自动重新连接：已启用
- 客户端自动重新连接身份验证：已禁用
- 客户端自动重新连接日志记录：已禁用

有关详细信息，请参阅客户端自动重新连接策略设置。

会话可靠性

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

会话可靠性将在网络中断时无缝重新连接 ICA 会话。会话可靠性将在设置中指定的时间之后关闭（或断开）用户会话。会话可靠性超时之后，客户端自动重新连接策略设置生效，尝试将用户重新连接到断开连接的会话。启用了会话可靠性时，将向用户发送应用程序和桌面网络中断通知，如下所示：

- **桌面。**会话窗口将变为半透明，并且倒计时器将显示重新连接发生之前的时间。
- **应用程序。**窗口将变为半透明，并且通知区域中显示连接已中断弹出通知。

会话可靠性处于活动状态时，用户不能与 ICA 会话交互。但是，击键等用户操作在网络中断后会立即缓冲几秒钟时间，并在网络可用时重新传输。

重新连接时，客户端和服务器将在交换协议的相同位置恢复。会话窗口不再半透明显示，并且将为应用程序显示恰当的通知区域弹出通知。

默认会话可靠性设置

- 会话可靠性超时：180 秒
- 重新连接用户界面透明度级别：80%
- 会话可靠性连接：已启用
- 会话可靠性端口号：2598

有关详细信息，请参阅会话可靠性策略设置。

启用了客户端自动重新连接和会话可靠性的 NetScaler

如果在服务器上启用了多流和多端口策略，并且满足以下任意或全部条件，客户端自动重新连接将不起作用：

- 会话可靠性在 NetScaler Gateway 上处于禁用状态。
- 故障转移发生在 NetScaler 设备上。
- NetScaler SD-WAN 与 NetScaler Gateway 结合使用。

适用于触屏设备的平板电脑模式

默认情况下，连接/漫游到 Windows 10 VDA 的启用触摸的任何设备都以平板电脑模式启动。

平板电脑模式要求最低版本为 XenServer 7.2。XenServer 7.2 与 XenDesktop VDA 集成，并更改虚拟机管理程序以便为二合一设备启用虚拟固件设置。Windows 10 根据此更新的 BIOS 在虚拟机上加载 GPIO 驱动程序。它用于在虚拟机中在平板电脑和桌面模式之间切换。有关详细信息，请参阅 http://docs.citrix.com/content/dam/docs/en-us/xenserver/current-release/downloads/xenserver-release-notes.pdf。

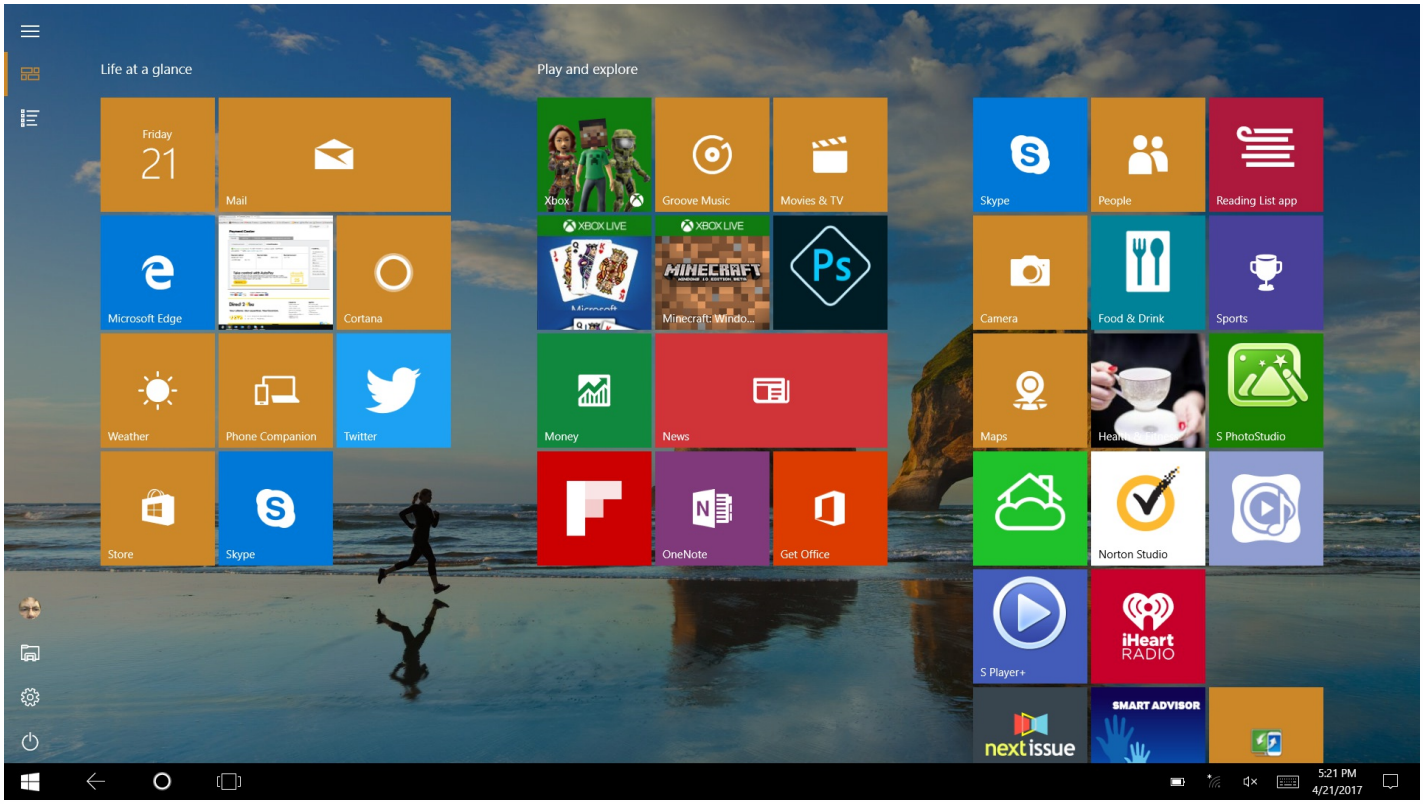
平板电脑模式提供了更适于触屏的用户界面：

- 稍大的按钮。
- 开始屏幕和您启动的任何应用程序都以全屏模式打开。
- 任务栏包含返回按钮。
- 从任务栏中删除了图标。

您可以访问文件资源管理器。

Web Receiver 不支持平板电脑模式。

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



运行 XenServer CLI 命令可在便携式计算机/平板电脑之间切换：

xe vm-param-set uuid= platform:acpi_laptop_slate=1

要禁用或启用平板电脑模式，请在 XenApp 和 XenDesktop 上配置以下注册表设置：

HKEY_LOCAL_MACHINE\Software\Citrix\Sessions

名称：CitrixEnhancedUserExperience
类型：REG_DWORD

值：
0（禁用）
1（启用）

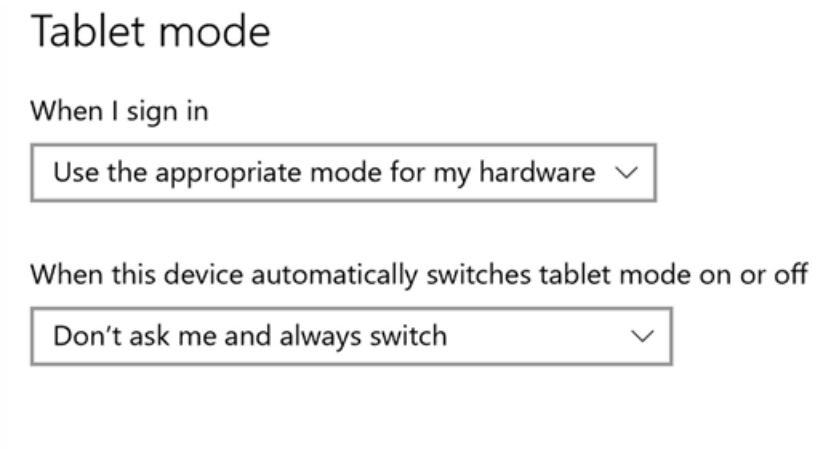
启动会话之前的准备工作

我们建议您在启动会话之前先在 VDA 上导航到 **Settings（设置）> System（系统）> Tablet Mode（平板电脑模式）**，并从下拉菜单中设置以下选项：

- Use the appropriate mode for my hardware（为我的硬件使用合适的模式）
- Don't ask me and always switch（不再询问并始终切换）

如果您未在启动会话之前设置这些选项，请在启动会话后设置这些选项并重新启动 VDA。

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



提高发送给用户设备的图像质量

下面的视频显示策略设置将控制从虚拟桌面发送到用户设备的图像质量。

- 视觉质量。控制在用户设备上显示的图像的视觉质量：中、高、始终无损、设为无损（默认 = 中）。使用默认设置“中”的实际视频质量取决于可用带宽。
- 目标帧速率。指定每秒从虚拟桌面发送到用户设备的最大帧数（默认 = 30）。对于 CPU 速度较慢的设备，指定较低的值可以改善用户体验。支持的最高每秒帧速率是 60。
- 显示内存限制。指定会话的最大视频缓冲区大小，以 KB 为单位（默认 = 65536 KB）。对于需要更高颜色深度和分辨率的连接，可增大该限值。可以计算所需的最大内存。

提高视频会议性能

多个常用视频会议应用程序已优化，可通过多媒体重定向从 XenApp 和 XenDesktop 交付（例如，请参阅 HDX RealTime Optimization Pack）。对于未优化的应用程序，HDX 网络摄像机视频压缩可提高在会话中的视频会议过程中网络摄像机的带宽效率和延迟容忍度。此技术通过一个专用多媒体虚拟通道使用流技术推送网络摄像机通信。与常时等量 HDX Plug-n-Play USB 重定向支持相比，此技术占用的带宽较少，并且可以通过 WAN 连接正常工作。

Citrix Receiver 用户可以通过选择 Desktop Viewer 麦克风和网络摄像机设置**不使用麦克风或网络摄像机**来覆盖默认行为。要阻止用户切换 HDX 网络摄像机视频压缩功能，请通过 ICA 策略设置 > “USB 设备”下的策略设置禁用 USB 设备重定向。

HDX 网络摄像机视频压缩功能需要启用以下策略设置（默认情况下均已启用）。

- 客户端音频重定向
- 客户端麦克风重定向
- 多媒体会议
- Windows Media 重定向

如果网络摄像机支持 H.264 硬件编码，默认情况下 HDX 视频压缩功能将采用硬件编码。硬件编码占用的带宽可能高于软件编码。要强制执行软件压缩，请向注册表项 HKCU\Software\Citrix\HdxRealTime 添加以下 DWORD 注册表项值：DeepCompress_ForceSWEncode=1。

网络流量优先级

对于使用支持服务质量 (QoS) 的路由器的会话，可以跨多个连接为网络流量分配优先级。可使用四个 TCP 流（实时、交互、后台和批量）和两个用户数据报协议 (UDP) 流（语音和 Framehawk 显示远程处理）在用户设备与服务器之间传输 ICA 通信。每个虚拟通道都有一个特定的优先级，并通过相应连接进行传输。可以根据连接所使用的 TCP 端口号分别设置这些通道。

对于安装在 Windows 10、Windows 8 和 Windows 7 计算机上的 Virtual Delivery Agent (VDA)，支持多通道流连接。请与贵公

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

司的网络管理员协作，确保在多端口策略设置中配置的通用网关协议 (CGP) 端口已正确分配到网络路由器。

仅在已配置多会话可靠性端口或 CGP 端口时，才支持服务质量 (QoS)。

小心：使用此功能时，请启用传输安全性。Citrix 建议您使用 Internet 协议安全性 (Internet Protocol Security, IPsec) 或传输层安全性 (Transport Layer Security, TLS)。仅当连接在支持多流 ICA 的 NetScaler Gateway 上进行遍历时，才支持 TLS 连接。在内部企业网络上时，不支持采用 TLS 的多流连接。

要为多流连接设置服务质量，请向策略中添加以下 Citrix 策略设置（有关详细信息，请参阅多流连接策略设置）：

- 多端口策略 – 此设置为跨多个连接的 ICA 通信指定端口，并确定网络优先级。
  - 从“CGP default port priority”（CGP 默认端口优先级）列表中，选择一种优先级。默认情况下，主端口 (2598) 拥有“高”优先级。
  - 根据需要在“CGP port1”（CGP 端口 1）、“CGP port2”（CGP 端口 2）和“CGP port3”（CGP 端口 3）中键入更多 CGP 端口，并标识每个端口的优先级。每个端口必须有唯一的优先级。

  将 VDA 上的防火墙显式地配置为允许其他 TCP 流量。
- 多流计算机设置 – 默认情况下禁用此设置。如果要在环境中使用具有“多流”支持功能的 Citrix NetScaler SD-WAN，则无需配置此设置。如果要使用第三方路由器或旧版 Branch Repeater 实现所需的服务质量 (QoS)，应配置此策略。
- 多流用户设置 – 默认禁用此设置。

要使包含这些设置的策略生效，用户必须注销后再登录到网络。

相关信息

> Graphics
> Multimedia
> General content redirection
> Adaptive transport

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

自适应传输

Apr 12, 2018

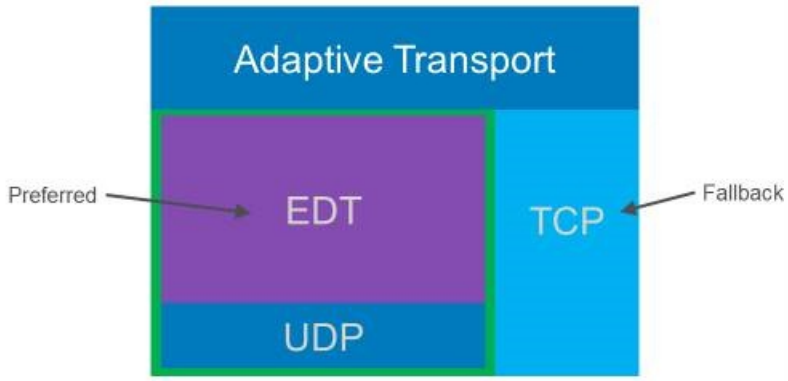
简介

自适应传输是 XenApp 和 XenDesktop 的新数据传输机制。此传输速度更快，更具可扩展性，改进了应用程序的交互性，并且在具有挑战性的远距离 WAN 和 Internet 连接中互动性更强。自适应传输维持高服务器可扩展性，并有效利用带宽。借助自适应传输，ICA 虚拟通道可以自动响应不断变化的网络条件。它们可以在新 Citrix 协议（名为 Enlightened Data Transport (EDT)）与 TCP 之间智能地切换底层协议，以提供最佳性能。这提高了所有 ICA 虚拟通道（包括 Thinwire 显示远程处理、文件传输（客户端驱动器映射）、打印和多媒体重定向）的数据吞吐量。相同的设置适用于 LAN 和 WAN 条件。

设置为**首选**时，请首先执行通过 EDT 进行的数据传输，并回退到 TCP。

默认情况下，禁用自适应传输（**关**），并始终使用 TCP。

出于测试目的，您可以设置**诊断模式**，在这种情况下，仅使用 EDT，并禁用回退到 TCP。



与 Citrix SD-WAN WAN 优化的互操作性

Citrix SD-WAN WAN 优化 (WANOP) 提供跨会话的标记化压缩（重复数据删除功能），包括基于 URL 的视频缓存。如果两个人或多个人在办公室观看同一个客户端提取的视频，或者传输或打印同一个文件或文档的重要部分，WANOP 将大幅度降低带宽。此外，通过在分支机构的设备上运行面向 ICA 数据缩减和打印作业压缩的进程，WANOP 将提供 VDA 服务器 CPU 卸载并启用更高的 XenApp 和 XenDesktop 服务器可扩展性。

重要： 将 TCP 用作数据传输协议时，Citrix WANOP 将支持优化功能，如前一段内容中所述。对网络连接使用 Citrix WANOP 时，请选择 TCP。通过使用 TCP 流控制和拥塞控制，WANOP 可确保在高延迟和一定程度的数据包丢失的情况下与 EDT 的等效交互。

要求和注意事项

- XenApp 和 XenDesktop：最低版本 7.13
- VDA for Desktop OS：最低版本 7.13
- VDA for Server OS：最低版本 7.13
- StoreFront：最低版本 3.9
- Citrix Receiver for Windows：最低版本 4.7
- Citrix Receiver for Mac：最低版本 12.5

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

- Citrix Receiver for iOS：最低版本 7.2
- Citrix Receiver for Linux：仅对于直接 VDA 连接，版本为 13.6，对于使用 NetScaler Gateway 的 DTLS 支持（或者直接 VDA 连接的 DTLS），版本为 13.7。
- Citrix Receiver for Android：仅对于直接 VDA 连接，版本为 3.12.3，对于使用 NetScaler Gateway 的 DTLS 支持（或者直接 VDA 连接的 DTLS），版本为 3.13。
- 仅限 IPv4 VDA。不支持 IPv6 配置以及 IPv6 和 IPv4 混合配置。
- NetScaler：最低版本 11.1-51.21。有关 NetScaler 配置的详细信息，请参阅将 NetScaler Gateway 配置为支持高级传输。

配置

1. 安装 XenApp 和 XenDesktop。
2. 安装 StoreFront。
3. 安装 VDA（适用于桌面操作系统或服务器操作系统）
4. 安装 Citrix Receiver for Windows（Citrix Receiver for Mac 或 Citrix Receiver for iOS）。
5. 在 Studio 中，启用策略设置“HDX 自适应传输”（默认禁用）。我们还建议您不要将此功能作为站点中所有对象的通用策略来启用。
   - 要启用该策略设置，请将值设置为“首选”，然后单击“确定”。
     - **首选。**尽可能使用基于 EDT 的自适应传输，并回退到 TCP。
     - **诊断模式。**TCP 强制打开，并禁用回退到 EDT。我们建议此设置仅用于故障排除。
     - **关。**强制启用 TCP，并禁用 EDT。
6. 单击“下一步”，完成向导中的步骤。
7. 此策略将在用户重新连接 ICA 会话时生效。尽管不需要，但您可以运行 **gpupdate /force** 以将该策略设置移动到服务器，但用户仍然必须重新连接 ICA 会话。
8. 请从受支持的 Citrix Receiver 启动会话以使用自适应传输建立连接。
9. 要进行安全的外部访问，请在 NetScaler Unified Gateway 上配置 DTLS 加密。有关详细信息，请参阅配置 NetScaler Gateway 以支持高级传输。

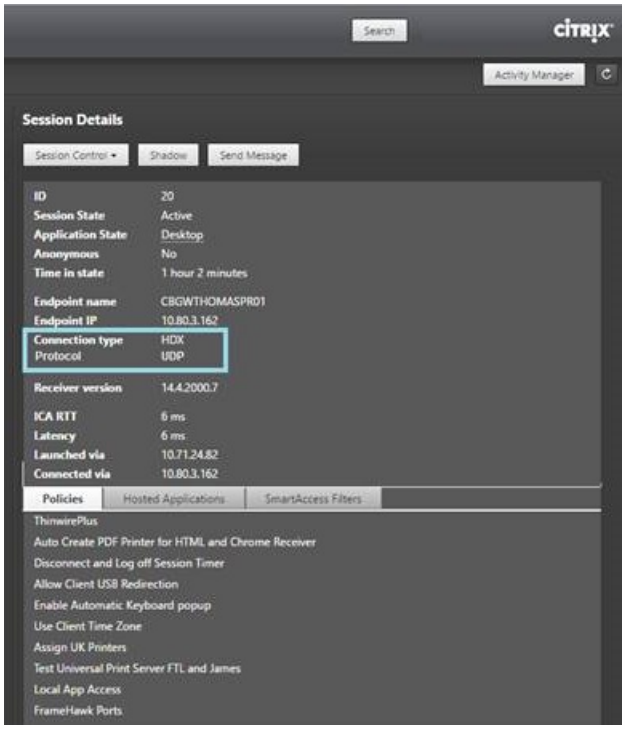
要确认策略设置是否已生效，请执行以下操作：

- 使用 **netstat -a** 检查是否在 VDA 上启用了 ICA 用户数据报协议 (UDP) 服务。
- 使用 VDA 上提供的 **Director** 或 **CtxSession.exe** 命令行实用程序检查虚拟通道是否通过 EDT 运行。

Director 示例

在 Director 中，**会话详细信息 > 连接类型**显示策略设置。查找连接类型 **HDX**。如果协议为 **UDP**，EDT 将可用于会话。如果协议为 **TCP**，会话将处于回退或默认模式。如果连接类型为 **RDP**，则不使用 ICA，并且协议为**不适用**。有关详细信息，请参阅监视会话。

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



CtxSession.exe 示例

此示例说明了 EDT over UDP 可用于会话。在命令行中键入 CtxSession.exe。

```
C:\Program Files (x86)\Citrix\System32>CtxSession

会话 2 传输协议：UDP -> CGP -> ICA
```

要查看详细统计信息，请使用 -v 开关：

```
>CtxSession -v
```


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

安装和配置

Dec 05, 2017

请在开始执行每个部署步骤之前查看参考文章，以了解部署过程中显示和指定的内容。

请按照以下顺序部署 XenApp 或 XenDesktop。

准备

查看准备安装，并完成所有必要的任务。

- 与概念、功能、与早期版本之间的差异、系统要求及数据库有关的信息的查找位置。
- 决定要在哪里安装核心组件时的考虑事项。
- 权限和 Active Directory 要求。
- 有关可用安装程序、工具和接口的信息。

安装核心组件

安装 Delivery Controller、Citrix Studio、Citrix Director、Citrix 许可证服务器和 Citrix StoreFront。有关详细信息，请参阅安装核心组件或使用命令行安装。

创建站点

安装核心组件并启动 Studio 后，系统会自动引导您完成创建站点的过程。

安装一个或多个 Virtual Delivery Agent (VDA)

在运行 Windows 操作系统的计算机上安装 VDA，在主映像上或直接在每台计算机上安装均可。请参阅安装 VDA 或使用命令行安装。如果要通过 Active Directory 安装 VDA，提供了示例脚本。

对于安装了 Linux 操作系统的计算机，请遵循 Linux Virtual Delivery Agent 中的指导。

对于 Remote PC Access 部署，在每个办公室 PC 上安装 VDA for Desktop OS。如果只需要核心 VDA 服务，请使用独立的 VDAWorkstationCoreSetup.exe 安装程序和现有的电子软件分发 (ESD) 方法。（准备安装中包含有关可用 VDA 安装程序的完整信息。）

安装其他可选组件

如果要使用 Citrix 通用打印服务器，请在您的打印服务器上安装其服务器组件。请参阅安装核心组件或使用命令行安装。

要让 StoreFront 使用各种身份验证选项（例如 SAML 断言），请安装 Citrix 联合身份验证服务。

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

要让最终用户对其用户帐户拥有更大的控制权限，请安装自助服务密码重置。有关详细信息，请参阅自助服务密码重置文档。

（可选）在 XenApp 或 XenDesktop 部署中集成更多 Citrix 组件。

- Provisioning Services 是 XenApp 和 XenDesktop 的可选组件，用于通过流技术将主映像推送到目标设备来置备计算机。
- Citrix NetScaler Gateway 是一款确保应用程序访问安全的解决方案，为管理员提供应用程序粒度级别的策略和操作控制，从而确保访问应用程序和数据的安全性。
- Citrix NetScaler SD-WAN 是一套用于优化 WAN 性能的设备。

有关安装说明信息，请参阅这些组件、功能和技术的文档。

创建计算机目录

在 Studio 中创建站点后，系统将引导您完成创建计算机目录的过程。

目录中可以包含物理机或虚拟机 (VM)。虚拟机可以从主映像创建。使用虚拟机管理程序或云服务提供 VM 时，请先在该主机上创建一个主映像。然后，在创建目录时，请指定该映像，创建 VM 时需要使用该映像。

创建交付组

在 Studio 中创建第一个计算机目录后，系统将引导您完成创建交付组的过程。

交付组指定哪些用户可以访问选定目录中的计算机以及可供这些用户使用的应用程序。

创建应用程序组（可选）

在创建交付组后，您可以选择创建应用程序组。可为在不同交付组之间共享，或由交付组中一个用户子集使用的应用程序创建应用程序组。

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

准备安装

Mar 01, 2018

要部署 XenApp 和 XenDesktop，请先安装以下组件。此过程将为向您的防火墙内部的用户交付应用程序和桌面做好准备。

- 一个或多个 Delivery Controller
- Citrix Studio
- Citrix Director
- Citrix StoreFront
- Citrix 许可证服务器
- 一个或多个 Citrix Virtual Delivery Agent (VDA)
- 可选组件和技术，例如，通用打印服务器、联合身份验证服务和自助服务密码重置

对于您的防火墙外部的用户，请安装并配置一个附加组件，例如 NetScaler。有关将 NetScaler 与 StoreFront 结合使用的简介，请参阅将 XenApp 和 XenDesktop 与 NetScaler Gateway 集成。

如何能够安装组件

可以使用 XenApp 和 XenDesktop ISO 中的完整产品安装程序部署很多组件和技术。可以使用独立的 VDA 安装程序来安装 VDA。所有的安装程序都提供图形界面和命令行接口。请参阅安装程序。

> 产品 ISO 包含用于在 Active Directory 中安装、升级或删除计算机组的 VDA 的示例脚本。也可以使用脚本来管理 Machine Creation Services (MCS) 和 Provisioning Services (PVS) 所使用的主映像。有关详细信息，请参阅使用脚本安装 VDA。

作为替代使用安装程序的一个自动化方法，Citrix Smart Tools 使用蓝图来创建 XenApp 和 XenDesktop 部署。有关详细信息，请参阅 Smart Tools 产品文档。

安装之前要查看的信息

- 技术概述：如果您不熟悉该产品及其组件。
- 7.x 中的更改：如果您要从 XenApp 6.x 或 XenDesktop 5.6 部署转到当前版本。
- 安全：计划您的部署环境时。
- 已知问题：在此版本中可能会遇到的问题。
- 数据库：了解系统数据库的相关信息以及如何配置这些数据库。在安装 Controller 过程中，可以安装 SQL Server Express 以用作站点数据库。大部分数据库信息都是在安装核心组件之后创建站点时配置的。
- Remote PC Access：如果您要部署一个让您的用户可以远程访问其在办公室的物理机的环境。
- 连接和资源：如果您要使用虚拟机管理程序或云服务为应用程序和桌面托管或置备 VM。（安装核心组件之后）可以在创建站点时配置第一个连接。在那之前随时设置您的虚拟化环境。
- Microsoft System Center Configuration Manager：如果您要使用 ConfigMgr 来管理对应用程序和桌面的访问，或者如果您要将局域网唤醒功能与 Remote PC Access 结合使用。

组件的安装位置

请查看系统要求了解支持的平台、操作系统和版本。必备组件会自动安装，除非另有说明。请参阅 Citrix StoreFront 和 Citrix

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

许可证服务器文档，了解其支持平台和必备条件。

您可以将核心组件安装在同一服务器或不同服务器上。

- 在一个服务器上安装所有核心组件适用于评估、测试或小型生产部署。
- 为了能够在将来扩展，请考虑在不同的服务器上安装组件。例如，将 Studio 安装在不同于安装了 Controller 的服务器的其他计算机上，您就可以远程管理站点。
- 对于大多数生产部署，建议在单独的服务器上安装核心组件。

可以在同一服务器上安装 Delivery Controller 和 VDA for Server OS。启动安装程序并选择 Delivery Controller（以及您希望在相应计算机上安装的任何其他核心组件）。然后再次启动安装程序并选择 Virtual Delivery Agent for Server OS。

确保每个操作系统都具有最新更新。例如，如果未安装 Windows KB2919355，在 Windows Server 2012 R2 安装 Controller 或者在 Windows 8.1 或 Windows Server 2012 R2 上安装 VDA 将失败。

确保所有计算机具有同步的系统时钟。保护计算机之间的通信的 Kerberos 基础结构要求同步。

面向 Windows 10 计算机的优化指南在 CTX216252 中提供。

不可安装组件的位置：

- 请勿在 Active Directory 域控制器上安装任何组件。
- 不支持在 SQL Server 群集安装或 SQL Server 镜像安装中的节点上安装 Controller，也不支持在运行 Hyper-V 的服务器上安装。
- 请勿在运行 XenApp 6.5 Feature Pack 2 for Windows Server 2008 R2 或任何早期版本的 XenApp 的服务器上安装 Studio。

权限和 Active Directory 要求

您必须是正在安装组件的计算机上的域用户和本地管理员。

要使用独立的 VDA 安装程序，必须提升了管理权限或使用**以管理员身份运行**。

请在开始安装之前配置 Active Directory 域。

- 系统要求列出了受支持的 Active Directory 功能级别。Active Directory 提供详细信息。
- 必须至少有一个运行 Active Directory 域服务的域控制器。
- 请勿在域控制器上安装任何 XenApp 或 XenDesktop 组件。
- 在 Studio 中指定组织单位名称时，请勿使用正斜杠 (/)。

用于安装 Citrix 许可证服务器的 Windows 用户帐户会自动配置为许可证服务器上的委派管理完全权限管理员。

相关详细信息：

- 最佳安全做法
- 委派管理
- 有关 Active Directory 配置说明的 Microsoft 文章

安装指导、注意事项和最佳做法

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

在安装任何组件过程中：
通常，如果组件有必备条件，安装程序会在它们不存在时部署它们。有些必备条件可能要求重新启动计算机。

在安装前、安装期间和安装完毕后创建对象时，为每个对象指定唯一的名称。例如，为网络、组、目录和资源提供唯一名称。

如果组件未成功安装，安装将停止并显示一条错误消息。成功安装的组件将会保留。不需要重新安装它们。

当安装（或升级）组件时，会自动收集分析数据。默认情况下，安装完成时，这些数据会自动上载到 Citrix。此外，在您安装组件时，您会自动在 Citrix 客户体验改善计划 (CEIP) 中注册，这会上载匿名数据。在安装过程中，您还可以选择参与收集用于维护和故障排除的诊断信息的其他 Citrix 技术（例如 Smart Tools）。有关这些计划的信息，请参阅 Citrix Insight Services。

在安装 VDA 过程中：

安装 VDA 时（除了使用 VDAWorkstationCoreSetup.exe 安装程序时）默认包括 Citrix Receiver for Windows。您可以将 Citrix Receiver 从安装中排除。您或您的用户可以从 Citrix Web 站点下载并安装（和升级）Citrix Receiver 和其他 Citrix Receiver。此外，也可以在您的 StoreFront 服务器上提供这些 Citrix Receiver。请参阅在服务器上提供 Citrix Receiver 安装文件，或者参阅您正在使用的 StoreFront 版本中的同等内容。

默认情况下，在受支持的 Windows 服务器上启用打印后台处理程序服务。如果禁用此服务，则无法成功安装 VDA for Windows Server OS，因此，请务必在安装 VDA 之前启用此服务。

大多数受支持的 Windows 版本都已附带安装 Microsoft 媒体基础。如果要安装 VDA 的计算机上未安装媒体基础（例如 N 版本），多项多媒体功能将不安装并且无法运行。您可以在安装媒体基础后确认该限制，或者终止 VDA 安装并在以后重新启动。在图形界面中，此选项在消息中提供。在命令行中，可以使用 /no_mediafoundation_ack 确认该限制。

安装 VDA 时，系统将自动创建名为“直接访问用户”的新本地用户组。在 VDA for Desktop OS 上，此组仅适用于 RDP 连接。在 VDA for Server OS 上，此组仅适用于 ICA 和 RDP 连接。

VDA 必须具有有效的 Controller 地址才能进行通信。否则无法建立会话。您可以在安装 VDA 时指定 Controller 地址，也可以在以后指定。但请记住，必须指定该地址。

在安装 VDA 之后和过程中重新启动：

VDA 安装结束时需要重新启动计算机。默认情况下会自动重新启动。

为了尽量减少安装 VDA 过程中所需的重新启动次数：

- 请务必在开始安装 VDA 之前安装受支持的 .NET Framework 版本。
- 对于 Windows 服务器操作系统计算机，请在安装 VDA 之前安装并启用 RDS 角色服务。

如果您未在安装 VDA 之前安装那些必备项：

- 如果您使用图形界面或使用命令行界面但未使用 /noreboot 选项，计算机在安装必备项后会自动重新启动。
- 如果您使用命令行接口并使用 /noreboot 选项，则必须启动重新启动操作。

每次重新启动后，重新运行安装程序或命令以继续安装 VDA。

安装程序

完整产品安装程序

使用 XenApp 和 XenDesktop ISO 中提供的完整产品安装程序，您可以：

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

- 安装、升级或删除 XenApp 和 XenDesktop 核心组件：Delivery Controller、Studio、Director、StoreFront、许可证服务器
- 安装或升级适用于服务器或桌面操作系统的 Windows VDA
- 在您的打印服务器上安装通用打印服务器 Ups 服务器组件
- 安装联合身份验证服务
- 安装自助服务密码重置服务

要从服务器操作系统为一个用户交付桌面（例如，用于 Web 部署），请使用完整产品安装程序的命令行接口。有关详细信息，请参阅服务器 VDI。

独立的 VDA 安装程序

Citrix 下载页面上提供独立的 VDA 安装程序。独立的 VDA 安装程序远小于完整产品 ISO。它们可以更轻松地适应以下部署：

- 使用本地暂存或复制的电子软件分发 (ESD) 软件包
- 具有物理计算机
- 具有远程办公室

默认情况下，自解压独立 VDA 中的文件被解压至 Temp 文件夹。提取到 Temp 文件夹时所需的计算机上的磁盘空间高于使用完整产品安装程序时所需的磁盘空间。但是，解压至 Temp 文件夹的文件在安装完成后会自动被删除。或者，可以使用 /extract 命令与绝对路径。

有三个独立的 VDA 安装程序供下载。

VDAServerSetup.exe：

安装 VDA for Server OS。它支持完整安装程序适用的所有 VDA for Server OS 选项。

VDAWorkstationSetup.exe：

安装 VDA for Desktop OS。它支持完整安装程序适用的所有 VDA for Desktop OS 选项。

VDAWorkstationCoreSetup.exe：

安装为 Remote PC Access 部署或核心 VDI 安装优化过的 VDA for Desktop OS。Remote PC Access 使用物理计算机。核心 VDI 安装是不用作主映像的 VM。在此类部署中，它只安装 VDA 连接所需的核心服务。因此，它只支持完整产品或 VDAWorkstationSetup 安装程序适用的选项中的一部分。

此安装程序不安装或包含用于以下项的组件：

- App-V。
- Profile Management。将 Citrix Profile Management 排除在安装之外将影响 Citrix Director 显示内容。有关详细信息，请参阅安装 VDA。
- Machine Identity Service。
- Personal vDisk 或 AppDisks。

VDAWorkstationCoreSetup.exe 安装程序不安装或包含 Citrix Receiver for Windows。

使用 VDAWorkstationCoreSetup.exe 相当于使用完整产品安装程序或 VDAWorkstationSetup 安装程序来安装 Desktop OS VDA，并且：

- 在图形界面中：在**环境**页面上选择“Remote PC Access”选项，并在**组件**页面上清除“Citrix Receiver”复选框。
- 在命令行接口中：指定 /remotepc 和 components /vda 选项。

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

- 在命令行接口中：指定 /components vda 和 /exclude "Citrix Personalization for App-V - VDA" "Personal vDisk" "Machine Identity Service" "Citrix User Profile Manager" "Citrix User Profile Manager WMI 插件"

可以在以后运行完整产品安装程序来安装忽略的组件/功能。该操作将安装所有缺少的组件。

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

Microsoft Azure 资源管理器虚拟化环境

Dec 05, 2017

使用 Microsoft Azure Resource Manager 在您的 XenApp 或 XenDesktop 部署中置备虚拟机时，请按本指导原则进行操作。

创建 XenApp 或 XenDesktop 站点（这包括创建连接）时，或者稍后创建主机连接（创建站点之后）时，可以通过配置 XenApp 或 XenDesktop 以在 Azure Resource Manager 中置备资源。

您应熟悉以下内容：

- Azure Active Directory：https://azure.microsoft.com/en-us/documentation/articles/active-directory-howto-tenant/
- 同意框架：https://azure.microsoft.com/en-us/documentation/articles/active-directory-integrating-applications/
- 服务主体：https://azure.microsoft.com/en-us/documentation/articles/active-directory-application-objects/

使用 Machine Creation Services 时不支持 Azure 磁盘加密。

创建到 Azure 资源管理器的连接

请参阅创建站点和连接和资源一文获取连接创建向导中所有页面的完整信息。以下信息仅涵盖与 Azure 资源管理器连接有关的详细信息。

可以通过两种方法建立与 Azure 资源管理器的主机连接：

- 通过向 Azure Resource Manager 进行身份验证以创建新的服务主体。
- 使用之前创建的服务主体的详细信息连接到 Azure Resource Manager。

通过向 Azure Resource Manager 进行身份验证以创建新的服务主体

开始之前，请务必：

- 在订阅的 Azure Active Directory 租户中具有一个用户帐户。
- Azure AD 用户帐户也是您希望用来置备资源的 Azure 订阅的协管理员。

在站点设置或添加连接和资源向导中：

1. 在**连接**页面上，选择 **Microsoft Azure** 连接类型和您的 Azure 环境。
2. 在**连接详细信息**页面上，输入 Azure 订阅 ID 和连接的名称。连接名称可以包含 1-64 个字符，不能仅包含空格或字符 \/:;#.*?=<>|[]{}'"()')。输入订阅 ID 和连接名称后，将启用**新建**按钮。
3. 输入 Azure Active Directory 帐户用户名和密码。
4. 单击**登录**。
5. 单击**接受**以将列出的权限授予 XenApp 或 XenDesktop。XenApp 或 XenDesktop 会创建一个允许它代表指定的用户管理 Azure Resource Manager 资源的服务主体。
6. 单击**接受**后，您会返回到 Studio 中的**连接**页面。请注意，成功完成 Azure 身份验证时，**新建**和**使用现有**按钮将被替换为**已连接**，同时出现绿色的复选标记指明已成功连接至您的 Azure 订阅。
7. 指明可以使用哪些工具来创建虚拟机，然后单击**下一步**。（在成功进行 Azure 身份验证和接受授予所需权限之前，您无法越过向导中的此页面。）

资源由区域和网络组成。

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

- 在**区域**页面上，选择一个区域。
- 在**网络**页面上，
  - 键入 1-64 字符的资源名称以帮助确定 Studio 中的区域和网络组合。资源名称不能仅包含空格，也不能包含字符 \/;:#.*?=<>|[]{}'"()'。
  - 选择一对儿虚拟网络和资源组。（由于您可能有不止一个具有相同名称的虚拟网络，将网络名称与资源组配对可提供唯一的组合。）如果在上一个不具有任何虚拟网络的页面中选择了一个区域，则需要返回至该页面并选择一个具有虚拟网络的区域。

完成向导。

使用之前创建的服务主体的详细信息连接到 Azure Resource Manager

要手动创建服务主体，请连接到 Azure Resource Manager 订阅并使用下方提供的 PowerShell cmdlet。

必备条件：

- $SubscriptionId：您希望置备 VDA 的订阅的 Azure Resource Manager 订阅 ID。
- $AADUser：订阅的 AD 租户的 Azure AD 用户帐户。
- 让 $AADUser 成为您的订阅的协管理员。
- $ApplicationName：将要在 Azure AD 中创建的应用程序名称。
- $ApplicationPassword：应用程序的密码。创建主机连接时，需要使用此密码作为应用程序机密。

要创建服务主体，请执行以下操作：

步骤 1：连接到 Azure Resource Manager 订阅。

```
Login-AzureRmAccount。
```

步骤 2：选择您想要创建服务主体的 Azure Resource Manager 订阅。

```
Select-AzureRmSubscription -SubscriptionID $SubscriptionId；
```

步骤 3：在您的 AD 租户中创建应用程序。

```
$AzureADApplication = New-AzureRmADApplication -DisplayName $ApplicationName -HomePage
"https://localhost/$ApplicationName" -IdentifierUris https://$ApplicationName -Password $ApplicationPassword
```

步骤 4：创建服务主体。

```
New-AzureRmADServicePrincipal -ApplicationId $AzureADApplication.ApplicationId
```

步骤 5：向服务主体分配角色。

```
New-AzureRmRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName
$AzureADApplication.ApplicationId –scope /subscriptions/$SubscriptionId
```

步骤 6：在 PowerShell 控制台的输出窗口中，记下 ApplicationId。创建主机连接时需要提供该 ID。

在站点设置或添加连接和资源向导中：

1. 在**连接**页面上，选择 **Microsoft Azure** 连接类型和您的 Azure 环境。
2. 在**连接详细信息**页面上，输入 Azure 订阅 ID 和连接的名称。（连接名称可以包含 1-64 个字符，不能仅包含空格或字符 \/;:#.*?=<>|[]{}'"()'）。

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

3. 单击**使用现有**。提供订阅 ID、订阅名称、身份验证 URL、管理 URL、存储后缀、Active Directory ID 或租户 ID、应用程序 ID 以及现有服务主体的应用程序机密。输入这些详细信息之后，将会启用**确定**按钮。单击**确定**。
4. 指明可以使用哪些工具来创建虚拟机，然后单击**下一步**。您提供的服务主体详细信息将用于连接到 Azure 订阅。（在提供“使用现有”选项的有效详细信息之前，您无法越过向导中的此页面。）

资源由区域和网络组成。

- 在**区域**页面上，选择一个区域。
- 在**网络**页面上：
  - 键入 1-64 字符的资源名称以帮助确定 Studio 中的区域和网络组合。资源名称不能仅包含空格，也不能包含字符 \/;:#.*?= <>|[]{}'"()'。
  - 选择一对儿虚拟网络和资源组。（由于您可能有不止一个具有相同名称的虚拟网络，将网络名称与资源组配对可提供唯一的组合。）如果在上一个不具有任何虚拟网络的页面中选择了一个区域，则需要返回至该页面并选择一个具有虚拟网络的区域。

完成向导。

使用 Azure Resource Manager 主映像创建计算机目录

此信息用于补充创建计算机目录一文中的指导信息。

主映像将作为用于在计算机目录中创建 VM 的模板。创建计算机目录之前，请在 Azure Resource Manager 中创建一个主映像。有关主映像的常规信息，请参阅“创建计算机目录”一文。

当您在 Studio 中创建计算机目录时：

- **操作系统**和**计算机管理**页面不包含 Azure 特定的信息。请遵循“创建计算机目录”一文中的指导信息。
- 在**主映像**页面上，选择某个资源组，然后导航（向下钻取）所有容器一直到您想要用作主映像的 Azure VHD。该 VHD 必须已经安装了 Citrix VDA。如果该 VHD 连接到某个 VM，该 VM 必须被停止。
- 只有在使用 Azure Resource Manager 主映像时，才会显示**存储和许可证类型**页面。

  选择一个存储类型：标准或高级。该存储类型影响在向导的虚拟机页面上提供哪些计算机大小。两个存储类型都会在单一数据中心中对您的数据进行多重同步复制。有关 Azure 存储类型和存储复制的详细信息，请参阅以下内容：

  https://azure.microsoft.com/en-us/documentation/articles/storage-introduction/

  https://azure.microsoft.com/en-us/documentation/articles/storage-premium-storage/

  https://azure.microsoft.com/en-us/documentation/articles/storage-redundancy/

  选择是否使用现有的本机 Windows Server 许可证。执行此操作并使用现有的本机 Windows Server 映像可利用 Azure Hybrid Use Benefits (HUB)。https://azure.microsoft.com/pricing/hybrid-use-benefit/ 上提供了更多详细信息。

  HUB 将在 Azure 中运行 VM 的成本降低到基本计算费率，因为它免除了源自 Azure 库的其他 Windows Server 许可证的代价。您需要将您的本机 Windows Server 映像交至 Azure 以使用 HUB。不支持 Azure 库映像。当前不支持本机 Windows Client 许可证。请参阅 https://blogs.msdn.microsoft.com/azureedu/2016/04/13/how-can-i-use-the-hybrid-use-benefit-in-azure/%23comment-145

  要检查置备的虚拟机是否成功利用 HUB，请运行 powershell 命令

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

```
Get-AzureRmVM -ResourceGroup MyResourceGroup -Name MyVM
```

并检查许可证类型是否为 Windows_Server。https://azure.microsoft.com/zh-cn/documentation/articles/virtual-machines-windows-hybrid-use-benefit-licensing/ 上提供了其他说明

- 在**虚拟机**页面上，指出您想要创建多少虚拟机；必须至少指定一个。选择计算机大小。创建完计算机目录之后，您将无法更改计算机大小。如果以后需要不同的大小，请删除该目录，然后创建使用相同主映像的新目录，并指定所需的计算机大小。

  虚拟机名称不能包含非 ASCII 字符和特殊字符。

- **网卡**、**计算机帐户**和**摘要**页面不包含特定于 Azure 的信息。请遵循“创建计算机目录”一文中的指导信息。

完成向导。

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

Microsoft Azure 虚拟化环境

Dec 05, 2017

连接配置

使用 Studio 创建 Microsoft Azure 连接时，需要使用 Microsoft Azure 发布设置文件中的信息。该 XML 文件中每个订阅的信息与下例类似（您的实际管理证书长度更长）：

```
ServiceManagementUrl="https://management.core.windows.net"
Id="o1455234-0r10-nb93-at53-21zx6b87aabb7p"
Name="Test1"
ManagementCertificate=";alkjdflaksdjfl;akjsdfl;akjsdfl; sdjfklasdfilaskjdfkluqweiopruaiopdfaklsdjfjsdilfasdkl;fjerioup" />
```

以下过程假定您正在从 Studio 创建连接，并且已启动站点创建向导或连接创建向导。

1. 在浏览器中，转至 https://manage.windowsazure.com/publishsettings/index。
2. 下载发布设置文件。
3. 在 Studio 中，在向导的**连接**页面上选择 Microsoft Azure 连接类型后，单击“导入”。
4. 如果您有多个订阅，系统将提示您选择所需的订阅。

ID 和证书将自动无提示导入到 Studio 中。

使用连接的电源操作取决于阈值。一般情况下，默认值适用，并且不应更改。但是，您可以编辑和更改连接（创建连接时，不能更改这些值）。有关详细信息，请参阅编辑连接。

虚拟机

在 Studio 中创建计算机目录时，选择每个虚拟机的大小取决于 Studio 提供的选项、选定 VM 实例类型的成本和性能以及可扩展性。

Studio 提供 Microsoft Azure 在选定地理区域提供的所有 VM 实例选项；Citrix 不能更改此显示内容。因此，您应熟悉自己的应用程序及其 CPU、内存和 I/O 要求。价格和性能点不同，提供的多个选项也有所差别；请参阅以下 Microsoft 文章，更好地了解这些选项。

- MSDN – Azure 虚拟机和云服务的大小：https://msdn.microsoft.com/zh-cn/library/azure/dn197896.aspx
- 虚拟机定价：http://azure.microsoft.com/zh-cn/pricing/details/virtual-machines

基本级别：前缀为“Basic”的 VM 表示基本磁盘。这些 VM 主要受 Microsoft 支持的 IOPS 级别 300 限制。不建议将其用于桌面操作系统 (VDI) 或服务器操作系统 RDSH（Remote Desktop Session Host，远程桌面会话主机）工作负载。

标准级别：标准级别 VM 显示在四个系列中：A、D、DS 和 G。

系列	在 Studio 中显示为
A	超小、小、中、大、超大、A5、A6、A7、A8、A9、A10、A11。建议分别使用桌面操作系统 (VDI) 或服务器操

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

	作系统 (RDSH) 工作负载对中型和大型 VM 进行测试。
D	标准_D1、D2、D3、D4、D11、D12、D13、D14。这些 VM 提供 SSD 用于临时存储。
DS	标准_DS1、DS2、DS3、DS4、DS11、DS12、DS13、DS14。这些 VM 为所有磁盘提供本地 SSD 存储。
G	标准_G1 – G5。这些 VM 用于高性能计算。

当在 Azure 高级存储中置备设备时，请确保选择在高级存储帐户中受支持的计算机大小。

各种 VM 实例类型的成本和性能

对于美国的标价，可以从以下地址获取每种 VM 实例类型每小时的成本：
https://azure.microsoft.com/zh-cn/pricing/details/virtual-machines/。

使用云环境时，了解您的实际计算要求非常重要。对于概念验证或其他测试活动，可以允许其利用高性能 VM 实例类型。还可以允许其使用性能最低的 VM 以节省成本。最好使用适用于任务的 VM。如果最初的目标是实现最佳性能，则可能不会获得需要的结果，并且随时时间的推移，成本可能会非常高，在某些情况下，一周内即可显示。如果 VM 实例类型的成本比较低，则性能和可用性可能都不适用于该任务。

对于桌面操作系统 (VDI) 或服务器操作系统 (RDSH) 工作负载，使用 LoginVSI 针对中型工作负载的测试结果显示，实例类型“中”(A2) 和“大”(A3) 提供最佳性价比。

评估工作负载时，“中”(A2) 和“大”（A3 或 A5）表示最佳性价比。不建议使用任何更小的工作负载。功能更强大的 VM 序列可能会为您的应用程序或用户提供所需的性能和可用性；但是，最好是以这三种实例类型之一为基础，确定成本更高、功能更强大的 VM 实例类型是否能够提供正确的值。

可扩展性

有多种限制会影响托管单元中的目录的可扩展性。可以通过联系 Microsoft Azure 技术支持增大默认值 (20) 来降低某些限制（例如 Azure 订阅中的 CPU 核心数）。不能更改其他限制，例如，每个订阅的虚拟网络中的 VM 数 (2048)。

Citrix 目前支持每个目录中 40 个 VM。

要增加目录或主机中的 VM 数，请联系 Microsoft Azure 技术支持。Microsoft Azure 默认限制阻止扩大到超出一定数量的 VM；但是，此限制经常更改，因此，请查看最新信息：http://azure.microsoft.com/zh-cn/documentation/articles/azure-subscription-service-limits/。

Microsoft Azure 虚拟网络最多支持 2048 个 VM。

Microsoft 建议每个云服务最多提供 40 个标准磁盘 VM 映像。扩展时，请考虑整个连接中的 VM 数量所需的云服务数。此外，还请考虑提供托管应用程序所需的 VMS。

请联系 Microsoft Azure 技术支持，确定是否需要增大默认 CPU 核心限制才能支持您的工作负载。

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

Microsoft System Center Virtual Machine Manager 虚拟化环境

Dec 05, 2017

如果您结合使用 Hyper-V 与 Microsoft System Center Virtual Machine Manager (VMM) 来提供虚拟机，请按本指导操作。

此版本支持系统要求一文中列出的 VMM 版本。

可以使用 Provisioning Services 和 Machine Creation Services 置备以下各项：

- 第 1 代桌面或服务器操作系统 VM
- 第 2 代 Windows Server 2012 R2、Windows Server 2016 和 Windows 10 VM（无论是否包含安全启动）

升级 VMM

- 从 VMM 2012 升级至 VMM 2012 SP1 或 VMM 2012 R2
  有关 VMM 和 Hyper-V 主机的要求，请参阅 http://technet.microsoft.com/zh-cn/library/gg610649.aspx。 有关 VMM 控制台的要求，请参阅 http://technet.microsoft.com/zh-cn/library/gg610640.aspx。

  不支持混合 Hyper-V 群集。混合群集的一个示例：群集 一部分运行 Hyper-V 2008，而另一部分则运行 Hyper-V 2012。

- 从 VMM 2008 R2 升级到 VMM 2012 SP1
  如果 从 VMM 2008 R2 上的 XenDesktop 5.6 进行升级，请遵循以下顺序以避免 XenDesktop 停机。
  1. 将 VMM 升级到 2012（现在运行的是 XenDesktop 5.6 和 VMM 2012）
  2. 将 XenDesktop 升级到最新版本（现在运行的是最新 XenDesktop 和 VMM 2012）
  3. 将 VMM 从 2012 升级到 2012 SP1（现在运行的是最新的 XenDesktop 和 VMM 2012 SP1）
- 从 VMM 2012 SP1 升级至 VMM 2012 R2
  如果 从 VMM 2012 SP1 上的 XenDesktop 或 XenApp 7.x 开始升级，请遵循以下顺序以 避免 XenDesktop 停机。
  1. 将 XenDesktop 或 XenApp 升级到最新版本（现在运行的是最新 XenDesktop 或 XenApp 和 VMM 2012 SP1）
  2. 将 VMM 2012 SP1 升级到 2012 R2（现在运行的是最新 XenDesktop 或 XenApp 和 VMM 2012 R2）

安装和配置摘要

1. 安装和配置虚拟机管理程序。
   1. 在服务器上安装 Microsoft Hyper-V Server 和 VMM。所有 Delivery Controller 必须与 VMM 服务器位于同一个林中。
   2. 在所有 Controller 上安装 System Center Virtual Machine Manager 控制台。
   3. 验证以下帐户信息：
      - 用于在 Studio 中指定主机的帐户是相关 Hyper-V 计算机的 VMM 管理员或 VMM 委派管理员。如果此帐户在 VMM 中仅具有委派管理员角色，则在主机创建过程中不会在 Studio 中列出存储数据。
      - 用于 Studio 集成的用户帐户还必须属于每个 Hyper-V Server 上的管理员本地安全组的成员，才能支持 VM 生命周期管理（例如 VM 创建、更新和删除）。

   注意：不支持在运行 Hyper-V 的服务器上安装 Controller。
2. 创建主 VM。
   1. 在主 VM 上安装 Virtual Delivery Agent，然后选择用于优化桌面的选项。这样会提高性能。
   2. 生成主 VM 的快照作为备份。
3. 创建虚拟桌面。如果要在创建站点或连接时使用 MCS 创建 VM，请执行以下操作：
   1. 选择 Microsoft 虚拟化主机类型。

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

2. 以主机服务器的完全限定的域名形式输入地址。
3. 输入先前设置的管理员帐户的凭据，该帐户应具有创建新 VM 的权限。
4. 在主机详细信息对话框中，选择创建新 VM 时将使用的群集或独立主机。
   重要：即使使用单 Hyper-V 主机部署，也请浏览并选择群集或独立主机。

SMB 3 文件共享上的 MCS

对于使用 VM 存储的 SMB 3 文件共享上的 MCS 创建的计算机目录，请确保按照以下要求设置凭据，以便来自 Controller 的虚拟机管理程序通信库 (HCL) 的调用能够成功连接到 SMB 存储：

- VMM 用户凭据必须包含对 SMB 存储的完全读取写入权限。
- VM 存储生命周期事件期间的存储虚拟磁盘操作通过 Hyper-V 服务器使用 VMM 用户凭据执行。

如果将 SMB 用作存储，请在 Windows Server 2012 上同时使用 VMM 2012 SP1 和 Hyper-V 时启用 Controller 到单个 Hyper-V 计算机的 身份验证凭据安全支持提供程序 (CredSSP)。有关详细信息，请参阅 CTX137465。

使用标准 PowerShell V3 远程会话，HCL 可使用 CredSSP 打开与 Hyper-V 计算机的连接。此功能可将 Kerberos 加密的用户凭据传递到 Hyper-V 计算机，并在使用所提供的凭据（本例中指 VMM 用户的凭据）运行的远程 Hyper-V 计算机上的此会话中传递 PowerShell 命令，以便存储的通信命令正确运行。

以下任务使用的 PowerShell 脚本源于 HCL，随后将被发送到 Hyper-V 计算机以作用于 SMB 3.0 存储。

- **合并主映像** - 主映像可创建新的 MCS 置备方案（计算机目录）。它将克隆并展平主 VM，以便准备好从新创建的磁盘创建新 VM（并删除对初始主 VM 的依赖）。
  ConvertVirtualHardDisk 位于 root\virtualization\v2 命名空间

  示例：
  ```
  $ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
  $result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)
  $result
  ```
- **创建差异磁盘** - 从合并主映像时产生的主映像创建差异磁盘。差异磁盘随后将连接到新 VM。
  CreateVirtualHardDisk 位于 root\virtualization\v2 命名空间

  示例：
  ```
  $ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
  $result = $ims.CreateVirtualHardDisk($vhdastext);
  $result
  ```
- **上载身份磁盘** - HCL 不能直接将身份磁盘上载到 SMB 存储。因此，Hyper-V 计算机必须将身份磁盘上载并复制到该存储。由于 Hyper-V 计算机无法从 Controller 中读取磁盘，因此 HCL 必须首先通过 Hyper-V 计算机复制身份磁盘，如下所述。
  1. HCL 通过管理员共享将身份上载到 Hyper-V 计算机。
  2. Hyper-V 计算机通过 PowerShell 远程会话中运行的 PowerShell 脚本将磁盘复制到 SMB 存储。将在 Hyper-V 计算机上创建一个文件夹，此文件夹的权限已锁定，仅 VMM 用户有权访问（通过远程 PowerShell 连接）。
  3. HCL 删除管理员共享中的文件。
  4. HCL 完成身份磁盘到 Hyper-V 计算机的上载后，远程 PowerShell 会话可将身份磁盘复制到 SMB 存储，然后将其从 Hyper-V 计算机中删除。
     如果删除了身份磁盘文件夹，将重新创建以便重复使用。

- **下载身份磁盘** - 与上载一样，身份磁盘通过 Hyper-V 计算机传递到 HCL。以下过程将在 Hyper-V 服务器上创建一个仅 VMM 用户有权访问的文件夹（如果尚不存在）。
  1. Hyper-V 计算机通过 PowerShell V3 远程会话中运行的 PowerShell 脚本将磁盘从 SMB 存储复制到本地 Hyper-V 存储。
  2. HCL 将 Hyper-V 计算机管理员共享中的磁盘读取到内存。

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

3. HCL 删除管理员共享中的文件。

- **创建个人虚拟磁盘** - 如果管理员在个人虚拟磁盘计算机目录中创建 VM，则必须创建一个空磁盘 (PvD)。
  创建空磁盘的调用无需直接访问存储。如果您所具有的 PvD 磁盘与主磁盘或操作系统磁盘位于不同的存储，请使用远程 PowerShell 在与创建的 VM 具有相同名称的目录文件夹中创建 PvD 磁盘。对于 CSV 或 LocalStorage，请勿使用远程 PowerShell。在创建空磁盘之前创该建目录可避免 VMM 命令失败。

  对于 Hyper-V 计算机，请在存储上执行 mkdir。

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

VMware 虚拟化环境

Dec 05, 2017

如果您使用 VMware 提供虚拟机，请按本指导操作。

安装 vCenter Server 以及相应的管理工具。（不支持 vSphere vCenter 链接模式操作。）

如果您计划使用 MCS，请勿在 vCenter Server 中禁用数据存储浏览器功能（如 https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2101567 中所述）。如果禁用此功能，MCS 无法正常工作。

所需权限

使用下面列出的一组或所有权限创建一个 VMware 用户帐户和一个或多个 VMware 角色。基于各用户权限所需的特定级别精细度进行角色创建，以随时请求各种 XenApp 或 XenDesktop 操作。如果要随时授予用户特定权限，请至少在数据中心级别将他们与各自的角色关联。

下表显示了 XenApp 与 XenDesktop 操作间的映射关系，以及所需的最低 VMware 权限。

添加连接和资源

SDK	**用户界面**
System.Anonymous、System.Read 和 System.View	自动添加。可以使用内置的只读角色。

置备计算机（计算机创建服务）

SDK	**用户界面**
Datastore.AllocateSpace	数据存储 > 分配空间
Datastore.Browse	数据存储 > 浏览数据存储
Datastore.FileManagement	数据存储 > 低级别文件操作
Network.Assign	网络 > 分配网络
Resource.AssignVMToPool	资源 > 将虚拟机分配到资源池
VirtualMachine.Config.AddExistingDisk	虚拟机 > 配置 > 添加现有磁盘

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

VirtualMachine.Config.AddNewDisk	虚拟机 > 配置 > 添加新磁盘
VirtualMachine.Config.AdvancedConfig	虚拟机 > 配置 > 高级
VirtualMachine.Config.RemoveDisk	虚拟机 > 配置 > 删除磁盘
VirtualMachine.Interact.PowerOff	虚拟机 > 交互 > 关闭
VirtualMachine.Interact.PowerOn	虚拟机 > 交互 > 打开
VirtualMachine.Inventory.CreateFromExisting	虚拟机 > 清单 > 从现有项创建
VirtualMachine.Inventory.Create	虚拟机 > 清单 > 新建
VirtualMachine.Inventory.Delete	虚拟机 > 清单 > 删除
VirtualMachine.Provisioning.Clone	虚拟机 > 置备 > 克隆虚拟机
VirtualMachine.State.CreateSnapshot	vSphere 5.0 Update 2 和 vSphere 5.1 Update 1：虚拟机 > 状态 > 创建快照 vSphere 5.5：虚拟机 > 快照管理 > 创建快照

如果希望标记您创建的 VM，请为用户帐户添加以下权限：

SDK	**用户界面**
Global.ManageCustomFields	全局 > 管理自定义属性
Global.SetCustomField	全局 > 设置自定义属性

要确保使用干净的基础映像创建新 VM，请标记使用 Machine Creation Services 创建的 VM，以将其从可用作基础映像的 VM 列表中排除。

置备计算机（置备服务）

所有来自“**置备计算机（计算机创建服务）**”的权限以及：

SDK	**用户界面**
VirtualMachine.Config.AddRemoveDevice	虚拟机 > 配置 > 添加或删除设备

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

VirtualMachine.Config.CPUCount	虚拟机 > 配置 > 更改 CPU 计数
VirtualMachine.Config.Memory	虚拟机 > 配置 > 内存
VirtualMachine.Config.Settings	虚拟机 > 配置 > 设置
VirtualMachine.Provisioning.CloneTemplate	虚拟机 > 置备 > 克隆模板
VirtualMachine.Provisioning.DeployTemplate	虚拟机 > 置备 > 部署模板

电源管理

SDK	用户界面
VirtualMachine.Interact.PowerOff	虚拟机 > 交互 > 关闭
VirtualMachine.Interact.PowerOn	虚拟机 > 交互 > 打开
VirtualMachine.Interact.Reset	虚拟机 > 交互 > 重置
VirtualMachine.Interact.Suspend	虚拟机 > 交互 > 挂起

映像更新及回滚

SDK	用户界面
Datastore.AllocateSpace	数据存储 > 分配空间
Datastore.Browse	数据存储 > 浏览数据存储
Datastore.FileManagement	数据存储 > 低级别文件操作
Network.Assign	网络 > 分配网络
Resource.AssignVMToPool	资源 > 将虚拟机分配到资源池
VirtualMachine.Config.AddExistingDisk	虚拟机 > 配置 > 添加现有磁盘

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

VirtualMachine.Config.AddNewDisk	虚拟机 > 配置 > 添加新磁盘
VirtualMachine.Config.AdvancedConfig	虚拟机 > 配置 > 高级
VirtualMachine.Config.RemoveDisk	虚拟机 > 配置 > 删除磁盘
VirtualMachine.Interact.PowerOff	虚拟机 > 交互 > 关闭
VirtualMachine.Interact.PowerOn	虚拟机 > 交互 > 打开
VirtualMachine.Interact.Reset	虚拟机 > 交互 > 重置
VirtualMachine.Inventory.CreateFromExisting	虚拟机 > 清单 > 从现有项创建
VirtualMachine.Inventory.Create	虚拟机 > 清单 > 新建
VirtualMachine.Inventory.Delete	虚拟机 > 清单 > 删除
VirtualMachine.Provisioning.Clone	虚拟机 > 置备 > 克隆虚拟机

删除置备的计算机

SDK	**用户界面**
Datastore.Browse	数据存储 > 浏览数据存储
Datastore.FileManagement	数据存储 > 低级别文件操作
VirtualMachine.Config.RemoveDisk	虚拟机 > 配置 > 删除磁盘
VirtualMachine.Interact.PowerOff	虚拟机 > 交互 > 关闭
VirtualMachine.Inventory.Delete	虚拟机 > 清单 > 删除

创建 AppDisk（适用于 VMware vSphere 最低版本 5.5 以及 XenApp 和 XenDesktop 最低版本 7.8）

SDK	**用户界面**

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

Datastore.AllocateSpace	数据存储 > 分配空间
Datastore.Browse	数据存储 > 浏览数据存储
Datastore.FileManagement	数据存储 > 低级别文件操作
VirtualMachine.Config.AddExistingDisk	虚拟机 > 配置 > 添加现有磁盘
VirtualMachine.Config.AddNewDisk	虚拟机 > 配置 > 添加新磁盘
VirtualMachine.Config.AdvancedConfig	虚拟机 > 配置 > 高级
VirtualMachine.Config.EditDevice	虚拟机 > 配置 > 修改设备设置
VirtualMachine.Config.RemoveDisk	虚拟机 > 配置 > 删除磁盘
VirtualMachine.Interact.PowerOff	虚拟机 > 交互 > 关闭
VirtualMachine.Interact.PowerOn	虚拟机 > 交互 > 打开

删除 AppDisk（适用于 VMware vSphere 最低版本 5.5 以及 XenApp 和 XenDesktop 最低版本 7.8）

SDK	**用户界面**
Datastore.Browse	数据存储 > 浏览数据存储
Datastore.FileManagement	数据存储 > 低级别文件操作
VirtualMachine.Config.RemoveDisk	虚拟机 > 配置 > 删除磁盘
VirtualMachine.Interact.PowerOff	虚拟机 > 交互 > 关闭

获取和导入证书

为了保护 vSphere 通信的安全，Citrix 建议您使用 HTTPS，而不使用 HTTP。HTTPS 需要数字证书。Citrix 建议您根据贵组织的安全策略使用由证书颁发机构所颁发的数字证书。

如果无法使用证书颁发机构所颁发的数字证书，而您组织的安全策略允许使用数字证书，则可以使用由 VMware 安装的自签名

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

证书。在每个 Controller 中添加 VMware vCenter 证书。请执行以下过程：

1. 将运行 vCenter Server 的计算机的完全限定域名 (FQDN) 添加到该服务器上的主机文件中，文件位于：%SystemRoot%/WINDOWS/system32/Drivers/etc/。只有当域名系统中尚不存在运行 vCenter Server 的计算机的 FQDN 时，才需要执行此步骤。
2. 使用以下任意方法获取 vCenter 证书：
   - 从 vCenter Server：
     1. 将 rui.crt 文件从 vCenter Server 复制到 Delivery Controller 上可访问的位置。
     2. 在 Controller 上，导航到导出的证书所在的位置，然后打开 rui.crt 文件。
   - 使用 Web 浏览器下载证书。如果使用 Internet Explorer，可能需要在 Internet Explorer 上单击鼠标右键，然后选择“以管理员身份运行”以下载或安装证书，具体取决于您的用户帐户。
     1. 打开 Web 浏览器，与 vCenter Server 建立安全 Web 连接，例如 https://server1.domain1.com
     2. 接受安全警告。
     3. 单击显示证书错误的地址栏。
     4. 查看证书并单击详细信息选项卡。
     5. 选择 Copy to file（复制到文件）并导出为 .CER 格式，在系统提示时提供名称。
     6. 保存导出的证书。
     7. 导航到导出的证书所在的位置，然后打开 .CER 文件。
   - 从以管理员身份运行的 Internet Explorer 中直接导入：
     1. 打开 Web 浏览器，与 vCenter Server 建立安全 Web 连接，例如 https://server1.domain1.com。
     2. 接受安全警告。
     3. 单击显示证书错误的地址栏。
     4. 查看证书。
   - 将证书导入到每个 Controller 上的证书存储中：
     1. 单击安装证书，选择本地计算机，然后单击下一步。
     2. 选择将所有证书放入以下存储，然后单击浏览。
     3. 如果使用 Windows Server 2008 R2：
        1. 选中显示物理存储复选框。
        2. 展开受信任的人员。
        3. 选择本地计算机。
        4. 单击下一步，然后单击完成。

        如果使用 Windows Server 2012、Windows Server 2012 R2 或 Windows Server 2016：

        1. 选择受信任的人员，然后单击确定。
        2. 单击下一步，然后单击完成。

   重要：如果在安装后更改 vSphere 服务器的名称，则在导入新证书前，必须在该服务器上生成新的自签名证书。

创建主 VM

使用主 VM 提供用户桌面和应用程序。在虚拟机管理程序上：

1. 在主 VM 上安装 VDA，选择用于优化桌面的选项，这样会提高性能。
2. 生成主 VM 的快照作为备份。

创建虚拟桌面

如果使用 Studio 创建 VM，而不是选择现有计算机目录，请在设置托管基础结构以创建虚拟桌面时指定以下信息。

1. 选择 VMware vSphere 主机类型。
2. 输入 vCenter SDK 访问点的地址。
3. 输入先前设置的 VMware 用户帐户的凭据，该帐户应具有创建新 VM 的权限。以 domain/username 形式指定用户名。

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

VMware SSL 指纹

VMware SSL 指纹功能解决了一个在与 VMware vSphere 虚拟机管理程序建立主机连接时经常报告的错误。以前，管理员必须在创建连接之前在站点中的 Delivery Controller 和虚拟机管理程序证书之间手动创建信任关系。而通过 VMware SSL 指纹功能，则无需手动操作：不受信任的证书的指纹存储在站点数据库中，因此，XenApp 和 XenDesktop 会始终将虚拟机管理程序视为可信任，尽管控制器不信任它们也是如此。

在 Studio 中创建 vSphere 主机连接时，可以通过一个对话框查看要连接的计算机的证书。然后，您可以选择是否信任该证书。

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

Microsoft System Center Configuration Manager 环境

Dec 05, 2017

通过这些集成选项，使用 Microsoft System Center Configuration Manager (Configuration Manager) 来管理对物理设备上的应用程序和桌面的访问的站点可以将这种用法扩展到 XenApp 或 XenDesktop。

- **Citrix Connector 7.5 for Configuration Manager 2012** – Citrix Connector 在 Configuration Manager 与 XenApp 或 XenDesktop 之间提供桥接。利用 Connector，您可以在 Configuration Manager 管理的各个物理环境与 XenApp 或 XenDesktop 管理的各个虚拟环境之间统一执行日常操作。有关 Connector 的信息，请参阅 Citrix Connector 7.5 for System Center Configuration Manager 2012。
- **Configuration Manager 唤醒代理功能** - Remote PC Access 局域网唤醒功能需要 Configuration Manager。有关详细信息，请参阅下文。
- **XenApp 和 XenDesktop 属性** - 利用 XenApp 和 XenDesktop 属性，您可以识别 Citrix 虚拟桌面以便通过 Configuration Manager 进行管理。Citrix Connector 会自动使用这些属性，但是，您也可以进行手动配置，如以下部分所述。

属性

属性可供 Microsoft System Center Configuration Manager 管理虚拟桌面之用。

在 Configuration Manager 中显示的布尔属性可能会显示为 1 或 0，而非 true 或 false。

这些属性适用于 Root\Citrix\DesktopInformation 命名空间中的 Citrix_virtualDesktopInfo 类。属性名称来源于 Windows Management Instrumentation (WMI) 提供程序。

属性	说明
AssignmentType	设置 IsAssigned 的值。有效值为： • ClientIP • ClientName • 无 • “用户”– 将 IsAssigned 设置为 True
BrokerSiteName	站点；返回的值与 HostIdentifier 相同。
DesktopCatalogName	与桌面关联的计算机目录。
DesktopGroupName	与桌面关联的交付组。
HostIdentifier	站点；返回的值与 BrokerSiteName 相同。
IsAssigned	如果为 True，则将桌面分配给用户，对于随机桌面则设置为 False。
IsMasterImage	允许有关环境的决定。例如，您可能希望在主映像而非置备的计算机上安装应用程序，尤其是当这些计算机在引导计算机上处于干净状态时。有效值为： • True：在用作主映像的 VM 上（该值在安装期间基于选项而设置）。

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

属性	说明
	• Cleared：在从该映像置备的 VM 上。
IsVirtualMachine	如果是虚拟机，则为 True；如果是物理机，则为 False。
OSChangesPersist	如果桌面操作系统映像在每次重新启动时都重置为清除状态，则为 False，否则为 True。
PersistentDataLocation	Configuration Manager 存储永久数据的位置。用户无法访问此位置。
PersonalvDiskDriveLetter	对于具有个人虚拟磁盘的桌面，是指分配给个人虚拟磁盘的驱动器盘符。
BrokerSiteName、DesktopCatalogName、DesktopGroupName、HostIdentifier	在桌面向 Controller 注册时确定；对于未完全注册的桌面，这些属性为空。

要收集属性，请在 Configuration Manager 运行硬件清单。要查看属性，请使用 Configuration Manager 资源浏览器。在这些实例中，名称可包括空格或与属性名称略不相同。例如，**BrokerSiteName** 可能会显示为 Broker Site Name。

- 配置 Configuration Manager 以便从 Citrix VDA 收集 Citrix WMI 属性
- 使用 Citrix WMI 属性创建基于查询的设备集合
- 根据 Citrix WMI 属性创建全局条件
- 使用全局条件定义应用程序部署类型要求

还可以使用 Root\ccm_vdi 命名空间中 Microsoft 类 CCM_DesktopMachine 中的 Microsoft 属性。有关详细信息，请参阅 Microsoft 文档。

Configuration Manager 和 Remote PC Access 局域网唤醒

要配置 Remote PC Access 局域网唤醒功能，在办公室 PC 机上安装 VDA 并使用 Studio 创建或更新 Remote PC Access 部署前，请完成以下操作：

- 在组织中配置 ConfigMgr 2012、2012 R2 或 2016。然后将 ConfigMgr 客户端部署到所有 Remote PC Access 计算机，从而使所安排的 SCCM 清单周期有时间运行（或在需要时强制运行一个周期）。在 Studio 中指定用来配置 ConfigMgr 连接的访问凭据必须包含该作用域中的集合以及 Remote Tools Operator 角色。
- 要支持 Intel 主动管理技术 (AMT)：
  - PC 上的最低受支持版本必须为 AMT 3.2.1。
  - 通过证书及相关置备进程置备 PC，以便使用 AMT。
  - 只能使用 ConfigMgr 2012 和 2012 R2，不能使用 ConfigMgr 2016。
- 要支持 ConfigMgr 唤醒代理和/或幻数据包功能：
  - 在每台 PC 的 BIOS 设置中配置局域网唤醒功能。
  - 要支持唤醒代理，请在 ConfigMgr 中启用该选项。对于组织中将使用 Remote PC Access 局域网唤醒功能的 PC 所属的每个子网，请确保有三台或更多的计算机可以作为标记计算机使用。
  - 要支持幻数据包功能，请将网络路由器和防火墙配置为允许使用子网定向的广播或单播发送幻数据包。

在办公室 PC 上安装 VDA 后，在 Studio 中创建 Remote PC Access 部署时，请启用或禁用电源管理。

- 如果启用电源管理，请指定详细的连接信息：ConfigMgr 地址和访问凭据以及一个连接名称。

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

- 如果不启用电源管理，可在以后添加电源管理 (Configuration Manager) 连接，然后编辑 Remote PC Access 计算机目录，以启用电源管理并指定新的电源管理连接。

可以编辑电源管理连接以配置使用 ConfigMgr 唤醒代理和幻数据包功能，以及更改数据包传输方式。

有关详细信息，请参阅 Remote PC Access。

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

Nutanix 虚拟化环境

Mar 01, 2018

在使用 Nutanix Acropolis 向您的 XenApp 或 XenDesktop 部署中提供虚拟机时，请遵循此指导。安装过程中包括以下任务：

- 在您的 XenApp 或 XenDesktop 环境中安装并注册 Nutanix 插件。
- 创建与 Nutanix Acropolis 虚拟机管理程序的连接。
- 创建一个将使用您在 Nutanix 虚拟机管理程序上创建的主映像的快照的计算机目录。

有关详细信息，请参阅可从 Nutanix 支持门户网站获取的《Nutanix Acropolix MCS 插件安装指南》：https://portal.nutanix.com。

有关 Nutanix 和 Provisioning Services 的支持信息，请参阅知识中心文章 CTX131239。

安装并注册 Nutanix 插件

在安装 XenApp 或 XenDesktop 组件后，请在 Delivery Controller 上完成以下步骤来安装并注册 Nutanix 插件。然后，即可使用 Studio 创建与 Nutanix 虚拟机管理程序的连接，并创建一个将使用您在 Nutanix 环境中创建的主映像的快照的计算机目录。

1. 从 Nutanix 获取 Nutanix 插件，并在 Delivery Controller 上安装此插件。
2. 验证是否已在 C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0 中创建 Nutanix Acropolis 文件夹。
3. 运行 **C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe –PluginsRoot “C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0”**.
4. 重新启动 Citrix Host Service、Citrix Broker Service 和 Citrix Machine Creation Service。
5. 运行以下 PowerShell cmdlet 以验证是否已注册 Nutanix Acropolis 插件：

    Add-PSSnapin Citrix*
    Get-HypHypervisorPlugin

创建与 Nutanix 的连接

请参阅文章创建站点和连接和资源，了解用于创建连接的向导中的所有页面的完整信息。

在“站点设置”或“添加连接和资源”向导中的**连接**页上选择 **Nutanix** 连接类型，然后指定虚拟机管理程序的地址和凭据以及连接名称。在**网络**页上，选择用于托管单元的网络。

使用 Nutanix 快照创建计算机目录

此信息用于补充创建计算机目录一文中的指导信息。此信息仅描述特定于 Nutanix 的字段。

您所选的快照是将用于创建计算机目录中的虚拟机的模板。在创建计算机目录之前，请在 Nutanix 中创建映像和快照。

- 有关主映像的常规信息，请参阅“创建计算机目录”一文。

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

- 关于用于创建映像和快照的 Nutanix 程序的信息，请参阅上面提到的 Nutanix 文档。

操作系统和**计算机管理**页面不包含特定于 Nutanix 的信息。请遵循“创建计算机目录”一文中的指导信息。

在**容器**页（特定于 Nutanix）上，选择将用于放置虚拟机的磁盘的容器。

在**主映像**页面上，选择映像快照。Acropolis 快照名称的前缀必须为“XD_”，才能在 XenApp 和 XenDesktop 中使用。如果需要，使用 Acropolis 控制台重命名快照。如果重命名快照，则重新启动“创建目录”向导以查看刷新的列表。

在**虚拟机**页面上，指示虚拟 CPU 数量和每个 vCPU 的核心数。

网卡、**计算机帐户**和**摘要**页面中不包含特定于 Nutanix 的信息。请遵循“创建计算机目录”一文中的指导信息。

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

安装核心组件

Dec 05, 2017

核心组件包括 Delivery Controller、Studio、Director、StoreFront 和许可证服务器。

重要：开始安装之前，请查看准备安装。此外，开始安装之前请查看本文。

本文介绍了安装核心组件时的安装向导顺序。提供了命令行等效命令。有关详细信息，请参阅使用命令行安装。

步骤 1. 下载产品软件并启动向导

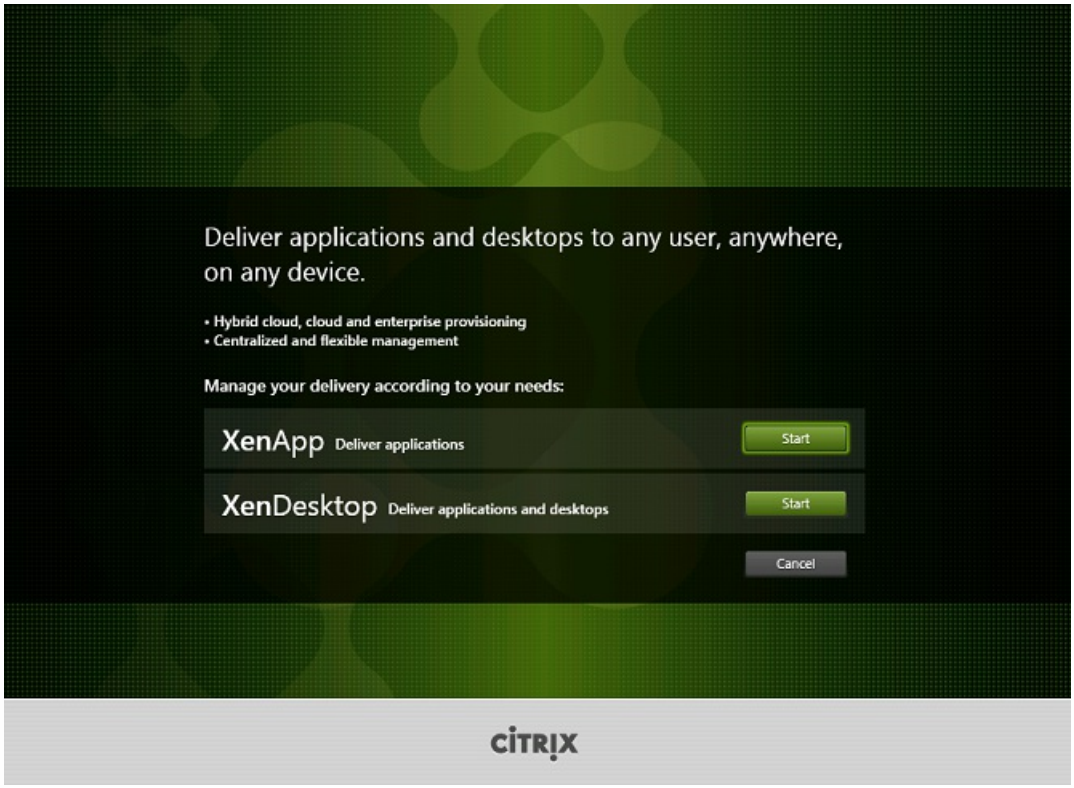
使用您的 Citrix 帐户凭据访问 XenApp 和 XenDesktop 下载页面。下载产品 ISO 文件。

解压文件。或者刻录 ISO 文件的 DVD。

使用本地管理员帐户，登录要在其中安装核心组件的计算机。

在驱动器中插入 DVD 或装载 ISO 文件。如果安装程序未自动启动，请双击 **AutoSelect** 应用程序或已装载的驱动器。

步骤 2. 选择要安装的产品



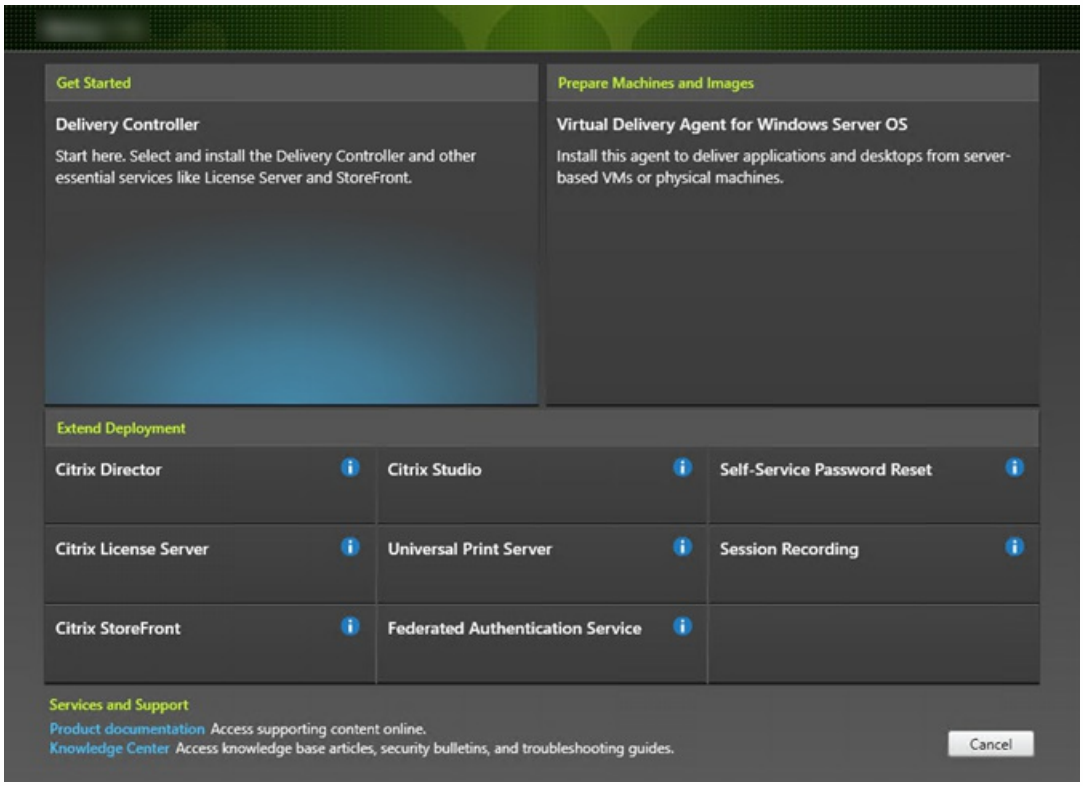
单击产品旁边的**开始**安装：XenApp 或 XenDesktop。

（如果计算机上已安装了 XenApp 或 XenDesktop 组件，此页面不会显示。）

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

命令行选项：/xenapp 用于安装 XenApp；如果忽略选项，则安装 XenDesktop

步骤 3. 选择要安装的内容



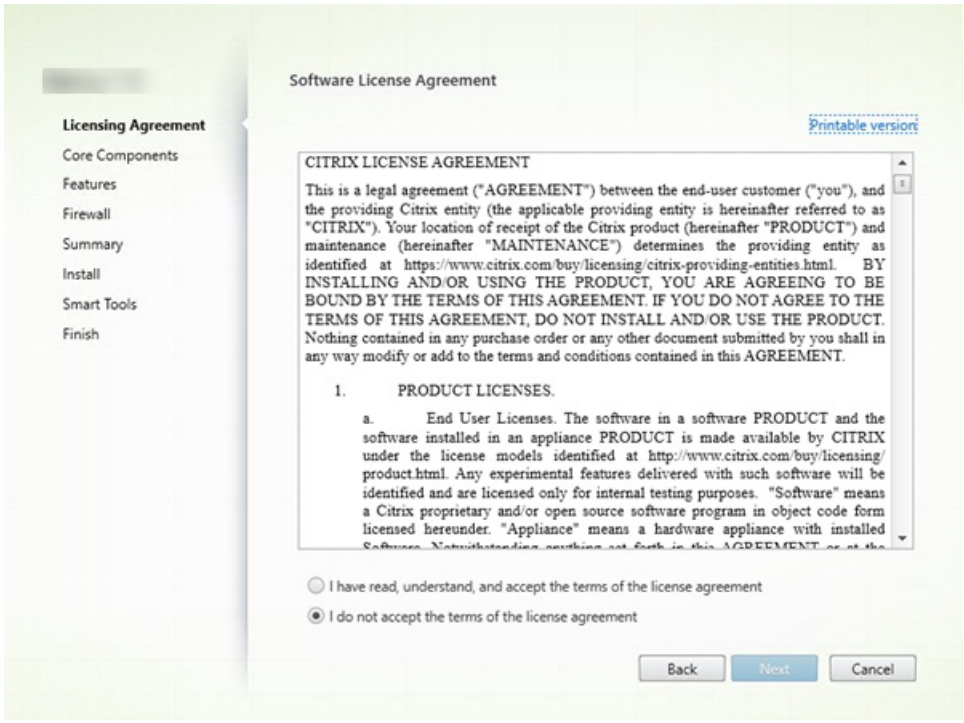
如果刚刚开始安装，请选择 **Delivery Controller**。（在下一页上，您将选择要在此计算机上安装的特定组件。）

如果您已安装 Controller（在此计算机或另一台计算机上）并要安装其他组件，请从“扩展部署”部分选择组件。

命令行选项：/components

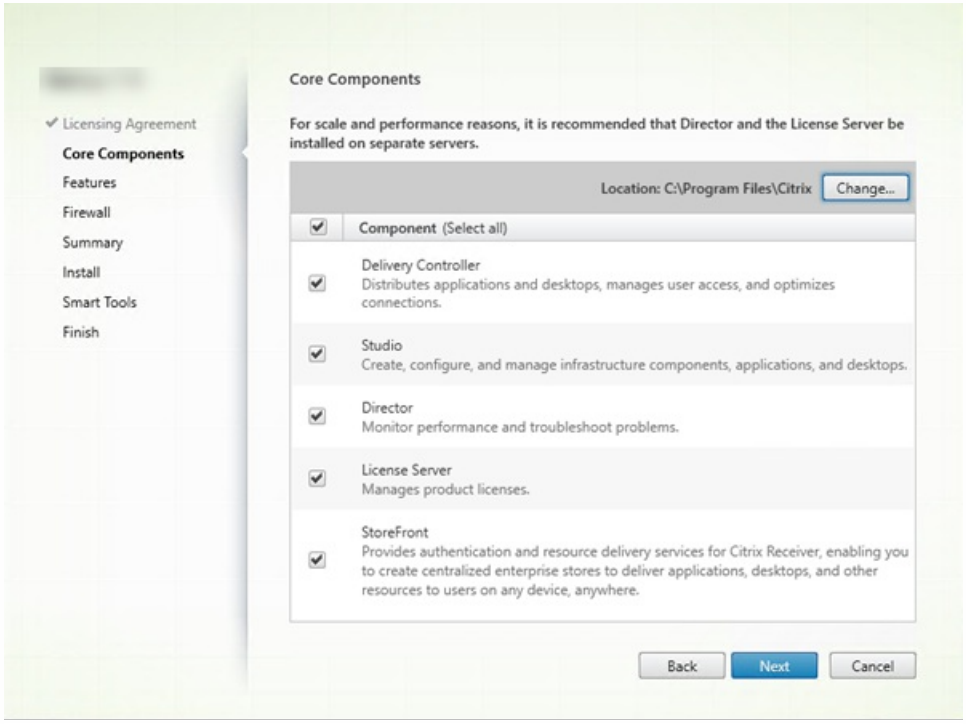
步骤 4. 阅读并接受许可协议

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



在**许可协议**页面上，阅读许可协议后，指明您已阅读并接受它。然后，单击**下一步**。

步骤 5. 选择要安装的组件及安装位置



在**核心组件**页面上：

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

- **位置**：默认情况下，组件安装在 C:\Program Files\Citrix 中。该默认设置适用于大多数部署。如果您指定一个不同的位置，它必须具有网络服务的执行权限。
- **组件**：默认情况下，所有核心组件对应的复选框都处于选中状态。在一个服务器上安装所有核心组件适用于概念验证、测试或小型生产部署。对于大型生产环境，Citrix 建议在单独的服务器上安装 Director、StoreFront 和许可证服务器。

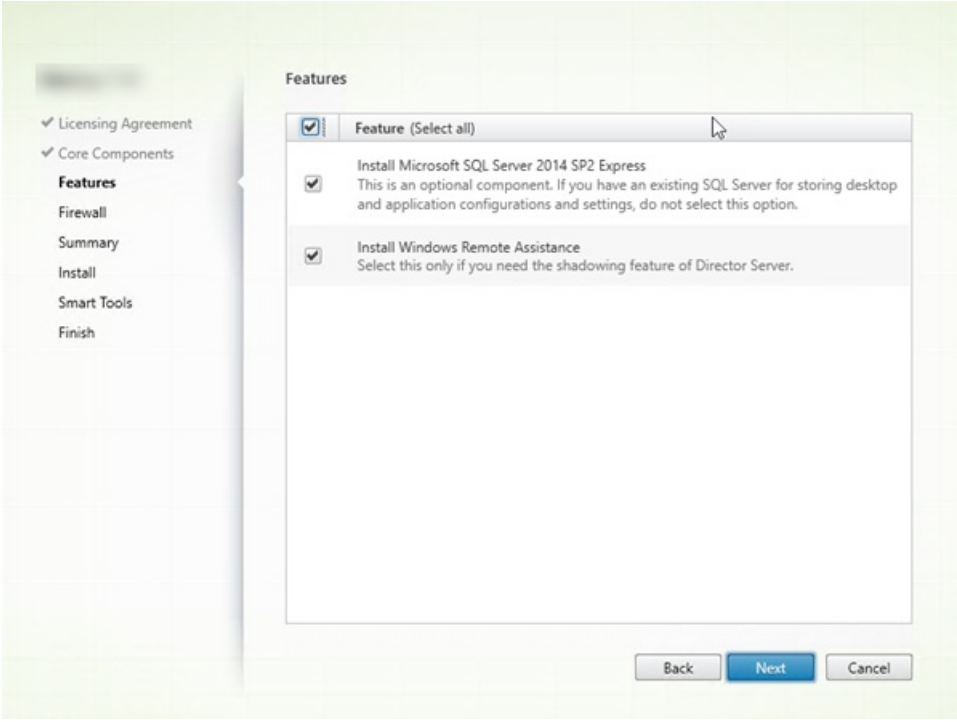
  仅选择要在此计算机上安装的组件。（在此计算机上安装了组件后，可以在其他计算机上重新运行安装程序以安装其他组件。）

  您选择不在此计算机上安装某个必需的核心组件时，系统会显示图标警报。该警报提醒您安装该组件，尽管不一定在此计算机上。

单击**下一步**。

命令行选项：/installdir、/components、/exclude

步骤 6. 启用或禁用功能



在**功能**页面上：

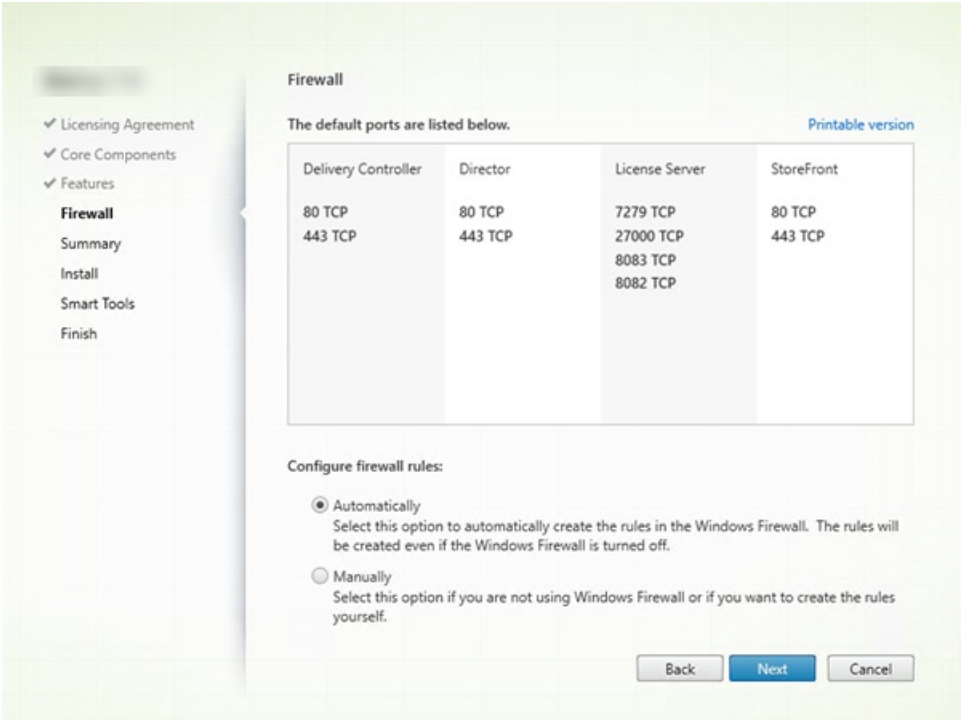
- 选择是否安装 Microsoft SQL Server Express 以用作站点数据库。默认情况下，启用此选择。如果您不熟悉 XenApp 和 XenDesktop 数据库，请查看数据库。
- 安装 Director 时，自动安装 Windows 远程协助。您选择是否在 Windows 远程协助中启用重影以与 Director 用户重影结合使用。启用重影将打开 TCP 端口 3389。默认情况下，启用此功能。该默认设置适用于大多数部署。此功能仅当安装 Director 时才会显示。

单击**下一步**。

命令行选项：/nosql（用于阻止安装）、/no_remote_assistance（用于阻止启用）

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

步骤 7. 自动打开 Windows 防火墙端口



默认情况下，如果 Windows 防火墙服务正在运行，那么即使未启用防火墙，**防火墙**页面上的端口也会自动打开。该默认设置适用于大多数部署。有关端口信息，请参阅网络端口。

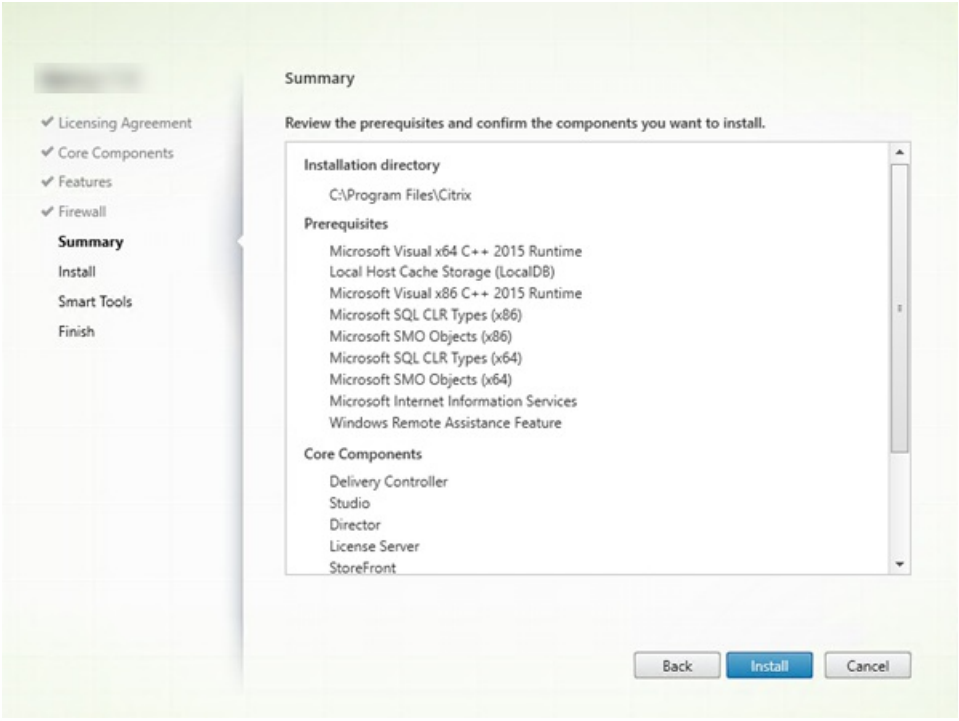
单击**下一步**。

（图中显示您在此计算机上安装所有核心组件时的端口列表。这种类型的安装通常仅用于测试部署。）

命令行选项：/configure_firewall

步骤 8. 查看必备条件并确认安装

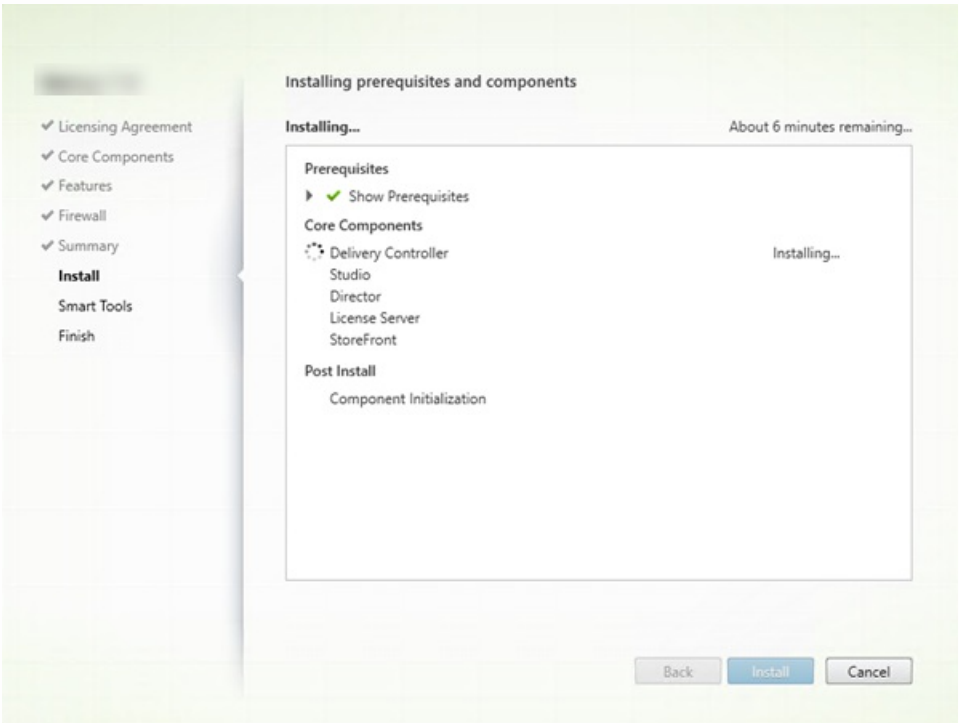
© 1999-2017 Citrix Systems, Inc. All rights reserved.



摘要页面上列出将安装的内容。如果需要，可使用“返回”按钮返回到之前的向导页面并更改选择。

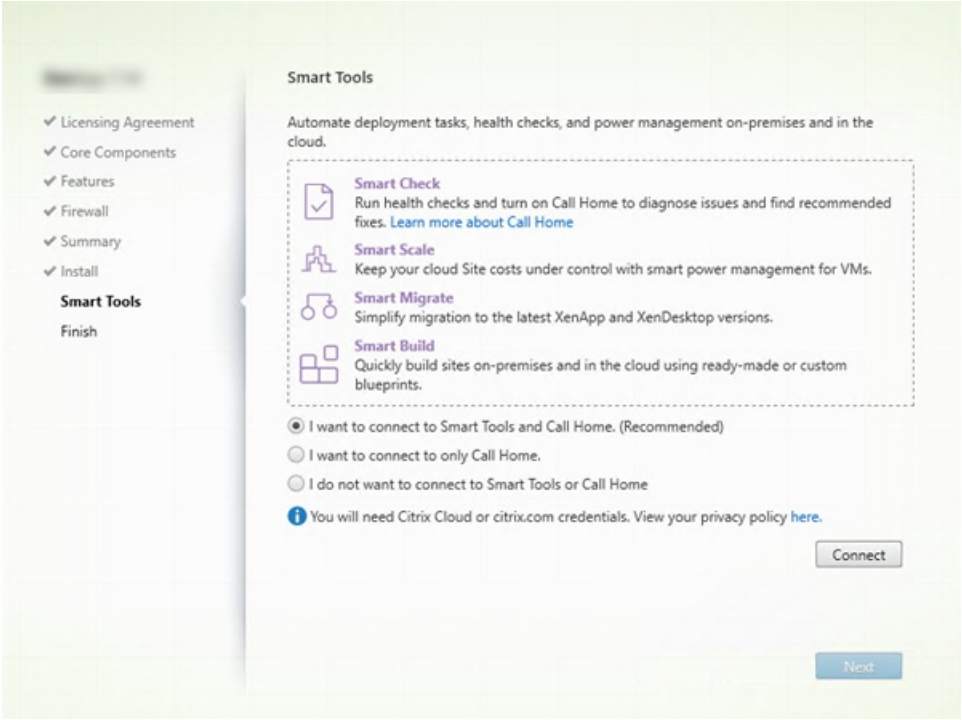
准备好时，单击**安装**。

系统将显示安装进度：



步骤 9. 连接到 Smart Tools 和 Call Home

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



安装或升级 Delivery Controller 时，Smart Agent 页面提供多个选项：

- 启用与 Smart Tools 和 Call Home 的连接。这是建议的选择。
- 启用与 Call Home 的连接。在升级过程中，如果已启用 Call Home 或如果安装程序遇到与 Citrix Telemetry Service 有关的错误，则不会显示此选项。
- 不启用与 Smart Tools 或 Call Home 的连接。

如果安装 StoreFront（而非 Controller），向导将显示 **Smart Tools** 页面。如果您安装其他核心组件（但不安装 Controller 和 StoreFront），则向导将不显示 **Smart Tools** 和 **Call Home** 页面。

如果您选择用于启用与 Smart Tools 和/或 Call Home 的连接的选项：

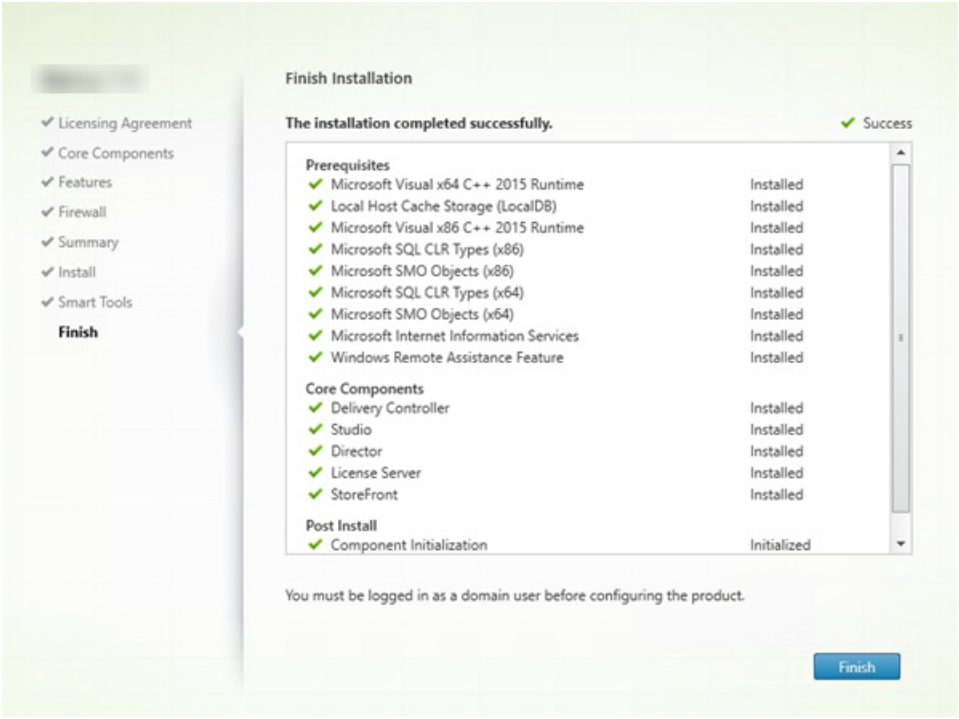
1. 单击**连接**。
2. 提供您的 Citrix 或 Citrix Cloud 凭据。
3. 验证了您的凭据后，该过程将下载 Smart Agent 证书。成功完成后，**连接**按钮旁边将显示绿色的复选标记。如果在此过程中出现错误，请更改您的参与选择（更改为“我不想...”）。您可以在以后注册。
4. 单击**下一步**以继续执行安装向导。

如果您选择不参与，请单击**下一步**。

命令行选项：/exclude "Smart Tools Agent"（用于阻止安装）

步骤 10. 完成此安装

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



完成页面上显示带绿色复选标记的所有已成功安装和初始化的必备条件和组件。

单击**完成**。

步骤 11：在其他计算机上安装其余核心组件

如果您在一台计算机上安装了所有核心组件，请继续执行后续步骤。否则，请在其他计算机上运行安装程序以安装其他核心组件。还可以在其他服务器上安装更多 Controller。

后续步骤

安装了所有必需的核心组件后，使用 Studio 创建站点。

创建了站点后，安装 VDA。

随时可以使用完整产品安装程序以采用以下组件扩展您的部署：

- 通用打印服务器的服务器组件：在打印服务器上启动安装程序。在“扩展部署”部分中选择**通用打印服务器**。接受许可协议，然后继续前进到向导结束。没有要指定或选择的任何其他内容。要从命令行安装此组件，请参阅使用命令行安装。
- 联合身份验证服务：请参阅联合身份验证服务。
- 自助服务密码重置服务：请参阅自助服务密码重置服务文档。

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

安装 VDA

Dec 05, 2017

适用于 Windows 计算机的 VDA 有两种类型：VDA for Server OS 和 VDA for Desktop OS。（有关适用于 Linux 计算机的 VDA 的信息，请参阅 Linux Virtual Delivery Agent 文档。）

重要：开始安装之前，请查看准备安装。例如，计算机应安装最新的 Windows 更新。如果所需的更新不存在（例如 KB2919355），安装将失败。

开始安装 VDA 之前，您应该已经安装了核心组件。您还可以在安装 VDA 之前创建站点。

本文介绍了安装 VDA 时的安装向导顺序。提供了命令行等效命令。有关详细信息，请参阅使用命令行安装。

步骤 1. 下载产品软件并启动向导

如果您要使用完整产品安装程序：

- 如果您尚未下载 XenApp 和 XenDesktop ISO：
  - 使用您的 Citrix 帐户凭据访问 XenApp 和 XenDesktop 下载页面。下载产品 ISO 文件。
  - 解压文件。或者刻录 ISO 文件的 DVD。
- 在您要安装 VDA 的映像或计算机上使用本地管理员帐户。在驱动器中插入 DVD 或装载 ISO 文件。如果安装程序未自动启动，请双击 **AutoSelect** 应用程序或已装载的驱动器。
- 将启动安装向导。

如果您要使用独立的安装程序：

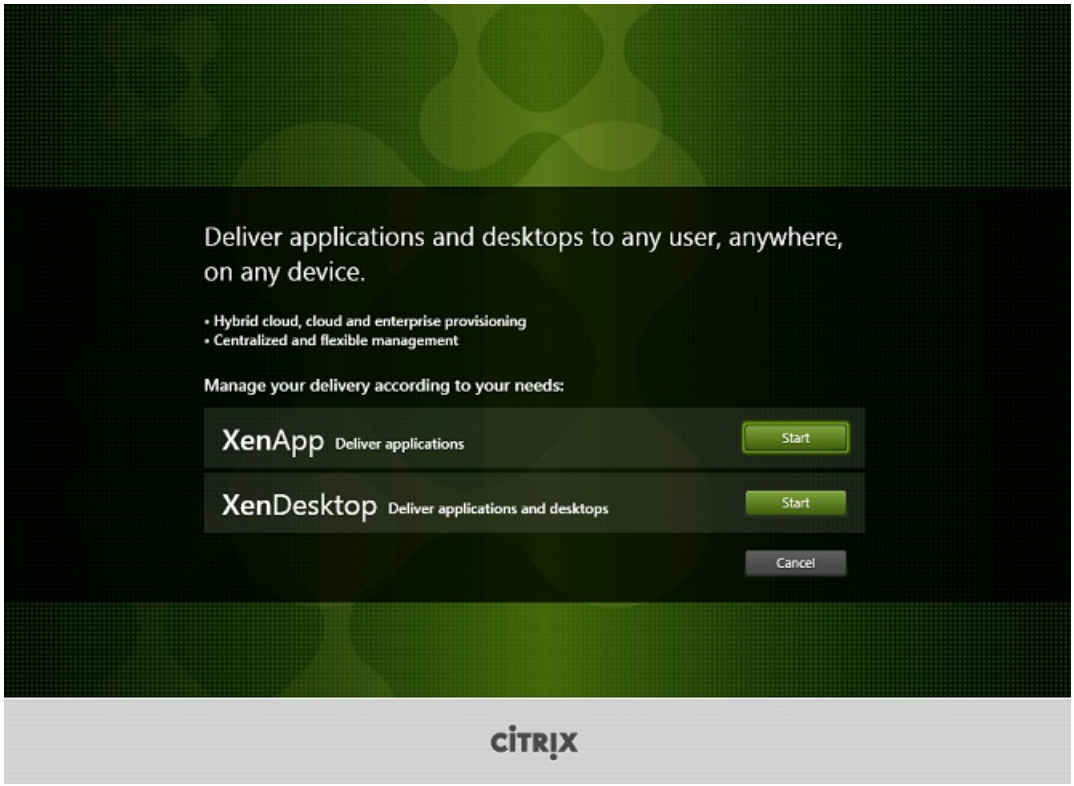
- 使用您的 Citrix 帐户凭据访问 XenApp 和 XenDesktop 下载页面。下载合适的软件包：

下载页面上的组件名称	**安装程序文件名**
Server OS Virtual Delivery Agent <*version*>	VDAServerSetup.exe
Desktop OS Virtual Delivery Agent <*version*>	VDAWorkstationSetup.exe
Desktop OS Core Services Virtual Delivery Agent <*version*>	VDAWorkstationCoreSetup.exe

- 右键单击下载的软件包，然后选择**以管理员身份运行**。
- 将启动安装向导。

步骤 2. 选择要安装的产品

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

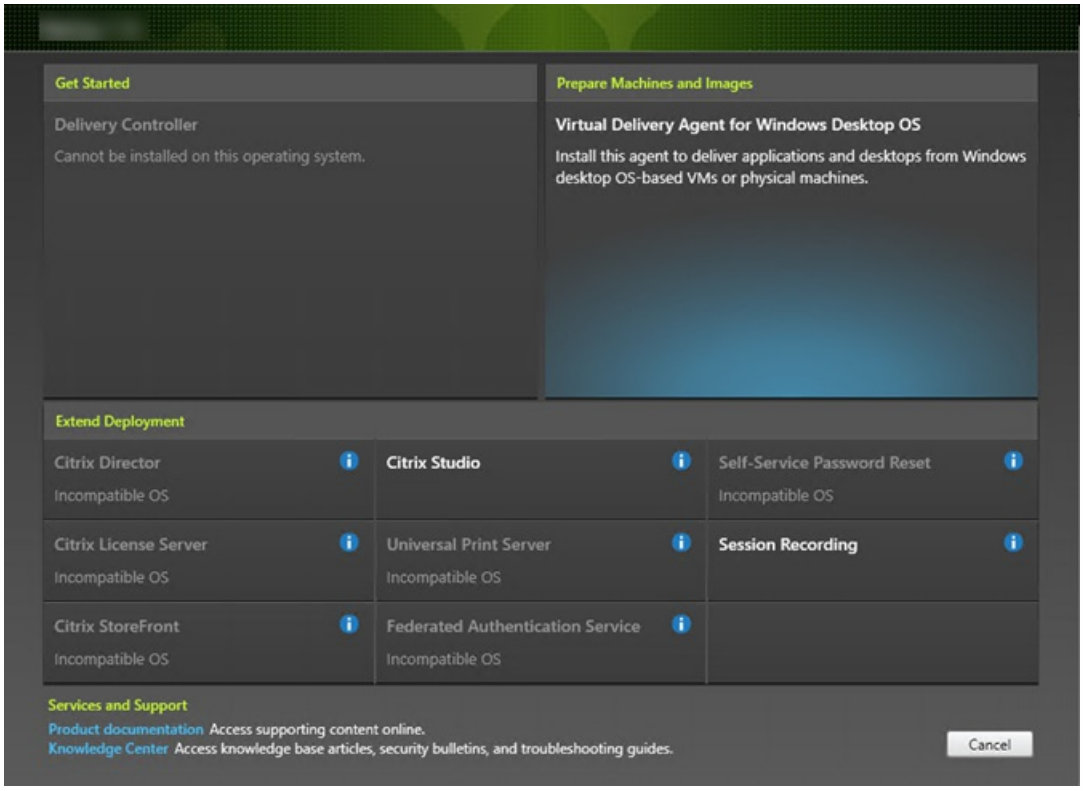


单击产品旁边的**开始**安装：XenApp 或 XenDesktop。（如果计算机上已安装了 XenApp 或 XenDesktop 组件，此页面不会显示。）

命令行选项：/xenapp 用于安装 XenApp；如果忽略选项，则安装 XenDesktop

步骤 3. 选择 VDA

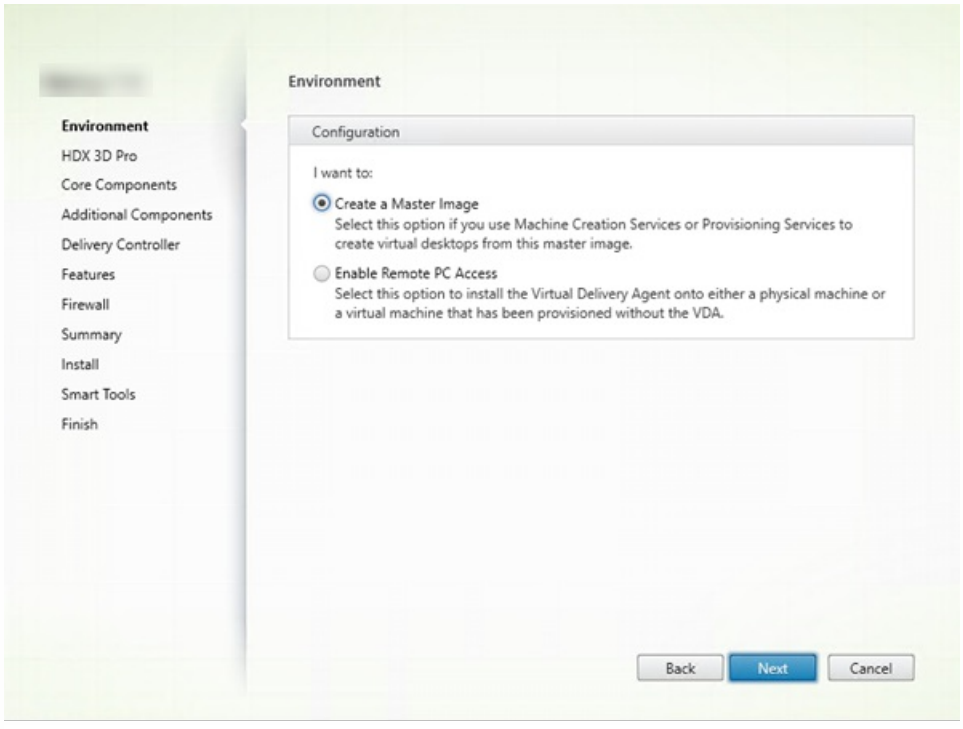
© 1999-2017 Citrix Systems, Inc. All rights reserved.



选择 Virtual Delivery Agent 条目。安装程序知晓自身是在桌面还是服务器操作系统中运行，因此仅提供恰当的 VDA 类型。

例如，在 Windows 10 计算机上运行安装程序时，会提供 VDA for Desktop OS 选项。而不会提供 VDA for Server OS 选项。

步骤 4. 指定 VDA 的使用方式



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

在**环境**页面上，指定您计划如何使用 VDA。选择以下方法之一：

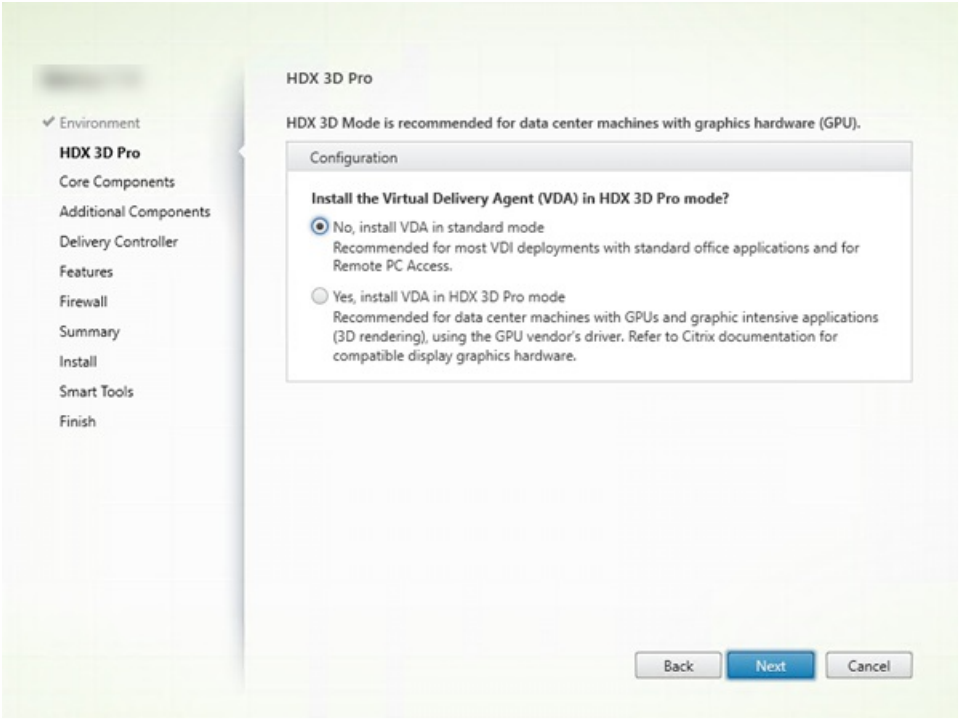
- **主映像：** （默认）在计算机映像上安装 VDA。计划使用 Citrix 工具（Machine Creation Services 或 Provisioning Services）从该主映像创建 VM。
- **启用与服务器计算机的连接**（如果要在服务器上安装）或 **Remote PC Access**（如果要在桌面计算机上安装）：您要在物理机或所置备的不包含 VDA 的 VM 上安装 VDA。如果选择“Remote PC Access”选项，则不安装/启用以下组件：
  - App-V
  - Profile Management
  - Machine Identify Service
  - Personal vDisk

单击**下一步**。

命令行选项：/masterimage、/remotepc

如果使用 VDAWorkstationCoreSetup.exe 安装程序，则此页面将不显示在向导中，且命令行选项无效。

步骤 5. 选择是否启用 HDX 3D Pro 模式



HDX 3D Pro 页面仅在安装 VDA for Desktop OS 时显示。

- 建议为大部分桌面选择标准 VDA，包括启用了 Microsoft RemoteFX 的桌面。标准 VDA 模式是默认设置。
- HDX 3D Pro VDA 模式优化了图形密集型程序和富媒体应用程序的性能。如果计算机访问图形处理器以进行 3D 渲染，建议选择 HDX 3D Pro VDA 模式。
- 对于 Remote PC Access，通常 VDA 配置为标准 VDA 模式。对于配置了 HDX 3D Pro 的 Remote PC Access，可通过以下方面支持显示器消隐功能

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

- Intel Iris Pro 图形和 Intel HD 图形 5300 及更高版本（第 5 代 Intel 酷睿处理器和第 6 代 Intel 酷睿 i5 处理器）
- NVIDIA Quadro 和 NVIDIA GRID GPU
- AMD RapidFire

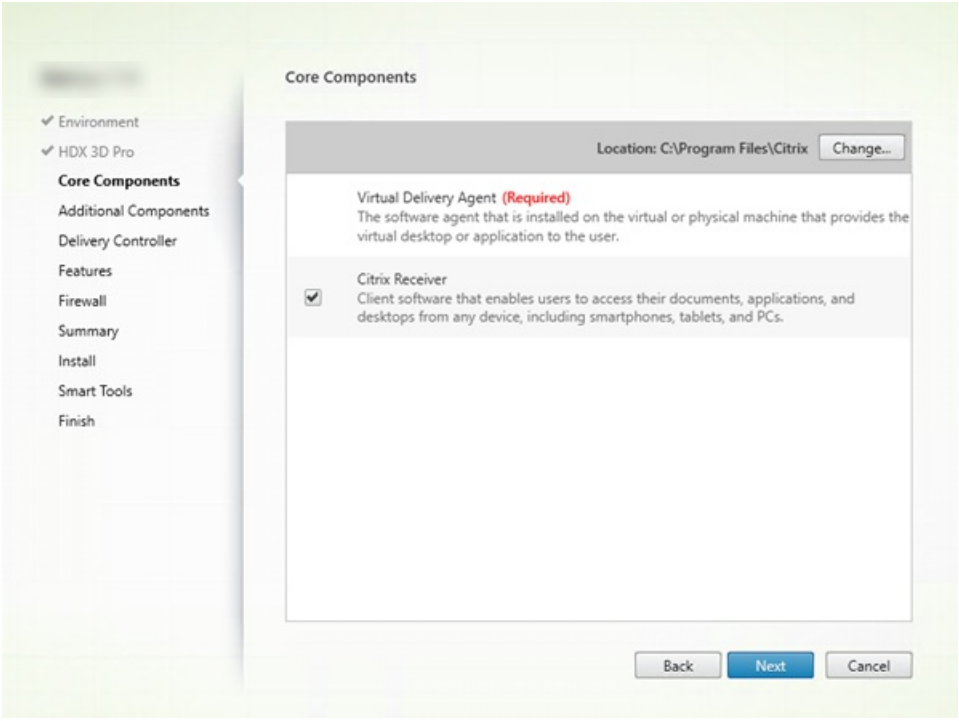
标准模式	**HDX 3D Pro 模式**
通常最适合于不带图形硬件加速功能的虚拟桌面以及 Remote PC Access。	通常最适合于带图形硬件加速功能的数据中心桌面，需使用四个以上显示器的情况除外。
任何 GPU 均可用于 Remote PC Access，但会有一些应用兼容性限制： • 在 Windows 7、8 和 8.1 上，DirectX 的 GPU 加速功能级别最高为 9.3。如果一些 DirectX 10、11、12 应用程序不支持回退到 DirectX 9，则这些应用程序可能无法运行。 • 在 Windows 10 上，为窗口化的 DirectX 10、11 和 12 应用程序提供了 GPU 加速。DX 9 应用程序由 WARP 呈现。DX 应用程序无法用于全屏模式。 • 远程会话中的 OpenGL 应用程序加速功能（如果受 GPU 供应商支持；目前仅限于 NVIDIA）。	支持通过任何 GPU 实现 GPU 加速功能。但控制台消隐、非标准屏幕分辨率和真正多显示器支持功能要求使用 NVIDIA GRID、Intel Iris Pro 或 AMD RapidFire 图形。 利用显卡供应商提供的驱动程序实现最广泛的应用程序兼容性： • 受 GPU 支持的所有 3D API（DirectX 或 OpenGL）。 • 通过 Intel Iris Pro（仅适用于 Win10）、NVIDIA GRID 和 AMD RapidFire 支持全屏 3D 应用程序。 • 支持自定义驱动程序扩展和 API。例如，CUDA 或 OpenCL。
任意显示器分辨率（由 Windows OS 和性能来决定限制）以及最多 8 个显示器。	最多支持四个显示器。
H.264 硬件编码适用于 Intel Iris Pro 图形处理器。	H.264 硬件编码适用于 Intel Iris Pro 图形处理器和 NVIDIA 卡。

单击**下一步**。

命令行选项：/enable_hdx_3d_pro

步骤 6. 选择要安装的组件及安装位置

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



在**核心组件**页面上：

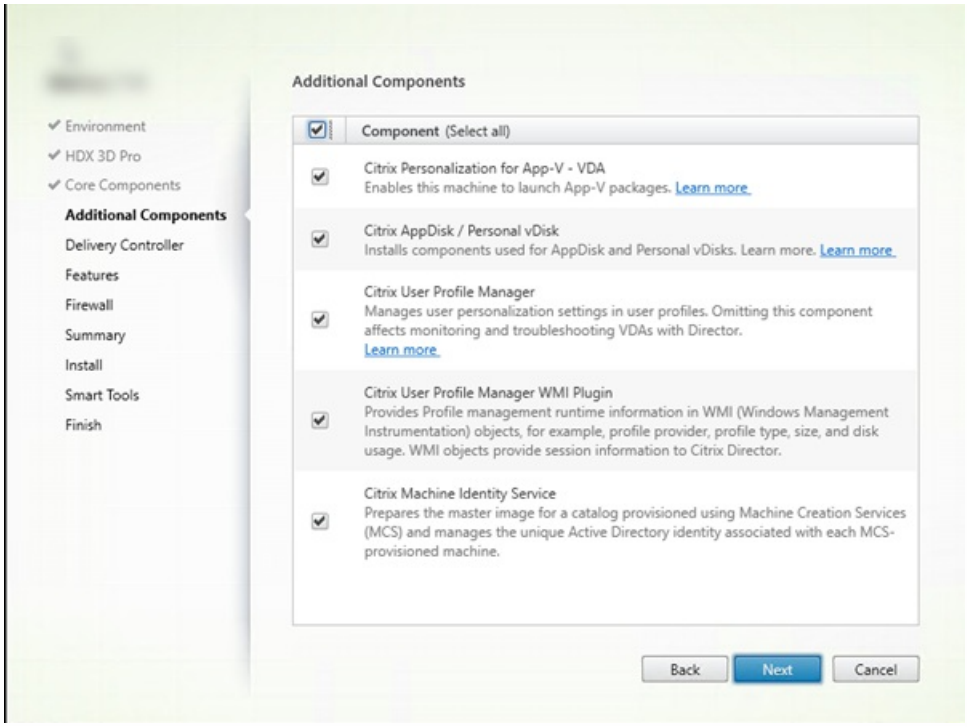
- **位置：** 默认情况下，组件安装在 C:\Program Files\Citrix 中。此默认设置适用于大多数部署。如果您指定一个不同的位置，该位置必须具有网络服务的执行权限。
- **组件：** 默认情况下，Citrix Receiver for Windows 与 VDA 一起安装（除非您使用 VDAWorkstationCoreSetup.exe 安装程序）。如果您不希望安装 Citrix Receiver，请清除复选框。如果您使用 VDAWorkstationCoreSetup.exe 安装程序，则从不安装 Citrix Receiver for Windows，因此此复选框不显示。

单击**下一步**。

命令行选项：使用 /installdir、"/components vda" 可阻止安装 Citrix Receiver for Windows

步骤 7. 安装其他组件

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



其他组件页面包含用于启用或禁用与 VDA 一起安装其他功能和技术的复选框。此页面在以下情况下不显示：

- 您使用的是 VDAWorkstationCoreSetup.exe 安装程序。此外，其他组件的命令行选项对该安装程序无效。
- 您要升级 VDA 并且所有其他组件都已安装。（如果已安装部分其他组件，此页面将仅列出未安装的组件。）

Citrix Personalization for App-V：

如果使用 Microsoft App-V 软件包中的应用程序，请安装此组件。有关详细信息，请参阅 App-V。

命令行选项 /exclude "Citrix Personalization for App-V – VDA" 阻止安装组件

Citrix AppDisk/Personal vDisk：

仅当在 VM 上安装 VDA for Desktop OS 时有效。安装用于 AppDisk 和 Personal vDisk 的组件。有关详细信息，请参阅 AppDisk 和 Personal vDisk。

命令行选项 /exclude "Personal vDisk" 阻止安装 AppDisk 和 Personal vDisk 组件

Citrix Profile Management：

此组件管理用户配置文件中的用户个性化设置。有关详细信息，请参阅 Profile Management。

将 Citrix Profile Management 排除在安装之外将影响通过 Citrix Director 对 VDA 执行的监视和故障排除操作。在“用户详细信息”和“端点”页面上，“个性化”面板和“登录持续时间”面板会出现故障。在“控制板”和“趋势”页面上，“平均登录时间”面板仅显示安装了 Profile Management 的计算机的数据。

即使您使用的是第三方用户配置文件管理解决方案，Citrix 仍建议您安装并运行 Citrix Profile Management Service。不需要启用 Citrix Profile Management Service。

命令行选项 /exclude "Citrix User Profile Manager" 阻止安装组件

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

Citrix Profile Management WMI 插件：

此插件在 WMI (Windows Management Instrumentation) 对象中提供 Profile Management 运行时信息（例如，配置文件提供程序、配置文件类型、大小和磁盘使用情况）。WMI 对象向 Director 提供会话信息。

命令行选项 /exclude "Citrix User Profile Manager WMI Plugin" 阻止组件安装

Citrix Machine Identity Service：

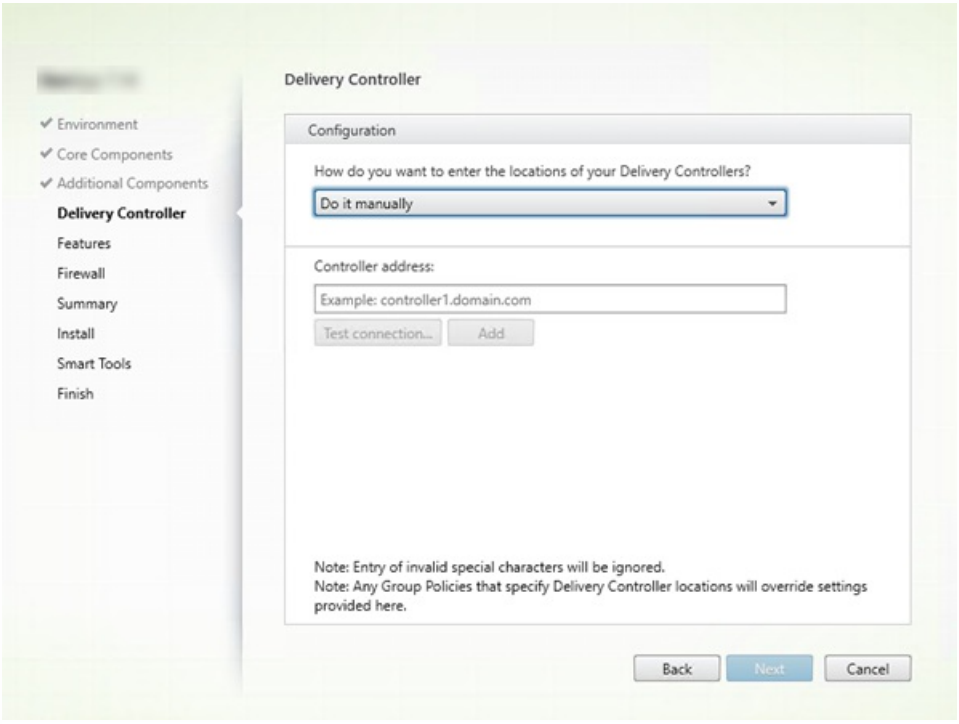
此服务为 MCS 置备的目录准备主映像。该服务还管理置备的每台计算机的唯一 Active Directory 标识。

命令行选项 /exclude "Machine Identity Service" 阻止安装组件

图形界面中的默认值：

- 如果在**环境**页面上选择“创建主映像”（步骤 4），则默认启用**其他组件**页面上的项目。
- 如果在**环境**页面上选择“启用 Remote PC Access”或“启用与服务器计算机的连接”，则默认禁用**其他组件**页面上的项目。

步骤 8. Delivery Controller 地址



在 **Delivery Controller** 页面上，选择您希望如何输入所安装的 Controller 的地址。Citrix 建议您在安装 VDA 时指定地址（“手动操作”）。VDA 有了此信息后才能向 Controller 注册。如果 VDA 无法注册，用户无法访问该 VDA 上的应用程序和桌面。

- **手动操作**（默认）：输入所安装 Controller 的 FQDN，然后单击**添加**。如果您已安装其他 Controller，请添加其地址。
- **以后(高级)**：如果选择此选项，向导将要求您确认那就是您在继续操作之前希望做的。要在以后指定地址，可以重新运行安装程序，或者使用 Citrix 组策略。向导还会在**摘要**页面上提醒您。
- **从 Active Directory 中选择位置**：仅当计算机已加入域且用户是域用户时有效。
- **让 Machine Creation Services 自动创建**：仅当使用 MCS 置备计算机时有效。

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

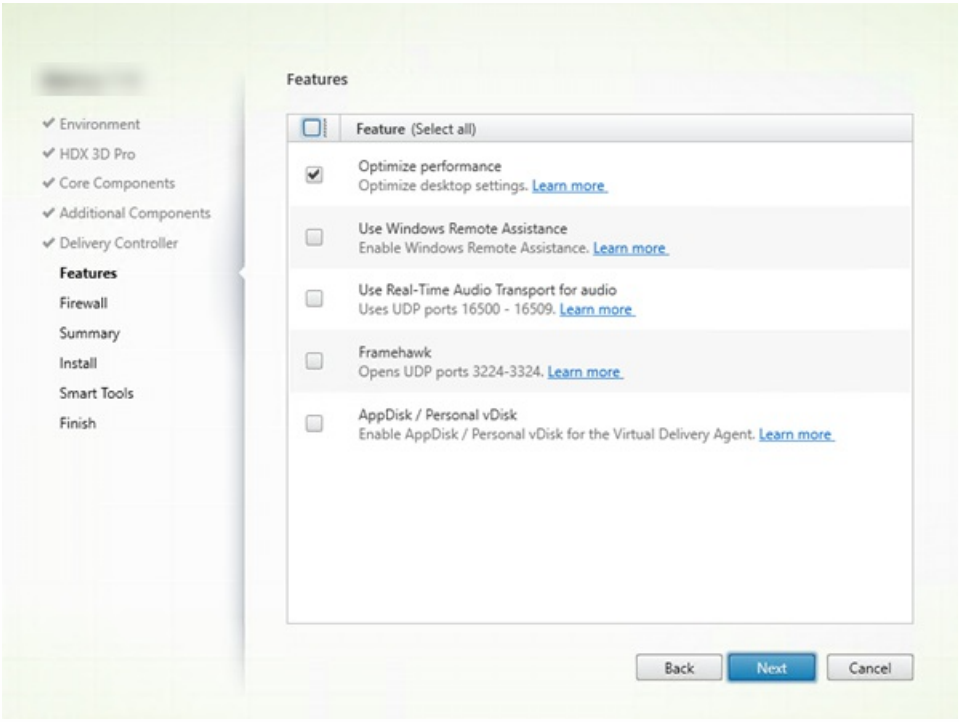
单击**下一步**。如果您选择了“以后(高级)”，系统将提示您确认将在以后指定 Controller 地址。

其他注意事项：

- 地址不能包含字符 { | } ~ [\ ] ^ ' : ; < = > ? & @ ! " # $ % ( ) + / ,
- 如果在 VDA 安装期间以及在组策略中指定了地址，这些策略设置将替代安装过程中提供的设置。
- 需要打开用于与 Controller 进行通信的防火墙端口，才能成功注册 VDA。在向导的**防火墙**页面上默认启用该操作。
- 在指定 Controller 位置（安装 VDA 期间或之后）之后，可以在添加或删除 Controller 时使用自动更新功能更新 VDA。有关 VDA 如何发现并向 Controller 注册的详细信息，请参阅 Delivery Controller。

命令行选项：/controllers

步骤 9. 启用或禁用功能



在**功能**页面上，使用复选框来启用或禁用要使用的功能。

优化性能：

仅在 VM（而非物理机）上安装 VDA 时有效。此功能处于启用状态时（默认），将对虚拟机管理程序上的 VM 中运行的 VDA 使用优化工具。VM 优化包括禁用脱机文件、禁用后台碎片整理，以及降低事件日志大小。有关详细信息，请参阅 CTX125874。

命令行选项：/optimize

如果使用 VDAWorkstationCoreSetup.exe 安装程序，则此功能将不显示在向导中，且命令行选项无效。如果要在 Remote PC Access 环境中使用其他安装程序，请禁用此功能。

使用 Windows 远程协助：

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

启用此功能后，Windows 远程协助与 Director 的用户重影功能结合使用。Windows 远程协助将在防火墙中打开动态端口。（默认禁用）

命令行选项：/enable_remote_assistance

对音频使用实时音频传输：

如果在您的网络中广泛使用 VoIP，则启用此功能。该功能可以通过有损网络降低延迟并提高音频恢复能力。它允许使用基于 UDP 的 RTP 传输功能传输音频数据。（默认禁用）

命令行选项：/enable_real_time_transport

Framehawk：

如果启用了此功能，则会打开双向 UDP 端口 3224-3324。（默认禁用）

可以在以后使用“Framehawk 显示通道端口范围”Citrix 策略设置更改端口范围。然后必须打开本地防火墙端口。必须在任何内部（VDA 至 Citrix Receiver 或 NetScaler Gateway）和外部（NetScaler Gateway 至 Citrix Receiver）防火墙上打开 UDP 网络路径。如果部署了 NetScaler Gateway，则会使用 DTLS（默认 UDP 端口 443）来加密 Framehawk 数据报。有关详细信息，请参阅 Framehawk 一文。

命令行选项：/enable_framehawk_port

AppDisk/Personal vDisk：

仅当在 VM 上安装 VDA for Desktop OS 时有效。仅当在**其他组件**页面上选择了“Citrix AppDisk/Personal vDisk”时，此复选框才可用。启用了此复选框时，可以使用 AppDisk 和 Personal vDisk。有关详细信息，请参阅 AppDisk 和 Personal vDisk。

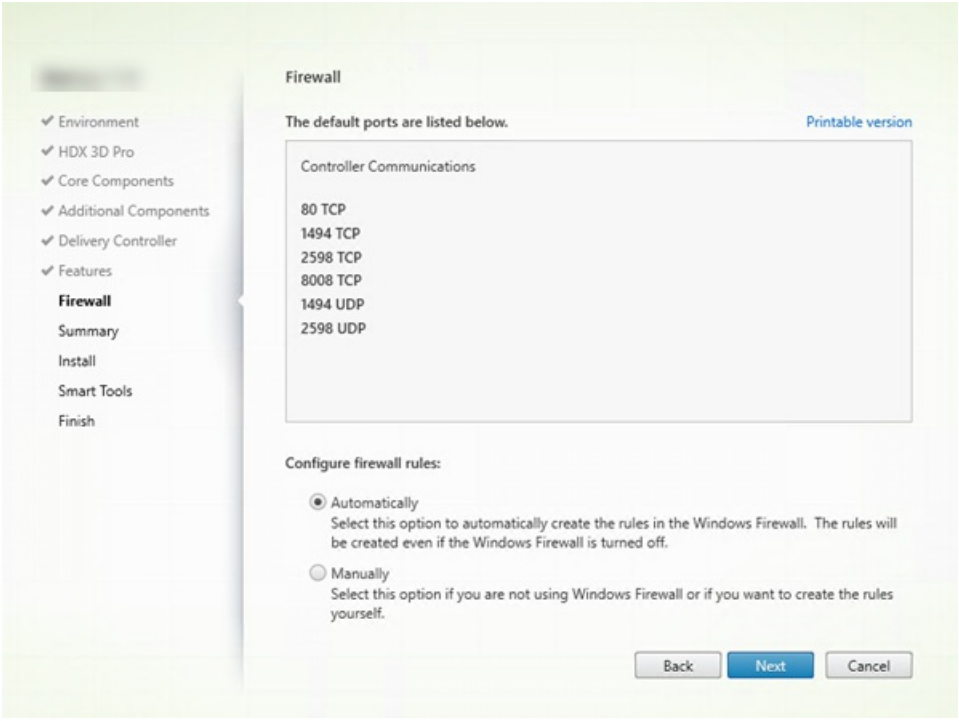
命令行选项：/baseimage

如果使用 VDAWorkstationCoreSetup.exe 安装程序，则此功能将不显示在向导中，且命令行选项无效。

单击**下一步**。

步骤 10. 防火墙端口

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



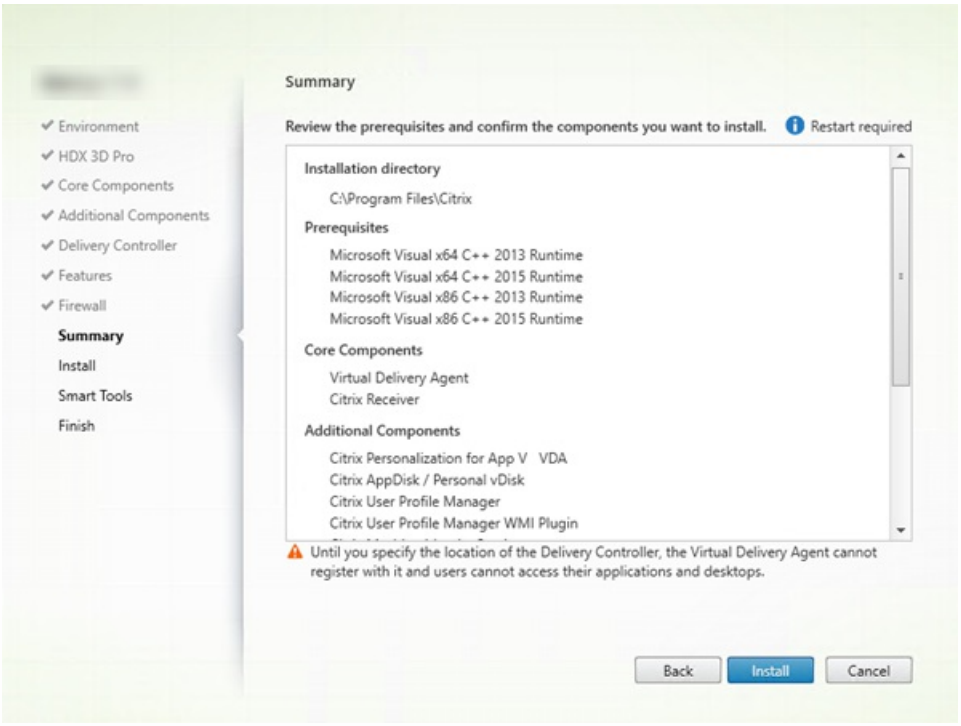
在**防火墙**页面上，默认情况下，如果 Windows 防火墙服务正在运行，那么即使未启用防火墙，也会自动打开端口。此默认设置适用于大多数部署。有关端口信息，请参阅网络端口。

单击**下一步**。

命令行选项：/enable_hdx_ports

步骤 11. 查看必备条件并确认安装

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

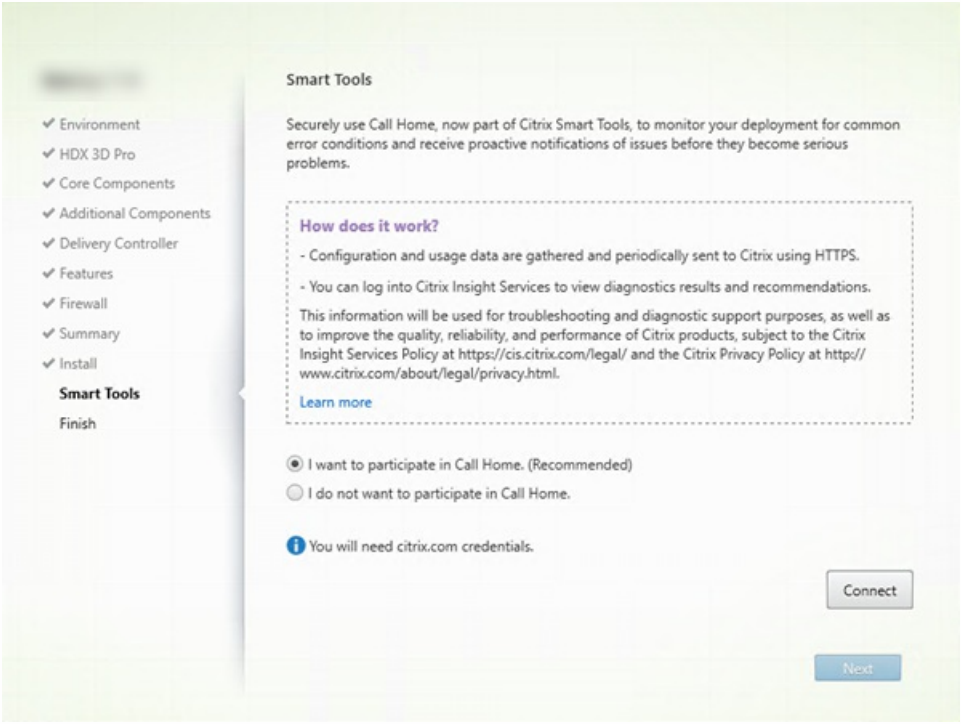


摘要页面上列出将安装的内容。可使用“返回”按钮返回到之前的向导页面并更改选择。

准备好时，单击**安装**。

如果必备项尚未安装/启用，计算机可能会重新启动一次或两次。请参阅准备安装。

步骤 12. 加入 Smart Tools

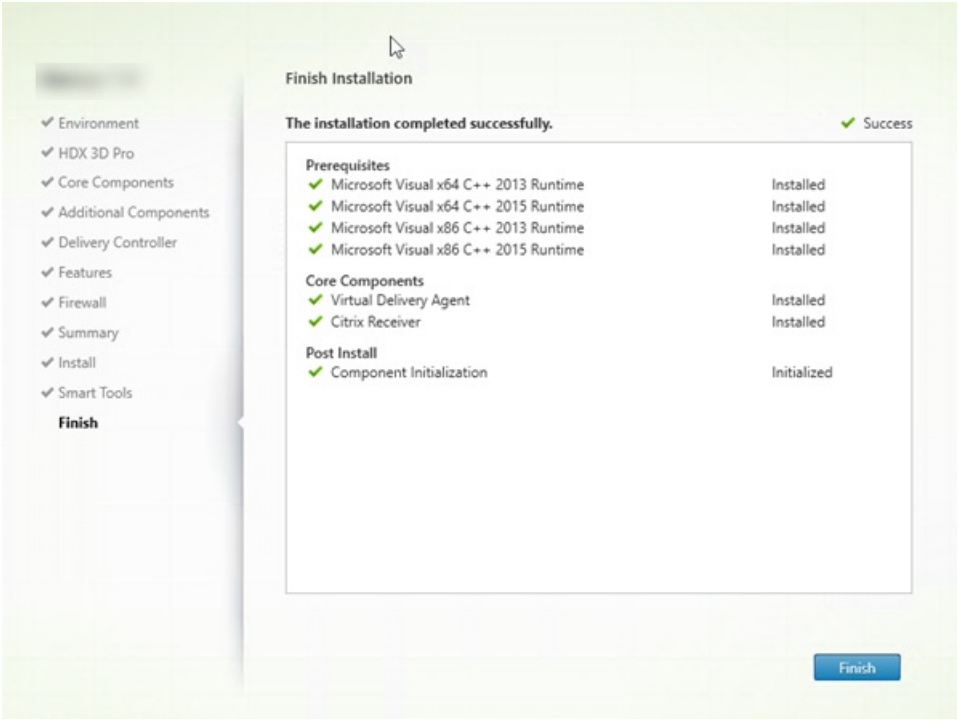


© 1999-2017 Citrix Systems, Inc. All rights reserved.

在 **Smart Tools** 页面上，选择是否参与 Citrix Call Home（现在是 Citrix Smart Tools 的一部分）。如果选择参与（默认设置），请单击**连接**。出现提示时，输入您的 Citrix 帐户凭据。

您的凭据通过验证后（或者如果选择不参与），单击**下一步**。

步骤 13. 完成此安装



完成页面上显示带绿色复选标记的所有已成功安装和初始化的必备条件和组件。

单击**完成**。默认情况下，计算机将自动重新启动。（尽管您可以禁用此自动重新启动，但在计算机重新启动之前，无法使用 VDA。）

下一步：安装其他 VDA 并继续进行配置

重复上述步骤在其他计算机或映像上安装 VDA（如果需要）。

安装了所有 VDA 后，启动 Studio。如果您尚未创建站点，Studio 将自动指导您执行该任务。完成后，Studio 将指导您创建计算机目录，然后创建交付组。请参阅：

- 创建站点
- 创建计算机目录
- 创建交付组

以后，如果要自定义已安装的 VDA：

1. 从用于删除或更改程序的 Windows 功能，选择 **Citrix Virtual Delivery Agent** 或 **Citrix Remote PC Access/VDI Core**

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

Services VDA。然后单击右键并选择**更改**。

2. 选择**自定义 Virtual Delivery Agent 设置**。安装程序启动时，您可以更改：

- Controller 地址
- 向 Controller 注册的 TCP/IP 端口（默认为 80）
- 是否自动打开 Windows 防火墙端口

故障排除

如果您的部署使用 Microsoft System Center Configuration Manager，VDA 安装可能会显示为失败，退出代码为 3，即使已成功安装 VDA 亦如此。要避免显示令人产生误解的消息，可以在 CMD 脚本中打包您的安装，或更改 Configuration Manager 软件包中的成功代码。有关详细信息，请参阅论坛讨论，网址为 http://discussions.citrix.com/topic/350000-sccm-install-of-vda-71-fails-with-exit-code-3/。

在交付组的 Studio 显示屏幕中，“详细信息”窗格中的“已安装的 VDA 版本”条目可能不是计算机上安装的版本。计算机的 Windows“程序和功能”将显示实际的 VDA 会话。

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

使用命令行安装

Jan 24, 2018

本文适用于在使用 Windows 操作系统的计算机上安装组件。有关适用于 Linux 操作系统的 VDA 的信息，请参阅 Linux Virtual Delivery Agent 文档。

在本文中：

- 使用完整产品安装程序
- 使用独立的 VDA 安装程序
- 用于安装核心组件的命令行选项
- 示例：安装核心组件
- 用于安装 VDA 的命令行选项
- 示例：安装 VDA
- 使用命令行自定义 VDA
- 使用命令行安装通用打印服务器

重要：本文介绍如何发出产品安装命令。在开始进行任何安装之前，请查看准备安装一文。这篇文章提供了可用安装程序的说明。

要查看命令的执行进度和返回值，您必须是原始管理员或者使用**以管理员身份运行**。有关详细信息，请参阅 Microsoft 命令文档。

作为对直接使用安装命令的补充，产品 ISO 中提供了示例脚本，它们用于在 Active Directory 中安装、升级或删除 VDA 计算机。有关详细信息，请参阅使用脚本安装 VDA。

使用完整产品安装程序

要访问完整产品安装程序的命令行接口，请执行以下操作：

1. 请从 Citrix 下载产品软件包。需要提供 Citrix 帐户凭据才能访问下载站点。
2. 解压文件。或者刻录 ISO 文件的 DVD。
3. 通过本地管理员帐户，登录要在其中安装组件的服务器。
4. 在驱动器中插入 DVD 或装载 ISO 文件。
5. 从介质上的 \x64\XenDesktop Setup 目录，运行相应的命令。

要安装核心组件，请执行以下操作：

运行 **XenDesktopServerSetup.exe** 命令，并使用安装核心组件的命令行选项中列出的选项。

要安装 VDA，请执行以下操作：

运行 **XenDesktopVDASetup.exe** 命令，并使用安装 VDA 的命令行选项中列出的选项。

要安装通用打印服务器，请执行以下操作：

请按照使用命令行安装通用打印服务器中的指导进行操作。

要安装联合身份验证服务，请执行以下操作：

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

Citrix 建议使用图形界面。

要安装自助服务密码重置服务，请执行以下操作：

请按照自助服务密码重置服务文档中的指导进行操作。

使用独立的 VDA 安装程序

需要提供 Citrix 帐户凭据才能访问下载站点。必须在开始安装之前提升管理员权限，或使用**以管理员身份运行**。

- 从 Citrix 下载合适的软件包：

下载页面上的组件名称	安装程序文件名
Server OS Virtual Delivery Agent <*version*>	VDAServerSetup.exe
Desktop OS Virtual Delivery Agent <*version*>	VDAWorkstationSetup.exe
Desktop OS Core Services Virtual Delivery Agent <*version*>	VDAWorkstationCoreSetup.exe

- 首先将软件包中的文件提取到一个现有目录，然后运行安装命令，或者只是运行该软件包。

  要在安装之前提取文件，请使用 **/extract** 和绝对路径，例如：.\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia。（该目录必须存在。否则，提取将失败。然后，在独立的命令行中，运行包含所提取内容的目录（在上例中为 CitrixVDAInstallMedia）中的 **XenDesktopVdaSetup.exe**。请使用用于安装 VDA 的命令行选项中的有效选项。

  要运行下载的软件包，请仅运行其名称：**VDAServerSetup.exe**、**VDAWorkstationSetup.exe** 或 **VDAWorkstationCoreSetup.exe**。请使用用于安装 VDA 的命令行选项中的有效选项。

  如果您熟悉完整产品安装程序：

  请运行独立的 VDAServerSetup.exe 或 VDAWorkstationSetup.exe 安装程序，就像它是 XenDesktopVdaSetup.exe 命令一样，除了名称不同。

  VDAWorkstationCoreSetup.exe 安装程序不同，因为它支持可用于其他安装程序的一部分选项。

用于安装核心组件的命令行选项

使用 **XenDesktopServerSetup.exe** 命令安装核心组件时，以下选项有效。有关选项的更多详细信息，请参阅安装核心组件。

/components <*组件*>[,<*组件*>] ...

要安装或删除的组件的列表（以逗号分隔）。有效值为：

CONTROLLER：Controller

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

DESKTOPSTUDIO：Studio

DESKTOPDIRECTOR：Director

LICENSESERVER：Citrix 许可证服务器

STOREFRONT ：StoreFront

如果忽略此选项，将安装所有组件（如果还指定了 /remove 选项，则删除所有组件）。

/configure_firewall

如果 Windows 防火墙服务正在运行，即使该防火墙并未启用，也会在 Windows 防火墙中打开正在安装的组件使用的所有端口。如果您使用的是第三方防火墙或未使用防火墙，则必须手动打开这些端口。

/disableexperiencemetrics

防止将安装、升级或删除过程中收集的分析自动上载到 Citrix。

排除

阻止安装一个或多个逗号分隔的功能、服务或技术，两边用引号括起来。有效值为：

“本地主机缓存存储(LocalDB)”：防止安装用于本地主机缓存的数据库。此选项对是否安装 SQL Server Express 以用作站点数据库没有任何影响。

“Smart Tools Agent”：防止安装 Citrix Smart Tools Agent。

/help 或 /h

显示命令帮助。

/installdir <*directory*>

用于安装组件的现有空目录。默认为 c:\Program Files\Citrix。

/logpath <*path*>

日志文件位置。指定的文件夹必须存在。安装程序不会创建它。默认路径为 %TEMP%\Citrix\XenDesktop Installer

/no_remote_assistance

仅当安装 Director 时有效。禁用可使用 Windows 远程协助的用户重影功能。

/noreboot

防止在安装完成后重新启动。（对于大多数核心组件，默认情况下不启用重新启动。）

/nosql

阻止在即将安装 Controller 的服务器上安装 Microsoft SQL Server Express。如果忽略此选项，将安装 SQL Server Express 以用作站点数据库。（此选项对安装用于本地主机缓存的 SQL Server Express LocalDB 没有任何影响。）

/quiet 或 /passive

安装过程中不显示任何用户界面。而只能在 Windows 任务管理器中找到安装过程的证据。如果忽略此选项，将启动图形

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

界面。

/remove

删除通过 /components 选项指定的核心组件。

/removeall

删除已安装的所有核心组件。

/sendexperiencemetrics

将安装、升级或删除过程中收集的分析自动发送到 Citrix。如果忽略此选项（或指定 /disableexperiencemetrics），分析会在本地收集，但不会自动发送。

/tempdir <*directory*>

安装过程中用于保存临时文件的目录。默认路径为：c:\Windows\Temp。

/xenapp

安装 XenApp。如果忽略此选项，则安装 XenDesktop。

示例：安装核心组件

以下命令将在服务器上安装 XenDesktop 控制器、Studio、Citrix Licensing 和 SQL Server Express。组件通信所需的防火墙端口会自动打开。

\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserver /configure_firewall

以下命令将在服务器上安装 XenApp Controller、Studio 和 SQL Server Express。组件通信所需的防火墙端口会自动打开。

\x64\XenDesktop Setup\XenDesktopServerSetup.exe /xenapp /components controller,desktopstudio /configure_firewall

用于安装 VDA 的命令行选项

以下选项在以下一个或多个命令中有效：**XenDesktopVDASetup.exe**、**VDAServerSetup.exe**、**VDAWorkstationSetup.exe** 或 **VDAWorkstationCoreSetup.exe**。

/baseimage

仅当在 VM 上安装 VDA for Desktop OS 时有效。为主映像启用个人虚拟磁盘。有关详细信息，请参阅 Personal vDisk。

此选项在使用 VDAWorkstationCoreSetup.exe 安装程序时无效。

/components <*component*>[,<*component*>]

要安装或删除的组件的列表（以逗号分隔）。有效值为：

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

VDA：Virtual Delivery Agent

插件：Citrix Receiver for Windows (CitrixReceiver.exe)

例如，要安装 VDA，但不安装 Citrix Receiver，请指定 /components vda。

如果忽略此选项，将安装所有组件。

此选项在使用 VDAWorkstationCoreSetup.exe 安装程序时无效。该安装程序不能安装 Citrix Receiver。

/controllers "<*controller*> [<*controller*>] [...]"

可与 VDA 通信的 Controller 的 FQDN，以空格分隔并用引号引起。请勿同时指定 /site_guid 和 /controllers 选项。

/disableexperiencemetrics

防止将安装、升级或删除过程中收集的分析自动上载到 Citrix。

/enable_framehawk_port

打开 Framehawk 所使用的 UDP 端口。默认值：False

/enable_hdx_3d_pro

以 HDX 3D Pro 模式安装 VDA。

/enable_hdx_ports

如果检测到 Windows 防火墙服务，即使防火墙未启用，也会在 Windows 防火墙中打开 Controller 和启用的功能（Windows 远程协助除外）所需的端口。如果使用其他防火墙或未使用防火墙，则必须手动配置防火墙。有关端口信息，请参阅网络端口。

提示：要打开 HDX 自适应传输功能用于与 Controller 通信的 UDP 端口，除 /enable_hdx_ports 选项外，还请指定 /enable_hdx_udp_ports 选项。

/enable_hdx_udp_ports

如果检测到 Windows 防火墙服务，即使未启用防火墙，也请在 Windows 防火墙中打开 HDX 自适应传输功能所需的 UDP 端口。如果使用其他防火墙或未使用防火墙，则必须手动配置防火墙。有关端口信息，请参阅网络端口。

提示：要打开 VDA 用于与 Controller 和已启用的功能通信的其他端口，除 /enable_hdx_udp_ports 选项外，还请指定 /enable_hdx_ports 选项。

/enable_real_time_transport

为音频数据包（实时音频传输）启用或禁用 UDP。启用该功能可提高音频性能。如果希望在检测到 Windows 防火墙服务时自动打开 UDP 端口，请包含 /enable_hdx_ports 选项。

/enable_remote_assistance

在 Windows 远程协助中启用重影功能以与 Director 结合使用。如果指定此选项，Windows 远程协助将在防火墙中打开动态端口。

/exclude "<*component*>"[,"<*component*>"]

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

阻止安装一个或多个逗号分隔的可选组件，可选组件由引号引起。例如，在不受 MCS 管理的映像上安装或升级 VDA 不需要 Personal vDisk 或 Machine Identity Service 组件。有效值为：

Personal vDisk

Machine Identity Service

Citrix User Profile Manager

Citrix User Profile Manager WMI 插件

Citrix 通用打印客户端

Citrix Telemetry Service

Citrix Personalization for App-V - VDA

将 Citrix Profile Management 排除在安装之外（使用 /exclude "Citrix User Profile Manager" 选项）会影响通过 Citrix Director 对 VDA 执行的监视和故障排除操作。在“用户详细信息”和“端点”页面上，“个性化”面板和“登录持续时间”面板会出现故障。在“控制板”和“趋势”页面上，“平均登录时间”面板仅显示安装了 Profile Management 的计算机的数据。

即使您使用的是第三方用户配置文件管理解决方案，Citrix 仍建议您安装并运行 Citrix Profile Management Service。不需要启用 Citrix Profile Management Service。

此选项在使用 VDAWorkstationCoreSetup.exe 安装程序时无效。该安装程序会自动排除这些项目中的很多项。

/h 或 /help

显示命令帮助。

/hdxflashv2only

阻止安装 Flash 重定向旧版二进制文件以增强安全性。

此选项在图形界面中不可用。

/installdir <*directory*>

用于安装组件的现有空目录。默认为 c:\Program Files\Citrix。

/logpath <*path*>

日志文件位置。指定的文件夹必须存在。安装程序不会创建它。默认路径为 %TEMP%\Citrix\XenDesktop Installer

此选项在图形界面中不可用。

/masterimage

仅当在 VM 上安装 VDA 时有效。将 VDA 设置为主映像。

此选项在使用 VDAWorkstationCoreSetup.exe 安装程序时无效。

/no_mediafoundation_ack

确认不安装 Microsoft 媒体基础，并且多项 HDX 多媒体功能将不安装并且无法运行。如果忽略此操作，并且不安装媒体

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

基础，VDA 安装将失败。大多数受支持的 Windows 版本都已附带安装 Microsoft 媒体基础，但 N 版本例外。

/nocitrixwddm

仅在不包含 WDDM 驱动程序的 Windows 7 计算机上有效。禁用 Citrix WDDM 驱动程序的安装。

此选项在图形界面中不可用。

/nodesktopexperience

（仅在安装 VDA for Server OS 时有效。）阻止启用 Enhanced Desktop Experience 功能。此功能还受 Enhanced Desktop Experience Citrix 策略设置的控制。

/noreboot

防止在安装完成后重新启动。重新启动后，才能使用 VDA。

/noresume

默认情况下，当安装过程中需要计算机重新启动时，安装程序将在重新启动完成后自动继续运行。要覆盖默认值，请指定 /noresume。如果在自动安装过程中必须重新装载介质或者要捕获信息，这将非常有用。

/optimize

仅当在 VM 上安装 VDA 时有效。启用对虚拟机管理程序上 VM 中运行的 VDA 进行优化。VM 优化包括禁用脱机文件、禁用后台碎片整理，以及降低事件日志大小。请勿为 Remote PC Access 部署指定此选项。有关详细信息，请参阅 CTX125874。

/portnumber <*port*>

仅当指定 /reconfig 选项时有效。用于在 VDA 和 Controller 之间进行通信的端口号。先前配置的端口如果不是 80，则会被禁用。

/quiet 或 /passive

安装过程中不显示任何用户界面。只能在 Windows 任务管理器中找到安装和配置过程的证据。如果忽略此选项，将启动图形界面。

/reconfig

与 /portnumber、/controllers 或 /enable_hdx_ports 选项结合使用时，自定义先前配置的 VDA 设置。如果指定此选项时未指定 /quiet 选项，将启动用于自定义 VDA 的图形界面。

/remotepc

仅适用于 Remote PC Access 部署。不在桌面操作系统中安装以下组件：

Citrix Personalization for App-V

Citrix User Profile Manager

Citrix User Profile Manager WMI 插件

Machine Identity Service

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

Personal vDisk

此选项在使用 VDAWorkstationCoreSetup.exe 安装程序时无效。该安装程序会自动排除这些组件的安装。

/remove

删除通过 /components 选项指定的组件。

/removeall

删除已安装的所有 VDA 组件。

/sendexperiencemetrics

将安装、升级或删除过程中收集的分析自动发送到 Citrix。如果忽略此选项（或指定 /disableexperiencemetrics 选项），分析会在本地收集，但不会自动发送。

/servervdi

在支持的 Windows Server 上安装 VDA for Desktop OS。在Windows Server 上安装 VDA for Server OS 时，请忽略此选项。使用此选项前，请参阅服务器 VDI。

此选项仅适用于完整产品 VDA 安装程序。此选项在图形界面中不可用。

/site_guid <*guid*>

站点 Active Directory 组织单位 (OU) 的全局唯一标识符。使用 Active Directory 进行发现时，该标识符可将虚拟桌面与站点相关联（建议和默认的发现方法为自动更新）。站点 GUID 是 Studio 中显示的站点属性。请勿同时指定 /site_guid 和 /controllers 选项。

/tempdir <*directory*>

安装过程中用于保存临时文件的目录。默认路径为：c:\Windows\Temp。

此选项在图形界面中不可用。

/virtualmachine

仅当在 VM 上安装 VDA 时有效。通过物理机的安装程序覆盖检测功能，在安装程序中，传递给 VM 的 BIOS 信息将其显示为物理机。

此选项在图形界面中不可用。

示例：安装 VDA

使用完整产品安装程序安装 VDA：

以下命令将在 VM 的默认位置安装 VDA for Desktop OS 和 Citrix Receiver。此 VDA 将用作主映像。VDA 将首先注册到域 mydomain 中名为 Contr-Main 的服务器上的 Controller。VDA 将使用个人虚拟磁盘、优化功能以及 Windows 远程协助。

\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins /controllers "Contr-Main.mydomain.local" /enable_hdx_ports /optimize /masterimage /baseimage /enable_remote_assistance

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

使用 VDAWorkstationCoreSetup 独立安装程序安装桌面操作系统 VDA：

以下命令在桌面操作系统上安装 Core Services VDA，以用于 Remote PC Access 或 VDI 部署。不安装 Citrix Receiver 和其他非核心服务。将会指定 Controller 的地址，且 Windows 防火墙服务中的端口将自动打开。管理员将处理重新启动。

```
VDAWorkstationCoreSetup.exe /quiet /controllers "Contr-East.domain.com" /enable_hdx_ports /noreboot
```

使用命令行自定义 VDA

安装 VDA 后，可以自定义多项设置。从产品介质上的 \x64\XenDesktop Setup 目录，使用用于安装 VDA 的命令行选项中介绍的下列一个或多个选项，运行 XenDesktopVdaSetup.exe 命令。

- /reconfigure（自定义 VDA 时需要）
- /h 或 /help
- /quiet
- /noreboot
- /controllers
- /portnumber 端口
- /enable_hdx_ports

使用命令行安装通用打印服务器

在各个打印服务器上运行下列其中一个命令：

- 在支持的 32 位操作系统中：从 Citrix 安装介质上的 \x86\Universal Print Server\ 目录中，运行 **UpsServer_x86.msi**。
- 在支持的 64 位操作系统中：从 Citrix 安装介质上的 \x64\Universal Print Server\ 目录中，运行 **UpsServer_x64.msi**。

在打印服务器上安装通用打印服务器组件后，请按照置备打印机中的指南进行配置。

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

使用脚本安装 VDA

Dec 05, 2017

本文适用于在使用 Windows 操作系统的计算机上安装 VDA。有关适用于 Linux 操作系统的 VDA 的信息，请参阅 Linux Virtual Delivery Agent 文档。

安装介质中包含用于在 Active Directory 中安装、升级或删除计算机的 Virtual Delivery Agent (VDA) 的示例脚本。您也可以使用脚本来维护 Machine Creation Services 和 Provisioning Services 所使用的主映像。

所需访问权限：

- 脚本需要对 VDA 安装命令所在的网络共享拥有“所有人可读”访问权限。安装命令是完整产品 ISO 中的 XenDesktopVdaSetup.exe，或独立安装程序中的 VDAWorkstationSetup.exe 或 VDAServerSetup.exe。
- 日志记录详细信息存储在本地计算机上。要集中记录结果以供查看和分析，脚本需要对相应网络共享拥有“所有人读/写”访问权限。

要检查运行脚本的结果，请查看中央日志共享。捕获的日志包括脚本日志、安装程序日志及 MSI 安装日志。每次的安装或删除尝试都记录在带时间戳的文件夹中。文件夹标题通过前缀 PASS 或 FAIL 来指示操作结果。您可以使用标准目录搜索工具在中央日志共享中查找失败的安装或删除。这些工具提供了在目标计算机上进行本地搜索的替代方法。

重要：开始执行任何安装之前，请阅读并完成准备安装中的任务。

使用脚本安装或升级 VDA

1. 从安装介质上的 \Support\AdDeploy\ 获取示例脚本 InstallVDA.bat。Citrix 建议您先备份原始脚本，再对其进行自定义。
2. 编辑脚本：
   - 指定要安装的 VDA 的版本：SET DESIREDVERSION。例如，版本 7 可以指定为 7.0。可以在安装介质上的 ProductVersion.txt 文件中找到完整值（例如 7.0.0.3018）。但是，无需完全匹配。
   - 指定要在其中调用安装程序的网络共享。指向布局的根目录（树结构的最高点）。脚本运行时会自动调用相应的安装程序版本（32 位或 64 位）。例如：SET DEPLOYSHARE=\\fileserver1\share1。
   - 也可以指定用于存储集中式日志的网络共享位置。例如：SET LOGSHARE=\\fileserver1\log1）。
   - 按照使用命令行安装中的说明指定 VDA 配置选项。默认情况下，脚本中包含 /quiet and /noreboot 选项，并且需要这些选项：SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT。
3. 通过组策略启动脚本，将脚本分配给包含您的计算机的 OU。此 OU 应仅包含要安装 VDA 的计算机。重新启动 OU 中的计算机后，脚本在所有这些计算机上运行。VDA 安装在具有支持的操作系统的每台计算机上。

使用脚本删除 VDA

1. 从安装介质上的 \Support\AdDeploy\ 获取示例脚本 UninstallVDA.bat。Citrix 建议您先备份原始脚本，再对其进行自定义。
2. 编辑脚本。
   - 指定要删除的 VDA 的版本：SET CHECK_VDA_VERSION。例如，版本 7 可以指定为 7.0。可以在安装介质上的 ProductVersion.txt 文件中找到完整值（例如 7.0.0.3018）。但是，无需完全匹配。
   - 也可以指定用于存储集中式日志的网络共享位置。
3. 通过组策略启动脚本，将脚本分配给包含您的计算机的 OU。此 OU 应仅包含要删除 VDA 的计算机。重新启动 OU 中的计算机后，脚本在所有这些计算机上运行。将从每台计算机中删除 VDA。

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

故障排除

脚本将生成说明脚本执行进度的内部日志文件。在开始部署的几秒内，脚本会将 Kickoff_VDA_Startup_Script 日志复制到中央日志共享。您可以确认整个过程正在运行。如果此日志未按预期复制到中央日志共享，请通过检查本地计算机进一步执行故障排除。脚本将两个调试日志文件放在每台计算机上的 %temp% 文件夹中：

- Kickoff_VDA_Startup_Script_.log
- VDA_Install_ProcessLog_.log

查看这些日志以确保该脚本：

- 按预期运行。
- 正确检测目标操作系统。
- 已正确配置为指向 DEPLOYSHARE 共享的 ROOT（包含名为 AutoSelect.exe 的文件）。
- 能够对 DEPLOYSHARE 和 LOG 共享进行身份验证。

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

创建站点

Dec 05, 2017

*站点*是您为 XenApp 或 XenDesktop 部署提供的名称。它包含 Delivery Controller、其他核心组件、Virtual Delivery Agent (VDA)、主机连接、计算机目录和交付组。在安装核心组件之后创建首个计算机目录和交付组之前创建站点。

在创建站点时，您将自动注册 Citrix 客户体验改善计划 (CEIP)。CEIP 会收集匿名统计信息和使用情况信息，然后将其发送到 Citrix。大约会在您创建站点七天后将第一个数据包发送到 Citrix。您可以在创建站点之后任何时间更改您的注册。即在 Studio 导航窗格中选择**配置**和"产品支持"选项卡并按相应说明操作。有关详细信息，请访问 http://more.citrix.com/XD-CEIP。

创建站点的用户将成为完全权限管理员；有关详细信息，请参阅委派管理。

启动站点创建向导之前请查看本文。

要创建站点，请执行以下操作：

如果 Studio 尚未打开，请将其打开。系统会自动将您引导至启动"站点创建"向导的操作。向导页面包含以下配置：

站点类型和名称

其中包括两种站点类型；请选择一个：

- **应用程序和桌面交付站点**。如果选择创建应用程序和桌面交付站点，则可以进一步选择是创建完整部署站点（推荐）还是空站点。空站点仅进行部分配置，通常由高级管理员创建。
- **Remote PC Access 站点**。Remote PC Access 站点允许指定用户通过安全连接远程访问办公室 PC。

如果立即创建应用程序和桌面交付部署，可在以后添加 Remote PC Access 部署。反之，如果此时创建 Remote PC Access 部署，则可以稍后添加完整部署。

键入站点的名称。创建站点后，其名称显示在 Studio 导航窗格的顶部：**Citrix Studio** (*站点名称*)。

数据库

数据库页面包含用于设置站点数据库、监视数据库和配置日志记录数据库的选项。有关数据库设置选项和要求的详细信息，请参阅数据库。

如果选择安装要用作站点数据库的 SQL Server Express（默认设置），则在安装了该软件后将重新启动。如果选择不安装要用作站点数据库的 SQL Server Express 软件，则不重新启动。

如果不使用默认的 SQL Server Express，请确保在创建站点之前在计算机上安装 SQL Server 软件。系统要求列出了受支持的版本。

如果希望向站点添加多个 Controller，并且已在其他服务器上安装了 Controller 软件，则可以从此页面添加那些 Controller。如果打算生成用于设置数据库的脚本，请在生成脚本之前添加 Controller。

许可

请考虑是要使用现有许可证，还是使用允许您以后添加许可证文件的 30 天免费试用。您还可以从站点创建向导内部添加或下载许可证文件。有关详细信息，请参阅许可文档。

采用*名称*[*端口*]格式指定许可证服务器地址。名称必须是 FQDN、NetBIOS 或 IP 地址。建议使用 FQDN。如果忽略端口号，则默认为 27000。单击**连接**。与许可证服务器成功建立连接之后，才能继续到下一页面。

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

电源管理（仅限 Remote PC Access）

请参阅 Remote PC Access。

主机连接、网络和存储

如果使用虚拟机管理程序或云服务上的虚拟机交付应用程序和桌面，则可以选择创建相应主机的第一个连接。也可以为此连接指定存储和网络资源。创建站点后，可以修改此连接和资源，以及创建更多连接。有关详细信息，请参阅管理和资源。

连接页面：请参阅连接类型信息来源。

如果不使用虚拟机管理程序或云服务上的虚拟机（或如果您使用 Studio 管理专用刀片式 PC 上的桌面），请选择连接类型**无**。

如果要配置 Remote PC Access 站点并计划使用局域网唤醒功能，请选择 **Microsoft System Center Configuration Manager** 类型。

除了连接类型外，还可以指定是否将使用 Citrix 工具（例如 Machine Creation Services）或其他工具创建 VM。

存储和网络页面：有关存储类型和管理方法的详细信息，请参阅主机存储、存储管理和存储选择。

附加功能

您可以选择功能来自定义站点。如果选中需要提供信息的项目所对应的复选框，则会显示一个配置框。

AppDNA 集成

您使用 AppDisk 并安装了 AppDNA 时有效。通过 AppDNA 集成，允许对 AppDisk 中的应用程序进行分析。以后可以检查兼容性问题以及采取补救措施来解决这些问题。有关详细信息，请参阅 AppDisk。

App-V 发布

如果使用 App-V 服务器上 Microsoft App-V 软件包中的应用程序，请选择此功能。提供 App-V 管理服务器的 URL 以及 App-V 发布服务器的 URL 和端口号。

如果仅使用网络共享位置上 App-V 软件包中的应用程序，则无需选择此功能。

您也可以日后在 Studio 中启用/禁用和配置此功能。有关详细信息，请参阅 App-V。

Remote PC Access

有关 Remote PC Access 部署的信息，请参阅 Remote PC Access。

如果使用局域网唤醒功能，在创建站点之前，请在 Microsoft System Center Configuration Manager 上完成配置步骤。有关详细信息，请参阅 Microsoft System Center Configuration Manager。

创建 Remote PC Access 站点时：

- 如果要使用局域网唤醒功能，请在**电源管理**页面上指定 Microsoft System Center Configuration Manager 地址、凭据和连接信息。
- 在**用户**页面上指定用户或用户组。不存在自动添加所有用户的默认操作。另外，在**计算机帐户**页面上指定计算机帐户（域或 OU）信息。

  要添加用户信息，请单击**添加用户**。选择用户和用户组，然后单击**添加用户**。

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

要添加计算机帐户信息，请单击**添加计算机帐户**。选择计算机帐户，然后单击**添加计算机帐户**。单击**添加 OU**。选择域和组织单位，然后指出是否包含子文件夹中的项目。单击**添加 OU**。

创建 Remote PC Access 站点时，会自动创建名为 Remote PC User Machine Accounts 的计算机目录。该目录包含您在站点创建向导中添加的所有计算机帐户。会自动创建名为 Remote PC User Desktops 的交付组。该组包含您已添加的所有用户和用户组。

总结

站点创建向导的最后一页汇总了您指定的信息。如果要进行更改，请使用**上一步**按钮。完成后，单击**创建**，开始创建站点。

测试站点配置

要在创建站点后运行测试，请选择导航窗格顶部的 **Citrix Studio (站点***站点名称***)**。然后单击中间窗格中的**测试站点**。可以查看站点测试结果的 HTML 报告。

对于 Windows Server 2016 上安装的 Controller，站点测试功能可能会失败。当本地 SQL Server Express 用于站点数据库而 SQL Server Browser 服务未启动时会失败。为了避免此问题，请完成下列任务。

1. 启用 SQL Server Browser 服务（如有必要），然后启动该服务。
2. 重新启动 SQL Server (SQLEXPRESS) 服务。

故障排除

配置站点后，可以安装 Studio 并通过 MMC 将其添加为远程计算机上的管理单元。如果以后尝试删除该管理单元，MMC 可能停止响应。解决方法：重新启动 MMC。

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

创建计算机目录

Apr 16, 2018

物理机或虚拟机的集合作为称为计算机目录的单个实体进行管理。目录中的所有计算机具有相同的操作系统类型：服务器或桌面。包含服务器操作系统计算机的目录可以包含 Windows 计算机或 Linux 计算机，不能同时包含二者。

Studio 会在您创建站点后指导您创建第一个计算机目录。创建第一个计算机目录后，Studio 会指导您创建第一个交付组。之后，您可以更改所创建的目录，也可以创建更多目录。

概述

在您创建 VM 的目录时，要指定如何置备这些 VM。您可以使用 Citrix 工具（例如 Machine Creation Services (MCS) 或 Provisioning Services (PVS)）。也可以使用您自己的工具来提供计算机。

- 如果使用 PVS 创建计算机，请参阅 Provisioning Services 文档以了解相关说明。
- 如果使用 MCS 置备 VM，则需要提供一个主映像（或快照）以在目录中创建完全相同的 VM。创建目录之前，先使用虚拟机管理程序或云服务工具创建并配置主映像。此过程包括在该映像上安装 Virtual Delivery Agent (VDA)。然后在 Studio 中创建计算机目录。选择该映像（或某个映像的快照），指定要在目录中创建的 VM 数以及配置其他信息。
- 如果您的计算机已可用（因此您无需主映像），您仍必须为那些计算机创建一个或多个计算机目录。

使用 MCS 或 PVS 创建第一个目录时，使用创建站点时配置的主机连接。之后（创建第一个目录和交付组后），可以更改该连接的信息或创建更多连接。

完成目录创建向导之后，将自动运行测试以确保目录配置正确。测试完成后，可以查看测试报告。您可以通过 Studio 随时运行测试。

仅限本地部署：使用 MCS 或 PVS 创建第一个目录时，使用创建站点时配置的主机连接。之后（创建第一个目录和交付组后），可以更改该连接的信息或创建更多连接。

提示：如果直接使用 PowerShell SDK 创建目录，可以指定虚拟机管理程序模板 (VMTemplates)，而不是映像或快照。

VDA 注册

必须向要在启动代理会话时考虑使用的 Delivery Controller（适用于本地部署）或 Cloud Connector（适用于 Citrix Cloud 部署）注册 VDA。未注册的 VDA 会导致无法充分利用原本可用的资源。VDA 未被注册的原因有很多，其中许多情况都可由管理员进行故障排除。Studio 在目录创建向导中以及在您向交付组中添加了某个目录中的计算机之后，提供故障排除信息。

在目录创建向导中，添加现有计算机之后，计算机帐户名称列表会指示每台计算机是否都适合添加到该目录。将鼠标悬停在每个计算机旁边的图标上，以显示有关该计算机的有用消息。

如果该消息确定存在一台有问题的计算机，您可以删除该计算机（使用**删除**按钮），也可以添加计算机。例如，如果一条消息指示无法获取有关某台计算机的信息（可能因为该计算机始终未注册），您可能会选择添加计算机。

有关功能级别的消息，请参阅 VDA 版本和功能级别。

有关 VDA 注册故障排除的详细信息，请参阅 CTX136668。

MCS 目录创建摘要

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

此处简要介绍您在目录创建向导中提供信息后要执行的默认 MCS 操作。

- 如果选择了主映像（而非快照），则 MCS 会创建快照。
- MCS 创建此快照的完整副本，并将副本放在主机连接中定义的各个存储位置。
- MCS 将计算机添加到 Active Directory，Active Directory 创建唯一身份。
- MCS 创建向导中指定的 VM 数，并为每个 VM 定义两个磁盘。除每个 VM 的两个磁盘外，主映像也存储在相同的存储位置。如果定义了多个存储位置，每个磁盘位置将获得以下磁盘类型：
  - 快照的完整副本（如上所述），该副本为只读且在所创建的 VM 之间共享。
  - 唯一的 16 MB 身份磁盘，为每个 VM 提供唯一身份。每个 VM 获得身份磁盘。
  - 唯一的差异磁盘，用于存储对 VM 执行的写操作。此磁盘采用精简置备（前提是主机存储支持）并在必要时增加到主映像的最大大小。每个 VM 获得一个差异磁盘。差异磁盘保存会话期间所做的更改。对于专有桌面，此磁盘为永久磁盘。对于池桌面，每次重启时会删除此磁盘并创建一个新磁盘。

或者，在创建 VM 以交付静态桌面时，您可以指定（在目录创建向导的**计算机**页面上）胖（完整复制）VM 克隆。完整克隆不需要在每个数据存储上保留主映像。每个 VM 均有自己的文件。

在虚拟机管理程序或云服务上准备主映像

提示：有关与虚拟机管理程序和云提供程序建立连接的信息，请参阅连接和资源。

主映像包含操作系统、非虚拟化应用程序、VDA 和其他软件。

须知事项：

- 主映像可能也称为克隆映像、黄金映像、基础 VM 或基础映像。主机供应商和云服务提供商可能会使用不同的术语。
- 使用 PVS 时，可以使用主映像或物理计算机作为主目标设备。PVS 不使用 MCS，而是使用其他术语表示映像；有关详细信息，请参阅 Provisioning Services 文档。
- 确保虚拟机管理程序或云服务具有足够多的处理器、内存和存储来容纳创建的计算机数。
- 正确配置桌面和应用程序所需的硬盘空间量。因为该值以后不能更改，也不能在计算机目录中更改。
- Remote PC Access 计算机目录不使用主映像。
- 在使用 MCS 时的 Microsoft KMS 激活注意事项：如果您的部署包括采用 XenServer 6.1 或 6.2、vSphere 或 Microsoft System Center Virtual Machine Manager 主机的 7.x VDA，则无需手动重新部署 Microsoft Windows 或 Microsoft Office。如果您的部署包括采用 XenServer 6.0.2 主机的 5.x VDA，请参阅 CTX128580。
- 在主映像上安装和配置以下软件：
  - 虚拟机管理程序的集成工具（如 XenServer Tools、Hyper-V Integration Services 或 VMware 工具）。如果您忽略此步骤，应用程序和桌面可能无法正常运行。
  - VDA。Citrix 建议安装最新版本，以便访问最新功能。在主映像上安装 VDA 失败会导致目录创建失败。
  - 所需的第三方工具（例如防病毒软件或电子软件分发代理）。使用适合用户和计算机类型的设置配置服务（如更新功能）。
  - 未虚拟化的第三方应用程序。Citrix 建议对应用程序进行虚拟化。进行虚拟化后，无需在添加或重新配置应用程序后更新主映像，从而降低成本。此外，减少安装的应用程序数量还可以减小主映像硬盘的大小，从而节约存储成本。
  - 具有建议设置的 App-V 客户端（如果计划发布 App-V 应用程序）。App-V 客户端可从 Microsoft 获取。
  - 使用 MCS 时，如果要本地化 Microsoft Windows，请安装区域设置和语言包。在置备期间，如果已创建快照，则已置备的 VM 使用已安装的区域设置和语言包。

重要：如果要使用 PVS 或 MCS，请勿在主映像上运行 Sysprep。

准备主映像：

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

1. 使用虚拟机管理程序的管理工具创建主映像，然后安装操作系统以及所有服务包和更新。指定 vCPU 数。如果使用 PowerShell 创建计算机目录，还可以指定 vCPU 值。使用 Studio 创建目录时不能指定 vCPU 数。配置桌面和应用程序所需的硬盘空间量。因为该值以后不能更改，也不能在目录中更改。
2. 确保硬盘连接在设备位置 0 处。大多数标准主映像模板在默认情况下都会配置此位置，但有些自定义模板可能不配置。
3. 在主映像上安装和配置上面列出的软件。
4. 使用 PVS 时，为主目标设备中的虚拟磁盘创建一个 VHD 文件，然后再将该主目标设备加入到域中。有关详细信息，请参阅 Provisioning Services 文档。
5. 如果未使用 MCS，请将主映像加入到应用程序和桌面所属的域中。确保主映像在创建计算机的主机上可用。如果使用 MCS，则不需要将主映像加入到域中。置备的计算机已加入在目录创建向导中指定的域中。
6. Citrix 建议您创建并命名主映像的快照，以便以后能识别该快照。如果您在创建目录时指定主映像而非快照，Studio 将创建一个快照，但您无法对其进行命名。

在 XenServer 上为支持 GPU 的计算机准备主映像

使用 XenServer 托管基础结构时，支持 GPU 的计算机需要专用的主映像。这些 VM 要求使用支持 GPU 的视频卡驱动程序。应配置支持 GPU 的计算机，以使 VM 与使用 GPU 进行操作的软件结合使用。

1. 在 XenCenter 中，创建一个具有标准 VGA、网络和 vCPU 的 VM。
2. 更新 VM 配置以启用 GPU 使用（直通或 vGPU）。
3. 安装支持的操作系统并启用 RDP。
4. 安装 XenServer Tools 和 NVIDIA 驱动程序。
5. 关闭虚拟网络计算 (Virtual Network Computing, VNC) 管理控制台以优化性能，然后重新启动 VM。
6. 系统将提示您使用 RDP。使用 RDP 安装 VDA，然后重新启动 VM。
7. 或者，创建 VM 的一个快照作为其他 GPU 主映像的基线模板。
8. 使用 RDP，安装在 XenCenter 中配置并使用 GPU 功能的客户特定应用程序。

使用 Studio 创建计算机目录

启动目录创建向导之前，请查看本节以了解您需要做出的选择以及需要提供的信息。

重要：如果要使用主映像，请确保创建目录之前已在此映像上安装 VDA。

在 Studio 中：

- 如果您已创建站点但尚未创建计算机目录，Studio 会指导您进入正确的起始位置以创建目录。
- 如果您已创建目录且希望创建另一目录，请在 Studio 导航窗格中选择**计算机目录**。然后在“操作”窗格中选择**创建计算机目录**。

向导将指导您完成下述项。根据您所做的选择，您看到的向导页面可能会有所不同。

操作系统

每个目录都只包含一种类型的计算机：

- **服务器操作系统**：服务器操作系统目录提供托管共享桌面和应用程序。计算机可以在受支持的 Windows 或 Linux 操作系统版本上运行，但目录不能同时包含这两种操作系统。（参阅 Linux VDA 文档了解该操作系统的详细信息。）
- **桌面操作系统**：桌面操作系统目录提供可分配给各种不同用户的 VDI 桌面和应用程序。
- **Remote PC Access**：Remote PC Access 目录为用户提供对其物理办公桌面计算机的远程访问权限。Remote PC Access 不需要 VPN 提供安全性。

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

计算机管理

此页面不会在创建 Remote PC Access 目录时显示。

计算机管理页面指出管理计算机的方式以及用于部署计算机的工具。

选择目录中的计算机是否通过 Studio 进行电源管理。

- 计算机通过 Studio 进行电源管理或通过云环境进行置备，例如，VM 或刀片式 PC。仅在已配置了与虚拟机管理程序或云服务的连接时，此选项才可用。
- 计算机不通过 Studio 进行电源管理，例如物理机。

如果选择计算机通过 Studio 进行电源管理或通过云环境进行置备，请选择要用于创建 VM 的工具。

- **Citrix Machine Creation Services (MCS)** – 使用主映像创建和管理虚拟机。云环境中的计算机目录使用 MCS。MCS 不可用于物理机。
- **Citrix Provisioning Services (PVS)** – 将目标设备作为设备集合进行管理。从主目标设备进行映像的 PVS 虚拟磁盘交付桌面和应用程序。此选项不可用于云部署。
- **其他** – 用于管理已位于数据中心内的计算机的工具。Citrix 建议您使用 Microsoft System Center Configuration Manager 或其他第三方应用程序，以确保目录中的计算机一致。

桌面类型（桌面体验）

此页面仅在创建包含桌面操作系统计算机的目录时显示。

桌面体验页面确定每次用户登录时发生的情况。选择以下其中之一：

- 用户在每次登录时均会连接至一个新的（随机的）桌面。
- 用户每次登录时连接至同一个（静态）桌面。

如果您选择第二项并使用 PVS 来置备计算机，您可以对如何处理用户对桌面所做的更改进行配置：

- 在单独的个人虚拟磁盘上保存用户对桌面所做的更改。
- 在本地磁盘上保存用户对桌面的更改。
- 在用户注销时放弃用户更改并清除虚拟桌面。

主映像

此页面仅在使用 MCS 来创建虚拟机时显示。

选择到主机虚拟机管理程序或云服务的连接，然后选择之前创建的快照或 VM。如果创建第一个目录，唯一可用的连接是您在创建站点时配置的连接。

谨记：

- 在您使用 MCS 或 PVS 时，请勿在主映像上运行 Sysprep。
- 如果您指定主映像而非快照，Studio 将创建一个快照，但您无法为其命名。

为了能够使用最新的产品功能，请务必在主映像上安装最新的 VDA 版本。请勿更改默认的最小 VDA 选择。但是，如果您必须使用较早的 VDA 版本，请参阅 VDA 版本和功能级别。

如果选择的快照或 VM 与您之前在向导中选择的计算机管理技术不兼容，将显示错误消息。

云平台和服务环境

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

当您使用云服务或平台来托管 VM（例如 Azure Resource Manager、Azure、Nutanix 或 Amazon Web Services）时，目录创建向导可能包含其他特定于相应主机的页面。

有关详细信息，请参阅哪里可查找有关连接类型的信息。

设备集合

此页面仅在使用 PVS 创建虚拟机时显示。它显示设备集合和尚未添加至目录的设备。

选择要使用的设备集合。有关详细信息，请参阅 Provisioning Services 文档。

计算机

此页面不会在创建 Remote PC Access 目录时显示。

此页面的标题取决于您在**计算机管理**页面上选择的内容：**计算机**、**虚拟机**或 **VM 和用户**。

使用 MCS 创建计算机时：

- 指定要创建的虚拟机数。
- 选择每个虚拟机将具有的内存量（以 MB 为单位）。
- **重要：**每个创建的虚拟机会有一个硬盘。硬盘的大小在主映像中进行设置；您不能在目录中更改硬盘大小。
- 如果您已在**桌面体验**页面指出将用户对专用桌面的更改保存到单独的个人虚拟磁盘上，请指定虚拟磁盘的大小（以 GB 为单位）和驱动器盘符。
- 如果部署包含多个区域，可以为此目录选择一个区域。
- 如果您正创建静态桌面虚拟机，请选择一个虚拟机复制模式。请参阅虚拟机复制模式。
- 如果您创建的是不使用个人虚拟磁盘的随机桌面虚拟机，您可以配置一个高速缓存，使其用于每台计算机上的临时数据。请参阅配置临时数据的高速缓存。

使用 PVS 创建计算机时：

设备页列出了设备集合中您在上一个向导页面中选择的计算机。您无法在此页面上添加或删除计算机。

使用其他工具装备计算机时：

添加（或导入一列）Active Directory 计算机帐户名称。在添加/导入了某个虚拟机后可以更改该虚拟机的 Active Directory 帐户名称。如果在**桌面体验**向导页上指定了静态计算机，您可以选择性地为每个添加的虚拟机指定 Active Directory 用户名。

添加或导入名称之后，可以使用**删除**按钮从列表中删除名称，而您始终位于此向导页面上。

使用 PVS 或其他工具（但不是 MCS）：

每个添加的（或导入的，或来自 PVS 设备集合的）计算机的图标和工具提示有助于确定那些可能不适合添加到目录，或可能无法通过 Delivery Controller 注册的计算机。有关详细信息，请参阅 VDA 版本和功能级别。

虚拟机复制模式

您在**计算机**页面上指定的复制模式可决定 MCS 从主映像创建瘦（快速复制）还是胖（完整复制）克隆。（默认为瘦克隆）

- 使用快速复制克隆以实现更高效的存储用途和更快速的计算机创建。
- 使用完整复制克隆以实现更好的数据恢复和迁移支持，但在创建了计算机之后可能导致更低的 IOPS。

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

VDA 版本和功能级别

目录的功能级别控制哪些产品功能可用于目录中的计算机。要使用新产品版本中采用的功能，可能需要使用新的 VDA。通过设置功能级别，该版本（及更高版本，如果功能级别未更改）中采用的所有功能均可用于目录中的计算机。但是，具有较早 VDA 版本的目录中的计算机将无法注册。

通过使用**计算机**（或**设备**）页面底部附近的下拉列表，您可以选择会成功注册的最低 VDA 级别；这会设置目录的最低功能级别。默认情况下，会针对内部部署选择最新的功能级别。如果您遵循 Citrix 建议，始终安装和升级 VDA 和核心组件至最新版本，则无需更改此选择。但是，如果必须继续使用较早的 VDA 版本，则请选择正确的值。

> XenApp 和 XenDesktop 版本可能不包括新 VDA 版本，或者新 VDA 不影响功能级别。在这种情况下，功能级别可能指示 VDA 版本早于已安装或已升级的组件。例如，尽管 XenApp 和 XenDesktop 7.15 LTSR 包含 7.15 VDA，但默认功能级别（7.9 或更高级别）仍保持最新版本。因此，安装 7.15 LTSR 或将组件从 7.9-7.14 升级到 7.15 LTSR 后，不需要更改默认功能级别。
>
> 在 Citrix Cloud 部署中，Studio 可以使用早于最新版本的默认功能级别。

选定的功能级别会影响其上面的计算机列表。在列表中，每个条目附近的工具提示会指示计算机的 VDA 是否与该功能级别下的目录兼容。

如果每台计算机上的 VDA 不符合或超过选定的最低功能级别，则会在页面上弹出消息提示。您可以继续进行本向导，但请注意这些计算机可能无法稍后再通过 Controller 来注册。或者，您可以：

- 从列表中删除包含较早 VDA 的计算机，升级它们的 VDA，然后将它们重新添加到目录。
- 选择较低的功能级别；但是，这会阻止访问最新的产品功能。

如果因为错误的计算机类型无法将某台计算机添加到目录，也会弹出消息。例如，尝试将一台服务器添加到桌面操作系统目录，或将一台原本为随机分配创建的桌面操作系统计算机添加到静态计算机的目录。

配置用于临时数据的缓存

在虚拟机本地缓存临时数据的行为是可选行为。当使用 MCS 管理目录中的合并（而非专用）计算机时，可以在计算机上启用临时数据缓存。如果目录使用一个用于指定临时数据存储的连接，则您可以在创建目录时启用并配置临数据缓存信息。

要支持临时数据缓存，目录中每台计算机上 VDA 的版本必须至少为 7.9。

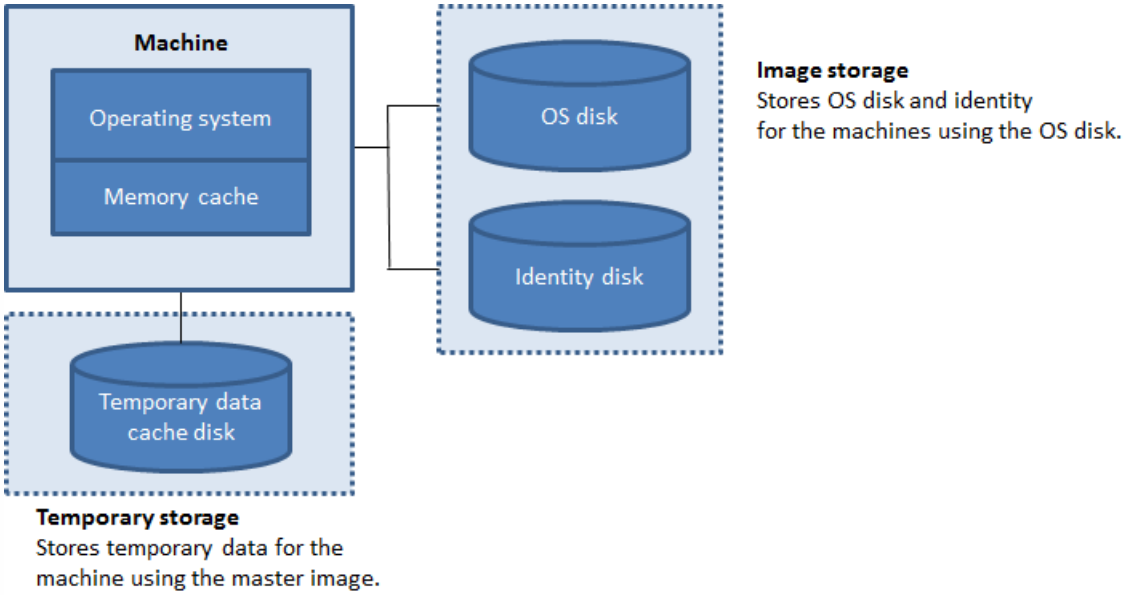
在创建目录使用的连接时，可以指定临时数据是使用共享还是使用本地存储；有关详细信息，请参阅连接和资源。在目录中启用和配置临时缓存将涉及两个复选框和值：**分配给缓存的内存(MB)** 和**磁盘缓存大小(GB)**。默认值随连接类型不同而异。通常，默认值足以满足大多数情况的要求；但是，需考虑下列项的空间要求：

- Windows 自己创建的临时数据文件（其中包括 Windows 页面文件）。
- 用户配置文件数据。
- 同步到用户的会话的 ShareFile 数据。
- 可由会话用户，或由可在会话内执行安装的任何应用程序用户创建或复制的数据。

Windows 将不允许会话使用显著大于原始主映像（已在计算机目录中从其置备计算机）上的可用空间量的缓存磁盘量。例如，如果主映像上只具有 10 GB 可用空间，则指定 20 GB 的磁盘缓存将没有意义。

如果启用**磁盘缓存大小**复选框，则临时数据最初会写入到内存缓存。当内存中缓存达到为其配置的限值（**分配给缓存的内存**值）时，最早的数据将移到临时数据缓存磁盘。

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



内存缓存是每台计算机上的总内存量的一部分；因此，如果启用**分配给缓存的内存**复选框，则可以考虑在每台计算机上增加内存总量。

如果清除**分配给缓存的内存**复选框并启用**磁盘缓存大小**复选框，则临时数据将直接写入缓存磁盘，从而仅使用最少量的内存缓存。

如果将**磁盘缓存大小**更改为除默认值外的值，可能会影响性能。此大小必须与用户需求以及计算机负载相匹配。

重要：如果磁盘缓存空间已用完，则用户的会话将变得不可用。

如果清除**磁盘缓存大小**复选框，将不会创建缓存磁盘。在这种情况下，需指定足够大的**分配给缓存的内存**值，以容纳所有临时数据；仅当具有可分配给每个虚拟机的大量 RAM 时，这才可行。

如果清除这两个复选框，则不缓存临时数据；临时数据将写入每个虚拟机的差异磁盘（位于操作系统存储中）。（这是在早于 7.9 的版本中执行的置备操作）。

如果要使用此目录创建 AppDisk，请勿启用缓存。

此功能在使用 Nutanix 主机连接时不可用。

在创建缓存值后，不能在计算机目录中更改此值。

网络接口卡 (NIC)

此页面不会在创建 Remote PC Access 目录时显示。

如果计划使用多个 NIC，请将虚拟网络与每个卡相关联。例如，可以分配一个卡用于访问特定的安全网络，另一个卡用于访问更为常用的网络。也可以从此页面添加或删除 NIC。

计算机帐户

此页面仅在创建 Remote PC Access 目录时显示。

指定要添加的对应于用户或用户组的 Active Directory 计算机帐户或组织单位 (OU)。请勿在 OU 名称中使用正斜杠 (/)。

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

您可以选择之前配置的电源管理连接，也可以选择不使用电源管理。如果要使用电源管理但尚未配置合适的连接，可以稍后创建该连接，然后编辑计算机目录以更新电源管理设置。

计算机帐户

此页面仅在使用 MCS 创建虚拟机时显示。

目录中的每台计算机都必须具有一个相应的 Active Directory 计算机帐户。指示是创建新帐户还是使用现有帐户，并指出这些帐户的位置。

- 如果要创建新帐户，则必须对计算机所在域的域管理员帐户具有访问权限。

  为将要创建的计算机指定帐户命名方案，使用哈希值标记来指示将显示连续数字或字母的位置。请勿在 OU 名称中使用正斜杠 (/)。名称不能以数字开头。例如，命名方案 PC-Sales-##（可以选择 0-9）将生成名为 PC-Sales-01、PC-Sales-02、PC-Sales-03 等的计算机帐户。

- 如果使用现有帐户，浏览到相应帐户，或单击“导入”并指定一个包含帐户名称的 .csv 文件。导入的文件内容必须使用以下格式：

  [ADComputerAccount]
  ADcomputeraccountname.domain

  ...

  确保所有要添加的计算机都有足够的帐户。由于 Studio 将管理这些帐户，因此应允许 Studio 重置所有帐户的密码或者指定帐户密码，所有帐户的密码必须相同。

对于包含物理机或现有计算机的目录，选择或导入现有帐户，并将每台计算机同时分配给 Active Directory 计算机帐户和用户帐户。

对于使用 PVS 创建的计算机，目标设备的计算机帐户的管理方式不同；请参阅 Provisioning Services 文档。

摘要、名称和描述

在向导的**摘要**页面上，检查所指定的设置。输入目录的名称和说明；此信息显示在 Studio 中。

检查您指定的信息后，单击**完成**以启动目录创建过程。

故障排除

利用本部分中的信息可对使用计算机目录时可能会出现的问题进行故障排除。

Citrix 建议收集日志以帮助支持团队提供解决方案；按照本部分中的步骤进行操作可生成日志文件：

1. 在主映像上，创建值为 1（以“DWORD (32 位)值”格式）的以下注册表项：

Code 复制

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

```
HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING
```

2. 关闭主映像并创建新快照。

3. 在 DDC 上，启动加载了 Citrix PowerShell 管理单元的 PowerShell 并运行以下命令：

Code 复制

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True
```

4. 根据该快照创建一个新目录。

5. 当准备 VM 是在虚拟机管理程序上创建的时，登录并从 C:\ 的根目录下的以下文件中提取：

- Image-prep.log
- PvsVmAgentLog.txt

6. 关闭计算机，此时将报告失败。

7. 运行以下 PowerShell 命令以重新启用映像准备计算机的自动关闭功能：

Code 复制

```
Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown
```


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

管理计算机目录

Dec 05, 2017

在本文中：

- 简介
- 向计算机目录中添加计算机
- 从计算机目录中删除计算机
- 更改计算机目录说明或更改 Remote PC Access 设置
- 重命名计算机目录
- 将计算机目录移动到其他区域
- 删除计算机目录
- 管理计算机目录中的 Active Directory 计算机帐户
- 更新计算机目录
- 升级计算机目录

简介

可以在计算机目录中添加或删除计算机，以及重命名、更改说明或管理目录的 Active Directory 计算机帐户。

维护目录还可以包括确保每台计算机都安装最新的操作系统更新、防病毒软件更新、操作系统升级或配置更改。

- 对于包含使用 Machine Creation Services (MCS) 创建的池随机目录，可以通过更新在目录中使用的主映像，然后更新计算机来维护计算机。这使您能够有效地更新大量用户计算机。对于使用 Provisioning Services 创建的计算机，计算机的更新将通过虚拟磁盘传播。有关详细信息，请参阅 Provisioning Services 文档。
- 对于包含静态永久性分配的计算机的目录以及 Remote PC Access 计算机目录，请使用第三方软件分发工具以单独或集中方式在 Studio 外部管理用户计算机的更新。

有关创建和管理主机虚拟机管理程序和云服务的连接的信息，请参阅连接和资源。

提示：对于状态为“电源状态未知”的计算机，请参阅 CTX131267 以获取相关指南。

向计算机目录中添加计算机

开始之前：

- 确保虚拟化主机（虚拟机管理程序或云服务提供程序）具有足够多的处理器、内存和存储空间来容纳更多的计算机。
- 确保有足够多的未使用 Active Directory 计算机帐户。如果要使用现有帐户，可以添加的计算机数受可用帐户数限制。
- 如果使用 Studio 为更多计算机创建 Active Directory 计算机帐户，必须具有相应的域管理员权限。

向目录中添加计算机：

1. 在 Studio 导航窗格中选择**计算机目录**。
2. 选择计算机目录，然后在“操作”窗格中选择**添加计算机**。
3. 选择要添加的虚拟机数。
4. 如果现有 Active Directory 帐户的数量不足，无法容纳要添加的 VM 数量，请选择要在其中创建帐户的域和位置。指定帐户

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

命名方案，从而使用哈希值标记来指示将显示连续数字或字母的位置。请勿在 OU 名称中使用正斜杠 (/)。名称不能以数字开头。例如，命名方案 PC-Sales-##（可以选择 0-9）将生成名为 PC-Sales-01、PC-Sales-02、PC-Sales-03 等的计算机帐户。

5. 如果使用现有 Active Directory 帐户，请浏览到相应的帐户，或者单击**导入**并指定一个包含帐户名称的 .csv 文件。确保所有要添加的计算机都有足够的帐户。由于 Studio 将管理这些帐户，因此应允许 Studio 重置所有帐户的密码或者指定帐户密码（所有帐户的密码必须相同）。

系统会将计算机创建过程作为后台进程来执行，创建大量计算机时，需要很长时间才能完成。即使关闭 Studio，计算机创建过程也会继续执行。

从计算机目录中删除计算机

从计算机目录中删除计算机后，用户将无法再访问，因此，删除计算机之前，请确保：

- 用户数据已备份或者不再需要。
- 所有用户均已注销。打开维护模式将停止连接到计算机的新连接。
- 计算机已关机。

从目录中删除计算机：

1. 在 Studio 导航窗格中选择**计算机目录**。
2. 选择一个目录，然后在“操作”窗格中选择**查看计算机**。
3. 选择一个或多个计算机，然后在“操作”窗格中选择**删除**。

选择是否删除要删除的计算机。如果选择删除计算机，请指示应保留、禁用还是删除这些计算机的 Active Directory 帐户。

更改计算机目录说明或更改 Remote PC Access 设置

1. 在 Studio 导航窗格中选择**计算机目录**。
2. 选择一个目录，然后在“操作”窗格中选择**编辑计算机目录**。
3. （仅限 Remote PC Access 目录）在**电源管理**页面上，可以更改电源管理设置和选择电源管理连接。在**组织单位**页面上，添加或删除 Active Directory OU。
4. 在**说明**页面上，更改目录说明。

注意：对于 Citrix Cloud XenApp and XenDesktop Service 环境中的 Remote PC Access 目录，请按照 CTX220737 中的指南进行操作。

重命名计算机目录

1. 在 Studio 导航窗格中选择**计算机目录**。
2. 选择一个目录，然后在“操作”窗格中选择**重命名计算机目录**。
3. 输入新名称。

将计算机目录移动到其他区域

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

如果您的部署包含多个区域，可以将某个目录从一个区域移动到另一个区域。

小心：将某个目录移动到除包含该目录中的 VM 的虚拟机管理程序或云服务以外的其他区域会影响性能。

1. 在 Studio 导航窗格中选择**计算机目录**。
2. 选择一个目录，然后在“操作”窗格中选择**移动**。
3. 选择要将目录移动到的区域。

删除计算机目录

删除编录之前，请确保：

- 所有用户均已注销且没有仍在运行的已断开连接的会话。
- 该目录中的所有计算机均已打开维护模式，以便无法建立新连接。
- 该目录中的所有计算机均已关闭。
- 该目录不与交付组关联。即，交付组不包含该目录中的计算机。

要删除目录，请执行以下操作：

1. 在 Studio 导航窗格中选择**计算机目录**。
2. 选择一个目录，然后在“操作”窗格中选择**删除计算机目录**。
3. 指明是否应删除目录中的计算机。如果选择删除计算机，请指示应保留、禁用还是删除这些计算机的 Active Directory 计算机帐户。

管理计算机目录中的 Active Directory 计算机帐户

要管理计算机目录中的 Active Directory 帐户，可以：

- 从桌面操作系统和服务器操作系统目录中删除 Active Directory 计算机帐户，从而释放未使用的计算机帐户。之后，这些帐户便可用于其他计算机。
- 添加帐户，以便在向此目录添加更多计算机时，有可用的计算机帐户。请勿在 OU 名称中使用正斜杠 (/)。

管理 Active Directory 帐户：

1. 在 Studio 导航窗格中选择**计算机目录**。
2. 选择一个目录，然后在“操作”窗格中选择**管理 AD 帐户**。
3. 选择是添加还是删除计算机帐户。如果添加帐户，请指定帐户密码的处理方式：重置所有密码还是输入一个适用于所有帐户的密码。如果不知道当前的帐户密码，则可能需要重置密码；必须具有重置密码的权限。如果输入一个密码，帐户在导入时会更改密码。如果删除帐户，请选择应在 Active Directory 中保留、禁用还是删除帐户。

注意：还可以指示从目录中删除计算机或删除目录时应保留、禁用还是删除 Active Directory 帐户。

更新计算机目录

Citrix 建议您在更新目录中的计算机之前保存主映像的副本或快照。数据库会保留每个计算机目录中使用主映像的历史记录。如果已部署到用户桌面的更新出现问题，可以将目录中的计算机回滚（还原）为使用上一版本的主映像，从而最大程度地缩短用户停机时间。请勿删除、移动或重命名主映像；否则，您无法将目录还原为使用这些主映像。

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

对于使用 Provisioning Services 的目录，必须发布新虚拟磁盘才能将更改应用到该目录。有关详细信息，请参阅 Provisioning Services 文档。

更新计算机后，计算机将自动重新启动。

更新或创建新主映像

提示：有关如何管理连接的信息，请参阅连接和资源。

更新计算机目录之前，请更新现有主映像或在主机虚拟机管理程序上创建一个新的主映像。

1. 在您的虚拟机管理程序或云服务提供程序上，创建当前 VM 的快照并为该快照提供一个有意义的名称。可以根据需要使用该快照还原（回滚）目录中的计算机。
2. 如有需要，请打开主映像的电源并登录。
3. 安装更新或对主映像做任何必要的更改。
4. 如果主映像使用个人虚拟磁盘，请更新清单。
5. 对于 WIndows 10 计算机，请参阅*准备安装*中链接的优化资源。
6. 关闭 VM 的电源。
7. 创建 VM 的快照并为该快照提供一个能够在 Studio 中更新目录时识别的有意义的名称。虽然 Studio 可以创建快照，Citrix 仍建议您使用虚拟机管理程序管理控制台创建快照，然后在 Studio 中选择该快照。使用此方法可以提供有意义的名称及说明，而非自动生成的名称。对于 GPU 主映像，只能通过 XenServer 的 XenCenter 控制台进行更改。

更新目录

准备并前滚目录中的所有计算机的更新：

1. 在 Studio 导航窗格中选择**计算机目录**。
2. 选择一个目录，然后在“操作”窗格中选择**更新计算机**。
3. 在**主映像**页面上，选择要前滚的主机和映像。
4. 在**前滚策略**页面上，选择使用新主映像更新计算机目录中的计算机的时间：下次关闭时或立即。有关详细信息，请参阅下文。
5. 验证**摘要**页面上的信息，然后单击**完成**。每台计算机都在更新后自动重新启动。

提示：如果要直接使用 PowerShell SDK 更新目录，而非使用 Studio，可以指定一个虚拟机管理程序模板 (VMTemplates)，作为映像或映像的快照的替换选项。

前滚策略

使用 Citrix Connector for System Center Configuration Manager 时，提供下次关闭时更新映像的选项。

如果选择立即更新映像，请配置分发时间和通知。

- **分发时间:** 您可以选择同时更新所有计算机，或者指定开始更新目录中的所有计算机所需的总时间长度。内部算法决定该间隔时间内每台计算机的更新时间和重新启动时间。
- **通知:** 在左侧的通知下拉菜单中，选择是否在更新开始之前在计算机上显示通知消息。默认情况下，不显示任何消息。如果您选择在更新开始之前 15 分钟显示消息，则可以选择（在右侧下拉菜单中）在首次显示消息之后每隔 5 分钟重复显示该消息。默认情况下，该消息不重复显示。除非选择同时更新所有计算机，否则，通知消息将在更新开始之前的恰当时间在每台计算机上显示，该时间由内部算法计算得出。

回滚更新

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

前滚更新后的/新的主映像之后，可以进行回滚。如果新更新的计算机出现问题，可能有必要进行回滚。回滚时，目录中的计算机将回滚到上一个工作映像。需要较新映像的任何新功能将不再可用。与前滚一样，回滚计算机也需要重新启动。

1. 在 Studio 导航窗格中选择**计算机目录**。
2. 选择目录，然后在“操作”窗格中选择**回滚计算机更新**。
3. 按上文前滚操作所述，指定对计算机应用早期计算机映像的时间。

回滚仅适用于需要还原的计算机。对于尚未使用新的/更新后的主映像进行更新的计算机（例如，具有尚未注销的用户的计算机），用户不会收到通知消息，也不会被强制注销。

升级计算机目录或还原升级

在将计算机上的 VDA 升级到更新版本之后，可以升级计算机目录。Citrix 建议您将所有 VDA 升级到最新版本，以使其能够访问所有最新的功能。

升级目录之前，请执行以下操作：

- 如果使用的是 Provisioning Services，请在 Provisioning Services 控制台中升级 VDA 版本。
- 启动升级后的计算机，使其注册到 Controller 中。这样，Studio 便可以确定目录中的计算机是否需要升级。

要升级目录，请执行以下操作：

1. 在 Studio 导航窗格中选择**计算机目录**。
2. 选择目录。下部窗格中的“详细信息”选项卡会显示版本信息。
3. 选择**升级目录**。如果 Studio 检测到目录需要升级，它会显示一条消息。按照提示进行操作。如果一台或多台计算机无法升级，则消息中会说明原因。Citrix 建议您在升级目录前解决计算机问题，以确保所有计算机均正常运行。

目录升级完成后，您可以通过选择该目录，然后在“操作”窗格中选择**撤消**，将计算机还原到其前一个 VDA 版本。

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

创建交付组

Dec 05, 2017

交付组是从一个或多个计算机目录中选择的计算机的集合。交付组指定哪些用户可以使用这些计算机，以及可供这些用户使用的应用程序和/或桌面。

在配置部署过程中，应首先创建站点和计算机目录，然后再创建交付组。完成后，可以更改第一个交付组中的初始设置并创建其他交付组。还有一些只能在编辑交付组（而非创建交付组）时配置的功能和设置。

对于 Remote PC Access，在创建站点时，系统会自动创建一个名为 **Remote PC Access 桌面**的交付组。

要创建交付组，请执行以下操作：

1. 如果您已创建站点和计算机目录，但尚未创建交付组，Studio 将引导您进入正确的起始位置以创建交付组。如果您已创建交付组，而希望再创建一个，请在 Studio 导航窗格中选择**交付组**，然后在“操作”窗格中选择**创建交付组**。
2. 此时将启动“创建交付组”向导，并打开一个**简介**页面，您可以在将来启动此向导时不再显示该页面。
3. 此向导将指导您完成下列页面。完成每个页面之后，请单击**下一步**，直到到达最后一个页面为止。

计算机

选择一个计算机目录并选择要从该目录中使用的计算机数。

须知事项：

- 在选定的计算机目录中，必须至少有一台计算机处于未使用状态。
- 可以在多个交付组中指定计算机目录；但是，只能在一个交付组中使用计算机。
- 交付组可以使用多个目录中的计算机；但是，这些目录必须包含相同的计算机类型（服务器操作系统、桌面操作系统或 Remote PC Access）。换言之，您无法在交付组中混合使用多个计算机类型。同样，如果您的部署中包含 Windows 计算机的目录和 Linux 计算机的目录，则交付组可以包含其中一种操作系统类型中的计算机，但不能同时包含这两种操作系统类型中的计算机。
- Citrix 建议您安装或升级安装了最新版本的 VDA 的所有计算机，然后根据需要升级计算机目录和交付组。创建交付组时，如果选择安装了不同 VDA 版本的多台计算机，交付组将与最新版本的 VDA 兼容。（这就是所谓的组*功能级别*。）例如，如果您选择的一台计算机安装的是 VDA 7.1，而其他计算机安装的是最新版本，则该组中的所有计算机都只能使用 VDA 7.1 支持的功能。这意味着，在该组中可能无法使用需要更高版本的 VDA 的某些功能。例如，要使用 AppDisk 功能，VDA（以及该组的功能级别）版本至少必须为 7.8。
- Remote PC Access 计算机目录中的每台计算机都会自动与一个交付组相关联；在创建 Remote PC Access 站点时，系统会自动创建一个名为 **Remote PC Access 计算机**的目录以及一个名为 **Remote PC Access 桌面**的交付组。

交付类型

只有选择了包含静态（已分配）桌面操作系统计算机的计算机目录后，才会显示此页面。在“交付类型”页面中选择**应用程序**或**桌面**；不能同时启用这两者。

如果您是从服务器操作系统或桌面操作系统随机（池）目录中选择计算机的，则会假设交付类型为应用程序和桌面：您可以交付应用程序，也可以交付桌面，或者可以同时交付这两者。

AppDisk

要添加 AppDisk，请单击**添加**。“选择 AppDisk”对话框会在左侧列中列出可用的 AppDisk。右侧列将列出 AppDisk 上的应用程序。（选择右侧列上方的**应用程序**选项卡可按照与“开始”菜单类似的方式列出应用程序；选择**已安装的软件包**选项卡可按照

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

与“程序和功能”列表类似的方式列出应用程序。）

选中一个或多个复选框。

有关详细信息，请参阅 AppDisk 一文。

用户

指定能够使用交付组中的应用程序和桌面的用户和用户组。

指定了用户列表的位置

Active Directory 用户列表在您创建或编辑以下内容时指定：

- 站点的用户访问列表（不通过 Studio 配置）。默认情况下，应用程序授权策略规则包括所有人；有关详细信息，请参阅 PowerShell SDK BrokerAppEntitlementPolicyRule cmdlet。
- 应用程序组（如果已配置）。
- 交付组。
- 应用程序。

能够通过 StoreFront 访问应用程序的用户的列表是由上述用户列表的交集组成的。例如，要配置为由特定部门使用应用程序 A，而不过度限制对其他组的访问：

- 使用包括所有人的默认应用程序授权策略规则。
- 配置交付组用户列表以允许所有总部用户使用在交付组中指定的任何应用程序。
- （如果已配置应用程序组）配置应用程序组用户列表，以允许行政和财务业务部的成员通过 L 访问应用程序 A。
- 配置应用程序 A 的属性，使其仅对行政和财务业务部的应收账款业务工作人员可见。

已通过身份验证的用户和未经身份验证的用户

用户类型有两种：已通过身份验证和未经身份验证（后者也称为匿名）。您可以在交付组中配置其中一种类型或这两种类型。

已完成身份验证

按名称指定的用户和组成员必须向 StoreFront 或 Citrix Receiver 提供凭据（例如智能卡或用户名和密码），才能访问应用程序和桌面。（对于包含桌面操作系统计算机的桌面组，您可以在编辑交付组之后导入用户数据（用户列表）。）

未经身份验证（匿名）

对于包含服务器操作系统计算机的交付组，允许用户在不向 StoreFront 或 Citrix Receiver 提供凭据的情况下访问应用程序和桌面。例如，在 kiosk 模式下，应用程序可能需要凭据，但 Citrix 访问门户和工具则不需要。安装第一个 Delivery Controller 时，会创建匿名用户组。

要向未经身份验证的用户授予访问权限，交付组中的每台计算机必须已安装 VDA for Windows Server OS（最低版本为 7.6）。启用未经身份验证的用户时，您必须具有未经身份验证的 StoreFront 存储。

启动会话时，将按需创建未经身份验证的用户帐户，并命名为 AnonXYZ，其中，XYZ 是一个唯一的三位数值。

未经身份验证的用户会话的默认空闲超时为 10 分钟，当客户端断开连接时，这些会话将自动注销。不支持重新连接、客户端之间漫游以及工作区控制。

下表介绍了“用户”页面上的选项：

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

启用访问权限的用户	是否添加/分配用户和用户组？	是否启用“Give access to unauthenticated users”（向未经身份验证的用户授予访问权限）复选框？
仅限已通过身份验证的用户	是	否
仅未经身份验证的用户	否	是
已通过身份验证的用户和未经身份验证的用户	是	是

应用程序

须知事项：

- 无法向 Remote PC Access 交付组中添加应用程序。
- 默认情况下，您添加的新应用程序将放置在“应用程序”文件夹中。可以指定其他文件夹。有关详细信息，请参阅“管理应用程序”一文。
- 您可以在将应用程序添加到交付组时更改其属性，也可以稍后更改这些属性。有关详细信息，请参阅“管理应用程序”一文。
- 如果您尝试添加某个应用程序，但同一文件夹中已存在同名应用程序，则系统将提示您重命名要添加的应用程序。如果拒绝，添加的应用程序将附带一个后缀，使其在该应用程序文件夹中成为唯一的存在。
- 如果要将一个应用程序添加到多个交付组中，但您没有足够的权限查看所有这些交付组中的应用程序，则会产生可见性问题。在这种情况下，可以咨询权限更高的管理员，或者扩展您的作用域，以包括将应用程序添加到的所有交付组。
- 如果使用相同名称向同一用户发布两个应用程序，请在 Studio 中更改应用程序名称(面向用户) 属性，否则，用户将在 Receiver 中看到重复的名称。

单击**添加**下拉菜单以显示应用程序源。

- **从“开始”菜单：**此类应用程序是在通过主映像创建的计算机上发现的，该主映像位于所选目录中。如果选择此源，则会启动一个新页面，其中会列出已发现的应用程序；请选择您要添加的应用程序，然后单击**确定**。
- **手动定义：**此类应用程序位于此站点上或网络中的其他位置。如果选择此源，则会启动一个新页面，您可以在其中键入可执行文件路径、工作目录、可选命令行参数以及显示给管理员和用户的名称。输入此信息后，请单击**确定**。
- **现有：**此类应用程序先前已添加到站点中，该站点可能位于另一个交付组。如果选择此源，则会启动一个新页面，其中会列出已发现的应用程序；请选择您要添加的应用程序，然后单击**确定**。
- **App-V：**App-V 软件包中的应用程序。如果选择此源，则会启动一个新页面，您可以在其中选择 App-V 服务器或应用程序库。从生成的显示结果中选择要添加的应用程序，然后单击**确定**。有关详细信息，请参阅 App-V 一文。

如果应用程序源或应用程序不可用或无效，则无法显示该应用程序，或者无法选择该应用程序。例如，如果该站点没有添加任何应用程序，则无法使用**现有：**源。或者，应用程序也可能与所选计算机目录中计算机支持的会话类型不兼容。

桌面（或桌面分配规则）

此页面的标题取决于您先前在向导中选择的计算机目录。

- 如果所选计算机目录包含池计算机，则此页面标题为“桌面”。
- 如果所选计算机目录包含已分配的计算机，并在“交付类型”页面上指定的是“桌面”，则此页面标题为“Desktop User Assignment”（桌面用户分配）。

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

- 如果所选计算机目录包含已分配的计算机，并在“交付类型”页面上指定的是“应用程序”，则此页面标题为“Application Machine User Assignment”（应用程序计算机用户分配）。

单击**添加**。在此对话框中：

- 在“显示名称”和“说明”字段中，输入要在 Receiver 中显示的信息。
- 要向桌面添加标记限制，请选择**限制启动带标记的计算机**，然后从下拉框中选择标记。（有关详细信息，请参阅标记一文。）
- 通过单选按钮指示谁可以启用桌面（对于包含池计算机的组）或在启用桌面时会为谁分配计算机（对于包含已分配计算机的组）。用户可以是可访问该交付组的任何人，也可以是特定的用户和用户组。
- 如果该组包含已分配的计算机，请指定每个用户的最多桌面数量。该值不得小于 1。
- 启用或禁用桌面（对于池计算机）或桌面分配规则（对于已分配计算机）。禁用桌面会停止交付桌面；禁用桌面分配规则会停止向用户自动分配桌面。
- 完成此对话框后，请单击**确定**。

总结

输入交付组的名称。您也可以输入一个说明，该说明将显示在 Receiver 和 Studio 中。

查看摘要信息，然后单击**完成**。如果您没有选择或指定任何要交付的应用程序或桌面，系统会询问您是否要继续。

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

管理交付组

Dec 05, 2017
在本文中：

- 简介
- 更改交付组中的用户设置
- 在交付组中添加或删除用户
- 更改交付组的交付类型
- 更改 StoreFront 地址
- 为桌面添加、更改或删除标记限制
- 升级交付组或还原升级
- 管理 Remote PC Access 交付组
- 关闭并在重新启动交付组中的计算机
- 对交付组中的计算机进行电源管理
- 为交付组中的计算机创建重新启动计划
- 为交付组中的计算机创建多个重新启动计划
- 禁止用户连接到交付组中的计算机（维护模式）
- 更改为交付组中的用户分配的计算机
- 更改交付组中每个用户的最大计算机数
- 对交付组中的计算机进行负载管理
- 从交付组中删除计算机
- 限制对交付组中计算机的访问
- 更新交付组中的计算机
- 注销或断开会话或者向“交付组”用户发送消息
- 配置会话预启动和会话延迟

简介

本文介绍了针对交付组的管理过程。除了更改在创建组时指定的设置，您还可以配置在创建交付组对您不可用的其他设置。

请参阅应用程序，了解有关如何管理交付组中的应用程序（包括如何在交付组中添加和删除应用程序以及如何更改应用程序属性）的信息。

要管理交付组，必须使用“交付组管理员”内置角色的委派管理权限。有关详细信息，请参阅委派管理。

提示 ：

- 在交付组的 Studio 显示屏幕中，“详细信息”窗格中的“已安装的 VDA 版本”可能与计算机上安装的实际版本不同。计算机的 Windows“程序和功能”将显示实际的 VDA 会话。
- 对于状态为“电源状态未知”的计算机，请参阅 CTX131267 以获取相关指南。

向 Delivery Controller 注册 VDA

启动代理会话时，不会考虑未使用 Delivery Controller 进行注册的 VDA，这样会导致无法充分利用原本可用的资源。VDA 无法

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

注册的原因有多种，其中许多都可由管理员进行故障排除。Studio 在目录创建向导中，以及在您向交付组添加了目录之后，提供故障排除信息。

创建了交付组之后，Studio 会显示与该组关联的计算机的详细信息。交付组的详细信息窗格中指示应该注册但未注册的计算机数。即，可能存在一台或多台已开启且不是处于维护模式但当前未向 Controller 注册的计算机。查看“应注册、但未注册的”计算机时，请查看详细信息窗格中“故障排除”选项卡了解可能的原因及建议的更正措施。

有关功能级别的消息，请参阅 VDA 版本和功能级别。

有关 VDA 注册故障排除的详细信息，请参阅 CTX136668。

更改交付组中的用户设置

此页面的名称可能显示为**用户设置**或**基本设置**。

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择一个组，然后在“操作”窗格中选择**编辑交付组**。
3. 在**用户设置**（或**基本设置**）页面中，更改下表中的任何设置。
4. 单击**应用**以应用您所做的任何更改并保持打开窗口，或单击**确定**应用更改并关闭窗口。

设置	**说明**
说明	StoreFront 使用且用户能够看到的文本。
启用交付组	是否启用交付组。
时区	
启用 Secure ICA	使用 SecureICA 确保与交付组中的计算机之间的通信安全，这会加密 ICA 协议（默认级别为 128 位；可使用 SDK 更改该级别）。Citrix 建议在遍历公共网络时使用其他加密方法（如 TLS 加密）。SecureICA 也不检查数据完整性。

在交付组中添加或删除用户

有关用户的详细信息，请参阅“创建交付组”一文的“用户”部分。

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择一个组，然后在“操作”窗格中选择**编辑交付组**。
3. 在**用户**页面上，要添加用户，请单击**添加**，然后指定要添加的用户。要删除用户，请选择一个或多个用户，然后单击**删除**。您还可以选中/取消选中允许或禁止未经身份验证的用户进行访问所对应的复选框。
4. 单击**应用**以应用您所做的任何更改并保持打开窗口，或单击**确定**应用更改并关闭窗口。

导入或导出用户列表

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

对于包含物理桌面操作系统计算机的交付组，您可以在创建交付组之后从 .csv 文件导入用户信息。您还可以将用户信息导出到 .csv 文件。.csv 文件可以包含来自先前产品版本的数据。

.csv 文件中的第一行必须包含以逗号分隔的列标题（任何顺序均可），其中可以包括：ADComputerAccount、AssignedUser、VirtualMachine 和 HostId。文件中的后续行包含以逗号分隔的数据。ADComputerAccount 条目可以是公用名、IP 地址、标识名或域和计算机名称对。

要导入或导出用户信息，请执行以下操作：

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择交付组，然后在“操作”窗格中选择**编辑交付组**。
3. 在**计算机分配**页面上，选择**导入**列表或**导出**列表按钮，然后浏览到文件位置。
4. 单击**应用**以应用您所做的任何更改并保持打开窗口，或单击**确定**应用更改并关闭窗口。

更改交付组的交付类型

交付类型指定组可以交付的内容：应用程序、桌面或二者。

将**仅应用程序**或**桌面和应用程序**类型更改为**仅桌面**类型之前，请从交付组中删除所有应用程序。

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择一个组，然后在“操作”窗格中选择**编辑交付组**。
3. 在**交付类型**页面上，选择所需的交付类型。
4. 单击**应用**以应用您所做的任何更改并保持打开窗口，或单击**确定**应用更改并关闭窗口。

更改 StoreFront 地址

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择一个组，然后在“操作”窗格中选择**编辑交付组**。
3. 在 **StoreFront** 页面上，选择或添加交付组中每台计算机上所安装的 Citrix Receiver 将要使用的 StoreFront URL。
4. 单击**应用**以应用您所做的任何更改并保持打开窗口，或单击**确定**应用更改并关闭窗口。

也可以通过在 Studio 导航窗格中依次选择**配置 > StoreFront** 来指定 StoreFront 服务器地址。

为桌面添加、更改或删除标记限制

重要：添加、更改和删除标记限制可能会对被考虑启动的桌面有意外的影响。请务必查看标记一文中的考虑事项和警告。

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择一个组，然后在“操作”窗格中选择**编辑交付组**。
3. 在**桌面**页面上，选择桌面并单击**编辑**。
4. 要添加标记限制，请选择**限制启动带标记的计算机**，然后选择标记。
5. 要更改或删除标记限制，请选择一个不同的标记，或通过清除**限制启动带标记的计算机**彻底删除标记限制。
6. 单击**应用**以应用您所做的任何更改并保持打开窗口，或单击**确定**应用更改并关闭窗口。

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

升级交付组或还原升级

升级交付组计算机上的 VDA 和计算机目录（包含交付组中使用的计算机）之后，升级交付组。

启动交付组升级之前：

- 如果您使用 Provisioning Services，则在 Provisioning Services 控制台中升级 VDA 版本。
- 启动包含升级 VDA 的计算机，以便这些计算机向 Delivery Controller 注册。此过程将指示 Studio 交付组中需要升级的内容。
- 如果必须使用早期的 VDA 版本，更新的产品功能可能不可用。有关详细信息，请参阅各种升级文章。

要升级交付组，请执行以下操作：

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择一个组，然后在“操作”窗格中选择**升级交付组**。**升级交付组**操作仅当 Studio 检测到已升级的 VDA 时显示。

启动升级过程之前，Studio 将指示您无法升级的计算机（如果有）及原因。您随后可以取消升级、解决计算机问题，然后再次启动升级。

升级完成后，您可以通过选择交付组，然后在“操作”窗格中选择**撤消**，将计算机还原到其先前状态。

管理 Remote PC Access 交付组

如果 Remote PC Access 计算机目录中的计算机未分配给用户，Studio 会暂时将该计算机分配给与该计算机目录关联的交付组。通过这种临时分配，之后可以将计算机分配给用户。

交付组与计算机目录的关联具有一个优先级值。优先级决定向系统注册计算机或用户需要计算机分配时，将计算机分配给哪个交付组：值越低，优先级越高。如果 Remote PC Access 计算机目录具有多个交付组分配，该软件将选择优先级最高的匹配项。您可以使用 PowerShell SDK 设置此优先级值。

首次创建后，Remote PC Access 计算机目录将与交付组关联。这意味着添加到目录的计算机帐户或组织单位稍后可以添加到交付组。此关联可以关闭或开启。

添加或删除 Remote PC Access 计算机目录与交付组的关联：

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择 Remote PC Access 组。
3. 在“详细信息”部分，选择**计算机目录**选项卡，然后选择 Remote PC Access 目录。
4. 要添加或还原关联，请选择 **添加桌面**。要删除关联，请选择**删除关联**。

关闭并在重新启动交付组中的计算机

Remote PC Access 计算机不支持此过程。

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择一个组，然后在“操作”窗格中选择**查看计算机**。
3. 选择计算机，然后在“操作”窗格中选择下列项之一（某些选项可能不可用，具体视计算机状态而定）：

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

- **强制关闭**。强行关闭计算机并刷新计算机列表。
- **重新启动**。请求关闭操作系统，然后再次启动计算机。如果操作系统无法关闭，计算机将保持其当前状态。
- **强制重新启动**。强行关闭操作系统，然后重新启动计算机。
- **挂起**。不关闭但暂停计算机并刷新计算机列表。
- **关闭**。请求关闭操作系统。

对于非强制操作，如果计算机在 10 分钟内没有关闭，则会关机。如果 Windows 尝试在关闭期间安装更新，可能面临在更新完成前计算机关闭的风险。

Citrix 建议阻止桌面操作系统计算机用户在会话中选择**关闭**。有关详细信息，请参阅 Microsoft 策略文档。

您也可以关闭并重新启动连接中的计算机；请参阅“连接和资源”一文。

对交付组中的计算机进行电源管理

您只能对虚拟桌面操作系统计算机进行电源管理，而不能对物理机（包括 Remote PC Access 计算机）进行电源管理。具有 GPU 功能的桌面操作系统计算机无法挂起，因此关机操作失败。对于服务器操作系统，您可以创建重新启动计划，本文也包含相关介绍。

在包含池计算机的交付组中，虚拟桌面操作系统计算机可以处于以下一种状态：

- 随机分配并且正在使用
- 未分配并且未连接

在包含静态计算机的交付组中，虚拟桌面操作系统计算机可以：

- 永久分配并且正在使用
- 永久分配并且未连接（但已就绪）
- 未分配并且未连接

在正常使用期间，静态交付组通常既包括永久分配的计算机，也包括未分配的计算机。最初，所有计算机均未分配（创建交付组时手动分配的计算机除外）。当用户连接时，计算机变为永久分配状态。您可以对这些交付组中的未分配计算机进行全面的电源管理，但对永久分配的计算机却只能进行部分管理。

池和缓冲区：对于包含未分配计算机的池交付组和静态交付组，池（在这种情况下）是一组保持为开启状态以供用户连接的未分配或临时分配的计算机；用户在登录后将立刻获得计算机。池大小（保持为启动状态的计算机数）可按一天中的具体时刻进行配置。对于静态交付组，请使用 SDK 配置池。

缓冲区是另外一组未分配的备用计算机，它们在池中的计算机数低于阈值（交付组大小的百分比）时打开。对于大型交付组，超过阈值时可能会打开大量计算机，因此请谨慎规划交付组大小或使用 SDK 调整默认缓冲区大小。

电源状态计时器：您可以使用电源状态计时器在用户断开连接指定时间后挂起计算机。例如，在非工作时间，计算机将在用户断开连接至少 10 分钟后自动挂起。除非您配置 SDK 中的 ShutdownDesktopsAfterUse 交付组属性，否则随机计算机或具有个人虚拟磁盘的计算机将在用户注销时自动关闭。

您可以针对工作日和周末以及峰值和非峰值间隔配置计时器。

永久分配计算机的部分电源管理：对于永久分配的计算机，您可以设置电源状态计时器，但对池和缓冲区则不可。这些计算机在每个高峰期到来时打开，在每个非高峰期到来时关闭。您无法像处理未分配计算机那样精细控制用来补偿被占用计算机的可用计算机数。

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

要对虚拟桌面操作系统计算机进行电源管理，请执行以下操作：

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择一个组，然后在“操作”窗格中选择**编辑交付组**。
3. 在**电源管理**页面上的“对计算机进行电源管理”下拉列表中选择**工作日**。默认情况下，工作日是指周一到周五。
4. 对于随机交付组，在**要开启的计算机**中，选择**编辑**并指定工作日期间的池大小。然后，选择要启动的计算机数。
5. 在**高峰小时数**中，设置每天的高峰时段和非高峰期间。
6. 设置工作日高峰时段和非高峰时段的电源状态计时器：在**高峰期间 > 断开连接时**中，指定挂起交付组中任何已断开连接的计算机前的延迟时间（分钟），然后选择“挂起”。在**非高峰期间 > 断开连接时**中，指定关闭交付组中任何已注销计算机前的延迟时间，然后选择**关闭**。此计时器不可用于具有随机计算机的交付组。
7. 在“对计算机进行电源管理”下拉列表中选择**周末**，然后配置周末的高峰时段和电源状态计时器。
8. 单击**应用**以应用您所做的任何更改并保持打开窗口，或单击**确定**应用更改并关闭窗口。

使用 SDK 可以执行以下操作：

- 关闭而非挂起计算机以响应电源状态计时器，或者在希望计时器基于注销数而非断开连接数时使用。
- 更改默认的工作日和周末定义。
- 禁用电源管理；请参阅 CTX217289。

为交付组中的计算机创建重新启动计划

注意：本节介绍如何在 Studio 中配置单个重新启动计划。也可以使用 PowerShell 为交付组中不同的计算机子集配置多个重新启动计划。有关详细信息，请参阅下一节。

重新启动计划指定定期重新启动交付组中所有计算机的时间。

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择一个组，然后在“操作”窗格中选择**编辑交付组**。
3. 在**重启计划**页面，如果不希望自动重新启动交付组中的计算机，请选择**否**单选按钮并跳过本过程的最后一步。这样将不会配置重新启动计划或前滚策略。如果之前已配置计划，选择此选项会将此计划取消。
4. 如果希望自动重新启动交付组中的计算机，请选择**是**单选按钮。
5. 对于**重新启动频率**，请选择**每天**或每周执行重新启动的日期。
6. 对于**重新启动开始时间**，请使用 24 小时制指定开始重新启动的时间。
7. 对于**重新启动持续时间**，请选择是否同时启动所有计算机，或选择开始重新启动交付组中的所有计算机的总时间。内部算法确定该间隔内每台计算机的重新启动时间。
8. 在左侧的**通知**下拉列表中，选择是否在重新启动开始之前显示关于受影响计算机的通知消息。默认情况下，不显示任何消息。如果选择在距离重新启动开始还有 15 分钟时显示消息，可以选择在第一次显示消息之后每 5 分钟重复显示此消息（在 **Repeat notification**（重复通知）下拉列表中）。默认情况下，该消息不重复显示。
9. 在**通知消息**框中，输入通知文本；系统不提供默认文本。如果希望消息包含重新启动开始前剩余的分钟数，可包含变量 **%m%**（示例：警告: 您的计算机将在 %m% 分钟后自动重新启动）。如果选择重复通知间隔并且消息中包含 %m% 占位符，此值将在每次重复显示消息时减去五分钟。除非选择同时启动所有计算机，否则，在重新启动开始前的相应时间（由内部算法计算），交付组中的每台计算机上均显示消息。
10. 单击**应用**以应用您所做的任何更改并保持打开窗口，或单击**确定**应用更改并关闭窗口。

不能在 Studio 中执行自动打开或关闭操作，只能执行重新启动操作。

为交付组中的计算机创建多个重新启动计划

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

可以使用 PowerShell cmdlet 为交付组中的计算机创建多个重新启动计划。每个计划可以配置为只影响组中有指定标记的那些计算机。此标记限制功能允许您为一个交付组中不同的计算机子集创建不同的重新启动计划。

例如，假设您对公司里的所有计算机使用一个交付组。您希望至少每周一次（星期日晚上）重新启动所有计算机，但是核算团队使用的计算机应该每天重新启动。您可以为所有计算机设置每周计划，且只为核算团队使用的计算机设置每日计划。

计划重叠

多个计划可能重叠。在上面的示例中，核算团队使用的计算机受两个计划影响，因此可能在星期日重新启动两次。

可设计计划规范避免重新启动相同计算机的次数超过需要的次数，但无法保证。如果两个计划的开始时间和持续时间完全一致，则很可能将只重新启动一次计算机。但是，计划在开始时间和/或持续时间上越不同，越有可能发生两次重新启动。另外，受计划影响的计算机数也会影响重叠的可能性。在该示例中，重新启动所有计算机的每周计划启动重新启动的速度可能远快于每日计划（取决于每个计划的配置持续时间）。

要求

目前只能通过 PowerShell 命令行，使用 XenApp 和 XenDesktop 7.12 中全新的 RebootScheduleV2 PowerShell cmdlet，支持创建多个重新启动计划以及在重新启动计划中使用标记限制。（本文中它们统称为“V2”cmdlet。）

要使用 V2 cmdlet，要求使用：

- Delivery Controller 版本 7.12（最低）。
  - 如果您将最新的 SDK 插件与早于 7.12 的 Controller 结合使用，则您创建的任何新计划都不会如期进行。
  - 在混合站点（其中部分而非全部 Controller 升级了）中，在数据库已升级，并且至少一个 Controller 已升级且正在使用（通过在 V2 cmdlet 中指定 –adminaddress 参数）之前，V2 cmdlet 无法运行。
  - 最佳做法：请勿在站点中的所有 Controller 都升级完之前创建任何新计划。
- XenApp 和 XenDesktop 7.12（最低）附带的 PowerShell SDK 管理单元。安装或升级组件和站点后，运行 asnp Citrix.* 加载最新的 cmdlet。

Studio 当前使用较早的 V1 RebootSchedule PowerShell cmdlet，因此将不会显示使用 V2 cmdlet 创建的计划。

创建了使用标记限制的重新启动计划后，之后使用 Studio 在重新启动时间间隔（周期）中从受影响的计算机删除标记，或在重新启动周期中将标记添加到其他计算机，那些更改将在下一次重新启动周期时才会生效。（这些更改不会影响当前重新启动周期。）

PowerShell cmdlet

可从命令行使用以下 RebootScheduleV2 cmdlet 来创建多个计划，并在计划中使用标记限制。

新 (V2) cmdlet	替代早期 (V1) cmdlet
New-BrokerRebootScheduleV2	New-BrokerRebootSchedule
Get-BrokerRebootScheduleV2	Get-BrokerRebootSchedule
Set-BrokerRebootScheduleV2	Set-BrokerRebootSchedule
Remove-BrokerRebootScheduleV2	Remove-BrokerRebootSchedule

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

Rename-BrokerRebootScheduleV2	-

要获得完整的 cmdlet 语法和参数说明，请输入 **Get-Help –full** <*cmdlet-name*>。

术语提醒：在 PowerShell SDK 中，DesktopGroup 参数用于标识交付组。

如果您熟悉用于创建重新启动计划的 Studio 界面，所有那些参数在使用 V2 cmdlet 创建或更新计划时都可用。此外，您可以：

- 将计划限于具有指定标记的计算机。
- 在发送第一个警告消息之前指定时间间隔，在此期间不会将新会话代理至受影响的计算机。

配置

如果配置使用标记限制的重新启动计划，还必须将该标记添加到该计划要影响的计算机。（有关详细信息，请参阅标记。）

1. 从 Studio 的导航窗格中选择**交付组**。
2. 选择包含将受计划影响的计算机的交付组。
3. 选择“查看计算机”，然后选择将为其添加标记的计算机。
4. 在“操作”窗格中选择**管理标记**。
5. 如果标记已存在，请启用标记名称旁边的复选框。如果标记不存在，请单击**创建**，然后指定标记名称。创建标记后，启用新建标记名称旁边的复选框。
6. 在“管理标记”对话框中单击**保存**。

创建并添加（应用）标记后，在使用 V2 cmdlet 创建或编辑计划时使用 –RestrictToTag 参数指定标记名称。

如果您已使用早期 XenApp 或 XenDesktop 版本创建了重新启动计划

Studio 当前使用 V1 RebootSchedule cmdlet。如果您有一个在升级到 7.12（最低）之前创建的重新启动计划，可以在 Studio 中使用 V1 cmdlet 继续对其进行管理，但是不能使用 Studio 将标记限制添加到该计划，也不能创建其他计划（因为 Studio 不支持 V2 cmdlet）。只要对现有计划使用 V1 cmdlet，Studio 将显示有关重新启动计划的正确信息。

也可以从命令行使用新的 V2 RebootSchedule cmdlet 编辑现有计划。使用新的 V2 cmdlet 时，可以在该计划中使用标记限制参数，以及创建其他重新启动计划。但是，使用 V2 cmdlet 更改现有计划后，Studio 将不会显示完整的计划信息（因为它只能识别 V1 信息）。您无法看到是否使用了标记限制以及计划的名称和说明。

禁止用户连接到交付组中的计算机（维护模式）

当您需要临时停止计算机的新连接时，可以针对交付组中的一个或所有计算机打开维护模式。您可能会在应用修补程序或使用管理工具之前执行此操作。

- 当服务器操作系统计算机处于维护模式时，用户可以连接到现有会话，但无法启动新会话。
- 当桌面操作系统计算机（或使用 Remote PC Access 的 PC）处于维护模式时，用户无法连接或重新连接。当前连接仍保持连接状态，直到其断开连接或注销。

要打开或关闭维护模式，请执行以下操作：

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择一个组。

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

3. 要针对交付组中的所有计算机打开维护模式，请在“操作”窗格中选择**打开维护模式**。要为一台计算机打开维护模式，请在“操作”窗格中选择**查看计算机**。选择计算机，然后在“操作”窗格中选择**打开维护模式**。
4. 要针对交付组中的一台或所有计算机关闭维护模式，请按照之前的说明操作，但要在“操作”窗格中选择**关闭维护模式**。

Windows 远程桌面连接 (RDC) 设置还影响服务器操作系统计算机是否处于维护模式。以下任一情况下，维护模式将打开：

- 维护模式设置为打开，如上所述。
- RDC 设置为 **Don't allow connections to this computer**（不允许连接到这台计算机）。
- RDC 不设置为 **Don't allow connections to this computer**（不允许连接到这台计算机），并且“Remote Host Configuration User Logon Mode”（远程主机配置用户登录模式）设置为 **Allow reconnections, but prevent new logons**（允许重新连接，但拒绝新用户登录）或 **Allow reconnections, but prevent new logons until the server is restarted**（允许重新连接，但服务器重新启动后才允许新用户登录）。

您也可以针对某个连接打开或关闭维护模式（影响使用此连接的计算机），或针对某个计算机目录打开或关闭维护模式（影响此目录中的计算机）。

更改为交付组中的用户分配的计算机

您可以更改桌面操作系统计算机的分配情况，不能更改服务器操作系统计算机或通过 Provisioning Services 创建的计算机的分配情况。

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择一个组。
3. 在“操作”窗格中选择**编辑交付组**。在**桌面**或**桌面分配规则**页面（仅其中一个页面可用，具体取决于交付组所使用的计算机目录类型）上，指定新用户。
4. 单击**应用**以应用您所做的任何更改并保持打开窗口，或单击**确定**应用更改并关闭窗口。

更改每个用户的最大计算机数

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择一个组，然后在“操作”窗格中选择**编辑交付组**。
3. 在**桌面分配规则**页面上，设置每个用户值对应的最大桌面数。
4. 单击**应用**以应用您所做的任何更改并保持打开窗口，或单击**确定**应用更改并关闭窗口。

对交付组中的计算机进行负载管理

只能对服务器操作系统计算机进行负载管理。

负载管理可测量服务器负载并决定在当前环境条件下选择哪个服务器。其选择的依据包括：

服务器维护模式状态：仅在维护模式关闭的情况下，才考虑将服务器操作系统计算机用于负载平衡。

服务器负载指数：确定交付服务器操作系统计算机的服务器接收连接的可能性。该指数是负载评估程序的组合：会话数和性能指标（如 CPU、磁盘和内存使用情况）的设置。负载评估程序在负载管理策略设置中指定。

您可以在 Director、Studio 搜索和 SDK 中监视负载指数。

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

在 Studio 中，“Server Load Index”（服务器负载指数）列默认处于隐藏状态。要显示该列，请选择计算机，通过右键选择列标题，然后选择选择列。在“计算机”类别中，选择负载指数。

在 SDK 中，使用 Get-BrokerMachine cmdlet。有关详细信息，请参阅和 CTX202150。

服务器负载指数为 10000 表示服务器处于全负载状态。如果没有其他服务器可用，则用户启动会话时可能会收到一条消息，说明桌面或应用程序当前不可用。

并发登录容差策略设置：登录到服务器的最大并发请求数。（在 7.5 之前的 XenApp 版本中，此设置等效于负载限制。）

如果所有服务器都等于或高于并发登录容错设置，则会将下一个登录请求分配给挂起登录最少的服务器。如果有多个服务器符合这些条件，则会选择负载指数最低的服务器。

从交付组中删除计算机

删除某台计算机会将其从交付组中删除，但不会从交付组所使用的计算机目录中删除。因此，可将计算机分配给其他交付组。

必须先关闭计算机，之后才能将其删除。要在删除计算机时暂时阻止用户连接到该计算机，请先将其置于维护模式，然后再关闭计算机。

请谨记，计算机可能包含个人数据，因此将其分配给其他用户之前应小心谨慎。您可能需要重新建立计算机映像。

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择一个组，然后在“操作”窗格中选择**查看计算机**。
3. 确保所有计算机已关闭。
4. 在“操作”窗格中选择**从交付组中删除**。

也可以通过计算机所采用的连接来删除交付组中的计算机。有关详细信息，请参阅管理和资源。

限制对交付组中计算机的访问

无论使用何种方法，为限制访问交付组中的计算机所做的任何更改都将取代以前的设置。可以执行以下操作：

使用委派管理作用域限制管理员的访问权限。可以创建并分配两个作用域，一个允许管理员访问所有应用程序，另一个仅允许访问某些特定的应用程序。有关详细信息，请参阅“委派管理”一文。

使用 SmartAccess 策略表达式限制用户的访问权限，这些策略表达式可以过滤通过 NetScaler Gateway 建立的用户连接。

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择组，然后在“操作”窗格中选择**编辑交付组**。
3. 在**访问策略**页面上，选择**通过 NetScaler Gateway 的连接**。
4. 要选择这些连接的一个子集，请选择**满足以下任意过滤器条件的连接**。然后定义 NetScaler Gateway 站点，并为允许的用户访问方案添加、编辑或删除 SmartAccess 策略表达式。有关详细信息，请参阅 NetScaler Gateway 文档。
5. 单击**应用**以应用您所做的任何更改并保持打开窗口，或单击**确定**应用更改并关闭窗口。

通过适用于您在 SDK 中设置的访问策略的**排除过滤器限制用户的访问权限**。访问策略应用于交付组，以对连接进行细化设置。例如，您可以仅限某个用户子集访问计算机，也可以指定允许的用户设备。排除过滤器可进一步细化访问策略。例如，出于安全性考虑，您可以拒绝某个用户子集或设备访问。默认情况下，排除过滤器处于禁用状态。

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

例如，对于企业网络子网上的教学实验室，要阻止从实验室访问某个特定交付组，而无论该实验室中的计算机使用者为何人，请使用以下命令：Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -

可以使用星号 (*) 通配符来匹配以相同策略表达式开头的所有标记。例如，如果在一台计算机中添加标记 VPDesktops_Direct，在另一台计算机中添加标记 VPDesktops_Test，则在 Set-BrokerAccessPolicy 脚本中将标记设置为 VPDesktops_* 将同时适用于这两台计算机的过滤器。

如果您是使用 Web 浏览器或者通过在应用商店中启用的统一 Citrix Receiver 用户体验功能连接的，则不能使用客户端名称排除过滤器。

更新交付组中的计算机

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择一个组，然后在“操作”窗格中选择**查看计算机**。
3. 选择一台计算机，然后在“操作”窗格中选择**更新计算机**。

要选择其他主映像，请选择**主映像**，然后选择一个快照。

要应用更改并通知计算机用户，请选择**向最终用户发出通知**。然后指定：何时更新主映像（立即还是下次重新启动时），重新启动分发时间（开始更新组内的所有计算机的总时间），用户是否收到重新启动通知，以及用户将收到的消息。

注销或断开会话或者向“交付组”用户发送消息

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择一个组，然后在“操作”窗格中选择**查看计算机**。
3. 要使用户注销会话，请选择会话或桌面，然后在“操作”窗格中选择**注销**。会话随即关闭，此时计算机可供其他用户使用，除非已将其分配给特定用户。
4. 要断开会话，请选择会话或桌面，然后在“操作”窗格中选择**断开连接**。应用程序继续运行，计算机仍分配给此用户。用户可以重新连接同一计算机。
5. 要向用户发送消息，请选择会话、计算机或用户，然后在“操作”窗格中选择**发送消息**。输入消息。

您可以将桌面操作系统计算机的电源状态计时器配置为自动处理未使用的会话。有关详细信息，请参阅“对计算机进行电源管理”部分。

配置交付组中的会话预启动和会话延迟

只有服务器操作系统计算机支持这些功能。

会话预启动和会话延迟功能在用户请求会话之前启动会话（会话预启动）、在用户关闭所有应用程序之后使应用程序会话保持活动状态（会话延迟），从而帮助指定用户快速访问应用程序。

默认情况下，不使用会话预启动和会话延迟：会话在用户启动应用程序时启动，在会话中最后一个开启的应用程序关闭之前保持活动状态。

注意事项：

- 交付组必须支持应用程序，而且计算机必须运行 VDA for Windows Server OS（最低版本为 7.6）。

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

- 这些功能仅在使用 Citrix Receiver for Windows 时受支持，而且还需其他 Citrix Receiver 配置。有关说明，请在您的 Citrix Receiver for Windows 版本的产品文档中搜索会话预启动。
- 请注意，不支持 Citrix Receiver for HTML5。
- 使用会话预启动时，如果用户的计算机置于“挂起”或“休眠”模式，预启动将不起作用（与会话预启动设置无关）。用户可以锁定其计算机/会话，但是，如果用户从 Citrix Receiver 中注销，会话将终止，预启动不再应用。
- 使用会话预启动时，物理客户端计算机无法使用挂起或休眠电源管理功能。客户端计算机用户可以锁定其会话，但不应注销。
- 预启动和延迟的会话会占用许可证，但仅在连接时占用。默认情况下，未使用的预启动和延迟会话在 15 分钟后断开连接。此值可在 PowerShell (New/Set-BrokerSessionPreLaunch cmdlet) 中配置。
- 对于自定义这些功能以实现互补而言，认真规划和监视用户的活动模式至关重要。最佳配置可以根据使用中许可证和已分配资源的成本，来平衡可供用户使用的早期应用程序的诸多优势。
- 也可以在 Citrix Receiver 中配置每天预定时刻的会话预启动。

未使用的预启动会话和延迟会话保持活动状态的时长

如果用户未启动应用程序，可以通过多种方法指定未使用的会话保持活动状态的时长：已配置的超时和服务器负载阈值。您可以配置上述全部项；首先发生的事件会导致未使用的会话结束。

- **超时：**配置的超时指定未使用的预启动或延迟会话保持活动状态的分钟数、小时数或天数。如果您配置的超时过短，预启动会话将在用户感受到应用程序访问速度加快之前便结束。如果您配置的超时过长，传入的用户连接可能因服务器资源不足而被拒绝。

  您无法从 Studio 禁用此超时，但可以在 SDK (New/Set-BrokerSessionPreLaunch cmdlet) 中禁用它。如果您禁用该超时，它将不会出现在该交付组的 Studio 显示或“Edit Delivery Group”（编辑交付组）向导中。

- **阈值：**如果服务器资源可用，根据服务器负载自动结束预启动和延迟会话可确保会话的开启时间尽可能长。未使用的预启动和延迟会话将不导致连接被拒绝，因为新用户会话需要资源时，它们不会自动结束。

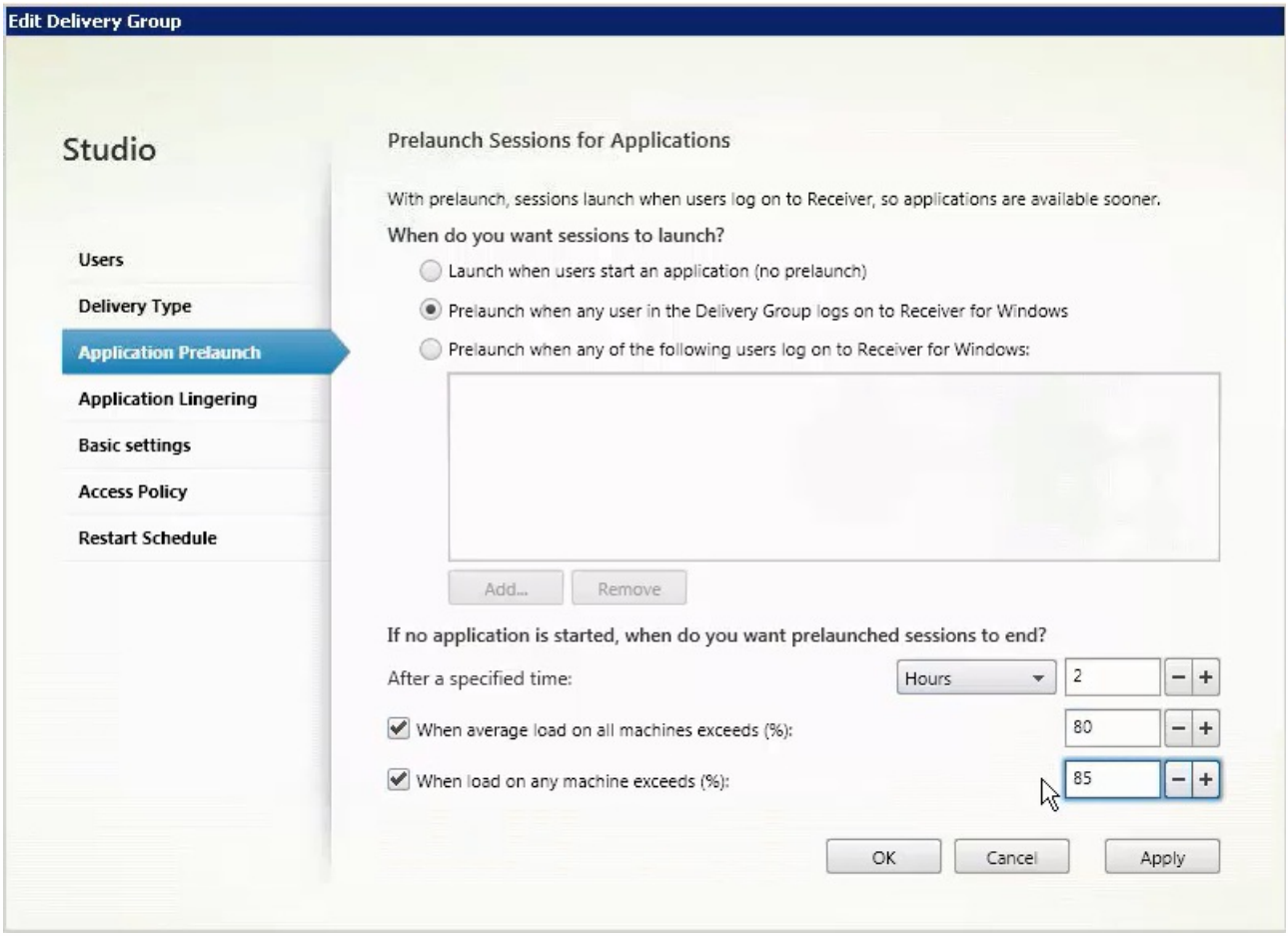
  您可以配置两个阈值：交付组中所有服务器的平均百分比负载和交付组中单个服务器的最大百分比负载。超过阈值时，时间最长的预启动或延迟会话将首先结束，其他会话则按分钟间隔逐个结束，直到负载降到阈值之下。（超过阈值时，不启动新的预启动会话）。

具有 VDA 且未向 Controller 注册的服务器和处于维护模式的服务器被视为全负载。计划外中断会导致预启动和延迟会话自动结束，从而释放容量。

启用会话预启动

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择交付组，然后在“操作”窗格中单击**编辑交付组**。
3. 在**应用程序预启动**页面上，通过选择何时应启动会话来启用会话预启动：
   - 当用户启动应用程序时。此为默认设置；会话预启动默认处于禁用状态。
   - 交付组中的任何用户登录到 Citrix Receiver for Windows 时。
   - 用户和用户组列表中的任何人登录到 Citrix Receiver for Windows 时。如果您选择此选项，请确保另外指定用户或用户组。

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



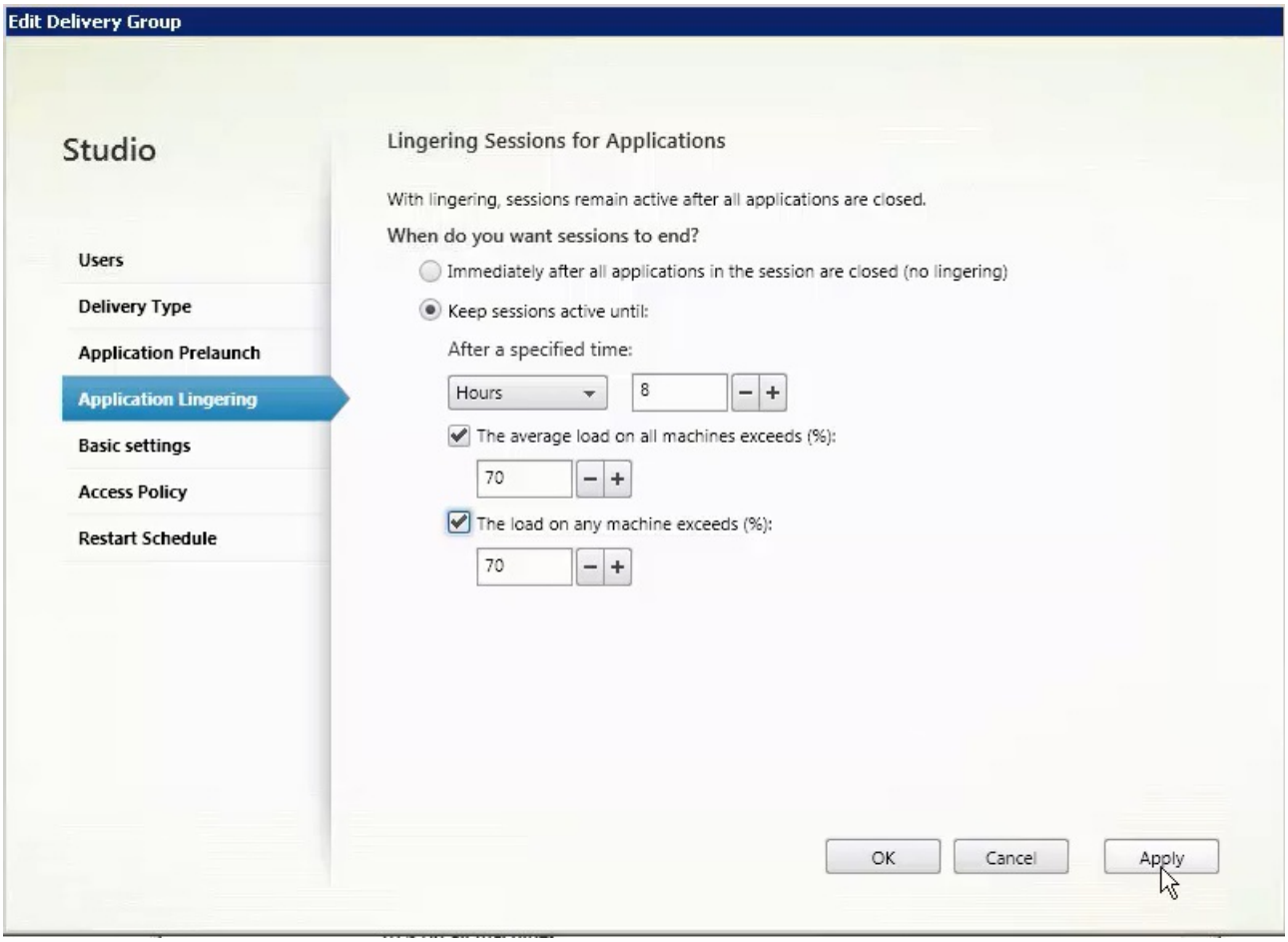
4. 当用户启动应用程序时，预启动会话由常规会话取代。如果用户未启动应用程序（预启动会话未使用），下列设置将影响会话保持活动状态的时长。
   - 经过指定的时间间隔时。您可以更改时间间隔（1-99 天、1-2376 小时或 1-142,560 分钟）。
   - 当交付组中所有计算机上的平均负载超过指定百分比 (1-99%) 时。
   - 当交付组中任一计算机上的负载超过指定百分比 (1-99%) 时。

   概述：预启动会话一直保持活动状态，直到下列任一事件发生：用户启动应用程序、经过指定的时间，或者超过指定的负载阈值。

启用会话延迟

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择交付组，然后在“操作”窗格中单击**编辑交付组**。
3. 在**应用程序延迟**页面上，通过选中**在此时间之前保持会话处于活动状态**单选按钮来启用会话延迟。

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



4. 如果用户未启动其他应用程序，有几项设置将影响延迟会话保持活动状态的时长。
   - 经过指定的时间间隔时。您可以更改时间间隔（1-99 天、1-2376 小时或 1-142,560 分钟）。
   - 当交付组中所有计算机上的平均负载超过指定百分比 (1-99%) 时。
   - 当交付组中任一计算机上的负载超过指定百分比 (1-99%) 时。

   概述：延迟会话一直保持活动状态，直到下列任一事件发生：用户启动应用程序、经过指定的时间，或者超过指定的负载阈值。

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

创建应用程序组

Dec 05, 2017

简介

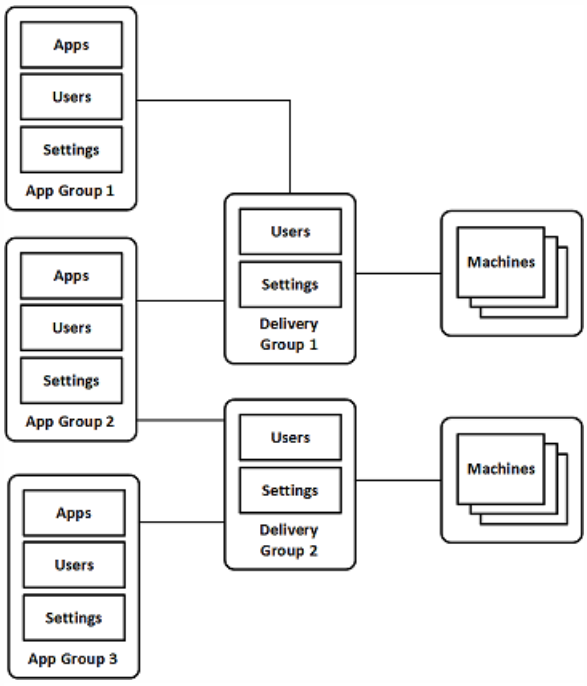
可以借助应用程序组管理应用程序的集合。可为在不同交付组之间共享的应用程序或由交付组中的部分用户使用的应用程序创建应用程序组。应用程序组是可选的；应用程序组提供向多个交付组添加相同的应用程序的备选方法。交付组可与多个应用程序组相关联，应用程序组可与多个交付组关联。

与使用多个交付组相比，使用应用程序组可以提供应用程序管理和资源控制优势：

- 通过对应用程序及其设置进行逻辑分组，可以作为一个单元来管理这些应用程序。例如，不需要一次向各个交付组中添加（发布）一个相同的应用程序。
- 在应用程序组之间共享会话可以节省占用的资源。在其他情况下，在应用程序组之间禁用会话共享可能非常有益。
- 可以使用*标记限制*功能从应用程序组发布应用程序，仅考虑所选交付组中的一部分计算机。通过使用标记限制，可以使用现有计算机来完成多个发布任务，从而节省与部署和管理其他计算机有关的成本。标记限制可以视为对交付组中的计算机进行划分（或分区）。对交付组中的一部分计算机进行隔离和故障排除时，将应用程序组或桌面与标记限制结合使用很有帮助。

示例 1

下图显示了一个包含多个应用程序组的 XenApp 或 XenDesktop 部署：



在此配置中，应用程序被添加到应用程序组中，而非添加到交付组中。交付组指定要使用的计算机。（虽然未显示，但计算机位于计算机目录中。）

应用程序组 1 与交付组 1 相关联。应用程序组 1 中的应用程序可以由在应用程序组 1 中指定的用户访问，只要这些应用程序同

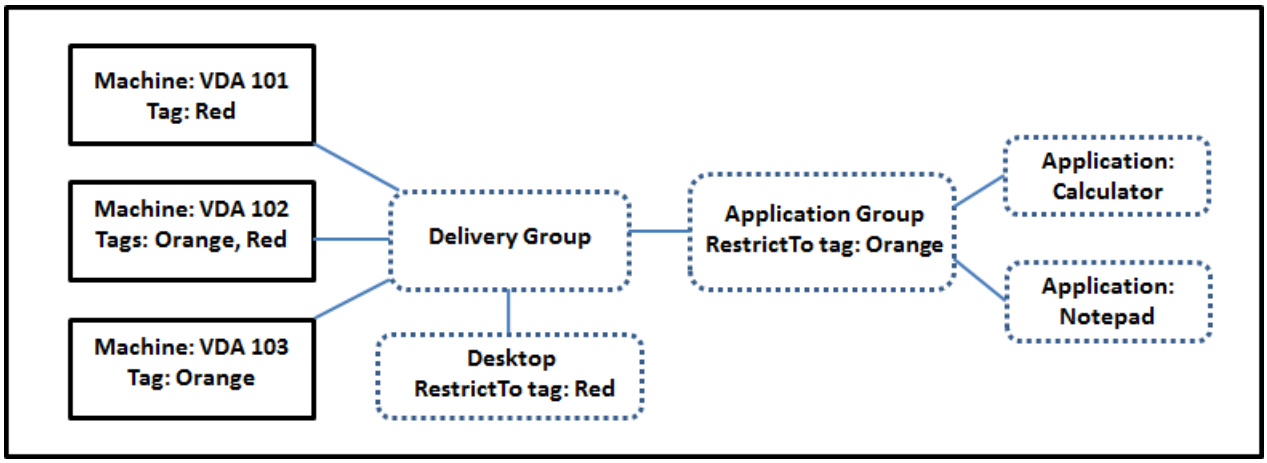
© 1999-2017 Citrix Systems, Inc. All rights reserved.

时位于交付组 1 的用户列表中。遵从的指导原则为：应用程序组的用户列表应属于相关联的交付组的用户列表的一部分（限制）。应用程序组 1 中的设置（例如，在应用程序组之间共享应用程序会话、相关联的交付组）适用于该组中的应用程序和用户。交付组 1 中的设置（例如，匿名用户支持）适用于应用程序组 1 和 2 中的用户，因为这些应用程序组已与该交付组相关联。

应用程序组 2 与两个交付组 1 和 2 相关联。可以在应用程序组 2 中为其中的每个交付组分配一个优先级，用于指示启动应用程序时交付组的检查顺序。优先级相等的交付组已实现负载平衡。应用程序组 2 中的应用程序可以由在应用程序组 2 中指定的用户访问，只要这些应用程序同时位于交付组 1 和交付组 2 的用户列表中。

示例 2：

此简单布局使用标记限制来限制哪些计算机将被考虑用于启动特定的桌面和应用程序。该站点有一个共享交付组、一个发布的桌面以及一个配置了两个应用程序的应用程序组。



已为所有三台计算机 (VDA 101-103) 添加了标记。

应用程序组创建时使用了“Orange”标记限制，因此它的所有应用程序（Calculator 和 Notepad）只能在该交付组中具有标记“Orange”的计算机（VDA 102 和 103）上启动。

有关将标记限制用于应用程序组（和用于桌面）的更全面的示例和指导，请参阅标记一文。

指导原则和注意事项

Citrix 建议您向应用程序组或交付组中添加应用程序，不要同时向两者中添加。否则，两种组类型中包含的应用程序的复杂性将增加，使其更加难以管理。

默认启用应用程序组。创建应用程序组后，可以编辑该组以更改此设置；请参阅管理应用程序组一文。

默认情况下，启用在应用程序组之间共享应用程序会话；请参阅下文在应用程序组之间共享会话。

Citrix 建议您将交付组升级到当前版本。这要求您依次执行以下操作：(1) 升级交付组中使用的计算机上安装的 VDA，(2) 升级包含这些计算机的计算机目录，(3) 升级交付组。有关详细信息，请参阅管理交付组。您的核心组件的最低版本必须为 7.9，才能使用应用程序组。

创建应用程序组需要交付组管理员内置角色的委派管理权限。有关详细信息，请参阅委派管理一文。

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

本文引用将一个应用程序与多个应用程序组相“关联”来区分该操作与从可用源中添加该应用程序的一个新实例。同样，多个交付组与多个应用程序组相关联（反之亦然），而非相互添加或作为对方的组件。

与应用程序组共享会话

启用了应用程序会话共享时，所有应用程序在同一应用程序会话中启动。这可节省与启动其他应用程序会话关联的成本，并允许使用涉及剪贴板的应用程序功能（例如复制粘贴操作）。但是，在某些情况下，您可能希望关闭会话共享。

使用应用程序组时，可以按以下三种方式配置应用程序会话共享，这些方式扩展了仅使用交付组时可用的标准会话共享行为：

- 在应用程序组之间已启用会话共享。
- 仅在同一应用程序组中的应用程序之间启用会话共享。
- 已禁用会话共享。

可以在应用程序组之间启用应用程序会话共享，也可以禁用它以将应用程序会话共享限制于仅同一应用程序组中的应用程序。

在应用程序组之间启用会话共享非常有用时的示例如下：

> 应用程序组 1 包含 Microsoft Office 应用程序，例如 Word 和 Excel。应用程序组 2 包含其他应用程序，例如记事本和计算器，这两个应用程序组都连接到同一个交付组。有权访问这两个应用程序组的用户通过启动 Word 启动一个应用程序会话，然后启动记事本。如果控制器发现运行 Word 的用户现有会话适合运行记事本，则在现有会话中启动记事本。如果无法从现有会话运行记事本（例如，如果标记限制将运行会话的计算机排除在外），则在合适的计算机上创建一个新会话，而不是使用会话共享。

在应用程序组之间禁用会话共享非常有用时的示例如下：

> 您有一组与同一计算机上安装的其他应用程序之间的互操作不顺畅的应用程序，例如，同一软件套件的两个不同的版本，或者同一 Web 浏览器的两个不同的版本。您不希望某个用户在同一会话中同时启动两个版本。
>
> 您为软件套件的每个版本分别创建一个应用程序组，并将软件套件的每个版本对应的应用程序添加到相应的应用程序组中。如果为其中每个应用程序组禁用了在组之间共享会话的功能，在这些组中指定的用户将能够在同一会话中运行同一版本的应用程序，并且同时仍然能够运行其他应用程序，只是不在同一会话中。如果该用户启动了版本不同的应用程序的其中一个版本（位于不同的应用程序组中），或者启动了未包含在应用程序组中的任何应用程序，该应用程序将在新会话中启动。

重要：在应用程序组之间共享会话的功能不属于安全沙盒功能。此功能非常复杂，并且无法阻止用户通过其他方式在其会话中启动应用程序（例如，通过 Windows 资源管理器）。

如果计算机已满载，则不会在其中启动新会话。将会根据需要使用会话共享在计算机上的现有会话中启动新应用程序（前提是这符合此处所述的会话共享限制）。

只能使预启动的会话可用于允许了应用程序会话共享的应用程序组。（使用会话延迟功能的会话可用于所有应用程序组。）必须在与应用程序组关联的每个交付组中启用和配置这些功能；不能在应用程序组中配置这些功能。

默认情况下，创建应用程序组时会在应用程序组之间启用会话共享；创建组时不能更改此行为。创建应用程序组后，可以编辑该组以更改此设置；请参阅管理应用程序组一文。

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

可以阻止同一应用程序组中的应用程序之间共享应用程序会话。

在应用程序组中禁用会话共享很有帮助时的示例如下：

> 您希望用户在单独的显示器上访问某个应用程序的多个同时进行的全屏会话。
>
> 可以创建一个应用程序组，并向其添加应用程序。如果在该应用程序组中的应用程序之间禁止会话共享，则当在其中指定的某个用户在另一个用户启动了一个应用程序之后启动它，则它们在单独的会话中启动，用户可以将各应用程序移到单独的显示器。

默认情况下，创建应用程序组时会启用应用程序会话共享；创建组时不能更改此行为。创建应用程序组后，可以编辑该组以更改此设置；请参阅管理应用程序组一文。

创建应用程序组

要创建应用程序组，请执行以下操作：

1. 在 Studio 导航窗格中选择**应用程序**，然后在“操作”窗格中选择**创建应用程序组**。
2. 此时将启动“创建应用程序组”向导，并打开一个**简介**页面，您可以在将来启动此向导时不再显示该页面。
3. 此向导将引导您完成下列页面。完成每个页面之后，请单击**下一步**，直到显示“摘要”页面为止。

系统会列出所有交付组，包括每个交付组包含的计算机数。

- **兼容的交付组**列表包含您能够选择的交付组。兼容的交付组包含随机（非永久分配或静态分配的）服务器或桌面操作系统计算机。
- **不兼容的交付组**列表包含您无法选择的交付组。每个条目都会解释不兼容的原因，例如，包含静态分配的计算机。

应用程序组可以与包含能够交付应用程序的共享（而非专用）计算机的交付组相关联。

还可以选择包含仅用于交付桌面的共享计算机的交付组，前提如下：(1) 交付组包含共享计算机，并且是通过早期的 XenDesktop 7.x 版本创建的，(2) 您具有“编辑交付组”权限。交付组类型在确认“创建应用程序组”向导时自动转换为“桌面和应用程序”。

虽然您能够创建没有关联交付组的应用程序组（或者能够组织整理应用程序或者用作当前未使用的应用程序的存储），但在至少指定一个交付组之前，不能使用应用程序组来交付应用程序。此外，如果未指定交付组，也不能从“开始”菜单源向应用程序组中添加应用程序。

所选交付组指定将用于交付应用程序的计算机。请选中要与应用程序组关联的交付组旁边的复选框。

要添加标记限制，请选择**限制启动带标记的计算机**，然后从下拉框中选择标记。请参阅标记一文了解完整的详细信息。

指定哪些人能够使用应用程序组中的应用程序。可以允许您在上一页面中选择的交付组中的所有用户和用户组使用，也可以从这些交付组中选择特定用户和用户组。如果限制为由指定的用户使用，则只有在交付组和应用程序组中指定的用户能够访问此应用程序组中的应用程序。实际上，应用程序组中的用户列表提供了一个与交付组中的用户列表有关的过滤器。

允许或禁止未经身份验证的用户使用应用程序功能仅在交付组中可用，在应用程序组中不可用。

指定了用户列表的位置

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

Active Directory 用户列表在您创建或编辑以下内容时指定：

- 交付组的授权用户列表（不通过 Studio 配置）。默认情况下，应用程序授权策略规则包括所有人；有关详细信息，请参阅 PowerShell SDK BrokerAppEntitlementPolicyRule cmdlet。
- 应用程序组用户列表。
- 交付组用户列表。
- 应用程序可见性属性。

能够通过 StoreFront 访问应用程序的用户的列表是由上述用户列表的交集组成的。例如，要将应用程序 A 配置为由特定部门使用，但不过分限制对其他组的访问，请执行以下操作：

- 使用包括所有人的默认应用程序授权策略规则。
- 配置交付组用户列表以允许所有总部用户使用在交付组中指定的任何应用程序。
- 配置应用程序组用户列表以允许管理部门和财务部门的成员访问名为 A 到 L 的应用程序。
- 配置应用程序 A 的属性，使其仅对行政和财务业务部的应收账款业务工作人员可见。

须知事项：

- 默认情况下，您添加的新应用程序将放置在“应用程序”文件夹中。可以指定其他文件夹。如果您尝试添加某个应用程序，但同一文件夹中已存在同名应用程序，则系统将提示您重命名要添加的应用程序。如果您同意使用建议的唯一名称，则会使用该新名称添加应用程序；否则，您必须先自己重命名该应用程序，才能添加。有关详细信息，请参阅管理应用程序文件夹。
- 您可以在添加时更改应用程序的属性（设置），或者在以后更改。请参阅更改应用程序属性。如果向同一用户发布同名的两个应用程序，请在 Studio 中更改“应用程序名称(面向用户)”属性；否则，用户将在 Citrix Receiver 中看到重复的名称。
- 如果要将一个应用程序添加到多个应用程序组中，但您没有足够的权限查看所有这些应用程序组中的应用程序，则会产生可见性问题。在这种情况下，可以咨询权限更高的管理员，或者扩展您的作用域，使其包括将应用程序添加到的所有组。

单击**添加**下拉菜单以显示应用程序源。

源	说明
从“开始”菜单	在计算机上发现的位于选定交付组中的应用程序。当您选择该源时，会打开一个新页面，其中包含已发现的应用程序的列表。选中要添加的应用程序的复选框，然后单击**确定**。 在下列情况下不能选择此源：(1) 您选择的应用程序组不与交付组关联，(2) 选择的应用程序组与不包含任何计算机的交付组关联，或者 (3) 选择的交付组不包含任何计算机。
手动定义	位于站点上或网络中的其他位置的应用程序。如果选择此源，则会启动一个新页面，您可以在其中键入可执行文件路径、工作目录、可选命令行参数以及显示给管理员和用户的名称。输入此信息后，请单击**确定**。
现有	以前添加到站点的应用程序。当您选择该源时，会打开一个新页面，其中包含已发现的应用程序的列表。选中要添加的应用程序的复选框，然后单击**确定**。 如果站点没有任何应用程序，则无法选择此源。

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

App-V	App-V 软件包中的应用程序。如果选择此源，则会启动一个新页面，您可以在其中选择 App-V 服务器或应用程序库。从生成的显示内容中，选中要添加的应用程序的复选框，然后单击**确定**。有关详细信息，请参阅 App-V 一文。 如果没有为站点配置 App-V，则无法选择此源（或者此源可能不显示）。

如前所述，如果没有该类型的有效源，则无法选择**添加**下拉菜单中的某些条目。不列出不兼容的源（例如，无法向应用程序组中添加应用程序组，因此，在创建应用程序组时不会列出该源）。

仅当您以前创建了作用域时才会显示此页面。默认情况下，选择**全部**作用域。有关详细信息，请参阅委派管理一文。

输入应用程序组的名称。还可以（选择性）输入说明。

查看摘要信息，然后单击**完成**。

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

管理应用程序组

Dec 05, 2017

在本文中：

- 简介
- 启用或禁用应用程序组
- 在应用程序组之间启用或禁用应用程序会话共享
- 在应用程序组中禁用应用程序会话共享
- 重命名应用程序组
- 添加、删除或更改与应用程序组的交付组关联的优先级
- 在应用程序组上添加、更改或删除标记限制
- 在应用程序组中添加或删除用户
- 更改应用程序组中的作用域
- 删除应用程序组

简介

本文介绍用于管理您创建的应用程序组的过程。

有关如何管理应用程序组或交付组中的应用程序的信息，包括如何执行以下操作的信息，请参阅应用程序：

- 在应用程序组中添加或删除应用程序。
- 更改应用程序组关联。

管理应用程序组需要具有交付组管理员内置角色的委派管理权限。有关详细信息，请参阅委派管理。

启用或禁用应用程序组

启用某个应用程序组时，可以提供已添加到该组中的应用程序。禁用某个应用程序组会禁用该组中的每个应用程序。但是，如果这些应用程序同时与其他已启用的应用程序组相关联，则可以从相应组中提供这些应用程序。同样，如果已将该应用程序显式添加到与应用程序组关联的交付组（添加到应用程序组除外），禁用应用程序组不会影响这些交付组中的应用程序。

创建应用程序组时会将其启用；无法在创建组时更改此行为。

1. 在 Studio 导航窗格中选择**应用程序**。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择**编辑应用程序组**。
3. 在**设置**页面上，选中或取消选中**启用应用程序组**复选框。
4. 单击**应用**以应用您所做的任何更改并保持打开窗口，或单击**确定**应用更改并关闭窗口。

在应用程序组之间启用或禁用应用程序会话共享

创建应用程序组时会在应用程序组之间启用会话共享；创建组时不能更改此行为。有关应用程序会话共享的详细信息，请参阅在应用程序组之间共享会话。

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

1. 在 Studio 导航窗格中选择**应用程序**。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择**编辑应用程序组**。
3. 在**设置**页面上，选中或取消选中**在应用程序组之间启用应用程序会话共享**复选框。
4. 单击**应用**以应用您所做的任何更改并保持打开窗口，或单击**确定**应用更改并关闭窗口。

在应用程序组中禁用应用程序会话共享

创建应用程序组时，默认情况下，在同一应用程序组中的应用程序之间启用会话共享。如果在应用程序组之间禁用应用程序会话共享，同一应用程序组中的应用程序之间会话共享保持启用状态。可以使用 Broker PowerShell SDK 为应用程序组配置在其所含应用程序之间禁用应用程序会话共享。某些情况下可能需要这样：例如，您可能希望用户在单独的显示器上完整大小的应用程序窗口中启动非无缝应用程序。有关应用程序会话共享的详细信息，请参阅与应用程序组共享会话。

在应用程序组中禁用应用程序会话共享时，该组中的每个应用程序都在新的应用程序会话中启动。如果有一个运行同一个应用程序的已断开连接的合适会话可用，则将其重新连接。例如，如果您启动记事本，此时有一个运行记事本的已断开连接会话，则将重新连接该会话，而不是创建新会话。如果有多个已断开连接的合适会话，则以随机但确定性的方式选择其中一个会话进行重新连接：如果在相同情况下再次出现这种情形，则选择同一会话，但在其他情况下，会话不一定可预测。
可以使用 Broker PowerShell SDK 来对某个现有应用程序组中的所有应用程序禁用应用程序会话共享，或创建禁用应用程序会话共享的应用程序组。

要禁用会话共享，请使用 Broker PowerShell cmdlet **New-BrokerApplicationGroup** 或 **Set-BrokerApplicationGroup**，并将参数 **-SessionSharingEnabled** 设置为 False，将参数 **-SingleAppPerSession** 设置为 True。

例如，要创建对所含所有应用程序禁用应用程序共享会话的应用程序组：

```
New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -SingleAppPerSession $True
```

例如，要在某个现有应用程序组中的所有应用程序之间禁用应用程序共享会话：

```
Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -SingleAppPerSession $True
```

- 要启用 SingleAppPerSession 属性，必须将 SessionSharingEnabled 属性设置为 False。不能同时启用这两个属性。SessionSharingEnabled 参数是指在应用程序组之间共享会话。
- 应用程序会话共享只适用于与应用程序组关联的应用程序，而不是与交付组关联的应用程序。（默认情况下，直接与交付组关联的所有应用程序共享会话。）
- 如果某个应用程序分配到多个应用程序组，请确保这些组的设置没有冲突（例如，一个组的选项设置为 True，另一个组的选项设置为 False），否则将导致发生不可预测的行为。

重命名应用程序组

1. 在 Studio 导航窗格中选择**应用程序**。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择**重命名应用程序组**。
3. 指定新的唯一名称，然后单击**确定**。

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

添加、删除或更改与应用程序组的交付组关联的优先级

应用程序组可以与包含能够交付应用程序的共享（而非专用）计算机的交付组相关联。

还可以选择包含仅用于交付桌面的共享计算机的交付组，前提如下：(1) 交付组包含共享计算机，并且是通过早期的 XenDesktop 7.x 版本创建的，(2) 您具有“编辑交付组”权限。交付组类型在确认“编辑交付组”对话框时自动转换为“桌面和应用程序”。

1. 在 Studio 导航窗格中选择**应用程序**。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择**编辑应用程序组**。
3. 选择**交付组**页面。
4. 要添加交付组，请单击**添加**。选中可用交付组对应的复选框。（不能选择不兼容的交付组。）完成选择后，单击**确定**。
5. 要删除交付组，请选中要删除的组对应的复选框，然后单击**删除**。出现提示后，确认删除。
6. 要更改交付组的优先级，请选中交付组对应的复选框，然后单击**编辑优先级**。输入优先级（0 = 最高优先级），然后单击**确定**。
7. 单击**应用**以应用您所做的任何更改并保持打开窗口，或单击**确定**应用更改并关闭窗口。

在应用程序组上添加、更改或删除标记限制

重要：添加、更改和删除标记限制可能会对被考虑用于启动应用程序的计算机有意外的影响。请务必查看标记一文中的考虑事项和警告。

1. 在 Studio 导航窗格中选择**应用程序**。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择**编辑应用程序组**。
3. 选择**交付组**页面。
4. 要添加标记限制，请选择**限制启动带标记的计算机**，然后从下拉框中选择标记。
5. 要更改或删除标记限制，请从下拉框中选择一个不同的标记，或通过清除**限制启动带标记的计算机**彻底删除标记限制。
6. 单击**应用**以应用您所做的任何更改并保持打开窗口，或单击**确定**应用更改并关闭窗口。

在应用程序组中添加或删除用户

有关用户的详细信息，请参阅创建应用程序组一文中的“用户”部分。

1. 在 Studio 导航窗格中选择**应用程序**。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择**编辑应用程序组**。
3. 选择**用户**页面。指出是允许关联交付组中的所有用户使用应用程序组中的应用程序，还是仅允许特定用户和组使用。要添加用户，请单击**添加**，然后指定要添加的用户。要删除用户，请选择一个或多个用户，然后单击**删除**。
4. 单击**应用**以应用您所做的任何更改并保持打开窗口，或单击**确定**应用更改并关闭窗口。

更改应用程序组中的作用域

仅当在创建作用域之后，才能更改作用域（不能编辑所有作用域）。有关详细信息，请参阅委派管理一文。

1. 在 Studio 导航窗格中选择**应用程序**。

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

2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择**编辑应用程序组**。
3. 选择**作用域**页面。选中或取消选中某个作用域旁边的复选框。
4. 单击**应用**以应用您所做的任何更改并保持打开窗口，或单击**确定**应用更改并关闭窗口。

删除应用程序组

一个应用程序必须至少与一个交付组或应用程序组相关联。如果尝试删除某个应用程序组，则会导致一个或多个应用程序不再属于某个组，并且系统会向您发出警告，指出删除该组还将删除这些应用程序。然后您可以确认或取消删除。

删除某个应用程序不会将其从原始源中删除，但是，如果要再次使其可用，则必须重新添加。

1. 在 Studio 导航窗格中选择**应用程序**。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择**删除组**。
3. 出现提示后，确认删除。

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

Remote PC Access

Dec 05, 2017

利用 Remote PC Access，最终用户几乎可以从任何地方远程登录到位于其办公室的物理 Windows PC。

办公室 PC 上安装有 Virtual Delivery Agent (VDA)，可将其注册到 Cloud Connector 或 Delivery Controller，并管理 PC 与最终用户客户端设备之间的 HDX 连接。Remote PC Access 支持自助模式；设置完允许用户访问的计算机白名单后，这些用户可以自己加入其办公室 PC，而无需管理员干预。通过在客户端设备上运行的 Citrix Receiver，用户可以从 Remote PC Access 桌面会话访问办公室 PC 上的应用程序和数据。

一个用户可以有多个桌面，包括多个物理 PC 或物理 PC 与虚拟桌面的组合。

注意：Remote PC Access 不支持睡眠模式和休眠模式。（针对本地 XenApp 和 XenDesktop 部署：Remote PC Access 仅对 XenDesktop 许可证有效；会话使用许可证的方式与其他 XenDesktop 会话一致。）

Active Directory 注意事项

在配置 Remote PC Access 部署站点之前，请设置组织单位 (OU) 和安全组，然后创建用户帐户。

如果在将计算机添加到计算机目录之后修改 Active Directory，Remote PC Access 将不会重新评估该分配。如果需要，可以将计算机手动重新分配到其他目录。

如果移动或删除 OU，用于 Remote PC Access 的 OU 将过时。VDA 可能不再与最合适的（甚至任何）计算机目录或交付组关联。

计算机目录和交付组注意事项

一台计算机只能同时分配到一个计算机目录和一个交付组。

可将计算机放置在一个或多个 Remote PC Access 计算机目录中。

为目录选择计算机帐户时，请选择最下面的适用 OU，以避免与另一计算机目录中的计算机发生冲突。例如，对于银行/主管/出纳，请选择“出纳”。

您可以通过单个或多个交付组分配一个 Remote PC Access 计算机目录中的所有计算机。例如，如果一组用户需要某些策略设置而另一组用户需要其他设置，则可以通过将用户分配给不同的交付组，来根据各个交付组过滤 HDX 策略。

如果您的 IT 基础结构根据地理位置、部门或其他类别分配服务用户的职责，您可以相应地对计算机和用户进行分组，以便允许进行委派管理。请确保管理员同时具有相关目录和相应交付组的权限。

部署注意事项

您可以先创建 Remote PC Access 部署，以后再添加传统虚拟桌面基础结构 (VDI) 桌面或应用程序。您还可以将 Remote PC Access 桌面添加到现有 VDI 部署中。

在办公室 PC 上安装 VDA 时，请考虑是否启用 Windows 远程协助复选框。此选项允许技术支持团队使用 Director 查看用户会

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

话，并通过 Windows 远程协助与用户会话进行交互。

请考虑如何将 VDA 部署到每台办公室 PC。Citrix 建议使用电子软件分发，例如 Active Directory 脚本和 Microsoft System Center Configuration Manager。安装介质中包含示例 Active Directory 脚本。

有关 Remote PC Acces 部署的信息，请查看安全注意事项。

Windows 10 当前支持适用于 Remote PC Access 的安全启动。

每台办公室 PC 必须使用有线网络连接加入到域。

办公室 PC 上支持 Windows 7 Aero，但不必使用该系统。

将键盘和鼠标直接连接到 PC 或便携式计算机上，而不能连接到可以关闭的显示器或其他组件上。如果必须将输入设备连接到显示器等组件上，则不应关闭这些组件。

如果使用的是智能卡，请参阅智能卡。

Remote PC Access 可以在大多数便携式计算机上使用。要提高可访问性并提供最佳连接体验，应根据台式 PC 的节能选项配置便携式计算机的节能选项。例如：

- 禁用休眠功能。
- 禁用睡眠功能。
- 将合盖操作设置为“不执行任何操作”。
- 将按下电源按钮的操作设置为“关闭”。
- 禁用显卡节能功能。
- 禁用网络接口卡节能功能。
- 禁用电池节能技术。

Remote PC Access 设备不支持以下操作：

- 插接和拔除便携式计算机。
- KVM 开关或其他可以断开会话的组件。
- 混合 PC，包括一体机和 NVIDIA Optimus 便携式计算机以及 PC。

Citrix 在安装了 Windows 10 的 Surface Pro 设备上支持 Remote PC Access。要提高可访问性并提供最佳连接体验，应以类似于台式或笔记本计算机的方式配置 Surface 设备。例如：

- 禁用休眠或睡眠功能
- 使用有线网络连接
- 在启动或重新连接会话时总是连接键盘
- 禁用电池节能技术

请在远程访问办公室 PC 的每个客户端设备上安装 Citrix Receiver。

远程访问同一办公室 PC 的多个用户在 Citrix Receiver 中可看到相同的图标。任何用户远程登录 PC 时，此资源显示为对其他用户不可用。

默认情况下，当本地用户在该计算机上启动会话时（通过按 CTRL+ATL+DEL），远程用户的会话自动断开连接。要阻止此自动操作，请在办公 PC 上添加以下注册表项，然后重新启动计算机。

小心：注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因“注册表编辑器”使用不当导致出现的问

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

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。

HKLM\SOFTWARE\Citrix\PortICA\RemotePC "SasNotification"=dword:00000001

在 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC 下进一步自定义此功能的行为

RpcaMode (dword):

1 = 如果远程用户没有在指定的超时期限内响应消息 UI，此用户将始终取胜。

2 = 本地用户将始终取胜。如果未指定此设置，默认情况下，远程用户始终取胜。

RpcaTimeout (dword):

向用户提供的时间（以秒为单位），超过此时间后，系统将确定要强制采用的模式。如果不指定此设置，默认值为 30 秒。此处的最低值应为 30 秒。用户必须重新启动计算机，才能使这些更改生效。

如果用户想要强制获取控制台访问权限：本地用户可以间隔 10 秒钟按 Ctr+Alt+Del 两次，以获取远程会话的本地控制权并强制断开连接。

更改注册表并重新启动计算机后，如果本地用户通过按 CTRL+ALT+DEL 登录到某个远程用户正在使用的 PC 上，此远程用户会收到提示，询问其是否接受本地用户的连接。允许此连接将会断开远程用户的会话连接。

Remote PC Access 和 HDX 3D Pro 模式

对于 Remote PC Access，通常使用标准 VDA 选项配置 VDA。对于配置有 HDX 3D Pro 的 Remote PC Access，可通过 Intel Iris Pro 和 NVIDIA GRID 和 Intel HD 5300 及更高版本 GPU（第 5 代 Intel 酷睿处理器和第 6 代 Intel 酷睿 i5 处理器）以及 NVIDIA Quadro 和NVIDIA GRIDGPU 支持显示器消隐功能。

有关详细信息，请参阅适用于 Windows 桌面操作系统的 GPU 加速。

局域网唤醒

注意：Citrix Cloud 中的 Renote PC Access 不支持局域网唤醒。

Remote PC Access 支持局域网唤醒功能，用户可以使用此功能远程开启物理 PC。借助此功能，用户可以在办公室 PC 不使用时将其关闭，以节约能源成本。用户还可以在计算机意外关闭（例如极端天气事件）时进行远程访问。

Remote PC Access 局域网唤醒功能在以下计算机上受支持：

- 在 BIOS 中启用了局域网唤醒功能的 PC。此支持包括唤醒代理和原始幻数据包，并且在使用 Microsoft System Cemter Configuration Manager (ConfigMgr) 2012、ConfigMgr 2012 R2 和 ConfigMgr 2016 时可用。
- 支持 Intel 主动管理技术 (AMT) 的 PC。在支持 AMT 的计算机上，局域网唤醒功能还支持在 Studio 和 Director 中执行强制关机和强制重启操作。此外，在 StoreFront 和 Citrix Receiver 中还可以使用“重新启动”操作。**重要：**AMT 支持仅在使用 ConfigMgr 2012 或 2012 R2 时可用，在使用 ConfigMgr 2016 时不可用。

将 ConfigMgr 配置为使用局域网唤醒功能。然后，当您使用 Studio 创建 Remote PC Access 部署（或添加另一个用于 Remote PC Access 的电源管理连接）时，请启用电源管理功能并指定 ConfigMgr 访问信息。

有关配置详细信息，请参阅 Configuration Manager 和 Remote PC Access 局域网唤醒。

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

要配置 Remote PC Access 局域网唤醒功能，请在办公室 PC 机上安装 VDA 之前完成以下操作：

- 在组织中配置 ConfigMgr 2012、2012 R2 或 2016。然后将 ConfigMgr 客户端部署到所有 Remote PC Access 计算机，从而使所安排的 SCCM 清单周期有时间运行（或在需要时强制运行一个周期）。在 Studio 中指定用来配置 ConfigMgr 连接的访问凭据必须包含该作用域中的集合以及 Remote Tools Operator 角色。
- 要支持 Intel 主动管理技术 (AMT)：
  - PC 上的最低受支持版本必须为 AMT 3.2.1。
  - 通过证书及相关置备进程置备 PC，以便使用 AMT。
  - 只能使用 ConfigMgr 2012 和 2012 R2，不能使用 ConfigMgr 2016。
- 要支持 ConfigMgr 唤醒代理和/或幻数据包功能：
  - 在每台 PC 的 BIOS 设置中配置局域网唤醒功能。
  - 要支持唤醒代理，请在 ConfigMgr 中启用该选项。对于组织中将使用 Remote PC Access 局域网唤醒功能的 PC 所属的每个子网，请确保有三台或更多的计算机可以作为标记计算机使用。
  - 要支持幻数据包功能，请将网络路由器和防火墙配置为允许使用子网定向的广播或单播发送幻数据包。

在办公室 PC 上安装 VDA 后，在创建连接和计算机目录时，请启用或禁用电源管理。

- 如果在目录中启用了电源管理，请指定详细的连接信息：ConfigMgr 地址和访问凭据以及连接名称。
- 如果不启用电源管理，可在以后添加电源管理 (Configuration Manager) 连接，然后编辑 Remote PC Access 计算机目录，以启用电源管理并指定新的电源管理连接。

可以编辑电源管理连接以配置高级设置。可以启用：

- ConfigMgr 提供的唤醒代理。
- 局域网唤醒（幻）数据包。如果启用局域网唤醒数据包，则可以选择局域网唤醒传输方法：“子网定向广播”或“单播”。

PC 使用 AMT 电源命令（如果支持）以及启用的任何高级设置。如果 PC 不使用 AMT 电源命令，则会使用高级设置。

Citrix Cloud 部署：配置顺序和注意事项

请参阅 CTX220737: How to Enable XenDesktop Remote PC Access in Citrix Cloud（CTX220737：如何在 Citrix Cloud 中启用 XenDesktop Remote PC Access）

本地部署：配置顺序和注意事项

创建 Remote PC Access 站点之前：

如果要使用 Remote PC Access 电源管理功能（又称 Remote PC Access 局域网唤醒），在 Studio 中创建 Remote PC Access 部署前，请在 PC 和 Microsoft System Center Configuration Manager (ConfigMgr) 上完成配置任务。有关详细信息，请参阅 Configuration Manager 和 Remote PC Access 局域网唤醒。

在站点创建向导中：

- 选择 Remote PC Access 站点类型。
- 在**电源管理**页面上，可以为默认 Remote PC Access 计算机目录中的计算机启用或禁用电源管理。如果启用电源管理，请指定 ConfigMgr 连接信息。
- 在**用户和计算机帐户**页面上，指定用户和计算机帐户。

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

创建 Remote PC Access 站点时会创建一个名为 Remote PC Access Machines 的默认计算机目录和一个名为 Remote PC Access Desktops 的默认交付组。

如果创建用于 Remote PC Access 的另一个计算机目录：

- 在**操作系统**页面上，选择“Remote PC Access”，然后选择一个电源管理连接。也可以选择不使用电源管理。如果尚未配置电源管理连接，可以在完成计算机目录创建向导后添加一个连接（连接类型 = Microsoft Configuration Manager 局域网唤醒），然后编辑该目录，指定该新连接。
- 在**计算机帐户**页面上，可以从显示的计算机帐户或组织单位 (OU) 中进行选择，也可以添加计算机帐户和 OU。

在用于本地和远程访问的办公室 PC 上安装 VDA。通常情况下，可通过使用软件包管理软件自动部署 VDA；但是，对于概念验证或小型部署，可以在每台办公室 PC 上手动安装 VDA。可以通过多种方式为 Remote PC Access 部署安装桌面 VDA。

使用完整产品或 VDAWorkstationSetup.exe 安装程序

- 图形界面：在向导的**环境**页面上选择 **Remote PC Access**。默认不选择**其他组件**页面上的组件。执行 Remote PC Access 操作不需要使用这些组件。
- 命令行界面：指定 /remotepc 选项。此选项阻止安装以下组件（等同于向导中的**其他组件**页面上的项目）：

  App-V
  Citrix User Profile Manager
  Citrix User Profile Manager WMI 插件
  Machine Identity Service
  Personal vDisk

  此外，也可以使用 /exclude 选项排除其中的每个组件。

使用 VDAWorkstationCoreSetup.exe 安装程序。Citrix Receiver 或任何其他组件都不能通过此安装程序安装。

安装 VDA 后，登录办公室 PC 上的控制台会话（在本地或通过 RDP）的下一个域用户将自动分配给 Remote PC Access 桌面。如果其他域用户登录控制台会话，这些用户也将添加到桌面用户列表，但需符合用户配置的限制。

要在 XenApp 或 XenDesktop 环境外部使用 RDP 连接，必须将用户或组添加到直接访问用户组。

指示用户在用于远程访问办公室 PC 的每台客户端设备上下载并安装 Citrix Receiver。可以从 http://www.citrix.com 或支持的移动设备的应用程序分发系统获取 Citrix Receiver。

故障排除

与 Remote PC Service 有关的诊断信息写入到 Windows 应用程序事件日志中。信息性消息不受限制。错误消息受限制，需删除重复消息。

- 3300（信息性消息）- 计算机已添加到目录
- 3301（信息性消息）- 计算机已添加到交付组
- 3302（信息性消息）- 计算机已分配给用户
- 3303（错误消息）- 异常

仅限本地部署：启用 Remote PC Access 电源管理时，子网定向广播可能无法启动与 Controller 不在同一子网上的计算机。如果需要使用子网定向广播跨子网管理电源且不支持 AMT，请尝试使用唤醒代理或“单播”方法（确保在电源管理连接的高级属性中启用这些设置）。

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

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

App-V

Dec 18, 2017

将 App-V 与 XenApp 和 XenDesktop 结合使用

利用 Microsoft Application Virtualization (App-V)，您可以将应用程序作为服务进行部署、更新及提供支持。这些应用程序无需安装在用户设备上即可供访问。借助 App-V 和 Microsoft User State Virtualization (USV)，用户无论身处何处，是否连接 Internet，均可对应用程序和数据进行访问。

下表列出了支持的版本。

App-V	XenDesktop 和 XenApp 版本	
	Delivery Controller	VDA
5.0 和 5.0 SP1	XenDesktop 7 至当前版本 XenApp 7.5 至当前版本	7.0 至当前版本
5.0 SP2	XenDesktop 7 至当前版本 XenApp 7.5 至当前版本	7.1 至当前版本
5.0 SP3 和 5.1	XenDesktop 7.6 至当前版本 XenApp 7.6 至当前版本	7.6.300 至当前版本
Windows Server 2016 中的 App-V	XenDesktop 7.12 至当前版本 XenApp 7.12 至当前版本	7.12 至当前版本

App-V 客户端不支持脱机访问应用程序。App-V 集成支持包括针对应用程序使用 SMB 共享。不支持 HTTP 协议。

如果您不熟悉 App-V，请参阅 Microsoft 文档。下面概述了本文提及的 App-V 组件：

- **管理服务器**。可提供一个中央控制台，用于管理 App-V 基础结构，并向 App-V 桌面客户端和远程桌面服务客户端交付虚拟应用程序。App-V 管理服务器将进行身份验证、发出请求并提供管理员所需的安全性、计量、监视及数据收集功能。服务器使用 Active Directory 和支持工具来管理用户和应用程序。
- **发布服务器**。可为 App-V 客户端提供适用于特定用户的应用程序，并托管要通过流技术推送的虚拟应用程序软件包。它从管理服务器提取应用程序包。
- **客户端**。检索虚拟应用程序、在客户端上发布应用程序以及在运行时自动设置和管理 Windows 设备上的虚拟环境。您可以在 VDA 上安装 App-V 客户端，用于存储特定用户的虚拟应用程序设置，例如各个用户的配置文件中的注册表和文件更改。

无需对操作系统设置进行任何预先配置或更改，即可无缝使用应用程序。可以从服务器操作系统和桌面操作系统交付组启动

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

App-V 应用程序：

- 通过 Citrix Receiver
- 从“开始”菜单
- 通过 App-V 客户端和 Citrix Receiver
- 同时由多个用户在多台设备上启动
- 通过 Citrix StoreFront

应用程序启动时，会实现修改的 App-V 应用程序属性。例如，对于修改过显示名称或具有自定义图标的应用程序，用户启动应用程序时会显示修改内容。

您可以使用通过 App-V Sequencer 创建的 App-V 软件包，并将这些软件包放在 App-V 服务器或网络共享上。

- **App-V 服务器：**使用 App-V 服务器上软件包中的应用程序，要求 Studio 和 App-V 服务器始终可以彼此通信，以便执行发现和配置操作并下载到 VDA。这样就会产生硬件、基础结构和管理开销。Studio 和 App-V 服务器必须始终保持同步，特别是对于用户权限来说更是如此。

  这种管理方法称为*双管理*，因为访问 App-V 软件包和应用程序需要同时使用 Studio 和 App-V 服务器控制台。这种方法最适合紧密耦合的 App-V 和 Citrix 部署环境。

- **网络共享：**将软件包放置在网络共享上，可以使 Studio 不再依赖于 App-V 服务器和数据库基础结构，从而降低了开销。（您仍然需要在每个 VDA 上安装 Microsoft App-V 客户端。）

  这种管理方法称为*单管理*，因为使用 App-V 软件包和应用程序只需要 Studio 控制台。您可以浏览到网络共享，并从此位置将一个或多个 App-V 软件包添加到站点级应用程序库中。

  应用程序库是一个 Citrix 术语，用于指代缓存存储库，该存储库可存储有关 App-V 软件包的信息。同时，应用程序库还可以存储有关其他 Citrix 应用程序交付技术的信息。

您可以使用其中一种管理方法，也可以同时使用这两种管理方法。换言之，在向交付组添加应用程序时，应用程序可能来自 App-V 服务器上的 App-V 软件包，也可能来自网络共享，或者同时来自这两者。

在 Studio 导航窗格中选择**配置 > App-V 发布**后，系统将显示 App-V 软件包名称和源。“源”列可指示软件包是位于 App-V 服务器上还是缓存在应用程序库中。选择一个软件包后，详细信息窗格会列出该软件包中的应用程序。

使用 App-V 单管理方法时，创建隔离组将允许您指定必须在沙盒中运行的互相依赖的应用程序组。该功能与 App-V 连接组相似，但并不完全一致。Citrix 使用“自动”和“显式”作为软件包部署选项，而非 App-V 管理服务器使用的强制和可选软件包术语。

- 用户启动 App-V 应用程序（主应用程序）时，会对隔离组进行搜索以查找其他标记为自动包含的应用程序软件包。这些软件包会自动下载并包含在隔离组中。您不必将其添加到包含主应用程序的交付组中。
- 只有在您已经将某个应用程序显式添加到包含主应用程序的同一个交付组的情况下，被标记为显式包含的隔离组中的该应用程序软件包才会下载。

这样，您可以创建包含各种全局适用于所有用户的自动包含应用程序的隔离组。此外，该组可以包含各种插件和其他（可能具有特定许可限制的）应用程序，您可以将其限制为某一组（通过交付组确定的）用户而无需创建更多的隔离组。

例如，应用程序“app-a”需要使用 JRE 1.7 才可运行。您可以创建一个包含 app-a（具有显式部署类型）和 JRE 1.7（具有自动部署类型）的隔离组。然后，将这些 App-V 软件包添加到一个或多个交付组中。用户启动 app-a 时，JRE 1.7 会通过它自动部

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

署。

可以将一个应用程序添加到多个 App-V 隔离组。但是，当用户启动该应用程序时，始终会使用该应用程序添加到的首个隔离组。无法对包含该应用程序的其他隔离组进行排序或优先级划分。

安装程序

下表按顺序总结了为在 XenApp 和 XenDesktop 中使用 App-V 而执行的设置任务。

管理方法		任务
单管理	双管理	
X	X	部署 App-V
X	X	打包和放置
	X	在 Studio 中配置 App-V 服务器地址
X	X	在 VDA 计算机上安装软件
X		向应用程序库添加 App-V 软件包
X		添加 App-V 隔离组（可选）
X	X	向交付组添加 App-V 应用程序

有关 App-V 部署说明，请访问 https://technet.microsoft.com/en-us/windows/hh826068。

（可选）更改 App-V 发布服务器设置。Citrix 建议在控制器上使用 SDK cmdlet。有关详细信息，请参阅 SDK 文档。

- 要查看发布服务器设置，请输入 **Get-CtxAppvServerSetting -AppVPublishingServer <*pubServer*>**。
- 要确保 App-V 应用程序正常启动，请输入 **Set-CtxAppvServerSetting –UserRefreshonLogon 0**。

如果您先前使用 GPO 策略设置管理发布服务器设置，则 GPO 设置会覆盖任何 App-V 集成设置，包括 cmdlet 设置。这样可能会导致 App-V 应用程序启动失败。Citrix 建议您先删除所有 GPO 策略设置，然后再使用 SDK 配置这些设置。

对于任一管理方法，请使用 App-V Sequencer 创建应用程序软件包。有关详细信息，请参阅 Microsoft 文档。

- 对于单管理方法，请确保将软件包放置在 UNC 或 SMB 共享网络位置上。确保向交付组添加应用程序的 Studio 管理员对该

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

位置至少具有读取访问权限。

- 对于双管理方法，请从 UNC 路径在 App-V 管理服务器上发布软件包。（不支持从 HTTP URL 发布。）

无论软件包是位于 App-V 服务器上还是位于网络共享上，请确保软件包都具有相应的安全权限，以使 Studio 管理员可以访问它们。必须与“已通过身份验证的用户”共享网络共享以确保默认情况下 VDA 和 Studio 具有读取权限。

> ## Important
>
> Citrix 建议在 Controller 上使用 PowerShell cmdlet 指定 App-V 服务器地址（如果这些服务器使用非默认属性值）。有关详细信息，请参阅 SDK 文档。如果要在 Studio 中更改 App-V 服务器地址，您指定的某些服务器连接属性可能会重置为默认值。这些属性在 VDA 上用于连接到 App-V 发布服务器。如果出现此情况，请重新配置服务器上所有已重置的属性的非默认值。

此过程仅适用于双管理方法。

在创建站点期间或创建之后，为双管理方法指定 App-V 管理和发布服务器地址。您可以在创建站点期间或创建之后执行此操作。

在创建站点期间：

在向导的 **App-V** 页面上，输入 Microsoft App-V 管理服务器的 URL 以及 App-V 发布服务器的 URL 和端口号。在继续向导之前，请测试此连接。如果测试失败，请参阅下文“故障排除”部分。

在创建站点之后：

1. 在 Studio 导航窗格中，选择**配置 > App-V 发布**。
2. 如果您先前未指定 App-V 服务器地址，请在“操作”窗格中选择**添加 Microsoft 服务器**。
3. 要更改 App-V 服务器地址，请在“操作”窗格中选择**编辑 Microsoft 服务器**。
4. 输入 Microsoft App-V 管理服务器的 URL 以及 App-V 发布服务器的 URL 和端口号。
5. 在关闭此对话框之前，请测试与这些服务器的连接。如果测试失败，请参阅下文“故障排除”部分。

之后，如果要删除指向 App-V 管理和发布服务器的所有链接，并阻止 Studio 从这些服务器中发现 App-V 软件包，请在“操作”窗格中选择**删除 Microsoft 服务器**。只有当目前没有在任何交付组中发布这些服务器上的软件包中的任何应用程序时，才允许执行此操作。如果已发布应用程序，您必须先从交付组中删除这些应用程序，然后才能删除 App-V 服务器。

包含 VDA 的计算机必须安装两组软件才能支持 App-V：一组来自 Microsoft，另一组来自 Citrix。

Microsoft App-V 客户端

此软件可检索虚拟应用程序、在客户端发布应用程序并在运行时自动设置和管理 Windows 设备上的虚拟环境。App-V 客户端可存储特定用户的虚拟应用程序设置，例如各个用户的配置文件中的注册表和文件更改。

App-V 客户端可从 Microsoft 获取。在包含 VDA 的每台计算机上或计算机目录用于创建 VM 的主映像上安装客户端。**注意**：Windows 10（1607 或更高版本）和 Windows Server 2016 已包括 App-V 客户端。请仅在这些操作系统中，通过运行 PowerShell **Enable-AppV** cmdlet（不带任何参数）来启用 App-V 客户端。**Get-AppVStatus** cmdlet 将检索当前的启用状态。

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

提示：在安装 App-V 客户端之后，请以管理员权限运行 PowerShell **Get-AppvClientConfiguration** cmdlet，并确保 EnablePackageScripts 设置为 1。如果未设置为 1，请运行 **Set-AppvClientConfiguration -EnablePackageScripts $true**。

Citrix App-V 组件

安装 VDA 时，会默认安装并启用 Citrix App-V 组件软件。

您可以在 VDA 安装过程中控制此默认操作。在图形界面中，取消选中**附加组件**页面上的 **Citrix Personalization for App-V - VDA** 复选框。在命令行接口中，将 **/exclude "Citrix Personalization for App-V - VDA"** 选项包括进来。

如果您在 VDA 安装过程中明确禁用了 Citrix App-V 组件的安装，但后来想使用 App-V 应用程序，请执行以下操作：在 Windows 计算机的“程序和功能”列表中，右键单击 **Citrix Virtual Delivery Agent** 条目，然后选择**更改**。此时将启动一个向导。在该向导中，请启用相应的选项以安装和启用 App-V 发布组件。

这些过程仅适用于单管理方法。

您必须对包含 App-V 软件包的网络共享至少具有读取访问权限。

向应用程序库添加 App-V 软件包

1. 在 Studio 导航窗格中，选择**配置** > **App-V 发布**。
2. 在“操作”窗格中，选择**添加包**。
3. 浏览到包含 App-V 软件包的共享并选择一个或多个软件包。
4. 单击**添加**。

从应用程序库删除 App-V 软件包

从应用程序库删除 App-V 软件包会将该软件包从 Studio App-V 发布节点显示中删除。但是，不会从交付组中删除其应用程序，这些应用程序仍然可以启动。该软件包仍会保留在其物理网络位置。（其效果与从交付组删除 App-V 应用程序是不同的。）

1. 在 Studio 导航窗格中，选择**配置** > **App-V 发布**。
2. 选择一个或多个要删除的软件包。
3. 在“操作”窗格中单击**删除包**。

添加一个 App-V 隔离组

1. 在 Studio 导航窗格中，选择 **App-V 发布**。
2. 在“操作”窗格中，选择**添加隔离组**。
3. 在**添加隔离组设置**对话框中，键入隔离组的名称和说明。
4. 从“可用软件包”列表中，选择您想要添加到隔离组中应用程序，然后单击右键。选定的应用程序现在应显示在“隔离组中的软件包”列表中。在每个应用程序旁边的**部署**下拉列表中，选择**显式**或**自动**。您也可以使用向上和向下箭头来更改列表中应用程序的顺序。
5. 操作完成后，单击**确定**。

编辑 App-V 隔离组

1. 在 Studio 导航窗格中，选择 **App-V 发布**。

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

2. 选择中间窗格中的**隔离组**选项卡，然后选择要编辑的隔离组。
3. 在“操作”窗格中选择**编辑隔离组**。
4. 在**编辑隔离组设置**对话框中，更改隔离组名称或说明，添加或删除应用程序，更改其部署类型，或更改应用程序顺序。
5. 操作完成后，单击**确定**。

删除 App-V 隔离组

删除隔离组不会删除应用程序软件包。只会删除分组。

1. 在 Studio 导航窗格中，选择 **App-V 发布**。
2. 选择中间窗格中的**隔离组**选项卡，然后选择要删除的隔离组。
3. 在“操作”窗格中选择**删除隔离组**。
4. 确认删除。

以下过程重点介绍如何向交付组添加 App-V 应用程序。有关创建交付组的完整详细信息，请参阅创建交付组。

步骤 1：选择您是要创建新的交付组还是要将 App-V 应用程序添加到现有交付组：

要创建包含 App-V 应用程序的交付组，请执行以下操作：

1. 在 Studio 导航窗格中选择**交付组**。
2. 在“操作”窗格中选择**创建交付组**。
3. 在一系列向导页面上，指定计算机目录和用户。

要将 App-V 应用程序添加到现有交付组，请执行以下操作：

1. 在 Studio 导航窗格中选择**应用程序**。
2. 在“操作”窗格中选择**添加应用程序**。
3. 选择要添加 App-V 应用程序的一个或多个交付组。

步骤 2：在向导的**应用程序**页面上，单击**添加**下拉列表以显示应用程序源。选择 **App-V**。

步骤 3：在**添加 App-V 应用程序**页面上，选择 App-V 源（App-V 服务器或应用程序库）。生成的显示内容包括应用程序名称及其软件包名称和软件包版本。选中要添加的应用程序旁边的复选框。然后，请单击**确定**。

步骤 4：完成向导。

须知事项：

- 如果在将 App-V 应用程序添加到交付组时更改了其属性，则所做更改将在应用程序启动时生效。例如，如果在将某个应用程序添加到组中时修改了其显示名称或图标，则在用户启动该应用程序时会显示所做的更改。
- 如果以后编辑包含 App-V 应用程序的交付组，而该组的交付类型从“桌面和应用程序”更改为“仅限应用程序”，则 App-V 应用程序性能不会发生变化。

故障排除

标有“（双）”的问题只有在使用双管理方法时才会发生。

（双）在 Studio 导航窗格中选择**配置** > **App-V 发布**时出现 PowerShell 连接错误。

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

- Studio 管理员是否同时是 App-V 服务器管理员？Studio 管理员必须属于 App-V 管理服务器上的“管理员”组才能与之通信。

（双）在 Studio 中指定 App-V 服务器地址时，测试连接操作返回错误。

- 是否已启动 App-V 服务器？请发送 Ping 命令或检查 IIS 管理器；每个 App-V 服务器均应处于“已启动”或“正在运行”状态。
- 是否已在 App-V 服务器上启用 PowerShell 远程处理？如果未启用，请参阅 http://technet.microsoft.com/zh-cn/magazine/ff700227.aspx。
- Studio 管理员是否同时是 App-V 服务器管理员？Studio 管理员必须属于 App-V 管理服务器上的“管理员”组才能与之通信。
- 是否已在 App-V 服务器上启用文件共享？在 Windows 资源管理器中或使用“运行”命令中输入 **\\<*App-V server FQDN*>**。
- App-V 服务器是否具有与 App-V 管理员相同的文件共享权限？在 App-V 服务器上的“Stored User Names and Passwords”（存储的用户名和密码）中为 \\<*App-V Server FQDN*> 添加一个条目，以指定对 App-V 服务器拥有管理员权限的用户的凭据。有关指南，请参阅 http://support.microsoft.com/kb/306541。
- App-V 服务器是否位于 Active Directory 中？

  如果 Studio 计算机与 App-V 服务器分别位于不存在信任关系的不同 Active Directory 域中，请从 Studio 计算机上的 PowerShell 控制台运行 **winrm s winrm/Config/client '@(TrustedHosts="<*App-V server FQDN*>")'**。

  如果 TrustedHosts 由 GPO 管理，将显示以下错误消息：“The config setting TrustedHosts cannot be changed because use is controlled by policies. The policy would need to be set to Not Configured to change the config setting.”（无法更改配置设置 TrustedHosts，因为使用受策略控制。策略需要设置为“未配置”才能更改配置设置）。在这种情况下，请在 GPO 的 TrustedHosts 策略中为 App-V 服务器名称添加一个条目（“管理模板”>“Windows 组件”>“Windows 远程管理(WinRM)”>“WinRM 客户端”）。

（双） 在将 App-V 应用程序添加到交付组时，发现失败。

- Studio 管理员是否同时是 App-V 管理服务器管理员？Studio 管理员必须属于 App-V 管理服务器上的“管理员”组才能与之通信。
- App-V 管理服务器是否正在运行？请发送 Ping 命令或检查 IIS 管理器；每个 App-V 服务器均应处于“已启动”或“正在运行”状态。
- 两个 App-V 服务器是否均已启用 PowerShell 远程处理？如果未启用，请参阅 http://technet.microsoft.com/zh-cn/magazine/ff700227.aspx。
- 软件包是否具有适当的安全权限以供 Studio 管理员访问？

App-V 应用程序不启动。

- （双）发布服务器是否正在运行？
- （双）App-V 软件包是否具有适当的安全权限以供用户访问？
- （双）在 VDA 上，确保 Temp 指向正确的位置，并且 Temp 目录具有足够的可用空间。
- （双）在 App-V 发布服务器上，运行 **Get-AppvPublishingServer *** 以显示发布服务器列表。
- （双）在 App-V 发布服务器上，确保 UserRefreshonLogon 设置为“False”。
- （双）在 App-V 发布服务器上，以管理员身份运行 **Set-AppvPublishingServer** 并将 UserRefreshonLogon 设置为“False”。
- VDA 上是否安装了受支持版本的 App-V 客户端？VDA 是否已启用“enable package scripts”（启用软件包脚本）设置？
- 在包含 App-V 客户端和 VDA 的计算机的“注册表编辑器” (regedit) 中，转到 HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppV。确保 AppVServers 注册表项的值采用以下格式：AppVManagementServer+metadata;PublishingServer（例如：http://xmas-demo-appv.blrstrm.com+0+0+0+1+1+1+0+1;http://xmas-demo-appv.blrstrm.com:8082）。
- 在包含 App-V 客户端和 VDA 的计算机或主映像上，检查 PowerShell ExecutionPolicy 是否已设置为“RemoteSigned”。Microsoft 提供的 App-V 客户端未进行签名，而此 ExecutionPolicy 允许 PowerShell 运行未签名的本地脚本和 cmdlet。请

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

使用以下两种方法之一设置 ExecutionPolicy：(1) 以管理员身份输入 cmdlet：**Set-ExecutionPolicy RemoteSigned**，或者 (2) 从“组策略”设置中，转到“计算机配置”>“策略”>“管理模板”>“Windows 组件”>“Windows PowerShell” >“启用脚本执行”。

如果这些步骤无法解决问题，则应启用并检查日志。

与 App-V 配置相关的所有日志均位于 C:\CtxAppvLogs 中。应用程序启动日志位于 %LOCALAPPDATA%\Citrix\CtxAppvLogs 中。LOCALAPPDATA 会解析为已登录用户的本地文件夹。检查应用程序启动失败的用户的本地文件夹。

要启用 App-V 所使用的 Studio 和 VDA 日志，您必须具有管理员权限。此外，您还需要使用文本编辑器（例如记事本）。

要启用 Studio 日志，请执行以下操作：

1. 创建文件夹 C:\CtxAppvLogs。
2. 转至 C:\Program Files\Citrix\StudioAppVIntegration\SnapIn\Citrix.Appv.Admin.V1。在文本编辑器中打开 CtxAppvCommon.dll.config，然后取消注释以下行：
3. 重新启动 Broker Service 以启动日志记录。

要启用 VDA 日志，请执行以下操作：

1. 创建文件夹 C:\CtxAppvLogs。
2. 转至 C:\Program Files\Citrix\Virtual Desktop Agent。在文本编辑器中打开 CtxAppvCommon.dll.config，然后取消注释以下行：
3. 取消注释以下行并将值字段设置为 1：
4. 重新启动计算机以启动日志记录。

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

AppDisk

Dec 05, 2017

概述

管理应用程序及其安装映像可能十分困难。Citrix AppDisk 为此提供了一种解决方案。AppDisk 可以将应用程序和应用程序组与操作系统分开，以便单独进行管理。

您可以创建不同的 AppDisk 来存放为各个用户组设计的应用程序，然后在您选择的主映像上将这些 AppDisk 组装起来。通过这种方式对应用程序进行分组和管理，可以帮助您更精细地控制应用程序，并减少要维护的主映像数量。这样可以简化 IT 管理并提高响应用户需求的速度。您可以通过交付组交付 AppDisk 中的应用程序。

如果您的部署还包括 Citrix AppDNA，您可以将其与 AppDisk 功能集成在一起；通过 AppDNA 可以让 XenApp 和 XenDesktop 自动分析每个 AppDisk 中的应用程序。使用 AppDNA 有助于充分发挥 AppDisk 的功能。如果没有此功能，则不会测试或报告应用程序兼容性。

AppDisk 在两方面与其他应用程序置备技术不同：隔离和变更管理。

- Microsoft App-V 可以通过隔离使不兼容的应用程序共存。而 AppDisk 功能不会隔离应用程序。它可以将应用程序（以及支持文件和注册表项）与操作系统分开。对于操作系统和用户来说，AppDisk 的外观和行为就像直接安装在主映像上一样。
- 变更管理（更新主映像并测试这些更新与已安装应用程序的兼容性）可能会花费巨大成本。AppDNA 报告有助于发现问题并提出修正步骤建议。例如，AppDNA 可以确定具有通用依赖项（如 .NET）的应用程序，以使您可以在一个通用基础映像中进行安装。此外，AppDNA 还可以确定在操作系统启动顺序早期加载的应用程序，以便您确保它们能够按预期运行。

须知事项：

- 更新映像后，由于验证以前安装的许可证的能力问题，有些应用程序可能无法正常运行。例如，升级映像后，启动 Microsoft Office 时可能显示与此类似的错误消息：

“Microsoft Office Professional Plus 2010 cannot verify the license for this application. A repair attempt failed or was canceled by the user, the application will not shut down.”（Microsoft Office Professional Plus 2010 无法验证此应用程序的许可证。修复尝试失败或被用户取消，应用程序将不会关闭。）

为了解决此问题，请卸载 Microsoft Office 并在基础映像上安装新版本。

- 在某些情况下，从 Windows 应用商店下载 Metro 应用程序到已发布的目录的虚拟机在很长一段时间后会失败。
- Citrix 建议始终将所有 Microsoft Office 组件置于同一 AppDisk 中。例如，一个 AppDisk 中存放具有 Project 的 Microsoft Office，另一个 AppDisk 中存放具有 Project 和 Visio 的 Microsoft Office。
- 在有些系统上，更新映像时 SCCM 会崩溃。对基础映像进行了更新并随后应用（这会导致 SCCM 客户端发生故障）时会发生这种情况。为了解决此问题，请先在基础映像中安装 SCCM 客户端实例。
- 在某些情况下，AppDisk 上安装的应用程序在其分配给交付组并分配了用户的虚拟机后，可能无法显示在 Windows“开始”菜单上。有关详细信息，请参阅应用程序如何在“开始”菜单中显示。
- 用户不会意识到应用程序与操作系统是分开的或 AppDisk 功能的任何其他方面。应用程序会像安装在映像上一样运行。如果 AppDisk 包含复杂应用程序，桌面启动可能会稍有延迟。
- 只能将 AppDisk 与托管共享池桌面结合使用。
- 您可以将 AppDisk 与托管共享桌面结合使用。
- 或许可以在不同的主映像和操作系统平台之间使每个应用程序共享 AppDisk；但是，并非所有应用程序都可以做到这一点。

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

如果您的应用程序使用适用于桌面操作系统的安装脚本，而该脚本会阻止这些应用程序在服务器操作系统上运行，则 Citrix 建议分别针对这两种操作系统对应用程序进行打包。

- 在许多情况下，AppDisk 可在不同的操作系统上运行。例如，您可以将在 Windows 7 VM 上创建的 AppDisk 添加到包含 Windows 2008 R2 计算机的交付组中，但前提是，这两个操作系统具有相同的位数（32 位或 64 位），并且都支持此应用程序。但是，Citrix 建议不要将在较高版本操作系统（如 Windows 10）上创建的 AppDisk 添加到包含运行较低版本操作系统（如 Windows 7）的计算机的交付组中，因为它可能无法正常运行。
- 如果要仅允许交付组中的一部分用户访问 AppDisk 的应用程序，Citrix 建议使用组策略对某些用户隐藏 AppDisk 中的应用程序。此时，仍然可以访问此应用程序的可执行文件，但这些用户无法运行它。
- 在运行 Windows 7 OS 的俄语和中文环境中，重新启动对话框无法自动消失；在这种情况下，登录到已交付的桌面后，重新启动对话框会显示并应该很快消失。
- 使用 **Upload-PvDDiags** 脚本工具时，如果用户的驱动器指定未设置为“P”，会缺少与 PVD 用户层相关的日志信息。
- 在设置为显示巴斯克语的环境中，Windows 7 OS 可能无法在重新启动提示屏幕上正确显示合适的语言。将语言设置为巴斯克语时，请确保已将法语或西班牙语安装为父语言，然后安装巴斯克语并将其设置为当前语言。
- 关闭计算机时，即使 PVD 磁盘设置只读模式，仍会弹出 PVD 更新提醒。
- 在原位升级过程中，可能会删除注册表文件 (DaFsFilter)，这会导致升级失败。

> **提示**
>
> 创建 AppDisk 时，请使用仅安装了操作系统的 VM（即，不包括其他应用程序）；操作系统应包含创建 AppDisk 之前的所有更新。

部署概述

下表总结了部署 AppDisk 的步骤。本文稍后将进行详细介绍。

1. 通过虚拟机管理程序管理控制台在 VM 上安装 Virtual Delivery Agent (VDA)。
2. 创建 AppDisk，其中包括完成虚拟机管理程序管理控制台和 Studio 中的步骤。
3. 通过虚拟机管理程序管理控制台在 AppDisk 上安装应用程序。
4. 封装 AppDisk（使用虚拟机管理程序管理控制台或 Studio）。通过封装，XenApp 和 XenDesktop 就可以将 AppDisk 的应用程序和支持文件记录在应用程序库 (AppLibrary) 中。
5. 在 Studio 中创建或编辑交付组，然后选择要包含的 AppDisk；此步骤称为*分配 AppDisk*（即使您在 Studio 中使用**管理 AppDisk** 操作也是如此）。当交付组中的 VM 启动时，XenApp 和 XenDesktop 会与 AppLibrary 进行协调，然后与 Machine Creation Services (MCS) 或 Provisioning Services (PVS) 以及 Delivery Controller 进行交互，以便在其中配置了 AppDisk 后对引导设备应用流技术。

要求

使用 AppDisk 时，除了系统要求一文所列要求之外，还需要满足其他一些要求。

AppDisk 功能仅在（至少）包含 XenApp 和 XenDesktop 7.8 下载中提供的 Delivery Controller 和 Studio 版本的部署中受支持，包括安装程序自动部署的必备项（例如 .NET 4.5.2）。

可以在 VDA 支持的相同 Windows 操作系统版本上创建 AppDisk。为要使用 AppDisk 的交付组选择的计算机必须至少安装 VDA 7.8 版。

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

Citrix 建议您使用最新版 VDA 安装或升级所有计算机，然后根据需要升级计算机目录和交付组。创建交付组时，如果选择安装了不同 VDA 版本的多台计算机，交付组将与最新版本的 VDA 兼容。（这就是所谓的组*功能级别*。）有关功能级别的详细信息，请参阅创建交付组一文。

要置备用于创建 AppDisk 的 VM，您可以使用：

- 配备 7.8 Controller（最低）的 MCS。
- 随您的 XenApp 和 XenDesktop 版本一起在下载页面上提供的 PVS 版本。
- 受支持的虚拟机管理程序：
  - XenServer
  - VMware（最低版本 5.1）
  - Microsoft System Center Virtual Machine Manager

不能将 AppDisk 与 XenApp 和 XenDesktop 支持的其他主机虚拟机管理程序和云服务类型结合使用。

对于 MCS 目录中的使用临时数据缓存功能的计算机而言，不支持创建 AppDisk。

> **注意**
>
> 可以使用写缓存将 AppDisk 附加到置备了 MCS 的计算机，但不能用于创建 AppDisk。

Remote PC Access 目录不支持 AppDisk。

必须在要创建 AppDisk 的 VM 上启用 Windows 卷影服务。默认情况下，此服务处于启用状态。

用于 AppDisk 的交付组可包含池随机计算机目录（含服务器操作系统或桌面操作系统计算机）中的计算机。不能将 AppDisk 与其他类型的目录中的计算机结合使用，例如池静态或专用（已分配）计算机目录。

除了任何其他已安装的 .NET 版本之外，安装 Studio 的计算机还必须安装 .NET Framework 3.5。

AppDisk 可能会影响存储。有关详细信息，请参阅存储和性能注意事项。

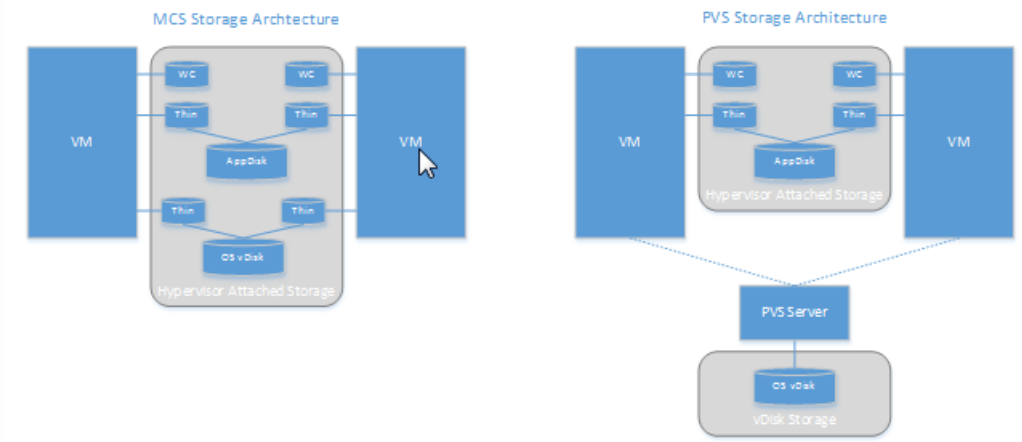
如果使用 AppDNA：

- 查看 AppDNA 文档和 AppDisk 常见问题解答。
- AppDNA 软件必须与 Controller 安装在不同的服务器上。请使用与此 XenApp 和 XenDesktop 版本一同提供的 AppDNA 版本。有关其他 AppDNA 要求，请参阅其文档。
- 在 AppDNA 服务器上，请确保对默认端口 8199 设置防火墙例外。
- 请勿在创建 AppDisk 时禁用 AppDNA 连接。
- 在创建 XenApp 或 XenDesktop 站点时，您可以通过站点创建向导的**附加功能**页面启用 AppDNA 的兼容性分析。另外，您也可以稍后在 Studio 导航窗格中选择**配置 > AppDNA** 来启用/禁用该功能。
- 单击 Studio 中的“查看问题报告”链接将显示 AppDNA 报告，但是，AppDNA 默认使用的操作系统组合为适用于桌面交付组的 Window 7 64 位和适用于服务器交付组的 Windows Server 2012 R2。如果您的交付组包含不同版本的 Windows，Studio 显示的报告中的默认映像组合将不正确。要解决此问题，请在 Studio 创建后手动编辑 AppDNA 中的解决方案。
- Studio 与 AppDNA 服务器的版本之间存在依赖关系。
  - 自版本 7.12 起，Studio 的版本必须与 AppDNA 服务器的版本相同，或者高于其版本。
  - 对于版本 7.9 和 7.11，Studio 的版本和 AppDNA 服务器的版本必须一致。
  - 下表概述了哪些版本可以一起运行（是 = 版本可以一起运行，- = 版本不能一起运行）：

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

Product Version	Studio 7.9	Studio 7.11	Studio 7.12	Studio 7.13	Studio 7.14	Studio 7.15
AppDNA 7.9	是	-	-	-	-	-
AppDNA 7.11	-	是	-	-	-	-
AppDNA 7.12	-	-	是	是	是	是
AppDNA 7.13	-	-	是	是	是	是
AppDNA 7.14	-	-	-	-	是	是
AppDNA 7.15	-	-	-	-	-	是

将应用程序与使用两个磁盘的操作系统分开并将这些磁盘存储在不同区域，可能会影响您的存储策略。下图展示了 MCS 和 PVS 存储体系结构。“WC”表示写入缓存，“Thin”表示用于存储 VM 的 AppDisk 和操作系统虚拟磁盘之间差异的精简磁盘。



在 MCS 环境下：

仍然可以按照企业现有的大小调整指导原则来平衡 AppDisk 和操作系统虚拟磁盘 (vDisk) 的大小。如果在多个交付组之间共享 AppDisk，则可以减少整体存储容量。

操作系统 vDisk 和 AppDisk 位于相同存储区域， 因此，请仔细规划您的存储容量需求，以避免在部署 AppDisk 时对容量产生任何负面影响。AppDisk 会产生开销，因此，请确保您的存储能够满足此开销和应用程序的要求。

由于操作系统 vDisk 和 AppDisk 位于相同存储区域，IOPS 不会受到影响。使用 MCS 时，无需考虑写入缓存。

在 PVS 环境下：

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

在将应用程序从 AppDisk 存储移动到与虚拟机管理程序连接的存储后，容量和 IOPS 会增加，您必须为此做出调整。

在 PVS 环境下，操作系统 vDisk 和 AppDisk 会使用不同存储区域。操作系统 vDisk 存储容量会减少，但与虚拟机管理程序连接的存储会增加。因此，为适应这些变更，应调整 PVS 环境的大小。

与虚拟机管理程序连接的存储中的 AppDisk 需要较高的 IOPS，而操作系统 vDisk 则需要较低的 IOPS。

写入缓存：PVS 会使用 NTFS 格式化的驱动器上的动态 VHDX 文件；在向写入缓存写入块时，VHDX 文件会动态扩展。在将 AppDisk 连接到相关 VM 后，它们会与操作系统 vDisk 进行合并，以便统一管理文件系统。此合并操作往往会导致将更多数据写入到写入缓存中，进而增加写入缓存文件的大小。在进行容量规划时，应考虑此问题。

无论是 MCS 还是 PVS 环境，请务必减少操作系统 vDisk 的大小，以便充分利用所创建的 AppDisk。否则，请计划使用更多的存储。

如果站点中的多位用户同时打开计算机（例如工作日开始），多个启动请求会对虚拟机管理程序造成压力，进而可能影响性能。对于 PVS，由于应用程序不在操作系统 vDisk 中，PVS 服务器收到的请求较少。因此，每个目标设备上的负载就比较轻，这样，PVS 服务器就可以推送到更多目标。但请注意，较高的目标服务器密度可能会对启动风暴性能造成负面影响。

创建 AppDisk

可以通过两种方法创建 AppDisk 并为其安装应用程序，然后对其进行封装。这两种方法都包括在虚拟机管理程序管理控制台和 Studio 中完成的步骤。这两种方法的不同之处在于，大多数步骤是在何处完成的。

无论使用哪种方法，请注意：

- 为 AppDisk 创建部分留出 30 分钟的时间。
- 如果使用 AppDNA，请按照上述要求部分中的指导进行操作。请勿在创建 AppDisk 时禁用 AppDNA 连接。
- 当您将应用程序添加到 AppDisk 时，确保为所有用户按照应用程序。重新装备使用密钥管理服务器 (KMS) 激活的任何应用程序。有关详细信息，请参阅相关应用程序文档。
- 在 AppDisk 创建期间在用户专用位置创建的文件、文件夹和注册表条目不会保留下来。此外，某些应用程序还会运行初次使用向导，以便在安装期间创建用户数据。请使用 Profile Management 解决方案来保留此数据，并防止每次启动 AppDisk 时都显示此向导。
- 如果正在使用 AppDNA，则在创建过程完成后会自动进行分析。在此间隔期间，AppDisk 在 Studio 中的状态为“正在分析”。

在 AppDisk 创建期间，由 Provisioning Services 创建的计算机目录中的计算机上的 AppDisk 还需要进行额外的配置。从 Provisioning Services 控制台中：

1. 创建与包含 VM 的设备集合相关的新版 vDisk。
2. 将 VM 置于维护模式。
3. 在 AppDisk 创建期间，每次重新启动 VM 时，请在引导屏幕上选择维护版本。
4. 封装 AppDisk 后，请将 VM 重新置于生产模式，然后删除所创建的 vDisk 版本。

此过程包括三项任务：创建 AppDisk、在 AppDisk 上创建应用程序以及封装 AppDisk。

创建 AppDisk：

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

1. 在 Studio 导航窗格中选择 **AppDisk**，然后在“操作”窗格中选择**创建 AppDisk**。
2. 查看向导的**简介**页面中的信息，然后单击**下一步**。
3. 在**创建 AppDisk** 页面中，选中**创建新 AppDisk** 单选按钮。选择预定义的磁盘大小（小型、中型或大型）或指定磁盘大小 (GB)；最小大小为 3 GB。磁盘大小应足以容纳要添加的应用程序。单击**下一步**。
4. 在**准备机**页面中，选择要用作主映像的随机池目录，AppDisk 将通过该主映像来构建。注意：此处会以列表形式显示站点中的所有计算机目录（按类型划分）；您只能选择至少包含一个可用计算机的目录。如果选择的目录不包含随机池 VM，AppDisk 创建将失败。从随机池目录选择 VM 后，请单击**下一步**。
5. 在**摘要**页面上，键入 AppDisk 的名称和说明。查看您在前面的向导页面中指定的信息。单击**完成**。

请记住：如果正在使用 PVS，请按照 PVS 注意事项中的指导进行操作。

向导关闭后，新 AppDisk 的 Studio 显示屏幕将指示“正在创建”。创建 AppDisk 后，显示屏幕将更改为“已准备好安装应用程序”。

在 AppDisk 上安装应用程序：

从您的虚拟机管理程序管理控制台中，在 AppDisk 上安装应用程序。（**提示：**如果忘记了 VM 的名称，请在 Studio 导航窗格中选择 **AppDisk**，然后在“操作”窗格中选择**安装应用程序**以显示其名称。）有关安装应用程序的信息，请参阅虚拟机管理程序文档。（**记住：**必须从您的虚拟机管理程序管理控制台中在 AppDisk 上安装应用程序。请勿使用 Studio 的“操作”窗格上的“安装应用程序”任务。）

封装 AppDisk：

1. 在 Studio 导航窗格中选择 **AppDisk**。
2. 选择所创建的 AppDisk，然后在“操作”窗格上选择**封装 AppDisk**。

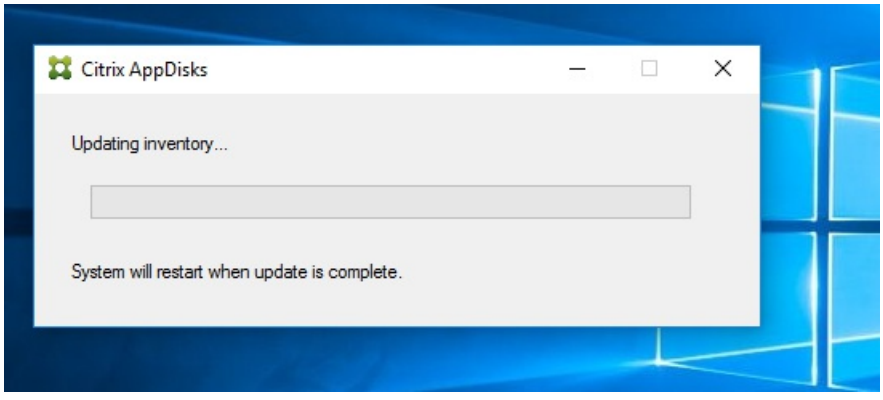
创建 AppDisk 后，请为其安装应用程序，然后对其进行封装，并分配到交付组。

取消 AppDisk 准备和封装

在某些情况下，管理员可能需要取消 AppDisk 创建和封装：

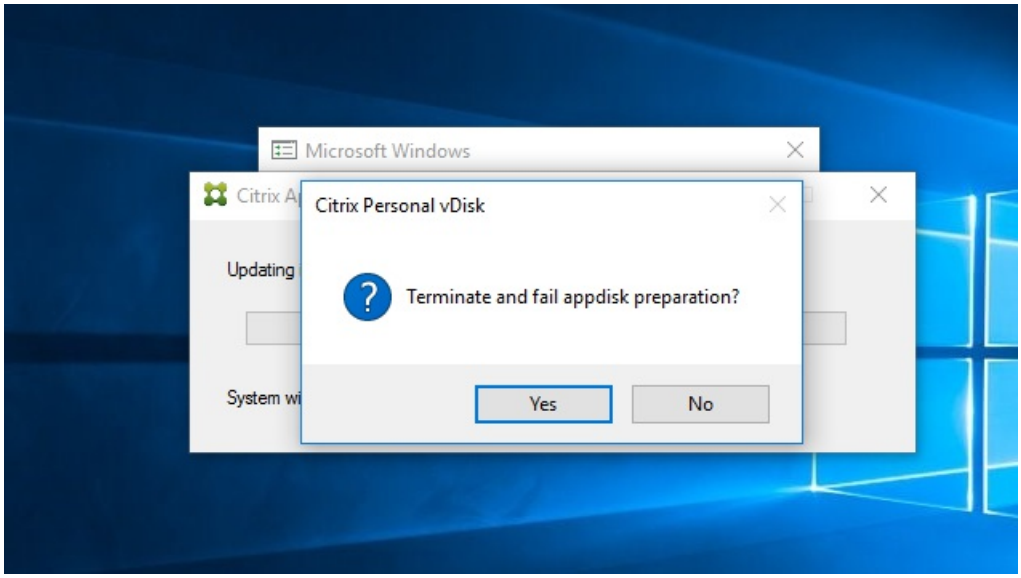
1. 访问 VM。

2. 关闭对话框：



3. 关闭对话框后，将显示一条弹出消息，请求验证以取消所选操作；请单击**是**。

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



注意

如果取消 AppDisk 操作，重新启动计算机会将其返回到初始状态，否则您需要创建一个干净的 VM。

在此过程中，您可以通过虚拟机管理程序管理控制台完成 AppDisk 创建和准备任务，然后将 AppDisk 导入到 Studio 中。

在虚拟机管理程序上准备、安装应用程序并封装 AppDisk：

1. 通过虚拟机管理程序管理控制台创建 VM 并安装 VDA。
2. 关闭计算机并创建快照。
3. 使用此快照创建新计算机，然后为其添加新磁盘。此磁盘将成为 AppDisk，其大小必须足以容纳要为其安装的所有应用程序。
4. 启动计算机，然后选择**启动 > 准备 AppDisk**。如果在虚拟机管理程序上没有“开始”菜单快捷方式，请运行 C:\Program Files\Citrix\personal vDisk\bin 打开命令提示窗口并键入：**CtxPvD.Exe –s LayerCreationBegin**。此时，计算机将重新启动并准备磁盘。在完成准备几分钟后，计算机将再次重新启动。
5. 安装要为用户提供的应用程序。
6. 双击计算机桌面的**打包 AppDisk** 快捷方式。此时，计算机将再次重新启动，并启动封装过程。当“in process”（正在处理）对话框关闭后，请关闭 VM 的电源。

使用 Studio 导入在虚拟机管理程序上创建的 AppDisk：

1. 在 Studio 导航窗格中选择 **AppDisk**，然后在“操作”窗格中选择**创建 AppDisk**。
2. 查看**简介**页面中的信息，然后单击**下一步**。
3. 在**创建 AppDisk**页面上，选中**导入现有 AppDisk**单选按钮。选择虚拟机管理程序上所创建的 AppDisk 所在的资源（网络和存储）。单击**下一步**。
4. 在**准备机**页面上，浏览到计算机，选择磁盘，然后单击**下一步**。
5. 在**摘要**页面上，键入 AppDisk 的名称和说明。查看您在前面的向导页面中指定的信息。单击**完成**。此时，Studio 将导入 AppDisk。

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

将 AppDisk 导入 Studio 后，请将其分配到交付组。

向交付组分配 AppDisk

您可以在创建交付组时向该交付组分配一个或多个 AppDisk，也可以在创建交付组之后再进行分配。您提供的 AppDisk 信息实际上是相同的。

要向正在创建的交付组添加 AppDisk，请按照“创建交付组”向导的 **AppDisk** 页面的指导进行操作。（有关此向导中其他页面的详细信息，请参阅创建交付组一文。

要在现有交付组中添加或删除 AppDisk，请执行以下操作：

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择交付组，然后在“操作”窗格中选择**管理 AppDisk**。请参阅 **AppDisk** 页面的以下指导信息。
3. 在交付组中更改 AppDisk 配置后，需要重新启动该组中的计算机。在**前滚策略**页面上，按照创建重新启动计划中的指导进行操作。

AppDisk 页面

“创建交付组”向导或“管理 AppDisk”流程中的 **AppDisk** 页面均会列出已为交付组部署的 AppDisk 及其优先级。（如果您正在创建交付组，则此列表为空。）有关详细信息，请参阅 AppDisk 优先级部分。

1. 单击**添加**。“选择 AppDisk”对话框将在左侧列中列出所有 AppDisk。已分配给此交付组的 AppDisk 所对应的复选框已被选中，因此无法选择。
2. 在左侧列中选中一个或多个可用 AppDisk 所对应的复选框。右侧列将列出 AppDisk 上的应用程序。（选择右侧列上方的**应用程序**选项卡可按照与“开始”菜单类似的方式列出应用程序；选择**已安装的软件包**选项卡可按照与“程序和功能”列表类似的方式列出应用程序。）
3. 选择一个或更多可用 AppDisk 后，请单击**确定**。
4. 在 AppDisk 页面上选择**下一步**。

如果为一个交付组分配了多个 AppDisk，则 **AppDisk** 页面（在“创建交付组”、“编辑交付组”和“管理 AppDisk”显示中）将按优先级降序顺序列出这些 AppDisk。此列表靠上的条目优先级较高。优先级是指处理 AppDisk 的顺序。

您可以使用与此列表相邻的向上和向下箭头更改 AppDisk 优先级。如果在 AppDisk 部署中集成了 AppDNA，则它会在将 AppDisk 分配到交付组时自动分析应用程序并设置优先级。之后，如果您要在该组中添加或删除 AppDisk，则可以单击 **Auto-Order**（自动排序）来指示 AppDNA 重新分析当前的 AppDisk 列表，然后确定优先级。此分析操作（以及必要的优先级重新排列）可能需要一段时间才能完成。

管理 AppDisk

在创建 AppDisk 并将其分配到交付组后，可以通过 Studio 导航窗格中的 AppDisk 节点更改 AppDisk 的属性。必须通过虚拟机管理程序管理控制台更改 AppDisk 中的应用程序。

> **Important**
>
> 可以使用 Windows 更新服务来更新 AppDisk 上的应用程序（例如 Office 套件）。但是，请勿使用 Windows 更新服务对 AppDisk 应

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

用操作系统更新。请对主映像（而不是 AppDisk）应用操作系统更新；否则，AppDisk 无法正确初始化。

- 在对 AppDisk 中的应用程序应用修补程序和其他更新时，只需应用这些应用程序所需的修补程序和其他更新。请勿应用其他应用程序的更新。
- 安装 Windows 更新时，请首先取消选择所有条目，然后选择要更新的 AppDisk 中的应用程序所需的条目。

针对 AppDisk 创建的防病毒注意事项

有些情况下，由于基础 VM 上安装了防病毒 (A/V) 代理，尝试创建 AppDisk 可能会遇到问题。在这种情况下，某些进程受 A/V 代理的阻碍时，AppDisk 创建可能会失败。必须将 **CtxPvD.exe** 和 **CtxPvDSrv.exe** 这些进程添加到基础 VM 使用的 A/V 代理的例外列表。

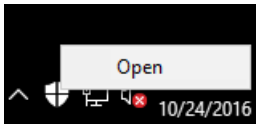
本节提供有关为以下防病毒应用程序添加例外的信息：

- Windows Defender（适用于 Windows 10）
- OfficeScan（版本 11.0）
- Symantec（版本 12.1.16）
- McAfee（版本 4.8）

如果基础 VM 使用 Windows Defender（版本 10）：

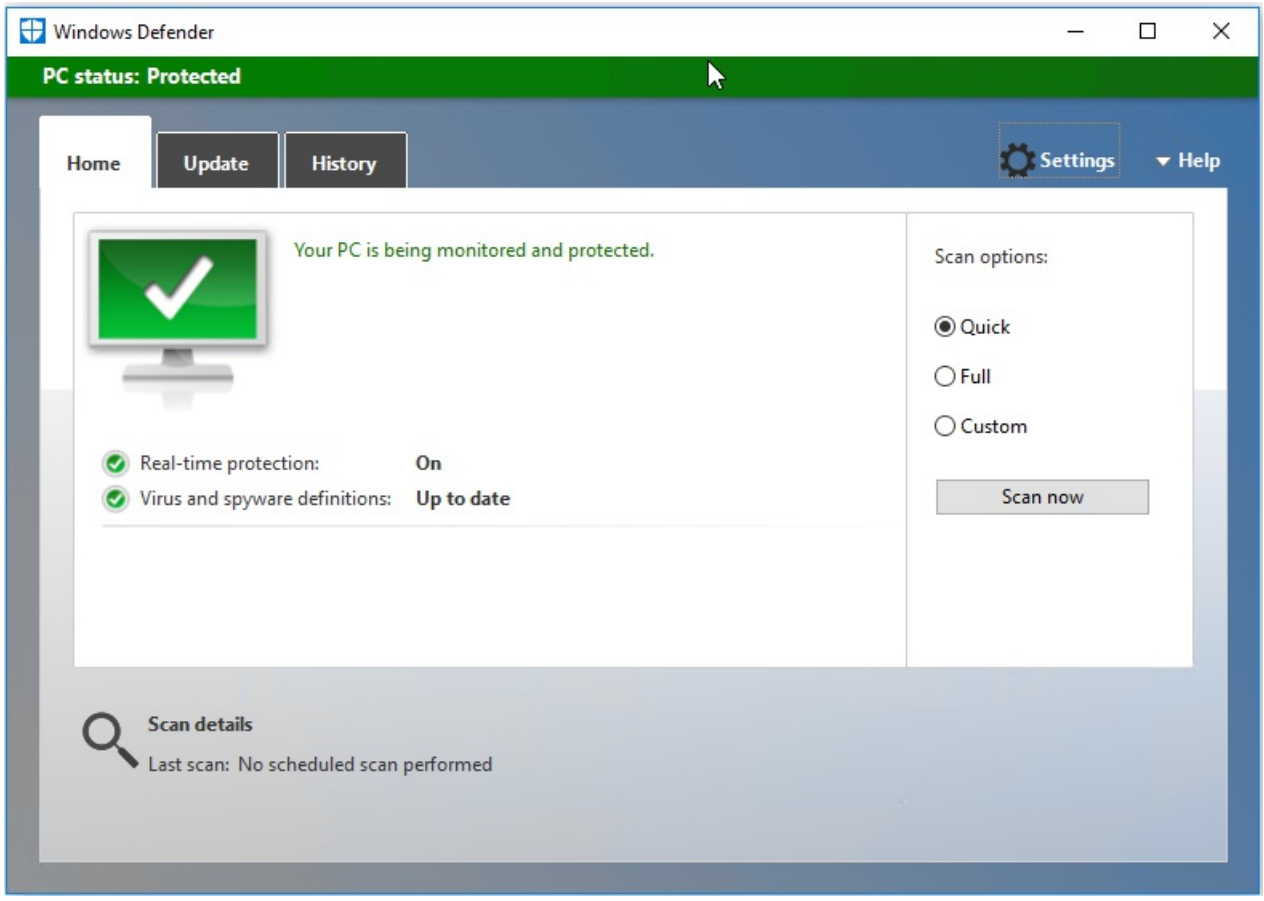
1. 使用本地管理员权限登录计算机。

2. 选择 Windows Defender 图标并单击右键以显示**打开**按钮：



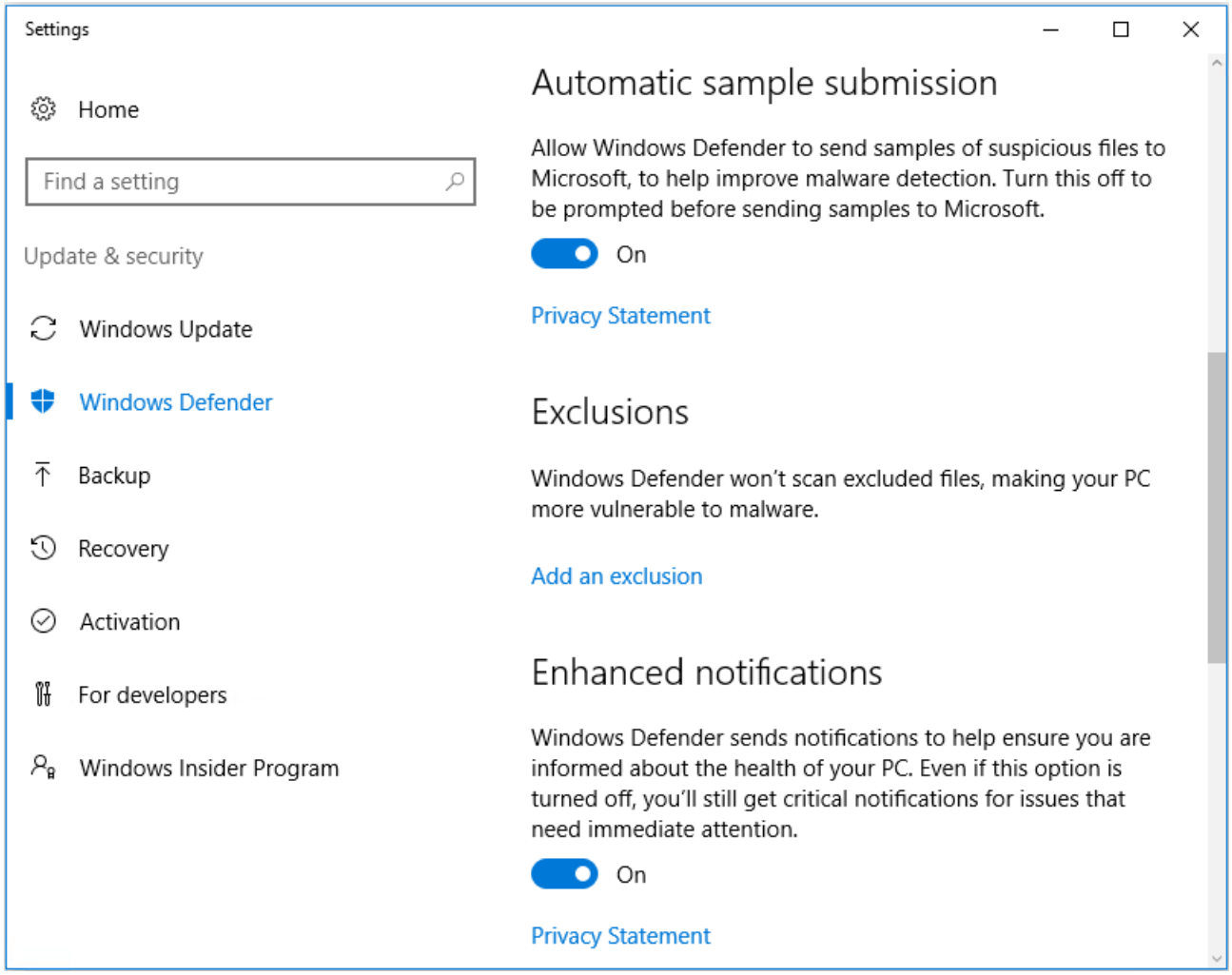
3. 在 Windows Defender 控制台中，选择界面右上部分的**设置**：

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



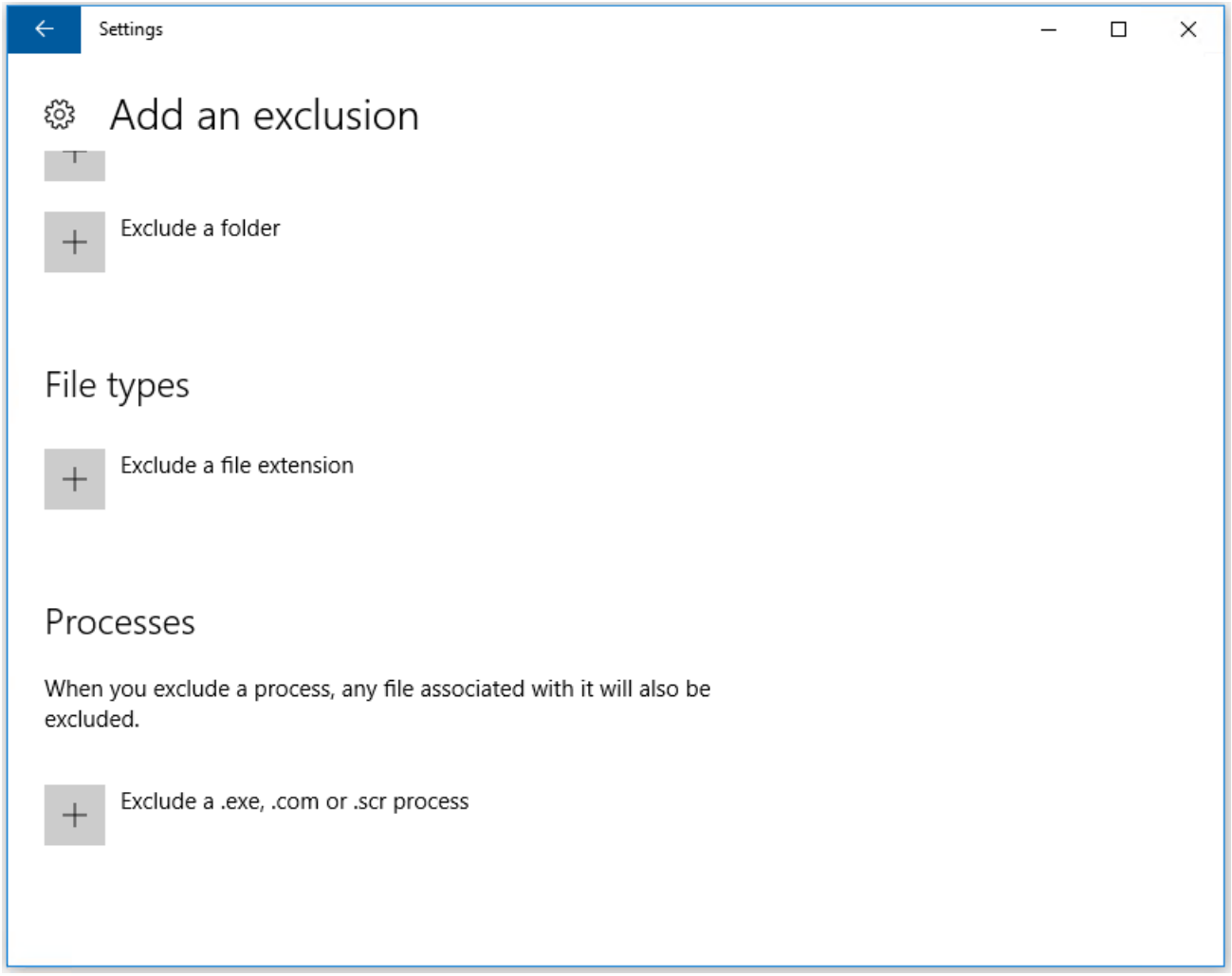
4. 在“设置”屏幕的**排除项**部分，单击**添加排除项**：

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

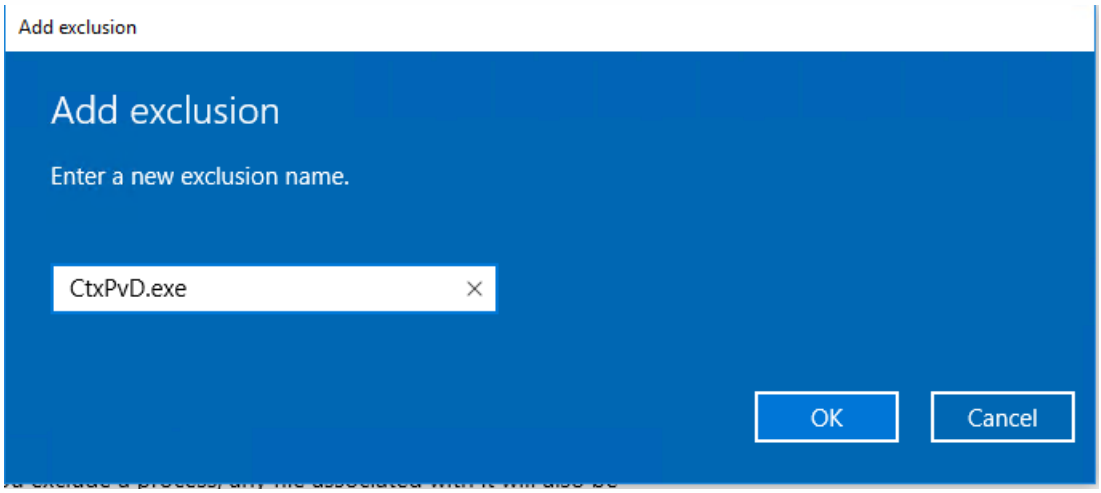


5. 在**添加排除项**屏幕中，选择**排除 .exe、.com 或 .scr 的进程**：

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

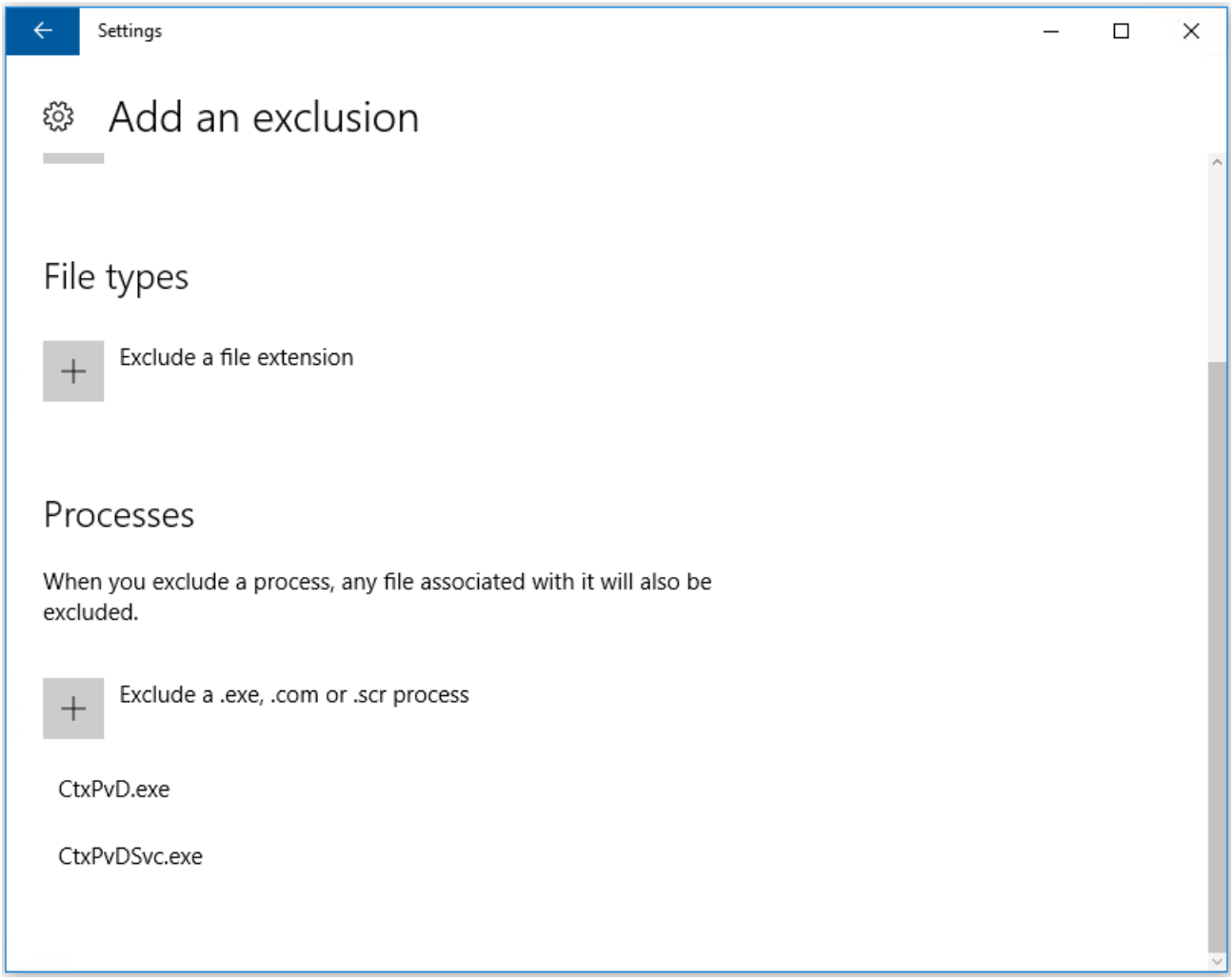


6. 在**添加排除项**屏幕中，输入排除的名称；必须添加 **CtxPvD.exe** 和 **CtxPvDSvc.exe** 以防止在创建 AppDisk 时发生冲突。输入排除名称后，单击**确定**：



添加排除项后，它们显示在**设置**屏幕中的已排除进程列表中：

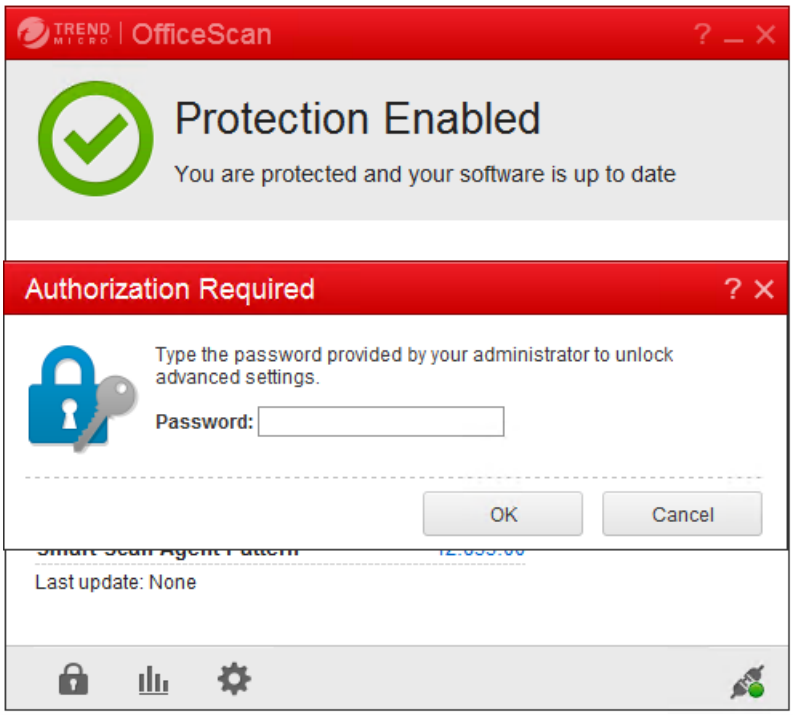
© 1999-2017 Citrix Systems, Inc. All rights reserved.



如果基础 VM 使用 OfficeScan（版本 11）：

1. 启动 OfficeScan 控制台。
2. 单击界面左下部分的锁图标，并输入密码：

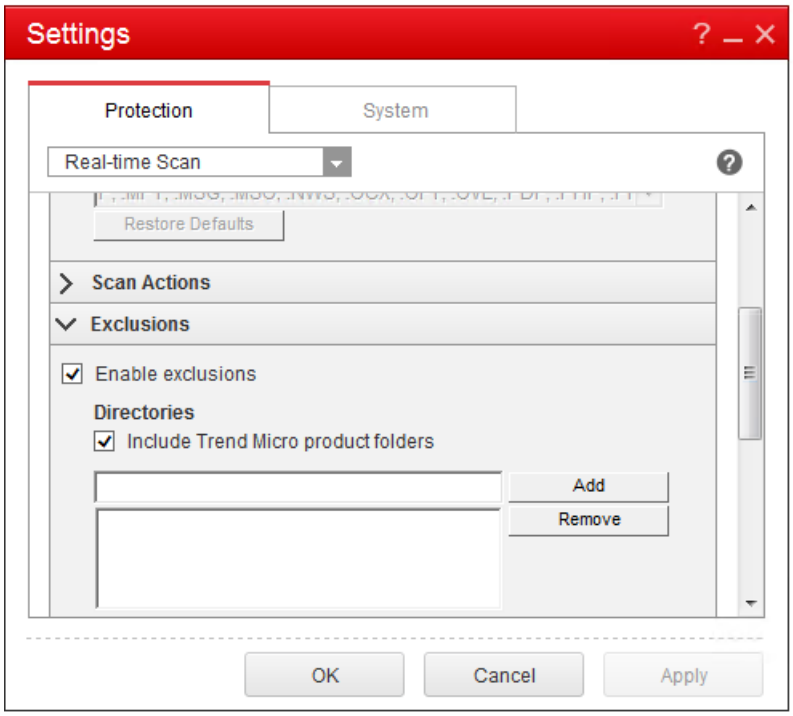
© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 单击**设置**图标显示配置选项。

4. 在“设置”屏幕中，选择**保护**选项卡。

5. 在“保护”选项卡中，向下滚动直至找到**排除项**部分。

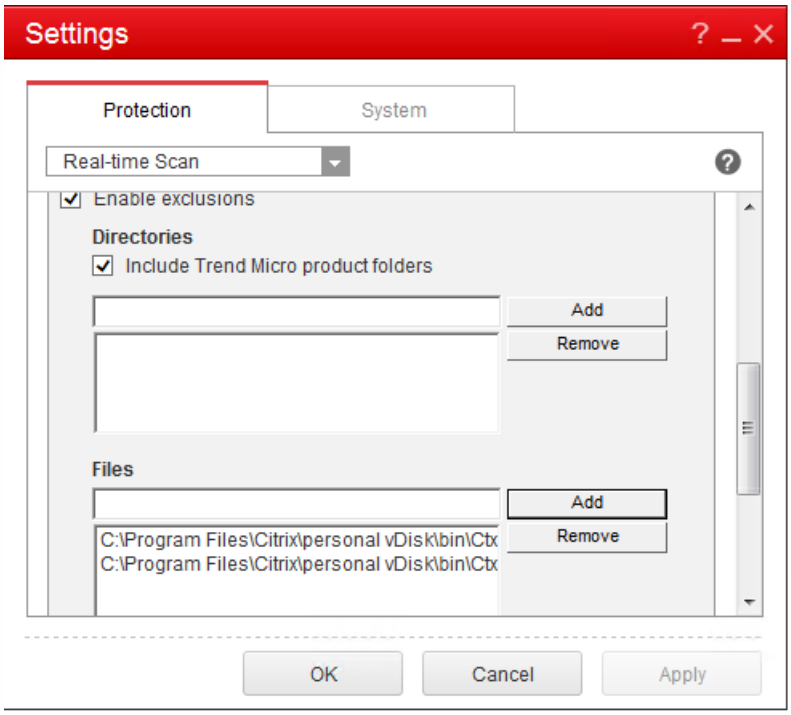


6. 在**文件**部分中，单击**添加**，将以下 AppDisk 进程输入到例外列表：

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

C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe

C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe

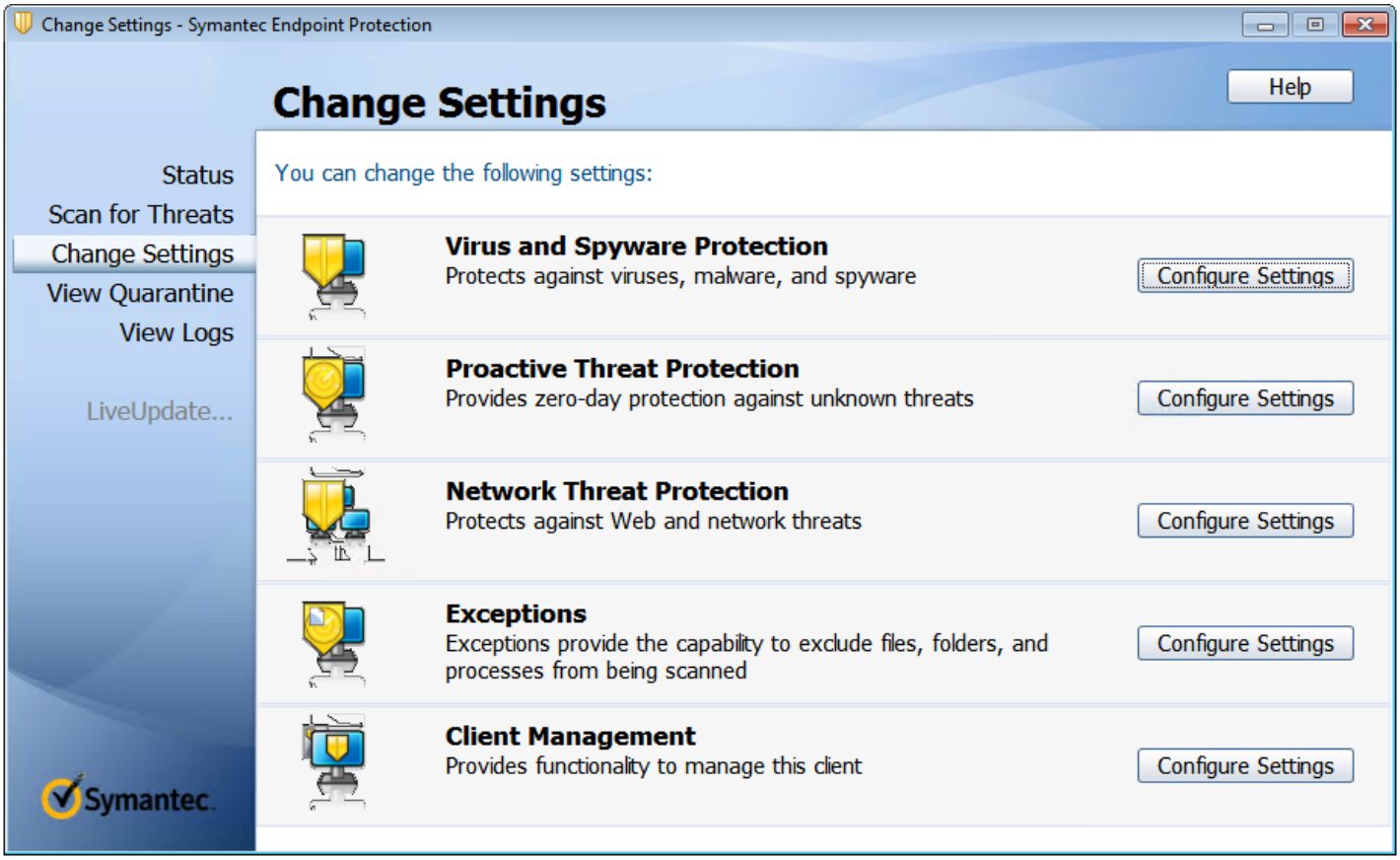


7. 单击**应用**，然后单击**确定**添加排除项。

如果基础 VM 使用 Symantec（版本 12.1.16）：

1. 启动 Symantec 控制台。
2. 单击 **Change Settings**（更改设置）。
3. 在 **Exceptions**（例外）部分，单击 **Configure Settings**（配置设置）：

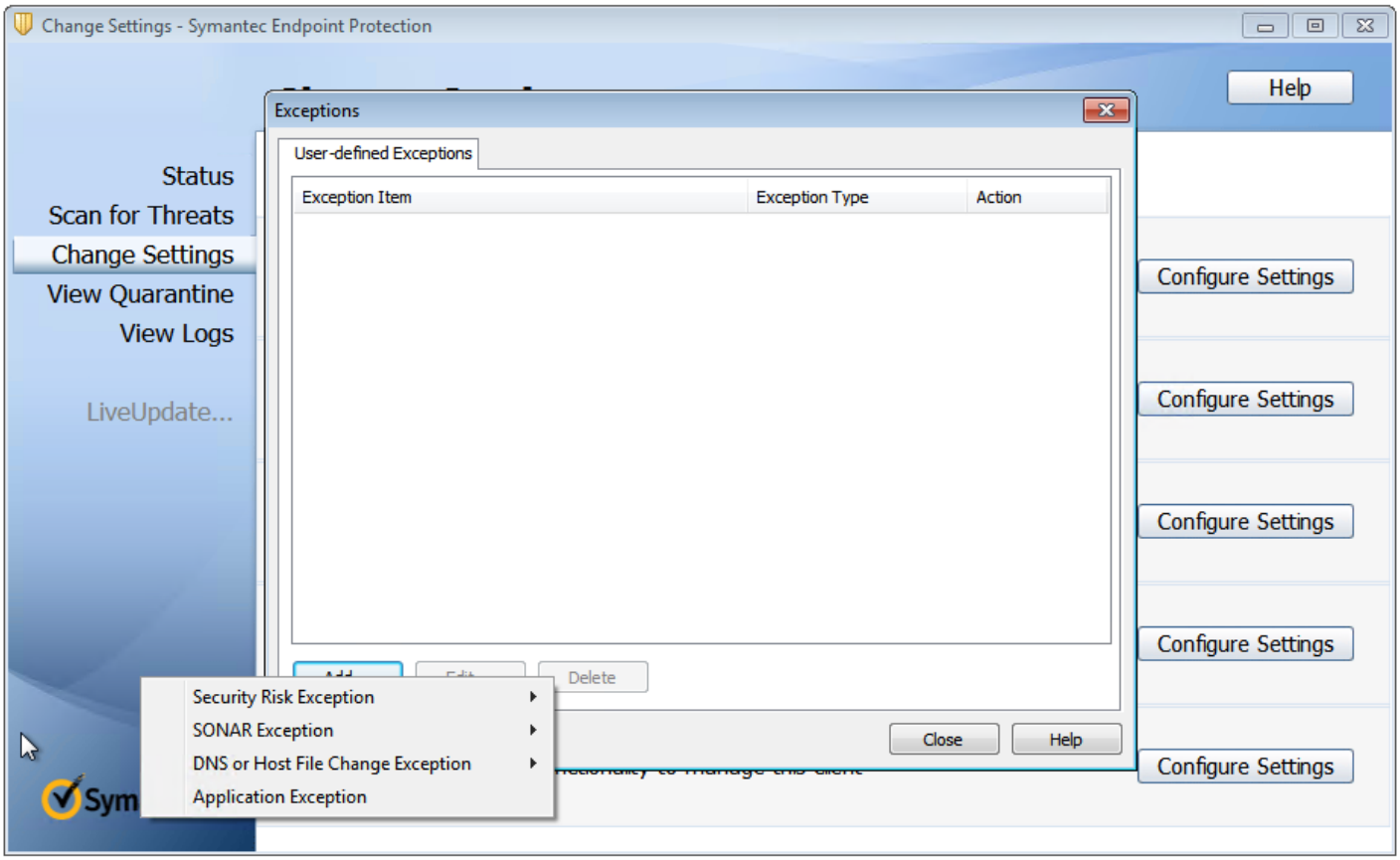
© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. 在“配置设置”屏幕中，单击**添加**。

5. 单击“添加”后，将显示一个上下文菜单，让您指定应用程序类型。选择 **Application Exception**（应用程序例外）：

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

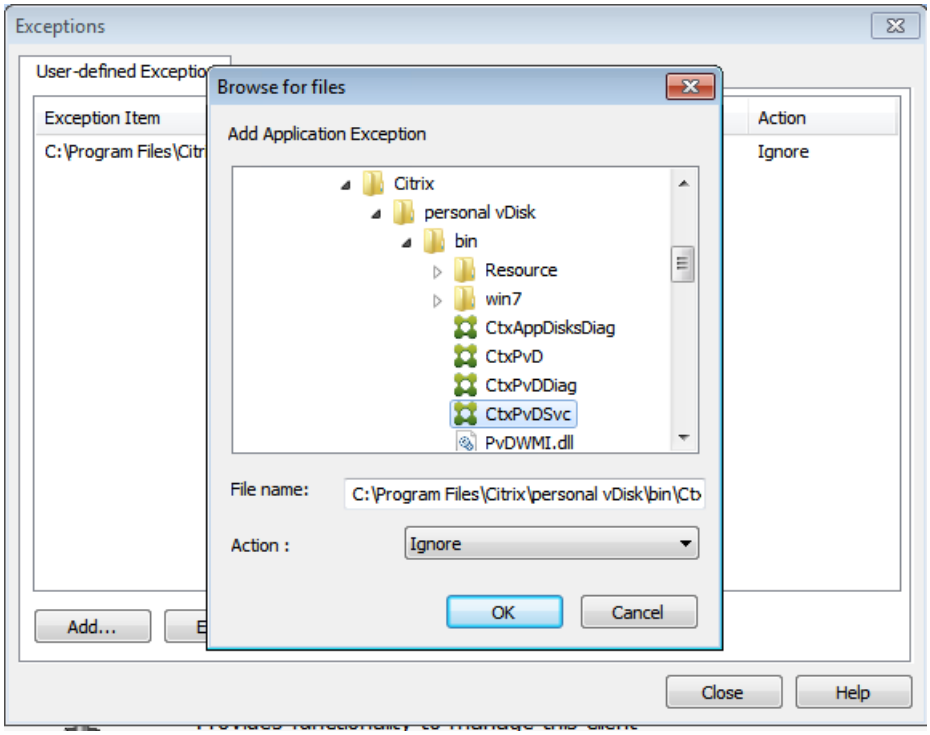


6. 在“例外”屏幕中，输入以下 AppDisk 文件路径，并将操作设置为**忽略**：

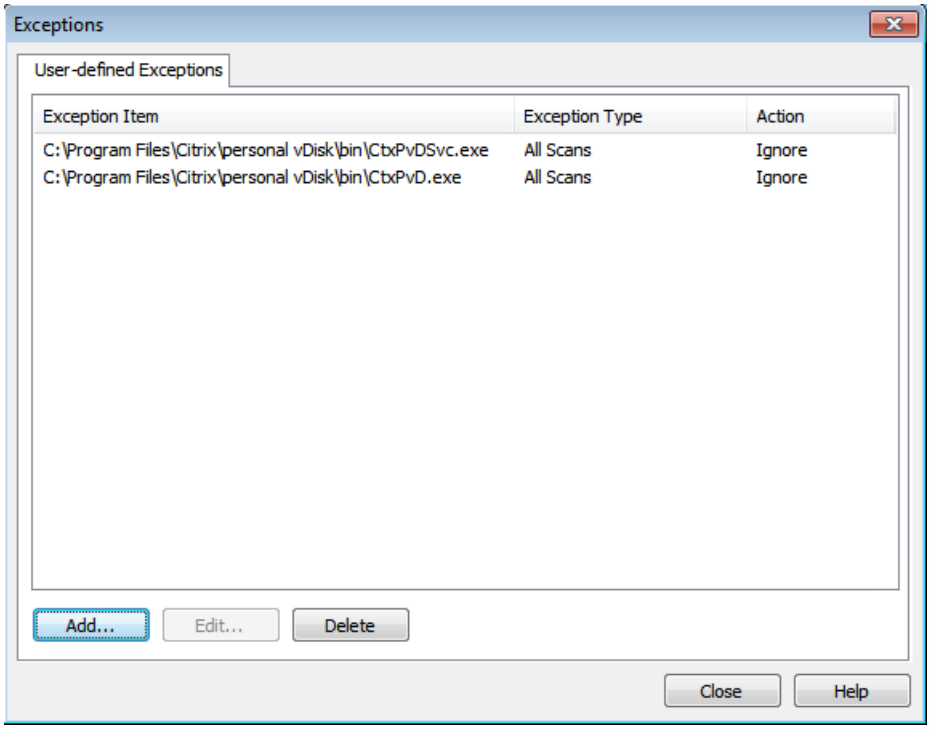
C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe

C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe

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



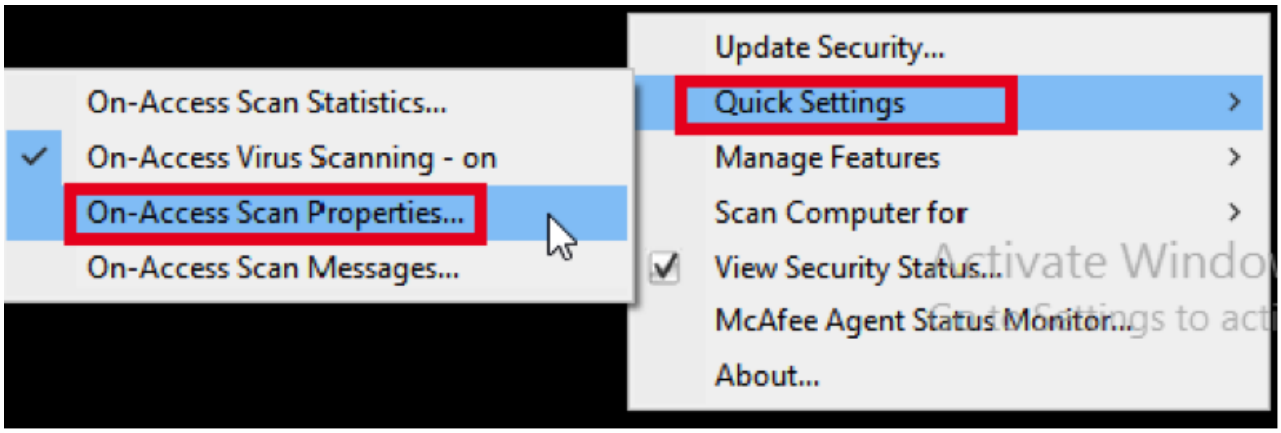
指出的例外将添加到列表。关闭窗口以应用更改：



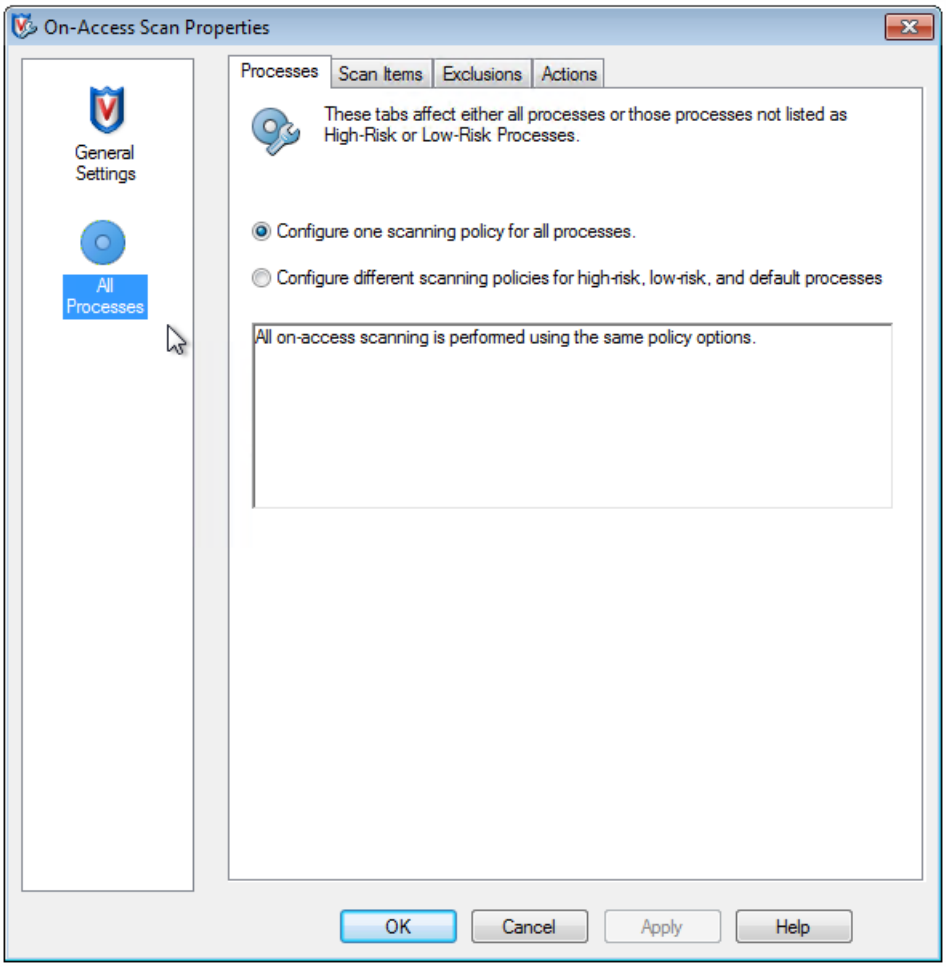
如果基础 VM 使用 McAfee（版本 4.8）：

1. 右键单击 McAfee 图标，展开 **Quick Settings**（快速设置）选项。
2. 在展开的菜单中，选择 **On-Access Scan Properties**（访问时扫描属性）：

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



3. 在**访问时扫描属性**屏幕中，单击**所有进程**：

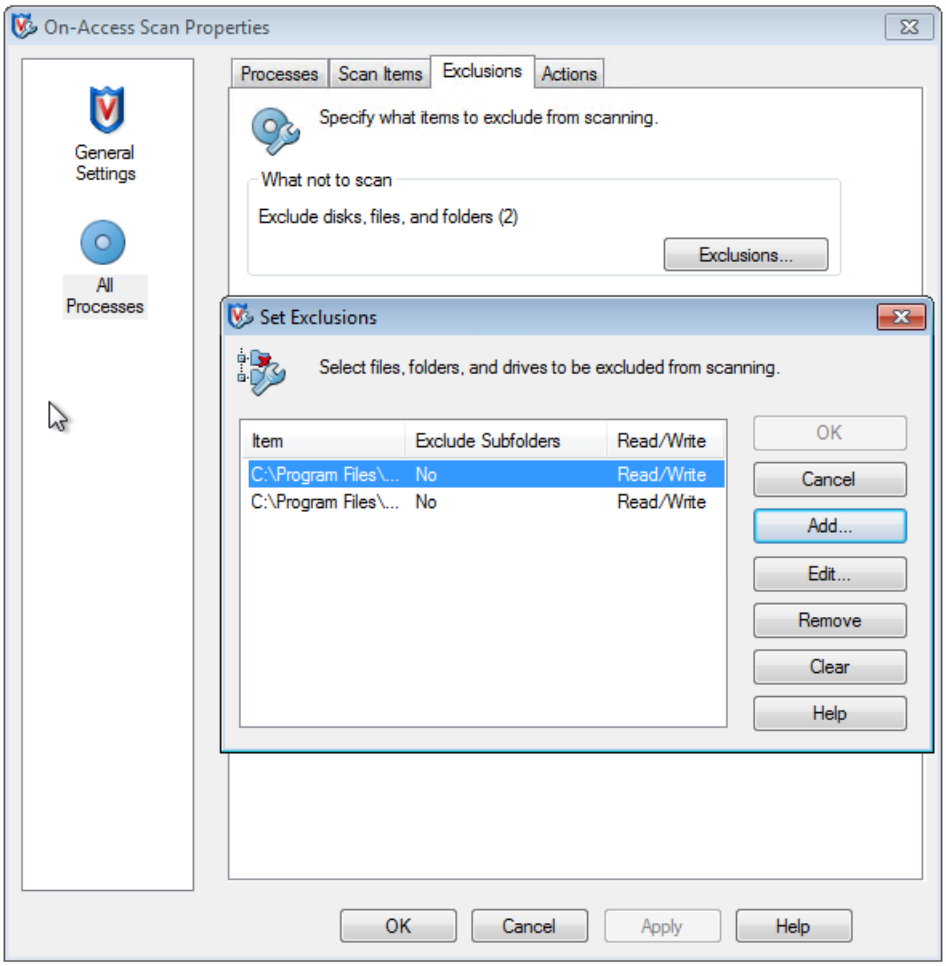


4. 选择**排除项**选项卡。

5. 单击**排除项**按钮。

6. 在**设置排除项**中，单击**添加**：

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



7. 在**添加排除项**屏幕中，选择**按名称/位置(可以包括通配符 * 或 ?)**。单击 **Browse**（浏览）找到排除可执行文件：

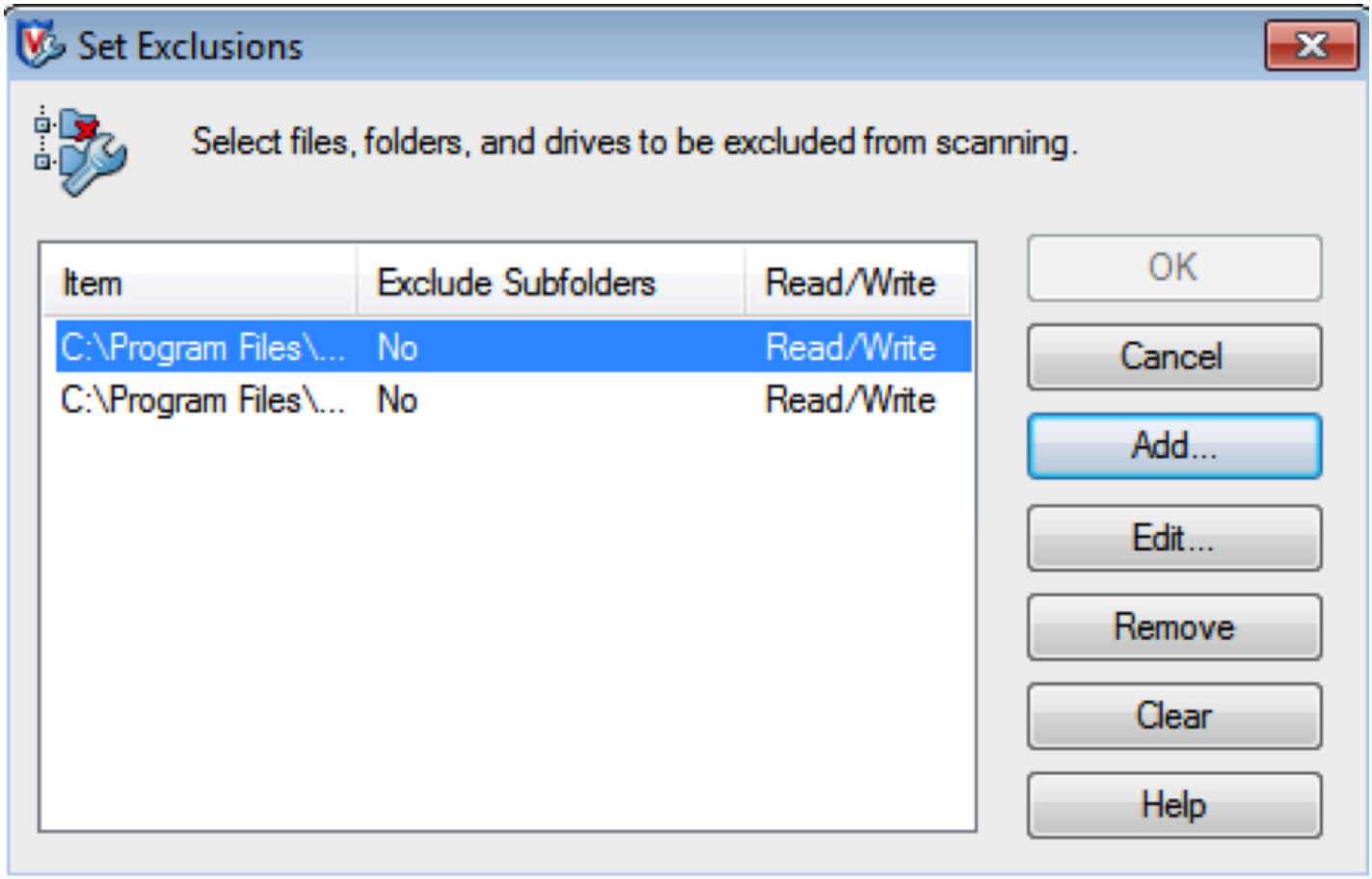
C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe

C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe

8. 单击**确定**。

9.**设置排除项**屏幕上立即显示添加的排除。单击 **OK**（确定）应用更改：

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



> **注意**
>
> 配置这些排除后，创建 AppDisk。

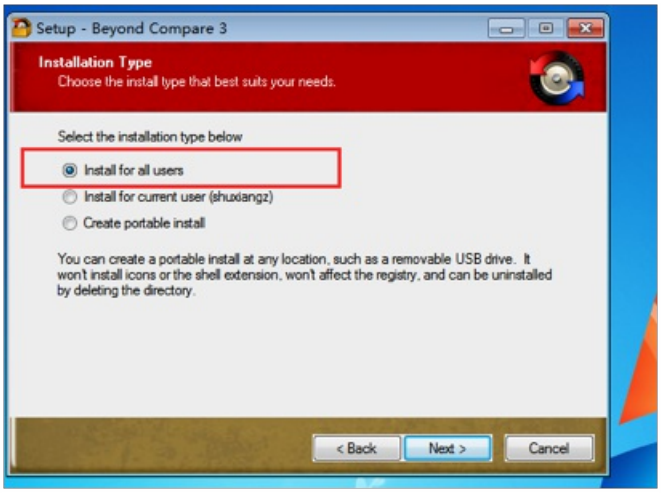
应用程序在“开始”菜单中的显示方式

如果创建了一个新 AppDisk，并使某个应用程序可供所有用户使用，且磁盘附加到桌面，则“开始”菜单中显示该应用程序的快捷方式。如果仅为当前用户创建并安装了一个 AppDisk，且磁盘附加到桌面，则“开始”菜单中不会显示该应用程序的快捷方式。

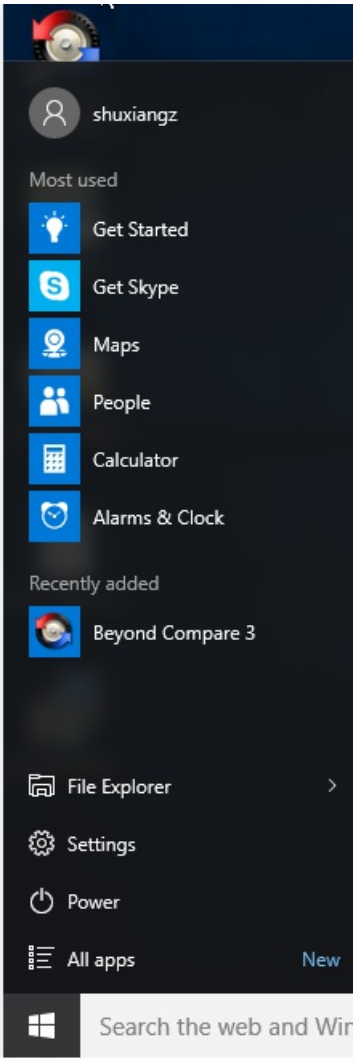
例如，创建一个新应用程序并使其可供所有用户使用：

1. 在 AppDisk 上安装一个应用程序（例如，*Beyond Compare* 是所选的应用程序）：

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



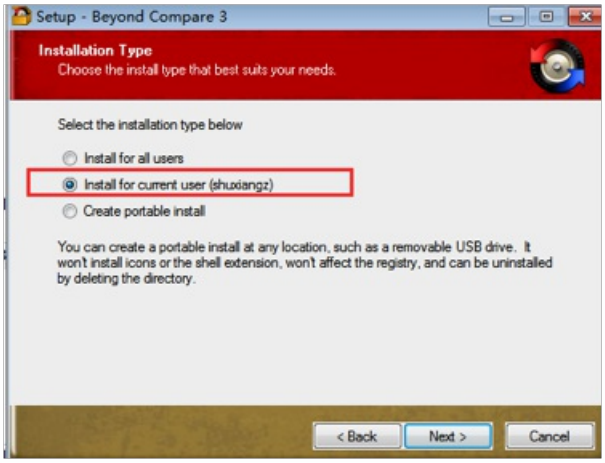
2. 将磁盘附加到桌面；新安装应用程序 (*Beyond Compare*) 的快捷方式显示在“开始”菜单中：



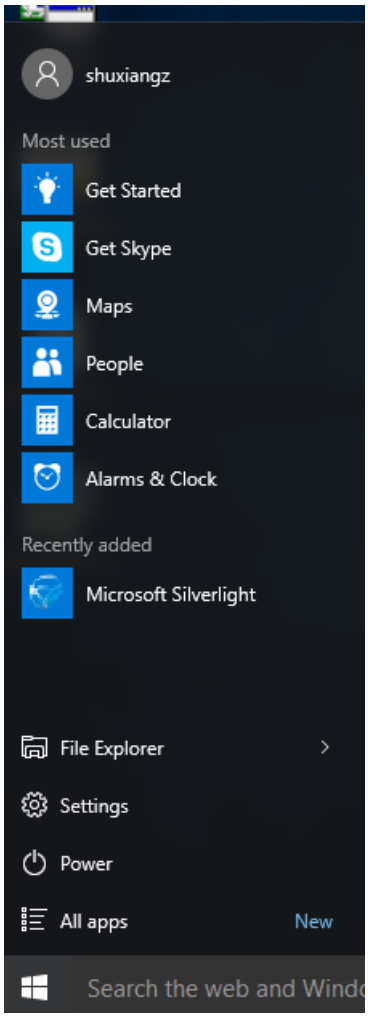
要仅为当前用户安装应用程序，请执行以下操作：

1. 在 AppDisk 上安装一个应用程序并使其可供当前用户使用：

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



2. 将磁盘附加到桌面；请注意，“开始”菜单中不会显示其快捷方式：



AppDisk 日志记录更新

本版本提供 AppDisk 日志记录的增强功能和支持范例。应用此更新后，AppDisk 用户现在可以获取诊断信息并有选择地将其上

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

载到 Citrix Insight Services (CIS) Web 站点。

此新增功能使用用于确定通过 AppDisk/PVD 创建的所有日志文件的基于脚本的 PowerShell 工具，收集来自 PowerShell 命令的包含与系统（和进程）有关的输出，将所有内容压缩到一个已编组的文件中，并最终提供用于在本地保存压缩后的文件夹的选项，或者将其上载到 CIS (Citrix Insight Services)。

> **注意**
>
> CIS 收集用于改进 AppDisk/PVD 功能的匿名诊断信息。请访问 Citrix CIS Web 站点以手动上载诊断包。必须使用您的 Citrix 凭据登录才能访问此站点。

使用 PowerShell 脚本收集 AppDisk/PVD 日志文件

AppDisk/PVD 安装程序增加了两个用于诊断数据收集的新脚本：

- Upload-AppDDiags.ps1 – 执行 AppDisk 诊断数据收集
- Upload-PvDDiags.ps1 – performs PvD diagnostic data collection

> **注意**
>
> 这些脚本添加到 C:\Program Files\Citrix\personal vDisk\bin\scripts 中。必须以管理员身份执行这些 PowerShell 脚本。

使用此脚本可启动 AppDisk 诊断数据收集功能，并且有选择地将数据手动上载到 CIS Web 站点。



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

```
SYNTAX

    Upload-AppDDiags [[-OutputFile] <string>] [-help] [<CommonParameters>]

        -OutputFile

            Local path for zip file instead of uploading to CIS

 EXAMPLES

    Upload-AppDDiags

        Upload diagnostic data to Citrix CIS website using credentials entered by interactive user.

    Upload-AppDDiags -OutputFile C:\MyDiags.zip

        Save AppDisk diagnostic data to the specified zip file. You can access https://cis.citrix.com/ to upload it later.
```

> **提示**
>
> 如果不存在 **–OutputFile** 参数，则会进行上载。如果指定了 **–OutputFile**，脚本将创建一个 zip 文件，您可以在以后手动上载该文件。

使用此脚本可启动 PvD 诊断数据收集功能，并且有选择地将数据手动上载到 CIS Web 站点。



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

```
SYNTAX

Upload-PvDDiags [[-OutputFile] <string>] [-help] [<CommonParameters>]

    -OutputFile

        Local path for zip file instead of uploading to CIS

EXAMPLES

    Upload-PvDDiags

        Upload PvD diagnostic data to Citrix CIS website using credentials entered by interactive user.

    Upload-PvDDiags -OutputFile C:\MyDiags.zip

        Save PvD diagnostic data to the specified zip file. You can access https://cis.citrix.com/ to upload it later.
```

提示

如果不存在 **–OutputFile** 参数，则会进行上载。如果指定了 **–OutputFile**，脚本将创建一个 zip 文件，您可以在以后手动上载该文件。

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

XenApp Secure Browser

Dec 05, 2017

随着应用程序逐步迁移到 Web，用户必须使用多个供应商和多个版本的浏览器，才能与基于 Web 的应用程序兼容。如果应用程序是内部托管的应用程序，组织往往需要安装和配置复杂的 VPN 解决方案，才能确保远程用户能够访问。典型的 VPN 解决方案还要求在多个操作系统之间维护一个客户端代理。

使用 XenApp Secure Browser，可以使基于 Web 的托管应用程序直接显示在用户的首选本地浏览器中，从而为用户提供基于 Web 的无缝应用程序体验。例如，用户的首选浏览器是 Mozilla Firefox，但应用程序仅与 Microsoft Internet Explorer 兼容。XenApp Secure Browser 会将与 Internet Explorer 兼容的应用程序作为标签显示在 Firefox 浏览器中。

部署 XenApp Secure Browser 版本

Citrix 建议您对 XenApp Secure Browser 使用 Citrix Smart Tools 蓝图以简化部署。

XenApp Secure Browser 蓝图包括自动执行以下任务的脚本：

- 安装 XenApp，包括 Citrix 许可证服务器和 StoreFront
- 创建 XenApp 交付站点
- 将置备的计算机加入现有域

要使用 Citrix Smart Tools 蓝图，请执行以下操作：

1. 在 Citrix Cloud 主页中，导航到“Services”（服务）；单击“Request Trial for Citrix Smart Tools”（申请 Citrix Smart Tools 试用版）。申请试用版后，如果推出试用服务，您会收到一封通知电子邮件。此过程通常需要 5 到 10 分钟。
2. 在申请试用版后收到的电子邮件中，单击“Manage”（管理）显示“Citrix Smart Tools”主页。
3. 从 Citrix 下载站点下载 Citrix XenApp Secure Browser Edition ISO。

下载 Secure Browser Edition ISO 后，请考虑执行以下操作：

- 按照 XenApp Secure Installation with a Citrix Smart Tools blueprint（使用 Citrix Smart Tools 蓝图安装 XenApp Secure）中的说明开始使用 XenApp Secure Browser 蓝图。
- 安装完成后，按照 XenApp Secure Browser Deployment Guide（《XenApp Secure Browser 部署指南》）中指定的配置步骤进一步优化 Web 应用程序交付环境。

手动安装 XenApp Secure Browser 版本：

1. 从 Citrix 下载站点下载 Citrix XenApp Secure Browser Edition ISO。
2. 按照安装说明所述安装 XenApp 的各个组件。
3. 安装完毕后，请通过执行以下步骤配置 Secure Browser 的版本和许可模式：

    a. 在 Delivery Controller 上，单击任务栏上的蓝色图标，或依次单击“开始”>“所有程序”>“附件”>“Windows PowerShell”>“Windows PowerShell”，从而启动 PowerShell 会话。

    注意：在 64 位系统上，此操作将启动 64 位版本的 PowerShell。32 位和 64 位版本的 PowerShell 均受支持。

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

b. 键入 Asnp Citrix* 并按 Enter，以加载 Citrix 专用的 PowerShell 模块。

注意：“Asnp”是指 Add-PSSnapin。

c. 运行 Get-ConfigSite cmdlet，检查当前站点设置和许可模式。

d. 运行 Set-ConfigSite -ProductCode XDT -ProductEdition BAS，将许可模式设置为 XenApp Secure Browser 版本。

e. 运行 Get-BrokerSite cmdlet，确认 XenApp Secure Browser 版本和许可模式设置正确无误。

注意

安装完成后，按照 XenApp Secure Browser Deployment Guide（《XenApp Secure Browser 部署指南》）中指定的配置步骤进一步优化 Web 应用程序交付环境。

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

发布内容

Dec 05, 2017

可以发布只是指向资源（例如 Microsoft Word 文档或 Web 链接）的 URL 或 UNC 路径的应用程序。此功能称为已发布的内容。发布内容功能提高了向用户交付内容的灵活性。您可从对应用程序的现有访问控制和管理中受益。并且，您可以指定用于打开内容的应用程序：本地应用程序或已发布的应用程序。

在 StoreFront 和 Citrix Receiver 中，已发布的内容就像其他应用程序一样显示。用户访问这些内容的方式与访问应用程序一样。在客户端上，资源按常规方式打开。

- 如果某个本地安装的应用程序合适，会启动它来打开资源。
- 如果定义了文件类型关联，则会启动已发布的应用程序来打开资源。

可使用 PowerShell SDK 发布内容。（不能使用 Studio 发布内容。但是，可以在发布了内容后，使用 Studio 编辑应用程序属性。）

配置概述和准备

发布内容通过使用 New-BrokerApplication cmdlet 与以下主要属性进行。（有关所有 cmdlet 属性的说明，请参阅 cmdlet 帮助。）

```
New-BrokerApplication –ApplicationType PublishedContent
-CommandLineExecutable <location> -Name <app-name>
-DesktopGroup <delivery-group-name>
```

ApplicationType 属性必须是 PublishedContent。

CommandLineExecutable 属性指定已发布的内容的位置。支持以下格式， 字符数上限为 255。

- HTML Web 站点地址（例如 http://www.citrix.com）
- Web 服务器上的文档文件（例如 https://www.citrix.com/press/pressrelease.doc）
- FTP 服务器上的目录（例如 ftp://ftp.citrix.com/code）
- FTP 服务器上的文档文件（例如 ftp://ftp.citrix.com/code/Readme.txt）
- UNC 目录路径（例如 file://myServer/myShare 或 \\myServer\myShare）
- UNC 文件路径（例如 file://myServer/myShare/myFile.asf 或 \\myServer\myShare\myFile.asf）

请确保您有正确的 SDK。

- 对于 XenApp and XenDesktop Service 部署，请下载并安装 XenApp and XenDesktop Remote PowerShell SDK。
- 对于本地 XenApp 和 XenDesktop 部署，请使用与 Delivery Controller 一起安装的 PowerShell SDK。如欲添加一款已发布内容应用程序，请使用最低为 7.11 版的 Delivery Controller。

以下过程使用多个示例。在这些示例中：

- 创建了计算机目录。
- 创建了名为 PublishedContentApps 的交付组。该组使用该目录中的服务器操作系统计算机。已将 WordPad 应用程序添加到该组。
- 分配了交付组名称、CommandLineExecutable 位置和应用程序名称。

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

入门

在包含 PowerShell SDK 的计算机上打开 PowerShell。

以下 cmdlet 添加合适的 PowerShell SDK 管理单元，以及分配返回的交付组记录。

```
Add-PsSnapin Citrix*
$dg = Get-BrokerDesktopGroup –Name PublishedContentApps
```

如果要使用 XenApp and XenDesktop Service，请输入您的 Citrix Cloud 凭据进行身份验证。如果有多个客户，请选择一个。

发布 URL

分配了位置和应用程序名称后，以下 cmdlet 将 Citrix 主页作为应用程序发布。

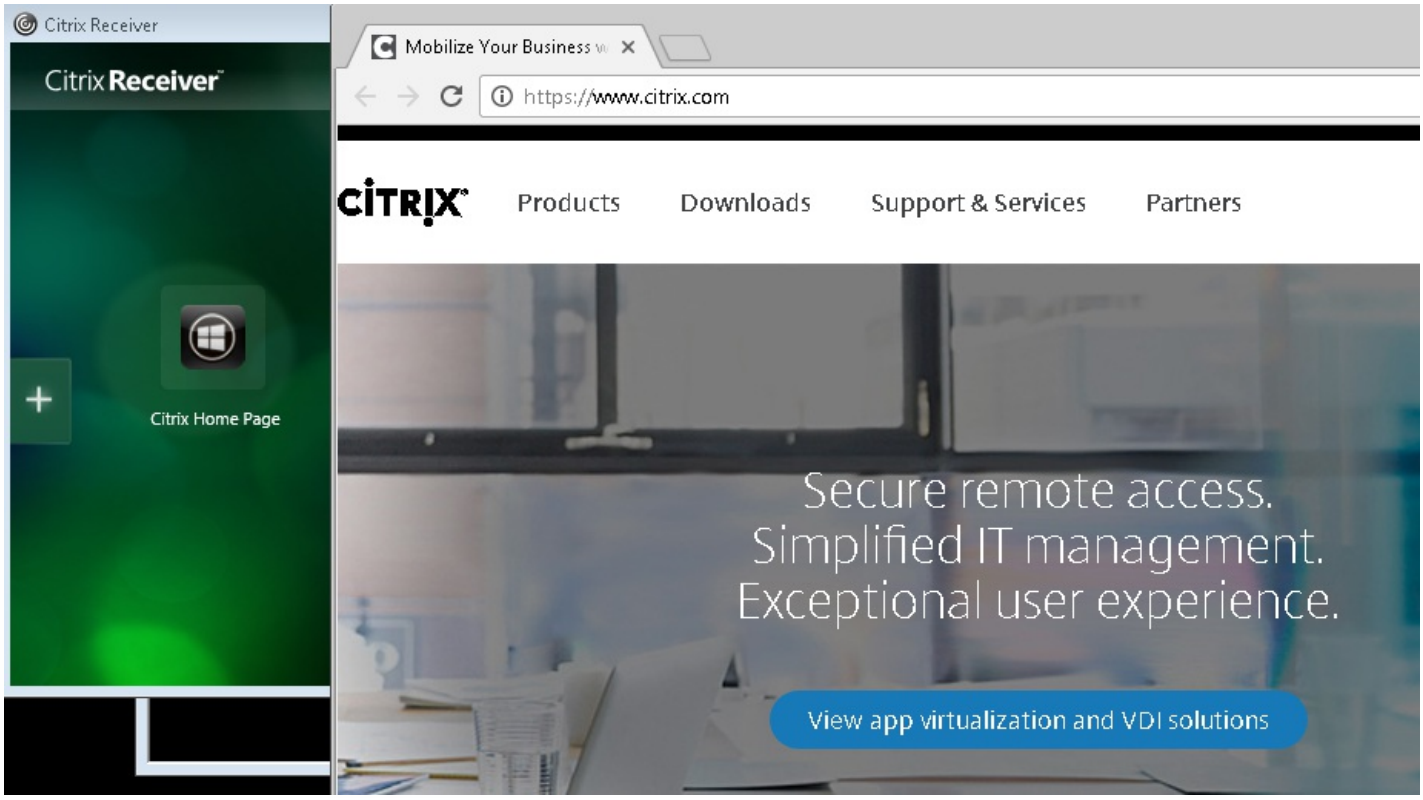
```
$citrixUrl = "https://www.citrix.com/"
$appName = "Citrix Home Page"

New-BrokerApplication –ApplicationType PublishedContent
–CommandLineExecutable $citrixURL –Name $appName
–DesktopGroup $dg.Uid
```

验证成功：

- 打开 StoreFront 以可以访问 PublishedContentApps 交付组中应用程序的用户身份登录。显示内容包括具有默认图标的新创建的应用程序。要了解如何自定义图标，请参阅 https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/。
- 单击 Citrix 主页应用程序。将在本地运行的默认浏览器实例中启动新选项卡并访问该 URL。

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



发布位于 UNC 路径的资源

在本示例中，管理员已创建了一个名为 PublishedResources 的共享。分配了位置和应用程序名称后，以下 cmdlet 在该共享中将 RTF 和 DOCX 文件作为资源发布。

```
$rtfUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedRTF.rtf"
$rtfAppName = "PublishedRTF"

New-BrokerApplication –ApplicationType PublishedContent
–CommandLineExecutable $rtfUNC -Name $rtfAppName
-DesktopGroup $dg.Uid

$docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx"
$docxAppName = "PublishedDOCX"

New-BrokerApplication –ApplicationType PublishedContent
–CommandLineExecutable $docxUNC -Name $docxAppName
-DesktopGroup $dg.Uid
```

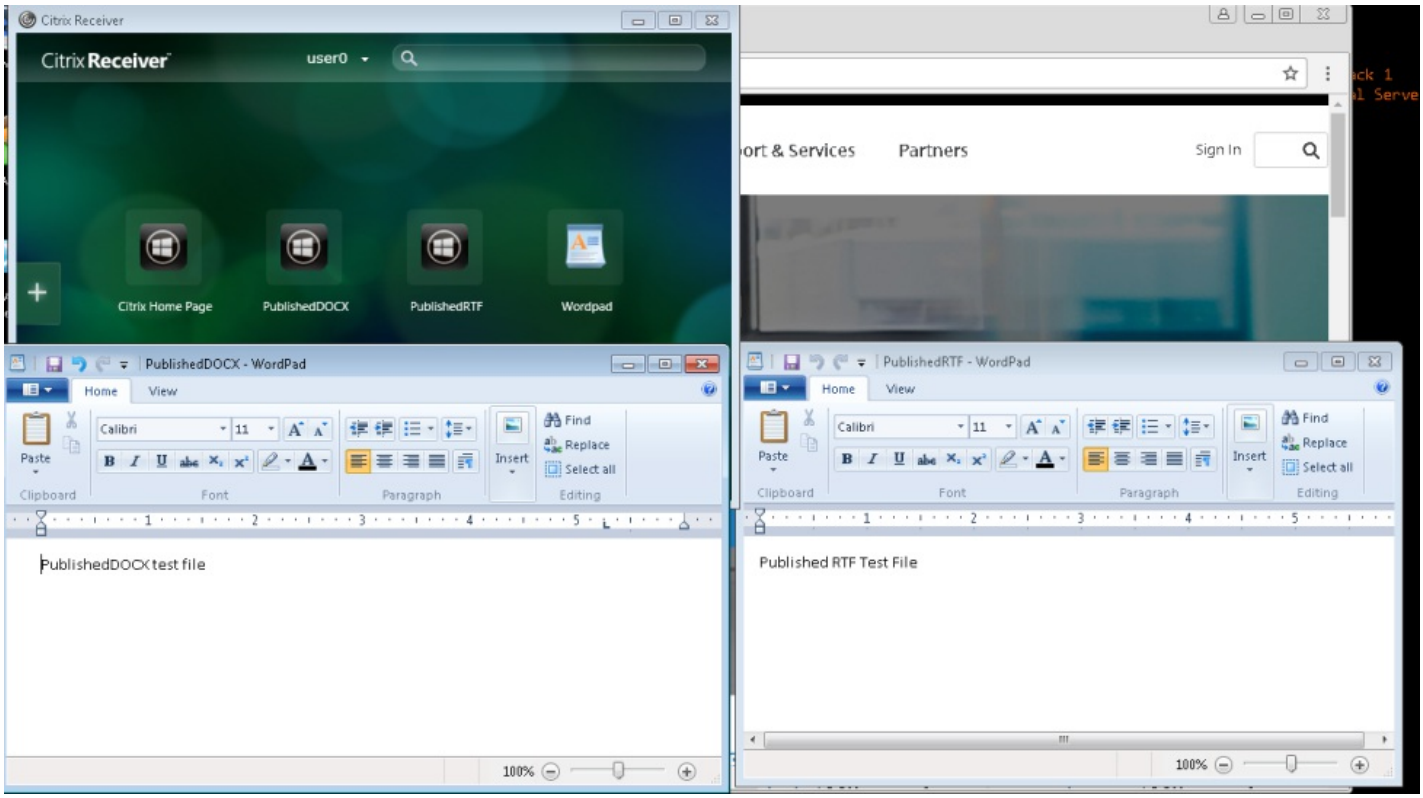
验证成功：

- 刷新 StoreFront 窗口查看新发布的文档。

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



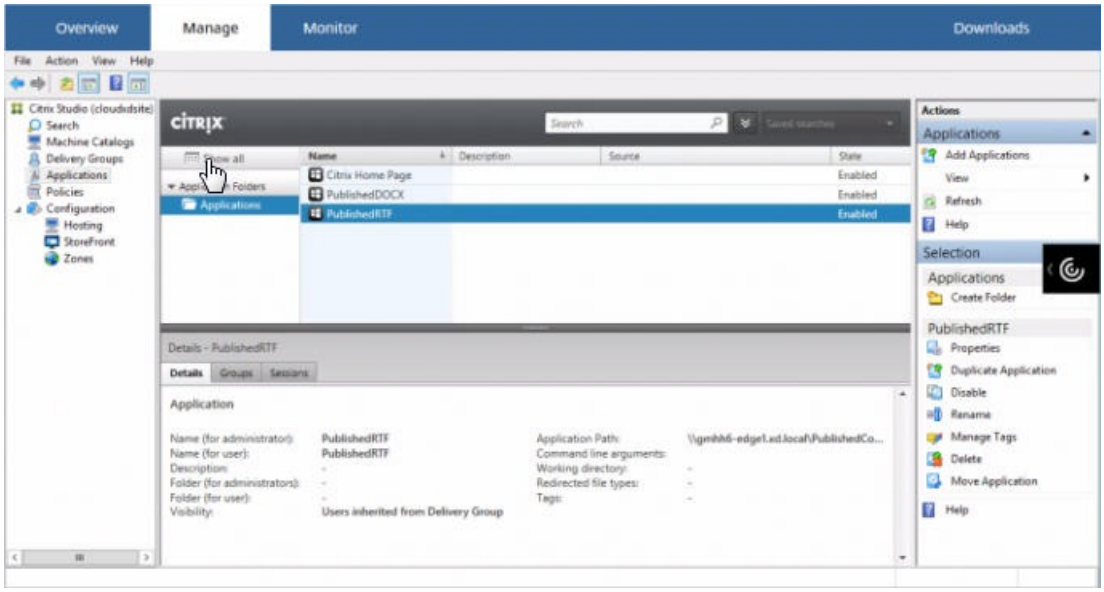
- 单击 PublishedRTF 和 PublishedDOCX 应用程序。各文档均在本地运行的 WordPad 中打开。



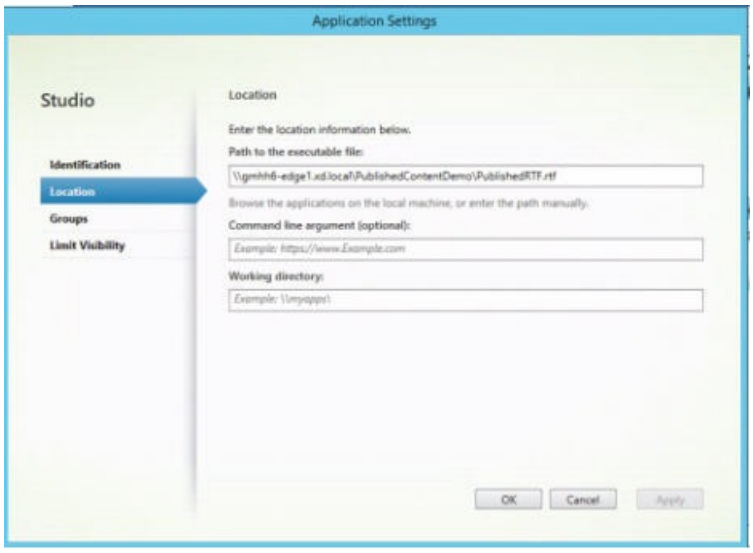
查看并编辑 PublishedContent 应用程序。

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

可使用与其他应用程序类型相同的方法管理已发布的内容。已发布的内容项显示在 Studio 中的应用程序列表中，且可在 Studio 中编辑。



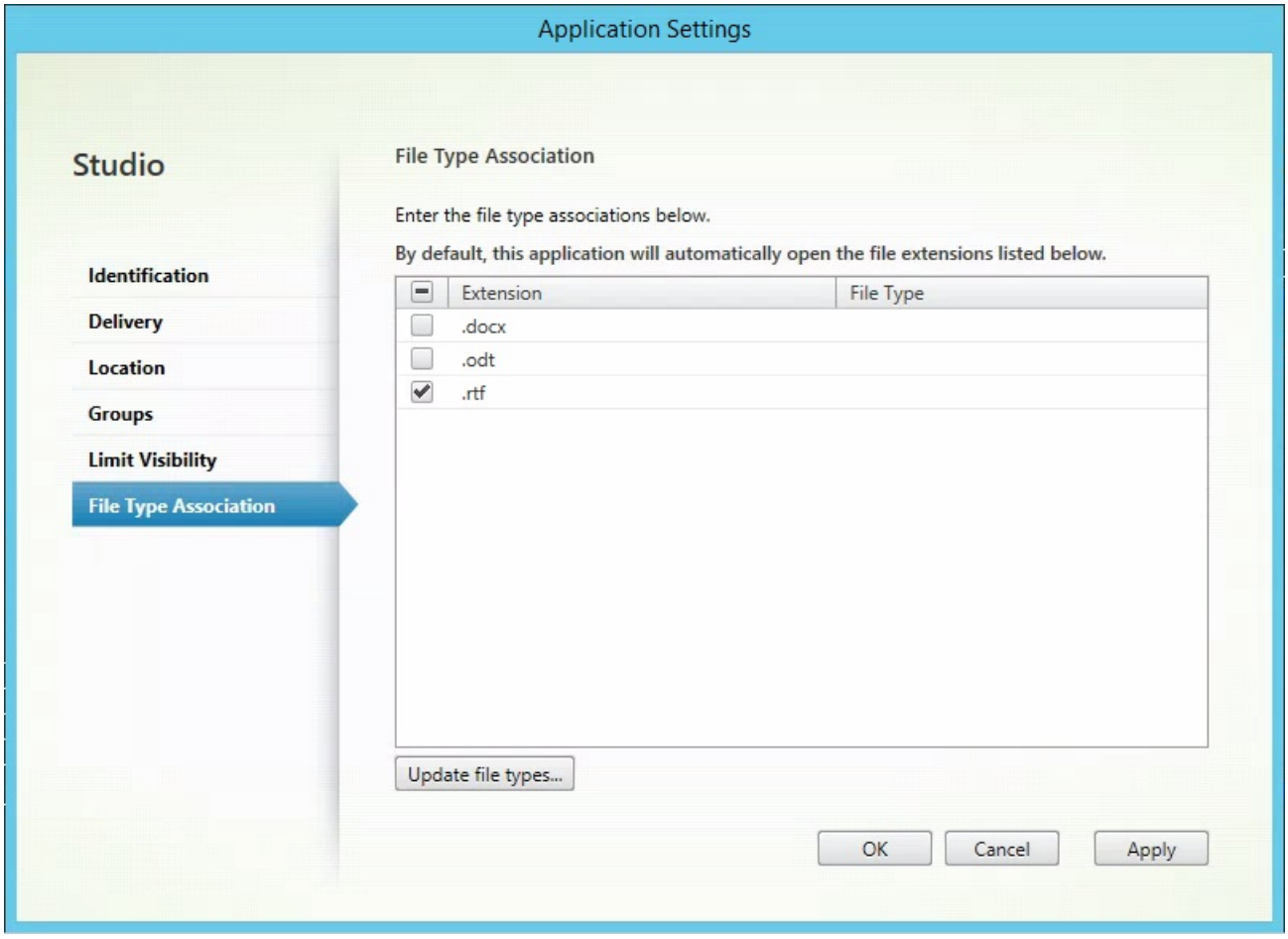
应用程序属性（例如用户可见性、组关联和快捷方式）会应用于已发布的内容。但是，您无法在**位置**页面上更改命令行参数和工作目录属性。要更改资源，请在该页面上修改“可执行文件的路径”字段。



要使用已发布的应用程序打开 PublishedContent 应用程序（而不是本地应用程序），请编辑已发布的应用程序的文件类型关联属性。在此示例中，已编辑了已发布的 WordPad 应用程序来为 .rtf 文件创建文件类型关联。

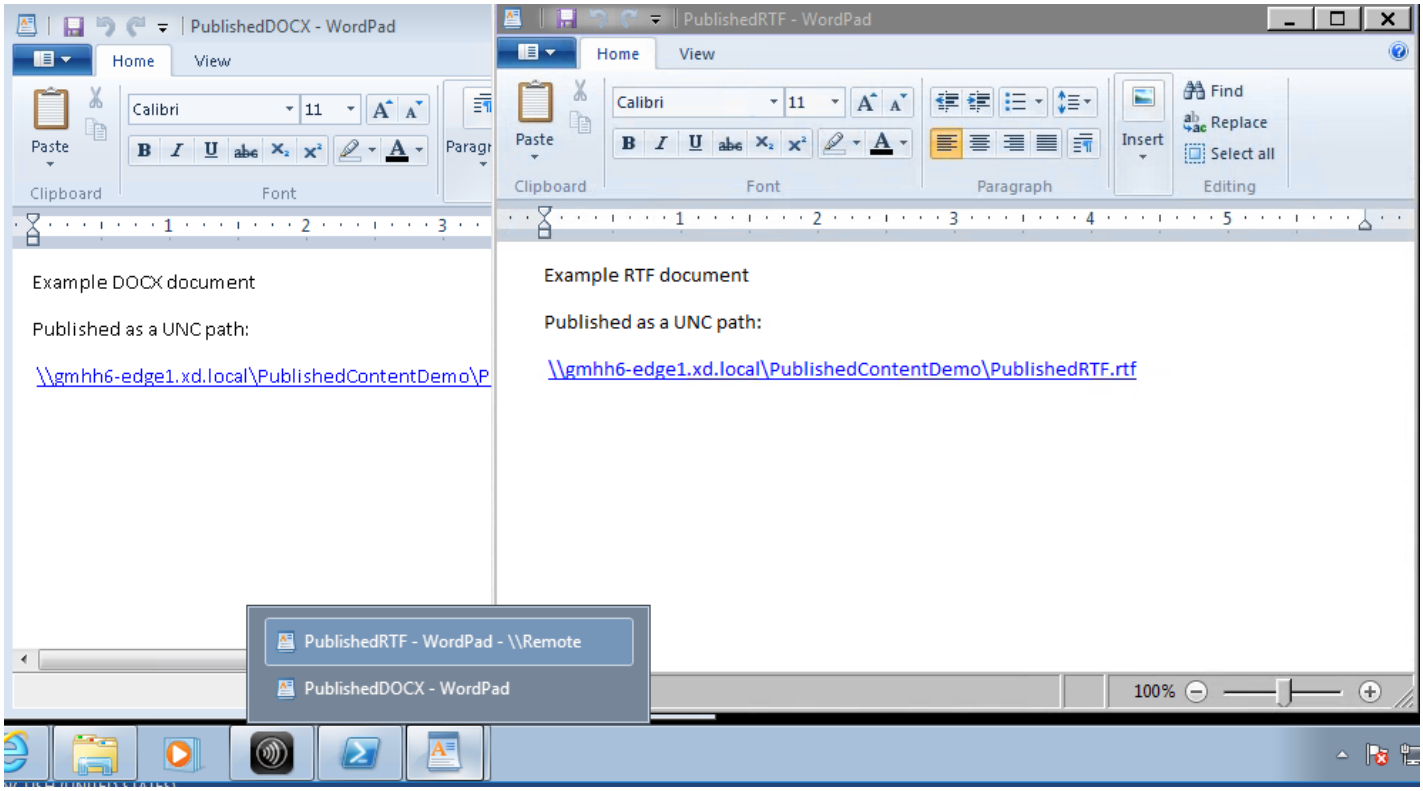
重要：请先为交付组打开维护模式，然后再编辑文件类型关联。请务必在完成编辑后关闭维护模式。

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



刷新 StoreFront 以加载文件类型关联更改，然后单击 PublishedRTF 和 PublishedDOCX 应用程序。请注意差异。PublishedDOCX 仍在本地 WordPad 中打开。但是，由于文件类型关联，PublishedRTF 现在在已发布的 WordPad 中打开。

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



相关详细信息

- 创建计算机目录
- 创建交付组
- 更改应用程序属性

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

服务器 VDI

Dec 05, 2017

通过“服务器 VDI”（虚拟桌面基础结构）功能，可以从服务器操作系统为单个用户交付桌面。

- 企业管理员可以将服务器操作系统作为 VDI 桌面进行交付，这对于工程师和设计师等用户非常有帮助。
- 服务提供商可以利用云提供桌面；这些桌面受 Microsoft 服务提供商许可协议 (SPLA) 约束。

通过 Citrix 策略设置“增强的桌面体验”，可以使服务器操作系统像桌面操作系统一样运行。

服务器 VDI 不支持以下功能：

- Personal vDisk
- 托管应用程序
- 本地应用程序访问
- 直接（非代理）桌面连接
- Remote PC Access

要使服务器 VDI 能够与扫描仪等 TWAIN 设备结合使用，必须安装 Windows Server 桌面体验功能。在 Windows Server 2012 中，这是一项可以从“管理工具”>“服务器管理器”>“功能”>“添加功能”>“桌面体验”中安装的可选功能。

服务器 VDI 与 VDA for Windows Server OS 受相同的服务器操作系统支持。

要安装服务器 VDI，请执行以下操作：

步骤 1. 准备 Windows 服务器以便进行安装。

- 通过 Windows 服务器管理器，确保未安装远程桌面服务角色服务。如果先前已安装这些服务，请将其删除。（如果安装这些角色服务，VDA 安装将失败。）
- 确保已启用“限制每个用户只能进行一个会话”属性。

  在 Windows Server 2008 R2 上，可通过访问“管理工具”>“远程桌面服务”>“远程桌面会话主机配置”。在“编辑设置”>“常规”部分中，“限制每个用户只能进行一个会话”设置应为“是”。

  在 Windows Server 2012 R2 或 Windows Server 2016 上，编辑注册表以设置终端服务器设置。在注册表项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer 中，将 DWORD fSingleSessionPerUser 设置为 1。

步骤 2. 对于 Windows Server 2008 R2，在安装 VDA 之前，在服务器上安装 Microsoft .NET Framework 3.5 SP1。

步骤 3. 使用安装程序的命令行界面在支持的服务器或服务器主映像上安装 VDA，同时指定 /quiet 和 /servervdi 选项。（默认情况下，安装程序的图形界面阻止在服务器操作系统中安装 Windows 桌面操作系统 VDA。使用命令行将替换此行为。）

  本地 XenApp 和 XenDesktop 部署：XenDesktopVdaSetup.exe /quiet /servervdi

  本地 XenApp 和 XenDesktop 或 XenDesktop 服务部署：VDAWorkstationSetup.exe /quiet /servervdi

可以通过 /controllers 选项指定 Delivery Controller 或 Cloud Connector。

使用 /enable_hdx_ports 选项打开防火墙中的端口，除非要手动配置防火墙。

如果要在映像上安装 VDA，并使用 MCS 从该映像创建服务器 VM，请添加 /masterimage 选项。

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

请勿包括服务器 VDI 不支持的功能所对应的选项，例如 /baseimage。

步骤 4. 为服务器 VDI 创建计算机目录。

- 在**操作系统**页面上，选择“桌面操作系统”。
- 在**摘要**页面上，为管理员指定可明确将其标识为服务器 VDI 的计算机目录名称和说明；在 Studio 中，只能通过该内容来指示目录支持服务器 VDI。
- 在 Studio 中使用搜索功能时，所创建的服务器 VDI 目录将显示在“桌面操作系统计算机”选项卡上，即使此 VDA 安装在服务器上也是如此。

步骤 5. 创建交付组，并为其分配在上一步中所创建的服务器 VDI 目录。

如果安装 VDA 时未指定 Delivery Controller 或 Cloud Connector，之后可使用 Citrix 策略设置、Active Directory 或通过编辑 VDA 计算机的注册表值进行指定。请参阅 VDA 注册。

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

Personal vDisk

Dec 05, 2017

Personal vDisk 功能保留了池桌面和流桌面的单映像管理功能，同时允许用户安装应用程序和更改自己的桌面设置。在涉及池桌面的传统虚拟桌面基础结构 (Virtual Desktop Infrastructure, VDI) 部署中，当管理员更改主映像时，用户将丢失自己的自定义设置和个人应用程序，而使用 Personal vDisk 功能的部署则与此不同，此部署会保留这些更改。这意味着管理员能够轻松地集中管理其主映像，同时向用户提供个性化的自定义桌面体验。

Personal vDisk 功能可以将对用户的 VM 所做的所有更改重定向到连接至用户 VM 的独立磁盘（即个人虚拟磁盘），从而将每位用户的个性化设置分隔开来。个人虚拟磁盘中的内容在运行时与主映像中的内容混合在一起，以提供一致的体验。通过这种方式，用户仍然能够访问主映像中由管理员置备的应用程序。

个人虚拟磁盘分为两个部分，这两个部分使用不同的驱动器盘符，且默认具有相同的大小：

- 用户配置文件 - 包含用户数据、文档和用户配置文件。默认情况下，这部分使用驱动器 P:，但可以在创建包含使用个人虚拟磁盘的计算机的目录时选择其他驱动器盘符。使用的驱动器还取决于 EnableUserProfileRedirection 设置。
- 虚拟硬盘 (.vhd) 文件 - 包含所有其他项目，如安装在 C:\Program Files 中的应用程序。这部分不在 Windows 资源管理器中显示，因为版本 5.6.7 不需要驱动器盘符。

Personal vDisk 支持置备部门级应用程序，以及用户下载并安装的应用程序，包括需要驱动程序（阶段 1 驱动程序除外）的应用程序、数据库和计算机管理软件。如果用户所做的更改与管理员所做的更改存在冲突，Personal vDisk 可提供一种简单的自动化方法来协调这些更改。

此外，也可以在用户的环境中置备本地管理的应用程序（例如由本地 IT 部门置备并管理的应用程序）。用户在可用性方面体会不到任何差异；Personal vDisk 功能可确保所做的所有更改以及安装的所有应用程序都存储在虚拟磁盘中。如果个人虚拟磁盘上的应用程序与主映像上的应用程序完全一致，将丢弃个人虚拟磁盘上的备份以节省空间，但用户仍然能够访问对应的应用程序。

可以在虚拟机管理程序上存储个人虚拟磁盘（以物理方式），但它们不必与连接到虚拟桌面的其他磁盘位于同一位置。这样可以降低个人虚拟磁盘存储的成本。

站点创建期间，创建连接时，应为虚拟机使用的磁盘定义存储位置。可以将个人虚拟磁盘与用于操作系统的磁盘分隔开来。每台 VM 都必须对这两种磁盘的存储位置具有访问权限。如果您为这两种磁盘使用本地存储，则本地存储必须可从同一虚拟机管理程序进行访问。为确保满足此要求，Studio 仅提供兼容的存储位置。稍后，还可以从 Studio 中的“配置”>“托管”将个人虚拟磁盘以及它们的存储添加到现有主机（而不是计算机目录）。

可使用任何偏好的方法定期备份个人虚拟磁盘。虚拟磁盘是虚拟机管理程序的存储层中的标准卷，因此，您可以像备份任何其他卷一样备份它们。

> ## 注意
>
> 有关 PvD 报告、消息和已知问题的信息，请参阅故障排除一文。

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

安装和升级

Dec 05, 2017

Personal vDisk 7.x 在从版本 5.6 到当前版本的 XenDesktop 上受支持。每个 XenDesktop 版本的“系统要求”文档中列出了 Virtual Delivery Agent (VDA) 支持的操作系统，支持的主机（虚拟资源）版本和 Provisioning Services。有关 Provisioning Services 任务的详细信息，请参阅当前的 Provisioning Services 文档。

可以在计算机上安装或升级 VDA for Desktop OS 时安装并启用 PvD 组件。这些操作在安装向导的**附加组件**和**功能**页面上分别进行选择。有关详细信息，请参阅安装 VDA。

如果在安装 VDA 后更新 PvD 软件，可使用 XenApp 或 XenDesktop 安装介质上所提供的 PvD MSI。

启用 PvD：

- 如果要使用 Machine Creation Services (MCS)，在创建将使用个人虚拟磁盘的桌面操作系统计算机的计算机目录时会自动启用 PvD。
- 如果要使用 Provisioning Services (PVS)，在主（基础）映像创建过程中运行清单时，或自动更新运行清单时，会自动启用 PvD。

因此，如果在 VDA 安装过程中安装 PvD 组件但不启用它们，可以使用同一映像创建 PvD 桌面和非 PvD 桌面，因为在目录创建过程中启用 PvD。

可以在配置站点时向主机添加个人虚拟磁盘。 在主机上，可以为 VM 和个人虚拟磁盘使用相同的存储，也可以为个人虚拟磁盘使用不同的存储。

之后，还可以将个人虚拟磁盘及其存储添加到现有主机（连接），但无法添加到计算机目录。

1. 在 Studio 导航窗格中，选择 配置 > 托管。
2. 在“操作”窗格中选择 添加 个人虚拟磁盘存储，并指定存储 位置。

将 Personal vDisk 从早期的 7.x 版本升级的最简单方法是，将桌面操作系统 VDA 升级到最新的 XenDesktop 版本提供的版本。然后，运行 PvD 清单。

可以使用两种方式中的任意一种删除 PvD 软件。

- 卸载 VDA；此操作也会删除 PvD 软件。
- 如果是使用 PvD MSI 更新 PvD，则可以从“程序”列表中将其卸载。

如果要卸载 PvD 并重新安装相同的版本或更新的版本，请备份注册表项 HKLM\Software\Citrix\personal vDisk\config，其中包含可能已更改的任何环境配置设置。然后，在安装 PvD 后，通过与备份的版本进行比较，重置可能已更改的注册表值。

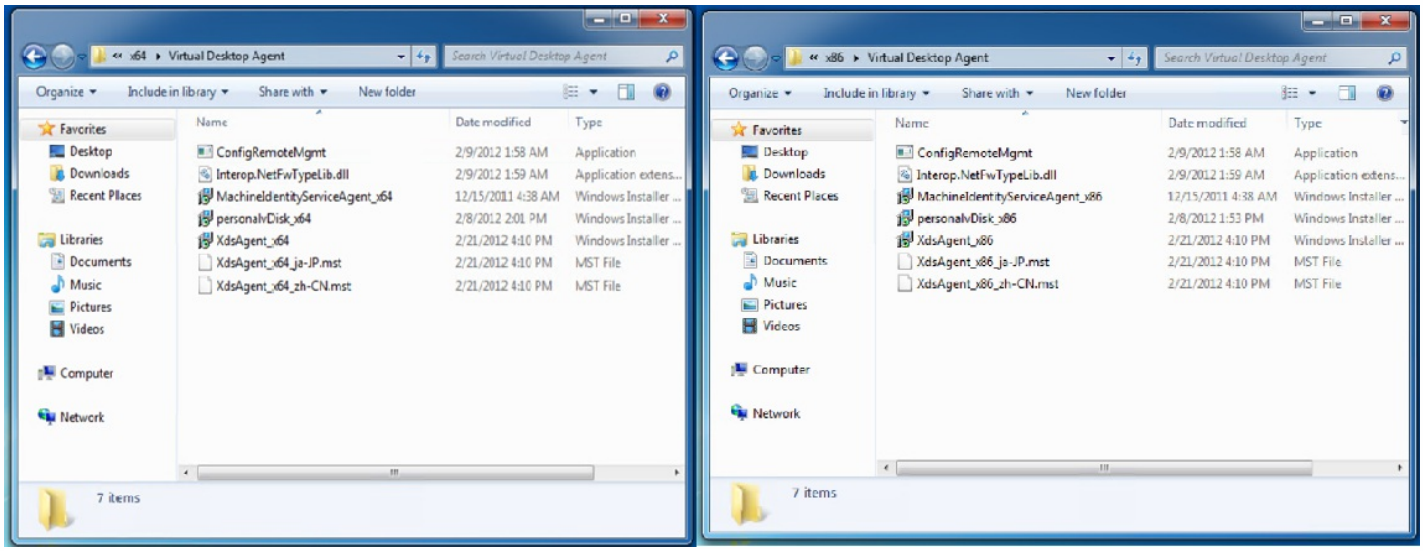
卸载 PvD 时的重要注意事项

在基础映像中安装了具有 Windows 7（64 位）的个人虚拟磁盘时，卸载可能会失败。要解决此问题，Citrix 建议您先删除个人虚拟磁盘，然后再进行升级：

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

1. 从 XenApp/XenDesktop 介质中选择虚拟磁盘安装程序的恰当副本。从 XenApp/XenDesktop ISO 的以下目录之一中找到最新的个人虚拟磁盘 MSI 安装程序（取决于升级后的 VM 是 32 位还是 64 位）：

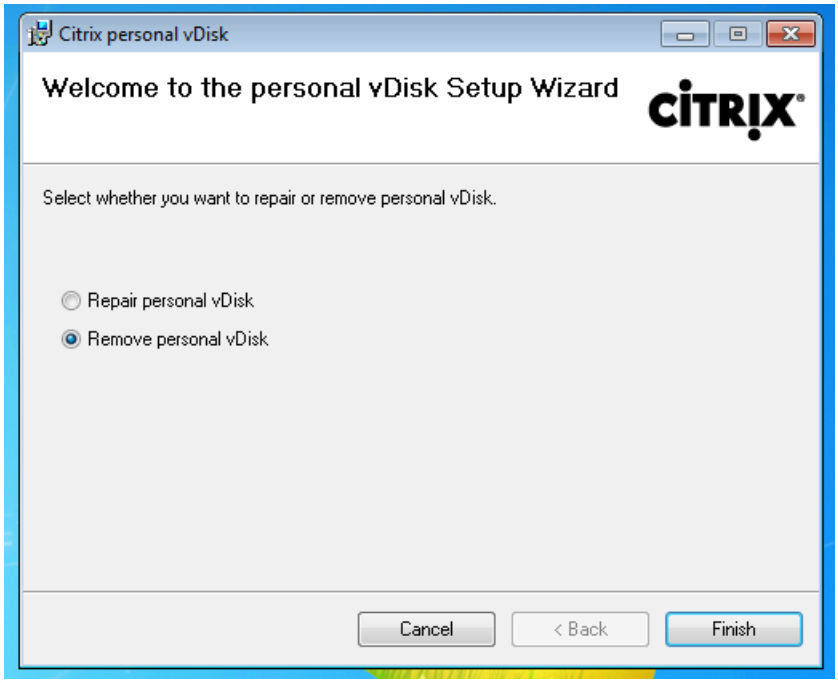
- 32 位：XA and XD\x86\Virtual Desktop Components\personalvDisk_x86.msi
- 64 位：XA and XD\x64\Virtual Desktop Components\personalvDisk_x64.msi



2. 删除个人虚拟磁盘安装。选择在步骤 1 中找到的个人虚拟磁盘 MSI 安装程序包。此时将显示个人虚拟磁盘安装程序屏幕。

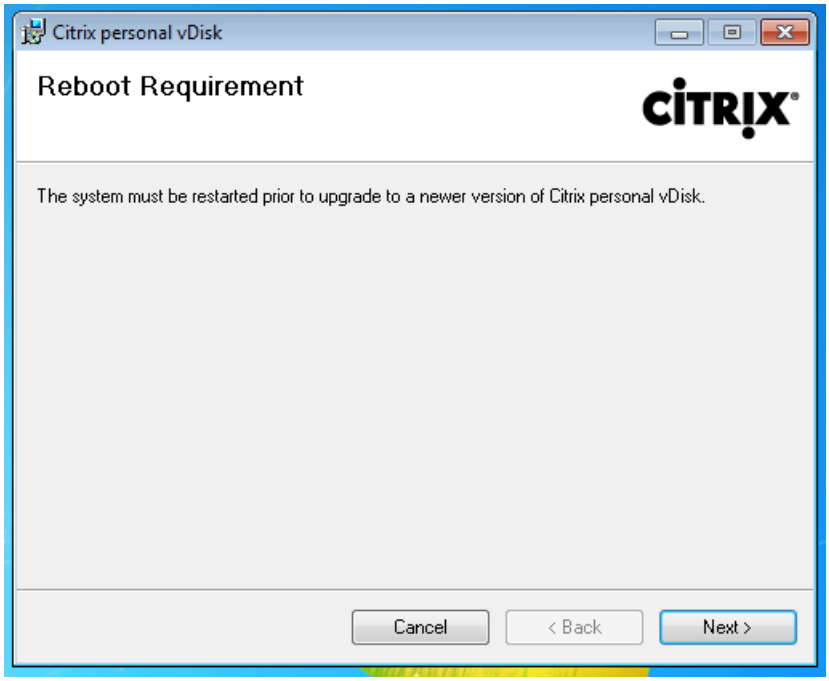
3. 选择“Remove personal vDisk”（删除个人虚拟磁盘）。

4. 单击**完成**。

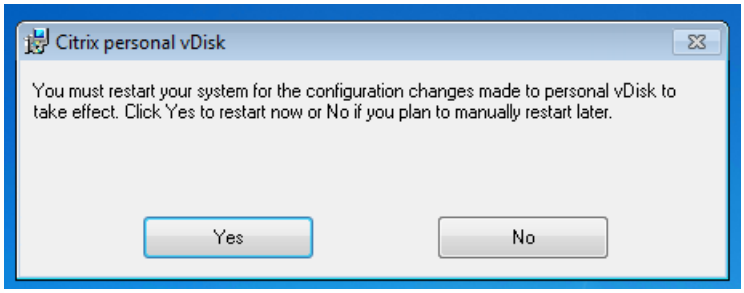


5. 此时将显示“Reboot Requirement”（重启要求）页面。单击 **Next**（下一步）：

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



6. 单击 Yes（是）重新启动系统并应用您对配置所做的更改：



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

配置与管理

Dec 05, 2017

本主题介绍配置和管理 Personal vDisk (PvD) 环境时需要考虑的项目，其中还包括最佳做法指导原则和任务描述。

对于 包括使用 Windows 注册表的过程：
小心：注册表编辑不当会导致严重问题，可能需要重新安装操作系统。 Citrix 无法保证因“注册表编辑器”使用不当导致出现的问题能够得以解决。 使用“注册表编辑器”需自担风险。在编辑注册表之前，请务必进行备份。

以下因素影响主个人虚拟磁盘卷的大小：

- **用户将在其 PvD 上安装的应用程序的大小**
  重新启动时，PvD 会确定应用程序区域 (UserData.v2.vhd) 中剩余的可用空间。如果可用空间低于 10%，应用程序区域将扩展到任何未使用的配置文件区域空间中（默认为驱动器 P: 上的可用空间）。添加到应用程序区域的空间大约占应用程序区域和配置文件区域中剩余的总可用空间的 50%。

  例如，如果 10 GB PvD 上的应用程序空间（默认大小为 5 GB）达到 4.7 GB，配置文件区域具有 3 GB 可用空间，则添加到应用程序区域的新增空间的计算方法如下：

  增加的空间 = (5.0-4.7)/2 + 3.0/2 = 1.65 GB

  添加到应用程序区域的空间只是一个大约值，因为会提供小额的补贴空间来存储日志以及用于开销。计算及可能的调整大小操作在每次重新启动时执行。

- **用户配置文件的大小（如果未使用独立的配置文件管理解决方案）**
  除应用程序所需的空间外，还应确保个人虚拟磁盘上有足够的可用空间来存储用户的配置文件。计算空间要求时请包括任何非重定向特殊文件夹（如“我的文档”和“我的音乐”）。可以从“控制面板”(sysdm.cpl) 获取现有配置文件的大小。

  某些配置文件重定向解决方案存储存根文件（标记文件）而非真实的配置文件数据。这些配置文件解决方案可能显示为最初未存储任何数据，但实际上每个存根文件占用文件系统中的一个文件目录条目；通常情况下，此数量大约为每个文件 4 KB。如果您采用此类解决方案，必须根据实际的配置文件数据（而非存根文件）来预估大小。

  企业文件共享应用程序（如 ShareFile 和 Dropbox）可能会将数据同步或下载到个人虚拟磁盘上的用户配置文件区域。如果您采用此类解决方案，预估大小时必须包括足够的空间来存储此数据。

- **包含 PvD 清单的模板 VHD 占用的开销**
  模板 VHD 包含 PvD 清单数据（与主映像内容对应的标记文件）。PvD 应用程序区域将基于此 VHD 创建。由于每个 sentinel 文件或文件夹由文件系统中的文件目录条目组成，因此，模板 VHD 内容将占用 PvD 应用程序空间，即使在最终用户安装任何应用程序之前也是如此。可以通过在创建清单后浏览主映像来确定模板 VHD 的大小。或者，也可以使用以下等式估算其大小：

  模板 VHD 大小 = (基础映像上的文件数) x 4 KB

  可以通过在基础 VM 映像中的驱动器 C: 上单击鼠标右键并选择属性来确定文件和文件夹的数量。例如，包含 25 万个文件的映像的模板 VHD 大小约为 1,024,000,000 字节（接近 1 GB）。此空间不可用于 PvD 应用程序区域中的应用程序安装。

- **PvD 映像更新操作的开销**
  执行 PvD 映像更新操作期间，PvD 的根目录处（默认为 P:）必须有足够的可用空间，以便合并来自两个映像版本的变更以及用户对其 PvD 所做的更改。通常情况下，PvD 会预留几百 MB 空间用于此目的，但写入到 P: 驱动器的额外数据可能会占

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

用这些预留的空间，致使没有足够的空间来成功完成映像更新。PvD 池统计数据脚本（位于 XenDesktop 安装介质上的 Support/Tools/Scripts 文件夹中）或 PvD 映像更新监视工具（位于 Support/Tools/Scripts\PvdTool 文件夹中）可以帮助识别目录中正在更新以及接近满载的 PvD 磁盘。

如果存在防病毒产品，可能会影响运行清单或执行更新所需的时间。如果将 CtxPvD.exe 和 CtxPvDSvc.exe 添加到防病毒产品的排除列表，则可以提高性能。这些文件位于 C:\Program Files\Citrix\personal vDisk\bin 中。从防病毒软件执行的扫描中排除这些可执行文件最高可将清单和映像更新的性能提升十倍。

- **非预期增长（非预期应用程序安装等）的开销**
  考虑在总大小的基础上额外留出一定的空间（固定量或虚拟磁盘大小的百分比），用于用户在部署期间执行的任何非预期应用程序安装。

可以通过设置 VHD 的初始大小手动调整用于决定相对于驱动器 P: 的 VHD 大小的自动调整大小算法。 例如，如果您知晓用户将安装大量应用程序，但这些应用程序过大，无法安装在 VHD 上，即使通过算法调整大小之后也是如此，则此操作将非常有用。 在此情况下，可以增加应用程序空间的初始大小，以容纳用户安装的应用程序。

更可取的做法是调整主映像上的 VHD 的初始大小。 或者，当用户没有足够的空间来安装应用程序时，也可以调整虚拟桌面上 VHD 的大小。 但是，必须在每个受影响的虚拟桌面上分别重复此操作；无法调整已创建目录中的 VHD 初始大小。

请确保 VHD 足够大，能够存储防病毒定义文件，这些文件通常都非常大。

查找并设置 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\personal vDisk\Config 中的注册表项。 （请勿修改此注册表项中的其他设置。）所有设置必须在主映像上指定（MinimumVHDSizeInMB 除外，可以在单台计算机上更改此设置）；在主映像上指定的设置在下一次映像更新时应用。

- MinimumVHDSizeMB
  指定 个人虚拟磁盘的应用程序部分 (C:) 的最低大小（以 MB 为单位）。 新大小必须大于现有大小，但小于磁盘 大小减去 PvDReservedSpaceMB 所得的值。

  增大 此值会将虚拟磁盘上配置文件部分中的可用空间分配给 C:。如果 使用的值小于当前 C: 驱动器的大小，或者如果 EnableDynamicResizeOfAppContainer 设置为 0， 则将忽略此设置。

  默认值 = 2048

- EnableDynamicResizeOfAppContainer
  启用或 禁用动态调整大小算法。
  - 设置为 1 时，当 C: 上的可用空间下降到 10% 以下时，应用程序空间（位于 C: 上）将自动调整大小。 允许使用的值为 1 和 0。需要重新启动才能使调整的大小生效。
  - 设置为 0 时，将根据 7.x 之前的 XenDesktop 版本中使用的方法确定 VHD 的大小。

  默认值 = 1

- EnableUserProfileRedirection
  启用或 禁用将用户的配置文件重定向到虚拟磁盘。
  - 设置为 1 时，PvD 将用户的配置文件重定向到个人虚拟磁盘驱动器（默认情况下为 P:）。 配置文件通常重定向到 P:\Users，与标准 Windows 配置文件相对应。 此重定向会保留配置文件，以防需要重置 PvD 桌面。
  - 如果设置为 0，虚拟磁盘上的所有空间减去 PvDReservedSpaceMB 所得的值将分配给 C:，即虚拟磁盘应用程序部分，并且虚拟磁盘驱动器 (P:) 在 Windows 资源管理器中处于隐藏状态。 Citrix 建议在使用 Citrix Profile Management 或其他漫游配置文件解决方案时通过将此设置更改为 0 来禁用重定向。
    此设置会将配置文件保留在 C:\Users 中（而非将其重定向到虚拟磁盘），并使漫游配置文件解决方案能够处理配置文

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

件。

此值可确保将 P: 上的所有空间都分配给应用程序。

本主题做以下假设，即将此值设置为 0 时，配置文件管理解决方案已准备就绪。 如果漫游配置文件解决方案未准备就绪，则建议不要禁用配置文件重定向，因为后续的 PvD 重置操作会导致删除配置文件。

更新映像时请勿更改 此设置，因为此设置不会更改现有配置文件的位置， 但会将个人虚拟磁盘上的所有空间分配 给 C: 并隐藏 PvD。

请在部署目录前 配置此值。部署目录后无法更改 此值。

重要：自 XenDesktop 7.1 以来，执行映像更新时不会 保留对此值所做的更改。在第一次创建配置文件的 来源目录时设置密钥值。以后将无法修改 重定向行为。
默认值 = 1

- PercentOfPvDForApps
  设置 虚拟磁盘的应用程序部分 (C:) 与配置文件部分之间的拆分。如果 将 EnableDynamicResizeOfAppContainer 设置为 0，则创建新 VM 时以及执行映像更新期间会使用此值。

  仅当 将 EnableDynamicResizeOfAppContainer 设置为 0 时， 更改 PercentOfPvDForApps 设置才会产生差别。默认情况下， 将 EnableDynamicResizeOfAppContainer 设置为 1（启用），这意味着仅当 AppContainer（您看到的是 C 驱动器）接近满载时，也就是可用空间低于 10% 时， 才得以扩展（即动态扩展）。

  增大 PercentOfPvDForApps 时仅增大允许 Apps 部分 扩展到的最大空间。该操作不会立即置备空间。您还 必须在主映像中配置拆分分配，所配置的设置将 在下次映像更新时应用。

  如果已 在将 EnableDynamicResizeOfAppContainer 设置为 1 的情况下生成计算机目录，请在主映像中将此设置更改为 0，以便下次 更新时应用，并配置一个恰当的分配拆分。只要请求的拆分大小 大于当前为 C 驱动器分配的大小， 则始终应用该大小。

  如果您希望 保持对空间拆分的完整控制，应将此值设置为 0。这 允许您完整控制 C 驱动器的大小，而不依赖占用的空间 低于阈值的用户扩展该驱动器。

  默认值：50% （为两部分分配相等的空间）

- PvDReservedSpaceMB
  指定虚 拟磁盘上为存储 Personal vDisk 日志及其他数据 而保留的空间大小（以 MB 为单位）。

  如果 您的部署包含 XenApp 6.5（或更早的版本）并使用应用程序 流技术推送，请根据 Rade 缓存的大小增大此值。

  默认值 = 512

- PvDResetUserGroup
  仅适用于 XenDesktop 5.6 - 允许指定的用户组重置个人虚拟磁盘。 之后的 XenDesktop 版本使用委派管理员实现此目的。

其他设置：

- **Windows Update 服务** - 确保在主映像中将 Windows 更新设置为 从不 检查更新，将 Windows Update 服务设置为 已禁用。如果需要在 PvD 上运行 Windows Update 服务，将其设置为 从不 检查更新有助于阻止在 关联的计算机上安装更新。Windows 8 应用商店需要运行此服务才能安装现代风格的应用程序。

- **Windows 更新** - 包括 Internet Explorer 更新，必须在主映像上应用。

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

- **更新要求 重新启动** - 应用到主映像的 Windows 更新可能要求 多次重新启动才能完全安装，具体取决于这些更新提供的 修补程序类型。请务必先正确重新启动主映像以全面完成应用到该映像的任何 Windows 更新的安装，然后再创建 PvD 清单。
- **应用程序更新** - 更新主映像上安装的应用程序以节省用户虚拟磁盘上的空间。 此设置还可避免重复更新每个用户的虚拟磁盘上的应用程序。

某个软件可能与 PvD 组成用户环境的方式相冲突，因此，必须将其安装在主映像上（而不是单台计算机上）以避免这些冲突。此外，尽管某些其他软件并不会与 PvD 操作冲突，Citrix 还是建议将其安装在主映像上。

必须安装在主映像上的应用程序：
- 代理和客户端（例如，System Center Configuration Manager Agent、App-V 客户端、Citrix Receiver）
- 用于安装或修改早期启动驱动程序的应用程序
- 用于安装打印机或扫描仪软件/驱动程序的应用程序
- 用于修改 Windows 网络堆栈的应用程序
- VMware Tools 和 XenServer Tools 等 VM 工具

应该安装在主映像上的应用程序：
- 分发给大量用户的应用程序。 在每种情况下，都请在部署之前关闭应用程序更新：
  - 使用批量许可的企业应用程序，例如 Microsoft Office、Microsoft SQL Server
  - 常见应用程序，例如 Adobe Reader、Firefox 和 Chrome
- 大型应用程序（例如 SQL Server、Visual Studio）和应用程序框架（例如 .NET）

以下建议和限制适用于用户在具有个人虚拟磁盘的桌面上安装的应用程序。 如果用户具有管理特权，则不能强制执行其中某些建议和限制：
- 用户不应卸载主映像上的应用程序并在其个人虚拟磁盘上重新安装相同的应用程序。
- 更新或卸载主映像上的应用程序时应小心谨慎。 在映像上安装某个版本的应用程序时，用户可能会安装一个需要此版本的加载项应用程序（例如插件）。 如果存在此类依赖项，则更新或卸载该映像上的应用程序可能会导致加载项无法正常使用。例如，在主映像上安装 Microsoft Office 2010 后，用户在其个人虚拟磁盘中安装 Visio 2010。 以后升级主映像上的 Office 可能会导致本地安装的 Visio 不可用。
- 不支持具有依赖于硬件的许可证的软件（通过硬件保护装置或基于签名的硬件）。

同时使用 Provisioning Services 和 PvD 时：
- 必须将 Soap Service 帐户添加到 Citrix Studio 的“管理员”节点，并且必须具有“计算机管理员”或权限更高的角色。这样可确保在将 Provisioning Services (PVS) 虚拟磁盘提升到生产模式时将 PvD 桌面置于“正在准备”状态。
- 必须使用 Provisioning Service 版本控制功能来更新 Personal vDisk。将版本提升到生产模式时，Soap Service 会将 PvD 桌面置于“正在准备”状态。
- 个人虚拟磁盘的大小应始终大于 Provisioning Services 写入缓存磁盘的大小（否则，Provisioning Services 可能错误地选择个人虚拟磁盘用作其写入缓存）。
- 创建交付组后，可以使用 PvD 映像更新监视工具或 resize 和 poolstats 脚本 (personal-vdisk-poolstats.ps1) 监视个人虚拟磁盘。

正确设置写入缓存磁盘的大小。正常操作期间，PvD 捕获大多数用户写入（更改）并将其重定向到个人虚拟磁盘。这表示您可以降低 Provisioning Services 写入缓存磁盘的大小。但是，当 PvD 不活动时（例如执行映像更新操作期间），小型 Provisioning Services 写入缓存磁盘可能会填满数据，导致计算机崩溃。

Citrix 建议根据 Provisioning Services 最佳做法来确定 Provisioning Services 写入缓存磁盘的大小，并且添加大小等于主映像上的模板 VHD 大小两倍的额外空间（以适应合并要求）。合并操作需要所有这些空间的可能性非常低，但仍存在这种可能性。

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

使用 Provisioning Services 部署包含启用 PvD 的计算机的目录时：

- 请遵循 Provisioning Services 文档中的指南。
- 可以通过编辑 Studio 中的连接，更改电源操作限制设置；请参阅下文。
- 如果更新 Provisioning Services 虚拟磁盘，请在安装/更新应用程序和其他软件并重新启动虚拟磁盘后，运行 PvD 清单，然后关闭 VM。然后，将新版本提升到生产模式。目录中的 PvD 桌面应自动进入“正在准备”状态。如果没有进入此状态，请检查 Soap Service 帐户在 Controller 上是否具有计算机管理员权限或更高权限。

利用 Provisioning Services 测试模式功能，您可以创建包含使用已更新主映像的计算机的目录。如果测试确认了测试目录的可行性，则可以将其提升为生产模式。

使用 Machine Creation Services (MCS) 部署包含启用 PvD 的计算机的目录时：

- 请遵循 XenDesktop 文档中的指南。
- 创建主映像后运行 PvD 清单，然后关闭 VM（如果不关闭 VM，PvD 无法正常运行。）然后，创建主映像的快照。
- 在“创建计算机目录”向导中，指定个人虚拟磁盘大小和驱动器盘符。
- 创建交付组后，可以使用 PvD 映像更新监视工具或 resize 和 poolstats 脚本 (personal-vdisk-poolstats.ps1) 监视个人虚拟磁盘。
- 可以通过编辑 Studio 中的连接，更改电源操作限制设置；请参阅下文。
- 如果您更新主映像，请在更新映像上的应用程序和其他软件后运行 PvD 清单，然后关闭 VM。然后，创建主映像的快照。
- 使用 PvD 映像更新监视工具或 personal-vdisk-poolstats.ps1 脚本验证将使用更新后的主映像且启用 PvD 的每个 VM 上是否有足够的空间。
- 更新计算机目录后，PvD 桌面进入“正在准备”状态，因为它们各自分别处理新主映像中的更改。这些桌面根据在计算机更新过程中指定的前滚策略进行更新。
- 使用 PvD 映像更新监视工具或 personal-vdisk-poolstats.ps1 脚本监视处于“正在准备”状态的 PvD。

使用规则文件从虚拟磁盘排除文件和文件夹。 可以在部署个人虚拟磁盘期间执行此项操作。 规则文件按 custom_*_rules.template.txt 格式命名并存储在 \config 文件夹中。 各个文件中的注释提供了其他文档。

如果启用 PvD 并在安装后对主映像进行了更新，之后应刷新磁盘的清单（称为“运行清单”）并创建新快照，这一点很重要。

由于管理员（而非用户）管理主映像，因此，如果您安装的某个应用程序将二进制文件放在管理员的用户配置文件中，则共享虚拟桌面（包括基于池计算机目录以及使用 PvD 的池计算机目录的共享虚拟桌面）的用户将无法使用此应用程序。用户必须自己安装此类应用程序。

完成下述过程中的每个步骤后，最好生成一张映像快照。

1. 通过执行以下操作升级主映像：安装任何应用程序或操作系统更新，然后在计算机上执行任何系统配置操作。
   对于以要通过 Personal vDisk 部署的 Windows XP 为基础的主映像，请确认未打开任何对话框（例如，确认软件安装情况的消息或使用未签名驱动程序的提示）。此环境中主映像上打开的对话框将阻止 VDA 注册到 Delivery Controller。可以使用“控制面板”防止显示使用未签名应用程序的提示。例如，导航到“系统”>“硬件”>“驱动程序签名”，然后选择忽略警告对应的选项。
2. 关闭计算机。对于 Windows 7 计算机，请在 Citrix Personal vDisk 阻止关机时单击取消。
3. 在 Citrix Personal vDisk 对话框中，单击更新清单。此步骤可能需要几分钟时间才能完成。
   重要：如果您中断了随后的关机过程（即使是对映像执行少量更新），Personal vDisk 的清单也不再与主映像一致。这将导致 Personal vDisk 功能停止运行。如果您中断了关闭过程，则必须重新启动计算机，将其关闭，然后在系统提示时再次单击

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

更新清单。

4. 清单操作关闭计算机后，请生成一张主映像快照。

可以将清单导出到网络共享，然后再将此清单导入到主映像。有关详细信息，请参阅导出和导入 PvD 清单。

Citrix Broker Service 控制提供桌面和应用程序的计算机的电源状态。 Broker Service 可以通过一个 Delivery Controller 控制多个虚拟机管理程序。 Broker 电源操作控制 Controller 与虚拟机管理程序之间的交互。 为避免虚拟机管理程序过载，向更改计算机电源状态的操作分配优先级，并使用限制机制将其发送到虚拟管理程序。 以下设置影响限制。 可以通过在 Studio 中编辑连接（“高级”页面）指定这些值。

要配置连接限制值，请执行以下操作：

1. 在 Studio 导航窗格中，选择“配置”>“托管”。
2. 选择 连接，然后在“操作”窗格中选择 编辑 连接。
3. 可以更改以下值：
   - **同步操作(所有类型)** - 允许同时进行的电源操作的最大数。 此设置同时指定虚拟机管理程序连接的绝对值和百分比。 使用两个值中的较小值。
     默认值：绝对值 100，20%
   - **同步个人虚拟存储清单更新** - 允许并发的个人虚拟磁盘电源操作的最大数。 此设置同时指定连接的绝对值和百分比。 使用两个值中的较小值。
     默认值：绝对值 50，25%

     计算绝对值：确定最终用户存储支持的 IOPS 总数 (TIOPS)（此值由制造商指定或通过计算机得出）。 每个 VM 使用 350 次 IOPS (IOPS/VM)，确定在给定时间存储上应该活动的 VM 数。 通过使用 IOPS 总数除以 IOPS/VM 计算此值。

     例如，如果最终用户存储为 14000 IPS，则活动 VM 数为 14000 IOPS / 350 IOPS/VM = 40。
   - **每分钟最大新操作数** - 每分钟可以发送给虚拟机管理程序的最大新电源操作数。 以绝对值形式提供。
     默认值 = 10

为帮助找出部署中有关这些设置的最佳值，请遵循以下说明：

1. 使用默认值测量测试目录的映像更新所需的总响应时间。 此值是指映像更新开始时间 (T1) 与目录中的最后一台计算机上的 VDA 向 Controller 注册的时间 (T2) 之间的差。 总响应时间 = T2 - T1。
2. 测量映像更新期间虚拟机管理程序存储的每秒钟输入/输出操作数 (IOPS)。 此数据可用作优化基准。（默认值可能是最佳设置；但是，系统也可能会达到最大 IOPS，此时需要降低设置值。）
3. 请按照下面的描述降低“同步个人虚拟存储清单更新”值（保持其他所有设置不变）。
   1. 将此值增加 10，并在每次更改后测量总响应时间。 继续将此值增加 10 并测试结果，直到总响应时间降低或无变化。
   2. 如果前一步的结果显示通过增加值未得到改善，则以 10 为增量降低此值，并在每次降低后测量总响应时间。 重复此步骤，直到总响应时间保持不变或未得到进一步改善。 此值很可能就是最佳的 PvD 电源操作值。
4. 获得 PvD 电源操作设置值后，调整“同步操作(所有类型)”值和“每分钟最大新操作数”值，每次调整一个。 按照以上所述过程（按增量增加或降低）测试其他值。

System Center Configuration Manager (Configuration Manager) 2012 无需任何特殊配置，可以像安装其他主映像应用程序那样安装。 下列信息仅适用于 System Center Configuration Manager 2007。 不支持 Configuration Manager 2007 之前的 Configuration Manager 版本。

要在 PvD 环境中使用 Configuration Manager 2007 代理软件，请完成以下步骤。

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

1. 在主映像上安装客户端代理。
    1. 在主映像上安装 Configuration Manager 客户端。
    2. 停止并禁用 ccmexec 服务（SMS 代理）。
    3. 按如下所示从本地计算机证书存储中删除 SMS 或客户端证书：
        - 混合 模式：证书(本地计算机)\SMS\证书
        - 本机模式
            - 证书(本地计算机)\个人\证书
            - 删除证书颁发机构颁发的客户端证书（通常为内部公钥基础结构）
    4. 删除或重命名 C:\Windows\smscfg.ini。
2. 删除唯一标识客户端的信息。
    1. （可选）删除或移动 C:\Windows\System32\CCM\Logs 中的日志文件。
    2. 安装 Virtual Delivery Agent（如果以前未安装）并创建 PvD 清单。
    3. 关闭主映像，创建快照，然后使用此快照创建计算机目录。
3. 验证 Personal vDisk 并启动服务。 在每个 PvD 桌面首次启动后执行一次这些步骤。 例如，可以使用域 GPO 完成此操作。
    - 通过检查是否存在注册表项 HKLM\Software\Citrix\personal vDisk\config\virtual 来确认 PvD 处于活动状态。
    - 将 ccmexec 服务（SMS 代理）设置为“自动”并启动该服务。 Configuration Manager 客户端与 Configuration Manager 服务器联系，并检索新的唯一证书和 GUID。

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

工具

Dec 05, 2017

可以使用以下工具和实用程序自定义、加快和监视 PvD 操作。

利用 PvD 提供的自定义规则文件，可以采用以下方式修改 PvD 映像更新的默认行为：

- PvD 上的文件的可见性
- 如何合并对文件所做的更改
- 文件是否可写入

有关自定义规则文件及 CoW 功能的详细说明，请参阅位于以下位置的文件中的注释：安装了 PvD 的计算机上的 C:\ProgramData\Citrix\personal vDisk\Config。 名为 custom_* 的文件介绍了相关规则及其启用方法。

提供了两个用于监视和管理 PvD 大小的脚本，位于 XenDesktop 安装介质中的 Support\Tools\Scripts 文件夹中。 还可以使用 PvD 映像更新监视工具，位于 Support\Tools\Scripts\PvdTool 文件夹中；有关详细信息，请参阅 http://blogs.citrix.com/2014/06/02/introducing-the-pvd-image-update-monitoring-tool/ 。

使用 resize-personalvdisk-pool.ps1 可增大某个目录的所有桌面中的 PvD 的大小。 必须在运行 Studio 的计算机上为您的虚拟机管理程序安装以下管理单元或模块：

- XenServer 需要 XenServerPSSnapin
- vCenter 需要 vSphere PowerCli
- System Center Virtual Machine Manager 需要 VMM 控制台

使用 personal-vdisk-poolstats.ps1 可检查映像更新的状态以及一组 PvD 中的应用程序和用户配置文件的空间。 在更新映像之前运行此脚本可检查任何桌面的空间是否已不足，有助于防止更新失败。 此脚本要求在 PvD 桌面上启用 Windows Management Instrumentation (WMI-In) 防火墙。 可以在主映像上或通过 GPO 启用该防火墙。

如果映像更新失败，则“Update”（更新）列中的条目将指出原因。

如果桌面损坏（由于安装损坏的应用程序或某些其他原因所致），可以将 PvD 的应用程序区域恢复到出厂默认（空）状态。 重置操作会使用户配置文件数据保持不变。

要重置 PvD 的应用程序区域，请使用以下方法之一：

- 以管理员身份登录用户的桌面。 启动命令提示窗口并运行命令 C:\Program Files\Citrix\Personal vDisk\bin\CtxPvD.exe -s Reset。
- 在 Citrix Director 中找到用户的桌面。 单击 重置 个人虚拟磁盘，然后单击 确定。

映像更新过程是将新映像推向 PvD 桌面的不可或缺部分，其中包括调整现有个人虚拟磁盘以用于新基础映像。 对于使用 Machine Creations Services (MCS) 的部署，可以将清单从活动 VM 导出到网络共享，然后再将其导入到主映像中。 在主映像中使用此清单计算差额。 尽管不强制使用导出/导入清单功能，但是此功能可以提高整个映像更新过程的性能。

要使用导出/导入清单功能，您必须是管理员。 如果需要，请使用“net use”向用于导出/导入的的文件共享进行身份验证。 用户上下文必须可以访问用于导出/导入的任何文件共享。

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

- 要导出清单，请在包含 VDA（版本最低为 7.6）且启用了 PvD 的计算机上以管理员身份运行导出命令：
  Ctxpvdsvc.exe exportinventory “<path-to-export-location>”

  软件会 检测当前清单的位置，并将清单导出到指定位置上 名为“ExportedPvdInventory”的文件夹中。下面是 命令输出摘录：
  C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe exportinventory
  \\share location\ExportedInventory
  Current inventory source location C:\CitrixPvD\Settings\Inventory\VER-LAS
  ...
  Exporting current inventory to location \\ ….
  ...
  Deleting any pre-existing inventory folder at \\ ….
  .Successfully exported current inventory to location \\ …. 错误代码 = OPS
- 要导入之前导出的清单，请在主映像上以管理员身份运行导入命令：

导入

在主映像上以管理员身份运行导入命令。

Ctxpvdsvc.exe importinventory “<path-to-exported-inventory>”

<path to exported inventory> 应为清单文件的完整路径，通常为 <network location\ExportedPvdInventory>。

从导入位置获取清单（之前使用 exportinventory 选项导出清单的位置）并将清单导入到主映像上的清单存储。 下面是命令输出摘录：
C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe importinventory
\\share location\ExportedInventory\ExportedPvdInventory
Importing inventory \\share location\ExportedInventory\ExportedPvdInventory
…
Successfully added inventory \\share location\ExportedInventory\ExportedPvdInventory to the
store at c:\ProgramData\Citrix\personal vDisk\InventoryStore
导出后，网络共享应包含以下文件名。 导入后，主映像上的清单存储中应包含相同的文件名。

- Components.DAT
- files_rules
- folders_rules
- regkey_rules
- RINGTHREE.DAT
- S-1-5-18.DAT
- SAM.DAT
- SECURITY.DAT
- SNAPSHOT.DAT
- SOFTWARE.DAT
- SYSTEM.CurrentControlSet.DAT
- VDCATALOG.DAT
- vDiskJournalData

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

显示、消息和故障排除

Dec 05, 2017

通过报告监视 PvD

可以使用诊断工具监视用户对其个人虚拟磁盘的用户数据部分和应用程序部分进行的更改。这些更改包括用户已安装的应用程序和他们修改的文件。更改存储在一组报告中。

1. 在要监视的计算机上，运行 **C:\Program Files\Citrix\personal vDisk\bin\CtxPvdDiag.exe**。
2. 浏览到要存储报告和日志的位置，选择要生成的报告，然后单击**确定**。下面列出了可用的报告。

软件配置单元报告：此报告生成两个文件：Software.Dat.Report.txt 和 Software.Dat.delta.txt。

oftware.Dat.Report.txt 文件记录用户对 HKEY_LOCAL_MACHINE\Software 配置单元所做的更改。它包括以下部分：

- 在基础上安装的应用程序的列表 — 第 0 层安装的应用程序。
- 用户已安装软件的列表 — 用户在个人虚拟磁盘的应用程序部分安装的应用程序。
- 用户卸载的软件的列表 — 用户删除的之前存在于 0 层的应用程序。

有关 Software.Dat.delta.txt 的信息，请参阅配置单元增量报告。

系统配置单元报告：生成的 SYSTEM.CurrentControlSet.DAT.Report.txt 文件记录用户对 HKEY_LOCAL_MACHINE\System 配置单元所做的更改。它包括以下部分：

- 用户安装的服务的列表 — 用户安装的服务和驱动程序。
- 更改了以下服务的启动 — 用户更改了启动类型的服务和驱动程序。

安全配置单元报告：生成的 SECURITY.DAT.Report.txt 文件监视用户在 HKEY_LOCAL_MACHINE\Security 配置单元中所做的全部更改。

Security Account Manager (SAM) 配置单元报告：生成的 SAM.DAT.Report.txt 文件监视用户在 HKEY_LOCAL_MACHINE\SAM 配置单元中所做的全部更改。

配置单元增量报告：生成的 Software.Dat.delta.txt 文件记录添加或删除的所有注册表项和值，以及用户在 HKEY_LOCAL_MACHINE\Software 配置单元中修改的所有值。

Personal vDisk 日志：默认情况下，在 P:\Users\<用户帐户>\AppData\Local\Temp\PVDLOGS 生成日志文件 Pud-IvmSupervisor.log、PvDActivation.log、PvDSvc.log、PvDWMI.log、SysVol-IvmSupervisor.log 和 vDeskService-<#>.log，但是这些文件会被移到选定的位置。

Windows 操作系统日志：

- EvtLog_App.xml 和 EvtLog_System.xml 是来自个人虚拟磁盘卷的 XML 格式的应用程序和系统事件日志。
- Setupapi.app.log 和 setuperr.log 包含 Personal vDisk 安装期间自 msiexec.exe 开始运行起生成的日志消息。
- Setupapi.dev.log 包含设备安装日志消息。
- Msinfo.txt 包含 msinfo32.exe 的输出。有关信息，请参阅 Microsoft 文档。

文件系统报告：生成的 FileSystemReport.txt 文件记录用户在以下部分对文件系统所做的更改：

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

- 重新定位的文件 — 用户由 0 层移至虚拟磁盘中的文件。0 层文件是由个人虚拟磁盘所连接的计算机从主映像继承的文件。
- 删除的文件 — 通过用户的操作（例如，删除应用程序）隐藏的 0 层文件。
- 添加的文件（MOF、INF、SYS） — 用户添加到个人虚拟磁盘的带有 .mof、.inf 或 .sys 扩展名的文件（例如，当用户安装 Visual Studio 2010 等注册 .mof 文件以供自动恢复的应用程序时）。
- 添加的其他文件 — 用户添加到虚拟磁盘的其他文件（例如，当用户安装应用程序时）。
- 修改但未重新定位的基础文件 — 已由用户修改但个人虚拟磁盘内核模式驱动程序未在虚拟磁盘中捕获到的 0 层文件。

映像更新

在 Studio 中，选择计算机目录中启用 PvD 的计算机时，“PvD”选项卡将提供映像更新期间的监视状态，以及预计完成时间和进度。在映像更新期间可能显示的状态为：就绪、正在准备、正在等待、失败和已请求。

映像更新失败可能由多种不同的原因，包括空间不足，或者桌面在足够的时间内未找到 PvD。Studio 指示映像更新失败时，会提供错误代码和描述性文本，以帮助进行故障排除。使用 Personal vDisk 映像更新监视工具或 personal-vdisk-poolstats.ps1 脚本监视映像更新进度并获取与失败有关的错误代码。

如果映像更新失败，以下日志文件可提供进一步的故障排除信息：
- PvD 服务日志 - C:\ProgramData\Citrix\personal vDisk\Logs\PvDSvc.log.txt
- PvD 激活日志 - P:\PVDLOGS\PvDActivation.log.txt

最近的内容显示在日志文件结尾。

以下错误消息对 PvD 7.6 及更高版本有效：
- **发生了内部错误。请查看 Personal vDisk 日志，进一步了解详细信息。错误代码 %d (%s)**
  此错误是对未分类错误的概括，因此没有数字值。在清单创建或 Personal vDisk 更新过程中遇到的所有异常错误均通过此错误代码指出。
  - 请收集日志并联系 Citrix 技术支持。
  - 如果此错误出现在目录更新过程中，请将目录回滚到之前的主映像版本。
- **规则文件中存在语法错误。请查看日志，进一步了解详细信息。**
  错误代码 2。规则文件包含语法错误。Personal vDisk 日志文件包含规则文件的名称和发现语法错误的行号。请修复规则文件中的语法错误，然后重试操作。
- **个人虚拟磁盘中存储的与早期版本的主映像对应的清单已损坏或无法访问。**
  错误代码 3。最近的清单存储在 \ProgramData\CitrixPvD\Settings\Inventory\VER-LAST 下的 UserData.V2.vhd 中。请通过从与早期主映像版本关联的已知可用的 PvD 计算机导入“VER-LAST”文件夹，还原与主映像的最近版本对应的清单。
- **个人虚拟磁盘中存储的与早期版本的主映像对应的清单版本较高。**
  错误代码 4。此错误是由于个人虚拟磁盘版本在最近的主映像与当前主映像之间不兼容所致。请在主映像中安装最新个人虚拟磁盘版本后重新尝试更新目录。
- **检测到变更日志工作流。**
  错误代码 5。USN 日志溢出是由于在创建清单过程中对主映像进行了大量更改所致。如果在多次尝试后仍出现此情况，请使用 procmon 来确定是否存在第三方软件在清单创建过程中创建/删除大量文件的情况。
- **Personal vDisk 找不到连接到系统的用于存储用户数据的磁盘。**
  错误代码 6。首先，通过虚拟机管理控制台验证 PvD 磁盘是否连接到 VM。此错误通常是由于“数据泄漏预防”软件阻止访问 PvD 磁盘所致。如果 PvD 磁盘已连接到 VM，请尝试在“数据泄漏预防”软件配置中添加“已连接磁盘”例外。

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

- **系统在安装后尚未重新启动。请重新启动以使更改生效。**
  错误代码 7。请重新启动桌面并重新尝试操作。

- **安装已损坏。请尝试重新安装 Personal vDisk。**
  错误代码 8。请安装 Personal vDisk 并重试。

- **个人虚拟磁盘清单不是最新的。请更新主映像中的清单，然后重试。**
  错误代码 9。关闭桌面前，个人虚拟磁盘清单在主映像中未更新。请重新启动主映像，并通过“更新 Personal vDisk”选项关闭桌面，然后创建新快照，并使用此快照更新目录。

- **启动个人虚拟磁盘时遇到内部错误。请查看 Personal vDisk 日志，进一步了解详细信息。**
  错误代码 10。出现此问题是由于内部错误或个人虚拟磁盘损坏导致 PvD 驱动程序无法启动虚拟会话所致。请尝试通过 Controller 重新启动桌面。如果问题仍然存在，请收集日志并联系 Citrix 技术支持。

- **尝试查找用于实现用户个性化设置的存储磁盘时 Personal vDisk 超时。**
  错误代码 11。如果 PvD 驱动程序在启动后 30 秒内未找到 PvD 磁盘，将会出现此错误。此问题通常是由于不受支持的 SCSI 控制器类型或存储冗余所致。如果目录中的所有桌面均出现此问题，请将与“模板 VM”/“主 VM”关联的 SCSI 控制器类型更改为 Personal vDisk 技术支持的类型。如果此问题仅出现在目录中的部分桌面上，则可能是因为大量桌面在同一时间启动导致存储冗余出现峰值所致。请尝试限制与主机连接关联的活动电源操作设置最大值。

- **Personal vDisk 已取消激活，因为检测到不安全的系统关闭。请重新启动计算机。**
  错误代码 12。这可能是由于在启用 PvD 的情况下，桌面无法完成启动过程所致。请尝试重新启动桌面。如果问题仍然存在，请通过虚拟机管理控制台观察桌面启动情况，并检查桌面是否崩溃。如果桌面在启动过程中崩溃，请从备份还原 PvD（如有存在维护的备份）或重置 PvD。

- **为装载 Personal vDisk 而指定的驱动器盘符不可用。**
  错误代码 13。出现此问题是因为在管理员指定的时间 PvD 无法装载 PvD 磁盘。如果驱动器盘符已由其他硬件使用，PvD 磁盘将无法装载。请选择其他盘符作为个人虚拟磁盘的装载点。

- **无法安装 Personal vDisk 内核模式驱动程序。**
  错误代码 14。Personal vDisk 在安装后首次更新清单时安装驱动程序。如果从安装上下文以外尝试安装，有些防病毒产品会阻止驱动程序的安装。请在首次创建清单期间，临时禁止防病毒实时扫描，或在防病毒产品中将 PvD 驱动程序添加为例外。

- **无法创建系统卷的快照。请务必启用卷影复制服务。**
  错误代码 15。出现此错误可能是因为禁用了卷影复制服务。请启用卷影复制服务并尝试重新创建清单。

- **变更日志无法激活。Try again after waiting for few minutes.（无法激活更改日志。请一段时间后重试。）**
  错误代码 16。Personal vDisk 使用更改日志来跟踪对主映像所做的更改。在清单更新期间，如果 PvD 检测到更改日志被禁用，PvD 会尝试将其启用；此尝试失败时会出现此错误。请稍等一段时间，然后重试。

- **系统卷上的可用空间不足。**
  错误代码 17。桌面的 C 驱动器上没有足够的可用空间来进行映像更新操作。请扩展系统卷，或删除系统卷中不再使用的文件以释放空间。映像更新应该会在下一次重新启动时重新开始。

- **个人虚拟磁盘存储上的可用空间不足。请扩展个人虚拟磁盘存储以提供更多空间。**
  错误代码 18。执行映像更新操作时，个人虚拟磁盘驱动器上的可用空间不足。请扩展个人虚拟磁盘存储或删除个人虚拟磁盘存储中不再使用的文件以释放空间。映像更新操作应该会在下次重新启动时重新开始。

- **个人虚拟磁盘存储已超负荷。请扩展个人虚拟磁盘存储以提供更多空间。**
  错误代码 19。个人虚拟磁盘驱动器上的可用空间不足，无法完全适应密集置备的“UserData.V2.vhd”。请扩展个人虚拟磁盘

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

存储或删除个人虚拟磁盘存储中不再使用的文件以释放空间。

- **系统注册表已损坏。**
  错误代码 20。系统注册表损坏、缺失或不可读。重置个人虚拟磁盘或通过之前的备份还原。

- **重置个人虚拟磁盘时遇到内部错误。请查看 Personal vDisk 日志，进一步了解详细信息。**
  错误代码 21。这是对在个人虚拟磁盘重置期间遇到的所有错误的概括。请收集日志并联系 Citrix 技术支持。

- **由于个人虚拟磁盘存储中的可用空间不足，无法重置 Personal vDisk。**
  错误代码 22。执行重置操作时，个人虚拟磁盘驱动器上的可用空间不足。请扩展个人虚拟磁盘存储或删除个人虚拟磁盘存储中不再使用的文件以释放空间。

以下错误消息对 7.6 之前的 PvD 7.x 版本有效：

- **启动失败。Personal vDisk 找不到用于存储用户个性化设置的存储磁盘。**
  PvD 软件找不到个人虚拟磁盘（默认为驱动器 P:）或 无法装载个人虚拟磁盘作为管理员在创建目录时选择的 装载点。
  - 检查 PvD 服务日志中是否存在以下条目：PvD 1 status --> 18:183（PvD 1 状态 --> 18:183）。
  - 如果您使用的是 5.6.12 之前的 PvD 版本，则升级到最新版本可解决此问题。
  - 如果您使用的是 5.6.12 版或更高版本，请使用磁盘管理工具 (diskmgmt.msc) 确定驱动器 P: 是否作为不可装入卷存在。 如果存在，请在该卷上运行 chkdsk 以确定其是否已损坏，然后尝试使用 chkdsk 对其进行恢复。
- **启动失败。Citrix Personal vDisk 无法启动。如需更多帮助 .... 状态代码：7， 错误代码：0x70**
  状态代码 7 表示尝试更新 PvD 时遇到错误。 错误代码可以是以下代码之一：

错误代码：	说明
0x20000001	无法保存差异软件包，最可能的原因是 VHD 中可用磁盘空间不足。
0x20000004	无法获取更新 PvD 所需的权限。
0x20000006	无法从 PvD 映像或 PvD 清单加载配置单元，最可能的原因是 PvD 映像或清单已损坏。
0x20000007	无法加载文件系统清单，最可能的原因是 PvD 映像或清单已损坏。
0x20000009	无法打开包含文件系统清单的文件，最可能的原因是 PvD 映像或清单已损坏。
0x2000000B	无法保存差异软件包，最可能的原因是 VHD 中可用磁盘空间不足。
0x20000010	无法加载差异软件包。
0x20000011	规则文件丢失。
0x20000021	PvD 清单已损坏。
0x20000027	目录 MojoControl.dat 已损坏。

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

错误代码	说明
0x2000002B	PvD 清单已损坏或丢失。
0x2000002F	无法在映像更新时注册用户安装的 MOF，请升级到 5.6.12 以修复此问题。
0x20000032	检查 PvDactivation.log.txt 中是否存在错误代码为 Win32 的最后一个日志条目。
0x20	无法装载应用程序容器以进行映像更新，请升级到 5.6.12 以修复此问题。
0x70	磁盘空间不足。

- **启动失败。Citrix Personal vDisk 无法启动 [或 Personal vDisk 遇到内部 错误]。如需更多帮助 .... 状态代码: 20，错误代码 0x20000028**
  找到了个人 虚拟磁盘，但无法创建 PvD 会话。

  请收集 日志并在 SysVol-IvmSupervisor.log 中查找是否存在会话创建失败：
  1. 检查是否存在以下日志条目：IvmpNativeSessionCreate: failed to create native session, status XXXXX（IvmpNativeSessionCreate: 无法创建本机会话，状态为 XXXXX）。
  2. 如果状态为 0xc00002cf，请通过将新版本的主映像添加到目录来修复此问题。 此状态代码表示由于在更新清单后执行了大量更改，导致 USN 日志溢出。
  3. 重新启动受影响的虚拟桌面。 如果问题仍然存在，请联系 Citrix 技术支持。
- **启动失败。Citrix Personal vDisk 已取消激活，因为检测到不安全的系统 关闭。要重试，请选择“重试”。如果问题继续存在，请联系 系统管理员。**
  在启用 PvD 的情况下，池 VM 无法完成其启动过程。请首先确定 启动无法完成的原因。可能是因为由于以下 原因显示蓝屏：
  - 主映像中存在不兼容的防病毒产品，例如旧版 Trend Micro。
  - 用户安装了与 PvD 不兼容的软件。 这种可能性不大，但是您可以通过向目录中添加一个新计算机并观察它能否成功重新启动来进行检查。
  - PvD 映像已损坏。 在版本 5.6.5 中观察到此问题。

  要检查 池 VM 是否显示蓝屏或过早重新启动，请执行以下操作：
  - 通过虚拟机管理程序控制台登录计算机。
  - 单击 重试并等待计算机关闭。
  - 通过 Studio 启动计算机。
  - 使用虚拟机管理程序控制台在计算机启动过程中对其进行监视。

  其他 故障排除方法：
  - 从显示蓝屏的计算机中收集内存转储，然后将其发送给 Citrix 技术支持进行进一步分析。
  - 检查事件日志中是否存在与 PvD 关联的错误：
    1. 使用 DiskMgmt.msc 通过单击 “Action”（操作）>“Attach VHD”（附加 VHD）从驱动器 P: 的根目录中装载 UserData.V2.vhd。
    2. 启动 Eventvwr.msc。
    3. 通过 单击“Action”（操作）>“Open saved logs”（打开保存的日志）从 UserData.V2.vhd 中打开系统事件日志 (Windows\System32\winevt\logs\system.evtx)。
    4. 通过 单击“Action”（操作）>“Open saved logs”（打开保存的日志）从 UserData.V2.vhd 中打开应用程序事件日志 (Windows\System32\winevt\logs\application.evtx)。
- **Personal vDisk 无法 启动。由于清单未更新，Personal vDisk 无法 启动。请更新主映像中的清单，然后重试。状态代**

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

码： 15，错误代码：0x0
管理员在创建或更新 PvD 目录时选择了错误的快照（即，在创建快照时未使用 更新 Personal vDisk 关闭主映像）。

如果未启用 Personal vDisk，可在 Windows 事件查看器中查看以下事件。 请在左侧窗格中选择应用程序节点，右侧窗格中的事件来源为 Citrix Personal vDisk。 如果启用 Personal vDisk，将不显示任何事件。

事件 ID 1 代表信息性消息，ID 2 代表错误。 并非所有事件都能在所有版本的 Personal vDisk 中使用。

事件 ID	说明
1	Personal vDisk 状态: 已开始更新清单。
1	Personal vDisk 状态：已完成清单更新。GUID：%s。
1	Personal vDisk 状态: 已开始执行映像更新。
1	Personal vDisk 状态: 已完成映像更新。
1	正在重置。
1	OK（正常）。
2	Personal vDisk 状态: 更新清单失败，错误为: %s。
2	Personal vDisk 状态: 映像更新失败，错误为: %s。
2	Personal vDisk 状态: 出现内部错误，映像更新失败。
2	Personal vDisk 状态: 出现内部错误，更新清单失败。
2	由于非正常关机，Personal vDisk 已禁用。
2	映像更新失败。错误代码 %d。
2	Personal vDisk 出现内部错误。状态代码[%d] 错误代码[0x%X]。
2	Personal vDisk 重置失败。
2	找不到用于存储用户个性化设置的磁盘。

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

事件 ID	说明
2	存储磁盘上可用空间不足，无法创建 Personal vDisk 容器。

与版本无关的已知问题

确定了以下 PvD 问题：

- 如果安装在个人虚拟磁盘 (PvD) 上的某个应用程序与另一个安装在主映像上具有相同版本的应用程序相关，在映像更新后，PvD 上的应用程序可能会停止工作。如果卸载主映像上的应用程序或将其升级到更新的版本，则会出现此问题，因为此操作从主映像上删除了 PvD 上的应用程序所需的文件。为防止发生此问题，请在主映像上保留包含 PvD 上的应用程序所需文件的应用程序。

  例如，主映像包含 Office 2007，并且用户在 PvD 上安装了 Visio 2007，Office 应用程序和 Visio 运行正常。之后，管理员在主映像上将 Office 2007 替换成 Office 2010，然后使用更新后的映像更新所有受影响的计算机。Visio 2007 将不再可用。为避免此问题，请在主映像上保留 Office 2007。[#320915]

- 如果使用 Personal vDisk，当部署 McAfee Virus Scan Enterprise (VSE) 时，请在主映像上使用版本 8.8 Patch 4 或更高版本。[#303472]
- 如果所创建的关于主映像中某个文件的快捷方式不再起作用（因为快捷方式目标在 PvD 中重命名），请重新创建快捷方式。[#367602]
- 请勿在主映像中使用绝对/硬盘链接。[#368678]
- Personal vDisk 不支持 Windows 7 备份和还原功能。[#360582]
- 应用更新后的主映像后，本地用户和组控制台变得无法访问或显示不一致的数据。要解决此问题，请在 VM 上重置用户帐户，为此需要重置安全配置单元。此问题在 7.1.2 版本中得以修复（适用于在之后的版本中创建的 VM），但是此修复对使用更早的版本创建然后又进行升级的 VM 不起作用。[#488044]
- 在 ESX 虚拟机管理程序环境中使用池 VM 时，如果选择的 SCSI 控制器类型为“VMware Paravirtual”，系统会向用户显示重新启动提示。要解决此问题，请使用 LSI SCSI 控制器类型。[#394039]
- 在通过 Provisioning Services 创建的桌面上重置 PvD 后，用户登录到 VM 后可能会收到重新启动提示。解决方法：重新启动桌面。[#340186]
- Windows 8.1 桌面用户可能无法登录其 PvD。管理员可能会看到消息“PvD was disabled due to unsafe shutdown”（由于不安全的关闭操作导致禁用 PvD），并且 PvDActivation 日志可能会包含消息“Failed to load reg hive [\Device\IvmVhdDisk00000001\CitrixPvD\Settings\RingCube.dat]”（无法加载 reg 配置单元 [\Device\IvmVhdDisk00000001\CitrixPvD\Settings\RingCube.dat]）。当用户的 VM 以不安全的方式关闭时，会出现此问题。解决方法：重置 Personal vDisk。[#474071]

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

删除组件

Dec 05, 2017

要删除组件，Citrix 建议使用专门用于删除或更改程序的 Windows 功能。也可以使用命令行或安装介质中的脚本删除组件。

删除组件时，不会删除必备项，也不会更改防火墙设置。删除 Controller 时，不会删除 SQL Server 软件和数据库。

删除 Controller 之前，请先将其从站点中删除。删除 Studio 或 Director之前，Citrix 建议先将其关闭。

如果从包含 Web Interface 的早期部署升级了 Controller，必须单独删除 Web Interface 组件；不能使用安装程序删除 Web Interface。

删除 VDA 时，默认情况下，计算机将在删除后自动重新启动。

使用专门用于删除或更改程序的 Windows 功能删除组件

使用专门用于删除或更改程序的 Windows 功能：

- 要删除 Controller、Studio、Director、许可证服务器或 StoreFront，请选择 Citrix XenApp <*版本*> 或 Citrix XenDesktop <*版本*>，然后单击鼠标右键并选择**卸载**。此时将启动安装程序，从中可选择要删除的组件。也可以通过在 **Citrix StoreFront** 上单击鼠标右键并选择**卸载**来删除 StoreFront。
- 要删除 VDA，请选择 **Citrix Virtual Delivery Agent** <*版本*>，然后单击鼠标右键并选择**卸载**。此时将启动安装程序，从中可选择要删除的组件。
- 要删除通用打印服务器，请选择 **Citrix 通用打印服务器**，然后单击鼠标右键并选择**卸载**。

使用命令行删除核心组件

从安装介质上的 \x64\XenDesktop Setup 目录中，运行 **XenDesktopServerSetup.exe** 命令。

- 要删除一个或多个组件，请使用 /remove 和 /components 选项。
- 要删除所有组件，请使用 /removeall 选项。

有关命令和参数的详细信息，请参阅使用命令行安装。

例如，以下命令可删除 Studio。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components studio
```

使用命令行删除 VDA

从安装介质上的 \x64\XenDesktop Setup 目录中，运行 **XenDesktopVdaSetup.exe** 命令。

- 要删除一个或多个组件，请使用 /remove 和 /components 选项。
- 要删除所有组件，请使用 /removeall 选项。

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

有关命令和参数的详细信息，请参阅使用命令行安装。

例如，以下命令可删除 VDA 和 Citrix Receiver。

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /removeall
```

要使用 Active Directory 中的脚本删除 VDA，请参阅使用脚本安装或删除 Virtual Delivery Agent。

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

升级和迁移

Dec 05, 2017

升级

通过升级可以将部署更改为最新的组件版本，而无需设置新的计算机或站点，这称为原位升级。可以从以下版本升级到当前版本：

- XenDesktop 5.6 *
- XenDesktop 7.0
- XenDesktop 7.1
- XenApp/XenDesktop 7.5
- XenApp/XenDesktop 7.6
- XenApp/XenDesktop 7.6 LTSR
- XenApp/XenDesktop 7.7
- XenApp/XenDesktop 7.8
- XenApp/XenDesktop 7.9
- XenApp/XenDesktop 7.11
- XenApp/XenDesktop 7.12
- XenApp/XenDesktop 7.13
- XenApp/XenDesktop 7.14
- XenApp/XenDesktop 7.15 LTSR

也可以将 XenApp 6.5 工作服务器升级到 VDA for Windows Server OS 的当前版本。这是迁移到 XenApp 6.5 的补充活动。请参阅将 XenApp 6.5 工作进程升级至新的 VDA for Windows Server OS

执行升级：

1. 在安装核心组件和 VDA 的计算机上运行安装程序。软件会确定是否有可用的升级并安装更新的版本。
2. 使用新升级的 Studio 来升级数据库和站点。

* 要从 XenDesktop 5.6 进行升级，请先升级到 7.6 LTSR（包含最新的 CU），然后再升级到 7.15 LTSR（包含最新的 CU）。

有关详细信息，请参阅升级部署。

有关安装 Controller 修补程序的信息，请参阅 CTX201988。

迁移

将数据从早期部署迁移到最新版本。可以迁移 XenApp 6 部署。迁移包括安装当前组件和创建新站点，从旧场导出数据，然后将数据导入到新站点。

提示：有关在 7.x 版本中引入的体系结构、组件和功能更改的信息，请参阅 7.x 中的变更一文。

要从 XenApp 6.5 进行迁移，请执行以下操作：

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

1. 安装核心组件并创建新的 XenApp 站点。
2. 从 XenApp 6.5 控制器，使用 PowerShell cmdlet 将策略和/或场数据导出到 XML 文件中。您可以编辑 XML 文件的内容以定制要导入的信息。
3. 从新站点，使用 PowerShell cmdlet 和 XML 文件将策略和/或应用程序数据导入到新站点。
4. 在新站点上完成迁移后需执行的任务。

有关详细信息，请参阅迁移 XenApp 6.x。

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

7.x 中的变更

Jan 03, 2018

XenApp 和 XenDesktop 体系结构、术语和功能从 7.x 版本开始已更改。如果您仅熟悉早期（7.x 之前）版本，本文可以帮助您熟悉这些更改。

提示：移至 7.x 版本后，新增功能中将列出对更高版本所做的变更。

除非明确说明，否则 *7.x* 是指 XenApp 7.5 版或更高版本，以及 XenDesktop 7 版或更高版本。

本文提供概述。有关从 7.x 之前版本移至最新版本的综合信息，请参阅升级到 XenApp 7。

XenApp 6 与当前 XenApp 版本之间的元素区别

尽管并不完全相同，但下表可帮助您将 XenApp 6.5 和早期版本中的功能元素与 XenApp 和 XenDesktop 7.x 及更高版本中的功能元素对应起来。后面提供了体系结构区别的说明。

XenApp ≤ 6.5 中被代替的元素：	XenApp 和 XenDesktop ≥ 7.x 中使用的元素：
Independent Management Architecture (IMA)	FlexCast Management Architecture (FMA)
场	站点
工作组	计算机目录 交付组
工作进程	Virtual Delivery Agent (VDA) 服务器操作系统计算机，服务器操作系统 VDA 桌面操作系统计算机，桌面操作系统 VDA
远程桌面服务 (RDS) 或终端服务计算机	服务器操作系统计算机，服务器操作系统 VDA
区域和数据收集器	Delivery Controller
交付服务控制台	Citrix Studio 和 Citrix Director
发布应用程序	交付应用程序
数据存储	数据库

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

负载评估程序	负载管理策略
管理员	委派的管理员 角色 范围

体系结构区别

从 7.x 版本开始，XenApp 和 XenDesktop 基于 FlexCast Management Architecture (FMA)。FMA 是面向服务的体系结构，可以实现跨 Citrix 各种技术的互操作性和模块化管理。FMA 为应用程序交付、移动性、服务、灵活置备和云管理提供了一个统一的平台。

FMA 取代了 XenApp 6.5 和早期版本中使用的 Independent Management Architecture (IMA)。

在考虑与 XenApp 6.5 和早期版本中的元素的关系时，以下是 FMA 中的关键元素：

- **交付站点**：场是 XenApp 6.5 和早期版本中的顶层对象。在 XenApp 7.x 和 XenDesktop 7.x 中，站点则是级别最高的项目。站点为用户组提供应用程序和桌面。FMA 要求您必须位于域中才能部署站点。例如，要安装服务器，您的帐户必须具有本地管理员权限并且是 Active Directory 中的域用户。
- **计算机目录和交付组**：XenApp 6.5 和早期版本中托管应用程序的计算机属于工作组，目的是便于有效地管理应用程序和服务器软件。管理员可以将一个工作组中的所有计算机作为一个单元进行管理，以满足其应用程序管理和负载平衡需求。使用文件夹来组织应用程序和计算机。在 XenApp 7.x 和 XenDesktop 7.x 中，结合使用计算机目录、交付组和应用程序组来管理计算机、负载平衡和托管应用程序或桌面。还可以使用应用程序文件夹。
- **VDA**：在 XenApp 6.5 和早期版本中，工作组中的工作计算机运行用户的应用程序并与数据收集器通信。在 XenApp 7.x 和 XenDesktop 7.x 中，则是 VDA 与管理用户连接的 Delivery Controller 通信。
- **Delivery Controller**：在 XenApp 6.5 和早期版本中，区域主服务器负责处理用户连接请求以及与虚拟机管理程序的通信。在 XenApp 7.x 和 XenDesktop 7.x 中，站点中的 Controller 负责分发和处理连接请求。在 XenApp 6.5 和早期版本中，区域提供了一种跨 WAN 连接聚合服务器和重复数据的方式。虽然区域在 XenApp 7.x 和 XenDesktop 7.x 中没有准确的等效功能，但是 7.x 区域和区域首选项功能仍允许您帮助远程地理区域的用户连接到资源，而不需要强制其连接遍历大部分 WAN。
- **Studio 和 Director**：使用 Studio 控制台配置环境并为用户提供访问应用程序和桌面的权限。Studio 取代了 XenApp 6.5 和早期版本中的交付服务控制台。管理员使用 Director 监视环境、重影用户设备和对 IT 问题进行故障排除。要重影用户，必须启用 Windows 远程协助；安装 VDA 时默认启用此功能。
- **交付应用程序**：XenApp 6.5 和早期版本使用“发布应用程序”向导来准备应用程序并将其交付给用户。在 XenApp 7.x 和 XenDesktop 7.x 中，使用 Studio 创建和添加应用程序，使其可供交付组和（可选）应用程序组中的用户使用。使用 Studio 时，首先配置站点，创建并指定计算机目录，然后创建使用这些目录中的计算机的交付组。交付组确定哪些用户可以访问您交付的应用程序。（可选）可以选择创建应用程序组来替代多个交付组。
- **数据库**：XenApp 7.x 和 XenDesktop 7.x 不使用 IMA 数据存储来存储配置信息，而是使用 Microsoft SQL Server 数据库来存储配置和会话信息。
- **负载管理策略**：在 XenApp 6.5 和早期版本中，负载评估程序使用预定义的衡量指标来确定计算机上的负载。用户连接可以匹配到负载较低的计算机。在 XenApp 7.x 和 XenDesktop 7.x 中，则使用负载管理策略跨多台计算机平衡负载。

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

- **委派管理**：在 XenApp 6.5 和早期版本中，创建自定义管理员并根据文件夹和对象为其分配权限。在 XenApp 7.x 和 XenDesktop 7.x 中，则基于角色和作用域对来创建自定义管理员。角色表示一种作业职能，并且具有定义的关联权限以允许委派。作用域表示对象集合。内置管理员角色具有特定的权限集，如技术支持、应用程序、托管和目录。例如，技术支持管理员只能与指定站点上的各个用户协作，而完全权限管理员可以监视整个部署并解决整个系统范围的 IT 问题。

功能比较

过渡到 FMA 意味着在 XenApp 6.5 和早期版本中提供的一些功能可能会采用其他方式实现，或者可能需要替换其他功能、组件或工具才能实现相同的目的。

XenApp 6.5 和更早版本中被代替的元素：	XenApp 和 XenDesktop 7.x 及更高版本中使用的元素：
使用策略设置配置会话预启动和会话延迟	通过编辑交付组设置配置会话预启动和会话延迟。 与 XenApp 6.5 中相同，这些功能通过以下方式帮助用户快速连接到应用程序：在用户请求会话之前启动会话（会话预启动），并在用户关闭所有应用程序之后使会话保持活动状态（会话延迟）。在 XenApp 和 XenDesktop 7.x 中，通过为现有交付组配置这些设置为指定用户启用这些功能。请参阅配置会话预启动和会话延迟。
通过在设置已发布应用程序的属性时向匿名用户授予权限来提供对未经身份验证（匿名）用户的支持	通过在设置交付组的用户属性时配置此选项来提供对未经身份验证（匿名）用户的支持。请参阅用户。
即使在与数据存储的连接不可用时，本地主机缓存仍允许工作服务器正常运行	本地主机缓存允许在 Controller 与站点数据库之间的连接失败时连接代理操作继续执行。此实施更强大，且需要的维护更少。请参阅“本地主机缓存”。 作为替代使用本地主机缓存的方法，连接租用使用户可以连接和重新连接到他们最后使用的应用程序和桌面，即使站点数据库不可用也是如此。请参阅连接租用。
应用程序流技术推送	Citrix App-V 提供流应用程序，这些应用程序是通过使用 Studio 进行管理。
Web Interface	Citrix 建议过渡到 StoreFront。
使用 SmartAuditor 记录用户会话的屏幕活动。	自 7.6 Feature Pack 1 起，此功能由 Session Recording 提供。还可以使用配置日志记录从管理角度记录所有会话活动。
使用电源和容量管理功能帮助降低电源消耗和管理服务器容量。	使用 Microsoft Configuration Manager。

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

功能支持和更改

XenApp 或 XenDesktop 7.x 及更高版本当前不提供、不再支持或已显著更改以下功能。

低于 128 位的安全 ICA 加密：在 7.x 之前的版本中，可以使用安全 ICA 加密客户端连接，以实现基本加密、40 位、56 位和 128 位加密。在 7.x 版本中，安全 ICA 加密仅适用于 128 位加密。

旧版打印：7.x 版本不支持以下打印功能：

- DOS 客户端和 16 位打印机的向后兼容性。
- 支持连接到 Windows 95 和 Windows NT 操作系统的打印机，包括增强型扩展打印机属性和 Win32FavorRetainedSetting。
- 启用或禁用自动保留和自动恢复的打印机的功能。
- DefaultPrnFlag。这是服务器上用于启用或禁用自动保留和自动恢复的打印机的一项注册表设置，存储在服务器上的用户配置文件中。

注意：支持旧版客户端打印机名称。

Secure Gateway：在 7.x 之前的版本中，Secure Gateway 是用于在服务器和用户设备之间提供安全连接的选项。NetScaler Gateway 是用于确保外部连接安全的替代选项。

重影用户：在 7.x 之前的版本中，管理员通过设置策略来控制用户对用户重影操作。在 7.x 版本中，重影最终用户是 Director 组件的一项集成功能，该功能使用 Microsoft 远程协助来允许管理员重影和解决与已交付的无缝应用程序和虚拟桌面有关的问题。

Flash v1 重定向：不支持第二代 Flash 重定向的客户端（包括 3.0 之前的 Citrix Receiver for Windows 版本、11.100 之前的 Citrix Receiver for Linux 版本以及 Citrix 联机插件 12.1）将回退到服务器端呈现，以实现旧版 Flash 重定向功能。7.x 版本中包括的 VDA 支持第二代 Flash 重定向功能。

本地文本回显：此功能与早期的 Windows 应用程序技术结合使用，用于在高延迟连接中，在用户设备上加速显示输入文本。由于图形子系统和 HDX SuperCodec 的功能得以增强，因此 7.x 版本中不提供此功能。

单点登录：此功能可以确保密码安全，但在 Windows 8、Windows Server 2012 和支持的更高 Windows 操作系统版本中不受支持。在 Windows 2008 R2 和 Windows 7 环境中仍支持此功能，但 7.x 版本不包括此功能。可以在 Citrix 下载 Web 站点找到此功能：http://citrix.com/downloads。

Oracle 数据库支持：7.x 版本要求使用 SQL Server 数据库。

运行状况监视与恢复 (HMR)：在 7.x 之前的版本中，HMR 可以在服务器场中的服务器上运行测试，以监视它们的状态并发现任何运行状况风险。在 7.x 版本中，Director 从 Director 控制台监视整个基础结构并提供警报，从而提供了一种从中央位置查看系统运行状况的方式。

自定义 ICA 文件：自定义 ICA 文件用于实现从用户设备（通过 ICA 文件）直接连接到特定计算机。在 7.x 版本中，此功能默认处于禁用状态。但在正常情况下，可以通过本地组将其启用。在 Controller 不可用时，还可以在高可用性模式中使用该功能。

Management Pack for System Center Operations Manager (SCOM) 2007：该管理包之前使用 SCOM 监视 XenApp 场的活动，但不支持 7.x 版本。请参阅当前的 Citrix SCOM Management Pack for XenApp and XenDesktop。

CNAME 功能：在 7.x 之前的版本中，默认启用 CNAME 功能。如果部署依赖于 CNAME 记录进行 FQDN 重新路由并且使用

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

NETBIOS 名称，则可能会失败。在 7.x 版本中，Delivery Controller 自动更新功能可以动态更新 Controller 的列表，并且还可以在向站点添加 Controller 或从站点删除 Controller 时自动向 VDA 发送通知。Controller 自动更新功能在 Citrix 策略中默认处于启用状态，但可以禁用。或者，也可以在注册表中重新启用 CNAME 功能，以继续使用现有部署并允许 FQDN 重新路由和使用 NETBIOS 名称。有关详细信息，请参阅 CTX137960。

快速部署向导：在 7.x 之前的 XenDesktop 版本中，利用此 Studio 选项可以对完整安装的 XenDesktop 部署进行快速部署。7.x 版本中提供简化的全新安装和配置工作流程，不需要再使用"快速部署"向导选项。

用于实现自动管理的 Remote PC Service 配置文件和 PowerShell 脚本：Remote PC Access 现在已集成到 Studio 和 Controller 中。

Workflow Studio：在 7.x 之前的版本中，Workflow Studio 是用于 XenDesktop 的工作流组合的图形界面。7.x 版本不支持此功能。

在客户端连接期间启动非发布程序：在 7.x 之前的版本中，此 Citrix 策略设置指定是否在服务器上通过 ICA 或 RDP 启动初始应用程序或已发布的应用程序。在 7.x 版本中，此设置仅指定是否在服务器上通过 RDP 启动初始应用程序或已发布的应用程序。

桌面启动：在 7.x 之前的版本中，此 Citrix 策略设置指定非管理员用户是否可以连接到桌面会话。在 7.x 版本中，非管理员用户必须属于 VDA 计算机的直接访问用户组才能连接到此 VDA 上的会话。桌面启用设置使 VDA 直接访问用户组的非管理员用户可以使用 ICA 连接连接到 VDA。桌面启动设置不影响 RDP 连接；无论是否启用此设置，VDA 直接访问用户组的用户都可以使用 RDP 连接与 VDA 建立连接。

颜色深度：在 7.6 之前的 Studio 版本中，在交付组的用户设置中指定颜色深度。自版本 7.6 起，可以使用 New-BrokerDesktopGroup 或 Set-BrokerDesktopGroup PowerShell cmdlet 设置交付组的颜色深度。

启动经过触控优化的桌面：此设置已禁用，不可用于 Windows 10 和 Windows Server 2016 计算机。有关详细信息，请参阅 移动体验策略设置。

COM 端口映射：COM 端口映射允许或阻止访问用户设备上的 COM 端口。在之前版本中，COM 端口映射默认处于启用状态。在 XenDesktop 和 XenApp 的 7.x 版本中，COM 端口映射默认处于禁用状态。有关详细信息，请参阅使用注册表配置 COM 端口和 LPT 端口重定向设置。

LPT 端口映射：LPT 端口映射控制旧版应用程序对 LPT 端口的访问。在之前版本中，LPT 端口映射默认处于启用状态。在 7.x 版本中，LPT 端口映射默认处于禁用状态。

PCM 音频编解码器：在 7.x 版本中，只有 HTML5 客户端支持 PCM 音频编解码器。

支持 Microsoft ActiveSync。

针对旧版本的代理支持：这包括：

- Microsoft Internet Security and Acceleration (ISA) 2006 (Windows Server 2003)
- Oracle iPlanet Proxy Server 4.0.14 (Windows Server 2003)
- Squid Proxy Server 3.1.14 (Ubuntu Linux Server 11.10)

有关详细信息，请参阅适用于您所用版本的 Citrix Receiver 文档。

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

升级部署

Feb 22, 2018

在本文中：

- 简介
- 升级顺序
- 可以升级的产品组件版本
- 准备和限制
- 混合环境注意事项
- 运行 Windows XP 或 Windows Vista 的计算机上的 VDA
- 运行 Windows 8.x 或 Windows 7 的计算机上的 VDA
- 混合 VDA 支持
- 升级过程
- 升级数据库和站点

简介

您可以将某些部署升级为更高版本，而无需事先设置新计算机或站点。该过程称为原位升级。请参阅升级了解可以升级的版本列表。

还可以使用当前的 XenApp 安装程序将 XenApp 6.5 工作服务器升级到当前的 VDA for Windows Server OS。这是迁移到 XenApp 6.5 的补充活动。请参阅将 XenApp 6.5 工作进程升级至新的 VDA for Windows Server OS。

要启动升级，请运行新版本的安装程序，以升级以前安装的核心组件（Delivery Controller、Citrix Studio、Citrix Director、Citrix 许可证服务器）和 VDA。然后升级数据库和站点。

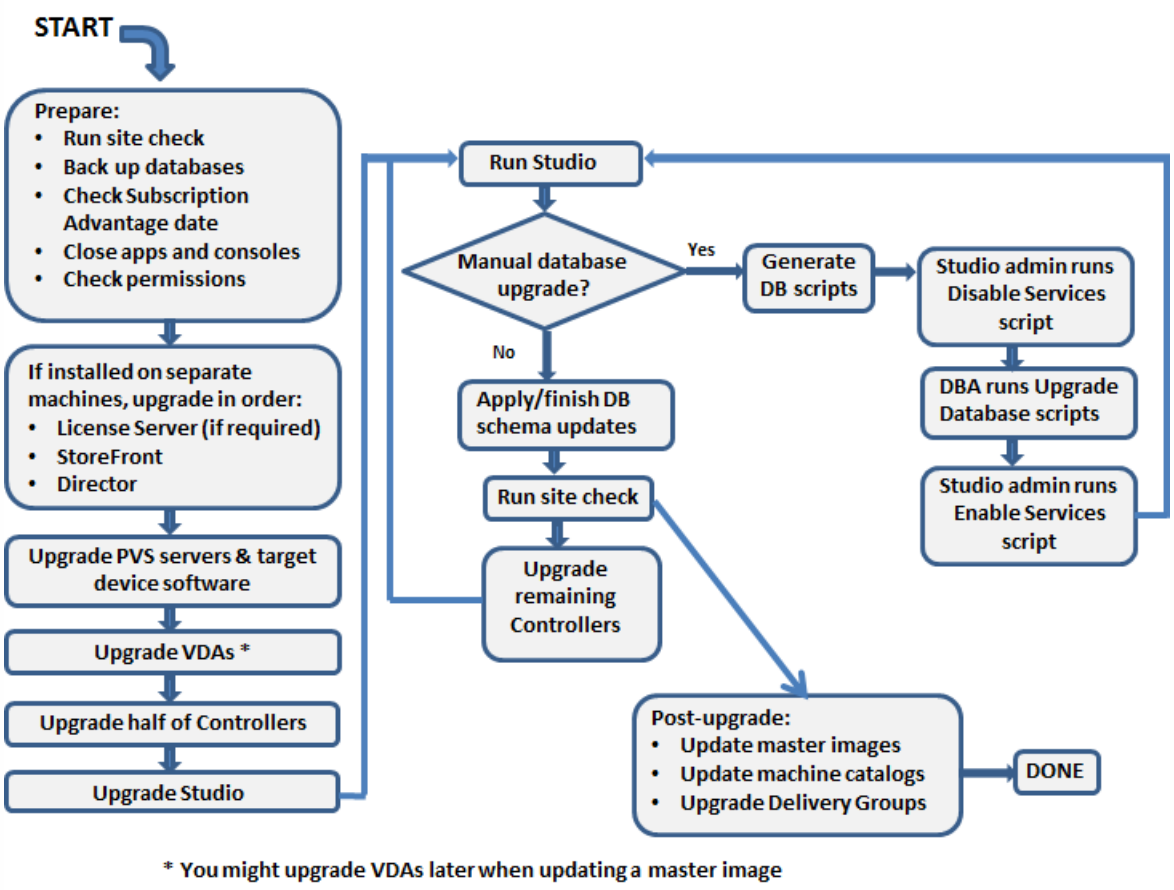
请务必在开始升级之前检查本文中的所有信息。

（如果要升级到 7.16 或更高版本，请参阅升级部署中的指南。）

升级顺序

下图概要介绍了升级顺序。下面的升级过程中提供了详细信息。例如，如果您在一台服务器上安装了多个核心组件，则在该计算机上运行安装程序将升级具有新版本的所有组件。您可能希望升级主映像中使用的 VDA，再更新该映像。然后，更新使用该映像的目录以及使用该目录的交付组。详细信息中还包括如何自动或手动升级站点数据库和站点。

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



可以升级的产品组件版本

使用产品安装程序，可以升级：

- Citrix 许可证服务器、Studio 和 StoreFront
- Delivery Controllers 5.6 或更高版本。
- VDA 5.6 或更高版本
  - 与早期 VDA 版本不同，必须使用产品安装程序来升级 VDA；不能使用 MSI。
  - 如果安装程序在计算机上检测到 Receiver for Windows (Receiver.exe)，则会将其升级到产品安装介质上包含的 Receiver 版本。
  - VDA 5.6 到 VDA 7.8：如果安装程序在计算机上检测到 Receiver for Windows Enterprise (CitrixReceiverEnterprise.exe)，会将其升级到 Receiver for Windows Enterprise 3.4。
- Director 1 或更高版本
- 数据库：此 Studio 操作将升级架构并迁移站点数据库的数据（以及配置日志记录和监视数据库，前提是从早期 7.x 版本进行升级）
- Personal vDisk

注意：要从 XenDesktop 5.6 进行升级，请先升级到 7.6 LTSR（包含最新的 CU），然后再升级到此版本。

如果需要，可以按照功能/产品文档中的说明升级以下组件：

- Provisioning Services（对于 XenApp 7.x 和 XenDesktop 7.x，Citrix 建议使用最新发布版本；支持的最低版本是 Provisioning

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

Services 7.0）。
  - 使用服务器滚动升级来升级 Provisioning Services 服务器，并使用虚拟磁盘版本化升级客户端。
  - Provisioning Services 7.x 不支持创建运行 XenDesktop 5 的新桌面。因此，虽然现有桌面仍可继续使用，但在升级 XenDesktop 之前，不能使用 Provisioning Services 7.x 来创建新桌面。如果规划一个装有 XenDesktop 5.6 和 7.x 站点的混合环境，不要将 Provisioning Services 升级到版本 7。
- 主机虚拟机管理程序版本。
- StoreFront。
- Profile Management。

限制

升级存在以下限制：

选择性组件安装

如果在安装任何组件或将任何组件升级到新版本时不升级不同计算机上其他需要升级的组件，Studio 将会提醒您。例如，假设一个升级包括新版本的 Controller 和 Studio。您升级 Controller，但您未在安装了 Studio 的计算机上运行安装程序。在您升级 Studio 之前，Studio.不允许您继续管理站点。

您不必升级 VDA，但 Citrix 建议升级所有 VDA 以使您能够使用所有可用功能。

低于 7.5 的 XenApp 版本

不能从低于 7.5 的 XenApp 版本升级。可以从 XenApp 6.x 迁移；请参阅迁移 XenApp 6.x。

尽管不能升级 XenApp 6.5 场，但可以将 Windows Server 2008 R2 计算机上的 XenApp 6.5 软件替换为当前 VDA for Server OS。请参阅将 XenApp 6.5 工作进程升级至新 VDA。

低于 5.6 的 XenDesktop 版本

不能从低于 5.6 的 XenDesktop 版本升级。

XenDesktop Express 版

不能升级 XenDesktop Express Edition。获取并安装当前支持版本的许可证，然后对其进行升级。

早期版本或技术预览版本

不能从 XenApp 或 XenDesktop 早期版本或技术预览版本升级。

Windows XP/Vista

如果在 Windows XP 或 Windows Vista 计算机上安装了 VDA，请参阅运行 Windows XP 或 Windows Vista 的计算机上的 VDA。

产品选择

从早期 7.x 版本升级时，无需选择或指定在初始安装过程中设置的产品（XenApp 或 XenDesktop）。

混合环境/站点

如果必须继续运行早期版本的站点和当前版本的站点，请参阅混合环境注意事项。

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

准备

开始升级之前：

决定要使用哪个安装程序和界面/接口

使用 XenApp 或 XenDesktop ISO 中的完整产品安装程序来升级核心组件。可以使用完整产品安装程序或其中一个独立的 VDA 安装程序来升级 VDA。所有的安装程序都提供图形界面和命令行接口。有关详细信息，请参阅安装程序。

不能通过从可以升级的版本导入或迁移数据来升级。（注意：对于一些比较低的版本，必须迁移，而不是升级；请参阅升级和迁移查看可以升级的版本列表。）

如果您最初是使用 VDAWorkstationCoreSetup.exe 安装程序安装桌面 VDA，Citrix 建议使用该安装程序对其升级。如果使用完整产品 VDA 安装程序或 VDAWorkstationSetup.exe 安装程序升级 VDA，可能会安装最初排除的组件，除非在升级中明确忽略/排除它们。

例如，如果您以前使用 VDAWorkstationCoreSetup.exe 安装了 7.13 版 VDA，之后使用完整产品安装程序将该 VDA 升级到 7.14 版，如果您接受默认设置或不使用 /exclude 命令行选项，则升级期间可能会安装在原始安装中排除的组件（如 Profile Management 或 Personal vDisk）。

检查站点的运行状况

在开始升级之前，请确保站点处于稳定的正常工作状态。如果站点存在问题，升级过程不会解决问题，并可能让站点处于难于恢复的复杂状态。要测试站点，请在 Studio 导航窗格中选择**站点**条目。在中间窗格的“站点配置”部分中，单击**测试站点**。

备份站点、监视和配置日志记录数据库

按照 CTX135207 中的说明进行操作。如果在升级后发现任何问题，可以还原备份。

（可选）备份模板并升级虚拟机管理程序（如果需要）。

完成您的业务连续性计划规定的任何其他准备任务。

确保您的 Citrix Licensing 是最新的

在升级之前，请确保您的客户成功服务/软件维护/专享升级服务日期对新产品版本有效。如果要从早期的 7.x 产品版本进行升级，日期必须至少为 2017.0801。（此日期适用于 7.15 LTSR 版本，不适用于之后发布的累积更新 (CU)。）

关闭应用程序和控制台

在开始升级之前，请关闭可能会导致文件锁定的所有程序，其中包括管理控制台和 PowerShell 会话。（重新启动计算机可确保清除任何文件锁定，以及不存在任何挂起的 Windows 更新。）

重要：开始升级之前，请停止并禁用所有第三方监视代理服务。

确保您有合适的权限

除了是域用户以外，您还必须是要升级产品组件的计算机上的本地管理员。

可以自动或手动升级网站数据库和网站。对于自动数据库升级，Studio 用户的权限必须能够更新 SQL Server 数据库架构（例如 db_securityadmin 或 db_owner 数据库角色）。有关详细信息，请参阅数据库一文。如果 Studio 用户没有这些权

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

限，则启动手动数据库升级将会生成脚本。Studio 用户可以从 Studio 运行某些脚本；数据库管理员可以使用 SQL Server Management Studio 等工具运行其他脚本。

混合环境注意事项

如果您的环境中包含的站点/场安装了不同的产品版本（混合环境），Citrix 建议使用 StoreFront 来汇总不同产品版本中的应用程序和桌面（例如，如果您有 XenDesktop 7.13 站点和 XenDesktop 7.14 站点）。有关详细信息，请参阅 StoreFront 文档。

- 在混合环境中，继续使用与每个发行版对应的 Studio 和 Director 版本，但要确保不同版本安装在单独的计算机上。
- 如果计划同时运行 XenDesktop 5.6 和 7.x 站点并同时为二者使用 Provisioning Services，无论是部署用于 7.x 站点的新 Provisioning Services，还是升级当前的 Provisioning Services，均无法在 XenDesktop 5.6 站点中置备新的工作负载。

在每个站点内，Citrix 建议升级所有组件。尽管某些组件的早期版本仍可使用，但最新版本中的所有功能可能无法使用。例如，尽管可以在含有早前版本 Controller 的部署中使用当前 VDA，但当前版本中的新增功能可能无法使用。使用非当前版本时，也可能会出现 VDA 注册问题。

- 具有 5.x 版本的 Controller 和 7.x 版本的 VDA 的站点将暂时保留在当前状态。理想情况下，应该尽快完成所有组件的升级。
- 请仅在准备好使用新版本时再升级独立 Studio 版本。

运行 Windows XP 或 Windows Vista 的计算机上的 VDA

不能将安装在运行 Windows XP 或 Windows Vista 的计算机上的 VDA 升级到 7.x 版本。必须使用安装了特定修补程序的 VDA 5.6 FP1；有关说明，请参阅 CTX140941。虽然早期版本 VDA 将在 7.x 的很多站点中运行，但它们无法使用其中的许多功能，包括：

- Studio 中需要更新 VDA 版本的功能。
- 从 Studio 配置 App-V 应用程序。
- 从 Studio 配置 StoreFront 地址。
- 使用 Machine Creation Services 时自动支持 Microsoft Windows KMS 许可。请参阅 CTX128580。
- Director 中的信息：
  - “控制板”、“趋势”和“用户详细信息”视图中影响登录持续时间的登录时间和登录结束事件。
  - HDX 连接和身份验证时间的登录时长细分详细信息，以及配置文件加载、GPO 加载、登录脚本和交互式会话建立的持续时间详细信息。
  - 多个类别的计算机和连接故障率。
  - “技术支持人员”和“用户详细信息”视图中的活动管理器。

Citrix 建议先对 Windows XP 和 Windows Vista 计算机重新建立到受支持操作系统版本的映像，然后再安装最新 VDA。

运行 Windows 8.x 或 Windows 7 的计算机上的 VDA

要将已安装 VDA 的 Windows 8.x 或 Window 7 计算机升级到 Windows 10，Citrix 建议先对 Windows 7 和 Windows 8.x 计算机重新建立到 Windows 10 的映像，然后再安装适用于 Windows 10 的 VDA。如果无法重置映像，请先卸载 VDA，然后再升级操作系统；否则，VDA 将处于不受支持的状态。

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

混合 VDA 支持

将产品升级到更高版本时，Citrix 建议升级所有核心组件和 VDA，以便访问您版本中的所有新功能和增强功能。

在某些环境中，可能无法将所有 VDA 升级到最新版本。在这种情况下，如果创建计算机目录，可以指定计算机上安装的 VDA 版本。默认情况下，此设置指定建议的最新 VDA 版本；只有在计算机目录包含装有早期 VDA 版本的计算机时才需要考虑更改此设置。但是，不建议在计算机目录中混合使用多个 VDA 版本。

如果计算机目录是使用建议的默认 VDA 版本设置创建的，并且此目录中的任何计算机都安装了早期 VDA 版本，则这些计算机将无法在 Controller 中注册并且将无法使用。

有关详细信息，请参阅 VDA 版本和功能级别。

升级过程

要运行产品安装程序图形界面，请登录到计算机，然后插入介质或装载新版本的 ISO 驱动器。双击 **AutoSelect**。要使用命令行接口，请参阅使用命令行安装。

步骤 1. 如果多个核心组件安装在同一服务器上（例如 Controller、Studio 和许可证服务器），并且其中的多个组件有新版本可供使用，则在该服务器上运行安装程序时，这些组件将全部进行升级。

如果任何核心组件安装在 Controller 以外的计算机上，请在其中的每台计算机上运行安装程序。建议顺序：许可证服务器、StoreFront 及 Director。

步骤 2. 如果使用 Provisioning Services，请按照 Provisioning Services 文档中的指导，升级 PVS 服务器和目标设备。

步骤 3. 在包含 VDA 的计算机上运行产品安装程序。（如果使用主映像和 Machine Creation Services，请参阅步骤 12。）

步骤 4. 在一半的 Controller 上运行产品安装程序。（这还会升级安装在这些服务器上的其他任何核心组件。）例如，如果您的站点包含四个 Controller，应在其中两个 Controller 上运行安装程序。

- 使另一半的 Controller 处于活动状态，以便用户能访问此站点。VDA 可以在其余 Controller 中进行注册。有时，站点容量可能会因可用 Controller 的减少而减少。升级仅导致在最终数据库升级步骤期间建立新的客户端连接时出现短暂的中断。直到整个站点都完成升级后，升级后的 Controller 才能处理请求。
- 如果站点中只有一个 Controller，则升级期间站点无法正常运行。

步骤 5. 如果安装 Studio 的计算机不是已升级的计算机，则在安装 Studio 的计算机上运行安装程序。

步骤 6. 从新升级的 Studio 升级站点数据库。有关详细信息，请参阅升级数据库和站点。

步骤 7. 从新升级的 Studio 的导航窗格中选择 **Citrix Studio** *站点名称*。选择**常规任务**选项卡。选择**升级其余的 Delivery Controller**。

步骤 8. 在其余的 Controller 上完成升级并确认完成之后，关闭 Studio，然后再重新打开。Studio 可能会提示额外进行一次站点升级，以在站点中注册 Controller 的服务，或者创建区域 ID（如果尚不存在）。

步骤 9. 在“常规任务”页面的“站点配置”部分中，选择**执行注册**。注册 Controller，使其可供站点使用。

步骤 10. 在升级完成时选择**完成**之后，可以在 Citrix 遥测程序中进行注册，从而收集有关您的部署的信息。可以利用该信息来

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

提高产品质量、可靠性及性能。

步骤 11. 升级组件、数据库和站点之后，请测试新升级的站点。从 Studio 的导航窗格中选择 **Citrix Studio** *站点名称*。选择**常规任务**选项卡，然后选择**测试站点**。这些测试是在升级数据库之后自动运行的，但您可以随时重新运行。

如果未启动 SQL Server Browser 服务，当本地 SQL Server Express 用于站点数据库时，对 Windows Server 2016 上安装的 Controller，测试站点功能可能会失败。为了避免此问题，请完成下列任务。

1. 启用 SQL Server Browser 服务（如果需要），然后启动该服务。
2. 重新启动 SQL Server (SQLEXPRESS) 服务。

步骤 12. 如果您使用 Machine Creation Services 并希望使用升级的 VDA：在升级并测试部署之后，请更新主映像中使用的 VDA（如果您尚未更新）。更新使用这些 VDA 的主映像。请参阅更新或创建新主映像。然后更新使用这些主映像的计算机目录，以及升级使用这些目录的交付组。

升级核心组件和 VDA 之后，使用新升级的 Studio 来启动数据库和站点的自动或手动升级。

谨记：请检查上面的准备部分了解权限要求。

- 对于自动数据库升级，Studio 用户的权限必须能够更新 SQL Server 数据库架构。
- 如果进行手动升级，Studio 用户从 Studio 运行其中一些生成的脚本。数据库管理员使用 SQLCMD 实用程序或 SQLCMD 模式下的 SQL Server Management Studio 运行其他脚本。否则，可能会出现不准确的错误。

重要：Citrix 强烈建议在升级之前备份数据库。请参阅 CTX135207。
数据库升级期间，禁用产品服务。此时，Controller 无法为站点代理任何新连接，因此应认真规划。

数据库升级完成且产品服务启用之后，Studio 会先对环境和配置进行测试，然后生成一份 HTML 报告。如果确定出现了问题，可以还原数据库备份。解决问题之后，可以重新升级数据库。

自动升级数据库和站点：

启动新升级的 Studio。选择自动启动站点升级并确认准备工作就绪之后，数据库和站点将继续升级。

手动升级数据库和站点：

步骤 1. 启动新升级的 Studio。选择手动升级站点之后，向导会检查许可证服务器兼容性并请求确认。确认数据库已备份之后，向导会生成并显示脚本以及升级步骤核对表。

步骤 2. 按照所示顺序运行以下脚本。

脚本	说明
DisableServices.ps1	由 Controller 上的 Studio 用户运行的 PowerShell 脚本，用于禁用产品服务。
UpgradeSiteDatabase.sql	由包含站点数据库的服务器上的数据库管理员运行的 SQL 脚本。
UpgradeMonitorDatabase.sql	由包含监视数据库的服务器上的数据库管理员运行的 SQL 脚本。

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

UpgradeLoggingDatabase.sql	由包含配置日志记录数据库的服务器上的数据库管理员运行的 SQL 脚本。只有在此数据库更改时（例如，在应用修补程序之后）才运行此脚本。
EnableServices.ps1	由 Controller 上的 Studio 用户运行的 PowerShell 脚本，用于启用产品服务。

步骤 3. 完成核对清单任务后，单击**完成升级**。

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

将 XenApp 6.5 工作进程升级至新 VDA

Dec 05, 2017

迁移 XenApp 6.5 场后，可以通过删除早期版本的软件，然后安装 VDA for Server OS 来使用在仅会话-主机模式（又称为仅会话或工作进程服务器）下配置的 XenApp 6.5 服务器。

注意：虽然可以升级 XenApp 6.5 工作进程服务器，但在干净计算机上安装当前的 VDA 软件可提供更高的安全性。

要将 XenApp 6.5 工作进程服务器升级到新 VDA，请执行以下操作：

1. 根据修补程序自述中的说明删除 Hotfix Rollup Pack 7 for XenApp 6.5。请参阅 CTX202095。
2. 根据删除角色和组件中的说明卸载 XenApp 6.5。此过程需要多次重新启动。如果卸载过程中出错，请检查错误消息中引用的卸载错误日志。该日志文件位于“%TEMP%\Citrix\XenDesktop Installation\XenApp 6.5 Uninstall Log Files\”文件夹中。
3. 使用随本版本提供的安装程序安装 VDA for Server OS。请参阅安装 VDA 或使用命令行安装。

安装新 VDA 后，从新 XenApp 站点中的 Studio 为升级后的工作服务器创建计算机目录（或编辑现有目录）

故障排除

症状：删除 XenApp 6.5 软件失败。卸载日志包含消息：“Error 25703. 将 XML 插入 Internet Information Server 时发生错误。安装程序无法将文件复制到 IIS 脚本目录。Please make sure that your IIS installation is correct.”（错误 25703。将 XML 插入 Internet Information Server 时出错。安装程序无法将文件复制到 IIS 脚本目录。请确保 IIS 安装正确无误。）

原因：在以下情况下系统上会出现此问题：(1) 首次安装 XenApp 6.5 时，您指示 Citrix XML Service (CtxHttp.exe) 不能与 IIS 共享一个端口，以及 (2) 安装了 .NET Framework 3.5.1。

分辨率:

1. 使用 Windows 删除服务器角色向导删除 Web 服务器 (IIS) 角色。（之后可以重新安装 Web 服务器 (IIS) 角色。）
2. 重新启动服务器。
3. 使用“添加/删除程序”卸载 Citrix XenApp 6.5 和 Microsoft Visual C++ 2005 可再发行软件包 (x64) 8.0.56336。
4. 重新启动服务器。
5. 安装 VDA for Windows Server OS。

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

迁移 XenApp 6.x

Dec 05, 2017

注意：不能将 Citrix Smart Migrate 产品与此版本的 XenApp 和 XenDesktop 结合使用。但提供了迁移工具。

XenApp 6.x 迁移工具

XenApp 6.x 迁移工具是 PowerShell 脚本的集合，这些脚本中包含用于迁移 XenApp 6.x（6.0 或 6.5）策略和场数据的 cmdlet。在 XenApp 6.x 控制器服务器上，运行导出 cmdlet 以将数据收集到 XML 文件中。然后，从 XenApp 7.6 控制器，运行导入 cmdlet，以使用在导出过程中收集的数据创建对象。

此处提供概述迁移工具的视频。

以下操作顺序概述了迁移过程，之后将提供详细信息。

1. 在 XenApp 6.0 或 6.5 控制器上：
    1. 导入 PowerShell 导出模块。
    2. 运行导出 cmdlet 以将策略和/或场数据导入到 XML 文件中。
2. 将 XML 文件和图标文件夹（如果在导出过程中选择不将图标文件夹嵌入到 XML 文件中）复制到 XenApp 7.6 控制器。
3. 在 XenApp 7.6 控制器上：
    1. 导入 PowerShell 导入模块。
    2. 运行导入 cmdlet，以使用 XML 文件作为输入导入策略和/或场数据（应用程序）。
4. 完成迁移后的步骤。

运行实际迁移之前，可以先导出 XenApp 6.x 设置，然后在 XenApp 7.6 站点执行预览导入。通过预览可以识别潜在的故障点，使您可以在实际运行导入之前解决问题。例如，预览可能会检测到新 XenApp 7.6 站点中已经存在同名的应用程序。您也可以将通过预览生成的日志文件作为迁移指南。

除非另有说明，否则术语 6.x 是指 XenApp 6.0 或 6.5。

2014 年 12 月版本（版本 20141125）包含下列更新：

- 如果在 XenApp 6.x 场中使用迁移工具时遇到问题，请将问题报告到支持论坛 http://discussions.citrix.com/forum/1411-xenapp-7x/，以便 Citrix 能够调查这些问题，进而发现工具的潜在可改进功能。
- 新软件包 XAMigration.zip 文件现在包含两个单独的独立软件包：ReadIMA.zip 和 ImportFMA.zip。 要从 XenApp 6.x 服务器导出，只需使用 ReadIMA.zip。 要导入到 XenApp 7.6 服务器，只需使用 ImportFMA.zip。
- Export-XAFarm cmdlet 支持新参数 (EmbedIconData)，从而无需再将图标数据复制到单独的文件中。
- Import-XAFarm cmdlet 支持三个新参数。
    - MatchServer - 从名称与表达式匹配的服务器导入应用程序
    - NotMatchServer - 从名称与表达式不匹配的服务器导入应用程序
    - IncludeDisabledApps - 导入已禁用的应用程序
- 不导入预启动应用程序。
- Export-Policy cmdlet 适用于 XenDesktop 7.x。

迁移工具在 XenApp 7.6 Citrix 下载站点下提供。XAMigration.zip 文件包含两个单独的独立软件包：

- ReadIMA.zip - 包含用于从 XenApp 6.x 场导出数据的文件，以及一些共享模块。

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

模块或文件	说明
ExportPolicy.psm1	用于将 XenApp 6.x 策略导出至 XML 文件的 PowerShell 脚本模块。
ExportXAFarm.psm1	用于将 XenApp 6.x 场设置导出至 XML 文件的 PowerShell 脚本模块。
ExportPolicy.psd1	脚本模块 ExportPolicy.psm1 的 PowerShell 清单文件。
ExportXAFarm.psd1	脚本模块 ExportXAFarm.psm1 的 PowerShell 清单文件。
LogUtilities.psm1	包含日志记录功能的共享 PowerShell 脚本模块。
XmlUtilities.psd1	脚本模块 XmlUtilities.psm1 的 PowerShell 清单文件。
XmlUtilities.psm1	包含 XML 功能的共享 PowerShell 脚本模块。

- ImportFMA.zip - 包含用于将数据导入到 XenApp 7.6 场的文件，以及一些共享模块。

模块或文件	说明
ImportPolicy.psm1	用于将策略导入 XenApp 7.6 的 PowerShell 脚本模块。
ImportXAFarm.psm1	用于将应用程序导入 XenApp 7.6 的 PowerShell 脚本模块。
ImportPolicy.psd1	脚本模块 ImportPolicy.psm1 的 PowerShell 清单文件。
ImportXAFarm.psd1	脚本模块 ImportXAFarm.psm1 的 PowerShell 清单文件。
PolicyData.xsd	策略数据的 XML 架构。
XAFarmData.xsd	XenApp 场数据的 XML 架构。
LogUtilities.psm1	包含日志记录功能的共享 PowerShell 脚本模块。
XmlUtilities.psd1	脚本模块 XmlUtilities.psm1 的 PowerShell 清单文件。
XmlUtilities.psm1	包含 XML 功能的共享 PowerShell 脚本模块。

- 并非导入所有的策略设置；请参阅未导入的策略设置。不受支持的设置将被忽略并记录到日志文件中。
- 尽管在导出操作过程中会将所有应用程序详细信息收集到输出 XML 文件中，但是仅将服务器安装的应用程序导入到 XenApp 7.6 站点。不支持已发布桌面、内容和大多数流应用程序（请参阅分步说明：导入数据中的 Import-XAFarm cmdlet 参数以了解例外情况）。
- 不会导入应用程序服务器。
- 许多应用程序属性均不会被导入，因为 XenApp 6.x Independent Management Architecture (IMA) 和 XenApp 7.6 FlexCast Management Architecture (FMA) 技术之间存在差异；请参阅应用程序属性映射。
- 导入过程中会创建交付组。有关使用参数过滤导入内容的详细信息，请参阅高级用法。
- 仅导入使用 AppCenter 管理控制台创建的 Citrix 策略设置；不导入使用 Windows 组策略对象 (GPO) 创建的 Citrix 策略设置。
- 迁移脚本仅用于从 XenApp 6.x 到 XenApp 7.6 的迁移。
- 深度超过五级的嵌入式文件夹不受 Studio 支持，并且不会被导入。如果您的应用程序文件夹结构中包含深度超过五级的文件夹，请考虑在导入之前减少嵌入式文件夹级别的数量。

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

导出脚本所创建的 XML 文件可以包含有关您的环境和组织的敏感信息，例如，用户名、服务器名及其他 XenApp 场、应用程序和策略配置数据。 在安全环境中存储和处理这些文件。

使用 XML 文件作为输入来导入策略和应用程序之前，请认真查看这些文件，以确保其中没有任何未经授权的修改。

策略对象分配（以前称为策略过滤器）用于控制策略的应用。 导入策略之后，请认真查看每个策略的对象分配，以确保导入不会导致任何安全漏洞。 导入后，可以对策略应用几组不同的用户、IP 地址或客户端名称。 导入后，允许/拒绝设置可能具有不同的含义。

脚本提供详尽的日志记录，这些日志记录跟踪所有的 cmdlet 执行、有意义的消息、cmdlet 执行结果、警告和错误。

- 记录大多数 Citrix PowerShell cmdlet 的使用。 记录用于创建新站点对象的导入脚本中的所有 PowerShell cmdlet。
- 记录脚本执行进度，包括要处理的对象。
- 记录影响流状态的主要操作，包括从命令行发出的流。
- 记录打印到控制台的所有消息，包括警告和错误。
- 每行都具有时间戳，精确到毫秒。

Citrix 建议在运行每个导出和导入 cmdlet 时指定日志文件。

如果不指定日志文件名，日志文件将存储在当前用户的主文件夹中（在 PowerShell $HOME 变量中指定），前提是存在此文件夹。否则，日志文件存储在脚本的当前执行文件夹中。 默认 日志名为“XFarmYYYYMMDDHHmmSS-xxxxxx”，后六位数字 组成一个随机数字。

默认情况下，会显示所有进度信息。 要禁止显示这些信息，请在导出和导入 cmdlet 中指定 NoDetails 参数。

通常，脚本在遇到错误时停止执行。您可以在清除错误条件后重新运行 cmdlet。

未被视为错误的条件将记录到日志中；多数条件作为警告报告，脚本继续执行。 例如，不受支持的应用程序类型将作为警告报告并且不会被导入。 已存在于 XenApp 7.6 站点中的应用程序不会被导入。 XenApp 7.6 中已弃用的策略设置不会被导入。

迁移脚本使用多个 PowerShell cmdlet，可能不会记录所有的潜在错误。 有关其他日志记录覆盖范围，请使用 PowerShell 日志记录功能。例如，PowerShell 脚本记录打印到屏幕的所有内容。 有关详细信息，请参阅 Start-Transcript 和 Stop-Transcript cmdlet 的帮助。

要迁移，必须使用 Citrix XenApp 6.5 SDK。可从 https://www.citrix.com/downloads/xenapp/sdks/powershell-sdk.html 下载该 SDK。

重要：请务必在开始迁移之前完整阅读本文。
您应该了解有关执行策略、模块、cmdlet 和脚本的 PowerShell 概念。虽然不需要具备全面的脚本编写专业知识，但也应该理解要执行的 cmdlet。请在执行 cmdlet 前，使用 Get-Help cmdlet 来查看每个迁移 cmdlet 的帮助信息。例如：
Get-Help -full Import-XAFarm
在命令行指定日志文件，并始终在运行 cmdlet 后查看日志文件。如果脚本失败，检查并修复日志文件中识别出的错误，然后重新运行 cmdlet。

须知事项：

- 同时运行两个部署（XenApp 6.x 场和新的 XenApp 7.6 站点）时，为方便应用程序交付，可以在 StoreFront 或 Web Interface 中聚合这两个部署。请参阅有关您的 StoreFront 或 Web Interface 版本的 eDocs 文档（“管理”>“创建应用商店”）。
- 应用程序图标数据采用以下两种方法之一处理：
  - 如果在 Export-XAFarm cmdlet 中指定 EmbedIconData 参数，导出的应用程序图标数据将嵌入到输出 XML 文件中。.
  - 如果不在 Export-XAFarm cmdlet 中指定 EmbedIconData 参数，导出的应用程序图标数据将存储在以输出 XML 文件的基础名称后附加字符串“-icons”的名称命名的文件夹下面。例如，如果 XmlOutputFile 参数为“FarmData.xml”，则会创建“FarmData-icons”文件夹来存储应用程序图标。
    此文件夹中的图标数据文件为 .txt 文件，采用已发布应用程序的浏览器名称命名（虽然这些文件是 .txt 文件，但存储的数据被编码为二进制图标数据，导入脚本可以读取这些数据以重新创建应用程序图标）。导入操作过程中，如果在导入 XML 文件所在的位置找不到图标文件夹，将为导入的每个应用程序使用常规图标。
- 脚本模块、清单文件、共享模块和 cmdlet 的名称相似。使用 Tab 键自动补齐功能时请小心操作以避免出错。例如，Export-XAFarm 是一个 cmdlet。ExportXAFarm.psd1 和 ExportXAFarm.psm1 是无法执行的文件。
- 在下面的分步说明部分中，大多数 <string> 参数值用引号括起来。这些是单字字符串可选项。

从 XenApp 6.x 服务器导出：

- 导出必须在配置了控制器和会话主机（通常称为控制器）服务器模式的 XenApp 6.x 服务器上运行。
- 要运行导出 cmdlet，您必须是具有对象读取权限的 XenApp 管理员。您还必须具有足够的 Windows 权限，以便可以运行 PowerShell 脚本；下面的分步过程包含相关说明。
- 开始导出前，确保 XenApp 6.x 场处于正常状态。备份场数据库。使用 Citrix IMA Helper 实用程序 (CTX133983) 确认场的完整性：从“IMA 数据存储”选项卡，运行主检查（然后使用 DSCheck 选项解析有效的条目）。在迁移前修复问题有助于预防导出失败。例如，如果错误地从场删除了服务器，其数据可能仍保留在数据库中，这可能导致导出脚本中的 cmdlet 失败（例如，Get-XAServer -ZoneName）。如果 cmdlet 失败，脚本便会失败。
- 可以在具有活动用户连接的活动场上运行导出 cmdlet；导出脚本仅读取静态场配置和策略数据。

导入到 XenApp 7.6 服务器：

- 可以将数据导入到 XenApp 7.6 部署（以及支持的更高版本）。必须先安装 XenApp 7.6 控制器和 Studio 并创建站点，然后再导入从 XenApp 6.x 场导出的数据。虽然导入设置不需要 VDA，但通过 VDA 可以使应用程序文件类型变为可用。
- 要运行导入 cmdlet，您必须是具有对象读取和创建权限的 XenApp 管理员。完全权限管理员具有这些权限。您还必须具有足够的 Windows 权限，以便可以运行 PowerShell 脚本；下面的分步过程包含相关说明。
- 导入过程中不得存在其他活动的用户连接。导入脚本会创建多个新对象，如果其他用户在同一时间更改了配置，可能会出现中断。

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

请记住，您可以导出数据，然后使用带有 -Preview 参数的 cmdlet 来查看实际导入过程中将要发生的情况，而无需实际执行导入操作。日志将指出实际导入过程中发生的情况；如果出现错误，可以在实际开始导入之前解决这些问题。

此处提供了展示导出完整过程的视频。

要将数据从 XenApp 6.x 控制器导出到 XML 文件，请完成以下步骤。

1. 从 Citrix 下载站点下载 XAMigration.zip 迁移工具包。方便起见，请将其放在 XenApp 6.x 场和 XenApp 7.6 站点均可以访问的网络文件共享位置。在网络文件共享位置解压 XAMigration.zip。解压后应包括两个 zip 文件：ReadIMA.zip 和 ImportFMA.zip。
2. 以至少具有只读权限和运行 PowerShell 脚本的 Windows 权限的 XenApp 管理员身份登录到 XenApp 6.x 控制器。
3. 将 ReadIMA.zip 从网络文件共享复制到 XenApp 6.x 控制器。在控制器上将 ReadIMA.zip 解压并提取到一个文件夹中（例如：C:\XAMigration）。
4. 打开 PowerShell 控制台，将当前目录设置为脚本位置。例如：
   cd C:\XAMigration
5. 通过运行 Get-ExecutionPolicy 检查脚本执行策略。
6. 将脚本执行策略至少设置为 RemoteSigned 以允许执行脚本。例如：
   Set-ExecutionPolicy RemoteSigned
7. 导入模块定义文件 ExportPolicy.psd1 和 ExportXAFarm.psd1：
   Import-Module .\ExportPolicy.psd1

   Import-Module .\ExportXAFarm.psd1

   须知事项：
   - 如果打算仅导出策略数据，可以只导入 ExportPolicy.psd1 模块定义文件。同样，如果打算仅导入场数据，则只需导入 ExportXAFarm.psd1。
   - 导入模块定义文件还会添加所需的 PowerShell 管理单元。
   - 请勿导入 .psm1 脚本文件。
8. 要导出策略数据，应运行 Export-Policy cmdlet。

参数	说明
-XmlOutputFile "<string>.xml"	XML 输出文件名；此文件将存储导出数据。必须包含 .xml 扩展名。此文件不得存在，但是如果指定了路径，父路径必须存在。 默认值：无；此为必需的参数。
-LogFile "<string>"	日志文件名。扩展名为可选。如果不存在此文件，将会创建。如果此文件存在并且也指定了 NoClobber 参数，将会生成错误；否则将覆盖文件的内容。 默认：请参阅日志记录和错误处理
-NoLog	不生成日志输出。如果也指定了 LogFile 参数，此参数会覆盖 LogFile 参数。 默认值：False；生成日志输出
-NoClobber	不覆盖 LogFile 参数中指定的现有日志文件。如果日志文件不存在，此参数无效。 默认值：False；覆盖现有日志文件
-NoDetails	不向控制台发送关于脚本执行情况的详细报告。 默认值：False；向控制台发送详细报告
-SuppressLogo	不向控制台打印消息“XenApp 6.x 至 XenApp/XenDesktop 7.6 迁移工具版本 #yyyyMMdd-hhmm#”。此消息标识脚本版本，在执行故障排除时非常有用；因此，Citrix 建议省略此参数。 默认值：False；向控制台打印此消息

   示例：以下 cmdlet 将策略信息导出到名为 MyPolicies.xml 的 XML 文件。操作记录到名为 MyPolicies.log 的文件中。
   Export-Policy -XmlOutputFile ".\MyPolicies.XML"
   -LogFile ".\MyPolicies.Log"
9. 要导出场数据，应运行 Export-XAFarm cmdlet，指定日志文件和 XML 文件。

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

参数	说明
-XmlOutputFile "<string>.xml"	XML 输出文件名；此文件将存储导出数据。必须包含 .xml 扩展名。此文件不得存在，但是如果指定了路径，父路径必须存在。 默认值：无；此为必需的参数。
-LogFile "<string>"	日志文件名。扩展名为可选。如果不存在此文件，将会创建。如果此文件存在并且也指定了 NoClobber 参数，将会生成错误；否则将覆盖文件的内容。 默认：请参阅日志记录和错误处理
-NoLog	不生成日志输出。如果也指定了 LogFile 参数，此参数会覆盖 LogFile 参数。 默认值：False；生成日志输出
-NoClobber	不覆盖 LogFile 参数中指定的现有日志文件。如果日志文件不存在，此参数无效。 默认值：False；覆盖现有日志文件
-NoDetails	不向控制台发送关于脚本执行情况的详细报告。 默认值：False；向控制台发送详细报告
-SuppressLogo	不向控制台打印消息“XenApp 6.x 至 XenApp/XenDesktop 7.6 迁移工具版本 #yyyyMMdd-hhmm#”。此消息标识脚本版本，在执行故障排除时非常有用；因此，Citrix 建议省略此参数。 默认值：False；向控制台打印此消息
-IgnoreAdmins	不导出管理员信息。有关用法信息，请参阅高级用法。 默认值：False；导出管理员信息
-IgnoreApps	不导出应用程序信息。有关用法信息，请参阅高级用法。 默认值：False；导出应用程序信息
-IgnoreServers	不导出服务器信息。 默认值：False；导出服务器信息
-IgnoreZones	不导出区域信息。 默认值：False；导出区域信息
-IgnoreOthers	不导出配置日志记录、负载评估程序、负载平衡策略、打印机驱动程序和工作组等信息。 默认值：False；导出其他信息 注意：-IgnoreOthers 开关的用途是允许您在存在不影响正在用于导出或导入的实际数据的错误时继续进行导出。
-AppLimit <integer>	要导出的应用程序数。有关用法信息，请参阅高级用法。 默认值：导出所有应用程序
-EmbedIconData	将应用程序图标数据作为其他对象嵌入到同一 XML 文件中。 默认值：单独存储图标。有关详细信息，请参阅要求、准备和最佳实践。

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

参数	说明
-SkipApps <integer>	跳过的应用程序数。有关用法信息，请参阅高级用法。 默认值：不跳过任何应用程序

示例：以下 cmdlet 将场信息导出到名为 MyFarm.xml 的 XML 文件中。操作记录到 MyFarm.log 文件中。创建名为“MyFarm-icons”的文件夹，用于存储应用程序图标数据文件；此文件夹与 MyFarm.XML 位于相同位置。

```
Export-XAFarm -XmlOutputFile ".\MyFarm.XML" -LogFile ".\MyFarm.Log"
```

导出脚本完成后，在命令行指定的 XML 文件包含策略和 XenApp 场数据。应用程序图标文件包含图标数据文件，日志文件指示导出过程中发生的情况。

此处提供了展示导入完整过程的视频。

请记住，您可以在执行实际导入之前运行预览导入（发出带有 Preview 参数的 Import-Policy 或 Import-XAFarm cmdlet）并查看日志文件。

要使用导出时生成的 XML 文件将数据导入到 XenApp 7.6 站点，请完成以下步骤。

1. 以具有读写权限和运行 PowerShell 脚本的 Windows 权限的管理员身份登录到 XenApp 7.6 控制器。
2. 如果没有在网络文件共享上解压迁移工具包 XAMigration，请在此时解压。将 ImportFMA.zip 从网络文件共享复制到 XenApp 7.6 控制器。在控制器上将 ImportFMA.zip 解压并提取到一个文件夹中（例如：C:\XAMigration）。
3. 将 XML 文件（导出过程中生成的输出文件）从 XenApp 6.x 控制器复制到 XenApp 7.6 控制器上提取 ImportFMA.zip 文件的位置。
   如果在运行 Export-XAFarm cmdlet 时选择不将应用程序图标数据嵌入到 XML 输出文件中，请确保将图标数据文件夹和文件复制到 XenApp 7.6 控制器上与输出 XML 文件相同的位置，此位置包含应用程序数据和提取的 ImportFMA.zip 文件。
4. 打开 PowerShell 控制台，将当前目录设置为脚本位置。
   cd C:\XAMigration
5. 通过运行 Get-ExecutionPolicy 检查脚本执行策略。
6. 将脚本执行策略至少设置为 RemoteSigned 以允许执行脚本。例如：
   Set-ExecutionPolicy RemoteSigned
7. 导入 PowerShell 模块定义文件 ImportPolicy.psd1 和 ImportXAFarm.psd1：
   Import-Module .\ImportPolicy.psd1

   Import-Module .\ImportXAFarm.psd1

   须知事项：
   - 如果打算仅导入策略数据，可以只导入 ImportPolicy.psd1 模块定义文件。同样，如果打算仅导入场数据，则只需导入 ImportXAFarm.psd1。
   - 导入模块定义文件还会添加所需的 PowerShell 管理单元。
   - 请勿导入 .psm1 脚本文件。
8. 要导入策略数据，请运行 Import-Policy cmdlet，并指定包含已导出的策略数据的 XML 文件。

参数	说明
-XmlInputFile " <string>.xml"	XML 输入文件名；此文件包含通过运行 Export-Policy cmdlet 收集到的数据。必须包含 .xml 扩展名。 默认值：无；此为必需的参数。
-XsdFile "<string>"	XSD 文件名。导入脚本使用此文件验证 XML 输入文件的语法。有关用法信息，请参阅高级用法。 默认值：PolicyData.XSD
-LogFile " <string>"	日志文件名。如果已将导出日志文件复制到此服务器，请考虑为导入 cmdlet 使用不同的日志文件名。 默认：请参阅日志记录和错误处理
-NoLog	不生成日志输出。如果也指定了 LogFile 参数，此参数会覆盖 LogFile 参数。 默认值：False；生成日志输出
-NoClobber	不覆盖 LogFile 参数中指定的现有日志文件。如果日志文件不存在，此参数无效。

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

参数	说明
	默认值：False；覆盖现有日志文件
-NoDetails	不向控制台发送关于脚本执行情况的详细报告。 默认值：False；向控制台发送详细报告
-SuppressLogo	不向控制台打印消息“XenApp 6.x 至 XenApp/XenDesktop 7.6 迁移工具版本 #yyyyMMdd-hhmm#”。此消息标识脚本版本，在执行故障排除时非常有用；因此，Citrix 建议省略此参数。 默认值：False；向控制台打印此消息
-Preview	执行预览导入：从 XML 输入文件读取数据，但不向站点导入对象。日志文件和控制台指示预览导入过程中发生的情况。预览向管理员显示实际导入过程中发生的情况。 默认值：False；发生实际导入

示例：以下 cmdlet 从名为 MyPolcies.xml 的 XML 文件导入策略数据。操作记录到名为 MyPolicies.log 的文件中。
Import-Policy -XmlInputFile ".\MyPolicies.XML"
-LogFile ".\MyPolicies.Log"

9. 要导入应用程序，应运行 Import-XAFarm cmdlet，指定包含已导出的场数据的日志文件和 XML 文件。

参数	说明
-XmlInputFile "<string>.xml"	XML 输入文件名；此文件包含通过运行 Export-XAFarm cmdlet 收集到的数据。必须包含 .xml 扩展名。 默认值：无；此为必需的参数。
-XsdFile "<string>"	XSD 文件名。导入脚本使用此文件验证 XML 输入文件的语法。有关用法信息，请参阅高级用法。 默认值：XAFarmData.XSD
-LogFile "<string>"	日志文件名。如果已将导出日志文件复制到此服务器，请考虑为导入 cmdlet 使用不同的日志文件名。 默认：请参阅日志记录和错误处理
-NoLog	不生成日志输出。如果也指定了 LogFile 参数，此参数会覆盖 LogFile 参数。 默认值：False；生成日志输出
-NoClobber	不覆盖 LogFile 参数中指定的现有日志文件。如果日志文件不存在，此参数无效。 默认值：False；覆盖现有日志文件
-NoDetails	不向控制台发送关于脚本执行情况的详细报告。 默认值：False；向控制台发送详细报告
-SuppressLogo	不向控制台打印消息“XenApp 6.x 至 XenApp/XenDesktop 7.6 迁移工具版本 #yyyyMMdd-hhmm#”。此消息标识脚本版本，在执行故障排除时非常有用；因此，Citrix 建议省略此参数。 默认值：False；向控制台打印此消息
-Preview	执行预览导入：从 XML 输入文件读取数据，但不向站点导入对象。日志文件和控制台指示预览导入过程中发生的情况。预览向管理员显示实际导入过程中发生的情况。 默认值：False；发生实际导入

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

参数	说明
-DeliveryGroupName "<string>"	所有导入应用程序的交付组名称。有关用法信息，请参阅高级用法。 默认值：<xenapp-farm-name> - Delivery Group
-MatchFolder "<string>"	仅导入名称与此字符串匹配的文件夹中的应用程序。有关用法信息，请参阅高级用法。 默认值：不进行匹配
-NotMatchFolder "<string>"	仅导入名称与此字符串不匹配的文件夹中的应用程序。有关用法信息，请参阅高级用法。 默认值：不进行匹配
-MatchServer "<string>"	仅从名称与此字符串匹配的服务器导入应用程序。有关用法信息，请参阅高级用法。
-NotMatchServer "<string>"	仅从名称与此字符串不匹配的服务器导入应用程序。有关用法信息，请参阅高级用法。 默认值：不进行匹配
-MatchWorkerGroup "<string>"	仅导入发布到名称与此字符串匹配的工作组中的应用程序。有关用法信息，请参阅高级用法。 默认值：不进行匹配
-NotMatchWorkerGroup "<string>"	仅导入发布到名称与此字符串不匹配的工作组中的应用程序。有关用法信息，请参阅高级用法。 默认值：不进行匹配
-MatchAccount "<string>"	仅导入发布到名称与此字符串匹配的用户帐户中的应用程序。有关用法信息，请参阅高级用法。 默认值：不进行匹配
-NotMatchAccount "<string>"	仅导入发布到名称与此字符串不匹配的用户帐户中的应用程序。有关用法信息，请参阅高级用法。 默认值：不进行匹配
-IncludeStreamedApps	导入“StreamedToClientOrServerInstalled”类型的应用程序。（不导入其他流应用程序。） 默认值：不导入流应用程序
-IncludeDisabledApps	导入已标记为禁用的应用程序。 默认值：不导入已禁用的应用程序

示例：以下 cmdlet 从名为 MyFarm.xml 的 XML 文件导入应用程序。操作记录到名为 MyFarm.log 的文件中。

```
Import-XAFarm -XmlInputFile ".\MyFarm.XML"
-LogFile ".\MyFarm.Log"
```

10. 导入成功完成后，完成迁移后任务。

成功将 XenApp 6.x 策略和场设置导入到 XenApp 7.6 站点中时，请使用以下指南确保数据已正确导入。

- **策略和策略设置**

  导入策略实际上是一种复制操作，已弃用的设置和策略除外，这些设置和策略不会被导入。迁移后检查本质上是将两个站点作比较。

  1. 日志文件列出导入和忽略的所有策略和设置。首先，检查日志文件并识别没有导入的设置和策略。

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

2. 比较 XenApp 6.x 策略和导入到 XenApp 7.6 的策略。设置的值应保持不变（已弃用的策略设置除外，如下一步骤所述）。
   - 如果策略的数量很小，可以采用并列视图的方式比较 XenApp 6.x AppCenter 中显示的策略和 XenApp 7.6 Studio 中显示的策略。
   - 如果策略的数量很大，通过视觉观察进行比较可能不太可行。在这种情况下，使用策略导出 cmdlet (Export-Policy) 将 XenApp 7.6 策略导出到其他 XML 文件，然后使用文本比较工具（如 windiff）将该文件的数据与从 XenApp 6.x 导出策略时使用的 XML 文件中的数据作比较。
3. 使用未导入的策略设置部分中的信息来确定导入过程中可能发生变化的内容。如果 XenApp 6.x 策略仅包含已弃用的设置，整个策略均不会被导入。例如，如果 XenApp 6.x 策略仅包含 HMR 测试设置，则会完全忽略此策略，因为 XenApp 7.6 中没有受支持的等效设置。
   有些 XenApp 6.x 策略设置不再受支持，但在 XenApp 7.6 中实现了等效的功能。例如，在 XenApp 7.6 中，可以通过编辑交付组为服务器操作系统计算机配置重新启动计划；此功能之前通过策略设置得以实现。
4. 检查并确认过滤器应用到 XenApp 7.6 站点的方式，并将其与在 XenApp 6.x 中的应用方式作比较；XenApp 6.x 场和 XenApp 7.6 站点的关键不同之处可能会改变过滤器的效果。

- **过滤器**

仔细检查每个策略的过滤器。为确保过滤器在 XenApp 7.6 中的作用与最初在 XenApp 6.x 中的作用相同，可能需要进行必要的更改。

过滤	注意事项
访问控制	访问控制应该包含与源 XenApp 6.x 过滤器相同的值，并且应该可以在不进行任何更改的情况下使用。
Citrix CloudBridge	简单的布尔值；应该可以在不进行任何更改的情况下即可使用。（此产品现在称为 NetScaler SD-WAN。）
客户端 IP 地址	列出客户端 IP 地址范围；每个范围应该是被允许或拒绝。导入脚本保存这些值，但是，如果其他客户端连接到 XenApp 7.6 VDA 计算机，可能需要更改这些值。
客户端名称	与客户端 IP 地址过滤器类似，导入脚本保存这些值，但是，如果其他客户端连接到 XenApp 7.6 VDA 计算机，可能需要更改这些值。
组织单位	可能会保留这些值，具体取决于在导入 OU 时是否可以对其解析。请仔细检查此过滤器，尤其是在 XenApp 6.x 和 XenApp 7.6 计算机驻留在不同的域中时。如果没有正确配置过滤器值，策略可能会应用到错误的 OU 集。 OU 仅通过名称来表示，因此，将某个 OU 名称解析后，目标 OU 可能会与 XenApp 6.x 域中的 OU 包含不同的成员，但这种可能性很小。即使保留了 OU 过滤器的某些值，仍应仔细检查这些值。
用户或组	可能会保留这些值，具体取决于在导入帐户时是否可以对其解析。 与 OU 类似，帐户仅使用名称解析。因此，如果 XenApp 7.6 站点包含的域具有相同域名和用户名，但实际上是两个不同的域和用户，解析后的帐户可能不同于 XenApp 6.x 域用户。如果不正确检查和修改过滤器值，可能会出现错误的策略应用情况。
工作组	XenApp 7.6 不支持工作组。请考虑使用 XenApp 7.6 支持（XenApp 6.x 不支持）的交付组、交付组类型和标记过滤器。 • 交付组：允许基于交付组应用策略。每个过滤器条目指定一个交付组，可以允许或拒绝此交付组。 • 交付组类型：允许基于交付组类型应用策略。每个过滤器条目指定一个交付组类型，可以允许或拒绝此交付组类型。 • 标记：基于为 VDA 计算机创建的标记指定策略应用。可以允许或拒绝各个标记。

总而言之，如果 XenApp 6.x 场和 XenApp 7.6 站点位于不同的域中，需要重点关注一下涉及到域用户变更的过滤器。由于导入脚本在新域中仅使用域和用户名字符串来解析用户，因此可能会解析部分帐户，而另一部分帐户没有被解析。虽然不同的域和用户具有相同名称的可能性很小，但是仍应该仔细检查这些过滤器，以确保它们包含正确的值。

- **应用程序**

应用程序导入脚本不仅导入应用程序，还创建对象，如交付组。如果应用程序导入涉及到多次迭代，原始应用程序文件夹层次结构可能会发生显著变化。

1. 首先，读取迁移日志文件（其中包含导入了哪些应用程序、忽略了哪些应用程序的详细信息）和 cmdlet（用于创建应用程序）。
2. 对于每个应用程序：
   - 通过视觉观察来确保导入过程中保留了基本属性。使用应用程序属性映射部分中的信息来确定哪些属性按原样导入、哪些没有被导入、哪些已经使用 XenApp 6.x 应用程序数据初始化。
   - 检查用户列表。导入脚本自动将用户的详细列表导入到 XenApp 7.6 中应用程序的限制可见性列表中。检查以确保此列表保持不变。
3. 不会导入应用程序服务器。这意味着尚不可访问导入的所有应用程序。必须将包含这些应用程序的交付组分配到计算机目录，这些计算机目录包含具有已发布应用程序的可执行映像的计算机。对于每个应用程序：
   - 确保可执行文件名和工作目录指向存在于分配到交付组的计算机中的可执行文件（通过计算机目录）。

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

- 检查命令行参数（可能是任何内容，如文件名、环境变量或可执行文件名）。确认参数对分配到交付组的计算机目录中的所有计算机有效。

- **日志文件**
  日志文件是进行导出和导入时最重要的参考资源。这是为什么在默认情况下不能覆盖现有日志文件，并且默认日志文件名应该唯一的原因。

  如"日志记录和错误处理"部分所述，如果选择通过 PowerShell Start-Transcript 和 Stop-Transcript cmdlet（记录输入和打印到控制台的所有内容）使用其他日志记录覆盖范围，该输出和日志文件将提供关于导入和导出活动的完整参考。

  使用日志文件中的时间戳可以诊断某些问题。例如，如果导出或导入运行很长时间，则可以确定存在故障的数据库连接或解析用户帐户是否占用了大部分时间。

  通过日志文件中记录的命令还可以了解读取或创建某些对象的方式。例如，要创建交付组，会执行多个命令，不仅创建交付组本身，还会创建其他对象，如允许将应用程序对象分配到交付组的访问策略规则。

  日志文件还可以用于诊断失败的导出或导入。通常，日志文件的最后一行会指出导致失败的原因；日志文件中还会保存失败错误消息。与 XML 文件结合使用时，日志文件还可以用于确定失败所涉及的对象。

检查和测试迁移后，您可以：

1. 通过在服务器上运行 7.6 安装程序，将 XenApp 6.5 工作服务器升级到最新的 Virtual Delivery Agents (VDA)，此操作会删除 XenApp 6.5 软件，然后自动安装最新的 VDA。有关说明，请参阅将 XenApp 6.5 工作进程升级至新的 VDA for Windows Server OS。
   对于 XenApp 6.0 工作服务器，必须手动从服务器卸载 XenApp 6.0 软件。然后，可以使用 7.6 安装程序安装最新的 VDA。无法使用 7.6 安装程序自动删除 XenApp 6.0 软件。

2. 从新 XenApp 站点中的 Studio，为升级后的工作服务器创建计算机目录（或编辑现有目录）。
3. 将升级后的计算机从计算机目录添加到包含这些 VDA for Windows Server OS 上安装的应用程序的交付组。

默认情况下，Export-Policy cmdlet 将所有策略数据导出到 XML 文件中。同样，Export-XAFarm 将所有场数据导出到 XML 文件中。您可以使用命令行参数更加精确地控制要导出和导入的内容。

- **导出部分应用程序** - 如果具有大量应用程序，并且您希望控制要导出到 XML 文件中的数量，请使用以下参数：
  - AppLimit - 指定要导出的应用程序的数量。
  - SkipApps - 指定在导出后续应用程序之前要跳过的应用程序的数量。

  可以同时使用这两个参数，以便于管理的批次导出大量应用程序。例如，首次运行 Export-XAFarm 时，希望仅导出前 200 个应用程序，则可以在 AppLimit 参数中指定该值。

  ```
  Export-XAFarm -XmlOutputFile "Apps1-200.xml"
  -AppLimit "200"
  ```

  下次运行 Export-XAFarm 时，您希望导出后面的 100 个应用程序，则可以使用 SkipApps 参数忽略已经导出的应用程序（即前 200 个应用程序），并使用 AppLimit 参数导出后面的 100 个应用程序。

  ```
  Export-XAFarm -XmlOutputFile "Apps201-300.xml"
  -AppLimit "100" -SkipApps "200"
  ```

- **不导出某些对象** - 可以忽略某些对象，从而无需导出这些对象，特别是不会被导入的对象；请参阅未导入的策略设置和应用程序属性映射。使用以下参数防止导出不需要的对象：
  - IgnoreAdmins - 不导出管理员对象
  - IgnoreServers - 不导出服务器对象
  - IgnoreZones - 不导出区域对象
  - IgnoreOthers - 不导出配置日志记录、负载评估程序、负载平衡策略、打印机驱动器和工作组对象
  - IgnoreApps - 不导出应用程序；通过此参数可以将其他数据导出到 XML 输出文件，然后再次运行导出，从而将应用程序导出到其他 XML 输出文件。

  也可以使用这些参数解决可能会导致导出失败的问题。例如，如果区域中存在损坏的服务器，区域导出可能会失败；但如果使用 IgnoreZones 参数，则可以继续导出其他对象。

- **交付组名称** - 如果不希望将所有应用程序放置在一个交付组中（例如，因为这些应用程序供不同的用户集合访问并且发布到不同的服务器集合中），则可以多次运行 Import-XAFarm，每次指定不同的应用程序和不同的交付组。尽管可以在迁移后使用 PowerShell cmdlet 将应用程序从一个交付组移动到另一个交付组，但有选择性地导入到唯一的交付组可以减少或省去之后再移动应用程序的繁琐。
  1. 结合使用 DeliveryGroupName 参数和 Import-XAFarm cmdlet。脚本在指定交付组不存在时创建相应的交付组。
  2. 结合使用以下参数和正则表达式基于文件夹、工作组、用户帐户和/或服务器名称来过滤要导入到交付组中的应用程序。建议在正则表达式两边使用单引号或双引号。有关正则表达式的信息，请参阅 http://msdn.microsoft.com/zh-cn/library/hs600312(v=vs.110).aspx。
     - MatchWorkerGroup 和 NotMatchWorkerGroup - 例如，对于发布到工作组的应用程序，以下 cmdlet 将名为"Productivity Apps"的工作组中的应用程序导入到具有相同名称的 XenApp 7.6 交付组中：

       ```
       Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log
       –MatchWorkerGroup 'Productivity Apps' –DeliveryGroupName 'Productivity Apps'
       ```

     - MatchFolder 和 NotMatchFolder - 例如，对于采用应用程序文件夹组织的应用程序，以下 cmdlet 将名为"Productivity Apps"文件夹中的应用程序

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

导入到 具有相同名称的 XenApp 7.6 交付组中。
Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log –MatchFolder 'Productivity Apps' –DeliveryGroupName 'Productivity Apps'
例如，下列 cmdlet 将名称中包含"MS Office Apps"的任何文件夹中的应用程序导入到默认交付组中。
Import-XAFarm -XmlInputFile .\THeFarmApps.XML -MatchFolder ".*/MS Office Apps/.*"

- MatchAccount 和 NotMatchAccount - 例如，对于发布到 Active Directory 用户或用户组的应用程序，以下 cmdlet 将发布到用户组"Finance Group"的应用程序导入到名为"Finance"的 XenApp 7.6 交付组中。
  Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log
  –MatchAccount 'DOMAIN\\Finance Group' –DeliveryGroupName 'Finance'
- MatchServer 和 NotMatchServer - 例如，对于服务器上组织的应用程序，下列 cmdlet 将不以"Current"命名的服务器关联的应用程序导入到名为"Legacy"的 XenApp 交付组中。
  Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.log
  -NotMatchServer 'Current' -DeliveryGroupName 'Legacy'

- **自定义** - PowerShell 程序可以创建自己的工具。例如，您可以将导出脚本用作清单工具来跟踪 XenApp 6.x 场中的更改。您还可以修改 XSD 文件（或创建自己的 XSD 文件）以存储其他数据或 XML 文件中采用其他格式的数据。您可以随每个导入 cmdlet 指定非默认的 XSD 文件。
  注意：尽管您可以修改脚本文件以满足特定迁移要求或高级迁移要求，但是仅支持未修改状态的脚本。Citrix 技术支持人员会建议还原到未修改的脚本以确定预期行为或在必要时提供支持。

- 如果要使用 PowerShell 版本 2.0，并且已使用 Add-PSSnapIn cmdlet 添加了 Citrix Group Policy PowerShell 提供程序管理单元或 Citrix Common Commands 管理单元，运行导出或导入 cmdlet 时，可能会出现错误消息"Object reference not set to an instance of an object"（未将对象引用设置为对象的实例）。此错误不会影响脚本的执行，可以将其忽略。
- 请避免在使用导出和导入脚本模块的控制台会话中添加或删除 Citrix Group Policy PowerShell 提供程序管理单元，因为这些脚本模块会自动添加此管理单元。如果单独添加或删除此管理单元，可能会看到以下其中一条错误：
  - "A drive with the name 'LocalGpo' already exists."（已存在名为"LocalGpo"的驱动器。）管理单元被添加两次时会出现此错误。管理单元尝试在驱动器 LocalGpo 已加载的情况下装载此驱动器，然后报告错误。
  - "A parameter cannot be found that matches parameter name 'Controller'."（找不到与参数名"Controller"匹配的参数。）当未添加管理单元，而脚本尝试装载驱动器时会出现此错误。脚本不知道管理单元已被删除。请关闭控制台并启动新会话。在新会话中，导入脚本模块；不要单独添加或删除管理单元。
- 导入模块时，如果在 .psd1 文件上单击鼠标右键并选择打开或使用 PowerShell 打开，PowerShell 控制台窗口将快速打开并关闭，直到您停止进程。为避免此错误，请直接在 PowerShell 控制台窗口中输入完整的 PowerShell 脚本模块名称（例如，Import-Module .\ExportPolicy.psd1）。
- 如果在运行导出或导入时收到权限错误，请确保您是具有对象读取权限（对于导出）或对象的读取和创建权限（对于导入）的 XenApp 管理员。必须具有运行 PowerShell 脚本的 Windows 权限。
- 如果导出失败，请通过在 XenApp 6.x 控制器服务器上运行 DSMAINT 和 DSCHECK 实用程序来检查 XenApp 6.x 场是否处于正常状态。
- 如果运行预览导入，然后再次运行导入 cmdlet 以执行实际迁移，结果发现未导入任何内容，请验证是否从导入 cmdlet 删除 Preview 参数。

由于不再支持以下计算机和用户策略设置，因此不会导入这些策略设置。 请注意，未过滤的策略永不导入。支持这些设置的功能和组件已由新技术/组件替代，或者由于架构和平台变化导致这些设置不再适用。

未导入的计算机策略设置

- 连接访问控制
- CPU 管理服务器级别
- DNS 地址解析
- 场名称
- 完整图标缓存
- 运行状况监视、运行状况监视测试
- 许可证服务器主机名、许可证服务器端口
- 限制用户会话、管理员会话限制
- 负载评估程序名称
- 记录登录限制事件 。
- 具有登录控制功能的服务器的最大百分比
- 内存优化、内存优化应用程序排除列表、内存优化时间间隔、内存优化计划: 月日期、内存优化计划: 周日期、内存优化计划: 时间
- 脱机应用程序客户端信任、脱机应用程序事件日志记录、脱机应用程序许可证期限、脱机应用程序用户
- 提示输入密码
- 重新启动自定义警告、重新启动自定义警告文本、重新启动登录禁止时间、重新启动计划频率、重新启动计划随机时间间隔、重新启动计划开始日期、重新启动计划时间、重新启动警告时间间隔、重新启动警告开始时间、重新启动对用户的警告、排定的重新启动
- 重影 *

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

- 信任 XML 请求（在 StoreFront 中配置）
- 虚拟 IP 适配器地址过滤、虚拟 IP 兼容性程序列表、虚拟 IP 增强兼容性、虚拟 IP 过滤器适配器地址程序列表
- 工作负载名称
- XenApp 产品版本、XenApp 产品模型
- XML Service 端口

* 由 Windows 远程协助取代

未导入的用户策略设置
- 自动连接客户端 COM 端口、自动连接客户端 LPT 端口
- 客户端 COM 端口重定向、客户端 LPT 端口重定向
- 客户端打印机名称
- 并发登录限制
- 从重影连接输入
- 延迟断开连接计时器间隔、延迟终止计时器间隔
- 记录重影尝试
- 通知用户有挂起的重影连接
- 预启动断开连接计时器间隔、预启动终止计时器间隔
- 会话重要性
- Single Sign-On、Single Sign-On 中央存储
- 可重影其他用户的用户、无法重影其他用户的用户 *

* 由 Windows 远程协助取代

不会导入以下应用程序类型。
- 服务器桌面
- 内容
- 流应用程序（App-V 是用于流应用程序的新方法）

场数据导入脚本仅导入应用程序。以下应用程序属性按原样导入。

IMA 属性	FMA 属性
AddToClientDesktop	ShortcutAddedToDesktop
AddToClientStartMenu	ShortcutAddedToStartMenu
ClientFolder	ClientFolder
CommandLineExecutable	CommandLineExecutable
CpuPriorityLevel	CpuPriorityLevel
说明	说明
DisplayName	PublishedName
已启用	已启用
StartMenuFolder	StartMenuFolder
WaitOnPrinterCreation	WaitForPrinterCreation

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

IMA 属性	FMA 属性
WorkingDirectory	WorkingDirectory
FolderPath	AdminFolderName

注意：IMA 和 FMA 对文件夹名称长度的限制不相同。在 IMA 中，文件夹名称限制是 256 个字符；FMA 限制是 64 个字符。导入时，会跳过文件夹路径中包含的文件夹名称超过 64 个字符的应用程序。此限制仅适用于文件夹路径中的文件夹名称；整个文件夹路径的长度可以大于此限制。为避免在导入时跳过某些应用程序，Citrix 建议在导入前检查应用程序文件夹名称的长度并根据需要将其缩短。

默认情况下，以下应用程序属性可能已初始化，也可能未初始化，或者设置为 XenApp 6.x 数据中提供的值：

FMA 属性	值
名称	初始化为完整路径名称，其中包含 IMA 属性 FolderPath 和 DisplayName，但是去掉前导字符串 "Applications\"。
ApplicationType	HostedOnDesktop
CommandLineArguments	使用 XenApp 6.x 命令行参数初始化
IconFromClient	未初始化；默认为 False
IconUid	初始化为使用 XenApp 6.x 图标数据创建的图标对象
SecureCmdLineArgumentsEnabled	未初始化；默认为 True
UserFilterEnabled	未初始化；默认为 False
UUID	只读，由 Controller 分配
可见	未初始化；默认为 True

以下应用程序属性将部分迁移：

IMA 属性	备注
FileTypes	只迁移存在于新 XenApp 站点上的文件类型。不存在于新站点上的文件类型将被忽略。文件类型只有在新站点上的文件类型更新之后才会导入。
IconData	如果已经为导出的应用程序提供图标数据，将创建新图标对象。
帐户	应用程序的用户帐户在交付组的用户列表和应用程序的用户列表之间分隔开。显式用户用于初始化应用程序的用户列表。此外，向交付组的用户列表中添加了用户帐户所在域的“域用户”帐户。

不会导入下列 XenApp 6.x 属性：

IMA 属性	备注
ApplicationType	忽略。
HideWhenDisabled	忽略。
AccessSessionConditions	由交付组访问策略替代。
AccessSessionConditionsEnabled	由交付组访问策略替代。

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

IMA 属性	备注
AnonymousConnectionsThroughAccessGatewayAllowed	由交付组访问策略替代。
OtherConnectionsAllowed	由交付组访问策略替代。
AlternateProfiles	FMA 不支持流应用程序。
OfflineAccessAllowed	FMA 不支持流应用程序。
ProfileLocation	FMA 不支持流应用程序。
ProfileProgramArguments	FMA 不支持流应用程序。
ProfileProgramName	FMA 不支持流应用程序。
RunAsLeastPrivilegedUser	FMA 不支持流应用程序。
AnonymousConnectionsAllowed	FMA 使用其他技术支持未经身份验证（匿名）连接。
ApplicationId、SequenceNumber	IMA 唯一数据。
AudioType	FMA 不支持高级客户端连接选项。
EncryptionLevel	在交付组中启用/禁用 SecureICA。
EncryptionRequired	在交付组中启用/禁用 SecureICA。
SslConnectionEnabled	FMA 使用其他 TLS 实现方法。
ContentAddress	FMA 不支持已发布的内容。
ColorDepth	FMA 不支持高级窗口外观。
MaximizedOnStartup	FMA 不支持高级窗口外观。
TitleBarHidden	FMA 不支持高级窗口外观。
WindowsType	FMA 不支持高级窗口外观。
InstanceLimit	FMA 不支持应用程序限制。
MultipleInstancesPerUserAllowed	FMA 不支持应用程序限制。
LoadBalancingApplicationCheckEnabled	FMA 使用其他技术支持负载平衡。
PreLaunch	FMA 使用其他技术支持会话预启动。
CachingOption	FMA 使用其他技术支持会话预启动。

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

FMA 属性	备注
HomeZoneNames	FMA 使用其他技术。
WorkerGroupNames	FMA 不支持工作组。

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

安全

Dec 05, 2017

XenApp 和 XenDesktop 提供设计安全的解决方案，使您可以根据安全需求定制环境。

IT 面临着移动工作人员数据丢失或被盗的安全隐患。通过托管应用程序和桌面，XenApp 和 XenDesktop 将所有数据存储在数据中心内，从而安全地将敏感数据和知识产权与终端设备分开。当启用策略以允许数据传输时，所有数据均会加密。

XenDesktop 和 XenApp 数据中心还提供集中式监视服务和管理服务，从而更易于响应事件。Director 允许 IT 监视和分析可通过网络访问的数据，Studio 允许 IT 修补和修复数据中心内的大部分漏洞，而不是在每个最终用户设备本地解决问题。

XenApp 和 XenDesktop 还简化了审计和法规遵从性操作，因为调查人员可以使用集中化审核追踪来确定哪些人员访问了哪些应用程序和数据。Director 通过访问配置日志记录和 OData API 收集有关系统更新和用户数据使用情况的历史数据。

通过委派管理员功能，您可以设置管理员角色，从而在某一粒度级别控制对 XenDesktop 和 XenApp 的访问。这样一来，在您的组织内可以灵活地向某些管理员授予任务、操作和作用域的完全访问权限，而其他管理员仅具有有限的访问权限。

XenApp 和 XenDesktop 通过在不同的网络级别（从本地级别到组织单位级别）应用策略，向管理员提供对用户的粒度级控制。这种策略控制确定用户、设备或用户和设备组是否可以连接、复制/粘贴或映射本地驱动器，从而尽可能地降低对第三方临时工作人员的安全顾虑。管理员还可以使用 Desktop Lock 功能，因此，当阻止对最终用户设备的本地操作系统进行访问时，最终用户仅可以使用虚拟桌面。

管理员还可以通过将站点配置为针对 Controller 或在最终用户和 Virtual Delivery Agent (VDA) 之间使用传输层安全性 (TLS) 协议，来增加 XenApp 或 XenDesktop 的安全性。也可以在站点上启用此协议，从而为 TCP/IP 连接提供服务器身份验证、数据流加密和消息完整性检查功能。

XenApp 和 XenDesktop 还支持向 Windows 或特定应用程序提供多重身份验证。多重身份验证还可以用于管理 XenApp 和 XenDesktop 交付的所有资源。这些方法包括：

- 令牌
- 智能卡
- RADIUS
- Kerberos
- 生物识别

XenDesktop 可以与从身份管理到防病毒软件等多种第三方安全解决方案集成。http://www.citrix.com/ready 提供了支持的产品列表。

选择用于通用准则标准认证的 XenApp 和 XenDesktop 版本。有关这些标准的列表，请访问 http://www.commoncriteriaportal.org/cc/。

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

安全注意事项和最佳做法

Apr 10, 2018

本文档介绍以下内容：

- 使用此版本时的常规最佳安全做法，以及此版本和传统计算机环境之间在安全性方面的区别
- 管理用户帐户
- 管理用户权限
- 管理登录权限
- 配置用户权限
- 配置服务设置
- 部署方案及其安全含义
- Remote PC Access 安全注意事项

您的组织可能需要符合特定安全标准才能满足监管要求。本文档不涉及此主题，因为这些安全标准随着时间的推移而发生变化。有关安全标准和 Citrix 产品的最新信息，请访问 http://www.citrix.com/security/。

最佳安全做法

使用安全修补程序使您环境中的所有计算机始终保持最新。一项优势是您可以将瘦客户端用作终端，从而简化此任务。

使用防病毒软件保护环境中的所有计算机。

请考虑使用特定于平台的反恶意软件，例如适用于 Windows 计算机的 Microsoft Enhanced Mitigation Experience Toolkit (EMET)。一些机构建议在其管理的环境内使用受 Microsoft 支持的最新 EMET 版本。请注意，根据 Microsoft 的声明，EMET 可能与一些软件不兼容，因此，应在生产环境中部署之前对您的应用程序进行彻底的测试。已在 XenApp 和 XenDesktop 的默认配置中测试 EMET 5.5。目前，不建议在已安装 Virtual Delivery Agent (VDA) 的计算机上使用 EMET。

使用外围防火墙保护环境中的所有计算机，包括区域边界上的计算机（视情况而定）。

如果您正在将传统环境迁移到此版本，可能需要重新定位现有外围防火墙或添加新的外围防火墙。例如，假设传统客户端与数据中心中的数据库服务器之间存在外围防火墙。使用此版本时，必须将此外围防火墙放在相应的位置，使虚拟桌面和用户设备位于一侧，数据中心中的数据库服务器和 Delivery Controller 位于另一侧。因此，应该考虑在数据中心内创建一个区域以包含数据库服务器和 Controller。另外，还应考虑在用户设备和虚拟桌面之间建立保护。

环境中的所有计算机均应使用个人防火墙进行保护。在安装核心组件和 VDA 时，如果检测到 Windows 防火墙服务（即使未启用防火墙），可以选择自动打开组件和功能通信所需的端口。您还可以选择手动配置这些防火墙端口。如果您使用其他防火墙，必须手动配置该防火墙。

注意：TCP 端口 1494 和端口 2598 用于 ICA 和 CGP，因此在防火墙上可能处于打开状态，以便数据中心之外的用户可以进行访问。Citrix 建议您不要为任何其他对象使用这些端口，以避免因疏忽而使管理接口处于打开状态，从而导致受到攻击。端口 1494 和 2598 是向 Internet 编号授权委员会 (http://www.iana.org/) 正式注册的端口。

所有网络通信都应该根据您的安全策略进行适当的保护和加密。您可以使用 IPSec 保护 Microsoft Windows 计算机之间的所有通信；有关如何执行此任务的详细信息，请参阅您的操作系统文档。此外，通过 Citrix SecureICA（默认情况下已配置为 128 位加密）保护用户设备和桌面之间的通信。可以在创建或更新交付组时配置 SecureICA。

应用帐户管理的 Windows 最佳做法。请勿在 Machine Creation Services 或 Provisioning Services 复制模板或映像之前，基于

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

模板或映像创建帐户。请勿使用存储的特权域帐户安排任务。请勿手动创建共享 Active Directory 计算机帐户。这些做法有助于阻止计算机攻击获取本地静态帐户密码，然后使用它们登录属于其他人的 MCS/PVS 共享映像。

管理用户权限

只授予用户使用所需功能的权限。Microsoft Windows 权限仍可以通过常规方法应用于桌面：通过“用户权限分配”配置权限，通过“组策略”对成员身份进行分组。此版本的一个优点是可以授予用户对桌面的管理权限，而不必同时授予对存储此桌面的计算机的物理控制权限。

规划桌面权限时，请注意：

- 默认情况下，当无特权的用户连接到桌面后，他们会看到运行桌面的系统的时区，而不是他们自己的用户设备的时区。有关如何使用户在使用桌面时看到自己的本地时间的信息，请参阅更改基础设置。
- 身份为某桌面管理员的用户可以完全控制该桌面。如果某桌面是池桌面，而不是专用桌面，则此桌面的所有其他用户（包括将来的用户）必须信任此用户。此桌面的所有用户都需要了解这种情况可能对数据安全性造成的永久风险。对于专用桌面则不需要考虑这个问题，因为专用桌面只有一个用户；此用户不应是其他任何桌面的管理员。
- 通常，身份为某桌面管理员的用户可以在此桌面上安装软件，包括潜在恶意软件。该用户可能还可以监视或控制任何连接到该桌面的网络上的通信。

某些应用程序需要桌面权限，即使其面向用户而非面向管理员亦如此。这些用户可能意识不到安全风险。

即使这些应用程序的数据不敏感，也请将其视为高度敏感的应用程序。请考虑采用以下方法来降低安全风险：

- 强制执行双重身份验证并对应用程序禁用任何单点登录机制
- 强制执行上下文访问策略
- 将应用程序发布到专用桌面。如果必须将应用程序发布到共享托管桌面，则请勿将任何其他应用程序发布到该共享托管桌面。
- 确保桌面权限仅应用到该桌面，而不应用到其他计算机
- 对应用程序启用 Session Recording。此外，请在应用程序中以及在 Windows 自身内部启用其他安全日志记录功能。
- 配置 XenApp 和 XenDesktop 以限制要在应用程序中使用的功能（例如，剪贴板、打印机、客户端驱动器以及 USB 重定向）
- 启用应用程序的任何安全功能。对其进行限制以严格满足用户的要求
- 配置 Windows 的安全功能以严格满足用户的要求仅当该单个应用程序发布到桌面时，这才属于一个较为简单的配置；例如，可以使用严格的 AppLocker 配置。控制对文件系统的访问权限。
- 计划重新配置、升级或替换应用程序，以便将来不再需要桌面权限

这些方法不会消除来自需要桌面权限的应用程序的所有安全风险。

管理登录权限

用户帐户和计算机帐户均需要登录权限。如果授予 Microsoft Windows 权限，登录权限将继续通过常规方法应用于桌面：通过“用户权限分配”配置登录权限，通过“组策略”对成员身份进行分组。

Windows 登录权限包括：本地登录、通过远程桌面服务登录、通过网络登录（从网络中访问此计算机）、作为批处理作业登录以及作为服务登录。

对于计算机帐户，仅授予计算机所需要的登录权限。需要“从网络中访问此计算机”登录权限：

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

- 在 VDA 上，针对 Delivery Controller 的计算机帐户
- 在 Delivery Controller 上，针对 VDA 的计算机帐户。请参阅基于 Active Directory OU 的控制器发现。
- 在 StoreFront 服务器上，针对位于相同 StoreFront 服务器组的其他服务器的计算机帐户

对于用户帐户，请仅授予用户所需的登录权限。

根据 Microsoft 的规定，默认情况下，“远程桌面用户”组被授予登录权限“允许通过远程桌面服务登录”（在域控制器上除外）。

贵组织的安全策略可能会明确声明应将此组从该登录权限中删除。请考虑使用以下方法：

- 适用于服务器操作系统的 Virtual Delivery Agent (VDA) 使用 Microsoft 远程桌面服务。可以将“远程桌面用户”组配置为受限组，并通过 Active Directory 组策略控制组的成员身份。有关详细信息，请参阅 Microsoft 文档。
- 对于 XenApp 和 XenDesktop 的其他组件（包括 VDA for Desktop OS），不需要“远程桌面用户”组。因此，对于这些组件，“远程桌面用户”组不需要登录权限“允许通过远程桌面服务登录”，可以将其删除。此外：
  - 如果通过远程桌面服务管理这些计算机，请确保所有此类管理员已属于“管理员”组的成员。
  - 如果不通过远程桌面服务管理这些计算机，请考虑在这些计算机上禁用远程桌面服务本身。

虽然可以向登录权限“拒绝通过远程桌面服务登录”中添加用户和组，但通常不建议使用拒绝登录权限。有关详细信息，请参阅 Microsoft 文档。

配置用户权限

Delivery Controller 安装会创建以下 Windows 服务：

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService)：管理虚拟机的 Microsoft Active Directory 计算机帐户。
- Citrix Analytics (NT SERVICE\CitrixAnalytics)：收集由 Citrix 使用的站点配置使用情况信息（如果站点管理员已批准执行此收集）。然后，将此信息提交给 Citrix 以帮助改进产品。
- Citrix App Library (NT SERVICE\CitrixAppLibrary)：支持对 AppDisk、AppDNA 集成进行管理和置备，支持对 App-V 进行管理。
- Citrix Broker Service (NT SERVICE\CitrixBrokerService)：选择对用户可用的虚拟桌面或应用程序。
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging)：记录由管理员对站点执行的所有配置更改和其他状态更改。
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService)：用于共享的配置的站点范围的存储库。
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin)：管理向管理员授予的权限。
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest)：管理其他 Delivery Controller 服务的自检。
- Citrix Host Service (NT SERVICE\CitrixHostService)：存储关于在 XenApp 或 XenDesktop 部署中使用的虚拟机管理程序基础结构的信息，并提供由控制台用于枚举虚拟机管理程序池中资源的功能。
- Citrix Machine Creation Service (NT SERVICE\CitrixMachineCreationService)：调配桌面虚拟机的创建过程。
- Citrix Monitor Service (NT SERVICE\CitrixMonitor)：收集 XenApp 或 XenDesktop 的指标、存储历史记录信息，并提供查询界面以用于故障排除和报告工具。
- Citrix Storefront Service (NT SERVICE\ CitrixStorefront)：支持对 StoreFront 进行管理。（它不包含在 StoreFront 组件自身中。）
- Citrix Storefront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService)：支持 StoreFront 的特权管理操作。（它不包含在 StoreFront 组件自身中。）
- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService)：将主站点数据库中的配置数据传播到本地主机缓存。
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService)：在主站点数据库不可用时，选择用户可用的虚拟

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

桌面或应用程序。

Delivery Controller 安装还会创建以下 Windows 服务。当与其他 Citrix 组件一起安装时也将创建这些服务：

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc)：支持收集由 Citrix 使用的诊断信息。
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService)：收集由 Citrix 用于执行分析的诊断信息，以使管理员可查看分析结果和建议信息，从而帮助诊断站点中的问题。

Delivery Controller 安装还会创建以下 Windows 服务。这在当前未使用。如果它已启用，请将其禁用。

- Citrix Remote Broker Provider (NT SERVICE\XaXdCloudProxy)

Delivery Controller 安装还会创建以下 Windows 服务。这些在当前未使用，但必须启用。请勿禁用它们。

- Citrix 的业务流程服务 (NT SERVICE\CitrixOrchestration)
- Citrix Trust Service (NT SERVICE\CitrixTrust)

除 Citrix Storefront Privileged Administration Service 外，这些服务均被授予登录权限“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”。您不需要更改这些用户权限。这些权限将不由 Delivery Controller 使用，并且已自动禁止。

配置服务设置

除 Citrix Storefront Privileged Administration Service 和 Citrix Telemetry Service 外，在前面的配置用户权限部分中列出的 Delivery Controller Windows 服务被配置为以“网络服务”身份登录。请不要更改这些服务设置。

Citrix Storefront Privileged Administration Service 被配置为登录本地系统 (NT AUTHORITY\SYSTEM)。这对于通常不会提供给服务的 Delivery Controller StoreFront 操作（包括创建 Microsoft IIS 站点）而言是必需的。请勿更改其服务设置。

Citrix Telemetry Service 被配置为以其自己的服务特定身份登录。

可以禁用 Citrix Telemetry Service。除此服务和已禁用的服务外，不要禁用这些 Delivery Controller Windows 服务中的任何其他服务。

配置注册表设置

不再需要在 VDA 文件系统中启用 8.3 文件名和文件夹的创建。可以配置注册表项 **NtfsDisable8dot3NameCreation** 以禁用 8.3 文件名和文件夹的创建。还可以使用 **fsutil.exe behavior set disable8dot3** 命令配置此功能。

部署方案安全含义

您的用户环境可以包含以下两种用户设备之一：不受您的组织管理而完全由用户控制的用户设备；由您的组织管理的用户设备。通常，这两种环境的安全注意事项不同。

受管理的用户设备

受管理的用户设备接受管理控制；它们由您自己控制或者由您信任的另一组织控制。可以配置用户设备并将其直接提供给用户；也可以提供单个桌面在仅全屏模式下运行的终端。对于所有受管理的用户设备，请遵循上述常规最佳安全做法。此版本具

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

有一项优点，即用户设备上所需的软件较少。

受管理的用户设备可以配置为在仅全屏模式或窗口模式下使用：

- 仅全屏模式：用户使用常见的“登录到 Windows”屏幕登录。然后使用相同的用户凭据自动登录到此版本。
- 用户在窗口中查看其桌面：用户首先登录到用户设备，然后通过随此版本提供的 Web 站点登录此版本。

非托管用户设备

不由可信组织管理的用户设备不能被假定为受到管理控制。例如，您可以准许用户获得并配置他们自己的设备，但用户可以不遵循上述一般安全性最佳做法。此版本的优势是可以安全地将桌面传送给非托管用户设备。这些设备应该仍具备基本的防病毒功能，可查杀键盘记录器和类似的输入攻击。

数据存储注意事项

使用此版本时，您可以阻止用户将数据存储到用户可以物理控制的用户设备中。然而，您还必须考虑到将数据存储到桌面所产生的影响。用户将数据存储在桌面上这种做法并不好；数据应该放在文件服务器、数据库服务器，或者可以适当受保护的其他存储库中。

您的桌面环境可能包含各种类型的桌面，例如池桌面和专用桌面。用户不应该将数据存储在用户之间共享的桌面（例如池桌面）上。如果用户将数据存储在专用桌面上，则以后其他用户使用该桌面时应该删除这些数据。

混合版本环境

在一些升级过程中，不可避免地会出现混合版本环境。请遵循最佳做法，尽可能缩短不同版本的 Citrix 组件共同存在的时间。例如，在混合版本环境中，安全策略可能不会统一实施。

注意：这是其他软件产品的典型特征；使用早期版本的 Active Directory 只能部分向更高版本的 Windows 实施组策略。

以下场景描述了在特定混合版本的 Citrix 环境中会发生的安全问题。使用 Citrix Receiver 1.7 连接到运行 XenApp 和 XenDesktop 7.6 Feature Pack 2 中的 VDA 的虚拟桌面时，在站点中启用了**允许在桌面与客户端之间传输文件**策略设置，但是无法通过运行 XenApp 和 XenDesktop 7.1 的 Delivery Controller 禁用此策略。它不能识别此策略设置，此策略仅在产品的更高版本中发布。此策略设置允许用户从其虚拟桌面上载文件和向其虚拟桌面下载文件，这是一种安全问题。要解决此问题，请将 Delivery Controller（或 Studio 的独立实例）升级到版本 7.6 Feature Pack 2，然后使用组策略禁用此策略设置。或者，在所有受影响的虚拟桌面上使用本地策略。

Remote PC Access 安全注意事项

Remote PC Access 实现了以下安全功能：

- 支持使用智能卡。
- 在远程会话连接时，办公室 PC 的显示器会显示空白。
- Remote PC Access 将所有键盘和鼠标输入重定向到远程会话，但 Ctrl+Alt+Del、启用 USB 的智能卡以及生物识别设备除外。
- SmoothRoaming 仅支持单个用户。
- 在用户发起连接到办公室 PC 的远程会话时，只有该用户可以恢复该办公室 PC 的本地访问。要恢复本地访问，用户需要在本地 PC 上按下 Ctrl-Alt-Del，然后使用远程会话所用的凭据进行登录。如果系统具有适当的第三方凭据提供程序集成功能，用户还可以通过插入智能卡或利用生物识别来恢复本地访问。通过启用基于组策略对象 (GPO) 的快速用户切换或编辑注册表，可以覆盖此默认行为。

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

注意：Citrix 建议您不要将 VDA 管理员权限分配给一般会话用户。

自动分配

默认情况下，Remote PC Access 支持将多个用户自动分配给 VDA。在 XenDesktop 5.6 Feature Pack 1 中，管理员可以通过使用 RemotePCAccess.ps1 PowerShell 脚本覆盖此行为。此版本使用注册表项来允许或禁止多个自动 Remote PC 分配。此设置适用于整个站点。

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

限制向单个用户执行自动分配：

在站点中的每个 Controller 中，设置以下注册表项：

HKEY_LOCAL_MACHINE\Software\Citrix|DesktopServer

名称：AllowMultipleRemotePCAssignments

类型：REG_DWORD

数据：0 = 禁止多用户分配，1 =（默认值）启用多用户分配。

如果存在任何现有用户分配，请使用 SDK 命令将其删除，以便接下来 VDA 可以执行单个自动分配。

- 从 VDA 中删除所有已分配的用户：$machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine
- 从交付组中删除 VDA：$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup

重新启动办公室物理 PC。

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

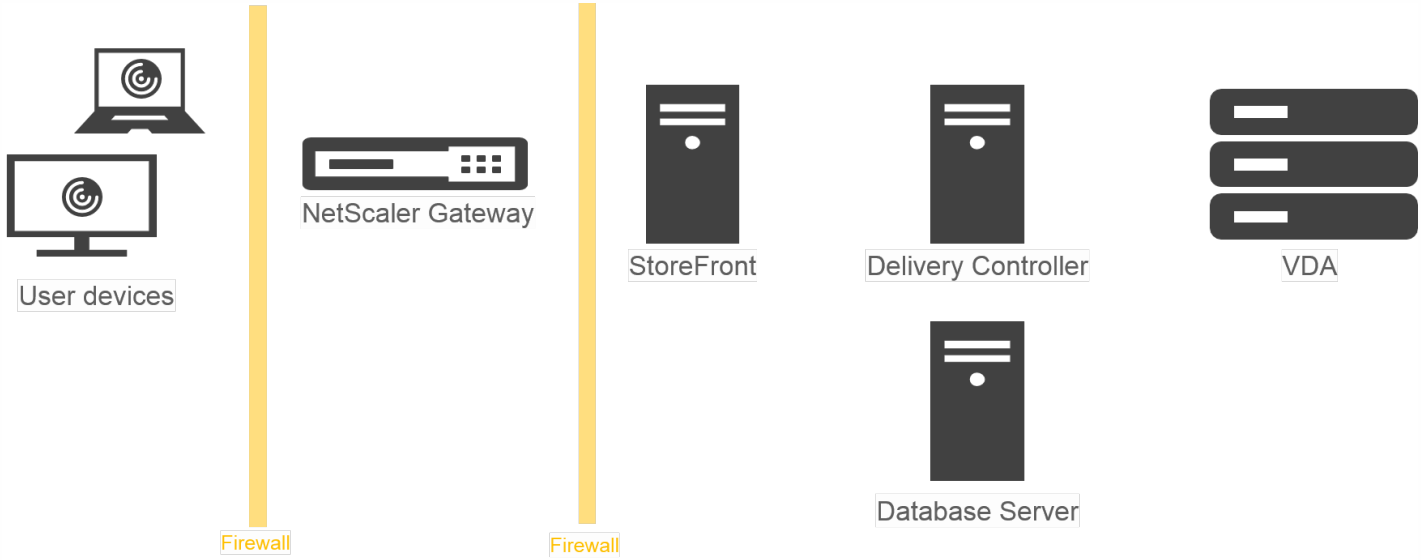
将 XenApp 和 XenDesktop 与 NetScaler Gateway 集成

Dec 05, 2017

要管理对已发布资源和数据的访问，可以部署和配置 StoreFront 服务器。为了进行远程访问，建议在 StoreFront 前面添加 NetScaler Gateway。

> **注意**
>
> 有关如何将 XenApp 和 XenDesktop 与 NetScaler Gateway 集成的详细配置步骤，请参阅 StoreFront 文档。

下图显示了包括 NetScaler Gateway 的 Citrix 简化的 Citrix 部署示例。NetScaler Gateway 与 StoreFront 通信来保护 XenApp 和 XenDesktop 提供的应用程序和数据。用户设备运行 Citrix Receiver 来创建安全连接以及访问其应用程序、桌面和文件。



用户使用 NetScaler Gateway 登录并进行身份验证。NetScaler Gateway 部署在 DMZ 中并受到保护。配置了双重身份验证。用户会根据用户凭据获得相关的资源和应用程序。应用程序和数据位于相应的服务器上（图中未显示）。安全性敏感应用程序和数据使用单独的服务器。

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

委派管理

Dec 05, 2017

“委派管理”模型可以使用角色和基于对象的控制机制灵活地与组织所需的管理活动委派方式相匹配。委派管理可以适应所有规模的部署，并且随着部署复杂性的增加，可以帮助您更细化地配置权限。委派管理基于三个概念：管理员、角色和作用域。

- **管理员** — 管理员是指由 Active Directory 帐户所标识的一个或一组人。每个管理员均与一个或多个角色和作用域对相关联。
- **角色** — 角色代表一项工作职能，并且具有定义的关联权限。例如，“交付组管理员”角色具有“创建交付组”和“从交付组中删除桌面”等权限。管理员在一个站点中可以具有多个角色，因此一个人既可以是交付组管理员，又可以是计算机目录管理员。角色可以内置或自定义。

  内置角色包括：

角色	权限
完全权限管理员	可以执行所有任务和操作。完全权限管理员始终与“全部”作用域结合。
只读权限管理员	可以查看指定作用域内的所有对象及全局信息，但不能更改任何内容。例如，作用域为“伦敦”的只读权限管理员可以查看所有全局对象（例如配置日志记录）和所有伦敦作用域内的对象（例如，伦敦交付组）。但是，该管理员无法查看“纽约”作用域（假设“纽约”作用域和“伦敦”作用域无重叠）中的对象。
技术支持管理员	可以查看交付组，并管理与之关联的会话和计算机。可以查看所监视的交付组的计算机目录和主机信息，还可以对这些交付组中的计算机执行会话管理和计算机电源管理操作。
计算机目录管理员	可以创建并管理计算机目录，并将计算机置备到这些目录中。可以从虚拟化基础结构、Provisioning Services 和物理机构建计算机目录。此角色可以管理基础映像并安装软件，但不可以向用户分配应用程序或桌面。
交付组管理员	可以交付应用程序、桌面和计算机，还可管理关联的会话。以及应用程序和桌面配置，如策略和电源管理设置。
主机管理员	可以管理主机连接及其关联的资源设置。可以向用户交付计算机、应用程序或桌面。

  在某些产品版本中，您可以根据组织的要求创建自定义角色，并可以更细致地委派权限。您可以使用自定义角色按照控制台中操作或任务的粒度来分配权限。

- **作用域** - 一个作用域代表一个对象集合。作用域用来根据组织的具体情况将对象分组（例如，销售团队使用的交付组集合）。对象可以属于多个作用域；可以将对象视为带有多个作用域的标记。系统提供一个内置的作用域“全部”，其包含全部

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

对象。“完全权限管理员”角色始终与“全部”作用域配对。

示例

XYZ 公司决定根据部门（会计、销售和仓库）和桌面操作系统（Windows 7 或 Windows 8）来管理应用程序和桌面。 管理员创建了五个作用域，并分别为每个交付组标记了两个作用域：一个用于所用的部门，另一个用于所用的操作系统。

创建了以下管理员：

管理员	角色	作用域
domain/fred	完全权限 管理员	全部 （ 完全权限管理员角色始终拥有全部作用域）
domain/rob	只读 权限管理员	全部
domain/heidi	只读 权限管理员 技术 支持管理员	全部 销售
domain/warehouseadmin	技术 支持管理员	仓库
domain/peter	交付 组管理员 计算机 目录管理员	Win7

- Fred 是完全权限管理员，可以查看、编辑和删除系统中的所有对象。
- Rob 可以查看站点中的所有对象，但无法编辑和删除对象。
- Heidi 可以查看所有对象并可以对销售作用域中的交付组执行技术支持任务。 因此她可以管理与这些组关联的会话和计算机，但无法对交付组执行更改，例如添加或删除计算机。
- warehouseadmins Active Directory 安全组成员中的任何人都可以查看“仓库”作用域中的计算机，并对这些计算机执行技术支持任务。
- Peter 是 Windows 7 专员，可以管理所有 Windows 7 计算机目录，还可以交付 Windows 7 应用程序、桌面和计算机，无论它们属于哪个部门作用域。 管理员曾考虑让 Peter 成为 Win7 作用域的完全权限管理员；但是，她决定不这样做，因为完全权限管理员对不属于作用域范围的所有对象（例如“站点”和“管理员”）也具有完全权限。

如何使用委派管理

一般而言，管理员的数量及其权限的粒度取决于部署的规模和复杂性。

- 对于小型部署或概念验证部署，一个或几个管理员便足以完成一切工作，无需委派。 在这种情况下，创建每个管理员时使其具有内置“完全权限管理员”角色，该角色拥有“全部”作用域。
- 在包含较多计算机、应用程序和桌面的大型部署中，需要较多委派。 多个管理员的职责（角色）划分可能更为明确。 例如，两个为完全权限管理员，其他则是技术支持管理员。 另外，管理员可能只管理特定的对象组（作用域），例如计算机目录。 在这种情况下，创建新的作用域，并创建具有内置角色之一及适当作用域的管理员。
- 更大型的部署可能需要更多（或更明确）的作用域，以及具有非常规角色的不同管理员。 在这种情况下，编辑或创建更多作用域，创建自定义角色，并根据内置或自定义角色以及现有和新作用域创建每个管理员。

为实现配置灵活性和方便性，可以在创建管理员时创建新作用域。 另外，还可以在创建或编辑计算机目录或连接时指定作用域。

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

创建和管理管理员

以本地管理员身份创建站点时，您的用户帐户将自动成为对所有对象具有完全权限的“完全权限管理员”。 创建了站点后，本地管理员没有任何特殊权限。

完全权限管理员角色始终具有“全部”作用域，此作用域无法更改。

默认情况下，启用管理员。 如果现在要创建新管理员，但此人要在之后某个时间才开始履行管理员职责，则禁用管理员可能很有必要。 对于已启用的现有管理员，重新组织对象/作用域时，您可能需要禁用多个管理员，当准备启用更新配置时，再将其重新启用。 如果禁用某个完全权限管理员会导致没有启用的完全权限管理员，将不能禁用此管理员。 在创建、复制或编辑管理员时，启用/禁用复选框将处于可用状态。

在复制、编辑或删除管理员时，如果删除角色/作用域对，此操作将仅删除此管理员的角色与作用域之间的关系，而不会删除角色或作用域本身，也不会影响配置了此角色/作用域对的其他任何管理员。

要对管理员进行管理，请在 Studio 导航窗格中单击 配置 > 管理员，然后单击中上方窗格中的 管理员选项卡。

- 要创建管理员，请在“操作”窗格中单击 创建新管理员。 键入或浏览到用户帐户名称，选择或创建一个作用域并选择一个角色。 默认情况下，启用新管理员；可以对此进行更改。
- 要复制管理员，请在中间窗格中选择管理员，然后在“操作”窗格中单击 复制 管理员。 键入或浏览到用户帐户名称。 可以选择任何角色/作用域对，然后进行编辑或删除，也可以添加新的角色/作用域对。 默认情况下，启用新管理员；可以对此进行更改。
- 要编辑管理员，请在中间窗格中选择管理员，然后在“操作”窗格中单击 编辑 管理员。 可以编辑或删除任何角色/作用域对，也可以添加新的角色/作用域对。
- 要删除管理员，请在中间窗格中选择管理员，然后在“操作”窗格中单击 删除管理员。 如果删除某个完全权限管理员会导致没有启用的完全权限管理员，将不能删除此管理员。

创建和管理角色

角色名称最多可以包含 64 个 Unicode 字符，并且不能包含以下字符：\（反斜线）、/（正斜线）、;（分号）、:（冒号）、#（英镑符号）、,（逗号）、*（星号）、?（问号）、=（等号）、<（左箭头）、>（右箭头）、|（竖线）、[]（左右方括号）、()（左右圆括号）、"（引号）和 '（单引号）。 说明最多可以包含 256 个 Unicode 字符。

无法编辑和删除内置角色。 无法删除任意管理员正在使用的自定义角色。

注意：只有特定产品版本支持自定义角色。 不支持自定义角色的版本在“操作”窗格中没有相关条目。
要管理角色，请在 Studio 导航窗格中单击 配置 > 管理员，然后单击中上方窗格中的 角色选项卡。

- 要查看角色详细信息，请在中间窗格中选择角色。 中间窗格下方列出了角色的对象类型及关联权限。 在下方窗格中单击 管理员选项卡，以显示当前具有此角色的管理员列表。
- 要创建自定义角色，请在“操作”窗格中单击 创建新角色。 输入名称和说明。 选择对象类型和权限。
- 要复制角色，请在中间窗格中选择角色，然后在“操作”窗格中单击 复制 角色。 根据需要更改名称、说明、对象类型和权限。
- 要编辑自定义角色，请在中间窗格中选择角色，然后在“操作”窗格中单击 编辑 角色。 根据需要更改名称、说明、对象类型和权限。
- 要删除自定义角色，请在中间窗格中选择角色，然后在“操作”窗格中单击 删除角色。 出现提示时，确认删除。

创建和管理作用域

创建站点时，唯一可用的作用域是不能删除的“全部”作用域。

可以使用以下过程创建作用域。 也可以在创建管理员时创建作用域；每个管理员必须至少与一个角色和作用域对相关联。 创建或编辑桌面、计算机目录、应用程序或主机时，可将其添加到现有作用域；如果未将其添加到作用域，则它们仍是“全部”作用

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

域的一部分。

站点创建和委派管理员对象（作用域和角色）均无法归入作用域内。 但是，无法归入作用域内的对象可包含在“全部”作用域内。（具有完全权限的管理员始终具有“全部”作用域。）计算机、电源操作、桌面和会话不直接归入作用域；可通过相关的计算机目录或交付组为管理员分配对这些对象的权限。

作用域名称可包含最多 64 个 Unicode 字符，并且不能包含以下字符：\（反斜线）、/（正斜线）、;（分号）、:（冒号）、#（英镑符号）、,（逗号）、*（星号）、?（问号）、=（等号）、<（左箭头）、>（右箭头）、|（竖线）、[]（左右方括号）、()（左右圆括号）、"（引号）和 '（单引号）。 说明最多可以包含 256 个 Unicode 字符。

复制或编辑作用域时，请注意，从作用域中删除对象会导致管理员无法访问这些对象。 如果编辑的作用域与一个或多个角色配对，请确保对作用域所做的更新不会使任何角色/作用域对无法使用。

要管理作用域，请在 Studio 导航窗格中单击 配置 > 管理员，然后单击中上方窗格中的 作用域选项卡。

- 要创建作用域，请在“操作”窗格中单击 创建新作用域。 输入名称和说明。 要包括特定类型的所有对象（例如交付组），请选择对象类型。 要包括特定对象，请展开类型，然后选择各个对象（例如销售团队使用的交付组）。
- 要复制作用域，请在中间窗格中选择作用域，然后在“操作”窗格中单击 复制 作用域。 输入名称和说明。根据需要更改对象类型和对象。
- 要编辑作用域，请在中间窗格中选择作用域，然后在“操作”窗格中单击 编辑 作用域。 根据需要更改名称、说明、对象类型和对象。
- 要删除作用域，请在中间窗格中选择作用域，然后在“操作”窗格中单击 删除作用域。 出现提示时，确认删除。

创建报告

可以创建两种类型的委派管理报告：

- HTML 报告，此报告将列出与管理员关联的角色/作用域对以及每种对象类型（例如，交付组和计算机目录）的各个权限。通过 Studio 生成此报告。
  要创建 此报告，请在导航 窗格中单击 配置 > 管理员。在中间窗格中选择管理员，然后在“操作”窗格中单击 创建报告。

  您还可以在 创建、复制或编辑管理员时请求此报告。

- 将所有内置和自定义角色映射到权限的 HTML 或 CSV 报告。 通过运行名为 OutputPermissionMapping.ps1 的 PowerShell 脚本生成此报告。
  要运行此 脚本，您必须是完全权限管理员、只读权限管理员或具有读取角色权限的 自定义管理员。此脚本位于： Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts\。

  语法：

  OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path <string>] [-AdminAddress <string>] [-Show] [<CommonParameters>]

参数	说明
-Help	显示脚本帮助。
-Csv	指定 CSV 输出。默认值：HTML
-Path <string>	输出的写入位置。默认值：stdout
-	要连接的 Delivery Controller 的 IP 地址或主机名。 默认名称为 localhost

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

AdminAddress 参数 <string>	说明
-Show	（仅当也指定了 -Path 参数时此参数才有效）将输出写入文件时，-Show 会在相应的程序（例如 Web 浏览器）中打开此输出。
	Verbose、Debug、ErrorAction、ErrorVariable、 WarningAction、WarningVariable、OutBuffer 和 OutVariable。有关详细信息，请参阅 Microsoft 文档。

以下示例将 HTML 表写入到名为 Roles.html 的文件，并在 Web 浏览器中打开此表。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
-Path Roles.html –Show
```

以下示例将 CSV 表写入名为 Roles.csv 的文件。 不显示此表。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
–CSV -Path Roles.csv
```

在 Windows 命令提示窗口中，上例命令为：

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'
-CSV -Path Roles.csv"
```


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

智能卡

Dec 05, 2017

根据本文中介绍的指导原则，智能卡以及等效技术均受支持。要对 XenApp 或 XenDesktop 使用智能卡，请执行以下操作：

- 了解贵组织的与使用智能卡有关的安全策略。例如，这些策略可能说明如何颁发智能卡，以及用户应该如何保护这些智能卡。在 XenApp 或 XenDesktop 环境中，可能需要重新评估这些策略的某些方面。
- 确定要与智能卡结合使用的用户设备类型、操作系统和已发布的应用程序。
- 熟悉智能卡技术以及选定智能卡供应商提供的硬件和软件。
- 了解如何在分布式环境中部署数字证书。

智能卡类型

企业和使用者智能卡具有相同的尺寸和电连接器，并且适合相同的智能卡读卡器。

供企业使用的智能卡包含数字证书。这些智能卡支持 Windows 登录，并且还可以与应用程序结合使用以进行数字签名以及文档和电子邮件的加密。XenApp 和 XenDesktop 支持这些用法。

供使用者使用的智能卡不包含数字证书，但包含一个共享机密。这些智能卡可以支持付款（例如，签名支付或芯片密码信用卡）。这些智能卡不支持 Windows 登录或典型的 Windows 应用程序。需要对这些智能卡使用专用 Windows 应用程序和适用的软件基础结构（例如，包括与支付卡网络建立连接）。要了解与支持在 XenApp 或 XenDesktop 上使用这些专用应用程序有关的信息，请联系您的 Citrix 代表。

对于企业智能卡，这些是能够以相似的方式使用的兼容等效物。

- 与智能卡等效的 USB 令牌直接连接到 USB 端口。这些 USB 令牌通常与 U 盘大小相同，但可以像手机中使用的 SIM 卡一样小。这些令牌显示为智能卡与 USB 智能卡读卡器的组合。
- 使用 Windows 受信任的平台模块 (TPM) 的虚拟智能卡显示为智能卡。使用的最低 Citrix Receiver 版本为 4.3 的 Windows 8 和 Windows 10 支持这些虚拟智能卡。
  - 7.6 FP3 之前的 XenApp 和 XenDesktop 版本不支持虚拟智能卡。
  - 有关虚拟智能卡的详细信息，请参阅虚拟智能卡概览。

  注意：术语“虚拟智能卡”还用于描述完全存储在用户计算机上的数字证书。这些数字证书严格而言不等同于智能卡。

XenApp 和 XenDesktop 的智能卡支持基于 Microsoft 个人计算机/智能卡 (Microsoft Personal Computer/Smart Card, PC/SC) 标准规范。智能卡和智能卡设备必须受底层 Windows 操作系统支持，并且必须获得 Microsoft Windows Hardware Quality Labs (WHQL) 批准，可在运行合格 Windows 操作系统的计算机上使用，这是最低要求。有关硬件 PC/SC 合规性的其他信息，请参阅 Microsoft 文档。其他类型的用户设备可能遵守 PS/SC 标准。有关详细信息，请参阅 http://www.citrix.com/ready/ 上的 Citrix Ready 计划。

一般情况下，每个供应商的智能卡或等效物都需要独立的设备驱动程序。但是，如果智能卡遵守诸如 NIST 个人身份验证 (PIV) 标准等标准，则可以对一系列智能卡使用单个设备驱动程序。必须将设备驱动程序同时安装在用户设备和 Virtual Delivery Agent (VDA) 上。设备驱动程序通常作为 Citrix 合作伙伴提供的智能卡中间件软件包的一部分提供；智能卡中间件软件包将提供高级功能。此外，还可以将设备驱动程序描述为加密服务提供程序 (CSP)、密钥存储提供程序 (KSP) 或微型驱动程序。

以下适用于 Windows 系统的智能卡和中间件的组合作为各自类型的代表，已经通过 Citrix 的测试。但是，也可以使用其他智能卡和中间件。有关与 Citrix 兼容的智能卡和中间件的详细信息，请参阅 http://www.citrix.com/ready。

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

中间件	相配的卡
ActivClient 7.0（启用 DoD 模式）	DoD CAC 卡
处于 PIV 模式的 ActivClient 7.0	NIST PIV 卡
Microsoft 微型驱动程序	NIST PIV 卡
适用于 .NET 卡的 GemAlto 微型驱动程序	GemAlto .NET v2+
Microsoft 本机驱动程序	虚拟智能卡 (TPM)

有关对其他设备类型使用智能卡的信息，请参阅 Citrix Receiver 文档中与该设备有关的内容。有关在 XenDesktop 中使用 PIV 的详细信息，请参阅为 Citrix XenDesktop 7.6 和 NetScaler Gateway 10.5 配置 PIV 智能卡身份验证。

有关对其他设备类型使用智能卡的信息，请参阅 Citrix Receiver 文档中与该设备有关的内容。

Remote PC Access

仅在远程访问运行 Windows 10、Windows 8 或 Windows 7 的办公室物理 PC 时支持智能卡；运行 Windows XP 的办公室 PC 不支持智能卡。

以下智能卡已通过 Remote PC Access 进行测试：

中间件	相配的卡
Gemalto .NET 微型驱动程序	Gemalto .NET v2+
ActivIdentity ActivClient 6.2	NIST PIV
ActivIdentity ActivClient 6.2	CAC
Microsoft 微型驱动程序	NIST PIV
Microsoft 本机驱动程序	虚拟智能卡

智能卡读卡器类型

智能卡读卡器可能内置在用户设备中，或者单独连接到用户设备（通常通过 USB 或蓝牙进行连接）。支持遵守 USB 芯片/智能

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

卡接口设备 (CCID) 规范的接触式读卡器。这些读卡器包含用户可插入智能卡的插槽或刷槽。Deutsche Kreditwirtschaft (DK) 标准定义了四种类别的接触式读卡器。

- 类别 1 智能卡读卡器最常见，通常仅包含一个插槽。随操作系统提供的标准 CCID 设备驱动程序通常支持类别 1 智能卡读卡器。
- 类别 2 智能卡读卡器还包含一个用户设备无法访问的安全数字小键盘。类别 2 智能卡读卡器可能内置在具有集成的安全数字小键盘的键盘中。要了解与类别 2 智能卡读卡器有关的信息，请联系您的 Citrix 代表；可能需要安装读卡器特有的驱动程序，才能启用安全数字小键盘功能。
- 类别 3 智能卡读卡器还包含一个安全显示屏。不支持类别 3 智能卡读卡器。
- 类别 4 智能卡读卡器还包含一个安全的交易模块。不支持类别 4 智能卡读卡器。

注意：智能卡读卡器类别与 USB 设备类别无关。

智能卡读卡器必须随相应的设备驱动程序一起安装在用户设备上。

有关受支持的智能卡读卡器的信息，请参阅您正在使用的 Citrix Receiver 的文档。在 Citrix Receiver 文档中，支持的版本通常在智能卡一文或系统要求一文中列出。

用户体验

智能卡支持功能通过默认启用的特定 ICA/HDX 智能卡虚拟通道集成在 XenApp 和 XenDesktop 中。

重要：请勿对智能卡读卡器使用通用 USB 重定向。该功能默认对智能卡读卡器禁用，如果启用，则不受支持。

在同一个用户设备上可以使用多个智能卡和多个读卡器，但是，如果正在使用直通身份验证，当用户启动虚拟桌面或应用程序时必须仅插入一个智能卡。在应用程序中使用智能卡时（例如，为了实现数字签名或加密功能），可能会出现要求插入智能卡或输入 PIN 的其他提示。同时插入多个智能卡时可能会发生这种情况。

- 当智能卡已插入读卡器中，但仍提示插入智能卡时，应选择取消。
- 如果提示输入 PIN，则应重新输入 PIN。

如果将 Windows Server 2008 或 2008 R2 上运行的托管应用程序与需要安装 Microsoft 基本智能卡加密服务提供程序的智能卡一起使用，您可能会发现如果某个用户运行了智能卡事务，则其他所有正在使用智能卡登录的用户都将被阻止。有关更多详细信息和用于解决此问题的修补程序，请参阅 http://support.microsoft.com/kb/949538。

您可以使用卡管理系统或供应商实用程序重置 PIN。

> **Important**
>
> 在 XenApp 或 XenDesktop 会话中，不支持对 Microsoft 远程桌面连接应用程序使用智能卡。这有时称为“双跃点”用法。

部署智能卡之前的准备工作

- 获取智能卡读卡器的设备驱动程序，并将其安装到用户设备。许多智能卡读卡器可以使用 Microsoft 提供的 CCID 设备驱动程序。
- 从智能卡供应商处获取设备驱动程序和加密服务提供程序 (CSP) 软件，然后将其安装在用户设备和虚拟桌面上。驱动程序和

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

CSP 软件必须与 XenApp 和 XenDesktop 兼容；请查阅供应商的文档以了解兼容性。对于支持并使用微型驱动程序模型的智能卡的虚拟桌面，智能卡微型驱动程序应自动下载，但您也可以从http://catalog.update.microsoft.com或从供应商处获取。此外，如果需要 PKCS#11 中间件，请从卡供应商处获取。

- 重要：Citrix 建议您首先在物理机上安装并测试驱动程序和 CSP 软件，然后再安装 Citrix 软件。
- 在 Windows 10 上的 Internet Explorer 中，为使用智能卡的用户将 Citrix Receiver for Web URL 添加到可信站点列表中。在 Windows 10 中，Internet Explorer 默认情况下不会针对可信站点采用受保护模式运行。
- 确保正确配置了您的公钥基础结构 (PKI)。包括确保针对 Active Directory 环境正确配置了证书至帐户的映射，并且可以成功执行用户证书验证。
- 确保您的部署符合与智能卡结合使用的其他 Citrix 组件（包括 Citrix Receiver 和 StoreFront）的系统要求。
- 确保可以访问您站点中的以下服务器：
  - 与智能卡上的登录证书相关联的用户帐户的 Active Directory 域控制器
  - Delivery Controller
  - Citrix StoreFront
  - Citrix NetScaler Gateway/Citrix Access Gateway 10.x
  - VDA
  - （对于 Remote PC Access 可选）：Microsoft Exchange Server

支持使用智能卡

步骤 1. 根据智能卡颁发策略向用户颁发智能卡。

步骤 2. （可选）设置智能卡以使用户能够启用 Remote PC Access。

步骤 3. 安装并配置 Delivery Controller 和 StoreFront（如果尚未安装）以实现智能卡远程连接。

步骤 4. 启用 StoreFront 以使用智能卡。有关详细信息，请参阅 StoreFront 文档中的配置智能卡身份验证。

步骤 5. 启用 NetScaler Gateway/Access Gateway 以使用智能卡。有关详细信息，请参阅 NetScaler 文档中的配置身份验证和授权及通过 Web Interface 配置智能卡访问权限。

步骤 6. 启用 VDAs 以使用智能卡。

- 确保 VDA 具有必需的应用程序和更新。
- 安装中间件。
- 设置智能卡远程连接功能，在用户设备上的 Citrix Receiver 与虚拟桌面会话之间启用智能卡数据的通信。

步骤 7. 使用户设备（包括加入域的计算机或未加入域的计算机）支持使用智能卡。有关详细信息，请参阅 StoreFront 文档中的配置智能卡身份验证。

- 向设备的密钥库中导入证书颁发机构根证书和颁发的证书颁发机构证书。
- 安装您的供应商提供的智能卡中间件。
- 安装并配置 Citrix Receiver for Windows，确保通过使用组策略管理控制台来导入 icaclient.adm 并启用智能卡身份验证。

步骤 8. 测试部署。使用测试用户的智能卡启动虚拟桌面，来确保已正确配置您的部署。测试所有可能的访问机制（例如，通过 Internet Explorer 和 Citrix Receiver 访问桌面）。

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

智能卡部署

Dec 05, 2017

本产品版本和包含本版本的混合环境支持下列类型的智能卡部署。其他配置可能可以运行，但不受支持。

类型	StoreFront 连接
加入本地域的计算机	直接连接
从加入域的计算机远程访问	通过 NetScaler Gateway 连接
未加入域的计算机	直接连接
从未加入域的计算机远程访问	通过 NetScaler Gateway 连接
访问桌面设备站点的未加入域的计算机和瘦客户端	通过桌面设备站点连接
通过 XenApp Services URL 访问 StoreFront 的加入域的计算机和瘦客户端	通过 XenApp Services URL 连接

部署类型由智能卡读卡器连接到的用户设备的以下特性定义：

- 设备是否已加入域。
- 设备连接到 StoreFront 的方式。
- 查看虚拟桌面和应用程序使用的软件。

此外，启用智能卡的应用程序（如 Microsoft Word 和 Microsoft Excel）也可在这些部署中使用。这些应用程序允许用户对文档进行数字签名或加密。

双模式身份验证

在其中的每个部署中，如有可能，Receiver 支持 双模式身份验证，允许用户在使用智能卡和输入其用户名和密码之间进行选择。 如果无法使用智能卡（例如，用户将智能卡遗忘在家中或登录证书已过期），此功能会很有用。

由于未加入域的设备的用户将直接登录到 Receiver for Windows，因此，您可以允许用户回退至显式身份验证。 如果您配置双模式身份验证，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。

如果您部署 NetScaler Gateway，则用户登录到设备后，Receiver for Windows 会提示用户完成 NetScaler Gateway 的身份验证。 对于加入域的设备和未加入域的设备均是如此。 用户可以使用智能卡和 PIN 或使用显式凭据登录到 NetScaler Gateway。 这样，您可以向用户提供 NetScaler Gateway 登录的双模式身份验证。 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。

多个 Active Directory 林注意事项

在 Citrix 环境中，在单个林中支持智能卡。 跨林进行智能卡登录要求对所有用户帐户启用直接双向林信任。 不支持涉及智能卡的更加复杂的多林部署（即，其中的信任仅为单向信任或具有不同的类型）。

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

可以在包括远程桌面的 Citrix 环境中使用智能卡。 可以在本地（在智能卡连接的用户设备上）或远程（在用户设备连接的远程桌面上）安装此功能。

智能卡移除策略

在产品上设置的智能卡移除策略用于确定当在会话期间从读卡器中移除智能卡时所发生的操作。 智能卡移除策略通过 Windows 操作系统进行配置，并且也由 Windows 操作系统来处理。

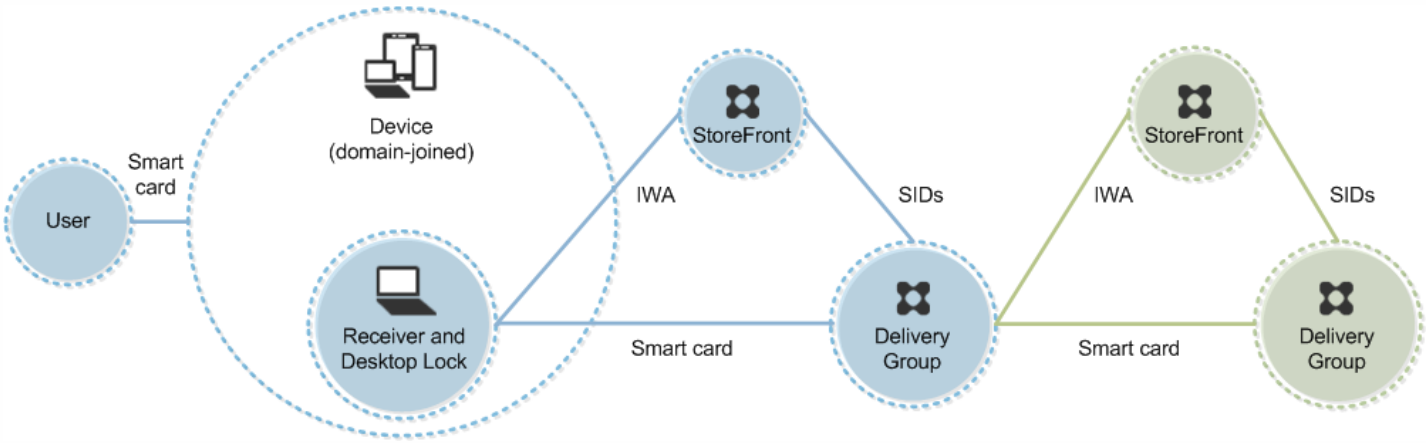
策略设置	桌面行为
无操作	不采取任何措施。
锁定工作站	桌面会话断开连接，并锁定虚拟桌面。
强制注销	将强制用户注销。如果网络连接已断开，并启用了此设置，则可能会注销会话，用户可能会丢失数据。
如果是远程终端服务会话，则断开连接	会话断开连接，并锁定虚拟桌面。

证书吊销检查

如果启用证书吊销检查，并且用户将具有无效证书的智能卡插入读卡器，用户将无法对与该证书相关的桌面或应用程序进行身份验证或访问。 例如，如果使用无效证书进行电子邮件解密，电子邮件将保持加密状态。 如果卡上的其他证书（例如，用于身份验证的证书）仍有效，这些功能将仍有效。

部署示例：加入域的计算机

此部署涉及运行 Desktop Viewer 并直接连接到 StoreFront 的已加入域的用户设备。



用户使用智能卡和 PIN 登录设备。Receiver 使用集成 Windows 身份验证 (IWA) 向 StoreFront 服务器进行用户身份验证。 StoreFront 将用户安全标识符 (SID) 传递到 XenApp 或 XenDesktop。 当用户启动虚拟桌面或应用程序时，系统不会提示用户重新输入 PIN，因为 Receiver 上已配置单点登录功能。

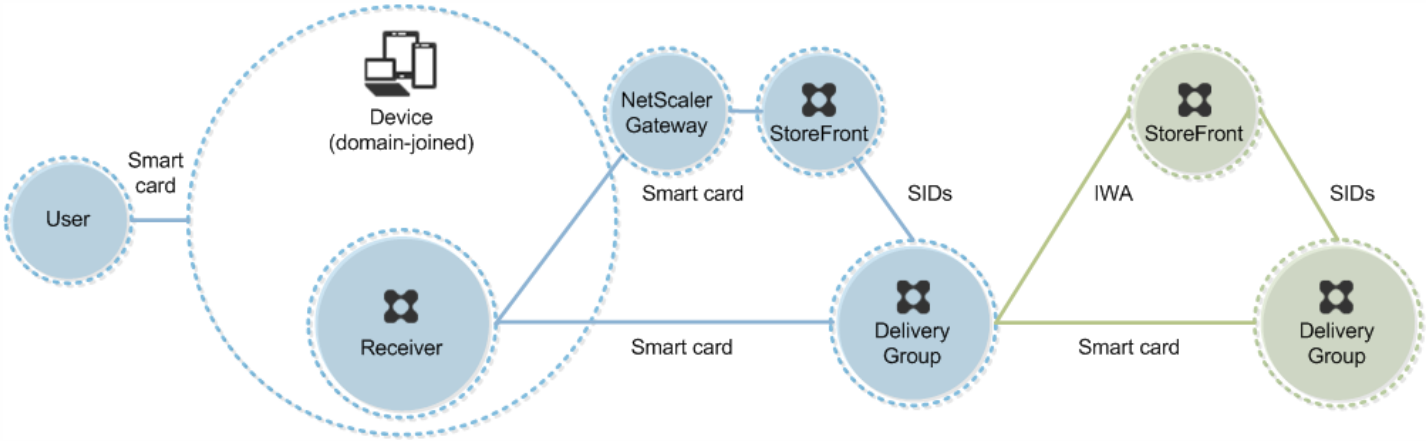
通过添加第二台 StoreFront 服务器和托管应用程序的服务器，此部署可以扩展到双跳。 虚拟桌面中的 Receiver 对第二台 StoreFront 服务器进行身份验证。 第二次连接时，可以使用任何身份验证方法。 第一个跃点显示的配置可在第二个跃点中重

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

复使用，也可以只在第二个跃点中使用。

部署示例：从加入域的计算机进行远程访问

此部署涉及运行 Desktop Viewer 并通过 NetScaler Gateway/Access Gateway 连接到 StoreFront 的已加入域的用户设备。



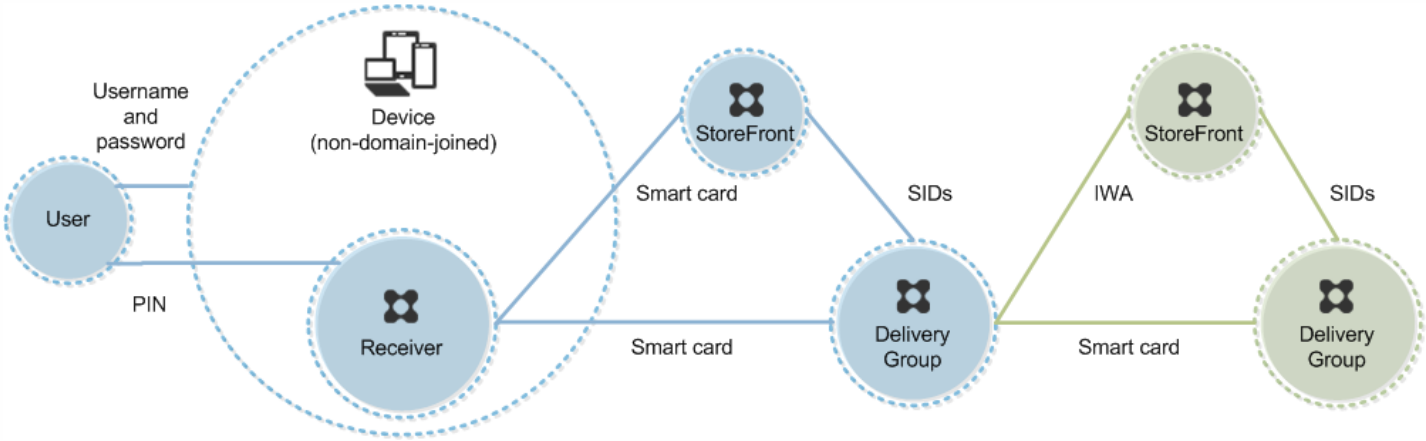
用户使用智能卡和 PIN 登录设备，然后重新登录到 NetScaler Gateway/Access Gateway。 第二次登录可以使用智能卡和 PIN，也可以使用用户名和密码，因为在此部署中 Receiver 允许双模式身份验证。

用户自动登录 StoreFront，将用户安全标识符 (SID) 传递到 XenApp 或 XenDesktop。 当用户启动虚拟桌面或应用程序时，系统不会提示用户重新输入 PIN，因为 Receiver 上已配置单点登录功能。

通过添加第二台 StoreFront 服务器和托管应用程序的服务器，此部署可以扩展到双跳。 虚拟桌面中的 Receiver 对第二台 StoreFront 服务器进行身份验证。 第二次连接时，可以使用任何身份验证方法。 第一个跃点显示的配置可在第二个跃点中重复使用，也可以只在第二个跃点中使用。

部署示例：未加入域的计算机

此部署涉及运行 Desktop Viewer 并直接连接到 StoreFront 的未加入域的用户设备。



用户登录设备。通常情况下，用户需要输入用户名和密码，但由于此设备未加入域，因此此登录的凭据是可选的。 因为在此部署中可使用双模式身份验证，因此 Receiver 会提示用户输入智能卡和 PIN，或使用用户名和密码。 然后 Receiver 对 StoreFront 进行身份验证。

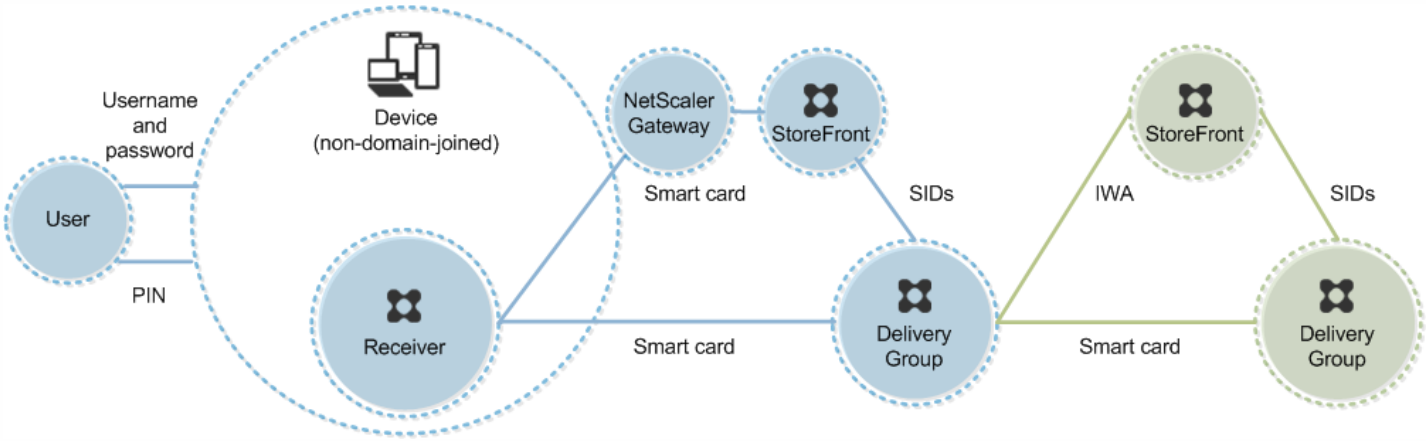
© 1999-2017 Citrix Systems, Inc. All rights reserved.

StoreFront 将用户安全标识符 (SID) 传递到 XenApp 或 XenDesktop。 当用户启动虚拟桌面或应用程序时，系统会提示用户重新输入 PIN，因为在此部署中未提供单点登录功能。

通过添加第二台 StoreFront 服务器和托管应用程序的服务器，此部署可以扩展到双跳。 虚拟桌面中的 Receiver 对第二台 StoreFront 服务器进行身份验证。 第二次连接时，可以使用任何身份验证方法。 第一个跃点显示的配置可在第二个跃点中重复使用，也可以只在第二个跃点中使用。

部署示例：从未加入域的计算机进行远程访问

此部署涉及运行 Desktop Viewer 并直接连接到 StoreFront 的未加入域的用户设备。



用户登录设备。通常情况下，用户需要输入用户名和密码，但由于此设备未加入域，因此此登录的凭据是可选的。 因为在此部署中可使用双模式身份验证，因此 Receiver 会提示用户输入智能卡和 PIN，或使用用户名和密码。 然后 Receiver 对 StoreFront 进行身份验证。

StoreFront 将用户安全标识符 (SID) 传递到 XenApp 或 XenDesktop。 当用户启动虚拟桌面或应用程序时，系统会提示用户重新输入 PIN，因为在此部署中未提供单点登录功能。

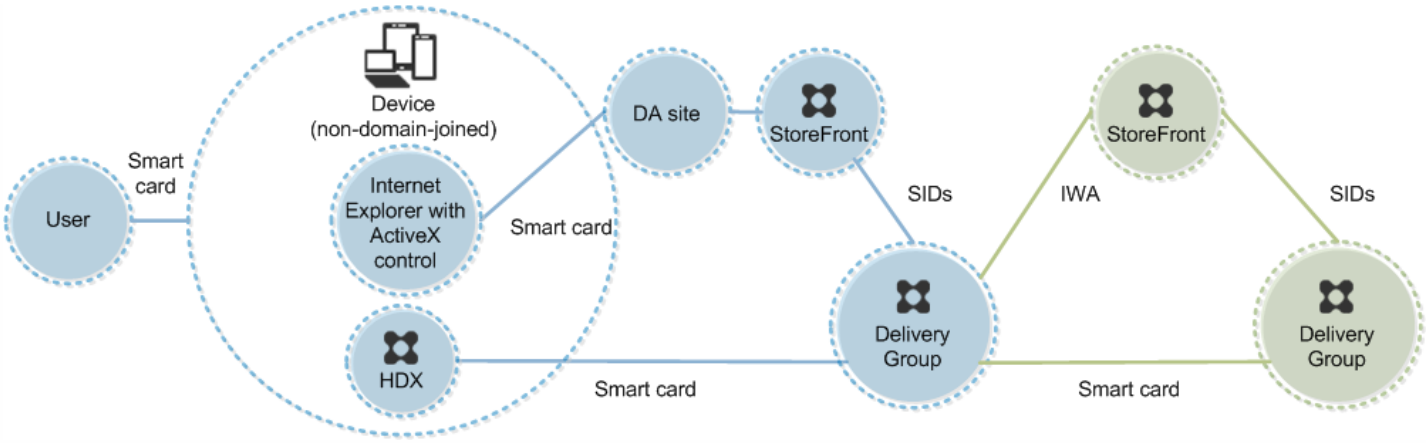
通过添加第二台 StoreFront 服务器和托管应用程序的服务器，此部署可以扩展到双跳。 虚拟桌面中的 Receiver 对第二台 StoreFront 服务器进行身份验证。 第二次连接时，可以使用任何身份验证方法。 第一个跃点显示的配置可在第二个跃点中重复使用，也可以只在第二个跃点中使用。

部署示例：未加入域的计算机和瘦客户端访问桌面设备站点

此部署涉及运行 Desktop Lock，并通过桌面设备站点连接到 StoreFront 的未加入域的用户设备。

Desktop Lock 是随 XenApp、XenDesktop 和 VDI-in-a-Box 一起发布的独立组件。 它是 Desktop Viewer 的替代项，主要是针对重新设计用途的 Windows 计算机和 Windows 瘦客户端而设计的。 Desktop Lock 取代了这些用户设备中的 Windows shell 和任务管理器，以阻止用户访问基础设备。 通过使用 Desktop Lock，用户可以访问 Windows Server 计算机桌面和 Windows 桌面计算机桌面。 可以选择安装 Desktop Lock。

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



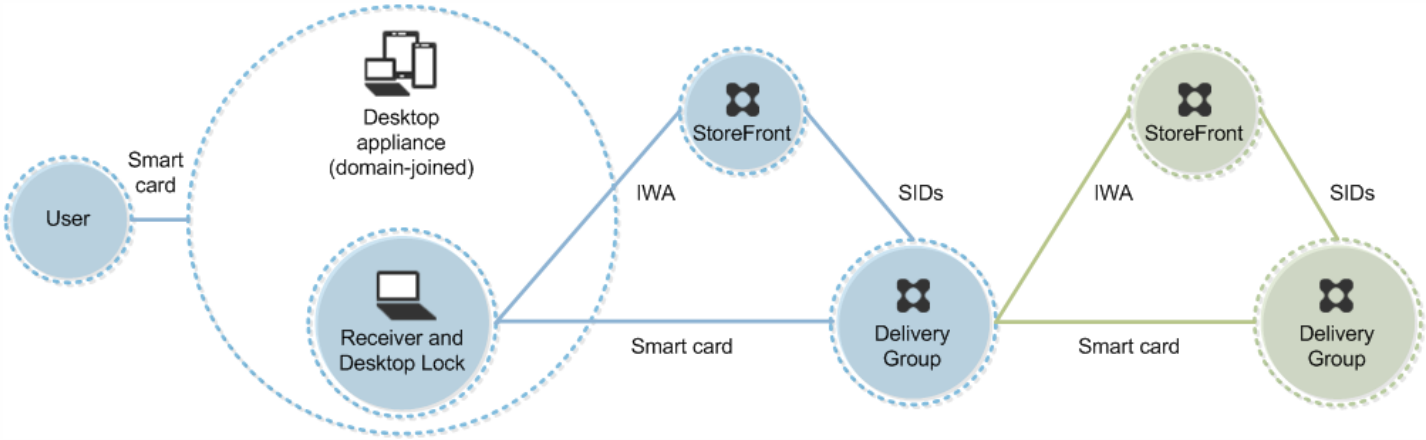
用户使用智能卡登录设备。如果 Desktop Lock 正在设备上运行，该设备配置为通过在 Kiosk 模式下运行的 Internet Explorer 启动桌面设备站点。 该站点上的 ActiveX 控件会提示用户输入 PIN，然后将其发送到 StoreFront。 StoreFront 将用户安全标识符 (SID) 传递到 XenApp 或 XenDesktop。 分配的桌面组列表（按字母顺序）中的第一个可用桌面将启动。

通过添加第二台 StoreFront 服务器和托管应用程序的服务器，此部署可以扩展到双跳。 虚拟桌面中的 Receiver 对第二台 StoreFront 服务器进行身份验证。 第二次连接时，可以使用任何身份验证方法。 第一个跃点显示的配置可在第二个跃点中重复使用，也可以只在第二个跃点中使用。

部署示例：加入域的计算机和瘦客户端通过 XenApp Services URL 访问 StoreFront

此部署涉及运行 Desktop Lock 并通过 XenApp Services URL 连接到 StoreFront 的加入域的用户设备。

Desktop Lock 是随 XenApp、XenDesktop 和 VDI-in-a-Box 一起发布的独立组件。 它是 Desktop Viewer 的替代项，主要是针对重新设计用途的 Windows 计算机和 Windows 瘦客户端而设计的。 Desktop Lock 取代了这些用户设备中的 Windows shell 和任务管理器，以阻止用户访问基础设备。 通过使用 Desktop Lock，用户可以访问 Windows Server 计算机桌面和 Windows 桌面计算机桌面。 可以选择安装 Desktop Lock。



用户使用智能卡和 PIN 登录设备。如果 Desktop Lock 正在设备上运行，它会使用集成 Windows 身份验证 (IWA) 向 StoreFront 服务器进行用户身份验证。 StoreFront 将用户安全标识符 (SID) 传递到 XenApp 或 XenDesktop。 当用户启动虚拟桌面时，系统不会提示用户重新输入 PIN，因为 Receiver 上已配置单点登录功能。

通过添加第二台 StoreFront 服务器和托管应用程序的服务器，此部署可以扩展到双跳。 虚拟桌面中的 Receiver 对第二台 StoreFront 服务器进行身份验证。 第二次连接时，可以使用任何身份验证方法。 第一个跃点显示的配置可在第二个跃点中重复使用，也可以只在第二个跃点中使用。

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

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

使用智能卡进行直通身份验证和单点登录

Dec 05, 2017

直通身份验证

运行 Windows 10、Windows 8 和 Windows 7 SP1 Enterprise Edition 和 Professional Edition 的用户设备支持使用智能卡对虚拟桌面进行直通身份验证。

运行 Windows Server 2016、Windows Server 2012 R2、Windows Server 2012 和 Windows Server 2008 R2 SP1 的服务器支持使用智能卡对托管应用程序进行直通身份验证。

要使用智能卡对托管应用程序进行直通身份验证，请确保在配置使用智能卡进行直通身份验证作为站点的身份验证方法时启用 Kerberos。

注意：使用智能卡进行直通身份验证的可用性取决于许多因素，包括但不限于以下因素：

- 贵组织关于直通身份验证的安全策略。
- 中间件类型和配置。
- 智能卡读卡器类型。
- 中间件 PIN 缓存策略。

Citrix StoreFront 上已配置使用智能卡进行直通身份验证。有关详细信息，请参阅 StoreFront 文档。

单点登录

单点登录是一项 Citrix 功能，用于实现对虚拟桌面和应用程序启动的直通身份验证。 可以在加入域的直接访问 StoreFront 以及加入域的通过 NetScaler 访问 StoreFront 智能卡部署中使用此功能，以减少用户输入其 PIN 的次数。 要在这些部署类型中使用单点登录，请在 default.ica 文件（位于 StoreFront 服务器上）中编辑以下参数：

- 加入域的直接访问 StoreFront 智能卡部署 - 将 DisableCtrlAltDel 设置为 Off
- 加入域的通过 NetScaler 访问 StoreFront 智能卡部署 - 将 UseLocalUserAndPassword 设置为 On

有关设置这些参数的更多说明，请参阅 StoreFront 或 NetScaler Gateway 文档。

单点登录功能的可用性取决于多种因素，包括但不限于以下因素：

- 您的组织关于单点登录的安全策略。
- 中间件类型和配置。
- 智能卡读卡器类型。
- 中间件 PIN 缓存策略。

注意：如果用户在连接了智能卡读卡器的计算机上登录到 Virtual Delivery Agent (VDA)，可能会显示一个 Windows 头像，表示上一次成功的身份验证模式，如智能卡或密码。 因此，当启用单点登录时，可能会显示单点登录头像。 要登录，用户必须选择切换用户以选择另一个头像，因为单点登录头像不起作用。

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

传输层安全性 (TLS)

Jan 05, 2018

将 XenApp 或 XenDesktop 站点配置为使用传输层安全性 (TLS) 协议包括以下过程：

- 获取服务器证书并在所有 Delivery Controller 上安装和注册，并使用 TLS 证书配置端口。有关详细信息，请参阅在 Controller 上安装 TLS 服务器证书。
  （可选）可以更改 Controller 用于侦听 HTTP 和 HTTPS 流量的端口。

- 通过完成以下任务在用户和 Virtual Delivery Agents (VDA) 之间启用 TLS 连接：
  - 在安装 VDA 的计算机上配置 TLS。（方便起见，后面将安装 VDA 的计算机简称为 VDA。）可以使用 Citrix 提供的 PowerShell 脚本，也可以手动配置。有关常见信息，请参阅关于 VDA 上的 TLS 设置。有关详细信息，请参阅使用 PowerShell 脚本在 VDA 上配置 TLS 和在 VDA 上手动配置 TLS。
  - 通过在 Studio 中运行一组 PowerShell cmdlet，在包含 VDA 的交付组中配置 TLS。有关详细信息，请参阅在交付组上配置 TLS。

  要求和注意事项：
  - 在用户和 VDA 之间启用 TLS 连接仅对 XenApp 7.6 和 XenDesktop 7.6 及后续受支持的版本有效。
  - 在安装组件、创建站点、创建计算机目录和创建交付组之后，在交付组中和 VDA 上配置 TLS。
  - 要在交付组中配置 TLS，必须具有更改 Controller 访问规则的权限。完全权限管理员具有此权限。
  - 要在 VDA 上配置 TLS，必须是安装 VDA 的计算机上的 Windows 管理员。
  - 如果打算在从早期版本升级的 VDA 上配置 TLS，请在升级之前卸载这些计算机上的 SSL Relay 软件。
  - PowerShell 脚本在静态 VDA 上配置 TLS，不会在通过 Machine Creation Services 或 Provisioning Services 置备的池 VDA 上配置 TLS。对于第二种情况，计算机映像在每次重新启动时重置。

> **警告**
>
> 有关涉及在 Windows 注册表中操作的任务 - 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。

有关为站点数据库启用 TLS 的信息，请参阅 CTX137556。

> **注意**
>
> 如果同时在 VDA 上启用了 TLS 和 UDT：
>
> - 如果直接访问 VDA，Citrix Receiver 将始终使用 TLS over TCP（而非 UDP 和 UDT）。
> - 如果使用 NetScaler Gateway 间接访问 VDA，Citrix Receiver 将使用 DTLS over UDP 与 NetScaler Gateway 进行通信。NetScaler Gateway 与 VDA 之间的通信使用 UDP，但不使用 DTLS。使用 UDT。

在 Controller 上安装 TLS 服务器证书

对于 HTTPS，XML Service 通过使用服务器证书而非客户端证书来支持 TLS 功能。要获取证书并在 Controller 上进行安装和注册，以及使用 TLS 证书配置端口，请遵循以下操作：

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

如果 Controller 中安装了 IIS，请按照 https://technet.microsoft.com/zh-cn/library/cc771438%28v=ws.10%29.aspx 中的指南操作。

如果控制器中未安装 IIS，配置证书的其中一种方法是：

1. 按照 http://blogs.technet.com/b/pki/archive/2009/08/05/how-to-create-a-web-server-ssl-certificate-manually.aspx 中所述获取 TLS 服务器证书并将其安装在 Controller 上。有关 certreq 工具的详细信息，请参阅 http://technet.microsoft.com/en-us/library/cc736326(WS.10).aspx。
   如果打算使用 PowerShell 脚本在 VDA 上配置 TLS，请确保证书位于证书存储的“本地计算机”>“个人”>“证书”区域，除非您打算指定 TLS 证书的指纹。如果多个证书位于此位置，将使用找到的第一个证书。
2. 使用证书配置端口；请参阅 http://msdn.microsoft.com/zh-cn/library/ms733791%28v=vs.110%29.aspx。

如果在 Windows Server 2016 上安装了 Controller，同时在 Windows Server 2012 上安装了 StoreFront，则需要对该 Controller 进行配置更改，以更改 TLS 密码套件的顺序。

> **注意**
>
> 具有其他 Windows Server 版本组合的 Controller 和 StoreFront 不需要此配置更改。

密码套件顺序列表应包括 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 和/或 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 密码套件，同时这些密码套件必须位于任何 TLS_DHE_ 密码套件之前。

> **注意**
>
> Windows Server 2012 不支持 GCM 密码套件 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 和 TLS_ECDHE_RSA_WITH_AES_128_GCM _SHA256。

1. 使用 Microsoft 组策略编辑器，浏览至“计算机配置”>“管理模板”>“网络”>“SSL 配置设置”。
2. 编辑策略“SSL 密码套件顺序”。默认情况下此策略被设置为“未配置”。将此策略设为“启用”。
3. 按正确的顺序安排套件，删除任何不需要使用的密码套件。

确保 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 或 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 位于任何 TLS_DHE_ 密码套件之前。

在 Microsoft MSDN 上，另请参阅 Schannel 密码套件优先级划分。

更改 HTTP 或 HTTPS 端口

默认情况下，Controller 上的 XML Service 在端口 80 上侦听 HTTP 流量，在端口 443 上侦听 HTTPS 流量。尽管可以使用非默认端口，但请注意：将 Controller 暴露在不受信任的网络上存在安全风险。部署独立 StoreFront 服务器比更改默认值更可取。

要更改 Controller 使用的默认 HTTP 或 HTTPS 端口，请从 Studio 运行以下命令：

BrokerService.exe -WIPORT <*http-port*> -WISSLPORT <*https-port*>

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

其中，<*http-port*> 是用于 HTTP 流量的端口号，<*https-port*> 是用于 HTTPS 流量的端口号。

> ### 注意
>
> 更改端口后，Studio 可能会显示关于许可证兼容性和升级的消息。要解决此问题，请使用以下 PowerShell cmdlet 序列重新注册服务实例：
>
> Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS |
>
> Unregister-ConfigRegisteredServiceInstance
>
> Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |
> Register-ConfigServiceInstance

仅会强制执行 HTTPS 流量

如果希望 XML Service 忽略默认端口上的 HTTP 流量，请在 Controller 上的 HKLM\Software\Citrix\DesktopServer\ 中创建以下注册表设置，然后重新启动 Broker Service。

要忽略 HTTP 流量，请创建 DWORD XmlServicesEnableNonSsl 并将其设置为 0。

提供了一个能够创建的用于忽略 HTTPS 流量的相应注册表 DWORD 值：DWORD XmlServicesEnableSsl。请确保未将其设置为 0。

VDA 上的 TLS 设置

交付组不能既包含已配置 TLS 的 VDA 又包含未配置 TLS 的 VDA。为交付组配置 TLS 时，应该已经为该交付组中的所有 VDA 配置 TLS

在 VDA 上配置 TLS 时，已安装 TLS 证书上的权限会被更改，向 ICA Service 授予读取证书私钥的权限，并向 ICA Service 告知以下信息：

- **证书存储中用于 TLS 的证书**。
- **用于 TLS 连接的 TCP 端口号**。

必须将 Windows 防火墙（如果启用）配置为允许此 TCP 端口上的传入连接。使用 PowerShell 脚本时会完成此配置。

- **允许的 TLS 协议版本。**

> ### Important
>
> Citrix 建议您查看您的 SSLv3 使用情况，并在适当的情况下重新配置那些部署以删除对 SSLv3 的支持。请参阅 CTX200238。

支持的 TLS 协议版本遵循以下层次结构（从最低到最高）：SSL 3.0、TLS 1.0、TLS 1.1 和 TLS 1.2。指定允许的最低版本；将允许使用此版本或更高版本的所有协议连接。

例如，如果指定 TLS 1.1 作为最低版本，则允许 TLS 1.1 和 TLS 1.2 协议连接。如果指定 SSL 3.0 作为最低版本，则允许所

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

有受支持版本的连接。如果指定 TLS 1.2 作为最低版本，则仅允许 TLS 1.2 连接。

- **允许的 TLS 密码套件。**

  密码套件选择将用于连接的加密。客户端和 VDA 可以支持不同的密码套件组。客户端（Citrix Receiver 或 StoreFront）连接并发送支持的 TLS 密码套件列表，VDA 将客户端的密码套件之一与其自己的配置密码套件列表中的密码套件之一进行匹配，并接受连接。如果没有匹配的密码套件，VDA 将拒绝连接。

  VDA 支持三组密码套件（也称为合规性模式）：GOV(ernment)、COM(mercial) 及 ALL。可接受的密码套件还取决于 Windows FIPS 模式；有关 Windows FIPS 模式的信息，请参阅 http://support.microsoft.com/kb/811833。下表列出了每组中的密码套件：

TLS 密码套件	GOV	COM	全部	GOV	COM	全部
FIPS 模式	关	关	关	开	开	开
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	x		x	x		x
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	x		x	x		x
TLS_RSA_WITH_AES_256_GCM_SHA384	x		x	x		x
TLS_RSA_WITH_AES_128_GCM_SHA256	x	x	x	x	x	x
TLS_RSA_WITH_AES_256_CBC_SHA256	x		x	x		x
TLS_RSA_WITH_AES_256_CBC_SHA	x		x	x		x
TLS_RSA_WITH_AES_128_CBC_SHA		x	x		x	x
TLS_RSA_WITH_RC4_128_SHA		x	x			
TLS_RSA_WITH_RC4_128_MD5		x	x			
TLS_RSA_WITH_3DES_EDE_CBC_SHA	x		x	x		x

Important

VDA 在 Windows Server 2012 R2、Windows Server 2016 或者 Windows 10 Anniversary Edition 或支持的更高版本上时，需要执行额外的步骤。这影响来自 Citrix Receiver for Windows（版本 4.6 到 4.9）、Citrix Receiver for HTML5 以及 Citrix Receiver for Chrome 的连接。其中也包括通过 NetScaler Gateway 建立的连接。

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

对于使用 NetScaler Gateway 的所有连接以及所有 VDA 版本（如果在 NetScaler Gateway 与 VDA 之间配置了 TLS），也需要执行此步骤。这影响所有 Citrix Receiver 版本。

在 VDA（Windows Server 2016 或 Windows 10 Anniversary Edition 或更高版本）上，使用组策略编辑器，转到“计算机配置”>“管理模板”>“网络”>“SSL 配置设置”>“SSL 密码套件顺序”。选择以下顺序：

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA

注意

前四项还指定椭圆曲线 P384 或 P256。请确保未选择 "curve25519"。FIPS 模式不会阻止使用 curve25519。

配置了此组策略设置时，VDA 将仅选择同时显示在两个列表中的密码套件：组策略列表和选定合规性模式列表（COM、GOV 或 ALL）。该密码套件还必须显示在客户端（Citrix Receiver 或 StoreFront）发送的列表中。

此组策略配置还影响 VDA 上的其他 TLS 应用程序和服务。如果您的应用程序要求使用特定的密码套件，您可能需要将它们添加到此组策略列表中。

Important

尽管组策略更改一旦应用便会显示，但对 TLS 配置的组策略更改只有在重新启动操作系统后才会生效。因此，对于池桌面，请将对 TLS 配置的组策略更改应用于基础映像。

使用 PowerShell 脚本在 VDA 上配置 TLS

Enable-VdaSSL.ps1 脚本可在 VDA 上启用或禁用 TLS 侦听器。此脚本位于安装介质上的“Support”（支持）>“Tools”（工具）>“SslSupport”文件夹中。

启用 TLS 时，此脚本为指定的 TCP 端口禁用现有的所有 Windows 防火墙规则，然后添加新规则以允许 ICA Service 仅接受 TLS TCP 端口上的传入连接。它还为以下各项禁用 Windows 防火墙规则：

- Citrix ICA（默认：1494）
- Citrix CGP（默认：2598）
- Citrix WebSocket（默认：8008）

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

产生的影响为用户只能使用 TLS；在不使用 TLS 的情况下，不能使用 ICA/HDX、启用了会话可靠性的 ICA/HDX 或采用 WebSocket 的 HDX。

请参阅网络端口。

此脚本包含以下语法描述以及额外的示例；可以使用 Notepad++ 等工具查看此信息。

> **Important**
>
> 指定 Enable 或 Disable 参数以及 CertificateThumbPrint 参数。其他参数为可选参数。

语法

```
Enable-VdaSSL {-Enable | -Disable} -CertificateThumbPrint ""
[–SSLPort ] [-SSLMinVersion ""] [-SSLCipherSuite""]
```

Parameter	Description
启用	在 VDA 上安装并启用 TLS 侦听器。此参数或 Disable 参数为必需参数。
禁用	在 VDA 上禁用 TLS 侦听器。此参数或 Enable 参数为必需参数。如果指定此参数，其他参数均无效。
CertificateThumbPrint ""	证书存储中 TLS 证书的指纹，两边用引号引起。脚本使用指定的指纹来选择要使用的证书。此参数为必需参数；否则，将选择错误的证书。
SSLPort	TLS 端口。默认值：443
SSLMinVersion ""	最低 TLS 协议版本，两边用引号引起。有效值包括： • "SSL_3.0" • "TLS_1.0" • "TLS_1.1" • "TLS_1.2" 默认值："TLS_1.0" **重要：**Citrix 建议客户查看其 SSLv3 的使用情况，并在适当的情况下重新配置其部署以删除对 SSLv3 的支持。请参阅 CTX200238。
SSLCipherSuite ""	TLS 密码套件，两边用引号引起。有效值包括： • "GOV" • "COM" • "ALL" 默认值："ALL"

示例

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

以下脚本安装并启用 TLS 1.2 协议版本值。指纹（在此示例中以 12345678987654321 表示）用于选择要使用的证书。

```
Enable-VdaSSL –Enable -CertificateThumbPrint "12345678987654321"
```

以下脚本安装并启用 TLS 侦听器，指定 TLS 端口 400、GOV 密码套件和最低 TLS 1.2 协议值。指纹（在此示例中以 12345678987654321 表示）用于选择要使用的证书。

```
Enable-VdaSSL – Enable
-CertificateThumbPrint "12345678987654321"
–SSLPort 400 'SSLMinVersion "TLS_1.2"
–SSLCipherSuite "GOV"
```

以下脚本在 VDA 上禁用 TLS 侦听器。

```
Enable-VdaSSL –Disable
```

在 VDA 上手动配置 TLS

在 VDA 上手动配置 TLS 时，可以向各个 VDA 上的相应服务授予 TLS 证书私钥的一般读取权限：NT SERVICE\PorticaService（适用于 VDA for Windows Desktop OS）或者 NT SERVICE\TermService（适用于 VDA for Windows Server OS）。在安装 VDA 的计算机上：

步骤 1. 启动 Microsoft 管理控制台 (MMC)：“开始”>“运行”> mmc.exe。

步骤 2. 将证书管理单元添加到 MMC：

1. 选择文件 > 添加/删除管理单元。
2. 选择证书，然后单击添加。
3. 收到“该管理单元将始终为下列帐户管理证书:”提示时，选择“计算机帐户”，然后单击“下一步”。
4. 收到“请选择需要这个管理单元管理的计算机”提示时，选择“本地计算机”，然后单击“完成”。

步骤 3. 在“证书(本地计算机)”>“个人”>“证书”下，在证书上单击鼠标右键，然后选择所有任务 > 管理私钥。

步骤 4. 访问控制列表编辑器显示“(友好名称)私钥的权限”，其中，(友好名称) 是 TLS 证书的名称。添加以下其中一项服务并向其授予读取权限：

- 对于 VDA for Windows Desktop OS："PORTICASERVICE"
- 对于 VDA for Windows Server OS："TERMSERVICE"

步骤 5. 双击已安装的 TLS 证书。在证书对话框中，选择“详细信息”选项卡，然后滚动到底部。单击指纹。

步骤 6. 运行 regedit 并转至 HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd。

1. 编辑 SSL 指纹注册表项并将 TLS 证书的指纹值复制到此二进制值中。可以忽略编辑二进制值对话框中的未知项（如 '0000' 和特殊字符），这样是安全的。
2. 编辑 SSLEnabled 注册表项并将 DWORD 值更改为 1。（之后要禁用 SSL，请将 DWORD 值更改为 0。）
3. 如果要更改默认设置（可选），请在相同注册表路径中使用以下值：

SSLPort DWORD – SSL 端口号。默认值：443。

SSLMinVersion DWORD – 1 = SSL 3.0、2 = TLS 1.0、3 = TLS 1.1、4 = TLS 1.2。默认值：2 (TLS 1.0)。

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

SSLCipherSuite DWORD – 1 = GOV、2 = COM、3 = ALL。默认值：3 (ALL)。

步骤 7. 如果 TLS TCP 端口不是默认值 443，请确保此端口在 Windows 防火墙中处于打开状态。（在 Windows 防火墙中创建入站规则时，请确保其属性已选中“允许连接”或“启用”条目）。

步骤 8. 确保没有其他应用程序或服务（如 IIS）正在使用 TLS TCP 端口。

步骤 9. 对于 VDA for Windows Server OS，重新启动计算机以使更改生效。（无需重新启动包含 VDA for Windows Desktop OS 的计算机）。

在交付组上配置 TLS

为包含已配置 TLS 连接的 VDA 的每个交付组完成此过程。

1. 从 Studio，打开 PowerShell 控制台。
2. 运行 **asnp Citrix.*** 以加载 Citrix 产品 cmdlet。
3. 运行 **Get-BrokerAccessPolicyRule -DesktopGroupName '<*delivery-group-name*>' | Set-BrokerAccessPolicyRule -HdxSslEnabled $true**。
4. 运行 **Set-BrokerSite -DnsResolutionEnabled $true**。

故障排除

如果连接出错，请检查 VDA 的系统事件日志。

使用 Citrix Receiver for Windows 时，如果收到指示 TLS 错误的连接错误（例如 1030），请禁用 Desktop Viewer，然后尝试重新连接。尽管连接仍将失败，但可能会提供基本 TLS 问题的解释。例如，您在从证书颁发机构申请证书时指定了错误的模板。

Controller 与 VDA 之间的通信

Controller 与 VDA 之间的通信通过 Windows Communication Framework (WCF) 消息级保护来确保安全。不需要执行使用 TLS 的传输层保护。WCF 配置使用 Kerberos 在 Controller 与 VDA 之间进行相互身份验证。加密使用处于 CBC 模式的带 256 位密钥的 AES。消息完整性使用 SHA-1。

根据 Microsoft，WCF 所使用的安全协议符合 OASIS（结构化信息标准促进组织）标准，包括 WS-SecurityPolicy 1.2。此外，Microsoft 还申明，WCF 支持安全策略 1.2 中列出的所有成套算法。

Controller 和 VDA 间的通信使用 basic256 算法套件，该套件的算法如上所述。

TLS 和 HTML5 视频重定向

可以使用 HTML5 视频重定向来重定向 HTTPS Web 站点。注入到这些 Web 站点的 JavaScript 必须与 VDA 上运行的 Citrix HDX HTML5 视频重定向服务建立 TLS 连接。为了实现这一点，在 VDA 上的证书存储中生成了两个自定义证书。

HTML5 视频重定向策略默认处于禁用状态。

有关 HTML5 视频重定向的详细信息，请参阅多媒体策略设置。

> **注意**
>
> 如果您未计划使用 HTML5 视频重定向，我们建议从本地计算机证书存储中删除两个证书。

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

这些证书为：

- 对于 CA（根）：**Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX In-Product CA)
  位置：证书(本地计算机) > 受信任的根证书颁发机构 > 证书。
- 对于最终实体（叶）：**Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX Service)
  位置：证书(本地计算机) > 个人 > 证书。

我们建议设置 Citrix HDX HTML5 视频重定向服务，以便其不自动启动。
停止此服务还将删除证书。

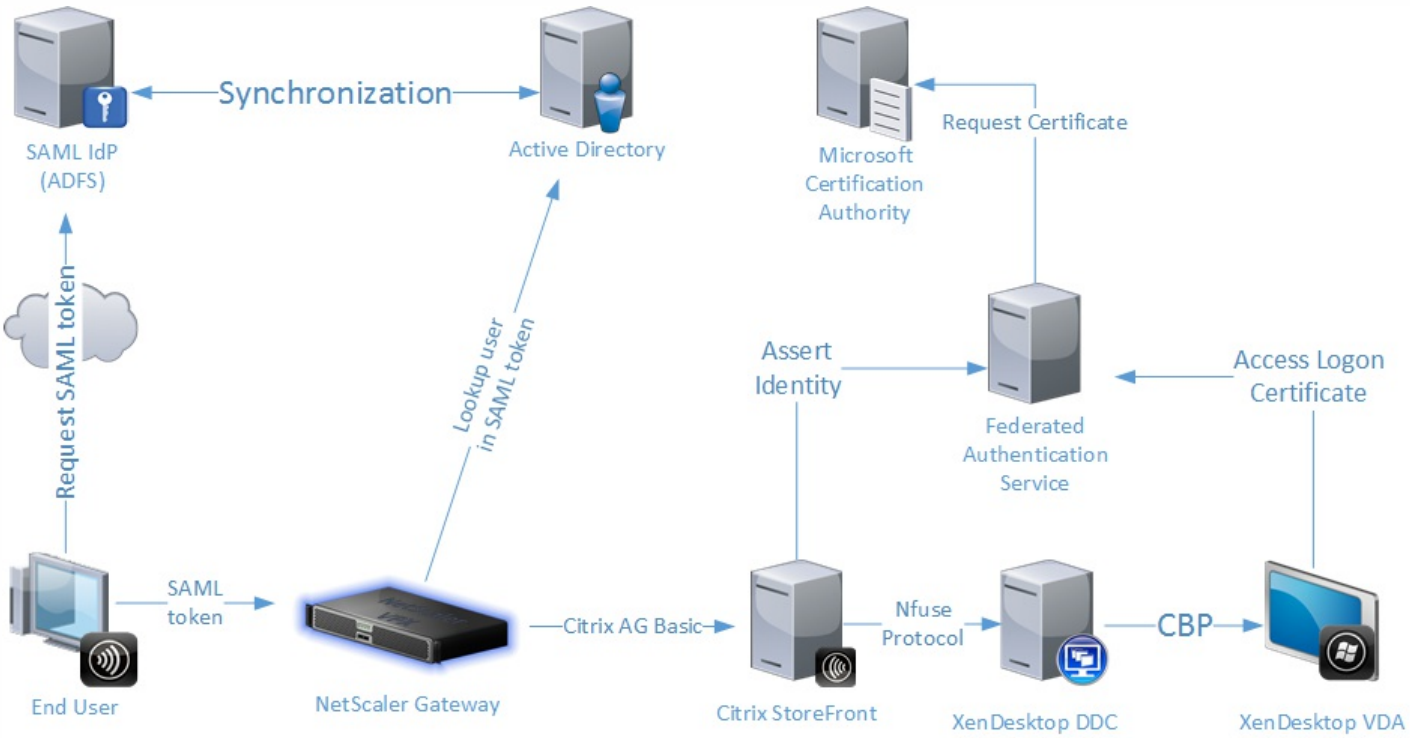
© 1999-2017 Citrix Systems, Inc. All rights reserved.

联合身份验证服务

Dec 05, 2017

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

下图显示了联合身份验证服务与 Microsoft 证书颁发机构集成，并向 StoreFront、XenApp 和 XenDesktop Virtual Delivery Agent (VDA) 提供支持服务。



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

要求

联合身份验证服务支持 Windows 服务器（Windows Server 2008 R2 或更高版本）。

- Citrix 建议在不包含其他 Citrix 组件的服务器上安装 FAS。
- Windows 服务器应受到保护。它将有权访问注册机构的证书和私钥，使其能够自动为域用户颁发证书，并将有权访问这些用户证书和私钥。

在 XenApp 或 XenDesktop 站点中：

- Delivery Controller 的版本必须至少为 7.9。
- VDA 的版本必须至少为 7.9。在以通常方式创建计算机目录之前，确认已向 VDA 正确应用联合身份验证服务组策略配置；

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

请参阅“配置组策略”部分了解详细信息。

- StoreFront 服务器的版本必须至少为 3.6（这是随 XenApp 和 XenDesktop 7.9 ISO 提供的版本）。

在规划该服务的部署时，请查看“安全注意事项”部分。

参考：

- Active Directory 证书服务

  https://technet.microsoft.com/zh-cn/library/hh831740.aspx

- 配置 Windows 的登录证书

  http://support.citrix.com/article/CTX206156

安装和设置过程

1. 安装联合身份验证服务
2. 在 StoreFront 服务器上启用“联合身份验证服务”插件
3. 配置组策略
4. 使用“联合身份验证服务”管理控制台执行以下操作：(a) 部署所提供的模板，(b) 设置证书颁发机构，以及 (c) 授权联合身份验证服务使用您的证书颁发机构
5. 配置用户规则

安装联合身份验证服务

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

将安装以下组件：

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

在 StoreFront 应用商店上启用联合身份验证服务插件

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

命令 复制

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

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

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName "FASClaimsFactory"

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider "FASLogonDataProvider"
```

要停止使用 FAS，请使用以下 PowerShell 脚本：

命令 复制

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

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName "standardClaimsFactory"

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""
```

配置 Delivery Controller

要使用联合身份验证服务，请配置 XenApp 或 XenDesktop Delivery Controller 以信任可与其连接的 StoreFront 服务器：运行 **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true** PowerShell cmdlet。

配置组策略

在安装联合身份验证服务后，必须使用安装中提供的组策略模板指定组策略中的 FAS 服务器的完整 DNS 地址。

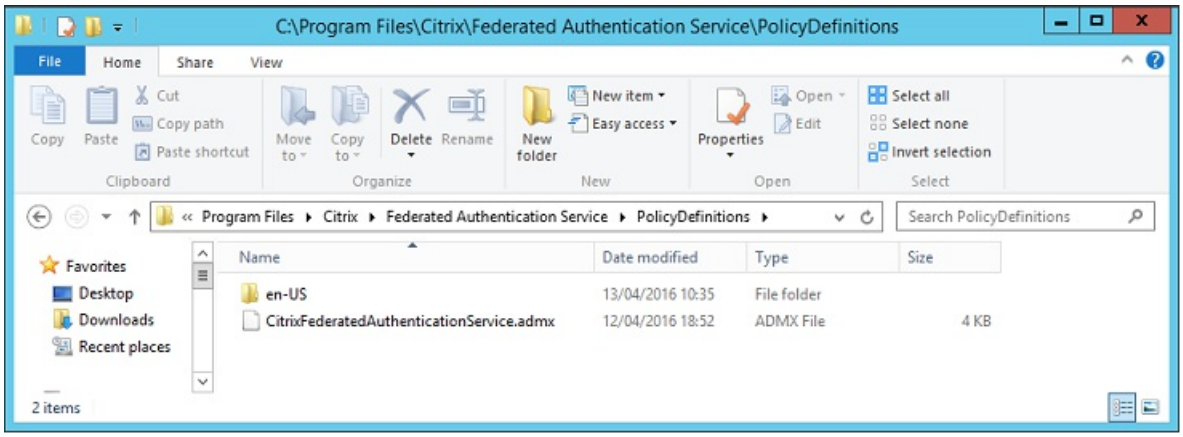
重要：确保请求票据的 StoreFront 服务器和找回票据的 VDA 具有相同的 DNS 地址配置，包括通过组策略对象应用的服务器自动编号。

为简单起见，以下示例在域级别配置单个策略以应用于所有计算机；但是，这并不是必需的。只要 StoreFront 服务器、VDA

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

以及正在运行 FAS 管理控制台的计算机查看到相同 DNS 地址列表，FAS 即可正常工作。请注意，“组策略”对象会向每一项添加一个索引号。如果使用多个对象，则索引号也必须匹配。

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

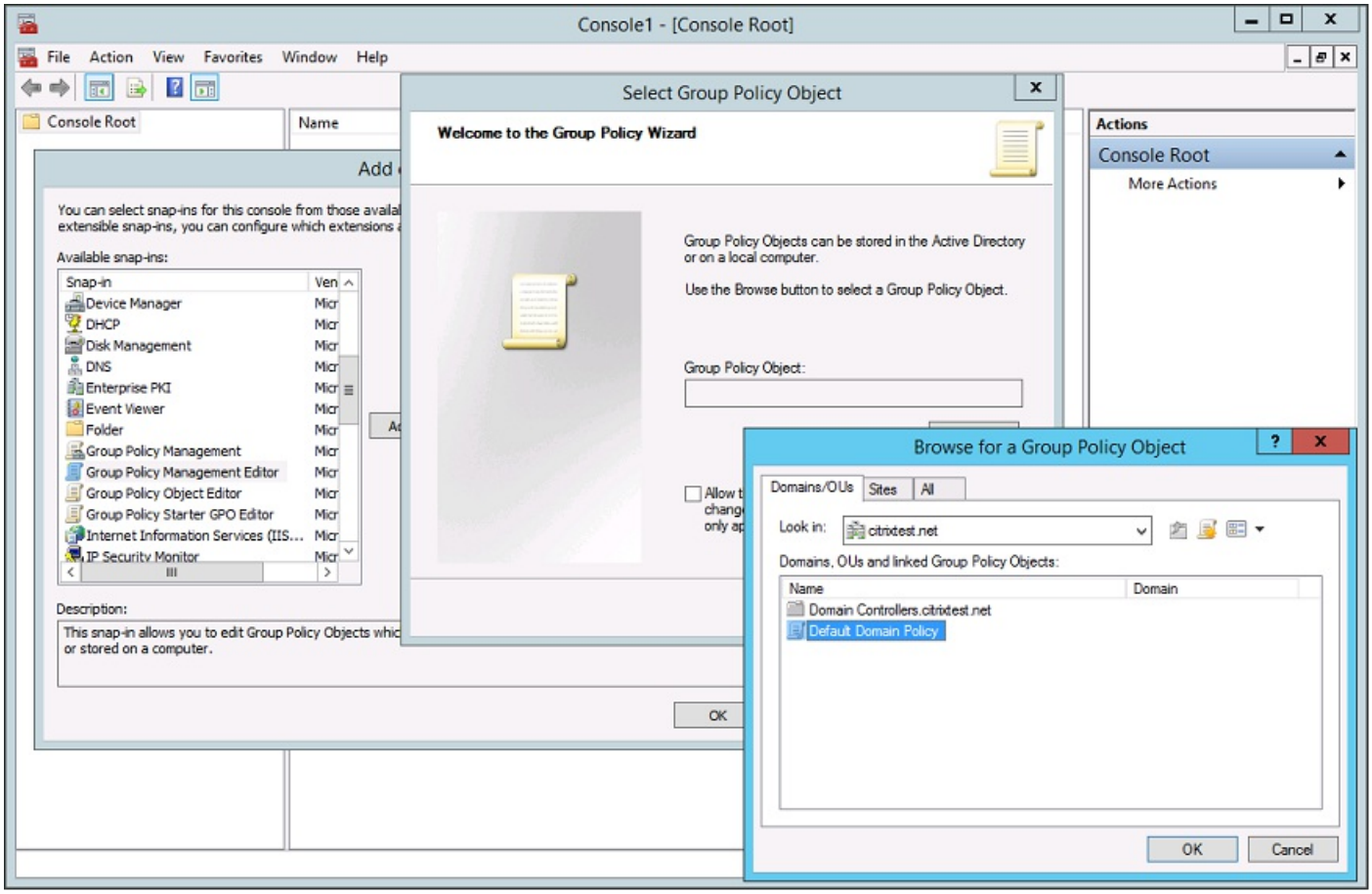


步骤 2. 将这些内容复制到您的域控制器，并将其放置在 C:\Windows\PolicyDefinitions 和 en-US 子文件夹中。

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

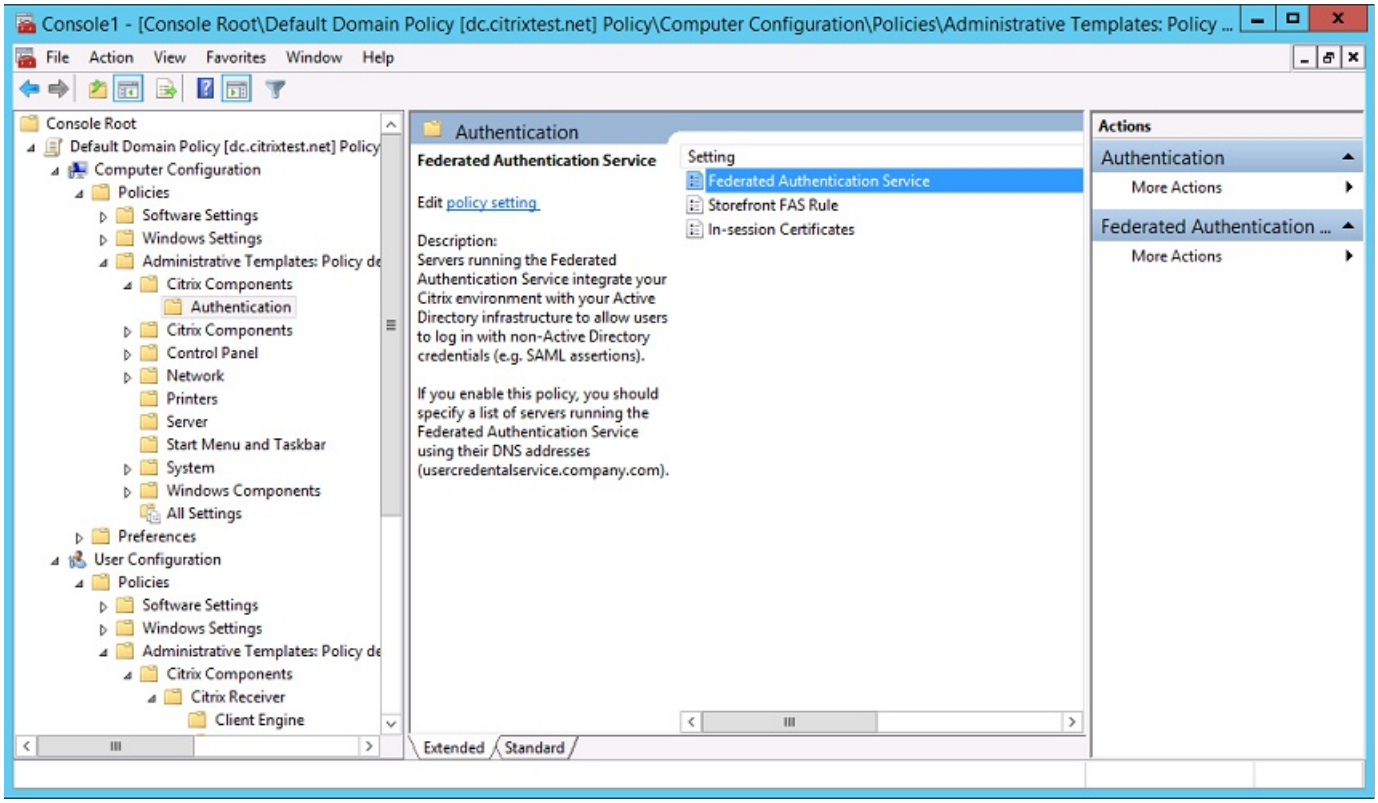
当提示输入组策略对象时，选择**浏览**，然后选择**默认域策略**。或者，也可以使用您选择的工具为环境创建并选择相应策略对象。必须向运行受影响 Citrix 软件（VDAs、 StoreFront 服务器、管理工具）的所有计算机应用策略。

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

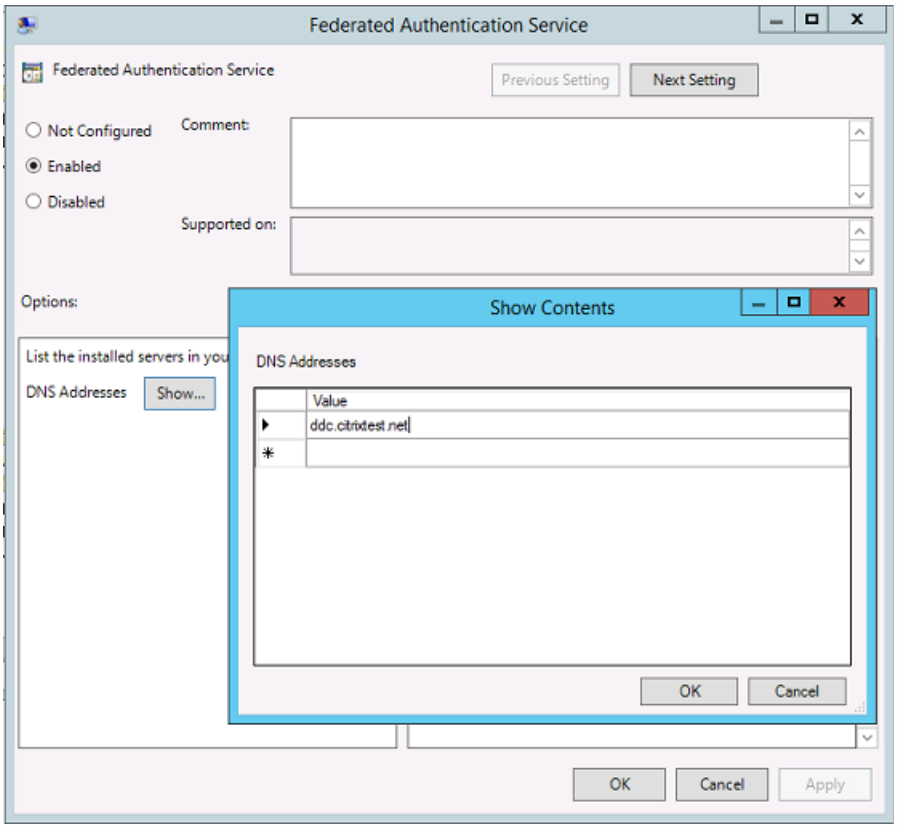


步骤 4. 导航到位于 Computer Configuration/Policies/Administrative Templates/Citrix Components/Authentication 的联合身份验证服务策略。

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



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



步骤 6. 输入用于托管联合身份验证服务的服务器的 DNS 地址。

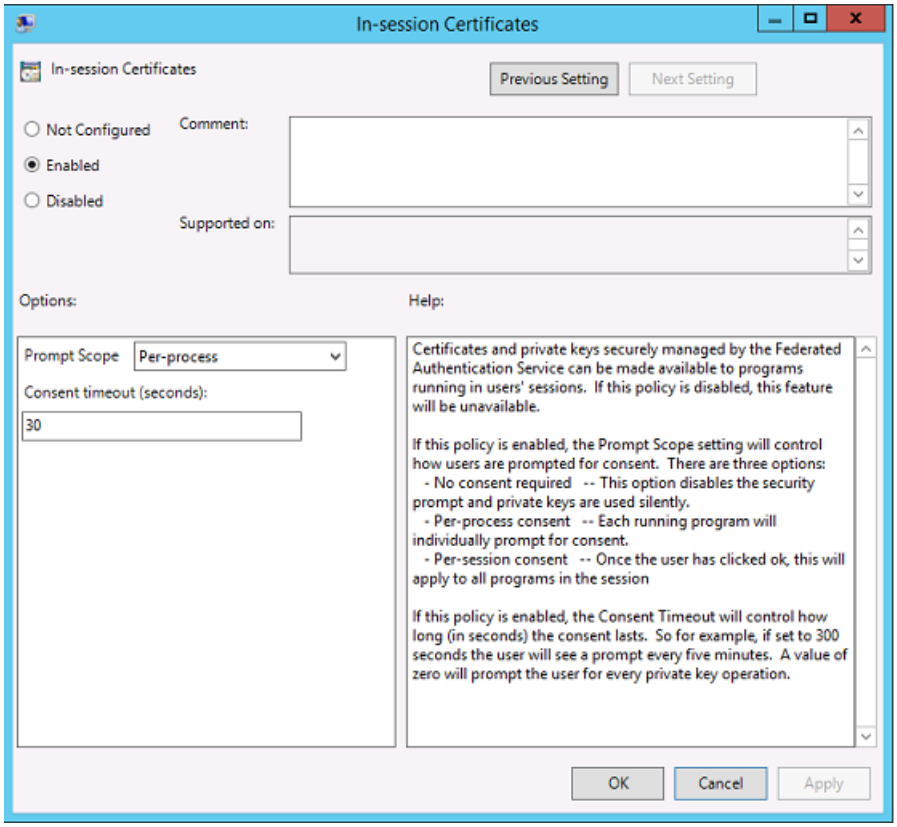
© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

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

启用会话中证书支持

在“组策略”模板中，可为系统配置会话中证书。这样，会在登录后将证书放置在用户的个人证书存储中，以供应用程序使用。例如，如果您需要在 VDA 会话中对 Web 服务器执行 TLS 身份验证，则可通过 Internet Explorer 使用证书。默认情况下，VDA 将不允许在登录后访问证书。

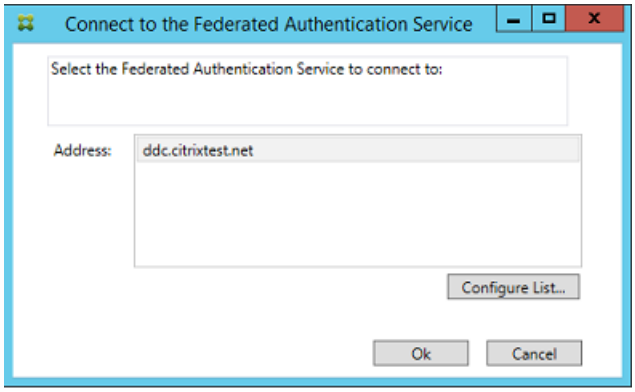


使用“联合身份验证服务”管理控制台

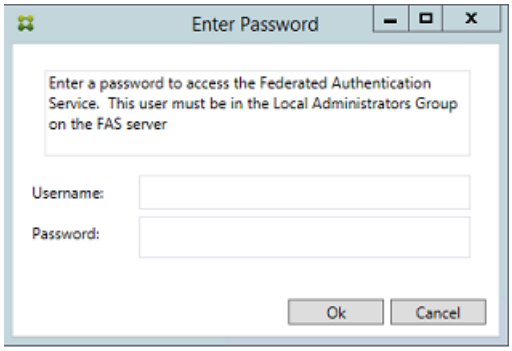
“联合身份验证服务”管理控制台作为联合身份验证服务的一部分安装。将在“开始”菜单中显示一个图标（Citrix 联合身份验证服务）。

控制台会尝试使用组策略配置来自动查找环境中的 FAS 服务器。如果失败，请参阅配置组策略部分。

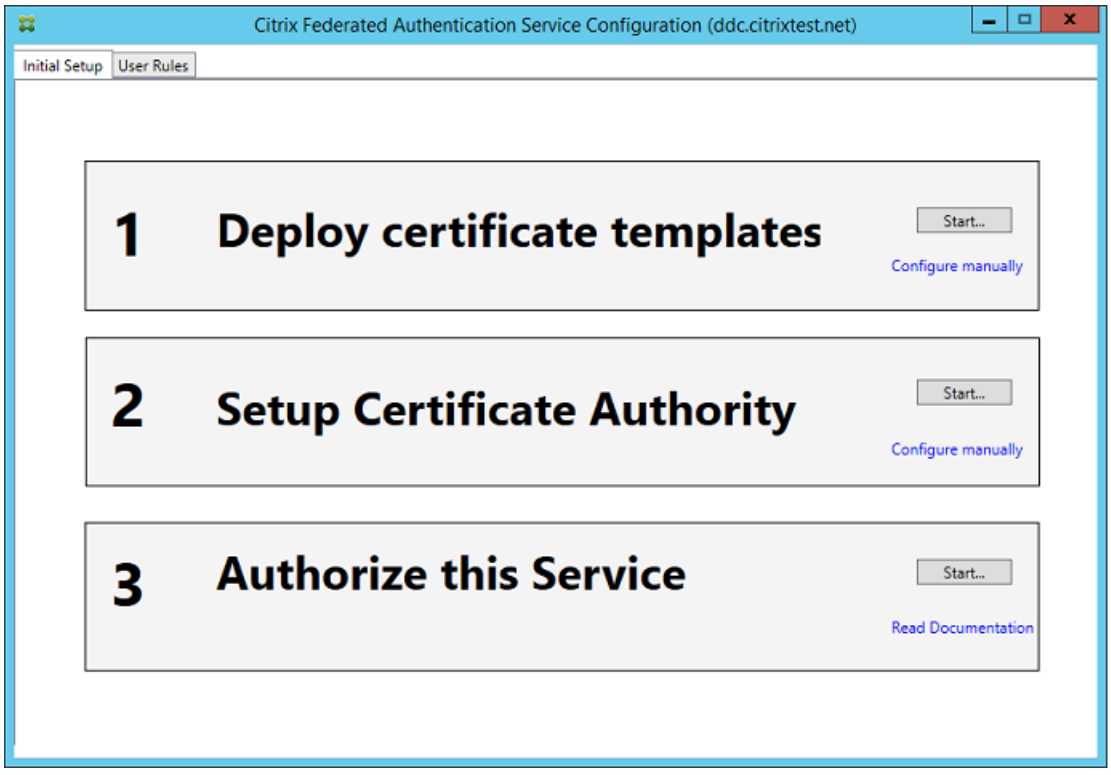
© 1999-2017 Citrix Systems, Inc. All rights reserved.



如果您的用户帐户不属于正在运行联合身份验证服务的计算机上的 Administrators 组，则会提示您输入凭据。



在第一次使用管理控制台时，它会引导您完成三个步骤，用于部署证书模板、设置证书颁发机构以及授权联合身份验证服务使用此证书颁发机构。也可以使用操作系统配置工具手动完成其中一些步骤。



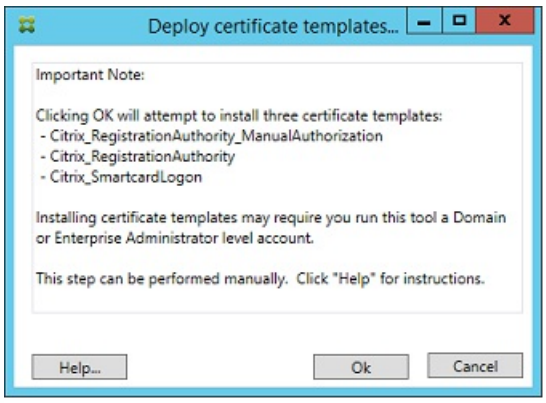
© 1999-2017 Citrix Systems, Inc. All rights reserved.

部署证书模板

为了避免发生与其他软件的互操作性问题，联合身份验证服务提供了三个 Citrix 证书模板以供其自己使用。

- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

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



可在随联合身份验证服务安装的 XML 文件（具有 .certificatetemplate 扩展名 ）中找到模板配置：

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

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

要手动安装这些模板，可以使用下面的 PowerShell 命令：

命令 复制

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

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

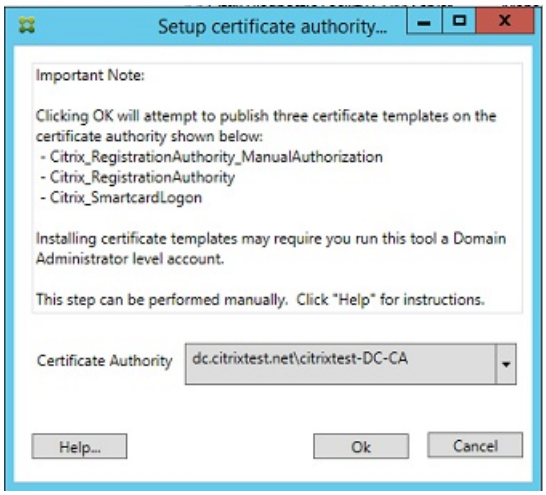
$writabletemplate = New-Object -ComObject X509Enrollment.CX509CertificateTemplateADWritable
$writabletemplate.Initialize($comtemplate)
$writabletemplate.Commit(1, $NULL)
```

设置 Active Directory 证书服务

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

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

（也可以使用 Microsoft 证书颁发机构控制台发布证书模板。）

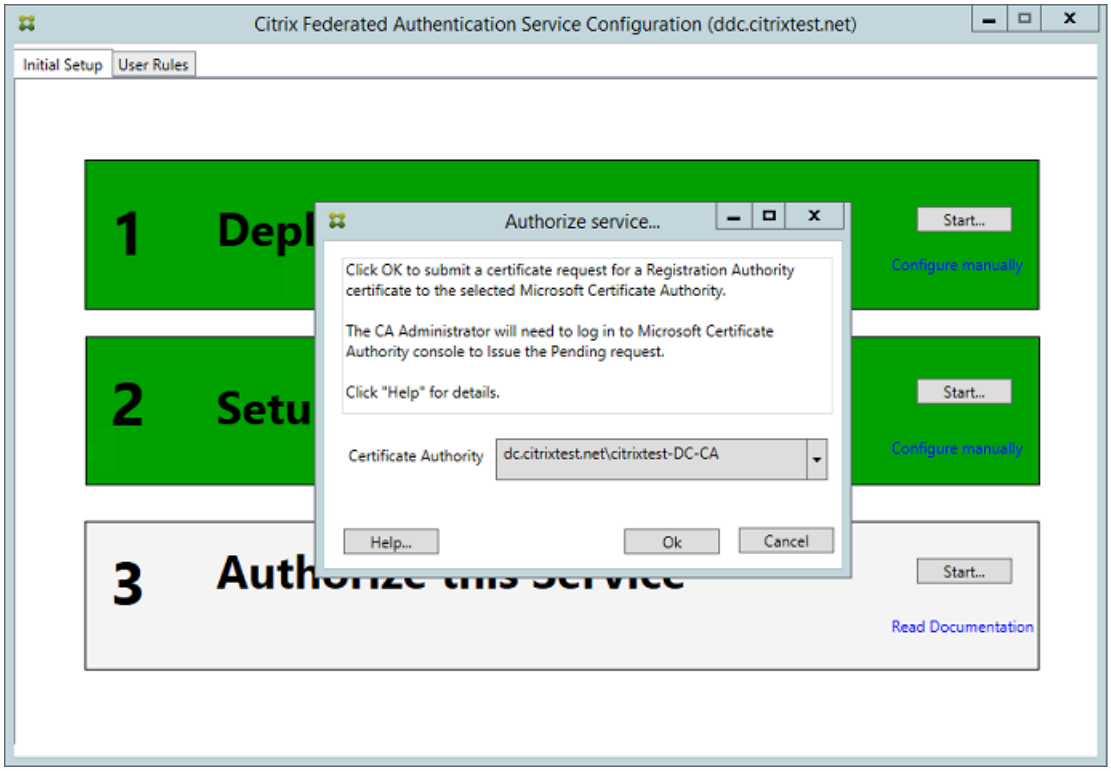


授权联合身份验证服务

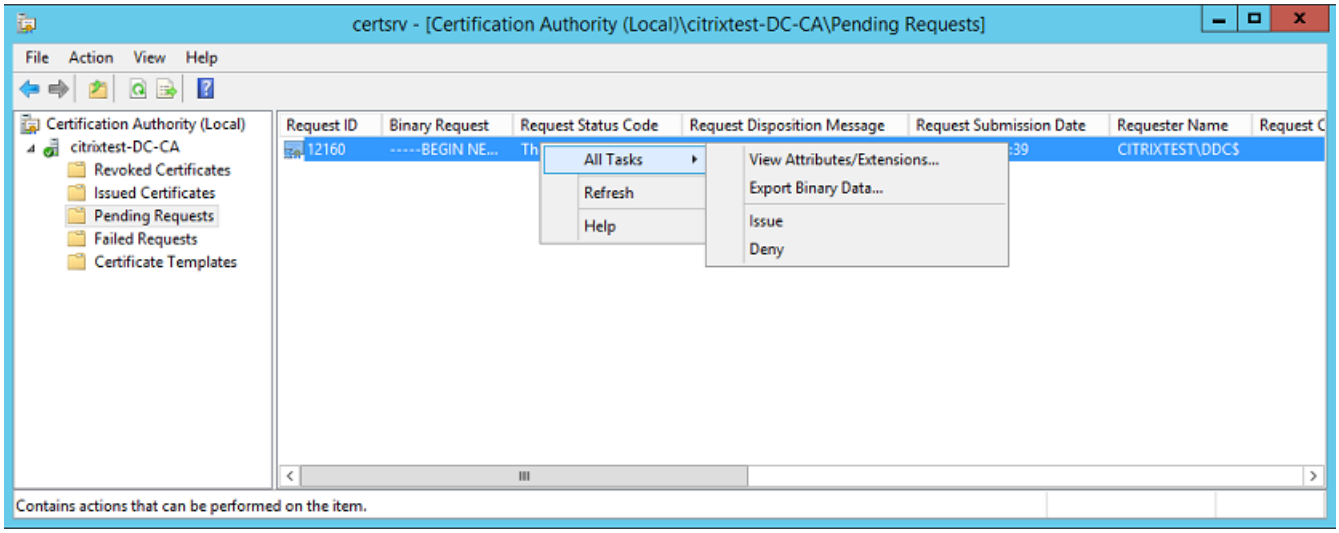
在控制台中执行的最后一个设置步骤将启动对联合身份验证服务的授权。管理控制台使用 Citrix_RegistrationAuthority_ManualAuthorization 模板生成一个证书申请，然后将其发送到用于发布该模板的证书颁发机构

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

之一。

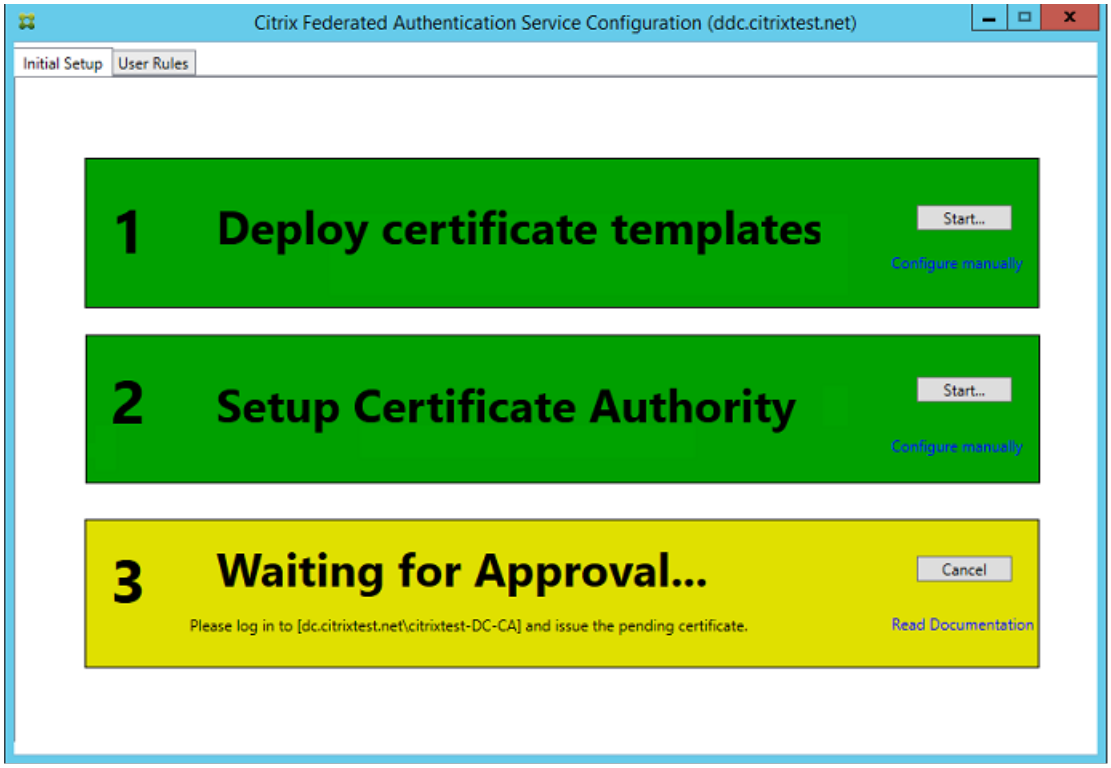


在发送请求后，该请求将出现在 Microsoft 证书颁发机构控制台的**挂起的请求**列表中。证书颁发机构管理员必须选择**颁发**或**拒绝**请求，然后才能继续配置联合身份验证服务。请注意，授权请求将显示为来自 FAS 计算机帐户的**挂起的请求**。



右键单击**所有任务**，然后选择**颁发**或**拒绝**证书申请。联合身份验证服务管理控制台会自动检测此过程的完成时间。这可能需要几分钟的时间。

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

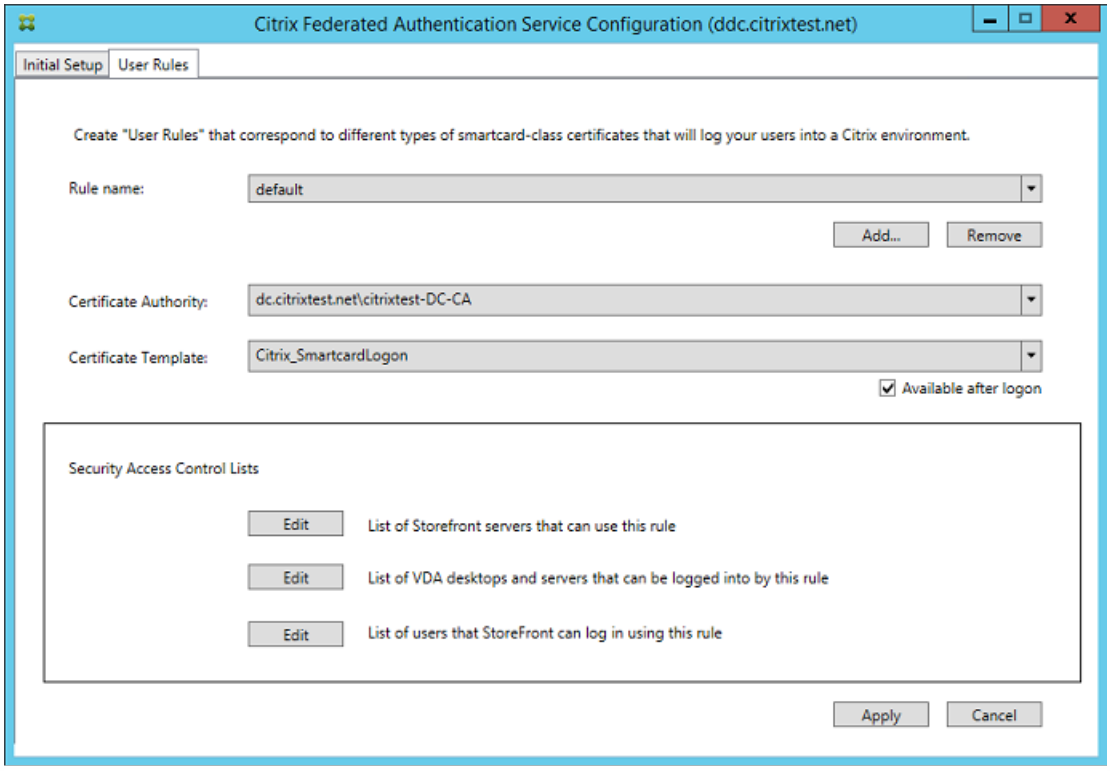


配置用户规则

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

要完成联合身份验证服务的设置，管理员必须通过以下操作来定义默认规则：切换到 FAS 管理控制台的“用户规则”选项卡，选择将向其发布 Citrix_SmartcardLogon 模板证书的颁发机构，并编辑 StoreFront 服务器列表。VDA 列表默认为“域计算机”，用户列表默认为“域用户”列表；如果默认值不适当，可以更改这些值。

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



字段：

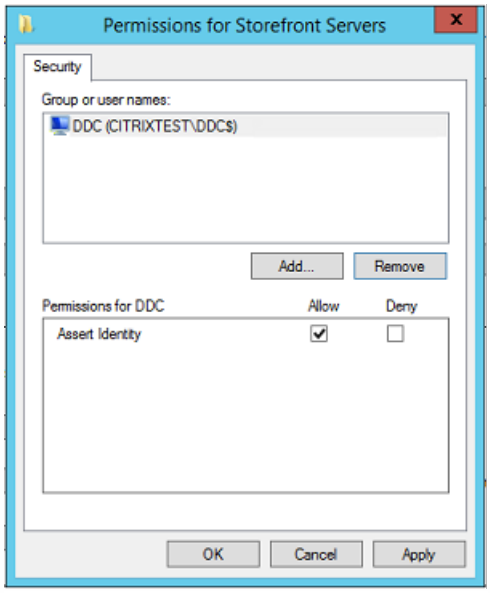
证书颁发机构和证书模板：将用于颁发用户证书的证书模板和证书颁发机构。在向其发布模板的其中一个证书颁发机构上，这应该是 Citrix_SmartcardLogon 模板，或此模板的经修改的副本。

FAS 支持使用 PowerShell 命令添加多个证书颁发机构以用于故障转移和负载平衡。同样地，也可以使用命令行和配置文件配置更高级的证书生成选项。请参阅 PowerShell 和硬件安全模块部分。

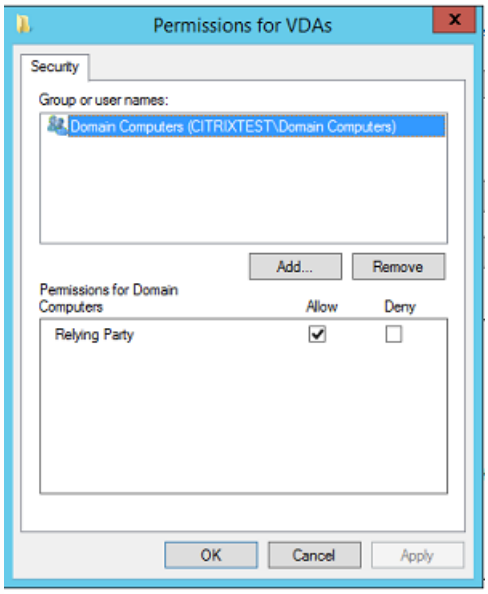
In-Session Certificates（会话中证书）：**Available after logon**（登录后可用）复选框可控制是否同时将证书用作会话中证书。如果未选中此复选框，则只会将证书用于登录或重新连接，并且用户将无法在身份验证后访问证书。

List of StoreFront servers that can use this rule（可以使用此规则的 StoreFront 服务器的列表）：被授权请求用于用户登录或重新连接过程的证书的可信 StoreFront 服务器计算机的列表。请注意，此设置对于安全性至关重要，因此必须谨慎地加以管理。

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

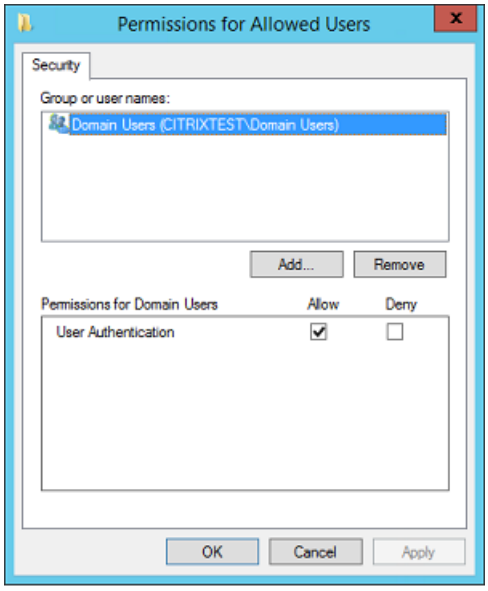


List of VDA desktops and servers that can be logged into by this rule（可通过此角色登录到的 VDA 桌面和服务器的列表）：可通过使用联合身份验证服务系统让用户登录的 VDA 计算机的列表。



List of users that StoreFront can log in using this rule（StoreFront 可通过使用此规则让其登录的用户的列表）：StoreFront 可通过使用此规则让其登录的的用户的列表。

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



高级用法

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

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

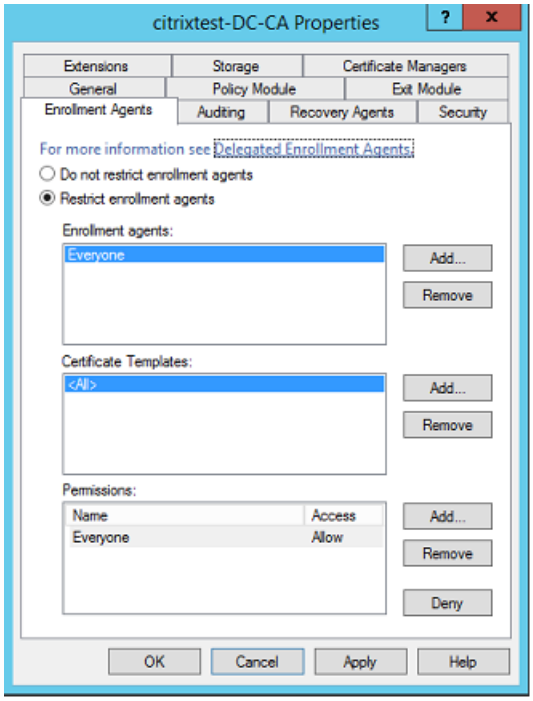
安全注意事项

联合身份验证服务具有注册授权证书，允许它代表您的域用户自主颁发证书。因此，必须制定并实施安全策略来保护 FAS 服务器，并限制它们的权限。

委派注册代理

Microsoft 证书颁发机构可以控制可由 FAS 服务器使用的模板，以及限制 FAS 服务器可为其颁发证书的用户。

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



Citrix 强烈建议配置这些选项，以便联合身份验证服务只能为目标用户颁发证书。例如，建议阻止联合身份验证服务向 Administration or Protected Users 组中的用户颁发证书。

访问控制列表配置

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

防火墙设置

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

事件日志监视

联合身份验证服务和 VDA 会将信息写入 Windows 事件日志。此信息可以用于监视和审核信息。事件日志部分列出了可生成的事件日志条目。

硬件安全模块

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

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

参数	说明
ProviderLegacyCsp	当设置为 true 时，FAS 将使用 Microsoft CryptoAPI (CAPI)。否则，FAS 将使用 Microsoft

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

	下一代加密技术 API (CNG)。
ProviderName	要使用的 CAPI 或 CNG 提供程序的名称。
ProviderType	请参阅 Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24。应该始终为 24，除非您使用 CAPI 与 HSM 并且 HSM 提供商另有规定。
KeyProtection	控制私钥的“可导出”标志。如果硬件支持，还允许使用可信平台模块 (TPM) 密钥存储。
KeyLength	RSA 私钥的密钥长度。支持的值包括 1024、2048 和 4096（默认值：2048）。

PowerShell SDK

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

以下命令将添加 PowerShell cmdlet：

Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1

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

命令	概述
*-FasServer	列出并重新配置当前环境中的 FAS 服务器。
*-FasAuthorizationCertificate	管理“注册机构”证书。
*-FasCertificateDefinition	控制由 FAS 用于生成证书的参数。
*-FasRule	管理在联合身份验证服务中配置的用户规则。
*-FasUserCertificate	列出并管理由联合身份验证服务缓存的证书。

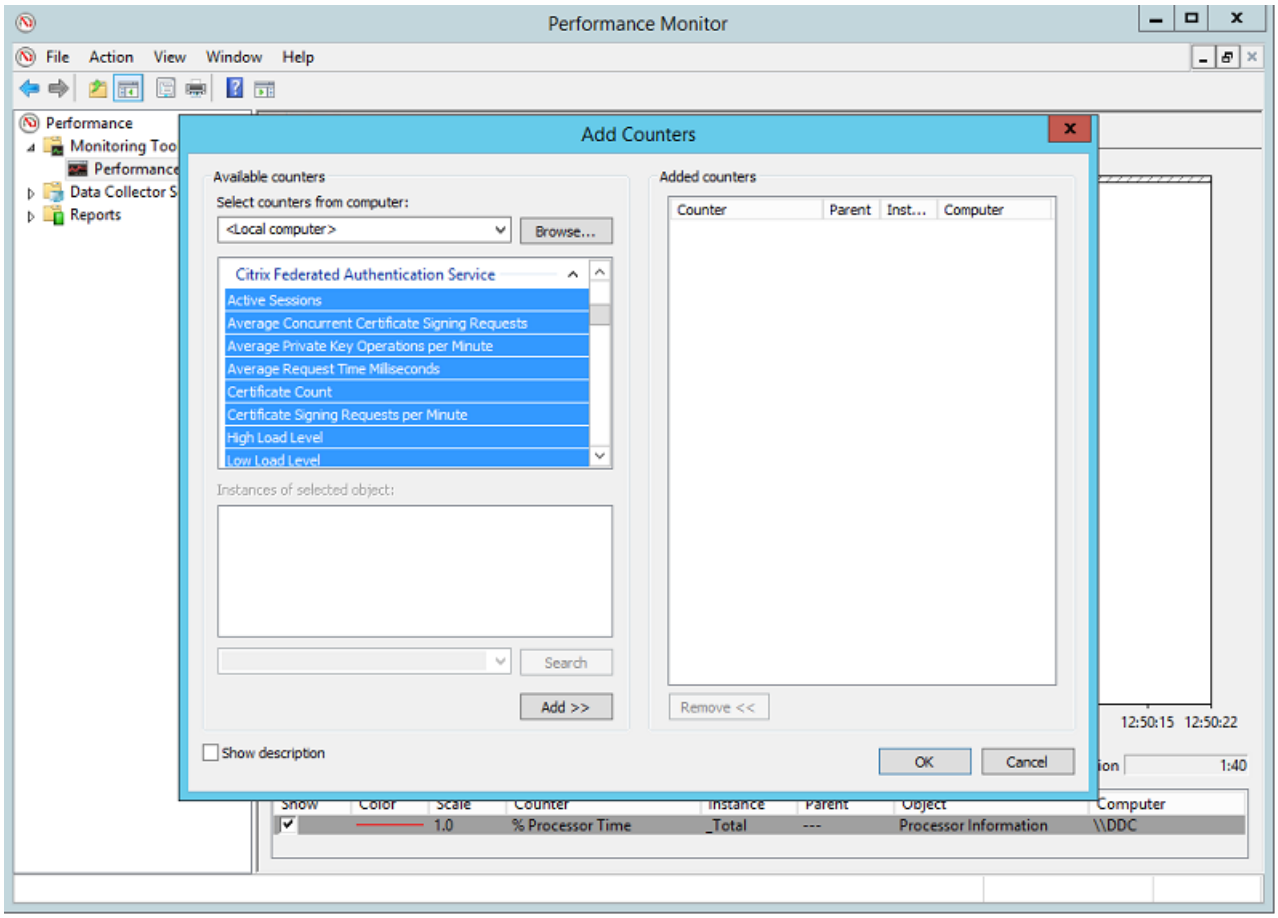
可通过指定 FAS 服务器地址来远程使用 PowerShell cmdlet。

您也可以下载其中包含所有 FAS PowerShell cmdlet 帮助文件的 zip 文件。请参阅 PowerShell SDK 一文。

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

性能计数器

联合身份验证服务包括一组用于跟踪负载的性能计数器。



下表列出了可用的计数器。大多数计数器会在五分钟后滚动平均值。

名称	说明
活动会话	由联合身份验证服务跟踪的连接数。
并发 CSR	在同一时间处理的证书申请数。
私钥 OPS	每分钟执行的私钥操作数。
请求时间	生成并签署证书所用的时间长度。
证书计数	在联合身份验证服务中缓存的证书数量。

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

每分钟的 CSR	每分钟处理的 CSR 数。
低/中/高	以“每分钟 CSR 数”为依据估算联合身份验证服务可接受的负载。如果超过“高负载”阈值，可能会导致会话启动失败。

事件日志

下表列出了由联合身份验证服务生成的事件日志条目。

管理事件

[事件来源：Citrix.Authentication.FederatedAuthenticationService]

将记录这些事件，以响应联合验证服务服务器的配置变化。

日志代码
[S001] ACCESS DENIED: User [{0}] is not a member of Administrators group
[S002] ACCESS DENIED: User [{0}] is not an Administrator of Role [{1}]
[S003] Administrator [{0}] setting Maintenance Mode to [{1}]
[S004] Administrator [{0}] enrolling with CA [{1}] templates [{2} and {3}]
[S005] Administrator [{0}] de-authorizing CA [{1}]
[S006] Administrator [{0}] creating new Certificate Definition [{1}]
[S007] Administrator [{0}] updating Certificate Definition [{1}]
[S008] Administrator [{0}] deleting Certificate Definition [{1}]
[S009] Administrator [{0}] creating new Role [{1}]
[S010] Administrator [{0}] updating Role [{1}]
[S011] Administrator [{0}] deleting Role [{1}]

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

[S012] Administrator [{0}] creating certificate [upn: {0} sid: {1} role: {2}][Certificate Definition: {3}]
[S013] Administrator [{0}] deleting certificates [upn: {0} role: {1} Certificate Definition: {2}]

日志代码
[S401] Performing configuration upgrade -- [From version {0}][to version {1}]
[S402] ERROR: The Citrix Federated Authentication Service must be run as Network Service [currently running as: {0}]

创建身份声明 [联合身份验证服务]

在运行期间，当可信服务器声明用户登录时，将在联合身份验证服务服务器上记录这些事件。

日志代码
[S101] Server [{0}] is not authorized to assert identities in role [{1}]
[S102] Server [{0}] failed to assert UPN [{1}] (Exception: {2}{3})
[S103] Server [{0}] requested UPN [{1}] SID {2}, but lookup returned SID {3}
[S104] Server [{0}] failed to assert UPN [{1}] (UPN not allowed by role [{2}])
[S105] Server [{0}] issued identity assertion [upn: {0}, role {1}, Security Context: [{2}]
[S120] Issuing certificate to [upn: {0} role: {1} Security Context: [{2}]]
[S121] Issuing certificate to [upn: {0} role: {1}] on behalf of account {2}
[S122] Warning: Server is overloaded [upn: {0} role: {1}][Requests per minute {2}].

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

作为信赖方 [联合身份验证服务]

在运行期间，当 VDA 用户登录时会在联合身份验证服务服务器上记录这些事件。

日志代码
[S201] Relying party [{0}] does not have access to a password.
[S202] Relying party [{0}] does not have access to a certificate.
[S203] Relying party [{0}] does not have access to the Logon CSP
[S204] Relying party [{0}] accessing the Logon CSP [Operation: {1}]
[S205] Calling account [{0}] is not a relying party in role [{1}]
[S206] Calling account [{0}] is not a relying party
[S207] Relying party [{0}] asserting identity [upn: {1}] in role: [{2}]
[S208] Private Key operation failed [Operation: {0}][upn: {1} role: {2} certificateDefinition {3}][Error {4} {5}].

会话中证书服务器 [联合身份验证服务]

当用户使用会话中证书时，会在联合身份验证服务服务器上记录这些事件。

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

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

登录 [VDA]

[事件来源：Citrix.Authentication.IdentityAssertion]

在登录阶段会在 VDA 上记录这些事件。

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

会话中证书 [VDA]

当用户尝试使用会话中证书时，会在 VDA 上记录这些事件。

日志代码
[S201] Virtual Smart Card Authorized [User: {0}][PID: {1} Name:{2}][Certificate {3}]
[S202] Virtual Smart Card Subsystem. No smart cards available in session {0}
[S203] Virtual Smart Card Subsystem. Access Denied [caller: {0}, session {1}, expected: {2}]
[S204] Virtual Smart Card Subsystem. Smart card support disabled.

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

证书申请和生成代码 [联合身份验证服务]

[事件来源：Citrix.TrustFabric]

当联合身份验证服务服务器执行日志级别的加密操作时，会记录这些低级别事件。

日志代码
[S0001]TrustArea::TrustArea: Installed certificate chain
[S0002]TrustArea::Join: Callback has authorized an untrusted certificate
[S0003]TrustArea::Join: Joining to a trusted server
[S0004]TrustArea::Maintain: Renewed certificate
[S0005]TrustArea::Maintain: Retrieved new certificate chain
[S0006]TrustArea::Export: Exporting private key
[S0007]TrustArea::Import: Importing Trust Area
[S0008]TrustArea::Leave: Leaving Trust Area
[S0009]TrustArea::SecurityDescriptor: Setting Security Descriptor
[S0010]CertificateVerification: Installing new trusted certificate
[S0011]CertificateVerification: Uninstalling expired trusted certificate
[S0012]TrustFabricHttpClient: Attempting single sign-on to {0}
[S0013]TrustFabricHttpClient: Explicit credentials entered for {0}
[S0014]Pkcs10Request::Create: Created PKCS10 request
[S0015]Pkcs10Request::Renew: Created PKCS10 request

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

[S0016]PrivateKey::Create
[S0017]PrivateKey::Delete
[S0018]TrustArea::TrustArea: Waiting for Approval
[S0019]TrustArea::Join: Delayed Join
[S0020]TrustArea::Join: Delayed Join
[S0021]TrustArea::Maintain: Installed certificate chain

日志代码
[S0101]TrustAreaServer::Create root certificate
[S0102]TrustAreaServer::Subordinate: Join succeeded
[S0103]TrustAreaServer::PeerJoin: Join succeeded
[S0104]MicrosoftCertificateAuthority::GetCredentials: Authorized to use {0}
[S0104]MicrosoftCertificateAuthority::SubmitCertificateRequest Error {0}
[S0105]MicrosoftCertificateAuthority::SubmitCertificateRequest Issued cert {0}
[S0106]MicrosoftCertificateAuthority::PublishCRL: Published CRL
[S0107]MicrosoftCertificateAuthority::ReissueCertificate Error {0}
[S0108]MicrosoftCertificateAuthority::ReissueCertificate Issued Cert {0}
[S0109]MicrosoftCertificateAuthority::CompleteCertificateRequest - Still waiting for approval
[S0110]MicrosoftCertificateAuthority::CompleteCertificateRequest - Pending certificate refused

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

[S0111]MicrosoftCertificateAuthority::CompleteCertificateRequest Issued certificate
[S0112]MicrosoftCertificateAuthority::SubmitCertificateRequest - Waiting for approval
[S0120]NativeCertificateAuthority::SubmitCertificateRequest Issued cert {0}
[S0121]NativeCertificateAuthority::SubmitCertificateRequest Error
[S0122]NativeCertificateAuthority::RootCARollover New root certificate
[S0123]NativeCertificateAuthority::ReissueCertificate New certificate
[S0124]NativeCertificateAuthority::RevokeCertificate
[S0125]NativeCertificateAuthority::PublishCRL

相关信息

- 通用 FAS 部署在联合身份验证服务体系结构概述一文中加以概括。
- 联合身份验证服务配置和管理一文介绍了“操作指南”文章。

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

联合身份验证服务体系结构概述

Dec 05, 2017

简介

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

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

本文介绍了一些顶级部署体系结构示例（按复杂性升序排列）。

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

提供了指向相关 FAS 文章的链接。对于所有体系结构，都可以将联合身份验证服务一文用作设置 FAS 时所参考的主要信息源。

工作原理

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

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

内部部署

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

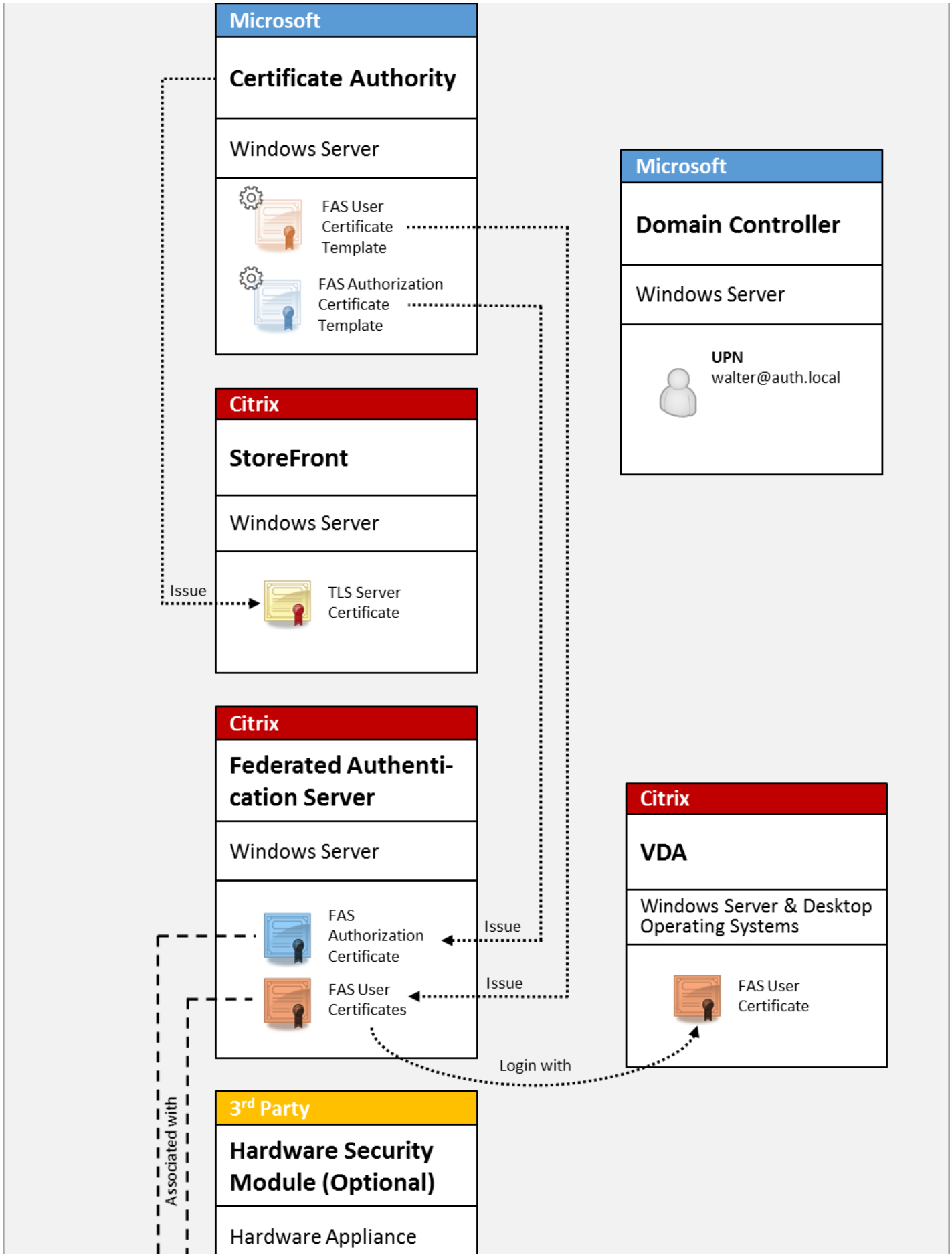
这允许在不提示最终用户输入凭据或智能卡 PIN 码且不使用“已保存密码管理”功能（例如单点登录服务）的情况下执行 Windows 身份验证。这可用于取代 XenApp 早期版本中的“Kerberos 约束委派”登录功能。

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

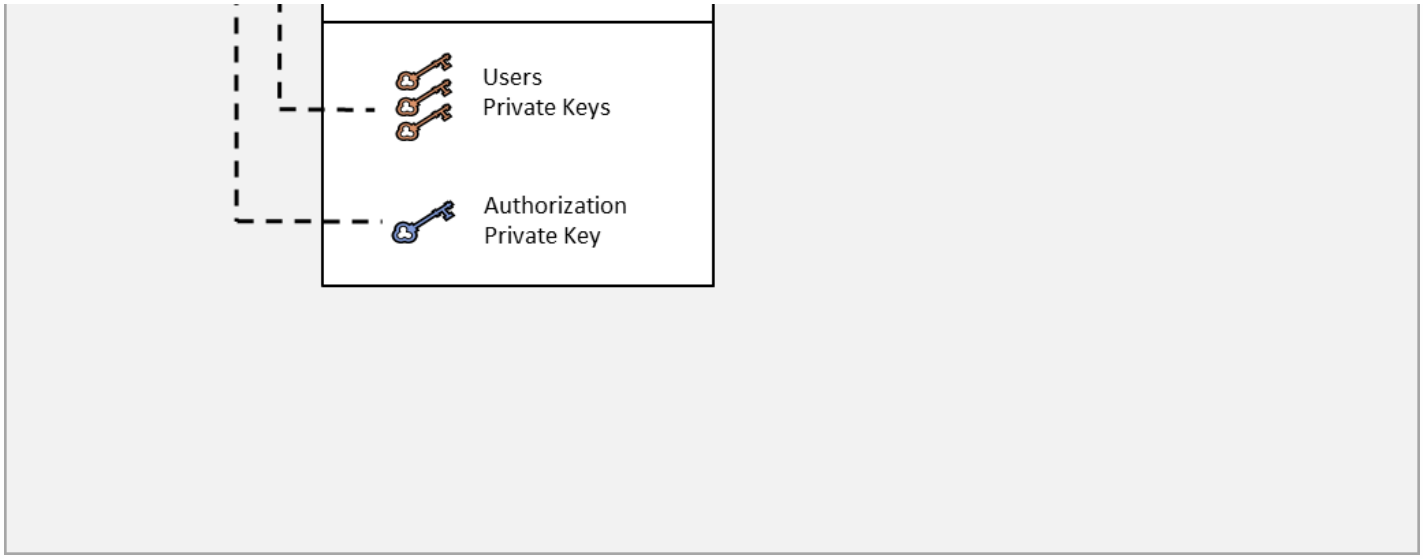
此部署中增加了一个用于运行 FAS 的新服务器，该服务器已获得代表用户颁发智能卡类证书的授权。这些证书之后在 Citrix HDX 环境中用于登录用户会话，就如同已使用智能卡登录一样。



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



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



必须以类似于智能卡登录的方式配置 XenApp 或 XenDesktop 环境，CTX206156 对此过程进行了说明。

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

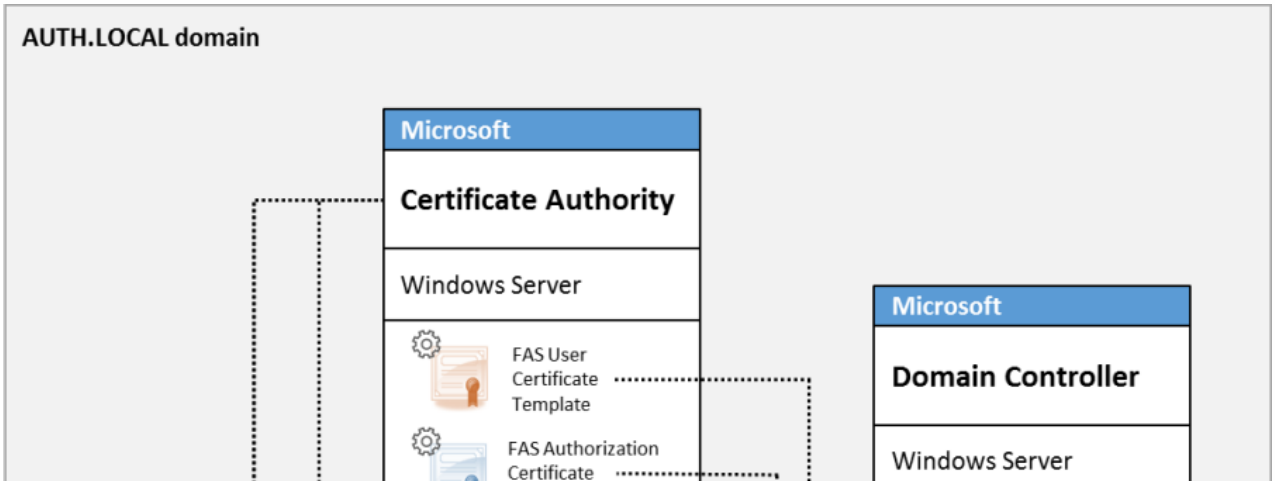
相关信息：

- 密钥可存储在硬件安全模块 (HSM) 或内置的可信平台模块 (TPM) 中。有关详细信息，请参阅联合身份验证服务私钥保护一文。
- 联合身份验证服务一文介绍了如何安装和配置 FAS。

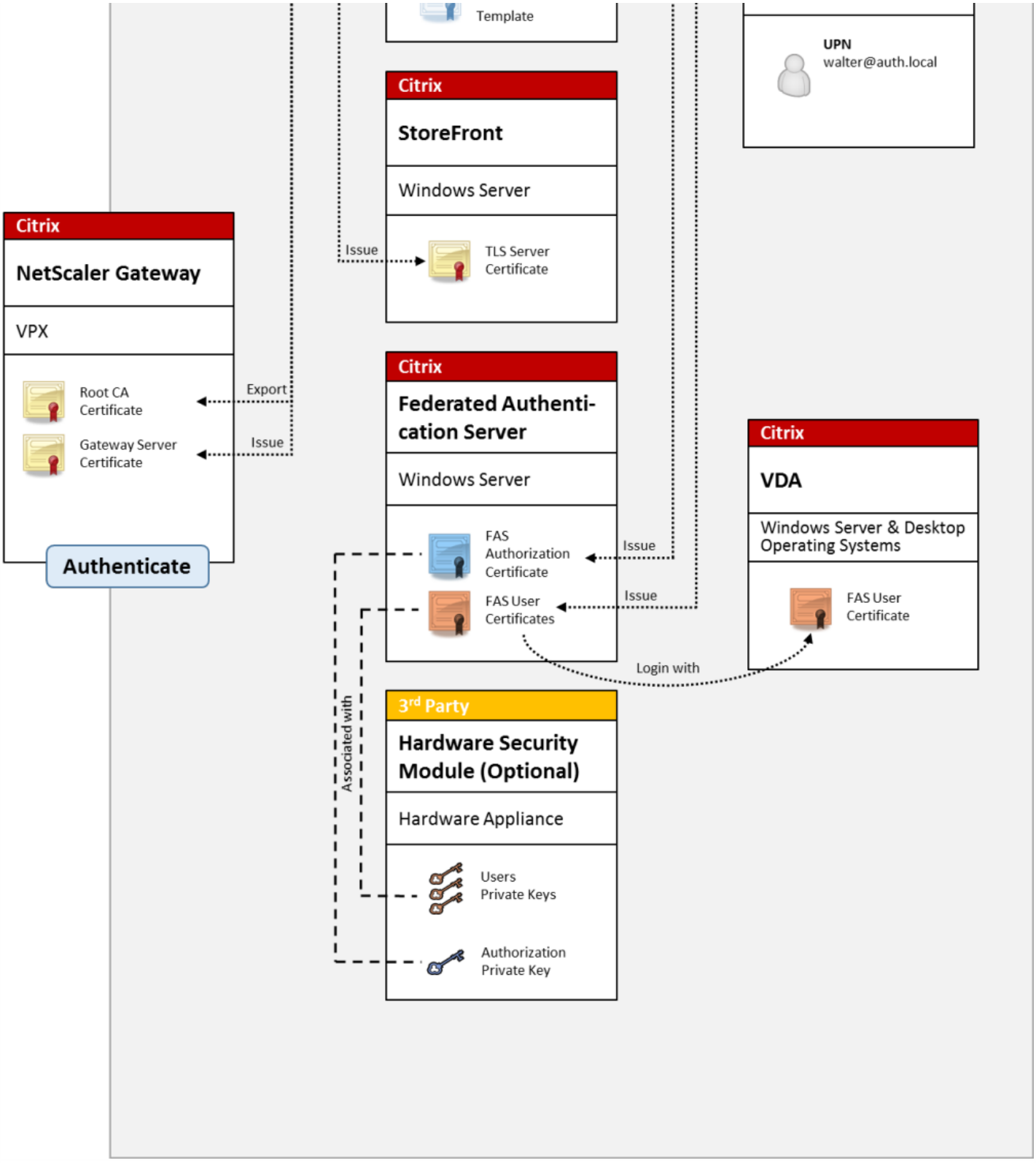
NetScaler Gateway 部署

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

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



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



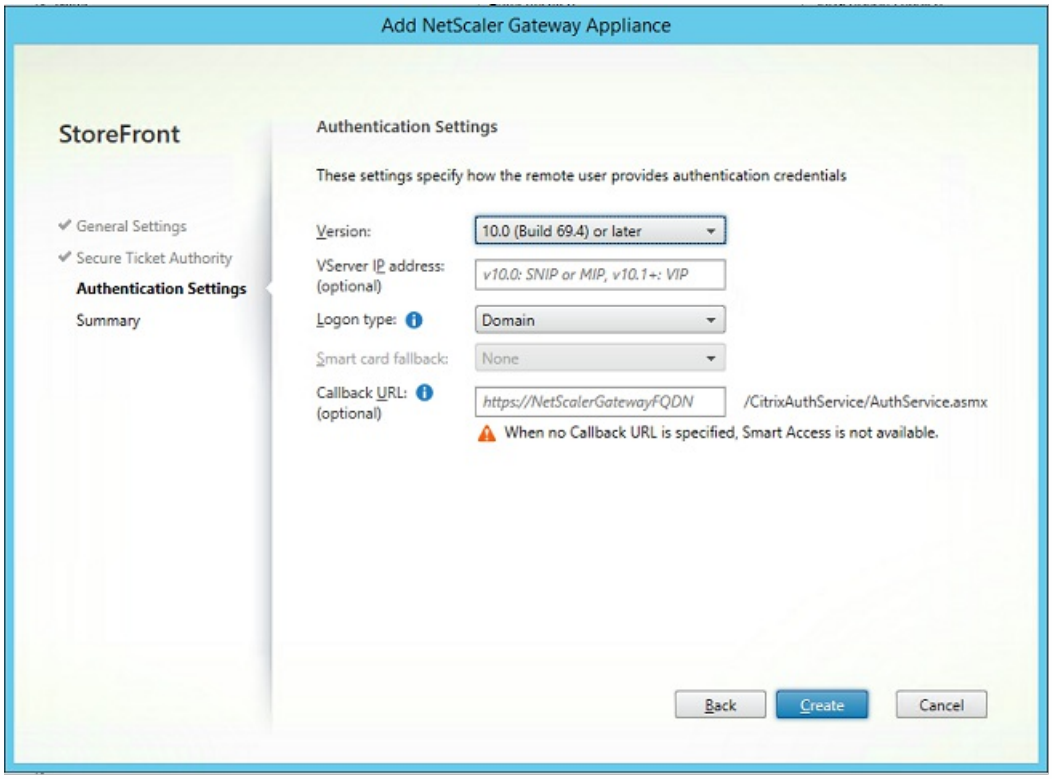
必须以类似于智能卡登录的方式配置 XenApp 或 XenDesktop 环境，CTX206156 对此过程进行了说明。

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

将 NetScaler 配置为主身份验证系统时，请确保 NetScaler 与 StoreFront 之间的所有连接都通过 TLS 确保安全。具体而言，

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

请务必将回调 URL 正确配置为指向 NetScaler 服务器，因为这可用于对此部署中的 NetScaler 服务器进行身份验证。



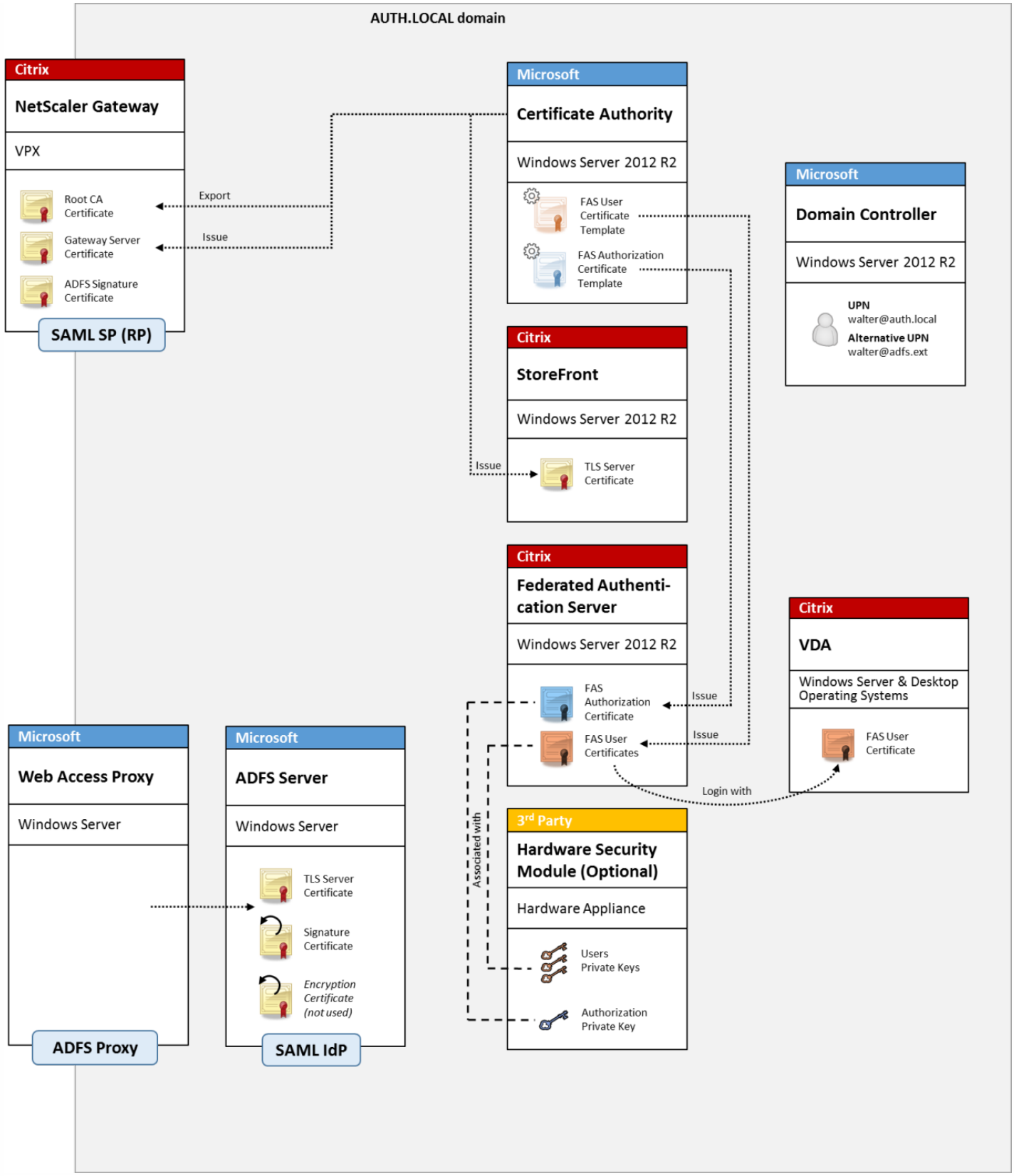
相关信息：

- 要配置 NetScaler Gateway，请参阅 How to Configure NetScaler Gateway 10.5 to use with StoreFront 3.6 and XenDesktop 7.6（如何配置 NetScaler Gateway 10.5 以与 StoreFront 3.6 和 XenDesktop 7.6 配合使用）。
- 联合身份验证服务一文介绍了如何安装和配置 FAS。

ADFS SAML 部署

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

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



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

相关信息：

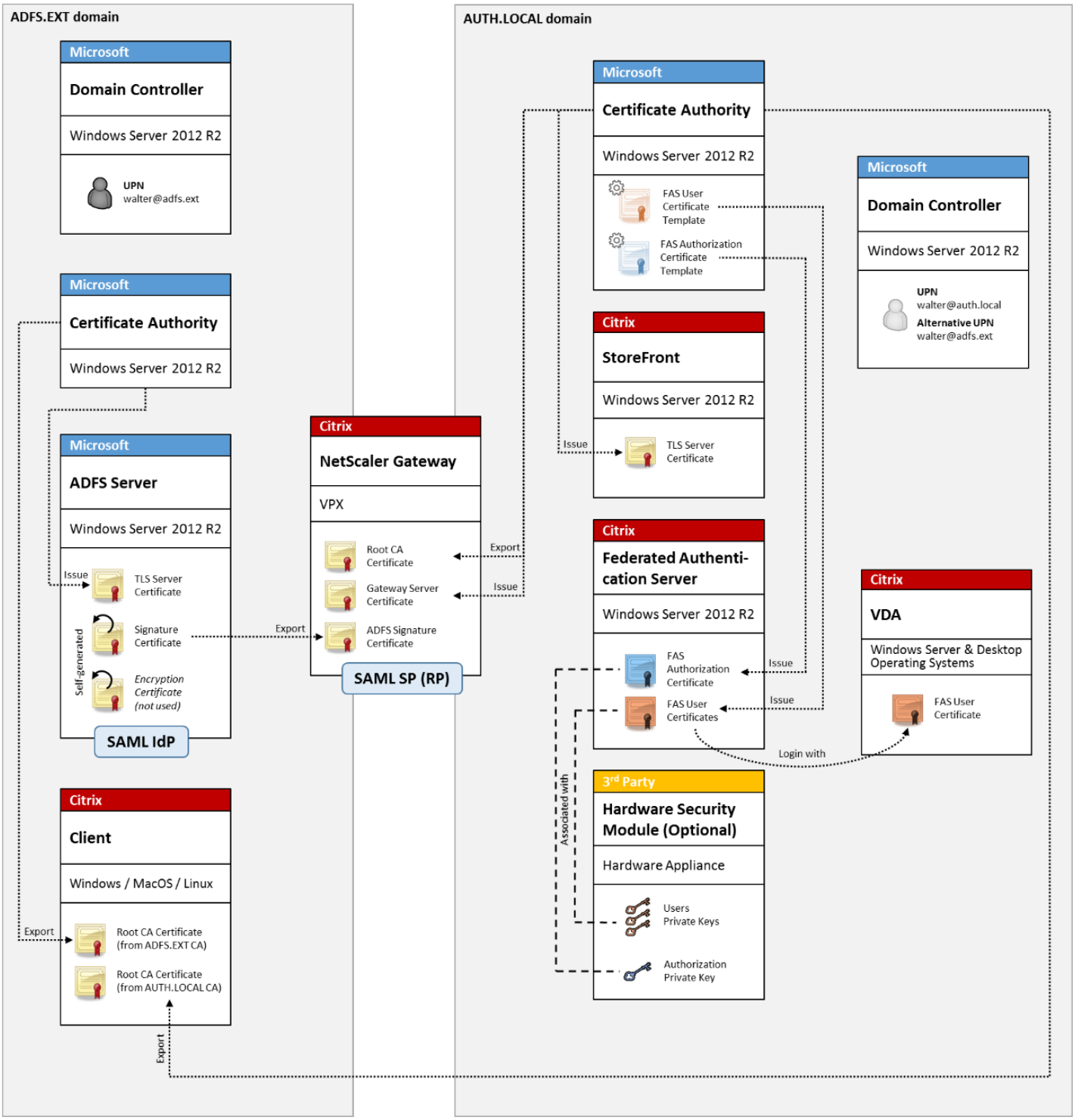
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 联合身份验证服务 ADFS 部署一文介绍了详细信息。
- 联合身份验证服务一文介绍了如何安装和配置 FAS。
- 本文中的 NetScaler Gateway 部署部分介绍了配置注意事项。

B2B 帐户映射

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

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



相关信息：

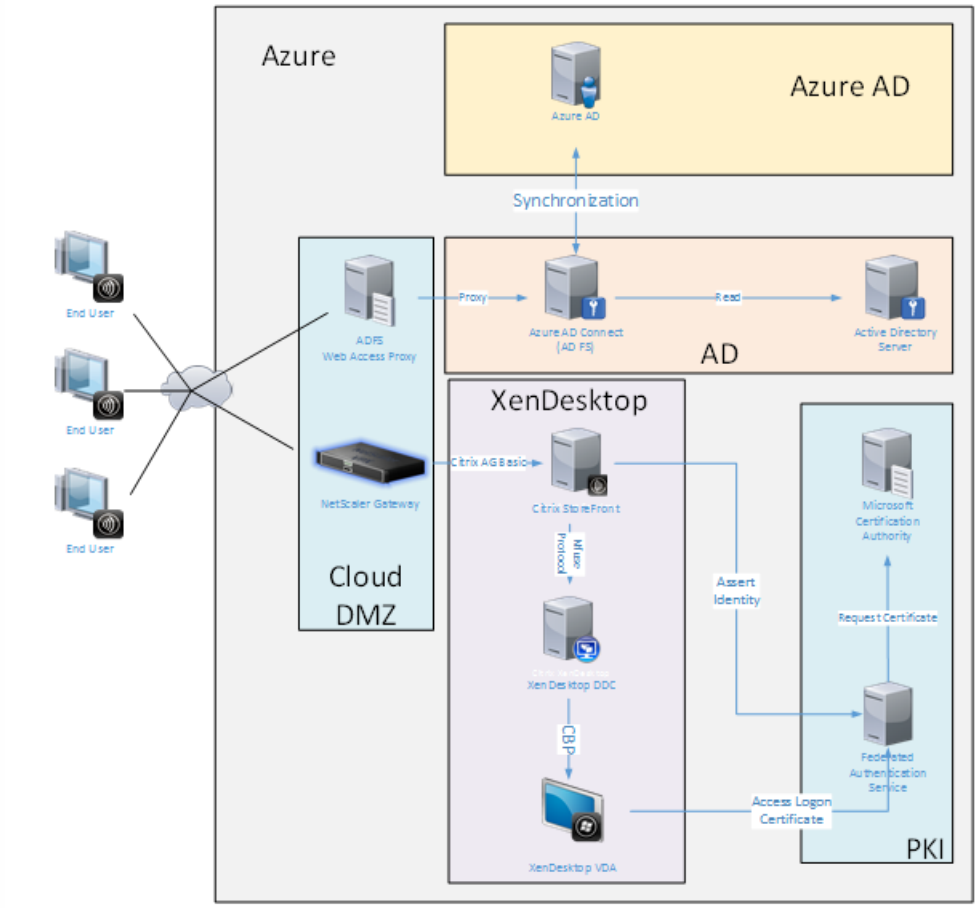
- 联合身份验证服务一文介绍了如何安装和配置 FAS。

Windows 10 Azure AD 联接

Windows 10 中引入了“Azure AD 联接”的概念，其概念与传统的 Windows 域加入类似，但主要针对“通过 Internet”的场景。此

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

功能特别适用于便携式计算机和平板电脑。与传统的 Windows 域加入相同，Azure AD 具有允许对公司 Web 站点和资源使用单点登录模式的功能。这些都能“识别 Internet”，因此，将从任何连接了 Internet 的位置进行工作，而非仅从办公室局域网进行工作。



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

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

相关信息：

- 联合身份验证服务一文介绍了如何安装和配置 FAS。
- 联合身份验证服务 Azure AD 集成一文介绍了详细信息。

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

联合身份验证服务 ADFS 部署

Dec 05, 2017

简介

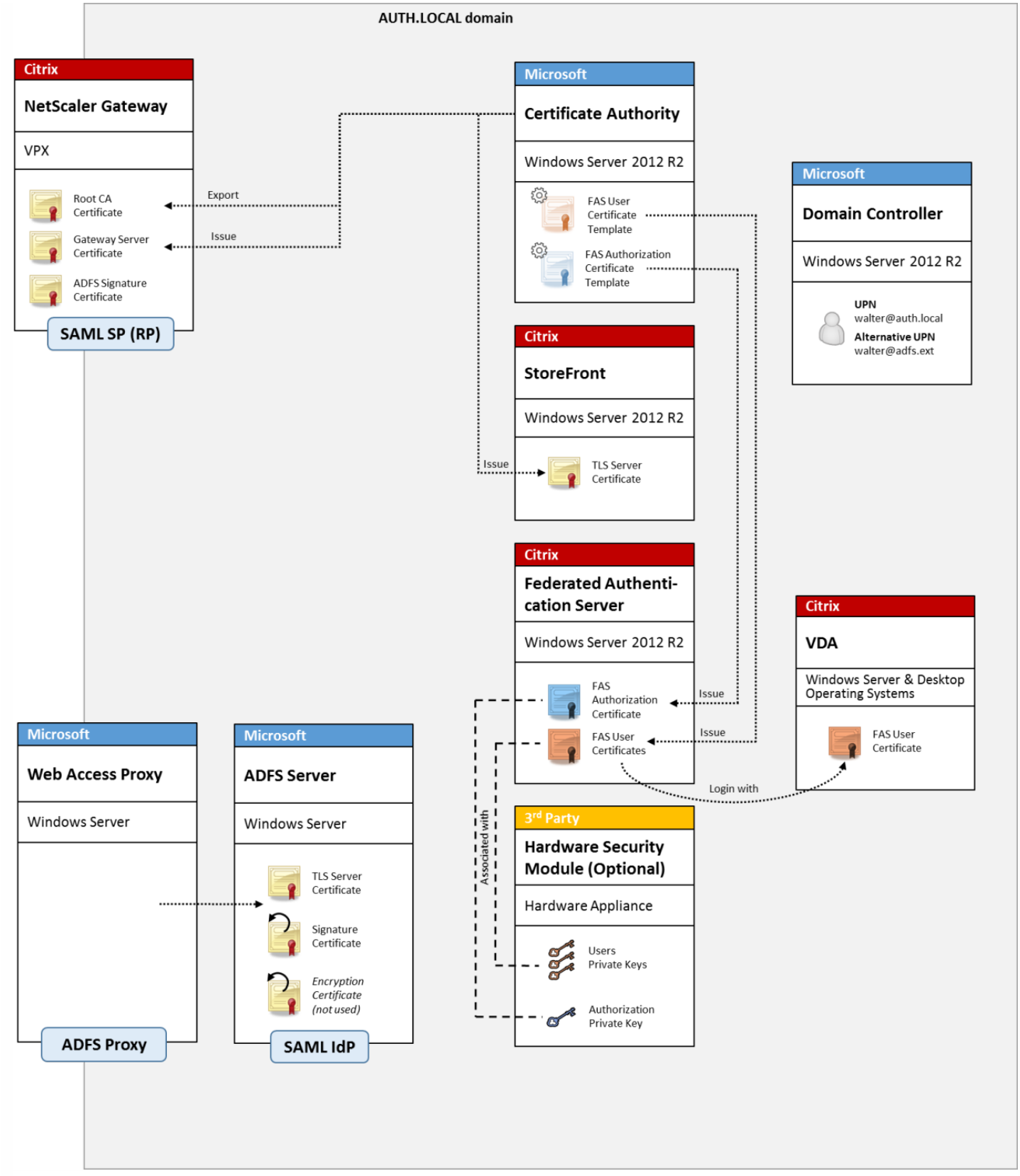
本文介绍了如何将 Citrix 环境与 Microsoft ADFS 相集成。

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

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

此部署集成 NetScaler 作为 Microsoft ADFS 的信赖方。

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



SAML 概述

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

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

重定向 URL [单点登录服务 URL]

NetScaler 发现用户需要进行身份验证时，会指示用户的 Web 浏览器在 ADFS 服务器上对 SAML 登录 Web 页面执行 HTTP POST。这通常是一个 https:// 地址，格式为 https://adfs.mycompany.com/adfs/ls。

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

标识符 [颁发者名称/实体 ID]

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

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

返回地址 [答复 URL]

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

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

签名证书 [IDP 证书]

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

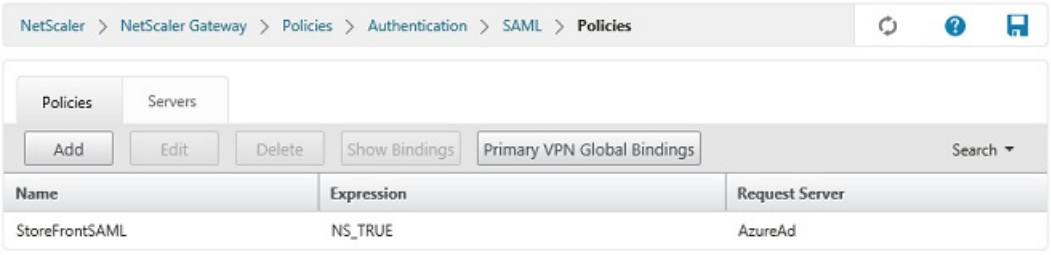
单点注销 URL [单点注销 URL]

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

这是一项可选功能，不需要配置。这通常是一个 https:// 地址，格式为 https://adfs.mycompany.com/adfs/logout。（请注意，此地址可以与单点登录 URL 相同。）

配置

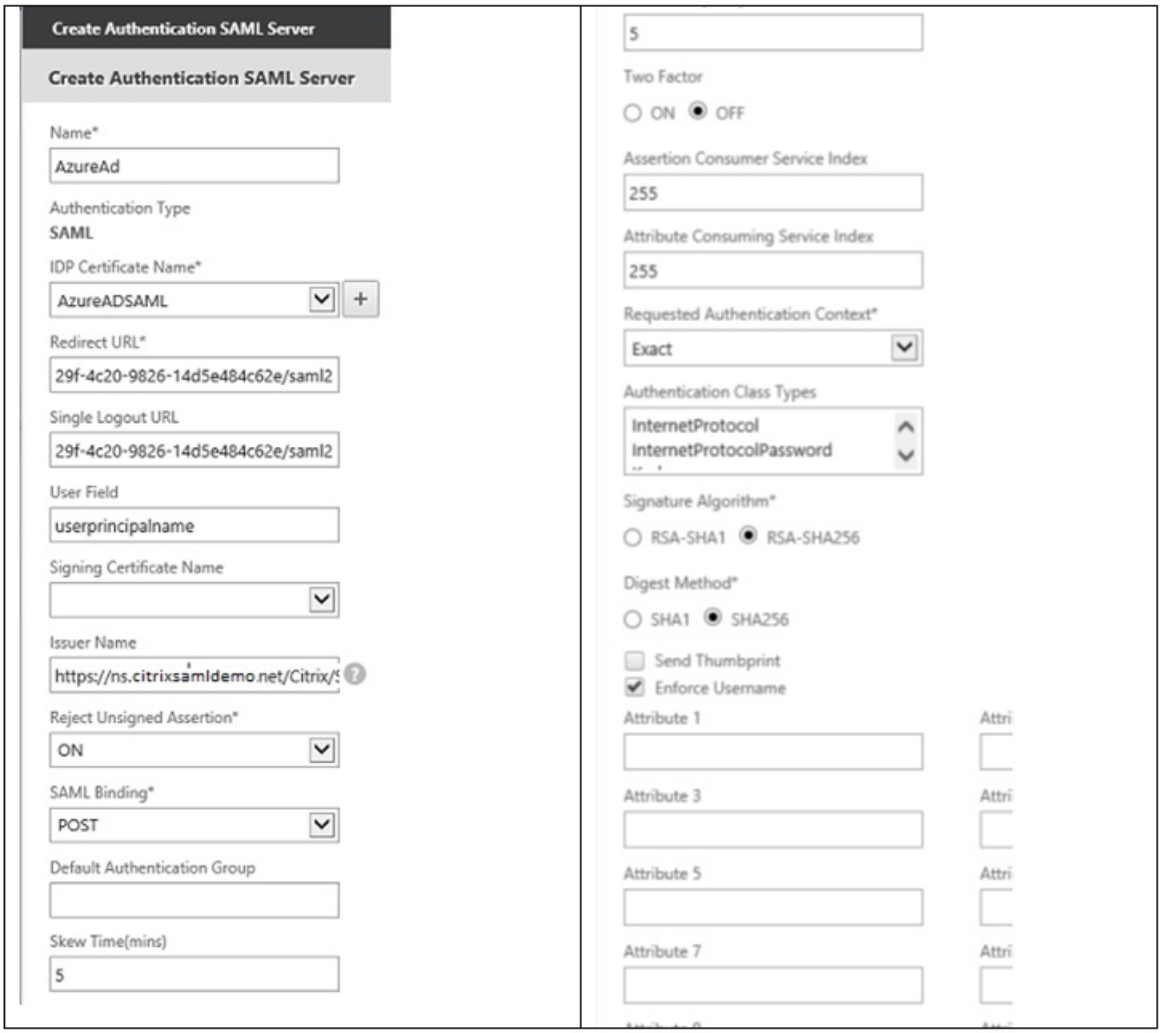
联合身份验证服务体系结构一文中的 NetScaler Gateway 部署部分介绍了如何使用 XenApp 和 XenDesktop NetScaler 设置向导设置 NetScaler Gateway 以处理标准 LDAP 身份验证选项。成功完成设置后，可以在 NetScaler 上创建一条允许进行 SAML 身份验证的新身份验证策略。此策略以后可以替换 NetScaler 安装向导使用的默认 LDAP 策略。



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

填充 SAML 策略

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



相关信息

- 联合身份验证服务一文是 FAS 安装和配置的主要参考资料。
- 通用 FAS 部署在联合身份验证服务体系结构概述一文中加以概括。
- 联合身份验证服务配置和管理一文介绍了“操作指南”文章。

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

联合身份验证服务 Azure AD 集成

Dec 05, 2017

在本文中：

- 简介
- 体系结构
- 创建 DNS 区域
- 创建云服务
- 创建 Windows 虚拟机
- 配置内部 DNS
- 配置外部 DNS 地址
- 配置安全组
- 创建 ADFS 证书
- 设置 Azure AD
- 启用 Azure AD 联接
- 安装 XenApp 或 XenDesktop
- 配置新 Azure AD 应用程序以单点登录到 StoreFront
- 安装并配置 NetScaler Gateway
- 配置 StoreFront 地址
- 启用 NetScaler SAML 身份验证支持
- 验证端到端系统
- 附录

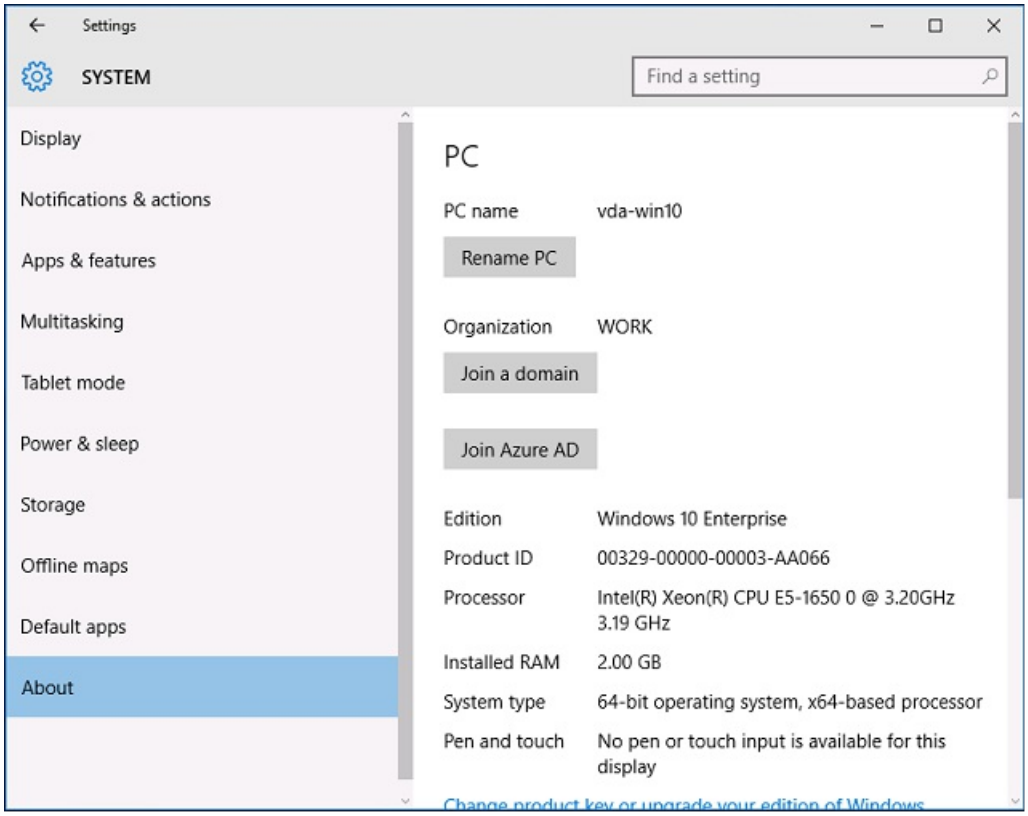
简介

本文档介绍如何将 Citrix 环境与 Windows 10 Azure AD 功能相集成。

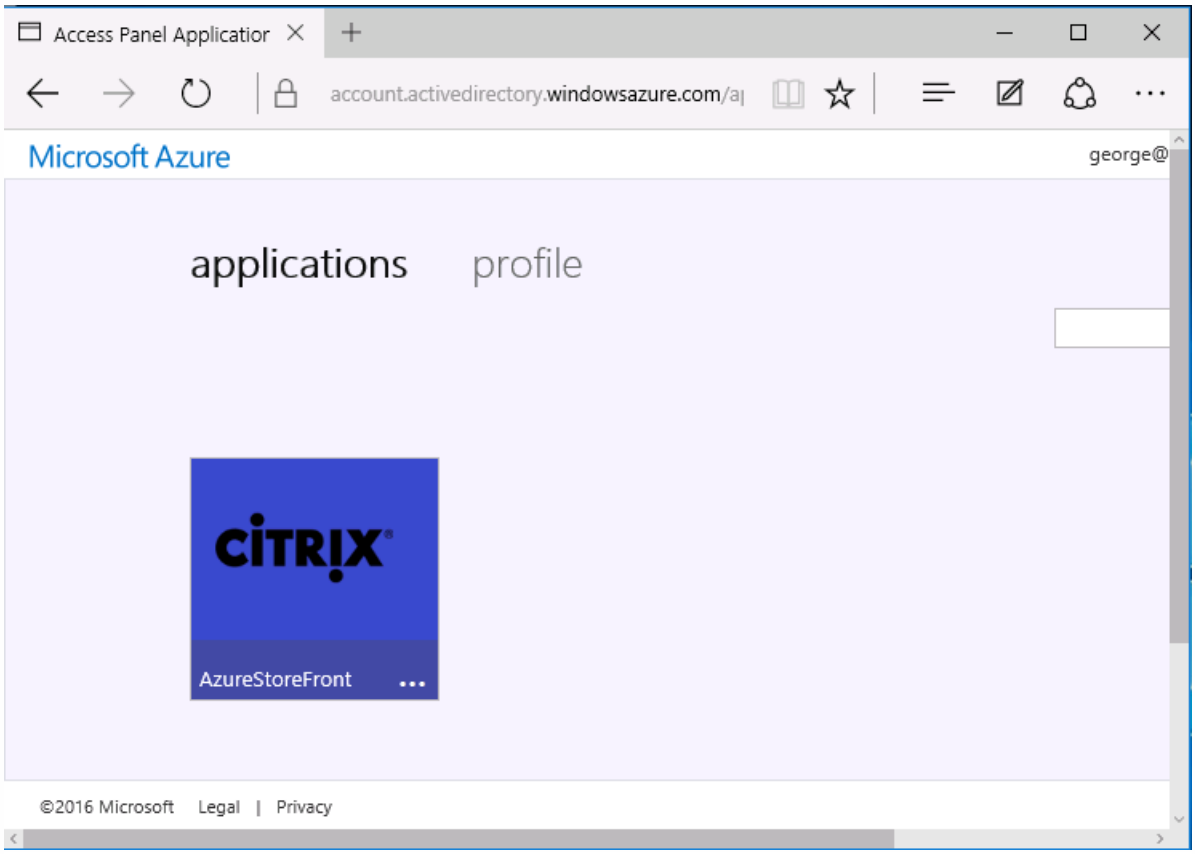
Windows 10 中引入了 Azure AD，这是一个新的域加入模块，可以在此模块中通过 Internet 将漫游便携式计算机加入企业域，以便进行管理和单点登录。

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

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



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

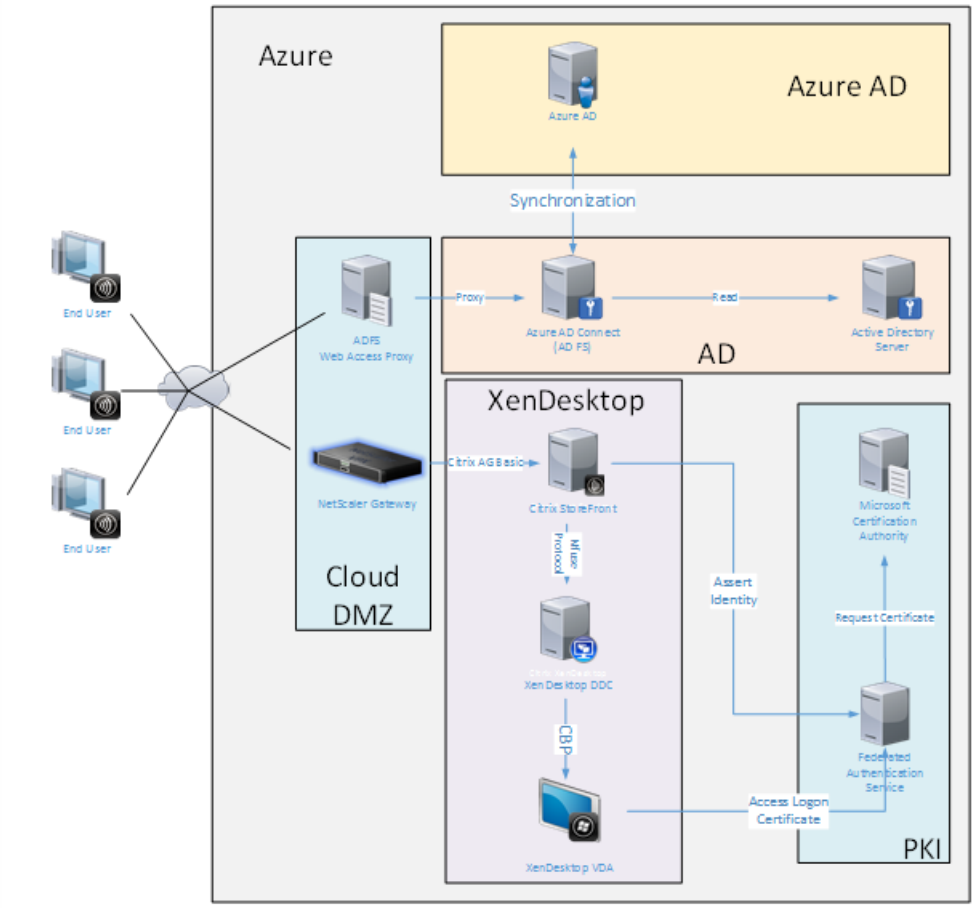


© 1999-2017 Citrix Systems, Inc. All rights reserved.

体系结构

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

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



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

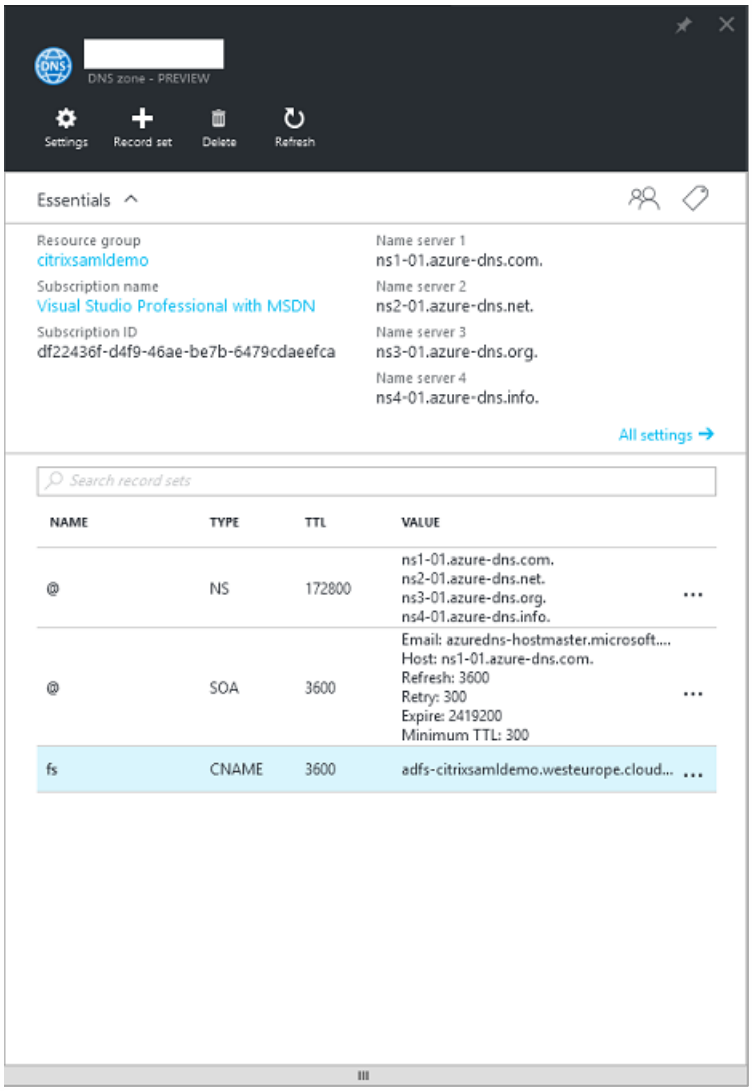
用户启动传统应用程序时，将使用 XenApp 和 XenDesktop 的已发布应用程序进行访问。 不同类型的应用程序使用 Microsoft Edge 的单点登录功能通过用户的 **Azure 应用程序**页面进行整理。 Microsoft 还提供能够枚举和启动 Azure 应用程序的 Android 和 iOS 应用程序。

创建 DNS 区域

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

下例使用 DNS 区域名称“citrixsamldemo.net”。

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



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

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

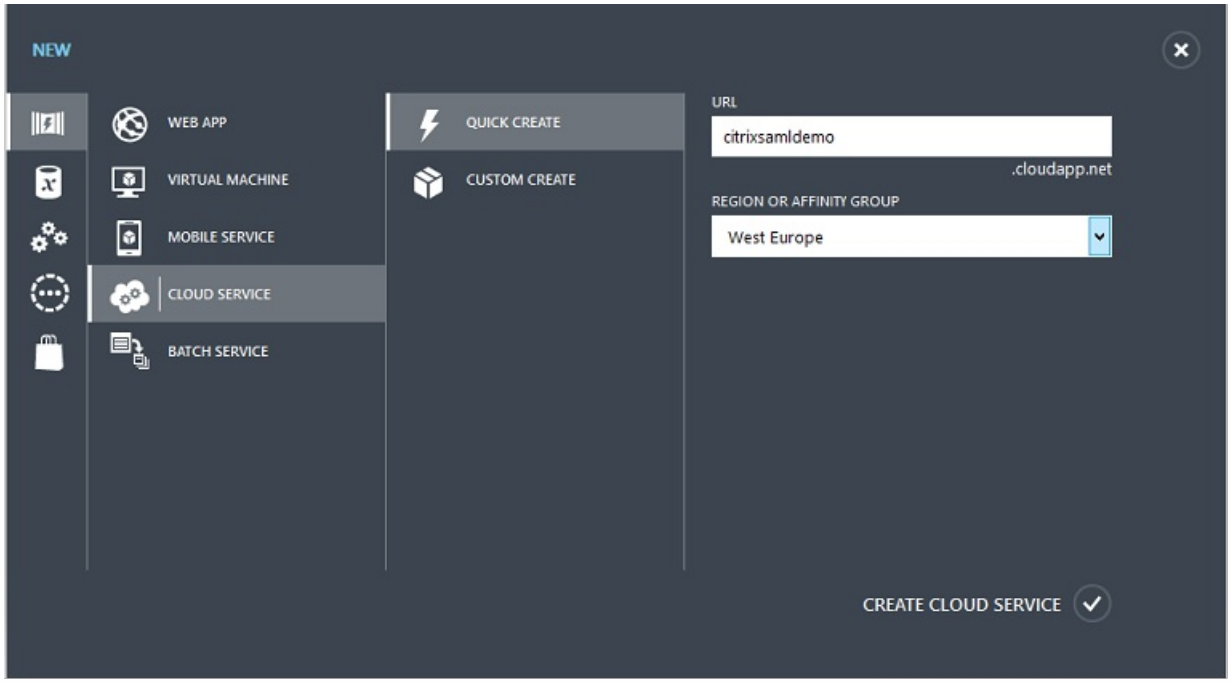
此部署的内部和外部 DNS 地址前缀都保持一致。 域为 citrixsamldemo.net，使用拆分 DNS（在内部为 10.0.0.*）。

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

创建云服务

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

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

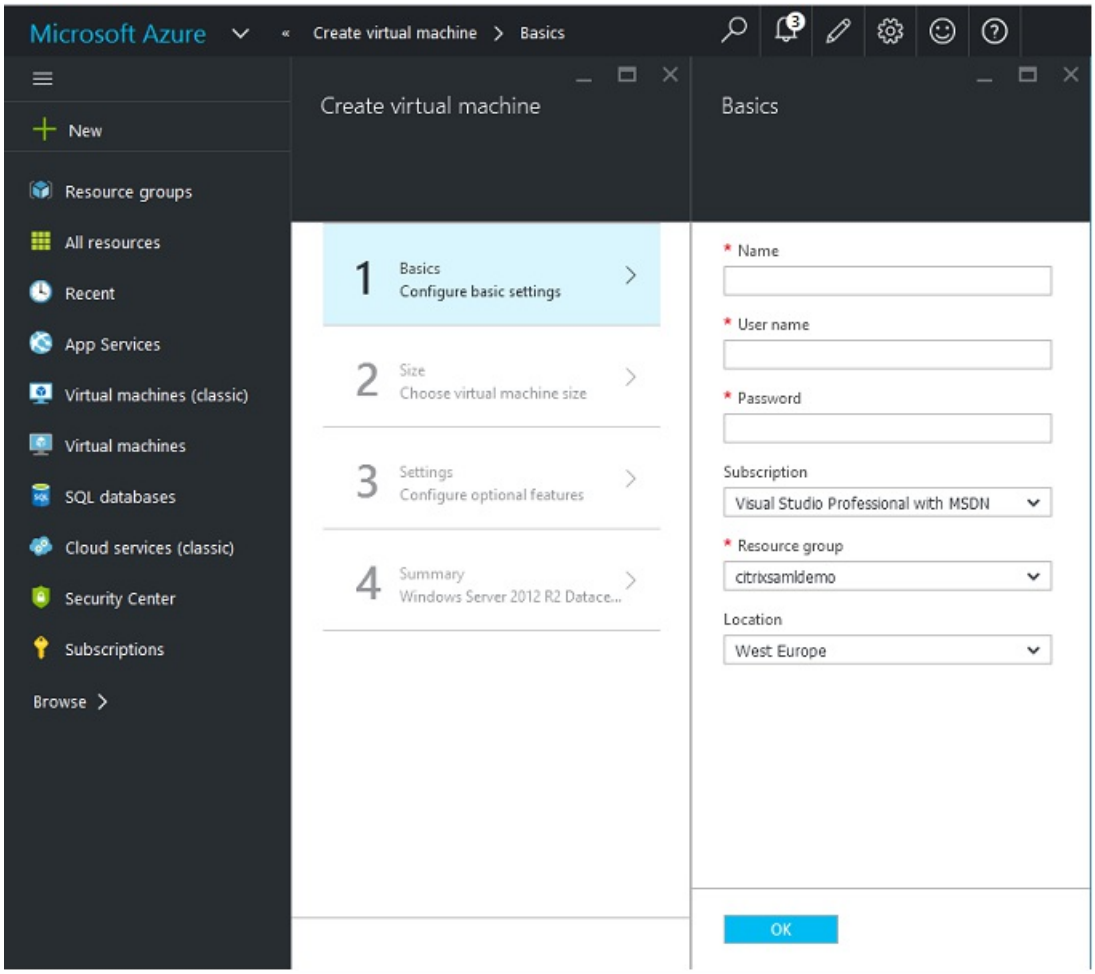


创建 Windows 虚拟机

创建五个在云服务中运行的 Windows VM：

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

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



域控制器

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

ADFS 控制器和 Web 应用程序代理服务器

- 将 ADFS 服务器加入到 citrixsamldemo domain 中。 Web 应用程序代理服务器应始终保留在独立的工作组中，因此，请手动向 AD DNS 注册 DNS 地址。
- 在这些服务器上运行 **Enable-PSRemoting –Force** cmdlet，以允许 PS 通过防火墙从 AzureAD Connect 工具远程连接。

XenDesktop Delivery Controller 和 VDA

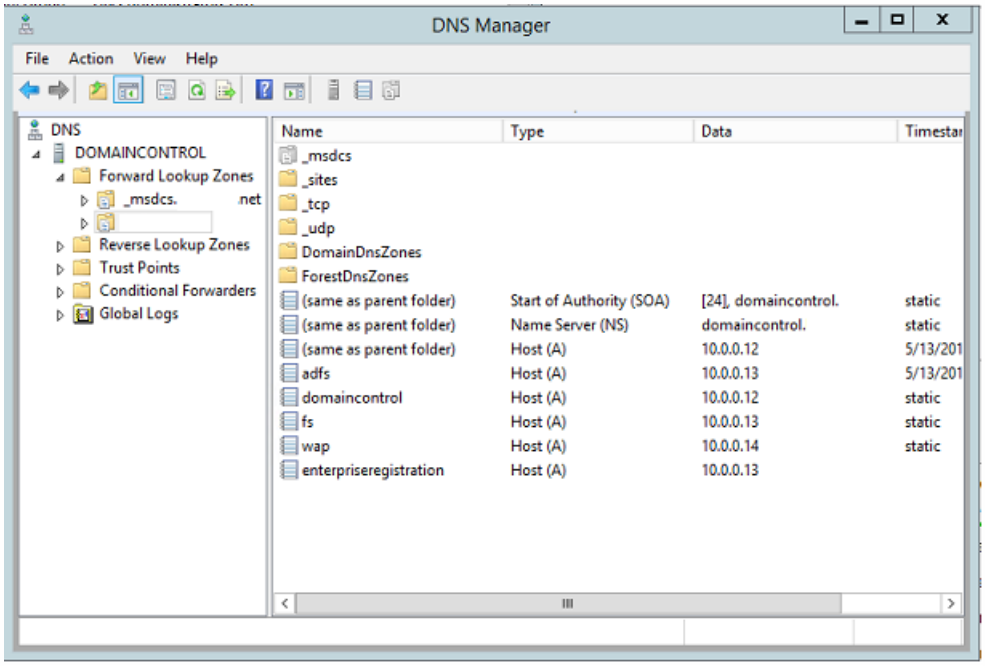
- 请在加入到 citrixsamldemo 的其余两个 Windows 服务器上安装 XenApp 或 XenDesktop Delivery Controller 以及 VDA。

配置内部 DNS

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

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

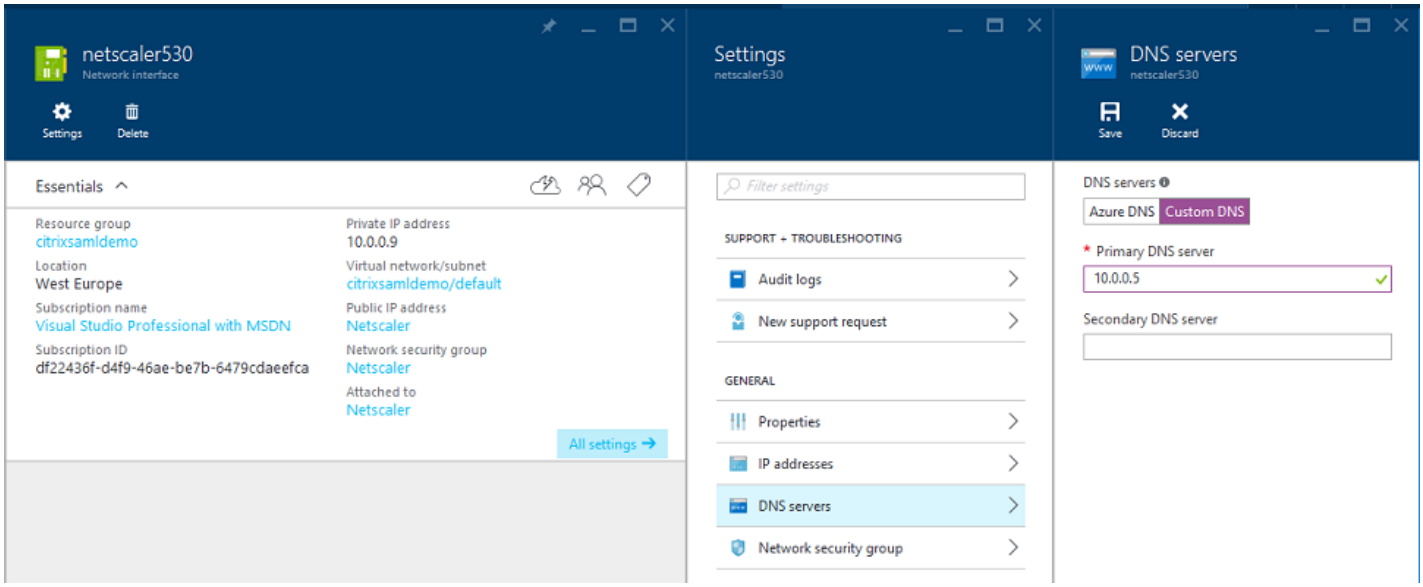
的转发器。



添加以下各项的静态记录：

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

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

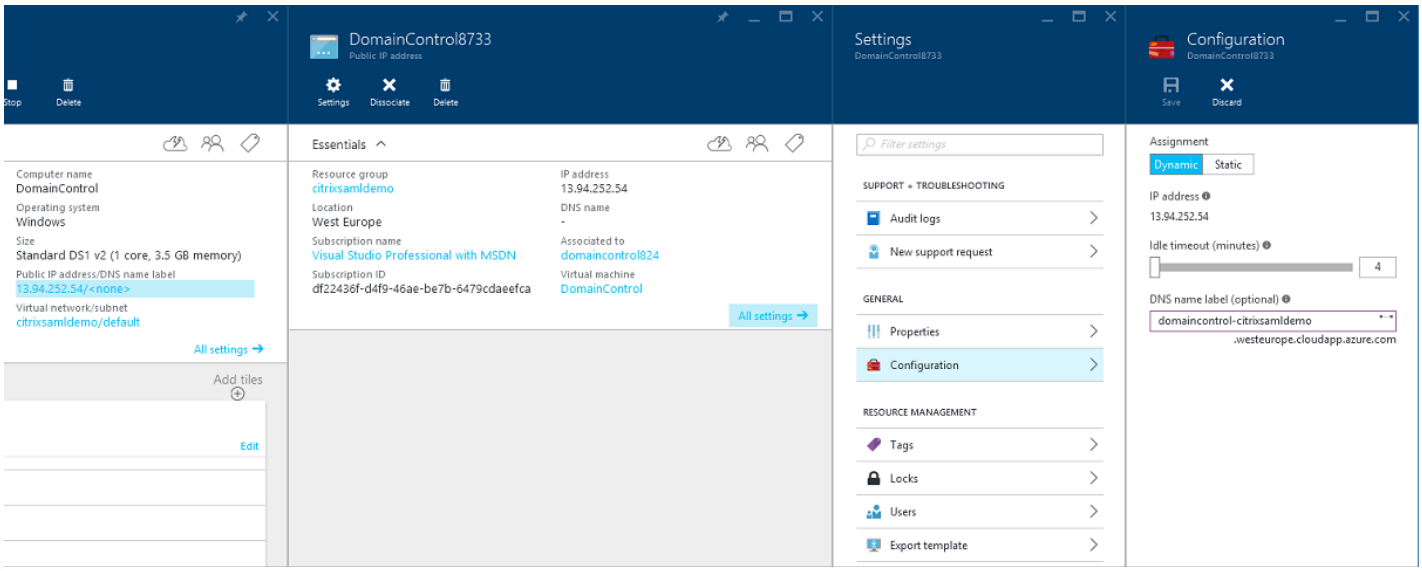


默认情况下，内部 IP (10.0.0.9) 地址动态分配。 可以使用 IP 地址设置永久分配 IP 地址。应对 Web 应用程序代理服务器和域控制器执行此操作。

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

配置外部 DNS 地址

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

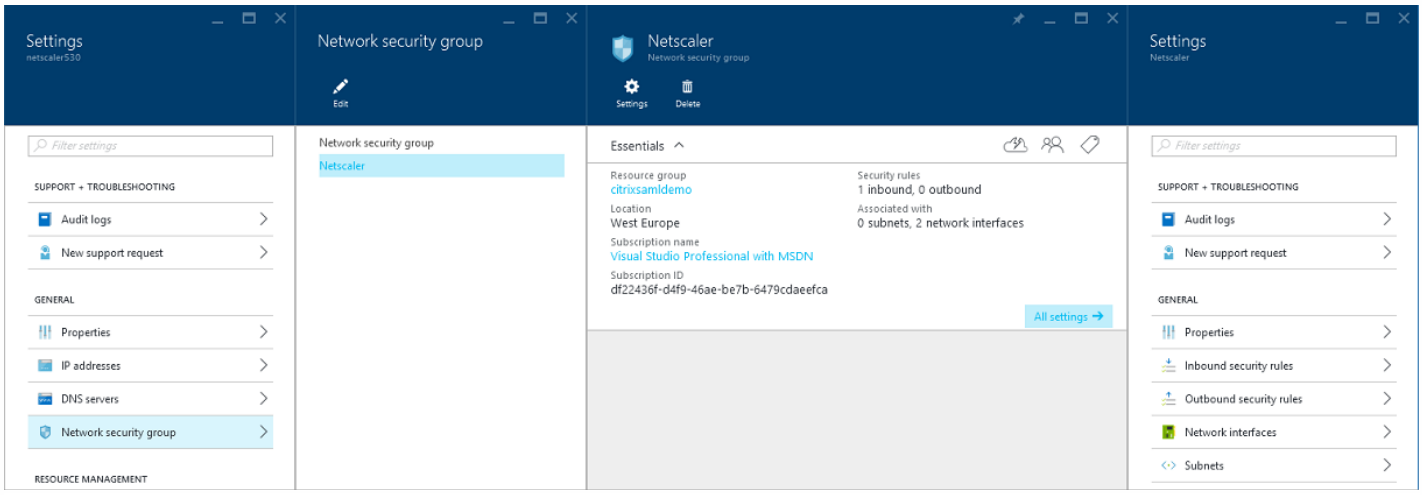


下例将 domaincontrol-citrixsamldemo.westeurope.cloudapp.azure.com 的 DNS 地址分配给域控制器。

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

配置安全组

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



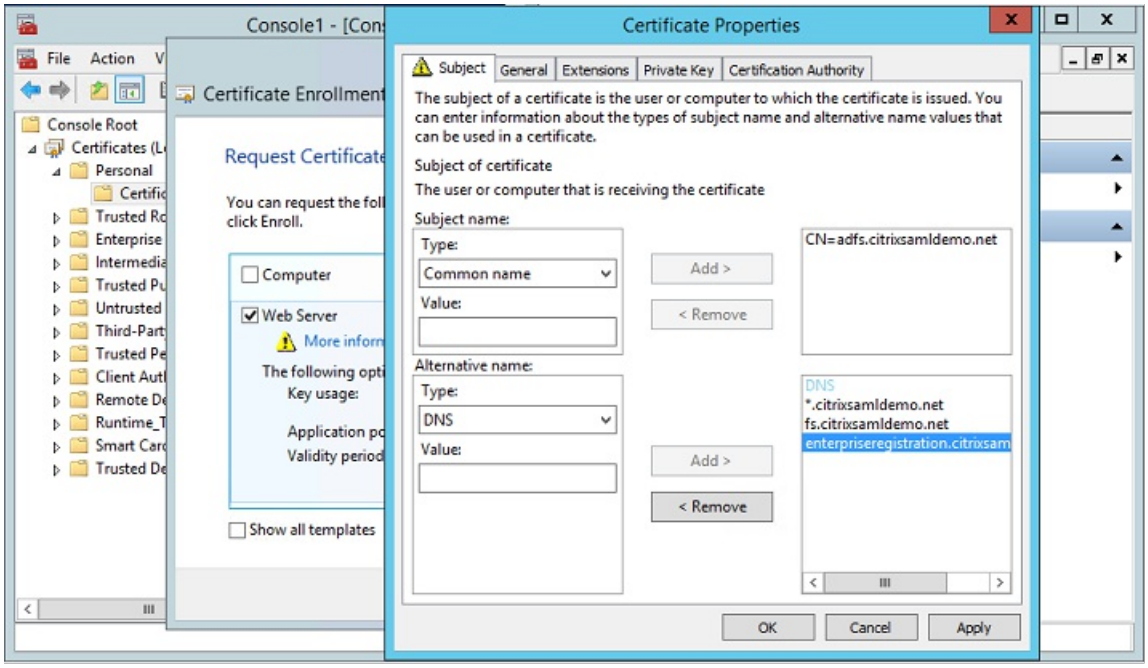
© 1999-2017 Citrix Systems, Inc. All rights reserved.

创建 ADFS 证书

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

颁发使用以下使用者名称的 Web 服务器证书：

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



将证书导出为 pfx 文件，包括受密码保护的私钥。

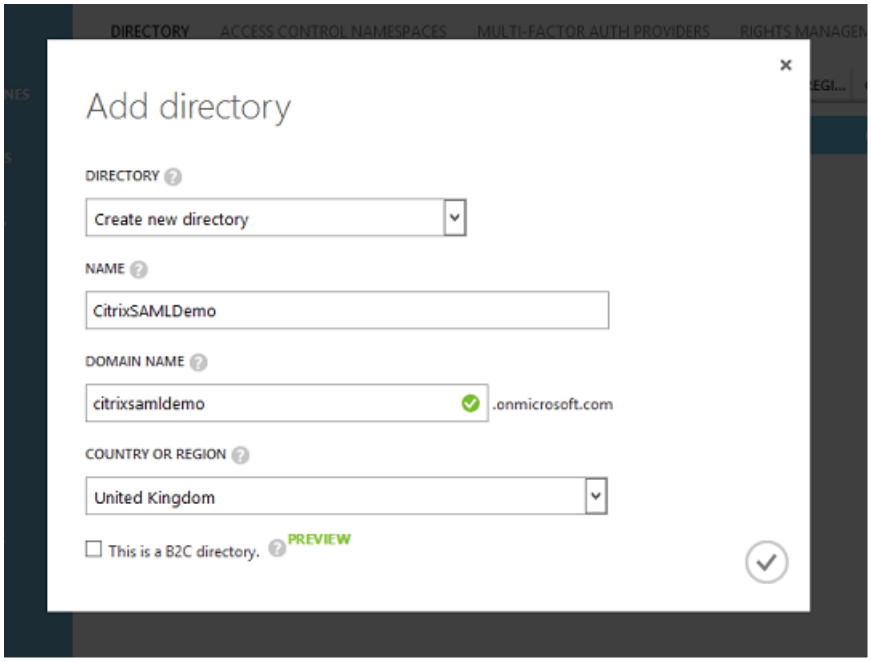
设置 Azure AD

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

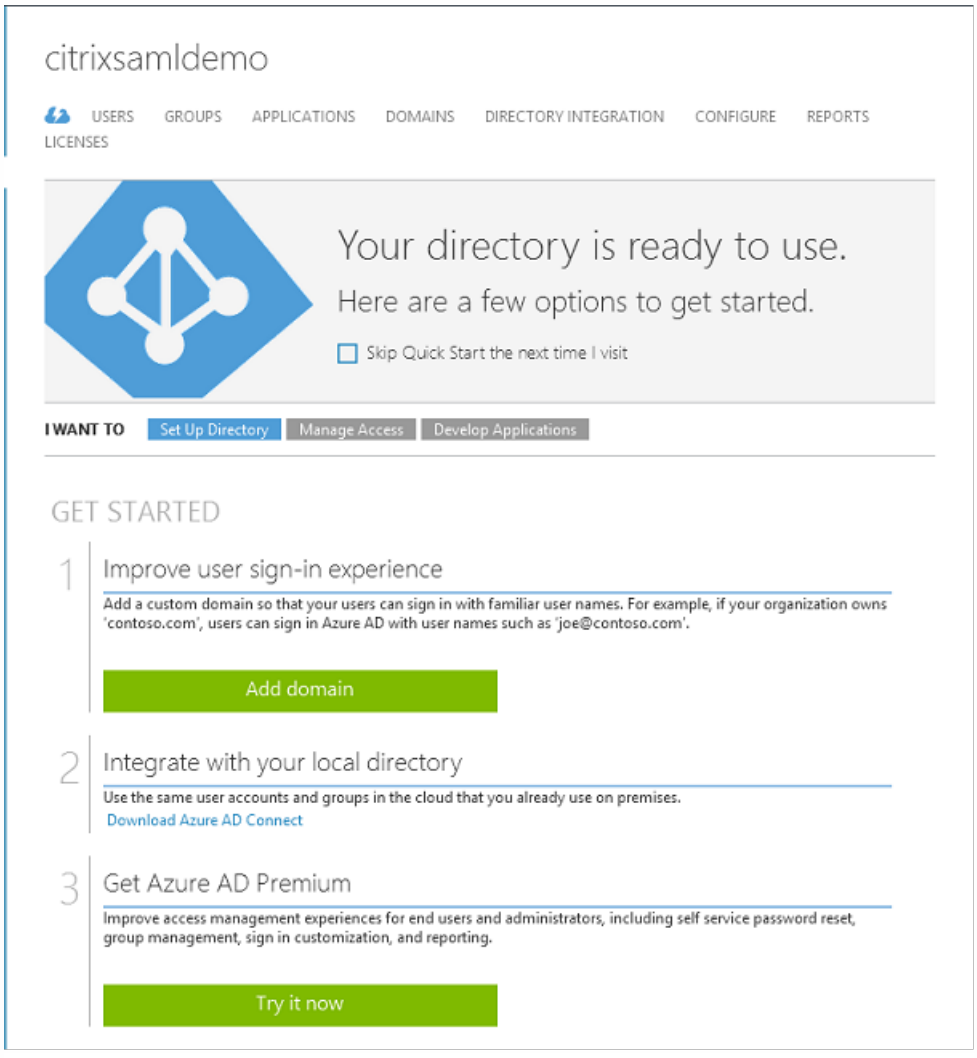
创建新目录

登录经典 Azure 门户并创建一个新目录。

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



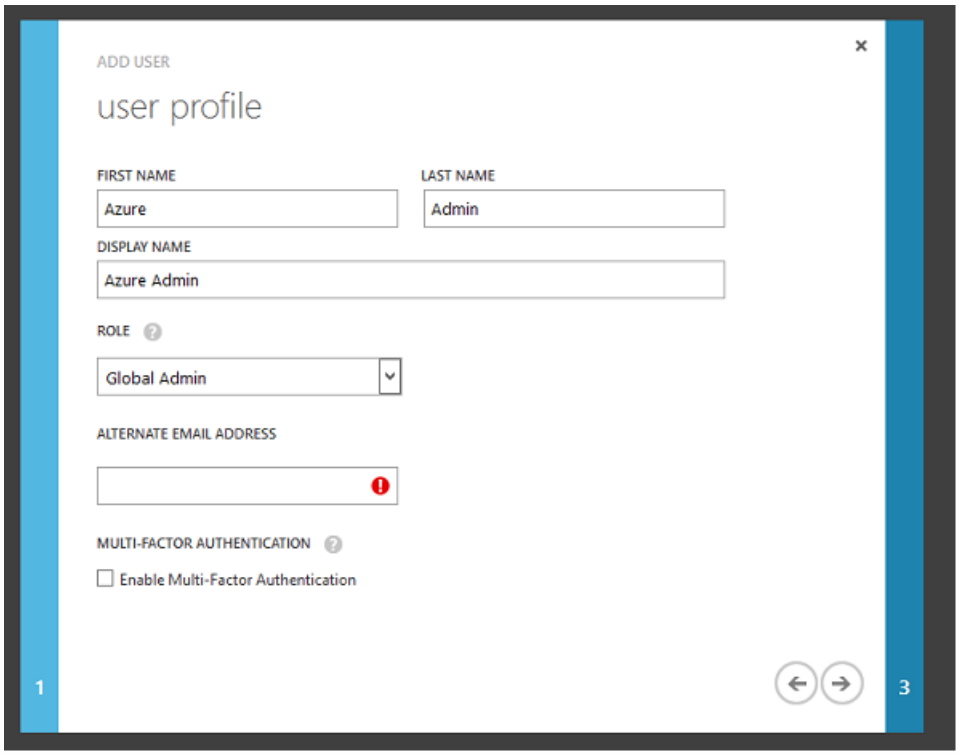
完成时，将显示一个摘要页面。



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

创建全局管理员用户 (AzureAdmin)

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



在 Azure AD 中注册您的域

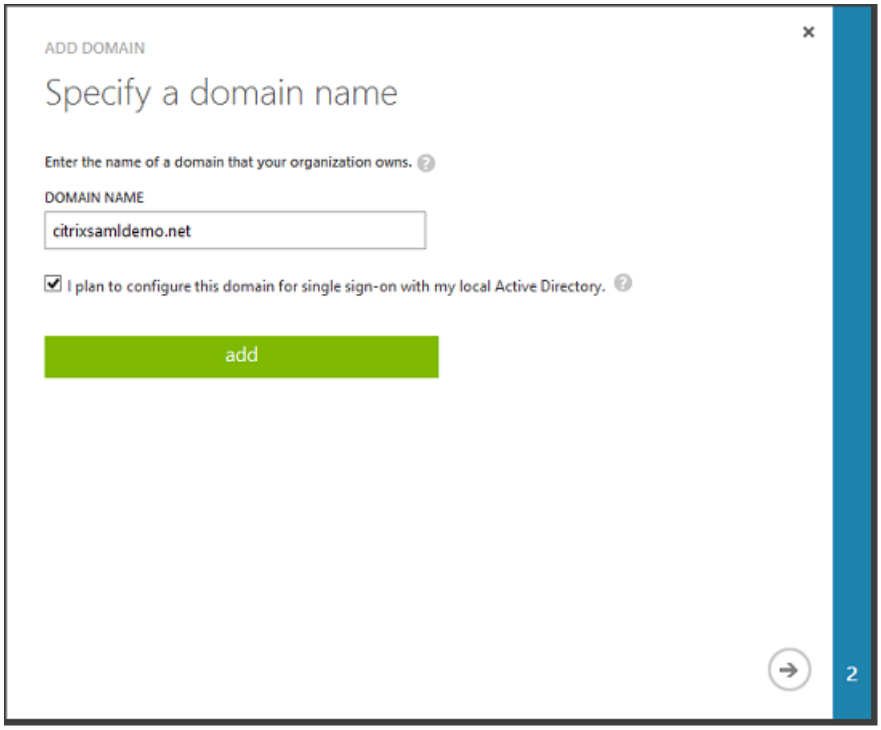
默认情况下，用户通过格式为 *<user.name>@<company>.onmicrosoft.com 的电子邮件地址进行标识。*

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

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

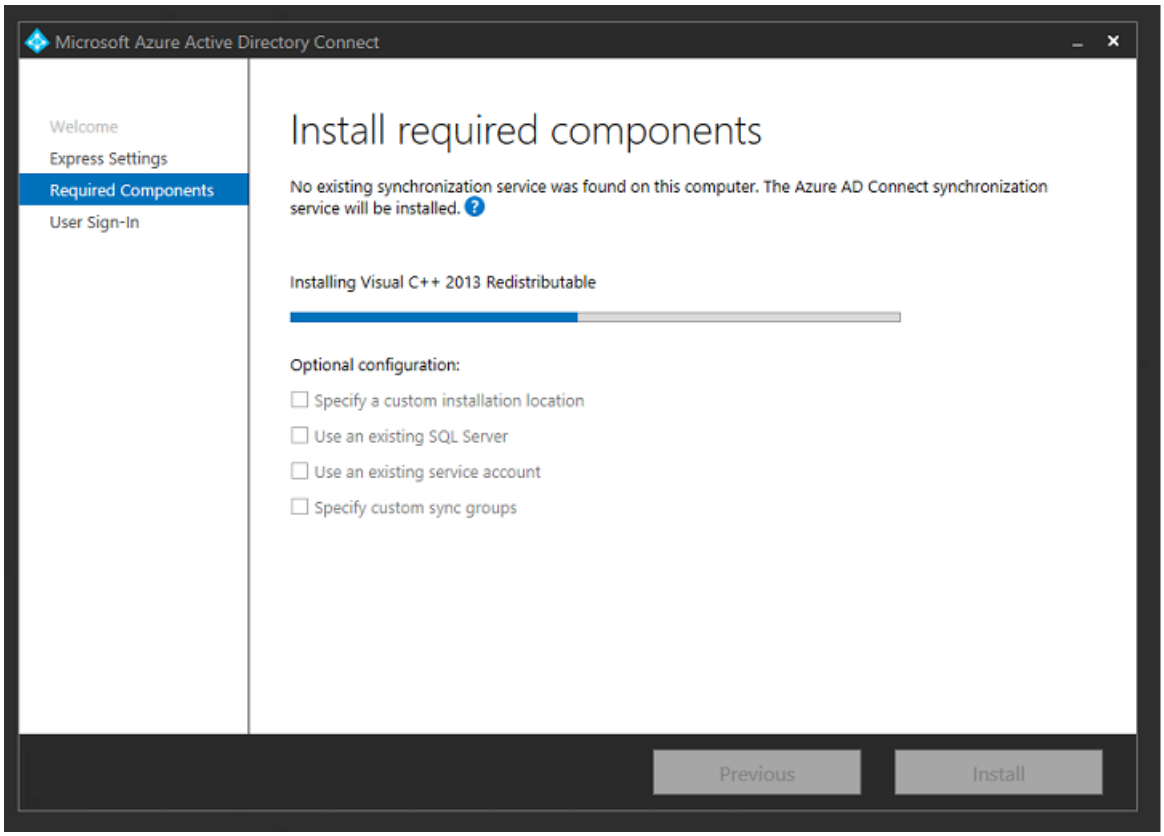
如果要设置 ADFS 以便进行单点登录，请启用该复选框。

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



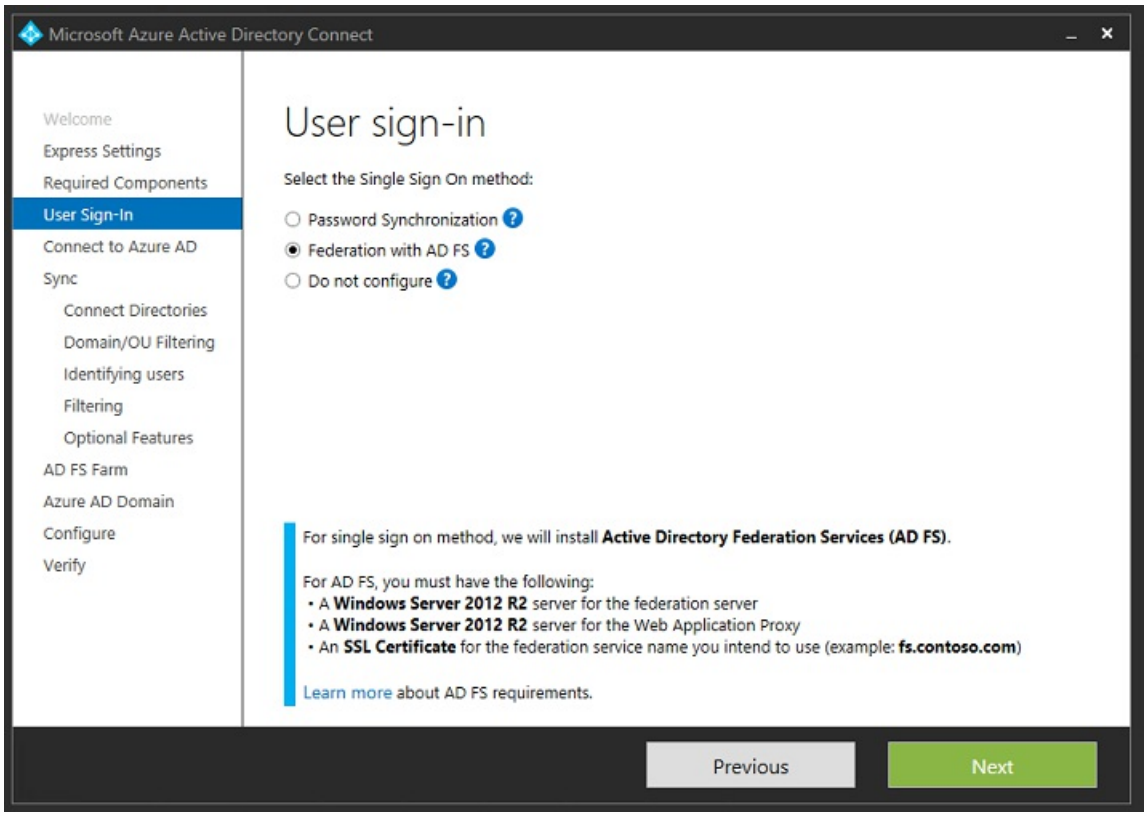
安装 Azure AD Connect

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

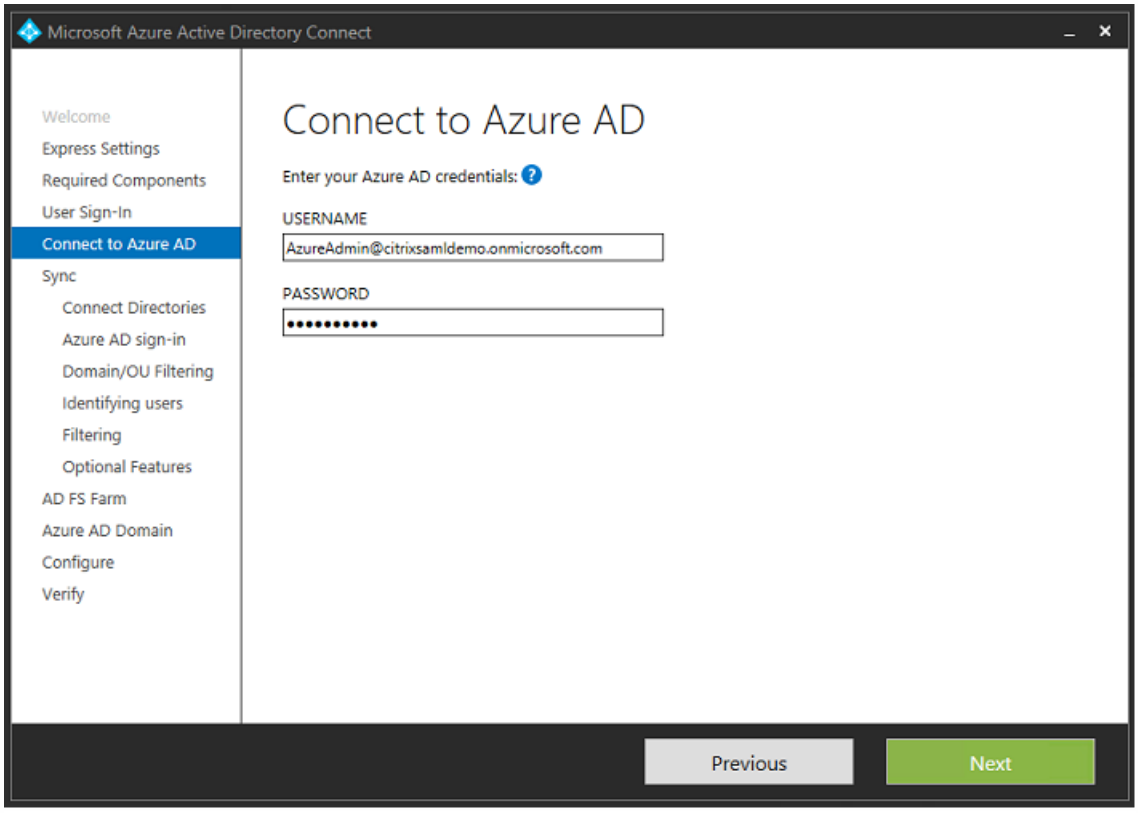


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

选择**使用 AD FS 进行联合身份验证**单点登录选项。

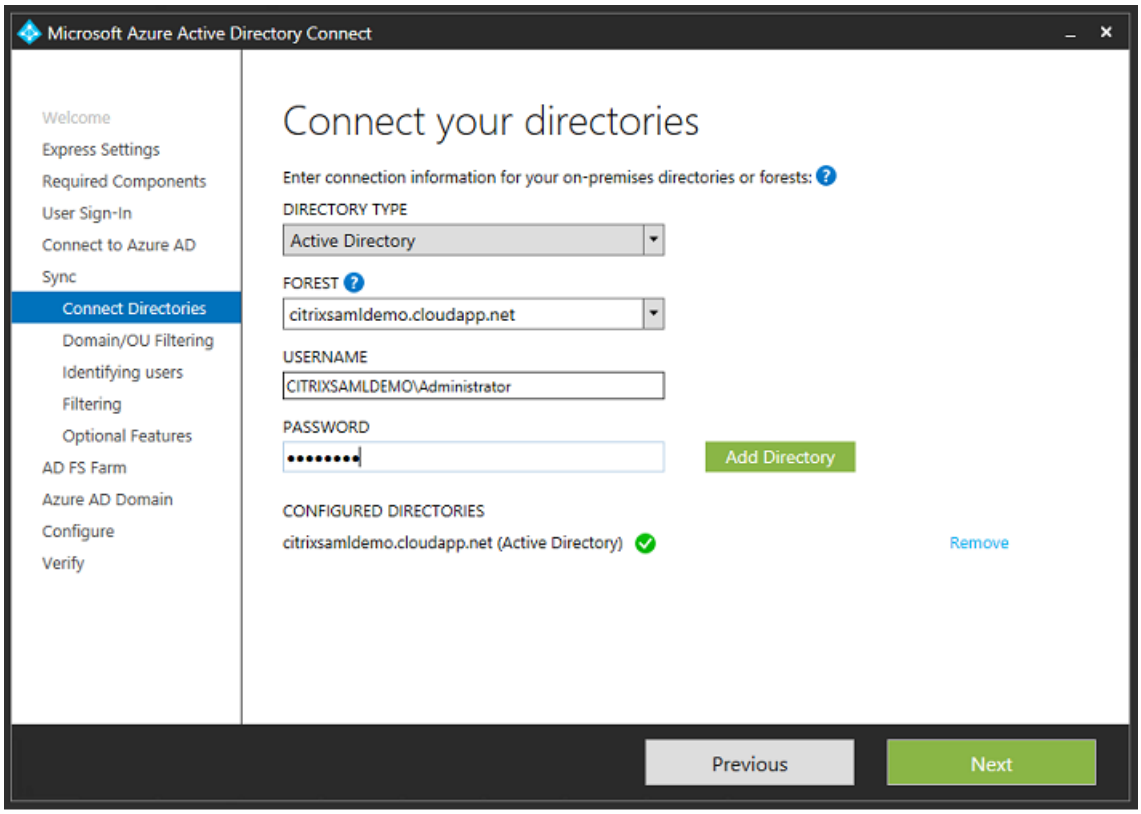


使用之前创建的管理员帐户连接到 Azure。

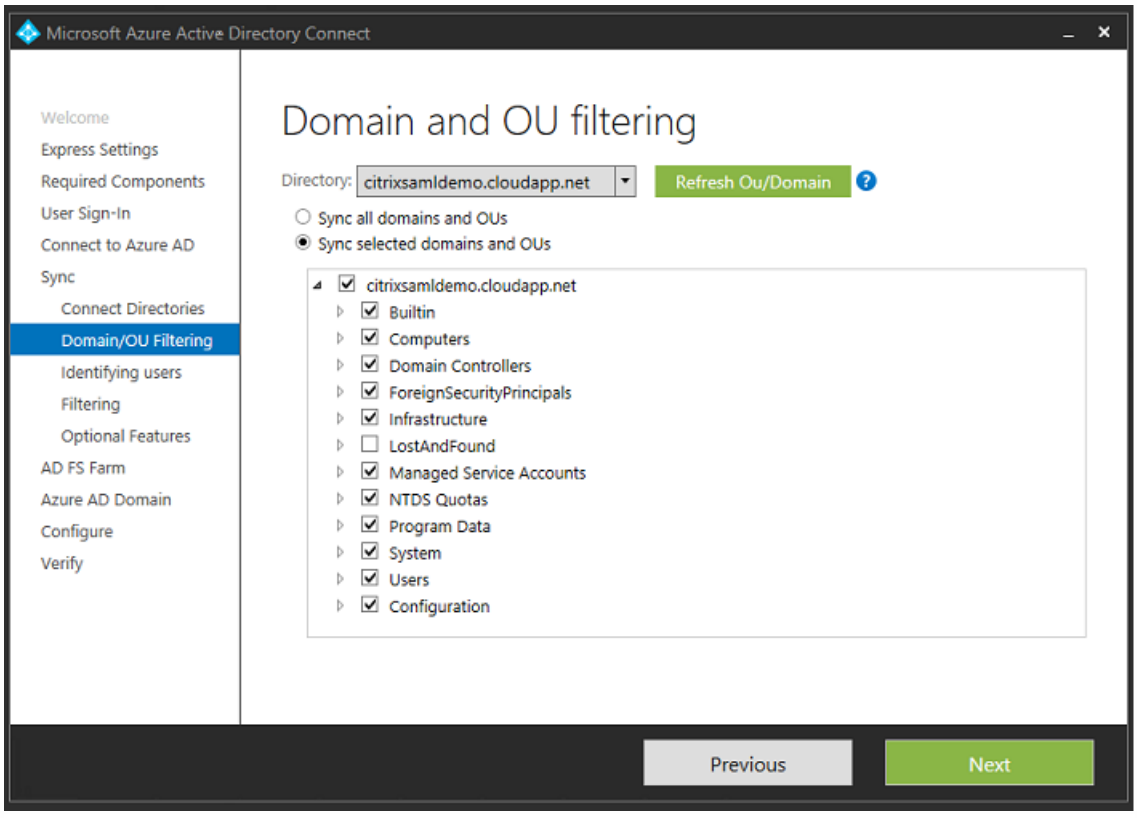


© 1999-2017 Citrix Systems, Inc. All rights reserved.

选择内部 AD 林。

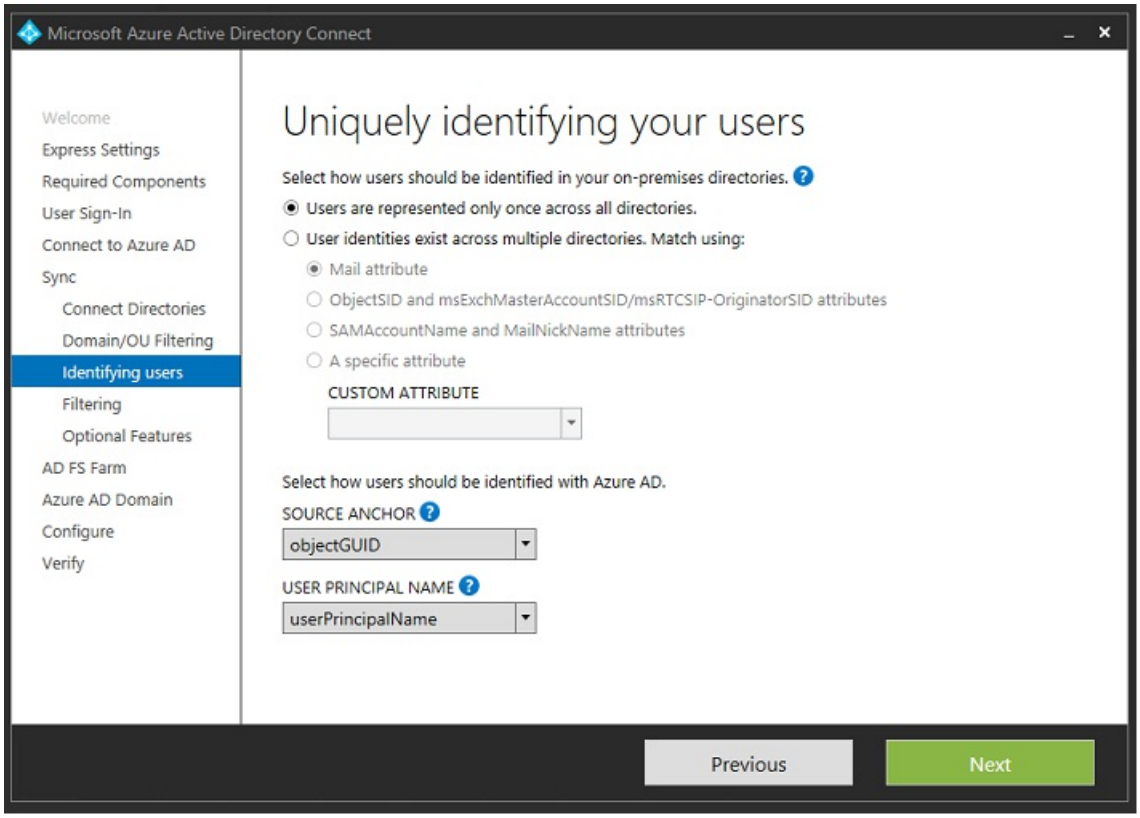


将所有旧 Active Directory 对象与 Azure AD 同步。

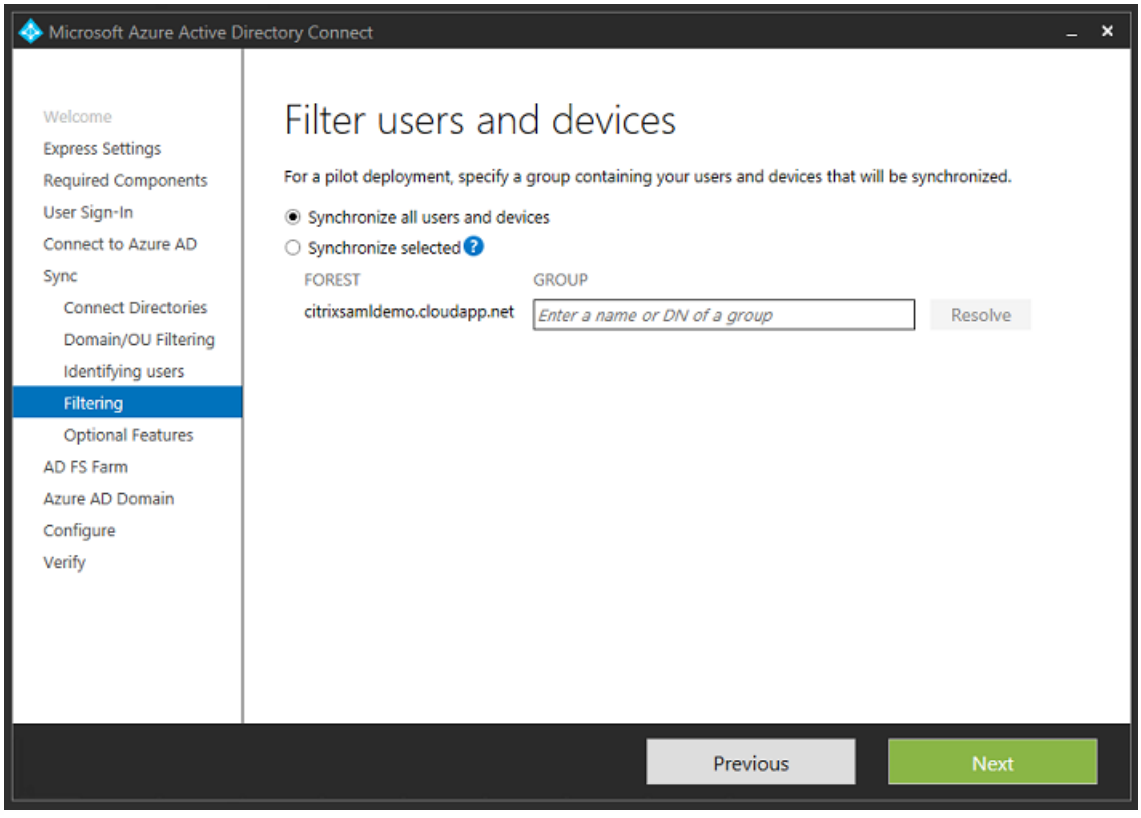


© 1999-2017 Citrix Systems, Inc. All rights reserved.

如果目录结构非常简单，可以依靠足够独特的用户名来识别登录的用户。

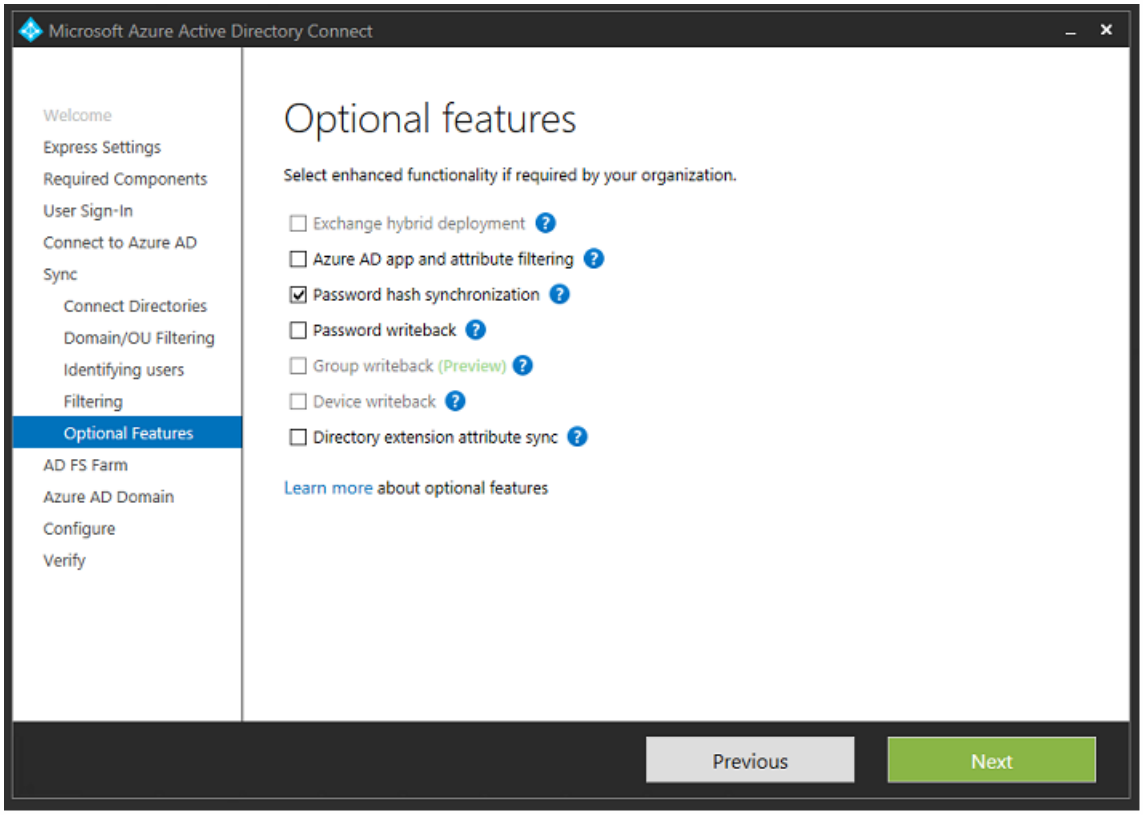


接受默认过滤选项，或者将用户和设备限制为一组特定的用户和设备。



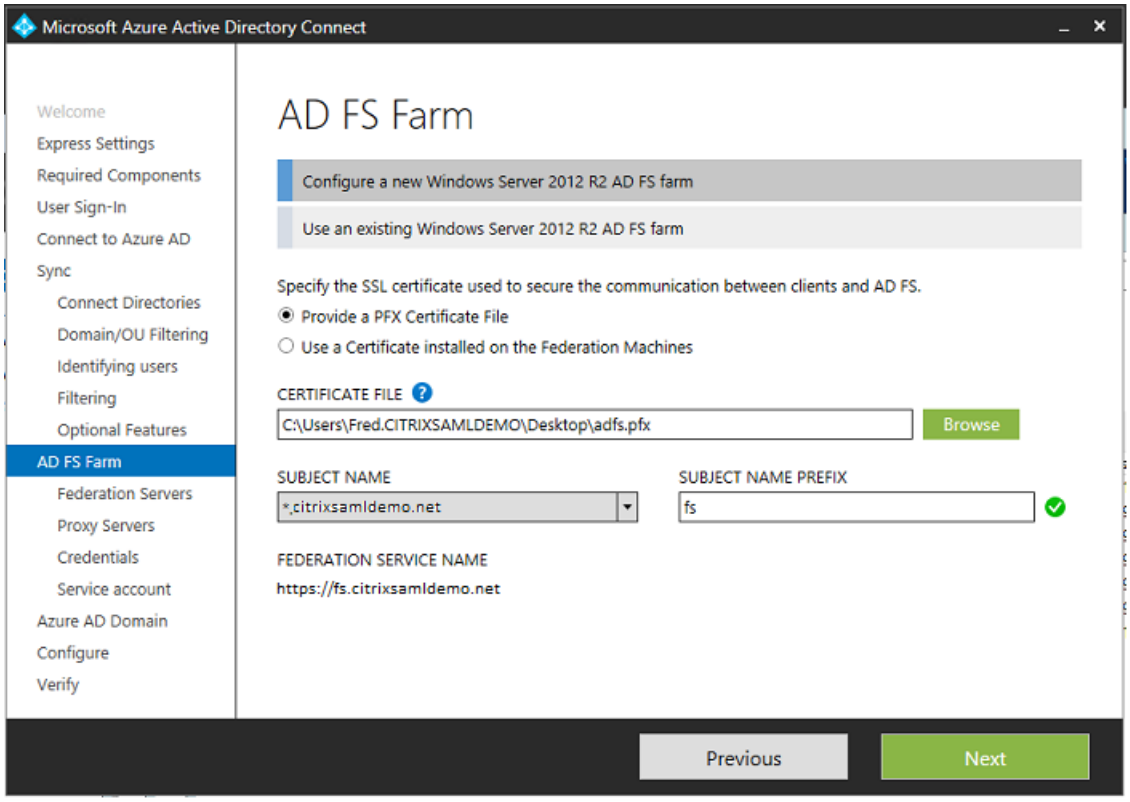
© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

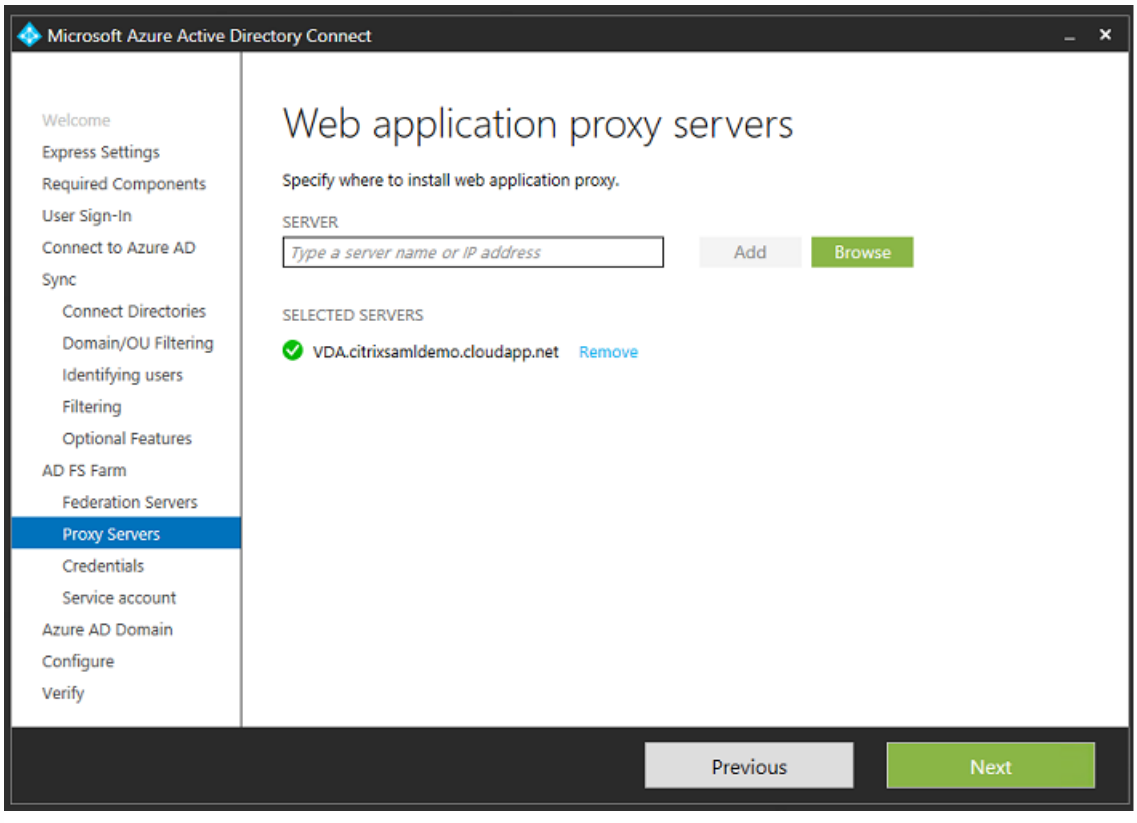


选择要在 AD FS 中使用的证书 PFX 文件，指定 fs.citrixsamldemo.net 作为 DNS 名称。

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



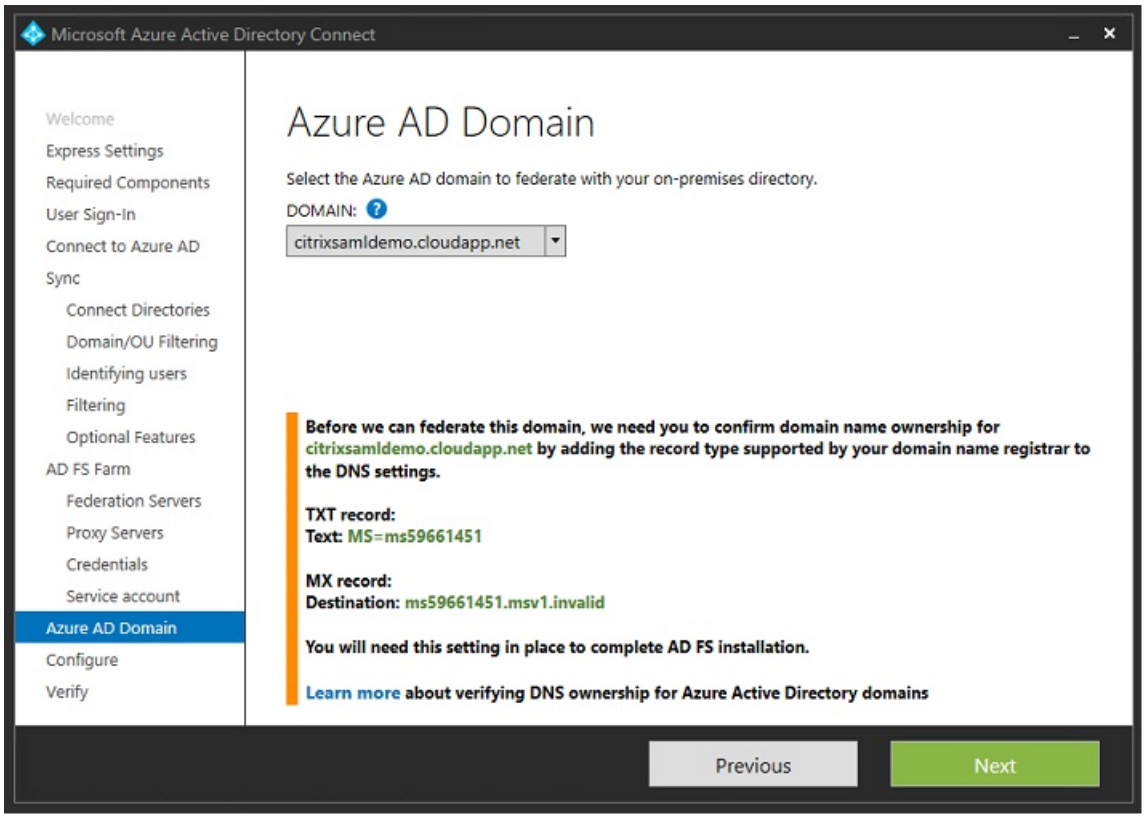
提示选择代理服务器时，输入 wap.citrixsamldemo.net 服务器的地址。 您可能需要在 Web 应用程序代理服务器上以管理员身份运行 **Enable-PSRemoting –Force** cmdlet，以便 Azure AD Connect 能够对其进行配置。



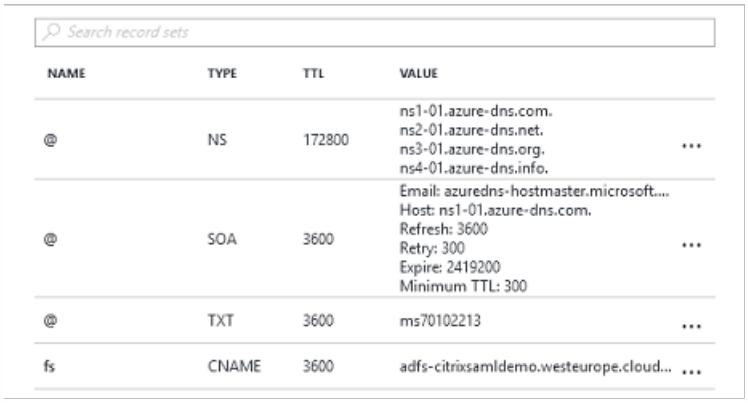
© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

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

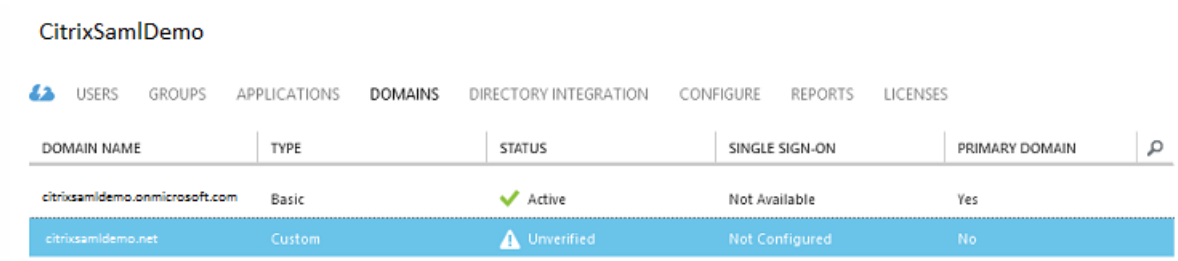


将 TXT 和 MX 记录添加到 Azure 中的 DNS 地址记录。



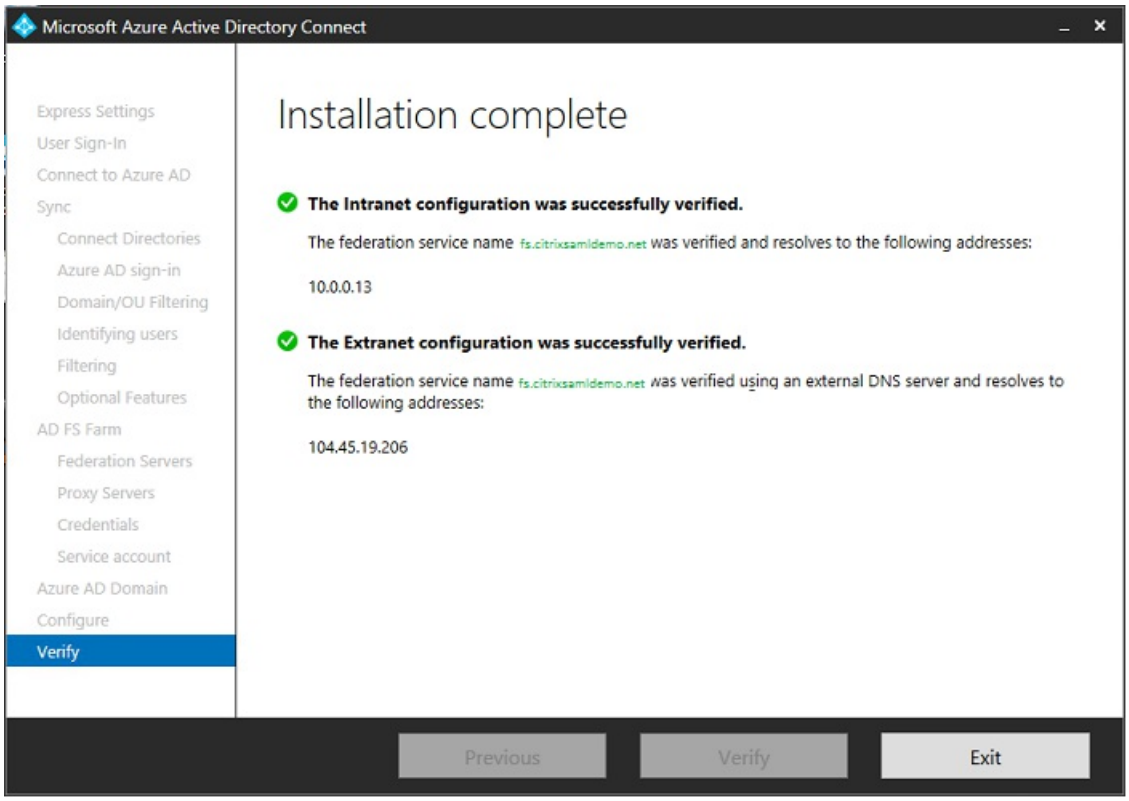
在 Azure 管理控制台中单击**验证**。

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



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

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

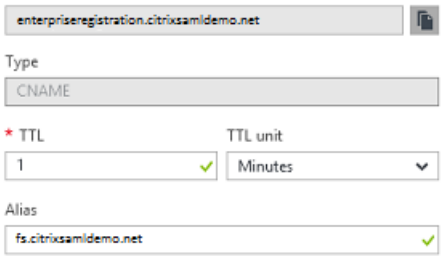


启用 Azure AD 联接

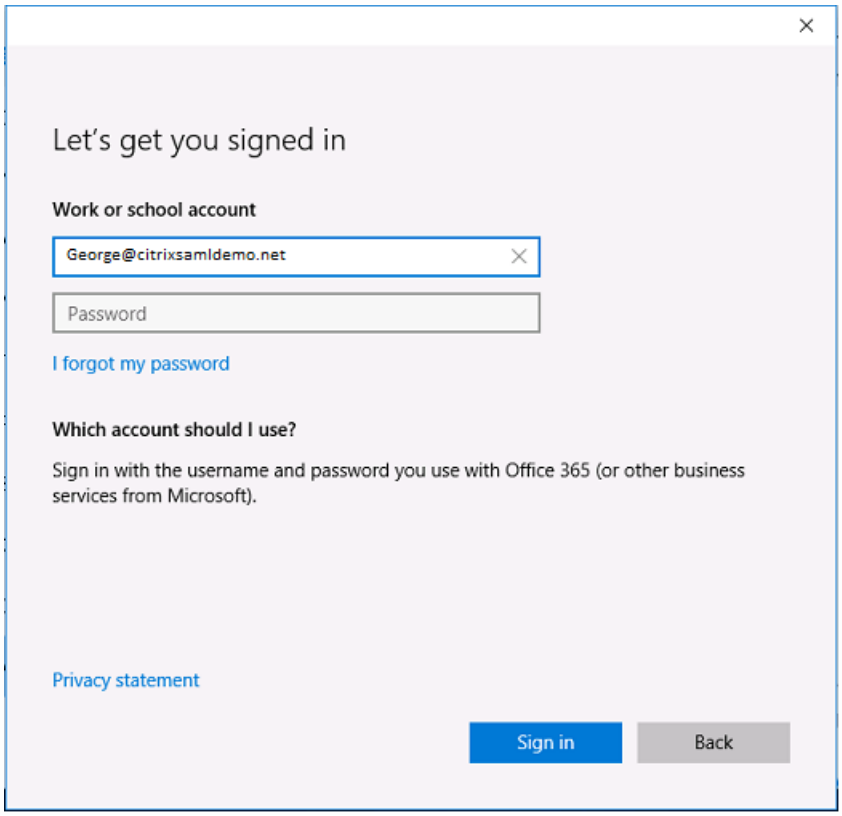
用户输入电子邮件地址以便 Windows 10 能够执行 Azure AD 联接操作时，DNS 后缀将用于构建应指向 ADFS 的 CNAME DNS 记录：enterpriseregistration.。

在此示例中为 fs.citrixsamldemo.net。

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

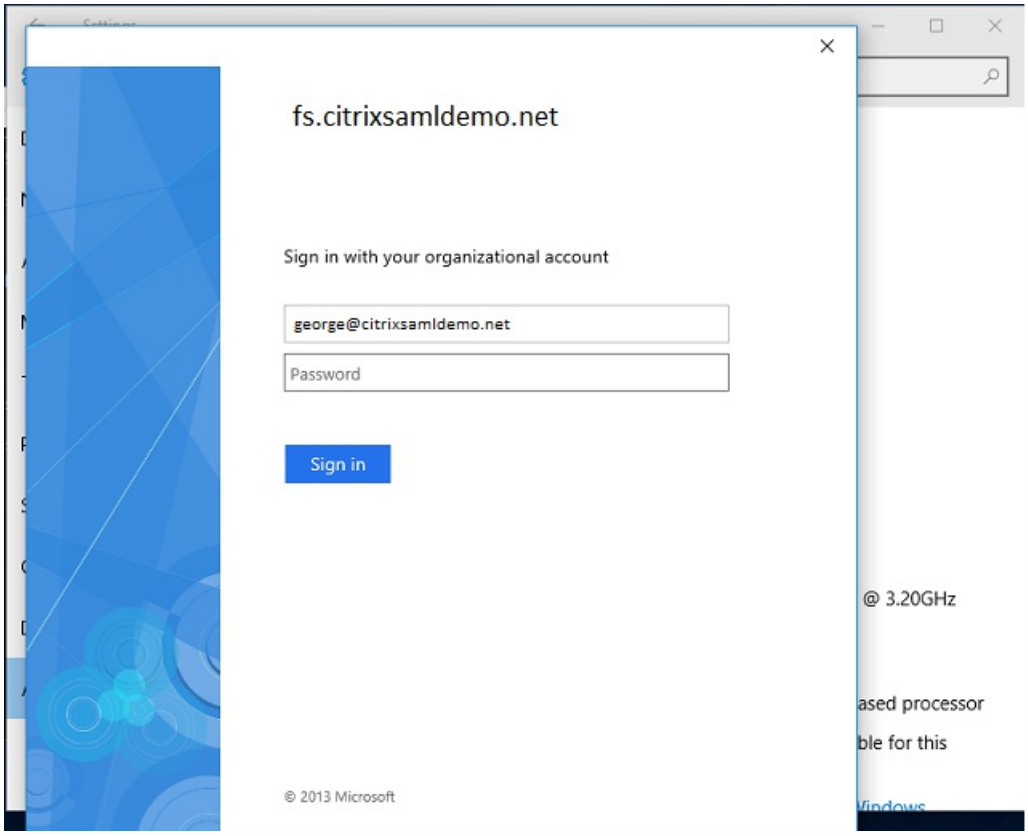


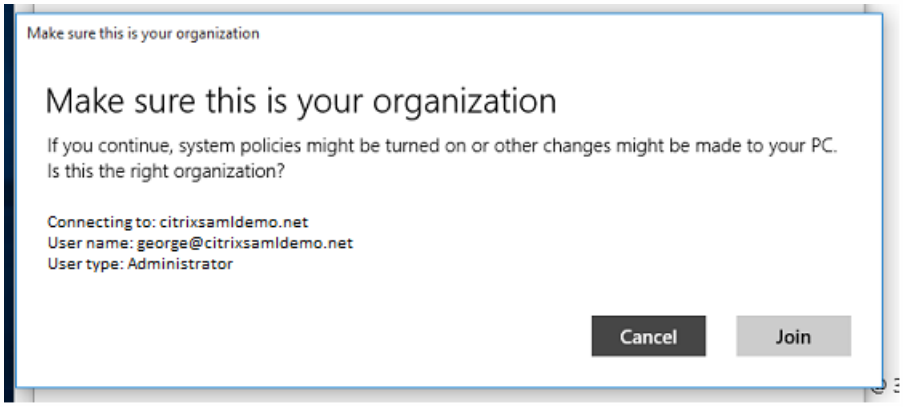
如果未使用公用 CA，请务必在 Windows 10 计算机上安装 ADFS 根证书，这样 Windows 将信任 ADFS 服务器。 使用之前生成的标准用户帐户执行 Azure AD 域加入操作。



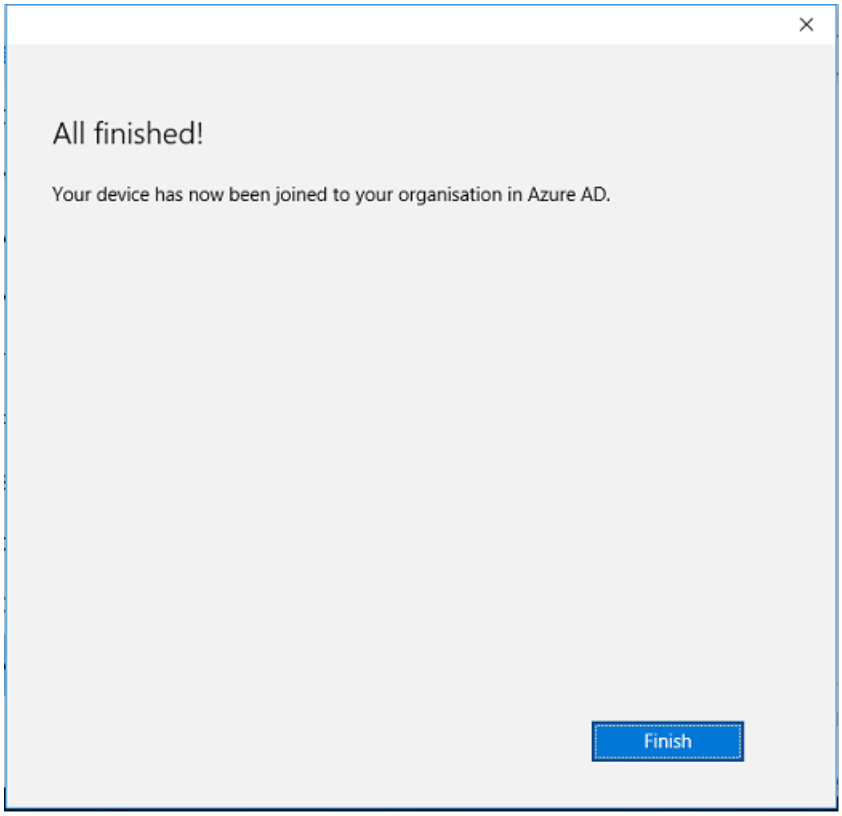
请注意：UPN 必须与 ADFS 域控制器能够识别的 UPN 匹配。

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





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



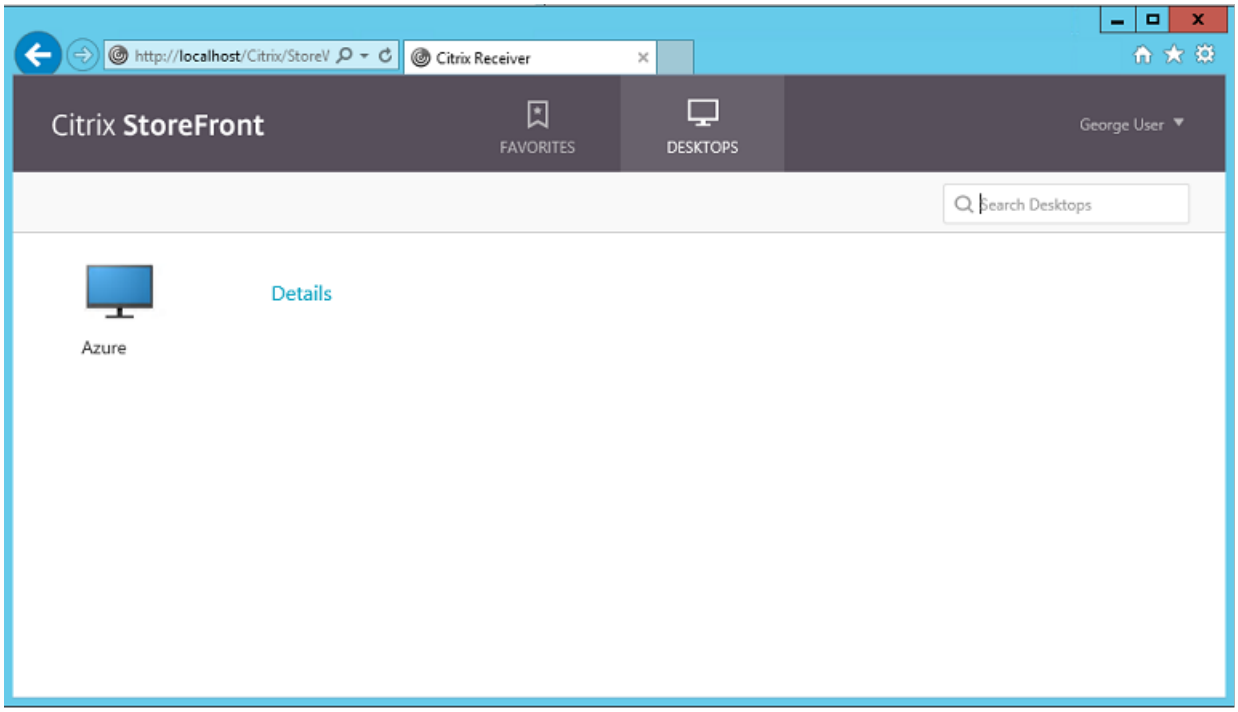
使用用户的电子邮件地址通过重新启动计算机并登录来验证 Azure AD 联接操作是否成功。 登录后，请启动 Microsoft Edge 并连接到 http://myapps.microsoft.com。该 Web 站点应自动使用单点登录功能。

安装 XenApp 或 XenDesktop

可以按常规方式在 Azure 中直接从 XenApp 或 XenDesktop ISO 安装 Delivery Controller 和 VDA 虚拟机。

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

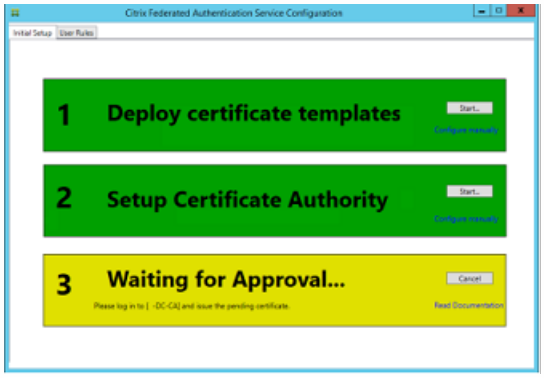
© 1999-2017 Citrix Systems, Inc. All rights reserved.



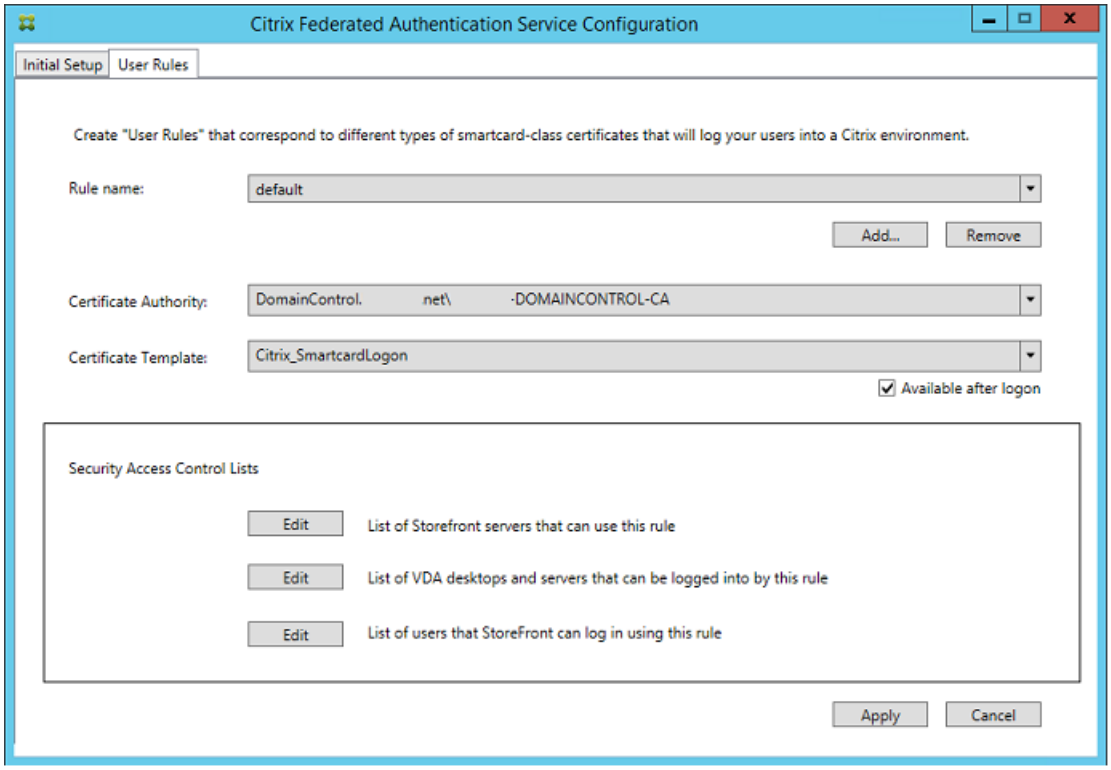
在 Controller 上运行 **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true** PowerShell cmdlet 以允许 StoreFront 不使用用户的凭据进行身份验证。

安装联合身份验证服务

在 ADFS 服务器上安装联合身份验证服务 (FAS) 组件，并为要用作可信 StoreFront 的 Controller 配置一条规则。

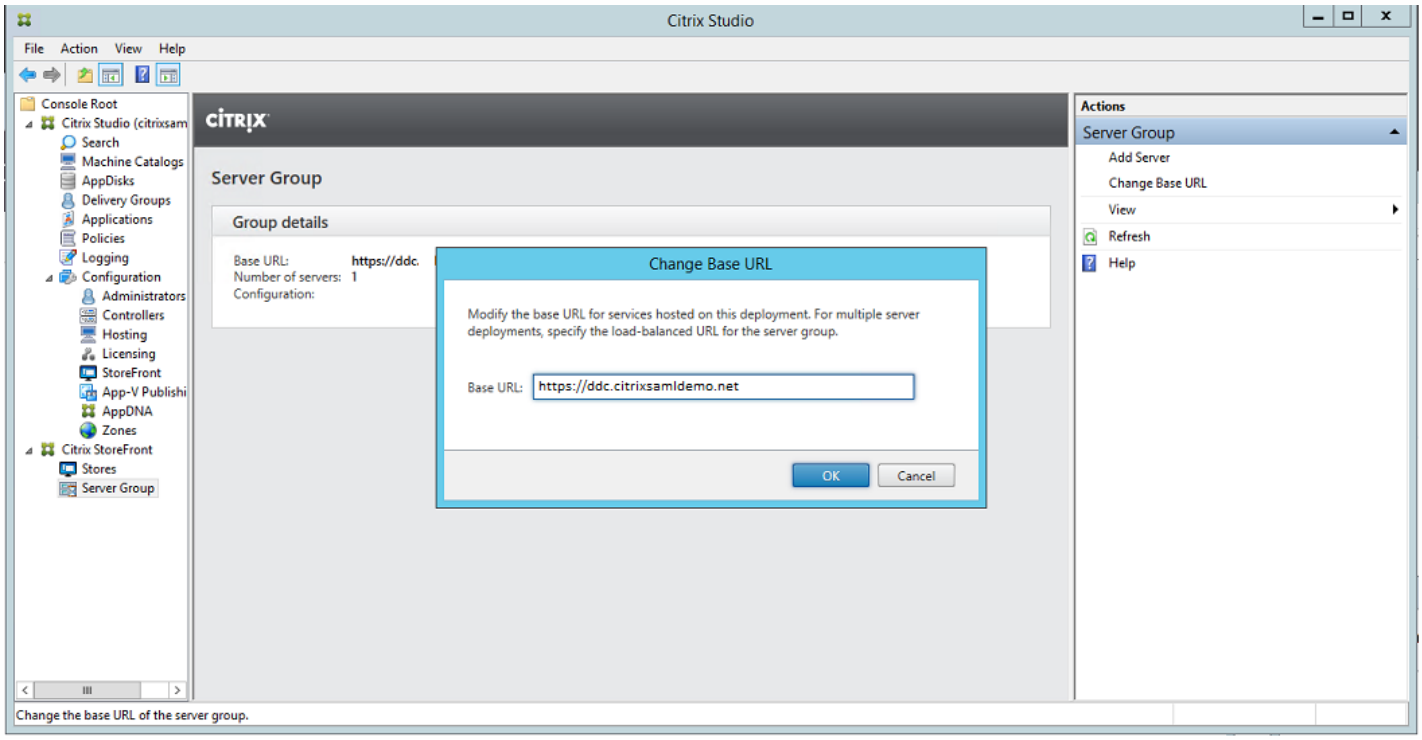


© 1999-2017 Citrix Systems, Inc. All rights reserved.



配置 StoreFront

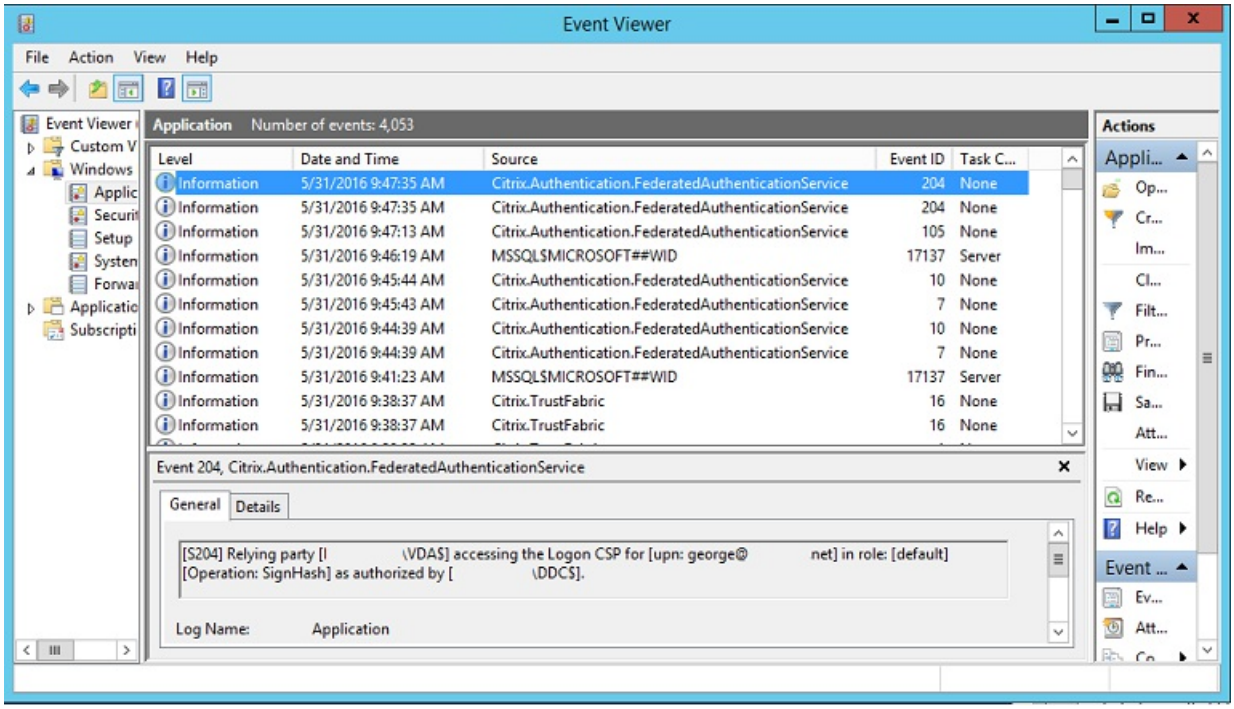
为 Delivery Controller 申请一个计算机证书，然后将 IIS 和 StoreFront 配置为使用 HTTPS，方法是为端口 443 设置 IIS 绑定，并将 StoreFront 基址更改为 https:。



将 StoreFront 配置为使用 FAS 服务器（使用联合身份验证服务一文中介绍的 PowerShell 脚本），然后在 Azure 中进行内部测

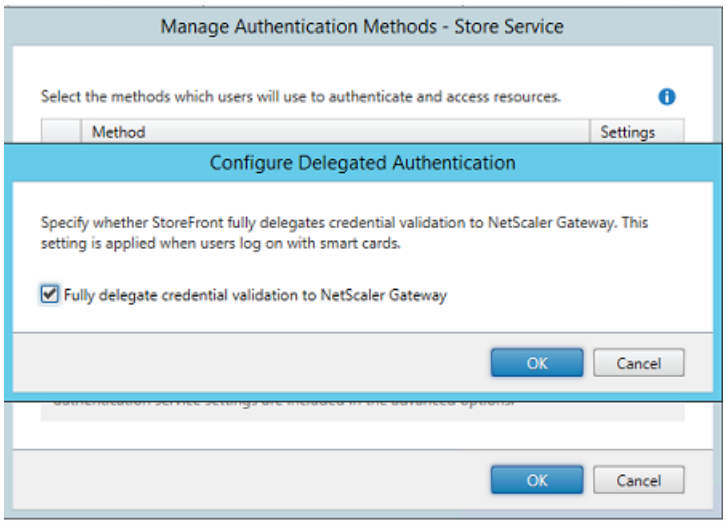
© 1999-2017 Citrix Systems, Inc. All rights reserved.

试，通过查看 FAS 服务器上的事件查看器来确保登录使用 FAS。



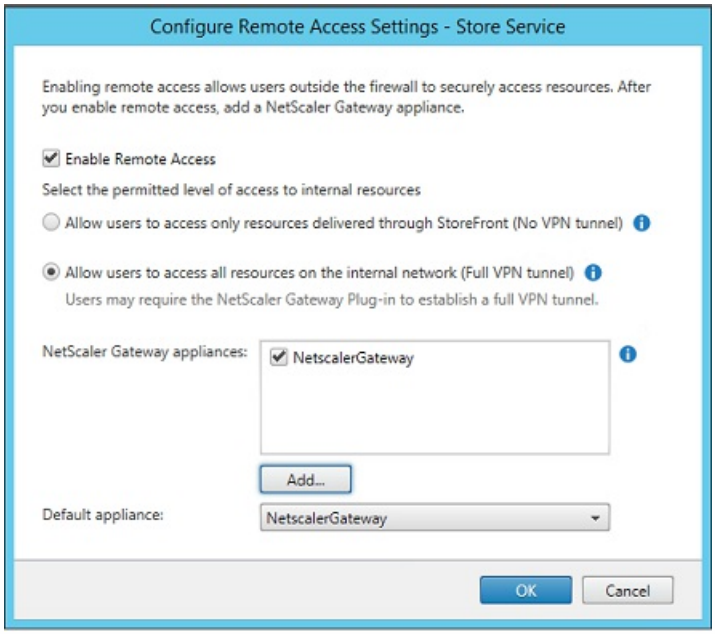
将 StoreFront 配置为使用 NetScaler

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



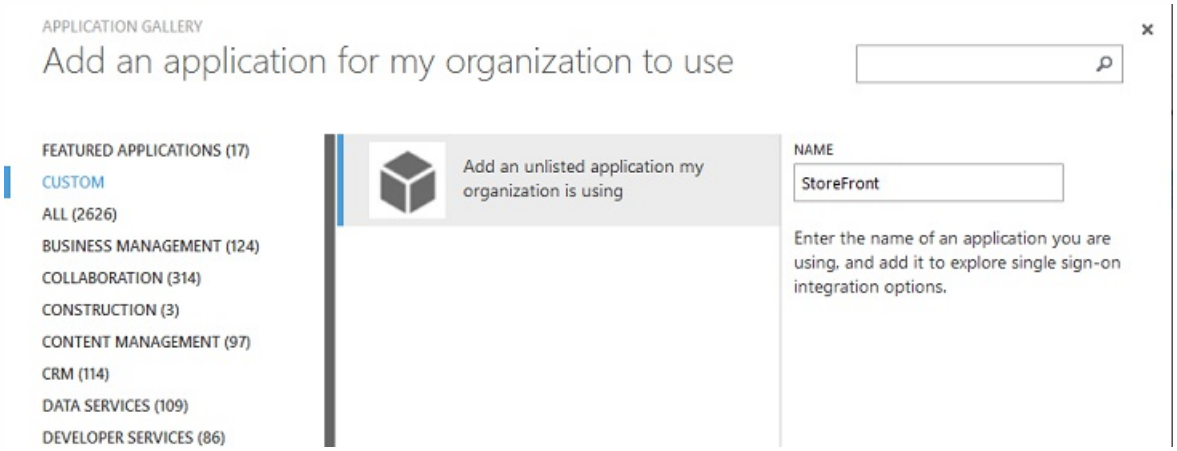
要集成 NetScaler 身份验证选项，请配置一个 Secure Ticket Authority (STA) 并配置 NetScaler Gateway 地址。

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



配置新 Azure AD 应用程序以单点登录到 StoreFront

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



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

配置图标

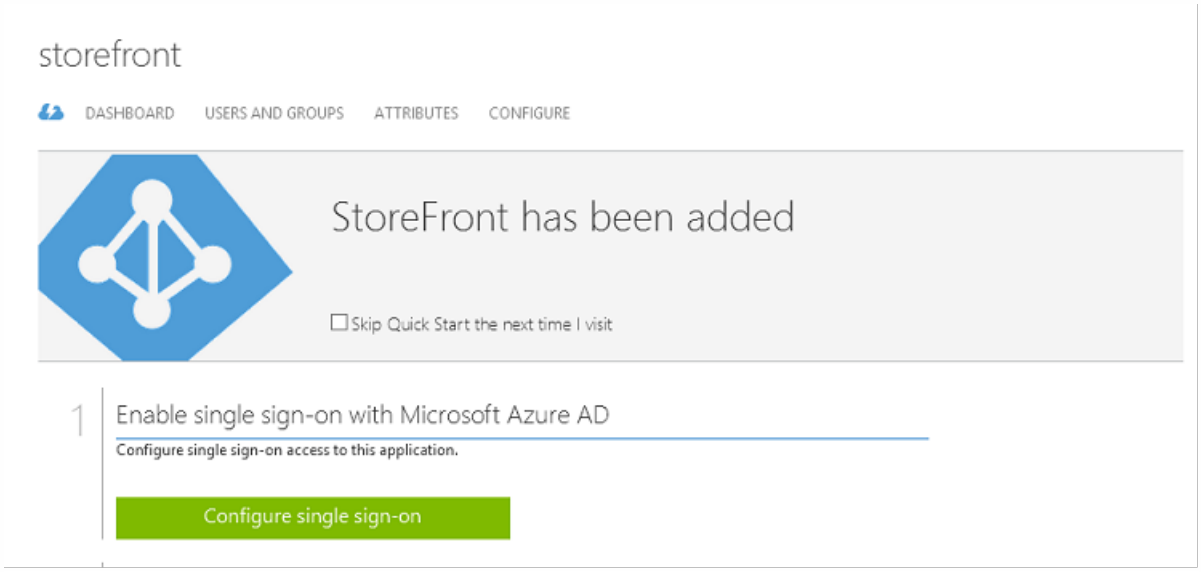
创建一个大小为 215 x 215 像素的图片并在“配置”页面上上载该图片以用作应用程序的图标。

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

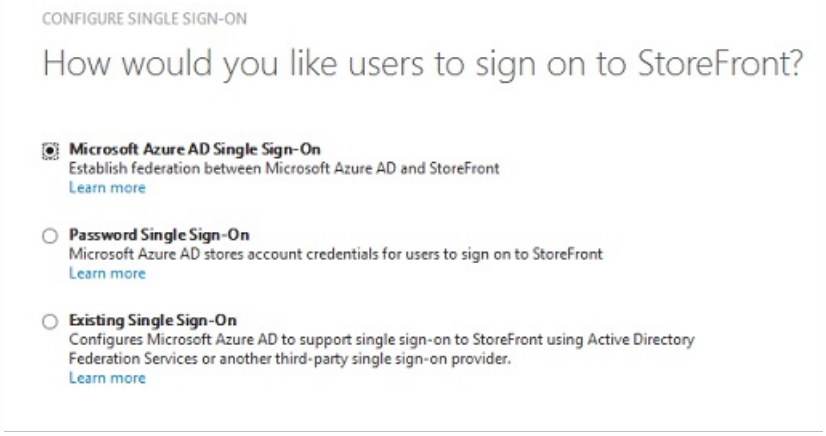


配置 SAML 身份验证

返回到“应用程序”控制板概览页面并选择**配置单点登录**。

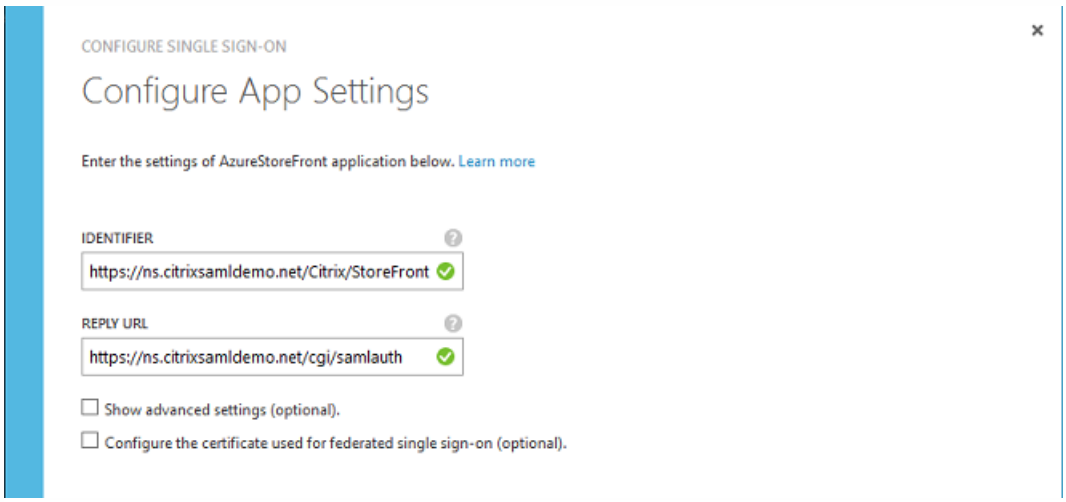


此部署将使用 SAML 2.0 身份验证，这与 **Microsoft Azure AD 单一登录**相对应。

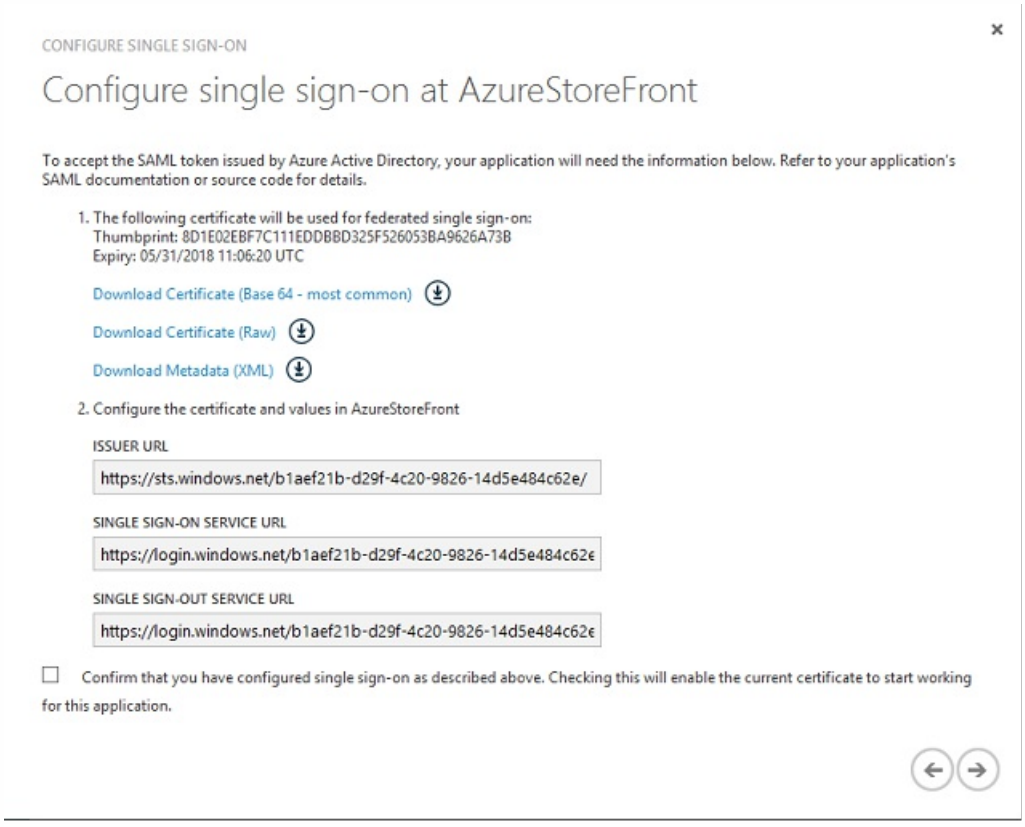


© 1999-2017 Citrix Systems, Inc. All rights reserved.

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



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



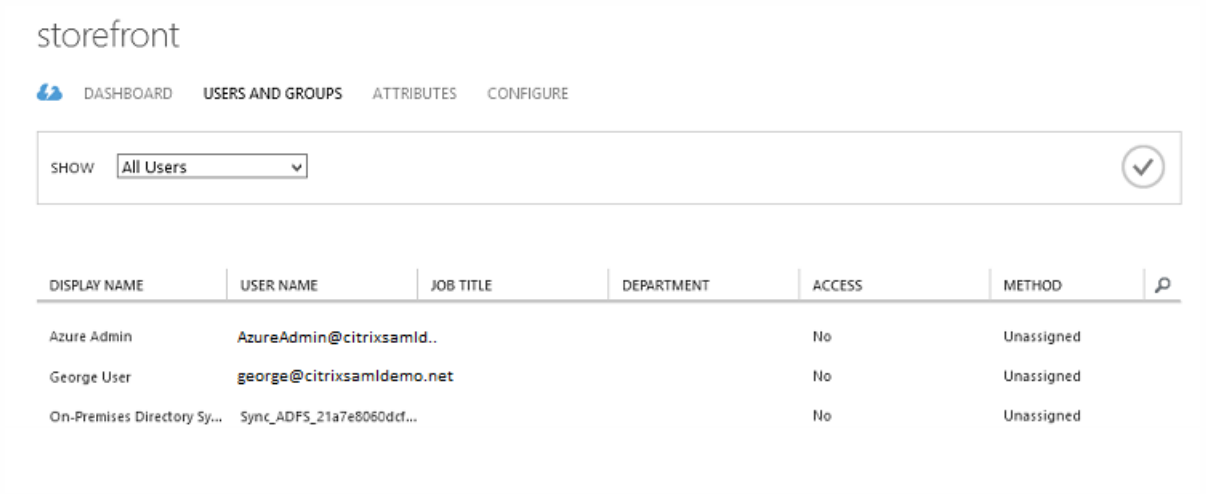
下载 Base 64 可信签名证书并复制登录和注销 URL。 您稍后将在 NetScaler 的配置屏幕中粘贴这些 URL。

向用户分配应用程序

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

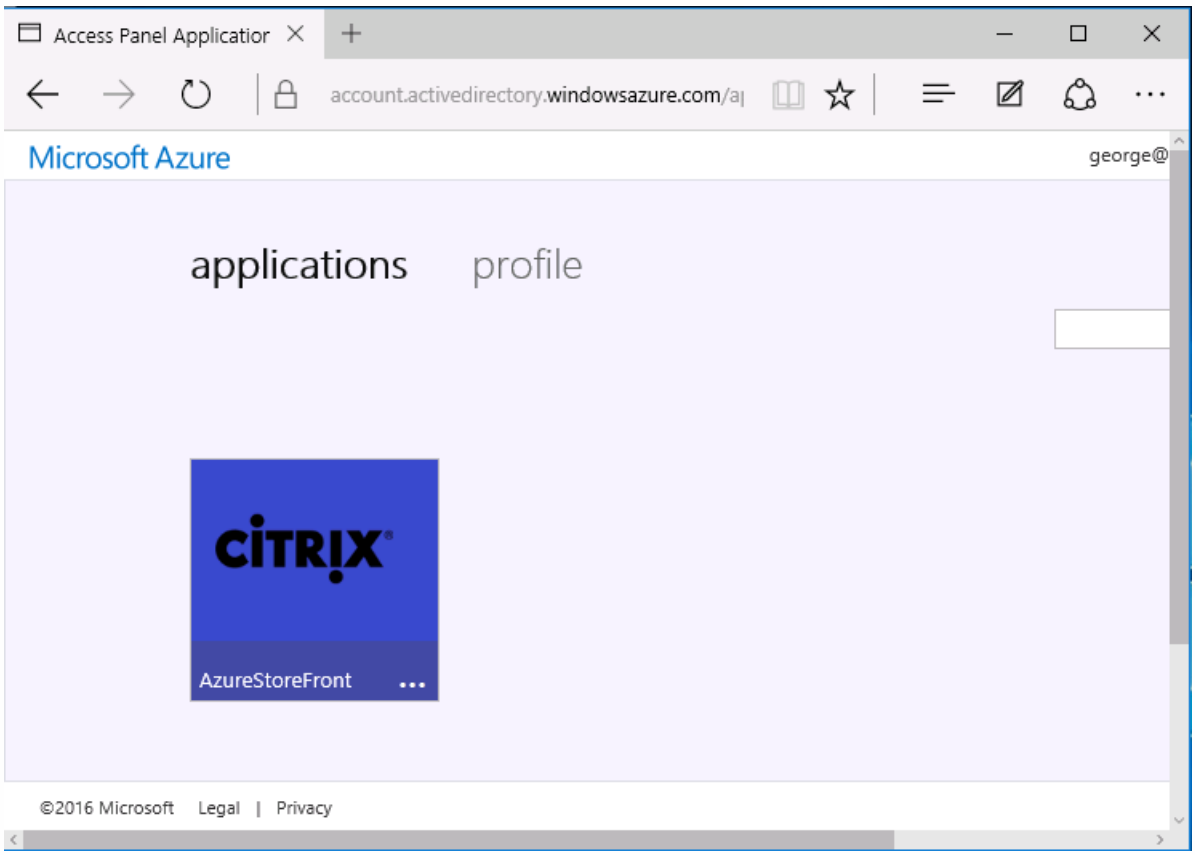
© 1999-2017 Citrix Systems, Inc. All rights reserved.

用 @ 格式。



MyApps 页面

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

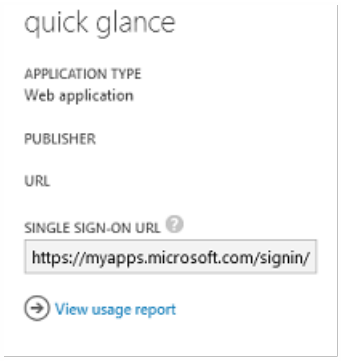


与 Azure AD 联接后，Windows 10 将支持登录用户单点登录到 Azure 应用程序。 单击图标会将浏览器定向到之前配置的 SAML cgi/samlauth Web 页面。

单点登录 URL

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

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



将此 URL 粘贴到 Web 浏览器中以确保 Azure AD 能够将您重定向到之前配置的 NetScaler cgi/samlauth Web 页面。 这仅适用于已分配的用户，并且仅对加入了 Windows 10 Azure AD 的登录会话提供单点登录。（系统将提示其他用户输入 Azure AD 凭据。）

安装并配置 NetScaler Gateway

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



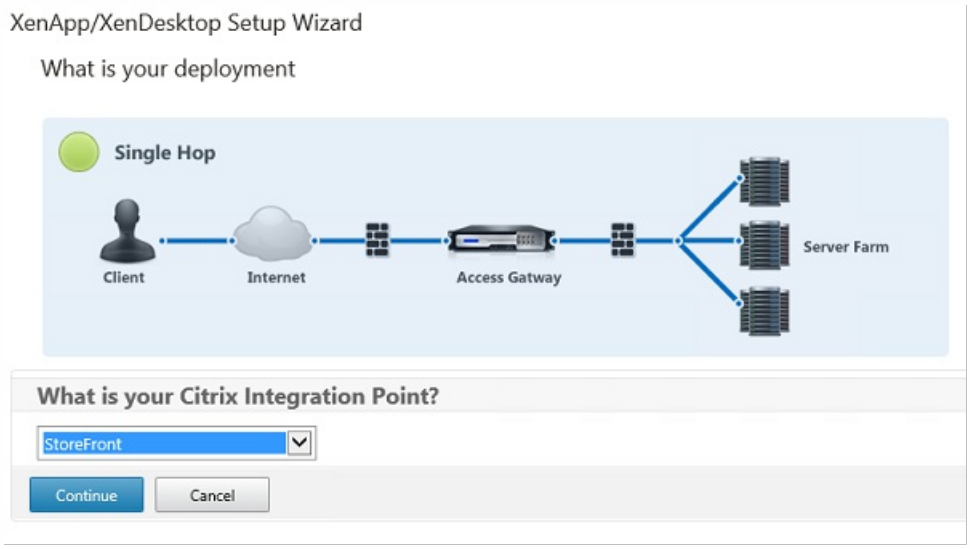
使用对用户进行身份验证时指定的凭据登录 NetScaler VM，从而将 Web 浏览器指向内部 IP 地址。 请注意，必须在 Azure AD VM 中更改用户 nsroot 的密码。

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

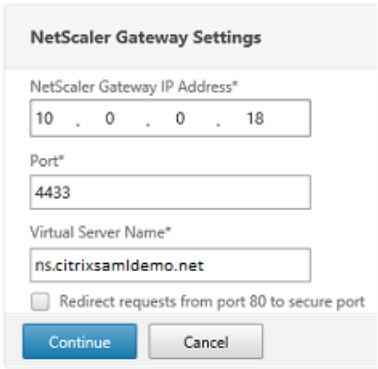
运行 XenApp 和 XenDesktop 设置向导

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

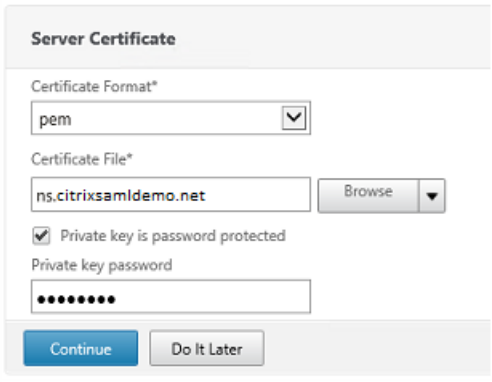
下例首先配置一个不带 SAML 的简单 StoreFront 集成。该部署运行后，将添加 SAML 登录策略。



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



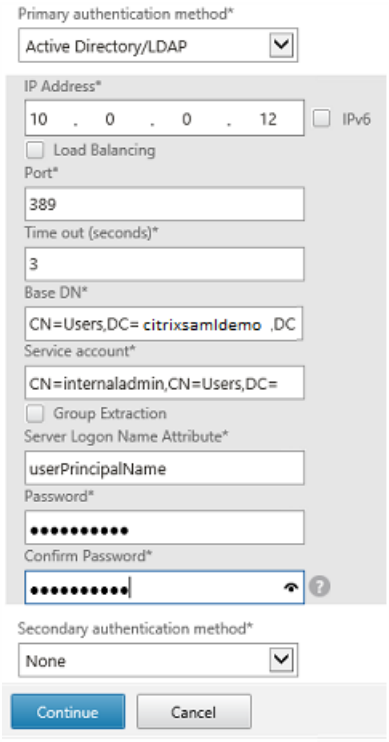
为简单起见，此示例将上载现有服务器证书以及存储在文件中的私钥。



配置域控制器以便管理 AD 帐户

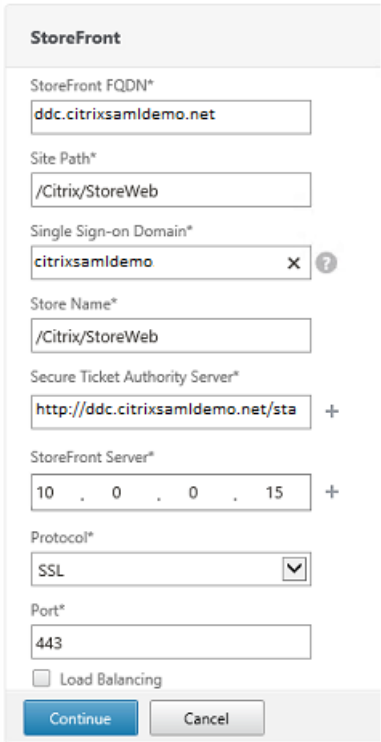
域控制器将用于帐户解析，因此，请将其 IP 地址添加到主身份验证方法中。 记录对话框中每个字段要求的格式。

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



配置 StoreFront 地址

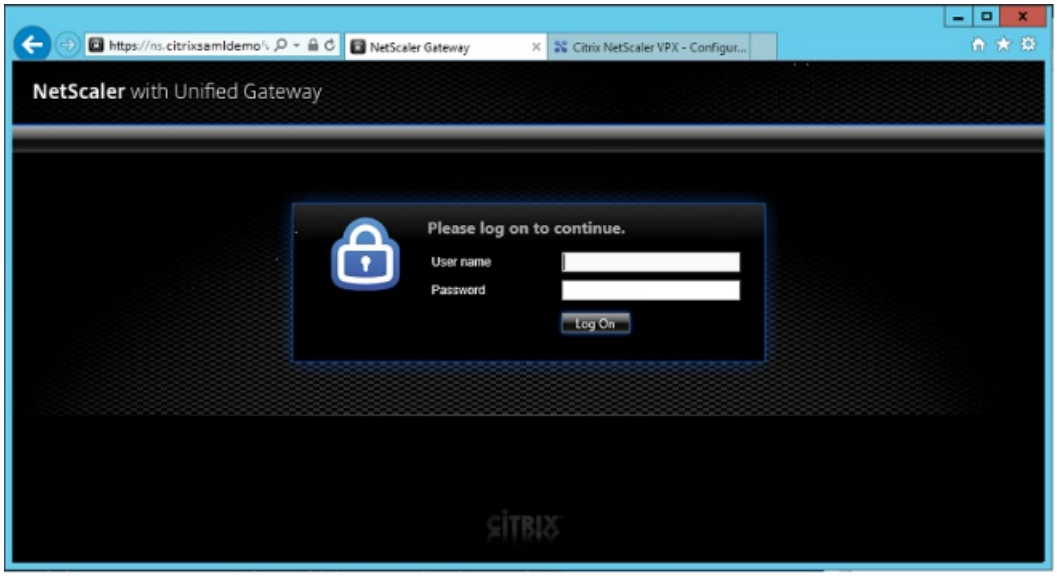
在此示例中，已使用 HTTPS 配置 StoreFront，因此，请选择 SSL 协议选项。



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

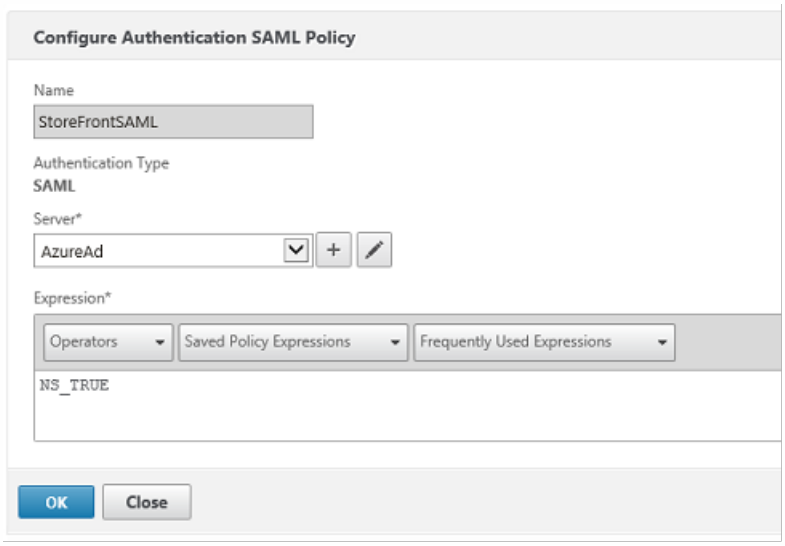
验证 NetScaler 部署

使用用户名和密码连接到 NetScaler 并检查身份验证和启动是否成功。



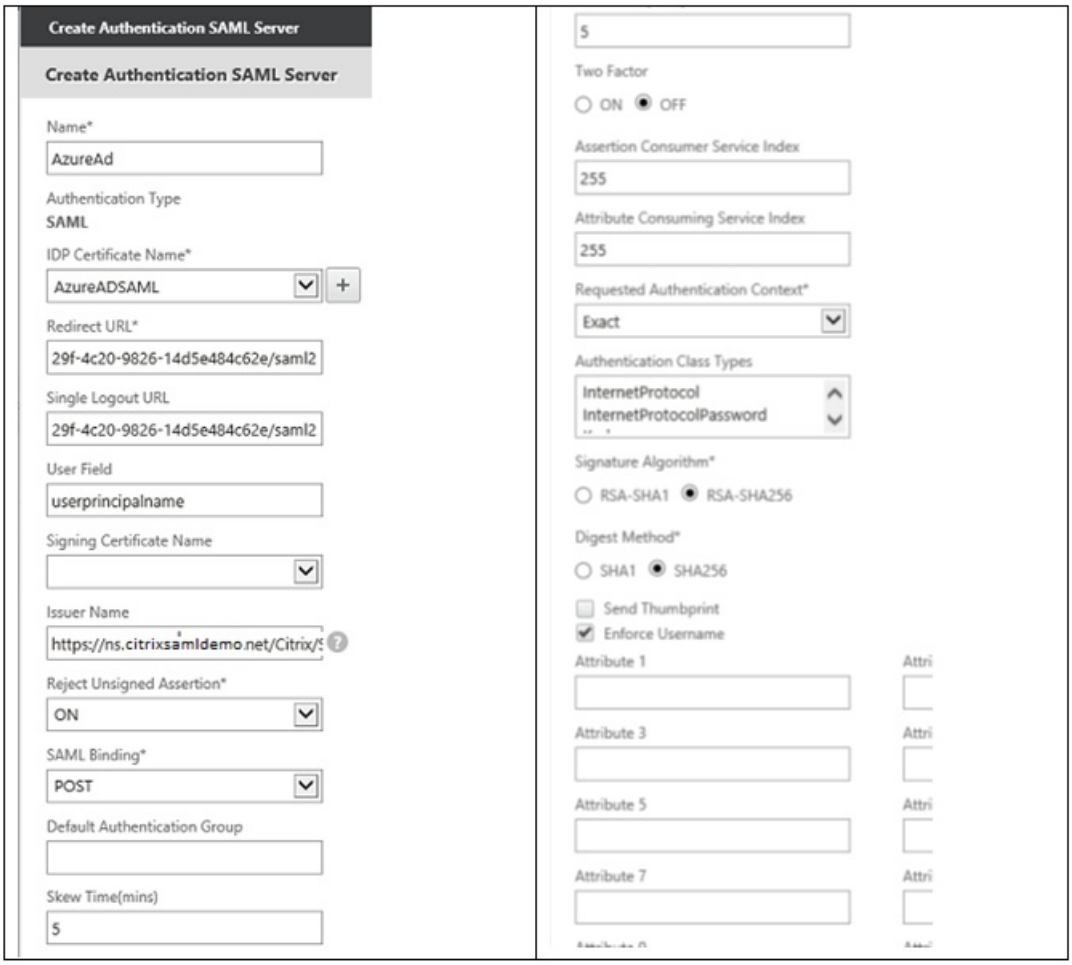
启用 NetScaler SAML 身份验证支持

在 StoreFront 中使用 SAML 与在其他 Web 站点中使用 SAMl 类似。 添加一条新 SAML 策略，表达式为 **NS_TRUE**。



使用之前从 Azure AD 获取的信息配置新 SAML IdP 服务器。

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

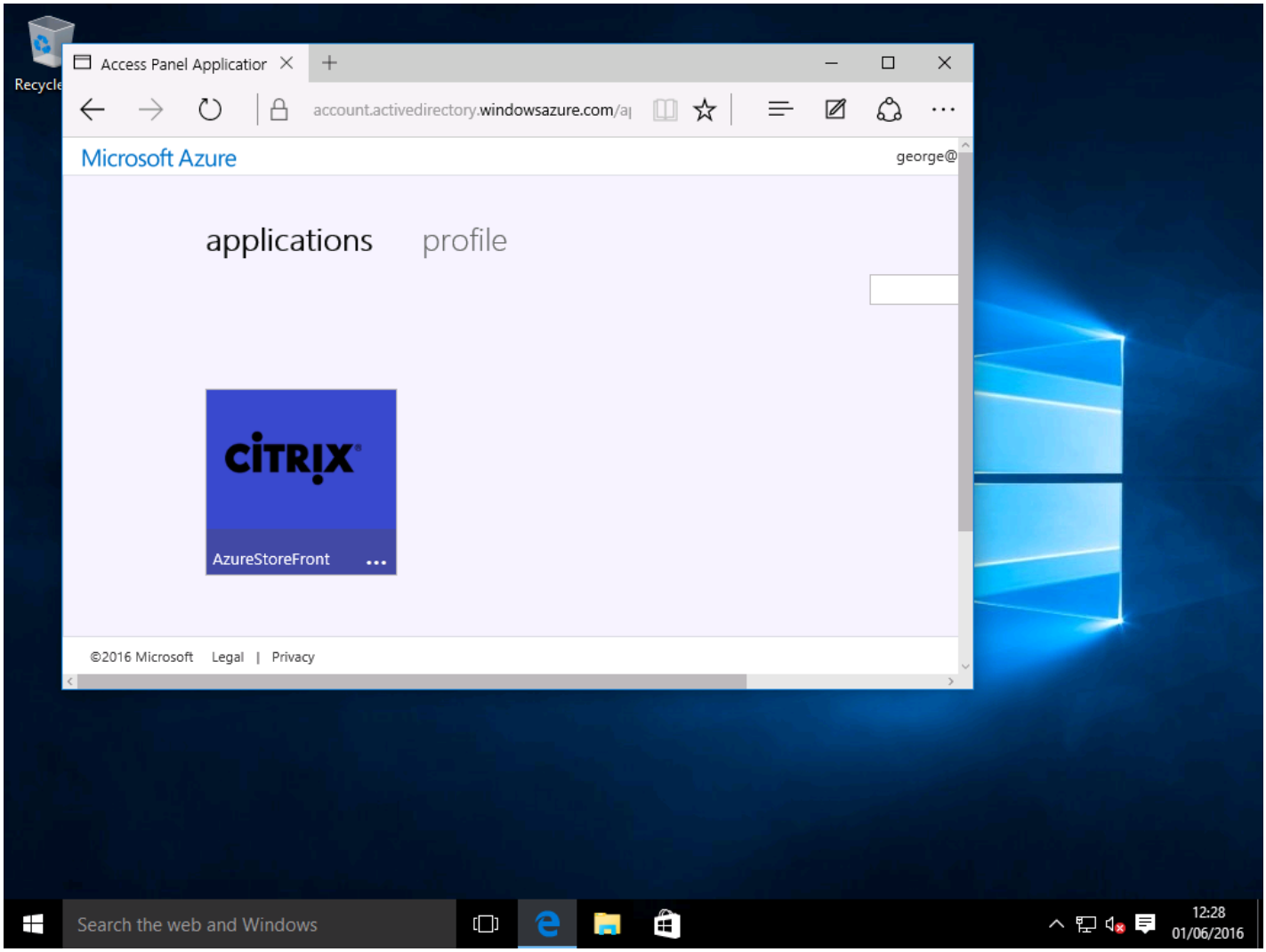


验证端到端系统

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

Web 浏览器应为用户显示 Azure AD 应用程序。

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



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

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

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

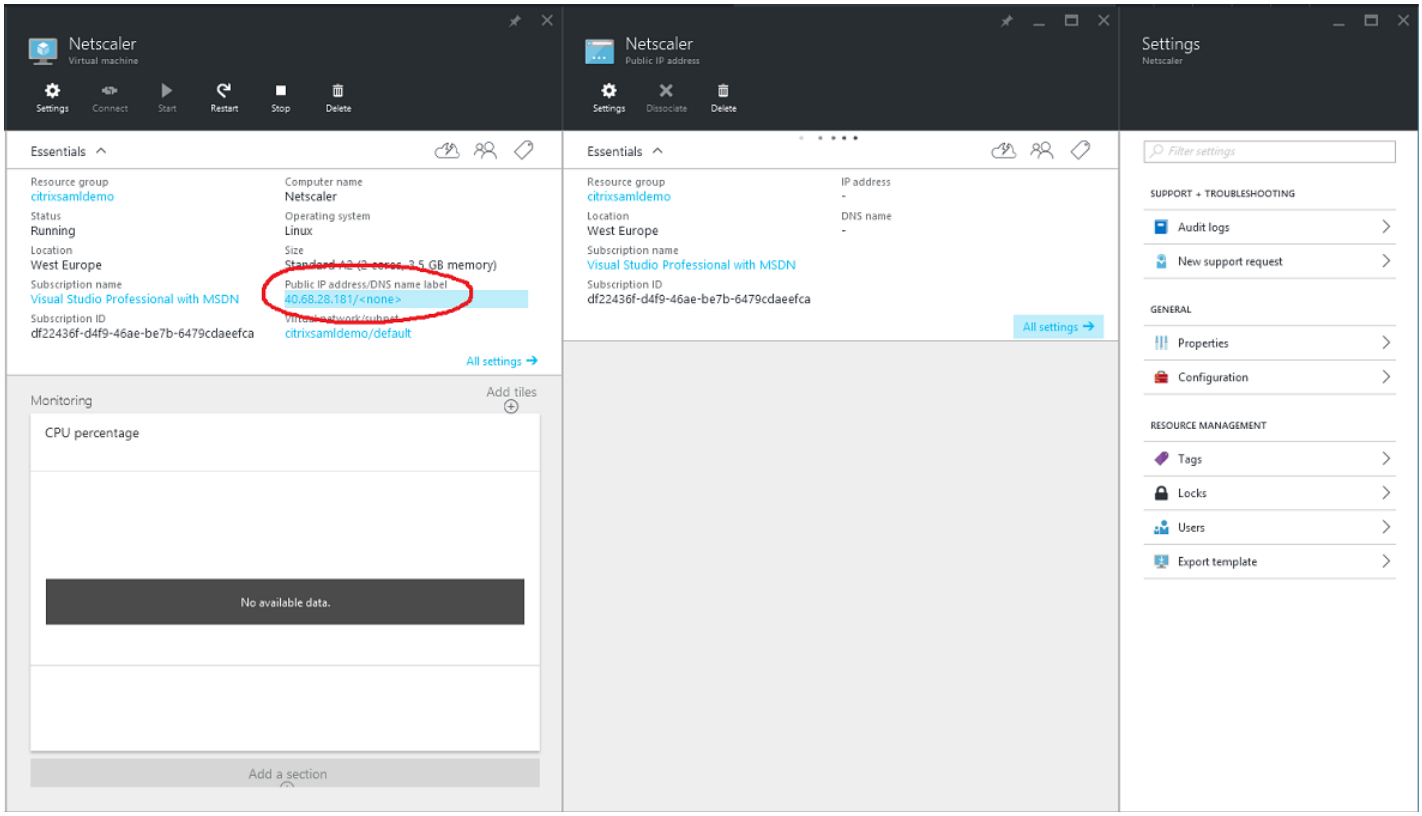
附录

在 Azure 中设置 VM 时应配置多个标准选项。

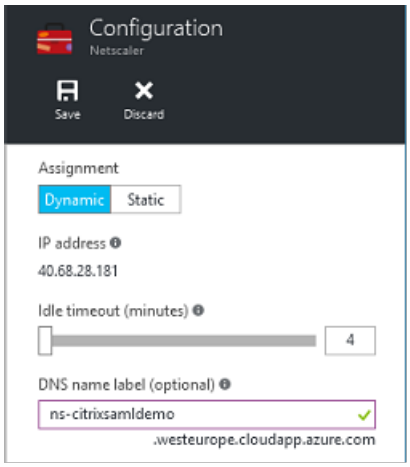
提供公用 IP 地址和 DNS 地址

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

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



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

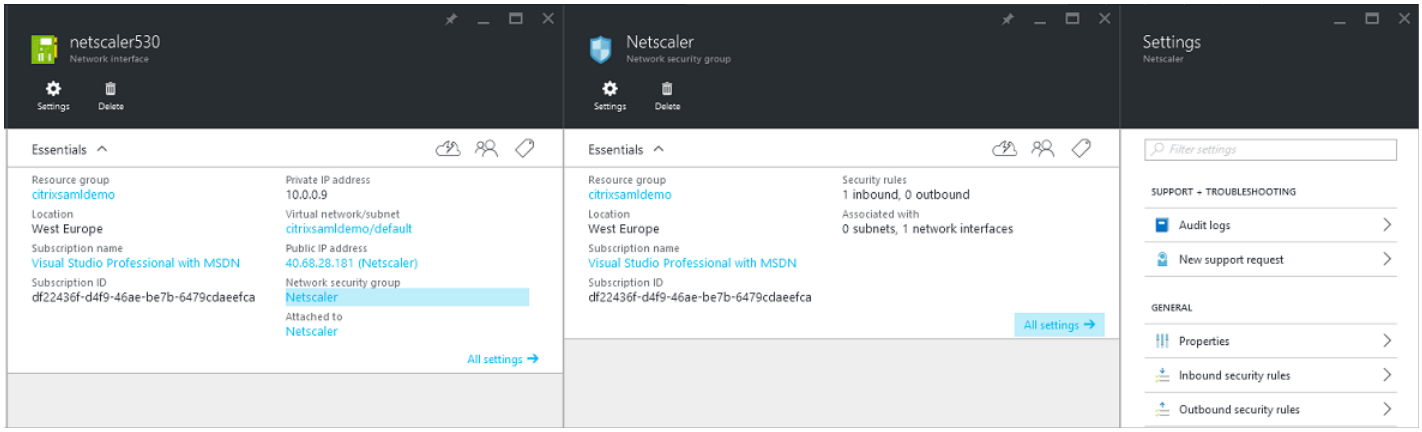


设置防火墙规则（安全组）

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

打开 VM 的**网络接口**，然后单击**网络安全组**标签。 配置**入站安全规则**以允许转发相应的网络流量。

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



相关信息

- 联合身份验证服务一文是 FAS 安装和配置的主要参考资料。
- 通用 FAS 部署在联合身份验证服务体系结构概述一文中加以概括。
- 联合身份验证服务配置和管理一文介绍了“操作指南”文章。

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

联合身份验证系统操作指南：配置和管理

Dec 05, 2017

以下“操作指南”文章提供了联合身份验证系统 (FAS) 的高级配置和管理指南：

- 私钥保护
- 证书颁发机构配置
- 安全性和网络管理
- 解决了 Windows 登录问题
- PowerShell SDK cmdlet 帮助文件

相关信息：

- FAS 的安装和初始设置的主要参考资料为联合身份验证服务一文。
- 联合身份验证服务体系结构概述一文总结了主要的 FAS 体系结构，并提供了指向与更复杂的体系结构有关的其他文章的链接。

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

“联合身份验证服务”证书颁发机构配置

Dec 05, 2017

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

设置用于 FAS 的多个 CA 服务器

本节介绍如何设置单个 FAS 服务器以使用多个 CA 服务器颁发证书。这将允许对 CA 服务器进行负载平衡和故障转移。

步骤 1：查找 FAS 可找到的 CA 服务器的数量

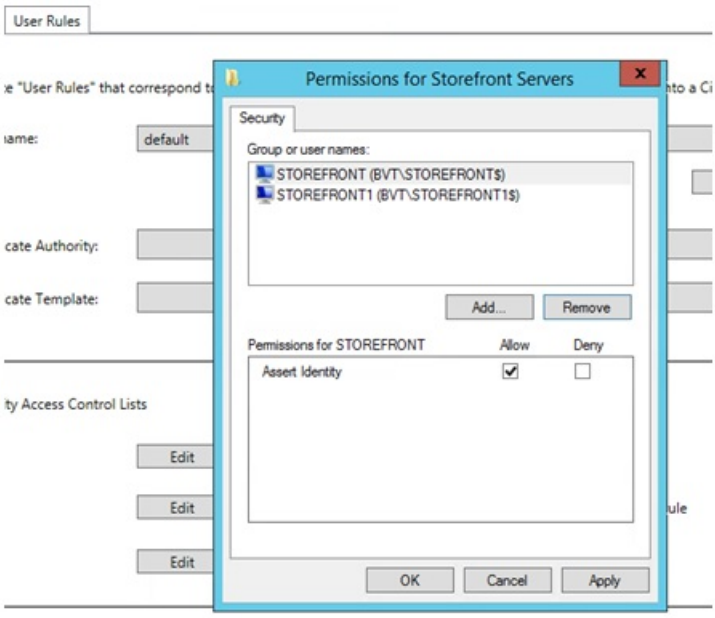
使用 Get-FASMsCertificateAuthority cmdlet 确定 FAS 可以连接到的 CA 服务器。在以下示例中，FAS 可连接到三个 CA 服务器。

```
PS > Add-PSSnapin Citrix*
PS > Get-FASMsCertificateAuthority

Address                          IsDefault PublishedTemplates
-------                          --------- ------------------
DC1.bvt.local\bvt-DC1-CA             False {Citrix_SmartcardLogon, Citrix_Regis...
ca1.bvt.local\CA1.bvt.local          False {Citrix_SmartcardLogon, Citrix_Regis...
ca2.bvt.local\ca2.bvt.local          False {Citrix_SmartcardLogon, Citrix_Regis...
```

步骤 2：修改现有证书定义

Citrix 建议您使用 FAS 管理控制台而不是 PowerShell 创建角色。这样可避免在以后手动添加 SDL。在下面的示例中，将创建一个名为“default”的角色并配置访问规则：



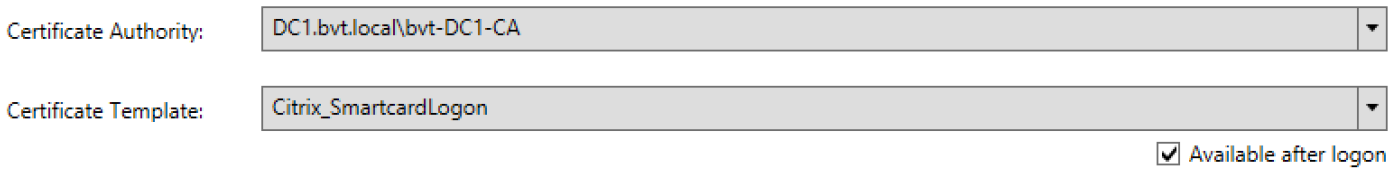
© 1999-2017 Citrix Systems, Inc. All rights reserved.

要向证书颁发机构字段（在此版本的管理控制台中不受支持）添加多个 CA，必须配置证书定义。首先，需要使用证书定义名称。无法从管理控制台中确定该名称；请使用 Get-FASCertificateDefinition cmdlet。

```
PS > Get-FASCertificateDefinition

Name                    : default_Definition
CertificateAuthorities  : {DC1.bvt.local\bvt-DC1-CA}
MsTemplate              : Citrix_SmartcardLogon
AuthorizationCertificate : 86ce221c-7599-43a3-9dbd-8e6a3c2be7b7
PolicyOids              : {}
InSession               : True
```

等效用户界面是：



在具有证书定义名称之后，修改证书定义以具有一组而非一个 CertificateAuthorities：

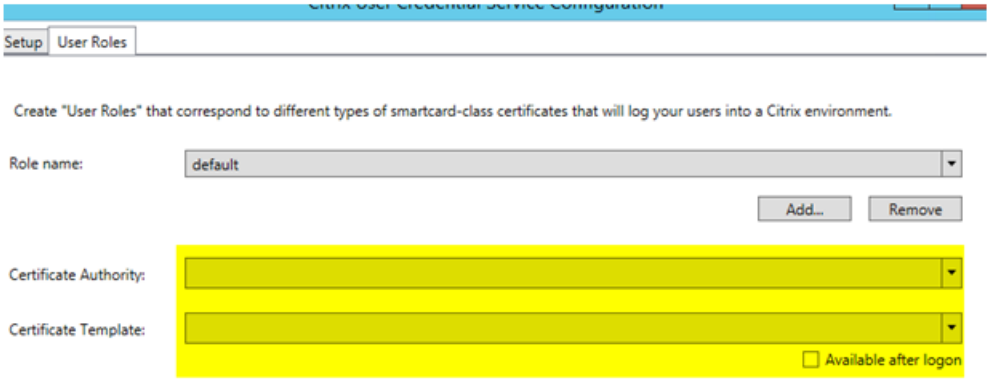
```
PS > Set-FASCertificateDefinition -Name default_Definition -CertificateAuthorities @("DC1.bvt.
local\bvt-DC1-CA", "ca1.bvt.local\CA1.bvt.local", "ca2.bvt.local\ca2.bvt.local")
```

FASCertificateDefinition cmdlet 现在将返回：

```
PS > Get-FASCertificateDefinition
Name                    : default_Definition
CertificateAuthorities  : {DC1.bvt.local\bvt-DC1-CA, ca1.bvt.local\CA1.bvt.local, ca2.bvt.local\ca2.bvt.local}
MsTemplate              : Citrix_SmartcardLogon
AuthorizationCertificate : 86ce221c-7599-43a3-9dbd-8e6a3c2be7b7
PolicyOids              : {}
InSession               : True
```

注意：在执行此操作后，FAS 管理控制台将不会工作。在加载时，会在“证书颁发机构”和“证书模板”中显示空字段：

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



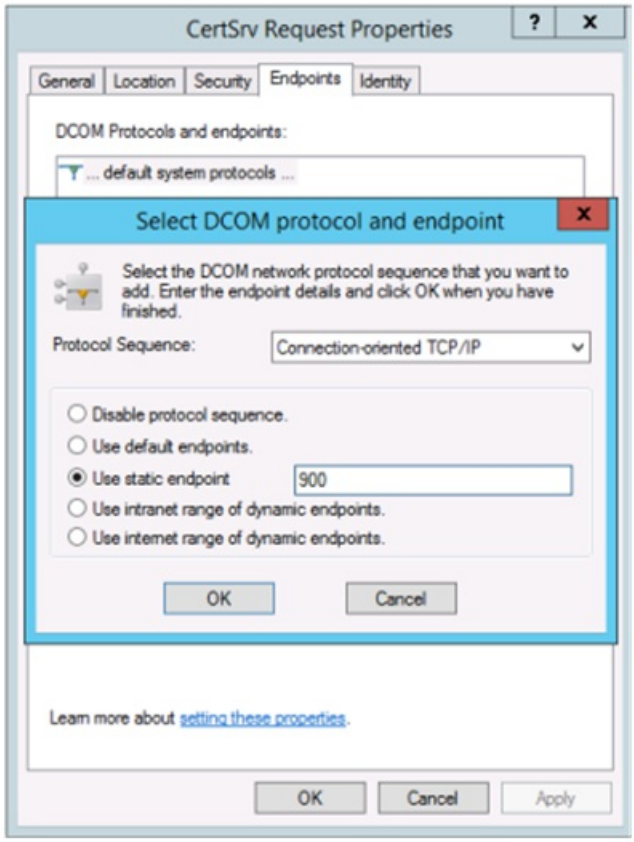
FAS 的功能仍然有效。如果您使用控制台修改访问规则，则只需重复步骤 2 以显示所有证书颁发机构即可。

预期的行为变化

在配置 FAS 服务器和多个 CA 服务器后，将在所有已配置的 CA 服务器之间分配用户证书生成任务。此外，如果配置的 CA 服务器之一发生故障，则 FAS 服务器将切换到另一个可用的 CA 服务器。

配置 Microsoft CA 以进行 TCP 访问

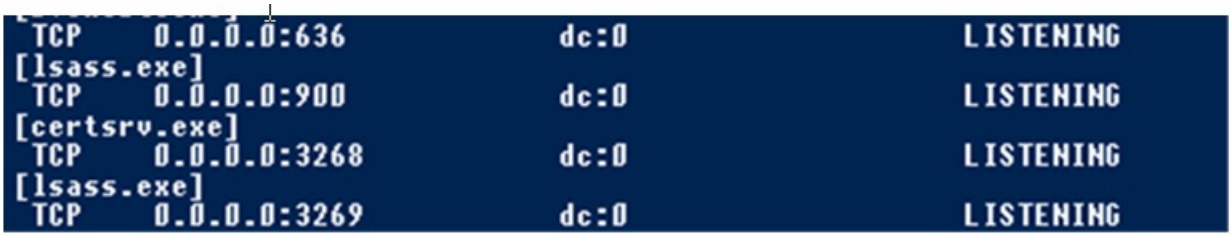
默认情况下，Microsoft CA 使用 DCOM 进行访问。这会导致需在实现防火墙安全功能时执行复杂的操作，因此，Microsoft 提供了一个置备项，可用于切换到静态 TCP 端口。在 Microsoft CA 中，打开 DCOM 配置面板并编辑“CertSrv Request”DCOM 应用程序的属性：



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

更改“端点”以选择静态端点，并指定 TCP 端口号（在上图中为 900）。

重新启动 Microsoft CA 并提交证书申请。如果您运行“netstat –a –n –b”，将看到 certsvr 在侦听端口 900：



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

预生成用户证书

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

获取 Active Directory 用户的列表

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

```
Import-Module ActiveDirectory

$searchbase = "cn=users,dc=bvt,dc=local" # AD User Base to Look for Users, leave it blank to search all
$filename = “user_list.csv” # Filename to save

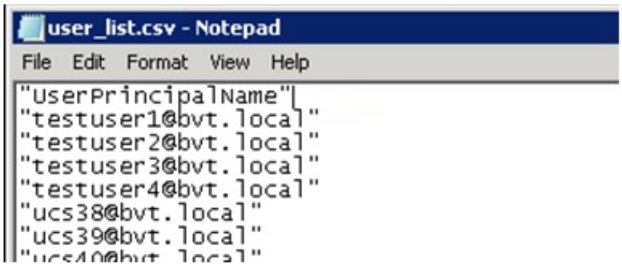
if ($searchbase –ne “”) {
   Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq "true")} -SearchBase $searchbase -Properties
UserPrincipalName |Select UserPrincipalName | Export-Csv -NoTypeInformation -Encoding utf8 -delimiter ","
$filename
} else {
   Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq "true")}  -Properties UserPrincipalName
|Select UserPrincipalName | Export-Csv -NoTypeInformation -Encoding utf8 -delimiter "," $filename
}
```

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

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

CSV 类似于如下所示：

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



FAS 服务器

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

```
Add-PSSnapin Citrix.A*

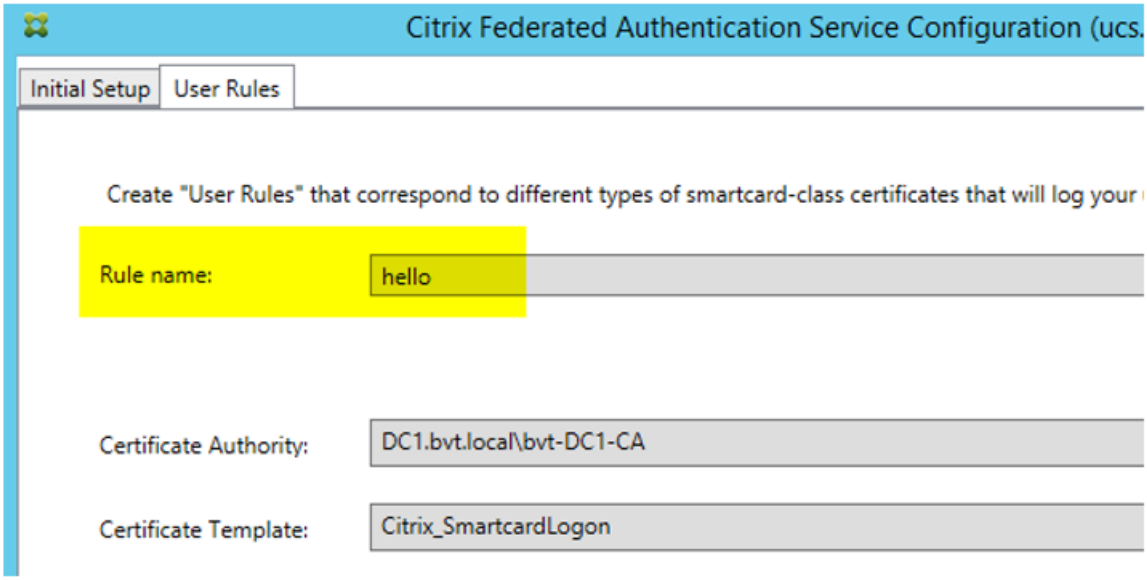
$csv = "user_list.csv"
$rule = "default" #rule/role in your admin console
$users = Import-Csv  -encoding utf8 $csv

foreach ( $user in $users )
{
  $server = Get-FASServerForUser -UserPrincipalNames $user.UserPrincipalName
  if ( $server.Server -ne $NULL ){
     New-FASUserCertificate -Address $server.Server -UserPrincipalName $user.UserPrincipalName -
CertificateDefinition $rule"_Definition" -Rule $rule
  }
  if ( $server.Failover -ne $NULL ){
     New-FASUserCertificate -Address $server.Failover -UserPrincipalName $user.UserPrincipalName -
CertificateDefinition $rule"_Definition" -Rule $rule
  }
}
```

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

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

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



更新注册授权证书

如果正在使用多个 FAS 服务器，则可以续订 FAS 授权证书而不会影响已登录的用户。注意：虽然也可以使用 GUI 取消授权和重新授权 FAS，但这会导致重置 FAS 配置选项。

请完成以下操作过程：

1. 创建新授权证书：

    New-FasAuthorizationCertificate

2. 记录由以下命令返回的新授权证书的 GUID：

    Get-FasAuthorizationCertificate

3. 使 FAS 服务器进入维护模式：

    Set-FasServer –Address -MaintenanceMode $true

4. 更换新授权证书：

    Set-FasCertificateDefinition –AuthorizationCertificate

5. 使 FAS 服务器退出维护模式：

    Set-FasServer –Address -MaintenanceMode $false

6. 删除旧授权证书：

    Remove-FasAuthorizationCertificate

相关信息

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

- 联合身份验证服务一文是 FAS 安装和配置的主要参考资料。
- 通用 FAS 部署在联合身份验证服务体系结构概述一文中加以概括。
- 联合身份验证服务配置和管理一文中介绍了其他“操作指南”文章。

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

联合身份验证服务私钥保护

Dec 05, 2017

简介

默认情况下，将通过网络服务帐户方式存储私钥并将其标记为不可导出。

有两种类型的私钥：

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

实际上有两个 RA 证书：Citrix_RegistrationAuthority_ManualAuthorization（默认有效期为 24 小时）及 Citrix_RegistrationAuthority（默认有效期为两年）。

> 在 FAS 管理控制台中的初始设置过程的步骤 3 中，当管理员单击“授权”时，FAS 服务器会生成一个密钥对，并向 CA 发送针对 Citrix_RegistrationAuthority_ManualAuthorization 证书的证书签名请求 (CSR)。这是一个临时证书，默认有效期为 24 小时。CA 不会自动颁发此证书；必须在 CA 上由管理员手动授权颁发此证书。一旦向 FAS 服务器颁发证书，FAS 将使用 Citrix_RegistrationAuthority_ManualAuthorization 证书自动获取 Citrix_RegistrationAuthority 证书（默认有效期为两年）。一旦 Citrix_RegistrationAuthority_ManualAuthorization 获得 Citrix_RegistrationAuthority 证书，FAS 服务器将删除它的证书和密钥。

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

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

- 同时针对 RA 证书和用户证书私钥的 Microsoft 增强 RSA 和 AES 加密提供程序或 Microsoft 软件密钥存储提供程序。
- 针对 RA 证书私钥的含可信平台模块 (TPM) 芯片的 Microsoft 平台密钥存储提供程序，以及针对用户证书私钥的 Microsoft 增强 RSA 和 AES 加密提供程序或 Microsoft 软件密钥存储提供程序。
- 同时针对 RA 证书和用户证书私钥的 Hardware Security Module (HSM) 供应商的加密服务或密钥存储提供程序与 HSM 设备。

私钥配置设置

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

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

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

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

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

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

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

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

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

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

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

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

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

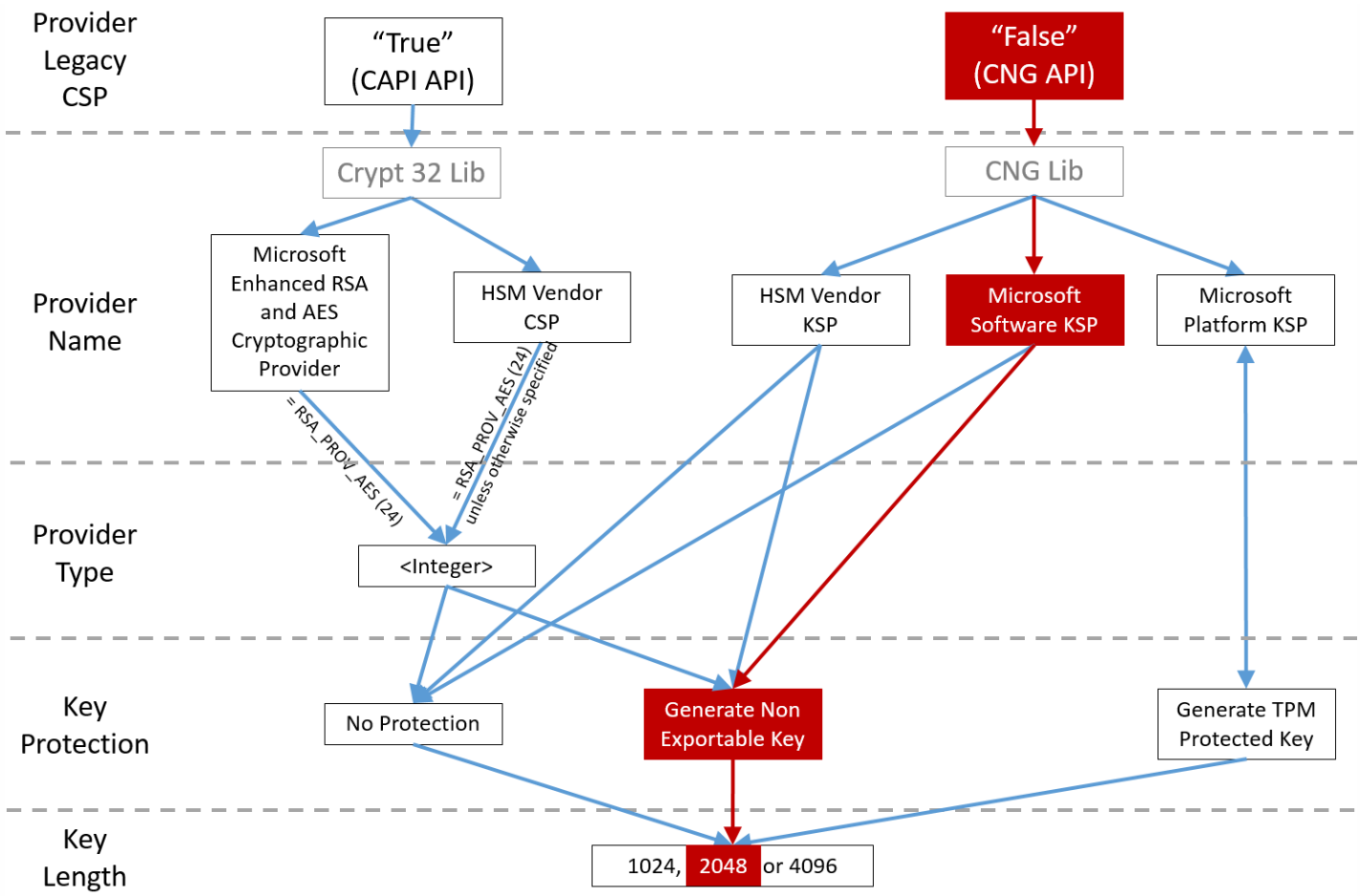
值	备注
NoProtection	可以导出私钥。
GenerateNonExportableKey	默认。无法导出私钥。
GenerateTPMProtectedKey	将使用 TPM 管理私钥。通过您在 ProviderName 中指定的 ProviderName（例如 Microsoft 平台密钥存储提供程序）存储私钥

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

值	备注
2048	默认值。也可以使用 1024 或 4096。

下方以图形方式显示了该配置文件的设置（默认安装设置显示为红色）：

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



配置方案示例

示例 1

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

这是默认的安装后配置。无需进行其他私钥配置。

示例 2

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

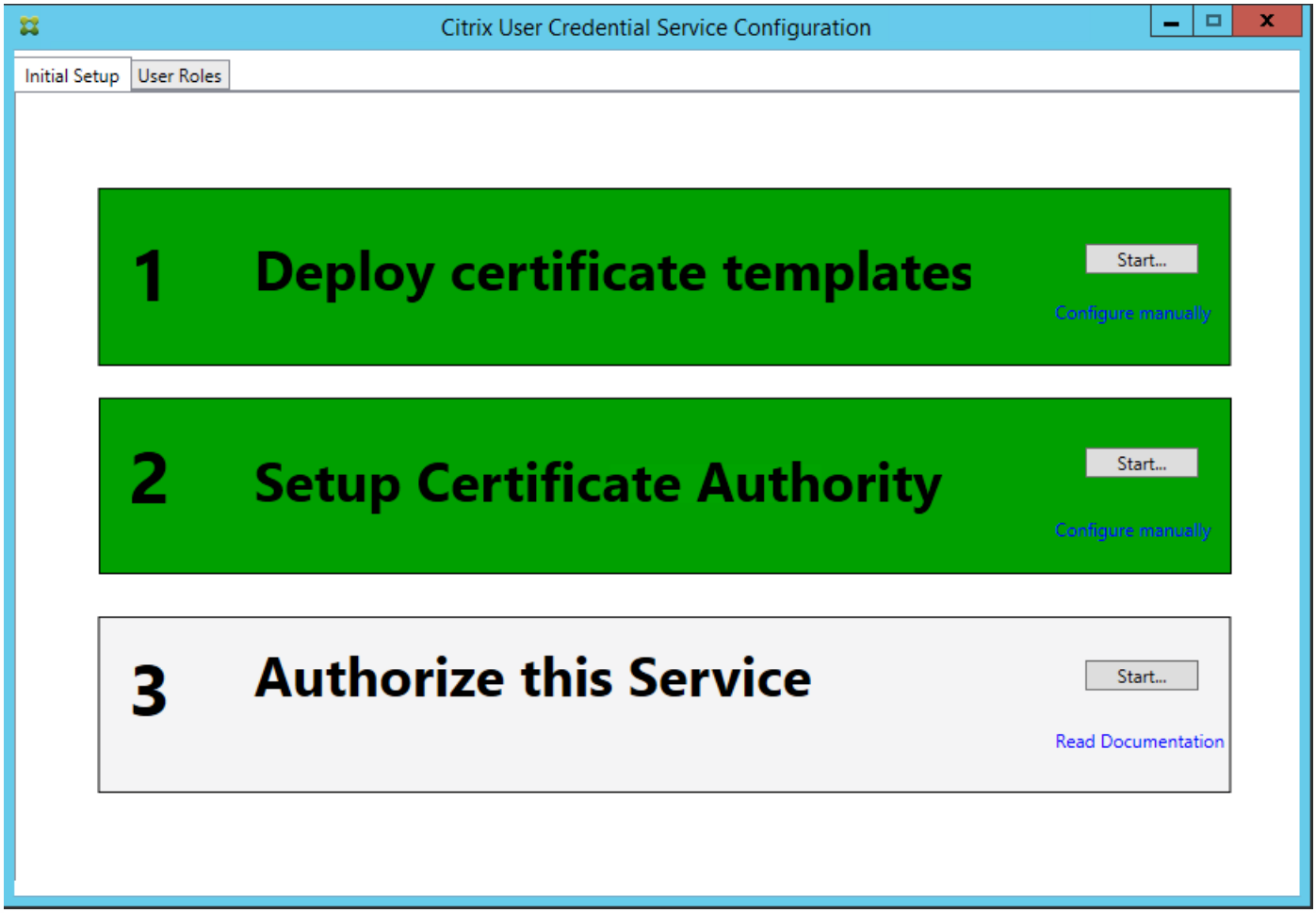
此方案假设您已根据 TPM 制造商文档在 BIOS 中启用 FAS 服务器主板上的 TPM，并已在 Windows 中初始化 TPM。请参阅 https://technet.microsoft.com/en-gb/library/cc749022(v=ws.10).aspx。

使用 PowerShell（建议）

可使用 PowerShell 以脱机方式请求 RA 证书。对于不希望其 CA 通过联机 CSR 颁发 RA 证书的组织，建议使用此方法。无法使用 FAS 管理控制台生成脱机 RA CSR。

步骤 1：在使用管理控制台对 FAS 配置进行初始设置期间，只完成前两个步骤："部署证书模板"和"设置证书颁发机构"。

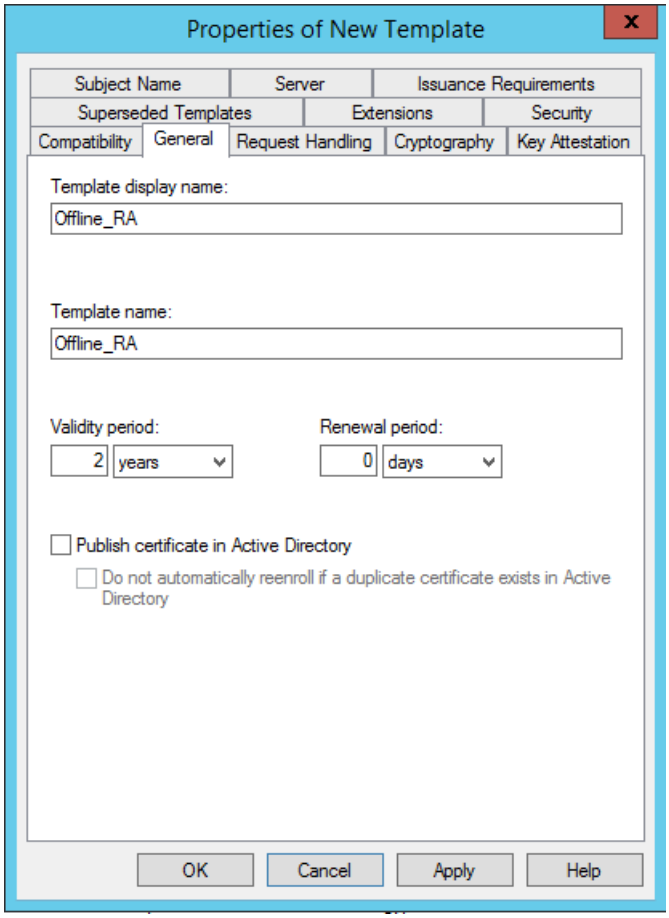
© 1999-2017 Citrix Systems, Inc. All rights reserved.



步骤 2：在 CA 服务器中，添加证书模板 MMC 管理单元。右键单击 **Citrix_RegistrationAuthority_ManualAuthorization** 模板，并选择 **Duplicate Template**（复制模板）。

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

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



步骤 3：在 CA 服务器中，添加 CA MMC 管理单元。右键单击**证书模板**。选择**新建**，然后单击**要颁发的证书模板**。选择刚才创建的模板。

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

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

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

```
New-FasAuthorizationCertificateRequest -UseTPM $true -address
```

例如：

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

将显示以下内容：

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

```
PS C:\Users\Administrator.AUTH> New-UcsAuthorizationCertificateRequest -UseTPM $true -address ucshsm.auth.local

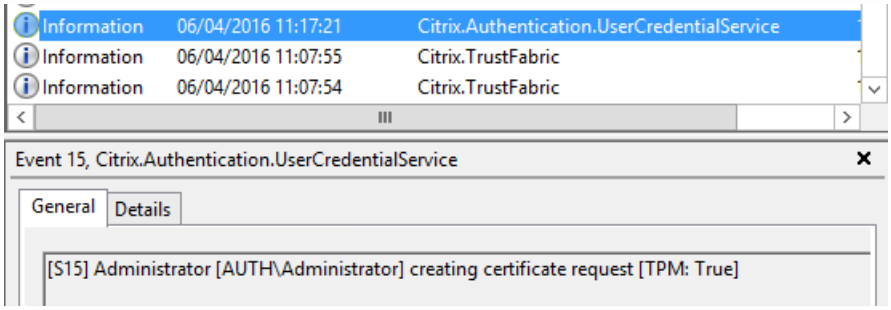
Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           :
CertificateRequest  : -----BEGIN CERTIFICATE REQUEST-----
                      MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXNORmFicmljMIIBIjANBgkq
                      hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwAtwoCLXJuJ3yIscT8Y5v/7zuYqBhbHkhZV3wTNfROXW
                      lhCMwi7X4YpTE7CbJtgiFY/9SEBa9StGeTVpeJi66gKoZCdxydc2BwX6JNZrLi9hAflbInFPgrz+
                      vbG3YjKuKtK35JpGqYWjUEDzKiQFaob3Dkh/pwP3V7DcEYthxB8CfbaN9MHOEFbepoSYOCAfunXW
                      snwIbXD9lc/fGyN/3f94P4fbNrjEIOHc+4Oy/WsPgPBgcq9XBwRjzpGjOgOWRoJS9g22OY5PwD77
                      7f7vZvoQkRy5NXXXATJ+xxYEPLp9JuJaE1WXrTJG+XP3SnG/oCCPit7iUIIc9FjGa3qTUQIDAQAB
                      oAAwDQYJKoZIhvcNAQENBQADggEBAIJV8jR9XWHlvztpjxPeJzAVDsrLpOsCfNdvYn9u+I7J8Gsr
                      4tuLjuQ+An4Y2Rw7b6pZxEICU8rqd5Gy+wtPnUZoAf6eLg1Vht2RVfb6d7Ns6+Mc+F5bFegLHs8c
                      Y1ITNOtmcHFKt4Loz5D5E+tQw39MProEj3p7GwF7HrGY+QSbFD38rbL19Z5cfNYYqMbsgyMgdR8F
                      3SmagQjN3C8lyqT8z1iF4l32xlmQrP/4XQvr1F+TD15PM5Fxjj6PEKWopWTYZXGzSC1ufxevcO1K
                      +tTH9tQYJM6xw3+6TIcfuWDjrd8KJjTdC5SMu7LJuIajTNZ5Z+1eM61TAT03XG/AB7o=
                      -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval


PS C:\Users\Administrator.AUTH> _
```

注意：

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

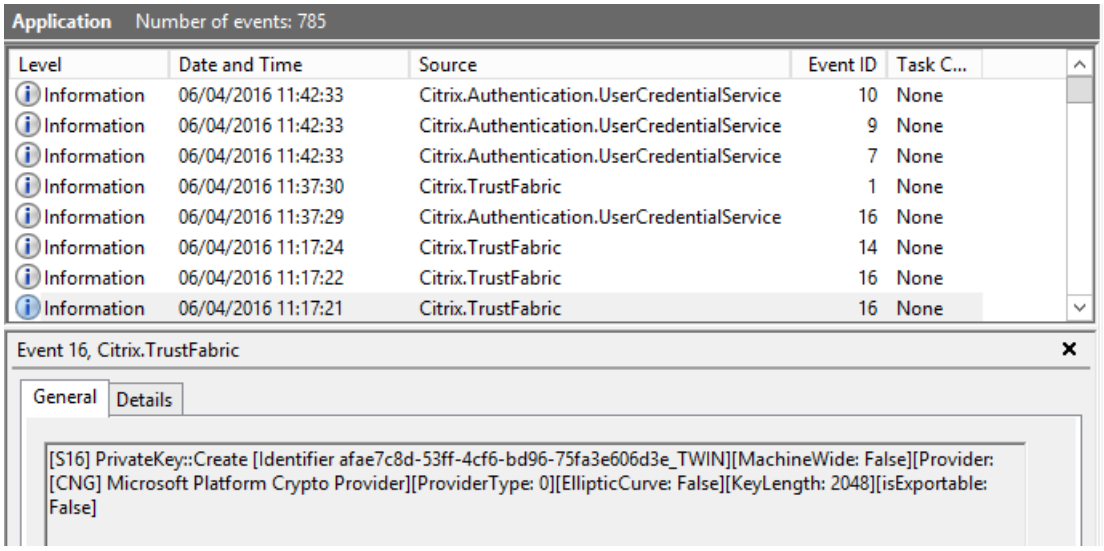
要验证用于生成密钥对的 TPM，请在生成密钥对时，在 FAS 服务器上的 Windows 事件查看器中查看应用程序日志。



记录“[TPM: True]”

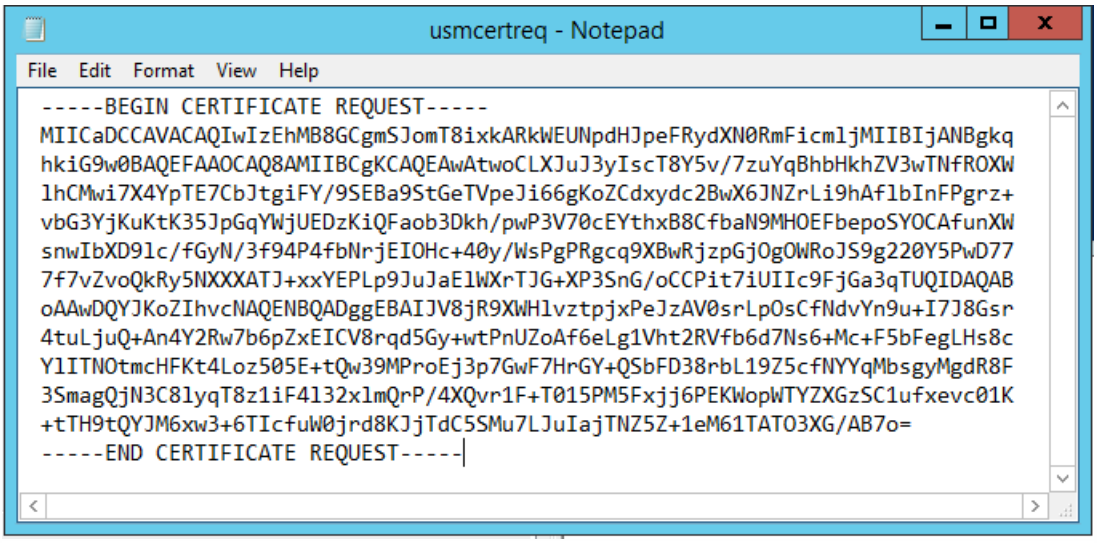
后跟：

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



记录“提供程序：[CNG] Microsoft 平台加密提供程序”

步骤 6：将证书请求部分复制到文本编辑器，并将其保存为磁盘上的文本文件。



步骤 7：通过在 FAS 服务器上的 PowerShell 中键入以下内容将 CSR 提交到 CA：

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

例如：

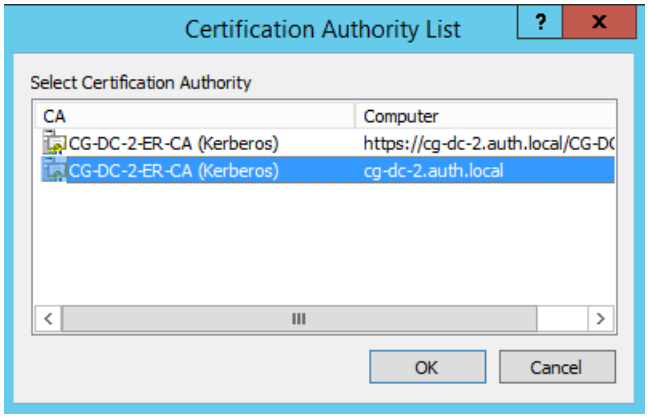
certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt

将显示以下内容：

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-0B0C-4D21-A4FD-2E29502177C2}
  ldap:
```


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

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



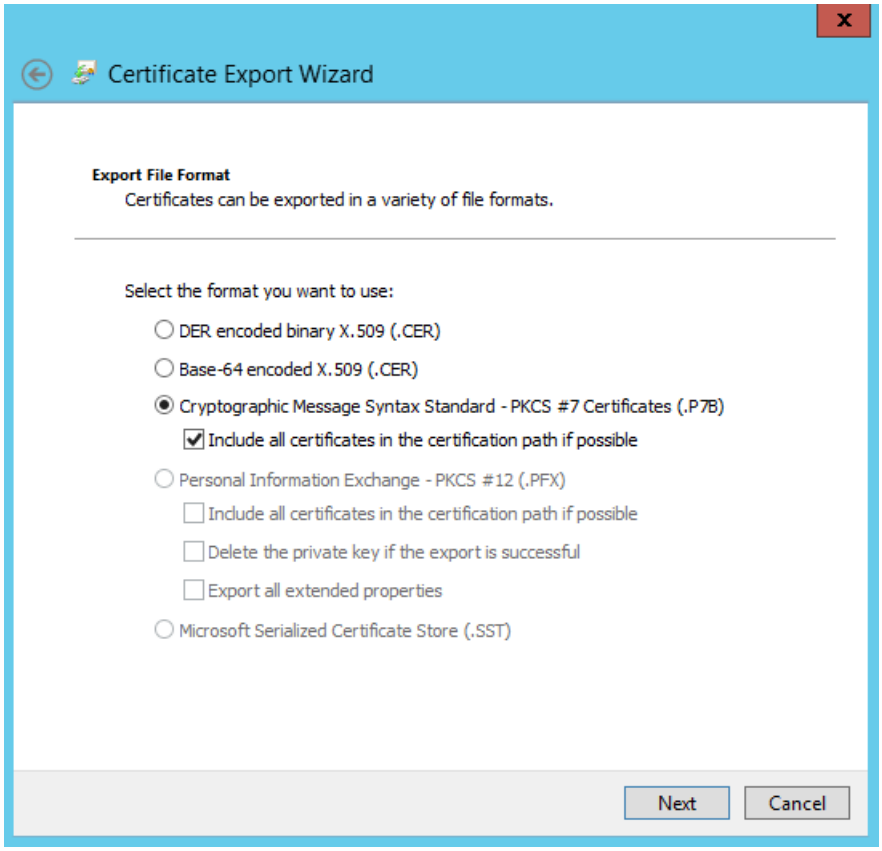
在已 CA 指定后，PowerShell 将显示 RequestID：

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-DBDC-4D21-A4FD-2E2950217C2}
  ldap:
RequestId: 106
RequestId: "106"
Certificate request is pending: Taken Under Submission (0)
PS C:\Users\Administrator.AUTH>
```

步骤 8：在 CA 服务器上，在 CA MMC 管理单元中单击 **Pending Requests**（挂起的请求）。记录请求 ID。然后右键单击该请求，并选择 **Issue**（颁发）。

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

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



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

步骤 10：将导出的证书文件复制到 FAS 服务器。

步骤 11：通过在 FAS 服务器中输入以下 PowerShell cmdlet 将 RA 证书导入 FAS 服务器注册表：

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

例如：

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

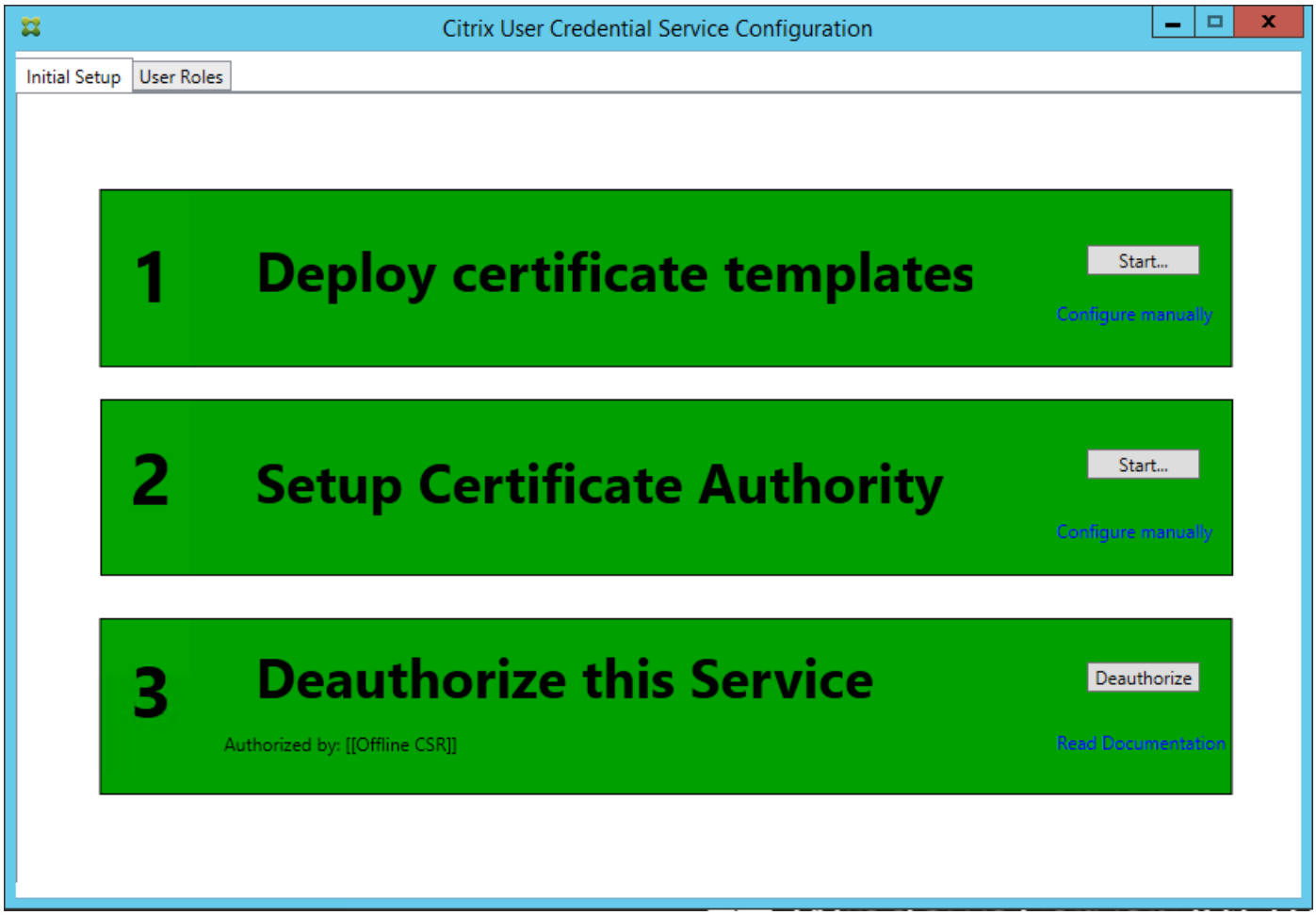
将显示以下内容：

```
PS C:\Users\Administrator.AUTH> Import-UcsAuthorizationCertificateResponse -address ucshsm.auth.local -Id 5ac3d8bd-b484-
4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile C:\Users\Administrator.AUTH\Desktop\TPM_UCS_Cert.p7b


Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           : a5c27fcc-1dd7-4c2b-8963-16ec31102dfc
CertificateRequest :
Status              : Ok
```


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

步骤 12：关闭然后重新启动 FAS 管理控制台。



请注意，步骤“授权此服务”已变为绿色，并且现在显示为“Deauthorize this Service”（取消授权此服务）。下面的条目指示“Authorized by: Offline CSR”（授权者: 脱机 CSR）

步骤 13：在 FAS 管理控制台中选择 **User Roles**（用户角色）选项卡，并编辑主要 FAS 文章中所述的设置。

注意：通过管理控制台取消授权 FAS 将会删除用户规则。

使用 FAS 管理控制台

FAS 管理控制台无法执行脱机 CSR，因此不建议使用它，除非您的组织允许为 RA 证书执行联机 CSR。

当执行 FAS 初始设置步骤时，在部署证书模板和设置 CA 之后、授权服务（配置程序中的步骤 3）之前：

步骤 1：通过更改下列行来编辑配置文件，如下所示：

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

该文件现在应显示如下：

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

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateTPMProtectedKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

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

步骤 2：授权服务。

步骤 3：从 CA 服务器手动发出挂起证书请求。获得 RA 证书后，安装过程中的步骤 3 将在管理控制台中显示为绿色。此时，将在 TPM 中生成 RA 证书的私钥。默认情况下该证书的有效期为 2 年。

步骤 4：将配置文件恢复为如下所示：

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

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

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

步骤 6：在 FAS 管理控制台中选择 User Roles（用户角色）选项卡，并按主要 FAS 文章中所述编辑设置。

注意：通过管理控制台取消授权 FAS 将会删除用户规则。

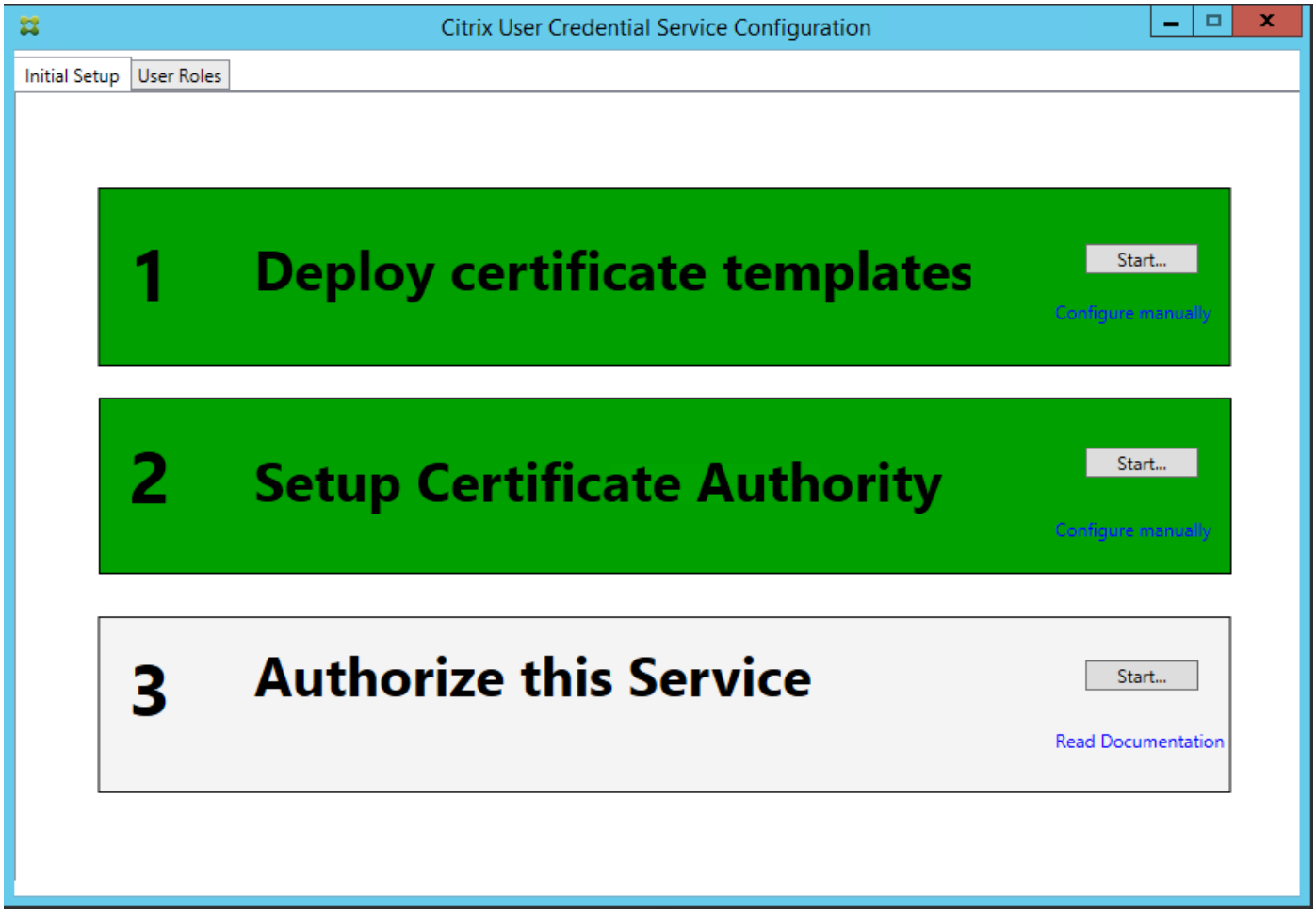
示例 3

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

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

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

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



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

步骤 3：编辑配置文件，如下所示：

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

该文件现在应显示如下：

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

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="HSM_Vendor's Key Storage Provider"/>

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

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

步骤 4：重新启动 Citrix 联合身份验证服务，以从配置文件中读取值。

步骤 5：在 HSM 内生成 RSA 密钥，并通过在 FAS 管理控制台的“Initial Setup”（初始设置）选项卡上单击 **Authorize**（授权）来创建 CSR。

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

```
[S16] PrivateKey::Create [Identifier e1608812-6693-4c54-a937-91a2e27df75b_TWIN][MachineWide: False][Provider: [CNG]
HSM_Vendor's Key Storage Provider][ProviderType: 0][EllipticCurve: False][KeyLength: 2048][isExportable: False]
```

注意：[提供程序：[CNG] HSM_Vendor's Key Storage Provider]

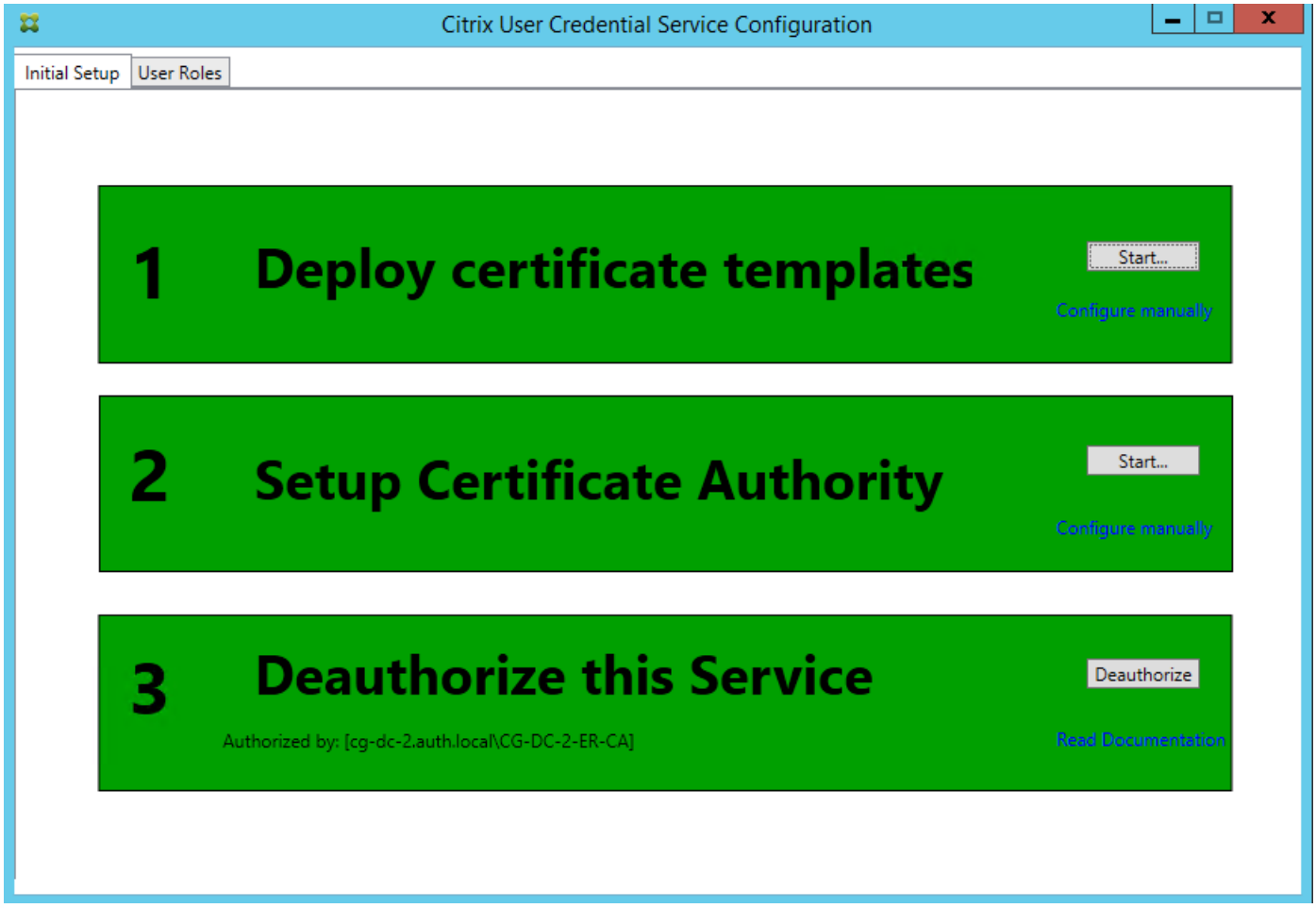
步骤 7：在 CA 服务器上的 CA MMC 中，选择 **Pending Requests**（挂起的请求）节点：

Request ID	Binary Request	Request Status Code	Request Disposition Message	Request Submission Date	Requester Name	Request Country/Region
107	-----BEGIN NE...	The operation compl...	Taken Under Submission	07/04/2016 14:04	AUTH\UCSHSM$	

右键单击该请求，并选择 **Issue**（颁发）。

请注意，步骤“授权此服务”已变为绿色，并且现在显示为“Deauthorize this Service”（取消授权此服务）。下面的条目指示“Authorized by: []”（授权者: []）

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



步骤 8：在 FAS 管理控制台中选择 **User Roles**（用户角色）选项卡，并按主要 FAS 文章中所述编辑设置。

注意：通过管理控制台取消授权 FAS 将会删除用户规则。

FAS 存储证书

FAS 不使用 FAS 服务器上的 Microsoft 证书存储来存储证书。它将使用注册表。

注意：当使用 HSM 存储私钥时，HSM 容器通过 GUID 进行标识。HSM 中的私钥 GUID 与注册表中相当证书的 GUID 匹配。

要确定 GUID RA 证书，请在 FAS 服务器中输入以下 PowerShell cmdlet：

```
Add-pssnapin Citrix.a*
Get-FasAuthorizationCertificate –address
```

例如：

```
Get-FasAuthorizationCertificate –address cg-fas-2.auth.net
```


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

```
PS C:\Users\Administrator.AUTH> Get-UcsAuthorizationCertificate -address cg-ucs-2.auth.local


Id                  : a3958424-b8c3-4cac-ba0d-7eb3ce24591c
Address             : cg-dc-2.auth.local\CG-DC-2-ER-CA
TrustArea           : 3df77088-00e0-4dca-a47a-28060dc16986
CertificateRequest  :
Status              : MaintenanceDue

Id                  : fcb185f9-5069-4e34-8625-a333ac126535
Address             : [Offline CSR]
TrustArea           :
CertificateRequest  : -----BEGIN CERTIFICATE REQUEST-----
                      MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXNORmFicmljMIIBIjANBgkq
                      hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxyNzaiWX8DhUnOZMS2YVSDhr36AV5BGeIYOGVCFKvZPe
                      Rmm/xOVM6cNKsLbew3dYlbo+vdgWg86DFRVxTORhollV86iazDZyOiYGgxe9/s8YZzCspVWN1nB1
                      zXOUJfo1qo9UsmImYr7MR/dhGAtkfsFUoPcd2+zcezmgOfq/4vmCIuerwqzRR5T/p4og7+IjR1se
                      ECz/CbXROOuiDhW+VWbjcsgklcavzvC/jR33F9dZSXNgKRiGHgfd/lBb3elZKA4OOoi90u64Q916
                      3ba9BnihqxIgvwWILOmyUfiJmCgbhLJV4TPBopOdKz/axZEIO5p5XYVjCcpXqhqL7Ppn1wIDAQAB
                      oAAwDQYJKoZIhvcNAQENBQADggEBAJhdvw6yrLGBMtAgo3oPL6o8/at+IqHjHKqgcJNJO/MU7/7X
                      bZB46drLPFzpzF88DkmfoCEgOxlbzFX9waaiFs9CHC/AcEzblN925y1gqljsfC3l5TCKBAeLFoMl
                      PSEkfYMQUOSBYCuLlkFn1LXLSeQ3qJTzSvptYROawFmUMQLffwLSR1vOuS8DJSrpASrwdXJk3TOa
                      GlO/xJo/NRMOwMH+AvGbBsgp3l+jnDjXED5RudqARfgVgcW714JP+XIeFrE1TZmUL2skNIXEPNHC
                      H8eAHdYD26caFigydfefbjx4fbaJDFHJs5+1tnrTZ9knCrawhUiIyOMLGZOOaiER+z8=
                      -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval
```

要获得用户证书列表，请输入：

Get-FasUserCertificate –address

例如：

Get-FasUserCertificate –address cg-fas-2.auth.net

```
PS C:\Users\Administrator.AUTH> Get-UcsUserCertificate -address cg-ucs-2.auth.local


ThumbPrint            : 7BA22879F40EE92125A2F96E7DD2D52C73820459
UserPrincipalName     : walter@adfs.ext
Role                  : default
CertificateDefinition : default_Definition
ExpiryDate            : 05/04/2016 12:02:13
```

相关信息

- 联合身份验证服务一文是 FAS 安装和配置的主要参考资料。
- 通用 FAS 部署在联合身份验证服务体系结构概述一文中加以概括。
- 联合身份验证服务配置和管理一文中介绍了其他“操作指南”文章。

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

联合身份验证服务的安全性和网络配置

Dec 05, 2017

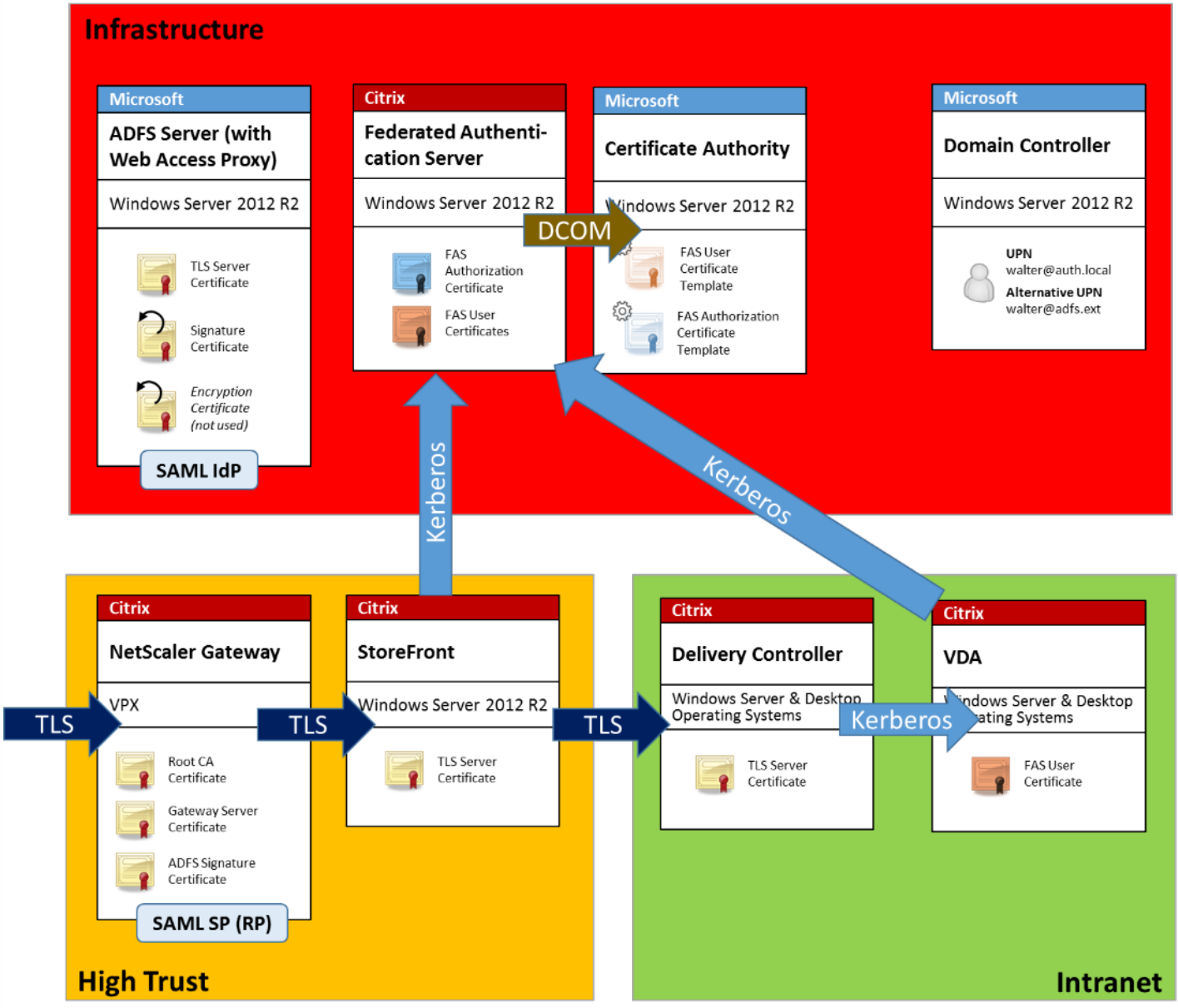
Citrix 联合身份验证服务 (FAS) 与 Microsoft Active Directory 和 Microsoft 证书颁发结构 (CA) 紧密集成。 确保恰当管理系统和确保系统安全非常重要，因此，请像对域控制器或其他关键性基础结构一样制定安全策略。

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

网络体系结构

下图显示了 FAS 部署中使用的主要组件和安全范围。

应将 FAS 服务器以及 CA 和域控制器视为安全关键型基础结构的一部分。 在联合环境中，Citrix NetScaler 和 Citrix StoreFront 是受信任的用于执行用户身份验证的组件；其他 XenApp 和 XenDesktop 组件不受引入 FAS 影响。



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

防火墙和网络安全性

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

StoreFront 服务器使用相互身份验证的 Kerberos 通过端口 80 访问 FAS 服务器。 身份验证使用 FAS 服务器的 Kerberos HOST/fqdn 标识以及 StoreFront 服务器的 Kerberos 计算机帐户标识。 这将生成 Citrix Virtual Delivery Agent (VDA) 登录用户时所需的一个使用一次的“凭据句柄”。

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

Microsoft CA 接受使用通过 Kerberos 验证的 DCOM 的通信，可以将其配置为使用固定 TCP 端口。 此外，CA 还要求 FAS 服务器提供通过受信任的注册代理证书签名的 CMC 数据包。

服务器	防火墙端口
联合身份验证服务	[输入] 从 StoreFront 和 VDA 至基于 HTTP 的 Kerberos [输出] DCOM 至 Microsoft CA
Netscaler	[输入] 从客户端计算机至 HTTPS [输入/输出] 从 StoreFront 服务器至 HTTPS 或从 HTTPS 至 StoreFront 服务器 [输出] HDX 至 VDA
StoreFront	[输入] 从 NetScaler 至 HTTPS [输出] HTTPS 至 Delivery Controller [输出] Kerberos HTTP 至 FAS
Delivery Controller	[输入] 从 StoreFront 服务器至 HTTPS [输入/输出] 从 VDA 至基于 HTTP 的 Kerberos
VDA	[输入/输出] 从 Delivery Controller 至基于 HTTP 的 Kerberos [输入] 从 NetScaler Gateway 至 HDX [输出] Kerberos HTTP 至 FAS

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

Microsoft CA	[输入] FAS 至 DCOM 且已签名

管理职责

可以将对环境的管理职责分为以下几组：

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

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

组策略设置

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

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

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

证书模板

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

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

重命名证书模板

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

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

修改常规属性

您可以修改证书模板中的有效期。

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

修改请求处理属性

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

修改加密属性

请勿修改这些属性。FAS 会忽略证书模板中的这些设置。

有关 FAS 提供的等效设置，请参阅联合身份验证服务私钥保护。

修改密钥证明属性

请勿修改这些属性。FAS 不支持密钥证明。

修改被取代的模板属性

请勿修改这些属性。FAS 不支持取代模板。

修改扩展属性

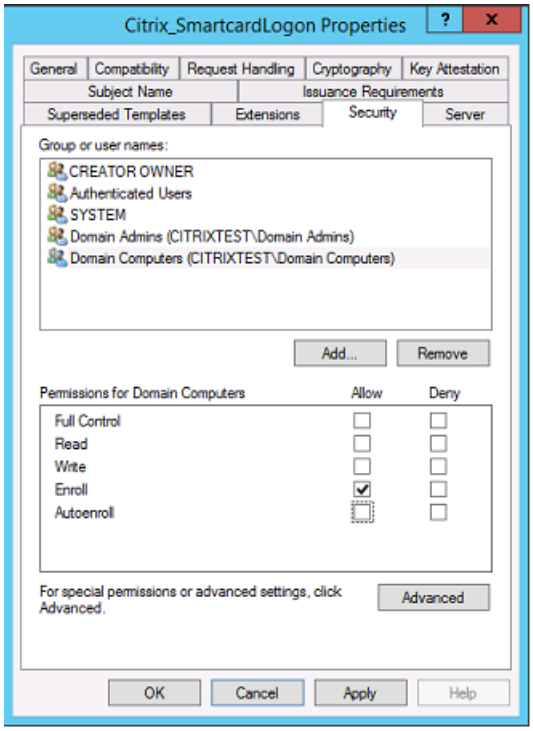
您可以修改这些设置以符合您的组织策略。

注意： 不合适的扩展设置可能会导致出现安全问题，或导致证书无法使用。

修改安全属性

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

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



修改使用者名称属性

您可以修改这些设置以符合您的组织策略（如果需要）。

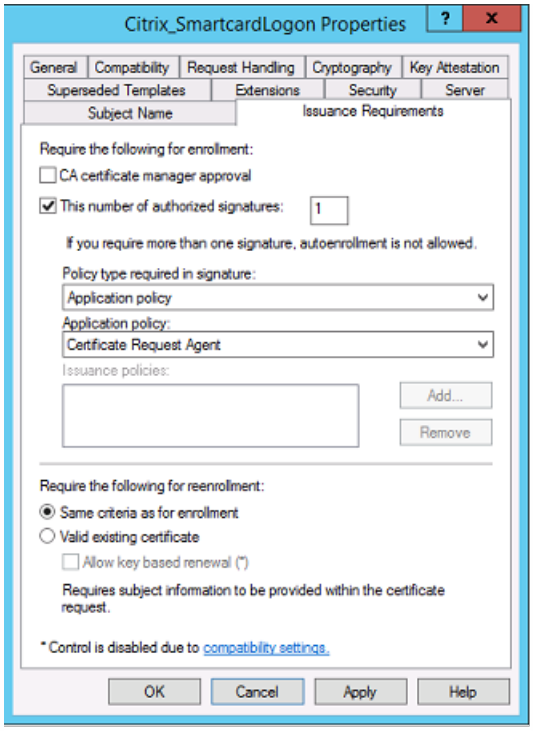
修改服务器属性

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

修改颁发要求属性

请勿修改这些设置。这些设置应该如下所示：

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



修改兼容性属性

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

证书颁发机构管理

CA 管理员负责配置 CA 服务器以及颁发 CA 服务器使用的证书私钥。

发布模板

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

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

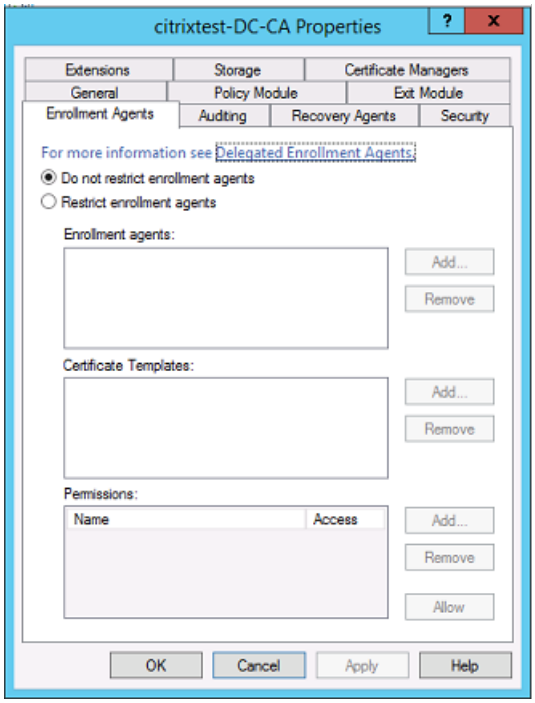
防火墙设置

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

限制注册

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

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



策略模块和审核

对于高级部署，可以使用自定义安全模块来跟踪和否决证书颁发。

FAS 管理

FAS 具有多项安全功能。

通过 ACL 限制 StoreFront、用户和 VDA

FAS 安全模块的核心是控制哪些 Kerberos 帐户能够访问功能：

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

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

配置规则

如果有多个独立 XenApp 或 XenDesktop 部署采用相同的 FAS 服务器基础结构，规则将非常有用。 每个规则都有一组独立的配置选项；具体而言，可以单独配置 ACL。

配置 CA 和模板

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

会话中证书和身份验证证书

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

私钥保护和密钥长度

FAS 管理员可以将 FAS 配置为在硬件安全模块 (HSM) 或可信平台模块 (TPM) 中存储私钥。 Citrix 建议您应至少通过将 RA 证书私钥存储在 TPM 中来保护私钥；此选项在“脱机”证书申请过程中提供。

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

事件日志

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

管理访问权限和管理工具

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

XenApp、XenDesktop 和 VDA 管理员

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

常规 Windows 服务器安全性

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

应将审核日志和事件日志安全地存储在远程计算机上。

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

相关信息

- 联合身份验证服务一文是 FAS 安装和配置的主要参考资料。

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

- 联合身份验证服务体系结构概述一文中介绍了 FAS 体系结构。
- 联合身份验证服务配置和管理一文中介绍了其他“操作指南”文章。

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

联合身份验证服务解决了 Windows 登录问题

Dec 05, 2017

在本文中：

- 证书和公钥基础结构
- UPN 名称和证书映射
- 控制登录域控制器选择
- 启用帐户审核事件
- 证书验证日志
- Kerberos 日志
- 事件日志消息
- 最终用户错误消息
- 相关信息

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

证书和公钥基础结构

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

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

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

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

UseCachedCRLOnlyAnd IgnoreRevocationUnknownErrors	禁用吊销检查（通常在域控制器上设置）。

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

UPN 名称和证书映射

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

Active Directory 中的 UPN 名称

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

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

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

证书映射服务

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

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

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

控制登录域控制器选择

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

控制域控制器选择

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

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

```
1.2.3.4   dcnetbiosname #PRE #DOM:mydomai
```


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

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

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

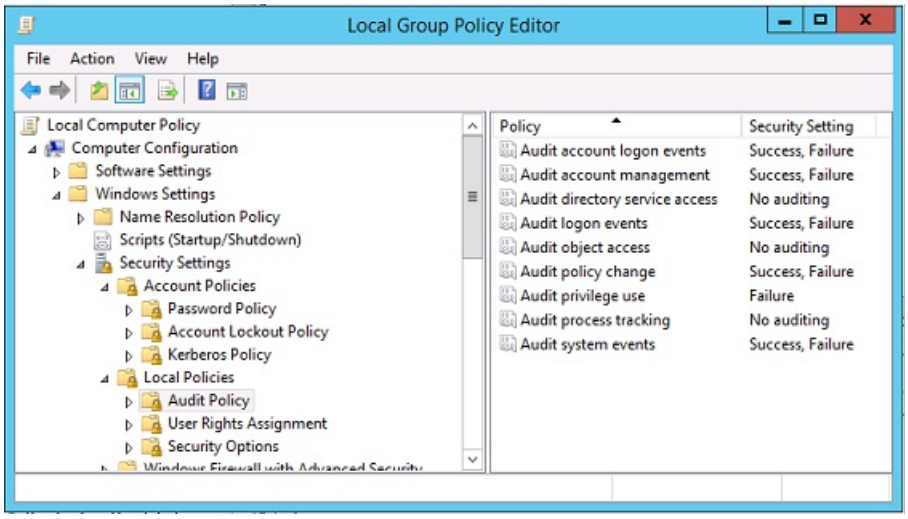
识别正在使用的域控制器

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

与身份验证有关的日志存储在此命令返回的计算机中。

启用帐户审核事件

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



证书验证日志

检查证书有效性

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

启用 CAPI 日志记录

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

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

值	说明
DiagLevel (DWORD)	详细级别（0 到 5）

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

DiagMatchAnyMask (QUADWORD)	事件过滤器（对所有事件使用 0xffffff）
DiagProcessName (MULTI_SZ)	按进程名称过滤（例如，LSASS.exe）

CAPI 日志

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

错误消息

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

Kerberos 日志

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

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

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

CurrentControlSet\Control\Lsa\Kerberos\Parameters	KerbDebuglevel	0xffffffff
CurrentControlSet\Services\Kdc	KdcDebugLevel	0x1
CurrentControlSet\Services\Kdc	KdcExtraLogLevel	0x1f

Kerberos 日志记录输出到系统事件日志中。

- “不受信任的证书”等消息应能够轻松诊断。
- 下面两个错误代码为信息性代码，可以安全地忽略：
  - KDC_ERR_PREAUTH_REQUIRED（用于与较旧的域控制器的后向兼容性）
  - 未知错误 0x4b

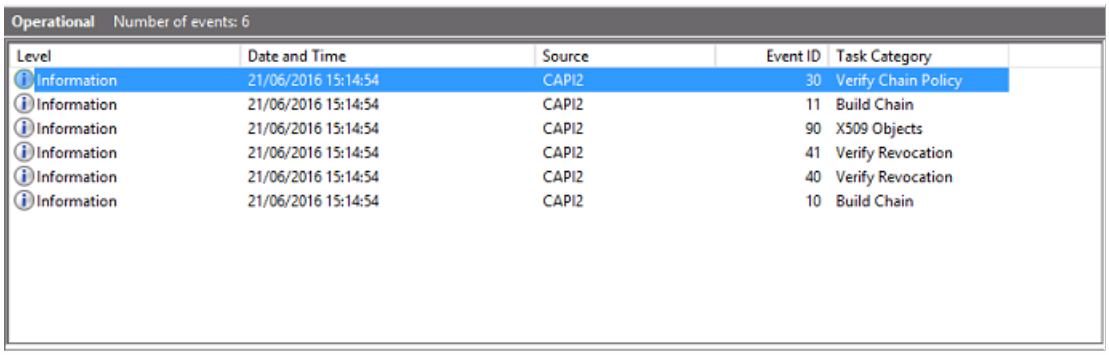
事件日志消息

本节介绍了用户使用证书登录时域控制器和工作站上的预期日志条目。

- 域控制器 CAPI2 日志
- 域控制器安全日志
- VDA 安全日志
- VDA CAPI 日志
- VDA 系统日志

域控制器 CAPI2 日志

登录过程中，域控制器将验证调用者的证书，从而生成以下格式的一系列日志条目。



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

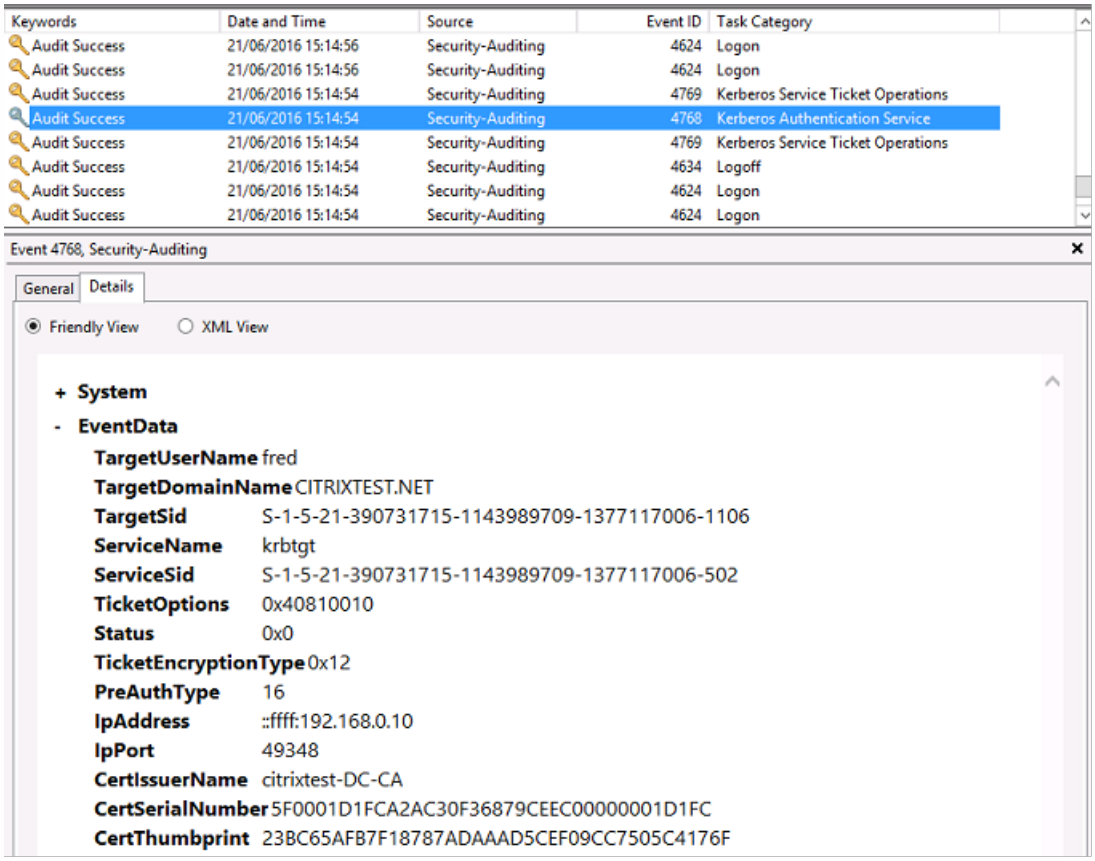
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **CertVerifyCertificateChainPolicy**
  - **Policy**
    - [**type**] CERT_CHAIN_POLICY_NT_AUTH
    - [**constant**] 6
  - **Certificate**
    - [**fileRef**] 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F.cer
    - [**subjectName**] fred
  - **CertificateChain**
    - [**chainRef**] {FF03F79B-52F8-4C93-877A-5DFFE40B9574}
  - **Flags**
    - [**value**] 0
  - **Status**
    - [**chainIndex**] -1
    - [**elementIndex**] -1
  - **EventAuxInfo**
    - [**ProcessName**] lsass.exe
  - **CorrelationAuxInfo**
    - [**TaskId**] {F5E7FD3F-628F-4C76-9B1C-49FED786318F}
    - [**SeqNumber**] 1
  - **Result**
    - [**value**] 0

域控制器安全日志

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

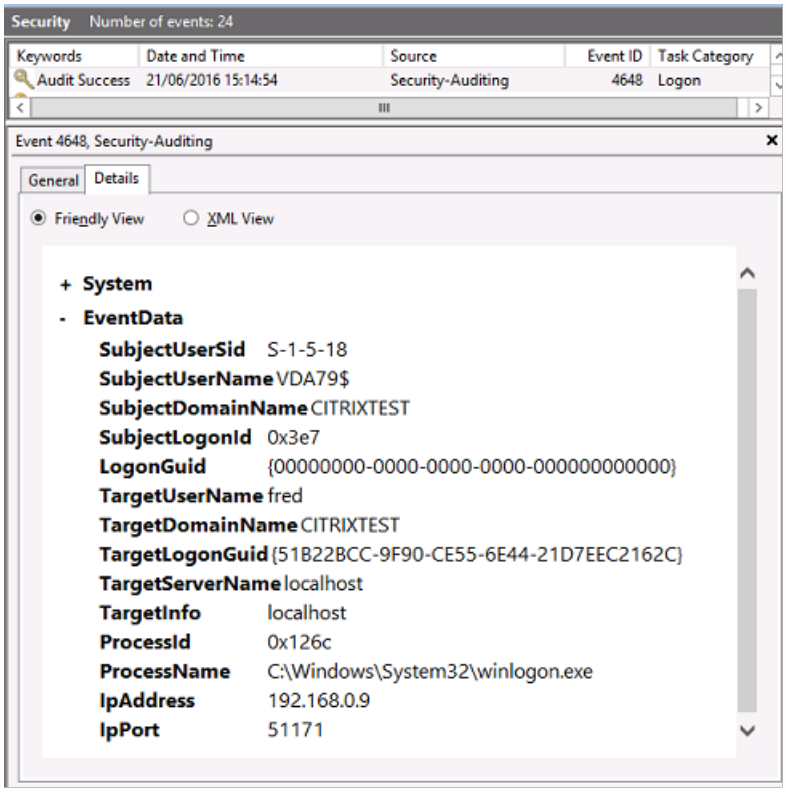
在此消息之前显示的消息将显示用于进行身份验证以登录域控制器的服务器的计算机帐户。在此消息之后显示的消息将显示属于正在用于针对域控制器进行身份验证的新 krbtgt 的用户帐户。



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

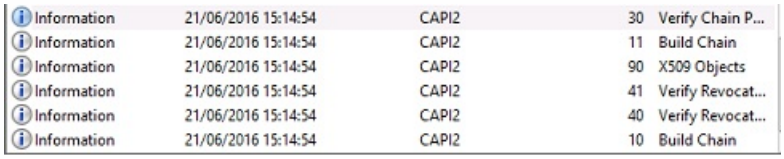
VDA 安全日志

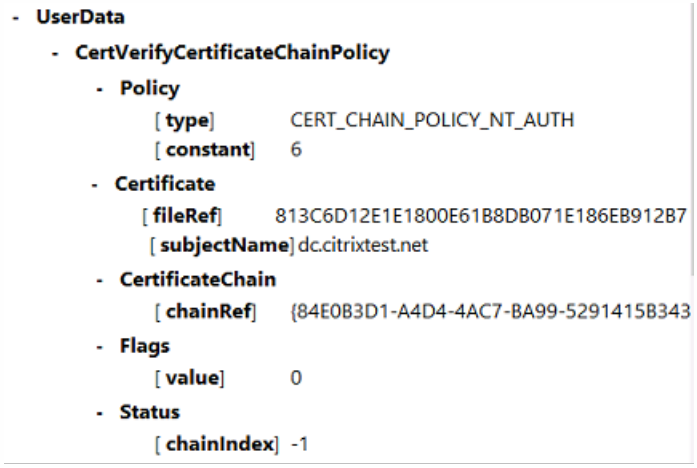
与登录事件相对应的 VDA 安全审核日志是指 winlogon.exe 中事件 ID 为 4648 的条目。



VDA CAPI 日志

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

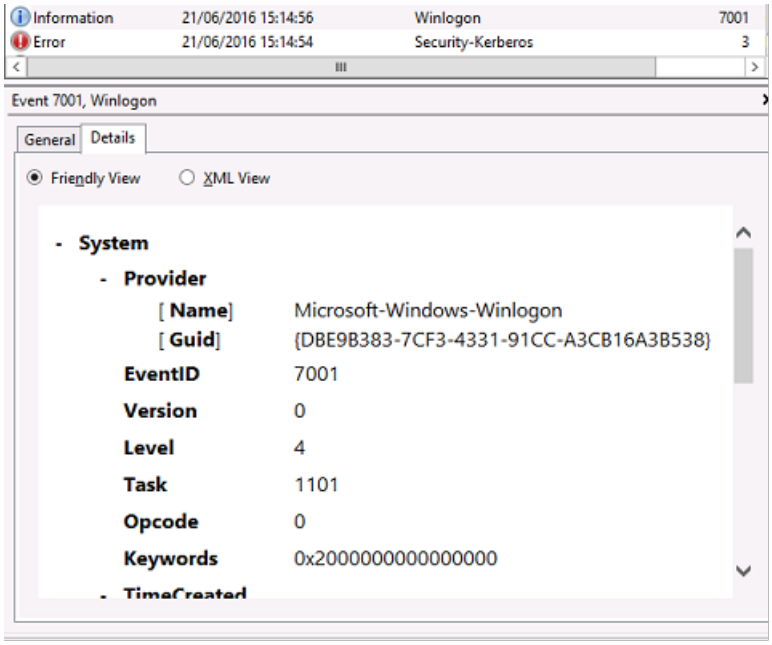




© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDA 系统日志

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



最终用户错误消息

本节列出了在 Windows 登录页面上向用户显示的常见错误消息。

显示的错误消息	说明和参考
无效用户名或密码	计算机相信您拥有有效的证书和私钥，但 Kerberos 域控制器拒绝了连接。参阅本文的 Kerberos 登录部分。
系统无法让您登录。无法验证您的凭据。 不支持该请求	无法访问域控制器，或者域控制器未安装恰当的证书。 在域控制器上重新注册“域控制器”和“域控制器身份验证”证书，如 CTX206156 中所述。此操作通常值得一试，即使在现有证书可能有效时也是如此。
系统无法让您登录。用于身份验证的智能卡证书不受信任。	未在本地计算机上安装中间证书和根证书。有关在未加入域的计算机上安装智能卡证书的说明，请参阅 CTX206156。此外，还请参阅本文中的证书和公钥基础结构部分。
无法登录的原因是您的帐户不支持智能卡登录。	未将工作组用户帐户完全配置为执行智能卡登录。

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

请求的密钥不存在	证书引用不可访问的私钥。PIV 卡未完全配置并且缺少 CHUID 或 CCC 文件时会出现此问题。
尝试使用智能卡时出错	未正确安装智能卡中间件。有关智能卡的安装说明，请参阅 CTX206156。
Insert a smart card（插入智能卡）	未检测到智能卡或读卡器。如果插入了智能卡，则此消息指示存在硬件或中间件问题。有关智能卡的安装说明，请参阅 CTX206156。
PIN 不正确	智能卡拒绝了用户输入的 PIN。
找不到有效的智能卡证书。	可能未正确设置证书上的扩展名，或者 RSA 密钥太短（小于 2048 位）。有关生成有效的智能卡证书的信息，请参阅 CTX206901。
智能卡被阻止	智能卡已被锁定（例如，用户多次输入了错误的 PIN）。 管理员可能对智能卡的 PIN 解锁 (puk) 代码具有访问权限，并且可以使用智能卡供应商提供的工具重置用户的 PIN。 如果 puk 代码不可用，或者被锁定，则必须将智能卡重置为出厂设置。
请求错误	智能卡私钥不支持域控制器要求的加密。例如，域控制器可能已申请“私钥解密”，但智能卡仅支持签名。 这通常指示未正确设置证书上的扩展名，或者 RSA 密钥太短（小于 2048 位）。有关生成有效的智能卡证书的信息，请参阅 CTX206901。

相关信息

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

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

联合身份验证服务 PowerShell cmdlet

Dec 05, 2017

可使用联合身份验证服务管理控制台执行简单的部署。不过，PowerShell 界面中提供了更多的高级选项。如果您计划使用未在控制台中提供的选项，Citrix 建议仅使用 PowerShell 进行配置。

以下命令将添加 FAS PowerShell cmdlet：

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

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

下面链接的 zip 文件中包含针对所有 FAS PowerShell SDK cmdlet 的帮助文件。要使用帮助文件，请单击相应链接。将下载 zip 文件。然后，将 zip 文件的内容解压缩到本地文件夹。index.html 文件列出了所有 cmdlet，以及指向各 cmdlet 的帮助文件的链接。



联合身份验证服务 PowerShell cmdlet 帮助文件

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

图形

Dec 05, 2017

Citrix HDX 图形包括一套广泛的图形加速和编码技术，用于优化从 XenApp 和 XenDesktop 进行的丰富图形应用程序的交付。使用图形密集型虚拟应用程序远程工作时，图形技术提供的体验与使用物理桌面时相同。

您可以使用软件或硬件进行图形呈现。软件呈现需要名为软件光栅器的第三方库。例如，Windows 包括适用于基于 DirectX 的图形的 WARP 光栅器。有时，您可能希望使用备用软件呈现器（例如， OpenGL Software Accelerator）。硬件呈现（硬件加速）需要图形处理器 (GPU)。

HDX 图形提供已针对常见用例优化的默认编码配置。使用 Citrix 策略时，IT 管理员还可以配置各种与图形有关的设置，以满足不同的要求和提供所需的用户体验。

Thinwire

Thinwire 是 XenApp 和 XenDesktop 中使用的 Citrix 默认显示远程处理技术。

显示远程处理技术允许一台计算机上生成的图形传输（通常跨网络）到另一台计算机上进行显示。图形是由于用户输入（例如，按键或鼠标操作）而生成。

HDX 3D Pro

借助 XenApp 和 XenDesktop 中的 HDX 3D Pro 功能，可以交付通过使用图形处理器 (GPU) 进行硬件加速实现最佳性能的桌面和应用程序。这些应用程序包括基于 OpenGL 和 DirectX 的 3D 专业图形应用程序。标准 VDA 仅支持 DirectX 的 GPU 加速。

适用于 Windows 桌面操作系统的 GPU 加速

使用 HDX 3D Pro 时，您可以在桌面操作系统计算机上随托管桌面或应用程序交付图形密集型应用程序。HDX 3D Pro 支持物理主机计算机（包括桌面、刀片式服务器和机架工作站）以及 XenServer、vSphere 和 Hyper-V（仅限直通）虚拟机管理程序提供的 GPU 直通和 GPU 虚拟化技术。

利用 GPU 直通功能，可以创建对专用图形处理硬件具有独占访问权限的 VM。可以在虚拟机管理程序上安装多个 GPU，并将 VM 一对一地分配给每个 GPU。

利用 GPU 虚拟化技术，多个虚拟机可以直接访问单个物理 GPU 的图形处理功能。

Windows 服务器操作系统 GPU 加速

通过 HDX 3D Pro，在 Windows 服务器操作系统会话中运行的图形密集型应用程序可以在服务器图形处理器 (GPU) 上呈现。通过将 OpenGL、DirectX、Direct3D 和 Windows Presentation Foundation (WPF) 呈现移至服务器 GPU，图形呈现不会降低服务器 CPU 的速率。服务器还能够处理更多图形，因为工作负载在 CPU 和 GPU 之间进行了拆分。

Framehawk

Framehawk 是适用于移动工作人员的显示远程处理技术，主要针对宽带无线连接（Wi-Fi 和 4G/LTE 蜂窝网络）。Framehawk 克服了光谱干扰和多径传播等挑战，为虚拟应用和桌面用户提供了流畅的交互式用户体验。

OpenGL Software Accelerator

OpenGL Software Accelerator 是一个适用于 OpenGL 应用程序（例如 ArcGIS、Google Earth、Nehe、Maya、Blender、Voxler、计算机辅助设计和计算机辅助制造）的软件光栅器。借助 OpenGL Software Accelerator，有时不需要使用图形卡即

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

可通过 OpenGL 应用程序提供优异的用户体验。

相关信息

- Thinwire
- HDX 3D Pro
- GPU acceleration for Windows Desktop OS
- GPU acceleration for Windows Server OS
- Framehawk
- OpenGL Software Accelerator

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

Framehawk

Dec 05, 2017

Framehawk 是适用于移动工作人员的显示远程处理技术，主要针对宽带无线连接（Wi-Fi 和 4G/LTE 蜂窝网络）。Framehawk 克服了光谱干扰和多径传播等挑战，为虚拟应用和桌面用户提供了流畅的交互式用户体验。对于少量数据包丢失即可造成用户体验降级的长距离（高延迟）宽带网络连接用户来说，Framehawk 可能是一种合适的选择。我们建议您为此用例使用自适应传输 - 有关详细信息，请参阅自适应传输。

您可以按照适合贵公司的方式，使用 Citrix 策略模板为一组用户和访问场景实施 Framehawk。Framehawk 以单屏移动用例为服务对象，例如，便携式计算机和平板电脑。在实时交互性能的商业价值为服务器资源和宽带连接需求的额外成本提供有力佐证的场合使用 Framehawk。

Framehawk 何以能够保持流畅的用户体验

可以将 Framehawk 设想为用软件实现的人眼，即观察帧缓冲区中的内容，并分辨出屏幕上显示的不同内容类型。对于用户来说，什么因素更重要呢？屏幕区域变化很快时，例如视频或移动图像，丢失部分像素对于人眼来说可能无关紧要，因为丢失的数据很快就会被新数据覆盖。

但是，对于保持静止的屏幕区域，例如通知区域或工具栏中的图标，或滚动到用户希望开始阅读的位置后显示的文本，人眼是非常挑剔。用户希望这些区域的像素能够完美呈现出来。与那些旨在从 **1 和 0** 角度实现技术准确性的协议不同，Framehawk 的目标与使用技术的人相关。

Framehawk 包括下一代 QoS 信号放大器和基于时间的热度地图，用以实现粒度精细且更加有效的工作负载识别。除了数据压缩，它还使用自动化的自愈式转换，并且可以避免数据重传，从而保持单击响应、准确性和一致的节奏。在失真的网络连接中，Framehawk 可以通过插补掩蔽丢失，用户仍可以感受到良好的图像质量，同时享受更加流畅的体验。此外，Framehawk 算法还可以智能地区分不同类型的数据包丢失。例如，随机丢失（发送更多数据进行补偿）与拥堵丢失（通道发生拥堵，不再发送更多数据）。

Citrix Receiver 中的 Framehawk Intent Engine 可以区分向上滚动或向下滚动、缩放、向左移或向右移、读取、键入及其他常见操作。引擎还使用共享字典管理传回到 Virtual Delivery Agent (VDA) 的通信。如果用户正在尝试阅读，文本的视觉质量必须出色。如果用户正在滚动，则必须快速且流畅。并且必须可中断，以便用户始终能够掌控与应用程序或桌面的交互。

通过测量网络连接的节奏（称为**传动**，类似于自行车链条的拉伸），Framehawk 逻辑会加快反应速度，从而在高延迟连接下提供卓越的体验。这种独特的传动系统专利产品可以持续提供关于网络情况的最新反馈，从而使 Framehawk 立即对带宽、延迟和丢失方面的变化做出反应。

使用 Thinwire 和 Framehawk 的设计要点

尽管 Thinwire 已成为带宽效率行业的领先技术并且适用于范围广泛的访问情形和网络条件，但它使用 TCP 来实现可靠的数据通信。因此，必须在有损或负载过重的网络上重新涮出数据包，从而导致在用户体验方面发展缓慢。基于启发式数据传输 (enlightened data transport, EDT) 层的 Thinwire 可用，从而解决了高延迟网络连接上 TCP 的限制。

Framehawk 使用基于用户数据报协议 (UDP) 构建的数据传输层。（UDP 是 Framehawk 解决数据丢失问题的方法的一小部分，这一点您可以在将 Framehawk 的性能与其他基于 UDP 的协议相比较时得出。UDP 为以人为中心的、使 Framehawk 分离的技术提供了重要的基础。

Framehawk 需要多少带宽？

无线带宽的重要性取决于多种因素，其中包括共享连接的用户数量、连接的质量和所使用的应用程序。为实现最佳性能，Citrix 建议 4 Mbps 或 5 Mbps 以及每个并发用户大约 150 Kbps 的基本设置。

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

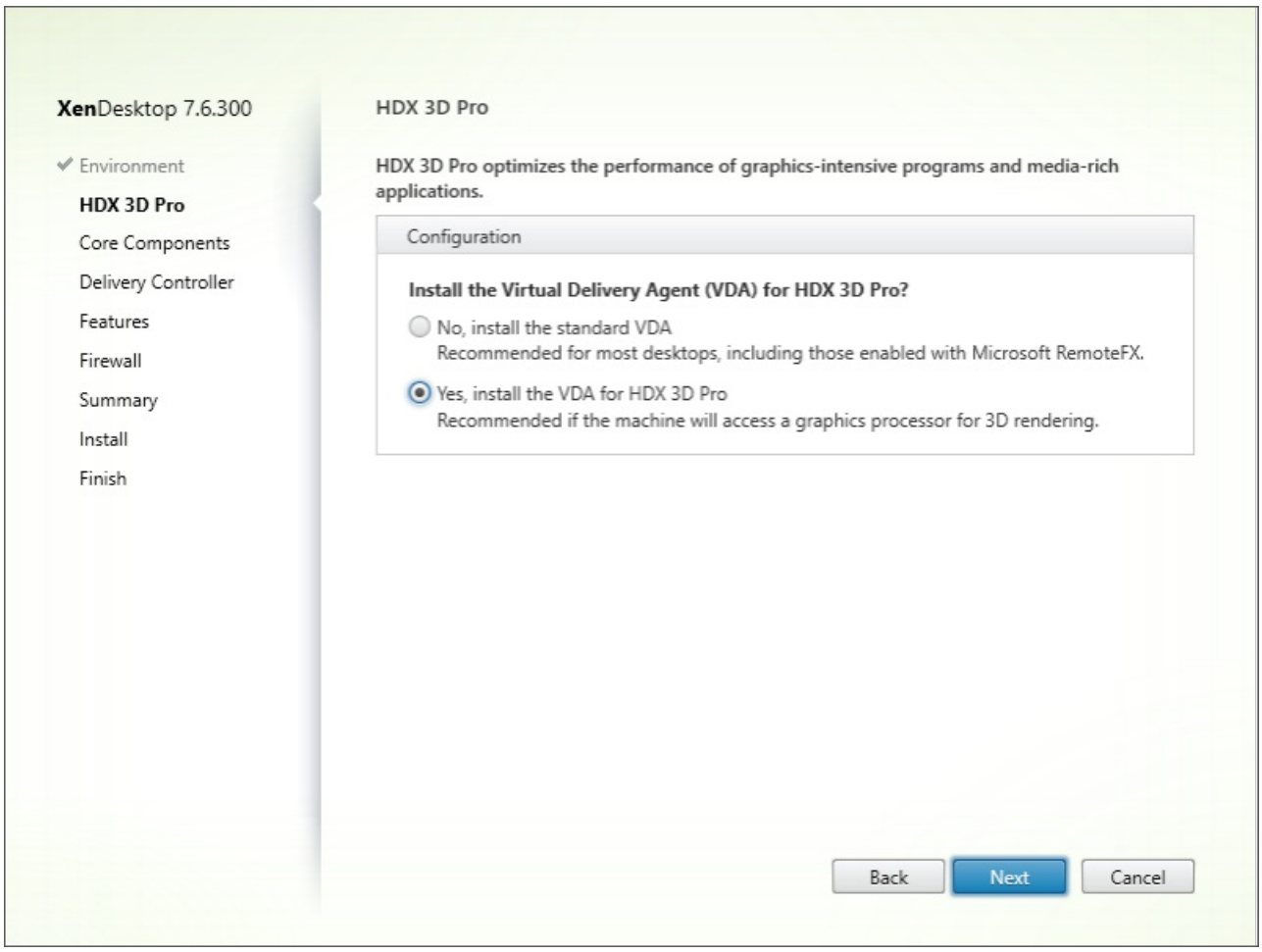
我们对 Thinwire 的带宽建议通常是每个用户在 1.5 Mbps 的基础上增加 150 Kbps。有关详细信息，请参阅 XenApp 和 XenDesktop 带宽博客。）数据包丢失率为 3% 时，您会发现通过 TCP 的 Thinwire 需要的带宽高于 Framehawk，才能维护正面的用户体验。

Thinwire 仍是 ICA 协议中主显示远程处理通道。默认情况下，Framehawk 处于禁用状态。Citrix 建议有选择地启用此功能，以解决组织内的带宽无线访问问题。请记住，Framehawk 需要的服务器资源（CPU 和内存）远高于 Thinwire。

Framehawk 和 HDX 3D Pro

Framehawk 支持 XenApp（服务器操作系统）应用程序和 XenDesktop（桌面操作系统）应用程序的所有 HDX 3D Pro 用例。已在延迟为 400-500 毫秒、数据包丢失率为 1-2% 的客户环境中对其进行验证。因此，使用典型的 3D 建模应用程序（例如 AutoCAD、Siemens NX 等）时提供了良好的交互性。借助此项支持，功能得到了扩展，无论是外出还是在离岸地点工作，或者在网络状况不佳的情况下，均可查看和操作大型 CAD 模型。（鼓励要求通过长距离网络连接交付 3D 应用程序的组织使用自适应传输功能。有关详细信息，请参阅自适应传输。）

启用该功能不需要执行任何其他配置任务。安装 VDA 时，请安装前选择 3DPro 选项：



选择此选项后，HDX 将使用 GPU 供应商视频驱动程序来代替 Citrix 视频驱动程序。通过 Thinwire 传输时，默认使用全屏 H.264 编码，而非常用的默认自适应显示和 Selective H.264 编码。

要求和注意事项

Framehawk 至少需要 VDA 7.6.300 和组策略管理 7.6.300。

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

端点必须至少具有 Citrix Receiver for Windows 4.3.100 或 Citrix Receiver for iOS 6.0.1。

默认情况下，Framehawk 会使用双向用户数据报协议 (UDP) 端口范围 (3224-3324) 与 Citrix Receiver 交换 Framehawk 显示通道数据。可以在策略设置 **Framehawk 显示通道端口范围**中自定义该范围。客户端与虚拟桌面之间的每个并发连接需要唯一的端口。对于多用户操作系统环境（如 XenApp 服务器），请定义足够多的端口以支持最大并发用户会话数。对于单用户操作系统（如 VDI 桌面），定义一个 UDP 端口即可满足要求。Framehawk 尝试使用第一个定义端口，逐渐使用到范围中定义的最后一个端口。这适用于通过 NetScaler Gateway 传递和直接与 StoreFront 服务器建立内部连接两种情况。

对于远程访问，必须部署 NetScaler Gateway。默认情况下，NetScaler 使用 UDP 端口 443 进行客户端 Citrix Receiver 与此网关之间的加密通信。此端口在任何外部防火墙上均应该处于打开状态以允许两个方向的安全通信。此功能称为数据报传输安全性 (Datagram Transport Security, DTLS)。

注意：FIPS 设备不支持 Framehawk/DTLS 连接。

从 NetScaler Gateway 11.0.62 和 NetScaler Unified Gateway 11.0.64.34 或更高版本开始，可支持加密的 Framehawk 连接。

从 XenApp 和 XenDesktop 7.12 开始支持 NetScaler 高可用性 (HA)。

在实施 Framehawk 之前请考虑以下最佳做法：

- 联系安全管理员以确认为 Framehawk 定义的 UDP 端口在防火墙上处于打开状态。安装过程不会自动配置防火墙。
- 通常情况下，NetScaler Gateway 可能会安装在 DMZ 中，在内外两侧均设置防火墙。请务必在外部防火墙中打开 UDP 端口 443。如果环境要使用默认端口范围，请务必在外部防火墙中打开 UDP 端口 3224-3324。

配置

小心：Citrix 建议仅为可能经历严重数据包丢失问题的用户启用 Framehawk。我们建议您不要启用 Framehawk 作为站点中所有对象的通用策略。

默认情况下，Framehawk 处于禁用状态。启用后，服务器将尝试对用户图形和输入使用 Framehawk。如果由于某些原因不满足必备条件，将使用默认模式 (Thinwire) 建立连接。

下列策略设置影响 Framehawk：

- Framehawk 显示通道：启用或禁用此功能。
- Framehawk 显示通道端口范围：指定 VDA 用于与用户设备交换 Framehawk 显示通道数据的 UDP 端口号范围（最低端口号到最高端口号）。VDA 会尝试使用每个端口，从最低端口号开始，然后每次尝试都增加端口号。端口处理入站和出站通信。

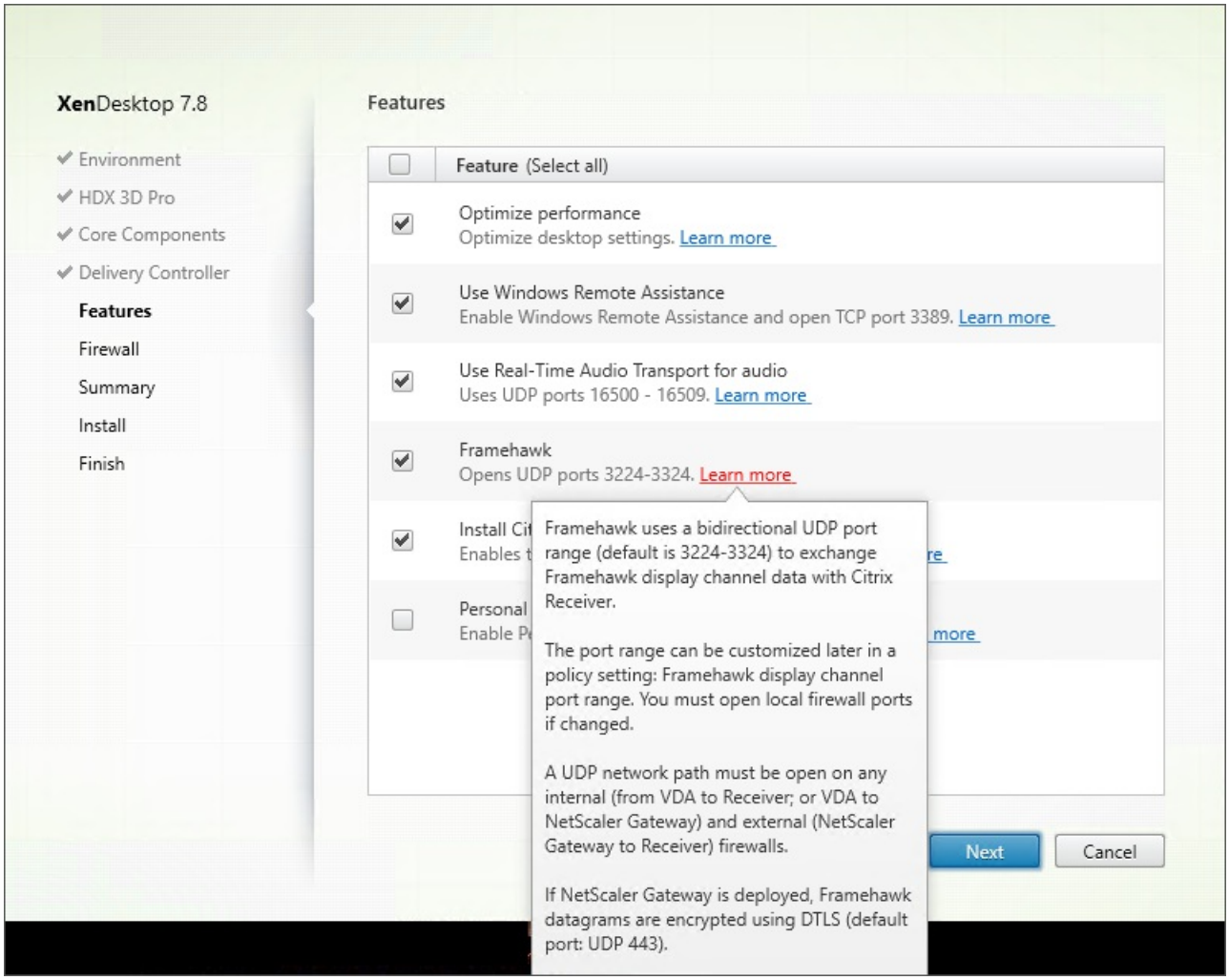
打开用于 Framehawk 显示通道的端口

从 XenApp 和 XenDesktop 7.8 开始，VDA 安装程序的**功能**步骤中提供了一个用于重新配置防火墙的选项。如果选中此复选框，则会在 Windows 防火墙中打开 UDP 端口 3224-3324。在某些情况下需要手动配置防火墙：

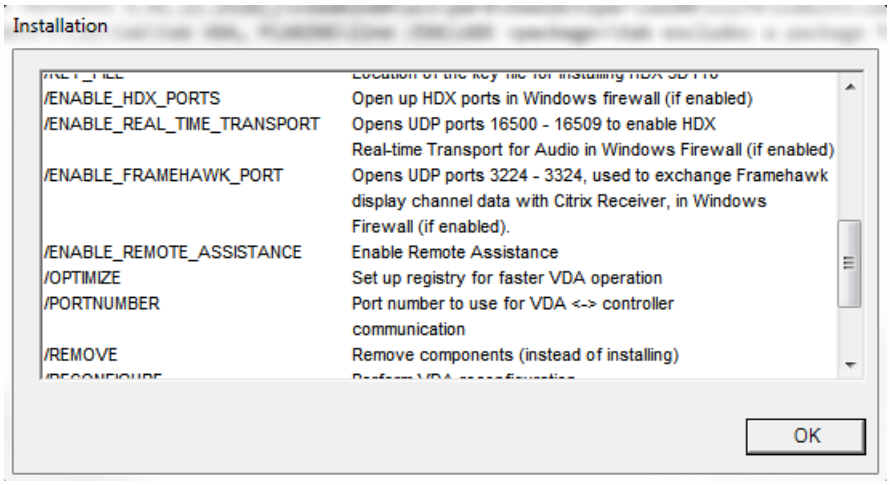
- 适用于所有网络防火墙。
  或者
- 默认端口范围是自定义的。

要打开这些 UDP 端口，请选中 **Framehawk** 复选框：

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



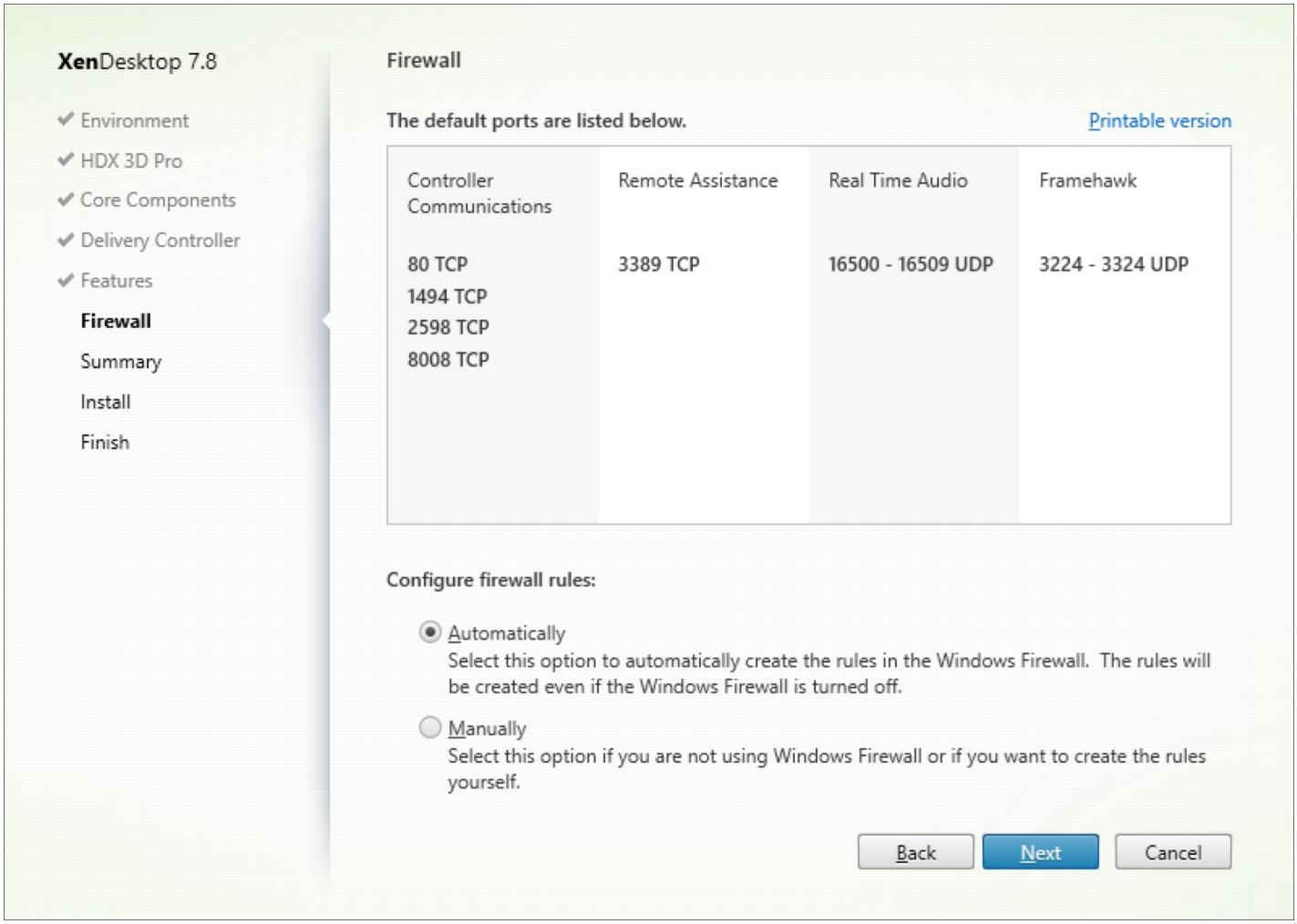
您也可以在命令行中使用 **/ENABLE_FRAMEHAWK_PORT** 打开用于 Framehawk 的 UDP 端口：



验证 Framehawk UDP 端口分配

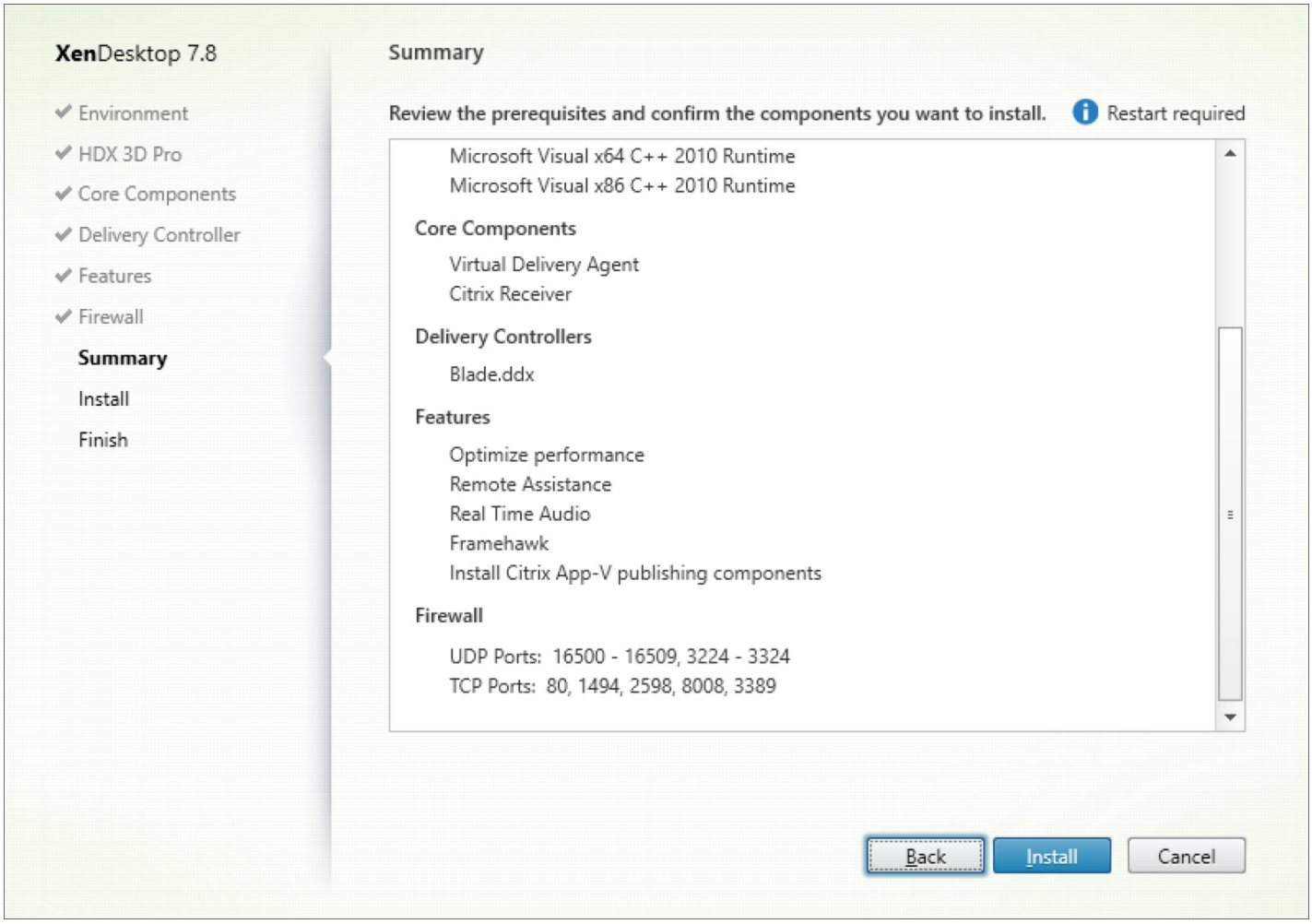
安装期间，您可以在**防火墙**屏幕中验证分配给 Framehawk 的 UDP 端口。

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



摘要屏幕会指示是否启用了Framehawk 功能：

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



NetScaler Gateway 对 Framehawk 的支持

NetScaler Gateway 11.0.62.10 或更高版本以及 NetScaler Unified Gateway 11.0.64.34 或更高版本均支持加密的 Framehawk 流量。

- NetScaler Gateway 是指可以直接从最终用户设备访问 Gateway VPN vServer 的部署体系结构。即，VPN vServer 分配有公用 IP 地址，并且用户直接连接到此 IP 地址。
- 采用 Unified Gateway 的 NetScaler 是指 Gateway VPN 虚拟服务器作为目标绑定到内容交换 (CS) 虚拟服务器的部署。在此环境中，CS vServer 具有公用 Internet 协议地址，Gateway VPN vServer 具有虚拟 Internet 协议地址。

要在 NetScaler Gateway 上启用 Framehawk 支持，必须启用 Gateway VPN 虚拟服务器级别的 DTLS 参数。启用此参数并正确更新 XenApp 或 XenDesktop 上的组件后，Framehawk 音频、视频和交互流量将在 Gateway VPN 虚拟服务器与用户设备之间加密。

Framehawk 支持 NetScaler Gateway、Unified Gateway 和 NetScaler Gateway + 全局服务器负载平衡。

Framehawk 不支持以下情景：

- HDX Insight
- 采用 IPv6 模式的 NetScaler Gateway
- NetScaler Gateway 双跳
- 采用群集设置的 NetScaler Gateway

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

方案	Framehawk 支持
NetScaler Gateway	是
NetScaler + 全局服务器负载平衡	是
采用 Unified Gateway 的 NetScaler	是 注意：支持 Unified Gateway 11.0.64.34 及更高版本。
HDX Insight	否
采用 IPv6 模式的 NetScaler Gateway	否
NetScaler Gateway 双跳	否
NetScaler Gateway 上的多个 Secure Ticket Authority (STA)	是
NetScaler Gateway 和高可用性 (HA)	是
NetScaler Gateway 和群集设置	否

配置 NetScaler 以支持 Framehawk

要在 NetScaler Gateway 上启用 Framehawk 支持，请在 Gateway VPN *vServer*级别启用 DTLS 参数。启用此参数并正确更新 XenApp 或 XenDesktop 上的组件后，Framehawk 音频、视频和交互流量将在 Gateway VPN 虚拟服务器与用户设备之间加密。

如果在 NetScaler Gateway 上为远程访问启用 UDP 加密，则需要执行此配置。

配置 NetScaler 以支持 Framehawk 时：

- 确保在所有外部防火墙上打开 UDP 端口 443
- 确保在所有外部防火墙上打开 CGP 端口（默认为 2598）
- 在设置中为 VPN 虚拟服务器启用 DTLS
- 取消并重新绑定 SSL 证书-密钥对。如果您使用的是 NetScaler 11.0.64.34 或更高版本，则不需要执行此步骤。

要配置 NetScaler Gateway 以支持 Framehawk，请执行以下操作：

1. 部署并配置 NetScaler Gateway 以与 StoreFront 通信并为 XenApp 和 XenDesktop 进行用户身份验证。
2. 在 NetScaler 的“Configuration”（配置）选项卡中，展开“NetScaler Gateway”，然后选择 **Virtual Servers**（虚拟服务器）。
3. 单击 **Edit**（编辑）以显示 VPN 虚拟服务器的基本设置；确认 DTLS 设置的状态。
4. 单击 **More**（更多）以显示更多配置选项：
5. 选择 **DTLS**，为数据报协议（如 Framehawk）提供通信安全。单击**确定**。VPN 虚拟服务器的“Basic Settings”（基本设置）

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

区域显示 DTLS 标志设置为 **True**（真）。

6. 重新打开“Server Certificate Binding”（服务器证书绑定）屏幕，单击 **+** 以绑定证书密钥对。
7. 选中之前的证书密钥对，单击 **Select**（选择）。
8. 保存对服务器证书绑定所做的更改。
9. 保存后，将显示证书密钥对。单击 **Bind**（绑定）。
10. 如果显示 **No usable ciphers configured on the SSL vserver/service**（SSL 虚拟服务器/服务上没有配置可用的密码）警告消息，请忽略。

适用于 NetScaler Gateway 早期版本的步骤

如果您正在使用 NetScaler Gateway 11.0.64.34 之前的版本，请执行以下操作：

1. 重新打开“Server Certificate Binding”（服务器证书绑定）屏幕，单击 + 以绑定证书密钥对。
2. 选中先前的证书密钥对，然后单击 **Select**（选择）。
3. 保存对服务器证书绑定所做的更改。
4. 保存后，将显示证书密钥对。单击 **Bind**（绑定）。
5. 如果显示 **No usable ciphers configured on the SSL vserver/service**（SSL 虚拟服务器/服务上没有配置可用的密码）警告消息，请忽略。

要配置 Unified Gateway 以支持 Framehawk，请执行以下操作：

1. 确保已安装和正确配置 Unified Gateway。有关其他信息，请参阅 Citrix 产品文档站点上的 Unified Gateway 信息。
2. 在已绑定到 CS *vServer* 作为目标 *vServer* 的 VPN *vServer* 上启用 DTLS 参数。

限制

如果客户端设备上存在 NetScaler Gateway 虚拟服务器的过时 DNS 条目，自适应传输和 Framehawk 可能会回退到 TCP 传输，而非 UDP 传输。如果发生回退到 TCP 传输，请刷新客户端上的 DNS 缓存并使用 UDP 传输重新连接以建立会话。

对其他 VPN 产品的支持

NetScaler Gateway 是唯一可支持 Framehawk 所需的 UDP 加密的 SSL VPN 产品。如果使用的是另一个 SSL VPN 或不正确的 NetScaler Gateway 版本，Framehawk 策略可能无法应用。传统的 IPsec VPN 产品支持没有任何修改的 Framehawk。

配置 Citrix Receiver for iOS 以支持 Framehawk

要配置较低版本的 Citrix Receiver for iOS 以支持 Framehawk，必须手动编辑 default.ica。

1. 在 StoreFront 服务器上，在 c:\inetpub\wwwroot\ 中访问应用商店的 App_Data 目录。
2. 打开 default.ica 文件并在 WFClient 部分添加以下行：Framehawk=On
3. 保存更改。

此过程允许在 iOS 设备上从兼容的 Citrix Receiver 建立 Framehawk 会话。如果您使用的是 Citrix Receiver for Windows，则不需要此步骤。

> **注意**
>
> 使用 Receiver for iOS 7.0 及更高版本时，不需要在 default.ica 文件中显式添加 **Framehawk=On** 参数。

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

监视 Framehawk

您可以从 Citrix Director 监视 Framehawk 的使用情况和性能。“HDX 虚拟通道详细信息”视图包含有助于监视所有会话中的 Framehawk 和排除其故障的有用信息。要查看与 Framehawk 有关的衡量指标，请选择 **Graphics-Framehawk**。

如果已建立 Framehawk 连接，详细信息页面中将显示 **Provider = VD3D**（提供程序 = VD3D）和 **Connected = True**（已连接 = True）。虚拟通道处于空闲状态为正常现象，因为它监视信号通道，仅在初始握手时使用。此页面还提供关于连接的其他有用统计信息。

如果遇到问题，请参阅 Framehawk 故障排除博客。

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

HDX 3D Pro

Dec 05, 2017

借助 XenApp 和 XenDesktop 的 HDX 3D Pro 功能，可以交付通过使用图形处理器 (GPU) 进行硬件加速实现最佳性能的桌面和应用程序。这些应用程序包括基于 OpenGL 和 DirectX 的 3D 专业图形应用程序。标准 VDA 仅支持 DirectX 的 GPU 加速。有关选择标准或 HDX 3D Pro VDA 的详细信息，请参阅安装 VDA 一文中的“步骤 5. 选择是否启用 HDX 3D Pro 模式”。

所有支持的 Citrix Receiver 都可以使用 3D 图形。为了在具有复杂 3D 工作负载、使用高分辨率显示器、多显示器配置和高帧速率应用程序时获得最佳性能，我们建议使用最新版本的 Citrix Receiver for Windows 和 Citrix Receiver for Linux。有关支持的 Citrix Receiver 版本的详细信息，请参阅 Citrix Receiver 的生命周期里程碑。

三维专业应用程序示例包括：

- 计算机辅助设计、制造和工程处理 (CAD/CAM/CAE) 应用程序
- 地理信息系统 (GIS) 软件
- 用于医学成像的图形存档与通信系统 (PACS)
- 使用最新 OpenGL、DirectX、NVIDIA CUDA、OpenCL 和 WebGL 版本的应用程序
- 使用 NVIDIA 统一计算设备架构 (CUDA) GPU 实现并行计算的计算密集型非图形应用程序

HDX 3D Pro 在任何带宽条件下均可提供最佳用户体验：

- 在 WAN 连接条件下：通过带宽低至 1.5 Mbps 的 WAN 连接提供交互式用户体验。
- 在 LAN 连接条件下：提供等同于使用 LAN 连接的本地桌面的用户体验。
  可以将图形处理转移到数据中心进行集中管理，从而以简单的用户设备代替复杂且昂贵的工作站。

HDX 3D Pro 为 Windows 桌面操作系统计算机和 Windows Server 操作系统计算机提供 GPU 加速。有关详细信息，请参阅适用于 Windows 桌面操作系统的 GPU 加速和适用于 Windows 服务器操作系统的 GPU 加速。

HDX 3D Pro 与以下虚拟机管理程序提供的 GPU 直通和 GPU 虚拟化技术兼容，也与裸机兼容：

- Citrix XenServer
  - 使用 NVIDIA GRID 和 Intel GVT-d 实现的 GPU 直通
  - 使用 NVIDIA GRID 和 Intel GVT-g 实现的 GPU 虚拟化
- Microsoft Hyper V
  - 使用 NVIDIA GRID 和 AMD 实现的 GPU 直通（离散设备分配）
- VMware vSphere
  - 使用 NVIDIA GRID、Intel 和 AMD IOMMU 实现的 GPU 直通 (vDGA)
  - 使用 NVIDIA GRID 和 AMD MxGPU 实现的 GPU 虚拟化

有关受支持的 XenServer 版本，请参阅 Citrix XenServer Hardware Compatibility List（Citrix XenServer 硬件兼容性列表）。

使用 HDX Monitor 工具可以验证 HDX 虚拟化技术的操作和配置，并可以对 HDX 问题进行诊断和故障排除。要下载此工具并了解其详细信息，请参阅 https://taas.citrix.com/hdx/download/。

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

适用于 Windows 桌面操作系统的 GPU 加速

Dec 05, 2017

通过 HDX 3D Pro，可在桌面操作系统计算机上随托管桌面或应用程序交付图形密集型应用程序。HDX 3D Pro 支持物理主机计算机（包括桌面、刀片式服务器和机架工作站）以及 XenServer、vSphere 和 Hyper-V（仅限直通）虚拟机管理程序提供的 GPU 直通和 GPU 虚拟化技术。

利用 GPU 直通功能，可以创建对专用图形处理硬件具有独占访问权限的 VM。可以在虚拟机管理程序上安装多个 GPU，并将 VM 一对一地分配给每个 GPU。

利用 GPU 虚拟化技术，多个虚拟机可以直接访问单个物理 GPU 的图形处理功能。强大的硬件 GPU 共享功能可提供适用于具有复杂和苛刻设计要求的用户的桌面。针对 NVIDIA GRID 卡的 GPU 虚拟化（请参阅 NVIDIA GRID）采用与非虚拟化操作系统上部署的 NVIDIA 图形驱动程序相同的驱动程序。对于具有 Intel Iris Pro 图形功能的第 5 代和第 6 代 Intel CPU，还支持采用 Intel GVT-g 的 GPU 虚拟化。有关这些 Intel 处理器系列的详细信息，请参阅第 5 代 Intel 酷睿处理器和第 6 代 Intel 酷睿 i5 处理器。AMD FirePro S 系列服务器卡也支持 GPU 虚拟化，请参阅 AMD 专业图形虚拟化解决方案。

HDX 3D Pro 提供以下功能：

- 基于 H.264 的自适应深度压缩，用于实现最佳的 WAN 和无线性能。HDX 3D Pro 使用基于 CPU 的全屏 H.264 压缩作为编码的默认压缩技术。对支持 NVENC 的 NVIDIA 卡使用硬件编码。
- 专用的无损压缩选项。HDX 3D Pro 还提供基于 CPU 的无损编解码器，可支持需要在像素级完美呈现图形的应用程序，例如医学成像。建议仅针对特殊用例使用真正的无损压缩，因为这种压缩方式占用相当多的网络和处理资源。
  使用无损压缩时：

  - 无损指示器（一个系统托盘图标）会通知用户显示的屏幕是有损帧还是无损帧。当“视觉质量”策略设置指定“设为无损”时，此功能很有用。当发送的是无损帧时，无损指示器将变绿。
  - 无损切换功能使用户能够在会话内随时切换到“始终无损”模式。要在会话内随时选择或取消选择“无损”，请在该图标上单击鼠标右键或使用快捷键 Alt+Shift+1。
    对于无损压缩：HDX 3D Pro 使用无损编解码器进行压缩，而不考虑通过策略选择的编解码器。

    对于有损压缩：HDX 3D Pro 使用原始编解码器，即默认编解码器或通过策略选择的编解码器。

    后续会话不会保留无损转换设置。要为每个连接使用无损编解码器，请在“视觉质量”策略设置中选择“始终无损”。

- 可以覆盖用于在会话内选择或取消选择“无损”的默认快捷方式 Alt+Shift+1。在 HKLM\SOFTWARE\Citrix\HDX3D\LLIndicator 配置新注册表设置。
  - 名称：HKLM_HotKey，类型：String
  - 配置快捷键组合的格式为 C=0|1, A=0|1, S=0|1, W=0|1, K=val。注册表项必须使用逗号（,）分隔。按键顺序无关紧要。
  - A、C、S、W 和 K 表示按键，其中 C=Control、A=ALT、S=SHIFT、W=Win 和 K=某个有效按键。K 允许的值包括 0-9、a-z 和所有虚拟键代码。有关虚拟键代码的详细信息，请参阅 MSDN 上的 Virtual-Key Codes（虚拟键代码）。
  - 例如：
    - 对于 F10，设置 K=0x79
    - 对于 Ctrl + F10，设置 C=1、K=0x79
    - 对于 Alt + A、设置 A=1、K=a 或 A=1、K=A 或 K=A、A=1
    - 对于 Ctrl + Alt + 5，设置 C=1、A=1、K=5 或 A=1、K=5、C=1
    - 对于 Ctrl + Shift + F5，设置 A=1、S=1、K=0x74

小心：注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因“注册表编辑器”使用不当导致出现的问

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

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。

- 多显示器和高分辨率显示器支持。对于桌面操作系统计算机，HDX 3D Pro 支持用户设备最多使用 4 个显示器。用户可以采用任意配置安排自己的显示器，并且可以混合使用分辨率和方向各不相同的显示器。显示器的数量受主机计算机 GPU 功能、用户设备以及可用带宽限制。HDX 3D Pro 支持所有显示器分辨率，并仅受主机计算机上 GPU 的功能限制。
  HDX 3D Pro 还对双显示器访问 Windows XP 桌面提供有限支持。有关详细信息，请参阅运行 Windows XP 或 Windows Vista 的计算机上的 VDA。

- 动态分辨率。可以将虚拟桌面或应用程序窗口的分辨率调整为任意大小。 **注意**：唯一受支持的更改分辨率的方法为调整 VDA 会话窗口的大小。不支持从 VDA 会话内部更改分辨率（使用“控制面板”>“外观和个性化”>“显示”>“屏幕分辨率”）。

- 支持 NVIDIA GRID 体系结构。HDX 3D Pro 支持 NVIDIA GRID 卡（请参阅 NVIDIA GRID）以实现 GPU 直通和 GPU 共享。NVIDIA GRID vGPU 允许多个 VM 使用在非虚拟操作系统中部署的相同 NVIDIA 图形驱动程序同时直接访问单个物理 GPU。
- 支持使用虚拟直接图形加速 (vDGA) 的 VMware vSphere 和 VMware ESX — 可针对 RDS 和 VDI 工作负载将 HDX 3D Pro 与 vDGA 结合使用。
- 支持使用 NVIDIA GRID vGPU 和 AMD MxGPU 的 VMware vSphere/ESX。
- 对使用 Windows Server 2016 中离散设备分配的 Microsoft HyperV 的支持。
- 对具有 Intel Xeon Processor E3 系列的数据中心图形的支持。HDX 3D Pro 支持多显示器（最多三个）、控制台消隐、自定义分辨率和受支持的 Intel 处理器系列的高帧速率功能。有关详细信息，请访问 http://www.citrix.com/intel 和 http://www.intel.com/content/www/us/en/servers/data-center-graphics.html。
- AMD FirePro S 系列服务器卡支持 AMD RapidFire。HDX 3D Pro 支持多显示器（最多 6 个）、控制台消隐、自定义分辨率和高帧速率功能。注意：针对 AMD MxGPU 的 HDX 3D Pro 支持（GPU 虚拟化）仅适用于 VMWare vSphere vGPU。
  XenServer 和 Hyper-V 支持 GPU 直通。有关详细信息，请参阅 AMD 虚拟化解决方案。

- 访问 NVIDIA GPU 和 Intel Iris Pro 图形处理器的高性能视频编码器。此功能由策略设置（默认启用）控制，允许使用硬件编码进行 H.264 编码（如果可用）。如果此类硬件不可用，VDA 会转而求助于使用软件视频编解码器的基于 CPU 的编码。有关详细信息，请参阅图形策略设置。

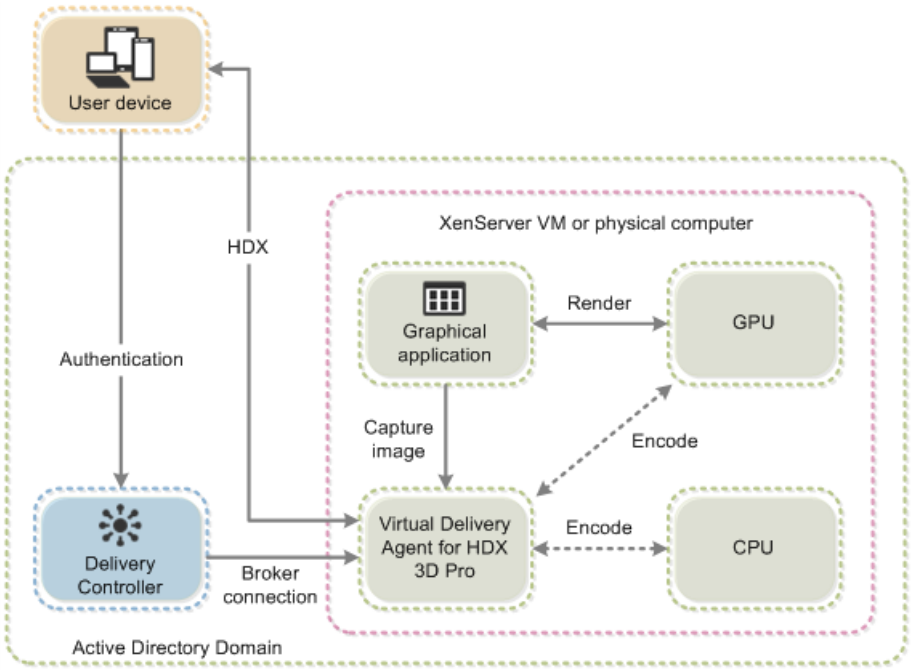
如下图所示：

- 用户登录到 Citrix Receiver 并访问虚拟应用程序或桌面时，控制器将对用户进行身份验证，并与 VDA for HDX 3D Pro 建立连接，以将连接转至托管图形应用程序的计算机。

  VDA for HDX 3D Pro 使用主机上相应的硬件来压缩完整桌面的视图或仅压缩图形应用程序的视图。

- 此桌面或应用程序视图以及用户与这些视图之间的交互将通过 Citrix Receiver 与 VDA for HDX 3D Pro 之间的直接 HDX 连接在主机计算机与用户设备之间传输。

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



使用安装程序的图形界面安装 VDA for Windows Desktop OS 时，在 HDX 3D Pro 页面上选择是。使用命令行接口时，请在 XenDesktop VdaSetup.exe 命令中包含 /enable_hdx_3d_pro 选项。

要升级 HDX 3D Pro，应先卸载单独的 HDX 3D for Professional Graphics 组件和 VDA，然后再以 HDX 3D Pro 模式安装 VDA。同样，要从适用于 Windows 桌面操作系统的标准 VDA 模式切换到 3D Pro 模式，请先卸载标准 VDA，然后再以 HDX 3D Pro 模式安装 VDA。

标准模式	**HDX 3D Pro 模式**
通常最适合于不带图形硬件加速功能的虚拟桌面以及 Remote PC Access。	通常最适合于含图形硬件加速功能的数据中心桌面，需使用多于四个显示器的情况除外。
任何 GPU 均可用于 Remote PC Access，但会有一些应用兼容性限制： • 在 Windows 7、8 和 8.1 上，DirectX 的 GPU 加速功能级别最高为 9.3。如果一些 DirectX 10、11、12 应用程序不支持回退到 DirectX 9，则这些应用程序可能无法运行。 • 在 Windows 10 上，为窗口化的 DirectX 10、11 和 12 应用程序提供了 GPU 加速。DX 9 应用程序由 WARP 呈现。DX 应用程序无法用于全屏模式。 • 远程会话中的 OpenGL 应用程序加速功能（如果受 GPU 供应商支持；目前仅限于 NVIDIA）。	支持通过任何 GPU 实现 GPU 加速功能，但控制台消隐、非标准屏幕分辨率和真正多显示器支持功能要求使用 NVIDIA GRID、Intel Iris Pro GPU 或 AMD RapidFire 图形。 利用显卡供应商提供的驱动程序实现最广泛的应用程序兼容性： • 受 GPU 支持的所有 3D API（DirectX 或 OpenGL）。 • 通过 Intel Iris Pro（仅限 Win10）、NVIDIA GRID 和 AMD RapidFire 支持全屏 3D 应用程序。 • 支持自定义驱动程序扩展和 API。例如，CUDA 或 OpenCL。

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

任意显示器分辨率（由 Windows OS 和性能来决定限制）以及最多 8 个显示器。	最多支持四个显示器。
H.264 硬件编码适用于 Intel Iris Pro 图形处理器。	H.264 硬件编码适用于 Intel Iris Pro 图形处理器和 NVIDIA 卡。

NVIDIA GRID API 提供了对 GPU 帧缓冲区的直接访问，为实现流畅的交互式用户体验提供了尽可能最快的帧速率。如果您在安装启用了 HDX 3D Pro 的 VDA 前安装 NVIDIA 驱动程序，则默认启用 NVIDIA GRID。

要在 VM 上启用 NVIDIA GRID，请从 Device Manager 禁用 Microsoft 基本显示适配器。运行以下命令，然后重新启动 VDA：**NVFBCEnable.exe -enable -noreset**

如果您在安装启用了 HDX 3D Pro 的 VDA 后安装 NVIDIA 驱动程序，NVIDIA GRID 将禁用。使用 NVIDIA 提供的 NVFBCEnable 工具启用 NVIDIA GRID。

要禁用 NVIDIA GRID，请运行以下命令，然后重新启动 VDA：**NVFBCEnable.exe -disable -noreset**

可以在安装 VDA 之前安装 Intel 图形驱动程序。仅当您在安装启用了 HDX 3D Pro 的 VDA 后安装 Intel 驱动程序或者 Intel 驱动程序已更新时，才需要执行以下步骤。

为了启用多显示器支持功能所需的 Intel 驱动程序，请使用 GfxDisplayTool.exe 运行以下命令，然后重新启动 VDA：**GfxDisplayTool.exe -vd enable**

GfxDisplayTool.exe 包含在 VDA 安装程序中。GfxDisplayTool.exe 位于 C:\Program Files\Citrix\ICAServices 中。

> **注意**
>
> 不支持在 ICA 会话中卸载 NVIDIA 或 Intel 驱动程序。

要将 HDX 3D Pro 用于多个显示器，请确保主机计算机已配置的显示器数不少于连接到用户设备的显示器数。连接到主机计算机的显示器可以是物理机，也可以是虚拟机。

在用户连接到提供图形应用程序的虚拟桌面或应用程序时，禁止将显示器（无论是物理机还是虚拟机）连接到主机计算机。否则，会引起用户会话持续时间的不稳定。

请告诉用户，图形应用程序会话运行期间，不支持（由用户或应用程序）对桌面分辨率进行更改。关闭应用程序会话后，用户可以在“Citrix Receiver - Desktop Viewer 首选项”中更改 Desktop Viewer 窗口的分辨率。

多位用户共享一个带宽有限的连接时（例如，在分支机构），Citrix 建议您使用总会话带宽限制策略设置，以限制每位用户可用的带宽。这样可确保用户登录和注销时可用带宽不会大幅波动。由于 HDX 3D Pro 可自动调整以充分利用所有可用带宽，因此，在用户会话过程中可用带宽大幅波动可能会对性能产生负面影响。

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

例如，如果 20 位用户共享一个 60 Mbps 的连接，每位用户可用的带宽可能在 3 Mbps 到 60 Mbps 之间变化，具体取决于并发用户的数量。要优化此种情形下的用户体验，应确定高峰时段每位用户所需的带宽，并将用户限制为始终使用此带宽量。

对于 3D 鼠标用户，Citrix 建议将通用 USB 重定向虚拟通道的优先级提高到 0。有关更改虚拟通道优先级的信息，请参阅 CTX128190。

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

Windows 服务器操作系统 GPU 加速

Dec 05, 2017

通过 HDX 3D Pro，在 Windows 服务器操作系统会话中运行的图形密集型应用程序可以在服务器的图形处理器 (GPU) 上呈现。通过将 OpenGL、DirectX、Direct3D 和 Windows Presentation Foundation (WPF) 呈现移到服务器的 GPU 上，服务器的 CPU 不会因图形呈现而变慢。此外，服务器还能够处理更多图形，因为工作负载在 CPU 和 GPU 之间进行了拆分。

由于 Windows Server 是多用户操作系统，因此由 XenApp 访问的 GPU 可以供多个用户共享，而无需 GPU 虚拟化 (vGPU)。

有关涉及到编辑注册表的过程，请注意：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。

GPU Sharing 使 GPU 硬件可以在远程桌面会话中呈现 OpenGL 和 DirectX 应用程序；它具有以下特点：

- 可用于裸机或虚拟机，以提高应用程序的可扩展性及性能。
- 启用多个并发会话以共享 GPU 资源（大多数用户并不需要专用 GPU 的呈现性能）。
- 无需任何特殊设置。

可以在虚拟机管理程序上安装多个 GPU，并将 VM 一对一地分配给每个 GPU：方法是安装一个配备有多个 GPU 的图形卡，或者安装多个分别配备一个或多个 GPU 的图形卡。建议不要在服务器上混合使用异类图形卡。

虚拟机需要以直接直通方式访问 GPU，这可通过使用 Citrix XenServer、VMware vSphere vDGA 和 Intel GVT-d 实现。当 HDX 3D Pro 与 GPU 直通结合使用时，服务器中的每个 GPU 支持一台多用户虚拟机。

GPU 共享不依赖任何特定的图形卡。

- 在虚拟机管理程序上运行时，请选择与虚拟机管理程序的 GPU 直通实现兼容的硬件平台和图形卡。有关已通过 XenServer GPU 直通证书测试的硬件列表，请访问 GPU 直通设备。
- 在裸机上运行时，建议使用操作系统启用的一个显示适配器。如果在硬件上安装了多个 GPU，请仅保留一个 GPU，并使用 Device Manager 禁用其余的 GPU。

使用 GPU Sharing 的可扩展性取决于多个因素：

- 正在运行的应用程序
- 占用的视频 RAM 量
- 图形卡的处理能力

一些应用程序处理视频 RAM 短缺的能力要优于其他应用程序。如果硬件严重过载，可能会导致图形卡驱动程序不稳定或崩溃。可限制并发用户的数量，以避免此类问题。

可以使用第三方工具（如 GPU-Z）来确定是否已实现 GPU 加速。GPU-Z 可从 http://www.techpowerup.com/gpuz/ 获取。

DirectX、Direct3D 和 WPF 呈现仅在具有支持显示驱动程序接口 (DDI) 9ex、10 或 11 版的 GPU 的服务器上可用。

- 在 Windows Server 2008 R2 上，DirectX 和 Direct3D 不需要特殊设置即可使用单个 GPU。
- 在 Windows Server 2016 和 Windows Server 2012 上，RD 会话主机服务器上的远程桌面服务 (RDS) 会话将 Microsoft 基本呈现驱动程序用作默认适配器。要在 Windows Server 2012 上的 RDS 会话中使用 GPU，请启用组策略“本地计算机策略”>“计算机配置”>“管理模板”>“Windows 组件”>“远程桌面服务”>“远程桌面会话主机”>“远程会话环境”中的对所有远程桌面服务会话使用硬件默认图形适配器。
- 要能够使用服务器的 GPU 呈现 WPF 应用程序，请在运行 Windows 服务器操作系统会话的服务器的注册表中创建以下设

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

置：

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Multiple Monitor Hook] "EnableWPFHook"=dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\ Multiple Monitor Hook] "EnableWPFHook"=dword:00000001

默认禁用在用户会话中运行的 CUDA 或 OpenCL 应用程序的 GPU 加速功能。

要使用 CUDA 加速 POC 功能，请启用以下注册表设置：

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "CUDA"=dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "CUDA"=dword:00000001

要使用 OpenCL 加速 POC 功能，请启用以下注册表设置：

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "OpenCL"=dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "OpenCL"=dword:00000001

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

OpenGL Software Accelerator

Dec 05, 2017

OpenGL Software Accelerator 是一个适用于 OpenGL 应用程序（例如 ArcGIS、Google Earth、Nehe、Maya、Blender、Voxler 以及 CAD/CAM 应用程序）的软件光栅器。借助 OpenGL Software Accelerator，有时不需要使用图形卡即可在 OpenGL 应用程序中提供极佳的用户体验。

> ## Important
>
> 我们*按原样*提供 OpenGL Software Accelerator，必须使用所有应用程序对其进行测试，因为该软件可能不支持某些应用程序。如果 Windows OpenGL 光栅器未提供足够的性能，可以试用该解决方案。如果 OpenGL Software Accelerator 支持您的应用程序，则可以用来避免 GPU 硬件的成本。

OpenGL Software Accelerator 在安装介质的“Support”（支持）文件夹中提供，在所有的有效 VDA 平台上受支持。

何时尝试使用 OpenGL Software Accelerator：

- 在未配备图形处理硬件的服务器上，如果 XenServer 或其他虚拟机管理程序上的虚拟机中运行的 OpenGL 应用程序存在性能问题。对某些应用程序而言，OpenGL Accelerator 优于 Windows 中包含的 Microsoft OpenGL 软件光栅器，因为 OpenGL Accelerator 使用 SSE4.1 和 AVX。OpenGL Accelerator 还支持使用 OpenGL 2.1 及之前版本的应用程序。
- 对于在工作站上运行的应用程序，请首先尝试使用工作站图形适配器所提供的默认 OpenGL 支持功能版本。如果图形卡是最新版本，该软件通常提供最佳性能。如果图形卡是旧版本或者无法提供令人满意的性能，请尝试使用 OpenGL Software Accelerator。
- 对于在使用基于 CPU 的软件光栅器时无法充分发挥功能的 3D OpenGL 应用程序，可能有必要使用 OpenGL GPU 硬件加速功能。此功能可用于裸机或虚拟机。

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

Thinwire

Dec 05, 2017

Thinwire 是 XenApp 和 XenDesktop 中使用的 Citrix 默认显示远程处理技术。

显示远程处理技术允许一台计算机上生成的图形传输（通常跨网络）到另一台计算机上进行显示。

成功的显示远程处理解决方案应该提供与本地 PC 类似的高度互动用户体验。Thinwire 通过使用一系列复杂有效的图像分析和压缩技术实现了这一点。Thinwire 最大程度地实现了服务器可扩展性，且占用的带宽少于其他显示远程处理技术。

由于这种平衡，Thinwire 满足大多数一般业务用例，并用作 XenApp 和 XenDesktop 中的默认显示远程处理技术。

Thinwire 应该用于传送典型的桌面工作负载，例如，桌面、办公效率或基于浏览器的应用程序。还建议将 Thinwire 用于多显示器、高分辨率或高 DPI 场景，以及用于混合了视频内容和非视频内容的工作负载。

Framehawk 应该用于数据包丢失间歇性较高的宽带无线连接中的移动工作人员。

根据其默认配置，Thinwire 可以传送 3D 或高度互动的图形，但是在安装 VDA for Desktop OS 过程中启用 HDX 3D Pro 模式是适用于此类情况的很好选择。3D Pro 模式为 Thinwire 配置全屏 H.264 编码，用于图形传输。这在 3D 专业图形方面提供更加流畅的体验。有关详细信息，请参阅 HDX 3D Pro 和适用于 Windows 桌面操作系统的 GPU 加速。

- Thinwire 已经过优化，适用于最新的操作系统，包括 Windows Server 2012 R2、Windows Server 2016、Windows 7 和 Windows 10。对于 Windows Server 2008 R2，建议使用旧图形模式。使用内置 Citrix 策略模板、“服务器高度可扩展性 – 旧版操作系统”和“针对广域网优化 – 旧版操作系统”为这些用例提供 Citrix 建议的策略设置组合。
- 在 XenApp 和 XenDesktop 7.6 FP3 及更高版本中的 VDA 版本上可以使用驱动 Thinwire 行为的策略设置**使用视频编解码器进行压缩**。在 XenApp 和 XenDesktop 7.9 及更高版本中的 VDA 版本上，**偏好时使用视频编解码器**选项是默认设置。
- 所有 Citrix Receiver 都支持 Thinwire。但有些 Citrix Receiver 可能支持其他 Citrix Receiver 不支持的 Thinwire 功能，例如，为了降低带宽使用量的 8 位或 16 位图形。此类功能支持由 Citrix Receiver 自动协商。
- 在多显示器或高分辨率情况下，Thinwire 将使用较多的服务器资源（CPU、内存）。可以调整 Thinwire 使用的资源量，但可能会导致带宽使用量增加。
- 在低带宽或高延迟情况下，可以考虑启用 8 位或 16 位图形来提高交互性，但视觉质量会受影响，尤其是使用 8 位颜色深度时。

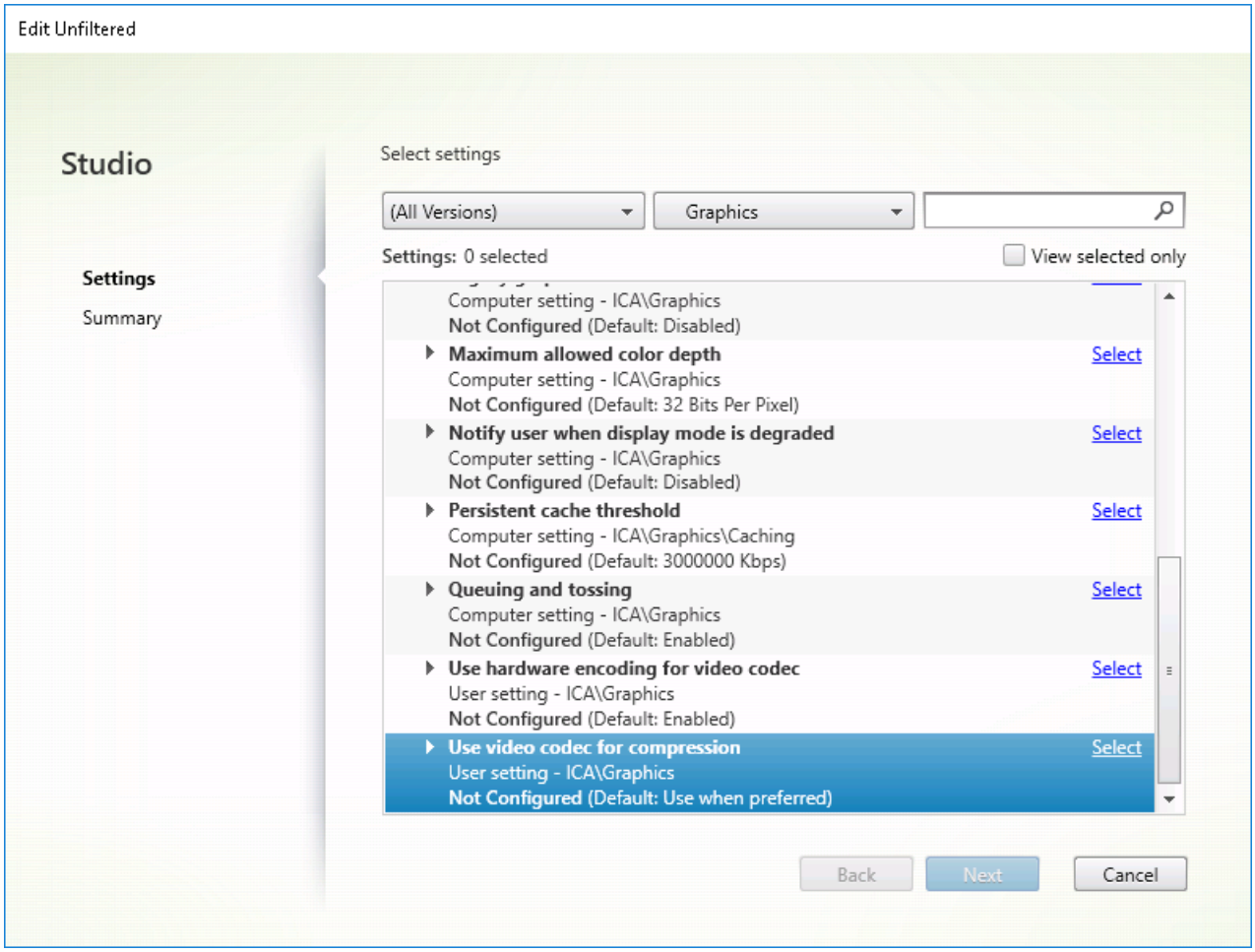
Thinwire 是默认显示远程处理技术。

以下“图形”策略设置会设置默认设置，并提供适用于不同用例的备选设置。

- 使用视频编解码器进行压缩
  - **偏好时使用视频编解码器**。此为默认设置。无需执行其他配置。将此设置保持为默认设置可确保为所有 Citrix 连接选择 Thinwire，且 Thinwire 已针对典型桌面工作负载在可扩展性、带宽和卓越图像质量方面经过优化，
- 此策略设置中的其他选项将继续使用 Thinwire 并与其他技术结合以适用于不同的用例。例如：

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

- **针对主动变化的区域**。Thinwire 中的自适应显示技术识别移动图像（视频、动态 3D），并只在图像移动的屏幕部分使用 H.264。
- **针对整个屏幕**。为 Thinwire 提供全屏 H.264，以针对改进用户体验和带宽使用情况进行优化，尤其是在大量使用 3D 图形的情况下。



很多其他策略设置（包括以下“视频显示”策略设置）可以用于对显示远程处理技术的性能进行完善，并且全部受 Thinwire 支持：

- 简单图形的首选颜色深度
- 目标帧速率
- 视觉质量

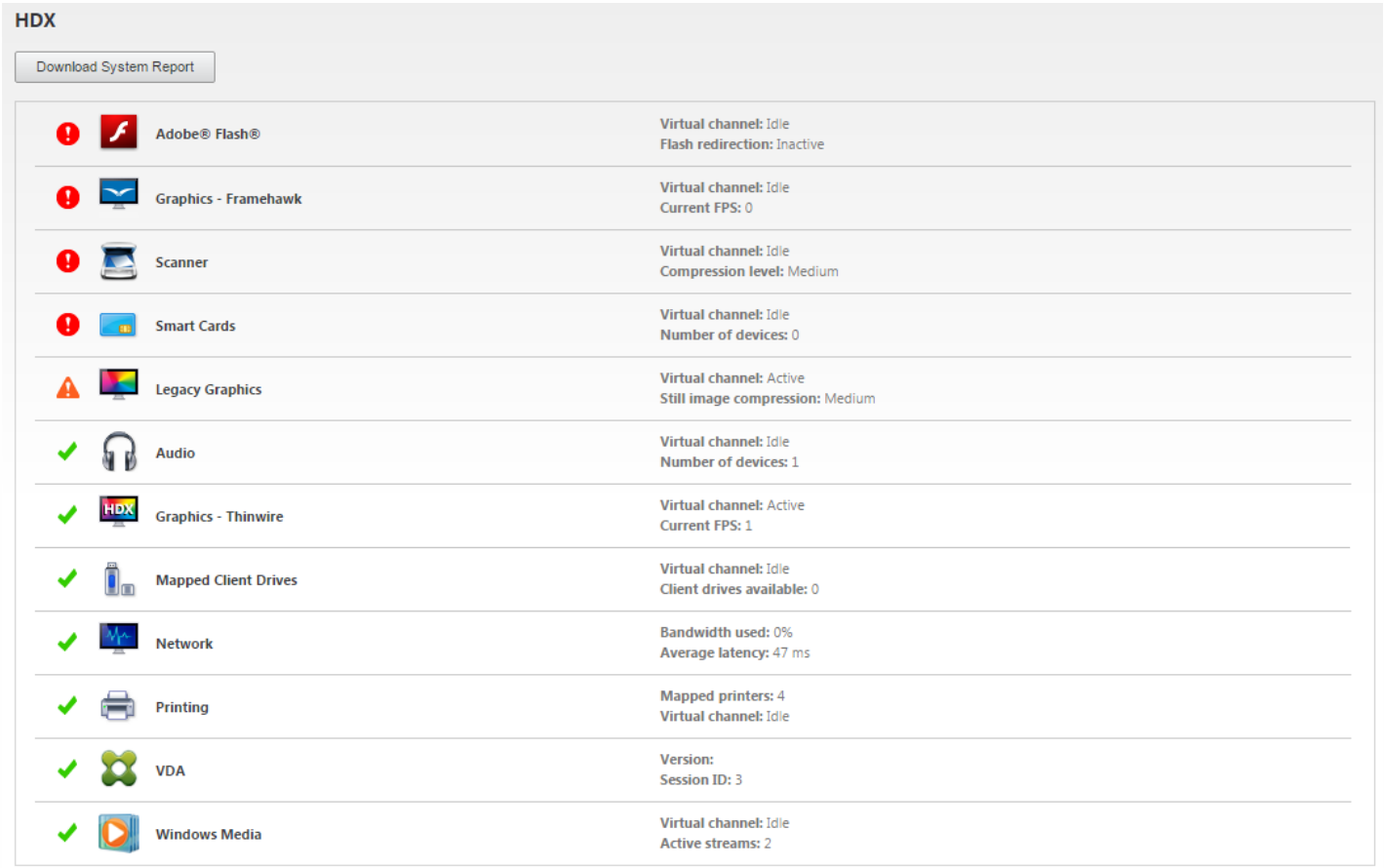
要获得适用于不同业务用例的 Citrix 建议策略设置组合，请使用内置 Citrix 策略模板。**高服务器可扩展性**和**超高清晰度用户体验**模板都结合使用 Thinwire 与符合您的组织的优先级要求和您的用户的期望的最优策略设置组合。

您可以从 Citrix Director 监视 Thinwire 的使用情况和性能。HDX 虚拟通道详细信息视图包含有助于对任何会话中的 Thinwire 进行监视和故障排除的有用信息。要查看 Thinwire 相关的指标，请执行以下操作：

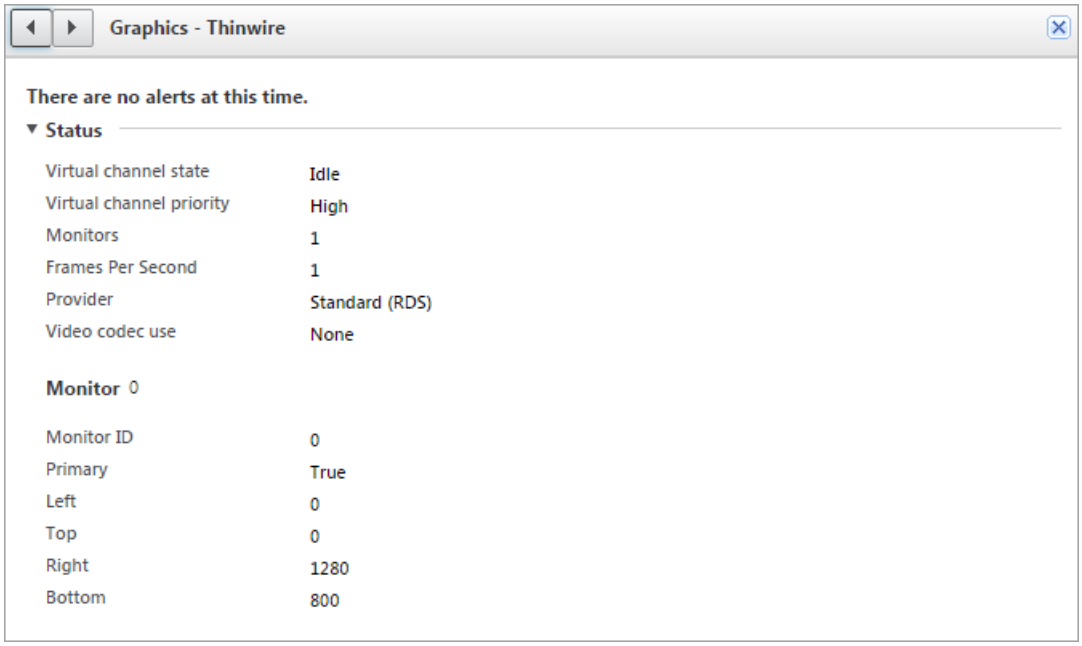
1. 在 Director 中，搜索用户、计算机或端点，打开一个活动会话并单击**详细信息**。也可以选择**过滤器** > **会话** > **所有会话**，打开一个活动会话并单击**详细信息**。

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

2. 向下滚动到 HDX 面板。



3. 选择图形 - Thinwire。



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

多媒体

Dec 05, 2017

HDX 技术堆栈支持通过两种互补的方法来交付多媒体应用程序：

- 服务器端呈现多媒体交付
- 客户端呈现多媒体重定向

此策略可确保您能够在将服务器可扩展性增加至最大以降低每个用户的成本时交付全部多媒体格式，并提供优异的用户体验。

使用服务器呈现的多媒体交付时，音频和视频内容将通过应用程序解码并在 XenApp 或 XenDesktop 服务器上呈现。该内容随后被压缩并通过 ICA 协议交付到用户设备上的 Citrix Receiver。此方法提供的与各种应用程序和媒体格式的兼容率最高。由于视频处理属于计算密集型操作，因此，服务器呈现的多媒体交付将大大受益于板载硬件加速。例如，对 DirectX 视频加速 (DXVA) 的支持将通过在单独的硬件中执行 H.264 解码来卸载 CPU 的负载。Intel Quick Sync 和 NVIDIA NVENC 技术提供硬件加速的 H.264 编码。

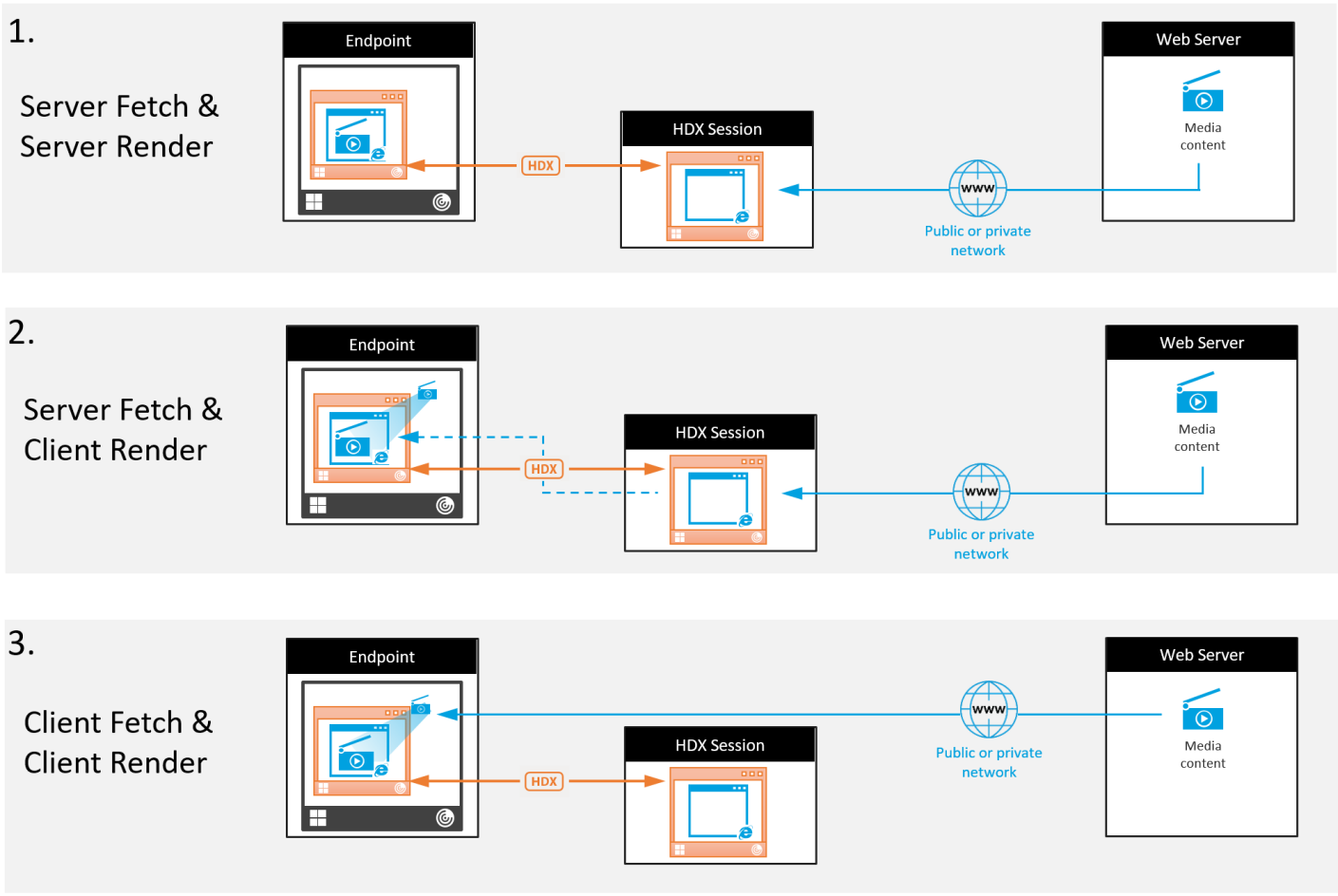
由于大多数服务器不对视频压缩提供硬件加速，因此，如果所有视频处理都在服务器 CPU 上完成，服务器可扩展性将受到负面影响。要保持高服务器可扩展性，可以将多种多媒体格式重定向到用户设备以进行本地呈现。Windows Media 重定向针对许多种通常与 Windows Media Player 关联的媒体格式来卸载服务器的负载。

Flash 重定向将 Adobe Flash 视频内容重定向到用户设备上本地运行的 Flash Player。
HTML5 视频已非常流行，Citrix 针对此类型的内容引入了重定向技术。
此外，您还可以对多媒体内容应用常规访问重定向技术“主机到客户端重定向”和“本地应用程序访问”。

如果未配置重定向，同时使用这些技术时，HDX 将执行服务器端呈现。
如果配置了重定向，HDX 将使用服务器提取和客户端呈现，或者客户端提取和客户端呈现。如果这些方法失败，HDX 将根据需要回退到服务器端呈现，并且遵从“回退防护”策略。

示例方案

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



方案 1. （服务器提取和服务器呈现）

1. 服务器从其来源提取媒体文件，进行解码，然后将内容提供给音频设备或显示设备。
2. 服务器分别从显示设备或音频设备提取提供的图像或声音。
3. 服务器有选择地对其进行压缩，然后将其传输到客户端。

此方法的 CPU 成本和带宽成本都非常高（如果提取的图像/声音未有效压缩），并且服务器可用性非常低。

Thinwire 和音频虚拟通道采用此方法。此方法的优势是降低了客户端的硬件和软件要求。使用此方法时，解码在服务器上进行，并且适用于许多种设备和格式。

方案 2. （服务器提取和客户端呈现）

此方法依赖在解码之前截获媒体内容并将其提供给音频设备或显示设备的能力。压缩后的音频/视频内容改为发送到客户端，之后将在客户端上对其进行本地解码和呈现。此方法的优势是解码和呈现卸载到客户端设备，缩短了服务器上的 CPU 周期。

但是，此方法还额外引入了一些针对客户端的硬件和软件要求。客户端必须能够解码可能会接收到的每种格式。

方案 3. （客户端提取和客户端呈现）

此方法依赖在从其来源提取之前截获媒体内容的 URL 的能力。URL 将被发送到客户端，并且媒体内容将在客户端本地提取、解码和呈现。此方法从概念上讲非常简单。其优势是缩短了服务器上的 CPU 周期并且节省了带宽，因为仅从服务器发送控制命令。但是，媒体内容并非始终可由客户端访问。

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

框架和平台

桌面操作系统（Windows、Mac OS X 和 Linux）提供允许更加简单、快速地部署多媒体应用程序的多媒体框架。下表列出了部分较为常见的多媒体框架。每种框架都将媒体处理划分为多个阶段，并使用基于管道的体系结构。

Framework	Platform
DirectShow	Windows（98 及更高版本）
媒体基础	Windows（Vista 及更高版本）
Gstreamer	Linux
Quicktime	Mac OS X

HDX Flash 重定向	否
Windows Media 重定向	是
HTML5 视频重定向	是
客户端重定向	否

相关信息

- Audio features
- Flash redirection
- HTML5 multimedia redirection
- Windows Media redirection
- General content redirection

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

音频功能

Dec 05, 2017

可以向某个策略配置并添加以下 Citrix 策略设置以优化 HDX 音频功能。有关详细用法以及与其他策略设置的关系和相关性，请参阅音频策略设置、带宽策略设置和多流连接策略设置。

> **Important**
>
> 尽管最好使用用户数据报协议 (UDP) 来代替 TCP 传输音频，但是，使用 DTLS 的 UDP 音频加密仅在 NetScaler Gateway 与 Citrix Receiver 之间可用。因此，有时使用 TCP 传输可能更为可取。TCP 支持从 VDA 到 Citrix Receiver 的端到端 TLS 加密。

通常情况下，音频质量越高，需要向用户设备发送的音频数据就越多，占用的带宽也就越多，服务器 CPU 使用率也就越高。借助声音压缩功能，可以在音频质量与整体会话性能之间取得平衡。可使用 Citrix 策略设置来配置要应用于声音文件的压缩级别。

默认情况下，音频质量策略设置会设置为“高 - 高清晰度音频”（使用 TCP 传输时）和“中 - 语音优化”（使用 UDP 传输（建议）时）。高清晰度音频设置提供高保真立体声音频，但占用的带宽高于其他质量设置。对于未优化的语音聊天或视频聊天应用程序（如软件电话），请不要使用此音频质量，因为此音频质量可能会在音频路径中产生延迟，不适合用于实时通信。对于实时音频，建议使用语音优化策略设置，无论选定的传输协议是什么。

带宽受限时，例如卫星连接或拨号连接，降低音频质量至**低**将占用可行的最低带宽。在这种情况下，请为使用低带宽连接的用户创建单独的策略，以便不会对使用高带宽连接的用户产生不利影响。

有关设置的详细信息，请参阅音频策略设置。请务必在用户设备上启用客户端自动设置；请参阅用户设备的音频设置策略。

要允许用户在用户设备上通过扬声器或其他音频设备（如耳机）从服务器上的应用程序接收音频，请让客户端音频重定向设置保持其默认值（允许）。

客户端音频映射为服务器和网络带来额外的负载；但是，禁止客户端音频重定向将禁用所有 HDX 音频功能。

有关设置的详细信息，请参阅音频策略设置。请务必在用户设备上启用客户端自动设置；请参阅用户设备的音频设置策略。

要允许用户使用用户设备上的麦克风等输入设备录制音频，请让客户端麦克风重定向设置保持其默认值（允许）。

出于安全考虑，当不受用户设备信任的服务器尝试访问麦克风时，系统会向用户发出警报。用户可以在使用麦克风之前选择接受或拒绝访问。用户可以在 Citrix Receiver 上禁用此警报功能。

有关设置的详细信息，请参阅音频策略设置。请务必在用户设备上启用客户端自动设置；请参阅用户设备的音频设置策略。

音频即插即用策略设置可控制是否允许使用多个音频设备来录制和播放声音。默认情况下，此设置处于**已启用**状态。使用音频即插即用功能时，音频设备即使是在建立了用户会话之后才插入，也能够被识别。

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

此设置仅适用于 Windows 服务器操作系统计算机。

有关设置的详细信息，请参阅音频策略设置。

音频重定向带宽限制策略设置指定在会话中播放和录制音频时所用的最大带宽 (Kbps)。音频重定向带宽限制百分比设置指定音频重定向功能所用的最大带宽占总会话带宽的百分比。默认情况下，这两项设置指定为零（无最大值）。如果同时配置了这两个设置，则使用最低带宽限制的那个设置。

有关设置的详细信息，请参阅带宽策略设置。请务必在用户设备上启用客户端自动设置；请参阅用户设备的音频设置策略。

默认情况下，Audio over User Datagram Protocol (UDP) Real-time Transport（通过用户数据报协议(UDP)进行的音频实时传输）设置为允许（如果在安装过程中选择），从而在服务器上打开一个 UDP 端口，以支持使用“Audio over UDP Real-time Transport”（通过 UDP 协议进行的音频实时传输）的连接。Citrix 建议为音频配置 UDP/RTP 协议，以确保在发生网络拥堵或数据包丢失时获得最佳的用户体验。对于软件电话应用程序等实时音频，现在更偏向于使用 UDP 音频来代替 EDT。UDP 允许在不重新传输的情况下存在数据包丢失，从而确保不会对数据包丢失率较高的连接增加任何延迟。

重要：如果未安装 NetScaler Access Gateway，则不加密通过 UDP 传输的音频数据。如果 NetScaler Access Gateway 配置为访问 XenApp 和 XenDesktop 资源，则端点设备与 NetScaler Access Gateway 之间的音频流量将使用 DTLS 协议确保安全。

音频 UDP 端口范围指定 Virtual Delivery Agent (VDA) 用来与用户设备交换音频数据包数据的端口号范围。
默认情况下，此范围为 16500 - 16509。

有关通过 UDP 协议的音频实时传输的设置详细信息，请参阅音频策略设置；有关音频 UDP 端口范围的详细信息，请参阅多流连接策略设置。请务必在用户设备上启用客户端自动设置；请参阅用户设备的音频设置策略。

1. 按照使用组策略对象模板配置 Receiver 进行操作，加载组策略模板。
2. 在组策略编辑器中，依次展开“管理模板”>“Citrix 组件”>“Citrix Receiver”>“用户体验”。
3. 对于**客户端音频设置**，请选择**未配置**、**启用**或**禁用**。
   - **未配置**。默认情况下，通过高质量音频或以前配置的自定义音频设置启用音频重定向。
   - **已启用**。音频重定向通过选定的选项启用。
   - **已禁用**。音频重定向已禁用。
4. 如果选择**已启用**，请选择一种音频质量。对于 UDP 音频，请仅使用**中**（默认设置）。
5. （仅适用于 UDP 音频）选择**启用实时传输**，然后设置用于在本地 Windows 防火墙中打开的传入端口的范围。
6. 要通过 NetScaler Access Gateway 使用 UDP 音频，请选择**允许通过网关实时传输**。应为 NetScaler Access Gateway 配置 DTLS。有关详细信息，请参阅通过 Netscaler Gateway 传输 UDP 音频。

作为管理员，如果您在端点设备上没有控制权限，无法进行更改（例如，BYOD 或使用家用计算机时），请使用 StoreFront 中的 default.ica 属性启用 UDP 音频。

1. 在 StoreFront 计算机上，使用编辑器（例如记事本）打开 C:\inetpub\wwwroot\Citrix\\App_Data\default.ica。
2. 将以下条目移至 [Application] 部分下。



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

```
; This is to enable Real-Time Transport

EnableRtpAudio=true

; This is to Allow Real-Time Transport Through gateway

EnableUDPThroughGateway=true

; This is to set audio quality to Medium

AudioBandwidthLimit=1-

; UDP Port range

RtpAudioLowestPort=16500

RtpAudioHighestPort=16509
```

如果您通过编辑 default.ica 启用用户数据报协议 (UDP) 音频，UDP 音频将对使用该存储的所有用户启用。

用户参与音频或视频会议时可能会听到回声。通常当扬声器和麦克风彼此间距离太近的时候会产生回声。因此，我们建议您在音频和视频会议中使用耳机。

HDX 提供了一个回声消除选项（默认情况下处于启用状态），可以将回声降低到最小。扬声器和麦克风之间的距离直接影响回声消除功能的效果。设备之间的距离不宜过近或过远。

您可以更改注册表设置以禁用回声消除功能。

> **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。

1. 在用户设备上使用注册表编辑器导航到以下位置：
   - 32 位计算机：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation
   - 64 位计算机：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation
2. 将值数据字段更改为 FALSE。

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

软件电话是指用作电话界面的软件。可以使用软件电话通过 Internet 从计算机或其他智能设备进行通话。使用软件电话时，可以拨打电话号码以及使用屏幕执行与电话有关的其他功能。

XenApp 和 XenDesktop 支持使用多种备用方法来提供软件电话。

- **控制模式**。托管的软件电话只需要控制物理电话机。在这种模式下，所有音频流量都不通过 XenApp 或 XenDesktop 服务器。
- **HDX RealTime 优化的软件电话支持**。媒体引擎在用户设备上运行，并且 IP 语音 (VoIP) 流量对等传输。例如，请参阅：
  - HDX RealTime Optimization Pack，优化了 Microsoft Skype for Business 和 Lync 的交付。
  - 适用于 Jabber 的 Cisco Virtualization Experience Media Engine (VXME)。
  - 适用于 one-X Communicator 和 one-X Agent 的 Avaya VDI Communicator。
- **本地应用程序访问**。这是一项 XenApp 和 XenDesktop 功能，允许软件电话等应用程序在用户设备上本地运行。Windows 设备尚未显示与其虚拟/已发布的桌面无缝集成。此功能会将所有音频处理卸载到用户设备。有关详细信息，请参阅本地应用程序访问和 URL 重定向。
- **HDX RealTime 通用软件电话支持。**VoIP-over-ICA。

通用软件电话支持

通用软件电话支持功能允许您在数据中心中的 XenApp 或 XenDesktop 上托管未经修改的软件电话。音频流量通过 Citrix ICA 协议（最好使用 UDP/RTP）传输到运行 Citrix Receiver 的用户设备。

通用软件电话支持是 HDX RealTime 的一项功能。此软件电话交付方法在以下情况下特别有用：

- 优化后的用于交付软件电话的解决方案不可用，并且用户未登录能够使用本地应用程序访问的 Windows 设备。
- 优化后的软件电话交付所需的媒体引擎尚未在用户设备上安装，或者该引擎不适用于用户设备上运行的操作系统版本。在这种情况下，通用 HDX RealTime 可提供重要的回退解决方案。

使用 XenApp 和 XenDesktop 时有两个软件电话交付注意事项：

- 如何将软件电话应用程序交付到虚拟/已发布的桌面。
- 如何将音频传输到最终用户的耳机、麦克风和扬声器或者 USB 电话机，以及如何从这些设备传输音频。

XenApp 和 XenDesktop 包括多种支持通用软件电话交付的技术：

- 针对语音优化的编解码器，实现了实时音频和带宽的快速编码。
- 低延迟音频堆栈。
- 服务器端抖动缓冲区，用于在网络延迟波动时使音频趋于平稳。
- 面向 QoS 的数据包标记（DSCP 和 WMM）。
  - 面向 RTP 数据包的 DSCP 标记（第 3 层）
  - 面向 Wi-Fi 的 WMM 标记

适用于 Windows、Linux、Chrome 和 Mac 的各 Citrix Receiver 版本也具备 VoIP 功能。Citrix Receiver for Windows 提供以下功能：

- 客户端抖动缓冲区 - 即使在网络延迟波动时也能确保音频平稳传输。
- 回声抵消 - 允许声音在未使用耳机的工作人员的麦克风与扬声器之间的距离内大幅波动。
- 音频即插即用 - 在启动会话之前不需要插入音频设备。可以随时插入这些设备。
- 音频设备路由 - 用户可以通过耳机的声音路径将铃声直接传输到扬声器。
- 多流 ICA - 启用通过网络完成的、基于 QoS 的灵活路由。

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

- ICA 支持四股 TCP 数据流和两股 UDP 数据流。其中一股 UDP 数据流支持通过 RTP 传输的实时音频。

有关 Citrix Receiver 功能的汇总，请参阅 Citrix Receiver 功能列表。

系统配置建议

客户端硬件和软件：
要提供最佳音频质量，我们建议您安装最新版本的 Citrix Receiver，并使用具有回声抵消 (AEC) 功能的优质耳机。适用于 Windows、Linux 和 Mac 的各 Citrix Receiver 版本均支持 VoIP。此外，Dell Wyse 提供对 ThinOS (WTOS) 的 VoIP 支持功能。

CPU 注意事项：
请监视 VDA 上的 CPU 使用率以确定是否有必要向每个虚拟机分配两个虚拟 CPU。实时语音和视频属于数据密集型数据。配置两个虚拟 CPU 可以缩短线程切换延迟。因此，我们建议您在 XenDesktop VDI 环境中配置两个 vCPU。

配置两个虚拟 CPU 并不一定意味着将物理 CPU 的数量增加两倍，因为物理 CPU 可以跨会话共享。

Citrix 网关协议 (CGP) 也会增加 CPU 占用量，该协议用于会话可靠性功能。在高质量的网络连接中，您可以在 VDA 中禁用此功能以降低 CPU 占用量。在功能强大的服务器上，可能没有必要执行上述任何步骤。

UDP 音频：
通过 UDP 传输的音频对网络拥挤和数据包丢失情况的容忍力非常强。我们建议您在可用时使用 UDP 来代替 TCP。

LAN/WAN 配置：
正确的网络配置对提供优质的实时音频质量非常重要。通常情况下，必须配置虚拟 LAN (VLAN)，因为过量的广播数据包会引入抖动。启用了 IPv6 的设备可能会生成大量的广播数据包。如果不需要 IPv6 支持，可以在这些设备上禁用 IPv6。请进行配置以支持 QoS。

使用 WAN 连接时的设置：
可以通过局域网 (LAN) 和广域网 (WAN) 连接使用语音聊天。在 WAN 连接中，音频质量取决于连接中的延迟、数据包丢失和抖动。如果在 WAN 连接中向用户提供软件电话，我们建议您在数据中心与远程办公室之间使用 NetScaler SD-WAN，以维持高服务质量。NetScaler SD-WAN 支持多流 ICA，包括 UDP。此外，如果使用单个 TCP 数据流，可以区分各种 ICA 虚拟通道的优先级，以确保高优先级的实时音频数据被优先处理。

使用 Director 或 HDX Monitor 验证您的 HDX 配置。

远程用户连接：
NetScaler Gateway 11 支持 DTLS，以在本机提供 UDP/RTP 流量（TCP 中无封装）。
必须双向打开防火墙，UDP 流量才能通过端口 443 传输。

编解码器选择和带宽占用量：
在数据中心中的用户设备与 Virtual Delivery Agent (VDA) 之间，我们建议您使用针对语音优化的编解码器设置，又称为“中”质量音频。在 VDA 平台与 IP-PBX 之间，软件电话使用编解码器的配置和协商结果。例如：

- G711 提供非常出色的语音质量，但带宽要求为每个通话 80 到 100 千位/秒（基于网络第 2 层开销）。
- G729 提供出色的语音质量，但带宽要求为每个通话 30 到 40 千位/秒（基于网络第 2 层开销）。

向虚拟桌面交付软件电话应用程序

可以通过两种方法向 XenDesktop 虚拟桌面交付软件电话：

- 可以在虚拟桌面映像中安装该应用程序。
- 可以使用 Microsoft App-V 通过流技术将该应用程序推送到虚拟桌面。此方法具有易管理的优势，因为虚拟桌面映像保持得

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

非常整洁。通过流技术推送到虚拟桌面后，该应用程序将在该环境中运行，就像按常规方式安装一样。并非所有应用程序都与 App-V 兼容。

向用户设备传输音频以及从用户设备传输音频

通用 HDX RealTime 支持两种向用户设备传输音频以及从用户设备传输音频的方法：

- **Citrix 音频虚拟通道**。我们通常建议使用 Citrix 音频虚拟通道，因为这种方法是专门针对音频传输而设计的。
- **通用 USB 重定向**。如果用户设备位于连接回 XenApp 或 XenDesktop 服务器的 LAN 或 LAN 等连接中，支持带按钮和/或显示屏的音频设备、人体学接口设备 (HID) 将非常有用。

Citrix 音频虚拟通道

双向 Citrix 音频虚拟通道 (CTXCAM) 允许音频通过网络有效传输。通用 HDX RealTime 从用户的耳机或麦克风获取音频，进行压缩，然后通过 ICA 将其发送到虚拟桌面上的软件电话应用程序。类似地，软件电话的音频输出将被压缩，并在另一个方向发送到用户的耳机或扬声器。此压缩与软件电话本身使用的压缩无关（例如 G.729 或 G.711）。此压缩是使用针对语音优化的编解码器完成的（“中”质量）。其特性对 VoIP 而言非常完美。此编解码器的特性是编码时间非常快，并且最高仅占用大约 56 千位/秒的网络带宽（每个方向 28 Kbps）。必须在 Studio 控制台中明确选择此编解码器，因为这不是默认音频编解码器。默认编解码器为高清音频编解码器（“高”质量）。此编解码器非常适用于高保真立体声声道，但与针对语音优化的编解码器相比，其编码速度较慢。

通用 USB 重定向

Citrix 通用 USB 重定向技术（CTXGUSB 虚拟通道）提供通用的远程连接 USB 设备的方法，包括复合设备（音频加 HID）以及常时等量 USB 设备。此方法仅限于通过 LAN 连接的用户使用，因为 USB 协议通常对网络延迟非常敏感，并且需要占用大量的网络带宽。常时等量 USB 重定向在使用部分软件电话时非常适用。此重定向提供出色的语音质量和低延迟，但 Citrix 音频虚拟通道仍为首选方法，因为后者已针对音频流量优化。主要异常发生在使用带按钮的音频设备时，例如，连接到通过 LAN 连接到数据中心的用户设备的 USB 电话。在这种情况下，通用 USB 重定向通过将信号发送回软件电话来支持电话机或耳机上用于控制功能的按钮。对于在设备上本地使用的按钮而言，这并不是问题。

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

Flash 重定向

Dec 05, 2017

Important

2017 年 7 月 25 日，Adobe 宣布了 Flash 生命周期结束 (EOL)。Adobe 计划在 2020 年底停止更新和分发 Flash Player。

Microsoft 宣布在此 Adobe 日期之前在 Internet Explorer 中逐步停止 Flash 支持。他们将在 2020 年底前从 Windows 中删除 Flash。那时，用户无法再在 Internet Explorer 中启用或运行 Flash。

在 2020 年底前，Citrix 会遵循 Microsoft 策略并继续维护和支持 HDX Flash 重定向。我们尚未决定在哪些版本的 XenApp 和 XenDesktop 中排除 Flash 重定向代码，但我们建议您尽可能切换到 HTML5 视频重定向。HTML5 视频重定向非常适合控制多媒体内容。例如，公司通信视频、培训视频或第三方托管内容时。

有关 HTML5 视频重定向的详细信息，请参阅 HTML5 多媒体重定向。

Flash 重定向功能可将大部分 Adobe Flash 内容（包括动画、视频和应用程序）处理工作卸载到连接至 LAN 和 WAN 的用户 Windows 和 32 位 Linux x86 设备，从而降低服务器和网络的负载。这样将提供更高的可扩展性，同时确保获得高清晰度用户体验。配置 Flash 重定向时，必须同时进行服务器端设置和客户端设置。
小心：使用 Flash 重定向功能时会在用户设备和服务器组件之间进行大量交互。只应在用户设备和服务器之间无需安全分隔的环境中使用此功能。此外，用户设备应配置为只在可信服务器上使用此功能。由于 Flash 重定向功能要求在用户设备上安装 Adobe Flash Player，因此，只有在 Flash Player 自身处于安全状态时启用此功能。

Flash 重定向功能在客户端和服务器上均受支持。如果客户端支持第二代 Flash 重定向功能，Flash 内容将在客户端上呈现。Flash 重定向功能包括支持用户通过 WAN 进行连接、智能回退和 URL 兼容性列表；请参阅下文了解详细信息。

Flash 重定向使用服务器上的 Windows 事件日志记录来记录 Flash 事件。事件日志将指示是否正在使用 Flash 重定向，并提供问题的详细信息。Flash 重定向记录的所有事件都具有以下共性：

- Flash 重定向向应用程序日志报告事件。
- 在 Windows 10、Windows 8 和 Windows 7 系统上，特定于 Flash 重定向功能的日志将显示在“应用程序和服务日志”节点中。
- “源”值为 Flash。
- “类别”值为“无”。

有关 HDX Flash 最新更新的兼容性，请参阅 CTX136588。

要在服务器上配置 Flash 重定向，请使用以下 Citrix 策略设置。有关详细信息，请参阅 Flash 重定向策略设置。

- 默认情况下，Flash 重定向已启用。要为个别 Web 页面和 Flash 实例覆盖此默认行为，请使用 Flash URL 兼容性列表设置。
- Flash 智能回退 - 检测 Flash 小电影的实例（例如，常用于播放广告的 Flash 小电影），并在服务器上呈现这些实例，而不是通过重定向在用户设备上呈现。此优化功能不会在加载 Web 页面或 Flash 应用程序时导致任何中断或故障。默认情况下，启用 Flash 智能回退。要重定向所有 Flash 内容实例，使其呈现在用户设备上，请禁用此策略设置。请注意，有些 Flash 内容可能无法成功重定向。
- Flash 服务器端内容提取 URL 列表允许您指定一些 Web 站点，这些站点的 Flash 内容应该下载到服务器，然后传输到用户设备以进行呈现。（默认情况下，Flash 重定向功能会将 Flash 内容直接下载到具有客户端提取功能的用户设备。）此设置与用户设备上的启用服务器端内容提取设置结合使用（并且前者要求使用后者），主要用于 Intranet 站点和内部 Flash 应用程序。请参阅下文了解详细信息。此设置还可以用于大多数 Internet 站点，可以在用户设备不直接访问 Internet 时（例如，由

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

XenApp 或 XenDesktop 服务器提供连接时）使用。
注意：服务器端内容提取功能不支持使用实时消息传送协议 (RTMP) 的 Flash 应用程序；此时应改为使用服务器端呈现功能，该功能支持 HTTP 和 HTTPS。

- Flash URL 兼容性列表 - 指定在何处呈现来自所列 Web 站点的 Flash 内容：在用户设备上、服务器上还是被阻止。
- Flash 背景色列表 - 可以将 Web 页面与 Flash 实例的颜色相匹配，从而在使用 Flash 重定向时改进 Web 页面的外观。

在用户设备上安装 Citrix Receiver 和 Adobe Flash Player。无需在用户设备上执行任何其他配置。

可以使用 Active Directory 组策略对象更改默认设置。导入并添加 HDX MediaStream Flash 重定向 - 客户端管理模板 (HdxFlashClient.adm)，位于以下文件夹：

- 对于 32 位计算机：%Program Files%\Citrix\ICA Client\Configuration\language
- 对于 64 位计算机：%Program Files (x86)%\Citrix\ICA Client\Configuration\language

策略设置显示在管理模板 > 经典管理模板(ADM) > HDX MediaStream Flash 重定向- 客户端下。请参阅 Microsoft Active Directory 文档了解 GPO 和模板的详细信息。

更改 Flash 重定向功能的使用时间

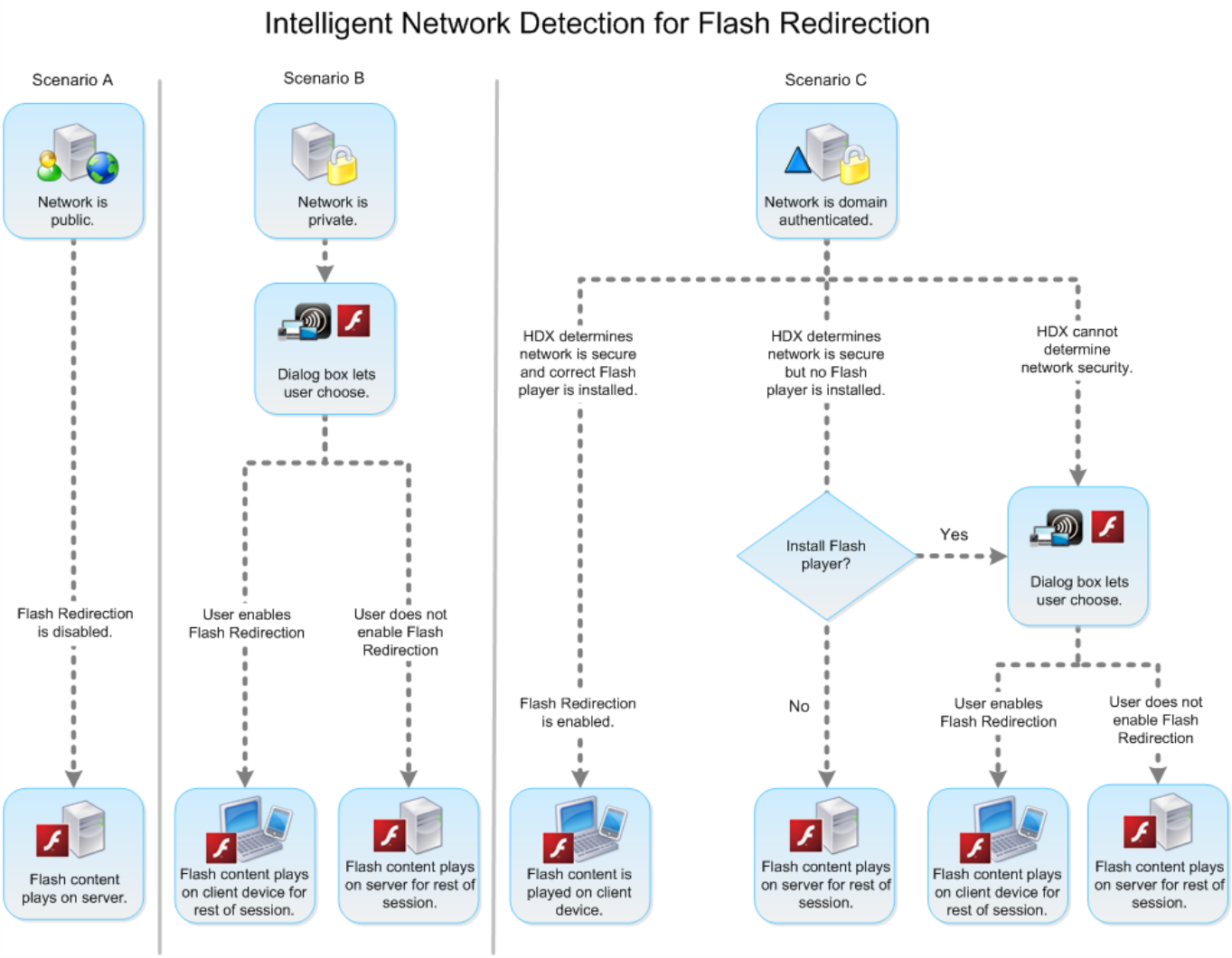
在用户设备上启用 HDX MediaStream Flash 重定向策略设置与服务器端设置结合使用，可控制是否将 Adobe Flash 内容重定向到用户设备，以便在本地呈现。默认情况下，Flash 重定向已启用，并使用智能网络检测功能来确定何时在用户设备上播放 Flash 内容。

如果未设置配置并且使用 Desktop Lock，则默认情况下，将在用户设备上启用 Flash 重定向。

要更改 Flash 重定向功能的使用时间，或在用户设备上禁用 Flash 重定向功能：

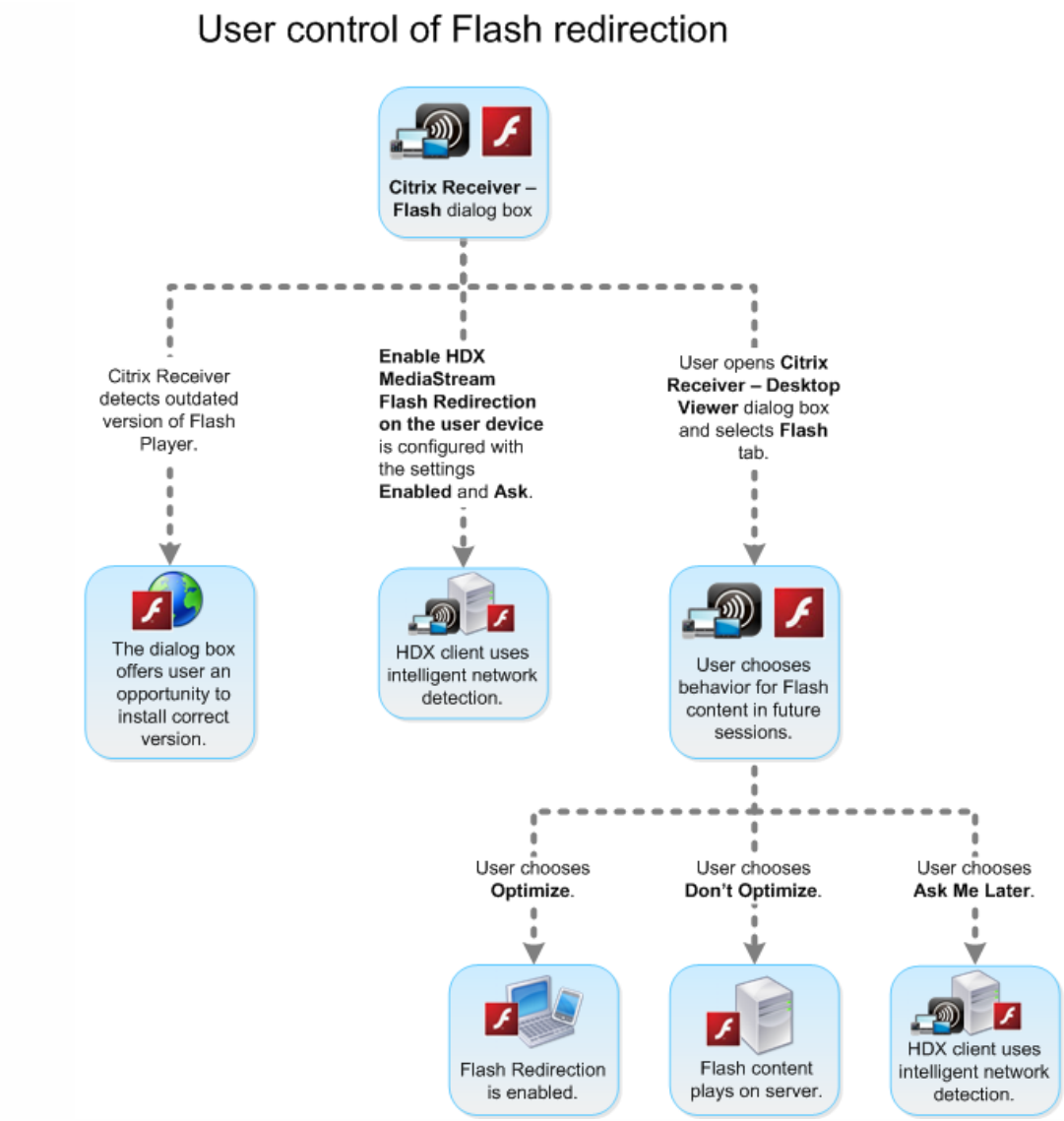
1. 从“设置”列表中，选择在用户设备上启用 HDX MediaStream Flash 重定向，然后单击策略设置。
2. 选择未配置、启用（默认设置）或禁用。
3. 如果选择启用，请从使用 HDX MediaStream Flash 重定向列表中选择一个选项：
   - 要在具有所需配置时使用最新 Flash 重定向功能，并在没有此配置时还原为在服务器端呈现，请选择仅使用第二代选项。
   - 要始终使用 Flash 重定向，请选择始终。将在用户设备上播放 Flash 内容。
   - 要始终不使用 Flash 重定向，请选择从不。将在服务器上播放 Flash 内容。
   - 要使用智能网络检测功能评估客户端网络的安全级别，以确定何时使用 Flash 重定向功能，请选择询问（默认设置）。如果无法确定网络安全性，系统会询问用户是否使用 Flash 重定向。如果无法确定网络安全级别，系统会提示用户选择是否使用 Flash 重定向。
     下图显示了 Flash 重定向针对各种网络类型的处理方式。

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



用户可以从 Citrix Receiver - Desktop Viewer 首选项对话框的 Flash 选项卡中选择优化或不优化，来覆盖智能网络检测。根据用户设备上的 Flash 重定向配置，可选择的选项将有所不同，如下图所示。

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



在客户端与服务器端之间同步 HTTP Cookie

默认情况下，客户端与服务器端之间的 HTTP Cookie 同步已禁用。启用同步功能，以从服务器下载 HTTP Cookie；这些 HTTP Cookie 用于客户端内容提取，并可供包含 Flash 内容的站点在需要时使用。
注意：客户端 Cookie 在同步期间不会被替换；即使之后同步策略被禁用，它们也将保持可用。

1. 从“设置”列表中，选择 Enable synchronization of the client-side HTTP cookies with the server-side（启用客户端与服务器端之间的 HTTP Cookie 同步），然后单击策略设置。
2. 选择未配置、启用或禁用（默认设置）。

启用服务器端内容提取

默认情况下，Flash 重定向功能会将 Adobe Flash 内容直接下载到用于播放此内容的用户设备。启用服务器端内容提取会使 Flash 内容下载到服务器上，然后再发送到用户设备。除非有覆盖策略（例如通过 Flash URL 兼容性列表策略设置阻止某个站点），否则 Flash 内容将在用户设备上播放。

当用户设备通过 NetScaler Gateway 连接到内部站点以及用户设备没有直接访问 Internet 的权限时，会频繁使用服务器端内容提取。

注意：服务器端内容提取功能不支持使用实时消息传送协议 (Real Time Messaging Protocols, RTMP) 的 Flash 应用程序。而应

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

对此类站点使用服务器端呈现功能。
Flash 重定向功能支持用于服务器端内容提取功能的三个启用选项。其中两个选项包含在用户设备上缓存服务器端内容的功能，这样一来，由于重复使用的内容已经存储在用户设备上用于呈现，因而提高了性能。该缓存的内容与用户设备上缓存的其他 HTTP 内容存储在不同的位置。

如果任一启用选项被选中并且客户端 .swf 文件提取操作失败，将自动开始回退到服务器端内容提取。

要启用服务器端内容提取功能，必须同时在客户端设备和服务器上进行设置。
1. 从“设置”列表中，选择启用服务器端内容提取，然后单击策略设置。
2. 选择未配置、启用或禁用（默认设置）。如果启用此设置，请从服务器端内容提取状态列表中选择一个选项：

选项	说明
已禁用	禁用服务器端内容提取，以覆盖服务器上的 Flash 服务器端内容提取 URL 列表设置。服务器端内容提取回退也已禁用。
已启用	为 Flash 服务器端内容提取 URL 列表中所标识的 Web 页面和 Flash 应用程序启用服务器端内容提取。可以使用服务器端内容提取回退功能，但是不会缓存 Flash 内容。
已启用(永久缓存)	为 Flash 服务器端内容提取 URL 列表中所标识的 Web 页面和 Flash 应用程序启用服务器端内容提取。可以使用服务器端内容提取回退。通过服务器端提取而获得的内容缓存在用户设备上，并在会话间存储。
已启用(临时缓存)	为 Flash 服务器端内容提取 URL 列表中所标识的 Web 页面和 Flash 应用程序启用服务器端内容提取。可以使用服务器端内容提取回退。通过服务器端提取而获得的内容缓存在用户设备上，并在会话结束时删除。

3. 在服务器上，启用 Flash 服务器端内容提取 URL 列表策略设置，并在其中填写目标 URL。

将用户设备重定向到其他服务器以实现客户端内容提取

可以使用客户端内容提取 URL 重写规则设置（第二代 Flash 重定向功能）将获取 Flash 内容的尝试重定向。配置此功能时，需要提供两个 URL 模式；如果用户设备尝试从与第一种模式（URL 匹配模式）相匹配的 Web 站点提取内容，会被重定向到由第二种模式（重写的 URL 格式）所指定的 Web 站点。

可以使用此设置作为内容交付网络 (CDN) 的补充。一些交付 Flash 内容的 Web 站点使用 CDN 重定向，使用户能够从包含相同内容的最近一组服务器获得内容。使用 Flash 重定向客户端内容提取功能时，将从用户设备请求 Flash 内容，而 Flash 内容所在的其余 Web 页面则由服务器请求。如果在使用 CDN，服务器请求会重定向到最近的服务器，用户设备请求也会到达同一位置。这可能并不是距离用户设备最近的位置；在加载 Web 页面和播放 Flash 内容之间可能存在明显的延迟，具体取决于距离。
1. 从“设置”列表中，选择客户端内容提取的 URL 重写规则，然后单击策略设置。
2. 选择未配置、已启用或已禁用。未配置是默认设置；选择已禁用将忽略在下一步中配置的任何 URL 重写规则。
3. 如果启用设置，请单击显示。使用 Perl 正则表达式语法在值名称框中键入 URL 匹配模式，并在值框中键入重写的 URL 格式。

> **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。

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

可以添加注册表设置，以指定使用 Citrix Receiver for Windows 或 Citrix Receiver for Linux 访问 VDA 的客户端设备进行 Flash 重定向所需的最低版本。此安全功能确保不会使用过时的 Flash 版本。

ServerFlashPlayerVersionMinimum 是一个字符串值，指定 ICA 服务器 (VDA) 上所需 Flash Player 的最低版本。

ClientFlashPlayerVersionMinimum 是一个字符串值，指定 ICA 客户端 (Citrix Receiver) 上所需 Flash Player 的最低版本。

这些版本字符串可以采用“10”、“10.2”或“10.2.140”格式指定。仅比较主版本号、次要版本号和内部版本号。修订版本号将被忽略。例如，指定“10”的版本字符串表示仅指定主版本号，次要版本号和内部版本号假定为零。

FlashPlayerVersionComparisonMask 是一个 DWORD 值，设置为零将禁止比较 ICA 客户端上的 Flash Player 与 ICA 服务器上的 Flash Player 的版本。比较掩码具有其他值，但由于任何非零掩码的意思可能会改变，因此不应使用。建议仅为所需的客户端将比较掩码设置为零。建议不要在客户端诊断设置下设置比较掩码。如果未指定比较掩码，Flash 重定向将要求 ICA 客户端上的 Flash Player 版本高于或等于 ICA 服务器上的 Flash Player 版本。此功能仅比较 Flash Player 的主要版本号来实现此要求。

要使重定向发生，除了使用比较掩码进行检查，还需要成功完成客户端和服务器最低版本检查。

子项 ClientID0x51 指定 Citrix Receiver for Linux。子项 ClientID0x1 指定 Citrix Receiver for Windows。此子项的命名方式是在字符串“ClientID”后面附加十六进制客户端产品 ID（无任何前导零）。

32 位 VDA 注册表配置示例

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer] 客户端诊断设置

"ClientFlashPlayerVersionMinimum"="13.0" ICA 客户端所需的最低版本 "ServerFlashPlayerVersionMinimum"="13.0" ICA 服务器所需的最低版本 [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x1] Windows ICA 客户端设置

"ClientFlashPlayerVersionMinimum"="16.0.0" 指定 Windows 客户端所需的 Flash Player 的最低版本 [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x51] Linux ICA 客户端设置

"FlashPlayerVersionComparisonMask"=dword:00000000 为 linux 客户端禁用版本比较检查（检查以确定客户端上的 Flash Player 版本高于服务器上的版本）"ClientFlashPlayerVersionMinimum"="11.2.0" 此设置指定 Linux 客户端的 Flash Player 的最低版本。

64 位 VDA 注册表配置示例

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]

"ClientFlashPlayerVersionMinimum"="13.0" "ServerFlashPlayerVersionMinimum"="13.0" [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x1]

"ClientFlashPlayerVersionMinimum"="16.0.0" [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x51]

"FlashPlayerVersionComparisonMask"=dword:00000000 "ClientFlashPlayerVersionMinimum"="11.2.0"

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

HTML5 多媒体重定向

Jan 05, 2018

HTML5 多媒体重定向扩展了 HDX MediaStream 的多媒体重定向功能，将 HTML5 音频和视频包括进来。由于多媒体内容联机分发（尤其是向移动设备）的增长，浏览器行业开发了更有效的音频和视频呈现方式。

Flash 曾是标准，但它需要插件、不能在所有设备上运行，并且在移动设备上运行时电池使用量较高。Youtube 和 NetFlix.com 等公司以及 Mozilla、Google 和 Microsoft 的更高浏览器版本正在转向 HTML5，使其成为新的标准。

与专有插件相比，基于 HTML5 的多媒体具有多个优势，包括：

- 独立于公司的标准 (W3C)
- 简化了数字版权管理 (DRM) 工作流
- 提高了性能，且没有由插件引起的安全问题

HTTP 渐进式下载

HTTP 渐进式下载是支持 HTML5 的基于 HTTP 的伪流技术推送方法。在渐进式下载中，浏览器在从 HTTP Web 服务器下载单个文件（以单一质量编码）的同时播放该文件。视频接收后存储在硬盘驱动器上并从硬盘驱动器播放。如果重新观看视频，浏览器可以从缓存中加载视频。

有关渐进式下载的示例，请参阅 HTML5 视频重定向测试页面。可在您的浏览器中使用开发人员工具检查 Web 页面中的视频元素以及在 HTML5 视频标记中查找来源（mp4 容器格式）。

HTML5 与 Flash 比较

Feature	HTML5	Flash
需要专有播放器	否	是
在移动设备上运行	是	一些
在不同平台上的运行速度	高	慢
受 iOS 支持	是	否
资源使用量	较少	较多
加载速度更快	是	否

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

要求

我们仅对 mp4 格式的渐进式下载支持重定向。我们不支持 WebM 和自适应比特率流推送技术（如 DASH/HLS）。

我们支持：

- 服务器端呈现
- 服务器提取客户端呈现
- 客户端提取

通过使用策略控制这些。有关详细信息，请参阅多媒体策略设置。

最低 Citrix Receiver 版本：

- Citrix Receiver for Windows 4.5
- Citrix Receiver for Linux 13.5

Minimum VDA browser version	Windows OS version/build/SP
Internet Explorer 11.0	Windows 10 x86 (1607 RS1) 和 x64 (1607 RS1) Windows 7 x86 和 x64 Windows Server 2016 RTM 14393 (1607) Windows Server 2012 R2
Firefox 47 手动向 Firefox 证书存储添加证书 或配置 Firefox 从 Windows 信任的证书存储中 搜索证书。有关详细信息，请参阅 https://wiki.mozilla.org/CA:AddRootToFirefox	Windows 10 x86 (1607 RS1) 和 x64 (1607 RS1) Windows 7 x86 和 x64 Windows Server 2016 RTM 14393 (1607) Windows Server 2012 R2
Chrome 51	Windows 10 x86 (1607 RS1) 和 x64 (1607 RS1) Windows 7 x86 和 x64 Windows Server 2016 RTM 14393 (1607) Windows Server 2012 R2

HTML5 视频重定向解决方案的组成部分

- **HdxVideo.js** - 在 Web 站点上截获视频命令的 JavaScript 挂接。HdxVideo.js 使用安全 WebSocket (SSL/TLS) 与

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

WebSocketService 通信。

- **WebSocket SSL 证书**
  - 对于 CA（根）：**Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX In-Product CA)
    位置：证书(本地计算机) > 受信任的根证书颁发机构 > 证书。
  - 对于最终实体（叶）：**Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX Service)
    位置：证书(本地计算机) > 个人 > 证书。
- **WebSocketService.exe** - 在本地系统上运行，并执行 SSL 终止和用户会话映射。TLS 安全 WebSocket 侦听 127.0.0.1 端口 9001。
- **WebSocketAgent.exe** - 在用户会话中运行，并根据 WebSocketService 命令的指示呈现视频。

如何启用 HTML5 视频重定向

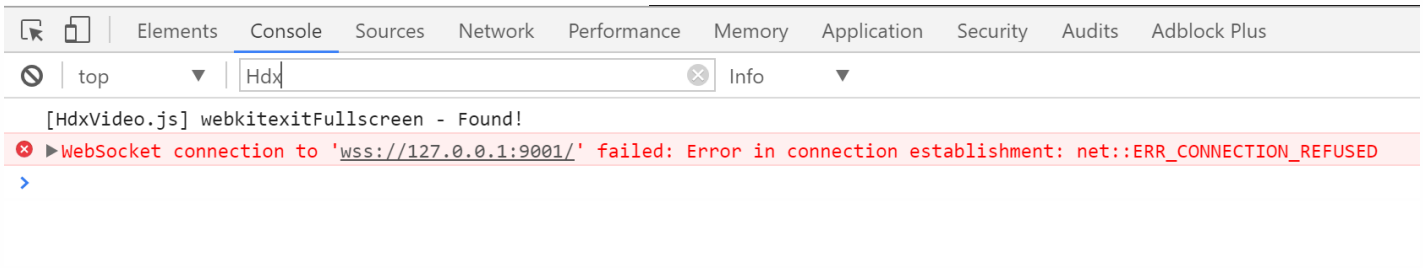
在此版本中，此功能仅用于受控 Web 页面。它要求将 HdxVideo.js JavaScript（包含在 XenDesktop 和 XenApp 安装介质中）添加到提供 HTML5 多媒体内容的 Web 页面。例如，内部培训站点上的视频。

youtube.com 等基于技术（例如 HTTP Live Streaming (HLS) 和 Dynamic Adaptive Streaming over HTTP (DASH)）的 Web 站点不受支持。

有关详细信息，请参阅*多媒体策略设置*。

故障排除提示

Web 页面尝试执行 HdxVideo.js 时可能出现错误。如果 JavaScript 无法加载，则 HTML5 重定向机制将失败。请通过在您的浏览器的开发人员工具窗口检查控制台，确保不存在与 HdxVideo.js 有关的错误。例如：



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

Windows Media 重定向

Dec 05, 2017

Windows Media 重定向控制和优化服务器向用户交付流音频和视频的方式。Windows Media 重定向通过在用户设备而非服务器上播放媒体运行时文件来降低播放多媒体文件时的带宽要求。Windows Media 重定向可提升虚拟 Windows 桌面上运行的 Windows Media Player 以及兼容播放器的性能。

如果不满足 Windows Media 客户端内容提取的要求，媒体交付将自动使用服务器端提取。此方法对用户而言是透明的。您可以使用 XenDesktop Collector 从 HostMMTransport.dll 执行 Citrix Diagnosis Facility (CDF) 跟踪，以确定使用的方法。

Windows Media 重定向在主机服务器上截获媒体管道，捕获本机压缩格式的媒体数据，然后将内容重定向到客户端设备。客户端设备随后重新创建媒体管道以解压和呈现从主机服务器接收的媒体数据。Windows Media 重定向在运行 Windows 操作系统的客户端设备上正常运行。这些设备具有所需的多媒体框架以重新构建媒体渠道，就像它已经存在于主机服务器上一样。Linux 客户端使用相同的开源媒体框架来重新构建媒体管道。

策略设置 **Windows Media 重定向**控制此功能，并且默认设置为**允许**。通常情况下，此设置可将从服务器上呈现的音频和视频的质量提高到一个可与客户端设备上本地播放的音频和视频的质量相提并论的级别。在极少数情况下，使用 Windows Media 重定向播放媒体的效果比使用基本 ICA 压缩和常规音频所呈现的效果差。您可以通过向策略中添加 **Windows Media 重定向**设置并将其值设置为**禁止**来禁用此功能。

有关策略设置的详细信息，请参阅多媒体策略设置。

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

常规内容重定向

Dec 05, 2017

内容重定向功能允许您控制用户是使用服务器上发布的应用程序来访问信息，还是使用用户设备上本地运行的应用程序来访问信息。

客户端文件夹重定向

客户端文件夹重定向改变了在主机端会话中访问客户端文件的方式。当仅在服务器上启用客户端驱动器映射时，客户端满载的卷会作为通用命名约定 (UNC) 链接自动映射到会话中。如果您在服务器上启用客户端文件夹重定向，同时用户也在 Windows 桌面设备上配置了客户端文件夹重定向，将重定向用户指定的部分本地卷。

主机到客户端重定向

请考虑对特定的不常见用例使用主机到客户端重定向。通常，其他形式的内容重定向更好。此类型的重定向仅在服务器操作系统 VDA（而非桌面操作系统 VDA）上受支持。

本地应用程序访问和 URL 重定向

本地应用程序访问可将本地安装的 Windows 应用程序无缝集成到托管的桌面环境中，而无需从一台计算机更改为另一台计算机。

USB 和客户端驱动器注意事项

HDX 技术为没有优化的支持的特殊设备或优化的支持不适用的场合提供**通用 USB 重定向**。

相关信息

> Client folder redirection
> Host to client redirection
> Local App Access and URL redirection
> USB and client drive considerations
> Multimedia

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

客户端文件夹重定向

Dec 05, 2017

客户端文件夹重定向改变了在主机端会话中访问客户端文件的方式。 当仅在服务器上启用客户端驱动器映射时，客户端满载的卷会作为通用命名约定 (UNC) 链接自动映射到会话中。 如果您在服务器上启用客户端文件夹重定向，同时用户也在用户设备上配置客户端文件夹重定向，将重定向用户指定的部分本地卷。

只有用户指定的文件夹会作为 UNC 链接显示在会话内，而不是显示用户设备上的完整文件系统。 如果通过注册表禁用 UNC 链接，客户端文件夹将在会话内显示为映射的驱动器。

只有 Windows 桌面操作系统计算机支持客户端文件夹 重定向。

分离和重新附加设备时，不保存面向外部 USB 驱动器的客户端文件夹重定向。

在服务器上启用客户端文件夹定向。然后，在客户端设备上，指定要重定向的文件夹（用于指定客户端文件夹选项的应用程序包含在此版本随附的 Citrix Receiver 中）。

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

1. 在服务器上：
    1. 创建注册表项 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection。
    2. 创建 REG_DWORD 值。
        - 名称：CFROnlyModeAvailable
        - 类型：REG_DWORD
        - 数据：设置为 1
2. 在用户设备上：
    1. 确保安装了最新版本的 Citrix Receiver。
    2. 从 Citrix Receiver 安装目录启动 CtxCFRUI.exe。
    3. 选择自定义单选按钮，并添加、编辑或删除文件夹。
    4. 断开连接然后重新连接会话，以使设置生效。

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

主机到客户端重定向

Dec 05, 2017

内容重定向功能允许您控制用户是使用在服务器上发布的应用程序来访问信息，还是使用用户设备上本地运行的应用程序来访问信息。

主机到客户端重定向是一种内容重定向。仅在服务器操作系统 VDA（而非桌面操作系统 VDA）上受支持。

- 启用了主机到客户端重定向时，URL 在服务器 VDA 上被截获并发送至用户设备。用户设备上的 Web 浏览器或多媒体播放器打开这些 URL。
- 如果您启用主机到客户端重定向，而用户设备无法连接到 URL，则该 URL 被重定向回服务器 VDA。
- 禁用了主机到客户端重定向时，用户使用服务器 VDA 上的 Web 浏览器或多媒体播放器打开 URL。
- 启用了主机到客户端重定向时，用户无法禁用它。

主机到客户端重定向以前称为**服务器到客户端重定向**。

在特定但不常见的情况下，为了提高性能、兼容性或合规性，可以考虑使用主机到客户端重定向。通常，其他形式的内容重定向更好。

性能

可以使用主机到客户端重定向以提高性能，以便无论何时在用户设备上安装应用程序，它的优先级都高于 VDA 上的应用程序。

请记住，主机到客户端重定向仅在特定情况下才能提高性能，因为 VDA 已优化 Adobe Flash 和其他类型的多媒体内容。首先，请考虑使用其他本文表格中记录的方式（策略设置），而非使用主机到客户端重定向。这些设置更加灵活，通常提供更加优异的用户体验，特别是针对功能较弱的用户设备。

兼容性

在以下用例中，可以使用主机到客户端重定向以获得兼容性：

- 使用 HTML 或多媒体之外的内容类型（例如，自定义 URL 类型）。
- 请使用利用多媒体重定向的 VDA 多媒体播放器不支持的传统媒体格式（例如 Real Media）。
- 只有少数已经在其用户设备上安装了适用于内容类型的应用程序的用户使用该应用程序。
- VDA 无法访问某些 Web 站点（例如，另一个组织内部的 Web 站点）。

合规性

在以下用例中，可以使用主机到客户端重定向以获得合规性：

- 应用程序或内容许可协议不允许通过 VDA 发布。
- 组织策略不允许将文档上载到 VDA。

复杂环境中更有可能存在一些情况，且当用户设备和 VDA 属于不同的组织时。

环境中可能有许多不同类型的用户设备。

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

用户设备	情况或环境	内容重定向方法
平板电脑	-	任何方法（请参阅下一个表）
便携式 PC	-	任何方法（请参阅下一个表）
桌面 PC	用户使用用户设备上安装的大量应用程序	任何方法（请参阅下一个表）
桌面 PC	用户仅使用用户设备上安装的一些已知应用程序	本地应用程序访问
桌面 PC	用户不使用用户设备上安装的应用程序	多媒体重定向和/或 Flash 重定向
桌面设备	供应商支持多媒体重定向和/或 Flash 重定向	多媒体重定向和/或 Flash 重定向
瘦客户端	供应商支持多媒体重定向、Flash 重定向及主机到客户端重定向	任何方法（请参阅下一个表）
零客户端	供应商支持多媒体重定向和/或 Flash 重定向	多媒体重定向和/或 Flash 重定向

以下示例用于帮助指导您选择内容重定向方法。

URL 链接	情况或环境	内容重定向方法
Web 页面或文档	VDA 无法访问 URL	主机到客户端重定向
Web 页面	Web 页面包含 Adobe Flash	Flash 重定向
多媒体文件或流	VDA 有兼容的多媒体播放器	多媒体重定向
多媒体文件或流	VDA 没有兼容的多媒体播放器	主机到客户端重定向
文档	VDA 没有适用于该文档类型的应用程序	主机到客户端重定向
文档	请勿将文档下载到用户设备上	无重定向
文档	请勿将文档上载到 VDA 上	主机到客户端重定向
自定义 URL 类型	VDA 没有适用于该自定义 URL 类型的应用程序	主机到客户端重定向

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

Citrix Receiver for Windows、Citrix Receiver for Mac、Citrix Receiver for Linux、Citrix Receiver for HTML5 及 Citrix Receiver for Chrome 支持主机到客户端重定向。

要使用主机到客户端重定向，用户设备上必须有 Web 浏览器、多媒体播放器或适用于内容的其他应用程序。如果用户设备是桌面设备、瘦客户端或零客户端，请确认它有合适的应用程序且功能足够强大。

启用了本地应用程序访问的用户设备使用不同的内容重定向机制，且不要求使用主机到客户端内容重定向。

可以使用 Citrix 策略以阻止对不合适的设备进行主机到客户端内容重定向。

URL 存在以下情况时使用主机到客户端重定向：

- 作为超链接嵌入应用程序中（例如，电子邮件消息或文档中）。
- 通过 VDA 应用程序菜单或对话框进行选择（如果该应用程序使用 Windows ShellExecuteEx API）。
- 在 Windows 的“运行”对话框中键入。

对于 Web 浏览器中的 URL（在 Web 页面上，或在 Web 浏览器的地址栏中键入），不使用主机到客户端重定向。

> **注意**
>
> 如果用户在 VDA 上更改其默认 Web 浏览器（例如，使用“Set Default Programs”（设置默认程序）），该更改会干扰应用程序的主机到客户端重定向。

启用了主机到客户端内容重定向时，用于打开 URL 的应用程序取决于用户设备上 URL 类型和内容类型的配置。例如：

- 具有 HTML 内容类型的 HTTP URL 在默认 Web 浏览器中打开。
- 具有 PDF 内容类型的 HTTP URL 可能在默认 Web 浏览器中打开，也可能在其他应用程序中打开。

主机到客户端内容重定向不控制此用户设备配置。如果您不控制用户设备的配置，请考虑使用 Flash 重定向和多媒体重定向，而不是主机到客户端内容重定向。

启用了主机到客户端重定向时，以下 URL 类型通过用户设备在本地打开：

- HTTP（超文本传输协议）
- HTTPS（安全超文本传输协议）
- RTSP（Real Player 和 QuickTime）
- RTSPU（Real Player 和 QuickTime）
- PNM（旧版 Real Player）
- MMS（Microsoft 媒体格式）

您可以更改要进行主机到客户端重定向的 URL 类型列表，以删除和添加 URL 类型，包括自定义 URL 类型。

要启用主机到客户端重定向，请先启用 Citrix 策略设置。

主机到客户端重定向策略设置位于文件重定向策略设置部分。默认情况下，禁用此设置。

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

此外，根据 VDA 操作系统，您可能需要为服务器 VDA 设置注册表项和组策略。

- 如果服务器 VDA 是 Windows Server 2008 R2 SP1，则不需要设置注册表项和组策略。
- 如果服务器 VDA 是 Windows Server 2012、Windows Server 2012 R2 或 Windows Server 2016，则必须设置注册表项和组策略。

> **警告**
>
> “注册表编辑器”使用不当会导致出现严重问题，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。

1. 复制下方“**Reg file start**”与“**Reg file end**”之间的文字，将其粘贴到记事本中。
2. 使用“另存为”以及类型“所有文件”和名称 ServerFTA.reg 来保存记事本文件。
3. 使用 Active Directory 组策略将 **ServerFTA.reg** 文件分发到服务器。



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

```
- Reg file start --

Windows Registry Editor Version 5.00



[HKEY_CLASSES_ROOT\ServerFTAHTML\shell\open\command]

@="\"C:\\Program Files (x86)\\Citrix\\system32\\iexplore.exe\" %1"



[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA]

@="ServerFTA"



[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities]

"ApplicationDescription"="Server FTA URL."

"ApplicationIcon"="C:\\Program Files (x86)\\Citrix\\system32\\iexplore.exe,0"

"ApplicationName"="ServerFTA"



[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities\URLAssociations]

"http"="ServerFTAHTML"

"https"="ServerFTAHTML"



[HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications]

"Citrix.ServerFTA"="SOFTWARE\\Citrix\\ServerFTA\\Capabilities"

-- Reg file end --
```

创建 XML 文件。例如，复制“xml file start”与“xml file end”之间的文字，将其粘贴到 XML 文件中，然后将该文件另存为 ServerFTAdefaultPolicy.xml。



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

```
-- xml file start --
<?xml version="1.0" encoding="UTF-8"?>
<DefaultAssociations>
<Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="ServerFTA" />
<Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName="ServerFTA" />
</DefaultAssociations>
-- xml file end --
```

从当前组策略管理控制台中，导航到 **Computer configuration**（计算机配置）> **Administrative Templates**（管理模板）> **Windows Components**（窗口组件）> **File Explorer**（文件资源管理器）> **Set a default associations configuration file**（设置默认关联配置文件），并提供您创建的 ServerFTAdefaultPolicy.xml 文件。

要更改要进行主机到客户端重定向的 URL 类型列表，请在服务器 VDA 上设置以下注册表项。

注册表项：HKLM\Software\Wow6432Node\Citrix\SFTA

要从列表中删除 URL 类型，请设置 DisableServerFTA 和 NoRedirectClasses：

名称：DisableServerFTA
类型：REG_DWORD
数据：1

名称：NoRedirectClasses
类型：REG_MULTI_SZ
数据：指定这些值的任意组合：http、https、rtsp、rtspu、pnm 或 mms。在单独的行中输入多个值。例如：

http

https

rtsp

要将 URL 类型添加到列表，请设置 ExtraURLProtocols：

名称：ExtraURLProtocols
类型：REG_MULTI_SZ
数据：指定 URL 类型的任意组合。每个 URL 类型必须包括 :// 前缀，多个值之间用分号分隔。例如：

customtype1://;customtype2://

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

要为一组特定的 Web 站点启用主机到客户端重定向，请在服务器 VDA 上设置以下注册表项。

注册表项：HKLM\Software\Wow6432Node\Citrix\SFTA

名称：ValidSites
类型：REG_MULTI_SZ
数据：指定完全限定的域名 (FQDN) 的任意组合。在单独的行中键入多个 FQDN。FQDN 只能在最左侧位置包含通配符。 这匹配一层域，与 RFC 6125 中的规则一致。例如：

www.example.com

*.example.com

要将 Internet Explorer 9 及更高版本用作已发布的浏览器，请在服务器 VDA 上更改以下注册表项值：

注册表项：

HKLM\Software\Classes\htmlfile\shell\opennew

HKLM\Software\Classes\http\shell\open

HKLM\Software\Classes\https\shell\open

HKCR\http\shell\open

HKCR\https\shell\open

HKCR\htmlfile\shell\opennew

从：

名称：CommandID

类型：REG_SZ

数据：IE.Protocol

更改为：

名称：CommandID

类型：REG_SZ

数据：IE.ProtocolX

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

本地应用程序访问和 URL 重定向

Dec 05, 2017

在本文中：

- 简介
- 要求、注意事项和限制
- 与 Windows 交互
- 配置本地应用程序访问和 URL 重定向

简介

本地应用程序访问可将本地安装的 Windows 应用程序无缝集成到托管的桌面环境中，而无需从一台计算机更改为另一台计算机。利用本地应用程序访问，您可以：

- 直接从虚拟桌面访问在物理便携式计算机、PC 或其他设备上本地安装的应用程序。
- 提供灵活的应用程序交付解决方案。如果用户具有您无法虚拟化或 IT 不予维护的本地应用程序，这些应用程序的行为就像安装在虚拟桌面上时一样。
- 通过将已发布应用程序的快捷方式放置在用户的 Windows 设备，当应用程序独立于虚拟桌面托管时可避免双跳延迟。
- 使用如下应用程序：
  - 视频会议软件，例如 GoToMeeting。
  - 尚未虚拟化的特殊或利基应用程序。
  - 采用其他方式时会将大量数据从用户设备传输到服务器再返回用户设备的应用程序和外围设备，例如 DVD 刻录机或 TV 调谐器。

在 XenApp 和 XenDesktop 中，托管桌面会话使用 URL 重定向启动本地应用程序访问应用程序。借助 URL 重定向，可通过多个 URL 地址获得应用程序。通过选择桌面会话中浏览器内部的嵌入式链接，可以启动本地浏览器（根据浏览器的 URL 黑名单）。如果导航至未列入黑名单的 URL，则此 URL 会再次在桌面会话中打开。

URL 重定向仅适用于桌面会话，不适用于应用程序会话。唯一可用于应用程序会话的重定向功能是主机到客户端的内容重定向，它是服务器 FTA（文件类型关联）重定向的一种类型。此 FTA 可将某些协议（如 http、https、rtsp 或 mms）重定向到客户端。例如，如果仅使用 http 打开嵌入式链接，这些链接将直接在客户端应用程序中打开。不支持 URL 黑名单或白名单。

启用本地应用程序访问时，对于作为本地运行应用程序、用户托管应用程序中的链接或作为桌面上的快捷方式显示给用户的 URL，将通过以下方式之一进行重定向：

- 从用户的计算机重定向到托管的桌面
- 从 XenApp 或 XenDesktop 服务器重定向到用户计算机
- 在启动（而非重定向）它们的环境中呈现

要指定特定 Web 站点中内容的重定向路径，请在 Virtual Delivery Agent 上配置 URL 白名单和 URL 黑名单。这些名单包含多字符串注册表项，用于指定 URL 重定向策略设置；有关详细信息，请参阅“本地应用程序访问策略设置”。

URL 可在 VDA 上呈现，但存在以下例外情况：

- 地理/区域设置信息 — 需要区域设置信息的 Web 站点，如 msn.com 或 news.google.com（根据地理信息打开特定于某个国家/地区的页面）。例如，如果从位于英国的数据中心置备 VDA，而客户端从印度进行连接，则用户将看到 in.msn.com，而不是 uk.msn.com。
- 多媒体内容 — 在客户端设备上呈现包含富媒体内容的 Web 站点时，最终用户将获得本地体验，甚至还可以节省高延迟网络中的带宽。虽然存在 Flash 重定向功能，作为一种补充，带有其他媒体类型（例如，Silverlight）的站点也可以实现重定向。

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

这是一个非常安全的环境。也就是说，管理员批准的 URL 在客户端上运行，而其余 URL 将重定向到 VDA。

除 URL 重定向外，还可以使用 FTA 重定向。FTA 在会话中遇到文件时会启动本地应用程序。如果启动本地应用程序，则该应用程序必须具有此文件的访问权限才能将其打开。因此，只能使用本地应用程序打开位于网络共享或客户端驱动器（使用客户端驱动器映射）上的文件。例如，当打开 PDF 文件时，如果 PDF 阅读器是本地应用程序，则文件使用 PDF 阅读器打开。由于本地应用程序可以直接访问文件，因此，无需通过 ICA 网络传输文件，即可打开此文件。

要求、注意事项和限制

本地应用程序访问在面向 VDA for Windows Server OS 和 VDA for Windows Desktop OS 的有效操作系统中受支持，需要 Citrix Receiver for Windows 4.1（最低版本）。支持以下浏览器：

- Internet Explorer 11。您可以使用 Internet Explorer 8、9 或 10，但 Microsoft 支持版本 11，而 Citrix 也建议使用版本 11。
- Firefox 3.5 至 21.0
- Chrome 10

使用本地应用程序访问和 URL 重定向时请阅读以下注意事项和限制。

- 本地应用程序访问专用于覆盖所有显示器的全屏虚拟桌面，如下所示：
  - 如果本地应用程序访问与在窗口模式下运行或未覆盖所有显示器的虚拟桌面结合使用，用户体验可能会非常混乱。
  - 对于多个显示器，如果最大化其中一个显示器，则该显示器将成为在该会话中启动的所有应用程序的默认桌面，即使随后的应用程序通常在其他显示器中启动也是如此。
  - 此功能支持一个 VDA；不存在与多个并发 VDA 的集成。
- 有些应用程序可能会出现异常行为，对用户产生以下影响：
  - 用户可能对驱动器盘符感到困惑，例如是本地 C:，而不是虚拟桌面 C: 驱动器。
  - 在虚拟桌面中可用的打印机对本地应用程序不可用。
  - 需要提升权限的应用程序不能作为客户端托管应用程序启动。
  - 不会对单实例应用程序（例如 Windows Media Player）进行特殊处理。
  - 本地应用程序随本地计算机的 Windows 主题出现。
  - 不支持全屏应用程序。包括可打开至全屏的应用程序，例如 PowerPoint 幻灯片演示或覆盖整个桌面的照片查看器。
  - 本地应用程序访问复制 VDA 上本地应用程序的属性，例如客户端桌面上的快捷方式和“开始”菜单；但是，不会复制其他属性，例如快捷键和只读属性。
  - 自定义如何处理重叠窗口顺序的应用程序可能会存在不可预测的结果。例如，有些窗口可能会隐藏。
  - 不支持快捷方式，包括我的电脑、回收站、控制面板、网络驱动器快捷方式以及文件夹快捷方式。
  - 不支持以下文件类型和文件：自定义文件类型、没有关联程序的文件、zip 文件和隐藏文件。
  - 不支持对混合的 32 位和 64 位客户端托管应用程序或 VDA 应用程序进行任务栏分组，例如将 64 位 VDA 应用程序和 32 位本地应用程序组合在一起。
  - 不能使用 COM 启动应用程序。例如，如果从 Office 应用程序中单击嵌入式 Office 文档，则检测不到进程启动，且本地应用程序集成失败。
- 用户从一个虚拟桌面会话内部启动另一个虚拟桌面的双跳场景不受支持。
- URL 重定向仅支持显式 URL（即，出现在浏览器的地址栏中或使用浏览器内的导航找到的 URL，具体取决于浏览器）。
- URL 重定向仅适用于桌面会话，不适用于应用程序会话。
- VDA 会话中的本地桌面文件夹不允许用户创建新文件。
- 对于本地运行的应用程序的多个实例而言，其行为方式取决于为虚拟桌面建立的任务栏设置。但是，本地运行应用程序的快捷方式不与这些应用程序的运行实例一起分组，也不与托管应用程序的运行实例或托管应用程序的固定快捷方式一起分组。用户只能从任务栏关闭本地运行的应用程序的窗口。尽管用户可以将本地应用程序窗口固定在桌面任务栏和“开始”菜单中，但使用这些快捷方式时，不一定总是可以启动这些应用程序。

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

与 Windows 交互

本地应用程序访问与 Windows 的交互包括以下行为：

- Windows 8 和 Windows Server 2012 快捷方式行为
  - 客户端上安装的 Windows 应用商店应用程序并不随本地应用程序访问快捷方式进行枚举。
  - 默认情况下，通常使用 Windows 应用商店应用程序打开图像和视频文件。但是，本地应用程序访问会枚举 Windows 应用商店应用程序，并使用桌面应用程序打开快捷方式。
- 本地程序
  - 对于 Windows 7，可从开始菜单中访问此文件夹。
  - 对于 Windows 8，仅当用户从“开始”屏幕中选择**所有应用程序**类别时，本地程序才可用。并非所有子文件夹均显示在本地程序中。
- 针对应用程序的 Windows 8 图形功能
  - 桌面应用程序限制在桌面区域内，并被“开始”屏幕和 Windows 8 风格应用程序所覆盖。
  - 在多显示器模式下，本地应用程序访问应用程序与桌面应用程序的行为有所不同。在多显示器模式下，“开始”屏幕和桌面显示在不同的显示器中。
- Windows 8 和本地应用程序访问 URL 重定向
  - 由于 Windows 8 Internet Explorer 未启用任何加载项，因此使用桌面 Internet Explorer 启用 URL 重定向。
  - 在 Windows Server 2012 中，Internet Explorer 默认情况下禁用加载项。要实现 URL 重定向，禁用 Internet Explorer 增强的配置。重置 Internet Explorer 选项并重新启动，以确保为标准用户启用加载项。

配置本地应用程序访问和 URL 重定向

要将本地应用程序访问和 URL 重定向用于 Citrix Receiver，请执行以下操作：

- 在本地客户端计算机上安装 Citrix Receiver。可以在 Citrix Receiver 安装期间启用这两项功能，或者使用组策略编辑器启用本地应用程序访问模板。
- 将**允许本地应用程序访问**策略设置为**启用**。也可以为 URL 重定向配置 URL 白名单和黑名单策略。有关详细信息，请参阅“本地应用程序访问策略设置”。

为所有本地应用程序启用本地应用程序访问和 URL 重定向：

1. 将**允许本地应用程序访问**策略设置为**启用**。启用此设置时，VDA 让客户端决定在会话中是否启用管理员发布的应用程序快捷方式和本地应用程序访问快捷方式。（禁用此设置时，管理员发布的应用程序快捷方式和本地应用程序访问快捷方式不适用于 VDA。）此策略设置适用于整台计算机，URL 重定向策略也是如此。
2. 在安装 Citrix Receiver 期间为计算机上的所有用户启用本地应用程序访问和 URL 重定向。此操作还会注册 URL 重定向所需的浏览器加载项。在命令提示窗口中，使用以下选项运行相应的命令以安装 Receiver：

   CitrixReceiver.exe /ALLOW_CLIENTHOSTEDAPPSURL=1

   CitrixReceiverWeb.exe /ALLOW_CLIENTHOSTEDAPPSURL=1

1. 运行 gpedit.msc。

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

2. 选择**计算机配置**。在**管理模板**上单击鼠标右键，然后依次选择**添加/删除模板 > 添加**。
3. 添加位于 Citrix Receiver Configuration 文件夹中的 icaclient.adm 模板（通常位于 c:\Program Files (x86)\Citrix\Online Plugin\Configuration）。（将 icaclient.adm 模板添加到计算机配置中以后，在用户配置中也可以使用此模板。）
4. 依次展开**管理模板 > 经典管理模板(ADM) > Citrix 组件 > Citrix Receiver > 用户体验**。
5. 选择**本地应用程序访问设置**。
6. 选择**启用**，然后选择**允许 URL 重定向**。对于 URL 重定向，按照如下所述使用命令行注册浏览器加载项。

仅提供对已发布应用程序的访问：

1. 在安装 Delivery Controller 的服务器上，运行 **regedit.exe**。
   1. 导航到 HKLM\Software\Wow6432Node\Citrix\DesktopStudio。
   2. 添加 REG_DWORD 条目 ClientHostedAppsEnabled，值为 1。（值为 0 表示禁用本地应用程序访问。）
2. 依次重新启动 Delivery Controller 服务器和 Studio。
3. 发布本地应用程序访问应用程序。
   1. 在 Studio 导航窗格中选择**交付组**，然后选择“应用程序”选项卡。
   2. 在“操作”窗格中选择**创建本地访问应用程序**。
   3. 选择桌面交付组。
   4. 在用户的本地计算机上输入应用程序的完整可执行路径。
   5. 指出虚拟桌面上的本地应用程序快捷方式是否显示在“开始”菜单、桌面或二者上。
   6. 接受“名称”页面上的默认值，然后检查设置。
4. 在安装 Citrix Receiver 期间为计算机上的所有用户启用本地应用程序访问和 URL 重定向。此操作还会注册 URL 重定向所需的浏览器加载项。在命令提示窗口中，使用以下选项运行命令以安装 Citrix Receiver：
   CitrixReceiver.exe /ALLOW_CLIENTHOSTEDAPPSURL=1
   CitrixReceiverWeb.exe /ALLOW_CLIENTHOSTEDAPPSURL=1
5. 将**允许本地应用程序访问**策略设置为**启用**。启用此设置时，VDA 让客户端决定在会话中是否启用管理员发布的应用程序快捷方式和本地应用程序访问快捷方式。（禁用此设置时，管理员发布的应用程序快捷方式和本地应用程序访问快捷方式不适用于 VDA。）

注意：使用 /ALLOW_CLIENTHOSTEDAPPSURL=1 选项从命令行安装 Citrix Receiver 时，会自动注册 URL 重定向所需的浏览器加载项。

可以使用以下命令注册和取消注册一个或所有加载项：

- 在客户端设备上注册加载项：<*客户端安装文件夹*>\redirector.exe /reg<*浏览器*>
- 在客户端设备上取消注册加载项：<*客户端安装文件夹*>\redirector.exe /unreg<*浏览器*>
- 在 VDA 上注册加载项：<*VDA 安装文件夹*>\VDARedirector.exe /reg<*浏览器*>
- 在 VDA 上取消注册加载项：<*VDA 安装文件夹*>\VDARedirector.exe /unreg<*浏览器*>

其中，<*浏览器*> 可以是 IE、FF、Chrome 或 All。

例如，以下命令在运行 Citrix Receiver 的设备上注册 Internet Explorer 加载项。

```
C:\Program Files\Citrix\ICA Client\redirector.exe/regIE
```

以下命令在 Windows Server OS VDA 上注册所有加载项。

```
C:\Program Files (x86)\Citrix\System32\VDARedirector.exe /regAll
```


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

- 默认情况下，Internet Explorer 重定向所输入的 URL。如果 URL 未列入黑名单中，但是通过浏览器或 Web 站点重定向到其他 URL，则即使最终 URL 在黑名单中，也不会重定向此 URL。

  为使 URL 重定向正常运行，请在浏览器提示时启用加载项。如果禁用使用 Internet 选项的加载项或提示中的加载项，URL 重定向将无法正常运行。

- Firefox 加载项始终重定向 URL。

  安装加载项时，Firefox 在新的选项卡页面上提示是否允许/阻止安装加载项。必须允许加载项，才能正常使用此功能。

- Chrome 加载项始终重定向导航到的最终 URL，而非输入的 URL。

  已在外部安装扩展。如果禁用扩展，URL 重定向功能在 Chrome 中将无法正常使用。如果在隐身模式中需要 URL 重定向，请在浏览器设置中允许扩展在该模式下运行。

1. 在托管桌面上，运行 **regedit.msc**。
2. 导航到 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Client Hosted Apps\Policies\Session State。对于 64 位系统，导航到 HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies\Session State。
3. 添加 REG_DWORD 条目 Terminate，并采用以下其中一个值：
   - 1 - 当用户从虚拟桌面注销或断开连接时，本地应用程序继续运行。一旦重新建立连接，如果本地应用程序在虚拟桌面中可用，将重新集成。
   - 3 - 当用户从虚拟桌面注销或断开连接时，本地应用程序关闭。

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

USB 和客户端设备注意事项

Dec 05, 2017

HDX 技术为大多数流行的 USB 设备提供了**优化的支持**。其中包括：

- 显示器
- 鼠标
- 键盘
- VoIP 电话
- 耳机
- 网络摄像机
- 扫描仪
- 摄像头
- 打印机
- 驱动器
- 智能卡读卡器
- 手写板
- 签名板

优化的支持可提供改进的用户体验和通过 WAN 实现的更高性能和带宽效率。通常情况下，优化的支持即是最佳选择，尤其对于存在高延迟的环境或对安全性极为敏感的环境更是如此。

HDX 技术为没有优化的支持的特殊设备或优化的支持不适用的场合提供**通用 USB 重定向**，例如：

- USB 设备具有其他不属于优化的支持的高级功能，诸如具有附加按钮的鼠标或网络摄像头。
- 用户需要不属于优化的支持的功能，例如刻录 CD。
- USB 设备属于专业化设备，诸如测试和测量设备或工业控制器。
- 某个应用程序需要直接访问该设备作为一个 USB 设备。
- 该 USB 设备仅具有一个可用的 Windows 驱动程序。例如，某个智能卡读卡器可能不具有适用于 Citrix Receiver for Android 的驱动程序。
- Citrix Receiver 的版本没有为这种类型的 USB 设备提供优化的支持。

利用通用 USB 重定向：

- 用户不需要在其设备上安装设备驱动程序。
- USB 客户端驱动程序安装在 VDA 计算机上。

注意

- 通用 USB 重定向可以与优化的支持一起使用。如果启用了通用 USB 重定向，请同时针对通用 USB 重定向和优化的支持配置 Citrix USB 设备策略设置，以避免出现不一致的意外行为。
- Citrix 策略设置客户端 USB 设备优化规则是针对通用 USB 重定向的特定设置，适用于某种特定的 USB 设备。而不是此处描述的优化的支持。
- 客户端 USB 即插即用设备重定向是一种相关的功能，可为诸如摄像头和媒体播放器等使用图片传输协议 (PTP) 或媒体传输协议 (MTP) 的设备提供优化的支持。客户端 USB 即插即用重定向不属于通用 USB 重定向。客户端 USB 即插即用重定向仅在服务器操作系统上可用。

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

通过通用 USB 重定向，对于某些类型的 USB 设备而言，网络延迟和带宽可能会影响用户体验和 USB 设备操作。例如，对时间极为敏感的设备可能无法在高延迟低带宽的链路上正常工作。可能的情况下可转而使用优化的支持。

某些 USB 设备需要高带宽才能使用，例如，3D 鼠标（与通常也需要使用高带宽的 3D 应用程序一起使用）。通过使用 Citrix 策略，可避免出现性能问题。有关详细信息，请参阅客户端 USB 设备重定向的带宽策略设置和多流连接策略设置。

某些 USB 设备本质上属于安全敏感型设备，例如智能卡读卡器、指纹读取器和电子签名板。诸如 USB 存储设备等其他 USB 设备可能会用于传输敏感的数据。

USB 设备经常用于散布恶意软件。Citrix Receiver、XenApp 和 XenDesktop 的配置可减少这些 USB 设备所带来的风险，但不会彻底消除风险。无论是否使用通用 USB 重定向或优化的支持，这种情况均适用。

> ## Important
>
> 对于安全敏感型设备和数据，请始终使用 TLS 或 IPSec 来保护 HDX 连接。
>
> 仅对您需要的 USB 设备启用支持。同时配置通用 USB 重定向和优化的支持来满足这种需求。
>
> 为用户提供安全使用 USB 设备的指导：仅使用从可信来源获得的 USB 设备；不要把 USB 设备留在无人照看的开放式环境中 — 例如网吧中的闪存；对在多台计算机上使用一个 USB 设备的风险进行解读。

通用 USB 重定向支持 USB 2.0 及更早的设备。通用 USB 重定向还支持连接到 USB 2.0 或 USB 3.0 端口的 USB 3.0 设备。通用 USB 重定向不支持 USB 3.0 中引入的 USB 功能，诸如超高速。

以下 Citrix Receiver 支持通用 USB 重定向：

- Citrix Receiver for Windows，请参阅配置您的 XenDesktop 环境
- Citrix Receiver for Mac，请参阅配置 Citrix Receiver for Mac
- Citrix Receiver for Linux，请参阅优化
- Citrix Receiver for Chrome OS，请参阅关于 Citrix Receiver for Chrome 2.1

对于 Citrix Receiver 的版本，请参阅 Citrix Receiver 功能表。

如果您使用的是较早的 Citrix Receiver 版本，请参阅 Citrix Receiver 文档以确认是否支持通用 USB 重定向。请参阅 Citrix Receiver 文档以了解有关受支持的 USB 设备类型的任何限制。

从 VDA for Desktop OS 7.6 版至当前版本运行的桌面会话支持通用 USB 重定向。

从 VDA for Server OS 7.6 版至当前版本运行的桌面会话支持通用 USB 重定向，但具有以下限制：

- VDA 必须运行 Windows Server 2012 R2 或 Windows Server 2016。
- 仅支持单跳场景。桌面托管应用程序会话不支持双跳通用 USB 重定向。
- USB 设备驱动程序必须完全兼容适用于 Windows 2012 R2 的远程桌面会话主机 (RDSH)，包括完整的虚拟化支持。

某些类型的 USB 设备不受通用 USB 重定向的支持，因为重定向这些设备不会有任何益处：

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

- USB 调制解调器。
- USB 网络适配器。
- USB 集线器。连接到 USB 集线器的 USB 设备被单独处理。
- USB 虚拟 COM 端口。使用 COM 端口重定向而非通用 USB 重定向。

有关已完成通用 USB 重定向测试的 USB 设备的信息，请参阅 CTX123569。某些 USB 设备在使用通用 USB 重定向时无法正确操作。

您可以控制哪些类型的 USB 设备可以使用通用 USB 重定向。这需要单独进行配置：

- 在 VDA 上，使用 Citrix 策略设置。有关详细信息，请参阅策略设置参考中的客户端驱动器和用户设备的重定向和 USB 设备策略设置
- 在 Citrix Receiver 中，使用依赖于 Citrix Receiver 的机制。例如，Citrix Receiver for Windows 配置有可通过管理模板控制的注册表设置。默认情况下，会允许某些类型的 USB 设备使用 USB 重定向功能，但拒绝其他类型的 USB 设备使用；请参阅 Citrix Receiver for Windows 文档中的配置您的 XenDesktop 环境了解详细信息。

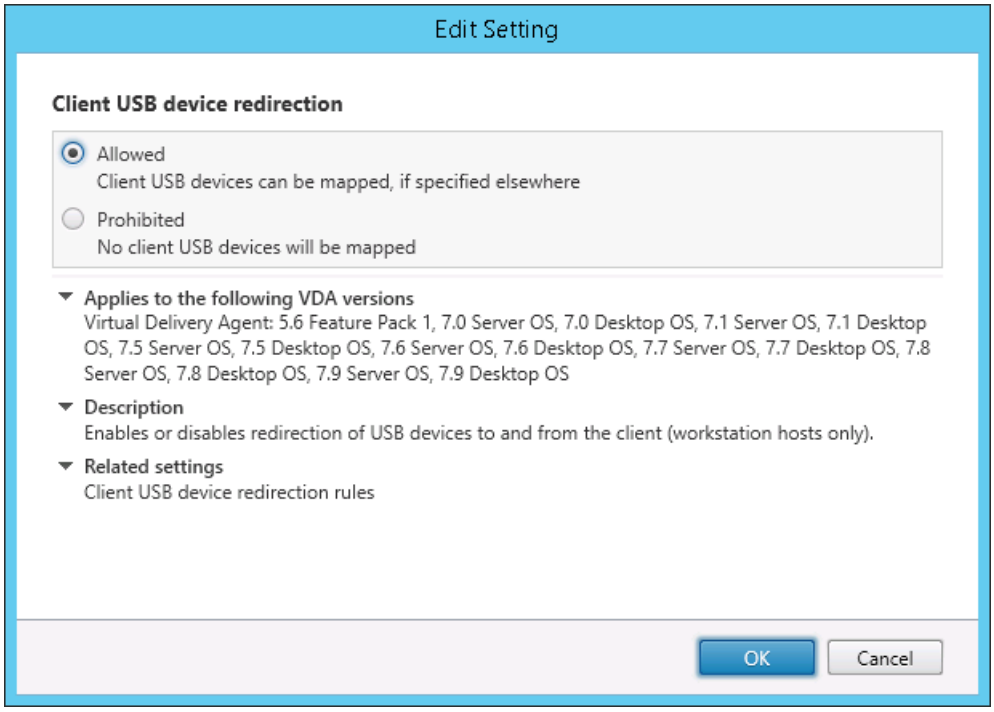
这种单独配置提供了灵活性。例如：

- 如果两个不同的组织或部门负责 Citrix Receiver 和 VDA，他们可以单独执行控制。当一个组织中的用户访问另一个组织中的应用程序时，可能适用于这种情况。
- 如果仅允许特定用户或某些只通过 LAN（而不是通过 NetScaler 网关）进行连接的用户使用 USB 设备，则可以通过 Citrix 策略设置来控制这种情况。

要启用通用 USB 重定向，请配置 Citrix 策略设置和 Citrix Receiver。

在 Citrix 策略设置中：

1. 向策略中添加客户端 USB 设备重定向，并将其值设置为**允许**。

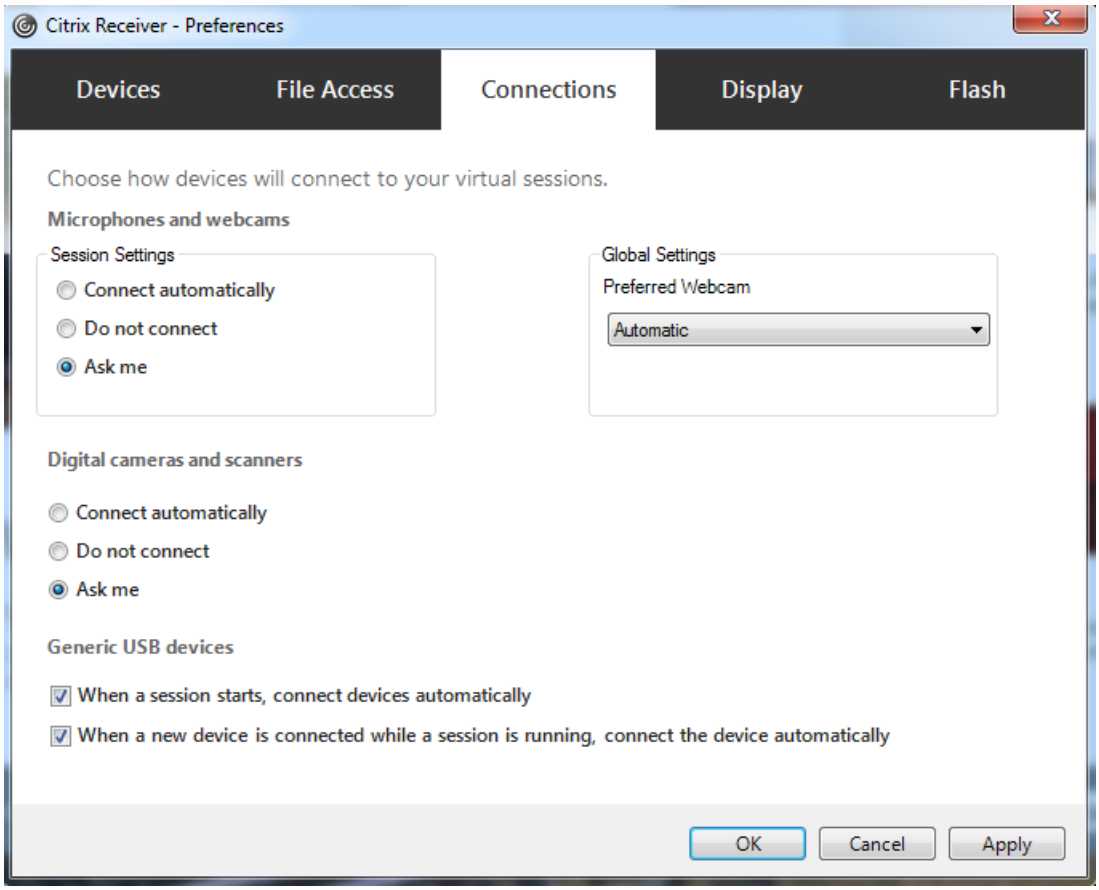


© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. （可选）要更新可进行重定向的 USB 设备的列表，请向策略中添加客户端 USB 设备重定向规则设置并指定 USB 策略规则。

在 Citrix Receiver 中：

3. 在用户设备上安装 Citrix Receiver 时启用 USB 支持。您可以使用管理模板执行此操作，或通过 Citrix Receiver for Windows > 首选项 > 连接。



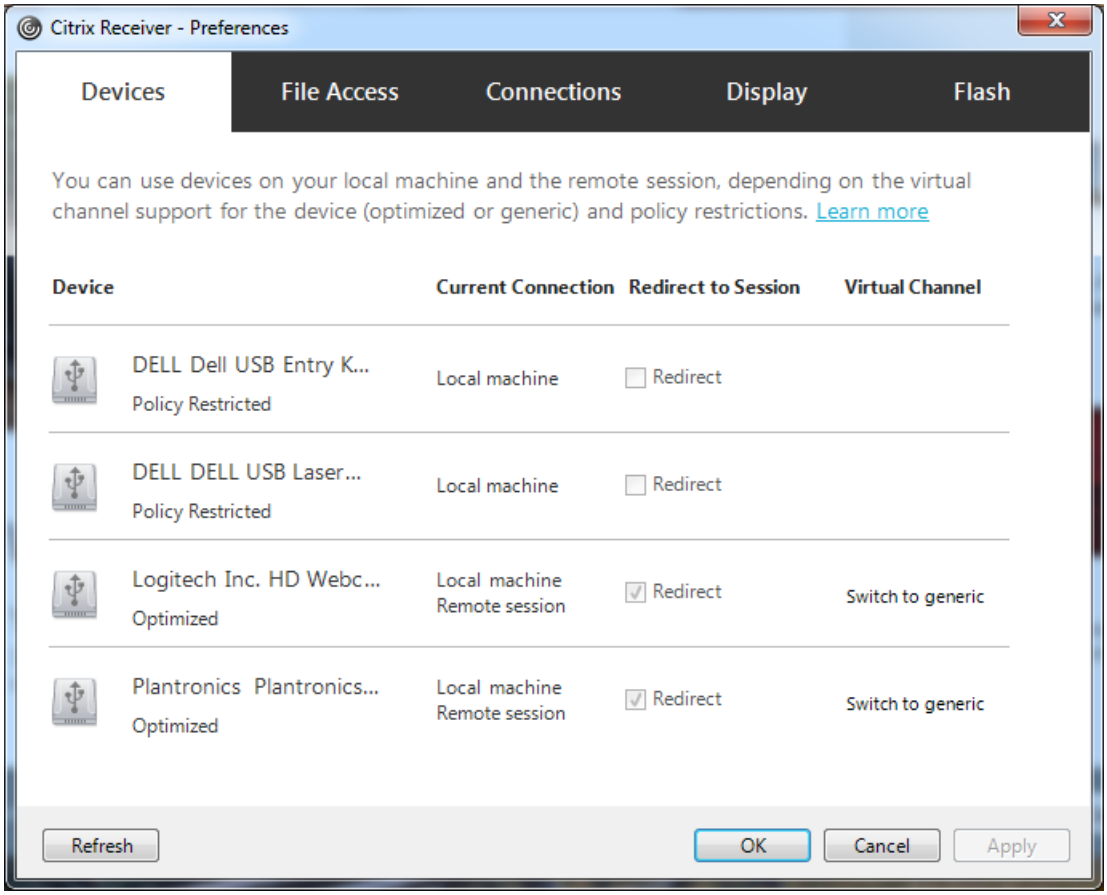
如果已在上一步中为 VDA 指定 USB 策略规则，请为 Citrix Receiver 指定相同的策略规则。

对于瘦客户端，请向制造商咨询有关 USB 支持以及任何所需配置的详细信息。

当已启用 USB 支持并将 USB 用户首选项设置配置为自动连接 USB 设备时，将自动重定向 USB 设备。当在桌面设备模式下运行并且不存在连接栏时，也会自动重定向 USB 设备。

用户可以明确地对未自动重定向的设备执行重定向操作，方法是从 USB 设备列表中选择这些设备。用户可以通过参阅 Citrix Receiver for Windows 用户帮助文章在 Desktop Viewer 中显示设备获取有关如何执行此操作的更多帮助。

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



要使用通用 USB 重定向而非优化的支持，您可以：

- 在 Citrix Receiver 中，手动选择 USB 设备以使用通用 USB 重定向，从首选项对话框的设备选项卡中选择**切换到通用**。
- 通过配置 USB 设备类型的自动重定向（例如，AutoRedirectStorage=1）并将 USB 用户首选项设置设为自动连接 USB 设备，可以自动选择 USB 设备以使用通用 USB 重定向。有关详细信息，请参阅 CTX123015。

注意：仅在某个网络摄像头被发现与 HDX 多媒体重定向不兼容时，才能配置通用 USB 重定向以与该网络摄像头一同使用。

要阻止列出或重定向 USB 设备，可以指定 Citrix Receiver 和 VDA 的设备规则。

对于通用 USB 重定向，至少需要了解 USB 设备类别和子类别。并非所有的 USB 设备都会使用其明显的 USB 设备类别和子类别。例如：

- 笔类设备使用鼠标设备类别。
- 智能卡读卡器可能使用供应商定义的或 HID 设备类别。

要想实现更为精确的控制，也需要了解供应商 ID、产品 ID 和版本 ID。您可以从设备供应商处获取这些信息。

Important

恶意的 USB 设备可能会呈现出某些不符合其预期用途的 USB 设备特征。设备规则并非为了防止这种行为。

可以通过同时为 VDA 和 Citrix Receiver 指定 USB 设备重定向规则以覆盖默认 USB 策略规则，来控制可进行通用 USB 重定向的

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

USB 设备。

对于 VDA：

- 通过组策略规则为服务器操作系统计算机编辑管理员覆盖规则。组策略管理控制台包含在安装介质上：
  - 对于 x64：dvd root \os\lang\x64\Citrix Policy\ CitrixGroupPolicyManagement_x64.msi
  - 对于 x86：dvd root \os\lang\x86\Citrix Policy\ CitrixGroupPolicyManagement_x86.msi

在 Citrix Receiver for Windows 上：

- 编辑用户设备注册表。安装介质中包含一个管理模板（ADM 文件），以便您可以通过 Active Directory 组策略更改用户设备：
  dvd root \os\lang\Support\Configuration\icaclient_usb.adm

> **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。

产品的默认规则存储在 HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules 中。请勿编辑这些产品默认规则，而应根据这些规则创建管理员覆盖规则，如下文中所述。GPO 覆盖规则将在产品默认规则之前进行评估。

管理员覆盖规则存储在 HKLM\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRules 中。GPO 策略规则的格式为 **{Allow:|Deny:}** ，后接一组以空格分隔的 *tag=value* 表达式。

支持以下标记：

标记	说明
VID	设备描述符中的供应商 ID
PID	设备描述符中的产品 ID
REL	设备描述符中的版本 ID
类	设备描述符或接口描述符中的类；请参阅 USB Web 站点 http://www.usb.org/ 了解可用的 USB 类代码
子类	设备描述符或接口描述符中的子类
端口	设备描述符或接口描述符中的协议

创建新策略规则时，应注意以下事项：

- 规则不区分大小写。

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

- 规则末尾可以带有以 # 开头的可选注释。无需分隔符，且将忽略注释以使规则匹配。
- 空白注释行和纯注释行会被忽略。
- 空格用作分隔符，但不能出现在数字或标识符中间。例如，Deny: Class = 08 SubClass=05 是有效规则，Deny: Class=0 Sub Class=05 则无效。
- 标识必须使用匹配运算符 =。例如，VID=1230。
- 每条规则都必须另起新行，或包含在以分号分隔的列表中。

> **注意**
>
> 如果使用 ADM 模板文件，则必须在一行中创建规则（以分号分隔的列表）。

示例：

- 以下示例显示了一个用于供应商和产品标识符的 USB 策略规则，由管理员定义：
  Allow: VID=046D PID=C626 # 允许 Logitech SpaceNavigator 3D 鼠标
  Deny: VID=046D # 拒绝所有 Logitech 产品
- 以下示例显示了一个用于已定义类、子类和协议的 USB 策略规则，由管理员定义：
  Deny: Class=EF SubClass=01 Prot=01 # 拒绝 MS 可用同步设备
  Allow: Class=EF SubClass=01 # 允许同步设备
  Allow: Class=EF # 允许所有 USB 其他设备

用户可以在启动虚拟会话之前或之后连接 USB 设备。

使用 Citrix Receiver for Windows 时，以下情况适用：
- 在会话启动后连接的设备将立即显示在 Desktop Viewer 的 USB 菜单中。
- 如果 USB 设备不能正确重定向，可等到虚拟会话启动后再连接设备，这样可以解决此问题。
- 为避免数据丢失，请使用 Windows 的“安全删除硬件”图标来删除 USB 设备。

为 USB 大容量存储设备提供了优化支持。这是 XenApp 和 XenDesktop 客户端驱动器映射的一部分。用户登录时，用户设备上的驱动器将自动映射至虚拟桌面上的驱动器盘符。这些驱动器显示为具有映射驱动器盘符的共享文件夹。要配置客户端驱动器映射，请使用 ICA 策略设置的文件重定向策略设置部分中的**客户端可移动驱动器**设置。

借助 USB 大容量存储设备，可以使用客户端驱动器映射和/或通用 USB 重定向，均由 Citrix 策略进行控制。主要的区别为：

功能	客户端驱动器映射	通用 USB 重定向
默认情况下启用	是	否
可配置只读访问权限	是	否
加密的设备访问	是，如果在访问设备前解锁加密	否

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

可在会话期间安全删除设备	否	是，只要用户按照操作系统建议进行安全删除

如果同时启用了通用 USB 重定向和客户端驱动器映射策略，并且在会话启动之前或之后插入了大容量存储设备，则将使用客户端驱动器映射对其进行重定向。如果同时启用了通用 USB 重定向和客户端驱动器映射策略，设备配置为自动重定向（请参阅 http://support.citrix.com/article/CTX123015），并且在会话启动之前或之后插入了大容量存储设备，则将使用通用 USB 重定向对其进行重定向。

> **注意**
>
> 低带宽连接（如 50 Kbps）条件下支持 USB 重定向，但是复制大型文件不起作用。

您可以控制用户是否能够将文件从虚拟环境复制到用户设备。默认情况下，可在读取/写入模式下从会话内部使用映射的客户端驱动器上的文件和文件夹。

要防止用户添加或修改映射的客户端设备上的文件和文件夹，请启用**只读客户端驱动器访问**策略设置。将此设置添加到策略中时，请确保**客户端驱动器重定向**设置为**允许**并且也已添加到策略。

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

打印

Dec 05, 2017

在您的环境下管理打印机的过程分为多个阶段：

1. 熟悉打印概念（如果您还不熟悉）。
2. 规划打印体系结构。此阶段包括分析业务需求、现有打印基础结构、用户和应用程序当前与打印过程的交互方式，以及哪种打印管理模式最适合您的环境。
3. 选择打印机置备方法，然后创建部署打印设计的策略，以配置打印环境。在添加新员工或服务器时更新策略。
4. 为用户部署打印配置前，首先对试验配置进行测试。
5. 管理打印机驱动程序并优化打印性能，以维护 Citrix 打印环境。
6. 对可能发生的问题进行故障排除。

在开始规划部署之前，一定要了解有关打印的以下核心概念：

- 可用的打印机置备类型
- 如何路由打印作业
- 打印机驱动程序管理基础知识

打印概念建立在 Windows 打印概念的基础上。要在您的环境下配置并成功管理打印，您必须了解 Windows 网络和客户端打印的工作原理，及其在此环境下的相应打印行为。

在此环境下，所有打印都在托管应用程序的计算机上由用户启动。打印作业通过网络打印服务器或用户设备重定向到打印设备。

虚拟桌面和应用程序的用户没有永久工作区。会话结束后，用户的工作区将被删除，因此在每个会话开始时需要重新构建所有设置。这样，每次用户启动新会话时，系统都必须重新构建用户的工作区。

用户执行打印时：

- 确定向用户提供的打印机。此过程也称作打印机置备。
- 恢复用户的打印首选项。
- 确定会话的默认打印机。

您可以通过配置打印机置备、打印作业路由、打印机属性保留以及驱动程序管理等选项来自定义这些任务的执行方式。请务必评估各种选项设置对您环境中的打印性能及用户体验有何影响。

在会话中启用打印机的过程称为置备。打印机置备通常采用动态处理方式，即不会预先确定和存储会话中出现的打印机，而是在登录和重新连接期间建立会话时基于策略来装配打印机。因此，打印机会随着策略、用户位置以及网络变化（只要策略中反映了这些内容）而变化。这样，漫游到不同位置的用户可以看到其工作区的变化。

系统还会监视客户端打印机，并根据客户端打印机的添加、删除和更改情况动态调整在会话中自动创建的打印机。动态打印机发现对移动用户很有益，因为他们从各种设备进行连接。

最常用的打印机置备方法有：

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

- **通用打印服务器** - Citrix 通用打印服务器为网络打印机提供通用打印支持。通用打印服务器使用通用打印驱动程序。通过此解决方案，您可以使用服务器操作系统计算机上的单个驱动程序以允许从任何设备进行网络打印。

  Citrix 建议针对远程打印服务器的情况使用 Citrix 通用打印服务器。通用打印服务器通过网络以经过优化和压缩的格式传输打印作业，从而最大程度地减少网络使用，并改善用户体验。

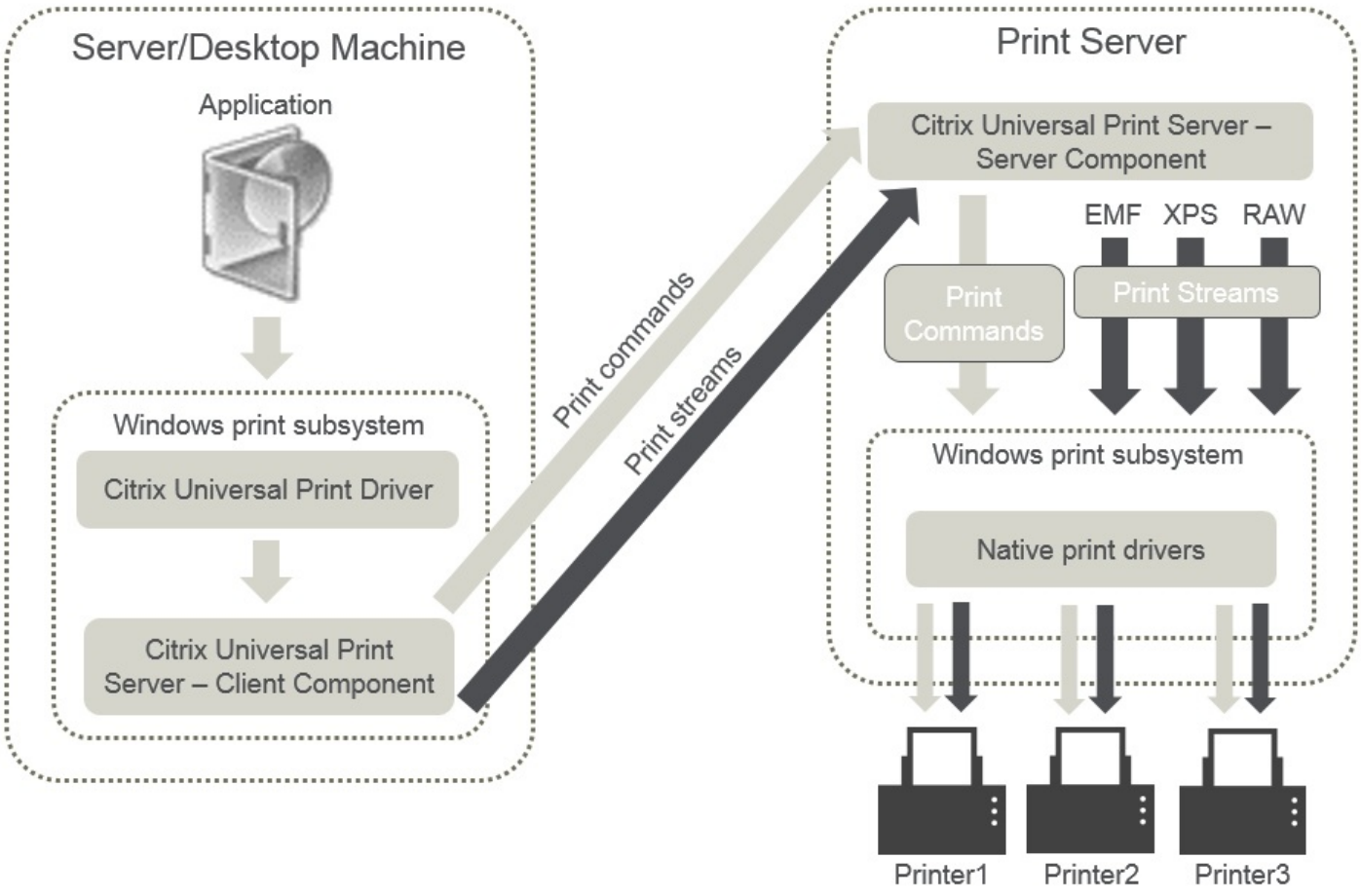
  通用打印服务器功能包含以下组件：

  客户端组件 **UPClient** - 在置备会话网络打印机并且使用通用打印驱动程序的每台服务器操作系统计算机上启用通用打印客户端。

  服务器组件 **UPServer** - 在置备会话网络打印机并且对会话打印机使用通用打印驱动程序的每台打印服务器上安装通用打印服务器（不管会话打印机是否集中置备）。

有关通用打印服务器要求和设置的详细信息，请参阅系统要求和安装一文。

下图显示了在使用通用打印服务器的环境中基于网络的打印机的典型工作流。



启用 Citrix 通用打印服务器时，所有连接的网络打印机都会通过自动发现利用该服务器。

注意：VDI-in-a-Box 5.3 同样支持通用打印服务器。有关利用 VDI-in-a-Box 安装通用打印服务器的信息，请参阅 VDI-in-a-Box 文档。

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

- **自动创建** - *自动创建*指每次启动会话时自动创建的打印机。远程网络打印机和本地连接的客户端打印机都可自动创建。对每个用户具有大量打印机的环境，请考虑仅自动创建默认客户端打印机。自动创建的打印机数量越少，服务器操作系统计算机需要的开销（内存和 CPU）就越少。尽量减少自动创建的打印机数量还可以缩短用户登录时间。
  自动创建的打印机基于：

  - 用户设备上安装的打印机。
  - 适用于会话的任何策略。
    通过自动创建策略，您可以限制自动创建的打印机的数量或类型。默认情况下，在用户设备上自动配置所有打印机（包括本地连接的打印机和网络打印机）时，打印机会在会话中启用。

  用户结束会话后，该会话使用的打印机将被删除。

  客户端和网络打印机自动创建的维护工作彼此关联。例如，要添加打印机，需要执行以下操作：

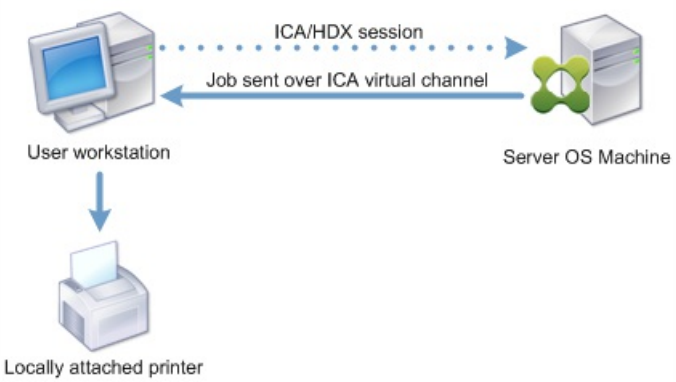
  - 更新会话打印机策略设置。
  - 使用“打印机驱动程序映射和兼容性”策略设置向所有服务器操作系统计算机添加驱动程序。

术语打印途径涉及两个方面：路由打印作业的路径以及对打印作业进行后台打印的位置。此概念的这两方面都很重要。路由会影响网络流量。后台打印会影响对处理打印作业的设备上的本地资源的使用。

在此环境中，打印作业可以由两种途径传送到打印设备：通过客户端或通过网络打印服务器。这两种途径称为客户端打印途径和网络打印途径。默认情况下选择哪种路径取决于所使用的打印机类型。

本地连接的打印机

系统将作业从服务器操作系统计算机通过客户端路由到本地连接的打印机，然后再路由到打印设备。ICA 协议将优化和压缩打印作业流量。打印设备本地连接到用户设备时，打印作业将通过 ICA 虚拟通道进行路由。



基于网络的打印机

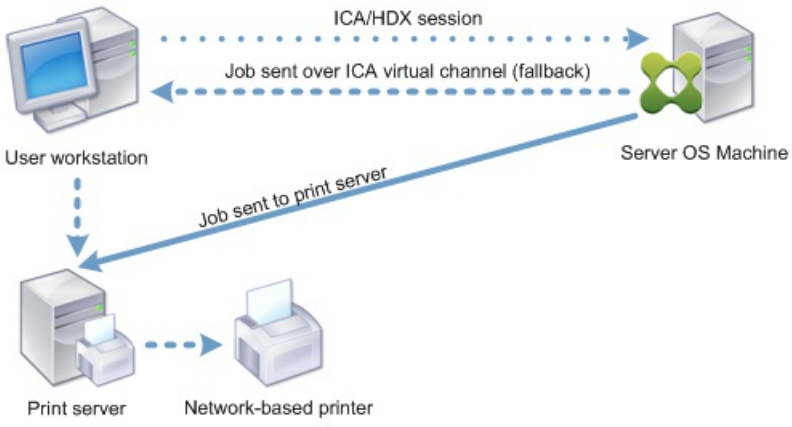
默认情况下，发往网络打印机的所有打印作业都会从服务器操作系统计算机通过网络直接路由到打印服务器。但是在以下情形中，打印作业会自动通过 ICA 连接进行路由：

- 如果虚拟桌面或应用程序无法连接打印服务器。
- 如果本机打印机驱动程序在服务器操作系统计算机上不可用。

如果未启用通用打印服务器，配置面向网络打印的客户端打印途径对低带宽连接（例如广域网）非常有用，这是因为通过 ICA 连接发送作业时会进行流量优化和压缩。

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

此外，客户端打印途径还允许您限制流量或限制分配给打印作业的带宽。如果不能通过用户设备路由作业，例如对于没有打印功能的瘦客户端，应将服务质量配置为优先处理 ICA/HDX 流量，并确保用户在会话中获得良好的体验。



Citrix 通用打印机驱动程序 (UPD) 是独立于设备的打印驱动程序，与大多数打印机兼容。Citrix UPD 由两个组件构成：

服务器组件。Citrix UPD 作为 XenApp 或 XenDesktop VDA 安装的一部分安装。VDA 将以下驱动程序与 Citrix UPD 一起安装：“Citrix 通用打印机”（EMF 驱动程序）和“Citrix XPS 通用打印机”（XPS 驱动程序）。

Name	Processor	Type
Citrix Universal Printer	x64	Type 3 - User Mode
Citrix XPS Universal Printer	x64	Type 3 - User Mode

启动打印作业时，驱动程序记录应用程序的输出，且不做任何修改地发送到端点设备。

客户端组件。Citrix UPD 作为 Citrix Receiver 安装的一部分安装。该驱动程序提取 XenApp 或 XenDesktop 会话的传入打印流。然后将打印流转发到使用设备特定的打印机驱动程序呈现打印作业的本地打印子系统。除了 Citrix UPD 外，Citrix PDF 通用打印机驱动程序也可以分别与 Citrix Receiver for HTML5 和 Citrix Receiver for Chrome 一起安装。

Citrix UPD 支持以下打印格式：

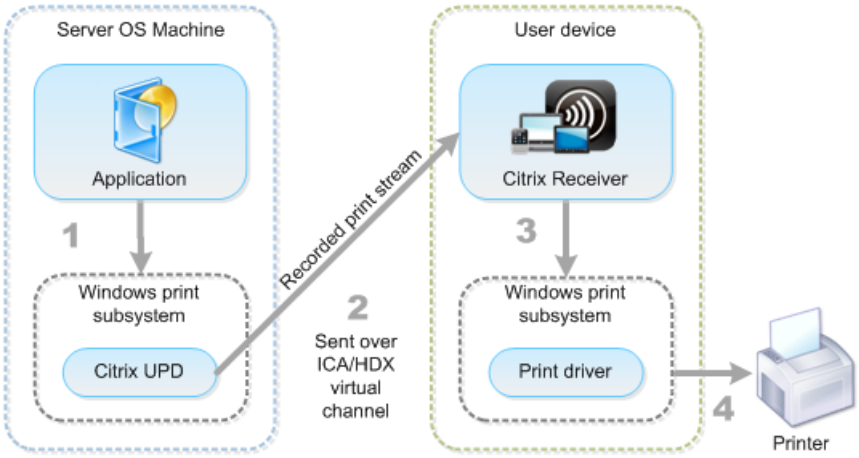
- 增强图元文件格式 (**EMF**)，默认设置。EMF 是 32 位版本的 Windows 图元文件 (WMF) 格式。EMF 驱动程序只能由基于 Windows 的客户端使用。
- XML 纸张规范 (**XPS**)。XPS 驱动程序使用 XML 创建独立于平台的“电子文件”，其格式与 Adobe PDF 格式类似。
- 打印机命令语言（**PCL5c** 和 **PCL4**）。PCL 是 Hewlett-Packard 最初为喷墨式打印机开发的打印协议。它用于打印基本文本和图形，在 HP LaserJet 和多功能外围设备上广受支持。
- PostScript (**PS**)。PostScript 是可以用于打印文本和矢量图形的计算机语言。该驱动程序在低价打印机和多功能外围设备上广泛使用。

PCL 和 PS 驱动程序最适用于使用基于非 Windows 的设备（例如 Mac 或 UNIX 客户端）的场合。可以使用通用驱动程序优先级策略设置来更改 Citrix UPD 尝试使用驱动程序的顺序。

Citrix UDP（EMF 和 XPS 驱动程序）支持高级打印功能，例如，装订和纸张来源选择。这些功能在本机驱动程序使用 Microsoft 打印功能技术允许其可用时才可用。本机驱动程序应在打印功能 XML 中使用标准化的打印架构关键字。如果使用非标准关键字，则高级打印功能将不能通过 Citrix 通用打印驱动程序使用。

下图显示了通用打印驱动程序组件和本地连接到设备的打印机的典型工作流。

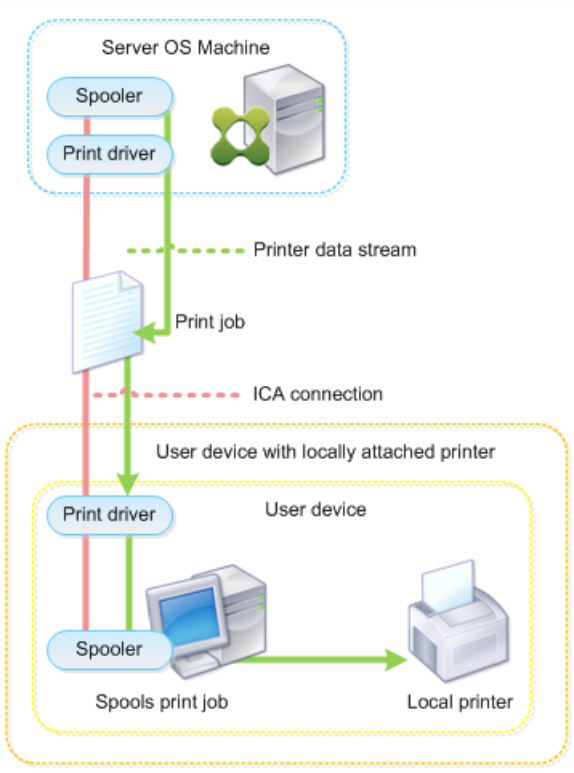
© 1999-2017 Citrix Systems, Inc. All rights reserved.



规划驱动程序管理策略时，请确定支持的驱动程序类型：通用打印驱动程序、设备特定的驱动程序或者两者。如果支持标准驱动程序，您必须确定：

在自动创建打印机期间，如果系统检测到有新的本地打印机连接至用户设备，即会在服务器操作系统计算机中检查是否有所需的打印机驱动程序。默认情况下，如果 Windows 本机驱动程序不可用，系统将使用通用打印驱动程序。

要使打印成功，服务器操作系统计算机上的打印机驱动程序和用户设备上的驱动程序必须匹配。下图显示了如何在两个位置使用打印机驱动程序进行客户端打印。



- 要支持的驱动程序类型。
- 当服务器操作系统计算机中缺少打印机驱动程序时，是否要自动安装打印机驱动程序。

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

- 是否要创建驱动程序兼容性列表。

- 打印配置示例
- 最佳做法、安全注意事项和默认操作
- 打印策略和首选项
- 置备打印机
- 维护打印环境

© 1999-2017 Citrix Systems, Inc. All rights reserved.

打印配置示例

Mar 26, 2018

根据您的需求和环境选择最 合适的打印配置方案可以 简化管理工作。尽管默认打印配置使用户 可以在大多数环境中进行打印，但默认设置可能无法在您的环境中提供预期的用户 体验或最佳网络使用率和管理 开销。

打印 配置取决于：

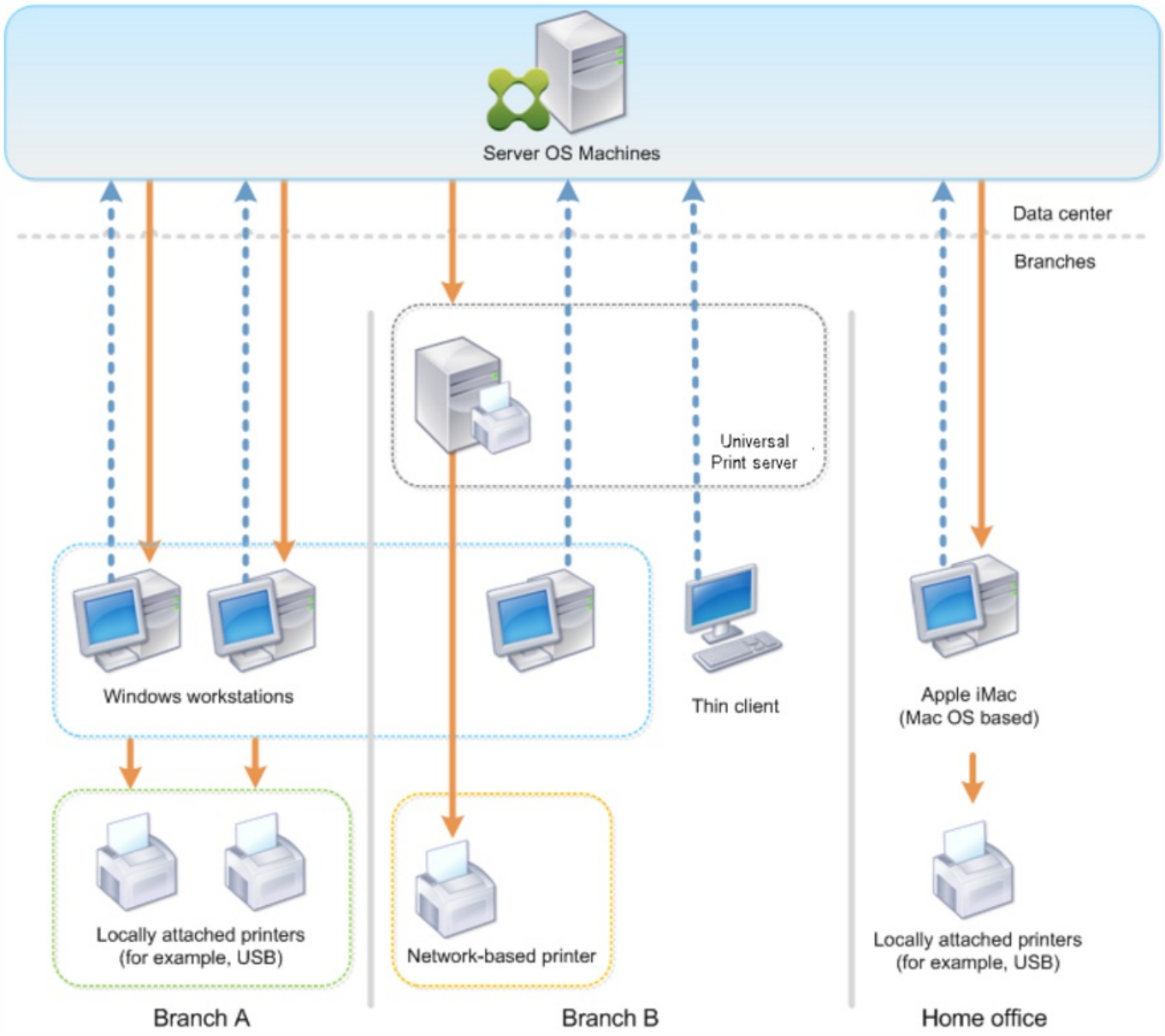
- 业务需求以及现有的打印基础设施。
  应根据贵组织的需求来设计打印配置。 定义打印配置时，现有的打印实现（用户是否可以添加打印机、哪些用户对哪些打印机拥有访问权限等）可以作为非常有用的参考。
- 组织是否设置了为特定用户保留专用打印机（例如人力资源或薪资专用打印机）的安全策略。
- 用户离开主要工作场所时是否需要打印，例如在不同工作站之间移动办公或者出差的工作人员。

在设计 打印配置时，应尽量为会话中的用户提供与 从本地用户设备打印时相同的体验。

下图显示了这些用例的打印部署：

- **分支机构 A** – 小型海外分支机构，具有少数几个 Windows 工作站。每个用户工作站都有一个本地连接的专用打印机。
- **分支机构 B** – 大型分支机构，具有瘦客户端和基于 Windows 的工作站。为了提高效率，此分支机构的用户共享基于网络的打印机（每个楼层一台）。位于分支机构内部的基于 Windows 的打印服务器管理着打印队列。
- **公司总部** – 公司总部，具有基于 Mac 操作系统的用户设备，可访问公司的 Citrix 基础结构。用户设备具有本地连接的打印机。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



以下部分介绍了可最大程度地降低环境复杂性并简化其管理的配置。

在分支机构 A 中，所有用户在基于 Windows 的工作站上工作，因此将使用自动创建的客户端打印机和通用打印机驱动程序。这些技术具有以下优势：

- 性能 — 打印作业通过 ICA 打印通道交付，这样可以压缩打印数据，从而节省带宽。
  为了确保打印大型文档的单个用户不会降低其他用户的会话性能，配置了一个 Citrix 策略以指定最大打印带宽。

  备选解决方案为利用多流 ICA 连接，在此连接中，打印流量在单独的低优先级 TCP 连接中进行传输。多流 ICA 适用于不在 WAN 连接上实施服务质量 (QoS) 时使用。

- 灵活性 – 使用 Citrix 通用打印机驱动程序，可确保还可以从虚拟桌面或应用程序会话使用连接到客户端的所有打印机，而无需在数据中心中集成新打印机驱动程序。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

在分支机构 B 中，所有打印机均基于网络并在 Windows 打印服务器上管理其队列，这样 Citrix 通用打印服务器便成为最有效的配置。

本地管理员在打印服务器上安装并管理所有必需的打印机驱动程序。将打印机映射到虚拟桌面或应用程序会话的工作流程如下：

- 对于基于 Windows 的工作站 — 本地 IT 团队帮助用户将基于网络的相应打印机连接到其 Windows 工作站。这样用户即可从本地安装的应用程序进行打印。
  在虚拟桌面或应用程序会话期间，本地配置的打印机通过自动创建进行枚举。然后，虚拟桌面或应用程序将作为直接网络连接连接到打印服务器（如果可能）。

  将安装并启用 Citrix 通用打印服务器组件，这样就不需要使用本机打印机驱动程序。如果更新驱动程序或修改打印队列，则无需在数据中心进行任何其他配置。

- 对于瘦客户端 — 对于瘦客户端用户，必须在虚拟桌面或应用程序会话内部连接打印机。为了给用户提供最简单的打印体验，管理员为每个楼层配置了一个 Citrix 会话打印机策略，以连接各楼层的默认打印机。
  为确保即使用户在楼层之间移动也能连接正确的打印机，请基于瘦客户端的子网或名称过滤策略。此配置称为邻近打印，允许维护本地打印机驱动程序（根据委派管理模式）。

  如果需要修改或添加打印队列，Citrix 管理员必须修改环境中相应的会话打印机策略。

由于将在 ICA 虚拟通道外部发送网络打印流量，因此必须实施 QoS。ICA/HDX 通信使用的端口上的入站和出站网络流量优先于所有其他网络流量。该配置可确保用户会话不受大型打印作业的影响。

公司总部的用户在非标准工作站工作并使用非托管打印设备，因此最简单的方法是使用自动创建的客户端打印机和通用打印机驱动程序。

概括而言，部署示例如下所示进行配置：

- 未在服务器操作系统计算机上安装任何打印机驱动程序。 仅使用 Citrix 通用打印机驱动程序。 禁用回退到本机打印和自动安装打印机驱动程序。
- 将策略配置为对所有用户自动创建所有客户端打印机。 默认情况下，服务器操作系统计算机将直接连接到打印服务器。 所需的唯一配置是启用通用打印服务器组件。
- 对分支机构 B 的每个楼层配置会话打印机策略，并应用于相应楼层的所有瘦客户端。
- 对分支机构 B 实施 QoS，以确保卓越的用户体验。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

最佳做法、安全注意事项和默认操作

Dec 05, 2017

多种因素决定了特定环境的最佳打印解决方案。其中一些最佳做法可能不适用于您的站点。

- 使用 Citrix 通用打印服务器。
- 使用通用打印机驱动程序或 Windows 本机驱动程序。
- 最大程度减少服务器操作系统计算机上安装的打印机驱动程序的数量。
- 使用映射到本机驱动程序的驱动程序。
- 切勿在生产站点上安装未经测试的打印机驱动程序。
- 避免更新驱动程序。而应尝试卸载驱动程序，重新启动打印服务器，然后安装替代的驱动程序。
- 卸载未使用的驱动程序或使用打印机驱动程序映射和兼容性策略，以防止通过驱动程序创建打印机。
- 尝试避免使用第 2 版内核模式驱动程序。
- 要确定打印机型号是否受支持，请联系制造商或在 www.citrix.com/ready 上查看 Citrix Ready 产品指南。
  一般而言，Microsoft 提供的所有打印机驱动程序都已经过终端服务测试，保证可以与 Citrix 结合使用。但是，在使用第三方打印机驱动程序之前，请咨询打印机驱动程序供应商，以确保该驱动程序已经过 Windows Hardware Quality Labs (WHQL) 程序的终端服务认证。Citrix 不为打印机驱动程序提供认证。

Citrix 打印解决方案采用安全设计。

- Citrix Print Manager Service 会持续监视并响应会话事件，例如登录与注销、断开连接、重新连接以及会话终止。它通过模仿实际会话用户来处理服务请求。
- Citrix 打印在会话中为每台打印机分配唯一的命名空间。
- Citrix 打印为自动创建的打印机设置默认安全描述符，以确保一个会话中自动创建的客户端打印机无法被其他会话中运行的用户所访问。默认情况下，管理员用户不会意外地打印到其他会话的客户端打印机，即使他们可以查看并手动调整任何客户端打印机的权限也是如此。

默认情况下，如果未配置任何策略规则，打印行为如下所述：

- 通用打印服务器处于禁用状态。
- 在每个会话开始时自动创建在用户设备上配置的所有打印机。
  此行为等效于通过自动创建所有客户端打印机选项配置 Citrix 策略设置自动创建客户端打印机。

- 系统将所有排队等候用户设备所连接的本地打印机的打印作业作为客户端打印作业进行路由（使用 ICA 通道或通过用户设备）。
- 系统将所有排队等候网络打印机的打印作业直接从服务器操作系统计算机进行路由。如果系统无法通过网络来路由打印作业，它会将这些作业作为重定向的客户端打印作业通过用户设备进行路由。
  此行为等效于禁用 Citrix 策略设置直接连接到打印服务器。

- 系统会尝试将打印属性存储在用户设备上，打印属性包括用户的打印首选项以及打印设备专用设置这两项内容。如果客户端不支持此操作，系统会将打印属性存储在服务器操作系统计算机上的用户配置文件中。
  此行为等效于通过仅当未保存在客户端时才保留在配置文件中选项配置 Citrix 策略设置打印机属性保留。

- 系统使用 Windows 版本的打印机驱动程序（如果该驱动程序在服务器操作系统计算机上可用）。如果该打印机驱动程序不可用，系统会尝试从 Windows 操作系统中安装该驱动程序。如果 Windows 中没有提供该驱动程序，XenDesktop 将使用

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix 通用打印驱动程序。
此行为等效于通过仅当请求的驱动程序不可用时才使用通用打印启用 Citrix 策略设置自动安装现成的打印机驱动程序并配置通用打印设置。

启用自动安装现有的打印机驱动程序可能会导致安装大量本机打印机驱动程序。

注意：如果不确定用于打印的原始默认设置，可以通过创建新策略并将所有打印策略规则设置为“启用”来显示这些默认设置。显示的选项即为默认设置。

Always-On 日志记录功能对 VDA 上的打印服务器和打印子系统可用。

要将日志整理为 ZIP 文件，以便通过电子邮件发送，或者要将日志自动上载到 Citrix Insight Services，请使用 **Start-TelemetryUpload** PowerShell cmdlet。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

打印策略和首选项

Dec 05, 2017

用户从已发布的应用程序访问 打印机时，可以配置 Citrix 策略以指定以下 设置：

- 如何置备打印机（或者如何将其添加到会话）
- 如何路由打印作业
- 如何管理打印机驱动程序

针对 不同的用户设备、用户或过滤策略时所依据的任何 其他对象，可以设置不同的打印配置。

大多数打印功能都是通过 Citrix 打印策略设置配置的。打印设置遵循标准 Citrix 策略行为。

如果用户的网络帐户有足够权限，系统可以在会话结束时将打印机设置写入打印机对象，或写入客户端打印设备。默认情况下，Receiver 在其他位置查找设置和首选项之前，将使用存储在会话中的打印机对象的设置。

默认情况下， 系统在用户设备上（如果设备 支持）或在服务器操作系统计算机上的用户配置文件中存储或保留打印机属性。如果用户 在会话期间更改打印机属性，这些更改会在计算机上的 用户配置文件中进行更新。下次用户登录或重新连接时， 用户设备会继承这些保留的设置。即，用户必须注销并 重新登录，用户设备上的打印机属性更改 才会影响当前会话。

在 Windows 打印环境中，对打印首选项所做的更改可以保存在本地计算机或文档中。在此环境中，用户修改打印设置时，设置将保存在以下位置：

- **在用户设备上** – Windows 用户可以在用户设备上更改设备设置，方法是在“控制面板”中的打印机上单击鼠标右键并选择打印首选项。例如，如果选择横向作为页面方向，则将把横向保存为该打印机的默认页面方向首选项。
- **在文档内部** – 在文字处理和桌面排版程序中，页面方向等文档设置通常保存在文档中。例如，排列文档进行打印时，Microsoft Word 通常将您指定的打印首选项（例如页面方向和打印机名称）保存在文档中。下次打印该文档时，默认情况下会显示这些设置。
- **从用户在会话期间所做的更改中** – 如果在会话中通过“控制面板”进行更改（即在服务器操作系统计算机上），系统将仅保留对自动创建的打印机的打印设置所做的更改。
- **在服务器操作系统计算机上** — 这些是与计算机上特定打印机驱动程序关联的默认设置。

根据用户做出更改的位置，任何基于 Windows 的环境中保留的设置均会有所差异。也就是说，出现在一个位置（例如电子表格程序中）的打印设置会与其他位置（例如文档中）的打印设置有所差别。因此，应用到特定打印机的打印设置在整个会话过程中可能会发生变化。

由于打印首选项可以保存在多个位置，因此系统会根据特定优先级对其进行处理。 此外，必须注意的是，设备设置与文档设置相互独立且通常优先于文档设置。

默认情况下，系统始终优先应用用户在会话期间修改的任何打印设置（即保留的设置），然后才会考虑其他设置。 当用户打印时，系统会将存储在服务器操作系统计算机上的默认打印机设置与任何保留的或客户端打印机设置进行合并然后应用。

Citrix 建议您不要更改打印机属性的存储位置。默认设置为将打印机属性保存在用户设备上，这是确保打印属性一致的最简便方法。如果系统无法在用户设备上保存属性，则会自动回退到服务器操作系统计算机上的用户配置文件。

请查看打印机属性保留策略设置，确定是否存在以下情况：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 是否使用了不允许用户在用户设备上存储打印机属性的旧版插件。
- 是否在 Windows 网络上使用了强制配置文件并希望保留用户的打印机配置文件。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

置备打印机

Dec 05, 2017

有三种打印机置备方法：

- Citrix 通用打印服务器
- 自动创建的客户端打印机
- 管理员分配的会话打印机

在确定适用于您的环境的最佳打印解决方案时，请考虑以下事项：

- 通用打印服务器提供的以下功能不适用于 Windows 打印提供程序：图像与字体缓存、高级压缩、优化和 QoS 支持。
- 通用打印驱动程序支持由 Microsoft 定义的独立于设备的公共设置。如果用户需要访问特定于打印驱动程序制造商的设备设置，最佳解决方案可能是与 Windows 本机驱动程序配对的通用打印服务器。使用此配置，您可以在保留通用打印服务器优势的同时，允许用户使用专用打印机的功能。需要考虑的一个平衡点是，Windows 本机驱动程序需要维护。
- Citrix 通用打印服务器为网络打印机提供通用打印支持。通用打印服务器使用通用打印驱动程序，该驱动程序是服务器操作系统计算机上的单个驱动程序，允许从任何设备（包括瘦客户端和平板电脑）进行本地打印或网络打印。

要将通用打印服务器与 Windows 本机驱动程序结合使用，请启用通用打印服务器。默认情况下，如果 Windows 本机驱动程序可用，请使用 Windows 本机驱动程序。否则，将使用通用打印驱动程序。要指定对该行为的更改，例如仅使用 Windows 本机驱动程序或仅使用通用打印驱动程序，请更新通用打印驱动程序使用策略设置。

安装通用打印服务器

要使用通用打印服务器，请按安装文档中所述在打印服务器上安装 UpsServer 组件并进行配置。有关详细信息，请参阅安装核心组件和使用命令行安装。

对于要单独部署 UPClient 组件的环境（例如采用 **XenApp 6.5**），请执行以下操作：

1. 下载适用于 Windows 桌面操作系统或 Windows 服务器操作系统的 XenApp 和 XenDesktop Virtual Delivery Agent (VDA) 独立软件包。
2. 根据使用命令行安装中介绍的命令行说明提取 VDA。
3. 从 \Image-Full\Support\VcRedist_2013_RTM 安装必备决条件：
   - Vcredist_x64 / vcredist_x86
     - 对于 32 位部署，仅运行 x86，对于 64 位部署，两个均运行。
4. 从 \Image-Full\x64\Virtual Desktop Components 或 \Image-Full\x86\Virtual Desktop Components 安装 cdf 必备条件。
   - Cdf_x64 / Cdf_x86
     - x86 用于 32 位，x64 用于 64 位
5. 在 \Image-Full\x64\Virtual Desktop Components 或 \Image-Full\x86\Virtual Desktop Components 中查找 UPClient 组件。
6. 解压并启动组件的 MSI 以安装 UPClient 组件。
7. 安装 UPClient 组件后需要重新启动。

退出针对通用打印服务器的 CEIP

在安装通用打印服务器时，您会自动注册 Citrix 客户体验改善计划 (CEIP)。在安装日期和时间后的七日时将首次上载数据。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

要退出 CEIP，请编辑注册表项 **HKLM\Software\Citrix\Universal Print Server\CEIPEnabled**，并将 **DWORD** 值设置为 **0**。

要重新加入，请将 DWORD 值设置为 1。

小心：注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因“注册表编辑器”使用不当导致出现的问题能够得以解决。使用“注册表编辑器”需自担风险。在编辑注册表之前，请务必进行备份。

有关详细信息，请参阅 Citrix Insight Services。

配置通用打印服务器

使用以下 Citrix 策略设置配置通用打印服务器。有关详细信息，请参阅屏幕上的策略设置帮助。

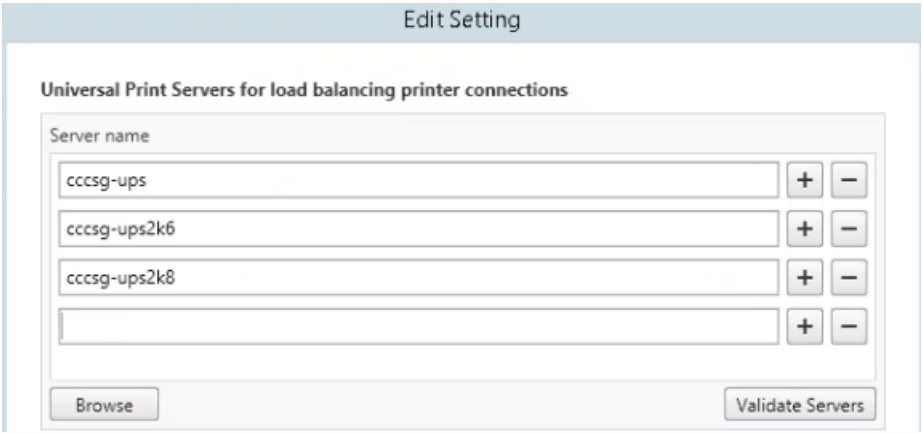
- **启用通用打印服务器**。默认情况下禁用通用打印服务器。启用通用打印服务器时，需要选择是否在通用打印服务器不可用时使用 Windows 打印提供程序。启用通用打印服务器之后，用户可以通过 Windows 打印提供程序和 Citrix 提供程序界面添加和枚举网络打印机。
- **通用打印服务器打印数据流(CGP)端口**。指定由通用打印服务器打印数据流 CGP（通用网关协议）侦听器使用的 TCP 端口号。默认为 **7229**。
- **通用打印服务器 Web 服务(HTTP/SOAP)端口**。指定由通用打印服务器侦听器使用的 TCP 端口号，用以侦听传入的 HTTP/SOAP 请求。默认值为 **8080**。

要更改通用打印服务器与 XenApp 和 XenDesktop VDA 进行通信的 HTTP 8080 默认端口，还必须创建以下注册表项，并修改通用打印服务器计算机上的端口号值：

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PrintingPolicies
"UpsHttpPort"=DWORD:

此端口号必须与 Studio 中的 HDX 策略“通用打印服务器 Web 服务(HTTP/SOAP)端口”匹配。

- **通用打印服务器打印流输入带宽限制(kbps)**。指定使用 CGP 从每个打印作业向通用打印服务器交付打印数据时的传输速率上限 (kbps)。默认为 0（无限制）。
- **用于负载平衡的通用打印服务器**。此设置列出了在评估其他 Citrix 打印策略设置后，用于对会话启动时建立的打印机连接执行负载平衡的通用打印服务器。为了优化打印机创建时间，Citrix 建议所有打印服务器具有相同的共享打印机集合。



- **通用打印服务器停止运行阈值**。指定负载平衡器应在多长时间内等待不可用的打印服务器恢复，在此之后负载平衡器将该服务器确定为永久脱机，并将其负载重新分配到其他可用的打印服务器。默认值是 180（秒）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

在 Delivery Controller 上修改打印策略后，可能需要几分钟时间来向 VDA 应用策略更改。

与其他策略设置的交互 - 通用打印服务器支持其他 Citrix 打印策略设置并如下表所述与之交互。下表中提供的信息基于以下假设：已启用通用打印服务器策略设置，已安装通用打印服务器组件，并已应用策略设置。

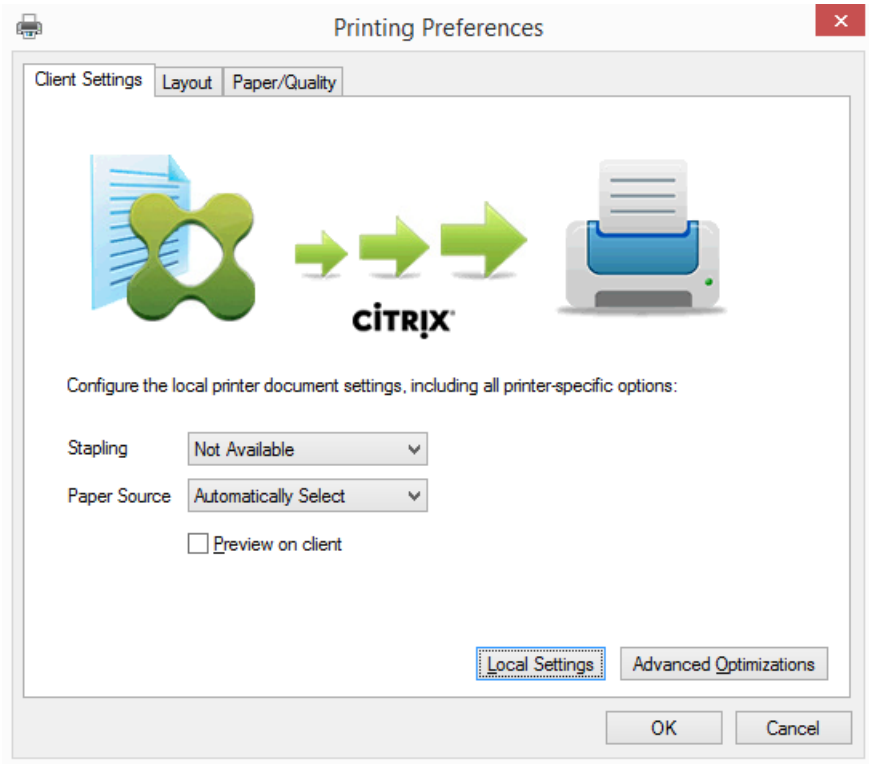
策略设置	交互
客户端打印机重定向，自动创建客户端打印机	启用通用打印服务器之后，将使用通用打印驱动程序（而非本机驱动程序）创建客户端网络打印机。用户看到的打印机名称与先前相同。
会话打印机	使用 Citrix 通用打印服务器解决方案时，将保留通用打印驱动程序策略设置。
与打印服务器的直接连接	启用通用打印服务器并将通用打印驱动程序使用策略设置配置为仅使用通用打印时，可使用通用打印驱动程序在打印服务器上创建直接网络打印机连接。
UPD 首选项	支持 EMF 和 XPS 驱动程序。

对用户界面的影响 - 通用打印服务器使用的 Citrix 通用打印驱动程序会禁用以下用户界面控件：

- “打印机属性”对话框中的“本地打印机设置”按钮
- “文档属性”对话框中的“本地打印机设置”和“在客户端上预览”按钮

Citrix 通用打印驱动程序（EMF 和 XPS 驱动程序）支持高级打印功能，例如，装订和纸张来源。用户可以从自定义 UPD 打印对话框中选择“装订”或“纸张来源”选项（如果映射到会话中的 UPD 的客户端或网络打印机支持这些功能）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



自定义 UPD 打印对话框

要设置非标准打印机设置（例如，装订和安全 PIN），请在客户的 UPD 打印对话框中，为使用 Citrix UPD EMF 或 XPS 驱动程序的任何客户端映射的打印机选择**本地设置**。映射的打印机的**打印首选项**对话框显示在客户端上会话之外（允许用户更改任何打印机选项），并且打印文档时，修改后的打印机设置用于活动会话中。

这些功能在本机驱动程序使用 Microsoft 打印功能技术允许其可用时才可用。本机驱动程序应在打印功能 XML 中使用标准化的打印架构关键字。如果使用非标准关键字，则高级打印功能将不能通过 Citrix 通用打印驱动程序使用。

使用通用打印服务器时，Citrix 打印提供程序的“添加打印机”向导与 Windows 打印提供程序的“添加打印机”向导相同，但有以下几点不同：

- 按名称或地址添加打印机时，可以提供打印服务器的 HTTP/SOAP 端口号。该端口号将成为打印机名称的一部分并出现在名称显示中。
- 如果 Citrix 通用打印驱动程序使用策略设置指定必须使用通用打印，则选择打印机时将显示通用打印驱动程序名称。Windows 打印提供程序无法使用通用打印驱动程序。

Citrix Print Provider 不支持客户端呈现。

有关通用打印服务器的详细信息，请参阅 CTX200328。

针对客户端打印机提供以下通用打印解决方案：

- **Citrix 通用打印机** – 在会话开始时创建的通用打印机，未绑定到打印设备。在登录期间枚举可用的客户端打印机不需要使用 Citrix 通用打印机，从而可以极大降低资源使用率并减少用户登录次数。通用打印机可以打印到任何客户端打印设备。Citrix 通用打印机不一定适用于您环境中的所有用户设备或 Citrix Receiver。Citrix 通用打印机需要 Windows 环境，不支持 Citrix 脱机插件或者流传输到客户端的应用程序。对于此类环境，请考虑使用自动创建的客户端打印机和通用打印驱动程

© 1999-2017 Citrix Systems, Inc. All rights reserved.

序。

要对非 Windows Citrix Receiver 使用通用打印解决方案，请使用基于 PostScript/PCL 并自动安装的其他通用打印驱动程序之一。

- **Citrix 通用打印驱动程序** - 独立于设备的打印机驱动程序。如果配置 Citrix 通用打印驱动程序，则系统默认使用基于 EMF 的通用打印驱动程序。
  此外，与旧版或较低级的打印机驱动程序相比，Citrix 通用打印驱动程序可能会创建更小的打印作业。但是，可能需要特定于设备的驱动程序才能优化专用打印机的打印作业。

配置通用打印 - 使用以下 Citrix 策略设置配置通用打印。有关详细信息，请参阅屏幕上的策略设置帮助。

- 通用打印。指定何时使用通用打印。
- 自动创建一般通用打印机。允许或禁止在使用与通用打印兼容的用户设备时为会话自动创建一般 Citrix 通用打印机对象。默认情况下不自动创建一般通用打印机对象。
- 通用驱动程序首选项。指定系统尝试使用通用打印驱动程序的顺序，从列表中的第一项开始。可以添加、编辑或删除驱动程序以及更改列表中驱动程序的顺序。
- 通用打印预览首选项。指定是否使用自动创建的打印机或一般通用打印机的打印预览功能。
- 通用打印 EMF 处理模式。控制在 Windows 用户设备上处理 EMF 后台打印文件的方法。默认情况下，系统将 EMF 记录直接后台打印到打印机中。借助直接后台打印到打印机中的方式，后台处理程序可以更快地处理记录，且使用的 CPU 资源更少。

有关更多策略，请参阅优化打印性能。要更改默认设置（例如纸张大小、打印质量、色彩、双面打印和份数），请参阅 CTX113148。

在用户设备中自动创建打印机 - 默认情况下，在会话开始时，系统会在用户设备上自动创建所有打印机。您可以控制为用户置备的打印机类型（如果有），并防止自动创建。

使用 Citrix 策略设置自动创建客户端打印机可控制自动创建。您可以指定以下内容：

- 在每个会话开始时自动创建对用户设备可见的所有打印机，包括网络打印机和本机连接的打印机（默认值）
- 自动创建以物理方式连接到用户设备的所有本地打印机
- 仅自动创建用户设备的默认打印机
- 对所有客户端打印机禁用自动创建

自动创建客户端打印机设置要求将客户端打印机重定向设置为允许（默认值）。

默认情况下，会话开始时会在用户设备上自动创建网络打印机。系统使您能够通过指定要在每个会话中创建的网络打印机，减少枚举或映射的网络打印机数量。这类打印机称为会话打印机。

您可以按 IP 地址过滤会话打印机策略以提供邻近打印。通过邻近打印，指定 IP 地址范围内的用户可以自动访问该范围内存在的网络打印设备。邻近打印由 Citrix 通用打印服务器提供，并且不需要进行本节所述的配置。

邻近打印可能涉及以下情况：

- 内部公司网络与为用户自动指定 IP 地址的 DHCP 服务器一起运行。
- 公司内的所有部门均具有唯一的指定 IP 地址范围。
- 网络打印机存在于每个部门的 IP 地址范围内。

如果配置了邻近打印，则员工从一个部门转移到另一个部门时，无需进行其他打印设备配置。只要用户设备在新部门的 IP 地址范围内得以识别，即对该范围内的所有网络打印机具有访问权限。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置要在会话中重定向的特定打印机 - 要创建由管理员分配的打印机，请配置 Citrix 策略设置会话打印机。使用以下方法之一向该策略添加网络打印机：

- 使用格式 \\servername\printername 输入打印机 UNC 路径。
- 浏览到网络上的打印机位置。
- 浏览特定服务器上的打印机。使用格式 \\servername 输入服务器名称，并单击浏览。

重要：服务器将合并所有已应用策略的所有已启用会话打印机设置，合并顺序为按优先级从最高到最低。如果在多个策略对象中配置了某个打印机，则仅采用配置了该打印机且具有最高优先级的策略对象中的自定义默认设置。
根据会话启动时所处的位置（通过对子网等对象进行过滤），使用会话打印机设置创建的网络打印机可能有所不同。

为会话指定默认网络打印机 - 默认情况下，用户的主打印机将用作会话的默认打印机。使用 Citrix 策略设置默认打印机更改会话中在用户设备上建立默认打印机的方式。

1. 在默认打印机设置页面上，为选择客户端的默认打印机选择一项设置：
   - Network printer name。此菜单中会显示使用会话打印机策略设置添加的打印机。选择用作该策略的默认打印机的网络打印机。
   - 不调整用户的默认打印机。使用默认打印机当前的终端服务或 Windows 用户配置文件设置。有关详细信息，请参阅屏幕上的策略设置帮助。
2. 将该策略应用于要施加影响的用户组（或其他过滤的对象）。

配置邻近打印 - Citrix 通用打印服务器还提供了邻近打印，这不需要本部分中所述的配置。

1. 为每个子网（或针对打印机位置）创建一个单独的策略。
2. 在每个策略中，将位于该子网所处地理位置的打印机添加到会话打印机设置。
3. 将默认打印机设置设置为不调整用户的默认打印机。
4. 按照客户端 IP 地址过滤策略。请确保更新这些策略，以反映对 DHCP IP 地址范围的更改。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

维护打印环境

Dec 05, 2017

维护打印环境包括：

- 管理打印机驱动程序
- 优化打印性能
- 显示打印机和管理打印队列

为了最大程度地降低管理开销和打印驱动程序出现问题的可能性，Citrix 建议使用 Citrix 通用打印驱动程序。

默认情况下，如果自动创建失败，系统会安装 Windows 提供的 Windows 本机打印机驱动程序。如果驱动程序不可用，系统将回退到通用打印驱动程序。有关打印机驱动程序默认值的详细信息，请参阅最佳做法、安全注意事项和默认操作。

如果 Citrix 通用打印驱动程序并不适用于所有方案，请映射打印机驱动程序以最大程度减少服务器操作系统计算机上安装的驱动程序数量。此外，通过映射打印机驱动程序，您可以执行以下操作：

- 允许指定的打印机仅使用 Citrix 通用打印驱动程序
- 允许或阻止使用指定的驱动程序创建打印机
- 使用性能良好的打印机驱动程序替换过时或已损坏的驱动程序
- 使用 Windows 服务器上可用的驱动程序替换客户端驱动程序名称

阻止自动安装打印机驱动程序 - 应禁用自动安装打印驱动程序，以确保服务器操作系统计算机之间的一致性。可以通过 Citrix 和/或 Microsoft 策略实现这一点。要阻止自动安装 Windows 本机打印机驱动程序，请禁用 Citrix 策略设置自动安装现有的打印机驱动程序。

映射客户端打印机驱动程序 - 每个客户端都会在登录期间提供有关客户端打印机的信息（包括打印机驱动程序名称）。在自动创建客户端打印机期间，会选择与客户端提供的打印机型号名称相对应的 Windows 服务器打印机驱动程序名称。然后，自动创建过程会使用已识别的可用打印机驱动程序构建重定向的客户端打印队列。

以下是定义驱动程序替换规则以及编辑映射客户端打印机驱动程序的打印设置的常规过程：

1. 要指定自动创建的客户端打印机的驱动程序替换规则，可以通过以下方法配置 Citrix 策略设置打印机驱动程序映射和兼容性：添加客户端打印机驱动程序名称，然后从查找打印机驱动程序菜单中选择要替换客户端打印机驱动程序的服务器驱动程序。可以在此设置中使用通配符。例如，要强制 HP 打印机使用特定的驱动程序，可以在策略设置中指定 HP*。
2. 要禁用打印机驱动程序，请选择驱动程序名称并选中不创建设置。
3. 根据需要，编辑现有映射，删除映射，或更改列表中驱动程序条目的顺序。
4. 要编辑映射客户端打印机驱动程序的打印设置，请选择打印机驱动程序，单击设置，然后指定打印质量、方向和颜色等设置。如果指定打印机驱动程序不支持的打印选项，该选项将不起任何作用。此设置将覆盖用户在先前会话期间设置的保留打印机设置。
5. Citrix 建议在映射驱动程序之后详细测试打印机的行为，因为某些打印机功能仅在特定的驱动程序中提供。

当用户登录时，系统将在设置客户端打印机前检查客户端打印机驱动程序兼容性列表。

要优化打印性能，请使用通用打印服务器和通用打印驱动程序。以下策略可控制打印优化和压缩：

- 通用打印优化默认值。指定在为会话创建通用打印机时所使用的通用打印机默认设置：
  - 所需图像质量指定应用到通用打印的默认图像压缩限制。默认情况下，启用标准质量，这意味着用户只能使用标准或降低

© 1999-2017 Citrix Systems, Inc. All rights reserved.

质量的压缩级别来打印图像。
  - 启用超级压缩用于启用或禁用在超出由“所需图像质量”所设置的压缩级别上减少带宽，而不降低图像质量。默认情况下，禁用超级压缩功能。
  - 图像与字体缓存设置指定是否缓存在打印流中多次出现的图像和字体，以确保每个唯一的图像或字体只发送给打印机一次。默认情况下，将缓存嵌入式图像和字体。
  - 允许非管理员修改这些设置指定用户是否可以更改会话内的默认打印优化设置。默认情况下，不允许用户更改默认打印优化设置。
- 通用打印图像压缩限制。定义通过通用打印驱动程序所打印的图像可使用的最高质量和最低压缩级别。默认情况下，图像压缩限制设置为最佳质量(无损压缩)。
- 通用打印打印质量限制。指定在会话中生成打印输出时可用的最高分辨率 (dpi)。默认情况下，指定“无限制”。

默认情况下，发往网络打印机的所有打印作业都会从服务器操作系统计算机通过网络直接路由到打印服务器。如果网络出现时间延迟或者带宽有限，请考虑通过 ICA 连接路由打印作业。要执行此操作，请禁用 Citrix 策略设置直接连接到打印服务器。通过 ICA 连接发送的数据会进行压缩，因此通过 WAN 传输数据占用的带宽更少。

通过限制打印带宽提升会话性能 - 当文件从服务器操作系统计算机打印到用户打印机时，其他虚拟通道（例如视频）可能会因为争用带宽而导致性能下降，特别是当用户通过速度较慢的网络访问服务器时。为避免出现此类性能下降，可以限制用户打印所用的带宽。通过限制打印的数据传输速率，可将 HDX 数据流中的更多带宽用于视频、按键以及鼠标数据的传输。

重要：打印机带宽限制始终会强制执行，即使其他通道处于不使用状态时也是如此。
使用以下 Citrix 策略带宽打印机设置来配置打印带宽会话限制。要为站点设置限制，请使用 Studio 执行此任务。要为单个服务器设置限制，请在每台服务器操作系统计算机上使用 Windows 中的组策略管理控制台从本地执行此任务。
- 打印机重定向带宽限制设置指定用于打印的带宽，以千字节/秒 (kbps) 为单位。
- 打印机重定向带宽限制百分比设置可将用于打印的带宽限制为可用总带宽的一定百分比。
  注意：要使用打印机重定向带宽限制百分比设置以百分比形式指定带宽，还需启用总会话带宽限制。
  如果为这两个设置都输入了值，将采用最严格的设置（即值较低的设置）。

要获取有关打印带宽的实时信息，请使用 Citrix Director。

可以通过向负载平衡解决方案添加更多打印服务器来扩展通用打印服务器解决方案。不存在单一故障点，因为每个 VDA 都具有自己的负载平衡器，用于将印刷负载分配到所有打印服务器。

可使用策略设置用于负载平衡的通用打印服务器和通用打印服务器停止运行阈值在负载平衡解决方案中的所有打印服务器上分配打印负载。

如果某打印服务器发生意外故障，则每个 VDA 中的负载平衡器的故障转移机制会将该故障打印服务器上已分配的打印机连接自动重新分配给其他可用打印服务器，使得所有现有会话和传入会话正常工作，而不会影响用户体验，并且不需要管理员立即进行干预。

管理员可以使用一组性能计数器来监视已进行负载平衡的打印服务器的活动，以便在 VDA 中跟踪以下项：

- VDA 上的负载平衡打印服务器及其状态（可用、不可用）的列表
- 每个打印服务器所接受的打印机连接数
- 每个打印服务器上的失败打印机连接数
- 每个打印服务器上的活动打印机连接数
- 每个打印服务器上的挂起打印机连接数

© 1999-2017 Citrix Systems, Inc. All rights reserved.

下表总结了在您的环境中可以显示打印机以及管理打印队列的位置。

	打印途径	是否启用了 UAC？	位置
客户端打印机（连接到用户设备的打印机）	客户端打印途径	开	Microsoft 管理控制台中的打印管理管理单元
		关	Windows 8 之前的系统：控制面板 Windows 8：打印管理管理单元
网络打印机（网络打印服务器上的打印机）	网络打印途径	开	打印服务器 > Microsoft 管理控制台中的打印管理管理单元
		关	打印服务器 > 控制面板
网络打印机（网络打印服务器上的打印机）	客户端打印途径	开	打印服务器 > Microsoft 管理控制台中的打印管理管理单元
		关	Windows 8 之前的系统：控制面板 Windows 8：打印管理管理单元
本地网络服务器打印机（来自网络打印服务器且已添加到服务器操作系统计算机）	网络打印途径	开	打印服务器 > 控制面板
		关	打印服务器 > 控制面板

注意：使用网络打印途径的网络打印机的打印队列是专用的，不能通过系统进行管理。

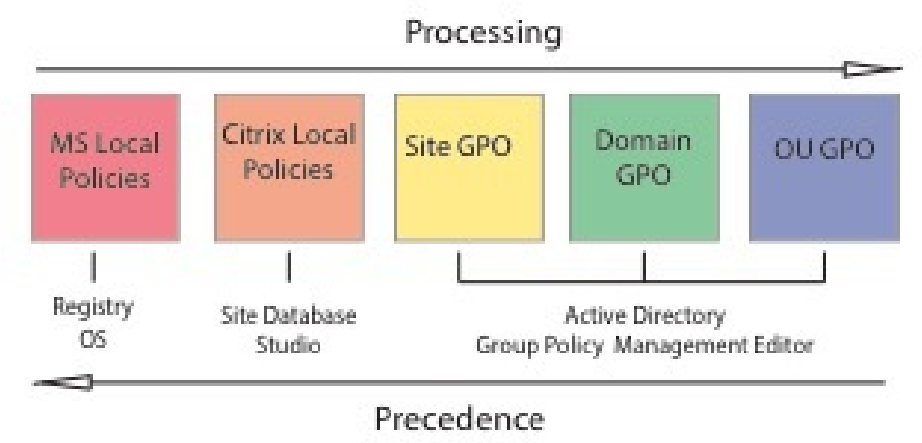
© 1999-2017 Citrix Systems, Inc. All rights reserved.

策略

Dec 05, 2017

策略是设置的集合，这些设置定义如何为一组用户、设备或连接类型管理会话、带宽和安全性。

可以为物理计算机和虚拟机或用户提供策略设置。可以向本地级别或 Active Directory 的安全组中的单个用户应用设置。配置定义具体的条件和规则，如果您没有明确分配策略，设置将应用于所有连接。



可以在网络的不同级别应用策略。位于组织单位 GPO 级别的策略设置在网络上具有最高优先级。域 GPO 级别的策略覆盖站点组策略对象级别的策略，后者覆盖 Microsoft 和 Citrix 本地策略级别上任何存在冲突的策略。

所有 Citrix 本地策略在 Citrix Studio 控制台上创建和管理，并存储在站点数据库中；而组策略使用 Microsoft 组策略管理控制台 (GPMC) 进行创建和管理，并存储在 Active Directory 中。Microsoft 本地策略在 Windows 操作系统中创建，存储在注册表中。

Studio 使用建模向导帮助管理员比较模板和策略中的配置设置，以便排除冲突和冗余设置。管理员可以使用 GPMC 设置 GPO 以配置设置并将其应用于网络上不同级别的目标用户集合中。

这些 GPO 保存在 Active Directory 中，大多数 IT 通常会限制对这些设置管理的访问以确保安全。

设置根据优先级及其条件合并。任何禁用设置都会覆盖等级较低的启用设置。未配置的策略设置会被忽略，且不会覆盖等级较低的设置。

本地策略也可能会与 Active Directory 中的组策略冲突，在这种情况下，二者会根据具体情况相互覆盖。

所有策略按照以下顺序处理：

1. 最终用户使用域凭据登录计算机。
2. 凭据被发送到域控制器。
3. Active Directory 应用所有策略（最终用户、端点、组织单位和域）。
4. 最终用户登录 Receiver 并访问应用程序或桌面。
5. 为最终用户和托管资源的计算机处理 Citrix 和 Microsoft 策略。
6. Active Directory 确定策略设置的优先级，并将其应用于端点设备的注册表和托管资源的计算机。
7. 最终用户从资源注销。最终用户和端点设备的 Citrix 策略不再起作用。
8. 最终用户注销用户设备，从而释放 GPO 用户策略。
9. 最终用户关闭设备，从而释放 GPO 计算机策略。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

为一组用户、设备和计算机创建策略时，有些成员可能会有其他要求，并可能需要设置某些策略设置的例外情况。例外通过 Studio 和 GPMC 中的过滤器方式实现，用以确定策略所影响的人员或内容。

注意：不支持在同一个 GPO 中混合使用 Windows 策略和 Citrix 策略。

- 使用策略
- 策略模板
- 创建策略
- 对策略进行比较、设定优先级、建模和故障排除
- 默认策略设置
- 策略设置参考

© 1999-2017 Citrix Systems, Inc. All rights reserved.

使用策略

Dec 05, 2017

配置 Citrix 策略以控制用户访问或会话环境。Citrix 策略是 控制连接、安全性和带宽设置最有效的 方法。您可以针对特定用户组、设备或 连接类型创建策略。每个策略可以包含多个设置。

可以使用以下工具处理 Citrix 策略。

- **Studio** - 如果您是 Citrix 管理员，但没有管理组策略的权限，可以使用 Studio 为您的站点创建策略。使用 Studio 创建的策略存储在站点数据库中，当虚拟桌面注册到代理或用户连接到虚拟桌面时，系统会将更新信息推送到该虚拟桌面。
- **本地组策略编辑器**（Microsoft 管理控制台管理单元） - 如果您的网络环境使用 Active Directory，并且您拥有管理组策略的权限，则可以使用本地组策略编辑器为站点创建策略。您配置的设置会对在组策略管理控制台中指定的组策略对象 (GPO) 产生影响。
  重要：必须使用本地组策略编辑器配置某些策略设置，包括与向 Controller 注册 VDA 相关的策略设置和与 App-V 服务器相关的策略设置。

组策略设置的处理顺序如下：

1. 本地 GPO
2. XenApp 或 XenDesktop 站点 GPO（存储在站点数据库中）
3. 站点级 GPO
4. 域级 GPO
5. 组织单位

但是，如果存在冲突，最后处理的策略设置会覆盖较早处理的策略设置。 这意味着策略设置的优先级顺序如下：

1. 组织单位
2. 域级 GPO
3. 站点级 GPO
4. XenApp 或 XenDesktop 站点 GPO（存储在站点数据库中）
5. 本地 GPO

例如，Citrix 管理员使用 Studio 创建了一个策略（策略 A），用于为公司的销售员工启用客户端文件重定向。 同时，另一名管理员使用组策略编辑器也创建了一个策略（策略 B），用于为销售员工禁用客户端文件重定向。 当销售员工登录到虚拟桌面时，将应用策略 B 而忽略策略 A，因为策略 B 在域级别处理，而策略 A 在 XenApp 或 XenDesktop 站点 GPO 级别处理。

但是，当用户启动 ICA 或远程桌面协议 (RDP) 会话时，Citrix 会话设置将覆盖在 Active Directory 策略中或使用远程桌面会话主机配置进行配置的相同设置。 这包括与典型的 RDP 客户端连接设置相关的设置（例如桌面墙纸、菜单动画以及拖动时查看窗口内容）。

使用多个策略时，可以向包含冲突设置的策略分配优先级，请参阅 对策略进行比较、设定优先级、建模和故障排除 了解详细信息。

策略的配置过程如下：

1. 创建策略。
2. 配置策略设置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. 将策略分配给计算机和用户对象。
4. 设定策略的优先级。
5. 通过运行 Citrix 组策略建模向导确认有效策略。

在本地组策略编辑器中，策略和设置分为两个类别显示：计算机配置和用户配置。每个类别都具有 Citrix 策略节点。请参阅 Microsoft 文档以了解导航和使用此管理单元的详细信息。

在 Studio 中，策略设置按其所影响的功能分为多个类别。例如，Profile Management 部分包含用于 Profile Management 的策略设置。

- 计算机设置（应用于计算机的策略设置）定义虚拟桌面的行为并在虚拟桌面启动时应用。即使虚拟桌面上没有活动的用户会话，也会应用这些设置。用户设置定义了使用 ICA 连接时的用户体验。当用户使用 ICA 连接或重新连接时应用用户策略。如果用户使用 RDP 连接或直接登录控制台，将不应用用户策略。

  要访问策略、设置或模板，请在 Studio 导航窗格中选择策略。
  - **策略**选项卡列出所有策略。选择某个策略时，右侧的选项卡显示：概览（名称、优先级、启用/禁用状态和说明）、设置（已配置设置的列表）和已分配给（策略当前分配到的用户和计算机对象）。有关详细信息，请参阅创建策略。
  - **模板**选项卡列出 Citrix 提供的模板和您创建的自定义模板。选择模板时，右侧的选项卡显示：说明（要使用此模板的原因）和设置（已配置设置的列表）。有关详细信息，请参阅策略模板。
  - 利用**比较**选项卡，您可以将某个策略或模板中的设置与其他策略或模板中的设置进行比较。例如，您可能希望验证设置值以确保符合最佳做法。有关详细信息，请参阅对策略进行比较、设定优先级、建模和故障排除。
  - 从**建模**选项卡，可以利用 Citrix 策略模拟连接场景。有关详细信息，请参阅对策略进行比较、设定优先级、建模和故障排除。

  要搜索策略或模板中的设置，请执行以下操作：
  1. 选择策略或模板。
  2. 在“操作”窗格中选择编辑策略或编辑模板。
  3. 在设置页面，首先输入设置的名称。

  可以通过选择特定的产品版本或类别（例如带宽），或通过选中仅查看所选对象复选框，或选择仅搜索已添加到选定策略中的设置，来精简搜索结果。对于未过滤的搜索，请选择所有设置。

- 要在策略中搜索设置，请执行以下操作：
  1. 选择该策略。
  2. 选择设置选项卡，首先输入设置的名称。

可以通过选择特定产品版本或类别精简搜索结果。对于未过滤的搜索，请选择所有设置。

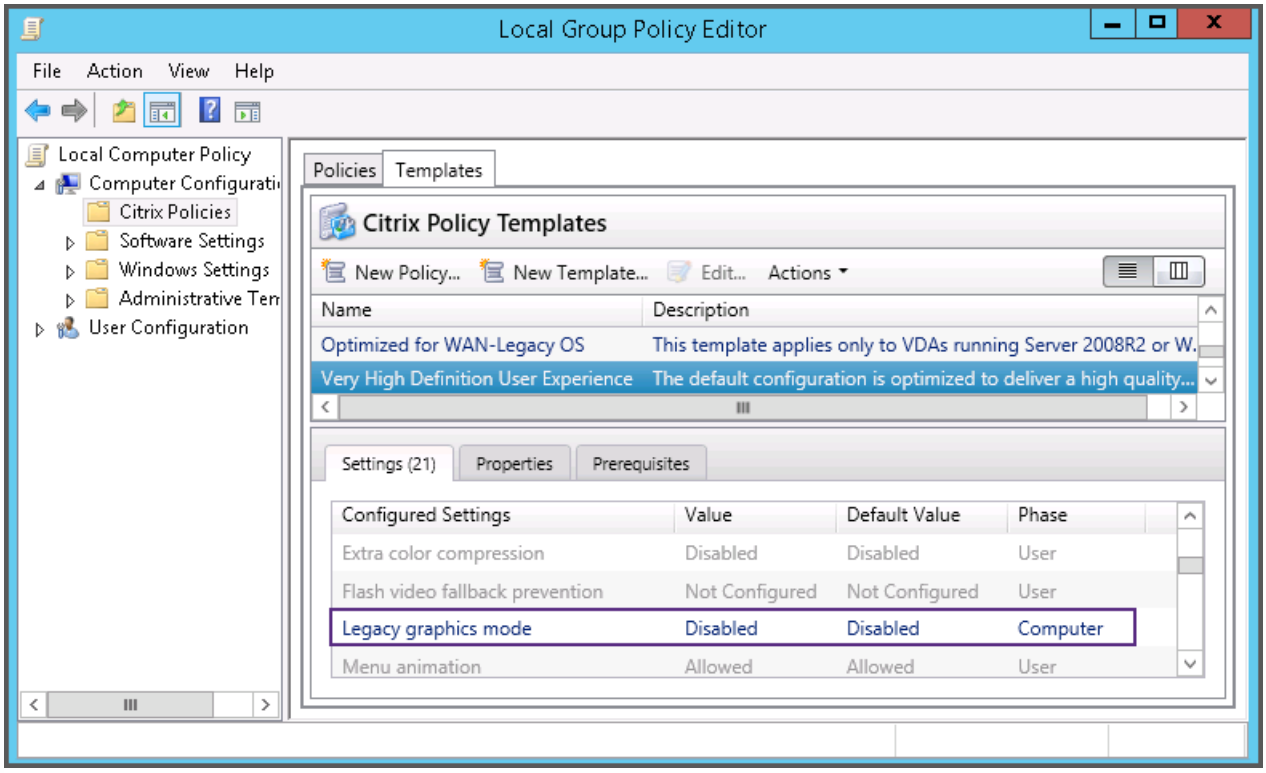
策略一旦创建，便完全独立于所使用的模板。您可以使用新策略的“说明”字段来跟踪所使用的源模板。

在 Studio 中，策略和模板显示在单个列表中，不管它们是否包含用户、计算机或两种设置类型，并且可以使用用户和计算机过滤器进行应用。

在组策略编辑器中，计算机和用户设置必须单独应用，即使是通过包含两种设置类型的模板创建也是如此。在此示例中，选择使用计算机配置中的超高清晰度用户体验：

- 旧图形模式是用于通过此模板创建的策略的计算机设置。
- 灰显的用户设置不用于通过此模板创建的策略。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

策略模板

Dec 05, 2017

模板是从预定义的起点创建策略的源。内置 Citrix 模板已针对特定环境或网络条件优化，可以用作：

- 用于创建自己的策略和模板以在站点之间共享的源。
- 易于在部署之间比较结果的参考，因为您将可以在结果两边加上引号，例如，“..when using Citrix template x or y..”。
- 通过导入或导出模板与 Citrix 支持或可信第三方通信策略的方法。

策略模板可以导入或导出。有关其他模板和内置模板的更新，请参阅 CTX202000。

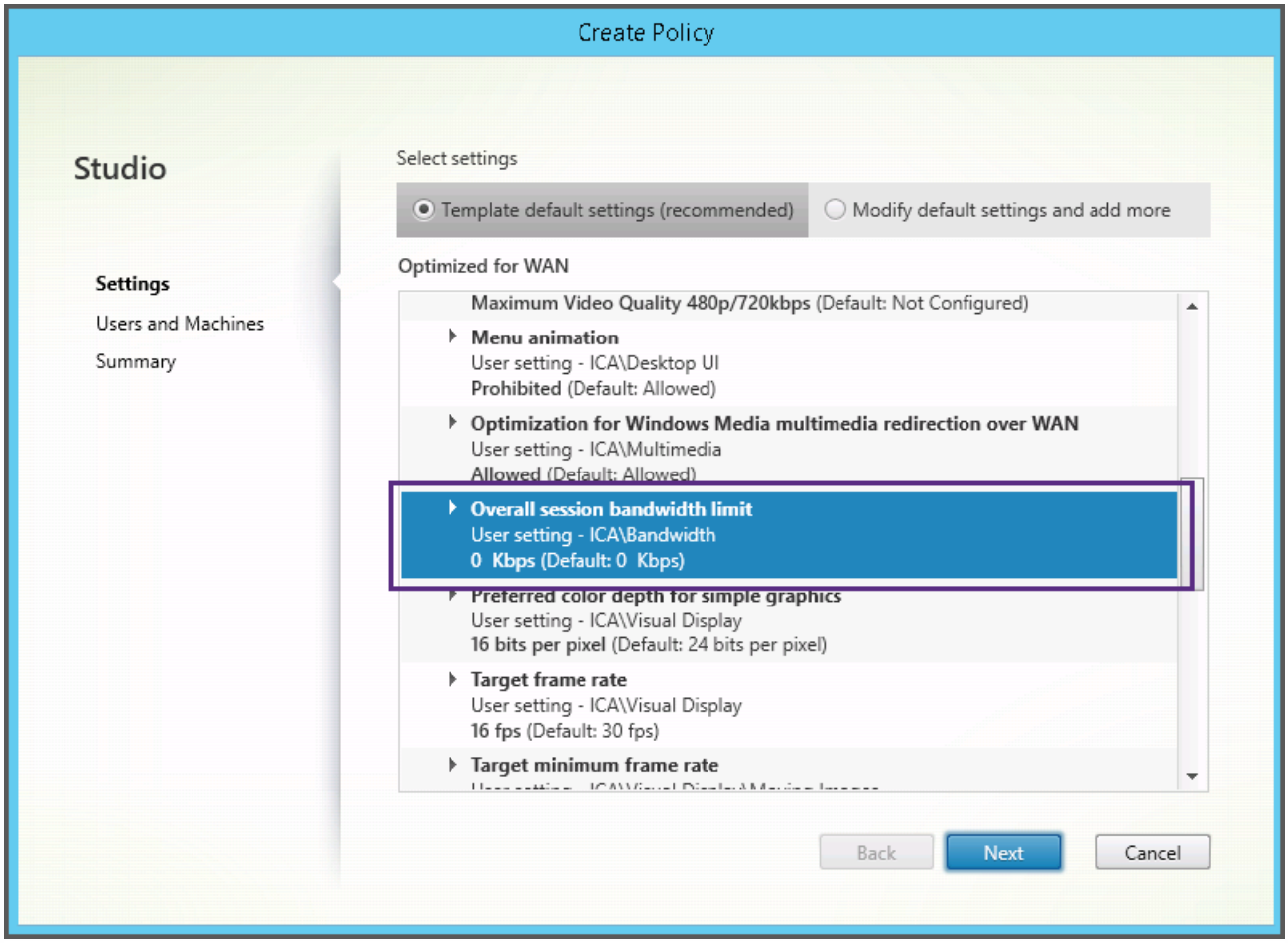
有关使用模板创建策略时的注意事项，请参阅 CTX202330。

以下策略模板可用：

- **超高清用户体验**。此模板强制实施尽可能实现最佳用户体验的默认设置。在按照优先级顺序处理多个策略的场景中使用此模板。
- **高服务器可扩展性**。应用此模板可节约服务器资源。此模板可以平衡用户体验和服务器可扩展性。它可以提供良好的用户体验，同时增加单个服务器上可以托管的用户数。此模板不使用视频编解码器压缩图像，并阻止服务器端进行多媒体呈现。
- **高服务器可扩展性-旧版操作系统**。此高服务器可扩展性模板仅适用于运行 Windows Server 2008 R2 或 Windows 7 及更早版本的 VDA。此模板依靠对这些操作系统较为有效的旧图形模式。
- **针对 NetScaler SD-WAN 优化。**对从具有 NetScaler SD-WAN 的分支机构工作的用户应用此模板以优化 XenDesktop 的交付。（NetScaler SD-WAN 是 CloudBridge 的新名称）。
- **WAN 优化**。此模板旨在用于满足以下条件的任务型工作人员：位于使用共享 WAN 连接的分支结构或采用低带宽连接的远程位置，访问具有简单图形用户界面且包含很少多媒体内容的应用程序。此模板通过降低视频回退体验和某些服务器可扩展性实现最佳带宽效率。
- **WAN 优化-旧版操作系统**。此 WAN 优化模板仅适用于运行 Windows Server 2008 R2 或 Windows 7 及更早版本的 VDA。此模板依靠对这些操作系统较为有效的旧图形模式。
- **安全性与控制**。在低风险容忍的环境中使用此模板，可尽量减少 XenApp 和 XenDesktop 中默认启用的功能。此模板中包含的设置可禁止在用户设备上访问打印、剪贴板、外围设备、驱动器映射、端口重定向以及 Flash 加速。应用此模板可能会占用更多带宽并降低每个服务器的用户密度。

虽然我们建议您使用内置 Citrix 模板及其默认设置，但是您会发现一些没有特定建议值的设置（例如，“WAN 优化”模板中包含的“总会话带宽限制”）。在这种情况下，模板将显示此设置，以便管理员了解此设置可能适用的情况。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



如果正在使用 XenApp 和 XenDesktop 7.6 FP3 之前的部署版本（策略管理和 VDA），但需要使用“高服务器可扩展性”和“WAN 优化”模板，请使用这些模版的旧版操作系统版本（如果这些版本适用）。

> **注意**
>
> 内置模板由 Citrix 创建，并由 Citrix 负责更新。您无法修改或删除这些模板。

基于模板创建新模板：

1. 在 Studio 导航窗格中选择**策略**。
2. 选择**模板**选项卡，然后选择创建新模板时要基于的模板。
3. 在“操作”窗格中选择**创建模板**。
4. 选择并配置要包含在新模板中的策略设置。删除不应包含的所有现有设置。为新模板输入一个名称。

单击**完成**后，新模板显示在**模板**选项卡中。

基于策略创建新模板：

1. 在 Studio 导航窗格中选择**策略**。
2. 选择**策略**选项卡，然后选择创建新模板时要基于的策略。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. 在“操作”窗格中选择**另存为模板**。
4. 选择并配置要包含在模板中的任何新策略设置。删除不应包含的所有现有设置。输入模板的名称和说明，然后单击**完成**。

导入模板：

1. 在 Studio 导航窗格中选择**策略**。
2. 选择**模板**选项卡，然后选择**导入模板**。
3. 选择要导入的模板文件，然后单击**打开**。如果您要导入的模板与某个现有模板同名，则可以选择覆盖现有模板，或使用自动生成的其他名称保存该模板。

导出模板：

1. 在 Studio 导航窗格中选择**策略**。
2. 选择**模板**选项卡，然后选择**导出模板**。
3. 选择模板的保存位置，然后单击**保存**。

将在指定位置创建一个 .gpt 文件。

从组策略编辑器中，展开 计算机配置或 用户配置。展开 策略节点，然后选择 Citrix 策略。在下面选择合适的操作。

任务	说明
基于现有策略创建新模板	在“策略”选项卡上，选择策略，然后选择 操作 > 另存为模板。
基于现有模板创建新策略	在“模板”选项卡上，选择模板，然后单击 新建策略。
基于现有模板创建新模板	在“模板”选项卡上，选择模板，然后单击 新建模板。
导入模板	在模板选项卡上，选择 操作 > 导入。
导出模板	在模板选项卡上，选择 操作 > 导出。
查看模板设置	在“模板”选项卡上，选择模板，然后单击“设置”选项卡。
查看模板属性的摘要	在“模板”选项卡上，选择模板，然后单击“属性”选项卡。
查看模板必备项	在“模板”选项卡上，选择模板，然后单击“必备项”选项卡。

策略模板存储在安装策略管理软件包的计算机上。此计算机为 Delivery Controller 计算机或组策略对象管理计算机，而不是 XenApp 和 XenDesktop 站点的数据库。这意味着策略模板文件由 Windows 管理权限（而非站点的委派管理角色和作用域）控制。

因此，站点中具有只读权限的管理员可以创建新模板。但是，因为模板是本地文件，实际上并未对环境进行任何更改。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

自定义模板仅对创建了这些模板的用户帐户可见，并且存储在用户的 Windows 配置文件中。要进一步显示自定义模板，请基于该模板创建一条策略，或将其导出到共享位置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

创建策略

Dec 05, 2017

创建策略前，确定将受此策略影响的用户或设备组。您可能希望基于用户工作职责、连接类型、用户设备或地理位置来创建策略。也可以使用用于 Windows Active Directory 组策略的条件。

如果已创建应用于某个组的策略，请考虑编辑该策略并配置适当的设置，而不是创建另一个策略。请避免单纯为了启用特定设置或拒绝将该策略应用到特定用户而创建新策略。

创建新策略时，可以将策略模板中的设置作为基础并根据需要自定义设置，也可以不使用模板，然后添加所需的全部设置。

在 Citrix Studio 中，除非明确选中了“启用策略”复选框，否则创建的新策略会设置为“已禁用”。

策略设置的状态可以是已启用、已禁用或未配置。 默认情况下，策略设置的状态是未配置，表示未将其添加到策略。 仅在将设置添加到策略后才应用这些设置。

某些策略设置可处于以下状态之一：

- 允许或禁止，允许或阻止由设置控制的操作。 在某些情况下，会允许或阻止用户在会话中管理设置的操作。 例如， 如果 菜单 动画设置为“允许”，则用户可以在其客户端环境中 控制菜单动画。
- 启用或禁用，打开或关闭设置。 如果禁用某个设置，则在等级较低的策略中都不会启用该设置。

此外，某些设置还可控制相关设置的效果。 例如， 客户端驱动器重定向控制是否允许用户访问其设备上的驱动器。 要允许用户访问其网络驱动器，必须同时将此设置和 客户端网络驱动器设置添加到策略中。 如果 客户端驱动器重定向设置处于禁用状态，用户将无法访问其网络驱动器，即使 客户端网络驱动器设置处于启用状态也是如此。

通常，影响计算机的策略设置更改会在虚拟桌面重新启动时或用户登录时生效。 影响用户的策略设置更改会在用户下次登录时生效。 如果您使用的是 Active Directory，策略设置会在 Active Directory 每隔 90 分钟定期重新评估策略时更新，并在虚拟桌面重新启动时或用户登录时应用。

对于某些策略设置，可在将设置添加到策略时输入或选择一个值。 可以通过选择 使用默认值限制对设置进行配置；这样可禁止对设置进行配置，在应用策略时仅允许使用设置的默认值，不考虑在选择 使用默认值之前输入的值。

最佳做法：

- 将策略分配给组，而非单个用户。 如果将策略分配给组，则将用户添加到组或从组中删除用户时，分配会自动更新。
- 请勿启用“远程桌面会话主机配置”中的冲突或重叠设置。 在某些情况下，“远程桌面会话主机配置”可提供与 Citrix 策略设置相似的功能。 如有可能，请将所有设置的状态保持一致（已启用或已禁用），以便轻松进行故障排除。
- 禁用未使用的策略。 未添加任何设置的策略会带来不必要的处理过程。

创建策略时，可以将该策略分配给某些用户和计算机对象；该策略会根据特定条件或规则应用于连接。一般情况下，可以根据条件组合向策略添加任意数量的分配。如果指定不进行分配，策略将应用于所有连接。

下表列出了可用的分配：

分配名称	应用策略的根据
访问控制	连接客户端所依据的访问控制条件 • 连接类型 - 将策略应用到使用 NetScaler Gateway 建立的连接还是不使用 NetScaler Gateway 建立

© 1999-2017 Citrix Systems, Inc. All rights reserved.

分配名称	应用策略的根据
	的连接。 ● NetScaler Gateway 场名称 - NetScaler Gateway 虚拟服务器的名称。 ● 访问条件 - 要使用的端点分析策略或会话策略的名称。
Citrix CloudBridge	是否通过 Citrix CloudBridge 启动用户会话。 注意：您只能向策略中添加一个 Citrix CloudBridge 分配。
客户端 IP 地址	用于连接到会话的用户设备的 IP 地址。 ● IPv4 示例：12.0.0.0、12.0.0.*、12.0.0.1-12.0.0.70、12.0.0.1/24 ● IPv6 示例：2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54
客户端名称	用户设备的名称 ● 精确匹配：ClientABCName ● 使用通配符：Client*Name
交付组	交付组成员身份。
交付组类型	桌面或应用程序的类型：专用桌面、共享桌面、专用应用程序或共享应用程序。
组织单位(OU)	组织单位。
标记	标记。 **注意**：为确保在使用标记时正确应用策略，请安装 CTX142439 中的修补程序。
用户或组	用户或组名称。

用户登录时，系统会确定与连接的分配相匹配的所有策略。这些策略按优先级排序，并对任意设置的多个实例进行比较。根据策略的优先级应用每个设置。任何已禁用的策略设置都优先于级别较低的已启用规则。未配置的策略设置会被忽略。

重要：如果使用组策略管理控制台同时配置 Active Directory 和 Citrix 策略，可能无法按预期应用分配和设置。有关详细信息，请参阅 CTX127461。
默认情况下，提供名为“未过滤”的策略。

- 如果使用 Studio 来管理 Citrix 策略，添加到“未过滤”策略的设置将应用到站点中的所有服务器、桌面和连接。
- 如果使用本地组策略编辑器管理 Citrix 策略，添加到“未过滤”策略的设置将应用到包含该策略的组策略对象 (GPO) 作用域内的所有站点和连接。例如，Sales 销售团队包含名为 Sales-US 的组策略对象，该组策略对象包含美国销售团队的所有成员。该 Sales-US GPO 是使用包含多项用户策略设置的“未过滤”策略进行配置的。美国的销售经理登录到站点时，“未过滤”策略中的设置会自动应用到会话，因为该用户属于 Sales-US GPO 的成员。

分配的模式决定策略是否仅应用到符合所有分配条件的连接。如果将模式设置为允许（默认设置），策略将仅应用到符合分配条件的连接。如果将模式设置为拒绝，将在连接不符合分配条件时应用策略。下例说明了存在多个分配时分配模式对 Citrix 策略的影响。

- **示例：模式不同但类型相同的分配** - 如果策略中包含两个类型相同的分配，其中一个设置为允许，一个设置为拒绝，假设连

© 1999-2017 Citrix Systems, Inc. All rights reserved.

接同时满足这两个分配，则设置为拒绝的分配优先级较高。例如：
策略 1 包含以下分配：
- 分配 A 指定销售组，且模式设置为允许
- 分配 B 指定销售经理的帐户，且模式设置为拒绝

由于分配 B 的模式设置为拒绝，因此即使销售经理属于销售组，在他登录到站点时也不会应用该策略。

- **示例：模式相同但类型不同的分配** - 在包含两个或更多个类型不同但模式设置为允许的策略中，连接必须至少满足每种类型的一个分配，才能应用该策略。例如：
  策略 2 包含以下分配：
  - 分配 C 为用户分配，用于指定销售组，且模式设置为允许
  - 分配 D 为客户端 IP 地址分配，用于指定 10.8.169.*（企业网络），且模式设置为允许

  销售经理从办公室登录到站点时，会应用该策略，因为连接同时满足这两个分配。

  策略 3 包含以下分配：
  - 分配 E 为用户分配，用于指定销售组，且模式设置为允许
  - 分配 F 为访问控制分配，用于指定 NetScaler Gateway 连接条件，且模式设置为允许

  销售经理从办公室登录到站点时，不会应用该策略，因为连接不满足分配 F。

1. 在 Studio 导航窗格中选择 策略。
2. 选择“模板”选项卡，然后选择一个模板。
3. 在“操作”窗格中选择 基于模板创建策略。
4. 默认情况下， 新策略使用模板中的所有默认设置（选中使用模板默认 设置单选按钮）。如果要更改设置，请选中 修改默认值并添加更多设置单选按钮，然后添加或删除设置。
5. 通过选择以下选项之一指定应用策略的方式：
   - 分配给所选用户和计算机对象并选择要应用策略的用户和计算机对象。
   - 分配给站点中的所有对象以将策略应用到站点中的所有用户和计算机对象。
6. 输入策略的名称（或接收默认名称）；考虑根据受影响的用户或对象来命名策略，例如，Accounting Department 或 Remote Users。 提供说明（可选）。
   策略 在默认情况下启用，您可以将其禁用。启用策略将使策略立即 应用到登录的用户。禁用策略可阻止 应用策略。如果您过后需要设定策略的优先级或添加设置， 请考虑禁用策略，直至准备好应用此策略。

1. 在 Studio 导航窗格中选择 策略。
2. 选择 策略选项卡。
3. 在“操作”窗格中选择 创建策略。
4. 添加并配置策略设置。
5. 通过选择以下选项之一指定应用策略的方式：
   - 分配给所选用户和计算机对象并选择要应用策略的用户和计算机对象。
   - 分配给站点中的所有对象以将策略应用到站点中的所有用户和计算机对象。
6. 输入策略的名称（或接收默认名称）；考虑根据受影响的用户或对象来命名策略，例如，Accounting Department 或 Remote Users。 提供说明（可选）。
   策略 在默认情况下启用，您可以将其禁用。启用策略将使策略立即 应用到登录的用户。禁用策略可阻止 应用策略。如果您过后需要设定策略的优先级或添加设置， 请考虑禁用策略，直至准备好应用此策略。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

从组策略编辑器中，展开 计算机配置或 用户配置。 展开 策略节点，然后选择 Citrix 策略。在下面选择合适的操作。

任务	说明
创建新策略	在“策略”选项卡上，单击 新建。
编辑现有策略	在“策略”选项卡上，选择策略，然后单击 编辑。
更改现有策略的优先级	在“策略”选项卡上，选择策略，然后单击 提高或 降低。
查看策略的摘要信息	在“策略”选项卡上，选择策略，然后单击“摘要”选项卡。
查看和修改策略设置	在“策略”选项卡上，选择策略，然后单击“设置”选项卡。
查看和修改策略过滤器	在“策略”选项卡上，选择策略，然后单击“过滤器”选项卡。
启用或禁用策略	在“策略”选项卡上，选择策略，然后选择 操作 > 启用或 操作 > 禁用。
基于现有模板创建新策略	在“模板”选项卡上，选择模板，然后单击 新建策略。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

对策略进行比较、设定优先级、建模和故障排除

Dec 05, 2017

您可以使用多个策略，以根据用户的工作职责、地理位置或连接类型来自定义您的环境，使其满足用户的需求。例如，出于安全考虑，您可能需要对经常使用高度敏感数据的用户组设置限制。您可以创建一个这样的策略：它可以阻止用户在其本地客户端驱动器上保存敏感文件。但是，如果用户组中的某些人员确实需要访问其本地驱动器，则可以仅针对此类用户创建另一个策略。然后，您可以对这两个策略分级或设定两个策略的优先级，以控制哪个策略的优先顺序较高。

使用多个策略时，需要确定如何设定策略的优先级、如何创建例外情况，以及如何在策略冲突时查看有效的策略。

通常情况下，策略会覆盖针对整个站点、特定 Delivery Controller 或在用户设备上配置的相似设置。此原则的唯一例外情况是安全性。环境中的最高加密设置（包含操作系统及限制性最强的重影设置）通常会覆盖其他设置和策略。

Citrix 策略会与您在操作系统中设置的策略进行交互。在 Citrix 环境中，Citrix 设置会覆盖在 Active Directory 策略中配置的相同设置或使用远程桌面会话主机配置的相同设置。这包括与典型的远程桌面协议 (RDP) 客户端连接设置相关的设置（例如桌面墙纸、菜单动画以及拖动时查看窗口内容）。对于某些策略设置（例如安全 ICA），策略中的设置必须与操作系统中的设置相匹配。如果在其他位置设置了优先级更高的加密级别，则会覆盖在策略中或在交付应用程序和桌面时指定的安全 ICA 策略设置。

例如，您在创建交付组时指定的加密设置应该与环境中指定的加密设置具有相同的级别。

注意：在双跃点场景的第二个跃点中，当桌面操作系统 VDA 连接到服务器操作系统 VDA 时，Citrix 策略将像在用户设备上一样在桌面操作系统 VDA 上发挥作用。例如，如果策略设置为在用户设备上缓存图像，则为双跃点场景中的第二个跃点缓存的图像将在桌面操作系统 VDA 计算机上缓存。

您可以将某个策略或模板中的设置与其他策略或模板中的设置进行比较。例如，您可能需要验证设置值以确保遵从最佳做法。您可能还希望将策略或模板中的设置与 Citrix 提供的默认设置进行比较。

1. 在 Studio 导航窗格中选择策略。
2. 单击“比较”选项卡，然后单击选择。
3. 选择要比较的策略或模板。要同时比较默认值，请选中与默认设置进行比较复选框。
4. 单击比较后，已配置的设置按列显示。
5. 要查看所有设置，请选择显示所有设置。要返回到默认视图，请选择显示常规设置。

通过设定策略的优先级，您可以定义包含冲突设置时策略的优先级。 用户登录时，系统会确定与连接的分配相匹配的所有策略。 这些策略按优先级排序，并对任意设置的多个实例进行比较。 根据策略的优先级应用每个设置。

可以在 Studio 中为策略分配不同的优先级编号，以设定其优先级。 默认情况下，新策略的优先级最低。 如果策略设置相冲突，则优先级较高的策略（优先级编号 1 为最高）会覆盖优先级较低的策略。 设置会根据优先级和设置情况（例如设置处于禁用还是启用状态）进行合并。 任何已禁用的设置都会覆盖等级较低的已启用设置。未配置的策略设置会被忽略，而且不会覆盖等级较低的设置的设置。

1. 在 Studio 导航窗格中选择 策略。确保选择“策略”选项卡。
2. 选择一个策略。
3. 在“操作”窗格中，选择 较低 优先级或 较高 优先级。

在为用户组、用户设备或计算机创建策略时，您可能会发现需要针对某些策略设置为组的部分成员创建例外。 可以通过以下方式创建例外情况：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 仅为需要使用例外情况的组成员创建策略，然后将该策略的优先级设置为高于适用于整个组的策略
- 为添加到策略的分配使用 拒绝模式

如果将分配设置为 拒绝模式，则只会对不符合分配条件的连接应用策略。 例如，某个策略包含以下分配：
- 分配 A 为客户端 IP 地址分配，指定范围 208.77.88.*，且模式设置为 允许
- 分配 B 为用户分配，指定特定的用户帐户，且模式设置为 拒绝

该策略适用于使用分配 A 中指定范围内的 IP 地址登录到站点的所有用户。但是，该策略不适用于使用分配 B 中指定的用户帐户登录到站点的用户，即使为该用户的计算机分配的 IP 地址在分配 A 中指定的范围内。

由于会应用多个策略，因此有时连接不会按预期响应。 如果优先级较高的策略也应用于某个连接，该策略将覆盖您在原始策略中配置的设置。 可以通过计算 策略的结果集来确定如何合并连接的最终策略设置。

可以通过以下方式计算策略的结果集：
- 使用 Citrix 组策略建模向导模拟连接方案并确定可以如何应用 Citrix 策略。 您可以为连接方案指定条件，例如域控制器、用户、Citrix 策略分配证据值以及慢速网络连接等模拟环境设置。 该向导生成的报告列出在连接方案中可能有效的 Citrix 策略。 如果您以域用户身份登录到控制器，该向导将使用站点策略设置和 Active Directory 组策略对象 (GPO) 计算策略的结果集。
- 使用组策略结果为给定用户和控制器生成一份报告，用于描述有效的 Citrix 策略。 组策略结果工具可帮助您评估环境中 GPO 的当前状态，并可生成一份报告，用于描述当前如何将这些对象（包括 Citrix 策略）应用到特定的用户和控制器。

可以从 Studio 的“操作”窗格启动 Citrix 组策略建模向导。 可以从 Windows 中的组策略管理控制台启动这两种工具。

如果从组策略管理控制台运行 Citrix 组策略建模向导或组策略结果工具，则策略的结果集内将不包含使用 Studio 创建的站点策略设置。

为确保得到最全面的策略的结果集，Citrix 建议从 Studio 启动 Citrix 组策略建模向导，除非您仅使用组策略管理控制台创建策略。

使用下列任意一种方法打开 Citrix 组策略建模向导：
- 在 Studio 导航窗格中选择 策略，选择 “建模”选项卡，然后在“操作”窗格中选择 启动 建模向导。
- 启动组 策略管理控制台 (gpmc.msc)，在树状窗格中的 Citrix 组策略建模上单击鼠标右键，然后选择 Citrix 组策略建模向导。

按照向导中的说明，选择要在模拟中使用的域控制器、用户、计算机、环境设置以及 Citrix 分配条件。 单击 完成后，向导会生成建模结果报告。 在 Studio 中，报告显示在中间窗格中的“建模”选项卡下方。

要查看报告，请选择 查看建模报告。

用户、IP 地址及其他分配对象可以具有多个同时应用的策略。 如果策略未按预期发挥作用，这可能会导致出现冲突。 运行 Citrix 组策略建模向导或组策略结果工具时，您可能会发现没有任何策略应用到用户连接。 如果发生这种情况，在满足策略评估条件的前提下连接到应用程序和桌面的用户将不受任何策略设置的影响。 在以下情况下会发生上述问题：
- 所有策略包含的分配都不满足策略评估条件。
- 满足分配条件的策略均未配置任何设置。
- 满足分配条件的策略处于禁用状态。

如果要对满足指定条件的连接应用策略设置，请确保：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 要应用到这些连接的策略已启用。
- 要应用的策略已配置合适的设置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

默认策略设置

Dec 05, 2017

下表列出了策略设置、其默认值以及设置应用到的 Virtual Delivery Agent (VDA) 版本。

名称	默认设置	VDA
客户端剪贴板重定向	允许	VDA 的所有版本
桌面启动	禁止	VDA for Server OS 7 至当前版本
EDT	关	VDA 7.13 请参阅自适应传输。
ICA 侦听器连接超时	120000 毫秒	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7 至当前版本
ICA 侦听器端口号	1494	VDA 的所有版本
在客户端连接期间启动非发布程序	禁止	VDA for Server OS 7 至当前版本
客户端剪贴板写入允许的格式	未指定格式	VDA 7.6 至当前版本
限制客户端剪贴板写入	禁止	VDA 7.6 至当前版本
限制会话剪贴板写入	禁止	VDA 7.6 至当前版本
会话剪贴板写入允许的格式	未指定格式	VDA 7.6 至当前版本

名称	默认设置	VDA
Flash 视频回退预防	未配置	VDA 7.6 FP3 至当前版本

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名称	默认设置	VDA
Flash 视频回退预防错误 *.swf		VDA 7.6 FP3 至当前版本

名称	默认设置	VDA
音频即插即用	允许	VDA for Server OS 7 至当前版本
音频质量	高 - 高清晰度音频	VDA 的所有版本
客户端音频重定向	允许	VDA 的所有版本
客户端麦克风重定向	允许	VDA 的所有版本

名称	默认设置	VDA
客户端自动重新连接	允许	VDA 的所有版本
客户端自动重新连接身份验证	不要求身份验证	VDA 的所有版本
客户端自动重新连接日志记录	不记录自动重新连接事件	VDA 的所有版本

名称	默认设置	VDA
音频重定向带宽限制	0 Kbps	VDA 的所有版本
音频重定向带宽限制百分比	0	VDA 的所有版本
客户端 USB 设备重定向带宽限制	0 Kbps	VDA 5.5、5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
客户端 USB 设备重定向带宽限制百分比	0	VDA 5.5、5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
剪贴板重定向带宽限制	0 Kbps	VDA 的所有版本
剪贴板重定向带宽限制百分比	0	VDA 的所有版本

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名称	默认设置	VDA
COM 端口重定向带宽限制	0 Kbps	VDA 的所有版本；对于 VDA 7.0 至 7.8 版本，使用注册表配置此设置
COM 端口重定向带宽限制百分比	0	VDA 的所有版本；对于 VDA 7.0 至 7.8 版本，使用注册表配置此设置
文件重定向带宽限制	0 Kbps	VDA 的所有版本
文件重定向带宽限制百分比	0	VDA 的所有版本
HDX MediaStream 多媒体加速带宽限制	0 Kbps	VDA 5.5、5.6 FP1、VDA for Server OS 7 和 VDA for Desktop OS 7 至最新的 VDA for Server OS 和 VDA for Desktop OS
HDX MediaStream 多媒体加速带宽限制百分比	0	VDA 5.5、5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
LPT 端口重定向带宽限制	0 Kbps	VDA 的所有版本；对于 VDA 7.0 至 7.8 版本，使用注册表配置此设置
LPT 端口重定向带宽限制百分比	0	VDA 的所有版本；对于 VDA 7.0 至 7.8 版本，使用注册表配置此设置
总会话带宽限制	0 Kbps	VDA 的所有版本
打印机重定向带宽限制	0 Kbps	VDA 的所有版本
打印机重定向带宽限制百分比	0	VDA 的所有版本
TWAIN 设备重定向带宽限制	0 Kbps	VDA 5.5、5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
TWAIN 设备重定向带宽限制百分比	0	VDA 5.5、5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本

名称	默认设置	VDA
允许应用程序使用客户端设备的物理位置	禁止	VDA 5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名称	默认设置	VDA
桌面组合重定向	已禁用（7.6 FP3 至当前版本） 已启用（5.6 至 7.6 FP2）	VDA 5.6、VDA for Desktop OS 7 至当前版本
桌面组合重定向图形质量	中	VDA 5.6、VDA for Desktop OS 7 至当前版本
桌面墙纸	允许	VDA 的所有版本
菜单动画	允许	VDA 的所有版本
拖动时查看窗口内容	允许	VDA 的所有版本

名称	默认设置	VDA
ICA 往返行程计算	已启用	VDA 的所有版本
ICA 往返行程计算间隔	15 秒	VDA 的所有版本
空闲连接的 ICA 往返行程计算	已禁用	VDA 的所有版本

名称	默认设置	VDA
增强的桌面体验	允许	VDA for Server OS 7 至当前版本

名称	默认设置	VDA
自动连接客户端驱动器	允许	VDA 的所有版本
客户端驱动器重定向	允许	VDA 的所有版本
客户端固定驱动器	允许	VDA 的所有版本

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名称	默认设置	VDA
客户端软盘驱动器	允许	VDA 的所有版本
客户端网络驱动器	允许	VDA 的所有版本
客户端光盘驱动器	允许	VDA 的所有版本
客户端可移动驱动器	允许	VDA 的所有版本
主机到客户端重定向	已禁用	VDA for Server OS 7 至当前版本
保留客户端驱动器盘符	已禁用	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7 至当前版本
只读客户端驱动器访问	已禁用	VDA 5.5、5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
特殊文件夹重定向	允许	仅限 Web Interface 部署；VDA for Server OS 7 至当前版本
使用异步写入	已禁用	VDA 的所有版本

名称	默认设置	VDA
允许执行视觉无损压缩	已禁用	VDA 7.6 至当前版本
显示内存限制	65536 Kb	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7 至当前版本
显示模式降级首选项	首先降低颜色深度	VDA 的所有版本
动态窗口预览	已启用	VDA 5.5、5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
图像缓存	已启用	VDA 5.5、5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
旧图形模式	已禁用	VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本

© 1999-2017 Citrix Systems, Inc. All rights reserved.

允许的最大颜色深度	32 位/像素	VDA 的所有版本
在显示模式降级时通知用户	已禁用	VDA for Server OS 7 至当前版本
排队与丢弃	已启用	VDA 的所有版本
使用视频编解码器进行压缩	偏好时使用视频编解码器	VDA 7.6 FP3 至当前版本
使用硬件编码进行视频编解码	已启用	VDA 7.11 至当前版本

名称	默认设置	VDA
永久缓存阈值	3000000 bps	VDA for Server OS 7 至当前版本

名称	默认设置	VDA
Framehawk 显示通道	已禁用	VDA 7.6 FP2 至当前版本
Framehawk 显示通道端口范围	3224,3324	VDA 7.6 FP2 至当前版本

名称	默认设置	VDA
ICA 保持活动状态超时	60 秒	VDA 的所有版本
ICA 保持活动状态	不发送 ICA 保持活动状态消息	VDA 的所有版本

名称	默认设置	VDA
允许本地应用程序访问	禁止	VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
URL 重定向黑名单	未指定任何站点	VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名称	默认设置	VDA
URL 重定向白名单	未指定任何站点	VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本

名称	默认设置	VDA
自动显示键盘	禁止	VDA 5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
启动触控优化桌面	允许	VDA 5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本 此设置已禁用，不适用于 Windows 10 和 Windows Server 2016 计算机。
远程控制组合框	禁止	VDA 5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本

名称	默认设置	VDA
HTML5 视频重定向	禁止	VDA 7.12 至当前版本
限制视频质量	未配置	VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
多媒体会议	允许	VDA 的所有版本
优化 WAN 中的 Windows Media 多媒体重定向	允许	VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
使用 GPU 以优化 WAN 中的 Windows Media 多媒体重定向	禁止	VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
Windows 媒体回退预防	未配置	VDA 7.6 FP3 至当前版本
Windows Media 客户端内容提取	允许	VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
Windows Media 重定向	允许	VDA 的所有版本

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Windows Media 重定向缓冲区大小	5 秒	VDA 5、5.5、5.6 FP1
Windows Media 重定向缓冲区大小的使用	已禁用	VDA 5、5.5、5.6 FP1

名称	默认设置	VDA
通过 UDP 传输音频	允许	VDA for Server OS 7 至当前版本
音频 UDP 端口范围	16500、16509	VDA 5.5、5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
多端口策略	主端口 (2598) 拥有“高”优先级	VDA 5.5、5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
多流计算机设置	已禁用	VDA 5.5、5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
多流用户设置	已禁用	VDA 5.5、5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本

名称	默认设置	VDA
自动连接客户端 COM 端口	已禁用	VDA 的所有版本；对于 VDA 7.0 至 7.8 版本，使用注册表配置此设置
自动连接客户端 LPT 端口	已禁用	VDA 的所有版本；对于 VDA 7.0 至 7.8 版本，使用注册表配置此设置
客户端 COM 端口重定向	禁止	VDA 的所有版本；对于 VDA 7.0 至 7.8 版本，使用注册表配置此设置
客户端 LPT 端口重定向	禁止	VDA 的所有版本；对于 VDA 7.0 至 7.8 版本，使用注册表配置此设置

名称	默认设置	VDA
客户端打印机重定向	允许	VDA 的所有版本
默认打印机	将默认打印机设置为客户端的主打印机	VDA 的所有版本
打印机分配	用户当前使用的打印机用作会话的默认打印机	VDA 的所有版本

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名称	默认设置	VDA
打印机自动创建事件日志首选项	记录错误和警告	VDA 的所有版本
会话打印机	未指定任何打印机	VDA 的所有版本
等待创建打印机(桌面)	已禁用	VDA 的所有版本

名称	默认设置	VDA
自动创建客户端打印机	自动创建所有客户端打印机	VDA 的所有版本
自动创建一般通用打印机	已禁用	VDA 的所有版本
客户端打印机名称	标准打印机名称	VDA 的所有版本
直接连接到打印服务器	已启用	VDA 的所有版本
打印机驱动程序映射和兼容性	未指定任何规则	VDA 的所有版本
打印机属性保留	仅当未保存在客户端时才保留在配置文件中	VDA 的所有版本
保留和恢复的客户端打印机	允许	VDA 5、5.5、5.6 FP1

名称	默认设置	VDA
自动安装现成的打印机驱动程序	已启用	VDA 的所有版本
通用驱动程序首选项	EMF、XPS、PCL5c、PCL4、PS	VDA 的所有版本
通用打印驱动程序用法	仅当请求的驱动程序不可用时才使用通用打印	VDA 的所有版本

名称	默认设置	VDA
启用通用打印服务器	已禁用	VDA 的所有版本

© 1999-2017 Citrix Systems, Inc. All rights reserved.

通用打印服务器打印数据流(CGP)端口	7229	VDA 的所有版本
通用打印服务器打印流输入带宽限制(kbps)	0	VDA 的所有版本
通用打印服务器 Web 服务(HTTP/SOAP)端口	8080	VDA 的所有版本
用于负载平衡的通用打印服务器		VDA 7.9 版至最新版本
通用打印服务器停止运行阈值	180（秒）	VDA 7.9 版至最新版本

名称	默认 设置	VDA
通用打印 EMF 处理模式	直接 后台打印到打印机	VDA 的所有 版本
通用打印图像压缩限制	最佳 质量(无损压缩)	VDA 的所有 版本
通用打印优化默认值	图像 压缩 • 所需图像质量 = 标准质量 • 启用超级压缩 = False 图像 和字体缓存 • 允许缓存嵌入的图像 = True • 允许缓存嵌入的字体 = True 允许 非管理员修改这些设置 = False	VDA 的所有 版本
通用打印预览首选项	不 对自动创建的打印机或一般通用打印机使用打印预览	VDA 的所有 版本
通用打印的打印质量限制	无限制	VDA 的所有 版本

名称	默认设置	VDA
SecureICA 最低加密等级	基本	VDA for Server OS 7 至当前版本

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名称	默认设置	VDA
服务器空闲计时器间隔	0 毫秒	VDA for Server OS 7 至当前版本

名称	默认设置	VDA
断开会话计时器	已禁用	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7 至当前版本
断开会话计时器间隔	1440 分钟	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7 至当前版本
会话连接计时器	已禁用	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7 至当前版本
会话连接计时器间隔	1440 分钟	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7 至当前版本
会话空闲计时器	Enabledf	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7 至当前版本
会话空闲计时器间隔	1440 分钟	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7 至当前版本

名称	默认设置	VDA
会话可靠性连接	允许	VDA 的所有版本
会话可靠性端口号	2598	VDA 的所有版本
会话可靠性超时	180 秒	VDA 的所有版本

名称	默认设置	VDA
估算旧版客户端的本地时间	已启用	VDA for Server OS 7 至当前版本
使用客户端本地时间	使用服务器时区	VDA 的所有版本

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名称	默认设置	VDA
客户端 TWAIN 设备重定向	允许	VDA 5.5、5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
TWAIN 压缩级别	中	VDA 5.5、5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本

名称	默认设置	VDA
客户端 USB 设备优化规则	启用（VDA 7.6 FP3 至当前版本） 禁用（VDA 7.11 至当前版本） 默认情况下，不指定任何规则	VDA 7.6 FP3 至当前版本
客户端 USB 设备重定向	禁止	VDA 的所有版本
客户端 USB 设备重定向规则	未指定任何规则	VDA 的所有版本
客户端 USB 即插即用设备重定向	允许	VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本

名称	默认设置	VDA
简单图形的首选颜色深度	24 位/像素	VDA 7.6 FP3 至当前版本
目标帧速率	30 fps	VDA 的所有版本
视觉质量	中	VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本

名称	默认设置	VDA
最低图像质量	标准	VDA 5.5、5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名称	默认设置	VDA
移动图像压缩	已启用	VDA 5.5、5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
渐进式压缩级别	无	VDA 5.5、5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
渐进式压缩阈值	2147483647 Kbps	VDA 5.5、5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
目标最低帧速率	10 fps	VDA 5.5、5.6 FP1、VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本

名称	默认设置	VDA
额外颜色压缩	已禁用	VDA 的所有版本
额外颜色压缩阈值	8192 Kbps	VDA 的所有版本
超级压缩	已禁用	VDA 的所有版本
有损压缩级别	中	VDA 的所有版本
有损压缩阈值	2147483647 Kbps	VDA 的所有版本

名称	默认设置	VDA
WebSocket 连接	禁止	VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
WebSocket 端口号	8008	VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
WebSocket 可信源服务器列表	通配符 * 用于信任所有 Receiver for Web URL	VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本

名称	默认设置	VDA
并发登录容错	2	VDA for Server OS 7 至当前版本
CPU 使用率	已禁用	VDA for Server OS 7 至当前版本

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名称 排除 CPU 使用率的进程优先级	默认设置 低于正常或低	VDA VDA for Server OS 7 至当前版本
磁盘使用情况	已禁用	VDA for Server OS 7 至当前版本
最大会话数	250	VDA for Server OS 7 至当前版本
内存使用率	已禁用	VDA for Server OS 7 至当前版本
内存使用基础负载	零负载: 768 MB	VDA for Server OS 7 至当前版本

名称	默认设置	VDA
禁用自动配置	已禁用	VDA 的所有版本
遇到问题时注销用户	已禁用	VDA 的所有版本
访问锁定文件的重试次数	5	VDA 的所有版本
注销时处理 Internet Cookie 文件	已禁用	VDA 的所有版本

名称	默认设置	VDA
主动写回	已禁用	VDA 的所有版本
启用 Profile Management	已禁用	VDA 的所有版本
排除的组	已禁用。处理所有用户组的成员。	VDA 的所有版本
脱机配置文件支持	已禁用	VDA 的所有版本
用户存储路径	Windows	VDA 的所有版本
处理本地管理员登录	已禁用	VDA 的所有版本
处理的组	已禁用。处理所有用户组的成员。	VDA 的所有版本

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名称	默认设置	VDA

名称	默认设置	VDA
跨平台设置用户组	已禁用。系统会处理在 处理的组中指定的所有用户组	VDA 的所有版本
启用跨平台设置	已禁用	VDA 的所有版本
跨平台定义路径	已禁用。未指定任何路径。	VDA 的所有版本
跨平台设置存储路径	已禁用。使用 Windows\PM_CM。	VDA 的所有版本
创建跨平台设置的来源	已禁用	VDA 的所有版本

名称	默认设置	VDA
排除列表 - 目录	已禁用。同步用户配置文件中的所有文件夹。	VDA 的所有版本
排除列表 - 文件	已禁用。同步用户配置文件中的所有文件。	VDA 的所有版本

名称	默认设置	VDA
同步的目录	已禁用。仅同步非排除的文件夹。	VDA 的所有版本
同步的文件	已禁用。仅同步非排除的文件。	VDA 的所有版本
镜像的文件夹	已禁用。不镜像任何文件夹。	VDA 的所有版本

名称	默认设置	VDA
授予管理员访问权限	已禁用	VDA 的所有版本
包含域名	已禁用	VDA 的所有版本

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名称	默认设置	VDA
“AppData(漫游)”路径	已禁用。未指定任何位置。	VDA 的所有版本
“AppData (漫游)”的重定向设置	内容将重定向到在 “AppData (漫游)”路径策略设置中指定的 UNC 路径	VDA 的所有版本

名称	默认设置	VDA
“联系人”路径	已禁用。未指定任何位置。	VDA 的所有版本
“联系人”的重定向设置	内容将重定向到在 “联系人”路径策略设置中指定的 UNC 路径	VDA 的所有版本

名称	默认设置	VDA
“桌面”路径	已禁用。未指定任何位置。	VDA 的所有版本
“桌面”的重定向设置	内容将重定向到在 “桌面”路径策略设置中指定的 UNC 路径	VDA 的所有版本

名称	默认设置	VDA
“文档”路径	已禁用。未指定任何位置。	VDA 的所有版本
“文档”的重定向设置	内容将重定向到在 “文档”路径策略设置中指定的 UNC 路径	VDA 的所有版本

名称	默认设置	VDA
“下载”路径	已禁用。未指定任何位置。	VDA 的所有版本
“下载”的重定向位置	内容将重定向到在 “下载”路径策略设置中指定的 UNC 路径	VDA 的所有版本

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名称	默认设置	VDA
“收藏夹”路径	已禁用。未指定任何位置。	VDA 的所有版本
“收藏夹”的重定向设置	内容将重定向到在 “收藏夹”路径策略设置中指定的 UNC 路径	VDA 的所有版本

名称	默认设置	VDA
“链接”路径	已禁用。未指定任何位置。	VDA 的所有版本
“链接”的重定向设置	内容将重定向到在 “链接”路径策略设置中指定的 UNC 路径	VDA 的所有版本

名称	默认设置	VDA
“音乐”路径	已禁用。未指定任何位置。	VDA 的所有版本
“音乐”的重定向设置	内容将重定向到在 “音乐”路径策略设置中指定的 UNC 路径	VDA 的所有版本

名称	默认设置	VDA
“图片”路径	已禁用。未指定任何位置。	VDA 的所有版本
“图片”的重定向设置	内容将重定向到在 “图片”路径策略设置中指定的 UNC 路径	VDA 的所有版本

名称	默认设置	VDA
“保存的游戏”路径	已禁用。未指定任何位置。	VDA 的所有版本
“保存的游戏”的重定向设置	内容将重定向到在 “保存的游戏”路径策略设置中指定的 UNC 路径	VDA 的所有版本

名称	默认设置	VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名称	默认设置	VDA
“搜索”路径	已禁用。未指定任何位置。	VDA 的所有版本
“搜索”的重定向设置	内容将重定向到在 “搜索”路径策略设置中指定的 UNC 路径	VDA 的所有版本

名称	默认设置	VDA
“开始”菜单路径	已禁用。未指定任何位置。	VDA 的所有版本
“开始”菜单的重定向设置	内容将重定向到在 “开始”菜单路径策略设置中指定的 UNC 路径	VDA 的所有版本

名称	默认设置	VDA
“视频”路径	已禁用。未指定任何位置。	VDA 的所有版本
“视频”的重定向设置	内容将重定向到在 “视频”路径策略设置中指定的 UNC 路径	VDA 的所有版本

名称	默认设置	VDA
Active Directory 操作	已禁用	VDA 的所有版本
常规信息	已禁用	VDA 的所有版本
常见警告	已禁用	VDA 的所有版本
启用日志记录	已禁用	VDA 的所有版本
文件系统操作	已禁用	VDA 的所有版本
文件系统通知	已禁用	VDA 的所有版本
注销	已禁用	VDA 的所有版本
登录	已禁用	VDA 的所有版

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名称	默认设置	VDA 本
日志文件最大大小	1048576	VDA 的所有版本
日志文件路径	已禁用。日志文件保存在默认位置 %SystemRoot%\System32\Logfiles\UserProfileManager。	VDA 的所有版本
个性化用户信息	已禁用	VDA 的所有版本
登录和注销时的策略值	已禁用	VDA 的所有版本
注册表操作	已禁用	VDA 的所有版本
注销时的注册表差异	已禁用	VDA 的所有版本

名称	默认设置	VDA
删除缓存的配置文件之前的延迟	0	VDA 的所有版本
注销时删除本地缓存的配置文件	已禁用	VDA 的所有版本
本地配置文件冲突处理	使用本地配置文件	VDA 的所有版本
迁移现有配置文件	本地配置文件和漫游配置文件	VDA 的所有版本
模板配置文件的路径	已禁用。在用户首次登录的计算机上，会通过默认用户配置文件创建新用户配置文件。	VDA 的所有版本
模板配置文件覆盖本地配置文件	已禁用	VDA 的所有版本
模板配置文件覆盖漫游配置文件	已禁用	VDA 的所有版本
模板配置文件用作所有登录的 Citrix 强制配置文件	已禁用	VDA 的所有版本

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名称	默认设置	VDA
排除列表	已禁用。用户注销时，将处理 HKCU 配置单元中的所有注册表项。	VDA 的所有版本
包含列表	已禁用。用户注销时，将处理 HKCU 配置单元中的所有注册表项。	VDA 的所有版本

名称	默认设置	VDA
总是缓存	已禁用	VDA 的所有版本
总是缓存的大小	0 Mb	VDA 的所有版本
Profile Streaming	已禁用	VDA 的所有版本
流用户配置文件组	已禁用。正常情况下，将处理 OU 内的所有用户配置文件。	VDA 的所有版本
挂起区域锁定文件超时(天数)	1 天	VDA 的所有版本

名称	默认设置	VDA
StoreFront 帐户列表	未指定任何存储	VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本

名称	默认设置	VDA
控制器注册 IPv6 网络掩码	未指定任何网络掩码	VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
控制器注册端口	80	VDA 的所有版本
控制器 SID	未指定任何 SID	VDA 的所有版本
控制器	未指定任何控制器	VDA 的所有版本
启用控制器自动更新	已启用	VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本

© 1999-2017 Citrix Systems, Inc. All rights reserved.

名称	默认设置	VDA
仅使用 IPv6 控制器注册	已禁用	VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
站点 GUID	未指定任何 GUID	VDA 的所有版本

名称	默认设置	VDA
启用无损	已启用	VDA 5.5、5.6 FP1
HDX 3D Pro 质量设置		VDA 5.5、5.6 FP1

名称	默认设置	VDA
启用进程监视	已禁用	VDA 7.11 至当前版本
启用资源监视	已启用	VDA 7.11 至当前版本

名称	默认设置	VDA
虚拟 IP 环回支持	已禁用	VDA 7.6 至当前版本
虚拟 IP 虚拟环回程序列表	无	VDA 7.6 至当前版本

© 1999-2017 Citrix Systems, Inc. All rights reserved.

策略设置参考

Dec 05, 2017

“策略”包含强制执行策略时应用的设置。本节中的说明还会指出要启用某项功能是否需要其他设置或与某项设置相似的其他设置。

以下各表列举了可以在策略内配置的设置。请在左列中查找要完成的任务，然后在右列中找出相应的设置。

对于此任务	使用此策略设置
控制是否允许使用多个音频设备	音频即插即用
控制是否允许从用户设备上的麦克风进行音频输入	客户端麦克风重定向
控制用户设备上的音频质量	音频质量
控制到用户设备上的扬声器的音频映射	客户端音频重定向

要限制用于以下项目的带宽	使用此策略设置
客户端音频映射	音频重定向带宽限制或 音频重定向带宽限制百分比
使用本地剪贴板执行的剪切和粘贴操作	剪贴板重定向带宽限制或 剪贴板重定向带宽限制百分比
会话中对本地客户端驱动器的访问	文件重定向带宽限制或 文件重定向带宽限制百分比
HDX MediaStream 多媒体加速	HDX MediaStream 多媒体加速带宽限制或 HDX MediaStream 多媒体加速带宽限制百分比
客户端会话	总会话带宽限制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

打印	打印机重定向带宽限制或 打印机重定向带宽限制百分比
TWAIN 设备（例如照相机或扫描仪）	TWAIN 设备重定向带宽限制或 TWAIN 设备重定向带宽限制百分比
USB 设备	客户端 USB 设备重定向带宽限制或 客户端 USB 设备重定向带宽限制百分比

对于此任务	**使用此策略设置**
控制是否在用户登录到服务器时连接用户设备上的驱动器	自动连接客户端驱动器
控制服务器与本地剪贴板之间的剪切-粘贴式数据传输	客户端剪贴板重定向
控制从用户设备映射驱动器的方式	客户端驱动器重定向
控制在会话中可否使用用户的本地硬盘驱动器	客户端固定驱动器和 客户端驱动器重定向
控制在会话中可否使用用户的本地软盘驱动器	客户端软盘驱动器和 客户端驱动器重定向
控制在会话中可否使用用户的网络驱动器	客户端网络驱动器和 客户端驱动器重定向
控制在会话中可否使用用户的本地 CD、DVD 或蓝光驱动器	客户端光盘驱动器和 客户端驱动器重定向
控制在会话中可否使用用户的本地可移动驱动器	客户端可移动驱动器和 客户端驱动器重定向
控制在会话中可否使用用户的 TWAIN 设备（如扫描仪和相机），并控制图像数据传输的压缩	客户端 TWAIN 设备重定向 TWAIN 压缩重定向

© 1999-2017 Citrix Systems, Inc. All rights reserved.

控制在会话中可否使用 USB 设备	客户端 USB 设备重定向和 客户端 USB 设备重定向规则
提高通过 WAN 将文件写入和复制到客户端磁盘的速度	使用异步写入

对于此任务	使用此策略设置
控制是否要使用从服务器到用户设备的内容重定向	主机到客户端重定向

对于此任务	使用此策略设置
控制是否在用户会话中使用桌面墙纸	桌面墙纸
拖动窗口时查看窗口内容	拖动时查看窗口内容

对于此任务	使用此策略设置
控制每秒从虚拟桌面发送到用户设备的最大帧数	目标帧速率
控制用户设备上显示的图像的视觉质量	视觉质量
控制是否在会话中呈现 Flash 内容	Flash 默认行为
控制在会话中访问时 Web 站点可否显示 Flash 内容	• Flash 服务器端内容提取 URL 列表 • Flash URL 兼容性列表 • Flash 视频回退预防策略设置 • Flash 视频回退预防错误 *.swf
控制服务器端呈现视频的压缩	• 使用视频编解码器进行压缩 • 使用硬件编码进行视频编解码
控制 HTML5 多媒体 Web 内容向用户的交付	HTML5 视频重定向

© 1999-2017 Citrix Systems, Inc. All rights reserved.

对于此任务	使用此策略设置
为跨多个连接的 ICA 通信指定端口并确定网络优先级	多端口策略
启用对服务器与用户设备之间多流连接的支持	多流（计算机和用户设置）

对于此任务	使用此策略设置
控制在用户设备上创建客户端打印机的行为	自动创建客户端打印机和 客户端打印机重定向
控制打印机属性的存储位置	打印机属性保留
控制客户端还是服务器处理打印请求	直接连接到打印服务器
控制用户可否访问连接到其用户设备的打印机	客户端打印机重定向
控制自动创建客户端和网络打印机时的本机 Windows 驱动程序的安装	自动安装现成的打印机驱动程序
控制何时使用通用打印机驱动程序	通用打印驱动程序用法
根据漫游用户的会话信息选择打印机	默认打印机
平衡通用打印服务器的负载并设置故障转移阈值	用于负载平衡的通用打印服务器 通用打印服务器停止运行阈值

注意：在桌面或应用程序会话中不能使用策略来启用屏幕保护程序。如果用户需要屏幕保护程序，可以在用户设备上实施屏幕保护程序。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ICA 策略设置

Dec 05, 2017

The ICA section contains policy settings related to ICA listener connections and mapping to the clipboard.

This setting allows or prevents data transport over EDT as primary and fallback to TCP.

By default, adaptive transport is disabled (**Off**) and TCP is always used.

1. In Studio, enable the policy setting, HDX adaptive transport (it is disabled by default). We also recommend that you do not enable this feature as a universal policy for all objects in the Site.
2. To enable the policy setting, set the value to **Preferred**, then click **OK**.

    Preferred. Adaptive transport over EDT is used when possible, with fallback to TCP.

    Diagnostic mode. EDT is forced on and fall back to TCP is disabled. We recommend this setting only for troubleshooting.

    Off. TCP is forced on, and EDT is disabled.

For more information, see Adaptive transport.

This setting specifies the wait timeout value in milliseconds for a session to wait for the first application to start. If the start of the application exceeds this time period, the session ends.

You can choose the default time (10000 milliseconds) or specify a number in milliseconds.

This setting allows or prevents the clipboard on the user device being mapped to the clipboard on the server.

By default, clipboard redirection is allowed.

To prevent cut-and-paste data transfer between a session and the local clipboard, select Prohibit. Users can still cut and paste data between applications running in sessions.

After allowing this setting, configure the maximum allowed bandwidth the clipboard can consume in a client connection using the Clipboard redirection bandwidth limit or the Clipboard redirection bandwidth limit percent settings.

When the Restrict client clipboard write setting is Enabled, host clipboard data cannot be shared with the client endpoint. You can use this setting to allow specific data formats to be shared with the client endpoint clipboard. To use this setting, enable it and add the specific formats to be allowed.

The following clipboard formats are system defined:

- CF_TEXT
- CF_BITMAP

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE

The following custom formats are predefined in XenApp and XenDesktop:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- HTML Format

HTML Format is disabled by default. To enable this feature:

- Ensure **Client clipboard redirection** is set to allowed.
- Ensure **Restrict client clipboard write** is set to enabled.
- Add an entry for **HTML Format** (and any other formats you want supported) in **Client clipboard write allowed formats**.

Note: Enabling HTML format clipboard copy support (HTML Format) copies any scripts (if they exist) from the source of the copied content to the destination. Check that you trust the source before proceeding to copy. If you do copy content containing scripts, they are live only if you save the destination file as an HTML file and execute it.

Additional custom formats can be added. The custom format name must match the formats to be registered with the system. Format names are case-sensitive.

This setting does not apply if either Client clipboard redirection or Restrict client clipboard write is set to Prohibited.

This setting allows or prevents non-administrative users in a VDA Direct Access Users group connecting to a session on that VDA using an ICA connection.

By default, non-administrative users cannot connect to these sessions.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

This setting has no effect on non-administrative users in a VDA Direct Access Users group who are using an RDP connection. These users can connect to the VDA whether this setting is enabled or disabled. This setting has no effect on non-administrative users not in a VDA Direct Access Users group. These users cannot connect to the VDA whether this setting is enabled or disabled.

Note: This setting applies only to Virtual Delivery Agents 5.0, 5.5, and 5.6 Feature Pack 1.

This setting specifies the maximum wait time for a connection using the ICA protocol to be completed.

By default, the maximum wait time is 120000 milliseconds, or two minutes.

This setting specifies the TCP/IP port number used by the ICA protocol on the server.

By default, the port number is set to 1494.

Valid port numbers must be in the range of 0-65535 and must not conflict with other well-known port numbers. If you change the port number, restart the server for the new value to take effect. If you change the port number on the server, you must also change it on every Citrix Receiver or plug-in that connects to the server.

This setting specifies whether to allow starting initial applications through RDP on the server.

By default, starting initial applications through RDP on the server is not allowed.

This setting specifies the duration to delay the logoff checker startup. Use this policy to set the time (in seconds) that a client session waits before disconnecting the session.

This setting also increases the time it takes for a user to log off the server.

If this setting is Allowed, host clipboard data cannot be shared with the client endpoint. You can allow specific formats by enabling the Client clipboard write allowed formats setting.

By default, this setting is Prohibited.

When this setting is Allowed, client clipboard data cannot be shared within the user session. You can allow specific formats by enabling the Session clipboard write allowed formats setting.

By default, this setting is Prohibited.

When the Restrict session clipboard write setting is Allowed, client clipboard data cannot be shared with session applications. You can use this setting to allow specific data formats to be shared with the session clipboard.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

The following clipboard formats are system defined:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE

The following custom formats are predefined in XenApp and XenDesktop:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- HTML Format

HTML Format is disabled by default. To enable this feature:

- Ensure **Client clipboard redirection** is set to allowed.
- Ensure **Restrict session clipboard write** is set to enabled.
- Add an entry for **HTML Format** (and any other formats you want supported) in **Session clipboard write allowed formats**.

Note: Enabling HTML Format clipboard copy support (HTML Format) copies any scripts (if they exist) from the source of the copied content to the destination. Check that you trust the source before proceeding to copy. If you do copy content containing scripts, they are live only if you save the destination file as an HTML file and execute it.

More custom formats can be added. The custom format name must match the formats to be registered with the system. Format names are case-sensitive.

This setting does not apply if either the Client clipboard redirection setting or Restrict session clipboard write setting is set to Prohibited.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

客户端自动重新连接策略设置

Dec 05, 2017

“客户端自动重新连接”部分包含用于控制会话自动重新连接的策略设置。

此设置允许或阻止同一客户端在连接中断后自动重新连接。

对于 Citrix Receiver for Windows 4.7 及更高版本，客户端自动重新连接仅使用 Citrix Studio 中的策略设置。在 Studio 中这些策略的更新会将客户端自动重新连接从服务器同步到客户端。使用旧版本的 Citrix Receiver for Windows 时，要配置客户端自动重新连接，请使用 Studio 策略并修改注册表或 default.ica 文件。

如果允许客户端自动重新连接，则当连接断开时，用户将可以从中断处继续执行原来的工作。自动重新连接会检测连接断开情形，然后将用户重新连接到其会话。

如果不使用包含会话 ID 和凭据的密钥的 Citrix Receiver cookie，自动重新连接可能会导致启动新会话。也就是说，不重新连接到现有会话。如果 Cookie 已过期（例如因为重新连接延迟，或者必须重新输入凭据），则不使用该 Cookie。如果用户有意断开连接，则不触发客户端自动重新连接。

重新连接过程中，会话窗口将显示为灰色。倒计时器显示重新连接会话之前的剩余时间。会话超时后将断开连接。

对于应用程序会话，允许自动重新连接时，通知区域中将显示一个倒计时器，指定重新连接会话之前的剩余时间。Citrix Receiver 将一直尝试重新连接会话，直到重新连接成功或者用户取消重新连接尝试为止。

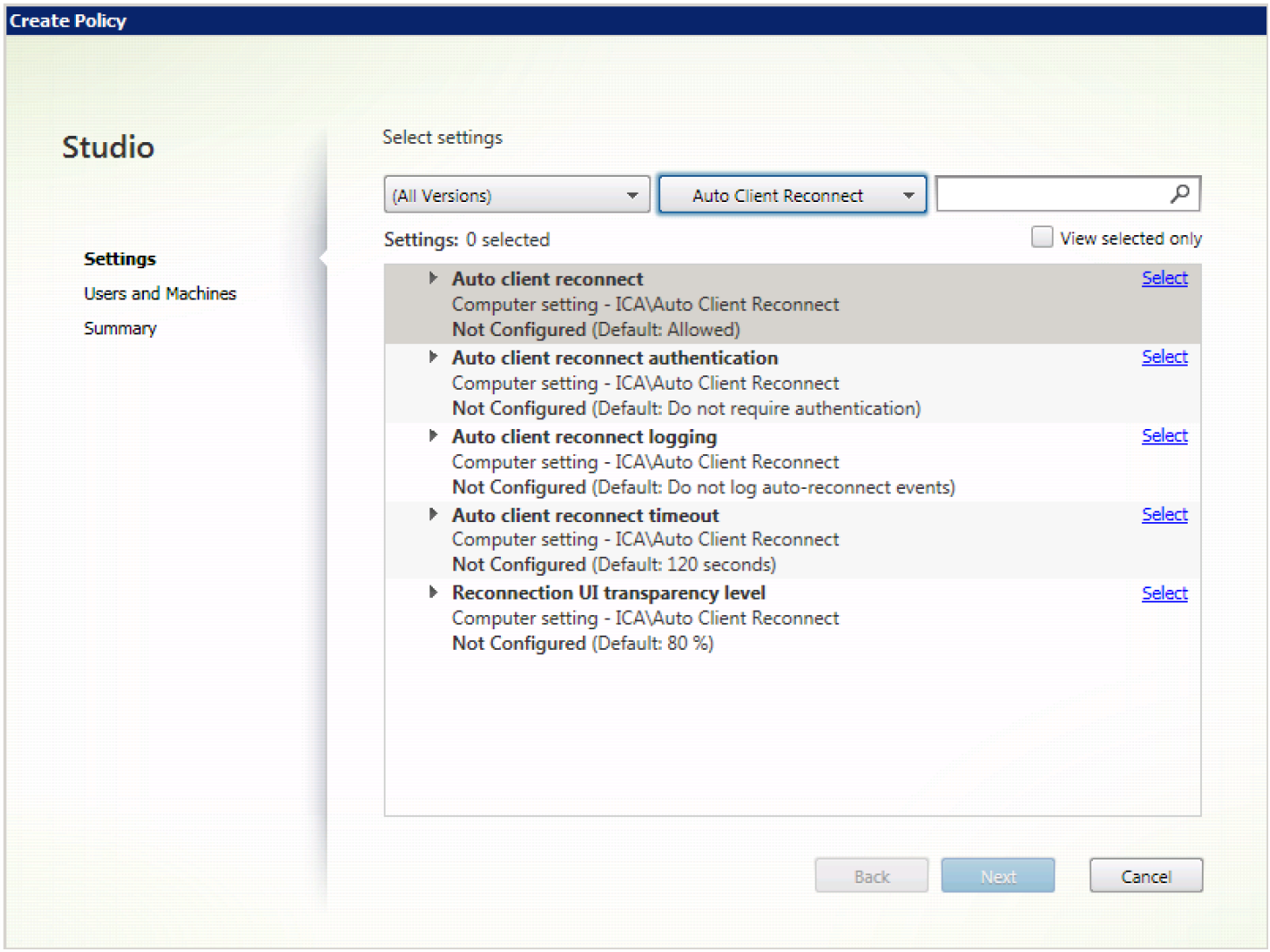
对于用户会话，允许自动重新连接时，Citrix Receiver 将在指定时间段内尝试重新连接会话，除非重新连接成功或者用户取消了重新连接尝试。默认情况下，此时间段为两分钟。要更改此时间期限，请编辑策略。

默认情况下，允许客户端自动重新连接。

要禁用客户端自动重新连接，请执行以下操作：

1. 启动 Citrix Studio。
2. 打开**客户端自动重新连接**策略。
3. 将策略设置为**禁止**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



此设置要求对客户端自动重新连接进行身份验证。

在用户最初登录时，其凭据将加密并存储在内存中，并创建一个包含加密密钥的 cookie。cookie 将发送到 Citrix Receiver。配置此设置后，将不使用 Cookie。而是在 Receiver 尝试自动重新连接时，向用户显示一个对话框，要求输入凭据。

默认情况下，无需进行身份验证。

要更改客户端自动重新连接身份验证，请执行以下操作：

1. 启动 Citrix Studio。
2. 打开**客户端自动重新连接身份验证**策略。
3. 启用或禁用身份验证。
4. 单击**确定**。

此设置启用或禁用在事件日志中记录客户端自动重新连接。

启用日志记录后，服务器系统日志将捕获与成功或失败的自动重新连接事件有关的信息。站点并不会提供所有服务器的重新连

© 1999-2017 Citrix Systems, Inc. All rights reserved.

接事件组合日志。

默认情况下，禁用日志记录。

要更改客户端自动重新连接日志记录，请执行以下操作：

1. 启动 Citrix Studio。
2. 打开**客户端自动重新连接日志记录**策略。
3. 启用或禁用日志记录。
4. 单击**确定**。

默认情况下，客户端自动重新连接超时设置为 120 秒，可配置的最大客户端自动重新连接超时值为 300 秒。

要更改客户端自动重新连接超时，请执行以下操作：

1. 启动 Citrix Studio。
2. 打开**客户端自动重新连接超时**策略。
3. 编辑超时值。
4. 单击**确定**。

可以使用 Studio 策略配置会话可靠性重新连接过程中应用到 XenApp 或 XenDesktop 会话窗口的不透明度级别。

默认情况下，重新连接用户界面透明度设置为 80%。

要更改重新连接用户界面不透明度级别，请执行以下操作：

1. 启动 Citrix Studio。
2. 打开**重新连接 UI 透明度级别**策略。
3. 编辑值。
4. 单击**确定**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

音频策略设置

Dec 05, 2017

“音频”部分 包含的策略设置允许用户设备在 会话中发送和接收音频，而不会降低性能。

此设置可允许或阻止使用用户数据报协议 (UDP) 通过 RTP 在 VDA 和用户设备之间传输和接收音频的功能。 禁用此设置后，将通过 TCP 发送和接收音频。

默认情况下，允许“通过 UDP 传输音频”。

此设置允许或阻止使用多个音频设备来录制和播放声音。

默认情况下，允许使用多个音频设备。

此设置仅适用于 Windows 服务器操作系统计算机。

该设置指定用户会话所接收的声音的质量等级。

默认情况下，音频质量设置为高 - 高清晰度音频。

要控制音频质量，请选择以下选项之一：

- 对于低带宽连接，请选择低 - 适用于低速连接。发送给用户设备的音频最高可压缩为 16 Kbps。这种压缩会大幅降低低带宽连接的音频质量，但是可以获得合理的性能。
- 选择中 - 语音优化可交付 IP 语音 (VoIP) 应用程序，或者在使用低于 512 Kbps 的线路或发生严重网络拥堵和数据包丢失的网络连接中交付媒体应用程序。此编解码器能够快速编码，非常适合在需要服务器端媒体处理时与软件电话和统一通信应用程序结合使用。
  发送给用户设备的音频最多可压缩至 64 Kbps。此压缩级别会导致用户设备上播放的音频质量适当下降，但是可缩短延迟并仅占用很少的带宽。如果 VoIP 质量无法满足需要，请确保将通过 UDP 实时传输音频策略设置为允许。

  目前，“通过 UDP 进行实时传输(RTP)”仅在选中此音频质量时受支持。即使在以下情况下交付媒体应用程序，也可以使用此音频质量：网络连接不畅，例如网速非常低（低于 512 Kbps）；网络拥堵且有数据包丢失。
- 对于带宽足够且音频质量很重要的连接，请选择高 - 高清晰度音频。客户端可以按照其本机速率播放声音。声音在保持最高达 CD 质量的高质量级别压缩，并使用最高 112 Kbps 的带宽。传输此数据量可能会导致 CPU 使用率增加以及网络拥塞。

只有在录制或播放音频时，才会占用带宽。如果两者同时发生，则会占用双倍带宽。

要指定最大带宽量，请配置音频重定向带宽限制或音频重定向带宽限制百分比设置。

此设置指定托管在服务器上的应用程序是否可以通过安装在用户设备上的音频设备来播放声音。 此设置还指定用户是否可以录制音频输入。

默认情况下，允许音频重定向。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

允许此设置之后，可以限制播放或录制音频占用的带宽。 限制音频占用的带宽量可提高应用程序性能，但也可能会降低音频质量。 只有在录制或播放音频时，才会占用带宽。 如果两者同时发生，则会占用双倍带宽。 要指定最大带宽量，请配置 音频重定向带宽限制或 音频重定向带宽限制百分比设置。

在 Windows 服务器操作系统计算机上，请确保将 音频即插即用设置为 启用以支持多个音频设备。

重要：禁止客户端音频重定向将禁用所有 HDX 音频功能。

此设置启用或禁用客户端麦克风重定向。 启用后，用户在会话中可以使用麦克风录制音频输入。

默认情况下，允许麦克风重定向。

出于安全考虑，当不受用户设备信任的服务器尝试访问麦克风时，系统会向用户发出警报。 用户可以选择是否接受访问。用户可以在 Citrix Receiver 上禁用警报。

在 Windows 服务器操作系统计算机上，请确保将 音频即插即用设置为 启用以支持多个音频设备。

如果在用户设备上禁用了 客户端音频重定向设置，则此规则不起任何作用。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

带宽策略设置

Dec 05, 2017

“带宽” 部分包含的一些策略设置可避免出现与 客户端会话带宽使用有关的性能问题。

重要：将这些策略设置与“多流”策略设置结合使用时，可能会导致意外的结果。 如果在某个策略中使用“多流”设置，请确保不要在该策略中包含这些带宽限制策略设置。

此设置指定在用户会话中播放或录制音频时允许使用的最大带宽 (Kbps)。

默认情况下，未指定最大值（零）。

如果为此设置和“音频重定向带宽限制百分比”设置都输入了一个值，则应用最严格（具有较低值）的设置。

此设置指定播放或录制音频时允许使用的最大带宽（占总会话带宽的百分比）。

默认情况下，未指定最大值（零）。

如果为此设置和“音频重定向带宽限制”设置都输入了一个值，则应用最严格（具有较低值）的设置。

如果配置此设置，还必须配置“总会话带宽限制”设置，后者用于指定客户端会话可用的带宽总量。

此设置指定允许往来于客户端的 USB 设备重定向所使用的最大带宽 (Kbps)。

默认情况下，未指定最大值（零）。

如果为此设置和“客户端 USB 设备重定向带宽限制百分比”设置都输入了一个值，则应用最严格（具有较低值）的设置。

此设置指定允许往来于客户端的 USB 设备重定向所使用的最大带宽（占总会话带宽的百分比）。

默认情况下，未指定最大值（零）。

如果为此设置和“客户端 USB 设备重定向带宽限制”设置都输入了一个值，则应用最严格（具有较低值）的设置。

如果配置此设置，还必须配置“总会话带宽限制”设置，后者用于指定客户端会话可用的带宽总量。

此设置指定在会话和本地剪贴板之间传输数据时允许使用的最大带宽 (Kbps)。

默认情况下，未指定最大值（零）。

如果为此设置和“剪贴板重定向带宽限制百分比”设置都输入了一个值，则应用最严格（具有较低值）的设置。

此设置指定在会话和本地剪贴板之间传输数据时允许使用的最大带宽（占总会话带宽的百分比）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

默认情况下，未指定最大值（零）。

如果为此设置和“剪贴板重定向带宽限制”设置都输入了一个值，则应用最严格（具有较低值）的设置。

如果配置此设置，还必须配置“总会话带宽限制”设置，后者用于指定客户端会话可用的带宽总量。

注意：对于 Virtual Delivery Agent 7.0 到 7.8，请使用注册表配置此设置。请参阅使用注册表配置 COM 端口和 LPT 端口重定向设置。
此设置指定在客户端连接中访问 COM 端口时允许使用的最大带宽 (Kbps)。如果为此设置输入一个值，并为 COM 端口重定向带宽限制百分比设置输入一个值，则应用最严格（具有较低值）的设置。

注意：对于 Virtual Delivery Agent 7.0 到 7.8，请使用注册表配置此设置。请参阅使用注册表配置 COM 端口和 LPT 端口重定向设置。
此设置指定在客户端连接中访问 COM 端口时允许使用的最大带宽（占总会话带宽的百分比）。

默认情况下，未指定最大值（零）

如果为此设置输入一个值，并为 COM 端口重定向带宽限制设置输入一个值，则应用最严格（具有较低值）的设置。

如果配置此设置，还必须配置总会话带宽限制设置，后者用于指定客户端会话可用的带宽总量

此设置指定在用户会话中访问客户端驱动器时允许使用的最大带宽 (Kbps)。

默认情况下，未指定最大值（零）。

如果为此设置和“文件重定向带宽限制百分比”设置都输入了一个值，则应用最严格（具有较低值）的设置。

此设置指定访问客户端驱动器时允许使用的最大带宽（占总会话带宽的百分比）。

默认情况下，未指定最大值（零）。

如果为此设置和”文件重定向带宽限制“设置都输入了一个值，则应用最严格（具有较低值）的设置。

如果配置此设置，还必须配置“总会话带宽限制”设置，后者用于指定客户端会话可用的带宽总量。

此设置 指定在通过 HDX MediaStream 多媒体加速 交付流音频和视频时允许使用的 最大带宽 (Kbps)。

默认情况下，未指定最大值（零）。

如果为此设置和“HDX MediaStream 多媒体加速带宽限制百分比”设置都输入了一个值，则应用最严格（具有较低值）的设置。

此设置指定在通过 HDX MediaStream 多媒体加速交付流音频和视频时允许使用的最大带宽（占总会话带宽的百分比）。

默认情况下，未指定最大值（零）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

如果为此设置和“HDX MediaStream 多媒体加速带宽限制”设置都输入了一个值，则应用最严格（具有较低值）的设置。

如果配置此设置，还必须配置“总会话带宽限制”设置，后者用于指定客户端会话可用的带宽总量。

注意：对于 Virtual Delivery Agent 7.0 到 7.8，请使用注册表配置此设置。请参阅使用注册表配置 COM 端口和 LPT 端口重定向设置。
此设置指定在单个用户会话中使用 LPT 端口的打印作业允许使用的最大带宽 (Kbps)。

默认情况下，未指定最大值（零）。

如果为此设置输入一个值，并为 LPT 端口重定向带宽限制百分比设置输入一个值，则应用最严格（具有较低值）的设置。

注意：对于 Virtual Delivery Agent 7.0 到 7.8，请使用注册表配置此设置。请参阅使用注册表配置 COM 端口和 LPT 端口重定向设置。
此设置指定在单个客户端会话中使用 LPT 端口的打印作业的带宽限制（占总会话带宽的百分比）。

默认情况下，未指定最大值（零）。

如果为此设置输入一个值，并为 LPT 端口重定向带宽限制设置输入一个值，则应用最严格（具有较低值）的设置。

如果配置此设置，还必须配置总会话带宽限制设置，后者用于指定客户端会话可用的带宽总量。

此设置指定用户会话可用的总带宽 (Kbps)。

最大可强制带宽上限为 10 Mbps (10,000 Kbps)。 默认情况下，未指定最大值（零）。

当客户端连接外的其他应用程序竞用有限带宽时，限制客户端连接所占用的带宽量可提高性能。

此设置指定在用户会话中访问客户端打印机时允许使用的最大带宽 (Kbps)。

默认情况下，未指定最大值（零）。

如果为此设置和“打印机重定向带宽限制百分比”设置都输入了一个值，则应用最严格（具有较低值）的设置。

此设置指定访问客户端打印机时允许使用的最大带宽（占总会话带宽的百分比）。

默认情况下，未指定最大值（零）。

如果为此设置和“打印机重定向带宽限制”设置都输入了一个值，则应用最严格（具有较低值）的设置。

如果配置此设置，还必须配置“总会话带宽限制”设置，后者用于指定客户端会话可用的带宽总量。

此设置指定从已发布的应用程序控制 TWAIN 成像设备时允许使用的最大带宽 (Kbps)。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

默认情况下，未指定最大值（零）。

如果为此设置和“TWAIN 设备重定向带宽限制百分比”设置都输入了一个值，则应用最严格（具有较低值）的设置。

此设置指定从已发布的应用程序控制 TWAIN 成像设备时允许使用的最大带宽（占总会话带宽的百分比）。

默认情况下，未指定最大值（零）。

如果为此设置输入一个值，并为 TWAIN 设备重定向带宽限制设置输入一个值，则应用最严格（具有较低值）的设置。

如果配置此设置，还必须配置总会话带宽限制设置，后者用于指定客户端会话可用的带宽总量。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

双向内容重定向策略设置

Dec 05, 2017

双向内容重定向部分包含用于启用或禁用客户端到主机和主机到客户端 URL 重定向的策略设置。服务器策略在 Studio 中设置，客户端策略则在 Citrix Receiver 组策略对象管理模板中设置。

尽管 Citrix 还提供主机到客户端重定向以及适用于客户端到 URL 重定向的本地应用程序访问，但我们建议您对加入域的 Windows 客户端使用双向内容重定向。

双向内容重定向要求 XenApp 或 XenDesktop 7.13 及更高版本以及 Citrix Receiver for Windows 4.7 及更高版本。

Important

- 请确保重定向规则不会导致出现循环配置。例如，在 VDA 上设置的客户端规则设置为 https://www.citrix.com，在客户端上设置的 VDA 规则设置为可能会导致无线循环的相同 URL。
- 我们仅支持加入域的端点设备。
- URL 重定向仅支持显式 URL（出现在浏览器地址栏中或使用浏览器内置导航找到的 URL，具体取决于浏览器）。我们不支持链接缩短器。
- 双向内容重定向仅支持 Internet Explorer 8 到 11。必须同时在用户设备和 VDA 上使用 Internet Explorer。
- 双向内容重定向需要 Internet Explorer 浏览器加载项。有关详细信息，请参阅注册浏览器加载项。
- 如果重定向由于会话启动问题失败，则不存在回退机制。
- 如果显示名称相同的两个应用程序配置为使用多个 StoreFront 帐户，主 StoreFront 帐户中的一个显示名称将用于启动。
- 仅支持 Citrix Receiver for Windows。
- 新浏览器窗口仅在 URL 重定向到客户端时显示。URL 重定向到 VDA 时，如果浏览器已打开，重定向的 URL 将在新选项卡中打开。
- 支持在文件（包括文档、电子邮件和 PDF）中使用嵌入式链接。
- 此功能适用于桌面会话和应用程序会话，这与本地应用程序访问 URL 重定向不同，后者仅适用于桌面会话。
- 如果为 URL 重定向启用了本地应用程序访问（在 VDA 或客户端上），双向内容重定向将不起作用。

请使用 Studio 配置主机到客户端（客户端）和主机到主机 (VDA) 重定向策略。

默认情况下，**禁止**双向内容重定向。

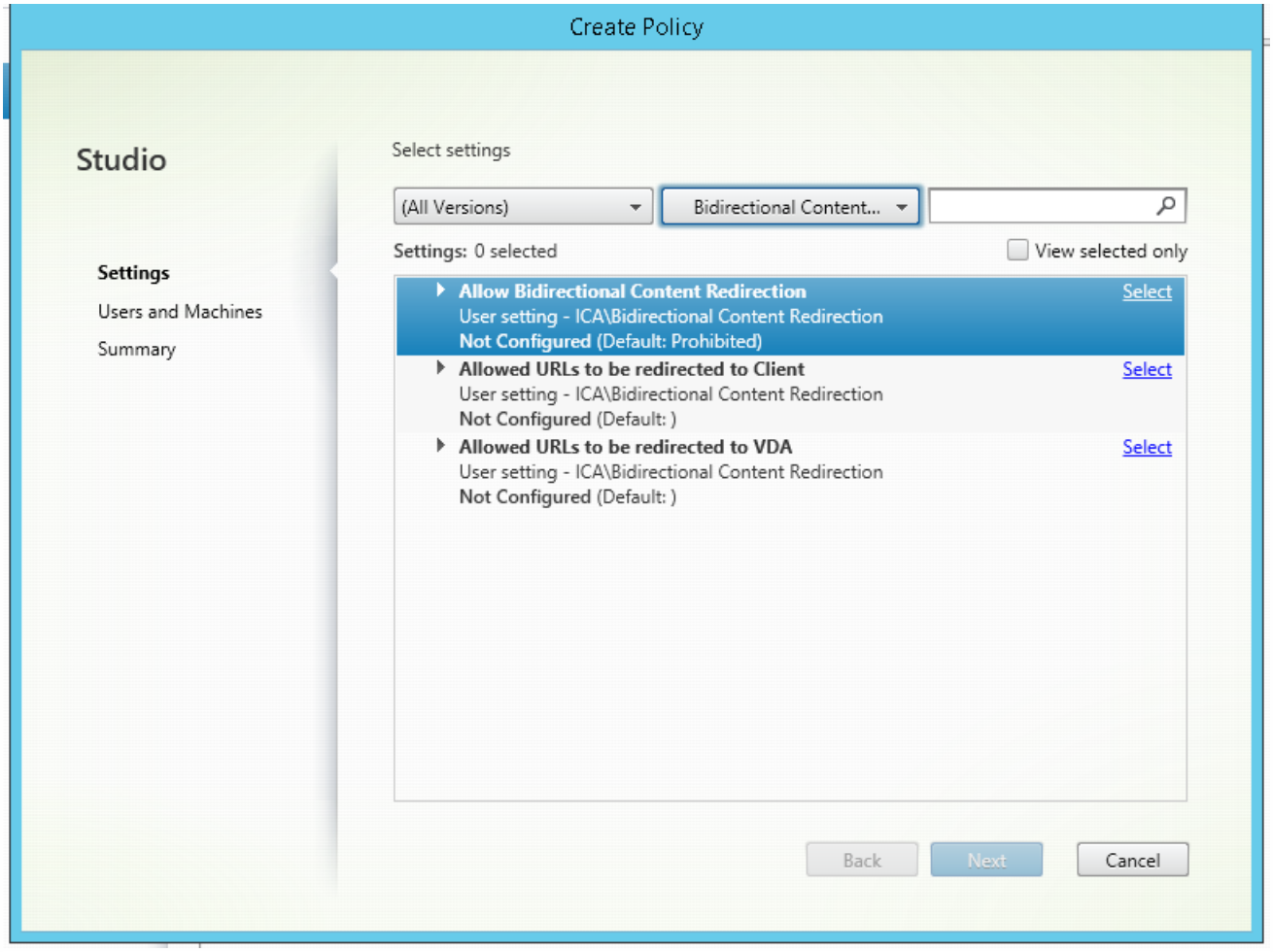
启用双向内容重定向

包括 URL 时，可以指定一个 URL 或以分号分隔的 URL 列表。可以在域名中使用星号 (*) 作为通配符。例如：

http://*.citrix.com; http://www.google.com

1. 启动 Citrix Studio。
2. 打开**双向内容重定向**策略。
3. 选择**允许双向内容重定向**，选择**允许**并单击**确定**。如果不允许此选项，您将无法完成此过程。
4. 选择**允许重定向到客户端的 URL**并指定一个 URL、URL 列表，或者选择默认值。
5. 选择**允许重定向到 VDA 的 URL**并指定一个 URL、URL 列表，或者选择默认值。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



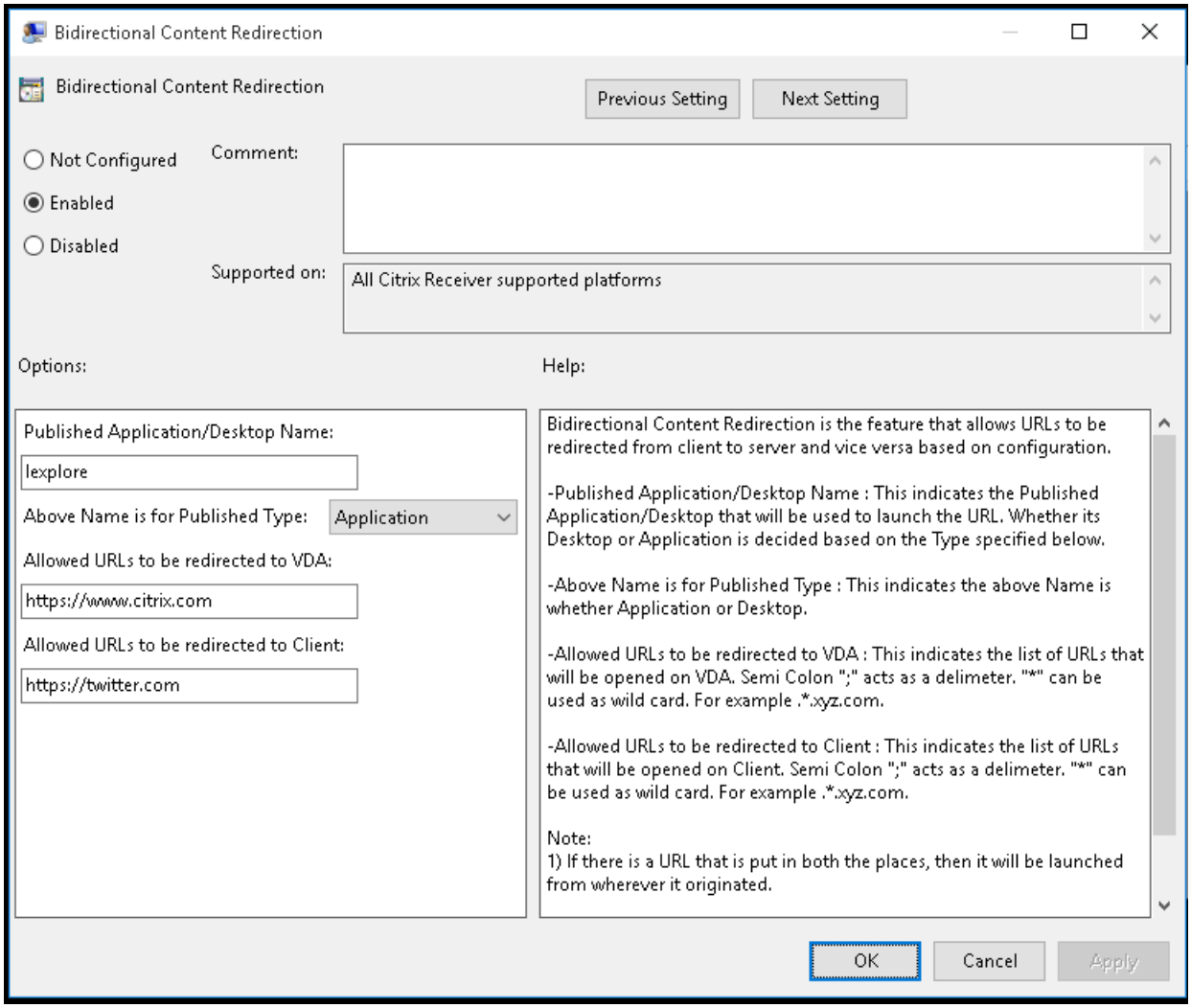
使用 Citrix Receiver 组策略对象管理模板可配置客户端到主机 (VDA) 和客户端到客户端（客户端）重定向。

启用双向内容重定向

包括 URL 时，可以指定一个 URL 或以分号分隔的 URL 列表。可以使用星号 (*) 作为通配符。

有关详细信息，请参阅 Citrix Receiver 文档中的配置双向内容重定向。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



双向内容重定向需要 Internet Explorer 浏览器加载项。

可以使用以下命令注册和取消注册 Internet Explorer 加载项：

- 在客户端设备上注册 Internet Explorer 加载项：<客户端安装文件夹>\redirector.exe /regIE
- 在客户端设备上取消注册 Internet Explorer 加载项：<客户端安装文件夹>\redirector.exe /unregIE
- 在 VDA 上注册 Internet Explorer 加载项：\VDARedirector.exe /regIE
- 在 VDA 上取消注册 Internet Explorer 加载项：\VDARedirector.exe /unregIE

例如，以下命令在运行 Citrix Receiver 的设备上注册 Internet Explorer 加载项。

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

以下命令在 Windows Server OS VDA 上注册 Internet Explorer 加载项。

C:\Program Files (x86)\Citrix\System32\VDARedirector.exe /regIE

© 1999-2017 Citrix Systems, Inc. All rights reserved.

客户端传感器策略设置

Dec 05, 2017

“客户端传感器” 部分中包含用于控制如何在用户会话中处理移动设备传感器 信息的策略设置。

此设置决定是否允许在移动设备上的会话中运行的应用程序使用用户设备的物理位置。

默认情况下，禁止使用位置信息。

如果禁用了此设置，则应用程序尝试检索位置信息时将返回值“权限遭拒”。

如果启用了此设置，用户可以通过拒绝 Citrix Receiver 访问位置的请求来禁止使用位置信息。Receiver 首次发出请求时，Android 和 iOS 设备将提示在每个会话中输入位置信息。

开发使用允许应用程序使用客户端设备的物理位置设置的托管应用程序时，请注意以下各项：

- 启用了位置功能的应用程序不应依赖于当前可用的位置信息，原因如下：
  - 用户可能不允许访问位置信息。
  - 位置可能不可用，或者在应用程序运行过程中可能会发生变化。
  - 用户可能会从不支持位置信息的其他设备连接到应用程序会话。
- 启用了位置功能的应用程序必须满足以下条件：
  - 默认关闭位置功能。
  - 提供一个用户选项，用于在应用程序运行过程中启用或禁用位置功能。
  - 提供一个用户选项，用于清除应用程序缓存的位置数据。（Citrix Receiver 不缓存位置数据。）
- 启用了位置功能的应用程序必须精确管理位置信息，以便获取的数据能够满足应用程序的需求，且遵守所有相关司法管辖区的法规。
- 使用定位服务时，应强制使用安全连接（例如，使用 TLS 或 VPN）。Citrix Receiver 应连接到可信服务器。
- 注意征求使用定位服务方面的法律意见。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

桌面 UI 策略设置

Dec 05, 2017

“桌面 UI”部分包含的策略设置可控制视觉效果（例如桌面墙纸、菜单动画以及拖放图像）以管理客户端连接占用的带宽。限制带宽使用量可以改善 WAN 上的应用程序性能。

此设置指定是否将用户设备上的图形处理器 (GPU) 或集成图形处理器 (IGP) 的处理功能用于执行本地 DirectX 图形呈现，从而为用户提供更流畅的 Windows 桌面体验。启用后，桌面组合重定向可提供高响应度的 Windows 体验，同时还能保持服务器的高度可扩展性。

默认情况下，禁用桌面组合重定向。

要关闭桌面组合重定向并减少用户会话所需的带宽，请在将此设置添加到策略时选择禁用。

此设置指定用于桌面组合重定向的图形质量。

默认设置为“高”。

可以从 高、 中、 低或 无损质量中进行选择。

此设置允许或禁止在用户会话中显示墙纸。

默认情况下，用户会话可以显示墙纸。

要关闭桌面墙纸并减少用户会话所需的带宽，请在将此设置添加到策略时选择 禁止。

此设置允许或禁止在用户会话中显示菜单动画。

默认情况下，允许菜单动画。

菜单动画是 Microsoft 个人首选项设置，目的是便于轻松访问。 启用后，将导致菜单在短暂延迟后通过滚动或淡入进行显示。箭头图标显示在菜单底部。指向该箭头时会显示此菜单。

如果此策略设置设为 允许，并且启用了菜单动画 Microsoft 个人首选项设置，则会在桌面上启用菜单动画。

注意：对菜单动画 Microsoft 个人首选项设置所做的更改即是对桌面所做的更改。 这意味着，如果桌面设置为在会话结束时丢弃更改，在会话中启用了菜单动画的用户在桌面上后续的会话中可能没有可用的菜单动画。 对于需要菜单动画的用户，请在桌面的主映像中启用 Microsoft 设置，或者请确保桌面保留用户所做的更改。

此设置允许或禁止在屏幕上拖动窗口时显示窗口内容。

默认情况下，允许查看窗口内容。

如果设置为 允许，拖动窗口时可看到整个窗口的移动。 如果设置为 禁止，则只能看到窗口框的移动，直至放下窗口。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

最终用户监控策略设置

Dec 05, 2017

“最终用户 监视”部分包含用于测量会话流量的策略设置。

此设置确定是否为活动连接执行 ICA 往返行程计算。

默认情况下，启用活动连接的计算。

默认情况下，每次 ICA 往返行程度量的启动都将延迟，直至指示有用户交互的通信出现。 此延迟的长度不限，以防止 ICA 往返行程度量成为产生 ICA 通信的唯一原因。

此设置指定 ICA 往返行程计算的执行间隔（以秒为单位）。

默认情况下，ICA 往返行程每 15 秒钟计算一次。

此设置确定是否为空闲连接执行 ICA 往返行程计算。

默认情况下，不为空闲连接执行计算。

默认情况下，每次 ICA 往返行程度量的启动都将延迟，直至指示有用户交互的通信出现。 此延迟的长度不限，以防止 ICA 往返行程度量成为产生 ICA 通信的唯一原因。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Enhanced Desktop Experience 策略设置

Dec 05, 2017

Enhanced Desktop Experience 策略设置可配置在服务器操作系统上运行的会话，使其看起来 像本地 Windows 7 桌面，从而为用户提供增强的桌面 体验。

默认情况下，此 设置为允许。

如果虚拟桌面上已存在 具有 Windows Classic 主题的用户配置文件，则启用此 策略将不会为该用户提供增强的桌面体验。如果用户 以 Windows 7 主题用户配置文件登录到运行未配置或禁用此策略的 Windows Server 2012 的虚拟桌面， 则会向该用户显示错误消息，指明应用主题失败。

在上述两种情况下， 重置用户配置文件即可解决问题。

如果策略 在具有活动用户会话的虚拟桌面上从启用状态更改为 禁用状态，则这些会话的外观会与 Windows 7 和 Windows Classic 桌面体验不一致。为避免出现此问题， 请确保在更改此策略设置后重新启动虚拟桌面。您还必须 删除虚拟桌面上的任何漫游配置文件。Citrix 还建议您 删除虚拟桌面上的任何其他用户配置文件，以避免配置文件之间的 不一致。

如果您在环境中使用 漫游用户配置文件，请确保对共享同一配置文件的所有虚拟桌面 启用或禁用 Enhanced Desktop Experience 功能。

Citrix 建议 不要在运行服务器操作系统和客户端 操作系统的虚拟桌面之间共享漫游配置文件。适用于客户端和服务器 操作系统的配置文件有所差别，跨两种类型的操作系统共享漫游配置文件可能会 导致用户在这两种操作系统之间移动时配置文件属性 不一致。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

文件重定向策略设置

Dec 05, 2017

“文件重定向” 部分包含与客户端驱动器映射和客户端 驱动器优化有关的策略设置。

此设置允许或禁止在用户登录时自动连接客户端驱动器。

默认情况下允许自动连接。

将此设置添加到策略时，请确保启用您希望自动连接的驱动器类型的设置。 例如，要允许自动连接到用户的 CD-ROM 驱动器，请配置此设置以及“客户端光盘驱动器”设置。

下列策略设置为 相关设置：

- 客户端驱动器重定向
- 客户端软盘驱动器
- 客户端光盘驱动器
- 客户端固定驱动器
- 客户端网络驱动器
- 客户端可移动驱动器

此设置启用或禁用往来于用户设备上的驱动器的文件重定向。

默认情况下，启用文件重定向。

启用时，用户可将文件保存到其所有客户端驱动器。 禁用时，将禁止所有文件重定向，而不考虑各文件重定向设置（例如“客户端软盘驱动器”和“客户端网络驱动器”）的状态。

下列策略设置为相关设置：

- 客户端软盘驱动器
- 客户端光盘驱动器
- 客户端固定驱动器
- 客户端网络驱动器
- 客户端可移动驱动器

此设置允许或禁止用户访问文件或将文件保存到用户设备上的固定驱动器。

默认情况下，允许访问客户端固定驱动器。

在策略中添加此设置时，请确保“客户端驱动器重定向”设置存在，并且设置为“允许”。 如果禁用这些设置，将不映射客户端固定驱动器，且用户无法手动访问这些驱动器，无论“客户端固定驱动器”设置的状态如何。

要确保在用户登录时自动连接固定驱动器，请配置“自动连接客户端驱动器”设置。

此设置允许或禁止用户访问文件或将文件保存到用户设备上的软盘驱动器。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

默认情况下，允许访问客户端软盘驱动器。

在策略中添加此设置时，请确保“客户端驱动器重定向”设置存在，并且设置为“允许”。 如果禁用这些设置，将不映射客户端固定驱动器，且用户无法手动访问这些驱动器，无论“客户端软盘驱动器”设置的状态如何。

要确保在用户登录时自动连接软盘驱动器，请配置“自动连接客户端驱动器”设置。

此设置允许或禁止用户通过用户设备访问文件或将文件保存到网络（远程）驱动器。

默认情况下，允许访问客户端网络驱动器。

在策略中添加此设置时，请确保“客户端驱动器重定向”设置存在，并且设置为“允许”。 如果禁用这些设置，将不映射客户端网络驱动器，且用户无法手动访问这些驱动器，无论“客户端网络驱动器”设置的状态如何。

要确保在用户登录时自动连接网络驱动器，请配置“自动连接客户端驱动器”设置。

此设置允许或禁止用户访问文件或将文件保存到用户设备上的 CD-ROM、DVD-ROM 和 BD-ROM 驱动器。

默认情况下，允许访问客户端光盘驱动器。

在策略中添加此设置时，请确保“客户端驱动器重定向”设置存在，并且设置为“允许”。 如果禁用这些设置，将不映射客户端光盘驱动器，且用户无法手动访问这些驱动器，无论“客户端光盘驱动器”设置的状态如何。

要确保在用户登录时自动连接光盘驱动器，请配置“自动连接客户端驱动器”设置。

此设置允许或禁止用户访问文件或将文件保存到用户设备上的 USB 驱动器。

默认情况下，允许访问客户端可移动驱动器。

在策略中添加此设置时，请确保“客户端驱动器重定向”设置存在，并且设置为“允许”。 如果禁用这些设置，将不映射客户端可移动驱动器，且用户无法手动访问这些驱动器，无论“客户端可移动驱动器”设置的状态如何。

要确保在用户登录时自动连接可移动驱动器，请配置“自动连接客户端驱动器”设置。

此设置启用或禁用将在用户设备上打开的 URL 及某些媒体内容的文件类型关联。 禁用时，内容在服务器上打开。

默认情况下，禁用文件类型关联。

启用此设置后，以下这些 URL 类型将在本地打开：

- 超文本传输协议 (HTTP)
- 安全超文本传输协议 (HTTPS)
- Real Player 和 QuickTime (RTSP)
- Real Player 和 QuickTime (RTSPU)
- 旧版 Real Player (PNM)
- Microsoft 媒体服务器 (MMS)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

此设置允许或禁止将客户端驱动器映射到会话中的同一驱动器号。

默认情况下，不保留客户端驱动器盘符。

在策略中添加此设置时，请确保“客户端驱动器重定向”设置存在，并且设置为“允许”。

该设置允许或阻止用户及应用程序创建或修改映射的客户端驱动器上的文件或文件夹。

默认情况下，可以修改映射的客户端驱动器上的文件和文件夹。

如果设置为“已启用”，则具有只读权限即可访问文件和文件夹。

在策略中添加此设置时，请确保“客户端驱动器重定向”设置存在，并且设置为“允许”。

此设置允许或阻止 Citrix Receiver 和 Web Interface 用户从会话中看到其本地文档和桌面特殊文件夹。

默认情况下，允许特殊文件夹重定向。

此设置可防止任何通过策略过滤的对象使用特殊文件夹重定向，无论其他位置存在何种设置。如果禁止此设置，将忽略为 StoreFront、Web Interface 或 Citrix Receiver 指定的任何相关设置。

要定义哪些用户可以使用特殊文件夹重定向，请选择允许，并将此设置包括在对您希望具有此功能的用户执行过滤的策略中。此设置将覆盖所有其他特殊文件夹重定向设置。

由于特殊文件夹重定向必须与用户设备交互，因此，禁止用户访问文件或将文件保存到本地硬盘驱动器的策略设置，也会禁止用户使用特殊文件夹重定向。

将此设置添加到策略中时，请确保客户端固定驱动器设置存在，且设置为允许。

此设置启用或禁用异步磁盘写入。

默认情况下，禁用异步写入。

异步磁盘写入可改善通过广域网执行文件传输和向客户端磁盘写入的速度，此类传输和写入的典型特征是相对较高的带宽以及高延迟。 但是，如果发生连接或磁盘故障，正在写入的客户端文件将被置于一种未定义状态。 如果发生这种情况，系统将显示一个弹出窗口，告知用户受影响的文件。 用户然后可以采取补救措施，例如在重新建立连接时或修复磁盘故障后重新启动中断的文件传输。

Citrix 建议仅为这样的用户启用异步磁盘写入：需要具有良好文件访问速度的远程连接，可以方便地恢复发生连接或磁盘故障时丢失的文件或数据。

将此设置添加到策略中时，请确保“客户端驱动器重定向设置”存在，且设置为“允许”。 如果禁用此设置，将不执行异步写入。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Flash 重定向策略设置

Dec 05, 2017

“Flash 重定向”部分包含用于处理用户会话中的 Flash 内容的策略 设置。

此设置允许或禁止 Flash 内容在用户设备上而非在服务器端呈现。 默认情况下，启用客户端 Flash 内容呈现。

注意：此设置用于 Citrix Online Plug-in 12.1 的旧版 Flash 重定向功能。
处于启用状态时，此设置会在用户设备上呈现 Flash 内容，从而降低了网络和服务器负载。 此外，“Flash URL 兼容性列表”设置将强制特定 Web 站点上的 Flash 内容在服务器上呈现。

在用户设备上，必须同时启用“在用户设备上启用 HDX MediaStream for Flash”设置。

此设置处于禁用状态时，所有 Web 站点（无论 URL 为何）上的 Flash 内容均在服务器上呈现。 要仅允许特定 Web 站点上的 Flash 内容在用户设备上呈现，请配置 Flash URL 兼容性列表设置。

该设置允许您设置指定 URL 的主要颜色。

默认情况下不指定主要颜色。

主要颜色显示在客户端呈现的 Flash 的后面，帮助提供可视区域检测。指定的主要颜色应非常特殊；否则可视区域检测功能可能不会正确执行。

有效条目包含一个 URL（在开头或结尾带有可选的通配符），后接 24 位 RGB 颜色的十六进制代码。例如：http://citrix.com 000003。

确保指定的 URL 是 Flash 内容的 URL，可能不同于 Web 站点的 URL。

> **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。

在运行 Windows 8 或 Windows 2012 的 VDA 计算机上，此设置可能无法设置 URL 的注册表项颜色。如果出现此情况，请在 VDA 计算机上编辑注册表。

对于 32 位计算机，请使用此注册表设置：

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]
"ForceHDXFlashEnabled"=dword:00000001

对于 64 位计算机，请使用此注册表设置：

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]
"ForceHDXFlashEnabled"=dword:00000001

© 1999-2017 Citrix Systems, Inc. All rights reserved.

此设置将允许或禁止使用早期版本的 Citrix Receiver（以前称为 Citrix 联机插件）具有的原始旧模式 Flash 重定向功能。

默认情况下，此设置处于启用状态。

在用户设备上，必须同时启用“在用户设备上启用 HDX MediaStream for Flash”设置。

第二代 Flash 重定向功能处于启用状态，以便与 Citrix Receiver 3.0 结合使用。 支持将旧模式重定向功能与 Citrix 联机插件 12.1 结合使用。 要确保使用第二代 Flash 重定向功能，服务器和用户设备都必须启用第二代 Flash 重定向功能。 如果在服务器或用户设备上启用了旧模式重定向功能，则将使用旧模式重定向功能。

此设置将确立第二代 Flash 加速功能的默认行为。

默认情况下启用 Flash 加速。

要配置此设置，请选择以下选项之一：

- 启用 Flash 加速。使用 Flash 重定向功能。
- 阻止 Flash Player。不使用 Flash 重定向和服务器端呈现功能。用户无法查看任何 Flash 内容。
- 禁用 Flash 加速。不使用 Flash 重定向功能。如果服务器上已安装与内容兼容的 Adobe Flash Player for Windows Internet Explorer 版本，则用户可以查看服务器端呈现的 Flash 内容。

对于单个 Web 页面和 Flash 实例，可以覆盖此设置，具体取决于 Flash URL 兼容性列表设置的配置。此外，用户设备必须启用在用户设备上启用 HDX MediaStream for Flash 设置。

此设置允许将 Flash 事件记录到 Windows 应用程序事件日志中。

默认情况下，允许记录。

在运行 Windows 7 或 Windows Vista 的计算机上，特定于 Flash 重定向的日志将显示在“应用程序和服务日志”节点下。

如果无需在客户端呈现，或者客户端呈现提供的用户体验较差，则此设置将允许或禁止自动尝试部署服务器端 Flash Player 实例呈现。

默认情况下，此设置处于启用状态。

此设置可指定介于 0 到 30 毫秒之间的阈值，以确定 Adobe Flash 内容的呈现位置。

默认情况下，阈值为 30 毫秒。

启动期间，HDX MediaStream for Flash 会测量服务器与用户设备之间的当前延迟。 如果延迟低于阈值，则将使用 HDX MediaStream for Flash 将 Flash 内容在用户设备上呈现。 如果延迟高于阈值，则在网络服务器上安装了 Adobe Flash 播放器的情况下，Flash 内容将在网络服务器端呈现。

启用此设置时，请确保 Flash 向后兼容设置同样存在，且设置为“启用”。

注意：仅在旧模式中使用 HDX MediaStream Flash 重定向时适用。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

此设置指定“小”Flash 内容是否向用户呈现和显示及对应的方式。

默认情况下未配置此设置。

要配置此设置，请选择以下选项之一：

- **仅限小型内容。**仅在服务器上呈现智能回退内容；其他 Flash 内容将替换为错误 *.swf。
- **仅限使用受支持客户端的小型内容。**如果客户端当前使用 Flash 重定向，仅在服务器上呈现智能回退内容；其他内容将替换为错误 *.swf。
- **无服务器端内容。**在服务器上，所有内容均会替换为错误 *swf。

要使用此策略设置，应指定一个 error *.swf 文件。此错误 *.swf 将取代任何您不希望在 VDA 上呈现的内容。

此设置指定错误消息的 URL，使用服务器负载管理时，此错误消息将取代 Flash 实例显示给用户。例如：

http://domainName.tld/sample/path/error.swf

此设置将指定一些 Web 站点，可以将这些站点的 Flash 内容下载到服务器，然后传输到用户设备以进行呈现。

默认情况下，不指定任何站点。

如果用户设备对 Internet 没有直接访问权限，则将使用此设置；服务器将提供 Internet 连接。 此外，用户设备必须启用“启用服务器端内容提取”设置。

第二代 Flash 重定向功能包括回退到在服务器端内容提取 Flash .swf 文件内容。 如果用户设备无法从某个 Web 站点提取 Flash 内容，但该 Web 站点在“Flash 服务器端内容提取 URL 列表”中进行了指定，则将自动执行服务器端内容提取。

向该列表中添加 URL 时，请：

- 添加 Flash 应用程序的 URL，而非可启动 Flash Player 的顶层 HTML 页面。
- 在 URL 的开头或结尾处使用星号 (*) 作为通配符。
- 使用后导通配符以包含所有子 URL（例如 http://www.citrix.com/*）。
- 显示时使用前缀 http:// 和 https://，但有效列表条目并非必须使用这些前缀。

此设置将指定一些规则，这些规则决定特定 Web 站点上的 Flash 内容是在用户设备上呈现，在服务器上呈现，还是受到阻止，无法呈现。

默认情况下，不指定任何规则。

向该列表中添加 URL 时，请：

- 排定列表的优先顺序，最重要的 URL、操作和呈现位置在前。
- 在 URL 的开头或结尾处使用星号 (*) 作为通配符。
- 使用后导通配符以包含所有子 URL（例如 http://www.citrix.com/*）。
- 显示时使用前缀 http:// 和 https://，但有效列表条目并非必须使用这些前缀。
- 将 Flash 内容无法 在用户设备上正确呈现的 Web 站点添加到该列表中，然后选择 在服务器上 呈现或 阻止选项。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

图形策略设置

Dec 05, 2017

“图形”部分包含用于控制如何在用户会话中处理图像的策略设置。

此设置允许为图像使用视觉无损压缩，而不是真正无损的压缩。相比于真正无损的压缩，视觉无损功能可提高性能，但会产生视觉上不易察觉的轻微损失。此设置可更改“视觉质量设置”值的使用方式。

默认情况下，禁用此设置。

此设置指定会话的最大视频缓冲区大小 (KB)。

默认情况下，显示内存限制为 65536 KB。

指定会话的最大视频缓冲区大小 (KB)。指定一个介于 128 到 4,194,303 之间的量 (KB)。最大值 4,194,303 不会限制显示内存。默认情况下，显示内存为 65536 KB。如果为连接使用更高的颜色深度和分辨率，则需要更多内存。在传统图形模式下，如果达到内存限制，则显示质量会根据“显示模式降级首选项”设置的情况而降级。

对于需要更高颜色深度和分辨率的连接，可增大该限值。使用如下公式计算所需的最大内存：

内存深度 (字节) = (颜色深度 (bpp) / 8) * (垂直分辨率 [像素]) * (水平分辨率 [像素])。

例如，当颜色深度为 32，垂直分辨率为 600，水平分辨率为 800 时，所需的最大内存为 (32 / 8) * (600) * (800) = 1920000 字节，从而可得显示内存限制为 1920 KB。

只有在已启用旧图形模式策略设置时，才能使用 32 位以外的其他颜色深度。

HDX 仅向每个会话分配所需的显示内存量。因此，如果只有一部分用户所需的内存量高于默认值，通过增加显示内存限制不会对可扩展性产生负面影响。

注意：对于 Virtual Delivery Agent 7.x，仅当启用 旧图形模式策略设置时，才会应用此策略设置。
此设置指定达到会话显示内存限制时的处理方式：首先降低颜色深度的级别还是首先降低分辨率的级别。

默认情况下，首先降低颜色深度的级别。

达到会话内存限制时，您可以选择首先降低颜色深度的级别还是首先降低分辨率的级别，来降低显示图像的质量。如果首先降低颜色深度的级别，显示图像将使用较少的颜色。如果首先降低分辨率的级别，显示图像每英寸将使用较少的像素。

要在降低颜色深度或分辨率的级别时通知用户，请配置 在显示模式降级时通知用户设置。

此设置启用或禁用以窗口切换、三维窗口切换、任务栏预览和透视窗口预览模式显示无缝窗口。

Windows Aero 预览选项	说明
任务栏预览	用户将鼠标悬停在某个窗口的任务栏图标上时，任务栏上方将显示该窗口的图像。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Windows Aero 预览选项	说明
窗口透视	用户将鼠标悬停在某个任务栏预览图像上时，屏幕上将显示完整大小的窗口图像。
窗口切换	用户按 Alt+Tab 时，每个打开的窗口显示一个小型预览图标。
三维窗口切换	用户按 Tab+Windows 徽标键时，屏幕上将层叠显示已打开窗口的大图像。

默认情况下，此设置处于启用状态。

注意：对于 Virtual Delivery Agent 7.x，仅当启用 旧图形模式策略设置时，才会应用此策略设置。
此设置启用或禁用在会话中缓存和取回图像分区。通过在需要时缓存分区中的图像和取回这些分区，用户可以更加顺畅地进行滚动，降低了通过网络传输的数据量，同时降低了需要在用户设备上处理的数据量。

默认情况下，启用图像缓存设置。

注意：图像缓存设置控制缓存和取回图像的方式，不控制是否缓存图像。如果启用了“旧图形模式”设置，则将缓存图像。

此设置禁用丰富的图形体验。使用此设置可还原为旧版图形体验，降低了使用 WAN 或移动连接时占用的带宽。XenApp 和 XenDesktop 7.13 中引入的带宽降低功能导致此模式过时。

默认情况下，禁用此设置，并向用户提供丰富的图形体验。

旧图形模式在 Windows 7 和 Windows Server 2008 R2 VDA 中受支持。

旧图形模式在 Windows 8.x、10 或 Windows Server 2012、2012 R2 和 2016 中不受支持。

请参阅 CTX202687 了解关于在 XenApp 和 XenDesktop 7.6 FP3 或更高版本中优化图形模式和策略的详细信息。

注意：对于 Virtual Delivery Agent 7.x，仅当启用旧图形模式策略设置时，才会应用此策略设置。
此设置指定会话允许的最大颜色深度。

默认情况下，允许的最大颜色深度是每像素 32 位。

此设置仅适用于 ThinWire 驱动程序和连接。不适用于将非 ThinWire 驱动程序用作主显示器驱动程序的 VDA，如将 Windows 显示驱动程序模型 (WDDM) 驱动程序用作主显示器驱动程序的 VDA。对于将 WDDM 驱动程序用作主显示器驱动程序的桌面操作系统 VDA（如 Windows 8），此设置无影响。 对于使用 WDDM 驱动程序的 Windows 服务器操作系统 VDA（例如 Windows Server 2012 R2），此设置可能会阻止用户连接到 VDA。

设置较高的颜色深度需要更多内存。要在达到内存限制时降低颜色深度的级别，请配置显示模式降级首选项设置。颜色深度降级后，显示图像将使用较少的颜色。

注意：对于 Virtual Delivery Agent 7.x，仅当启用 旧图形模式策略设置时，才会应用此策略设置。
此设置在降低颜色深度或分辨率的级别时，向用户显示简要说明。

默认情况下，禁用用户通知。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

注意：对于 Virtual Delivery Agent 7.x，仅当启用 旧图形模式策略设置时，才会应用此策略设置。
此设置放弃由其他图像替代的排队图像。

默认情况下，启用排队与丢弃。

这将改进向用户设备发送图片时的响应速度。配置此设置会导致由于丢弃帧而使动画断断续续。

允许视频解码在端点上可用时使用视频编解码器 (H.264) 压缩图形。选中**针对整个屏幕**时，视频编解码器将用作所有项的默认编解码器。选中**针对主动变化的区域**时，视频编解码器将用于屏幕上存在不断变化的区域，其他数据将使用静态图像压缩和位图缓存。视频解码在端点上不可用时，或者当您指定了**不使用**时，将同时使用静态图像压缩和位图缓存。选中了**偏好时使用视频编解码器**时，系统会基于各种因素进行选择。结果可能会因版本而异，因为选择方法已得以增强。

选择**偏好时使用视频编解码器**以允许系统尽可能为当前场景选择适合的设置。

选择**针对整个屏幕**以针对改进用户体验和带宽使用情况进行优化，尤其是在大量使用服务器端呈现的视频和 3D 图形的情况下。

选择**针对主动变化的区域**以针对改进视频性能进行优化（尤其是低带宽的性能），同时维持静态和缓慢变化的内容的可扩展性。多显示器部署中支持此设置。

选择**不使用视频编解码器**以优化服务器 CPU 负载和改善不大量使用服务器端呈现的视频或其他图形密集型应用程序的情况的性能。

默认为**偏好时使用视频编解码器**。

此设置允许使用图形硬件（如果可用）并采用视频 (H.264) 编解码器来压缩屏幕元素。如果此类硬件不可用，VDA 会转而求助于使用软件视频编解码的基于 CPU 的编码。

此策略设置的默认选项为**启用**。

支持使用多个显示器。

任何支持 H.264 解码的 Citrix Receiver 均可随 NVENC 硬件编码一起使用。

支持有损 (4:2:0) 压缩和视觉无损 (4:4:4) 压缩。视觉无损（图形策略设置，允许视觉无损压缩）要求使用 Receiver for Windows 4.5 或更高版本。

NVIDIA

对于 NVIDIA GRID GPU，HDX 3D Pro 模式下的 VDA for Desktop OS 支持硬件编码。

NVIDIA GPU 必须支持 NVENC 硬件编码。请参阅 NVIDIA 视频编解码器 SDK 获取受支持的 GPU 列表。

NVIDIA GRID 要求使用 3.1 或更高版本的驱动程序。NVIDIA Quadro 要求使用 362.56 或更高版本的驱动程序。Citrix 推荐使用 NVIDIA Release R361 分支版中的驱动程序。

无损文本是按标准模式（而非 HDX 3D Pro）配置的 VDA 的一个功能，该功能与 NVENC 硬件编码不兼容。如果已经按 HDX 3D Pro 模式启用了无损文本，该功能的优先级会高于 NVENC 硬件编码。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

不支持针对主动变化的区域选择性地使用 H.264 硬件编解码器。

Intel

对于 Intel Iris Pro 图形处理器，VDA for Desktop OS（标准模式或 HDX 3D Pro 模式下）和 VDA for Server OS 支持硬件编码。

支持 Intel Broadwell 处理器系列及更高系列中的 Intel Iris Pro 图形处理器。需要 Intel Iris Pro 硬件编码器 SDK，可从 Intel Web 站点下载：Remote Displays SDK。

支持无损文本。

支持针对主动变化的区域选择性地使用 H.264 硬件编解码器。

Windows 10 和 Windows Server 2012 及更高版本支持。

在 3D Pro 模式下的 VDA 上，Intel 编码器在最多有八个编码会话时（例如，使用八台显示器的一个用户或各使用一台显示器的八个用户）可提供良好的用户体验。如果需要的编码会话超过八个，请检查虚拟机连接的显示器数量。为了保持良好的用户体验，管理员可以决定按每个用户或每台计算机配置此策略设置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

缓存策略设置

Dec 05, 2017

“缓存”部分 包含能够在客户端连接的带宽受限时， 在用户设备上缓存图像数据的策略设置。

注意：对于 Virtual Delivery Agent 7.x，仅当启用“旧图形模式”策略设置时，才会应用此策略设置。
此设置用于在用户设备的硬盘驱动器上缓存位图。 通过这种方式，可以重复使用之前会话中频繁使用的大型图像。

默认情况下，该阈值为 3000000 bps。

该阈值表示永久性缓存功能生效的上限点。 例如，使用默认值时，当带宽低于 3000000 bps 时，将在用户设备的硬盘驱动器上缓存位图。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Framehawk 策略设置

Dec 05, 2017

Framehawk 部分包含用于在服务器上启用和配置 Framehawk 显示通道的策略设置。

Framehawk 显示通道

启用后，服务器将尝试为用户的图形和远程输入处理使用 Framehawk 显示通道。此显示通道将使用 UDP 在具有高损失和高延迟特征的网络上提供更好的用户体验；但是，相对于其他图形模式，它可能会占用更多的服务器资源和带宽。

默认情况下，禁用 Framehawk 显示通道。

Framehawk 显示通道端口范围

此策略设置指定 VDA 用于与用户设备交换 Framehawk 显示通道数据的 UDP 端口范围（格式为*最低端口号,最高端口号*）。VDA 会尝试使用每个端口，从最低端口号开始，后面每次尝试都增加端口号。端口处理入站和出站通信。

默认情况下，端口范围为 3224,3324。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

保持活动状态策略设置

Dec 05, 2017

“保持活动状态” 部分包含用于管理 ICA 保持活动状态消息的策略设置。

ICA 保持活动状态超时

此设置指定相邻 ICA 保持活动状态消息之间间隔的秒数。

默认情况下，保持活动状态消息之间的间隔是 60 秒。

可为 ICA 保持活动状态消息的发送间隔指定 1 到 3600 秒之间的一个值。 如果您的网络监视软件负责关闭非活动连接，则不要配置此设置。

ICA 保持活动状态

此设置允许或禁止定期发送 ICA 保持活动状态消息。

默认情况下，不发送 ICA 保持活动状态消息。

启用此设置可防止中断的连接被断开连接。 如果服务器检测不到活动，此设置可防止远程桌面服务 (RDS) 断开会话连接。 服务器将每隔几秒钟发送一次保持活动状态消息，以检测会话是否处于活动状态。 如果会话不再处于活动状态，服务器会将该会话标记为已断开连接。

ICA 保持活动状态在使用会话可靠性时将无效。 请仅为不使用会话可靠性的连接配置 ICA 保持活动状态。

相关策略设置： 会话可靠性连接。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

本地应用程序访问策略设置

Dec 05, 2017

“本地应用程序访问” 部分包含的策略设置可管理在托管桌面环境中用户 本地安装的应用程序与托管应用程序的 集成。

允许本地应用程序访问

此设置允许或阻止托管桌面环境中用户本地安装的应用程序与托管应用程序的集成。

当用户启动本地安装的应用程序时，即使其实际上是在本地运行，也会看起来是在其虚拟桌面上运行。

默认情况下，禁止本地应用程序访问。

URL 重定向黑名单

此设置指定被重定向到本地 Web 浏览器并在其中启动的 Web 站点。 这可能包括需要区域设置信息的 Web 站点（如 msn.com 或 newsgoogle.com），或者包含可更好地呈现在用户设备上的富媒体内容的 Web 站点。

默认情况下，不指定任何站点。

URL 重定向白名单

此设置指定在其启动环境中呈现的 Web 站点。

默认情况下，不指定任何站点。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

移动体验策略设置

Dec 05, 2017

“移动体验”部分包含用于处理 Citrix Mobility Pack 的策略设置。

自动显示键盘

此设置用于启用或禁用移动设备屏幕上的键盘自动显示功能。

默认情况下，键盘的自动显示功能处于禁用状态。

启动触控优化桌面

此设置已禁用，不适用于 Windows 10 或 Windows Server 2016 计算机。

此设置通过允许或禁止使用为平板电脑设备优化的触控友好界面，控制 Citrix Receiver 的整体界面行为。

默认情况下，将使用触控友好界面。

如果仅使用 Windows 界面，请将此策略设置为“禁止”。

远程控制组合框

此设置确定移动设备上的会话中可显示的组合框类型。要显示设备本机组合框控件，请将此策略设置为允许。此设置为允许时，用户可以将 Citrix Receiver for iOS 会话的设置更改为使用 Windows 组合框。

默认情况下，禁止使用远程控制组合框的功能。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

多媒体策略设置

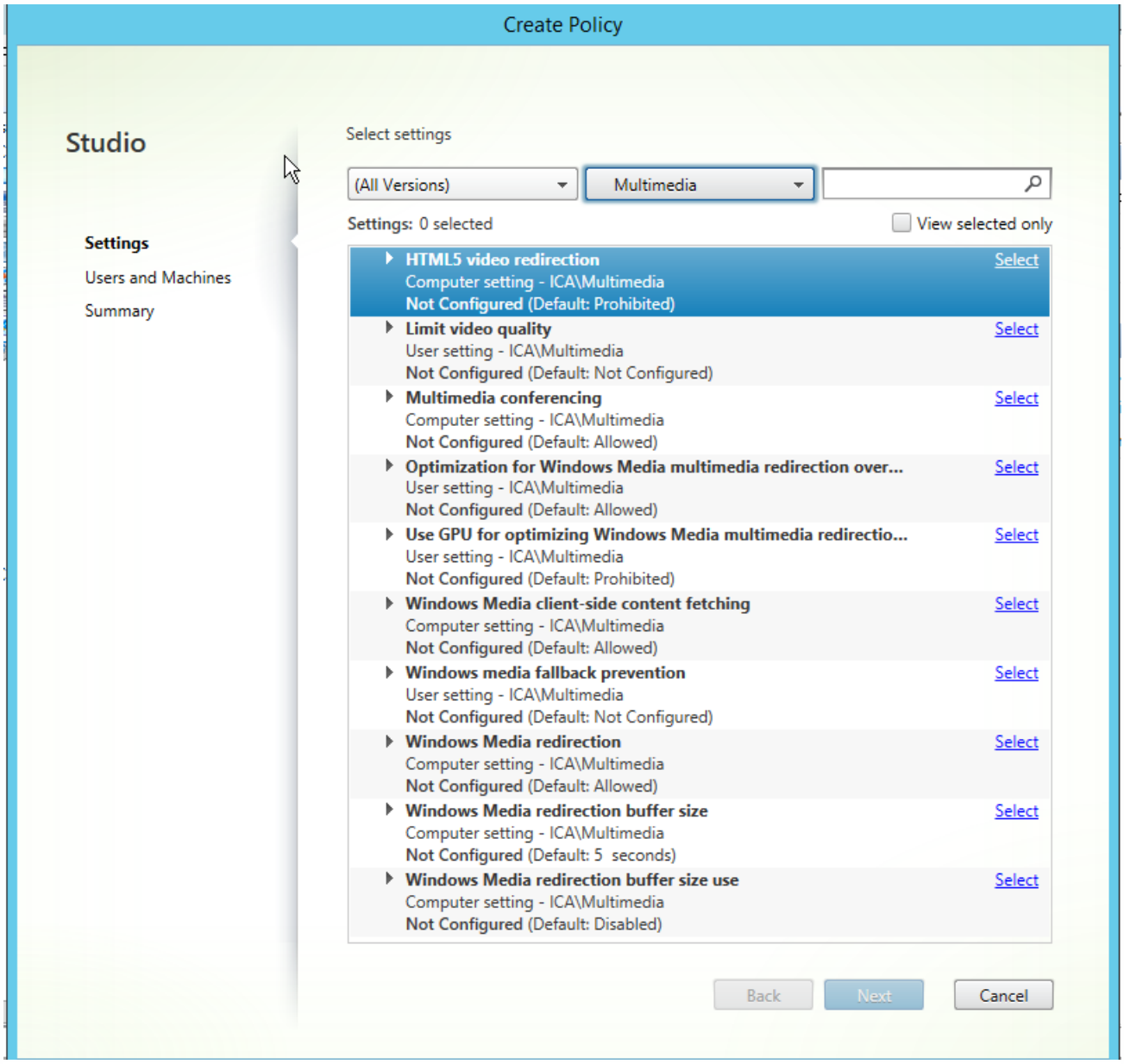
Jan 05, 2018

“多媒体”部分包含用于管理用户会话中的流 HTML5 和 Windows 音频和视频的策略设置。

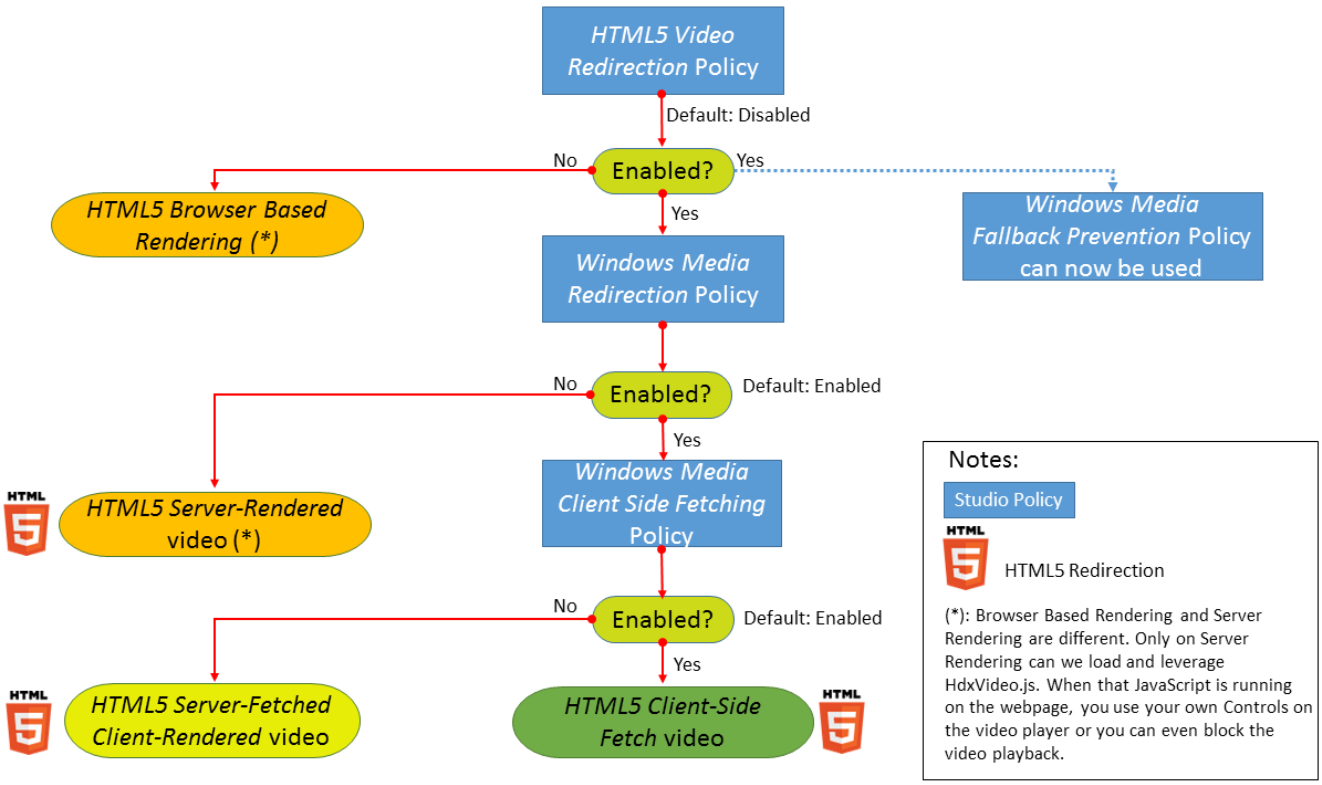
HTML5 视频重定向

控制和优化 XenApp 和 XenDesktop 服务器向用户交付 HTML5 多媒体 Web 内容的方式。

默认情况下，禁用此设置。



© 1999-2017 Citrix Systems, Inc. All rights reserved.



在此版本中，此功能仅用于受控 Web 页面。它要求向提供 HTML5 多媒体内容（例如，内部培训站点上的视频）的 Web 页面添加 JavaScript。

配置 HTML5 视频重定向：

1. 将文件 **HdxVideo.js** 从 VDA 安装上的 %Program Files%/Citrix/ICA Service/HTML5 Video Redirection 复制到您的内部 Web 页面位置。
2. 将此行插入您的 Web 页面（如果您的 Web 页面有其他脚本，请将 **HdxVideo.js** 放在那些脚本之前）：

注意：如果 HdxVideo.js 与您的 Web 页面不在同一位置，请使用 **src** 属性指定其完整路径。

如果未将 JavaScript 添加到您的受控 Web 页面且用户播放 HTML5 视频，则 XenApp 和 XenDesktop 将默认进行服务器端呈现。

为了能够重定向 HTML5 视频，请允许 ***Windows Media 重定向***。要进行服务器提取客户端呈现，必需此策略，要进行客户端提取，需要此策略（进而还要求允许 *Windows Media 客户端内容提取*）。

Microsoft Edge 不支持此功能。

HdxVideo.js 会将浏览器 HTML5 播放器控件替换为自己的控件。要检查 HTML5 视频重定向策略是否在某个特定 Web 站点上生效，请将播放器控件与禁止 ***HTML5 视频重定向***策略的情况进行比较：

（允许该策略时的 Citrix 自定义控件）



© 1999-2017 Citrix Systems, Inc. All rights reserved.

（禁止或未配置该策略时的原始 Web 页面控件）



支持以下视频控制功能：

- 播放
- 暂停
- 搜寻
- 重复
- 音频
- 全屏

您可以查看 HTML5 视频重定向测试页面：https://www.citrix.com/virtualization/hdx/html5-redirect.html。

TLS 和 HTML5 视频重定向

可以使用 HTML5 视频重定向来重定向 HTTPS Web 站点。注入到这些 Web 站点的 JavaScript 必须与 VDA 上运行的 Citrix HDX HTML5 视频重定向服务 (WebSocketService.exe) 建立 TLS 连接。为了实现此重定向并维护 Web 页面的 TLS 完整性，Citrix HDX HTML5 视频重定向服务将在 VDA 上的证书存储中生成两个自定义证书。

HdxVideo.js 使用安全的 Websocket 与 VDA 上运行的 WebSocketService.exe 进行通信。此过程在本地系统中运行，并执行 SSL 终止和用户会话映射。

WebSocketService.exe 在 127.0.0.1 端口 9001 上进行侦听。

限制视频质量

此设置仅适用于 Windows Media，而不适用于 HTML5。它要求您启用*在 WAN 中对 Windows Media 多媒体重定向进行优化*。

此设置指定 HDX 连接允许使用的最大视频质量级别。配置后，最大视频质量将限制为指定值，确保在环境中保持多媒体服务质量 (QoS)。

默认情况下未配置此设置。

要限制允许使用的最大视频质量级别，请选择以下任一选项：

- 1080p/8.5mbps
- 720p/4.0mbps
- 480p/720kbps
- 380p/400kbps
- 240p/200kbps

在同一台服务器上同时播放多个视频会消耗大量资源，并且可能影响服务器的可扩展性。

多媒体会议

此设置允许或阻止视频会议应用程序使用优化的网络摄像机重定向技术。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

默认情况下，允许视频会议支持。

将此设置添加到某个策略时，请确保“Windows Media 重定向”设置存在，并且设置为“允许”（默认设置）。

使用多媒体会议时，请确保满足以下条件：

- 在客户端上安装了制造商为用于多媒体会议的网络摄像机提供的驱动程序。
- 先将网络摄像机连接到用户设备，然后再启动视频会议会话。服务器在任何给定的时间只使用一个已安装的网络摄像机。如果用户设备上安装了多个网络摄像机，服务器会依次尝试使用每个网络摄像机，直至成功创建视频会议会话。

使用通用 USB 重定向对网络摄像机进行重定向时，不需要此策略。在这种情况下，请在 VDA 上安装网络摄像机驱动程序。

在 WAN 中对 Windows Media 多媒体重定向进行优化

此设置仅适用于 Windows Media，而不适用于 HTML5。该设置支持实时多媒体代码转换，允许在状况不佳的网络中通过流技术将音频和视频媒体推送到移动设备，并利用改善通过 WAN 交付 Windows Media 内容的方式增强了用户体验。

默认情况下，已优化通过 WAN 的 Windows Media 内容交付。

将此设置添加到策略时，请确保 **Windows Media 重定向**设置存在，且设置为**允许**。

启用此设置后，将根据需要自动部署实时多媒体代码转换以启用媒体流，因此即使在恶劣的网络条件下也可以提供无缝用户体验。

使用 GPU 优化 WAN 中的 Windows Media 多媒体重定向

此设置仅适用于 Windows Media，并支持在 Virtual Delivery Agent (VDA) 上的图形处理器 (GPU) 中执行实时多媒体代码转换。这会改善服务器可扩展性。仅在 VDA 具有支持硬件加速的 GPU 时，GPU 代码转换才可用。否则，代码转换将回退到 CPU。

注意：只有 NVIDIA GPU 支持 GPU 代码转换。

默认情况下，禁止使用 VDA 上的 GPU 通过 WAN 优化 Windows Media 内容交付。
将此设置添加到策略后，请确保 Windows Media 重定向和在 WAN 中对 Windows Media 多媒体重定向进行优化设置存在，且设置为允许。

Windows Media 回退预防

此设置适用于 HTML5 和 Windows Media。为了此设置适用于 HTML5，请将 ***HTML 视频重定向***策略设置为**允许**。

管理员可以使用 Windows Media 回退预防策略设置指定向用户交付流内容时尝试使用的方法。

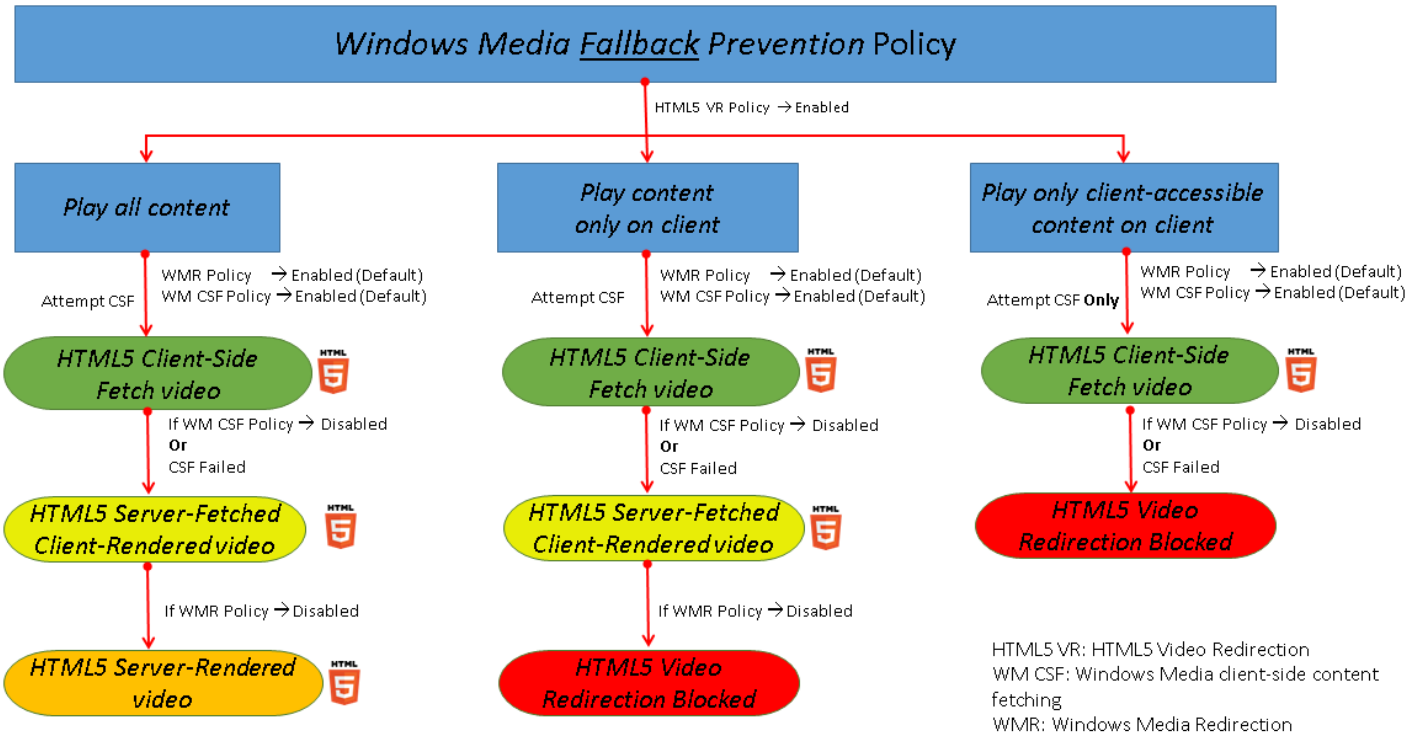
默认情况下未配置此设置。该设置设为“未配置”时，行为与**播放所有内容**相同。

要配置此设置，请选择以下选项之一：

- **播放所有内容**。尝试执行客户端内容提取，然后执行 Windows Media 重定向。如果不成功，则在服务器上播放内容。
- **仅在客户端上播放所有内容**。尝试执行客户端提取，然后执行 Windows Media 重定向。如果不成功，则不播放内容。
- **仅在客户端上播放客户端可访问的内容**。仅尝试执行客户端提取。如果不成功，则不播放内容。

内容不播放时，播放器窗口会显示错误消息“由于缺少资源，因此公司阻止了该视频”（默认持续时间为 5 秒）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



可以通过 VDA 上的以下注册表项自定义此错误消息的持续时间。如果该注册表项不存在，持续时间将默认为 5 秒。

> **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。

注册表路径因 VDA 的体系结构而异：

\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream

或者

\HKLM\SOFTWARE\Citrix\HdxMediastream

注册表项：

名称：VideoLoadManagementErrDuration

类型：DWORD

范围： 1 - 最大 DWORD 限制（默认值 = 5）

单位：秒

Windows Media 客户端内容提取

此设置适用于 HTML5 和 Windows Media。该设置支持用户设备能够通过流技术直接从 Internet 或 Intranet 上的源提供程序

© 1999-2017 Citrix Systems, Inc. All rights reserved.

推送多媒体文件，而非通过 XenApp 或 XenDesktop 主机服务器推送。

默认情况下，此设置为**允许**。允许此设置后，可将对媒体的任何处理过程从主机服务器转到用户设备，提高了网络使用和服务器可扩展性。此外，还不需要在用户设备上安装 Microsoft DirectShow 或媒体基础等高级多媒体框架。用户设备只需要能够播放 URL 中的文件。

将此设置添加到策略时，请确保 **Windows Media 重定向**设置存在，且设置为**允许**。如果禁用 **Windows Media 重定向**，也会禁用通过流技术将多媒体文件直接从源提供程序推送到用户设备。

Windows Media 重定向

此设置适用于 HTML5 和 Windows Media，并可控制和优化服务器向用户交付流音频和视频的方式。

默认情况下，此设置为**允许**。对于 HTML5，如果策略 ***HTML5 视频重定向*** 为**禁止**，此设置将无法生效。

允许此设置后，可将服务器上呈现的音频和视频质量提高到一个级别，可与用户设备上本地播放的音频和视频质量相媲美。服务器会将多媒体以原始压缩格式通过流技术推送到客户端，并允许用户设备解压缩和呈现该媒体。

Windows Media 重定向可优化使用编解码器编码的多媒体文件，这些编解码器遵循 Microsoft DirectShow、DirectX 媒体对象 (DMO) 和媒体基础标准。要播放给定的多媒体文件，用户设备上必须存在与多媒体文件的编码格式兼容的编解码器。

默认情况下，在 Citrix Receiver 上禁用音频。要允许用户在 ICA 会话中运行多媒体应用程序，请打开音频或授予用户在其 Citrix Receiver 接口上自行打开音频的权限。

仅当使用 Windows Media 重定向播放媒体的效果比使用基本 ICA 压缩和常规音频所呈现的效果差时，才选择**已禁止**。这种情况很少见，但在带宽较低的情况下可能会发生。例如，当播放关键帧的频率非常低的媒体时。

Windows Media 重定向缓冲区大小

此设置是一个旧设置，不适用于 HTML5。

此设置为多媒体加速指定 1 到 10 秒的缓冲区大小。

默认情况下，缓冲区大小为 5 秒。

Windows Media 重定向缓冲区大小的使用

此设置是一个旧设置，不适用于 HTML5。

此设置启用或禁用使用 **Windows Media 重定向缓冲区大小**设置中所指定的缓冲区大小。

默认情况下，不使用指定的缓冲区大小。

如果禁用此设置，或如果未配置“Windows Media 重定向缓冲区大小”设置，服务器将使用默认缓冲区大小值（5 秒）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

多流连接策略设置

Dec 05, 2017

“多流连接”部分中包含的策略设置可用于在一个会话中管理多个 ICA 连接的服务质量 (QoS) 优先级顺序。

通过 UDP 传输音频

此设置允许或阻止在服务器上通过 UDP 传输音频。

默认情况下，允许在服务器上通过 UDP 传输音频。

启用后，此设置在服务器上打开一个 UDP 端口以支持配置为使用“通过 UDP 实时传输音频”的所有连接。

音频 UDP 端口范围

此设置指定 Virtual Delivery Agent (VDA) 用来与用户设备交换音频数据包数据的端口号范围（采用 lowest port number,highest port number 形式）。 VDA 尝试使用每个 UDP 端口对与用户设备交换数据，从最小端口号开始尝试，之后每尝试一次，端口号增加 2。 每个端口可同时处理入站和出站通信。

默认情况下，此项设置为 16500,16509。

多端口策略

此设置指定用于 ICA 通信的 TCP 端口并为每个端口建立网络优先级。

默认情况下，主端口 (2598) 拥有“高”优先级。

配置端口时，可以分配以下优先级：

- 很高 - 适用于实时活动，例如视频会议。
- 高 - 适用于交互元素，例如屏幕、键盘和鼠标
- 中 - 适用于批量进程，例如客户端驱动器映射
- 低 - 适用于后台活动，例如打印

每个端口必须有唯一的优先级。 例如，不能同时为 CGP 端口 1 和 CGP 端口 3 分配“很高”优先级。

要从优先级顺序中删除某个端口，请将其端口号设置为 0。 您无法删除主端口，也无法修改其优先级。

配置此设置时，请重新启动服务器。 只有启用了 多流计算机设置策略设置时，此设置才会生效。

多流计算机设置

此设置在服务器上启用或禁用“多流”功能。

默认情况下，禁用“多流”功能。

如果要在环境中使用具有“多流”支持功能的 Citrix NetScaler SD-WAN，则无需配置此设置。如果要使用第三方路由器或旧版 Branch Repeater 实现所需的服务质量 (QoS)，应配置此策略。

配置此策略时，应重新启动服务器以确保所做的更改生效。
重要：将此策略设置与带宽限制策略设置（例如总会话带宽限制）结合使用可能会产生意外结果。如果要在策略中包含此设置，请确保将带宽限制设置排除在外。

多流用户设置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

此设置在用户设备上启用或禁用“多流”功能。

默认情况下，对所有用户禁用“多流”功能。

只有在启用了 多流计算机设置策略设置的主机上，此设置才会生效。
重要：将此策略设置与带宽限制策略设置（例如 总会话带宽限制）结合使用可能会产生意外结果。 如果要在策略中包含此设置，请确保将带宽限制设置排除在外。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

端口重定向策略设置

Dec 05, 2017

端口重定向部分包含用于客户端 LPT 和 COM 端口映射的策略设置。

对于 **7.0 之前**的 Virtual Delivery Agent 版本，请使用以下策略设置来配置端口重定向。对于 VDA 版本 **7.0 至 7.8**，请使用注册表来配置这些设置；请参阅使用注册表配置 COM 端口和 LPT 端口重定向设置。对于 VDA **7.9** 版本，请使用以下策略设置。

自动连接客户端 COM 端口

此设置启用或禁用用户登录到站点时用户设备上 COM 端口的自动连接。

默认情况下，不自动连接客户端 COM 端口。

自动连接客户端 LPT 端口

此设置启用或禁用用户登录到站点时用户设备上 LPT 端口的自动连接。

默认情况下，不自动连接客户端 LPT 端口。

客户端 COM 端口重定向

此设置允许或阻止访问用户设备上的 COM 端口。

默认情况下，禁止 COM 端口重定向。

下列策略设置为相关设置：

- COM 端口重定向带宽限制
- COM 端口重定向带宽限制百分比

客户端 LPT 端口重定向

此设置允许或阻止访问用户设备上的 LPT 端口。

默认情况下，禁止 LPT 端口重定向。

只有将打印作业发送至 LPT 端口（而非发送至用户设备上的打印对象）的旧版应用程序才可使用 LPT 端口。目前大多数应用程序都可将打印作业发送至打印机对象。只有用于托管打印至 LPT 端口的旧版应用程序的服务器，才有必要使用此策略设置。

请注意，虽然客户端 COM 端口重定向是双向的，但是在 ICA 会话中仅会输出 LPT 端口，并重定向到 \\client\LPT1 和 \\client\LPT2。

下列策略设置为相关设置：

- LPT 端口重定向带宽限制
- LPT 端口重定向带宽限制百分比

© 1999-2017 Citrix Systems, Inc. All rights reserved.

打印策略设置

Dec 05, 2017

“打印”部分包含用于管理客户端打印的策略设置。

客户端打印机重定向

此设置控制在用户登录到会话时客户端打印机是否映射到服务器。

默认情况下，允许客户端打印机映射。如果禁用此设置，则不会自动创建会话的 PDF 打印机。

相关策略设置：自动创建客户端打印机

默认打印机

此设置指定在会话中如何在用户设备上建立默认打印机。

默认情况下，用户的当前打印机用作会话的默认打印机。

要为默认打印机使用当前的远程桌面服务或 Windows 用户配置文件设置，请选择 不调整用户的默认打印机。如果选择此选项，默认打印机将不会保存在用户配置文件中，并且不会随其他会话或客户端属性而改变。会话中的默认打印机将是该会话中自动创建的第一个打印机，可以是：

- 第一台通过 控制面板 > 设备和打印机添加到 Windows 服务器的本地打印机。
- 第一台自动创建的打印机（如果没有向服务器添加任何本地打印机）。

可以使用此选项通过配置文件设置向用户呈现最近的打印机（即邻近打印）。

打印机分配

此设置是 默认打印机和 会话打印机设置的一个替代方案。使用单独的 默认打印机和 会话打印机设置对站点、大型组或组织单位的行为进行配置。使用打印机分配设置，可以将大型的打印机组分配给多个用户。

此设置指定在会话中如何在所列的用户设备上建立默认打印机。

默认情况下，用户的当前打印机用作会话的默认打印机。

该设置还指定了在会话中将为每个用户设备自动创建的网络打印机。默认情况下，不指定任何打印机。

- 在设置默认打印机的值时：
  要使用用户设备当前默认的打印机，请选择 不调整。

  要使用默认打印机当前的远程桌面服务或 Windows 用户配置文件设置，请选择 不调整。如果选择此选项，默认打印机将不会保存在用户配置文件中，并且不会随其他会话或客户端属性而改变。会话中的默认打印机将是该会话中自动创建的第一个打印机，可以是：

  - 第一台通过 控制面板 > 设备和打印机添加到 Windows 服务器的本地打印机。
  - 第一台自动创建的打印机（如果没有向服务器添加任何本地打印机）。
- 设置会话打印机值时：要添加打印机，请键入要自动创建的打印机的 UNC 路径。添加打印机后，可以在每次登录时为当前会话应用自定义设置。

打印机自动创建事件日志首选项

© 1999-2017 Citrix Systems, Inc. All rights reserved.

此设置指定在打印机自动创建过程中记录哪些事件。可以选择不记录错误或警告、只记录错误或者记录错误和警告。

默认情况下，记录错误和警告。

以下事件就是警告示例：未能安装打印机的本机驱动程序，而是安装了通用打印驱动程序。要在此情形中使用通用打印驱动程序，可将 通用打印驱动程序用法设置配置为 仅使用通用打印或 仅当请求的驱动程序不可用时才使用通用打印。

会话打印机

此设置指定在会话中将自动创建的网络打印机。

默认情况下，不指定任何打印机。

要添加打印机，请键入要自动创建的打印机的 UNC 路径。添加打印机后，可以在每次登录时为当前会话应用自定义设置。

等待创建打印机(服务器桌面)

此设置允许或阻止连接到会话时发生延迟，此延迟便于自动创建服务器桌面打印机。

默认情况下不发生连接延迟。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

客户端打印机策略设置

Dec 05, 2017

“客户端打印机” 部分包含用于客户端打印机的策略设置（包括 自动创建客户端打印机、保留打印机属性以及连接到打印 服务器的设置）。

自动创建客户端打印机

此设置指定自动创建的客户端打印机。此设置可覆盖默认的客户端打印机自动创建设置。

默认情况下，所有客户端打印机都是自动创建的。

仅当客户端打印机重定向设置存在，且设置为允许时，此设置才能生效。

将此设置添加到策略时，请选择一个选项：

- 自动创建所有客户端打印机可在用户设备上自动创建所有打印机。
- 仅自动创建客户端的默认打印机仅自动创建选择作为用户设备上的默认打印机的打印机。
- 仅自动创建本地(非网络)客户端打印机将仅自动创建通过 LPT、COM、USB、TCP/IP 或其他本地端口直接连接到用户设备的打印机。
- 不自动创建客户端打印机在用户登录时关闭所有客户端打印机的自动创建功能。这会导致在优先级较低的策略中，以自动创建客户端打印机的远程桌面服务 (RDS) 设置覆盖此设置。

自动创建一般通用打印机

注意：用于解决此策略设置问题的修补程序以知识库文章 CTX141565 和 CTX141566 的方式提供。
此设置启用或禁用为所使用的用户设备与通用打印兼容的会话自动创建一般 Citrix 通用打印机对象。

默认情况下，不自动创建一般通用打印机对象。

下列策略设置为相关设置：

- 通用打印驱动程序用法
- 通用驱动程序首选项

客户端打印机名称

此设置为自动创建的客户端打印机选择命名约定。

默认情况下，使用标准打印机名称。

选择标准打印机名称可使用诸如“HPLaserJet 4 from clientname in session 3”之类的打印机名称。

选择旧版打印机名称可让使用 MetaFrame Presentation Server 3.0 或较旧版本的用户或组使用旧版客户端打印机名称并保留向后兼容性。旧版打印机名称示例：“Client/clientname#/HPLaserJet 4”。此选项不够安全。
注意：仅提供此选项以用于向后兼容旧版 XenApp 和 XenDesktop。

直接连接到打印服务器

此设置为可访问的网络共享上托管的客户端打印机启用或禁用从托管应用程序的虚拟桌面或服务器到打印服务器的直接连接。

默认情况下，启用直接连接。

如果托管应用程序的虚拟桌面或服务器未通过 WAN 与网络打印服务器连接，请启用直接连接。 如果网络打印服务器和托管应用程序的虚拟桌面或服务器位于相同的 LAN，那么直接通信可加快打印速度。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

如果网络通过 WAN、延迟较大或者带宽有限，请禁用直接连接。 打印作业通过将其重定向到网络打印服务器的用户设备进行路由。 发送到用户设备的数据会经过压缩，因此通过 WAN 传输数据会占用较少的带宽。

如果存在两台同名的网络打印机，则会使用与用户设备位于相同网络的打印机。

打印机驱动程序映射和兼容性

此设置为自动创建的客户端打印机指定驱动程序替换规则。

此设置配置为从自动创建的客户端打印机列表中排除 Microsoft OneNote 和 XPS Document Writer。

定义驱动程序替代规则时，可以允许或禁止使用指定的驱动程序创建打印机。此外，可以允许创建的打印机仅使用通用打印驱动程序。驱动程序替换将覆盖或映射用户设备提供的打印机驱动程序名称，从而替换服务器上的等效驱动程序。这样可使服务器应用程序有权访问与服务器具有相同驱动程序，但驱动程序名称不同的客户端打印机。

可以添加驱动程序映射，编辑现有映射，覆盖映射的自定义设置，删除映射或更改驱动程序条目在列表中的顺序。添加映射时，请输入客户端打印机驱动程序名称，然后选择要替换的服务器驱动程序。

打印机属性保留

此设置指定是否存储打印机属性以及打印机属性的存储位置。

默认情况下，系统会决定是将打印机属性存储在用户设备上（如果有），还是存储在用户配置文件中。

将此设置添加到策略时，请选择一个选项：

- 仅保存在客户端 设备上适用于拥有不保存的强制配置文件或漫游配置文件的用户设备。 仅当场中的所有服务器都运行 XenApp 5 及更高版本，并且用户使用 Citrix 联机插件 9 至 12.x 版或使用 Citrix Receiver 3.x 时，才选择此选项。
- 仅保留在用户 配置文件中适用于受带宽（此选项会减少网络流量）和登录速度限制的用户设备，或适用于使用旧插件的用户。 此选项将打印机属性存储在服务器上的用户配置文件中，并阻止与用户设备交换任何属性。 如果使用 MetaFrame Presentation Server 3.0 或更低版本和 MetaFrame Presentation Server Client 8.x 或更低版本，请使用此选项。 请注意，此选项仅在使用远程桌面服务 (RDS) 漫游配置文件时适用。
- 仅当未保存在客户端时才 保留在配置文件中允许系统决定打印机属性的存储位置。 打印机属性会存储在用户设备上（如果有）或用户配置文件中。 虽然此选项最为灵活，但也会延长登录时间，且需要使用额外的带宽执行系统检查。
- 不保留打印机 属性将阻止存储打印机属性。

保留和恢复的客户端打印机

此设置启用或禁用在用户设备上保留和重新创建打印机。 默认情况下，自动保留和自动恢复客户端打印机。

保留的打印机属于用户创建的打印机，在下一个会话启动时会再次创建（或被记住）。 XenApp 重新创建保留的打印机时，它会考虑使用除 自动创建客户端打印机设置以外的所有策略设置。

恢复的打印机属于管理员完全自定义的打印机，其保存状态为永久连接到客户端端口。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

驱动程序策略设置

Dec 05, 2017

“驱动程序”部分 包含与打印机驱动程序有关的策略设置。

自动安装现成的打印机驱动程序

此设置启用或禁用从 Windows 现成驱动程序集或从使用 pnputil.exe /a 在主机上暂存的驱动程序包来自动安装打印机驱动程序。

默认情况下，会根据需要安装这些驱动程序。

通用驱动程序首选项

此设置指定使用通用打印机驱动程序的顺序，从列表中的第一个条目开始。

默认情况下，首选顺序为：

- EMF
- XPS
- PCL5c
- PCL4
- PS

可以在列表中添加、编辑或删除驱动程序，以及更改驱动程序的顺序。

通用打印驱动程序用法

此设置指定何时使用通用打印。

默认情况下，仅当请求的驱动程序不可用时才使用通用打印。

通用打印使用一般打印机驱动程序而不是特定于型号的标准驱动程序，从而潜在地减轻了在主机计算机上管理驱动程序的负担。 通用打印驱动程序的可用性取决于用户设备、主机和打印服务器软件的功能。 在某些配置中，通用打印可能不可用。

将此设置添加到策略时，请选择一个选项：

- 仅使用特定于打印机型号的 驱动程序指定客户端打印机仅使用在登录时自动创建的特定于打印机型号的 标准驱动程序。如果请求的驱动程序不可用，将无法自动创建客户端打印机。
- 仅使用通用 打印指定不使用特定于型号的标准驱动程序。 仅使用通用打印驱动程序创建打印机。
- 仅当请求的驱动程序不可用时 才使用通用打印使用标准的特定于打印机型号的 驱动程序来创建打印机（如果这些驱动程序可用）。如果该驱动程序在服务器上不可用，则使用合适的通用驱动程序自动创建客户端打印机。
- 仅当通用打印不可用时 才使用打印机型号专用的驱动程序在通用打印驱动程序可用时 将使用此驱动程序如果该驱动程序在服务器上不可用，则使用特定于型号的合适打印机驱动程序来自动创建客户端打印机。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

通用打印服务器策略设置

Dec 05, 2017

“通用打印 服务器”部分包含用于处理通用打印 服务器的策略设置。

启用通用打印服务器

此设置启用或禁用托管应用程序的虚拟桌面或服务器上的“通用打印服务器”功能。 此策略设置适用于包含托管应用程序的虚拟桌面或服务器的组织单位 (OU)。

默认情况下，通用打印服务器处于禁用状态。

将此设置添加到策略时，请选择以下选项之一：

- **已启用并回退到 Windows 的本机远程打印**。通用打印服务器将在可能的情况下提供网络打印机连接服务。 如果通用打印服务器不可用，将使用 Windows 打印提供程序。 Windows 打印提供程序将继续处理之前使用 Windows 打印提供程序创建的所有打印机。
- **已启用但不回退到 Windows 的本机远程打印**。通用打印服务器将独自提供网络打印机连接服务。 如果通用打印服务器不可用，网络打印机连接将失败。 此设置可以有效禁用通过 Windows 打印提供程序进行的网络打印。 当启用了包含此设置的策略时，将不会创建之前曾使用 Windows 打印提供程序创建的打印机。
- **已禁用**。禁用通用打印服务器功能。 在连接到具有 UNC 名称的网络打印机时，不会尝试连接通用打印服务器。 与远程打印机的连接将继续使用 Windows 本机远程打印工具。

通用打印服务器打印数据流(CGP)端口

此设置指定通用打印服务器的打印数据流通用网关协议 (CGP) 侦听器使用的 TCP 端口号。 此策略设置仅适用于包含打印服务器的 OU。

默认情况下，此端口号设置为 7229。

有效的端口号必须在 1 到 65535 范围内。

通用打印服务器打印流输入带宽限制(kbps)

此设置指定每个打印作业使用 CGP 向通用打印服务器传输打印数据的速率上限值 (Kbps)。 此策略设置适用于包含托管应用程序的虚拟桌面或服务器的 OU。

默认值为 0，表示不指定上边界。

通用打印服务器 Web 服务(HTTP/SOAP)端口

此设置用于指定通用打印服务器的 Web 服务 (HTTP/SOAP) 侦听器所使用的 TCP 端口号。通用打印服务器是一个可选组件，允许将 Citrix 通用打印驱动程序用于网络打印场景。在使用通用打印服务器时，打印命令将从 XenApp 和 XenDesktop 主机通过 SOAP over HTTP 发送到通用打印服务器。此设置将修改通用打印服务器侦听传入的 HTTP/SOAP 请求所使用的默认 TCP 端口。

必须配置相同的主机和打印服务器 HTTP 端口。如果配置的端口不相同，主机软件将连接不到通用打印服务器。此设置更改 XenApp 和 XenDesktop 上的 VDA。此外，还必须更改通用打印服务器上的默认端口。

默认情况下，此端口号设置为 8080。

有效端口号必须在 0 到 65535 范围内。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

用于负载平衡的通用打印服务器

此设置列出了在评估其他 Citrix 打印策略设置后，用于对会话启动时建立的打印机连接执行负载平衡的通用打印服务器。为了优化打印机创建时间，Citrix 建议所有打印服务器具有相同的共享打印机集合。对于可添加以用于负载平衡的打印服务器数量而言，没有上限。

此设置还可实现打印服务器故障转移检测和打印机连接恢复。将定期检查打印服务器的可用性。如果检测到某服务器发生故障，会从负载平衡方案中删除该服务器，并在其他可用的打印服务器中重新分配该服务器上的打印机连接。发生故障的打印服务器在恢复后将重新加入负载平衡方案。

单击**验证服务器**，检查每个服务器是否为打印服务器，以及是否所有服务器都已安装一组相同的共享打印机。此操作可能需要一些时间。

通用打印服务器停止运行阈值

此设置指定负载平衡器应在多长时间内等待不可用的打印服务器恢复，在此之后负载平衡器将该服务器确定为永久脱机，并将其负载重新分配到其他可用的打印服务器。

默认情况下，此阈值设置为 180（秒）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

通用打印策略设置

Dec 05, 2017

“通用 打印”部分包含用于管理通用打印的策略设置。

通用打印 EMF 处理模式

此设置控制在 Windows 用户设备上处理 EMF 后台打印文件的方法。

默认情况下，系统将 EMF 记录直接后台打印到打印机中。

将此设置添加到策略时，请选择一个选项：

- 为打印机重新处理 EMF 强制重新处理 EMF 后台打印文件， 并通过用户设备上的 GDI 子系统发送。可以将此设置用于需要重新处理 EMF 但在会话中可能未自动选择这样执行的驱动程序。
- 直接后台打印到 打印机，与 Citrix 通用打印驱动程序一起使用时，确保 EMF 记录后台打印并交付到用户设备进行处理。通常，这些 EMF 后台打印文件直接插入到客户端的后台打印队列中。 对于与 EMF 格式兼容的打印机和驱动程序，这是速度最快的打印方法。

通用打印图像压缩限制

此设置指定通过 Citrix 通用打印驱动程序打印的图像的最高质量和最低压缩级别。

默认情况下，图像压缩限制设置为 最佳质量(无损压缩)。

如果选择 无压缩，将仅对 EMF 打印禁用压缩。

将此设置添加到策略时，请选择一个选项：

- 无压缩
- 最佳质量(无损压缩)
- 高质量
- 标准质量
- 降低质量(最大压缩)

将该此设置添加到包含通用打印优化默认设置的策略时，应注意以下几点：

- 如果 通用打印图像压缩限制设置中的压缩级别低于 通用打印优化默认值设置中所定义的级别，将按照 通用打印图像压缩限制设置中所定义的级别对图像进行压缩。
- 如果 禁用压缩，则 通用打印优化默认值设置的 所需图像质量和 启用 超级压缩选项在策略中 不起作用。

通用打印优化默认值

此设置指定为会话创建通用打印驱动程序时打印优化的默认值。

- 所需图像 质量指定应用到 通用打印的默认图像压缩限制。默认情况下，启用 标准质量，这意味着用户只能使用标准或降低质量的压缩级别来打印图像。
- 启用超级 压缩用于启用或禁用在超出由 所需图像质量所设置的 压缩级别上减少带宽，而不降低图像质量。 默认情况下，禁用超级压缩功能。
- 图像与字体 缓存设置指定是否缓存在打印流中 多次出现的图像和字体，以确保每个唯一的图像或 字体只发送给打印机一次。默认情况下，将缓存嵌入式图像和字体。 请注意，只有在用户设备支持此行为时，这些设置才适用。
- 允许非管理员 修改这些设置指定用户是否可以更改会话内的 默认打印优化设置。默认情况下，不允许用户更改默认打印优化设置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

注意：EMF 打印支持所有这些选项。 对于 XPS 打印，则仅支持 所需图像质量选项。
将此设置添加到包含通用打印图像压缩限制设置的策略时，应注意以下几点：

- 如果 通用打印图像压缩限制设置中的压缩级别低于 通用打印优化默认值设置中所定义的级别，将按照 通用打印图像压缩限制设置中所定义的级别对图像进行压缩。
- 如果 禁用压缩，则 通用打印优化默认值设置的 所需图像质量和 启用 超级压缩选项在策略中 不起作用。

通用打印预览首选项

此设置指定是否对自动创建的打印机或一般通用打印机使用打印预览功能。

默认情况下，不对自动创建的打印机或一般通用打印机使用打印预览。

将此设置添加到策略时，请选择一个选项：

- 不对自动创建的打印机或一般通用打印机使用打印预览
- 仅对自动创建的打印机使用打印预览
- 仅对一般通用打印机使用打印预览
- 对自动创建的打印机和一般通用打印机均使用打印预览

通用打印的打印质量限制

此设置指定在会话中生成打印输出时可用的最高分辨率 (dpi)。

默认情况下，启用 无限制，这意味着用户可以选择其连接的打印机所允许的最高打印质量。

如果配置此设置，它将在输出分辨率方面限制用户可以达到的最高打印质量。 打印质量本身和用户所连接的打印机的打印质量能力受所配置设置的限制。 例如，如果打印质量设置配置为 中分辨率(600 DPI)，则用户打印输出限制为最高质量为 600 DPI，“通用打印机”对话框的“高级”选项卡中的“打印质量”设置显示的分辨率设置最高只能达到“中质量(600 DPI)”。

将此设置添加到策略时，请选择一个选项：

- 草稿(150 DPI)
- 低分辨率(300 DPI)
- 中分辨率(600 DPI)
- 高分辨率(1200 DPI)
- 无限制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

安全策略设置

Nov 27, 2017

“安全”部分 介绍了配置会话加密和登录数据加密的 相关策略设置。

SecureICA 最低加密级别

此设置指定服务器与用户设备之间所传输会话数据的最低加密级别。

重要：对于 Virtual Delivery Agent 7.x，只能使用此策略设置来启用通过“RC5 (128 位)”加密实现的登录数据加密。其他设置仅在用于向后兼容旧版 XenApp 和 XenDesktop 时提供。

对于 VDA 7.x，使用 VDA 交付组的基本设置来设置会话数据的加密。如果为交付组选择了“启用安全 ICA”，会话数据将通过“RC5 (128 位)”加密进行加密。如果没有为交付组选择“启用安全 ICA”，会话数据将通过“基本”加密进行加密。

将此设置添加到策略时，请选择一个选项：

- 基本可使用一种非 RC5 算法加密客户端连接。它保护数据流使之不能被直接读取，但可以解密。默认情况下，服务器对客户端-服务器通信流使用基本加密。
- 仅限 RC5 (128 位)登录使用 RC5 128 位加密来加密登录数据，使用基本加密来加密客户端连接。
- RC5 (40 位) 使用 RC5 40 位加密来加密客户端连接。
- RC5 (56 位) 使用 RC5 56 位加密来加密客户端连接。
- RC5 (128 位) 使用 RC5 128 位加密来加密客户端连接。

为客户端-服务器加密指定的设置可能会与您的环境和 Windows 操作系统中的任何其他加密设置进行交互。如果在服务器或用户设备上设置了优先级更高的加密级别，则您为已发布的资源指定的设置可能会被覆盖。

您可以为特定用户提高加密级别，以进一步加强其通信安全和消息的完整性。如果某项策略需要更高的加密级别，则使用较低加密级别的 Citrix Receiver 将被拒绝连接。

SecureICA 不执行身份验证，也不检查数据完整性。要为站点提供端到端加密，请将 SecureICA 与 TLS 加密一起使用。

SecureICA 不使用符合 FIPS 标准的算法。如果这样会带来问题，请将服务器和 Citrix Receiver 配置为避免使用 SecureICA。

SecureICA 使用 RFC 2040 中介绍的 RC5 块密码来保密。块大小为 64 位（32 位字单位的倍数）。密钥长度为 128 位。循环次数为 12。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

服务器限制策略设置

Dec 05, 2017

“服务器限制” 部分包含用于控制空闲连接的策略设置。

服务器空闲计时器间隔

此设置确定如果用户未输入任何内容，用户会话可以保持多久不中断（以毫秒为单位）。

默认情况下，空闲连接不会断开连接（服务器空闲计时器间隔 = 0）。Citrix 建议将此值最小设置为 60000 毫秒（60 秒）。

> ### 注意
>
> 使用此策略设置时，如果会话空闲超过指定的时间，可能会向用户显示“空闲计时器已过期”对话框。此消息是一个 Mircosoft 对话框，不受 Citirx 策略设置控制。有关详细信息，请参阅 http://support.citrix.com/article/CTX118618。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

会话限制策略设置

Dec 05, 2017

“会话限制”部分包含的策略设置可用于控制会话在强制注销前可保持连接的时间长度。这些设置不适用于 Windows 服务器 VDA。

断开会话计时器

此设置启用或禁用计时器，用于指定断开连接的锁定桌面在注销会话之前可以保持锁定状态的时间长度。

默认情况下，断开连接的会话不注销。

断开会话计时器间隔

此设置用于指定断开连接的锁定桌面在注销会话前可保持锁定状态的时间长度（分钟）。

默认情况下，此时间段为 1440 分钟（24 小时）。

会话连接计时器

此设置启用或禁用计时器，用于指定用户设备与桌面之间实现不间断连接的最长持续时间。

默认情况下，禁用此计时器。

会话连接计时器间隔

此设置用于指定用户设备与桌面之间实现不间断连接的最长持续时间（分钟）。

默认情况下，最长持续时间为 1440 分钟（24 小时）。

会话空闲计时器

此设置启用或禁用计时器，用于指定在没有用户输入的情况下用户设备与桌面之间实现不间断连接的时间长度。

默认情况下，启用此计时器。

会话空闲计时器间隔

此设置用于指定如果用户不输入任何内容，用户设备与桌面的连接可以保持多久不中断。

默认情况下，空闲连接将保持 1440 分钟（24 小时）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

会话可靠性策略设置

Dec 05, 2017

会话可靠性部分包含用于管理会话可靠性连接的策略设置。

会话可靠性连接

此设置允许或阻止会话在失去网络连接期间保持打开状态。会话可靠性与客户端自动重新连接一起允许用户在从网络中断恢复时自动重新连接到其 Citrix Receiver 会话。

对于 Citrix Receiver for Windows 4.7 及更高版本，会话可靠性仅使用 Citrix Studio 中的策略设置。对 Studio 中这些策略的更新会将会话可靠性从服务器同步到客户端。对于较早版本的 Citrix Receiver for Windows，要配置会话可靠性，应使用 Studio 策略并修改注册表或 default.ica 文件。

注意：在 Citrix Receiver 组策略对象管理模板或 Citrix Studio 策略中将**启用会话可靠性**选项设置为**已禁用**会禁用会话可靠性。如果未在 Citrix Studio 策略中配置**启用会话可靠性**选项，但在 Citrix Receiver 组策略对象管理模板中将其设置为**已禁用**，则将启用会话可靠性。

会话可靠性使会话在网络连接中断时保持活动状态并显示在用户的屏幕上。用户仍然可以看到他们正在使用的应用程序，直至网络连接恢复。

会话可靠性可使会话在服务器上保持活动状态。为了指示连接已断开，用户显示变为不透明。用户在连接中断期间可能会看到冻结的会话，在网络连接恢复后可以继续与应用程序交互。会话可靠性可重新连接用户而不提示进行重新身份验证。

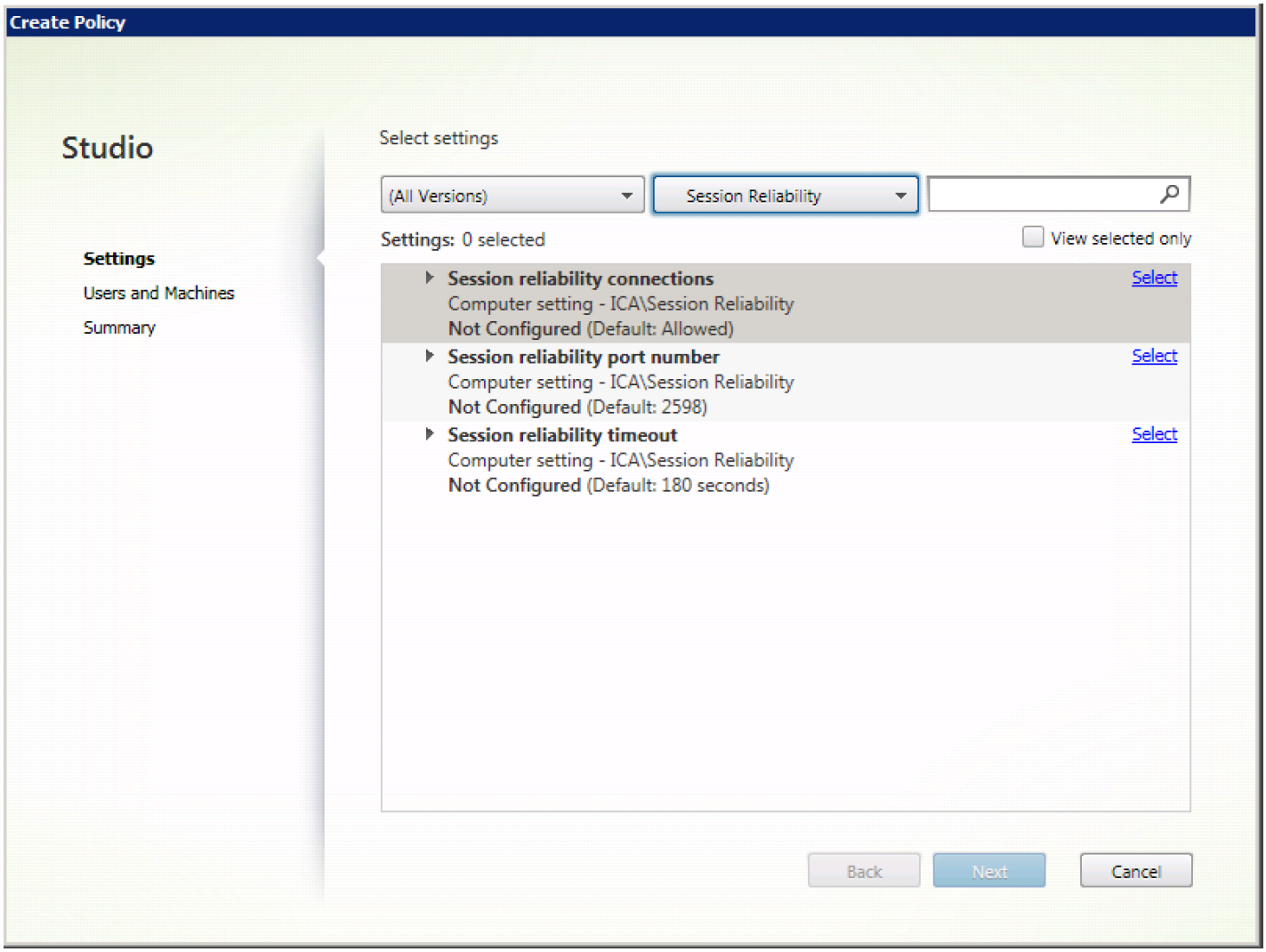
如果您同时使用了会话可靠性和客户端自动重新连接，这两项功能将按顺序发挥作用。会话可靠性将在会话可靠性超时设置中指定的时间之后关闭（或断开）用户会话。之后，客户端自动重新连接策略设置生效，尝试将用户重新连接到断开连接的会话。

默认情况下，会话可靠性为“允许”。

要禁用会话可靠性，请执行以下操作：

1. 启动 Citrix Studio。
2. 打开**会话可靠性连接**策略。
3. 将策略设置为**禁止**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



会话可靠性端口号

此设置为传入会话可靠性连接指定 TCP 端口号。

默认情况下，此端口号设置为 2598。

修改会话可靠性端口号：

1. 启动 Citrix Studio。
2. 打开**会话可靠性端口号**策略。
3. 编辑端口号。
4. 单击**确定**。

会话可靠性超时

此设置指定会话可靠性代理等待用户重新连接的时间长度（以秒为单位），达到该时间后将允许会话断开连接。

尽管您可以延长会话保持打开状态的时间长度，此功能是提供方便，它不会提示用户重新进行身份验证。会话打开的时间越长，用户让设备置于无人看管状态并使其会被未经授权的用户访问的可能性越高。

默认情况下，此超时设置为 180 秒或 3 分钟。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

更改会话可靠性超时：

1. 启动 Citrix Studio。
2. 打开**会话可靠性超时**策略。
3. 编辑超时值。
4. 单击**确定**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

时区控制策略设置

Dec 05, 2017

“时区 控制”部分包含与在会话中使用本地时间相关的 策略设置。

估算旧版客户端的本地时间

此设置启用或禁用对向服务器发送了不准确时区信息的用户设备进行的本地时区估算。

默认情况下，服务器在必要时将估算本地时区。

此设置旨在用于不向服务器发送时区详细信息的旧版 Citrix Receiver 或 ICA 客户端。用于向服务器发送时区详细信息的 Citrix Receiver（例如支持的 Citrix Receiver for Windows 版本）时，此设置不起作用。

使用客户端本地时间

此设置确定用户会话的时区设置。 可以是用户会话的时区，也可以是用户设备的时区。

默认情况下，使用用户会话的时区。

为使此设置生效，请在组策略编辑器中启用“允许时区重定向”设置（“用户配置”>“管理模板”>“Windows 组件”>“远程桌面服务”>“远程桌面会话主机”>“设备和资源重定向”）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

TWAIN 设备策略设置

Dec 05, 2017

“TWAIN 设备”部分包含的策略设置与以下内容相关：映射客户端 TWAIN 设备（例如数码相机或扫描仪），优化从服务器到客户端的图像传输。

> **注意**
>
> TWAIN 2.0 支持 Citrix Receiver for Windows 4.5。

客户端 TWAIN 设备重定向

此设置允许或禁止用户从服务器上托管的图像处理应用程序访问用户设备上的 TWAIN 设备。 默认情况下，允许 TWAIN 设备重定向。

下列策略设置为 相关设置：

- TWAIN 压缩级别
- TWAIN 设备重定向带宽限制
- TWAIN 设备重定向带宽限制百分比

TWAIN 压缩级别

此设置指定从客户端到服务器的图像传输的压缩级别。 “低”可提供最佳图像质量，“中”可提供良好图像质量，“高”可提供低图像质量。 默认情况下，应用中级压缩。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

USB 设备策略设置

Dec 05, 2017

“USB 设备”部分包含用于管理 USB 设备文件重定向的策略设置。

客户端 USB 设备优化规则

可以对设备应用客户端 USB 设备优化规则以禁用优化，或者更改优化模式。

用户插入 USB 输入设备时，主机检查 USB 策略设置是否允许此设备。如果不允许此设备，主机则检查此设备的**客户端 USB 设备优化规则**。如果未指定任何规则，则不会优化设备。对于签名设备，建议使用捕获模式 (04)。对于其他因更高延迟而降级性能的设备，管理员可以启用交互模式 (02)。请参阅下面的说明以了解可用模式。

须知事项

- 如果要使用 Wacom 签名板和平板电脑，Citrix 建议您禁用屏幕保护程序。本节结尾介绍执行此操作的步骤。
- 安装 XenApp 和 XenDesktop 策略时已经预配置了对优化 Wacom STU 签名板和平板电脑系列的支持。
- 签名设备在整个 XenApp 和 XenDesktop 中均可以使用，且无需使用驱动程序作为签名设备。Wacom 包含可以安装以进一步自定义设备的其他软件。请参阅 http://www.wacom.com/。
- 手写板。某些手写输入设备在 PCI/ACPI 总线上可能显示为 HID 设备，不受支持。这些设备应该连接到客户端上的 USB 主机控制器，以便在 XenDesktop 会话内重定向。

策略规则采用以空格分隔的 tag=value 表达式格式。支持以下标记：

标记名称	说明
模式	为输入设备支持优化模式，类 =**03**。支持的模式包括： 无优化 - 值 **01**。 交互模式 - 值 **02**。手写板和 3D 专业鼠标等设备的建议模式。 捕获模式 - 值 **04**。签名板等设备的首选模式。
VID	设备描述符中的供应商 ID。
PID	设备描述符中的产品 ID。
REL	设备描述符中的版本 ID。
类	设备描述符或接口描述符中的类。
子类	设备描述符或接口描述符中的子类。
端口	设备描述符或接口描述符中的协议。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

示例

Mode=00000004 VID=1230 PID=1230 class=03 #输入设备在捕获模式下运行

Mode=00000002 VID=1230 PID=1230 class=03 #输入设备在交互模式下运行（默认）

Mode=00000001 VID=1230 PID=1230 class=03 #输入设备在未进行任何优化的情况下运行

Mode=00000100 VID=1230 PID=1230 # 设备设置优化禁用（默认）

Mode=00000200 VID=1230 PID=1230 # 设备设置优化启用

为 Wacom 签名板设备禁用屏幕保护程序

对于使用 Wacom 签名板和平板电脑的情况，Citrix 建议您按如下所示禁用屏幕保护程序：

1. 重定向设备后安装 **Wacom-STU-Driver**。
2. 安装 **Wacom-STU-Display MSI** 以获取签名板控制面板的访问权限。
3. 转至**控制面板 > Wacom STU Display > STU430** 或 **STU530**，选择所需模式对应的选项卡。
4. 单击 **Change**（更改），然后在弹出 UAC 安全窗口时选择 **Yes**（是）。
5. 选择**禁用幻灯片**，然后选择**应用**。

为一种签名板模型设置此设置后，此设置将应用于所有模型。

客户端 USB 设备重定向

此设置允许或阻止 USB 设备与用户设备之间往来的重定向。

默认情况下，不重定向 USB 设备。

客户端 USB 设备重定向规则

此设置指定 USB 设备重定向规则。

默认情况下，不指定任何规则。

用户插入 USB 设备时，主机设备会依次根据每条策略规则对其进行检查，直至找到匹配项。任何设备的第一个匹配项都被视为最终选择。如果第一个匹配项是一条“允许”规则，则该设备将远程连接到虚拟桌面。如果第一个匹配项是一条“Deny”规则，则该设备只能连接本地桌面。如果未找到匹配项，则使用默认规则。

策略规则的格式为 {Allow:|Deny:} 后接一组以空格分隔的 tag=value 表达式。支持以下标记：

标记名称	说明
VID	设备描述符中的供应商 ID
PID	设备描述符中的产品 ID
REL	设备描述符中的版本 ID
类	设备描述符或接口描述符中的类

© 1999-2017 Citrix Systems, Inc. All rights reserved.

标记名称	说明
子类	设备描述符或接口描述符中的子类
端口	设备描述符或接口描述符中的协议

创建新策略规则时，请注意：

- 规则不区分大小写。
- 规则末尾可以带有以 # 开头的可选注释。
- 空白注释行和纯注释行会被忽略。
- 标识必须使用匹配运算符 =（例如，VID=1230_）。
- 每条规则都必须另起新行，或包含在以分号分隔的列表中。
- 请参阅 USB Implementers Forum, Inc. Web 站点上提供的 USB 类代码。

管理员定义的 USB 策略规则示例：

- Allow: VID=1230 PID=0007 # ANOther Industries, ANOther Flash Drive
- Deny: Class=08 subclass=05 # Mass Storage
- 要创建一条拒绝所有 USB 设备的规则，请使用未附带任何其他标记的“DENY:”。

客户端 USB 即插即用设备重定向

此设置允许或禁止在客户端会话中使用即插即用设备，例如照相机或销售点 (POS) 设备。

默认情况下，允许即插即用设备重定向。 当设置为“允许”时，将重定向特定用户或组的即插即用设备。 当设置为“禁止”时，将不重定向任何设备。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

视频显示策略设置

Dec 05, 2017

“视频显示”部分中包含用于控制从虚拟桌面发送到用户设备的图像质量的策略设置。

简单图形的首选颜色深度

此策略设置在 VDA 版本 7.6 FP3 及更高版本中提供。8 位选项在 VDA 版本 7.12 及更高版本中提供。

使用此设置，可以降低通过网络发送简单图形时使用的颜色深度。降低到 8 位/像素或 16 位/像素可能会提高使用低带宽连接时的响应能力，但会略微降低图像质量。使用视频编解码器进行压缩策略设置设置为“针对整个屏幕”时，不支持 8 位颜色深度。

默认的首选颜色深度是 24 位/像素。

如果在 VDA 版本 7.11 及更低版本上应用 8 位设置，VDA 将回退至 24 位（默认）颜色深度。

目标帧速率

此设置指定每秒从虚拟桌面发送到用户设备的最大帧数。

默认情况下，最大值为 30 帧/秒。

设置一个较高的每秒帧数值（例如 30）可改进用户体验，但需要占用更多带宽。减小每秒帧数值（例如 10）可将服务器可扩展性提高至最高水平，但用户体验将非常差。对于 CPU 速度较慢的用户设备，指定较低的值可以改善用户体验。

支持的最高每秒帧速率是 60。

视觉质量

此设置指定在用户设备上显示的图像所需的视觉质量。

默认情况下，此参数设置为“中”。

要指定图像质量，请选择下列选项之一：

- **低**
- **中** - 在大多数用例中可提供最佳性能和最高带宽效率
- **高** - 如果需要视觉上无损的图像质量，建议采用此设置
- **设为无损** - 在高网络活动期间向用户设备发送有损图像，在网络活动减少后发送无损图像。此设置可改进带宽有限的网络连接条件下的性能
- **始终无损** - 如果保留图像数据非常重要（例如，显示不允许有质量损失的 X 光图像时），选择始终无损可确保不会将有损数据发送到用户设备。

如果在策略中启用了 **旧图形模式**设置，**视觉质量**设置在此策略中无效。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

移动图像策略设置

Dec 05, 2017

“移动图像” 部分包含使您能够删除或更改 动态图像的压缩的设置。

最低图像质量

注意： 对于 Virtual Delivery Agent 7.x，仅当启用 旧图形模式策略设置时，才会应用此策略设置。
此设置指定自适应显示功能可接受的最低图像质量。 使用的压缩程度越低，所显示图像的质量越高。 可以从“超高”、“很高”、“高”、“正常”或“低”压缩程度中进行选择。

默认情况下，此项设置为“正常”。

移动图像压缩

此设置指定是否启用自适应显示功能。自适应显示功能可根据可用带宽自动调整视频以及幻灯片放映中过渡性幻灯片的图像质量。启用自适应显示功能后，用户应看到顺畅的展示效果，质量没有任何损失。
默认情况下，启用“自适应显示”功能。

对于版本 7.0 至 7.6 的 VDA，此设置仅在启用旧图形模式时应用。对于版本为 7.6 FP1 或更高版本的 VDA，此设置在启用旧图形模式时应用，或在禁用旧图形模式并且未使用视频编解码器来压缩图形时应用。

启用旧图形模式时，必须重新启动会话，策略更改才能生效。自适应显示与渐进式显示相互排斥；启用自适应显示将禁用渐进式显示，反之亦然。但是，可以同时禁用自适应显示和渐进式显示。渐进式显示是一项旧功能，建议不要用于 XenApp 和 XenDesktop。设置渐进式阈值级别将禁用自适应显示。

渐进式压缩级别

注意： 对于 Virtual Delivery Agent 7.x，仅当启用 旧图形模式策略设置时，才会应用此策略设置。
此设置提供的图像的初始显示细节较少但速度更快。

默认情况下，不应用渐进式压缩。

细节更丰富的图像（由常规有损压缩设置定义）在可用时显示。 使用“很高”或“超高”压缩可改善需要占用大量带宽的图形（例如照片）的查看速度。

要使渐进式压缩生效，其压缩级别必须高于 有损压缩级别设置。
注意：提高与渐进式压缩相关联的压缩级别，还会提高客户端连接上动态图像的交互性。 动态图像 （例如旋转的三维模型）的质量在图像停止动作前会暂时 降低，之后会应用标准 有损压缩设置。
下列策略设置为相关设置：

- 渐进式压缩阈值
- 渐进式超级压缩

渐进式压缩阈值

注意： 对于 Virtual Delivery Agent 7.x，仅当启用 旧图形模式策略设置时，才会应用此策略设置。
此设置表示应用渐进式压缩的连接的最大带宽 (Kbps)。 此设置仅适用于低于此带宽的客户端连接。

默认情况下，该阈值为 2147483647 Kbps。

下列策略设置为相关设置：

- 渐进式压缩阈值

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 渐进式超级压缩

目标最低帧速率

此设置为动态图像指定了低带宽条件下，系统尝试保持的最低每秒帧速率。
默认情况下设置为 10 fps。

对于版本 7.0 至 7.6 的 VDA，此设置仅在启用旧图形模式时应用。对于版本为 7.6 FP1 及更高版本的 VDA，此设置在禁用或启用旧图形模式时均可以应用。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

静态图像策略设置

Dec 05, 2017

“静态图像” 部分包含使您能够删除或更改 静态图像的压缩的设置。

额外颜色压缩

此设置允许或禁止当通过带宽受限制的客户端连接交付图像时，这些图像使用额外颜色压缩，从而以降低显示图像质量的方式来提高响应能力。
默认情况下，禁用额外颜色压缩。

启用后，则只有当客户端连接带宽低于额外颜色压缩阈值的值时，才会应用额外颜色压缩。如果客户端连接带宽高于该阈值，或者选择了已禁用，则不会应用额外颜色压缩。

额外颜色压缩阈值

注意： 对于 Virtual Delivery Agent 7.x，仅当启用 旧图形模式策略设置时，才会应用此策略设置。
此设置表示连接的最大带宽 (Kbps)，如果低于该带宽，则会应用额外颜色压缩。 如果客户端连接带宽低于设置的值，则会应用额外颜色压缩（如果启用）。

默认情况下，该阈值为 8192 Kbps。

超级压缩

注意： 对于 Virtual Delivery Agent 7.x，仅当启用 旧图形模式策略设置时，才会应用此策略设置。
此设置启用或禁用使用一种更为高级但会占用更多 CPU 资源的图形算法，在不损失图像质量的情况下降低渐进式压缩之外的压缩占用的带宽。

默认情况下，禁用超级压缩功能。

如果启用超级压缩，它会应用到所有有损压缩设置。 这种压缩在 Citrix Receiver 上受支持，但对其他插件不起作用。

下列策略设置为相关设置：

- 渐进式压缩级别
- 渐进式压缩阈值

有损压缩级别

注意： 对于 Virtual Delivery Agent 7.x，仅当启用 旧图形模式策略设置时，才会应用此策略设置。
此设置控制通过带宽受限的客户端连接交付的图像上所用的有损压缩程度。 在此类情况下，显示未压缩的图像速度会很慢。

默认情况下，选择中等压缩。

为改善占用大量带宽的图像的响应速度，请使用高压缩。 当保留图像数据非常重要（例如显示不允许有质量损失的 X 光图像时），您可能不希望使用有损压缩。

相关策略设置：有损压缩阈值

有损压缩阈值

注意： 对于 Virtual Delivery Agent 7.x，仅当启用 旧图形模式策略设置时，才会应用此策略设置。
此设置表示应用有损压缩的连接的最大带宽 (Kbps)。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

默认情况下，该阈值为 2147483647 Kbps。

将 有损压缩级别设置添加到策略且不指定阈值可以提高通过 LAN 传输的高清晰位图（例如照片）的显示速度。

相关策略设置：有损压缩级别

© 1999-2017 Citrix Systems, Inc. All rights reserved.

WebSocket 策略设置

Dec 05, 2017

WebSocket 部分包含用于使用 Citrix Receiver for HTML5 访问虚拟桌面和托管应用程序的策略设置。WebSocket 功能通过在基于浏览器的应用程序和服务器之间进行双向通信（无需打开多个 HTTP 连接），从而提高安全性并减少开销。

WebSocket 连接

此设置允许或禁止 WebSocket 连接。

默认情况下，禁止 WebSocket 连接。

WebSocket 端口号

此设置可识别传入的 WebSocket 连接的端口。

默认情况下，此值为 8008。

WebSocket 可信源服务器列表

此设置提供了一个逗号分隔的可信原始服务器列表，通常是 Citrix Receiver for Web，表示为 URL。服务器仅接受来自下列地址之一的 WebSocket 连接。

默认情况下，通配符 * 用于信任所有 Citrix Receiver for Web URL。

如果您选择在列表中键入地址，请使用以下语法：

<protocol>://<Fully qualified domain name of host>:[port]

此协议应为 HTTP 或 HTTPS。如果未指定端口号，则端口 80 用于 HTTP，端口 443 用于 HTTPS。

通配符 * 可用于 URL，但不能作为 IP 地址 (10.105.*.*) 的一部分。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

负载管理策略设置

Dec 05, 2017

“负载管理”部分包含用于在交付 Windows 服务器操作系统计算机的服务器之间启用和配置负载管理的策略设置。

有关计算负载评估器指数的信息，请参阅 CTX202150。

并发登录容错

此设置指定服务器可以接受的最大并发登录数。

默认情况下，此范围设置为 2。

启用了此设置时，负载平衡功能将尝试避免服务器 VDA 上同时出现多个指定的活动登录。但是，该限制并不严格执行。要执行该限制（导致超出指定数量的并发登录失败），请创建以下注册表项：

HKLM\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit
类型：DWORD
值：1

CPU 使用率

此设置指定服务器报告满负载时的 CPU 使用率，以百分比表示。 启用时，服务器报告满负载的默认值是 90%。

默认情况下，此设置处于禁用状态，负载计算中不包括 CPU 使用率。

排除 CPU 使用率的进程优先级

此设置指定从 CPU 使用率负载指数中排除进程 CPU 使用率时的优先级。

默认情况下，此参数设置为“低于正常”或“低”。

磁盘使用情况

此设置指定服务器报告 75% 满负载时的磁盘队列长度。 启用时，磁盘队列长度的默认值为 8。

默认情况下，此设置处于禁用状态，负载计算中不包括磁盘使用情况。

最大会话数

此设置指定服务器可以托管的最大会话数。 启用时，服务器可托管最大会话数的默认设置为 250。

默认情况下，此设置处于启用状态。

内存使用率

此设置指定服务器报告满负载时的内存使用率，以百分比表示。 启用时，服务器报告满负载的默认值是 90%。

默认情况下，此设置处于禁用状态，负载计算中不包括内存使用率。

内存使用基础负载

此设置指定基本操作系统内存使用空间的近似值，并定义服务器被视为零负载时的内存使用空间（以 MB 为单位）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

默认情况下，将其设置为 768 MB。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Profile Management 策略设置

Dec 05, 2017

Profile Management 部分包含的策略设置用于启用 Profile Management 并指定要在 Profile Management 处理中包含或排除的组。

其他信息（如等效 .ini 文件设置的名称和策略设置需要的 Profile Management 版本）可从 Profile Management 策略中获取。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

高级策略设置

Dec 05, 2017

“高级 设置”部分包含与 Profile Management 高级 配置相关的策略设置。

禁用自动配置

此设置允许 Profile Management 检查您的环境；例如，检查是否存在个人虚拟磁盘，并相应地配置组策略。 系统仅调整处于“未配置”状态的 Profile Management 策略，因此之前所做的任何自定义设置都将保留。 此功能加快了部署，并简化了优化过程。 此功能无需任何配置，但您可以在升级（保留早期版本的设置）或进行故障排除时禁用自动配置。 自动配置在 XenApp 或其他环境中无法使用。

默认情况下允许自动配置。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，将开启自动配置功能，以便当环境发生变化时可以更改 Profile Management 设置。

遇到问题时注销用户

此设置允许 Profile Management 在遇到问题（例如，用户存储不可用）时注销用户。 启用时，在用户被注销前，系统会向用户显示一条错误消息。 禁用时，系统会为用户提供一个临时配置文件。

默认情况下，此设置处于禁用状态，遇到问题时，系统会为用户提供一个临时配置文件。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，将提供一个临时配置文件。

访问锁定文件的重试次数

此设置指定 Profile Management 尝试访问锁定文件的次数。

默认情况下，此参数设置为重试 5 次。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则将使用默认值。

注销时处理 Internet Cookie 文件

此设置允许 Profile Management 在注销时处理 index.dat，从而删除持续浏览后保留在文件系统中可能会导致配置文件膨胀的 Internet Cookie。 启用此设置会延长注销时间，因此，请仅在遇到此问题时才启用此设置。

默认情况下，此设置处于禁用状态，Profile Management 不会在注销时处理 index.dat。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果该设置没有在此配置，也在 .ini 文件中，则将不处理 Index.dat。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

基本策略设置

Dec 05, 2017

“基本设置” 部分包含与 Profile Management 基本配置有关的 策略设置。

主动写回

此设置允许在会话过程中或注销之前将修改后的文件和文件夹（但不包括注册表设置）同步到用户存储。

默认情况下，禁止在会话过程中同步到用户存储。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果该设置没有在此配置，也不在 .ini 文件中，则将处于启用状态。

启用 Profile Management

此设置允许 Profile Management 处理登录和注销。

默认情况下，此设置已禁用，以方便部署。

重要：Citrix 建议仅在执行所有其他设置任务并测试 Citrix 用户配置文件在环境中的执行情况后，再启用 Profile Management。
如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果该设置没有在此配置，也不在 INI 文件中，则 Profile Management 不会以任何方式处理 Windows 用户配置文件。

排除的组

此设置指定从 Profile Management 处理范围中排除哪些计算机本地组和域组（本地组、全局组和通用组）排除之外。

启用时，Profile Management 不会处理指定用户组的成员。

默认情况下，此设置处于禁用状态，此时将处理所有用户组的成员。

按 <DOMAIN NAME>\<GROUP NAME> 格式指定域组。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果未在此处也未在 .ini 文件中配置此设置，则将处理所有用户组的成员。

脱机配置文件支持

此设置可启用脱机配置文件支持，使配置文件能够在网络连接断开后尽早与用户存储进行同步。

默认情况下，脱机配置文件支持处于禁用状态。

此设置适用于使用便携式计算机或移动设备的漫游用户。 网络连接断开时，即使在便携式计算机或移动设备重新启动或进入休眠状态后，设备上的配置文件仍将保持原样。 移动用户工作时，其配置文件将在本地更新，并在重新建立网络连接时与用户存储进行同步。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，将禁用对脱机配置文件的支持。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

用户存储路径

此设置指定用于保存用户设置（如注册表设置和同步文件）的目录路径（用户存储）。

默认情况下，将使用主驱动器上的 Windows 目录。

如果禁用此设置，用户设置将保存在主目录的 Windows 子目录中。

路径可以是：

- **相对路径**。此路径必须是相对于主目录的路径，通常配置为 Active Directory 中用户的 #homeDirectory# 属性。
- **绝对 UNC 路径**。 此路径通常指定服务器共享或 DFS 命名空间。
- **已禁用或 未配置**。在此情况下，假设值为 #homeDirectory#\Windows。

配置此策略设置时，请使用以下类型的变量：

- 百分号括起的系统环境变量（例如 %ProfVer%）。 请注意，系统环境变量通常需要额外设置。
- 井号括起的 Active Directory 用户对象属性（例如 #sAMAccountName#）。
- Profile Management 变量。 有关详细信息，请参阅 Profile Management 文档。

您也可以使用 %username% 和 %userdomain% 用户环境变量并创建自定义属性，以完全定义位置或用户等组织变量。 属性区分大小写。

示例：

- \\server\share\#sAMAccountName# 将用户设置存储到 UNC 路径 \\server\share\JohnSmith（如果当前用户的 #SAMAccountName# 解析为 JohnSmith）
- \\server\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_PROFILEVER!!CTX_OSBITNESS! 可以扩展为 \\server\profiles$\JohnSmith.DOMAINCONTROLLER1\v2x64

重要：无论使用哪种属性或变量，均请确认此设置是否可以扩展到包含 NTUSER.DAT 的文件夹的上层文件夹。 例如，如果此文件包含在 \\server\profiles$\JohnSmith.Finance\v2x64\UPM_Profile 中，则应将用户存储路径设置为 \\server\profiles$\JohnSmith.Finance\v2x64，而非 \UPM_Profile 子文件夹。
如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果未在此处也未在 .ini 文件中配置此设置，则将使用主驱动器上的 Windows 目录。

处理本地管理员登录

此设置指定是否处理 BUILTIN\Administrators 组成员的登录。 这使具有本地管理员权限的域用户（通常是已分配虚拟桌面的用户）可以跳过任何处理过程而直接登录，并对出现 Profile Management 问题的桌面进行故障排除。

如果在服务器操作系统上禁用或未配置该设置，Profile Management 会假定必须处理域用户登录，但不处理本地管理员登录。在桌面操作系统上，会处理本地管理员登录。

默认情况下，此设置处于禁用状态，不会处理本地管理员登录。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则不会处理本地管理员登录。

处理的组

此设置指定哪些计算机本地组和域组（本地组、全局组和通用组）包括在 Profile Management 处理范围内。

启用时，Profile Management 仅处理指定用户组的成员。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

默认情况下，此设置处于禁用状态，此时将处理所有用户组的成员。

按 <DOMAIN NAME>\<GROUP NAME> 格式指定域组。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果未在此处也未在 .ini 文件中配置此设置，则将处理所有用户组的成员。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

跨平台策略设置

Dec 05, 2017

“跨平台” 部分包含与配置 Profile Management 跨平台设置功能有关的策略设置。

跨平台设置用户组

此设置指定在跨平台设置功能启用时处理其配置文件的 Windows 用户组。

默认情况下，此 设置处于禁用状态，系统会处理在 处理的组策略设置中指定的所有用户组。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则会处理所有用户组。

启用跨平台设置

此设置启用或禁用跨平台设置功能，允许在用户连接到多个操作系统中运行的同一应用程序时迁移和漫游用户的配置文件。

默认情况下，禁用跨平台设置功能。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则不应用任何跨平台设置。

跨平台定义路径

此设置将从下载软件包中复制的定义文件的网络位置指定为 UNC 路径。

注意：用户必须对此位置具有读取权限，管理员必须对此位置具有写入权限，并且此位置必须是服务器消息块 (SMB) 或通用 Internet 文件系统 (CIFS) 文件共享。
默认情况下，不指定路径。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则不应用任何跨平台设置。

跨平台设置存储路径

此设置指定跨平台设置存储的路径，即用于保存用户跨平台设置的文件夹。 该路径可以是 UNC 路径，也可以是相对于主目录的路径。

注意：用户必须对跨平台设置存储具有写入权限。
默认情况下，禁用此设置，此时将使用路径 Windows\PM_CP。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则将使用默认值。

创建跨平台设置的来源

如果为平台的 OU 启用此设置，则此设置会将某个平台指定为 基础平台。 数据将从基础平台的配置文件迁移到跨平台设置存储中。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

每个平台自有的一组配置文件存储在独立的 OU 中。 这意味着您必须决定使用哪个平台的配置文件数据来设置跨平台设置存储。 这称为基础平台。

启用时，如果跨平台设置存储中包含无任何数据的定义文件，或者单平台配置文件中的缓存数据比存储中的定义数据新，则 Profile Management 会将数据从单平台配置文件迁移到存储中。

重要：如果在多个 OU、多个用户或计算机对象中启用了此设置，则第一个用户登录到的平台将作为基础配置文件。
默认情况下，禁用此设置，Profile Management 不会将数据从单平台配置文件迁移到存储中。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

文件系统策略设置

Dec 05, 2017

“文件系统”部分包含的策略设置用于配置用户配置文件中的哪些文件和目录将在安装配置文件的系统和用户存储之间进行同步。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

排除策略设置

Dec 05, 2017

“排除” 部分包含的策略设置用于配置将 用户配置文件中的哪些文件和目录从同步过程中排除。

排除列表 - 目录

此设置指定用户配置文件中将在同步过程中忽略的文件夹的列表。

以相对于用户配置文件的路径 (%USERPROFILE%) 指定文件夹名。

默认情况下，禁用此设置，将会同步用户配置文件中的所有文件夹。

示例：Desktop 表示忽略用户配置文件中的 Desktop 文件夹

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则将同步用户配置文件中的所有文件夹。

排除列表 - 文件

此设置指定用户配置文件中将在同步过程中忽略的文件的列表。

默认情况下，禁用此设置，将会同步用户配置文件中的所有文件。

以相对于用户配置文件的路径 (%USERPROFILE%) 指定文件名。 请注意，允许使用通配符，但以递归方式应用。

示例：Desktop\Desktop.ini 表示忽略 Desktop 文件夹中的 Desktop.ini 文件

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则将同步用户配置文件中的所有文件。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

同步策略设置

Dec 05, 2017

“同步” 部分包含的策略设置用于指定将在 安装配置文件的系统与用户存储之间同步用户配置文件中的 哪些文件和文件夹。

同步的目录

此设置指定您希望 Profile Management 在同步过程中包含的已排除文件夹中的任何文件。默认情况下，Profile Management 将同步用户配置文件中的所有内容。无需通过将用户配置文件的子文件夹添加到该列表中来包括这些子文件夹。有关详细信息，请参阅包含和排除项目。

该列表中的路径必须是相对于用户配置文件的路径。

示例：Desktop\exclude\include 确保同步 include 子文件夹，即使不同步 Desktop\exclude 文件夹

默认情况下，禁用此设置，不指定任何文件夹。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则仅对用户配置文件中没有排除的文件夹进行同步。

同步的文件

此设置指定您希望 Profile Management 在同步过程中包含的已排除文件夹中的任何文件。默认情况下，Profile Management 将同步用户配置文件中的所有内容。无需通过将用户配置文件中的文件添加到该列表中来包括这些文件。有关详细信息，请参阅包含和排除项目。

该列表中的路径必须是相对于用户配置文件的路径。相对路径解释为相对于用户配置文件。允许使用通配符，但只能用于文件名。不能嵌套通配符，将递归应用通配符。

示例：

- AppData\Local\Microsoft\Office\Access.qat 指定了默认配置中排除的文件夹中的文件
- AppData\Local\MyApp*.cfg 指定了配置文件夹 AppData\Local\MyApp 及其子文件夹中扩展名为 .cfg 的所有文件

默认情况下，禁用此设置，不指定任何文件。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则仅会对用户配置文件中没有排除的文件夹进行同步。

镜像的文件夹

此设置指定要镜像的、相对于用户配置文件根文件夹的文件夹。 配置此策略设置有助于解决与任何事务性文件夹（也称为引用文件夹）有关的问题，该文件夹包含互相依赖的文件，即其中一个文件引用其他文件。

通过镜像文件夹，Profile Management 可将事务性文件夹及其内容作为单个实体进行处理，从而避免配置文件膨胀。 请注意，在这些情况下，“后写入内容有效”。因此，镜像的文件夹中包含的在多个会话中被修改的文件会被最新的更新覆盖，导致配置文件更改丢失。

例如，您可以镜像 Internet Explorer Cookie 文件夹，从而可以将 Index.dat 与其索引的 Cookie 同步。

假设用户具有两个 Internet Explorer 会话，分别位于不同的服务器上，并且服务器在每个会话中访问不同的站点，则每个站点

© 1999-2017 Citrix Systems, Inc. All rights reserved.

的 Cookie 会添加到相应的服务器。 用户从第一个会话注销时（或者在会话过程中，前提是配置了活动写回功能），第二个会话中的 Cookie 应替代第一个会话中的 Cookie。 但是，这两个会话却合并在一起，而且对 Index.dat 中的 Cookie 的引用将过期。 进一步浏览新会话会导致重复合并以及 Cookie 文件夹膨胀。

镜像 Cookie 文件夹可解决上述问题，因为该操作在每次用户注销时都将用最后一次会话中的 Cookie 覆盖之前的 Cookie，从而使 Index.dat 保持为最新。

默认情况下，禁用此设置，不镜像任何文件夹。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此策略，则不会镜像任何文件夹。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

文件夹重定向策略设置

Dec 05, 2017

“文件夹重定向”部分包含的策略设置用于指定是否将经常出现在配置文件中的文件夹重定向到共享网络位置。

授予管理员访问权限

此设置使管理员可以访问用户重定向的文件夹的内容。

默认情况下，此设置处于禁用状态，用户被授予独占访问其重定向文件夹内容的权限。

包含域名

此设置允许将 %userdomain% 环境变量包含在为重定向文件夹指定的 UNC 路径中。

默认情况下，此设置处于禁用状态，%userdomain% 环境变量不包括在为重定向文件夹指定的 UNC 路径中。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

“AppData (漫游)”策略设置

Dec 05, 2017

“AppData (漫游)” 部分包含的策略设置用于指定是否将“AppData (漫游)”文件夹的 内容重定向到共享网络位置。

“AppData(漫游)”路径

此设置指定“AppData (漫游)”文件夹的内容将重定向到的网络位置。

默认情况下，此设置处于禁用状态，不指定任何位置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“AppData (漫游)”的重定向设置

此设置指定如何重定向“AppData (漫游)”文件夹的内容。

默认情况下，内容重定向到 UNC 路径。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

“联系人”策略设置

Dec 05, 2017

“联系人”部分 包含的策略设置用于指定是否将 “联系人”文件夹的内容重定向到共享网络位置。

“联系人”路径

此设置指定“联系人”文件夹的内容将重定向到的网络位置。

默认情况下，此设置处于禁用状态，不指定任何位置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“联系人”的重定向设置

此设置指定如何重定向“联系人”文件夹的内容。

默认情况下，内容重定向到 UNC 路径。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

桌面策略设置

Dec 05, 2017

“桌面”部分 包含的策略设置用于指定是否将 “桌面”文件夹的内容重定向到共享网络位置。

“桌面”路径

此设置指定“桌面”文件夹的内容将重定向到的网络位置。

默认情况下，此设置处于禁用状态，不指定任何位置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“桌面”的重定向设置

此设置指定如何重定向“桌面”文件夹的内容。

默认情况下，内容重定向到 UNC 路径。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

“文档”策略设置

Dec 05, 2017

“文档”部分 包含的策略设置用于指定是否将 “文档”文件夹的内容重定向到共享网络位置。

“文档”路径

此设置指定“文档”文件夹中的文件将重定向到的网络位置。

默认情况下，此设置处于禁用状态，不指定任何位置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

必须启用 文档路径设置，以将文件重定向到“文档”文件夹，同时将文件重定向到“音乐”、“图形”和“视频”文件夹。

“文档”的重定向设置

此设置指定如何重定向“文档”文件夹的内容。

默认情况下，内容重定向到 UNC 路径。

要控制如何重定向“文档”文件夹的内容，请选择以下选项之一：

- 重定向到以下 UNC 路径。将内容重定向到 “文档”路径策略设置中指定的 UNC 路径。
- 重定向到用户的主 目录。将内容重定向到用户主目录，通常配置为 Active Directory 中用户的 #homeDirectory# 属性。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

“下载”策略设置

Dec 05, 2017

“下载”部 分包含的策略设置用于指定是否将 “下载”文件夹的内容重定向到共享网络位置。

“下载”路径

此设置指定“下载”文件夹中的文件将重定向到的网络位置。

默认情况下，此设置处于禁用状态，不指定任何位置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“下载”的重定向位置

此设置指定如何重定向“下载”文件夹的内容。

默认情况下，内容重定向到 UNC 路径。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

“收藏夹”策略设置

Dec 05, 2017

“收藏夹” 部分包含的策略设置用于指定是否将 “收藏夹”文件夹的内容重定向到共享网络位置。

“收藏夹”路径

此设置指定“收藏夹”文件夹的内容将重定向到的网络位置。

默认情况下，此设置处于禁用状态，不指定任何位置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“收藏夹”的重定向设置

此设置指定如何重定向“收藏夹”文件夹。

默认情况下，内容重定向到 UNC 路径。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

“链接”策略设置

Dec 05, 2017

“链接”部分 包含的策略设置用于指定是否将 “链接”文件夹的内容重定向到共享网络位置。

“链接”路径

此设置指定“链接”文件夹的内容将重定向到的网络位置。

默认情况下，此设置处于禁用状态，不指定任何位置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“链接”的重定向设置

此设置指定如何重定向“链接”文件夹的内容。

默认情况下，内容重定向到 UNC 路径。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

“音乐”策略设置

Dec 05, 2017

“音乐”部分 包含的策略设置用于指定是否将 “音乐”文件夹的内容重定向到共享网络位置。

“音乐”路径

此设置指定“音乐”文件夹的内容将重定向到的网络位置。

默认情况下，此设置处于禁用状态，不指定任何位置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“音乐”的重定向设置

此设置指定如何重定向“音乐”文件夹的内容。

默认情况下，内容重定向到 UNC 路径。

要控制如何重定向“音乐”文件夹的内容，请选择以下选项之一：

- 重定向到以下 UNC 路径。将内容重定向到 “音乐” 路径策略设置中指定的 UNC 路径。
- 相对于 “文档”文件夹重定向。将内容重定向到相对于“文档”文件夹的文件夹。

要将内容重定向到相对于“文档”文件夹的文件夹，必须启用 “文档”路径设置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

“图片”策略设置

Dec 05, 2017

“图片”部分 包含的策略设置用于指定是否将 “图片”文件夹的内容重定向到共享网络位置。

“图片”路径

此设置指定“图片”文件夹的内容将重定向到的网络位置。

默认情况下，此设置处于禁用状态，不指定任何位置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“图片”的重定向设置

此设置指定如何重定向“图片”文件夹的内容。

默认情况下，内容重定向到 UNC 路径。

要控制如何重定向“图片”文件夹的内容，请选择以下选项之一：

- 重定向到以下 UNC 路径。将内容重定向到 “图片” 路径策略设置中指定的 UNC 路径。
- 相对于 “文档”文件夹重定向。将内容重定向到相对于“文档”文件夹的文件夹。

要将内容重定向到相对于“文档”文件夹的文件夹，必须启用 “文档”路径设置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

“保存的游戏”策略设置

Dec 05, 2017

“保存的游戏” 部分包含的策略设置用于指定是否将“保存的游戏”文件夹的内容 重定向到共享网络位置。

“保存的游戏”的重定向设置

此设置指定如何重定向“保存的游戏”文件夹的内容。

默认情况下，内容重定向到 UNC 路径。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“保存的游戏”路径

此设置指定“保存的游戏”文件夹的内容将重定向到的网络位置。

默认情况下，此设置处于禁用状态，不指定任何位置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

“搜索”策略设置

Dec 05, 2017

“搜索” 部分包含的策略设置用于指定是否将 “搜索”文件夹的内容重定向到共享网络位置。

“搜索”的重定向设置

此设置指定如何重定向“搜索”文件夹的内容。

默认情况下，内容重定向到 UNC 路径。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“搜索”路径

此设置指定“搜索”文件夹的内容将重定向到的网络位置。

默认情况下，此设置处于禁用状态，不指定任何位置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

“开始”菜单策略设置

Dec 05, 2017

“开始菜单” 部分包含的策略设置用于指定是否将“开始菜单”文件夹的 内容重定向到共享网络位置。

“开始”菜单的重定向设置

此设置指定如何重定向“开始”菜单文件夹的内容。

默认情况下，内容重定向到 UNC 路径。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“开始”菜单路径

此设置指定“开始”菜单文件夹的内容将重定向到的网络位置。

默认情况下，此设置处于禁用状态，不指定任何位置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

“视频”策略设置

Dec 05, 2017

“视频”部分 包含的策略设置用于指定是否将 “视频”文件夹的内容重定向到共享网络位置。

“视频”的重定向设置

此设置指定如何重定向“视频”文件夹的内容。

默认情况下，内容重定向到 UNC 路径。

要控制如何重定向“视频”文件夹的内容，请选择以下选项之一：

- 重定向到以下 UNC 路径。将内容重定向到 “视频” 路径策略设置中指定的 UNC 路径。
- 相对于 “文档”文件夹重定向。将内容重定向到相对于“文档”文件夹的文件夹。

要将内容重定向到相对于“文档”文件夹的文件夹，必须启用 “文档”路径设置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“视频”路径

此设置指定“视频”文件夹的内容将重定向到的网络位置。

默认情况下，此设置处于禁用状态，不指定任何位置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

“日志”策略设置

Dec 05, 2017

“日志”部分 包含的策略设置用于配置 Profile Management 日志记录。

Active Directory 操作

此设置启用或禁用对 Active Directory 中执行的操作进行详细日志记录。

默认情况下，禁用此设置。

启用此设置时，请确保也启用 启用日志记录设置。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则将记录错误和常规信息。

常规信息

此设置启用或禁用对常规信息进行详细日志记录。

默认情况下，禁用此设置。

启用此设置时，请确保也启用 启用日志记录设置。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则将记录错误和常规信息。

常见警告

此设置启用或禁用对常见警告进行详细日志记录。

默认情况下，禁用此设置。

启用此设置时，请确保也启用 启用日志记录设置。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则将记录错误和常规信息。

启用日志记录

此设置启用或禁用在调试（详细日志记录）模式下进行 Profile Management 日志记录。 在调试模式下，大量的状态信息记录在“%SystemRoot%\System32\Logfiles\UserProfileManager”下的日志文件中。

默认情况下，禁用此设置，只记录错误。

Citrix 建议您仅在对 Profile Management 进行故障排除时才启用此设置。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则将只记录错误。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

文件系统操作

此设置启用或禁用对文件系统中执行的操作进行详细日志记录。

默认情况下，禁用此设置。

启用此设置时，请确保也启用 启用日志记录设置。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则将记录错误和常规信息。

文件系统通知

此设置启用或禁用对文件系统通知进行详细日志记录。

默认情况下，禁用此设置。

启用此设置时，请确保也启用 启用日志记录设置。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则将记录错误和常规信息。

注销

此设置启用或禁用对用户注销进行详细日志记录。

默认情况下，禁用此设置。

启用此设置时，请确保也启用 启用日志记录设置。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则将记录错误和常规信息。

登录

此设置启用或禁用对用户登录进行详细日志记录。

默认情况下，禁用此设置。

启用此设置时，请确保也启用 启用日志记录设置。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则将记录错误和常规信息。

日志文件最大大小

此设置指定 Profile Management 日志文件的最大允许大小（以字节为单位）。

默认情况下，此项设置为 1048576 字节 (1 MB)。

如果您有足够的磁盘 空间，Citrix 建议您 将此文件的大小增加到 5 MB 或更高。如果日志文件大小超出最大大小，则将删除现有文件备份 (.bak)，将日志文件重命名为 .bak，并创建一个新日志文件。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

日志文件在 %SystemRoot%\System32\Logfiles\UserProfileManager 中创建。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则将使用默认值。

日志文件路径

此设置指定用于保存 Profile Management 日志文件的备用路径。

默认情况下，禁用此设置，日志文件保存在默认位置：%SystemRoot%\System32\Logfiles\UserProfileManager。

该路径可以指向本地驱动器或基于网络的远程驱动器（UNC 路径）。 远程路径在大型分布式环境中很有用，但可能会带来大量网络流量，因此可能不适用于日志文件。 对于已置备的具有静态硬盘驱动器的虚拟机，应设置该驱动器的一个本地路径。 这样可以确保重新启动虚拟机时能够保留日志文件。对于没有静态硬盘驱动器的虚拟机，设置一个 UNC 路径让您能够保留日志文件，但该虚拟机的系统帐户必须具有对 UNC 共享的写入权限。 对于受脱机配置文件功能管理的任何便携式计算机，应使用本地路径。

如果对日志文件使用的是 UNC 路径，Citrix 建议对日志文件文件夹应用恰当的访问控制列表，以确保只有授权用户或计算机帐户能够访问存储的文件。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则使用默认位置 %SystemRoot%\System32\Logfiles\UserProfileManager。

个性化用户信息

此设置启用或禁用对个性化用户信息进行详细日志记录。

默认情况下，禁用此设置。

启用此设置时，请确保也启用 启用日志记录设置。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则将记录错误和常规信息。

登录和注销时的策略值

此设置启用或禁用对用户登录和注销时的策略值进行详细日志记录。

默认情况下，禁用此设置。

启用此设置时，请确保也启用 启用日志记录设置。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则将记录错误和常规信息。

注册表操作

此设置启用或禁用对在注册表中执行的操作进行详细日志记录。

默认情况下，禁用此设置。

启用此设置时，请确保也启用 启用日志记录设置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则将记录错误和常规信息。

注销时的注册表差异

此设置启用或禁用对用户注销时的任何注册表差异进行详细日志记录。

默认情况下，禁用此设置。

启用此设置时，请确保也启用 启用日志记录设置。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则将记录错误和常规信息。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

“配置文件处理”策略设置

Dec 05, 2017

“配置文件处理” 部分包含的策略设置用于配置 Profile Management 对 用户配置文件的处理方式。

删除缓存的配置文件之前的延迟

此设置 指定注销时 Profile Management 在删除本地缓存的 配置文件之前的可选延迟时间（分钟）。

值为 0 时会在注销过程结束时立即删除配置文件。 Profile Management 每分钟检查一次注销，因此值为 60 可确保在用户注销后一到两分钟内删除配置文件（取决于最后一次检查的时间）。 如果已知注销期间进程会使文件或用户注册表配置单元处于打开状态，延长延迟时间将很有用。 对于大型配置文件，这种做法还可以加快注销速度。

默认情况下，此参数设置为 0，Profile Management 会立即删除本地缓存的配置文件。

启用此设置时，请确保“注销时删除本地缓存的配置文件”也处于启用状态。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则会立即删除配置文件。

注销时删除本地缓存的配置文件

此设置指定在用户注销后是否删除本地缓存的配置文件。

如果启用此设置，用户注销后，将删除其本地配置文件缓存。 Citrix 建议您为终端服务器启用此设置。

默认情况下，此设置处于禁用状态，用户注销后，将继续保留用户本地配置文件缓存。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果该设置没有在此配置，也不在 INI 文件中，则不会删除缓存的配置文件。

本地配置文件冲突处理

If you enable the Citrix Personalization for App-V - VDA check box在既存在用户存储中的用户配置文件，又存在本地 Windows 用户配置文件（非 Citrix 用户配置文件）的情况下，此设置用于配置 Profile Management 的行为。

默认情况下，Profile Management 将使用本地 Windows 配置文件，但不通过任何方式更改该配置文件。

要控制 Profile Management 的行为，请选择以下选项之一：

- 使用本地 配置文件。Profile Management 将使用本地配置文件，但不通过任何方式更改该配置文件。
- 删除本地 配置文件。Profile Management 将删除本地 Windows 用户配置文件，然后导入用户存储中的 Citrix 用户配置文件。
- 重命名本地 配置文件。Profile Management 将重命名本地 Windows 用户配置文件（用于备份），然后导入用户存储中的 Citrix 用户配置文件。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果该设置没有在此配置，也不在 INI 文件中，则使用现有本地配置文件。

迁移现有配置文件

© 1999-2017 Citrix Systems, Inc. All rights reserved.

此设置指定当用户在用户存储中没有当前配置文件时，会在登录期间迁移到用户存储的配置文件的类型。

如果用户在用户存储中没有配置文件，则登录期间 Profile Management 可以即时迁移现有配置文件。 此后，Profile Management 将在当前会话以及通过相同用户存储路径配置的任何其他会话中使用用户存储配置文件。

默认情况下，会在登录期间将本地配置文件和漫游配置文件迁移到用户存储。

要指定登录期间迁移到用户存储的配置文件的类型，请选择以下选项之一：
- 本地配置文件和漫游 配置文件 。
- 本地
- 漫游
- 无（已禁用）

如果选择“无”，系统将使用现有 Windows 机制创建新配置文件，就像在未安装 Profile Management 的环境中一样。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果该设置没有在此配置，也不在 .ini 文件中，则将迁移现有的本地配置文件和漫游配置文件。

模板配置文件的路径

此设置指定希望 Profile Management 用来创建新用户配置文件的模板配置文件的路径。

指定的路径必须为文件夹的完整路径，其中包含 NTUSER.DAT 注册表文件以及模板配置文件所需的其他任何其他文件夹和文件。
注意： 请勿在路径中包括 NTUSER.DAT。 例如，对于文件 \\myservername\myprofiles\template\ntuser.dat，应将路径设置为 \\myservername\myprofiles\template。
应使用绝对路径，绝对路径可以是 UNC 路径，也可以是本地计算机上的路径。 例如，可以使用后者指定永久存在于 Citrix Provisioning Services 映像中的模板配置文件。 不支持相对路径。

注意：此设置不支持扩展 Active Directory 属性、系统环境变量或 %USERNAME% 和 %USERDOMAIN% 变量。
默认情况下，此设置处于禁用状态，系统将根据用户首次登录的设备上的默认用户配置文件创建新用户配置文件。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果未在此处也未在 .ini 文件中配置此设置，则不使用任何模板。

模板配置文件覆盖本地配置文件

此设置允许在创建新用户配置文件时以模板配置文件覆盖本地配置文件。

如果用户没有 Citrix 用户配置文件，但存在本地 Windows 用户配置文件，默认情况下将使用本地配置文件（如果没有禁用迁移，还将会迁移至用户存储）。 启用此策略设置后，模板配置文件可以覆盖在创建新用户配置文件时所使用的本地配置文件。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果未在此处也未在 .ini 文件中配置此设置，则不使用任何模板。

模板配置文件覆盖漫游配置文件

此设置可在创建新用户配置文件时以模板配置文件覆盖漫游配置文件。

如果用户没有 Citrix 用户配置文件，但存在漫游 Windows 用户配置文件，则默认情况下将使用漫游配置文件（如果没有禁用迁移，还会迁移至用户存储）。 启用此策略设置后，模板配置文件可以覆盖在创建新用户配置文件时所使用的漫游配置文件。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果未在此处也未在 .ini 文件中配置此设置，则不使用任何模板。

模板配置文件用作所有登录的 Citrix 强制配置文件

此设置使 Profile Management 可以将模板配置文件用作创建所有新用户配置文件时使用的默认配置文件。

默认情况下，此设置处于禁用状态，系统将根据用户首次登录的设备上的默认用户配置文件创建新用户配置文件。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果未在此处也未在 .ini 文件中配置此设置，则不使用任何模板。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

“注册表”策略设置

Dec 05, 2017

“注册表”部分 包含的策略设置用于指定在 Profile Management 处理中要包含或 排除的注册表项。

排除列表

此设置指定 HKCU 配置单元中注册表项的列表，当用户注销时，这些注册表项将从 Profile Management 处理中排除。

如果启用此项，当用户注销时，会从处理中排除此列表中指定的注册表项。

默认情况下，禁用此设置，当用户注销时，会处理 HKCU 配置单元中的所有注册表项。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则不会从处理中排除任何注册表项。

包含列表

此设置指定 HKCU 配置单元中注册表项的列表，当用户注销时，这些注册表项将包括在 Profile Management 处理中。

如果启用此项，当用户注销时，仅处理此列表中指定的注册表项。

默认情况下，禁用此设置，当用户注销时，会处理 HKCU 配置单元中的所有注册表项。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则将处理整个 HKCU。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

“流用户配置文件”策略设置

Dec 05, 2017

“流用户 配置文件”部分包含的策略设置用于指定 Profile Management 处理流用户配置文件的方式。

总是缓存

此设置指定 Profile Management 在用户登录后是否立即缓存流文件。 在用户登录后缓存文件可以节省网络带宽，从而增强用户体验。

将此设置与 Profile Streaming 设置结合使用。

默认情况下，禁用此设置，用户登录后不会立即缓存流文件。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则禁用此设置。

总是缓存的大小

此设置指定通过流技术推送的文件大小的下限（以 MB 为单位）。 Profile Management 会在用户登录后立即缓存任何等于或大于此大小的文件。

默认情况下，将其设置为 0（零），并使用 缓存整个配置文件功能。 启用缓存整个配置文件功能时，Profile Management 会在用户登录后，通过后台任务提取用户存储中的所有配置文件内容。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则禁用此设置。

Profile Streaming

此设置启用和禁用 Citrix 流用户配置文件功能。 如果启用，只有当用户在登录后访问配置文件中的文件和文件夹时，这些文件和文件夹才会从用户存储提取到本地计算机中。 注册表项以及挂起区域中的文件会立即提取。

默认情况下，禁用 Profile Streaming。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则禁用此设置。

流用户配置文件组

此设置基于 Windows 用户组指定通过流技术推送 OU 中的哪些用户配置文件。

启用时，仅通过流技术推送指定用户组中的用户配置文件。 所有其他用户配置文件将按正常方式进行处理。

默认情况下，禁用此设置，OU 中的所有用户配置文件将按正常方式进行处理。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则会处理所有用户配置文件。

启用 Profile Streaming 排除

© 1999-2017 Citrix Systems, Inc. All rights reserved.

启用 Profile Streaming 排除后，Profile Management 不会对排除列表中的文件夹执行流操作，用户登录时，所有文件夹会立即从用户存储中提取到本地计算机。

有关详细信息，请参阅启用 Profile Streaming 排除。

挂起区域锁定文件超时

此设置指定天数，如果服务器无响应并且用户存储处于锁定状态，则经过这些天后，用户文件从挂起区域写回到用户存储。 这样可以防止挂起区域膨胀，并确保用户存储始终包含最新的文件。

默认情况下，此项设置为 1（一）天。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果在此处和 .ini 文件中均未配置此设置，则将使用默认值。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Receiver 策略设置

Dec 05, 2017

注意：除非另有说明，否则 Receiver 是指 Citrix Receiver。

Receiver 部分包含的策略设置用于指定要推送到虚拟桌面上运行的 Citrix Receiver for Windows 的 Storefront 地址列表。

StoreFront 帐户列表

此设置指定一个 StoreFront 存储列表，管理员可选择将其推送到在虚拟桌面上运行的 Citrix Receiver for Windows。创建交付组时，管理员可选择要将哪些存储推送到在此组内的虚拟桌面上运行的 Citrix Receiver for Windows。

默认情况下，不指定任何存储。

对于每个存储，以分号分隔条目的形式指定以下信息：

- 应用商店名称。向存储用户显示的名称。
- 存储 URL。存储的 URL。
- 存储启用状态。存储是否可供用户使用。此状态为“启用”或“禁用”。
- 存储说明。显示给存储用户的说明。

例如：Sales Store;https://sales.mycompany.com/Citrix/Store/discovery;On;Store for Sales staff

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Virtual Delivery Agent 策略设置

Dec 05, 2017

Virtual Delivery Agent (VDA) 部分包含的策略设置可以控制 VDA 与站点控制器之间的通信。

重要：如果没有使用自动更新功能，VDA 需要使用这些设置提供的信息向 Delivery Controller 注册。由于此信息是进行注册所必需的信息，因此，除非在 VDA 安装期间提供了此信息，否则必须使用组策略编辑器配置下列设置：

- 控制器注册 IPv6 网络掩码
- 控制器注册端口
- 控制器 SID
- 控制器
- 仅使用 IPv6 控制器注册
- 站点 GUID

控制器注册 IPv6 网络掩码

此策略设置允许管理员将 VDA 限制为仅在首选的子网（而非全局 IP，如果已注册）中使用。此设置指定 VDA 要注册的 IPv6 地址和网络。VDA 将仅在与指定网络掩码匹配的第一个地址上进行注册。仅当启用仅使用“IPv6 控制器注册”策略设置时，此设置才有效。

默认情况下，此设置为空。

控制器注册端口

仅当禁用“启用控制器自动更新”设置时，才使用此设置。

此设置指定 VDA 向控制器注册时所用的 TCP/IP 端口号（如果使用基于注册表的注册方式）。

默认情况下，此端口号设置为 80。

控制器 SID

仅当禁用“启用控制器自动更新”设置时，才使用此设置。

此设置指定 VDA 向控制器注册时所用的控制器安全标识符 (SID) 的空格分隔列表（如果使用基于注册表的注册方式）。此设置为可选设置，可与控制器设置结合使用，用以限制可用于注册的控制器列表。

默认情况下，此设置为空。

控制器

仅当禁用“启用控制器自动更新”设置时，才使用此设置。

此设置用于指定 VDA 向控制器注册时所用的控制器完全限定域名 (FQDN) 的空格分隔列表（如果使用基于注册表的注册方式）。此设置为可选设置，可与控制器 SID 设置结合使用。

默认情况下，此设置为空。

启用控制器自动更新

通过此设置，VDA 可在安装后自动向控制器注册。

VDA 注册后，注册的控制器将向 VDA 发送当前控制器 FQDN 和 SID 的列表。VDA 会将此列表写入到静态存储。每个控制器还

© 1999-2017 Citrix Systems, Inc. All rights reserved.

将每隔 90 分钟在站点数据库中检查一次控制器信息；如果在上次检查后添加或删除了控制器，或者如果策略发生更改，控制器将向注册的 VDA 发送更新后的列表。VDA 将接受所接收最新列表中的所有控制器的连接。

默认情况下，此设置处于启用状态。

仅使用 IPv6 控制器注册

此设置可控制 VDA 向控制器注册时所用的地址格式：

- 启用后，VDA 将使用计算机的 IPv6 地址向控制器注册。当 VDA 与控制器进行通信时，将使用以下地址顺序：全局 IP 地址、唯一本地地址 (ULA)、链接本地地址（如果没有其他可用的 IPv6 地址）。
- 禁用后，VDA 将使用计算机的 IPv4 地址向控制器注册并与之通信。

默认情况下，禁用此设置。

站点 GUID

仅当禁用“启用控制器自动更新”设置时，才使用此设置。

此设置用于指定 VDA 向控制器注册时所用的站点的全局唯一标识符 (GUID)（如果使用基于 Active Directory 的注册方式）。

默认情况下，此设置为空。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

HDX 3D Pro 策略设置

Dec 05, 2017

HDX 3D Pro 部分包含用于为用户启用和配置图像质量 配置工具的策略设置。该工具使用户能够实时调整图像质量 与响应速度之间的平衡点，从而优化对 可用带宽的使用情况。

启用无损

此设置指定用户是否能够使用图像质量配置工具启用和禁用无损压缩功能。 默认情况下，用户可以选择启用无损压缩功能。

用户启用无损压缩功能后，图像质量将自动设置为在图像配置工具中可用的最大值。 默认情况下，可以根据用户设备和主机计算机的功能，使用基于 GPU 或 CPU 的压缩。

HDX 3D Pro 质量设置

此设置指定图像质量配置工具中用于定义用户可用的图像质量调整范围的最小值和最大值。

可以指定 0 到 100 之间（包括 0 和 100）的图像质量值。 最大值必须大于或等于最小值。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

监视策略设置

Dec 05, 2017

“监视”部分包含用于进程、资源监视和应用程序故障监视的策略设置。

这些策略的作用域可以根据站点、交付组、交付组类型、组织单位和标记进行定义。

用于进程和资源监视的策略

CPU、内存和进程的每个数据点均通过 VDA 收集，并存储在监视数据库中。发送来自 VDA 的数据点会消耗网络带宽，存储这些数据点会占用监视数据库中的大量空间。如果您不想监视某一特定作用域（例如，特定的交付组或组织单位）的资源数据或/和进程数据，建议您禁用此策略。

启用进程监视

启用此设置以通过 VDA 监视计算机上运行的进程。诸如 CPU 和内存使用等统计信息会发送至 Monitoring Service。该统计信息用于 Director 中的实时通知和历史报告。

此设置默认情况下为禁用。

启用资源监视

启用此设置以通过 VDA 监视计算机上的关键性能计数器。统计信息（例如 CPU 和内存数据、IOPS 和磁盘延迟数据）会发送至 Monitoring Service。该统计信息用于 Director 中的实时通知和历史报告。

此设置默认情况下为启用。

可扩展性

CPU 和内存数据按 5 分钟间隔从每个 VDA 推送至数据库；进程数据（如已启用）按 10 分钟间隔推送至数据库。IOPS 和磁盘延迟数据按 1 小时间隔推送至数据库。

CPU 和内存数据

CPU 和内存数据默认情况下为**启用**。数据保留期限值如下（Platinum 许可证）：

数据粒度	天数
5 分钟数据	1 天
10 分钟数据	7 天
小时数据	30 天
日数据	90 天

© 1999-2017 Citrix Systems, Inc. All rights reserved.

IOPS 和磁盘延迟数据

默认情况下，**启用** IOPS 和磁盘延迟数据。数据保留期限值如下（Platinum 许可证）：

数据粒度	天数
小时数据	3 天
日数据	90 天

根据上文所述的数据保留期限设置，大约需要 276 KB 的磁盘空间即可存储一个 VDA 一年时间的 CPU、内存、IOPS 和磁盘延迟数据。

计算机数	所需的大约存储
1	276 KB
1K	270 MB
40K	10.6 GB

进程数据

默认情况下，**禁用**进程数据。建议根据需要对一部分计算机启用进程数据。进程数据的默认数据保留设置如下：

数据粒度	天数
10 分钟数据	1 天
小时数据	7 天

如果进程数据已启用，在使用默认保留设置的情况下，进程数据在为期一年的时间内每 VDA 会消耗大约 1.5 MB，每终端服务 VDA (TS VDA) 会消耗大约 3 MB。

计算机数	VDA 所需的大约存储	TS VDA 所需的大约存储
1	1.5 MB	3 MB
1K	1.5 GB	3 GB

© 1999-2017 Citrix Systems, Inc. All rights reserved.

> **注意**
>
> 以上数字不包含索引空间。同时，所有上述计算为近似计算，可能依部署的不同而有所不同。

可选配置

您可以修改默认保留期限设置以满足您的需求。但是，这会占用额外的存储空间。通过启用以下设置，您可以获得更高的进程利用率数据准确性。可以启用的配置为：

EnableMinuteLevelGranularityProcessUtilization

EnableDayLevelGranularityProcessUtilization

这些配置可以通过 Monitoring Powershell cmdlet 来启用：Set-MonitorConfiguration

应用程序故障监视策略

默认情况下，**应用程序故障**选项卡仅显示服务器操作系统 VDA 中的应用程序故障。可以通过以下监视策略修改应用程序故障监视的设置：

启用应用程序故障的监视

使用此设置可配置应用程序故障监视，以监视应用程序错误或故障（崩溃和未处理的异常），或者监视两者。
通过将**值**设置为**无**禁用应用程序故障监视。
此设置的默认值为“仅限应用程序故障”。

在桌面操作系统 VDA 上启用应用程序故障的监视

默认情况下，仅监视服务器操作系统 VDA 上托管的应用程序中的故障。要监视桌面操作系统 VDA，请将此策略设置为**允许**。
此设置的默认值为**禁止**。

从故障监视中排除的应用程序列表

指定不监视其故障的应用程序的列表。
此列表默认为空。

存储计划提示

组策略。如果您对监视资源数据或进程数据不感兴趣，可以使用组策略来关闭两者或其中之一。有关详细信息，请参阅创建策略的“组策略”部分。

数据整理。可以对默认的数据保留设置进行修改，以尽早整理数据并释放存储空间。有关整理设置的详细信息，请参阅使用 API 访问数据中的数据粒度和保留。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

虚拟 IP 策略设置

Dec 05, 2017

“虚拟 IP”部分包含的策略设置用于控制会话是否具有自己的虚拟环回地址。

虚拟 IP 环回支持

启用此设置时，每个会话具有自己的虚拟环回地址。 禁用时，会话不具有单独的虚拟环回地址。

默认情况下，禁用此设置。

虚拟 IP 虚拟环回程序列表

此设置指定可使用虚拟环回地址的应用程序可执行文件。 将程序添加到列表时，仅指定可执行文件名称，无需指定完整路径。

默认情况下，不指定任何可执行文件。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

使用注册表配置 COM 端口和 LPT 端口重定向设置

Feb 19, 2018

在 VDA 版本 7.0 到 7.8 中，COM 端口和 LPT 端口设置只能使用注册表进行配置。对于 7.0 之前的 VDA 版本和 VDA 7.9 及更高版本，这些设置可以在 Studio 中进行配置。有关详细信息，请参阅端口重定向策略设置和带宽策略设置。

用于 COM 端口和 LPT 端口重定向的策略设置位于 VDA 映像或计算机上的 HKLM\Software\Citrix\GroupPolicy\Defaults\Deprecated 下方 。

要启用 COM 端口 和 LPT 端口重定向，请添加类型为 REG_DWORD 的新注册表项，如下所示：

小心： 注册表编辑不当会导致严重问题，可能需要重新安装操作系统。 Citrix 无法保证因“注册表编辑器”使用不当导致出现的问题能够得以解决。 使用“注册表编辑器”需自担风险。 在编辑注册表之前，请务必进行备份。

注册表项	说明	允许使用的值
AllowComPortRedirection	允许或禁止使用 COM 端口重定向	1（允许）或 0（禁止）
LimitComBw	COM 端口重定向通道的带宽限制	数值
LimitComBWPercent	COM 端口重定向通道的带宽限制（占总会话带宽的百分比）	0 到 100 之间的数值
AutoConnectClientComPorts	从用户设备自动连接 COM 端口	1（允许）或 0（禁止）
AllowLptPortRedirection	允许或禁止使用 LPT 端口重定向	1（允许）或 0（禁止）
LimitLptBw	LPT 端口重定向通道的带宽限制	数值
LimitLptBwPercent	LPT 端口重定向通道的带宽限制（占总会话带宽的百分比）	0 到 100 之间的数值
AutoConnectClientLptPorts	从用户设备自动连接 LPT 端口	1（允许）或 0（禁止）

配置这些设置后，请修改您的计算机目录，使其使用新主映像或更新的物理机。用户下次注销时，将使用新设置更新桌面。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Connector for Configuration Manager 2012 策略设置

Dec 05, 2017

Connector for Configuration Manager 2012 部分包含用于配置 Citrix Connector 7.5 代理的策略设置。

重要：警告、注销和重新启动消息策略仅适用于手动管理或由 Provisioning Services 管理的服务器操作系统计算机目录的部署。对于这些计算机目录，当存在待定的应用程序安装 或软件更新时，Connector 服务将向用户 发出警报。
对于 MCS 管理的目录，使用 Studio 通知用户。对于手动管理的桌面操作系统目录，使用 Configuration Manager 通知用户。
对于由 Provisioning Services 管理的桌面操作系统目录，使用 Provisioning Services 通知用户。

提前警告频率时间间隔

此设置定义将提前警告消息显示给用户的时间间隔。

时间间隔的设置采用 ddd.hh:mm:ss 格式，其中：
- ddd 为天数， 为介于 0 到 999 之间的可选参数。
- hh 为介于 0 到 23 之间的小时数。
- mm 为介于 0 到 59 之间的分钟数。
- ss 为介于 0 到 59 之间的秒数。

默认情况下，间隔设置为 1 小时 (01:00:00)。

提前警告消息框正文文本

此设置包含显示给用户的可编辑消息文本，用以通知用户即将进行软件更新或维护，需要用户注销。

默认情况下，消息为：“{TIMESTAMP} Please save your work. The server will go offline for maintenance in {TIMELEFT}”（{TIMESTAMP} 请保存您的工作。服务器将在 {TIMELEFT} 内脱机进行维护）

提前警告消息框标题

此设置包含显示给用户的提前警告消息的可编辑标题栏文本。

默认情况下，标题为：“Upcoming Maintenance”（即将进行维护）

提前警告时间段

此设置定义在维护前多久首次显示提前警告消息。

时间是使用 ddd.hh:mm:ss 格式设置的，其中:
- ddd 为天数， 为介于 0 到 999 之间的可选参数。
- hh 为介于 0 到 23 之间的小时数。
- mm 为介于 0 到 59 之间的分钟数。
- ss 为介于 0 到 59 之间的秒数。

默认情况下，该设置为 16 小时 (16:00:00)，表示第一个提前警告消息大约在维护前 16 小时显示。

最终强制注销消息框正文文本

此设置包含可编辑的消息文本，警告用户开始强制注销。

默认情况下，消息为：“The server is currently going offline for maintenance”（服务器当前正在进入脱机模式以进行维护）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

最终强制注销消息文本框标题

此设置包含最终强制注销消息的可编辑标题栏文本。

默认情况下，标题为：“Notification From IT Staff”（来自 IT 人员的通知）

强制注销宽限期

此设置定义从通知用户注销到实施强制注销以处理待解决维护之间的时间段。

时间是使用 ddd.hh:mm:ss 格式设置的，其中:

- ddd 为天数， 为介于 0 到 999 之间的可选参数。
- hh 为介于 0 到 23 之间的小时数。
- mm 为介于 0 到 59 之间的分钟数。
- ss 为介于 0 到 59 之间的秒数。

默认情况下，强制注销宽限期设置为 5 分钟 (00:05:00)。

强制注销消息框正文文本

此设置包含可编辑的文本，在开始强制注销之前通知用户保存其工作并注销。

默认情况下，此消息中包含以下内容：“{TIMESTAMP} Please save your work and log off. The server will go offline for maintenance in {TIMELEFT}”（{TIMESTAMP} 请保存您的工作并注销。服务器将在 {TIMELEFT} 内脱机进行维护）

强制注销消息文本框标题

此设置包含强制注销消息的标题栏的可编辑文本。

默认情况下，标题为：“Notification From IT Staff”（来自 IT 人员的通知）

托管映像模式

Connector Agent 将自动检测其是在 Provisioning Services 还是 MCS 管理的 计算机克隆上运行。该 Agent 会阻止 Configuration Manager 在托管映像克隆上更新， 并自动在目录的主映像上安装更新。

更新主 映像后，请使用 Studio 调配 MCS 目录克隆的重新启动行为。在 Configuration Manager 维护时段， Connector Agent 将自动调配 PVS 目录克隆的 重新启动行为。要覆盖 此行为以便软件由 Configuration Manager 安装在目录克隆上， 请将托管映像模式更改为已禁用。

重新启动消息框正文文本

此设置包含可编辑的消息文本，用于在服务器即将重新启动时通知用户。

默认情况下，消息为：“The server is currently going offline for maintenance”（服务器当前正在进入脱机模式以进行维护）

代理任务运行的常规时间间隔

此设置决定 Citrix Connector Agent 任务的运行频率。

时间是使用 ddd.hh:mm:ss 格式设置的，其中:

- ddd 为天数， 为介于 0 到 999 之间的可选参数。
- hh 为介于 0 到 23 之间的小时数。
- mm 为介于 0 到 59 之间的分钟数。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- ss 为介于 0 到 59 之间的秒数。

默认情况下，常规时间间隔设置为 5 分钟 (00:05:00)。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

管理权限

Dec 05, 2017

管理 XenApp 或 XenDesktop 站点包括各种项目和任务。

许可

创建站点时，需要与 Citrix 许可证服务器建立有效连接。之后，可以从 Studio 完成各种许可任务，包括添加许可证、更改许可证类型或模式以及管理许可证管理员。还可以从 Studio 访问许可证管理控制台。

应用程序

管理交付组和应用程序组（可选）中的应用程序。

区域

在地理位置分散的部署中，可以使用区域使应用程序和桌面距离用户更近，这样可以改善性能。安装和配置站点时，所有 Controller、计算机目录和主机连接位于一个主区域中。之后，您可以使用 Studio 创建包含这些项目的卫星区域。站点具有多个区域后，可以指定新创建的计算机目录、主机连接或添加的 Controller 将位于哪个区域。还可以在区域之间移动项目。

连接和资源

如果要使用虚拟机管理程序或云服务托管将向用户交付应用程序和桌面的计算机，应在创建站点时创建与该虚拟机管理程序或云服务的第一个连接。此连接的存储和网络详细信息形成其*资源*。之后，可以更改此连接及其资源并创建新连接。您还可以管理使用已配置连接的计算机。

本地主机缓存

本地主机缓存允许在 Delivery Controller 与站点数据库之间的连接失败时站点中的连接代理操作继续执行。它是 Citrix 为 XenApp 和 XenDesktop 提供的最全面的高可用性功能。

连接租用

Citrix 建议尝试使用本地主机缓存，而不是连接租用。本地主机缓存是更强大的替代功能。

虚拟 IP 和虚拟环回

Microsoft 虚拟 IP 地址功能为每个会话的已发布应用程序提供动态分配的唯一 IP 地址。借助 Citrix 虚拟环回功能，可以将依赖于与 localhost（默认为 127.0.0.1）通信的应用程序配置为使用 localhost 范围 (127.*) 之内的唯一虚拟环回地址。

Delivery Controller

本文详细介绍在站点中添加和删除 Controller 时的考虑事项和过程。此外还介绍如何将 Controller 移至另一个区域或站点，以及如何将 VDA 移至另一个站点。

向 Controller 注册 VDA

VDA 必须向 Controller 注册（建立通信）才能有助于应用程序和桌面的交付。可以按多种方式指定 Controller 地址，本文对这些方式进行了介绍。在站点中添加、移动和删除 Controller 时，VDA 及时具有最新信息至关重要。

会话

© 1999-2017 Citrix Systems, Inc. All rights reserved.

维护会话处于活动状态对于提供最佳用户体验至关重要。多项功能可以优化会话的可靠性，减少不便之处、停机时间以及生产力损失。

- 会话可靠性
- 客户端自动重新连接
- ICA 保持活动状态
- 工作区控制
- 会话漫游

在 Studio 中使用搜索

如果希望在 Studio 中查看有关计算机、会话、计算机目录、应用程序或交付组的信息，可使用灵活的搜索功能。

标记

使用标签来识别各个项目，例如计算机、应用程序、组和策略。然后，您可以自定义特定操作以应用于带有特定标签的项目。

IPv4/IPv6

XenApp 和 XenDesktop 支持纯 IPv4 部署、纯 IPv6 部署，以及使用重叠 IPv4 和 IPv6 网络的双协议栈部署。本文介绍并举例说明这些部署。本文还介绍控制使用 IPv4 还是 IPv6 的 Citrix 策略设置。

用户配置文件

默认情况下，安装 VDA 会自动安装 Citrix Profile Management。如果使用此配置文件解决方案，查阅本文可了解常规信息，有关完整的详细信息，可参阅 Profile Management 文档。

Citrix Insight Services

Citrix Insight Services (CIS) 是用于性能监测、遥测以及生成业务洞察的 Citrix 平台。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

许可

Dec 05, 2017

> **注意**
>
> Studio 和 Director 不支持 Citrix License Server VPX。有关 Citrix License Server VPX 的详细信息，请参阅 Citrix Licensing 文档。

如果许可证服务器与 Studio 位于相同的域内或位于可信域内，则可以通过 Studio 管理和跟踪许可。有关其他许可任务的信息，请参阅许可文档和多类型许可。

您必须是完全权限许可证管理员才能完成下述任务（查看许可证信息除外）。要在 Studio 中查看许可证信息，管理员必须至少具有读取许可委派管理权限；内置的完全权限管理员和只读权限管理员角色具有该权限。

下表列出了支持的版本和许可证模式：

产品	版本	许可模式
XenApp	• 铂金版 • 企业 • 高级	并发
XenDesktop	• 铂金版 • 企业 • 应用程序 • VDI Edition	• 用户/设备 • 并发

要查看许可证信息，请**在 Studio 导航窗格中**选择 配置 > 许可。此时将显示站点的许可证使用情况和设置的摘要，同时显示当前安装在指定许可证服务器上的所有许可证的列表。

从 Citrix 下载许可证：

1. 在 Studio 导航窗格中，选择**配置 > 许可**。
2. 在“操作”窗格中选择**分配许可证**。
3. 键入许可证访问代码，此代码在 Citrix 发送的电子邮件中提供。
4. 选择产品并单击**分配许可证**。系统将分配并下载适用于该产品的所有许可证。分配并下载适用于特定许可证访问代码的所有许可证后，将无法再次使用该许可证访问代码。要使用该代码执行其他交易，请登录“我的账户”。

添加存储在本地计算机或网络上的许可证：

1. 在 Studio 导航窗格中，选择**配置 > 许可**。
2. 在“操作”窗格中选择**添加许可证**。
3. 浏览到许可证文件并将其添加到许可证服务器中。

更改许可证服务器：

1. 在 Studio 导航窗格中，选择**配置 > 许可**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. 在“操作”窗格中选择**更改许可证服务器**。
3. 以 name:port 格式键入许可证服务器的地址，其中，name 为 DNS、NetBIOS 或 IP 地址。如果不指定端口号，则会使用默认端口 (27000)。

选择要使用的许可证类型：

- 配置站点时，在指定许可证服务器之后，系统会提示您选择要使用的许可证类型。如果服务器上没有许可证，则会自动选择在没有许可证的情况下试用产品 30 天的选项。
- 如果服务器上有许可证，则会显示其详细信息，您可以选择其中的一个许可证。或者，您可以将许可证文件添加到服务器中，然后选择该文件。

更改产品版本和许可模式：

1. 在 Studio 导航窗格中，选择**配置 > 许可**。
2. 在“操作”窗格中选择**编辑产品版本**。
3. 更新相应选项。

要访问许可证管理控制台，请在“操作”窗格中选择**许可证管理控制台**。控制台将立即显示，或者如果将控制板配置为受密码保护，系统将提示您输入许可证管理控制台凭据。有关如何使用控制台的详细信息，请参阅许可文档。

添加许可管理员：

1. 在 Studio 导航窗格中，选择**配置 > 许可**。
2. 在中间窗格中选择许可管理员选项卡。
3. 在“操作”窗格中选择**添加许可管理员**。
4. 浏览找到要作为管理员添加的用户，然后选择权限。

要更改许可管理员的权限或删除许可管理员，请执行以下操作：

1. 在 Studio 导航窗格中，选择**配置 > 许可**。
2. 在中间窗格中选择许可管理员选项卡，然后选择管理员。
3. 在“操作”窗格中，选择**编辑许可管理员**或**删除许可管理员**。

添加许可管理员组：

1. 在 Studio 导航窗格中，选择**配置 > 许可**。
2. 在中间窗格中选择许可管理员选项卡。
3. 在“操作”窗格中选择**添加许可管理员组**。
4. 浏览找到要作为许可管理员的组，然后选择权限。添加 Active Directory 组可以将许可管理员权限授予该组内的用户。

要更改许可管理员组的权限或删除许可管理员组，请执行以下操作：

1. 在 Studio 导航窗格中，选择**配置 > 许可**。
2. 在中间窗格中选择许可管理员选项卡，然后选择管理员组。
3. 在“操作”窗格中，选择**编辑许可管理员组**或**删除许可管理员组**。

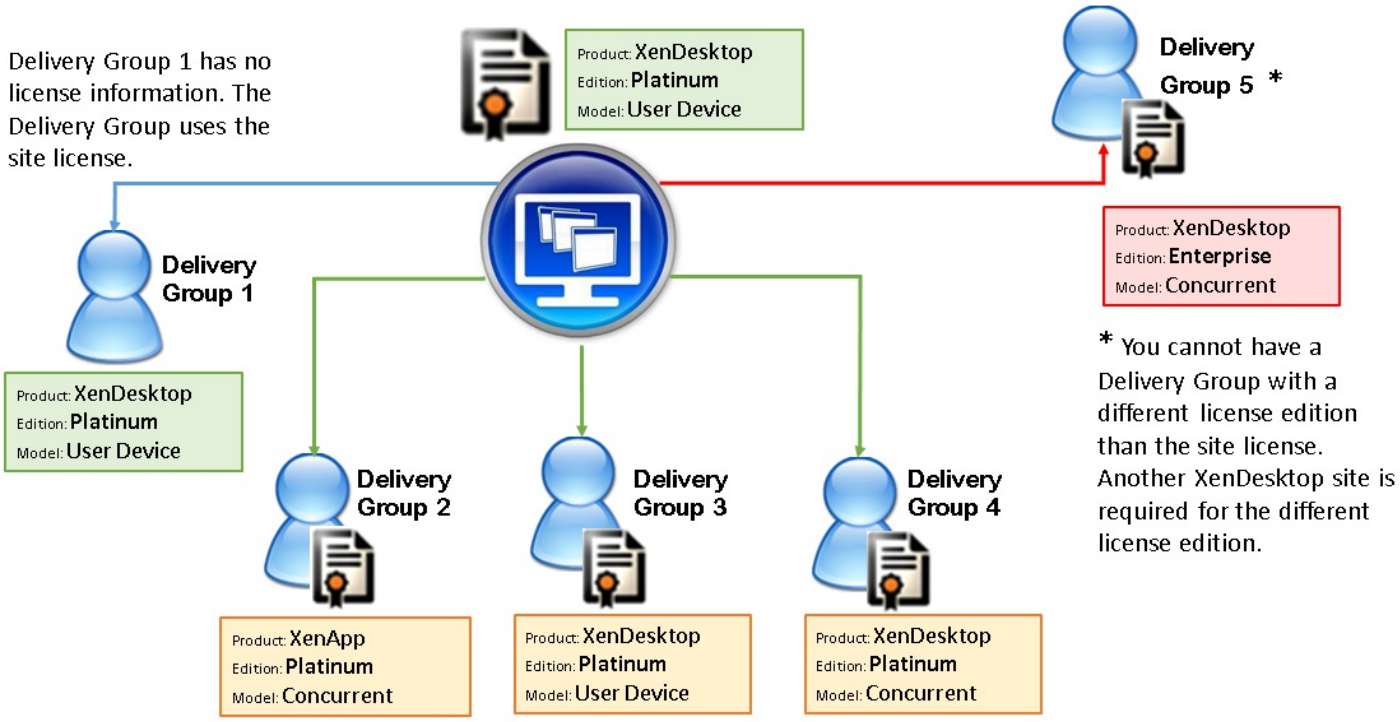
© 1999-2017 Citrix Systems, Inc. All rights reserved.

多类型许可

Dec 05, 2017

多类型许可支持在单个 XenApp 或 XenDesktop 站点上为交付组使用不同的许可证类型。**类型**是产品 ID（XDT、MPS）和模式（UserDevice、Concurrent）的单一组合。交付组必须使用为站点设置的产品版本。

如果未配置多类型许可，则仅当在各独立站点上全部配置时才能使用不同的许可证类型。交付组使用站点许可证。



要确定使用不同许可证类型的交付组，请使用以下 Broker PowerShell cmdlet：

- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

要安装许可证，请使用：

- Citrix Studio
- Citrix Licensing Manager
- 许可证管理控制台
- citrix.com

专享升级服务日期与每个许可证文件以及与每个产品和模式有关。以不同方式设置的交付组的专享升级服务日期可能会不同。

Broker PowerShell SDK

DesktopGroup 对象具有以下两个属性，您可以使用关联的 New-BrokerDesktopGroup 和 Set-BrokerDesktopGroup cmdlet

© 1999-2017 Citrix Systems, Inc. All rights reserved.

进行控制。

Name	Value	Restriction
LicenseModel	指定组的许可模式的枚举（Concurrent或 UserDevice）。	如果禁用功能切换，尝试设置属性将失败。
ProductCode	指定组的许可产品 ID 的文本字符串 XDT （表示 XenDesktop）或 MPS（表示 XenApp）。	如果禁用功能切换，尝试设置属性将失败。

New-BrokerDesktopGroup

创建桌面组以便对多组桌面的代理进行管理。有关此 cmdlet 的详细信息，请参阅 https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/。

Set-BrokerDesktopGroup

禁用或启用现有 Broker 桌面组或更改其设置。有关此 cmdlet 的详细信息，请参阅 https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/

Get-BrokerDesktopGroup

检索匹配指定条件的桌面组。Get-BrokerDesktopGroup cmdlet 的输出包括组的 ProductCode 和 LicenseModel 属性。如果未使用 New-BrokerDesktopGroup 或 Set-BrokerDesktopGroup 设置这些属性，则返回空值。如果为空，则使用站点范围的许可模式和产品代码。有关此 cmdlet 的详细信息，请参阅 https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/。

示例

此 PowerShell cmdlet 示例说明如何为两个现有交付组设置多类型许可，然后创建并设置第三个交付组。

要查看与交付组关联的许可产品和许可模式，请使用 **Get-BrokerDesktopGroup** PowerShell cmdlet。

1. 为第一个交付组设置 XenApp 和 Concurrent。
   Set-BrokerDesktopGroup -Name "Delivery Group for XenApp Platinum Concurrent" -ProductCode MPS -LicenseModel Concurrent
2. 为第二个交付组设置 XenDesktop 和 Concurrent。
   Set-BrokerDesktopGroup -Name "Delivery Group for XenDesktop Platinum Concurrent" -ProductCode XDT -LicenseModel Concurrent
3. 创建第三个交付组并为其设置 XenDesktop 和 UserDevice。
   New-BrokerDesktopGroup -Name "Delivery Group for XenDesktop Platinum UserDevice" -PublishedName "MyDesktop" -DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

特殊注意事项

多类型许可与常规 XenApp 和 XenDesktop 许可的功能不同。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

没有来自 Director 和 Studio 的警告和通知：

- 临近许可限制时没有任何信息，不会触发补充宽限期，也不存在补充宽限期到期。
- 特定组出现问题时不显示任何通知。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

应用程序

Dec 05, 2017

简介

如果您的部署仅使用交付组（而不使用应用程序组），则将应用程序添加到交付组。如果您也具有应用程序组，则通常应将应用程序添加到应用程序组。本指南可提供更轻松的管理过程。应用程序必须始终至少属于一个交付组或应用程序组。

在“添加应用程序”向导中，您可以选择一个或多个交付组或应用程序组，但不能同时选择两者。虽然您可在之后更改应用程序的组关联（例如，将应用程序从应用程序组移动到交付组），但是建议不要增加此复杂性。应使应用程序保持在一个类型的组中。

如果要将一个应用程序关联到多个交付组或应用程序组，但您没有足够权限来查看所有这些组中的应用程序，则会产生可见性问题。在这种情况下，可以咨询权限更高的管理员，或者扩展您的作用域，以包括要与应用程序关联的所有组。

如果向同一用户发布同名的两个应用程序（可能来自不同的组），请在 Studio 中更改“应用程序名称(面向用户)”属性；否则，用户将在 Citrix Receiver 中看到重复的名称。

您可以在添加时更改应用程序的属性（设置），或者在以后更改。还可以在添加应用程序使或在此之后更改用于放置应用程序的应用程序文件夹。

有关信息：

- 交付组，请参阅创建交付组一文。
- 应用程序组，请参阅创建应用程序组一文。
- 标记，可以将其添加到应用程序；请参阅标记一文。

添加应用程序

可以在创建交付组或应用程序组时添加应用程序；这些过程在文章“创建交付组”和“创建应用程序组”中进行了详细介绍。以下过程描述如何在您创建组之后添加应用程序。

须知事项：

- 无法向 Remote PC Access 交付组中添加应用程序。
- 不能使用“添加应用程序”向导从交付组或应用程序组中删除应用程序。必须单独执行该操作。

要添加一个或多个应用程序，请执行以下操作：

1. 在 Studio 导航窗格中选择**应用程序**，然后在“操作”窗格中选择**添加应用程序**。
2. 此时将启动“添加应用程序”向导，并打开一个**简介**页面，您可以在将来启动此向导时不再显示该页面。
3. 该向导将引导您访问“组”、“应用程序”和“摘要”页面，如下所述。完成每个页面之后，请单击**下一步**，直到显示“摘要”页面为止。

用于替代步骤 1 的方法（如果要将应用程序添加到单个交付组或应用程序组）：

- 要将应用程序只添加到一个交付组，请在步骤 1 中于 Studio 导航窗格中选择**交付组**，在中间窗格中选择一个交付组，然后

© 1999-2017 Citrix Systems, Inc. All rights reserved.

在“操作”窗格中选择**添加应用程序**。该向导将不会显示**组**页面。

- 要只将应用程序添加到一个应用程序组，请在步骤 1 中于 Studio 导航窗格中选择**应用程序**，在中间窗格中选择一个**应用程序组**，然后在“操作”窗格中应用程序组的名称下选择**添加应用程序**条目。该向导将不会显示**组**页面。

组

此页面列出了站点中的所有交付组。如果您还创建了应用程序组，则该页面将列出应用程序组和交付组。您可以从其中任何一个组进行选择，但不能同时从这两个组中选择。即，不能同时将应用程序添加到应用程序组和交付组。总体而言，如果您使用的是应用程序组，则应将应用程序添加到应用程序组而非交付组。

在添加应用程序时，必须选中至少一个交付组或应用程序组（如果有）旁的复选框，因为每个应用程序必须始终至少与一个组关联

应用程序

单击**添加**下拉菜单以显示应用程序源。

源	**说明**
从“开始”菜单	在计算机上发现的位于选定交付组中的应用程序。当您选择该源时，会打开一个新页面，其中包含已发现的应用程序的列表。选中要添加的应用程序的复选框，然后单击**确定**。 在下列情况下不能选择此源：(1) 您选择的应用程序组不与交付组关联，(2) 选择的应用程序组与不包含任何计算机的交付组关联，或者 (3) 选择的交付组不包含任何计算机。
手动定义	位于站点上或网络中的其他位置的应用程序。如果选择此源，则会启动一个新页面，您可以在其中键入可执行文件路径、工作目录、可选命令行参数以及显示给管理员和用户的名称。输入此信息后，请单击**确定**。
现有	以前添加到站点的应用程序。当您选择该源时，会打开一个新页面，其中包含已发现的应用程序的列表。选中要添加的应用程序的复选框，然后单击**确定**。 如果站点没有任何应用程序，则无法选择此源。
App-V	App-V 软件包中的应用程序。如果选择此源，则会启动一个新页面，您可以在其中选择 App-V 服务器或应用程序库。从生成的显示内容中，选中要添加的应用程序的复选框，然后单击**确定**。有关详细信息，请参阅 App-V 一文。 如果没有为站点配置 App-V 则无法选择此源。
应用程序组	应用程序组。当您选择该源时，会打开一个新页面，其中包含应用程序组的列表。（虽然显示内容也会列出各个组中的应用程序，但是您只能选择组，而不能选择单个应用程序。）将添加选定组中的所有当前和将来的应用程序。选中要添加的应用程序组的复选框，然后单击**确定**。 在下列情况中不能选择此源：(1) 没有应用程序组，或 (2) 所选交付组不支持应用程序组（例如，含静态分配的计算机的交付组）。

如果不存在该类型的有效源，则“添加”下拉列表中的一些源无法选择（如表中所示）。下拉列表中不包括不兼容的源（例如，您不能将应用程序组添加到应用程序组）。无法选择已添加到您所选择的应用程序组的应用程序。

要从分配的 AppDisk 添加应用程序，请选择**从“开始”菜单**。如果那里没有应用程序，请选择**手动定义**并提供详细信息。如果发生文件夹访问错误，请将文件夹配置为“共享”文件夹，并重新尝试通过**手动定义**添加应用程序。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

可以在此页面中更改应用程序的属性（设置），或在以后进行此更改。

默认情况下，您添加的应用程序位于名为 Applications 文件夹中。可从该页面中更改应用程序，或在以后执行此更改。如果您尝试添加某个应用程序，但同一文件夹中已存在同名应用程序，系统将提示您重命名要添加的应用程序。您可以接受系统提供的新名称，也可以拒绝，然后重命名应用程序或选择不同的文件夹。例如，如果 Applications 文件夹中已经存在“app”，而您尝试将另一个名为“app”的应用程序添加到该文件夹，则将提供新名称“app_1”。

总结

如果要添加 10 个或更少的应用程序，则它们的名称会列在**要添加的应用程序**中。如果要添加超过 10 个的应用程序，应指定总数。

查看摘要信息，然后单击**完成**。

更改应用程序的组关联

添加应用程序后，可以更改与应用程序关联的交付组和应用程序组。

可以使用拖放操作将应用程序与其他组相关联。可使用此操作代替在“操作”窗格中使用命令的操作。

如果应用程序与多个交付组或应用程序组相关联，则可使用组优先级指定对多个组进行检查以发现应用程序的顺序。默认情况下，所有组都具有优先级 0（最高优先级）。将对具有相同优先级的组进行负载平衡。

可将应用程序与交付组（其中包含共享（非专用）的可提供应用程序的计算机）。还可以选择包含仅用于交付桌面的共享计算机的交付组，前提如下：(1) 交付组包含共享计算机，并且是通过早期的 XenDesktop 7.x 版本创建的，(2) 您具有“编辑交付组”权限。在提交属性对话框时，“交付组”类型将自动转换为“桌面和应用程序”。

1. 在 Studio 导航窗格中选择**应用程序**，然后在中间窗格中选择应用程序。
2. 在“操作”窗格中选择**属性**。
3. 选择**组**页面。
4. 要添加组，请单击**添加**下拉列表，并选择**应用程序组**或**交付组**。（如果尚未创建任何应用程序组，则唯一条目是“交付组”。）然后选择一个或多个可用的组。无法选择不兼容的，或已与应用程序关联的应用程序。
5. 要删除组，请选择一个或多个组，然后单击**删除**。如果删除组关联，将导致应用程序不再与任何应用程序组或交付组关联。系统会提醒您，指出该应用程序将被删除。
6. 要更改某个组的优先级，请选择该组，然后单击**编辑优先级**。选择一个优先级值，然后单击**确定**。
7. 完成操作后，单击**应用**以应用您执行的更改并保持打开窗口，或单击**确定**应用更改并关闭窗口。

复制、启用/禁用、重命名或删除应用程序

使用下列这些操作：

- **复制**：您可能希望复制应用程序以创建具有不同参数或属性的不同版本。复制应用程序时，应用程序会通过唯一的后缀自动重命名并放置在与原始应用程序相邻的位置。您可能还需要复制应用程序并将其添加到不同的组。（复制后，可通过最简单的拖放方法来移动它。）
- **启用或禁用**：启用和禁用应用程序的过程与启用和禁用交付组或应用程序组的过程不同。
- **重命名**：一次只能重新命名一个应用程序。如果您尝试重命名某个应用程序，但同一文件夹或组中已存在同名应用程序，系统将提示您指定一个不同的名称。
- **删除**：如果删除应用程序，会将其从关联的交付组和应用程序组中删除，但不会从最初用于添加此应用程序的源中删除。删

© 1999-2017 Citrix Systems, Inc. All rights reserved.

除应用程序的过程与从交付组或应用程序组中删除应用程序的过程不同。

复制、启用/禁用、重命名或删除应用程序：

1. 在 Studio 导航窗格中选择**应用程序**。
2. 在中间窗格中选择一个或多个应用程序，然后在“操作”窗格中选择相应的任务。
3. 在系统提示时，确认所做操作。

从交付组中删除应用程序

应用程序必须至少关联（或属于）一个交付组或应用程序组。如果您尝试从交付组删除某个应用程序，将删除该应用程序与任何交付组或应用程序组的关联。如果继续操作，您会收到通知，指出应用程序将被删除。当发生这种情况时，如果要交付应用程序，则必须再次从有效源添加中应用程序。

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择交付组。在中下部分的窗格中，选择**应用程序**选项卡，然后选择要删除的应用程序。
3. 在“操作”窗格中选择**删除应用程序**。
4. 确认删除。

从应用程序组中删除应用程序

应用程序必须至少属于一个交付组或应用程序组。如果您尝试从应用程序组删除某个应用程序，将导致该应用程序不再属于任何交付组或应用程序组。如果继续操作，您会收到通知，指出应用程序将被删除。当发生这种情况时，如果要交付应用程序，则必须再次从有效源添加中应用程序。

1. 在 Studio 导航窗格中选择**应用程序**。
2. 在中间窗格中选择应用程序组，然后在中间窗格中选择一个或多个应用程序。
3. 在“操作”窗格中选择**从应用程序组中删除**。
4. 确认删除。

更改应用程序属性

一次只能更改一个应用程序的属性。

要更改应用程序的属性，请执行以下操作：

1. 在 Studio 导航窗格中选择**应用程序**。
2. 选择一个应用程序，然后在“操作”窗格中选择**编辑应用程序属性**。
3. 选择包含要更改的属性的页面。
4. 完成操作后，单击**应用**以应用您所做的任何更改并保持打开窗口，或单击**确定**应用更改并关闭窗口。

属性	**选择此页面**
在 Receiver 中用于显示应用程序的类别/文件夹	交付

© 1999-2017 Citrix Systems, Inc. All rights reserved.

命令行参数（请参阅“将参数传递给已发布应用程序”部分）	位置
其中包含可用应用程序的交付组和应用程序组	组
说明	标识
文件扩展名和文件类型关联：将由应用程序自动打开的扩展名	文件类型关联
图标	交付
StoreFront 的关键字	标识
限制（请参阅“配置应用程序限制”部分）	交付
名称：向用户和管理员显示的名称	标识
可执行文件夹路径（请参阅“将参数传递给已发布应用程序”部分）	位置
用户桌面上的快捷方式：启用或禁用	交付
可见性：限制可查看 Citrix Receiver 中的应用程序的用户（可见的应用程序仍可启动；要使其不可用并不可见，请将其添加到不同的组）	限制可见性
工作目录	位置

在当前的应用程序用户注销其会话之前，应用程序更改可能不对其生效。

配置应用程序限制

配置应用程序限制可帮助管理应用程序的使用。例如，可以使用应用程序限制来管理同时访问某个应用程序的用户数量。同样，也可以使用应用程序限制来管理资源密集型应用程序的同时运行的实例数，这样有助于维护服务器性能，阻止服务性能下降。

重要：此功能限制 Controller 代理的应用程序启动的数量（例如，从 Citrix Receiver 和 StoreFront 中），不限制可以通过其他方法启动的正在运行的应用程序数量。这意味着应用程序限制可以在管理并发使用时向管理员提供帮助，但并不强制在所有情况下使用。例如，Controller 处于租用连接模式时，不能应用应用程序限制。

默认情况下，不限制可以同时运行的应用程序实例数。有两个应用程序限制设置；可以配置其中一个或两个设置：

- 交付组中的所有用户运行的并发应用程序实例数上限。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 交付组中的每个用户运行应用程序的一个实例

如果配置了某个限制，则当用户尝试启动会超出该配置限制的应用程序的实例时，将生成一条错误消息。

使用应用程序限制的示例：

- **同时运行的实例数上限。**在交付组中，可以将应用程序 Alpha 同时运行的实例数上限配置为 15。以后，该交付组中的用户可以同时运行该应用程序的 15 个实例。如果该交付组中的任何用户现在尝试启动 Alpha，则会生成一条错误消息，并且 Alpha 不启动，因为这将超出所配置的同时运行的应用程序实例数限制 (15)。
- **“每个用户运行一个实例”应用程序限制**在另一个交付组中，您为应用程序 Beta 启用了每个用户运行一个实例选项。用户 Tony 成功启动了应用程序 Beta。当天晚些时候，当该应用程序仍在 Tony 的会话中运行时，他尝试启动 Beta 的另一个实例。此时将生成一条错误消息，并且 Beta 不启动，因为这将超出一个用户运行一个实例的限制。
- **同时运行的实例数上限和限制一个用户运行一个实例。**在另一个交付组中，可以将应用程序 Delta 同时运行的实例数上限配置为 10，并启用一个用户运行一个实例选项。以后，当该交付组中的十个用户每人运行一个 Delta 实例时，该交付组中尝试启动 Delta 的任何其他用户都会收到一条错误消息，并且 Delta 不启动。如果当前十个 Delta 用户中的任何一个用户尝试启动该应用程序的第二个实例，也会收到一条错误消息，并且第二个实例不启动。

如果应用程序实例还通过除 Controller 代理以外的其他方法启动（例如，当 Controller 处于租用连接模式时），并且超出了配置的限制，用户将无法启动额外的实例，直至其关闭足够的实例以便不再超出限制为止。超出限制的实例不会被强制关闭，但不允许其继续运行，直至用户将其关闭。

如果禁用了会话漫游，请禁用每个用户运行一个应用程序实例限制。如果启用了每个用户运行一个应用程序实例限制，请勿配置允许新会话在新设备上运行的两个值中的任一值。有关漫游的信息，请参阅会话一文。

配置应用程序限制：

1. 在 Studio 导航窗格中选择**应用程序**，然后选择一个应用程序。
2. 在“操作”窗格中选择**编辑应用程序属性**。
3. 在**交付**页面上，选择下面列出的其中一个选项。完成操作后，单击**确定**或**应用**。（单击**确定**将应用所做更改并关闭“编辑应用程序属性”对话框；单击**应用**将应用所做更改，但不关闭该对话框。）

- 允许无限制使用应用程序。不限制同时运行的实例数。这是默认值。
- 为应用程序设置限制。有两种限制类型，请指定其中的一种或两种类型。
  - 指定可以并发运行的实例数上限
  - 限制每个用户运行一个应用程序实例

将参数传递给已发布应用程序

使用某个应用程序属性的“位置”页面输入命令行，并将参数传递给已发布应用程序。

将已发布应用程序与文件类型相关联时，符号 "%*" （双引号中含百分号和星号）会附加在应用程序命令行的末尾。这些符号充当传递给用户设备的参数的占位符。

如果已发布应用程序在应该启动时没有启动，请确认其命令行包含的符号是否正确。默认情况下，在附加符号“%*”时会验证用户设备提供的参数。对于使用用户设备提供的自定义参数的已发布应用程序，"%**" 符号会附加到命令行末尾来禁用命令行验证。如果您在应用程序的命令行中看不到这些符号，请手动进行添加。

如果可执行文件的路径包含带空格的目录名称（例如 "C:\Program Files"），请使用双引号引起应用程序的命令行，以指示空格属于该命令行。要执行此操作，请使用双引号引起该路径，并使用另一个双引号引起 %* 符号。应确保在路径的右引号与 %*

© 1999-2017 Citrix Systems, Inc. All rights reserved.

符号的左引号之间留有一个空格。

例如：已发布应用程序 Windows Media Player 的命令行为：

"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"

管理应用程序文件夹

默认情况下，添加到交付组中的新应用程序将放置在名为**应用程序**的文件夹中。您可以在创建交付组时、添加应用程序时或以后指定其他文件夹。

须知事项：

- 您无法重命名或删除 Applications 文件夹，但可以将其包含的所有应用程序移动到您创建的其他文件夹。
- 文件夹名称可以包含 1-64 个字符。允许使用空格。
- 文件夹最多可以嵌套五个级别。
- 文件夹并非必须包含应用程序；它们可以为空。
- 除非您在创建文件夹时对其进行移动或指定了其他位置，否则在 Studio 中文件夹按字母顺序列出。
- 您可以具有多个名称相同的文件夹，只要其父文件夹不同即可。同样，您可以具有多个名称相同的应用程序，只要其位于不同的文件夹中即可。
- 您必须具有查看应用程序权限才能查看文件夹中的应用程序；必须对文件夹中的所有应用程序都具有编辑应用程序属性权限，才能删除、重命名或删除包含应用程序的文件夹。
- 以下大部分过程都要求使用 Studio 中的“操作”窗格进行操作。也可以在菜单上单击鼠标右键或拖放。例如，如果您在不理想的位置创建或移动了文件夹，则可以将其拖动/放置到正确的位置。

要管理应用程序文件夹，请选择 Studio 导航窗格中的**应用程序**。请按下列指导进行操作。

- 要查看所有文件夹（不包括嵌套文件夹），请单击文件夹列表上方的**全部显示**。
- 要在最高级别创建文件夹（不嵌套），请选择“应用程序”文件夹。要将新文件夹置于 Applications 之外的其他现有文件夹下，请选择该文件夹。然后，在“操作”窗格中选择**创建文件夹**。请输入名称。
- 要移动某个文件夹，请选择该文件夹，然后在“操作”窗格中选择**移动文件夹**。一次只能移动一个文件夹，除非文件夹包含嵌套文件夹。提示：最简便的移动文件夹的方法是使用拖放操作。
- 要重命名某个文件夹，请选择该文件夹，然后在“操作”窗格中选择**重命名文件夹**。请输入名称。
- 要删除某个文件夹，请选择该文件夹，然后在“操作”窗格中选择**删除文件夹**。删除包含应用程序和其他文件夹的某个文件夹时，这些对象也随之删除。通过删除应用程序，可将分配的应用程序从交付组删除，但不会将其从计算机中删除。
- 要将应用程序移至某个文件夹，请选择一个或多个应用程序。然后，在“操作”窗格中选择**移动应用程序**。选择文件夹。

您也可以在“创建交付组”和“创建应用程序组”向导中的**应用程序**页面上，将要添加的应用程序放置于一个特定文件夹（即使是新文件夹也可）。默认情况下，所添加的应用程序将进入 Applications 文件夹；单击**更改**可选择或创建一个文件夹。）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

通用 Windows 平台应用程序

Dec 05, 2017

XenApp 和 XenDesktop 支持在 Windows 10 和 Windows Server 2016 计算机上结合使用通用 Windows 平台 (UWP) 应用程序和 VDA。有关 UWP 应用程序的信息，请参阅以下 Microsoft 文档：

- 什么是通用 Windows 平台 (UWP) 应用程序？
- 离线分发应用程序
- 通用 Windows 平台 (UWP) 应用程序指南

术语“通用应用程序”在本文中泛指 UWP 应用程序。

要求和限制

Windows 10 和 Windows Server 2016 上的 VDA 支持通用应用程序。

这些 VDA 的版本至少应为 7.11。

以下 XenApp 和 XenDesktop 功能在使用通用应用程序时不受支持或受到限制：

- 不支持文件类型关联。
- 不支持本地应用程序访问。
- 动态预览：如果会话中运行的应用程序重叠，该预览会显示默认图标。动态预览所使用的 Win32 API 不受通用应用程序支持。
- 操作中心远程处理：通用应用程序可以使用操作中心来显示会话中的消息。将这些消息重定向至端点以向用户显示。

Windows 10 VDA 不支持从同一个服务器启动通用应用程序和非通用应用程序。对于 Windows Server 2016，通用应用程序和非通用应用程序应位于单独的交付组和应用程序组。

已列举出了所有安装在计算机上的通用应用程序；因此，Citrix 建议禁止用户访问 Windows 应用商店。这防止一个用户安装的通用应用程序被另一个用户访问。

在旁加载过程中，通用应用程序将安装在计算机上，且可供其他用户使用。任何其他用户启动该应用程序时，应用程序已经安装。操作系统然后会更新其 AppX 数据库以向启动该应用程序的用户指示“已安装”。

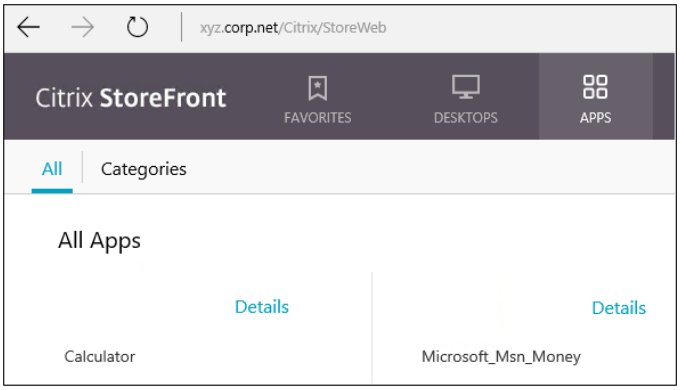
如果从一个在无缝或固定窗口中启动的已发布通用应用程序中正常注销，则该会话不会关闭，而用户则被注销。在这种情况下，该会话中存在的多个进程会阻止该会话正常关闭。要解决此问题，请确定哪个进程在阻止会话关闭，然后将其添加到“LogoffCheckSysModules”注册表键值中，并遵循 CTX891671 中的指南。

通用应用程序的应用程序显示名称和描述可能不具有正确的名称。在将这些应用程序添加到交付组时编辑并更正这些属性。

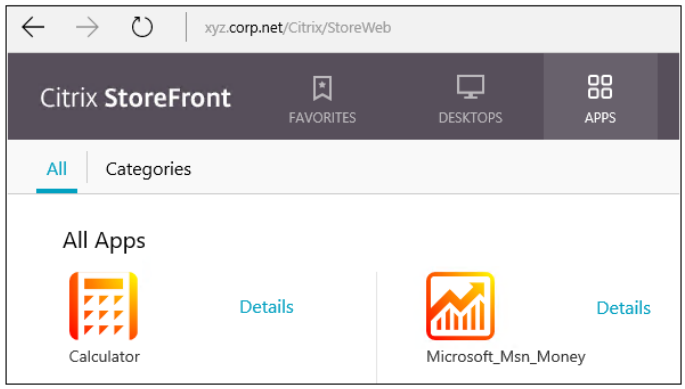
检查已知问题一文了解任何其他问题。

当前，多个通用应用程序具有已启用透明度的白色图标，这导致在 StoreFront 显示屏的白色背景下看不见图标。要避免此问题，您可以更改背景。例如，在 StoreFront 计算机上，编辑 C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css 文件。在文件的末端，添加 **.storeapp-icon {background-image: radial-gradient(circle at top right, yellow, red); }**。以下图形阐释了该示例前后变化的情况。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Before



After

在 Windows Server 2016 上，服务器管理器也可能会在启动某个通用应用程序时启动。要防止此问题发生，请使用 HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon 注册表键禁止服务器管理器在登录过程中自动启动。有关详细信息，请参阅 https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/。

安装和发布通用应用程序

默认情况下已启用对通用应用程序的支持。

要禁止在 VDA 上使用通用应用程序，请在 HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle 中添加注册表设置 **EnableUWASeamlessSupport** 并将其设为 **0**。

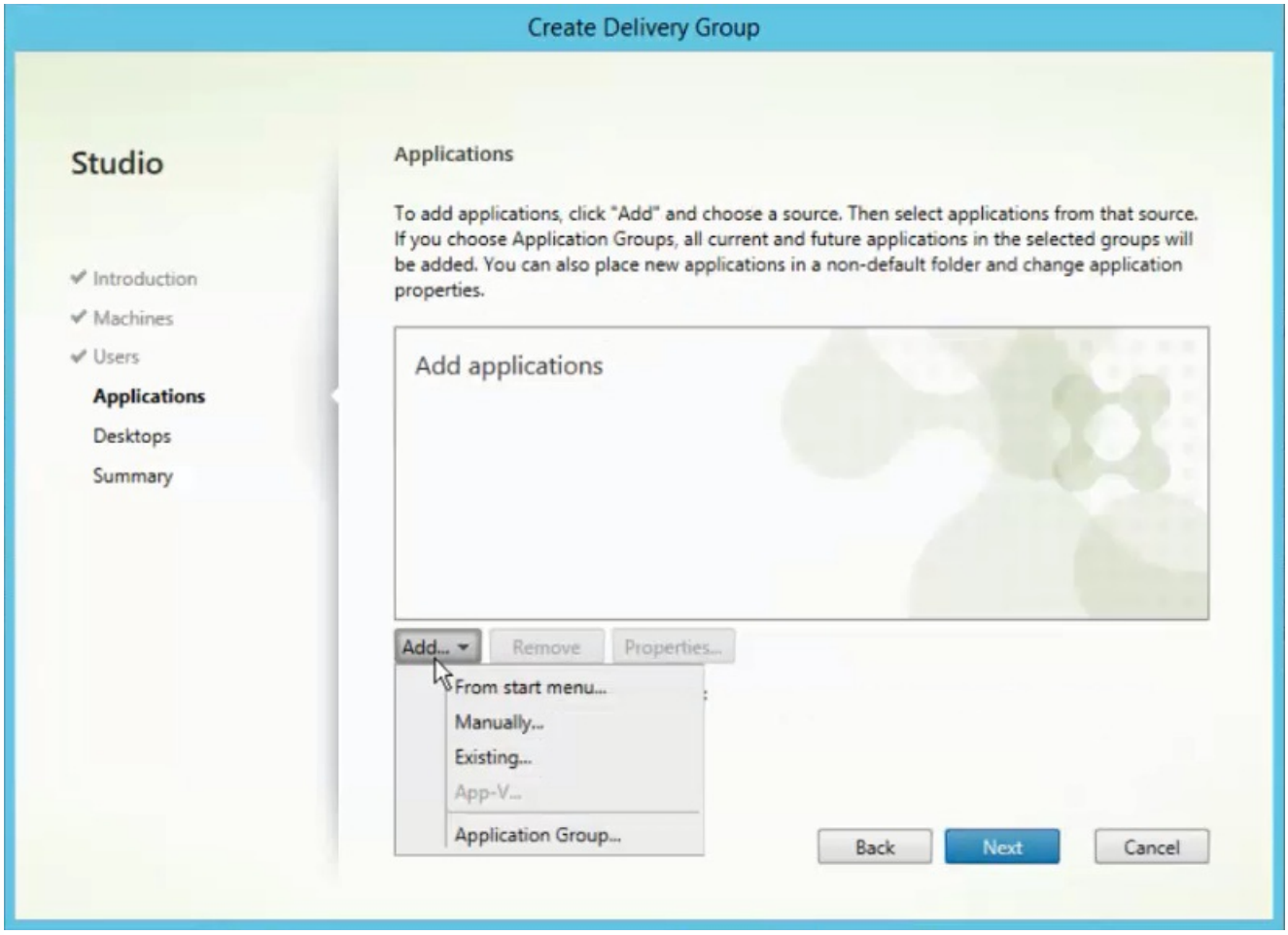
要在 VDA 上安装一个或多个通用应用程序（或一个主映像），请使用以下一种方法：

- 通过 Windows Store for Business 完成离线安装，使用诸如 Deployment Image Servicing and Management (DISM) 等工具将应用程序部署至桌面映像。有关详细信息，请参阅 https://technet.microsoft.com/zh-cn/itpro/windows/manage/distribute-offline-apps。
- 旁加载应用程序。有关详细信息，请参阅 https://technet.microsoft.com/zh-cn/itpro/windows/deploy/sideload-apps-in-windows-10。

要在 XenApp 或 XenDesktop 中添加（发布）一个或多个通用应用程序，请执行以下操作：

> 在计算机上安装了通用应用程序之后，将通用应用程序添加到交付组或应用程序组。您可以在创建一个组时执行此操作，或稍后执行。在向导的应用程序页面上，选择**从“开始”菜单**源。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



显示应用程序列表时，选择您想要发布的通用应用程序的复选框。然后，单击**下一步**。

卸载通用应用程序

使用诸如 Remove-AppXPackage 等命令卸载通用应用程序时，仅可由管理员卸载该项目。要从已经启动和使用该应用程序的用户的计算机上删除应用程序，您必须在每台计算机上运行删除命令。无法通过一条命令从所有用户的计算机上卸载 AppX 软件包。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

区域

Dec 12, 2017

如果部署横跨分布广泛且通过 WAN 进行连接的位置，则会面临网络延迟和可靠性带来的挑战。可以通过两种方案来缓解这些挑战：

- 部署多个站点，每个站点都有自己的 SQL Server 站点数据库。

  建议对大型企业部署使用此方案。分别管理多个站点，每个站点需要有各自的 SQL Server 站点数据库。每个站点是一个独立的 XenApp 部署。

- 在单个站点内配置多个区域。

  配置区域可帮助远程地理区域的用户连接到资源，而不需要强制其连接遍历大部分 WAN。使用区域可实现从单个 Citrix Studio 控制台、Citrix Director 和站点数据库有效地管理站点。这样可以节约部署、配备人员、许可和操作包含远程位置中的多个数据库的额外站点的成本。

  区域在各种大小的部署中会非常有用。可以使用区域来保持应用程序和桌面对最终用户触手可用，从而提高性能。一个区域可以包含一个或多个安装在本地的 Controller 以实现冗余和复原，但并非必须安装一个或多个 Controller。

  站点中配置的 Controller 数会影响某些操作（例如，向站点自身添加新 Controller）的性能。为了避免此问题，建议将您的 XenApp 或 XenDesktop 站点中的区域数限制在 50 以内。

  注意：区域的网络延迟超过 250 ms RTT 时，建议部署多个站点而不是区域。

在本文中，术语“本地”是指正在讨论的区域。例如，“VDA 注册到本地 Controller 中”是指 VDA 注册到 VDA 所在的区域中的 Controller。

本版本中的区域非常相似，但与 XenApp 6.5 及更早版本中的区域不同。例如，在此区域的实现中，不包含数据收集器。站点中的所有 Controller 都与主要区域中的一个站点数据库进行通信。此外，在本版本中，故障转移和首选区域的工作方式不同。

区域类型

一个站点始终有一个主要区域。一个站点也可以有一个或多个卫星区域。可以为灾难恢复、地理位置相隔很远的数据中心、分支机构、云或云中的可用性区域使用卫星区域。

主要区域

主要区域的默认名称为“主要”，该区域中包含 SQL Server 站点数据库（和高可用性 SQL Server，如果使用）、Studio、Director、Citrix StoreFront、Citrix 许可证服务器和 NetScaler Gateway。站点数据库应始终位于主要区域中。

主要区域还应至少包含两个 Controller 以实现冗余，并且可能包含一个或多个安装了与数据库和基础结构紧密配对的应用程序的 VDA。

卫星区域

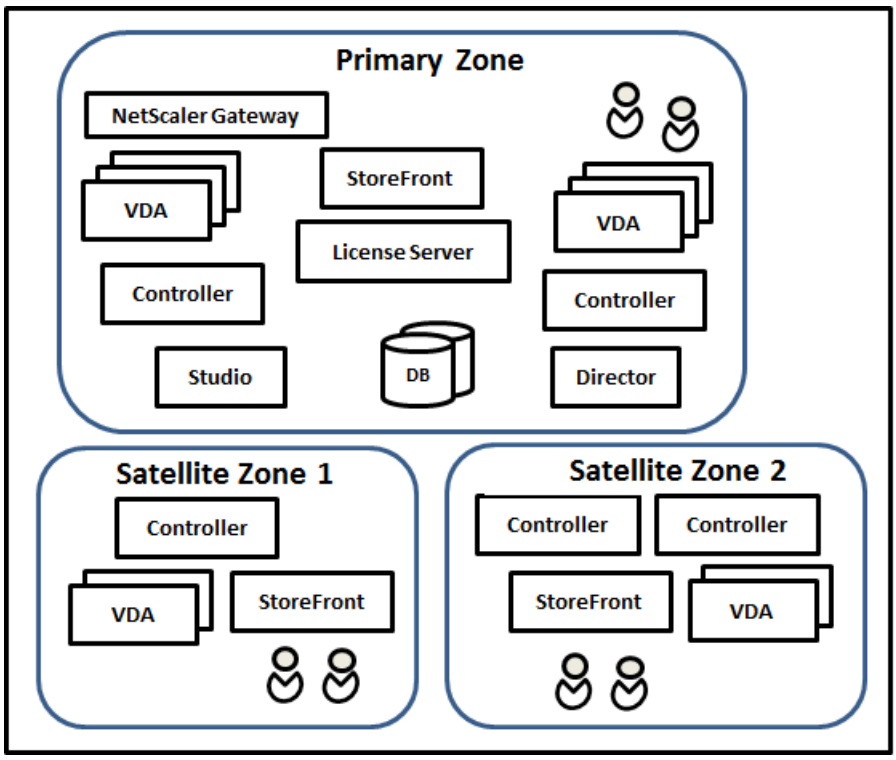
一个卫星区域包含一个或多个 VDA、Controller、StoreFront 服务器和 NetScaler Gateway 服务器。在正常情况下，卫星区域中的 Controller 直接与主要区域中的数据库进行通信。

卫星区域（特别是大型卫星区域）可能还包含虚拟机管理程序，用于置备和/或存储该区域的计算机。配置卫星区域时，

© 1999-2017 Citrix Systems, Inc. All rights reserved.

可以将虚拟机管理程序或云服务连接与其关联。（请确保使用该连接的所有计算机目录都位于相同的区域。）

站点可以包含不同配置的卫星区域，具体取决于您的独特需求和环境。下图显示了一个主要区域以及卫星区域的示例。



- 主要区域包含两个 Controller、Studio、Director、StoreFront、许可证服务器和站点数据库（以及高可用性 SQL Server 部署）。主要区域还包含多个 VDA 和一个 NetScaler Gateway。
- 卫星区域 1 - 包含 Controller 的 VDA

  卫星区域 1 包含一个 Controller、多个 VDA 和一个 StoreFront 服务器。此卫星区域中的 VDA 注册到本地 Controller 中。本地 Controller 与主要站点中的站点数据库和许可证服务器进行通信。

  如果 WAN 出现故障，连接租用功能将允许该卫星区域中的 Controller 继续代理与该区域中的 VDA 的连接。如果办公室里的工作人员使用本地 StoreFront 站点和本地 Controller 访问其本地资源，则此类部署会非常有效，即使将其办公室连接到企业网络的 WAN 链接出现故障也是如此。
- 卫星区域 2 - 包含冗余 Controller 的 VDA

  卫星区域 2 包含两个 Controller、多个 VDA 和一个 StoreFront 服务器。这是复原能力最强的区域类型，能够在 WAN 和其中一个本地 Controller 同时出现故障时提供保护。

VDA 注册的位置以及 Controller 故障转移的位置

在包含主要区域和卫星区域的站点中，VDA 的最低版本为 7.7：

- 主要区域中的 VDA 注册到主要区域中的 Controller。主要区域中的 VDA 永不尝试注册到卫星站点中的 Controller。
- 卫星区域中的 VDA 注册到本地 Controller 中（如有可能）。（这称为首选 Controller）。如果本地 Controller 都不可用（例如，由于本地 Controller 无法接受更多 VDA 注册，或者本地 Controller 出现故障），VDA 将尝试注册到主要区域中的

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Controller。在这种情况下，VDA 保持注册到主要区域中，即使卫星区域中的 Controller 再次可用也是如此。一个卫星区域中的 VDA 永不尝试注册到另一个卫星站点中的 Controller。

- 如果为 Controller 的 VDA 发现启用了自动更新，并且在 VDA 安装期间指定了一个 Controller 地址列表，则会从该列表中随机选择一个 Controller 以完成初始注册（无论 Controller 驻留在哪个区域）。重新启动包含该 VDA 的计算机后，该 VDA 将启动，以便首先选择注册到其本地区域中的 Controller。
- 如果卫星区域中的 Controller 出现故障，则会故障转移到另一个本地 Controller（如有可能）。如果所有本地 Controller 都不可用，则会故障转移到主要区域中的 Controller。
- 如果您将 Controller 移入或移出某个区域，并且启用了自动更新，则这两个区域中的 VDA 会收到更新后的列表，指出哪些属于本地 Controller，哪些位于主要区域中，这样可以确定其能够注册到哪个 Controller 以及接受来自哪个 Controller 的连接。
- 如果将某个计算机目录移动到另一个区域，该目录中的 VDA 将重新注册到移动了该目录的区域中的 Controller。（当您将某个目录移动到与当前区域的连接质量非常差的区域时，例如，通过高延迟或低带宽网络建立连接，请务必同时将任何关联的主机连接移动到相同的区域。）
- 主要区域中的 Controller 将保留所有区域的连接租用数据。卫星区域中的 Controller 保留各自的区域以及主要区域的连接租用数据，但不保留任何其他卫星区域的数据。

如果主要区域中的所有 Controller 都出现故障：

- Studio 无法连接到站点。
- 无法与主要区域中的 VDA 建立连接。
- 站点性能将大幅下降，直至主要区域中的 Controller 可用。

对于包含版本 7.7 之前的 VDA 的站点：

- 卫星区域中的 VDA 将接受来自其本地区域和主要区域中的 Controller 的请求。（最低版本为 7.7 的 VDA 可以接受来自其他卫星区域的 Controller 请求。）
- 卫星区域中的 VDA 将随机注册到主要区域或本地区域中的 Controller。（最低版本为 7.7 的 VDA 首先选择本地区域。）

区域偏好

重要：要使用区域偏好功能，您必须至少使用 StoreFront 3.7 和 NetScaler Gateway 11.0-65.x。

在多个区域的站点中，区域偏好功能为管理员提供更多的灵活性来控制哪些 VDA 可用于启动一款应用程序或桌面。

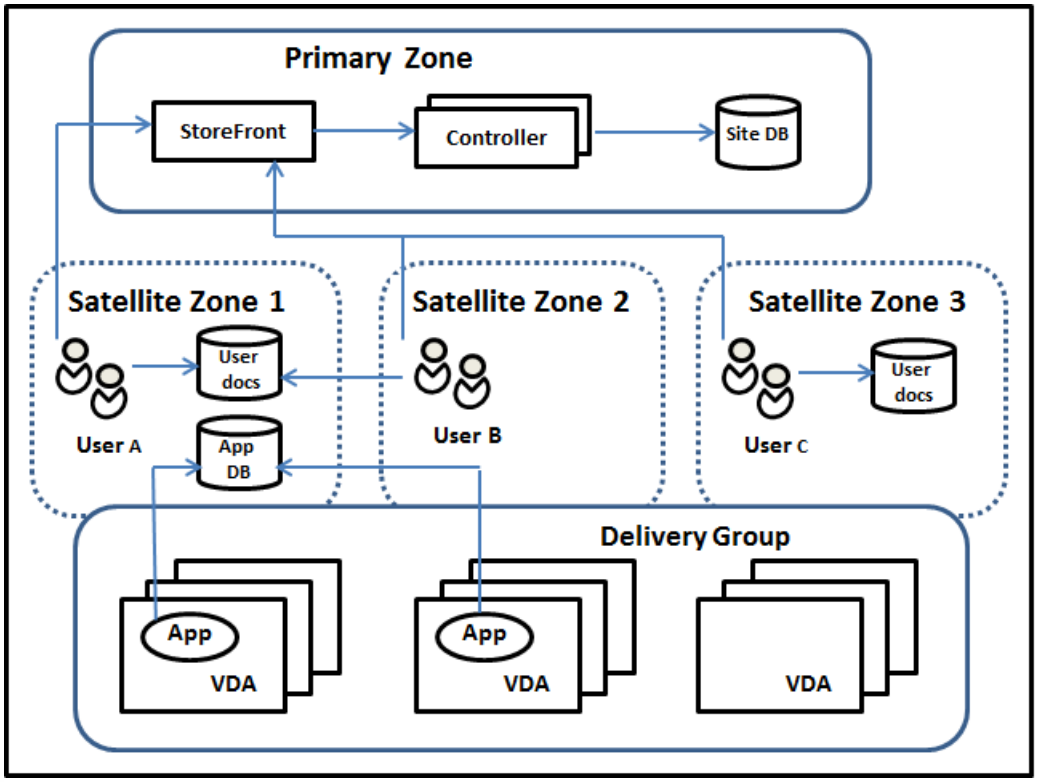
区域偏好的工作方式

有三种形式的区域偏好。您可能更喜欢使用特定区域中的 VDA，基于：

- 应用程序数据的存储位置。这称为应用程序的主区域。
- 用户的主区域数据的位置，例如配置文件或主区域共享。这称为用户的主区域。
- 用户的当前位置（Citrix Receiver 正在运行的位置）。这称为用户位置。

下图显示了多区域配置示例。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



在此示例中，VDA 分布在三个卫星区域中，但都处在同一个交付组中。因此，代理可以选择针对用户启动请求使用哪个 VDA。本示例指出用户可以在多个位置运行其 Citrix Receiver 端点：用户 A 正在卫星区域 1 中使用具有 Citrix Receiver 的设备；用户 B 正在卫星区域 2 中使用某个设备。用户的文档可以存储在多个位置：用户 A 和 B 使用卫星区域 1 中的共享；用户 C 使用卫星区域 C 中的共享。此外，其中一个已发布的应用程序使用位于卫星区域 1 中的数据库。

您可以通过为用户或应用程序配置一个主区域的方法将其与某个区域关联。然后，Delivery Controller 中的代理会使用这些关联来帮助选择将会在其中启动会话的区域（如果资源可用）。您：

- 通过向某个区域添加用户的方法来为用户配置主区域。
- 通过编辑应用程序属性来为某个应用程序配置主区域。

一名用户或一个应用程序一次只能有一个主区域。（在由于用户组成员关系而出现多个区域成员关系时，可能会出现用户的例外；请参阅“其他注意事项”部分。但是，即使在这种情况下，代理只能使用一个主区域。）

尽管可以配置用户和应用程序的区域偏好，代理一次启动只能选择一个首选的区域。选择首选区域的默认优先次序为应用程序主区域 > 用户主区域 > 用户位置。（如下一部分中所述，您可以限制顺序）当用户启动一个应用程序时：

- 如果该应用程序具有一个已配置的区域关联（一个应用程序主区域），那么首选的区域就是该应用程序的主区域。
- 如果该应用程序不具有配置的区域关联，但用户具有配置的区域关联（用户主区域），则首选的区域为该用户的主区域。
- 如果应用程序和用户都不具有配置的区域关联，则首选的区域为用户正运行 Citrix Receiver 实例的区域（用户位置）。如果该区域未定义，则使用随机的 VDA 和区域选择。负载平衡适用于首先区域中的所有 VDA。如果没有首选区域，负载平衡适用于交付组中所有 VDA。

定制区域偏好

配置（或删除）某个用户或应用程序的主区域时，也可以进一步限制如何使用（或不使用）区域偏好。

- **强制用户主区域使用：**在一个交付组中，可以指定应在用户的主区域（如果该用户具有一个主区域）中启动一个会话，且在

© 1999-2017 Citrix Systems, Inc. All rights reserved.

主区域中资源不可用的情况下不会故障转移至另一个区域。在您需要避免在多个区域间复制大型配置文件或数据文件而带来的风险时，这一限制会很有用。换而言之，您宁可拒绝一次会话启动，也不愿在不同的区域中启动会话。

- **强制应用程序主区域使用**：同样，配置某个应用程序的主区域时，可以指示仅应在该区域启动应用程序，且在应用程序的主区域中资源不可用时不会故障转移到另一个区域。
- **无应用程序主区域，且忽略配置的用户主区域**：如果不指定某个应用程序的主区域，还可以指示在启动该应用程序时不应该考虑任何配置的用户区域。例如，您可能希望用户在一个靠近他们使用的计算机（Citrix Receiver 正运行的位置）的 VDA 上运行一个特定应用程序，使用用户位置区域偏好，即使某些用户可能拥有不同的主区域。

首选区域如何影响会话使用

用户启动一个应用程序或桌面时，代理希望使用首选的区域，而不是使用现有的会话。

如果启用应用程序或桌面的用户已经具有一个适合被启动资源的会话（例如，可以使用某个应用程序的会话共享，或一个已经在运行被启动资源的会话），但该会话正在不同于该用户/应用程序首选区域的区域中的 VDA 上运行，那么系统可能会创建新的会话。这满足了在正确的区域中启动的需求（如果具有可用的容量），而无需重新连接到该用户会话要求的较不理想区域中的会话。

要防止出现无法访问的孤立会话，允许对现有的断开连接的会话进行重新连接，即便它们处在非首选的区域中也是如此。

可满足一次启动的会话的理想顺序为：

1. 重新连接到首选区域中的现有会话。
2. 重新连接到不同于首选区域的区域中的现有断开连接会话。
3. 在首选区域中启动新的会话。
4. 重新连接到不同于首选区域的区域中的现有已连接会话。
5. 在不同于首选区域的区域中启用一个新的会话。

其他区域偏好注意事项

- 如果您配置一个用户组（例如安全组）的主区域，该组的用户（通过直接或间接成员关系）关联到指定的区域。但是，用户可以是多个安全组的成员，因此可能具有通过其他组成员关系配置的不同主区域。在这种情况下，可能无法清晰确定该用户的主区域。

  如果用户具有一个不通过组成员关系获得的已配置主区域，该区域将用于区域偏好。任何通过组成员关系获得的区域关联将被忽略。

  如果该用户具有多个仅通过组成员关系获得的不同区域关联，则代理会在这些区域中进行随机选择。代理完成选择之后，该区域将用于后续的会话启动，直到用户的组成员关系变更为止。

- 用户位置区域偏好要求由连接设备的 Citrix NetScaler Gateway 来检测端点设备上的 Citrix Receiver。必须对 NetScaler 进行配置，以将 IP 地址范围与特定区域关联，同时必须通过 StoreFront 将已发现的区域身份传递给 Controller。

有关区域首选项的详细信息，请参阅 Zone preference internals（区域首选项内部）。

注意事项、要求和最佳做法

- 您可以将以下项目放置在一个区域中：Controller、计算机目录、主机连接、用户和应用程序。如果计算机目录使用主机连接，则该目录和连接都应位于相同的区域中，以便其之间的连接属于低延迟高带宽连接。
- 如果将多个项目放置在一个卫星区域中，会影响站点与这些项目以及与跟它们相关的其他对象的交互方式。
  - 多个 Controller 计算机放置一个卫星区域中时，假定这些计算机与同一卫星区域中的虚拟机管理程序和 VDA 计算机的

© 1999-2017 Citrix Systems, Inc. All rights reserved.

（本地）连接情况很好。那么，在处理这些虚拟机管理程序和 VDA 计算机时，优先使用该卫星区域中的 Controller，而不是主要区域中的 Controller。
    - 某个虚拟机管理程序连接放置在一个卫星区域中时，假定通过该虚拟机管理程序连接管理的所有虚拟机管理程序也都位于该卫星区域中。那么，通过该虚拟机管理程序连接进行通信时，优先使用该卫星区域中的 Controller，而不是主要区域中的 Controller。
    - 某个计算机目录放置在一个卫星区域中时，假定该目录中的所有 VDA 计算机都位于该卫星区域中。首次注册了各个 VDA 后，并且激活了 Controller 列表自动更新机制后，尝试向站点注册时，优先使用本地 Controller，而不是主要区域中的 Controller。
    - NetScaler Gateway 实例也可以与区域关联。对于此处所述其他元素，这是在 StoreFront 最佳 HDX 路由配置中完成的，而不是在 XenApp 或 XenDesktop 站点配置中完成的。某个 NetScaler Gateway 与某个区域关联后，使用与该区域中的 VDA 计算机的 HDX 连接时，优先使用该 NetScaler Gateway。
- 创建生产站点，然后创建第一个计算机目录和交付组时，所有项目都位于主要区域中；完成该初始设置之后才能创建卫星区域。（如果创建一个空站点，主要区域最初将仅包含一个 Controller；您可以在创建计算机目录和交付组之前或之后创建卫星区域。）
- 创建第一个包含一个或多个项目的卫星区域时，站点中的所有其他项目将保留在主要区域中。
- 主要区域的默认名称为“主要”；可以更改该名称。尽管 Studio 显示内容指示哪个区域是主要区域，但是，最佳做法是为主要区域使用易于识别的名称。可以重新分配主要区域（即，将另一个区域设为主要区域），但应始终包含站点数据库和高可用性服务器。
- 站点数据库应始终位于主要区域中。
- 创建区域后，稍后可以将项目从一个区域移动到另一个区域。请注意，这种灵活性可能会允许您分隔大体匹配的最适合的项目；例如，将某个计算机目录移动到与创建该目录中的计算机的连接不同的区域可能会影响性能。因此，在区域之间移动项目之前，请考虑预料之外的潜在影响。请保持目录与其使用的主机连接位于相同的区域中，或者位于连接信号良好的区域中（例如，通过低延迟高带宽网络建立连接）。
- 要实现最佳性能，请仅在主要区域中安装 Studio 和 Director。如果希望另一个 Studio 位于卫星区域中（例如，如果正在将包含多个 Controller 的某个卫星区域用于在主要区域不可访问时进行故障转移），请运行 Studio 作为本地发布的应用程序。也可以从卫星区域访问 Director，因为 Director 属于 Web 应用程序。
- 理想情况下，应对从其他区域或外部位置传入到该区域的用户连接使用卫星区域中的 NetScaler Gateway，即使您能够对该区域内部的连接使用 NetScaler Gateway 也是如此。
- **谨记：**要使用区域首选项功能，您必须至少使用 StoreFront 3.7 和 NetScaler Gateway 11.0-65.x。
- 有关更多技术详细信息和性能注意事项，请参阅区域深度探讨。

连接质量限制

卫星区域中的 Controller 直接执行与站点数据库的 SQL 交互。这对卫星区域与包含站点数据库的主要区域之间的链接的质量造成了一些限制。具体限制与该卫星区域中部署的 VDA 数和那些 VDA 上的用户会话数相关。因此，与具有大量 VDA 和会话数的卫星区域相比，只有少量 VDA 和会话数的卫星区域在与数据库的连接质量较差时也可以正常运行。

有关详细信息，请参阅延迟和 SQL 阻塞查询改进功能。

延迟对代理性能的影响

尽管区域允许用户使用延迟较高的链接，假定有一个本地 Broker，额外的延迟不可避免地会影响最终用户体验。对于用户执行的大多数操作，他们体验到的慢速是由卫星区域中的 Controller 与站点数据库之间的往返造成的。

对于启动应用程序，会话代理过程识别合适的 VDA 来向其发送会话启动请求时，会发生额外的延迟。

创建和管理区域

© 1999-2017 Citrix Systems, Inc. All rights reserved.

完全权限管理员可以执行所有区域创建和管理任务。但是，还可以创建允许您创建、编辑或删除区域的自定义角色。在区域之间移动项目不需要区域相关权限（区域读取权限除外）；但是，必须对要移动的区域具有编辑权限。例如，要将计算机目录从一个区域移动到另一个区域，必须对该计算机目录具有编辑权限。有关详细信息，请参阅"委派管理"一文。

如果使用 Provisioning Services：本版本中提供的 Provisioning Services 控制台无法识别区域，因此，Citrix 建议您使用 Studio 创建要放置在卫星区域中的计算机目录。可以使用 Studio 向导创建目录，并指定恰当的卫星区域。因此，可以使用 Provisioning Services 控制台在该目录中置备计算机。（如果使用 Provisioning Services 向导创建目录，则会将该目录放置在主要区域中，并且您以后需要使用 Studio 将其移动到卫星区域中。）

创建区域

1. 在 Studio 导航窗格中，选择**配置 > 区域**。
2. 在"操作"窗格中选择**创建区域**。
3. 输入该区域的名称和说明（可选）。该名称在站点中必须唯一。
4. 选择要放置在新区域中的项目。可以过滤或搜索要从中选择项目的列表。也可以创建空区域；不需要选择任何项目。
5. 单击**保存**。

作为此方法的备选方法，可以在 Studio 中选择一个或多个项目，然后在"操作"窗格中选择**创建区域**。

更改区域名称或说明

1. 在 Studio 导航窗格中，选择**配置 > 区域**。
2. 在中间窗格中选择一个区域，然后在"操作"窗格中选择**编辑区域**。
3. 更改区域名称和/或说明。如果要更改主要区域的名称，请确保该区域仍可轻松识别为主要区域。
4. 单击**确定**或**应用**。

将项目从一个区域移动到另一个区域

1. 在 Studio 导航窗格中，选择**配置 > 区域**。
2. 在中间窗格中选择一个区域，然后选择一个或多个项目。
3. 将项目拖动到目标区域，或者在"操作"窗格中选择**移动项目**，然后指定要将项目移动到的区域。

此时将显示一条列出所选项目的确认消息，并询问您是否确实要移动全部项目。

记住：如果计算机目录使用连接到虚拟机管理程序或云服务的主机连接，则该目录和连接都应位于相同的区域中。否则，性能可能会受到影响。如果移动一个项目，请同时移动另一个。

删除区域

区域必须不包含任何内容才能将其删除。不能删除主要区域。

1. 在 Studio 导航窗格中，选择**配置 > 区域**。
2. 在中间窗格中选择一个区域。
3. 在"操作"窗格中选择**删除区域**。如果该区域不为空（包含项目），系统会要求您选择要移动这些项目的区域。
4. 确认删除。

添加用户的主区域

配置用户的主区域也称为*将用户添加到区域*。

1. 在 Studio 导航窗格中选择**配置 > 区域**，然后在中间窗格中选择一个区域。
2. 在"操作"窗格中选择**将用户添加到区域**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. 在**将用户添加到区域**对话框中，单击**添加**，然后选择要添加到该区域的用户和用户组。如果您指定了已经具有主区域的用户，一条消息会提供两个选择：**是** = 仅添加您指定的不具有主区域的用户；**否** = 返回至用户选择对话框。
4. 单击**确定**。

对于具有已配置主区域的用户，您可能需要仅从他们的主区域启动会话：

1. 创建或编辑交付组。
2. 在**用户**页面上，选择**如果已配置，则会话必须在用户的主区域中启动**对话框。

   由该交付组中用户启动的所有会话必须在用户的主区域中从计算机启动。如果交付组中的用户不具有已配置的主区域，此设置无效。

删除用户的主区域

此步骤也称为从区域中删除用户。

1. 在 Studio 导航窗格中选择**配置 > 区域**，然后在中间窗格中选择一个区域。
2. 在“操作”窗格中选择**从区域中删除用户**。
3. 在**将用户添加到区域**对话框中，单击**删除**，然后选择要从该区域中删除的用户和用户组。请注意，此操作仅从该区域中删除用户；这些用户仍保留在他们所属的交付组和应用程序组。
4. 系统提示时确认删除。

管理应用程序的主区域

配置应用程序的主区域也称为将应用程序添加到区域。默认情况下，在多区域环境中，应用程序不具有主区域。

应用程序的主区域在该应用程序的属性中指定。您可以在将应用程序添加到组时配置应用程序属性，也可以稍后配置，方法是通过选择 Studio 中的应用程序并编辑其属性。

- 在创建交付组、创建应用程序组或将应用程序添加到现有组时，请在向导的**应用程序**页面上选择**属性**。
- 要在添加应用程序后更改应用程序的属性，请在 Studio 导航窗格中选择**应用程序**。选择一个应用程序，然后在“操作”窗格中选择**编辑应用程序属性**。

在应用程序的属性/设置的**区域**页面上：

- 如果您想要该应用程序具有一个主区域：
  - 选择**使用选定的区域来决定**单选按钮，然后从下拉菜单中选择该区域。
  - 如果您希望该应用程序仅从选定的区域（不从任何其他区域）中启动，请选中该区域选择下方的复选框。
- 如果您不希望该应用程序具有一个主区域：
  - 选择**请勿配置主区域**单选按钮。
  - 如果您不希望代理在启动该应用程序时考虑任何配置的用户区域，请选中该单选按钮下方的复选框。在此情况下，不会使用应用程序或用户主区域来确定从何处启动该应用程序。

包括指定区域在内的其他操作

添加主机连接，或者创建计算机目录（站点创建过程中除外）时，可以指定要将项目分配到的区域，前提是您已至少创建一个卫星区域。

在大多数情况下，主要区域为默认区域。使用 Machine Creation Services 创建计算机目录时，将自动选择为主机连接配置的区域。

如果站点中不包含任何卫星区域，则会假定主要区域，并且区域选择对话框不显示。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

连接和资源

Dec 05, 2017

在本文中：

- 简介
- 与连接类型有关的信息的查找位置
- 主机存储
- 创建连接和资源
- 编辑连接设置
- 打开或关闭连接的维护模式
- 删除连接
- 重命名或测试连接
- 查看连接上的计算机详细信息
- 管理连接上的计算机
- 编辑存储
- 删除、重命名或测试资源
- 将 IntelliCache 用于 XenServer 连接
- 连接计时器

简介

在创建站点时，可以选择性创建与托管资源的第一个连接。之后，可以更改该连接并创建其他连接。配置连接包括从受支持的虚拟机管理程序和云服务中选择连接类型。选择的存储和网络组成了该连接的资源。

只读权限管理员可以查看连接和资源详细信息；只有完全权限管理员才可以执行连接和资源管理任务。有关详细信息，请参阅委派管理一文。

与连接类型有关的信息的查找位置

可以使用受支持的虚拟化平台托管和管理 XenApp 或 XenDesktop 环境中的计算机。系统要求一文列出了支持的类型。可以使用受支持的云部署解决方案托管产品组件和置备虚拟机。这些解决方案汇集了各种计算资源，可以构建公有云、私有云和混合型基础设施即服务 (IaaS) 云。

有关详细信息，请参阅以下来源。

Microsoft Hyper-V

- Microsoft System Center Virtual Machine Manager 虚拟化环境一文。
- Microsoft 文档。

Microsoft Azure

- Microsoft Azure 虚拟化环境一文。
- Microsoft 文档。

Microsoft Azure Resource Manager

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Microsoft Azure Resource Manager 虚拟化环境一文。
- Microsoft 文档。

Amazon Web Services (AWS)

- Citrix XenDesktop on AWS。
- AWS 文档。
- 在 Studio 中创建连接时，必须提供 API 密钥和密钥值。可以先从 AWS 中导出包含这些值的密钥文件，然后再导入。此外，还必须提供地理区域、可用区、VPC 名称、子网地址、域名、安全组名称和凭据。
- root AWS 帐户的凭据文件（从 AWS 控制台检索）的格式与为标准 AWS 用户下载的凭据文件的格式不同。因此，Studio 不能使用此文件来填充 API 密钥和密钥字段。请务必使用 AWS IAM 凭据文件。

CloudPlatform

- CloudPlatform 文档。
- 在 Studio 中创建连接时，必须提供 API 密钥和密钥值。可以先从 CloudPlatform 中导出包含这些值的密钥文件，然后将这些值导入到 Studio 中。

Citrix XenServer

- Citrix XenServer 文档。
- 创建连接时，必须提供 VM 超级管理员或更高级别用户的凭据。
- Citrix 建议使用 HTTPS 确保与 XenServer 的通信安全。要使用 HTTPS，必须替换 XenServer 上安装的默认 SSL 证书；请参阅 CTX128656。
- 如果 XenServer 上已启用高可用性，则可以配置高可用性。Citrix 建议您选择池中的所有服务器（从“编辑高可用性”中），以便在池主服务器出现故障时能够与 XenServer 进行通信。
- 如果 XenServer 支持 vGPU，可以选择 GPU 类型和组，或直通。显示内容将指示所选项是否具有专用 GPU 资源。

Nutanix Acropolis

- Nutanix 虚拟化环境一文。
- Nutanix 文档。

VMware

- VMware 虚拟化环境一文。
- VMware 产品文档。

主机存储

置备计算机时，数据将按类型分类：

- 操作系统数据，其中包括主映像。
- 临时数据，其中包括写入 MCS 置备计算机的非持久性数据、Windows 页面文件、用户配置文件数据，以及与 ShareFile 同步的任何数据。计算机每次重新启动时将丢弃该数据。
- 存储在个人虚拟磁盘上的个人数据。

为每种数据类型提供独立的存储可以降低每个存储设备上的负载并提高 IOPS 性能，从而充分利用主机的可用资源。此外，这样还允许对不同的数据类型使用适当的存储。因为对某些数据而言，永久性和恢复能力比其他方面更加重要。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

存储可以是虚拟机管理程序的共享存储（位于中央位置，与所有主机使用的任何主机分隔开来），也可以是其本地存储。例如，中央共享存储可以是一个或多个 Windows Server 2012 群集化存储卷（无论是否包含附加存储），也可以是存储供应商提供的设备。中央存储还可以提供自己的优化设置，例如，虚拟机管理程序存储控制路径以及通过合作伙伴插件直接访问。

在本地存储临时数据可避免必须遍历网络才能访问共享存储的问题。这样还可降低共享存储设备上的负载 (IOPS)。共享存储的成本更高，因此，在本地存储数据可以降低费用。这些优势必须与虚拟机管理程序服务器上充足的存储空间的可用性进行权衡。

创建连接时，可以选择以下两种存储管理方法之一：虚拟机管理程序共享的存储或虚拟机管理程序的本地存储。

注意：在一个或多个 XenServer 主机上使用本地存储作为临时数据存储时，请确保池中的每个存储位置都具有唯一的名称。（要在 XenCenter 中更改名称，请右键单击该存储并编辑名称属性。）

虚拟机管理程序共享的存储

虚拟机管理程序共享的存储方法存储需要长期存储在中央位置的数据，提供中央备份和管理。该存储保留操作系统磁盘和个人虚拟磁盘。

选择此方法时，可以选择是否对不需要永久存在或恢复能力不需要与共享存储中的数据相同的临时计算机数据使用本地存储（位于相同的虚拟机管理程序池中的服务器上）。这称为*临时数据缓存*。本地磁盘有助于降低传输到主操作系统存储的流量。此磁盘在每次计算机重新启动后清除。此磁盘通过直写内存缓存进行访问。请记住，如果为临时数据使用本地存储，置备的 VDA 将绑定到特定的虚拟机管理程序主机；如果该主机出现故障，VM 将无法启动。

例外：如果使用群集存储卷 (Clustered Storage Volumes, CSV)，Microsoft System Center Virtual Machine Manager 则不允许在本地存储上创建临时数据缓存磁盘。

创建连接时，如果启用了本地存储临时数据的选项，则可以在创建使用该连接的计算机目录时，为每个 VM 的缓存磁盘大小和内存大小启用并配置非默认值。但是，默认值是根据连接类型定制的，满足大多数情况下的需求。有关详细信息，请参阅创建计算机目录一文。

虚拟机管理程序还可以通过磁盘映像的读取缓存在本地提供优化技术；例如，XenServer 提供 IntelliCache。这样还可以降低传输到中央存储的网络流量。

虚拟机管理程序的本地存储

虚拟机管理程序的本地存储在虚拟机管理程序上本地存储数据。使用此方法时，主映像和其他操作系统数据将被传输到在站点中使用的所有虚拟机管理程序，用于初始计算机创建和将来的映像更新。这会导致管理网络中存在大量流量。映像传输也很耗时，并且映像对每个主机可用的时间也不同。

选择此方法时，可以选择是否为个人虚拟磁盘使用共享存储，以提供恢复能力以及对备份和灾难恢复系统的支持。

创建连接和资源

创建站点时，可以选择性创建第一个连接。站点创建向导包含与连接有关的页面，如下所述：连接、存储管理、存储选择和网络。

如果要在创建站点后创建连接，请从下面的步骤 1 开始操作。

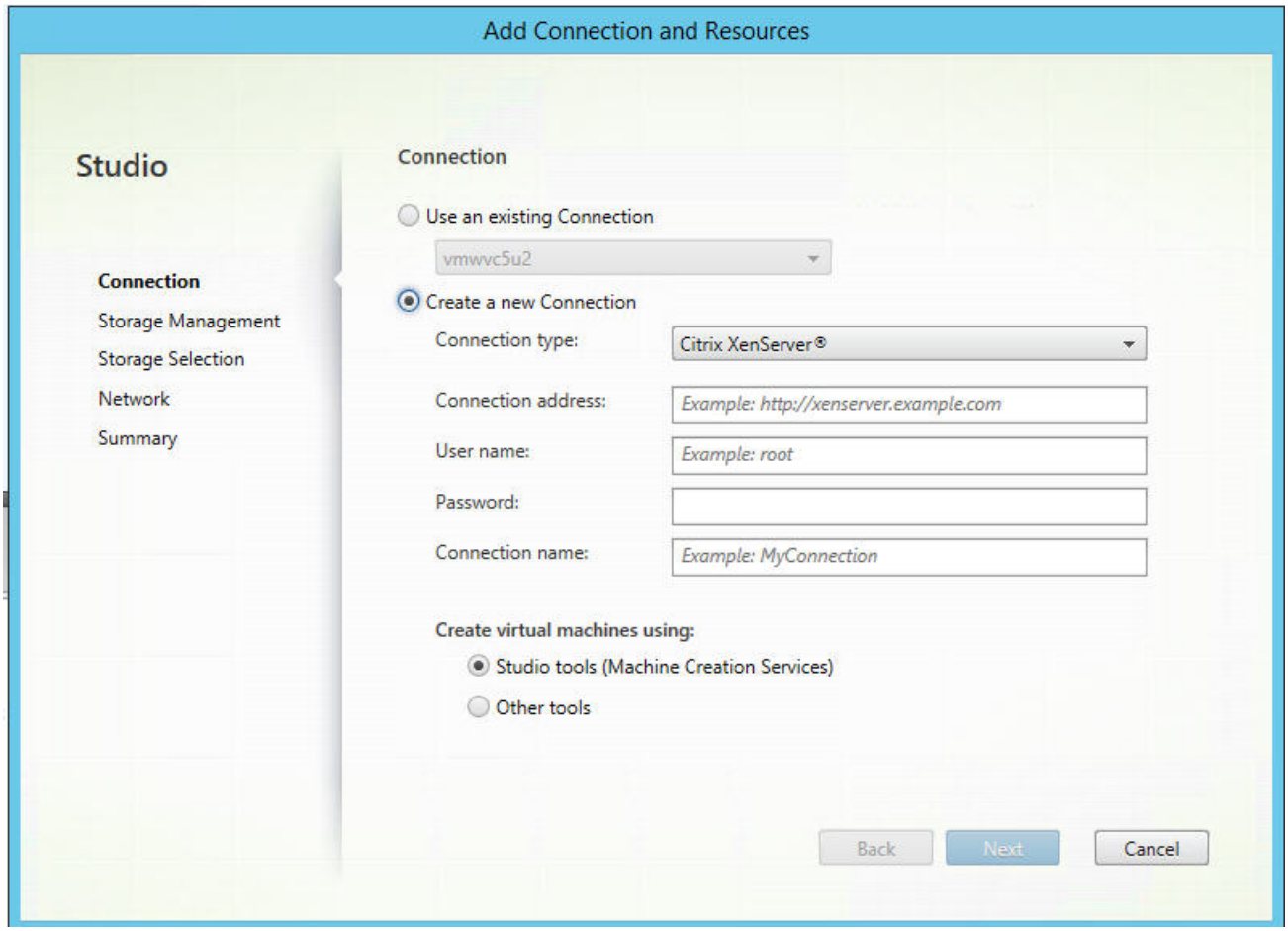
重要：创建连接之前，主机资源（存储和网络）必须可用。

- 在 Studio 导航窗格中，选择**配置 > 托管**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 在“操作”窗格中，选择**添加连接和资源**。
- 该向导将引导您完成以下页面（具体的页面内容取决于所选连接类型）。完成每一页之后，请单击**下一步**，直到到达**摘要**页为止。

连接

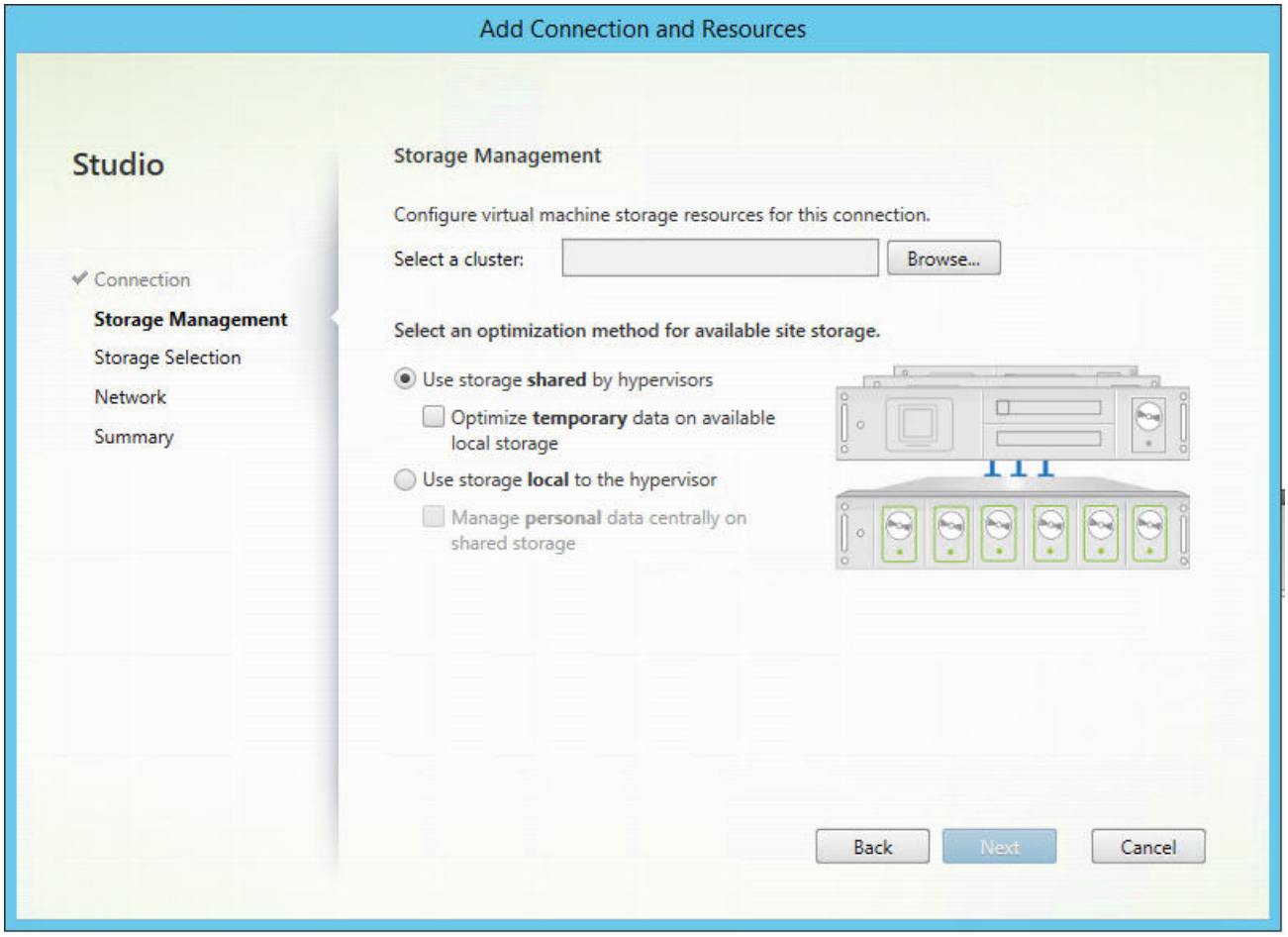


在**连接**页面上：

- 要创建一个新的连接，请选择**创建新连接**。要基于相同的主机配置创建一个连接作为现有的连接，请选择**使用现有连接**，然后选择相关连接。
- 在**连接类型**字段中选择要使用的虚拟机管理程序或云服务。
- 连接地址和凭据字段因所选连接类型而异。输入请求的信息。
- 输入连接名称。此名称将在 Studio 中显示。
- 选择要用于创建虚拟机的工具：Studio 工具（例如，Machine Creation Services 或 Provisioning Services）或其他工具。

存储管理

© 1999-2017 Citrix Systems, Inc. All rights reserved.



有关存储管理类型和方法的信息，请参阅主机存储。

如果要配置与 Hyper-V 或 VMware 主机的连接，请浏览到群集名称并选择一个名称。其他连接类型不需要群集名称。

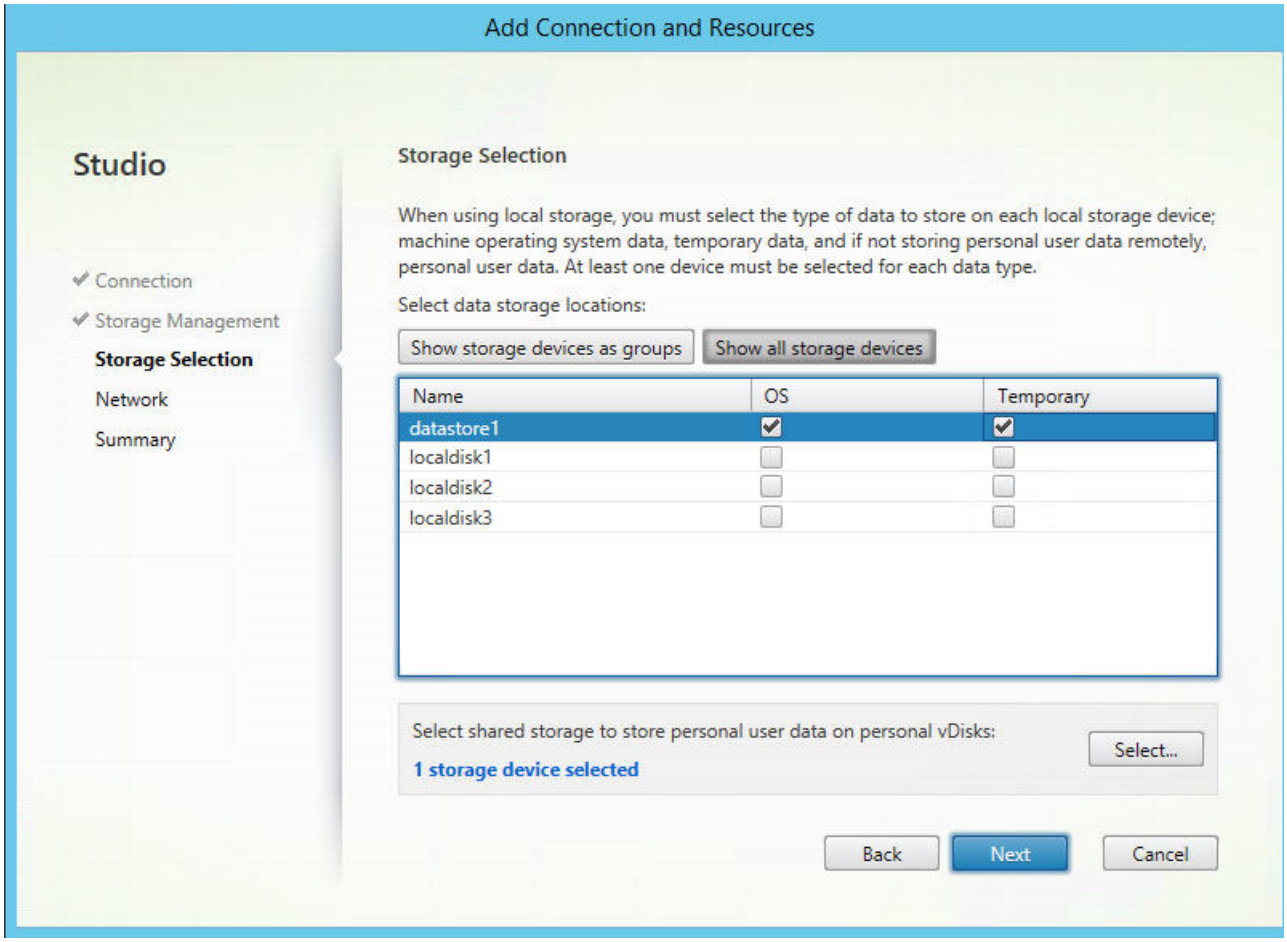
选择存储管理方法：虚拟机管理程序共享的存储或虚拟机管理程序的本地存储。

- 如果选择虚拟机管理程序共享的存储，请指出是否要在可用的本地存储上保存临时数据。（可以在使用此连接的计算机目录中指定非默认临时存储大小。）**例外**：使用群集存储卷 (CSV) 时，Microsoft System Center Virtual Machine Manager 不允许在本地存储上创建临时数据缓存磁盘，因此，在 Studio 中配置该存储管理设置将失败。
- 如果选择虚拟机管理程序的本地存储，请指出是否要在共享存储上管理个人数据（个人虚拟磁盘）。

如果使用 XenServer 虚拟机管理程序上的共享存储，请指出是否要使用 IntelliCache 来降低共享存储设备上的负载。请参阅将 IntelliCache 用于 XenServer 连接。

存储选择

© 1999-2017 Citrix Systems, Inc. All rights reserved.



有关存储选择的详细信息，请参阅主机存储。

请至少为每种可用的数据类型选择一个主机存储设备。在上一页面中选择的存储管理方法将影响此页面上可供选择的数据类型。必须至少为每种受支持的数据类型选择一个存储设备，才能继续进入向导中的下一页面。

如果您在上一页面中选择了以下类型之一，**选择存储**页面将包含附加配置选项。

- 如果选择虚拟机管理程序共享的存储，并启用 **Optimize temporary data on available local storage**（优化可用本次存储中的临时数据）复选框，则可以选择用于存储临时数据的本地存储设备（在相同的虚拟机管理程序池中）。
- 如果选择虚拟机管理程序的本地存储，并启用 **Manage personal data centrally on shared storage**（在共享存储上集中管理个人数据）复选框，则可以选择用于存储个人 (PvD) 数据的共享设备。

系统会显示当前选择的存储设备数量（在上图中，显示“已选择 1 个存储设备”）。将鼠标悬停在该条目上时，将显示所选设备的名称（除非未配置任何设备）。

1. 单击**选择**更改要使用的存储设备。
2. 在**选择存储**对话框中，选中或取消选中存储设备复选框，然后单击**确定**。

网络

输入资源的名称；此名称在 Studio 中显示，以表示与连接关联的存储和网络组合。

选择 VM 要使用的一个或多个网络。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

总结

检查所做的选择；如果要做出更改，请使用返回到上一个向导页面。完成检查后，请单击**完成**。

记住：如果选择在本地存储临时数据，则可以在创建包含使用此连接的计算机的计算机目录时为临时数据配置非默认值。请参阅创建计算机目录一文。

编辑连接设置

请勿使用此过程来重命名连接或创建新连接。它们属于不同的操作。仅在当前主机有新地址时才能更改地址；输入其他计算机的地址会中断连接的计算机目录。

无法更改连接的 GPU 设置，因为访问此资源的计算机目录必须使用恰当的 GPU 特定的主映像。创建新连接。

1. 在 Studio 导航窗格中，选择**配置 > 托管**。
2. 选择连接，然后在“操作”窗格中选择**编辑连接**。
3. 编辑连接时，请按照下面面向可用设置的指南进行操作。
4. 完成后，单击**应用**以应用您执行的所有更改并保持打开窗口，或者单击**确定**应用更改并关闭窗口。

连接属性页面：

- 要更改连接地址和凭据，请选择**编辑设置**，然后输入新信息。
- 要为 XenServer 连接指定高可用性服务器，请单击**编辑高可用性服务器**。Citrix 建议选择池中的所有服务器，以便在池主服务器出现故障时允许与 XenServer 实现通信。

高级页面：

对于 Microsoft System Center Configuration Manager (ConfMgr) 局域网唤醒连接类型（通过 Remote PC Access 发出），请输入 ConfMgr 唤醒代理、幻数据包和数据包传输信息。

限制阈值设置允许您指定允许对连接执行的电源操作数上限。在电源管理设置允许同时启动的计算机过多或过少时，这些设置非常有用。每种连接类型具有适用于大多数情况的特定默认值，通常不应更改。

同步操作（所有类型）和**同步个人虚拟磁盘清单更新**设置指定两个值：一个是可在此连接上同时发生的最大绝对值，另一个是占使用此连接的所有计算机的最大百分比。必须同时指定绝对值和百分比值；应用的实际限制是所配置值中的较小值。

例如，在包含 34 台计算机的部署中，如果**同步操作(所有类型)** 设置为绝对值 10 且百分比值为 10，则所应用的实际限制为 3（即，34 的 10% 四舍五入到最接近的整数，此值小于 10 台计算机这一绝对值）。

每分钟最大新操作数是一个绝对值；没有百分比值。

注意：在**连接选项**字段中输入信息时，请务必在 Citrix 技术支持代表的指导下进行。

打开或关闭连接的维护模式

打开连接的维护模式可防止任何新电源操作影响此连接上存储的任何计算机。计算机处于维护模式时，用户无法连接到计算机。如果已经连接用户，维护模式将在其注销后生效。

1. 在 Studio 导航窗格中，选择**配置 > 托管**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. 选择连接。要打开维护模式，请在“操作”窗格中选择**打开维护模式**。要关闭维护模式，请选择**关闭维护模式**。

另外，也可以针对单台计算机打开或关闭维护模式。此外，还可以为计算机目录或交付组中的计算机打开或关闭维护模式。

删除连接

小心：如果删除连接，则会导致大量计算机被删除，并会导致数据丢失。请确保受影响计算机上的用户数据已经备份，或者已不再需要。

删除连接之前，请确保：

- 所有用户都已从该连接上所存储的计算机中注销。
- 没有仍在运行的已断开连接的用户会话。
- 已为池计算机和专用计算机打开维护模式。
- 关闭连接使用的计算机目录中的所有计算机。

删除计算机目录引用的连接时，该目录会变为不可用。如果有目录引用此连接，可以选择删除该目录。删除目录前，请确保其他连接未使用此目录。

1. 在 Studio 导航窗格中，选择**配置 > 托管**。
2. 选择连接，然后在“操作”窗格中选择**删除连接**。
3. 如果此连接上存储了计算机，系统会询问您是否删除这些计算机。如果要将其删除，请指定应对关联的 Active Directory 计算机帐户执行的操作。

重命名或测试连接

1. 在 Studio 导航窗格中，选择**配置 > 托管**。
2. 选择连接，然后在“操作”窗格中选择**重命名连接**或**测试连接**。

查看连接上的计算机详细信息

1. 在 Studio 导航窗格中，选择**配置 > 托管**。
2. 选择连接，然后在“操作”窗格中选择**查看计算机**。

上方窗格列出通过此连接访问的计算机。选择某台计算机可在下方窗格查看其详细信息。对于打开的会话，还会提供会话详细信息。

使用搜索功能可快速查找计算机。从窗口顶部的列表中选择保存的搜索，或者创建新的搜索。可以通过键入完整或部分计算机名称进行搜索，也可以构建表达式进行高级搜索。要构建表达式，请单击**展开**，然后从属性和运算符列表中进行选择。

管理连接上的计算机

1. 在 Studio 导航窗格中，选择**配置 > 托管**。
2. 选择连接，然后在“操作”窗格中选择**查看计算机**。
3. 在“操作”窗格中，选择以下选项之一。某些操作可能不可用，具体取决于计算机状态和连接主机类型。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **启动**：启动计算机（如果计算机已关闭或挂起）。
- **挂起**：不关闭但暂停计算机并刷新计算机列表。
- **关闭**：请求关闭操作系统。
- **强制关闭**：强行关闭计算机并刷新计算机列表。
- **重新启动**：请求关闭操作系统，然后再次启动计算机。如果操作系统无法关闭，则计算机仍保持当前状态。
- **启用维护模式**：暂时停止连接到计算机。在此状态下用户无法连接计算机。如果已经连接用户，则维护模式会在其注销后生效。（还可以为通过某个连接进行访问的所有计算机打开或关闭维护模式，请参阅上文。）
- **从交付组中删除**：将计算机从交付组中删除并不会将其从交付组使用的计算机目录中删除。仅当计算机未连接任何用户时，才能将其删除；在删除计算机时，可打开维护模式暂时阻止用户连接此计算机。
- **删除**：删除计算机后，用户将不再具有访问该计算机的权限，该计算机将从计算机目录中删除。删除计算机之前，应确保所有用户数据都已备份，或者不再需要这些数据。仅当计算机未连接任何用户时，才能将其删除；在删除计算机时，可打开维护模式暂时停止用户连接此计算机。

对于涉及关闭计算机的操作，如果计算机在 10 分钟内未关闭，则会关机。如果 Windows 尝试在关闭期间安装更新，可能面临在更新完成前计算机关机的风险。

编辑存储

可以显示用于存储使用连接的 VM 的操作系统、临时数据和个人 (PvD) 数据的服务器的状态。还可以指定用于每种数据类型的存储的服务器。

1. 在 Studio 导航窗格中，选择“配置”>“托管”。
2. 选择连接，然后在“操作”窗格中选择“编辑存储”。
3. 在左侧窗格中，选择数据类型：操作系统、个人虚拟磁盘或临时数据。
4. 选中或取消选中所选数据类型的一个或多个存储设备对应的复选框。
5. 单击“确定”。

列表中的每个存储设备都包含其名称和存储状态。有效存储状态值如下：

- **使用中**：存储正用于创建新计算机。
- **被取代**：存储正仅用于现有计算机。不会将新计算机添加到此存储中。
- **未在使用中**：存储未用于创建计算机。

如果取消选中当前处于**使用中**状态的设备对应的复选框，其状态将更改为**被取代**。现有计算机将继续使用该存储设备（并且可以向其中写入数据），因此，即使在该位置停止用于创建新计算机后，该位置也有可能会满载。

删除、重命名或测试资源

1. 在 Studio 导航窗格中，选择**配置 > 托管**。
2. 选择资源，然后在“操作”窗格中选择相应的条目：**删除资源**、**重命名资源**或**测试资源**。

将 IntelliCache 用于 XenServer 连接

通过使用 IntelliCache，托管的 VDI 部署将更节省成本，因为您可以将共享存储与本地存储结合使用。这会提高性能并降低网络流量。本地存储对共享存储的主映像进行缓存，从而减少了共享存储上的读操作数量。对于共享桌面，对不同磁盘写入的内

© 1999-2017 Citrix Systems, Inc. All rights reserved.

容将写入到主机上的本地存储而不是共享存储中。

- 使用 IntelliCache 时，共享存储必须为 NFS。
- Citrix 建议您使用高性能本地存储设备来保证实现最快速的数据传输。

要使用 IntelliCache，必须在此产品和 XenServer 中均启用 IntelliCache。

- 安装 XenServer 时，选择**启用精简置备(XenDesktop 的优化存储)**。Citrix 不支持由启用了 Intellicache 的服务器和未启用 IntelliCache 的服务器构成的混合池。有关详细信息，请参阅 XenServer 文档。
- 在 XenApp 和 XenDesktop 中，默认情况下禁用 IntelliCache。只能在创建 XenServer 连接时更改此设置；之后将无法禁用 IntelliCache。从 Studio 添加 XenServer 连接时：
  - 选择**共享**作为存储类型。
  - 选中**使用 IntelliCache** 复选框。

连接计时器

可以使用策略设置来配置三种连接计时器：

- **最大连接计时器**：确定保持用户设备和虚拟桌面之间连接不中断的最长持续时间。使用**会话连接计时器**和**会话连接计时器间隔**策略设置。
- **连接空闲计时器**：确定如果用户不输入任何内容，用户设备与虚拟桌面之间的连接可以保持多久不中断。使用**会话空闲计时器**和**会话空闲计时器间隔**策略设置。
- **断开连接计时器**：确定在会话注销之前，已断开连接且锁定的虚拟桌面可以保持锁定状态的时间。使用**断开连接的会话计时器**和**断开连接的会话计时器间隔**策略设置。

如果更新其中任何一项设置，请确保部署中的设置一致。

有关详细信息，请参阅策略设置文档。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

本地主机缓存

Mar 12, 2018

为确保 XenApp 和 XenDesktop 站点数据库始终可用，Citrix 建议按照 Microsoft 的高可用性最佳做法开始部署容错 SQL Server。（系统要求一文中的“数据库”一节列出了 XenApp 和 XenDesktop 中支持的 SQL Server 高可用性功能。）但是，网络问题和中断可能会导致用户无法连接到其应用程序或桌面。

本地主机缓存 (LHC) 功能允许在发生中断时，XenApp 或 XenDesktop 站点中的连接代理操作能够继续。Delivery Controller 与站点数据库之间的连接失败时会出现中断。在站点数据库无法访问达 90 秒时，将使用本地主机缓存。

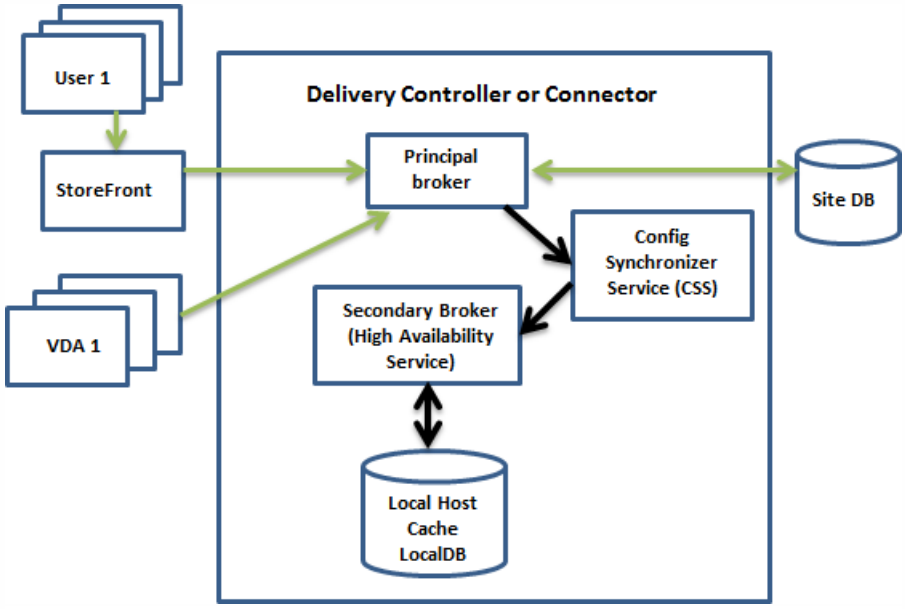
本地主机缓存是 XenApp 和 XenDesktop 中最全面的高可用性功能。它是替代 XenApp 7.6 中引入的连接租用功能的更强大功能。

注意：虽然连接租用在版本 7.15 LTSR 中受支持，但将在以下版本中删除该功能。

尽管此本地主机缓存实施与 XenApp 6.x 及更早 XenApp 版本中的本地主机缓存功能的名称相同，但进行了显著的改进。此实施更强大且不易损坏。维护要求降低到最小，例如，不再需要定期运行 dsmaint 命令。此本地主机缓存在技术上是完全不同的实施；请继续阅读，了解其工作原理。

工作原理

下图说明了正常操作过程中本地主机缓存组件和通信路径。



正常操作过程中：

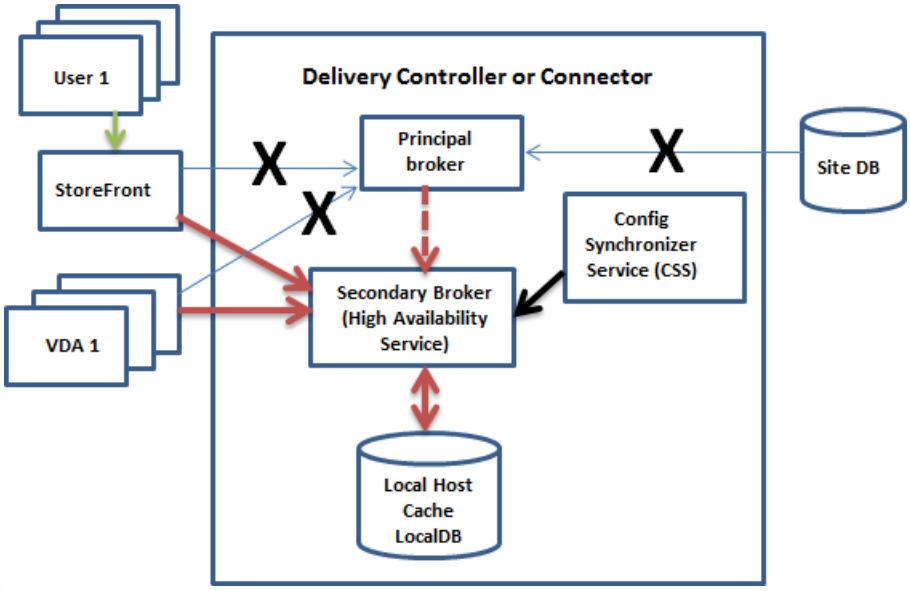
- Controller 上的*主 Broker* (Citrix Broker Service) 接受来自 StoreFront 的连接请求，并与站点数据库通信，以将用户与已向 Controller 注册的 VDA 连接。
- 每两分钟进行一次检查，以确定是否对主 Broker 的配置进行了更改。PowerShell/Studio 操作（例如，更改交付组属性）或系统操作（例如，计算机分配）可能会启动那些更改。
- 如果自上次检查后做了更改，主 Broker 将使用 Citrix Config Synchronizer Service (CSS) 将信息同步（复制）到 Controller 上

© 1999-2017 Citrix Systems, Inc. All rights reserved.

的*辅助 Broker*(Citrix High Availability Service)。所有 Broker 配置数据都会被复制，而不仅仅是自上次检查后更改的项。辅助 Broker 将数据导入 Controller 上的 Microsoft SQL Server Express LocalDB 数据库。CSS 确保辅助 Broker 的 LocalDB 数据库中的信息与站点数据库中的信息一致。每次同步时，都会重新创建 LocalDB 数据库。

- 如果自上次检查后没有进行任何更改，则不复制数据。

下图说明了主 Broker 失去与站点数据库的联系时（中断开始）通信路径的变化：



中断开始时：

- 主 Broker 不能再与站点数据库通信，并停止侦听 StoreFront 和 VDA 信息（图中标记了 X）。然后，主 Broker 指示辅助 Broker (High Availability Service) 开始侦听并处理连接请求（图中用红色虚线标记）。
- 中断开始时，辅助 Broker 没有当前 VDA 注册数据，但当 VDA 与其通信时，就会立即触发重新注册过程。在该过程中，辅助 Broker 还获取有关该 VDA 的当前会话信息。
- 在辅助 Broker 处理连接的同时，主 Broker 继续监视与站点数据库的连接。恢复连接时，主 Broker 指示辅助 Broker 停止侦听连接信息，且主 Broker 恢复代理操作。下次 VDA 与主 Broker 通信时，将触发重新注册过程。辅助 Broker 将删除之前中断中的任何剩余的 VDA 注册，并使用从 CSS 收到的配置更改来更新 LocalDB 数据库。

在同步期间发生中断这种不太可能发生的事件中，会丢弃当前导入，并使用已知的最后一个配置。

事件日志提供有关同步和中断的信息。请参阅下文的“监视”一节了解详细信息。

您还可以有意触发中断；请参阅下文的“强制中断”一节了解有关为什么及如何执行此操作的详细信息。

具有多个 Controller 的站点

除了其他任务外，CSS 还定期向辅助 Broker 提供有关区域中所有 Controller 的信息。（如果您的部署中没有多个区域，则此操作影响站点中的所有 Controller。）有了那些信息，每个辅助 Broker 都可以了解所有对等辅助 Broker。

辅助 Broker 在单独的通道中相互通信。如果发生中断，它们使用正在其中运行的计算机的 FQDN 名称的字母列表来确定（选择）哪个辅助 Broker 将负责在区域中执行代理操作。在中断期间，所有 VDA 向选定的辅助 Broker 重新注册。区域中的非选定辅助 Broker 将主动拒绝传入连接和 VDA 注册请求。

如果在中断期间某个选定的辅助 Broker 发生故障，将选择另一个辅助 Broker 来接管，且 VDA 将向新选定的辅助 Broker 重新注册。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

在中断期间，如果重新启动某个 Controller：

- 如果该 Controller 不是选定的主 Broker，则无法重新启动。
- 如果该 Controller 是选定的主 Broker，此时选择另一个 Controller，这会导致 VDA 重新注册。重新启动的 Controller 开启后，它会自动接管代理，这会导致 VDA 再次重新注册。在这种情况下，在重新注册期间，性能可能会受影响。

如果在正常操作期间关闭某个 Controller，然后在中断期间将其开启，如果该 Controller 被选为主 Broker，则无法在该 Controller 上使用本地主机缓存。

事件日志提供有关选择的信息。请参阅下文的“监视”一节。

设计考虑事项和要求

对于服务器托管的应用程序和桌面以及静态（分配的）桌面，支持本地主机缓存；而对于池 VDI 桌面（由 MCS 或 PVS 创建），不支持本地主机缓存。

对中断模式下的操作没有时间限制。但应尽快将站点恢复到正常操作。

中断期间不可用或更改内容

- 无法使用 Studio 或运行 PowerShell cmdlet。
- 无法从 Host Service 获取虚拟机管理程序凭据。所有计算机都处于未知电源状态，因此无法发出任何电源操作。但是，已打开电源的主机上的 VM 可以用于连接请求。
- 仅当在正常操作过程中发生了分配时，才可以使用分配的计算机。在中断期间不能执行新分配。
- 不能自动注册和配置 Remote PC Access 计算机。但是，正常操作过程中注册和配置的计算机可以使用。
- 如果资源在不同的区域中，服务器托管的应用程序和桌面用户使用的会话可能超过其配置的会话限制。
- 用户只能从包含当前处于活动状态的/选定的（二级）Broker 的区域中已注册的 VDA 启动应用程序和桌面。断电期间不支持跨区域启动（从一个区域中的 Broker 到另一个区域中的 VDA）。

默认情况下，发生中断时，启用了“ShutdownDesktopsAfterUse”属性的池交付组中进行电源管理的桌面 VDA 被置于维护模式。您可以更改此默认值，以允许在中断期间使用这些桌面。但是，中断期间您无法依赖电源管理。（正常操作恢复后，电源管理恢复。）此外，由于这些桌面未重新启动，它们可能包含前一个用户的数据。

要覆盖默认行为，必须在站点范围内并针对受影响的每个交付组启用它。运行以下 PowerShell cmdlet。

```
Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
Set-BrokerDesktopGroup -Name "<name>" -ReuseMachinesWithoutShutdownInOutage $true
```

在站点和交付组中启用此功能不会影响配置的“ShutdownDesktopsAfterUse”属性在正常操作期间的作用方式。

RAM 大小

LocalDB 服务可以使用大约 1.2 GB 的 RAM（每个数据库缓存最多 1 GB，另加 200 MB 用于运行 SQL Server Express LocalDB）。如果中断持续较长时间，且发生了很多登录（例如，12 个小时内 10K 用户），则 High Availability Service 最多可以使用 1 GB 的 RAM。这些内存要求是 Controller 的正常 RAM 要求之外的要求，因此您可能需要增加 RAM 总容量。

请注意，如果您对站点数据库使用 SQL Server Express 安装，则服务器将有两个 sqlserver.exe 进程。

CPU 核心和套接字配置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Controller 的 CPU 配置，尤其是可用于 SQL Server Express LocalDB 的核心数，直接影响本地主机缓存性能，甚至比内存分配还要严重。仅在数据库不可访问且 High Availability Service 处于活动状态时，在中断期间观察此 CPU 开销。

虽然 LocalDB 可以使用多个核心（最多 4 个），但只能使用一个套接字。添加多个套接字不会提高性能（例如，每个有 4 个套接字和 1 个核心）。相反，Citrix 建议结合使用多个套接字和多个核心。在 Citrix 测试中，2x3（2 个套接字，3 个核心）配置提供的性能优于 4x1 和 6x1 配置。

存储

由于在中断期间用户访问资源，LocalDB 会增长。例如，在以每秒 10 次登录运行的登录/注销测试期间，数据库以每 2-3 分钟 1 MB 的速度增长。在正常操作恢复时，将重新创建本地数据库并返还空间。但是，Broker 必须在安装 LocalDB 的驱动器上有足够的空间，以允许在中断期间数据库增长。在中断期间，本地主机缓存中还会发生其他 I/O 操作：大约每秒 3 MB 的写入操作，以及数十万次读取操作。

性能

在中断期间，一个 Broker 处理所有连接，因此，在正常操作过程中在多个 Controller 之间进行负载平衡的站点（或区域）中，选定的 Broker 需要处理的请求数可能远高于中断期间的正常数。因此，CPU 需求会比较高。站点（区域）中的每个 Broker 都必须能够处理 LocalDB 和所有受影响的 VDA 造成的额外负载，因为在中断期间选择的 Broker 可能会更改。

VDI 限制：

- 在单区域 VDI 部署中，中断期间最多可以有效处理 10,000 个 VDA。
- 在多区域 VDI 部署中，中断期间在每个区域中最多可以有效处理 10,000 个 VDA，在站点中最多可以处理 40,000 个 VDA。例如，在中断期间，可以有效处理以下站点之一：
  - 具有四个区域的站点，每个区域包含 10,000 个 VDA。
  - 具有七个区域的站点，一个区域包含 10,000 个 VDA，另外六个区域每个包含 5,000 个 VDA。

在中断期间，站点内的负载管理可能会受到影响。负载评估器（尤其是会话计数规则）可能会超额。

在所有 VDA 向 Broker 重新注册的这段时间，该 Broker 可能没有有关当前会话的完整信息。因此，在该时间间隔内的用户连接请求可能会导致启动新会话，即使有可能重新连接到现有会话也是如此。此时间间隔（在此期间，在重新注册过程中，“新”Broker 从所有 VDA 获取会话信息）无法避免。请注意，在该过渡时间间隔内，中断开始时已连接的会话不受影响，但新会话和会话重新连接会受影响。

每当 VDA 必须向不同的 Broker 重新注册时，都会出现此时间间隔：

- 中断开始：从主 Broker 迁移到辅助 Broker 时。
- 中断期间 Broker 发生故障：从发生故障的辅助 Broker 迁移到新选定的辅助 Broker 时。
- 从中断恢复：正常操作恢复且主 Broker 恢复控制时。

可以通过降低 Citrix Broker Protocol 的 HeartbeatPeriodMs 注册表值（默认为 600000 毫秒，即 10 分钟）来缩短该时间间隔。此检测信号值是 VDA 执行 ping 操作的时间间隔的两倍，因此，默认值将导致 ping 操作每隔 5 分钟执行一次。

例如，以下命令将检测信号更改为 5 分钟（300000 毫秒），这将导致 ping 操作每隔 2.5 分钟执行一次：

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name HeartbeatPeriodMs
-PropertyType DWORD –Value 300000
```

无论 VDA 注册的速度有多快，都无法完全消除该时间间隔。

在 Broker 之间同步所需的时间会随对象（例如 VDA、应用程序、组）数增加。例如，同步 5000 个 VDA 可能需要 10 分钟或更

© 1999-2017 Citrix Systems, Inc. All rights reserved.

长时间来完成。请参阅下文的“监视”一节，了解有关事件日志中的同步条目的信息

管理本地主机缓存

SQL Server Express LocalDB

在安装 Controller 或从低于 7.9 的版本升级 Controller 时，会自动安装本地主机缓存使用的 Microsoft SQL Server Express LocalDB。不需要对 LocalDB 执行管理员维护操作。仅辅助 Broker 与此数据库通信；不能使用 PowerShell cmdlet 更改有关此数据库的任何内容。LocalDB 不能在多个 Controller 之间共享。

无论是否启用本地主机缓存，都会安装 SQL Server Express LocalDB 数据库软件。

> 要阻止其安装，请使用 XenDesktopServerSetup.exe 命令安装或升级 Controller，并包含 /exclude "Local Host Cache Storage (LocalDB)" 选项。但是，请注意，没有数据库时，无法使用本地主机缓存功能，并且不能将不同的数据库用于辅助 Broker。

注意：安装此 LocalDB 数据库对您是否安装 SQL Server Express 以用作站点数据库没有影响。

安装和升级 XenApp 或 XenDesktop 后的默认设置

全新安装 XenApp 和 XenDesktop 的过程中，默认启用本地主机缓存。（连接租用默认处于禁用状态。）

升级后，本地主机缓存设置保持不变。例如，如果本地主机缓存在早期版本中处于启用状态，在升级后的版本中也会保持启用状态。如果本地主机缓存在早期版本中处于禁用状态（或不受支持），在升级后的版本中也会保持禁用状态。

启用和禁用本地主机缓存

要启用本地主机缓存，请输入：

> **Set-BrokerSite -LocalHostCacheEnabled $true -ConnectionLeasingEnabled $false**

此 cmdlet 还禁用连接租用功能。请勿启用本地主机缓存和连接租用。

要确定是否已启用本地主机缓存，请输入：

> **Get-BrokerSite**

检查 LocalHostCacheEnabled 属性是否为 True 以及 ConnectionLeasingEnabled 属性是否为 False。

要禁用本地主机缓存（和启用连接租用），请输入：

> **Set-BrokerSite -LocalHostCacheEnabled $false -ConnectionLeasingEnabled $true**

强制中断

您可能希望有意强制数据库中断。

- 如果您的网络反复开启和关闭。在网络问题解决之前强制中断可以防止持续在正常模式和中断模式之间转换。
- 要测试灾难恢复计划。
- 更换或维修站点数据库服务器时。

要强制中断，请编辑包含 Delivery Controller 的每个服务器的注册表。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 在 HKLM\Software\Citrix\DesktopServer\LHC 中，将 OutageModeForced 设置为 1。这指示 Broker 进入中断模式，无论数据库的状态是什么。（将该值设置为 0 将使服务器退出中断模式。）
- 在 Citrix Cloud 场景中，连接器进入中断模式，无论与控制平面或主要区域的连接的状态是什么。

监视

事件日志记录何时发生同步和中断。

Config Synchronizer Service

正常操作过程中，CSS 通过使用 High Availability Service（辅助 Broker）复制并导出 Broker 配置，然后将其导入 LocalDB 时，会发生以下事件。

- 503：发现主 Broker 配置有更改，且正在开始导入。
- 504：已将 Broker 配置复制、导出并成功导入 LocalDB。
- 505：导入 LocalDB 失败；请参阅下文了解详细信息。

High Availability Service

- 3502：发生了中断，辅助 Broker (High Availability Service) 正在执行代理操作。
- 3503：已解决中断并已恢复正常操作。
- 3504：指示选择哪个辅助 Broker，以及参与选择的其他 Broker。

故障排除

向 LocalDB 的同步导入失败且发布了 505 事件时，可以使用多个故障排除工具。

CDF 跟踪：包含用于 ConfigSyncServer 模块和 BrokerLHC 模块的选项。那些选项与其他 Broker 模块一起可能会确定问题。

报告：可以生成并提供详细记录故障点的报告。此报告功能影响同步速度，因此，Citrix 建议在不使用时禁用它。

要启用并生成 CSS 跟踪报告，请输入：

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -PropertyType DWORD -Value 1
```

HTML 报告发布在 C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.htmll

生成报告后，禁用报告功能：

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```

报告 Broker 配置：提供准确的配置以用于调试目的。

```
Export-BrokerConfiguration | Out-File < file-pathname>
```

例如，Export-BrokerConfiguration | Out-File C:\BrokerConfig.xml。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

连接租用

Dec 05, 2017

重要：本地主机缓存 (LHC) 是首选的 XenApp 和 XenDesktop 高可用性解决方案，而不是连接租用。有关详细信息，请参阅本地主机缓存。

- 在版本中，XenApp 和 XenDesktop 的全新安装过程中，连接租用默认处于禁用状态。
- 自本 XenApp 和 XenDesktop 7.15 长期服务版本之后的当前版本起，不再提供连接租用。

为确保站点数据库始终可用，Citrix 建议按照 Microsoft 的高可用性最佳做法开始部署容错 SQL Server。但是，网络问题和中断可能会阻止 Delivery Controller 访问数据库，从而使用户无法连接到其应用程序或桌面。

通过连接租用功能，用户可以连接以及重新连接到其最近使用的应用程序和桌面，即使在站点数据库不可用时也能连接，补充了 SQL Server 高可用性最佳做法。

即使用户可以获得大量的已发布资源，但他们通常只使用其中的一小部分。启用连接租用后，在正常操作期间，每个 Controller 都会缓存用户最近使用的应用程序和桌面的连接（前提是数据库可用）。

在每个 Controller 上生成的租用将上载到站点数据库，以便定期同步到站点上的其他 Controller。除了租用外，每个 Controller 的缓存还会保存应用程序、桌面、图标和工作进程信息。租用及相关信息存储在每个 Controller 的本地磁盘上。如果数据库变为不可用，Controller 将进入租用连接模式，并在用户尝试从 StoreFront 连接或重新连接到最近使用的应用程序或桌面时“重播”缓存的操作。

连接会缓存为期两周的租用期。因此，如果数据库变为不可用，仍可通过 StoreFront 对用户在前两周启动的桌面和应用程序进行访问。但是，如果桌面和应用程序在上一个为期两周的租用期内未启动，则当数据库不可用时，无法对其进行访问。例如，如果某个应用程序上次是在三周前启动的，而其租用期已过，若数据库现在变为不可用，则无法启动该应用程序。对于长时间处于活动状态或者已断开连接的应用程序或桌面会话，请延长其租用期限，以便不将其视为过期。

默认情况下，连接租用会影响整个站点；但是，可以撤消特定用户的所有租用，从而阻止其在 Controller 处于租用连接模式时访问任何应用程序或桌面。可以在 Controller 的基础上应用其他几项注册表设置。

注意事项和限制

虽然连接租用可以提高连接恢复能力和用户工作效率，但需要注意与其他功能的可用性、操作和性能相关的事项。

服务器托管的应用程序和桌面以及静态（已分配）桌面支持连接租用；数据库不可用时，池 VDI 桌面或未分配桌面的用户不支持连接租用。

Controller 处于租用连接模式时：

- 管理员不能使用 Studio、Director 或 PowerShell 控制台。
- 工作区控制不可用。用户登录 Citrix Receiver 时，会话不会自动重新连接，用户必须重新启动应用程序。
- 如果在数据库不可用后立即创建新租用，但租用信息尚未在所有 Controller 中进行同步，则在数据库变为不可用后用户可能无法启动该资源。
- 服务器托管的应用程序和桌面用户使用的会话数可能会超过所配置的会话限制。例如：
  - Controller 未处于租用连接模式时，用户从一台设备（通过 NetScaler Gateway 在外部连接）启动会话，而在 Controller 处于租用连接模式时，从 LAN 上的另一台设备进行连接，这种情况下，该会话可能不会漫游。
  - 如果应用程序恰好在数据库变为不可用之前启动，重新连接会话可能会失败；在这种情况下，将启动新的会话和应用程序实例。
- 静态（已分配）桌面的电源无法管理。如果 Controller 进入租用连接模式后 VDA 关闭电源，则在恢复数据库连接之

© 1999-2017 Citrix Systems, Inc. All rights reserved.

前，VDA 一直不可用，除非管理员手动打开 VDA 电源。

- 如果启用了会话预启动和会话延迟功能，则新的预启动会话将不会启动。根据配置的阈值，当数据库不可用时，预启动的会话和延迟会话将不会结束。
- 站点内的负载管理可能会受到影响。基于服务器的连接将路由到最近使用的 VDA。负载评估器（尤其是会话计数规则）可能会超额。
- 如果使用 SQL Server Management Studio 使数据库进入脱机状态，Controller 将不会进入租用连接模式。相反，应使用以下一种 Transact-SQL 语句：
  - ALTER DATABASE <database-name> SET OFFLINE WITH ROLLBACK IMMEDIATE
  - ALTER DATABASE <database-name> SET OFFLINE WITH ROLLBACK AFTER <seconds>

  两个语句均会取消任何挂起的事务，并导致 Controller 丢失与数据库的连接。然后，Controller 进入租用连接模式。

启用连接租用时，在两个短暂时间间隔内用户无法进行连接或重新连接：(1) 从数据库变为不可用到 Controller 进入租用连接模式；(2) 从 Controller 退出租用连接模式到数据库访问完全恢复并且已重新注册 VDA。

如果配置了非默认会话漫游值，则当 Controller 进入租用连接模式时，会话重新连接将还原为其默认值。有关详细信息，请参阅连接租用和会话漫游。

有关保留连接租用数据的位置的相关信息，请参阅区域一文。

有关更多注意事项，请参阅 XenDesktop 7.6 连接租用设计注意事项。

配置和部署

将部署配置为接受连接租用时：

- VDA 的版本至少为 7.6，使用这些计算机的计算机目录以及交付组必须满足这一最低要求（或使用受支持的更高版本）。
- 站点数据库大小的要求将会增加。
- 每个 Controller 都需要使用额外的磁盘空间来保存缓存的租用文件。

可以通过 PowerShell SDK 或 Windows 注册表启用或禁用连接租用。通过 PowerShell SDK，还可以删除当前租用。以下 PowerShell cmdlet 影响连接租用；有关详细信息，请参阅 cmdlet 帮助。

- Set-BrokerSite -ConnectionLeasingEnabled $true | $false - 启用或禁用连接租用。默认值 = $true
- Get-BrokerServiceAddedCapability - 输出本地 Controller 的“ConnectionLeasing”。
- Get-BrokerLease - 检索所有当前租用或过滤的租用集合。
- Remove-BrokerLease - 将一个租用或过滤的租用集合标记为删除。
- Update-BrokerLocalLeaseCache – 更新本地 Controller 上的连接租用缓存。这些数据将在下次同步时重新同步。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

虚拟 IP 和虚拟环回

Dec 05, 2017

注意：这些功能仅适用于受支持的 Windows 服务器计算机。不适用于 Windows 桌面操作系统计算机。

Microsoft 虚拟 IP 地址功能为每个会话的已发布应用程序提供动态分配的唯一 IP 地址。借助 Citrix 虚拟环回功能，可以将依赖于与 localhost（默认为 127.0.0.1）通信的应用程序配置为使用 localhost 范围 (127.*) 之内的唯一虚拟环回地址。

一些应用程序（例如 CRM 和计算机电话集成 (CTI)）将 IP 地址用于寻址、许可、身份验证或其他目的，因此，这些应用程序在会话中需要使用唯一的 IP 地址或环回地址。其他应用程序可能绑定到某个静态端口，因此，在多用户环境中尝试启动应用程序的其他实例将失败，因为该端口已在使用中。要使这些应用程序能够在 XenApp 环境中正常运行，需要为每个设备设置唯一的 IP 地址。

虚拟 IP 和虚拟环回是两个独立的功能。可以使用其中一项功能，也可以同时使用两项功能。

管理员操作摘要：

- 要使用 Microsoft 虚拟 IP，请在 Windows 服务器上启用并配置此功能。（不需要 Citrix 策略设置。）
- 要使用 Citrix 虚拟环回，请在 Citrix 策略中配置两项设置。

虚拟 IP

在 Windows 服务器上启用并配置虚拟 IP 后，会话中运行的每个已配置应用程序显示为具有唯一的地址。 用户可以在 XenApp 服务器上访问这些应用程序，访问方式与访问任何其他已发布应用程序的方式相同。 进程在以下情况下需要虚拟 IP：

- 进程使用硬编码的 TCP 端口号
- 进程使用 Windows 套接字并需要唯一 IP 地址或指定的 TCP 端口号

确定应用程序是否需要使用虚拟 IP 地址：

1. 获得 Microsoft 提供的 TCPView 工具。 此工具可以列出所有绑定特定 IP 地址和端口的应用程序。
2. 禁用“解析 IP 地址”功能，这样您看到的将是地址而不是主机名。
3. 启动应用程序，然后使用 TCPView 查看该应用程序打开了哪些 IP 地址和端口以及哪些进程名称正在打开这些端口。
4. 配置任何打开服务器的 IP 地址（0.0.0.0 或 127.0.0.1）的进程。
5. 为确保应用程序不会在其他端口上打开相同的 IP 地址，请启动该应用程序的另一个实例。

Microsoft 远程桌面 (RD) IP 虚拟化的工作方式

- 必须在 Microsoft 服务器上启用虚拟 IP 寻址。
  例如， 在 Windows Server 2008 R2 环境中，从服务器管理器， 展开“远程桌面服务”>“RD 会话主机连接”以启用 RD IP 虚拟化功能， 并配置设置以使用动态主机配置协议 (DHCP) 服务器 基于每个会话或每个程序动态分配 IP 地址。 请参阅 Microsoft 文档以了解相关说明。

- 启用此功能后，服务器将在会话启动时从 DHCP 服务器请求动态分配的 IP 地址。
- RD IP 虚拟化功能在每会话或每程序基础上将 IP 地址分配给远程桌面连接。 如果为多个程序分配 IP 地址，它们将共享每会话 IP 地址。
- 将地址分配给会话后，该会话将在进行以下调用时使用虚拟地址，而不是系统的主 IP 地址：bind、closesocket、connect、WSAConnect、WSAAccept、getpeername、getsockname、sendto、WSASendTo、WSASocketW、gethostbyaddr、getnameinfo 和 getaddrinfo

在“远程桌面”会话托管配置中使用 Microsoft IP 虚拟化功能时，在应用程序和 Winsock 函数调用之间插入“过滤器”组件，可将该应用程序绑定到特定的 IP 地址。 然后，应用程序只能看到自己应该使用的 IP 地址。 该应用程序对侦听 TCP 或 UDP 通信的任何尝试都会自动绑定到其分配的虚拟 IP 地址（或环回地址），并且该应用程序打开的任何原始连接都源自绑定到该应用程序的 IP 地址。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

在返回地址的函数（如 GetAddrInfo()，由 Windows 策略控制）中，如果请求本地主机 IP 地址，则虚拟 IP 将查看返回的 IP 地址并将其更改为会话的虚拟 IP 地址。 尝试通过此类名称函数获得本地服务器 IP 地址的应用程序，仅会看到分配给该会话的唯一虚拟 IP 地址。 此 IP 地址通常用于后续套接字调用，如 bind 或 connect。

通常，应用程序会请求绑定到一个端口以侦听地址 0.0.0.0。 如果应用程序发出此请求并使用静态端口，您无法启动该应用程序的多个实例。 虚拟 IP 地址功能也会在这些类型的调用中查找 0.0.0.0，然后将调用更改为侦听特定虚拟 IP 地址。这样一来，多个应用程序便可侦听同一台计算机上的同一端口，因为这些应用程序侦听的地址是各不相同的。 仅当调用在 ICA 会话中进行并且虚拟 IP 地址功能处于启用状态时，才可以更改调用。 例如，如果在不同会话中运行的应用程序的两个实例同时尝试绑定到所有接口 (0.0.0.0) 和特定端口（例如 9000），它们将分别绑定到 VIPAddress1:9000 和 VIPAddress2:9000，因而不会发生冲突。

虚拟环回

启用 Citrix 虚拟 IP 环回策略设置后，每个会话都可以拥有自己的通信用虚拟环回地址。如果应用程序在 Winsock 调用中使用本地主机地址（默认设置为 127.0.0.1），则虚拟环回功能只需将 127.0.0.1 替换为 127.X.X.X，其中 X.X.X 表示会话 ID + 1。例如，会话 ID 为 7 的地址是 127.0.0.8。万一会话 ID 超过第四个八位字节（大于 255），地址将滚动到下一个八位字节 (127.0.1.0)，直至达到最大值 127.255.255.255。

进程在以下情况下需要虚拟环回：

- 进程使用 Windows 套接字环回 (localhost) 地址 (127.0.0.1)
- 进程使用硬编码的 TCP 端口号

将虚拟环回策略设置应用于使用环回地址进行进程间通信的应用程序。无需执行其他配置。虚拟环回独立于虚拟 IP，因此无需配置 Microsoft 服务器。

- 虚拟 IP 环回支持。启用后，此策略设置允许每个会话有其自己的虚拟环回地址。默认情况下，禁用此设置。此功能仅适用于虚拟 IP 虚拟环回程序列表策略设置指定的应用程序。
- 虚拟 IP 虚拟环回程序列表。此策略设置指定使用虚拟 IP 环回功能的应用程序。此设置仅在启用了虚拟 IP 环回支持策略设置时有效。

相关功能

可以使用以下注册表设置来确保虚拟环回的优先级高于虚拟 IP；这称为环回优先。但是，操作时请注意以下事项：

- 首选环回仅在 Windows Server 2008 R2 和 Windows Server 2012 R2 中受支持。
- 仅在同时启用了虚拟 IP 和虚拟环回的情况下使用环回优先；否则可能会导致意外结果。
- 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。

在应用程序所在的服务器运行注册表。

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP（对于 32 位计算机为 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VIP）
- 名称：PreferLoopback，类型：REG_DWORD，数据：1
- 名称：PreferLoopbackProcesses，类型：REG_MULTI_SZ，数据：<list of processes>

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Delivery Controller

Dec 05, 2017

Delivery Controller 是负责管理用户访问的服务器端组件，它还负责代理和优化连接。Controller 还提供用于创建桌面和服务器映像的 Machine Creation Services。

站点必须至少有一个 Controller。安装首个 Controller 后，可以在创建站点时或创建站点后添加更多 Controller。在一个站点中安装多个 Controller 有两大主要优势。

- 冗余性：生产站点应始终确保至少拥有两个位于不同物理服务器上的 Controller，这是最佳做法。如果一个 Controller 出现故障，其他的 Controller 可以管理连接和站点。
- 可扩展性：随着站点活动的增加，Controller 上的 CPU 使用率将提高，数据库活动也会增加。更多的 Controller 可以处理更多用户以及更多的应用程序和桌面请求，并且可以提升整体响应能力。

每个 Controller 直接与站点数据库通信。在包含多个区域的站点中，每个区域中的 Controller 与主区域中的站点数据库通信。

重要：请勿在配置站点后更改 Controller 的计算机名称或域成员关系。

VDA 如何向 Controller 注册

VDA 必须首先向站点的 Delivery Controller 注册（建立连接），然后该 VDA 才可以使用。有关 VDA 注册的信息，请参阅向 Controller 注册 VDA。

（在早期 XenApp 和 XenDesktop 7.x 版本的文档中，有关 VDA 注册的信息包括在本文中。这些信息已增多，现在位于上面链接的文章中。）

添加、删除或移动 Controller

要添加、移动或删除 Controller，必须具有*数据库*一文中列出的服务器角色和数据库角色权限。

注意：在 SQL 群集或 SQL 镜像安装中，不支持在节点上安装 Controller。

如果您的部署使用数据库镜像：

- 在添加、删除或移动 Controller 之前，请确保主体数据库和镜像数据库均处于运行状态。另外，如果您通过 SQL Server Management Studio 使用脚本，请在执行脚本之前启用 SQLCMD 模式。
- 要在添加、删除或移动 Controller 后验证镜像，请运行 PowerShell **get-configdbconnection** cmdlet，以确保在镜像的连接字符串中设置了 Failover Partner 的值。

在添加、删除或移动 Controller 后：

- 如果已启用自动更新，VDA 将在 90 分钟内接收已更新的 Controller 列表。
- 如果未启用自动更新，请确保更新了所有 VDA 的 Controller 策略设置或 ListOfDDCs 注册表项。将 Controller 移至其他站点后，更新两个站点上的策略设置或注册表项。

添加 Controller

可以在创建站点时或创建站点后添加 Controller。无法将安装了旧版软件的 Controller 添加到使用此版本创建的站点中。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. 在使用受支持操作系统的服务器上运行安装程序。安装 Delivery Controller 组件和所需的任何其他核心组件。完成安装向导。
2. 如果尚未创建站点，请启动 Studio；系统会提示您创建一个站点。在站点创建向导的“数据库”页面上，单击“选择”按钮，然后添加已安装其他 Controller 的服务器的地址。**重要：**如果计划生成将初始化数据库的脚本，请在生成脚本前添加 Controller。
3. 如果已经创建站点，请将 Studio 指向已安装其他 Controller 的服务器。单击**扩展部署**并输入站点地址。

删除 Controller

从站点删除 Controller 时，不会卸载 Citrix 软件或任何其他组件；会从数据库中删除 Controller，这样它将再也无法用于代理连接和执行其他任务。如果删除 Controller，您可以稍后将其添回到同一个站点中或添加到其他站点中。一个站点至少需要一个 Controller，因此无法删除 Studio 中列出的最后一个 Controller。

从站点中删除 Controller 时，不会删除登录数据库服务器时使用的 Controller 登录信息。这样可以避免删除同一计算机上由其他产品的服务所使用的登录信息的可能性。如果不再需要，则必须手动删除登录信息；需要具有 securityadmin 服务器角色权限才能删除登录信息。

重要：请先将 Controller 从站点中删除，然后再将其从 Active Directory 中删除。

1. 确保打开 Controller 的电源，以使 Studio 能够在一小时内加载。Studio 加载要删除的 Controller 时，请在系统提示您关闭 Controller 的电源时执行此操作。
2. 在 Studio 导航窗格中选择**配置 > Controller**，然后选择要删除的 Controller。
3. 在“操作”窗格中单击**删除 Controller**。如果没有正确的数据库角色和权限，可以选择生成一个脚本，数据库管理员可以通过该脚本为您删除 Controller。
4. 您可能需要从数据库服务器中删除 Controller 的计算机帐户。在执行此操作之前，请检查是否有其他服务在使用该帐户。

使用 Studio 删除 Controller 之后，该 Controller 的流量可能会出现短时间的延迟，以确保当前任务正常完成。如果要在极短的时间内删除 Controller，Citrix 建议在服务器的安装位置将其关闭，或从 Active Directory 中删除该服务器。然后在该站点上重新启动其他 Controller，确保不再与删除的 Controller 进一步通信。

将 Controller 移至其他区域

如果站点包含多个区域，可以将 Controller 移至其他区域。有关此操作对 VDA 注册和其他操作的影响，请参阅*区域*一文。

1. 在 Studio 导航窗格中选择**配置 > Controller**，然后选择要移动的 Controller。
2. 在“操作”窗格中选择**移动**。
3. 指定要移动 Controller 的区域。

将 Controller 移至其他站点

无法将 Controller 移至使用此软件的早期版本创建的站点。

1. 在 Controller 当前所在的站点（旧站点）上，从 Studio 导航窗格中选择**配置 > Controller**，然后选择要移动的 Controller。
2. 在“操作”窗格中单击**删除 Controller**。如果您没有相应的数据库角色和权限，可以选择生成一个脚本，以允许具有这些权限的人员（如数据库管理员）为您删除 Controller。一个站点至少需要一个 Controller，因此无法删除 Studio 中列出的最后一个 Controller。
3. 在要移动的 Controller 上，打开 Studio，出现相应提示时重置服务，然后选择**加入现有站点**，并输入新站点的地址。

将 VDA 移至另一个站点

如果 VDA 是使用 Provisioning Services 置备的或者 VDA 是现有映像，您可以在升级时或者将在测试站点中创建的 VDA 映像移至生产站点时将 VDA 移至另一个站点（从站点 1 移至站点 2）。无法将使用 Machine Creation Services (MCS) 置备的 VDA 从

© 1999-2017 Citrix Systems, Inc. All rights reserved.

一个站点移至另一个站点，因为 MCS 不支持更改 ListOfDDCs（一项 VDA 检查）以在 Controller 中注册；使用 MCS 置备的 VDA 始终检查与在其中创建了该 VDA 的站点关联的 ListOfDDCs。

可以通过以下两种方式将 VDA 移至另一个站点：使用安装程序或 Citrix 策略。

安装程序：运行安装程序并添加 Controller，在站点 2 中为控制器指定 FQDN（DNS 项）。**重要**：仅当未使用 Controller 策略设置时，才在安装程序中指定 Controller。

组策略编辑器：以下是在站点之间移动多个 VDA 的示例。

1. 在站点 1 中创建包含以下设置的策略，然后过滤此策略至交付组级别，以在站点间发起分阶段的 VDA 迁移。
   控制器 – 包含站点 2 中一个或多个控制器的 FQDN（DNS 条目）。
   启用控制器自动更新 – 已设置为禁用。
2. 在新策略创建 90 分钟内，交付组中的每个 VDA 都将收到警告。VDA 将忽略其收到的控制器列表（因为自动更新已禁用）；它会选择在策略（其列出了站点 2 中的控制器）中指定的一个控制器。
3. 当 VDA 在站点 2 的控制器中成功注册后，它将接收站点 2 的 ListOfDDCs 和策略信息，默认情况下，自动更新功能已启用。由于 VDA 在站点 1 中注册的控制器不在站点 2 控制器所发送的列表上，因此，VDA 将从站点 2 列表中选择控制器并重新注册。从此时开始，VDA 会从站点 2 中自动更新信息。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDA 注册

Jan 02, 2018

简介

VDA 必须先向站点中的一个或多个 Controller 或 Cloud Connector 注册（建立连接），然后该 VDA 才可以使用。（在本地 XenApp 和 XenDesktop 部署中，VDA 在 Controller 中注册。在 XenApp 和 XenDesktop 服务部署中，VDA 在 Cloud Connector 中注册。）VDA 通过检查名为 ListofDDCs 的列表来查找 Controller 或 Connector。VDA 上的 ListOfDDCs 包含将该 VDA 指向站点中的 Controller 或 Cloud Connector 的 DNS 条目。为实现负载平衡，VDA 会自动在列表中的所有 Controller 或 Cloud Connector 之间分发连接。

为什么 VDA 注册如此重要？

- 从安全角度而言，注册是一种敏感操作：您将在 Controller 或 Cloud Connector 与 VDA 之间建立连接。对于此类敏感操作，如果所有情况未达到良好状态，预期行为是拒绝连接。您将有效地建立两个单独的通信通道：VDA 至 Controller 或 Cloud Connector 和 Controller 或 Cloud Connector 至 VDA。连接使用 Kerberos，因此不允许存在时间同步和域成员身份问题。Kerberos 使用服务主体名称 (SPN)，因此您不能使用负载平衡的 IP\主机名。
- 添加和删除 Controller 或 Cloud Connector 后，如果 VDA 没有准确的 Controller 或 Cloud Connector 最新信息，VDA 可能会拒绝未列出的 Controller 或 Cloud Connector 代理的会话启动。无效的项会使虚拟桌面系统软件的启动发生延迟。VDA 不会接受来自未知的不可信 Controller 或 Cloud Connector 的连接。

除了 ListOfDDCs 外，还有 ListOfSIDs（安全 ID）指示信任 ListOfDDCs 中的哪些计算机。ListOfSIDs 可用于降低 Active Directory 上的负载或避免来自受感染 DNS 服务器的潜在安全威胁。有关详细信息，请参阅下面的 *ListOfSIDs*。

如果 ListOfDDCs 指定多个 Controller 或 Cloud Connector，VDA 将尝试以随机顺序连接这些 Controller 或 Cloud Connector。在本地部署中，ListOfDDCs 还可以包含 Controller 组。VDA 将尝试连接组中的每个 Controller，然后转向 ListOfDDCs 中的其他项。

XenApp 和 XenDesktop 会在 VDA 安装期间自动测试与配置的 Controller 或 Cloud Connector 的连接。如果无法访问 Controller 或 Cloud Connector，会显示错误。如果您忽略无法访问 Controller 或 Cloud Connector 的警告（或者在 VDA 安装期间您不指定 Controller 或 Cloud Connector 地址时），系统会显示消息提醒您。

Controller 或 Cloud Connector 地址配置方法

管理员将选择 VDA 首次注册时使用的配置方法。（这称为首次注册。）在首次注册期间，会在 VDA 上创建永久性缓存。在后续注册期间，除非检测到配置更改，否则 VDA 将从此本地缓存中检索 Controller 或 Cloud Connector 列表。

在后续注册期间检索该列表的最简单的方法是使用自动更新功能。默认情况下启用自动更新。有关详细信息，请参阅”自动更新“。

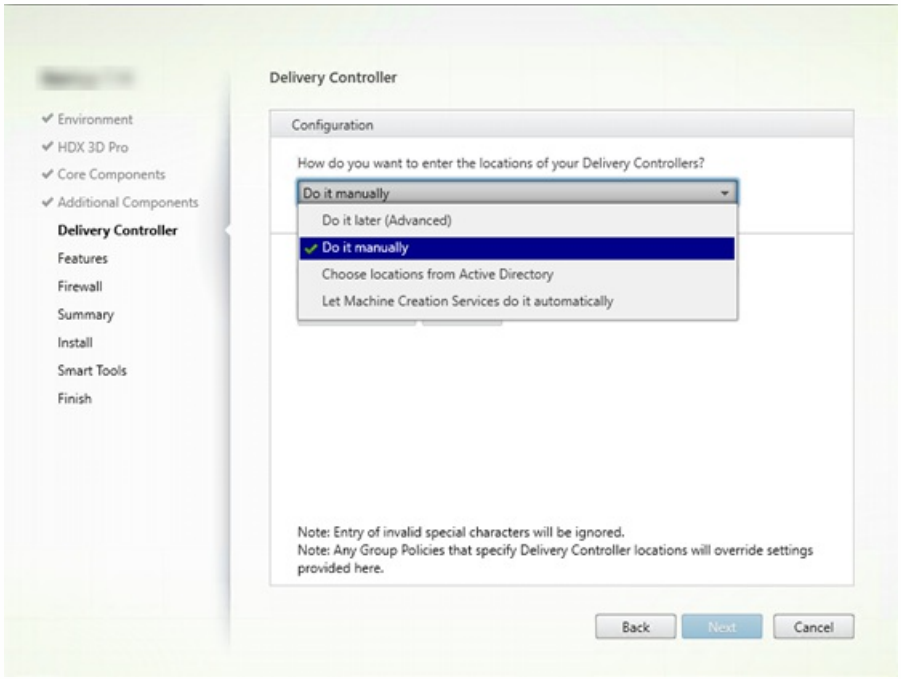
在 VDA 上配置 Controller 或 Cloud Connector 地址的方法有多种。

- 基于策略（LGPO 或 GPO）
- 基于注册表（手动、GPP、在 VDA 安装期间指定）
- 基于 Active Directory OU（旧 OU 发现）
- 基于 MCS (personality.ini)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

首次注册方法在安装 VDA 时指定。（如果禁用自动更新，则在 VDA 安装期间选择的方法也将用于后续注册。）

下图显示了 VDA 安装向导的 **Delivery Controller** 页面。



基于策略 (LGPO\GPO)

Citrix 建议 VDA 首次注册时使用 GPO。它的优先级最高。（上面列出的自动更新的优先级最高，但仅在首次注册之后使用自动更新。）基于策略的注册具有使用组策略进行配置的集中优势。

要指定此方法，请完成以下两个步骤：

- 在 VDA 安装向导中的 **Delivery Controller** 页面上，选择**以后(高级)**。该向导会多次提醒您指定 Controller 地址，即使您在 VDA 安装期间不指定它们也是如此。（因为 VDA 注册如此重要！）
- 可以在“Virtual Delivery Agent 设置”>“控制器”设置中通过 Citrix 策略启用或禁用基于策略的 VDA 注册。（如果安全性的优先级最高，请使用“Virtual Delivery Agent 设置”>“控制器 SID”设置。）

  此设置存储在 HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs) 下面。

基于注册表

要指定此方法，请完成以下步骤之一：

- 在 VDA 安装向导中的 **Delivery Controller** 页面上，选择**手动操作**。然后输入所安装 Controller 的 FQDN，并单击**添加**。如果您已安装其他 Controller，请添加其地址。
- 对于命令行 VDA 安装，请使用 /controllers 选项并指定所安装 Controller 或 Cloud Connector 的 FQDN。

此信息通常存储在注册表项 HKLM\Software\Citrix\VirtualDesktopAgent 或 HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent 下面的注册表值 ListOfDDCs 中。

还可以手动配置此注册表项或使用组策略首选项 (GPP)。此方法可能优于基于策略的方法（例如，如果您要对不同的 Controller 或 Cloud Connector 进行有条件的处理，如：对名称以 XDW-001- 开头的计算机使用 XDC-001）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

更新 ListOfDDCs 注册表项，该注册表项用于列出站点中所有 Controller 或 Cloud Connector 的 FQDN。（此注册表项相当于 Active Directory 站点 OU。）

HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)

如果注册表位置 HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent 包括 ListOfDDCs 和 FarmGUID 两个注册表项，则 ListOfDDCs 用于 Controller 或 Cloud Connector 发现。如果在 VDA 安装期间指定站点 OU，则存在 FarmGUID。（这可能用于旧部署中。）

（可选）更新 ListOfSIDs 注册表项（有关详细信息，请参阅下面的 *ListOfSIDs*）：

HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)

谨记：如果您还通过 Citrix 策略启用基于策略的 VDA 注册，则该配置会覆盖您在 VDA 安装期间指定的设置，因为该方法的优先级更高。

基于 Active Directory OU（旧）

支持此方法主要是为了向后兼容，建议不要使用此方法。如果您仍在使用此方法，Citrix 建议改为其他方法。

要指定此方法，请完成以下两个步骤：

- 在 VDA 安装向导中的 **Delivery Controller** 页面上，选择**从 Active Directory 中选择位置。**
- 使用 Set-ADControllerDiscovery.ps1 脚本（在每个 Controller 上都可用）。此外，在每个 VDA 上配置 FarmGuid 注册表项以指向正确的 OU。可以使用组策略配置此设置。

有关更多详细信息，请参阅基于 Active Directory OU 的发现。

基于 MCS

如果您计划只使用 MCS 来置备 VM，可以指示 MCS 设置 Controller 或 Cloud Connector 列表。此功能适用于自动更新：在首次置备期间（创建计算机目录时），MCS 将 Controller 或 Cloud Connector 列表填入 Personality.ini 文件中。自动更新会使该列表保持最新。

建议不要将此方法用于大型环境中。在下列情况下，可以使用此方法：

- 小型环境
- 不会在站点之间移动 VDA
- 只使用 MCS 置备 VM
- 您不想使用组策略

要指定此方法，请执行以下操作：

- 在 VDA 安装向导中的 **Delivery Controller** 页面上，选择 **Let Machine Creation Services do it**（让 Machine Creation Services 完成）。

建议

最佳做法：

- 首次注册时使用组策略注册方法。
- 使用自动更新（默认情况下启用）使 Controller 列表保持最新。
- 在多区域部署中，首次配置时使用组策略（至少有两个 Controller 或 Cloud Connector）。将 VDA 指向其区域中的本地

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Controller 或 Cloud Connector。使用自动更新使其保持最新。自动更新会自动优化卫星区域中 VDA 的 ListOfDDCs。

自动更新

默认情况下启用自动更新（在 XenApp 和 XenDesktop 7.6 中引入）。这是使 VDA 注册保持最新的最有效方法。尽管首次注册时不使用自动更新，但在首次注册时，自动更新软件会下载 ListOfDDCs 并将其存储在 VDA 上的永久性缓存中。对每个 VDA 都会执行此操作。（此缓存中还保存计算机策略信息，这样可以确保在重新启动后保留策略设置。）

使用 MCS 或 PVS 置备计算机时支持自动更新，但 PVS 服务器端缓存除外（这不是常见场景，因为自动更新缓存没有对应的静态存储）。

要指定此方法，请执行以下操作：

- 通过包含该设置的 Citrix 策略启用或禁用：Virtual Delivery Agent 设置 > 启用控制器自动更新。默认情况下启用此设置。

工作原理：

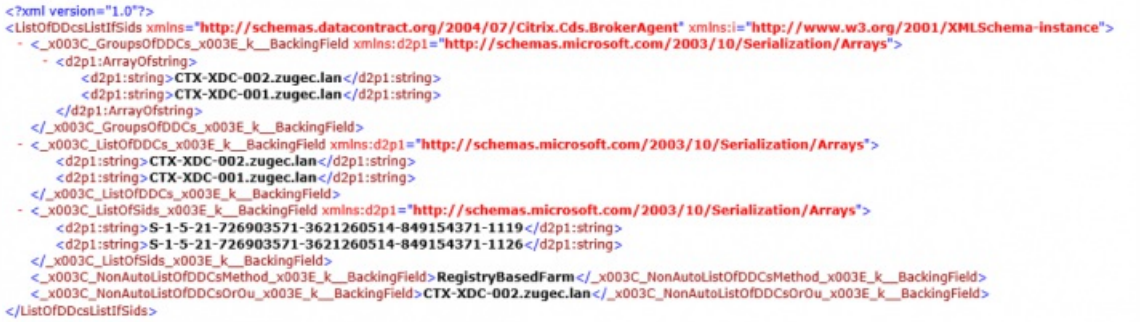
- 每次 VDA 重新注册时（例如，重新启动计算机后），都会更新缓存。此外，每个 Controller 或 Cloud Connector 每 90 分钟检查一次站点数据库。如果自上次检查后添加或删除了 Controller 或 Cloud Connector，或者如果发生了影响 VDA 注册的策略更改，Controller 或 Cloud Connector 会向其注册的 VDA 发送更新列表，并更新缓存。VDA 接受来自其最新缓存列表中所有 Controller 或 Cloud Connector 的连接。
- 如果 VDA 接收的列表不包括其注册的 Controller 或 Cloud Connector（即，已从站点中删除该 Controller 或 Cloud Connector），VDA 将从 ListOfDDCs 中选择 Controller 或 Cloud Connector 并重新注册。

例如：

- 某个部署包含三个 Controller： A、B 和 C。VDA 向 Controller B 注册（该 Controller 在 VDA 安装期间指定）。
- 之后，将 D 和 E 两个 Controller 添加到站点中。在 90 分钟内，VDA 收到更新的列表，然后接受来自 Controller A、B、C、D 和 E 的连接。（在重新启动 VDA 之前，负载不会平均分布到所有 Controller。）
- 再之后，Controller B 移至另一个站点。在 90 分钟内，原始站点中的 VDA 收到更新的列表，因为自上次检查后 Controller 已发生更改。最初已向 Controller B 注册的 VDA（该 Controller 已不在列表中）将从当前列表（A、C、D 和 E）中选择 Controller 并重新注册。

在一个多区域部署中，卫星区域中的自动更新会先自动缓存所有本地 Controller。主要区域中的所有 Controller 都缓存在备份组中。如果卫星区域中无本地 Controller 可用，将尝试向主要区域中的 Controller 注册。

如下例所示，缓存文件包含主机名和安全 ID 列表 (ListOfSIDs)。VDA 不会查询 SID，这会降低 Active Directory 负载。



可以使用 WMI 调用来检索缓存文件；但是，它存储在只有 SYSTEM 帐户可读的位置中。重要：提供此信息只是供参考。请勿

© 1999-2017 Citrix Systems, Inc. All rights reserved.

修改此文件。如果修改此文件或文件夹，会导致配置不受支持。

```
Get-WmiObject -Namespace “Root\Citrix\DesktopInformation”
-Class “Citrix_VirtualDesktopInfo” -Property “PersistentDataLocation”
```

如果出于安全原因（不同于降低 Active Directory 负载）需要手动配置 ListOfSIDs，不能使用自动更新功能。有关详细信息，请参阅下面的 *ListOfSIDs*。

自动更新优先级例外情况

尽管通常情况下，在所有 VDA 注册方法中自动更新的优先级最高，它会覆盖其他方法的设置，仍有一个例外情况。缓存中的 NonAutoListOfDDCs 元素指定 VDA 首次配置方法。自动更新会监视此信息。如果首次注册方法更改，则注册过程会跳过自动更新，并使用配置的优先级次高的方法。将 VDA 移至另一个站点时（例如，在灾难恢复期间），这很有用。

配置注意事项

Controller 或 Cloud Connector 地址

无论使用哪种方法指定 Controller 或 Cloud Connector，Citrix 都建议使用 FQDN 地址。IP 地址并不视为可信配置，因为与 DNS 记录相比，IP 更容易受影响。如果手动填充 ListOfSIDs，可以在 ListOfDDCs 中使用 IP。但是，仍建议使用 FQDN。

负载平衡

如前所述，VDA 会自动在 ListOfDDCs 中的所有 Controller 或 Cloud Connector 之间分发连接。Citrix 代理协议 (CBP) 中内置了故障转移和负载平衡功能。如果在配置中指定多个 Controller 或 Cloud Connector，需要时，注册会自动在这些 Controller 或 Cloud Connector 之间进行故障转移。由于自动更新功能，会自动为所有 VDA 进行故障转移。

出于安全原因，不能使用网络负载平衡器（例如 NetScaler）。VDA 注册使用 Kerberos 双向身份验证，在这种验证中，客户端 (VDA) 必须向服务 (Controller) 证明其身份。但是，Controller 或 Cloud Connector 必须向 VDA 证明其身份。这意味着 VDA 和 Controller 或 Cloud Connector 同时用作服务器和客户端。如本文开头所述，有两种通信通道：VDA -> Controller/Cloud Connector 和 Controller/Cloud Connector -> VDA。

此过程中的组件称为服务主体名称 (SPN)，它作为属性存储在 Active Directory 计算机对象中。VDA 连接到 Controller 或 Cloud Connector 时，它必须指定要与“谁”通信；此地址是 SPN。如果使用负载平衡的 IP，则 Kerberos 双向身份验证会正确识别该 IP 不属于预期的 Controller 或 Cloud Connector。

有关详细信息，请参阅：

Kerberos 简介：https://blogs.technet.microsoft.com/askds/2008/03/06/kerberos-for-the-busy-admin/

使用 Kerberos 进行双向身份验证：https://msdn.microsoft.com/en-us/library/ms677600

自动更新替代 CNAME

自动更新功能替代了 XenApp 和 XenDesktop 7.x 之前版本中的 CNAME（DNS 别名）功能。从 XenApp 和 XenDesktop 7 开始，禁用 CNAME 功能。使用自动更新替代 CNAME。（如果必须使用 CNAME，请参阅 CTX137960。为了持续使用 DNS 别名，请勿同时使用自动更新和 CNAME。）

Controller/Cloud Connector 组

© 1999-2017 Citrix Systems, Inc. All rights reserved.

在有些情况下，您可能希望按组处理 Controller 或 Cloud Connector，一个组作为首选组，其他组用于在该组中所有 Controller/Cloud Connector 发生故障时进行故障转移。请记住，Controller 或 Cloud Connector 是随机从列表中选择的，因此，分组可以有助于实施优先使用。

使用括号指定 Controller/Cloud Connector 组。例如，有四个 Controller（两个主要，两个备份），分组方式可以如下：

(XDC-001.cdz.lan XDC-002.cdz.lan) (XDC-003.cdz.lan XDC-004.cdz.lan)。

在此示例中，先处理第一个组（001 和 002）中的 Controller。如果它们都发生故障，则处理第二个组中的 Controller（003 和 004）。

ListOfSIDs

VDA 可以访问以进行注册的 Controller 列表是 ListOfDDCs。VDA 还必须知道信任哪些 Controller；VDA 不会自动信任 ListOfDDCs 中的 Controller。ListOfSIDs（安全 ID）用于标识可信 Controller。VDA 将只向可信 Controller 尝试注册。

在大多数环境中，会自动基于 ListOfDDCs 生成 ListOfSIDs。可以使用 CDF 跟踪来读取 ListOfSIDs。

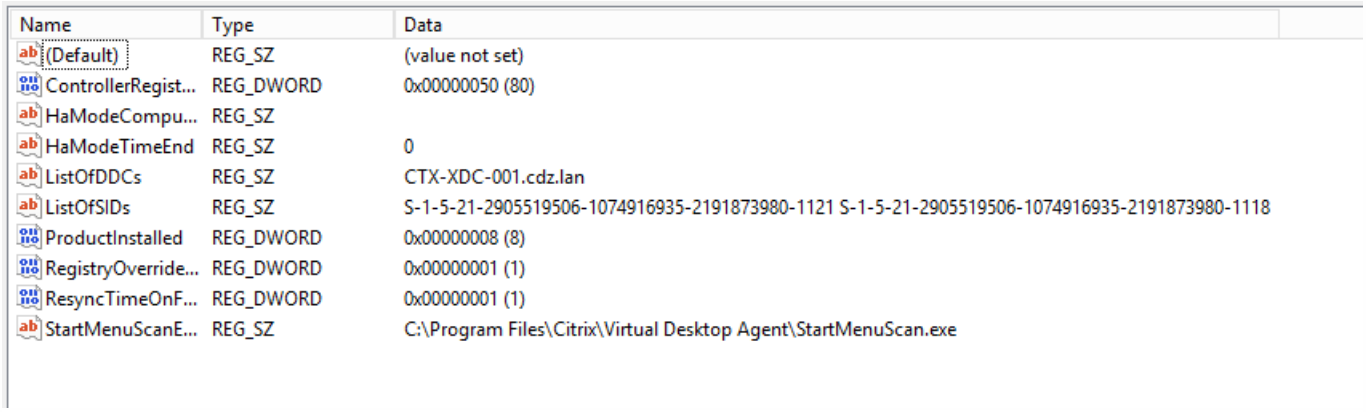
通常，无需手动修改 ListOfSIDs。存在几种例外情况。由于有了较新的技术，前两种例外情况已不存在。

- **Controller 使用单独的角色：**在 XenApp 和 XenDesktop 7.7 中引入区域之前，仅当一部分 Controller 用于注册时手动配置 ListOfSIDs。例如，如果使用 XDC-001 和 XDC-002 作为 XML Broker，使用 XDC-003 和 XDC-004 进行 VDA 注册，则在 ListOfSIDs 中指定所有 Controller，在 ListOfDDCs 中指定 XDC-003 和 XDC-004。这不是典型配置也不是建议的配置，不应在较新环境中使用。而是改用区域。
- **降低 Active Directory 负载：**在 XenApp 和 XenDesktop 7.6 中引入自动更新功能之前，使用 ListOfSIDs 来降低域控制器上的负载。通过预填充 ListOfSIDs，可以跳过从 DNS 名称到 SID 的解析。但是，有了自动更新功能后，不再需要执行此操作，因为此永久性缓存中包含 SID。Citrix 建议使自动更新功能保持启用状态。
- **安全性：**在一些受到高度保护的环境中，手动配置了可信 Controller 的 SID 以避免来自受感染 DNS 服务器的潜在安全威胁。但是，如果执行此操作，还必须禁用自动更新功能；否则将使用永久性缓存中的配置。

因此，除非有特殊原因，否则请勿修改 ListOfSIDs。

如果必须修改 ListOfSIDs，请在 HKLM\Software\Citrix\VirtualDesktopAgent 下面创建名为 ListOfSIDs (REG_SZ) 的注册表项。值为可信 SID 列表，如果有多个，用空格分隔开。

在以下示例中，一个 Controller 用于 VDA 注册 (ListOfDDCs)，两个 Controller 用于代理 (List OfSIDs)。



Name	Type	Data
(Default)	REG_SZ	(value not set)
ControllerRegist...	REG_DWORD	0x00000050 (80)
HaModeCompu...	REG_SZ	
HaModeTimeEnd	REG_SZ	0
ListOfDDCs	REG_SZ	CTX-XDC-001.cdz.lan
ListOfSIDs	REG_SZ	S-1-5-21-2905519506-1074916935-2191873980-1121 S-1-5-21-2905519506-1074916935-2191873980-1118
ProductInstalled	REG_DWORD	0x00000008 (8)
RegistryOverride...	REG_DWORD	0x00000001 (1)
ResyncTimeOnF...	REG_DWORD	0x00000001 (1)
StartMenuScanE...	REG_SZ	C:\Program Files\Citrix\Virtual Desktop Agent\StartMenuScan.exe

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDA 注册问题故障排除

如前所述，必须向要在启动代理会话时考虑使用的 Delivery Controller 注册 VDA。未注册的 VDA 会导致无法充分利用原本可用的资源。VDA 未被注册的原因有很多，其中许多情况都可由管理员进行故障排除。Studio 在目录创建向导中，以及在您创建了交付组之后，提供故障排除信息。

在计算机目录创建期间发现问题：

在目录创建向导中，添加现有计算机之后，计算机帐户名称列表会指示每台计算机是否都适合添加到该目录。将鼠标悬停在每个计算机旁边的图标上，以显示有关该计算机的有用消息。

如果该消息确定存在一台有问题的计算机，您可以删除该计算机（使用**删除**按钮），也可以添加计算机。例如，如果一条消息指示无法获取有关某台计算机的信息（可能因为它始终未向 Delivery Controller 注册），您可能会选择添加计算机。

目录的功能级别控制哪些产品功能可用于目录中的计算机。要使用新产品版本中采用的功能，可能需要使用新的 VDA。通过设置功能级别，该版本（及更高版本，如果功能级别未更改）中采用的所有功能均可用于目录中的计算机。但是，具有较早 VDA 版本的目录中的计算机将无法注册。

在创建了交付组之后发现问题：

创建了交付组之后，Studio 会显示与该组关联的计算机的详细信息。交付组的详细信息窗格中指示应该注册但未注册的计算机数。即，可能存在一台或多台已开启且不是处于维护模式但当前未向 Controller 注册的计算机。查看“应注册、但未注册的”计算机时，请查看详细信息窗格中“故障排除”选项卡了解可能的原因及建议的更正措施。

有关功能级别的详细信息，请参阅创建计算机目录中的 *VDA 版本和功能级别*部分。

有关 VDA 注册故障排除的详细信息，请参阅 CTX136668。

还可以使用 Citrix Health Assistant 对 VDA 注册和会话启动进行故障排除。有关详细信息，请参阅 CTX207624。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

会话

Dec 05, 2017

维护会话处于活动状态对于提供最佳用户体验至关重要。如果由于网络不稳定、网络延迟变化无常以及无线设备的覆盖范围受限等因素而使连接断开，会令用户感到沮丧。对于许多移动工作人员（如医院的医护工作人员）而言，首先要能够在多个工作站之间快速切换，并在每次登录时访问同一组应用程序。

使用以下功能可以优化会话的可靠性，减少不便之处、停机时间以及生产力损失，还可以为移动用户提供在设备间快速、轻松漫游的能力。

- 会话可靠性
- 客户端自动重新连接
- ICA 保持活动状态
- 工作区控制
- 会话漫游

登录时间间隔部分介绍了如何更改默认设置。

您还可以使用户注销会话、断开会话连接以及配置会话预启动和延迟，请参阅管理交付组一文。

会话可靠性

会话可靠性使会话在网络连接中断时保持活动状态并显示在用户的屏幕上。用户仍然可以看到他们正在使用的应用程序，直至网络连接恢复。

此功能对于使用无线连接的移动用户尤为有用。例如，使用无线连接的用户进入铁路隧道后将暂时失去连接。通常，会话会断开连接并从用户屏幕上消失，然后该用户必须重新连接到已断开连接的会话。会话可靠性可使会话在计算机上保持活动状态。为指示连接已断开，用户的显示内容将冻结，且光标变成一个旋转的沙漏，直至用户到达隧道的另一端后恢复连接。用户在连接中断期间可继续访问显示内容，在网络连接恢复后可继续与应用程序交互。会话可靠性可重新连接用户而不提示进行重新身份验证。

Citrix Receiver 用户无法覆盖 Controller 设置。

结合使用会话可靠性与传输层安全性 (TLS)。TLS 仅对用户设备和 NetScaler Gateway 之间发送的数据进行加密。

使用以下策略设置启用和配置会话可靠性：

- “会话可靠性连接”策略设置可允许或阻止会话可靠性。
- “会话可靠性超时”策略设置的默认值为 180 秒（3 分钟）。尽管您可以延长通过会话可靠性使会话保持打开状态的时间长度（此功能的主要目标是为用户提供方便，因此，它不会提示用户重新进行身份验证）。但是，如果您延长会话保持打开状态的时间，则可能导致用户感到不耐烦而离开用户设备，从而使未经授权的用户有机会访问该会话。
- 传入会话可靠性连接使用端口 2598，除非更改“会话可靠性端口号”策略设置中的端口号。
- 如果您不希望用户无需重新进行身份验证即可重新连接到已中断的会话，请使用客户端自动重新连接功能。您可以配置“客户端自动重新连接身份验证”策略设置，以便在用户重新连接到中断的会话时提示用户重新进行身份验证。

如果您同时使用了会话可靠性和客户端自动重新连接，这两项功能将按顺序发挥作用。经过在“会话可靠性超时”策略设置中指定的时间长度之后，会话可靠性将关闭或断开用户会话。之后，客户端自动重新连接策略设置将生效，尝试将用户重新连接到断开连接的会话。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

客户端自动重新连接

通过客户端自动重新连接功能，Citrix Receiver 可以检测到 ICA 会话的意外断开连接，并自动将用户重新连接到受影响的会话。在服务器上启用此功能后，用户无需手动进行重新连接即可继续工作。

对于应用程序会话，Citrix Receiver 将一直尝试重新连接会话，直到重新连接成功或者用户取消重新连接尝试。

对于桌面会话，Citrix Receiver 将在指定时间段内尝试重新连接会话，除非重新连接成功或者用户取消了重新连接尝试。默认情况下，此时间段为五分钟。要更改此时间段，请在用户设备上编辑以下注册表项：

HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;

其中，<*seconds*> 是以秒为单位的数字，经过这些秒数后，将不再尝试重新连接会话。

使用以下策略设置启用和配置客户端自动重新连接：

- **客户端自动重新连接**。允许或禁止在连接中断后由 Citrix Receiver 自动重新连接。
- **客户端自动重新连接身份验证**。允许或禁止自动重新连接时要求用户进行身份验证。
- **客户端自动重新连接日志记录**。允许或禁止在事件日志中记录重新连接事件。默认情况下，禁用日志记录。启用后，服务器的系统日志会捕获与成功和失败的自动重新连接事件有关的信息。每台服务器都会将与重新连接事件有关的信息存储在自己的系统日志中；站点不会提供所有服务器的综合性重新连接事件日志。

客户端自动重新连接包含基于加密用户凭据的身份验证机制。当用户最初登录到站点时，服务器会加密用户凭据并将其存储在内存中，然后创建并向 Citrix Receiver 发送包含加密密钥的 Cookie。Citrix Receiver 将该密钥提交给服务器以便重新连接。服务器会解密这些凭据，并将其提交到 Windows 登录以便进行身份验证。Cookie 过期后，用户必须重新进行身份验证才能重新连接到会话。

如果启用“客户端自动重新连接身份验证”设置，则不使用 Cookie。在 Citrix Receiver 试图自动重新连接时，用户会看到一个对话框，要求输入凭据。

要最大程度地保护用户凭据和会话，请对客户端与站点之间的所有通信使用加密。

可以使用 icaclient.adm 文件对 Citrix Receiver for Windows 禁用客户端自动重新连接。有关详细信息，请参阅您的 Citrix Receiver for Windows 版本的文档。

连接设置也会影响客户端自动重新连接：

- 默认情况下，通过策略设置在站点级别启用客户端自动重新连接，如上所述。无需对用户重新进行身份验证。但是，如果将服务器的 ICA TCP 连接配置为在出现中断的通信链路时重置会话，则不会发生自动重新连接。在连接中断或超时的情况下服务器会断开与会话的连接，仅在此时客户端自动重新连接才会发挥作用。在这种情况下，ICA TCP 连接引用 TCP/IP 网络上用于会话的服务器虚拟端口（而非实际的网络连接）。
- 默认情况下，服务器上的 ICA TCP 连接设置为在连接中断或超时的情况下断开会话。断开连接的会话在系统内存中保持不变，并可供 Citrix Receiver 进行重新连接。
- 可将连接配置为对中断或超时的连接重置或注销会话。如果会话重置，尝试重新连接会启动新会话；并非将用户还原到正在使用的应用程序中的同一位置，而是重新启动应用程序。
- 如果将服务器配置为重置会话，客户端自动重新连接会创建新会话。此过程要求用户输入其凭据才能登录到服务器。
- 如果 Citrix Receiver 或插件提交错误的身份验证信息，自动重新连接可能会失败。在受到攻击期间或者服务器认定距检测到断开连接的时间过长，可能会发生这种情况。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ICA 保持活动状态

启用 ICA 保持活动状态功能可防止断开已损坏的连接。启用此功能后，此功能可防止在服务器未检测到任何活动（例如，无时钟变化、无鼠标移动、无屏幕更新）时，远程桌面服务与该会话断开连接。服务器每隔几秒钟会发送一次保持活动状态数据包，以检测会话是否处于活动状态。如果会话不再处于活动状态，服务器会将该会话标记为已断开连接。

注意：ICA 保持活动状态功能仅在不使用会话可靠性的情况下起作用。会话可靠性自身具有防止被破坏的连接被断开连接的机制。请仅为不使用会话可靠性的连接配置 ICA 保持活动状态。

ICA 保持活动状态设置将覆盖 Microsoft Windows 组策略中配置的保持活动状态设置。

使用以下策略设置启用和配置 ICA 保持活动状态：

- **ICA 保持活动状态超时**。指定用于发送 ICA 保持活动状态消息的间隔（1 至 3600 秒）。如果您希望网络监视软件关闭环境（其中连接很少断开，是否允许用户重新连接到会话并不重要）中处于非活动状态的连接，请勿配置此选项。
  默认间隔是 60 秒：每 60 秒向用户设备发送一次 ICA 保持活动状态数据包。如果用户设备在 60 秒内没有响应，则 ICA 会话的状态将变为断开连接。
- **ICA 保持活动状态**。发送或阻止发送 ICA 保持活动状态消息。

工作区控制

工作区控制允许桌面和应用程序随用户从一个设备移动到另一个设备。此漫游功能使用户在登录后可从任何位置访问所有桌面或打开应用程序，而无需在每个设备中重新启动桌面或应用程序。例如，工作区控制可以帮助医院的医务人员，使他们可以在不同的工作站之间快速移动，并可在每次登录后访问同一组应用程序。如果您将工作区控制选项配置为允许上述功能，则这些工作人员可以与一个客户端设备中的多个应用程序断开连接，然后在其他客户端设备上重新连接以打开相同的应用程序。

工作区控制将影响下列活动：

- **登录**：默认情况下，工作区控制使用户能够在登录时自动重新连接到所有正在运行的桌面和应用程序，而无需手动重新打开它们。通过工作区控制，用户可以打开已断开连接的桌面或应用程序，以及其他客户端设备上的任何活动桌面或应用程序。与桌面或应用程序断开连接后，该桌面或应用程序将继续在服务器上运行。如果您的漫游用户需要在一个客户端设备上使部分桌面或应用程序保持运行状态，同时在另一客户端设备上重新连接到部分桌面或应用程序，您可以将登录重新连接行为配置为仅打开用户先前断开连接的桌面或应用程序。
- **重新连接**：登录到服务器后，用户可以随时单击“重新连接”来重新连接到所有桌面或应用程序。默认情况下，单击“重新连接”将打开已断开连接的桌面或应用程序，以及当前正在另一个客户端设备上运行的任何桌面或应用程序。可以将“重新连接”配置为仅打开用户先前断开连接的桌面或应用程序。
- **注销**：对于通过 StoreFront 打开桌面或应用程序的用户，您可以将“注销”命令配置为使用户从 StoreFront 和所有活动会话一起注销，也可以将其配置为仅从 StoreFront 注销。
- **断开连接**：用户可以一次与所有正在运行的桌面和应用程序断开连接，而无需与每个应用程序逐个断开连接。

工作区控制仅适用于通过 Citrix StoreFront 连接访问桌面和应用程序的 Citrix Receiver 用户。默认情况下，已为虚拟桌面会话禁用工作区控制，但已为托管的应用程序启用该功能。默认情况下，不会在已发布的桌面与这些桌面内部运行的任何已发布应用程序之间进行会话共享。

当用户移动到新客户端设备时，用户策略、客户端驱动器映射和打印机配置将随之进行适当更改。（用户）策略和（客户端驱动器）映射是根据用户当前登录到会话所使用的客户端设备来应用的。例如，如果医务人员从医院急救室的客户端设备注销，

© 1999-2017 Citrix Systems, Inc. All rights reserved.

然后登录到该医院的 X 射线实验室的工作站，则适用于 X 射线实验室中的会话的策略、打印机映射和客户端驱动器映射将在该会话启动时生效。

您可以自定义用户位置发生变化后为其显示哪些打印机。您还可以控制用户是否可以打印到本地打印机、用户进行远程连接时消耗的带宽量，以及用户打印体验的其他方面。

有关为用户启用和配置工作区控制的信息，请参阅 StoreFront 文档。

会话漫游

默认情况下，用户的会话在客户端设备之间漫游。当用户启动会话，然后再移动到另一台设备时，将使用相同的会话，并且应用程序在两台设备上均可用。不管使用哪台设备或者会话是否存在，应用程序均继续。在很多情况下，分配给应用程序的打印机和其他资源也继续。

尽管此默认行为提供很多优势，但它可能不是所有情况的理想设置。您可以使用 PowerShell SDK 阻止会话漫游。

示例 1：医疗人员使用两台设备，一台桌面 PC 用于填写保险单，一台平板电脑用于查找患者信息。

- 如果启用会话漫游，这两个应用程序可以同时显示在这两台设备上（在一台设备上启动的应用程序在所使用的全部设备上均可见）。这可能不满足安全要求。
- 如果禁用会话漫游，则患者记录不会显示在桌面 PC 上，保险单也不会显示在平板电脑上。

示例 2：生产经理在其办公室的 PC 上启动一个应用程序。设备名称和位置确定该会话可以使用的打印机及其他资源。当天晚些时候，该经理进入隔壁大楼的一件办公室参加会议，此会议需要他使用打印机。

- 如果启用会话漫游，该生产经理可能无法访问该会议室附近的打印机，因为他之前在自己的办公室启动的应用程序已导致为其分配了该办公室附近的打印机和其他资源。
- 如果禁用会话漫游，当他使用其他计算机时（使用相同的凭据），则会启动新会话，并且他可以使用附近的打印机和资源。

配置会话漫游

要配置会话漫游，请使用以下带有“SessionReconnection”属性的授权策略规则 cmdlet。也可以指定“LeasingBehavior”属性；请参阅下面的连接租用和会话漫游。

对于桌面会话：

> Set-BrokerEntitlementPolicyRule <*Delivery-Group-name*> -SessionReconnection <*value*> -LeasingBehavior Allowed|Disallowed

对于应用程序会话：

> Set-BrokerAppEntitlementPolicyRule <*Delivery-Group-name*> -SessionReconnection <*value*> -LeasingBehavior Allowed|Disallowed

其中，<*value*> 可以是下列其中一个值：

- **Always**。会话始终漫游，不管所使用的客户端设备和会话是连接还是断开连接。此为默认值。
- **DisconnectedOnly**。仅重新连接到已断开连接的会话；否则启动新会话。（可以通过首先断开会话连接在客户端设备之间漫游会话，也可以使用工作区控制显式漫游会话。）绝不使用另一台客户端设备上处于连接状态的活动会话；而是启动新会话。
- **SameEndpointOnly**。用户所使用的每个客户端设备具有唯一会话。此选项完全禁用漫游。用户只能重新连接到之前在会话

© 1999-2017 Citrix Systems, Inc. All rights reserved.

中使用的同一设备。

“LeasingBehavior”属性在下文介绍。

其他设置的影响

禁用会话漫游受交付组内应用程序属性中的应用程序限制“Allow only one instance of the application per user”（仅允许每个用户具有一个应用程序实例）的影响。

- 如果禁用会话漫游，则会禁用“Allow only one instance ...”（仅允许每个用户具有...）应用程序限制。
- 如果启用“Allow only one instance ...”（仅允许每个用户具有...）应用程序限制，请勿配置允许在新设备上建立新会话的两个值。

连接租用和会话漫游

如果您不熟悉连接租用，请参阅连接租用一文。

Controller 进入租用连接模式时，会话重新连接恢复到其默认值，仅将用户重新连接到桌面或应用程序的其中一个活动会话或已断开连接的会话。

对于其他安全性，如果已配置非默认会话漫游值，并具有在多个设备上共享相同登录凭据的多个用户，请注意为包含该用户帐户的交付组禁用连接租用功能。

为什么呢？在此场景下，一个会话在多个设备之间共享。这在某些时候并不可取，例如，当 Controller 处于租用连接模式时，某个人显示了机密信息，但此信息不能被使用相同凭据进行重新连接的其他人看到。

在授权策略中禁用连接租用可以消除这种可能性：即使 Controller 处于租用连接模式，用户也将无法看到使用相同登录的另一个用户的会话。其他授权策略可以保持原样；单个用户帐户可以在单独的授权中使用连接租用功能。

要在授权策略中禁用连接租用，请将“LeasingBehavior Disallowed”属性添加到授权策略 cmdlet 中。如果禁用连接租用，必须手动删除任何已为该授权策略创建并缓存的启动租用；否则，在数据库中断时用户将仍可以进行重新连接。

登录时间间隔

如果包含桌面 VDA 的虚拟机在登录进程完成之前关闭，可以将更多时间分配给该进程。7.6 及更高版本的默认值为 180 秒（7.0-7.5 的默认值为 90 秒）。

在计算机（或计算机目录中使用的主映像）上，设置以下注册表项：

注册表项：HKLM\SOFTWARE\Citrix\PortICA

值：AutoLogonTimeout

类型：DWORD

以秒为单位指定十进制时间，范围为 0-3600。

如果更改了主映像，请更新目录。

注意：此设置仅适用于包含桌面（工作站）VDA 的 VM；Microsoft 控制包含服务器 VDA 的计算机上的登录超时。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

在 Studio 中使用搜索

Dec 05, 2017

使用“搜索”功能可查看有关特定计算机、会话、计算机目录、应用程序或交付组的信息。

1. 在 Studio 导航窗格中选择 搜索。
   注意：无法使用 “搜索”框在计算机目录或“交付组”选项卡中进行 搜索。使用导航窗格中的“搜索”节点。
   要在显示画面中显示 其他搜索条件，请单击 “搜索”下拉字段旁边的加号。单击减号可删除搜索条件。

2. 输入名称，或使用下拉列表选择用于查找项目的其他搜索选项。
3. （可选） 选择 另存 为保存您的搜索。此搜索即会显示在“保存的搜索”列表中。

或者，单击“展开搜索”图标（两个向下的尖括号）可显示搜索属性下拉列表；可通过从下拉列表的属性中生成表达式来执行高级搜索。

可加快搜索速度的提示：

- 要在显示 画面中显示作为搜索和排序依据的 其他特性，请在任意列上单击鼠标右键，然后选择 选择 列。
- 要查找已连接到计算机的用户设备，请使用“客户端(IP)”和“是”，然后输入设备的 IP 地址。
- 要查找活动会话，请使用“会话状态”、“是”和“已连接”。
- 要列出 交付组中的所有计算机，请在导航窗格中选择 交付 组，再选择相应组，然后 在“操作”窗格中选择 查看 计算机。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

标记

Dec 05, 2017

简介

标记是指用于标识计算机、应用程序、桌面、交付组、应用程序组和策略等项目的字符串。创建标记并将其添加到项目后，就可以定制某些操作，以便仅应用于具有指定标记的项目。

- 在 Studio 中定制搜索显示内容。

  例如，要仅显示已针对测试人员优化的应用程序，可创建名为“测试”的标记，然后将其添加（应用）到那些应用程序。现在就可以使用标记“测试”过滤 Studio 搜索。

- 从交付组中的应用程序组或特定桌面发布应用程序，仅考虑所选交付组中的一部分计算机。这称为*标记限制*。

  通过使用标记限制，可以使用现有计算机来完成多个发布任务，从而节省与部署和管理其他计算机有关的成本。标记限制可以视为对交付组中的计算机进行划分（或分区）。其功能类似于 XenApp 7.x 之前版本中的工作组，但不完全一样。

  对交付组中的一部分计算机进行隔离和故障排除时，将应用程序组或桌面与标记限制结合使用很有用。

  请参阅下文了解使用标记限制的详细信息和示例。

- 为交付组中的一部分计算机安排定期重新启动。

  通过对计算机使用标记限制，您可以使用新的 PowerShell cmdlet 为交付组中的一部分计算机配置多个重新启动计划。有关示例和详细信息，请参阅管理交付组一文中的“为交付组中的计算机创建多个重新启动计划”一节。

- 对交付组中的一部分计算机、交付组类型或具有（或没有）指定标记的 OU 定制 Citrix 策略的应用（分配）。

  例如，如果您只想将 Citrix 策略应用于功能更强大的工作站，可为那些计算机添加名为“功能强大”的标记。然后，在“创建策略”向导中的**分配策略**页面上，选择该标记，同时选中**启用**复选框。您也可以为交付组添加标记，然后将 Citrix 策略应用于该组。有关详细信息，请参阅创建策略一文和此博客文章。（请注意，自从博客文章发布后，用于向计算机添加标记的 Studio 界面已更改。）

可以将标记应用于以下项目：

- 计算机
- 应用程序
- 交付组
- 应用程序组

可以在 Studio 中创建或编辑以下项时配置标记限制：

- 共享交付组中的桌面
- 应用程序组

用于桌面或应用程序组的标记限制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

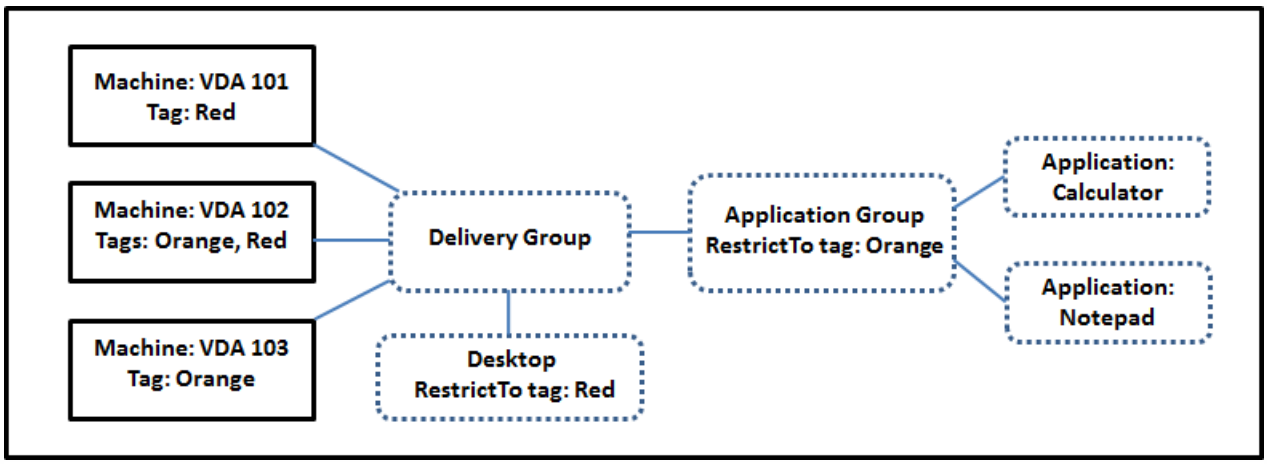
标记限制涉及多个步骤：

- 创建标记，然后将其添加（应用）到计算机。
- 使用标记限制创建或编辑组（即，“限制启动带标记 x 的计算机”）。

标记限制延长了 Broker 计算机选择过程。Broker 从受限于访问策略、配置的用户列表、区域首选项、启动就绪情况以及标记限制（如果存在）的关联交付组中选择计算机。对于应用程序，Broker 按优先级顺序回退到其他交付组，对考虑的每个交付组应用相同的计算机选择规则。

示例 1

此示例介绍一个简单布局，它使用标记限制来限制哪些计算机将被考虑用于启动特定的桌面和应用程序。该站点有一个共享交付组、一个发布的桌面以及一个配置了两个应用程序的应用程序组。



- 已为所有三台计算机 (VDA 101-103) 添加了标记。
- 共享交付组中的桌面创建时使用了名为“Red”的标记限制，因此，桌面只能在该交付组中具有标记“Red”的计算机（VDA 101 和 102）上启动。
- 应用程序组创建时使用了“Orange”标记限制，因此它的所有应用程序（Calculator 和 Notepad）只能在该交付组中具有标记“Orange”的计算机（VDA 102 和 103）上启动。

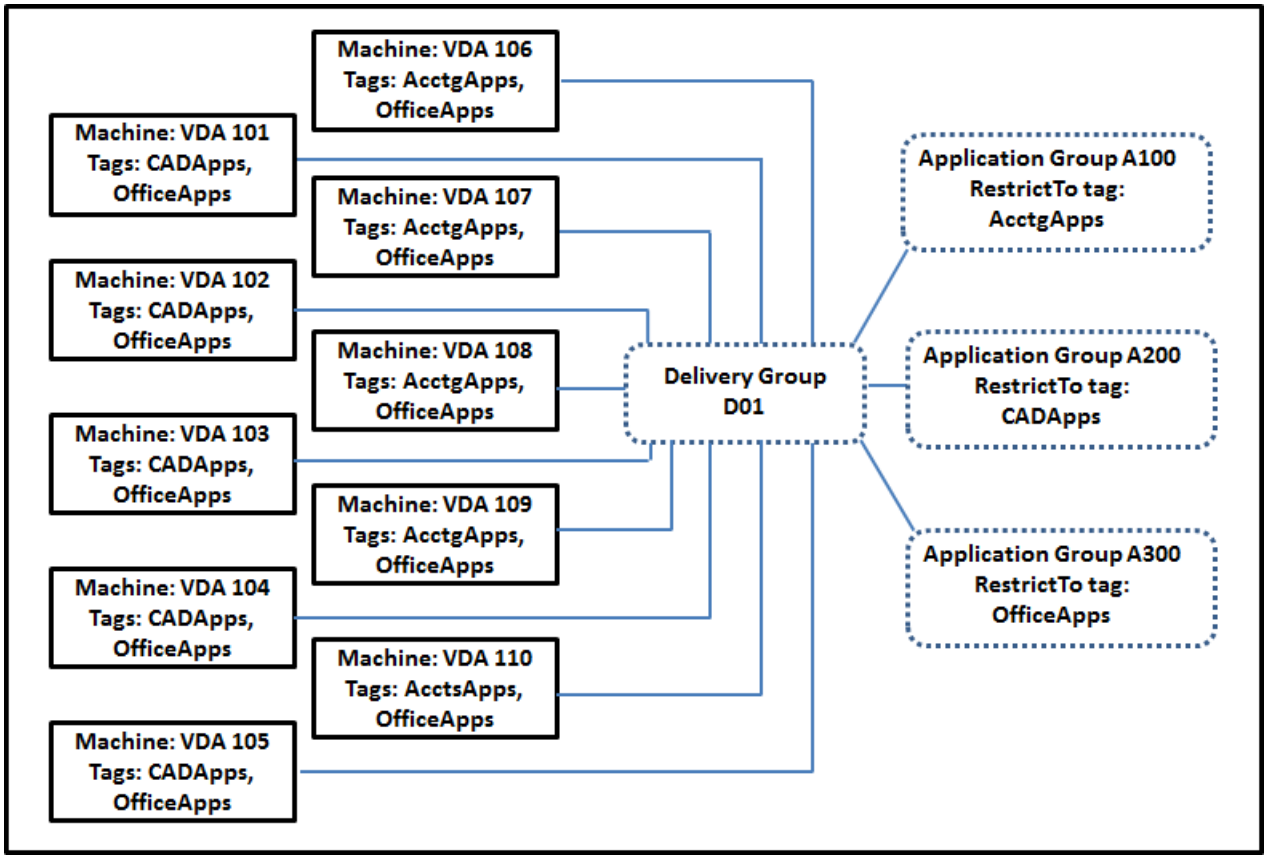
请注意，计算机 VDA 102 有两个标记（Red 和 Orange），因此该计算机可以被考虑用于启动应用程序和桌面。

示例 2

此示例包含创建时使用了标记限制的多个应用程序组。这样，相比仅使用交付组时，可以使用更少的计算机来交付更多应用程序。

（“如何配置示例 2”一节介绍了用于创建和应用标记以及之后配置此示例中的标记限制的步骤。）

© 1999-2017 Citrix Systems, Inc. All rights reserved.



此示例使用十台计算机 (VDA 101-110)、一个交付组 (D01) 和三个应用程序组（A100、A200 和 A300）。通过将标记应用于每台计算机，然后在创建每个应用程序组时指定标记限制：

- 组中的核算用户可以访问五台计算机 (VDA 101–105) 上他们所需的应用程序。
- 组中的 CAD 设计师可以访问五台计算机 (VDA 106-110) 上他们所需的应用程序。
- 组中需要 Office 应用程序的用户可以访问十台计算机 (VDA 101-110) 上的 Office 应用程序。

仅使用十台计算机，且只有一个交付组。单独使用交付组（不使用应用程序组）需要的计算机数可能是使用应用程序组时的两倍，因为一台计算机只能属于一个交付组。

管理标记和标记限制

标记是通过 Studio 中的**管理标记**操作来创建、添加（应用）、编辑以及从选定项目删除。

> **例外情况：**用于策略分配的标记是通过 Studio 中的**管理标记**操作来创建、编辑以及删除；但标记是在创建策略时应用（分配）；请参阅创建策略一文了解详细信息。

标记限制是当您在交付组中创建或编辑桌面时以及当您创建和编辑应用程序组时配置。有关创建和编辑组的完整信息，请参阅以下文章：

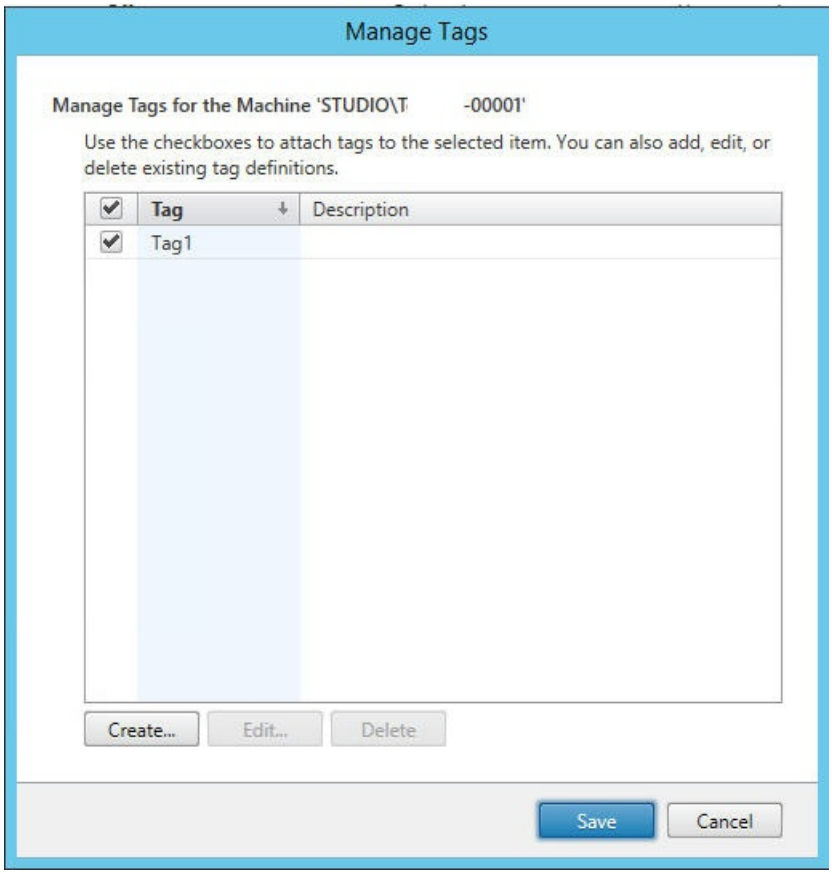
- 创建交付组
- 管理交付组
- 创建应用程序组
- 管理应用程序组

© 1999-2017 Citrix Systems, Inc. All rights reserved.

使用 Studio 中的“管理标记”对话框

在 Studio 中，选择要应用标记的项目（一台或多台计算机、应用程序、桌面、交付组或应用程序组），然后在“操作”窗格中选择**管理标记**。“管理标记”对话框将列出在站点中创建的所有标记，而不仅限于为所选项目创建的标记。

- 包含复选标记的复选框表示标记已经添加到选定项目。（在下方屏幕截图中，选定计算机应用了名为“Tag1”的标记。）
- 如果您选择了多个项目，则包含连字符的复选框表示部分（而非所有）选定项目添加了标记。



可以从“管理标记”对话框中执行以下操作。请务必查看“小心”部分。

要创建标记，请执行以下操作：

单击**创建**。输入名称和说明。标记名称必须是唯一的，并且不区分大小写。然后，请单击**确定**。（创建标记不会自动将其应用于您选择的任何项目。请使用复选框应用标记。）

要添加（应用）一个或多个标记，请执行以下操作：

启用标记名称旁边的复选框。**注意：**如果您选择了多个项目，且标记旁边的复选框包含一个连字符（表示部分（而非所有）选定项目已经应用了标记），将其更改为复选标记将影响所有选定计算机。

如果您尝试将标记添加到一台或多台计算机，且该标记当前用作一个应用程序组中的限制，系统会警告您该操作会导致那些计算机可以用于启动。如果这是您希望得到的结果，请继续。

要删除一个或多个标记，请执行以下操作：

清除标记名称旁边的复选框。**注意：**如果您选择了多个项目，且标记旁边的复选框包含一个连字符（表示部分（而非所

© 1999-2017 Citrix Systems, Inc. All rights reserved.

有）选定项目已经应用了标记），清除复选框将从所有选定计算机删除标记。

如果您尝试从正在将标记用作限制的计算机删除该标记，将显示警告消息，说明这会影响将被考虑用于启动的那些计算机。如果这是您希望得到的结果，请继续。

要编辑标记，请执行以下操作：

选择一个标记，然后单击**编辑**。输入新名称和/或说明。一次只能编辑一个标记。

要删除一个或多个标记，请执行以下操作：

选择标记，然后单击**删除**。“删除标记”对话框将显示当前使用所选标记的项目数（例如，“2 台计算机”）。单击项目可显示详细信息。例如，单击“2 台计算机”项目将显示应用了标记的两台计算机的名称。确认是否要删除标记。

不能使用 Studio 删除用作限制的标记。必须先编辑应用程序组并删除标记限制或选择一个不同的标记。

在“管理标记”对话框中完成时，单击**保存**。

提示：要查看某台计算机是否应用了任何标记，请执行以下操作：

在导航窗格中选择**交付组**。在中间窗格中选择一个交付组，然后在“操作”窗格中选择**查看计算机**。在中间窗格中选择一台计算机，然后在下面的“详细信息”窗格中选择“标记”选项卡。

管理标记限制

配置标记限制是一个多步骤过程：首先创建标记，并将其添加/应用到计算机。然后，将限制添加到应用程序组或桌面。

要创建和应用标记，请执行以下操作：

使用上文所述的**管理标记**操作来创建标记，然后将其添加（应用）到将受标记限制影响的计算机。

要将标记限制添加到应用程序组，请执行以下操作：

创建或编辑应用程序组。在“交付组”页面上，选择**限制启动带标记的计算机**，然后从下拉框中选择标记。

要更改或删除应用程序组上的标记限制，请执行以下操作：

编辑组。在“交付组”页面上，从下拉框中选择一个不同的标记，或通过清除**限制启动带标记的计算机**彻底删除标记限制。

要将标记限制添加到桌面，请执行以下操作：

创建或编辑交付组。在“桌面”页面上，单击**添加**或**编辑**。在“添加桌面”对话框中，选择**限制启动带标记的计算机**，然后从下拉框中选择标记。

要更改或删除交付组上的标记限制，请执行以下操作：

编辑组。在“桌面”页面上，单击**编辑**。在对话框中，从下拉框中选择一个不同的标记，或通过清除**限制启动带标记的计算机**彻底删除标记限制。

将标记添加到项目或从项目删除标记时的注意事项

应用于项目的标记可以用于不同的目的，因此请注意，添加和删除标记可能会有意外的影响。可以使用标记对 Studio 搜索字段中的计算机显示排序。配置应用程序组或桌面时可以将相同标记用作限制，这会将启动考虑范围仅限于指定的交付组中具有该标记的计算机。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

如果您尝试在标记已配置为桌面或应用程序组的标记限制后将该标记添加到一台或多台计算机，Studio 会警告您添加该标记可能会使计算机可用于启动其他应用程序或桌面。如果这是您希望得到的结果，请继续。如果不是，您可以取消操作。

> 例如，假设您创建一个具有“Red”标记限制的应用程序组。后来，您在该应用程序组使用的相同交付组中添加多个其他计算机。如果您之后尝试将“Red”标记添加到那些计算机，Studio 将显示与此类似的消息：“标记“Red”已用作以下应用程序组上的限制。添加此标记可能会使选定的计算机可用于启动此应用程序组中的应用程序。” 您随后可以确认或取消向这些附加计算机添加该标记。

同样，如果一个标记正用于一个应用程序组中以限制启动，Studio 会警告您不能删除该标记，直到您通过编辑组删除作为限制的该标记。（如果您已被允许删除用作应用程序组中的限制的标记，那可能会导致允许应用程序在与该应用程序组关联的交付组中的所有计算机上启动。）如果标记当前正用作桌面启动的限制，适用相同的禁止删除标记做法。编辑交付组中的应用程序组或桌面以删除相应标记限制后，可以删除标记。

所有计算机不能有相同的应用程序集合。用户可能属于多个应用程序组，每个组都有不同的标记限制和属于交付组的不同或重叠计算机集合。下表列出了如何决定计算机考虑范围。

应用程序已添加到以下应用程序组时	**选定交付组中的这些计算机被考虑用于启动**
没有标记限制的一个应用程序组	任何计算机
具有标记限制 A 的一个应用程序组	应用了标记 A 的计算机
两个应用程序组，一个具有标记限制 A，另一个具有标记限制 B	同时具有标记 A 和标记 B 的计算机；如果不存在，则是具有标记 A 或标记 B 的计算机
两个应用程序组，一个具有标记限制 A，另一个没有标记限制	具有标记 A 的计算机；如果不存在，则是任何计算机

如果您在计算机重新启动计划中使用了标记限制，则影响标记应用或限制的任何更改都将影响下一个计算机重新启动周期。但不会影响进行更改时正在进行的任何重新启动周期。（请参阅“管理交付组”一文。）

如何配置示例 2

以下顺序显示了创建和应用标记以及之后为上面的第二个示例中说明的应用程序组配置标记限制的步骤。

VDA 和应用程序已经安装在计算机上，且已创建交付组。

创建标记并将其应用于计算机：

1. 在 Studio 中，选择交付组 D01，然后在“操作”窗格中选择**查看计算机**。
2. 选择计算机 VDA 101-105，然后在“操作”窗格中选择**管理标记**。
3. 在“管理标记”对话框中，单击**创建**，然后创建名为 CADApps 的标记。单击**确定**。
4. 重新单击**创建**，并创建名为 OfficeApps 的标记。单击**确定**。
5. 仍在“管理标记”对话框中，通过启用每个标记名称（CADApps 和 OfficeApps）旁边的复选框将新创建的标记添加（应用）到选定的计算机，然后关闭该对话框。
6. 选择交付组 D01，然后在“操作”窗格中选择**查看计算机**。
7. 选择计算机 VDA 106-110，然后在“操作”窗格中选择**管理标记**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

8. 在“管理标记”对话框中，单击**创建**，然后创建名为 AcctgApps 的标记。单击**确定**。
9. 通过单击每个标记名称旁边的复选框将新创建的 AcctgApps 标记和 OfficeApps 标记应用到选定的计算机，然后关闭该对话框。

创建具有标记限制的应用程序组。

1. 在 Studio 的导航窗格中，选择**应用程序**，然后在“操作”窗格中选择**创建应用程序组**。“创建应用程序组”向导将启动。
2. 在向导的**交付组**页面上，选择交付组 D01。选择**限制启动带标记的计算机**，然后从下拉框中选择 AcctgApps 标记。
3. 完成向导，同时指定核算用户和核算应用程序。（添加应用程序时，请选择“从“开始”菜单”来源，这将搜索具有 AcctgApps 标记的计算机上的应用程序。）在**摘要**页面上，为组命名 A100。
4. 重复上述步骤以创建应用程序组 A200，同时指定具有 CADApps 标记的计算机，以及合适的用户和应用程序。
5. 重复步骤以创建应用程序组 A300，同时指定具有 OfficeApps 标记的计算机，以及合适的用户和应用程序。

更多信息

博客文章：How to assign desktops to specific servers（如何向特定服务器分配桌面）。这篇文章还包含以下视频。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

IPv4/IPv6 支持

Dec 05, 2017

此版本支持纯 IPv4 部署、纯 IPv6 部署，以及使用重叠 IPv4 和 IPv6 网络的双协议栈部署。

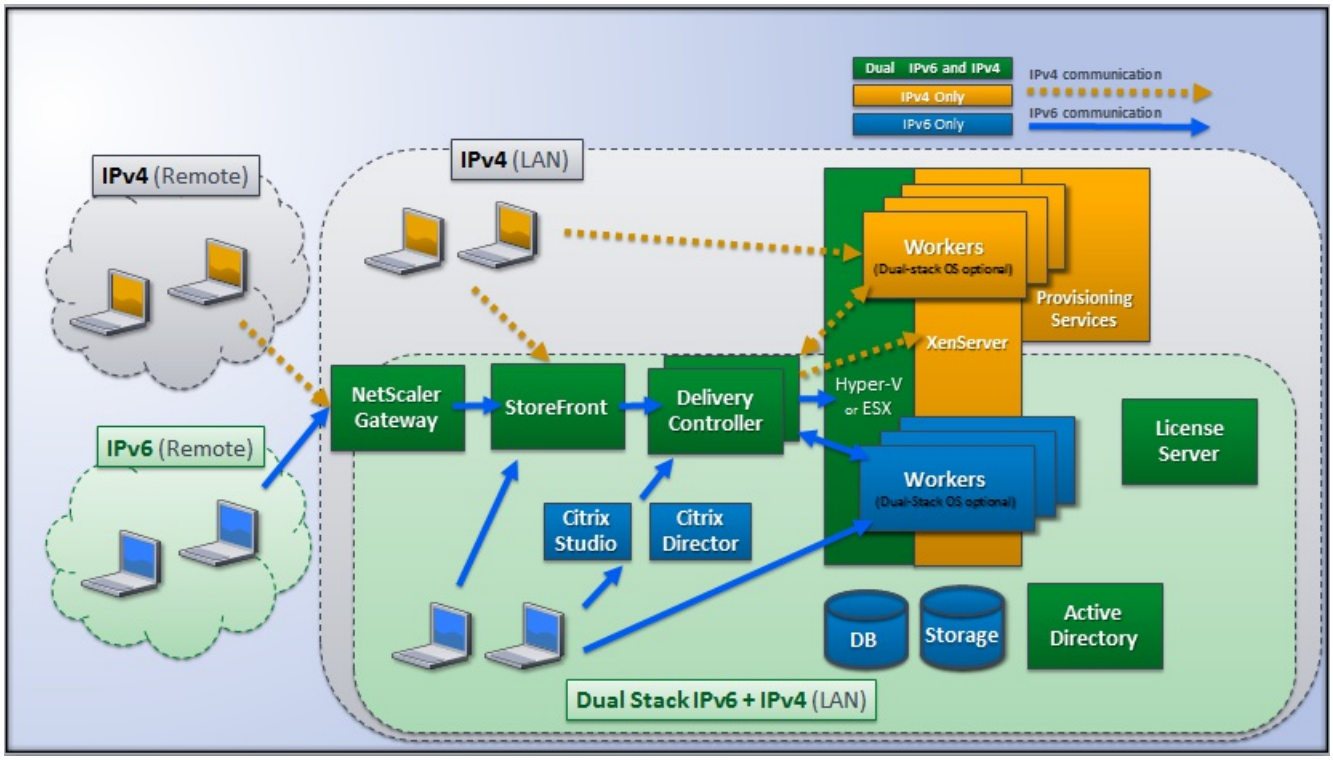
IPv6 通信通过与 Virtual Delivery Agent (VDA) 连接相关的两个 Citrix 策略设置进行控制：

- 强制使用 IPv6 的主要设置：仅使用 IPv6 控制器注册。
- 定义 IPv6 网络掩码的从属设置：控制器注册 IPv6 网络掩码。

启用“仅使用 IPv6 控制器注册”策略设置时，对于传入连接，VDA 将使用 IPv6 地址向 Delivery Controller 注册。

双堆栈 IPv4/IPv6 部署

下图说明了双协议栈 IPv4/IPv6 部署。在此情景中，工作者是安装在虚拟机管理程序或者物理系统上的 VDA，主要用于启用应用程序和桌面的连接。支持双 IPv6 和 IPv4 的组件在使用隧道或双协议软件的操作系统上运行。



这些 Citrix 产品、组件和功能仅支持 IPv4：

- Provisioning Services
- XenServer 6.x 版
- 不由**仅使用 IPv6 控制器注册**策略设置控制的 VDA
- XenApp 7.5 之前的版本、XenDesktop 7 之前的版本及 Director

对于此部署：

- 如果一个团队经常使用 IPv6 网络，而管理员希望他们使用 IPv6 通信，管理员将基于启用了主要 IPv6 策略设置（即启用仅使用 IPv6 控制器注册）的工作者映像或组织单位 (OU) 来发布 IPv6 桌面和应用程序。

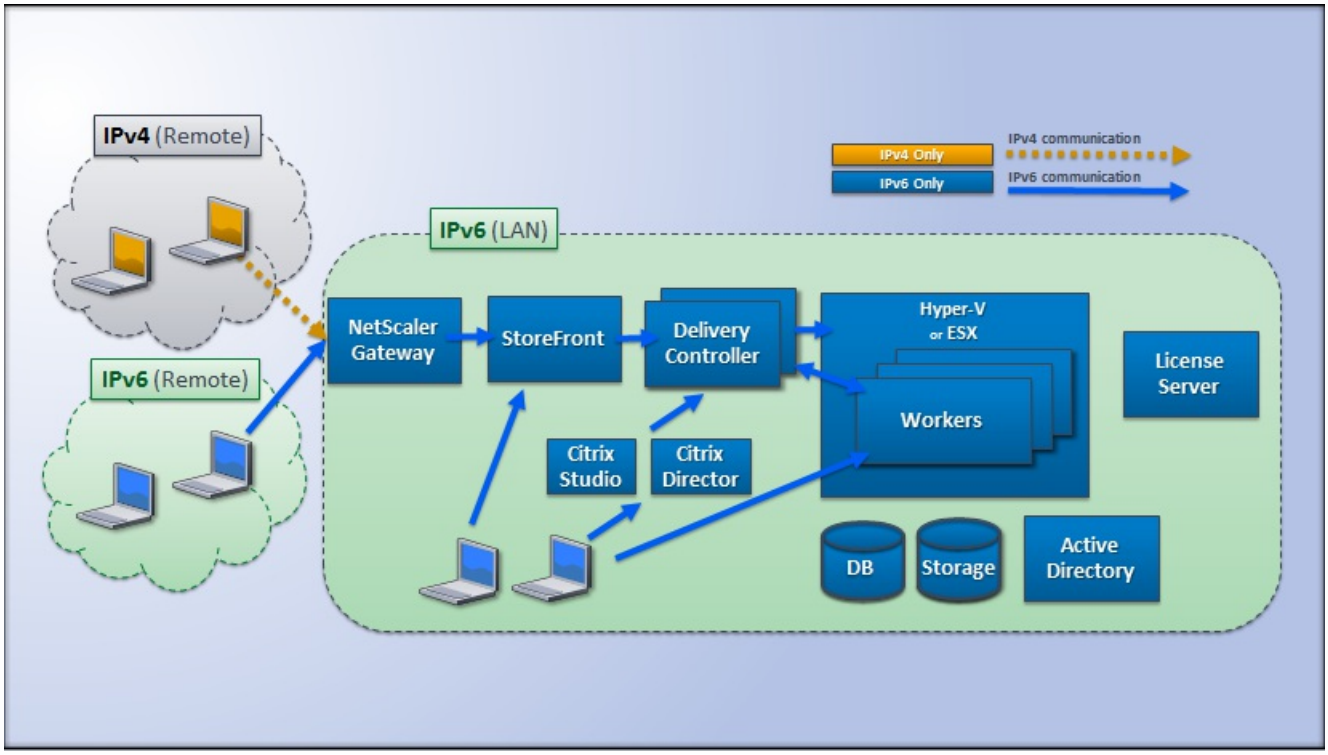
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 如果一个团队经常使用 IPv4 网络，管理员将基于关闭了主要 IPv6 策略设置（即禁用仅使用 IPv6 控制器注册）的工作者映像或 OU 来发布 IPv4 桌面和应用程序。

纯 IPv6 部署

下图说明了纯 IPv6 部署。在此情景中：

- 组件在配置为支持 IPv6 网络的操作系统上运行。
- 对所有 VDA 启用主要 Citrix 策略设置（仅使用 IPv6 控制器注册）；他们必须使用 IPv6 地址向控制器注册。



IPv6 的策略设置

有两个 Citrix 策略设置会影响对纯 IPv6 或双协议栈 IPv4/IPv6 实现的支持。请配置与连接相关的以下策略设置：

- **仅使用 IPv6 控制器注册**：控制 Virtual Delivery Agent (VDA) 使用哪种形式的地址来向 Delivery Controller 注册。默认情况下已禁用
  - VDA 与控制器进行通信时，将按以下优先级选择使用单个 IPv6 地址：全局 IP 地址、唯一本地地址 (ULA)、链接本地地址（仅当没有其他 IPv6 地址可用时）。
  - 禁用后，VDA 将使用计算机的 IPv4 地址向控制器注册并与之通信。
- **控制器注册 IPv6 网络掩码**：一台计算机可以具有多个 IPv6 地址；此策略设置允许管理员将 VDA 限定到首选子网而非全局 IP（如果已注册一个全局 IP）。此设置指定 VDA 将要注册的网络：VDA 仅在与指定网络掩码匹配的第一个地址上注册。仅当启用仅使用 IPv6 控制器注册策略设置时，此设置才有效。默认值 = 空字符串

重要：VDA 使用 IPv4 还是 IPv6 完全由这些策略设置决定。换言之，要使用 IPv6 寻址，VDA 必须由启用了**仅使用 IPv6 控制器注册**设置的 Citrix 策略控制。

部署注意事项

如果您的环境同时包含 IPv4 和 IPv6 网络，您将需要对仅 IPv4 客户端和可以访问 IPv6 网络的客户端分开进行交付组配置。 考虑使用命名、手动 Active Directory 组分配或智能访问过滤器来区分用户。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

如果连接在 IPv6 网络上发起，但随后尝试从仅具有 IPv4 访问权限的内部客户端再次进行连接，可能无法重新连接到会话。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

用户配置文件

Dec 05, 2017

默认情况下，在安装 Virtual Delivery Agent 时，Citrix Profile Management 以静默方式安装在主映像上，但您不必将 Profile Management 用作配置文件解决方案。

为迎合用户需求的不断变化，可使用 XenApp 和 XenDesktop 策略为每个交付组中的计算机应用不同的配置文件行为。例如，一个交付组可能需要 Citrix 强制配置文件（其模板保存在一个网络位置），而另一个交付组可能需要 Citrix 漫游配置文件（保存在包括多个重定向文件夹的其他位置）。

- 如果组织中的其他管理员负责 XenApp 和 XenDesktop 策略，应与他们合作以确保他们跨交付组设置任何配置文件相关的策略。
- 还可在组策略、Profile Management .ini 文件和各个本地虚拟机中设置 Profile Management 策略。定义配置文件行为的这些方式按照以下顺序读取：
  1. 组策略（.adm 或 .admx 文件）
  2. 策略节点中的 XenApp 和 XenDesktop 策略
  3. 用户连接的虚拟机上的本地策略
  4. Profile management .ini 文件

  例如，如果您在组策略和策略节点中配置相同的策略，系统会读取组策略中的策略设置，而忽略 XenApp 和 XenDesktop 策略设置。

无论选择哪个配置文件解决方案，Director 管理员都可以访问这些用户配置文件的诊断信息并进行故障排除。有关详细信息，请参阅 Director 文档。

如果您使用 Personal vDisk 功能，Citrix 用户配置文件将默认存储在虚拟桌面的 Personal vDisk 中。不要在 Personal vDisk 上仍有配置文件副本时删除用户存储中的配置文件副本。这样做会造成 Profile Management 错误，并导致登录虚拟桌面将使用临时配置文件。

自动配置

会根据 Virtual Delivery Agent 安装自动检测桌面类型，并且，除了您在 Studio 中所做的配置选择，还会相应地设置 Profile Management 默认值。

Profile Management 调整的策略如下表所示。 此功能将保留任何非默认策略设置，且不会将其覆盖。 有关各策略的详细信息，请参阅 Profile Management 文档。 创建配置文件的计算机类型会影响调整的策略。 主要因素为计算机属于静态计算机还是预先置备的计算机，以及这些计算机是由多个用户共享还是专门仅供一个用户使用。

静态系统具有某些类型的本地存储，这些本地存储中的内容在关闭系统时有望继续存在。 静态系统可能会采用存储区域网络 (SAN) 等存储技术提供本地磁盘模仿。 与此相反，预先置备的系统是基于基础磁盘和某些类型的身份磁盘即时创建的。 本地存储通常通过 RAM 磁盘或网络磁盘进行模拟，网络磁盘通常由具有高速链路的 SAN 提供。 置备技术通常为 Provisioning Services 或 Machine Creation Services（或第三方的等效技术）。 预先置备的系统有时具有静态本地存储（可能由 Personal vDisk 提供）；此类计算机归类为静态计算机。

总而言之，这两类因素定义了以下计算机类型：

- **静态 专用计算机** — 例如，具有静态分配以及通过 Machine Creation Services 创建的 个人虚拟磁盘的桌面操作系统计算机、具有通过 VDI-in-a-Box 创建的 个人虚拟磁盘的桌面、物理工作站和 便携式计算机
- **静态 共享计算机** — 例如，通过 Machine Creation Services 创建的服务器操作系统计算机
- **预先置备的 专用计算机** — 例如，具有静态分配但 不具有通过 Provisioning Services 创建的个人虚拟磁盘的桌面操作系统计算机

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **预先置备的 共享计算机** — 例如，具有通过 Provisioning Services 创建的 随机分配的桌面操作系统计算机、 不具有通过 VDI-in-a-Box 创建的个人虚拟磁盘的桌面

以下 Profile Management 策略设置是针对不同的计算机类型建议的指导原则。 这些设置在大多数情况下能够正常发挥作用，但根据部署要求，您可能希望使用与之有所差别的设置。

重要：注销时删除本地缓存的配置文件、Profile Streaming 和总是缓存是自动配置功能强制使用的策略。 手动调整其他策略。

静态计算机

策略	静态专用计算机	静态共享计算机
注销时删除本地缓存的配置文件	已禁用	已启用
Profile Streaming	已禁用	已启用
总是缓存	已启用（备注 1）	已禁用（备注 2）
主动写回	已禁用	已禁用（备注 3）
处理本地管理员登录	已启用	已禁用（备注 4）

已置备的计算机

策略	预先置备的专用计算机	预先置备的共享计算机
注销时删除本地缓存的配置文件	已禁用（备注 5）	已启用
Profile Streaming	已启用	已启用
总是缓存	已禁用（备注 6）	已禁用
主动写回	已启用	已启用
处理本地管理员登录	已启用	已启用（备注 7）

1. 由于 Profile Streaming 对此类计算机禁用，因此将始终忽略 总是 缓存设置。
2. 禁用 总是 缓存。但是，可以通过启用此策略并用其定义一个文件大小限制 (MB) 来确保在登录后尽快将大型文件加载到配置文件中。 等于或大于此大小的任何文件都会尽快在本地缓存。
3. 禁用 主动 写回，但在 XenApp 服务器间 漫游的用户的配置文件中保存更改时除外。在这种情况下，请启用此策略。
4. 对除托管共享桌面以外的桌面禁用 处理 本地管理员登录。 在这种情况下，请启用此策略。
5. 禁用 注销时删除 本地缓存的配置文件。这样将保留本地缓存的配置文件。 由于计算机会在注销时重置，但分配给单个用

© 1999-2017 Citrix Systems, Inc. All rights reserved.

户，因此，如果缓存了其配置文件，登录速度将会更快。

6. 禁用 总是 缓存。但是，可以通过启用此策略并用其定义一个文件大小限制 (MB) 来确保在登录后尽快将大型文件加载到配置文件中。 等于或大于此大小的任何文件都会尽快在本地缓存。
7. 启用 处理本地 管理员登录，但不对在 XenApp 和 XenDesktop 服务器间 漫游的用户的配置文件启用此策略。在这种情况下，请禁用此策略。

文件夹重定向

通过文件夹重定向，可以将用户数据存储在配置文件的存储位置以外的网络共享上。 这将减少配置文件大小和加载时间，但是可能会影响网络带宽。 文件夹重定向不需要使用 Citrix 用户配置文件。 您可以选择自己管理用户配置文件，仍可以重定向文件夹。

在 Studio 中使用 Citrix 策略配置文件夹重定向。

- 确保用于存储重定向文件夹内容的网络位置可用，并且具有适当的权限。 已验证位置属性。
- 重定向文件夹已在网络上设置，并且已在登录时从用户的虚拟桌面填充其内容。

注意：仅使用 Citrix 策略或 Active Directory 组策略对象配置文件夹重定向，请勿同时使用二者。 同时使用这两个策略引擎配置文件夹重定向可能会导致意外行为。

高级文件夹重定向

在包含多个操作系统的部署中，您可能希望每个操作系统共享用户的某些配置文件。 其余配置文件则不共享，仅由一个操作系统使用。 要确保在各个操作系统间提供一致的用户体验，需要对每个操作系统进行不同的配置。 这就是高级文件夹重定向。 例如，在两个操作系统上运行的应用程序的不同版本可能需要读取或编辑一个共享文件，因此您决定将共享文件重定向到两个版本均可访问的一个网络位置。 或者，由于两个操作系统中的“开始”菜单文件夹内容在结构上有所不同，因此您决定仅重定向一个文件夹，而非两个文件夹。 这将分隔每个操作系统上的“开始”菜单文件夹及其内容，从而确保一致的用户体验。

如果您的部署需要高级文件夹重定向，则必须了解用户配置文件数据的结构，并确定配置文件的哪些部分可在操作系统间共享。 这一点非常重要，因为如果不正确使用文件夹重定向，可能会导致不可预测的行为。

在高级部署中重定向文件夹：

- 为每个操作系统使用单独的交付组。
- 了解虚拟应用程序（包括虚拟桌面上的虚拟应用程序），存储用户数据和设置的位置，并了解数据的结构。
- 对于可安全漫游（由于其结构在每个操作系统中均相同）的共享配置文件数据，请重定向每个交付组中的包含文件夹。
- 对于无法漫游的非共享配置文件数据，请仅重定向一个桌面组中的包含文件夹，通常选择使用最常用操作系统或其中的数据最相关的桌面组。 对于无法在操作系统间漫游的非共享数据，请重定向两个系统中的包含文件夹以分隔网络位置。

高级部署示例 - 此部署中的一些应用程序（包括 Microsoft Outlook 和 Internet Explorer 版本）运行在 Windows 8 桌面上，另一些应用程序（包括 Outlook 和 Internet Explorer 的其他版本）则由 Windows Server 2008 交付。 为实现此目的，您已为两个操作系统设置两个交付组。 用户希望在这两个应用程序的两个版本中访问同一组联系人和收藏夹。

重要：以下决策和建议对介绍的操作系统和部署有效。 在您的组织中，您选择重定向的文件夹以及是否决定共享这些文件夹取决于特定于您的具体部署的多种因素。

- 使用应用到交付组的策略选择下列要重定向的文件夹。

文件夹	已在 Windows 8 中重定向？	已在 Windows Server 2008 中重定向？
我的文档	是	是
应用程序数据	否	否
通讯录	是	是

© 1999-2017 Citrix Systems, Inc. All rights reserved.

文件夹	已在 Windows 8 中重定向？	已在 Windows Server 2008 中重定向？
桌面	是	否
下载	否	否
收藏夹	是	是
链接	是	否
我的音乐	是	是
我的图片	是	是
我的视频	是	是
搜索	是	否
保存的游戏	否	否
“开始”菜单	是	否

- 对于共享的重定向文件夹：
  - 在分析不同版本的 Outlook 和 Internet Explorer 保存的数据结构后，您确定可以安全共享“联系人”和“收藏夹”文件夹
  - 您知道“我的文档”、“我的音乐”、“图片收藏”和“我的视频”的结构在各个操作系统间均一致，因此将其存储在每个交付组的同一网络位置中非常安全
- 对于非共享的重定向文件夹：
  - 不重定向 Windows Server 交付组中的桌面、链接、搜索或“开始”菜单文件夹，因为这些文件夹中数据的组织结构在两个操作系统中有所不同。 因此无法共享。
  - 要确保此非共享数据的可预测行为，只能在 Windows 8 交付组中重定向此数据。 选择 Windows 8 而非 Windows Server 交付组是因为 Windows 8 在用户的日常工作中使用更频繁；他们只会偶尔访问服务器交付的应用程序。 另外，在此情况下，非共享数据与桌面环境而非应用程序环境更为相关。 例如，桌面快捷方式存储在“桌面”文件夹中，如果它们源自 Windows 8 计算机而非 Windows Server 计算机，则可能非常有用。
- 对于非重定向的文件夹：
  - 您不希望使存储用户下载文件的服务器变得混乱，因此您选择不重定向“下载”文件夹
  - 来自单独应用程序的数据可能导致兼容性和性能问题，因此您决定不重定向“应用程序数据”文件夹

有关文件夹重定向的详细信息，请参阅 http://technet.microsoft.com/en-us/library/cc766489%28v=ws.10%29.aspx。

文件夹重定向和排除

在 Citrix Profile Management（而非 Studio）中，一项性能增强功能可防止使用排除处理文件夹。如果使用此功能，请不要排除任何重定向文件夹。文件夹重定向和排除功能配合使用，因此确保未排除重定向文件夹，可在您稍后决定不重定向这些文件夹时，让 Profile Management 再次将其移回配置文件的文件夹结构，同时保持数据完整性。有关排除的详细信息，请参阅包

© 1999-2017 Citrix Systems, Inc. All rights reserved.

含和排除项目。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix Insight Services

Dec 05, 2017

Citrix Insight Services (CIS) 是用于性能监测、遥测以及生成业务洞察的 Citrix 平台。通过其性能监测和遥测功能，技术用户（客户、合作伙伴和工程师）就可以自行诊断和修复问题并优化其环境。有关 CIS 及其工作原理的最新详细信息，请访问 https://cis.citrix.com（需要 Citrix 帐户凭据）。

Citrix Insight Services 提供的功能继续增强和发展，现在已成为 Citrix Smart Tools 的不可或缺部分。借助 Smart Tools，您可以自动执行部署任务、运行状况检查和电源管理。有关这些技术的信息，请参阅 Citrix Smart Tools 文档。

上载到 Citrix 的所有信息均用于故障排除和诊断问题，以及提高产品的质量、可靠性和性能，对这些信息的使用将遵循以下策略：

- 位于 https://cis.citrix.com/legal 的 Citrix Insight Services 策略
- 位于 http://www.citrix.com/about/legal/privacy.html 的 Citrix 隐私政策

此 XenApp 和 XenDesktop 版本支持以下工具和技术。

- XenApp 和 XenDesktop 安装和升级分析
- Citrix 客户体验改善计划
- Citrix Smart Tools
- Citrix Call Home（Citrix Smart Tools 的一部分）
- Citrix Scout

安装和升级分析

当您使用完整产品安装程序部署或升级 XenApp 或 XenDesktop 组件时，将在安装/升级组件的计算机上收集和存储有关安装过程的匿名信息。这些数据用于帮助 Citrix 改善其客户的安装体验。有关详细信息，请参阅 http://more.citrix.com/XD-INSTALLER。

该信息以本地方式存储在 %ProgramData%\Citrix\CTQs 下面。

在完整产品安装程序的图形界面和命令行接口中，默认启用自动上载该数据。

- 可以在注册表设置中更改该默认值。如果在安装/升级之前更改注册表设置，则将在使用完整产品安装程序时使用该值。
- 如果使用命令行接口进行安装/升级，可以通过在命令中指定选项来覆盖该默认设置。

控制自动上载安装/升级分析数据的注册表设置（默认值为 1）：

位置：HKLM:\Software\Citrix\MetaInstall
名称：SendExperienceMetrics
值：0 = 已禁用，1 = 已启用

使用 PowerShell 时，以下 cmdlet 禁用自动上载安装/升级分析数据：

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name SendExperienceMetrics -PropertyType DWORD -Value 0
```

要在 XenDesktopServerSetup.exe 或 XenDesktopVDASetup.exe 命令中禁用自动上载，请包含 /disableexperiencemetrics 选

© 1999-2017 Citrix Systems, Inc. All rights reserved.

项。

要在 XenDesktopServerSetup.exe 或 XenDesktopVDASetup.exe 命令中启用自动上载，请包含 /sendexperiencemetrics 选项。

Citrix 客户体验改善计划 (CEIP)

当您参与 Citrix 客户体验改善计划 (CEIP) 时，将向 Citrix 发送匿名的统计数据和使用情况信息，帮助 Citrix 提高 Citrix 产品的质量和性能。有关详细信息，请参阅 http://more.citrix.com/XD-CEIP。

创建或升级站点期间注册

（安装了第一个 Delivery Controller 后）在创建 XenApp 或 XenDesktop 站点时，您会自动在 CEIP 中注册。大约会在您创建站点七天后上载第一个数据包。您可以在创建站点后随时停止参与此计划。为此，请在 Studio 导航窗格中选择**配置**节点，并按相应说明操作。

在升级 XenApp 或 XenDesktop 部署时：

- 如果从不支持 CEIP 的版本升级，系统将询问您是否要参与此计划。
- 如果从支持 CEIP 的版本升级，且已启用计划参与功能，则将在升级后启用 CEIP。
- 如果从支持 CEIP 的版本升级，且已禁用计划参与功能，则将在升级后的 Web 站点中禁用 CEIP。
- 如果从支持 CEIP 的版本升级，且计划参与情况未知，则系统会询问您是否要参与计划。

所收集的信息是匿名的，因此在上载到 Citrix Insight Services 之后无法查看。

安装 VDA 时注册

默认情况下，安装 Windows VDA 时您会自动在 CEIP 中注册。可以在注册表设置中更改此默认设置。如果在安装 VDA 之前更改注册表设置，则将使用该值。

控制 CEIP 中的自动注册的注册表设置（默认值为 1）：

位置：HKLM:\Software\Citrix\Telemetry\CEIP
名称：已启用
值：0 = 已禁用，1 = 已启用

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
```

大约在您安装 VDA 七天后第一次上载数据。

安装其他产品和组件时注册

您也可以在安装相关 Citrix 产品、组件和技术（如 Provisioning Services、AppDNA、Citrix 许可证服务器、Citrix Receiver for Windows、通用打印服务器和 Session Recording）时参与 CEIP 计划。请参阅这些产品、组件和技术的文档，以了解有关其安装和计划参与过程的默认设置的详细信息。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix Smart Tools

安装 Delivery Controller 时可以启用 Smart Tools 访问。

默认情况下选择启用 Smart Tools 访问的选项（及参与 Call Home，如果未启用）。单击**连接**。此时将打开浏览器窗口并自动导航到 Smart Services Web 页面，您在此页面输入您的 Citrix Cloud 帐户凭据。（如果您没有 Citrix Cloud 帐户，只需输入您的 Citrix 帐户凭据，系统会自动为您创建新的 Citrix Cloud 帐户。）您通过身份验证后，系统会在 Smart Tools 代理目录中无提示安装证书。

要使用 Smart Tools 技术，请参阅 Smart Tools 文档。

Citrix Call Home

在安装 XenApp 或 XenDesktop 的某些组件和功能时，您可以选择是否参与 Citrix Call Home。Call Home 会收集诊断数据，然后定期将包含该数据的遥测包直接上载到 Citrix Insight Services（在默认端口 443 上通过 HTTPS）以进行分析和故障排除。

在 XenApp 和 XenDesktop 中，Call Home 作为一个后台服务以名称 Citrix Telemetry Service 运行。有关详细信息，请参阅 http://more.citrix.com/XD-CALLHOME。

Citrix Scout 中也提供 Call Home 计划功能。有关详细信息，请参阅 Citrix Scout。

收集内容

Citrix 诊断工具 (CDF) 将跟踪可用于执行故障排除的日志信息。Call Home 将收集 CDF 跟踪信息子集，此信息有助于排除常见故障，例如 VDA 注册和应用程序/桌面启动。此技术称为“始终启用跟踪”(AOT)。Call Home 不会收集任何其他 Event Tracing for Windows (ETW) 信息，也无法在经过配置后执行此类操作。

Call Home 还会收集其他一些信息，如：

- 由 XenApp 和 XenDesktop 在 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix 下创建的注册表项
- 位于 Citrix 命名空间下的 Windows Management Instrumentation (WMI) 信息
- 正在运行的进程的列表
- Citrix 进程的存储于 %PROGRAM DATA%\Citrix\CDF 中的崩溃转储

在收集跟踪信息时将压缩此信息。Citrix Telemetry Service 最多保留 10 MB 压缩后的近期跟踪信息，最长时间期限为 8 天。

- 通过压缩数据，Call Home 可在 VDA 中占用较少的空间。
- 跟踪信息保留在内存中，以避免在置备的计算机上发生 IOP。
- 跟踪缓冲区采用循环机制在内存中保留跟踪信息。

HTM [Call Home 关键数据点]

Call Home collects these key datapoints.

配置和管理摘要

可以在使用完整产品安装向导期间注册 Call Home，也可在以后使用 PowerShell cmdlet 进行此注册。您注册后，默认情况下，会在当地时间每个星期日大约凌晨 3:00 收集诊断信息并上载到 Citrix。上载将从指定的时间开始在两小时的时间间隔内随机进行。这意味着使用默认计划执行的上载操作会在凌晨 3:00 和 5:00 之间发生。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

如果您不想根据计划上载诊断信息（或者如果您希望更改计划），可以使用 PowerShell cmdlet 手动收集和上载诊断信息或将其存储在本地。

在注册按计划的 Call Home 上载时，以及手动向 Citrix 上载诊断信息时，必须提供 Citrix 帐户或 Citrix Cloud 凭据。Citrix 会将凭据更换为用于标识客户以及上载数据的上载令牌。凭据不会被保存。

上载时，系统会向与 Citrix 帐户关联的地址发送一封电子邮件。

必备条件

- 计算机必须运行 PowerShell 3.0 或更高版本。
- 计算机上必须运行 Citrix Telemetry Service。
- 系统变量 PSModulePath 必须设置为 Telemetry 的安装路径，例如 C:\Program Files\Citrix\Telemetry Service\。

在组件安装期间启用 Call Home

在安装或升级 VDA 期间：在完整产品安装程序中使用图形用户界面安装或升级 Virtual Delivery Agent 时，系统会询问您是否希望参与 Call Home。有两种选择：

- 参与 Call Home。
- 不参与 Call Home。

如果您是升级 VDA 且以前注册了 Call Home，则不会显示该向导页面。

在安装或升级 Controller 期间：使用图形用户界面安装或升级 Delivery Controller 时，系统会询问您是否希望参与 Call Home 并连接到 Citrix Smart Tools。有三个选项：

- 连接到 Citrix Smart Tools，这包括通过 Smart Tools 代理实现的 Call Home 功能。这是默认的推荐选项。如果选择此选项，则将配置 Smart Tools 代理。（无论是否选择此选项，都将安装 Smart Tools 代理。）
- 仅参与 Call Home，但不连接到 Smart Tools。如果选择此选项，则将安装但不配置 Smart Tools 代理。Call Home 功能通过 Citrix Telemetry Service 和 Citrix Insight Services 提供。
- 不连接到 Smart Tools，也不参与 Call Home。

安装 Controller 时，如果服务器具有应用了策略设置“作为服务登录”的 Active Directory GPO，您将无法在安装向导中的 Call Home 页面上配置信息。有关详细信息，请参阅 CTX218094。

如果您是升级 Controller 且以前注册了 Call Home，则该页面中将仅显示有关 Smart Tools 的问题。如果您已注册了 Call Home 且已安装了 Smart 代理，则不会显示该向导页面。

有关 Smart Tools 的信息，请参阅 Smart Tools 文档。

PowerShell cmdlet

PowerShell 可帮助提供全面的语法，包括对并用于这些常见情况的 cmdlet 和参数的说明。

要使用代理服务器进行上载，请参阅配置代理服务器。

启用按计划上载

诊断收集信息会自动上载到 Citrix。如果没有为自定义计划输入其他 cmdlet，则会使用默认的计划。

```
$cred = Get-Credential
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
Enable-CitrixCallHome -Credential $cred
```

要确认已启用按计划上载，请输入 get-CitrixCallHome。此 cmdlet 应返回 IsEnabled=True 和 IsMasterImage=False。

为从主映像创建的计算机启用按计划上载

通过在主映像中启用按计划上载，无需对计算机目录中创建的每台计算机进行配置。

```
Enable-CitrixCallHome -Credential $cred -MasterImage
```

要确认已启用按计划上载，请输入 get-CitrixCallHome。此 cmdlet 应返回 IsEnabled=True 和 IsMasterImage=True。

创建自定义计划

为诊断收集和上载创建每天或每周计划。

```
$timespan = New-TimeSpan –Hours -Minutes
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek -UploadFrequency {Daily|Weekly}
```

取消按计划上载

取消按计划上载后，仍可以使用 PowerShell cmdlet 上载诊断数据。

```
Disable-CitrixCallHome
```

要确认已禁用按计划上载功能，请输入 get-CitrixCallHome。此 cmdlet 应返回 IsEnabled=False 和 IsMasterImage =False。

示例

以下 cmdlet 会创建一个在每天晚上 11:20 打包并上载数据的计划。请注意，Hours 参数采用 24 小时制时间。当 UploadFrequency 参数值为 Daily 时，将忽略 DayOfWeek 参数（如果已指定）。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

要确认计划，请输入 Get-CitrixCallHomeSchedule。在上面的示例中，此 cmdlet 应返回 StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency=Daily。

以下 cmdlet 会创建一个计划，在每个星期三晚上 11:20 上载数据。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed -UploadFrequency Weekly
```

要确认计划，请输入 Get-CitrixCallHomeSchedule。在上面的示例中，此 cmdlet 应返回 StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly。

配置代理服务器以完成 Call Home 上载

在启用了 Call Home 的计算机上完成以下任务。以下过程中的示例图中包含服务器地址和端口 10.158.139.37:3128。您的信息将会不同。

步骤 1. 在您的浏览器中添加代理服务器信息。在 Internet Explorer 中，依次选择 **Internet 选项 > 连接 > 局域网设置**。选择**为 LAN 使用代理服务器**并输入代理服务器地址和端口号。

步骤 2. 在 PowerShell 中，运行 **netsh winhttp import proxy source=ie**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
PS C:\Users\administrator.JLGXH> netsh winhttp import proxy source=ie

Current WinHTTP proxy settings:

    Proxy Server(s) :  10.108.124.245:8080
    Bypass List     :  (none)
```

步骤 3. 使用文本编辑器，编辑 TelemetryService.exe 配置文件，该文件位于 C:\Program Files\Citrix\Telemetry Service 中。添加下面的红框中显示的信息。



步骤 4. 重新启动 Telemetry Service。

在 PowerShell 中运行 Call Home cmdlet。

手动收集和上载诊断信息

可以使用 CIS Web 站点向 CIS 上载诊断信息包。也可以使用 PowerShell cmdlet 收集诊断信息并将其上载到 CIS。

要使用 CIS Web 站点上载包，请执行以下操作：

1. 使用 Citrix 帐户凭据登录到 Citrix Insight Services。
2. 选择 **My Workspace**（我的工作区）。
3. 选择**运行状况检查**，然后导航至您数据所在的位置。

CIS 支持多个用于管理数据上载操作的 PowerShell cmdlet。本文档介绍了用于两种常见情况的 cmdlet：

- 使用 Start-CitrixCallHomeUpload cmdlet 手动收集诊断信息包并将其上载到 CIS。（信息包不在本地保存。）
- 使用 Start-CitrixCallHomeUpload cmdlet 手动收集数据，并在本地存储诊断信息包。这使您能够预览数据。然后，在以后的时间里使用 Send-CitrixCallHomeBundle cmdlet 手动将该包的副本上载到 CIS。（您最初保存的数据仍会在本地保留。）

PowerShell 可帮助提供全面的语法，包括对并用于这些常见情况的 cmdlet 和参数的说明。

当您输入一个 cmdlet 以将数据上载到 CIS 时，系统会提示您确认此上载。如果在上载完成之前 cmdlet 超时，请在系统事件日志中检查上载操作的状态。如果服务已在执行上载操作，则上载请求可能会被拒绝。

收集数据并向 CIS 上载包

Start-CitrixCallHomeUpload [-Credential] [-InputPath] [-Description] [-IncidentTime] [-SRNumber] [-Name] [-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

UploadHeader] [-AppendHeaders] [-Collect] []

收集数据并将其保存在本地

Start-CitrixCallHomeUpload -OutputPath [-InputPath] [-Description] [-IncidentTime] [-SRNumber] [-Name] [-UploaderHeader] [-AppendHeaders] [-Collect] []

参数	说明
凭据	指示上载至 CIS。
InputPath	要包括在包内的 zip 文件的位置。这可能是 Citrix 支持部门要求提供的一个附加文件。请务必包括“.zip”扩展名。
OutputPath	将在其中保存诊断信息的位置。在本地保存 Call Home 数据时，此参数是必需的。
描述和事件时间	关于上载操作的自由形式的信息。
SRNumber	Citrix 技术支持事件编号。
名称	用于标识包的名称。
UploadHeader	JSON 格式的字符串，用于指定上载到 CIS 的上载标头。
AppendHeaders	JSON 格式的字符串，用于指定上载到 CIS 的附加标头。
Collect	JSON 格式的字符串，用于指定要收集或忽略的数据。采用 {'collector':{'enabled':Boolean}}" 形式，其中 Boolean 为 true 或 false。 有效的 collector 值为： • 'wmi' • 'process' • 'registry • "crashreport' • 'trace' • 'localdata' • 'sitedata' • 'sfb' 默认情况下，会启用除 'sfb' 之外的所有收集器。 'sfb' 收集器经过专门设计，可根据需求用于诊断 Skype for Business 问题。除 'enabled' 参数以外，'sfb' 收集器支持使用 'account' 和 'accounts' 参数来指定目标用户。使用以下一种形式： "-Collect "{'sfb':{'account':'domain\\user1'}}" -Collect "{'sfb':{'accounts':['domain\\user1', 'domain\\user2']}}"
常用参数	请参阅 PowerShell 帮助。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

上载以前在本地保存的数据

```
Send-CitrixCallHomeBundle -Credential -Path []
```

Path 参数可指定以前保存的包的位置。

示例

以下 cmdlet 会请求将 Call Home 数据上载（不包括从 WMI 收集器获取的数据）到 CIS。此数据（在下午 2:30 记录）与 PVS VDA 的失败注册相关，对应的 Citrix 支持案例编号为 123456。除了 Call Home 数据外，会将文件“c:\Diagnostics\ExtraData.zip”包含到上载包中。

```
C:\PS>Start-CitrixCallHomeUpload -InputPath "c:\Diagnostics\ExtraData.zip" -Description "Registration failures with PVS VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name "RegistrationFailure-021812016" -Collect "{'wmi':{'enabled':false}}" -UploadHeader "{'key1':'value1'}" -AppendHeaders "{'key2':'value2'}"
```

以下 cmdlet 可保存与 Citrix 支持案例编号 223344 相关的 Call Home 数据（在早上 8:15 记录）。该数据将保存在网络共享上的 mydata.zip 文件中。除 Call Home 数据外，还会将文件“c:\Diagnostics\ExtraData.zip”包含到保存的包中。

```
C:\PS>Start-CitrixCallHomeUpload -OutputPath \\mynetwork\myshare\mydata.zip -InputPath "c:\Diagnostics\ExtraData.zip" -Description "Diagnostics for incident number 223344" -IncidentTime "8:15" -SRNumber 223344
```

以下 cmdlet 可上载以前保存的数据包。

```
$cred=Get-Credential
C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \\mynetwork\myshare\mydata.zip
```

Citrix Scout

有关完整的详细信息，请参阅 Citrix Scout。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix Scout

Dec 05, 2017

在本文中：

- 简介
- 必备项和注意事项
- 收集诊断信息
- 跟踪和重现
- 计划收集

简介

Citrix Scout 收集可以用于在 XenApp 和 XenDesktop 部署中进行主动维护的诊断信息。Citrix 通过 Citrix Insight Services 提供综合的自动分析。您还可以使用 Scout 自己或在 Citrix Support 的指导下对问题进行故障排除。您可以将收集文件上载到 Citrix 以供分析及从 Citrix 支持获得指导。也可以将收集信息保存在本地供自己查看，以及以后将收集文件上载到 Citrix 以供分析。

Scout 提供三个主要过程：

- **收集**：在站点中所选计算机上运行一次性诊断信息收集。然后，将包含收集信息的文件上载到 Citrix 或保存在本地。
- **跟踪和重现**：在所选计算机上启动手动跟踪。然后，在这些计算机上重新创建问题。重现问题后，将停止跟踪。然后，Scout 将收集其他诊断信息并将包含跟踪和收集信息的文件上载到 Citrix 或保存在本地。
- **计划安排**：安排在所选计算机上在每天或每周的指定时间执行诊断信息收集。包含每次收集信息的文件会自动上载到 Citrix。

本文所述图形界面是使用 Scout 的主要方式。也可以使用 PowerShell 界面配置一次性或计划的诊断信息收集和上载。请参阅 Call Home。

Scout 运行位置：

- 在本地 XenApp 和 XenDesktop 部署中，从 Delivery Controller 运行 Scout 来捕获一个或多个 Virtual Delivery Agent (VDA) 和 Delivery Controller 中的诊断信息。还可以从 VDA 运行 Scout 来收集本地诊断信息。
- 在使用 XenApp and XenDesktop Service 的 Citrix Cloud 环境中，从 VDA 运行 Scout 来收集本地诊断信息。

收集内容

Scout 收集的诊断信息包括 Citrix Diagnostic Facility (CDF) 跟踪日志文件。还包括称为 AlwaysOn 跟踪 (AOT) 的一部分 CDF 跟踪。对常见问题（例如，VDA 注册和应用程序/桌面启动）进行故障排除时，AOT 信息很有用。系统不会收集任何其他 Event Tracing for Windows (ETW) 信息。

收集的信息包括：

- 由 XenApp 和 XenDesktop 在 HKEY_LOCAL_MACHINE\SOFTWARE\CITRIX 下创建的注册表项。
- 位于 Citrix 命名空间下的 Windows Management Instrumentation (WMI) 信息。
- 运行的进程。
- Citrix 进程的存储于 %PROGRAM DATA%\Citrix\CDF 中的故障转储。

关于跟踪信息：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 跟踪信息在收集时进行压缩处理，在计算机上占用空间较少。
- 在每台计算机上，Citrix Telemetry Service 最多保留 10 MB 压缩后的近期跟踪信息，最长时间期限为 8 天。
- 跟踪信息保留在内存中，以避免在置备的计算机上发生 IOP。
- 跟踪缓冲区采用循环机制在内存中保留跟踪信息。

有关 Scout 收集的数据点列表，请参阅 Scout 关键数据点。

必备项和注意事项

权限

- 您必须是要从中收集诊断信息的每台计算机的本地管理员和域用户。
- 必须对每台计算机上的 LocalAppData 目录具有写入权限。
- 启动 Scout 时使用**以管理员身份运行**。

对于要从中收集诊断信息的每台计算机：

- Scout 必须能够与计算机通信。
- 必须打开文件和打印机共享。
- 必须启用 PSRemoting 和 WinRM。计算机还必须运行 PowerShell 3.0 或更高版本。
- 计算机上必须运行 Citrix Telemetry Service。
- 要设置诊断信息收集的计划，计算机必须运行随 XenApp 和 XenDesktop 7.14 或受支持的更高版本随附的 Scout 版本。

Scout 在所选计算机上运行验证测试，以确保满足上述要求。

验证测试

在开始收集诊断信息之前，验证测试将针对选定的每台计算机自动运行。这些测试将确保满足上面列出的要求。如果某台计算机的测试失败，Scout 将显示一条消息，提供建议的更正措施。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Error message	Corrective action
Scout 无法访问此计算机	请确保： • 计算机已打开电源。 • 网络连接正确运行。（这可以包括验证您的防火墙是否已正确配置。） • 已打开文件和打印机共享。请参阅 Microsoft 文档以了解相关说明。
启用 PSRemoting 和 WinRM	可以同时启用 PowerShell 远程处理和 WinRM。使用“以管理员身份运行”选项，运行 **Enable-PSRemoting** cmdlet。有关详细信息，请参阅 Microsoft 帮助中的 cmdlet。
Scout 要求 PowerShell 3.0 (最低版本)	在计算机上安装 PowerShell 3.0（或更高版本），然后启用 PowerShell 远程处理。
无法访问此计算机上的 LocalAppData 目录	确保帐户对计算机上的 LocalAppData 目录具有写入权限。
找不到 Citrix Telemetry Service	确保 Citrix Telemetry Service 已在计算机上安装并启动。
无法获取计划	将计算机（最低）升级到 XenApp 和 XenDesktop 7.14。

版本兼容性

此版本的 Scout (3.x) 要在（最低）XenApp 和 XenDesktop 7.14 Controller 和 VDA 上运行。

早期 XenApp 和 XenDesktop 部署提供了早期版本的 Scout。有关早期版本的信息，请参阅 CTX130147。

如果将 7.14 之前的 Controller 或 VDA 升级到版本 7.14（或受支持的更高版本），早期版本的 Scout 会替换为当前版本。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Feature	Scout 2.23	Scout 3.0
支持 XenApp 和 XenDesktop 7.14（最低版本）	是	是
支持 XenDesktop 5.x、7.1 至 7.13	是	否
支持 XenApp 6.x、7.5 至 7.13	是	否
与产品一起提供	7.1 至 7.13	自 7.14 起
可以从 CTX 文章中下载	是	否
捕获 CDF 跟踪	是	是
捕获 AlwaysOn 跟踪 (AOT)	否	是
允许收集诊断数据	一次最多 10 台计算机（默认）	无限制（受资源可用性约束）
允许诊断数据发送到 Citrix	是	是
允许诊断数据保存在本地	是	是
支持 Citrix Cloud 凭据	否	是
支持 Citrix 凭据	是	是
支持使用代理服务器进行上载	是	是
调整计划	不适用	是
脚本支持	命令行（仅限本地 Controller）	使用 Call Home cmdlet 的 PowerShell（安装了遥测的任何计算机）

安装

默认情况下，安装 VDA 或 Controller 时，Scout 会自动作为 Citrix Telemetry Service 的一部分安装。

如果在安装 VDA 时忽略 Citrix Telemetry Service，或者以后删除了该服务，请运行 XenApp 或 XenDesktop ISO 中 x64\Virtual

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Desktop Components 或 x86\Virtual Desktop Components 文件夹中的 TelemetryServiceInstaller_xx.msi。

上载授权

如果您计划将诊断收集信息上载到 Citrix，必须有 Citrix 或 Citrix Cloud 帐户。（这些是访问 Citrix 下载或访问 Citrix Cloud 控制中心时使用的凭据。）验证了您的帐户凭据后，系统会发出令牌。

- 如果您使用 Citrix 帐户进行身份验证，发出令牌的过程不可见。您只需输入您的帐户凭据。Citrix 验证凭据后，您可以继续使用 Scout 向导。
- 如果您使用 Citrix Cloud 帐户进行身份验证，则单击链接访问 Citrix Cloud（在您的默认浏览器中使用 HTTPS）。输入您的 Citrix Cloud 凭据后，将显示令牌。请将令牌复制并粘贴到 Scout 中。然后您就可以继续使用 Scout 向导。

令牌存储在运行 Scout 的计算机本地。如果要下次使用该令牌，请选择**收集**或**跟踪和重现**，然后选中**存储令牌并在将来跳过此步骤**复选框。

您每次在 Scout 的打开页面上选择**计划**时都必须重新授权。创建或更改计划时不能使用存储的令牌。

使用代理进行上载

如果要使用代理服务器将收集信息上载到 Citrix，可以指示 Scout 使用为浏览器的 Internet 属性配置的代理设置，也可以指定代理服务器的 IP 地址和端口号。

收集诊断信息

收集过程包括选择计算机、开始收集诊断信息以及将包含收集信息的文件上载到 Citrix 或将其保存在本地。

步骤 1. 启动 Scout

从计算机的“开始”菜单依次选择：**Citrix > Citrix Scout**。在打开的页面上，单击**收集**。

步骤 2. 选择计算机

“选择计算机”页面上列出站点中的所有 VDA 和 Controller。可以按计算机名称过滤显示内容。选中要从中收集诊断信息的每台计算机旁边的复选框，然后单击**继续**。

Scout 将自动在选择的每台计算机上启动验证测试，确保计算机满足验证测试中所列的条件。如果验证失败，将在“状态”列中发布一条消息，且取消选中相应计算机的复选框。您可以执行下列操作之一：

- 解决问题，然后重新选中相应计算机的复选框。这将触发重试验证测试。
- 跳过相应的计算机（让其复选框处于取消选中状态）。系统将不会从该计算机收集诊断信息。

验证测试完成时，单击**继续**。

步骤 3. 从计算机收集诊断信息

摘要中列出将从中收集诊断信息的所有计算机（您选择的通过验证测试的计算机）。单击**开始收集**。

在收集期间：

- “状态”列指示计算机的当前收集状态。
- 要停止单台计算机上正在进行的收集，请在该计算机对应的“操作”列中单击**取消**。
- 要停止所有正在进行的收集，请单击页面右下角的**停止收集**。系统会保留已完成收集的计算机的诊断信息。要恢复收集，请

© 1999-2017 Citrix Systems, Inc. All rights reserved.

在每台计算机对应的“操作”列中单击**重试**。
- 完成所有选定计算机的收集时，右下角的**停止收集**按钮将变为**继续**。
- 如果某台计算机的收集已成功，而您要重新从该计算机收集诊断信息，请在该计算机的“操作”列中单击**重新收集**。较新的收集信息将覆盖较早的收集信息。
- 如果收集失败，可以在“操作”列中单击**重试**。仅成功完成的收集信息会上载或保存。
- 完成所有选定计算机的收集后，请勿单击**返回**。如果单击该按钮并确认提示，收集信息将会丢失。

收集完成时，单击**继续**。

步骤 4. 保存或上载收集信息

选择是将包含所收集诊断信息的文件上载到 Citrix，还是将其保存在本地计算机上。

如果选择立即上载该文件，请继续执行步骤 5。

如果选择在本地保存该文件：

- 将显示 Windows 的“保存”对话框。导航到所需位置。
- 完成本地保存时，将显示文件的路径名并提供链接。您可以查看该文件。您可以在以后从 Citrix 上载该文件；请参阅 CTX136396 了解 Citrix Insight Services，或参阅 Smart Tools 支持。

单击**完成**返回 Scout 的打开页面。在此过程中，不需要完成任何进一步的步骤。

步骤 5. 为上载验证身份及（可选）指定代理

有关此过程的详细信息，请查看上载授权。

- 如果您之前没有通过 Scout 进行身份验证，请继续执行此步骤。
- 如果您之前已通过 Scout 完成身份验证，默认使用存储的授权令牌。如果您没有问题，请选择此选项并单击**继续**。系统不会提示您为此收集提供凭据；继续执行步骤 6。
- 如果您之前已通过身份验证，但希望重新授权并让系统发出新令牌，请单击**更改/重新授权**并继续执行此步骤。

选择您要使用 Citrix 凭据还是 Citrix Cloud 凭据对上载进行身份验证。单击“继续”。仅当您不使用存储的令牌时才会显示凭据页面。

在凭据页面上：

- 如果要使用代理服务器进行文件上载，请单击**配置代理**。您可以指示 Scout 使用为浏览器的 Internet 属性配置的代理设置，也可以输入代理服务器的 IP 地址和端口号。关闭代理对话框。
- 对于 Citrix Cloud 帐户，请单击**生成令牌**。您的默认浏览器将启动并打开显示令牌的 Citrix Cloud 页面。请将令牌复制并粘贴到 Scout 页面中。
- 对于 Citrix 帐户，请输入您的凭据。

完成后，请单击**继续**。

步骤 6. 提供有关上载的信息

输入上载详细信息：

- 名称字段包含将包含所收集诊断信息的文件的默认名称。尽管您可以更改该名称，但这对于大多数收集来说应该足够了。（如果您删除默认名称，并使名称字段留空，系统将使用默认名称。）
- （可选）指定 8 位数的 Citrix 支持案例号。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 在可选的“说明”字段中，描述问题并指示问题的发生时间（如果适用）。

完成时，单击**开始上载**。

在上载期间，页面左下部分显示已完成的上载百分比近似值。要取消正在进行的上载，请单击**停止上载**。

上载完成时，将显示其位置的 URL 并提供链接。您可以访问该链接前往 Citrix 位置查看上载的分析情况，也可以复制该链接。

单击**完成**返回 Scout 的打开页面。

跟踪和重现

跟踪和重现过程包括选择计算机、在这些计算机上开始跟踪、在这些计算机上重现问题、完成诊断信息收集以及将包含跟踪和收集信息的文件上载到 Citrix 或将其保存在本地。

此过程与标准的收集过程类似。但是，您可以在计算机上开始跟踪，然后在这些计算机上重现问题。所有诊断信息收集包括 AOT 信息；此过程会添加 CDF 跟踪以帮助进行故障排除。

步骤 1. 启动 Scout

从计算机的“开始”菜单依次选择：**Citrix > Citrix Scout**。在打开的页面上，单击**跟踪和重现**。

步骤 2. 选择计算机

“选择计算机”页面上列出站点中的所有 VDA 和 Controller。可以按计算机名称过滤显示内容。选中要从中收集跟踪和诊断信息的每台计算机旁边的复选框，然后单击**继续**。

Scout 会在选择的每台计算机上启动验证测试，确保计算机满足验证测试中所列的条件。如果某台计算机的验证失败，将在“状态”列中发布一条消息，且取消选中该计算机的复选框。您可以执行下列操作之一：

- 解决问题，然后重新选中相应计算机的复选框。这将触发重试验证测试。
- 跳过相应的计算机（让其复选框处于取消选中状态）。系统将不会从该计算机收集诊断和跟踪信息。

验证测试完成时，单击**继续**。

步骤 3. 跟踪

摘要中列出将从中收集跟踪信息的所有计算机。单击**开始跟踪**。

在一台或多台选定的计算机上，重现遇到的问题。在您执行该操作时，跟踪收集操作继续进行。完成问题重现后，在 Scout 中单击**继续**。这将停止跟踪。

停止跟踪后，请指示是否在跟踪期间重现了问题。

步骤 4. 从计算机收集诊断信息

单击**开始收集**。

在收集期间：

- “状态”列指示计算机的当前收集状态。
- 要停止单台计算机上正在进行的收集，请在该计算机对应的“操作”列中单击**取消**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 要停止所有正在进行的收集，请单击页面右下角的**停止收集**。系统会保留已完成收集的计算机的诊断信息。要恢复收集，请在每台计算机对应的“操作”列中单击**重试**。
- 完成所有选定计算机的收集时，右下角的**停止收集**按钮将变为**继续**。
- 如果某台计算机的收集已成功，而您要重新从该计算机收集诊断信息，请在该计算机的“操作”列中单击**重新收集**。较新的收集信息将覆盖较早的收集信息。
- 如果收集失败，可以在“操作”列中单击**重试**。仅成功完成的收集信息会上载或保存。
- 完成所有选定计算机的收集后，请勿单击**返回**按钮。如果单击该按钮并确认提示，收集信息将会丢失。

收集完成时，单击**继续**。

步骤 5. 保存或上载收集信息

选择是将包含所收集诊断信息的文件上载到 Citrix，还是将其保存在本地计算机上。

如果选择立即上载该文件，请继续执行步骤 6。

如果选择在本地保存该文件：

- 将显示 Windows 的“保存”对话框。选择所需位置。
- 完成本地保存时，将显示文件的路径名并提供链接。您可以查看该文件。谨记：您可以在以后从 Citrix 上载该文件；请参阅 CTX136396 了解 Citrix Insight Services，或参阅 Citrix Smart Tools。

  单击**完成**返回 Scout 的打开页面。在此过程中，不需要完成任何进一步的步骤。

步骤 6. 为上载验证身份及（可选）指定代理

有关此过程的详细信息，请查看上载授权。

- 如果您之前没有通过 Scout 进行身份验证，请继续执行此步骤。
- 如果您之前已通过 Scout 完成身份验证，默认使用存储的授权令牌。如果您没有问题，请选择此选项并单击**继续**。系统不会提示您为此收集提供凭据；继续执行步骤 7。
- 如果您之前已通过身份验证，但希望重新授权并让系统发出新令牌，请单击**更改/重新授权**并继续执行此步骤。

  选择您要使用 Citrix 凭据还是 Citrix Cloud 凭据对上载进行身份验证。单击**继续**。仅当您不使用存储的令牌时才会显示凭据页面。

在凭据页面上：

- 如果要使用代理服务器进行文件上载，请单击**配置代理**。您可以指示 Scout 使用为浏览器的 Internet 属性配置的代理设置，也可以输入代理服务器的 IP 地址和端口号。关闭代理对话框。
- 对于 Citrix Cloud 帐户，请单击**生成令牌**。您的默认浏览器将启动并打开显示令牌的 Citrix Cloud 页面。请将令牌复制并粘贴到 Scout 页面中。
- 对于 Citrix 帐户，请输入您的凭据。

完成后，请单击**继续**。

步骤 7. 提供有关上载的信息

输入上载详细信息：

- 名称字段包含将包含所收集诊断信息的文件的默认名称。尽管您可以更改该名称，但这对于大多数收集来说应该足够了。（如果您删除默认名称，并使名称字段留空，系统将使用默认名称。）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- （可选）指定 8 位数的 Citrix 支持案例号。
- 在可选的“说明”字段中，描述问题并指示问题的发生时间（如果适用）。

完成时，单击**开始上载**。

在上载期间，页面左下部分显示已完成的上载百分比近似值。要取消正在进行的上载，请单击**停止上载**。

上载完成时，将显示其位置的 URL 并提供链接。您可以访问该链接前往 Citrix 位置查看上载的分析情况，也可以复制该链接。

单击**完成**返回 Scout 的打开页面。

计划收集

计划过程包括选择计算机以及设置或取消计划。计划的收集信息会自动上载到 Citrix。（您可以使用 PowerShell 界面在本地保存计划的收集信息。请参阅 Citrix Call Home。）

步骤 1. 启动 Scout

从计算机的“开始”菜单依次选择：**Citrix > Citrix Scout**。在打开的页面上，单击**计划**。

步骤 2. 选择计算机

“选择计算机”页面上列出站点中的所有 VDA 和 Controller。可以按计算机名称过滤显示内容。

使用图形界面安装 VDA 和 Controller 时，系统曾让您选择是否参与 Call Home。有关详细信息，请参阅 Citrix Call Home。（Call Home 具有相当于 Scout 的计划功能。）默认情况下，Scout 显示这些设置。可以使用此版本的 Scout 首次开始计划的收集，也可以更改以前配置的计划。

请注意，尽管您基于每台计算机启用/禁用了 Citrix Call Home，在 Scout 中设置计划时使用相同命令，却会影响选择的所有计算机。

选中要从中收集诊断信息的每台计算机旁边的复选框，然后单击**继续**。

Scout 会在选择的每台计算机上启动验证测试，确保计算机满足验证测试中所列的条件。如果某台计算机的验证失败，将在“状态”列中发布一条消息，且取消选中该计算机的复选框。您可以执行下列操作之一：

- 解决问题，然后重新选中相应计算机的复选框。这将触发重试验证测试。
- 跳过相应的计算机（让其复选框处于取消选中状态）。将不会从该计算机收集诊断（或跟踪）信息。

验证测试完成时，单击**继续**。

摘要页面上列出将应用计划的计算机。单击**继续**。

步骤 3. 设置计划

指示要何时收集诊断信息。谨记：计划会影响所有选定计算机。

- 要为选定计算机配置每周计划，请单击**每周**。选择星期几，并输入开始收集诊断信息的一天中的时间（24 小时制）。
- 要为选定计算机配置每天计划，请单击**每天**。输入开始收集诊断信息的一天中的时间（24 小时制）。
- 要为选定计算机取消现有计划（且不替换为其他计划），请单击**关闭**。这将取消之前为这些计算机配置的任何计划。

单击**继续**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

步骤 4. 为上载验证身份及（可选）指定代理

有关此过程的详细信息，请查看上载授权。谨记：使用 Scout 计划时，不能使用存储的令牌进行身份验证。

选择您要使用 Citrix 凭据还是 Citrix Cloud 凭据对上载进行身份验证。单击**继续**。

在凭据页面上：

- 如果要使用代理服务器进行文件上载，请单击配置代理。您可以指示 Scout 使用为浏览器的 Internet 属性配置的代理设置，也可以输入代理服务器的 IP 地址和端口号。关闭代理对话框。
- 对于 Citrix Cloud 帐户，请单击**生成令牌**。您的默认浏览器将启动并打开显示令牌的 Citrix Cloud 页面。请将令牌复制并粘贴到 Scout 页面中。
- 对于 Citrix 帐户，请输入您的凭据。

完成后，请单击**继续**。

查看配置的计划。单击**完成**返回 Scout 的打开页面。

进行每个计划的收集时，每个选定计算机的 Windows 应用程序日志都会包含有关收集和上载的条目。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

监视

Dec 05, 2017

管理员和技术支持人员可以使用各种功能和工具监视 XenApp 和 XenDesktop 站点。使用这些工具，您可以监视

- 用户会话和会话使用情况
- 登录性能
- 连接和计算机，包括失败情况
- 负载评估
- 历史趋势
- 基础结构

Citrix Director

Director 是一款实时 Web 工具，您可以利用此工具进行监视和排除故障以及为最终用户执行支持任务。

有关详细信息，请参阅 Director 一文。

会话录制

通过 Session Recording，您可以在遵守公司政策和法规的前提下，从运行 XenApp 的任意服务器通过任意类型的连接录制任意用户会话的屏幕活动。Session Recording 对会话进行记录、编录和存档，以便进行检索和播放。

Session Recording 使用灵活的策略自动触发应用程序会话的录制。这样就可以使 IT 能够监视和检查应用程序（如金融运营和医疗患者信息系统）的用户活动，在遵守法规和安全监视方面加强内部控制。同样，Session Recording 也通过加快问题识别及问题解决时间在技术支持方面予以帮助。

有关详细信息，请参阅 Session Recording 一文。

配置日志记录

利用配置日志记录功能，管理员可以跟踪对站点所做的管理更改。配置日志记录可以帮助管理员诊断和排除配置更改后出现的问题，辅助进行变更管理和跟踪配置，并报告管理活动。

您可以从 Studio 查看和生成关于已记录信息的报告。还可以在 Director 中使用 Trend View 界面查看记录的项目，以提供配置更改通知。此功能对不具有 Studio 访问权限的管理员很有用。

Trends View 提供一段时间内的配置更改历史数据，使管理员可以访问对站点所做的更改、更改时间和执行更改的人员，以便查找问题的原因。此视图将配置信息细分为三类。

- 连接失败
- 出现故障的桌面计算机
- 出现故障的服务器计算机

有关如何启用和配置“配置日志记录”的详细信息，请参阅配置日志记录一文。Director 一文介绍如何通过该工具查看记录的信息。

事件日志

XenApp 和 XenDesktop 服务记录发生的事件。事件日志可以用于对操作进行监视和故障排除。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

有关详细信息，请参阅事件日志一文。各功能文章可能也包含某些事件信息。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

会话录制

Dec 05, 2017

通过 Session Recording，您可以在遵守公司政策和法规的前提下，通过任意类型的连接录制从 VDA for Server OS 或 VDA for Desktop OS 托管的任何用户会话的屏幕活动。Session Recording 对会话进行记录、编录和存档，以便进行检索和播放。

Session Recording 使用灵活的策略自动触发应用程序会话的录制。这样， IT 就可以监视和检查应用程序（如金融运营和医疗患者信息系统）的用户活动，在遵守法规和安全监视方面加强内部控制。同样，Session Recording 也通过加快问题识别及问题解决时间在技术支持方面予以帮助。

优势

通过日志记录和监视增强安全性。 Session Recording 允许组织录制处理敏感信息的应用程序屏幕上的用户活动。这对于医疗和金融等管制行业来说尤为重要。其中包括禁止录制的个人信息，策略控制允许进行选择性录制。

强大的活动监视。 Session Recording 可捕获并存档屏幕更新，包括鼠标活动和安全视频录制中可见的按键输出，从而记录特定用户、应用程序及服务器的活动。

Session Recording 并非为收集法律诉讼证据而设计的。Citrix 建议使用 Session Recording 的组织使用其他技术进行证据收集，例如传统的视频录制，结合传统的以文字为基础的 eDiscovery 工具。

更快地解决问题。 用户向技术支持致电的问题是难以重现的问题时，客服人员可启用用户会话记录。再次出现该问题时，Session Recording 会提供该错误的带时间戳的影像记录，之后该记录可用于更加快速地进行故障排除。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Session Recording 入门

Dec 05, 2017

执行以下步骤之后，即可开始录制和查看 XenApp 和 XenDesktop 会话。

1. 熟悉 Session Recording 组件。
2. 选择适用于您的环境的部署方案。
3. 验证安装要求。
4. 安装 Windows 角色和功能必备项。
5. 安装 Session Recording。
6. 配置 Session Recording 组件以允许录制和查看会话。

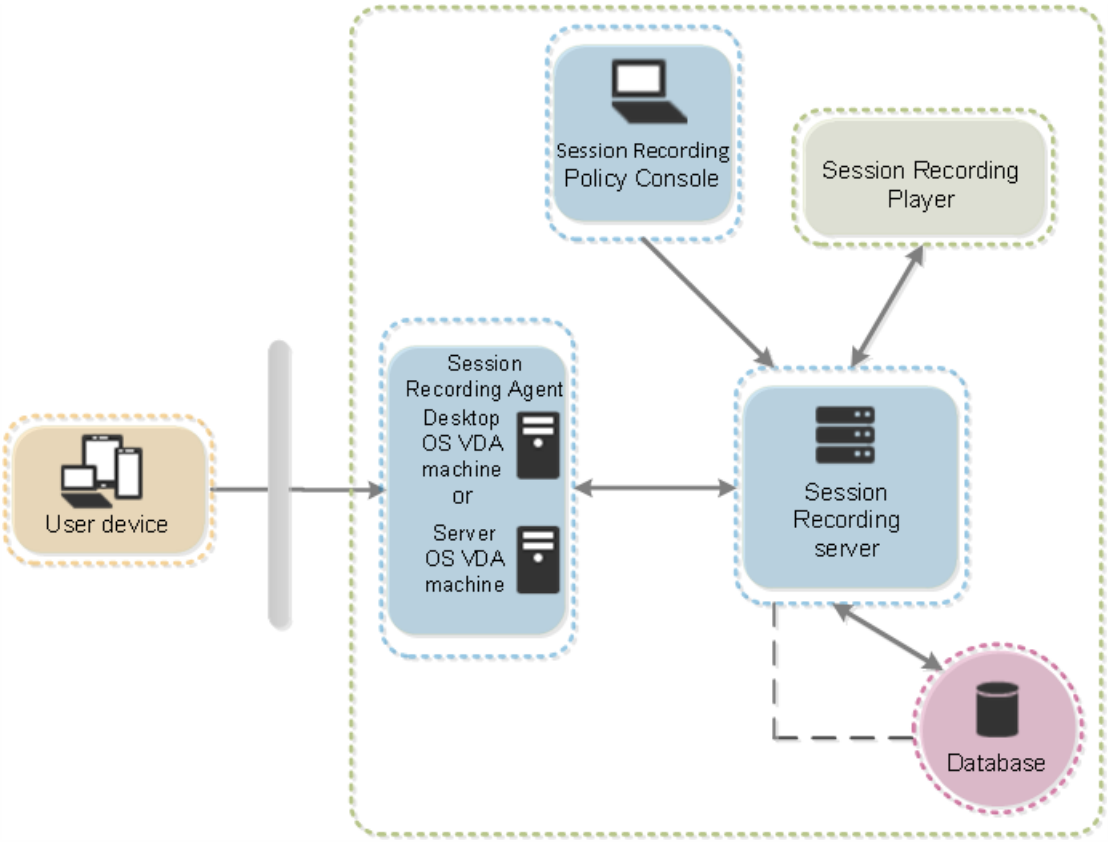
Session Recording 包括 5 个组件：

- **Session Recording Agent**。安装在每个 VDA for Server OS 或 VDA for Desktop OS 上的组件，用于支持录制。负责录制会话数据。
- **Session Recording Server**。用于托管以下各项的服务器：
  - Broker。IIS 6.0+ 托管的 Web 应用程序，可处理 Session Recording Player 发出的搜索查询和文件下载请求，处理 Session Recording 策略控制台发出的策略管理请求，以及评估每个 XenApp 和 XenDesktop 会话的录制策略。
  - 存储管理器。管理从每个已启用 Session Recording 且运行 XenApp 和 XenDesktop 的计算机接收到的录制会话文件的 Windows 服务。
  - 管理员日志记录。随 Session Recording Server 一起安装的可选子组件，用于记录管理活动。所有的日志记录数据均存储在名称为 **CitrixSessionRecordingLogging** 的单独的 SQL Server 数据库中。
- **Session Recording Player**。一种用户界面，用户可从工作站进行访问以播放录制的 XenApp 和 XenDesktop 会话文件。
- **Session Recording 数据库**。管理 SQL Server 数据库的组件，用于存储录制的会话数据。安装此组件后，它会创建一个名为 **CitrixSessionRecording** 的数据库。此名称无法更改。
- **Session Recording 策略控制台**。用于创建策略以指定要录制的会话的控制台。

下图显示了 Session Recording 的各个组件以及各组件之间的关系：

在此处显示的部署示例中，Session Recording Agent、Session Recording Server、Session Recording 数据库、Session Recording 策略控制台以及 Session Recording Player 均位于安全防火墙后面。Session Recording Agent 安装在 VDA for Server OS 或 VDA for Desktop OS 上。第二台服务器用于托管 Session Recording 策略控制台，第三台服务器用作 Session Recording Server，第四台服务器用于托管 Session Recording 数据库。Session Recording Player 安装在工作站上。位于防火墙外的客户端设备与安装了 Session Recording Agent 的 VDA for Server OS 进行通信。在防火墙内部，Session Recording Agent、Session Recording 策略控制台、Session Recording Player 以及 Session Recording 数据库都与 Session Recording Server 进行通信。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

计划部署

Dec 05, 2017

限制和注意事项

Session Recording 不支持桌面组合重定向 (DCR) 显示模式。默认情况下，如果要通过录制策略来录制会话，则 Session Recording 会在该会话中禁用 DCR。您可以在 Session Recording Agent Properties 中配置该行为。

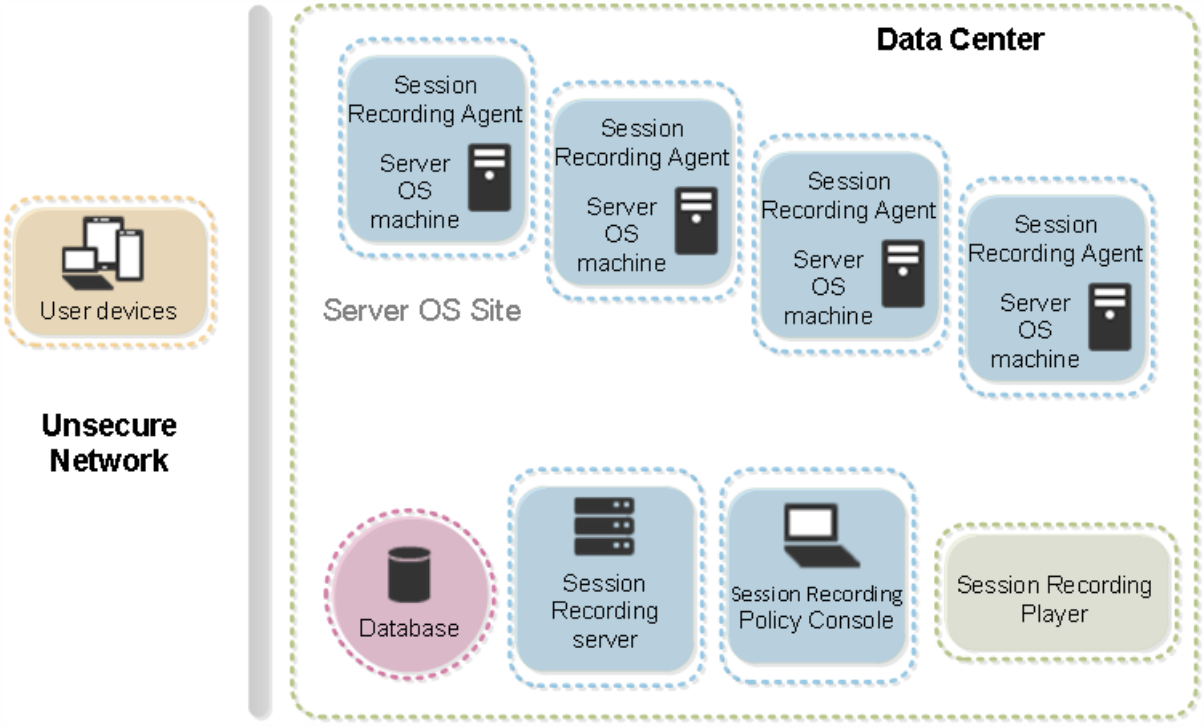
可以通过不同的方案对 Session Recording 组件进行部署，具体取决于您的环境。

Session Recording 部署不必限制为单个站点。除 Session Recording Agent 外， 其他所有组件均独立于服务器站点。 例如，您可以配置多个站点使用单个 Session Recording Server。

或者，如果您 拥有包含多个代理的大型站点，并计划录制许多图形密集型 应用程序（例如，AutoCAD 应用程序），或者您有许多会话要 录制，则可能对 Session Recording Server 具有较高性能要求。要 缓解性能问题，可以在不同的计算机上安装多个 Session Recording Server，并将 Session Recording Agent 指向这些 不同的计算机。请谨记，一次只能将一个代理指向一台 服务器。

建议的服务器站点部署

此类部署用于录制一个或多个站点的会话。在站点中的每个 VDA for Server OS 上安装 Session Recording Agent。站点位于安全防火墙后面的数据中心。Session Recording Administration 组件（Session Recording 数据库、Session Recording Server、Session Recording 策略控制台）安装在其他服务器上，Session Recording Player 安装在工作站上，全部位于防火墙后面，而非位于数据中心中。XenApp 客户端（例如工作站、移动设备以及便携式计算机）位于防火墙之外的不安全网络环境中。



重要部署注意事项

- 为使 Session Recording 组件能够互相通信，请确保将这些组件安装在同一个域中，或者能够相互传递信任关系的不同可信域中。不能将系统安装在工作组中，也不能跨具有外部信任关系的域进行安装。
- 由于播放大型录制件时图形比较密集，并且内存使用率高，Citrix 建议不要将 Session Recording Player 作为已发布应用程序

© 1999-2017 Citrix Systems, Inc. All rights reserved.

进行安装。

- 为 Session Recording 安装配置 TLS/HTTPS 通信。确保在 Session Recording Server 上安装证书，并且根证书颁发机构 (CA) 在 Session Recording 组件上受信任。
- 如果在运行 SQL Server 2016 Express Edition、SQL Server 2014 Express Edition、SQL Server 2012 Express Edition 或 SQL Server 2008 R2 Express Edition 的独立服务器上安装 Session Recording 数据库，该服务器必须启用 TCP/IP 协议，且必须运行 SQL Server Browser 服务。默认情况下，禁用这些设置，但必须启用它们才能使 Session Recording Server 与数据库进行通信。有关启用这些设置的信息，请参阅 Microsoft 文章为 SQL Server 启用 TCP/IP 网络协议和 SQL Server Browser 服务。
- 规划 Session Recording 部署时，请考虑会话共享的效果。已发布应用程序的会话共享可能会与已发布应用程序的 Session Recording 策略规则相冲突。Session Recording 将活动策略与用户打开的第一个已发布应用程序相匹配。用户打开第一个应用程序之后，随后在同一会话中打开的任何应用程序都将继续遵循对第一个应用程序有效的策略。例如，如果某策略指出只应录制 Microsoft Outlook，则录制将在用户打开 Outlook 时开始。不过，如果用户接着打开已发布的 Microsoft Word（在 Outlook 运行时），也会对 Word 进行录制。相反，如果活动策略没有指定应该对 Word 进行录制，并且用户在启动 Outlook（根据策略应进行录制）之前启动 Word，则不会对 Outlook 进行录制。
- 尽管可以在 Delivery Controller 上安装 Session Recording Server，但 Citrix 不建议这么做，因为这会带来性能问题。
- 您可以在 Delivery Controller 上安装 Session Recording 策略控制台。
- 您可以在同一个系统上同时安装 Session Recording Server 和 Session Recording 策略控制台。
- 请确保 Session Recording Server 的 NetBIOS 名称不超过 15 个字符的限制（Microsoft 对主机名长度设置了 15 个字符的限制）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

安全性建议

Dec 05, 2017

Session Recording 可以部署在一个安全网络中，并由管理员进行访问，因此，Session Recording 非常安全。即开即用部署设计为简单易用，且具有可选择性配置的数字签名和加密等安全功能。

Session Recording 组件之间的 通信通过 Internet Information Services (IIS) 以及 Microsoft 消息队列 (MSMQ) 实现。IIS 在每个 Session Recording 组件 之间提供网络服务通信链接。MSMQ 提供了 可靠的数据传输机制，可用于从 Session Recording Agent 向 Session Recording Server 发送录制的会话数据。

> **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。

规划部署时，请考虑如下 安全性建议：

- 确保正确隔离企业网络、Session Recording 系统和单台计算机上的不同管理员角色。否则，可能会引发安全威胁，进而可能影响系统功能或导致滥用系统。Citrix 建议将不同的管理员角色分配给不同的人员或帐户，并且不允许常规会话用户拥有 VDA 系统的管理权限。
  - XenApp 和 XenDesktop 管理员不应为已发布应用程序或桌面的任何用户授予 VDA 本地管理员角色。如果必须授予本地管理员角色，请使用 Windows 机制或第三方解决方案保护 Session Recording Agent 组件。
  - 单独分配 Session Recording 数据库管理员和 Session Recording 策略管理员。
  - Citrix 建议您不要将 VDA 管理员权限分配给一般会话用户，特别是使用 Remote PC Access 时。
  - 必须严格保护 Session Recording Server 本地管理帐户的安全。
  - 控制对安装有 Session Recording Player 的计算机的访问权限。请勿向未获得播放器角色授权的用户授予任何播放器计算机的本地管理员角色。禁用匿名访问。
  - Citrix 建议使用物理计算机作为 Session Recording 的存储服务器。
- 无论数据敏感性如何，Session Recording 均会录制会话图形活动。在某些情形下，可能会不小心录制了敏感数据（包括但不限于用户凭据、隐私信息和第三方屏幕）。请采取以下措施以避免风险：

  + 除非出于具体故障排除的目的，否则请禁用 VDA 的核心内存转储。

    要禁用核心内存转储，请执行以下操作：

    1. 右键单击**我的电脑**，然后单击**属性**。
    2. 单击**高级**选项卡，然后单击**启动和恢复**下的**设置**。
    3. 在**写入调试信息**下选择 **(无)**。

    请参阅 Microsoft 文章 https://support.microsoft.com/zh-cn/kb/307973。

  + 会话所有者应通知与会者，在录制桌面会话时，可能会录制线上会议和远程协助软件。

  + 确保登录凭据或安全信息不会出现企业内部发布或使用的所有本地和 Web 应用程序中，也不会由 Session Recording 录制。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

+ 在切换到远程 ICA 会话之前，用户应关闭所有可能暴露敏感信息的应用程序。

+ 我们建议仅允许使用自动身份验证方法（例如单点登录、智能卡）访问已发布的桌面或软件即服务 (SaaS) 应用程序。

- Session Recording 需要某些硬件和硬件基础结构（例如企业网络设备、操作系统）才能正常运行并满足安全要求。在基础结构级别采取措施防止基础结构遭到损害或滥用，并保证 Session Recording 功能安全、可靠。
  - 正确保护支持 Session Recording 的网络基础结构并保证该基础结构始终可用。
  - Citrix 建议使用第三方安全解决方案或 Windows 机制来保护 Session Recording 组件。Session Recording 组件包括：
    - 在 Session Recording Server 上
      - 进程：SsRecStoragemanager.exe 和 SsRecAnalyticsService.exe
      - 服务：CitrixSsRecStorageManager 和 CitrixSsRecAnalyticsService
      - 所有文件均位于 Session Recording Server 安装文件夹中
      - 注册表项位于 HOTKEY_LOCAL_MACHINE\Software\Citrix\SmartAuditor\Server 下
    - 在 Session Recording Agent 上
      - 进程：SsRecAgent.exe
      - 服务：CitrixSmAudAgent
      - 所有文件均位于 Session Recording Agent 安装文件夹中
      - 注册表项位于 HOTKEY_LOCAL_MACHINE\Software\Citrix\SmartAuditor\Agent 下
- 在 Session Recording Server 上为消息队列 (MSMQ) 设置访问控制列表 (ACL) 以限制可向 Session Recording Server 发送 MSMQ 数据的 VDA 或 VDI 计算机，并防止未授权的计算机向 Session Recording Server 发送数据。

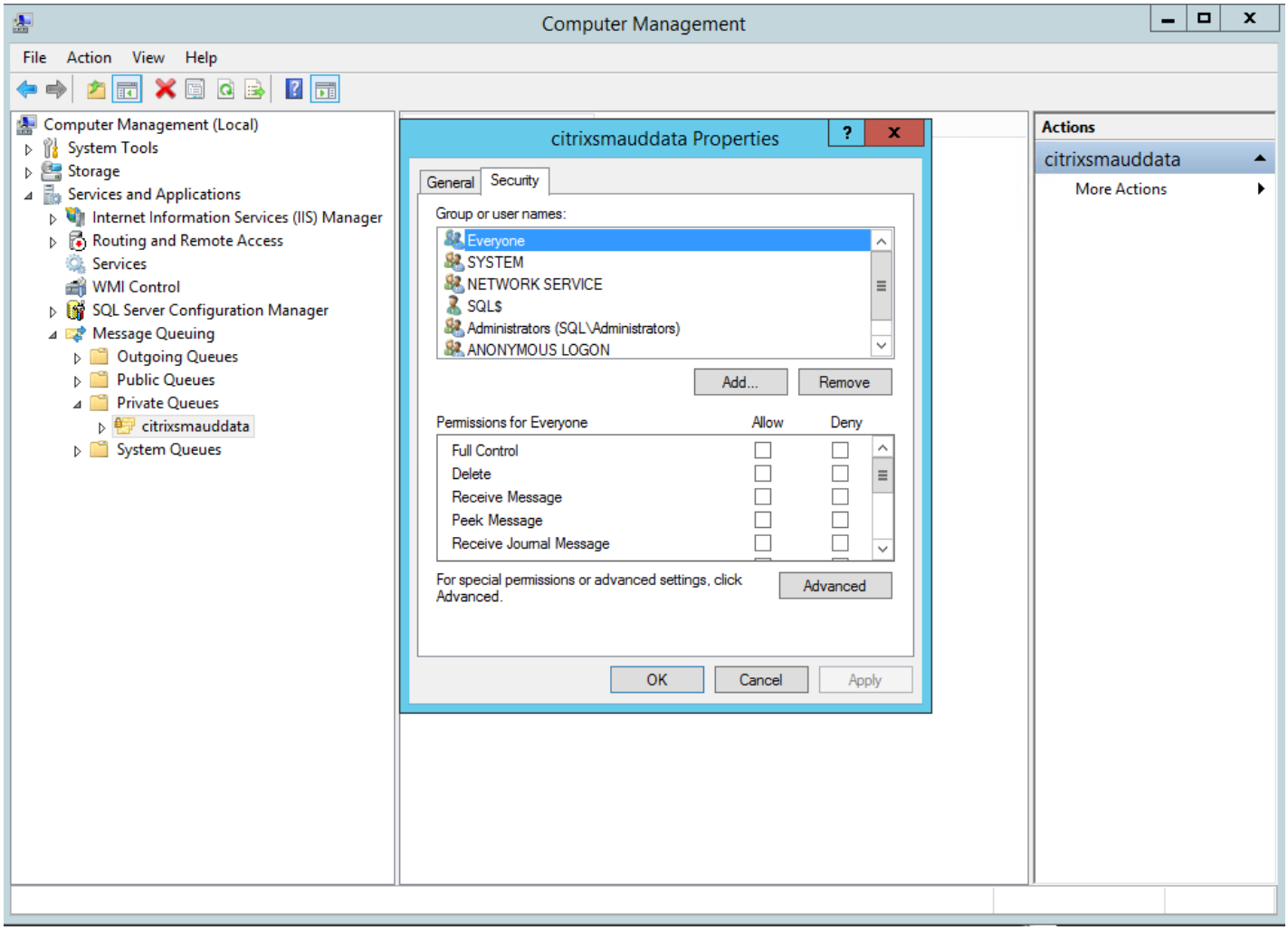
  1) 在启用了 Session Recording 的每个 Session Recording Server 以及 VDA 或 VDI 计算机上安装服务器功能目录服务器集成，然后重新启动消息队列服务。

  2) 从每个 Session Recording Server 上的 Windows **开始**菜单打开**管理工具** > **计算机管理**。

  3) 打开**服务和应用程序** > **消息队列** > **专用队列**。

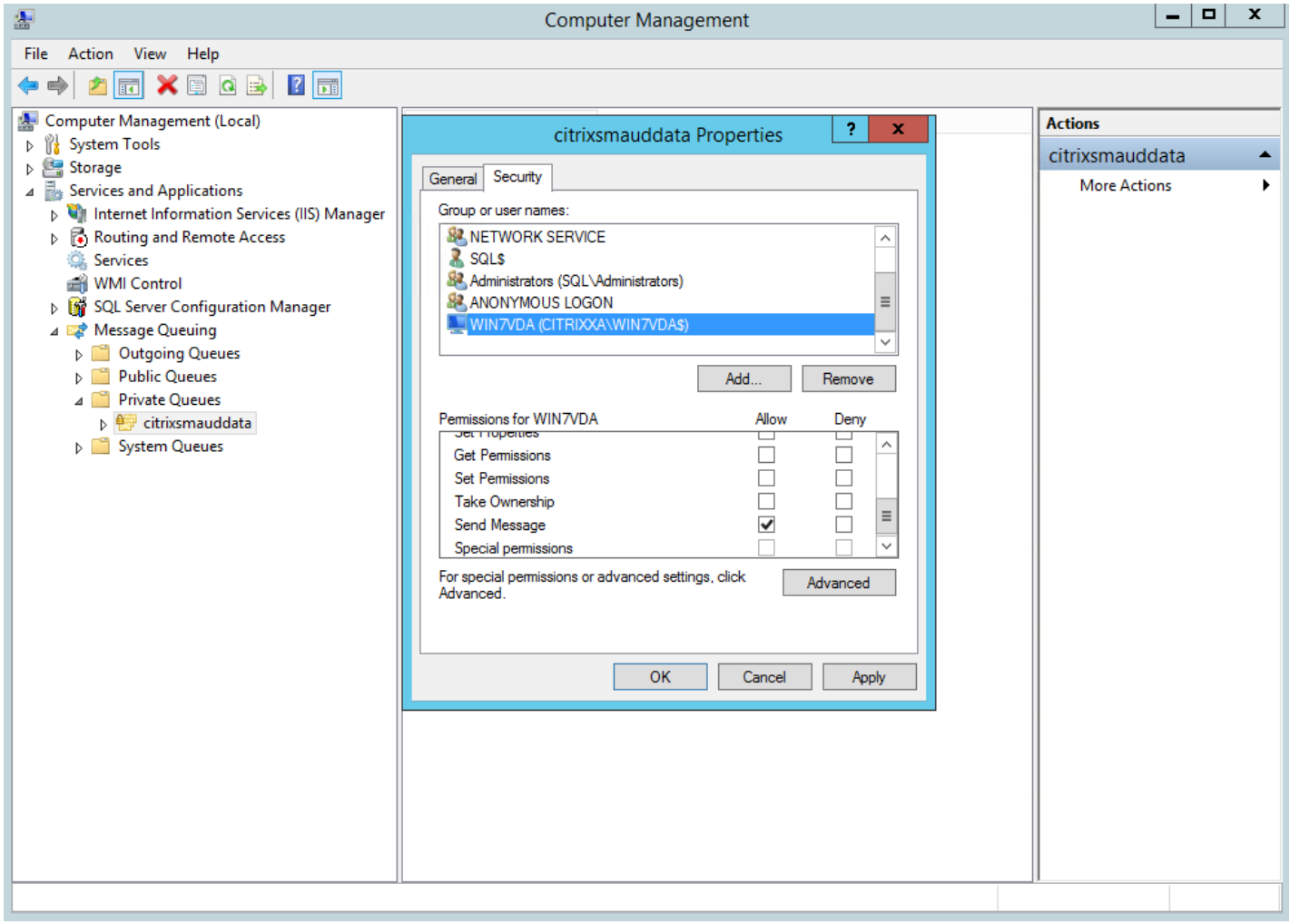
  4) 单击专用队列 **citrixsmauddata** 以打开**属性**页面，然后选择**安全性**选项卡。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5) 添加要向此服务器发送 MSMQ 数据的计算机或 VDA 安全组，并为其授予**发送消息**权限。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- 正确保护 Session Record Server 和 Session Recording Agent 的事件日志。建议使用 Windows 或第三方远程日志记录解决方案来保护事件日志，或者将事件日志重定向到远程服务器。
- 确保运行 Session Recording 组件的服务器在物理上是安全的。如有可能，请将这些计算机锁在一个安全的房间内，只有授权人员能够直接取用。
- 隔离在单独子网或域上运行 Session Recording 组件的服务器。
- 在 Session Recording Server 与其他服务器之间安装防火墙，防止访问其他服务器的用户访问录制的会话数据。
- 安装 Microsoft 提供的最新安全更新，保持 Session Recording Admin Server 和 SQL 数据库为最新版本。
- 限制非管理员登录到管理计算机。
- 严格限制授权人员更改录制策略及查看录制的会话。
- 安装数字证书，使用 Session Recording 文件签名功能，并在 IIS 中设置 TLS 通信。
- 通过将 **Session Recording Agent Properties** 中列出的 MSMQ 协议设置为 HTTPS，设置 MSMQ 使用 HTTPS 作为传输协议。有关详细信息，请参阅 MSMQ 故障排除。
- 在 Session Recording Server 和 Session Recording 数据库上使用 TLS 1.1 或 TLS 1.2（推荐）并禁用 SSLv2、SSLv3、TLS 1.0。有关详细信息，请参阅 Microsoft 文章 http://support.microsoft.com/default.aspx?scid=kb;en-us;187498。

在 Session Recording Server 和 Session Recording 数据库上禁用 TLS 的 RC4 密码套件：

1. 使用 Microsoft 组策略编辑器，导航到**计算机配置** > **管理模板** > **网络** > **SSL 配置设置**。
2. 将 **SSL 密码套件顺序**策略设置为**启用**。默认情况下，此策略设置为**未配置**。
3. 删除任何 RC4 密码套件。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 使用播放保护功能。播放保护是一项 Session Recording 功能，在文件下载到 Session Recording Player 前对文件进行加密。默认情况下，此选项处于启用状态，且位于 **Session Recording Server 属性**中。
- 按照加密密钥长度和加密算法的 NSIT 指南进行操作。
- 为 Session Recording 配置 TLS 1.2 支持。
  - Citrix 建议使用 TLS 1.2 作为通信协议，以确保 Session Recording 组件的端到端安全性。

  要配置 Session Recording 的 TLS 1.2 支持，请执行以下操作：

  1. 登录托管 Session Recording Server 的计算机，安装合适的 SQL Server 客户端组件和驱动程序，并为 .NET Framework（版本 4 或更高版本）设置强加密
     a. 为 SQL Server 安装 Microsoft ODBC 驱动程序 11（或更高版本）。
     b. 应用 .NET Framework 的最新修补程序汇总。
     c. 根据您的 .NET Framework 版本安装 ADO.NET - SqlClient。有关详细信息，请参阅 https://support.microsoft.com/en-us/kb/3135244。
     d. 在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NetFramework\v4.0.30319 和 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319 下添加 DWORD 值 SchUseStrongCrypto = 1。
     e. 重新启动计算机。
  2. 登录托管 Session Recording 策略控制台的计算机以应用 .NET Framework 的最新修补程序汇总，并为 .NET Framework（版本 4 或更高版本）设置强加密。用于设置强加密的方法与子步骤 1-d 和 1-e 相同。如果您选择在与 Session Recording Server 相同的计算机上安装 Session Recording 策略控制台，则可以忽略这些步骤。

要为 SQL Server 2016 之前的版本配置 TLS 1.2 支持，请参阅 https://support.microsoft.com/en-us/kb/3135244。要利用 TLS 1.2，请将 HTTPS 配置为 Session Recording 组件的通信协议。

有关配置 Session Recording 安全功能的信息，请参阅知识库文章 CTX200868。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

可扩展性注意事项

Dec 05, 2017

除运行 XenApp 所需的资源外，安装和运行 Session Recording 几乎不需要其他资源。但是，如果您计划使用 Session Recording 录制大量会话，或者如果您计划录制的会话会导致出现大量会话文件（例如，图形密集型应用程序），请在规划 Session Recording 部署时注意系统的性能。

有关构建高度可扩展的 Session Recording 系统的详细信息，请参阅 Citrix 文章 CTX200869。

硬件 建议

考虑要向每台 Session Recording Server 发送的数据量，以及服务器可以处理和存储此数据的速率。系统可以存储输入数据的速率必须快于数据输入速率。

要估算数据输入速率，请将录制的会话数乘以每个录制的会话的平均大小，然后除以录制会话所需的时间。例如，在 8 小时工作日中，您可能录制了 5,000 个 Microsoft Outlook 会话，每个会话的大小为 20MB。在这种情况下，数据输入速率大约为 3.5 Mbps。（5,000 个会话乘以 20MB，除以 8 小时，再除以每小时 3,600 秒。）

通过优化单个 Session Recording Server 的性能或在不同计算机上安装多个 Session Recording Server，可以提升性能。

磁盘和存储 硬件

磁盘和存储硬件是规划 Session Recording 部署时要考虑的最重要的因素。存储解决方案的写入性能尤为重要。数据写入磁盘的速度越快，系统的整体性能越高。

适合使用 Session Recording 的存储解决方案包括由本地磁盘控制器或连接的存储区域网络 (SAN) 作为 RAID 阵列控制的一组本地磁盘。

注意：由于存在与向网络驱动器写入录制数据有关的性能和安全问题，因此，请勿将 Session Recording 与网络连接存储 (NAS) 一起使用。
对于本地驱动器设置，具有内置缓存内存的磁盘控制器的性能会有所增强。缓存磁盘控制器必须具有电池备份装置，以在电源出现故障时确保数据完整性。

网络 容量

100Mbps 的网络链接适合连接 Session Recording Server。千兆位以太网连接可能会提高性能，但不会将性能比 100Mbps 链接提高 10 倍。

确保 Session Recording 不与可能会争夺可用网络带宽的第三方应用程序共享网络交换机。理想情况下，网络交换机专用于 Session Recording Server。

计算机 处理能力

对于安装了 Session Recording Server 的计算机，请考虑以下规格：

- 建议使用双 CPU 或双核 CPU
- 建议使用 4GB RAM

超过这些规格不会显著提高性能。

部署多台 Session Recording Server

© 1999-2017 Citrix Systems, Inc. All rights reserved.

如果单台 Session Recording Server 不满足性能要求，您可以在不同计算机上安装多台 Session Recording Server。 在此类型的部署中，每台 Session Recording Server 都具有其自己的专用存储、网络交换机以及数据库。 要分发负载，在部署中将 Session Recording Agent 指向不同的 Session Recording Server。

数据库 可扩展性

Session Recording 数据库要求使用 Microsoft SQL Server 2016、Microsoft SQL Server 2014、Microsoft SQL Server 2012 或 Microsoft SQL Server 2008 R2。发送到该数据库的数据量非常少，因为该数据库仅存储与录制的会话有关的元数据。录制的会话本身的文件会写入到单独的磁盘中。通常情况下，每个录制的会话只需约 1KB 数据库空间，除非使用 Session Recording 事件 API 将可搜索事件插入到会话中。

Express Edition 版本的 Microsoft SQL Server 2016、Microsoft SQL Server 2014、Microsoft SQL Server 2012 和 Microsoft SQL Server 2008 R2 将数据库大小限制为 10GB。以每个录制会话大小为 1KB 计算，该数据库可编录大约 400 万个会话。Microsoft SQL Server 的其他版本没有数据库大小限制，仅由可用磁盘空间限制。数据库中会话数量逐渐增多，但数据库的性能以及搜索速度的降低几乎可以忽略不计。

如果没有通过 Session Recording 事件 API 进行自定义，每个录制的会话将生成四个数据库事务：录制启动时生成两个、用户登录到正在录制的会话时生成一个、录制结束时生成一个。如果使用 Session Recording 事件 API 对会话进行了自定义，录制的每个可搜索事件都会生成一个事务。由于即使是最基本的数据库部署在一秒钟内也可处理数百个交易，因此数据库上的处理负载不可能非常重。影响非常低，Session Recording 数据库可以与其他数据库（包括 XenApp 或 XenDesktop 数据存储数据库）在相同的 SQL Server 上运行。

如果 Session Recording 部署需要在数据库中编录数百万个录制的会话，请按照 Microsoft 对 SQL Server 可扩展性的指导原则进行操作。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

安装、升级和卸载 Session Recording

Dec 05, 2017

本章详细介绍如何使用 XenApp/XenDesktop 安装程序安装 Session Recording。它包括以下部分：

安装核对表

安装 Session Recording Administration 组件

将 Director 配置为使用 Session Recording Server

安装 Session Recording Agent

安装 Session Recording Player

自动安装

升级 Session Recording

卸载 Session Recording

安装核对表

从 7.14 版起，可以使用 XenApp/XenDesktop 安装程序安装 Session Recording 组件。

开始安装之前，请完成以下列表中的步骤：

✔	步骤
	选择要安装每个 Session Recording 组件的计算机，并确保每台计算机都满足要安装的组件对硬件和软件的要求。
	使用您的 Citrix 帐户凭据访问 XenApp 和 XenDesktop 下载页面并下载产品 ISO 文件。解压缩该 ISO 文件或刻录该文件的 DVD。
	要使用 TLS 协议在 Session Recording 组件之间进行通信，请在您的环境中安装正确的证书。
	为 Session Recording 组件安装任何所需的修补程序。可以从 Citrix 支持页面下载修补程序。
	配置 Director 以创建并激活 Session Recording 策略。有关详细信息，请参阅配置 Director 以使用 Session Recording Server。

注意：

- Citrix 建议您根据录制策略将已发布的应用程序划分到独立的交付组中，因为如果已发布的应用程序位于相同的交付组中，

© 1999-2017 Citrix Systems, Inc. All rights reserved.

其会话共享可能会与活动策略冲突。Session Recording 将活动策略与用户打开的第一个已发布应用程序相匹配。

- 如果计划使用 Machine Creation Services (MCS) 或 Provisioning Services，请准备一个唯一的 QMId。未能遵守会导致录制数据丢失。
- SQL Server 要求启用 TCP/IP、运行 SQL Server Browser 服务并使用 Windows 身份验证。
- 要使用 HTTPS，请为 TLS/HTTPS 配置服务器证书。
- 确保**本地用户和组** > **组** > **用户**下的用户对 C:\windows\Temp 文件夹具有写入权限。

安装 Session Recording Administration 组件

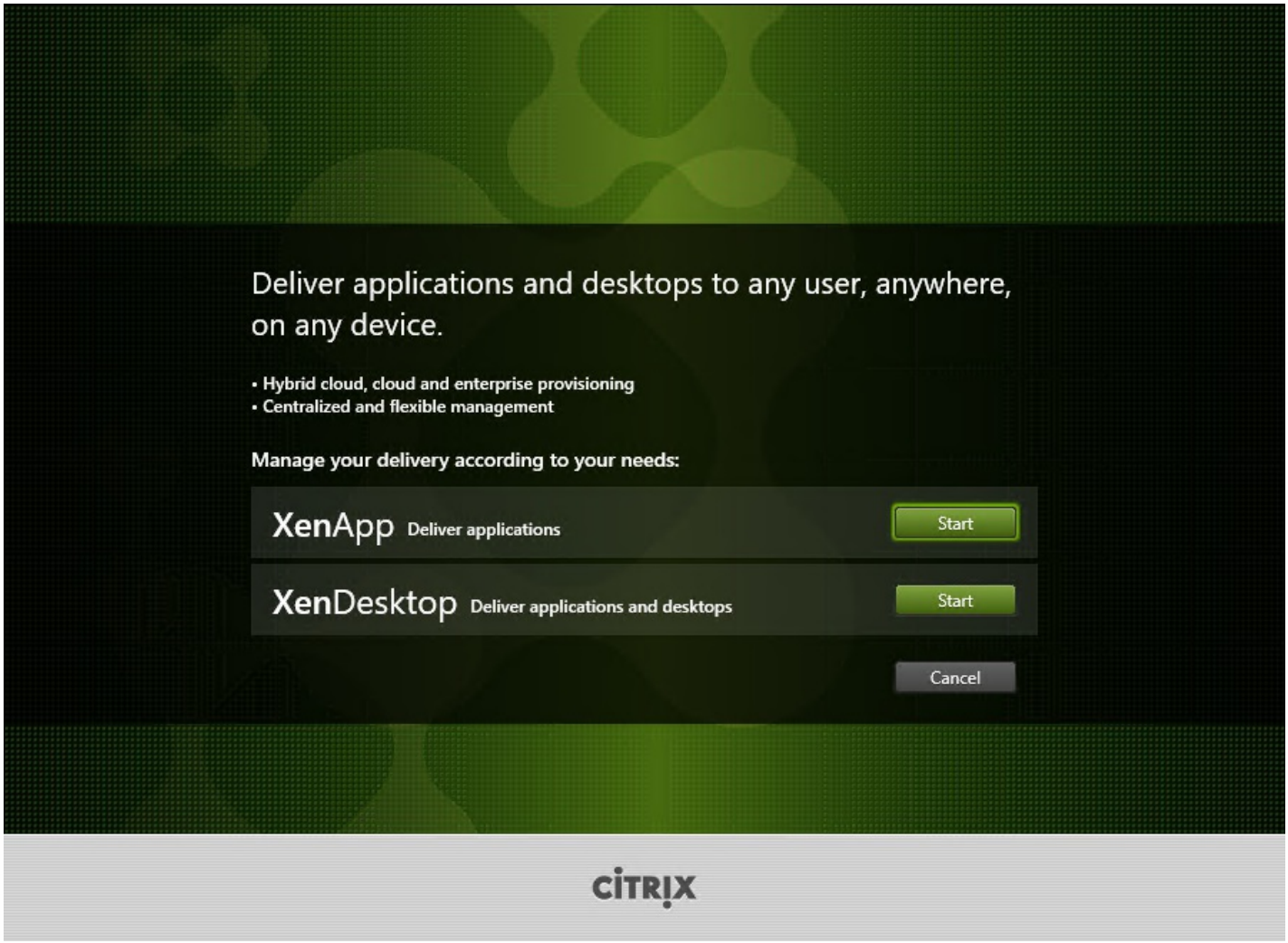
Citrix 建议在单独的服务器上安装 Session Recording Administration、Session Recording Agent 和 Session Recording Player 组件。Session Recording Administration 组件包括 Session Recording 数据库、Session Recording Server 和 Session Recording 策略控制台。可以选择要在服务器上安装上述哪些组件。

步骤 1：下载产品软件并启动向导

1. 如果尚未下载 XenApp 和 XenDesktop ISO，请使用您的 Citrix 帐户凭据访问 XenApp 和 XenDesktop 下载页面并下载产品 ISO 文件。解压缩该 ISO 文件或刻录该文件的 DVD。
2. 使用本地管理员帐户，登录要在其中安装 Session Recording Administration 组件的计算机。在驱动器中插入 DVD 或装载 ISO 文件。如果安装程序未自动启动，请双击 **AutoSelect** 应用程序或已装载的驱动器。
   将启动安装向导。

步骤 2：选择要安装的产品

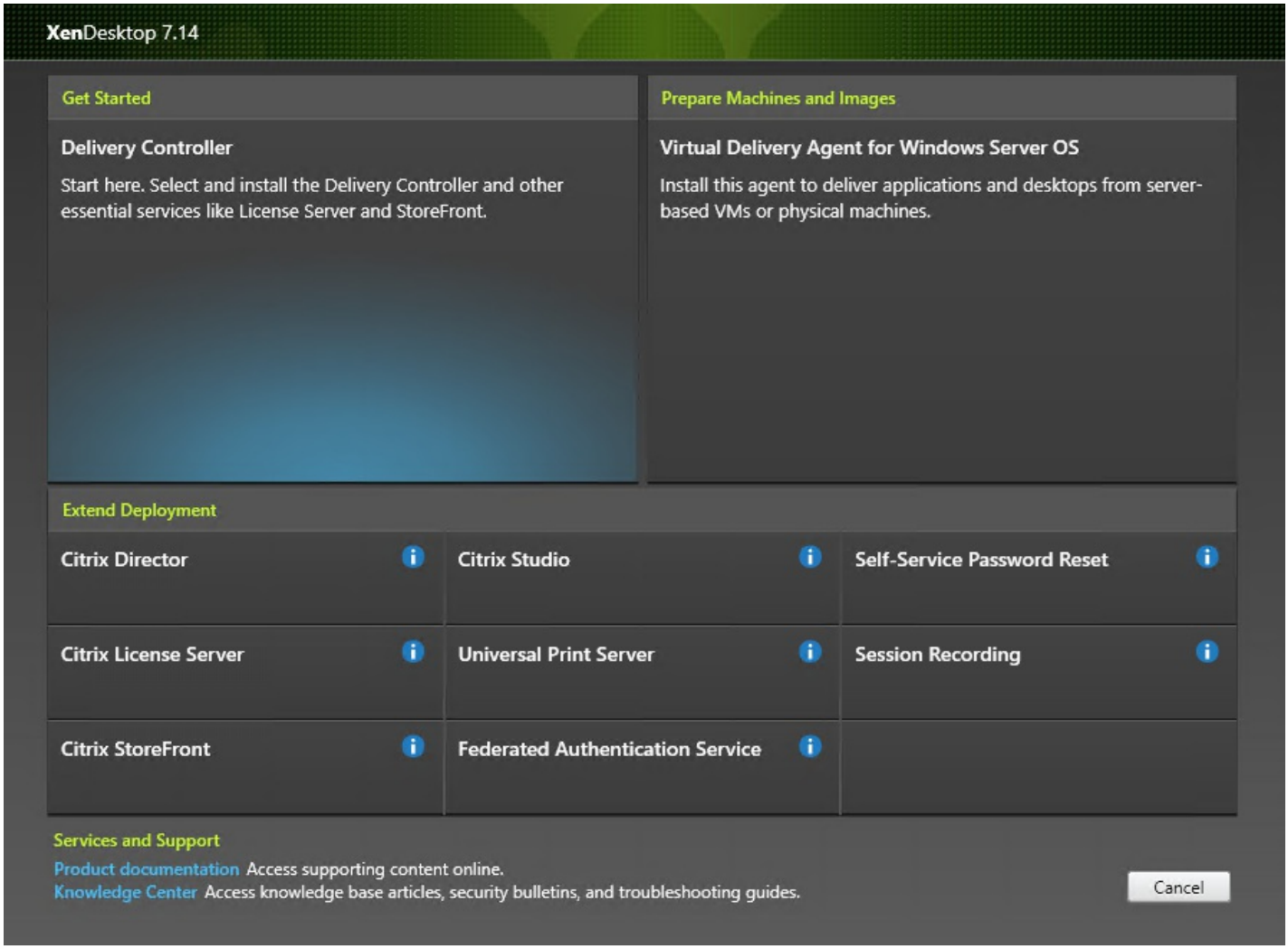
© 1999-2017 Citrix Systems, Inc. All rights reserved.



单击产品旁边的**开始**安装：**XenApp** 或 **XenDesktop**。

步骤 3：选择 Session Recording

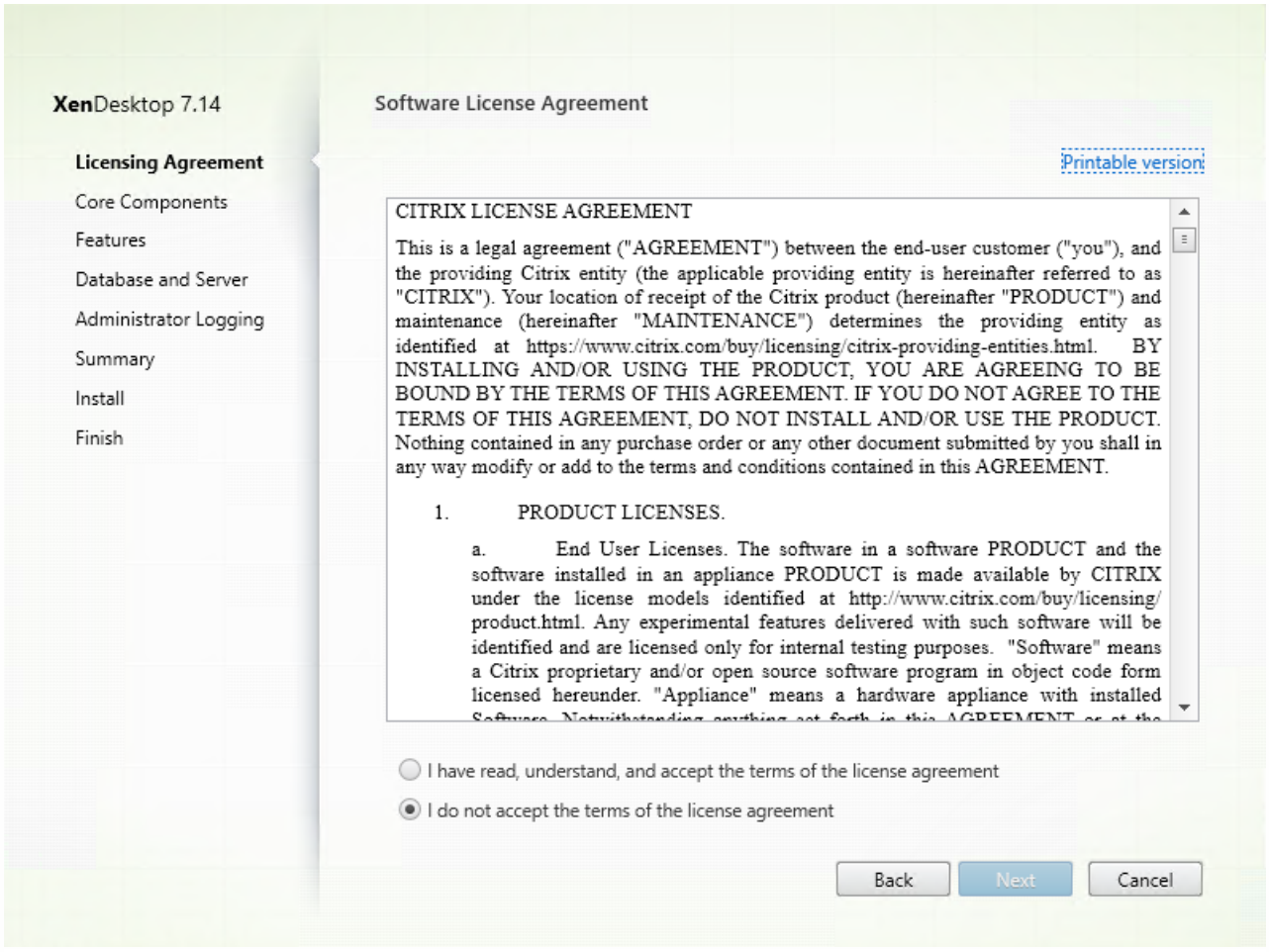
© 1999-2017 Citrix Systems, Inc. All rights reserved.



选择 **Session Recording** 条目。

步骤 4：阅读并接受许可协议

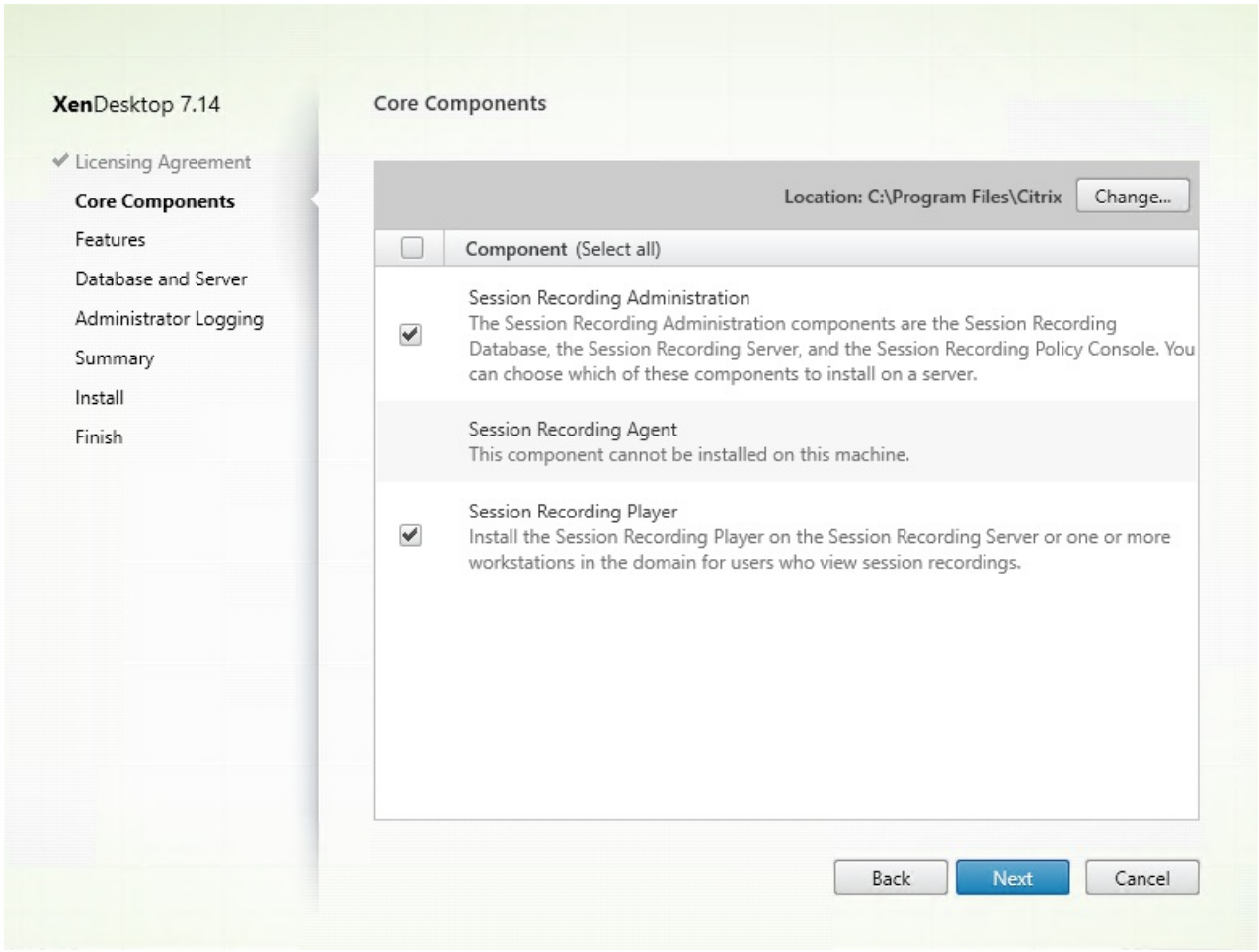
© 1999-2017 Citrix Systems, Inc. All rights reserved.



在**软件许可协议**页面上，阅读并接受许可协议，然后单击**下一步**。

步骤 5：选择要安装的组件及安装位置

© 1999-2017 Citrix Systems, Inc. All rights reserved.

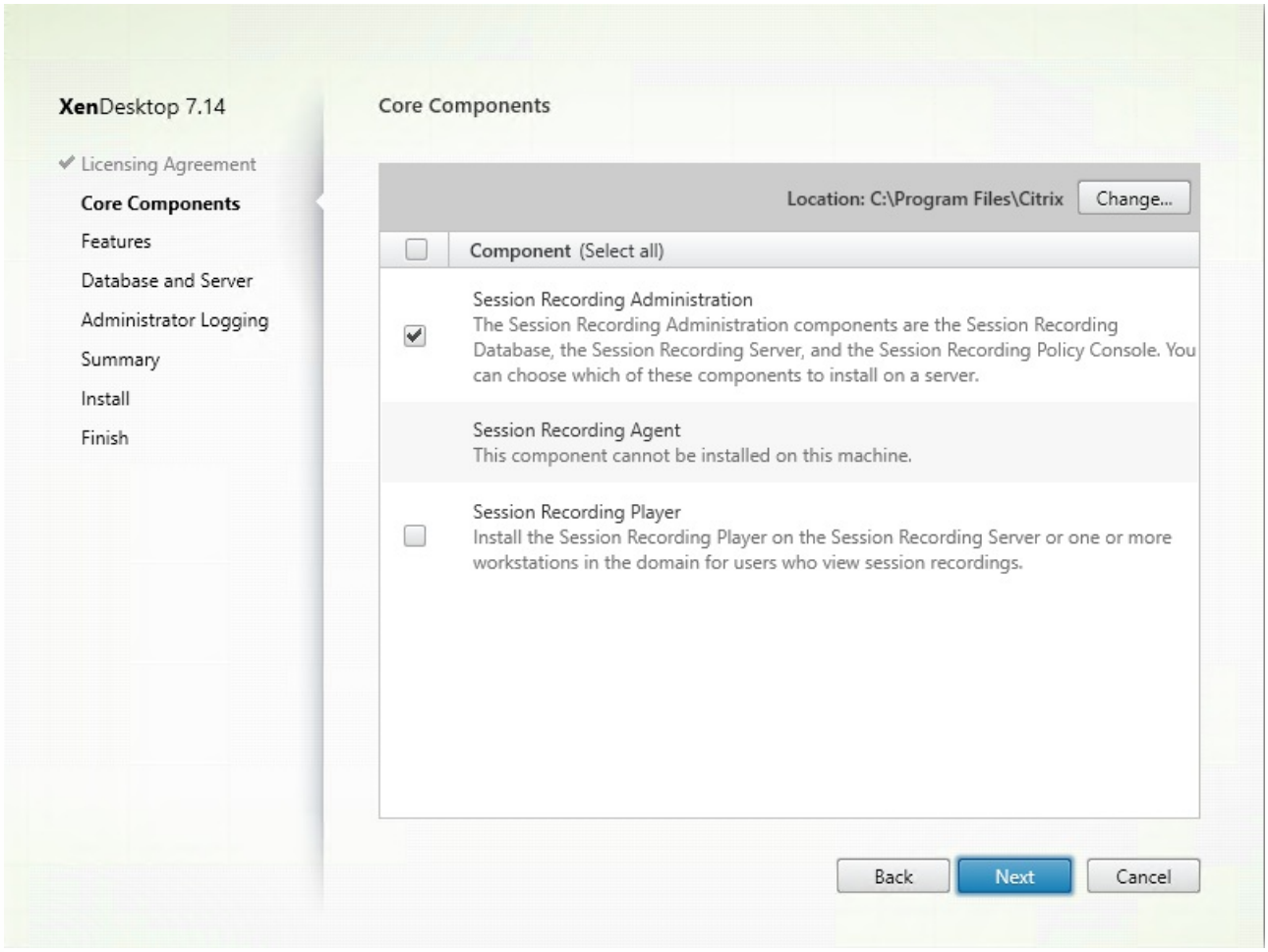


在**核心组件**页面上：

- **位置**：默认情况下，组件安装在 C:\Program Files\Citrix 中。该默认位置适用于大多数部署。您可以指定自定义安装位置。
- **组件**：默认情况下，可以安装的组件旁边的所有复选框都被选中。安装程序知晓自身是在桌面操作系统还是服务器操作系统中运行。它只允许 Session Recording Administration 组件安装在服务器操作系统上，不允许 Session Recording Agent 安装在没有提前安装 VDA 的计算机上。如果在没有提前安装 VDA 的计算机上安装 Session Recording Agent，**Session Recording Agent** 选项将不可用。

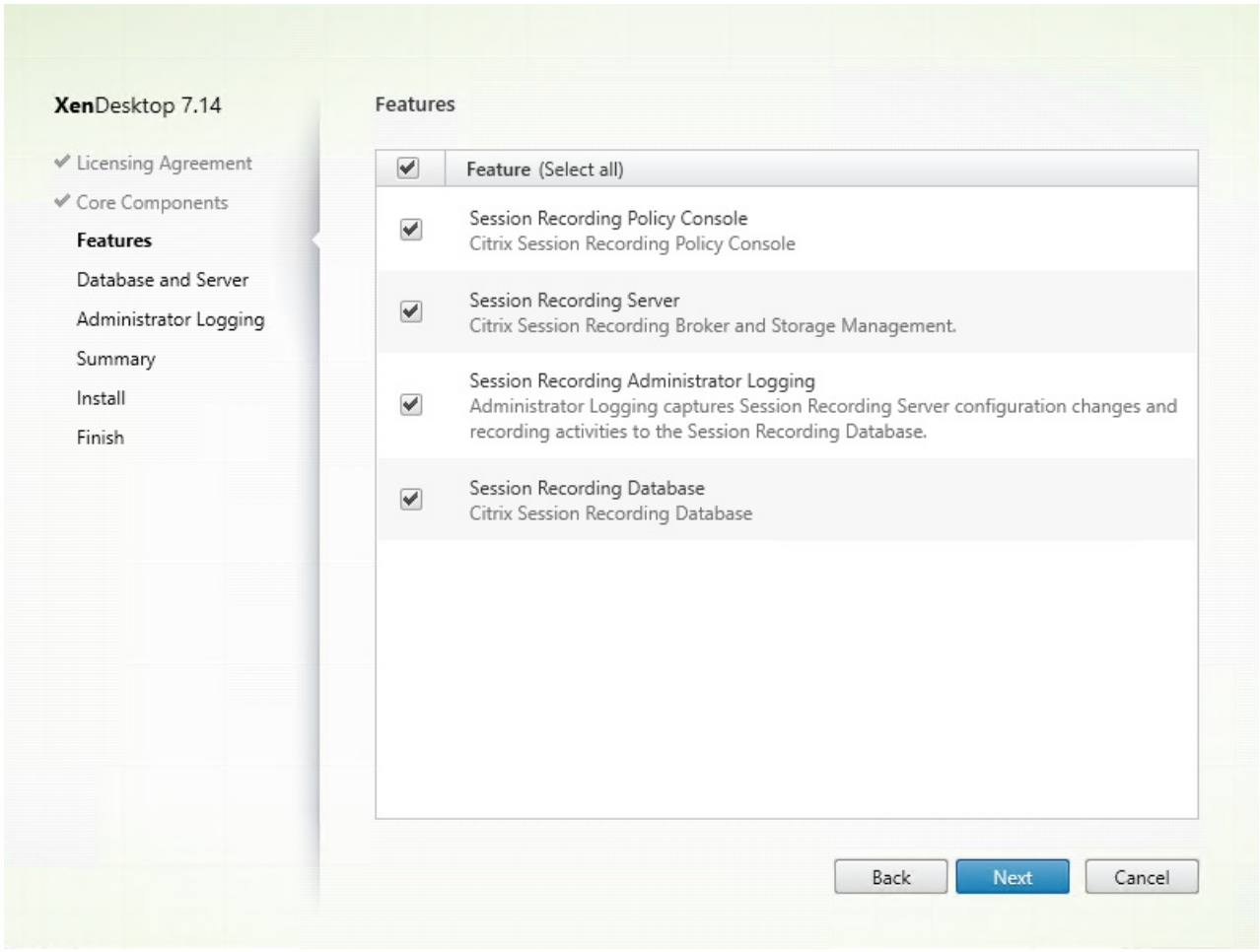
选择 **Session Recording Administration** 并单击**下一步**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



步骤 6：选择要安装的功能

© 1999-2017 Citrix Systems, Inc. All rights reserved.



在**功能**页面上：

- 默认情况下，可以安装的功能旁边的所有复选框都被选中。在一台服务器上安装所有这些服务器适用于概念验证。但是，对于大型生产环境，Citrix 建议将 Session Recording 策略控制台安装在一台单独的服务器上，将 Session Recording Server、Session Recording 管理员日志记录和 Session Recording 数据库安装在另一台单独的服务器上。请注意，Session Recording 管理员日志记录是 Session Recording Server 的可选子功能。必须先选择 Session Recording Server，然后才能选择 Session Recording 管理员日志记录。
- 要在选择功能并将其安装在服务器上后在同一服务器上添加其他功能，只能运行 msi 软件包，而不能重新运行安装程序。

选择要安装的功能，然后单击**下一步**。

步骤 6.1：安装 Session Recording 数据库

注意：Session Recording 数据库不是实际数据库。它是负责在安装期间创建和配置 Microsoft SQL Server 实例中所需数据库的组件。Session Recording 支持基于 Microsoft SQL Server 的三种数据库高可用性解决方案。有关详细信息，请参阅安装具有数据库高可用性的 Session Recording。

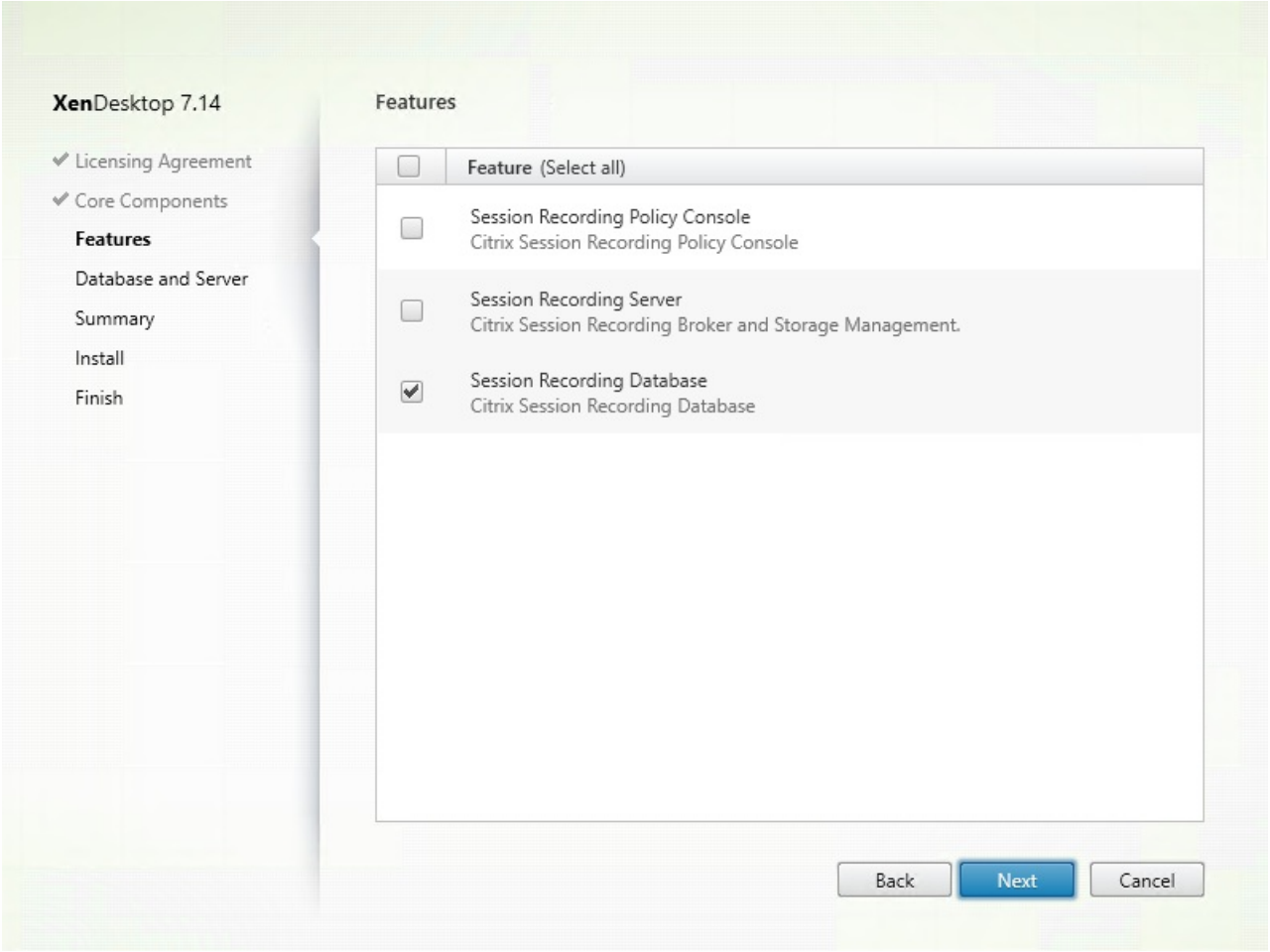
Session Recording 数据库和 Microsoft SQL Server 的部署通常有以下三种类型：

- 部署 1：在同一台计算机上安装 Session Recording Server 和 Session Recording 数据库，在远程计算机上安装 Microsoft SQL Server。（**推荐**）
- 部署 2：在同一台计算机上安装 Session Recording Server、Session Recording 数据库和 Microsoft SQL Server。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

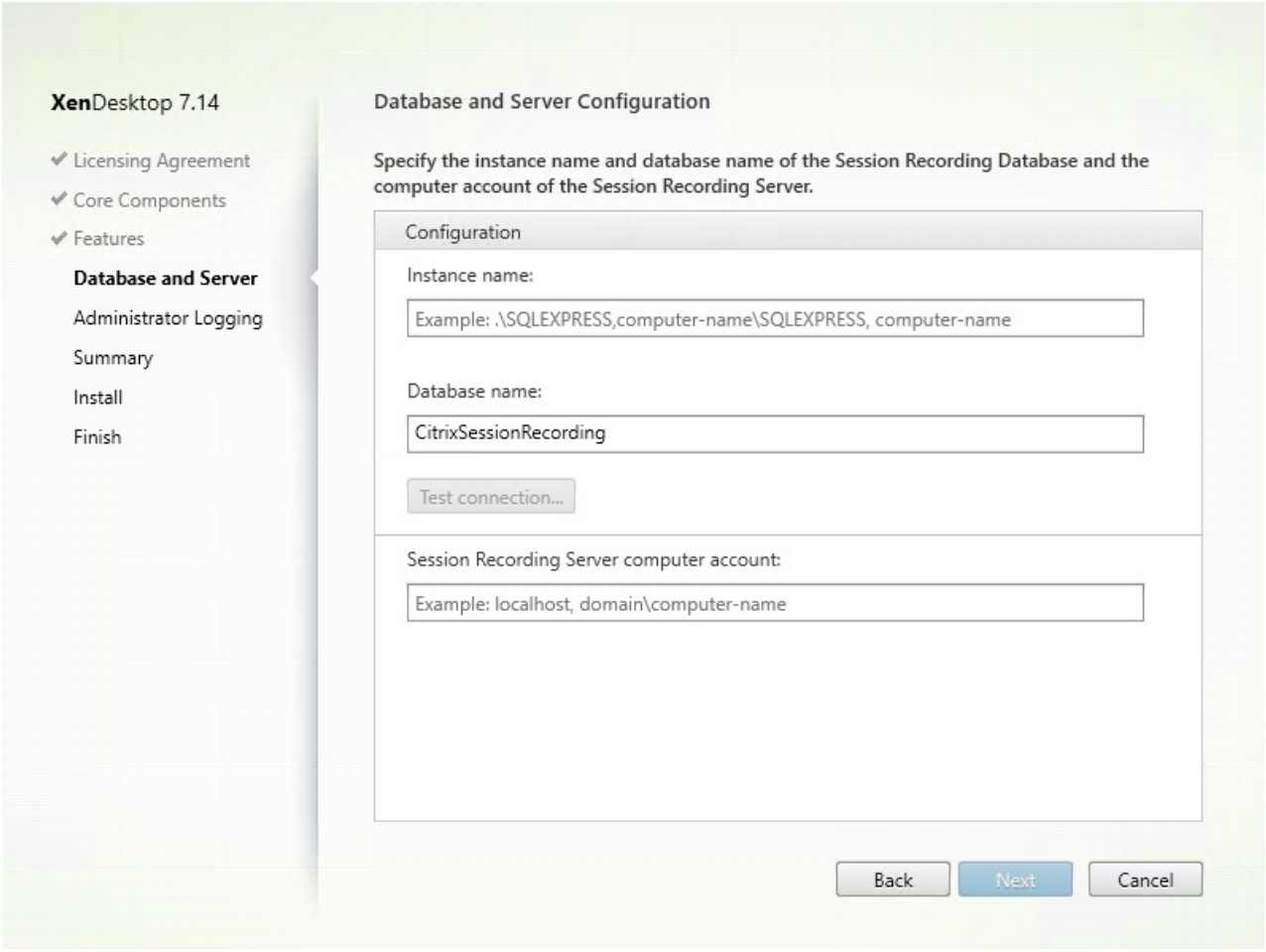
- 部署 3：在一台计算机上安装 Session Recording Server，在另一台计算机上安装 Session Recording 数据库和 Microsoft SQL Server。（**不推荐**）

1. 在**功能**页面上，选择 **Session Recording 数据库**并单击**下一步**。



2. 在**数据库和服务器配置**页面上，指定 Session Recording 数据库的实例名称和数据库名称以及 Session Recording Server 的计算机帐户。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



在**数据库和服务器配置**页面上：

- **实例名称**：如果数据库实例不是您在设置实例时配置的命名实例，您只能使用 SQL Server 的计算机名称。如果您已为此实例命名，请使用 computer-name\instance-name 作为数据库实例名称。要确定使用的服务器实例名称，请在 SQL Server 上运行 **select @@servername**；返回值为准确的数据库实例名称。
- **数据库名称**：在**数据库名称**文本框中键入自定义数据库名称，或者使用文本框中已有的默认数据库名称。单击**测试连接**测试与 SQL Server 实例的连接以及数据库名称的有效性。

> ## Important
>
> 自定义数据库名称必须仅包含 A-Z、a-z 和 0-9，并且不能超过 123 个字符。

- 必须对数据库具有 **securityadmin** 和 **dbcreator** 服务器角色权限。如果没有这些权限，您可以：
  - 要求数据库管理员分配安装权限。安装完成后，就不再需要 **securityadmin** 和 **dbcreator** 服务器角色权限了，可以安全删除。
  - 或者使用 SessionRecordingAdministrationx64.msi 软件包（解压缩 ISO 文件，可以在 ...\x64\Session Recording 下面找到此 msi 软件包）。在 msi 安装期间，会显示一个对话框，提示提供具有 **securityadmin** 和 **dbcreator** 服务器角色权限的数据库管理员的凭据。请输入正确的凭据，然后单击**确定**以继续安装。

    安装将创建新 Session Recording 数据库，并添加 Session Recording Server 的计算机帐户 **db_owner**。

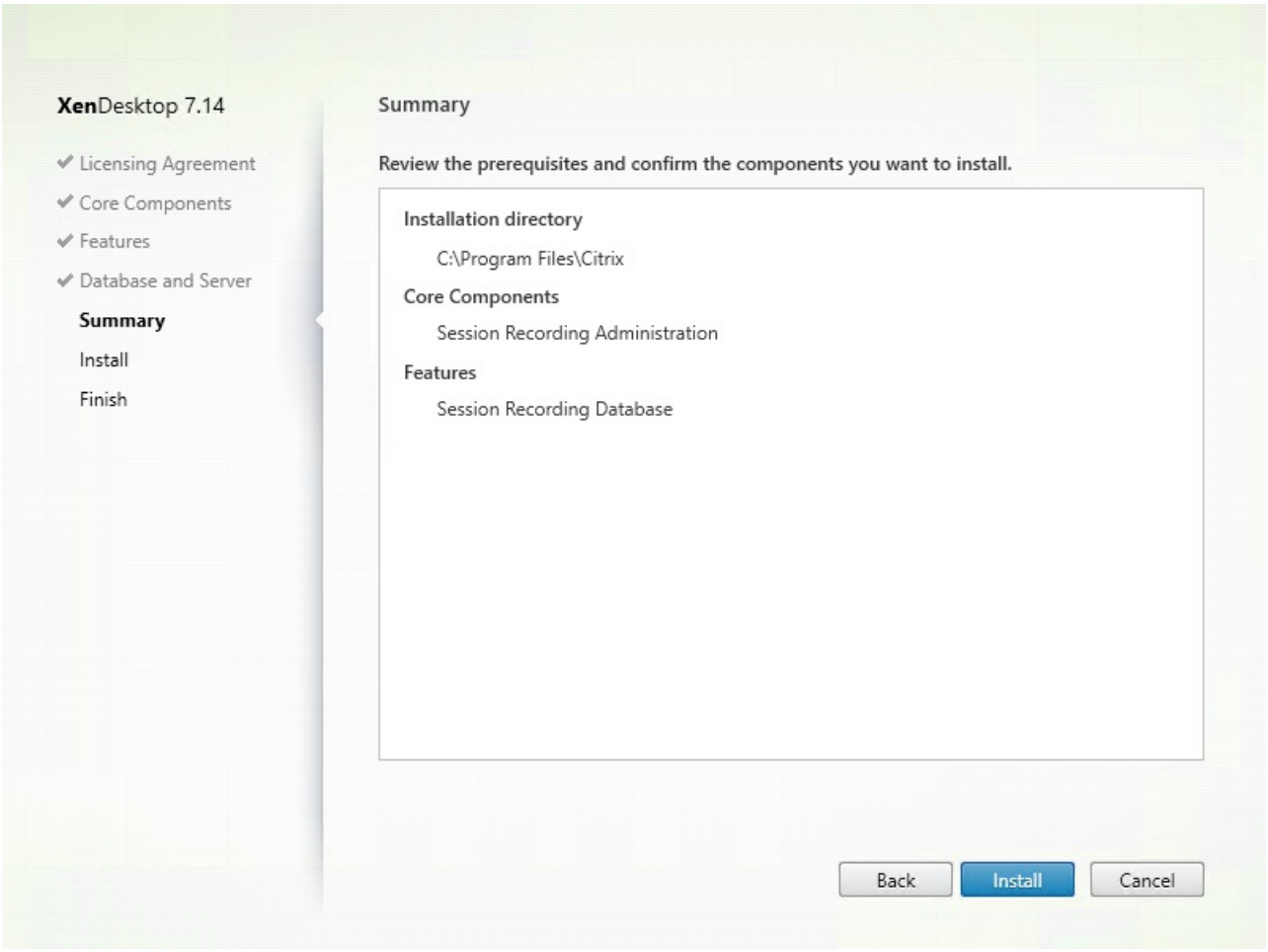
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Session Recording Server 计算机帐户**：
  - **部署 1 和 2**：在 **Session Recording Server 计算机帐户**字段中键入 **localhost**。
  - **部署 3**：使用 domain\computer-name 格式键入托管 Session Recording Server 的计算机的名称。Session Recording Server 计算机帐户即为用于访问 Session Recording 数据库的用户帐户。

    注意：在 **Session Recording Server 计算机帐户**字段中设置了域名时，尝试安装 Session Recording Administration 组件会失败并显示错误代码 1603。解决方法：在 **Session Recording Server 计算机帐户**字段中键入 **localhost** 或 NetBIOS 域名\计算机名称。

单击**下一步**。

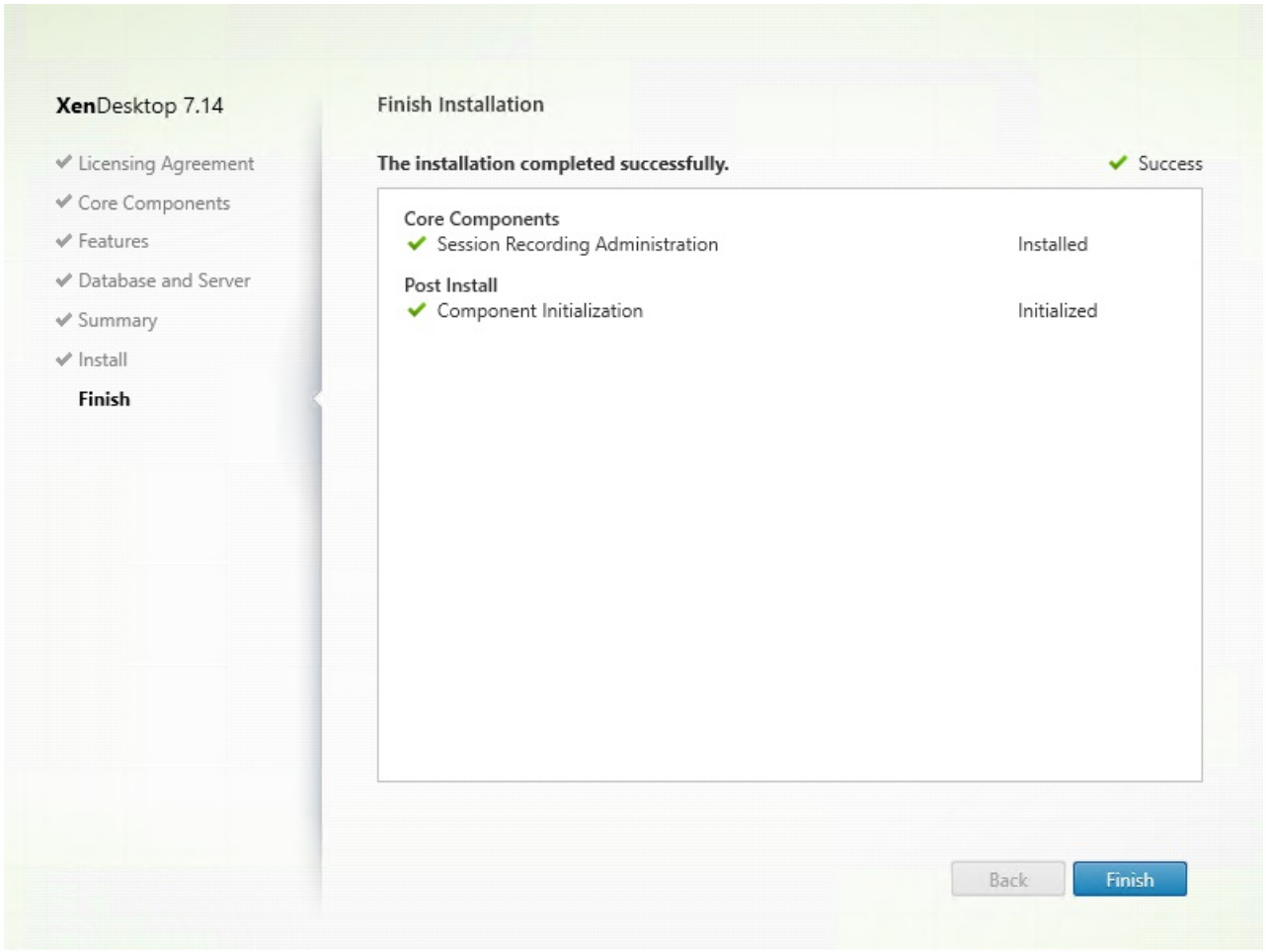
3. 查看必备项并确认安装。



摘要页面上将显示您所做安装选择。可以单击**返回**返回到之前的向导页面并进行更改。或者单击**安装**开始安装。

4. 完成安装。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



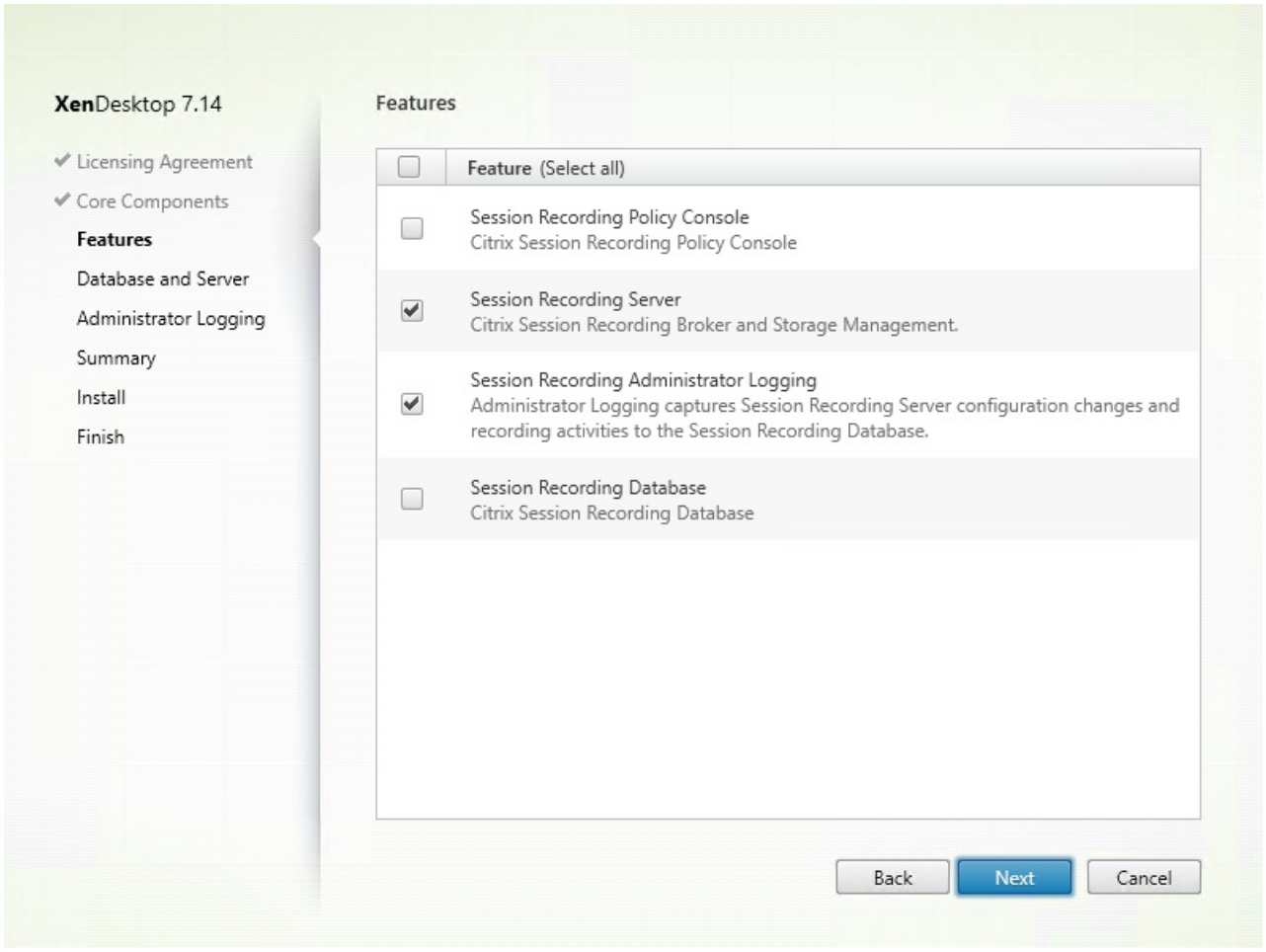
完成安装页面上显示带绿色复选标记的所有已成功安装和初始化的必备项和组件。

单击**完成**以完成 Session Recording 数据库的安装。

步骤 6.2：安装 Session Recording Server

1. 在 **功能**页面上，选择 **Session Recording Server** 和 **Session Recording 管理员日志记录**。单击**下一步**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

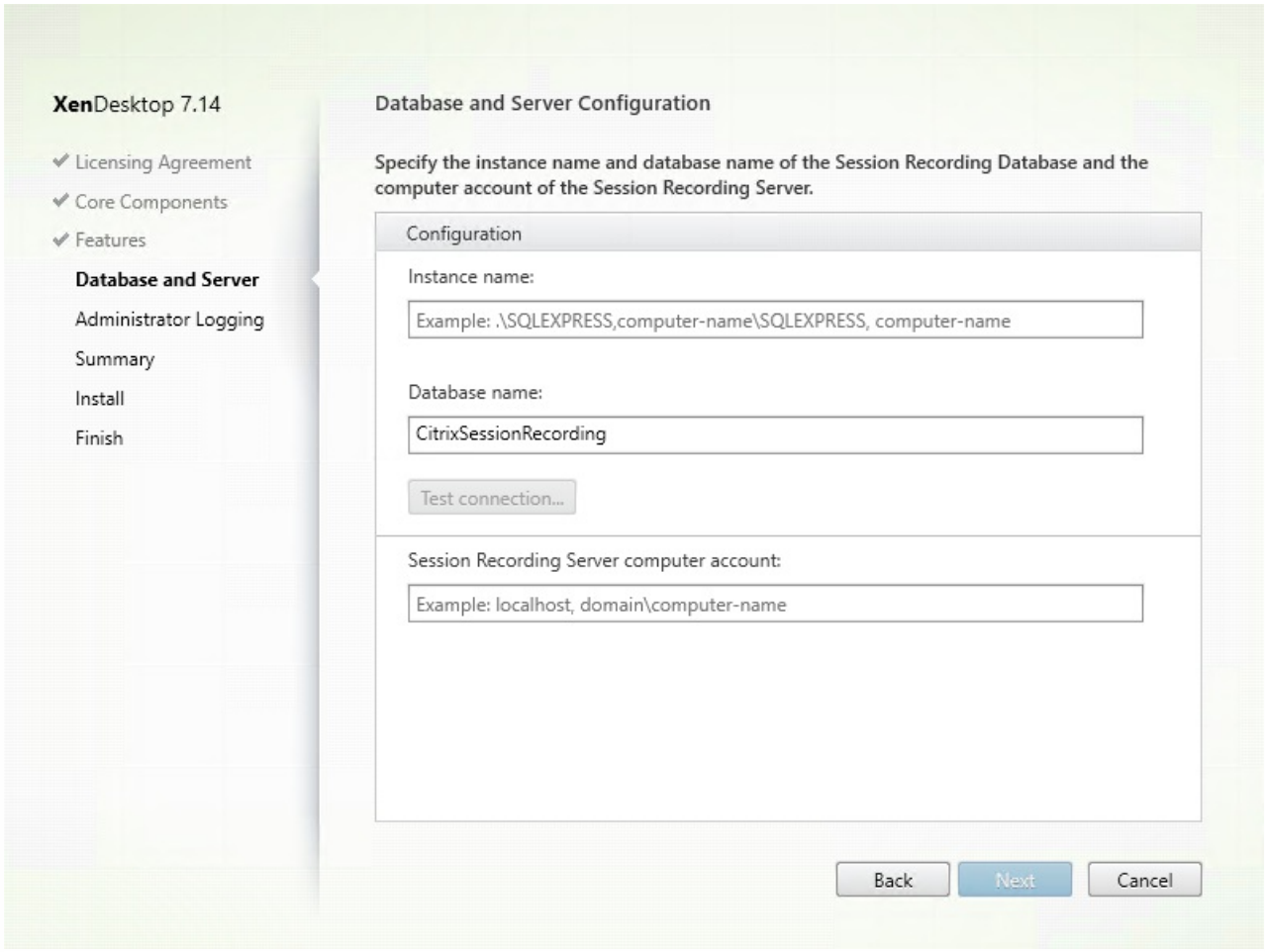


注意：

- Session Recording 管理员日志记录是 Session Recording Server 的可选子功能。必须先选择 Session Recording Server，然后才能选择 Session Recording 管理员日志记录。
- Citrix 建议同时在一起安装 Session Recording 管理员日志记录和 Session Recording Server。如果您不希望启用管理员日志记录功能，可以在后面的页面上禁用该功能。但是，如果您在开始时选择不安装此功能，但希望以后添加此功能，只能使用 SessionRecordingAdministrationx64.msi 软件包手动添加此功能。

2. 在 **数据库和服务器配置**页面上，指定配置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

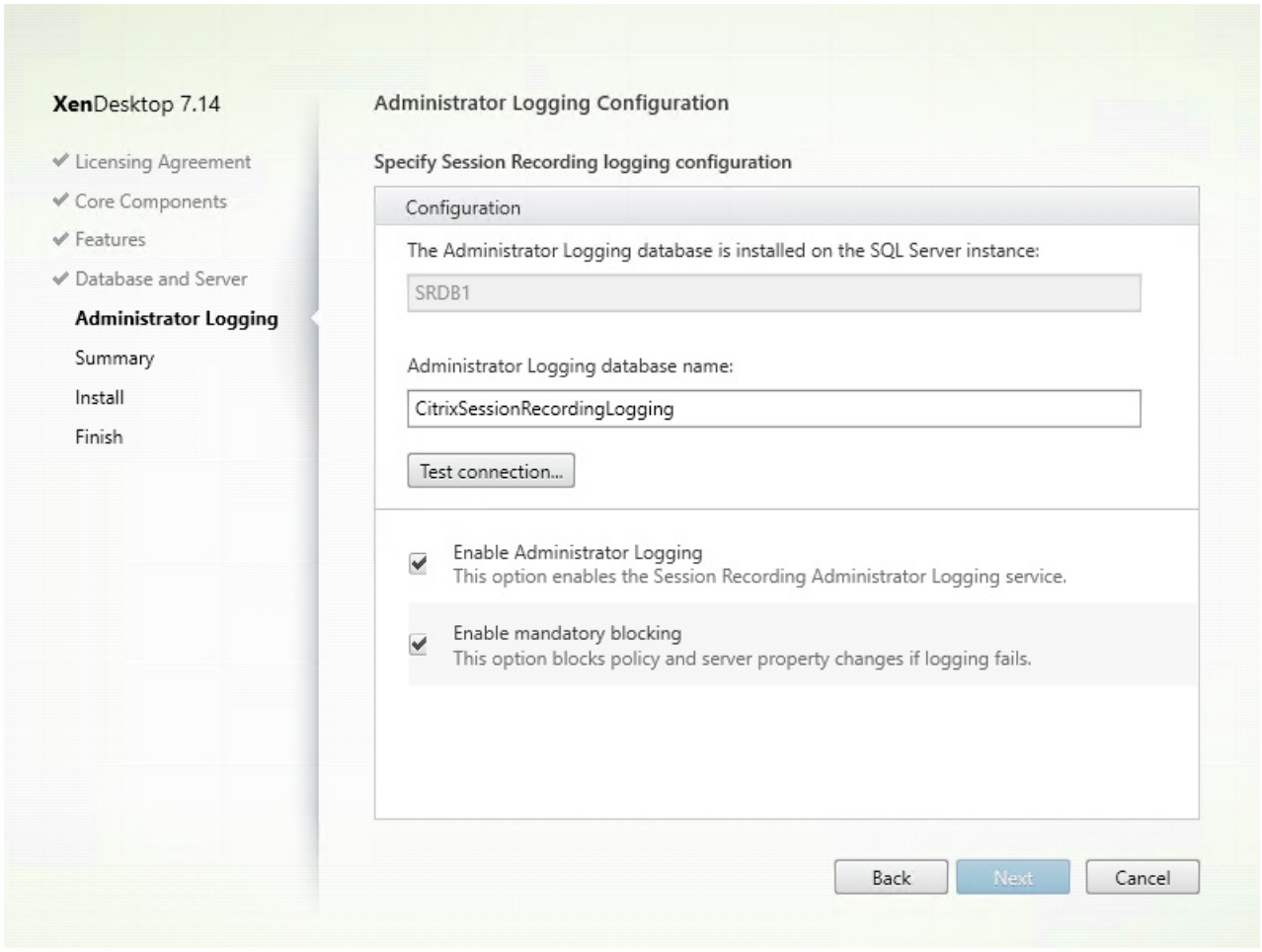


在**数据库和服务器配置**页面上：

- **实例名称**：在**实例名称**文本框中键入 SQL Server 的名称。如果要使用命名实例，请键入 computer-name\instance-name；否则，请只能键入 computer-name。
- **数据库名称**：在**数据库名称**文本框中键入自定义数据库名称，或者使用文本框中已有的默认数据库名称 **CitrixSessionRecording**。
- 必须对数据库具有 **securityadmin** 和 **dbcreator** 服务器角色权限。如果没有这些权限，您可以：
  - 要求数据库管理员分配安装权限。安装完成后，就不再需要 **securityadmin** 和 **dbcreator** 服务器角色权限了，可以安全删除。
  - 或者使用 SessionRecordingAdministrationx64.msi 软件包安装 Session Recording Server。在 msi 安装期间，会显示一个对话框，提示提供具有 **securityadmin** 和 **dbcreator** 服务器角色权限的数据库管理员的凭据。请输入正确的凭据，然后单击**确定**以继续安装。
- 键入正确的实例名称和数据库名称后，单击**测试连接**测试与 Session Recording 数据库的连接。
- 输入 Session Recording Server 计算机帐户，然后单击**下一步**。

3. 在**管理日志记录配置**页面上，指定管理日志记录功能的配置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



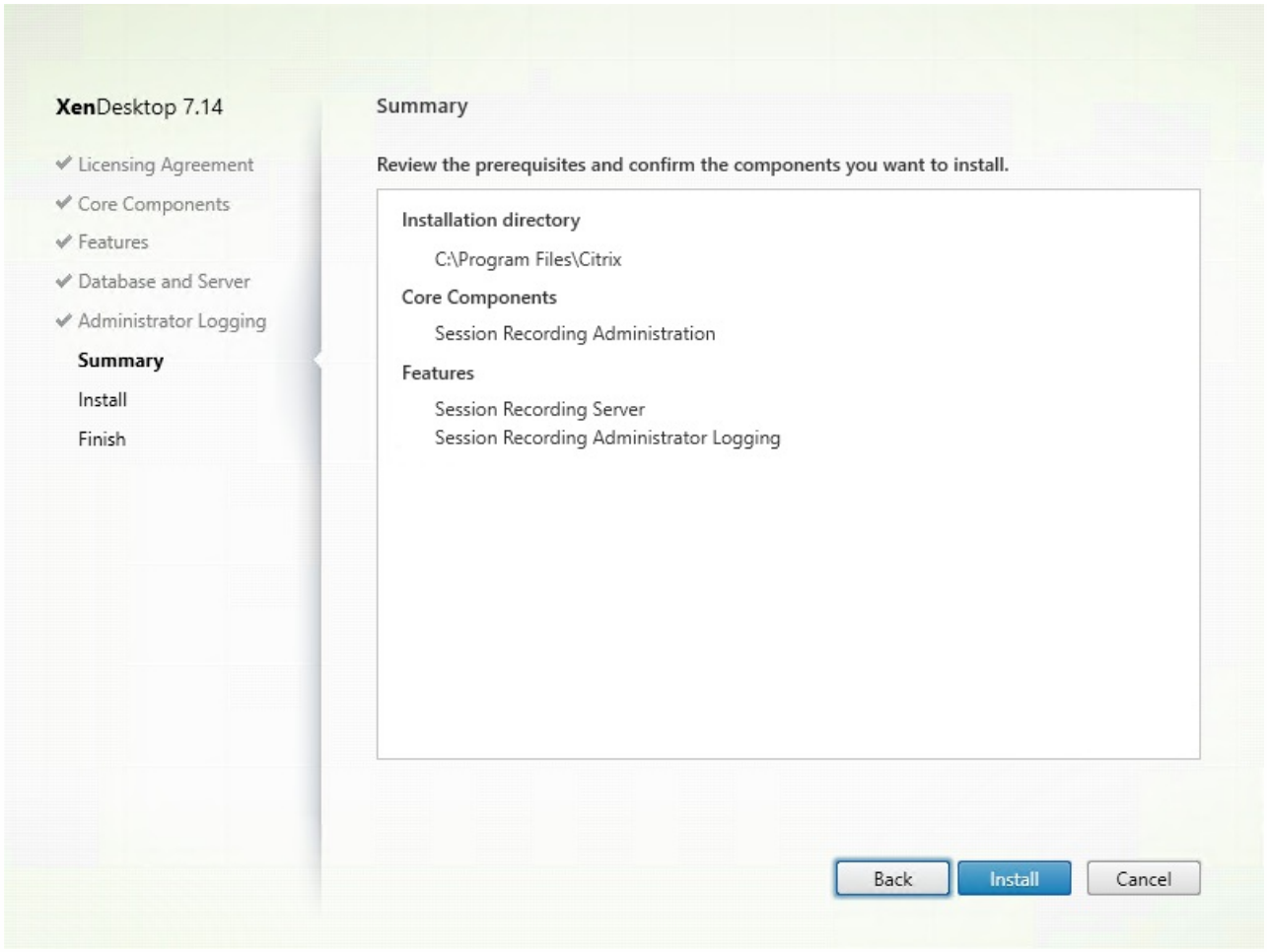
在**管理日志记录配置**页面上：

- **管理日志记录数据库安装在 SQL Server 实例上**：此文本框不可编辑。管理日志记录数据库的 SQL Server 实例名称是自动从您在**数据库和服务器配置**页面上键入的实例名称中抓取的。
- **管理员日志记录数据库名称**：如果选择安装 Session Recording 管理员日志记录功能，请在此文本框中键入管理员日志记录数据库的自定义数据库名称，或者使用文本框中已有的默认数据库名称 **CitrixSessionRecordingLogging**。
  注意：管理员日志记录数据库名称必须与在上一页**数据库和服务器配置**上的**数据库名称**文本框中设置的 Session Recording 数据库名称不同。
- 键入管理员日志记录数据库名称后，单击**测试连接**测试与管理员日志记录数据库的连接。
- **启用管理日志记录**：默认情况下，启用管理日志记录功能。可以通过取消选中相应复选框禁用该功能。
- **启用强制阻止**：默认情况下启用强制阻止。如果日志记录失败，则可能会阻止正常功能。可以通过取消选中相应复选框禁用强制阻止。

单击**下一步**继续安装。

4. 查看必备项并确认安装。

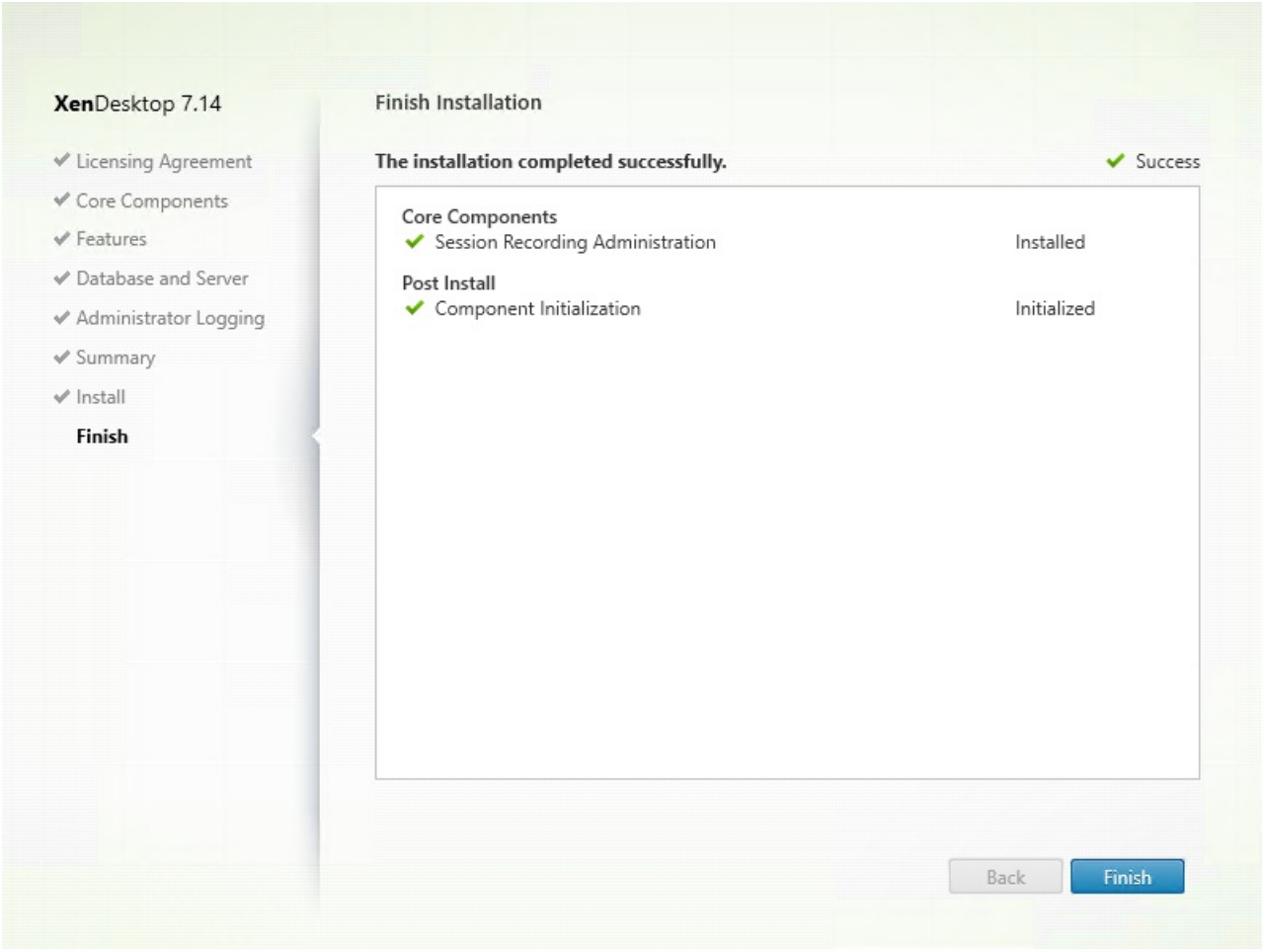
© 1999-2017 Citrix Systems, Inc. All rights reserved.



摘要页面上将显示您所做安装选择。可以单击**返回**返回到之前的向导页面并进行更改。或者单击**安装**开始安装。

5. 完成安装。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



完成安装页面上显示带绿色复选标记的所有已成功安装和初始化的必备项和组件。

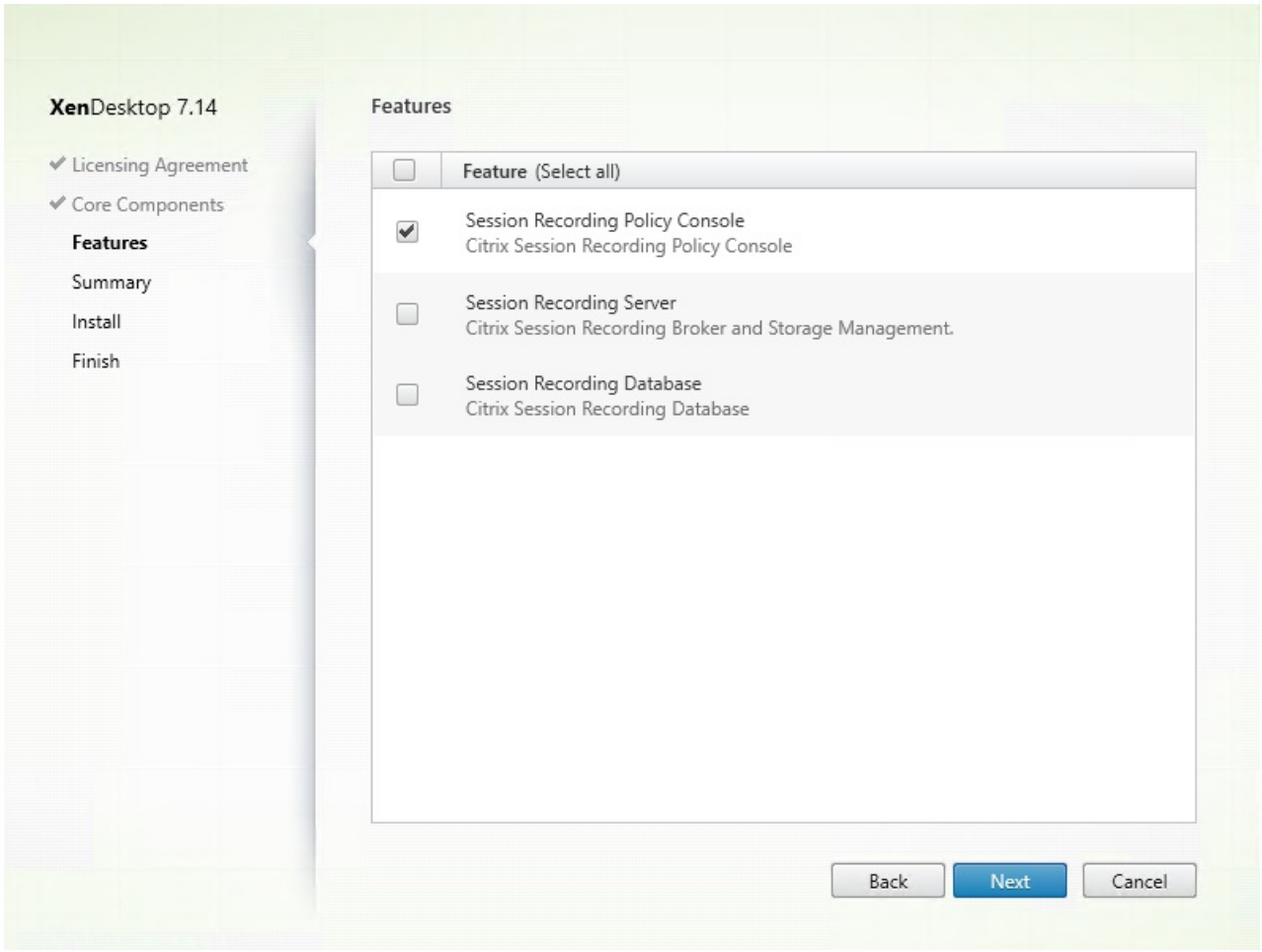
单击**完成**以完成 Session Recording Server 的安装。

注意：Session Recording Server 默认安装使用 HTTPS/TLS 来确保通信安全。如果在 Session Recording Server 的默认 IIS 站点中没有配置 TLS，则使用 HTTP。为此，请在 IIS 管理控制台中通过执行以下操作取消选择 SSL：导航到 Session Recording Broker 站点，打开 SSL 设置，并取消选中**要求 SSL** 复选框。

步骤 6.3：安装 Session Recording 策略控制台

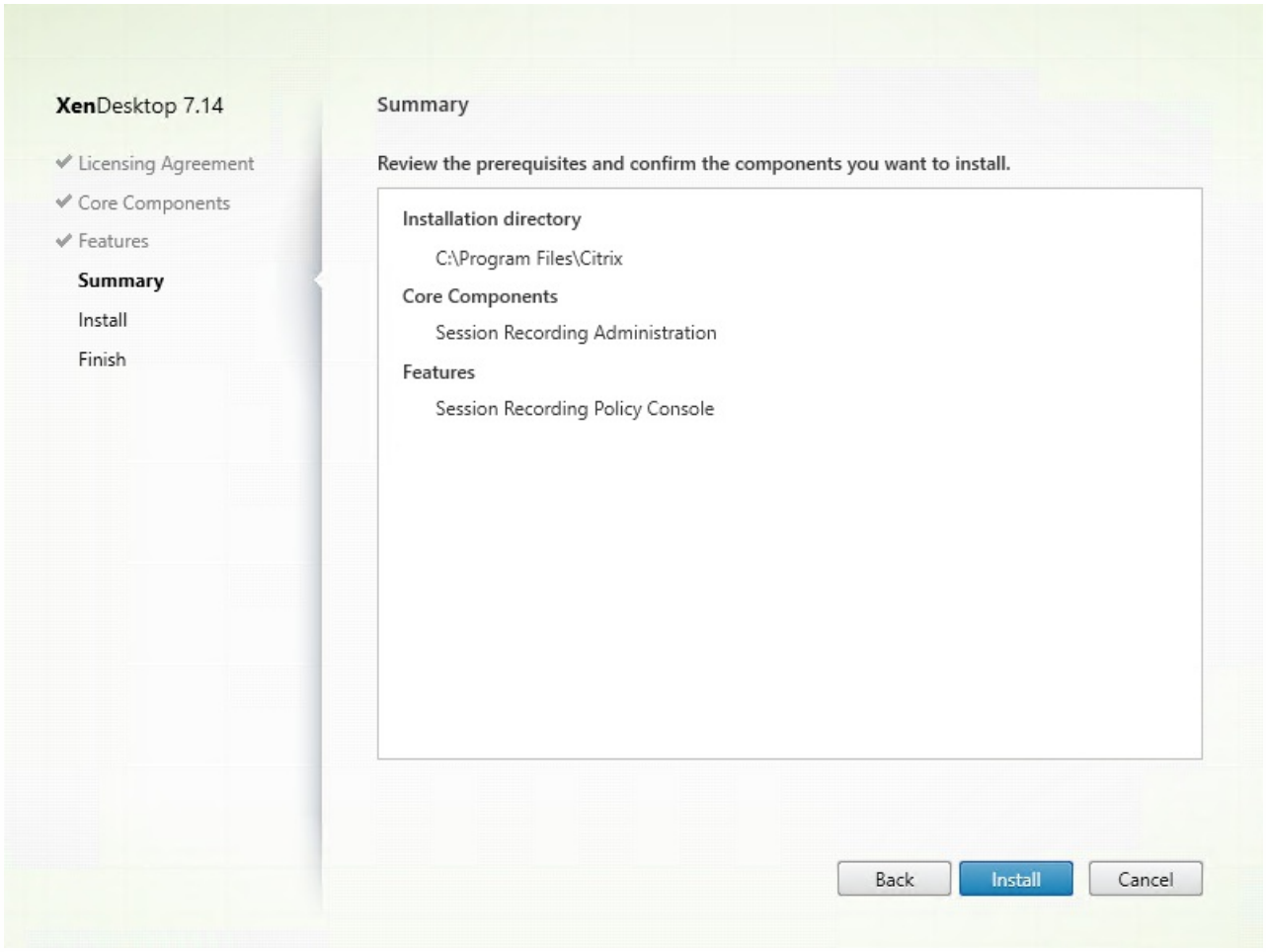
1. 在**功能**页面上，选择 **Session Recording 策略控制台**并单击**下一步**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. 查看必备项并确认安装。

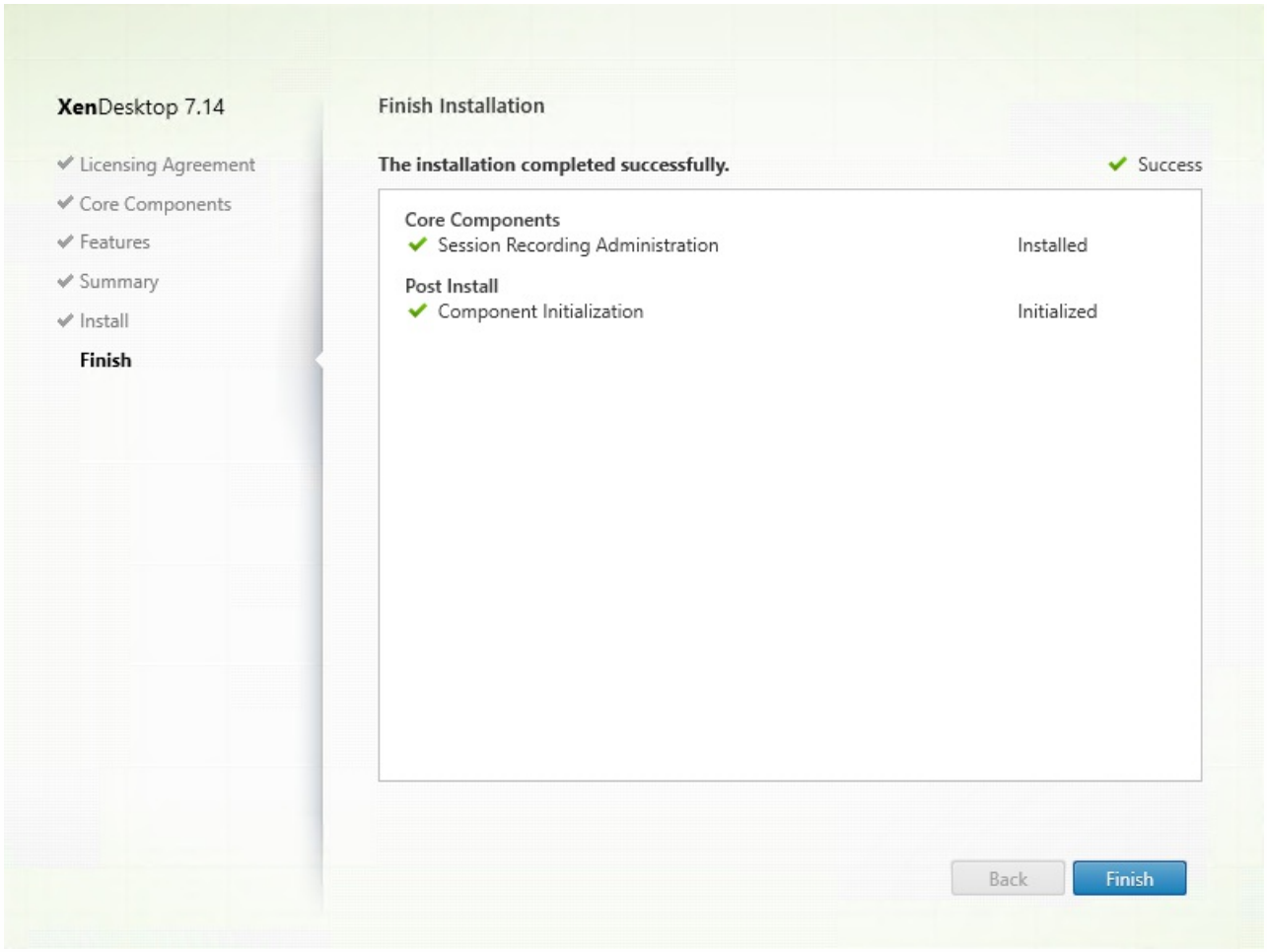
© 1999-2017 Citrix Systems, Inc. All rights reserved.



摘要页面上将显示您所做安装选择。可以单击**返回**返回到之前的向导页面并进行更改。或者单击**安装**开始安装。

3. 完成安装。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



完成安装页面上显示带绿色复选标记的所有已成功安装和初始化的必备项和组件。

单击**完成**以完成 Session Recording 策略控制台的安装。

步骤 7：安装 Broker_PowerShellSnapIn_x64.msi

重要：必须安装 Broker PowerShell 管理单元 (Broker_PowerShellSnapIn_x64.msi)，才能使用 Session Recording 策略控制台。该管理单元不能由安装程序自动安装。请在 XenApp/XenDesktop ISO (\layout\image-full\x64\Citrix Desktop Delivery Controller) 中找到该管理单元，然后按照说明手动安装。否则，会导致出现错误。

将 Director 配置为使用 Session Recording Server

可以使用 Director 控制台创建并激活 Session Recording 策略。

1. 对于 HTTPS 连接，请在 Director 服务器的可信根证书中安装证书以信任 Session Recording Server。
2. 要配置 Director 服务器以使用 Session Recording Server，请运行以下命令：**C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configsessionrecording**
3. 在 Director 服务器上输入 Session Recording Server 的 IP 地址或 FQDN 以及 Session Recording Agent 用于连接到 Session Recording Broker 的端口号和连接类型 (HTTP/HTTPS)。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

安装 Session Recording Agent

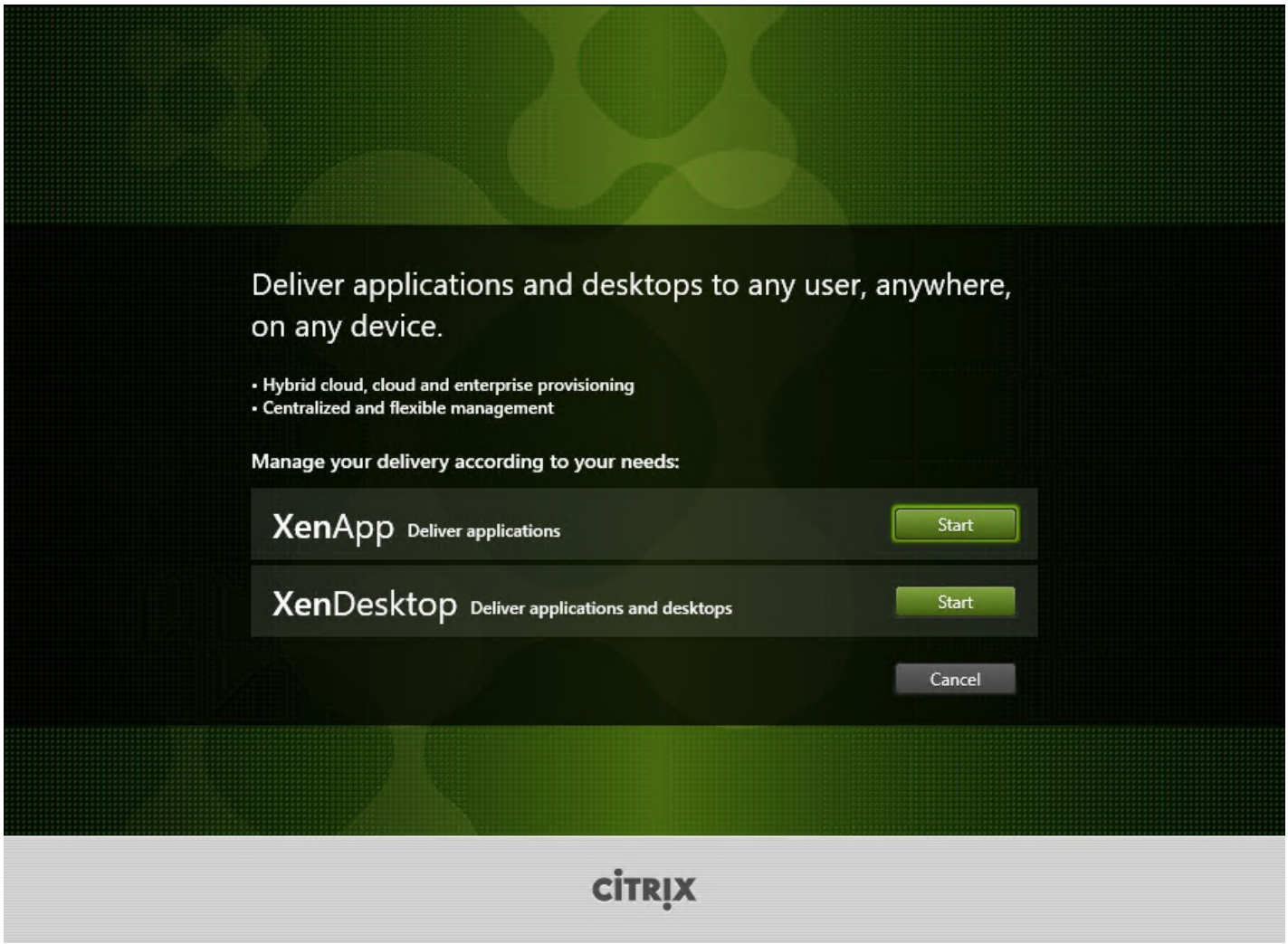
必须在要录制会话的 VDA 或 VDI 计算机上安装 Session Recording Agent。

步骤 1：下载产品软件并启动向导

使用本地管理员帐户，登录要在其中安装 Session Recording Agent 组件的计算机。在驱动器中插入 DVD 或装载 ISO 文件。如果安装程序未自动启动，请双击 **AutoSelect** 应用程序或已装载的驱动器。

将启动安装向导。

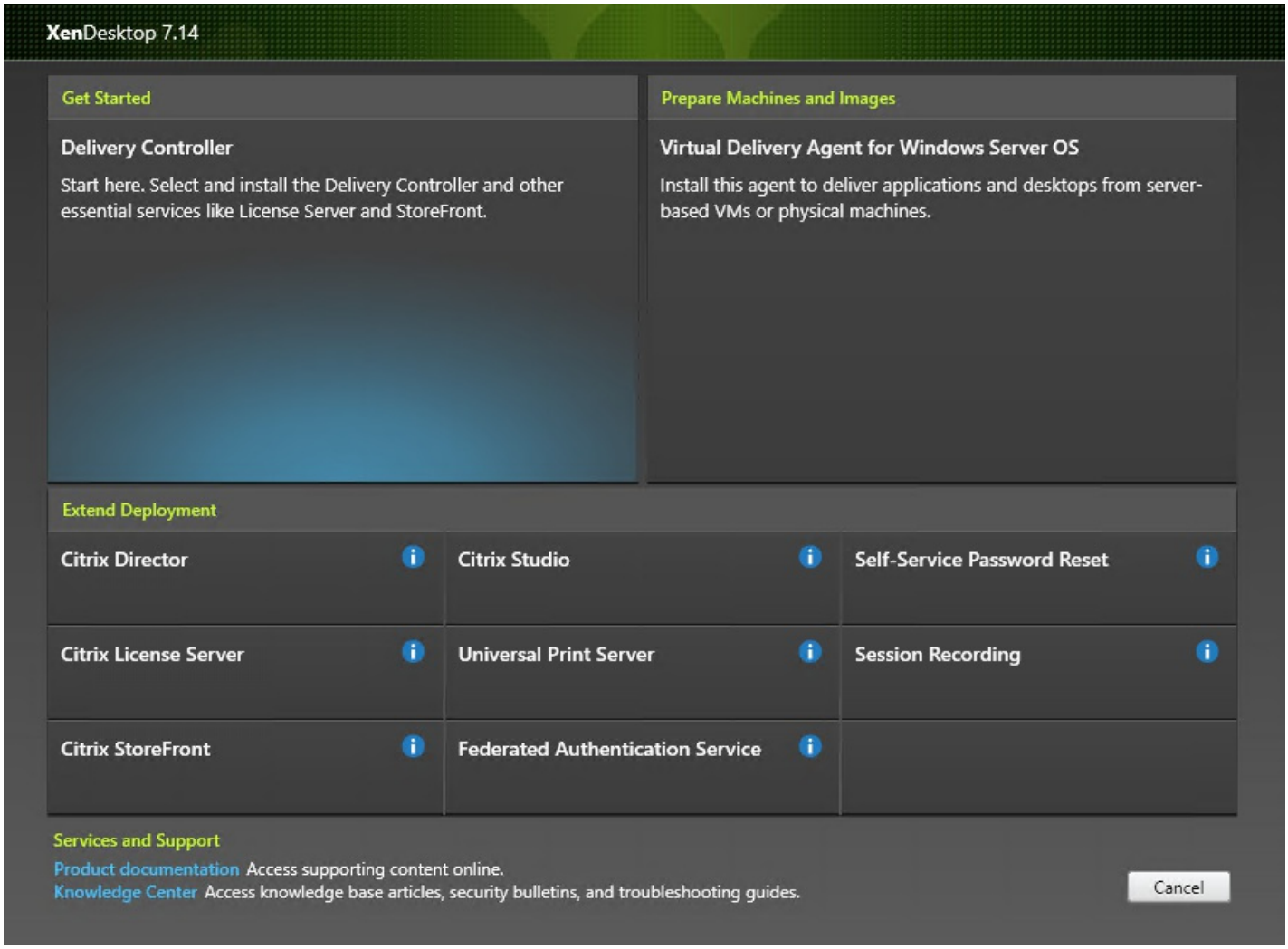
步骤 2：选择要安装的产品



单击产品旁边的**开始**安装：**XenApp** 或 **XenDesktop**。

步骤 3：选择 Session Recording

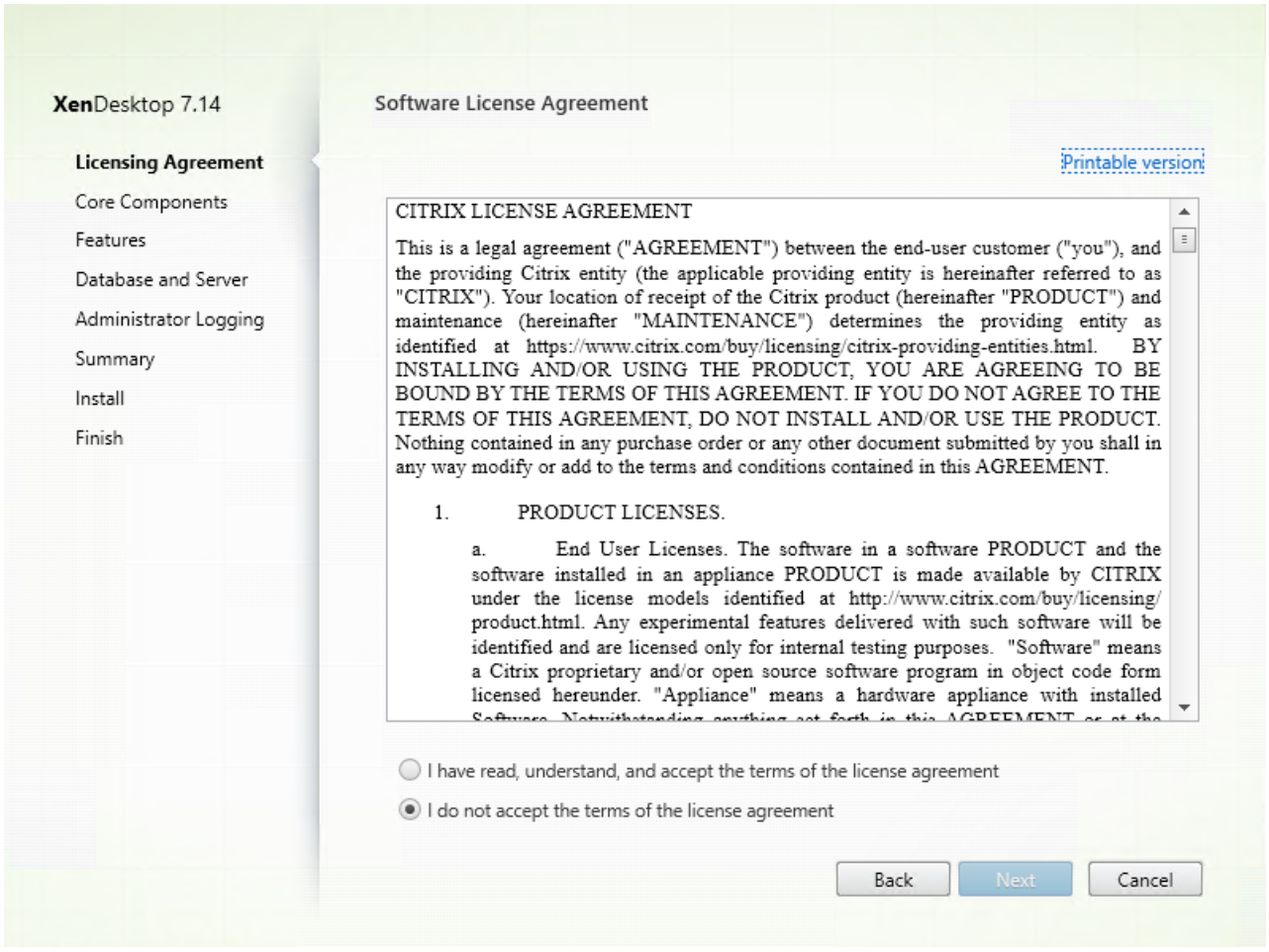
© 1999-2017 Citrix Systems, Inc. All rights reserved.



选择 **Session Recording** 条目。

步骤 4：阅读并接受许可协议

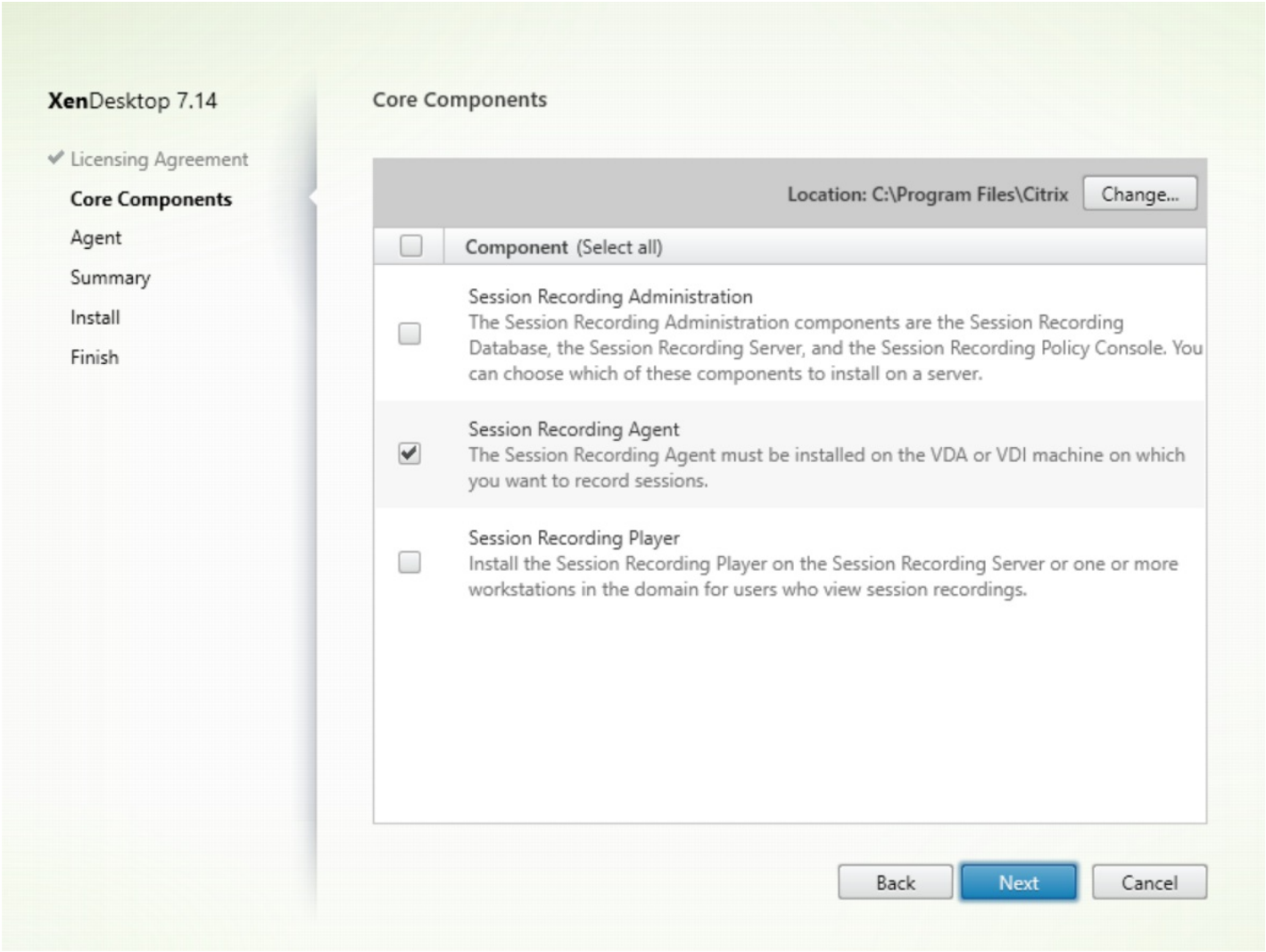
© 1999-2017 Citrix Systems, Inc. All rights reserved.



在**软件许可协议**页面上，阅读并接受许可协议，然后单击**下一步**

步骤 5：选择要安装的组件及安装位置

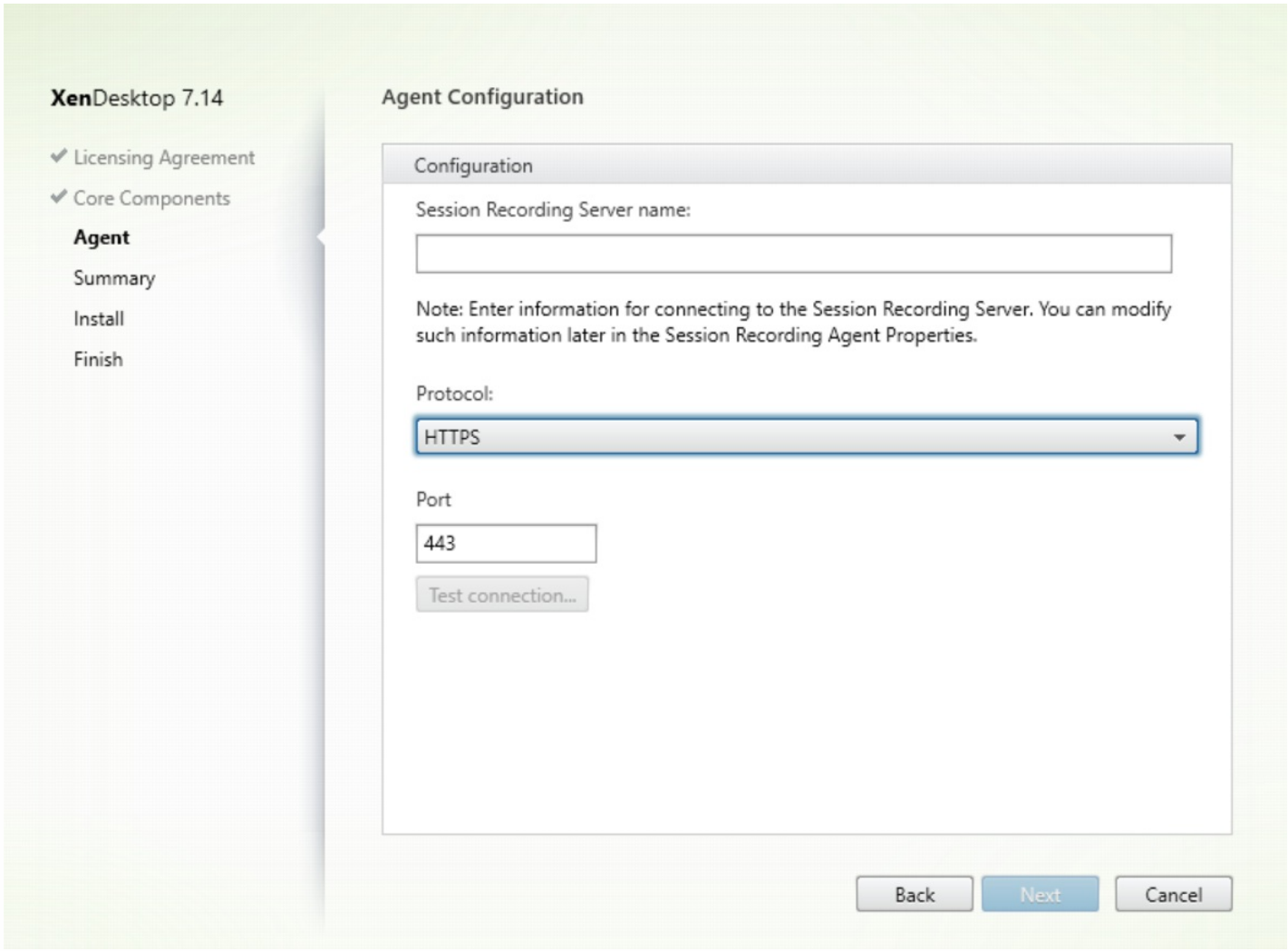
© 1999-2017 Citrix Systems, Inc. All rights reserved.



选择 **Session Recording Agent** 并单击下一步。

步骤 6：指定代理配置

© 1999-2017 Citrix Systems, Inc. All rights reserved.



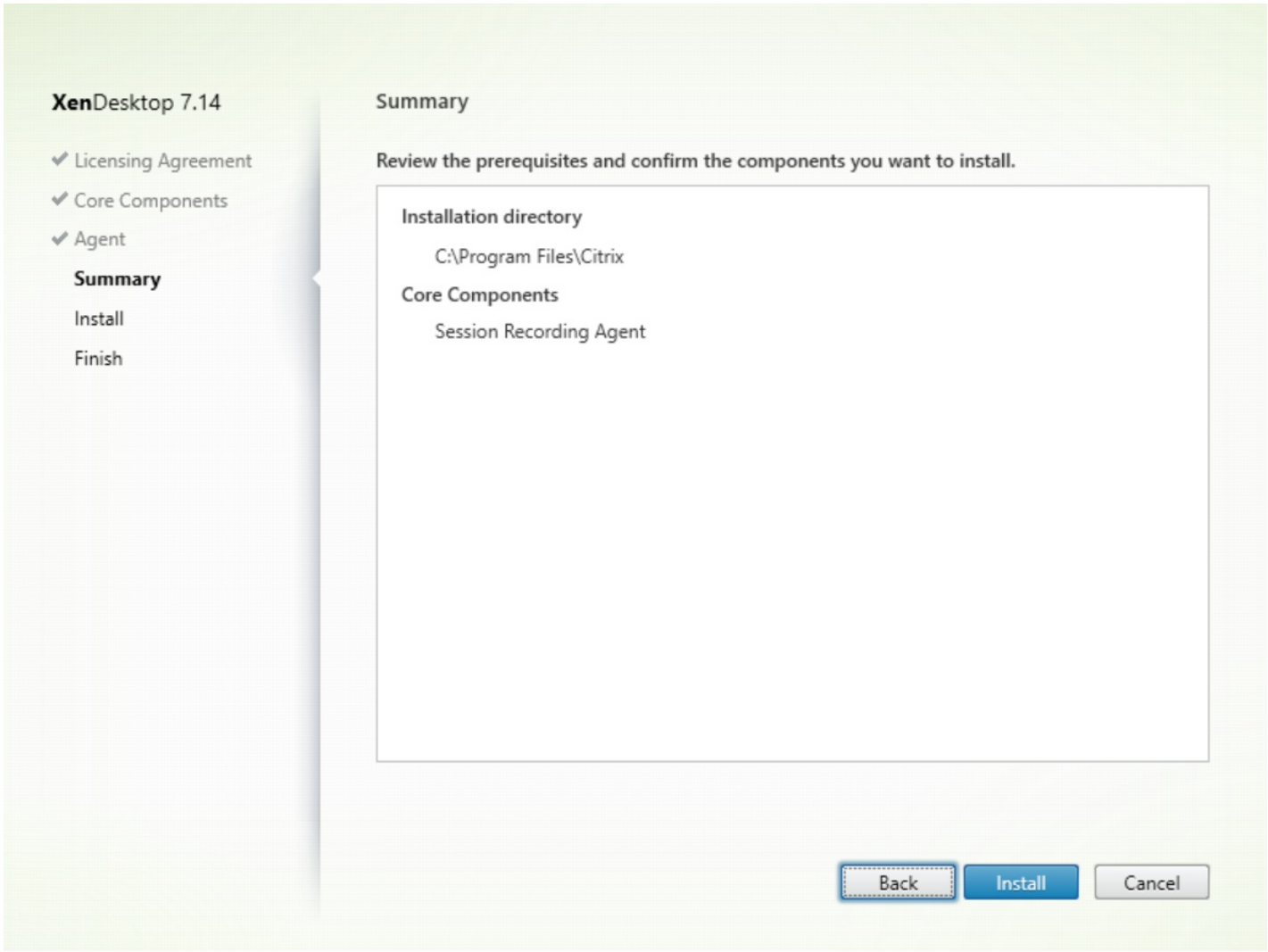
在**代理配置**页面上：

- 如果提前安装了 Session Recording Server，请输入安装了 Session Recording Server 的计算机名称，以及用于连接到 Session Recording Server 的协议和端口信息。如果尚未安装 Session Recording，以后可以在 **Session Recording Agent 属性**中修改此类信息。

注意：安装程序的测试连接功能存在限制。它不支持“HTTPS 需要 TLS 1.2”的情况。如果您在这种情况下使用安装程序，测试连接会失败，但您可以忽略失败，并单击 **下一步**继续安装。这不影响正常的功能运行。

步骤 7：查看必备项并确认安装

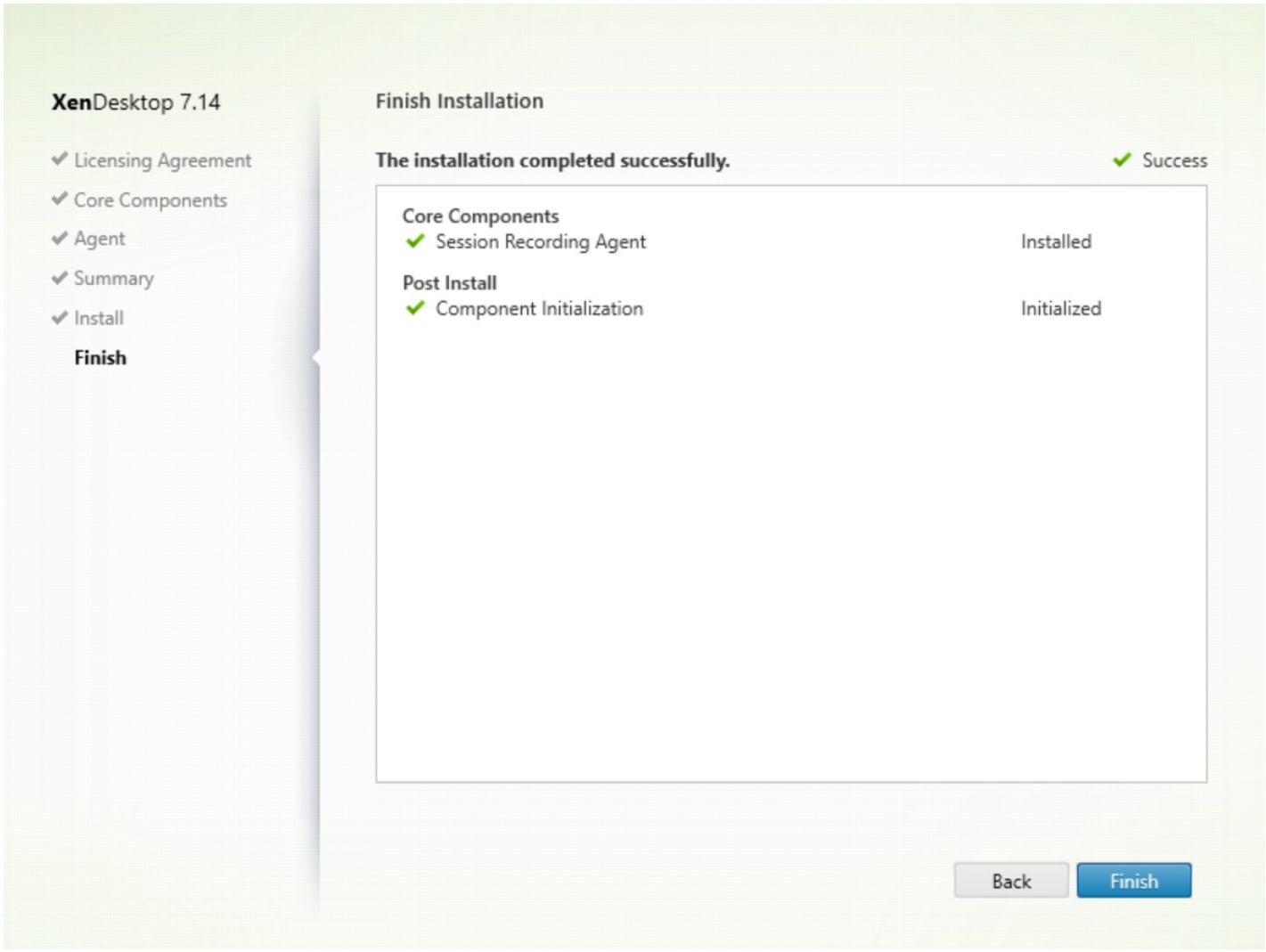
© 1999-2017 Citrix Systems, Inc. All rights reserved.



摘要页面上将显示您所做安装选择。可以单击**返回**返回到之前的向导页面并进行更改。或者单击**安装**开始安装。

步骤 8：完成安装

© 1999-2017 Citrix Systems, Inc. All rights reserved.



完成安装页面上显示带绿色复选标记的所有已成功安装和初始化的必备项和组件。

单击**完成**以完成 Session Recording Agent 的安装。

注意：如果 Machine Creation Services (MCS) 或 Provisioning Services (PVS) 创建的多个 VDA 具有配置的主映像并安装了 Microsoft 消息队列 (MSMQ)，则在某些情况下，这些 VDA 可能具有相同的 QMId。这样可能会导致各种问题，例如：

- 即使接受了录制协议，也可能无法录制会话。
- Session Recording Server 可能收不到会话注销信号，从而导致会话可能始终处于活动状态。

解决方法：为每个 VDA 创建唯一的 QMId，并且因部署方法而异。

如果安装了 Session Recording Agent 的桌面操作系统 VDA 是在静态桌面模式下使用 PVS 7.7 或更高版本以及 MCS 7.9 或更高版本创建的，则无需执行任何额外的操作；即，经过配置后，VDA 的独立个人虚拟磁盘或本地磁盘上的所有更改都是永久性的。

如果通过 MCS 或 PVS 创建的服务器操作系统 VDA 或桌面操作系统 VDA 配置为在用户注销时放弃所有更改，请使用 GenRandomQMID.ps1 脚本在系统启动时修改 QMId。请修改电源管理策略，以确保在用户尝试登录之前正在运行足够的 VDA。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

要使用 GenRandomQMID.ps1 脚本，请执行以下操作：

1. 确保在 PowerShell 中，将执行策略设置为 **RemoteSigned** 或**不限制**。

   Set-ExecutionPolicy RemoteSigned

2. 创建一项计划任务并在系统启动时设置一个触发器，然后在 PVS 或 MCS 主映像计算机上通过 SYSTEM 帐户运行。

3. 将该命令添加为启动任务。

   powershell .exe -file C:\GenRandomQMID.ps1

GenRandomQMID.ps1 脚本的摘要如下：

1. 从注册表中删除当前 QMId。
2. 将 SysPrep = 1 添加到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Parameters。
3. 停止相关访问，包括 CitrixSmAudAgent 和 MSMQ。
4. 要生成随机 QMId，请启动之前已停止的服务。

GENRANDOMQMID.PS1（供参考） 复制

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
# Remove old QMId from registry and set SysPrep flag for MSMQ

Remove-Itemproperty -Path HKLM:Software\Microsoft\MSMQ\Parameters\MachineCache -Name QMId -Force

Set-ItemProperty -Path HKLM:Software\Microsoft\MSMQ\Parameters -Name "SysPrep" -Type DWord -Value 1

# Get dependent services

$depServices = Get-Service -name MSMQ -dependentservices | Select -Property Name

# Restart MSMQ to get a new QMId

Restart-Service -force MSMQ

# Start dependent services

if ($depServices -ne $null) {

    foreach ($depService in $depServices) {

        $startMode = Get-WmiObject win32_service -filter "NAME = '$($depService.Name)'" | Select -Property StartMode

        if ($startMode.StartMode -eq "Auto") {

            Start-Service $depService.Name

        }

}

}
```

安装 Session Recording Player

在 Session Recording Server 或域中的一个或多个工作站上为查看会话录制件的用户安装 Session Recording Player。

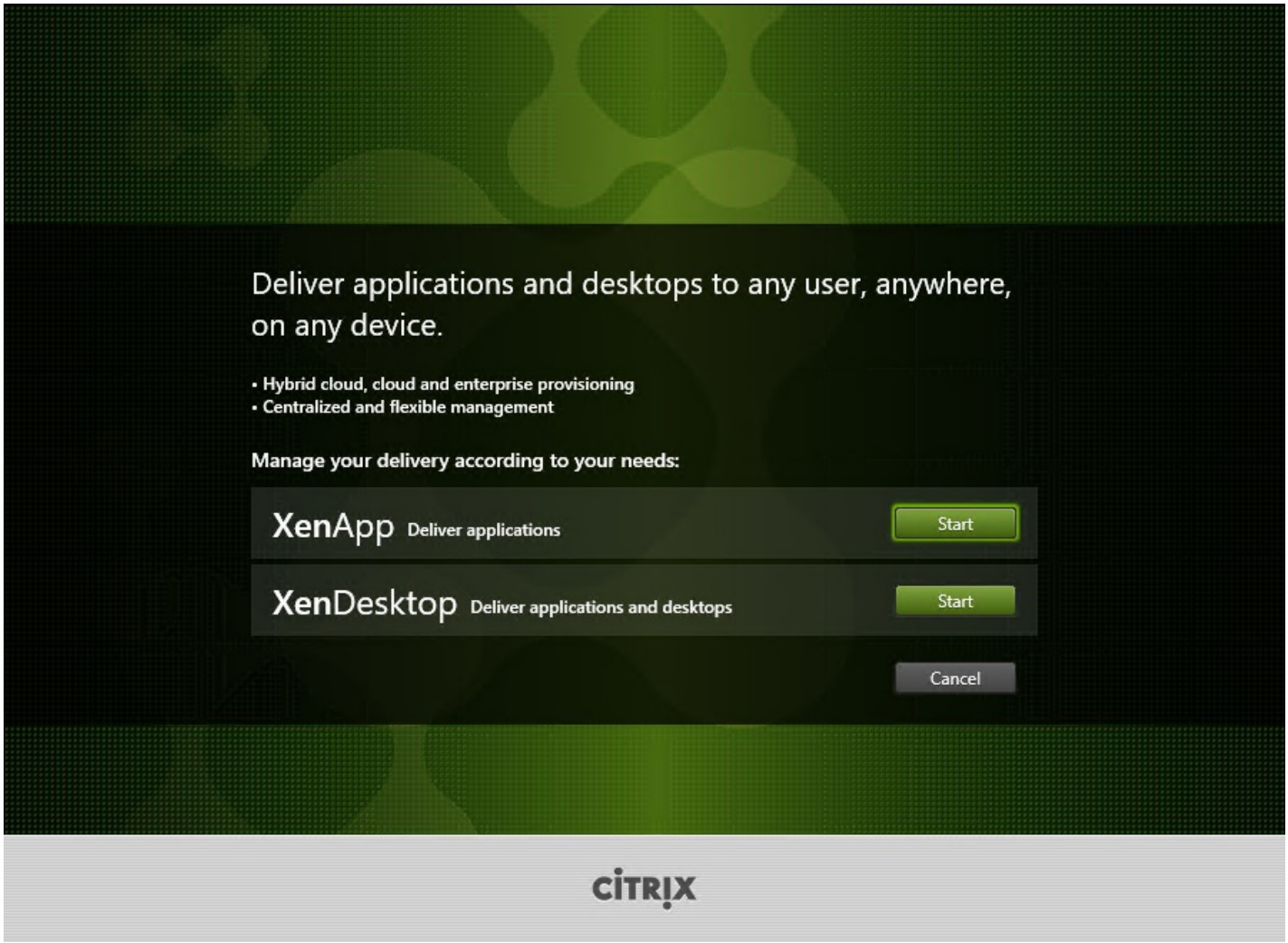
步骤 1：下载产品软件并启动向导

© 1999-2017 Citrix Systems, Inc. All rights reserved.

使用本地管理员帐户，登录要在其中安装 Session Recording Player 组件的计算机。在驱动器中插入 DVD 或装载 ISO 文件。如果安装程序未自动启动，请双击 **AutoSelect** 应用程序或已装载的驱动器。

将启动安装向导。

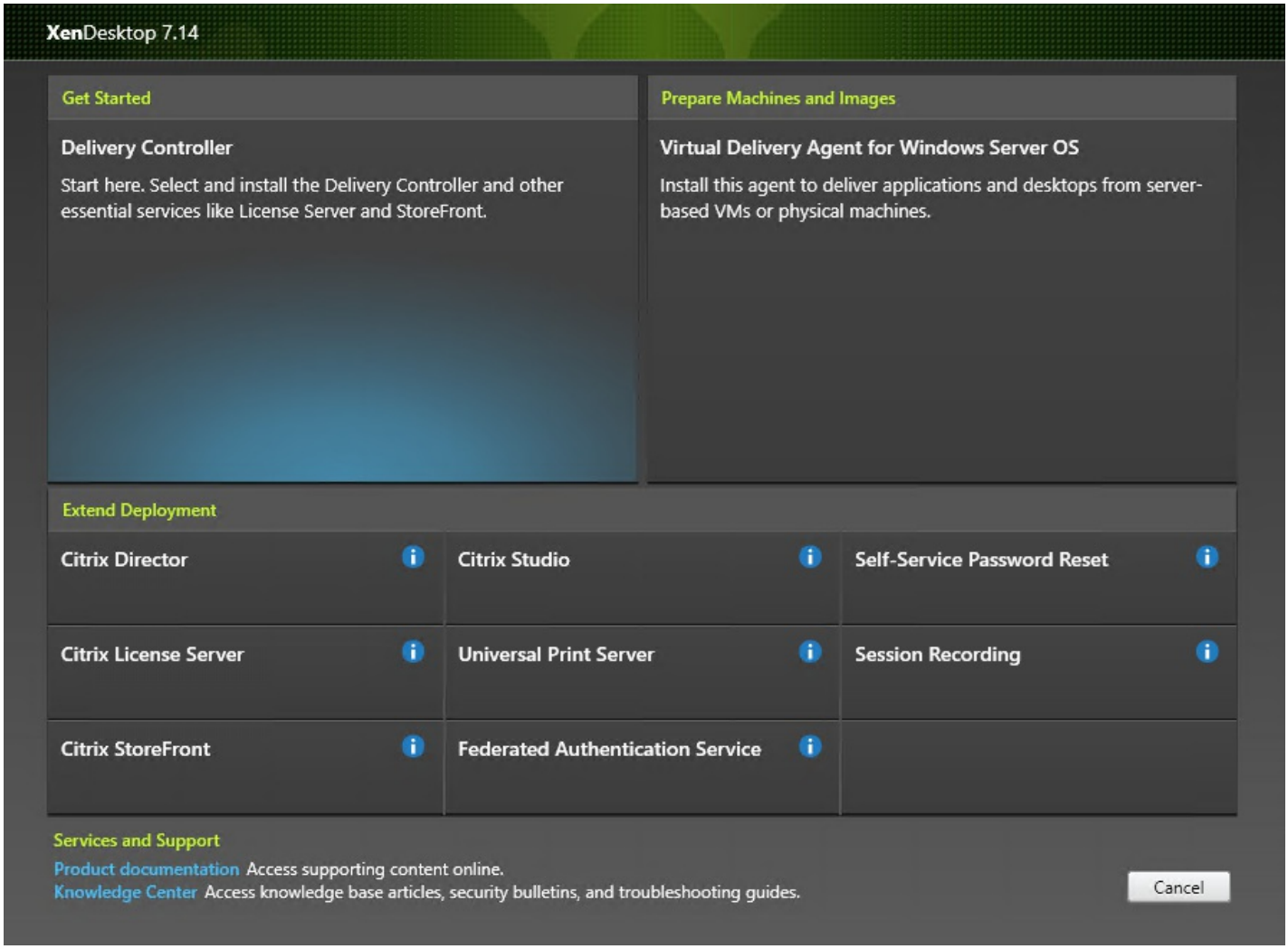
步骤 2：选择要安装的产品



单击产品旁边的**开始**安装：**XenApp** 或 **XenDesktop**。

步骤 3：选择 Session Recording

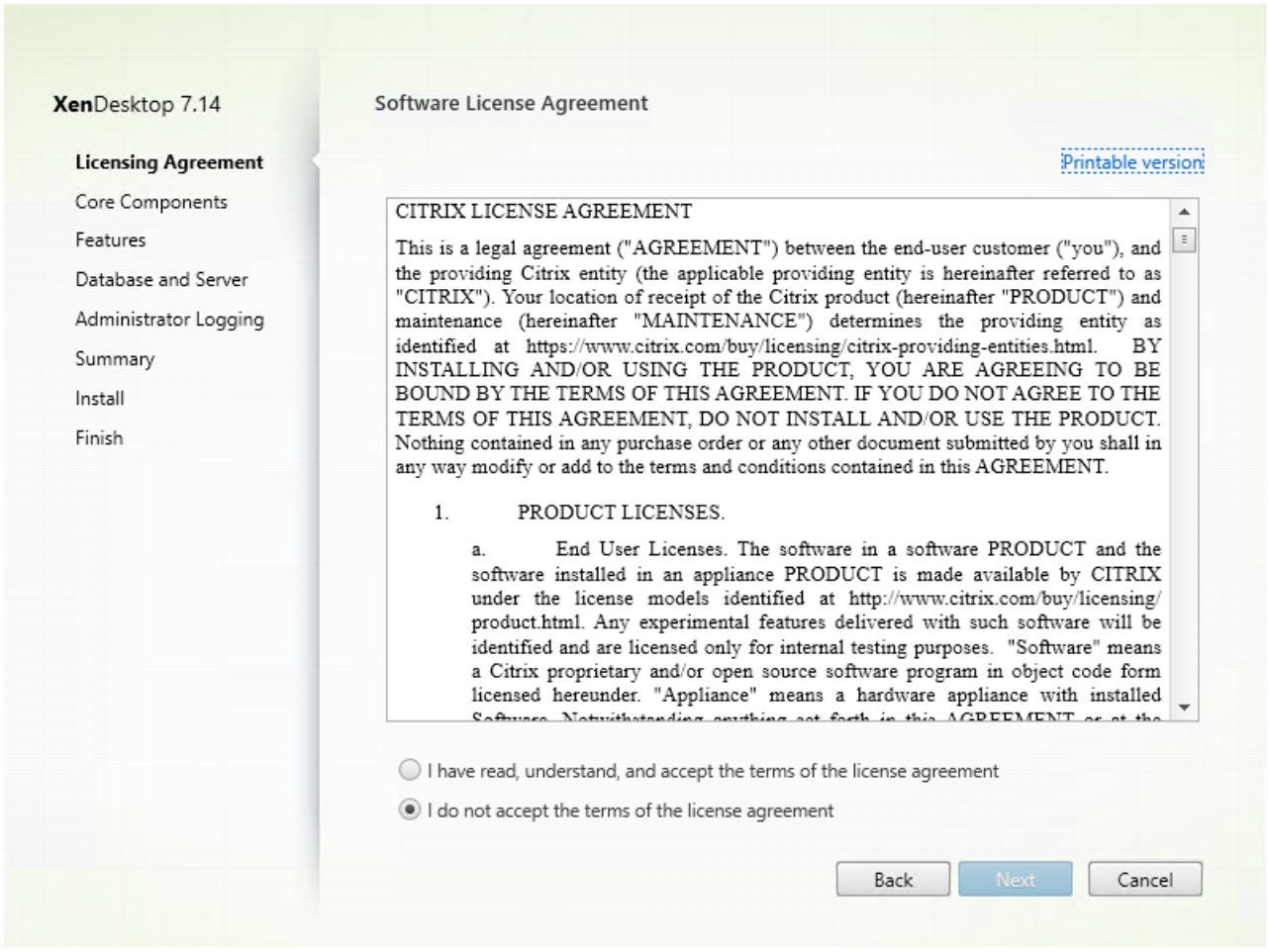
© 1999-2017 Citrix Systems, Inc. All rights reserved.



选择 **Session Recording** 条目。

步骤 4：阅读并接受许可协议

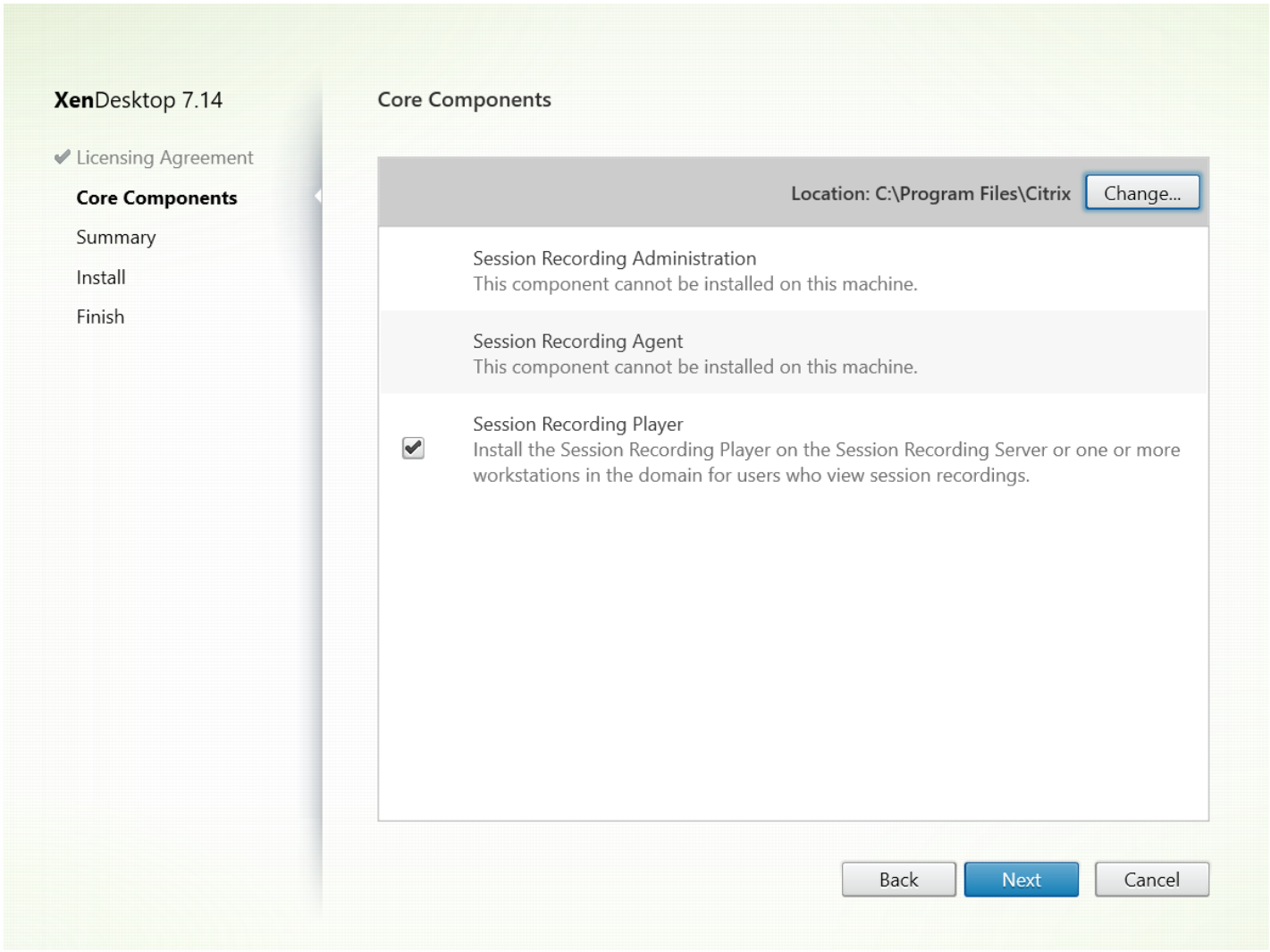
© 1999-2017 Citrix Systems, Inc. All rights reserved.



在**软件许可协议**页面上，阅读并接受许可协议，然后单击**下一步**

步骤 5：选择要安装的组件及安装位置

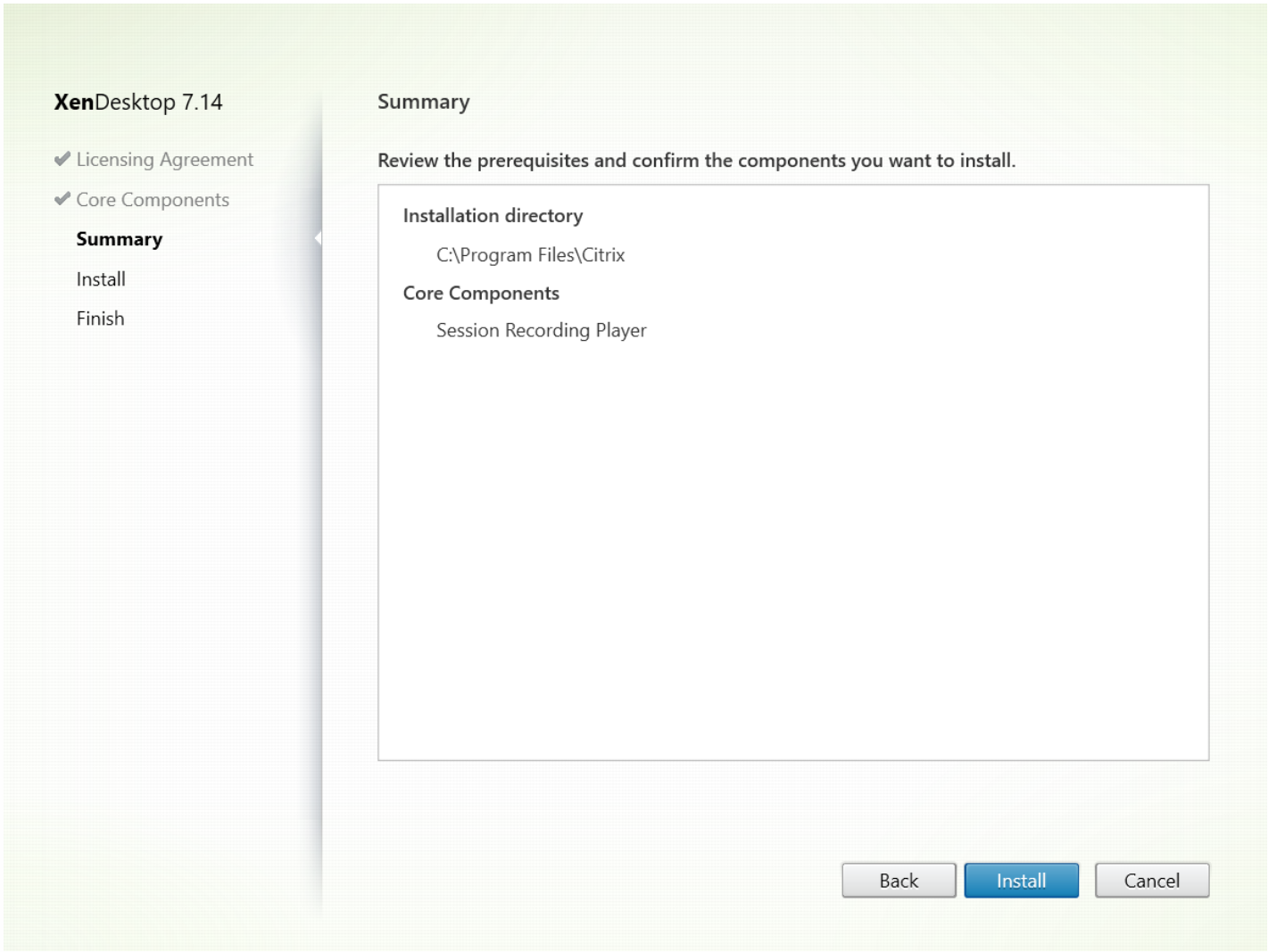
© 1999-2017 Citrix Systems, Inc. All rights reserved.



选择 **Session Recording Player** 并单击下一步。

步骤 6：查看必备项并确认安装

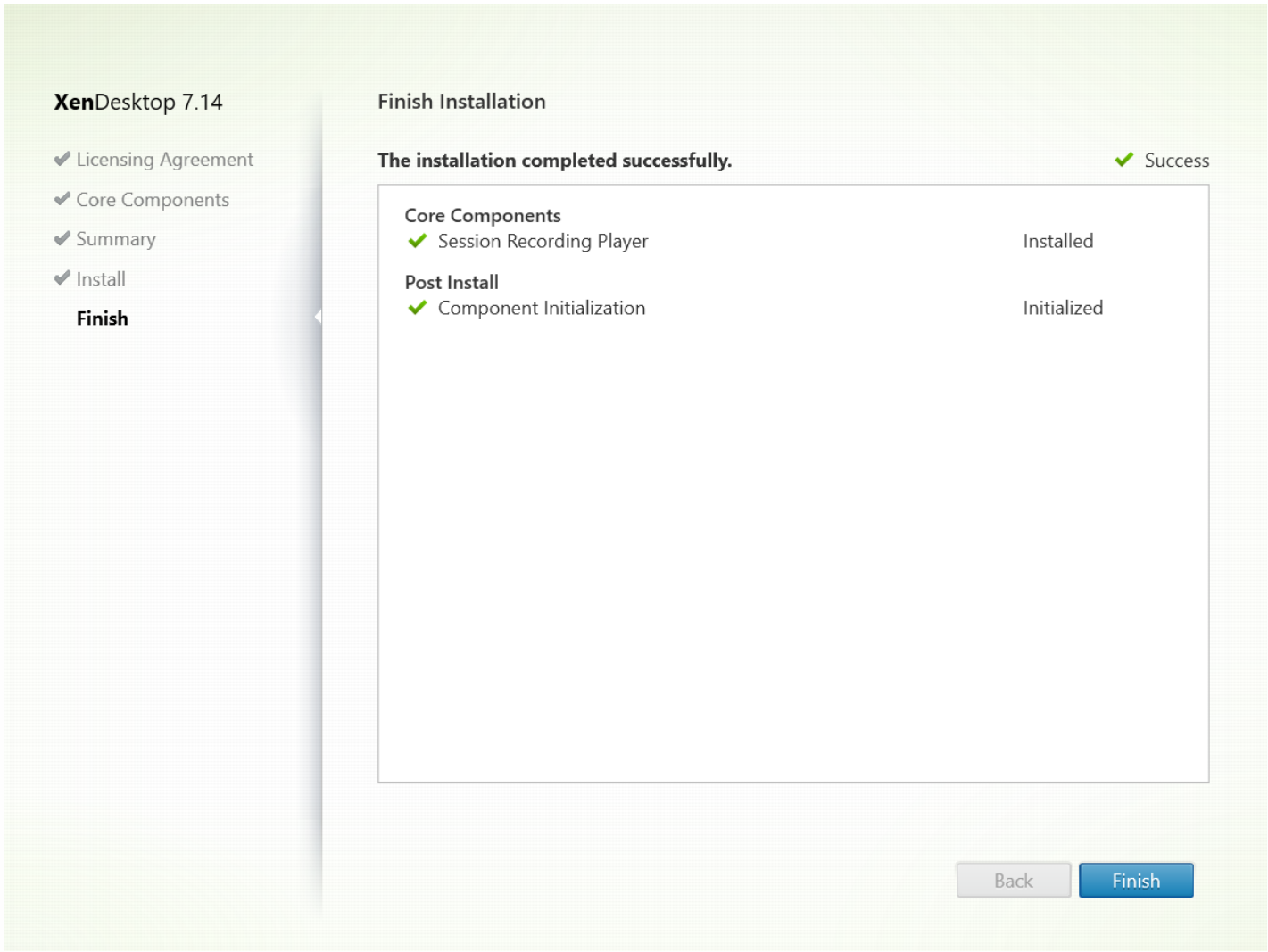
© 1999-2017 Citrix Systems, Inc. All rights reserved.



摘要页面上将显示您所做安装选择。可以单击**返回**返回到之前的向导页面并进行更改。或者单击**安装**开始安装。

步骤 7：完成安装

© 1999-2017 Citrix Systems, Inc. All rights reserved.



完成安装页面上显示带绿色复选标记的所有已成功安装和初始化的必备项和组件。

单击**完成**以完成 Session Recording Player 的安装。

自动安装

要在多台服务器上安装 Session Recording Agent，请编写一个进行无提示安装的脚本。

以下命令行可安装 Session Recording Agent，并创建一个日志文件，用于捕获安装信息。

对于 64 位系统：

msiexec /i SessionRecordingAgentx64.msi /q /l*vx *yourinstallationlog* SESSIONRECORDINGSERVERNAME=yourservername SESSIONRECORDINGBROKERPROTOCOL=yourbrokerprotocol SESSIONRECORDINGBROKERPORT=yourbrokerport

注意：XenApp/XenDesktop ISO 中的 SessionRecordingAgentx64.msi 文件位于 \layout\image-full\x64\Session Recording 下面。

在 32 位系统中：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

msiexec /i SessionRecordingAgent.msi /q /l*vx *yourinstallationlog* SESSIONRECORDINGSERVERNAME=yourservername SESSIONRECORDINGBROKERPROTOCOL=yourbrokerprotocol SESSIONRECORDINGBROKERPORT=yourbrokerport

注意：XenApp/XenDesktop ISO 中的 SessionRecordingAgent.msi 文件位于 \layout\image-full\x86\Session Recording 下面。

其中：

yourservername 是托管 Session Recording Server 的计算机的 NetBIOS 名称或 FQDN。如未指定，则此值默认为 **localhost**。

yourbrokerprotocol 是指 Session Recording Agent 与 Session Recording Broker 进行通信时使用的 HTTP 或 HTTPS。如果未指定，则此值默认为 HTTPS。

yourbrokerport 是 Session Recording Agent 用于与 Session Recording Broker 通信的端口号。如未指定，则此值默认为零，从而指示 Session Recording Agent 使用所选协议的默认端口号：对于 HTTP 使用 80，对于 HTTPS 使用 443。

/l*v 指定详细模式日志记录。

yourinstallationlog 是安装日志文件的位置。

/q 指定无提示模式。

升级 Session Recording

您可以将某些部署升级到更高版本，而无需事先设置新计算机或站点。可以将 Session Recording 7.6（或更高版本）升级到最新发布的 Session Recording。

注意：

- 将 Session Recording Administration 从 7.6 升级到 7.13 或更高版本时，如果在 Session Recording Administration 中选择**修改**以添加管理员日志记录服务，SQL Server 实例名称将不显示在**管理员日志记录配置**页面上。单击**下一步**时将显示以下错误消息：数据库连接测试失败。请输入正确的数据库实例名称。解决方法：将 localhost 用户的读取权限添加到以下 SmartAuditor 服务器注册表文件夹：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server。
- 如果计算机上仅安装了一个组件，尝试升级 Session Recording 数据可能会失败。在这种情况下，请检查 HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\SmartAuditor\Database 下是否存在以下注册表项。如果不存在，请先手动添加这些注册表项，然后再升级。

注册表项名称	注册表项类型	注册表项值
SmAudDatabaseInstance	字符串	您的 Session Recording 数据库的实例名称
DatabaseName	字符串	您的 Session Recording 数据库的数据库名称

要求、准备和限制

注意：不能从技术预览版进行升级。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

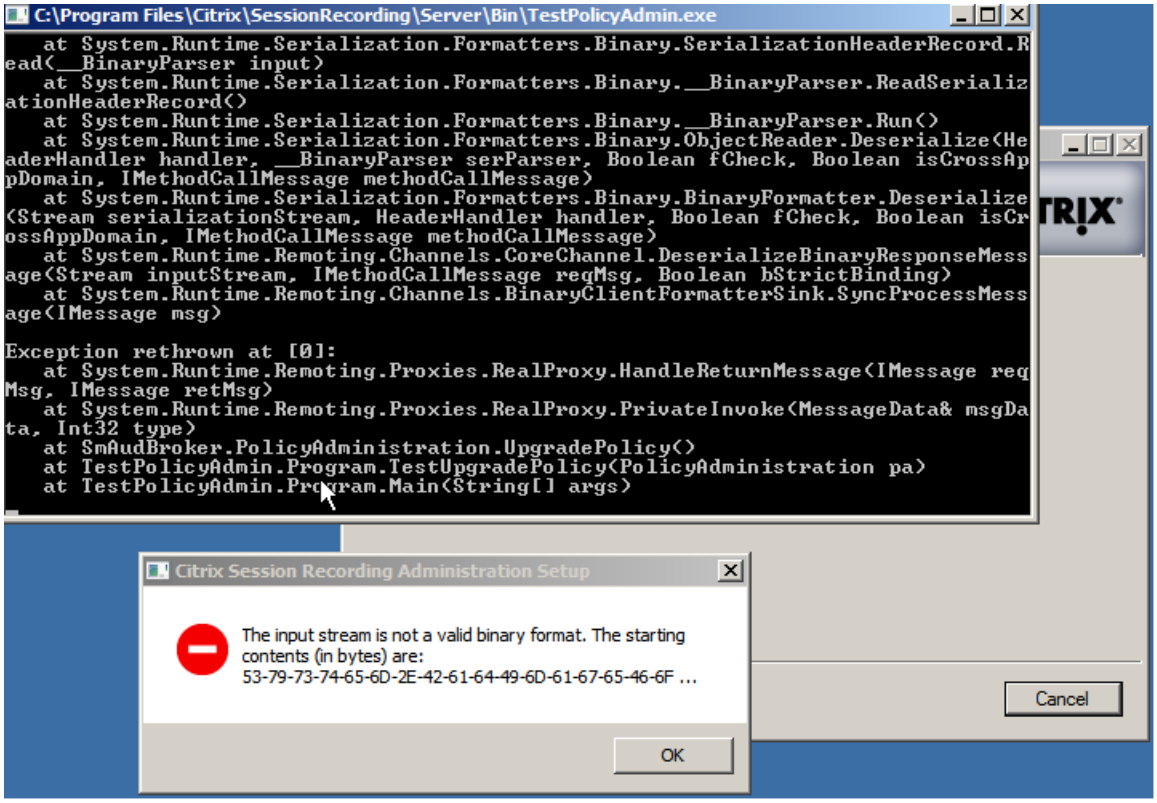
- 必须在安装了 Session Recording 组件的计算机上使用 Session Recording 安装程序的图形界面或命令行界面来升级 Session Recording 组件。
- 在开始任何升级活动之前，请备份 SQL Server 实例中名为 CitrixSessionRecording 的数据库，这样，如果在该数据库升级之后发现任何问题，您就可以进行还原。
- 您不仅要具有域用户的身份，还必须是要升级 Session Recording 组件的计算机上的本地管理员。
- 如果 Session Recording Server 和 Session Recording 数据库未安装在同一台服务器上，则您必须具有升级 Session Recording 数据库的数据库角色权限；否则，您可以
  - 要求数据库管理员分配用于升级的 **securityadmin** 和 **dbcreator** 服务器角色权限。升级完成后，就不再需要 **securityadmin** 和 **dbcreator** 服务器角色权限了，可以安全删除。
  - 或者使用 SessionRecordingAdministrationx64.msi 软件包升级。在 msi 升级期间，会显示一个对话框，提示提供具有 **securityadmin** 和 **dbcreator** 服务器角色权限的数据库管理员的凭据。请输入正确的凭据，然后单击**确定**以继续升级。
- 如果不想同时升级所有 Session Recording Agent，则可以将 Session Recording Agent 7.6.0（或更高版本）与最新（当前）版本的 Session Recording Server 结合使用。但是，某些新增功能和缺陷修复可能不起作用。
- 在 Session Recording Server 升级过程中启动的任何会话不会进行录制。
- 执行全新安装或升级后，默认情况下启用 Session Recording Agent 属性中的**图形调整**，以与桌面组合重定向模式保持兼容。可以在执行全新安装或升级后手动禁用此选项。
- 从不包含管理员日志记录功能的之前版本更新 Session Recording 之后，不会安装管理员日志记录功能。要添加该新功能，请在升级之后修改安装。
- 如果升级过程开始时存在实时录制会话，能够完成录制的可能性非常小。
- 请查看以下升级顺序，以便您能够制定规划并避免可能出现的中断。

升级顺序

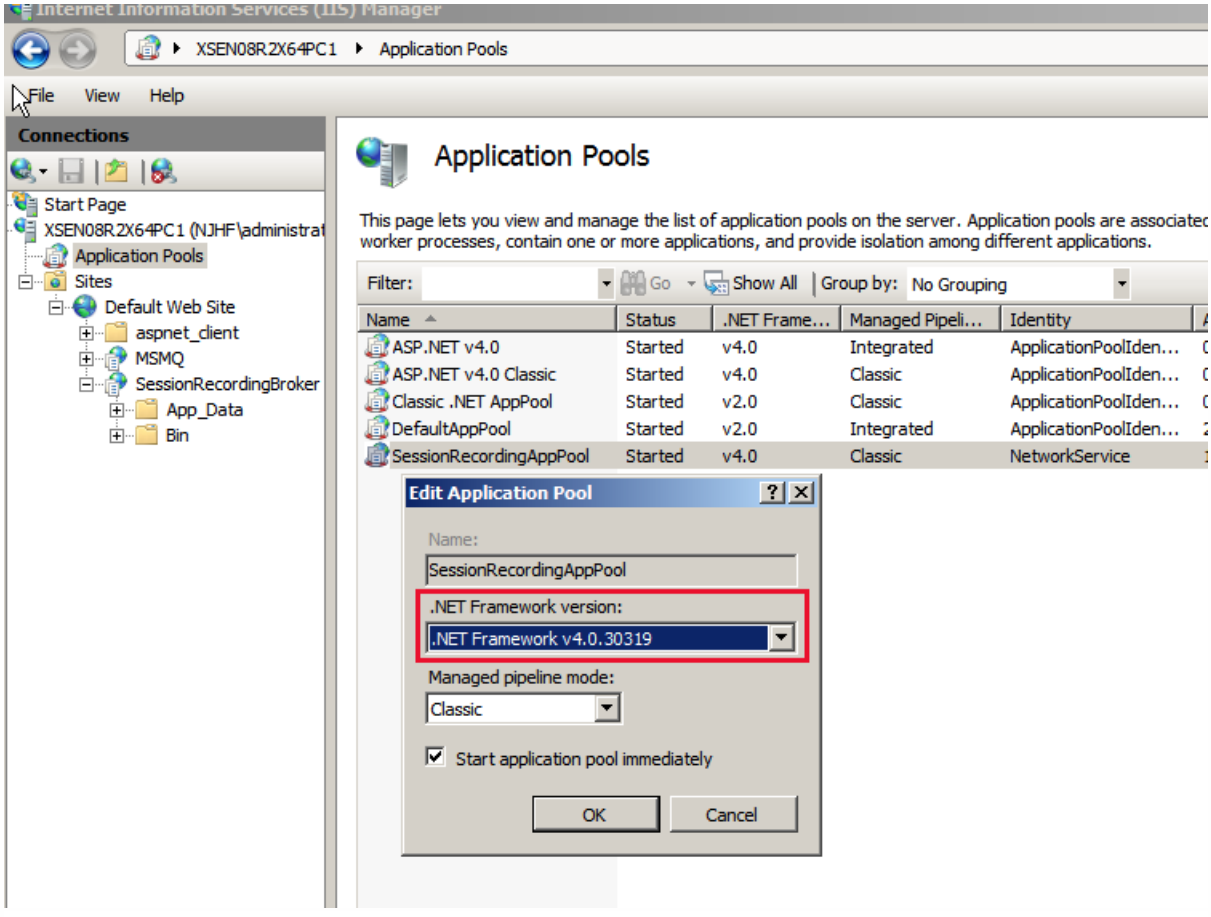
1. 如果 Session Recording 数据库和 Session Recording Server 安装在不同服务器上，请在 Session Recording Server 上手动停止 Session Recording Storage Manager 服务，然后优先升级 Session Recording 数据库。
2. 请确保 Session Recording Broker 正在与 IIS 服务同时运行。升级 Session Recording Server。如果 Session Recording 数据库和 Session Recording Server 安装在同一台服务器上，则 Session Recording 数据库也会同时升级。
3. Session Recording Server 升级完成后，Session Recording 服务会自动恢复联机。
4. （在主映像上）升级 Session Recording Agent。
5. 同时升级 Session Recording 策略控制台和 Session Recording Server，或者先升级 Session Recording Server，再升级 Session Recording 策略控制台。
6. 升级 Session Recording Player。

注意：升级 Windows Server 2008 R2 上的 Session Recording Administration 组件时可能会出现以下错误。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



在这种情况下，请将“SessionRecordingAppPool”的“.NET Framework version”更改为“.NET Framework v4”，然后再重新升级。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

卸载 Session Recording

要从服务器或工作站中删除 Session Recording 组件，请使用 Windows“控制面板”中提供的卸载或删除程序选项。要删除 Session Recording 数据库，您必须具有与安装时同样的 **securityadmin** 和 **dbcreator** SQL Server 角色权限。

出于安全原因，在卸载组件之后不会删除管理员日志记录数据库。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置 Session Recording

Dec 05, 2017

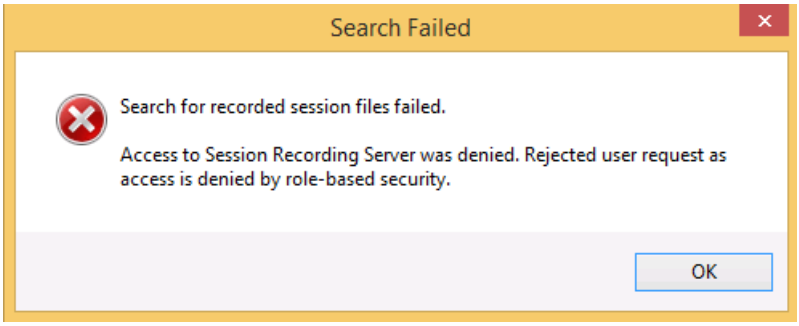
配置用于播放和录制会话的 Session Recording

安装 Session Recording 组件后，执行以下步骤以将 Session Recording 配置为录制 XenApp 或 XenDesktop 会话并允许用户查看这些会话：

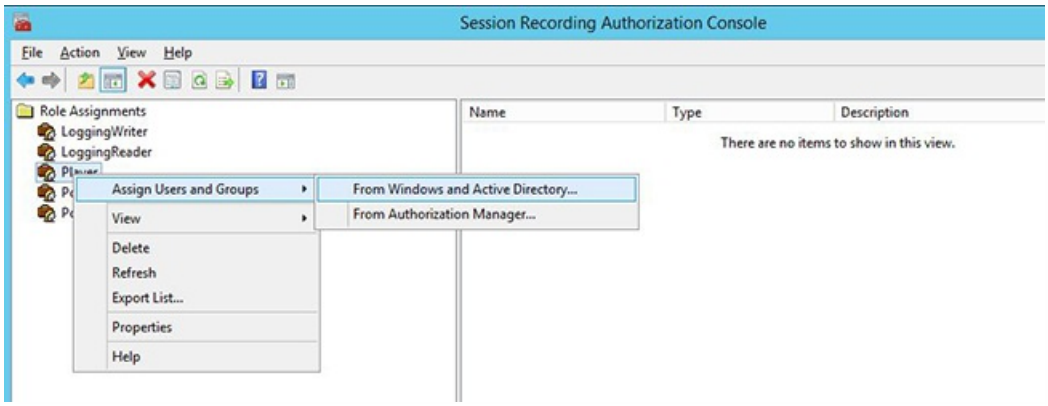
- 授权用户播放录制件
- 授权用户管理录制策略
- 将活动录制策略设置为录制会话
- 配置自定义策略
- 配置用于连接至 Session Recording Server 的 Session Recording Player

授权用户播放录制的会话

安装 Session Recording 时，所有用户都没有播放录制的会话的权限。必须向包括管理员在内的每位用户分配权限。如果用户没有播放录制的会话所需的权限，则在尝试播放录制的会话时会收到以下错误消息：



1. 以管理员身份登录托管 Session Recording Server 的计算机。
2. 启动 Session Recording Authorization 控制台。
3. 在 Session Recording Authorization 控制台上，选择播放器。
4. 添加要授权其查看录制的会话的用户和组，这些用户和组将填充到右侧窗格中。



授权用户管理录制策略

安装 Session Recording 时，域管理员默认授予控制录制策略的权限。您可以更改授权设置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

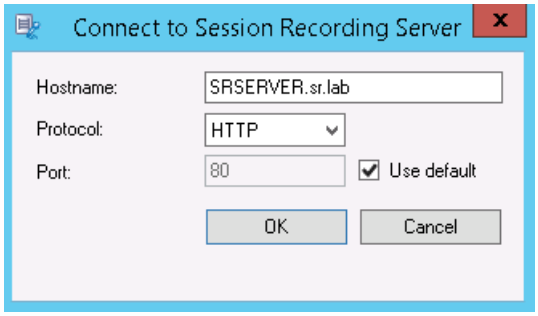
1. 以管理员身份登录托管 Session Recording Server 的计算机。
2. 启动 Session Recording Authorization 控制台并选择策略管理员。
3. 添加能够管理录制策略的用户和组。

将活动录制策略设置为录制会话

活动录制策略用于指定安装了 Session Recording Agent 并连接到 Session Recording Server 的所有 VDA 或 VDI 上的会话录制行为。安装 Session Recording 时，活动录制策略为**不录制**。更改活动录制策略之后才会录制会话。

重要：一个策略中可以包含多条规则，但一次只能运行一个活动策略。

1. 以授权策略管理员身份登录安装了 Session Recording 策略控制台的服务器。
2. 启动 Session Recording 策略控制台。
3. 如果显示**连接到 Session Recording Server**对话框，请确保托管 Session Recording Server 的计算机名称、协议和端口号正确无误。



4. 在 Session Recording 策略控制台中，展开**录制策略**。此时将显示安装 Session Recording 时提供的录制策略，以及一个复选标记，用于指示处于活动状态的策略：
   - **不录制**。此为默认策略。如果未指定其他策略，则不会录制会话。
   - **录制每个人并通知**。如果选择此策略，则会录制所有会话。将显示一个窗口来通知发生录制事件。
   - **录制每个人但不通知**。如果选择此策略，则将录制所有会话。不显示任何窗口来通知发生录制事件。
5. 选择要设置为活动策略的策略。
6. 从菜单栏中，依次选择**操作** > **激活策略**。

Session Recording 允许您创建自己的录制策略。创建录制策略时，创建的策略将在 Session Recording 策略控制台的“录制策略”文件夹中显示。
通用录制策略可能不满足您的要求。可以根据用户、VDA 和 VDI 服务器、交付组以及应用程序配置策略和规则。有关自定义策略的详细信息，请参阅创建自定义录制策略。
注意：借助 Session Recording 的管理员日志记录功能，您可以记录录制策略更改。有关详细信息，请参阅日志管理活动。

配置 Session Recording Player

在 Session Recording Player 可以播放会话之前，必须对其进行配置，使其连接到存储已录制会话的 Session Recording Server。每个 Session Recording Player 均可配置为能够与多个 Session Recording Server 连接，但一次只能连接到一个 Session Recording Server。如果此 Player 在经过配置后能够连接到多个 Session Recording Server，则用户可以通过选中**工具** > **选项**中**连接**选项卡上的复选框来更改此 Player 要连接到的 Session Recording Server。

1. 登录到安装了 Session Recording Player 的工作站。
2. 启动 Session Recording Player。
3. 从 Session Recording Player 菜单栏，选择**工具** > **选项**。
4. 在**连接**选项卡中，单击**添加**。
5. 在**主机名**字段中，键入托管 Session Recording Server 的计算机的名称或 IP 地址，然后选择协议。默认情况下，Session

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Recording 会配置为使用 HTTPS/SSL 来保证通信安全。如果未配置 SSL，请选择“HTTP”。

6. 要配置 Session Recording Player，使其能够连接到多个 Session Recording Server，请对每个 Session Recording Server 重复步骤 4 和 5。
7. 请务必选中要连接到的 Session Recording Server 对应的复选框。

配置与 Session Recording Server 的连接

安装 Session Recording Agent 时，通常会配置 Session Recording Agent 与 Session Recording Server 之间的连接。要在安装 Session Recording Agent 后配置此连接，请使用 Session Recording Agent Properties。

1. 登录到安装了 Session Recording Agent 的服务器。
2. 从**开始**菜单中，选择 **Session Recording Agent Properties**。
3. 单击**连接**选项卡。
4. 在 **Session Recording Server** 字段中，键入服务器名称或其 IP 地址。
5. 在 **Session Recording Storage Manager 消息队列**部分，选择 Session Recording Storage Manager 用于进行通信的协议并修改默认端口号（如有必要）。
6. 在**消息生存期**字段中，接受默认值 7200 秒（2 小时），或者键入一个新值，表示在通信失败后每条消息在队列中保留的秒数。超过此时间段之后，将删除该消息，且文件可播放，直至数据丢失点停止。
7. 在 **Session Recording Broker** 部分中，选择 Session Recording Broker 用于通信的通信协议，并修改默认端口号（如果需要）。
8. 出现系统提示时，重新启动 **Session Recording Agent 服务**以接受所做更改。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

授予用户访问权限

Dec 05, 2017

> **Important**
>
> 出于安全原因，请只授予用户执行特定功能（例如查看记录的会话）所需的权限。

可以通过使用 Session Recording Server 上的 Session Recording Authorization 控制台为 Session Recording 用户分配角色来授予其访问权限。Session Recording 用户具有三个角色：

- **播放者。**具有查看录制的 XenApp 会话的权限。此角色中没有默认成员身份。
- **策略查询者。**允许托管 Session Recording Agent 的服务器请求录制策略评估。默认情况下，经过身份验证的用户属于此角色的成员。
- **策略管理员。**具有查看、创建、编辑、删除以及启用录制策略的权限。默认情况下，托管 Session Recording Server 的计算机管理员属于此角色的成员。

Session Recording 支持在 Active Directory 中定义的用户和组。

向用户分配角色

1. 以管理员或策略管理员角色的成员身份登录到托管 Session Recording Server 的计算机。
2. 启动 Session Recording Authorization 控制台。
3. 选择要分配给用户的角色。
4. 从菜单栏中，依次选择**操作** > **Assign Windows Users and Groups**（分配 Windows 用户和组）。
5. 添加用户和组。

对控制台所做的任何更改都将于每分钟执行一次的更新期间生效。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

创建并激活录制策略

Dec 05, 2017

使用 Session Recording 策略控制台可创建并激活用于确定要录制的会话的策略。

重要：必须安装 Broker PowerShell 管理单元 (Broker_PowerShellSnapIn_x64.msi)，才能使用 Session Recording 策略控制台。该管理单元不能由安装程序自动安装。请在 XenApp/XenDesktop ISO (\layout\image-full\x64\Citrix Desktop Delivery Controller) 中找到该管理单元，然后按照说明手动安装。否则，会导致出现错误。

可以在安装 Session Recording 时激活可用的系统策略，也可以创建并激活自己的自定义策略。Session Recording 系统策略将单个规则应用于所有用户、已发布应用程序以及服务器。自定义策略指定要录制的用户、已发布应用程序以及服务器。

活动策略确定要录制的会话。 每次只能有一个策略处于活动状态。

系统策略

Session Recording 提供了以下系统策略：

- **不录制**。此为默认策略。如果未指定其他策略，则不会录制会话。
- **录制每个人并通知**。如果选择此策略，则会录制所有会话。此时将显示一个弹出窗口，通知出现录制事件。
- **录制每个人但不通知**。如果选择此策略，则会录制所有会话。此时不显示弹出窗口以通知出现录制事件。

无法修改或删除系统策略。

激活策略

1. 登录到安装了 Session Recording 策略控制台的服务器。
2. 启动 Session Recording 策略控制台。
3. 如果系统提示**连接到 Session Recording Server** 弹出窗口，请确保 Session Recording Server 名称、协议和端口正确无误。单击**确定**。
4. 在 Session Recording 策略控制台中，展开**录制策略**。
5. 选择要指定为活动策略的策略。
6. 从菜单栏中，依次选择**操作** > **激活策略**。

创建自定义录制策略

创建您自己的策略时，可以制定规则以指定录制哪些用户和组、已发布应用程序以及服务器的会话。Session Recording 策略控制台中的向导可帮助您创建规则。要获取已发布的应用程序和服务器列表，您必须具有站点管理员读取权限。在此站点的 Delivery Controller 上配置该权限。

对于创建的每条规则，您都需要指定录制操作以及规则条件。录制操作将应用到满足规则条件的会话。

对于每条规则，请选择一种录制操作：

- **不录制**。（在**规则**向导中选择**禁用会话录制**。）此录制操作将指定不录制满足规则条件的会话。
- **录制并通知**。（在**规则**向导中选择**启用会话录制并通知**。）此录制操作将指定录制满足规则条件的会话。此时将显示一个弹出窗口，通知出现录制事件。
- **录制但不通知**。（在**规则**向导中选择**启用会话录制但不通知**。）此录制操作将指定录制满足规则条件的会话。用户不知道系统正在录制其会话。

对于每条规则，请至少选择以下项目之一来创建规则条件：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **用户或组**。创建要应用规则的录制操作的用户或组列表。
- **已发布的资源**。创建要应用规则的录制操作的已发布应用程序或桌面列表。在**规则**向导中，请选择包含这些应用程序或桌面的一个或多个 XenApp/XenDesktop 站点。
- **交付组或计算机**。创建要应用规则的录制操作的交付组或计算机列表。在**规则**向导中，请选择交付组或计算机所在的位置。
- **IP 地址或 IP 范围**。创建要应用规则的录制操作的 IP 地址或 IP 地址范围列表。在**选择 IP 地址和 IP 范围**屏幕中，添加将为其启用或禁用录制的有效 IP 地址或 IP 范围。

注意：Session Recording 策略控制台支持在一条规则中配置多个条件。规则适用时，将使用 AND 和 OR 逻辑运算符来计算最终操作。一般而言，OR 运算符在某个条件内部的项目之间使用，AND 运算符在多个条件之间使用。如果结果为 true，Session Recording 策略引擎将执行规则的操作。否则，将转至下一条规则并重复该过程。

在一条录制策略中创建多条规则时，某些会话可能满足多条规则的条件。在这些情况下，具有最高优先级的规则会应用到这些会话。

规则的录制操作决定其优先级：

- **不录制**操作的规则优先级最高
- **录制并通知**操作的规则优先级次之
- **录制但不通知**操作的规则优先级最低

某些会话可能不满足录制策略中的任何规则条件。对于这些会话，将应用策略回退规则的录制操作。回退规则的录制操作始终为**不录制**。无法修改或删除回退规则。

要配置自定义策略，请执行以下操作：

1. 以授权策略管理员身份登录安装了 Session Recording 策略控制台的服务器。
2. 启动 Session Recording 策略控制台，然后选择左侧窗格中的**录制策略**从菜单栏中，依次选择**操作** > **添加新策略**。
3. 右键单击**新建策略**并选择**添加规则**。
4. 选择录制选项 - 在**规则**向导中，选择**禁用会话录制**、**启用会话录制并通知**（或**不通知**），然后单击**下一步**。
5. 选择规则条件 - 可以选择以下选项之一或其任意组合：
   用户或组
   已发布的资源
   交付组或计算机
   IP 地址或 IP 范围
6. 编辑规则条件 - 要进行编辑，请单击带下划线的值。这些值会根据上一步选择的条件加上下划线。
   注意：如果选择**已发布的资源**的带下划线的值，**站点地址**将为 IP 地址、URL 或计算机名称（如果 Controller 位于本地网络中）。**应用程序名称**列表显示显示名称。
7. 按照向导完成配置。

使用 Active Directory 组

Session Recording 允许您在创建策略时使用 Active Directory 组。使用 Active Directory 组代替单个用户可简化规则和策略的创建和管理。例如，如果公司财务部门中的用户包含在名为“Finance”的 Active Directory 组中，那么您可以通过在创建规则时在**规则**向导中选择“Finance”组来创建此组的所有成员要应用的规则。

将用户列入白名单

可以创建 Session Recording 策略，确保绝不会录制组织中某些用户的会话。这称为将这些用户*列入白名单*。对于负责处理隐私相关信息的用户或当您所在的组织不希望录制某些级别的员工会话时，列入白名单功能很有用。

例如，如果公司内的所有经理都属于名为“Executive”的 Active Directory 组中的成员，那么您可以创建规则来禁

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

用“Executive”组的会话录制，从而确保这些用户的会话绝不会被录制。包含此规则的策略处于活动状态时，不会录制“Executive”组成员的会话。组织内其他成员的会话根据活动策略中的其他规则进行录制。

使用 IP 地址或 IP 范围规则条件

可以使用客户端 IP 地址作为用于策略匹配的规则条件。例如，如果要从使用特定 IP 地址或在某个 IP 范围内的客户端录制会话，请使用**规则**向导来创建只应用于那些客户端的规则。

创建新策略

注意：使用**规则**向导时，如果未显示有下划线的值，系统可能会提示您“单击有下划线的值以编辑”。只有适用时才显示有下划线的值。如果未显示有下划线的值，请忽略此步骤。

1. 登录到安装了 Session Recording 策略控制台的服务器。
2. 启动 Session Recording 策略控制台。
3. 如果系统提示**连接到 Session Recording Server** 弹出窗口，请确保 Session Recording Server 名称、协议和端口正确无误。单击**确定**。
4. 在 Session Recording 策略控制台中，选择**录制策略**。
5. 从菜单中选择**添加新策略**。左侧窗格中将显示名为**新建策略**的策略。
6. 右键单击新策略，然后从菜单中选择**重命名**。
7. 键入要创建的策略名称，然后按 **Enter** 键或单击新名称外部的任意位置。
8. 右键单击策略，然后从菜单中选择**添加新规则**以启动**规则**向导。
9. 按照说明为此策略创建规则。

修改策略

1. 登录到安装了 Session Recording 策略控制台的服务器。
2. 启动 Session Recording 策略控制台。
3. 如果系统提示**连接到 Session Recording Server** 弹出窗口，请确保 Session Recording Server 名称、协议和端口正确无误。单击**确定**。
4. 在 Session Recording 策略控制台中，展开**录制策略**。
5. 选择要修改的策略。策略规则将显示在右侧窗格中。
6. 添加新规则、修改规则或删除规则：
   - 从菜单栏中，依次选择**操作** > **添加新规则**。如果策略处于活动状态，系统将显示一个弹出窗口，请求您确认该操作。请使用**规则**向导创建新规则。
   - 选择要修改的规则，单击鼠标右键，并选择**属性**。请使用**规则**向导修改规则。
   - 选择要删除的规则，单击鼠标右键，并选择**删除规则**。

删除策略

注意：无法删除系统策略或处于活动状态的策略。

1. 登录到安装了 Session Recording 策略控制台的服务器。
2. 启动 Session Recording 策略控制台。
3. 如果系统提示**连接到 Session Recording Server** 弹出窗口，请确保 Session Recording Server 名称、协议和端口正确无误。单击**确定**。
4. 在 Session Recording 策略控制台中，展开**录制策略**。
5. 在左侧窗格中，选择要删除的策略。如果该策略处于活动状态，必须激活其他策略。
6. 从菜单栏中，依次选择**操作** > **删除策略**。
7. 选择**是**确认该操作。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

注意：有关预启动应用程序会话的限制：

- 如果活动策略尝试匹配应用程序名称，则不会匹配在预启动会话中启动的应用程序，从而导致不录制会话。
- 如果活动策略录制每个应用程序，则当用户登录 Citrix Receiver for Windows（同时建立预启动会话）时，将显示录制通知，并且录制预启动的（空）会话以及将来在该会话中启动的所有应用程序。

解决方法：根据其录制策略，在单独的交付组中发布应用程序。请勿将应用程序名称用作录制条件。这样可确保能够录制预启动的会话。但是，仍显示通知。

了解滚动行为

激活策略之后，之前的活动策略仍然有效，直至用户的会话结束。但是，在某些情况下，新策略将在文件滚动时生效。文件达到最大大小时会发生滚动。有关最大录制文件大小的信息，请参阅指定录制件的文件大小。

下表详细说明了在录制会话并发生滚动的过程中应用新策略时会出现的情况：

如果之前的策略为：	新策略为：	滚动后策略将变为：
不录制	任何其他策略	不更改。仅当用户登录到新会话时新策略才生效。
录制但不通知	不录制	停止录制。
	录制并通知	继续录制并显示一条通知消息。
录制并通知	不录制	停止录制。
	录制但不通知	继续录制。下次用户登录时不显示任何消息。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

创建通知消息

Dec 05, 2017

如果活动录制策略指定录制用户的会话时应向用户发送通知，则系统会在用户键入其凭据后弹出一个窗口，显示通知消息。默认通知消息为“正在录制您在最近启动的一个或更多程序中执行的活动。如果您不同意此条件，请关闭相关应用程序。” 用户可以单击**确定** 消除该窗口并继续进行其会话。

默认通知消息会以托管 Session Recording Server 的计算机的操作系统使用的语言显示。

可以使用您选择的语言创建自定义通知，但一种语言只能创建一条通知消息。通知消息的显示语言与用户的首选本地设置的语言相同。

创建新通知消息

1. 登录到托管 Session Recording Server 的计算机。
2. 从**开始**菜单中选择 **Session Recording Server 属性**。
3. 在 **Session Recording Server 属性**中，单击**通知**选项卡。
4. 单击**添加**。
5. 选择消息使用的语言并键入新消息。一种语言只能创建一条消息。

接受并激活后，新消息将显示在特定于语言的通知消息框中。

注意：借助 Session Recording 的管理员日志记录功能，您可以记录 Session Recording 服务器策略更改。有关详细信息，请参阅日志管理活动。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

禁用或启用录制

Dec 05, 2017

在要录制会话的每个 VDA for Server OS 上安装 Session Recording Agent。可通过每个代理中的设置对安装了该代理的服务器启用录制。启用录制之后，Session Recording 会评估活动录制策略，从而确定要录制的会话。

安装 Session Recording Agent 时，将启用录制。Citrix 建议您禁用未录制的服务器上的 Session Recording，因为即使未进行录制，这些服务器的性能也会受到些许影响。

在服务器上禁用或启用录制

1. 登录到安装了 Session Recording Agent 的服务器。
2. 从**开始**菜单中选择 **Session Recording Agent Properties**。
3. 在**会话录制**下，选中或清除**对此服务器操作系统 VDA 启用会话录制**复选框，以指定是否录制此服务器的会话。
4. 系统提示时，重新启动 Session Recording Agent 服务以接受所做的更改。

注意： 安装 Session Recording 时，活动策略为**不录制**（任何服务器上都不会录制会话）。要开始录制，请使用 Session Recording 策略控制台激活其他策略。

启用自定义事件录制

Session Recording 允许您使用第三方应用程序将自定义数据（称为事件）插入到已录制的会话中。使用 Session Recording Player 查看会话时会显示这些事件。它们属于已录制会话文件的一部分，无法在录制会话之后对其进行修改。

例如，某个事件可能包含以下文本“用户打开了一个浏览器”。在录制会话过程中，每当用户打开浏览器时，都会在录制件中插入此文本。在使用 Session Recording Player 播放此会话时，查看器可以通过 Session Recording Player 中“事件和书签”列表所显示的标记数来定位和计算用户打开浏览器的次数。

将自定义事件插入到服务器上的录制件中：

- 使用 **Session Recording Agent Properties** 在要插入自定义事件的每台服务器上启用设置。必须分别启用每台服务器。不能全局启用站点中的所有服务器。
- 使用每个用户的 XenApp 会话中运行的事件 API 编写应用程序，以便将数据插入到录制件中。

Session Recording 安装包括一个事件录制 COM 应用程序 (API)，允许您将文本从第三方应用程序插入到录制件中。可以使用以多种编程语言（包括 Visual Basic、C++ 或 C# ）编写的 API。有关详细信息，请参阅 Citrix 文章 CTX226844。Session Recording Event API .dll 作为 Session Recording 安装的一部分进行安装。可以在 C:\Program Files\Citrix\SessionRecording\Agent\Bin\Interop.UserApi.dll 下找到该文件。

要在服务器上启用自定义事件记录，请执行以下操作：

1. 登录到安装了 Session Recording Agent 的服务器。
2. 从**开始**菜单中，选择 **Session Recording Agent Properties**。
3. 在 **Session Recording Agent Properties** 中，单击**录制**选项卡。
4. 在**自定义事件录制**下，选中 **Allow third party applications to record custom data on this server**（允许第三方应用程序在此服务器上录制数据）复选框。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

启用或禁用实时会话播放和播放保护

Dec 05, 2017

启用或禁用实时会话播放

使用 Session Recording Player 可以在录制会话之后或录制会话过程中对其进行查看。查看正在录制的会话与查看实时进行的操作类似；但是，从 XenApp 或 XenDesktop 服务器传送数据时实际存在 1 到 2 秒的延迟。

查看未完全录制的会话时某些功能不可用：

- 完成录制之后才能分配数字签名。如果数字签名处于启用状态，则可以查看实时播放会话，但未对这些会话进行数字签名，并且完成录制之后您才能查看证书。
- 完成录制之后才能应用播放保护。如果播放保护处于启用状态，则可以查看实时播放会话，但完成会话之后您才能对其进行加密。
- 完成录制之后才能缓存文件。

默认情况下，实时会话播放处于启用状态。

1. 登录到托管 Session Recording Server 的计算机。
2. 从**开始**菜单中选择 **Session Recording Server 属性**。
3. 在 **Session Recording Server 属性**中，单击**播放**选项卡。
4. 选中或清除**允许实时会话播放**复选框。

启用或禁用播放保护

为了安全起见，Session Recording 将在 Session Recording Player 中下载并查看录制的文件之前自动对文件进行加密。此播放保护可防止未下载录制文件的任何用户复制和查看这些文件。无法在其他工作站上播放录制的文件，也无法由其他用户播放。加密的文件通过 .icle 扩展名进行标识，未加密的文件通过 .icl 扩展名进行标识。录制的文件在安装了 Session Recording Player 的工作站上的缓存中始终处于加密状态，直至授权用户将其打开。

Citrix 建议使用 HTTPS 来保护数据传输。

默认情况下，播放保护处于启用状态。

1. 登录到托管 Session Recording Server 的计算机。
2. 从**开始**菜单中，选择 **Session Recording Server 属性**。
3. 在 **Session Recording Server 属性**中，单击**播放**选项卡。
4. 选中或清除**加密下载供播放的会话录制文件**复选框。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

启用和禁用数字签名

Dec 05, 2017

如果您在安装了 Session Recording 组件的计算机上安装证书，则可以通过向会话录制分配数字签名来增强 Session Recording 部署的安全性。

默认情况下，数字签名处于禁用状态。在您选择了用于对录制件进行签名的证书后，Session Recording 会为 Session Recording Storage Manger 服务授予写入权限。

启用数字签名

1. 登录到托管 Session Recording Server 的计算机。
2. 从**开始**菜单中选择 **Session Recording Server 属性**。
3. 在 **Session Recording Server 属性**中，单击**签名**选项卡。
4. 浏览至可以在安装了 Session Recording 组件的计算机之间实现安全通信的证书。

禁用数字签名

1. 登录到托管 Session Recording Server 的计算机。
2. 从**开始**菜单中选择 **Session Recording Server 属性**。
3. 在 **Session Recording Server 属性**中，单击**签名**选项卡。
4. 单击**清除**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

指定录制件的存储位置

Dec 05, 2017

使用“Session Recording Server 属性”可指定录制件的存储位置以及存档录制件的还原位置以便进行播放。

注意：要存档文件或还原删除的文件，请使用 ICLDB 命令。有关详细信息，请参阅如何存档和还原录制件。

指定用于存储录制件的目录

默认情况下，录制件存储在托管 Session Recording Server 的计算机的 drive:**\SessionRecordings** 目录中。可以更改录制件的存储目录，添加其他目录以平衡多个卷之间的负载，或者利用其他空间。列表中有多个目录表明录制件在多个目录之间处于负载平衡状态。可以多次添加一个目录。负载平衡在这些目录之间进行循环。

1. 登录到托管 Session Recording Server 的计算机。
2. 从**开始**菜单中选择 **Session Recording Server 属性**。
3. 在 **Session Recording Server 属性**中，单击**存储**选项卡。
4. 使用**文件存储目录**列表来管理录制件的存储目录。

选择目录后，Session Recording 会为其服务授予对这些目录的完全控制权限。

可在本地驱动器上、SAN 卷上或 UNC 网络路径指定的位置处创建文件存储目录。网络映射的驱动器盘符不受支持。由于存在与向网络驱动器写入录制数据有关的严重性能和安全问题，因此，请勿将 Session Recording 与网络连接存储 (NAS) 一起使用。

指定用于还原存档的录制件的目录以便进行播放

默认情况下，存档的录制件在托管 Session Recording Server 的计算机的 drive:**\SessionRecordingsRestore** 目录中还原。可以更改该目录。

1. 登录到托管 Session Recording Server 的计算机。
2. 从**开始**菜单中选择 **Session Recording Server 属性**。
3. 在 **Session Recording Server 属性**中，单击**存储**选项卡。
4. 在**存档文件的还原目录**字段中，键入用于还原存档的录制件的目录。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

指定录制件的文件大小

Dec 05, 2017

录制件大小越大，下载文件所需的时间越长，且在播放过程中使用搜寻滑块进行导航时文件的反应速度越慢。要控制文件的大小，请为文件指定阈值限制。录制达到此限制之后，Session Recording 会关闭该文件并打开一个新文件以继续进行录制。此操作称为滚动。

重要：滚动设置不适用于 XenDesktop 7.8 和 Session Recording Agent 的 VDI 桌面会话。在这些情况下，每个录制文件的最大大小为 1 GB，达到此限制后，就不会再录制活动。

可以为一个滚动指定两个阈值：

- **文件大小。**文件达到指定的兆字节数之后，Session Recording 会关闭该文件并打开一个新文件。默认情况下，文件在达到 50 MB 之后会发生滚动；但您可以将限制指定为 10 MB 至 1 GB 之间。
- **持续时间。**会话录制达到指定的小时数之后，会关闭该文件并打开一个新文件。默认情况下，录制达到 12 小时之后文件会进行滚动；但您可以将限制指定为 1 至 24 小时之间。

Session Recording 会检查这两个字段，确定先发生哪个事件，从而决定滚动时间。例如，如果指定文件大小为 17 MB 且持续时间为 6 小时，而录制件在 3 小时内达到 17 MB，Session Recording 就会对 17 MB 的文件大小作出反应，关闭该文件并打开一个新文件。

为防止创建许多小文件，Session Recording 会在至少一小时之后才进行滚动（这一时间是您可以输入的最小值），而不考虑文件大小的指定值。文件大小超过 1 GB 属此规则的例外情况。

指定录制件的最大文件大小

1. 登录到托管 Session Recording Server 的计算机。
2. 从**开始**菜单中选择 **Session Recording Server 属性**。
3. 在 **Session Recording Server 属性**中，单击**滚动**选项卡。
4. 输入一个 10 至 1,024 之间的整数，以指定文件的最大大小（以 MB 为单位）。
5. 输入一个 1 至 24 之间的整数，以指定录制的最大持续时间（以小时为单位）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

日志管理活动

Dec 05, 2017

Session Recording 管理员日志记录可记录以下活动：

- 在 Session Recording 策略控制台或 Citrix Director 中对录制策略所做的更改。
- Session Recording Server 属性的变更。
- Session Recording Player 中录制件的下载情况。
- 在策略查询之后由 Session Recording 录制会话。
- 在未经授权情况下试图访问管理员日志记录服务。

> **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。

禁用或启用管理员日志记录

安装之后，您可以在 Session Recording Server 属性中禁用或启用 Session Recording 管理员日志记录功能。

1. 以管理员身份登录到安装了 Session Recording 管理员日志记录的服务器。
2. 从**开始**菜单中选择 **Session Recording Server 属性**。
3. 单击**日志记录**选项卡。

禁用 Session Recording 管理员日志记录后，不会记录任何新的活动。您可以通过基于 Web 的 UI 查询现有的日志。

启用了**强制阻止**后，会在日志记录失败时阻止以下活动。也会记录具有事件 ID 6001 的系统事件：

- 在 Session Recording 策略控制台或 Citrix Director 中对录制策略所做的更改。
- Session Recording Server 属性的变更。

强制阻止设置不会影响会话的录制。

授予用户访问权限

出于安全原因，请只授予用户执行特定功能（例如查询管理员日志记录的日志）所需的权限。

可以通过使用 Session Recording Server 上的 Session Recording Authorization 控制台为用户分配角色来授予其访问权限。管理员日志记录有两个角色：

- **LoggingWriter**。授予写入管理员日志记录日志的权限。默认情况下，本地管理员和网络服务是此角色的成员。

  注意：修改默认的 **LoggingWriter** 成员关系可能会导致日志写入失败。

- **LoggingReader**。授予查询管理员日志记录日志的权限。此角色中没有默认成员身份。

向用户分配角色

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. 以管理员身份登录托管 Session Recording Server 的计算机。
2. 启动 **Session Recording Authorization 控制台**。
3. 选择要分配给用户的角色。
4. 从菜单栏中，依次选择**操作** > **Assign Windows Users and Groups**（分配 Windows 用户和组）。
5. 添加用户和组。

对控制台所做的任何更改都将于每分钟执行一次的更新期间生效。

配置管理员日志记录服务帐户

默认情况下，管理员日志记录作为 Web 应用程序在 Internet Information Services (IIS) 中运行，其身份为网络服务。要提高安全级别，您可以将此 Web 应用程序的身份更改为服务帐户或特定的域帐户。

1. 以管理员身份登录托管 Session Recording Server 的计算机。
2. 在 IIS 管理器中，单击**应用程序池。**
3. 在**应用程序池**中，右键单击 **SessionRecordingLoggingAppPool**，然后选择**高级设置**。
4. 将**身份**属性更改为您希望使用的特定帐户。
5. 向 Microsoft SQL Server 中 **CitrixSessionRecordingLogging** 数据库的帐户授予 **db_owner** 权限。
6. 针对位于 **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server** 的注册表项为帐户授予读权限。

禁用或启用录制操作日志记录

默认情况下，管理员日志记录会记录策略查询完成后的每个录制操作。这可能会生成大量的日志记录。要改进性能和保存存储，请在注册表中禁用这种日志记录。

1. 以管理员身份登录托管 Session Recording Server 的计算机。
2. 打开“注册表编辑器”。
3. 浏览至 **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server**。
4. 将 **EnableRecordingActionLogging** 的值设置为：

   0 禁用录制操作日志记录

   1 启用录制操作日志记录

查询管理员日志记录数据

Session Recording 可提供基于 Web 的 UI 来查询所有管理员日志记录。

在托管 Session Recording Server 的计算机上执行以下操作：

1. 从**开始**菜单选择 **Session Recording 管理员日志记录**。
2. 输入 **LoggingReader** 用户的凭据。

在其他计算机上：

1. 打开 Web 浏览器并访问管理员日志记录的 Web 页面。

   对于 HTTPS： https://*servername*/SessionRecordingLoggingWebApplication/，其中 *servername* 为托管 Session Recording Server 的计算机的名称。

   对于 HTTP： http://*servername*/SessionRecordingLoggingWebApplication/，其中 *servername* 为托管 Session Recording

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Server 的计算机的名称。

2. 输入 **LoggingReader** 用户的凭据。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

安装具有数据库高可用性的 Session Recording

Dec 05, 2017

Session Recording 支持以下基于 Microsoft SQL Server 的数据库高可用性解决方案。主体或主 SQL Server 出现故障时，数据库可以自动故障转移，这样可确保 Session Recording 能够继续按预期运行。

- AlwaysOn 可用性组

  AlwaysOn 可用性组功能是提供数据库镜像的企业级替换方案的高可用性和灾难恢复解决方案。AlwaysOn 可用性组在 SQL Server 2012 中引入，最大限度地为企业提升了一组用户数据库的可用性。AlwaysOn 可用性组要求 SQL Server 实例必须驻留在 Windows Server 故障转移群集 (WSFC) 节点上。有关详细信息，请参阅 http://msdn.microsoft.com/en-us/library/hh510230。

- SQL Server 群集化

  Microsoft SQL 群集化技术允许一台服务器自动接管另一台故障服务器的任务和职责。但是，此解决方案的设置非常复杂，并且自动故障转移过程通常比其他备选方案（例如 SQL Server 数据库镜像）更慢。有关详细信息，请参阅 https://msdn.microsoft.com/en-us/library/ms189134.aspx。

- SQL Server 数据库镜像

  数据库镜像可确保在活动数据库服务器出现故障时在几秒钟内进行自动故障转移。与其他两种解决方案相比，此解决方案更加昂贵，因为需要在每个数据库服务器上安装完全权限 SQL Server 许可证。不能在镜像环境中使用 SQL Server Express Edition。有关详细信息，请参阅 https://msdn.microsoft.com/en-us/library/ms189852.aspx。

用于安装具有数据库高可用性的 Session Recording 的方法

要安装具有数据库高可用性的 Session Recording，请执行以下操作之一：

- 请先安装 Session Recording Server 组件，然后再为所创建的数据库配置数据库高可用性。
  可以在将数据库配置为安装在预先配置的 SQL Server 实例上的情况下安装 Session Recording Administration 组件，然后为所创建的数据库配置数据库高可用性。
  - 对于 AlwaysOn 高可用性组和群集化解决方案，必须在 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\SmAudDatabaseInstance 中将 SQL Server 实例名称手动更改为高可用性侦听器或 SQL Server 网络的名称。
  - 对于数据库镜像，必须在 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\DatabaseFailoverPartner 和 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\LoggingDatabaseFailoverPartner 中手动添加数据库的故障转移合作伙伴。
- 先为空数据库配置数据库高可用性，然后再安装 Session Recording Administration 组件。
  可以在预期的主 SQL Server 实例中创建两个空数据库作为 Session Recording 数据库和管理员日志记录数据库并配置高可用性。然后在安装 Session Recording Server 组件时输入 SQL Server 实例名称：
  - 要使用 AlwaysOn 可用性组解决方案，请输入可用性组侦听器的名称
  - 要使用数据库群集化解决方案，请输入主体 SQL Server 的名称
  - 要使用群集化解决方案，请输入您的 SQL Server 的网络名称

© 1999-2017 Citrix Systems, Inc. All rights reserved.

查看录制

Dec 05, 2017

使用 Session Recording Player 查看和搜索录制的 XenApp 或 XenDesktop 会话，并为这些会话添加书签。

如果录制会话时启用了实时播放功能，则可以查看正在进行的会话（有数秒延迟），也可查看已完成的会话。

如果会话的持续时间较长或文件大小较大，超出 Session Recording 管理员配置的限制，则会显示在多个会话文件中。

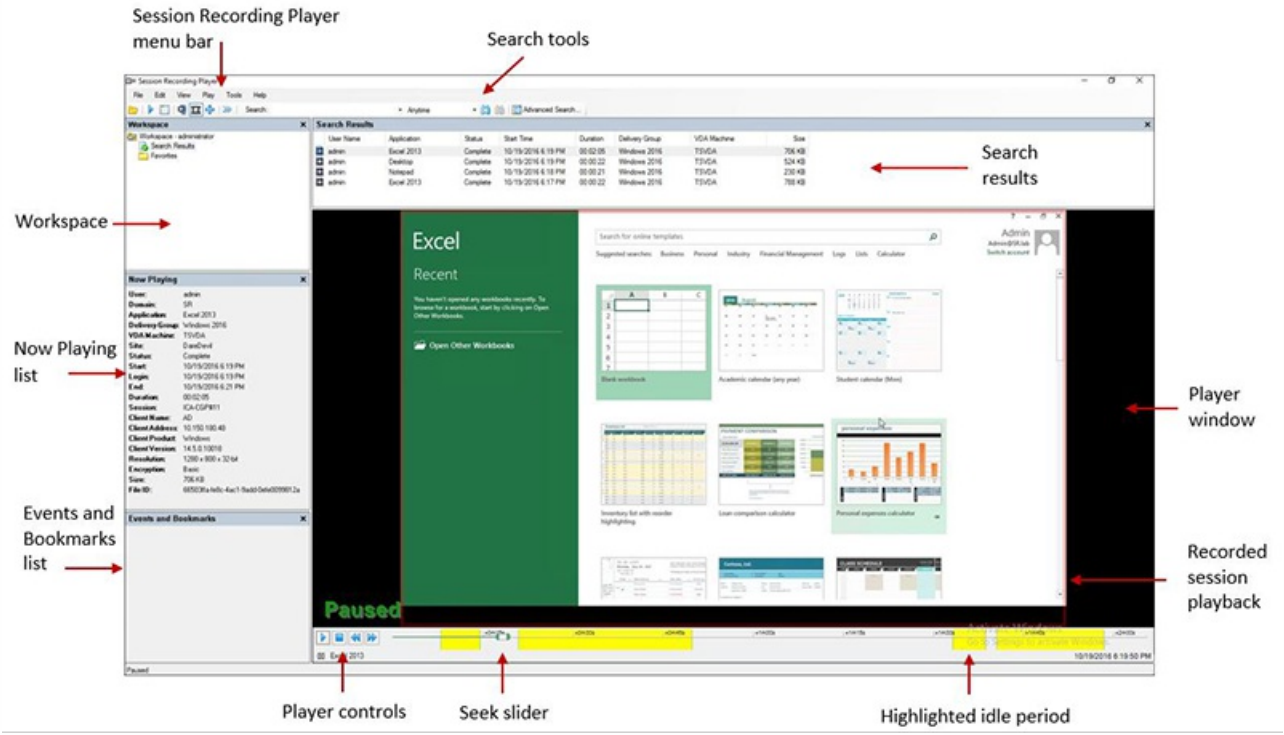
注意：Session Recording 管理员必须授予用户访问录制的 VDA for Server OS 会话的权限。如果您被拒绝访问查看会话，请与 Session Recording 管理员联系。

安装 Session Recording Player 时，Session Recording 管理员通常会设置 Session Recording Player 与 Session Recording Server 之间的连接。如果未设置此连接，首次执行文件搜索时，系统会提示您进行设置。有关设置信息，请与您的 Session Recording 管理员联系。

启动 Session Recording Player

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始** 菜单中选择 **Session Recording Player**。
   将显示 Session Recording Player。

下图显示的 Session Recording Player 用插图编号指出了其主要元素。以下整篇文章都介绍了这些元素的功能。



显示或隐藏窗口元素

Session Recording Player 包含将打开和关闭的窗口元素。

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始** 菜单中选择 **Session Recording Player**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. 从 **Session Recording Player** 菜单栏中，选择**查看**。
4. 选择要显示的元素。选择某元素之后，该元素会立即显示。复选标记指示该元素处于选中状态。

更改 Session Recording Server

如果 Session Recording 管理员为您的 Session Recording Player 设置了可连接多个 Session Recording Server 的功能，则可以选择 Session Recording Player 连接到的 Session Recording Server。Session Recording Player 一次只能连接到一个 Session Recording Server。

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始** 菜单中选择 **Session Recording Player**。
3. 从 **Session Recording Player** 菜单栏中，依次选择**工具** > **选项** > **连接** 。
4. 选择要连接的 Session Recording Server。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

打开和播放录制件

Dec 05, 2017

可以用三种方式打开 Session Recording Player 中的会话录制：

- 使用 Session Recording Player 执行搜索。满足搜索条件的录制的会话将显示在搜索结果区域中。
- 直接从本地磁盘驱动器或共享驱动器访问录制的会话文件。
- 从“收藏夹”文件夹访问录制的会话文件。

打开未使用数字签名录制的文件时，系统会显示一条警告消息，指出未验证该文件的来源和完整性。如果您确信该文件的完整性，请在警告弹出窗口中单击**是** 以打开该文件。

注意：借助 Session Recording 的管理员日志记录功能，您可以记录 Session Recording Player 中的录制的下载情况。有关详细信息，请参阅日志管理活动。

打开和播放搜索结果区域中的录制件

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始**菜单中选择 **Session Recording Player**。
3. 执行搜索。
4. 如果未显示搜索结果区域，请在“工作区”窗格中选择**搜索结果**。
5. 在搜索结果区域中，选择要播放的会话。
6. 执行以下任何操作：
   - 双击会话
   - 单击鼠标右键并选择**播放**
   - 从 **Session Recording Player** 菜单栏中，选择**播放** > **播放速度**

通过访问文件打开和播放录制件

录制的会话文件的名称以“i_”开头，依次后跟唯一的字母数字文件 ID 和 .icl 或 .icle 文件扩展名。.icl 扩展名表示录制件未应用播放保护；.icle 扩展名表示录制件应用了播放保护。录制的会话文件保存在一个包含会话的录制日期的文件夹中。例如，在 2014 年 12 月 22 日录制的会话文件，保存在文件夹路径 2014\12\22 下。

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始**菜单中选择 **Session Recording Player**。
3. 执行以下任何操作：
   - 在 **Session Recording Player** 菜单栏中，依次选择**文件** > **打开**，并浏览文件
   - 使用 Windows 资源管理器，导航至文件，并将文件拖动到**播放器**窗口中
   - 使用 Windows 资源管理器，导航至文件，并双击该文件
   - 如果在“工作区”窗格中创建了“收藏夹”，请选择**收藏夹** ，并通过与在搜索结果区域中打开文件相同的方法从“收藏夹”区域打开该文件

使用收藏夹

通过创建“收藏夹”文件夹，您可以快速访问经常查看的录制件。这些“收藏夹”文件夹引用存储在工作站或网络驱动器上的录制的会话文件。可以将这些文件导入及导出到其他工作站，并且可以与其他 Session Recording Player 用户共享这些文件夹。

注意：只有对 Session Recording Player 具有访问权限的用户才能下载与“收藏夹”文件夹相关联的录制的会话文件。请与您的 Session Recording 管理员联系获取访问权限。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

创建“收藏夹”子文件夹：

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始**菜单中选择 **Session Recording Player**。
3. 在 **Session Recording Player** 中，选择“工作区”窗格中的**收藏夹**文件夹。
4. 从菜单栏中，依次选择**文件** > **文件夹** > **新建文件夹**。**收藏夹**文件夹下将显示一个新文件夹。
5. 键入文件夹名称，然后按 **Enter** 或单击任意位置以接受新名称。

使用**文件** > **文件夹**菜单中显示的其他选项可删除、重命名、移动、复制、导入和导出文件夹。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

搜索录制的会话

Dec 05, 2017

Session Recording Player 允许您执行快速搜索、执行高级搜索，以及指定应用到所有搜索的选项。搜索结果显示在 Session Recording Player 的搜索结果区域。

注意：要显示所有可用的录制会话（搜索中可以显示的最大会话数），在执行搜索时请不要指定任何搜索参数。

执行快速搜索

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始**菜单中选择 **Session Recording Player**。
3. 定义搜索条件：
   - 在**搜索** 字段中输入搜索条件。有助于您实现以下操作：
   - 将鼠标指针移动到**搜索** 标签上以显示要用作指导的参数列表
   - 单击**搜索**字段右侧的箭头以显示最近执行的 64 次搜索的文本
   - 使用**搜索** 字段右侧的下拉列表以选择用于指定会话录制时间的时段或持续时间。
4. 单击下拉列表右侧的望远镜图标以启动搜索。

执行高级搜索

提示：高级搜索可能最多需要 20 秒即可返回包含 150,000 个以上条目的结果。Citrix 建议使用更精确的搜索条件（例如日期范围或用户）以减少结果数量。

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始**菜单中选择 **Session Recording Player**。
3. 在 **Session Recording Player** 窗口中，单击工具栏上的**高级搜索**，或者依次选择**工具** > **高级搜索**。
4. 在**高级搜索**对话框的选项卡中定义搜索条件：
   - **通用** 允许您按域或帐户授权、站点、组、VDA for Server OS、应用程序或文件 ID 进行搜索。
   - **日期/时间**允许您搜索日期、星期几和一天中的时间。
   - **事件**允许您搜索 Session Recording 管理员插入到会话中的自定义事件。
   - **其他** 允许您按会话名称、客户端名称、客户端地址以及录制持续时间进行搜索。它还允许您为此搜索指定搜索结果的最大显示数目以及搜索中是否包含存档文件。

   指定搜索条件时，您正在创建的查询将显示在对话框底部的窗格中。
5. 单击**搜索**以开始搜索。

提示：可以保存和检索高级搜索查询。在**高级搜索** 对话框中单击**保存** 可保存当前的查询。在**高级搜索**对话框中单击**打开** 可检索已保存的查询。查询另存为扩展名为 .isq 的文件。

设置搜索选项

Session Recording Player 搜索选项允许您限制搜索结果中显示的最大会话录制件数，以及指定搜索结果中是否包含存档会话文件。

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始**菜单中选择 **Session Recording Player**。
3. 在 **Session Recording Player** 菜单栏中，依次选择**工具** > **选项** > **搜索**。
4. 在**要显示的最大结果数量**字段中，键入要显示的搜索结果数量。最多可显示 500 条结果。
5. 要设置搜索中是否包含存档文件，请选择或清除**包括存档文件**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

播放录制的会话

Dec 05, 2017

在 Session Recording Player 中打开录制的会话之后，可以使用以下方法浏览录制的会话：

- 使用播放器控件播放、停止、暂停以及提高或降低播放速度
- 使用搜寻滑块快进或快退

如果您在录制件中插入了标记，或者录制的会话中包含自定义事件，也可以通过转到这些标记和事件来浏览录制的会话。

注意：

- 在播放录制的会话期间，可能会显示第二个鼠标指针。如果用户在 Internet Explorer 中浏览时单击了一个图像，而该图像的原始大小比屏幕大，但自动被 Internet Explorer 缩小，则会在录制件中显示第二个指针。虽然会话期间仅显示一个指针，但播放过程中可能会显示两个。
- 此 Session Recording 版本不支持适用于 XenApp 的 SpeedScreen Multimedia Acceleration，或适用于 XenApp 的 Flash 品质调节策略设置。如果启用了此选项，播放将显示一个黑色方块。
- 使用 HDX RealTime Optimization Pack 时，Session Recording 无法录制 Lync 网络摄像机视频。
- 使用高于或等于 4096 x 4096 的分辨率录制会话时，录制件中可能会出现片段。
- 如果 XenDesktop 站点策略启用了**旧图形模式**，并且 Citrix Receiver for Windows 策略启用了**基于磁盘的缓存**，则无法正确录制 Windows 7 桌面会话。这些录制件将显示黑屏。
  解决方法：通过安装了 Citrix Receiver for Windows 的计算机上的 GPO 禁用**基于磁盘的缓存**。有关禁用**基于磁盘的缓存**的详细信息，请参阅 CTX123169 和使用组策略对象管理模板进行配置。
- Session Recording 不支持 Framehawk 显示模式。不能正确录制和播放 Framehawk 显示模式的会话。在 Framehawk 显示模式下录制的会话可能不包含会话的活动。

使用播放器 控件

可以单击播放器窗口下方的播放器控件，也可以从 **Session Recording Player** 菜单栏中选择**播放**来访问这些控件。使用播放器控件可以实现以下操作：

	播放所选会话文件。
	暂停播放。
	停止播放。如果单击**停止**，然后单击**播放**，记录将从文件开头重新开始播放。
	将当前播放速度减半，最多可减至正常速度的四分之一。
	将当前播放速度加倍，最多可增加到正常播放速度的 32 倍。

使用搜寻 滑块

使用播放器窗口下方的定位滑块可跳至录制的会话中的不同位置。可以将搜寻滑块拖动到录制件中要查看的点，也可以单击滚动条的任意位置以移动到该位置。

还可以使用以下键盘快捷键来控制搜寻滑块：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

键：	搜寻操作：
住宅	搜寻到开头。
结束时间	搜寻到结尾。
右箭头键	向前搜寻 5 秒。
左箭头键	向后搜寻 5 秒。
将鼠标滚轮向下滚动一格	向前搜寻 15 秒。
将鼠标滚轮向上滚动一格	向后搜寻 15 秒。
Ctrl + 右箭头键	向前搜寻 30 秒。
Ctrl + 左箭头键	向后搜寻 30 秒。
PgDn	向前搜寻 1 分钟。
PgUp	向后搜寻 1 分钟。
Ctrl + 将鼠标滚轮向下滚动一格	向前搜寻 90 秒。
Ctrl + 将鼠标滚轮向上滚动一格	向后搜寻 90 秒。
Ctrl + Page Down	向前搜寻 6 分钟。
Ctrl + Page Up	向后搜寻 6 分钟。

注意：调整搜寻滑块的速度：从 **Session Recording Player** 菜单栏中，依次选择**工具** > **选项** > **播放器**，并拖动滑块以增加或减少搜寻响应时间。响应时间越快，所需内存越多。响应速度可能会很慢，具体取决于录制内容的大小和计算机的硬件。

更改播放速度

您可以对 Session Recording Player 进行设置，使其能够以正常播放速度的 1/4 到 32 倍逐渐增加的顺序来播放录制的会话。

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始**菜单中选择 **Session Recording Player**。
3. 从 **Session Recording Player** 菜单栏中，选择**播放** > **播放速度**。
4. 选择一个速度选项。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

速度会立即调整。在播放器窗口控件的下方将显示一个数字，指示增加或减少的速度。指示指数率的文本在播放器窗口中会暂时显示为绿色。

突出显示录制的会话的空闲时间段

录制的会话的空闲期间是其中没有执行任何操作的部分。Session Recording Player 可以在播放时突出显示录制的会话的空闲期间。选项默认为**开**。

请注意，使用 Session Recording Player 播放实时会话时不会突出显示空闲期间。

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始**菜单中选择 **Session Recording Player**。
3. 从 **Session Recording Player** 菜单栏中，选择**查看** > **空闲期间**并选中或取消选中选项框。

跳过没有操作的空白部分

在快速查看模式下，可以将 Session Recording Player 设置为跳过录制的会话中没有发生操作的部分。此设置可节省观看播放的时间；但是，它不会跳过连续动画，例如连续移动的鼠标指针、闪烁的光标或显示的包含秒针移动的时钟。

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始**菜单中选择 **Session Recording Player**。
3. 从 **Session Recording Player** 菜单栏中，依次选择**播放** > **快速查看模式**。

该选项将打开或关闭。每次选择该选项时，其状态在播放器窗口中会暂时显示为绿色。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

使用事件和书签

Dec 05, 2017

可以使用事件和书签帮助浏览录制的会话。

可以使用事件 API 和第三方应用程序在会话录制过程中将事件插入到会话中。事件作为会话文件的一部分进行保存。无法使用 Session Recording Player 删除或修改事件。

书签是使用 Session Recording Player 插入到录制的会话中的标记。删除之前，书签会一直与该录制的会话相关联，但它们不作为会话文件的一部分进行保存。默认情况下，每个书签都标有文本**书签**，但您可以将其更改为最多包含 128 个字符的任何文本附注。

事件和书签在播放器窗口的下面部分显示为圆点。事件显示为黄色圆点，书签显示为蓝色圆点。将鼠标移动到这些圆点上可显示与其相关联的文本标签。还可以在 Session Recording Player 的**事件和书签**列表中显示事件和书签。在此列表中，事件和书签与其文本标签及其在录制的会话中显示的次数一起显示（按时间顺序显示）。

可以使用事件和书签帮助浏览录制的会话。通过转到事件或书签，可以跳至录制的会话中事件或书签的插入点。

显示列表中的事件和书签

事件和书签列表显示当前正在播放的录制会话中插入的事件和书签。可以只显示事件、只显示书签，也可以同时显示二者。

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始**菜单中选择 **Session Recording Player**。
3. 将鼠标指针移到**事件和书签**列表区域，然后单击鼠标右键以显示菜单。
4. 选择**只显示事件**、**只显示书签**或**全部显示**。

插入书签

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始**菜单中选择 **Session Recording Player**。
3. 开始播放要添加书签的录制会话。
4. 将搜寻滑块移动到要插入书签的位置。
5. 将鼠标指针移动到播放器窗口区域，然后单击鼠标右键以显示菜单。
6. 使用默认**书签**标签添加书签，或创建附注：
   - 要使用默认**书签**标签添加书签，请选择**添加书签**。
   - 要使用您创建的描述性文本标签添加书签，请选择**添加附注**。键入要指定给该书签的文本标签（最多包含 128 个字符）。单击**确定**。

添加或更改附注

创建书签后，可以向其添加附注或更改其附注。

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始**菜单中选择 **Session Recording Player**。
3. 开始播放包含书签的录制会话。
4. 确保事件和书签列表可显示书签。
5. 选择**事件和书签**列表中的书签，然后单击鼠标右键以显示菜单。
6. 选择**编辑附注**。
7. 在显示的窗口中，键入新附注，然后单击**确定**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

删除书签

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始**菜单中选择 **Session Recording Player**。
3. 开始播放包含书签的录制会话。
4. 确保事件和书签列表可显示书签。
5. 选择事件和书签列表中的书签，然后单击鼠标右键以显示菜单。
6. 选择**删除**。

转到事件或书签

转到事件或书签会导致 Session Recording Player 转到录制的会话中事件或书签的插入点。

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始**菜单中选择 **Session Recording Player**。
3. 开始播放包含事件或书签的会话录制件。
4. 转到事件或书签：
   - 在播放器窗口的下面部分中，单击表示事件或书签的圆点以转到事件或书签。
   - 在**事件和书签**列表中，双击要转到的事件或书签。要转到下一个事件或书签，请选择列表中的任何事件或书签，单击鼠标右键以显示菜单，然后选择**搜寻至书签**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

更改播放显示

Dec 05, 2017

通过“选项”，您可以更改录制的会话在播放器窗口中的显示方式。可以平移和缩放图像、全屏显示播放、在单独的窗口中显示播放器窗口，以及在录制的会话周围显示红色边框以与播放器窗口背景进行区分。

全屏显示播放器窗口

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始**菜单中选择 **Session Recording Player**。
3. 从 **Session Recording Player** 菜单栏中，依次选择**查看** > **全屏播放**。
4. 要返回原始大小，请按 Esc 或 F11。

在单独的窗口中显示播放器窗口

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始**菜单中选择 **Session Recording Player**。
3. 从 **Session Recording Player** 菜单栏中，依次选择**查看** > **播放器在单独窗口中**。将显示一个包含播放器窗口的新窗口。您可以拖动该窗口以及调整其大小。
4. 要将播放器窗口嵌入到主窗口中，请依次选择**查看** > **播放器在单独窗口中**，或按 **F10**。

缩放会话播放使其适应播放器窗口

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始**菜单中选择 **Session Recording Player**。
3. 从 **Session Recording Player** 菜单栏中，依次选择**播放** > **平移和缩放** > **缩放以适应窗口**。
   - **缩放以适应窗口(快速呈现)** 在提供良好质量的同时会缩小图像。与使用“高质量”选项相比，图像的绘制速度更快，但图像和文本不清晰。如果在使用“高质量”模式时遇到性能问题，请使用此选项。
   - **缩放以适应窗口(高质量)** 在提供高质量的同时会缩小图像。使用此选项可能会导致图像的绘制速度比使用“快速呈现”选项慢。

平移图像

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始**菜单中选择 **Session Recording Player**。
3. 从 **Session Recording Player** 菜单栏中，依次选择**播放** > **平移和缩放** > **平移**。指针变为手形，并且播放器窗口的右上角会显示屏幕的小图示。
4. 拖动图像。小图示指示您在图像中的位置。
5. 要停止平移，请选择其中一个缩放选项。

在 Session Recording 周围显示红色边框

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始**菜单中选择 **Session Recording Player**。
3. 从 **Session Recording Player** 菜单栏中，依次选择**工具** > **选项** > **播放器**。
4. 选中**显示会话录制件周围的边框**复选框。

   提示： 如果未选中**显示会话录制件周围的边框** 复选框，可以将鼠标指针放在播放器窗口中，单击并按住鼠标左键以临时显示红色边框。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

缓存录制的会话文件

Dec 05, 2017

每次打开录制的会话文件时，Session Recording Player 都会从录制件的存储位置下载该文件。如果您经常下载相同的文件，则可以通过在工作站上缓存文件来节省下载所需的时间。缓存的文件存储在工作站上的以下文件夹中：

userprofile**AppData\Local\Citrix\SessionRecording\Player\Cache**

您可以指定用于缓存的磁盘空间量。录制件填满指定的磁盘空间之后，Session Recording 会删除最旧、使用次数最少的录制件，从而为新录制件释放空间。可以随时清空缓存来释放磁盘空间。

启用缓存

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始**菜单中选择 **Session Recording Player**。
3. 从 **Session Recording Player** 菜单栏中，依次选择**工具** > **选项** > **缓存**。
4. 选中**将下载的文件缓存在本地计算机**复选框。
5. 如果要限制用于缓存的磁盘空间量，请选择**限制要使用的磁盘空间量**复选框，并指定要用于缓存的兆字节数。
6. 单击**确定**。

清空缓存

1. 登录到安装了 Session Recording Player 的工作站。
2. 从**开始**菜单中选择 **Session Recording Player**。
3. 从 **Session Recording Player** 菜单栏中，依次选择**工具** > **选项** > **缓存**。
4. 选中**将下载的文件缓存在本地计算机**复选框。
5. 在 Session Recording Player 中，依次选择**工具** > **选项** > **缓存**。
6. 单击**清除缓存**，然后单击**确定**以确认操作。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Session Recording 故障排除

Dec 05, 2017

此故障排除信息可以为在安装 Session Recording 组件期间或之后可能遇到的一些问题提供解决方案：

- 组件无法相互连接
- 无法录制会话
- Session Recording Player 或 Session Recording 策略控制台的问题
- 与通信协议有关的问题

> **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。

Session Recording Agent 无法连接时，将记录 **Exception caught while sending poll messages to Session Recording Broker**（向 Session Recording Broker 发送轮询消息时捕获到异常）事件消息，后跟异常文本。此异常文本提供连接失败的原因。这些原因包括：

- **基础连接已关闭。无法为 SSL/TLS 安全通道建立信任关系。**此异常表示 Session Recording Server 使用的是 Session Recording Agent 所在的服务器不信任或没有 CA 证书的 CA 签发的证书。或者，证书可能已过期或已被吊销。

  解决方案：验证托管 Session Recording Agent 的服务器上是否安装了正确的 CA 证书，或者使用可信 CA。

- **远程服务器返回错误: (403) 已禁止。** 此为尝试使用 HTTP（非安全协议）进行连接时出现的标准 HTTPS 错误。托管 Session Recording Server 的计算机拒绝连接，因为该计算机仅接受安全连接。

  解决方案：使用 Session Recording Agent Properties 将 Session Recording Broker 协议更改为 **HTTPS**。

Session Recording Broker 在评估录制策略查询时返回未知错误。错误代码 5（访问被拒绝）。有关详细信息，请参阅 Session Recording Server 上的事件日志。启动会话并申请进行录制策略评估时会发生此错误。导致此错误的原因为：从 Session Recording Authorization 控制台的策略查询角色中删除了已通过身份验证的用户组（此为默认成员）。

解决方案：将已通过身份验证的用户组添加回此角色，或将托管每个 Session Recording Agent 的每个服务器添加到策略查询角色中。

基础连接已关闭。服务器关闭了本应保持活动状态的连接。此错误表示 Session Recording Server 已关闭或无法接受请求。这可能是因为 IIS 处于脱机状态或重新启动，或者整个服务器可能处于脱机状态。

解决方案：验证 Session Recording Server 是否已启动、IIS 是否正在该服务器上运行，以及该服务器是否已连接到网络。

安装 Session Recording Server 组件失败，并显示错误代码 2503 和 2502。
解决方案：
查看文件夹 C:\windows\Temp 的访问控制列表 (ACL)，以确保“本地用户和组”对此文件夹具有写入权限。否则，请手动添加写

© 1999-2017 Citrix Systems, Inc. All rights reserved.

入权限。

当 Session Recording Server 无法连接到 Session Recording 数据库时，可能会显示类似以下内容的错误消息之一：

事件来源：

与 SQL Server 建立连接时发生与网络相关的或实例特有的错误。此错误会显示在托管 Session Recording Server 的计算机上事件查看器中的应用程序事件日志中，ID 为 2047。

Citrix Session Recording Storage Manager Description: Exception caught while establishing database connection.（事件源: Citrix Session Recording Storage Manager 描述: 建立数据库连接时捕获到异常。） 此错误在托管 Session Recording Server 的计算机的事件查看器中的应用程序事件日志中显示。

无法连接到 Session Recording Server。Ensure that the Session Recording Server is running.（无法连接到 Session Recording Server。请确保 Session Recording Server 正在运行。） 启动 Session Recording 策略控制台时会显示此错误消息。

分辨率:

- Microsoft SQL Server 2008 R2 Express Edition、Microsoft SQL Server 2012 Express Edition、Microsoft SQL Server 2014 Express Edition 或 Microsoft SQL Server 2016 Express Edition 安装在独立的服务器上，并且没有为 Session Recording 配置的正确服务或设置。该服务器必须启用 TCP/IP 协议，并运行 SQL Server Browser 服务。有关启用这些设置的信息，请参阅 Microsoft 文档。
- Session Recording 安装期间（“管理”部分）提供了错误的服务器和数据库信息。卸载 Session Recording 数据库并重新安装，以提供正确的信息。
- Session Recording 数据库服务器处于关闭状态。请验证该服务器是否处于连接状态。
- 托管 Session Recording Server 的计算机或托管 Session Recording 数据库服务器的计算机无法解析对方的 FQDN 或 NetBIOS 名称。请使用 ping 命令验证这些名称是否可解析。
- 检查 Session Recording 数据库中的防火墙配置，以确保允许 SQL Server 连接。有关详细信息，请参阅 Microsoft 文章 https://msdn.microsoft.com/en-us/library/cc646023.aspx。

Logon failed for user 'NT_AUTHORITY\ANONYMOUS LOGON'.（用户“NT_AUTHORITY\ANONYMOUS LOGON”登录失败。）此错误消息表示用户以 .\administrator 身份错误地登录了服务。

解决方案：请以本地系统用户身份重新启动服务，并重新启动 SQL 服务。

如果未成功录制应用程序会话，请先检查运行 Session Recording Agent 和 Session Recording Server 的 VDA for Server OS 上的事件查看器中的应用程序事件日志。此日志可能会提供有价值的诊断信息。

如果未录制会话，以下问题可能是导致该问题的原因：

- **组件连接和证书。**如果 Session Recording 组件相互之间无法进行通信，可能会导致会话录制失败。要解决录制问题，请验证是否已将所有组件正确配置为指向正确的计算机，以及所有证书是否均有效且已正确安装。
- **非 Active Directory 域环境。**Session Recording 设计为在 Microsoft Active Directory 域环境中运行。如果您不在 Active Directory 环境中运行，可能会遇到录制问题。确保所有 Session Recording 组件都在属于 Active Directory 域成员的计算机上运行。
- **会话共享与活动策略冲突。**Session Recording 将活动策略与用户打开的第一个已发布应用程序相匹配。随后在同一会话中打开的应用程序都将继续遵循对第一个应用程序有效的策略。要防止会话共享与活动策略冲突，请在单独的 VDA for Server

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

OS 上发布冲突的应用程序。

- **未启用录制。**默认情况下，在 VDA for Server OS 上安装 Session Recording Agent 会启用服务器的录制功能。将活动录制策略配置为允许启用此功能之后，才开始录制。
- **活动录制策略不允许录制。**对于要录制的会话，活动录制策略必须允许录制用户、服务器或已发布应用程序的会话。
- **Session Recording 服务未运行。**对于要录制的会话，Session Recording Agent 服务必须在 VDA for Server OS 上运行，并且 Session Recording Storage Manager 服务必须在托管 Session Recording Server 的计算机上运行。
- **未配置 MSMQ。**如果未在运行 Session Recording Agent 的服务器上以及托管 Session Recording Server 的计算机上正确配置 MSMQ，可能会出现录制问题。

如果在使用 Session Recording Player 查看录制件时遇到困难，可能会显示以下错误消息：

下载录制的会话文件失败。不允许实时会话播放。服务器配置为不允许此功能。此错误表明服务器配置为不允许此操作。

解决方案：在 **Session Recording Server 属性**中，选择**播放** 选项卡，然后选择**允许实时会话播放** 复选框。

- 使用 Session Recording Player 查看录制件时，如果录制件损坏或不完整，Session Recording Agent 上的事件日志中还会显示警告消息。

  事件来源：Citrix Session Recording Storage Manager

  说明：录制文件 过程中数据丢失使用 Machine Creation Services (MCS) 或 Provisioning Services (PVS)

  创建的 VDA 配置了主映像并安装了 Microsoft Message Queuing (MSMQ) 时通常会出现此问题。在这种情况下，VDA 的 MSMQ 的 QMId 将相同。

  解决方法：为每个 VDA 创建唯一的 QMId。有关详细信息，请参阅此处（位于安装、升级和卸载 Session Recording 部分中）。

- 在播放某一录制文件时，Session Recording Player 可能会报告内部错误，并显示以下消息："**正在播放的文件报告在其原始录制期间发生一个内部系统错误(错误代码: 9)。该文件可继续播放到发生录制错误的点。**"。

  这通常是在录制图形密集型会话时，Session Recording Agent 缓冲区大小不足造成的。

  解决方法：在 Session Recording Agent 中将 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\SmAudBufferSizeMB 的注册表值更改为较高值，然后重新启动计算机。

安装 Session Recording 数据库或 Session Recording Server 时，测试连接失败并显示错误消息 **Database connection test failed. Please correct Database instance name**（数据库连接测试失败。请更正数据库实例名称），即使数据库实例名称正确也是如此。

在此情况下，请确保当前用户具有公共 SQL Server 角色权限，可以更正权限限制失败。

在 Windows Server 2008 R2 SP1 中，安装管理员日志记录功能之前，请首先安装 **.Net Framework 3.5 Features > WCF**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Activation > HTTP Activation，然后安装 .Net Framework 4.5 或更高版本。请勿以相反的顺序安装这两个要求。否则，管理员日志记录可能不会正常工作。在尝试使用 Server Properties 控制台更改 Session Recording 配置时，或者在启用了强制日志记录的情况下使用策略控制台更新 Session Recording 策略时，可能会遇到操作阻塞的问题。

要解决此问题，请执行以下操作：

1. 打开 Internet Information Services (IIS) 管理器并导航至**应用程序池**节点。
2. 右键单击 **SessionRecordingLoggingAppPool** 并打开**基本设置**对话框。
3. 将 .NET Framework 版本更改为 .NET Framework v4.0。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

验证组件连接

Dec 05, 2017

安装 Session Recording 的过程中，组件可能无法连接至其他组件。所有组件都能与 Session Recording Server (Broker) 通信。默认情况下，Broker（一种 IIS 组件）使用 IIS 默认的 Web 站点证书来确保安全。如果某个组件无法连接至 Session Recording Server，则其他组件在尝试连接时可能也会失败。

Session Recording Agent 和 Session Recording Server（存储管理器和 Broker）会将连接错误记入应用程序事件日志，该日志位于托管 Session Recording Server 的计算机的事件查看器中，而 Session Recording 策略控制台和 Session Recording Player 会在无法连接时在屏幕上显示连接错误消息。

1. 登录到安装了 Session Recording Agent 的服务器。
2. 从**开始**菜单中选择 **Session Recording Agent Properties**。
3. 在 **Session Recording Agent Properties** 中，单击**连接**。
4. 验证 Session Recording Server 的值是否为托管 Session Recording Server 的计算机的正确服务器名称。
5. 验证您的 VDA for Server OS 是否可以访问作为 Session Recording Server 的值提供的服务器。

注意：检查应用程序事件日志中是否记录了错误和警告。

小心：注册表编辑器使用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。

1. 登录到托管 Session Recording Server 的计算机。
2. 打开“注册表编辑器”。
3. 浏览至 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server。
4. 验证 **SmAudDatabaseInstance** 的值是否正确引用了 SQL Server 实例上安装的 Session Recording 数据库。

1. 使用 SQL 管理工具打开包含安装的 Session Recording 数据库的 SQL 实例。
2. 打开 Session Recording 数据库的安全性权限。
3. 验证 Session Recording 计算机帐户是否可以访问数据库。例如，如果托管 Session Recording Server 的计算机在 MIS 域中命名为 **SsRecSrv**，则应将数据库中的计算机帐户配置为 **MIS\SsRecSrv$**。该值会在安装 Session Recording 数据库期间进行配置。

通过使用 Web 浏览器访问 Session Recording Broker Web 页面来测试与 Session Recording Server IIS 站点的连接有助于确定 Session Recording 组件间的通信问题是否来自错误配置的协议配置、证书问题或启动 Session Recording Broker 时出现的问题。

验证 Session Recording Agent 的 IIS 连接：

1. 登录到安装了 Session Recording Agent 的服务器。
2. 启动 Web 浏览器，并输入以下地址：
   - HTTPS 地址：**https://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl**，其中 *servername* 是托管

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Session Recording Server 的计算机的名称
- HTTP 地址：**http://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl**，其中 *servername* 是托管 Session Recording Server 的计算机的名称

3. 如果系统提示您进行 NT LAN Manager (NTLM) 身份验证，请使用域管理员帐户进行登录。

验证 Session Recording Player 的 IIS 连接：

1. 登录到安装了 Session Recording Player 的工作站。
2. 启动 Web 浏览器，并输入以下地址：
   - HTTPS 地址：**https://servername/SessionRecordingBroker/Player.rem?wsdl**，其中 *servername* 是托管 Session Recording Server 的计算机的名称
   - **HTTP 地址：http://servername/SessionRecordingBroker/Player.rem?wsdl**，其中 *servername* 是托管 Session Recording Server 的计算机的名称
3. 如果系统提示您进行 NT LAN Manager (NTLM) 身份验证，请使用域管理员帐户进行登录。

验证 Session Recording 策略控制台的 IIS 连接：

1. 登录到安装了 Session Recording 策略控制台的服务器。
2. 启动 Web 浏览器，并输入以下地址：
   - HTTPS 地址：**https://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl**，其中 *servername* 是托管 Session Recording Server 的计算机的名称
   - HTTP 地址：**http://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl**，其中 *servername* 是托管 Session Recording Server 的计算机的名称
3. 如果系统提示您进行 NT LAN Manager (NTLM) 身份验证，请使用域管理员帐户进行登录。

如果您在浏览器中看到 XML 文档，则表明运行 Session Recording 策略控制台的计算机已通过配置的协议连接到托管 Session Recording Server 的计算机。

如果您将 HTTPS 作为通信协议，则必须使用服务器证书对托管 Session Recording Server 的计算机进行配置。 所有组件与 Session Recording Server 的连接均必须具有根证书颁发机构 (CA)。 否则，组件之间的连接尝试将失败。

可以在测试 IIS 连接时根据需要通过访问 Session Recording Broker Web 页面来测试证书。 如果能够访问各个组件的 XML 页面，则证书配置正确。

下面是证书问题导致连接失败的一些常见方式：

- **证书无效或丢失。** 如果运行 Session Recording Agent 的服务器没有 用于信任服务器证书的根证书，则无法建立信任，并通过 HTTPS 连接至 Session Recording Server，最终导致连接 失败。请验证所有组件是否均信任 Session Recording Server 上的服务器证书。
- **命名不一致。** 如果分配给托管 Session Recording Server 的计算机的服务器证书是使用完全限定域名 (FQDN) 创建的， 则连接至 Session Recording Server 时， 所有连接的组件均必须使用 FQDN。如果使用的是 NetBIOS 名称，请通过 Session Recording Server 的 NetBIOS 名称对组件进行配置。
- **证书已过期。**如果服务器的证书已过期， 则通过 HTTPS 与 Session Recording Server 的连接会失败。请验证分配给 托管 Session Recording Server 的计算机的 服务器证书是否有效且未过期。如果使用同一证书对会话录制进行 数字签名，则托管 Session Recording Server 的计算机的 事件日志会提供错误消息，表明证书已过期， 或在证书即将过期时提供警告信息。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

如果 Session Recording Player 失败，搜索录制件

Dec 05, 2017

如果使用 Session Recording Player 搜索录制件时遇到困难，则可能会显示以下错误消息：

- **搜索录制的会话文件失败。无法解析远程服务器名称：servername.**，其中 servername 为 Session Recording Player 尝试连接到的服务器的名称。Session Recording Player 无法访问 Session Recording Server。出现此种情况有两种可能原因：键入了错误的服务器名称，或者 DNS 无法解析服务器名称。
  解决方案：从播放器菜单栏中，依次选择**工具** > **选项** > **连接** ，并验证 **Session Recording Servers** 列表中列出的服务器名称是否正确。如果正确，请在命令提示窗口下运行 ping 命令，以查看是否可解析该名称。Session Recording Server 处于关闭或脱机状态时，搜索录制的会话文件失败，错误消息为**无法访问远程服务器**。

- **无法访问远程服务器。**Session Recording Server 处于关闭或脱机状态时会发生此错误。
  解决方案：验证 Session Recording Server 是否已连接。

- **访问被拒绝。**如果用户未被授予搜索和下载录制的会话文件的权限，可能会发生访问被拒绝错误。
  解决方案：使用 Session Recording Authorization 控制台向用户分配播放者角色。

- **分配播放者角色时访问被拒绝。**在安装了 Session Recording Server 的相同计算机上安装 Session Recording Player 时，同时已启用 UAC 的情况下，通常会出现此错误。在将域管理员或管理员用户组指定为播放者角色时，包含在该组中的非内置管理员用户在使用 Session Recording Player 搜索录制文件时可能无法通过基于角色的检查。
  解决方案：

  + 以管理员身份运行 Session Recording Player。

  + 将特定用户而非整个组指定为播放者角色。

  + 在单独的计算机而非 Session Recording Server 中安装 Session Recording Player。

- **搜索录制的会话文件失败。基础连接已关闭。无法为 SSL/TLS 安全通道建立信任关系。** 导致此异常的原因为：Session Recording Server 使用的是客户端设备不信任或没有 CA 证书的 CA 签发的证书。
  解决方案：在安装了 Session Recording Player 的工作站上安装正确或可信的 CA 证书。

- **远程服务器返回错误: (403) 已禁止。**此为尝试使用 HTTP（非安全协议）进行连接时出现的标准 HTTPS 错误。服务器拒绝连接，因为默认情况下，将其配置为仅接受安全连接。
  解决方案：从 **Session Recording Player** 菜单栏中，依次选择**工具** > **选项** > **连接**。从 **Session Recordings Servers** 列表中选择服务器，然后单击**修改**。将协议从 **HTTP** 更改为 **HTTPS**。

如果用户看到通知消息，但在 Session Recording Player 中执行搜索后无法找到相关录制件，MSMQ 可能存在问题。请验证队列是否已连接到 Session Recording Server（存储管理器），并使用 Web 浏览器测试是否存在连接错误（如果您将 HTTP 或 HTTPS 用作 MSMQ 通信协议）。

验证队列是否已连接：

1. 登录到托管 Session Recording Agent 的服务器，然后查看传出队列。
2. 验证到托管 Session Recording Server 的计算机的队列是否具有连接状态。
   - 如果此状态为 **waiting to connect**（等待连接），而队列中有大量消息，并且协议为 HTTP 或 HTTPS（与 **Session Recording Agent Properties** 中的**连接**选项卡上所选的协议一致），请执行步骤 3。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 如果此状态为**已连接**，而队列中没有消息，则表示托管 Session Recording Server 的服务器可能出现问题。请跳过步骤 3 并执行步骤 4。

3. 如果队列中有多条消息，请启动 Web 浏览器并键入以下地址：
   - HTTPS 地址：**https://servername/msmq/private$/CitrixSmAudData**，其中 *servername* 是托管 Session Recording Server 的计算机的名称
   - HTTP 地址：**http://servername/msmq/private$/CitrixSmAudData**，其中 *servername* 是托管 Session Recording Server 的计算机的名称

   如果此页面返回一个错误，例如 **The server only accepts secure connections**（服务器仅接受安全连接），请将 **Session Recording Agent Properties** 中列出的 MSMQ 协议更改为 HTTPS。否则，如果此页面报告 Web 站点的安全证书存在问题，则表示 TLS 安全通道的信任关系可能出现问题。在这种情况下，请安装正确的 CA 证书，或使用可信 CA。

4. 如果队列中没有消息，请登录到托管 Session Recording Server 的计算机，并查看专用队列。选择 **citrixsmauddata**。如果队列中有多条消息（消息列的数目），请验证 Session Recording StorageManager 服务是否已启动。如果未启动，请重新启动服务。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

更改通信协议

Dec 05, 2017

出于安全原因，Citrix 建议不要将 HTTP 用作通信协议。Session Recording 安装配置为使用 HTTPS。要使用 HTTP 来代替 HTTPS，必须更改多项设置。

1. 登录到托管 Session Recording Server 的计算机，然后禁用 IIS 中的 Session Recording Broker 安全连接。
2. 在安装了 Session Recording Agent 的每台服务器上，将 **Session Recording Agent 属性**中的协议设置从“HTTPS”更改为“HTTP”：
   1. 登录到安装了 Session Recording Agent 的每台服务器。
   2. 从**开始**菜单中选择 **Session Recording Agent 属性**。
   3. 在 **Session Recording Agent 属性**中选择**连接**选项卡。
   4. 在 **Session Recording Broker** 区域中，从**协议**下拉列表中选择 **HTTP**，然后单击**确定**以接受所做的更改。如果系统提示重新启动服务，请选择**是**。
3. 在 Session Recording Player 设置中将协议设置从“HTTPS”更改为“HTTP”：
   1. 登录到安装了 Session Recording Player 的每个工作站。
   2. 从**开始**菜单中选择 **Session Recording Player**。
   3. 从 **Session Recording Player** 菜单栏中，依次选择**工具** > **选项** > **连接**，然后选择服务器并选择**修改**。
   4. 从**协议**下拉列表中选择 **HTTP**，然后单击确定两次以接受所做的更改，并退出该对话框。
4. 在 Session Recording 策略控制台中将协议设置从“HTTPS”更改为“HTTP”：
   1. 登录到安装了 Session Recording 策略控制台的服务器。
   2. 从**开始**菜单中选择 **Session Recording 策略控制台**。
   3. 从**协议**下拉列表中选择 **HTTP**，然后单击确定以进行连接。如果连接成功，则在下次启动 Session Recording 策略控制台时，系统会记住此设置。

1. 登录到托管 Session Recording Server 的计算机，然后启用 IIS 中的 Session Recording Broker 安全连接。
2. 在安装了 Session Recording Agent 的每台服务器上，将 **Session Recording Agent 属性**中的协议设置从“HTTP”更改为“HTTPS”：
   1. 登录到安装了 Session Recording Agent 的每台服务器。
   2. 从**开始**菜单中选择 **Session Recording Agent 属性**。
   3. 在 **Session Recording Agent 属性**中选择**连接**选项卡。
   4. 在 **Session Recording Broker** 区域中，从**协议**下拉列表中选择 **HTTPS**，然后单击**确定**以接受所做的更改。如果系统提示重新启动服务，请选择**是**。
3. 在 Session Recording Player 设置中将协议设置从“HTTP”更改为“HTTPS”：
   1. 登录到安装了 Session Recording Player 的每个工作站。
   2. 从**开始**菜单中选择 **Session Recording Player**。
   3. 从 **Session Recording Player** 菜单栏中，依次选择**工具** > **选项** > **连接**，然后选择服务器并选择**修改**。
   4. 从**协议**下拉列表中选择 **HTTPS**，然后单击**确定**两次以接受所做的更改，并退出该对话框。
4. 在 Session Recording 策略控制台中将协议设置从“HTTP”更改为“HTTPS”：
   1. 登录到安装了 Session Recording 策略控制台的服务器。
   2. 从**开始**菜单中选择 **Session Recording 策略控制台**。
   3. 从**协议**下拉列表中选择 **HTTPS**，然后单击**确定** 以进行连接。如果连接成功，则在下次启动 Session Recording 策略控制台时，系统会记住此设置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

参考：管理您的数据库记录

Dec 05, 2017

ICA 日志数据库 (ICLDB) 实用程序是用于管理会话录制数据库记录的数据库命令行实用程序。此实用程序在 Session Recording 安装期间安装在托管 Session Recording Server 软件的服务器上的 drive:\Program Files\Citrix\SessionRecording\Server\Bin 目录中。

下表列出了 ICLDB 实用程序可用的命令和选项。使用以下格式键入命令：

icldb [version | locate | dormant | import | archive | remove | removeall] 命令选项 [/l] [/f] [/s] [/?]

注意：与此实用程序关联的帮助中提供了更多详细说明。要访问帮助，请在命令提示窗口中键入 drive:\Program Files\Citrix\SessionRecording\Server\Bin 目录，然后键入 **icldb /?**。要访问特定命令的帮助，请键入 **icldb *命令* /?**。

命令	说明
archive	存档超过指定的保留期的会话录制文件。 此命令用于存档文件。
dormant	显示或计数被视为休眠的会话录制文件。休眠文件是指由于数据丢失而未完成的会话录制。 此命令用于在您怀疑有数据丢失时进行验证。可以验证是整个数据库的会话录制文件都进入休眠，还是只有指定天数、小时数或分钟数内录制件进入休眠。
import	将会话录制文件导入 Session Recording 数据库。 此命令用于在丢失数据库录制时重建数据库。 此外，此命令还用于合并数据库（如果您有两个数据库，则可以导入其中一个数据库中的文件）。
locate	将会话录制文件 ID 用作条件查找并显示该文件的完整路径。 查找会话录制文件的存储位置时可使用此命令。 此命令还可用于通过特定文件来验证数据库是否为最新。
remove	从数据库中删除对会话录制文件的引用。 此命令用于清理数据库（使用时需谨慎）。指定要用作条件的保留期。 也可以删除关联的物理文件。
removeall	从 Session Recording 数据库中删除对会话录制文件的所有引用，并将数据库返回原始状态。不会删除实际物理文件；但您无法在 Session Recording Player 中搜索这些文件。 此命令用于清理数据库（使用时需谨慎）。只能通过从备份中恢复来还原删除的引用。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

命令	说明
version	显示 Session Recording 数据库架构版本。
/l	将结果和错误记录到 Windows 事件日志。
/f	强制运行命令而不提示。
/s	不显示版权信息。
/?	显示命令的帮助。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置日志记录

Dec 05, 2017

配置日志记录捕获针对数据库的站点配置更改和管理活动。您可以使用记录的内容进行以下操作：

- 在发生配置更改后诊断问题和故障排除；日志提供导航路径记录
- 协助变更管理及跟踪配置
- 报告管理活动

您可以设置配置日志记录首选项，显示配置日志，并从 Citrix Studio 生成 HTML 和 CSV 报告。您可以按日期范围和全文搜索结果过滤显示的配置日志。如果启用强制日志记录，可以阻止进行配置更改，除非这些更改可以记入日志。只要具有适当的权限，即可删除配置日志中的条目。您无法使用配置日志记录功能编辑日志内容。

配置日志记录使用 PowerShell SDK 和 Configuration Logging Service。Configuration Logging Service 会在站点中的每个 Controller 上运行；如果某个 Controller 出现故障，另一个 Controller 上的服务将自动处理日志记录请求。

默认情况下，启用配置日志记录功能，它使用在您创建站点时所创建的数据库（站点配置数据库）。您可以为数据库指定不同位置。配置日志记录数据库与站点配置数据库支持相同的高可用性功能。

对配置日志记录的访问通过委派管理进行控制，需要具有编辑日志记录首选项和查看配置日志权限。

配置日志会在创建时进行本地化。例如，以英语创建的日志将以英语显示，而无论阅读器的区域设置如何。

记录的内容

通过 Studio、Director 和 PowerShell 脚本启动的配置更改和管理活动都在记录范围之内。记录的配置更改包括对以下项目的处理（创建、编辑、删除和分配）：

- 计算机目录
- 交付组（包括更改电源管理设置）
- 管理员角色和作用域
- 主机资源和连接
- 通过 Studio 管理的 Citrix 策略

记录的管理更改示例包括：

- 虚拟机或用户桌面的电源管理
- Studio 或 Director 向用户发送消息

以下操作不在记录范围之内：

- 自动操作，如虚拟机的池管理启动。
- 通过组策略管理控制台 (GPMC) 实施的策略操作；使用 Microsoft 工具查看这些操作的日志。
- 通过注册表、直接访问数据库或从 Studio、Director 或 PowerShell 以外的来源进行的更改。
- 初始化部署后，配置日志记录从在 Configuration Service 中注册首个 Configuration Logging Service 实例时开始可用。因此，早期阶段的配置不会记入日志（例如，获取和应用数据库架构以及初始化虚拟机管理程序期间的配置）。

管理配置日志记录

© 1999-2017 Citrix Systems, Inc. All rights reserved.

默认情况下，配置日志记录使用在您创建站点时所创建的数据库（也称为站点配置数据库）。Citrix 建议您为配置日志记录数据库（和监视数据库）使用单独的位置，原因如下：

- 配置日志记录数据库的备份策略可能与站点配置数据库的备份策略有所不同。
- 通过配置日志记录（以及 Monitoring Service）收集的数据量可能会对站点配置数据库的可用空间造成负面影响。
- 它会针对三个数据库拆分单点故障。

注意：不支持配置日志记录的产品版本在 Studio 中没有日志记录节点。

启用和禁用配置日志记录以及强制日志记录

默认情况下，启用配置日志记录，禁用强制日志记录。

1. 在 Studio 导航窗格中，选择**日志记录**。
2. 在“操作”窗格中选择**首选项**。“配置日志记录”对话框中包含数据库信息，并指示配置日志记录和强制日志记录处于启用还是禁用状态。
3. 选择所需的操作：

   要启用配置日志记录，请选择**启用**单选按钮。此为默认设置。如果无法向数据库写入信息，则日志记录信息将被丢弃，但操作仍继续。

   要禁用配置日志记录，请选择**禁用**单选按钮。如果先前已启用日志记录，现有的日志仍然可通过 PowerShell SDK 进行读取。

   要启用强制日志记录，请选择**阻止在数据库不可用时更改站点配置**单选按钮。不允许写入通常会写入日志的配置更改或管理活动，除非可将其写入配置日志记录数据库。仅当启用配置日志记录，即选择**启用**单选按钮时，才能启用强制日志记录。如果 Configuration Logging Service 出现故障，并且未使用高可用性，则会使用强制日志记录。在这种情况下，将不会执行通常会记入日志的操作。

   要禁用强制日志记录，请选择**允许在数据库不可用时更改站点配置**单选按钮。即使配置日志记录的数据库无法访问，也允许执行配置更改和管理活动。此为默认设置。

更改配置日志记录数据库的位置

注意：启用强制日志记录时无法更改数据库位置，因为更改位置时会断开连接一小段时间，在此期间无法进行日志记录。

1. 使用支持的 SQL Server 版本创建数据库服务器。
2. 在 Studio 导航窗格中，选择**日志记录**。
3. 在“操作”窗格中选择**首选项**。
4. 在“日志记录首选项”对话框中，选择**更改日志记录数据库**。
5. 在“更改日志记录数据库”对话框中，指定包含新数据库服务器的服务器的位置。有效格式在“数据库”一文中列出。
6. 要允许 Studio 创建数据库，请单击**确定**。出现提示时，单击**确定**，系统将自动创建数据库。Studio 会尝试使用当前 Studio 用户的凭据访问数据库；如果此操作失败，系统会提示您输入数据库用户的凭据。然后，Studio 会将数据库架构上载到数据库。（凭据只会在创建数据库期间保留。）
7. 要手动创建数据库，请单击**生成数据库脚本**。生成的脚本包括有关手动创建数据库的说明。在上载架构之前，请确保数据库为空，且至少有一个用户有权访问并更改该数据库。

先前数据库中的配置日志记录数据不会导入新数据库中。检索日志时，不能合并来自两个数据库的日志。新配置日志记录数据

© 1999-2017 Citrix Systems, Inc. All rights reserved.

库中的第一个日志条目将指明发生了数据库更改，但无法确定先前的数据库。

显示配置日志内容

启动配置更改和管理活动时，Studio 的中上部窗格中将显示 Studio 和 Director 创建的高级别操作。高级别操作会导致一个或多个服务和 SDK 调用，后者为低级别操作。在中上部窗格中选择一项高级别操作时，中下部窗格将显示低级别操作。

如果操作在完成之前失败，可能无法在数据库中完成日志操作；例如，开始记录将没有对应的停止记录。在这种情况下，日志会指出缺少信息。在基于时间范围显示日志时，如果不完整日志中的数据符合条件，则会显示这些不完整的日志。例如，当请求过去五天的所有日志时，如果存在的某个日志的开始时间在过去五天内但没有结束时间，则会包括该日志。

在使用脚本调用 PowerShell cmdlet 时，如果您在创建低级别操作时不指定高级别父操作，则配置日志记录将创建替代的高级别操作。

要显示配置日志内容，请在 Studio 导航窗格中选择**日志记录**。默认情况下，在中心窗格显示的内容会按时间顺序列出日志内容（最新的条目在最前面），并按日期进行分隔。

显示内容过滤条件	完成此操作
搜索结果	在中间窗格顶部的搜索框中输入文本。过滤的显示内容包括搜索结果的数量。要返回到标准的日志记录显示，请清除搜索框中的文本。
列标题	单击列标题可以按该字段对显示内容排序。
日期范围	从中间窗格顶部搜索框旁边的下拉列表框中选择一个时间间隔。

生成报告

您可以生成包含配置日志数据的 CSV 和 HTML 报告。

- CSV 报告包含指定时间间隔内的所有日志记录数据。数据库中的分层数据被简化为单个 CSV 表。所有数据项在此文件中都不具有优先级。不进行任何格式化，也不假定具有可读性。文件（名称为 MyReport）只包含通用格式的数据。CSV 文件通常用于存档数据，或作为报告或数据操作工具（如 Microsoft Excel）的数据源。
- HTML 报告以便于用户理解的格式提供指定时间间隔内的日志记录数据。它提供层次分明的导航视图，便于检查更改。HTML 报告包括两个文件，名称分别为“摘要”和“详细信息”。“摘要”列出了高级别操作：每个操作发生的时间、执行者和结果。单击每个操作旁边的详细信息链接可转至提供其他信息的“详细信息”文件中的低级别操作。

要生成配置日志报告，请在 Studio 导航窗格中选择**日志记录**，然后在“操作”窗格中选择**创建自定义报告**。

- 选择报告的日期范围。
- 选择报告格式：CSV、HTML 或二者。
- 浏览到报告的保存位置。

删除配置日志内容

© 1999-2017 Citrix Systems, Inc. All rights reserved.

要删除配置日志，必须具有特定的委派管理和 SQL Server 数据库权限。

- **委派管理** — 必须具有允许读取部署配置的委派管理角色。内置的完全权限管理员角色具有此权限。自定义角色必须具有在“其他权限”类别中选择的“只读”或“管理”权限。
  要在删除配置日志记录数据之前为其创建备份，自定义角色还必须具有在“日志记录权限”类别中选择的“只读”或“管理”权限。

- **SQL Server 数据库** — 必须具备拥有可从数据库中删除记录权限的 SQL Server 登录。有两种方式实现此要求：
  - 使用具有 sysadmin 服务器角色的 SQL Server 数据库登录名，该角色允许在数据库服务器上执行任何活动。此外，serveradmin 或 setupadmin 服务器角色还允许执行删除操作。
  - 如果部署需要更高的安全性，请使用映射到具有从数据库中删除记录权限的数据库用户的非 sysadmin 数据库登录名。
    1. 在 SQL Server Management Studio 中，以“sysadmin”以外的服务器角色创建 SQL Server 登录名。
    2. 将登录名映射到数据库中的某个用户；SQL Server 将自动在数据库中以登录名创建用户。
    3. 在数据库角色成员身份中，为数据库用户至少指定一种角色成员身份：ConfigurationLoggingSchema_ROLE 或 dbowner。

    有关更多信息，请参阅 SQL Server Management Studio 文档。

要删除配置日志，请执行以下操作：

1. 在 Studio 导航窗格中，选择**日志记录**。
2. 在“操作”窗格中选择**删除日志**。
3. 在删除日志前，系统会询问是否要创建日志备份。如果选择创建备份，请浏览到应保存备份存档的位置。备份将以 CSV 文件格式创建。

在清除配置日志后，日志删除是发布到空日志的第一项活动。该条目将提供有关删除日志的用户以及时间的详细信息。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

事件日志

Dec 05, 2017

下列文章包含 XenApp 和 XenDesktop 服务可以记录的事件的列表和说明。

此信息不全面；读者应检查各功能文章了解其他事件信息。

- Citrix Broker Service 事件
- Citrix FMA Service SDK 事件
- Citrix Configuration Service 事件
- Citrix Delegated Administration Service 事件

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Director

Dec 05, 2017

在本文中：

关于 Director

部署和配置 Director

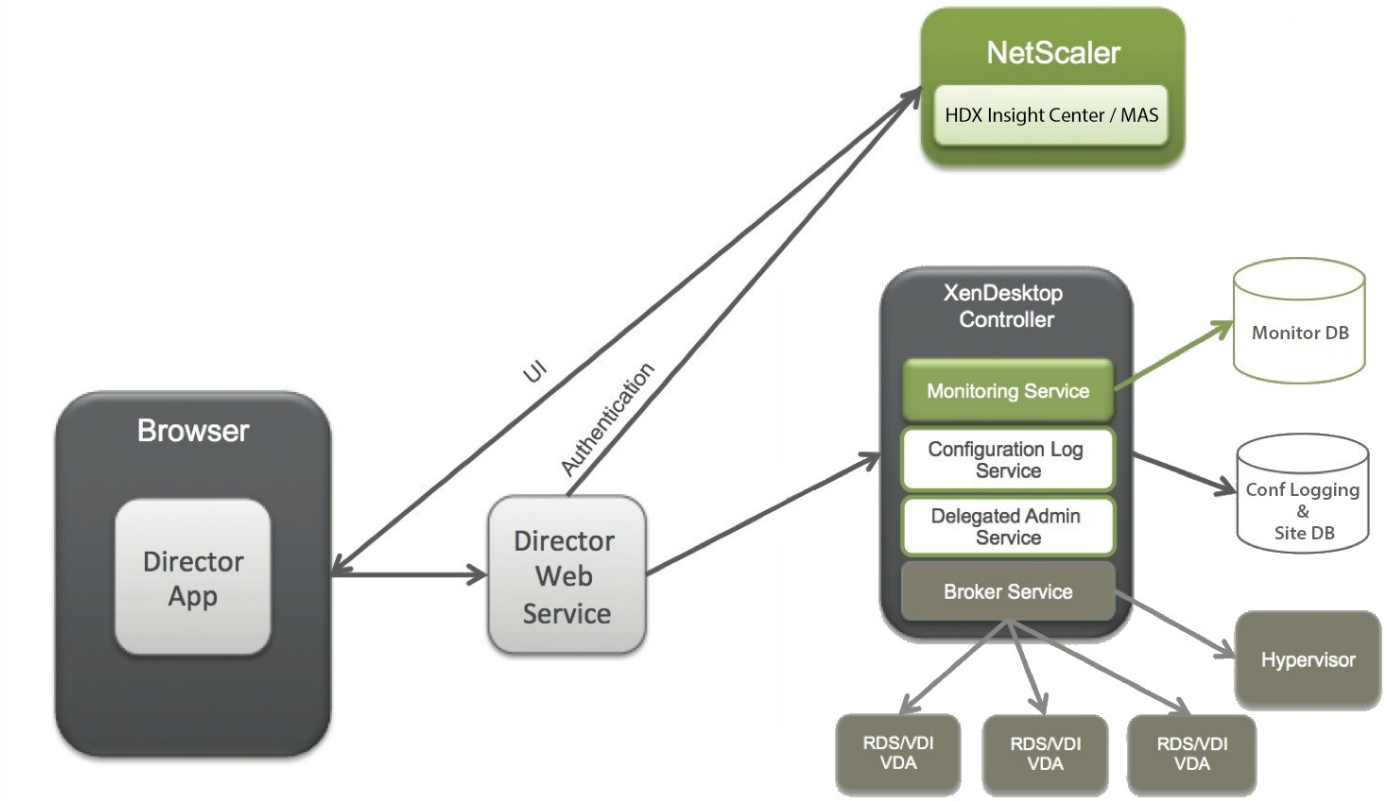
安装 Director

安装 Director for XenApp 6.5

登录 Director

将 Director 与集成 Windows 身份验证结合使用

Director 是适用于 XenApp 和 XenDesktop 的监视和故障排除控制台。



Director 可以访问：

- 使用集成了 Analytics、Performance Manager 和 Network Inspector 的统一控制台访问来自 Broker Agent 的实时数据。
  - Analytics 包括用于运行状况、容量保障、历史趋势和网络分析的性能管理，由 NetScaler Insight Center 或 NetScaler MAS 提供技术支持，可识别由 XenApp 或 XenDesktop 环境中的网络导致的瓶颈。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 存储在监视数据库中的历史数据，用于访问配置日志记录数据库。
- 使用 NetScaler Insight Center 或 NetScaler MAS 的 NetScaler Gateway 中的 ICA 数据。
  - 可以了解 XenApp 或 XenDesktop 的虚拟应用程序、桌面和用户的最终用户体验。
  - 将网络数据与应用程序数据和实时指标关联起来，以便有效进行故障排除。
  - 与 XenDesktop 7 Director 监视工具集成。
- 允许运行时监视的个人虚拟磁盘数据显示基本分配，并使技术支持管理员能够重置个人虚拟磁盘（重置为仅在必要时使用）。
  - 命令行工具 CtxPvdDiag.exe 用于将用户日志信息收集到一个文件中，以供执行故障排除使用。

Director 使用故障排除控制板。此控制板提供对 XenApp 或 XenDesktop 站点的实时和历史运行状况监视。利用此功能，您可以实时查看故障，更好地了解最终用户的体验。

有关 Director 功能与 Delivery Controller (DC)、VDA 以及任何其他依赖组件的兼容性的详细信息，请参阅功能兼容性列表。

界面视图

Director 提供了面向特定管理员定制的不同界面 视图。产品权限决定显示的内容和可用的命令。

例如，技术支持管理员可以看到专为技术支持任务定制的界面。Director 允许技术支持管理员搜索报告问题的用户并显示与该用户相关联的活动，例如用户的应用程序和进程的状态。他们可以通过执行相应操作来快速解决问题，例如终止无响应的应用程序或进程、重影用户计算机上的操作、重新启动计算机或重置用户配置文件。

相比之下，完全权限管理员可以查看和管理整个站点，并且可以对多个用户和计算机执行命令。控制板提供了部署各主要方面的概况，例如会话状态、用户登录和站点基础结构。信息每分钟更新一次。如果出现问题，将会自动显示有关所发生故障的数量和类型的详细信息。

默认情况下，Director 作为 Web 站点安装在 Delivery Controller 上。有关必备项和其他详细信息，请参阅此版本的系统要求文档。

此版本的 Director 与 6.5 版之前的 XenApp 部署或 7 版之前的 XenDesktop 部署不兼容。

当在包含多个站点的环境中使用 Director 时，请确保对安装了 Controller、Director 和其他核心组件的所有服务器上的系统时钟进行同步。否则，站点可能无法在 Director 中正确显示。

提示：如果您计划监视 XenApp 6.5 和 XenApp 7.5 或 XenDesktop 7.x 站点，Citrix 建议将 Director 与用于监视 XenApp 6.5 站点的 Director 控制台安装在不同的服务器上。

重要：要保护通过网络使用纯文本发送的用户名和密码的安全，Citrix 强烈建议您仅允许使用 HTTPS（而不是 HTTP）进行 Director 连接。某些工具可以读取 HTTP（未加密）网络数据包中的纯文本用户名和密码，这会对用户造成潜在安全风险。

配置权限

要登录 Director，具有 Director 权限的管理员必须是 Active Directory 域用户并且必须具有以下权限：

- 对要搜索的所有 Active Directory 林的读取权限（请参阅高级配置）。
- 配置的委派管理员角色（请参阅委派管理和 Director）。
- 要重影用户，必须使用适用于 Windows 远程协助的 Microsoft 组策略来配置管理员。此外：
  - 安装 VDA 时，确保在所有用户设备（默认处于选中状态）上启用 Windows 远程协助功能。
  - 在服务器上安装 Director 时，确保已安装 Windows 远程协助（默认处于选中状态）。但默认情况下服务器上禁用此功

© 1999-2017 Citrix Systems, Inc. All rights reserved.

能。无需对 Director 启用此功能，即可为最终用户提供协助。Citrix 建议将此功能保持禁用状态，以提高服务器的安全性。

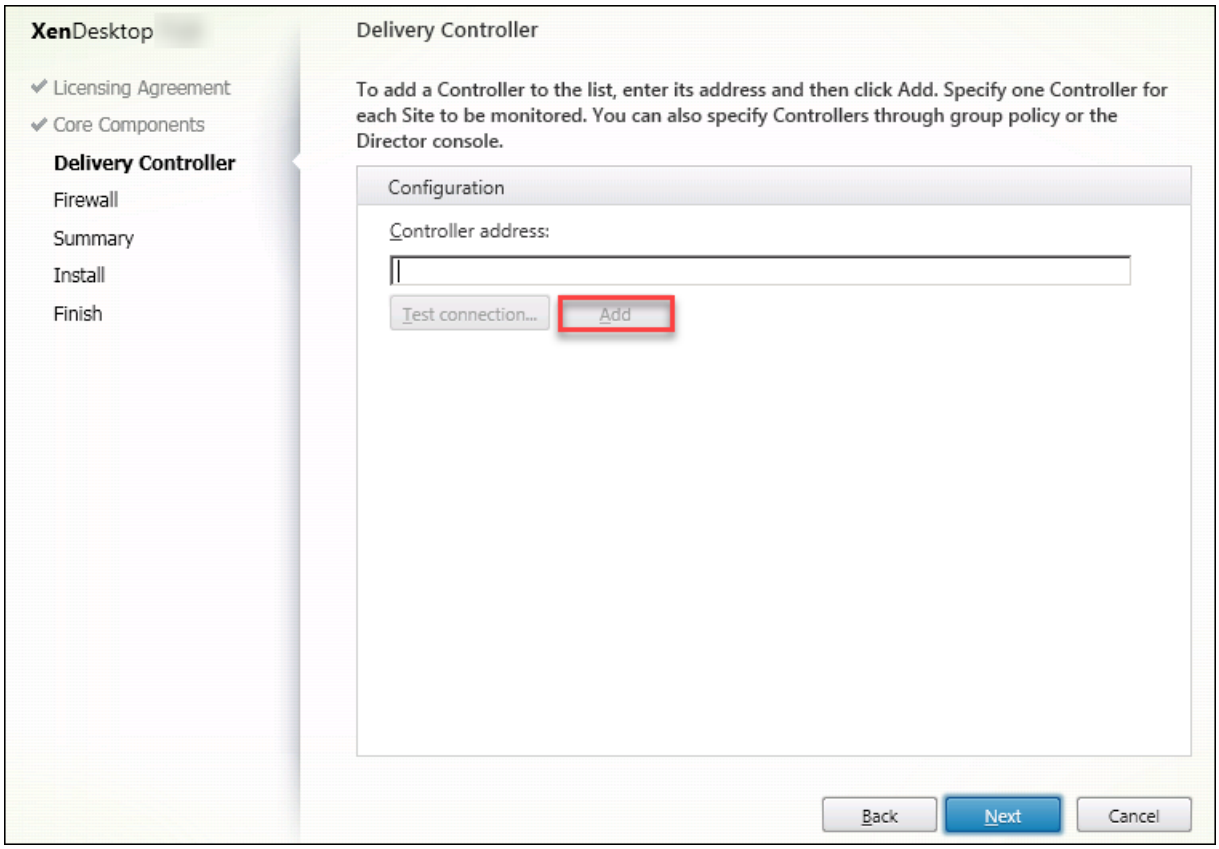
- 要使管理员能够启动 Windows 远程协助，请使用远程协助的相应 Microsoft 组策略设置向其授予所需的权限。有关信息，请参阅 CTX127388: How to Enable Remote Assistance for Desktop Director（如何为 Desktop Director 启用远程协助）。

- 对于安装了版本 7 之前的 VDA 的用户设备，必须执行附加配置。请参阅为 XenDesktop 7 之前版本的 VDA 配置权限。

使用 XenApp 和 XenDesktop 完整产品 ISO 安装程序安装 Director，该安装程序将检查必备项，安装任何缺少的组件，设置 Director Web 站点，以及执行基本配置。ISO 安装程序提供的默认配置可处理典型部署。如果在安装期间未安装 Director，请使用 ISO 安装程序添加 Director。要添加任何其他组件，请重新运行 ISO 安装程序并选择要安装的组件。有关使用 ISO 安装程序的信息，请参阅安装文档中的安装核心组件。Citrix 建议仅使用完整产品 ISO 安装程序进行安装，而不是使用 .MSI 文件。

当 Director 安装在 Controller 上时，将自动配置 localhost 作为服务器地址，并且默认情况下，Director 将与本地 Controller 进行通信。

要在 Controller 的远程专用服务器上安装 Director，系统将提示您输入 Controller 的 FQDN 或 IP 地址。



注意：可单击**添加**来添加要监视的 Controller。

默认情况下，Director 与指定的 Controller 进行通信。仅为监视的每个站点指定一个 Controller 地址。Director 将自动发现同一站点中的所有其他 Controller，并且如果您指定的 Controller 出现故障，则将回退到其他 Controller。

注意：Director 无法在 Controller 之间平衡负载。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

为确保浏览器与 Web 服务器之间的通信安全，Citrix 建议您在托管 Director 的 IIS Web 站点上实施 TLS。有关说明，请参阅 Microsoft IIS 文档。无需对 Director 执行任何配置即可启用 TLS。

要安装 Director for XenApp 6.5，请执行以下步骤。通常，将 Director 与 XenApp Controller 安装在不同的计算机上。

1. 从 XenApp 安装介质安装 Director。如果已为 XenDesktop 安装 Director，请跳过此步骤并继续执行下一个步骤。
2. 在每台 Director 服务器上，使用 IIS 管理器控制台在应用程序设置中更新 XenApp 服务器地址的列表，如高级配置中的**向 Director 中添加站点**部分所述。
   按 XenApp 站点提供一个 Controller 的服务器地址：XenApp 站点中的所有其他 Controller 自动用于故障转移。Director 无法在 Controller 之间平衡负载。
   重要：对于 XenApp 地址，请确保使用设置 Service.AutoDiscoveryAddressesXA，而非默认设置 Service.AutoDiscoveryAddresses。
3. Director WMI 提供程序的安装程序位于 DVD 上的 **Support\DirectorWMIProvider** 文件夹中。将其安装在所有合适的 XenApp 服务器（运行会话的 Controller 和工作服务器）上。
   如果未配置 **winrm**，应运行 **winrm qc** 命令。
4. 将每台 XenApp 工作服务器配置为接受 WinRM 查询，如配置权限中所述。
5. 为端口 2513 配置防火墙例外，Director 与 XenApp 之间进行通信时使用此端口。
6. 为确保浏览器与 Web 服务器之间的通信安全，Citrix 建议您在托管 Director 的 IIS Web 站点上实施 TLS。
   有关说明，请参阅 Microsoft IIS 文档。无需对 Director 执行任何配置即可启用 TLS。

注意：要允许 Director 查找场中的所有 XenApp 工作组，必须在此场使用的 DNS 服务器上为 XenApp 服务器所在的子网添加反向 DNS 区域。

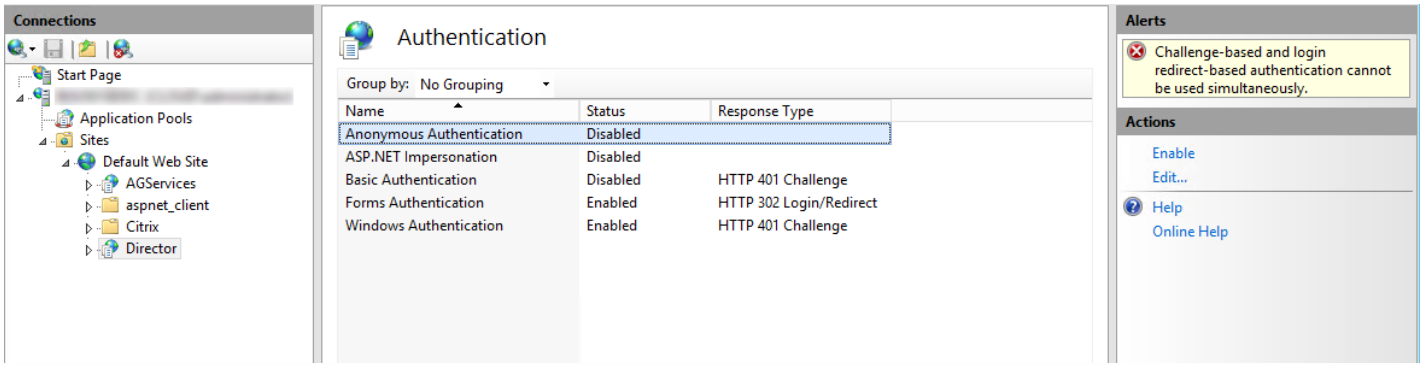
Director Web 站点位于 https 或 http:///Director 处。

如果在多站点部署中，一个站点出现故障，则 Director 登录在尝试连接到出现故障的站点时会花费较长的时间。

通过集成 Windows 身份验证，加入了域的用户可以获得直接访问 Director 的权限，而不需要重新在 Director 登录页面上键入其凭据。使用集成 Windows 身份验证和 Director 的必备条件如下：

- 在托管 Director 的 IIS Web 站点上启用集成 Windows 身份验证。安装 Director 时，启用匿名和表单身份验证。要使用集成 Windows 身份验证和 Director，请禁用匿名身份验证并启用 Windows 身份验证。对于非域用户的身份验证，表单身份验证仍必须设置为“已启用”。
  1. 启动 IIS 管理器。
  2. 转至**站点** > **默认 Web 站点** > **Director**。
  3. 选择**身份验证**。
  4. 右键单击**匿名身份验证**，然后选择**禁用**。
  5. 右键单击 **Windows 身份验证**，然后选择**启用**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- 为 Director 计算机配置 Active Directory 委派权限。如果 Director 和 Delivery Controller 安装在单独的计算机上，则需要配置此设置。
  1. 在 Active Directory 计算机上，打开 Active Directory 管理控制台。
  2. 在 Active Directory 管理控制台中，导航到**域名** > **计算机**。选择 Director 计算机。
  3. 单击鼠标右键并选择**属性**。
  4. 在“属性”中，选择**委派**选项卡。
  5. 选择选项**信任此计算机来委派任何服务(仅 Kerberos)**。

- 用于访问 Director 的浏览器必须支持集成 Windows 身份验证。在 Firefox 和 Chrome 中，可能需要执行额外的配置步骤才能支持该身份验证。有关详细信息，请参阅浏览器文档。
- Monitoring Service 必须运行 Microsoft .NET Framework 4.5.1 或 Director 的系统要求中列出的受支持的更高版本。有关详细信息，请参阅系统要求。

用户注销 Director 时，或者如果会话超时，将显示登录页面。在登录页面中，用户可以将“身份验证类型”设置为**自动登录**或**用户凭据**。

Google Analytics 执行的使用数据收集

Director Service 会在安装 Director 后使用 Google Analytics 匿名收集使用数据。会收集有关“趋势”页面及其选项卡的使用情况的统计数据和信息默认情况下，安装 Director 时启用数据收集。

要选择退出 Google Analytics 数据收集，请在安装 Director 的计算机上编辑注册表项 HKEY_LOCAL_MACHINE\Software\Citrix\MetaInstall，如 Citrix Insight Services 中的“安装和升级分析”部分所述。

注意：HKEY_LOCAL_MACHINE\Software\Citrix\MetaInstall 注册表项控制 Citrix Insight Services 以及 Google Analytics 执行的使用数据的收集。对注册表值所做的任何更改都将影响这两项服务执行的收集操作。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

高级配置

Dec 05, 2017

在本文中：

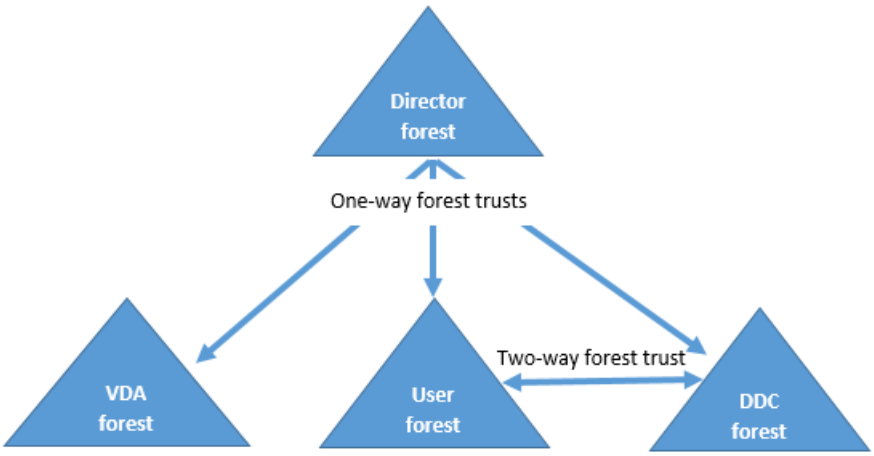
使 Director 能够在多林环境中工作的建议配置

向 Director 添加站点

在活动管理器中禁止显示运行中的应用程序

Director 可支持跨越一个林配置的多林环境，其中用户、Domain Delivery Controller (DDC)、VDA 和 Director 均位于不同的林中。这要求在这些林中和配置设置中正确设置信任关系。

建议的 配置要求在这些林中使用整个域身份验证创建传出和传入林信任 关系。



通过 Director 中的信任关系，管理员可以对位于不同林的用户会话、VDA 和域控制器中出现的问题进行故障排除。

可以通过 Internet Information Services (IIS) Manager 中定义的设置来控制 Director 所需的用于支持多林的高级配置。
重要：如果更改了 IIS 中的某项设置，Director 服务会自动重新启动并注销用户。
使用 IIS 配置 高级设置：

1. 打开 Internet Information Services (IIS) 管理器模块。
2. 转到默认 Web 站点下的 Director Web 站点。
3. 双击“应用程序设置”。
4. 双击某个设置以对其进行编辑。

默认情况下，铂金版许可证保留 90 天以内的数据。有关配置的详细信息，请参阅数据粒度和保留。

Director 使用 Active Directory 搜索用户并查找其他用户和计算机信息。默认情况下，Director 搜索：

- 管理员帐户所属的域或林。
- Director Web 服务器所属的域或林（如果不相同）。

Director 将尝试使用 Active Directory 全局目录在林级别执行搜索。如果您没有相应的权限，无法在林级别执行搜索，则仅搜

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

索域。

要搜索或查询其他 Active Directory 域或林中的数据，必须明确设置要搜索的域或林。配置以下设置：

```
Connector.ActiveDirectory.Domains = (user),(server)
```

值属性“user”和“server”分别代表 Director user（管理员）和 Director server 所在的域。

要使用户能够从其他域或林中进行搜索，请将该域的名称添加到列表中，如下例中所示：

```
Connector.ActiveDirectory.Domains = (user),(server),,
```

对于列表中的每个域，Director 将尝试在林级别执行搜索。如果您没有相应的权限，无法在林级别执行搜索，则仅搜索域。

注意：在包含多个林的环境中，Director 不显示已使用域本地组分配给 XenDesktop 交付组的其他林中的用户的会话详细信息。

如果已安装 Director，可将其配置为使用多个站点。要执行此操作，请在每个 Director 服务器上使用 IIS 管理器控制台来更新应用程序设置中服务器地址的列表。

将每个站点中的 Controller 地址添加到以下设置中：

Service.AutoDiscoveryAddresses = SiteAController,SiteBController

其中 *SiteAController* 和 *SiteBController* 为两个不同站点中的 Delivery Controller 地址。

对于 XenApp 6.5 站点，请将每个 XenApp 场中的 Controller 地址添加到以下设置中：

Service.AutoDiscoveryAddressesXA = FarmAController,FarmBController

其中 *FarmAController* 和 *FarmBController* 为两个不同场中的 XenApp Controller 的地址。

对于 XenApp 6.5 站点，从 XenApp 场添加 Controller 的另一种方法为：

DirectorConfig.exe /xenapp FarmControllerName

默认情况下，Director 中的活动管理器显示用户会话正在运行的所有应用程序的列表。对 Director 中的活动管理器功能具有访问权限的所有管理员均可以查看此信息。对于委派管理员角色，完全权限管理员、交付组管理员和技术支持管理员均可以查看此信息。

为保护用户及其正在运行的应用程序的隐私，您可以禁止“应用程序”选项卡以列出正在运行的应用程序。

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。

1. 在 VDA 上，修改位于 HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed 的注册表项。默认情况下，该注册表项设置为 1。将值更改为 0，这表示信息不是从 VDA 中收集的，因此不在活动管理器中显示。
2. 在安装了 Director 的服务器上，修改用于控制正在运行的应用程序可见性的设置。默认情况下，该值为 true，表示允许应

© 1999-2017 Citrix Systems, Inc. All rights reserved.

用程序选项卡显示正在运行的应用程序。将该值更改为“false”，表示禁用其可见性。此选项仅影响 Director 中的活动管理器，不影响 VDA。

修改以下设置的值：

UI.TaskManager.EnableApplications = false

重要：要禁止查看运行中的应用程序，Citrix 建议进行上述两项更改，以确保在活动管理器中不显示这些数据。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

显示器部署

Feb 01, 2018

在本文中：

监视站点

监视会话

过滤数据以排除故障

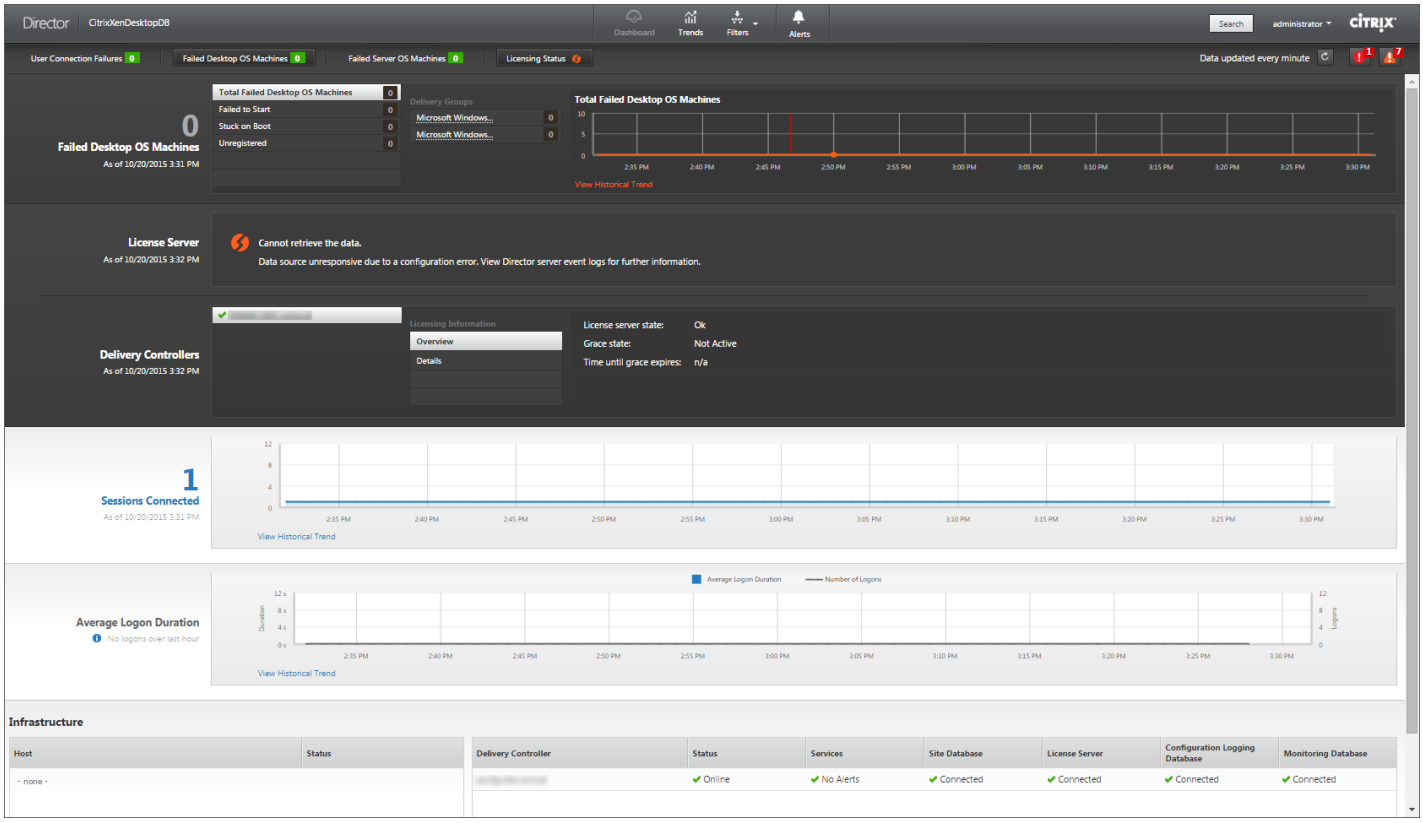
监视站点的历史趋势

监视修补程序

控制用户计算机电源状态

阻止与计算机连接

如果您具有完全权限管理员权限，在打开 Director 时，控制板将提供一个中央位置来监视站点的运行状况和使用情况。



如果当前没有故障或者在过去 60 分钟内没有发生故障，各个面板将保持折叠状态。 发生故障时，将自动显示特定的故障面板。

注意：某些选项或功能可能不可用，具体取决于组织的许可证和您的管理员权限

© 1999-2017 Citrix Systems, Inc. All rights reserved.

面板	说明
用户连接失败次数	过去 60 分钟内的连接故障。单击总数旁的类别可以查看该类型故障的指标。在相邻的表中，该数量按照交付组细分。连接故障包括达到应用程序限制导致的故障。有关应用程序限制的详细信息，请参阅应用程序。
发生故障的桌面操作系统计算机或发生故障的服务器操作系统计算机	在过去 60 分钟内按照交付组细分的所有故障。按类型（包括无法启动、引导时卡住以及未注册）细分的故障。对于服务器操作系统计算机，故障还包括计算机达到最大负载。
许可状态	• 许可证服务器警报显示许可证服务器发送的警报以及解决警报所需执行的操作。需要许可证服务器 11.12.1 或更高版本。 • Delivery Controller 警报显示向 Controller 显示的以及 Controller 发送的许可状态的详细信息。需要适用于 XenApp 7.6 或 XenDesktop 7.6 或更高版本的 Controller。 可以在 Studio 中设置警报的阈值。
已连接的会话	过去 60 分钟所有交付组中已连接的会话。
平均登录时长	过去 60 分钟的登录数据。左侧的大数值表示该小时内的平均登录持续时间。 此平均值中不包括 XenDesktop 7.0 之前版本的 VDA 的登录数据。 有关详细信息，请参阅诊断用户登录问题。
基础结构	列出站点的基础结构 – 主机和 Controller。 对于 XenServer 或 VMware 中的基础结构，可以查看性能警报。 例如，可以将 XenCenter 配置为在某个托管服务器或虚拟机的 CPU、网络 I/O 或磁盘 I/O 超过特定阈值时生成性能警报。默认情况下，警报重复时间间隔是 60 分钟，但您也可以配置此时间间隔。有关详细信息，请参阅《Citrix XenServer 7.0 管理员指南》中的“XenCenter 性能警报”。

注意：如果未显示某特定指标的图标，则表明您所使用的主机类型不支持该指标。例如，不提供 System Center Virtual Machine Manager (SCVMM) 主机、AWS 和 CloudStack 的运行状况信息。
继续使用以下选项（见下文）对问题进行故障排除：

- 控制用户计算机电源
- 阻止与计算机连接

如果会话断开连接，它将继续处于活动状态，其应用程序仍会运行，但用户设备将不再与该服务器通信。

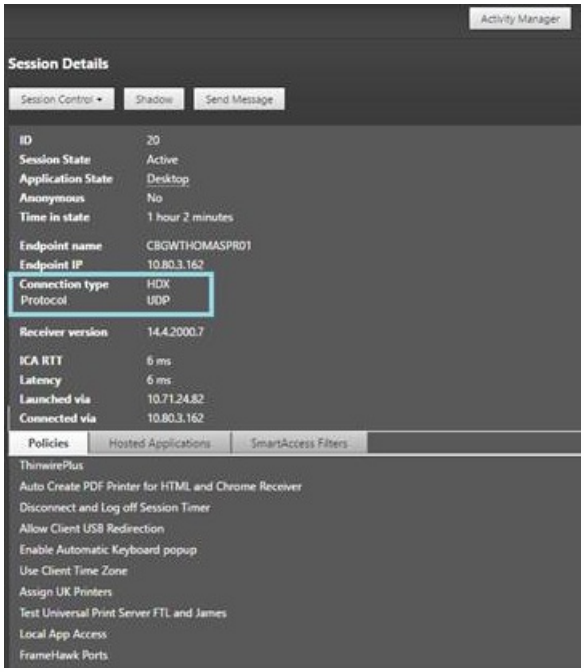
操作	说明
查看用户当前连接的计算机或会话	在“活动管理器”和“用户详细信息”视图中，查看用户当前连接的计算机或会话，以及

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	该用户有权访问的所有计算机和会话的列表。要访问此列表，请单击用户标题栏中的会话切换程序图标。有关详细信息，请参阅还原会话。
查看跨所有交付组的连接会话总数	从控制板的已连接的会话窗格中，查看最后 60 分钟内跨所有交付组的连接会话总数。然后单击较大的总数，打开过滤器视图，您可在其中根据所选交付组及跨交付组的范围和使用情况显示图形会话数据。
结束空闲会话	“会话过滤器”视图中显示与所有活动会话相关的数据。可根据关联用户、交付组、会话状态和大于某个阈值时间段的空闲时间来过滤会话。从过滤的列表中，选择要注销或断开连接的会话。有关详细信息，请参阅应用程序故障排除。
查看更长时间段内的数据	在“趋势”视图上，选择“会话”选项卡，逐级浏览更长时间段内连接和断开连接的会话更为具体的使用数据（即最后 60 分钟之前的会话总数）。要查看此信息，请单击“查看历史趋势”

注意：如果用户设备运行的是旧版的 Virtual Delivery Agent (VDA)，例如版本 7 以前的 VDA 或 Linux VDA，Director 将无法显示有关会话的完整信息。相反，它会显示指出信息不可用的消息。

在“会话详细信息”面板中查看当前会话中用于 HDX 连接类型的传输协议。对于在 VDA 7.13 版或更高版本上启动的会话，提供此信息。



- 对于 **HDX** 连接类型，
  - 如果 EDT 用于 HDX 连接，协议显示为 **UDP**。
  - 如果 TCP 用于 HDX 连接，协议显示为 **TCP**。
- 对于 **RDP** 连接类型，协议显示为**不适用**。

配置了自适应传输时，会话传输协议根据网络状况在 EDT（基于 UDP）与 TCP 之间动态切换。如果无法使用 EDT 建立 HDX

© 1999-2017 Citrix Systems, Inc. All rights reserved.

会话，则回退到 TCP 协议。

有关自适应传输配置的详细信息，请参阅自适应传输。

在控制板上单击数字或从过滤器菜单选择一个预定义的过滤器时，过滤器视图将打开，并根据选择的计算机或故障类型显示数据。

无法编辑预定义过滤器，但是可以将其保存为自定义过滤器，然后再进行修改。此外，可以跨所有交付组创建计算机、连接、会话和应用程序实例的自定义过滤视图。

1. 选择视图：
   - **计算机**。选择桌面操作系统计算机或服务器操作系统计算机。这些视图显示了已配置计算机的数量。“服务器操作系统计算机”选项卡还包括负载评估器指数，如果将鼠标悬停在链接上，则会指示性能计数器的分布情况和会话计数的工具提示。
   - **回话**。还可以从“会话”视图中查看会话计数。空闲时间度量值用于识别空闲时间超过阈值时间段的会话。
   - **连接**。按不同时间段显示的过滤连接，包括过去 60 分钟、过去 24 小时或过去 7 天。
   - **应用程序实例**此视图显示服务器和桌面操作系统的 VDA 上所有应用程序实例的属性。会话空闲时间度量值可用于服务器操作系统的 VDA 上的应用程序实例。
2. 对于**过滤依据**，请选择条件。
3. 根据需要，对每个视图使用其他选项卡以完成过滤。
4. 根据需要，选择其他列以执行进一步的故障排除。
5. 保存并命名过滤器。
6. 要从多台 Director 服务器访问过滤器，请将过滤器存储在可从那些服务器访问的共享文件夹中：
   - Director 服务器上的帐户对该共享文件夹必须具有修改权限。
   - 必须对 Director 服务器进行配置以便访问该共享文件夹。为此，请运行 IIS Manager。在 Sites > Default Web Site > Director > Application Settings（站点 > 默认 Web 站点 > Director > 应用程序设置）中，修改 Service.UserSettingsPath 设置以反映共享文件夹的 UNC 路径。
7. 以后要打开过滤器，请从“过滤器”菜单中选择过滤器类型（计算机、会话、连接或应用程序实例），然后选择保存的过滤器。
8. 如有需要，对于**计算机**或**连接**视图，请为在过滤列表中选择的所有计算机使用电源控制。对于“会话”视图，使用会话控制或消息发送选项。
9. 在**计算机**视图和**连接**视图中，单击故障计算机或失败连接的**故障原因**以获取有关故障的详细说明以及排除故障的建议操作。Citrix Director 7.12 Failure Reasons Troubleshooting Guide（《Citrix Director 7.12 故障原因排除指南》）中提供了计算机故障和连接失败的故障/失败原因和建议的操作。
10. 在**计算机**视图中，单击计算机名称链接转到相应的**计算机详细信息**页面。此页面显示计算机的详细信息、提供电源控制、显示 CPU、内存、磁盘监视以及 GPU 监视图。此外，单击**查看历史利用率**可查看计算机的资源利用率趋势。有关详细信息，请参阅计算机故障排除。
11. 在**应用程序实例**视图中，可根据大于某个阈值时间段的**空闲时间**进行排序或过滤。选择要结束的空闲应用程序实例。注销或断开连接应用程序实例会结束在同一会话中的所有活动应用程序实例。有关详细信息，请参阅应用程序故障排除。
    注意：如果 Director、Delivery Controller 和 VDA 是 7.13 版或更高版本，则提供应用程序实例过滤页面和会话过滤页面上的空闲时间度量值。

“趋势”视图提供每个站点的会话、连接故障、计算机故障、登录性能、负载评估、容量管理、计算机使用情况、资源利用率以及网络分析的历史趋势信息。要查找此信息，请单击**趋势**菜单。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

借助放大明细功能，您可以通过放大时间段（单击图中的数据点）和不断细分来导航浏览趋势图，以查看与趋势关联的详细信息。借助此功能，您可以更好地详细了解所显示的趋势影响了哪些人员或哪些方面。

要更改每个图形的默认作用域，请对数据应用其他过滤器。

选择您要获取历史趋势信息的时间段；时间段可用情况取决于您的 Director 部署，如下所示：

- 在获得 Platinum 许可的站点中，提供最多去年（365 天）的趋势报告。
- 在获得 Enterprise 许可的站点中，提供最多上个月（31 天）的趋势报告。
- 在未获得 Platinum 许可和未获得 Enterprise 许可的站点中，提供最多过去 7 天的趋势报告。

注意：

- 在所有 Director 部署中，时间段设置为“上个月”（**截至现在**）或更短的时间时，会话、故障和登录性能趋势信息以图形和表格的形式提供。选择时间段“上个月”（带有自定义结束日期）或“去年”时，趋势信息将以图形的形式提供，而不是表格。
- Monitoring Service 使用的趋势数据整理保留期限的默认值在数据粒度和保留中提供。获得 Platinum 许可的站点上的客户可以将整理保留期限更改为其所需的保留天数。

操作	说明
查看会话的趋势	从“会话”选项卡，选择“交付组”和时间段以查看关于并发会话计数的详细信息。
查看连接故障的趋势	在“故障”选项卡中，选择连接、计算机类型、故障类型、交付组和时间段，以查看包含有关站点中用户连接故障的更多详细信息的图形。
查看计算机故障的趋势	在“桌面操作系统计算机故障”选项卡或“服务器操作系统计算机”选项卡中，选择故障类型、交付组和时间段，以查看包含有关站点中计算机故障的更多详细信息的图形。
查看登录性能的趋势	在“登录性能”选项卡中，选择交付组和时间段，以查看包含有关站点中用户登录次数的持续时间以及登录次数是否影响性能的更多详细信息的图形。此视图还显示各个登录时期的平均持续时间，例如代理持续时间和 VM 启动时间。 此数据特别针对用户登录，不包括尝试重新连接已断开会话连接的用户。 图下方的表格显示了“登录持续时间(按用户会话)”。您可以选择要显示的列，并按任何列对报告进行排序。 有关详细信息，请参阅诊断用户登录问题。
查看负载评估的趋势	从“负载评估器指数”选项卡，查看包含负载在服务器操作系统计算机之间分发情况的更多详细信息的图表。此图表的过滤选项包括交付组或交付组中的服务器操作系统计算机、服务器操作系统计算机（仅当选择了交付组中的服务器操作系统计算机时才可用）和范围。
查看托管应用程序使用情况	此功能的可用性取决于组织的许可证。 从“容量管理”选项卡，选择“托管应用程序使用情况”选项卡，选择交付组和时间段，以查看一个显示最大并发使用情况的图和一个显示基于应用程序的使用情况的表。从“基于应用程序的使用情况”表格中，可以选择特定应用程序以查看详细信息和正在使用或曾经使

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	用此应用程序的用户列表。
查看桌面和服务器操作系统使用情况	“趋势”视图按站点和交付组显示桌面操作系统的使用情况。选择站点时，使用情况按交付组显示。选择交付组时，使用情况按用户显示。 “趋势”视图还按站点、交付组和计算机显示服务器操作系统的使用情况。选择站点时，使用情况按交付组显示。选择交付组时，使用情况分别按计算机和用户显示。选择计算机时，使用情况按用户显示。
查看虚拟机使用情况	在“计算机使用情况”选项卡中，选择“桌面操作系统计算机”或“服务器操作系统计算机”以获取 VM 使用情况的实时视图，以便能够快速评估您的站点的容量需求。 桌面操作系统可用性 - 根据可用性显示整个站点或特定交付组的桌面操作系统计算机 (VDI) 的当前状态。 服务器操作系统可用性 - 根据可用性显示整个站点或特定交付组的服务器操作系统计算机的当前状态。
查看资源利用率	在“资源利用率”选项卡中，选择桌面操作系统计算机或服务器操作系统计算机以获取有关每个 VDI 计算机的 CPU 和内存使用情况以及 IOPS 和磁盘延迟的历史趋势数据分析，从而更好地实现容量规划。 此功能需要 Delivery Controller 和 VDA **7.11 版**或更高版本。 图形会显示平均 CPU、平均内存、平均 IOPS、磁盘延迟和峰值并发会话的数据。您可以深入了解计算机，查看 CPU 占用排名前 10 的进程的数据和图表。按交付组和时间段过滤。提供过去 2 小时、24 小时、7 天、上个月和上一年的 CPU、内存使用情况和峰值并发会话图形。提供过去 24 小时、上个月和上一年的平均 IOPS 和磁盘延迟图形。 **注意**： • 必须将监视策略设置启用进程监视设置为“允许”以在“历史计算机利用率”页面上“排名前 10 的进程”表中收集并显示数据。默认情况下，该策略设置为“禁止”。 • 默认情况下会收集所有资源利用率数据。可以使用启用资源监视策略设置禁用此行为。 图形下方的表格显示每台计算机的资源利用率数据。 **注意**： 平均 IOPS 显示的是每日平均值。峰值 IOPS 的计算方式为取选定时间范围的 IOPS 平均值的最高值。（IOPS 平均值是在 VDA 上一个小时中收集的每小时 IOPS 平均值。）
查看网络分析数据	**注意**：此功能的可用性取决于组织的许可证和管理员权限。此功能需要 Delivery Controller **7.11 版**或更高版本。 在“网络”选项卡中，监视您的网络分析，其中提供网络的用户、应用程序和桌面上下文视图。在本版本中，Director 通过 NetScaler Insight Center or NetScaler MAS 中的 HDX Insight 报告提供您的部署中的 ICA 通信的高级分析。有关详细信息，请参阅配置网络分析。
	“应用程序故障”选项卡显示与 VDA 上已发布的应用程序关联的故障。 **注意**：此功能要求 Delivery Controller 和 VDA 7.15 或更高版本。支持运行 Windows Vista 及更高版本的桌面操作系统 VDA 以及运行 Windows Server 2008 及更高版本的服

© 1999-2017 Citrix Systems, Inc. All rights reserved.

查看应用程序故障	务器操作系统 VDA。 有关详细信息，请参阅“对应用程序进行故障排除”中的历史应用程序故障监视。 默认情况下，仅显示服务器操作系统 VDA 中的应用程序故障。可以使用“监视”策略设置应用程序故障的监视。有关详细信息，请参阅监视策略设置。
创建自定义报告	“自定义报告”选项卡中提供一个用户界面，用于以表格形式生成包含来自监视数据库的实时数据和历史数据的自定义报告。 **注意：**此功能需要 Delivery Controller 7.12 或更高版本。 从以前保存的自定义报告查询列表中，可以单击**执行**来导出 CSV 格式的报告、单击**复制 OData** 来复制和共享对应的 OData 查询，或单击**编辑**来编辑查询。 可以根据计算机、连接、会话或应用程序实例创建新的自定义报告查询。根据字段（例如，计算机、交付组或时间段）指定过滤条件。指定您的自定义报告中所需的其他列。预览显示报告数据示例。保存自定义报告查询会将其添加到保存的查询列表中。 可以根据复制的 OData 查询创建新的自定义报告查询。为此，请选择 OData 查询选项，并粘贴复制的 OData 查询。可以保存结果查询供以后执行。 **注意**使用 OData 查询生成的“Preview and Export”（预览和导出）报告中的列名未本地化，而是以英语显示。

图表上的旗帜图标表示此特定时间范围内的重要事件或操作。将鼠标悬停在旗帜上并单击时，可列出事件或操作。

注意：

- 对于版本 7 之前的 VDA 版本，不会收集 HDX 连接登录数据。对于更早版本的 VDA，图表数据将显示为 0。
- 可以在 Director 的“趋势”过滤器中选择在 Citrix Studio 中删除的交付组，直至清除与其相关的数据。选择已删除的交付组将显示未保留的可用数据的图表。但是，这些表格不显示数据。
- 将包含活动会话的计算机从一个交付组移至另一个交付组会导致新交付组的**资源利用率和负载评估器指数**表显示从新交付组和旧交付组合并的衡量指标。

您可以导出趋势数据以生成常规使用情况和容量管理报告。导出操作支持 PDF、Excel 和 CSV 报告格式。PDF 和 Excel 格式的报告包含以图表和表格表示的趋势。CSV 格式的报告包含表格数据，这种数据可以通过处理生成视图或进行存档。

要导出报告，请执行以下操作：

1. 转至**趋势**选项卡。
2. 设置过滤条件和时间段并单击**应用**。趋势图表和表格填充有数据。
3. 单击**导出**并输入报告的名称和格式。

Director 会根据您选择的过滤条件生成报告。如果更改了过滤条件，请单击**应用**，然后再单击**导出**。

注意：导出大量的数据时，会导致 Director 服务、Delivery Controller 和 SQL Server 中内存和 CPU 消耗大幅增加。支持的并发导出操作数和可以导出的数据量被设置为默认限制，以实现最佳的导出性能。

支持的导出限制

导出的 PDF 和 Excel 格式的报告包含满足选定过滤条件的完整图表。但是，超出对表格中的行数或记录数设置的默认限制的所有报告格式的表格数据都将被截断。默认的受支持记录数根据报告格式确定。

您可以通过在 Internet Information Services (IIS) 中配置 Director 应用程序设置的方法来更改默认限制。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

报告格式	默认的受支持记录数	Director 应用程序设置中的字段	最大的受支持记录数
PDF	500	UI.Export Pdf Drilldown Limit	5000
Excel	100,000	UI.Export Excel Drilldown Limit	100,000
CSV	100,000（在“会话”选项卡中为 10,000,000）	UI.Export Csv Drilldown Limit	100,000

要更改可以导出的记录数的限制，请执行以下操作：

1. 打开 IIS 管理器控制台。
2. 转到默认 Web 站点下的 Director Web 站点。
3. 双击**应用程序设置**。
4. 编辑字段或添加新的字段。

在“应用程序设置”中添加这些字段值，覆盖默认值。

警告：如果将字段值设置为高于最大的受支持记录数，可能会影响导出的性能，因此不建议这样操作。

错误处理

本节介绍有关处理在导出操作过程中可能遇到的错误的信息。

- **Director 超时**

  此错误出现的原因可能是网络问题，或者与 Director 服务器或 Monitor Service 的高资源使用率有关。

  默认的超时持续时间为 100 秒。要增加 Director 服务的超时持续时间，请在 Internet Information Services (IIS) 的 Director 应用程序设置中，设置 **Connector.DataServiceContext.Timeout** 字段的值：

  1. 打开 IIS 管理器控制台。

  2. 转到默认 Web 站点下的 Director Web 站点。

  3. 双击**应用程序设置**。

  4. 编辑 **Connector.DataServiceContext.Timeout** 的值。

- **显示器超时**

  此错误出现的原因可能是网络问题，或者与 Monitor Service 或 SQL Server 的高资源使用率有关。

  要增加 Monitor Service 的超时持续时间，请在 Delivery Controller 上运行以下 PowerShell 命令：



© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
asnp Citrix.*

Get-MonitorConfiguration

Set-MonitorConfiguration -MonitorQueryTimeoutSeconds <timeout value>
```

- **正在进行最大并发导出或预览操作**

  Director 支持一个导出或预览实例。如果遇到**正在进行最大并发导出或预览操作**错误，请稍后再尝试下一个导出操作。

  虽然可以增加并发导出或预览操作数，但 Director 的性能会受到影响，因此不建议这样做：

  1. 打开 IIS 管理器控制台。
  2. 转到默认 Web 站点下的 Director Web 站点。
  3. 双击**应用程序设置**。
  4. 编辑 **UI.ConcurrentExportLimit** 的值。

- **Director 中的磁盘空间不足**

  每个导出操作最多需要 Windows Temp 文件夹提供 2GB 的硬盘空间。清理空间后再尝试导出，或者在 Director 服务器上添加更多的硬盘空间。

要查看安装在特定计算机 VDA（物理或 VM）上的修补程序，请选择 计算机详细信息视图。

要对您在 Director 中选择的计算机状态进行控制，请使用电源控制选项。这些选项对桌面操作系统计算机可用，但可能对服务器操作系统计算机不可用。

注意：对于物理机或使用 Remote PC Access 的计算机，此功能不可用。

命令	函数
重新启动	对 VM 执行顺序（软）关闭。在重新启动 VM 前，所有正在运行的进程将逐一停止。例如，选择 Director 中显示为“启动失败”的计算机，并使用此命令重新启动这些计算机。
强制重新启动	在不预先执行任何关闭程序的情况下重新启动 VM。此命令与拔出然后插好物理服务器，并再次启动该服务器时作用相同。
关闭	对 VM 执行顺序（软）关闭；所有运行的进程将分别停止。
强制关闭	在不预先执行任何关闭程序的情况下关闭 VM。此命令与拔出物理服务器时作用相同。强制关闭可能不会始终关闭所有正在运行的进程，如果用这种方式关闭 VM，可能会有丢失数据的风险。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

命令 挂起	函数 将处在运行的 VM 挂起在其当前状态，并将此状态保存在默认存储库中的某个文件里。此选项可让您关闭 VM 的主机服务器，在重新启动后恢复 VM，从而将其还原到原始运行状态。
恢复	恢复挂起的 VM 并还原其原始运行状态。
开始	在 VM 关闭后启动（也称为冷启动）。

如果电源控制操作失败，请将鼠标悬停在警报上，此时将显示一条弹出消息，其中包含有关故障的详细信息。

在相应的管理员执行映像维护任务时，使用维护模式临时阻止新连接。

在计算机上启用维护模式后，将不允许新连接，直到禁用该模式。如果用户已登录，维护模式将在所有用户注销后生效。对于未注销的用户，请发送一条消息，通知他们计算机将在某个特定时间关闭，并使用电源控制项强制关闭计算机。

1. 从用户详细信息视图选择计算机，或在过滤器视图中选择一组计算机。
2. 选择维护模式，然后打开选项。

如果用户尝试连接到分配的桌面但此桌面处于维护模式，将显示一条消息，指示此桌面当前不可用。无法进行新连接，直到您禁用维护模式。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

警报和通知

Dec 05, 2017

在本文中：

监视警报

创建警报策略

警报策略条件

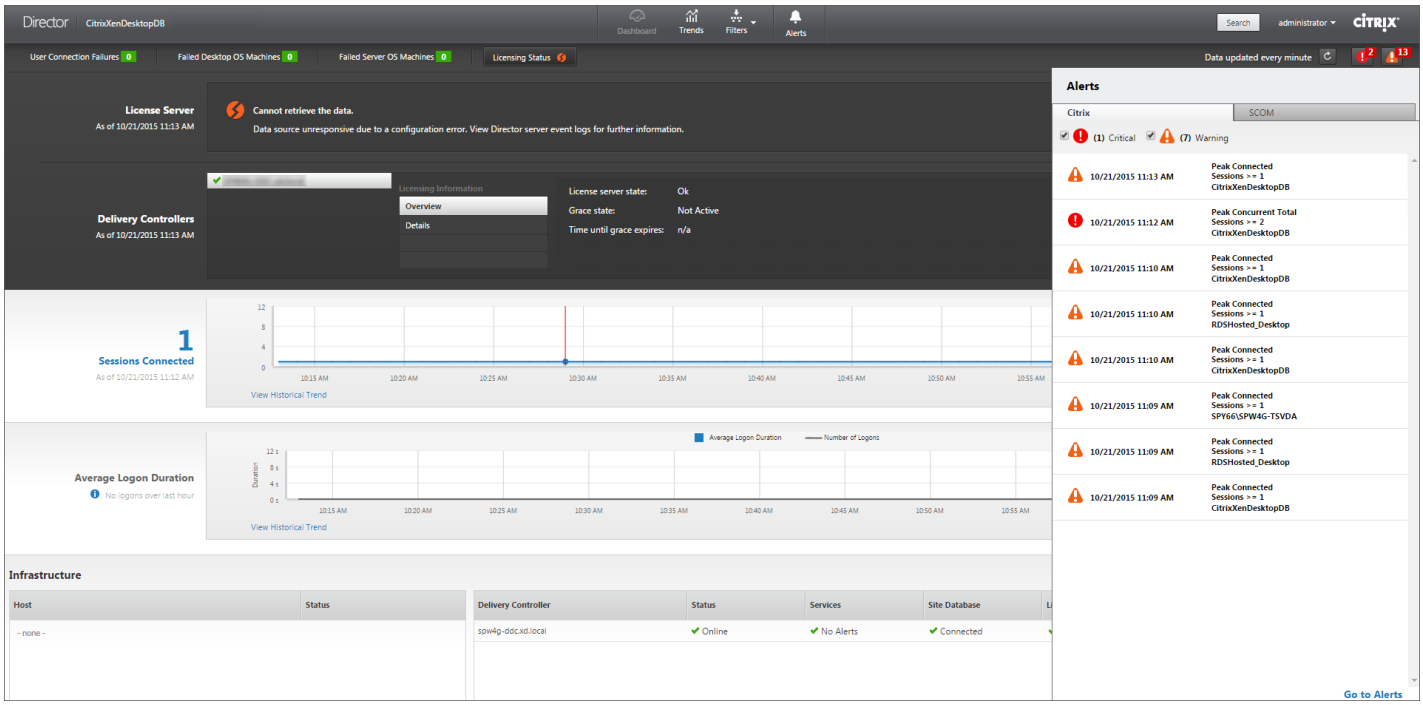
使用 Octoblu webhook 配置警报策略

使用 SNMP 陷阱配置警报策略

SCOM 警报

配置 SCOM 集成

警报在 Director 中的控制板上以及其他高级别视图中显示，带有警告和严重警报符号。警报适用于获得 Platinum 许可的站点。警报每分钟自动更新一次；也可以根据需要更新警报。



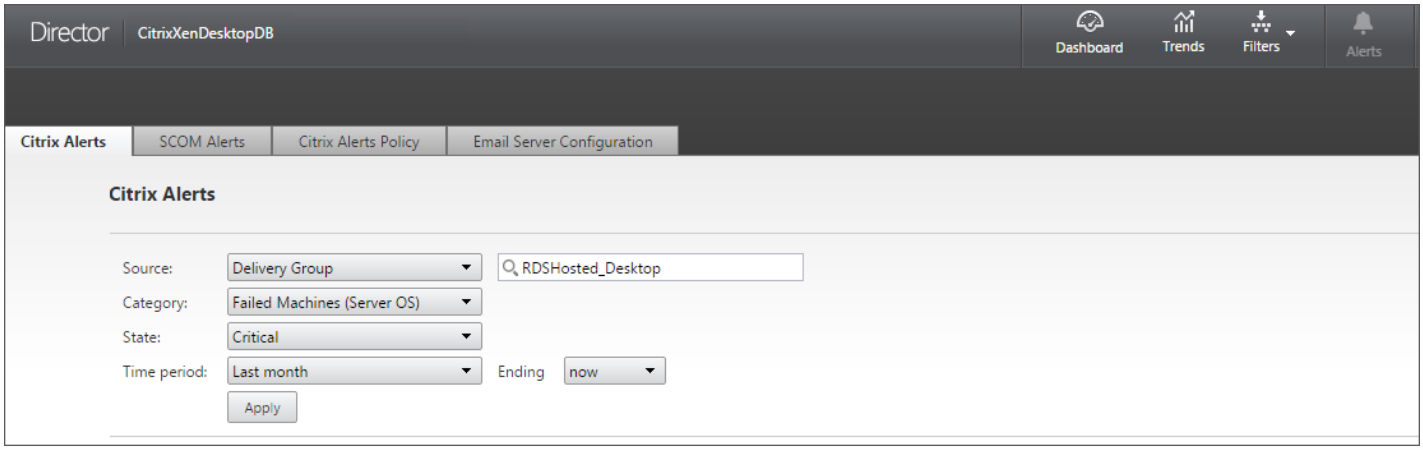
警告警报（琥珀色三角形）指示已达到或超过条件的警告阈值。

严重警报（红色圆形）显示已达到或超过条件的严重阈值。

可以查看与警报有关的更加详细的信息，方法是从边栏中选择警报，单击边栏底部的**转至“警报”**链接，或者在 Director 页面顶部选择**警报**。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

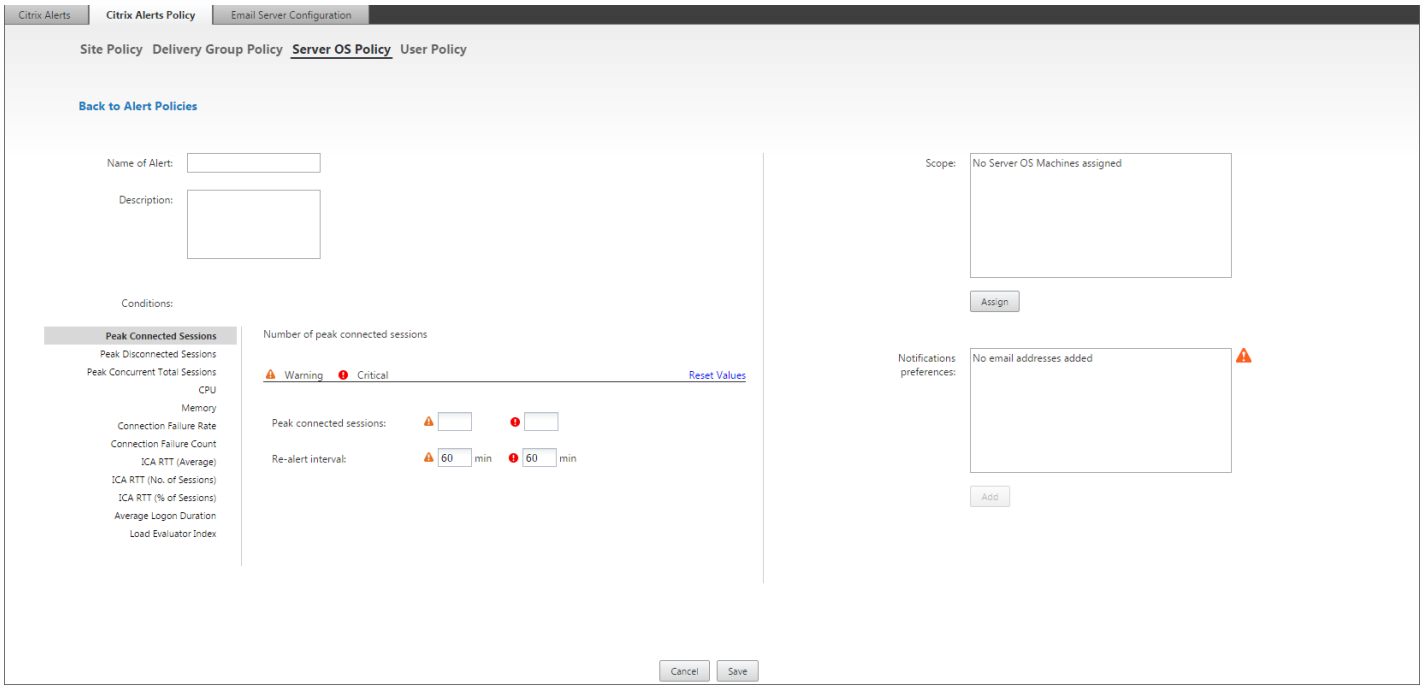
在“警报”视图中，可以过滤和导出警报。例如，上个月中针对特定交付组的出现故障的服务器操作系统计算机，或针对特定用户的所有警报。有关详细信息，请参阅导出报告。



Citrix 警报。Citrix 警报是指在 Director 中监视且源自 Citrix 组件的警报。可以在 Director 内部的**警报** > **Citrix 警报策略**中配置 Citrix 警报。作为配置的一部分，可以设置要在警报超出所设置的阈值时通过电子邮件向个人和组发送的通知。还可以将通知配置为 Octoblu webhook 或 SNMP 陷阱。有关设置 Citrix 警报的详细信息，请参阅创建警报策略。

SCOM 警报。SCOM 警报显示来自 Microsoft System Center 2012 Operations Manager (SCOM) 的警报信息，以在 Director 内部提供更具综合性的数据中心运行状况和性能指标。有关详细信息，请参阅 SCOM 警报。

展开边栏之前在警报图标旁边显示的警报数量是 Citrix 警报和 SCOM 警报的总和。



创建新警报策略，例如，在满足一组特定会话计数条件时生成警报：

1. 转至**警报** > **Citrix 警报策略**，然后选择“服务器操作系统策略”（例如）。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. 单击**创建**。
3. 命名并描述该策略，然后设置触发警报时必须满足的条件。例如，指定“最大已连接会话数”、“最大已断开会话数”和“最大并发会话总数”对应的警告和严重警报数。警告值不得大于严重警报值。有关详细信息，请参阅警报策略条件。
4. 设置重新发出警报的时间间隔。如果仍满足警报的条件，则在达到此时间间隔时会再次出发警报，如果在警报策略中设置了此时间间隔，则会生成电子邮件通知。已消除的警报在达到重新发出警报的时间间隔时不生成电子邮件通知。
5. 设置作用域。例如，为特定交付组进行设置。
6. 在“通知”首选项中，指定触发警报时应通过电子邮件向哪些用户发送通知。必须在**电子邮件服务器配置**选项卡中指定电子邮件服务器，才能在“警报策略”中设置电子邮件通知首选项。
7. 单击**保存**。

有关 Octoblu webhook 配置的信息，请参阅使用 Octoblu webhook 配置警报策略。

有关 SNMP 陷阱配置的信息，请参阅使用 SNMP 陷阱配置警报策略。

创建一条包含在作用域中定义的 20 个或更多交付组的策略大约需要 30 秒才能完成配置。此时将显示一个微调器。

如果为最多 20 个不同的交付组创建 50 多个策略（共 1000 个交付组目标），可能会导致响应时间增加（超过 5 秒）。

将包含活动会话的计算机从一个交付组移至另一个交付组可能会触发使用计算机参数定义的错误交付组警报。

警报策略条件	**说明和建议执行的操作**
最大已连接会话数	最大已连接的会话数。 • 查看 Director 的“会话趋势”视图，获取最大已连接会话数。 • 检查以确保容量足以容纳会话负载。 • 根据需要添加新计算机。
最大已断开会话数	最大已断开连接的会话数。 • 查看 Director 的“会话趋势”视图，获取最大已断开会话数。 • 检查以确保容量足以容纳会话负载。 • 根据需要添加新计算机。 • 根据需要注销断开的会话。
最大并发会话总数	最大并发会话总数。 • 查看 Director 中的 Director“会话趋势”视图，获取最大并发会话总数。 • 检查以确保容量足以容纳会话负载。 • 根据需要添加新计算机。 • 根据需要注销断开的会话。
	CPU 使用率百分比。 • 确定消耗 CPU 的进程或资源。 • 必要时结束进程。结束进程会导致未保存的数据丢失。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

CPU	• 如果一切均正常工作，请以后再添加其他 CPU 资源。 **注意**：在具有 VDA 的计算机上，默认会允许使用**启用资源监视**策略设置，以监视 CPU 和内存性能计数器。如果禁用此策略设置，则不会触发 CPU 和内存状况警报。有关详细信息，请参阅监视策略设置。
内存	内存使用率百分比。 • 确定消耗内存的进程或资源。 • 必要时结束进程。结束进程会导致未保存的数据丢失。 • 如果一切均正常工作，请以后再添加其他内存。 **注意**：在具有 VDA 的计算机上，默认会允许使用**启用资源监视**策略设置，以监视 CPU 和内存性能计数器。如果禁用此策略设置，则不会触发 CPU 和内存状况警报。有关详细信息，请参阅监视策略设置。
连接失败率	过去一小时内连接失败的百分比。根据失败总次数除以尝试连接的总次数计算得来。 • 检查 Director 的“连接失败趋势”视图，了解配置日志中记录的事件。 • 确定桌面或应用程序是否可访问。
连接失败次数	过去一小时内连接失败的次数。 • 检查 Director 的“连接失败趋势”视图，了解配置日志中记录的事件。 • 确定桌面或应用程序是否可访问。
ICA RTT（平均值）	平均 ICA 往返时间。 • 检查 NetScaler HDX Insight 或 MAS，获取 ICA RTT 中的故障信息以确定根本原因。有关详细信息，请参阅 NetScaler Insight Center - HDX Insight 或 NetScaler MAS - Analytics: HDX Insight 文档。 • 如果 NetScaler 不可用，请检查“Director 用户详细信息”视图以获取 ICA RTT 和延迟信息，并确定是网络问题还是 XenApp 和 XenDesktop 问题。
ICA RTT（会话数）	超过 ICA 往返时间阈值的会话数。 • 检查 NetScaler HDX Insight 或 MAS 以获取具有高 ICA RTT 的会话数。有关详细信息，请参阅 NetScaler Insight Center - HDX Insight 或 NetScaler MAS - Analytics: HDX Insight 文档。 • 如果 NetScaler 不可用，请与网络团队协作共同确定根本原因。
ICA RTT（会话百分比）	超过平均 ICA 往返时间的会话百分比。 • 检查 NetScaler HDX Insight 或 MAS 以获取具有高 ICA RTT 的会话数。有关详细信息，请参阅 NetScaler Insight Center - HDX Insight 或 NetScaler MAS - Analytics: HDX Insight 文档。 • 如果 NetScaler 不可用，请与网络团队协作共同确定根本原因。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ICA RTT（用户）	应用于由指定用户启动的会话的 ICA 往返时间。如果 ICA RTT 高于至少一个会话中的阈值，则会触发该警报。
出现故障的计算机数(桌面操作系统)	出现故障的桌面操作系统计算机数。 • 可能会因多种原因而出现故障，如在 Director 的“控制板”和“过滤器”视图中所示。请运行 Citrix Scout 诊断以确定根本原因。有关详细信息，请参阅对用户问题进行故障排除。
出现故障的计算机数(服务器操作系统)	出现故障的服务器操作系统计算机数。 • 可能会因多种原因而出现故障，如在 Director 的“控制板”和“过滤器”视图中所示。请运行 Citrix Scout 诊断以确定根本原因。
平均登录时长	过去一小时内的登录的平均登录时长。 • 查看 Director 的“控制板”，获取与登录时长有关的最新指标。大量用户在短时间内登录会延长登录持续时间。 • 请查看登录的基准时间和中断时间，以缩小原因范围。 有关详细信息，请参阅诊断用户登录问题。
登录时长(用户)	过去一小时内发生的指定用户的登录的登录时长。
负载评估器指数	过去 5 分钟内负载评估器指数的值。 • 查看 Director 中可能具有峰值负载（最大负载）的服务器操作系统计算机。 • 查看“控制板”（失败）和“趋势负载评估器指数”报告。

除了电子邮件通知，您还可以使用 Octoblu webhook 配置警报策略，以启动 IoT 服务。

注意：此功能需要 Delivery Controller 7.11 版或更高版本。

可以利用警报的 IoT 服务示例包括向支持人员发送 SMS 通知，或与自定义事件解决平台集成以帮助跟踪通知。

可以使用 PowerShell cmdlet 配置采用 HTTP 回调或 HTTP POST 的警报策略。它们已扩展，可以支持 webhook。

有关创建新 Octoblu 工作流和获取对应的 webhook URL 的信息，请参阅 Octoblu Developer Hub。

要为新的警报策略或现有的策略配置 Octoblu webhook URL，请使用以下 PowerShell cmdlet。

使用 webhook URL 创建新警报策略：



© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -Description <Policy description> -Enabled $true -Webhook <Webhook UR
```

将 webhook URL 添加到现有的警报策略：

```
Set-MonitorNotificationPolicy - Uid <Policy id> -Webhook <Webhook URL>
```

有关 PowerShell 命令的帮助，请使用 PowerShell 帮助，例如：

```
Get-Help  <Set-MonitorNotificationPolicy>
```

有关使用 PowerShell 配置警报策略的详细信息，请参阅“高级概念”中的 Director 7.7：使用 Powershell 管理和配置警报与通知。

警报策略生成的通知会触发 webhook，同时向 webhook URL 发出 POST 调用。该 POST 消息包含 JSON 格式的通知消息：

{"NotificationId" : <通知 Id>,

"Target" : <通知目标 Id>,

"Condition" : <违反的条件>,

"Value" : <条件的阈值>,

"Timestamp": <通知生成时的 UTC 时间>,

"PolicyName": <警报策略的名称>,

"Description": <警报策略的说明>,

"Scope" : <警报策略的作用域>,

"NotificationState": <通知状态为严重、警告、正常或已消除>,

"Site" : <站点名称>}

© 1999-2017 Citrix Systems, Inc. All rights reserved.

触发使用 SNMP 陷阱配置的警报时，对应的 SNMP 陷阱消息会转发至配置的网络侦听器以做进一步处理。Citrix 警报支持 SNMP 版本 2 及更高版本的陷阱。当前，陷阱消息可以转发至一个侦听器。

注意：此功能需要 Delivery Controller 7.12 版或更高版本。

要配置 SNMP 陷阱，请使用以下 PowerShell cmdlet：

- 获取当前 SNMP 服务器配置：

```
Get-MonitorNotificationSnmpServerConfiguration
```

- 为 SNMP 版本 2 设置服务器配置：

```
Set-MonitorNotificationSnmpServerConfiguration -ServerName <Server IP> -PortNumber <Port ID> -SnmpSender <Sender name> -Com
```

- 为 SNMP 版本 3 设置服务器配置：

```
$authpass = "<authentication password>" | ConvertTo-SecureString -AsPlainText -Force

$privpass = "<Privacy password>" | ConvertTo-SecureString -AsPlainText -Force

Set-MonitorNotificationSnmpServerConfiguration -ServerName <Server IP> -PortNumber <Port ID> -SnmpSender <Sender name> -Engi
```

- 为现有警报策略启用 SNMP 陷阱：

```
Set-MonitorNotificationPolicy -IsSnmpEnabled $true -Uid <Policy ID>
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 使用 SNMP 陷阱配置创建新警报策略：

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -IsSnmpEnabled $true -Description <Policy description> -Enabled $true
```

来自 Director 的 SNMP 陷阱消息中的 OID 的结构如下：
1.3.6.1.4.1.3845.100.1.
其中， 是依次为在 Director 中定义的每个警报策略生成的。因此，OID 对每个用户环境都是唯一的。

- 使用 1.3.6.1.4.1.3845.100.1 可过滤来自 Director 的所有陷阱消息。
- 使用 1.3.6.1.4.1.3845.100.1. 可过滤和处理特定警报的陷阱消息。

使用以下 cmdlet 可获取您的环境中定义的警报策略的 UID：

```
Get-MonitorNotificationPolicy
```

可以将 SNMP 陷阱转发至 SCOM。为此，为 SCOM 配置 Delivery Controller 以侦听陷阱消息。

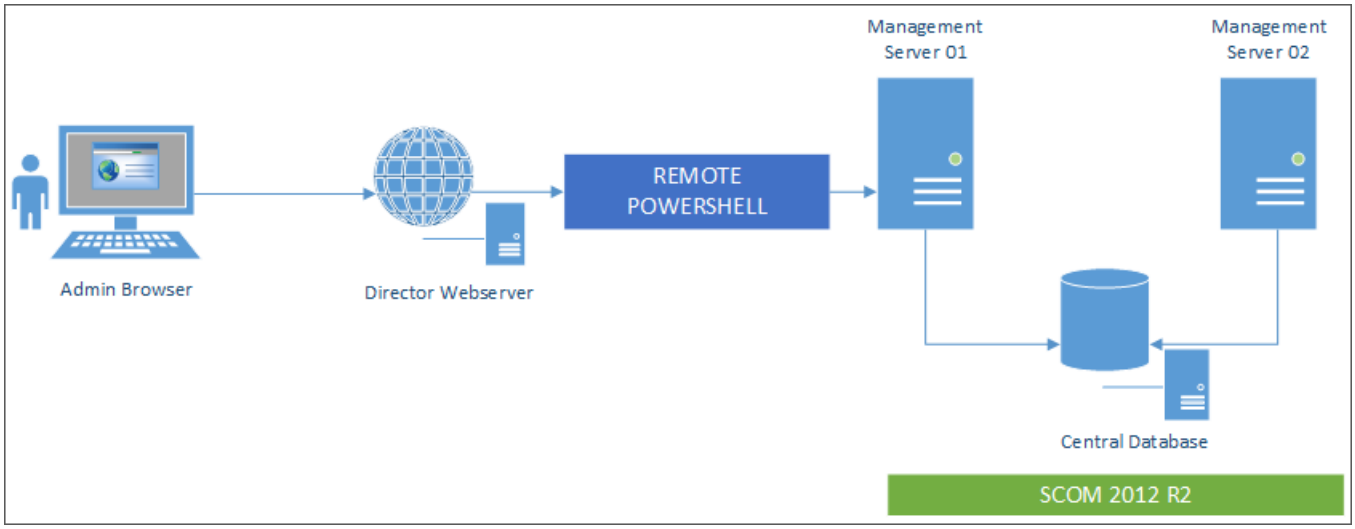
SCOM 与 Director 的集成允许您在 Director 中的“控制板”以及其他高级别视图中查看来自 SCOM 的警报信息。

SCOM 警报与 Citrix 警报一起在屏幕上显示。可以从边栏中的“SCOM”选项卡访问和进一步查看 SCOM 警报。

可以查看长达过去一个月内的历史警报、排序、过滤以及将过滤的信息导出为 CSV、Excel 和 PDF 报告格式。有关详细信息，请参阅导出报告。

SCOM 集成使用远程 PowerShell 3.0 或更高版本查询 SCOM 管理服务器中的数据，并维护用户的 Director 会话中的持续型运行空间连接。Director 和 SCOM 服务器必须具有相同的 PowerShell 版本。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



SCOM 集成的要求如下：

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager
- PowerShell 3.0 或更高版本（Director 和 SCOM 服务器上安装的 PowerShell 版本必须一致）
- 四核 CPU，16 GB RAM（建议）
- 必须在 Director web.config 文件中配置 SCOM 的主管理服务器。可以使用 DirectorConfig 工具进行配置。

注意：

- Citrix 建议您将 Director 管理员帐户配置为 SCOM 操作员角色，以便能够在 Director 中检索完整的警报信息。如果不可能，则可以使用 DirectorConfig 工具在 web.config 文件中配置 SCOM 管理员帐户。
- Citrix 建议您为每个 SCOM 管理服务器配置的 Director 管理员数量不要超过 10 个以确保性能最佳。

在 Director 服务器上执行以下操作：

1. 键入 **Enable-PSRemoting** 以启用 PowerShell 远程处理。

2. 将 SCOM 管理服务器添加到 TrustedHosts 列表中。打开 PowerShell 提示符并执行以下命令：

    a. 获取 TrustedHosts 的当前列表

```
Get-Item WSMAN:\localhost\Client\TrustedHosts
```

    b. 将 SCOM 管理服务器的 FQDN 添加到 TrustedHosts 列表中。<旧值> 表示 Get-Item cmdlet 返回的现有条目集。

```
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
Set-Item WSMAN:\localhost\Client\TrustedHosts -Value "<FQDN SCOM Management Server>,<Old Values>"
```

3. 使用 DirectorConfig 工具配置 SCOM。

```
C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configscom
```

在 SCOM 管理服务器上执行以下操作：

1. 将 Director 管理员分配给 SCOM 管理员角色。

    a. 打开 SCOM 管理控制台，转至**管理** > **安全** > **用户角色**。

    b. 在“用户角色”中，可以创建新用户角色或修改现有用户角色。有四种类型的 SCOM 操作员角色可用来定义对 SCOM 数据的访问性质。例如，具有只读权限的角色看不到“管理”窗格，无法发现或管理规则、计算机或帐户。操作员角色属于完全权限管理员角色。

    注意：如果将 Director 管理员分配给非操作员角色，以下操作将不可用。

        i. 如果配置了多个管理服务器，则当主管理服务器不可用时，Director 管理员将无法连接到辅助管理服务器。主管理服务器是指在 Director web.config 文件中配置的服务器，该服务器与在上述步骤 3 中通过 DirectorConfig 工具指定的服务器相同。辅助管理服务器是指主服务器的对等管理服务器。

        ii. 过滤警报时，Director 管理员无法搜索警报的来源。该操作需要操作员级别的权限。

    c. 要修改任何用户角色，请右键单击该角色，然后单击**属性**。

    d. 在“用户角色属性”对话框中，可以从指定的用户角色中添加或删除 Director 管理员。

2. 将 Director 管理员添加到 SCOM 管理服务器上的“远程管理用户”组。这允许 Director 管理员建立远程 PowerShell 连接。

3. 键入 **Enable-PSRemoting** 以启用 PowerShell 远程处理。

4. 设置 WS-Management 属性限制：

    a. 修改 MaxConcurrentUsers：

    在 CLI 中：

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
winrm set winrm/config/winrs @{MaxConcurrentUsers = "20"}
```

在 PS 中：

```
Set-Item WSMan:\localhost\Shell\MaxConcurrentUsers 20
```

b. 修改 MaxShellsPerUser：

在 CLI 中：

```
winrm set winrm/config/winrs @{MaxShellsPerUser="20"}
```

在 PS 中：

```
Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20
```

c. 修改 MaxMemoryPerShellMB：

在 CLI 中：

```
winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}
```

在 PS 中：

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
Set-Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 1024
```

5. 要确保 SCOM 集成在混合域环境中运行，请设置以下注册表项。

    路径：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

    注册表项：LocalAccountTokenFilterPolicy

    类型：DWord

    值：1

小心：注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因“注册表编辑器”使用不当导致出现的问题能够得以解决。使用“注册表编辑器”需自担风险。在编辑注册表之前，请务必进行备份。

设置 SCOM 集成后，系统可能会显示消息“无法获取最新的 SCOM 警报。有关详细信息，请查看 Director 服务器事件日志。”服务器事件日志将帮助您确定并更正问题。原因可能包括：

- Director 或 SCOM 计算机上的网络连接断开。
- SCOM 服务不可用或太忙，无法响应。
- 由于所配置的用户的权限发生变化，授权失败。
- 处理 SCOM 数据时 Director 中出现错误。
- Director 与 SCOM 服务器之间的 PowerShell 版本不一致。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

委派管理和 Director

Dec 05, 2017

委派管理基于三个概念：管理员、角色和作用域。权限基于管理员的角色以及该角色的作用域。例如，可以为管理员分配技术支持管理员角色，其作用域只包括负责一个站点上的最终用户。

有关创建委派管理员的信息，请参阅委派管理文档。

管理权限决定着向管理员呈现的 Director 界面以及他们可以执行的任务。 权限决定着以下事项：

- 用户可以访问的页面，统称为视图。
- 管理员可以查看并与之交互的桌面、计算机和会话。
- 管理员可以执行的命令，例如重影用户的会话或启用维护模式。

内置角色和权限还决定着管理员对 Director 的使用方式：

管理员角色	在 Director 中的权限
完全权限管理员	对所有视图具有完全访问权限，并且可以执行所有命令，包括重影用户的会话、启用维护模式和导出趋势数据。
交付组管理员	对所有视图具有完全访问权限，并且可以执行所有命令，包括重影用户的会话、启用维护模式和导出趋势数据。
只读权限管理员	可以访问所有视图并查看指定作用域中的所有对象，还可以查看全局信息。可以从 HDX 通道下载报告，并且可以使用“趋势”视图中的“导出”选项导出趋势数据。无法执行任何其他命令或在视图中进行任何更改。
技术支持管理员	只可以访问“技术支持”和“用户详细信息”视图，并且只可以查看委派管理员进行管理的对象。可以重影用户会话并为该用户执行命令。可以执行维护模式操作。可以对桌面操作系统计算机使用电源控制选项。无法访问控制板、“趋势”、“警告”或“过滤器”视图。无法对服务器操作系统计算机使用电源控制选项。
计算机目录管理员	无访问权限。Director 不支持此管理员，因此其无法查看数据。此用户可以访问“计算机详细信息”页面（基于计算机的搜索）。
主机管理员	无访问权限。Director 不支持此管理员，因此其无法查看数据。

配置 Director 管理员的自定义角色

© 1999-2017 Citrix Systems, Inc. All rights reserved.

在 Studio 中，还可以配置 Director 特定的自定义角色，以更好地满足组织的需求，并且更灵活地委派权限。 例如，您可以限制内置的技术支持管理员角色，使该管理员无法从会话注销。

如果通过 Director 权限创建一个自定义角色，还必须向该角色分配其他通用权限：

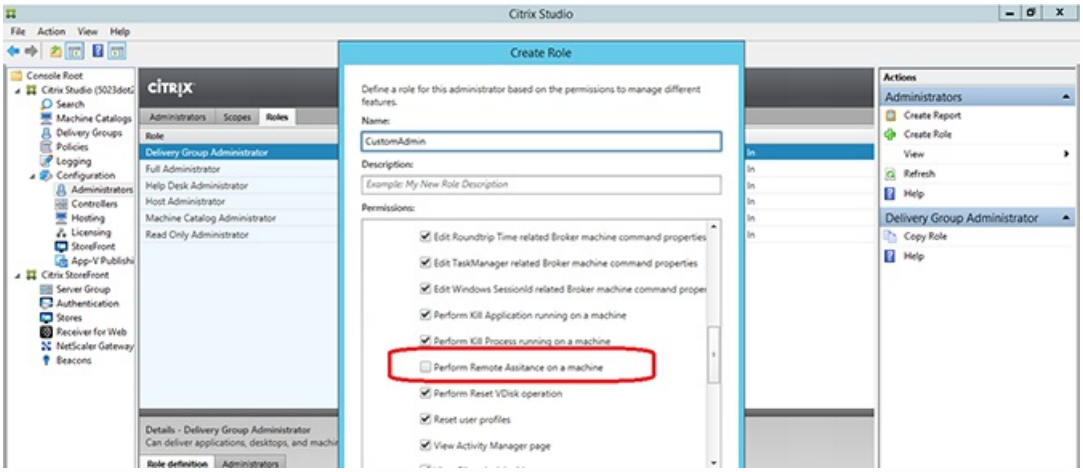
- Delivery Controller 登录 Director 的权限 - 至少需要管理员节点中的只读权限
- 用于查看与 Director 中的交付组相关的数据的交付组权限 - 至少需要只读权限

此外，还可以通过复制现有角色创建自定义角色，并包括不同视图的附加权限。 例如，可以复制技术支持角色并包括用于查看“控制板”或“过滤器”页面的权限。

为自定义角色选择 Director 权限，包括：

- 在计算机上执行终止应用程序的操作
- 在计算机上执行终止进程的操作
- 在计算机上执行远程协助
- 执行重置虚拟磁盘的操作
- 重置用户配置文件
- 查看“客户端详细信息”页面
- 查看控制板页
- 查看“过滤器”页面
- 查看“计算机详细信息”页面
- 查看“趋势”页面
- 查看“用户详细信息”页面

在此示例中，重影（在计算机上执行远程协助）关闭。



某种权限可以对其他权限具有依赖关系，以在用户界面上变得适用。例如，选择**在计算机上执行终止应用程序的操作**权限将仅在角色具有权限的面板中启用**结束应用程序**功能。可以选择以下面板权限：

- 查看“过滤器”页面
- 查看“用户详细信息”页面
- 查看“计算机详细信息”页面
- 查看“客户端详细信息”页面

另外，从其他组件的权限列表中，请考虑选择交付组中的以下权限：

- 使用交付组成员身份启用/禁用计算机的维护模式。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 使用交付组成员身份在 Windows 桌面计算机上执行电源操作。
- 使用交付组成员身份在计算机上执行会话管理。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

安全 Director 部署

Feb 01, 2018

本文重点介绍在部署和配置 Director 时可能会影响系统安全的几个方面。

可以配置具有受限 IIS 配置的 Director。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。

Director 要求在请求过滤中使用以下文件扩展名：

- .aspx
- .css
- .html
- .js
- .png
- .svc

Director 要求在请求过滤中使用以下 HTTP 谓词。可以不允许使用未列出的谓词。

- GET
- POST
- HEAD

Director 不需要以下各项：

- ISAPI 过滤器
- ISAPI 扩展
- CGI 程序
- FastCGI 程序

重要：

- Director 要求完全信任。请勿将全局 .NET 信任级别设置为“高”或更低。
- Director 维护独立的应用程序池。要修改 Director 的设置，请选择 Director 站点并进行修改。

安装 Director 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 Director 使用，并且自动禁用。

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 Director 与您的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 使用传输层安全性 (TLS) 协议

© 1999-2017 Citrix Systems, Inc. All rights reserved.

提供强大的数据加密。

注意：

- Citrix 强烈建议您不要在生产环境中启用指向 Director 的不安全连接。
- 来自 Director 的安全连接需要为每个连接单独配置。
- 不建议使用 SSL 协议。请改为使用更安全的 TLS 协议。
- 必须使用 TLS（而非 IPsec）保护与 NetScaler 的通信安全。

要保护 Director 与 XenApp 和 XenDesktop 服务器之间的通信安全（以实现监视和报告功能），请参阅 Data Access Security（数据访问安全性）。

要保护 Director 与 NetScaler 之间的通信安全（针对 NetScaler Insight），请参阅配置网络分析。

要保护 Director 与许可证服务器之间的通信安全，请参阅保护许可证管理控制台。

如果您在与 Director 相同的 Web 域（域名和端口均相同）中部署任何 Web 应用程序，这些 Web 应用程序中存在的任何安全风险都可能会潜在地降低 Director 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 Director。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

为 XenDesktop 7 之前版本的 VDA 配置权限

Dec 05, 2017

如果用户的 VDA 版本低于 XenDesktop 7，Director 会通过 Windows 远程管理 (WinRM) 从部署中补充有关实时状态和指标的信息。

此外，使用此过程配置 WinRM，使其能与 XenDesktop 5.6 Feature Pack1 中的 Remote PC 兼容使用。

默认情况下，只有桌面计算机的本地管理员（通常为域管理员及其他特权用户）才具有查看实时数据所需的权限。

有关安装并配置 WinRM 的信息，请参阅 CTX125243。

要使其他用户能够查看实时数据，必须向其授予相应权限。 例如，假定有多个 Director 用户（HelpDeskUserA、HelpDeskUserB 等等）同属于名为 HelpDeskUsers 的 Active Directory 安全组。 已在 Studio 中为该组指定了技术支持管理员角色，从而为这些用户提供了必需的 Delivery Controller 权限。 但该组还需要具有从桌面计算机访问实时数据所需的权限。

要提供所需的访问权限，可以通过以下两种方式之一配置必需的权限：

- 向 Director 用户授予权限（模拟模式）
- 向 Director 服务授予权限（可信子系统模式）

向 Director 用户授予权限（模拟 模式）

默认情况下，Director 使用模拟模式：WinRM 与桌面计算机之间通过 Director 用户身份进行连接。 因此，Desktop Director 用户必须在该台式机上具有相应的权限。

可以通过以下两种方式（本文档稍后会介绍）之一配置这些权限：

1. 将用户添加到桌面计算机的本地管理员组中。
2. 向用户授予 Director 所需的特定权限。 此选项避免了授予 Director 用户（例如，HelpDeskUsers 组）计算机上的完全管理权限。

向 Director 服务授予权限（可信子系统 模式）

可以对 Director 进行配置，使 WinRM 连接使用服务标识，并仅向该服务标识授予相应的权限，而无需向 Director 用户授予对桌面计算机的相应权限。

在此模式下，Director 用户本身将无权执行 WinRM 调用。 他们可以使用 Director 访问数据。

IIS 中的 Director 应用程序池配置为以服务标识方式运行。 默认情况下，这是 APPPOOL\Director 虚拟帐户。 执行远程连接时，此帐户将显示为服务器的 Active Directory 计算机帐户，例如 MyDomain\DirectorServer$。 必须将此帐户配置为具有相应权限。

如果部署了多个 Director Web 站点，则必须将每个 Web 服务器的计算机帐户都置于配置了相应权限的 Active Directory 安全组中。

要将 Director 设置为使用 WinRM 的服务标识而非用户身份，请按高级配置中所述配置以下设置：

```
Service.Connector.WinRM.Identity = Service
```

可以通过以下两种方式之一配置这些权限：

1. 将服务帐户添加到桌面计算机上的本地管理员组中。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. 向服务帐户授予 Director 所需的特定权限（如下文介绍）。 此选项可避免向服务帐户授予计算机的完全管理权限。

向特定用户或用户组分配权限

要使 Director 能够通过 WinRM 从桌面计算机访问所需的信息，需要具有以下权限：

- WinRM RootSDDL 中的读取和执行权限
- WMI 命名空间权限：
  - root/cimv2 - 远程访问权限
  - root/citrix - 远程访问权限
  - root/RSOP - 远程访问权限和执行权限
- 这些本地组的成员关系：
  - 性能监视用户
  - 事件日志读者

用于自动授予上述权限的 ConfigRemoteMgmt.exe 工具分别位于 x86\Virtual Desktop Agent 文件夹和 x64\Virtual Desktop Agent 文件夹中的安装介质上以及 C:\inetpub\wwwroot\Director\tools 文件夹中的安装介质上。必须向所有 Director 用户授予上述权限。

要向 Active Directory 安全组、用户和计算机帐户授予这些权限，或授予执行结束应用程序和结束进程操作的权限，使用管理权限从命令提示窗口运行此工具，并在运行时采用以下参数：

ConfigRemoteMgmt.exe /configwinrmuser domain\name
其中 name 为安全组、用户或计算机帐户。

要向某个用户安全组授予所需的权限，请运行：

ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers
要向特定计算机帐户授予权限，请运行：

ConfigRemoteMgmt.exe /configwinrmuser domain\DirectorServer$
对于结束进程、结束应用程序和重影操作：

ConfigRemoteMgmt.exe /configwinrmuser domain\name /all
要向某个用户组授予权限，请运行：

ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers /all
要显示工具的帮助，请运行：

ConfigRemoteMgmt.exe

© 1999-2017 Citrix Systems, Inc. All rights reserved.

配置网络分析

Dec 05, 2017

注意：此功能的可用性取决于组织的许可证和管理员权限。

Director 与 NetScaler Insight Center 或 NetScaler MAS 相集成以提供网络分析和性能管理：

- 网络分析利用 NetScaler Insight Center 或 NetScaler MAS 提供的 HDX Insight 报告来提供网络的应用程序和桌面环境视图。通过此功能，Director 对部署中的 ICA 通信进行高级分析。
- 性能管理提供历史保留和趋势报告。通过历史数据保留与实时评估，可以创建趋势报告，其中包括容量趋势和运行状况趋势。

在 Director 中启用此功能后，HDX Insight 报告可为 Director 提供更多信息：

- “趋势”页面中的“网络”选项卡显示对整个部署中的应用程序、桌面和用户产生的延迟和带宽影响。
- 用户详细信息页可以显示特定于某个特殊用户会话的延迟和带宽信息。

限制：

- ICA 会话的往返程时间 (RTT) 可正确显示 Receiver for Windows 3.4 或更高版本以及 Receiver for Mac 11.8 或更高版本的数据。对于早期版本的 Receiver，数据无法正确显示。
- 在“趋势”视图中，不会针对早于版本 7 的 VDA 收集 HDX 连接登录数据。对于更早版本的 VDA，图表数据将显示为 0。

要启用网络分析，必须在 Director 中安装并配置 NetScaler Insight Center 或 NetScaler MAS。Director 要求 NetScaler MAS 11.1 Build 49.16 或更高版本。Insight Center 和 MAS 是在 Citrix XenServer 中运行的虚拟设备。通过使用网络分析，Director 可以传送和收集与部署相关的信息。

有关详细信息，请参阅 NetScaler Insight Center 或 NetScaler MAS 文档。

1. 在安装了 Director 的服务器上，在 C:\inetpub\wwwroot\Director\tools 中找到 DirectorConfig 命令行工具，并在命令提示窗口中使用参数 /confignetscaler 运行该工具。
2. 系统提示时，请输入 NetScaler Insight Center 或 NetScaler MAS 计算机名称（FQDN 或 IP 地址）、用户名、密码、HTTP 或 HTTPS 连接类型，然后选择 NetScaler Insight 或 NetScaler MAS 集成。
3. 要验证更改，请先注销，然后再重新登录。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

对用户问题进行故障排除

Dec 05, 2017

使用 Director 的**技术支持**视图（**活动管理器**页面）查看用户相关信息：

- 检查与用户登录、连接和应用程序相关的详细信息。
- 重影用户计算机。
- 录制 ICA h会话。
- 执行下表中建议的操作对问题进行故障排除，并将其上报给相应的管理员。

故障排除提示

用户问题	建议
登录时间过长，或者间歇或重复性地出现登录失败。	诊断用户登录问题
应用程序运行缓慢或不响应	解决应用程序故障
连接失败	还原桌面连接
会话执行缓慢或不响应	还原会话
录制会话	录制会话
视频加载缓慢或画质差	运行 HDX 通道系统报告

注意：为确保计算机不处于维护模式，请从“用户详细信息”视图查看“计算机详细信息”面板。

搜索提示

当您在“搜索”字段中键入用户名称时，Director 会在 Active Directory 中跨所有配置为支持 Director 的站点搜索用户。

在“搜索”字段中输入多用户计算机名称时，Director 显示特定计算机的计算机详细信息。

在“搜索”字段中输入端点名称时，Director 使用连接到指定端点的未经身份验证（匿名）的会话和经过身份验证的会话，从而对未经身份验证的会话进行故障排除。请确保端点名称唯一以启用对未经身份验证的会话进行故障排除。

搜索结果中也包括当前未使用计算机或未分配给计算机的用户。

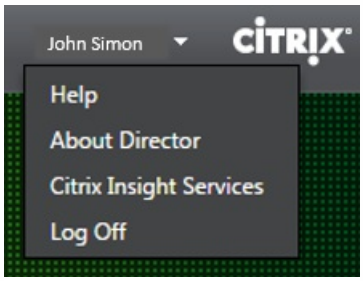
- 搜索时不区分大小写。
- 不完整的输入会产生一个可能匹配的列表。
- 您键入一个由两部分构成且中间以空格分隔的名称（用户名、姓氏和名字或显示名称）的几个字母后，搜索结果中将包含与这两个字符串均匹配的条目。例如，如果您键入 jo rob，搜索结果中可能包括“John Robertson”或 Robert, Jones 等字符串。

要返回登录页面，请单击 Director 徽标。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

访问 Citrix Insight Services

您可以从 Director 的“用户'下拉菜单中访问 Citrix Insight Services (CIS) 以获得其他诊断见解。CIS 中的数据来自拨打住宅电话功能以及 Citrix Scout 等。



将故障诊断信息上载给 Citrix 技术支持部门

从单个 Delivery Controller 或 VDA 运行 Citrix Scout 可捕获关键数据点和 Citrix Diagnostics Facility (CDF) 跟踪以对所选计算机进行故障排除。Scout 提供将数据安全地上载到 CIS 平台以帮助 Citrix 技术支持进行故障排除的功能。Citrix 技术支持使用 CIS 平台可缩短解决客户报告的问题所需的时间。

Scout 随 XenApp 或 XenDesktop 组件一起安装。安装或升级到 XenDesktop 7.1、XenDesktop 7.5、XenApp 7.5、XenDesktop 7.6、XenApp 7.6、XenDesktop 7.7 或 XenApp 7.7 时，Scout 在 Windows“开始”菜单或“开始”屏幕上显示，具体取决于 Windows 版本。

要启动 Scout，请从“开始”菜单或“开始”屏幕中选择 Citrix > Citrix Scout。

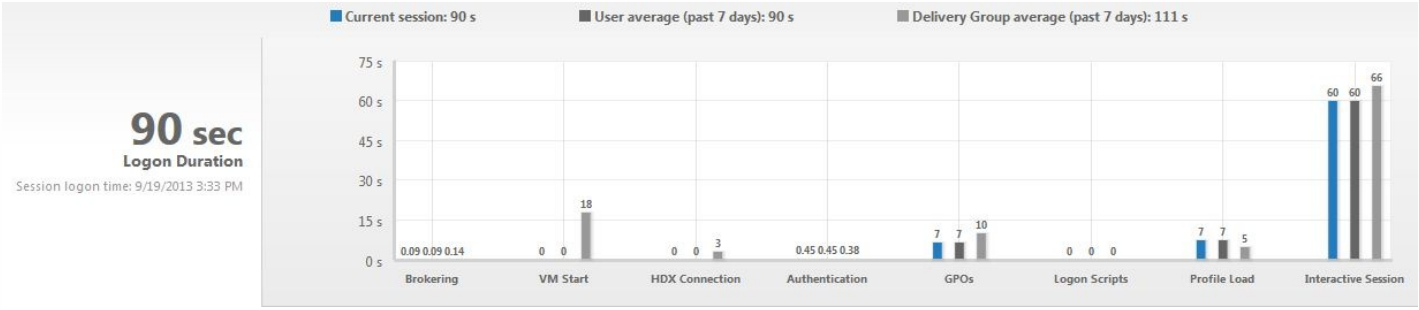
有关使用和配置 Scout 的信息以及常见问题解答，请参阅 CTX130147。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

诊断用户登录问题

Dec 05, 2017

使用“登录时长”数据解决用户登录问题。在“用户详细信息”视图中，登录时长显示为一个数值，在其下方显示了登录时间以及登录过程阶段图形。



“用户详细信息”视图中的“登录时长”面板

在用户登录到 XenApp 和 XenDesktop 时，Monitor Service 将跟踪登录过程（从用户在 Citrix Receiver 中进行连接到桌面准备就绪）的各阶段。左侧的大数字是总登录时间，其计算方式为：将建立连接和从 Delivery Controller 获得桌面所用的时间与执行身份验证和登录虚拟桌面所用的时间相结合。在管理员的 Web 浏览器中，时长信息表示为本地时间中的秒（或秒的小数部分）。

可使用以下常规步骤解决用户登录问题：

1. 从**用户详细信息**视图，使用“登录时长”面板对登录状态进行故障排除。
   - 如果用户正在登录，视图会反映登录进度。
   - 如果用户当前已登录，“登录时长”面板会显示用户登录当前会话所用的时间。
2. 检查登录过程中的各个阶段。

登录过程阶段	**说明**
正在代理	在决定向用户分配哪个桌面时所用的时间。
VM 启动	如果会话需要启动计算机，则为启动虚拟机所用的时间。
HDX 连接	在设置从客户端到虚拟机的 HDX 连接期间需执行的步骤所用的时间。
身份验证	完成远程会话的身份验证所用的时间。
GPO	如果在虚拟机上启用了组策略设置，则为应用组策略对象所用的时间。
登录脚本	如果为会话配置了登录脚本，则为执行登录脚本所用的时

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	间。
配置文件加载	如果为用户或虚拟机配置了配置文件设置，则为加载配置文件所用的时间。
交互式会话	这是在加载用户配置文件后向用户“移交”键盘和鼠标控制权所用的时间。它通常是登录过程的所有阶段中发生的最长的时长，其计算公式如下： 交互式会话时长 = 桌面就绪事件时间戳 (EventId 1000 on VDA) - 用户配置文件加载事件时间戳 (EventId 2 on VDA)

总登录时间并不是这些阶段的精确总和。例如，一些阶段并行发生，而在某些阶段中会发生额外处理，这可能会导致登录时长大于阶段总和。

注意：“登录持续时间”图形将显示各登录阶段（以秒为单位）。任何小于一秒的时长将显示为次秒值。大于一秒的值将四舍五入为最接近的 0.5 秒值。此图形可将最大 y 轴值显示为 200 秒。任何大于 200 秒的值都显示为实际值，位于栏上方。

要在图表中找到异常值或意外值，请将当前会话每个阶段所用的时间与最近七天此用户的平均时长以及最近七天此交付组所有用户的平均时长进行比较。

如有必要请进行上报。例如，如果 VM 启动速度缓慢，问题可能存在于虚拟机管理程序中，因此您可以将问题上报给虚拟机管理程序管理员。而如果代理速度缓慢，您可以将问题上报给站点管理员，让其检查 Delivery Controller 上的负载平衡情况。

检查异常的差异，其中包括：

- 缺少（当前）登录栏
- 当前时长与此用户平均时长之间存在很大差异。原因可能包括：
  - 已安装新应用程序。
  - 发生操作系统更新。
  - 更改了配置。
  - 用户配置文件很大。在这种情况下，“配置文件加载”值将很大。
- 用户的登录次数（当前时长和平均时长）与交付组平均时长之间存在很大差异。

如果需要，请单击**重新启动**，观察用户的登录过程，以对问题进行故障排除，比如 VM 启动或代理方面的问题。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

重影用户

Dec 05, 2017

在 Director 中，使用 重影 用户功能直接在用户虚拟机或 会话中进行查看和操作。用户必须连接到您要执行重影操作的计算机。 可通过检查用户标题栏中所列的计算机名称来验证此项操作。

1. 在 用户 详细信息视图中，选择用户会话。
2. 为所选用户会话激活重影：
   - 要执行计算机监视，请在 活动管理器视图中，单击 重影。
   - 要监视会话，请在 用户 详细信息视图中，查找 会话详细信息面板，然后单击 重影。
3. 连接初始化后，将显示一个对话框，提示您打开或保存 .msrcincident 文件。
4. 请使用远程协助查看器（如果默认情况下尚未选择）打开事件文件。 此时将在用户设备上显示一个确认提示窗口。
5. 指导用户单击“是”启动计算机或会话共享。

要执行其他控制，请要求用户共享键盘和鼠标控制。

将 Microsoft Internet Explorer 浏览器配置为：通过远程协助客户端自动打开已下载的 Microsoft 远程协助 (.msra) 文件。

为此，您必须在组策略编辑器中启用文件下载自动提示设置：

计算机配置 > 管理模板 > Windows 组件 > Internet Explorer > Internet 控制面板 > 安全页面 > Internet 区域 > 文件下载自动提示。

默认情况下，此选项对本地 Intranet 区域中的站点启用。如果 Director 站点不在本地 Intranet 区域中，请考虑将该站点手动添加到此区域。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

向用户发送消息

Dec 05, 2017

在 Director 中，向连接到一台或多台计算机的用户发送消息。例如，使用此功能发送有关管理操作（如即将发生的桌面维护、计算机注销和重新启动以及配置文件重置）的即时通知。

1. 在 活动管理器视图中，选择用户，然后单击 详细信息。
2. 在 用户 详细信息视图中，查找 会话详细信息面板，然后单击 发送 消息。
3. 在“主题”和“消息”字段中键入您的消息信息，然后单击“发送”。

如果消息发送成功，将在 Director 中显示确认消息。 如果用户计算机已连接，则将在其中显示消息。

如果消息未发送成功，则将在 Director 中显示错误消息。 根据错误消息对问题进行故障排除。 完成后，再次键入主题和消息文本，然后单击“重试”。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

解决应用程序故障

Dec 05, 2017

在活动管理器视图中，单击应用程序选项卡。您可以查看此用户访问的所有计算机上的所有应用程序，其中包括当前连接的计算机的本地应用程序和托管应用程序，以及每个应用程序的当前状态。

注意：如果应用程序选项卡处于灰显状态，请联系有权启用此选项卡的管理员。

列表仅包含已经在会话中启动的应用程序。

对于服务器操作系统计算机和桌面操作系统计算机，会列出各个已断开连接的会话的应用程序。如果用户未建立连接，将不会显示任何应用程序。

操作	**说明**
终止不响应的应用程序	选中不响应的应用程序并单击“结束应用程序”。终止应用程序后，请求用户重新启动应用程序。
终止不响应的进程	如果您拥有必需的权限，请单击“进程”选项卡。选择与应用程序相关的进程或者占用大量 CPU 资源或内存的进程，然后单击**结束进程**。 但是，如果您没有终止进程所需的权限，尝试结束进程操作将失败。
重新启动用户的计算机	对于所选会话，请单击**重新启动**，此操作仅适用于桌面操作系统计算机。 或者，从“计算机详细信息”视图，使用电源控制项重新启动或关闭计算机。指导用户再次登录，以便您重新检查应用程序。 对于服务器操作系统计算机，重新启动选项不可用，而是需要用户注销，然后再重新登录。
将计算机置于维护模式	如果计算机的映像需要维护（如安装修补程序或其他更新），请将计算机置于维护模式。从**计算机详细信息**视图中，单击**详细信息**，然后启用维护模式选项。上报给相应的管理员。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

还原桌面连接

Dec 05, 2017

从 Director 的用户标题栏检查当前计算机的用户连接状态。

如果桌面连接失败，将会显示导致连接失败的错误，以帮助您确定如何进行故障排除。

操作	说明
确保计算机未处于维护模式	请确保在用户详细信息页面上已关闭维护模式。
重新启动用户的计算机	选择计算机，然后单击重新启动。如果用户计算机没有响应或无法连接，比如计算机占用异常高的 CPU 资源（这会导致 CPU 不可用），请使用此选项。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

还原会话

Dec 05, 2017

如果会话断开连接，它将继续处于活动状态，其应用程序仍会运行，但用户设备将不再与该服务器通信。

在用户详细信息视图的会话详细信息面板中，对会话故障进行故障排除。您可以查看当前会话的详细信息（以会话 ID 指示）。

操作	说明
终止不响应的应用程序或进程	单击应用程序选项卡。选中不响应的应用程序并单击结束应用程序。同样，选中对应的不响应的进程并单击结束进程。此外，结束占用过多内存或 CPU 资源的进程，因为这种进程可能会导致 CPU 无法使用。
断开 Windows 会话的连接	单击会话控制并选择断开连接。此选项仅适用于代理服务器操作系统计算机。对于非代理会话，则禁用此选项。
从会话中注销用户	单击会话控制并选择注销。

要测试会话，用户可尝试再次登录会话。您也可以重影该用户，更密切地监控此会话。

注意：如果用户设备正在运行的 VDA 版本早于 XenDesktop 7，Director 将无法显示有关该会话的完整信息；相反，将会显示一条关于无法获取信息的消息。这些消息可能会在用户详细信息页面和活动管理器中显示。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

运行 HDX 通道系统报告

Dec 05, 2017

在用户详细信息视图的 HDX 面板中，检查用户计算机上 HDX 通道的状态。只有在用户计算机使用 HDX 连接时，才可使用此面板。

如果出现了一条指示当前无法获取信息的消息，请等待一分钟以便页面进行刷新，或选择刷新按钮。HDX 数据更新时间比其他数据更新时间稍长。

单击错误或警告图标，以了解更多信息。

提示：可以在同一对话框中，通过单击标题栏左角的向左和向右箭头，查看其他通道的相关信息。

HDX 通道系统报告主要供 Citrix 技术支持用来进行进一步的故障排除。

1. 在 HDX 面板中，单击“下载系统报告”。
2. 可以查看或保存 .xml 报告文件。
   - 要查看 .xml 文件，请单击“打开”。 .xml 文件将出现在 Director 应用程序所在的窗口中。
   - 要保存 .xml 文件，请单击“保存”。 此时将显示 另存 为窗口，提示您提供 Director 计算机上的文件下载位置。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

重置 Personal vDisk

Dec 05, 2017

小心：重置磁盘时，各设置会还原为出厂默认值，并且磁盘中的所有数据都将删除，包括应用程序。除非修改了 Personal vDisk 默认设置（用于重定向来自 C: 驱动器的配置文件），或不是使用第三方配置文件解决方案，否则将保留此配置文件数据。
要进行重置，必须运行启用 Personal vDisk 的计算机；但用户无需登录该计算机。

此选项仅适用于桌面操作系统计算机；对服务器操作系统计算机则禁用此选项。

1. 从 技术 支持视图中，选择目标桌面操作系统计算机。
2. 从此视图中 或在 用户 详细信息视图的 个性化面板中，单击 重置 Personal vDisk。
3. 单击 重置。 此时将显示一条警告消息，提醒用户将注销。 用户注销（如果用户已登录）之后，计算机将重新启动。

如果重置 成功， 用户 详细信息视图 个性化面板中的 Personal vDisk 状态字段值将为 正在运行。如果重置失败，将在 正在运行值的右侧显示一个红色的 X。指向此 X 时，将显示失败的相关信息。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

重置用户配置文件

Dec 05, 2017

小心：重置配置文件时，虽然用户的文件夹和文件都已保存并复制到新的配置文件，但大部分用户配置文件数据仍将被删除（例如，注册表被重置，应用程序设置可能被删除）。

1. 从 Director，搜索要重置其配置文件的用户，并选择此用户的会话。
2. 单击**重置配置文件**。
3. 指示用户从所有会话中注销。
4. 指导用户重新登录。从用户配置文件保存的文件夹和文件已复制到新的配置文件。

   重要：如果用户在多个平台（如 Windows 8 和 Windows 7）上具有配置文件，请指导用户首先重新登录用户报告有问题的同一桌面或应用程序。这样可确保重置正确的配置文件。

   如果此配置文件是 Citrix 用户配置文件，那么它在用户桌面显示时已重置。如果此配置文件是 Microsoft 漫游配置文件，文件夹还原可能短时间内仍在进行。在还原完成前，用户必须保持登录状态。

注意：上述步骤假定您使用的是 XenDesktop（桌面 VDA）如果您使用的是 XenApp（服务器 VDA），则需要登录才能执行配置文件重置。用户随后需要注销，然后重新登录才能完成配置文件重置。

如果配置文件未能成功重置（例如，用户无法成功重新登录计算机或部分文件已丢失），您必须手动还原原始配置文件。

用户配置文件中的文件夹（及其文件）将保存并复制到新配置文件中。将按照所列顺序复制这些文件：

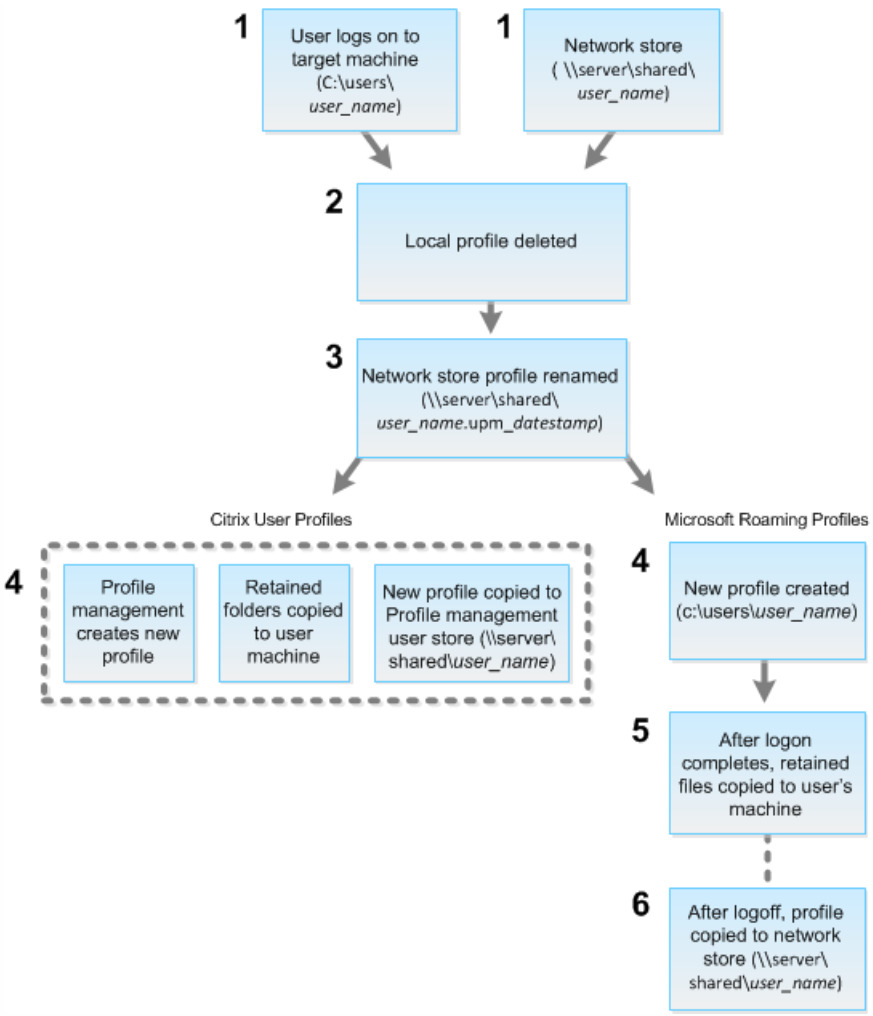
- 桌面
- cookie
- 收藏夹
- 文档
- 图片
- 音乐
- 视频

注意：在 Windows 8 或更高版本中，重置配置文件时不会复制 Cookie。

所有 Citrix 用户配置文件或 Microsoft 漫游配置文件均可重置。在用户注销并且您选择重置命令（在 Director 中或使用 PowerShell SDK）后，Director 首先识别正在使用的用户配置文件并发出相应的重置命令。Director 通过 Profile Management 接收信息，包括有关配置文件大小、类型和登录时间的信息。

下图显示了用户登录后的过程。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



1. Director 发出的重置命令会指定配置文件类型。然后，Profile Management Service 将尝试重置此类型的配置文件，并查找相应的网络共享（用户存储）。如果用户由 Profile Management 处理，但却接收到漫游配置文件命令，用户将被拒绝（反之亦然）。
2. 如果存在本地配置文件，则会将其删除。
3. 重命名网络配置文件。
4. 下一步操作取决于要重置的配置文件是 Citrix 用户配置文件还是 Microsoft 漫游配置文件。
   - 对于 Citrix 用户配置文件，将使用 Profile Management 导入规则创建新配置文件，然后将文件夹复制回网络配置文件，之后用户可以继续正常登录。如果将漫游配置文件用于重置，则漫游配置文件中的任何注册表设置将保留在重置配置文件中。

     注意：如果需要，您可以配置 Profile Management，以使模板配置文件覆盖漫游配置文件。
   - 对于 Microsoft 漫游配置文件，使用 Windows 创建新配置文件，然后在用户登录时，将文件夹复制回用户设备。用户再次注销时，新配置文件将复制到网络存储中。

1. 指示 用户从所有会话中注销。
2. 删除本 地配置文件（如果存在）。
3. 查找网络共享上的 存档文件夹，即文件夹名称中 包含日期和时间且扩展名为 .upm_datestamp 的文件夹。
4. 删除 当前配置文件名称，即不包含 upm_datestamp 扩展名的文件。
5. 使用原配置文件名称重命名 存档文件夹，即删除日期和 时间扩展名。 此时 已将配置文件恢复为其重置之前的原始状态。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

录制会话

Dec 05, 2017

在 Director 中，可以使用**用户详细信息**和**计算机详细信息**中的 Session Recording 控件录制 ICA 会话。此功能适用于 **Platinum** 站点上的客户。

要使用 DirectorConfig 工具在 Director 中配置 Session Recording，请参阅安装、升级和卸载 Session Recording 中的“ 配置 Director 以使用 Session Recording Server”部分。

仅当已登录的用户具有修改 Session Recording 策略的权限时，Session Recording 控件才会在 Director 中可用。可以在 Session Recording Authorization 控制台上设置此权限，如创建和激活录制策略中所述。

注意：通过 Director 或 Session Recording 策略控制台对 Session Recording 设置所做的更改自后续的 ICA 会话开始生效。

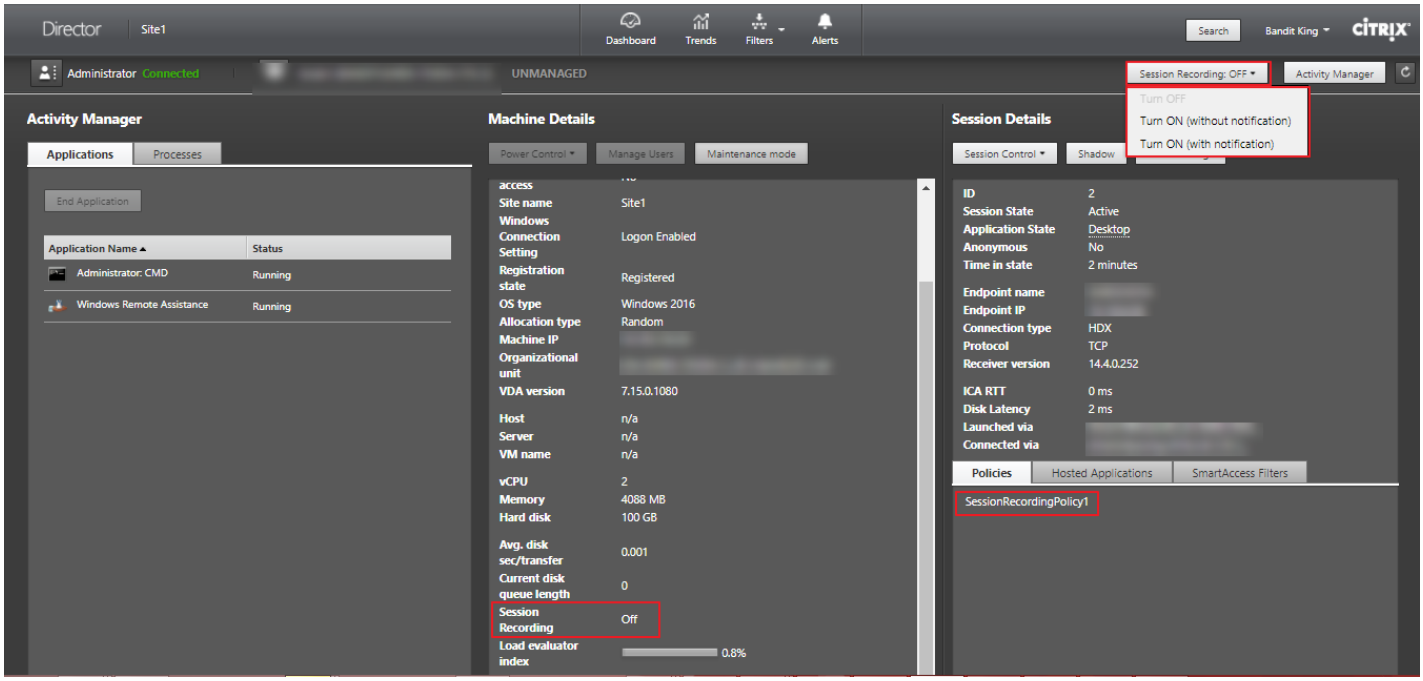
Director 中的 Session Recording 控件

可以在**活动管理器**或**用户详细信息**屏幕中为特定用户启用 Session Recording。后续会话将在受支持的所有服务器上针对特定用户录制。

可以执行以下操作：

- 打开（并通知）- 登录到 ICA 会话时，通知用户与正在录制的会话有关的信息。
- 打开（但不通知）- 无提示录制会话，不通知用户任何信息。
- 关闭 - 对用户禁用会话录制。

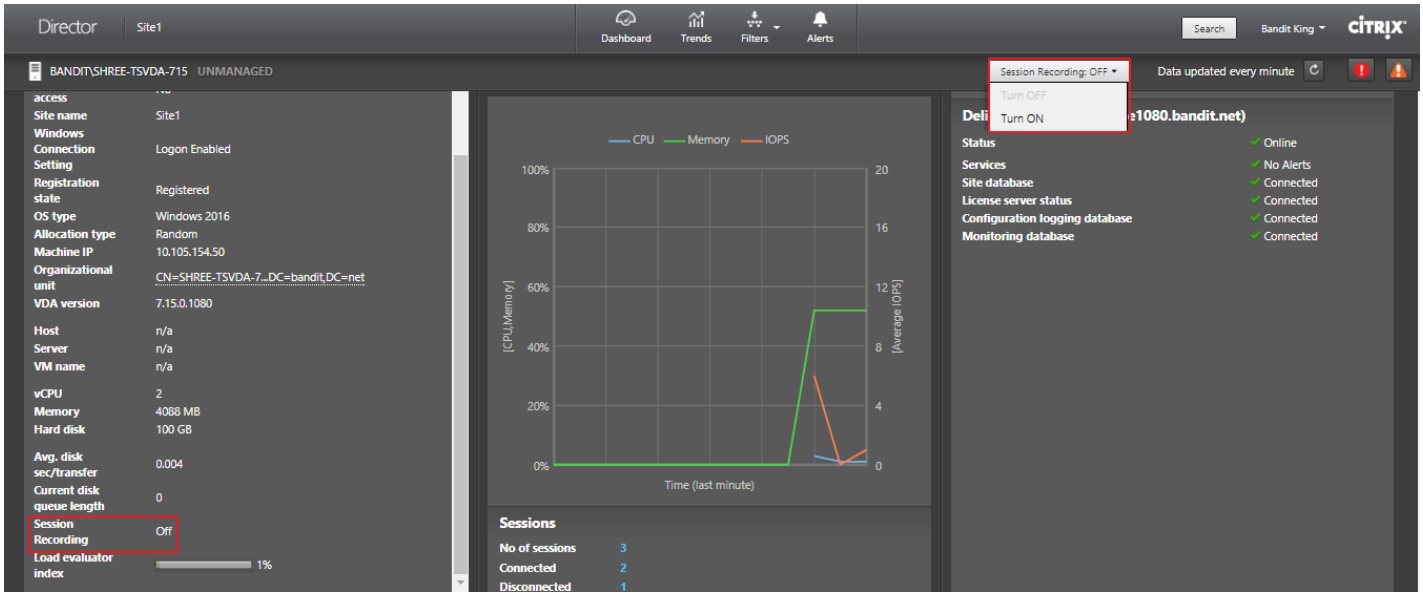
“策略”面板显示活动 Session Recording 策略的名称。



可以从“计算机详细信息”页面为特定计算机启用 Session Recording。该计算机上的后续会话将被录制。“计算机详细信息”面板

© 1999-2017 Citrix Systems, Inc. All rights reserved.

显示该计算机的 Session Recording 策略状态。



© 1999-2017 Citrix Systems, Inc. All rights reserved.

应用程序故障排除

Dec 05, 2017

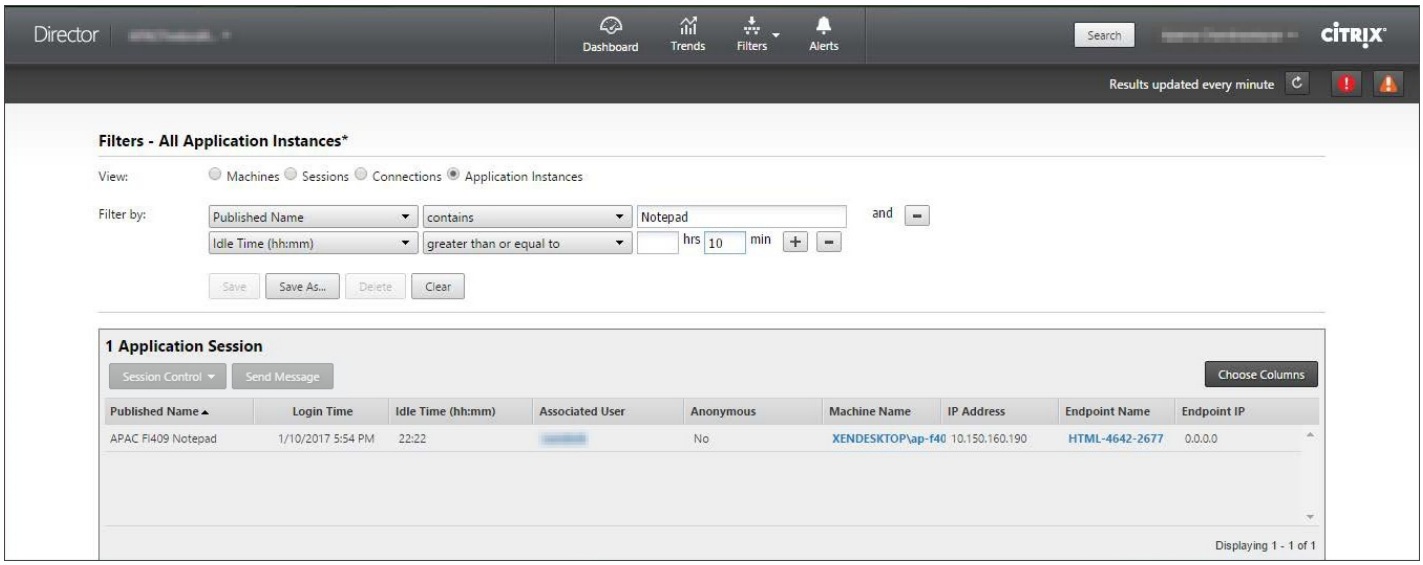
可以使用空闲时间衡量指标对应用程序和会话进行故障排除以确定特定时间限制以外处于空闲状态的实例。

基于应用程序的故障排除的典型用例是在卫生保健部门，在此部门中，员工将共享应用程序许可证。在此部门中，必须结束空闲会话和应用程序实例才能清除 XenApp 和 XenDesktop 环境、重新配置性能较差的服务器或者维护和升级应用程序。

应用程序实例过滤器页面列出服务器和桌面操作系统 VDA 上的所有应用程序实例。将显示已至少空闲 10 分钟的服务器操作系统 VDA 上的应用程序实例的关联空闲时间量化指标。

注意：在所有许可证版本的站点上都提供应用程序实例指标。

使用此信息可确定在特定时间段以外处于空闲状态的应用程序实例并根据需要注销或断开其连接。为此，请选择**过滤器 > 应用程序实例**，然后选择预先保存的过滤器或选择**所有应用程序实例**并创建您自己的过滤器。

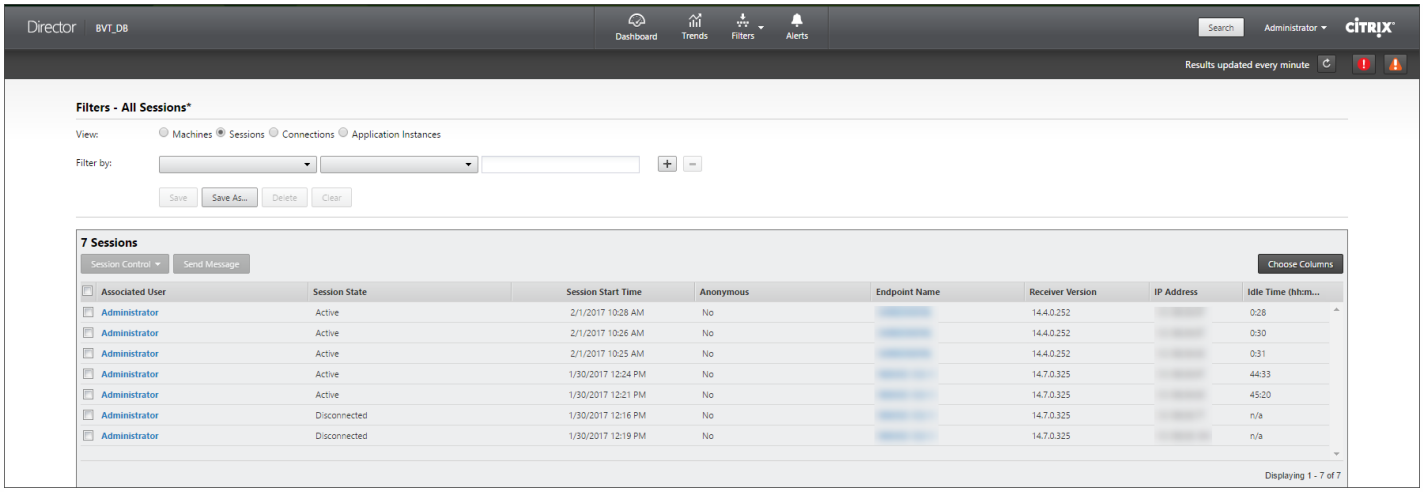


过滤器的一个示例如下。对于**过滤依据**条件，请选择（应用程序的）**发布的名称**和**空闲时间**。然后，将**空闲时间**设置为**大于或等于**特定时间限制并保存该过滤器以供重复使用。从过滤的列表中，选择应用程序实例。选择用于发送消息的选项，或者从**会话控制**下拉菜单中，选择**注销**或**断开连接**，以结束实例。

注意：注销或断开应用程序会话将注销或断开当前会话，因此结束属于同一会话的所有应用程序实例。

可以使用会话状态和会话空闲时间衡量指标确定**会话**过滤器页面中的空闲会话。请按**空闲时间**列进行排序或定义一个过滤器以确定特定时间限制以外处于空闲状态的会话。将列出已至少空闲 10 分钟的服务器操作系统 VDA 的会话的空闲时间。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



会话或应用程序实例处于以下状态时**空闲时间**将显示为**不适用**

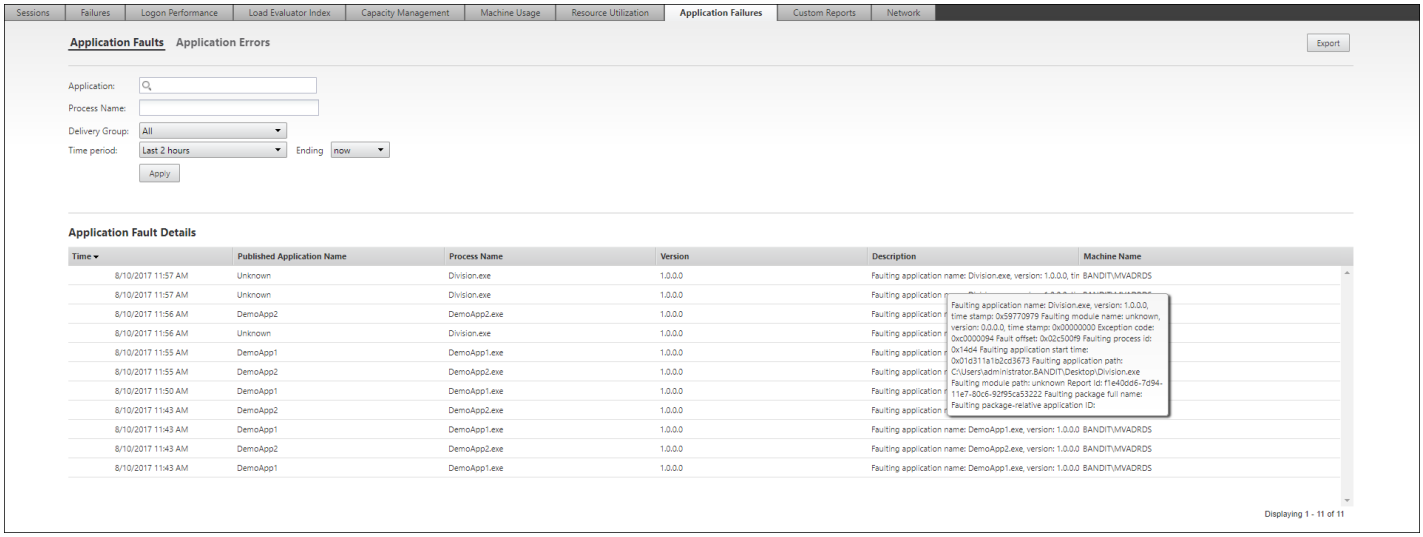
- 空闲时间未超过 10 分钟，
- 是在服务器操作系统 VDA 上启动的，或者
- 是在运行 7.12 或早期版本的 VDA 上启动的。

趋势 -> **应用程序故障**选项卡显示与 VDA 上已发布的应用程序关联的故障。

对于 Platinum 和 Enterprise 许可的站点，可以获取过去 2 小时、24 小时、7 天和 1 个月内的应用程序故障趋势。对于其他许可证类型，可以获取过去 2 小时、24 小时和 7 天内的应用程序故障趋势。记录到事件查看器中的来源为“应用程序错误”的应用程序故障将被监视。单击**导出**可生成 CSV、Excel 或 PDF 格式的报告

对于 Platinum 和非 Platinum 许可的站点，应用程序故障监视的整理保留期限设置 GroomApplicationErrorsRetentionDays 和 GroomApplicationFaultsRetentionDays 默认设置为 1 天。可以使用 PowerShell 命令更改此设置：

Set-MonitorConfiguration -



根据其严重性，这些故障显示为**应用程序故障**或**应用程序错误**。“应用程序故障”选项卡显示与功能或数据的丢失有关的故障。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

“应用程序错误”指示不直接相关的问题；这些错误表示可能会导致将来出现问题的条件。

可以根据**已发布的应用程序名称**、**进程名称**或**交付组**以及“**时间段”对故障进行过滤。**下表显示了故障或错误代码以及故障的简短说明。详细的故障说明以工具提示的方式显示。

注意：无法派生相应的应用程序名称时，“已发布的应用程序名称”显示为“未知”。已启动的应用程序在桌面会话中出现故障时，或者该应用程序由于依赖的可执行文件导致的未处理的异常而出现故障时，通常会出现此问题。

默认仅监视服务器操作系统 VDA 上托管的应用程序故障。可以通过监视组策略修改监视设置：“启用应用程序故障的监视”、“在桌面操作系统 VDA 上启用应用程序故障的监视”以及“从故障监视中排除的应用程序列表”。有关详细信息，请参阅“监视策略设置”中的应用程序故障监视策略。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

计算机故障排除

Dec 05, 2017

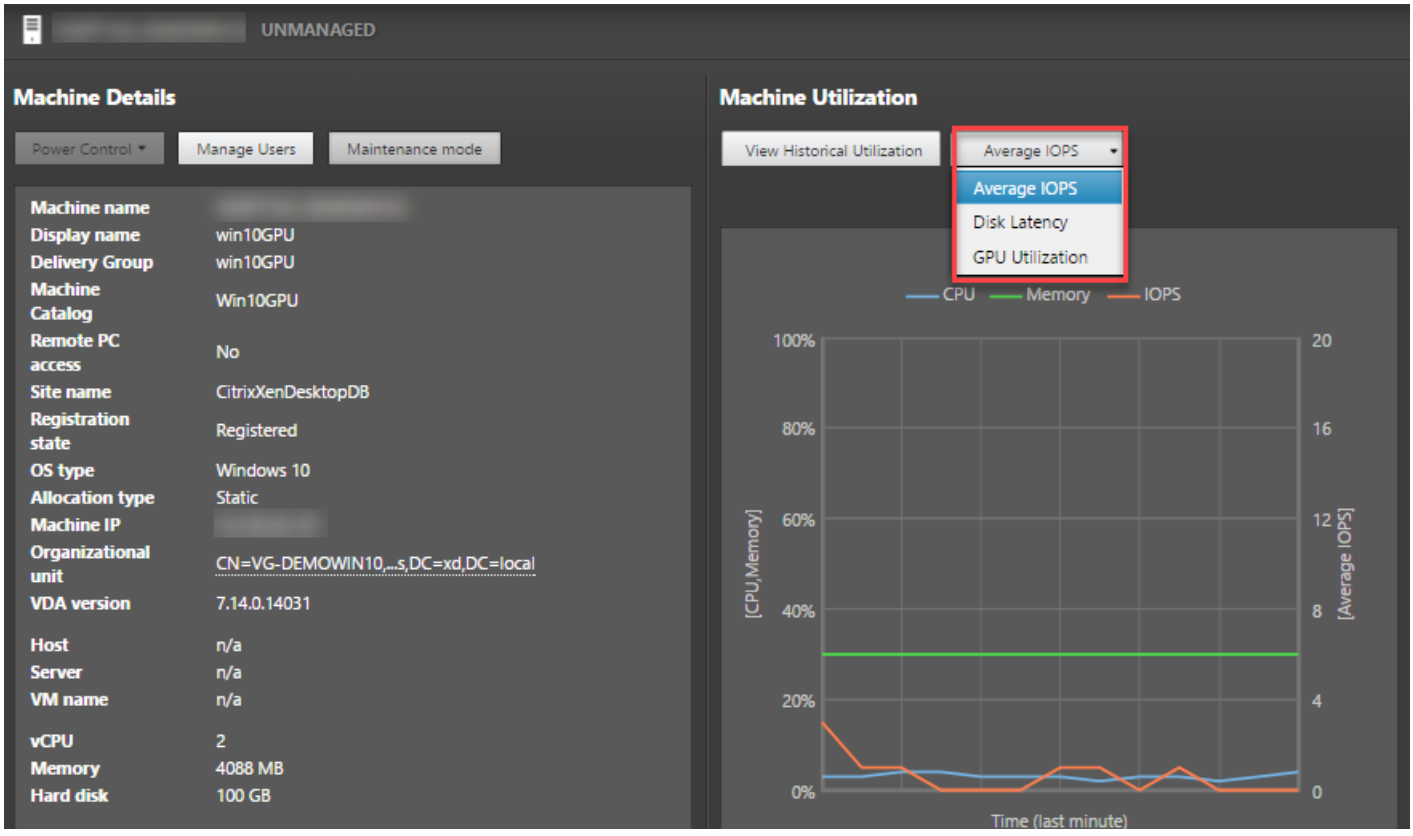
在**过滤器 > 计算机**视图中，选择**桌面操作系统计算机**或**服务器操作系统计算机**可查看站点中配置的计算机。“服务器操作系统计算机”选项卡包括负载评估器指数，如果将鼠标悬停在链接上，则会指示性能计数器的分布情况和会话计数的工具提示。

单击故障计算机的**故障原因**可获取有关故障的详细说明以及排除故障的建议操作。Citrix Director 7.12 Failure Reasons Troubleshooting Guide（《Citrix Director 7.12 故障原因排除指南》）中提供了计算机故障和连接失败的故障/失败原因和建议的操作。

单击计算机名称链接可转到**计算机详细信息**页面。“计算机详细信息”页面列出计算机详细信息、基础结构详细信息和计算机上应用的修补程序的详细信息。**计算机利用率**面板显示计算机利用率图。

计算机利用率面板提供显示 CPU 和内存实时利用率的图形。此外，对于具有 Delivery Controller 和 VDA **7.14** 版或更高版本的站点，还提供磁盘和 GPU 监视图。

磁盘监视图、平均 IOPS 和磁盘延迟是重要的性能衡量指标，可帮助您监视与 VDA 磁盘有关的问题并对其进行故障排除。平均 IOPS 图显示磁盘的平均读写次数。选择**磁盘延迟**可查看请求数据与从磁盘返回数据之间的延迟图（以毫秒为单位）。



选择 **GPU 利用率**可查看 GPU、GPU 内存以及编码器和解码器的利用率百分比，从而对服务器或桌面操作系统 VDA 上的 GPU 相关问题进行故障排除。仅对运行配备了 NVIDIA Tesla M60 GPU 的 64 位 Windows 的 VDA 和运行显示驱动程序 369.17 版或更高版本的 VDA 提供 GPU 利用率图。

VDA 必须启用了 HDX 3D Pro 才能实现 GPU 加速。有关详细信息，请参阅“适用于 Windows 桌面操作系统的 GPU 加速”和“适

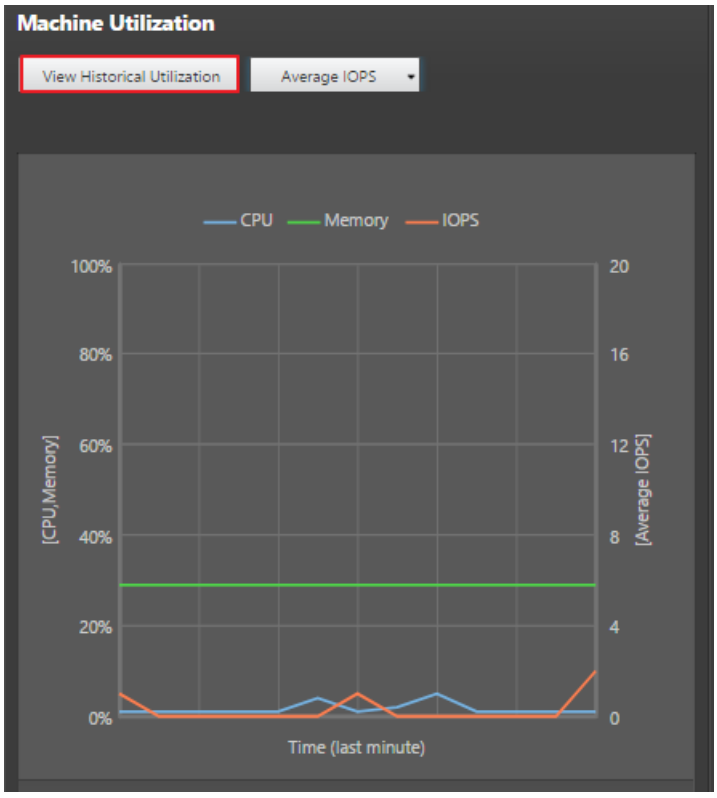
© 1999-2017 Citrix Systems, Inc. All rights reserved.

用于 Windows 服务器操作系统的 GPU 加速”。
VDA 访问多个 GPU 时，利用率图将显示从各个 GPU 收集的 GPU 指标的平均值。GPU 指标是针对整个 VDA 收集，而不是针对各个进程收集。

在**计算机利用率**面板中，单击**查看历史利用率**可查看选定计算机上资源的历史使用情况。
利用率图包括 CPU、内存、最大并发会话数、平均 IOPS 和磁盘延迟的关键性能计数器。

注意：必须将监视策略设置**启用进程监视**设置为“允许”才能在“历史计算机利用率”页面上“排名前 10 的进程”表中收集并显示数据。默认情况下禁止收集。

默认情况下会收集 CPU 和内存利用率、平均 IOPS 和磁盘延迟数据。可以使用**启用资源监视**策略设置禁用收集。



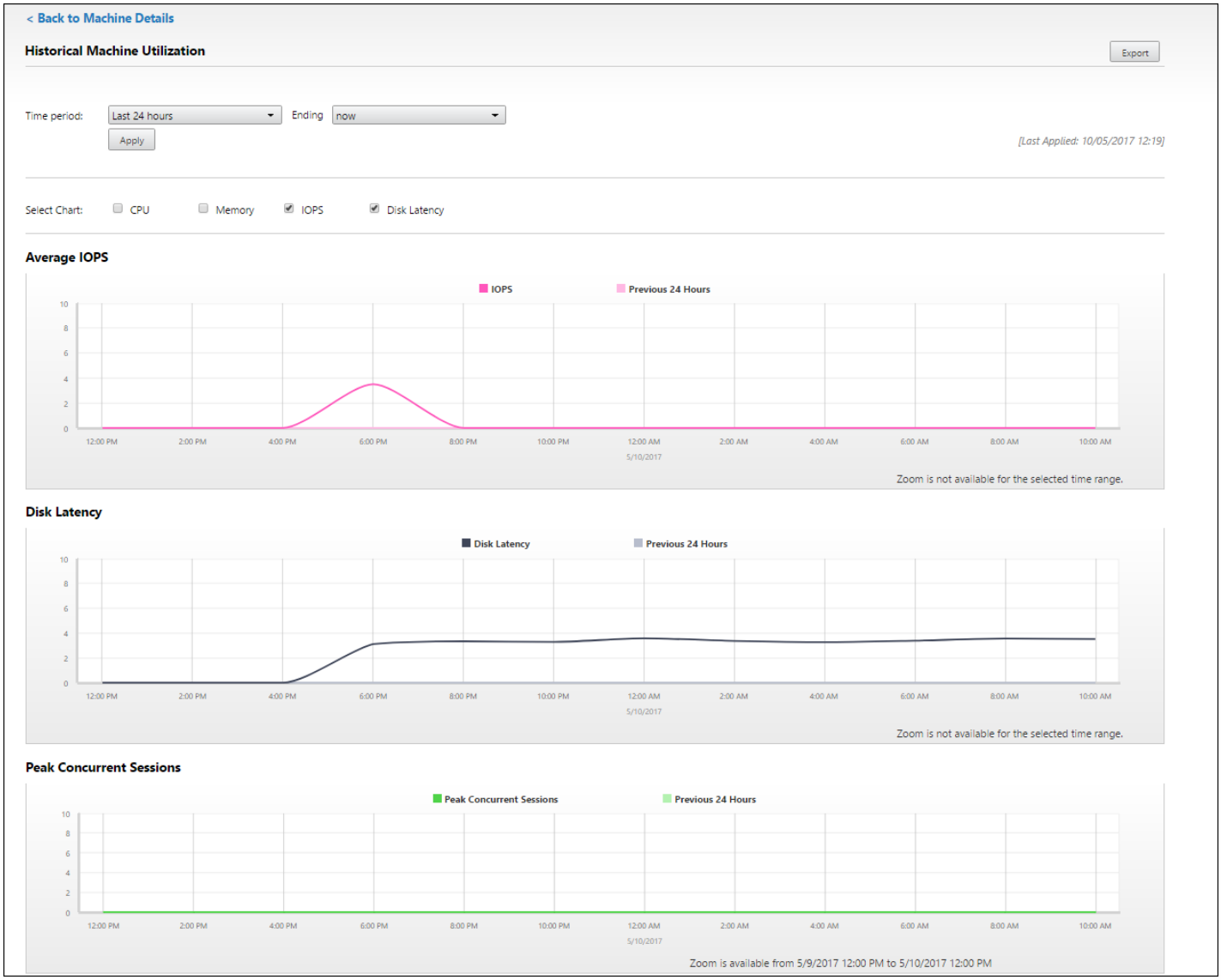
1. 在**计算机详细信息**视图的**计算机利用率**面板中，选择**查看历史利用率**。这将打开**历史计算机利用率**页面。

2. 设置**时间段**以查看过去 2 小时、24 小时、7 天、上个月或上一年的使用情况。
注意：提供截至现在的过去 24 小时、上个月和上一年的平均 IOPS 和磁盘延迟使用数据。不支持自定义结束时间。

3. 单击**应用**并选择所需图形。

4. 将鼠标悬停在图形的不同部分，以查看选定时间段的详细信息。

© 1999-2017 Citrix Systems, Inc. All rights reserved.



例如，如果您选择**过去 2 小时**，则基准期为选定时间范围前的 2 小时。查看过去 2 小时和基准时间内的 CPU、内存和会话趋势。
如果选择**上个月**，则基准期为上个月。选择可查看上个月和基准时间内的平均 IOPS 和磁盘延迟。

5. 单击**导出**可导出所选时间段的资源利用率数据。有关详细信息，请参阅“监视部署”中的导出报告部分。

6. 在图形下方，表中列出了基于 CPU 或内存利用率排名前 10 的进程。您可以按照任何列进行排序，其中显示有选定时间范围内的应用程序名称、用户名、会话 ID、平均 CPU 、峰值 CPU、平均内存以及峰值内存。IOPS 和磁盘延迟列不能排序。

注意：系统进程的会话 ID 显示为 0000。

7. 要查看特定进程的资源消耗的历史趋势，请进一步查看排名前 10 的进程中的任何一个。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

功能兼容性列表

Dec 05, 2017

在每个站点中，尽管早期版本的 VDA 或 Delivery Controller 仍可使用，但最新版本的 Director 中的所有功能可能无法使用。此外，功能可用性还取决于站点许可证版本。Citrix 建议使用相同版本的 Director、Delivery Controller 和 VDA。

注意：升级 Delivery Controller 后，系统将在您打开 Studio 时提示您升级站点。有关详细信息，请参阅升级部署中的**升级顺序**部分。

下表列出了 Director 功能以及 Delivery Controller (DC)、VDA 和许可版本所需的任何其他依赖组件的最低版本。

Director 版本	功能	依赖组件 - 所需的最低版本	版本
7.15	应用程序故障监视	DC 7.15 || VDA 7.15	全部
7.14	以应用程序为中心的故障排除	DC 7.13 || VDA 7.13	全部
	磁盘监视	DC 7.14 || VDA 7.14	全部
	GPU 监视		
7.13	以应用程序为中心的故障排除	DC 7.13 || VDA 7.13	铂金版
	“会话详细信息”面板上的传输协议	DC 7.x || VDA 7.13	全部
7.12	用户友好的连接和计算机故障说明	DC 7.12 || VDA 7.x	全部
	提高了 Enterprise Edition 中历史数据的可用性		企业
	自定义报告		铂金版
	使用 SNMP 陷阱自动处理 Director 通知		铂金版
7.11	资源利用率报告	DC 7.11 || VDA 7.11	全部
	警报扩展为针对 CPU、内存和 ICA RTT 条件		铂金版
	导出报告改进		全部

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	借助 Citrix Octoblu 实现 Director 通知自动化	DC 7.11 || VDA 7.x	铂金版
	与 NetScaler MAS 相集成	DC 7.11 || VDA 7.x || MAS 11.1 Build 49.16	铂金版
7.9	登录持续时间细分	DC 7.9 || VDA 7.x	全部
7.7	主动监视和警告	DC 7.7 || VDA 7.x	铂金版
	SCOM 集成	DC 7.7 || VDA 7.x || SCOM 2012 R2 || PowerShell 3.0 或更高版本*	铂金版
	Windows 身份验证集成	DC 7.x || VDA 7.x	全部
	桌面和服务器操作系统使用情况	DC 7.7 || VDA 7.x	铂金版
7.6.300	支持 Framehawk 虚拟通道	DC 7.6 || VDA 7.6	全部
7.6.200	Session Recording 集成	DC 7.6 || VDA 7.x	铂金版
7	HDX Insight 集成	DC 7.6 || VDA 7.x || NetScaler Insight Center	铂金版

© 1999-2017 Citrix Systems, Inc. All rights reserved.

数据粒度和保留

Apr 23, 2018

数据值聚合

Monitor Service 收集多种数据，其中包括用户会话使用情况、用户登录 性能详细信息、会话负载平衡详细信息，以及连接和计算机 故障信息。根据其类别，数据以不同的方式聚合。 了解使用 OData Method API 提供的数据值的聚合是解释数据的关键。例如：

- 一段时间内发生的连接的会话故障和计算机故障。因此它们显示为一段时间内的最大值。
- 登录持续时间是时间长度的度量，因此它们显示为一段时间内的平均值。
- 登录计数和连接故障是一段时间内这类事件的计数，因此它们显示为一段时间内的总数。

并发数据评估

会话必须 重叠才能视为并发。但是，当时间间隔为 1 分钟时，该时间内的所有会话（无论会话是否重叠）都将被 视为并发：由于时间间隔太小，计算精度时所涉及的 性能开销有些 得不偿失。如果会话发生在同一小时，但不同 分钟内，则不会被视为重叠。

关联汇总表和行数据

数据模型 以两种不同方式表示指标：

- 汇总表以每分钟、每小时和每天的时间粒度表示指标的聚合视图。
- 行数据表示单个事件或在会话、连接、应用程序或其他对象中跟踪到的当前状态。

尝试 跨 API 调用或在数据模型自身内部关联数据时， 必须理解以下概念和限制：

- **不存在部分时间间隔的汇总数据。** 指标汇总是为了洞察长时间内的历史趋势。 这些指标应该聚合到完整时间间隔的汇总表中。 不存在仅包含数据收集的开始时间（最早的可用数据）而不包含结束时间的部分时间间隔的汇总数据。 这意味着，当查看一天（时间间隔=1440）的聚合时，最早和最近的不完整日期将不包含数据。 尽管存在这些部分时间间隔的行数据，但不会汇总这些行数据。 对于特定时间粒度，可以通过从特定汇总表提取最小和最大 SummaryDate，确定最早和最近的聚合时间间隔。 SummaryDate 列表示时间间隔的开始时间。Granularity 列表示聚合数据的时间间隔长度。
- **按时间关联。**如上所述，指标聚合到完整时间间隔的汇总表中。 它们可以用于了解历史趋势，但是行事件的状态可能更新，不能通过汇总进行趋势分析。 基于时间比较汇总数据和行数据时，应注意不存在可能发生的任何部分时间间隔或时间段的开头和结尾部分的汇总数据。
- **缺失的事件和延迟事件。** 如果在聚合时间段有事件缺失或延迟，聚合到汇总表中的指标可能会略有误差。 尽管 Monitor Service 尝试维护准确的最新状态，但是它不会针对缺失或延迟的事件后退到过去重新计算汇总表中的聚合值。
- **连接高可用性。** 在连接 HA 期间，当前连接的汇总数据计数会存在误差，但是会话实例仍在行数据中运行。
- **数据保留期限。** 汇总表中的数据保留整理计划不同于行事件数据的计划。 由于数据已从汇总表或行表格加以整理，因此可能会有所缺失。 不同粒度的汇总数据的保留期限也有所差异。 粒度较低的数据（分钟）的整理速度高于粒度较高的数据（天）。 如果由于整理导致数据在某个粒度缺失，可以在更高的粒度找到此数据。 由于 API 调用仅返回所请求的指定粒度，接收不到某个粒度的数据并不表示同一时间段的数据在更高的粒度上也不存在。
- **时区。**指标采用 UTC 时间戳存储。 汇总表按照小时时区边界聚合。 对于没有位于小时边界上的时区，数据聚合的时间可能会有所差异。

数据粒度和保留

Director 检索的 聚合数据粒度是所请求的时间 (T) 跨度的 函数。规则如下：

- 0 < T <= 1 小时采用每分钟粒度。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 0 < T <= 30 天采用每小时粒度。
- T > 31 天采用每天粒度。

非来源于聚合数据的请求数据来源于原始会话和连接信息。此数据往往增长很快，因此具有自己的整理设置。通过整理可确保仅长期保留相关数据。这样可以确保实现更好的性能，同时维护报告所需的粒度。获得 Platinum 许可的站点上的客户可以将整理保留期限更改为他们所需的保留天数，如未更改，将使用默认值。

要访问设置，请在 Delivery Controller 上运行以下 PowerShell 命令：

```
asnp Citrix.*

Get-MonitorConfiguration

Set-MonitorConfiguration -<setting name> <value>
```

采用以下 设置来控制整理：

	设置名称	受影响的整理	Platinum 默认值（天）	非 Platinum 默认值（天）
1	GroomSessionsRetentionDays	会话终止后的会话和连接记录保留期限	90	7
2	GroomFailuresRetentionDays	MachineFailureLog 和 ConnectionFailureLog 记录	90	7
3	GroomLoadIndexesRetentionDays	LoadIndex 记录	90	7
4	GroomDeletedRetentionDays	LifecycleState 状态为“Deleted”的 Machine、Catalog、DesktopGroup 和 Hypervisor 条目。	90	7

© 1999-2017 Citrix Systems, Inc. All rights reserved.

		这还将删除任何相关的 Session、SessionDetail、Summary、Failure 或 LoadIndex 记录。		
5	GroomSummariesRetentionDays	DesktopGroupSummary、FailureLogSummary 和 LoadIndexSummary records。聚合数据 - 日粒度。	90	7
6	GroomMachineHotfixLogRetentionDays	应用至 VDA 和 Controller 计算机的修补程序	90	90
7	GroomMinuteRetentionDays	聚合数据 - 分钟粒度	3	3
8	GroomHourlyRetentionDays	聚合数据 - 小时粒度	32	7
9	GroomApplicationInstanceRetentionDays	应用程序实例历史记录	90	0
10	GroomNotificationLogRetentionDays	通知日志记录	90	
11	GroomResourceUsageRawDataRetentionDays	资源利用率数据 - 原始数据	1	1
12	GroomResourceUsageMinuteDataRetentionDays	资源利用率汇总数据 - 分钟粒度	7	7
13	GroomResourceUsageHourDataRetentionDays	资源利用率汇总数据 - 小时粒度	30	7
14	GroomResourceUsageDayDataRetentionDays	资源利用率汇总数据 - 天粒度	90	7
15	GroomProcessUsageRawDataRetentionDays	进程利用率数据 - 原始数据	1	1
16	GroomProcessUsageMinuteDataRetentionDays	进程利用率数据 - 分钟粒度	3	3

© 1999-2017 Citrix Systems, Inc. All rights reserved.

17	GroomProcessUsageHourDataRetentionDays	进程利用率数据 - 小时粒度	7	7
18	GroomProcessUsageDayDataRetentionDays	进程利用率数据 - 天粒度	30	7
19	GroomSessionMetricsDataRetentionDays	会话指标数据	7	7
20	GroomMachineMetricDataRetentionDays	计算机指标数据	3	3
21	GroomMachineMetricDaySummaryDataRetentionDays	计算机指标汇总数据	90	7
22	GroomApplicationErrorsRetentionDays	应用程序错误数据	1	1
23	GroomApplicationFaultsRetentionDays	应用程序故障数据	1	1

小心：修改 Monitor Service 数据库上的值需要重新启动此服务才能使新值生效。建议仅在 Citrix 技术支持人员的指导下修改 Monitor Service 数据库。

整理保留期限注意事项：

- 获得了 Platinum 许可的站点 – 可以将上述整理保留设置更新为任意天数。
  - 异常：GroomApplicationErrorsRetentionDays 和 GroomApplicationFaultsRetentionDays 限制为 31 天。
- 获得了 Enterprise 许可的站点 – 所有站点的整理保留设置都限制为 31 天。
- 所有其他站点 – 所有站点的整理保留设置都限制为 7 天。

长期保留数据会对表格大小产生以下影响：

- **小时数据。**如果允许小时粒度的数据在数据库中最多保留两年，具有 1000 个交付组的站点将导致数据库按以下方式增长：1000 个交付组 x 24 小时/天 x 365 天/年 x 2 年 = 17,520,000 行数据。聚合表中存在如此巨大的数据量对性能的影响是非常显著的。如果从此表格提取控制板数据，将需要使用大型数据库服务器。数据量过大会对性能造成巨大影响。

- **会话和事件数据。**这是指每次启动会话和建立连接/重新连接时收集的数据。对于大型站点（10 万个用户），此数据的增长速度非常快。例如，经过两年时间，这些表格中收集的数据将超过 1 TB，这将要求使用企业级高端数据库。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

SDK 和 API

Dec 05, 2017

本版本提供多种 SDK 和 API。有关详细信息，请参阅开发人员文档。在该文档中，可以访问以下对象的编程信息：

- Delivery Controller
- Monitor Service OData
- StoreFront

Citrix Group Policy SDK 可用来显示并配置组策略设置和过滤器。它使用 PowerShell 提供程序创建与计算机和用户的设置及过滤器相对应的虚拟驱动器。提供程序以 New-PSDrive 扩展的形式显示。要使用组策略 SDK，必须安装 Studio 或 XenApp 和 XenDesktop SDK。有关详细信息，请参阅组策略 SDK。

Delivery Controller SDK

SDK 由多个 PowerShell 管理单元组成，在安装 Delivery Controller 或 Studio 组件时，安装向导会自动安装这些管理单元。

权限：必须使用拥有 Citrix 管理员权限的身份运行 shell 或脚本。尽管在 Controller 上，本地管理员组的成员自动拥有完全管理权限以允许安装 XenApp 或 XenDesktop，但 Citrix 建议，对于常规操作，应创建拥有相应权限的 Citrix 管理员，而不要使用本地管理员帐户。如果运行的是 Windows Server 2008 R2，必须以 Citrix 管理员身份运行 shell 或脚本，而不要使用本地管理员组成员身份。

访问并运行 cmdlet：

1. 在 PowerShell 中启动 shell：打开 Studio，选择 **PowerShell** 选项卡，然后单击**启动 PowerShell**。
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 -PSSnapin** cmdlet 将需要的管理单元添加到 PowerShell 环境中。

    V1 和 V2 表示管理单元的版本（XenDesktop 5 管理单元为版本 1；XenDesktop 7 管理单元为版本 2。例如，要安装 XenDesktop 7 管理单元，请键入 Add-PSSnapin Citrix.ADIdentity.Admin.V2）。要导入所有 cmdlet，请键入：Add-PSSnapin Citrix.*.Admin.V*

添加管理单元后，可以访问 cmdlet 及其关联的帮助。

注意：要查看当前的 XenApp 和 XenDesktop PowerShell cmdlet 帮助，请执行以下操作：

1. 在 PowerShell 控制台中，添加 Citrix 管理单元：Add – PSSnapin Citrix.*.Admin.V*。
2. 请按照 PowerShell 集成脚本环境 (ISE) 中的说明进行操作。

组策略 SDK

要使用组策略 SDK，必须安装 Studio 或 XenApp 和 XenDesktop SDK。

要添加组策略 SDK，请键入 **Add-PSSnapin citrix.common.grouppolicy**。（要访问帮助，请键入 **help New-PSDrive -path localgpo:/**）

© 1999-2017 Citrix Systems, Inc. All rights reserved.

要创建虚拟驱动器并加载该驱动器以及设置，请键入：New-PSDrive <*Standard Parameters*> [-PSProvider] CitrixGroupPolicy -Controller <*string*>，其中 Controller 字符串为要连接到并从中加载设置的站点中的 Controller 的完全限定域名。

© 1999-2017 Citrix Systems, Inc. All rights reserved.

针对 XenApp and XenDesktop 7.15 LTSR 的 Citrix VDI 最佳实践

Jan 19, 2018

Citrix VDI Handbook and Best Practices

In traditional business environments, workers suffer from productivity loss in many ways, including downtime during PC refreshes, patches and updates, or simply when they are away from the office. Application and desktop virtualization centralizes apps and desktops in the datacenter, rather than on local devices. This allows IT to deliver apps and desktops to users on demand, to any device, anywhere.

Take the following response from a desktop virtualization user:

Experience from the Field

"As a remote employee for [company], I struggled every time I needed to access the company's intranet, which forced me to VPN into the network. I also kept data on my local device because trying to access it over my broadband connection was too slow. Some coworkers did the same and lost data due to a virus, thankfully I was luckier.

Depending on my mood (and the weather), changing devices and locations was a challenge as I had to have my applications and data copied to many different endpoints. I know this was unsecure, but I didn't care because I was more concerned with flexibility.

Since moving to a virtual desktop, I'm able to use any device. I'm able to work from any location. And best of all, I don't have to worry about copying my data and applications onto all of my personal devices."

Unfortunately, organizations sometimes struggle to achieve this level of success. Why does one organization succeed while another organization struggles?

If we compare the factors between success and failure between desktop virtualization and other technology related projects, we see that there is little difference:

Lack of justification – Without a solid business reason, desktop virtualization is simply a new way to deliver a desktop. A business justification gives the project team a goal to strive towards.

Lack of a methodology – Many people who try and struggle to deploy a desktop virtualization solution do so because they jump right in without understanding or implementing the appropriate prerequisites. A structured methodology provides the path for the project.

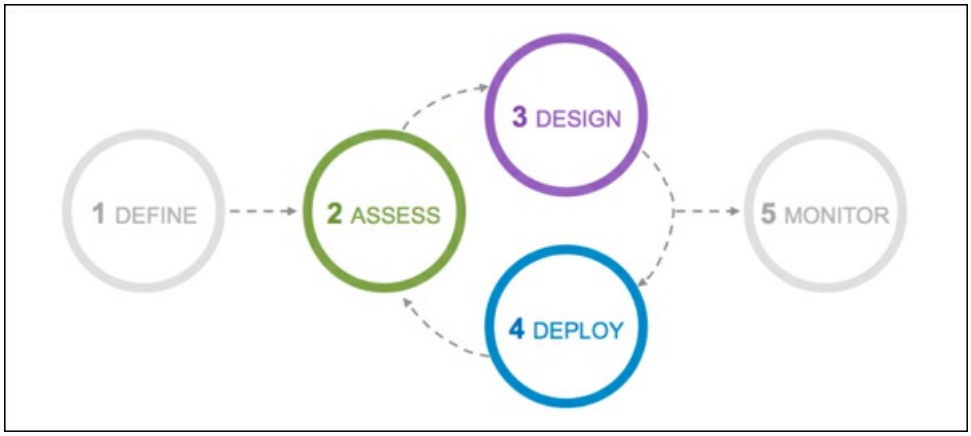
Lack of experience – For many who embark on a desktop virtualization project, there is a lack of experience, which creates a lack of confidence in the design. Architects begin to second-guess themselves and the project stalls.

Our hope is that this handbook can alleviate the anxiety associated with desktop virtualization by showing how challenges can be resolved in a manner that is technically sound, but also feasible and effective for organizations facing deadlines and other organizational challenges.

Citrix has successfully employed the methodology, experience and best practices shared within this handbook across thousands of desktop virtualization projects.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

The Citrix VDI Handbook follows the Citrix Consulting methodology. A proven methodology that has been successfully employed across thousands of desktop virtualization projects. Each phase includes guidance on the important questions to ask, what tools to use and tips to help you succeed. The Citrix Consulting methodology consists of five phases:



1. Define – Builds the business case for desktop virtualization by creating a high-level project roadmap, prioritizing activities and estimating storage and hardware requirements.

2. Assess – Key business drivers are rated so that work effort can be prioritized accordingly. In addition, the current environment is reviewed for potential problems and to identify use cases for the project. This information will be used to set the direction of the Citrix deployment, upgrade, or expansion.

3. Design – Define architecture required to satisfy key business drivers and success criteria identified during the assess phase. Topics such as environment scalability, redundancy and high availability are addressed.

4. Deploy – During the deploy phase, the infrastructure is installed and configured as described in the design phase. All components of the infrastructure should be thoroughly unit and regression tested before users are provided with access to the environment.

5. Monitor – Define architectural and operational processes required to maintain the production environment.

The Citrix Consulting methodology follows an iterative Assess > Design > Deploy process for each major initiative of your project. In doing so, your organization is left with tangible improvements to the environment at the end of each engagement. For example, high priority user groups can progress through the assess, design and deploy phases earlier than other user groups.

> **注意**
>
> The VDI Handbook provides content on the Assess, Design and Monitor phases of the Citrix Consulting methodology.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

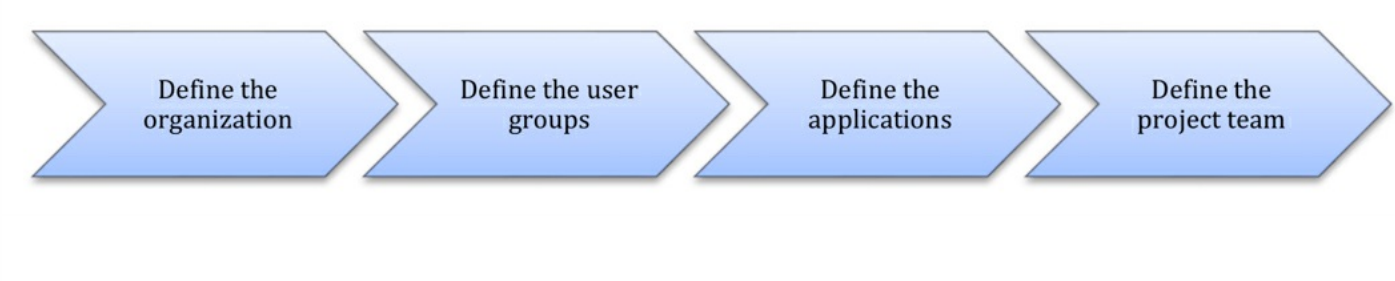
评估

Jan 29, 2018

Creating an app and desktop delivery solution begins with a proper assessment. Architects that fail to properly assess the current environment find that they require the assess information later on, forcing them to backtrack, which can potentially stall and put the project at risk.

By gathering all of the information from the outset, the architect will gain an appreciation for the current environment and be able to work from the beginning on properly aligning business and user requirements with the overall solution.

The assess phase is a four-step, simple to follow process:



The first step in your virtual desktop project should be to understand and prioritize the strategic imperatives of the organization. This enables the project management team to define success criteria and allows the design team to create a tailored and optimized architecture.

Requirements can be captured during meetings or by distributing questionnaires. Meetings are more time consuming, but allow for follow-up questions to be asked and help to simplify the prioritization process. It is important that this exercise be completed jointly by both business managers and IT decision makers since both groups will have significantly different viewpoints.

Take the following examples of what certain organizations faced, which drove their selection of desktop virtualization.

Experience from the Field

- Finance – A large financial institution had a base of operations in the city designated as the host city for an upcoming G8 summit. As these types of meetings historically include riots, protests and other issues that can disrupt business and the safety of their employees, the financial organization needed an alternative allowing their users to work from the safety of their homes.
- Agriculture – Due to thin margins, an agriculture organization wanted to save money by extending the life of desktop PCs while still being able to run the latest applications.
- Healthcare – A large healthcare organization was in need of a solution to simplify application updates as the main application required updates on a weekly basis. Due to the distributed nature of the endpoint devices, the organization was in need of a better application delivery solution.

These are just a few examples, but they demonstrate how organizations think about their priorities. Most organizations do not focus on technology, they focus on the needs of the user and of the organization. These needs can be met with technical solutions but it is imperative the team understands the “Why” of the project.

In addition to the three real-world examples, the following table identifies a few other priorities often stated from many

© 1999-2017 Citrix Systems, Inc. All rights reserved.

organizations:

Requester	Requirement
Business Managers	**Better IT agility and responsiveness** – Flexible desktop solution that is capable of accommodating periods of change such as rapid growth or downsizing. For example, enabling the business to setup project offices or temporary points of sale very rapidly without long delays, hardware acquisitions or IT notification periods. **Bring your own device** – Empower employees to choose their own devices to improve productivity, collaboration and mobility. **Collaboration** – With an increase in both globalization and mobility, team members are often dispersed across multiple physical locations. Powerful collaboration capabilities are required to ensure high levels of productivity, efficiency and quality. **Work from anywhere** – The business needs to support home workers in order to attract and retain top talent, and / or travelling employees
IT decision makers	**Better desktop management** – Simplify the management of desktop infrastructure. IT is not as proactive as they would like and spend too much time "fighting fires". **Increase security** – Data theft or the loss of devices containing sensitive data is a big risk and preventive measures are a top priority. **Extend desktop hardware lifecycle** – Replacing workstations every three to five years in order to keep up with the requirements of the operating system or the applications has been very costly. **Reducing IT Management Scope** – Improve IT efficiency by focusing on only the aspects driving the business while offloading remaining functions to 3rd parties via cloud or service providers. **Improving user experience** - Increasing performance or enabling features which would otherwise not be possible with a geographically dispersed user population

The prioritization process should be completed in collaboration with the project team, business managers and IT managers so that all views are considered.

Although there are multiple approaches towards defining user groups, it is often easiest to align user groups with departments as most users within the same department or organizational unit consumes the same set of applications.

Depending on the size of the department, there might be a subset of users with unique requirements. Each defined user group should be evaluated against the following criteria to determine if the departmental user group needs to be further divided into more specialized user groups.

- Primary datacenter – Each user will have a primary datacenter or cloud resource location assigned that will be used to host their virtual desktop, data, and application servers. Identify the datacenter that the user should be assigned to rather than the datacenter they are currently using. Users will be grouped based on their primary datacenter so that a unique design can be created for each one.
- Personalization – Personalization requirements are used to help determine the appropriate VDI model for each user group. For example, if a user group requires complete personalization, a personal desktop will be recommended as the optimal solution. There are three classifications available:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Personalization	Requirement
None	User cannot modify any user or application settings, for example - kiosk.
Basic	User can modify user-level settings of desktops and applications.
Complete	User can make any change, including installing applications.

- Security – Security requirements are used to help determine the appropriate desktop and policy (or policies) for each user group. For example, if a user group requires high security, a hosted pooled desktop or a local VM desktop will be recommended as the optimal solution. There are three classifications available:

Security level	Description
Low	Users are allowed to transfer data in and out of the virtualized environment.
Medium	All authentication and session traffic should be secured; users should not be able to install or modify their virtualized environment.
High	In addition to traffic encryption, no data should leave the data center (such as through printing or copy/paste); all user access to the environment should be audited.

- Mobility – Mobility requirements are used to help determine the appropriate desktop model for each user group. For example, if a user group faces intermittent network connectivity, then any VDI model requiring an active network connection is not applicable. There are four classifications available:

Mobility	Requirement
Local	Always uses the same device, connected to an internal, high-speed and secured network.
Roaming Local	Connects from different locations on an internal, high-speed, secured network.
Remote	Sometimes connects from external variable-speed, unsecure networks.
Mobile	Often needs access when the network is intermittent or unavailable.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Desktop Loss Criticality – Desktop loss criticality is used to determine the level of high availability, load balancing and fault tolerance measures required. For example, if there is a high risk to the business if the user's resource is not available, the user should not be allocated a local desktop because if that local desktop fails, the user will not be able to access their resources. There are three classifications available:

Desktop loss criticality	Requirement
Low	No major risk to products, projects or revenue.
Medium	Potential risk to products, projects or revenue.
High	Severe risk to products, projects or revenue.

- Workload – Types and number of applications accessed by the user impacts overall density and the appropriate VDI model. Users requiring high-quality graphics will either need to utilize a local desktop implementation or a professional graphics desktop. There are three classifications available:

User type	Characteristics
Light	1-2 office productivity apps or kiosk.
Medium	2-10 office productivity apps with light multimedia use.
Heavy	Intense multimedia, data processing or application development.

> **注意**
>
> Performance thresholds are not identified based on processor, memory or disk utilization because these characteristics will change dramatically following the application rationalization and desktop optimization process. In addition, it is likely that the user's management tools and operating system will change during the migration process. Instead, workload is gauged based on the number and type of applications the user runs.

Experience from the Field

- Utility company – A large utility company collected data on every user in their organization. During the user segmentation process, it was realized that the organization's existing role definitions were sufficiently well defined that all the users within a role shared the same requirements. This allowed a significant amount of time to be saved by reviewing a select number of users per group.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Government – A government organization discovered that there was significant deviation between user requirements within each role, particularly around security and desktop loss criticality. As such, each user needed to be carefully reviewed to ensure that they were grouped appropriately.

As with physical desktops, it is not possible to meet every user requirement with a single type of VDI. Different types of users need different types of resources. Some users may require simplicity and standardization, while others may require high levels of performance and personalization. Implementing a single VDI model across an entire organization will inevitably lead to user frustration and reduced productivity.

Citrix offers a complete set of VDI technologies that have been combined into a single integrated solution. Because each model has different strengths, it is important that the right model is chosen for each user group within the organization.

The following list provides a brief explanation of each VDI model.

- Hosted Apps – The hosted apps model delivers only the application interface to the user. This approach provides a seamless way for organizations to deliver a centrally managed and hosted application into the user's local PC. The Hosted Apps model is often utilized when organizations must simplify management of a few line-of-business applications. Hosted apps includes a few variants:
  - Windows Apps – The Windows apps model utilizes a server-based Windows operating system, resulting in a many users accessing a single VM model.
  - VM Hosted Apps – The VM hosted apps model utilizes a desktop-based Windows operating system, resulting in a single user accessing a single VM model. This model is often used to overcome application compatibility challenges with a multi-user operating system, like Windows 2008, Windows 2012 and Windows 2016.
  - Linux Apps – The Linux apps model utilizes a server-based Windows operating system, resulting in a many users accessing a single VM model.
  - Browser Apps – The browser apps model utilizes a server-based Windows operating system to deliver an app as a tab within the user's local, preferred browser. This approach provides a seamless way for organizations to overcome browser compatibility challenges when users want to use their preferred browser (Internet Explorer, Microsoft Edge, Google Chrome, Mozilla Firefox, etc.) but the web application is only compatible with a specific browser.
- Shared Desktop – With the shared desktop model, multiple user desktops are hosted from a single, server-based operating system (Windows 2008, 2012, 2016, Red Hat, SUSE, CentOS and Ubuntu). The shared desktop model provides a low-cost, high-density solution; however, applications must be compatible with a multi-user server based operating system. In addition, because multiple users share a single operating system instance, users are restricted from performing actions that negatively impact other users, for example installing applications, changing system settings and restarting the operating system.
- Pooled Desktop – The pooled desktop model provides each user with a random, temporary desktop operating system (Windows 7, Windows 8 and Windows 10). Because each user receives their own instance of an operating system, overall hypervisor density is lower when compared to the shared desktop model. However, pooled desktops remove the requirement that applications must be multi-user aware and support server based operating systems.
- Personal Desktop – The personal desktop model provides each user with a statically assigned, customizable, persistent desktop operating system (Windows 7, Windows 8, Windows 10, Red Hat, SUSE, CentOS and Ubuntu). Because each user receives their own instance of an operating system, overall hypervisor density is lower when compared to the shared desktop model. However, personal desktops remove the requirement that applications must be multi-user aware and support server based operating systems.
- Pro Graphics Desktop – The pro graphics desktop model provides each user with a hardwarebased graphics processing unit (GPU) allowing for higher-definition graphical content.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Local Streamed Desktop – The local streamed desktop model provides each user with a centrally managed desktop, running on local PC hardware.
- Local VM Desktop – The local VM desktop model provides each user with a centrally managed desktop, running on local PC hardware capable of functioning with no network connectivity.
- Remote PC Access – The remote PC access desktop model provides a user with secure remote access to their statically assigned, traditional PC. This is often the fastest and easiest VDI model to deploy as it utilizes already deployed desktop PCs.

Each user group should be compared against the following table to determine which VDI model best matches the overall user group requirements. In many environments, a single user might utilize a desktop VDI model and an app VDI model simultaneously.

In this table:

- Y indicates "Recommended"
- N indicates "Not Recommended"
- o indicates "Viable"

Segmentation Characteristic	Hosted Apps	Hosted Shared Desktop	Hosted Pooled Desktop	Hosted Personal Desktop	Hosted Pro Graphics Desktop	Local Streamed Desktop	Local VM Desktop	Remote PC Access
Workload								
Light	Y	o	o	o	N	o	o	o
Medium	o	Y	Y	o	o	o	o	o
Heavy	N	N	N	o	Y	Y	Y	o
Mobility								
Local	Y	Y	Y	o	o	Y	o	o
Roaming Local	Y	Y	Y	o	o	N	o	o
Remote	Y	Y	Y	o	o	N	o	Y
Mobile	N	N	N	N	N	N	Y	N
Personalization								

© 1999-2017 Citrix Systems, Inc. All rights reserved.

None	Y	Y	Y	N	o	o	o	o
Basic	Y	Y	Y	N	o	o	o	o
Complete	N	N	N	Y		N	Y	Y
	Security							
Low	o	o	o	o	o	o	o	o
Medium	Y	Y	Y	o	o	o	o	o
High	o	o	Y	N	o	Y	Y	N
	Desktop Loss Criticality							
Low	o	o	o	o	o	o	o	o
Medium	Y	Y	Y	o	o	o	o	N
High	Y	Y	Y	N	o	o	N	N

Don't forget to follow these top recommendations from Citrix Consulting based on years of experience:

Citrix Consulting Tips for Success

1. Start with Windows apps, shared and pooled desktops – As you can see in the VDI capability table above, the Windows apps, hosted shared and pooled desktop models can be used in the majority of situations. The local streamed and local VM desktop models should only be used on an exception basis. By reducing the number of VDI models required, you will help to reduce deployment time and simplify management.
2. Perfect match – It may not be possible to select a VDI model that is a perfect match for the user group. For example, you can't provide users with a desktop that is highly secure and offers complete personalization at the same time. In these situations, select the VDI model which is the closest match to the organization's highest priorities for the user group.
3. Desktop loss criticality – There are only three VDI models that meet the needs of a high desktop loss criticality user group (backup desktops available) – none of which allow for complete personalization. If a high-desktop loss criticality user group also requires the ability to personalize their desktop they could be provided with a pool of backup desktops (hosted shared, pooled) in addition to their primary desktop. Although these desktops would not include customizations made to their primary desktop, they would allow users to access core applications such as mail, Internet and Microsoft Office.
4. Consider Operations & Maintenance – The ongoing support of each VDI model should be factored in when deciding on a VDI model. For example, pooled desktops can be rebooted to a known good state which often leads to reduced

© 1999-2017 Citrix Systems, Inc. All rights reserved.

maintenance versus a personal desktop where each desktop is unique.

Once the users have been divided up in to groups the next step is to determine which applications they require. This is a two-step process:

1. Application rationalization – Help to simplify the application assessment by removing redundant applications from the inventory that were captured during the data capture.

2. Link apps to users – Use the results from the data capture process to map applications to user groups.

The number of applications identified during the inventory is often surprising, even for organizations that believe they have a high-level of control over applications. To help reduce complexity as well as overall time required, it's important to take the time to consolidate the list of applications. The following guidelines will help ensure that your application list is consolidated appropriately:

- Multiple versions – Different versions of the same application may have been identified during the inventory. There are various reasons for this, including an inconsistent patching or upgrade process, decentralized application management, limited licenses and situations where users require specific application versions for compatibility with other applications, macros and document formats. Where possible, work with the application owners to reduce the number of versions required. The leading practice is to standardize on a single version of each application, typically the latest.
- Non-business applications – Applications that are not required by the business should be removed from the application inventory to reduce resource requirements and to help simplify the overall project. Non-business related applications are typically found in an application inventory when users have been provided with the ability to install their own applications and typically include games, communication clients, screen savers, peripheral software and media players.
- Legacy applications – The inventory may identify legacy applications that have since been retired or that are no longer required within the business. These applications may not have been removed from the desktops because there is no established process to do so or because there are always more high-priority activities to complete. These applications should be consolidated during the rationalization stage of the application assessment.
- Management applications – The antivirus, application delivery, monitoring, inventory, maintenance and backup applications will be completely re-designed across the organization during the desktop virtualization project. These applications should also be consolidated during this stage.

Experience from the field:

Government: A government organization identified that there were 2,660 applications installed across their desktop estate. Most of which were installed by users with local administrative rights. By following the application rationalization recommendations above, it was possible to reduce the number of applications required to 160.

Each application included in the project should be categorized based on certain criteria, which will help determine the most appropriate way to host and integrate the app. Each application can be installed directly into the image, virtualized in an isolated container and streamed to the desktop (Microsoft App-V), captured in a unique layer and attached to the virtual machine (Citrix App Layering) or installed locally on the user's endpoint device and seamlessly integrated into the user's virtual desktop (Citrix Local App Access). Due to the uniqueness of every application, many large-scale deployments simultaneously utilize multiple approaches. Each application should be categorized as follows:

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

- Common Apps - Every organization includes a suite of applications utilized by almost every user, Microsoft Office for example. This suite of applications is often the most utilized application in a desktop VDI model.
- Departmental Apps - A certain set of applications are only relevant for a unique business unit or department. For example, an engineering department will often require software development applications.
- User Apps - Often making up the largest grouping of apps are the apps used by very few individual users. In a traditional PC implementation, these applications are installed by the user as a temporary requirement or a personal requirement, often not directly impacting the business.
- Management Apps – Many desktop deployments include a combination of antivirus, monitoring, inventory, maintenance and backup applications. Many of these applications have unique virtualization requirements and are often required across the entire organization.

Workload	Requirement
Resource intensive	Application requires 1 GB or more of RAM or averages 50% or more CPU utilization.
None	The application is not resource intensive.

The following characteristics should be identified for each application so that the right application delivery model can be selected during the design phase of the project:

- Complex – An application should be classified as complex or technically challenging if it is difficult to set up, has extensive dependencies on other applications or requires a specialized configuration, for example an Electronic Medical Records (EMR) application. Complex applications need to be identified during the application assessment because they are not generally appropriate for installation in a pooled/personal desktop model or delivery by application streaming. Delivering complex applications as a hosted app often helps to reduce the complexity of the base desktop image.
- Demanding – Collecting application resource requirements allows the virtualization infrastructure to be sized and an appropriate application delivery model to be selected. For example, demanding or resource intensive applications will not be delivered via a pooled/personal desktop model because there is limited control over how the resources are shared between users. There are two classifications available in the user assessment worksheet:

- Mobile – Some user groups may require the ability to work while mobile, sometimes when offline. If so, it is important that the design can determine which applications will work without a network connection and which ones will not. Applications that require backend infrastructure such as web and database servers are not typically available offline.
- Peripherals – If applications require connectivity with peripheral devices, identify the interface required so that it can be made available to the application when it is run from a virtual session.
- Restrictions – Application access may need to be restricted due to insufficient licenses /resources and to protect sensitive data / tools. For example, applications with a limited number of licenses should not be installed on a base image that is shared with unlicensed users. There are three restricted access categories in the application assessment workbook:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Restricted Access	Requirement
No	There are no restrictions for the application and it can be accessed by any user within the organization.
User Group	The application may be installed on a multi-user operating system but only a specific group of users should be provided with an icon.
Virtual machine	Application should only be installed on a virtual machine that is accessible by authorized users, often because of licensing requirements.

Desktop virtualization is a fundamental change that requires close collaboration between various business and technical teams in order to be successful. For example, the virtualization and desktop teams need to work together to ensure that the virtual desktop image meets user needs while also being optimized for the datacenter. Failure to build a cohesive project team that consists of the right roles and skillsets can negatively impact performance, availability, user experience and supportability while also increasing costs and risk.

The following tables identify the business and technical roles required during an enterprise virtual desktop deployment. Although the list may seem quite large, many of these roles are only required for a short time and multiple roles may be performed by a single person. The project manager and Citrix architect are considered to be full time roles with other team members being brought in only when required. The project manager role is key to ensuring that the right people are involved in the project at the right time.

Role	Description	Example Responsibilities
Project sponsor	The project sponsor is a senior company executive who recognizes the benefits that desktop virtualization will bring to the business. The project sponsor role is often performed by the chief technology officer (CTO).	**Pre-project** • Promote desktop virtualization within business. • Identify members of the steering committee. **Secure funding** • Assess general costs associated with solution. • Identify and prioritize key business drivers.
		All steps • Define key project

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Role	Description	Example Responsibilities
Project manager	The project manager directs the project team and is responsible for ensuring that project objectives are completed on time and within budget.	• Create and update project plan. • Track progress against plan. • Track expenditure against budget. • Maintain issue and risk register. • Manage scope changes. • Create weekly project reports. • Brief steering committee on progress. • Organize project workshops and meetings. • Ensure project teams are synchronized. • Ensure pre-requisites are in place. • Creates change control requests.
Business manager	Depending on company structure and size, business managers oversee planning and performance at a department, region or company level. A business manager understands the requirements necessary for their employees to be successful.	Assess • Assist with application consolidation project. • Provide details on connectivity requirements of user group, including offline usage. • Provide details on risk tolerance of user group. • Identify requirements for peripherals. Deploy • Promote benefits of desktop virtualization. • Assist with coordinating the rollout.
		Assess • Provide Citrix architect with detailed understanding of the current business

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Role	Description	Example Responsibilities
Business continuity manager	The business continuity manager ensures that an organization can continue to function after a disruptive event such as natural disaster, crime or human/computer error.	**Design** • Update business continuity plan to incorporate the new Citrix infrastructure. **Deploy** • Test business continuity plan.
Test manager	The test manager is responsible for ensuring that the test and user acceptance environments match the production environment as closely as possible. The test manager helps to reduce risk by ensuring that changes are fully tested before being implemented in production.	**Assess** • Provide Citrix architect with detailed understanding of current testing infrastructure and processes. **Design** • Work with Citrix architect to design an appropriate testing infrastructure and test plan for new Citrix environment. **Deploy** • Ensure that testing design is implemented correctly and new Citrix infrastructure is fully tested before rollout.
Application owners	An application owner is a subject matter expert on specific applications deployed within the business. Application owners are responsible for ensuring that problems with the applications are resolved and that upgrades/updates are performed without issue. Application owners are also responsible for managing support agreements with the application vendors.	**Assess** • Assist with application consolidation project. • Identify application licensing limitations. • Provide details on security restrictions. • Provide details on application dependencies. • Provide location of backend resources. **Deploy** • Provide installation pre-requisites and install guide

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Role	Description	Example Responsibilities
		installing and testing applications in VDI environment
Service desk manager	The service desk manager helps to improve productivity and end-user satisfaction by ensuring that production issues are logged, escalated and resolved in a timely manner. The service desk manager is also responsible for reporting on common issues, call volumes and service desk performance.	**Assess** • Identify common issues with existing environment. • Provide details on support tools currently used. **Design** • Assist Citrix architect with designing a delegated administration model. • Participate in operations and support design workshops. • Work with training manager to identify training requirements. **Deploy** • Monitor helpdesk calls for rollout related issues.
Training manager	The training manager ensures that support staff and end-users are proficient with new areas of technology. The training manager also has responsibility for ensuring that the training plan is up-to-date and followed appropriately.	**Assess** • Determine current skill set for support staff and end users. **Design** • Create training plan for support staff and end users. **Deploy** • Implement training plan for support staff and end users.
		Design • Work with project manager to create communications plan. **Deploy**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Role	Description	Example Responsibilities
		• desktop virtualization. • Inform users of key migration dates. • Ensure expectations are set accordingly.

Technical Roles

Role	Description	Example Responsibilities
Citrix desktop architect	The Citrix architect acts as the design authority for all Citrix products and liaises with other architects to ensure that the Citrix infrastructure is successfully integrated into the organization.	**Assess** • Work with project sponsor and key stakeholders to identify and prioritize key business drivers. • Oversee user segmentation and app. assessment. • Map VDI models to user groups. • Perform capabilities assessment to determine current state of readiness. • Identify areas of risk and provides remedial actions. **Design** • Create Citrix design that includes hardware and storage estimates. • Coordinate with other architects to integrate Citrix infrastructure into organization. • Work with monitoring architect to ensure that Citrix environment is monitored appropriately. • Create operations and support design. • Create implementation and rollout design. • Create test plan **Deploy** • Ensure that the Citrix environment is implemented in accordance with design. • Verify that implementation passes test plan. • Ensure that the Citrix design is implemented correctly.
Archive directory architect	Design authority on Microsoft Active Directory, including Organizational Units (OU) and Group Policy Objects (GPOs).	**Assess** • Provide Citrix architect with detailed understanding of current Active Directory architecture. **Design** • Work with the Citrix architect to design OU structure, group policies, permissions, service accounts, etc. for new Citrix environment. • Update Active Directory infrastructure design to reflect centralization of user data and accounts. **Deploy**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

		correctly.
Role	Description	Example Responsibilities
Visualization architect	Design authority on server and desktop virtualization using Citrix XenServer, Microsoft Hyper-V, Nutanix Acropolis or VMware vSphere.	**Assess** • Provide Citrix architect with detailed understanding of current virtualization architecture **Design** • Work with Citrix architect to design hardware, networking, storage, high availability, etc. for server and desktop virtualization • Work with monitoring architect to ensure that virtualization environment is monitored appropriately **Deploy** • Ensure that the virtualization design is implemented correctly
Network architect	Design authority on networking, including routing, VLANs, DHCP, DNS, VPN and firewalls.	**Assess** • Provide Citrix architect with detailed understanding of current networking architecture. **Design** • Work with Citrix architect to design physical network, virtual networks, routing, firewalls, quality of service, remote access, network optimization, etc. for new Citrix environment. • Work with monitoring architect to ensure that network is monitored appropriately. **Deploy** • Ensure that network design is implemented correctly.
Desktop architect	Design authority on Microsoft desktop operating systems, including Windows XP, Windows 7 and Windows 8.	**Assess** • Provide Citrix architect with detailed understanding of current desktop environment. **Design** • Work with Citrix architect to design core desktop virtual image, core applications, desktop optimizations, etc. for new Citrix environment. • Work with monitoring architect to ensure that the virtual desktops are monitored appropriately. **Deploy** • Ensure that desktop design is implemented correctly.
		Assess • Provide Citrix architect with detailed understanding of current shared storage environment.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Role	Description	Example Responsibilities
Storage architect	Design authority on storage solutions, including directattached storage, storageattached networks and network attached storage.	• Work with Citrix architect to design storage architecture, tiers, sizing, connectivity, etc. for new Citrix environment. • Work with monitoring architect to ensure that storage is monitored appropriately. **Deploy** • Ensure that storage design is implemented correctly.
Backup architect	Design authority on backup and recovery, including virtual machines, desktops, servers, user data and databases.	**Assess** • Provide Citrix architect with detailed understanding of current backup architecture and processes **Design** • Work with Citrix architect and disaster recovery architect to design backup architecture, process, schedule, retention, etc. for new Citrix environment **Deploy** • Ensure that backup design is implemented correctly
Application package architect	Design authority on packaging applications for deployment via the systems management team	**Assess** • Provide Citrix architect with detailed understanding of current application packaging process and status **Deploy** • Ensure that all required applications are packaged according to design
Monitoring architect	Design authority on monitoring, including hardware, network, servers, storage and security appliances.	**Assess** • Provide Citrix architect with detailed understanding of current monitoring architecture and processes. **Design** • Work with Citrix architect to design monitoring architecture, metrics, alerts, etc. for new Citrix environment and supporting infrastructure. **Deploy** • Ensure that monitoring design is implemented correctly. • Provide regular reports on capacity and trends during rollout .
System management	Design authority on systems management, including server/desktop build process, patching and automated	**Assess** • Provide Citrix architect with a detailed understanding of the current systems management processes. **Design** • Works with Citrix architect to define server/desktop build process, patching and application delivery

© 1999-2017 Citrix Systems, Inc. All rights reserved.

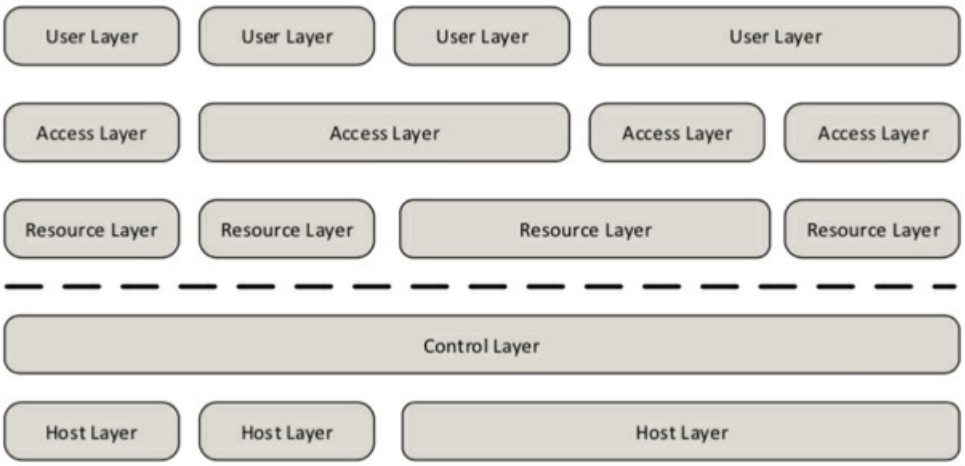
Role	Description	Example Responsibilities
		Deploy • Ensure that the systems management design is implemented correctly.
Security architect	Design authority on security, including desktops, servers, networks and VPNs.	Assess • Provide Citrix architect with detailed understanding of current security policy. Design • Work with Citrix architect to design security standards for new Citrix environment, including authentication, encryption, port numbers, firewall rules, etc. Deploy • Ensure that security design is implemented correctly.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

设计

Jan 30, 2018

Designing a desktop virtualization solution is simply a matter of following a proven process and aligning technical decisions with organizational and user requirements. Without the standardized and proven process, architects tend to randomly jump from topic to topic, which leads to confusion and mistakes. The recommended approach focuses on working through five distinct layers:



The top three layers are designed for each user group independently, which were identified during the user segmentation section of the assess phase. These layers define the users' resources and how users access their resources. Upon completion of these three layers, the foundational layers (control and hardware) are designed for the entire solution.

This process guides the design thinking in that decisions made higher up impact lower level design decisions.

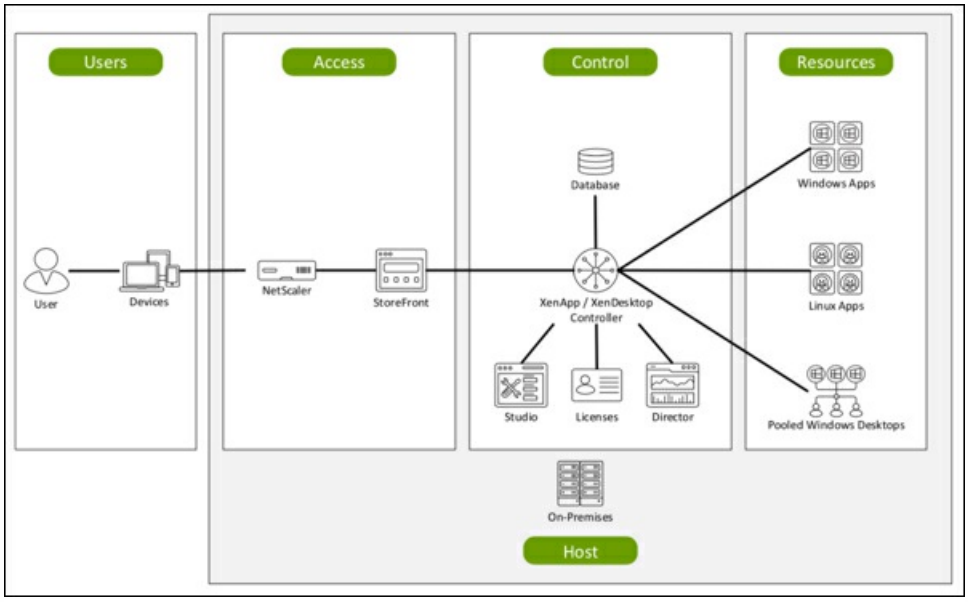
The conceptual architecture helps define the overarching strategies for the entire solution based on business objectives and organizational structure.

Although an organization's conceptual architecture will change over the coming years, it is worthwhile to start the design phase by defining the long-term objectives around delivery models and the physical, geographical distribution of solution.

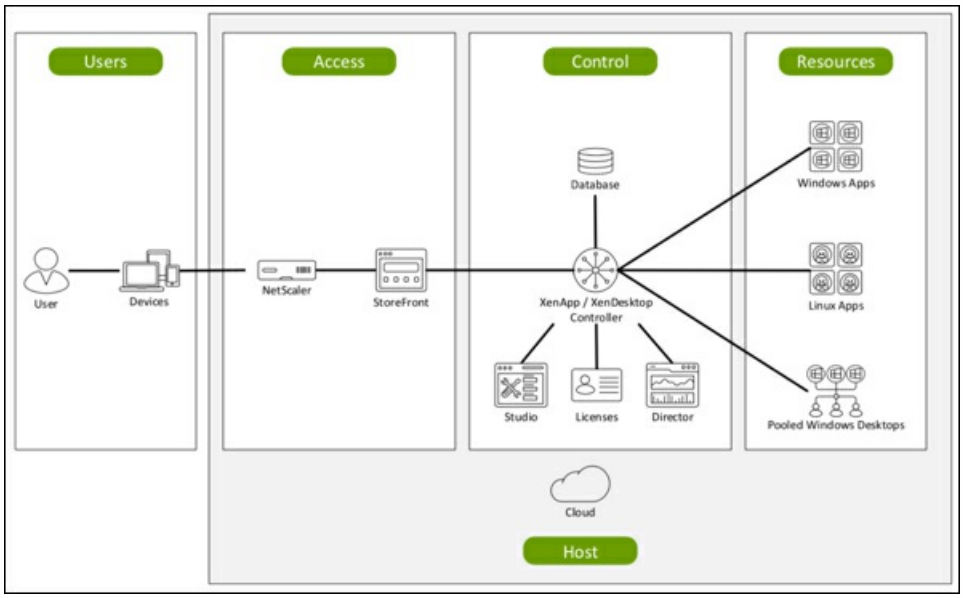
A XenDesktop and XenApp solution can take on many delivery forms. The organization's business objectives help select the right approach. Even though the infrastructure remains the same for all delivery models, the local IT team's management scope changes.

- **On Premises** - All components hosted from the organization's local data center. The onpremises model requires the local IT team to manage every aspect of the solution.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

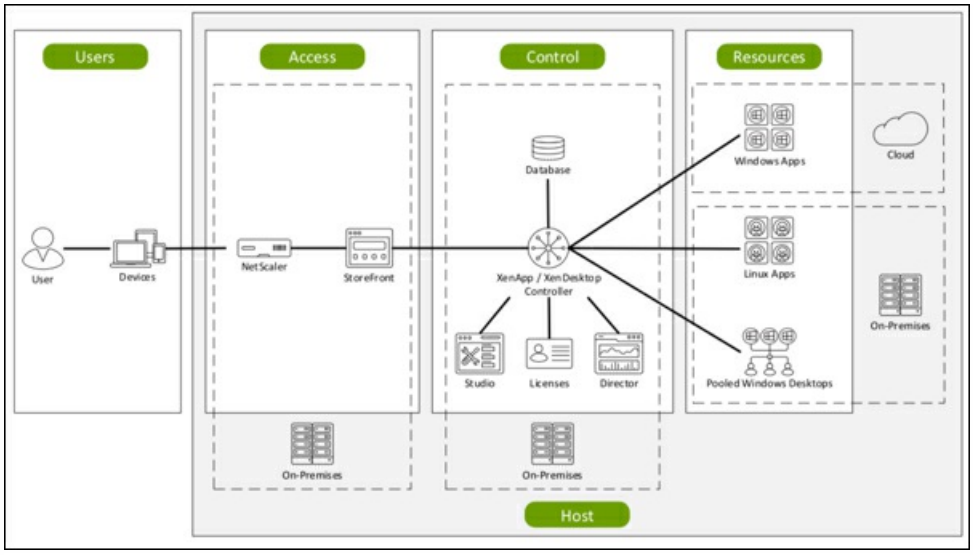


- **Public Cloud** - All components hosted from a public cloud infrastructure using Infrastructure as a Service (IaaS). The public cloud model eliminates hardware management from the local IT team's management scope.

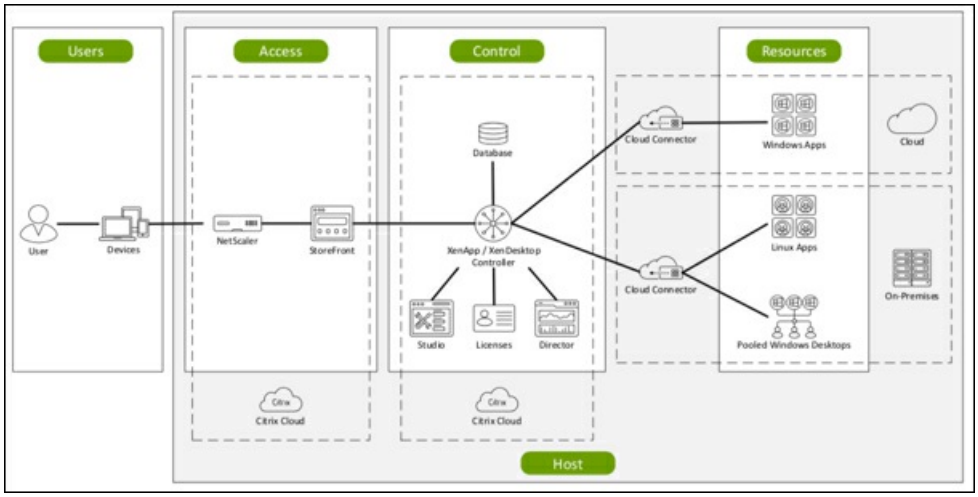


- **Hybrid Cloud** - A single implementation executes from an on-premises data center as well as the public cloud. Even though components of the solution are using different hosting providers, the entire solution is a single solution using the same code and managed as a single entity. The local IT team continues to manage all aspects of the solution except for the hardware associated with the cloud-hosted resources.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



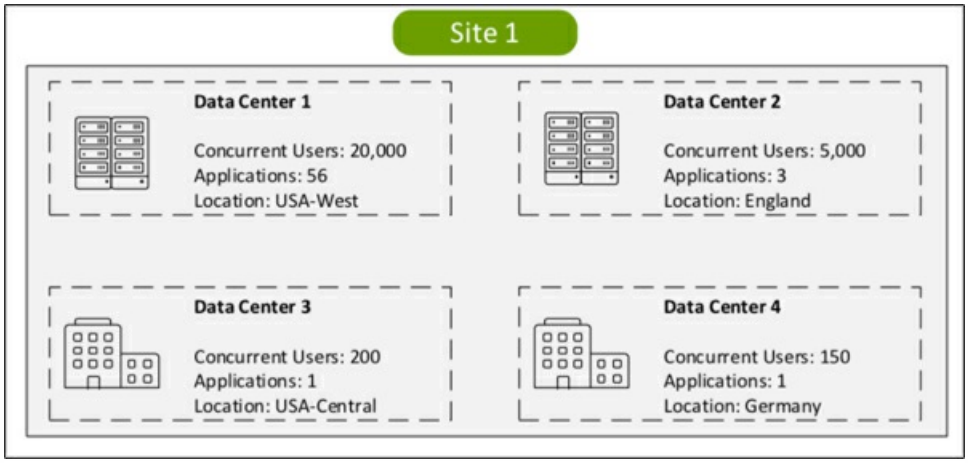
- **Citrix Cloud** - The XenApp and XenDesktop Service offering from Citrix Cloud breaks a typical deployment into multiple management domains. The access and control layer components are hosted and managed in the Citrix cloud by Citrix while the resource layer components continues to be managed by the local IT team either as an on-premises, public cloud or hybrid cloud model. Citrix manages the hardware, sizing and updates to the access and control components while the local IT team manages the resources. In addition, if the public cloud hosts the resources, the local IT team does not have to manage the resource hardware. Citrix Cloud continues to expand the number of offerings to help solve specific user cases. To learn more and understand the full array of offerings, please explore the workspace services within the Citrix Cloud.

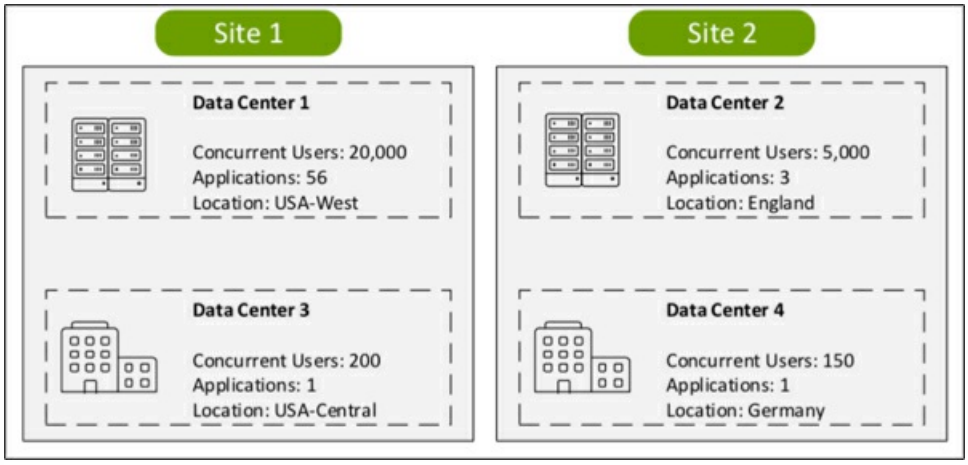


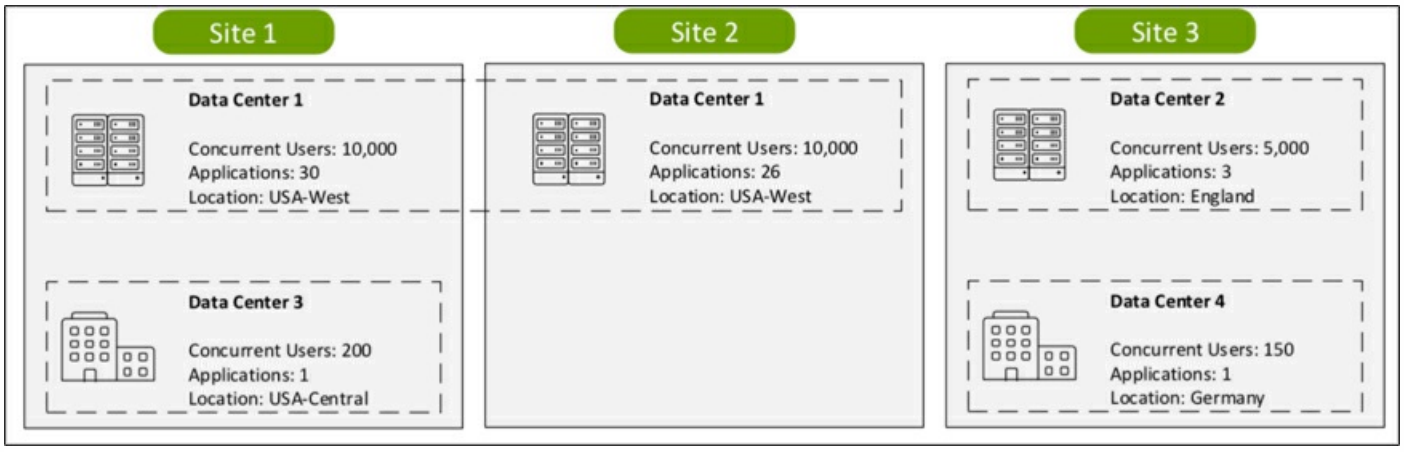
A XenApp and XenDesktop site groups desktops and applications together to form a single architectural and management entity. All persistent and dynamic data for the site, including site configuration, desktop assignments, and session state, is stored in a site's database.

A site can be contained within a single location, span across multiple locations or be a partial location. Through rigorous testing, a single XenApp/XenDesktop site can support 40,000 or more concurrent sessions.

© 1999-2017 Citrix Systems, Inc. All rights reserved.







Zones subdivide single sites, often associated with geographical locations. There are several factors to consider when determining the overall topology of the XenApp and XenDesktop solution:

- **Risk Tolerance** – Create multiple XenDesktop sites to minimize the impact from a site-wide outage. For example, corruption of the XenDesktop site database could affect site-wide availability. For many organizations, the decreased risk from implementing multiple sites outweighs the additional management overhead and supporting infrastructure required.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Experience from the Field

Finance – A large financial institution hosts 10,000 desktops from a single datacenter. To reduce risk, it was decided that no site should exceed 5,000 desktops. Therefore, despite the desktops being connected by a fast and redundant network, two sites were created.

- **Security** – Although delegated administration is available, high-security organizations may require complete separation between environments to demonstrate compliance with specific service level agreements.

Experience from the Field

Retail – A retail organization required complete separation for employees responsible for managing financial data. To meet this requirement, two separate sites were created within the same datacenter – one for t he financial employees and a second for all other employees.

- **Administrative Boundaries** – Due to billing/charge back requirements or how IT is structured, multiple sites might be required to separate administrative boundaries.
- **Geographical Connectivity** – Although the implementation of zones does allow a single site to span geographical locations, there must be enough bandwidth between the satellite zone and primary zone for the site database to capture the session information. Higher latency or larger zones impacts response times for the user.

Variable	XenApp and XenDesktop 7.13	XenApp and XenDesktop 7.11
Latency (ms)	90	250
Concurrent requests	48	48
Average response time	3.7	7.6
Brokering requests per second	12.6	6.3
Time to launch 10,000 users	13 minutes	26 minutes

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Session count	Max concurrent sessions launches	Min site-to-site bandwidth	Max site-to-site round trip latency
Less than 50	20	1 Mbps	250 ms
50 to 500	25	1.5 Mbps	100 ms
500 to 1,000	30	2 Mbps	50 ms
1,000 to 3,000	60	8 Mbps	10 ms
Over 3,000	60	8 Mbps	5 ms

In general, administrators should minimize the number of XenDesktop sites and zones to reduce architectural complexity and administrative effort.

A XenApp and XenDesktop solution requires the creation and management of master images. Organizations must decide early what strategy to pursue for image management.

Installed Images

An installed image requires the administrator to install the operating system and applications for each image. This approach is straightforward but creates a duplication of effort as the admin installs the same operating system and core applications across multiple master images.

Maintaining master images also includes duplication of effort as the same operating system version and core applications are part of multiple images, each requiring the same update process.

Scripted Images

Administrators can automate many of the tasks associated with installed images with scripting or automation tools. Many operating system and application installs support automated scripting, which mitigates the duplication of effort impact on the administrator's time with installed images.

Unfortunately, learning, creating, and maintaining a scripting framework for the entire image is challenging and time consuming. Scripting an entire build takes time and often results in unexpected failures if directory structures change, processes take too long to complete or a filename changes.

Layered Images

Each unique operating system (Windows 10, Windows 2012R2 and Windows 2016), platform (XenApp/XenDesktop 7.13 VDA, XenApp/XenDesktop 7.14 VDA and XenApp/XenDesktop 7.15 VDA) and application (Microsoft Office, Adobe Acrobat, Google Chrome and Mozilla Firefox) is a layer. A master image is the merging of one operating system layer, one platform and many applications.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

A layered image approach eliminates the duplication of effort challenges associated with installed and scripted images. Each unique layer is available to any master image. When an application requires an update, that layer receives the updates and all master images utilizing the layer receives the update. If an organization requires ten unique Windows 10 images, each of the ten images shares the same Windows 10 layer. When the administrator needs to upgrade the VDA from version 7.14 to 7.15 across ten images, the administrator only updates a single platform layer.

Initially, the layered image approach does require more time to deploy because the administrator must build the organization's library of layers. However, once the layers are available, the time to maintain the images is drastically reduced.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Design methodology user layer

Jan 30, 2018

The top layer of the design methodology is the user layer, which each unique user group defines.

The user layer appropriately sets the overall direction for each user group's environment. This layer incorporates the assessment criteria for business priorities and user group requirements in order to define effective strategies for endpoints and Citrix Receiver. These design decisions affect the flexibility and functionality for each user group.

Endpoint Selection

There are a variety of endpoints devices available, all with differing capabilities, including:

- Tablet based
- Laptop
- Desktop PC
- Thin client
- Smartphone

The user's primary endpoint device must align with the overall business objectives as well as each user's role and associated requirements. In many circumstances, multiple endpoints may be suitable, each offering differing capabilities.

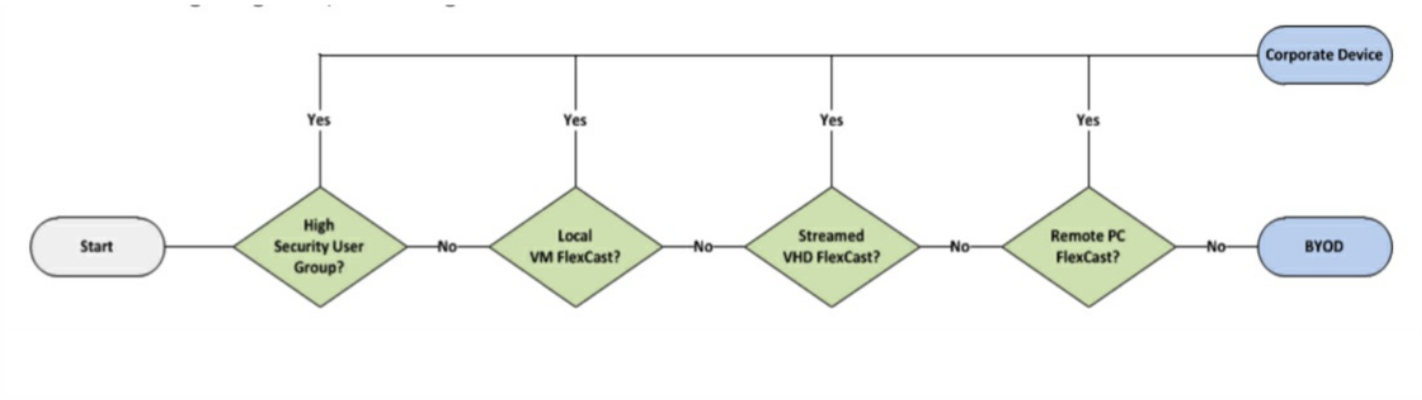
In many organizations, endpoint devices are corporate owned and managed. However, more and more organizations are now introducing bring your own device (BYOD) programs to improve employee satisfaction, reduce costs and to simplify device management. Even if BYOD is a business priority, it does not mean that every user should be allowed to use a personal device in the corporate environment.

Certain user requirements, which were identified during the user segmentation, can greatly impact the suitability of personal devices:

- **Security** – Users requiring a high-level of security might not be able to bring a personal device into the secured environment for risk of data theft.
- **Mobility** – Users operating in a disconnected mode might not be able to use a personal device, as the local VM desktop VDI model associated with this type of requirement can have specific hardware requirements, or special maintenance requirements.
- **Desktop loss criticality** – Users with a high desktop loss criticality rating might require redundant endpoints in the event of failure. This would require the user to have an alternative means for connecting in the event their personal device fails, likely making these users poor candidates for a BYOD program.
- **VDI models** – A personal device should not be recommended for user groups utilizing a local VDI model like a local streamed desktop, local VM desktop or Remote PC Access. These VDI models typically require a specific hardware configuration or installation that will restrict device selection.

The following diagram provides guidance on when user owned devices could be used:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Organizations may choose to repurpose devices in order to extend refresh cycles or to provide overflow capacity for contract workers. Endpoints now offer more capabilities allowing them to have longer useful lifespans. In many cases, these hardware capabilities vastly outstrip the needs of a typical user. When coupled with the ability to virtualize application and desktop workloads, this provides new options to administrators such as repurposing existing workstations. These options go well beyond the simple three-year PC refresh cycle. However, the benefits of repurposing or reallocating a workstation should be balanced against the following considerations.

- **Minimum standards** – While cost factors of repurposing existing workstations may be compelling, certain minimum standards should be met to guarantee a good user experience. At a minimum, it is recommended that repurposed workstations have a 1GHz processor, 1GB of RAM, 16GB of free disk space and a GPU that is capable of supporting HDX features.
- **Business drivers** – Priorities underpin the success of any major project. Those organizations that have prioritized reducing capital expenditure by means of prolonging the hardware refresh cycle can benefit from repurposing hardware. Conversely, if an organization's business drivers include reducing power consumption as part of an overall green initiative, purchasing newer endpoints may be beneficial in order to take advantage of the latest generation of power management capabilities available in the most modern devices.
- **Workload** – The type of work and VDI model for an end user can determine whether they are a good candidate for a repurposed endpoint, or may be better served with a new device. If the work performed by the individual involves locally installed applications, the individual may be best served by a new endpoint that offers the most powerful and recently updated processor and graphics architecture. However, if a user is largely performing tasks associated with virtualized applications that do not involve the latest multimedia capabilities such as webcams, VoIP and media redirection, then a repurposed workstation should be a viable alternative.

The following planning matrix outlines considerations when repurposing existing hardware:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Endpoint provisioning criteria	Repurpose existing	Procure new
Capital restrained environment	X	
High number of virtualized applications	X	
Desire to prolong hardware refresh cycle	X	
High failure rate among existing desktops		X
Outmoded client-side feature set		X
Power consumption or green initiative(s)		X

VDI allows users to work on any device from any location while still getting access to their apps and data. With distributed users accessing the environment across multiple devices, including mobile devices, administrators need to be able to centrally secure and support the mobile devices. Administrators need to:

- Selectively wipe a device if the device is lost, stolen, or out of compliance.
- Require passcode security standards.
- Define geo-location device restrictions.
- Simplify Exchange ActiveSync configuration.
- Define WiFi parameters for office locations.
- Integrate certificates to secure communications.

Managing the distributed endpoints is only part of the challenge. Administrators need to define levels of access. Administrators need to secure and control access to the apps and data. Security becomes a greater concern when users have access to corporate XenApp and XenDesktop resources from personal devices. A few things to consider when delivering XenApp and XenDesktop apps to mobile devices:

- What resources can a jailbroken device access?
- Can users copy/paste between personal apps and XenApp and XenDesktop apps?
- Can a device with no configured passcode get access to corporate resources?
- Can users continue to use a native or untrusted third party email client?
- Can mobile device users access Intranet sites with a browser optimized for mobile devices or with a published desktop browser?

UEM Solutions, like Citrix XenMobile, protects app data and lets admins control app data sharing. UEM also allows for the management of corporate data and resources, separately from personal data.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDI allows users to work on any device from any location while still getting access to their apps and data. With distributed users accessing the environment across multiple devices, including mobile devices, administrators need to be able to centrally secure and support the mobile devices, which is knows as Mobile Device Management (MDM).

MDM solutions, like Citrix XenMobile, enables organizations to protect devices and data on devices at a system level. For example,

- Selectively wipe a device if the device is lost, stolen, or out of compliance.
- Require passcode security standards.
- Define geo-location device restrictions.
- Simplify Exchange ActiveSync configuration.
- Define Wi-Fi parameters for office locations.
- Integrate certificates to secure communications.

MDM is typically suitable for corporate-owned mobile devices because most users with personal devices do not want to give the IT team that much control over their personal devices.

With a distributed workforce accessing the XenApp and XenDesktop environment across numerous devices, administrators need to secure and control access to the apps and data. Security becomes a greater concern when users have access to corporate XenApp and XenDesktop resources from personal devices. A few things to consider when delivering XenApp and XenDesktop apps to mobile devices:

- What resources can a jailbroken device access?
- Can users copy/paste between personal apps and XenApp and XenDesktop apps?
- Can a device with no configured passcode get access to corporate resources?
- Can users continue to use a native or untrusted third party email client?
- Can mobile device users access Intranet sites with a browser optimized for mobile devices or with a published desktop browser?

MAM solutions, like Citrix XenMobile, protects app data and lets admins control app data sharing. MAM also allows for the management of corporate data and resources, separately from personal data.

MAM is often suitable for bring-your-own (BYO) devices because, although the device is unmanaged, corporate data remains protected.

The capabilities of endpoints have grown along with efficiencies offered in thin client form factors. Even mid-range thin clients now have graphics capabilities that allow utilization of HDX features such as multi-monitor support while offering management and power efficiency benefits. Citrix has developed a three-tiered classification for thin clients based on their HDX capabilities: HDX Ready, HDX Premium, and HDX 3D Pro, which can be used to help narrow the field of appropriate thin client devices based on the use case requirements. This expansion of capabilities has given IT administrators more options and flexibility than ever before.

Most organizations will likely deploy a mixture of fully featured clients as well as thin clients. However, certain endpoint devices are more appropriate when used in combination with certain VDI models as explained in the following table.

In the table:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Yes** indicates recommended.
- **No** indicates not recommended.
- o indicates viable.

VDI model	Thin clients	Desktop PC	Laptop	Tablet	Smartphone
Hosted Windows Apps	Yes	Yes	Yes	Yes	Yes
Hosted Browser Apps	Yes	Yes	Yes	Yes	Yes
Hosted Shared Desktop	Yes	Yes	Yes	o	o
Hosted Pooled Desktop	Yes	Yes	Yes	o	o
Hosted Personal Desktop	Yes	Yes	Yes	o	o
Hosted Pro Graphics Desktop	Yes	Yes	o	o	o
Local Streamed Desktop	No	Yes	No	No	No
Local VM Desktop	No	o	Yes	No	No
Remote PC Access	No	Yes	Yes	o	o

Experience from the Field

- **Large systems integrator** – A large systems integrator recommended that a customer deploy a single type of low-end, limited capability endpoint for all users. Upon deployment to production, users immediately complained that they received a poor user experience when viewing multimedia content over the WAN. At great cost, the systems integrator and customer re-assessed the environment and chose to deploy endpoints that supported HDX MediaStream. The mistake caused a schism between systems integrator and the customer, resulting in lost time, capital and the end of a business relationship that was fostered over many years. It is critical that the endpoints assigned to each user group can support their requirements.

Citrix Receiver is an easy-to-install software client that provides access to applications, desktops and data easily and securely from any device, including smartphones, tablets, PCs and Macs.

The following section provides a series of design decisions that should be considered when deploying Citrix Receiver.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

While most organizations should simply deploy the latest Citrix Receiver compatible with their endpoint, it is important to recognize that there are certain differences between editions. The following table should be referenced to determine the most appropriate edition of Citrix Receiver for each user group. For the latest feature matrix, please refer to Receiver Feature Matrix.

There are several deployment options available for delivering Citrix Receiver to an endpoint. Although it is usually a best practice to have a full version of Citrix Receiver deployed to an endpoint to provide the greatest level of functionality, it is important to consider fallback options such as the HTML5 Receiver for those situations where the installation of Citrix Receiver is simply not possible. Note that although the HTML5 Receiver can be used as a fallback option, like the Java client was with Web Interface, it is not generally recommended as the primary Receiver for enterprises to standardize on due to the limited feature set and common browser restrictions around unsecured WebSockets connections (see CTX134123 for more information).

Experience from the Field

- **Furniture distributor** – A furniture distributor maintains a configurator application for various furniture options. The configurator application is accessed via a limited functionality kiosk that is deployed at various furniture outlets, including small, independent retailers with little to no IT staff present. The kiosks are completely locked down in many situations, to the point where even the running of Java applications is limited. The kiosks do feature a modern browser (Google Chrome), and therefore, are able to utilize the HTML5 Receiver in order to provide access to the configurator application.
- **County government** – A government IT organization provides services to all agencies operating in the county. A mixture of full desktops are applications are deployed to both Windows based desktops and iPads. Since the desktops are joined to the Active Directory domain, GPOs are utilized to deploy and configure Citrix Receiver. Mobile users accessing the Citrix environment via an iPad install and configure Receiver from the App Store. To allow for seamless provisioning, email based discovery was configured. This allows users to configure Receiver for both internal and external access through NetScaler Gateway by entering in their email address.

The following mechanisms are commonly used to deploy and update Citrix Receiver:

- **StoreFront** – If Citrix StoreFront is available, administrators can deploy Citrix Receiver via a Receiver for Web site by enabling the “Client Detection” feature. When deployed, a Receiver for Web site enables users to access StoreFront stores through a web page. If the Receiver for Web site detects that a user does not have a compatible version of Citrix Receiver, the user is prompted to download and install Citrix Receiver. The Receiver clients can be hosted on the StoreFront server, or users can be directed to citrix.com for the latest Receiver files.
- **Internal download site** – Users may be prevented from downloading software from the Internet, even if they have permission to install applications. Administrator can create an internal website for supported Citrix Receivers or host them on a common software distribution point for a more seamless user experience. This could be an alternative to enabling Client Detection on the StoreFront Receiver for Web site, which can result in an inconsistent user experience depending on browser’s ActiveX settings.
- **Markets and stores** –Citrix Receiver is available on the Windows, Android and iOS stores.
- **Enterprise software deployment** – Many organizations employ an enterprise software deployment (ESD) or Mobile Application Management (MAM) solution. ESD/MAM solutions can be used to deploy Citrix Receiver to managed endpoint devices. Employee-owned devices can only be managed if the user successfully registered the device with the management tool.
- **Master image** – Most organizations have a group of master desktop images, which are deployed to each business owned desktop, laptop, server, or virtual desktop. A common mechanism to ensure access to virtual desktops and applications is to include a supported version of Citrix Receiver in the master image. Subsequent updates to Citrix

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Receiver are handled either by enterprise software deployment tools or manually.

- **Group policy** – For customers without a robust ESD solution, it is possible to deploy and configure Citrix Receiver via Microsoft Group Policy. Sample start-up scripts that deploy and remove Citrix Receiver are available on Citrix XenApp and XenDesktop media:

  Citrix Receiver and Plugins\Windows\Receiver\Startup_Logon_Scripts

- **Manual install** – All supported versions of Citrix Receiver are available from the Citrix Receiver Download site. Upon landing on this site, client detection is performed and a platform and operating system specific link is provided to allow users to download an appropriate edition of Citrix Receiver. It is important to note that no configuration will be accomplished via this download, so users will receive the first time use prompt to enter a server URL or email address. This option is likely to be utilized in a BYOD environment.

Selecting the appropriate deployment method is based on the type of Citrix Receiver selected. The following table should be referenced to help identify the appropriate deployment options for Citrix Receiver.

In the table,

- **Y** indicates "recommended.
- **N** equals "not recommended.

Deployment options	Thin clients	Desktop PC	Laptop	Tablet	Smartphone
Base image	Y	Y	Y	N	N
EDS/MAM	N	Y	Y	N	N
Group Policy	N	Y	Y	N	N
Receiver for Web site	N	Y	Y	N	N
Internal download site	N	Y	Y	N	N
App store	N	N	N	Y	Y

Citrix Receiver must be configured in order to provide access to enterprise resources. The method of configuration varies by Citrix Receiver edition, the form factor of the device, and lastly the access method (local or remote) that is involved. Several methods may be viable for an organization. The method utilized is contingent on the resources (people, systems, time) available as well as larger organizational initiatives such as BYOD programs.

The following methods can be used to configure Citrix Receiver:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Email based discovery** – The latest releases of Citrix Receiver can be configured by entering an email address. Email based discovery requires Citrix StoreFront as well as an SRV DNS record which points to the FQDN of the StoreFront server.

  Note: Any DNS platform should support email-based discovery, however only Windows DNS has been explicitly tested.

  For remote access, NetScaler Gateway must be utilized with the corresponding SRV record in external DNS. A valid server certificate on the NetScaler Gateway appliance or StoreFront server must be present in order to enable email-based account discovery. This configuration assumes that the portion of the email address after the "@" is the DNS namespace that should be queried for this SRV record. This can be challenging for customers with different external and internal namespaces or email addresses that are different from DNS namespaces.

- **Group policy** – Microsoft Group Policy can be used to configure Citrix Receiver. This can be done via start up scripts used to deploy Receiver by ensuring there is a value for the SERVER_LOCATION=Server_URL parameter or by using the ADMX/ADML template files included with the installation of Citrix Receiver to set the StoreFront Account List option in conjunction with another Receiver deployment method. Provide the URL of the server running Citrix StoreFront in the format https://baseurl/Citrix/storename/discovery.
- **Provisioning file** – For environments running StoreFront, it is possible to provide users with a provisioning file that contains store information. Provisioning files are exported from the StoreFront console. The file is saved with a "*.cr" extension and can then be placed on a shared network resource, a Receiver for Web site, or other web based resource or emailed to users. The file can then be launched from an endpoint, which automatically configures Citrix Receiver to use the store(s). If users browse to the Receiver for Web site and select the "Activate" option under their username, this also automatically downloads this same ".cr" file and configure the Receiver client for users.
- **Manually** – If allowed, it is usually possible to configure Citrix Receiver manually by entering the server URL. This method should be reserved for administrators or users that have advanced knowledge.
- **Studio** – In addition to the above methods, in order to configure Receiver deployed on a virtual desktop or server image (within a XenDesktop or XenApp environment), it is possible to set the StoreFront address via the properties of the Delivery Group.

Citrix Receiver is in active development. As such, periodic updates are released that provide enhanced functionality or address user issues. As with any actively developed product, the latest version of these products should be deployed to the endpoints so that users benefit from the latest functionality and to maintain compliance with product support lifecycles. There are multiple methods available to update Citrix Receiver and, if applicable, associated plug-ins.

- **Auto-Update** – Receiver for Windows 4.8+ and Receiver for Mac 12.6+ includes an autoupdate capability that automatically checks for newer versions of Receiver. The autoupdate service can be configured to allow users to defer updates as well as to skip any updates that are not long-term service release (LTSR) versions. Receiver for iOS and Android are automatically updated through their appropriate store.
- **Enterprise software deployment** – ESD tools provide an organization with direct control over the time/frequency of Receiver updates to managed devices. Additional thought must be given to updating unmanaged devices and endpoints outside of the corporate firewall.
- **Manual updates** – When no automated solution is available, manual methods can be used to update Citrix Receiver. Whether deployed on Receiver for Web site, StoreFront, an internal Citrix Receiver site, or an external site, these options will require user involvement in updating Citrix Receiver. Due to the involved nature of manual updates coupled with the opportunity for a user mistake, this option should only be considered as a last resort.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Design methodology access layer

Apr 23, 2018

The second layer of the design methodology is the access layer, which is defined for each user group.

Creating an appropriate design for the access layer is an important part of the desktop virtualization process. This layer handles user validation through authentication and orchestrates access to all components necessary to establish a secure virtual desktop connection.

The access layer design decisions are based on the mobility requirements of each user group as well as the endpoint devices used.

Getting access to resources is based on the user's identity. Defining the authentication strategy takes into account the user's entry point into the environment as well as how the user will authenticate.

Traditionally, users required an Active Directory username and password to get access to their XenApp and XenDesktop resources. As most organizations standardized on an on-premises Active Directory deployment, this particular requirement was simple to achieve.

Organizations are using external contractors, which requires an account to get access to the XenApp and XenDesktop resources.Organizations are investigating the use of a third party identity provider (IdP) like Azure Active Directory, Google, LinkedIn, etc., instead of managing their own.

With the implementation of Citrix Federated Authentication Service, XenApp and XenDesktop supports the use of a third party IdP. An administrator can have a contractor use their Google account to gain access to their approved applications and desktops, simplifying onboarding.

Before a user connects to a virtual resource, they must first authenticate. The place of authentication is often determined by the user group's mobility requirements, which were defined during the user segmentation process. There are two authentication points available in XenDesktop:

- **StoreFront** – Citrix StoreFront provides authentication and resource delivery services for Citrix Receiver, enabling centralized enterprise stores to deliver desktops, applications and other resources.
- **NetScaler Gateway** – NetScaler Gateway is an appliance providing secure application access and granular application-level policy controls to applications and data while allowing users to work from anywhere.

The following table lists preferred authentication points according to user group mobility requirements:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

User Group's Mobility Requirement	Preferred Authentication Point
Local	StoreFront
Roaming Local	StoreFront
Remote	NetScaler Gateway
Local	NetScaler Gateway

Authentication for user groups with a mobility requirement of remote or mobile may occur directly on StoreFront where required. For example, DMZ security policies may prohibit access from the NetScaler Gateway to the domain, which is required to support Smartcard client certificate authentication. Access to StoreFront for authentication may then be delivered via a NetScaler SSL_BRIDGE virtual server, which provides a conduit for https traffic. Typically, the virtual server would be hosted alongside a NetScaler Gateway on the same NetScaler configured to provide HDX Proxy access to the virtual desktop environment. Although such a use case may sometimes be necessary, the recommended best practice is to authenticate external users via NetScaler Gateway.

Once the authentication point has been identified, the type of authentication must be determined. The following options are the primary methods available:

- **StoreFront** – Supports a number of different authentication methods, although not all are recommended depending on the user access method, security requirements and network location. Note that by default StoreFront authenticates users directly with Active Directory, not via XML as Web Interface did. StoreFront 3.0+ can be optionally configured to delegate authentication to XML if required (such as if the StoreFront servers are in a domain that does not trust the user domains).
  - **User name and password** – Requires users to logon directly to the site by entering a user name and password.
  - **Domain pass-through** – Allows pass-through of domain credentials from users' devices. Users authenticate to their domain-joined Windows computers and are automatically logged on when they access their stores.
  - **NetScaler Gateway pass-through** – Allows pass-through authentication from NetScaler Gateway. Users authenticate to NetScaler Gateway and are automatically logged on when they access their stores.
  - **Smart card** – Allows users to authenticate using smart cards and PINs through Citrix Receiver for Windows and NetScaler Gateway. To enable smart card authentication, user accounts must be configured either within the Microsoft Active Directory domain containing the StoreFront servers or within a domain that has a direct two-way trust relationship with the StoreFront server domain. Multi-forest deployments involving one-way trust or trust relationships of different types are not supported.
  - **Anonymous** – Allow users to access applications and desktops without presenting credentials to StoreFront or Citrix Receiver. Local anonymous accounts are created on demand on the Server VDA when sessions are launched. This requires a StoreFront store configured for authenticated access, a Server OS based VDA, and a XenApp Delivery Group configured for unauthenticated users.
- **NetScaler Gateway** – The NetScaler Gateway supports several authentication methods. The list below includes those

© 1999-2017 Citrix Systems, Inc. All rights reserved.

primarily used in virtual desktop environments. Each may be used individually, but are often combined to provide multi-factor authentication.

- **LDAP** – The lightweight directory access protocol (LDAP) is used to access directory information services such Microsoft Active Directory. NetScaler Gateway uses LDAP to authenticate users and extract their group membership information.
- **RADIUS (token)** – Remote authentication dial in user service (RADIUS) is a UDP based network security protocol that provides authentication, authorization and accounting. A network access server (NetScaler Gateway in this case) forwards credentials to a RADIUS server that can either check the credentials locally, or check them against a directory service. The RADIUS server could then accept the connection, reject the connection, or challenge and request a second form of authentication such as a token.
- **Client certificate** – Users logging on to a NetScaler Gateway virtual server can also be authenticated based on the attributes of a client certificate presented to the virtual server. Client certificates are usually disseminated to users in the form of smartcards or common access cards (CACs) that are read by a reader attach to each user's device.

The authentication type for a user group is often determined based on security requirements as well as the authentication point used. The following table helps define the appropriate solution for each user group based on the level of security required:

Authentication Point	Security Requirement	Authentication Type
StoreFront	• Low • Medium • High	Low: • LDAP user name and password • Pass-through Medium • LDAP user name and password • Pass-through High: LDAP and/or Smartcard
NetScaler Gateway	• Low • Medium • High	Low: LDAP user name and password Medium: LDAP user name and password High: • LDAP and Token • LDAP and Smartcard • Token and Smartcard

Experience from the Field

- **Retail** – A small private retail company provides virtual desktop users with access to non-sensitive data such as marketing catalogs and email. They are not required to adhere to security regulations such as Sarbanes Oxley. Therefore, LDAP authentication has been implemented based on user name and password.
- **Financial** – A medium financial enterprise provides their virtual desktop users with access to confidential data such as banking transaction records. They are governed by security regulations such as the Statement on Accounting Standards (SAS) 70 and are required to utilize multi-factor authentication for remote access users. LDAP authentication has been implemented based on user name and password along with RADIUS authentication using tokens.
- **Government** – A large federal institution provides virtual desktop users with access to highly confidential data such as

© 1999-2017 Citrix Systems, Inc. All rights reserved.

private citizens' personal records. They are subject to regulation by Department of Defense (DOD) security standards. LDAP authentication has been implemented based on user name and password, along with Client Certificate authentication using CAC cards.
- **Healthcare** - A hospital is using XenApp to deliver their EMR application to users. ThinClient devices on stationary and mobile carts are being used by doctors and nurses to capture and retrieve patient data. Unauthenticated access has been configured to prevent medical staff from having to authenticate to the domain as well as the EMR application.

Citrix StoreFront authenticates users to XenApp and XenDesktop resources. StoreFront enumerates and aggregates available desktops and applications into a single interface that users access through Citrix Receiver for Windows, iOS, Android, or the StoreFront web site.

If the server hosting StoreFront is unavailable, users will not be able to launch new virtual desktops, published applications or manage their subscriptions. Therefore at least two StoreFront servers should be deployed to prevent this component from becoming a single point of failure. By implementing a load balancing solution, users will not experience an interruption in their service. Options include:

- **Hardware load balancing** – An intelligent appliance, which is capable of verifying the availability of the StoreFront service and actively load balance user requests appropriately. Citrix NetScaler is a great example of a hardware load balancer. Citrix NetScaler is an ideal load balancer, coming pre-configured with StoreFront health checks.
- **DNS round robin** – Provides rudimentary load balancing across multiple servers without performing any checks on availability. If a StoreFront server becomes unavailable, DNS round robin would still route users to the failed server. Because of this, DNS round robin is not recommended by Citrix.
- **Windows network load balancing** – A Windows service capable of performing rudimentary checks to verify the server is available but cannot determine the status of individual services. This can cause users to be forwarded to StoreFront servers which are not able to process new requests. The user would then not be able to access applications or desktops.

To provide users with desktops and applications, StoreFront must be configured with the IP address or DNS name of at least one Controller in each XenDesktop and XenApp site. For fault tolerance, multiple controllers should be entered for each site and/or farm specified. By default, StoreFront treats a list of servers in failover order (active/passive).

For large deployments or environments with a high logon load an active distribution of the user load (active/active) is recommended. This can be achieved by means of a load balancer with built-in XML monitors, such as Citrix NetScaler or by configuring StoreFront to load balance the list of Controllers instead of treating them as an ordered list.

Citrix Receiver uses beacons (websites) to identify whether a user is connected to an internal or external network. Internal users are connected directly to StoreFront for authentication while external users are connected via Citrix NetScaler Gateway. It is possible to control what a user sees by restricting applications due to which beacon they have access to.

The internal beacon should be a site that is not resolvable externally. By default, the internal beacon is the StoreFront base URL. This will have to be adjusted if the same external and internal URL is configured. The external beacon can be any external site that produces an http response. Citrix Receiver continuously monitors the status of network connections (for example, link up, link down or change of the default gateway). When a status change is detected, Citrix Receiver first verifies that the internal beacon points can be accessed before moving on to check the accessibility of external beacon

© 1999-2017 Citrix Systems, Inc. All rights reserved.

points. StoreFront provides Citrix Receiver with the http(s) addresses of the beacon points during the initial connection/configuration download process and provides updates as necessary. It is necessary to specify at least two highly available external beacons that can be resolved from public networks.

By default, StoreFront allows users to choose (subscribe) to the resources they want to regularly use after they logon (favorites). This approach, deemed “Self-Service,” allows users to restrict the resources that they see on their home screen to the ones that they use on a regular basis. The resources chosen by every user for each store are recorded by the subscription store service and stored locally on each StoreFront server (synced automatically between servers in the same server group) so that they can be displayed on the Citrix Receiver home screen from any device that the user connects from. Although by default subscriptions are per store and per server group, administrators can configure two stores within a server group to share a subscription database and/or sync subscriptions between two identically named stores in two separate server groups on a defined schedule if required.

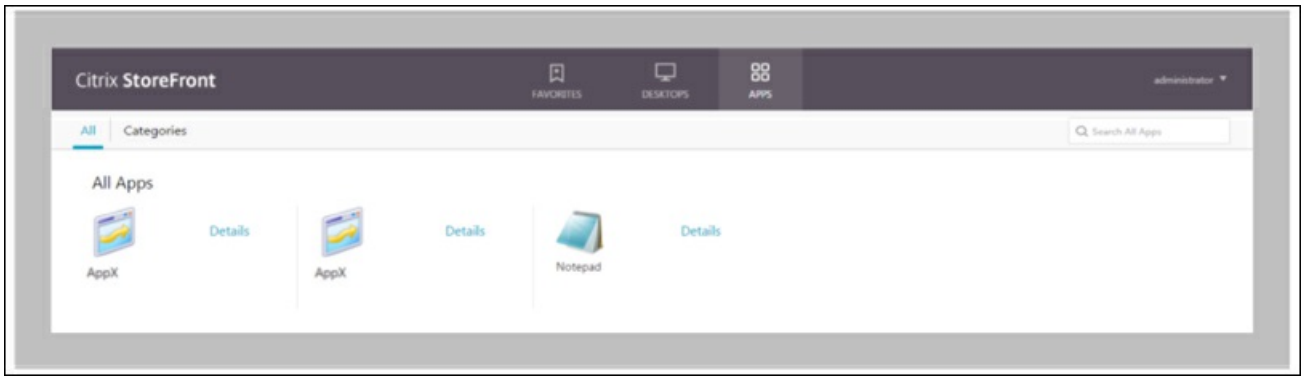
Administrators should determine which applications should always be displayed to users on their home screen or the featured tab. In general, these applications are common applications such as the Microsoft Office Suite and any other applications that every user in an environment may need. StoreFront can filter/present these resources using Keywords defined within the published application properties Description field.

The following table explores the Keyword options:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

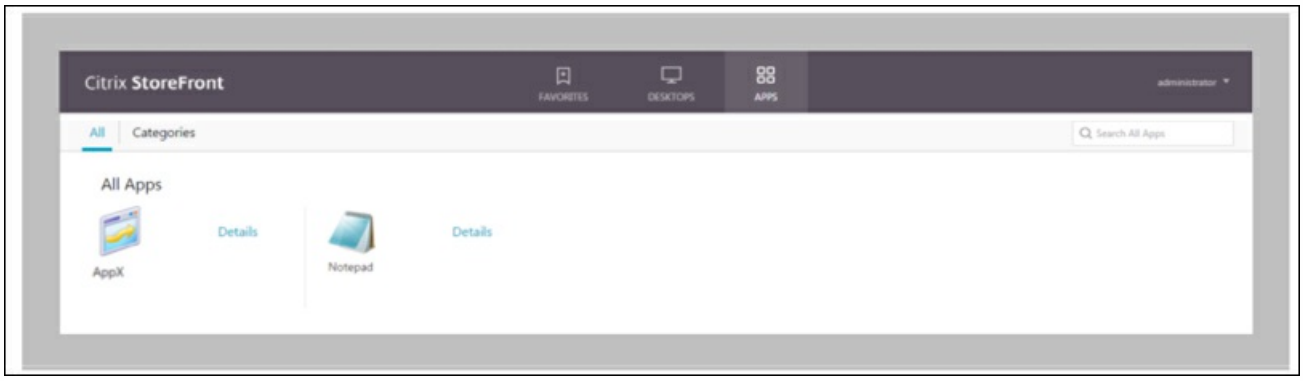
Keyword	Description
Auto	Automatically subscribes all users of a store to an application. When users log on to the store, the application is automatically provisioned without users needing to manually subscribe to the application. Users can choose to subsequently remove this subscription if desired.
Mandatory	New in StoreFront 2.5, the Mandatory keyword will make applications automatically be subscribed to users of the store. However, users will not have the option to remove the application. This setting is useful when creating a core set of applications which must always be presented to all users.
Featured	Advertise applications to users or make commonly used applications easier to find by listing them in the Receiver Featured list.
Prefer	Specify a locally installed application should be used instead of an application available in Receiver. Receiver searches for the specified name/path to determine if the application is installed locally. If it is, Receiver subscribes the application and does not create a shortcut. When the user starts the application from the Receiver window, Receiver starts the locally installed (preferred) application. If a user uninstalls a preferred application outside of Receiver, the application is unsubscribed during the next Receiver refresh. If a user uninstalls a preferred application from the Receiver window, Receiver unsubscribes the application but does not uninstall it.
TreatAsApp	By default, XenDesktop VDI desktops and XenApp hosted shared desktops are treated like other desktops by Receiver for Web sites. By using the keyword "TreatAsApp," the desktop will be displayed in the application views of Receiver for Web sites rather than the desktop views. Users are required to subscribe before they can access the desktop.
Primary	When in a multi-site deployment, using this keyword ensures that an application is delivered from a designated site. If an application is available from multiple sites, with the same name, the application from the secondary site will only be displayed if the application is not available from the primary site.
Secondary	A same property as the "Primary" keyword, except it designates an application in the secondary site.

If the XenApp/XenDesktop solution includes multiple delivery sites, StoreFront merges the available resources together so the user has a single interface for all published resources. However, if multiple sites publish the same resources, the user might experience confusion as a single application appears multiple times.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

StoreFront aggregation groups define how the resources in multiple sites merge to provide the user with a single, easy to understand view. StoreFront aggregates duplicate published resources into a single icon.



The administrator must determine how to load balance users across the different XenApp/XenDesktop sites when the icon is an aggregation. The options are:

- **Load Balancing** – Used when the duplicate sites are created based on capacity recommendations. StoreFront distributes user requests across all configured sites.
- **Failover** – Used when geographies need to have resources available in the event of an outage or when migrating users from one site to another site (like a XenApp migration project).

It is advisable to document the users, stores and aggregation methods during the design phase.

User Group	Available Store(s)	Load Balancing Stores	Failover Stores
NA_FinanceUsers	NA_West_Store NA_East_Store EMEA_Store	NA_West_Store NA_East_Store	EMEA_Store
EMEA_SalesUsers	EMEA_Store NA_East_Store	EMEA_Store	NA_East_Store

The number of Citrix Receiver users supported by a single StoreFront server depends on the resources assigned and level of user activity. Note that Receiver for Web users will consume more RAM on average than native Receiver users, but a minimum of 4 GB of RAM is recommended per StoreFront server in all cases as a baseline. Additionally, more sites/farms enumerated per store will increase both CPU utilization and server response time, with XenApp IMA farms having a greater scalability impact than XenApp/XenDesktop FMA site.

StoreFront deployment	CPU Usage	Simultaneous activities
Standalone deployment • 4CPUs	75%	291 per second

© 1999-2017 Citrix Systems, Inc. All rights reserved.

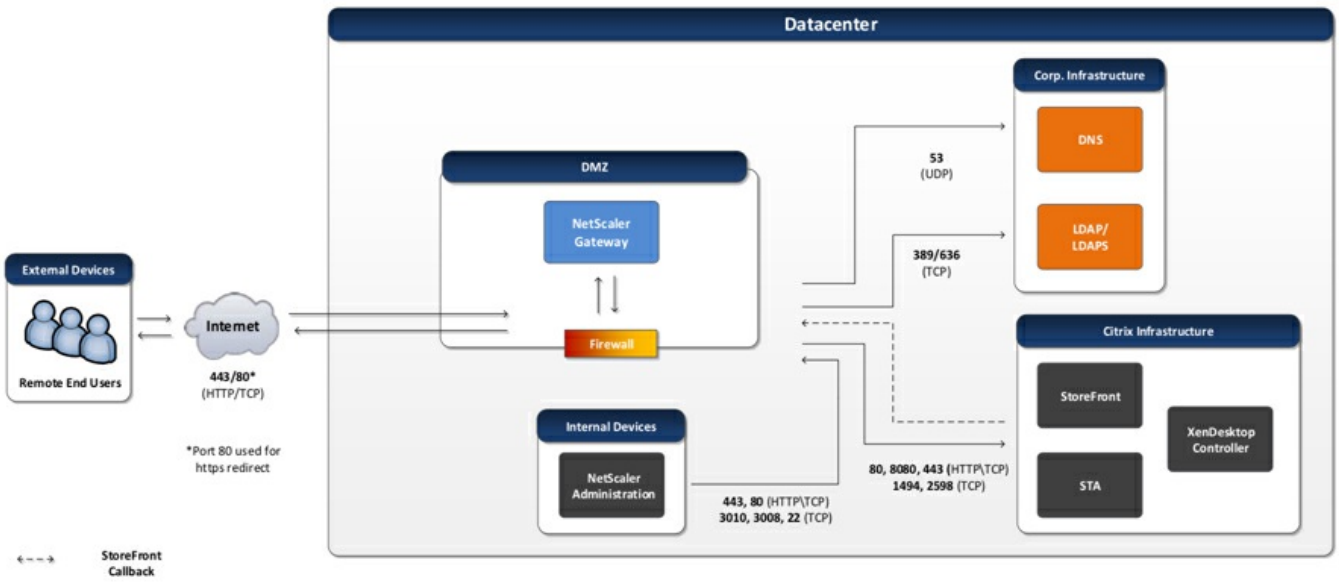
• 4 GB RAM • Heavy Usage (logon, enumerate, subscribe, unsubscribe, logoff)	90%	375 per second
Cluster StoreFront deployment 2 Nodes each with: • 4 CPUs • 4 GB RAM • Heavy Usage (logon, enumerate, subscribe, unsubscribe, logoff)	75%	529 per second
	90%	681 per second

Tests have shown diminishing returns after a single StoreFront deployment grows beyond 3-4 StoreFront nodes with a maximum of 5-6 servers supported in a single server group.

User groups utilizing NetScaler Gateway as their authentication point have additional design decisions to consider. These design decisions are not applicable for non-NetScaler Gateway authentication points.

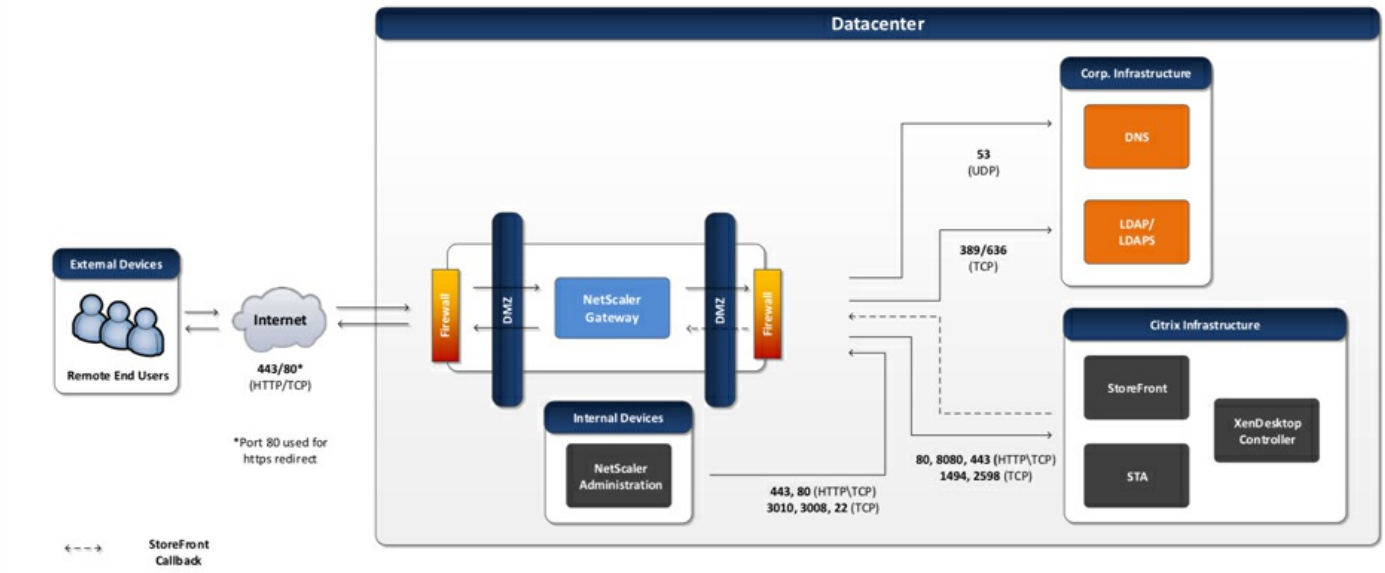
Selection of the network topology is central to planning the remote access architecture to ensure that it can support the necessary functionality, performance and security. The design of the remote access architecture should be completed in collaboration with the security team to ensure adherence to corporate security requirements. There are two primary topologies to consider, each of which provides increasing levels of security:

- **1-Arm (normal security)** – With a 1-arm topology, the NetScaler Gateway utilizes one physical or logical bonded interface, with associated VLAN and IP subnet, to transport both frontend traffic for users and backend traffic for the virtual desktop infrastructure servers and services.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **2-Arm (high security)** – With a 2-arm topology, the NetScaler Gateway utilizes two or more physically or logically bonded interfaces, with associated VLANS and IP subnets. Transport of the frontend traffic for users is directed to one of these interfaces. The frontend traffic is isolated from backend traffic, between the virtual desktop infrastructure servers and services, which is directed to a second interface. This allows the use of separate demilitarized zones (DMZs) to isolate frontend and backend traffic flows along with granular firewall control and monitoring.



If the NetScaler Gateway is unavailable, remote users will not be able to access the environment. Therefore at least two NetScaler Gateway hosts should be deployed to prevent this component from becoming a single point of failure.

When configuring NetScaler Gateway in a high availability (active/passive) pair, the secondary NetScaler Gateway monitors the first appliance by sending periodic messages, also called a heartbeat message or health check, to determine if the first appliance is accepting connections. If a health check fails, the secondary NetScaler Gateway tries the connection again for a specified amount of time until it determines that the primary appliance is not working. If the secondary appliance confirms the health check failure, the secondary NetScaler Gateway takes over for the primary NetScaler Gateway.

Note that in firmware 10.5 and above, clustering is also possible with multiple NetScaler Gateway instances to provide high availability, although support for spotted versus stripped configurations varies by firmware and Gateway configuration (full SSL VPN versus ICA proxy).

(http://docs.citrix.com/en-us/netscaler/11-1/clustering/cluster-features-supported.html)

In order to identify an appropriate NetScaler platform to meet project requirements, the key resource constraints must be identified. Since all remote access traffic will be secured using the secure sockets layer (SSL), transported by Hypertext Transfer Protocol (HTTP) in the form of HTTPs, there are two resource metrics that should be targeted:

- **SSL throughput** – The SSL throughput is the gigabits of SSL traffic that may be processed per second (Gbps).
- **SSL transactions per second (TPS)** – The TPS metric identifies how many times per second an Application Delivery Controller (ADC) may execute an SSL transaction. The capacity varies primarily by the key length required. TPS capacity is

© 1999-2017 Citrix Systems, Inc. All rights reserved.

primarily a consideration during the negotiation phase when SSL is first setup and it is less of a factor in the bulk encryption / decryption phase, which is the majority of the session life. While TPS is an important metric to monitor, field experience has shown that SSL throughput is the most significant factor in identifying the appropriate NetScaler Gateway.

The SSL bandwidth overhead average is often considered negligible relative to the volume of virtual desktop traffic and is not typically accounted for as part of required SSL throughput. However, making provisions for SSL bandwidth will help ensure the total throughput estimated is sufficient. The fixed bandwidth added to packet headers can vary according to the encryption algorithms used and the overall percentage of bandwidth may vary widely according to packet size. Ideally, the overhead should be measured during a proof of concept or pilot. However, in the absence of such data incrementing the workload bandwidth by 2% is a reasonable rule of thumb. Therefore, to determine the SSL throughput required by a NetScaler platform, multiply the maximum concurrent bandwidth for a datacenter by 1.02:

□□□ □*h*□□□□*h*□□□ = □□□□□□□ □□□□□□□□□□ □□□□□□□□*h* ∗ 1.02

For example, assuming 128Mbps maximum concurrent bandwidth, the appropriate NetScaler model can be determined as follows:

~130□□□□ = 128□□□□ ∗ 1.02

The SSL throughput value should be compared to the throughput capabilities of various NetScaler platforms to determine the most appropriate one for the environment. There are three main platform groups available, each of which provides broad scalability options.

- **VPX** – A NetScaler VPX device provides the same full functionality as hardware NetScaler. However, NetScaler VPXs can leverage 'off the shelf' servers for hosting and are suitable for small to medium sized environments. Typically, organizations create a baseline cap for the VPX instances at 500 users.
- **MPX** – A NetScaler MPX is the hardware version of the NetScaler devices. The MPX device is more powerful than the virtual NetScaler and can support network optimizations for larger scale enterprise deployments, particularly when SSL offload will be configured as this is done in software on the VPX versus dedicated SSL chips on the MPX.
- **SDX** – A NetScaler SDX is a blend between the virtual and physical NetScaler devices. An SDX machine is a physical device capable of hosting multiple virtual NetScaler devices. This consolidation of devices aids with reducing required shelf space and device consolidation. NetScaler SDXs are suitable for handling network communications for large enterprise deployments and/or multi-tenant hosting providers.

SSL throughput capabilities of the NetScaler platforms may be found in the Citrix NetScaler data sheet. Therefore, based on the example calculation above, a NetScaler MPX 5550 appliance would be sufficient to handle the required load. However, actually scalability will depend on security requirements. NetScaler SSL throughput decreases with the use of increasingly complex encryption algorithms and longer key lengths. Also, this calculation represents a single primary NetScaler. At a minimum, N+1 redundancy is recommended which would call for an additional NetScaler of the identical platform and model.

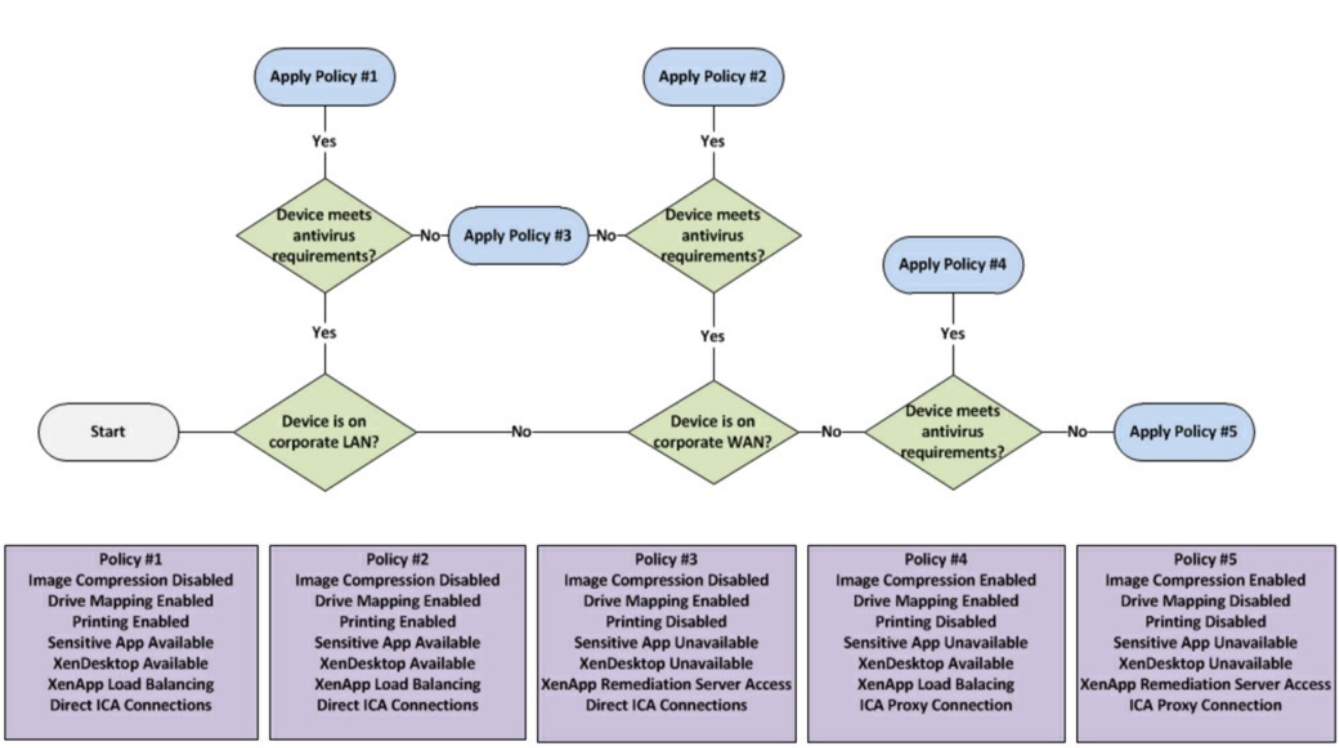
> **注意**
>
> The Citrix NetScaler data sheet typically represents throughput capabilities under optimal conditions for performance. However, performance is directly affected by security requirements. For example, if the RC4 encryption algorithm and a 1k key length are used, a VPX platform may be able to handle more than 500 HDX proxy connections. However, if a 3DES encryption algorithm and 2k key length are used (which are becoming more common), the throughput may be halved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

An optional pre-authentication policy may be applied to user groups with NetScaler Gateway as their authentication point. Pre-authentication policies limit access to the environment based on whether the endpoint meets certain criteria through Endpoint Analysis (EPA) Scans.

Pre-authentication access policies can be configured to test antivirus, firewall, operating system, or even registry settings. These policies can be used to prevent access entirely or can be used by XenDesktop to control session features such as clipboard mapping, printer mapping and even the availability of specific applications and desktops. For example, if a user device does not have antivirus installed, a filter can be set to hide sensitive applications.

The following figure provides an overview of how multiple policies can be used to customize the features of a virtualization resource:



Experience from the Field

- **Retail** – A small private retail company use EPA to scan for the presence of updated antivirus definitions prior to allowing access.
- **Financial** – A medium financial enterprise use EPA scans of the Domain SID to verify that users are members of the enterprise domain prior to allowing access.
- **Government** – A large federal institution use EPA to scan endpoint devices to ensure that a specific certificate (or set of certificates) has been installed on the device prior to allowing access.

User groups with NetScaler Gateway as their authentication point must have corresponding session policies defined. Session policies are used to define the overall user experience postauthentication.

Organizations create sessions policies based on the type of Citrix Receiver used. For the purpose of session policy

© 1999-2017 Citrix Systems, Inc. All rights reserved.

assignment, devices are commonly grouped as either non-mobile (such as Windows, Mac and Linux OS based), or mobile (such as iOS or Android). Therefore, a decision on whether to provide support for mobile devices, non-mobile devices, or both should be made based on client device requirements identified during the assess phase.

To identify devices session policies, include expressions such as those discussed in this article.

- **Mobile devices** – The expression is set to REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver which is given a higher priority than the non-mobile device policy to ensure mobile devices are matched while non-mobile devices are not.
- **Non-mobile devices** – The expression is set to ns_true which signifies that it should apply to all traffic that is sent to it.

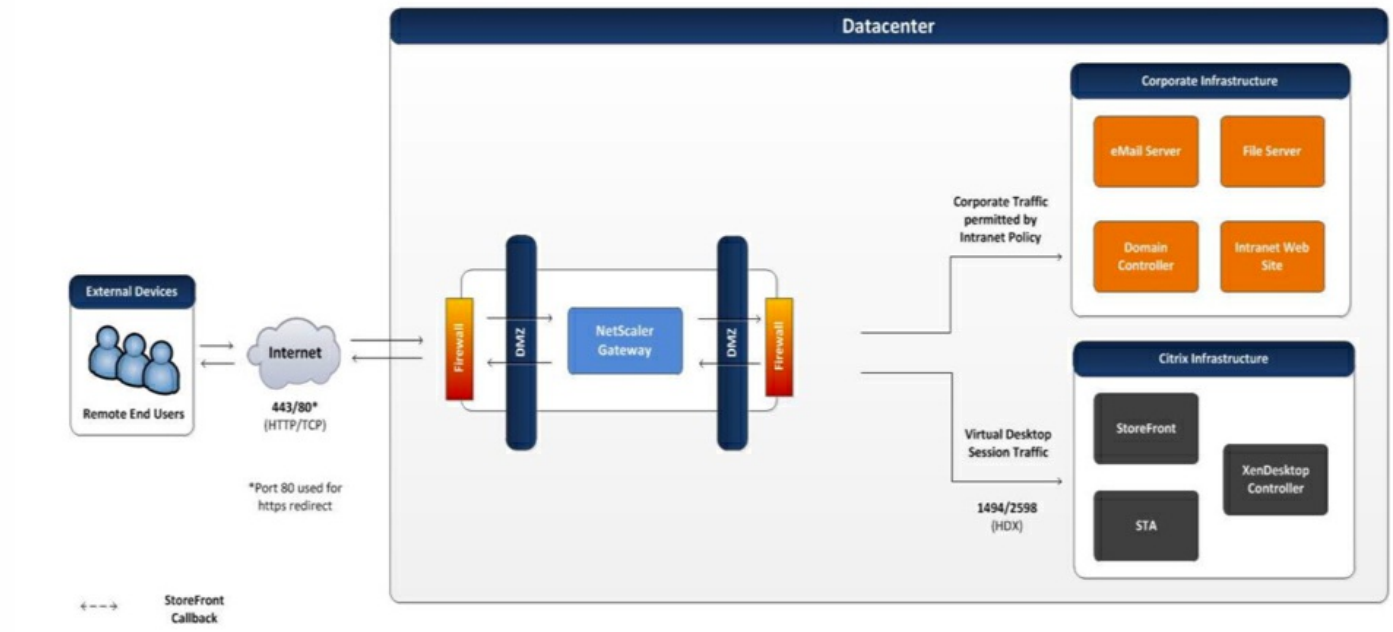
An alternative use of session policies is to apply endpoint analysis expressions. These session policies are applied post authentication yet mimic the previously mentioned pre-authentication policies. Use of session policies is an option to provide a fallback scenario to endpoints that do not meet full security requirements such read-only access to specific applications.

Each session policy must have a corresponding session profile defined. The session profile defines details required for the user group to gain access to the environment. There are two primary forms of session profiles that determine the access method to the virtual desktop environment:

- **SSLVPN** – Users create a virtual private network and tunnel all traffic configured by IP addresses through the internal network. The user's client device is able to access permitted intranet resources as if it were on the internal network. This includes XenDesktop sites and any other internal traffic such as file shares or intranet websites. This is considered a potentially less secure access method since network ports and routes to services outside of the virtual desktop infrastructure may be opened leaving the enterprise susceptible to risks that may come with full VPN access. These risks may include denial of service attacks, attempts at hacking internal servers, or any other form of malicious activity that may be launched from malware, Trojan horses, or other viruses via an Internet based client against vulnerable enterprise services via routes and ports.

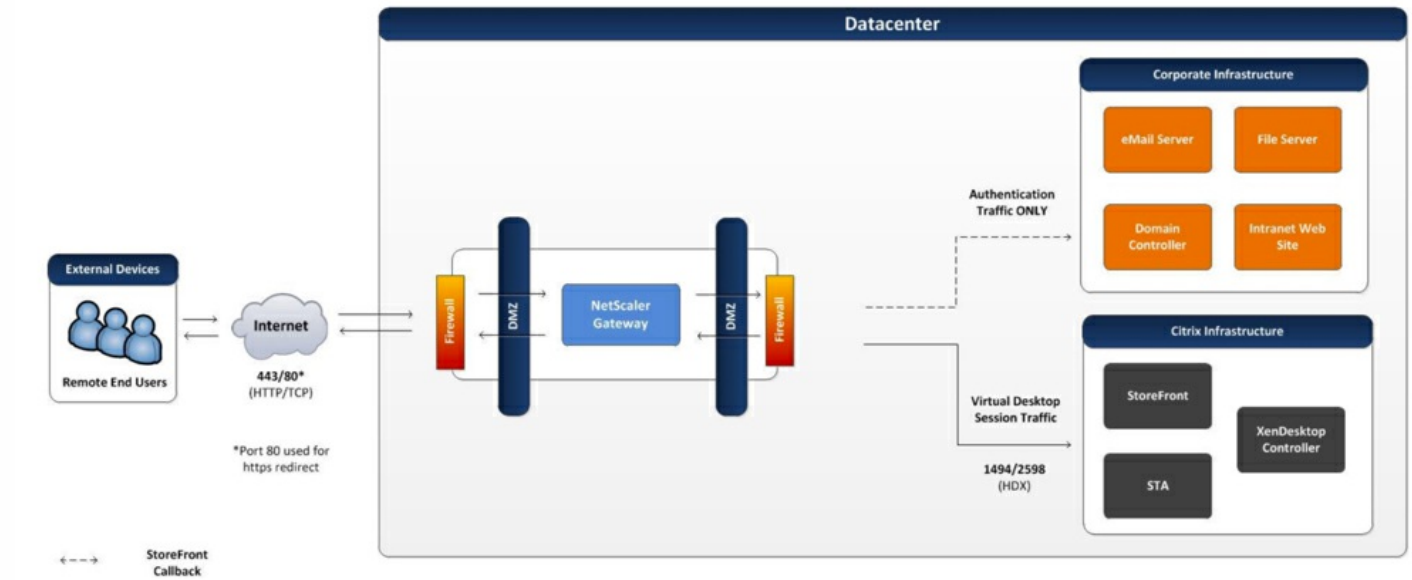
  Another decision to consider when SSLVPN is required is whether to enable split tunneling for client network traffic. By enabling split tunneling, client network traffic directed to the intranet by Citrix Receiver may be limited to routes and ports associated with specific services. By disabling split tunneling, all client network traffic is directed to the intranet, therefore both traffic destined for internal services as well as traffic destined for the external services (Internet) traverses the corporate network. The advantage of enabling split tunneling is that exposure of the corporate network is limited and network bandwidth is conserved. The advantage of disabling split tunneling is that client traffic may be monitored or controlled through systems such as web filters or intrusion detection systems

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- **HDX proxy** – With HDX Proxy, users connect to their virtual desktops and applications through the NetScaler Gateway without exposing internal addresses externally. In this configuration, the NetScaler Gateway acts as a micro VPN and only handles HDX traffic. Other types of traffic on the client's endpoint device, such as private mail or personal Internet traffic do not use the NetScaler Gateway.

  Based on the endpoint and Citrix Receiver used, a decision must be made as to whether this method is supported for each user group. HDX Proxy is considered a secure access method for remote virtual desktop access since only traffic specific to the desktop session is allowed to pass through to the corporate infrastructure. Most Citrix Receivers support HDX Proxy and it is the preferred method:



Enterprises often have multiple active datacenters providing high availability for mission critical applications. Some virtual

© 1999-2017 Citrix Systems, Inc. All rights reserved.

desktops or applications may fall into that category while others may only be accessed from a specific preferred datacenter. Therefore, the initial NetScaler Gateway that a user authenticates to in a multi-active datacenter environment may not be within the preferred datacenter corresponding to the user's VDI resources. StoreFront is able to determine the location of the user's assigned resources and direct the HDX session to those resources; however, the resulting path may be sub-optional (WAN connection from the NetScaler Gateway to the virtual desktop/application resources as opposed to LAN connection).

There are static and dynamic methods available to direct HDX sessions to their virtual desktop resources in their primary datacenter. The decision regarding which method to select should be based on the availability of technology to dynamically assign sites links such as Global Server Load Balancing (GSLB) along with the network assessment of intranet and Internet bandwidth as well as Quality of Service (QoS) capabilities.

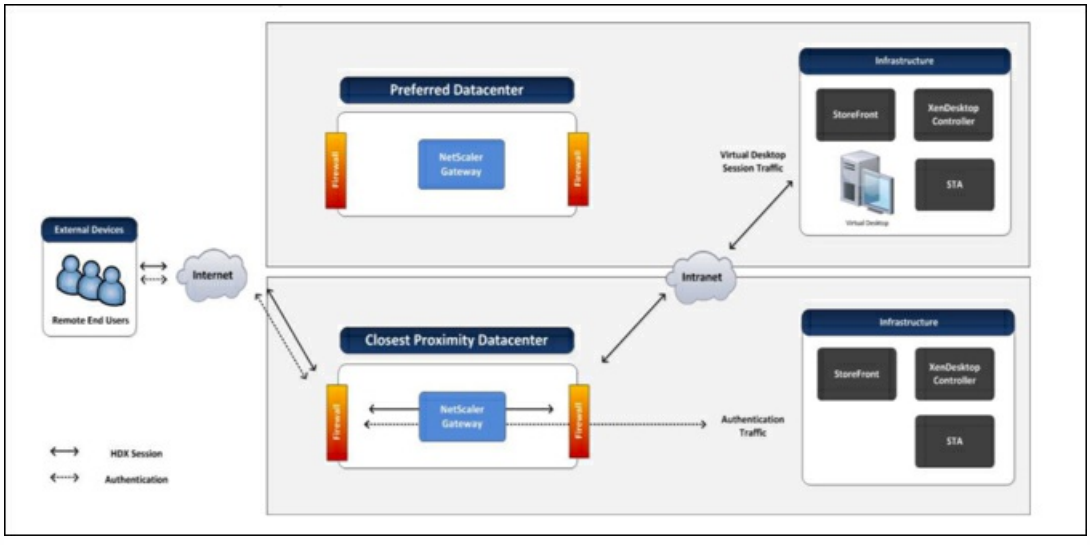
> **注意**
>
> For more information on configuring the static and dynamic methods of GSLB, please refer to Citrix Product Documentation - Configuring GSLB for Proximity.

Static

- **Direct** – The user may be given a FQDN mapped to an A record that is dedicated to the primary datacenter NetScaler Gateway(s) allowing them to access their virtual desktop directly wherever they are in the world. This approach eliminates a layer of complexity added with dynamic allocation. However, it also eliminates fault tolerance options such as the ability to access the virtual desktop through an alternative intranet path when a primary datacenter outage is limited to the access infrastructure.

Dynamic

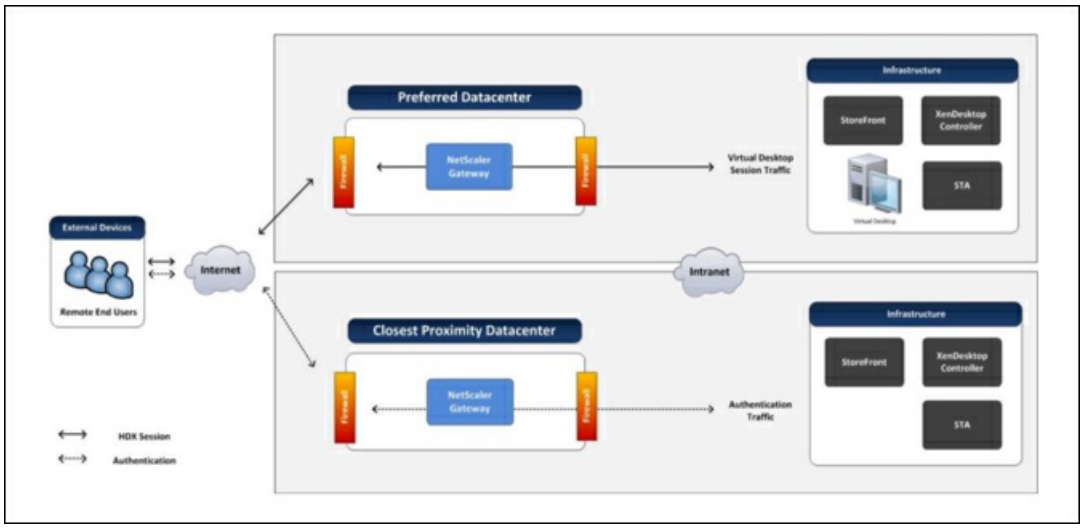
- **Intranet** – For most dynamic environments, the initial datacenter selected for authentication is the one closest to the user. Protocols such as GSLB dynamic proximity calculate the least latency between the user's local DNS server and the NetScaler Gateway. Thereafter, by default, the HDX session is routed through the same NetScaler Gateway to whichever datacenter is hosting the user's virtual desktops and applications. The advantage of this approach is that the majority of the HDX session would traverse the corporate WAN where quality of service may be used.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Internet** - Alternatively, the HDX session can be re-routed through an alternate NetScaler Gateway proximate to the backend VDI desktop / XenApp server, resulting in most of the HDX session travelling over the Internet. For example, a user with a dedicated desktop in the United Stated, traveling in Europe may be directed to a NetScaler Gateway hosted in a European datacenter based on proximity. However, when the user launches their desktop, an HDX connection will be established to the virtual desktop via a NetScaler Gateway hosted in the preferred datacenter in the United States.

  This conserves WAN network usage (at the cost of QoS) and is recommended in cases where the user's Internet connection may provide a more reliable experience than the corporate WAN.



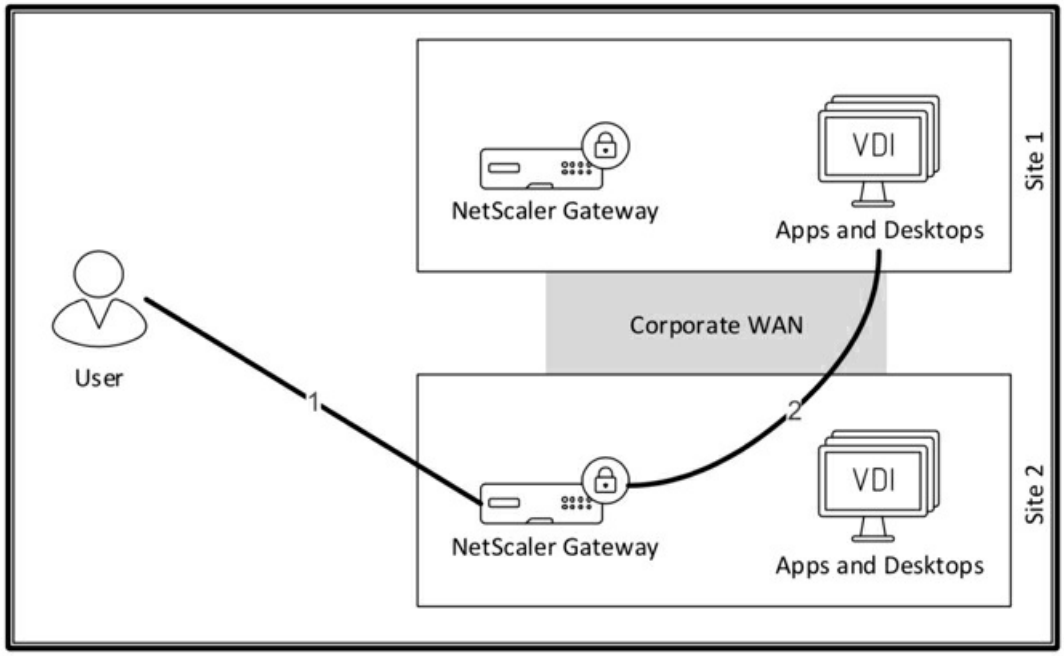
Some customers will use a combination of these methods, such as geo-specific dynamic URLs such that fault tolerance is provided within a geographic area (such as North America) without incurring the complexity of global GSLB.

A XenApp and XenDesktop site is capable of spanning multiple locations, In order to successfully implement a multi-site solution, the design must take into account the site-to-site links and XenApp and XenDesktop session routing between locations in order to provide the best user experience.

In a multi-site XenApp and XenDesktop solution, certain criteria, like fastest response time or closest proximity, routes users to the optimal site. These algorithms do not take into account the resources a user wants to access.

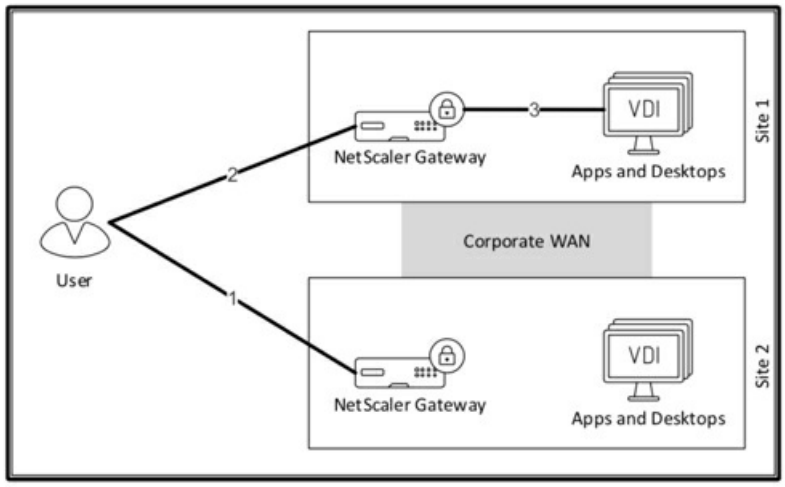
Improper routing of a user's session results in the following:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



1. User routed to the most preferred site, based on proximity or response time
2. NetScaler Gateway proxies the ICA traffic to the correct resource, which could be across the corporate WAN.

Ideally, optimized routing should resemble the following:



1. User routed to the most preferred site, based on proximity or response time
2. Based on the selected resource, NetScaler Gateway reroutes the session to a NetScaler Gateway in the preferred site.
3. NetScaler Gateway proxies the ICA traffic to the correct resource, which stays on the local LAN.

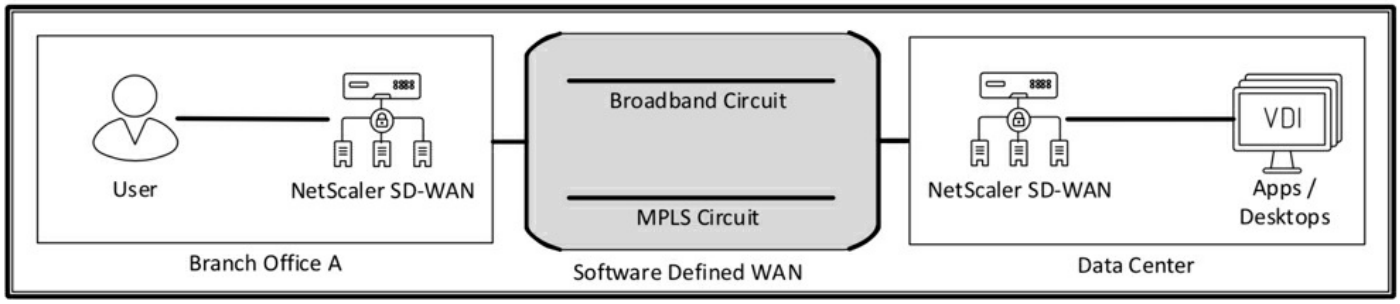
Using the optimized HDX routing option within StoreFront offloads traffic from the corporate WAN and places it on the public network

In branch office scenarios, a XenApp and XenDesktop design must evaluate the branch office's connection to the data centers hosting the application and desktop resources. If the WAN connection between the branch office and data center

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

is not able to meet the user requirements, the overall user experience degrades. Organizations have a couple of options on their WAN connections:

- **Scale Up** – Organizations can simply increase the size of the WAN pipe connecting the branch offices to the data center, typically at a sizable cost.
- **Scale Out** – Organizations can maintain their current WAN connection and augment it with multiple low-cost alternatives. The integration of all connections between the branch office and data center creates a software defined virtual WAN, like NetScaler SDWAN. The appliance sends duplicate network packets across all WAN connections defined within the virtual WAN. The appliance on the other end of the WAN uses the first arriving packet, discarding all subsequent packets. As the conditions of the multiple links change throughout the day, this approach guarantees the best experience possible.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Design methodology resource layer

Apr 23, 2018

The resource layer is the third layer of the design methodology and the final layer focused specifically on the user groups.

The overall user acceptance of the solution is defined by the decisions made within the resource layer. Profiles, printing, applications and overall desktop image design play a pivotal role in how well the desktop is aligned with the user group's requirements, which were identified within the assess phase.

Perception is everything when it comes to a good VDI experience. Users expect an experience similar to or better than that of a traditional, physical desktop.

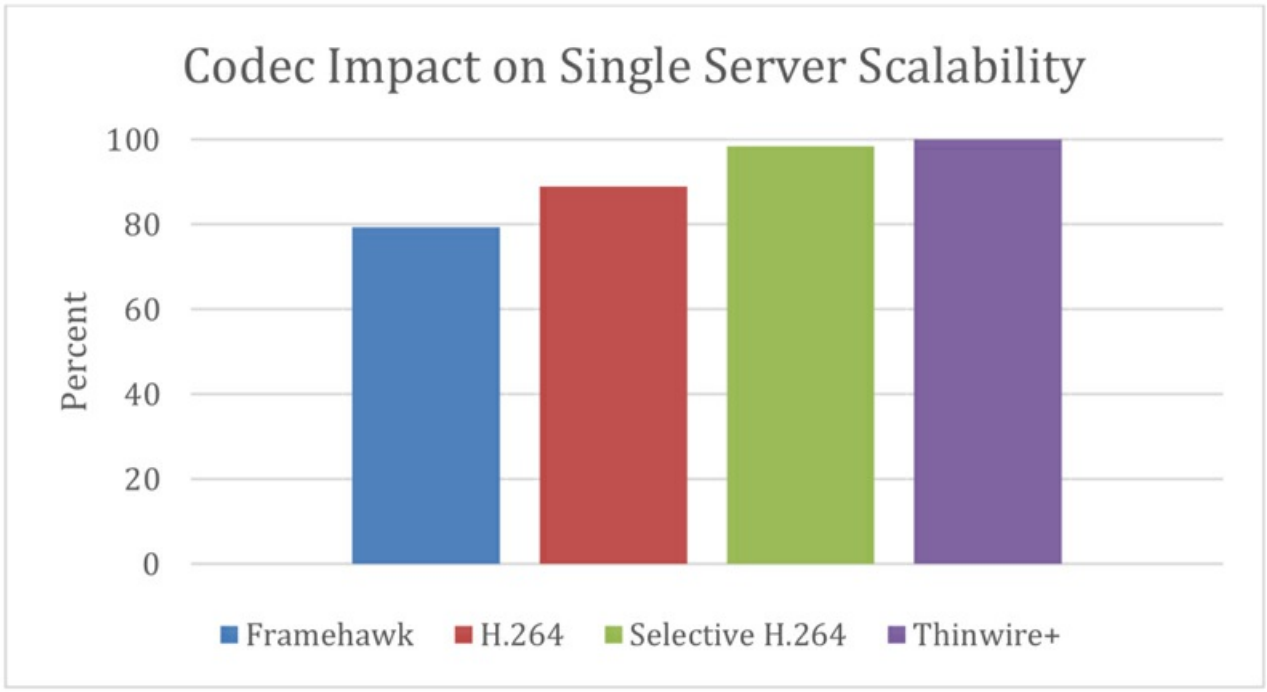
Codecs, transport protocols and self-service capabilities affects the overall experience. Poor quality graphics, lagging video or 120 second logon times can destroy the user experience. A proper user experience design can meet any network challenge.

Selecting the correct display protocol determines the quality of static images, video and text within the user's session as well as determining the impact on single server scalability. Administrators have the following options:

- Legacy - optimized for Windows 7 and Windows 2008R2 graphic engines (GDI/GDI+).
- Desktop Composition Redirection – offloads desktop Windows manager DirectX commands to the endpoint, but only supports a Windows desktop VDA. Plus, in the 7.15 LTSR release, Desktop Composition Redirection is a depreciated feature.
- Framehawk – a UDP-based protocol that is able to provide high refresh rates in environments with high latency and high packet loss scenarios at the cost of greater network bandwidth utilization, commonly found on broadband wireless connections.
- H.264 – Often referred as the video codec, which provides the highest frame rates required for high quality video while saving network bandwidth. It does come at the expense of CPU processing time, reducing single server scalability. H.264 is the preferred codec when users predominately use multimedia applications.
- Thinwire – Based on the original Citrix patents from the 1990s that thinly transfers data over a wire. Use Thinwire in the majority of use cases as it provides a good user experience with minimal resource costs. There are two variations of Thinwire:
  - Legacy - Optimized for Windows 7 and Windows 2008R2 graphic engines (GDI/GDI+).
  - Thinwire+ - Optimized for Desktop Windows Manager (DWM) graphics engine in Windows 8, Windows 10, Windows 2012 and Windows 2016
- Selective H.264 (Adaptive Display) - utilizes multiple codecs (H.264 and Thinwire+) simultaneously for portions of the screen
  - Do not use – Only uses Thinwire+ and not H.264. Best for users without server-rendered video or other graphically intense applications.
  - For entire screen – Only uses H.264. Best for users with heavy use of server-rendered video and 3D graphics, especially in low-bandwidth situations.
  - For actively changing regions – Uses H.264 for the portions of the screen that are constantly changing while the remainder of the screen uses Thinwire+. This is the best option for most users.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Selecting the right codec not only has an impact on the overall user experience, but also on the scalability of the server.



There are three ways to transport the HDX protocol across the network:

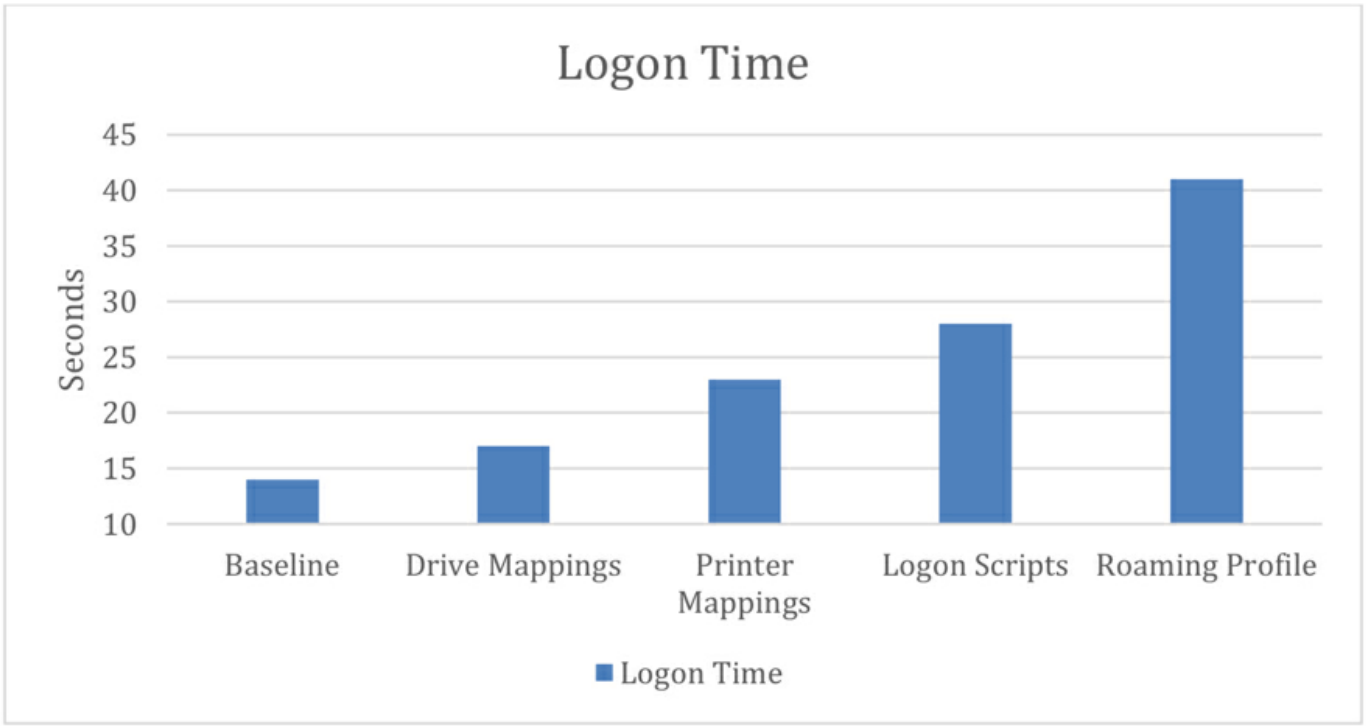
- **TCP** – Uses the industry standard TCP transport protocol. Common transport protocol over LAN and low-latency WAN connections, but suffers when connection distances increases, thus increasing latency and incurring more retransmissions.
- **EDT** – Uses a Citrix proprietary transport protocol called Enlightened Data Transport, based on UDP. Meant for high latency/packet loss networks, most common on long-distance WAN links. Provides a more interactive experience for the user without increasing CPU load on the server, but consumes more network bandwidth than TCP.
- **Adaptive Transport** – Uses TCP and EDT transport protocols. EDT used unless the network does not support transporting EDT over the network, which then automatically changes to TCP.

Most environments will use Adaptive Transport as the standard transport option unless the network does not have the appropriate firewall ports opened or NetScaler Gateway configured appropriately.

Every time a user logs onto a XenApp/XenDesktop session, the logon process must complete, which includes session initialization, user profile loading, group policy preferences execution, drive mapping, printer mapping, logon script execution and desktop initialization. Each process takes time and increases logon duration.

Most organizations include many mappings and complex logon scripts. When each of these items executes, the logon time drastically increases.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Workspace Environment Management removes drive mappings, printer mappings, logon scripts and roaming profiles from the standard logon process. With logon optimization, Workspace Environment Management applies the mappings/scripts/profiles in the background after the session and desktop initializes. The user receives the same environment but they receive their desktop interface faster. To learn more, review the following Logon Optimization video.

Most environments should enable logon optimization as a default configuration.

Self-service allows users to modify, update and troubleshoot their environments on their own without requiring help desktop intervention. Most organizations have policies in place that require users to change their passwords every 60-90 days. When users have multiple endpoint devices with saved passwords, it is extremely easy for their account to be locked out until each device is updated.

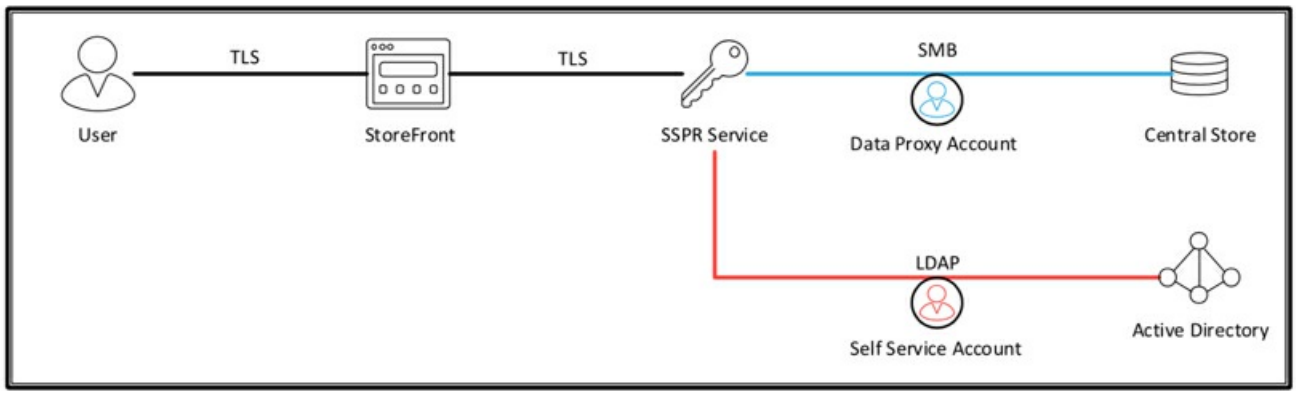
With StoreFront, can save time by self-servicing their own accounts with the following capabilities:

- **Account Unlock** – When the user's account is locked due to too many failed logon attempts, common with multiple devices, they can unlock their account if they know answers to their security questions.
- **Password Reset** – When users forgot their newly created password, they can reset their password if they know the answers to their security questions.

The self-service password reset architecture introduces the SSPR Service, Central Store and two accounts:

- **Data Proxy Account** – Responsible for accessing the central store, which contains encrypted answers to the user's security questions.
- **Self Service Account** – An Active Directory account with password reset and account unlock rights.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



In addition, properly designing self-service password reset requires the admin to create security questions that users will answer. Ideally, admins should create groups of questions around different categories then require users to answer a subset of questions for each group. The questions must be something the user knows that does not change and is not known by others.

A user's profile plays a critical role in delivering a consistently positive experience within a virtual desktop or virtual application scenario. Even a well-designed virtual desktop solution can fail if users are frustrated due to lengthy logon times or lost settings.

The user profile solution chosen must align with the personalization characteristics of the user group captured during the assess phase as well as the VDI model selected.

This section provides an overview on the different profile types available and provides guidance on the optimal user profile for each VDI model.

- **Local profiles** – Local profiles are stored on each server or desktop operating system and are initially created based on the default user profile. Therefore, a user accessing these resources would create an independent profile on each system. Users are able to retain changes to their local profile on each individual system, but changes are only accessible for future sessions on that system. Local profiles require no configuration; if a user logging into a server or desktop operating system does not have a profile path administratively defined, a local profile is created by default.
- **Roaming profiles** – Roaming profiles are stored in a centralized network repository for each user. Roaming profiles differ from local profiles in that the information in the profile (whether it is a printer, a registry setting, or a file stored in the documents folder) can be made available to user sessions accessed from all systems in the environment. Configuring a user for a roaming profile requires an administrator to designate the user's profile path (for virtual desktops) or terminal server profile path to a particular network share. The first time the user logs on to a server or desktop operating system, the default user profile is used to create the user's roaming profile. During logoff, the profile is copied to the administrator-specified network location.
- **Mandatory profiles** – Mandatory profiles are typically stored in a central location for many users. However, the user's changes are not retained at logoff. Configuring a user for a mandatory profile requires an administrator to create a mandatory profile file (NTUSER.MAN) from an existing roaming or local profile and assign users with a terminal services profile path. This can be achieved by means of Microsoft Group Policy, customizing the user properties in Active Directory or Citrix Profile Management.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Hybrid profiles** – Hybrid profiles combine a robust profile core (a mandatory profile or a local default profile) with user specific registry keys or files that are merged during logon. This technique enables administrators to tightly control which changes are retained and to keep the user profiles small in size. Furthermore, hybrid profiles address the last write wins issue using mature queuing techniques that automatically detect and prevent simultaneous writes that could potentially overwrite changes made in another session. Thus minimizing user frustration resulting from lost profile changes when accessing multiple servers or virtual desktops simultaneously. In addition, they capture and record only the changes within the profile, rather than writing the entire profile at logoff. A good example of a hybrid profile solution is Citrix Profile Management, which will be discussed in detail within this chapter.
  The following table compares the capabilities of each profile type.

  In the table:
  - **Y** indicates Functionality available.
  - **o** indicates Optional.
  - **N** indicates Functionality not available.

Feature	Local	Roaming	Mandatory	Hybrid
Central management / roams with user	N	Y	o	Yes
User settings are stored persistently	Y	Y	N	Yes
Granular capture of user settings	N	N	N	Yes

In order to select the optimal profile type for each user group it is important to understand their personalization requirements in addition to the VDI model assigned.

The following table provides recommendations on selecting the appropriate user profile type based on VDI resource:

In the table:

- **Y** indicates Recommended.
- **X** indicates Not Recommended.
- **o** indicates Viable.

	Local	Roaming	Mandatory	Hybrid
User setting persistence required (personalization characteristic: basic / complete)				
Hosted Windows App	X	Y	X	Y
Hosted Browser App	X	Y	X	Y

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Hosted Shared Desktop	X	Y	X	Y
Hosted Pooled Desktop	X	Y	X	Y
Hosted Personal Desktop	º	Y	X	Y
Hosted Pro Graphics Desktop	º	Y	X	Y
Local Streamed Desktop	X	Y	X	Y
Local VM Desktop	Y	º	X	º
Remote PC Access	Y	º	X	º
User setting persistence not required or not desired (personalization characteristic: none)				
Hosted Windows App	X	X	Y	X
Hosted Browser App	X	X	Y	X
Hosted Shared Desktop	X	X	Y	X
Hosted Pooled Desktop	Y	X	Y	X
Hosted Personal Desktop	X	X	Y	X
Hosted Pro Graphics Desktop	º	X	Y	X
Local Streamed Desktop	Y	X	Y	X

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Local VM Desktop	o	X	Y	X
Remote PC Access	o	X	Y	X

Redirecting special folders can supplement any of the described profile types. While redirecting profile folders, such as user documents and favorites, to a network share is a good practice to minimize profile size, architects need to be aware that applications may frequently read and write data to profile folders such as AppData, causing potential issues with file server utilization and responsiveness. It is important to thoroughly test profile redirection before implementation in production to avoid these issues. Therefore, it is important to research profile read / write activities and to perform a pilot before moving to production. Microsoft Outlook is an example of an application that regularly performs profile read activities, as the user signature is read from the user profile every time an email is created.

The following table provides general recommendations to help identify the appropriate folders to redirect:

In the table:

- Y indicates Recommended.
- X indicates Not Recommended.
- o indicates Viable.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Folder	Local	Roaming	Mandatory	Hybrid
Application Data	X	o	X	o
Contacts	X	Y	X	o
Desktop	X	Y	X	o
Downloads	X	o	X	o
Favorites	o	Y	o	Y
Links	X	Y	X	o
My Documents	o	Y	o	Y
My Music	o	Y	o	o
My Pictures	o	Y	o	o
My Videos	o	Y	o	o
Saved Games	X	o	X	o
Searches	X	Y	X	o
Start Menu	X	X	X	X

Excluding folders from being persistently stored as part of a roaming or hybrid profile can help to reduce profile size and logon times. By default Windows excludes the AppData\Local and AppData\LocalLow folders, including all subfolders, such as History, Temp and Temporary Internet Files. In addition, the downloads and saved games folders should also be excluded. All folders that are redirected should be excluded from the profile solution.

Local caching of roaming or hybrid user profiles on a server or virtual desktop is default Windows behavior and can reduce login times and file server utilization / network traffic. With profile caching, the system only has to download changes made

© 1999-2017 Citrix Systems, Inc. All rights reserved.

to the profile. The downside of profile caching is that it can consume significant amounts of local disk storage on multi-user systems, such as a hosted shared desktop hosts.

In certain VDI models and configurations, the VDI resource is reset to a pristine state. Having locally cached profiles be deleted upon logoff is an unnecessary consumption of resources. Based on this, the leading recommendation is to not deleting locally cached profiles for the following VDI models:

- Hosted Personal Desktops
- Hosted Pooled Desktops – only in situations where a reboot occurs after logoff.
- Local VM Desktops
- Remote PC Access

Configuring the "Delay before deleting cached profiles" Citrix policy sets an optional extension to the delay before locally cached profiles are deleted at logoff. Extending the delay is useful if a process keeps files or the user registry hive open during logoff. This can also reduce logoff times for large profiles.

For security reasons, administrators, by default, cannot access user profiles. While this level of security may be required for organizations that deal with very sensitive data, it is unnecessary for most environments and can complicate operations and maintenance. Therefore, consider enabling the "Add the Administrators security group to roaming user profiles" policy setting. The configuration of this policy should be aligned with the security characteristics of the user groups captured during the assess phase. For more information on the permissions required for the file share hosting user profiles and data, please refer to Microsoft TechNet - Deploying Roaming Profiles.

Determining the network path for the user profiles is one of the most significant decisions during a user profile design process. In general, it is strongly recommended to leverage a redundant and high performance file server or NAS device. There are four topics that must be considered for the profile share:

- **Performance** – File server performance will affect logon and logoff times, and depending on other decisions such as redirected folders and profile streaming, can impact the user's experience within the session. For large virtual desktop infrastructures, a single file server cluster may not be sufficient to handle periods of peak activity. In order to distribute the load across multiple file servers, the file server address and share name will need to be adjusted.
- **Location** – User profiles are transferred over the network by means of the SMB protocol, which does not perform well on high-latency network connections. Furthermore, WAN connections are typically bandwidth constrained, which can add additional delay to the profile load process. Therefore, the file server should be located in close proximity to the servers and virtual desktops to minimize logon times.
- **Operating system platforms** – User profiles have a tight integration with the underlying operating system and it is not supported to reuse a single user profile on different operating systems or different platforms like 64-Bit (x64) and 32-Bit (x86).
  For more information, please refer to the Microsoft knowledge base article KB2384951 – Sharing 32 and 64-bit User Profiles. Windows 2008 and Windows Vista introduced a new user profile structure, which can be identified by .V2 profile directory suffix, which makes older user profiles incompatible with newer operating systems such as Windows 2012, 7 and 8. In order to ensure that a separate profile is used per platform, the profile directory has to be adapted.
- **Indexing capabilities** – To take full advantage of Windows Search functionality on a user's redirected data, Windows file servers that index the user's data must be used, as opposed to a share on a NAS appliance. This is important for use cases that are heavily dependent on Windows Search or are especially sensitive to perception of slowness or latency

© 1999-2017 Citrix Systems, Inc. All rights reserved.

There are two methods that can be used to address these challenges that are based on Windows built-in technology:

- **User object** – For every user object in Active Directory, an individual profile path, which contains file server name and profile directory, can be specified. Since only a single profile path can be specified per user object, it is not possible to ensure that a separate profile is loaded for each operating system platform.
- **Computer group policy** or **system variables** – The user profile path can also be configured by means of computer specific group policies or system variables. This enables administrators to ensure that a user profile is dedicated to the platform. Since computer specific configurations affect all users of a system, all user profiles will be written to the same file server. To load balance user profiles across multiple servers dedicated XenDesktop delivery groups have to be created per file server.

Note: Microsoft does not support DFS-N combined with DFS-R for actively used user profiles.

For more information, please refer to the Microsoft articles:

- Information about Microsoft support policy for a DFS-R and DFS-N deployment scenario
- Microsoft Support Statement Around Replicated User Profile Data

When using Citrix Profile Management, a third option is available to address these challenges:

User object attributes and variables – Citrix Profile Management enables the administrator to configure the profile path by means of a computer group policy using attributes of the user object in Active Directory to specify the file server dynamically. In order to achieve this, three steps are required:

1. Create a DNS alias (for example, fileserver1) that refers to the actual file server
2. Populate an empty LDAP attribute of the user object (for example, l or UID) with the DNS Alias
3. Configure Citrix Profile Management by means of GPO to use a profile path that refers to the LDAP attribute (for example, if attribute UID is used the profile path becomes \\#UlD#\Profiles\profiledirectory)

In addition, Citrix Profile Management automatically populates variables to specify the profile path dynamically based on the operating system platform. Valid profile management variables are:

- !CTX_PROFILEVER! – Expands to v1 or v2 depending on the profile version.
- !CTX_OSBITNESS! – Expands to x86 or x64 depending on the bit-level of the operating system.
- !CTX_OSNAME! – Expands to the short name of the operating system, for example- Windows 7.

By combining both capabilities of Citrix Profile Management, a fully dynamic user profile path can be created, which can be load balanced across multiple file servers and ensure profiles of different operating system platforms are not mixed. An example of a fully dynamic user profile path is shown below:

\\#UID#\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!!CTX_OSBITNESS!

Note: The following design decision only applies to those environments that use Citrix Profile Management.

With user profile streaming, files and folders contained in a profile are fetched from the user store (file server) to the local computer when a user accesses them. During the logon process, Citrix Profile Management immediately reports that the profile load process has completed reducing profile load time to almost zero.

Citrix recommends enabling profile streaming for all scenarios. If it is desired to keep a local cached copy of the user profile for performance reasons, it is recommended to enable the “Always Cache” setting and configure a size of 0. This ensures

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

that the user profile is downloaded in the background and enables the system to use this cached copy going forward.

Experience from the Field

- General – Some poorly written applications might load faster if their AppData has already been streamed to the VDI resource. Enabling the "Always Cache" option for profile streaming can help improve performance when the AppData folder is not redirected.

Note: The following design decision only applies to those environments that use Citrix Profile Management.

By enabling the active write back feature, Citrix Profile Manager detects when an application has written and closed a file and copies the file back to the network copy of the profile during idle periods. In scenarios where a single user leverages multiple virtual desktops or hosted shared desktops simultaneously, this feature can be tremendously beneficial. However, Citrix Profile Management does not copy any registry changes back to the network, except during an ordered logoff. As such, there is a risk that the registry and files may get out of alignment on non-persistent systems, where locally cached profile information is wiped upon reboot. Therefore, it is recommended to disable active write back functionality for non-persistent scenarios.

Note: The following design decision only applies to those environments that use Citrix Profile Management.

Citrix Profile Management can be configured by means of an ".ini" file, Microsoft Group Policy and Citrix Policy (Citrix Profile Management 5.0 and newer). While each option offers the same configuration settings, Group Policy is recommended because it allows administrators to perform Windows and Citrix profile configurations from a single point, minimizing the tools necessary for profile management.

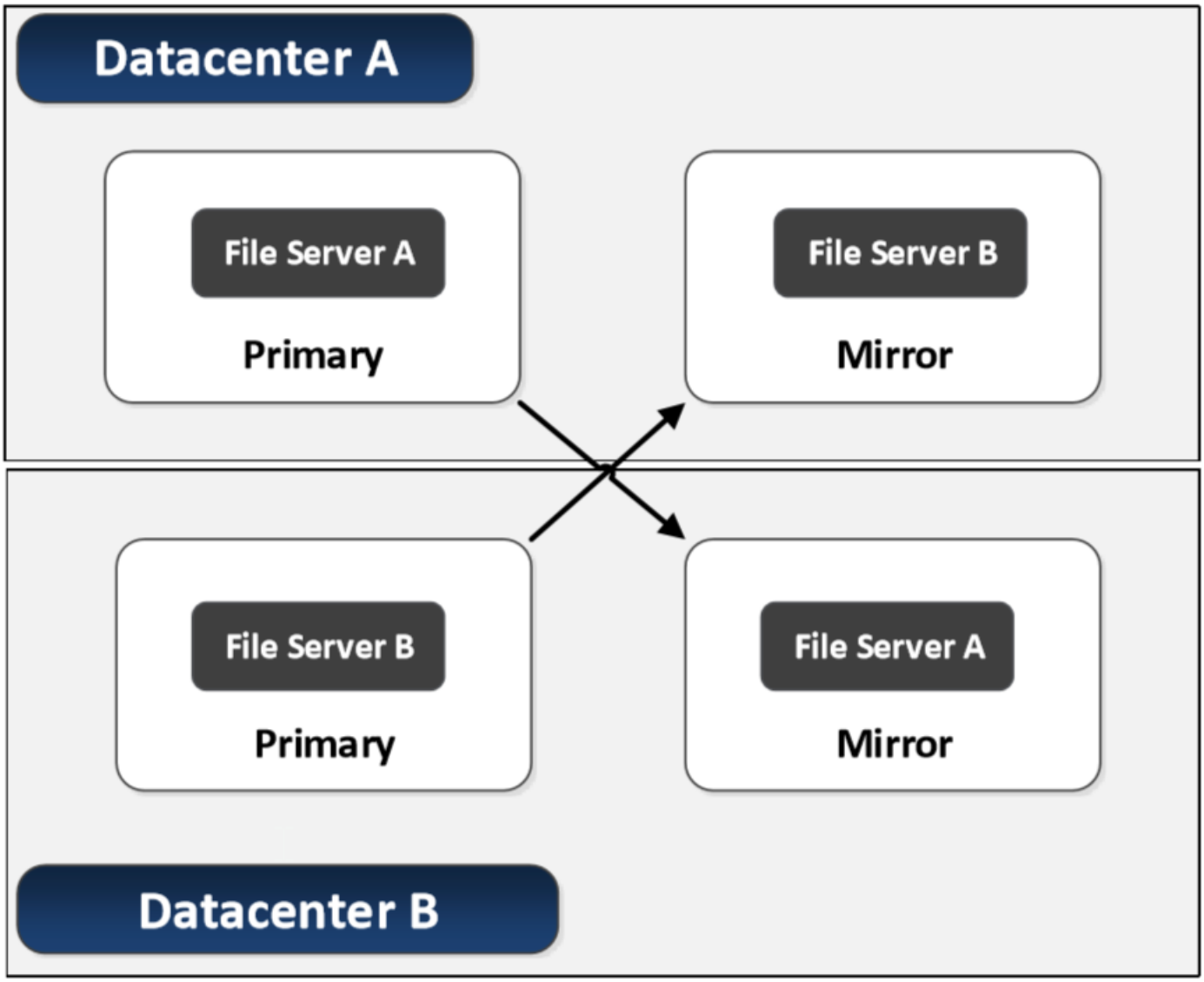
Note: With Citrix Profile Management 5.0 and newer, the desktop type is automatically detected and Citrix Profile Management policies set accordingly. For more information, please refer to Citrix Docs – How automatic configuration works.

While having an active/active datacenter on a network level is easily accomplished with GSLB, the replication of user data makes having a fully active/active deployment complex in most situations. To have an active/active configuration where users are not statically assigned to a specific datacenter, will require users to have no form of personalization requirements. This will limit the user's ability to make any configuration changes and will not allow them to create any documents or persistent data. The exception to this is when a high-speed, low latency connection such as dark fiber is available between datacenters. This will let resources in both locations can point to the same file server allowing for a true active/active solution. Also, an active/active configuration can be accomplished when applications are used that rely solely on a backend database that is actively replicated between datacenters and do not store any data in the user profile.

For redundancy and failover purposes, user data such as Windows profiles and documents should be synchronized between datacenters. Although it is recommended to replicate user data between datacenters, the replication would be an active/passive configuration. This means the data can only be actively consumed from a single datacenter. The reason for this limitation is the distributed file locking method inside Windows that only allows a single user to actively write to a file. Therefore, active/active replication of user data is not supported. Any supported configuration consists of a one-way replication of data that is active in a single datacenter at any point in time.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

For example, the figure below describes a scenario where user data is passively replicated from Datacenter A to Datacenter B. In this example, File Server A is the primary location for user data in Datacenter A and File Server B is the primary location in Datacenter B. One-way replication of the user data occurs for each fileserver to allow for the user data to be available in the opposite datacenter if a failover occurs. Replication technologies such as Microsoft DFS can be configured to mirror user profiles and documents to a file server in another datacenter. DFS Namespaces can also be used to have a seamless path for the location of the user data. However, implementing a replication solution like this requires an administrator familiar with Microsoft DFS and user profiles.



In order to be effective, users must access their data. The data must be in close proximity to the application for the user to have a good experience. As the distance between the application and data increases, latency also increases, which slows down any file operation (opening, saving, modifying).

In a VDI-based environment, administrators must understand where users store their data and impact of access.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

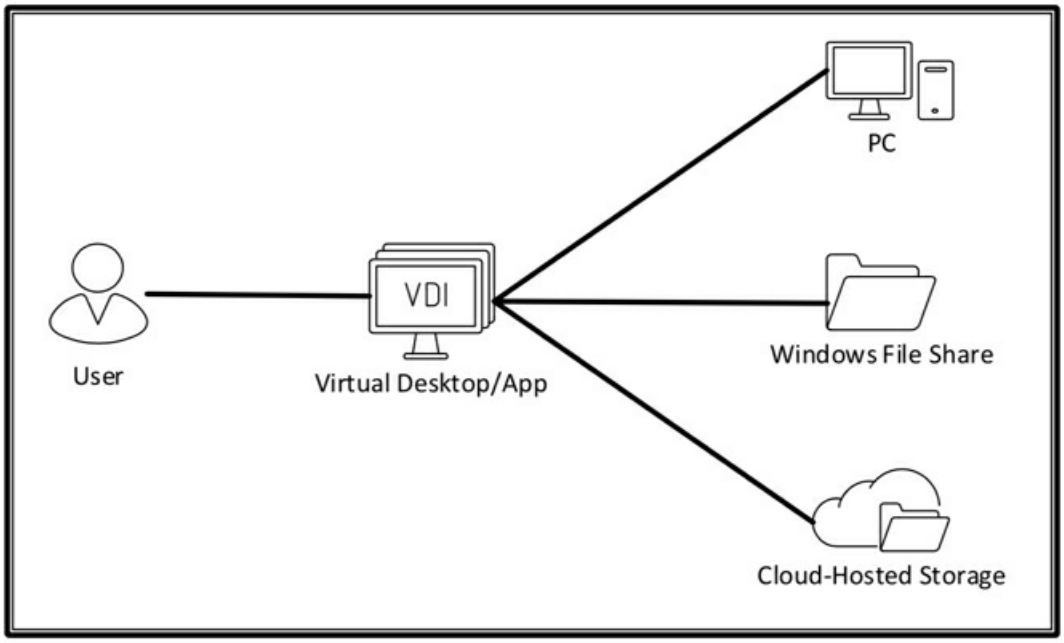
Users traditionally stored their data on their local device or on a network file server designated with a drive mapping. Due to IT storage space limitations or the inability to have the data follow the user to other mobile devices, users turned to free, cloud-based storage offerings like OneDrive, DropBox and Box. To get access to the data, the user would install the storage vendor's agent on their traditional Windows PC, allowing them direct access to the cloud-hosted storage repository.

Administrators must design the solution to take into account user storage by looking at the following options:

- **Multi-Agent Strategy** – In VDI, users require the admin to install and configure the agent for each storage provider, which assumes the storage agent supports the non-persistent VDI model. Each agent is a new application that the admin must manage and maintain.
- **Storage Connector Strategy** – A single agent consolidates storage repositories from numerous cloud-hosted and on-premises providers into a single folder structure. For example, when a user connects to Citrix ShareFile, they see a consolidated folder structure containing their user data from the cloud (ShareFile, OneDrive, DropBox, Box and Google Drive) and from on-premises (SharePoint, Windows network shares and local endpoint shares).

A critical aspect to a successful VDI solution is for the user experience to remain the same as it was with a traditional PC. If users open files from within the application, that functionality must continue to function. If users navigate with Explorer to access a file, that functionality must continue to function.

A user's data can exist on the local PC, on a network file share and hosted in the cloud.



With local PC, on-premises network shares and cloud-hosted storage options available to users, administrators need to understand how users accessing their data affects the infrastructure and VDI experience.

- **Direct Data Access** – Users access a file on a remote server (on-premises Windows server or cloud-hosted storage provider). The distance between the application and file directly affects the experience. Longer distances equates to higher latency. Each file operation (navigate, open, close, save, etc.) takes more time as the latency between application and file storage increases. Windows file servers are often located in the same data center as the user's VDI desktop

© 1999-2017 Citrix Systems, Inc. All rights reserved.

making direct data access feasible; but cloud-hosted solutions and local PC Access will experience poor response times if the connection between the VDI desktop and the storage repository has high latency.

- **Local Synchronization** – With a traditional PC, users are accustomed to having files local, which mitigates any slow application response times due to extremely low latency. Many cloud-hosted solutions provide data synchronization to enable access speeds similar to a local storage model. Many of the cloud-hosted solutions provide full synchronization or user-configured partial synchronization of certain folders and files. With partial synchronization, only the synchronized files are visible and accessible on the device, causing user confusion. Full and partial synchronization increases VDI costs. Each session is an entirely new desktop requiring synchronization of user's folders/files, which takes time, network bandwidth and VDI storage space. Every file synchronized to the VDI desktop must be stored within the organization's data center for the duration of the VDI session.
- **On-Demand Synchronization** – When navigating Explorer, users see a complete, but virtual, file/folder structure even though those files/folders do not physically exist on the desktop. Selecting a file begins an automatic synchronization to the VDI desktop for that single file. At this point, file access is local, which creates a user experience like that of a traditional PC. When the user saves or closes the file, the file synchronizes back to the cloud. Only the files accessed synchronize, eliminating the waste incurred with the local data access model. Citrix ShareFile includes Drive Mapper, allowing the user to interact with their data via Explorer while utilizing on-demand synchronization when accessing a file. As only accessed files synchronize, the impact to the underlying storage infrastructure and associated storage costs are minimal.

In the table:

- **Y** indicates recommended.
- **N** indicates Not recommended.

	Direct Data Access	Local Synchronization	On-Demand Synchronization
Network File Server	Y		
Cloud-hosted	N	N	Y
Local PC	N	N	Y

File corruption is an issue most users experience. Improperly shutting down the application or PC (hitting the power button instead of closing the application and shutting down the operating system gracefully) often causes many corruption issues.

A few options exist to provide users with data recovery options:

- **Multi-File** – With a traditional PC, users have few recovery options if the files are local. Users often manually create a new copy of the file each day in order to provide some level of recovery. This solution is hard to manage.
- **Backup/Restore** – Administrators can implement a backup and restore solution to help with file recovery. However, these solutions rarely work with local files and for a network file share, the backup process usually only runs nightly or weekly. In addition, restoring a corrupted file requires the user to call support.
- **Versioning** –Cloud-hosted options, like Citrix ShareFile, include file versioning, which automatically creates new versions

© 1999-2017 Citrix Systems, Inc. All rights reserved.

of the file as changes are saved. Versioning requires no user intervention and allows users to recover from corruption quickly and with little loss of data.



Uploaded	Title	Creator
7/20/17 3:22 ...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller
7/20/17 2:15 ...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller
7/20/17 1:16 ...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller
7/20/17 1:08 ...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller
7/20/17 1:07 ...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller
7/20/17 12:5...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller
7/20/17 12:5...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller
7/20/17 12:1...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller

Policies provide the basis to configure and fine tune XenApp and XenDesktop environments, allowing organizations to control connection, security and bandwidth settings based on various combinations of users, devices or connection types.

When making policy decisions it is important to consider both Microsoft and Citrix policies to ensure that all user experience, security and optimization settings are considered. For a list of all Citrix-related policies, please refer to the Citrix Policy Settings Reference.

Organizations have the option to configure Citrix policies via Citrix Studio or through Active Directory group policy using Citrix ADMX files, which extend group policy and provide advanced filtering mechanisms.

Using Active Directory group policy allows organizations to manage both Windows policies and Citrix policies in the same location, and minimizes the administrative tools required for policy management. Group policies are automatically replicated across domain controllers, protecting the information and simplifying policy application.

Citrix administrative consoles should be used if Citrix administrators do not have access to Active Directory policies. Architects should select one of the above two methods as appropriate for their organization's needs and use that method consistently to avoid confusion with multiple Citrix policy locations.

It is important to understand how the aggregation of policies, known as policy precedence flows in order to understand how a resultant set of policies is created. With Active Directory and Citrix policies, the precedence is as follows:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Policy Precedence	Policy Type
Processed first (lowest precedence)	Local server policies
Processed second	Citrix policies created using the Citrix administrative consoles
Processed third	Site level AD policies
Processed fourth	Domain level AD policies
Processed fifth	Highest level OU in domain
Processed sixth and subsequent	Next level OU in domain
Processed last (highest precedence)	Lowest level OU containing object

Policies from each level are aggregated into a final policy that is applied to the user or computer. In most enterprise deployments, Citrix administrators do not have rights to change policies outside their specific OUs, which will typically be the highest level for precedence. In cases where exceptions are required, the application of policy settings from higher up the OU tree can be managed using “block inheritance” and “no override” settings. Block inheritance stops settings from higher-level OUs (lower precedence) from being incorporated into the policy. However, if a higher-level OU policy is configured with no override, the block inheritance setting will not be applied. Given this, care must be taken in policy planning, and available tools such as the “Active Directory Resultant Set of Policy” tool or the “Citrix Group Policy Modeling” wizard should be used to validate the observed outcomes with the expected outcomes.

> **注意**
>
> Some Citrix policy settings, if used, need to be configured through Active Directory group policy, such as Controllers and Controller registration port, as these settings are required for VDAs to register.

When configuring policies, organizations often require both Active Directory policies and Citrix policies to create a completely configured environment. With the use of both policy sets, the resultant set of policies can become confusing to determine. In some cases, particularly with respect to Windows Remote Desktop Services (RDS) and Citrix policies, similar functionality can be configured in two different locations. For example, it is possible to enable client drive mapping in a Citrix policy and disable client drive mapping in a RDS policy. The ability to use the desired feature may be dependent upon the combination of RDS and Citrix policy. It is important to understand that Citrix policies build upon functionality available in Remote Desktop Services. If the required feature is explicitly disabled in RDS policy, Citrix policy will not be able to affect a configuration as the underlying functionality has been disabled.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

In order to avoid this confusion, it is recommended that RDS policies only be configured where required and there is no corresponding policy in the XenApp and XenDesktop configuration, or the configuration is specifically needed for RDS use within the organization. Configuring policies at the highest common denominator will simplify the process of understanding resultant set of policies and troubleshooting policy configurations.

Once policies have been created, they need to be applied to groups of users and/or computers based on the required outcome. Policy filtering provides the ability to apply policies against the requisite user or computer groups. With Active Directory based policies, a key decision is whether to apply a policy to computers or users within site, domain or organizational unit (OU) objects. Active Directory policies are broken down into user configuration and computer configuration. By default, the settings within the user configuration apply to users who reside within the OU at logon, and settings within the computer configuration are applied to the computer at system startup, and will affect all users who logon to the system. One challenge of policy association with Active Directory and Citrix deployments revolves around three core areas:

- **Citrix environment specific computer policies** – Citrix servers and virtual desktops often have computer policies that are created and deployed specifically for the environment. Applying these policies is easily accomplished by creating separate OU structures for the servers and the virtual desktops. Specific policies can then be created and confidently applied to only the computers within the OU and below and nothing else. Based upon requirements, virtual desktops and servers may be further subdivided within the OU structure based on server roles, geographical locations or business units.
- **Citrix specific user policies** – When creating policies for XenApp and XenDesktop there are a number of policies specific to user experience and security that are applied based on the user's connection. However, the user's account could be located anywhere within the Active Directory structure, creating difficulty with simply applying user configuration based policies. It is not desirable to apply the Citrix specific configurations at the domain level as the settings would be applied to every system any user logs on to. Simply applying the user configuration settings at the OU where the Citrix servers or virtual desktops are located will also not work, as the user accounts are not located within that OU. The solution is to apply a loopback policy, which is a computer configuration policy that forces the computer to apply the assigned user configuration policy of the OU to any user who logs onto the server or virtual desktop, regardless of the user's location within Active Directory. Loopback processing can be applied with either merge or replace settings. Using replace overwrites the entire user GPO with the policy from the Citrix server or virtual desktop OU. Merge will combine the user GPO with the GPO from the Citrix server or desktop OU. As the computer GPOs are processed after the user GPOs when merge is used, the Citrix related OU settings will have precedence and be applied in the event of a conflict. For more information, please refer to the Microsoft TechNet article - Understand User Group Policy Loopback Mode.
- **Active Directory policy filtering** – In more advanced cases, there may be a need to apply a policy setting to a small subset of users such as Citrix administrators. In this case, loopback processing will not work, as the policy should only be applied to a subset of users, not all users who logon to the system. Active Directory policy filtering can be used to specify specific users or groups of users to which the policy is applied. A policy can be created for a specific function, and then a policy filter can be set to apply that policy only to a group of users such as Citrix administrators. Policy filtering is accomplished using the security properties of each target policy.

Citrix policies created using Citrix Studio have specific filter settings available, which may be used to address policy-filtering situations that cannot be handled using group policy. Citrix policies may be applied using any combination of the following filters:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Filter Name	Filter Description	Scope
Access control	Applies a policy based on access control conditions through which a client is connecting. For example, users connecting through a Citrix NetScaler Gateway can have specific policies applied.	User settings
Citrix CloudBridge	Applies a policy based on whether or not a user session was launched through Citrix CloudBridge.	User settings
Client IP address	Applies a policy based on the IPv4 or IPv6 address of the user device used to connect the session. Care must be taken with this filter if IPv4 address ranges are used in order to avoid unexpected results.	User settings
Client name	Applies a policy based on the name of the user device used to connect the session.	User settings
Delivery group	Applies a policy based on the delivery group membership of the desktop running the session.	User settings
Delivery group type	Applies a policy based on the type of machine running the session. For example, different policies can be set depending upon whether a desktop is pooled, dedicated or streamed.	User and computer settings
Organizational unit	Applies a policy based on the OU of the desktop or server running the session.	User and computer settings
Tag	Applies a policy based on any tags applying to the desktop running the session. Tags are strings that can be added to virtual desktops in XenDesktop environments that can be used to search for or limit access to desktops.	User and computer settings
User or Group	Applies a policy based on the Active Directory group membership of the user connecting to the session.	User settings

> **注意**
>
> Citrix policies in XenDesktop 7.x provide a merged view of settings that apply at the user and computer level. In table 24, the Scope column identifies whether the specified filter applies to user settings, computer settings, or both.

A baseline policy should contain all common elements required to deliver a high-definition experience to the majority of users within the organization. A baseline policy creates the foundation for user access, and any exceptions that may need to be created to address specific access requirements for groups of users. It should be comprehensive to cover as many use cases as possible and should have the lowest priority, for example 99 (a priority number of “1” is the highest priority), in order to create the simplest policy structure possible and avoid difficulties in determining the resultant set of policies. The unfiltered policy set provided by Citrix as the default policy may be used to create the baseline policy as it is applied to all users and connections. In the baseline configuration, all Citrix policy settings should be enabled, even those that will be

© 1999-2017 Citrix Systems, Inc. All rights reserved.

configured with the default value, in order to explicitly define desired/expected behavior, and to avoid confusion should default settings change over time.

Citrix Policy templates can be used to configure Citrix policies to effectively manage the end-user experience within an environment and can serve as an initial starting point for a baseline policy. Templates consist of pre-configured settings that optimize performance for specific environments or network conditions. The built-in templates included in XenDesktop are shown below:

Built-in Templates	Description
High definition user experience	Includes settings for providing high quality audio, graphics, and video to users.
High server scalability	Includes settings for providing an optimized user experience while hosting more users on a single server.
Optimized bandwidth for WAN	Includes settings for providing an optimized experience to users with low bandwidth or high latency connections.
Security and control	Includes settings for disabling access to peripheral devices, drive mapping, port redirection, and Flash acceleration on user devices.

For more information on Citrix policy templates, please refer to Citrix Docs - Manage Citrix Policy Templates.

A baseline policy configuration should also include Windows policies. Windows policies reflect user specific settings that optimize the user experience and remove features that are not required or desired in a XenDesktop environment. For example, one common feature turned off in these environments is Windows update. In virtualized environments, particularly where desktops and servers may be streamed and non-persistent, Windows update creates processing and network overhead, and changes made by the update process will not persist a restart of the virtual desktop or application server. Also in many cases, organizations use Windows software update service (WSUS) to control Windows updates. In these cases, updates are applied to the master disk and made available by the IT department on a scheduled basis.

In addition to the above considerations, an organization's final baseline policy may include settings specifically created to address security requirements, common network conditions, or to manage user device or user profile requirements:

Citrix XenApp and Citrix XenDesktop support a variety of different printing solutions. In order to plan and successfully implement the proper printing solution it is important to understand the available technologies as well as their benefits and limitations.

The process of creating printers at the start of a XenApp or XenDesktop session is called printer provisioning. There are multiple approaches available:

- User Added – Allowing users to manually add printers gives them the flexibility to select printers by convenience. The drawback to manually adding network-based printers is that it requires the users to know the network name or path of the printers. There is also a chance that the native print driver is not installed in the operating system and the Citrix

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Universal Print Driver is not compatible, thereby requiring the user to seek administrative assistance. Manually adding printers is best suited in the following situations:
  - Users roam between different locations using the same client device (i.e. laptop, tablet).
  - Users work at assigned stations or areas whose printer assignments will rarely change.
  - Users have personal desktops with sufficient rights to install necessary printer drivers.
- **Auto Created** – Auto-creation is a form of dynamic provisioning that attempts to create some or all of the available printers on the client device at the start of a user session. This includes locally attached printers as well as network-based printers. Auto-creating all client printers can increase the session logon time as each printer is enumerated during the logon process.
- **Session Based** – Session printers are a set of network-based printers assigned to users through a Citrix policy at the start of each session.
  - Proximity based session printers are filtered by IP subnet. The network printers created under this policy may vary based on where the user's endpoint device is located. Proximity printing is recommended in situations where: Users roam between different locations using the same endpoint device (i.e. laptop, tablet) and where thin clients are used, which do not have the ability to connect to network-based printers directly.
  - Session printers may be assigned using the "Session Printer" policy or the "Printer Assignments" policy. The "Session printer" policy is intended to be used to set default printers for a farm, site, large group, or OU. The "Printer Assignments" policy is used to assign a large group of printers to multiple users. If both policies are enabled and configured, the session printers will be merged into a single list.
- **Universal Printer** – The Citrix Universal Printer is a generic printer object that is autocreated at the start of a session and is not linked to a printing device. When using the Citrix Universal Printer, it is not required to enumerate the available client printers during logon, which can greatly reduce resource usage and decrease user logon times. By default, the Citrix Universal Printer will print to the client's default printer, however the behavior can be modified to allow the user to select any of their compatible local or network-based printers.

The Citrix Universal Printer is best suited for the following scenarios:

- The user requires access to multiple printers both local and network-based which may vary with each session.
- The user's logon performance is a priority and the Citrix policy "Wait for printers to be created" must be enabled due to application compatibility.
- The user is working from a Windows based device or thin client.

> **注意**
>
> Other options for provisioning printers, such as Active Directory group policy, "follow-me" centralized print queue solutions, and other 3rd party print management solutions can be used to provision printers into a Citrix session.

Managing print drivers in XenApp and XenDesktop can be a tedious task, especially in large environments with hundreds of printers. In XenApp and XenDesktop there are several methods available to assist with print driver management.

- **User Installed** – When adding a printer within a XenApp or XenDesktop session and the native print driver is not available, the drivers can be installed manually, by the user. Many different print drivers can potentially be installed on different resources creating inconsistencies within the environment. Troubleshooting printing problems and maintenance of print drivers can become very challenging since every hosted resource may have different sets of print drivers installed. To ensure consistency and simplify support and troubleshooting, user installed drivers is not recommended.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

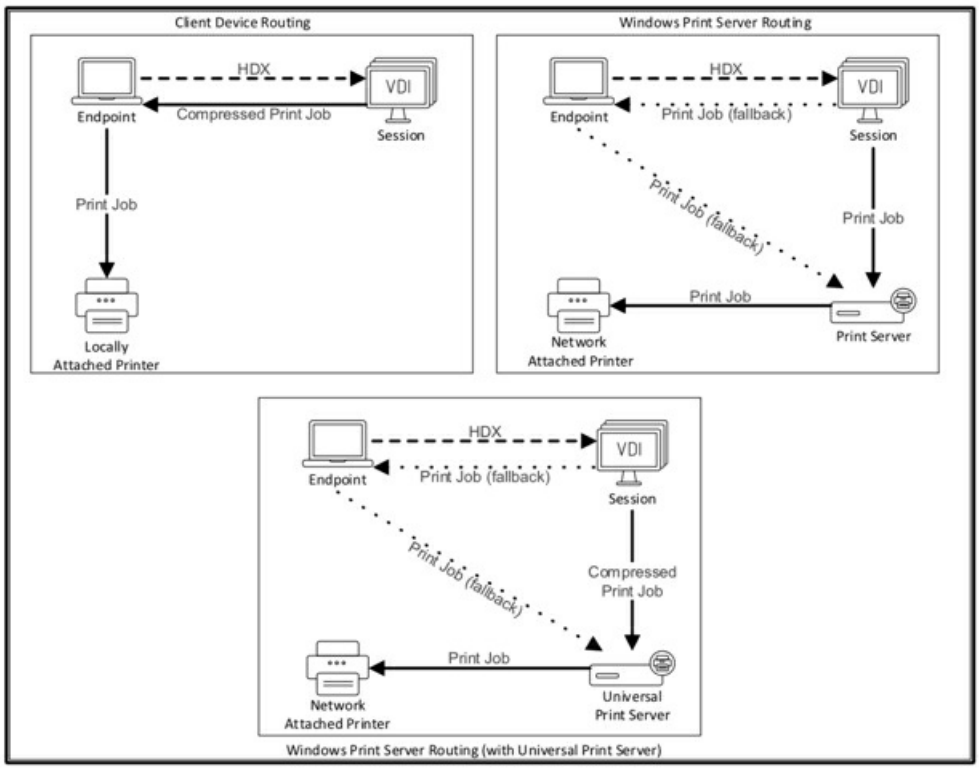
- **Automatic Installation** – When connecting a printer within a XenApp or XenDesktop session, a check is made to see if the required print driver is already installed in the operating system. If the print driver is not already installed, the native print driver, if one exists, will be installed automatically. If users roam between multiple endpoints and locations, this can create inconsistencies across sessions since users may access a different hosted resource every time they connect. When this type of scenario occurs, troubleshooting printing problems and maintenance of print drivers can become very challenging since every hosted resource may have different sets of print drivers installed. To ensure consistency and simplify support and troubleshooting, automatic installed drivers is not recommended.
- **Universal Print Driver** – The Citrix Universal Printer Driver (UPD) is a device independent print driver, which has been designed to work with most printers. The Citrix Universal Printer Driver (UPD) simplifies administration by reducing the number of drivers required on the master image. For auto created client printers, the driver records the output of the application and sends it, without any modification, to the end-point device. The endpoint uses local, device-specific drivers to finish printing the job to the printer. The UPD can be used in conjunction with the Citrix Universal Print Server (UPServer) to extend this functionality to network printers.

Print jobs can be routed along different paths: through a client device or through a print server.

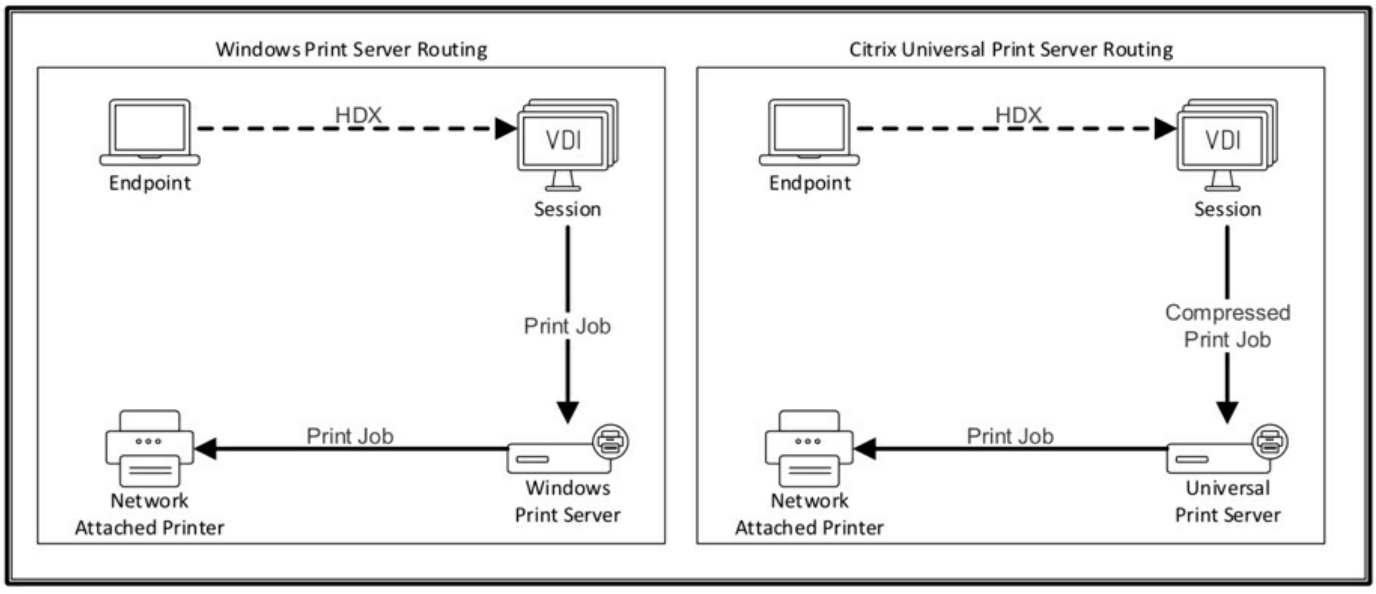
- **Client Device Routing** – Client devices with locally attached printers (printers attached through USB, LPT, COM, TCP, etc.) will route print jobs directly from the client device to the printer.
- **Windows Print Server Routing** – By default, print jobs sent to auto-created networkbased printers will be routed from the user's session to the print server. However, the print job will take a fallback route through the client device when any of the following conditions are true:
  - The session cannot contact the print server
  - The print server is on a different domain without a trust established.
  - The native print driver is not available within the user's session
- **Citrix Universal Print Server Routing** – Print job routing follows the same process as Windows Print Server Routing except that the Universal Print Driver is used between the user's session and the Citrix Universal Print Server.

The specifics with print job routing are based on the printer provisioning method. Auto-created and user-added printers can route print jobs based on the following diagrams:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



However, if the printers are provisioned as session printers, the print job routing options changes slightly. The jobs are no longer able to route through the user's endpoint device.



The recommended option is based on the network location of the endpoint device, the user's session and the print server.

- Client Device Routing
  - Use for locally attached printer implementations.
  - Use if a Windows endpoint device and printer are on the same high-speed, lowlatency network as the Windows Print

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Server.

- **Windows Print Server Routing**
  - Use if the printer is on the same high-speed, low-latency network as the Windows Print Server and user session.
- **Windows Print Server Routing (with Universal Print Server)**
  - Use if non-Windows endpoint device and printer are on the same high-speed, low-latency network as the Windows Print Server.

Network-based printers, managed with a Microsoft print server or the Citrix Universal Print Server should be configured with redundancy in order to eliminate a single point of failure. The Citrix Universal Print Server redundancy should be defined within a Citrix Policy.

Experience from the Field

A print media company leverages Thin Clients and Windows-based workstations at the company headquarters. Network based printers are placed throughout the building (one per floor). Windows print servers reside in the datacenter and manage the network printers. XenDesktop and XenApp servers also reside in the datacenter.

A regional office has numerous Windows, Linux and Mac endpoints with network attached printers. A remote branch office has a few Windows workstations with locally attached printers.

Three different print strategies are applied:

- **Headquarters** - A Citrix Universal Print Server is used for printing within the XenApp and XenDesktop session. Native print drivers are not required on the Windows based workstations. A session printer policy is configured per floor which connects the floor printer as the default printer. The policies are filtered based on the subnet of the thin client for proximity printing. Quality of Service (QoS) policies are implemented. Inbound and outbound network traffic on ports TCP 1494 and TCP 2598 are prioritized over all other network traffic. This will prevent HDX user sessions from being impacted by large print jobs.
- **Regional Office** - A Universal Print Server is deployed within the regional office. The print job uses the Universal Print Driver and is compressed and delivered from the user's session to the Universal Print Server, across the WAN. The job is then sent to the network-attached printer in the office.
- **Branch Office** - Since all branch users work on Windows based workstations, auto-created client printers in conjunction with the Citrix Universal Printer Driver are used. Since the print job is delivered over ICA, the print data is compressed which saves bandwidth. The Citrix Universal Printer Driver ensures all printers connected to the client can be used within the XenApp or XenDesktop session without concern of the printer model used.

Properly integrating an application requires understanding compatibility and how the user/business requirements influences the appropriate delivery method.

VDI typically requires significant changes to be made to an organization's application delivery and management strategy. For example, many organizations will take the opportunity to upgrade their desktop operating system and to simplify management by reducing the number of applications installed into the base image using techniques such as application streaming and application layering. These are significant changes that require comprehensive compatibility testing. Important compatibility requirements that may need to be verified include:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Operating system** – The application must be compatible with the preferred operating system.
- **Multi-User** – Some applications may be more appropriate for delivery via a hosted shared desktop or a hosted Windows App. In these situations, the compatibility of the application must be verified against the multi-user capabilities of a server operating system like Windows Server 2012R2.
- **Application architecture** – It is important to understand whether the application includes 16-bit, 32-bit or 64-bit code so that an appropriate operating system can be selected. 16-bit code cannot be executed on a 64-bit operating system. However, a 16-bit application can be delivered to users as a Hosted Windows App from a 32-bit desktopbased operating system like x86 editions of Windows 7, 8 or 10.
- **Interoperability** – Some applications may experience complications if they coexist on the same operating system. Possible causes include shared registry hives, dll files or INI files as well as incompatible dependencies. Application interoperability issues should be identified so that appropriate remediation steps can be taken or an alternative delivery model selected.
- **Dependency** – Applications may need to interact with each other to provide the users with a seamless experience. For example, applications that present information in a PDF format require a suitable PDF viewer to be available. Many times, the dependent (child) applications are version specific to the parent application.
- **Application virtualization** – The use of application virtualization techniques, like streaming and layering, helps to simplify image management by reducing the number of applications installed into the base image. However, not all applications are suitable for streaming and layering because they may install device drivers, use COM+ or form part of the operating system.

Application compatibility can be achieved by doing a combination of manual, user testing, utilizing pre-verified lists maintained by the software vendor, or using an automated application compatibility solution, like Citrix AppDNA, which runs through thousands of tests to verify compatibility.

It is unlikely that a single delivery method will meet all requirements. Based on the outcome of the application categorization assessment process and the overall image management strategy (installed images, scripted images and layered images), several application delivery methods can be considered.

Choosing one of the appropriate application delivery method helps improve scalability, management and user experience.

- **Installed app** – The application is part of the base desktop image. The install process involves dll, exe and other files copied to the image drive as well as registry modifications.
- **Streamed App (Microsoft App-V)** – The application is profiled and delivered to the desktops across the network on-demand. Application files and registry settings placed in a container on the virtual desktop and isolated from the base operating system and each other, which helps to address compatibility issues.
- **Layered App (Citrix App Layering)** – Each layer contains a single application, agent or operating system. Layering simplifies ongoing maintenance, as an OS, agent and application exists in a single layer; update the layer and all deployed images containing that layer are updated. App Layering has two different delivery options:
  - **Layered Image** – By integrating one OS layer, one platform layer (XenApp/XenDesktop VDA, Provisioning Services agent) and many application layers, an administrator can easily create new, deployable images.
  - **Elastic Layer** – A XenApp and XenDesktop user can dynamically receive a new app layer based at logon. On a XenApp host, an elastic layer is session-aware, where an attached layer is only available to a user's session granted access to the layer.
- **Hosted Windows App** - An application installed on a multi-user XenApp host and deployed as an application and not a desktop. A user accesses the hosted Windows app seamlessly from the VDI desktop or endpoint device, hiding the fact that the app is executing remotely.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Local App** – An application deployed on the endpoint device. The application interface appears within the user's hosted VDI session even though it executes on the endpoint.

The following table provides recommendations on the preferred approaches for integrating applications into the overall solution.

In the table:

- **Y** indicates Recommended.
- **N** indicates Not Recommended.
- **o** indicates Viable.

App Category	Installed App	Streamed App	Layered App	Hosted Windows App	Local App
Common	Y	o	Y	o	N
Departmental	o	Y	Y	Y	N
User	N	o	Y	o	Y
Management	Y	N	Y	o	N

Experience from the Field

- **Energy** – An energy company installs applications on the base image for the majority of users and streams departmental applications as required.
- **Financial** – A banking customer maintains and deploys multiple desktop images containing user group focused applications as required by various departments.

Virtual resources require proper allocation of the processor, memory and disk. These decisions have a direct impact on the amount of hardware required as well as the user experience.

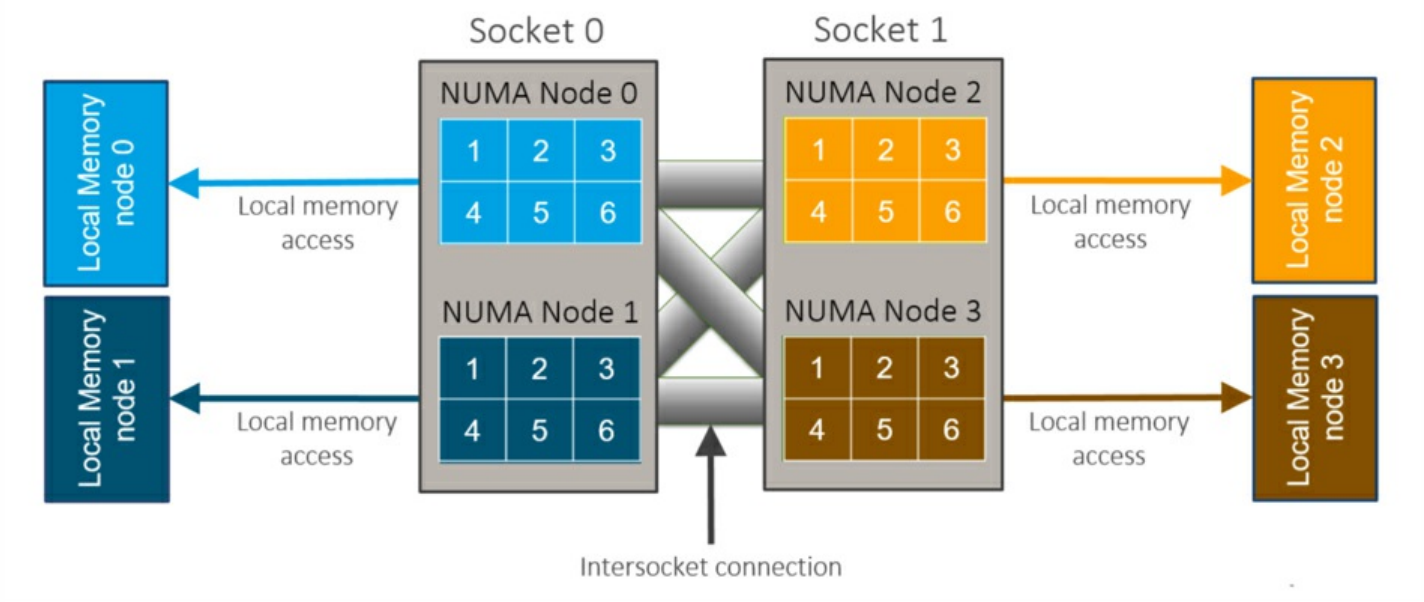
The key to successful resource allocation is to ensure that virtual desktops and applications offer similar levels of performance to physical desktops. Otherwise, productivity and overall user satisfaction will be affected. Allocating resources to the virtual machines above their requirements however is inefficient and expensive for the business.

The resources allocated should be based on the workload characteristic of each user group, identified during the assess phase.

For hosted desktop-based VDI models (hosted pooled desktops and hosted personal desktops), the general recommendation is two or more vCPUs per virtual machine so that multiple threads can be executed simultaneously. Although a single vCPU could be assigned for extremely light workloads, users are more likely to experience session hangs.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

For hosted server-based VDI models (hosted Windows apps, hosted browser apps, hosted shared desktops), the proper vCPU allocation is based on the Non-Uniform Memory Access (NUMA) architecture of the processors.



Each socket is divided into one or more NUMA nodes. Hosted server-based VDI models will often utilize 4 or more processors. Allocating more vCPU than the NUMA node contains results in a performance hit. Allocating a portion of a NUMA node to a virtual machine results in a performance hit if the portion allocated is not easily divisible by the size of the NUMA node. It is often ideal to allocate the number of cores within a NUMA node to a virtual machine or allocate ½ of the cores to a virtual machine, while doubling the number of virtual machines.

User Workload	Operating System	vCPU Configured for Scale	vCPU Configured for Experience
Light	Windows 7	2 vCPU	2 vCPU
	Windows 10	2 vCPU	2 vCPU
	Windows 2012R2	NUMA or ½ of NUMA	NUMA or ½ of NUMA
	Windows 2016	NUMA or ½ of NUMA	NUMA or ½ of NUMA
Medium	Windows 7	2 vCPU	3 vCPU
	Windows 10	2 vCPU	3 vCPU
	Windows 2012R2	NUMA or ½ of NUMA	NUMA or ½ of NUMA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Windows 2016	NUMA or ½ of NUMA	NUMA or ½ of NUMA
Heavy	Windows 7	3 vCPU	4 vCPU
	Windows 10	3 vCPU	4 vCPU
	Windows 2012R2	NUMA or ½ of NUMA	NUMA or ½ of NUMA
	Windows 2016	NUMA or ½ of NUMA	NUMA or ½ of NUMA

> **注意**
>
> Windows 2012 R2 recommendations are based on the hosted Windows app, hosted browser app and hosted shared desktop VDI model.

In a shared and virtualized environment, a single user can monopolize CPU resources due to a runaway process or an intense data processing operation in Excel. If the processor is oversubscribed, it will not be able to fulfill other users' requests, resulting in a hung session.

Citrix Workspace Environment Management, a component of XenApp and XenDesktop, incorporates CPU optimization. When a process consumes a certain percentage of the CPU over a defined timeframe, the process priority lowers from normal to low or very low, giving all remaining processes a higher priority and overcoming the runaway process risk. CPU optimization will also remember processes that triggered CPU protection and automatically start the process at a lower priority on future launches.

Most environments should enable CPU optimization as a default configuration.

The amount of memory allocated to each resource is a function of the user's expected workload and application footprint. Assigning insufficient memory to the virtual machines will cause excessive paging to disk, resulting in a poor user experience; allocating too much RAM increases the overall cost of the solution.

The following table provides guidance on the virtual RAM that should be assigned based on workload.

User Workload	Operating System	vRAM Configured for Scale	vRAM Configured for Experience
Light	Windows 7	2 GB	3 GB

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Windows 10	2 GB	3 GB
	Windows 2012R2	256 MB per user	
	Windows 2016	320 MB per user	
Medium	Windows 7	3 GB	4 GB
	Windows 10	3 GB	4 GB
	Windows 2012R2	512 MB per user	
	Windows 2016	640 MB per user	
Heavy	Windows 7	6 GB	8 GB
	Windows 10	6 GB	8 GB
	Windows 2012R2	1024 MB per user	
	Windows 2016	1280 MB per user	

注意

- Windows 2012R2 recommendations are based on the hosted Windows app, hosted browser app and hosted shared desktop VDI model.
- Memory allocation above 4GB requires a 64-bit operating system.
- If used, the Machine Creation Services and Provisioning Services cache in RAM amount should be added onto the virtual machine RAM specifications.

Even though users only work within a single application at a time, most have five or more applications running but idle. When a process moves from active to idle, the application and operating system releases a portion of the process's active working set of memory to free up system resources. However, this is only a small percentage of the applications working set. The rest remains locked for the application, severely limiting available system resources.

Using RAM Optimization within Citrix Workspace Environment Management, applications that are idle (have not been interacted with by a user) for a certain time are forced to release excess memory until they are no longer idle. When the application returns to an active state, the released memory is loaded back into the active working set.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Most environments should enable RAM optimization as a default configuration. A RAM optimization exclusion list is available if certain processes encounter issues with optimization.

The amount of storage that each VM requires will vary based on the workload and the image type. If creating hosted personal desktop without leveraging an image management solution, each VM will require enough storage for the entire OS and locally installed applications.

Deploying machines through Machine Creation Services or Provisioning Services can substantially reduce the storage requirements for each virtual machine. Disk space requirements for the write cache and difference disk will depend on application usage and user behavior. However, the following table provides a starting point for estimating disk space requirements based on machine sized with vCPU and vRAM as per the following guidelines:

User Workload	Operating System	Storage Space (Differencing Disk / Write Cache Disk)
Light	Windows 7	10 GB
	Windows 10	10 GB
	Windows 2012R2	40 GB
	Windows 2016	60 GB
Medium	Windows 7	15 GB
	Windows 10	15 GB
	Windows 2012R2	40 GB
	Windows 2016	60 GB
Heavy	Windows 7	20 GB
	Windows 10	20 GB
	Windows 2012R2	40 GB
	Windows 2016	60 GB

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Provisioning Services and Machine Creation Services have the capability to utilize a portion of the virtual machine's RAM as a buffer for the storage cache. The RAM cache is used to improve the performance of traditional storage by sharing the virtual machine's non-paged pool memory.

User Workload	Operating System	RAM Cache Configured for Scale	RAM Cache Configured for Experience
Light	Windows 7	128 MB	256 MB
	Windows 10	128 MB	256 MB
	Windows 2012R2	2GB	
	Windows 2016	4GB	
Medium	Windows 7	256 MB	512 MB
	Windows 10	256 MB	512 MB
	Windows 2012R2	4GB	
	Windows 2016	8GB	
Heavy	Windows 7	512 MB	1024 MB
	Windows 10	512 MB	1024 MB
	Windows 2012R2	6GB	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Windows 2016	10 GB

> **注意**
>
> - If used, the Machine Creation Services and Provisioning Services cache in RAM amount should be added onto the virtual machine RAM specifications.
> - If additional RAM is available on the host, the RAM Cache amounts can be increased to provide even greater levels of performance.

Storage performance is limited by the number of operations it can handle per second, referred to as IOPS. Under allocating storage IOPS results in a VDI desktop where apps, web pages and data are slow to load.

The following table provides guidance on the number of storage IOPS generated per user based on workload and operating system. Storage IO activity will be higher during user logon/logoff.

User Workload	Operating System	Storage IOPS (without RAM-Based Cache)	Storage IOPS (with RAM-Based Cache)
Light	Windows 7	10 IOPS	1 IOPS
	Windows 10	12 IOPS	1 IOPS
	Windows 2012R2	3 IOPS	0.5 IOPS
	Windows 2016	4 IOPS	1 IOPS
Medium	Windows 7	15 IOPS	1 IOPS
	Windows 10	20 IOPS	1.5 IOPS
	Windows 2012R2	4 IOPS	0.5 IOPS
	Windows 2016	6 IOPS	1 IOPS
Heavy	Windows 7	25 IOPS	2 IOPS

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Windows 10	35 IOPS	3 IOPS
	Windows 2012R2	5 IOPS	0.5 IOPS
	Windows 2016	8 IOPS	1 IOPS

With shared environments, every user's IO process receives an equal share of resources. A user running some IO intensive task can affect mission critical applications. Citrix Workspace Environment Management allows administrators to define IO priorities for processes.

If a process requires more IO resources or the process is monopolizing IO resources, the process and process priority is manually increased or decreased via the console. This advanced configuration is only used in special circumstances.

Without a graphical processing unit (GPU), graphical processing is rendered with software by the CPU. A graphical processing unit (GPU) can be leveraged to improve server scalability and user experience or enable the use of graphically intensive applications. During the desktop design it is important to decide how the GPU (if used) will be mapped to the virtual machines. There are three methods available.

- **Pass-Through GPU** – Each physical GPU is passed through to a single virtual machine (hosted apps or hosted desktops).
- **Hardware Virtualized GPU** – Using a hypervisor's vGPU technology, an NVIDIA GRID or Intel Iris Pro is virtualized and shared between multiple machines. Each virtual machine has the full functionality of GPU drivers and direct access to the GPU.
- **Software Virtualized GPU** – The GPU is managed by the hypervisor and intercepts requests made by the VDI desktops. This process is used if a GPU is not installed within the host.

In the table:

- **Y** indicates Available.
- **X** indicates Not Supported.

	Pass-Through GPU	Hardware Virtualized GPU (NVidia)	Hardware Virtualized GPU (Intel)	Hardware Virtualized GPU (AMD)	Software Emulated GPU
Citrix XenServer					
XenDesktop	Y	Y	Y	X	Y
XenApp	Y	Y	Y	X	Y
Microsoft Hyper-V					

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenDesktop	Y	X	X	X	Y
XenApp	Y	X	X	X	Y
VMware vSphere					
XenDesktop	Y	Y	X	Y	Y
XenApp	Y	Y	X	Y	Y

User groups with a heavy use of graphical applications will often require the use of a NVidia hardware virtualized GPU. User groups who rely on office-based applications can have an observable benefit with the use of a hardware virtualized GPU from Intel.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Design methodology control layer

Apr 23, 2018

The control layer is the fourth layer of the design methodology.

Multi-forest deployments, by default, do not have inter-domain trust relationships between the forests. An AD administrator can establish trust relationships between the multiple forests, allowing the users and computers from one forest to authenticate and access resources in another forest.

For forests that have inter-domain trusts, it is recommended that the appropriate settings be configured to allow the Delivery Controllers to communicate with both domains. When the appropriate trusts are not configured, multiple XenDesktop sites for each forest must be configured. This section outlines the storage requirements on a per product basis and provides sizing calculations. For more information, please refer to Citrix article: CTX134971 – Successfully Deploying XenDesktop in a Complex Active Directory Environment

Infrastructure components for a XenApp and XenDesktop deployment should reside within their own dedicated organizational units (OUs); separating workers and controllers for management purposes. By having their own OUs, the objects inside will have greater flexibility with their management while allowing Citrix administrators to be granted delegated control.

A sample Citrix OU structure can be seen below.



Whenever possible, permissions and authorization should be assigned to user groups rather than individual users, thereby eliminating the need to edit a large amount of resource permissions and user rights when creating, modifying, or deleting user accounts. Permission application example:

- An application published to one group of 1,000 users requires the validation of only one object for all 1,000 users.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- The same application published to 1,000 individual user accounts requires the validation of all 1,000 objects.

The majority of Citrix products discussed within this document require a database. The following table outlines the usage on a per product basis:

In this table:

- **Y** indicates Available.
- **O** indicates Optional.

Product	Configuration Data	Runtime Data	Audit/Change Log Data	Monitoring Data
XenDesktop	Y	Y	Y	Y
Provisioning Services	Y		O	
Desktop Player	Y	Y	Y	

There are multiple editions of Microsoft SQL Server 2012: Express, Web, Standard, Business Intelligence, and Enterprise. Based on the capabilities of the various SQL Server editions available, the Standard edition is often used for hosting the XenApp and XenDesktop databases in production environments.

The Standard edition provides an adequate amount of features to meet the needs of most environments. For more information on the databases supported with Citrix products please refer to the Citrix Database Support Matrix. Different versions of Citrix products support different versions of the SQL server; therefore, it is important to check the support matrix to ensure the version of SQL server used is compatible with the Citrix product being deployed.

The SQL Server must be sized correctly to ensure the performance and stability of an environment. Since every Citrix product uses SQL server in a different way, no generic all-encompassing sizing recommendations can be provided. Instead, per-product SQL server sizing recommendations are provided below.

XenApp and XenDesktop

XenApp and XenDesktop Brokers use the database as a message bus for broker communications, storing configuration data and storing monitoring and configuration log data. The databases are constantly in use and the performance impact on the SQL server can be considered as high.

Based on results from Citrix internal scalability testing the following SQL server specification for a server hosting all XenDesktop databases are recommended:

- 2 Cores / 4 GB RAM for environments up to 5,000 users
- 4 Cores / 8 GB RAM for environments up to 15,000 users

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 8 Cores / 16 GB RAM for environments with 15,000+ users

The database files and transaction logs should be hosted on separate hard disk subsystems in order to cope with a high number of transactions. For example, registering 20,000 virtual desktops during a 15-minute boot storm causes ~500 transactions / second and 20,000 users logging on during a 30-minute logon storm causes ~800 transactions / second on the XenDesktop Site Database.

Provisioning Services

In addition to static configuration data provisioning servers store runtime and auditing information in the database. Depending on the boot and management pattern, the performance impact of the database can be considered as low to medium.

Based on this categorization, a SQL server specification of 4 Cores and 4 GB RAM is recommended as a good starting point. The SQL server should be carefully monitored during the testing and pilot phase in order to determine the optimal configuration of the SQL server.

When sizing a SQL database, two aspects are important:

- **Database file** – Contains the data and objects such as tables, indexes, stored procedures and views stored in the database.
- **Transaction log file** – Contains a record of all transactions and database modifications made by each transaction. The transaction log is a critical component of the database and, if there is a system failure, the transaction log might be required to bring the database back to a consistent state. The usage of the transaction log varies depending on which database recovery model is used:
  - **Simple recovery** – No log backups required. Log space is automatically reclaimed, to keep space requirements small, essentially eliminating the need to manage the transaction log space. Changes to the database since the most recent backup are unprotected. In the event of a disaster, those changes must be redone.
  - **Full recovery** – Requires log backups. No work is lost due to a lost or damaged database data file. Data of any arbitrary point in time can be recovered (for example, prior to application or user error). Full recovery is required for database mirroring.
  - **Bulk-logged** – Requires log backups. This is an adjunct of the full recovery model that permits high-performance bulk copy operations. It is typically not used for Citrix databases.

For further information, please refer to the Microsoft Developer Network – SQL Server Recovery Models.

In order to estimate storage requirements, it is important to understand the disk space consumption for common database entries. This section outlines the storage requirements on a per product basis and provides sizing calculations. For more information, please refer to Citrix article: CTX139508 – XenDesktop 7.x Database Sizing.

XenDesktop General

XenApp 7.x and XenDesktop 7.x use three distinct databases:

- **Site Configuration database** – Contains static configuration and dynamic runtime data
- **Monitoring database** – Contains monitoring data which is accessible via Director
- **Configuration logging database** – Contains a record for each administrative change performed within the site (accessible via Studio)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Site Database

Since the database of a XenApp or XenDesktop site contains static configuration data and dynamic runtime data, the size of the database file depends not only on the physical size of the environment but also user patterns. The following factors all impact the size of the database file:

- The number of connected sessions
- The number of configured and registered VDAs
- The number of transactions occurring during logon
- VDA heartbeat transactions

The size of the Site Database is based on the number of VDAs and active sessions. The following table shows the typical maximum database size Citrix observed when scale testing XenApp and XenDesktop with a sample number of users, applications, and desktop delivery methods.

Users	Applications	Desktop Types	Expected Maximum Size (MB)
1,000	50	Hosted Shared	30
10,000	100	Hosted Shared	60
100,000	200	Hosted Shared	330
1,000	N/A	Hosted Pooled	30
10,000	N/A	Hosted Pooled	115
40,000	N/A	Hosted Pooled	390

> **注意**
>
> This sizing information is a guide only. Actual database sizes may differ slightly by deployment due to how databases are maintained.

Determining the size of the transaction log for the Site database is difficult due to factors that can influence the log including:

- The SQL Database recovery model
- Launch rate at peak times
- The number of desktops being delivered

© 1999-2017 Citrix Systems, Inc. All rights reserved.

During XenDesktop scalability testing, Citrix observed the transaction log growth rate at 3.5MB an hour when the system is idle, and a per user per day growth rate of ~32KB. In a large environment, transaction log usage requires careful management and a regular backup, to prevent excessive growth. This can be achieved by means of scheduled jobs or maintenance plans.

Monitoring Database

Of the three databases, the Monitoring database is expected to be the largest since it contains historical information for the site. Its size is dependent on many factors including:

- Number of Users
- Number of sessions and connections
- Number of workers
- Retention period configuration – Platinum customers can keep data for over a year (default 90 days). Non-platinum customers can keep data for up to 7 days (default 7 days).
- Number of transaction per second. Monitoring service tends to execute updates in batches. It is rare to have the number of transactions per second go above 20.
- Background transaction caused by regular consolidation calls from the Monitoring service.
- Overnight processing carried out to remove data outside the configured retention period.

The following table shows the estimated size of the Monitoring database over a period of time under different scenarios. This data is an estimate based on data seen within scale testing XenApp and XenDesktop (assuming a 5 day working week).

Users	Type	1 week (MB)	1 month (MB)	3 months (MB)	1 year (MB)
1,000	HSD	20	70	230	900
10,000	HSD	160	600	1,950	7,700
100,000	HSD	1,500	5,900	19,000	76,000
1,000	VDI	15	55	170	670
10,000	VDI	120	440	1,400	5,500
40,000	VDI	464	1,700	5,400	21,500
Estimates with 2 connections and 1 session per user with a 5 day work week					
Users	**Type**	**1 week (MB)**	**1 month (MB)**	**3 months (MB)**	**1 year (MB)**
1,000	HSD	30	100	330	1,300

© 1999-2017 Citrix Systems, Inc. All rights reserved.

10,000	HSD	240	925	3,000	12,000
100,000	HSD	2,400	9,200	30,000	119,000
1,000	VDI	25	85	280	1,100
10,000	VDI	200	750	2,500	9,800
40,000	VDI	800	3,000	9,700	38,600

> **注意**
>
> The 100,000 HSD tests are based on a test environment consisting of:
>
> - 2 Delivery Controllers
> - 43 Hosted Shared Desktop workers
> - 3 SQL servers, configured with databases held within one Always On Availability Group.
>
> For more information please see the Citrix Support article – XenDesktop 7.x Database Sizing.

The size of the transaction log for the Monitoring Database is very hard to estimate, but XenApp and XenDesktop scalability testing showed a growth rate of about 30.5 MB an hour when the system is idle, and a per user per day growth rate of ~9 KB.

Configuration Logging Database

The Configuration Logging Database is typically the smallest of the three databases. Its size and the size of the related transaction log depends on the daily administrative activities initiated from Studio, Director or PowerShell scripts, therefore its size is difficult to estimate. The more configuration changes are performed, the larger the database will grow. Some factors that can affect the size of the database include:

- The number of actions performed in Studio, Director and PowerShell.
- Minimal transactions which occur on the database when no configuration changes are taking place.
- The transaction rate during updates. Updates are batched whenever possible.
- Data manually removed from the database. Data within the Configuration Logging Database is not subject to any retention policy, therefore it is not removed unless done so manually by an administrator.
- Activities that have an impact on sessions or users, for example, session logoff and reset.
- The mechanism used for deploying desktops.

In XenApp environments not using MCS, the database size tends to fall between 30 and 40MB. For MCS environments, database size can easily exceed 200MB due to the logging of all VM build data.

Temporary Database

In addition to the Site, Monitoring, and Configuration Logging databases, a system-wide temporary database (tempdb) is

© 1999-2017 Citrix Systems, Inc. All rights reserved.

provided by SQL Server. This temporary database is used to store Read-Committed Snapshot Isolation data. XenApp 7.x and XenDesktop 7.x uses this SQL Server feature to reduce lock contention on the XenApp and XenDesktop databases. Citrix recommends that all XenApp 7.x and XenDesktop 7.x databases use Read-Committed Snapshot Isolation. For more information please see How to Enable Read-Committed Snapshot in XenDesktop.

The size of the tempdb database will depend on the number of active transactions, but in general it is not expected to grow more than a few MBs. The performance of the tempdb database does not impact the performance of XenApp and XenDesktop brokering, as any transactions that generate new data require tempdb space. XenApp and XenDesktop tend to have short-lived transactions, which help keep the size of the tempdb small.

The tempdb is also used when queries generate large intermediate result sets. Guidance and sizing the tempdb can be found on the Microsoft TechNet article Optimizing tempdb Performance.

Provisioning Services

The Provisioning Services farm database contains static configuration and configuration logging (audit trail) data. The record size requirements outlined below can be used to help size the database:

Configuration Item	DB Space Required (KB)	Number of Items (Example)	Total (KB)
Base farm configuration	112	-	112
User group w/ farm access	50	10	250
Site	4	5	20
Device collection	10	50	500
Farm view	4	10	40
Farm view to device relationship	5	1	5,000
Site View	4	5	20
Site view to device relationship	5	1	5,000
Device	2	5,000	10,000

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Device bootstrap	10	-	-
Device to disk relationship	35	1	175,000
Device printer relationship	1	-	-
Device personality data	1	-	-
Device status (when booted)	1	5,000	5,000
Device custom property	2	-	-
vDisk	1	20	20
vDisk version	3	5	300
Disk locator	10	1	200
Disk locator custom property	2	-	-
Server	5	10	50
Server IP	2	1	20
Server status (when booted)	1	20	20
Server custom property	2	-	-
vDisk store	8	5	40

© 1999-2017 Citrix Systems, Inc. All rights reserved.

vDisk store to server relationship	4	1	40
Connection to XenServer (VirtualHostingPool)	4	-	-
vDisk update task	10	10	100
Administrative change (auditing enabled)	1	10,000	10,000
Total			**211,732KB (~212MB)**

During the PVS farm setup, a database with an initial file size of 20MB is created. Due to the nature of the data in the PVS farm database the transaction log is not expected to grow very quickly, unless a large amount of configuration is performed.

In contrast to XenApp, which also offers the ability to track administrative changes, the related information is not written to a dedicated database but directly to the Provisioning Services farm database. In order to limit the size of the Provisioning Services database it is recommended to archive the audit trail data on a regular schedule.

By default, the Configuration Logging and Monitoring databases are located within the Site Configuration database. Citrix recommends changing the location of these secondary databases as soon as the configuration of the site has been completed, in order to simplify sizing, maintenance and monitoring. All three databases can be hosted on the same server or on different servers. An ideal configuration would be to host the Monitoring database on a different server from the Site Configuration and Configuration Logging databases since it records more data, changes occur more frequently and the data is not considered to be as critical as the other databases. For more information, please refer to Citrix Docs – Change secondary database locations.

> **注意**
>
> The location of the Configuration Logging database cannot be changed when mandatory logging is enabled.

The following table highlights the impact to XenApp, XenDesktop and Provisioning Services when there is a database outage:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	Impact of Database Outage
Site configuration database	Users will be unable to connect or reconnect to a virtual desktop. **Note**: Local Host Cache allows users with Hosted Shared Desktops, Hosted Windows and Browser Applications, and Personal Desktops to reconnect to their applications and desktops even when the site database is unavailable.
Monitoring database	Director will not display any historical data and Studio cannot be started. Brokering of incoming user requests and existing user sessions will not be affected.
Configuration logging database	If allow changes when the database is disconnected has been enabled within XenApp and XenDesktop logging preferences, an outage of the configuration logging database will have no impact (other than configuration changes not being logged). Otherwise, administrators will be unable to make any changes to the XenApp and XenDesktop site configuration. Users are not impacted.
Provisioning Services farm database	When offline database support is enabled and the database becomes unavailable, the stream process uses a local copy of the database to retrieve information about the provisioning server and the target devices supported by the server. This allows provisioning servers and the target devices to remain operational. However, when the database is offline, the console and the management functions listed below become unavailable: • Auto Add target devices • vDisk creation and updates • Active Directory password changes • Stream process startup • Image update service • PowerShell and MCLI based management If offline database support has not been enabled, all management functions become unavailable and the boot and failover of target devices will fail.

> **注意**
>
> Please review HA options for 3rd party databases (for example, App-V, SCVMM or vCenter) with the respective software vendor.

In addition to the built-in database redundancy options, Microsoft SQL Server, as well as the underlying hypervisor (in virtual environments), offer a number of high availability features. These enable administrators to ensure single server outages will have a minimal impact (if any) on the XenApp and XenDesktop infrastructure. The following the SQL / hypervisor high availability features are available:

- **VM-level HA** – This high availability option is available for virtual SQL servers only, which need to be marked for High Availability at the hypervisor layer. In case of an unexpected shutdown of the virtual machine or the underlying hypervisor host, the hypervisor will try to restart the VM immediately on a different host. While VM-level HA can minimize downtimes in power-outage scenarios, it cannot protect from operating system level corruption. This solution is less expensive than mirroring or clustering because it uses a built-in hypervisor feature. However, the automatic failover process is slower, as it can take time detect an outage and start the virtual SQL server on another host. This may interrupt the service to users.
- **Mirroring** – Database mirroring increases database availability with almost instantaneous failover. Database mirroring can be used to maintain a single standby or mirror database, for a corresponding principal or production database.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Database mirroring runs with either synchronous operation in high-safety mode, or asynchronous operation in high-performance mode. In high-safety mode with automatic failover (recommended for XenDesktop) a third server instance, known as a witness, is required, which enables the mirror server to act as a hot standby server. Failover from the principal database to the mirror database happens automatically and is typically completed within a few seconds. It is a good practice to enable VM-level HA (or a similar automatic restart functionality) for at least the witness to ensure SQL service availability in case of a multi-server outage.

> **注意**
>
> Microsoft is planning to remove mirroring as a high availability option in a future release of SQL Server and is discouraging its use in new network development. Please refer to the Microsoft article – Database Mirroring (SQL Server) for more information

- **AlwaysOn Failover Cluster Instances** – Failover clustering provides high-availability support for an entire instance of Microsoft SQL Server. A failover cluster is a combination of two or more nodes, or servers, using a shared storage. A Microsoft SQL Server AlwaysOn Failover Cluster Instance, introduced in SQL Server 2012, appears on the network as a single computer, but has functionality that provides failover from one node to another if the current node becomes unavailable. The transition from one node to the other node is seamless for the clients connected to the cluster. AlwaysOn Failover cluster Instances require a Windows Server Failover Clustering (WSFC) resource group. The number of nodes supported in the WSFC resource group will depend on the SQL Server edition. (Please refer to the table in the Decision: Edition earlier in this chapter.) For more information please refer to MSDN – AlwaysOn Failover Cluster Instances (SQL Server).
- **AlwaysOn Availability Groups** – AlwaysOn Availability Groups is an enterprise-level highavailability and disaster recovery solution introduced in Microsoft SQL Server 2012, which enables administrators to maximize availability for one or more user databases. AlwaysOn Availability Groups require that the Microsoft SQL Server instances reside on Windows Server failover clustering (WSFC) nodes. Similar to failover clustering a single virtual IP / network name is exposed to the database users. In contrast to failover clustering, shared storage is not required since the data is transferred using a network connection. Both synchronous and asynchronous replication to one or more secondary servers is supported. As opposed to mirroring or clustering secondary servers can be actively used for processing incoming read-only requests, backups or integrity checks. This feature can be used to offload user resource enumeration requests to a secondary SQL server in XenDesktop environments to essentially scale-out a SQL server infrastructure. Since the data on active secondary servers can lag multiple seconds behind the primary server, the read-only routing feature cannot be used for other XenDesktop database requests at this point in time. For more information, please refer to MSDN – AlwaysOn Availability Groups (SQL Server).

The following table outlines the recommended high availability features for Citrix databases:

In the table:

- **Y** indicates Recommended.
- **o** indicates Viable.
- **N** indicated Not Supported.
- **T** indicates for test environments only.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	VM Level - HA	Mirroring	AlwaysOn Failover Cluster Instances	AlwaysOn Availability Groups
Site database	T	Y	o	o
Configuration logging database	T	o	o	o
Monitoring database	T	Y	o	o
Provisioning Services farm database	T	Y	o	N
DesktopPlayer database	T	N	o	o

Citrix offers organizations the flexibility of multiple licensing models that align with common usage scenarios. The different licensing models vary based on the Citrix product used, but can include per user/device and per concurrent user. Several Citrix products use the license server, while other products require a license to be installed on the product itself.

Citrix License Server

- XenDesktop
- XenApp
- Provisioning Services
- XenServer

On the product:

- NetScaler
- NetScaler Gateway

For more information on XenDesktop 7.x licensing, please refer to CTX128013 - XenDesktop Licensing.

For more information on Microsoft Licensing, please refer to the Microsoft document – Licensing Microsoft's Virtual Desktop Infrastructure Technology.

Internal scalability testing has shown that a single virtual license server with two cores and 2GB of RAM can issue approximately 170 licenses per second or 306,000 licenses per half hour. If necessary, the specification of the license server can be scaled out to support a higher number of license requests per second.

For a typical environment, a single license server is sufficient. Should the license server become unavailable, dependent Citrix products will enter a 30-day grace period, which provides more than enough time to resolve connectivity issues and/or

© 1999-2017 Citrix Systems, Inc. All rights reserved.

restore or rebuild the license server.

> **注意**
>
> - If the license server and the Citrix product do not communicate within 2 heartbeats (5-10 min), the Citrix product will enter a grace period and will allow connections for up to 30 days. Once communication with the license server is re-established, the license server will reconcile the temporary and actual licenses.
> - A CNAME record in DNS is a convenient way to reference the license server. Using CNAMEs allows the license server name to be changed without updating the Citrix products.

If additional redundancy is required, Citrix supports the following high availability solutions for the license server.

- **Windows Clustering** – Cluster servers are groups of computers that work together in order to increase availability. Clustering allows the license server role to automatically failover in the event of a failure. For more information on clustering, please see the Citrix Docs article – Clustered License Servers.
- **Duplication of license server** – Create a VM level backup of the license server. This backup should not be stored on the same host as the license server. Instead, it should be stored in a safe location, such as a highly available storage solution, or backed up to tape or disk. The duplicate server is not active, and will remain on standby until the need arises to restore the active license server. Should the license server be restored using this backup, any new licenses must be re-downloaded to the server.

For more information, please refer to Citrix eDocs – Licensing Architecture Overview.

Each method allows an administrator to exchange a single license server for another without an interruption in service; assuming that the change occurs during the grace period and that the following limitations are considered.

- License files will reference the server specified during the allocation process. This means that the license files can only be used on a server with the same binding information (Hostname) as the server that was previously specified.
- Two Windows-based, domain joined license servers cannot share the same name and be active in the environment at the same time.
- Because license servers do not communicate with each other, any additional licenses must be placed on both the active and backup license server.

License server performance can be optimized by tuning the number of “receive” and “processing” threads. If the thread count is set too low, requests will be queued until a thread becomes available. Conversely, if the thread count is set too high, the license server will become overloaded.

The optimal values are dependent on the server hardware, site configuration, and license request volume. Citrix recommends testing and evaluating different values to determine the proper configuration. Setting the maximum number of processing threads to 30 and the maximum number of receiving threads to 15 is a good starting point for large scale deployments.

This optimization will improve the Citrix License Server ‘s ability to provide licenses by increasing its ability to receive and process license requests.

For more information, please refer to the Citrix Docs – Improving Performance by Specifying Thread Use.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Delivery Controller scalability is based on CPU utilization. The more processor cores available, the more virtual desktops a controller can support. Each desktop startup, registration, enumeration and launch request impacts the controller's processor. As the storm increases in intensity, the CPU utilization of the controller will increase. If the CPU reaches a critical threshold, roughly 80%, the site will need to either scale up or scale out.

Adding additional CPU cores to a Delivery Controller will lower the overall CPU utilization, thus allowing for greater numbers of desktops supported by a single controller. This is really only feasible when dealing with virtualized controllers as adding virtual CPUs is fairly easy and straightforward. The other alternative is to add another controller into the site configuration. The controller would have the same configuration as other controllers, and the load would be evenly distributed across all controllers, thus helping to reduce the overall load on each single controller.

Testing has shown that a single Delivery Controller, using the following configuration, can support more than 5,000 desktops.

Component	Specification
Processor	4 vCPU
Memory	4 GB RAM
Network	Bonded virtual NIC
Host Storage	40-GB shared storage
Operating System	Windows Server 2012 R2
XenDesktop	7

The following formula can be used to calculate the number of Delivery Controllers required for a Citrix site.

$$Number\ of\ Delivery\ Controllers = \frac{Number\ of\ Active\ Sessions\ per\ Site}{5{,}000} + 1$$

If the server hosting the Delivery Controller is unavailable, users will not be able to access their virtual desktops or published applications. Therefore at least two Delivery Controllers (N+1 redundancy) should be deployed per zone on different physical servers to prevent this component from becoming a single point of failure. If one controller fails, the others can manage connections and administer the site.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

The locations of all Delivery Controllers are specified on the VDA, allowing it to automatically failover if communication with one Delivery Controller is unavailable. The VDA checks the following locations, in order, stopping at the first place it finds the Delivery Controller:

1. A persistent storage location maintained for the auto-update feature. This location contains controller information when auto-update is enabled and after the VDA successfully registers for the first time after installation.
   For its initial registration after installation, or when auto-update is disabled, the VDA checks the following locations.
2. Policy settings (Delivery Controllers, Delivery Controller SIDs).
3. The Delivery Controller information under the VDA ListofDDCs registry key. The VDA installer initially populates these values, based on the information specified when installing the VDA.
4. OU-based discovery. This is a legacy method maintained for backward compatibility.
5. The Personality.ini file created by Machine Creation Services.

Citrix Consulting recommends utilizing the auto-update feature (enabled by default). This feature will simplify management of the environment by keeping VDA's updated when adding and removing Delivery Controllers.

Even if the SQL database is highly available, there is the risk of not having access to the database if the network connection between the delivery controller and SQL database fails, which is an important concern for sites that span geographical locations.

To overcome this risk, the delivery controllers can utilize the local host cache feature that creates a local copy of the SQL database, used only if the delivery controller loses contact with the database.

The following must be considered when using local host cache:

- **Elections** – When the zones loses contact with the SQL database, an election occurs nominating a single delivery controller as master. All remaining controllers go into idle mode. A simple alphabetical order determines the winner of the election.
- **Sizing** – When using local host cache mode, a single delivery controller is responsible for all VDA registrations, enumerations, launches and updates. The elected controller must have enough resources (CPU and RAM) to handle the entire load for the zone. A single controller can scale to 10,000 users, which influences the zone design.
  - **RAM** – The local host cache services can consume 2+GB of RAM depending on the duration of the outage and the number of user launches during the outage.
  - **CPU** – The local host cache can use up to 4 cores in a single socket.
  - **Storage** – During local host cache mode, storage space increased 1MB every 2-3 minutes with an average of 10 logons per second.
- **Power Options** – Powered off virtual resources will not start when the delivery controller is in local host cache mode. Pooled virtual desktops that reboot at the end of a session are placed into maintenance mode.
- **Consoles** – When using local host cache mode, Studio and PowerShell are not available.

In a typical session, the StoreFront server passes credentials to the Citrix XML Service on a Delivery Controller. The Citrix XML protocol uses clear text to exchange all data, with the exception of passwords, which are transmitted using obfuscation.

If the traffic between the Storefront servers and the XenDesktop Controllers can be intercepted it will be vulnerable to the following attacks:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Attackers can intercept the XML traffic and steal resource set information and tickets.
- Attackers with the ability to crack the obfuscation can obtain user credentials.
- Attackers can impersonate the XenDesktop Controller and intercept authentication requests.

For most organizations, the Citrix XML traffic will be isolated on a dedicated physical or virtual datacenter network making interception unlikely. However, for safety consider using SSL encryption to send StoreFront data over a secure HTTP connection.

Default Load Management policies are applied to all Server OS delivery groups. The default settings specify the maximum number of sessions a server can host at 250 and do not consider CPU and Memory usage. Capping session count does not provide a true indication of load, which can lead to an overburdening of Server OS delivery groups resulting in a degradation of performance or an underutilization of Server OS delivery groups resulting in an inefficient usage of resources.

Citrix Consulting recommends creating unique "custom" Load Management policies for each Delivery Group based on performance and scalability testing. Different rules and thresholds can be applied to each Delivery Group depending on the different resource bottlenecks identified during testing. For more information on the available Load Management policy configurations refer to Citrix Docs – Load Management policy settings.

If adequate testing cannot be performed prior to production, Citrix Consulting recommends implementing the following "custom" Load Management policy which can be applied to all servers as a baseline:

- **CPU Usage** - Full Load: 80%
- **CPU usage excluded process priority** – Below Normal or Low
- **Memory Usage** - Full Load: 80%
- **Memory Usage base load** – Report zero load (MBs): 786
- **Maximum number of sessions** – X

The "Maximum number of sessions" policy is included for capping purposes – this is considered a best practice for resiliency. Organizations can choose an initial value of 250 (denoted by "X" above). **It is highly recommended that this value and others be customized based on the results from scalability testing**.

The XenApp and XenDesktop Service within Citrix Cloud utilize a set of services contained within the Citrix Cloud Connector. A redundant set of Cloud Connector virtual machines must be placed in each data center/resource location containing VDA hosts.

Cloud Connector scalability is based on CPU utilization. The more processor cores available, the more virtual desktops a cloud connector can support. Each desktop startup, registration, enumeration and launch request affects the cloud connector's processor. As the storm increases in intensity, the CPU utilization of the cloud connector will increase. If the CPU reaches a critical threshold, roughly 80%, the site will need to either scale up or scale out.

Testing has shown that a single Cloud Connector Controller, using the following configuration, can support 5,000 desktops.

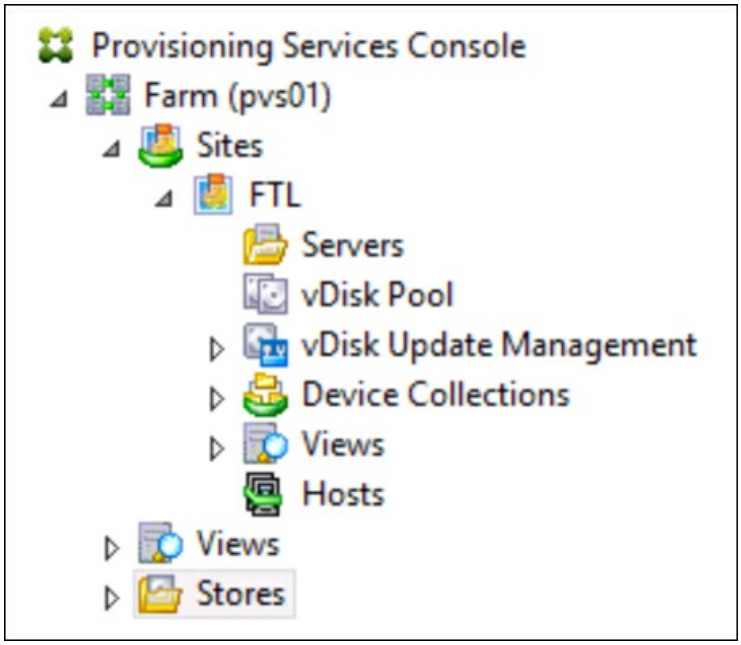
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	On Premises Specifications	Azure Hosted Specifications
Number of VMs (with N+1 Fault Tolerance)	3	6 Standard_A2_V2 instances
Processors per VM	4 vCPU	2 vCPU
Memory per VM	4 GB RAM	4 GB RAM
Host Storage per VM	40 GB shared storage	200 GB temp storage
Operating System	Windows Server 2012 R2	Windows Server 2012 R2

Citrix Provisioning Services (PVS) uses streaming technology to simplify the deployment of virtual and physical machines. Computers are provisioned and re-provisioned in real-time from a single shared-disk image. In doing so, administrators can completely eliminate the need to manage and patch individual systems. Instead, all image management is performed on the master image.

A Provisioning Services farm represents the top level of the Provisioning Services infrastructure, which can be further broken down into sites. All provisioning servers in a farm share the same SQL database and Citrix license server.

Each site is a logical entity containing provisioning servers, vDisk pools and target device collections. Although all sites within a farm share the same database, target devices can only fail over to other provisioning servers within the same site.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

There are factors that must be considered when determining the overall Provisioning Services topology:

- **Network** – Provisioning servers are constantly communicating with the farm database to retrieve system configuration settings. Therefore, separate farms should be created for each physical location where target devices reside, unless they are connected to the database server by a fast and robust connection.
- **Administration** – Organizations may need to maintain the separation of administrative duties at a departmental, regional or countrywide basis. Additional Provisioning Services farms will add some complexity to the management of the environment. However, this overhead is typically limited to initial configuration, desktop creation and image updates.
- **Organization** – A practical reason for building multiple sites is due to organizational changes. For example, two companies may have recently merged through acquisition, but need to keep resources separate while integration takes place. Configuring the organization to use separate sites is one way to keep the businesses separate but managed centrally through the Provisioning Services console.

Only create additional sites if the business requirements warrant it. A single site per farm is easier to manage and requires no additional configuration.

Device collections provide the ability to create and manage logical groups of target devices. Creating device collections simplifies device management by allowing actions to be performed at the collection level rather than the target device level.



Device collections can represent physical locations, subnet ranges, chassis or different departments within an organization. Collections can also be used to logically separate production target devices from test and maintenance ones.

Consider creating device collections based on vDisk assignment so that the status of all target devices assigned to a particular vDisk can be quickly identified.

Provisioning Services is a critical component of the virtual desktop infrastructure. The following recommendations should be followed to eliminate single points of failure:

- **Provisioning Server** – A minimum of two provisioning servers should always be implemented per site. Sufficient redundancy should be incorporated into the design so that a single server failure does not reduce the total number of target devices that can be supported per site. The Provisioning Services boot file should be configured for high availability. Up to four Provisioning Servers may be listed in the boot file. Target devices will try to contact the servers in the order that they are listed. The server that responds may not necessarily be the server that will provide streaming services to the target device. If Load Balancing is enabled, the target device may be reassigned to another server in the site that is less loaded than the others.
- **vDisks and Storage** – For vDisk stores hosted on local, Direct Attached Storage (DAS) or Storage Area Network (SAN),

© 1999-2017 Citrix Systems, Inc. All rights reserved.

replication should be used to synchronize the vDisks. If using Network Attached Storage (NAS), ensure that the vDisks are hosted on a highly available network share.

- **Networking** – The provisioning servers should have redundant NICs. If the provisioning server is deployed as a physical server, redundant NICs should be teamed and if the provisioning server is deployed as a virtual server, the underlying hypervisor should incorporate redundant NICs.

> **注意**
>
> The target devices will only failover to NICs that are on the same subnet as the PXE boot NIC.

Trivial File Transfer Protocol (TFTP) is a communications protocol used for transferring configuration or boot files between machines. Provisioning services can use TFTP to deliver the bootstrap file to target devices. There are several options available to make the TFTP service highly available. Some of the more commonly used options are:

- **DNS Round Robin** – A DNS entry is created for the TFTP service with multiple A records corresponding to the TFTP services running on the provisioning servers in the farm. This method is not recommended since the state of the TFTP service is not monitored. Clients could potentially be sent to a non-functioning server.
- **Hardware load balancer** – Use a hardware load balancer, such as Citrix NetScaler, to create virtual IPs that corresponds to the provisioning servers. The NetScaler can intelligently route traffic between the provisioning servers. In the event that one of the servers becomes unavailable, NetScaler will automatically stop routing TFTP requests to that server. This is the best method for making TFTP highly available, but can be complicated to setup.
- **Multiple DHCP Option 66 entries** – This method is easy to implement but requires a DHCP service that supports entering multiple entries in option 66. Microsoft DHCP server allows one option 66 entry so this method would not be feasible in environments with Microsoft DHCP services. If using a non-Microsoft DHCP server or appliance, check with the manufacturer to verify that multiple option 66 entries is supported.

There are other options available that can achieve the same result without having to use TFTP:

- **Proxy DHCP** – Use the provisioning servers PXE service to provide the bootstrap information. If one of the servers is down, the next available server in the farm can provide the bootstrap information. This method requires the provisioning servers to be on the same broadcast domain as the target devices. If there are other PXE services running on the network (Altiris, SCCM, etc.) then multiple VLANs may be required to keep the PXE services from interfering with each other.
- **Boot Device Manager** – Use the Boot Device Manager to create a bootstrap file that is either placed on the local hard drive, or used as a bootable ISO file. If the ISO file is used, configure the target devices to boot from the CD/DVD-ROM drive, and place the ISO file on a highly available shared network location or local storage of each target device. When either method is utilized, the TFTP service is not used at all.

High availability should always be incorporated into the Provisioning Services design. Although high availability may require additional resources and increased costs, it will provide a highly stable environment so that users experience minimal impact due to service outages.

A target device initiates the boot process by first loading a bootstrap program which initializes the streaming session between the target device and the provisioning server. There are three methods in which the target device can receive the

© 1999-2017 Citrix Systems, Inc. All rights reserved.

bootstrap program:

Using DHCP Options –

1. When the target device boots, the target device sends a broadcast for IP address and boot information. DHCP will process this request and provide an IP as well as scope option settings 66 (the name or IP address of the Provisioning Services TFTP server) and 67 (the name of the bootstrap file).

> **注意**
>
> If using a load balancer for the TFTP service then the address of the load balancer is entered in option 66.

2. Using TFTP, a request for the bootstrap file is sent from the target device to the provisioning server. The target device downloads the boot file from the provisioning server.

3. The target device boots the assigned vDisk image.

> **注意**
>
> Requires UDP/DHCP Helper to be configured when targets are not on the same subnet as the DHCP servers in order to receive PXE broadcasts.

Using PXE Broadcasts –

1. When a target device boots from the network, the target device sends a broadcast for an IP address and boot information. DHCP will process this request and provide an IP address. In addition, all provisioning servers that receive the broadcast will return boot server and boot file name information. The target device will merge the information received and start the boot process.

2. Using TFTP, a request for the bootstrap file is sent from the target device to the provisioning server which responded first. The target device downloads the boot file from the provisioning server.

> **注意**
>
> - Make sure no other PXE services are in use on the same subnet, such as the Altiris PXE service, or isolate using VLANs otherwise conflicts may occur with Provisioning Services.
> - Requires UDP/DHCP Helper to be configured when targets are not on the same subnet as the DHCP and PVS servers in order to receive PXE broadcasts.

Using Boot Device Manager – The Boot Device Manager (BDM) creates a boot file that target devices obtain through a physical CD/DVD, a mounted ISO image or as a virtual hard disk assigned to the target device. A BDM partition can be upgraded in one of three ways:

- By collection

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- By a group of highlighted devices
- By a single device

A summary of the advantages and disadvantages for each delivery method is listed in the following table:

Delivery Method	Advantages	Disadvantages
DHCP Options	Easy to implement	Requires changes to production DHCP service. DHCP service may only allow one option 66 entry. Requires UDP/DHCP helper for targets on different subnets.
PXE	Easy to implement	Can interfere with other running PXE services on the same subnet. Requires UDP/DHCP helper for targets on different subnets.
BDM ISO	Does not require PXE or TFTP services	Extra effort required to boot physical target devices. BDM ISO is regarded as a single point of failure if a single file is used.
BDM Partition	The BDM boot partition upgrade does not require PXE, TFTP, or TSB; it's considered a single stage bootloader, at boot time it automatically finds all relevant PVS server information and does not need external services provided by PXE, TFTP, or TSB.	An extra 8MB partition is created for each target device.

> **注意**
>
> When configuring the bootstrap file, up to four provisioning servers may be listed. The order in which the provisioning servers appear in the list determines the order which the provisioning servers are accessed. If the first server does not respond, the next server in the list is contacted.

Provisioning Services supports the use of fixed-size or dynamic vDisks:

- **Fixed-size disk** – For vDisks in private mode, fixed-size prevents disk fragmentation, and offers improved write

© 1999-2017 Citrix Systems, Inc. All rights reserved.

performance over dynamic disks.

- **Dynamic disk** – Dynamic disks require less storage space than fixed-size disks, but offer significantly lower write performance. Although vDisks in Shared mode do not perform writes to the vDisk, the time required to complete vDisk merge operations will increase with dynamic disks. This is not a common occurrence as more environments choose to create new vDisks when updating.

Since most reads will be to the System Cache in RAM, there is no significant change in performance when utilizing fixed-size or dynamic disks. In addition, dynamic disks require significantly less storage space. Therefore, dynamic disks are recommended.

vDisks hosted on a local, Direct Attached Storage or a SAN must be replicated between vDisk stores whenever a vDisk is created or changed. Provisioning Services supports the replication of vDisks from stores that are local to the provisioning server as well as replication across multiple sites that use shared storage. The replication of vDisks can be performed manually or automatically:

- **Manual** – Manual replication is simple, but can be time consuming, depending on the number of vDisks and vDisk stores. If an error occurs during the replication process, administrators can catch them straight away and take the appropriate steps to resolve them. The risk of manual replication is vDisk inconsistency across the provisioning servers which will result in load balancing and failover to not work properly. For example, if a vDisk is replicated across three servers and then one of the vDisks is updated, that vDisk is no longer identical and will not be considered if a server failover occurs. Even if the same update is made to the other two vDisks, the timestamps on each will differ, and therefore the vDisks are no longer identical.
- **Automated** – For large environments, automated replication is faster than the manual method due to the number of vDisks and vDisk Stores required. Some automated tools, such as Microsoft DFS-R, support bandwidth throttling and Cross File Remote Differential Compression (CF-RDC), which use heuristics to determine whether destination files are similar to the file being replicated. If so, CF-RDC will use blocks from these files to minimize the amount of data transferred over the network. The risk of automated replication is that administrator do not typically monitor replication events in real-time and do not respond quickly when errors occur, unless the automation tool has an alerting feature. Some tools can be configured to automatically restart the copy process in the event of a failure. For example, Robocopy supports “resume copying” in the event that the network connection is interrupted.

For medium and large projects, use a tool to automate vDisk replication. Select a tool that is capable of resuming from network interruptions, copying file attributes and preserving the original timestamp.

> **注意**
>
> Load balancing and high availability will not work unless the vDisks have identical timestamps.

Generally, a Provisioning Server is defined with the following specifications:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	Specification
Model	Virtual
Processor	4 - 8 vCPU
Memory	2GB + (# of vDisks * 2GB)
Network	10 GBps NIC
Network	40 GB shared storage
vDisk Storage	Depending on number of images/revisions
Operating System	Windows Server 2012 R2

Citrix Provisioning Services can be installed on virtual or physical servers:

- **Virtual** – Offers rapid server provisioning, snapshots for quick recovery or rollback scenarios and the ability to adjust server resources on the fly. Virtual provisioning servers allow target devices to be distributed across more servers helping to reduce the impact from server failure. Virtualization makes more efficient use of system resources.
- **Physical** – Offers higher levels of scalability per server than virtual servers. Physical provisioning servers mitigate the risks associated with virtual machines competing for underlying hypervisor resources.

  In general, virtual provisioning servers are preferred when sufficient processor, memory, disk and networking resources can be made available and guaranteed to be available.

> **注意**
>
> For high availability, ensure that virtual Provisioning Servers are distributed across multiple virtualization hosts. Distributing the virtual servers across multiple hosts will eliminate a single point of failure and not bring down the entire Provisioning Services farm in the event of a host failure.

Provisioning Services is not CPU intensive. However, under allocating the number of CPUs does impact the optimization of the network streams. The number of streams that a Provisioning Services server can run concurrently can be determined by the following formula:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

□□□ □□□□□□ □□ □□□□□□□ = # □□ □□□□□ ∗ # □□ □h□□□□□/□□□□

By default, the Streaming Service is configured with 20 sequential network ports, and 8 threads per port. Therefore, by default, a provisioning server can support 160 concurrent targets. If more than 160 streams are required, Provisioning Services continuously switches between streaming different target devices

Ideally, if the environment needs to support more than 160 concurrent targets, the number of ports, and threads per port can be adjusted in the Provisioning Services console. Best performance is attained when the threads per port is not greater than the number of cores available on the provisioning server. If the provisioning server does not have sufficient cores, the server will show a higher CPU utilization, and target devices waiting for requests to be processed will have a higher read latency.

Even though Provisioning Services is not CPU intensive, allocating 2 CPUs will require a larger contiguous network port range.

- Small environments (up to approximately 500 virtual machines) 4 vCPUs are recommended.
- Larger environments 8 vCPUs are recommended.

RAM

The Windows operating system hosting Provisioning Services partially caches the vDisks in memory (system cache) reducing the number of reads required from storage. Reading from storage is significantly slower than reading from memory. Therefore, Provisioning Servers should be allocated sufficient memory to maximize the benefit from this caching process.

The following formula can be used to determine the optimal amount of memory that should be allocated to a provisioning server:

□□□□□ □□□□□□ □□□ = 2□□ + (# □□ □□□□□□ ∗ 2□□)

Network

Unlike most other XenApp and XenDesktop components, Provisioning Services does not bottleneck the CPU. Provisioning Services scalability is based on network throughput.

The following table shows the approximate amount of data that Provisioning Services requires to boot different operating systems:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Operating system	Avg Boot Data Usage (MB)
Windows 10 x64	240
Windows 8 x86	178
Windows 8 x64	227
Windows 7 x86	166
Windows 7 x64	210
Windows 2012	225
Windows 2012 R2	232
Windows 2008 R2	251
Windows Vista x86	190
Windows Vista x64	240

Determining how much time will be required to boot the target devices can be estimated using the following formula:

$$Seconds\ to\ Boot = \frac{(Number\ of\ Targets\ *\ MB\ Usage)}{\text{Network Throughput}}$$

Operating System	Number of VMs	Network Throughtput	Time to boot
Windows 10 x64	500	1 GBps	960 Seconds (16 minutes)
Windows 10 x64	500	10 GBps	96 Seconds (1 minute, 36 seconds)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

A 10Gbps network is recommended for use with Provisioning Services. If a 10Gbps network is not available, consider link aggregation to provide additional bandwidth to the provisioning servers, or a dedicated physical streaming network.

> **提示**
>
> Firewalls can add latency and create bandwidth bottlenecks in Provisioning Services environments. If the use of firewalls cannot be avoided, refer to the Citrix whitepaper CTX101810 – Communication Ports Used By Citrix Technologies, for the list of ports that should be enabled for full functionality.

Growth

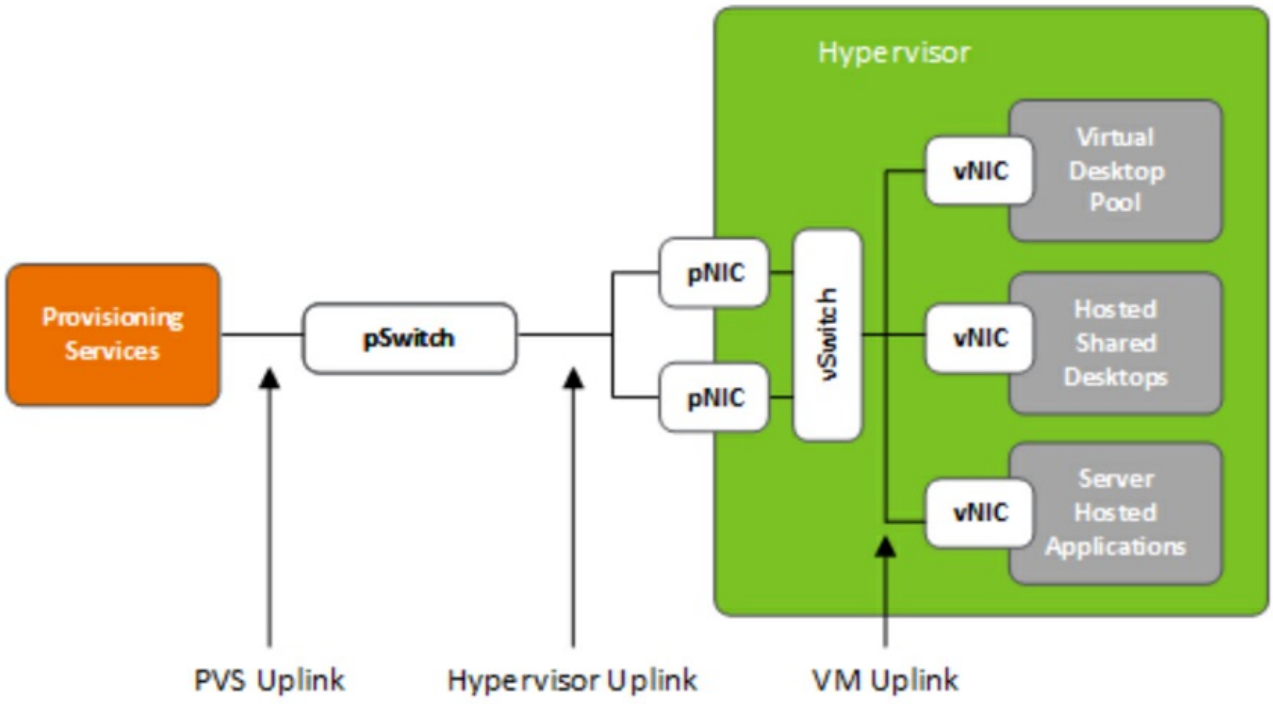
As the farm grows, administrators will need to decide whether to add more resources to the provisioning servers or to add more provisioning servers to the farm.

There are a number of environmental factors that need to be considered when determining whether the Provisioning Servers should be scaled up or scaled out:

- **Redundancy** – Spreading user load across additional less-powerful servers helps reduce the number of users affected from a single provisioning server failure. If the business is unable to accept the loss of a single high-specification server, consider scaling out.
- **Failover times** – The more target devices connected to a single provisioning server, the longer it will take for them to failover in the event that the server fails. Consider scaling out to reduce the time required for target devices to failover to another server.
- **Data center capacity** – The data center may have limited space, power and/or cooling available. In this situation, consider scaling up.
- **Hardware costs** – Initially, it may be more cost effective to scale up. However, there will be a point where scaling out actually becomes more cost effective. A cost analysis should be performed to make that determination.
- **Hosting costs** – There may be hosting and/or maintenance costs based on the number of physical servers used. If so, consider scaling up to reduce the long-term cost of these overheads.

As mentioned before it is essential that the network is sized correctly to prevent network bottlenecks causing high disk access times and directly affecting virtual desktop performance. The following diagram outlines a common Provisioning Services network infrastructure:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



The following network configuration is recommended for the network sections outline within the diagram:

- **PVS Uplink** – All disk access from the target devices will be transferred via the PVS network uplink. This means hundreds or even thousands of devices will use this network connection. Therefore, it is vital that this connection is redundant and can failover without any downtime. Furthermore, Citrix recommends a minimum bandwidth of 1Gbps per 500 target devices. For virtual provisioning servers a respective QoS quota or a dedicated physical network uplink should be configured to ensure best performance.
- **Hypervisor Uplink** – Used by all PVS target devices hosted on a particular hypervisor host. Therefore, redundancy with transparent failover is strongly recommended. Unless the target devices run a very I/O intensive workload or perform I/O intensive tasks (e.g. booting) simultaneously, a bandwidth of 1Gbps is sufficient for this uplink.
- **VM Uplink** – All network traffic for a virtual machine, including PVS streaming traffic, will traverse this virtual network connection. Unless the workload is extremely I/O intensive a bandwidth of 100 Mbps is sufficient to handle even peak loads during I/O intensive tasks, such as booting from vDisk. For example, a Windows 2012 R2 Server will read approximately 232MB during a period of 90 seconds from the vDisk until the Windows Logon Screen is shown. During this period an average data rate of 20.5 Mbps with peaks up to 90 Mbps can be observed.

The following switch settings are recommended for Provisioning Services:

- **Disable Spanning Tree** or **Enable PortFast** – In a switching environment the Spanning Tree Protocol (STP) places ports into a blocked state while it transmits Bridged Protocol Data Units (BPDUs) and listens to ensure the BPDUs are not in a loopback configuration. The port is not placed in a forwarding state until the network converges, which depending on the size of the network, may incur enough time to cause Preboot Execution Environment (PXE) timeouts. To eliminate this issue, disable STP on edgeports connected to clients or enable PortFast.
- **Storm Control** - Storm Control is a feature available on Cisco switches that allows a threshold to be set whereby, multicast, broadcast, or unicast traffic may be suppressed. Its purpose is to prevent malicious or erroneous senders from flooding a LAN and affecting network performance. PVS Servers may send a large amount of traffic by design that falls within a storm control threshold, therefore the feature should be configured accordingly.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Broadcast Helper** – The broadcast helper is required to direct broadcasts from clients to servers that would otherwise not be routed. In a PVS environment it is necessary to forward PXE boot requests when clients are not on the same subnet as the servers. If possible the recommended network design is to have PVS servers residing on the same subnet as the target devices. This mitigates the risk of any service degradation due to other networking infrastructure components.

The following network interface features should be taken into consideration when selecting a network interface for Provisioning Services:

- **TCP Offloading** – Offloading I/O tasks to the network interface reduces CPU usage and improves overall system performance, however, PVS Streaming Services can be negatively impacted when Large Send Offload is enabled due to the extra work placed on the network adapter. Many network adapters will have Large Send Offload and TCP checksum offload enabled by default.

> **注意**
>
> If Large Send Offload is enabled and the switch that the traffic is passing through does not support the frame size sent by the Large Send Offload engine, the switch will drop the frame causing data retransmission. When retransmitting, the operating system will segment the frames instead of the network adapter, which can lead to severe performance degradation.

- **Receive Side Scaling (RSS)** – Receive side scaling enables packets received from a network adapter to be balanced across multiple CPUs which allows incoming TCP connections to be load balanced, preventing bottlenecks from occurring to a single CPU. In Windows Server 2008 R2 and Windows Server 2012/2012 R2, RSS is enabled by default.

> **注意**
>
> For more information on PVS networking best practices please refer to Best Practices for Configuring Provisioning Services Server on a Network.
>
> For Provisioning Services implementations on low bandwidth networks (1Gbps or slower), performance may be improved by isolating streaming traffic from other network traffic on the LAN.
>
> Microsoft does not support NIC teaming with Hyper-V on Windows Server 2008 R2; however, third party solutions are available. Microsoft does support NIC teaming with Hyper-V on Windows Server 2012/2012 R2. All support queries regarding teaming with Hyper-V should be directed to the NIC OEM.

The Provisioning Services Subnet Affinity is a load balancing algorithm that helps to ensure target devices are connected to the most appropriate provisioning server. When configuring subnet affinity, the following options are available:

- **None** – Ignore subnets; uses the least busy server.
- **Best Effort** – Uses the least busy server/NIC combination from within the same subnet. If no server/NIC combination is available within the subnet, select the least busy server from outside the subnet. If more than one server is available within the selected subnet, perform load balancing between those servers. This is the default setting.
- **Fixed** – Use the least busy server/NIC combination from within the same subnet. Perform load balancing between servers within that subnet. If no server/NIC combination exists in the same subnet, do not boot target devices assigned

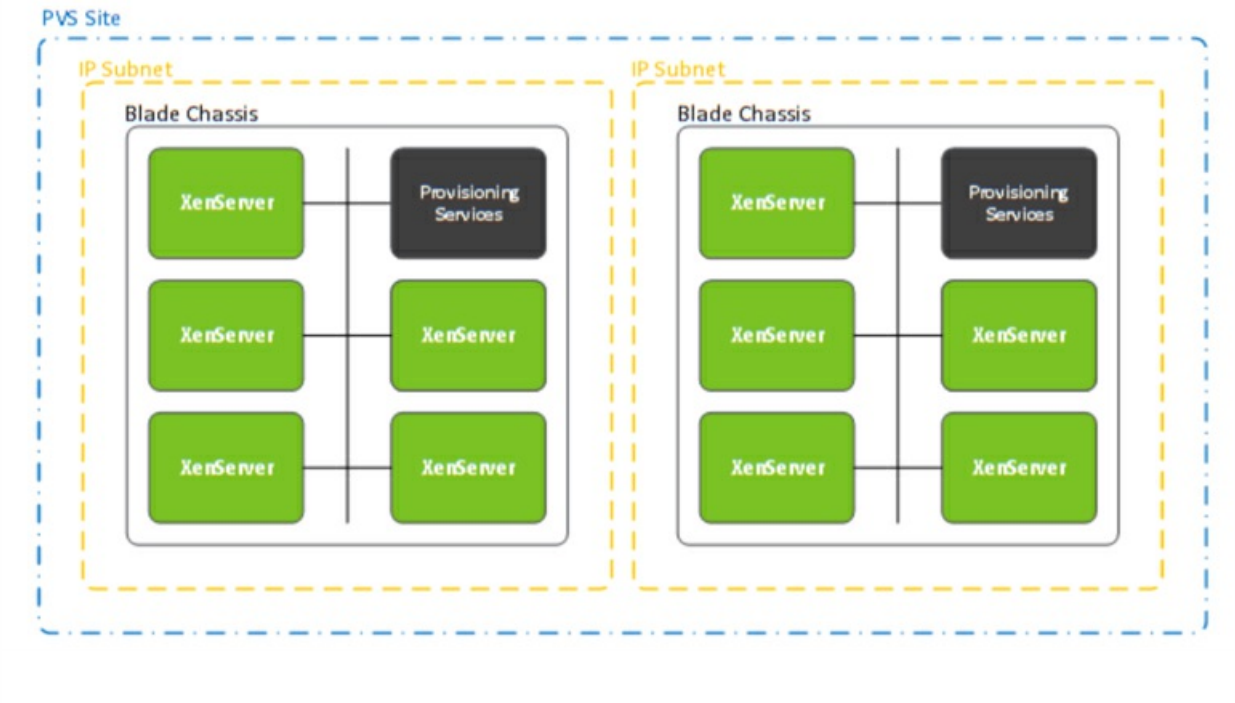
© 1999-2017 Citrix Systems, Inc. All rights reserved.

to this vDisk.

The following examples show common network configurations for physical provisioning servers. Similar configurations can be implemented for virtual provisioning servers without compromising on performance or functionality.

Blade Design

The provisioning servers and the target devices that they support reside within the same chassis. In most cases, the chassis will have a dedicated 10Gbps switch shared among all blade servers within the chassis.

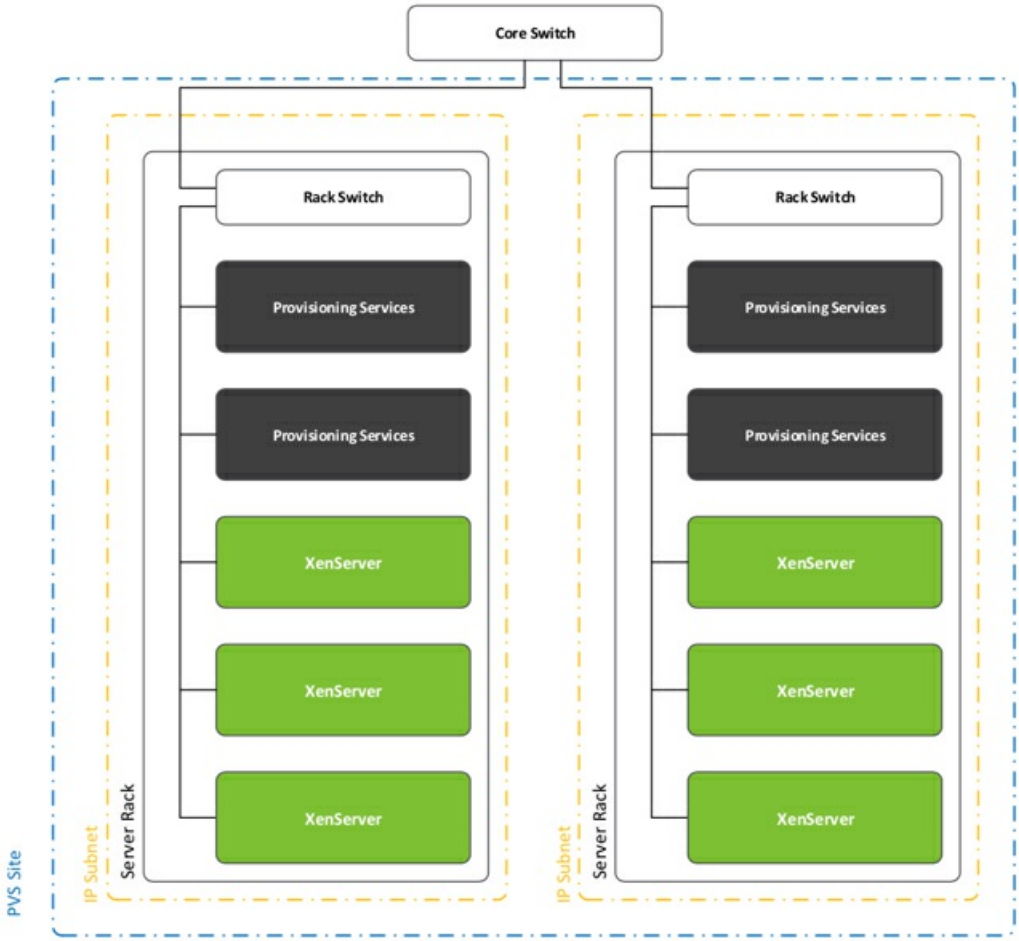


The “Best Effort” subnet affinity option is used to keep Provisioning Services traffic within the same chassis. Should the provisioning server become unavailable, the targets will failover to the second provisioning server in the second chassis, but same Provisioning Services site.

Rack Design

The second example is based on a rack design that uses rack switches to keep the provisioning traffic within the rack.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



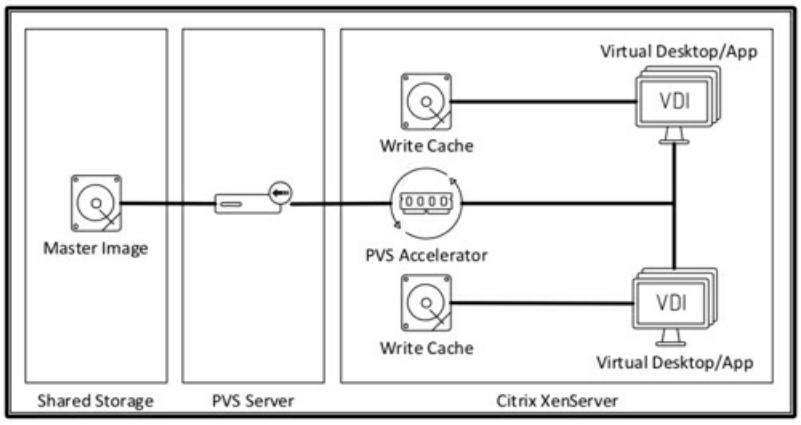
As opposed to the blade chassis design, the subnet affinity feature is not used. Instead a Provisioning Services site with two provisioning servers will be configured per server rack. This will ensure that the target devices are streamed from provisioning servers within the same rack.

Experience from the Field

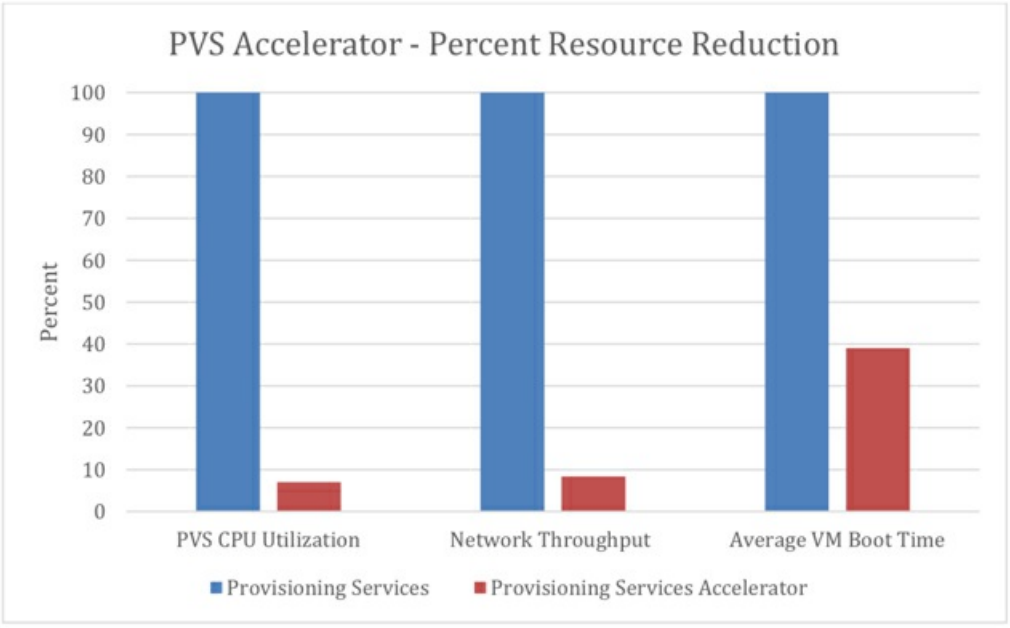
Manufacturing – A manufacturing company is designing a Provisioning Services solution to support five thousand virtual desktops. The company has concerns that Provisioning Services streaming traffic will create a bottleneck on the network affecting other applications. The company chose to build the environment on blade servers so that provisioning traffic is contained within the blade enclosure and will not impact other traffic on the network.

PVS Accelerator enables a PVS proxy to reside in the XenServer's Control Domain on a host where streaming of a Provisioning Services vDisk is cached at the proxy before being forwarded to the virtual machine. Using the cache, subsequent booting (or any I/O requests) of the virtual machine on the same host can be streamed from the proxy rather than streaming from the server over the network. PVS Accelerator requires more local resources on the XenServer host, but streaming from the server over the network saves resources, effectively improving performance.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



PVS Accelerator is a XenServer only capability. Utilizing this integrated technology reduces the load on the PVS server, reduces the overall network utilization and reduces the time it takes to boot a virtual machine.



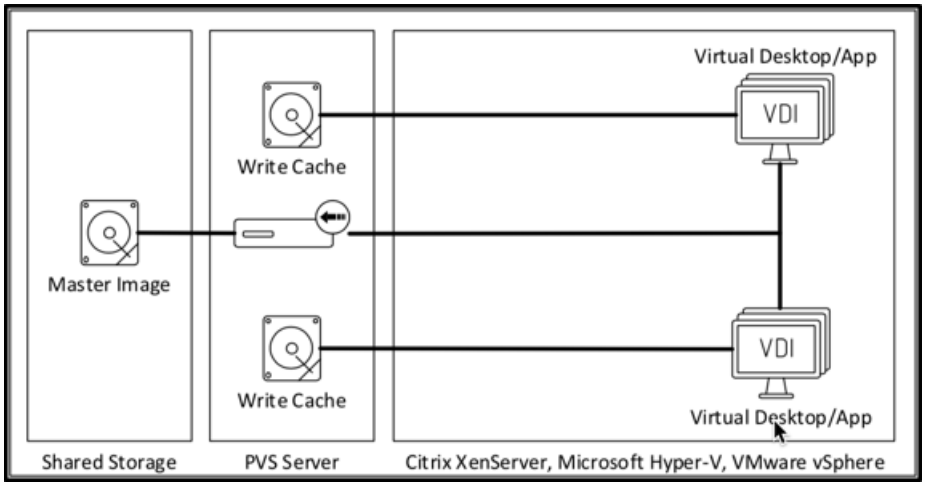
For more information on the relationship among XenServer and Provisioning Services, see the blog XenServer and PVS: Better Together.

Because the master image is read-only, each virtual machine has a writable disk to store all changes. The administrator must decide where to store the write cache disk.

PVS Server – Local Storage

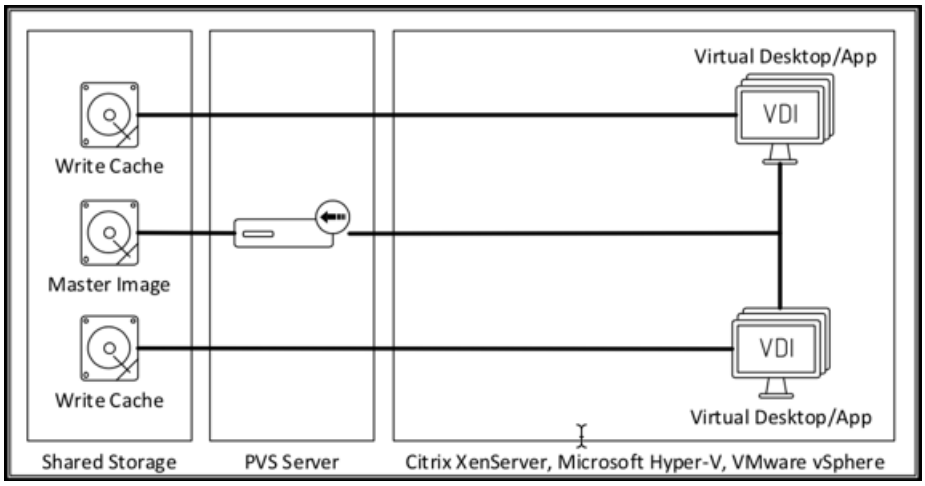
The Provisioning Services local storage holds the write cache drives for each target virtual machine. Although this is the default setting, it does increase network bandwidth requirements and increases the utilization of the Provisioning Services server.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



PVS Server – Shared Storage

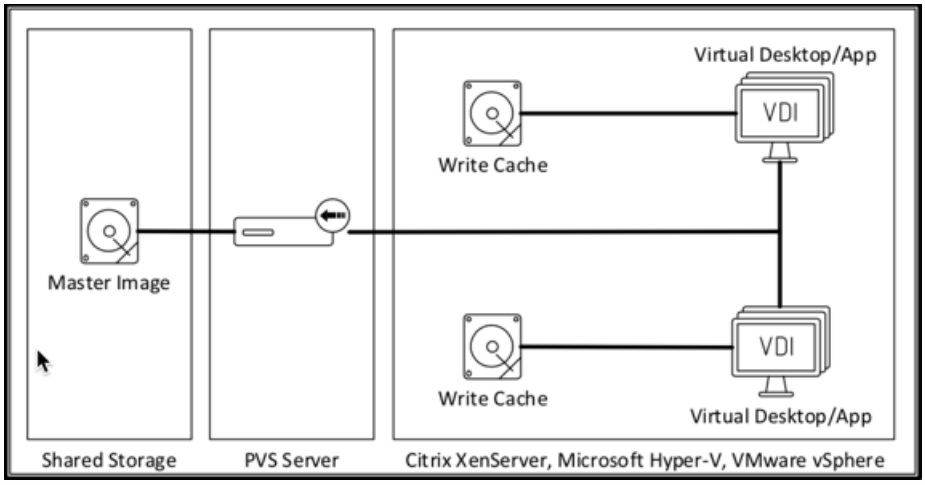
Shared storage associated with the Provisioning Services server holds the write cache drives for each target virtual machine. This option does increase network bandwidth requirements and increases the utilization of the Provisioning Services server. It also places temporary data (write cache) on expensive shared storage.



VM – Local Storage

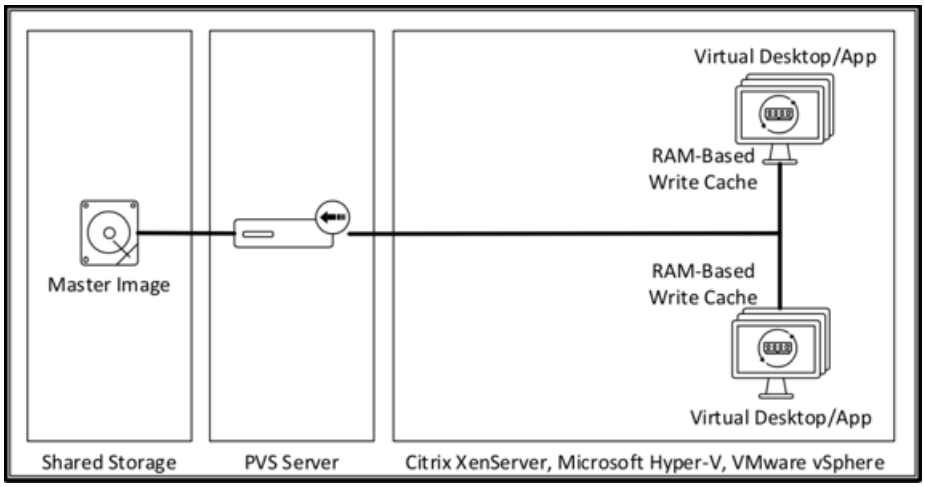
Local storage associated with the virtual machine holds the write cache drives for each target virtual machine. This option uses low cost local storage and does not consume additional resources on the Provisioning Services server. However, the local storage must be capable of support the IOPS of all virtual machines on the host.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



VM – Cache in RAM

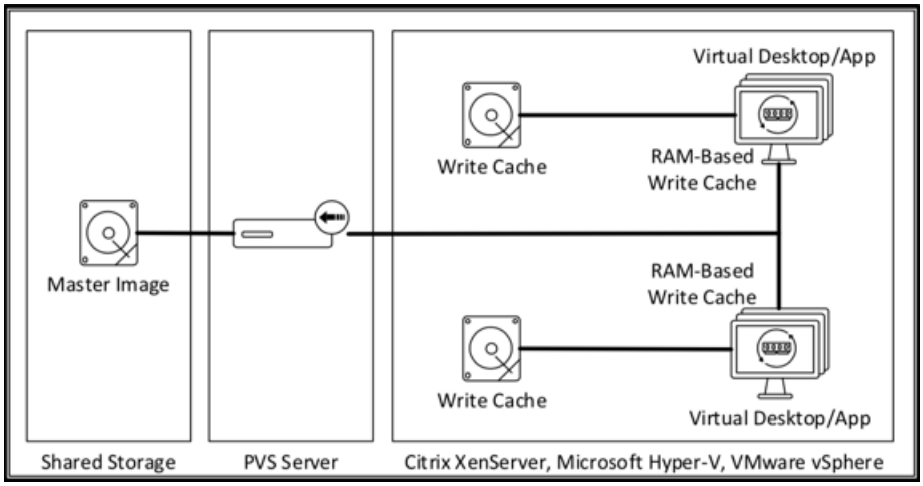
RAM associated with the virtual machine holds the write cache drives for each target virtual machine. This option provides high performance due to the speed of RAM. However, if the RAM cache runs out of space, the virtual machine will become unusable. In order to use this option, significant amounts of RAM must be allocated to each virtual machine, increasing the overall cost.



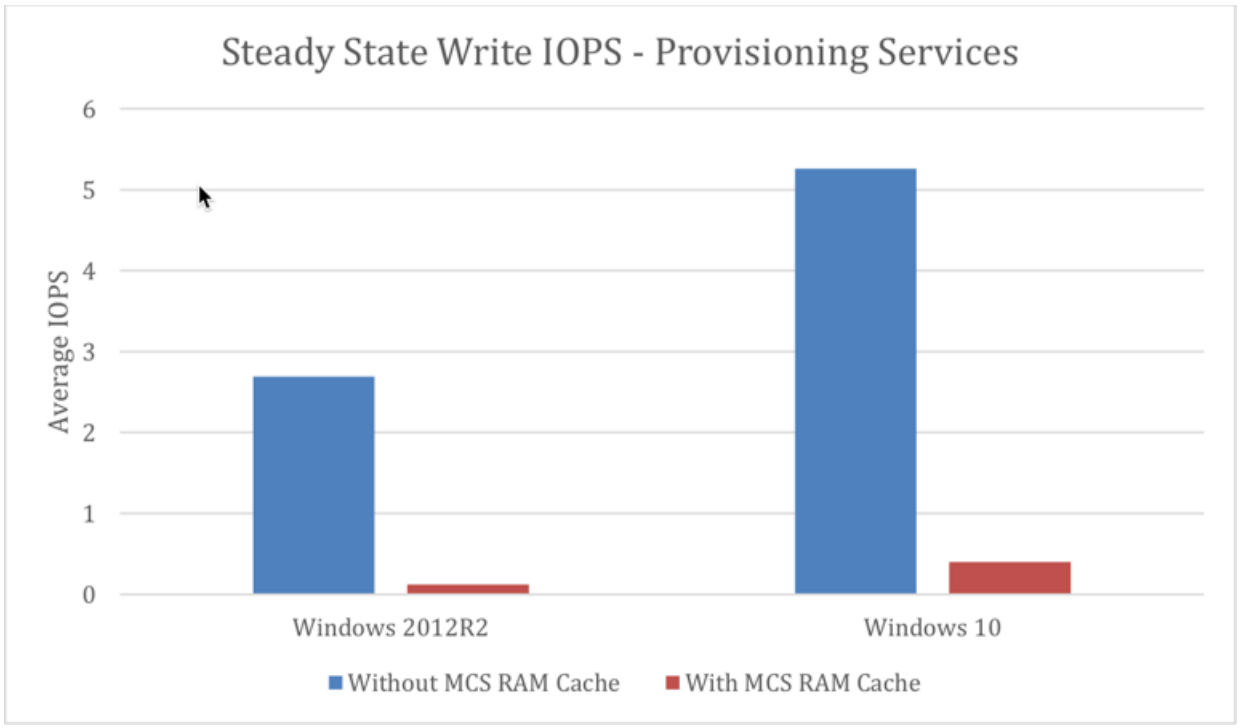
A combination of RAM and local storage is used for the write cache. First, writes are stored within the RAM cache, providing high performance. As the RAM cache is consumed, large blocks are removed from the RAM cache and placed onto the local storage write cache disk. This option provides high-levels of performance with the low cost of local storage.

Utilizing this integrated technology reduces write IOPS by 95%.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Cache in RAM with Overflow to Disk is the recommended option.



By default, most antivirus products scan all files and processes, which has a significant impact on Provisioning Services performance. For details on how antivirus software can be optimized for Provisioning Services, please refer to CTX124185 – Provisioning Services Antivirus Best Practices.

Antivirus software can cause file-locking issues on provisioning servers. The vDisk Store and write cache should be excluded from antivirus scans in order to prevent file contention issues.

When a virtual disk is running in standard mode and needs to be restarted, it downloads all of the previously loaded virus definitions. This can cause performance degradation when restarting several target devices at a time, often causing network congestion while the operation persists. In extreme cases, the target device and provisioning server can become

© 1999-2017 Citrix Systems, Inc. All rights reserved.

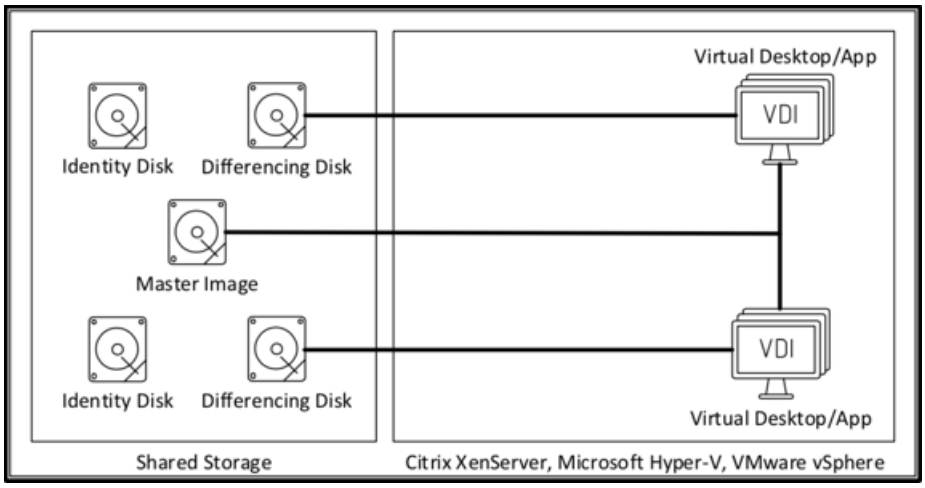
sluggish and consume more resources than necessary. If the antivirus software supports it, definition files should be redirected to the write cache drive so that they are preserved between reboots.

Machine Creation Services (MCS) uses disk-cloning technology to simplify the deployment of virtual machines. Computers are provisioned and re-provisioned in real-time from a single shared-disk image. In doing so, administrators can eliminate the need to manage and patch individual systems. Instead, administrators perform all image management on the master image.

Machine Creation Services allows administrators to break up a virtual desktop into multiple components and store those pieces on different storage arrays.

Shared Storage

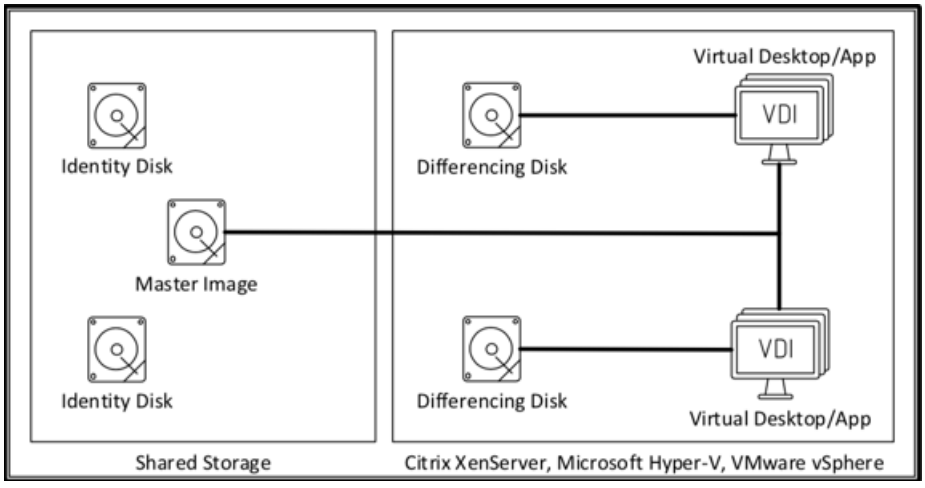
The first option utilizes shared storage for the operating system disk and the differencing disk.



Although this option allows the sharing of the master image across multiple hypervisor hosts, it puts more strain on the storage array because it must also host the differencing disk, which is temporary data.

Hybrid Storage

The second option uses shared storage for the operating system disk and local hypervisor storage for the differencing disk.



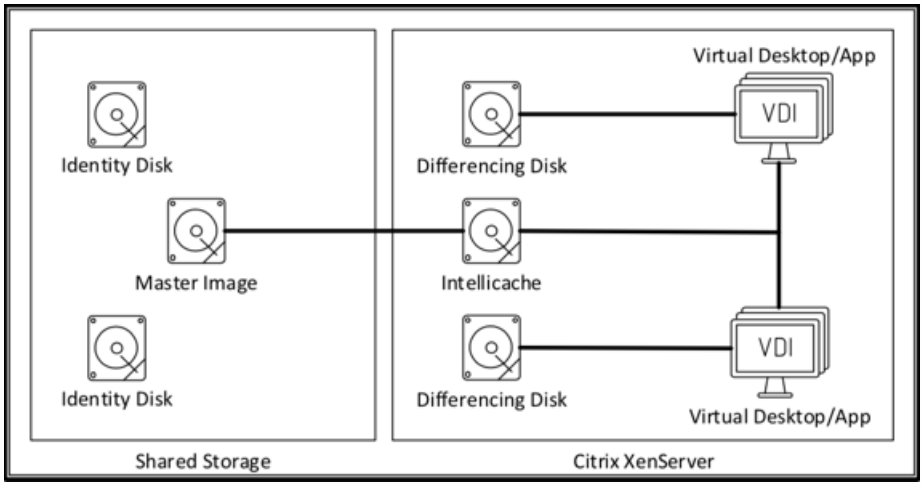
© 1999-2017 Citrix Systems, Inc. All rights reserved.

This is the most common option giving the administrator the benefits of sharing of the master image across multiple hypervisor hosts while offloading expensive, temporary write IOPS to cheap, local hypervisor storage.

XenServer IntelliCache Storage

The third option uses shared storage for the operating system disk and local hypervisor storage for the differencing disk and local XenServer storage for a local cache of the operating system disk.

This is only an option for XenServer implementations. It provides the same value as the hybrid storage approach while also reducing read IOPS from shared storage. IntelliCache can coexist with the XenServer RAM-based read cache, if XenServer RAM is limited.



Machine Creation Services incorporates two types of cloning techniques.

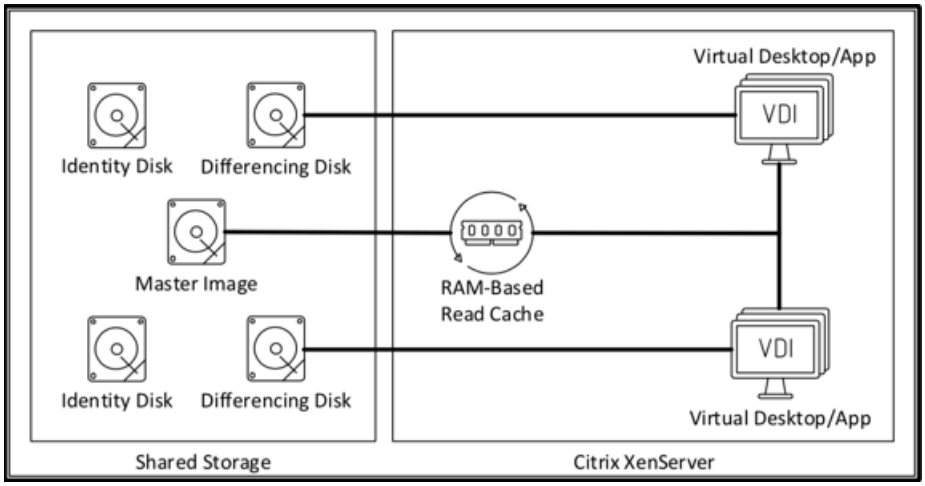
- **Thin** - Every VM within the catalog utilizes a single, read-only virtual disk for all reads. A second virtual disk, unique for each VM, captures all write IO activity.
- **Full** – Every VM within the catalog receives a full copy of the master disk image. Each VM fully owns the disk, allowing for read/write activity. Full cloning technology is only available for personal virtual desktops, where a dedicated virtual machine saves all changes to a local disk.

Administrators should consider the following when deciding between thin and full cloning technologies:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

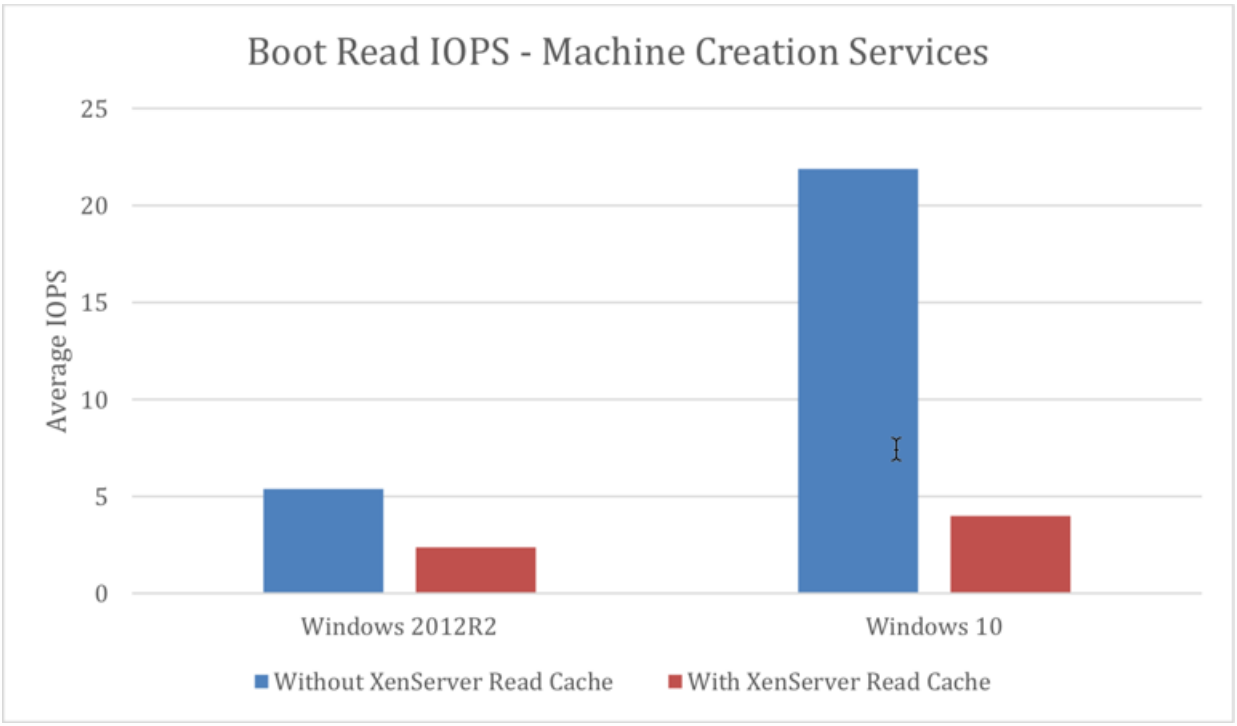
	Thin Clone	Full Clone
Storage space requirements	Has greatest storage space savings. A single master disk image is shared across multiple VMs. Only the differencing disk (writes) consume space, which continues to grow until the VM reboots	High storage space requirements Each VM receives a full copy of the master image. The size continues to grow as changes are made to the VM.
Backup/Restore	Difficult Many 3rd party Backup/DR solutions do not support snapshot/delta disks, making thin provisioned VMs hard/impossible to backup or move to other storage arrays.	Easy The VM exists within a single virtual disk, making it easy to backup and restore.
Provisioning Speed	Fast Only requires a single disk image	Slow (can be mitigated) Each VM requires a full copy of the master image. Storage optimization technologies can help mitigate.
Performance	Slower A read I/O can occur twice, one for master disk and one for differencing disk, increasing read IOPS.	Faster All read/write direct to a single disk.
Boot Storm	High Impact In a boot storm, all differencing disks re- size to hold all writes from Windows start up; placing a high load on the storage as it happens all at once.	Low Impact

During boot and logon, virtual desktops incur high levels of storage read IOPS, which can put a strain on the underlying storage subsystem. When deployed on Citrix XenServer, Shared and Pooled VDI modes utilize a RAM-based read cache hosted on each XenServer.

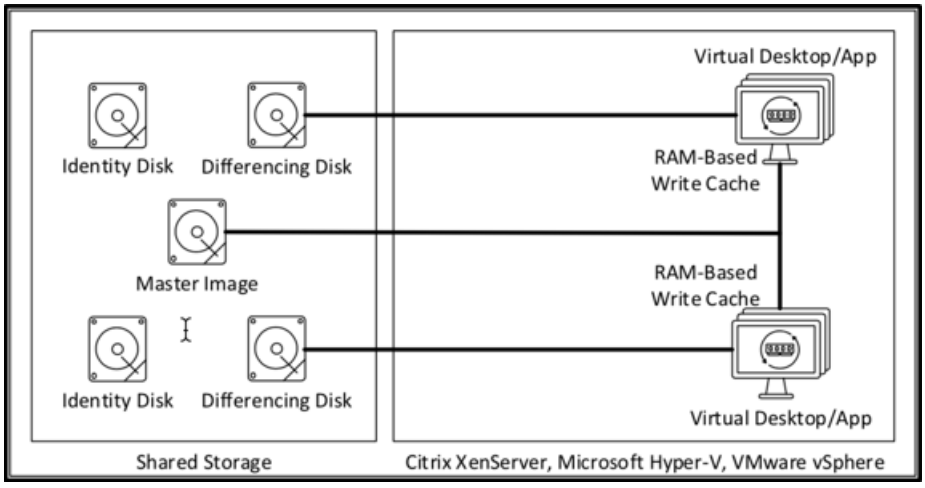


Utilizing this integrated technology reduces read IOPS by 50-80%.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

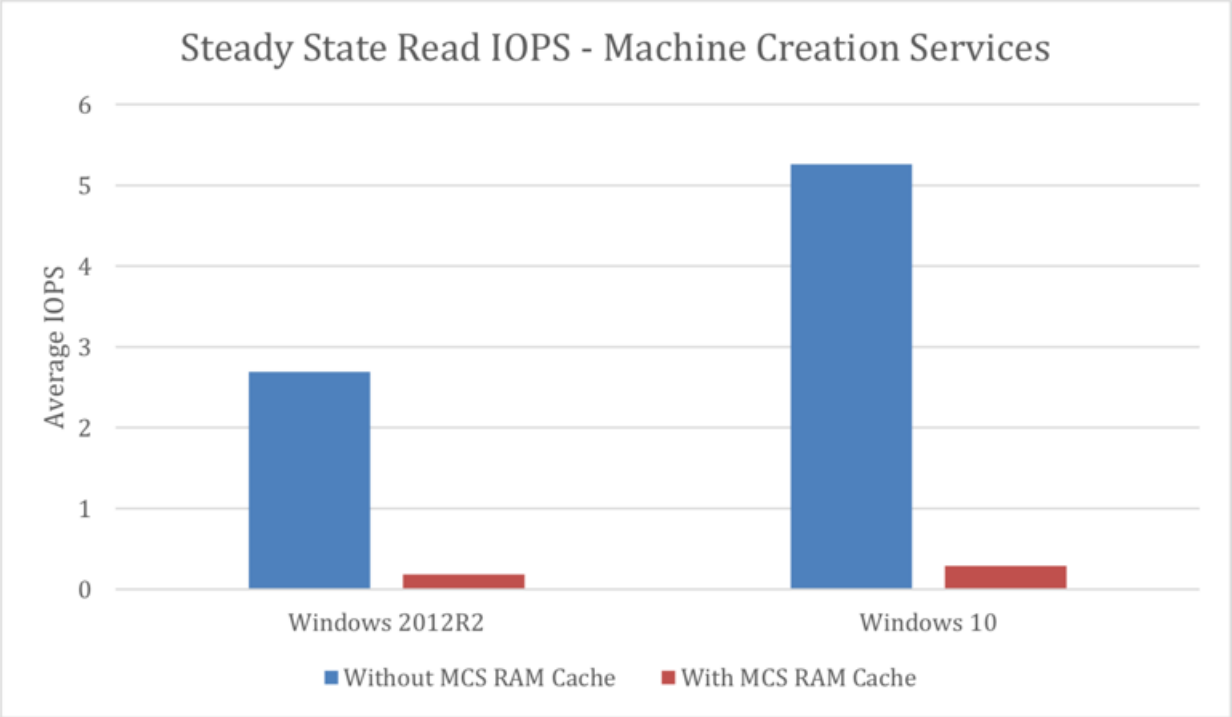


During steady state, virtual desktops incur high levels of storage write IOPS, which can put a strain on the underlying storage subsystem. Shared and Pooled VDI modes can utilize a RAMbased write cache by using non-paged pool RAM from the virtual machines operating system.



Utilizing this integrated technology reduces write IOPS by 95%.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Depending on the requirements of the organization, different security standards should be implemented within the solution. It is advisable refer to the following papers:

- Getting Started Guide for Security
- End-to-End Encryption
- System Hardening Guide
- Common Criteria
- Secure Browsing

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Design methodology hardware layer

Apr 23, 2018

This section covers hardware sizing for the virtual infrastructure servers, virtual desktops, and virtual application hosts. The sizing of these servers is typically done in two ways.

- The first and preferred way is to plan ahead and purchase hardware based on the workload requirements.
- The second way is to use existing hardware in the best configuration to support the different workload requirements.

This section will discuss decisions related to both methods.

When implementing a XenApp and XenDesktop deployment, the workloads for the infrastructure, XenDesktop, and XenApp workloads can be separated into dedicated resource clusters or mixed on the same physical hosts. Citrix recommends using resource clusters to separate the workloads, especially in an enterprise deployment. This allows better host sizing as each workload has unique requirements such as overcommit ratios and memory usage.

In smaller environments where resource clusters are cost prohibitive, the workloads may be mixed in a manner which still allows for a highly available environment. Citrix leading practice is to separate the workloads however mixed workloads is a cost based business decision.

The following table provides guidance on the number of virtual desktops that can be supported for light, medium and heavy workloads per physical core. Each desktop correlates to a single concurrent user, with the assumption that the operating system underwent optimization.

User Workload	Operating System	Users per Physical Core
Light	Windows 7	13
	Windows 8	12
	Windows 10	12
	Windows 2008R2	18
	Windows 2012R2	21
	Windows 2016	21
Medium	Windows 7	10
	Windows 8	9

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Windows 10	9
	Windows 2008R2	12
	Windows 2012R2	14
	Windows 2016	14
Heavy	Windows 7	5
	Windows 8	4
	Windows 10	4
	Windows 2008R2	6
	Windows 2012R2	7
	Windows 2016	7

The estimate for "Users per Physical Core" is a baseline number running Microsoft Office 2010. The baseline number must be adjusted based on specific infrastructure requirements. As a general guideline, the following characteristics are baseline changes to server density.

Characteristic	Server Density Impact
Antivirus (not optimized)	25% decrease
Real-time Monitoring	15% decrease
Office 2013	20% decrease
Office 2016	25% decrease
Hyper-threading	20% increase

© 1999-2017 Citrix Systems, Inc. All rights reserved.

To estimate the total number of physical cores required for the XenApp and XenDesktop workload, use the following formula for each user group:

$$\text{Total XenDesktop pCPU} = \sum Usersi \,/ UsersPerCorei * (1 + (AV + Mon + Off13 + Off16 - HV))$$

$$\text{Total XenApp pCPU} = \sum Usersi \,/ UsersPerCoreii * (1 + (AV + Mon + Off13 + Off16 - HV))$$

∑ represents the sum of all user group combinations “i”.

Usersi = Number of concurrent users per user groups

UsersPerCorei = Number of users per physical core

AV = Antivirus impact (default = 0.25)

Mon = Monitoring tools impact (default = 0.15)

Off13 = Office 2013 impact (default = .2)

Off16 = Office 2016 impact (default = .25)

HT = Hyper-Threading impact (default = .2)

If workloads will be separated (XenApp and XenDesktop workloads), the formula should be calculated twice, once for all XenDesktop users and the second for all XenApp users in order

The recommended method for sizing memory to a physical host is to size based on the total memory required to support the virtual machines and the CPU capacity of the host. In order to calculate the total memory required for XenApp and XenDesktop, simply multiply the number of virtual machines by the amount of memory allocated to the virtual machines. The sum of all of the machine catalogs will be the total RAM required for XenApp and XenDesktop hosts. This is shown in the formula below.

$$Total\ XenDesktop\ pRAM = \sum_i VM_i * vRAM_i$$

$$Total\ XenApp\ pRAM = \sum_i VM_i * vRAM_i$$

∑ represents the sum of all user group combinations “i”.

VMi = Number of concurrent users per user groups

vRAMi = Amount of RAM assigned to each virtual machine

If workloads will be separated onto different hosts (XenApp and XenDesktop workloads), the formula should be calculated twice, once for all XenDesktop users and the second for all XenApp users.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

In most situations, the number of physical hosts (pHost) to support the XenApp and XenDesktop workloads will be limited on the number of processor cores available. The following formula provides an estimate for the number of hosts required for the user workloads. The formula is based on the best practice of separating the XenApp and XenDesktop workloads due to the different recommended CPU overcommit ratios for each.

[illegible] = ([illegible] / [illegible] +1)

[illegible] = ([illegible] / [illegible]+ 1)

Once the number of physical hosts has been determined based on processor cores, the amount of RAM for each host is calculated.

[illegible] = [illegible] + ([illegible] / [illegible] – 1)

[illegible] = [illegible] + ([illegible] / [illegible] – 1)

Hosts used to deliver graphical workloads require graphics processors to deliver a high end user experience. Specific hardware hosts and graphics cards are required to support high end graphics using HDX 3D Pro. An updated list of tested hardware is available in a knowledge base article. Sizing of the desktop and application hosts of high end graphics users should be based on the GPU requirements ensuring that the host then has adequate CPU and memory resource to support the workload.

NVIDIA GRID cards can be leveraged with vGPU profiles to support multiple users. Sizing guidelines are provided from NVIDIA in the table below.

In the table, **Y** indicates that application certificates are available.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

NVIDIA GRID Graphics Board	Virtual GPU Profile	Application Certifications	Graphics Memory	Max Displays Per User	Max Resolution Per Display	Max vGPU Per Graphics Board	Use Case
GRID K2	K280Q	Y	4,096 MB	4	2560 x 1600	2	Designer
	K260Q	Y	2,048 MB	4	2560 X 1600	4	Designer / Power User
	K240Q	Y	1,024 MB	2	2560 x 1600	8	Designer / Power User
	K220Q	Y	512 MB	2	2560 x 1600	16	Knowledge Worker
	K200		256 MB	2	1900 x 1200	16	Power User
GRID K1	K180Q	Y	4,096 MB	4	2560 x 1600	4	Power User
	K160Q	Y	2,048 MB	4	2560 x 1600	8	Power User
	K140Q	Y	1,024 MB	2	2560 x 1600	16	Power User
	K120Q	Y	512 MB	2	2560 x 1600	32	Power User
	K100		256 MB	2	1900 x 1200	32	Knowledge Worker

The primary storage architectures are as follows:

- **Local Storage** - Uses hard disks directly attached to the computer system. The disks cannot be shared with other computer systems, but if the computer is hosting pooled or hosted shared desktops, a shared storage solution is not necessary. In many cases local storage can perform as well as shared storage. Scalability is limited to the number of drive bays available in the computer system. Many blade servers for example have just two drive bays, so using local storage to support a XenDesktop deployment may not be optimal.
- **DAS** - Storage sub-system directly attached to a server or workstation using a cable. It uses block-level storage and can be a hard disk local to the computer system or a disk shelf with multiple disks attached by means of external cabling. Unlike local disks, disk shelves require separate management. Storage shelves can be connected to multiple servers so the data or disks can be shared.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **NAS** - Provides file-level storage to computer systems through network file shares. The NAS operates as a file server, and NAS systems are networked appliances which contain one or more hard drives, often arranged into logical, redundant storage containers or RAID arrays. Access is typically provided using standard Ethernet and network file sharing protocols such as NFS, SMB/CIFS, or AFP.

> **注意**
>
> NAS can become a single point of failure. If the network share becomes unavailable, all target devices streamed from the disk will be unavailable as well.

- **SAN** - Dedicated storage network that provides access to consolidated, block-level storage. SANs allow computers to connect to different storage devices, so no server has ownership of the storage subsystem enabling data to be shared among multiple computers. A SAN will typically have its own dedicated network of storage devices that are generally not accessible through the network by standard means. In order to connect a device to the SAN network a specialized adapter called the Host Bus Adapter (HBA) is required. SANs are highly scalable with no noticeable change in performance as more storage and devices are connected. SANs can be a costly investment both in terms of capital and the time required to learn, deploy and manage the technology.
- **Hybrid** - A NAS head refers to a NAS which does not have any on-board storage, but instead connects to a SAN. In effect, it acts as a translator between the file-level NAS protocols (NFS, CIFS, etc.) and the block-level SAN protocols (Fibre Channel and iSCSI). Thus it can combine the advantages of both technologies and allows computers without Host Bus Adapters (HBA) to connect to centralized storage.

The following table summarizes the storage options available and rates their suitability for XenDesktop deployments.

Storage Properties	Local	DAS	NAS	SAN
Implementation costs	Low	Medium	Medium	High
Administration	Low	Medium	Medium	High
Performance	High	Med - High	Med - High	High
Redundancy	Low - Med	Med - High	Med - High	High
Scalability	Low	Med - High	Med - High	High
Typical use case	Small to medium production and test environments	Small to medium production environments	Small to medium production environments	Medium to large production environments

© 1999-2017 Citrix Systems, Inc. All rights reserved.

> **注意**
>
> Hyper-V 2008 R2 does not support NAS technology. Hyper-V 2012/2012 R2 only supports NAS solutions that support the SMB 3.0 protocol. For more information please refer to the HyperV 2008 R2 and Hyper-V 2012 R2 sections of the handbook.

Local storage is best suited for storing virtual machines which do not have high availability requirements or persistent data attached such as random (pooled) desktops or hosted shared desktops. Local and DAS is suited for storing user data and home directory files. If using Machine Creation Services, master images as well as any updates must be replicated to each server.

NAS and SAN storage is best suited for infrastructure servers supporting the XenDesktop environment, and virtual machines with persistent data such as static (dedicated) desktops.

To choose the optimal RAID level, it is necessary to consider the IOPS and read/write ratio generated by a given application or workload in combination with the individual capabilities of a RAID level. For hosting read intensive workloads, such as the Provisioning Services vDisk store, RAID levels that are optimized for read operations such as RAID 1, 5, 6, 10 are optimal. This is because these RAID levels allow read operations to be spread across all disks within the RAID set simultaneously.

For hosting write intensive workloads, such as Provisioning Services write cache and Machine Creation Services differencing disks, RAID levels such as RAID 1 or 10 are optimal, as these are optimized for writes and have a low write penalty.

The following table outlines the key quantitative attributes of the most commonly used RAID levels:

RAID	Capacity (%)	Fault Tolerance	Read Performance	Write Performance	Minimum number of disks
0	100	None	Very High	High (Write Penalty 1)	2
1	50	Single-drive failure	Very High	Medium (Write Penalty 2)	2
5	67 - 94	Single-drive failure	High	Low (Write Penalty 4)	3
6	50 - 88	Dual-drive failure	High	Low (Write Penalty 6)	4
10	50	Single-drive failure in each sub array	Very High	Medium (Write Penalty 2)	4

> **注意**
>
> The write penalty is inherent in RAID data protection techniques, which require multiple disk I/O requests for each application write request, and ranges from minimal (mirrored arrays) to substantial (RAID levels 5 and 6).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

To determine the number of disks required it is important to understand the performance characteristics of each disk, the characteristics of the RAID level and the performance requirements of the given workload. The basic calculation for determining the total number of disks needed is:

□□□□□ # □□ □□□□□ =
(□□□□□ □□□□ □□□□ + (□□□□□ □□□□□ □□□□ ∗ □□□□ □□□□□□□))/□□□□ □□□□□ □□□□

For example, a disk manufacturer is reporting that a particular disk array which they have developed has a total workload IOPS of 2000. The raw IOPS per disk is 175. To determine how many disks are required to support a workload with 20% read operations and 80% write operations on RAID 10:

□□□□□ # □□ □□□□□ =((20% ∗ 2000) + (80% ∗ 2000) ∗ 2) /175= 20.57 □□ 21 □□□□□

Based on the previous example, the following table shows how the disk count will vary based on the RAID level and the read/write ratio.

RAID	RAW IOPS (per disk)	Workload IOPS	Read %	Write %	Disk Count
0	175	2000	20	80	12
	175	2000	80	20	12
1 / 10	175	2000	20	80	21
	175	2000	80	20	14
5	175	2000	20	80	39
	175	2000	80	20	19

Hard disk drives (HDDs) are the traditional variation of disk drives. These kinds of disks consist of rotating platters on a motor-driven spindle within a protective enclosure. The data is magnetically written to and read from the platter by read/write heads.

Different implementations of this technology are available on the market, which differ in terms of performance, cost and reliability.

- Serial ATA (SATA) disk transmit data serially over two pairs of conductors. One pair is for differential transmission of data, and the other pair is for differential receiving of data. SATA drives are widely found in consumer desktop and laptop

© 1999-2017 Citrix Systems, Inc. All rights reserved.

computers. Typical SATA drives have transfer speeds ranging from 1500 – 6000Mbps and support hot-swapping by design.

- Small Computer Systems Interface (SCSI) disks use a buffered, peer to peer interface that uses handshake signals between devices. Many SCSI devices require a SCSI initiator to initiate SCSI transactions between the host and SCSI target. SCSI disks are common in workstations and servers and have throughputs ranging from 40 – 5120Mbps. iSCSI (Internet Small Computer System Interface) is a mapping of the regular SCSI protocol over TCP/IP, more commonly over Gigabit Ethernet.
- Fibre Channel (FC) disk is the successor to the parallel SCSI disk and is common in SAN storage devices. Fibre Channel signals can run on an electrical interface or fibre-optic cables. Throughput can range from 1 – 20Gbps, and connections are hot-pluggable.
- Serial Attached SCSI (SAS) disk uses a new generation serial communication protocol to allow for higher speed data transfers than SATA disks. Throughput can range from 2400 – 9600Mbps.

In contrast to traditional hard disks, Solid State Disks (SSDs) use microchips to retain data in either NAND non-volatile memory chips (flash) or DRAM and contain no moving parts. SSDs are less susceptible to physical shock, have lower access times and latency and have higher I/O rates. SSDs have significantly higher random read performance. An SSD drive can attain anywhere from 5,000 to 20,000 random reads per second. SSDs are also more expensive per gigabyte (GB) and typically support a limited number of writes over the life of the disk.

Flash memory-based SSDs can be either based on multi-level cells (MLC) or single-level cells (SLC). SLC devices only store one bit of information in each cell. MLC devices can store multiple bits of information with each cell. Flash based SSDs cost lower than DRAM based SSDs but perform slower. DRAM based SSD devices are used primarily to accelerate applications that would otherwise be held back by the latency of flash SSDs or traditional HDDs.

SSDs were previously not viable for enterprise storage solutions because of the high cost, low capacity and fast wear of the drives. Improvements in SSD technology and lowering costs are making them more favorable over HDDs. Solid state hybrid drives (SSHD) combine the features of SSDs and HDDs, by containing a large HDD drive with an SSD cache to improve performance of frequently accessed data.

Comparing SSDs and HDDs is difficult since HDD benchmarks are focused on finding the performance aspects such as rotational latency time and seek time. As SSDs do not spin, or seek, they may show huge superiority in such tests. However, SSDs have challenges with mixed reads and writes and their performance may degrade over time.

The following table compares the transfer rates of some of the more common storage types available on the market today.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Technology	Rate (MBps)
iSCI over Fast Ethernet	100
Ultra-2 wide SCSI (16 bits/40 MHz)	640
iSCI over Gigabit Ethernet	1,000
SATA rev 3	6,000
SAS 3	9,600
FCoE over 10 GbE	10,000
SATA rev 3.2 - SATA Express	16,000
iSCI over Infiniband	32,000

SCSI and SATA disks are best suited for storing data that does not have high performance requirements like the PVS vDisk store. SAS, Fibre Channel, or SSD drives are best suited for storing data that have high performance requirements like the PVS write cache.

Storage bandwidth is the connectivity between servers and the storage subsystem. Understanding bandwidth requirements can help determine the proper hardware for delivering data and applications at speeds for a positive end user experience. For most datacenters 10Gbps Ethernet or 10Gbps FCoE is sufficient for storage connections. Smaller environments however may only need 1Gbps bandwidth. In virtualized environments it is not just important to look at the bandwidth requirements of the physical host and storage subsystem, but determining how much bandwidth is required for each virtual machine plays a factor too.

In order to plan for the required bandwidth, it is necessary to determine the throughputs for every individual system that uses a shared component or network path. For example, the following information is provided for an environment with 100 similar virtual machines (hosted on 10 virtualization hosts and connected to one NAS head).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Average	Peak
Throughput per VM	10 MBps	30 MBps
Throughput per host	100 MBps (10 VMs x 10 MBps)	300 MBps (10VMs x 30 MBps)
Throughput per storage	1 GBps (10 hosts x 100 MBps)	3 GBps (10 hosts x 300 MBps)

The NIC used for storage communication needs to be a 1Gbps adapter in order to handle the peak load. The NAS head as well as its network connection need to support 3Gbps worth of data traffic in order to support the peak load of all systems.

A one-size-fits-all storage solution is unlikely to meet the requirements of most virtual desktop implementations. The use of storage tiers provides an effective mechanism for offering a range of different storage options differentiated by performance, scalability, redundancy and cost. In this way, different virtual workloads with similar storage requirements can be grouped together and a similar cost model applied.

For example, a XenDesktop implementation using tiered storage may look like the following:

- **Tier 1 storage group** - Write intensive files such as the write cache and differencing disks are placed in a storage group consisting of SSDs.
- **Tier 2 storage group** - Mission critical data, or data that requires high availability, are placed in a storage group consisting of less expensive high performing drives.
- **Tier 3 storage group** - Seldom used data files, read-only files, or other non-mission critical data placed in a storage group consisting of low cost and lower performing drives.

Thin provisioning allows more storage space to be presented to the virtual machines than is actually available on the storage repository. This lowers storage costs by allowing virtual machines access to disk space that is often unused. This is particularly beneficial to Machine Creation Services which uses a linked-clone approach to provisioning virtual machines. Thin provisioning minimizes the storage space required for the master image copies used to build virtual machines. Thin provisioning is possible at the physical storage layer, a feature usually available with most SAN solutions, and at the virtual layer. NFS based storage solutions will usually have thin provisioning enabled by default.

At the physical storage layer, it is important to ensure that sufficient storage is available to prevent the risk of virtual machines not being available in a storage “overcommit” scenario when available disk space is exhausted. Organizations should decide if the cost savings thin provisioning provides outweighs the associated risk and consider enabling if the storage solution supports it.

> **注意**
>
> Virtual machines may not function if disk space is exhausted so it is important to have a process in place, either through alerts or

© 1999-2017 Citrix Systems, Inc. All rights reserved.

notifications that will give administrators enough time to add more disks to the storage solution so that the XenDesktop environment is not impacted.

Data de-duplication is a data compression technique whereby duplicate data is replaced with pointers to a single copy of the original item. This reduces storage requirements and costs by improving storage utilization, however it can impact storage performance.

There are two implementations of de-duplication available:

- **Post-process de-duplication** – The de-duplication is performed after the data has been written to disk. Post-process de-duplication should be scheduled outside business hours to ensure that it does not impact system performance. Post Process de-duplication offers minimal advantages for random desktops as the write-cache/difference disk is typically reset on a daily basis.
- **In-line de-duplication** – Examines data before it is written to disk so that duplicate blocks are not stored. The additional checks performed before the data is written to disk can sometimes cause slow performance. If enabled, in-line duplication should be carefully monitored to ensure that it is not affecting the performance of the XenDesktop environment.

If the storage solution supports it, enabling post-process data de-duplication is recommended for minimal impact to XenDesktop performance.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

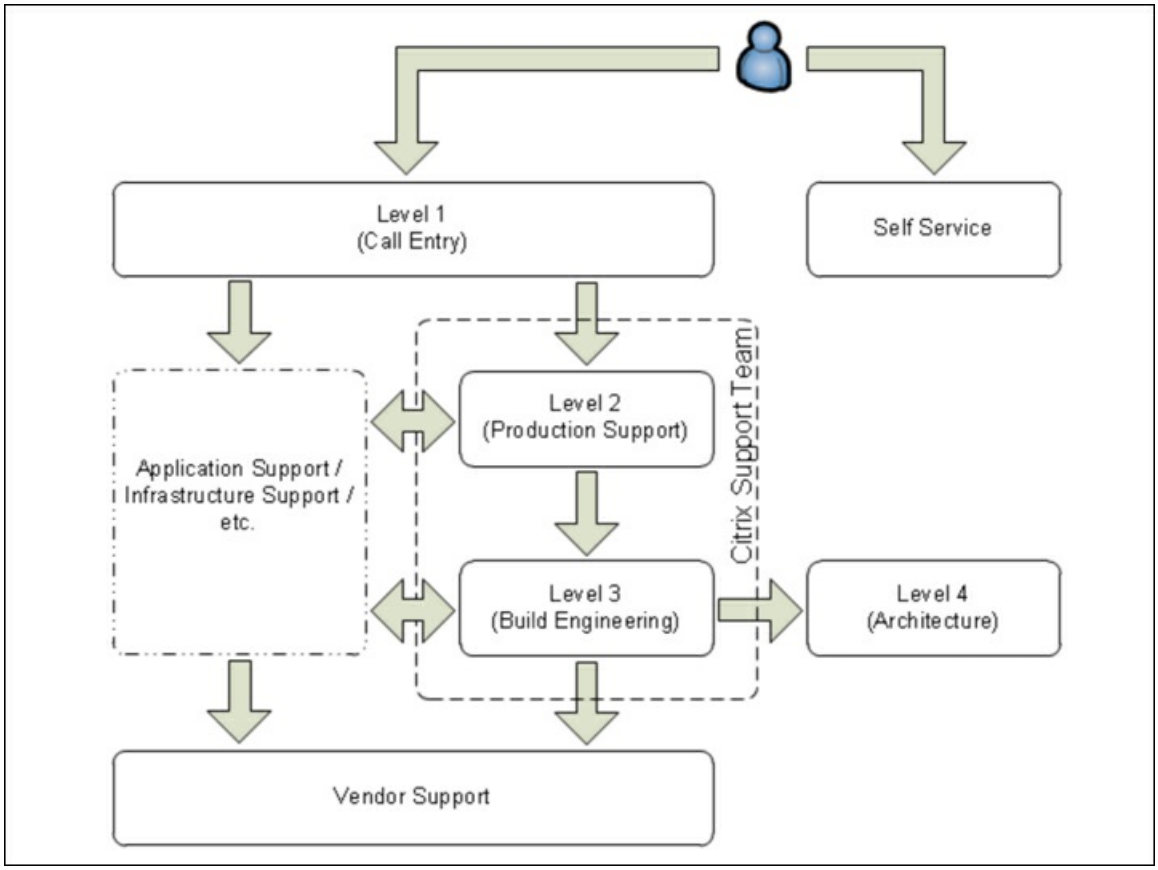
监视

Jan 29, 2018

Like any integrated system, monitoring and maintenance is critical to the overall health of the solution. Without proper support, operations and health monitoring systems in place, the user experience will slowly start to degrade.

When problems arise, technical support is the first point of contact. This section addresses the proper staffing, organization, training, delegated administration and tools that should be used to maintain the Citrix deployment.

Multiple levels of support have been found to be the most effective ways of addressing support issues. Low criticality, low complexity or frequently occurring issues should be managed and resolved at the lower support levels. High criticality and complex issues are escalated to more experienced architects or infrastructure owners. The diagram below outlines a common multi-level support structure.



If a user encounters an issue, Level-1 support (help desk) is the entry point to the support system. Level-1 should resolve 75% of all issues encountered, of which a majority will be routine problems that only require a limited knowledge of the Citrix environment. At this level, issues are quickly resolved and some may be automated (self-service), for example password resets and resource provisioning.

Non-routine problems that exceed Level-1's abilities are escalated to Level-2 (Operators). This support level is generally

© 1999-2017 Citrix Systems, Inc. All rights reserved.

comprised of administrators supporting the production Citrix environment. Information on the end user's problem and attempted troubleshooting steps are documented at the first level allowing Level-2 technicians to immediately begin addressing the problem. Level-2 technicians should handle only 20% of the support tickets and are highly knowledgeable on the Citrix environment.

Complex issues that exceed Level-2's abilities should be escalated to Level-3 (Implementers). Level-2 and Level-3 support may often both be members of the Citrix Support Team, with Level-3 comprising the senior staff maintaining the Citrix environment. Level-3 issues are complicated and often mission critical requiring expert knowledge of the virtual desktop and application environment. Level-3 support tickets should amount to no more than 5% of all support issues.

The final level, Level-4 (Architects), is focused on the strategic improvements for the solution, testing new technologies, planning migrations, and other high level changes. Generally, Level-4 is not involved in active support of a production environment.

Should support discover an issue that is related to an application or underlying infrastructure, the ticket is handed to the appropriate team for troubleshooting. If a program bug is discovered, the issue is then re-escalated and a ticket is established with the appropriate vendor.

The following table highlights the recommended characteristics of each support level.

Support level	Description	Responsibilities	Skill set
Level 1 - Help	Provide first-line support of reported issues. Initially, servicing support messages and phone calls. This level needs to perform	• Perform issue definition, initial analysis and basic issue resolution • Perform initial troubleshooting to determine the nature of the issue • Create ticket, collect user information, and log all troubleshooting steps performed • Resolve basic Citrix related issues, connectivity problems and application related issues using existing knowledge base articles • Escalate issue to Level-2 if advanced skills or elevated	• General Citrix XenApp/XenDesktop knowledge (CCA, CCA-V) • General Windows client OS/server OS

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Support level	Description	Responsibilities	Skill set
	issue resolution. Often processes requests for application access or support with configuring plugins.	required • Ability to isolate the issue to be Citrix related, Microsoft related or third party Application related • If it affects the production environment or is potentially causing a system level outage, escalate directly to Level-3 • Generate requests for additional issue resolution guides as necessary • Follow up with end users when a support ticket is closed to ensure the problem has been satisfactorily resolved	• General Active Directory knowledge • General Networking knowledge (CCNA)
		• Perform intermediate issue analysis and resolution. • Identify root cause of issues. • Respond to server alerts and system outages. • Create weekly report on number of issues, close rate, open issues, etc. • Review vendor knowledge base articles. • Respond to out-of-hours helpdesk calls. • Respond to critical monitoring alerts. • Generate internal knowledge base articles and issue	Experience with Microsoft Windows Server including but not limited to: • Configuring operating system options • Understanding Remote Desktop Services policies and profiles • Using Active Directory • Creating users/managing permissions and administrator rights • Creating and modifying Active Directory group policies Basic administration

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Support level	Description	Responsibilities	Skill set
Level-2 (Operators)	Primarily supporting day-to-day operations of the Citrix environment, may include proactive monitoring and management. In addition, this role should also perform intermediate level troubleshooting and utilize available monitoring or troubleshooting tools. Assist with resolving issues escalated by Level-1 support.	Level-1 troubleshooting workflows. • Perform basic server maintenance and operational procedures. • Manage user profiles and data. • Escalate ticket to Level-3 or appropriate technology owner if advanced skills or elevated permissions are required. • Generate requests for additional issue resolution scripts and knowledge base articles as necessary. • Able to read built-in event logs for Windows and Citrix to do basic troubleshooting following public information via Google/Bing.	protocols (TCP) • An understanding of firewall concepts • An understanding of email administration and account creation • An understanding of Remote Desktop Services policies and profiles • The ability to create shares and give access to shared folders/files Experience performing the following: • Managing, maintaining, monitoring and troubleshooting Citrix solutions • Backing up components in Citrix environments • Updating components in Citrix environments • Creating reports for trend analysis
		• Perform advanced issue analysis and resolution. • Perform maintenance and environment upgrades. • Addresses high severity issues and service outages. • Manage the Citrix environment. • Oversee and lead administrative tasks performed by Level-2. • Manage network and storage	Knowledge of how the following Windows components integrate with Citrix technologies: • Active Directory Domain Services • Active Directory

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Support level	Description	Responsibilities	Skillset
		relates to the Citrix environment (depending on size of company or Citrix environment). • Review periodic reports of server health, resource usage, user experience, and overall environment performance. • Review vendor knowledge base articles and newly released updates. • Perform policy-level changes and make Active Directory updates. • Review change control requests that impact the Citrix environment. • Perform advanced server and infrastructure maintenance. • Review knowledge base articles and issue resolution scripts for accuracy, compliance, and feasibility. • Create knowledge base articles and issue resolution scripts to address Level-2 requests. • Escalate ticket to vendor specific technical support, when necessary, and notify Level-4 of the issue.	• Policies • Domain Name System (DNS) • Dynamic Host Configuration Protocol (DHCP) • Group Policy Objects (GPOs) • NTFS Permissions • Authentication and Authorization • Knowledge of IIS • Microsoft Windows Operating Systems: Windows 10, Windows 8.1, Windows 7 Windows Server 2012 R2 Windows Server 2008 R2 • Roles and features of Windows Server • Knowledge of SQL 2008 R2 and newer • Knowledge of SQL Clustering, Mirroring and AlwaysOn Availability Groups. • General networking skills (i.e. routing, switching) • Knowledge of hypervisors. • Knowledge of shared storage configuration and management.
Level-3 (Implementer)	Central point for implementing, administering and maintaining Citrix desktop and application virtualization infrastructure. This role focuses on deploying new use cases and leading lifecycle management initiatives. Generally, one Implementer could focus on one use-case at a time. For example, three new concurrent use cases would require three Implementers. Escalates issues to software vendor specific technical support and notifies Level-4 about this issue.		
		• Provide technical leadership for	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Support level	Description	Responsibilities	Skill set
Level-4 (Architect)	The Level-4 team has minimal exposure to administrative tasks but focuses on scoping, planning and executing Citrix-specific service and project requests. An architect translates business requirements into a technical design.	• Lead design updates and architecture revisions. • Address high severity issues and service outages. • Oversee technology integration workflows. • Review periodic reports of server health, resource usages, user experience, and overall environment performance to determine next steps and upgrade paths. • Initiate load testings to determine capacity of environment. • Review frequently recurring helpdesk issues. • Ensure technical specifications continue to meet business needs. • Update design documentation.	Advanced architectural assessment and design skills for: • Citrix XenApp • Citrix XenDesktop • Citrix XenServer, VMware vSphere, Microsoft Hyper-V • Citrix Provisioning Services • Citrix NetScaler • Citrix StoreFront • Active Directory • Storage solutions • Networking • Application delivery • Disaster recovery • Policies/policy structures and security restrictions • Licensing • Methodology Intermediate knowledge of: • General networking skills • Change control process • Project management • Risk assessment
Vendor support	Vendor assistance may be necessary should defects in a program be discovered. At this stage, Level-3 engineers need to establish a support ticket with the appropriate vendor to assist with finding a solution.		
Self-service	A self-service portal should be utilized for noncritical tasks, such as application access, permissions, password resets, etc. The portal can range from a simple FAQ page to a fully automated process requiring no human interaction. The purpose of the self-service portal is to add an additional touch point for end users to address basic issues, preventing the creation of new support tickets.		

© 1999-2017 Citrix Systems, Inc. All rights reserved.

The following table details the recommended training, certifications and experience for each support level.

Role	Recommended training	Recommended course(s)	Recommended certification	Relevant experience
Help Desk (Level 1)	Level-1 support personnel should be provided with basic training on Citrix XenApp, Citrix XenDesktop and supporting technologies. This can include internal training from subject matter experts or from a Citrix Authorized Learning Center. The training provided should focus on the following topics: • High level overview of the XenApp and XenDesktop implementation • Using Citrix Director to manage user sessions • Troubleshooting Citrix XenApp and XenDesktop sessions • Troubleshooting methodology In addition, regular training should be provided to the Tier-1 team members on the latest troubleshooting recommendations from the Level-2 and Level-3 teams as well as details on any relevant changes to the environment. This will help to ensure a good baseline knowledge level across the team and consistent customer service.	CXD-105: Citrix XenApp and XenDesktop Help Desk Support	N/A	1+ years (Entry level also acceptable)
Operator (Level 2)	Level-2 personnel should conduct regular team training sessions to refine administrative skills and ensure a baseline knowledge level across the team. Formalized trainings are also essential when there are architectural updates to the environment and the Level-2 team is working with unfamiliar technologies. All members of the Level-2 team should achieve the Citrix Certified Associate (CCA) certification for Citrix XenApp and XenDesktop. Advanced training on Windows concepts will also be essential for Level-2 team members who do not have desktop or server support experience. Finally, on-the-job training along with close integration with Level-3 administrators is essential as the Level-2 roles are formalized and responsibilities are handed over from Level-3 to Level-2.	CXD-210 XenApp and XenDesktop 7.1x Administration	Citrix Certified Associate - Virtualization	2-3 years
Implementer (Level-3)	Level-3 support team members hold a minimum of three years of enterprise experience implementing and supporting XenApp, XenDesktop, Provisioning Services and Windows operating systems. Level-3 staff should also complete the Citrix Certified Professional (CCP) certification track as this will prepare them to proactively manage the user community and implement Citrix solutions according to Citrix leading practices.	CXD-400: Designing App and Desktop Solutions with Citrix XenApp and XenDesktop after completion of level-3 CXD-310	Citrix Certified Expert - Virtualization	3-4 years
	Experience is essential for Level-4 staff. A qualified Level-4 resource should have a minimum of five of experience	CXD-400:		

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Role	Recommended training	Recommended course(s)	Recommended certification	Relevant experience
Architect (Level 4)	architect role for a XenApp and/or XenDesktop environment as well as additional administrative experience with integrated technologies such as application and profile management solutions. The ideal candidate will have served in such a capacity at two or more environments for purposes of product exposure and in at least one environment of over 1,200 concurrent users. A Citrix Certified Expert (CCE) certification or comparable training and experience should be a prerequisite of the role.	CXD-400: Designing App and Desktop Solutions with Citrix XenApp and XenDesktop after completion of level-3 CXD-310	Citrix Certified Expert - Virtualization	5+ years

The following table provides guidance on the recommended number of support staff.

Role	Small Environment: Sites: 1; Users: <500; Images: 1-2	Mid-size Environment: Sites: 1-2; Users: 1000-5000; Images: 3-5	Large Environment: Sites: 2+; Users: >5000; Images: 5+
Help Desk (Level-1)	3	5-10	15-20
Operator (Level-2)	1-2	2-3	4-5
Implementer (Level-3)	1	1-2	2-3
Architect (Level-4)	1	1	1-2

> **注意**
>
> This table should only be used as a baseline. Support staffing decisions should be evaluated against the defined requirements, projected workloads, and operational procedures of an organization. Multiple levels can be combined, for example there may be insufficient design projects to have a dedicated architect role or a more senior member of the Citrix team can act as an Operator and Implementer.

General Support Tools: The following table details tools that should be made available to all support levels.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Tools	Details
Ticket Management System	Used to document customer information and issues. A typical ticket management system provides the following functionality: • Monitoring the queue of tickets. • Setting a limit on the number of open tickets. • Establishing thresholds such as how long a certain type of ticket should take to be answered. • Identifying a group of users or individuals who require higher priority assistance. Informing the user when their ticket is open, updated, or closed. • Provide an internal knowledge base for the support professionals to search for known resolved issues.
Call Scripts	The first contact help desk personnel should have documented scripts to ensure that all relevant data is captured while the user is on the phone. This practice also assists in proper triage and allows the next support level to perform research prior to customer contact. A sample call script is provided for reference.
Remote Assistance Tools	Remote assistance tools are useful when troubleshooting user issues. Support technicians and administrators can remotely observe a user's actions.
Knowledge Base	Documentation should be created and maintained in a knowledge base or library of known issues. Articles should be searchable for quick recovery. Knowledge bases help support staff to quickly resolve known issues and reduce the need to perform time consuming research.

The following table provides recommendations on the Citrix support tools that should be made available to each support level.

Tool	Description	Products				Support Level			
		XenDesktop	XenApp	Provisioning Services Console	XenServer	L1	L2	L3	L4
Citrix Director	Citrix Director provides an overview of hosted desktops and application sessions. It enables support teams to monitor and troubleshoot issues.	X	X			X	X	X	X
Citrix Studio	Citrix Studio enables administrators to								

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	perform configuration as well as maintenance tasks for a XenApp and XenDesktop site and associated virtual desktops or hosted applications.	X	X			X	X	X	X
Citrix Insights Services	Run from a single Citrix Delivery Controller to capture key data points and CDF traces for selected computers followed by a secure and reliable upload of the data package to Citrix Technical Support for escalation.	X	X	X	X			X	X
HDX Monitor	HDX Monitor is a tool to validate the operation of the Citrix ICA/HDX stack of a user session. HDX Monitor provides information about client capabilities, network performance/activity, session settings and many more items.	X	X			X	X	X	X
Provisioning Services Console	The Provisioning Services Console enables administrators to perform configuration and maintenance tasks for a Provisioning Services farm.			X				X	X

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenCenter	XenCenter enables administrators to perform configuration and maintenance tasks for a XenServer Resource Pool.				X			X	X

Administrators can utilize Citrix Insight Services to simplify the support and troubleshooting of the Citrix environment. Citrix Insight Services is run locally to collect environment information. Online analysis capabilities analyze that information and provide administrators recommendations based on their Citrix environment and configuration. Additional information regarding Citrix Insight Services can be referenced in the Citrix Support article CTX131233 - FAQ: Citrix Insight Services.

A full list of the available tools provided by Citrix Support to assist with troubleshooting can be referenced in Citrix Supportability Pack.

The following call script can be used as an initial baseline for a Citrix Help Desk team. Citrix Consulting recommends reviewing this sample call guide and adding any environment specific details that may need to be collected.

1. **What is the name and location of the user?**
   This question will identify if the user is accessing the environment from an external or internal network location.
2. **Is the problem always reproducible?**
   If it is a Yes, get the exact reproduce steps. This question is very important for the support team to troubleshooting an issue.
3. **Do any other users at the site/location experience the same issue? Can they have a colleague logon from same and/or different workstation?**
   These questions help to determine if this is a workstation issue or a user issue.
4. **What type of endpoint device is the user utilizing? (Corporate device, BYOD, thin client, pc, laptop, etc.)**
   This question will help determine if the issue is related to the user's endpoint.
5. **What is the Citrix Receiver version and connection information?**
   This question will verify if the user is using the right version of Receiver (the latest Receiver version or the version standardized by the company).
6. **Can the user see the StoreFront authentication page?**
   This question helps to identify network issues.
7. **What is the name of the application (or virtual desktop) the user is attempting to use? Does the user see the appropriate application or desktop icon on the StoreFront site?**
   These questions help to determine if there is an issue with user access and/or group membership.
8. **Does the application (or desktop) launch when the icon is selected? Does the application logon screen appear (if applicable)?**
   These questions help to determine if a connection is made into the Citrix XenDesktop infrastructure.
9. **Can the user authenticate into the application (if applicable)? Does the issue occur after the application is launched?**
   This question helps to determine if the issue is with the application rather than the application delivery infrastructure.
10. **What is the specific error seen (if applicable)?**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

This question identifies the specific error. The user should be requested to provide a screenshot, if available.

Each support level must be provided with sufficient rights to effectively perform their role. The following tables provide guidance on the recommended privileges per support level.

Administrator role	Support Level
Help Desk Administrator	Level-1
Full Administrator	Level-2
Full Administrator	Level-3
Full Administrator	Level-4

For further information about delegated rights within a XenApp/XenDesktop Site, please refer to Citrix Product Documentation - XenApp and XenDesktop Delegated Administration.

Administrator Role	Support Level
N/A	Level-1
Site Administrator	Level-2
Farm Administrator	Level-3
Full Administrator	Level-4

For further information about delegated rights within a Provisioning Services Site, please refer to Citrix eDocs - Provisioning Services Managing Administrative Roles.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Administrator Role	Support Level
N/A	Level-1
N/A	Level-2
Local Administrator on StoreFront Server	Level-3
Full Administrator	Level-4

Users with local administrator rights have access to view and manage all objects within StoreFront or Web Interface. These users can create new sites and modify existing ones.

Administrator Role	Support Level
N/A	Level-1
N/A	Level-2
Administrator	Level-3
Administrator	Level-4

By default, the account used during the installation of the license server becomes the administrator for the console. Often the accounts used for the installation are not the intended accounts for the regular administration tasks. For the steps on how to change the default administrator, please reference CTX135841 - How to Change the Default Administrator for the Citrix Licensing Server Version 11.10. All users created through this process are full administrators of the Citrix License Server.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Administrator Role	Support Level
N/A	Level-1
Virtual Machine Operator	Level-2
Pool Administrator	Level-3
Full Administrator	Level-4

For further information about delegated rights within a XenServer Resource Pool, please refer to XenServer 7.0 Administrators Guide (see chapter Role Based Access Control).

This section defines routine operations for the Citrix environment that help to improve stability and performance.

The Citrix Support Team should perform regular operations and maintenance tasks to ensure a stable, scalable Citrix environment. Each operation is categorized by the associated component of the solution as well as the frequency of the operation (ongoing, daily, weekly and yearly). Tasks have been aligned to the roles described within Decision: Support Responsibilities and Skill Set.

If the administrators performing operations are the same the support team, then the designations are linked as follows:

- Level 2 Support = Operators
- Level 3 Support = Implementers

The following table outlines the tasks that should be performed by the Citrix Support Team on a daily basis.

Component	Task	Description	Responsible
Generic	Review Citrix Director, Windows Performance Monitor, Event Log, and other monitoring software alerts	Check for warnings or alerts within Citrix Director, event logs, or other monitoring software. Investigate the root cause of the alert if any. **Note**: A computer and monitor can be set up to display the Citrix Director dashboard to create a Heads Up Display for the Citrix department. This ensures the status of the environment is clearly visible. Monitoring recommendations for XenDesktop and XenApp 7.x are included in the Monitoring section of the VDI Handbook.	Operators
		Verify all scheduled backups have been completed successfully.	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	Task	Description	Responsible
		• User data (user profiles/home folders) • Application data	
Generic	Verify backups completed successfully	• Citrix databases • StoreFront configuration • Web Interface configuration • Provisioning Services vDisks (virtual desktops and application servers) • XenServer VM/Pool metadata (or equivalent for other hypervisors) • Dedicated virtual desktops • License files	Operators
Generic	Test environment access	Simulate a connection both internally and externally to ensure desktop and application resources are available before most users log on for the day. This should be tested throughout the day and may even be automated.	Operators
XenApp and XenDesktop	Virtual machine power checking	Verify that the appropriate number of idle desktops and application servers are powered on and registered with the Delivery Controllers to ensure availability for user workloads.	Operators
XenApp and XenDesktop	Perform incremental backup of Citrix related databases	Perform incremental-data backups of the following Citrix databases: • Site Database • Configuration Logging Database • Monitoring Database	Operators, Database team (if Citrix environment is using a shared SQL)
Provisioning Services	Check Citrix Provisioning Server utilization	Check the number of target devices connected to the Citrix Provisioning Servers and balance the load across servers, if required.	Operators
Provisioning Services	Perform incremental backup of Citrix PVS database	Incremental backup of Citrix Provisioning Server database hosted on SQL Server infrastructure.	Operators, Database team (if Citrix environment is using a shared SQL)

The following table outlines the tasks that should be performed by the Citrix Support Team on a weekly basis.

Component	Task	Description	Responsible
Generic	Review latest hotfixes and patches	Review, test, and deploy the latest Citrix hotfixes and ascertain whether the Delivery Controllers and Server-Based OS / Desktop-Based OS virtual machines require them. **Note**: Any required hotfixes should be tested using the recommended testing process prior to implementation in production.	Operators, Implementers (review process)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	Task	Description	Responsible
Generic	Create Citrix environment status report	Create report on overall environment performance (server health, resource usage, user experience) and number of Citrix issues (close rate, open issues, and so on).	Operators
Generic	Review status report	Review Citrix status report to identify any trends or common issues.	Implementers, Architect
Generic	Maintain internal support knowledge base	Create knowledge base articles and issue resolution scripts to address Level-1 and Level-2 support requests. Review knowledge base articles and issue resolution scripts for accuracy, compliance, and feasibility.	Operators (Level-2 requests), Implementers (Level-3 requests, and review process)
XenApp and XenDesktop	Check Configuration Logging report	Confirm that Citrix site-wide changes implemented during the previous week were approved through change control.	Auditors
XenApp and XenDesktop	Perform full backup of Citrix related databases	Perform full-data backups of the following Citrix databases: • Site Database • Configuration Logging Database • Monitoring Database	Operators, Database team (if Citrix environment is using a shared SQL)
Provisioning Services	Check storage capacity (only prior to updating a vDisk)	Review storage utilization, used and free storage space, for vDisk store and each vDisk. **Note**: Lack of space within the vDisk repository will be an issue only when the vDisks are updated using versioning or when a vDisk is placed in private mode during an update procedure. Storage utilization within vDisk should also be investigated. For example, a 20GB vDisk may only have 200MB of free storage. If the vDisk itself is limited for storage, then it needs to be extended. Citrix does not support resizing of a VHD file. Refer to the Microsoft link Resize-VHD for information on resizing a VHD file.	Operators
Provisioning Services	Perform vDisk updates (as necessary)	Perform a full backup of the vDisk before implementing any updates. Update the master vDisk image files and apply the following: • Windows software updates and patches • Operating system and application changes • Anti-virus pattern and definitions updates **Note**: Updates should be tested using the recommended testing process prior to implementation in production.	Auditors
Provisioning Services	Check auditing reports	Review the Citrix Provisioning Services auditing Logs. **Note**: Provisioning Server auditing is off by default and can be enabled to record configuration actions on components within the Provisioning Services farm. To enable auditing refer to the Citrix production documentation article, Enabling Auditing Information.	Operators, Database team (if Citrix environment is using a shared SQL)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	Task	Description	Responsible
Provisioning Services	Backup of Citrix PVS database	Backup of Citrix Provisioning Server database hosted on SQL Server infrastructure.	Citrix environment is using shared SQL)

The following table outlines the tasks that should be performed by the Citrix Support Team on a monthly basis.

Component	Task	Description	Responsible
Generic	Perform capacity assessment	Perform capacity assessment of the Citrix environment to determine environment utilization and any scalability requirements. **Note**: Recommendations for performing a capacity assessment are included in Decision: Capacity Management in the Monitoring section below.	Architect

The following table outlines the tasks that should be performed by the Citrix Support Team on a yearly basis.

Component	Task	Description	Responsible
Generic	Conduct Citrix policy assessment	Review Citrix policies and determine whether new policies are required and existing policies need to be updated.	Implementers
Generic	Review software upgrades	Review and assess the requirement for new Citrix software releases or versions.	Implementers
Generic	Business Continuity Plan (BCP)/ Disaster Recovery (DR) test	Conduct functional BCP/DR test to confirm DR readiness. This plan should include a yearly restore test to validate the actual restore process from backup data is functioning correctly.	Architect
Generic	Perform application assessment	Review the usage of applications outside and within the Citrix environment. Assess the validity of adding additional applications to the Citrix site, removing applications that are no longer required, or upgrading the applications to the latest version.	Architect
Provisioning Services	Archive audit reports	Perform an archive of the Citrix Provisioning Server Audit Trail Information for compliance requirements.	Auditors

The location of backups directly effects the recovery time and reliability of the Citrix environment. It is recommended to store backups of critical data both onsite and at an offsite location. If offsite backups are not possible due to costs

© 1999-2017 Citrix Systems, Inc. All rights reserved.

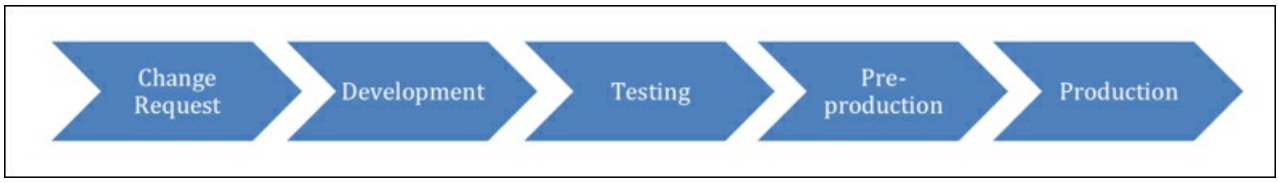
associated or sensitivity of the data, backups should be placed at separate physical locations within the same datacenter.

Each backup option is discussed further below.

- Onsite Backups – Onsite backups should be located on a storage device in the datacenter that will allow the data to be recovered quickly in the event of a failure. Onsite backups are ideal for issues that only affect a small subnet of hardware in the datacenter. Backups can also be stored on a cold storage solution such as tape. While this medium is slower to recover from, it provides additional protection since it is only active during the backup process.
- Offsite Backups – Although the time to recover is much higher, offsite backups provide additional protection in the event of a disaster. Offsite backups may require transferring data over the Internet to a third party provider or they are created onsite and then transported to a remote location on storage mediums such as tape. It is typical to put a limited number of backups offsite. For example, one backup a week or month.

Regular updates and maintenance are an everyday part of IT operations. Standard processes must be followed to ensure updates do not negatively impact the production environment. This includes maintaining a dedicated testing infrastructure where modifications can be validated prior to being implemented in production.

Since changes to Citrix infrastructure can impact thousands of virtual desktop and application users, multi-phase testing is critical for the reliability and performance of the environment. As such, the process for testing should resemble the following:



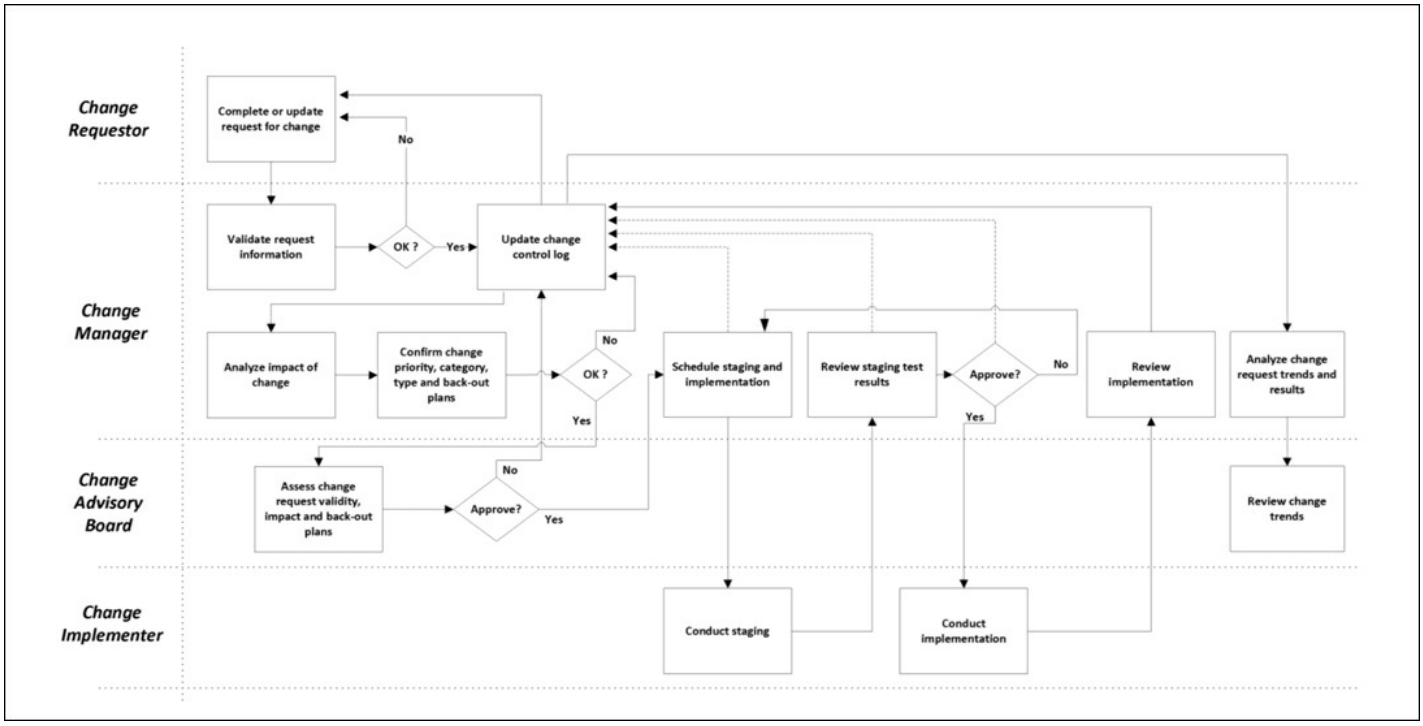
- Development - The development infrastructure exists outside of the production network. Typically, it consists of short-lived virtual machines whose configuration matches production as closely as possible. The purpose of the development phase is to provide change requestors a non-production environment to perform proof of concepts, determine integration requirements and perform iterative testing as part of a discovery phase. Proposed changes should be documented so they can be applied in the test phase.
- Testing - The test environment is a standalone 1:1 copy of the production infrastructure and is used to confirm that the proposed changes can be easily repeated prior to the preproduction staging environment. The changes made should follow documentation from the development stage. If testing fails within the testing stage, the architect must determine the severity of failure and determine whether minor updates to documentation is sufficient or a full development cycle is needed.
- Pre-production - The pre-production environment should mimic the current production environment. The goal of staging is to implement the proposed changes with little risk or uncertainty. It is expected that any changes made to the staging infrastructure have been tested and documented for repeatability. There should not be any iterations or adjustments required within this phase. During this phase and within this environment User Acceptance Testing (UAT) should be performed.
- Production - The production environment is a fully redundant and scalable solution designed for normal usage by end users. There should be minimal changes to the environment. If possible, all approved changes should be rolled out in stages to the production environment. This process is known as a staged rollout and mitigates risk by allowing changes to be rolled back, if necessary, without impacting the entire environment.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Standardized processes that manage changes throughout a system's lifecycle are necessary to ensure consistent and accountable performance. The following change control leading practices should be considered.

- Use a change control window so that all applicable parties know when there might be downtime. Make sure that all teams are represented in the Change Advisory Board (CAB).
- Every change should have a roll back plan.
- If a change fails have a "hot wash" to determine what went wrong.
- Always use an automated change control system so that support staff can quickly and easily identify changes.
- When available, ensure configuration logging is enabled to track any changes made to the Citrix environment.

The change control process should be closely followed starting with a change request. A change request form should be filled out detailing changes requested, reasons for the change, and intended timeframes for the action. This is then reviewed and edited if required by a Change Manager and advisory board. When the change request has gone through the entire change approval process it is given to a change implementer who stages the change for testing, and finally conducts the implementation in production. A sample change control process, including detailed steps, is provided in the diagram below:



The process is as follows:

1. The Change Request (CR) form is completed by any person requesting a change.

2. After appropriate manager approvals have been acquired, the CR is forwarded to the appropriate Change Manager(s).

3. The Change Manager validates the CR for completeness and logs the CR information into the Change Control Log for tracking. Incomplete change requests are returned to the requestor for update and re-submission.

4. The Change Manager assesses the impact of the change in conjunction with subject matter experts and/or managers of

© 1999-2017 Citrix Systems, Inc. All rights reserved.

the teams associated/affected by this change.

5. The Change Manager works with the associated/affected teams as well as the change requestor in order to confirm the priority, category and type of the change as well as the proposed rollback plan.

6. If the change is approved by the Change Manager, the CR is forwarded to the CAB for approval. If the change is rejected, the Change Control Log is updated with the current status as well as the reason of the rejection and the CR is send back to the requestor.

7. The CAB reviews and validates the change in detail, and discusses and evaluates purpose, reasons, impact, cost and benefits. Each board member represents their department and provides guidance on the change requests. The CAB also reviews multiple requests to coordinate implementations and "package" requests into a single release schedule.

8. Upon approval the change is sent back to the Change Manager to schedule the change for implementation into the staging environment.

9. The change is implemented and tests are conducted. The results are sent back to the Change Manager.

10. If the staging implementation and testing are successful, the change is scheduled for production implementation. In case the staging phase was not successful another staging iteration will be conducted.

11. If possible, the change is rolled out in stages to the production environment. This process is known as a staged rollout and mitigates risk by allowing changes to be rolled back, if necessary, without impacting the entire environment. A rollback plan should be in place if there is an issue implementing a change in the production environment.

12. The Change Manager reviews the implementation and finally updates the Change Control Log.

13. On a periodic basis, the Change Manager reviews the Change Control Log to identify trends on type, frequency and size of changes and forwards the results to the CAB for review. In an emergency, the processes may be expedited. Should an issue be declared an emergency, a change request form is still filled out and delivered to the appropriate change management representative. When approved, the requested change is immediately implemented and the advisory board notified.

Availability testing is focused on ensuring resources are still available in the instance of a component failure. These tests are essential to ensuring users always have access to business critical resources. The testing should be conducted during nonbusiness hours or during a scheduled maintenance weekend when appropriate notice has been given to end users to make them aware if any unforeseen issues arise.

The following is a list of the key components that should be tested on a regular basis.

- StoreFront – StoreFront should be load balanced and health checked by a NetScaler or other load balancing device. To validate its configuration, all but one of the StoreFront servers should be shutdown. This will validate that the load balancing device is detecting the failure and directing users to the functioning server.
- SQL – SQL Server should be in a high availability configuration. To validate the configuration, the primary SQL server should be taken offline and then the Citrix Studio console should be opened. Since Citrix Studio will not be accessible without a functioning SQL server, it will validate that the SQL server failover mechanisms are functioning properly.
- Delivery Controllers - Resources deployed should be configured with a list of multiple Delivery Controllers. If one is made unavailable, desktops and application hosts will automatically establish a connection to another server in the list. To validate this, shutdown one of the Delivery Controller hosts and determine if the resources initially connected to it

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

automatically register to another server. This can be determined by viewing the registration status of the resources inside Citrix Studio.

Prerequisites and configuration requirements:

- Hypervisor, XenApp, and XenDesktop services are up and running.
- At least two PVS servers are installed and configured, providing the streamed disk image.
- Resilient networking and storage infrastructure with multiple links to each server.
- Test users are active on the XenApp or XenDesktop machines.

Steps	Expected Results
PVS Server Outage • Shutdown one of the Provisioning Servers. • Validate PVS continues to function. • Restart PVS Server. • Validate connections rebalance between PVS Servers. • Try the other(rest) PVS server(s) one by one.	• Existing XenApp/XenDesktop machines connect to another PVS server. • There is limited to no impact to the users utilizing that server. • New XenApp/XenDesktop machines can be booted and start correctly. • SCOM reports that the PVS server is down/not available. • Live connections are rebalanced between both PVS servers once both PVS servers are made available again.
PVS Bond Disruption: Disable / unplug a NIC in the PVS Streaming Bond on the PVS server.	Provisioning Server continues to stream over remaining NICS in PVS Streaming Bond.
SQL Server PVS Database Mirror Failover • Admin logs on to Principle SQL Server. • Initiate failover of PVS database. • Validate PVS continues to function. • Initiate failback of PVS database. • Validate PVS continues to function.	PVS continues to function.
SQL Service Outage • Admin reboots both Principle & Mirror SQL Servers simultaneously. • Validate PVS continues to function, but that administration is not possible. • Wait for the SQL Server to come back online. • Validate PVS administrative functions are once again possible.	• PVS continues to function. • PVS administrative functions are no longer available. • PVS administrative functions are available once the SQL services are restored.

Prerequisites and configuration requirements:

- Hypervisor, XenDesktop, and StoreFront services are up and running.
- Network and storage services available.
- Provisioning Services is providing the streamed disk images.
- Test users are active on the virtual machines.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- SQL (Mirroring) and XenDesktop servers are up and running.
- Ensure multiple StoreFront servers are running.
- NetScaler load balancing services.

Steps	Expected Results
XenApp/XenDesktop 7.x Delivery Controller Citrix Broker Service Outage: • Stop the Citrix Broker Service on one of the Delivery Controller servers. • Validate virtual desktops or applications can still be enumerated and launched. • Start the Citrix Broker Service on the Delivery Controller server. • Shutdown one of the Desktop Controllers. • Validate virtual desktops or applications can still be enumerated and launched. • With a desktop launched, determine which Controller owns the host connection. Shut the Controller down and verify that another Controller takes over the session. **Note**: This should be done during the maintenance window. Once complete, the VDI resources should be rebooted so the VDAs are evenly distributed across all controllers.	• StoreFront correctly identifies service as being unavailable and redirects connections to remaining Delivery Controller. • Desktops continue to be enumerated and launch successfully. • Launched desktop can be supported if a hosting Controller goes down.
SQL Server Database Mirror Failover: • Admin logs on to principle SQL Server. • Initiate failover of XenApp/XenDesktop database. • Validate XenApp/XenDesktop continues to function.	• The database should failover and the Citrix Studio should pick up the failover database with no issues. • Existing sessions are not impacted. • New sessions are possible. • Administrative functions are possible.
SQL Service Outage: • Admin restarts both principle & mirror SQL Servers simultaneously. • Validate XenApp/XenDesktop continues to function, but that administration is not possible. Wait for the SQL Service to come back online. • Validate administrative functions are once again possible.	• Existing XenDesktop sessions are not impacted • Recently used applications, hosted shared desktops and assigned VDI can be accessed due to local host cache. • XenDesktop Administrative functions are not possible • XenDesktop Administrative functions are possible once SQL service is available.

Prerequisites and configuration requirements:

- Citrix Licensing Server up and running (with valid licenses installed).
- Hypervisor, XenApp/XenDesktop and StoreFront services are up and running.
- Users are active on the Server OS or Desktop OS machines.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Steps	Expected Results
Server: • Shutdown the Citrix Licensing server. • Reboot an existing Server OS machine. • Logon to the Citrix StoreFront and launch a published application. • Reboot an existing Desktop OS machine. • Logon to the Citrix StoreFront and launch a virtual desktop.	• License Server connectivity error posted in Event Log. • Provisioned Server OS boots successfully. • Users are able to launch published applications. • Provisioned Desktop OS boots successfully. • User is able to launch a virtual desktop. • Administrators will have 30 days grace to recover the Citrix Licensing Server.

By having an in-depth understanding of current and expected behavior of the Citrix environment and its components, administrators are better equipped to discover an issue before it affects the user community. Furthermore, the data tracked during normal operations is beneficial for trending and capacity planning. This section defines the monitoring recommendations for a Citrix environment as well as some recommended tools.

Depending on the size and scope of the XenApp and XenDesktop solution, it can take considerable time for an administrator to verify services, events, capacity and performance. It is advisable for administrators to investigate automation into their monitoring strategy.

Citrix includes a cloud-hosted monitoring solution called Smart Check (https://smart.cloud.com), which is a free service for any organization with active Citrix Customer Success Services: Select offering. Smart Check executes the following in a XenApp and XenDesktop environment:

- Site Health Checks – Evaluates all services with the XenApp and XenDesktop site
- Apps and Desktops Checks = Verifies delivery group availability
- Update Checks – Tracks and recommends patches and hotfixes for delivery controllers
- LTSR Checks – Verifies the delivery controllers and VDAs within the site comply with LTSR versions.
- Custom Checks – Allows administrators to import their own custom scripts to test across their XenApp and XenDesktop site.

A list of the current Smart Check capabilities, review the Smart Check documentation.

Monitoring the performance of the overall environment is crucial towards making sure all components are available and performing effectively to ensure users have a high quality experience.

Different components within the overall solution require monitoring of unique metrics with appropriately set thresholds. The metrics and thresholds presented are based on real world experience but may not apply to all environments. Organizations will need to perform their own baselining, validity testing and validation before implementing within a production environment.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

> **注意**
>
> Some hypervisors, such as VMware vSphere and Hyper-V, provide specific performance counters for tracking CPU and Memory utilization within virtual machines (i.e. “VM Processor \ % Processor Time”). These performance counters should be used in addition to the general counters listed below.

These performance counters should be used to monitor the key performance metrics of the Citrix infrastructure, application servers, and virtual desktops.

Metric	Description	Warning (Yellow)	Critical (Red)	Troubleshooting/Remediation
Processor - % Processor Time	% Processor Time is the percentage of elapsed time that the processor spends to execute a non-Idle thread. It is calculated by measuring the duration of the idle thread is active in the sample interval, and subtracting that time from interval duration. (Each processor has an idle thread that consumes cycles when no other threads are ready to run). This counter is the primary indicator of processor activity, and displays the average percentage of busy time observed during the sample interval. It is calculated by monitoring the time that the service is inactive and subtracting that value from 100%.	80% for 15 minutes	95% for 15 minutes	Identify the processes/services consuming processor time using Task Manager or Resource Monitor. If all processes/services work within normal parameters and the level of CPU consumption is an expected behavior it should be considered to add additional CPU resources to this system in the future. If a process/service can be identified which works outside normal parameters, the process should be killed. Please note that killing a process can cause unsaved data to be lost.
System - Processor Queue Length	Processor queue length is the number of threads in the processor queue. Unlike the disk counters, this counter shows ready threads only, not threads that are running. There is a single queue for processor time even on computers with multiple processors. Therefore, if a computer has multiple processors, you need to divide this value by the number of processors servicing the workload. A sustained processor queue of less than ten threads per processor is normally acceptable, dependent of the workload.	5 (per core) for 5 minutes or 6 (per core) for 15 minutes	10 (per Core) for 10 minutes or 12 (per core) for 30 minutes	A long CPU queue is a clear symptom of a CPU bottleneck. Please follow the steps outlined for counter “Processor - % Processor Time”.
				Identify the processes/services

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Metric	Description	Warning (Yellow)	Critical (Red)	Troubleshooting/Remediation
Memory – Available Bytes	Available memory indicates the amount of memory that is left after nonpaged pool allocations, paged pool allocations, process' working sets, and the file system cache have all taken their piece.	<30% of total RAM or 20% of physical memory over 6 minutes	<15% of total RAM or 5% of physical memory over 6 minutes	Manager or Resource Monitor. If all processes/services work within normal parameters and the level of memory consumption is an expected behavior it should be considered to add additional memory to this system in the future. If a process/service can be identified which works outside normal parameters, the process should be killed. Please note that killing a process can cause unsaved data to be lost.
Memory – Pages/sec	Pages/sec is the rate at which pages are read from or written to disk to resolve hard page faults.	>10	>20	A high value reported for this counter typically indicates a memory bottleneck, except if "Memory – Available Bytes" reports a high value at the same time. In this case most likely an application is sequentially reading a file from memory. Please refer to Microsoft Knowledge Base article KB139609 – High Number of Pages/Sec Not Necessarily Low Memory for further information.
Paging File - %Usage	This is the percentage amount of the Page File instance in use.	>40% or 80% over 60 minutes	>70% or 95% over 60 minutes	Review this value in conjunction with "Memory - Available Bytes" and "Memory - Pages/sec" to understand paging activity on the affected system.
LogicalDisk/PhysicalDisk - % Free Space	% Free Space is the percentage of total usable space on the selected logical disk drive that is free.	<20% of physical disk or 20% reported after 2 minutes	<10% of physical disk or 15% reported after 1 minute	Identify which files or folders consume disk space and delete obsolete files if possible. In case no files can be deleted, consider increasing the size of the affected partition or add additional disks.
LogicalDisk/PhysicalDisk - % Disk Time	% Disk Time marks how busy the disk is.	>70% consistently or 90% over 15 minutes	>90% consistently or 95% over 15 minutes	Identify the processes / services consuming disk time using Task Manager or Resource Monitor. If all processes/services work within normal parameters and the level of disk consumption is an expected behavior it should be considered to move the affected partition to a more capable disk subsystem in the future.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Metric	Description	Warning (Yellow)	Critical (Red)	Troubleshooting/Remediation
				identified which works outside normal parameters, the process should be killed. Please note that killing a process can cause unsaved data to be lost.
LogicalDisk/PhysicalDisk – Current Disk Queue Length	Current disk queue length provides a primary measure of disk congestion. It is an indication of the number of transactions that are waiting to be processed.	>=1 (per spindle) consistently or 3 over 15 minutes (_Total)	>=2 (per spindle) consistently or 10 over 30 minutes (_Total)	A long disk queue length typically indicated a disk performance bottleneck. This can be caused by either processes/services causing a high number of I/Os or a shortage of physical memory. Please follow the steps outlined for counter "LogicalDisk/PhysicalDisk - % Disk Time" and counter "Memory – Available Bytes"
LogicalDisk/PhysicalDisk – Avg. Disk Sec/Read – Avg. Disk Sec/Write – Avg. Disk Sec/Transfer	The Average Disk Second counters show the average time in seconds of a read/write/transfer from or to a disk.	>=15ms consistently	>=20ms consistently	High disk read or write latency indicates a disk performance bottleneck. Systems affected will become slow, unresponsive and application or services may fail. Please follow the steps outlined for counter "LogicalDisk/PhysicalDisk - % Disk Time"
Network Interface – Bytes Total/sec	Bytes Total/sec shows the rate at which the network adaptor is processing data bytes. This counter includes all application and file data, in addition to protocol information, such as packet headers.	<8MB/sfor 100 Mbit/s adaptor <80 MB/s for 1000 Mbit/s adaptor or 60% of NIC speed inbound and outbound traffic for 1 min.	70% of NIC speed inbound and outbound traffic for 1 min.	Identify the processes / services consuming network using Task Manager or Resource Monitor. If all processes/services work within normal parameters and the level of bandwidth consumption is an expected behavior it should be considered to move the respective process/service to a dedicated NIC (or team of NICs). If a process/service can be identified which works outside normal parameters, the process should be killed. Please note that killing a process can cause unsaved data to be lost.

These performance counters are specific to the Delivery Controllers.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Metric	Description	Warning (Yellow)	Critical (Red)	Troubleshooting/Remediation
Database Avg. Transaction Time	The time on average, in seconds, taken to execute a database transaction. A baseline needs to be established in the environment in order to accurately establish threshold values.	Based on baseline values	Based on baseline values	In case the reported values exceed the baseline response time constantly, a potential performance issue needs to be investigated at the SQL server level.
Database Connected	Indicates whether this service is in contact with its database. (1 is connected; 0 is not connected).	0	0 (for over 30 minutes)	Both values report connectivity issues of the XenDesktop Broker service with the database. In case issues are reported, SQL server and network availability needs to be verified.
Database Transaction Errors/sec	The rate at which database transactions are failing.	None	> 0	Both values report connectivity issues of the XenDesktop Broker service with the database. In case issues are reported, SQL server and network availability needs to be verified.

These performance counters are specific to the StoreFront servers.

Metric	Description	Warning (Yellow)	Critical (Red)
ASP.NET – Request Queued	The number of requests waiting to be processed by ASP. A baseline needs to be established in the environment in order to accurately establish threshold values.	Based on baseline values	Based on baseline values
ASP.NET – Requests Rejected	The number of requests rejected because the request queue was full.	None	> = 1
APP_POOL_WAS\Current Application Pool State\Citrix Receiver for Web	3		
APP_POOL_WAS\Current Application Pool State\Citrix Delivery Services Authentication	3		
APP_POOL_WAS\Cur rent Application Pool State\Citrix Delivery Services Resource	3		
Request response	Regardless it is authentication, enumerate or subscription) should be 3 to 5 seconds (http://www.perftestplus.com/resources/how_fast.pd f		

© 1999-2017 Citrix Systems, Inc. All rights reserved.

These performance counters are specific to the Citrix License Server

Metric	Description	Warning (Yellow)	Critical (Red)	Troubleshooting/Remediation
Citrix Licensing – Last Recorded License Check-Out Response Time	Displays the last recorded license check-out response time in milliseconds.	>2000 ms	> 5000 ms	If the reported values exceed the 5000 ms response time, a potential performance issue needs to be investigated in the Citrix License Server.
Citrix Licensing – License Server Connection Failure	Displays the number of minutes that XenDesktop has been disconnected from the License Server.	> 1 minute	> 1440 minutes	Both values report connectivity issues with the License Server. In case issues are reported, License Server and network availability needs to be verified.

Windows services that are critical to basic server functionality should be automatically monitored to ensure that they are running properly. The following table provides a list of the common Windows services that should be monitored. When any of these services are restarted or stopped a warning (Yellow) or critical (Red) alert should be assigned respectively. The recommended recovery actions for the services listed below are as follows:

- First failure: Restart the Service
- Second Failure: Restart the Service
- Subsequent Failures: Put the server in maintenance mode and investigate the root cause

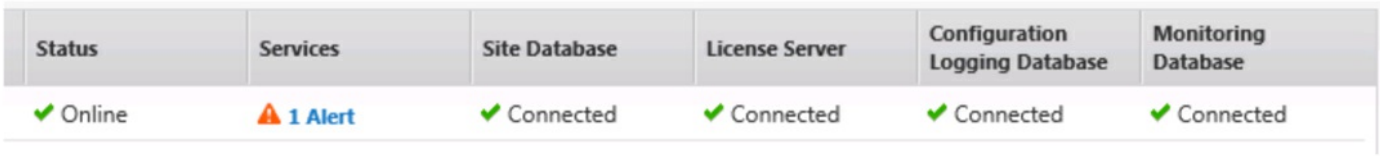
Service	Functionality	Administration Risk
Citrix AD Identity Service	Manages Active Directory computer accounts. Dependencies: WMI Service	Machine Creation Service relies on this service to create virtual machines. Administrators will be unable to create new or modify existing Machine Catalogs. Administrators will be unable to establish new connections to Citrix Studio.
Citrix Broker Service	Manages connections to virtual machines and applications.	If this service is stopped administrators will be unable to make changes to the environment or establish new connections to Citrix Studio. Any existing administrator connections to Citrix Studio can also be terminated. If this service is stopped existing user connections are not affected. No new connections can be established. Users logging into StoreFront will be unable to see any resources available for selection. Once the service is restarted users will need to re-login to StoreFront to establish connections.
Citrix Configuration Logging	Logs administrator activity and configuration changes	If this service is stopped XenApp/XenDesktop will be unable to communicate with the Configuration Logging Database. Administrators will be unable make changes to the

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Service	Functionality	Administration Risk
	deployment.	
Citrix Configuration Service	Stores service configuration information. Dependencies: WMI Service	If this service is stopped administrators will be unable to make changes to the environment or establish new connections to Citrix Studio.
Citrix Delegated Administration Service	Manages configuration of delegated administration permissions.	If this service is stopped XenApp/XenDesktop cannot assign administrative permissions. Administrators will be unable to make changes to the environment or establish new connections to Citrix Studio. Administrators will be unable to establish new connections to Citrix Director and existing sessions within Citrix Director will be interrupted.
Citrix Diagnostic Facility COM Server Service	Manages and controls Citrix diagnostic trace sessions on the system. Dependencies: RPC Service	This service has no impact on the production environment. It is used to generate CDF trace files which aid in troubleshooting issues.
Citrix Environment Test Service	Manages tests for evaluating the state of a XenDesktop Site.	If this service is stopped administrators will be unable to establish new connections to Citrix Studio. Administrators will also be unable to check the status of the Citrix site configuration, machine catalogs, and delivery groups by running the tests under "Common Tasks" in the Citrix Studio administration console.
Citrix Host Services	Manages host and hypervisor connections. Dependencies: WMI Service	Administrators will be unable to create new Machine Catalogs or control virtual machine power settings via Citrix Studio. Administrators will be unable to establish new connections to Citrix Studio. Users may experience issues connecting to virtual desktops when this service is not available. If this service is stopped existing connections are not affected.
Citrix Machine Creation Service	Creates new virtual machines. Dependencies: WMI Service	Administrators will be unable to create new or modify existing Machine Catalogs or establish new connections to Citrix Studio. Administrators will be unable to establish new connections to Citrix Studio.
Citrix Monitor Service	Monitors the FlexCast system.	If this service is stopped XenApp/XenDesktop will be unable to communicate with the Monitoring Database. Citrix Director will be unable to retrieve any data on the environment. Administrators will be unable to establish new connections to Citrix Studio.
Citrix StoreFront Service	Manages deployment of StoreFront.	Administrators will be unable to establish new connections to Citrix Studio.

The Infrastructure pane within the Citrix Director dashboard provides status of the services running on the Delivery Controllers and will provide warning indications if a service or Controller is unavailable. These alerts can be accessed by clicking the Alert hyperlink within the Infrastructure pane.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Status	Services	Site Database	License Server	Configuration Logging Database	Monitoring Database
✔ Online	⚠ 1 Alert	✔ Connected	✔ Connected	✔ Connected	✔ Connected

Service	Functionality	Risk
Citrix PVS PXE Service	Provides the PVS PXE Boot Server functionality. **Note**: Only applicable when PXE boot is used.	On failure of this service target devices may not be able to boot successfully if PXE booting is leveraged.
Citrix PVS Stream Service	Streams contents of the vDisk to the target device on demand.	If this service stopped it will not be possible to stream vDisk images.
Citrix PVS SOAP Service	Provides framework for external or existing solutions to interface with Provisioning services. **Note**: Only impacts console operations. User is unaffected	If this service fails PVS Server to PVS Server communication as well as PVS Console to PVS Server communication is not possible.
Citrix PVS TFTP Service	Provides the TFTP Server functionality. **Note**: Only applicable when TFTP is used.	On failure of this service target devices may not be able to boot if this server is used as TFTP server for the bootstrap.
Citrix PVS Two-Stage Boot Service	Provides the bootstrap functionality for devices booting by means of a BDM ISO file. **Note**: Only when BDM boot partitions are used.	On failure of this service target devices may not be able to boot if a BDM ISO file is used.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Service	Functionality	Risk
Citrix Cluster Join Service	Provides Server Group join services.	This service is started when adding additional StoreFront servers to a Server Group. If this service does not start or is interrupted when this process is initiated the additional server will be unable to join the indicated Server Group and the process will result in an error.
Citrix Configuration Replication	Provides access to Delivery Services configuration information.	This service only exists on the primary StoreFront server of a Server Group. If this service is stopped additional StoreFront servers will be unable to join the Server Group and any changes made to the primary StoreFront server will not be replicated to other servers. This can result in servers within the Server Group being out of sync.
Citrix Credential Wallet	Provides a secure store of credentials. Dependencies: Citrix Peer Resolution Service	If this service is stopped users will be unable to login to access their desktops or applications. Users logged into StoreFront will be unable to launch new application or desktop sessions. Existing application or desktop sessions are unaffected.
Citrix Default Domain Services	Provides authentication, change password, and other domain services.	If this service is stopped users will be unable to login to access their desktops or applications. Users currently logged in will not be affected.
Citrix Peer Resolution Service	Resolves peer names within peer-to-peer meshes.	On failure of this service both the Citrix Credential Wallet and Citrix Subscriptions store are stopped generating the risks associated with those services.
Citrix Storefront Privileged Administration Service	Manages privileged operations on Storefront	
Citrix Subscriptions Store	Provides a store and replication of user subscriptions. Dependencies: Citrix Peer Resolution Service	If this service is stopped Citrix Receiver cannot add, remove, and reposition applications within StoreFront. Users will need to re-add applications and all changes made to their selection of applications within the StoreFront store will not be saved or replicated to other sessions. Original user configuration will be restored once the service is restarted.
World Wide Web Publishing Service	Provides web connectivity and administration through the Internet Information Services Manager. Dependencies: • HTTP • RPC Service	Access to published applications or published desktops will not be available through StoreFront. Users will be unable to resolve the Receiver for Web login page. Users logged into StoreFront will be unable to launch new application or desktop sessions and will need to reenter credentials when the service is restarted. Existing application or desktop sessions are unaffected.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Service	Functionality	Risk
World Wide Web Publishing Service	Provides web connectivity and administration through the Internet Information Services Manager. Dependencies: • HTTP • RPC Service	Access to published applications or published desktops will not be available through Web Interface if the WWW service is not available.

Service	Functionality	Risk
Citrix Licensing Service	Provides licensing services for Citrix products.	Licensing mode changes to grace period when service is stopped or License Server cannot be contacted. If not monitored, functionality of Citrix products will cease after grace period expires.
Citrix Licensing Support Service	This account controls reading the license files and updating strings with license trailers (data dictionary functionality).	None
Citrix Licensing WMI	The Citrix License Management Console collects license data information using the WMI service.	None

Monitoring the Windows Event Log for unknown or critical events can help to proactively discover issues and allow administrators to understand event patterns:

- Licensing - Errors in the Event Log dealing with Remote Desktop licensing should be investigated. This might be a result of the installed Citrix product not being able to contact the Remote Desktop Licensing Server or the Citrix Licensing Server. If errors in the Event Log are not reviewed, users might eventually be denied access because they cannot acquire a valid license.
- Hardware Failure - Any event notification that relates to a hardware failure should be looked at immediately. Any device that has failed will have an impact on the performance of the system. At a minimum, a hardware failure will remove the redundancy of the component.
- Security Warnings - Customers should investigate security warnings or audit failure events regarding failed logons in the security log. This could be an indication that someone is attempting to compromise the servers.
- Disk Capacity - As the drives of a Windows system reach 90% of capacity, an event error message will be generated. To ensure continuous service, customers should poll these event errors. As the system runs out of hard disk space, the system is put at severe risk. The server might not have enough space left to service the requests of users for temporary file storage.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Application / Service errors - Any event notification that relates to application or services errors should be investigated.
- Citrix errors - All Citrix software components will leverage the Windows Event Log for error logging. A list of the known Event Log warnings and errors issued by Citrix components can be found at the following links:
  - Event Codes Generated by PVS
  - XenDesktop 7 - Event Log Messages

It is important to periodically check the Event Viewer for Citrix related warnings or errors. Warnings or errors that repeatedly appear in the logs should be investigated immediately, because it may indicate a problem that could severely impact the Citrix environment if not properly resolved.

In multi-server environments it becomes easier to administer the servers when logs can be collected and reviewed from a central location. Most enterprise grade monitoring solutions provide this functionality. More sophisticated monitoring solutions enable an administrator to correlate event information with other data points such as performance metrics or availability statistics. In case the selected monitoring solution does not provide this functionality the Windows Server 2008 R2 or Windows Server 2012/2012 R2 Event Log subscription feature can be used. This feature allows administrators to receive events from multiple servers and view them from a designated collector computer. Please see Microsoft TechNet article Manage Subscriptions for more information.

XenServer is also capable of sending its logs to a central syslog server. The administrator sets the IP address of the syslog daemon server in the properties of each XenServer in the pool. This configuration allows administrators to capture real-time activity across multiple XenServer hosts. Further information can be found within the XenServer Admin Guide.

In addition to the day-to-day monitoring of system-level metrics, performance metrics should be tracked from a historical perspective to help plan for future growth as more users access the environment.

A baseline of the environment performance should be taken so that it can be compared against performance over time. For example, if a user complains of poor performance, this baseline can be used for comparison purposes to identify if the issues are related to the user load exceeding the capacity of the environment.

An example of baseline performance metrics for capacity management would include historical data for CPU, Memory, and network utilization on the Delivery Controller and application servers or desktops.

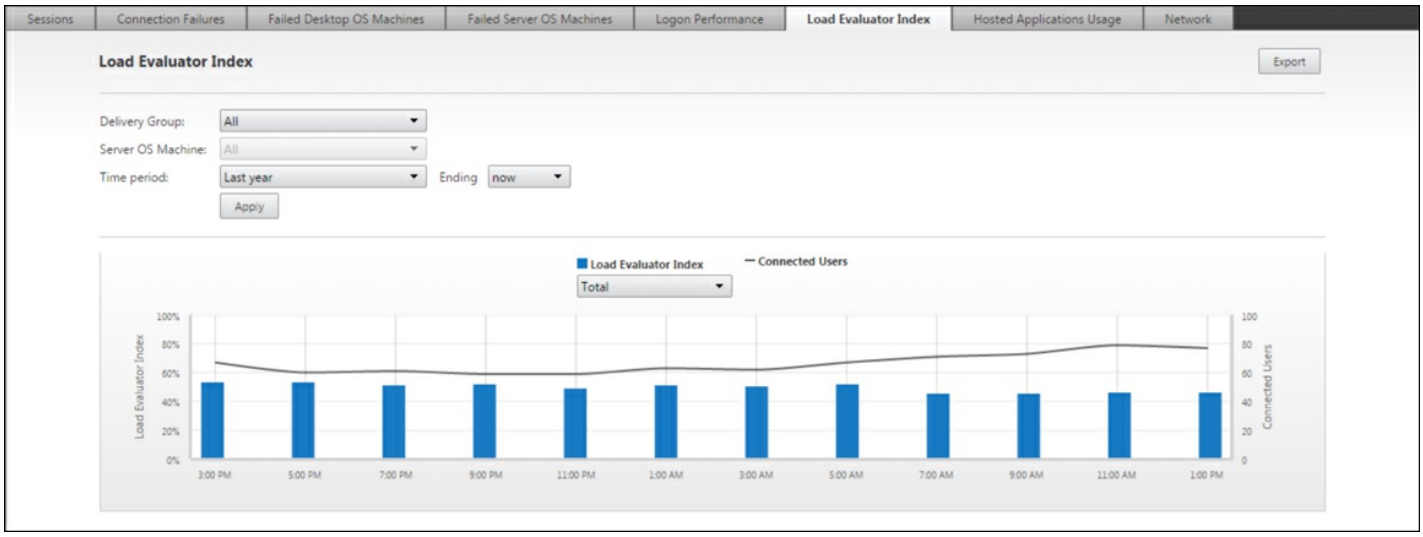
Administrators can utilize the Trends view within Citrix Director to track different parameters of the Citrix XenApp/XenDesktop deployment over time. These parameters can be leveraged for capacity planning of the Citrix environment.

From the Trends view, administrators can see historical data that is broken up into several categories including:

- **Sessions** - Provides the concurrent session usage over time enabling the ability to size the environment appropriately.
- **Connection Failures** - Gives an overview of the different types of connection failures that have occurred across different Delivery Groups.
- **Failed Desktop OS Machines** – Gives an overview of the different problems associated with failures in desktop machines.
- **Failed Server OS Machines** - Gives an overview of the different problems associated with failures in server machines.
- **Logon Performance** – Shows how long it takes for users to log on to their applications and desktops.
- **Load Evaluator Index** – Provides various performance counter-based metrics, including CPU, Memory, and Disk Usage for Server OS machines.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Capacity Management** – Shows utilization of published applications and desktops.
- **Resource Utilization** – Provides information on CPU, Memory and storage resource utilization.
- **Custom Reports** – Allows administrators to create custom historical reports on numerous metrics captured by the system.
- **Hosted Application Usage** – Details all applications published in the site and can provide usage information about each individual applications in detail (concurrent instances, launches, usage duration, and so on). **Note**: Requires XenApp or XenDesktop Platinum licensing
- **Network** – Network analytics provided through NetScaler HDX Insight.



For more information on Citrix Director Trends, please refer to the following.

- Citrix Blogs – Citrix Director: Trends Explained
- Citrix Support – CTX139382 - Best Practices for Citrix Director

The creation of the handbook is a time consuming process and requires real deployment experience across many scenarios. Citrix would like to thank the authors and subject matter experts who contributed to the Citrix VDI Handbook.

© 1999-2017 Citrix Systems, Inc. All rights reserved.