

XenApp 和 XenDesktop 7.8

Jun 17, 2016

新增功能

[XenApp 7.8 和 XenDesktop 7.8 中已修复的问题](#)

[已知问题](#)

[本版本中不提供的功能](#)

[第三方声明](#)

系统要求

技术概述

[概念和组件](#)

[Active Directory](#)

[数据库](#)

[交付方法](#)

[参考体系结构](#)

[设计指南](#)

[实施指南](#)

安装和配置

[准备安装](#)

[使用图形界面进行安装](#)

[使用命令行安装](#)

[使用脚本安装 VDA](#)

[安装 Red Hat Linux VDA](#)

[安装 SUSE Linux VDA](#)

[创建站点](#)

[创建计算机目录](#)

[管理计算机目录](#)

[创建交付组](#)

[管理交付组](#)

[Remote PC Access](#)

[App-V](#)

[AppDisk](#)

[本地应用程序访问和 URL 重定向](#)

[XenApp Secure Browser](#)

[Server VDI](#)

[Personal vDisk](#)

[删除组件](#)

升级和迁移

[升级部署](#)

[迁移 XenApp 6.x](#)

[迁移 XenDesktop 4](#)

安全

[安全注意事项和最佳做法](#)

[委派管理](#)

[智能卡](#)

[传输层安全性 \(TLS\)](#)

[Citrix XenApp 和 XenDesktop 安全性入门](#)

打印

[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](#)

HDX

[Thinwire 兼容模式](#)

[Framehawk 虚拟通道](#)

[HDX 3D Pro](#)

[Flash 重定向](#)

[适用于 Windows 桌面操作系统的 GPU 加速](#)

[Windows Server 操作系统 GPU 加速](#)

[OpenGL Software Accelerator](#)

[音频功能](#)

[网络流量优先级](#)

[USB 和客户端设备注意事项](#)

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](#)

管理

[许可](#)

[区域](#)

[连接和资源](#)

[连接租用](#)

[虚拟 IP 和虚拟环回](#)

[Delivery Controller](#)

[会话](#)

[在 Studio 中使用搜索](#)

[标记](#)

[IPv4/IPv6 支持](#)

[客户端文件夹重定向](#)

[用户配置文件](#)

[Citrix Insight Services](#)

监视

[Session Recording](#)

[配置日志记录](#)

[监视个人虚拟磁盘](#)

Director

[高级配置](#)

[监视部署](#)

警报和通知

委派管理和 Director

安全 Director 部署

为 XenDesktop 7 之前版本的 VDA 配置权限

配置 HDX Insight

对用户问题进行故障排除

SDK 和 API

Monitor Service OData API

FIPS 部署示例

适用于 XenApp 和 XenDesktop 的 Citrix SCOM 管理包

适用于许可证服务器的 Citrix SCOM 管理包

新增功能

Apr 25, 2016

在本文中：

- [关于此版本](#)
- [XenApp 和 XenDesktop 7.8](#)
- [Virtual Delivery Agent \(VDA\) 7.8](#)
- [HDX 技术](#)
- [Session Recording](#)

关于此版本

XenApp 和 XenDesktop 7.8 由新版 Windows 和 Linux VDA 以及多个新版 XenApp 和 XenDesktop 核心组件组成。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 VDA。这样，您就可以使用下面总结的所有最新功能了。有关说明，请参阅[准备安装](#)或[更新部署](#)一文。

- **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，您仍可通过安装（或升级到）新的 VDA 来使用多个最新的 HDX 及其他功能。如果要在非生产环境下测试增强功能，这一点往往会很有用。下面总结了 VDA 中的新增功能以及更新功能。有关说明，请参阅以下文章：

[使用独立 VDA 安装程序的图形界面安装或升级 VDA](#)

[从独立 VDA 安装程序的命令行界面安装或升级 VDA](#)

此版本的 XenApp 和 XenDesktop 下载页面还包括以下软件的更新版本。有关功能信息和安装说明，请参阅组件文档。

- [AppDNA](#)
- [StoreFront](#)
- [Provisioning Services](#)
- [许可](#)

XenApp 和 XenDesktop 7.8

此产品版本包括下列新增功能和增强功能。

- **XenApp Secure Browser**

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。

有关详细信息，请参阅 [XenApp Secure Browser](#) 一文。

- AppDisk

新增的 AppDisk 功能可以将应用程序和应用程序组与主映像的操作系统分开，以便单独对这些应用程序进行管理。现在，您可以将应用程序作为一个独立的实体 (AppDisk) 进行管理。

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。与 Microsoft App-V 不同的是，AppDisk 不会隔离应用程序，而是将它们分开。对于企业来说，变更管理（即更新主映像并测试更新与已安装的应用程序是否兼容）可能会耗费巨大成本。将 AppDNA 与 AppDisk 结合使用即可提供这种变更管理功能。AppDNA 可以发现映像更新可能存在的问题，并提出修正步骤建议。

有关详细信息，请参阅 [AppDisks](#) 一文。

- 改进了对 Microsoft Application Virtualization (App-V) 的支持

现在，您无需在 Studio 中配置和管理 Microsoft App-V 管理和发布服务器，就可以向用户提供 Microsoft App-V 应用程序。您只需直接将 App-V 软件包从网络共享导入到 Citrix Studio 中的应用程序库即可。可以通过交付组从该库向用户提供 App-V 应用程序，就像从主映像或 Microsoft App-V 服务器发现其他应用程序（如果有）一样。可以使用全新的“单管理员”管理方法来代替或补充现有的“双管理员”管理方法。

有关详细信息，请参阅 [App-V](#) 一文。

- Studio 中的应用程序节点

借助 Studio 导航窗格中全新的应用程序节点，可以集中管理所有应用程序，而不管交付组分配情况如何。该节点的一大优势是，可以一次向多个交付组添加应用程序。

在先前版本中，要管理应用程序，您需要在 Studio 导航窗格中选择一个交付组，然后在中间窗格中选择“应用程序”选项卡。现在，您只需在导航窗格中选择应用程序即可。

如果将应用程序添加到多个交付组，您可以指定每个交付组的优先级（最高为 0）；XenApp 或 XenDesktop 将尝试从优先级最高的交付组开始启动该应用程序；如果优先级最高的交付组无法启动，则尝试在第二优先级的交付组中启动该应用程序，依此类推。

“添加应用程序”向导提供了一个下拉菜单，您可以从中选择应用程序来源：计算机目录中创建的计算机、App-V 软件包、已添加至站点的应用程序（可能位于其他交付组）或手动定义的应用程序。

有关详细信息，请参阅[管理应用程序](#)和[创建交付组](#)两篇文章。

- 更新了“创建交付组”向导和“编辑交付组”界面

在先前版本中，“创建交付组”向导会通过一个页面来指定交付组类型（应用程序和桌面、仅限应用程序或仅限桌面）。在此版本中，只有在选择了一个包含所分配桌面操作系统计算机的计算机目录时，才会显示交付类型页面；此时，您可以指定该目录中的计算机是否交付桌面或应用程序。对于所有其他计算机类型，组中的计算机均可交付应用程序和桌面。在某些情况下，您可以稍后通过编辑交付组来更改交付类型。

在先前版本中，“创建交付组”向导会通过一个页面来指定 StoreFront 地址。在此版本中，“创建交付组”向导不再显示

StoreFront 页面。系统将假定您从 Studio 中的 StoreFront 节点提供 StoreFront 服务器地址。您也可以稍后通过编辑交付组来指定 StoreFront 信息。

现在，“创建交付组”向导中的**应用程序**页面提供了一个新的下拉菜单，您可以从中选择要添加到交付组的应用程序的来源：所选计算机目录中创建的计算机、App-V 软件包、已添加至站点的应用程序（可能位于其他交付组）或手动定义的应用程序。

通过**桌面（或桌面分配规则）**页面，您可以指定哪些用户或组可以启动 VM、使用桌面或分配桌面。如果交付组包含的计算机来自静态分配的目录，您还可以指定每个用户的最大桌面数量。

现在，**摘要**页面提供了一个可选的说明字段，该字段显示在 Citrix Receiver 中。您可以稍后通过编辑交付组来更改此说明。

有关详细信息，请参阅[创建交付组](#)和[管理应用程序](#)两篇文章。

- **改进了 Studio 中的标记界面**

标记是指用于标识计算机、应用程序、交付组、策略等项目的字符串。在为项目添加标记后，您就可以定制搜索查询和策略分配，使其仅适用于具有指定标记的项目。

在先前版本中，可以使用一个对话框来添加和编辑标记，并且只能将标记分配给策略。而此版本中的界面功能更强大，使用更方便，并且适用范围更广。

有关详细信息，请参阅[标记](#)一文。

- **要求、安装和配置更新**

除以下项目之外，另请参阅本文的 [Virtual Delivery Agent \(VDA\)](#) 一节以了解 7.8 VDA 和 VDA 安装程序中的变更内容。

更新了 Citrix Director 和 HDX Flash 重定向功能的 Internet Explorer 版本支持。尽管您可以使用“系统要求”一文所述的任一版本，但 Microsoft 支持版本 11，而且 Citrix 也建议使用此版本。

对于 Microsoft .NET Framework 必备项组件，如果计算机安装的是 .NET Framework 4.5.1 或更低版本（或没有安装 .NET Framework），则安装程序将部署 .NET 4.5.2。其中包括 Delivery Controller、Studio、Director 和 VDA。

您可以在运行 Windows Server 2016 Technology Preview 的服务器上安装 Delivery Controller、Studio、Director 和 Windows VDA；但是，此项支持仅为实验功能，不可用于生产环境。

更改了站点创建向导。新的**附加功能**页面列出了一些项目，您可以选择这些项目对站点进行自定义。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。在先前版本中，App-V 信息位于站点创建向导中的一个单独页面上。在此版本中，新增了 AppDisk 与 AppDNA 的集成。

AppDNA 集成：如果您要使用 AppDisk，并且已安装 AppDNA，请启用该功能，以便可以分析应用程序和操作系统、查看兼容性问题并采取修正措施解决这些问题。有关详细信息，请参阅 [AppDisks](#) 一文。

App-V 发布：如果您要使用 App-V 服务器上的软件包中的应用程序，请启用该功能。如果您只想使用网络共享位置上的 App-V 软件包中的应用程序，则不必启用该功能。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](#) 一文。

如果创建的计算机目录使用某个虚拟机管理程序或云服务提供程序中的主映像，则 Studio 会提供一个经过改进的提醒功能，以便在该映像上安装 VDA。如果省略 VDA，则在一段间隔之后，目录创建会失败，此间隔往往会很长。

- **拨打住宅电话**

Citrix 拨打住宅电话功能会定期收集您的系统和产品配置以及性能、错误和其他信息。这些信息会发送至 Citrix Insight Services，以供主动分析和解决。

有关详细信息，请参阅 [Citrix Insight Services](#) 一文。

- 在 Director 中提供了 Citrix Insight Services 链接

您可以从 Director 的“用户”下拉菜单中访问 [Citrix Insight Services](#) (CIS) 以获取更多诊断方面的见解。CIS 中的数据来自拨打住宅电话功能以及 Citrix Scout 等。

- 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。

Virtual Delivery Agent (VDA) 7.8

VDA for Server OS 和 VDA for Desktop OS 7.8 版提供了以下增强功能：

- Linux VDA 1.2 版具有以下功能和增强功能：
 - 适用于 Linux 的 HDX 3D Pro
 - 本地打印支持
 - HDX 实时音频播放和输入
 - 1 级和 2 级语言本地化
- App-V 和 Framewhawk 安装程序选项。VDA 安装程序还提供了两个额外的项目，您可以在图形界面中的功能页面上进行选择，也可以在命令行中进行指定。

Framewhawk。 打开 UDP 端口 3224-3324。Framewhawk 会通过双向 UDP 端口范围（默认为 3224-3324）与 Citrix Receiver 交换 Framewhawk 显示通道数据。有关详细信息，请参阅 [Framewhawk 虚拟通道](#)。

Citrix App-V 发布组件。 如果您要使用 Microsoft App-V 软件包中的应用程序，请安装所需组件。有关详细信息，请参阅 [App-V](#)。

- HDX 3D Pro 产品版本可用性。现在，在所有 XenApp 7.8 和 XenDesktop 7.8 产品版本中，适用于 Windows 桌面操作系统的 VDA 及所有 Linux VDA 均提供了 HDX 3D Pro。而在先前版本中，只有某些产品才支持 3D Pro VDA。Windows 10 当前不支持 HDX 3D Pro。
- KACD .MSI 文件已加入到 VDA 软件包中。该文件是为了支持未来自定义的身份验证功能。先前版本不包括该文件。

HDX 技术

VDA 提供了以下新增或增强的 HDX 技术功能：

- 为 HDX 3D Pro VDI 提供了 Framewhawk 支持。为 Framewhawk 虚拟通道提供了更广泛的 HDX 3D Pro 支持，不仅限于

XenApp，还包括 XenDesktop VDI。这样，用户就可以更灵活地随时随地查看大型 CAD 模型，无论是在企业或公共无线网络中，还是通过高延迟连接在离岸地点工作。有关 Framehawk 的详细信息，请参阅 [Framehawk 虚拟通道](#)。

- **提高了 Framehawk 服务器可扩展性。**内存占用空间平均减少 40% 以上。CPU 效率提升多达 20%。
- **改进了 Framehawk 触控滚动功能。**通过触控输入进行滚动时，宽带效率提升多过 50%。帧速率得以大幅提升，用户体验更流畅。
- **在 Windows 10 VDA 上为 DirectX 窗口模式应用程序提供了 GPU 加速功能。**此版本支持在 Windows 10 VDA 上为 DirectX 10、11 和 12 提供 GPU 加速功能。
- **改进了 Thinwire 设为无损功能**对 Thinwire 的“设为无损”视觉质量进行了更新，与 XenApp 和 XenDesktop 7.6 FP3 相比，锐化模糊图片的速率更高，有损或无损帧检测功能更强。有关 Thinwire 的重要文章，请参阅 [Thinwire 兼容性模式](#)。
- **减少了 Thinwire 的 VDA 内存占用空间。**现在，处理管道的图形编码器在无视频编解码器压缩的情况下运行 Thinwire 时无需再使用中间帧缓冲区。
- **在双跃点会话中提供了客户端名称直通功能。**应用程序可以使用经过更新的 WFAPI SDK 来查询客户端端点名称，并将此信息从任何 Citrix Receiver 传递到已发布的桌面 (XenApp/XenDesktop)，并进而传递到 XenApp 应用程序（一个“双跃点”应用程序）。XenApp 会话中的客户端名称感知功能指的是，用户可以在不同位置之间无缝漫游，如客户端名称发生更改，则系统会通知“双跃点”应用程序，而不必断开会话连接或重新连接会话。有关如何编写符合条件的应用程序的详细信息，请参阅 [WFAPI SDK 文档](#)或咨询您的应用程序 SI/ISV。

Session Recording

Session Recording 7.8.0 支持 Platinum XenApp 7.8 和 XenDesktop 7.8。此功能包括：

- 桌面操作系统 VDA 支持会话录制。在遵守公司政策和法规的前提下，通过任何一种连接录制桌面操作系统 VDA 托管的用户会话屏幕活动。
- 录制远程 PC 上的会话。Remote PC Access 支持会话录制。
- 交付组规则。
- 在规则配置过程中过滤关键字。
- 为不支持的图形模式提供了特殊处理方式。
- 支持 Windows 10。
- 支持 Thinwire 兼容性模式。

有关详细信息，请参阅[会话录制](#)一文。

XenApp 7.8 和 XenDesktop 7.8 中已修复的问题

Mar 17, 2016

以下问题自版本 7.7 起已修复：

- 尝试注册设为土耳其语系统区域设置的 VDA 时可能会失败，并生成 1048 错误。

[#LC2704]

- 如果在相关已发布应用程序正在运行时向用户设备文件夹添加文件，然后尝试从该应用程序中打开该文件，则该应用程序的“打开文件”对话框可能无法显示该文件，即使单击刷新按钮也是如此。

[#LC4073]

- 如果站点数据存储不可用，则即使控制器处于租用连接模式，尝试重新连接时也可能失败。

[#LC4077]

- 尝试从 Citrix Director 终止用户会话中运行的进程时，可能显示以下错误信息：

“操作失败。数据源未响应或报告了一个错误。请查看服务器事件日志了解更多信息。”

[#LC4384]

- 使用 App-V 集成的应用程序可能无法使用正确的工作目录。

[#LC1623]

- 此项修复解决了运行 App-V 应用程序发现时 Citrix Studio 出现内存泄漏的问题。

[#LC2559]

- 关闭 PowerShell 资源时，Citrix Studio 可能无响应。

[#LC3612]

- 在 Citrix Studio 中运行策略建模向导时，报告显示为空白。

[#LC3726]

- 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]

- 执行 Set-BrokerDBConnection 以及相关命令时，Citrix Studio 中的相关配置日志记录条目会列出相应的“主要任务”，并且其状态为“正在进行”，任务完成后，此状态不会更新。

[#LC3479]

- 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]

- 当多个用户在多个 Studio 会话内创建策略时，Desktop Studio 刷新时，创建的最新策略会覆盖之前的策略。

[#LA5533]

- Citrix 策略引擎可能导致服务器无响应。如果发生此问题，Citrix Receiver 和 RDP 的连接请求将失败。

[#LC1817]

- 通过此增强功能，无需单击“查看建模报告”，即可在 Citrix Studio 的中间窗格显示由 Citrix 组策略建模向导创建的建模报告。

[#LC2189]

- 以域用户身份在 AppCenter 的策略节点上运行组策略建模向导时，可能无法显示所应用的用户和计算机策略。

[#LC3284]

- 在 Citrix Studio 中运行策略建模向导时，报告显示为空白。

[#LC3726]

- 在设置为法语系统区域设置的许可证服务器上，Citrix Studio 以西班牙语显示许可模式。

[#LC3450]

- 如果某个服务项目包含两个或更多的租户，则在尝试通过 App Orchestration 2.6 为该服务项目置备更多资源时，可能会失败。

[#LC4170]

- Microsoft 画图会话的录制件无法在 Session Recording Player 中正确播放。

[#604700]

- 播放的多监视器用户设备上录制的会话时出现错误。

[#6051290]

- Session Recording 不支持名为“桌面”的已发布应用程序。此类应用程序无法通过策略控制台添加到录制规则中。

[#588707]

- 您可能会在以下两种情况下收到**安装失败**错误消息。可以忽略此消息，但要避免收到此消息，请在重新安装 Session Recording 组件前重新启动计算机。

[#544579]

- 卸载 Session Recording 组件后，在未重新启动计算机的情况下重新安装它们。
- 安装失败并发生回滚，然后尝试在未重新启动计算机的情况下重新安装 Session Recording 组件。

- 在某些情况下，通过会话可靠性进行连接的桌面会话可能会断开音频连接。

[#LC1257]

- Ctxgfx.exe 进程可能无响应。

[#LC2410]

- 如果您在 VDA 会话中运行 Citrix GoToMeeting 并被设置为演示者，则您的鼠标指针可能会开始闪烁。如果会话禁用了“旧图形模式”策略设置，则会发生此问题。

[#LC3033]

- 如果本地用户和远程桌面组包含域用户对象，则尝试安装 VDA 将失败。如果本地和远程桌面用户组包含本地或域组对象，则不会发生此问题。

[#LC3100]

- 在启用了本地应用程序访问的 VDA 会话中，无法激活屏幕保护程序。

[#LC3182]

- 在使用通用 USB 重定向功能重定向后，可能无法在 HDX 3D Pro 会话中显示鼠标光标。

[#LC3353]

- 操作系统中的 picadms.sys 出现错误，并显示蓝屏和停止代码 0x20。

[#LC3473]

- Citrix Device Redirector 服务可能无法完成 I/O 操作，事件查看器显示以下错误消息：

“The Citrix Device Redirector service could not complete an IO operation with Redirector Bus.” (Citrix Device Redirector 服务无法使用重定向程序总线完成 IO 操作。)

[#LC3497]

- SSL 连接 (HTTPS) 可能无法在 VDA 会话中正常运行。

[#LC3535]

- 在管理员尝试从 Hyper-V 控制台访问虚拟机时，如果某个会话已断开连接，但处于活动状态，则会显示黑屏。在使用 XPDM 驱动程序的部署环境中会发生此问题。

[#LC3536]

- 尝试从 VDA 或 RDP 会话中重新启动 Citrix Device Redirector 服务可能会使该服务始终保持无响应状态，而不是实际重新启动。

[#LC3544]

- 最大化的已发布应用程序窗口可能会盖住从显示分辨率不同的设备进行漫游的会话的用户设备会话任务栏。

[#LC3671]

- 即使相关已发布应用程序关闭了文件，WFICA32.exe 进程也仍会使该文件保持锁定状态。因此，在一段时间内无法编辑该文件。

[#LC3724]

- VDA 可能不再接受连接。启动“旧图形模式”策略后，VDA 将再次开始接受连接。

[#LC3749]

- 无缝应用程序可能无响应，它在 Windows 任务栏中的图标将还原为通用 Citrix Receiver 图标。

[#LC3783]

- 启用 Citrix Windows XP 显示驱动程序模型 (XPDM) 显示驱动程序后，鼠标阴影设置将始终处于启用状态，即使在控制面板中将其禁用也是如此。

[#LC3806]

- 在 HDX 3D Pro 桌面上使用 Microsoft Internet Explorer 时，如果您将鼠标光标从左边缘位置移回窗口内部，该光标不会从“水平调整”还原为“普通”形状。

[#LC3849]

- picadm.sys 上的死锁可能导致已发布应用程序无响应。

[#LC3872]

- 如果启用了 Excelhook，则在最小化后还原 Excel 工作簿时，可能导致 Excel 窗口丢失焦点。

[#LC3873]

- 操作系统中的 picadm.sys 出现错误，并显示蓝屏和停止代码 0x50。

[#LC3921]

- 在 HDX 3D Pro 双监视器配置中，在一个监视器上锁定 Windows 可能不会使第二个监视器屏幕显示空白。如果与一个双监视器客户端会话断开连接后，从一个监视器客户端重新连接，然后从该会话中断开连接，再从该双监视器客户端重新连接，则会发生此问题。

[#LC3934]

- 尝试使用 attrib 命令更改已映射客户端驱动器上的文件的文件属性可能会失败。

[#LC3958]

- 关闭一个无缝已发布应用程序后，焦点将转到另一个已发布应用程序，而不是典型 Windows Z 顺序中的窗口。

[#LC4009]

- 在将 VDA for Desktop OS 升级到 7.6.300 版后，VDA 可能会发生致命异常，从而导致在用户登录时显示蓝屏。

[#LC4044]

- 在将 VDA for Desktop OS 或 Server OS 升级到 7.6.300 版后，Citrix Print Manager Service (CpSvc.exe) 可能会在注销时意外退出。

[#LC4102]

- 对于使用非永久配置文件的用户来说，在安装了 PowerShell 3.0 或更高版本的计算机上可能需要很长时间才能启动已发布的 App-V 应用程序。

[#LC4147]

- 将鼠标放置在 Microsoft Notepad 应用程序窗口边缘时，鼠标指针可能无法呈现正确的形状。

要启用此项修复，必须设置以下注册表项：

- 在 32 位 Windows 上：
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D
名称：EnableUnknownCursorHandling
类型：REG_DWORD
值：1
- 在 64 位 Windows 上：
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HDX3D
名称：EnableUnknownCursorHandling
类型：REG_DWORD
值：1

[#LC4160]

- 由于 picadm.sys 上的死锁，VDA 可能会在出现“欢迎”屏幕后无响应。

[#LC4195]

- VDA 可能会在 picadd.sys 上发生致命异常，并显示蓝屏。

[#LC4207]

- 启用通用 USB 重定向功能后，每当在会话中与通用重定向的 USB 设备断开物理连接并重新连接时，该设备都会被视为新设

备。因此，每次重新连接这种 USB 设备时，系统都会为其另外创建一个 GUID。

[#LC4259]

- 尝试调整会话屏幕分辨率可能会间歇性失败，从而使 DesktopViewer 窗口灰显。

[#LC4261]

- 操作系统中的 picadm.sys 出现错误，并显示蓝屏和停止代码 0x000000C1。

[#LC4334]

- 如果启用了本地应用程序访问，则在重新连接到已断开的会话后单击某个应用程序快捷方式，可能无法启动相关的应用程序。

[#LC4362]

- 如果本地用户和远程桌面组包含域用户对象，则尝试安装 VDA 将失败。如果本地和远程桌面用户组包含本地或域组对象，则不会发生此问题。

[#LC3100]

- 如果您在 VDA 会话中运行 Citrix GoToMeeting 并被设置为演示者，则您的鼠标指针可能会开始闪烁。如果会话禁用了“旧图形模式”策略设置，则会发生此问题。

[#LC3033]

- 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。

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。

[#LC3167]

- 在启用了本地应用程序访问的 VDA 会话中，无法激活屏幕保护程序。

[#LC3182]

- 通过此增强功能，不再需要从影子任务栏 (cshadow.exe) 向主域控制器进行身份验证。应用此修复后，此任务栏将查询常规域控制器。

[#LC3381]

- 操作系统中的 picadm.sys 出现错误，并显示蓝屏和停止代码 0x20。

[#LC3473]

- Citrix Device Redirector 服务可能无法完成 I/O 操作，事件查看器显示以下错误消息：

“The Citrix Device Redirector service could not complete an IO operation with Redirector Bus.” (Citrix Device Redirector 服务无法使用重定向程序总线完成 IO 操作。)

[#LC3497]

- SSL 连接 (HTTPS) 可能无法在 VDA 会话中正常运行。

[#LC3535]

- 尝试从 VDA 或 RDP 会话中重新启动 Citrix Device Redirector 服务可能会使该服务始终保持无响应状态，而不是实际重新启动。

[#LC3544]

- 服务器上的 picadms.sys 可能发生致命异常，并显示错误检测代码 0x20。

[#LC3564]

- 最大化的已发布应用程序窗口可能会盖住从显示分辨率不同的设备进行漫游的会话的用户设备会话任务栏。

[#LC3671]

- 即使相关已发布应用程序关闭了文件，WFICA32.exe 进程也仍会使该文件保持锁定状态。因此，在一段时间内无法编辑该文件。

[#LC3724]

- 无缝应用程序可能无响应，它在 Windows 任务栏中的图标将还原为通用 Citrix Receiver 图标。

[#LC3783]

- 在第三方 CAD 应用程序中移动鼠标时，鼠标指针可能无法呈现正确的上下文形状。

[#LC3852]

- picadms.sys 上的死锁可能导致已发布应用程序无响应。

[#LC3872]

- 如果启用了 Excelhook，则在最小化后还原 Excel 工作簿时，可能导致 Excel 窗口丢失焦点。

[#LC3873]

- 如果具有只写权限的用户打开某个已映射客户端驱动器上的文件，则在尝试向该文件附加数据时可能会失败。在第二次运行 PowerShell 命令“get-process | out-file -filepath “\\client\c\$\temp\proclist.txt” -Append”时会发生此问题。

[#LC3895]

- 操作系统中的 picadms.sys 出现错误，并显示蓝屏和停止代码 0x50。

[#LC3921]

- 尝试使用 attrib 命令更改已映射客户端驱动器上的文件的文件属性可能会失败。

[#LC3958]

- 关闭一个无缝已发布应用程序后，焦点将转到另一个已发布应用程序，而不是典型 [Windows Z 顺序](#) 中的窗口。

[#LC4009]

- 在将 VDA for Desktop OS 升级到 7.6.300 版后，VDA 可能会发生致命异常，从而导致在用户登录时显示蓝屏。

[#LC4044]

- 在将 VDA for Desktop OS 或 Server OS 升级到 7.6.300 版后，Citrix Print Manager Service (CpSvc.exe) 可能会在注销时意外退出。

[#LC4102]

- 在安装了 XenApp 6.5 Hotfix Rollup Pack 6 的服务器上，某些第三方应用程序可能无法在 RDP 会话中启动。

[#LC4141]

- 对于使用非永久配置文件的用户来说，在安装了 PowerShell 3.0 或更高版本的计算机上可能需要很长时间才能启动已发布的 App-V 应用程序。

[#LC4147]

- 由于 picadm.sys 上的死锁，VDA 可能会在出现“欢迎”屏幕后无响应。

[#LC4195]

- VDA 可能会在 picadd.sys 上发生致命异常，并显示蓝屏。

[#LC4207]

- 启用 USB 重定向功能后，每次在会话中断开某些重定向的 USB 设备并重新连接时，这些设备都会被视为新设备。因此，每次重新连接这种 USB 设备时，系统都会为其另外创建一个 GUID。

[#LC4259]

- 升级到 VDA for Server OS 7.6.300 版时，COM 端口映射可能会间歇性失败。

[#LC4267]

- 操作系统中的 picadm.sys 出现错误，并显示蓝屏和停止代码 0x000000C1。

[#LC4334]

- 如果启用了本地应用程序访问，则在重新连接到已断开的会话后单击某个应用程序快捷方式，可能无法启动相关的应用程序。

[#LC4362]

- 安装 Microsoft 修补程序 KB3124266（对于 Windows 10）或 KB3124263（对于 Windows 10 1511）后，尝试登录到 Windows 10 上运行的 XenDesktop VDA 7.6.300 或 7.7 可能会失败。有关详细信息，请参阅知识中心文章 [CTX205398](#)。

注意：如果您已安装 KB3124266 或 KB3124263，并希望应用此更新，请执行以下操作：

1. 重新启动并使用安全模式登录到 Windows 10 计算机，然后卸载 KB3124266 或 KB3124263
2. 重新启动 Windows 10 计算机，然后安装此更新。

3. 重新安装 KB3124266 或 KB3124263。
[#LC4540]

已知问题

May 12, 2016

以下警告适用于任何建议更改注册表项的解决方法。

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。

XenApp 和 XenDesktop

XenApp 7.8 和 XenDesktop 7.8 版包含以下问题：

- 使用鼠标滚轮滚动时，在 Framehawk 会话内单击可能会导致意外结果。当前解决方法是换一个鼠标。[#618657]
- AppDisk 封装过程会过度占用时间和 CPU 使用率，因为驱动程序读取每个文件的元数据，这会导致病毒检查程序检查磁盘上的每个比特。要避免此问题，请在启动密封进程前，将 CtxPvD.exe 和 CtxPvDSvc.exe 添加到防病毒程序的排除列表。这些文件位于 c:\Program Files\Citrix\personal vDisk\bin 中。不建议禁用您的防病毒程序。[#602819]
- 无法使用 **Firefox** 和 **Chrome** 的 NPAPI 界面启用本地应用程序访问和 URL 重定向浏览器插件，如相关软件支持文章所述。这是一个已知问题，建议客户使用 Internet Explorer 来解决。[#620101]
- 如果在启用了 Aero 但未启用图形硬件加速 (GPU) 的 Windows 7 上使用 VDA for Windows Desktop OS 连接到高分辨率监视器（例如 4096 x 2160），则可能发生屏幕损坏。要解决此问题，可将桌面主题更改为无 Aero 主题或降低分辨率。[#618121]
- 如果注册了拨打住宅电话功能，而 Controller、StoreFront 和 VDA 安装在同一台服务器上，则卸载其中任一组件可能也会从该服务器中删除拨打住宅电话组件。解决方法：重新注册拨打住宅电话功能。[#616142]
- 在从版本 7.5 升级后，或者如果已从版本 7.5 升级，则在从版本 7.6 升级后，Studio 或高级别 SDK 可能无法启动，因为 FMAUtils.dll 文件无法安装。如果站点升级失败，则会显示消息：“Could not load file or assembly 'FMAUtils, Version ... The system cannot find the file specified.’”（无法加载文件或程序集 FMAUtils, 版本 ... 系统找不到指定文件。）解决方法：完成 Studio MSI ([XDInstallerRoot]\x64\DesktopStudio\DesktopStudio_x64.msi) 或高级别 SDK MSI ([XDInstallerRoot]\x64\Citrix Desktop Delivery Controller\XDPoshSnapin.msi) 的修复安装。[#617897]
- 通过 App-V 发布时，名称包含下划线 (_) 的应用程序可能无法启动。[#618488]
- 在站点创建期间，如果将许可证导入本地计算机，这些许可证可能无法显示（如果已将这些许可证导入外部计算机，则不会发生此问题）。如果发生这种情况，请完成站点创建过程。在 Studio 中，检查“配置”>“许可”以确保已正确设置产品版本（默认为 Platinum）。导入的许可证将在大约五分钟后显示出来。[#618538]
- 如果在从站点删除 Controller 后尝试将计算机目录移动到其他区域，则操作可能失败。解决方法：使用 Set-BrokerHypervisorConnection -PreferredController cmdlet 并指定空值以自动选择首选 Controller (Get-BrokerHypervisorConnection -PreferredController \$null | Set-BrokerHypervisorConnection -PreferredController \$null)，或者指定一个特定的 Controller。[#619345]
- 如果在先前版本中为应用程序创建了标记，则在升级到此版本后，将 Studio 将无法显示这些标记。（这些标记起初是存储在应用程序元数据中的，而不是存储为标记对象的。）但是，如果您的脚本使用这些标记，这些标记在该脚本中仍然有效。[#620041]
- 如果 XenDesktop 站点处于租用连接模式，则在重新启动置备的资源后，用户无法与这些资源建立会话，除非该站点退出租用连接模式（即 Controller 可以再次访问站点数据库）。[#621521]
- 在因站点数据库不可用而进入租用连接模式后，如果站点恢复正常运行，Studio 可能仍会将 VM 显示为“未知”状态，而将主机连接显示为“不可用”状态。解决方法：对受影响的连接启用维护模式，等待大约 30 秒，然后关闭维护模式。这样就可以还原正确的状态显示以及可用的电源操作。[#620941]
- 此问题仅影响 VMware 虚拟机管理程序上的计算机。在从已连接 AppDisk 的交付组中删除计算机时，从虚拟机管理程序删除最后一个计算机后，可能会从虚拟机管理程序存储中删除 AppDisk。只有在删除此计算机时 AppDisk 始终连接到此计算机的情况下，才会发生此问题。要避免此问题，请从 Studio 中完成以下任务，以确保 AppDisk 未连接到最后要删除的计算机。
 1. 从计算机目录中删除除最后一台计算机之外的所有计算机（如果正在使用 Provisioning Services，则随后手动删除相应的 VM）。
 2. 启动最后一台计算机。（请务必从 Studio 执行此操作，而不是从虚拟机管理程序执行此操作。）
 3. 关闭最后一台计算机。
 4. 删除最后一台计算机（如果正在使用 Provisioning Services，则随后手动删除相应的 VM）。

[#621002]

您可以在 [Windows Server 2016 技术预览版论坛](#) 中查看在将此 XenApp 和 XenDesktop 版本与 Windows Server 2016 技术预览版结合使用时发现的一系列问题。

其他组件

单独在 XenApp 和 XenDesktop 下载页面上提供的组件具有以下已知问题。

- 安装 Session Recording Server 组件失败，并显示错误代码 2503 和 2502。解决方案：检查文件夹 C:\windows\Temp 的访问控制列表 (ACL)，以确保本地用户组 > 组 > 用户具有对该文件夹的写入权限。否则，请手动添加写入权限。[#611487]
- 由于 Session Recording 不支持 Framehawk 显示模式，无法正确录制和播放 Framehawk 显示模式下的会话。在此模式下录制的会话可能不包含会话活动。[#622085]
- 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：通过向安装 Citrix Receiver for Windows 的计算机部署 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 <http://support.citrix.com/article/CTX123169> 和 <http://docs.citrix.com/zh-cn/receiver/windows/4-4/ica-overview-receiver-config/ica-import-icaclient-template-v2.html>。[#618237]
- 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都会限制为 1 GB，超过此限制后，就不会再录制活动。[#584890]
- 如果 Machine Creation Services (MCS) 或 Provisioning Services 使用已配置的主映像和已安装的 Microsoft 消息队列 (MSMQ) 创建了多个 VDA，则这些 VDA 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，从而导致会话始终处于活动状态。[#528678]

根据部署方法，为每个 VDA 创建唯一的永久性 QMId 的解决方法各不相同。

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 或更高版本创建的，则无需执行任何额外操作；例如，经过配置后，VDA 中单独的个人虚拟磁盘或本地磁盘上的所有更改都是永久性的。

对于在静态桌面模式下由 MCS 或 PVS 创建的服务器操作系统 VDA 或由 MCS 创建的专用桌面操作系统 VDA，如果经过配置后，VDA 中单独的个人虚拟磁盘或本地磁盘上的所有更改都是永久性的，请使用脚本 (GenQMID.ps1) 在系统启动时修改 QMId。

如果由 MCS 或 PVS 创建的桌面操作系统 VDA 经过配置后会在用户注销时放弃所有更改，请使用另一个脚本 (GenRandomQMID.ps1) 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。

要使用脚本，请执行以下操作：

1. 确保在 PowerShell 中将执行策略设置为“RemoteSigned”或“Unrestricted”。

Set-ExecutionPolicy RemoteSigned

2. 创建计划任务并将触发器设置为“在系统启动时”，然后在 Provisioning Services 或 MCS 主映像计算机上使用 SYSTEM 帐户运行。

3. 将此命令添加为启动任务。

powershell.exe -file C:\GenQMID.ps1
或


```
powershell .exe -file C:\GenRandomQMID.ps1
```

GenQMID.ps1 摘要：

1. 生成基于计算机 UUID 哈希值的 QMId。
2. 停止相关访问，包括 CitrixSmAudAgent 和 MSMQ。
3. 启动先前停止的服务以应用 QMId 更改。

```
function ConvertHexStringToByte($theString)

{

    $bytes = New-Object Byte[] ($theString.Length / 2)

    for ($i = 0; $i -lt $theString.Length; $i += 2) {

        $bytes[$i / 2] = [System.Convert]::ToByte($theString.Substring($i, 2), 16)

    }

    return $bytes

}

Try {

    # Get UUID of machine

    $strUUID = (Get-WmiObject -Class Win32_ComputerSystemProduct | Select-Object -Property UUID).UUID

    # Remove "-"

    $strUUID = $strUUID.ToString().Replace("-", "")

    # Convert string to bytes

    $UUID = ConvertHexStringToByte($strUUID)
```

```

# Set UUID as QMId

$new_QMID = $UUID

}

Catch {

# IF exception occurred, just use MD5 digest of FQDN as QMID

# Get FQDN

$fqdn = [System.Net.Dns]::GetHostByName(($env:computerName)).HostName

# Calculate MD5 hash of FQDN

$md5 = new-object -TypeName System.Security.Cryptography.MD5CryptoServiceProvider

# Set md5 digest as QMID

$utf8 = new-object -TypeName System.Text.UTF8Encoding

$new_QMID = $md5.ComputeHash($utf8.GetBytes($fqdn))

}

# Write new_QMID into registry

Set-ItemProperty -Path HKLM:\Software\Microsoft\MSMQ\Parameters\MachineCache -Name "QMId" -Value $new_QMID

# Restart MSMQ to adopt new QMId

# Get dependent services

```

```
$depServices = Get-Service -name MSMQ -dependentservices | Select -Property Name

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

        }

    }

}
```

GenRandomQMID.ps1 摘要：

1. 从注册表中删除当前的 QMId。
2. 在 HKLM\Software\Microsoft\MSMQ\Parameters 中添加 SysPrep = 1。
3. 停止相关访问，包括 CitrixSmAudAgent 和 MSMQ。
4. 启动先前停止的服务以生成随机 QMId。

```

# 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

        }

    }

}

```

- 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。[#524973]
- 更改 XenApp 或 XenDesktop 许可证类型时，所做的更改不会在 Session Recording 中立即生效。解决方法：重新启动 VDA 计算机。[#532393]
- Session Recording 在支持预启动的应用程序会话方面的限制 [#561109]
 - 问题：
 - 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，从而导致不进行会话录制。

- 如果活动策略录制每个应用程序，当用户登录 Windows Receiver（同时建立预启动会话）时，将显示关于录制的通知，并且录制空会话以及之后在此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。这样可确保录制预启动会话。但是，仍显示通知。

本版本中不提供功能

Apr 25, 2016

提示：如果您最新的体验是使用 XenApp 6.5（或早期版本的 XenApp）获得的，还应查看[此处](#)所述的体系结构、术语和元素差异。

当前未提供或不再支持以下功能。

- **启动触控优化桌面** - 此设置已针对 Windows 10 计算机禁用。有关详细信息，请参阅 [移动体验策略设置](#)。
- **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：
 - 向后兼容 DOS 客户端和 16 位打印机，包括旧版客户端打印机名称。
 - 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。
- **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。
- **电源和容量管理** - 在 7.x 之前的版本中，可以使用电源和容量管理功能来降低电耗并管理服务器容量。Microsoft Configuration Manager 工具替代了此功能。
- **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 Online Plug-in 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。
- **Smart Auditor** - 在 7.x 之前的版本中，可以通过 Smart Auditor 录制用户会话的屏幕活动。自 7.6 Feature Pack 1 起，此功能由 Session Recording 提供。
- **单点登录** - 此功能可以保证密码安全，但在 Windows 8 和 Windows Server 2012 环境中不受支持。在 Windows 2008 R2 和 Windows 7 环境中仍然支持此功能，但 7.x 版不提供此功能。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 版需要使用 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 文件用于从用户设备（使用 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 监视场的活动，但不支持 7.x 版本。
- **CNAME 功能** - 在 7.x 之前的版本中，CNAME 功能默认处于启用状态。如果部署依赖于 CNAME 记录进行 FQDN 重新路由并且使用 NETBIOS 名称，则可能会失败。在 7.x 版本中，Delivery Controller 自动更新是其替代功能，该功能可以动态更新

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，但可以通过创建策略禁用该功能。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 Studio 版本中，利用此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 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。
 - **颜色深度** - 在 7.6 之前的 Studio 版本中，您在交付组的用户设置中指定了颜色深度。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。
 - **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，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**设置不会影响 RDP 连接；无论是否启用了此设置，VDA 直接访问用户组的用户均可通过 RDP 连接来连接到 VDA
-
- **COM 端口映射** — COM 端口映射可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** — 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)

第三方声明

Apr 25, 2016

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：

- [XenApp 7.8 和 XenDesktop 7.8 第三方声明](#)
- [FLEXnet Publisher 补充文档：FlexNet Publisher 11.13.1 中使用的第三方软件和开源软件](#)
- [Linux 虚拟桌面 1.2 版本第三方声明](#)

系统要求

Jun 17, 2016

在本文中：

- [Delivery Controller](#)
- [数据库](#)
- [Citrix Studio](#)
- [Citrix Director](#)
- [Virtual Delivery Agent \(VDA\) for Desktop OS](#)
- [Virtual Delivery Agent \(VDA\) for Server OS](#)
- [主机/虚拟化资源](#)
- [Active Directory 功能级别](#)
- [HDX](#)
- [Session Recording](#)
- [通用打印服务器](#)
- [其他](#)

简介

本文档中的系统要求在发布此产品版本时有效；将定期发布更新。本文档中未涉及的组件（例如 StoreFront、主机系统、Citrix Receiver 和插件以及 Provisioning Services）的系统要求在其各自的文档中进行说明。

重要：请在开始安装之前，阅读[准备安装](#)。

除非另有说明，否则如果在计算机上未检测到所需版本的软件必备项，则组件安装程序会自动部署这些软件必备项（如 .NET 和 C++ 软件包）。Citrix 安装介质还包含部分必备软件。

安装介质包含多个第三方组件。使用 Citrix 软件之前，请检查是否存在第三方安全更新并进行安装。

磁盘空间值仅为估计值，且是除产品映像、操作系统和其他软件所需空间以外的额外空间。

如果在单个服务器上安装所有核心组件（包括 Controller、SQL Server Express、Studio、Director、StoreFront 和 Licensing），最低需要 4 GB RAM 才能评估产品；建议为用户运行环境时使用更多 RAM。性能会因为您的具体配置而有所不同，包括用户数量、应用程序、桌面以及其他因素。

有关全球化信息，请参阅 [CTX119253](#)。

Delivery Controller

支持的操作系统：

- Windows Server 2016 当前技术预览版：此版本对此操作系统的支持是一项实验功能，不能用于生产环境
- Windows Server 2012 R2 Standard Edition 和 Datacenter Edition
- Windows Server 2012 Standard Edition 和 Datacenter Edition
- Windows Server 2008 R2 SP1 Standard Edition、Enterprise Edition 和 Datacenter Edition

要求：

- Microsoft .NET Framework 3.5.1（仅限 Windows Server 2008 R2）。
- Microsoft .NET Framework 4.5.2（也支持 4.6）。
- Windows PowerShell 2.0（随 Windows Server 2008 R2 提供）或 3.0（随 Windows Server 2016 技术预览版、Windows Server 2012 R2 和 Windows Server 2012 提供）。
- Visual C++ 2008 SP1 可再发行组件包。
- 磁盘空间：100 MB。

使用可选功能会增加磁盘空间需求。例如，默认情况下会启用连接租用，用于连接租用的空间量取决于用户和应用程序的数量以及所用模式：如果 RDS 用户数为 100,000 个，而最近使用的应用程序数量为 100 个，则连接租用大约需要 3 GB 空间；部署中的应用程序越多，需要的空间越多。对于专用 VDI 桌面，40,000 个桌面至少需要 400-500 MB。无论何种情况，Citrix 建议提供数 GB 的额外空间。

数据库

站点配置数据库、配置日志记录数据库和监视数据库支持的 Microsoft SQL Server 版本如下：

- SQL Server 2014 Express Edition、Standard Edition 和 Enterprise Edition。
- SQL Server 2012 SP1 和 SP2、Express Edition、Standard Edition 和 Enterprise Edition。默认情况下，如果未检测到支持的现有 SQL Server 安装，安装 Controller 时将安装 SQL Server 2012 SP2 Express。
- SQL Server 2008 R2 SP2 Express Edition、Standard Edition、Enterprise Edition 和 Datacenter Edition。

支持下列数据库功能（SQL Server Express 除外，此版本仅支持独立模式）：

- SQL Server 群集实例
- SQL Server 镜像
- SQL Server 2012 AlwaysOn 可用性组

Controller 与 SQL Server 数据库之间的连接需要 Windows 身份验证。

有关详细信息，请参阅[数据库](#)一文。

Citrix Studio

支持的操作系统：

- Windows 10 Pro Edition、Enterprise Edition 和 Educational Edition
- Windows 8.1 Professional Edition 和 Enterprise Edition
- Windows 8 Professional Edition 和 Enterprise Edition
- Windows 7 Professional Edition、Enterprise Edition 和 Ultimate Edition
- Windows Server 2016 当前技术预览版：此版本提供的支持是一项实验功能，不能用于生产环境
- Windows Server 2012 R2 Standard Edition 和 Datacenter Edition
- Windows Server 2012 Standard Edition 和 Datacenter Edition
- Windows Server 2008 R2 SP1 Standard Edition、Enterprise Edition 和 Datacenter Edition

要求：

- 磁盘空间：75 MB
- Microsoft .NET Framework 4.5.2 (也支持 4.6)
- Microsoft .NET Framework 3.5 SP1 (仅限 Windows Server 2008 R2 和 Windows 7)
- Microsoft Management Console 3.0 (随所有支持的操作系统提供)
- Windows PowerShell 2.0 (随 Windows 7 和 Windows Server 2008 R2 提供) 或 3.0 (随 Windows 10、Windows 8.1、Windows 8、Windows Server 2016 技术预览版、Windows Server 2012 R2 和 Windows Server 2012 提供)

Citrix Director

支持的操作系统：

- Windows Server 2016 当前技术预览版：此版本提供的支持是一项实验功能，不能用于生产环境
- Windows Server 2012 R2 Standard Edition 和 Datacenter Edition
- Windows Server 2012 Standard Edition 和 Datacenter Edition
- Windows Server 2008 R2 SP1 Standard Edition、Enterprise Edition 和 Datacenter Edition

要求：

- 磁盘空间：140 MB。
- Microsoft .NET Framework 4.5.2 (也支持 4.6)。
- Microsoft .NET Framework 3.5 SP1 (仅限 Windows Server 2008 R2)
- Microsoft Internet Information Services (IIS) 7.0 和 ASP.NET 2.0。确保 IIS 服务器角色已安装静态内容角色服务。如果尚未安装这些服务，系统会提示您插入 WindowsServer 安装介质并进行安装。

System Center Operations Manager (SCOM) 集成要求：

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

支持查看 Director 的浏览器：

- Internet Explorer 11。可以使用 Internet Explorer 10，但 Microsoft 支持版本 11，而 Citrix 也建议使用版本 11。Internet Explorer 不支持兼容模式。您必须使用建议的浏览器设置访问 Director。安装 Internet Explorer 时，接受默认设置以使用建议的安全性和兼容性设置。如果已经安装了浏览器并选择不使用建议的设置，请转到“工具 > Internet 选项 > 高级 > 重置”并按照说明进行操作。
- Microsoft Edge。
- Firefox ESR (扩展支持版本)。
- Chrome。

有关适用于 Director 控制台的最佳分辨率的信息，请参阅[此博客文章](#)。

Virtual Delivery Agent (VDA) for Desktop OS

支持的操作系统：

- Windows 10 Professional、Enterprise 和 Educational Edition (Windows 10 不支持以下功能：HDX 3D Pro、GPU 加速、桌面组合重定向、旧图形模式、安全启动、使用 VM 托管应用程序发布通用 Windows 应用程序)
- Windows 8.1 Professional Edition 和 Enterprise Edition

- Windows 8 Professional Edition 和 Enterprise Edition
- Windows 7 SP1 Professional Edition、Enterprise Edition 和 Ultimate Edition

要使用服务器 VDI 功能，可以在受支持的服务器操作系统上使用命令行界面安装 VDA for Windows Desktop OS；请参阅[服务器 VDI](#) 一文获得相关指导。

- Windows Server 2016 当前技术预览版：此版本提供的支持是一项实验功能，不能用于生产环境
- Windows Server 2012 R2 Standard Edition 和 Datacenter Edition
- Windows Server 2012 Standard Edition 和 Datacenter Edition
- Windows Server 2008 R2 SP1 Standard Edition、Enterprise Edition 和 Datacenter Edition

要求：

- Microsoft .NET Framework 4.5.2（也支持 4.6）
- Microsoft .NET Framework 3.5.1（仅限 Windows 7）
- Microsoft Visual C++ 2008 SP1、2010 SP1 和 2013 Runtime（32 位和 64 位）

Remote PC Access 使用此 VDA（您可将其安装在办公室物理 PC 上）。

多种多媒体加速功能（如 HDX MediaStream Windows Media 重定向）要求在安装 VDA 的计算机上安装 Microsoft 媒体基础。如果该计算机未安装媒体基础，将无法安装和使用多媒体加速功能。请勿在安装 Citrix 软件后从计算机上删除媒体基础；否则，用户将无法登录到此计算机。在大多数受支持的 Windows 桌面操作系统版本上，已经安装了媒体基础支持，不能将其删除。但是，N 版本不包括某些与媒体相关的技术；您可以从 Microsoft 或第三方获取该软件。

在 VDA 安装期间，可以选择安装 HDX 3D Pro 版的 VDA for Windows Desktop OS。此版本特别适合与 DirectX 和 OpenGL 驱动的应用程序以及视频等富媒体结合使用。请注意，Windows 10 不支持该功能。有关其他支持信息，请参阅[HDX 3D Pro](#) 部分。

不能在运行 Windows XP 或 Windows Vista 的计算机上安装当前版本的 VDA；但如果需要，您可以在这些操作系统上安装早期版本的 Virtual Desktop Agent。有关详细信息，请参阅[CTX140941](#)。此版本中的 Remote PC Access 版本在 Windows Vista 操作系统上不受支持。

Virtual Delivery Agent (VDA) for Server OS

支持的操作系统：

- Windows Server 2016 当前技术预览版：此版本提供的支持是一项实验功能，不能用于生产环境
- Windows Server 2012 R2 Standard Edition 和 Datacenter Edition
- Windows Server 2012 Standard Edition 和 Datacenter Edition
- Windows Server 2008 R2 SP1 Standard Edition、Enterprise Edition 和 Datacenter Edition

安装程序将自动部署以下必要的组件，这些组件也可以在 Citrix 安装介质上的 Support 文件夹中找到：

- Microsoft .NET Framework 4.5.2（也支持 4.6）
- Microsoft .NET Framework 3.5.1（仅限 Windows Server 2008 R2）
- Microsoft Visual C++ 2008 SP1、2010 SP1 和 2013 Runtime（32 位和 64 位）

如果尚未安装并启用远程桌面服务角色服务，安装程序会自动安装并启用。

多种多媒体加速功能（如 HDX MediaStream Windows Media 重定向）要求在安装 VDA 的计算机上安装 Microsoft 媒体基

础。如果该计算机未安装媒体基础，将无法安装和使用多媒体加速功能。请勿在安装 Citrix 软件后从计算机上删除媒体基础；否则，用户将无法登录到此计算机。在大多数 Windows Server 2012 R2、Windows Server 2012 和 Windows Server 2008 R2 版本中，媒体基础功能通过服务器管理器进行安装（对于 Windows Server 2012 R2 和 Windows Server 2012：ServerMediaFoundation；对于 Windows Server 2008 R2：DesktopExperience）。但是，N 版本不包括某些与媒体相关的技术；您可以从 Microsoft 或第三方获取该软件。

主机/虚拟化资源

某些 XenApp 和 XenDesktop 功能可能并非在所有主机平台或所有平台版本上都受支持。例如，XenServer 和 VMware 主机支持 AppDisk。有关详细信息，请参阅相关功能的文档。

受支持的主机平台：

XenServer

- XenServer 6.5 和 SP1
- XenServer 6.2 SP1 加上修补程序（必须应用 SP1 才能应用将来的修补程序）
- XenServer 6.1

VMware vSphere。不支持 vSphere vCenter“链接模式”操作。

- VMware vSphere 6.0 和 Update 1
- VMware vSphere 5.5 和 Update 1 到 Update 3
- VMware vSphere 5.1 Update 2 和 Update 3
- VMware vSphere 5.0 Update 2 和 Update 3
- VMware vCenter 5.5/6 设备

System Center Virtual Machine Manager。包括可以注册到受支持的 System Center Virtual Machine Manager 版本中的任何 Hyper-V 版本。

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

Nutanix Acropolis 4.5。使用此平台时，多项 XenApp 和 XenDesktop 功能不可用；有关详细信息，请参阅 [CTX202032](#)。有关结合使用此产品与 Acropolis 的详细信息，请参阅 <https://portal.nutanix.com/#/page/docs>。

受支持的云环境：

Amazon Web Services (AWS)

- 可以在支持的 Windows 服务器操作系统上置备应用程序和桌面。
- SQL Server 2012 Enterprise 在 AWS 上不可用。
- AWS 不提供桌面操作系统实例。
- 不支持 Amazon Relational Database Service (RDS)。
- 有关其他信息，请参阅 AWS 文档和 [CTX140631](#)。

Citrix CloudPlatform

- 支持的最低版本为含修补程序 4.2.1-4 的 4.2.1 版。

- 部署经过 XenServer 6.2（具有 Service Pack 1 和修补程序 XS62ESP1003）和 vSphere 5.1 虚拟机管理程序的测试。
- CloudPlatform 不支持 Hyper-V 虚拟机管理程序。
- CloudPlatform 4.3.0.1 支持 VMware vSphere 5.5。
- 有关其他支持信息和基于 Linux 的系统要求信息，请参阅 CloudPlatform 文档（包括您的 CloudPlatform 版本的发行说明）和 [CTX140636](#)。

Microsoft Azure

Remote PC Access 局域网唤醒功能需要 Microsoft System Center Configuration Manager 2012。

Active Directory 功能级别

支持以下 Active Directory 林和域功能级别：

- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003
- Windows 2000 本机（不支持域控制器）

HDX

Receiver for Windows 和 Citrix Receiver for Linux 13 支持多流 ICA 的 UDP 音频。

Citrix Receiver for Windows 支持回声消除。

请参阅下文具体的 HDX 功能支持和要求。

Windows 用户设备或瘦客户端必须支持或包含：

- DirectX 9
- Pixel Shader 2.0（硬件支持）
- 32 位/像素
- 1.5 GHz 32 位或 64 位处理器
- 1 GB RAM
- 图形卡或集成图形处理器上具有 128 MB 视频内存

HDX 将查询 Windows 设备，以验证设备是否具备所需的 GPU 功能，如果不具备所需功能，则自动恢复为服务器端桌面组合。具有所需 GPU 功能、但不符合处理器速度或 RAM 规格要求的设备将列在从桌面组合重定向中排除的设备 GPO 组中。

最小可用带宽为 1.5 Mbps；建议带宽为 5 Mbps。这些值包含了端到端延迟。

以下客户端支持 Windows Media 客户端内容提取、Windows Media 重定向和实时 Windows Media 多媒体转码功能：Citrix Receiver for Windows、Citrix Receiver for iOS 和 Citrix Receiver for Linux。

要在 Windows 8 设备上使用 Windows Media 客户端内容提取，请将 Citrix Multimedia Redirector 设置为默认程序：在控制面板 > 程序 > 默认程序 > 设置默认程序中，选择 Citrix Multimedia Redirector，然后单击将此程序设置为默认程序或选择此程序的默认值。执行 GPU 代码转换需使用具有 Compute Capability 1.1 或更高版本且支持 NVIDIA CUDA 的 GPU；请参阅 <http://developer.nvidia.com/cuda/cuda-gpus>。

支持以下客户端和 Adobe Flash Player：

- Citrix Receiver for Windows（对于第二代 Flash 重定向功能）- 第二代 Flash 重定向功能需要安装适用于其他浏览器的 Adobe Flash Player（有时称为 NPAPI Flash Player，即 Netscape 插件应用程序编程接口 Flash Player）。
- Citrix Receiver for Linux（支持第二代 Flash 重定向功能）- 第二代 Flash 重定向功能需要安装适用于其他 Linux 的 Adobe Flash Player 或 Adobe Flash Player for Ubuntu。
- Citrix 联机插件 12.1（支持旧的 Flash 重定向功能）- 旧的 Flash 重定向功能要求安装 Adobe Flash Player for Windows Internet Explorer（有时称为 ActiveX 播放器）。

用户设备上的 Flash Player 主版本号必须大于或等于服务器上的 Flash Player 主版本号。如果用户设备上安装了早期版本的 Flash Player，或者用户设备上无法安装 Flash Player，则 Flash 内容将在服务器上呈现。

运行 VDA 的计算机需要：

- Adobe Flash Player for Windows Internet Explorer（ActiveX 播放器）
- Internet Explorer 11（非现代 UI 模式）。可以使用 Internet Explorer 7-10，但 Microsoft 支持版本 11，而 Citrix 也建议使用版本 11。Flash 重定向要求在服务器上安装 Internet Explorer；对于其他浏览器，Flash 内容将在服务器上呈现。
- 在 Internet Explorer 中禁用保护模式（不要选中“工具”>“Internet 选项”>“安全”选项卡>“启用保护模式”复选框）。重新启动 Internet Explorer 以使更改生效。

安装 VDA for Windows Desktop OS 时，可以选择安装 HDX 3D Pro 版本（例外：运行 Windows 10 的计算机）。

托管应用程序的物理机或虚拟机可以使用 GPU 直通或虚拟 GPU (vGPU) 功能：

- Citrix XenServer 中提供了 GPU 直通功能。GPU 直通也可随 VMware vSphere 和 VMware ESX 获得，此时它称为虚拟直接图形加速 (VDGA)。
- Citrix XenServer 和 VMware vSphere 提供了 vGPU 功能；请访问 www.citrix.com/go/vGPU（需要提供 Citrix“我的帐户”凭据）。

Citrix 建议的主机计算机规格如下：至少 4 GB RAM，4 个时钟速度至少为 2.3 GHz 的虚拟 CPU。

图形处理器 (GPU)：

- 对于基于 CPU 的压缩（包括无损压缩），HDX 3D Pro 支持主机计算机上与要交付的应用程序兼容的任何显示适配器。
- 为通过 NVIDIA GRID API 实现优化的 GPU 帧缓冲访问，HDX 3D Pro 要求安装具有最新 NVIDIA 驱动程序 of NVIDIA Quadro 图形卡。NVIDIA GRID 将提供较高的帧速率，从而实现高度互动的用户体验。
- 对于使用 XenServer 的 vGPU，HDX 3D Pro 的要求包括 NVIDIA GRID K1 和 K2 卡。

用户设备：

- HDX 3D Pro 支持主机计算机上的 GPU 支持的所有显示器分辨率。但是，要在建议的最低用户设备和 GPU 规格条件下实现最佳性能，Citrix 提出了以下建议：对于 LAN 连接，建议为用户设备将显示器最大分辨率设置为 1920 x 1200 像素，对于 WAN 连接，建议将其设置为 1280 x 1024 像素。

- Citrix 建议的用户设备规格如下：至少 1 GB RAM，1 个时钟速度至少为 1.6 GHz 的 CPU。要使用适用于低带宽连接的默认的深度压缩编解码器，需要功能更强大的 CPU，除非解码在硬件上完成。要获得最佳性能，Citrix 建议用户设备至少配有一个 2 GB 的 RAM 以及一个时钟速度至少为 3 GHz 的双核 CPU。
- 对于多监视器访问，Citrix 建议在用户设备中配备四核 CPU。
- 用户设备无需配备 GPU 即可访问通过 HDX 3D Pro 交付的桌面或应用程序。
- 必须安装 Citrix Receiver。

有关详细信息，请参阅 [HDX 3D Pro 一文](#)和 www.citrix.com/xenapp/3d。

支持的客户端：Citrix Receiver for Windows、Citrix Receiver for Mac 和 Citrix Receiver for Linux。

支持的视频会议应用程序：

- Adobe Connect
- Cisco WebEx
- Citrix GoToMeeting HDFaces
- Google+ Hangouts
- IBM Sametime
- Windows 8.x、Windows Server 2012 和 Windows Server 2012 R2 上基于 Media Foundation 的视频应用程序
- Microsoft Lync 2010 和 2013
- Microsoft Office Communicator
- Microsoft Skype 6.7

要在 Windows 客户端上使用 Skype，请在客户端和服务器的注册表：

客户端注册表项 HKEY_CURRENT_USER\Software\Citrix\HdxRealTime

名称：DefaultHeight，类型：REG_DWORD，数据：240

名称：DefaultWidth，类型：REG_DWORD，数据：320

服务器注册表项 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Vd3d\Compatibility

名称：skype.exe，类型：REG_DWORD，数据：设置为 0

其他用户设备要求：

- 产生声音的相应硬件。
- 与 DirectShow 兼容的网络摄像机（使用网络摄像机默认设置）。支持硬件编码的网络摄像机会降低客户端的 CPU 使用率。
- 如有可能，应安装网络摄像机制造商提供的网络摄像机驱动程序。

Session Recording

此部分介绍了以下组件的系统要求：

[Session Recording Administration 组件](#)

[Session Recording Agent](#)

Session Recording Administration 组件（Session Recording 数据库、Session Recording Server、Session Recording 策略控制台）可以安装在单台服务器或不同服务器上。

Session Recording 数据库

支持的操作系统：

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1

支持的 Microsoft SQL Server 版本：

- Microsoft SQL Server 2014 Enterprise、Express 和 Standard 版本
- Microsoft SQL Server 2012 SP2 Enterprise Edition 和 Express Edition
- Microsoft SQL Server 2008 R2 SP3 Enterprise Edition 和 Express Edition

要求：.NET Framework 3.5 SP1（仅限 Windows Server 2008 R2）或 .NET Framework 4.5.2 或 4.6。

Session Recording Server

支持的操作系统：

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1

必须先安装必备项，然后再安装 Session Recording Server。在服务器管理器中，添加 IIS 角色并选择以下选项：

- 应用程序开发 > ASP.NET 4.5（在 Server 2012 和 Server 2012 R2 上）或 ASP.NET（在 Server 2008 R2 上）。其他组件将自动选择；单击**添加**接受所需角色。
- 安全性 > Windows 身份验证
- “管理工具”>“IIS 6 管理兼容性”：“IIS 6 元数据库兼容性”、“IIS 6 WMI 兼容性”、“IIS 6 脚本工具”、“IIS 6 管理控制台”

其他要求：

- .NET Framework 3.5 SP1（仅限 Windows Server 2008 R2）或 .NET Framework 4.5.2 或 4.6。
- 如果 Session Recording Server 使用 HTTPS 作为其通信协议，请添加有效证书。默认情况下，Session Recording 使用 HTTPS（Citrix 推荐）。
- Microsoft 消息队列 (MSMQ)，Active Directory 集成处于禁用状态，MSMQ HTTP 支持处于启用状态。

Session Recording 策略控制台

支持的操作系统：

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1

要求：.NET Framework 3.5 SP1（仅限 Windows Server 2008 R2）或 .NET Framework 4.5.2 或 4.6。

在要录制会话的每台 XenApp 和 XenDesktop 服务器上安装 Session Recording Agent。

支持的操作系统：

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows 10
- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7 SP1

要求：

- 已安装 Platinum 许可证的 XenApp 7.8 或 XenDesktop 7.8
- .NET Framework 4.5.2 或 4.6
- Microsoft 消息队列 (MSMQ)，Active Directory 集成处于禁用状态，MSMQ HTTP 支持处于启用状态

支持的操作系统：

- Microsoft Windows 10
- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7 SP1

要求：.NET Framework 3.5 SP1（仅限 Windows 7）、4.5.2 或 4.6。

要获得最佳结果，在以下工作站上安装 Session Recording Player：

- 屏幕分辨率为 1024 x 768
- 颜色深度至少为 32 位
- 1 GB RAM（最低）；更多 RAM 和 CPU/GPU 资源可提高播放图形密集型录制件时的性能，特别是当录制件中有大量动画时

搜寻响应时间取决于录制件的大小和计算机的硬件规格。

通用打印服务器

通用打印服务器由客户端和服务端组件组成。UpsClient 组件包含在 VDA 安装中。UPServer 组件安装在每台打印服务器上，在用户会话中通过 Citrix 通用打印驱动程序置备的共享打印机驻留在这些打印服务器上。

以下操作系统支持 UpsServer 组件：

- Windows Server 2012 R2 和 2012
- Windows Server 2008 R2 SP1
- Windows Server 2008（32 位）

要求：Microsoft Visual C++ 2013 Runtime

对于 VDA for Windows Server OS，打印操作期间的用户身份验证要求通用打印服务器加入与 VDA 相同的域。

也可以下载独立的客户端和服务组件软件包。

有关详细信息，请参阅[准备打印机](#)一文。

其他

Citrix 建议安装或升级到在安装介质中为此版本提供的组件软件版本。

- StoreFront 需要 2 GB 内存。有关系统要求，请参阅 StoreFront 文档。StoreFront 2.6 是此版本所支持的最低版本。
- 将 Provisioning Services 与此版本结合使用时，支持的最低 Provisioning Services 版本是 7.0。
- Citrix 许可证服务器需要 40 MB 磁盘空间。有关系统要求，请参阅许可文档。仅支持 Citrix License Server for Windows。支持的最低版本是 11.13.1。

如果您将 Citrix 策略信息存储在 Active Directory 而非站点配置数据库中，则需要 Microsoft 组策略管理控制台 (GPMC)。有关详细信息，请参阅 Microsoft 文档。

支持多个网络接口卡。

默认情况下，安装 VDA 时将安装 Citrix Receiver for Windows。有关详细信息，请参阅 Citrix Receiver for Windows 文档。

有关受支持的 Microsoft App-V 版本，请参阅[App-V](#)一文。

有关本地应用程序访问支持的浏览器信息，请参阅[本地应用程序访问](#)一文。

客户端文件夹重定向 - 支持的操作系统：

- 服务器：Windows Server 2008 R2 SP1、Windows Server 2012 和 Windows Server 2012 R2
- 客户端（具有最新的 Citrix Receiver for Windows）：Windows 7、Windows 8 和 Windows 8.1

技术概述

Mar 17, 2016

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。
- 管理员管理网络并提供或限制对选定设备或全部设备的访问。
- 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 的关键功能是可以由单个站点和集成置备运行多个版本的 XenApp 或 XenDesktop。

FMA 的关键功能

典型的 XenApp 或 XenDesktop 环境包括几项关键技术组件。这些组件在用户连接到应用程序和桌面时相互作用，并记录有关站点活动的数据。

Citrix Receiver：一款安装在用户设备上的软件客户端，通过 TCP 端口 80 或 443 提供与虚拟机的连接，并使用 StoreFront Service API 与 StoreFront 通信。

Citrix StoreFront：用于对用户进行身份验证、管理应用程序和桌面并托管应用程序存储的接口。StoreFront 使用 XML 与 Delivery Controller 通信。

Delivery Controller：XenApp 或 XenDesktop 站点的中央管理组件，由用于管理资源、应用程序和桌面的服务组成，负责优化和平衡用户连接的负载。

Virtual Delivery Agent (VDA)：安装在运行 Windows 服务器或 Windows 桌面操作系统的计算机上的代理，允许这些计算机及其所托管的资源供用户使用。在运行 Windows 服务器操作系统的计算机上安装的 VDA 允许此计算机托管多个用户的多个连接，并通过以下其中一个端口连接到用户：

- 如果启用 TLS：TCP 端口 80 或端口 443
- 如果启用了通用网关协议 (CGP)（用于启用会话可靠性）：TCP 端口 2598
- 如果禁用 CGP 或用户使用旧版客户端进行连接：TCP 端口 1494

Broker Service：一种 Delivery Controller 服务，用于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 并通过 TCP 端口 80 与 Broker Agent 通信。它不可以使用 TCP 端口 443。

Broker agent：托管多个插件并收集实时数据的代理。Broker Agent 位于 VDA 上并通过 TCP 端口 80 连接到 Controller。它不可以使用 TCP 端口 443。

Monitor Service：一种 Delivery Controller 组件，用于收集历史数据并在默认情况下将其存放在站点数据库中。监视服务通过 TCP 端口 80 或 443 通信。

ICA 文件/堆栈：捆绑的用户信息，在连接到 VDA 时需要此信息。

站点数据库：Microsoft SQL Server 数据库，用于存储 Delivery Controller 的数据，如站点策略、计算机目录和交付组。

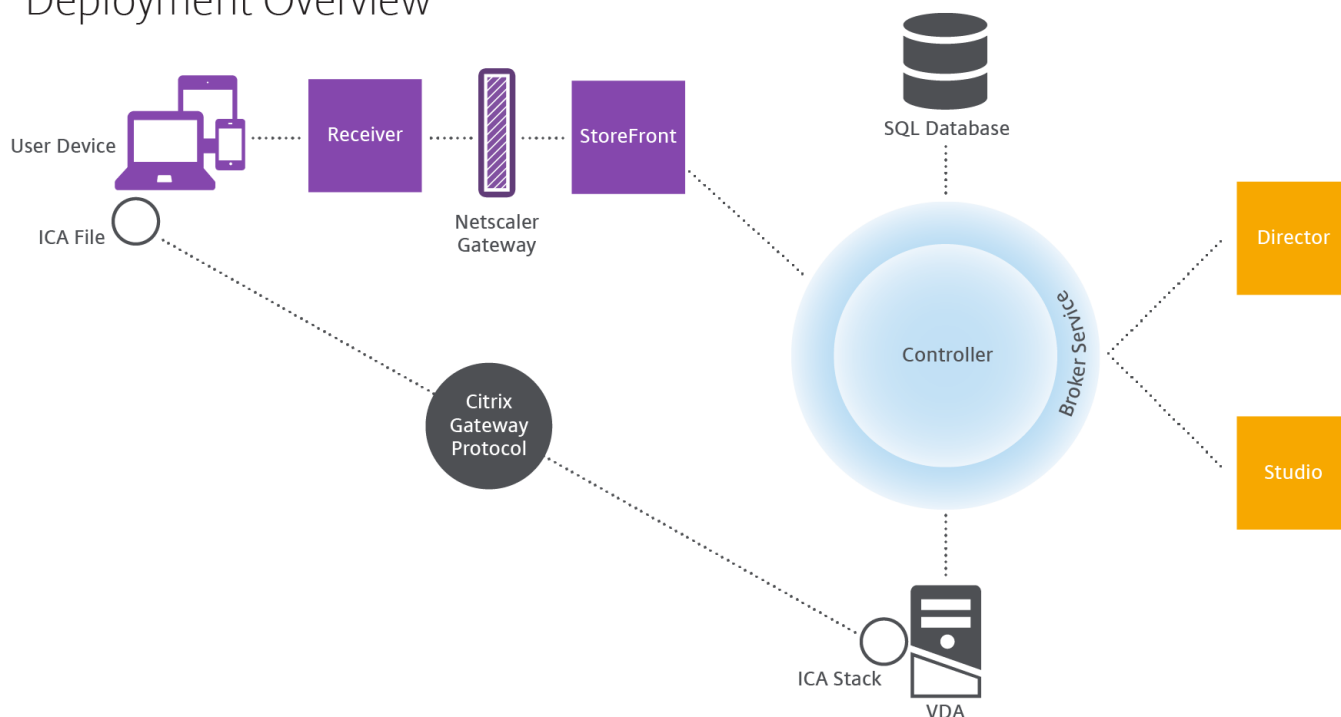
NetScaler Gateway：数据访问解决方案，使用其他凭据在 LAN 防火墙内外提供安全访问。

Citrix Director：基于 Web 的工具，允许管理员和技术支持人员访问 Broker Agent 的实时数据、站点数据库中的历史数据和 NetScaler 中的 HDX 数据，以进行故障排除和提供支持。Director 通过 TCP 端口 80 或 443 与 Controller 通信。

Citrix Studio：管理控制台，允许管理员配置和管理站点，授予对 Broker Agent 中的实时数据的访问权限。Studio 通过 TCP 端口 80 与 Controller 通信。

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，并提供设计安全的解决方案。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。

Deployment Overview



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 上以实现 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。

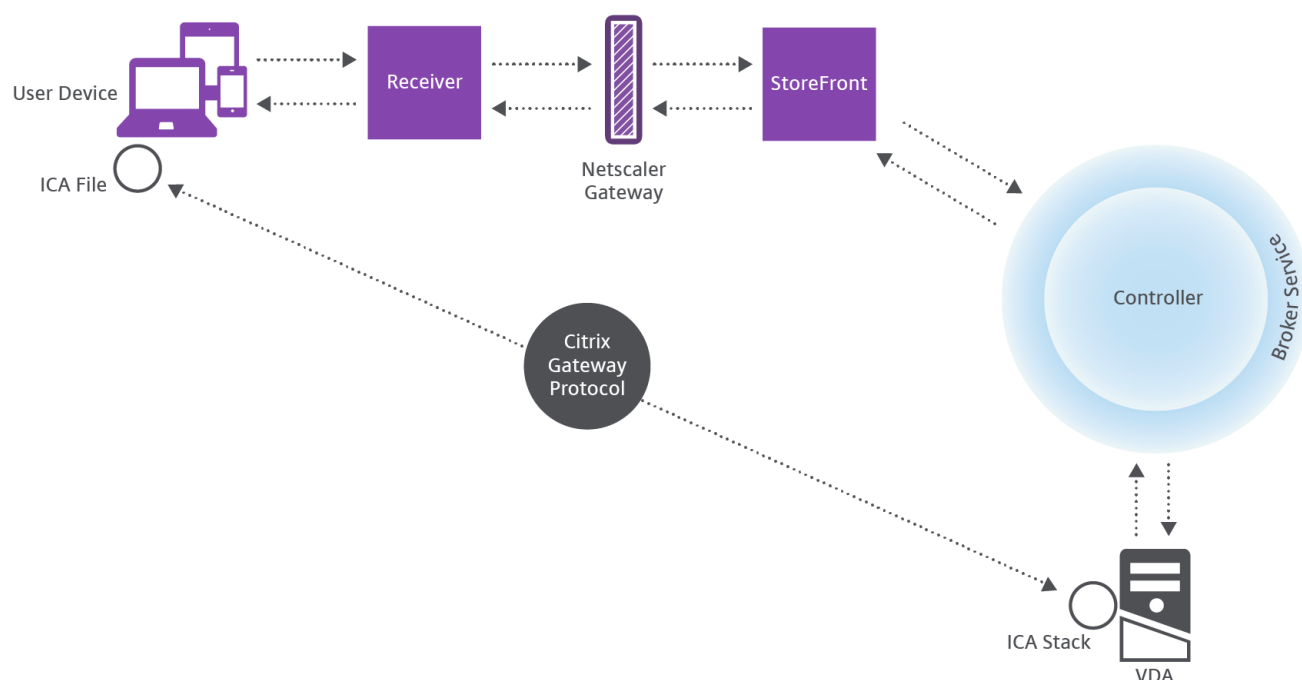
用户绝对不能直接访问 Controller。VDA 充当用户和 Controller 之间的媒介。当用户使用 StoreFront 登录到站点时，其凭据被传递到 Broker Service。Broker Service 根据为用户设置的策略获取其配置文件和可用资源。

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

在 Citrix Receiver 内部，用户选择所需的物理或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，后者通过与 Broker Service 通信确定所需的资源。建议管理员在 StoreFront 上放置一个 SSL 证书以加密来自 Receiver 的凭据。

User connections



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，并将关于用户和连接的所有数据发送给 VDA。VDA 接受连接，并将该信息按原路径返回给 Citrix Receiver。Citrix Receiver 将会话中已生成的所有信息绑定在一起，从而在用户设备上（如果 Citrix Receiver 安装在本地）或 Citrix RFW 上（如果通过 Web 访问）创建 Independent Computing Architecture (ICA) 文件。只要站点经过正确设置，凭据在整个流程均保留加密状态。

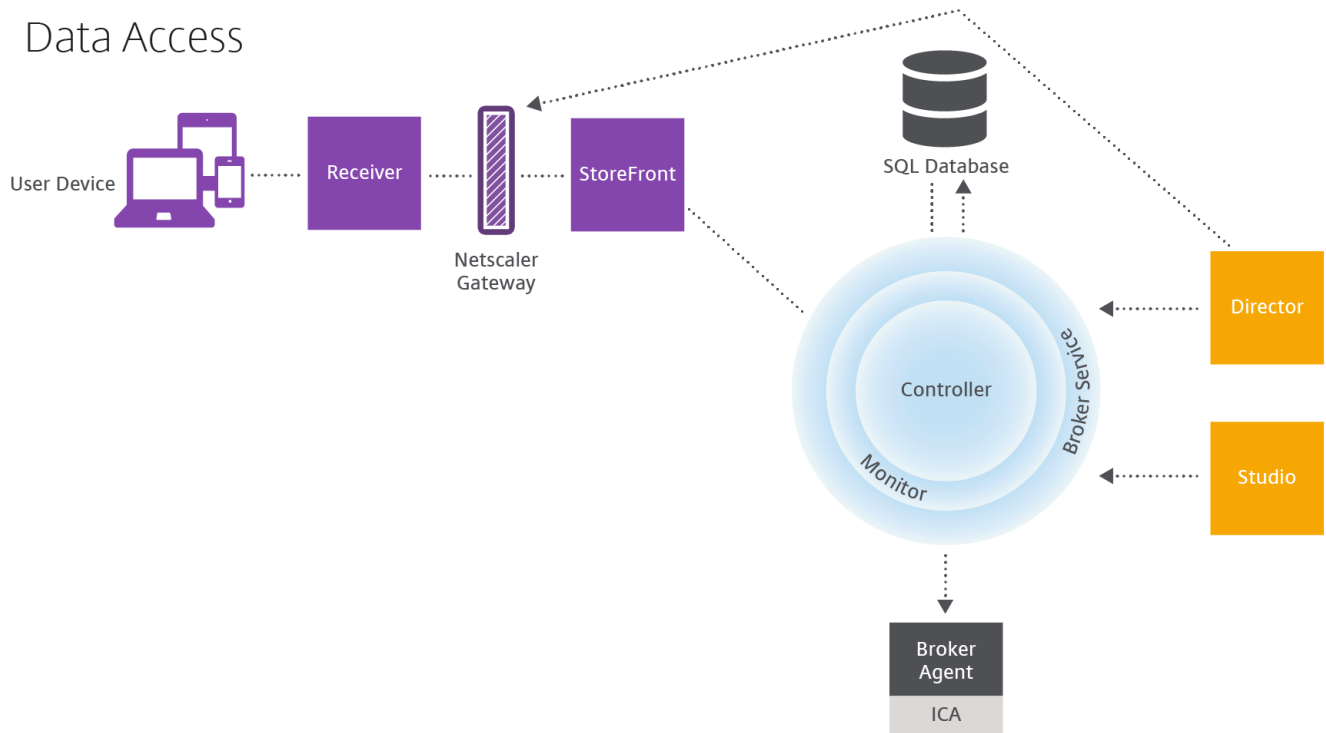
ICA 文件被复制到用户设备上，并在设备与 VDA 上运行的 ICA 堆栈之间建立直接连接。此连接绕过管理基础结构：Citrix Receiver、StoreFront 和 Controller。

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 Studio 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。

IT 可以通过 Studio 或 Director 访问每个 XenApp 或 XenDesktop 会话生成的数据。Studio 允许管理员访问 Broker Agent 中的实时数据，以便更好地管理站点。Director 可以访问此实时数据、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。

Data Access



在 Controller 内部，Broker Service 报告虚拟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存储在监视数据库中。

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

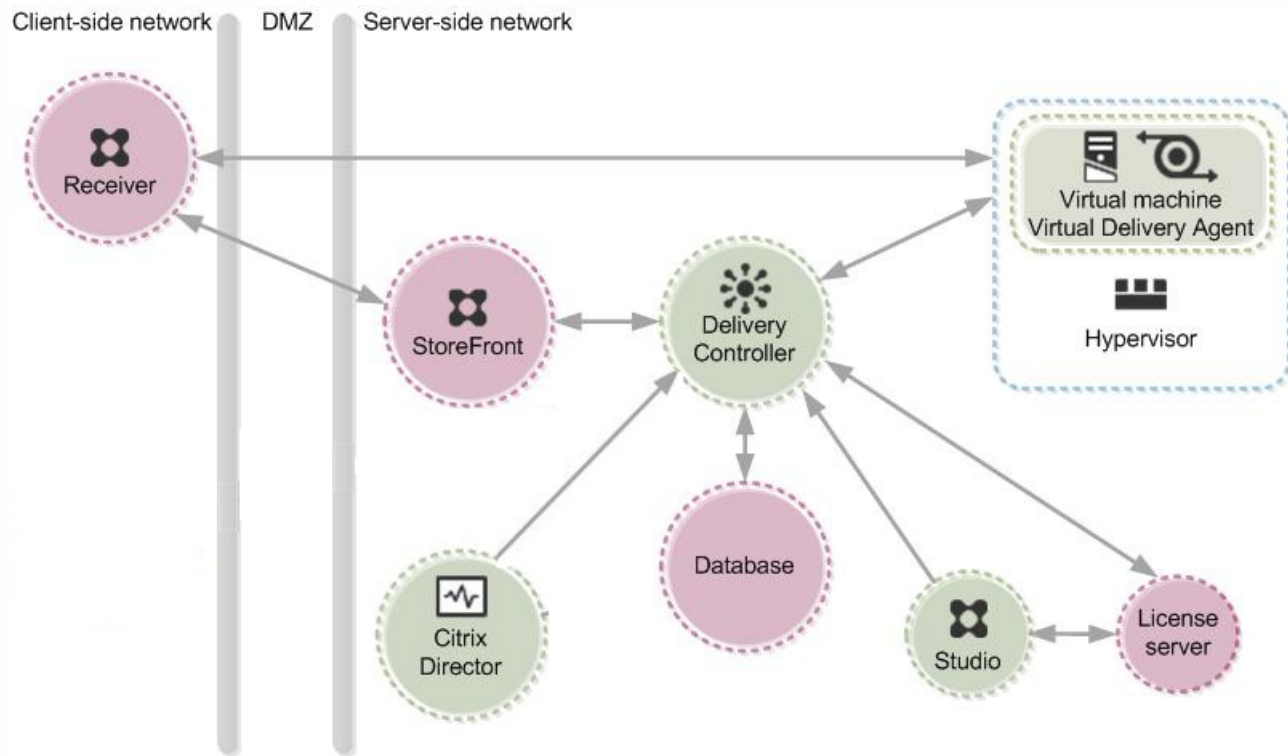
Director 还可以访问 NetScaler Gateway 以获取 HDX 数据信息。

- 概念和组件
- 交付方法

概念和组件

Jun 17, 2016

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



此图中的组件包括：

- **Delivery Controller** : Delivery Controller 是任何 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，请将 Controller 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。
各个服务的数据存储在站点数据库中。

Controller 管理桌面的状态，并根据需要和管理配置启动/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 站点至少具有一个 Microsoft SQL Server 数据库，用于存储所有配置信息和会话信息。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 建立永久连接。
- **Virtual Delivery Agent (VDA)** : VDA 安装在站点中要供用户使用的各个物理计算机或虚拟机上。它使计算机向 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。
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。

- **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，以确保在多个设备之间向用户提供一致的体验。
- **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 Web 浏览器提供连接。
- **Citrix Studio** : 是可用于配置和管理 XenDesktop 部署的管理控制台，使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。
- **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进行故障排除，以避免这些问题危及系统。此外，还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 显示来自以下位置的会话和站点信息：
 - 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** : 虚拟机管理程序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虚拟机，也可以是用于托管 XenApp 和 XenDesktop 组件的虚拟机。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。
Citrix XenServer 虚拟机管理程序包含在 XenApp 和 XenDesktop 中；可以使用其他受支持的虚拟机管理程序，例如 Microsoft Hyper-V 或 VMware vSphere。

尽管许多 XenApp 和 XenDesktop 实现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（包含在某些 XenApp 和 XenDesktop 版本中）而非 MCS 时来置备虚拟机。

XenApp 或 XenDesktop 部署中也可能包含以下其他组件（未显示在上面的插图中）：

- **Provisioning Services** : Provisioning Services 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，Provisioning Services 采用流技术将主映像推送到用户设备。Provisioning Services 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计算机。站点中包含 Provisioning Services 时，Provisioning Services 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，此版本可以使用 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。
- **Citrix CloudBridge** : 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 CloudBridge（以前称为 Citrix 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，分支机构用户将在 WAN 上体验到像 LAN 一般的性能。例如，CloudBridge 可以设置用户体验不同部分的优

优先级，以便通过网络发送大文件或打印作业时，分支机构的用户体验不会降低。带有 CloudBridge 的 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。有关详细信息，请参阅 Citrix CloudBridge 文档。

设置和分配资源：计算机目录和交付组

请通过计算机目录设置希望向用户提供的资源，但是，可以通过交付组指定能够访问这些资源的用户。

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。这些计算机及其上的应用程序或虚拟桌面是要提供给用户的资源。计算机目录中的所有计算机安装相同的操作系统和 VDA，并且，这些计算机上提供相同的应用程序或虚拟桌面。通常情况下，您创建一个主映像，然后使用该主映像在目录中创建完全相同的虚拟机。创建计算机目录时，请为目录中的计算机指定计算机的类型和置备方法。

- **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个计算机建立连接。
- **Remote PC Access**：白名单中包括的用户设备，这些设备使用户可以从任何运行 Citrix Receiver 的设备远程访问其办公室 PC 上的资源。Remote PC Access 使您可以通过 XenDesktop 部署管理对脱机 PC 的访问。

置备方法

- **Machine Creation Services (MCS)**：一组服务，可以根据需要从主映像创建虚拟服务器和桌面、优化存储利用率并在用户每次登录时为其提供虚拟机。MCS 完全集成于 Citrix Studio 中，并在其中进行管理。
- **Provisioning Services**：允许从单个共享磁盘映像实时置备或重新置备计算机。Provisioning Services 将目标设备作为一个设备集合进行管理。桌面和应用程序通过从主目标设备获得映像的 Provisioning Services 虚拟磁盘进行交付，并使您能够利用物理硬件或虚拟机的处理能力。Provisioning Services 通过其自身的控制台进行管理。
- **现有映像**：适用于已迁移到数据中心内的虚拟机的桌面和应用程序。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。

交付组

交付组是用户的集合，这些用户具有通用资源组的访问权限。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 组和交付组都是将具有相似要求的用户分成一组，因此，通常按照用户所在的 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。可以设置一个交付组以交付应用程序、桌面或同时交付两者。可以定义交付组中的用户能够访问的资源。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。

XenApp 和 XenDesktop 7.x 与 XenApp 6.5 和早期版本之间的区别

如果您熟悉 XenApp 6.5 和 XenApp 的早期版本，可能会有助于您了解 XenApp 和 XenDesktop 7.x 与这些较早版本的不同之处。

注意：在本部分内容中，7.x 是指 XenApp 7.5 或更高版本以及 XenDesktop 7 或早期版本。

尽管并不完全相同，但以下表格可帮助您将 XenApp 6.5 和早期版本中的功能元素与 XenApp 7.x 和 XenDesktop 7.x 中的功能元素对应起来：

XenApp 6.5 和更早版本中被代替的元素：	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
负载评估程序	负载管理策略
管理员	委派的管理员 角色 作用域

XenApp 7.x 和 XenDesktop 7.x 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 则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端软件。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和交付组来管理计算机、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。
- **Virtual Delivery Agents (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。
- **Citrix Studio 和 Citrix Director**：使用 Studio 控制台配置环境并为用户提供对应用程序和桌面的访问权限。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。
- **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更少的计算机。在 XenApp 7.x 和 XenDesktop 7.x 中，则使用负载管理策略跨多个计算机平衡负载。
- **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向其分配权限。在 XenApp 7.x 和 XenDesktop 7.x 中，则基于角色和作用域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。

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 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	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。连接租用功能是对 SQL Server 高可用性最佳实践的补充。请参阅 连接租用 。
应用程序流技术推送	App-V 提供流应用程序，并使用 Studio 进行管理。
Web Interface	Citrix 建议过渡到 StoreFront。
SmartAuditor	使用 Session Recording。还可以使用配置日志记录从管理角度记录所有会话活动。

Active Directory

Mar 17, 2016

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。

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：

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。

- 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：

- 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\brokeragent.config.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.config.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](#)。

数据库

Jul 26, 2016

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，现有连接将继续正常运行，直到用户注销或断开连接。如果数据库服务器不可用，新连接将无法建立，某些配置了连接租用的情况除外。

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。有关说明，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** — 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/en-us/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，您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 高可用性最佳实践。有关详细信息，请参阅[连接租用](#)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](#)。

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。

此安装程序使用默认 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。数据库可以位于一个或多个计算机上。

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。

如果稍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。

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。

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，如果需要，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。

- 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 组成员关系获取。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 XenDesktop 数据库的镜像角色中的数据库服务器	securityadmin *	

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. 选择要为其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。

交付方法

Mar 17, 2016

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。

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

升级物理计算机是一项艰巨的任何，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。不断增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。

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，如键盘、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。

切换到新操作系统时，IT 可能会面临交付旧版和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

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政压力。

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。

所有文件存储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。

维护足够的员工以应对高峰期，同时又不会在不忙时过度配置计算机，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标准桌面的访问权限。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。

XenApp 发布的应用程序和桌面

Mar 17, 2016

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。

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。

VM 托管应用程序

Mar 17, 2016

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。

在旧版操作系统（如 Windows XP 或 Windows Vista）或旧版体系结构（32 位或 16 位）上运行的应用程序。通过将每个应用程序隔离在其各自的虚拟机上，如果一台计算机发生故障，也不会影响其他用户。

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。

VDI 桌面

Mar 17, 2016

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。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，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。定义有关计算机目录的桌面体验时，确定用户在每次登录时连接到新的 VM 还是在每次登录时连接到同一台计算机，并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。

安装和配置

May 12, 2016

请在开始执行每个部署步骤之前查看参考文章，以便熟悉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](#)一文，并完成所有必要的任务。这些任务包括：

- 熟悉 XenApp 和 XenDesktop – 阅读该文章后，您将知晓从何处查找与概念、功能、与早期版本的区别、系统要求以及数据库有关的信息。
- 设置虚拟化、托管或支持环境（如果使用其中一种）。
- 设置要在上面安装组件的计算机。
- 设置 Active Directory 环境。

本文还介绍安装组件和启用功能时需要选择或指定的信息。

如果要安装 Linux VDA，请务必在开始安装之前查看 [Red Hat Linux VDA](#) 和 [SUSE Linux VDA](#)。

安装核心组件

安装 Delivery Controller、Citrix Studio、Citrix Director、Citrix 许可证服务器和 Citrix StoreFront。可以使用基于向导的[图形界面](#)或[命令行界面](#)，这样可以启用通过脚本进行安装。两种方法都会自动安装大部分必备组件。

创建站点

安装核心组件并启动 Studio 后，系统会自动使用“站点创建”向导引导您完成[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，在要用于创建虚拟机的主映像上或直接在每个计算机上安装均可。可以使用[图形界面](#)或[命令行界面](#)。如果要通过 Active Directory 安装 VDA，还提供示例[脚本](#)。

对于安装了 Linux 操作系统的计算机，请按照安装 [Red Hat Linux VDA](#) 或 [SUSE Linux VDA](#) 的说明进行操作。

对于 Remote PC Access 部署，请在每个办公 PC 上安装 VDA for Desktop OS；为提高效率，请使用[独立的 VDA 安装程序的命令行界面](#)以及现有的电子软件分发 (Electronic Software Distribution, ESD) 方法。

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。可以使用[图形界面](#)或[命令行界面](#)。

(可选) 在 XenApp 或 XenDesktop 部署中集成其他 Citrix 组件。例如：

- 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。请参阅 Provisioning Services 文档。
- 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。请参阅 Citrix NetScaler Gateway 文档。
- Citrix CloudBridge 是一套用于优化 WAN 性能的设备。请参阅 Citrix CloudBridge 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。如果要使用受支持的虚拟机管理程序或云服务提供 VM，必须先在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计算机目录中的计算机以及可供这些用户使用的应用程序。

准备安装

Apr 25, 2016

在本文中：

- [常规安装指南](#)
- [安装核心组件时需要指定的内容](#)
- [VDA 安装指南](#)
- [安装 VDA 时需要指定的内容](#)

常规安装指南

- 如果您不熟悉本产品及其组件，请查看[技术概览](#)一文。如果您的当前部署为 XenApp 6.x 或更低版本，请参阅[概念和组件](#)一文，其中列出了 XenApp 和 XenDesktop 7.x 之间的区别。
- 规划部署时，请参阅[安全](#)一文。
- 有关您可能会遇到的安装问题，请查看[已知问题](#)一文。
- 如果使用受支持的虚拟机管理程序或云服务为应用程序和桌面提供虚拟机，请在安装组件后创建站点时配置与该主机之间的第一个连接。但是，可以在之前的任何时间配置虚拟化环境。请参阅[此处](#)列出的信息来源。
- 如果使用 Microsoft System Center Configuration Manager 管理对应用程序和桌面的访问权限，请参阅[本文](#)。
- 如果某个组件具有 .NET 必备项，则安装程序将部署所需的 .NET 版本（如果此版本尚未安装）。安装 .NET 可能需要重新启动计算机。
- 请参阅[数据库](#)一文，了解系统数据库的相关信息以及如何配置这些数据库。安装 Controller 过程中，可以选择是否在同一服务器上安装 Microsoft SQL Server 2012 Express。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。
- 安装 Citrix 许可证服务器时，该用户帐户会自动成为许可证服务器上的完全权限管理员。有关详细信息，请参阅[委派管理](#)一文。
- 在安装前、安装期间和安装完成后创建对象时，最好为每个对象（例如，网络、组、目录和资源）指定唯一的名称。
- 如果组件未成功安装，此过程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。
- Citrix Studio 在安装后自动启动。使用图形界面时，可以在向导的最后一个页面上禁用此操作。
- 可以使用产品 ISO 中包含的安装程序安装核心组件和 Virtual Delivery Agent (VDA)；此过程称为“完整产品安装程序”。要安装 VDA，可以使用完整产品安装程序或独立的 VDA 安装程序（可以从产品下载站点获取）。这两种安装程序都提供[图形界面](#)和[命令行界面](#)。
- 产品安装介质包含用于在 Active Directory 中安装、升级或删除计算机组的 VDA 的示例脚本。也可以将脚本应用于单个计算机，并用来管理 Machine Creation Services 和 Provisioning Services 使用的主映像。有关详细信息，请参阅[使用脚本安装 VDA](#)一文。
- 可以使用完整产品安装程序通过图形界面或命令行界面在打印服务器上安装通用打印服务器服务器组件的服务器组件 (UpsServer)。产品下载站点可能还包含 UpsServer 下载软件包。
- 产品 ISO 中不再包含 Citrix Receiver for Mac 和 Citrix Receiver for Linux 的各个版本。您（或您的用户）可以从 Citrix Web 站点下载并安装 Citrix Receiver。此外，可以在 StoreFront 服务器上提供这些 Citrix Receiver（请参阅 StoreFront 3.0.x 文档中的[在服务器上提供 Citrix Receiver 安装文件](#)部分，或者参阅您正在使用的 StoreFront 版本中的等效内容）。

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，必须在开始安装之前提升管理权限，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](#)一文列出了受支持的 Active Directory 功能级别。[Active Directory](#)一文中包含其他支持信息。
- 必须至少有一个运行 Active Directory 域服务的域控制器。
- 请勿尝试在域控制器上安装任何组件。
- 在 Studio 中指定组织单位名称时，请勿使用正斜杠 (/)。
- 请参阅 Microsoft 文章，了解 Active Directory 配置说明。

确定组件的安装位置，然后准备计算机和操作系统。

- 参阅[系统要求](#)一文，了解 Controller、Studio、Citrix Director、虚拟化资源（主机）和 VDA 支持的操作系统及版本。大部分组件必备项都是自动安装的；该文章中还注明了例外项。参阅 Citrix StoreFront 和 Citrix 许可证服务器文档，了解支持的平台。
- 您可以将核心组件安装在同一服务器或不同服务器上。例如，要远程管理较小的部署，可以将 Studio 与 Controller 安装在不同服务器上。为适应将来的扩展，请考虑将组件安装在单独的服务器上；例如，将许可证服务器和 Director 安装在不同的服务器上。
- 可以在相同的服务器上安装 Delivery Controller 和适用于 Windows 服务器操作系统的 Virtual Delivery Agent。为此，请启动安装程序并选择 Delivery Controller（以及要在该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适用于 Windows 服务器操作系统的 Virtual Delivery Agent。
- 请勿在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。
- 确保每个操作系统都具有最新更新。
- 确保所有计算机具有同步的系统时钟。对于 Kerberos 基础结构而言，必需实现同步，以保护计算机之间的通信。

安装核心组件时需要指定的内容

以下部分说明了您在安装过程中看到和指定的内容。遵循[图形界面向导](#)的顺序；此外，还提供了等效[命令行](#)选项。安装文章提供了与如何启动向导和发布带选项的命令有关的详细信息。

选择或指定是否安装 Microsoft SQL Server Express。如果您不熟悉数据库，请查看[数据库](#)一文。（命令行选项：/nosql，用于阻止安装）

安装 Director 时，自动安装 Windows 远程协助。可以选择是否在 Windows 远程协助中启用阴影操作以与 Director 用户阴影操作结合使用，并打开 TCP 端口 3389。默认启用此功能。（命令行选项：/no_remote_assistance）

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，以下端口也会自动打开。如果使用第三方防火墙或未使用防火墙，或者更喜欢亲自打开，则可以禁用此默认操作，然后手动打开端口。有关此产品及其他 Citrix 产品的完整端口信息，请参阅 [CTX101810](#)。（命令行选项：/configure_firewall）

- Controller：TCP 80、443
- Director：TCP 80、443
- 许可证服务器：TCP 7279、8082、8083、27000
- StoreFront：TCP 80、443

VDA 安装指南

- VDA 安装程序提供[图形界面](#)和[命令行界面](#)。
- 请查看[系统要求](#)一文，了解 VDA 支持的操作系统和版本。大部分组件必备项都是自动安装的；该文章中还注明了例外项。安装 VDA for Windows Server OS 时，Remote Desktop Services 角色服务会自动安装并启用（如果尚未安装和启用）。
- 如果要在 Windows 7 或 Windows Server 2008 R2 计算机上安装 VDA，请先确认是否已安装 .NET 3.5.1，然后再开始安装 VDA。下面的[重新启动](#)部分介绍了其他安装必备项的注意事项。
- 默认情况下，在受支持的 Windows 服务器上启用后台打印程序服务。如果禁用了此服务，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。

- 安装 VDA 期间，将自动安装 Profile Management。虽然您可以在使用命令行界面时将此组件排除在外，但会影响包含 Director 的 VDA 的监视和故障排除。
- 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 Windows Desktop OS 上，此用户组仅适用于 RDP 连接；在 VDA for Windows Server OS 上，此用户组则适用于 ICA 和 RDP 连接。
- 对于 Remote PC Access 配置，请在用户将远程访问的每台物理办公室 PC 上安装 VDA for Windows Desktop OS。请勿启用优化功能。
- 如果要在运行受支持的 Linux 操作系统上安装 VDA，请参阅 [Red Hat Linux VDA](#) 或 [SUSE Linux VDA](#) 了解基础信息。
- VDA 必须具有有效的控制器地址才能进行通信，否则无法建立会话。您可以在安装 VDA 时指定控制器地址，也可以稍后再指定该地址；但请记住，必须执行此操作！有关详细信息，请参阅下面的 [Delivery Controller 地址](#) 部分。
- 在 Windows Server 2012 R2 系统上安装 VDA for Server OS 后，请使用 Kerberos Enable Tool (XASsonKerb.exe) 以确保 Citrix Kerberos 身份验证正确运行。此工具位于安装介质上的“Support”（支持）>“Tools”（工具）>“XASsonKerb”文件夹；必须具有本地管理员权限才能使用此工具。请从服务器上的命令提示窗口运行 **xassonkerb.exe -install**。如果稍后应用更改注册表位置 HKLM\System\CurrentControlSet\Control\LSA\OSConfig 的更新，请重新运行命令。要查看所有可用工具选项，请运行带有 -help 参数的命令。

可以使用完整产品安装程序或独立的安装程序包安装 VDA。这两种安装程序都提供图形界面和命令行界面。

完整产品安装程序会自动检测您的操作系统，并允许您仅在该系统上安装支持的 Windows VDA：VDA for Windows Server OS 或 VDA for Windows Desktop OS。

独立的 VDA 安装程序包

较小的独立软件包可以更轻松地容纳使用本地暂存或复制的电子软件分发 (ESD) 程序包、具有物理机或远程办公室的部署。独立的程序包主要用于使用命令行（无提示）安装的部署，支持的命令行参数与完整产品安装程序使用。该程序包还提供与完整产品安装程序等效的图形界面。

[如何使用独立 VDA 安装程序的图形界面。](#)

[如何使用独立 VDA 安装程序的命令行界面。](#)

有两种独立的自解压 VDA 安装程序包：一种用于在受支持的服务器操作系统上执行安装，另一种用于受支持的工作站（桌面）操作系统计算机。

默认情况下，该程序包中的文件将提取到 Temp 文件夹中。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。提取到 Temp 文件夹的文件将自动删除，但您可以在安装完成后手动将其删除（从 C:\Windows\Temp\Ctx-* 中，其中 * 为随机全局唯一标识符）。或者，可以使用 /extract 命令与绝对路径。

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/>。

VDA 安装结束时需要重新启动计算机。

如果要尽量减少安装过程中需要额外重新启动的次数，请执行以下操作：

- 请务必在安装之前安装受支持的 .NET Framework 版本。
- 对于 Windows Server 操作系统计算机，请在安装 VDA 之前安装并启用 RDS 角色服务。

其他必备项通常不要求重新启动计算机，因此您可以允许安装程序自动为您处理。

如果在开始安装 VDA 之前未安装必备项，但为命令行安装指定了 /noreboot 选项，则必须管理重新启动。例如，使用自动必备项部署功能时，安装程序将在安装 RDS 后暂停，等待重新启动；请务必在重新启动计算机之后再次运行该命令以继续安装。

VDA。

Windows XP 或 Windows Vista 不支持最新版本的 VDA；此外，不能在这些操作系统上使用本版本以及其他较新版本中的某些功能。Citrix 建议您将这些系统替换为当前支持的 Windows 桌面操作系统版本，然后安装此版本中的 VDA。如果必须继续容纳运行 Windows XP 或 Windows Vista 的计算机，可以安装早期的 Virtual Desktop Agent 版本（包含某些修补程序的 5.6 FP1）。有关详细信息，请参阅 [CTX140941](#)。请谨记：

- 不能在 Windows XP 或 Windows Vista 系统上安装核心组件（Controller、Studio、Director、StoreFront、许可证服务器）。
- 如果您使用的是 Windows XP 或 Windows Vista 系统，则在创建包含这些计算机的计算机目录时，请确保在“主映像”页面的“选择... 安装的 VDA 版本”列表框中选择 5.6 FP1 条目。
- Windows Vista 系统不支持 Remote PC Access。
- Microsoft 已于 2014 年 4 月 8 日终止对 Windows XP 提供支持，此时 Citrix 不再支持 Windows XP。
- 继续使用旧的 VDA 可能会影响功能的可用性以及向 Controller 注册 VDA，请参阅混合环境注意事项。

安装 VDA 时需要指定的内容

以下部分说明了您在安装过程中指定的内容。遵循图形界面向导的顺序；此外，还提供了等效的命令行选项。安装文章提供了与如何启动向导或发布带选项的命令有关的详细信息。

安装完 VDA 后，请查看 [VDA 安装指导](#) 以核对您可能需要完成的任务。

VDA 环境指定您将如何使用 VDA：

- 默认“主映像”选项指示您将使用 Machine Creation Services (MCS) 或 Provisioning Services 根据在虚拟机管理程序或云服务中创建的主映像创建虚拟机。请在主映像上安装 VDA。（命令行选项：/masterimage）
- “Remote PC Access”选项指示您将在物理机或未配置 VDA 的 VM 上安装 VDA。

安装 VDA for Windows Desktop OS 时，系统会提供用于安装标准 VDA 或 HDX 3D Pro 版 VDA 的选项。

- 建议为大部分桌面选择标准 VDA，包括启用了 Microsoft RemoteFX 的桌面。这是默认安装的版本。
- VDA for HDX 3D Pro 优化了图形密集型程序和富媒体应用程序的性能。如果计算机将访问图形处理器以进行 3D 渲染，建议选择此版本。（命令行选项：/enable_hdx_3d_pro）

组件默认安装在 C:\Program Files\Citrix 中。可以在安装过程中指定其他位置，但该位置必须具有网络服务的执行权限。（命令行选项：/installdir，用于指定非默认目录）

默认情况下会随 VDA 安装 Citrix Receiver for Windows。可以禁用此默认操作。（命令行选项：使用 /components vda 可阻止安装 Citrix Receiver）

可以在安装 VDA（建议）时或以后指定已安装的 Controller 的地址 (FQDN)。虽然不要求您在安装 VDA 时指定 Controller 地

址，但请记住，如果未提供此信息，则不能在 Controller 中注册 VDA。如果 VDA 无法注册，包含这些 VDA 的计算机上的用户将无法访问其应用程序和桌面。（命令行选项：/controllers）

- 如果您在安装 VDA 时指定了 Controller 的 FQDN，安装程序将尝试连接到指定地址。如果连接尝试失败，安装程序将提供信息消息。
- 如果选择在以后指定 Controller 地址，安装程序将提醒您该要求。如果安装了 VDA，但未指定 Controller 地址，可以在以后重新运行安装程序，或者使用 Citrix 组策略。

如果在 VDA 安装期间以及在组策略中指定了 Controller 地址，这些策略设置将替代安装过程中提供的设置。

请记住，还需要打开用于与 Controller 进行通信的防火墙端口，才能成功注册 VDA。

在初次指定 Controller 位置（安装 VDA 时或以后）之后，可以在安装其他 Controller 时使用自动更新功能更新 VDA。

有关 VDA 如何发现并在 Controller 中注册的详细信息，请参阅 [Delivery Controller](#) 一文。

可以启用或禁用与 VDA 结合使用的以下功能：

- **Optimize performance:**（优化性能：）（默认启用）如果选择了此功能，则会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](#)。如果要使用 Remote PC Access，请勿启用此选项。（命令行选项：/optimize）
- **Use Windows Remote Assistance:**（使用 Windows 远程协助：）（默认启用）如果选择了此功能，Windows 远程协助将与 Director 的用户重影功能结合使用，并且 Windows 会自动在防火墙中打开 TCP 端口 3389，即使您选择手动打开防火墙端口也是如此。（命令行选项：/enable_remote_assistance）
- **Use Real-Time Audio Transport for audio:**（对音频使用实时音频传输：）（默认启用）如果选择了此功能，则会对音频数据包使用 UDP，这样可以提高音频性能。（命令行选项：/enable_real_time_transport）
- **Framehawk：**（默认启用）如果选择了此功能，则会打开双向 UDP 端口 3224-3324。（您可以稍后使用 Citrix 策略设置“Framehawk 显示通道端口范围”来更改端口范围；然后，您必须打开本地防火墙端口。）所有内部（VDA 到 Citrix Receiver；或者 VDA 到 NetScaler Gateway）和外部（NetScaler Gateway 到 Citrix Receiver）防火墙都必须打开 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）
- **Install Citrix App-V publishing components:**（安装 Citrix App-V 发布组件：）（默认启用）如果要使用 Microsoft App-V 软件包中的应用程序，请选择此功能。有关详细信息，请参阅 [App-V](#) 一文。（命令行选项：/install_appv）
- **个人虚拟磁盘：**（默认启用；只有在 VM 上安装 VDA for Desktop OS 时才可用）。如果选择了此功能，则可以将个人虚拟磁盘与主映像结合使用。有关详细信息，请参阅 [个人虚拟磁盘](#) 一文。（命令行选项：/baseimage）

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，以下端口也会自动打开。如果使用第三方防火墙或未使用防火墙，或者更喜欢亲自打开，则可以禁用此默认操作，然后手动打开端口。有关端口的完整信息，请参阅 [CTX101810](#)。（命令行选项：/enable_hdx_ports）

- 控制器通信：TCP 80、1494、2598 和 8008。要在用户设备与虚拟桌面之间进行通信，请将端口 1494 和 2598 上的入站 TCP 配置为端口例外。为安全起见，Citrix 建议您不要将这些已注册的端口用于除 ICA 协议和通用网关协议之外的任何用途。要在 Controller 与虚拟桌面之间进行通信，请将入站端口 80 配置为端口例外。
- 远程协助：TCP 3389。如果在上一页中启用了 Windows 远程协助功能，则即使选择手动打开端口，Windows 也会自动打开该端口。
- 实时音频：UDP 16500-16509。

- Framehawk : UDP 3224-3324。

查看完所提供的信息并单击**安装**后，系统将显示安装进度。安装完毕后，必须重新启动计算机，才能使用 VDA。

VMware 虚拟化环境

Jun 17, 2016

如果您使用 VMware 提供虚拟机，请按本指导操作。

1. 安装 vCenter Server 以及相应的管理工具。（不支持 vSphere vCenter 链接模式操作。）
2. 创建在数据中心级至少具有以下权限的 VMware 用户帐户。此帐户具有创建新 VM 的权限，用来与 vCenter 进行通信。

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
System.Anonymous、System.Read 和 System.View	自动添加。
Task.Create	任务 > 创建任务
VirtualMachine.Config.AddRemoveDevice	虚拟机 > 配置 > 添加或删除设备
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.CPUCount	虚拟机 > 配置 > 更改 CPU 计数
VirtualMachine.Config.Memory	虚拟机 > 配置 > 内存
VirtualMachine.Config.RemoveDisk	虚拟机 > 配置 > 删除磁盘
VirtualMachine.Config.Resource	虚拟机 > 配置 > 更改资源

SDK	用户界面
VirtualMachine.Config.Settings	虚拟机 > 配置 > 设置
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
VirtualMachine.Inventory.Create	虚拟机 > 清单 > 新建
VirtualMachine.Inventory.CreateFromExisting	虚拟机 > 清单 > 从现有项创建
VirtualMachine.Inventory.Delete	虚拟机 > 清单 > 删除
VirtualMachine.Inventory.Register	虚拟机 > 清单 > 注册
VirtualMachine.Provisioning.Clone	虚拟机 > 置备 > 克隆虚拟机
VirtualMachine.Provisioning.CloneTemplate	虚拟机 > 置备 > 克隆模板
VirtualMachine.Provisioning.DiskRandomAccess	虚拟机 > 置备 > 允许磁盘访问
VirtualMachine.Provisioning.GetVmFiles	虚拟机 > 置备 > 允许虚拟机下载
VirtualMachine.Provisioning.PutVmFiles	虚拟机 > 置备 > 允许虚拟机文件上载
VirtualMachine.Provisioning.DeployTemplate	虚拟机 > 置备 > 部署模板
VirtualMachine.Provisioning.MarkAsVM	“Virtual machine”（虚拟机）>“置备”>“Mark as virtual machine”（标记为虚拟机）
VirtualMachine.State.CreateSnapshot	vSphere 5.0、Update 2 和 vSphere 5.1、Update 1 : “Virtual machine”（虚拟机）>“状态”>“Create snapshot”（创建快照） vSphere 5.5 : “Virtual machine”（虚拟机）>“Snapshot management”（快照管理）>“Create snapshot”（创建快照）
VirtualMachine.State.RemoveSnapshot	vSphere 5.0、Update 2 和 vSphere 5.1、Update 1 : “Virtual machine”（虚拟机）>“状态”>“Remove snapshot”（删除快照） vSphere 5.5 : “Virtual machine”（虚拟机）>“Snapshot management”（快照管理）>“Remove

SDK	snapshot" (删除快照) 用户界面
VirtualMachine.State.RevertToSnapshot	vSphere 5.0、Update 2 和 vSphere 5.1、Update 1 : "Virtual machine" (虚拟机) > "状态" > "Revert to snapshot" (还原为快照) vSphere 5.5 : "Virtual machine" (虚拟机) > "Snapshot management" (快照管理) > "Revert to snapshot" (还原为快照)

3. 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。

4. 要创建 AppDisk，用户帐户必须具有下列附加权限：

SDK: VirtualMachine.Config.EditDevice
User Interface: Virtual machine > Configuration > Modify Device Settings

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 安装的自签名证书。在每个 Controller 中添加 VMware vCenter 证书。请执行以下过程：

- 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。
- 使用以下任意方法获取 vCenter 证书：
 - 从 vCenter Server：
 - 将 rui.crt 文件从 vCenter Server 复制到 Delivery Controller 上可访问的位置。
 - 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。
 - 打开 Web 浏览器，与 vCenter Server 建立安全 Web 连接，例如 https://server1.domain1.com
 - 接受安全警告。
 - 单击显示证书错误的地址栏。
 - 查看证书并单击详细信息选项卡。
 - 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。
 - 保存导出的证书。
 - 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：
 - 打开 Web 浏览器，与 vCenter Server 建立安全 Web 连接，例如 https://server1.domain1.com。
 - 接受安全警告。
 - 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 或 Windows Server 2012 R2：
 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。

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。

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。以域/用户名格式指定用户名。

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。

Microsoft System Center Virtual Machine Manager 虚拟化环境

Mar 17, 2016

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：

- VMM 2012 — 提供改进的管理功能，使您能够管理整个虚拟化数据中心以及虚拟机。此版本现在可安排群集主机修补以及与 Windows Server Update Services 的集成，以允许您定义每个主机所需的修补程序的基线。
- VMM 2012 SP1 — 在具有群集共享卷和存储区域网络 (SAN) 的文件服务器上使用 SMB 3.0 时，可提供有关 Machine Creation Services (MCS) 的性能改进。这些文件共享可在 SAN 存储上提供低成本缓存并降低 IO，从而提高性能。
- VMM 2012 R2 — 实现了主要 Windows Server 2012 R2 功能的现有规模管理，包括运行 VM 快照、动态调整 VHDX 的大小以及存储空间。

此版本仅支持安装了 VMM 2012 R2 的第一代虚拟机。Machine Creation Services (MCS) 和 Provisioning Services 部署不支持第二代虚拟机。使用 MCS 或 Provisioning Services 创建 VM 时，第二代 VM 不出现在主 VM 的选择列表中；它们默认启用 Secure Boot，从而防止 VDA 正常工作。

- 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 升级到 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）

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。
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。

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, $vhdaText) $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 = $ims.CreateVirtualHardDisk($vhdaText); $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。
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。如果您所具有的路径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建该目录可避免 VMM 命令失败。

对于 Hyper-V 计算机，请在存储上执行 mkdir。

Microsoft Azure 虚拟化环境

Mar 17, 2016

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; sdjfl klasdfilaskjdf kluqweiopruaiopdfaklsdjfjsdiltf asdklf;feriouip" />
```

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

	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。

对于美国标价，每种 VM 实例类型的每小时成本可从以下网址获取：
<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。对于概念证明或其他测试活动，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。

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/en-us/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。

Microsoft System Center Configuration Manager 环境

Mar 17, 2016

通过这些集成选项，使用 System Center Configuration Manager (Configuration Manager) 2012 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** – 无论您的环境是否包含 Citrix Connector，使用 Remote PC Access 局域网唤醒功能均需要 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。

属性可供 Microsoft System Center Configuration Manager 2012 和 2012 R2 管理虚拟桌面之用。

在 Configuration Manager 2012 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）。

属性	说明
IsVirtualMachine	Cleared : 在从该映像置备的 VM 上。 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。
PersonalDiskDriveLetter	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。有关这些任务的信息，请参阅 <http://support.citrix.com/article/ctx140905>。

- 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。

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 Configuration Manager 2012，然后将 Configuration Manager 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 Configuration Manager 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。
- 要支持 Configuration Manager 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。
 - 要获取 Configuration Manager 唤醒代理支持，请在 Configuration Manager 中启用此选项。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：Configuration Manager 地址和访问凭据以及名称。

- 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使用 Configuration Manager 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](#) 一文。

使用图形界面进行安装

Mar 17, 2016

注意：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 [Red Hat Linux VDA](#) 和 [SUSE Linux VDA](#)。

在本文中：

- [简介](#)
- [使用完整产品安装程序](#)
- [使用独立的 VDA 安装程序](#)
- [自定义 VDA](#)

简介

重要：开始执行任何安装之前，请查看[准备安装](#)一文，文章介绍了安装程序以及您应在安装之前熟悉的任何内容。此外，该文章还将引导您完成在图形界面向导中看到和指定的项目。本文介绍了如何启动产品安装程序中的图形界面。

可以使用图形界面执行以下操作：

- 安装一个或多个核心组件：Delivery Controller、Citrix Studio、Citrix Director、许可证服务器和 StoreFront。
- 在主映像、虚拟机或物理机上安装 Virtual Delivery Agent (VDA)。还可以对介质上提供的脚本进行自定义，然后使用这些脚本在 Active Directory 中安装和删除 VDA。
- 自定义先前安装的 VDA。
- 安装“通用打印服务器”服务器组件。Controller 已具备“通用打印服务器”客户端功能；您只需在环境中的打印服务器上安装 UpsServer 组件。安装该组件后，请按照“配置打印机”一文中的配置说明进行操作。
- 升级组件；请参阅[升级部署](#)一文。

完整产品安装程序和独立的 VDA 安装程序都有图形界面。

使用完整产品安装程序

可以使用完整产品安装程序安装核心组件、VDA 和“通用打印服务器”服务器组件。

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，登录要在安装组件的服务器。
4. 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。
5. 选择要安装 XenApp 还是 XenDesktop。
6. 选择要安装的组件：
 - 如果刚刚开始安装，请在左侧列中选择 **Delivery Controller**。在向导继续进行的过程中，可以选择要在运行安装程序的计算机上安装的组件（Delivery Controller、Studio、Director、许可证服务器、StoreFront）。
 - 如果已经安装了一些组件并且希望对部署进行扩展，请在右侧的列中单击要安装的组件。此列提供核心组件和通用打印服务器。
 - 要安装 VDA，请单击中间列中可用的 VDA 项；安装程序可以为运行安装程序的操作系统选择合适的版本。

按照向导提示操作。记住：[准备安装](#)一文提供与您在向导中看到和指定的信息有关的指南。如果要安装 VDA，则在安装完成时默认启用自动重新启动；必须先重新启动，才能在站点中使用 VDA。

使用独立的 VDA 安装程序

重要： [准备安装](#)一文提供与您在安装过程中看到和指定的信息有关的指南，特别是与使用独立的 VDA 安装程序时处理重新启动和提取空间有关的指南。

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**。禁用用户帐户控制 (UAC)。

1. 从 Citrix 下载适用的软件包：**VDAServerSetup.exe**（适用于服务器操作系统计算机）或 **VDAWorkstationSetup.exe**（适用于桌面操作系统计算机）。对于单用户、单服务器操作系统部署（例如，将 Windows Server 2012 交付给一个用户，用于进行 Web 开发），请使用 VDAWorkstationSetup.exe 软件包。有关详细信息，请参阅“服务器 VDI”一文。
2. 右键单击下载的软件包，然后选择**以管理员身份运行**。
3. 按照向导提示操作。安装完成时默认启用自动重新启动；必须先重新启动，才能在站点中使用 VDA。

自定义 VDA

如果要自定义已安装的 VDA，请执行以下操作：

1. 从用于删除或更改程序的 Windows 功能，选择 Citrix **Virtual Delivery Agent <版本>**，然后单击鼠标右键并选择**更改**。
2. 选择自定义 **Virtual Delivery Agent 设置**。安装程序启动后，可更改 Controller 地址、向注册 Controller 的 TCP/IP 端口（默认值 = 80）或者是否自动开启 Windows Firewall 端口例外。

使用命令行安装

May 12, 2016

注意：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 [Red Hat Linux VDA](#) 和 [SUSE Linux VDA](#)。

在本文中：

- [简介](#)
- [使用完整产品安装程序](#)
- [使用独立的 VDA 安装程序](#)
- [使用命令行自定义 VDA](#)
- [用于安装核心组件的命令行选项](#)
- [用于安装 VDA 的命令行选项](#)
- [使用命令行安装通用打印服务器](#)

简介

重要：开始执行任何安装之前，请查看[准备安装](#)一文，文章介绍了安装程序以及您应在安装之前熟悉的任何内容。该文章还将介绍命令随附的选项。本文介绍了如何启动产品安装程序中的命令行界面。

可以使用命令行界面执行以下操作：

- 安装一个或多个核心组件：Delivery Controller、Citrix Studio、Citrix Director、许可证服务器和 StoreFront。
- 在主映像、虚拟机或物理机上安装 Virtual Delivery Agent (VDA)。还可以对介质上提供的脚本进行自定义，然后使用这些脚本在 Active Directory 中安装和删除 VDA。
- 自定义先前安装的 VDA。
- 安装通用打印服务器，用于置备网络会话打印机。Controller 已具备通用打印服务器功能；您只需在环境中的打印服务器上安装通用打印服务器。
- 升级组件；请参阅[升级部署](#)一文。

还可以使用 /remove 或 /removeall 选项从以前安装的此版本中删除组件。有关详细信息，请参阅[删除组件](#)一文。

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。

完整产品安装程序和独立的 VDA 安装程序都有命令行界面。

如果使用提供的示例脚本在 Active Directory 中安装、升级或删除 VDA 计算机，可以指定 VDA 配置选项，这些选项在下面用于安装 VDA 部分的命令行选项中列出。有关示例脚本的信息，请参阅[使用脚本安装 VDA](#)一文。

使用完整产品安装程序

可以使用完整产品安装程序安装核心组件和 VDA。

- 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。
- 解压文件。或者刻录 ISO 文件的 DVD。
- 通过本地管理员帐户，登录要在安装组件的服务器。
- 在驱动器中插入 DVD 或装载 ISO 文件。
- 在介质上的 \x64\XenDesktop Setup 目录中，运行以下命令：

要安装核心组件，请运行 `XenDesktopServerSetup.exe` 命令。请使用下文[用于安装核心组件的命令行选项](#)部分中列出的选项。

要安装 VDA，请运行 `XenDesktopVDASetup.exe` 命令。请使用下文[用于安装 VDA 的命令行选项](#)部分中列出的选项。

示例 1：以下命令将在服务器上安装 XenDesktop 控制器、Studio、Citrix Licensing 和 SQL Server Express。将自动打开组件通信所需的端口。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserver  
/configure_firewall
```

示例 2：以下命令将在服务器上安装 XenApp 控制器、Studio 和 SQL Server Express。将自动打开组件通信所需的端口。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /xenapp /components controller,desktopstudio  
/configure_firewall
```

示例 1：以下命令将在 VM 的默认位置安装 VDA for Windows 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，并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
```

示例 2：以下命令将在办公室 PC 上的默认位置安装 VDA for Windows Desktop OS 和 Citrix Receiver，该 PC 将与 Remote PC Access 结合使用。安装 VDA 后不会重新启动计算机；但是，必须重新启动才能使用 VDA。VDA 将首先注册到域 mydomain 中名为 Contr-East 的服务器上的 Controller，并将对音频数据包使用 UDP。如果检测到 Windows 防火墙服务，将会打开 HDX 端口。

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins /controllers "Contr-  
East.mydomain.local" /enable_hdx_ports /enable_real_time_transport /noreboot
```

使用独立的 VDA 安装程序

重要：[准备安装](#)一文提供与您安装过程中看到和指定的信息有关的指南，特别是与使用独立的 VDA 安装程序时处理重新启动和提取空间有关的指南。

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](#)。

1. 从 Citrix 下载适用的软件包：**VDA Server Setup.exe**（适用于服务器操作系统计算机）或 **VDA Workstation Setup.exe**（适用于桌面操作系统计算机）。对于单用户、单服务器操作系统部署（例如，将 Windows Server 2012 交付给一个用户，用于进行 Web 开发），请使用 VDA Workstation Setup.exe 软件包。有关详细信息，请参阅[服务器 VDI](#)一文。
2. 首先提取软件包中的文件，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：`.\VDAWorkstationSetup.exe /extract %temp%\CitrixVDAInstallMedia`。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 命令。请使用下文[用于安装 VDA 的命令行选项](#)部分中列出的选项。

要仅运行下载的软件包，请运行其名称：VDA Server Setup.exe 或 VDA Workstation Setup.exe。请使用下文[用于安装 VDA 的命令行选项](#)部分中列出的选项。（如果您熟悉完整产品安装程序：运行下载的独立软件包，就像该软件包是任何安装程序中的 XenDesktop VdaSetup.exe 命令一样，名称除外。）

以下安装命令通常用于 Remote PC Access。该命令将在物理办公室 PC 上安装 VDA，但不安装 Citrix Receiver 或 Citrix Profile Manager。安装 VDA 后不会自动重新启动计算机；但是，必须重新启动计算机才能使用 VDA。VDA 最初与 Controller 一起在名为 Contr-East 的服务器上注册。如果检测到 Windows 防火墙服务，则会打开端口。

```
VDAWorkstationSetup.exe /quiet /components vda /exclude "Citrix User Profile Manager" /controllers "Contr-East.domain.com" /enable_hdx_ports /noreboot
```

注意

从安装中排除 Citrix User Profile Manager 将影响对带有 Citrix Director 的 VDA 进行监视和故障排除。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”面板将出现故障。在“控制板”和“趋势”页面上，“平均登录时间”面板将仅显示安装了 Profile Management 的计算机的数据。

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，使用前文介绍过的下列一个或多个选项，运行 XenDesktopVdaSetup.exe 命令，如下文[用于安装 VDA 的命令行选项](#)部分中所述。

- /reconfigure – 自定义 VDA 时，必须使用此选项
- /h 或 /help
- /quiet
- /noreboot
- /controllers
- /portnumber 端口
- /enable_hdx_ports

用于安装核心组件的命令行选项

下表列出了 XenDesktopServerSetup.exe 命令的有效选项。

选项	说明
/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

	• 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需要的所有端口。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。
/help 或 /h	显示命令帮助。
/installdir 目录	用于安装组件的现有空目录。默认为 c:\Program Files\Citrix。
/logpath 路径	日志文件位置。指定的文件夹必须已存在；安装程序无法创建该文件夹。默认路径为 %TEMP%\Citrix\XenDesktop Installer
/no_remote_assistance	（仅当安装 Director 时有效。）禁用使用 Windows 远程协助的用户阴影操作功能。
/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，则将安装 SQL Server Express。
/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。
/tempdir 目录	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。

用于安装 VDA 的命令行选项

下表列出了 **XenDesktopVDASetup.exe** 命令的有效选项。

安装与 Remote PC Access 结合使用的 VDA 时，请仅指定在物理机（而非 VM 或主映像）上有效的选项以及适用于 VDA for Windows Desktop OS 的选项。

除非另有说明，否则这些选项将应用于物理机和虚拟机，以及 VDA for Windows Desktop OS 和 VDA for Windows Server OS。

选项	说明
/baseimage	（仅当在 VM 上安装 VDA for Windows 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 个人虚拟磁盘 一文。
/components component[,component]	要安装或删除的组件的列表（以逗号分隔）。有效值为： • VDA – 安装 VDA • PLUGINS – 安装 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。
/controllers "controller [controller] [...]"	可与 VDA 通信的 Controller 的完全限定的域名 (FQDN)，以空格分隔并用引号引起。请勿同时指定 /site_guid 和 /controllers 选项。
/enable_framehawk_port	打开 Framehawk 所使用的 UDP 端口。默认值：False
/enable_hdx_3d_pro	安装 VDA for HDX 3D Pro。有关详细信息，请参阅 HDX 3D Pro 一文。
/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 和指定功能（Windows 远程协助、实时传输和优化）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。
/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	启用与 Director 结合使用的 Windows 远程协助中的阴影操作功能。如果指定此选项，Windows 将在防火墙中打开 TCP 端口 3389，即使忽略了 /enable_hdx_ports 选项也是如此。
/exclude "component"["component"]	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 Machine Creation Services 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 从 VDA 安装中排除 Citrix User Profile Manager 将影响对带有 Citrix Director 的 VDA 进行监视和故障排除。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”面板将出现故障。在“控制板”和“趋势”页面上，“平均登录时间”面板将仅显示安装了 Profile Management 的计算机的数据。
/h 或 /help	显示命令帮助。
/installdir 目录	用于安装组件的现有空目录。默认为 c:\Program Files\Citrix。

/installwithsecurebootenabled	启用安全引导时允许安装 VDA。如果忽略此选项，则将显示“必须禁用安全引导才能成功安装 VDA”的警告。（此选项在图形界面中不可用。）
/logpath 路径	日志文件位置。指定的文件夹必须已存在；安装程序无法创建该文件夹。（此选项在图形界面中不可用。）默认路径为：%TEMP%\Citrix\XenDesktop Installer
/masterimage	（仅在 VM 上安装 VDA 时有效。）将 VDA 设置为主映像。
/no_appv	阻止安装 Citrix App-V 组件。有关详细信息，请参阅 App-V 一文。
/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。
/nodesktopexperience	（仅在安装 VDA for Windows 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。只有在重新启动后，才能使用 VDA 的全部功能。
/optimize	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 指定此选项。有关优化工具的详细信息，请参阅 CTX125874 。
/portnumber 端口	（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	阻止在桌面（工作站）操作系统中安装以下组件： • App V 组件 - Citrix Personalization for App-V - VDA • Upm 组件 - Citrix User Profile Manager • UpmVdaPlugin 组件 - Citrix User Profile Manager WMI Plugin • Mps 组件 - Machine Identity Service • 虚拟磁盘组件 - Personal vDisk 升级过程中，如果安装了上述任意组件，安装程序都会检测该组件并进行更新。
/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。
/servervdi	在支持的 Windows Server 上安装 VDA for Windows Desktop OS。在 Windows Server 上安装 VDA for

	Windows Server OS 时，请忽略此选项。使用此选项之前，请参阅 服务器 VDI 一文。（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 目录	安装过程中用于保存临时文件的目录。（此选项在图形界面中不可用。）默认路径为：c:\Windows\Temp。
/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。
/xa_server_location url	Windows 服务器应用程序的服务器的 URL。

使用命令行安装通用打印服务器

注意：如果要在 32 位 Windows 2008 服务器上安装 UpsServer 组件，请先阅读[本文](#)。

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。

Citrix 建议您将设置为 1 的命令行选项 /ENABLE_CEIP 包括在内，以选择加入 Citrix 客户体验改善计划 (CEIP)。例如：

```
msiexec /i UpsServer.msi ENABLE_CEIP=1
```

选择加入后，系统会将匿名统计数据和使用的信息发送到 Citrix 以帮助改善 Citrix 产品的质量和性能。

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](#)一文中的指南进行配置。

在 32 位 Windows 2008 计算机上部署 UpsServer_x86.msi 之前，必须使用 Visual Basic 脚本或 Orca 等工具调整 cdf_x86.msi 和 UpsServer_x86.msi 的 Windows Installer 的最低版本。

- 将 CDF 和 UPS msi 文件的 32 位版本（cdf_x86.msi 和 UpsServer_x86.msi）复制到某个临时文件夹。
- 安装 WiSumInf.vbs 脚本或 Orca 工具，两者均可在 [Windows SDK Components for Windows Installer Developers](#) 软件包中获取。有关脚本的信息，请参阅 MSDN 文章 [Manage Summary Information](#)（管理摘要信息）。
- 可以使用下面方法之一修改 Windows Installer 的最低版本：

使用 WiSumInf.vbs 脚本：将 WiSumInf.vbs 复制到两个 Citrix msi 所在的相同临时文件夹。然后，使用 WiSumInf.vbs cdf_x86.msi Pages=405 和 WiSumInf.vbs UpsServer_x86.msi Pages=405 运行每个软件包的脚本。

使用 Orca：分别打开 cdf_x86.msi 和 UpsServer_x86.msi 软件包，转至“View”（查看）菜单 >“Summary Information”（摘要信息），将 Schema（架构）文本框的值更改为 405。

完成上述过程后，在打印服务器上安装通用打印服务器。

使用脚本安装 VDA

Mar 17, 2016

注意：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 [Red Hat Linux VDA](#) 和 [SUSE Linux VDA](#)。

安装介质包含用于在 Active Directory 中安装、升级或删除计算机组的 Virtual Delivery Agent (VDA) 的示例脚本。您也可以将脚本应用于单个计算机，并用来维护 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。如果您还要集中记录结果以供查看和分析，则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 来指示操作是否成功。您可以使用标准目录搜索工具在中央日志共享中快速查找失败的安装或删除，而不是在目标计算机上进行本地搜索。

重要：开始执行任何安装之前，请阅读并完成[准备安装](#)一文中的任务。

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，在版本 7 中，可以将版本指定为 7.0；可以在 ProductVersion.txt file 中的安装介质上找到其完整值（如 7.0.0.3018）；但是，无需完全匹配。
 - 指定要从中调用安装程序的网络共享位置。指向布局的根目录（树结构的最高点）：将会在脚本运行时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](#)一文中的说明指定 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 Active Directory 中计算机所在的 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，在具有受支持操作系统的各计算机上安装 VDA。

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 DESIREDVERSION。例如，在版本 7 中，可以将版本指定为 7.0；可以在 ProductVersion.txt file 中的安装介质上找到其完整值（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 Active Directory 中计算机所在的 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，从各计算机中删除 VDA。

故障排除

脚本将生成说明脚本执行进度的内部日志文件。在开始对计算机进行部署的几秒内，脚本会将 Kickoff_VDA_Startup_Script 日志复制到中央日志共享，以便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，您可以通过检查本地计算机进一步执行故障诊断：脚本将两个调试日志文件放在各计算机的 %temp% 文件夹中，以便尽早进行故障排除：

- Kickoff_VDA_Startup_Script_.log
- VDA_Install_ProcessLog_.log

查看这些日志的内容，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。

安装 Red Hat Linux VDA

Apr 25, 2016

您可以基于 Red Hat 分发包创建 Linux 虚拟桌面。准备您的 Linux 虚拟机，在其上安装新的 [Linux VDA 软件](#)，配置 Delivery Controller，然后使用 Studio 向用户提供这些桌面。

有关详细信息，请参阅以下文档。

 [《面向 Red Hat Enterprise Linux 的 Linux 虚拟桌面安装指南》](#)
含 Red Hat Linux VDA 1.2 版本安装和设置说明的 PDF 文件。

注意

本文中使用的 Linux shell 命令经确认可在 GNU Bash shell 上使用。

本文包括以下几节：

- [系统要求](#)
- [配置 Delivery Controller](#)
- [准备 Linux 计算机以安装 VDA](#)
- [配置 Linux 计算机目录和交付组](#)
- [安装 Linux VDA 软件](#)
- [运行 VDA 软件](#)
- [卸载 Linux VDA 软件](#)
- [故障排除](#)
- [已知问题](#)
- [词汇表](#)

系统要求

Linux 虚拟桌面产品支持以下 Linux 发行版：

- SUSE Linux Enterprise :
 - Desktop 11 Service Pack 4
 - Desktop 12 Service Pack 1
 - Server 11 Service Pack 4
 - Server 12 Service Pack 1
- Red Hat Enterprise Linux
 - Workstation 6.7
 - Workstation 7.2
 - Server 6.7
 - Server 7.2

注意

在所有情况下，支持的处理器架构均为 x86-64。

Linux VDA 支持以下版本的 XenDesktop：

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.7
- XenDesktop 7.8

Linux VDA 与 Windows VDA 的配置过程稍有不同。但是，所有 Delivery Controller 场都能为 Windows 和 Linux 桌面提供代理服务。

注意

Linux VDA 与 XenDesktop 7.0 或更低版本不兼容。

支持使用以下版本的 Citrix Receiver：

- Citrix Receiver for Windows 4.4 或更高版本（相当于 v14.4 版本的 wfica32.exe）
- Citrix Receiver for Linux 13.3 或更高版本
- Citrix Receiver for Mac OSX 12.1 或更高版本
- Citrix Receiver for Android 3.8 或更高版本
- Citrix Receiver for iOS 6.1.4 或更高版本
- Citrix Receiver for Chrome/HTML5 1.9 版本（只能通过 Access Gateway 使用）

支持使用以下虚拟机管理程序托管 Linux VDA 客户机虚拟机：

- XenServer
- VMware ESX 和 ESXi
- Microsoft Hyper-V

也支持裸机托管。

提示

有关支持的平台的列表，请参阅虚拟机管理程序提供商的文档。

Linux VDA 支持以下 Active Directory 集成软件包或产品：

- Samba Winbind
- Quest Authentication Services v4.1 或更高版本
- Centrify DirectControl

提示

有关支持的平台的列表，请参阅 Active Directory 集成软件包提供商的文档。

使用以下虚拟机管理程序、Linux 发行版和 NVIDIA GRID™ GPU 才能支持 HDX 3D Pro。

虚拟机管理程序

支持以下虚拟机管理程序：

- XenServer
- VMware ESX 和 ESXi

Linux 发行版

以下 Linux 发行版支持 HDX 3D Pro：

- Red Hat Enterprise Linux - Workstation 7.2

GPU

支持以下 GPU：

- NVIDIA GRID™ 3.0 - Tesla M60
- NVIDIA GRID™ - K2

配置 Delivery Controller

XenDesktop 7.7 或更高版本包括为支持 Linux 虚拟桌面而作出的必要更改，但以前的版本需要安装修补程序或更新脚本。本节将介绍这些产品的安装和验证工作。

对于 XenDesktop 7.6 SP2，请应用 Hotfix Update 2 更新 Linux 虚拟桌面的 Broker。Hotfix Update 2 可在以下位置找到：

- [CTX142438](#)：Hotfix Update 2 - 适用于 Delivery Controller 7.6（32 位）– 英文版
- [CTX142439](#)：Hotfix Update 2 - 适用于 Delivery Controller 7.6（64 位）– 英文版

对于先前版本的 XenDesktop，可使用名为 **Update-BrokerServiceConfig.ps1** 的 PowerShell 脚本更新 Broker Service 配

置。此脚本可在以下软件包中找到：

- citrix-linuxvda-scripts-1.2.0.zip

对场内的每个 Delivery Controller 重复以下步骤：

1. 将 **Update-BrokerServiceConfig.ps1** 脚本复制到 Delivery Controller 计算机。
2. 在本地管理员上下文中打开 Windows PowerShell 控制台。
3. 浏览到脚本所在的文件夹。
4. 执行脚本：

```
.\Update-BrokerServiceConfig.ps1
```

注意

PowerShell 的默认配置是禁止执行 PowerShell 脚本。如果脚本运行失败，您可能需要先更改 PowerShell 执行策略，然后再重试：

```
Set-ExecutionPolicy Unrestricted
```

Update-BrokerServiceConfig.ps1 脚本会使用 Linux VDA 所需的新 WCF 端点更新 Broker Service 配置文件，然后重新启动 Broker Service。该脚本会自动确定 Broker Service 配置文件的位置。系统会在同一个目录中为原始配置文件创建备份，其扩展名为 **.prelinux**。

这些更改不会影响配置为使用同一个 Delivery Controller 场的 Windows VDA 的代理。因此，一个 Controller 场可同时无缝管理 Windows 和 Linux VDA 的代理会话。

要验证所需的配置更改是否已应用于 Delivery Controller，请确认字符串 **EndpointLinux** 是否在以下文件中出现五次：

```
%PROGRAMFILES%\Citrix\Broker\Service\BrokerService.exe.config
```

从 Windows 命令提示窗口，以本地管理员身份登录：

```
cd "%PROGRAMFILES%" \Citrix\Broker\Service\
```

```
findstr EndpointLinux BrokerService.exe.config
```

准备 Linux 计算机以安装 VDA

Citrix 建议先连接并正确配置网络，然后再继续操作。

仅限 RHEL 6：设置主机名

为确保正确报告该计算机的主机名，请更改 **/etc/sysconfig/network** 文件，使其仅包含该计算机的主机名。

```
HOSTNAME=hostname
```

仅限 RHEL 7：设置主机名

为确保正确报告计算机主机名，请更改 `/etc/hostname` 文件，使其仅包含计算机主机名。

为主机名分配环回地址

为确保正确报告该计算机的 DNS 域名和 FQDN，请更改 `/etc/hosts` 文件中的以下行，使其前两个条目包含该 FQDN 和主机名：

```
127.0.0.1 hostname-fqdn hostname localhost localhost.localdomain localhost4 localhost4.localdomain4
```

例如：

```
127.0.0.1 vda01.example.com vda01 localhost localhost.localdomain localhost4 localhost4.localdomain4
```

从该文件中的其他条目删除对 `hostname-fqdn` 或 `hostname` 的任何其他引用。

注意

Linux VDA 当前不支持 NetBIOS 名称截断，因此主机名不得超过 15 个字符。

检查主机名

验证主机名设置是否正确无误：

```
hostname
```

这应该仅返回计算机的主机名，而不是完全限定的域名 (FQDN)。

验证 FQDN 设置是否正确无误：

```
hostname -f
```

这应该返回计算机的 FQDN。

检查名称解析和服务可访问性

验证能否解析 FQDN 并 Ping 通域控制器和 XenDesktop Delivery Controller：

```
nslookup domain-controller-fqdn
```

```
ping domain-controller-fqdn
```

```
nslookup delivery-controller-fqdn
```

```
ping delivery-controller-fqdn
```

如果无法解析 FQDN 或 Ping 不通上述任一计算机，请先检查相关步骤，然后再继续。

确保 VDA、XenDesktop Controller 和域控制器之间的时钟始终精确同步至关重要。将 Linux VDA 托管为虚拟机可能会导致时

钟偏差问题。出于此原因，最好使用远程时间服务来同步时间。

RHEL 6.x 和早期版本使用 NTP 守护程序 (ntpd) 同步时钟，默认 RHEL 7.x 环境则转而使用更新的 Chrony 守护程序 (chronyd)。两个服务的配置和操作过程十分类似。

仅限 RHEL 6：配置 NTP 服务

以 root 用户身份，编辑 `/etc/ntp.conf` 并为每个远程时间服务器添加一个服务器条目：

```
server peer1-fqdn-or-ip-address iburst  
  
server peer2-fqdn-or-ip-address iburst
```

在典型部署中，时间应从本地域控制器同步，而不是直接从公共 NTP 池服务器同步。为域中的每个 Active Directory 域控制器添加一个服务器条目。

删除列出的任何其他 `server` 条目，包括环回 IP 地址、本地主机和公共服务器 `*.pool.ntp.org` 条目。

保存更改并重新启动 NTP 守护程序：

```
sudo /sbin/service ntpd restart
```

仅限 RHEL 7：Chrony 服务

以 root 用户身份，编辑 `/etc/chrony.conf` 并为每个远程时间服务器添加一个服务器条目：

```
server peer1-fqdn-or-ip-address iburst  
  
server peer2-fqdn-or-ip-address iburst
```

在典型部署中，时间应从本地域控制器同步，而不是直接从公共 NTP 池服务器同步。为域中的每个 Active Directory 域控制器添加一个服务器条目。

删除列出的任何其他 `server` 条目，包括环回 IP 地址、本地主机和公共服务器 `*.pool.ntp.org` 条目。

保存更改并重新启动 Chrony 守护程序：

```
sudo /sbin/service chronyd restart
```

RHEL 6 上的一个特有问题是，用户会收到弹出窗口，要求其在登录后输入 root 用户密码。

要解决此问题，请以 root 用户身份，在文本编辑器中创建 `/etc/polkit-1/localauthority/30-site.d/20-no-show-proxy-dialog.pkla` 文件，并添加以下内容：

```
[No Show Proxy Dialog]  
  
Identity=unix-user:*  
  
Action=org.freedesktop.packagekit.system-network-proxy-configure  
  
ResultAny=no  
  
ResultInactive=no
```

ResultActive=no

注意

有关此问题的详细信息，请参阅[这里](#)的 RedHat 解决方案页面。正确的解决方法如注释部分所述。

Linux VDA 依赖于 OpenJDK。运行时环境应作为操作系统安装的一部分进行安装。

仅限 RHEL 6 : OpenJDK 1.7

使用以下命令确认版本是否正确：

```
sudo yum info java-1.7.0-openjdk
```

预先封装的 OpenJDK 可能为早期版本。请根据需要更新为最新版本：

```
sudo yum -y update java-1.7.0-openjdk
```

将以下行添加到 `~/.bashrc` 文件，从而设置 `JAVA_HOME` 环境变量：

```
export JAVA_HOME=/usr/lib/jvm/java
```

打开新的 shell，然后确认 Java 版本：

```
java -version
```

仅限 RHEL 7.0 : OpenJDK 1.8

使用以下命令确认版本是否正确：

```
sudo yum info java-1.8.0-openjdk
```

预先封装的 OpenJDK 可能为早期版本。请根据需要更新为最新版本：

```
sudo yum -y update java-1.8.0-openjdk
```

将以下行添加到 `~/.bashrc` 文件，从而设置 `JAVA_HOME` 环境变量：

```
export JAVA_HOME=/usr/lib/jvm/java
```

打开新的 shell，然后确认 Java 版本：

```
java -version
```

提示

为避免问题，请确保仅安装 1.7.0 或 1.8.0 版本的 OpenJDK。删除系统上的所有其他版本 Java。

Linux VDA 要求在 RHEL 6 上使用 PostgreSQL 8.4 或更高版本，或在 RHEL 7 上使用 PostgreSQL 9.2 或更高版本。

安装以下软件包：

```
sudo yum -y install postgresql-server
```

```
sudo yum -y install postgresql-jdbc
```

此时需要执行一些安装后步骤，以便初始化数据库，并确保服务在引导时启动。这会在 `/var/lib/pgsql/data` 下创建数据库文件。此命令在 PostgreSQL 8 和 9 上有所不同。

仅限 RHEL 6：PostgreSQL 8

```
sudo /sbin/service postgresql initdb
```

仅限 RHEL 7：PostgreSQL 9

```
sudo postgresql-setup initdb
```

启动 PostgreSQL

对于任一版本的 PostgreSQL，请将服务配置为在引导时启动，以及立即启动：

```
sudo /sbin/chkconfig postgresql on
```

```
sudo /sbin/service postgresql start
```

使用以下命令检查 PostgreSQL 版本：

```
psql --version
```

使用 **psql** 命令行实用程序确认数据目录已设置：

```
sudo -u postgres psql -c 'show data_directory'
```

Linux VDA 要求使用 **motif** 或 **openmotif** 软件包，具体取决于发行版。

仅限 RHEL 6：打开 Motif

```
sudo yum -y install openmotif
```

仅限 RHEL 7：Motif

```
sudo yum -y install motif
```

Linux VDA 要求使用 **cups** 和 **foomatic** 筛选器。

仅限 RHEL 6：打印支持

```
sudo yum -y install cups
```

```
sudo yum -y install foomatic
```

仅限 RHEL 7 : 打印支持

```
sudo yum -y install cups
```

```
sudo yum -y install foomatic-filters
```

安装所需的其他软件包：

```
sudo yum -y install redhat-lsb-core
```

```
sudo yum -y install ImageMagick
```

在支持的虚拟机管理程序上将 Linux VDA 当作虚拟机运行时，需要作出一些更改。根据使用的虚拟机管理程序平台作出以下更改。如果正在裸机硬件上运行 Linux 计算机，则无需作出任何更改。

修复 Citrix XenServer 上的时间同步问题

如果启用了 XenServer 时间同步功能，则在每个半虚拟化 Linux VM 中，您会发现 NTP 和 XenServer 都在尝试管理系统时钟。为避免时钟与其他服务器不同步，每个 Linux 客户机中的系统时钟都必须与 NTP 同步。这要求禁用主机时间同步。无需在 HVM 模式下进行任何更改。

在某些 Linux 发行版中，如果正在运行半虚拟化 Linux 内核，并安装了 XenServer Tools，您可以检查 XenServer 时间同步功能是否存在，以及是否已在 Linux VM 中启用：

```
su -
```

```
cat /proc/sys/xen/independent_wallclock
```

此时会返回以下任一项：

- 0 - 时间同步功能已启用，并需要禁用。
- 1 - 时间同步功能已禁用，无需采取任何操作。

如果 /proc/sys/xen/indepent_wallclock 文件不存在，则无需执行以下步骤。

如果已启用，请向该文件写入 1 以禁用时间同步功能：

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
```

要使此更改成为永久更改，并在重新启动后仍然有效，请编辑 /etc/sysctl.conf 文件并添加以下行：

```
xen.independent_wallclock = 1
```

要验证这些更改，请重新启动系统：

```
reboot
```


重新启动后，请检查此设置是否正确无误：

```
su -  
  
cat /proc/sys/xen/independent_wallclock
```

此时应返回值 1。

在 Microsoft Hyper-V 上修复时间同步问题

安装了 Hyper-V Linux 集成服务的 Linux VM 可利用 Hyper-V 时间同步功能来使用主机操作系统的时间。为确保系统时钟始终精确可靠，此功能应随 NTP 服务一同启用。

从管理操作系统中：

1. 打开 Hyper-V 管理器控制台。
2. 为设置 Linux VM，请选择 **Integration Services**（集成服务）。
3. 确保已选择 **Time synchronization**（时间同步）。

注意

此方法与 VMware 和 XenServer 不同，这两种产品会禁用主机时间同步功能，以免与 NTP 发生冲突。Hyper-V 时间同步可以与 NTP 时间同步共存并互补。

修复 ESX 和 ESXi 上的时间同步问题

如果启用了 VMware 时间同步功能，则在每个半虚拟化 Linux VM 中，您会发现 NTP 和虚拟机管理程序都在尝试同步系统时钟。为避免时钟与其他服务器不同步，每个 Linux 客户机中的系统时钟都必须与 NTP 同步。这要求禁用主机时间同步。

如果正在运行安装了 VMware Tools 的半虚拟化 Linux 内核：

1. 打开 vSphere Client。
2. 编辑 Linux VM 设置。
3. 在 **Virtual Machine Properties**（虚拟机属性）对话框中，打开 **Options**（选项）选项卡。
4. 选择 **VMware Tools**。
5. 在 **Advanced**（高级）框中，取消选中 **Synchronize guest time with host**（与主机同步客户机时间）。

将 Linux 计算机添加至 XenDesktop for Linux 支持的 Active Directory 域有多种方法：

- Samba Winbind
- Quest Authentication Service
- Centrify DirectControl

根据所选的方法，按以下说明执行操作。

Samba Winbind

安装或更新所需软件包

安装或更新所需软件包：

```
sudo yum -y install samba-winbind \
    samba-winbind-clients \
    krb5-workstation \
    authconfig \
    oddjob-mkhomedir
```

启用 Winbind 守护程序以在引导时启动

Winbind 守护程序必须配置为在引导时启动：

```
sudo /sbin/chkconfig winbind on
```

配置 Winbind 身份验证

将计算机配置为使用 Winbind 执行 Kerberos 身份验证：

```
sudo authconfig \
    --disablecache \
    --disablesd \
    --disablesdauth \
    --enablewinbind \
    --enablewinbindauth \
    --disablewinbindoffline \
    --smbsecurity=ads \
    --smbworkgroup=domain \
    --smbrealm=REALM \
    --krb5realm=REALM \
    --krb5kdc=fqdn-of-domain-controller \
    --winbindtemplateshell=/bin/bash \
    --enablemkhomedir --updateall
```

其中，**REALM** 为大写的 Kerberos 领域名称，而 **domain** 为 Active Directory 域的简短 NetBIOS 名称。

如果需要通过 DNS 查找 KDC 服务器和领域名称，请将以下两个选项添加至上述命令：

```
--enablekrb5kcdns --enablekrb5realmdns
```

忽略 **authconfig** 命令返回的有关 winbind 服务无法启动的错误。出现这些错误的原因是，authconfig 尝试在计算机尚未加入域的情况下启动 winbind 服务。

打开 **/etc/samba/smb.conf** 并将以下条目添加到 **[Global]** 部分下，但要放在 authconfig 工具生成的部分后面。

```
kerberos method = secrets and keytab  
  
winbind refresh tickets = true
```

Linux VDA 需要使用系统 keytab 文件 **/etc/krb5.keytab** 执行身份验证并向 Delivery Controller 进行注册。计算机首次加入域后，上面的 **kerberos method** 设置将迫使 Winbind 创建系统 keytab 文件。

加入 Windows 域

这要求域控制器可访问，而且您具有有权将计算机添加到域的 Active Directory 用户帐户。

```
sudo net ads join REALM -U user
```

其中，REALM 是大写的 Kerberos 领域名称，而 user 是有权将计算机添加到域的域用户。

为 Winbind 配置 PAM

默认情况下，Winbind PAM 模块 (**pam_winbind**) 配置不会启用 Kerberos 票据缓存，也不会创建主目录。打开 **/etc/security/pam_winbind.conf**，并在 **[Global]** 部分下添加或更改以下条目：

```
krb5_auth = yes  
  
krb5_ccache_type = FILE  
  
mkhomedir = yes
```

确保删除每个设置中的前置分号。这些更改要求重新启动 Winbind 守护程序：

```
sudo /sbin/service winbind restart
```

提示

计算机加入域后，winbind 守护程序会一直运行。

打开 **/etc/krb5.conf** 并将 **[libdefaults]** 部分下的以下设置从 KEYRING 更改为 FILE 类型：

```
default_ccache_name = FILE:/tmp/krb5cc_%{uid}
```

验证域成员身份

XenDesktop Controller 要求所有 VDA 计算机（不论是 Windows 还是 Linux）都要在 Active Directory 中有一个计算机对象。

使用 Samba 的 **net ads** 命令确认计算机已加入域：

```
sudo net ads testjoin
```

使用以下命令验证其他域和计算机对象信息：

```
sudo net ads info
```

验证 Kerberos 配置

要验证 Kerberos 已正确配置为可与 Linux VDA 配合使用，请检查系统 keytab 文件是否已创建并含有有效密钥：

```
sudo klist -ke
```

此时应显示各种主体名称与密码套件组合可用的密钥列表。运行 Kerberos **kinit** 命令，使用这些密钥向域控制器验证计算机的身份：

```
sudo kinit -k MACHINE\${@REALM}
```

计算机和领域名称必须指定为大写，而美元符号 (\$) 必须使用反斜杠 (\) 进行转义，以免发生 shell 替换。在某些环境中，DNS 域名与 Kerberos 领域名称不同；请确保使用领域名称。如果此命令成功运行，则不会显示任何输出。

使用以下命令验证计算机帐户的 TGT 票据已缓存：

```
sudo klist
```

使用以下命令检查计算机帐户详细信息：

```
sudo net ads status
```

验证用户身份验证

使用 **wbinfo** 工具验证是否可向域验证域用户的身份：

```
wbinfo --krb5auth=domain\\username%password
```

这里指定的域为 AD 域名，而不是 Kerberos 领域名称。对于 bash shell，必须使用另一个反斜杠对反斜杠 (\) 字符进行转义。此命令会返回一条成功或失败消息。

要验证 Winbind PAM 模块是否配置正确，请使用以前未曾登录计算机的域用户帐户在本地登录。

```
ssh localhost -l domain\\username
```

```
id -u
```

检查是否为 **id -u** 命令返回的 uid 创建了对应的 Kerberos 凭据缓存文件：

```
ls /tmp/krb5cc_uid
```

检查用户 Kerberos 凭据缓存中的票据是否有效且未过期：

```
klist
```

退出会话：

```
exit
```

直接登录 Gnome 或 KDE 控制台也可执行类似测试。

Quest Authentication Service

在域控制器上配置 Quest

这里假定您已在 Active Directory 域控制器上安装并配置了 Quest 软件，而且已获得管理权限，有权在 Active Directory 中创建计算机对象。

允许域用户登录 Linux VDA 计算机

对于需要在 Linux VDA 计算机上建立 HDX 会话的每个域用户：

1. 在 Active Directory 用户和计算机管理控制台中，为该用户帐户打开 Active Directory 用户属性。
2. 选择 **Unix Account**（Unix 帐户）选项卡。
3. 选中 **Unix-enabled**（已启用 Unix）。
4. 将 **Primary GID Number**（首选 GID 编号）设为实际域用户组的组 ID。

注意

这些说明相当于设置域用户，以便他们可以使用控制台、RDP、SSH 或任何其他远程协议进行登录。

在 Linux VDA 上配置 Quest

SELinux 策略强制实施解决方法

默认 RHEL 环境会强制实施 SELinux。这会影响 Quest 使用的 Unix 域套接字 IPC 机制，并阻止域用户登录。

[这里](#)概述了几种解决方法。

最简单的方法是禁用 SELinux。以 root 用户身份，编辑 /etc/selinux/config 并更改 SELinux 设置：

```
SELINUX=disabled
```

此更改要求重新启动：

```
reboot
```

Important

请谨慎使用此设置。禁用后重新启用 SELinux 策略强制实施会导致完全锁定，即便是对 root 用户和其他本地用户也是如此。

配置 VAS 守护程序

自动续订 Kerberos 票据功能需要启用并断开，而身份验证（脱机登录）功能需要禁用：

```
sudo /opt/quest/bin/vastool configure vas vasd \  
    auto-ticket-renew-interval 32400  
sudo /opt/quest/bin/vastool configure vas vas_auth \  
    allow-disconnected-auth false
```

这会持续订间隔设为 9 小时 (32400 秒) , 即比默认的 10 小时票据生命周期短 1 小时。请在票据生命周期较短的系统上设置较低的值。

配置 PAM 和 NSS

Quest 要求将 PAM 和 NSS 手动配置为允许域用户通过 HDX 和其他服务 (例如 su、ssh 和 RDP) 进行登录。配置 PAM 和 NSS :

```
sudo /opt/quest/bin/vastool configure pam
```

```
sudo /opt/quest/bin/vastool configure nss
```

加入 Windows 域

使用 Quest vastool 命令将 Linux 计算机加入 Active Directory 域 :

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

用户为有权将计算机加入 Active Directory 域的域用户。域名为域的 DNS 名称, 例如 example.com。

验证域成员身份

XenDesktop Controller 要求所有 VDA 计算机 (不论是 Windows 还是 Linux) 都要在 Active Directory 中有一个计算机对象。验证 Quest 加入的 Linux 计算机是否位于域中 :

```
sudo /opt/quest/bin/vastool info domain
```

如果计算机已加入域, 这会返回域名。如果未加入, 则会显示以下错误 :

```
ERROR: No domain could be found.
```

```
ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm
```

```
default_realm not configured in vas.conf. Computer may not be joined to domain
```

验证用户身份验证

要验证 Quest 能否使用 PAM 对域用户进行身份验证, 请使用以前未曾登录计算机的域用户帐户进行登录 :

```
ssh localhost -l domain\\username
```

```
id -u
```

检查是否为 id -u 命令返回的 UID 创建了对应的 Kerberos 凭据缓存文件 :

```
ls /tmp/krb5cc_uid
```

检查用户 Kerberos 凭据缓存中的票据是否有效且未过期 :

```
/opt/quest/bin/vastool klist
```

退出会话 :

```
exit
```

直接登录 Gnome 或 KDE 控制台也可执行类似测试。

Centrify DirectControl

加入 Windows 域

安装 Centrify DirectControl Agent 后，请使用 Centrify **adjoin** 命令将 Linux 计算机加入 Active Directory 域：

```
su -  
  
adjoin -w -V -u user domain-name
```

user 参数为有权将计算机加入 Active Directory 域的任何 Active Directory 域用户。domain-name 参数为将 Linux 计算机加入到的域的名称。

验证域成员身份

XenDesktop Controller 要求所有 VDA 计算机（不论是 Windows 还是 Linux）都要在 Active Directory 中有一个计算机对象。验证 Centrify 加入的 Linux 计算机是否位于域中：

```
su -  
  
adinfo
```

检查 **Joined to domain** 值是否有效以及 **CentrifyDC mode** 是否返回了 **connected**。如果模式仍然卡在启动状态，则表明 Centrify 客户端遇到了服务器连接或身份验证问题。

使用以下命令可获得更全面的系统和诊断信息：

```
adinfo --sysinfo all  
  
adinfo --diag
```

测试与各种 Active Directory 和 Kerberos 服务的连接：

```
adinfo --test
```

安装 NVIDIA GRID 驱动程序

启用 HDX 3D Pro 时需要执行额外安装步骤，以便在虚拟机管理程序和 VDA 计算机上安装所需的图形驱动程序。

配置以下设置：

1. Citrix XenServer
2. VMware ESX

根据所选的虚拟机管理程序，按以下说明执行操作。

Citrix XenServer

此部分详细说明了如何在 [Citrix XenServer](#) 上逐步安装和配置 NVIDIA GRID 驱动程序。

VMware ESX

按照本指南中的信息执行操作，并为 [VMware ESX](#) 安装和配置 NVIDIA GRID 驱动程序。

VDA 计算机

按照这些步骤为每个 Linux VM 客户机安装并配置驱动程序：

1. 开始前，请确保 Linux VM 已关闭。
2. 在 XenCenter 中，将处于 GPU 直通模式的 GPU 添加至虚拟机。
3. 启动 RHEL 虚拟机。

要准备计算机以使用 NVIDIA GRID 驱动程序，请执行以下步骤：

```
# yum install gcc

# yum install "kernel-devel-uname-r == $(uname -r)"

# systemctl set-default multi-user.target
```

完成后，按照 [Red Hat Enterprise Linux 文档](#) 中的步骤安装 NVIDIA GRID 驱动程序。

注意

安装 GPU 驱动程序期间，为每个问题选择默认答案 (no)。

Important

启用 GPU 直通后，无法再通过 XenCenter 访问 Linux VM，因此您需要使用 SSH 建立连接。

要确认 NVIDIA GRID™ 图形驱动程序是否安装正确，请运行“nvidia-smi”；此时应显示以下结果：

```
nvidia-smi

+-----+
| NVIDIA-SMI 352.70      Driver Version: 352.70      |
+-----+-----+
| GPU   Name           Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan   Temp   Perf    Pwr:Usage/Cap|      Memory-Usage | GPU-Util  Compute M. |
+-----+-----+-----+-----+-----+-----+
|    0   Tesla M60             Off | 0000:00:05.0     Off |                    Off |
| N/A    20C    P0           37W / 150W | 19MiB / 8191MiB |      0%      Default |
+-----+-----+-----+-----+-----+-----+

+-----+
| Processes:                                     GPU Memory |
|  GPU       PID    Type    Process name                     Usage      |
+-----+-----+-----+-----+-----+-----+
| No running processes found                                     |
+-----+
```

为图形卡设置正确的配置：

```
etc/X11/ctx-nvidia.sh
```

要利用高分辨率和多监视器功能，您需要获得有效的 NVIDIA 许可证。要应用许可证，请按照“GRID Licensing Guide.pdf - DU-07757-001 September 2015”产品文档执行操作。

配置 Linux 计算机目录和交付组

创建计算机目录和添加 Linux VDA 计算机的过程与传统的 Windows VDA 方法十分类似。有关如何完成这些任务的更全面说明，请参阅联机 [Citrix 产品文档](#)。

创建含有 Linux VDA 计算机的计算机目录时会面临一些限制，这不同于为 Windows VDA 计算机创建计算机目录的过程：

- 对于操作系统，请：
 - 为托管共享桌面交付模型，选择 Window 服务器操作系统或服务器操作系统选项。
 - 为 VDI 专用桌面交付模型，选择 Windows 桌面操作系统或桌面操作系统选项。
- 确保计算机未执行电源管理设置。
- 由于 Linux VDA 不支持 PVS 和 MCS，请选择“Another service or technology”（其他服务或技术）（现有映像）部署方法。
- 请勿在同一个计算机目录中混合使用 Linux 和 Windows VDA 计算机。

注意

早期版本的 Citrix Studio 不支持“Linux 操作系统”的概念；但是，选择 Windows 服务器操作系统或服务器操作系统选项等同于使用托管共享桌面交付模型。选择 Windows 桌面操作系统或桌面操作系统选项等同于使用 XenDesktop 每计算机一个用户交付模型。

有关创建计算机目录的 Citrix 文档如下所列：

- [XenDesktop 7.1](#)
- [XenDesktop 7.5](#)
- [XenDesktop 7.6](#)
- [XenDesktop 7.7](#)
- [XenDesktop 7.8](#)

更低版本的 XenDesktop 不支持使用。

提示

如果计算机离开后又重新加入 Active Directory 域，则需要先删除计算机，然后再将其重新添加到计算机目录。

创建交付组及添加含有 Linux VDA 计算机的计算机目录的过程与 Windows VDA 计算机几乎相同。有关如何完成这些任务的更全面说明，请参阅联机 Citrix 产品文档。

创建含有 Linux VDA 计算机目录的交付组时会面临以下限制：

- 对于交付类型，请选择“桌面”。Linux VDA 计算机不支持应用程序交付。
- 确保所选的 AD 用户和组已正确配置，可以登录到 Linux VDA 计算机。
- 请勿允许未经身份验证的（匿名）用户登录。

- 请勿在交付组中混入含有 Windows 计算机的计算机目录。

有关创建交付组的 Citrix 文档如下所列：

- [XenDesktop 7.1](#)
- [XenDesktop 7.5](#)
- [XenDesktop 7.6](#)
- [XenDesktop 7.7](#)
- [XenDesktop 7.8](#)

更低版本的 XenDesktop 不支持使用。

安装 Linux VDA 软件

如果之前安装的 Linux VDA 版本低于 v1.0，则应先卸载该版本，然后再安装新版本。

停止 Linux VDA 服务：

```
sudo /sbin/service ctxvda stop
```

```
sudo /sbin/service ctxhdx stop
```

卸载软件包：

```
sudo rpm -e XenDesktopVDA
```

Important

不支持将技术预览版升级至 v1.0、v1.1 或 v1.2。

安装 Linux VDA

使用 RPM 软件包管理器安装 Linux VDA 软件：

对于 RHEL 6：

```
sudo rpm -i XenDesktopVDA-1.2.0.282-1.el6.x86_64.rpm
```

对于 RHEL 7.2：

```
sudo rpm -i XenDesktopVDA-1.2.0.282-1.el7.x86_64.rpm
```

Important

安装 Linux VDA 后，Citrix 建议运行以下命令来提高安全性：

```
sudo sed -i '/ip addr | awk /a xhost"-LOCAL:""/usr/local/bin/ctxsession.sh
```

如果之前安装了 Linux VDA v1.1，请使用 RPM 软件包管理器升级 Linux VDA 软件：

对于 RHEL 6：

```
sudo rpm -U XenDesktopVDA-1.2.0.282-1.el6.x86_64.rpm
```

对于 RHEL 7.2：

```
sudo rpm -U XenDesktopVDA-1.2.0.282-1.el7.x86_64.rpm
```

Important

升级 Linux VDA 后，Citrix 建议运行以下命令来提高安全性：

```
sudo sed -i '/ip addr | awk /a xhost"-LOCAL:""/usr/local/bin/ctxsession.sh
```

安装软件包后，您需要运行 ctxsetup.sh 脚本来配置 Linux VDA。如果升级了软件包，您需要运行 ctxsetup.sh 脚本来完成升级操作。执行任何更改前，此脚本会验证环境，确保所有依赖项都已安装。如果需要，您也可以随时重新运行此脚本来更改设置。

该脚本可在出现提示时手动运行，也可使用预配置的响应自动运行。继续操作前，请查看此脚本的帮助信息：

```
sudo /usr/local/sbin/ctxsetup.sh -help
```

提示配置

运行会提示各种问题的手动配置：

```
sudo /usr/local/sbin/ctxsetup.sh
```

自动配置

自动安装时，设置脚本所需的选项可由环境变量提供。如果所需的所有变量都存在，则脚本不会提示用户提供任何信息，从而通过脚本完成安装过程。

支持的环境变量包括：

- CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N - Virtual Delivery Agent 支持使用 DNS CNAME 记录指定 Delivery Controller 名称。这通常设为 N。
- CTX_XDL_DDC_LIST = list-ddc-fqdns - Virtual Delivery Agent 要求提供由空格分隔的 Delivery Controller 完全限定的域名 (FQDN) 列表来向 Delivery 进行注册。必须至少指定一个 FQDN 或 CNAME 别名。
- CTX_XDL_VDA_PORT = port-number - Virtual Delivery Agent 会使用 TCP/IP 端口与 Delivery Controller 通信。这通常是端口 80。

- CTX_XDL_REGISTER_SERVICE = Y | N - Linux 虚拟桌面服务支持在引导期间启动。这通常设为 Y。
- CTX_XDL_ADD_FIREWALL_RULES = Y | N - Linux 虚拟桌面服务要求允许传入网络连接通过系统防火墙。您可以在系统防火墙中自动为 Linux 虚拟桌面打开所需端口（默认端口 80 和 1494）。这通常设为 Y。
- CTX_XDL_AD_INTEGRATION = 1 | 2 | 3 - Virtual Delivery Agent 要求使用 Kerberos 配置设置对 Delivery Controller 进行身份验证。Kerberos 配置根据系统上已安装和已配置的 Active Directory 集成工具确定。指定要使用且受支持的 Active Directory 集成方法：
 - 1 - Samba Winbind
 - 2 - Quest Authentication Service
 - 3 - Centrify DirectControl
- CTX_XDL_HDX_3D_PRO = Y | N - Linux 虚拟桌面支持 HDX 3D Pro，这是一系列图形加速技术，旨在优化富图形应用程序的虚拟化水平。HDX 3D Pro 要求安装兼容的 NVIDIA Grid 图形卡。如果选择了 HDX 3D Pro，则需要为 VDI 桌面（单会话）模式配置 Virtual Delivery Agent –（即 CTX_XDL_VDI_MODE=Y）。这在 SUSE 上不受支持。确保将此值设为 N。
- CTX_XDL_VDI_MODE = Y | N - 将计算机配置为专用桌面交付模型 (VDI) 还是托管共享桌面交付模型。对于 HDX 3D Pro 环境，此变量需要设置为 Y。这通常设为 N。
- CTX_XDL_SITE_NAME = dns-name - Virtual Delivery Agent 会使用 DNS 发现 LDAP 服务器，从而查询 LDAP 服务记录。要将 DNS 搜索结果限制为本地站点，可能需要指定 DNS 站点名称。此变量通常为空 [none]。
- CTX_XDL_LDAP_LIST = list-ldap-servers - 默认情况下，Virtual Delivery Agent 会通过查询 DNS 来发现 LDAP 服务器，但如果 DNS 无法提供 LDAP 服务记录，您可以提供一个 LDAP 完全限定的域名 (FQDN) 和 LDAP 端口（例如 ad1.mycompany.com:389）的列表，并以空格分隔。此变量通常为空 [none]。
- CTX_XDL_SEARCH_BASE = search-base - 默认情况下，Virtual Delivery Agent 会使用一个搜索基础来查询 LDAP，该搜索基础会设置为 Active Directory 域的根（例如 DC=mycompany,DC=com），但是，要提高搜索性能，您也可以指定一个搜索基础（例如 OU=VDI,DC=mycompany,DC=com）。此变量通常为空 [none]。
- CTX_XDL_START_SERVICE = Y | N - 在完成 Linux VDA 配置后，是否启动 Linux VDA 服务。这通常设为 Y。

设置环境变量并运行配置脚本：

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST=list-ddc-fqdns

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base

export CTX_XDL_START_SERVICE=Y|N

sudo -E /usr/local/sbin/ctxsetup.sh
```

您必须为 `sudo` 提供 `-E` 选项，以便将现有环境变量传递给它所创建的新 shell。Citrix 建议使用上述命令并在第一行加上 `#!/bin/bash` 来创建 shell 脚本文件。

另外，也可以使用一个命令来指定所有参数：

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \  
CTX_XDL_DDC_LIST=list-ddc-fqdns \  
CTX_XDL_VDA_PORT=port-number \  
CTX_XDL_REGISTER_SERVICE=Y|N \  
CTX_XDL_ADD_FIREWALL_RULES=Y|N \  
CTX_XDL_AD_INTEGRATION=1|2|3 \  
CTX_XDL_HDX_3D_PRO=Y|N \  
CTX_XDL_VDI_MODE=Y|N \  
CTX_XDL_SITE_NAME=dns-name \  
CTX_XDL_LDAP_LIST=list-ldap-servers \  
CTX_XDL_SEARCH_BASE=search-base \  
CTX_XDL_START_SERVICE=Y|N \  
  
/usr/local/sbin/ctxsetup.sh
```

删除配置更改

在某些情形下，您可能需要删除 `ctxsetup.sh` 脚本对配置所做的更改，而不卸载 Linux VDA 软件包。

继续操作前，请查看此脚本的帮助信息：

```
sudo /usr/local/sbin/ctxcleanup.sh --help
```

删除配置更改：

```
sudo /usr/local/sbin/ctxcleanup.sh
```

Important

此脚本会从数据库删除所有配置数据，从而使 Linux VDA 无法使用。

配置日志

`ctxsetup.sh` 和 `ctxcleanup.sh` 脚本会在控制台上显示错误，并将详细信息写入配置日志文件：

```
/tmp/xdl.configure.log
```

重新启动 Linux VDA 服务，确保更改生效。

运行 VDA 软件

使用 ctxsetup.sh 脚本配置 Linux VDA 后，请使用以下命令控制 Linux VDA。

启动 Linux VDA 服务：

```
sudo /sbin/service ctxhdx start
```

```
sudo /sbin/service ctxvda start
```

停止 Linux VDA 服务：

```
sudo /sbin/service ctxvda stop
```

```
sudo /sbin/service ctxhdx stop
```

重新启动 Linux VDA 服务：

```
sudo /sbin/service ctxvda stop
```

```
sudo /sbin/service ctxhdx restart
```

```
sudo /sbin/service ctxvda start
```

检查 Linux VDA 服务的运行状态：

```
sudo /sbin/service ctxvda status
```

```
sudo /sbin/service ctxhdx status
```

卸载 Linux VDA 软件

检查 Linux VDA 是否安装并查看已安装软件包的版本：

```
rpm -q XenDesktopVDA
```

查看更多详细信息：

```
rpm -qi XenDesktopVDA
```


注意

卸载 Linux VDA 软件会删除关联的 PostgreSQL 和其他配置数据。但是，在安装 Linux VDA 前设置的 PostgreSQL 软件包和其他依赖软件包不会遭到删除。

本文未介绍包括 PostgreSQL 在内的依赖软件包的删除操作。

故障排除

确认 Linux 计算机已准备妥当

最常见的问题都与 Linux 计算机配置不当（主要是网络、NTP 时间服务器配置或 Active Directory 域成员身份配置不当）有直接关系。修复 Linux 计算机配置通常可以解决 VDA 软件问题。

配置日志记录和跟踪

Broker 代理和 HDX Service 会将日志记录到 syslog。Citrix 支持会提供一套工具，用于在支持通话期间跟踪更多信息。

HDX Service 日志记录

HDX Service 会出厂配置为将日志记录到 syslog 中，无需进行其他配置。

Broker 代理日志记录

Broker 代理（也称为 ctxvda 服务）会通过网络套接字将日志数据写入 syslog。这可能并未现成配置妥当。要启用 Broker 代理日志记录，以便将日志记录到 syslog，需要进行以下配置：

编辑 /etc/rsyslog.conf 文件并添加以下行：

```
$ModLoad imudp
```

```
$UDPServerRun 514
```

保存并关闭 rsyslog.conf 文件。重新启动 rsyslog 服务，以使更改生效：

```
sudo /sbin/service rsyslog restart
```

HDX 会话无法启动时的解决方法

确保不存在任何孤立进程，以免其阻碍新会话启动：

```
sudo pkill -9 ctxhdx
```

```
sudo pkill -9 ctxgfx
```

```
sudo pkill -9 ctxlogin
```

```
sudo pkill -9 ctxvfb
```

重新启动 Linux VDA 服务并重新尝试连接。

确认关键目录和文件的所有权和权限

检查以下目录和文件的文件所有权和权限：

- /var - Owner: root, Group: root, Permissions: 0755
- /var/xdl - Owner: ctxsrvr, Group: ctxadm, Permissions: 0755
- /var/xdl/.isacagent - Owner: root, Group: root, Permissions: 0666
- /var/xdl/.winsta - Owner: ctxsrvr, Group: ctxadm, Permissions: 0777
- /var/xdl/vda - Owner: root, Group: root, Permissions: 0755

HDX 3D Pro 多监视器重绘问题

如果在非主监视器屏幕上发生重绘问题，请检查 NVIDIA GRID 许可证是否可用。

听不到声音

确认运行 Citrix Receiver 的设备以及 Linux 桌面的音量控件未设为静音或未设为较低的音量。

确认在 Linux VDA 上启用了音频。使用 ctxreg 工具查询配置项目 fDisableCam 的值：

```
sudo ctxreg read -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v fDisableCam
```

值 0x1 表示禁用音频。要启用音频，请将 fDisableCam 设置为 0x0：

```
sudo ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v fDisableCam -d 0x00000000
```

如果仍听不到声音，请检查 pulseaudio 是否加载了 Citrix 音频接收器。此 PulseAudio 模块会在会话启动时加载到 pulseaudio 守护程序中。使用 pacmd 工具检查 Citrix 音频接收器是否已加载：

```
pacmd list-sinks
```

如果 Citrix 音频接收器已加载，则输出应为：

```
name:
```

```
driver:
```

如果 Citrix 音频接收器未加载，请终止 ctxaudio 进程并重新启动该进程。

无法录制音频

检查是否在 Linux VDA 上启用了音频以及是否在 ICA 客户端上启用了音频录制。如果仍无法录制音频，请检查 pulseaudio 是否加载了 Citrix 音频源。如果 ICA 客户端上启用了音频录制，此 PulseAudio 模块会在会话启动时加载到 pulseaudio 守护程序。使用 pacmd 工具检查 Citrix 音频源是否已加载：

```
pacmd list-sources
```

如果 Citrix 音频源已加载，则输出应为：

```
name:
```

```
driver:
```

如果 Citrix 音频源未加载，请终止 ctxaudio 进程并重新启动该进程。

无法打印

打印不正常时要检查若干项目。打印守护程序是一个按会话进程，应在会话期间内运行。检查打印守护程序是否正在运行。

```
ps -ef | grep ctxlpmngt
```

如果 ctxlpmngt 进程未在运行，请从命令行手动启动 ctxlpmngt。

如果仍无法打印，请在 CUPS 框架中检查下一个项目。ctxcups 服务用于打印机管理，并负责与 Linux CUPS 框架通信。此进程在每个计算机上有一个，可通过以下方式检查：

```
service ctxcups status
```

如果服务未在运行，请手动启动：

```
service ctxcups start
```

打印输出乱码

输出乱码可能是打印机驱动程序不兼容造成的。系统中为每个用户提供了驱动程序配置，该配置可通过编辑 ~/.CtxlpProfile 配置文件进行配置。

```
[DEFAULT_PRINTER]
```

```
printername=
```

```
model=
```

```
ppdpath=
```

```
drivertype=
```

printername 字段含有当前客户端默认打印机的名称。这是一个只读值，不应进行编辑。

Important

不应同时设置 ppdpath、model 和 drivertype 字段，因为映射的打印机只能使用其中一个字段。

如果通用打印机驱动程序与客户端打印机不兼容，则本机打印机驱动程序的型号可使用 model= 选项配置。打印机的当前型号名称可使用 lpinfo 命令查找。

```
lpinfo -m
```

```
...
```

```
xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
```

```
xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
```

```
xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
```

...

随后，可设置与打印机匹配的型号：

```
Model=xerox/ph3115.ppd.gz
```

如果通用打印机驱动程序与客户端打印机不兼容，则可以配置本机打印机驱动程序的 ppd 文件路径。ppdpath 值为本机打印机驱动程序文件的绝对路径。

例如，/home/tester/NATIVE_PRINTER_DRIVER.ppd 下就有一个 ppd 驱动程序。

```
ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
```

Citrix 提供了三种类型的通用打印机驱动程序（postscript、pcl5 和 pcl6）。如果本机打印机驱动程序不可用，则可在驱动程序类型中配置这些驱动程序。

例如，如果客户端默认打印机驱动程序类型为 PCL5。

```
drivertype=pcl5
```

注意

Citrix Receiver for Mac 和 Citrix Receiver for Linux 仅支持 Postscript 打印机，因此 PCL5 和 PCL6 通用打印机驱动程序不适用。在此情况下，本机打印机驱动程序的 ppdpath 或型号应设为非 Postscript 打印机。

已知问题

Citrix Receiver for Android CAPS LOCK 状态可能会在会话漫游时反转

与 Citrix Receiver for Android 的现有连接漫游时，CAPS LOCK 状态可能会丢失。解决方法是使用扩展键盘上的 shift 键切换大小写。

使用 Citrix Receiver for Mac 连接至 Linux VDA 时，含 ALT 的快捷键并不总是正常工作

默认情况下，对于左侧和右侧 Options/Alt 键，Citrix Receiver for Mac 都会发送 AltGr。此设置可在 Citrix Receiver 设置内更改，但在不同应用程序上的更改效果各异。

在 SuSE Linux Enterprise Desktop 11 上，较新的 X 客户端库可能会导致键盘映射问题

在 SuSE Linux Enterprise Desktop 11 上，较新版本的 xorg-x11-libX11 软件包在处理键盘映射更改时可能会出现问题，进而可能导致 HDX 会话期间的键盘功能出现问题。已安装的软件包版本在 7.4-5.11.11.1 至 7.4-5.11.15.1 范围内时可能会出现此问题。

解决方法是将 xorg-x11-libX11 软件包回滚至原来的 SP3 版本，从而使得键盘映射更改能够正常发挥作用。例如：

```
rpm -i --force xorg-x11-libX11-7.4-5.9.1
```

```
rpm -i --force xorg-x11-libX11-32bit-7.4-5.9.1
```

```
rpm -e xorg-x11-libX11-7.4-5.11.15.1
```

```
rpm -e xorg-x11-libX11-32bit-7.4-5.11.15.1
```

需要在用户登录到计算机之前完成此设置。如果在会话处于活动状态期间完成，则只有在用户下次登录时，这些设置才会生效。

如果要从原来的 SP3 进行升级，则上述 xorg-x11-libX11 软件包会锁定为当前已安装版本，从而确保它们不会在升级期间发生更改。升级前，请先运行以下命令，然后再照常执行升级操作：

```
zypper al xorg-x11-libX11
```

```
zypper al xorg-x11-libX11-32bit
```

如果在 XenDesktop v7.1 中将 Linux VDA 与 Delivery Controller 结合使用，则会话启动时间可能会较长

之所以启动较慢，是因为 v7.1 Delivery Controller 生成的 ICA 文件中存在 CGP 设置。如果存在这些设置，Citrix Receiver 会尝试使用 TCP 端口 2598 建立连接。在某些 Linux 发行版（例如 SLED 12）上，默认防火墙设置会丢弃 TCP SYN 数据包，从而导致超时，并延长会话启动时间。解决方法是，在 Linux VDA 上配置防火墙，使其拒绝端口 2598 上的 TCP SYN。在新版 Delivery Controller 中，此问题已得到解决。

Linux VDA 重新加入域时注册失败

在某些情况下，在 Linux VDA 重新加入域且生成一组全新的 Kerberos 密钥后，Broker 无法与 VDA 建立安全上下文。出现此问题的原因通常是，Broker 使用的是缓存的过时 VDA 服务票据，该票据是基于先前的一组 Kerberos 密钥的。此问题不会阻止 VDA 连接到 Broker，但 Broker 将无法与 VDA 建立返回安全上下文。常见症状是 VDA 注册失败。

由于 VDA 服务票据迟早会过期并进行续订，因此此问题最终会自行解决，但是，服务票据的有效期一般会很长。此过程可能需要数小时。

解决方法是清除 Broker 的票据缓存。您只需重新启动 Broker 或在 Broker 上以管理员身份从命令提示窗口运行以下命令：

```
klist -li 0x3e4 purge
```

此命令会清除 Citrix Broker Service 运行所在的网络服务主体持有的 LSA 缓存中的所有服务票据。此命令也会删除其他 VDA 的服务票据，因而可能会影响其他服务。但是，此操作不会造成负面影响，因为这些服务会在需要时从 KDC 重新获取这些服务票据。

在将 HDX 3D Pro 和 GNOME 结合使用时，缺少锁屏界面图标

在 NVIDIA Grid 驱动程序处于活动状态时，Gnome Desktop Manager (GDM) 未处于活动状态，而 GDM 锁屏界面功能不可用。

不支持音频即插即用

建议先将音频捕获设备连接至客户端计算机，然后再开始在 ICA 会话中录制音频。如果在启动音频录制应用程序后再连接设备，应用程序可能会无响应。如果出现此问题，只需重新启动应用程序即可。如果在录制期间拔下捕获设备，也会出现类似的问题。

音频失真

Windows 10 Receiver 可能会在音频录制期间遇到音频失真问题。

CTXPS 驱动程序与部分 PLC 打印机不兼容

如果发现打印输出损坏，请将打印机驱动程序设置为制造商提供的本机打印机驱动程序。

打印大文档时打印速度较慢

在本地客户端打印机上打印大文档时，打印文件会通过服务器连接进行传输。如果连接的速度很慢，这一过程就可能需要很长时间。

其他会话中的打印机和打印作业通知

Linux 的会话概念与 Windows 操作系统不同。因此，所有用户都会获得系统范围的通知。管理员可禁用这些通知，方法是修改 CUPS 配置文件 `/etc/cups/cupsd.conf`。

查找文件中配置的当前策略名称。

```
DefaultPolicy default
```

如果策略名称为 `default`，则将以下行添加到默认策略 XML 块中。

```
# Job/subscription privacy...

JobPrivateAccess default

JobPrivateValues default

SubscriptionPrivateAccess default

SubscriptionPrivateValues default

... ..

Require user @OWNER

Order deny,allow

Order deny,allow
```

词汇表

Broker - XenDesktop 组件，负责将 HDX 会话代理给 XenDesktop 部署中的不同 VDA。也称为 DDC 或 XenDesktop Controller。

Broker 代理 - Linux VDA 计算机上的组件，负责提供要交付的桌面。Broker 代理会与 Broker 通信，以启用会话代理服务。它由两个关键组件构成，分别是 VDA Service 和 HDX Service。

Citrix Director - Citrix 帮助台/支持控制台，用于监控和控制 XenDesktop VDA。

Citrix Studio - Citrix 管理控制台，用于配置 XenDesktop。

DDC - XenDesktop Desktop Delivery Controller。也称为 Broker 或 Delivery Controller。

FQDN - 完全限定的域名

HDX - 高清体验协议。以前称为 Citrix ICA 协议。

HDX Service - 一种 Linux 服务 (ctxhdx)，用来通过 HDX 协议远程控制 Linux 虚拟桌面。它会与 VDA 服务通信，以便启用会话代理服务。

RHEL - Red Hat Enterprise Linux。Red Hat 提供的商用 Linux 发行版。

SLED - SUSE Linux Enterprise Desktop。Novell 提供的商用 Linux 发行版。

SLES - SUSE Linux Enterprise Server。Novell 提供的商用 Linux 发行版。

VDA - Virtual Delivery Agent。

VDA Service - 一种 Linux 服务 (ctxvda)，用来与 Broker 通信，以启用会话代理服务。它也会与 HDX Service 通信，从而进行远程会话交付。

安装 SUSE Linux VDA

Apr 25, 2016

您可以基于 SUSE 发行版创建 Linux 虚拟桌面。准备您的 Linux 虚拟机，在其上安装新的 [Linux VDA 软件](#)，配置 Delivery Controller，然后使用 Studio 向用户提供这些桌面。

有关详细信息，请参阅以下文档。

 [安装 SUSE Linux VDA](#)

含有 SUSE Linux VDA 1.2 版安装和设置说明的 PDF 文件。

注意

本文中使用的 Linux shell 命令经确认可在 GNU Bash shell 上使用。

本文包括以下几节：

- [系统要求](#)
- [配置 Delivery Controller](#)
- [准备 Linux 计算机以安装 VDA](#)
- [配置 Linux 计算机目录和交付组](#)
- [安装 Linux VDA 软件](#)
- [运行 VDA 软件](#)
- [卸载 Linux VDA 软件](#)
- [故障排除](#)
- [已知问题](#)
- [词汇表](#)

系统要求

Linux 虚拟桌面产品支持以下 Linux 发行版：

- SUSE Linux Enterprise :
 - Desktop 11 Service Pack 4
 - Desktop 12 Service Pack 1
 - Server 11 Service Pack 4
 - Server 12 Service Pack 1
- Red Hat Enterprise Linux
 - Workstation 6.7
 - Workstation 7.2
 - Server 6.7
 - Server 7.2

注意

在所有情况下，支持的处理器架构均为 x86-64。

Linux VDA 支持以下版本的 XenDesktop：

- XenDesktop 7.1
- XenDesktop 7.5
- XenDesktop 7.6
- XenDesktop 7.7
- XenDesktop 7.8

Linux VDA 与 Windows VDA 的配置过程稍有不同。但是，所有 Delivery Controller 场都能为 Windows 和 Linux 桌面提供代理服务。

注意

Linux VDA 与 XenDesktop 7.0 或更低版本不兼容。

支持使用以下版本的 Citrix Receiver：

- Citrix Receiver for Windows 4.4 或更高版本（相当于 v14.4 版本的 wfica32.exe）
- Citrix Receiver for Linux 13.3 或更高版本
- Citrix Receiver for Mac OSX 12.1 或更高版本
- Citrix Receiver for Android 3.8 或更高版本
- Citrix Receiver for iOS 6.1.4 或更高版本
- Citrix Receiver for Chrome/HTML5 1.9 版本（只能通过 Access Gateway 使用）

支持使用以下虚拟机管理程序托管 Linux VDA 客户机虚拟机：

- XenServer
- VMware ESX 和 ESXi
- Microsoft Hyper-V

也支持裸机托管。

提示

有关支持的平台的列表，请参阅虚拟机管理程序提供商的文档。

Linux VDA 支持以下 Active Directory 集成软件包或产品：

- Samba Winbind
- Quest Authentication Services v4.1 或更高版本
- Centrify DirectControl

提示

有关支持的平台的列表，请参阅 Active Directory 集成软件包提供商的文档。

配置 Delivery Controller

XenDesktop 7.7 或更高版本包括为支持 Linux 虚拟桌面而作出的必要更改，但以前的版本需要安装修补程序或更新脚本。本节将介绍这些产品的安装和验证工作。

对于 XenDesktop 7.6 SP2，请应用 Hotfix Update 2 更新 Linux 虚拟桌面的 Broker。Hotfix Update 2 可在以下位置找到：

- [CTX142438](#)：Hotfix Update 2 - 适用于 Delivery Controller 7.6（32 位）– 英文版
- [CTX142439](#)：Hotfix Update 2 - 适用于 Delivery Controller 7.6（64 位）– 英文版

对于早期版本的 XenDesktop，可使用名为 **Update-BrokerServiceConfig.ps1** 的 PowerShell 脚本更新 Broker Service 配置。此脚本可在以下软件包中找到：

- citrix-linuxvda-scripts-1.2.0.zip

为场内的每个 Delivery Controller 重复以下步骤：

1. 将 **Update-BrokerServiceConfig.ps1** 脚本复制到 Delivery Controller 计算机。
2. 在本地管理员上下文中打开 Windows PowerShell 控制台。
3. 浏览到脚本所在的文件夹。
4. 执行脚本：

```
.\Update-BrokerServiceConfig.ps1
```

注意

PowerShell 的默认配置是禁止执行 PowerShell 脚本。如果脚本运行失败，您可能需要先更改 PowerShell 执行策略，然后再重试：

```
Set-ExecutionPolicy Unrestricted
```

Update-BrokerServiceConfig.ps1 脚本会为 Broker Service 配置文件更新 Linux VDA 所需的全新 WCF 端点，然后重新启动 Broker Service。该脚本会自动确定 Broker Service 配置文件的位置。同一个目录中会创建原始配置文件的备份，该备份的扩展名为 **.prelinux**。

这些更改不会影响配置为使用同一个 Delivery Controller 场的 Windows VDA 的代理。因此，一个 Controller 场可同时无缝管理 Windows 和 Linux VDA 的代理会话。

要验证所需的配置更改是否已应用于 Delivery Controller，请确认字符串 **EndpointLinux** 是否在以下文件中出现五次：

```
%PROGRAMFILES%\Citrix\Broker\Service\BrokerService.exe.config
```

从 Windows 命令提示窗口，以本地管理员身份登录：

```
cd "%PROGRAMFILES%" \Citrix\Broker\Service\  
findstr EndpointLinux BrokerService.exe.config
```

准备 Linux 计算机以安装 VDA

SUSE Linux Enterprise YaST 工具用于对操作系统执行方方面面的配置。

启动基于文本的 YaST 工具：

```
su -
```

```
yast
```

或者，启动基于 UI 的 YaST 工具：

```
su -
```

```
yast2 &
```

以下几节介绍如何配置 Linux VDA 使用的各种网络设置和服务。网络配置应通过 YaST 工具执行，而不得使用其他方法，例如 Network Manager。以下说明介绍的是使用基于 UI 的 YaST 工具的情形；基于文本的 YaST 工具也可以使用，但导航方法稍有不同，对此本文未作介绍。

配置主机名和 DNS

1. 打开 YaST 网络设置。
2. 仅限 SLED 12：在 **Global Options**（全局选项）选项卡上，将 **Network Setup Method**（网络设置方法）更改为 **Wicked Service**（Wicked 服务）。
3. 打开 **Hostname/DNS**（主机名/DNS）选项卡。
4. 取消选中 **Change hostname via DHCP**（通过 DHCP 更改主机名）。
5. 选中 **Assign Hostname to Loopback IP**（向环回 IP 分配主机名）。
6. 编辑以下内容，以反映所作的网络设置：

- 主机名 – 添加计算机的 DNS 主机名。
- 域名 – 添加计算机的 DNS 域名。
- 名称服务器 – 添加 DNS 服务器的 IP 地址。这通常是 AD 域控制器的 IP 地址。

- 域搜索列表 – 添加 DNS 域名。

注意

Linux VDA 当前不支持 NetBIOS 名称截断，因此主机名不得超过 15 个字符。

禁用多播 DNS

只有在 SLED 上，默认设置才会启用多播 DNS (mDNS)，而这可能会导致名称解析结果不一致。默认情况下，SLES 上未启用 mDNS，因此无需任何操作。

要禁用 mDNS，请编辑 `/etc/nsswitch.conf`，并更改含有以下内容的行：

```
hosts: files mdns_minimal [NOTFOUND=return] dns
```

更改为：

```
hosts: files dns
```

检查主机名

验证主机名设置是否正确无误：

```
hostname
```

这应该仅返回计算机的主机名，而不是完全限定的域名 (FQDN)。

验证 FQDN 设置是否正确无误：

```
hostname -f
```

这应该返回计算机的 FQDN。

检查名称解析和服务可访问性

验证能否解析 FQDN 并 Ping 通域控制器和 XenDesktop Delivery Controller：

```
nslookup domain-controller-fqdn
```

```
ping domain-controller-fqdn
```

```
nslookup delivery-controller-fqdn
```

```
ping delivery-controller-fqdn
```

如果无法解析 FQDN 或 Ping 不通上述任一计算机，请先检查相关步骤，然后再继续。

确保 VDA、XenDesktop Controller 和域控制器之间的时钟始终精确同步至关重要。将 Linux VDA 托管为虚拟机可能会导致时钟偏差问题。出于此原因，最好使用远程 NTP 服务来保持时间同步。默认 NTP 设置可能需要作一些更改：

1. 打开 YaST 的“NTP Configuration”（NTP 配置），然后选择 **General Settings**（常规设置）选项卡。
2. 在“Start NTP Daemon”（启动 NTP 守护程序）部分，选中 **Now and on Boot**（现在及引导时）。
3. 如果存在 **Undisciplined Local Clock (LOCAL)**（无序本地时钟 (LOCAL)）项目，请选择该项目，然后单击 **Delete**（删除）。
4. 单击 **Add**（添加），添加一个 NTP 服务器条目。
5. 选择 **Server Type**（服务器类型），然后单击 **Next**（下一步）。
6. 在“Address”（地址）字段输入 NTP 服务器的 DNS 名称。此服务通常托管在 Active Directory 域控制器上。
7. 将“Options”（选项）字段保持不变。
8. 单击 **Test**（测试）检查 NTP 服务是否可访问。
9. 在随后的一系列窗口中一直单击 **OK**（确定）保存更改。

注意

对于 SLES 12 实施，如果 NTP 守护程序启动失败，这可能是 SUSE 上与 AppArmor 策略有关的一个已知问题造成的。有关详细信息，请参照[此处](#)的解决方案。

适用于 Suse Linux Enterprise 的 Linux VDA 软件依赖于以下软件包：

- PostgreSQL
 - SLED/SLES 11：9.1 或更高版本
 - SLED/SLES 12：9.3 或更高版本
- OpenJDK 1.7.0
- OpenMotif Runtime Environment 2.3.1 或更高版本
- Cups
 - SLED/SLES 11：1.3.7 或更高版本
 - SLED/SLES 12：1.6.0 或更高版本
- Foomatic 筛选器
 - SLED/SLES 11：3.0.0 或更高版本
 - SLED/SLES 12：1.0.0 或更高版本
- ImageMagick
 - SLED/SLES 11：6.4.3.6 或更高版本
 - SLED/SLES 12：6.8 或更高版本

添加存储库

一些必需的软件包在某些 Suse Linux Enterprise 存储库中不可用：

- SLED 11：PostgreSQL 在 SLES 11 中可用，但在 SLED 11 中不可用。
- SLES 11：OpenJDK 和 OpenMotif 在 SLED 11 中可用，但在 SLES 11 中不可用。
- SLED 12：PostgreSQL 在 SLES 12 中可用，但在 SLED 12 中不可用。ImageMagick 可通过 SLE 12 SDK ISO 或联机存储库提供。
- SLES 12：没有问题；所有软件包都可用。ImageMagick 可通过 SLE 12 SDK ISO 或联机存储库提供。

要解决此问题，建议的方法是从正在安装的 SLE 的替换版本的介质中获取缺失的软件包。也就是说，从 SLES 介质中获取 SLED 安装缺失的软件包，以及从 SLED 介质中获取 SLES 安装缺失的软件包。下述方法会装载 SLED 和 SLES ISO 介质文件并

添加存储库。

SLED 11	<pre>sudo mkdir -p /mnt/sles sudo mount -t iso9660 \ path-to-iso/SLES-11-SP3-DVD-x86_64-GM-DVD1.iso /mnt/sles sudo zypper ar -f /mnt/sles sles</pre>
SLES 11	<pre>sudo mkdir -p /mnt/sled sudo mount -t iso9660 \ path-to-iso/SLED-11-SP3-DVD-x86_64-GM-DVD1.iso /mnt/sled sudo zypper ar -f /mnt/sled sled</pre>
SLED 12	<pre>sudo mkdir -p /mnt/sles sudo mount -t iso9660 \ path-to-iso/SLES-12-DVD-x86_64-GM-DVD1.iso /mnt/sles sudo zypper ar -f /mnt/sles sles</pre>
SLED/SLES 12	<pre>sudo mkdir -p /mnt/sdk sudo mount -t iso9660 \ path-to-iso/SLE-12-SDK-DVD-x86_64-GM-DVD1.iso /mnt/sdk sudo zypper ar -f /mnt/sdk sdk</pre>

安装 Kerberos 客户端

安装 Kerberos 客户端，在 Linux VDA 与 XenDesktop Controller 之间实现双向身份验证：

```
sudo zypper install krb5-client
```

Kerberos 客户端配置依赖于所使用的 Active Directory 集成方法，后者将在下文说明。

安装 OpenJDK

Linux VDA 依赖于 OpenJDK 1.7.0。

提示

为避免问题，请确保仅安装 1.7.0 版本的 OpenJDK。删除系统上的所有其他版本 Java。

SLED	在 SLED 上，Java 运行时环境应该已随操作系统一起安装。使用以下命令进行确认： <pre>sudo zypper info java-1_7_0-openjdk</pre> 如果状态显示为过时，请更新为最新版本： <pre>sudo zypper update java-1_7_0-openjdk</pre> 检查 Java 版本： <pre>java -version</pre>
SLES	在 SLES 上，您需要安装 Java 运行时环境： <pre>sudo zypper install java-1_7_0-openjdk</pre> 检查 Java 版本： <pre>java -version</pre>

安装 PostgreSQL

SLED/SLES 11	安装软件包： <pre>sudo zypper install libecpg6</pre> <pre>sudo zypper install postgresql?init</pre> <pre>sudo zypper install postgresql91</pre> <pre>sudo zypper install postgresql91?server</pre> <pre>sudo zypper install postgresql?jdbc</pre> 此时需要执行一些安装后步骤，以便初始化数据库服务，并确保 PostgreSQL 在引导时启动： <pre>sudo /sbin/insserv postgresql</pre> <pre>sudo /etc/init.d/postgresql restart</pre>
SLED/SLES 12	安装软件包： <pre>sudo zypper install postgresql-init</pre> <pre>sudo zypper install postgresql93-server</pre> <pre>sudo zypper install postgresql-jdbc</pre> 此时需要执行安装后步骤，以便初始化数据库服务，并确保 PostgreSQL 在引导时启动：

	<pre>sudo systemctl enable postgresql</pre> <pre>sudo systemctl restart postgresql</pre> 数据库文件将驻留在 /var/lib/pgsql/data 下。

安装 OpenMotif 运行时环境

Linux VDA 要求使用 motif 或 openmotif 软件包，具体取决于发行版。

SLED/SLES 11	安装软件包： <pre>sudo zypper install openmotif-libs</pre>
SLED/SLES 12	安装软件包： <pre>sudo zypper install motif</pre>

安装打印支持

Linux VDA 要求使用 cups 和 foomatic 筛选器。

SLED/SLES 11	安装软件包： <pre>sudo zypper install cups</pre> <pre>sudo zypper install foomatic-filters</pre>
SLED/SLES 12	安装软件包： <pre>sudo zypper install cups</pre> <pre>sudo zypper install cups-filters-foomatic-rip</pre>

安装 ImageMagick

安装 ImageMagick 软件包：

```
sudo zypper install ImageMagick
```

删除存储库

安装依赖的软件包后便可以删除之前设置的替代版本存储库并卸载介质：

SLED 11	删除以下软件包： <pre>sudo zypper rr sles</pre>

	<pre>sudo umount /mnt/sles</pre> <pre>sudo rmdir /mnt/sles</pre>
SLES 11	删除以下软件包： <pre>sudo zypper rr sled</pre> <pre>sudo umount /mnt/sled</pre> <pre>sudo rmdir /mnt/sled</pre>
SLED 12	删除以下软件包： <pre>sudo zypper rr sles</pre> <pre>sudo umount /mnt/sles</pre> <pre>sudo rmdir /mnt/sles</pre>
SLED/SLES 12	删除以下软件包： <pre>sudo zypper rr sdk</pre> <pre>sudo umount /mnt/sdk</pre> <pre>sudo rmdir /mnt/sdk</pre>

在支持的虚拟机管理程序上将 Linux VDA 当作虚拟机运行时，需要作出一些更改。根据使用的虚拟机管理程序平台作出以下更改。如果正在裸机硬件上运行 Linux 计算机，则无需作出任何更改。

修复 Citrix XenServer 上的时间同步问题

如果启用了 XenServer 时间同步功能，则在每个半虚拟化 Linux VM 中，您会发现 NTP 和 XenServer 都在尝试管理系统时钟。为避免时钟与其他服务器不同步，每个 Linux 客户机中的系统时钟都必须与 NTP 同步。这要求禁用主机时间同步。无需在 HVM 模式下进行任何更改。

在某些 Linux 发行版中，如果正在运行半虚拟化 Linux 内核，并安装了 XenServer Tools，您可以检查 XenServer 时间同步功能是否存在，以及是否已在 Linux VM 中启用：

```
su -
```

```
cat /proc/sys/xen/independent_wallclock
```

此时会返回以下任一项：

- 0 - 时间同步功能已启用，并需要禁用。
- 1 - 时间同步功能已禁用，无需采取任何操作。

如果 `/proc/sys/xen/indepent_wallclock` 文件不存在，则无需执行以下步骤。

如果已启用，请向该文件写入 1 以禁用时间同步功能：

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
```

要使此更改成为永久更改，并在重新启动后仍然有效，请编辑 `/etc/sysctl.conf` 文件并添加以下行：

```
xen.independent_wallclock = 1
```

要验证这些更改，请重新启动系统：

```
reboot
```

重新启动后，请检查此设置是否正确无误：

```
su -
```

```
cat /proc/sys/xen/independent_wallclock
```

此时应返回值 1。

在 Microsoft Hyper-V 上修复时间同步问题

安装了 Hyper-V Linux 集成服务的 Linux VM 可利用 Hyper-V 时间同步功能来使用主机操作系统的时间。为确保系统时钟始终精确可靠，此功能应随 NTP 服务一同启用。

从管理操作系统中：

1. 打开 Hyper-V 管理器控制台。
2. 对于 Linux VM 的设置，请选择 **Integration Services**（集成服务）。
3. 确保已选择 **Time synchronization**（时间同步）。

注意

此方法与 VMware 和 XenServer 不同，这两种产品会禁用主机时间同步功能，以免与 NTP 发生冲突。Hyper-V 时间同步可以与 NTP 时间同步共存并互补。

修复 ESX 和 ESXi 上的时间同步问题

如果启用了 VMware 时间同步功能，则在每个半虚拟化 Linux VM 中，您会发现 NTP 和虚拟机管理程序都在尝试同步系统时钟。为避免时钟与其他服务器不同步，每个 Linux 客户机中的系统时钟都必须与 NTP 同步。这要求禁用主机时间同步。

如果正在运行安装了 VMware Tools 的半虚拟化 Linux 内核：

1. 打开 vSphere Client。
2. 编辑 Linux VM 设置。
3. 在 **Virtual Machine Properties**（虚拟机属性）对话框中，打开 **Options**（选项）选项卡。
4. 选择“VMware Tools”。
5. 在 **Advanced**（高级）框中，取消选中 **Synchronize guest time with host**（与主机同步客户机时间）。

将 Linux 计算机添加至 XenDesktop for Linux 支持的 Active Directory 域有多种方法：

- Samba Winbind
- Quest Authentication Service
- Centrify DirectControl

根据所选的方法，按以下说明执行操作。

Samba Winbind

加入 Windows 域

这需要您的域控制器可访问，而且您的 Active Directory 用户帐户有权将计算机添加到域：

1. 打开 YaST 的“Windows Domain Membership”（Windows 域成员身份）。
2. 执行以下更改：
 - 将域或工作组设为 Active Directory 域的名称或域控制器的 IP 地址。确保输入的域为大写。
 - 选中“Also Use SMB information for Linux Authentication”（同时为 Linux 身份验证使用 SMB 信息）。
 - 选中“Create Home Directory on Login”（在登录时创建主目录）。
 - 选中“Single Sign-on for SSH”（为 SSH 使用单点登录）。
 - 确保未选中“Offline Authentication”（脱机身份验证）。此选项与 Linux VDA 不兼容。
3. 单击“OK”（确定）。如果提示安装某些软件包，请单击“Install”（安装）。
4. 如果找到域控制器，则会询问您是否要加入域。单击是。
5. 出现提示时，输入有权将计算机添加至域的域用户的凭据，然后单击“OK”（确定）。
6. 此时会显示一条消息，说明添加成功。
7. 如果提示安装某些 samba 和 krb5 软件包，请单击“Install”（安装）。

YaST 可能会说明这些更改需要重新启动一些服务或需要重新启动计算机。建议执行重新启动：

```
su -
```

```
reboot
```

仅限 SLED/SLES 12：修补 Kerberos 凭据缓存名称

SLED/SLES 12 已将默认 Kerberos 凭据缓存名称规范从常用的 FILE:/tmp/krb5cc_%{uid} 更改为 DIR:/run/user/{uid}/krb5cc。这种全新 DIR 缓存方法与 Linux VDA 不兼容，必须进行手动更改。以 root 用户身份，编辑 /etc/krb5.conf 并在 [libdefaults] 部分下添加以下设置（如果尚未设置）：

```
default_ccache_name = FILE:/tmp/krb5cc_%{uid}
```

验证域成员身份

XenDesktop Controller 要求所有 VDA 计算机（不论是 Windows 还是 Linux）都要在 Active Directory 中有一个计算机对象。

使用 Samba 的 net ads 命令验证计算机已加入域：

```
sudo net ads testjoin
```

使用以下命令验证其他域和计算机对象信息：

```
sudo net ads info
```

验证 Kerberos 配置

要验证 Kerberos 已正确配置为可与 Linux VDA 配合使用，请检查系统 keytab 文件是否已创建并含有有效密钥：

```
sudo klist -ke
```

此时应显示各种主体名称与密码套件组合可用的密钥列表。运行 Kerberos kinit 命令，使用这些密钥向域控制器验证计算机的身份：

```
sudo kinit -k MACHINE/$@REALM
```

计算机和领域名称必须指定为大写，而美元符号 (\$) 必须使用反斜杠 (\) 进行转义，以免发生 shell 替换。在某些环境中，DNS 域名与 Kerberos 领域名称不同；请确保使用领域名称。如果此命令成功运行，则不会显示任何输出。

使用以下命令验证计算机帐户的 TGT 票据已缓存：

```
sudo klist
```

使用以下命令检查计算机帐户详细信息：

```
sudo net ads status
```

验证用户身份验证

使用 wbinfo 工具验证是否可向域验证域用户的身份：

```
wbinfo --krb5auth=domain\\username%password
```

这里指定的域为 AD 域名，而不是 Kerberos 领域名称。对于 bash shell，必须使用另一个反斜杠对反斜杠 (\) 字符进行转义。此命令会返回一条成功或失败消息。

要验证 Winbind PAM 模块是否配置正确，请使用以前未曾登录计算机的域用户帐户在本地登录：

```
ssh localhost -l domain\\username
```

```
id -u
```

检查是否为 id -u 命令返回的 uid 创建了对应的 Kerberos 凭据缓存文件：

```
ls /tmp/krb5cc_uid
```

检查用户 Kerberos 凭据缓存中的票据是否有效且未过期：

```
klist
```

退出会话：

```
exit
```

直接登录 Gnome 或 KDE 控制台也可执行类似测试。

Quest Authentication Service

在域控制器上配置 Quest

这里假定您已在 Active Directory 域控制器上安装并配置了 Quest 软件，而且已获得管理权限，有权在 Active Directory 中创建计算机对象。

允许域用户登录 Linux VDA 计算机

对于需要在 Linux VDA 计算机上建立 HDX 会话的每个域用户：

1. 在 Active Directory 用户和计算机管理控制台中，为该用户帐户打开 Active Directory 用户属性。
2. 选择“Unix Account”（Unix 帐户）选项卡。
3. 选中“Unix-enabled”（已启用 Unix）。
4. 将“Primary GID Number”（首选 GID 编号）设为实际域用户组的组 ID。

注意

这些说明相当于设置域用户，以便他们可以使用控制台、RDP、SSH 或任何其他远程协议进行登录。

在 Linux VDA 上配置 Quest

配置 VAS 守护程序

自动续订 Kerberos 票据功能需要启用并断开，而身份验证（脱机登录）功能需要禁用：

```
sudo /opt/quest/bin/vastool configure vas vasd \  
    auto-ticket-renew-interval 32400  
  
sudo /opt/quest/bin/vastool configure vas vas_auth \  
    allow-disconnected-auth false
```

这会将续订间隔设为 9 小时（32400 秒），即比默认的 10 小时票据生命周期短 1 小时。请在 Kerberos 票据生命周期较短的系统上设置较低的值。

配置 PAM 和 NSS

Quest 要求将 PAM 和 NSS 手动配置为允许域用户通过 HDX 和其他服务（例如 su、ssh 和 RDP）进行登录。配置 PAM 和 NSS：

```
sudo /opt/quest/bin/vastool configure pam  
  
sudo /opt/quest/bin/vastool configure nss
```

加入 Windows 域

使用 Quest vastool 命令将 Linux 计算机加入 Active Directory 域：

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

用户为有权将计算机加入 Active Directory 域的域用户。域名为域的 DNS 名称，例如 example.com。

验证域成员身份

XenDesktop Controller 要求所有 VDA 计算机（不论是 Windows 还是 Linux）都要在 Active Directory 中有一个计算机对象。验证 Quest 加入的 Linux 计算机是否位于域中：

```
sudo /opt/quest/bin/vastool info domain
```

如果计算机已加入域，则会返回域名。如果未加入，则会显示以下错误：

```
ERROR: No domain could be found.
```

```
ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm
```

```
default_realm not configured in vas.conf. Computer may not be joined to domain
```

验证用户身份验证

要验证 Quest 能否使用 PAM 对域用户进行身份验证，请使用以前未曾登录计算机的域用户帐户进行登录：

```
ssh localhost -l domain\\username
```

```
id -u
```

检查是否为 id -u 命令返回的 uid 创建了对应的 Kerberos 凭据缓存文件：

```
ls /tmp/krb5cc_uid
```

检查用户 Kerberos 凭据缓存中的票据是否有效且未过期：

```
/opt/quest/bin/vastool klist
```

退出会话：

```
exit
```

直接登录 Gnome 或 KDE 控制台也可执行类似测试。

Centrify DirectControl

加入 Windows 域

安装 Centrify DirectControl Agent 后，请使用 Centrify **adjoin** 命令将 Linux 计算机加入 Active Directory 域：

```
su -
```

```
adjoin -w -V -u user domain-name
```

user 参数为有权将计算机加入 Active Directory 域的任何 Active Directory 域用户。**domain-name** 参数为将 Linux 计算机加入到的域的名称。

验证域成员身份

XenDesktop Controller 要求所有 VDA 计算机（不论是 Windows 还是 Linux）都要在 Active Directory 中有一个计算机对象。验证 Centrify 加入的 Linux 计算机是否位于域中：

```
su -  
  
adinfo
```

检查 **Joined to domain** 值是否有效以及 **CentrifyDC mode** 是否返回了 **connected**。如果模式仍然卡在启动状态，则表明 Centrify 客户端遇到了服务器连接或身份验证问题。

使用以下命令可获得更全面的系统和诊断信息：

```
adinfo --sysinfo all  
  
adinfo -diag
```

测试与各种 Active Directory 和 Kerberos 服务的连接：

```
adinfo --test
```

配置 Linux 计算机目录和交付组

创建计算机目录和添加 Linux VDA 计算机的过程与传统的 Windows VDA 方法十分类似。有关如何完成这些任务的更全面说明，请参阅联机 [Citrix 产品文档](#)。

创建含有 Linux VDA 计算机的计算机目录时会面临一些限制，这不同于为 Windows VDA 计算机创建计算机目录的过程：

- 对于操作系统，请：
 - 为托管共享桌面交付模型，选择 **Window 服务器操作系统或服务器操作系统选项**。
 - 为 VDI 专用桌面交付模型，选择 **Windows 桌面操作系统或桌面操作系统选项**。
- 确保计算机未执行电源管理设置。
- 由于 Linux VDA 不支持 PVS 和 MCS，请选择 **Another service or technology**（其他服务或技术）（现有映像）部署方法。
- 请勿在同一个计算机目录中混合使用 Linux 和 Windows VDA 计算机。

注意

早期版本的 Citrix Studio 不支持“Linux 操作系统”的概念；但是，选择 **Windows 服务器操作系统或服务器操作系统选项** 等同于使用托管共享桌面交付模型。选择 **Windows 桌面操作系统或桌面操作系统选项** 等同于使用 XenDesktop 每计算机一个用户交付模型。

有关创建计算机目录的 Citrix 文档如下所列：

- [XenDesktop 7.1](#)
- [XenDesktop 7.5](#)
- [XenDesktop 7.6](#)
- [XenDesktop 7.7](#)

- [XenDesktop 7.8](#)

更低版本的 XenDesktop 不支持使用。

提示

如果计算机离开后又重新加入 Active Directory 域，则需要先删除计算机，然后再将其重新添加到计算机目录。

创建交付组及添加含有 Linux VDA 计算机的计算机目录的过程与 Windows VDA 计算机几乎相同。有关如何完成这些任务的更全面说明，请参阅联机 Citrix 产品文档。

创建含有 Linux VDA 计算机目录的交付组时会面临以下限制：

- 对于交付类型，请选择“桌面”。Linux VDA 计算机不支持应用程序交付。
- 确保所选的 AD 用户和组已正确配置，可以登录到 Linux VDA 计算机。
- 请勿允许未经身份验证的（匿名）用户登录。
- 请勿在交付组中混入含有 Windows 计算机的计算机目录。

有关创建交付组的 Citrix 文档如下所列：

- [XenDesktop 7.1](#)
- [XenDesktop 7.5](#)
- [XenDesktop 7.6](#)
- [XenDesktop 7.7](#)
- [XenDesktop 7.8](#)

更低版本的 XenDesktop 不支持使用。

安装 Linux VDA 软件

如果之前安装的 Linux VDA 版本低于 v1.0，则应先卸载该版本，然后再安装新版本。

停止 Linux VDA 服务：

```
sudo /sbin/service ctxvda stop
```

```
sudo /sbin/service ctxhdx stop
```

卸载软件包：

```
sudo rpm -e XenDesktopVDA
```

Important

不支持将技术预览版升级至 v1.0、v1.1 或 v1.2。

使用 RPM 软件包管理器安装 Linux VDA 软件：

对于 SuSE 11：

```
sudo rpm -i XenDesktopVDA-1.2.0.282-1.x86_64.rpm
```

对于 SuSE 12：

```
sudo rpm -i XenDesktopVDA-1.2.0.282-1.x86_64.rpm
```

Important

安装 Linux VDA 后，Citrix 建议运行以下命令来提高安全性：

```
sudo sed -i '/ip addr | awk /a xhost"-LOCAL:""/usr/local/bin/ctxsession.sh
```

如果之前安装了 Linux VDA v1.1，请使用 RPM 软件包管理器升级 Linux VDA 软件：

对于 SuSE 11：

```
sudo rpm -U XenDesktopVDA-1.2.0.282-1.x86_64.rpm
```

对于 SuSE 12：

```
sudo rpm -U XenDesktopVDA-1.2.0.282-1.x86_64.rpm
```

Important

升级 Linux VDA 后，Citrix 建议运行以下命令来提高安全性：

```
sudo sed -i '/ip addr | awk /a xhost"-LOCAL:""/usr/local/bin/ctxsession.sh
```

安装软件包后，您需要运行 **ctxsetup.sh** 脚本来配置 Linux VDA。如果升级了软件包，您需要运行 **ctxsetup.sh** 脚本来完成升级操作。执行任何更改前，此脚本会验证环境，确保所有依赖项都已安装。如果需要，您也可以随时重新运行此脚本来更改设置。

该脚本可在出现提示时手动运行，也可使用预配置的响应自动运行。继续操作前，请查看此脚本的帮助信息：

```
sudo /usr/local/sbin/ctxsetup.sh -help
```

提示配置

运行会提示各种问题的手动配置：

```
sudo /usr/local/sbin/ctxsetup.sh
```

自动配置

自动安装时，设置脚本所需的选项可由环境变量提供。如果所需的所有变量都存在，则脚本不会提示用户提供任何信息，从而通过脚本完成安装过程。

支持的环境变量包括：

- CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N - Virtual Delivery Agent 支持使用 DNS CNAME 记录指定 Delivery Controller 名称。这通常设为 N。
- CTX_XDL_DDC_LIST = list-ddc-fqdns - Virtual Delivery Agent 要求提供由空格分隔的 Delivery Controller 完全限定的域名 (FQDN) 列表来向 Delivery 进行注册。必须至少指定一个 FQDN 或 CNAME 别名。
- CTX_XDL_VDA_PORT = port-number - Virtual Delivery Agent 会使用 TCP/IP 端口与 Delivery Controller 通信。这通常是端口 80。
- CTX_XDL_REGISTER_SERVICE = Y | N - Linux 虚拟桌面服务支持在引导期间启动。这通常设为 Y。
- CTX_XDL_ADD_FIREWALL_RULES = Y | N - Linux 虚拟桌面服务要求允许传入网络连接通过系统防火墙。您可以在系统防火墙中自动为 Linux 虚拟桌面打开所需端口（默认端口 80 和 1494）。这通常设为 Y。
- CTX_XDL_AD_INTEGRATION = 1 | 2 | 3 - Virtual Delivery Agent 要求使用 Kerberos 配置设置对 Delivery Controller 进行身份验证。Kerberos 配置根据系统上已安装和已配置的 Active Directory 集成工具确定。指定要使用且受支持的 Active Directory 集成方法：
 - 1 - Samba Winbind
 - 2 - Quest Authentication Service
 - 3 - Centrify DirectControl
- CTX_XDL_HDX_3D_PRO = Y | N - Linux 虚拟桌面支持 HDX 3D Pro，这是一系列图形加速技术，旨在优化富图形应用程序的虚拟化水平。HDX 3D Pro 要求安装兼容的 NVIDIA Grid 图形卡。如果选择了 HDX 3D Pro，则需要为 VDI 桌面（单会话）模式配置 Virtual Delivery Agent - （即 CTX_XDL_VDI_MODE=Y）。这在 SUSE 上不受支持。确保将此值设为 N。
- CTX_XDL_VDI_MODE = Y | N - 将计算机配置为专用桌面交付模型 (VDI) 还是托管共享桌面交付模型。对于 HDX 3D Pro 环境，此变量需要设置为 Y。这通常设为 N。
- CTX_XDL_SITE_NAME = dns-name - Virtual Delivery Agent 会使用 DNS 发现 LDAP 服务器，从而查询 LDAP 服务记录。要将 DNS 搜索结果限制为本地站点，可能需要指定 DNS 站点名称。此变量通常为空 [none]。
- CTX_XDL_LDAP_LIST = list-ldap-servers - 默认情况下，Virtual Delivery Agent 会通过查询 DNS 来发现 LDAP 服务器，但如果 DNS 无法提供 LDAP 服务记录，您可以提供一个 LDAP 完全限定的域名 (FQDN) 和 LDAP 端口（例如 ad1.mycompany.com:389）的列表，并以空格分隔。此变量通常为空 [none]。
- CTX_XDL_SEARCH_BASE = search-base - 默认情况下，Virtual Delivery Agent 会使用一个搜索基础来查询 LDAP，该搜索基础会设置为 Active Directory 域的根（例如 DC=mycompany,DC=com），但是，要提高搜索性能，您也可以指定一个搜索基础（例如 OU=VDI,DC=mycompany,DC=com）。此变量通常为空 [none]。
- CTX_XDL_START_SERVICE = Y | N - 在完成 Linux VDA 配置后，是否启动 Linux VDA 服务。这通常设为 Y。

注意

HDX 3D Pro 当前不适用于 SUSE。

设置环境变量并运行配置脚本：

```

export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST=list-ddc-fqdns

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base

export CTX_XDL_START_SERVICE=Y|N

sudo -E /usr/local/sbin/ctxsetup.sh

```

您必须为 **sudo** 提供 **-E** 选项，以便将现有环境变量传递给它所创建的新 shell。Citrix 建议使用上述命令并在第一行加上 **#!/bin/bash** 来创建 shell 脚本文件。

另外，也可以使用一个命令来指定所有参数：

```

sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \
    CTX_XDL_DDC_LIST=list-ddc-fqdns \
    CTX_XDL_VDA_PORT=port-number \
    CTX_XDL_REGISTER_SERVICE=Y|N \
    CTX_XDL_ADD_FIREWALL_RULES=Y|N \
    CTX_XDL_AD_INTEGRATION=1|2|3 \
    CTX_XDL_HDX_3D_PRO=Y|N \
    CTX_XDL_VDI_MODE=Y|N \
    CTX_XDL_SITE_NAME=dns-name \
    CTX_XDL_LDAP_LIST=list-ldap-servers \
    CTX_XDL_SEARCH_BASE=search-base \
    CTX_XDL_START_SERVICE=Y|N \
    /usr/local/sbin/ctxsetup.sh

```

删除配置更改

在某些情形下，您可能需要删除 `ctxsetup.sh` 脚本对配置所作的更改，而不卸载 Linux VDA 软件包。

继续操作前，请查看此脚本的帮助信息：

```
sudo /usr/local/sbin/ctxcleanup.sh --help
```

删除配置更改：

```
sudo /usr/local/sbin/ctxcleanup.sh
```

Important

此脚本会从数据库删除所有配置数据，从而使 Linux VDA 无法使用。

配置日志

`ctxsetup.sh` 和 `ctxcleanup.sh` 脚本会在控制台上显示错误，并将详细信息写入配置日志文件：

```
/tmp/xdl.configure.log
```

重新启动 Linux VDA 服务，确保更改生效。

运行 VDA 软件

使用 `ctxsetup.sh` 脚本配置 Linux VDA 后，请使用以下命令控制 Linux VDA。

启动 Linux VDA 服务：

```
sudo /sbin/service ctxhdx start
```

```
sudo /sbin/service ctxvda start
```

停止 Linux VDA 服务：

```
sudo /sbin/service ctxvda stop
```

```
sudo /sbin/service ctxhdx stop
```

重新启动 Linux VDA 服务：

```
sudo /sbin/service ctxvda stop
```

```
sudo /sbin/service ctxhdx restart
```

```
sudo /sbin/service ctxvda start
```

检查 Linux VDA 服务的运行状态：

```
sudo /sbin/service ctxvda status
```

```
sudo /sbin/service ctxhdx status
```

卸载 Linux VDA 软件

检查 Linux VDA 是否安装并查看已安装软件包的版本：

```
rpm -q XenDesktopVDA
```

查看更多详细信息：

```
rpm -qi XenDesktopVDA
```

卸载 Linux VDA 软件包：

```
sudo rpm -e XenDesktopVDA
```

注意

卸载 Linux VDA 软件会删除关联的 PostgreSQL 和其他配置数据。但是，在安装 Linux VDA 前设置的 PostgreSQL 软件包和其他依赖软件包不会遭到删除。

本文未介绍包括 PostgreSQL 在内的依赖软件包的删除操作。

故障排除

最常见的问题都与 Linux 计算机配置不当（主要是网络、NTP 时间服务器配置或 Active Directory 域成员身份配置不当）有直接关系。修复 Linux 计算机配置通常可以解决 VDA 软件问题。

Broker 代理和 HDX Service 会将日志记录到 syslog。Citrix 支持人员会提供一套工具，可用来在支持期间跟踪更多信息。

HDX Service 日志记录

HDX Service 的现成配置即可将消息记录到 syslog，因此无需进一步配置。

Broker 代理日志记录

Broker 代理（也称为 ctxvda 服务）会通过网络套接字将日志数据写入 syslog。这可能并未现成配置妥当。要启用 Broker 代理将日志记录到 syslog 的功能，您需要执行以下配置：

SLED/SLES 11

编辑 /etc/syslog-ng/syslog-ng.conf 文件，并在 s_sys 部分添加以下行：

```
udp(ip(127.0.0.1) port(514));
```

保存并关闭 syslog-ng.conf 文件。重新启动 syslog-ng 服务，应用更改：

```
sudo service syslog-ng restart
```

SLED/SLES 12

编辑 /etc/rsyslog.conf 文件并添加以下行：

```
$ModLoad imudp
```

```
$UDPServerRun 514
```

保存并关闭 rsyslog.conf 文件。重新启动 rsyslog 服务，应用更改：

```
sudo service rsyslog restart
```

确保不存在任何孤立进程，以免其阻碍新会话启动：

```
sudo pkill -9 ctxhdx
```

```
sudo pkill -9 ctxgfx
```

```
sudo pkill -9 ctxlogin
```

```
sudo pkill -9 ctxvfb
```

重新启动 Linux VDA 服务并重新尝试连接。

检查以下目录和文件的文件所有权和权限：

- /var - Owner: root, Group: root, Permissions: 0755
- /var/xdl - Owner: ctxsrvr, Group: ctxadm, Permissions: 0755
- /var/xdl/.isacagent - Owner: root, Group: root, Permissions: 0666
- /var/xdl/.winsta - Owner: ctxsrvr, Group: ctxadm, Permissions: 0777
- /var/xdl/vda - Owner: root, Group: root, Permissions: 0755

确认运行 Citrix Receiver 的设备以及 Linux 桌面的音量控件未设为静音或未设为较低的音量。

确认在 Linux VDA 上启用了音频。使用 ctxreg 工具查询配置项目 fDisableCam 的值：

```
sudo ctxreg read -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v fDisableCam
```

值 0x1 表示禁用音频。要启用音频，请将 fDisableCam 设置为 0x0：

```
sudo ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -v fDisableCam -d 0x00000000
```

如果仍听不到声音，请检查 pulseaudio 是否加载了 Citrix 音频接收器。此 PulseAudio 模块会在会话启动时加载到 pulseaudio 守护程序中。使用 pacmd 工具检查 Citrix 音频接收器是否已加载：

```
pacmd list-sinks
```

如果 Citrix 音频接收器已加载，则输出应为：

```
name:
```

```
driver:
```

如果 Citrix 音频接收器未加载，请终止 ctxaudio 进程并重新启动该进程。

检查是否在 Linux VDA 上启用了音频以及是否在 ICA 客户端上启用了音频录制。如果仍无法录制音频，请检查 pulseaudio 是否加载了 Citrix 音频源。如果 ICA 客户端上启用了音频录制，此 PulseAudio 模块会在会话启动时加载到 pulseaudio 守护程序。使用 pacmd 工具检查 Citrix 音频源是否已加载：

```
pacmd list-sources
```

如果 Citrix 音频源已加载，则输出应为：

```
name:
```

```
driver:
```

如果 Citrix 音频源未加载，请终止 ctxaudio 进程并重新启动该进程。

打印不正常时要检查若干项目。打印守护程序是一个按会话进程，应在会话期间内运行。检查打印守护程序是否正在运行。

```
ps -ef | grep ctxlpmngt
```

如果 ctxlpmngt 进程未在运行，请从命令行手动启动 ctxlpmngt。

如果仍无法打印，请在 CUPS 框架中检查下一个项目。ctxcups 服务用于打印机管理，并负责与 Linux CUPS 框架通信。此进程在每个计算机上有一个，可通过以下方式检查：

```
service ctxcups status
```

如果服务未在运行，请手动启动：

```
service ctxcups start
```

输出乱码可能是打印机驱动程序不兼容造成的。系统中为每个用户提供了驱动程序配置，该配置可通过编辑 `~/.CitrixProfile` 配置文件进行配置。

```
[DEFAULT_PRINTER]
```

```
printername=
```

```
model=
```

```
ppdpath=
```

```
drivertype=
```

`printername` 字段含有当前客户端默认打印机的名称。这是一个只读值，不应进行编辑。

Important

不应同时设置 `ppdpath`、`model` 和 `drivertype` 字段，因为映射的打印机只能使用其中一个字段。

如果通用打印机驱动程序与客户端打印机不兼容，则本机打印机驱动程序的型号可使用 `model=` 选项配置。打印机的当前型号名称可使用 `lpinfo` 命令查找。

```
lpinfo -m
```

```
...
```

```
xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
```

```
xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
```

```
xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
```

```
...
```

随后，可设置与打印机匹配的型号：

```
Model=xerox/ph3115.ppd.gz
```

如果通用打印机驱动程序与客户端打印机不兼容，则可以配置本机打印机驱动程序的 `ppd` 文件路径。`ppdpath` 值为本机打印机驱动程序文件的绝对路径。

例如，`/home/tester/NATIVE_PRINTER_DRIVER.ppd` 下就有一个 `ppd` 驱动程序。

```
ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
```

Citrix 提供了三种类型的通用打印机驱动程序（`postscript`、`pcl5` 和 `pcl6`）。如果本机打印机驱动程序不可用，则可在驱动程序类型中配置这些驱动程序。

例如，如果客户端默认打印机驱动程序类型为 `PCL5`。

```
drivertype=pcl5
```

注意

Citrix Receiver for Mac 和 Citrix Receiver for Linux 仅支持 Postscript 打印机，因此 PCL5 和 PCL6 通用打印机驱动程序不适用。在此情况下，本机打印机驱动程序的路径或型号应设为非 Postscript 打印机。

已知问题

Citrix Receiver for Android CAPS LOCK 状态可能会在会话漫游时反转

与 Citrix Receiver for Android 的现有连接漫游时，CAPS LOCK 状态可能会丢失。解决方法是使用扩展键盘上的 shift 键切换大小写。

使用 Citrix Receiver for Mac 连接至 Linux VDA 时，含 ALT 的快捷键并非总能使用

默认情况下，Citrix Receiver for Mac 会为左侧和右侧 Options/Alt 键发送 AltGr。此设置可在 Citrix Receiver 设置内更改，但在不同应用程序上的更改效果各异。

在 SuSE Linux Enterprise Desktop 11 上，较新的 X 客户端库可能会导致键盘问题

在 SuSE Linux Enterprise Desktop 11 上，较新版本的 xorg-x11-libX11 软件包在处理键盘映射更改时可能会出现问题，进而可能导致 HDX 会话期间的键盘功能出现问题。已安装的软件包版本在 7.4-5.11.11.1 至 7.4-5.11.15.1 范围内时可能会出现此问题。

解决方法是将 xorg-x11-libX11 软件包回滚至原来的 SP3 版本，从而使得键盘映射更改能够正常发挥作用。例如：

```
rpm -i --force xorg-x11-libX11-7.4-5.9.1
```

```
rpm -i --force xorg-x11-libX11-32bit-7.4-5.9.1
```

```
rpm -e xorg-x11-libX11-7.4-5.11.15.1
```

```
rpm -e xorg-x11-libX11-32bit-7.4-5.11.15.1
```

需要在用户登录到计算机之前完成此设置。如果在会话处于活动状态期间完成，则只有在用户下次登录时，这些设置才会生效。

如果要从原来的 SP3 进行升级，则上述 xorg-x11-libX11 软件包会锁定为当前已安装版本，从而确保它们不会在升级期间发生更改。升级前，请先运行以下命令，然后再照常执行升级操作：

```
zypper al xorg-x11-libX11
```

```
zypper al xorg-x11-libX11-32bit
```

如果在 XenDesktop v7.1 中将 Linux VDA 与 Delivery Controller 结合使用，则会话启动时间可能会较长

之所以启动较慢，是因为 v7.1 Delivery Controller 生成的 ICA 文件中存在 CGP 设置。如果存在这些设置，Citrix Receiver 会尝试使用 TCP 端口 2598 建立连接。在某些 Linux 发行版（例如 SLED 12）上，默认防火墙设置会丢弃 TCP SYN 数据包，从而导致超时，并延长会话启动时间。解决方法是，在 Linux VDA 上配置防火墙，使其拒绝端口 2598 上的 TCP SYN。在新版 Delivery Controller 中，此问题已得到解决。

Linux VDA 重新加入域时注册失败

在某些情况下，在 Linux VDA 重新加入域且生成一组全新的 Kerberos 密钥后，Broker 无法与 VDA 建立安全上下文。出现此问题的原因通常是，Broker 使用的是缓存的过时 VDA 服务票据，该票据是基于先前的一组 Kerberos 密钥的。此问题不会阻止 VDA 连接到 Broker，但 Broker 将无法与 VDA 建立返回安全上下文。常见症状是 VDA 注册失败。

由于 VDA 服务票据迟早会过期并进行续订，因此此问题最终会自行解决，但是，服务票据的有效期一般会很长。因此，此过程可能需要很长时间。

解决方法是清除 Broker 的票据缓存。您只需重新启动 Broker 或在 Broker 上以管理员身份从命令提示窗口运行以下命令：

```
klist -li 0x3e4 purge
```

此命令会清除 Citrix Broker Service 运行所在的网络服务主体持有的 LSA 缓存中的所有服务票据。此命令也会删除其他 VDA 的服务票据，因而可能会影响其他服务。但是，此操作不会造成负面影响，因为这些服务会在需要时从 KDC 重新获取这些服务票据。

不支持音频即插即用

建议先将音频捕获设备连接至客户端计算机，然后再开始在 ICA 会话中录制音频。如果在启动音频录制应用程序后再连接设备，应用程序可能会无响应。如果出现此问题，只需重新启动应用程序即可。如果在录制期间拔下捕获设备，也会出现类似的问题。

音频失真

Windows 10 Receiver 可能会在音频录制期间遇到音频失真问题。

CTXPS 驱动程序与部分 PLC 打印机不兼容

如果发现打印输出损坏，请将打印机驱动程序设置为制造商提供的本机打印机驱动程序。

打印大文档时打印速度较慢

在本地客户端打印机上打印大文档时，打印文件会通过服务器连接进行传输。如果连接的速度很慢，这一过程就可能需要很长时间。

在其他会话中看到打印机和打印作业通知

Linux 的会话概念与 Windows 操作系统不同。因此，所有用户都会获得系统范围的通知。管理员可禁用这些通知，方法是修改 CUPS 配置文件 /etc/cups/cupsd.conf。

查找文件中配置的当前策略名称：

```
DefaultPolicy default
```

如果策略名称为 default，则将以下行添加到默认策略 XML 块中。

```
# Job/subscription privacy...  
  
JobPrivateAccess default  
  
JobPrivateValues default  
  
SubscriptionPrivateAccess default
```

SubscriptionPrivateValues default

... ..

Require user @OWNER

Order deny,allow

Order deny,allow

词汇表

Broker - XenDesktop 组件，负责将 HDX 会话代理给 XenDesktop 部署中的不同 VDA。也称为 DDC 或 XenDesktop Controller。

Broker 代理 - Linux VDA 计算机上的组件，负责提供要交付的桌面。Broker 代理会与 Broker 通信，以启用会话代理服务。它由两个关键组件构成，分别是 VDA Service 和 HDX Service。

Citrix Director - Citrix 帮助台/支持控制台，用于监控和控制 XenDesktop VDA。

Citrix Studio - Citrix 管理控制台，用于配置 XenDesktop。

DDC - XenDesktop Desktop Delivery Controller。也称为 Broker 或 Delivery Controller。

FQDN - 完全限定的域名

HDX - 高清体验协议。以前称为 Citrix ICA 协议。

HDX Service - 一种 Linux 服务 (ctxhdx)，用来通过 HDX 协议远程控制 Linux 虚拟桌面。它会与 VDA 服务通信，以便启用会话代理服务。

RHEL - Red Hat Enterprise Linux。Red Hat 提供的商用 Linux 发行版。

SLED - SUSE Linux Enterprise Desktop。Novell 提供的商用 Linux 发行版。

SLES - SUSE Linux Enterprise Server。Novell 提供的商用 Linux 发行版。

VDA - Virtual Delivery Agent。

VDA Service - 一种 Linux 服务 (ctxvda)，用来与 Broker 通信，以启用会话代理服务。它也会与 HDX Service 通信，从而进行远程会话交付。

创建站点

Mar 17, 2016

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 Agents (VDA)、主机连接（如果使用）以及您创建和管理的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。

启动站点创建向导之前请查看本文；本文包括实际创建站点前需要完成的任务和考虑的决策。

站点创建向导

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区域：

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](#)一文。

如果不打算使用默认的 SQL Server Express Edition 安装，请确保创建站点之前在计算机上安装 SQL Server 软件；“系统要求”一文中列出了支持的版本。

如果希望向站点添加多个 Delivery Controller，并且已在其他服务器上安装了 Controller 软件，则在站点创建向导中可以从此页面将其添加到站点中。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。

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 天免费试用许可证。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。名称必须为完全限定的域名 (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。

请参阅下面的 [Remote PC Access](#) 部分。

如果要在虚拟机管理程序或云服务上使用 VM 来提供应用程序和桌面，请在创建站点之前设置主机环境。（请参阅下文列出的[信息源](#)。）

在站点创建向导中创建到主机的第一个连接，之后可以修改此连接和创建其他连接。如果不使用虚拟主机，或者将使用 Studio 管理专用刀片式服务器 PC 上托管的用户桌面，请将连接类型选择为无。

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 主机类型。

指定是使用 Machine Creation Services (MCS) 还是其他工具在主机上创建 VM。

选择连接类型和工具后，向导中的后续页面指定连接将要使用的存储信息和网络；这些内容形成连接的[资源](#)。创建站点后，Studio 中的资源名标识该连接的存储和网络组合。

- 指定要使用主机上的共享存储还是本地存储。共享存储可以通过您选择的网络获取。如果结合使用共享存储和 XenServer，则可以使用 IntelliCache 降低存储设备的负载；有关详细信息，请参阅[连接](#)一文。
- 如果要创建桌面操作系统计算机，请指定是否使用 Personal vDisk 并选择它们要使用的存储。Personal vDisks 可以与 VM 使用相同的存储或不同的存储。有关详细信息，请参阅 [Personal vDisk](#) 一文。
- 选择 VM 将使用的可用网络。

VMware

- [VMware 虚拟化环境](#)一文。
- VMware 产品文档。

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](#)文档。
- Microsoft 文档。
- 在 Studio 中创建连接时，可以自动导入从 <https://manage.windowsazure.com/publishsettings/index> 下载的发布设置文件中的信息。

Amazon Web Services (AWS)

- [CTX140427](#)。
- 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、可用性区域、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。

Citrix CloudPlatform

- [CTX140428](#)。
- Citrix 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，然后再导入这些值。

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允许与

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。

您可以选择其他功能来自定义站点。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

如果您在使用 AppDisk 时已安装 AppDNA，则选择此功能可以对 AppDisk 中的应用程序进行分析，并查看兼容性问题，然后采取补救措施来解决这些问题。有关详细信息，请参阅 [AppDisk](#) 一文。

App-V 发布

如果要使用 App-V 服务器上 Microsoft App-V 软件包中的应用程序，请选择此功能。如果选中此复选框，则系统将提示您提供 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](#) 一文。

如果要使用局域网唤醒功能，在创建站点前，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](#) 一文。

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，在向导的**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**。选择用户和组，然后单击**添加用户**。

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，然后指出是否应包含子文件夹中的项目。单击**添加 OU**。

注意：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，其中包含您在站点创建向导中添加的所有计算机帐户。自动创建名为 Remote PC User Desktops 的交付组，其中包含您已添加的所有用户和用户组。

- 站点创建向导会询问您是否参与 Citrix 客户体验改善计划。加入此计划后，会将匿名统计信息和使用情况信息发送到 Citrix；有关详细信息，请参阅 <http://more.citrix.com/XD-CEIP>。
- 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。
- 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](#)一文。

测试站点配置

可以查看站点测试结果的 HTML 报告。

要在创建站点后运行测试，请选择导航窗格顶部的 **Citrix Studio (Site 站点名称)**，然后单击中间窗格中的**测试站点**。

创建计算机目录

Mar 17, 2016

物理机或虚拟机的集合作为一个称为*计算机目录*的实体进行管理。计算机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

创建将包含 VM 的目录时，指定这些 VM 的置备方式：可以使用 Studio 支持的工具，如 Machine Creations Services (MCS) 或 Provisioning Services，也可以使用您自己的工具来提供计算机。如果已经为您提供了计算机（因此您无需使用主映像），您仍需要为自己的计算机创建一个或多个计算机目录。

- 如果要使用 Provisioning Services 创建计算机，请参阅 Provisioning Services 文档以了解相关说明。
- 如果选择使用 MCS 置备 VM，则需要提供一个主映像（或快照），作为在目录中创建完全相同的 VM 的指南。创建目录之前，首先在虚拟机管理程序或云服务上使用工具创建并配置主映像，其中包括在此映像上安装 Virtual Delivery Agent (VDA)。然后，在 Studio 中创建计算机目录时，选择此映像（或其快照），指定要在目录中创建的 VM 数并配置其他信息。

使用 MCS 或 PVS 创建第一个计算机目录时，使用创建站点时配置的主机连接。之后（创建第一个计算机目录和交付组后），可以更改此连接的信息或创建其他连接。

完成计算机目录创建向导之后，将自动运行测试以确保计算机目录配置正确。测试完成后，可以查看测试报告。以后，您随时可以从 Studio 导航窗格中的 **Citrix Studio 站点名称** 运行测试。

提示：如果直接使用 PowerShell SDK 创建目录而不使用 Studio，可以指定虚拟机管理程序模板 (VM Templates)，作为映像或映像快照的备选方法。

如果使用的是安装 Windows XP 或 Windows Vista 的计算机，这些计算机必须使用早期版本的 VDA，并且将无法使用最新的产品功能。如果无法将这些计算机升级到支持的 Windows 操作系统版本，Citrix 建议将其保存在单独的计算机目录中。

此处简要介绍您在“创建计算机目录”向导中提供信息后要执行的 MCS 操作。

- 如果在向导中选择主映像（而非快照），MCS 会创建一个快照。
- MCS 创建此快照的完整副本，并将此副本放在主机连接中定义的各个存储位置。
- MCS 将桌面添加到 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）并在需要时增加到主映像的最大大小。每个 VM 获得一个差异磁盘。此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。

在虚拟机管理程序或云服务上准备主映像

提示：如果需要了解连接类型信息的来源，请转至[此处](#)。

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：

- 主映像也可称为克隆映像、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 Provisioning Services 时，可以使用主映像或物理计算机作为主目标设备。Provisioning Services 不使用 MCS，而是使用其他术语表示映像；有关详细信息，请参阅其文档。
- 确保主机的处理器、内存和存储空间足以支持要创建的计算机数。
- 正确配置桌面和应用程序所需的硬盘空间量，因为该值后续不能更改或在计算机目录中更改。
- Remote PC Access 计算机目录不使用主映像。
- 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 建议虚拟化应用程序，因为这样在添加或重新配置应用程序后无需更新主映像，进而显著降低成本。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 且要本地化 Microsoft Windows 时，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 Provisioning Services 或 MCS，请勿在主映像上运行 Sysprep。

准备主映像：

1. 使用虚拟机管理程序的管理工具创建新的主映像，然后安装操作系统以及所有服务包和更新。vCPU 数和内存量此时并不重要，因为创建计算机目录时可以更改这些值。但是，请确保配置桌面和应用程序所需的硬盘空间量，因为该值不能后续更改或在计算机目录中更改。
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 Provisioning Services 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. 将主映像加入到应用程序和桌面所属的域中，并确保主映像将在将要创建计算机的主机上可用。请注意，如果使用 MCS，无须将主映像加入域中：置备的计算机已加入在创建计算机目录向导中指定的域中。
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。如果您在创建计算机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。

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，且必须对 VM 进行配置，使其与使用 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 and 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

启动计算机目录创建向导之前，请查看本部分以了解您需要做出的选择以及需要提供的信息。启动向导时，根据您所做的选择，下面介绍的某些项可能不显示，或者可能具有不同的标题。

重要：如果要使用主映像，请确保创建计算机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 将指导您进入正确的起始位置以创建计算机目录。
- 如果您已创建计算机目录并希望创建另一目录，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。

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可由多个用户共享的桌面和应用程序。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。
- **桌面操作系统：**桌面操作系统目录提供分配给各种不同用户的桌面和应用程序。
- **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。

计算机管理页面指出管理计算机的方式以及将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。仅在已配置到虚拟机管理程序或云环境的连接时，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，请选择将用于部署这些计算机的工具。

- **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。
- **Provisioning Services** – 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 Provisioning Services 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。

桌面体验页面（仅在创建包含桌面操作系统计算机的目录时显示）确定将创建的桌面的类型。根据桌面是否分配给用户，以及计算机重新启动时对用户所做更改执行的操作，此类型会有所不同。

共有三种类型：

- **池，随机：**桌面随机分配 – 用户每次登录时连接到新（随机）桌面。用户注销时，桌面变为可供其他用户使用。桌面重新启动时，将丢弃所做的全部更改。
- **池，静态：**桌面永久分配 – 用户每次登录时连接到同一（静态）桌面。用户注销时，桌面保持在仅可供此用户使用的状态。桌面重新启动时，将丢弃所做的全部更改。
- **专用：**桌面永久分配给某个用户。用户注销时，桌面保持在仅可供此用户使用的状态。桌面重新启动时，保留所做的全部更改。可以将更改保存到本地 VM 磁盘或单独的个人虚拟磁盘上的指定驱动器盘符。

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。如果正在创建第一个计算机目录，唯一可用的连接是您在创建站点时配置的连接。

谨记：

- 如果要使用 Provisioning Services 或 MCS，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。

为确保可以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。请勿在向导页面上更改默认的选择安装的 VDA 版本选项。

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。

为 VM 选择一个或多个安全组；这些组仅在可用区域支持安全组时显示。

选择计算机将要使用共享硬件还是帐户专用硬件。

此页面的标题取决于您在**计算机管理**页面上选择的部署方法。

- 如果选择 MCS，此页面的标题为**虚拟机**。
- 如果选择 Provisioning Services，此页面的标题为**设备集合**。
- 如果选择“其他”工具，此页面的标题为**VM 和用户**。

在此页面上：

- 指定要创建的虚拟机数。
- 选择每个计算机将具有的内存量（以 MB 为单位）。每个 VM 都将具有 32 GB 硬盘；此值在主映像中设置，无法在目录中更改。
- 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。

（仅对 Remote PC Access 目录有效）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 (/)。

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。

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 Provisioning Services 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。

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。

管理计算机目录

Mar 17, 2016

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) 创建的池随机计算机目录，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。

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. 选择一个计算机目录，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。

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

如果您的站点包含多个区域，可以将某个目录从一个区域移动到另一个区域。

警告：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

删除某个计算机目录之前，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。

删除计算机目录：

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**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，可以执行以下操作：

- 从桌面操作系统和服务器操作系统计算机目录中删除 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。

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。

提示：如果需要了解连接类型信息的来源，请转至[此处](#)。

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. 查看操作系统优化指南并对您的环境应用优化：[Windows 7 Optimization Guide](#)（《Windows 7 优化指南》）和 [Windows 8/8.1 Virtual Desktop Optimization Guide](#)（《Windows 8/8.1 虚拟桌面优化指南》）。
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。

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 (VM Templates)，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 and 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。

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。

升级计算机目录之前，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 便可以确定计算机目录中的计算机是否需要升级。

要升级计算机目录，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 检测到计算机目录需要升级，则会显示一条消息。按照提示进行操作。如果一个或多个计算机无法升级，则消息中会说明原因。Citrix 建议您在升级计算机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。

注意：如果使用的是安装 Windows XP 或 Windows Vista 的计算机，这些计算机必须使用早期版本的 VDA，并且无法使用最新的产品功能。如果无法将这些计算机升级到当前支持的 Windows 操作系统，Citrix 建议将其保存在一个单独的目录中。

创建交付组

Mar 17, 2016

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，必须至少有一个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。

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。

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。
- 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，要限制财务部门的用户启动“应用程序 A”的能力，可以执行以下操作：

- 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用户使用在交付组中指定的任何应用程序。
- 配置应用程序 A 的属性以将其可见性限制为仅限财务部门的用户。

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。

已通过身份验证

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：

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）。
- 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。
- 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大桌面数量。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**。

摘要

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。

管理交付组

Mar 17, 2016

简介

创建交付组之后，可以更改创建交付组时指定的设置；也可以配置创建交付组时无法配置的其他设置。

有关其他交付组管理过程，请参阅以下文章：

- [管理应用程序](#)
- [管理计算机](#)
- [管理会话](#)

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**）页面上，更改以下某些项，然后单击**确定**或**应用**。

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。
每个用户的桌面数	（仅限分配的桌面操作系统计算机）用户可以同时激活的最大共享桌面数。 在第一次使用时指定的部署中，此值指定了用户可为其自身分配的桌面数。
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**确定或应用**。

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。

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**确定或应用**。

更改 StoreFront 信息

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**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**确定或应用**。

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。

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此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**。

管理交付组中的计算机

Mar 17, 2016

简介

您也可以管理计算机目录中的计算机；请参阅[管理计算机目录](#)一文。

关闭和重新启动计算机

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）：
 - **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。

计算机电源管理

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）是一组保持为启动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十分钟后自动挂起。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，但对池或缓冲区则不可。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，因此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。

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，选择对计算机进行电源管理下拉菜单中的**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，指定挂起交付组中任何已断开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，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”下拉菜单中选择**周末**，然后配置周末的高峰时段和电源状态计时器。
8. 单击**确定或应用**。

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。

创建重新启动计划

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

确定该间隔内每个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），交付组中的每个计算机上均显示消息。
10. 单击**确定或应用**。

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。

阻止用户连接到计算机（维护模式）

当您需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。
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，不过，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）。

更改用户的计算机分配情况

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. 要重新分配多个计算机，请在“操作”窗格中选择**编辑交付组**。在**计算机分配**（用户分配）页面上，选择计算机并指定新用户。然后，单击**确定或应用**。
4. 要重新分配一个计算机，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**更改用户**。添加或删除用户。

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**用户设置**（或**基本设置**）页面上，设置每个用户的桌面数值。
4. 单击**确定或应用**。

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：决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。

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**。

限制访问计算机

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，此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**确定或应用**。

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。

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标记。例如，如果在计算机中添加标记 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。

更新计算机

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**向最终用户发送前滚通知**。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。

管理应用程序

Mar 17, 2016

在本文中：

- [添加应用程序](#)
- [复制、启用/禁用、重命名或删除应用程序](#)
- [从交付组中删除应用程序](#)
- [更改应用程序属性](#)
- [配置应用程序限制](#)
- [管理应用程序文件夹](#)

将应用程序添加至交付组

须知事项：

- 无法向 Remote PC Access 交付组中添加应用程序。
- 一个应用程序必须至少属于一个交付组。
- 您可以在将应用程序添加到交付组时更改该应用程序的属性，也可以稍后再更改。
- 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。
- 如果同一文件夹中已存在与尝试添加的应用程序同名的应用程序，系统将提示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。
- 不能使用“添加应用程序”向导从一个或多个交付组中删除应用程序。必须单独执行该操作。
- 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。
- 另外，您也可以按照以下过程将应用程序添加到一个或多个交付组。您可以在创建交付组时为其添加应用程序，也可以稍后通过选择交付组并选择“操作”窗格中的**添加应用程序**来添加应用程序，但此时应用程序只能添加到该组中。

要添加一个或多个应用程序，请执行以下操作：

步骤 1：选择 Studio 导航窗格中的**应用程序**，然后选择“操作”窗格中的**添加应用程序**。此时将打开“添加应用程序”向导。

步骤 2：选择要包含应用程序的一个或多个交付组。

步骤 3：在**应用程序**页面中，单击**添加**下拉菜单以显示应用程序源，然后选择所需的源。

- **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，该主映像位于所选交付组中使用的计算机目录。
- **手动定义：**您可以为管理员和用户在此类应用程序的可执行文件路径、工作目录、可选命令行参数和显示名称。
- **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。（如果没有任何其他交付组或所有应用程序均被删除，则无法使用此源）。
- **App-V：**App-V 软件包中的应用程序。

如果某个应用程序源不可用或无效，则无法选择该应用程序源，或者会显示一条消息。例如，如果先前没有将任何应用程序添加到任何交付组中，则无法选择**现有**源。同样，如果某个应用程序与所选交付组中计算机支持的会话类型不兼容，则无法选择该应用程序源，或者会显示一条消息。

步骤 4：列出在所选源中发现的应用程序。选择或指定要添加的应用程序，然后单击**确定**。

步骤 5：在摘要页面中，确认相关信息，然后单击**完成**。

复制、启用/禁用、重命名或删除应用程序

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。

须知事项：

- 如果您先前在某个交付组中复制了一个应用程序，以便可以将其添加到另一个交付组中，则可以使用“添加应用程序”向导将该应用程序添加到多个交付组中，或者通过应用程序的属性更改交付组成员身份。
- 删除某个应用程序会将其从交付组中删除，而不会从计算机目录使用的主映像中删除（如果该主映像是该应用程序的源）。删除应用程序操作不同于从交付组中删除应用程序，请参阅下文。
- 启用和禁用应用程序不同于启用和禁用交付组，请参阅“编辑交付组”一文。

要复制、启用、禁用或删除应用程序，请执行以下操作：

1. 在 Studio 导航窗格中选择**应用程序**。
2. 选择一个应用程序，然后在“操作”窗格中选择适当的任务。

从交付组中删除应用程序

一个应用程序必须至少与一个交付组关联（或属于一个交付组）。如果您尝试从交付组中删除某个应用程序会删除该应用程序与任何交付组的关联，系统将改为提供用于删除该应用程序的选项。在这种情况下，如果选择不删除该应用程序，则可以将其添加到其他交付组中，然后将其从原始交付组中删除。

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**。

更改应用程序属性

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。完成更改后，在该页面上单击**确定**或**应用**。（单击**确定**可应用所做更改并关闭“编辑应用程序属性”对话框；单击**应用**可应用所做更改，但不关闭该对话框。）

属性	选择此页面
Receiver 中的类别/文件夹	交付
命令行参数	位置

交付组关联	组
说明	标识
文件扩展名	文件类型关联
文件类型关联	文件类型关联
图标	交付
StoreFront 的关键字	标识
限制（请参阅下文）	交付
名称	标识
可执行文件夹路径	位置
用户桌面上的快捷方式	交付
可见性	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并发实例数，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。
- 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)。
- **限制每个用户运行一个应用程序实例。** 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。完成后，单击**确定**或**应用**。（单击**确定**可应用所做更改并关闭“编辑应用程序属性”对话框；单击**应用**可应用所做更改，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

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。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**。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**。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。
(要在“创建交付组”向导中将应用程序移至其他文件夹，请在该向导的**应用程序**页面上选择**更改**，然后选择或创建一个文件夹。)

通过交付组管理会话

Mar 17, 2016

除以下过程外，还请参阅[会话管理](#)一文，了解与会话可靠性、会话漫游、客户端自动重新连接、ICA 保持活动状态以及工作区控制有关的信息。

注销或断开会话，或者向用户发送消息

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[管理交付组中的计算机](#)一文中的[计算机电源管理](#)部分。

配置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）。
- 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。

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；首先发生的事件将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。

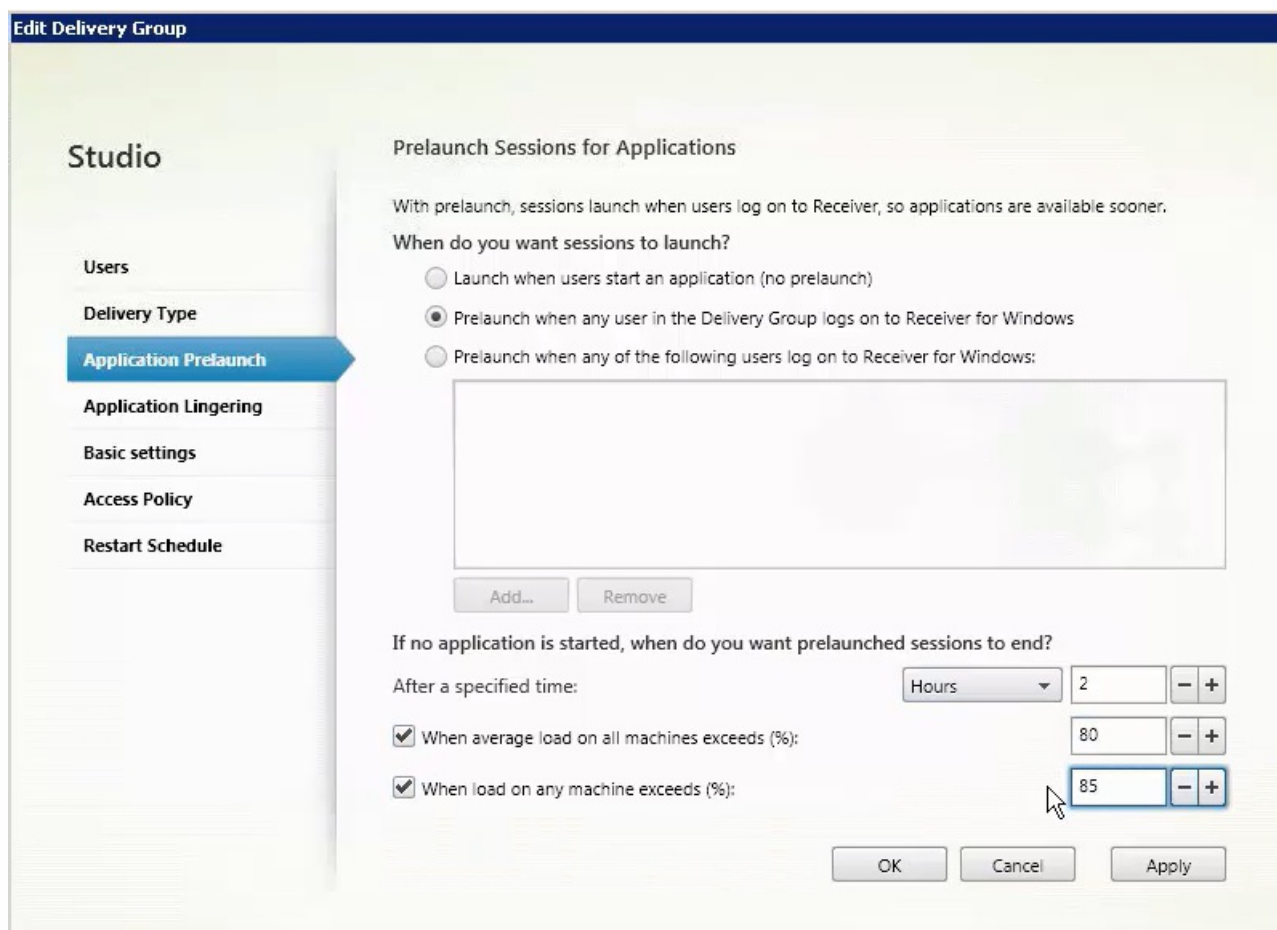
您无法从 Studio 禁用此超时，但可以在 SDK (New/Set-BrokerSessionPreLaunch cmdlet) 中禁用它。如果您禁用该超时，它将不会出现在该交付组的 Studio 显示或“Edit Delivery Group”（编辑交付组）向导中。

- **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。计划外断电将导致预启动和延迟会话自动结束，从而释放容量。

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择一个交付组，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。

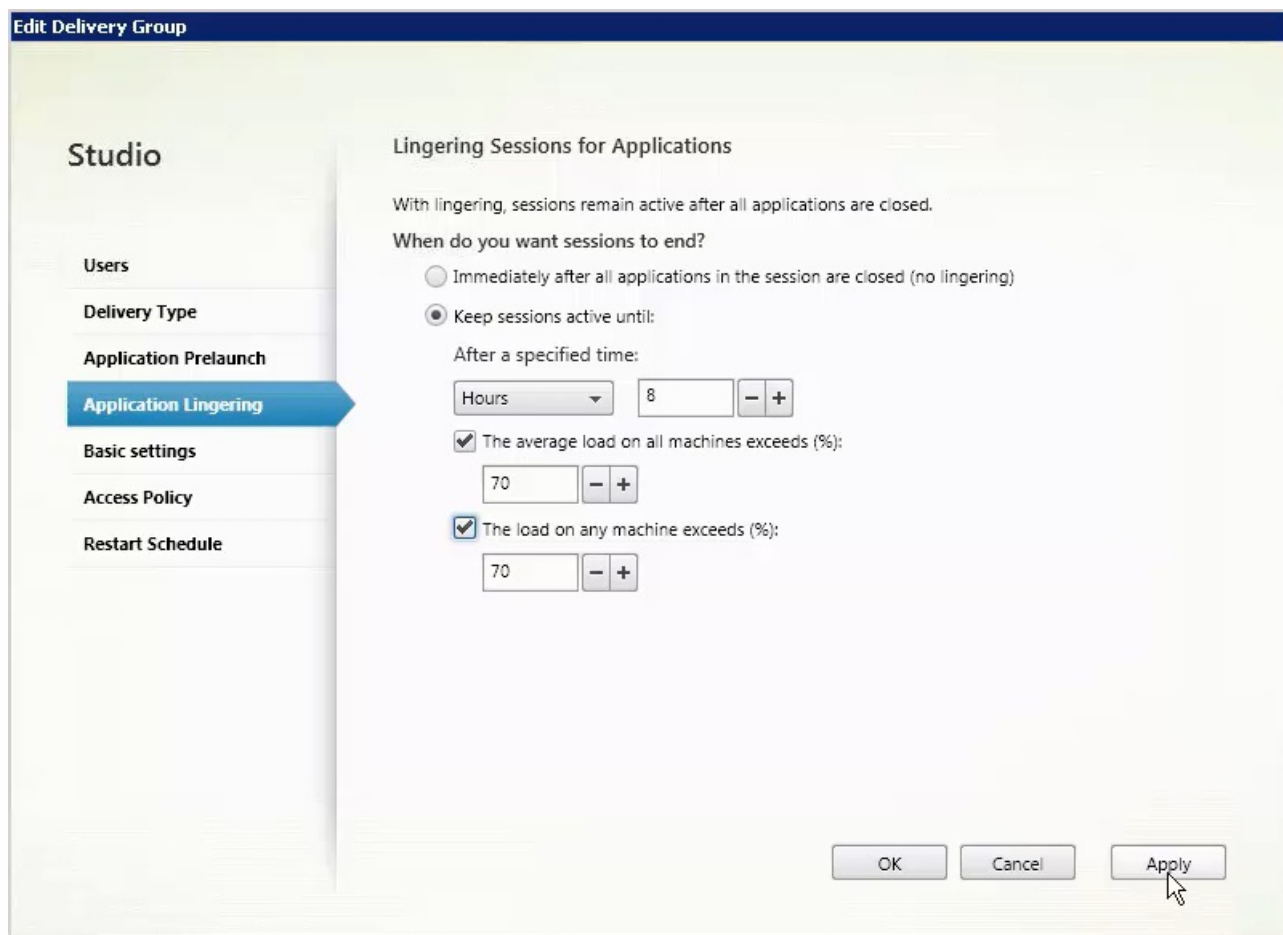


4. 当用户启动应用程序时，预启动会话由常规会话取代。如果用户未启动应用程序（预启动会话未使用），下列设置将影响会话保持活动状态的时长。

- 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。

1. 在 Studio 导航窗格中选择**交付组**。
2. 选择一个交付组，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。



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。

Remote PC Access

Jun 17, 2016

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 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，这些用户可以自己将其办公室 PC 加入站点中，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：不支持 Remote PC Access 的睡眠模式和休眠模式。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。使用这些帐户为用于提供 Remote PC Access 的交付组指定用户。

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

一台计算机一次只能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。

为计算机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计算机目录和相应交付组的权限。

对于办公室 PC 运行 Windows XP 的用户，应为这些系统创建单独的计算机目录和交付组。在 Studio 中为该目录选择计算机帐户时，选中的复选框应指示某些计算机在运行 Windows XP。

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 Access 部署的信息，请查看[安全注意事项](#)。

当前不支持安全启动功能。如果打算部署工作站 VDA，请禁用安全启动功能。

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。

Remote PC Access 部署不支持以下 XenDesktop 功能：

- 创建主映像和虚拟机
- 交付托管应用程序
- Personal vDisk
- 客户端文件夹重定向

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+ALT+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。

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。

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 Ctrl+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。

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。

以下计算机都支持 Remote PC Access 局域网唤醒功能：

- 支持 Intel 主动管理技术 (AMT) 的 PC
- 在 BIOS 中启用了局域网唤醒功能的 PC

必须配置 Microsoft System Center Configuration Manager (ConfigMgr) 2012，才能使用局域网唤醒功能。ConfigMgr 提供访问权限以调用 PC 的 AMT 电源命令以及唤醒代理和幻数据包支持。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，可启用电源管理并指定 ConfigMgr 访问信息。

此外，还要：

- 为保证安全性及可靠性，最好使用 AMT 电源操作；但是，系统还支持两种非 AMT 方式：ConfigMgr 唤醒代理和原始幻数据包。
- 在仅支持 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 Receiver 中还可以使用“重新启动”操作。

有关详细信息，请参阅 [Configuration Manager 与 Remote PC Access 局域网唤醒](#)。

有关实验版局域网唤醒 SDK（使您或第三方局域网唤醒解决方案可以在不使用 System Center 2012 R2 的情况下创建连接器）的信息，请参阅 [CTX202272](#)。

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。
- On the Users and Machine Accounts pages, specify users and machine accounts.

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：

- On the Operating System page, select Remote PC Access and choose a power management connection. 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），然后编辑计算机目录，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。

从命令行安装 VDA 时，请包括 `/remotepc` 选项。这将阻止在桌面（工作站）操作系统上安装以下组件：

- App V 组件 - Citrix Personalization for App-V - VDA
- Upm 组件 - Citrix User Profile Manager
- UpmVdaPlugin 组件 - Citrix User Profile Manager WMI Plugin
- Mps 组件 - Machine Identity Service
- 虚拟磁盘组件 - Personal vDisk

升级过程中，如果安装了上述任意组件，安装程序都会检测该组件并进行升级。

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> 或受支持移动设备的应用程序分发系统获取 Citrix Receiver。

配置高级连接设置

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。

故障排除

Delivery Controller 可将以下 Remote PC Access 诊断信息写入 Windows 应用程序事件日志。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

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。如果需要使用时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）。

App-V

Mar 17, 2016

在本文中：

- [将 App-V 与 XenApp 和 XenDesktop 结合使用](#)
 - [管理方法](#)
- [设置](#)
 - [部署 App-V](#)
 - [打包和放置](#)
 - [在 Studio 中配置 App-V 服务器地址](#)
 - [在 VDA 计算机上安装软件](#)
 - [向应用程序库添加 App-V 软件包](#)
 - [向交付组添加 App-V 应用程序](#)
 - [从应用程序库删除 App-V 软件包](#)
- [故障排除](#)
 - [日志](#)

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

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 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。

设置

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	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/zh-cn/virtualization/hh710199>。

(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 管理员对该位置至少具有读取访问权限。
- 对于双管理方法，请在 App-V 管理服务器上发布软件包。

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。

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，如果您要删除指向 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 的每个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。

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

在安装 VDA 时，系统会默认安装并启用 Citrix App-V 组件软件；在此过程中，还会创建一个帐户，该帐户拥有访问 App-V 发布组件的本地管理员权限。

您可以在 VDA 安装过程中控制此默认操作。在图形界面中，请清除功能页面上的 **Install App-V publishing components**（安装 App-V 发布组件）复选框。在命令行界面中，请使用 `/no_appv` 选项。

如果您在 VDA 安装过程中明确禁用了 Citrix App-V 组件功能，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。

此过程仅适用于单管理方法。

您必须对包含 App-V 软件包的共享至少具有读取访问权限。

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。

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](#)一文。

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。
- 如果稍后要编辑包含 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。

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**。

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 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 [https://technet.microsoft.com/zh-cn/magazine/ff700227\(en-us\).aspx](https://technet.microsoft.com/zh-cn/magazine/ff700227(en-us).aspx)。
- Studio 管理员是否同时是 App-V 服务器管理员？
- 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：“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？
- 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 <https://technet.microsoft.com/zh-cn/magazine/ff700227%28en-us%29.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，检查 UserRefreshonLogon 是否设置为“False”。如果不是，则第一个 App-V 应用程序通常无法启动。
- （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”。
- 包含 VDA 的计算机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 的计算机上，确保 CtxAppVCOMAdmin 具有管理员权限。此用户帐户一般会在 VDA 安装期间创建，并添加到 VDA 计算机上的本地管理员组中。但是，根据 Active Directory 策略，此用户可能会丢失管理关联。运行 `compmgmt.msc` 并浏览到本地用户和组用户。如果 CtxAppVCOMAdmin 不是管理员，请编辑组策略，以使此用户帐户始终具有管理权限。
- 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

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。确保签入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. 转到 C:\ProgramFiles\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. 转到 C:\ProgramFiles\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。

AppDisk

Apr 25, 2016

在本文中：

- [概述](#)
- [部署概述](#)
- [要求](#)
- [创建 AppDisk](#)
- [向交付组分配 AppDisk](#)
- [管理 AppDisk](#)

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：

- 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。
- 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。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。

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。

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、Machine Creation Services (MCS) 或 Provisioning Services (PVS) 以及 Delivery Controller 进行协调，以便分布所选的 AppDisk。

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。

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：

- 随 Controller 7.8（最低版本）提供的 MCS 或在下载页面上随 XenApp 和 XenDesktop 版本提供的 PVS 版本。
- 受支持的 XenServer 版本（请参阅《系统要求》一文）或 VMware 5.1（最低要求）。（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。）

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。

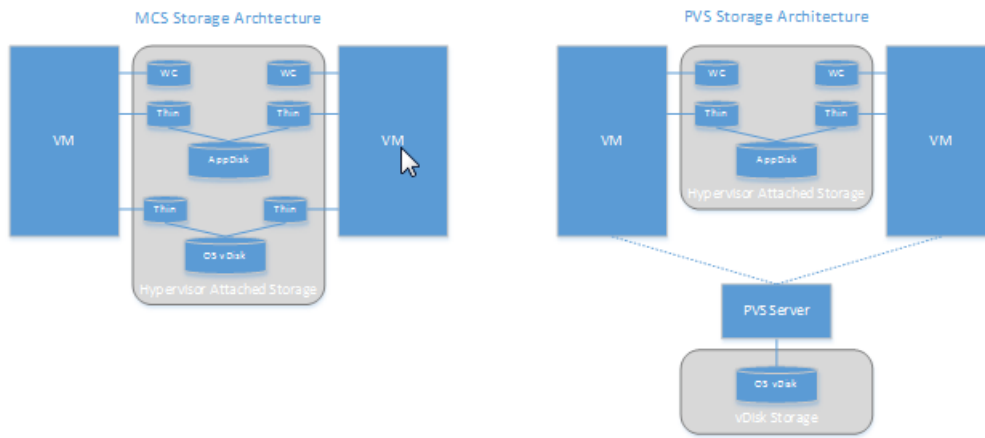
除了任何其他已安装的 .NET 版本之外，安装 Studio 的计算机还必须安装 .NET Framework 3.5。

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。

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准则来平衡 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：

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 (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：

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. 查看此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。

关闭向导后，新的 AppDisk 在 Studio 中将显示为“正在创建”。创建 AppDisk 后，此显示状态将更改为“已准备好安装应用程序”。

在 AppDisk 上安装应用程序：

通过虚拟机管理程序管理控制台在 AppDisk 上安装应用程序。（提示：如果忘记 VM 名称，请在 Studio 导航窗格中选择 **AppDisk**，然后选择“操作”窗格上的**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。（请记住：必须通过虚拟机管理程序管理控制台在 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](#)。

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。

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. 在左侧列中选中的一个或多个可用 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. 选择一个或多个可用 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。

重要：可以使用 Windows 更新服务来更新 AppDisk 上的应用程序（如 Office 套件）。但是，请勿使用 Windows 更新服务对 AppDisk 应用操作系统更新。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。

本地应用程序访问和 URL 重定向

Mar 17, 2016

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 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 站点中内容重定向的路径，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。

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，还可以使用文件类型关联 (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。
- 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。

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个计算机，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。从命令提示窗口，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。
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。从命令提示窗口中，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
```

- 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 **gpedit.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本地环境中可用，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。

XenApp Secure Browser

May 12, 2016

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 建议对 XenApp Secure Browser 使用 Lifecycle Management 蓝图，以简化部署。XenApp 7.8 启动过程中，订购了有效的软件维护服务 (SWM) 或专享升级服务 (SA) 的所有现有 XenApp 和 XenDesktop 客户都能够访问 Citrix Lifecycle Management 的部署版本。

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

使用 Citrix Lifecycle Management 蓝图：

1. 从 [Workspace Cloud](#) 主页导航到“Services”（服务），然后单击“Request Trial for Lifecycle Management”（申请 Lifecycle Management 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“Lifecycle Management Overview”（Lifecycle Management 概览）页面。
3. 从 [Citrix 下载站点](#) 下载 Citrix XenApp Secure Browser 7.8 ISO。

下载 Secure Browser 7.8 ISO 后，请考虑执行以下操作：

- 按照 [XenApp Secure Installation with a Citrix Lifecycle Management Blueprint](#)（《使用 Citrix Lifecycle Management 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 7.8：

1. 从 [Citrix 下载站点](#) 下载 Citrix XenApp Secure Browser 7.8 ISO。
2. 按照[安装说明](#)所述安装 XenApp 的各个组件。
3. 安装完毕后，请继续执行以下步骤，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。

b. 键入 `Asnp Citrix*` 并按 Enter，以便加载 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。

Server VDI

Mar 07, 2016

Use the Server VDI (Virtual Desktop Infrastructure) feature to deliver a desktop from a server operating system for a single user.

- Enterprise administrators can deliver server operating systems as VDI desktops, which can be valuable for users such as engineers and designers.
- Service Providers can offer desktops from the cloud; those desktops comply with the Microsoft Services Provider License Agreement (SPLA).

You can use the Enhanced Desktop Experience Citrix policy setting to make the server operating system look like a Windows 7 operating system.

The following features cannot be used with Server VDI:

- Personal vDisks
- HDX 3D Pro
- Hosted applications
- Local App Access
- Direct (non-brokered) desktop connections
- Remote PC Access

Server VDI is supported on the same server operating systems as the VDA for Windows Server OS.

1. Prepare the Windows server for installation: ensure that Remote Desktop Services role services are not installed and that users are restricted to a single session:
 - Use Windows Server Manager to ensure that the Remote Desktop Services role services are not installed. If they were previously installed, remove them.
 - Ensure that the 'Restrict each user to a single session' property is enabled.
 - On Windows Server 2008 R2, access this property through Administrative Tools > Remote Desktop Services > Remote Desktop Session Host Configuration. In the Edit settings > General section, the Restrict each user to a single session setting should indicate Yes.
 - On Windows Server 2012, edit the registry to set the Terminal Server setting. In registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer to set DWORD fSingleSessionPerUser to 1.
2. For Windows Server 2008 R2, install Microsoft .NET Framework 3.5 SP1 on the server before installing the VDA.
3. Use the [command line interface](#) to install a VDA on a supported server or server master image, specifying the /quiet and /servervdi options. (By default, the installer blocks the Windows Desktop OS VDA on a server operating system; using the command line overrides this behavior.)

XenDesktopVdaSetup.exe /quiet /servervdi

You can specify the Delivery Controller or Controllers while installing the VDA using the command line, using the **/controllers** option.

Use the **/enable_hdx_ports** option to open ports in the firewall, unless the firewall is to be configured manually.

Add the **/masterimage** option if you are installing the VDA on an image, and will use MCS to create server VMs from that image.

Do not include options for features that are not supported with Server VDI, such as `/baseimage`, `/enable_hdx_3d_pro`, or `/xa_server_location`.

4. Create a Machine Catalog for Server VDI.

1. On the Operating System page, select **Desktop OS**.
2. On the Summary page, specify a machine catalog name and description for administrators that clearly identifies it as Server VDI; this will be the only indicator in Studio that the catalog supports Server VDI.

When using Search in Studio, the Server VDI catalog you created is displayed on the Desktop OS Machines tab, even though the VDA was installed on a server.

5. Create a Delivery Group and assign the Server VDI catalog you created in the previous step.

If you did not specify the Delivery Controllers while installing the VDA, specify them afterward using Citrix policy setting, Active Directory, or by editing the VDA machine's registry values.

Personal vDisk

Mar 17, 2016

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，则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。

您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相同的位置。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。

Personal vDisk 7.6.1 中的新增功能

本版本中包括以下增强功能：

- 本版本的 Personal vDisk 中包含的性能增强功能缩短了对个人虚拟磁盘目录应用映像更新所需的时间。

本版本中修复了以下已知问题：

- 尝试将基础虚拟机从 Microsoft Office 2010 原位升级到 Microsoft Office 2013 导致显示一个重新配置窗口，后跟以下错误消息：Error 25004. The product key you entered cannot be used on this machine。（错误 25004。输入的产品密钥不能在此计算机上使用。）过去，建议您先卸载基础虚拟中的 Office 2010，然后再安装 Office 2013。现在，对基础虚拟机执行原位升级时不再需要卸载 Office 2010 (#391225)。

- 映像更新过程中，如果用户的个人虚拟磁盘上存在更高版本的 Microsoft .Net，该版本将被基础映像中较低版本覆盖。这会导致运行个人虚拟磁盘上安装的某些需要更高版本的应用程序（例如 Visual Studio）的用户遇到问题 (#439009)。
- 不能使用安装并启用了个人虚拟磁盘的 Provisioning Services 映像磁盘创建非个人虚拟磁盘计算机目录。此限制已删除 (#485189)。

关于 Personal vDisk 7.6

版本 7.6 中的新增功能：

- 改进了 Personal vDisk 错误处理和报告功能。在 Studio 中，显示目录中启用 PvD 的计算机时，“PvD”选项卡提供映像更新期间的监视状态，以及预计完成时间和进度。还提供了增强的状态显示。
- 早期版本的 Personal vDisk 映像更新监视工具可以从 ISO 介质 (ISO\Support\Tools\Scripts\PvdTool) 中获取。早期版本支持监视功能，但报告功能不如当前版本强大。
- Provisioning Services 测试模式允许在测试目录中使用更新的映像引导计算机。验证其稳定性后，可以将个人虚拟磁盘的测试版本提升为生产版本。
- 提供了一项新功能。利用此功能，可以计算两个清单之间的增量，而非针对每个 PvD 桌面进行计算。提供了可以导出和导入 MCS 目录的早期清单的新命令。（Provisioning Services 主虚拟磁盘已经具有之前的清单。）

版本 7.6 中修复的 7.1.3 中的已知问题：

- 中断 Personal vDisk 安装升级可能会损坏现有 Personal vDisk 安装。[#424878]
- 如果 Personal vDisk 长时间运行，并发生非分页内存泄露，虚拟桌面可能会无响应。[#473170]

版本 7.6 中的已知新问题：

- 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 PROCESS 排除列表中，会提高性能。这些文件位于 C:\Program Files\Citrix\personal vDisk\bin 中。[#326735]
- 继承自主映像的文件之间的硬链接不会保留在 Personal vDisk 目录中。[#368678]
- 在 Personal vDisk 主映像上将 Office 2010 升级到 2013 后，Office 可能无法在虚拟机上启动，因为 Office KMS 许可产品密钥已在升级期间删除。解决方法是：卸载 Office 2010 并在主映像上重新安装 Office 2013。[#391225]
- Personal vDisk 目录不支持 VMware Paravirtual SCSI (PVSCSI) 控制器。要防止出现此问题，请使用默认的控制器的。[#394039]
- 对于使用 Personal vDisk 5.6.0 版本创建并升级到 7 的虚拟桌面，之前登录到主虚拟机 (VM) 的用户可能无法在其池 VM 中找到所有文件。这是因为用户登录到其池 VM 时创建了新的用户配置文件。此问题无法解决。[#392459]
- 启用 Windows 系统保护功能时，运行 Windows 7 的个人虚拟磁盘无法使用备份和还原功能。如果系统保护处于禁用状态，将会备份用户配置文件，但不对 userdata.v2.vhd 文件进行备份。Citrix 建议禁用系统保护并使用备份和还原功能来备份用户配置文件。[#360582]
- 使用磁盘管理工具在基础 VM 上创建 VHD 文件时，可能无法装载 VHD。解决方法为，将 VHD 复制到 PvD 卷。[#355576]
- 删除 Office 2010 软件后，其快捷方式仍保留在虚拟桌面上。要解决此问题，请删除快捷方式。[#402889]
- 使用 Microsoft Hyper-V 时，如果计算机存储在本地，而虚拟磁盘存储在群集共享卷 (CSV) 上，则可能无法创建具有个人虚拟磁盘的计算机的目录；目录创建失败并出现错误。要解决此问题，请对虚拟磁盘使用备用存储设置。[#423969]
- 首次登录基于 Provisioning Services 目录创建的虚拟桌面时，如果个人虚拟磁盘已重置（使用命令 ctxpvd.exe -s reset），该桌面会提示用户重新启动。要解决此问题，请根据提示重新启动桌面。此为一次性重置，重新登录时不需要再执行此操作。[#340186]
- 如果您在个人虚拟磁盘上安装了 .NET 4.5，而稍后执行映像更新时安装或修改了 .NET 4.0，依赖 .NET 4.5 的应用程序将无法启动。要解决此问题，请分发基础映像中的 .NET 4.5 作为映像更新。
- 另请参阅 XenApp 和 XenDesktop 7.6 版本的
— 已知问题
文档。

关于 Personal vDisk 7.1.3

版本 7.1.3 中修复的 7.1.1 中的已知问题：

- 从 Personal vDisk 5.6.0 直接升级到 Personal vDisk 7.x 可能会导致 Personal vDisk 失败。[#432992]
- 用户有时只能连接到具有个人虚拟磁盘的虚拟桌面。[#437203]
- 如果在将 Personal vDisk 5.6.5 或更高版本升级到 Personal vDisk 7.0 或更高版本的过程中个人虚拟磁盘映像更新操作中断，以后执行更新操作可能会失败。[#436145]

关于 Personal vDisk 7.1.1

版本 7.1.1 中修复的 7.1 中的已知问题：

- 通过映像更新升级到 Symantec Endpoint Protection 12.1.3 会导致 symhelp.exe 报告损坏的防病毒软件定义。[#423429]
- 如果服务控制管理器 (services.exe) 崩溃，Personal vDisk 会导致池桌面重新启动。[#0365351]

版本 7.1.1 中的已知新问题：无

关于 Personal vDisk 7.1

版本 7.1 中的新增功能：

- 现在，可将 Personal vDisk 与运行 Windows 8.1 的桌面结合使用，事件日志记录功能也已得到改进。
- 此版本不再支持写入时复制 (CoW) 功能。Personal vDisk 从版本 7.0 升级 7.1 时，由 CoW 管理的所有数据更改都将丢失。这是 XenDesktop 7 中的实验性功能，默认情况下处于禁用状态，因此如果不启用该功能，将不会有任何影响。

版本 7.1 中修复的 7.0.1 中的已知问题：

- 如果将 Personal vDisk 注册表项 EnableProfileRedirection 的值设置为 1 或 ON，随后在更新映像时，将其更改为 0 或 OFF，则可能将整个个人虚拟磁盘空间分配给用户安装的应用程序，而没有为仍保留在虚拟磁盘上的用户配置文件留出空间。如果为某个目录禁用此配置文件重定向功能，而在映像更新期间将其启用，则用户可能无法登录其虚拟桌面。[#381921]
- Personal vDisk 清单更新失败时，桌面服务不会在事件查看器中记录正确的错误消息。[#383331]
- 升级到 Personal vDisk 7.x 时，修改的规则无法保留下来。对于版本 7.0 到 7.1 的升级，此问题已得到修复。从版本 5.6.5 升级到版本 7.1 时，必须首先保存规则文件，然后在升级后重新应用这些规则。[#388664]
- 运行 Windows 8 的个人虚拟磁盘无法从 Windows 应用商店中安装应用程序。将出现错误消息“您的购买无法完成”。启用 Windows Update Service 无法解决此问题，现在此问题已得到修复。但是，系统重新启动后，必须重新安装用户安装的应用程序。[#361513]
- 在带有个人虚拟磁盘的 Windows 7 池桌面中，某些符号链接丢失。这样，对于将图标存储在 C:\Users\All Users 中应用程序，其图标将不会显示在“开始”菜单中。[#418710]
- 由于在更新清单后对系统做了大量更改，因此，如果更新序列号 (Update Sequence Number, USN) 日志溢出，个人虚拟磁盘可能无法启动。[#369846]
- 状态代码为 0x20 且错误代码为 0x20000028 时，个人虚拟磁盘不会启动。[#393627]
- Symantec Endpoint Protection 12.1.3 显示“Proactive Threat Protection is malfunctioning”（主动威胁保护功能出现故障）消息，并且无法获得此组件的实时更新状态。[#390204]

版本 7.1 中的已知新问题：请参阅 XenDesktop 7.1 版本的

— 已知问题
文档。

关于 Personal vDisk 7.0.1

版本 7.0.1 中的新增功能：Personal vDisk 现在更能适应环境的变化。具有个人虚拟磁盘的虚拟桌面现在注册到 Delivery Controller，即使映像更新失败也是如此，并且不安全地关闭系统不会再将虚拟磁盘置于永久禁用状态。此外，现在还可以使用规则文件在部署期间从虚拟磁盘排除文件和文件夹。

版本 7.0.1 中修复的 5.6.13 中的已知问题：

- 用户在池虚拟桌面上对组成员关系所做的更改在映像更新后可能会丢失。[#286227]
- 映像更新失败并出现磁盘空间不足错误，即使个人虚拟磁盘具有足够的空间也是如此。[#325125]
- 某些应用程序无法安装在具有个人虚拟磁盘的虚拟桌面上，并显示一条消息，指出需要重新启动。这是由一项待执行的重命名操作所致。[#351520]
- 在主映像中创建的符号链接在具有个人虚拟磁盘的虚拟桌面上无效。[#352585]
- 在使用 Citrix Profile Management 和 Personal vDisk 的环境中，如果启用了配置文件重定向，负责检查系统卷上的用户配置文件的程序可能无法正确运行。[#353661]
- 清单大于 2 GB 时，清单更新过程在主映像上失败。[#359768]
- 映像更新失败，错误代码 112，并且个人虚拟磁盘损坏，即使虚拟磁盘具有足够的可用空间来执行更新也是如此。[#363003]
- 对于具有超过 250 个桌面的目录，调整大小脚本失败。[#363365]
- 用户对环境变量所做的更改在执行映像更新时丢失。[#372295]
- 在具有个人虚拟磁盘的虚拟桌面上创建的本地用户在执行映像更新时丢失。[#377964]
- 由于在更新清单后对系统做了大量更改，因此，如果更新序列号 (Update Sequence Number, USN) 日志溢出，个人虚拟磁盘可能无法启动。为避免出现此问题，将主映像中的 USN 日志大小增加到最小 32 MB 并执行映像更新。[#369846]
- 已在个人虚拟磁盘上发现问题，该问题会在取代模式下使用 AppSense 时阻止 AppSense Environment Manager 注册表单元配置操作正常工作。Citrix 和 AppSense 正共同努力解决此问题，该问题与安装 Personal vDisk 时 RegRestoreKey API 的行为有关。[#0353936]

与版本无关的已知问题

- 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。为解决此问题，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。作为一种解决方法，可重新启动桌面。[#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。为解决此问题，可重置 Personal vDisk。[#474071]

安装和升级

Mar 17, 2016

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 Provisioning Services 文档。

安装并启用 PvD

在计算机上安装或升级 VDA for Desktop OS 时会自动安装 PvD。如果在安装 VDA 后更新 PvD 软件，请使用[此处](#)提供的 PvD MSI（需要具有 Citrix 帐户凭据）。

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。

VDA 安装提供启用 PvD 的选项（通过在图形界面中选中“Personal vDisk”复选框，或在命令行接口中指定 /baseimage 选项）。但是，在 VDA 安装过程中省略此操作（默认）仍可以使用相同的映像来创建 PvD 桌面和非 PvD 桌面，因为会在目录创建过程中启用 PvD。

添加个人虚拟磁盘

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（连续），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。

升级 PvD

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。

也可以使用[此处](#)提供的 PvD MSI 只升级 PvD。

卸载 PvD

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。

配置与管理

Mar 17, 2016

本主题介绍配置和管理 Personal vDisk (PvD) 环境时需要考虑的项目， 其中还包括最佳实践指南和任务描述。

对于包括使用 Windows 注册表的过程：

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。

注意事项：个人虚拟磁盘大小

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) × 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

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。

方法：配置个人虚拟磁盘大小和分配

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，可以在单个计算机上更改此设置）；在主映像上指定的设置在下次映像更新时应用。

- **MinimumVHDSIZEInMB**

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

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。

- **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。

注意事项：主映像上的应用程序

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（而不是单个计算机上）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）。

注意事项：Provisioning Services

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。常规操作期间，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 最佳实践来确定 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。

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。

注意事项：Machine Creation Services

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。

方法：排除虚拟磁盘中的文件和文件夹

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。

方法：更新主映像时运行清单

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

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](#)。

方法：配置连接限制设置

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 $14000 \text{ IOPS} / 350 \text{ IOPS/VM} = 40$ 。

- **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) 与目录中的最后一个计算机上的 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。

方法：具有 PvD 的 System Center Configuration Manager 2007

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。

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。

工具

Mar 17, 2016

可以使用以下工具和实用程序自定义、加快和监视 PVD 操作。

自定义规则文件

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 VM 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。

resize 和 poolstats 脚本

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。此脚本需要在 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。

重置应用程序区域

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。

导出和导入 PVD 清单

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，但是此功能可以改善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。如需要，请使用“net use”对用于导出/导入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。

- 要导出清单，请在包含 VDA（版本最低为 7.6）且启用 PVD 的计算机上以管理员身份运行导出命令。
Ctxpvdsc.exe exportinventory “<导出位置的路径>”

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 ... Exportin
```

- 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。

```
Ctxpvdsc.exe importinventory “<导出清单的路径>”
```

<导出清单的路径> 应为清单文件的完整路径，通常为 <网络位置\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\ExportedPv
```

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

备份和还原

重要：这两个脚本不会将 PVD 移至新存储位置。您必须通过另外某种方法执行该操作。

可以利用产品安装介质上提供的两个 PowerShell 脚本（在 Support\Tools\Scripts 文件夹中）来备份和还原个人虚拟磁盘。使用备份和还原脚本可将现有 PVD 和用户关联从一个目录迁移到其他目录。如果要更改 PVD 存储，则运行备份和还原脚本将非常有用。备份脚本会创建一个包含现有目录中的元数据的 .xml 文件。该元数据中包含存储上的 PVD 的当前位置以及与 PVD 的用户关联。还原脚本使用该 .xml 文件将 PVD 与新目录关联，并将正确的用户分配给 PVD。

- migration-backup.ps1 可以捕获每个用户与其计算机目录中个人虚拟磁盘之间的映射，并将此信息存储在 .xml 文件中
- migration-restore.ps1 使用该 .xml 文件在计算机目录中重新创建用户桌面

在执行备份和还原之前，请注意以下问题：

- 这些脚本使用虚拟机管理程序 API，因此，必须在执行脚本的 Controller 上安装虚拟机管理程序的 PowerShell 管理单元
- 从一个有权访问用来创建计算机目录的 Controller 的位置运行脚本
- 以下虚拟机管理程序平台支持这些脚本：Citrix XenServer、Microsoft Hyper-V 和 VMware ESX

备份计算机目录

在更改计算机目录时执行备份。可以在计算机目录中的计算机处于活动状态时执行备份。

使用 migration-backup.ps1 备份包含个人虚拟磁盘的任何计算机目录。此脚本将要求提供计算机目录的名称以及虚拟机管理程序的连接信息。然后对计算机目录中所有用户分配的计算机进行迭代，并且将存储每个计算机的个人虚拟磁盘存储和已分配用户之间的映射。此信息位于 .xml 文件中，此文件具有如下结构：

- PvdMigration.hypervisor.Type 支持 VMware ESX、Citrix XenServer 和 Microsoft Hyper-V。
- PvdMigration.PVD 存储有关个人虚拟磁盘的存储位置和与其关联的用户的信息。
- PvdMigration.PVD.DiskId 是执行备份时所在的虚拟机管理程序上的虚拟磁盘的唯一标识符。
- PvdMigration.PVD.DiskName 是 .vhd 或 .vmdk 文件的名称。
- PvdMigration.PVD.SRName 是执行备份时存储提供程序的名称。
- PvdMigration.PVD.SRID 是执行备份时所在的虚拟机管理程序上的存储提供程序的唯一标识符。
- PvdMigration.PVD.UserName 是与此虚拟磁盘关联的用户名称。
- PvdMigration.PVD.UserSid 是与此虚拟磁盘关联的用户 SID。
- PvdMigration.PVD.State 指示此虚拟磁盘的状态。此状态可以为“已备份”或“已处理”。在初始备份之后，此状态为“已备份”；在使用 .xml 文件从备份中进行还原之后，此状态将变为“已处理”。

还原计算机目录

在执行还原之前，请注意以下问题：

- 只能还原与备份的计算机目录共享同一主映像的计算机目录
- 必须通过更新创建备份的计算机目录所在的主映像清单来创建新的主映像

使用 migration-restore.ps1 可还原包含个人虚拟磁盘的任何计算机目录。此脚本所需的输入如下：

- 在备份过程中创建的 .xml 文件
- 要还原的计算机目录的名称
- 未连接的个人虚拟磁盘的存储位置的名称。此信息已在 .xml 文件中列出
- 虚拟机管理程序连接信息

migration-restore.ps1 脚本可以找出计算机目录中所有未分配的计算机，并将用户分配给这些计算机。另外还将用户的个人虚拟磁盘连接到这些计算机。

示例方案 1：使用新的计算机名称还原计算机目录及其个人虚拟磁盘

在此方案中，将还原整个计算机目录以及其中连接到计算机的个人虚拟磁盘。将为这些计算机提供新名称。虚拟机管理程序或存储主机发生故障时或者将用户迁移到新的基础结构时，可能需要执行此方案。

1. 运行 migration-backup.ps1 捕获 .xml 文件中的用户到个人虚拟磁盘的映射。
2. 使用备份解决方案将原始计算机目录中的个人虚拟磁盘移动或捕获至磁盘：
 - VMware ESX 或 Microsoft Hyper-V：个人虚拟磁盘位于 Controller 指定的存储上，该存储位于包含虚拟磁盘所连接计算机的名称的文件夹中。
 - Citrix XenServer：个人虚拟磁盘位于 Controller 指定的存储的根目录中。每个虚拟磁盘的名称为 GUID。
3. 使用存储备份解决方案从原始计算机目录中还原个人虚拟磁盘：
 - ESX 或 Hyper-V：将虚拟磁盘置于新存储资源的新文件夹中。或者，将虚拟磁盘保留在新存储资源上的原始路径中。
 - XenServer：将虚拟磁盘置于新存储资源的根目录中。
4. 从用于创建失败的计算机目录的主映像中创建 Provisioning Services 虚拟磁盘或 Machine Creation Services 快照。
5. 从虚拟磁盘或快照的“开始”菜单中运行更新清单。
6. 使用与失败的（原始）计算机目录不同的命名约定在 Studio 中重新创建计算机目录。此操作将生成新计算机的目录，每台计算机均具有站点数据库可识别的新个人虚拟磁盘。
7. 确认已将重新创建的计算机目录分配给正确的交付组。
8. 确认交付组处于维护模式且其中的计算机已关闭。
9. 编辑备份脚本生成的 .xml 文件：
 - ESX 或 Hyper-V：如果在步骤 3 中将虚拟磁盘还原到新存储资源上的新文件夹，对于该文件中的每个 PVD 部分，请将 DiskName 中的文件夹名称替换为还原的虚拟磁盘的位置。如果将虚拟磁盘还原到新存储上的原始路径，请跳过此步骤。
 - XenServer：请跳过此步骤。
10. 在 Controller 上，运行 migration-restore.ps1，并指定 .xml 文件的名称以及存储备份虚拟磁盘的位置。

示例方案 2：重复使用现有计算机名称还原计算机目录及其个人虚拟磁盘

在此方案中，将还原整个计算机目录以及其中连接到计算机的个人虚拟磁盘。将重复使用现有（失败的）计算机名称。虚拟机管理程序或存储主机发生故障时，可能需要执行此方案。

1. 运行 migration-backup.ps1 捕获用户到个人虚拟磁盘的映射。
2. 使用备份解决方案将原始计算机目录中的个人虚拟磁盘移动或捕获至磁盘：
 - ESX 或 Hyper-V：个人虚拟磁盘位于 Controller 指定的存储上，该存储位于包含虚拟磁盘所连接计算机的名称的文件夹中。
 - XenServer：个人虚拟磁盘位于 Controller 指定的存储的根目录中。每个虚拟磁盘的名称为 GUID。
3. 使用存储备份解决方案从原始计算机目录中还原个人虚拟磁盘：
 - ESX 或 Hyper-V：将虚拟磁盘置于新存储资源的新文件夹中。
 - XenServer：将虚拟磁盘置于新存储资源的根目录中。
4. 从用于创建失败的计算机目录的主映像中创建 Provisioning Services 虚拟磁盘或 Machine Creation Services 快照。
5. 从虚拟磁盘或快照的“开始”菜单中运行更新清单。
6. 使用与失败的计算机目录相同的命名约定在 Studio 中重新创建计算机目录。此操作将生成新计算机的目录，每台计算机均具有站点数据库可识别的新个人虚拟磁盘。
7. 确认已将重新创建的计算机目录分配给正确的交付组。
8. 确认桌面组处于维护模式且其中的计算机已关闭。
9. 编辑备份脚本生成的 .xml 文件：
 - ESX 或 Hyper-V：对于该文件中的每个 PVD 部分，请将 DiskName 中的文件夹名称替换为还原的虚拟磁盘的位置。
 - XenServer：请跳过此步骤。

10. 在 Controller 上运行 migration-restore.ps1 脚本，并使用修改的 .xml 文件作为输入。该脚本无需移动虚拟磁盘便可对其进行连接。
11. 确认已成功还原用户的数据。

示例方案 3：在计算机目录中还原个人虚拟磁盘的子集。

在此方案中，计算机目录中的一些但并非全部个人虚拟磁盘发生故障并得到还原。目录中的虚拟机未发生故障。

1. 运行 migration-backup.ps1 捕获 .xml 文件中的用户到个人虚拟磁盘的映射。
2. 在该 .xml 文件中，针对计算机目录中的每个用户均具有 PVD 部分。对于无需还原个人虚拟磁盘的所有用户，请从该文件中删除这些用户及其关联的部分。
3. 使用备份解决方案从原始计算机目录中还原个人虚拟磁盘，如其他方案之一中所述：
 - 要使用新的计算机名称，请采用示例方案 1。
 - 要保留计算机名称，请采用示例方案 2。
4. 确保目录中存在足够的未分配计算机。根据需要添加计算机。每个要还原虚拟磁盘的用户均需要新的计算机。
5. 确认桌面组处于维护模式且其中的计算机已关闭。
6. 在 Controller 上运行 migration-restore.ps1，并使用修改的 .xml 文件作为输入。
7. 确认已成功还原用户的数据。

显示、消息和故障排除

Mar 17, 2016

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。

错误消息：7.6 及更高版本

以下错误消息对 PvD 7.6 及更高版本有效：

- **出现内部错误。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黄金映像版本。
- **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。
- **Change journal overflow was detected. (检测到更改日志溢出。)**
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。
- **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“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，则可能是由于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。
- **为装载个人虚拟磁盘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。
- **无法安装个人虚拟磁盘内核模式驱动程序。**
 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。
- **The change journal failed to activate. 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。
- **系统卷上没有足够的可用空间。**
 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。
- **Failed to reset the Personal vDisk because there is not enough free space in the personal vDisk storage.** (由于个人虚拟磁盘存储上的可用空间不足，无法重置个人虚拟磁盘。)
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。

错误消息：7.6 之前的版本

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。
0x2000002B	PvD 清单已损坏或丢失。

0x2000002F 错误代码：	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。 说明
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	磁盘上空间不足。

- **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）。

Personal vDisk 记录的事件

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：已启动清单更新。
1	Personal vDisk 状态：已完成清单更新。 GUID：%s。
1	Personal vDisk 状态：已启动映像更新。
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：清单更新失败，出现错误：%s。
2	Personal vDisk 状态：映像更新失败，出现错误：%s。
2	Personal vDisk 状态：映像更新失败，出现内部错误。
2	Personal vDisk 状态：清单更新失败，出现内部错误。
2	Personal vDisk 因不正常关机而被禁用。
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。
2	存储磁盘空间不足，无法创建 Personal vDisk 容器。

删除组件

Mar 17, 2016

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。

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。

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 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](#)。

升级和迁移

Mar 17, 2016

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。可以执行以下升级：

- 从 XenDesktop 版本 5（或更高版本）升级到 XenDesktop 的当前版本
- 从 XenApp 版本 7.5 升级到 XenApp 的当前版本

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。

要升级 XenDesktop 5（或更高版本）场或 XenApp 7.5 站点，请执行以下操作：

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。

有关详细信息，请参阅[升级部署](#)。

有关安装 Controller 修补程序的详细信息，请参阅知识中心文章 [CTX201988](#)。

要将 XenApp 6.5 工作服务器升级到 VDA 的当前版本，请执行以下操作：

1. 在 XenApp 6.5 工作服务器上运行产品安装程序。此软件从 XenApp 6.5 场删除服务器，删除 XenApp 6.5 软件，并安装 VDA for Windows Server OS 的当前版本。
2. 升级服务器后，将其添加到当前站点中的计算机目录和交付组。

有关详细信息，请参阅[将 XenApp 6.5 工作进程升级至新的 VDA for Windows Server OS](#)。

迁移

将数据从早期部署迁移到最新版本。可以迁移 XenApp 6.5 或 XenDesk 4 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。

要从 XenApp 6.5 进行迁移，请执行以下操作：

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](#)。

要从 XenDesktop 4 进行迁移，请执行以下操作：

1. 安装核心组件并创建新的 XenDesktop 站点。
2. 从 XenDesktop 4 场，使用导出命令工具将场数据导出到 XML 文件。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，使用导入命令工具和 XML 文件将场数据导入到新站点。
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 XenDesktop 4](#)。

升级部署

Apr 25, 2016

在本文中：

- 简介
- 可以升级的产品组件版本
- 要求、限制和准备工作
- 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
- 升级顺序

简介

可以将某些部署升级到较新版本，而无需先设置新计算机或站点；这称为原位升级。可以执行以下升级：

- 从 XenDesktop 版本 5（或更高版本）升级到最新发布（当前）的 XenDesktop 版本
- 从 XenApp 版本 7.5（或更高版本）升级到最新发布（当前）的 XenApp 版本

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。安装程序会先确定哪些组件需要升级，然后在您的命令处启动升级。升级组件之后，使用新升级的 Studio 来升级站点数据库和站点。

在本文档中，除非另有说明，否则“产品”一词是指 XenApp 7.x 或 XenDesktop 7.x。

可以升级的产品组件版本

使用产品安装程序和 Studio，可以升级：

- Delivery Controller 5 或更高版本
- VDA 5.0 SP1 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。
 - 如果安装程序在计算机上检测到 Receiver for Windows Enterprise (CitrixReceiverEnterprise.exe)，则会将其升级到 Receiver for Windows Enterprise 3.4。
- Director 1 或更高版本
- 数据库：这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

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 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。
- Microsoft System Center Virtual Machine Manager SCVMM。当前产品支持 SCVMM 2012 和 SCVMM 2012 SP1; XenDesktop 5.x 支持早期版本。为避免停机, 可以按照以下顺序进行升级:
 1. 如果 Controller 运行低于 XenDesktop 5.6 FP1 的版本, 则将其升级到 XenDesktop 5.6 FP1 (请参阅此版本的 XenDesktop 文档)。
 2. 将 SCVMM 服务器升级到 SCVMM 2012; 有关说明, 请参阅 Microsoft 文档。
 3. 将 XenDesktop 组件升级到当前版本。
 4. (可选) 将 SCVMM 服务器升级到 SCVMM 2012 SP1。
- StoreFront。

要求、限制和准备工作

- 必须使用产品安装程序的图形界面或命令行界面来升级核心组件和 VDA; 不能从早期版本导入或迁移数据。
- 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, 如果升级中包含新版本的 Controller 和 Studio, 但您只升级 Controller (不在安装了 Studio 的计算机上运行安装程序), Studio 将不允许您继续管理站点, 直到升级 Studio 为止。
- 在升级 Citrix 许可证服务器之前, 请确保新产品版本的专享升级服务日期有效。如果要从早期 7.x 产品版本进行升级, 此日期必须至少为 2015 年 11 月 18 日。
- 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。
- 在开始任何升级活动之前, 请按照 CTX135207 中所述备份数据库, 以便在数据库升级后发现任何问题时对数据库进行还原。
- (可选) 备份模板并升级虚拟机管理程序 (如果使用)。
- 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。
- 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。
- 如果不打算将所有 VDA 升级到最新版本, 请查阅混合 VDA 支持。
- 如果您的部署包含 Web Interface, Citrix 建议使用 StoreFront。
- 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。
- 请查看以下升级顺序, 以便规划并减少可能出现的中断。

无法进行以下升级:

- 从早期版本或技术预览版本升级
- 从 7.5 之前的 XenApp 版本升级 (将服务器上的 XenApp 6.5 软件替换为当前的 VDA for Server OS 除外, 请参阅[迁移 XenApp 6.x](#))
- 从 5.6 之前的 XenDesktop 版本升级, 请参阅[迁移 XenDesktop 4](#)
- 从 XenApp 升级到 XenDesktop, 或从 XenDesktop 升级到 XenApp

混合环境注意事项

如果您的环境中包含的站点和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 7.1 站点和 XenDesktop 7.5 站点）。有关详细信息，请参阅 StoreFront 文档。

- 在混合环境中，仍在每个站点中对每个发行版使用 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，也可能出现 VDA 注册问题。请参阅下文的“混合 VDA 注意事项”。

- 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 Receiver 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 Windows 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。如果无法重新映像，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。

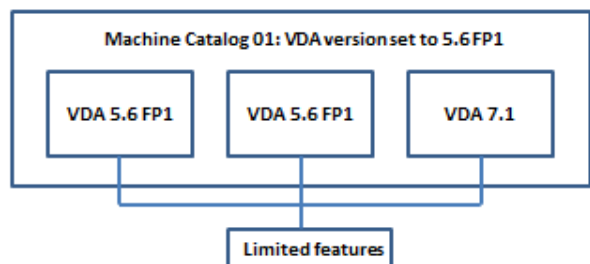
混合 VDA 支持

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。例如，要使用 7.6 版本中的会话预启动、会话延迟结束及未经身份验证的用户功能，必须至少安装 VDA 7.6 版本。

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，如果在计算机目录中混合使用多个 VDA 版本，可能会产生意外的结果

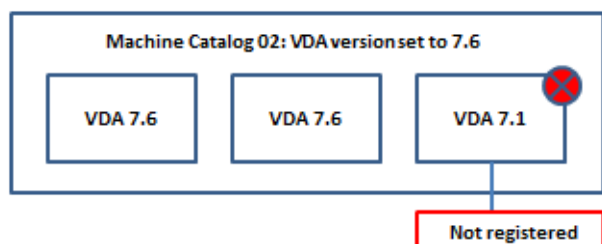
如上所述，如果您的部署包含 Windows XP 和 Windows Vista 系统，则必须使用早期 VDA 版本，并且包含这些计算机的计算机目录必须指定 VDA 版本 5.6 FP1。VDA 将在 Controller 中成功注册，但这些计算机将无法使用 7.x 版本中的很多新功能（包括 StoreFront）。这也适用于任何已添加到此目录中且装有 7.x 版本 VDA 的计算机。下图说明了这一点。



在上述情况下，如果必须继续使用旧 VDA，请将它们放入自身的计算机目录中。

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。

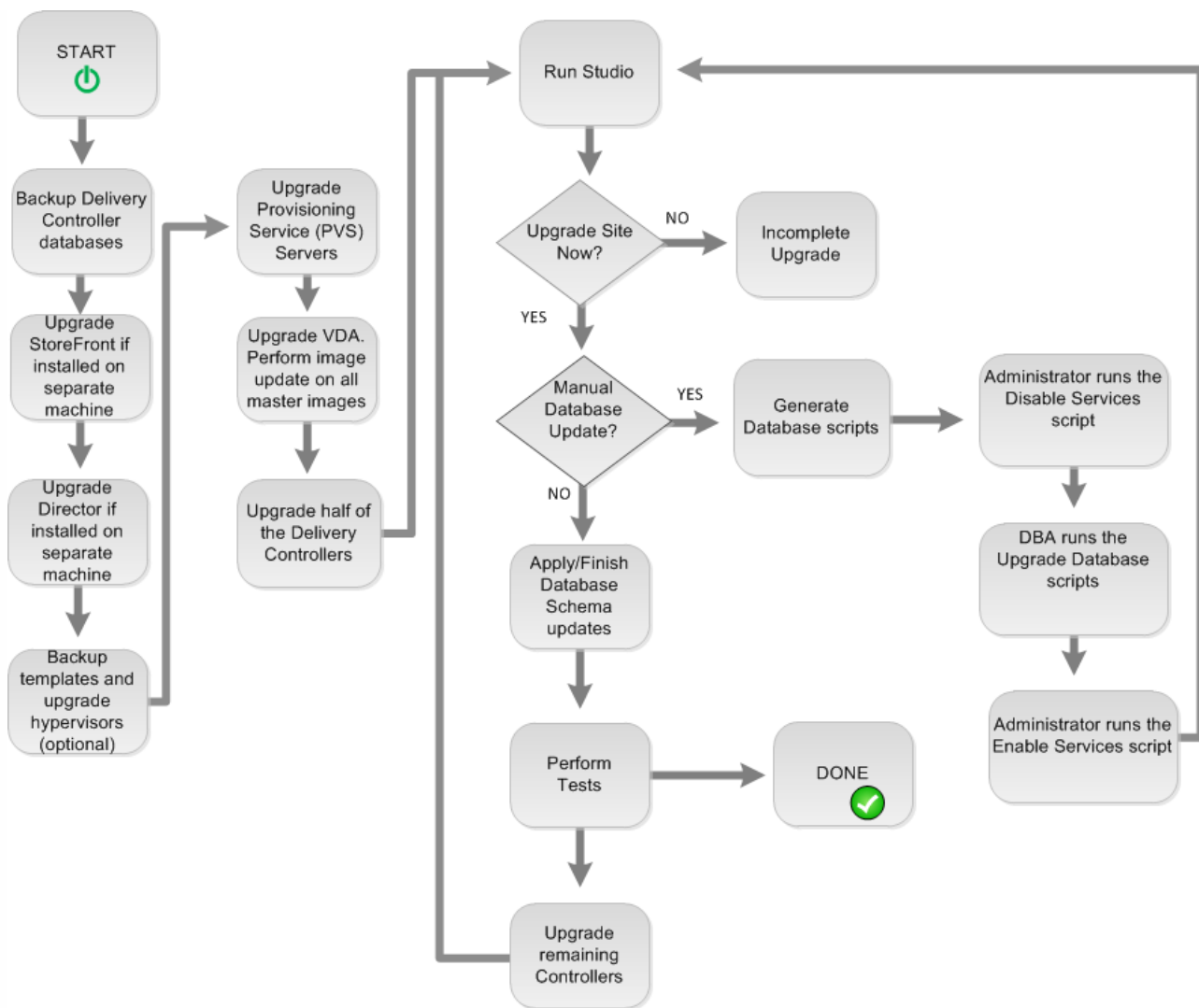
例如，假定最新 VDA 版本是 7.6。使用默认 VDA 设置创建计算机目录：“7.6 (建议，以访问最新功能)”。然后，向此目录添加三个计算机：其中两个装有 VDA 7.6；一个装有 VDA 7.1。



在本例中，装有 VDA 7.1 的计算机将无法在 Controller 中注册。如果无法升级此 VDA，请考虑先创建一个单独的计算机目录并将 VDA 设置配置为“版本 7.0 或更高版本”，然后再添加此计算机。虽然此计算机将无法利用 7.6 中的新功能，但它可以在 Controller 中进行注册。

升级顺序

升级顺序如下图所示；后面是说明。如果组件安装在不同的计算机上，可以在其中的每个计算机上运行安装程序。



升级组件

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”。

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，请在其中的每个计算机上运行安装程序（首选顺序如下：先是许可证服务器，然后是 StoreFront，最后是 Director）。
2. 按照 Provisioning Services 文档中的说明，升级 Provisioning Services 服务器和客户端。
3. 在包含 VDA 的计算机上运行产品安装程序。虽然在升级 Controller 前后均可以升级 VDA，但 Citrix 建议在升级 Controller 之前升级 VDA，因为这样便能在升级之后快速启用新功能。

从早期 7.x 版本升级安装在物理机（包括 Remote PC Access）上的 VDA 时，使用命令行接口和以下参数：/EXCLUDE "Personal vDisk","Machine Identity Service"。例如：

```
C:\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /EXCLUDE "Personal vDisk","Machine Identity Service"
```

4. 在一半的 Controller 上运行产品安装程序。（这还将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，以使用户能访问此站点。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。
5. 如果 Studio 未安装在上一步中所升级的其中一个 Controller 上，则在安装 Studio 的计算机上运行安装程序。
 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](#)。
 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**。
 8. 完成升级并确认完成之后，关闭 Studio，然后再重新打开。
 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。
 10. 在升级完成时选择**完成**之后，可以在 Citrix 客户体验改善计划 (CEIP) 中进行注册，从而收集有关部署的匿名信息。之后，可以利用此信息来提高产品质量、可靠性及性能。
 11. 升级组件、数据库和站点之后，使用 Studio 执行以下操作：
 - 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。
 - 更新使用升级后的 VDA 的所有主映像。
 - 升级计算机目录和交付组。

升级站点数据库和站点

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。

- 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，请参阅数据库文章。
- 如果 Studio 用户没有这些权限，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。如果 SQL 脚本手动运行，则应使用 SQLCMD 实用程序或在 SQLCMD 模式下使用 SQL Management Studio 运行。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（如 [CTX135207](#) 中所述）。

数据库升级期间，产品服务处于禁用状态。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：此过程包括生成脚本和运行脚本。

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。
2. 按照显示的顺序运行以下脚本：

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使用 SQL Server Management Studio 等工具运行的 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使用 SQL Server Management Studio 等工具运行的 SQL 脚本。

UpgradeLoggingDatabase.sql 脚本	说明 由包含配置日志记录数据库的服务器上的数据库管理员使用 SQL Server Management Studio 等工具运行的 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。

3. 完成显示的核对表任务之后，请选择**完成升级**。

将 XenApp 6.5 工作进程升级至新 VDA

Mar 17, 2016

在 XenApp 6.5 工作进程服务器上运行当前产品安装程序时，此安装程序将：

- 从 XenApp 6.5 场删除服务器（此任务自动调用 XenApp 6.5 安装程序的命令行接口）
- 删除 XenApp 6.5 软件
- 安装新的（XenApp 7.6 或受支持的更高版本）VDA for Windows Server OS

使用安装程序的图形界面时，所遵循的向导与在新 XenApp 站点中安装 VDA for Windows Server OS 时使用的向导相同。同样，命令行接口使用的命令和参数与安装其他 VDA 时使用的命令和参数相同。

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。

您可能已经熟悉使用安装程序安装 XenApp 核心组件和其他 VDA 的操作。在 XenApp 6.5 工作进程服务器上启动安装程序（[使用图形界面进行安装](#)）或发布命令（[使用命令行安装 VDA](#)）。

须知事项：

- 此升级在仅会话主机模式下配置的 XenApp 6.5 服务器上有效（也称为仅会话或工作服务器）。
- 卸载 XenApp 6.5 需要重新启动多个服务器。使用命令行接口时，可以使用 /NOREBOOT 选项禁止自动操作；但是，必须重新启动服务器才能使卸载和后续安装生效。
- 如果卸载 XenApp 过程中出错，请检查错误消息中引用的卸载错误日志。卸载日志文件位于“%TEMP%\Citrix\XenDesktop Installation\XenApp 6.5 Uninstall Log Files”文件夹中。
- 升级后，请检查 IMA 特定的设置和注册表项，以及与 HDX 有关的系统设置和注册表。某些设置可能不再适用，或者工作方式不再相同。
- 升级 XenApp 6.5 工作服务器后，从新 XenApp 站点中的 Studio 中，为升级后的工作进程创建计算机目录（或编辑现有目录）。
- 如果从 XenApp 6.5 控制器服务器迁移策略和应用程序设置（请参阅[迁移 XenApp 6.x](#)），请将包含已迁移的发布应用程序的交付组分配到在 XenApp 6.5 中托管这些应用程序的计算机目录。

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. An error occurred while plugging XML into Internet Information Server. Setup cannot copy files to your IIS Scripts directory. 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。
- **解决方案：**
 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”卸载以下程序：
 1. Citrix XenApp 6.5
 2. Microsoft Visual C++ 2005 可再发行组件包 (x64)，版本 8.0.56336
 4. 重新启动服务器。
 5. 运行 XenApp 安装程序以安装 VDA for Windows Server OS。

迁移 XenApp 6.x

Mar 17, 2016

重要：请在开始迁移之前完整阅读本文。

XenApp 6.x 迁移工具（简称迁移工具）是关于 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。

- 在 XenApp 6.0 或 6.5 控制器上：
 - 导入 PowerShell 导出模块。
 - 运行导出 cmdlet 以将策略和/或场数据导入到 XML 文件中。
- 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。
- 在 XenApp 7.6 控制器上：
 - 导入 PowerShell 导入模块。
 - 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）。
- 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。

本版本中的新增功能

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。

迁移工具包

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 场导出数据的数据，以及一些共享模块。

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 模块或文件	ExportPolicy.psm1 脚本模块的 PowerShell 清单文件。 说明
ExportXAFarm.psd1	ExportXAFarm.psm1 脚本模块的 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	XmlUtilities.psm1 脚本模块的 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	ImportPolicy.psm1 脚本模块的 PowerShell 清单文件。
ImportXAFarm.psd1	ImportXAFarm.psm1 脚本模块的 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	XmlUtilities.psm1 脚本模块的 PowerShell 清单文件。
XmlUtilities.psm1	包含 XML 功能的共享 PowerShell 脚本模块。

限制

- 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。

安全注意事项

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。

日志记录和错误处理

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。

要求、准备和最佳实践

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。ExportXAFarmpsd1 和 ExportXAFarmpsm1 是无法执行的文件。
- 在下面的分步说明部分中，大多数 <字符串> 参数值用引号括起来。这些是单字符串可选项。

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。

您可以导出数据，然后使用带有 -Preview 参数的 cmdlets 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。

分步说明：导出数据

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，如果打算仅导出场数据，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 "<字符串 >.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 "<字符串>"	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 to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#”（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。

参数	说明
-XmlOutputFile "<字符串>.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。

参数	说明
-LogFile "<字符串>"	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 to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#”（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、负载均衡策略、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。
-ApplLimit <整数>	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。
-SkipApps <整数>	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。

分步说明：导入数据

[此处](#)提供了展示导入完整过程的视频。

您可以在执行实际导入之前运行预览导入（发布带有 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 "<字符串>.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 "<字符串>"	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 "<字符串>"	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 to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#”（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

参数	说明
	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 MyPolicies.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 "<字符串>.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 "<字符串>"	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 "<字符串>"	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 to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#”（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
-DeliveryGroupName "<字符串>"	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 场名称> - 交付组"
-MatchFolder "<字符串>"	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 "<字符串>"	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 。

参数	说明
-MatchServer "<字符串>"	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 "<字符串>"	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 "<字符串>"	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 "<字符串>"	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 "<字符串>"	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 "<字符串>"	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。

迁移后需执行的任务

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。
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。

过滤器	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。
客户端 IP 地址	列出客户端 IP 地址范围；每个范围应该被允许或拒绝。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。

- 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）。
- 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。
- 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）。
 - 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：

- 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。

高级用法

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](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。

故障排除

- 如果要使用 PowerShell 2.0，并且已使用 Add-PSSnapIn cmdlet 添加 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 已加载的情况下加载此驱动器，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 DSMMAINT 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。

未导入的策略设置

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
- 全图标缓存
- 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
- 登录限制事件日志记录
- 具有登录限制的最大服务器百分比
- 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 *
- 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

未导入的应用程序类型

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）

应用程序属性映射

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
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

FMA 属性	值
Visible	集初始化；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。
ConnectionsThroughAccessGatewayAllowed	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-unique 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。

FMA 属性	备注
ContentAddress	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均衡。
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。
ServerNames	FMA 使用其他技术。
WorkerGroupNames	FMA 不支持工作组。

迁移 XenDesktop 4

Mar 17, 2016

可以使用迁移工具将 XenDesktop 4 场的数据和设置传输到 XenDesktop 7.x 站点，此工具位于 XenDesktop 安装介质上的 Support > Tools > MigrationTool 文件夹中。此工具包括：

- 导出工具 XdExport，用于将 XenDesktop 4 场数据导出到 XML 文件（默认名称：XdSettings.xml）。XML 文件架构位于 XdFarmxsd 文件中。
- 导入工具 XdImport，用于通过运行 PowerShell 脚本 Import-XdSettings.ps1 导入数据。

要成功使用迁移工具，两个部署必须具有相同的虚拟机管理程序版本（例如 XenServer 6.2）和 Active Directory 环境。

不能使用此工具迁移 XenApp，也不能将 XenDesktop 4 迁移到 XenApp。

提示：可以将 XenDesktop 5（或更高 XenDesktop 版本）升级到当前 XenDesktop 版本；请参阅[升级部署](#)。
限制

并非所有数据和设置都可以导出。以下配置项无法迁移，因为它们可以导出但不能导入：

- 管理员
- 委派管理设置
- 桌面组文件夹
- 许可配置
- 注册表项

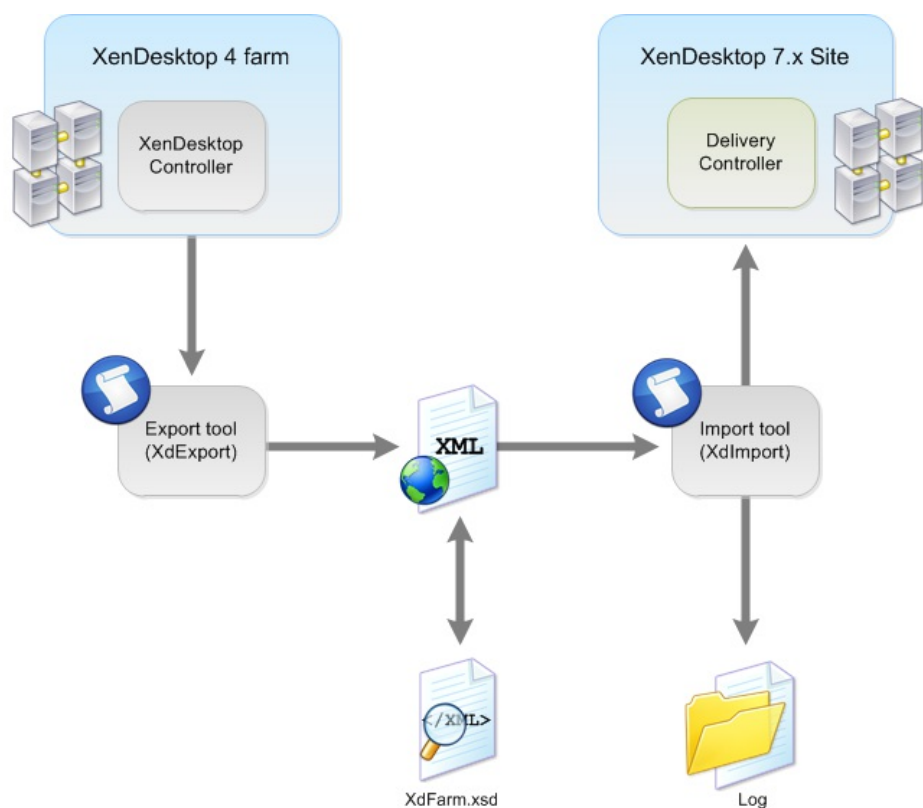
在迁移中不直接支持以下用例：

- 合并策略或桌面组的设置或托管设置。
- 将专用桌面合并到随机交付组。
- 通过迁移工具调整现有的组件设置。

有关详细信息，请参阅[迁移和不迁移的内容](#)。

迁移步骤

下图总结了迁移过程。



迁移过程按照以下顺序进行：

1. 在 XenDesktop 4 控制器上的 Studio 控制台中，打开所有要导出的计算机的维护模式。
2. 使用 XdExport 将数据和设置从 XenDesktop 4 场导出到 XML 文件中；请参阅[从 XenDesktop 4 场中导出](#)。
3. 编辑 XML 文件，使其仅包含要导入到新 XenDesktop 站点中的数据和设置；请参阅[编辑迁移工具 XML 文件](#)。
4. 使用 XdImport 将数据和设置从 XML 文件导入到新 XenDesktop 站点；请参阅[导入 XenDesktop 4 数据](#)。
5. 要进行其他更改，请重复步骤 3 和 4。进行更改后，您可能需要将其他桌面导入到现有交付组。为此，请在导入时使用 Mergedesktops 参数。
6. 完成迁移后需执行的任务；请参阅[迁移后需执行的任务](#)。

迁移之前

在开始迁移之前，请完成以下操作：

- 确保您了解可以导出和导入哪些数据，以及如何应用于您自己的部署。请参阅[迁移和不迁移的内容](#)。
- Citrix 强烈建议您手动备份站点数据库，以便您可以在发现问题时进行还原。
- 安装 XenDesktop 7.x 组件并创建站点，包括数据库。
- 要从 XenDesktop 4 进行迁移，所有 VDA 必须处于 XenDesktop 5.x 级别，以便与 XenDesktop 4 和 XenDesktop 7.x 控制器兼容。Controller 基础结构全面运行 XenDesktop 7.x 后，Windows 7 VDA 可升级至 XenDesktop 7.x。有关详细信息，请参阅[迁移示例](#)。

从 XenDesktop 4 场中导出

Mar 17, 2016

导出工具 XdExport 可以从单个 XenDesktop 4 场中提取数据，并根据数据值的表示形式生成 XML 文件。

XML 文件的架构位于 XdFarm.xsd 文件中，该文件包含在下述迁移工具下载包中：XdExport.zip 和 XdImport.zip。

在要导出数据的场中的 XenDesktop 4 控制器上运行 XdExport。该计算机必须已安装 XenDesktop 4 PowerShell SDK。必须具有以下权限才可以导出数据：

- 用户身份至少是场的只读权限 Citrix 管理员。
- 读取注册表的权限。

您可以在 XenDesktop 控制器处于有效使用状态（例如，用户已登录 VDA）时运行该工具，但建议您不这样做。

Citrix 强烈建议：

- 在安装了公共修补程序的最新 XenDesktop 4 控制器上运行导出工具。
- 当导出运行时不更改站点的配置（例如，删除桌面组）。

1. 下载 XdExport.zip，并将文件提取到 XenDesktop 4 控制器中。
2. 在命令行提示窗口中，运行具有以下可选参数的 XdExport.exe：

参数	说明
-Verbose	生成提供详细进度信息的信息。
-FilePath <路径>	指示场数据要导出到的 XML 文件的位置。默认位置为 .\XdSettings.xml
- Overwrite	覆盖在 -Filepath 中指定的位置处存在的所有文件。如果未提供此参数，但已存在一个输出文件，此工具将无法运行，并显示以下错误消息：“错误: 文件已存在。请指定 -Overwrite 以允许覆盖该文件。”
-? 或 - help	显示描述参数的文本，如果没有导出任何数据则退出。

3. 如果导出工具成功运行，则将显示完成消息。文件 XdSettings.xml 位于 FilePath 参数所指定的位置。如果导出工具运行失败，则将显示一条错误消息。

编辑迁移工具 XML 文件

Mar 17, 2016

将数据导入 XenDesktop 7.x 站点之前，请检查并编辑由导出工具 (XdExport) 生成的 XML 文件的内容（尤其是在分多个阶段执行迁移时），并导入部分用户、交付组和策略，然后再导入其他数据。

可以使用任意文本编辑器查看或更改文件内容，也可以使用专用 XML 编辑器，例如 Microsoft XML Notepad。

XML 内容中的某些元素必须存在，以便 XML 文件能被导入工具 (XdImport) 所接受。

所需的 XML 架构在 XdFarm.xsd 文件中定义，该文件作为迁移工具下载包的一部分提供。使用此文件时：

- 如果 minOccurs 属性的值为 1 或更大的值，则表示如果父元素存在，一些特定元素也必须存在。
- 如果提供给导入工具的 XML 文件无效，该工具将终止，并将显示一条错误消息，提示您如何找到该问题在 XML 文件中的位置。

导入桌面或交付组的子集

要仅导入交付组和桌面的子集，可编辑 DesktopGroups 元素的内容。DesktopGroups 元素可以容纳多个 DesktopGroup 元素，并且在每个 DesktopGroup 元素中，都存在一个可以包含多个 Desktop 元素的 Desktops 元素。

请勿删除 DesktopGroups 元素，尽管您能够删除所有 DesktopGroup 元素并将其保留为空。同样，在每个 DesktopGroup 元素中，必须存在 Desktops 元素，但可以不包含任何 Desktop 元素。

删除 Desktop 或 DesktopGroup 元素以避免导入单个特定计算机或整个交付组。例如，XML 文件包含：

```
...      ...      ...      ...      ...      ...      ...
```

在此示例中，您的编辑操作将阻止导入 Group1 组，而只会导入 Group2 组中的 Machine3：

```
...      ...      ...
```

管理名称重复的交付组

在 XenDesktop 4 中，桌面组可以通过文件夹形式组织，名称相同的桌面组可以显示在不同文件夹中，内部桌面组名称是显示给用户的名称。在此版本中，不可以将交付组置于文件夹中，每个交付组必须有唯一的内部名称，显示给用户的名称可以不同于内部名称。为反映这些不同，您可能必须重命名桌面组。

例如，在 XenDesktop 4 场中可以存在两个不同的桌面组，这两个桌面组显示给两个不同用户的名称均为“我的桌面”，这可以使用桌面组文件夹来实现。如果这些交付组要在 XenDesktop 7.x 站点中保持独立，您必须在 XML 文件中编辑桌面组名称，使这些名称为唯一的名称。

如果 XenDesktop 7.x 站点中的某个交付组与要导入的桌面组同名，并且这些交付组要在 XenDesktop 7.x 站点中保持独立，您必须在 XML 文件中编辑 XenDesktop 4 的桌面组名称，使该名称在站点中保持唯一。如果要导入的桌面组实际上与 XenDesktop 7.x 交付组相同，并且要将 XML 文件中的计算机合并到现有的桌面组中，这种情况下，无需重命名该交付组；为导入工具指定 -MergeDesktops 参数即可。例如，如果 XML 文件包含：

```
... \Sales      ... \Finance
```

删除重复的名称，如下所示：

```
... \Sales      ... \Finance
```

管理策略导入

可以从 XML 文件中删除策略，并且可以指定唯一的名称以避免策略名称重复。不支持合并策略。

- 导入策略数据时有两种情形：成功导入所有策略，或者不导入任何策略数据（如有任何故障）。
- 导入大量带有许多设置的策略时，导入过程可能需要数小时的时间。
- 如果您批量导入策略，它们的原始优先级可能会受到影响。导入策略时，所导入策略的相对优先级将会保留，但这些策略的

优先级高于站点中已存在的策略。例如，如果要导入优先级分别为 1 到 4 的四个策略，并决定分两批导入这些策略，则应首先导入优先级为 3 和 4 的策略，因为第二批策略会自动获得更高的优先级。

要仅将策略的子集导入到 XenDesktop 7.x 站点中，请编辑 Policies 元素的内容。Policies 元素可以容纳多个 Policy 元素。请勿删除 Policies 元素，尽管您能够删除所有 Policy 元素并将其保留为空。删除全部 Policy 元素以避免导入特定的 XenDesktop 4 策略。例如，如果 XML 文件包含：

... ..

为避免导入任何 XenDesktop 4 策略，并避免与已在 XenDesktop 7.x 站点中配置的策略相冲突，请按如下所示编辑该文件以删除各 Policy 元素：

或者，也可以按如下所示编辑该文件，以使用其他名称导入策略：

... ..

导入 XenDesktop 4 数据

Mar 17, 2016
导入工具 XdImport 从 XenDesktop 4 读取导出工具 XdExport 生成的 XML 文件中包含的设置，并将这些设置应用到现有 XenDesktop 7.x 站点。 导入工具使用 PowerShell 脚本 Import-XdSettings.ps1。

要仅应用所导出数据子集，请先编辑此 XML 文件，然后再运行导入工具。例如，您可能希望删除在 XenDesktop 7.x 部署中不需要的桌面组和策略。如果您将全部元素留空，则导入工具可以成功运行。例如，您可以删除所有桌面组而不会出现任何问题。 导入工具始终先验证 XML 文件，然后再尝试导入任何数据。

在已安装所有 XenDesktop 7.x SDK 的任意计算机上运行 XdImport。您必须具有完全权限 XenDesktop 管理员身份才能运行此工具。

在导入之前，请确保已设置 XenDesktop 7.x 站点，包括其数据库。Citrix 建议您先完成对 XenDesktop 7.x 的导入操作，然后再执行任何用户测试或常规站点配置。请仅在站点未使用时合并配置。

- 1. 创建一个 XenDesktop 7.x 站点。
- 2. 下载 XdImport.zip，并将文件提取到要运行导入工具的计算机中。
- 3. 在 PowerShell 会话中，运行带有以下参数的 Import-XdSettings.ps1：

参数	说明
- HypervisorConnectionCredentials	(必需。) PowerShell 哈希表，用于根据创建虚拟机管理程序连接的需要将虚拟机管理程序地址映射到 PSCredential 实例。 默认值为 @{} 输入 XenDesktop 4 场连接的虚拟机管理程序的凭据。 对于单个虚拟机管理程序，可以按如下所示创建参数： <pre>\$credential = Get-Credential \$mappings = @{ "http://" = \$credential } .\Import-XdSettings.ps1 -FilePath .\XdSettings.xml -HypervisorConnectionCredentials \$mappi</pre> 在哈希表中指定的地址必须与 XML 文件中的地址完全一致。 例如，对于 XenServer 和 VMware 虚拟机管理程序，可以创建以下参数： <pre>\$Xencredential = Get-Credential \$VMWcredential = Get-Credential \$mappings = @{ "http://" = \$Xencredential; "http://SDK" = \$VMWcredential } .\Import-XdSetting</pre>
-FilePath <路径>	(<路径> 的值为必需。) 要从中导入场数据的 XML 文件的位置。
-AdminAddress	XenDesktop 7.x 站点中的控制器名称。默认名称为 localhost
-MergeDesktops	将在 XML 文件中定义的桌面添加到 XenDesktop 7.x 站点中与该 XML 文件中所述的组同名的交付组中。 同时还将添加相关联的计算机和用户。 如果未提供此参数，则不会将任何内容添加到 XenDesktop 7.x 站点的现有交付组中。
-SkipMachinePolicy	此脚本不创建包含站点级别设置的计算机策略。如果您未提供此参数，但站点的计算机策略存在，脚本运行将失败。
-WhatIf	完成试运行，以确定在 XenDesktop 7.x 站点中将发生哪些更改或添加哪些内容。如果包括此参数，则会向日志文件发送信息，但不会更改站点。
-LogFilePath <路径>	指明日志文件的完整路径。日志文件中包含针对 XenDesktop 7.x 站点执行的所有写操作的说明文本。默认值 = .\Import-XdSettings.log
-? 或 -help	显示有关参数的信息，如果没有导入任何数据则退出。

如果 XML 文件中包含策略数据，则系统或者成功导入所有策略，或者不导入任何策略数据（如有任何故障）。 导入大量带有许多设置的策略时，导入过程可能需要数小时的时间。

脚本完成时，将显示完成消息。从 XML 文件中成功导入数据后，可以进一步反复运行导出和导入过程，或者，如果已导入所有相关数据，则完成迁移后任务。

迁移后需执行的任务

Mar 17, 2016

从 XenDesktop 4 场成功将数据导入 XenDesktop 7.x 站点后，在使用新站点进行生产工作之前，请执行以下任务：

- 升级 Virtual Delivery Agent (VDA)。Citrix 建议您在升级控制器、Studio 或 Director 之前先升级 VDA，但这并非必需操作。
 - 对于 Windows Vista 和 Windows XP，请升级到 XenDesktop 5.6 Feature Pack 1 Virtual Desktop Agent。
 - 对于 Windows 7，请升级到 XenDesktop 7.x Virtual Delivery Agent。
- 为 XenDesktop 7.x 站点创建所需的管理员。
- 更新用户设备 — Citrix 建议使用最新版本的 Citrix Receiver 更新用户设备，以获取修补程序所带来的好处以及获取对最新功能的支持。
- 修改导入的桌面以使用基于注册表的控制器发现，并使用以下任一方法将其指向 XenDesktop 7.x 控制器：
 - 手动编辑注册表以删除不必要的组织单位 (OU) GUID 注册表项，并添加 ListOfDDCs 注册表项。
 - 设置一个计算机策略以通过使用 Active Directory 策略 GPMC.msc 将控制器列表分发给各个桌面。不能使用 Studio 配置此设置。

对于 XenDesktop 7.x 来说，基于注册表的 Controller 发现为其默认使用的发现方法，但仍然可以使用基于 Active Directory 的发现。

- 或者，还可以选择实施 [CTX133384](#) 的 XenDesktop 基于注册表的注册最佳做法中所述的以下注册表项设置：
 - HeartbeatPeriodMS
 - PrepareSessionConnectionTimeoutSec
 - MaxWorkers
 - DisableActiveSessionReconnect
 - ControllersGroupGuid

如果您不执行此操作，则使用这些注册表项的默认 XenDesktop 7.x 设置。

- 使导入的计算机脱离维护模式（如果这些计算机在 XenDesktop 4 中处于维护模式），然后再生成 XML 文件。
- 检查 XenDesktop 7.x 设置以确保其正确无误，特别是当您在 XenDesktop 4 中更改了 PortICAConfig XML 文件时。
- 检查所有已迁移的组件，确保迁移已成功。

迁移示例

Mar 17, 2016

示例 1：将单个大型 XenDesktop 4 场迁移到 XenDesktop 7 站点

在本例中，XenDesktop 4 场正在使用。XenDesktop 4 场有 50 个桌面组，每个组中平均包含 100 个桌面。XenDesktop 4 桌面是通过 Provisioning Services (PVS) 提供的，并且计算机在 VMware ESX 虚拟机管理程序上运行。所有 VM 上安装的 VDA 均为 XenDesktop 4 版本。

迁移步骤

1. 将所有 XenDesktop 4 VDA 升级至 XenDesktop 5.6 Feature Pack 1 VDA 软件。这样，VDA 便可以在 XenDesktop 4 控制器和 XenDesktop 7 Delivery Controller 中注册。
 - 对于 Windows 7 VDA，请参阅在 [VM 或刀片式计算机上升级 Virtual Desktop Agent](#)。
 - 对于 Windows XP 和 Windows Vista VDA，请参阅 [Windows XP 或 Windows Vista 上的 Virtual Desktop Agent](#)。
2. 确保所有用户均已从 XenDesktop 4 场注销。
3. 确保所有这些计算机均处于维护模式。
4. 在 XenDesktop 4 场中运行导出工具 (XdExport)。
5. 安装 XenDesktop 7 组件。
 1. 使用 Studio 创建全面生产模式站点。
 2. 如果 Provisioning Services 是部署的一部分，请升级 Provisioning Services 服务器和代理。
 3. 升级许可证服务器及关联的许可证。
6. 将导入工具 (XdImport) 解压缩到 XenDesktop 7 Controller 上的本地目录。
7. 将导出工具在步骤 4 中生成的 XML 文件 (XdSettings.xml) 复制到本地目录。
8. 从 XenDesktop 7 站点上 Studio 根节点的 PowerShell 控制台中，启动 PowerShell 会话。
9. 运行导入工具 (XdImport)，以传递关联虚拟机管理程序凭据和 XML 文件路径。
10. 从 Studio 导航窗格中的“管理员”节点重新手动创建管理员设置；有关详细信息，请参阅[委派管理](#)。
11. 修改导入的桌面，以使用基于注册表的 Controller 发现；并将其指向新的 XenDesktop 7 控制器。
12. 对于在 Windows 7 上运行的 VDA，Citrix 建议升级这些 VDA，以使用 XenDesktop 7 VDA for Windows Desktop OS，这样便可以访问所有新功能。

针对目录或交付组中的计算机将 VDA 升级到 XenDesktop 7 后，升级目录（请参阅[管理计算机目录](#)）和交付组（请参阅[管理交付组中设置](#)）。
13. 关闭交付组的维护模式。
14. 配置 StoreFront 以提供之前通过 Web Interface 提供的桌面。请参阅 StoreFront 文档。

示例 2：通过部分导入到 XenDesktop 7.1 站点完成 XenDesktop 4 场导出

在本例中，迁移分为多个步骤进行，每个步骤均会迁移部分剩余桌面。XenDesktop 4 场正在使用，XenDesktop 7.1 站点已创建并且正在使用。XenDesktop 4 场有 50 个桌面组，每个组中平均包含 100 个桌面。XenDesktop 4 桌面是通过 Provisioning Services 提供的，并且计算机在 Citrix XenServer 虚拟机管理程序上运行。所有 VM 上安装的 VDA 均为 XenDesktop 4 版本。

迁移步骤

1. 在 XenDesktop 4 场中运行导出工具。
 1. 在场中的一个 Desktop Delivery Controller 上解压缩导出工具 (XdExport)。
 2. 以 Citrix 管理员身份运行不具有参数的导出工具。
2. 复制并编辑生成的 XML 文件，以使其仅包含要迁移的组和桌面。
3. 在 XenDesktop 4 场中，确保要迁移的桌面上的所有用户均已注销，并打开要迁移的所有桌面的维护模式。

4. 将导入工具 (XdiImport) 解压缩到 XenDesktop 7.1 Delivery Controller 上的本地目录。
5. 将已编辑的 XML 复制到本地目录。
6. 从 XenDesktop 7.1 站点上 Studio 根节点的 PowerShell 控制台中，启动 PowerShell 会话。
7. 运行导入工具 (XdiImport)，以传递关联虚拟机管理程序凭据和 XML 文件路径。
8. 从 Studio 导航窗格中的“管理员”节点重新手动创建管理员设置；有关详细信息，请参阅[委派管理](#)。
9. 修改导入的桌面，以使用基于注册表的 Controller 发现；并将其指向新的 XenDesktop 7.1 控制器。
10. 将所有 VDA 升级至相应的 VDA 软件：
 - 对于 Windows 7 VDA：
 - 按在 [VM 或刀片式计算机上升级 Virtual Desktop Agent](#) 中所述升级到 XenDesktop 7 Virtual Delivery Agent。
 - 针对目录或交付组中的计算机将所有 VDA 软件升级到 XenDesktop 7 后，升级目录（请参阅[管理计算机目录](#)）和交付组（请参阅[管理交付组中设置](#)）。
 - 对于 Windows XP 和 Windows Vista VDA，请升级到 XenDesktop 5.6 FP1；请参阅 [Windows XP 或 Windows Vista 上的 Virtual Desktop Agent](#)。
11. 关闭交付组的维护模式。
12. 配置 StoreFront 以提供之前通过 Web Interface 提供的桌面。请参阅 StoreFront 文档。

迁移和不迁移的内容

Mar 17, 2016

迁移的内容

下表的描述虽不全面，但介绍了迁移到此版本的过程中最重要的数据所发生的行为。除非另有说明，否则导入数据类型。

数据类型	备注
桌面组	在本版本中桌面组变为交付组。桌面组图标不导出。 如果在 XenDesktop 4 中 DefaultEncryptionLevel 未设置为 Basic，则 SecureIcaRequired 将设置为 True。 如果 XenDesktop 4 场中的一个桌面组与 XenDesktop 7.x 站点中的某个交付组同名，则可以将属于 XenDesktop 4 组的桌面添加到目标站点内的同名交付组中。 为此，请在运行导入工具时指定 MergeDesktops 参数。XenDesktop 4 组的设置并不覆盖 XenDesktop 7.x 交付组的设置。如果未指定此参数，但存在一个与 XML 文件中定义的组同名的组，则在导入任何数据之前，该工具将显示一条错误并停止。
桌面	无法将专用桌面添加到随机交付组中。无法将随机桌面添加到静态交付组中。
计算机	计算机导入到四个计算机目录中。导入工具在 XenDesktop 7.x 站点中自动创建以下计算机目录： • 已导入现有随机（针对池 VM） • 已导入现有静态（针对已分配的 VM） • 已导入物理随机（针对池 PC 或刀片式服务器） • 已导入物理静态（针对专有 PC 或刀片式服务器）。 后续任何计算机导入操作都将使用这四个计算机目录。
Pool Management 池	包括多池的池以及空闲池设置（包括时间安排）。 • 默认情况下，PeakBufferSizePercent 设置为 10%。 • 默认情况下，OffPeakBufferSizePercent 设置为 10%。 • 在本版本中，XenDesktop 4 的工作日设置中所有未选中的日期都将作为“周末电源时间方案”的组成部分导入。 • HostingXD4 操作时间向上舍入到最接近的分钟。 • 开始时间将向下舍入到最接近的小时。 • 结束时间将向上舍入到最接近的小时。
场设置	以下场设置将作为计算机策略导入： • IcaKeepAlive • AutoClientReconnect • SessionReliability 不导入用于启用 Flash 播放器的设置。

数据类型	备注工具将导入某些策略数据，过滤器、设置和打印机均作为用户策略导入。有关用户策略导出并导入的更多详细信息，请参阅本文档中的其他表格。 - 新访问策略规则将根据 XenDesktop 4 组设置进行创建。 - 导入策略时，将保留其相对优先级顺序。但在添加策略时，使用的优先级始终高于 XenDesktop 7.x 站点中任何现有策略的优先级。 - 不支持合并策略功能。 不存在用于将策略导入 Active Directory 中的选项。这些策略始终存储在站点中。
用户分配	
虚拟机管理程序设置	使用 XdImport 工具时，此参数为必需项。 导出工具将导出虚拟机管理程序地址，但不导出访问这些虚拟机管理程序所需的凭据。要在 XenDesktop 7.x 站点中创建虚拟机管理程序连接，必须从 XML 文件中提取地址，并创建一个 Powershell 哈希表，用于将这些地址映射到相关的凭据实例。然后在导入工具 HypervisorConnectionCredentials 参数中指定此哈希表。有关更多详细信息，请参阅导入 XenDesktop 4 数据 不支持合并或更新现有桌面组和虚拟机管理程序连接的虚拟机管理程序设置。
管理员	(不导入。) 导入工具不导入任何管理员数据，其中包括与委派的管理员有关的数据。需要为 XenDesktop 7.x 站点创建新的管理员。
许可配置	(不导入。) 包括诸如许可证服务器名称和版本等信息。不导出许可证文件。
桌面组文件夹	(不导入。) 本版本不支持桌面组文件夹。存在重复的桌面组名称（原因是 XenDesktop 4 场中不同的文件夹包含同名的组）时，如果您不在 XML 文件中编辑名称，导入工具将终止。
注册表项	(不导入。) 有关实现注册表项的信息，请参阅 迁移后需执行的任务 。

用户策略数据

下表介绍了如何导出和导入用户策略数据。

XenDesktop 4 类别和设置	XML 文件	XenDesktop 7.x 类别和设置
带宽\视觉效果\会话限制 OEM 虚拟通道	ClientOEMVCBandwidth	不导入
客户端设备\资源\其他 关闭 OEM 虚拟通道	DisableOEMVirtualChannels	不导入

~~XenDesktop 7.x~~ 类别和设置 不使用客户端的本地时间	~~XML 文件~~ ClientLocalTime	~~XenDesktop 7.x~~ 类别和设置
安全性\加密 SecureICA 加密	ClientSecurityRequirement	不导入
带宽\SpeedScreen 使用有损压缩的图像加速	LossyCompression 设置	ICA\视频显示\静止图像 有损压缩级别 有损压缩阈值 超级压缩 ICA\视频显示\移动图像 渐进式压缩级别 渐进式压缩阈值
带宽\视觉效果 关闭桌面墙纸	TurnOffWallpaper	ICA\桌面 UI 桌面墙纸
带宽\视觉效果 菜单动画	TurnOffMenuWindowAnimation	ICA\桌面 UI 菜单动画
带宽\视觉效果 拖动时关闭窗口内容	DoNotShowWindowContentsWhileDragging	ICA\桌面 UI 拖动时查看窗口内容
带宽\视觉效果\会话限制 音频	ClientAudioBandwidth__AllowedBandWidth	ICA\带宽 音频重定向带宽限制
带宽\视觉效果\会话限制 剪贴板	ClientClipboardBandwidth__AllowedBandWidth	ICA\带宽 剪贴板重定向带宽限制
带宽\视觉效果\会话限制 COM 端口	ClientComBandwidth__AllowedBandWidth	COM 端口重定向功能在 XenDesktop 7.x 中已弃用
带宽\视觉效果\会话限制	ClientDriveBandwidth__AllowedBandWidth	ICA\带宽

驱动器 XenDesktop 4 类别和设置	XML 文件	文件重定向带宽限制 XenDesktop 7.x 类别和设置
带宽\视觉效果\会话限制 LPT 端口	ClientLptBandwidth__AllowedBandWidth	LPT 端口重定向功能在 XenDesktop 7.x 中已弃用
带宽\视觉效果\会话限制 整体会话	OverallBandwidth__AllowedBandWidth	ICA\带宽 总会话带宽限制
带宽\视觉效果\会话限制 打印机	LimitPrinterBandWidth__AllowedBandWidth	ICA\带宽 打印机重定向带宽限制
客户端设备\资源\音频 麦克风	ClientAudioMicrophone__TurnOn	ICA\音频 客户端麦克风重定向
客户端设备\资源\音频 音频质量	ClientAudioQuality__Quality	ICA\音频 音频质量
客户端设备\资源\音频 关闭扬声器	DisableClientAudioMapping	ICA\音频 客户端音频重定向
客户端设备\资源\驱动器 连接	ConnectClientDriveAtLogon__TurnOn	ICA\文件重定向 自动连接驱动器
客户端设备\资源\驱动器 关闭软盘驱动器	DisableClientDriveMapping__DisableFloppyDrive	ICA\文件重定向 客户端软盘驱动器
客户端设备\资源\驱动器 关闭硬盘驱动器	DisableClientDriveMapping__DisableHardDrive	ICA\文件重定向 客户端固定驱动器
客户端设备\资源\驱动器 关闭 CD-ROM 驱动器	DisableClientDriveMapping__DisableCdrom	ICA\文件重定向 客户端光盘驱动器
客户端设备\资源\驱动器 关闭远程驱动器	DisableClientDriveMapping__DisableRemote	ICA\文件重定向 客户端网络驱动器

XenDesktop 4 类别和设置 客户端设备\资源\驱动器 关闭 USB 磁盘驱动器	XML 文件 DisableClientDriveMapping__DisableUSB	XenDesktop 7.x 类别和设置 ICA\文件重定向 客户端可移动驱动器
客户端设备\资源\驱动器 \优化 异步写入	CDMAsyncWrites	ICA\文件重定向 用户异步写入
客户端设备\资源\其他 关闭剪贴板映射	DisableClientClipboardMapping	ICA 客户端剪贴板重定向
客户端设备\资源\端口 关闭 COM 端口	DisableClientCOMPortMapping	COM 端口重定向功能在 XenDesktop 7.x 中已弃用
客户端设备\资源\端口 关闭 LPT 端口	DisableClientLPTPortMapping	LPT 端口重定向功能在 XenDesktop 7.x 中已弃用
客户端设备\资源\USB USB	RemoteUSBDevices__DisableRemoteUSBDevices	ICA\USB 设备 客户端 USB 设备重定向
打印\客户端打印机 自动创建	ConnectClientPrinterAtLogon__Flag	ICA\打印\客户端打印机 自动创建客户端打印机
打印\客户端打印机 旧版客户端打印机	LegacyClientPrinters__TurnOn	ICA\打印\客户端打印机 客户端打印机名称
打印\客户端打印机 打印机属性保留	ModifiedPrinterProperties__WriteMethod	ICA\打印\客户端打印机 打印机属性保留
打印\客户端打印机 打印作业路由	ClientPrintingForNetworkPrinter__TurnOn	ICA\打印\客户端打印机 直接连接到打印服务器
打印\客户端打印机 关闭客户端打印机映射	DisableClientPrinterMapping	ICA\打印 客户端打印机重定向

打印\驱动程序 XenDesktop 4 类别和设置 本地打印机驱动程序自动安装	PrintDriverAutoInstall__TurnOn XML 文件	ICA\打印\驱动程序 XenDesktop 7.x 类别和设置 自动安装现成的打印机驱动程序
打印\驱动程序 通用驱动程序	ClientPrintDriverToUse	ICA\打印\驱动程序 通用打印驱动程序使用
打印\会话打印机 会话打印机	NetworkPrinters	ICA\打印 会话打印机
打印\会话打印机 选择客户端的默认打印机	DefaultToMainClientPrinter__NetworkDefault DefaultToMainClientPrinter__TurnOn	ICA\打印 默认打印机

不迁移的内容

此版本不支持所有的 XenDesktop 4 组件。将不迁移以下项目：

- **Virtual Delivery Agent** - 必须先将 VDA 升级到 XenDesktop 5.x 的最低版本，XenDesktop 7.x Delivery Controller 才能从 XenDesktop 4 管理虚拟桌面。有关升级 VDA 的详细信息，请参阅[迁移后需执行的任务](#)。
- **Controller** - 必须部署新的 Controller 服务器。无法将 XenDesktop 4 Controller 升级到 XenDesktop 7.x 站点。XenDesktop 7.x 站点无法加入 XenDesktop 4 场，XenDesktop 4 Controller 无法加入 XenDesktop 7.x 站点。另外，每个版本具有不同的服务器要求；XenDesktop 4 要求 Windows Server 2003；XenDesktop 7.x 要求更高的 Windows Server 版本。
- **Web Interface** - Citrix 建议在 XenDesktop 7.x 中使用 StoreFront。有关安装和设置详细信息，请参阅 StoreFront 文档。当 XenDesktop 安装程序检测到 Web Interface 时，它将安装 StoreFront，但不会删除 Web Interface。
- **Active Directory 组织单位 (OU) 配置** - 不支持在两个场或两个站点之间或者在场与站点之间共享组织单位 (OU)。如果您计划将新站点配置为使用基于 Active Directory 的控制器发现（而非默认的基于注册表的控制器发现），必须创建一个新的 OU，用以对其提供支持。
- **PortICAConfig XML 文件** - 如果更改了此文件的默认设置，可能需要通过组策略对象为新站点配置这些设置。
- 通过 **XenDesktop 4 Service Pack 1** 提供的配置日志记录设置。
- **Provisioning Services** 的相关数据。
- 应用程序。
- **Controller** 列表。
- **NetScaler Gateway**。
- 事件日志限制设置。

安全

May 12, 2016

Citrix XenApp 和 XenDesktop 安全性入门

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/>。

相关内容

- [安全最佳实践和注意事项](#)
- [委派管理](#)
- [智能卡](#)
- [TLS](#)

安全注意事项和最佳做法

Jun 17, 2016

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。

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 Virtual Delivery Agent (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。您可以在创建或更新交付组时配置 SecureICA；请参阅[更改用户设置](#)。

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。

管理用户帐户

如果在安装 Virtual Delivery Agent (VDA) 时选择了用于安装 App-V 发布组件的选项，或者如果在后来添加了此功能，则会将本地管理帐户 CtxAppVCOMAdmin 添加到 VDA。如果您在使用 App-V 发布功能，请不要修改该帐户。如果不需要使用 App-V 发布功能，请不要在安装时选择它。如果您在以后决定不使用 App-V 发布功能，则可以禁用或删除该帐户。

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以下几点：

- 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[更改用户设置](#)。
- 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。

管理登录权限

请仅授予用户所需的登录权限。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、以批处理作业方式登录以及以服务方式登录。

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 组策略配置组的成员身份。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 installation creates the following Windows services:

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService): Manages Microsoft Active Directory computer accounts

for VMs.

- Citrix Analytics (NT SERVICE\CitrixAnalytics): Collects site configuration usage information for use by Citrix, if this collection been approved by the site administrator. It then submits this information to Citrix, to help improve the product.
- Citrix App Library (NT SERVICE\CitrixAppLibrary): Supports management and provisioning of AppDisks, AppDNA integration, and management of App-V.
- Citrix Broker Service (NT SERVICE\CitrixBrokerService): Selects the virtual desktops or applications that are available to users.
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging): Records all configuration changes and other state changes made by administrators to the site.
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService): Site-wide repository for shared configuration.
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin): Manages the permissions granted to administrators.
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest): Manages self-tests of the other Delivery Controller services.
- Citrix Host Service (NT SERVICE\CitrixHostService): Stores information about the hypervisor infrastructures used in a XenApp or XenDesktop deployment, and also offers functionality used by the console to enumerate resources in a hypervisor pool.
- Citrix Machine Creation Service (NT SERVICE\CitrixMachineCreationService): Orchestrates the creation of desktop VMs.
- Citrix Monitor Service (NT SERVICE\CitrixMonitor): Collects metrics for XenApp or XenDesktop, stores historical information, and provides a query interface for troubleshooting and reporting tools.
- Citrix Storefront Service (NT SERVICE\CitrixStorefront): Supports management of StoreFront. (It is not part of the StoreFront component itself.)
- Citrix Storefront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService): Supports privileged management operations of StoreFront. (It is not part of the StoreFront component itself.)

Delivery Controller installation also creates the following Windows services. These are also created when installed with other Citrix components:

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc): Supports the collection of diagnostic information for use by Citrix Support.
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService): Collects diagnostic information for analysis by Citrix, such that the analysis results and recommendations can be viewed by administrators to help diagnose issues with the site.

Except for the Citrix Storefront Privileged Administration Service, these services are granted the logon right Log on as a service and the privileges Adjust memory quotas for a process, Generate security audits, and Replace a process level token. 您不需要更改这些用户权限。 These privileges are not used by the Delivery Controller and are automatically disabled.

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 服务均配置为以 NETWORK SERVICE 身份登录。 Do not alter these service settings.

The Citrix Storefront Privileged Administration service is configured to log on Local System (NT AUTHORITY\SYSTEM). This is required for Delivery Controller StoreFront operations that are not normally available to services (including creating Microsoft IIS sites). Do not alter its service settings.

The Citrix Telemetry Service is configured to log on as its own service-specific identity.

You can disable the Citrix Telemetry Service. Apart from this service, and services that are already disabled, do not disable any other of these Delivery Controller Windows services.

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他们之间共享的桌面（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。

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。

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。

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`

重新启动物理办公室 PC。

委派管理

Mar 17, 2016

“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	可以执行全部任务和操作。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以及全局信息，但无法更改任何内容。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，并可以管理与这些组关联的会话和计算机。可以查看所监控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；还可以管理关联的会话，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）管理应用程序和桌面以及桌面操作系统（Windows 7 或 Windows 8）。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，但无法编辑或删除对象。
- 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，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。

- 对于小规模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，将每个管理员均创建为具有内置“完全权限管理员”角色，该角色拥有“全部”作用域。
- 在包含更多计算机、应用程序和桌面的较大规模部署中，需要更多委派。多个管理员的职责（角色）划分可能更为明确。例如，设置两个完全权限管理员，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），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。
- 更大规模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创建每个管理员以及现有和新的作用域。

为实现配置灵活性和方便性，可以在创建管理员时创建新的作用域。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。

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”。站点创建完成之后，本地管理员不具有任何特殊权限。

完全权限管理员角色始终具有“全部”范围，此范围无法更改。

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/范围时，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。

要管理管理员，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 Create new Administrator（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，新管理员处于启用状态；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，新管理员处于启用状态；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。

无法编辑或删除内置角色。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”窗格中没有相关项。

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对象类型和角色的相关权限。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。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、桌面和会话不会直接归入作用域；管理员可通过相关的计算机目录或交付组分配对这些对象的权限。

作用域名称最多可以包含 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。

在复制或编辑作用域时，请记住，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（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，销售团队使用的各个交付组）。
- 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/作用域以及对每种对象类型（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] [<通用参数>]
```

参数	说明
-Help	显示脚本帮助。
-Csv	指定 CSV 输出。默认值：HTML
-Path <字符串>	输出的写入位置。默认值：stdout
-AdminAddress <字符串>	要连接的 Delivery Controller 的 IP 地址或主机名。默认名称为 localhost
-Show	（仅当指定了 -Path 参数时此参数才有效）将输出写入到文件时，-Show 会在相应的程序中打开此输出，例如 Web 浏览器。
<通用参数>	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 表写入到名为 Roles.csv 的文件。未显示此表。
 & "\$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"

智能卡

Mar 17, 2016

支持依照此处所述的指导原则来实现智能卡身份验证。

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，就应该重新输入 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>。

您的组织可能具有有关智能卡使用的特定安全策略。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。

您可以使用卡管理系统或供应商实用程序重置 PIN。

智能卡支持还涉及 Citrix 合作伙伴提供的组件。这些组件由合作伙伴独立更新，这些文档不提供相关信息。有关详细信息，请参阅 <http://www.citrix.com/ready/> 上的 Citrix Ready 计划。

读卡器支持：

- 支持符合 USB 芯片/智能卡接口设备 (CCID) 规范的 ZKA (Zentraler Kredit Ausschuss 或 Central Credit Committee) 1 类接触式读卡器。这些读卡器包含用户可插入智能卡的插槽或刷槽。不支持包括 2 类（具有用于输入 PIN 的键盘的读卡器）在内的其他类和非接触式读卡器。
- 运行 Receiver for Windows 4.3 和 Windows 10 或 8 的用户设备支持虚拟智能卡（基于 Microsoft Windows 可信平台模块的虚拟智能卡）。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 Microsoft Windows TechCenter 中的 [Virtual Smart Card Overview](#)（虚拟智能卡概述）。
- 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 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。

Important

首先安装驱动程序和 CSP 软件，再在其上安装任何 Citrix 软件。

- Citrix 建议首先在物理机上安装和测试驱动程序，然后再安装 Citrix 软件。
- 对于通过支持并使用微型驱动程序模型的智能卡运行 Windows 7 的虚拟桌面，智能卡微型驱动程序应该会自动下载，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。

通过智能卡实现 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：
 - Gemalto .NET v2+ 及 Gemalto .Net 微型驱动程序
 - NIST PIV 卡及 ActivIdentity ActivClient 6.2
 - NIST PIV 卡及 Microsoft 微型驱动程序
 - CAC 卡及 ActivIdentity ActivClient 6.2
 - 虚拟智能卡及 Microsoft 本机驱动程序

用户设备必须运行 Citrix Receiver、相应的中间件和以下操作系统之一：Windows 7 或 Windows 8（包括 Embedded Edition）32 位和 64 位版本。

中间件：

- Receiver 对智能卡的支持基于 Microsoft 个人计算机/智能卡 (Microsoft Personal Computer/Smart Card, PC/SC) 标准规范。智能卡和智能卡设备必须受底层 Windows 操作系统支持，且必须获得 Microsoft Windows Hardware Quality Labs (WHQL) 批准，可用于运行合格 Windows 操作系统的计算机，此为最低要求。有关硬件 PC/SC 合规性的其他信息，请参阅 Microsoft 文档。
- 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/zh>。

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)

部署智能卡之前：

- 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。
- 配置组件以使用 TLS 1.0 进行智能卡登录。
- 确保您的部署符合与智能卡结合使用的其他 Citrix 组件（包括 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
 - Virtual Delivery Agent
 - （对于远程访问可选）：Microsoft Exchange Server
- 您应该熟悉一般的智能卡技术和您所选的特定技术以及 SDK。还应该了解如何在分布式环境中安装和维护证书。

1. 启用产品对智能卡的使用。
 1. 根据卡颁发策略向用户颁发智能卡。
 2. (可选) 设置智能卡, 以便为用户启用 Remote PC Access。
 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功能。
2. 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](#)
。
3. 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](#)
。
4. 启用 Virtual Delivery Agent (VDA) 以使用智能卡。
 1. 确保 Virtual Delivery Agent 具有必需的应用程序和更新。
 2. 安装中间件。
 3. 设置智能卡远程连接功能, 在用户设备上的 Receiver 与虚拟桌面会话之间启用智能卡数据的通信。
5. 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](#)
。
 1. 将证书颁发机构根证书和证书颁发机构证书导入到设备的密钥库中。
 2. 安装供应商的加密中间件。
 3. 安装并配置 Receiver for Windows, 确保使用组策略管理控制台导入 icaclient.adm 并启用智能卡身份验证。
6. 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 Receiver 访问桌面) 。

智能卡部署

Mar 17, 2016

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
加入域的本地计算机	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。

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），此功能会很有帮助。

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。如果您配置了双模式身份验证，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 and 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。

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）。

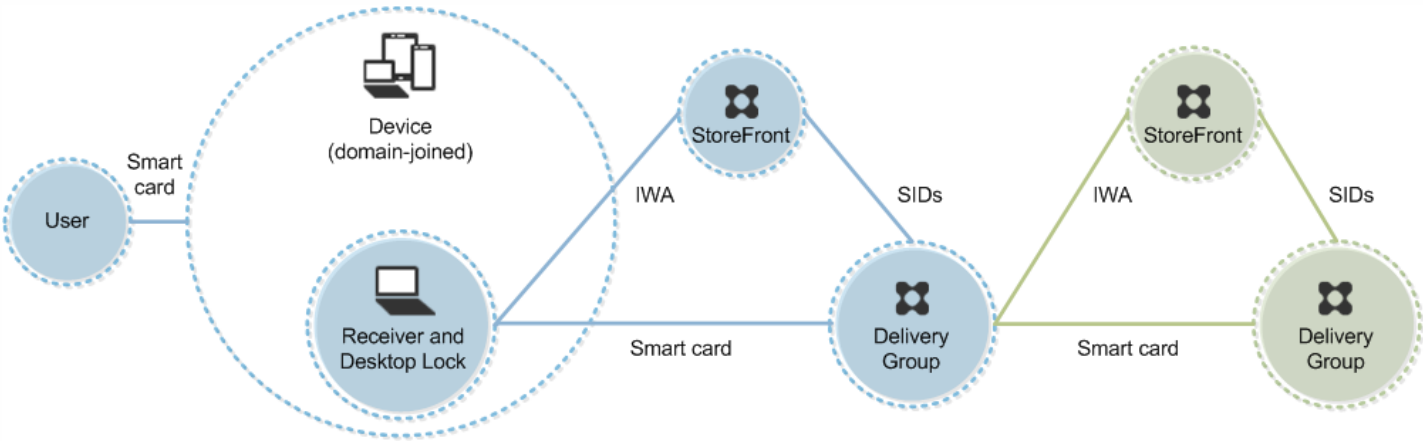
您可以在包括远程桌面的 Citrix 环境中使用智能卡。可以在本地（在智能卡连接的用户设备上）或远程（在用户设备连接的远程桌面上）安装此功能。

在产品上设置的智能卡删除策略用于确定当在会话期间从读卡器中删除智能卡时所发生的操作。智能卡删除策略通过 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
不采取任何措施	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，则此会话可能会注销，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。

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。

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。

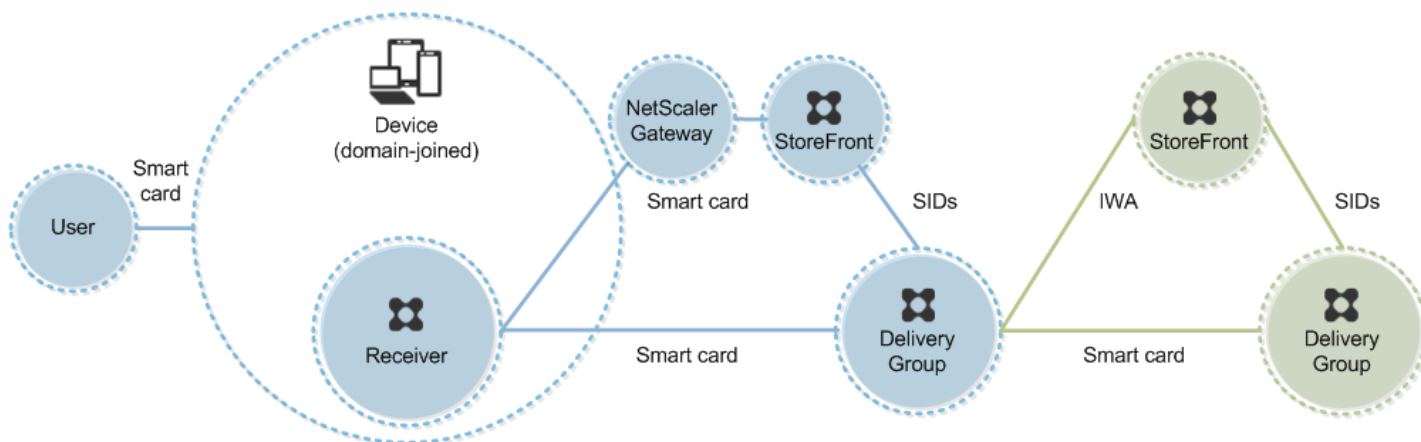


用户使用智能卡和 PIN 登录设备。Receiver 使用集成 Windows 身份验证 (IWA) 向 StoreFront 服务器进行用户身份验证。StoreFront 将用户安全标识符 (SID) 传递到 XenApp 或 XenDesktop。当用户启动虚拟桌面或应用程序时，系统不会提示用户重新输入 PIN，因为 Receiver 上已配置单点登录功能。

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

新使用，或仅能在第二个跃点中使用。

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。

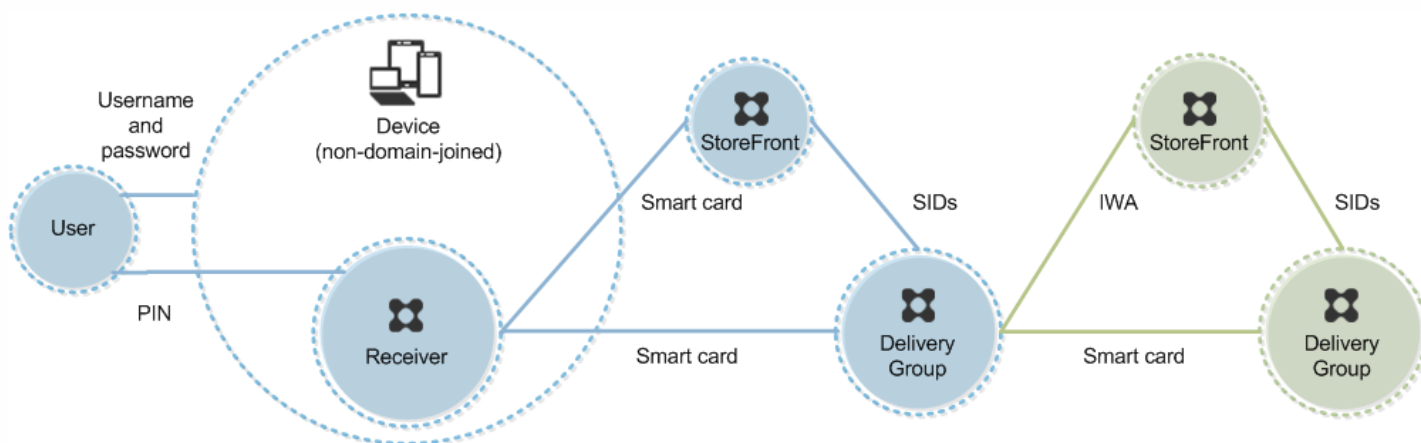


用户使用智能卡和 PIN 登录设备，然后重新登录到 NetScaler Gateway/Access Gateway。第二次登录可以使用智能卡和 PIN，也可以使用用户名和密码，因为在此部署中 Receiver 允许双模式身份验证。

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。虚拟桌面的 Receiverd 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新使用，或仅能在第二个跃点中使用。

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。

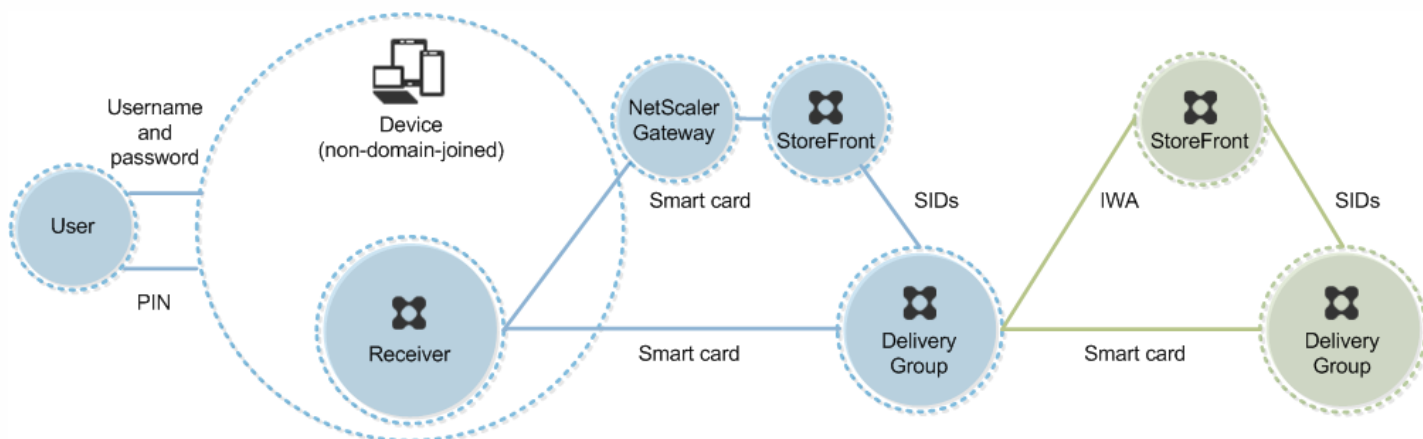


用户登录设备。通常情况下，用户需要输入用户名和密码，但由于此设备未加入域，因此此登录的凭据是可选的。因为在此部署中可使用双模式身份验证，因此 Receiver 会提示用户输入智能卡和 PIN，或使用用户名和密码。然后 Receiver 对 StoreFront 进行身份验证。

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新使用，或仅能在第二个跃点中使用。

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。



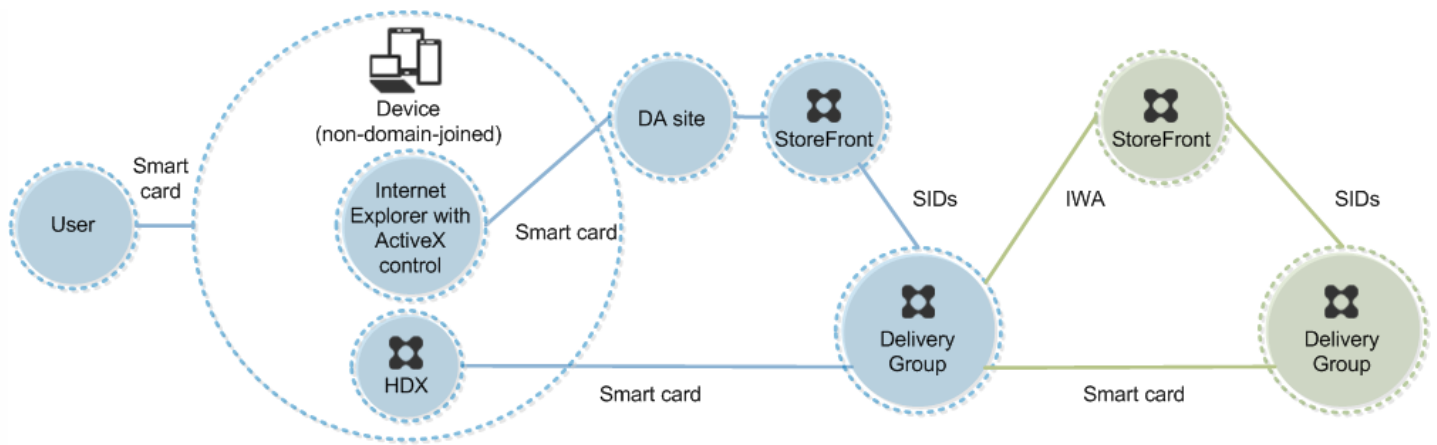
用户登录设备。通常情况下，用户需要输入用户名和密码，但由于此设备未加入域，因此此登录的凭据是可选的。因为在此部署中可使用双模式身份验证，因此 Receiver 会提示用户输入智能卡和 PIN，或使用用户名和密码。然后 Receiver 对 StoreFront 进行身份验证。

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新使用，或仅能在第二个跃点中使用。

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。

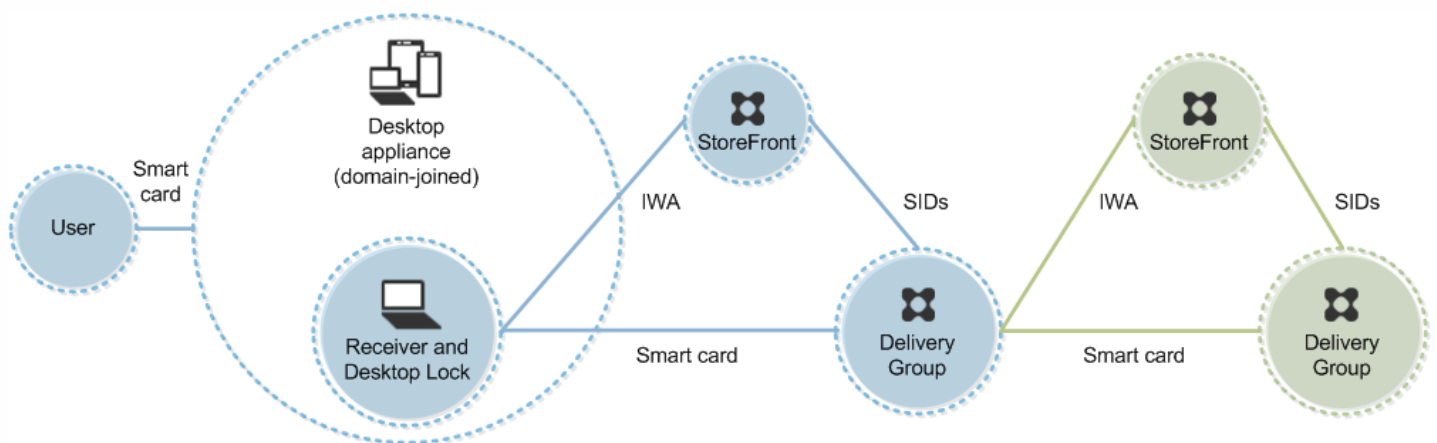


用户使用智能卡登录设备。如果 Desktop Lock 正在设备上运行，该设备配置为通过在 Kiosk 模式下运行的 Internet Explorer 启动桌面设备站点。该站点上的 ActiveX 控件会提示用户输入 PIN，然后将其发送到 StoreFront。StoreFront 将用户安全标识符 (SID) 传递到 XenApp 或 XenDesktop。分配的桌面组列表（按字母顺序）中的第一个可用桌面将启动。

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。虚拟桌面的 Receiverd 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新使用，或仅能在第二个跃点中使用。

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。虚拟桌面的 Receiverd 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新使用，或仅能在第二个跃点中使用。

使用智能卡进行直通身份验证和单点登录

Mar 17, 2016

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 2008 和 Windows Server 2012 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。请参阅 StoreFront 文档中的

— [配置身份验证服务](#)

以了解详细信息。

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。您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。

传输层安全性 (TLS)

Jun 17, 2016

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 SSL 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 SSL。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，计算机映像会在每次重新启动时重置。

对于包括使用 Windows 注册表的任务：

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。

有关为站点数据库启用 TLS 的信息，请参阅 [CTX137556](#)。

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 SSL 证书配置端口，请遵循以下操作：

- 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> 中所述获得 SSL 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\(W5.10\).aspx](http://technet.microsoft.com/en-us/library/cc736326(W5.10).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 SSL 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>。

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 端口> -WISSLPOROT <https 端口>

其中，<http 端口> 是用于 HTTP 流量的端口号，<https 端口> 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

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\ 中设置以下注册表值，然后重新启动 Broker Service。

要忽略 HTTP 流量，请将 XmlServicesEnableNonSsl 设置为 0。

提供了一个用于忽略 HTTPS 流量的相应注册表值：XmlServicesEnableSsl。请确保未将其设置为 0。

在 VDA 上配置 TLS 时，会更改已安装 SSL 证书上的权限，向 ICA Service 授予证书私钥的读取权限，并将以下信息告知 ICA Service：

- 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](#)。

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。
密码集是常用 TLS 密码的列表。客户端连接并发送受支持的 TLS 密码列表时，VDA 将客户端的其中一个密码与其已配置密码集中的其中一个密码相匹配并接受连接。如果客户端发送的密码不在 VDA 的密码集中，VDA 将拒绝连接。

支持三种密码集：GOV(ernment)、COM(mercial) 和 ALL。这些密码集中的密码取决于 Windows FIPS 模式；有关 Windows FIPS 模式的信息，请参阅 <http://support.microsoft.com/kb/811833>。下表列出了受支持的每种密码集中的密码。

TLS 密码集	GOV	COM	ALL	GOV	COM	ALL
FIPS 模式	关	关	关	开	开	开
RSA_KEYX	x	x	x	x	x	x
RSA_SIGN	x	x	x	x	x	x
3DES	x		x	x		x
RC4		x	x			
MD5	x	x	x			
SHA	x	x	x	x	x	x
SHA_256	x	x	x	x	x	x
SHA_384	x	x	x	x	x	x
SHA_512	x	x	x	x	x	x
AES	x	x	x	x	x	x

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，应该已经为此交付组中的所有 VDA 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。它还以下为各项禁用 Windows 防火墙规则：

- Citrix ICA（默认：1494）
- Citrix CGP（默认：2598）
- Citrix WebSocket（默认：8008）

结果，用户仅可以通过 TLS 连接，而不能使用原始 ICA、CGP 或 WebSocket 进行连接。

此脚本包含以下语法描述以及其他示例；您可以使用 Notepad++ 等工具查看此信息。

必须指定 -Enable 或 -Disable 参数；其他所有参数为可选参数。

语法

Enable-VdaSSL {-Enable | -Disable} [-SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite "<suite>"] [-CertificateThumbPrint "<thumbprint>"]

参数	说明
-Enable	在 VDA 上安装并启用 TLS 侦听器。必须带此参数或 -Disable 参数。
-Disable	在 VDA 上禁用 TLS 侦听器。必须带此参数或 -Enable 参数。如果指定此参数，其他参数均无效。
-SSLPort <端口>	TLS 端口。默认值：443
-SSLMinVersion "<最低 ssl 版本>"	最低 TLS 协议版本，两边用引号括起来。有效值："SSL_3.0"、"TLS_1.0"、"TLS_1.1" 和 "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 "<密码集>"	TLS 密码集，两边用引号括起来。有效值："GOV"、"COM" 和 "ALL"。默认值："ALL"
-CertificateThumbPrint "<指纹>"	证书存储中 SSL 证书的指纹，两边用引号括起来。通常在证书存储中包含多个证书时使用此参数；脚本使用指纹来选择要使用的证书。默认值：在证书存储区域的“本地计算机”>“个人”>“证书”区域找到的第一个可用证书。

示例

以下脚本安装并启用 TLS 1.2 协议版本值。
Enable-VdaSSL -Enable
以下脚本安装并启用 TLS 侦听器，指定 TLS 端口 400、GOV 密码集和最低 TLS 1.2 SSL 协议值。
Enable-VdaSSL -Enable -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 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：

1. 启动 Microsoft 管理控制台 (MMC)：“开始”>“运行”> mmc.exe。
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。
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。
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 SSL 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”
5. 双击已安装的 SSL 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。
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 SSL 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)。
 - SSLCipherSuite DWORD – 1 = GOV、2 = COM、3 = ALL。默认值：3 (ALL)。
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）。
8. 确保没有其他应用程序或服务（如 IIS）正在使用 TLS TCP 端口。
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）。

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 '<交付组名称>' | Set-BrokerAccessPolicyRule -HdxSslEnabled \$true。
其中，<交付组名称> 是包含 VDA 的交付组的名称。
4. 运行 Set-BrokerSite -DnsResolutionEnabled \$true。

如果连接出错，请检查 VDA 的系统事件日志。

使用 Receiver for Windows 时，如果收到指示 TLS 错误的连接错误（如 1030），请禁用 Desktop Viewer，然后尝试重新连接。尽管连接仍会失败，但可能会提供对基本 TLS 问题的解释（例如，在从证书颁发机构申请证书时指定了错误的模板）。

打印

Apr 25, 2016

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：

- **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。

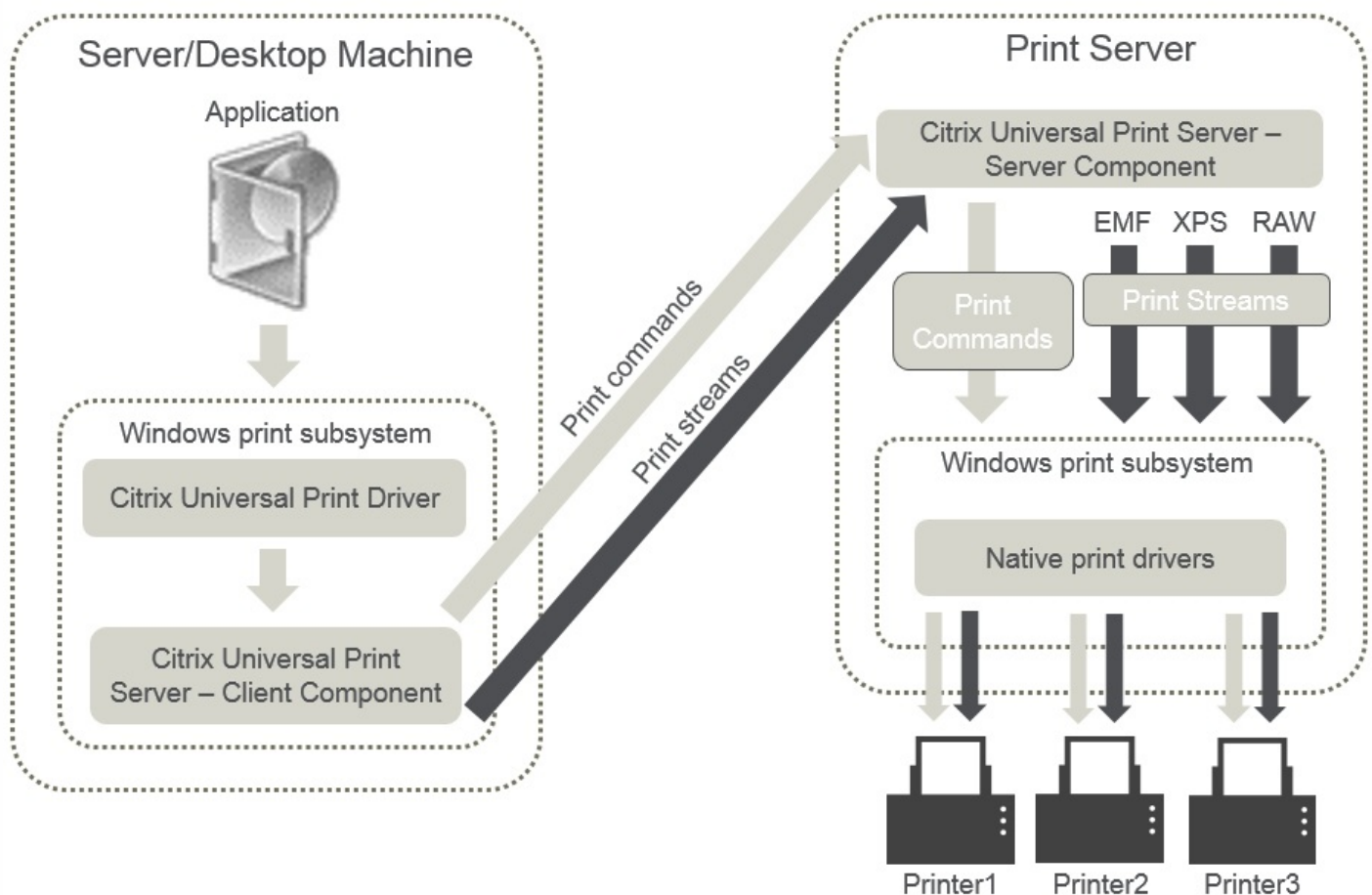
Citrix 建议针对远程打印服务器的情况使用 Citrix 通用打印服务器。通用打印服务器通过网络以经过优化和压缩的格式传输打印作业，从而最大程度地减少网络使用，并改善用户体验。

通用打印服务器功能包含以下组件：

- 客户端组件（通用打印客户端）- 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（通用打印服务器）- 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。

- **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：

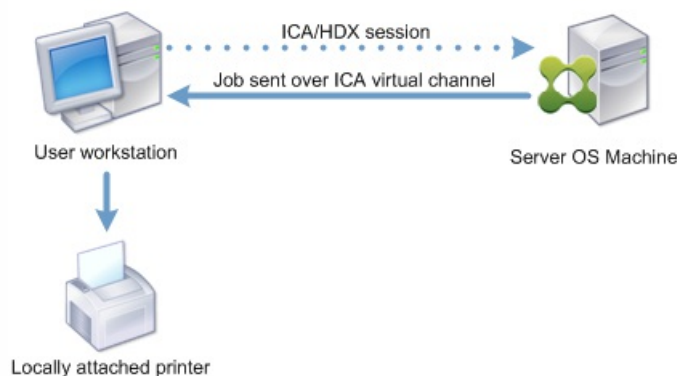
- 更新会话打印机策略设置。
- 使用“打印机驱动程序映射和兼容性”策略设置向所有服务器操作系统计算机添加驱动程序。

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。



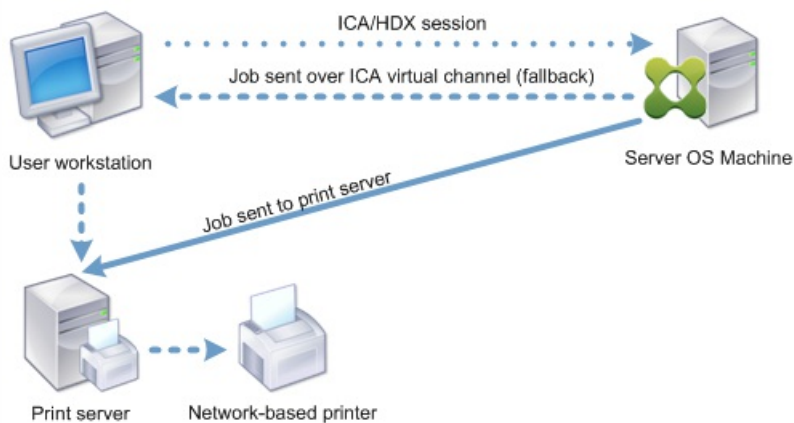
基于网络的打印机

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。

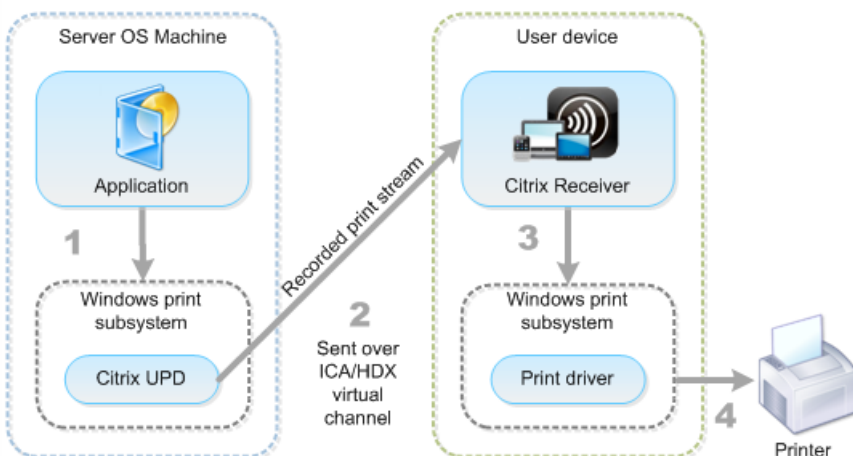
如果未启用通用打印服务器，配置面向网络打印的客户端打印途径对低带宽连接（例如广域网）非常有用，这是因为通过 ICA 连接发送作业时会进行流量优化和压缩。

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。



为简化此环境中的打印，Citrix 建议使用 Citrix 通用打印驱动程序。通用打印驱动程序是一种独立于设备的驱动程序，支持任何打印设备，它使得所需驱动程序的数量得以减少，从而简化了管理。

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。

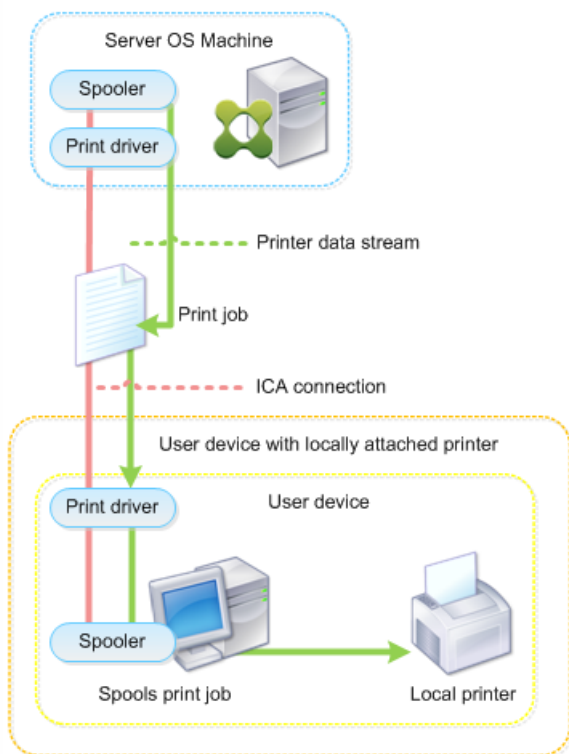


规划驱动程序管理策略时，请确定支持的驱动程序类型：通用打印驱动程序、设备特定的驱动程序或者两者。如果支持标准驱动程序，您需要确定：

- 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。
- 是否要创建驱动程序兼容性列表。

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。



- 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

打印配置示例

Mar 17, 2016

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。

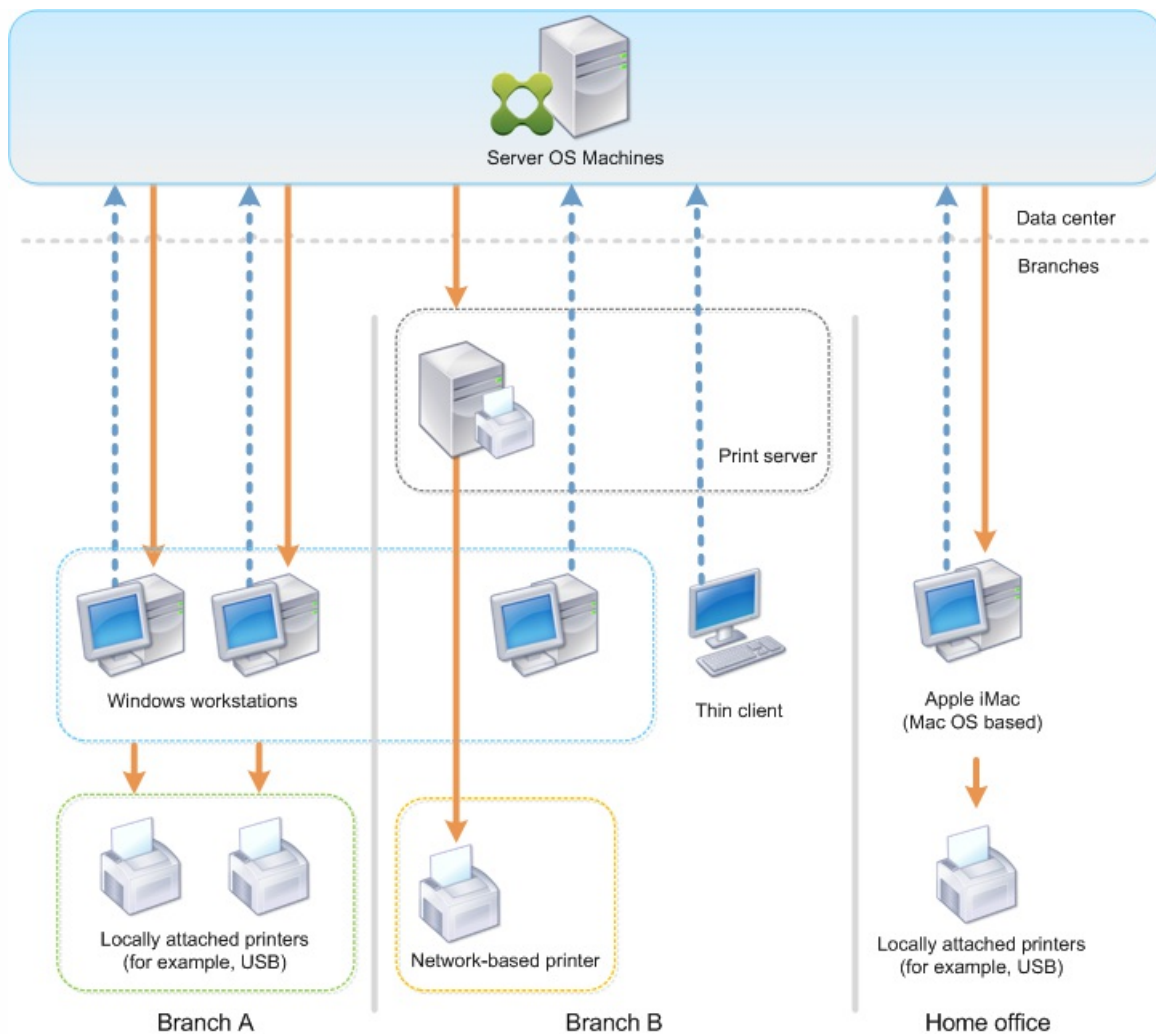
打印配置取决于：

- 业务需求以及现有的打印基础设施。
应根据您公司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。



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 low 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，而无需在数据中心的集成新打印机驱动程序。

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。

最佳做法、安全注意事项和默认操作

Mar 17, 2016

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

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传到 Citrix Insight Services，请使用 **Start-TelemetryUpload** PowerShell cmdlet。

打印策略和首选项

Apr 25, 2016

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：

- 如何设置打印机（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设置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：

- 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。

置备打印机

Apr 25, 2016

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[使用图形界面进行安装](#)和[使用命令行进行安装](#)。

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. 根据命令行说明提取 VDA，如[使用独立的 VDA 安装程序](#)中所述。
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 中安装 cdf pre-requisite。
 - 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。

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）。

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。
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

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 记录直接后台处理到打印机中。借助直接后台处理到打印机中的方式，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。

您可以按要提供邻近打印的 IP 地址过滤会话打印机策略。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，并且不需要进行本部分所述的配置。

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。

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：
 - 网络打印机名称。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。

维护打印环境

Mar 17, 2016

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，标准质量处于启用状态，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，超级压缩功能处于禁用状态。
- 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、击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。

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

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）	打印途径	是否启用了 UAC ？	Windows 8 : 打印管理管理单元位置
	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。

HDX

Mar 17, 2016

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 MediaStream 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。通过工作区控制功能，用户可以暂停虚拟桌面和应用程序，然后使用其他设备从上次暂停的位置开始继续工作。
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 功能可适应环境变化，通过为每种独特的用户实际情况应用最佳技术来平衡性能和带宽，而不管用户是从企业网络本地访问桌面或应用程序，还是从公司防火墙外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，而无论客户端设备的能力如何。将压缩的多媒体信息以其原有格式直接发送给用户设备。 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 是 EdgeSight Network Inspector 和 EdgeSight Performance Management 与 Director 的集成，可捕获有关 ICA 通信的数据，并提供“控制板”视图来显示实时信息及历史详情，如客户端和服务器端 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 HDX 是如何向虚拟桌面交付丰富的视频内容的：请观看含有高清视频的 Web 站点上的视频，例如 <http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/>。
- 了解 Flash 重定向功能如何加速交付 Flash 多媒体内容：
 - 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。
 - 在 Desktop Viewer 工具栏上，单击首选项。在 Desktop Viewer 首选项对话框中，单击 Flash 选项卡并选择优化内容。
 - 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（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。但可以通过观察在 Flash 播放器启动前短暂显示的一个色块，来确认是否在使用 Flash 重定向。
- 了解 HDX 如何交付高清晰度音频：
 - 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。
 - 在桌面上使用数字音频播放器（如 iTunes）播放音乐文件。

默认情况下，对于大多数用户来说，无需执行任何配置即可从 HDX 获得卓越的图形和视频体验。Citrix 策略设置在大多数情况下均可提供最佳的开箱即用体验，默认情况下，会启用这些策略。

- 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。
- HDX 可向任何客户端上的虚拟桌面用户提供 Windows Aero 体验。
- 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。如果此客户端内容提取功能所需的条件无法得到满足，媒体交付将由 Windows Media 重定向功能执行，将在用户设备而不是在主机服务器上播放媒体运行时文件。在大多数情况下，无需调整 Windows Media 功能策略。

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，请参阅适用于本版本的
— Citrix 策略
文档。
- 有关在注册表中操作的说明，请采用以下注意事项：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。

默认情况下，HDX 将向通过受支持的 Windows 用户设备访问的虚拟桌面提供高响应度的 Windows Aero 或 Windows 8 桌面体验。为此，HDX 将使用用户设备上的图形处理器 (GPU) 或集成图形处理器 (IGP) 实现本地的 DirectX 图形呈现。此功能称为桌面组合重定向，可在服务器上保持高可扩展性。有关详细信息，请参阅 <http://blogs.citrix.com/20106-3-11/go-supersonic-with-xendesktop-7-x-bandwidth-supercodecs/> 上的“What to do with all these choices”（如何使用这些选项）部分。

为了降低用户会话中所需的带宽，可考虑调整以下 Citrix 策略设置。请记住，更改这些设置可能会降低用户体验的质量。

- **桌面组合重定向。** 仅适用于通过 Windows 用户设备访问的 Windows 桌面操作系统计算机，并且仅适用于 Windows 桌面组合。将在服务器上呈现应用程序窗口，除非将 Citrix 策略设置允许本地应用程序访问配置为“允许”。
- **桌面组合重定向图形质量。** 对桌面组合使用高质量图形，除非已启用无缝应用程序或本地应用程序访问功能。要降低带宽需求，应降低图形质量。
- **动态窗口预览。** 控制以窗口切换、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。要降低带宽需求，应禁用此策略设置。

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）。
- **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）。在许多情况下，可以通过指定更大的值来改善用户体验。对于 CPU 速度较慢的设备，指定较低的值可以改善用户体验。
- **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。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 网络摄像机视频压缩可提高在会话中的视频会议过程中的带宽效率和延迟容忍度。此技术通过一个专用的多媒体虚拟通道使用流技术推送网络摄像机通信；相比常时等量 HDX Plug-n-Play 支持，可大幅减少带宽占用，并可以通过 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。

默认情况下，Citrix Receiver for Windows 上已经启用 HDX 网络摄像机视频压缩功能，但在 Citrix Receiver for Linux 上必须进行相应配置。有关详细信息，请参阅 Citrix Receiver 文档。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。硬件编码将使用额外的带宽，因此不适用于低带宽网络。要强制在低带宽网络上执行软件压缩，请向注册表项 HKCU\Software\Citrix\HdxRealTime 添加以下 DWORD 键值：DeepCompress_ForceSWEncode=1。

对于服务器可扩展性优先级高于用户体验的部署情况，可以使用旧的图形系统，方法是添加旧图形模式策略设置，并配置各个旧版图形策略设置。使用旧的图形系统会影响通过 WAN 和移动连接进行连接的用户体验。

Thinwire 兼容模式

Mar 17, 2016

Thinwire 兼容模式使用新的屏幕分解和缓存技术，可以实现低带宽占用和高服务器可扩展性，并且不会降低最终用户的体验。

Thinwire 兼容模式包括以下功能：

- 适用于仅位图提供程序的智能位图匹配。
 - 用于有效窗口移动和滚动的位图转换分析。
- 向后兼容。无需进行客户端或 Citrix Receiver 升级或硬件加速。
 - 在大量达到和超过 5 年的旧瘦客户端上进行了测试。
- 通过优化实现了极低的服务器 CPU 使用率并改善了服务器可扩展性。
- 仿真 16 位模式，将典型工作负载的带宽进一步降低了 15-20%。
- 用于服务器端呈现视频内容的暂存检测。
 - 多路暂存处理改善了多媒体体验。例如，观看多个视频或行情显示系统时。
 - 选择性锐化停留在暂存状态的区域。
- 通过优化实现了 CloudBridge 加速。在测试中，我们观察到 Office 类型工作负载的带宽降低率达到 6:1。
- 自适应显示，可以通过策略设置进行调整。有关详细信息，请参阅[移动图像策略设置](#)中的[移动图像压缩](#)。
- 最高可支持 VDA 和 Windows 操作系统的 Windows 10 VDA。
- 用于 3D Pro 的新“设为无损”模式，改善了响应能力、交互能力和可中断锐化，从而在低带宽条件下实现更好的用户体验。
- 默认静态摄影图片质量高于旧图形模式。

对于“视觉质量”设置“低”、“中”（默认）和“高”，暂存检测器动态评估屏幕更新，以确定是否以较低的质量发送高动画区域（与自适应显示策略保持一致），从而改善客户端性能并降低带宽占用。

对于**设为无损**视觉质量，Thinwire 兼容模式为大屏幕更新使用“模糊优先”方法。此设置面向操作 3D 模型或其他图形密集型应用程序的 3D Pro 用户。如果活动继续，则认为进入暂存模式，一旦暂存活动停止，受影响的区域将进行锐化并缓存。对于最初的大型更改，将会对更改区域执行轻型映像分析，以确定是否使用“模糊暂存”或“锐化暂存”（无损），例如，旋转线框时。对于 FPS（每秒的帧数）和带宽，使用 Citrix 无损编解码器编码简单图形更加有效，并且质量不会受损。

“设为无损”中锐化到无损的步骤也有所不同。区域按照预先确定好的块进行锐化，而不是一步完成受影响区域的锐化，这样有助于维护交互性，使用户体验更加流畅。将较大的更改区域锐化为中间暂存（例如，移动瞬间停止的三维模型，然后再次移动）之前会导致形成“隔栏”，这在低带宽线路上尤为明显。这些锐化块的大小取决于为尝试和维护最低目标帧速率而降低质量的程度，即自适应显示策略设置。如果质量显著受损，锐化块将更小，最低大小为 128 x 128 像素。如果质量并未受损，当客户端有足够的处理能力和带宽时，锐化块最大可以达到 384 x 384 像素。

Framehawk 虚拟通道

Apr 25, 2016

简介

在发生严重的数据包丢失或网络拥堵的情况下，Framehawk 虚拟通道可优化向采用宽带无线网络连接和有损远程宽带网络连接的用户交付虚拟桌面和应用程序的操作。您可以采用适合网络特征并符合整体可扩展性和性能预期的方式，使用 Citrix 策略向一系列用户实施 Framehawk 或 Thinwire。

通常，用户体验关注于将帧速率和视觉质量作为实现良好用户体验的基础。Framehawk 增强了线性方面的清晰度。用户需要享受使用过程，不应该被问题分散注意力。在网络状况不佳的情况下，用户需要应对干扰所有协议的“橡皮筋”效应。此效应包括点击-等待-点击现象，即用户不确定屏幕是否会响应，导致单击次数过多，使情况变得越来越糟。Framehawk 会使此类体验变得更流畅，尤其是在网络负载较大的情况下。

家庭高速 Internet 连接经常遇到性能问题，这可能是由于与附近的 Wi-Fi 信号冲突，或者是受到无线设备的频谱干扰或其他原因。越来越多的用户通过 3G 或 4G/LTE 手机数据网络或使用空中 Internet 服务连接到托管应用程序和数据。其他人则喜欢在喝咖啡休息时或在宾馆利用公共 Wi-Fi 热点，在此类情况下，经常会出现网络拥堵问题。

利用 Framehawk，用户体验更具交互性（即用户回显线性更强），但延迟较高。

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？如果屏幕区域变化很快，例如视频或移动图像，则丢失某些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，如系统托盘或工具栏中的图标，或滚动到用户希望开始阅读的位置后显示的文本，人眼是非常挑剔的；用户希望这些区域的像素能够完美呈现出来。与那些旨在从零一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 可以通过插补掩盖丢失，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）。

Framehawk Intent Engine 可以区分向上滚动或向下滚动、缩放、移动到左侧或右侧、读取、键入及其他常见操作，并使用共享字典管理传回 Virtual Delivery Agent (VDA) 的通信。如果用户正在尝试阅读，则需要出色的文本视觉质量。如果用户正在滚动，则需要快速且流畅，并且必须可中断，以使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（我们称之为“传动”，类似于自行车链条的拉伸），Framehawk 逻辑就可以加快反应速度，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，但是它基于 TCP 实现可靠的数据通信，因此必须在丢失时重传数据包或使网络负载过重，从而导致在用户体验方面发展缓慢。

Framehawk 基于 UDP，在数据传输方面采用尽力而为的方法。UDP 只是 Framehawk 克服丢失问题的一小部分，通过与其他基于 UDP 的协议比较 Framehawk 的性能可以看出这一点，但是它为 Framehawk 借以脱颖而出的以人为中心的技术提供了重要基础。

Framehawk 需要多少带宽？

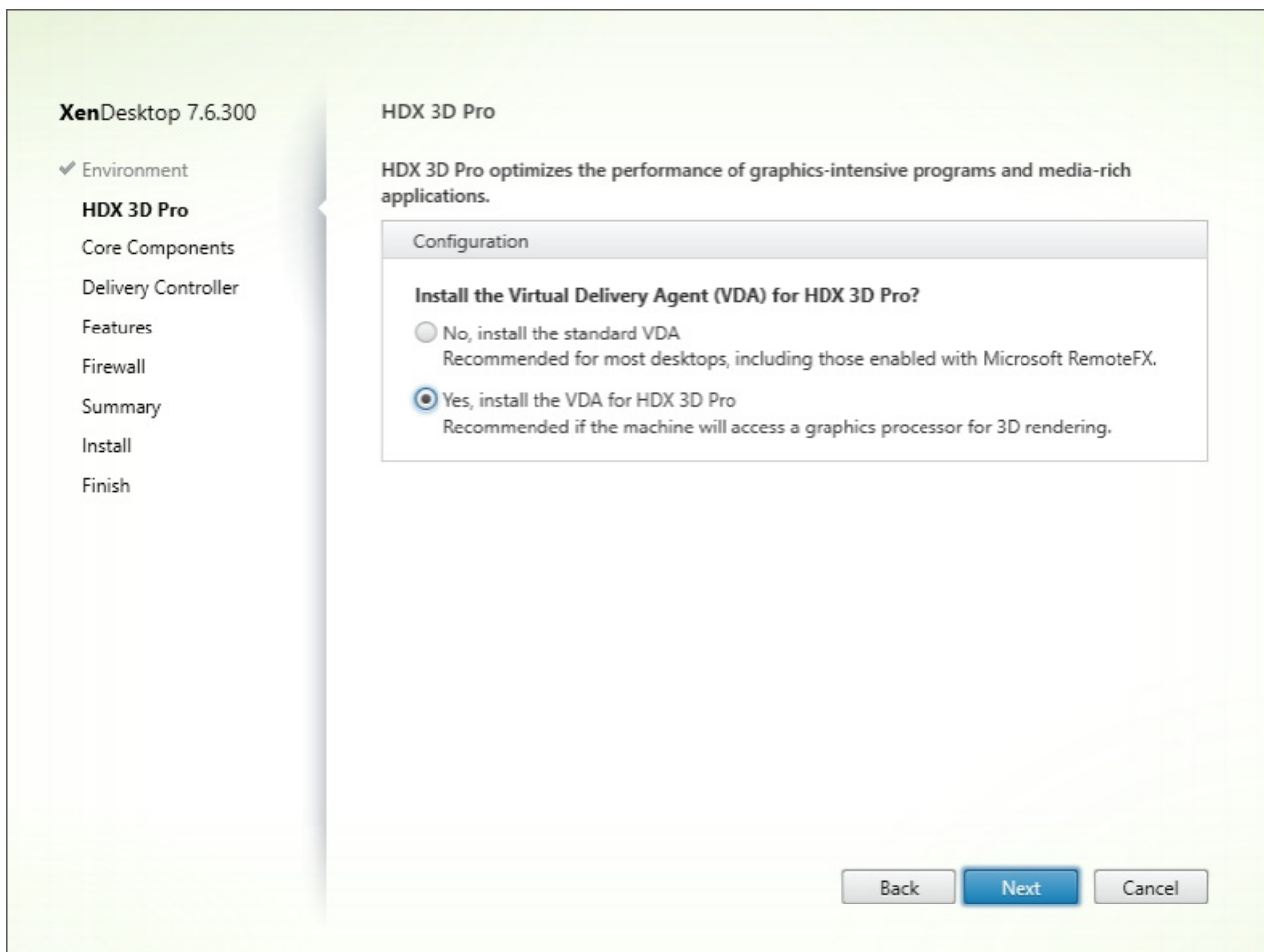
无线带宽的重要性取决于多种因素，其中包括共享连接的用户数量、连接的质量和所使用的应用程序。为实现最佳性能，Citrix 建议 4 或 5 Mbps 以及每个并发用户大约 150 Kbps 的基本设置。

Citrix 为 Thinwire 推荐的带宽一般为基本带宽 1.5 Mbps 加上为每个用户提供的 150 Kbps（有关详细信息，请参阅 XenApp 和 XenDesktop 带宽博客），但是，假定数据包丢失率为 3%，您会发现要维护良好的用户体验，Thinwire 需要的带宽远远高于 Framehawk。

注意：Thinwire 仍是 ICA 协议中主显示器远程处理通道。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。

现在，Framehawk 可支持所有的 HDX 3D Pro 用例，既包括 XenApp（服务器操作系统）应用程序，又包括 XenDesktop（桌面操作系统）应用程序。在早期预览版中，已通过延迟为 400-500 毫秒且数据包丢失率为 1-2% 的客户环境进行了验证，可以使用诸如 AutoCAD、Siemens NX 或其他典型 3D 建模应用程序提供出色的交互能力。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。

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：



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。

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 使用双向 UDP 端口范围 (3224-3324) 与 Citrix Receiver 交换 Framehawk 显示通道数据；该范围可以在策略设置“Framehawk 显示通道端口范围”中自定义。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），需要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。

实现 Framehawk 虚拟通道时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。
- 在很多情况下，NetScaler Gateway 可能会安装在 DMZ 中，在内外两侧均面临防火墙。如果环境要使用默认端口范围，请确保在外部防火墙上打开 UDP 端口 443，并在内部防火墙上打开 UDP 端口 3224-3324。

配置

警告： Citrix 建议仅为经历严重数据包丢失问题的用户启用 Framehawk。建议不要作为站点中所有对象的通用策略启用 Framehawk。

默认情况下，Framehawk 虚拟通道处于禁用状态。启用后，服务器将尝试对用户的图形和输入使用 Framehawk 虚拟通道。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。

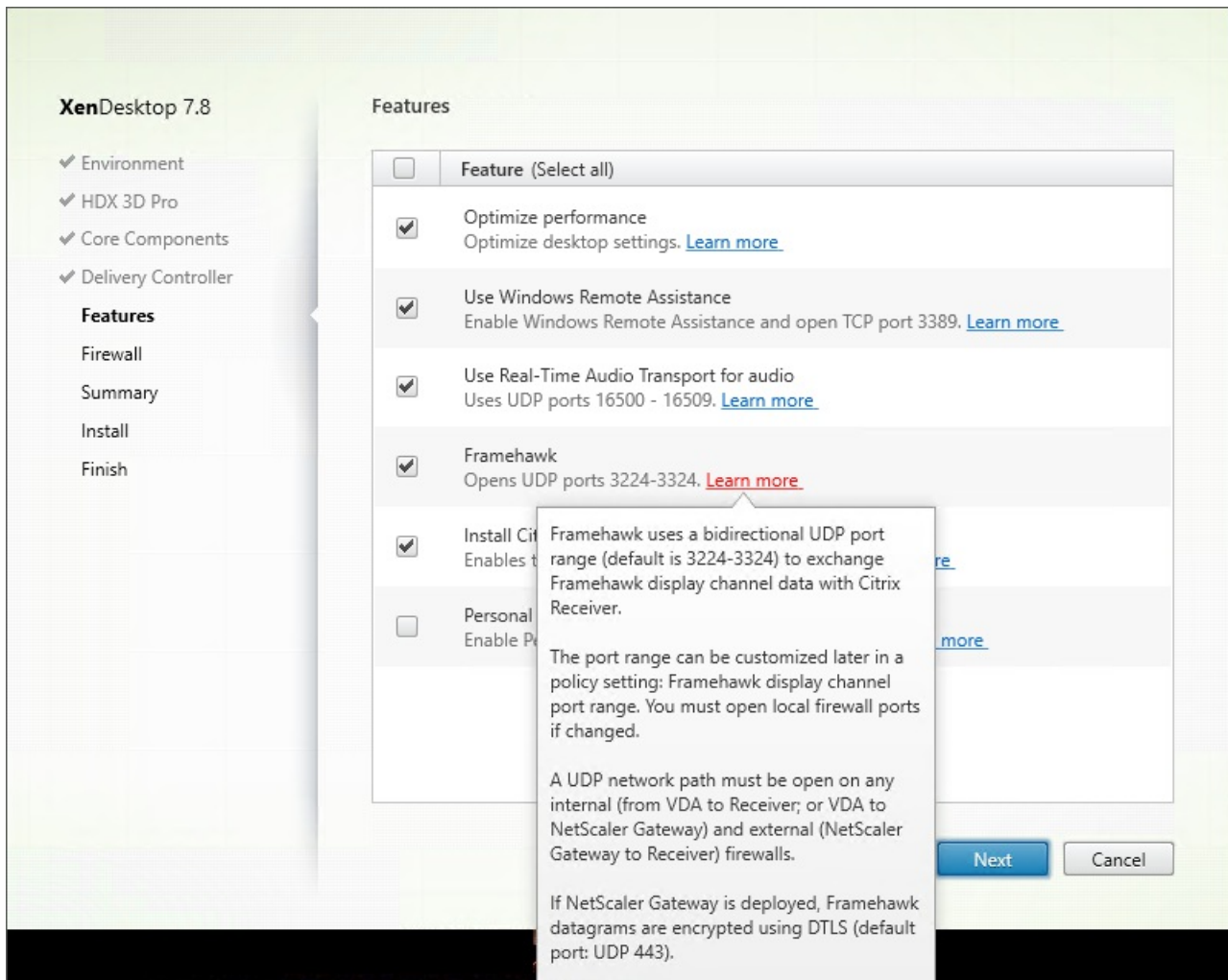
下列策略设置影响 Framehawk：

- **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，后面每次尝试都增加端口号。端口处理入站和出站通信。

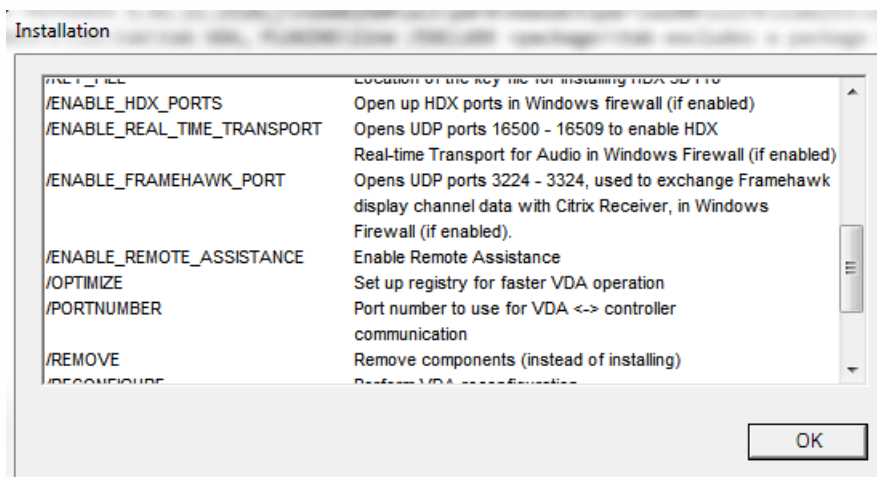
在 7.8 版中，VDA 安装程序的功能步骤提供了一个新选项，可用于重新配置防火墙。如果选中该复选框，则会在 Windows 防火墙中打开 UDP 端口 3224-3324。请注意，在某些情况下需要手动配置防火墙：

- 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：

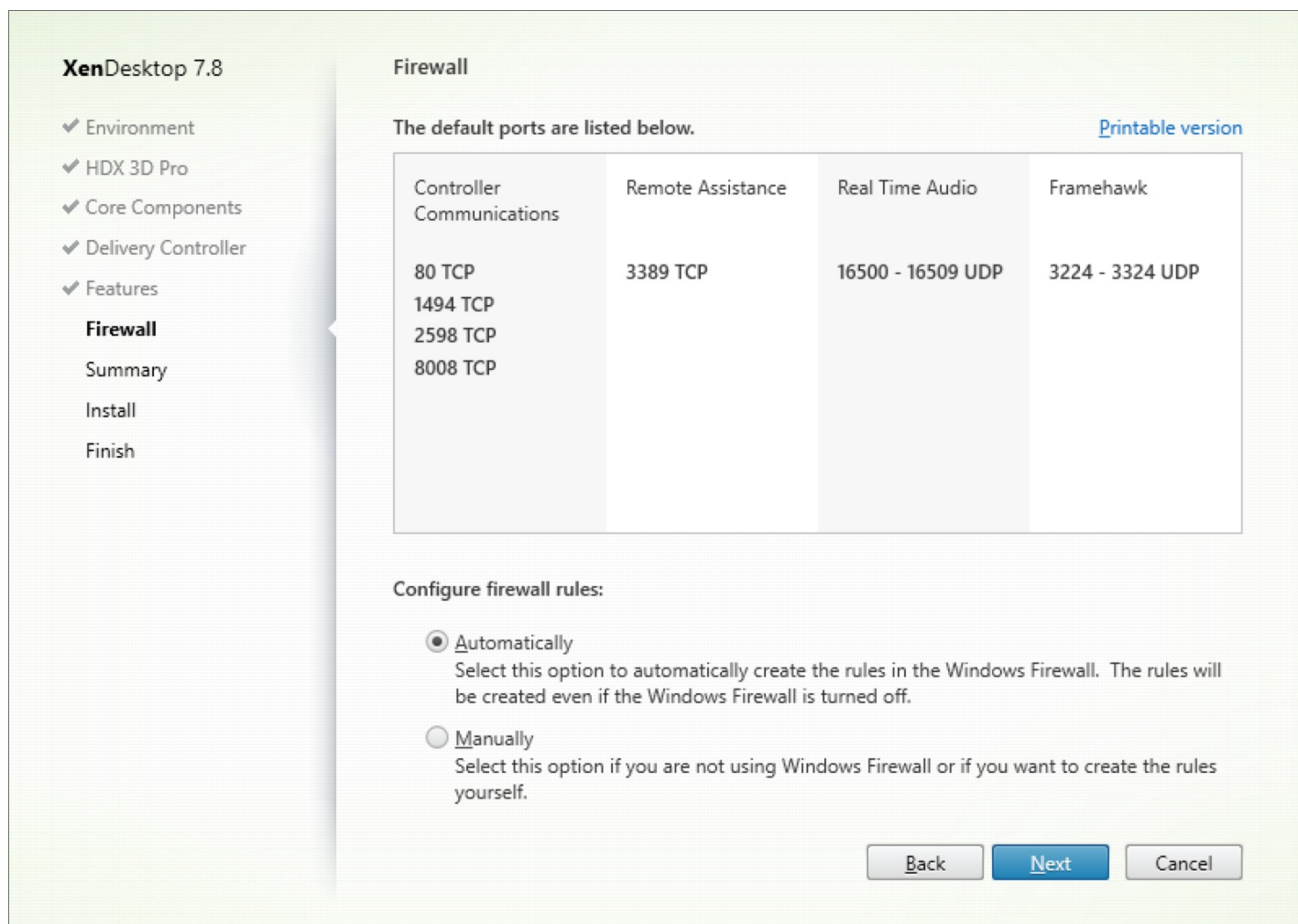


您也可以在命令行中使用 `/ENABLE_FRAMEHAWK_PORT` 打开用于 Framehawk 虚拟通道的 UDP 端口：

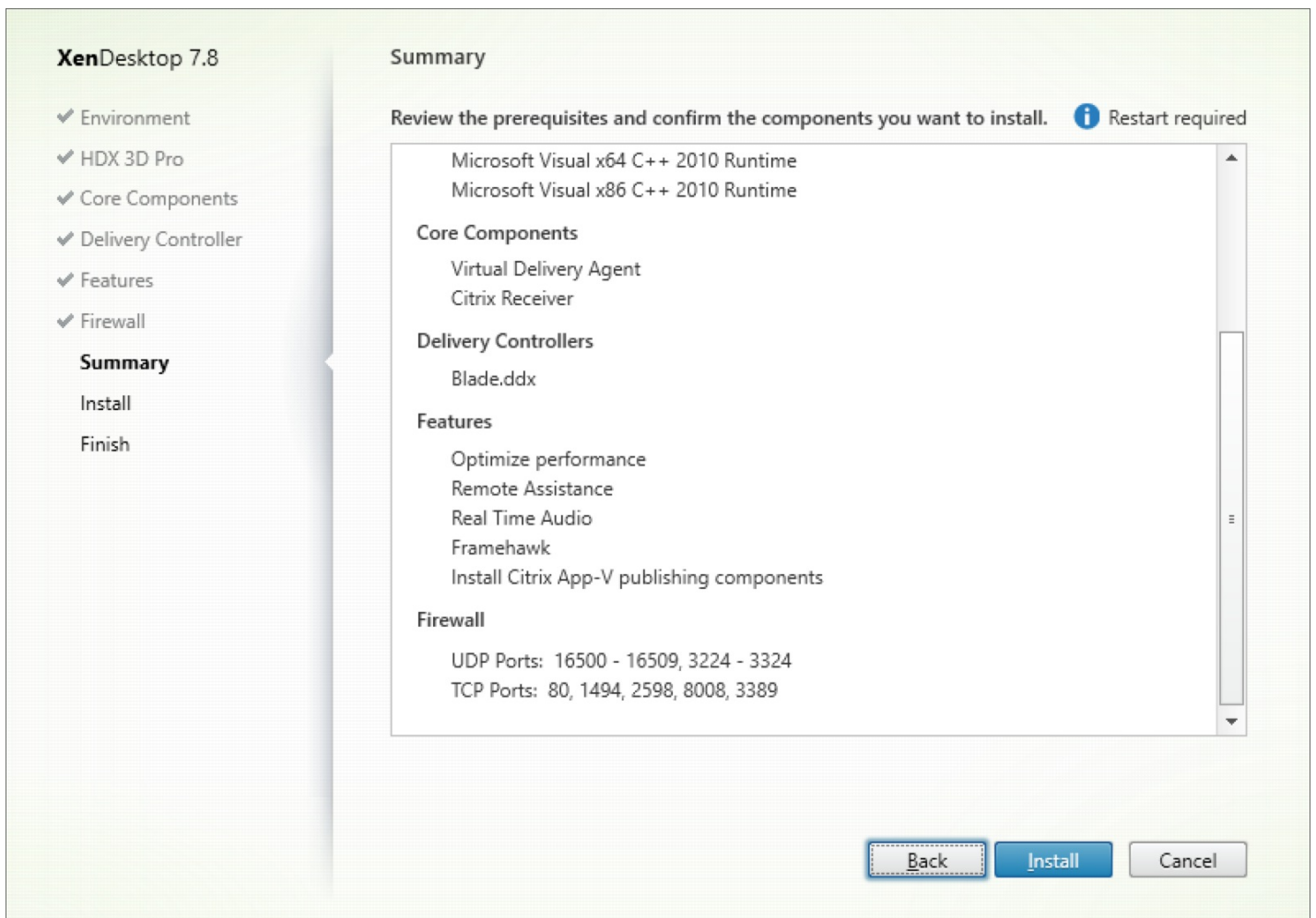


验证 Framehawk UDP 端口分配

安装期间，您可以在防火墙屏幕中验证分配给 Framehawk 虚拟通道的 UDP 端口。



摘要屏幕会指示是否启用了 Framehawk 虚拟通道功能。



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 虚拟服务器的部署体系结构；VPN 虚拟服务器分配有公用 IP 地址，用户直接连接到此 IP。
- 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。在此部署中，CS 虚拟服务器具有公共 IP，Gateway VPN 虚拟服务器具有虚拟 IP。

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
- NetScaler Gateway 上的多个 Secure Ticket Authority (STA)
- 采用高可用性 (HA) 的 NetScaler Gateway
- 采用群集设置的 NetScaler Gateway

方案	Framehawk 支持
NetScaler Gateway	是
NetScaler + 全局服务器负载均衡	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)	否
采用高可用性 (HA) 的 NetScaler Gateway	否
采用群集设置的 NetScaler Gateway	否

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。

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 NetScaler 与 XenApp 和 XenDesktop 服务器之间的所有内部防火墙上都开放了 CGP 端口（默认为 2598）
- 在设置中为 VPN 虚拟服务器启用 DTLS
- 取消绑定并重新绑定 SSL 证书-密钥对；请注意，如果您使用的是 NetScaler 11.0.64.34 或更高版本，则不需要执行此操作。

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）以显示其他配置选项：
5. 选择 **DTLS**，为数据报协议（如 Framehawk）提供通信安全。单击 **OK**（确定）。VPN 虚拟服务器的“Basic Settings”（基本设置）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 早期版本的其他步骤

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. 确保已正确安装和配置 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. 在绑定到用作目标 vServer 的 CS vServer 的 VPN vServer 上启用 DTLS 参数。

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 NetScaler Gateway 的版本不正确，则 Framehawk 策略可能就无法应用。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 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。

此操作允许在 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。

监视 Framehawk

您可以从 Citrix Director 监视 Framehawk 的使用情况和性能。“HDX Virtual Channel Details”（HDX 虚拟通道详细信息）视图包含有助于监控所有会话中的 Framehawk 虚拟通道和排除其故障的有用信息。要查看与 Framehawk 相关的指标，请选择图形 - Framehawk。

如果已建立 Framehawk 连接，将会在详细信息页面看到 **Provider = VD3D**（提供程序 = VD3D）和 **Connected = True**（已连接 = 是）。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](#)。

HDX 3D Pro

Mar 17, 2016

HDX 3D Pro 使您能够交付可利用图形处理器 (GPU) 实现硬件加速、展现最佳性能的桌面和应用程序，包括基于 OpenGL 和 DirectX 的三维专业图形应用程序。（标准 VDA 仅支持 DirectX 的 GPU 加速。）

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 和 OpenCL 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：

- 在广域网 (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。
 - 在局域网 (LAN) 连接条件下：在带宽 100 Mbps 的 LAN 连接下提供等同于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。与 Citrix XenServer 和 NVIDIA GRID GPU 结合使用时，HDX 3D Pro 为 Windows 桌面操作系统计算机提供虚拟 GPU (vGPU) 加速。有关支持的 XenServer 版本，请参阅 [Citrix 虚拟 GPU 解决方案](#)。

使用 HDX Monitor 工具（取代了运行状况检查工具）可以验证 HDX 虚拟化技术的操作和配置，并且能够诊断和解决 HDX 问题。要下载此工具并了解详细信息，请参阅 <https://taas.citrix.com/hdx/download/>。

Flash 重定向

Mar 17, 2016

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）处理工作转移到连接至 LAN 和 WAN 的用户 Windows 设备，从而降低服务器和网络的工作负载。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。

警告：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 Flash Player，因此，只有在 Flash Player 自身处于安全状态时才应启用 Flash 重定向。

旧版和第二代 Flash 重定向功能是独立解决方案，并在单独的虚拟通道中运行。

- 旧版 Flash 重定向功能仅在客户端受支持。如果用户设备上安装了早期版本的 Flash Player，或者无法安装 Flash Player，Flash 内容将在服务器上呈现。
- 第二代 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。第二代 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；请参阅下文了解详情。

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 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](#)。

- Flash 默认行为可确定默认的 Flash 加速行为。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），并将这些实例呈现在服务器上，而不是通过重定向呈现在用户设备上。此功能不会在加载 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。
- 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 内容可以下载到服务器，然后传输到用户设备以进行呈现。（默认情况下，Flash 重定向会将 Flash 内容下载到用于播放此内容的用户设备。）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，主要用于 Intranet 站点和内部 Flash 应用程序；请参阅下文了解详情。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 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\语言
- 对于 64 位计算机：%Program Files (x86)\Citrix\ICA Client\Configuration\语言

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。

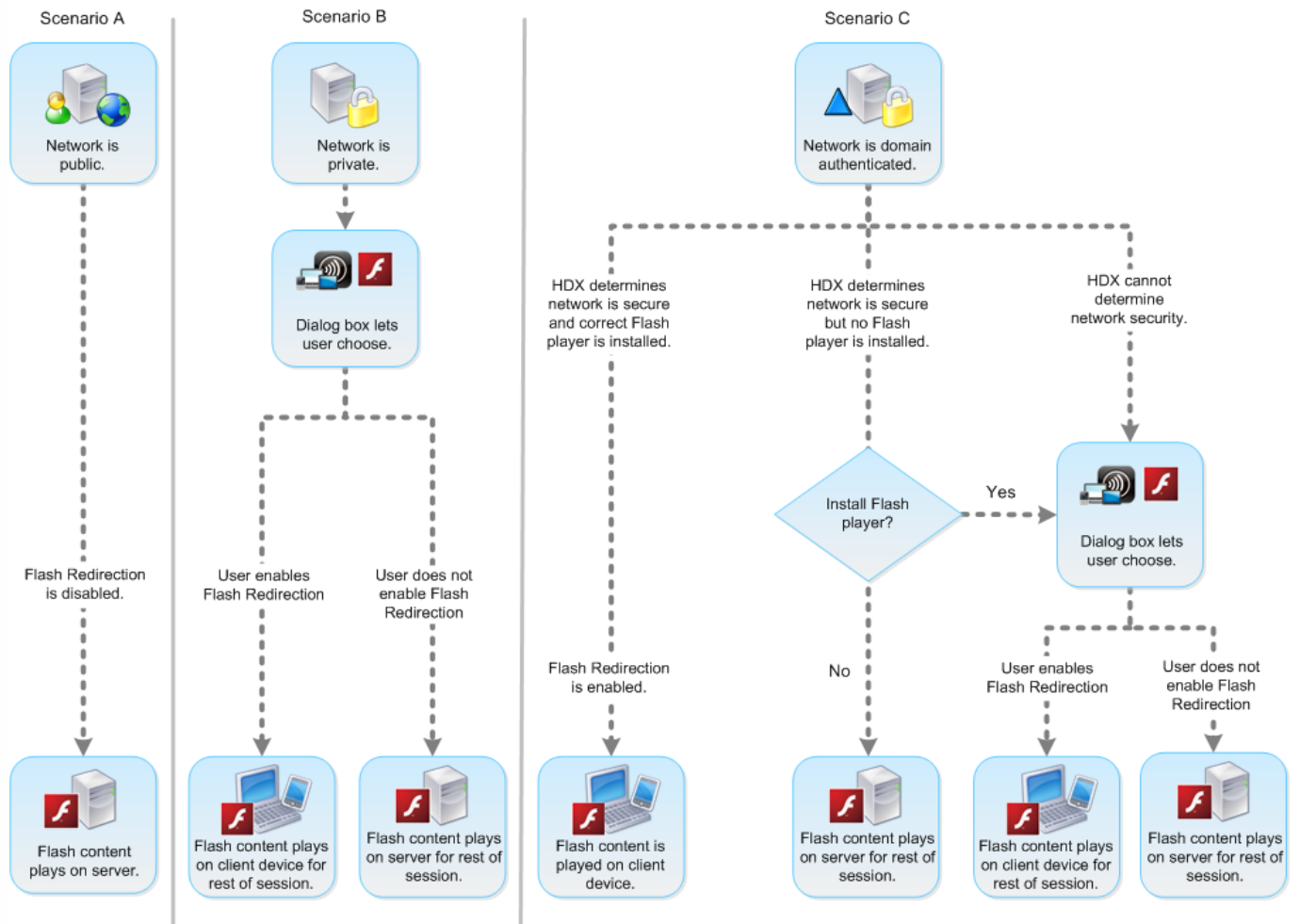
如果未设置配置并且使用 Desktop Lock，则默认情况下，将在用户设备上启用 Flash 重定向。

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。

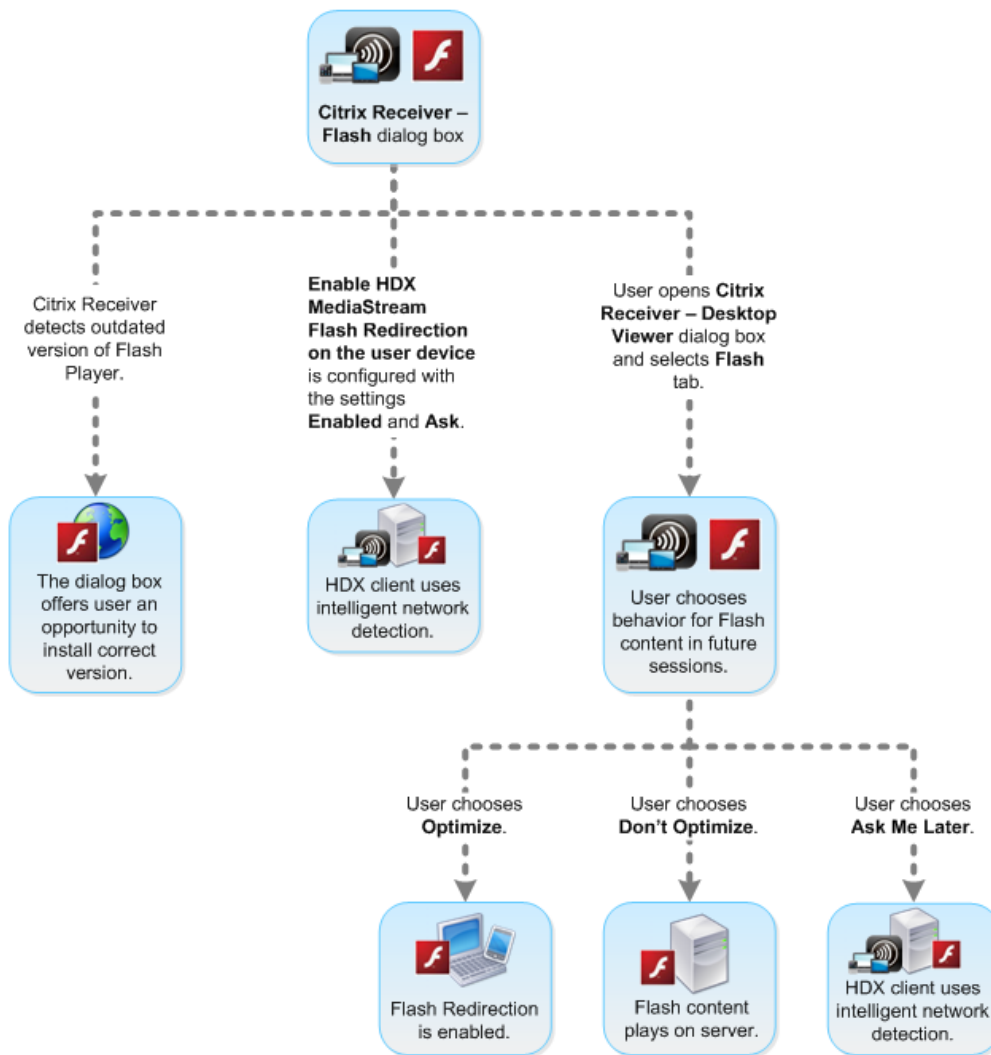
下图显示了 Flash 重定向针对各种网络类型的处理方式。

Intelligent Network Detection for Flash Redirection



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。

User control of Flash redirection



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。而应对此类站点使用服务器端呈现功能。

第二代 Flash 重定向功能支持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。

使用第二代 Flash 重定向时，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，将自动开始执行服务器端内容提取回退操作。

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。
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。

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。

警告

注册表编辑不当可能会导致严重问题，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。

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。目前，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的最低版本检查。

子项 ClientID0x51 指定 Linux ICA 客户端。子项 ClientID0x1 指定 Windows ICA 客户端。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）。Mobile SDK for Windows Apps 文档 <http://www.citrix.com/mobilitysdk/docs/clientdetection.html> 中提供了客户端 ID 的完整列表

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"

适用于 Windows 桌面操作系统的 GPU 加速

Mar 17, 2016

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 支持物理主计算机（包括桌面、刀片式计算机和机架工作站）、具有 GPU 直通功能的 XenServer VM 以及具有虚拟 GPU (vGPU) 的 XenServer VM。

利用 XenServer GPU 直通功能，可以创建对专用图形处理硬件具有独占访问功能的 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 XenServer vGPU，多个虚拟机可以直接访问单个物理 GPU 的图形处理功能。真正的硬件 GPU 共享功能可以为具有复杂和苛刻设计要求的用户提供完整而又合适的 Windows 7 或 Windows 2008 R2 SP1 桌面。GPU 共享功能适用于 NVIDIA GRID K1 和 K2 卡，使用非虚拟化操作系统上部署的相同 NVIDIA 图形驱动程序。

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 的深度压缩作为编码的默认压缩技术。此技术提供了最佳压缩性能，可动态适应网络情况。

基于 H.264 的深度压缩编解码器不再与 NVIDIA GPU 上 CUDA 核心的图形呈现争用资源。深度压缩编解码器在 CPU 上运行并提供带宽效率。

- 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

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。

- 多监视器和高分辨率监视器支持。对于 Windows 7 和 Windows 8 桌面，HDX 3D Pro 支持最多配有四个显示器的用户设备。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](#)。

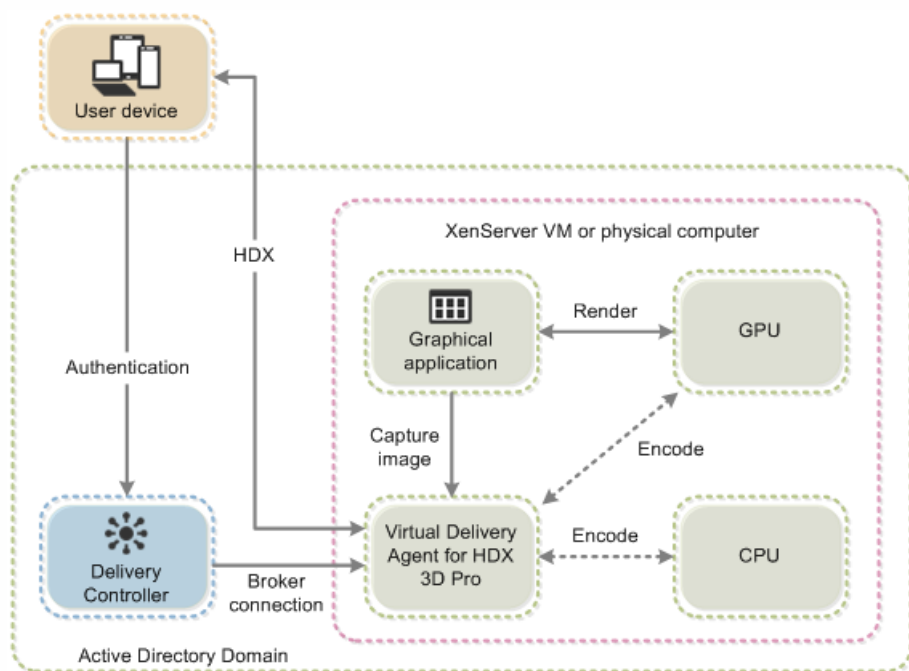
- 动态分辨率。可以将虚拟桌面或应用程序窗口的分辨率调整为任意大小。**注意：**唯一受支持的更改分辨率的方法为调整 VDA 会话窗口的大小。不支持从 VDA 会话内部更改分辨率（使用“控制面板”>“外观和个性化”>“显示”>“屏幕分辨率”）。
- 支持 NVIDIA Kepler 体系结构。HDX 3D Pro 支持 NVIDIA GRID K1 和 K2 卡，以便实现 GPU 直通和 GPU 共享。NVIDIA GRID vGPU 允许多个 VM 使用在非虚拟化操作系统中部署的相同 NVIDIA 图形驱动程序同时直接访问单个物理 GPU。
- 支持使用虚拟直接图形加速 (vDGA) 的 VMware vSphere 和 VMware ESX — 可针对 RDS 和 VDI 工作负载将 HDX 3D Pro 与 vDGA 结合使用。当 HDX 3D Pro 与 Virtual Shared Graphics Acceleration (vSGA) 结合使用时，仅支持一个显示器。将 vSGA 用于大型 3D 模型会导致性能问题，因为它使用 API 截获技术。有关详细信息，请参阅 [VMware vSphere 5.1 - Citrix 已知问题](#)。

如下图所示：

- 主机计算机必须与 Delivery Controller 驻留在相同的 Active Directory 域中。
- 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。



使用安装程序的图形界面安装 VDA for Windows Desktop OS 时，只需在 HDX 3D Pro 页面选择是。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 组件以及 VDA，然后再安装 VDA for HDX 3D Pro。同样，要从标准 VDA for Windows Desktop OS 切换到 HDX 3D Pro VDA，请先卸载标准 VDA，然后再安装 VDA for HDX 3D Pro。

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 VDA with HDX 3D Pro 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：Montereyenable.exe -enable -noreset

如果您在安装 VDA with HDX 3D Pro 后安装 NVIDIA 驱动程序，NVIDIA GRID 将禁用。使用 NVIDIA 提供的 Montereyenable 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：Montereyenable.exe -disable -noreset

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，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。

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](#)。

Windows Server 操作系统 GPU 加速

Apr 25, 2016

通过 HDX 3D Pro，在 Windows Server 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。

使用 HDX 3D Pro 时，多个用户可以共享图形卡。当 HDX 3D Pro 与 XenServer GPU 直通结合使用时，单台服务器可托管多个图形卡，每个虚拟机托管一个。

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。

虚拟机需要直接传递访问 GPU，这可通过使用 Citrix XenServer 或 VMware vSphere 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 Sharing 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

例如，对于运行 ESRI ArcGIS 等应用程序的 NVIDIA Q6000 和 M2070Q 卡，已报告具有 8 至 10 位用户的可扩展性。这些卡提供 6 GB 的视频 RAM。较新的 NVIDIA GRID 卡提供 8 GB 的视频 RAM 和显著提高的处理能力（更多 CUDA 核心）。使用 NVIDIA GRID K2 卡时，每个 GRID K2 卡支持 20 用户时可实现良好的性能。其他应用程序可能会提高更多，在高端 GPU 上达到 32 个并发用户。

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 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置：
 - [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\Applnit_Dlls\Multiple Monitor Hook]
"EnableWPFHook"=dword:00000001
 - [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\Applnit_Dlls\Multiple Monitor Hook]
"EnableWPFHook"=dword:00000001

支持对用户会话中运行的 CUDA 和 OpenCL 应用程序进行 GPU 加速（实验阶段）。默认情况下，会禁用此支持功能，但可以启用该功能以进行测试和评估。

要使用 CUDA 加速功能（实验阶段），请启用以下注册表设置：

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\Applnit_Dlls\Graphics Helper] "CUDA"=dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\Applnit_Dlls\Graphics Helper]
"CUDA"=dword:00000001

要使用 OpenCL 加速功能（实验阶段），请启用以下注册表设置：

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\Applnit_Dlls\Graphics Helper] "OpenCL"=dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\Applnit_Dlls\Graphics Helper]
"OpenCL"=dword:00000001

OpenGL Software Accelerator

Mar 17, 2016

OpenGL Software Accelerator 是一个适用于 OpenGL 应用程序（例如 ArcGIS、Google Earth、Nehe、Maya、Blender、Voxler、CAD 和 CAM）的软件光栅器。在某些情况下，借助 OpenGL Software Accelerator，无需使用图形卡即可在 OpenGL 应用程序中提供极佳的用户体验。

重要：OpenGL Software Accelerator 按“原样”提供，必须使用所有应用程序进行测试。OpenGL Software Accelerator 可能不适用于某些应用程序，旨在解决 Windows OpenGL 光栅器性能低下的问题。如果 OpenGL Software Accelerator 与应用程序结合使用，可用来避免 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。

何时应尝试使用 OpenGL Software Accelerator？

- 如果 XenServer 或其他虚拟机管理程序上的虚拟机中运行的应用程序存在性能问题，可尝试使用 OpenGL Accelerator。对某些应用程序而言，OpenGL Accelerator 优于 Windows 中的 Microsoft OpenGL 软件光栅器，因为 OpenGL Accelerator 采用 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，则大多数情况下它将提供最佳性能。如果图形卡是旧版本或者无法提供令人满意的性能，则可以尝试使用 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。

音频功能

Mar 17, 2016

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](#)。

重要：大多数音频功能都通过 ICA 流进行传输，这些功能受安全保护的方式与其他 ICA 通信流相同。未安装 NetScaler Access Gateway 时，用户数据报协议 (User Datagram Protocol, UDP) 音频使用独立的未受安全保护的传输机制。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。

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，音频质量策略设置为高 - 高清晰度音频。此设置可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。

考虑为拨号用户组和通过 LAN 或 WAN 连接的用户组创建单独的策略。如果使用通常限制带宽的拨号连接，对用户而言，下载速度比声音质量更加重要。因此，您可能需要为拨号连接和 LAN 或 WAN 连接分别创建单独的策略，前者所应用的音频压缩级别较高，后者所应用的音频压缩级别较低。

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，请添加客户端音频重定向设置，此设置的默认值为允许。

客户端音频映射可能导致服务器和网络负载过大；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，请添加客户端麦克风重定向设置，此设置的默认值为允许。

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，此设置处于启用状态。

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，通过 UDP 协议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“通过 UDP 协议的音频实时传输”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。

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。



```
; 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
```

如果通过编辑 default.ica 启用 UDP 音频，则 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，Citrix 建议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；这些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。在注册表中操作时请注意：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。

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。

网络流量优先级

Mar 17, 2016

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/IP 流（实时、交互、后台和批量通信）和一个 UDP/RTP 流（语音通信）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 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)。

警告：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功能的 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 默认端口优先级列表选择一个优先级；默认情况下，主端口 (2598) 的优先级为“高”。
 - 根据需要在 CGP 端口 1、CGP 端口 2 和 CGP 端口 3 中键入其他 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 CloudBridge，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 – 默认情况下禁用此设置。

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。

USB 和客户端设备注意事项

Mar 17, 2016

利用 HDX USB 设备重定向，用户可以将闪存驱动器连接到本地计算机，并从虚拟桌面或桌面托管应用程序远程访问该驱动器。在会话期间，用户可以使用即插即用设备，包括图片传输协议 (PTP) 设备（如数码相机）、媒体传输协议 (MTP) 设备（如数字音频播放器或便携式媒体播放器）以及销售点 (POS) 设备。

桌面托管应用程序会话不支持双跳 USB。

USB 重定向适用于 Citrix Receiver for Windows 和 Citrix Receiver for Linux。

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 文档了解详细信息。您可以通过更新支持重定向功能的 USB 设备的列表来限制可用于虚拟桌面的 USB 设备类型。

Important

对于需要将用户设备和服务器安全分离的环境，请向用户提供关于应避免使用的 USB 设备类型的指导信息。

经过优化的虚拟通道可用于重定向最常用的 USB 设备，并可以通过 WAN 提供性能和带宽效率。所提供的支持级别取决于用户设备上安装的 Citrix Receiver。通常，最好选择经过优化的虚拟通道，尤其对于高延迟环境更是如此。

为了执行 USB 重定向，此产品将以处理鼠标的相同方式来处理 SMART 板。

此产品支持对 USB 3.0 设备和 USB 3.0 端口使用优化的虚拟通道，例如，用于查看摄像机上的文件或向耳麦提供音频的 CDM 虚拟通道。此产品还支持连接到 USB 2.0 端口的 USB 3.0 设备的通用 USB 重定向。

对于没有优化虚拟通道的特殊设备，将退为使用通用的 USB 虚拟通道，该通道可提供原始的 USB 重定向功能。有关已在 XenDesktop 中经过测试的 USB 设备的信息，请参阅 [CTX123569](#)。

一些特定于设备的高级功能，如网络摄像机上的人体学接口设备 (HID) 按钮，在优化的虚拟通道中可能无法按预期运行；如果发生此问题，请使用通用 USB 虚拟通道。

默认情况下不会重定向某些设备，这些设备只能用于本地会话。例如，不应通过对通过内部 USB 连接到用户设备系统板的网络接口卡进行重定向。

下列 Citrix 策略设置可控制 USB 支持功能：

- **客户端 USB 设备优化规则。** 类=03 的输入设备支持此优化模式，例如签名设备和手写平板。如果未指定任何规则，将按照交互模式 (02) 处理设备。对于签名设备，建议使用捕获模式 (04)。
- **客户端 USB 设备重定向。** 默认设置为禁止。
- **客户端 USB 设备重定向规则。** 规则仅适用于使用通用 USB 重定向的设备；因此，这些规则不适用于使用专用或优化重定向的设备，例如 CDM。
- **客户端 USB 即插即用设备重定向。** 默认情况下设置为允许，即允许在用户会话中使用即插即用的 PTP、MTP 和 POS 设备。
- **客户端 USB 设备重定向带宽限制。** 默认设置为 0（无最大值）。
- **客户端 USB 设备重定向带宽限制百分比。** 默认设置为 0（无最大值）。

关于通用 USB 重定向

通用 USB 重定向适用于没有优化的虚拟通道的专用 USB 设备。此功能可将任意 USB 设备从客户端计算机重定向到虚拟桌面；利用此功能，最终用户可以在桌面会话中选择与多种通用 USB 设备交互，其效果与物理连接这些设备一样。

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

从 VDA for Desktop OS（最低版本 7.6）运行的桌面会话支持此功能。

从 VDA for Server OS（最低版本 7.6）运行的桌面会话也支持此功能，但具有以下限制：

- VDA 计算机必须运行 Windows Server 2012 R2
- 仅支持单跳场景
- USB 客户端驱动程序必须与适用于 Windows 2012 R2 的 RDSH 兼容
- 不支持 USB 存储设备、音频设备、智能卡读卡器以及未完全虚拟化的设备

有关配置通用 USB 重定向的详细信息，请参阅 [CTX137939](#)。

启用 USB 支持

1. 向策略中添加客户端 USB 设备重定向设置，并将其值设置为允许。
2. （可选）要更新可进行远程连接的 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。
3. 在用户设备上安装 Citrix Receiver 时启用 USB 支持。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。

更新可进行远程连接的 USB 设备的列表 (Citrix Receiver for Windows 4.2)

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。但在某些情况下，您可能不希望自动重定向所有 USB 设备。有关详细信息，请参阅 [CTX123015](#)。

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。要阻止列出或重定向 USB 设备，可以在客户端和 VDA 上指定设备规则，如下文中所述。

可以通过同时为 Citrix Receiver 和 VDA 指定 USB 设备重定向规则以覆盖默认 USB 策略规则，来更新可进行远程连接的 USB 设备范围。

- 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。
- 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

警告

注册表编辑不当可能会导致严重问题，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。组策略对象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。组策略对象策略规则的格式为 {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
设备	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
SubClass	设备描述符或接口描述符中的子类
Prot	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。
- 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。

Important

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）。

使用优化设备（例如大容量存储设备）时，通常使用专用 CDM 通道而非策略规则重定向设备。但是，可以通过以下方式之一覆盖此行为：

- 使用“通用 USB 重定向”手动重定向优化的设备：从首选项对话框的设备选项卡中选择 切换到通用。
- 使用“通用 USB 重定向”自动重定向优化的设备：设置存储设备的自动重定向（例如 AutoRedirectStorage = 1），并将 USB 用户首选项设置设置为自动连接 USB 设备；有关详细信息，请参阅 [CTX123015](#)。

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 # Allow Logitech SpaceNavigator 3D Mouse Deny: VID=046D # Deny all Logitech products
- 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 # Deny MS Active Sync devices Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF # Allow all USB-Miscellaneous devices

更新可进行远程连接的 USB 设备列表

默认情况下，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，将自动对 USB 设备执行重定向操作。此外，对于桌面设备站点或桌面托管应用程序，也将自动重定向 USB 设备。但在某些情况下，您可能不希望自动重定向所有 USB 设备。有关详细信息，请参阅 [CTX123015](#)。

Desktop Viewer 用户可以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。要阻止列出或重定向 USB 设备，可以在用户设备和 VDA 上指定设备规则。

可以通过同时为 Citrix Receiver 和 VDA 指定 USB 设备重定向规则以覆盖默认 USB 策略规则，来更新可进行远程连接的 USB 设备范围。设备规则将同时对 Citrix Receiver 和 VDA 强制实施。请确保同时执行更改，以便设备远程连接可以如您所期望的那样进行。

- 编辑用户设备的注册表（对于 Citrix Receiver for Linux，则应编辑 .ini 文件）。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。
- 在服务器操作系统计算机上的 VDA 注册表中编辑管理员覆盖规则。安装介质中包含一个 ADM 文件，以便您通过 Active Directory 组策略更改 VDA：dvd root os\lang\Support\Configuration\vda_usb.adm。

警告

注册表编辑不当可能会导致严重问题，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。组策略对象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。组策略对象策略规则的格式为 {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
设备	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
SubClass	设备描述符或接口描述符中的子类
Prot	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。
 - 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。

Important

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）。

使用优化设备（例如大容量存储设备）时，通常使用专用 CDM 通道而非策略规则重定向设备。但是，可以通过以下方式之一覆盖此行为：

- 使用“通用 USB 重定向”手动重定向优化的设备：从首选项对话框的设备选项卡中选择 切换到通用。
- 使用“通用 USB 重定向”自动重定向优化的设备：设置存储设备的自动重定向（例如 AutoRedirectStorage = 1），并将 USB 用户首选项设置为自动连接 USB 设备；有关详细信息，请参阅 [CTX123015](#)。

- 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 # Allow Logitech SpaceNavigator 3D Mouse Deny: VID=046D # Deny all Logitech products
 - 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 # Deny MS Active Sync devices Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF # Allow all USB-Miscellaneous devices

使用和删除 USB 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。

USB 大容量存储设备

远程访问可以通过客户端驱动器映射（即用户登录时，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）实现，这仅适用于大容量存储设备。 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。

两种类型的远程连接策略之间的主要区别如下：

功能	客户端驱动器映射	通用 USB 重定向
默认情况下处于启用状态	是	否
可配置只读访问权限	是	否
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 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 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 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。

适用于映射的客户端驱动器的文件访问

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。

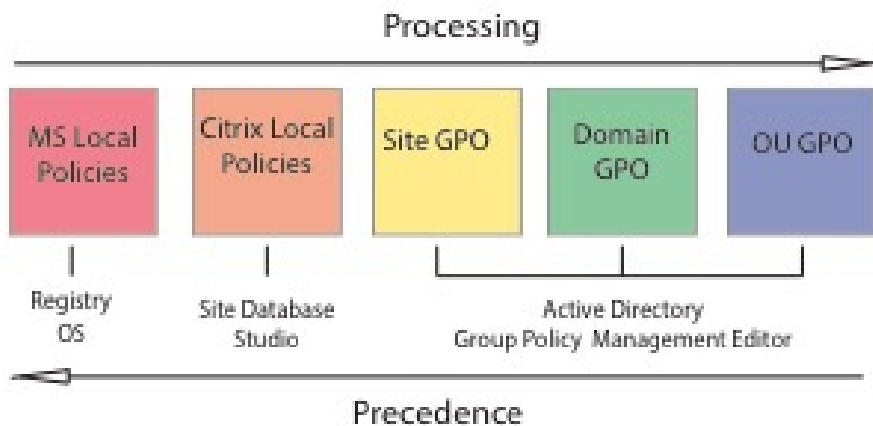
要防止用户添加或修改映射的客户端设备上的文件和文件夹，请启用只读客户端驱动器访问策略设置。将此设置添加到策略中时，请确保客户端驱动器重定向设置为允许并且也已添加到策略。

策略

Mar 17, 2016

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。

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。

相关内容

- [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](#)

使用策略

Mar 17, 2016

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。

处理 Citrix 策略的工具

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。

策略处理顺序和优先级

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。

Citrix 策略工作流

策略的配置过程如下：

1. 创建策略。
2. 配置策略设置。

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。

导航 Citrix 策略和设置

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实践。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。

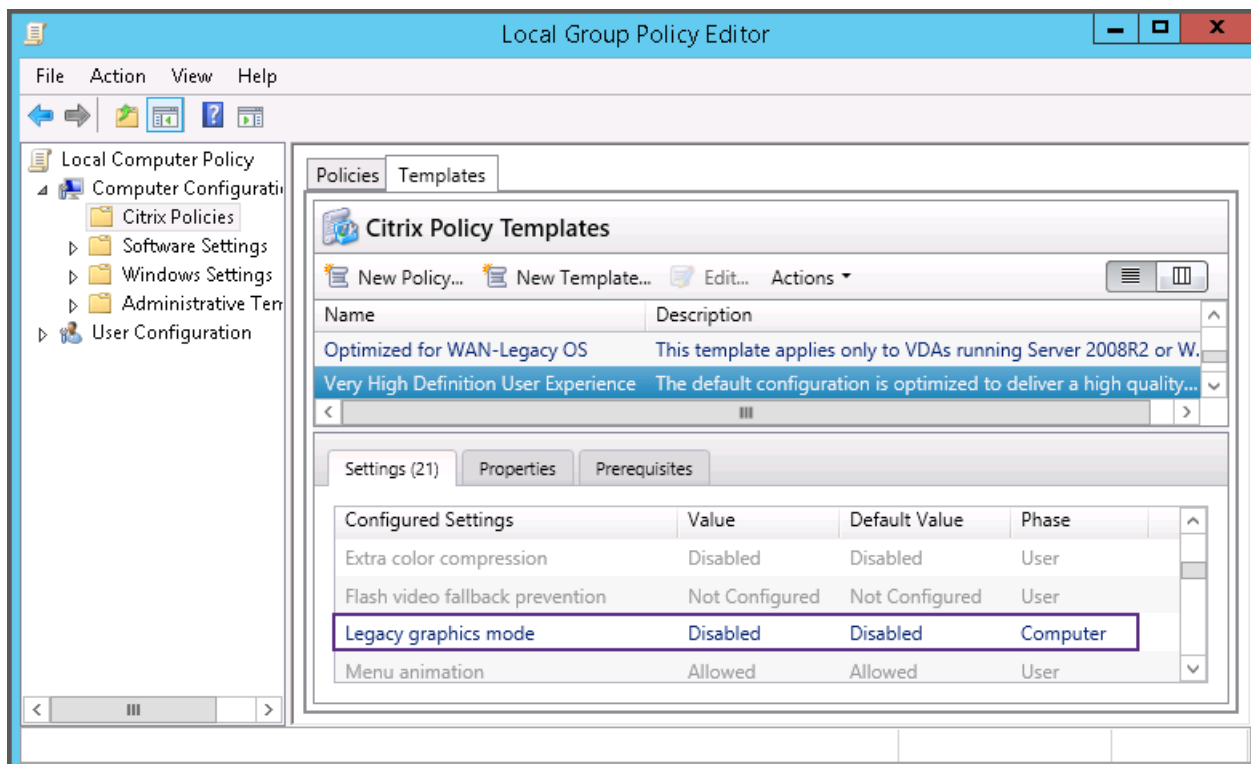
可以通过选择特定产品版本或类别精简搜索结果。对于未过滤的搜索，请选择所有设置。

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。



策略模板

May 12, 2016

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](#)。

内置 Citrix 模板

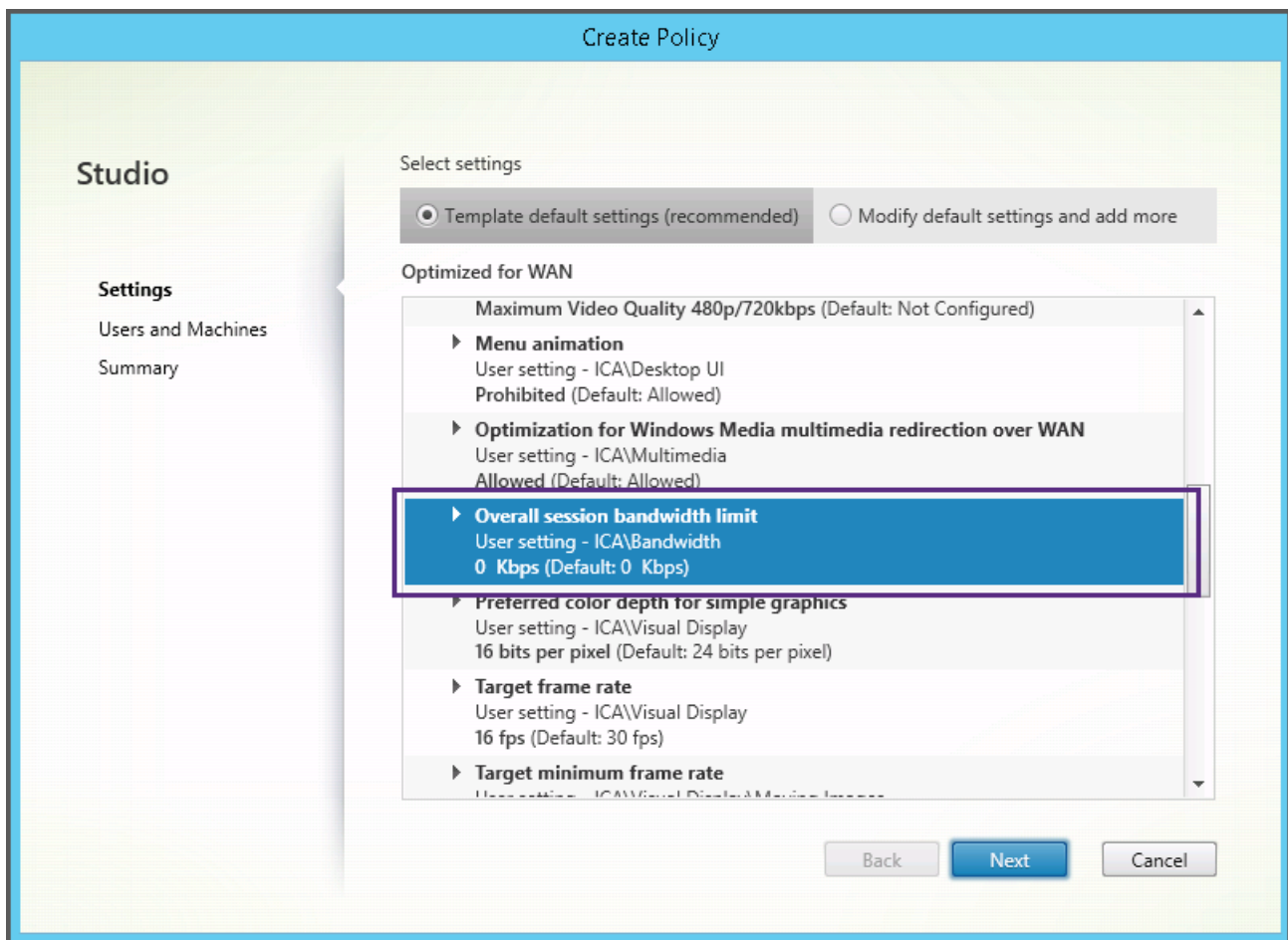
以下策略模板可用：

- **超高清晰度用户体验。** 此模板强制使用最大程度提供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 CloudBridge 优化。** 对从部署了 CloudBridge 的分支机构工作的用户应用此模板以优化 XenDesktop 的交付。这些位置通常具有利用率非常高的链接和/或高延迟。此模板优化此类情况下的带宽效率。

设置：

- 桌面组合重定向
- 菜单动画
- 拖动时查看窗口内容
- **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。



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，请使用这些模板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。

使用 Studio 创建和管理模板

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。

- 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。

使用组策略编辑器创建和管理模板

从组策略编辑器，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。 从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。

模板和委派管理

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。

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。

创建策略

Mar 17, 2016

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。

策略设置

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。如果禁用了某个设置，则在任何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设置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，分配的策略会自动更新。
- 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。

策略分配

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 建立的连接。 ● NetScaler Gateway 场名称 - NetScaler Gateway 虚拟服务器的名称。

分配名称	访问条件。要使用的端点分析策略或会话策略的名称。 应用策略的根据
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 组策略对象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 组策略对象的成员。

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。

使用 Studio 基于模板创建新策略

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. 通过选择以下其中一个选项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。

使用 Studio 创建新策略

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. 通过选择以下其中一个选项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。

使用组策略编辑器创建和管理策略

从组策略编辑器，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。从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。

对策略进行比较、设定优先级、建模和故障排除

Mar 17, 2016

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 策略中配置的同设置或使用远程桌面会话主机配置的同设置。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。

比较策略和模板

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实践。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。

设定策略的优先级

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。

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。

例外

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：

- 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 指定的范围内。

确定应用于连接的策略

由于会应用多个策略，因此有时连接不会按预期响应。如果优先级更高的策略也应用于某个连接，该策略将覆盖您在原策略中配置的设置。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。您可以为连接场景指定条件，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了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对象（包括 Citrix 策略）应用到特定的用户和控制器。

您可以从 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 Citrix 组策略建模向导

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 (gpmmc.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，选择希望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。

要查看报告，请选择查看建模报告。

故障排除策略

用户、IP 地址及其他分配对象可以具有多个可同时应用的策略。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：

- 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。

默认策略设置

May 12, 2016

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。

ICA

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
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

ICA/Adobe Flash 交付/Flash 重定向

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
Flash 视频回退预防错误 *.swf		VDA 7.6 FP3 至当前版本

ICA/音频

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

名称	默认设置	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

ICA/客户端自动重新连接

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

ICA/带宽

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
COM 端口重定向带宽限制	0 Kbps	VDA 的所有版本；对于 VDA 7 至当前版本，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 至当前版本，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

名称	默认设置	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 至当前版本，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 至当前版本，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

ICA/客户端传感器

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

ICA/桌面 UI

名称	默认设置	VDA
桌面组合重定向	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
桌面组合重定向图形质量	中	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7 至当前版本
桌面墙纸	允许	VDA 的所有版本

名称 菜单动画	默认设置 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

ICA/最终用户监视

名称	默认设置	VDA
ICA 往返程计算	已启用	VDA 的所有版本
ICA 往返程计算间隔	15 秒	VDA 的所有版本
空闲连接的 ICA 往返程计算	已禁用	VDA 的所有版本

ICA/增强的桌面体验

名称	默认设置	VDA
Enhanced Desktop Experience	允许	VDA for Server OS 7 至当前版本

ICA/文件重定向

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
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

名称 保留客户端驱动器盘符	默认设置 已禁用	VDA 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
使用异步写操作	已禁用	VDA 的所有版本

ICA/图形

名称	默认设置	VDA
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
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

ICA/图形/缓存

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

ICA/图形/Framehawk

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

ICA/保持活动状态

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

ICA/本地应用程序访问

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
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

ICA/移动体验

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
启动经过触控优化的桌面	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 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

ICA/多媒体

名称	默认设置	VDA
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
通过 WAN 优化 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 以通过 WAN 优化 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
视频负载管理策略设置	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
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

ICA/多流连接

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

ICA/端口重定向

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.x，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.x，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.x，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.x，使用注册表配置此设置

ICA/打印

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
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

ICA/打印/客户端打印机

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

打印机属性保留名称	默认设置	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

ICA/打印/驱动程序

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
通用打印驱动程序使用	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

ICA/打印/通用打印服务器

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
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 (kpbs)	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

ICA/打印/通用打印

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 图像与字体缓存 - 允许缓存嵌入的图像 = True - 允许缓存嵌入的字体 = True	VDA 的所有版本

名称	默认设置	VDA
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
通用打印打印质量限制	无限制	VDA 的所有版本

ICA/安全性

名称	默认设置	VDA
SecureICA 最低加密级别	基本	VDA for Server OS 7 至当前版本

ICA/服务器限制

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

ICA/会话限制

名称	默认设置	VDA
断开连接的会话计时器	已禁用	VDA 5、5.5、5.6 FP1、VDA for Desktop OS 7 至当前版本
断开连接的会话计时器间隔	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

ICA/会话可靠性

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

名称	默认设置	VDA
会话可靠性超时	180 秒	VDA 的所有版本

ICA/时区控制

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

ICA/TWAIN 设备

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

ICA/USB 设备

名称	默认设置	VDA
客户端 USB 设备优化规则	未指定任何规则	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

ICA/视频显示

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
使用视频编解码器进行压缩	使用视频编解码器(可用时)	VDA 7.6 FP3 至当前版本

ICA/视频显示/移动图像

名称	默认设置	VDA
最低图像质量	正常	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
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

ICA/视频显示/静止图像

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

ICA/WebSockets

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 名称	8008 默认设置	VDA for Server OS 7 至当前版本、VDA for Desktop OS 7 至当前版本
WebSocket 可信原始服务器列表	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

负载管理

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
排除 CPU 使用率的进程优先级	“低于正常”或“低”	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

Profile Management/高级设置

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

Profile Management/基本设置

名称	默认设置	VDA
活动写回	已禁用	VDA 的所有版本

名称	默认设置	VDA
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

Profile Management/跨平台设置

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策略设置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

Profile Management/文件系统/排除项

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

Profile Management/文件系统/同步

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

名称	默认设置	VDA
镜像的文件夹	已禁用。不镜像任何文件夹。	VDA 的所有版本

Profile Management/文件夹重定向

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

Profile Management/文件夹重定向/AppData (漫游)

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

Profile Management/文件夹重定向/联系人

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

Profile Management/文件夹重定向/桌面

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

Profile Management/文件夹重定向/文档

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
Profile Management/文件夹重定向/下载		

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”的重定向设置	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

Profile Management/文件夹重定向/收藏夹

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

Profile Management/文件夹重定向/链接

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

Profile Management/文件夹重定向/音乐

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

Profile Management/文件夹重定向/图片

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

Profile Management/文件夹重定向/保存的游戏

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

Profile Management/文件夹重定向/搜索

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

Profile Management/文件夹重定向/开始菜单

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

Profile Management/文件夹重定向/视频

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

Profile Management/日志设置

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

名称	默认设置	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

Management/Profile Management/配置文件处理

名称	默认设置	VDA
删除缓存配置文件前的延迟	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

名称	默认设置	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

Profile Management/注册表

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

Profile Management/流用户配置文件

名称	默认设置	VDA
始终缓存	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
挂起区域锁定文件的超时期限（天）	1 天	VDA 的所有版本

用户

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

Virtual Delivery Agent

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

名称	默认设置	VDA
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
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

虚拟 IP

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

HDX 3D Pro

名称	默认设置	VDA
启用无损压缩	已启用	VDA 5.5、5.6 FP1
HDX 3D Pro 质量设置		VDA 5.5、5.6 FP1

策略设置参考

Mar 17, 2016

“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。

快速引用

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。

音频

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

用户设备带宽

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

打印机 要限制用于以下项目的带宽	• 打印机重定向带宽限制或 • 使用此策略设置 • 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

客户端驱动器和用户设备的重定向

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
控制是否可以在会话中使用用户的本地 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
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

对于此任务 通过 WAN 将文件写入和复制到客户端磁盘的速度	使用此策略设置

内容重定向

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

桌面 UI

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

图形和多媒体

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

确定多流网络流量优先级

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 对于此任务	多流 (计算机和用户设置) 使用此策略设置

打印

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
控制由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	通用打印驱动程序使用
根据漫游用户的会话信息选择打印机	默认打印机

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。

ICA 策略设置

Apr 25, 2016

ICA 部分包含与 ICA 侦听器连接和到剪贴板的映射相关的策略设置。

客户端剪贴板重定向

此设置允许或阻止将用户设备上的剪贴板映射到服务器上的剪贴板。

默认情况下，允许剪贴板重定向。

要阻止剪贴数据在会话与本地剪贴板之间传输，请选择禁止。用户仍可以在会话中运行的应用程序之间剪切和粘贴数据。

启用此设置之后，使用剪贴板重定向带宽限制或剪贴板重定向带宽限制百分比设置来配置剪贴板在客户端连接中可以占用的最大允许带宽。

客户端剪贴板写入允许的格式

启用限制客户端剪贴板写入设置时，主机剪贴板数据无法与客户端端点共享，但是您可以利用此设置来允许与客户端端点剪贴板共享指定的数据格式。要使用此设置，请启用此设置并添加允许的指定格式。

以下剪贴板格式是系统定义的格式：

- 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

以下自定义格式是 XenApp 和 XenDesktop 中的预定义格式：

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

- HTML 格式

默认情况下会禁用 HTML 格式。启用该功能：

- 确保将**客户端剪贴板重定向**设置为允许。
- 确保将**限制客户端剪贴板写入**设置为启用。
- 在**客户端剪贴板写入允许的格式**中为 **HTML 格式**（以及您想支持的任何其他格式）添加相应的条目。

注意：启用 HTML 格式剪贴板复制支持（HTML 格式）会将所有脚本（如果存在）从所复制内容的源位置复制到目标位置。在继续复制前，请确保您信任此源位置。在复制了包含脚本的内容后，只有在您将目标文件保存为 HTML 文件并执行它时，这些脚本才处于活动状态。

可以添加其他自定义格式。自定义格式名称必须与要向系统注册的格式匹配。格式名称区分大小写。

如果将客户端剪贴板重定向或限制客户端剪贴板写入设置为“禁止”，将无法应用此设置。

桌面启动

此设置允许或阻止 VDA 直接访问用户组中的非管理员用户使用 ICA 连接来连接到该 VDA 上的会话。

默认情况下，非管理用户无法连接到这些会话。

此设置对 VDA 直接访问用户组中使用 RDP 连接的非管理员用户没有影响；不管是否启用此设置，这些用户都可以连接到 VDA。此设置对不属于 VDA 直接访问用户组的非管理员用户没有影响；不管是否启用此设置，这些用户都不可以连接到 VDA。

ICA 侦听器连接超时

注意：此设置仅适用于 Virtual Delivery Agent 5.0、5.5 和 5.6 Feature Pack 1。

此设置指定完成使用 ICA 协议的连接需要等待的最长时间。

默认情况下，需要等待的最长时间为 120000 毫秒（或两分钟）。

ICA 侦听器端口号

此设置指定服务器上 ICA 协议使用的 TCP/IP 端口号。

默认情况下，此端口号设置为 1494。

有效端口号必须在介于 0 到 65535 的范围内，且不得与其他已知端口号相冲突。如果更改端口号，请重新启动服务器，新值才能生效。如果在服务器上更改端口号，还必须在每个连接到该服务器的 Citrix Receiver 或插件上更改该端口号。

在客户端连接期间启动非发布程序

此设置指定是否允许通过服务器上的 RDP 启动初始应用程序。

默认情况下，不允许通过服务器上的 RDP 启动初始应用程序。

限制客户端剪贴板写入

如果将其设置为“允许”，主机剪贴板数据无法与客户端端点共享。可以通过启用客户端剪贴板写入允许的格式设置允许特定格式。

默认情况下，此设置为“禁止”。

限制会话剪贴板写入

此设置为“允许”时，客户端剪贴板数据无法在用户会话中共享。可以通过启用会话剪贴板写入允许的格式设置允许特定格式。

默认情况下，此设置为“禁止”。

会话剪贴板写入允许的格式

将限制会话剪贴板写入设置为“允许”时，客户端剪贴板数据无法与会话应用程序共享，但是您可以利用此设置来允许与会话剪贴板共享指定的数据格式。

以下剪贴板格式是系统定义的格式：

- 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

以下自定义格式是 XenApp 和 XenDesktop 中的预定义格式：

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- HTML 格式

默认情况下会禁用 HTML 格式。启用该功能：

- 确保将**客户端剪贴板重定向**设置为允许。
- 确保将**限制会话剪贴板写入**设置为启用。
- 在**会话剪贴板写入允许的格式**中为 **HTML 格式**（以及您想支持的任何其他格式）添加相应的条目。

注意：启用 HTML 格式剪贴板复制支持（HTML 格式）会将所有脚本（如果存在）从所复制内容的源位置复制到目标位置。在继续复制前，请确保您信任此源位置。在复制了包含脚本的内容后，只有在您将目标文件保存为 HTML 文件并执行它时，这些脚本才处于活动状态。

可以添加其他自定义格式。自定义格式名称必须与要向系统注册的格式匹配。格式名称区分大小写。

如果将客户端剪贴板重定向或限制会话剪贴板写入设置为“禁止”，将无法应用此设置。

客户端自动重新连接策略设置

Mar 17, 2016

“客户端重新连接”部分包含用于控制会话自动重新连接的策略设置。

客户端自动重新连接

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。

默认情况下，允许自动重新连接。

如果允许自动重新连接，则当连接断开时，用户将可以在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。

但是，如果未使用 Citrix Receiver Cookie（包括会话 ID 的密钥和凭据），自动重新连接可能会导致启动新会话（而不是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。

对于应用程序会话，允许自动重新连接时，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，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;<seconds>

其中，<秒数> 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。

客户端自动重新连接身份验证

此设置要求对客户端自动重新连接进行身份验证。

默认情况下，无需进行身份验证。

用户最初登录时，其凭据将加密并存储在内存中，并创建一个包含发送到 Citrix Receiver 的加密密钥的 Cookie。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。

客户端自动重新连接日志记录

此设置启用或禁用将事件日志中记录客户端自动重新连接。

默认情况下，禁用日志记录。

启用日志记录后，服务器的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接事件组合日志。

音频策略设置

Mar 17, 2016

“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。

通过 UDP 实时传输音频

此设置可允许或阻止使用用户数据报协议 (User Datagram Protocol, 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。

音频即插即用

该设置允许或阻止适用多个音频设备来记录和播放声音。

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。

音频质量

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 协议的音频实时传输策略设置为允许。
- 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。

客户端音频重定向

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。

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。

客户端麦克风重定向

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。

带宽策略设置

Mar 17, 2016

“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。

音频重定向带宽限制

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）。

如果为此设置输入一个值，并为音频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。

音频重定向带宽限制百分比

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）。

如果为此设置输入一个值，并为音频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

客户端 USB 设备重定向带宽限制

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）。

如果针对此设置和客户端 USB 设备重定向带宽限制百分比设置都输入了值，将应用最严格（具有较低值）的设置。

客户端 USB 设备重定向带宽限制百分比

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）。

如果针对此设置和客户端 USB 设备重定向带宽限制设置都输入了值，将应用最严格（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

剪贴板重定向带宽限制

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）。

如果为此设置输入一个值，并为剪贴板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。

剪贴板重定向带宽限制百分比

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）。

默认情况下，未指定最大值（零）。

如果为此设置输入一个值，并为剪贴板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

COM 端口重定向带宽限制

注意：对于 Virtual Delivery Agent 7.x，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。

COM 端口重定向带宽限制百分比

注意：对于 Virtual Delivery Agent 7.x，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

文件重定向带宽限制

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）。

如果为此设置输入一个值，并为文件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。

文件重定向带宽限制百分比

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）。

如果为此设置输入一个值，并为文件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

HDX MediaStream 多媒体加速带宽限制

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）。

如果为此设置以及 HDX MediaStream 多媒体加速带宽限制百分比设置都输入值，将应用最严格的设置（两者中较小者）。

HDX MediaStream 多媒体加速带宽限制百分比

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）。

如果为此设置以及 HDX MediaStream 多媒体加速带宽限制设置都输入了值，则会应用最严格的设置（即两者中较小者）。

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

LPT 端口重定向带宽限制

注意：对于 Virtual Delivery Agent 7.x，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。

LPT 端口重定向带宽限制百分比

注意：对于 Virtual Delivery Agent 7.x，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

总会话带宽限制

此设置指定用户会话可用的总带宽 (Kbps)。

最大可强制带宽上线为 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。

打印机重定向带宽限制

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）。

如果为此设置输入一个值，并为打印机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。

打印机重定向带宽限制百分比

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）。

如果为此设置输入一个值，并为打印机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

TWAIN 设备重定向带宽限制

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)。

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百分比设置输入一个值，则应用最严格（具有较低值）的设置。

TWAIN 设备重定向带宽限制百分比

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

客户端传感器策略设置

Mar 17, 2016

“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。

允许应用程序使用客户端设备的物理位置

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。

桌面 UI 策略设置

Mar 17, 2016

“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。限制带宽使用率可以改善 WAN 上的应用程序性能。

桌面组合重定向

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，桌面组合重定向已启用。

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。

桌面组合重定向图形质量

此设置将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。

桌面墙纸

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。

菜单动画

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。

拖动时查看窗口内容

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。

最终用户监控策略设置

Mar 17, 2016

“最终用户监控”部分包含用于测量会话流量的策略设置。

ICA 往返程计算

此设置确定是否为活动连接执行 ICA 往返程计算。

默认情况下，启用活动连接的计算。

默认情况下，每次 ICA 往返程度量的启动都将延迟，直至指示有用户交互的通信流出现。此延迟的长度不限，以防止 ICA 往返程度量成为产生 ICA 通信流的唯一原因。

ICA 往返程计算间隔

此设置指定 ICA 往返程计算的执行间隔（以秒为单位）。

默认情况下，ICA 往返程每 15 秒钟计算一次。

空闲连接的 ICA 往返程计算

此设置确定是否为空闲连接执行 ICA 往返程计算。

默认情况下，不为空闲连接执行计算。

默认情况下，每次 ICA 往返程度量的启动都将延迟，直至指示有用户交互的通信流出现。此延迟的长度不限，以防止 ICA 往返程度量成为产生 ICA 通信流的唯一原因。

Enhanced Desktop Experience 策略设置

Mar 17, 2016

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，启用此设置。

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的配置文件的配置有所差别，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。

文件重定向策略设置

Mar 17, 2016

“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。

自动连接客户端驱动器

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

客户端驱动器重定向

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

客户端固定驱动器

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。

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。

客户端软盘驱动器

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软盘驱动器。

默认情况下，允许访问客户端软盘驱动器。

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。

客户端网络驱动器

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。

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。

客户端光盘驱动器

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 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。

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。

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 USB 驱动器。

默认情况下，允许访问客户端可移动驱动器。

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。

主机到客户端重定向

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 Media Server (MMS)

保留客户端驱动器盘符

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。

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并且设置为允许。

只读客户端驱动器访问

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。

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并且设置为允许。

特殊文件夹重定向

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。

在将此设置添加到策略中时，请确保已存在客户端固定驱动器设置，并设置为允许。

使用异步写操作

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。

Flash 重定向策略设置

Mar 17, 2016

“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。

Flash 加速

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。

Flash 背景色列表

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”使用不当可能会导致严重问题，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。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
```

Flash 向后兼容性

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 Online Plug-in 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。

Flash 默认行为

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。
- 阻止 Flash 播放器。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。

Flash 事件日志记录

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。

Flash 智能回退

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。

Flash 延迟阈值

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。

Flash 视频回退预防

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一个错误 *.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。

Flash 视频回退预防错误 *.swf

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`

Flash 服务器端内容提取 URL 列表

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，但在 Flash 服务器端内容提取 URL 列表中指定了该 Web 站点，则会自动提取服务器端内容。

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。

Flash URL 兼容性列表

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。

图形策略设置

Mar 17, 2016

“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。

显示内存限制

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。

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。

显示模式降级首选项

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，或者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还是分辨率的级别，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。

要在颜色深度或分辨率降级时通知用户，请配置在显示模式降级时通知用户设置。

动态窗口预览

该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。
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，系统将为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。

图像缓存

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。

此设置将在会话中启用或禁用图像分区的缓存和取回。通过在需要时缓存分区中的图像和取回这些图像，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。

旧图形模式

此设置将禁用丰富的图形体验并可回退到旧图形体验功能，以改善通过 WAN 或移动连接时的可扩展性。

默认情况下，此设置处于禁用状态，并向用户提供丰富的图形体验。

允许的最大颜色深度

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（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。

在显示模式降级时通知用户

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。

此设置在颜色深度或分辨率降级时，向用户显示简要说明。

默认情况下，禁用用户通知。

排队与丢弃

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。

缓存策略设置

Mar 17, 2016

“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。

永久缓存阈值

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。

Framehawk 策略设置

Mar 17, 2016

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，Framehawk 显示通道处于禁用状态。

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。

保持活动状态策略设置

Mar 17, 2016

“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。

本地应用程序访问策略设置

Mar 17, 2016

“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。

移动体验策略设置

Mar 17, 2016

“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。

启动经过触控优化的桌面

此设置已禁用，不适用于 Windows 10 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。

多媒体策略设置

Mar 17, 2016

“多媒体”部分包含用于管理用户会话中的流音频和视频的策略设置。

限制视频质量

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：

- 1080 p/8.5 mbps
- 720 p/4.0 mbps
- 480 p/720 kbps
- 380 p/400 kbps
- 240 p/200 kbps

注意：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

此设置启用或禁用对视频会议应用程序的支持。

默认情况下，允许视频会议支持。

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。

使用多媒体会议时，请确保满足以下条件：

- 必须安装制造商为用于多媒体会议的网络摄像机提供的驱动程序。
- 必须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。

通过 WAN 优化 Windows Media 多媒体重定向

此设置启用了实时多媒体代码转换，允许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 以通过 WAN 优化 Windows Media 多媒体重定向

此设置支持在 Virtual Delivery Agent (VDA) 上的图形处理器 (GPU) 中执行实时多媒体代码转换，以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 才支持 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。

视频回退预防

管理员可以使用视频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。这允许客户端提取到 RAVE 再到服务器端回退。

要配置此设置，请选择以下选项之一：

- **服务器提取 - 服务器端呈现。** 允许客户端提取到 RAVE 再到服务器端回退。
- **服务器提取 - 客户端呈现。** 允许客户端提取到 RAVE 回退，但阻止 RAVE 到服务器端呈现回退。
- **客户端提取 - 客户端呈现。** 阻止客户端提取到 RAVE 再到服务器端呈现回退。

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”。

Windows Media 客户端内容提取

此设置使用户设备能够通过流技术直接从 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。

默认情况下，允许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。

启用此设置可将对媒体的任何处理过程从主机服务器移动到用户设备，提高了网络利用率和服务器可扩展性。此外，启用此设置后，将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。如果禁用此设置，将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，允许向用户交付流音频和视频。

启用此设置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 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

该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）。

多流连接策略设置

Mar 17, 2016

“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

此设置允许或阻止通过 UDP 在服务器上传输音频。

默认情况下，允许通过 UDP 在服务器上传输音频。

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) 用于与用户设备交换音频数据包数据的端口号范围（采用最小端口号.最大端口号格式）。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，此范围设置为 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

此设置可在服务器上启用或禁用“多流”功能。

默认情况下，“多流”功能处于禁用状态。

如果要在环境中使用具有“多流”支持功能的 Citrix CloudBridge，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

此设置可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。

端口重定向策略设置

Mar 17, 2016

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。

注意：对于 Virtual Delivery Agent 7.x，请使用注册表配置这些设置。请参阅[使用注册表配置 COM 端口和 LPT 端口重定向设置](#)。

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。

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

打印策略设置

Mar 17, 2016

“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：添加打印机，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

此设置指定在打印机自动创建过程中记录哪些事件。您可以选择不记录错误或警告，只记录错误，或同时记录错误和警告。

默认情况下，将记录错误和警告。

以下事件就是警告的一个例子：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。要在此案例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。

客户端打印机策略设置

Mar 17, 2016

“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，请选择以下选项之一：

- 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。
该设置为所使用的用户设备与通用打印兼容的会话启用或禁用一般 Citrix 通用打印机对象的自动创建。

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：

- 通用打印驱动程序使用
- 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。

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。

默认情况下，不指定任何规则。

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，请选择以下选项之一：

- 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 Online Plug-in 9 至 12.x 版或使用 Citrix Receiver 3.x 时，才选择该选项。
- 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 或较旧版本和 MetaFrame Presentation Server Client 8.x 或较旧版本，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

此设置启用或禁用用户设备上的打印机的保留和重新创建。默认情况下，客户端打印机将自动保留和自动恢复。

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。

驱动程序策略设置

Mar 17, 2016

“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

该设置启用或禁用从 Windows 现成驱动程序集或从在主机上分段的驱动程序包（使用 pnputil.exe /a）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

您可以在列表中添加、编辑或删除驱动程序，以及更改驱动程序的顺序。

通用打印驱动程序使用

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取代标准的特定于打印机型号的驱动程序，从而潜在地减轻了在主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，请选择以下选项之一：

- 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打印机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，则使用合适的特定于打印机型号的驱动程序来自动创建客户端打印机。

通用打印服务器策略设置

Mar 17, 2016

“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：

- **启用并允许回退到 Windows 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。
- **启用但不允许回退到 Windows 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 (kpbs)

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。

有效的端口号必须在 0 到 65535 范围内。

通用打印策略设置

Mar 17, 2016

“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

该设置控制在 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 记录直接后台处理到打印机中。

将此设置添加到策略时，请选择以下选项之一：

- 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。可以将该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，请选择以下选项之一：

- 不压缩
- 最佳质量(无损压缩)
- 高质量
- 标准质量
- 降低质量(最大压缩)

将该设置添加到包含通用打印优化默认设置的策略中时，应注意以下几项：

- 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

该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，标准质量处于启用状态，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超出由所需图像质量所设置的压缩级别时减少带宽，而不降低图像质量。默认情况下，超级压缩功能处于禁用状态。
- 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。

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。

将该设置添加到包含通用打印图像压缩限制设置的策略中时，应注意以下几项：

- 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，请选择以下选项之一：

- 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都使用打印预览

通用打印打印质量限制

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，无限制处于启用状态，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限制为已配置的设置。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“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，请选择以下选项之一：

- 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

安全策略设置

Mar 17, 2016

“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，请选择以下选项之一：

- 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。

服务器限制策略设置

Mar 17, 2016

“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）。

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。这是 Microsoft 对话框，不受 Citrix 策略设置控制。有关详细信息，请参阅 <http://support.citrix.com/article/CTX118618>。

会话限制策略设置

Mar 17, 2016

“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。

断开连接的会话计时器

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。

断开连接的会话计时器间隔

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）。

会话可靠性策略设置

Mar 17, 2016

“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。

默认情况下，允许启用会话可靠性。

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。要指示连接已断开，用户的显示内容将冻结，且光标变成一个旋转的沙漏，直至连接恢复。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。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，请将客户端自动重新连接身份验证设置配置为要求进行身份验证。这样，在重新连接到中断的会话时，将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。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。

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。

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。

默认情况下，此时间设置为 180 秒或 3 分钟。

尽管您可以延长会话保持打开状态的时间长度，此功能的主要目的是为用户提供方便，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。

时区控制策略设置

Mar 17, 2016

“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”）。

TWAIN 设备策略设置

Mar 17, 2016

“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

当前不支持 TWAIN 2.0。

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。

USB 设备策略设置

Mar 17, 2016

“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，将按照交互模式 (02) 处理设备。对于签名设备，建议使用捕获模式 (04)。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。本部分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。
设备	设备描述符或接口描述符中的类。
SubClass	设备描述符或接口描述符中的子类。
Prot	设备描述符或接口描述符中的协议。

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
```

使用注册表设置禁用优化模式

可以通过注册表标记在系统范围内禁用优化模式：

```
HKLM\System\CurrentControlSet\Services\Icausb\Parameters
DisableInputOptimization DWORD - 将值设置为 1
```

需要重新启动系统才能使此注册表更改生效。

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 **Disable slideshow**（禁用幻灯片放映），然后单击 **Apply**（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

标记名称	说明
PID	设备描述符中的产品 ID
REL	设备描述符中的版本 ID
设备	设备描述符或接口描述符中的类
SubClass	设备描述符或接口描述符中的子类
Prot	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。

视频显示策略设置

Mar 17, 2016

“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

降低颜色深度，将简单图形设置为 **16 位/像素**，可能会提高低带宽连接下的响应速度，但图像质量可能会稍有下降。此选项仅在不使用视频编解码器压缩图形时受支持。

默认情况下，设置为 24 位/像素。

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。

使用视频编解码器进行压缩

允许视频解码在端点上可用时使用视频编解码器压缩图形。视频解码在端点上不可用时，或者当您指定了**不使用视频编解码器**时，将同时使用静态图像压缩和位图缓存。

默认情况下，设置为“使用视频编解码器(可用时)”。

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。

移动图像策略设置

Mar 17, 2016

“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。

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最低可接受的图像质量。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。

默认设置为“正常”。

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。

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，不应用任何渐进式压缩。

细节更丰富的图像（由常规无损压缩设置定义）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无损压缩级别设置。

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，之后会应用标准无损压缩设置。

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

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

- 渐进式超级压缩

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。

静态图像策略设置

Mar 17, 2016

“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。

当通过带宽受限制的客户端连接交付图像时，此设置可以允许或禁止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。

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。

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。

此设置允许或禁止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，超级压缩功能处于禁用状态。

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

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。

为改善带宽密集型图像的响应速度，请使用高压压缩。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

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)。

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

WebSocket 策略设置

Mar 17, 2016

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。

此设置允许或禁止 WebSocket 连接。

默认情况下，禁止 WebSocket 连接。

此设置可识别传入的 WebSocket 连接的端口。

默认情况下，此值为 8008。

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。

负载管理策略设置

Mar 17, 2016

“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](#)。

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，此参数设置为 2。

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。

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”。

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。

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。

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。

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）。

默认情况下，将其设置为 768 MB。

Profile Management 策略设置

Mar 17, 2016

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。

高级策略设置

Mar 17, 2016

“高级设置”部分包含与 Profile Management 高级配置相关的策略设置。

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。

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。

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，将使用默认值。

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。

基本策略设置

Mar 17, 2016

“基本设置”部分包含与 Profile Management 基本配置有关的策略设置。

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。

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。

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 <域名>\<组名> 格式指定域组。

如果未在此处配置此设置，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，则会处理所有用户组的成员。

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。

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。

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。

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。

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 <域名>\<组名> 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。

如果该设置没有在此配置，也不在 INI 文件中，则会处理所有用户组的成员。

跨平台策略设置

Mar 17, 2016

“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。

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。

如果该设置没有在此配置，也不在 .ini 文件中，则会处理所有用户组。

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，跨平台设置功能处于禁用状态。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果未在此处也未在 .ini 文件中配置此设置，则将不应用任何跨平台设置。

此设置将从下载包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。

如果未在此处也未在 .ini 文件中配置此设置，则将不应用任何跨平台设置。

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，此设置处于禁用状态，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，将使用默认值。

如果在平台的 OU 中启用此设置，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。

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，则第一位用户登录到的平台将作为基础配置文件。默认情况下，此设置处于禁用状态，Profile Management 不会将数据从单平台配置文件迁移到存储中。

文件系统策略设置

Mar 17, 2016

“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。

排除策略设置

Mar 17, 2016

“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。

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，此设置处于禁用状态，系统会同步用户配置文件中的所有文件夹。

示例：Desktop 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，则将对用户配置文件中的所有文件夹进行同步。

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，此设置处于禁用状态，系统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 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，则将对用户配置文件中的所有文件进行同步。

同步策略设置

Mar 17, 2016

“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。

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，此设置处于禁用状态，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。

如果该设置没有在此配置，也不在 INI 文件中，则仅对用户配置文件中没有排除的文件夹进行同步。

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，此设置处于禁用状态，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。

如果该设置没有在此配置，也不在 INI 文件中，则仅会对用户配置文件中没有排除的文件夹进行同步。

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

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，此设置处于禁用状态，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。

如果未在此处也未在 .ini 文件中配置此策略，则不会镜像任何文件夹。

文件夹重定向策略设置

Mar 17, 2016

“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。

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。

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。

“AppData (漫游)”策略设置

Mar 17, 2016

“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。

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。

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。

“联系人”策略设置

Mar 17, 2016

“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。

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。

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。

桌面策略设置

Mar 17, 2016

“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。

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。

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。

“文档”策略设置

Mar 17, 2016

“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。

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。

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。

“下载”策略设置

Mar 17, 2016

“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。

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。

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。

“收藏夹”策略设置

Mar 17, 2016

“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。

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。

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。

“链接”策略设置

Mar 17, 2016

“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。

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。

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。

“音乐”策略设置

Mar 17, 2016

“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。

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。

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。
- 重定向到相对于“文档”文件夹的路径。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。

“图片”策略设置

Mar 17, 2016

“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。
- 重定向到相对于“文档”文件夹的路径。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。

“保存的游戏”策略设置

Mar 17, 2016

“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。

“搜索”策略设置

Mar 17, 2016

“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。

“开始菜单”策略设置

Mar 17, 2016

“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。

“视频”策略设置

Mar 17, 2016

“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。
- 重定向到相对于“文档”文件夹的路径。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。

“日志”策略设置

Mar 17, 2016

“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，请确保启用日志记录设置也处于启用状态。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果该设置没有在此配置，也不在 INI 文件中，则记录错误和常规信息。

常规信息

此设置启用或禁用常规信息的详细日志记录。

默认情况下，禁用此设置。

启用此设置时，请确保启用日志记录设置也处于启用状态。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果该设置没有在此配置，也不在 INI 文件中，则记录错误和常规信息。

常见警告

此设置启用或禁用常见警告的详细日志记录。

默认情况下，禁用此设置。

启用此设置时，请确保启用日志记录设置也处于启用状态。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果该设置没有在此配置，也不在 INI 文件中，则记录错误和常规信息。

启用日志记录

此设置启用或禁用调试（详细日志记录）模式下的 Profile Management 日志记录。在调试模式中，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，此设置处于禁用状态，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。

如果该设置没有在此配置，也不在 INI 文件中，则只记录错误。

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，请确保启用日志记录设置也处于启用状态。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果该设置没有在此配置，也不在 INI 文件中，则记录错误和常规信息。

文件系统通知

此设置启用或禁用文件系统通知的详细日志记录。

默认情况下，禁用此设置。

启用此设置时，请确保启用日志记录设置也处于启用状态。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果该设置没有在此配置，也不在 INI 文件中，则记录错误和常规信息。

注销

此设置启用或禁用用户注销的详细日志记录。

默认情况下，禁用此设置。

启用此设置时，请确保启用日志记录设置也处于启用状态。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果该设置没有在此配置，也不在 INI 文件中，则记录错误和常规信息。

登录

此设置启用或禁用用户登录的详细日志记录。

默认情况下，禁用此设置。

启用此设置时，请确保启用日志记录设置也处于启用状态。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果该设置没有在此配置，也不在 INI 文件中，则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（字节）。

默认情况下，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。

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，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，此设置处于禁用状态，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非常有用，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 路径将使您能够保留日志文件，但该虚拟机的系统帐户必须具有 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，则 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。

如果该设置没有在此配置，也不在 INI 文件中，则使用默认位置 %SystemRoot%\System32\Logfiles\UserProfileManager。

个性化用户信息

此设置启用或禁用个性化用户信息的详细日志记录。

默认情况下，禁用此设置。

启用此设置时，请确保启用日志记录设置也处于启用状态。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果该设置没有在此配置，也不在 INI 文件中，则记录错误和常规信息。

登录和注销时的策略值

此设置启用或禁用用户登录及注销时策略值的详细日志记录。

默认情况下，禁用此设置。

启用此设置时，请确保启用日志记录设置也处于启用状态。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果该设置没有在此配置，也不在 INI 文件中，则记录错误和常规信息。

注册表操作

此设置启用或禁用注册表中执行的操作的详细日志记录。

默认情况下，禁用此设置。

启用此设置时，请确保启用日志记录设置也处于启用状态。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果该设置没有在此配置，也不在 INI 文件中，则记录错误和常规信息。

注销时的注册表差异

此设置启用或禁用用户注销时任何注册表差异的详细日志记录。

默认情况下，禁用此设置。

启用此设置时，请确保启用日志记录设置也处于启用状态。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果该设置没有在此配置，也不在 INI 文件中，则记录错误和常规信息。

“配置文件处理”策略设置

Mar 17, 2016

“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。

删除缓存配置文件前的延迟

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

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

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
- Local
- 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。

如果该设置没有在此配置，也不在 INI 文件中，则不会使用任何模板。

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。

如果该设置没有在此配置，也不在 INI 文件中，则不会使用任何模板。

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。

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。

如果该设置没有在此配置，也不在 INI 文件中，则不会使用任何模板。

“注册表”策略设置

Mar 17, 2016

“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 注册表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，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，此设置处于禁用状态，当用户注销时，会处理 HKCU 注册表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 注册表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，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，此设置处于禁用状态，当用户注销时，会处理 HKCU 注册表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，将处理整个 HKCU。

“流用户配置文件”策略设置

Mar 17, 2016

“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。

始终缓存

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，增强用户体验。

将此设置与 Profile Streaming 设置结合使用。

默认情况下，此设置处于禁用状态，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。

如果未在此处也未在 .ini 文件中配置此设置，则将处于禁用状态。

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 (MB)。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。

如果未在此处也未在 .ini 文件中配置此设置，则将处于禁用状态。

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，Profile Streaming 处于禁用状态。

如果未在此处配置此设置，则将使用 .ini 文件中的值。

如果未在此处也未在 .ini 文件中配置此设置，则将处于禁用状态。

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，此设置处于禁用状态，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。

挂起区域锁定文件超时

此设置指定一个一天为单位的时间段，如果服务器无响应并且用户存储处于锁定状态，则经过这一时间段后，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，并保证用户存储始终包含最新的文件。

默认情况下，此参数设置为 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，将使用默认值。

Receiver 策略设置

Mar 17, 2016

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

Virtual Delivery Agent 策略设置

Mar 17, 2016

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二个地址上进行注册。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。

HDX 3D Pro 策略设置

Mar 17, 2016

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。

启用无损压缩

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。

虚拟 IP 策略设置

Mar 17, 2016

“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。

使用注册表配置 COM 端口和 LPT 端口重定向设置

Mar 17, 2016

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：

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。

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。

Connector for Configuration Manager 2012 策略设置

Mar 17, 2016

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。

间隔使用 ddd.hh:mm:ss 格式进行设置，其中：

- ddd 代表天数，是介于 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 是介于 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。

时间使用 ddd.hh:mm:ss 格式进行设置，其中：

- ddd 代表天数，是介于 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 是介于 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” (服务器当前即将脱机进行维护)

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。

时间使用 ddd.hh:mm:ss 格式进行设置，其中：

- ddd 代表天数，是介于 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 是介于 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。服务器将在 {TIMELEFT} 内脱机进行维护）

强制注销消息框标题

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”（服务器当前即将脱机进行维护）

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。

时间使用 ddd.hh:mm:ss 格式进行设置，其中：

- ddd 代表天数，是介于 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 是介于 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)。

管理

Mar 17, 2016

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。

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 应位于哪个区域。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到此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。

连接租用

通过连接租用功能，用户可以连接和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 高可用性最佳实践。虽然连接租用可以提高连接恢复能力和用户工作效率，但本文还包含 Controller 处于租用连接模式时，与其他功能的可用性、操作和性能相关的注意事项。

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 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

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。Controller 地址可以在安装 VDA 时指定、在 Citrix 策略设置、注册设置中指定或以其他多种方式指定。在站点中添加、移动或删除 Controller 时，VDA 及时获得最新信息至关重要。本文介绍 VDA 注册的方式和时间，更新 Controller 信息的方法以及添加、移动和删除 Controller 的方式。

会话

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。

IPv4/ipv6

此 XenApp 和 XenDesktop 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。本文介绍并举例说明这些部署。本文还介绍确定是使用 IPv4 还是 IPv6 的 Citrix 策略设置。

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。

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。

许可

Mar 17, 2016

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。

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	- Platinum - Enterprise - 高级	并发
XenDesktop	- Platinum - Enterprise - App - 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**。
2. 在“操作”窗格中选择**更改许可证服务器**。
3. 以 name:port 形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**。

区域

Mar 17, 2016

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。

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。

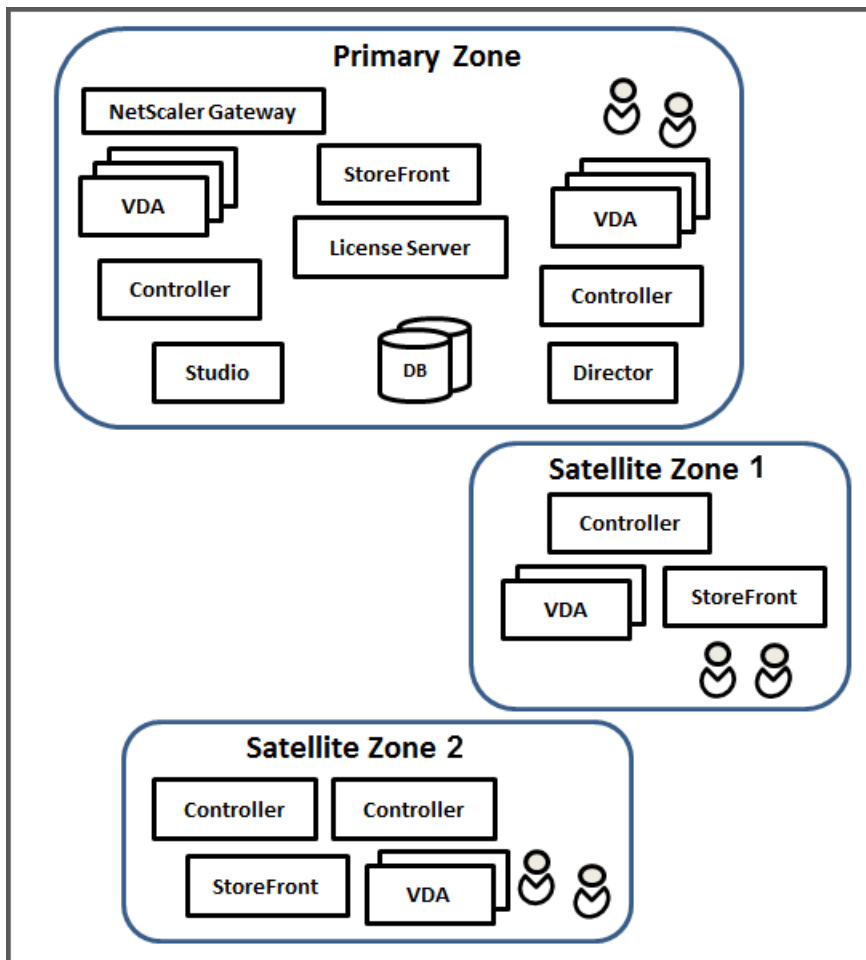
主要区域还应至少包含两个 Controller 以实现冗余，并且可能包含一个或多个安装了与数据库和基础结构紧密配对的应用程序的 VDA。

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，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。）

站点可以包含多种不同类型的卫星区域，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 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。（移动目录时，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。

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。）

注意事项、要求和最佳做法

- 可以将以下项目放置在区域中：Controller、计算机目录和主机连接。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。
- 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。请将其使用的目录和主机连接保留在相同的区域中。
- 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。

创建和管理区域

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. 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. 选择一个或多个项目。
3. 完成以下操作之一：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. 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。

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。

连接和资源

Mar 17, 2016

在本文中：

- [简介](#)
- [创建连接和资源](#)
- [通过现有连接创建连接和资源](#)
- [添加存储](#)
- [编辑存储](#)
- [编辑连接](#)
- [打开或关闭连接的维护模式](#)
- [删除连接](#)
- [重命名连接](#)
- [查看连接上的计算机详细信息](#)
- [管理连接上的计算机](#)
- [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，将创建与托管资源的第一个连接。之后，可以更改此连接并创建新连接。配置连接包括从受支持的虚拟机管理程序或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。

连接类型信息来源

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。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。

VMware

- [VMware 虚拟化环境一文](#)。
- VMware 产品文档。

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。
- 在 Studio 中创建连接时，可以自动导入从 <https://manage.windowsazure.com/publishsettings/index> 下载的发布设置文件中的信息。

Amazon Web Services (AWS)

- [CTX140427](#)。

- 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、可用性区域、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。

Citrix CloudPlatform

- [CTX140428](#)。
- Citrix 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，然后再导入这些值。

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允许与 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

- [CTX202032](#)
- <https://portal.nutanix.com/#/page/docs>

创建连接和资源

在创建连接之前，托管资源必须可用。

1. 在 Studio 导航窗格中，选择**配置 > 托管**。
2. 在“操作”窗格中，选择**添加连接和资源**。
3. 选择**创建新连接**。
4. 在**连接**页面上，选择连接类型并输入连接名称。选择有助于管理员确定主机类型和部署地址的名称。
5. 其他所需信息取决于选择的连接类型。
6. 选择创建虚拟机所要使用的工具。对于提供 GPU 资源的虚拟机管理程序，请选择 **Studio 工具**。
7. 在**存储**页面上，选择存储类型和设备。使用 Machine Creation Services 时，请为新虚拟机选择网络和存储资源。如果使用 XenServer 连接上的共享存储，则可以启用 IntelliCache 来降低存储设备上的负载。有关使用 IntelliCache 的信息，请参阅[下文](#)。
8. 如果连接具有 GPU 功能，请选择使用图形虚拟化的选项，然后选择 GPU 类型和组。
9. 输入资源的名称。

通过现有连接创建连接和资源

1. 在 Studio 导航窗格中，选择**配置 > 托管**。
2. 在“操作”窗格中，选择**添加连接和资源**。
3. 选择**使用现有连接**，然后选择相关连接。
4. 选择创建虚拟机所要使用的工具。对于提供 GPU 资源的虚拟机管理程序，请选择 **Studio 工具**。如果连接具有 GPU 功能，请选择使用图形虚拟化的选项，然后选择 GPU 类型和组。
5. 输入资源的名称。

添加存储

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**添加存储**。
3. 选择要添加的存储。

编辑存储

1. 在 Studio 导航窗格中，选择**配置 > 托管**。
2. 在某个连接下选择一个资源条目，然后在“操作”窗格中选择**编辑存储**。
3. 在**标准存储**页面上，选中或取消选中用于存储虚拟机的存储位置对应的复选框。如果取消选择用于接受新虚拟机的存储位置，该位置将不再接受新虚拟机。现有虚拟机将继续使用该位置（并向其中写入数据）；因此，即使在某个存储位置停止接受新虚拟机后，该位置也有可能满载。
如果使用 Personal vDisk 存储，请同时选中或取消选中 **PvD 存储** 页面上的相应复选框。

编辑连接

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。

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。

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。

- **同步操作(所有类型)**和**同步个人虚拟存储清单更新**设置可指定两个值：一个是可能在此连接上同步发生的最大绝对值，另一个则是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。

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。

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**。
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，也可以针对单个计算机打开或关闭维护模式，请参阅[下文](#)。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

警告：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**。

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。选择某个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。

- **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。

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，IntelliCache 默认情况下处于禁用状态。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。

连接租用

Mar 17, 2016

为确保站点数据库始终可用，Citrix 建议按照 Microsoft 的高可用性最佳实践开始部署容错 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 高可用性最佳实践。

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 <数据库名称> SET OFFLINE WITH ROLLBACK IMMEDIATE
- ALTER DATABASE <数据库名称> SET OFFLINE WITH ROLLBACK AFTER <秒数>

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。

连接租用默认为启用状态。

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。

虚拟 IP 和虚拟环回

Mar 17, 2016

注意：这些功能仅对 Windows Server 2008 R2 和 Windows Server 2012 R2 计算机有效。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。
- 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 地址。
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，则它们将共享每会话 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分配的虚拟地址，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。

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 调用中使用了 localhost 地址（默认为 127.0.0.1），虚拟环回功能只将 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，此设置处于禁用状态。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：

- 环回优先仅在 Windows 2008 R2 上受支持。
- 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。
- 注册表编辑不当可能会导致严重问题，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：<进程列表>

Delivery Controller

Mar 17, 2016

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 — 随着站点活动的增长，Controller 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。

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。

VDA 发现 Controller 的方式

VDA 必须首先向站点的 Controller 进行注册（建立连接），然后该 VDA 才可以使用。VDA 通过检查称为 ListOfDDCs 的 Controller 列表来查找 Controller。ListOfDDCs 包括一个或多个用于将 VDA 指向站点 Controller 的 DNS 项或 IP 地址。为实现负载均衡，VDA 会自动在列表中的所有 Controller 之间分发连接。

除 ListOfDDCs 以外，ListOfSIDs 用于指明 VDA 允许哪些计算机安全 ID (SID) 作为 Controller 与其进行联系。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。

随着在站点中添加和删除 Controller，确保所有 VDA 上的 ListOfDDCs 和 ListOfSIDs 始终包含最新的信息十分重要。如果未更新这些列表，VDA 可能会拒绝由未在列表中的 Controller 所代理的会话启动。无效的项会使虚拟桌面系统软件的启动发生延迟。要确保列表包含最新内容，您可以：

- 使用自动更新功能，以便随着 Controller 的添加或删除自动更新 ListOfDDCs 和 ListOfSIDs。默认情况下，自动更新功能处于启用状态。
- 自我管理 – 也就是说，手动更新用于标识 Controller 的策略或注册表设置。

在 ListOfDDCs 和 ListOfSIDs 中的信息可以来源于部署中的多个位置。VDA 按顺序检查以下位置，并在发现列表的第一个位置停止：

1. 为自动更新功能所维护的静态存储位置。在启用自动更新并且 VDA 在安装后首次成功完成注册后，此位置包含 Controller 信息。（此存储还包括计算机策略信息，这样可以确保在重新启动后保留策略设置。）安装后首次注册时，或者禁用自动更新时，VDA 将检查以下位置：
2. 策略设置（Controller、Controller SID）。
3. 注册表中 Virtual Desktop Agent 注册表项下的 Controller 信息。VDA 安装程序首次将根据在安装 VDA 时指定的信息填充这些值。
4. 基于 OU 的 Controller 发现。这是一种为实现向后兼容性而维护的传统方法。
5. 由 Machine Creation Services 创建的 Personality.ini 文件。

如果 ListOfDDCs 指定多个 Controller，VDA 将尝试以随机顺序连接这些 Controller。ListOfDDCs 还可以包含 Controller 组，

在这些组的名称中，用括号将两个或多个 Controller 项括起。VDA 将尝试连接组中的每个 Controller，然后转向 ListOfDDCs 中的其他项。

对于已从 7.0 之前版本升级的 XenDesktop 用户，自动更新功能将替代先前版本的 CNAME 功能。如有需要，可以手动重新启用 CNAME 功能；但是，要使 DNS 失真继续工作，您将无法同时使用自动更新功能和 CNAME 功能。有关重新启用 CNAME 功能的信息，请参阅 [CTX137960](#)。

有关在包含多个区域的站点中 VDA 尝试进行注册的位置信息，请参阅 [区域](#) 一文。

选择自动更新或自我管理的注意事项

默认情况下，用于启用/禁用自动更新的策略设置处于启用状态。

以下类型的部署无法使用自动更新，而必须使用自我管理。

- 使用 Controller 组的部署。
- 出于安全原因使用 ListOfSIDs 的部署。（对于使用 ListOfSIDs 来降低 Active Directory 负载的部署，可以使用自动更新。）
- 使用 Provisioning Services 但不使用写回磁盘的部署。
- 使用 Controller 或 Controller SID 策略设置的部署。

自动更新

启用控制器自动更新策略 设置位于 Virtual Delivery Agent 类别中。要启用自动更新，请启用策略设置；这是默认设置。要禁用自动更新，请禁用策略设置。

如果启用自动更新，在安装 VDA 时，VDA 将尝试已在安装 VDA 时指定的其中一个 Controller 值中进行注册。安装程序会将在 VDA 安装期间指定的控制器信息写入 ListOfDDC 注册表值。

VDA 注册完成后，该 VDA 所注册的控制器将向该 VDA 发送控制器完全限定的域名 (FQDN) 和安全 ID (SID) 的最新列表。VDA 会将此列表写入自动更新静态存储中。每个控制器还将每隔 90 分钟检查站点配置数据库以获取控制器信息 - 如果自上次检查后添加或删除了控制器，或如果发生策略更改，则控制器会将已更新的列表发送到其注册的 VDA 中。VDA 将接受所接收最新列表中的所有控制器的连接。

如果 VDA 接收的列表不包括其注册的控制器（换句话说，已从站点中删除该控制器），VDA 将从列表中选择控制器并重新注册。VDA 完成注册或重新注册后，会收到更新的列表。

例如：

1. 某部署中包括三个控制器：A、B 和 C。VDA 安装后，向控制器 B 注册（该控制器在 VDA 安装期间指定）。
2. 将 D 和 E 两个控制器添加到站点中。VDA 会在 90 分钟内收到更新的列表，并将接受来自控制器 A、B、C、D 和 E 的连接。（只有在重新启动 VDA 后，负载才会均衡分散到所有控制器上。）
3. 将控制器 B 从站点中删除。VDA 会在 90 分钟内收到更新的列表，因为自上次检查后控制器已发生更改。在第 1 步中安装的 VDA 已向控制器 B 注册，但该控制器已不在列表中，这样 VDA 将从当前列表（A、C、D 和 E）中选择控制器并重新注册。

自我管理

如果不使用自动更新功能，则在站点中添加、移动或删除 Delivery Controller 后，必须更新站点中每个 VDA 的 Citrix 策略设置或注册表值。还可以使用组策略对象更新注册表更改。

要使用 Citrix 策略设置进行自我管理，请执行以下操作：

1. 更新控制器策略设置中指定的 FQDN 值。此策略设置位于 Virtual Delivery Agent 类别中。
2. 如果部署中还使用 ListOfSIDs，请更新在控制器 SID 策略设置中指定的 SID 值。

要使用注册表进行自我管理，请执行以下操作：

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. 更新 ListOfDDCs 注册表项，该注册表项用于列出站点中所有控制器的 FQDN。（此注册表项相当于 Active Directory 站点 OU。）各个值之间以空格分隔。使用括号将控制器组括起来。

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 用于控制器发现；如果在 VDA 安装期间指定站点 OU，则 FarmGUID 位于此位置。

2. 或者，也可以更新 ListOfSIDs 注册表项：

HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)

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。

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。

基于 Active Directory OU 的控制器发现

支持此 Delivery Controller 发现方法主要是为实现向后兼容性，这种方法仅适用于 Virtual Delivery Agent (VDA) for Windows Desktop OS，而不适用于 VDA for Windows Server OS。进行基于 Active Directory 的发现时，要求站点中的所有计算机都是域的成员，并且在控制器所使用的域与桌面所使用的域之间存在相互信任的关系。如果您使用此方法，则必须在每个桌面注册表中配置 OU 的 GUID。

要执行基于 OU 的控制器发现，请运行控制器的 Set-ADControllerDiscovery.ps1 PowerShell 脚本（每个控制器都包含此脚本，位于 \$Env:ProgramFiles\Citrix\Broker\Service\Setup Scripts 文件夹中）。要运行该脚本，必须在父 OU 上拥有 CreateChild 权限，以及完全管理员权限。

如果希望桌面通过 Active Directory 发现站点中的控制器，在创建站点时，必须在 Active Directory 中创建相应的组织单位 (OU)。可以在包含您计算机的林的任何域中创建该 OU。最佳做法是，将站点中的控制器也包含在该 OU 内，但这不是强制或必需的条件。具有适当权限的域管理员可以创建 OU 作为一个空容器，然后通过该 OU 将管理权限委派给 Citrix 管理员。

该脚本会创建多个关键的对象。但只创建和使用标准的 Active Directory 对象。扩展架构是没有必要的。

- 一个控制器安全组。站点中所有控制器的计算机帐户必须是此安全组中的成员。只有当控制器是此安全组的成员时，站点中的桌面才会接受来自这些控制器的数据。
确保所有控制器对运行 VDA 的所有虚拟桌面都具有“从网络中访问此计算机”权限。为此，您可以向控制器安全组授予此权限。如果控制器没有此权限，VDA 将不会注册。
- 一个服务连接点 (SCP) 对象，包含有关站点的信息（例如站点名称）。如果您使用 Active Directory 用户和计算机管理工具来检查站点 OU，可能需要启用“查看”菜单中的“高级功能”，才能看到 SCP 对象。
- 一个称为 RegistrationServices 的容器，在站点 OU 中创建。容器中针对站点内的每个控制器包含一个 SCP 对象。每次启动控制器时，都会验证其 SCP 内容并根据需要进行更新。

如果在完成初始安装后，可能有多个管理员要添加和删除控制器，则他们需要对 RegistrationServices 容器具有创建和删除子项的权限，对控制器安全组具有写属性权限；这些权限自动授予运行 Set-ADControllerDiscovery.ps1 脚本的管理员。域管理员或原始安装管理员可以授予这些权限，Citrix 建议您设置安全组来执行此任务。

如果使用站点 OU：

- 只有在安装或卸载此软件，或者控制器启动并需要更新其 SCP 中的信息时（例如，由于重命名了控制器或更改了通信端口），信息才会写入 Active Directory。默认情况下，Set-ADControllerDiscovery.ps1 脚本会相应设置对于站点 OU 中对象的权限，为控制器授予对其 SCP 的写访问权限。站点 OU 中对象的内容用于在桌面与控制器之间建立信任关系。请确保：
 - 只有经过授权的管理员才可以使用安全组的访问控制列表 (ACL) 在控制器安全组中添加或删除计算机。
 - 只有经过授权的管理员和各自的控制器才可以更改控制器 SCP 中的信息。
- 如果部署使用复制，请确保了解潜在的延迟；有关详细信息，请参阅 Microsoft 文档。如果要在域控制器位于多个 Active

Directory 站点的域中创建站点 OU，这一点尤其重要。如果您在最初创建站点 OU 时、安装或卸载控制器时或者更改控制器名称或通信端口时，对 Active Directory 进行了更改，则在信息被复制到适当的域控制器之前，这些更改可能对桌面不可见，具体取决于桌面、控制器和域控制器的位置。此类复制延迟的表现包括桌面无法与控制器建立通信，因此不可用于用户连接。

- 此软件在 Active Directory 中使用多个标准的计算机对象属性来管理桌面。根据您的部署，存储于桌面的 Active Directory 记录中的计算机对象完全限定的域名，可以包含在返回给用户用以建立连接的连接设置中。请确保此信息与 DNS 环境中的信息一致。

要使用基于 OU 的 Controller 发现将 Controller 移动到其他站点，请按照上述移动 Controller 的指示操作。从旧站点删除 Controller（第 2 步）后，运行 PowerShell 脚本 **Set-ADControllerDiscover -sync**。该脚本会将 OU 与控制器的当前设置进行同步。加入现有站点（第 3 步）后，在新站点中的所有控制器上运行相同脚本。

会话

Apr 25, 2016

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。对于许多移动工作者（如医院的医护工作者）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[通过交付组管理会话](#)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。如果连接已断开，用户的显示内容将冻结，且光标变成一个旋转的沙漏，直至用户到达通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。

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;<秒数>

其中，<秒数> 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。

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，

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 <交付组名称> -SessionReconnection <值> -LeasingBehavior Allowed | Disallowed
```

对于应用程序会话：

```
Set-BrokerAppEntitlementPolicyRule <交付组名称> -SessionReconnection <值> -LeasingBehavior Allowed | Disallowed
```

其中，<值> 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。

在 Studio 中使用搜索

Mar 17, 2016

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“Expand Search”（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“Client (IP)”（客户端(IP)）和“Is”（是），然后输入设备的 IP 地址。
- 要查找活动的会话，请使用 Session State（会话状态）、Is（是）和 Connected（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。

标记

Mar 17, 2016

标记是指用于标识计算机、应用程序、交付组、策略等项目的字符串。在创建标记并将其添加到一个项目中后，您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，如果您希望仅显示已针对测试人员优化的应用程序，可为这些应用程序添加名为“测试”的标记。然后，使用标记“测试”过滤 Studio 搜索结果。同样，如果您希望仅显示包含测试团队成员的交付组，可为包含测试团队成员的交付组添加“测试”标记，然后使用标记“测试”筛选 Studio 搜索结果。

- 将 Citrix 策略应用（分配）到具有（不具有）指定标记的应用程序、计算机或交付组中。

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。

管理标记

在 Studio 中选择计算机、应用程序或交付组，然后选择“操作”窗格中的**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。

- 如果启用了相应复选框，则表示该标记已添加到所选项目中。
- 如果您选择的是一个组，并且复选框包含连字符，则表示该标记已添加到该组中的部分项目（而非所有项目）中。

可以从“管理标记”对话框中执行以下操作：

- 要添加或删除标记，请启用或清除要添加或删除的标记旁边的复选框。
- 要创建标记，请选择**创建标记**。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**。
- 要编辑标记，请选择一个标记，然后选择**编辑标记**。输入新的名称和/或说明，然后单击**保存**。一次只能编辑一个标记。
- 要删除一个或多个标记，请选择相应标记，然后选择**删除标记**。“删除标记”对话框将列出当前使用所选标记的项目数量。单击某个项目可显示更多信息；例如，如果两台计算机会受到影响，则单击该项目将显示这两台计算机的名称。查看受影响项目后，请确认您是否要删除这些标记。

IPv4/IPv6 支持

Mar 17, 2016

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。

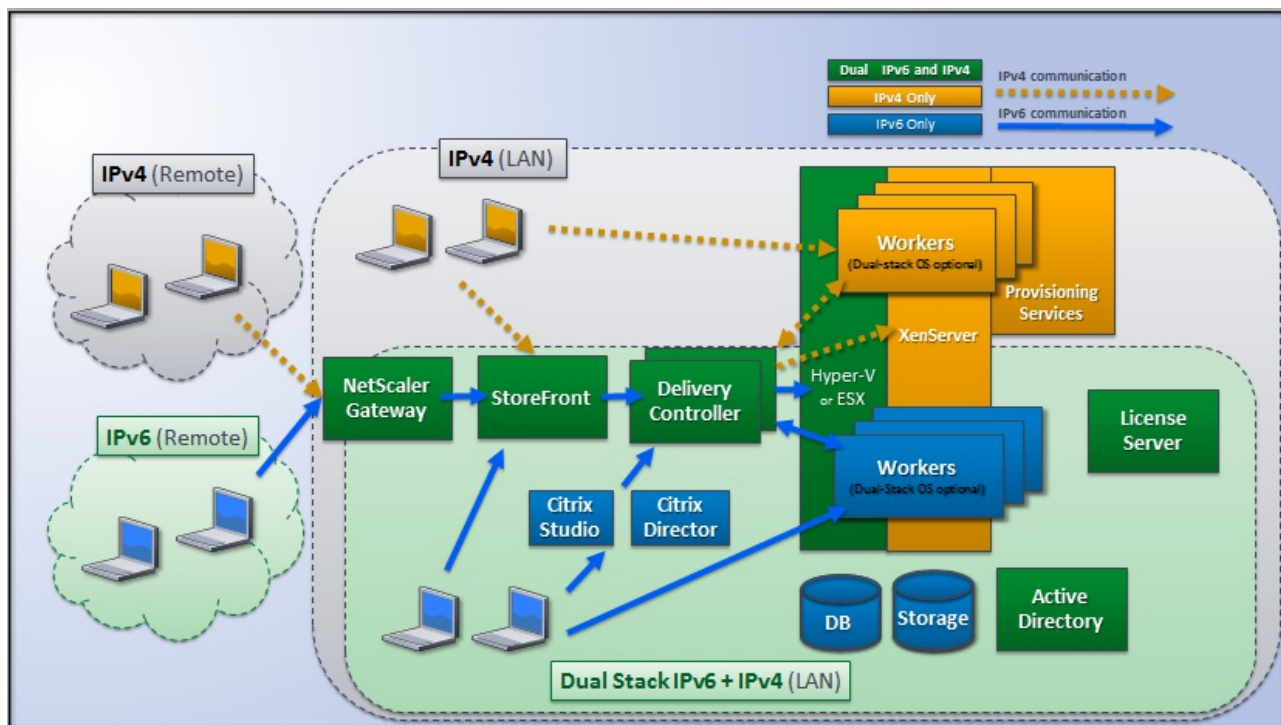
IPv6 通信通过与 Virtual Delivery Agent (VDA) 连接相关的两个 Citrix 策略设置进行控制：

- 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。

双协议栈 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 EdgeSight

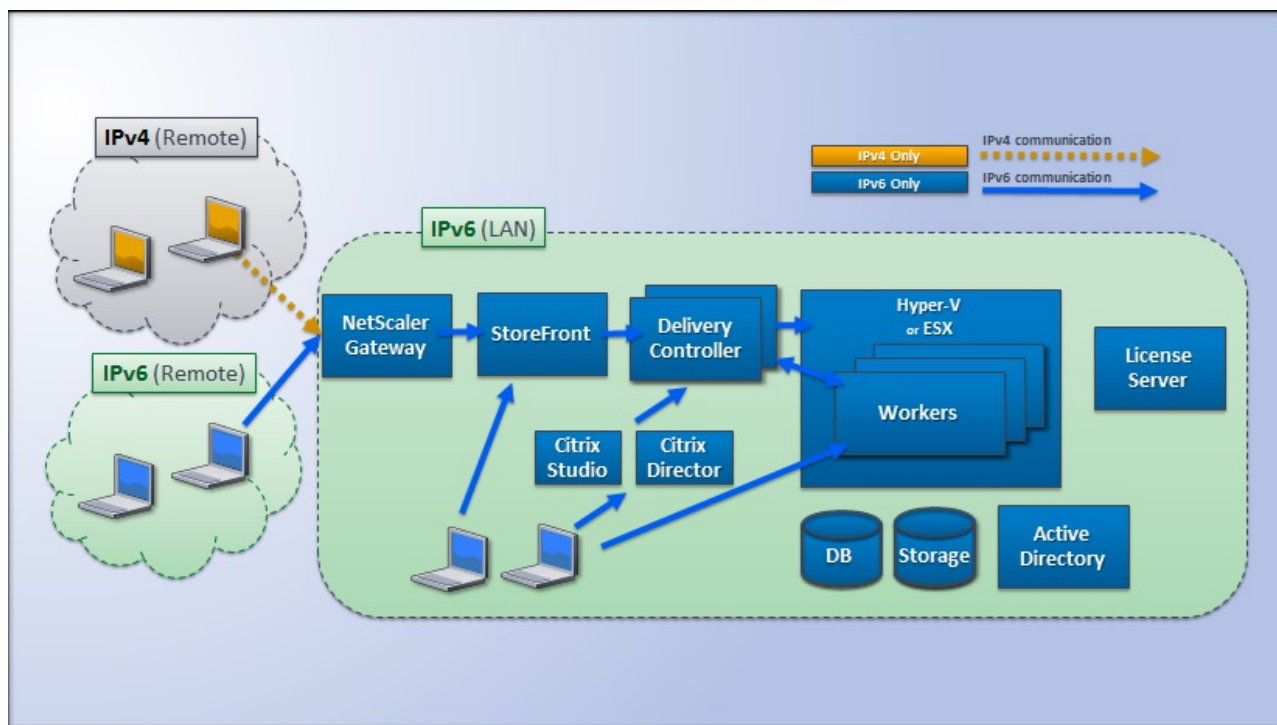
对于此部署：

- 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。
- 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二个地址上注册。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。

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。

客户端文件夹重定向

Mar 17, 2016

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）。

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。

用户配置文件

Mar 17, 2016

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可能继续存在。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

- **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方针。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
始终缓存	已启用（备注 1）	已禁用（备注 2）
活动写回	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
始终缓存	已禁用（备注 6）	已禁用
活动写回	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) 来确保在登录后立即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立即在本地缓存。
3. 禁用活动写回，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

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) 来确保在登录后立即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立即在本地缓存。
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？
My Documents	是	是
Application Data	否	否
联系人	是	是

文件夹 桌面	已在 Windows 8 中重定向？ 是	已在 Windows Server 2008 中重定向？ 否
下载	否	否
收藏夹	是	是
链接	是	否
我的音乐	是	是
图片收藏	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](#)

含和排除项目。

Citrix Insight Services

Jun 17, 2016

Citrix Insight Services (CIS) 是用于执行诊断和故障排除的 Citrix 旗舰平台。它使技术用户（客户、合作伙伴和工程师）能够自行诊断和修复问题，并优化他们的环境。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）。

此版本的 XenApp 和 XenDesktop 支持以下 CIS 工具和技术。

Citrix 客户体验改善计划 (CEIP)

选择加入 CEIP 后，系统会将匿名统计数据和使用信息发送到 Citrix 以帮助它改善 Citrix 产品的质量和性能。有关详细信息，请访问 <http://more.citrix.com/XD-CEIP>。

在执行以下任务时，您可以选择加入 CEIP。此列表并不全面；我们会不断提供更多可加入该计划的机会。

- 创建 XenApp 或 XenDesktop 站点。
- 升级 XenApp 或 XenDesktop 站点。
- 通过命令行在打印服务器上安装通用打印服务器 UpsServer 组件。
- 安装 Session Recording Server。

拨打住宅电话技术预览

Citrix 拨打住宅电话功能会定期收集您的系统和产品配置以及性能、错误和其他信息。此信息会随后发送到 CIS，以供 Citrix 支持和产品团队主动解决问题时使用。

有关拨打住宅电话功能的最新信息，请访问以下网站（需要 Citrix 帐户凭据）：

- 关于：<https://www.citrix.com/community/cx/call-home.html>
- 博客：<https://www.citrix.com/blogs/2016/01/21/citrix-call-home-technology-preview/>
- 下载：<https://www.citrix.com/downloads/xenapp/betas-and-tech-previews/call-home.html>

Monitor

Mar 07, 2016

Administrators and help-desk personnel can monitor XenApp and XenDesktop Sites using a variety of features and tools. Using these tools, you can monitor

- User sessions and session use
- Logon performance
- Connections and machines, including failures
- Load evaluation
- Historical trends
- Infrastructure

Citrix Director

Director is a real-time web tool you can use to monitor, troubleshoot, and perform support tasks for end users.

For details, see the [Director](#) articles.

Session Recording

Session Recording allows you to record the on-screen activity of any user's session, over any type of connection, from any server running XenApp subject to corporate policy and regulatory compliance. Session Recording records, catalogs, and archives sessions for retrieval and playback.

Session Recording uses flexible policies to trigger recordings of application sessions automatically. This enables IT to monitor and examine user activity of applications — such as financial operations and healthcare patient information systems — supporting internal controls for regulatory compliance and security monitoring. Similarly, Session Recording also aids in technical support by speeding problem identification and time-to-resolution.

For details, see the [Session Recording](#) articles.

Configuration Logging

Configuration Logging is a feature that allows administrators to keep track of administrative changes to a Site. Configuration Logging can help administrators diagnose and troubleshoot problems after configuration changes are made, assist change management and track configurations, and report administration activity.

You can view and generate reports about logged information from Studio. You can also view logged items in Director with the Trend View interface to provide notifications of configuration changes. This feature is useful for administrators who do not have access to Studio.

The Trends View gives historical data of configuration changes over a period of time so administrators can assess what changes were made to the Site, when they were made, and who made them to find the cause of an issue. This view sorts configuration information into three categories.

- Connection Failures
- Failed Desktop Machines
- Failed Server Machines

For details about how to enable and configure Configuration Logging, see the [Configuration Logging](#) article. The [Director](#) articles describe how to view logged information from that tool.

Monitor Service API using the OData protocol

Administrators can use the Site's Monitor Service API to search historical data using the OData protocol. This allows IT to analyze historical trends for planning purposes, to perform detailed troubleshooting of connection and machine failures, and extract information for feeding into other tools and processes.

The Monitor Service schema provides the following types of data:

- Data relating to connection failures
- Machines in a failure state
- Session usage
- Logon duration
- Load balancing data

For details, see the [Monitor Service OData API](#) articles.

Personal vDisk diagnostic tool

Use the PvD diagnostic tool to monitor changes made by users to the user and application parts of their personal vDisks, such as applications they have installed and files they have modified.

For details, see the [Personal vDisk monitoring](#) article.

Session Recording

Apr 25, 2016

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服务器操作系统 VDI 计算机托管的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，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 可以捕获屏幕更新，并对这些更新进行存档（包括鼠标活动，以及安全视频录制中可见的击键输出），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。 用户由于难以重现问题而致电技术支持时，客服人员可启用用户会话记录。再次出现该问题时，Session Recording 会提供该错误的时间戳直观记录，该记录可用于更加快速地进行故障排除。

Session Recording 入门

Apr 25, 2016

执行以下步骤之后，即可开始录制和查看 XenApp 和 XenDesktop 会话。

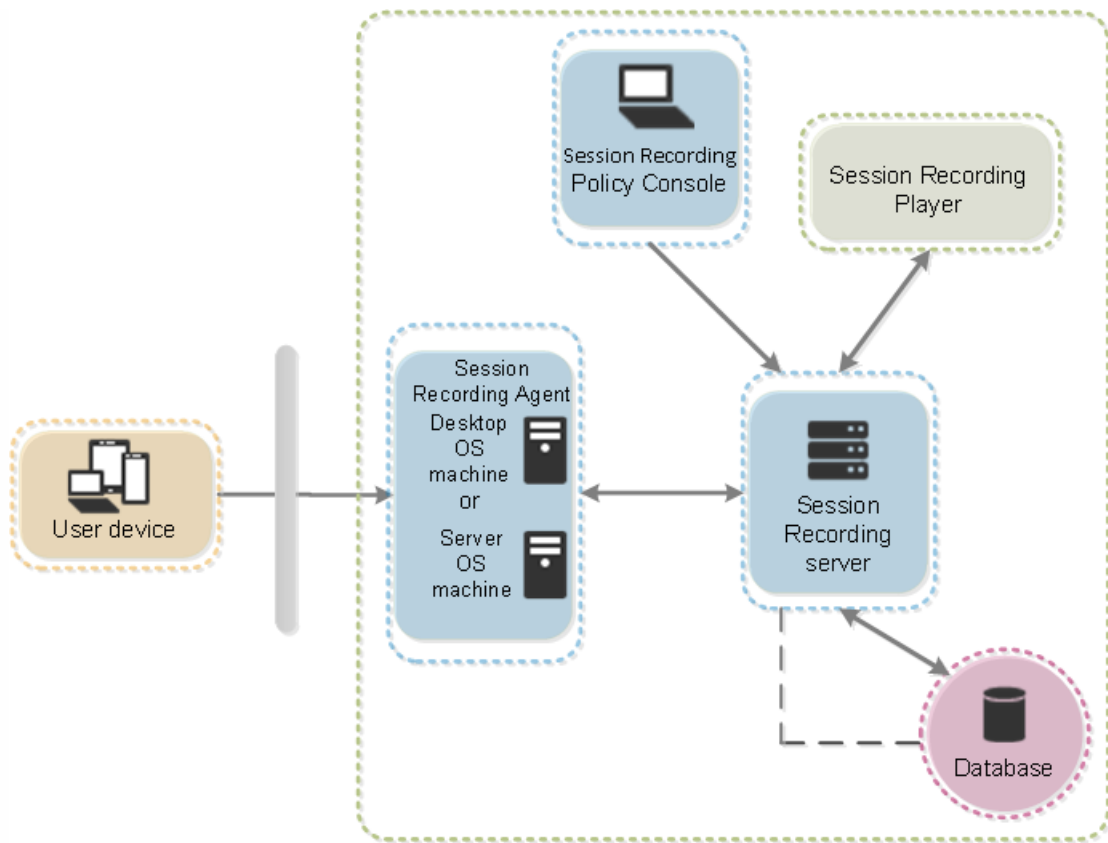
1. 熟悉 Session Recording 组件。
2. 选择适用于您的环境的部署方案。
3. 验证安装要求。
4. 安装 Windows 角色和功能必备项。
5. 安装 Session Recording。
6. 配置 Session Recording 组件以允许录制和查看会话。

Session Recording 包括 5 个组件：

- **Session Recording Agent**。安装在每台服务器操作系统和 VDI 计算机上，用于启用录制。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。
- **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，用来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 安装在服务器操作系统计算机上。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 的服务器操作系统计算机进行通信。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。



计划部署

Apr 25, 2016

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 属性中配置该行为。

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。请记住，一次只能将一个代理指向一台服务器。

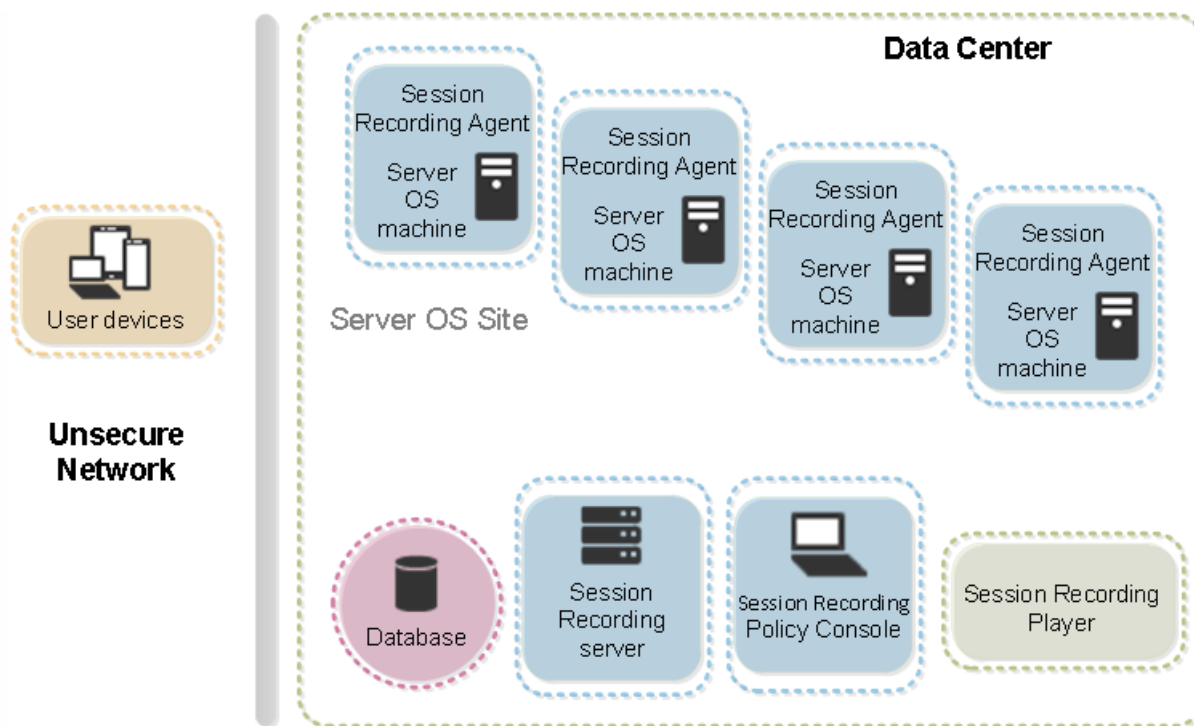
推荐的部署方案

以下是推荐的两种 Session Recording 部署配置：

- 在单台服务器操作系统计算机上部署 Session Recording Agent。
- 在站点上的多台服务器操作系统或工作站操作系统计算机上部署 Session Recording Agent。

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。在站点中每台服务器操作系统计算机上安装 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，全部位于防火墙背后，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。
- Session Recording 不支持在一次部署中使用两个或更多 Session Recording Server 组成群集。
- 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 2014 Express Edition 或 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，这些设置处于禁用状态，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 文档。
- 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 录制策略规则相冲突。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。

安全性建议

Apr 25, 2016

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。

规划部署时，请考虑如下安全性建议：

- 确保正确地隔离企业网络、Session Recording 系统和单个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 建议不要向常规会话用户分配 VDA 管理员特权，尤其是使用 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 计算机的核心内存转储。

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>。

+ 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。

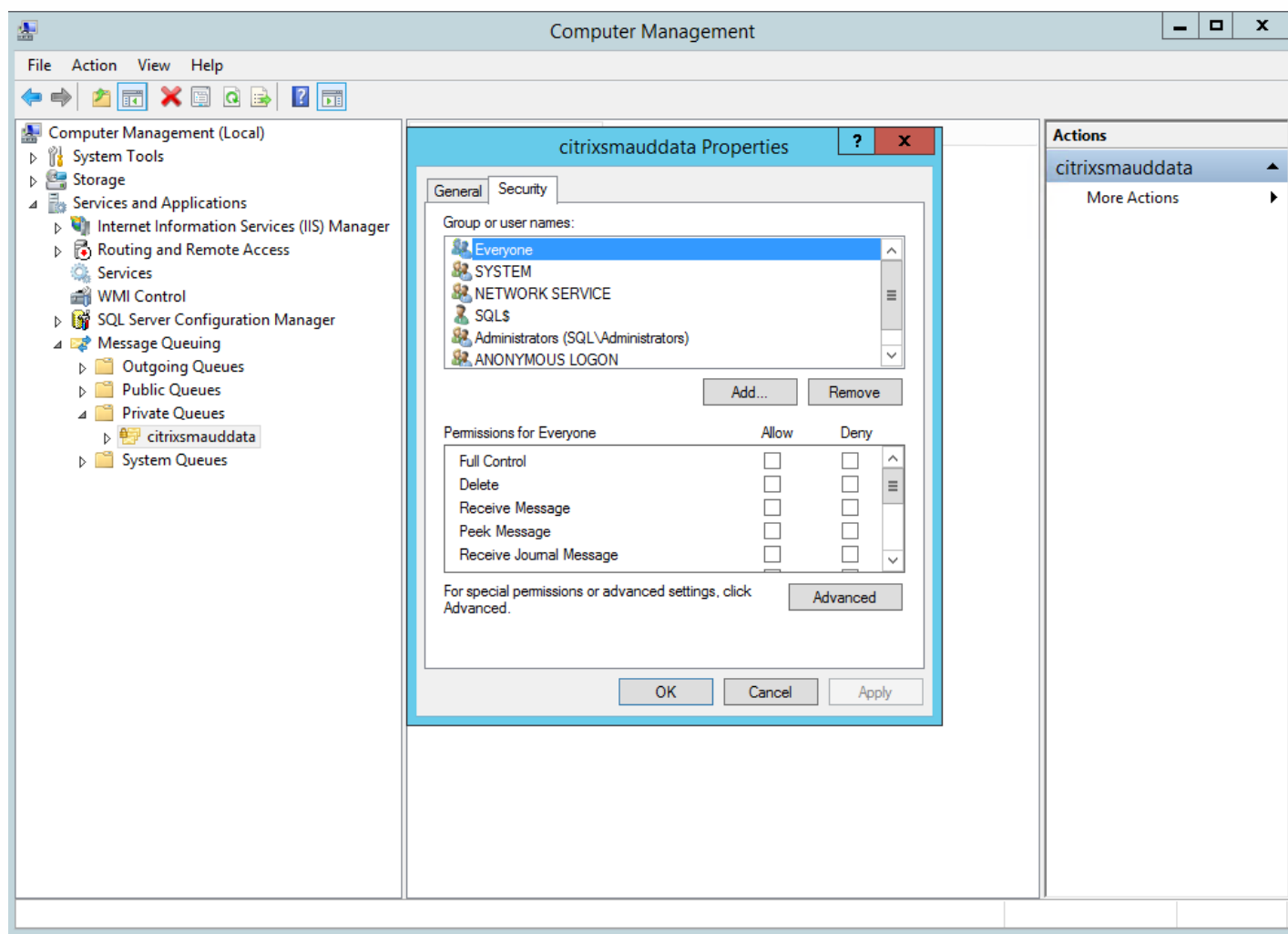
+ 在切换到远程 ICA 会话之前，用户应关闭所有可能暴露敏感信息的应用程序。

+ 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。

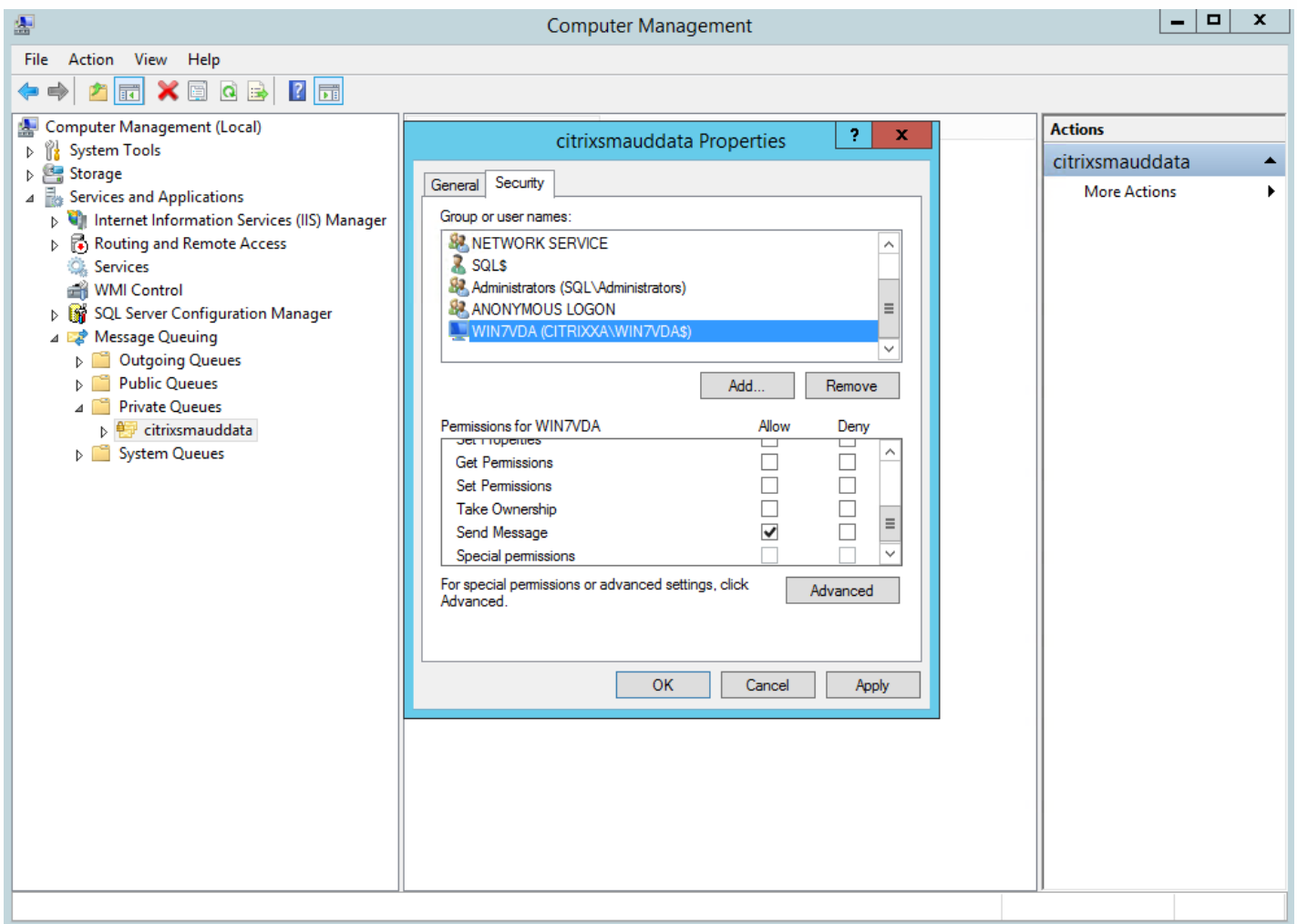
+ 仅允许使用自动身份验证方法（例如单点登录、智能卡）访问已发布的桌面或应用程序。

- 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 HKLM\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 HKLM\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。



5) 添加要向此服务器发送 MSMQ 数据的计算机或 VDA 计算机安全组，并为其授予“发送消息”权限。



- 正确保护 Session Record Server 和 Session Recording Agent 的事件日志。Citrix 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 对话框中列出的 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 1.2 并禁用 SSLv2、SSLv3 和 RC4 密码。有关详细信息，请参阅 Microsoft 文章 <http://support.microsoft.com/default.aspx?scid=kb;en-us;187498> 和 <http://support.microsoft.com/kb/245030/zh-cn>。
- 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 Properties”中。

- 请勿在 Amazon Web Service (AWS) 等公有云上部署 Session Recording。
- 按照加密密钥长度和加密算法的 NSIT 指南进行操作。

有关配置 Session Recording 功能的信息，请参阅 <http://support.citrix.com/article/CTX200868>。

可扩展性注意事项

Mar 17, 2016

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 <http://support.citrix.com/article/CTX200869>。

在本文中：

硬件建议

磁盘和存储硬件

网络容量

计算机处理能力

部署多台 Session Recording Server

数据库可扩展性

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 5000 个 Microsoft Outlook 会话，每个会话的大小为 20MB。在这种情况下，数据输入速率约为 3.5MBps。（5000 个会话乘以 20MB，除以 8 小时，再除以每小时 3600 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 2GB 到 4GB RAM

超过这些规格不会显著提高性能。

部署多台 Session Recording Server

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 数据库需要安装 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 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 可扩展性的指南进行操作。

安装 Session Recording

Apr 25, 2016

本文包含以下部分：

[安装核对表](#)

[使用脚本添加 Windows 角色和功能必备项](#)

[安装 Session Recording Administration 组件](#)

[安装 Session Recording 数据库](#)

[安装 Session Recording Server](#)

[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

开始安装之前，请完成以下列表中的步骤：

	步骤
	开始安装之前，请安装必备项。请参阅 系统要求 和 使用脚本添加 Windows 角色和功能必备项 。
	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。
	从 Citrix 下载页面下载 Session Recording，下载位置为： XenApp > https://www.citrix.com.cn/downloads/xenapp.html 或 XenDesktop > https://www.citrix.com.cn/downloads/xendesktop.html

	如果使用 SSL 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，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。
- 如果要将 Machine Creation Services (MCS) 或 Provisioning Services 与 XenApp 结合使用，请为服务器准备一个唯一的 QMId；请参阅“已知问题”中的说明。 执行此步骤失败可能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。
- 如果要使用 HTTPS，请为 TLS/HTTPS 配置服务器证书。

Session Recording 安装文件：

- **Session Recording Administration 文件**
 - Broker_PowerShellSnapIn_x64.msi
 - SessionRecordingAdministrationx64.msi
- **Session Recording Agent 文件**
 - SessionRecordingAgentx64.msi
- **Session Recording Player 文件**
 - SessionRecordingPlayer.msi

使用脚本添加 Windows 角色和功能必备项

要使 Session Recording 正常运行，必须在安装 Session Recording 组件之前添加某些 Windows 角色和功能必备项。 鉴于您可能无法查找和安装某些角色和功能，本文提供了使用 Citrix 脚本的过程。 在安装 Session Recording 组件之前，请运行此脚本以安装 Windows 角色和功能必备项。

安装 Windows 角色和功能必备项

1. 如果您要使用 Citrix 脚本，请参阅[用于安装 Windows 角色和功能必备项的脚本](#)。

2. 在要安装 Session Recording Administration 组件的计算机上执行以下操作：

a) 确保在 PowerShell 中将执行策略设置为 **RemoteSigned** 或 **Unrestricted**。

Set-ExecutionPolicy RemoteSigned

b) 以管理员身份启动命令提示窗口，然后运行此命令：

powershell.exe -file InstallPrereqsforSessionRecordingAdministration.ps1

此脚本将显示已成功添加的功能，然后会停止。

c) 执行此脚本之后，请务必按照公司政策将此执行策略设置为正确的值。

3. 在要计划安装 Session Recording Agent 组件的计算机上执行以下操作：

a) 确保在 PowerShell 中将执行策略设置为 **RemoteSigned** 或 **Unrestricted**。

Set-ExecutionPolicy RemoteSigned

b) 以管理员身份启动命令提示窗口，然后运行此命令：

```
powershell.exe -file InstallPrereqsforSessionRecordingAgent.ps1
```

此脚本将显示已成功添加的功能，然后会停止。

c) 执行此脚本之后，请务必按照公司政策将此执行策略设置为正确的值。

4. 安装完 Windows 角色和功能之后，请继续安装 Session Recording。

安装 Session Recording Administration 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。

开始安装 Session Recording Administration 组件之前，请务必安装所有必备项。请参阅 [Session Recording 系统要求](#)。

要提高安全性，可以在安装数据库后删除这些权限。

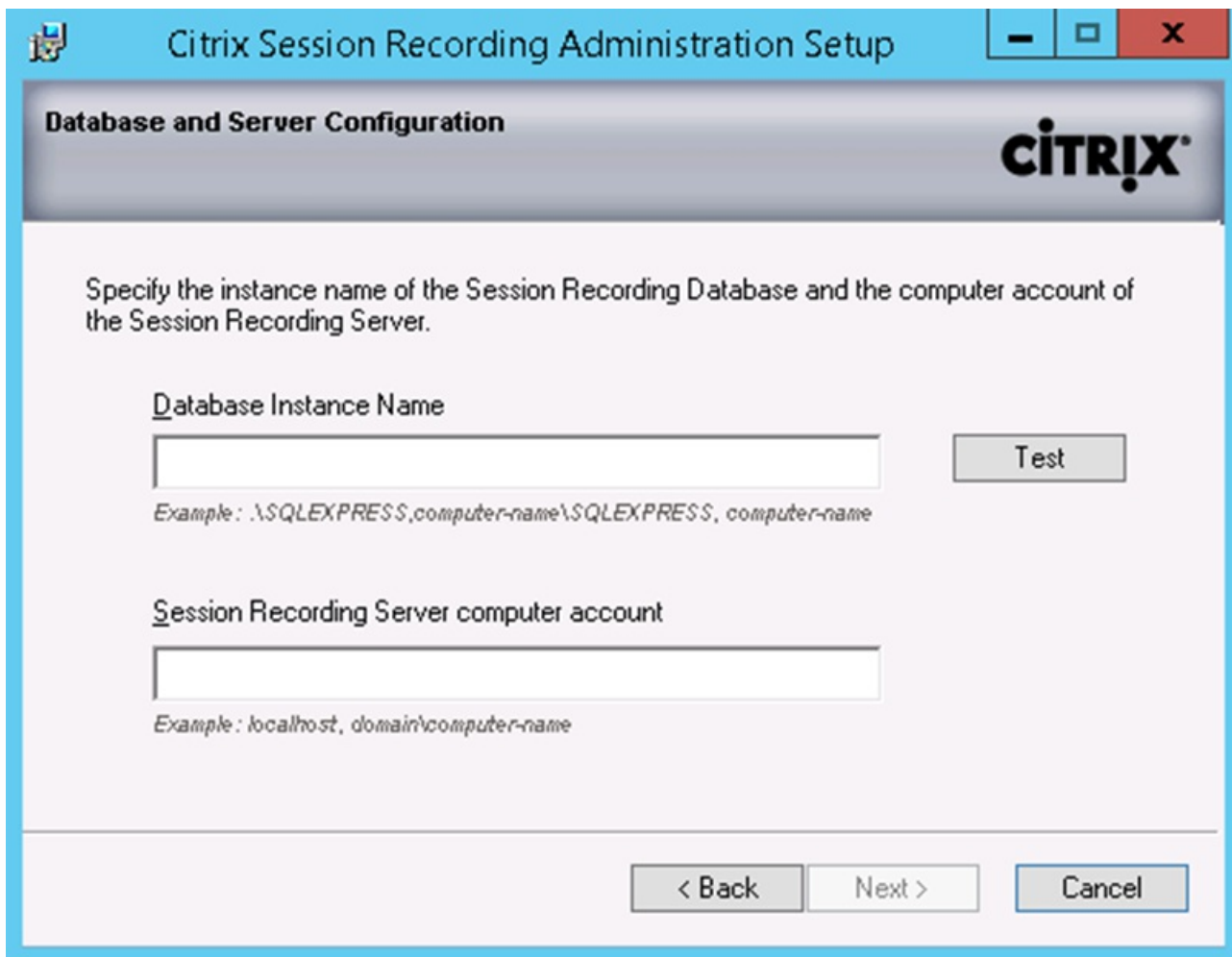
1. 运行 **Broker_PowerShellSnapIn_x64.msi** 并按照说明完成安装。
2. 以管理员身份启动 Windows 命令提示符，然后运行命令 **msiexec /i SessionRecordingAdministrationx64.msi** 或双击 .msi 文件。
3. 在安装用户界面上，选择下一步并接受许可协议。
4. 在“Session Recording Administration 安装程序”屏幕上，选择要安装的 Session Recording Administration 组件。

安装 Session Recording 数据库

开始安装 Session Recording 数据库之前，请务必安装所有必备项。请参阅 [Session Recording 系统要求](#)。

一般来说，Session Recording 数据库组件和 Microsoft SQL Server 部署有以下三种类型：

- 部署 1：在同一台服务器上安装 Session Recording Server 和 Session Recording 数据库，并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。
 - 部署 3：在一台服务器上安装 Session Recording Server，并在与 Session Recording Server 计算机不同的同一台计算机上安装 Session Recording 数据库和 Microsoft SQL Server。（**不推荐**）。
1. 在“数据库配置”页面上：
 - 部署 1 和 2：在 Session Recording Server 计算机帐户字段中键入 **localhost**。
 - 部署 3：按以下格式键入托管 Session Recording Server 的计算机的名称：**domain\computer-name**。Session Recording Server 计算机帐户即为用于访问数据库的用户帐户。



The image shows a Windows-style dialog box titled "Citrix Session Recording Administration Setup". The subtitle is "Database and Server Configuration". The Citrix logo is in the top right corner. The main text says: "Specify the instance name of the Session Recording Database and the computer account of the Session Recording Server." There are two input fields. The first is labeled "Database Instance Name" and has a "Test" button to its right. Below it is an example: "Example: .\SQLEXPRESS,computer-name\SQLEXPRESS, computer-name". The second input field is labeled "Session Recording Server computer account" and has an example below it: "Example: localhost, domain\computer-name". At the bottom are three buttons: "< Back", "Next >", and "Cancel".

如果数据库实例不是您在设置实例时配置的命名实例，您可以仅使用 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。

单击**测试**，测试与 SQL Server 的连接。确保当前用户具有公共 SQL Server 角色权限；否则，测试将由于权限限制而失败。然后，单击**下一步**继续安装。

2. 按照说明完成安装。安装期间，如果当前用户不是数据库管理员，则会显示一个对话框，提示需要数据库管理员的凭据和 sysadmin 服务器角色权限。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**。

安装完成后，就不再需要 sysadmin 服务器角色权限了，可以从当前用户安全删除。

Important

您无法更改 **CitrixSessionRecording** 数据库名称。

安装 Session Recording Server

开始安装 Session Recording Server 之前，请务必安装所有必备项。请参阅 [Session Recording 系统要求](#)。

1. 在“数据库实例名称”文本框中输入 SQL Server 的名称。如果要使用命名实例，请输入 *computer-name\instance-name*，否则，请仅输入计算机名称。
2. 单击**测试**以测试与 SQL Server 的连接。确保当前用户具有公共 SQL Server 角色权限；否则，测试将由于权限限制而失败。然后，单击**下一步**以继续安装，并按照说明完成安装。
3. 在安装向导的结尾，您可以选择是否参与 Citrix 客户体验改善计划。加入此计划时，匿名统计信息和使用情况信息将发送到 Citrix；有关详细信息，请参阅[关于 Citrix 客户体验改善计划 \(CEIP\)](#)。

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/FQDN、从 Session Recording Agent 到 Session Recording Broker 的端口和连接类型 (http/https)。

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。

1. 使用服务器管理器在 XenApp 7.8 服务器操作系统 VDA 或 XenDesktop 7.8 VDI 上安装 .NET Framework 3.5 和 Microsoft 消息队列 (MSMQ) 并启用 HTTP 支持。
2. 以管理员身份启动 Windows 命令提示窗口，然后运行此命令：

msiexec /i SessionRecordingAgentx64.msi

或

msiexec /i SessionRecordingAgent.msi

或双击 .msi 文件。

根据平台类型使用正确的 .msi 文件：对于 32 位系统，请使用 **SessionRecordingAgent.msi**；对于 64 位系统，请使用 **SessionRecordingAgentx64.msi**。

3. 在安装用户界面上，选择下一步并接受许可协议。
4. 在“Session Recording Agent 配置”页面上，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。

The image shows a Windows-style window titled "Citrix Session Recording Agent Setup". The window has a header bar with the Citrix logo and the title. Below the header, the main area is titled "Session Recording Agent Configuration". A note says: "Enter the Session Recording Server connection information below. Note that you can modify these values at a later date by running the Session Recording Agent properties." There are three input fields: "Session Recording Server Name" (empty), "Protocol" (a dropdown menu with "HTTP" and "HTTPS" options, where "HTTPS" is selected), and "Port" (containing the number "443"). Below the "Port" field is a "Test" button. At the bottom of the window are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

Session Recording 默认安装使用 HTTPS/TLS 来确保通信安全。如果未配置 TLS，请使用 HTTP。为此，请导航到 Session Recording Broker 站点，在 IIS 管理控制台中取消选中 SSL。打开 SSL 设置，取消选中“需要 SSL”复选框。

5. 按照说明完成安装。

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。

运行 **SessionRecordingPlayer.msi** 并按照说明完成安装。

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。

在 **64 位系统** 中：

```
msiexec /i SessionRecordingAgentx64.msi sessionrecordingservername=yourservername
```

sessionrecordingbrokerprotoco=yourbrokerprotocol sessionrecordingbrokerport=yourbrokerport /!*v yourinstallationlog /q

在 32 位系统中：

msiexec /i SessionRecordingAgent.msi sessionrecordingservername=yourservername

sessionrecordingbrokerprotoco=yourbrokerprotocol sessionrecordingbrokerport=yourbrokerport /!*v yourinstallationlog /q

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 HTTP 或 HTTPS，表示 Session Recording Agent 用于与 Session Recording Broker 进行通信的协议；如未指定，此值默认为 HTTPS。

yourbrokerport 是一个整数，表示 Session Recording Agent 用于与 Session Recording Broker 进行通信的端口。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。

*/!*v* 用于指定详细模式日志记录

yourinstallationlog 是所创建的安装日志文件的位置。

/q 用于指定无提示模式。

升级 Session Recording

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。可以将 Session Recording 7.6.0（或更高版本）升级为最新发布的（当前）Session Recording 版本。

要求、准备和限制

注意：不能从技术预览版进行升级。

- 必须在安装了相应 Session Recording 组件的计算机上使用 Session Recording 安装程序的图形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，则您必须具有此数据库的 sysadmin 角色权限才能升级 Session Recording 数据库；否则，系统会在升级期间要求您提供 sysadmin 角色凭据。
- 如果您不想同时升级所有 Session Recording Agent，则可以将 Session Recording Agent 7.6.0（或更高版本）与最新发布的（当前）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。
- 如果开始升级时存在实时录制会话，录制有时可能无法完成。
- 请查看以下升级顺序，以便进行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. 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。

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”中的卸载或删除程序功能。要删除 Session Recording 数据库，您必须具有与安装时同样的 sysadmin SQL Server 角色权限。

用于添加 Windows 角色和功能必备项的脚本

Mar 17, 2016

您可以使用以下脚本来安装 Session Recording 正常运行所需的 Windows 角色和功能必备项。有关详细信息，请参阅[使用脚本添加 Windows 角色和功能必备项](#)。

安装 Session Recording Administration 的必备项

复制

```
<#

.Synopsis

    Installs Prereqs for Session Recording Administration

.Description

    Supports Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 R2.

    Install below windows feature on this machine:

    -Application Development - ASP.NET 4.5 on Server 2012 and Server 2012 R2, Application Development - ASP.NET on Server 2008 R2

    -Security - Windows Authentication

    -Management Tools - IIS 6 Management Compatibility

        IIS 6 Metabase Compatibility

        IIS 6 WMI Compatibility

        IIS 6 Scripting Tools

        IIS 6 Management Console

    -Microsoft Message Queuing (MSMQ), with Active Directory integration disabled, and MSMQ HTTP support enabled.

#>

function AddFeatures($featurename)

{

    try

    {

        $feature=Get-WindowsFeature | ? {$_.DisplayName -eq $featurename -or $_.Name -eq $featurename}

        Add-WindowsFeature $feature

    }

}
```

```

}

catch

{

    Write-Host "Addition of Windows feature $featurename failed"

    Exit 1

}

Write-Host "Addition of Windows feature $featurename succeeded"

}

$system= gwmi win32_operatingSystem | select name

if (-not (($system -Like "*Microsoft Windows Server 2012*") -or ($system -Like "*Microsoft Windows Server 2008 R2*")))

{

    Write-Host("This is not a supported server platform. Installation aborted.")

    Exit

}

# Start to install Windows feature

Import-Module ServerManager

if ($system -Like "*Microsoft Windows Server 2012*")

{

    AddFeatures('Web-Asp-Net45') #ASP.NET 4.5

}

if($system -like "*Microsoft Windows Server 2008 R2*")

{

    AddFeatures('Web-Asp-Net') #ASP.NET

```

```

}

AddFeatures('Web-Mgmt-Console') #IIS Management Console

AddFeatures('Web-Windows-Auth') # Windows Authentication

AddFeatures('Web-Metabase') #IIS 6 Metabase Compatibility

AddFeatures('Web-WMI') #IIS 6 WMI Compatibility

AddFeatures('Web-Lgcy-Scripting')#IIS 6 Scripting Tools

AddFeatures('Web-Lgcy-Mgmt-Console') #IIS 6 Management Console

AddFeatures('MSMQ-HTTP-Support') #MSMQ HTTP Support

```

安装 Session Recording Agent 的必备项

复制

```

<#

.Synopsis

    Installs Prereqs for Session Recording Administration

.Description

    Supports Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows 7, Windows 8, Windows 8.1 and Windows 10.

    Install below windows feature on this machine:

    -Microsoft Message Queuing (MSMQ), with Active Directory integration disabled, and MSMQ HTTP support enabled.

#>

function AddFeatures($featurename)

{

    try

    {

        $feature=Get-WindowsFeature | ? {$_.DisplayName -eq $featurename -or $_.Name -eq $featurename}

        Add-WindowsFeature $feature

    }

}

```



```

catch

{

    Write-Host "Addition of Windows feature $featurename failed"

    Exit 1

}

Write-Host "Addition of Windows feature $featurename succeeded"

}

# Start to install Windows feature

$system= gwmi win32_operatingSystem | select name

if (-not (($system -Like "**Microsoft Windows Server 2012**") -or ($system -Like "**Microsoft Windows Server 2008 R2**")-or ($system -Like "**

{

    Write-Host("This is not a supported platform. Installation aborted.")

    Exit

}

if ($system -Like "**Microsoft Windows Server**")

{

    Import-Module ServerManager

    AddFeatures('MSMQ') #Message Queuing

    AddFeatures('MSMQ-HTTP-Support')#MSMQ HTTP Support

}

else

{

    try

```

```
{

if($system -Like "**Microsoft Windows 7*")

{

    dism /online /enable-feature /featurename:IIS-WebServerRole /featurename:IIS-WebServer /featurename:IIS-IIS6ManagementCo

    dism /online /enable-feature /featurename:MSMQ-Container

    dism /online /enable-feature /featurename:MSMQ-Server

    dism /online /enable-feature /featurename:MSMQ-HTTP

}

else

{

    dism /online /enable-feature /featurename:MSMQ-HTTP /all

}

}

catch

{

    Write-Host "Addition of Windows feature MSMQ HTTP Support failed"

    Exit 1

}

write-Host "Addition of Windows feature MSMQ HTTP Support succeeded"

}
```

配置 Session Recording

Mar 17, 2016

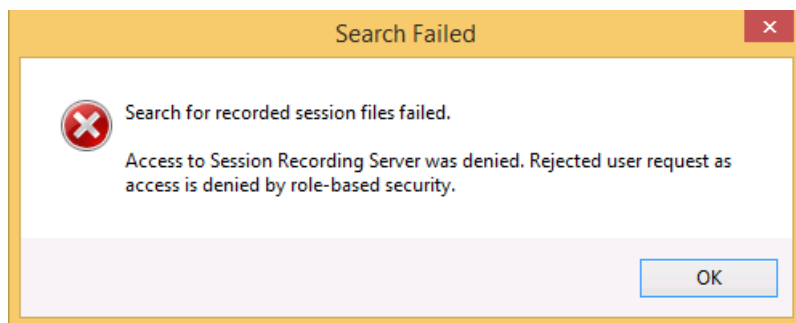
配置用于播放和录制会话的 Session Recording

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：

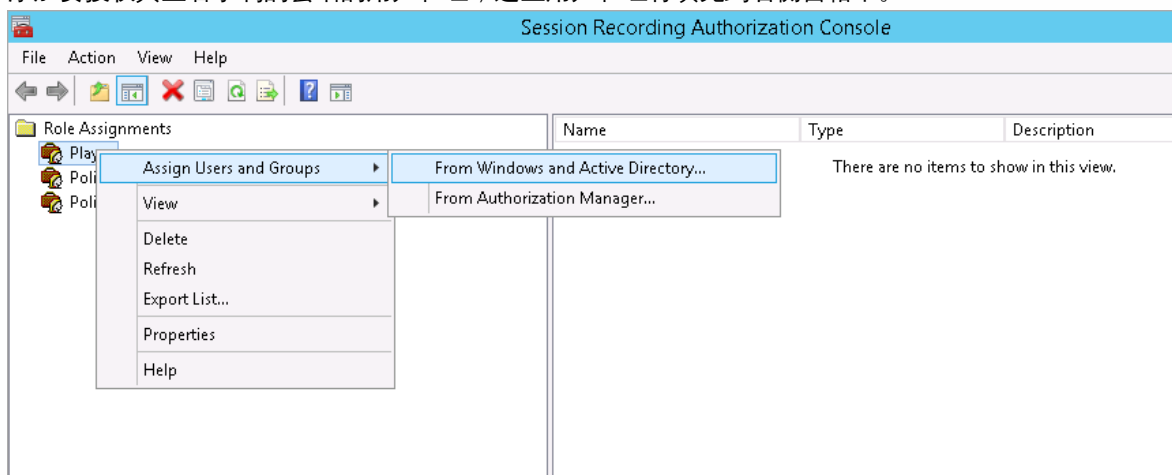
- 授权用户播放录制件
- 授权用户管理录制策略
- 将活动录制策略设置为会话录制策略
- 配置自定义策略
- 配置用于连接至 Session Recording Server 的 Session Recording Player

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。

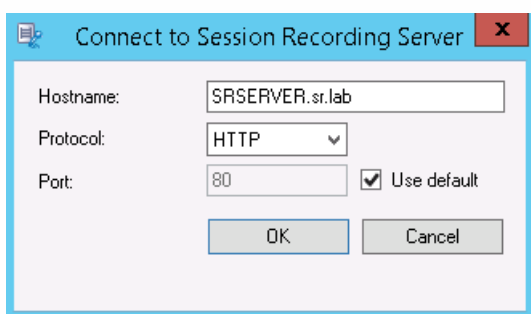
1. 以管理员身份登录托管 Session Recording Server 的计算机。
2. 启动 Session Recording Authorization 控制台并选择 策略管理员。
3. 添加能够管理录制策略的用户和组。

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，但一次只能运行一条活动策略。

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. 如果系统提示连接到 Session Recording Server 弹出窗口，请确保托管 Session Recording Server 的计算机名称、协议和端口正确无误。



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。系统将显示一个弹出窗口，通知用户正在录制其会话。
 - 录制每个人但不通知。如果选择此策略，则会录制所有会话。系统不显示用于通知用户正在录制其会话的弹出窗口。
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。

注意：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 策略控制台内的“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](#)。

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台 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 的计算机名称或 Internet 协议 (IP) 地址，然后选择协议。默认情况

下，Session 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. 如果要配置 Session Recording Player，使其能够连接到多台 Session Recording Server，请对每台 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 Internet 协议 (IP) 地址。
5. 在 **Session Recording Storage Manager 消息队列** 部分中，选择 Session Recording Storage Manager 用于通信的协议并修改默认端口号（如果需要）。
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。

授予用户访问权限

Mar 17, 2016

注意：出于安全原因，请只授予用户执行特定功能（例如查看录制的会话）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。

创建并激活录制策略

Mar 17, 2016

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。

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。

使用系统策略

Session Recording 提供了以下系统策略：

- **不录制。** 如果选择此策略，则不会录制会话。此为默认策略；如果未指定其他策略，则不录制会话。
- **录制每个人并通知。** 如果选择此策略，则会录制所有会话。系统将显示一个弹出窗口，通知用户正在录制其会话。
- **录制每个人但不通知。** 如果选择此策略，则会录制所有会话。系统不显示用于通知用户正在录制其会话的弹出窗口。

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记录。）此记录操作将指定不记录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记录并通知。）此记录操作将指定记录满足规则条件的会话。系统将显示一个弹出窗口，通知用户正在录制其会话。
- **录制但不通知。**（在规则向导中选择启用会话记录而不通知。）此记录操作将指定记录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，请至少选择以下选项之一来创建规则条件：

- **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。

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该会话。

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。

配置自定义策略

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 策略控制台并选择左窗格中的**录制策略**，然后从菜单栏中选择**操作 > Add New Policy**（增加新策略）。
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** - 可以选择一个选项，也可以选择三个选项的任意组合形式。

用户或组

已发布资源

交付组或计算机

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。
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。

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 OK（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 Add New Policy（添加新策略）。左侧窗格中将显示名为新策略的策略。
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 或单击新名称之外的任意位置。
8. 右键单击策略，然后从菜单中选择 Add New Rule（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 OK（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 OK（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。

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。但在某些情况下，文件滚动后新策略才生效。文件达到最大大小限制时会发生滚动。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。

创建通知消息

Mar 17, 2016

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。默认通知消息如下：“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，请关闭这些程序。”用户可以单击确定以放弃该窗口并继续会话。

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。

可以您所选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。通知消息所用的语言与用户的首选区域设置相对应。

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 Properties。
3. 在 Session Recording Server Properties 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。

禁用或启用录制

Mar 17, 2016

在要录制会话的每台服务器操作系统计算机上安装 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：“用户已打开浏览器”。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：

- 可使用“Session Recording Agent Properties”启用要插入自定义事件的每台服务器上的设置。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。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。

启用服务器上的自定义事件记录

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。

启用或禁用实时会话播放和播放保护

Mar 17, 2016

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。查看当前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 服务器传送数据的过程中实际上存在 1 至 2 秒的延迟。

查看未完成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 Properties。
3. 在 Session Recording Server Properties 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。

启用和禁用数字签名

Mar 17, 2016

如果您在安装了 Session Recording 组件的计算机上安装了证书，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 Properties。
3. 在 Session Recording Server Properties 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 Properties。
3. 在 Session Recording Server Properties 中，单击签名选项卡。
4. 单击清除。

指定录制件的存储位置

Mar 17, 2016

使用“Session Recording Server Properties”可指定录制件的存储位置以及存档录制件的还原位置。

注意：要存档文件或还原删除的文件，请使用 icldb 命令。

指定记录文件的位置

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 Properties。
3. 在 Session Recording Server Properties 中，单击存储选项卡。
4. 使用文件存储目录列表，来管理录制的存储目录。

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。

指定存档文件的还原目录

默认情况下，存档的录制件会还原到托管 Session Recording Server 的计算机的 drive:\SessionRecordingsRestore 目录中。可以更改存档录制件的还原目录。

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 Properties。
3. 在 Session Recording Server Properties 中，单击存储选项卡。
4. 在归档文件的还原目录字段中，键入已还原的归档文件的目录。

指定录制的文件大小

Mar 17, 2016

录制文件大小越大，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都会限制为 1 GB，超过此限制后，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，而不考虑文件大小的指定值，这一时间是您可以输入的最小值。文件大小超过 1 GB 属此规则的例外情况。

为文件指定最大限制

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 Properties。
3. 在 Session Recording Server Properties 中，单击滚动选项卡。
4. 输入一个 10 至 1024 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）。

查看录制

Mar 17, 2016

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。

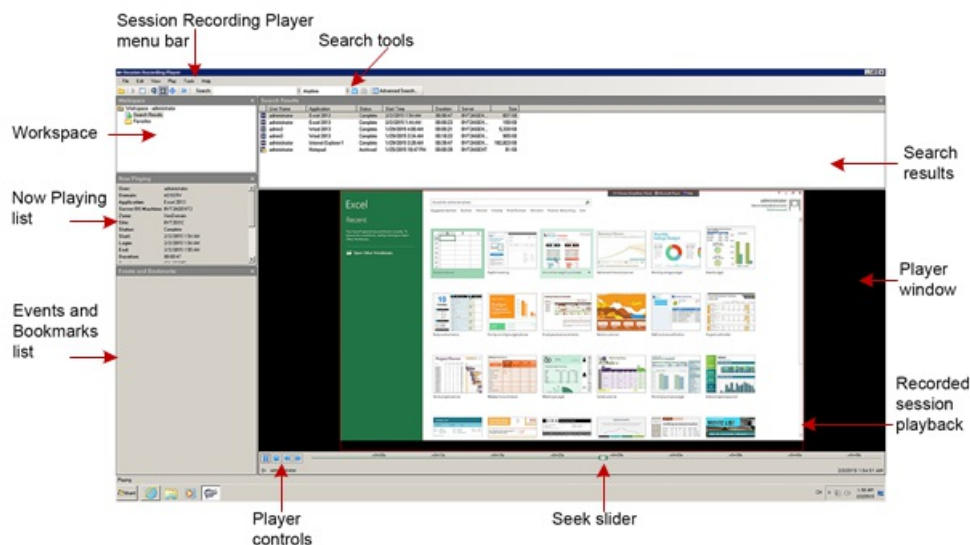
注意：Session Recording 管理员必须授予用户访问录制的服务器操作系统计算机会话的权限。如果您被拒绝访问查看会话，请与 Session Recording 管理员联系。

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. 从开始菜单上选择 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. 从开始菜单上选择 Session Recording Player。
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. 从开始菜单上选择 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。

打开和播放录制件

Mar 17, 2016

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。

打开和播放搜索结果区域中的记录

1. 登录到安装了 Session Recording Player 的工作站。
2. 从开始菜单上选择 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

通过访问文件打开和播放录制件

录制的会话文件名以 i_ 开头，后面依次是唯一的字母数字文件 ID、.icl 和 .icle 文件扩展名：.icl 是未应用播放保护的录制件，而 .icle 是应用了播放保护的录制件。Session Recording 将录制的会话文件保存在包含会话录制日期的目录结构中。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. 从开始菜单上选择 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 workstation 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 workstation，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 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。

创建“收藏夹”子文件夹：

1. 登录到安装了 Session Recording Player 的工作站。
2. 从开始菜单上选择 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。

搜索录制的会话

Mar 17, 2016

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（搜索中可以显示的会话的最大数量），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. 从开始菜单上选择 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 15 万个以上条目的结果。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. 从开始菜单上选择 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、服务器操作系统计算机、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. 单击搜索以启动搜索。

提示：可以保存和检索高级搜索查询。在高级搜索对话框内单击保存可保存当前的查询。在高级搜索对话框内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会话录制件的最大数量，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. 从开始菜单上选择 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。

播放录制的会话

Mar 17, 2016

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搜寻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：

键：	搜寻操作：
主页	搜寻到开头。
End	搜寻到结尾。

鼠标右键	向前搜寻 5 秒。
向左键	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 + 向右键	向前搜寻 30 秒。
Ctrl + 向左键	向后搜寻 30 秒。
Page Down	向前搜寻 1 分钟。
Page Up	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. 从开始菜单上选择 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。

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。

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. 从开始菜单上选择 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。

使用事件和书签

Mar 17, 2016

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下方显示为圆点。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. 从开始菜单上选择 Session Recording Player。
3. 将鼠标指针移动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、只显示书签或显示全部。

插入书签

1. 登录到安装了 Session Recording Player 的工作站。
2. 从开始菜单上选择 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. 使用默认标签书签添加书签，或创建附注：
 - 要使用默认标签书签添加书签，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. 从开始菜单上选择 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。

删除书签

1. 登录到安装了 Session Recording Player 的工作站。
2. 从开始菜单上选择 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. 从开始菜单上选择 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：
 - 在播放器窗口下方的区域中，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。

更改播放显示

Mar 17, 2016

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、以全屏模式显示播放、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。

以全屏模式显示播放器窗口

1. 登录到安装了 Session Recording Player 的工作站。
2. 从开始菜单上选择 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. 从开始菜单上选择 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. 从开始菜单上选择 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) 在提供高质量图像的同时会缩小图像。与使用“高质量”选项时相比，图像的绘制速度更快，但图像和文本的锐度要差一些。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) 在提供高质量图像和文本的同时会缩小图像。使用此选项可能会导致图像的绘制速度比使用“快速呈现”选项慢得多。

平移图像

1. 登录到安装了 Session Recording Player 的工作站。
2. 从开始菜单上选择 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。

在会话录制件周围显示红色边框

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。

缓存录制的会话文件

Mar 17, 2016

每次打开录制的会话文件时，Session Recording Player 都会从录制的存储位置下载该文件。如果您经常下载相同的文件，您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。录制内容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文件，从而为新录制文件释放空间。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. 从开始菜单上选择 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。

Session Recording 故障排除

Mar 17, 2016

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

Session Recording Agent 无法连接

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。此异常文本会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。导致此错误的原因有：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

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”具有对此文件夹的写入权限。否则，请手动添加写入权限。

Session Recording Server 无法连接到 Session Recording 数据库

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：

Event Source:

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。

Unable to connect to the 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。

解决方案：

- Microsoft SQL Server 2008 R2 Express Edition、Microsoft SQL Server 2012 Express Edition 或 Microsoft SQL Server 2014 Express Edition 安装在独立服务器上，并且为 Session Recording 配置的服务或设置不正确。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。请参阅 Microsoft 文章：<https://msdn.microsoft.com/zh-cn/library/cc646023.aspx>。

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。

未录制会话

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 的服务器操作系统计算机上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，请在单独的服务器操作系统计算机上发布冲突的应用程序。
- **未启用录制。** 默认情况下，在服务器操作系统计算机上安装 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 服务必须在服务器操作系统计算机上运行，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。

无法查看实时会话播放

如果在使用 Session Recording Player 查看录制件时遇到困难，屏幕上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 Properties 对话框中，选择播放选项卡，然后选择允许实时会话播放复选框。

录制损坏或不完整

使用 Session Recording Player 查看录制件时，如果录制件损坏或不完整，则 Session Recording Agent 的事件日志还会显示警告消息。

Event Source: Citrix Session Recording Storage Manager

Description: Data lost while recording file （事件源：Citrix Session Recording Storage Manager 描述：录制文件 期间数据丢失）

使用 Machine Creation Services (MCS) 或 Provisioning Services 创建安装了已配置的主映像和 Microsoft Message Queuing (MSMQ) 的 VDA 时通常会出现此问题。在这种情况下，VDA 的 QMId 与 MSMQ 相同。

解决方案：为每个 VDA 创建唯一的 QMId。 [已知问题](#) 中介绍了解决方案。

安装 Session Recording 数据库或 Session Recording Server 时，测试数据库实例的连接性失败。

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。

解决方案：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。

验证组件连接

Mar 17, 2016

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。

验证 Session Recording Agent 是否已连接

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 Server 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. 验证服务器操作系统计算机是否可以访问作为 Session Recording Server 的值给定的服务器。

注意：检查应用程序事件日志中是否记录了错误和警告。

验证 Session Recording Server 是否已连接

警告：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 实例中安装的 Session Recording 数据库。

验证 Session Recording 数据库是否已连接

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。

测试 IIS 连接

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 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。

如果您在浏览器中看到 XML 文档，则表明运行 Session Recording Agent 的计算机已通过配置协议连接到托管 Session Recording Server 的计算机。

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。

如果您在浏览器中看到 XML 文档，则表明运行 Session Recording Player 的计算机已通过配置协议连接到托管 Session Recording Server 的计算机。

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协议连接到托管 Session Recording Server 的计算机。

对证书问题进行故障排除

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。

如果 Session Recording Player 失败，搜索录制件

Mar 17, 2016

如果使用 Session Recording Player 搜索录制件时遇到困难，屏幕上可能显示以下错误消息：

- 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* 是 Session Recording Player 尝试连接到的服务器名称。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。
- 访问被拒绝错误。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器角色。
- 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。

MSMQ 故障排除

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 对话框中连接选项卡上所选的协议一致），请执行步骤 3。
 - 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（例如该服务器仅接受安全连接），请将 Session Recording Agent Properties 对话框中列出的 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 citrixmauddata。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。

更改通信协议

Mar 17, 2016

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。如果希望使用 HTTP 来代替 HTTPS，必须更改多项设置。

将 HTTP 用作通信协议

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. 在每个 Session Recording Agent Properties 对话框中将协议设置从“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 Properties。
 3. 在 Session Recording Agent Properties 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，然后选择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，然后选择确定以进行连接。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。

恢复为将 HTTPS 用作通信协议

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. 在每个 Session Recording Agent Properties 对话框中将协议设置从“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 Properties。
 3. 在 **Session Recording Agent Properties** 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，然后选择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，然后选择确定以进行连接。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。

参考：管理您的数据库记录

Mar 17, 2016

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 软件的服务器的驱动器:\Program Files\Citrix\SessionRecording\Server\Bin 目录中。

快速参考表

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，请在命令提示窗口处键入驱动：\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。

version 命令	说明
/l	显示 Session Recording 数据库架构版本。 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。

第三方声明

Mar 17, 2016

Session Recording 可能包含根据以下条款许可的第三方软件组件。此列表是在截止到列出之日使用第三方软件生成的。此列表可能会变更具体的产品版本并且可能不完整；此列表“按原样”提供。在适用法律允许的范围内，CITRIX 或其供应商对于此列表或其准确性或完整性，或使用或分发此列表造成的结果概不负责，也不做任何明示、暗示、法定或其他形式的担保。使用或分发此列表表示您同意，在任何情况下，CITRIX 对于因使用或分发此列表造成的任何特殊的、直接的、间接的或后果性的损害或任何其他损害不承担任何法律责任。

MMC .NET Library

根据 Common Public License 1.0 版许可。

配置日志记录

Mar 17, 2016

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 2.0 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，配置日志记录功能处于启用状态，它使用创建站点时所创建的数据库（站点配置数据库）。Citrix 强烈建议您在创建站点后尽快更改配置日志记录数据库的位置。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。
- 通过注册表和直接访问数据库进行的更改，或来自 Studio、Director 或 PowerShell 以外的源的更改。
- 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更改）。

管理配置日志记录

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，配置日志记录处于启用状态，强制日志记录处于禁用状态。

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**启用日志记录**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**禁用日志记录**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，请清除**数据库断开连接时允许更改**复选框。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**启用配置日志记录**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，请选中**数据库断开连接时允许更改**复选框。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

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

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。

监视个人虚拟磁盘

Mar 17, 2016

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它们修改的文件。更改存储在—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`。

`Software.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 `changes the user made to the 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-lvmSupervisor.log`、`PvDActivation.log`、`PvDSvc.log`、`PvDWMI.log`、`SysVol-lvmSupervisor.log` 和 `vDeskService-<#>.log`，但是这些文件会被移动到选定的位置。

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：

- 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。

Director

May 12, 2016

在本文中：

[关于 Director](#)

[部署和配置 Director](#)

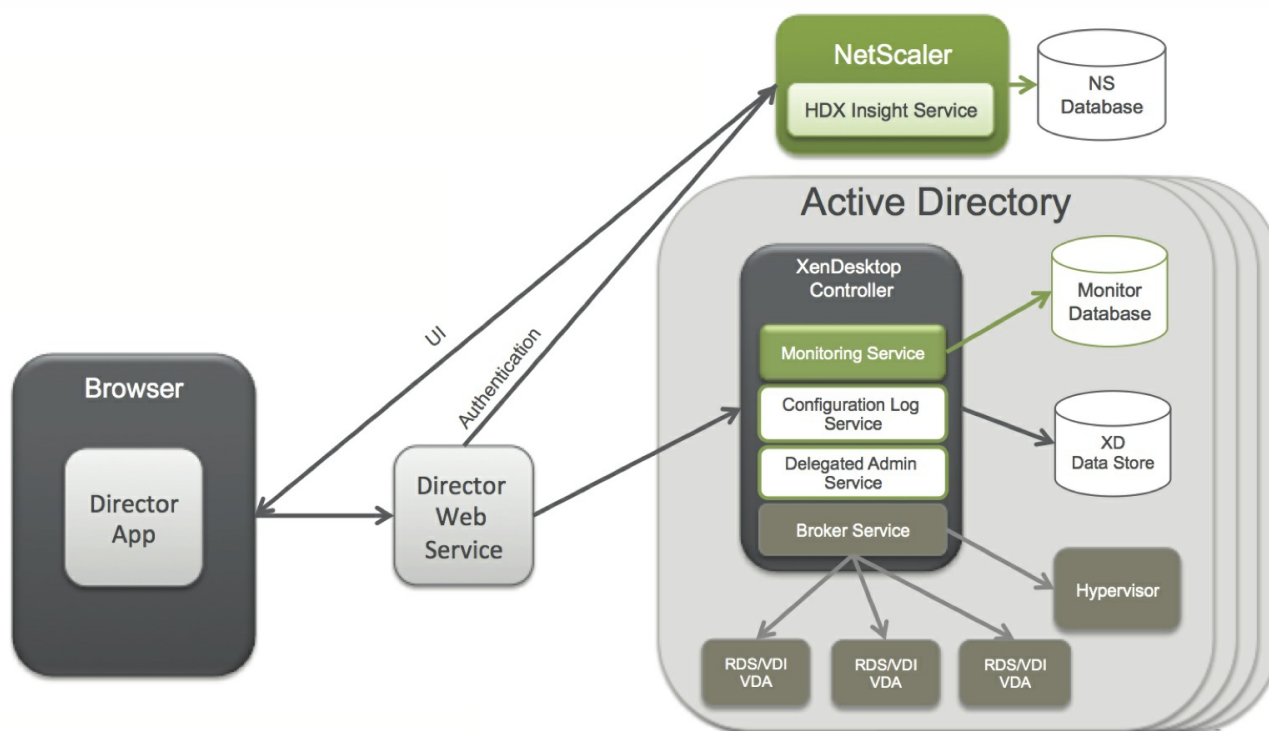
[安装 Director](#)

[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 是一款实时 Web 工具，管理员可以利用此工具进行监视、排除故障和为用户执行支持任务。



Director 可以访问：

- 使用集成 EdgeSight 功能、Performance Manager 和 Network Inspector 的统一控制台访问来自 Broker Agent 的实时数据。
 - EdgeSight 功能包括用于运行状况、容量保障、历史趋势和网络分析的性能管理，由 NetScaler HDX Insight 提供技术支持，可识别由 XenApp 或 XenDesktop 环境中的网络导致的瓶颈。
- 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 HDX Insight 访问 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 IT 人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 站点的实时运行状况监视。利用此功能，管理员可以实时查看故障，更好地了解最终用户的体验。

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该用户相关的活动，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 版本之前的 XenApp 部署或 7 版本之前的 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[XenDesktop 7 之前版本的 VDA 配置权限](#)。

使用 XenApp 和 XenDesktop 完整产品安装程序安装 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。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，请使用安装程序添加 Director。要添加任何其他组件，请重新运行安装程序并选择要安装的组件。有关使用安装程序的信息，请参阅安装文档中的[使用图形界面安装](#)。Citrix 建议仅使用产品安装程序进行安装，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。默认情况下，Director 与指定的 Controller 进行通信。仅为要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。

要确保浏览器与 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 控制器安装在不同的计算机上。

1. 从 XenApp 7.7 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. 在每个 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“向 Director 中添加站点”部分所述。

按 XenApp 场提供一个控制器的服务器地址：XenApp 场中的所有其他控制器自动用于故障转移。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（运行会话的控制器和工作服务器）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

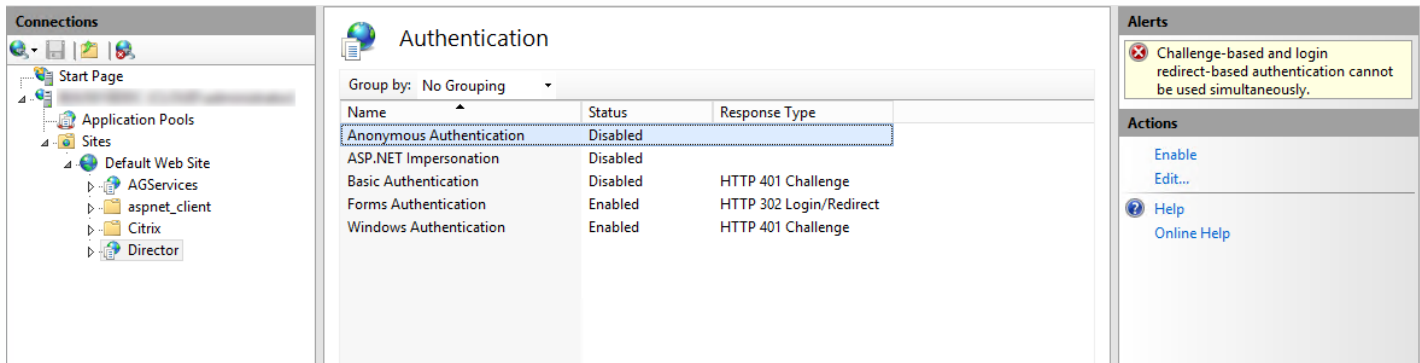
要允许 Director 查找场中的所有 XenApp 工作组，需要在此场使用的 DNS 服务器上为 XenApp 服务器所在的子网添加反向 DNS 区域。

Director 网站位于 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，启用匿名和窗体身份验证。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，窗体身份验证仍应设置为“已启用”。
 - 启动 IIS 管理器。
 - 转至**站点 > 默认 Web 站点 > Director**。
 - 选择**身份验证**。
 - 右键单击**匿名身份验证**，然后选择**禁用**。
 - 右键单击**Windows 身份验证**，然后选择**启用**。



- 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。
 - 在 Active Directory 计算机上，打开 Active Directory 管理控制台。
 - 打开 Active Directory 管理控制台后，导航到**域名 > 计算机** > 选择要向其分配委派权限的 Director 计算机。
 - 单击鼠标右键并选择**属性**。
 - 在“属性”中，选择**委派**选项卡。
 - 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。

高级配置

May 12, 2016

在本文中：

[支持跨多个 Active Directory 域和林的用户](#)

[向 Director 中添加站点](#)

[在活动管理器中禁止显示运行中的应用程序](#)

某些高级 Director 配置（例如，支持多个站点或多个 Active Directory 林）通过 Internet Information Services (IIS) 管理器中的设置进行控制。

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。如果管理员没有相应的权限，无法在林级别执行搜索，则仅搜索域。

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 用户（管理员）的域和 Director 服务器的域。

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。如果管理员没有相应的权限，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 场中的控制器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 控制器的地址。

对于 XenApp 6.5 站点，从 XenApp 场添加控制器的另一种方法为：

`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 `HKLM\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，这表示在活动管理器中将不显示信息。
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`

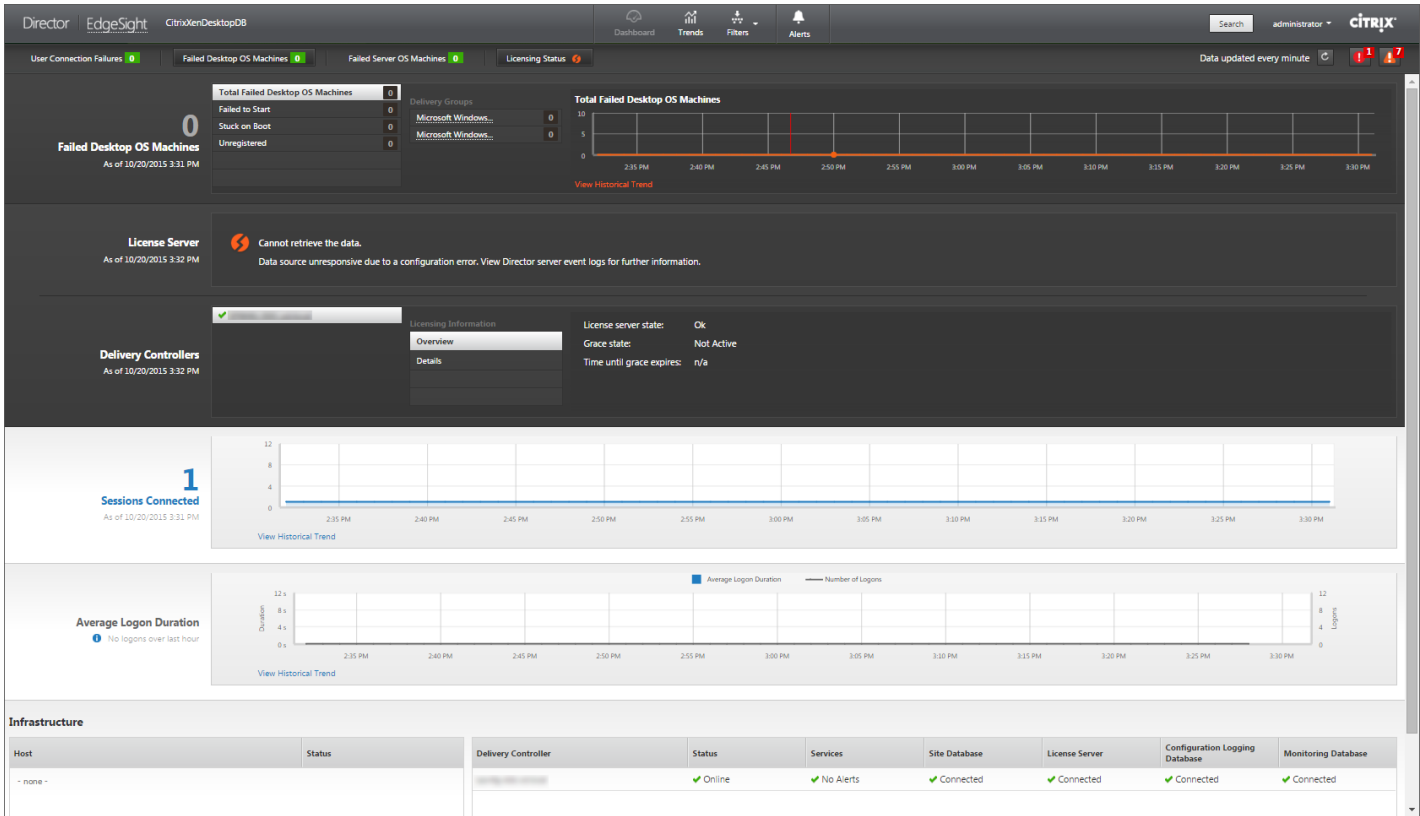
重要：要禁止查看运行中的应用程序，Citrix 建议进行上述两项更改，以确保在活动管理器中不显示这些数据。

监视部署

Jun 17, 2016
在本文中：

- 监视站点
- 监视会话
- 过滤数据以排除故障
- 监视站点间的历史趋势
- 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。

面板	说明
用户连接故障	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 管理应用程序 。
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	- 许可证服务器警报由许可证服务器发送，并且还显示解决警报所需的操作。 - Delivery Controller 警报由 Delivery Controller 发送，显示 Controller 看到的许可状态的详细信息。 可以在 Studio 中设置警报的阈值。 如果许可证服务器版本早于 11.12.1 且/或 Delivery Controller 早于 XenApp 7.6 或 XenDesktop 7.6，则不显示许可证服务器和/或 Delivery Controller 警报。
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时长。此平均值中不包括 XenDesktop 7.0 之前版本的 VDA 的登录数据。
基础结构	站点的主机、控制器和基础结构的运行状态。查看性能警报。 对于主机，通过来自 XenServer 或 VMware 的信息监视连接状态及 CPU、内存、带宽（网络使用率）和存储器（磁盘使用情况）的运行状况。 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 XenServer 文档中的配置性能警报。

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	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，以及该用户具有访问权限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。请参阅 还原会

会话操作	说明
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。
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情况数据（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、连接和会话的自定义过滤视图。

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。
- **会话。** 还可以从“计算机”视图查看会话计数。
- **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。

2. 对于“故障方式”，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。

以后要打开过滤器，请从过滤器菜单中选择故障类型（计算机、会话或连接），然后选择已保存的过滤器。

6. 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。

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

“趋势”视图提供每个站点的会话、连接故障、计算机故障、登录性能和负载评估的历史趋势信息。要查找此信息，请在控制板或“过滤器”视图中，单击“趋势”。

通过放大细节功能，管理员可以通过放大时间段（单击图标中的数据点）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。

操作	说明

导出图形数据	选择包含要导出的数据的选项卡。单击“导出”，然后选择文件格式：.PDF、Excel 或 .CSV。
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	从“连接故障”选项卡，选择计算机类型、故障类型、交付组和时间段，以查看包含有关站点间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	从“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，选择故障类型、交付组和时间段，以查看包含有关站点间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间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。该视图还显示了登录阶段的平均持续时间，例如代理时长、VM 开始时间等等。 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。
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，以便能够快速访问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 (VDI) 的当前状态。
使用 HDX Insight 查看网络分析数据	此功能的可用性取决于组织的许可证和管理员权限。 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。通过此功能，Director 对部署中的 ICA 通信进行高级分析。

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。

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

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	功能
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。
挂起	将正在运行的 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

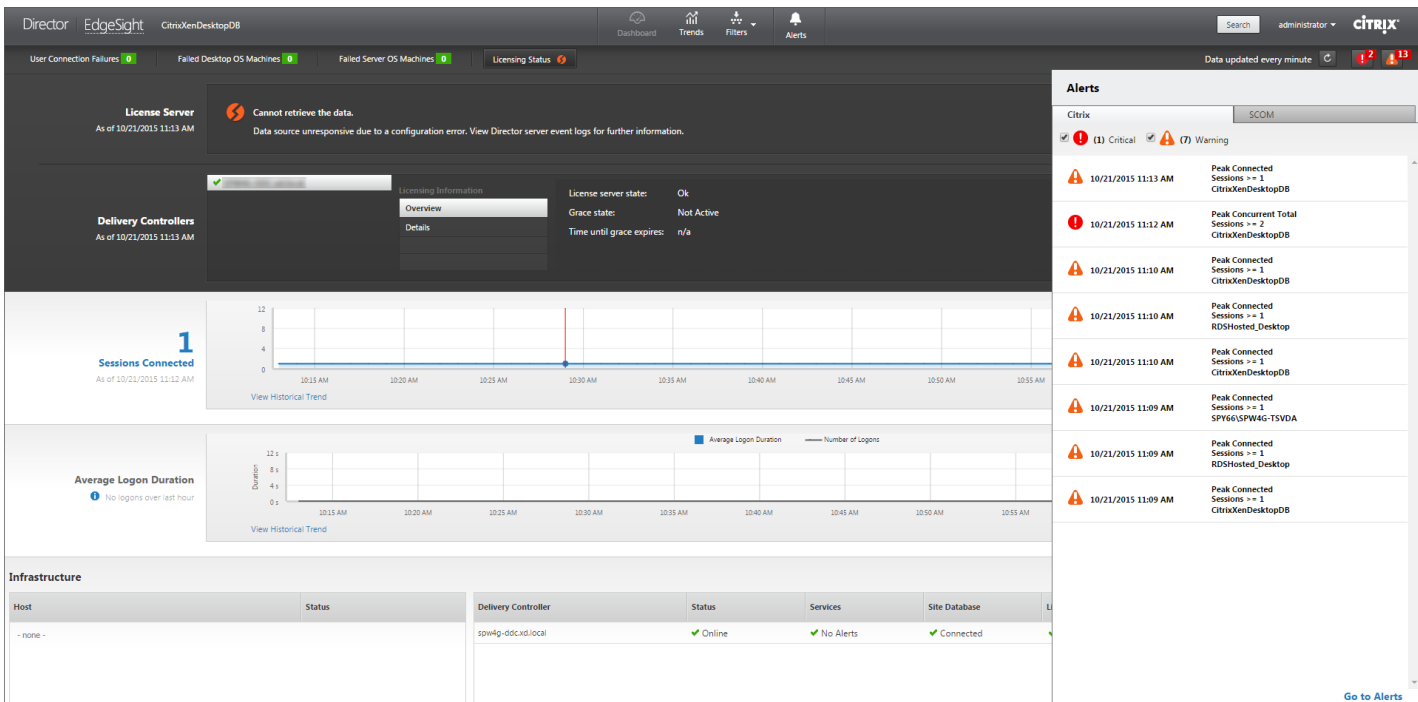
禁用维护模式。

警报和通知

Jul 26, 2016
在本文中：

- 监视警报
- 创建警报策略
- 警报策略条件
- 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。警报每分钟自动更新一次；也可以根据需要更新警报。



警告警报（黄色三角形）指示已满足条件的最低阈值。

严重警报（红色圆形）显示已超过条件的最高阈值。

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。

在“警报”视图中，可以过滤和导出警报。例如，上个月某个特定交付组的出现故障的服务器操作系统计算机。

Director | EdgeSight | CitrixXenDesktopDB

Dashboard | Trends | Filters | Alerts

Citrix Alerts | SCOM Alerts | Citrix Alerts Policy | Email Server Configuration

Citrix Alerts

Source:

Category:

State:

Time period: Ending:

Citrix 警报。 Citrix 警报是指在 Director 中监视的源自 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，可以设置要在警报达到和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。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”和“配置 SCOM 集成”。

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。

Director | EdgeSight | CitrixXenDesktopDB

Dashboard | Trends | Filters | Alerts

Search administrator Citrix

Citrix Alerts | SCOM Alerts | Citrix Alerts Policy | Email Server Configuration

Site Policy | Delivery Group Policy | **Server OS Policy**

[Back to Alert Policies](#)

Name of Alert:

Description:

Conditions:

- Peak Connected Sessions** (Warning icon)
- Peak Disconnected Sessions
- Peak Concurrent Total Sessions
- Connection Failure Rate
- Connection Failure Count
- Average Logon Duration
- Load Evaluator Index

Number of peak connected sessions

Warning Critical [Reset Values](#)

Peak connected sessions: mins mins

Re-alert interval: mins mins

Scope: No Server OS Machines assigned

Notifications preferences: No email addresses added

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）。
2. 单击**创建**。
3. 命名并描述该策略，然后设置触发警报必须满足的条件。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发出警报，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**。

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。

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。 建议在警报显示时执行的操作： • 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。 建议在警报显示时执行的操作： • 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。 • 根据需要注销已断开连接的会话。
最大并发会话总数	最大并发会话总数。 建议在警报显示时执行的操作： • 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。 • 根据需要注销已断开连接的会话。
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。

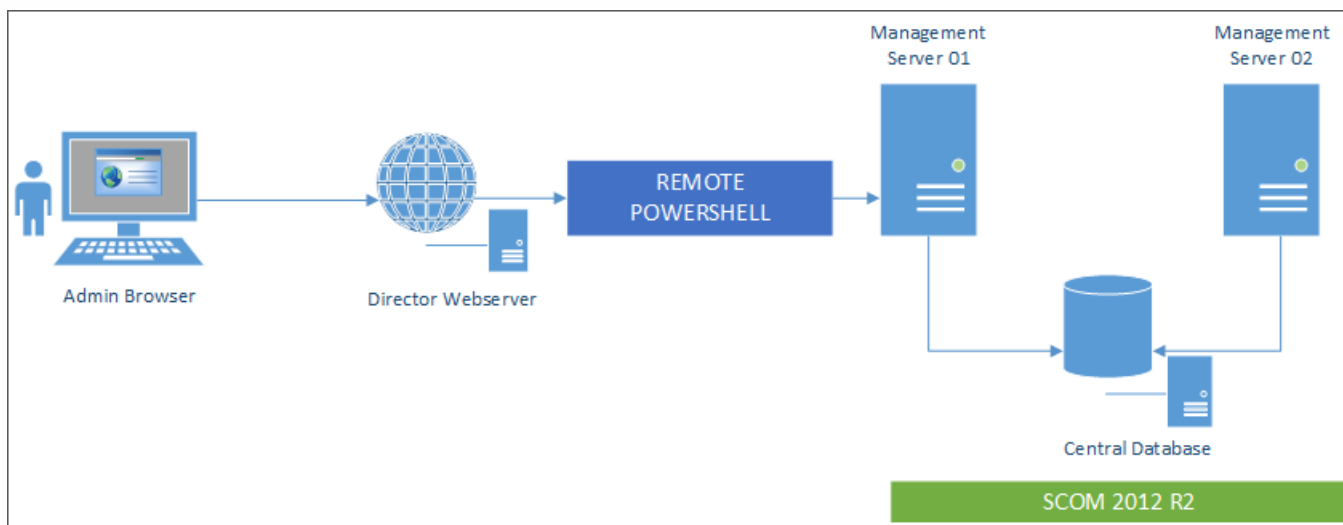
连接失败次数	过去一小时内连接失败的次数。 建议在警报显示时执行的操作： • 检查 Director 的“连接失败趋势”视图，了解配置日志中记录的事件。 • 确定桌面或应用程序是否可访问。
出现故障的计算机数(桌面操作系统)	出现故障的桌面操作系统计算机数。 建议在警报显示时执行的操作： • 可能会因多种原因而出现故障，如在 Director 的“控制板”和“过滤器”视图中所示。请运行 Citrix Scout 诊断以确定根本原因。有关详细信息，请参阅“对用户问题进行故障排除”。
出现故障的计算机数(服务器操作系统)	出现故障的服务器操作系统计算机数。 建议在警报显示时执行的操作： • 可能会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	过去一小时内的平均登录时长。 建议在警报显示时执行的操作： • 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导致登录时间延长。 • 请查看登录的基准时间和中断时间，以缩小原因范围。
负载评估器指数	过去 5 分钟内负载评估器指数的值。 建议在警报显示时执行的操作： • 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。

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 Microsoft System Center 2012 Operations Manager (SCOM) 的信息。

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。

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 服务器安装的 PowerShell 版本必须相同。



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。
- Citrix 建议您将 Director 管理员帐户配置为 SCOM 操作员角色，以便其能够获取 Director 中完整的警报信息。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，但不建议这样操作。
- 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。这是为了确保适度加载 SCOM 管理服务以实现最优性能。

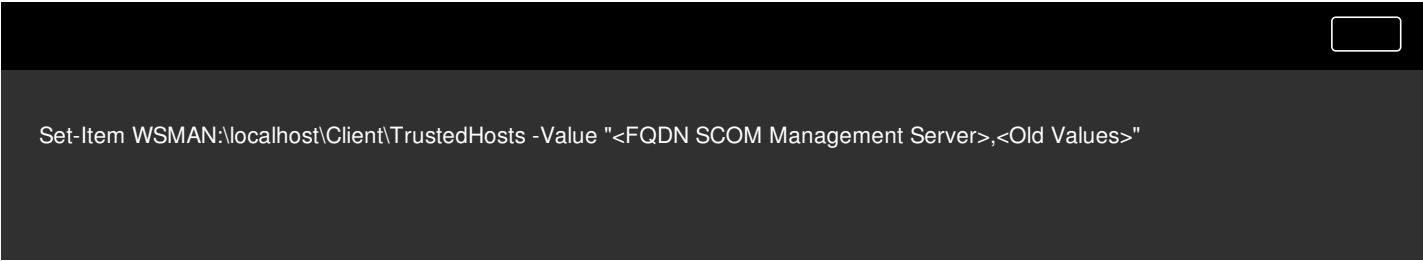
在 Director 服务器上执行以下操作：

1. 在 Director 服务器上，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。从提升的 PowerShell 命令中打开提升的 PowerShell 提示符，并执行以下命令：

- a. 获取 TrustedHosts 的当前列表

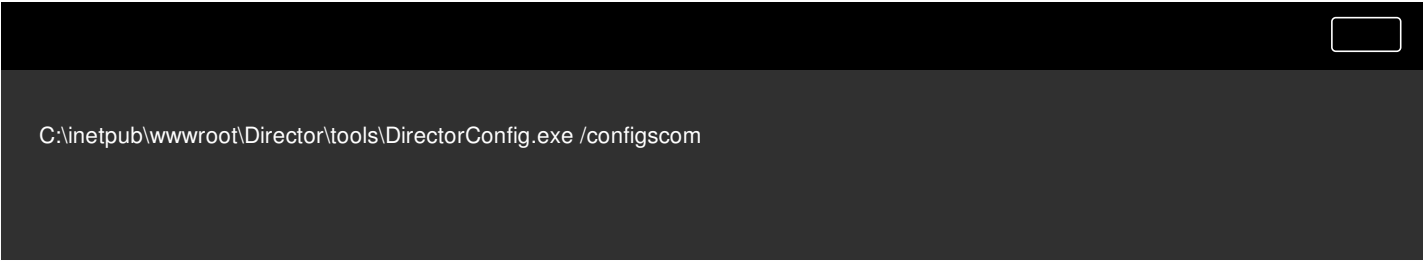


- b. 将 SCOM 管理服务器的 FQDN 添加到 TrustedHosts 列表中。<旧值> 表示从 Get-Item cmdlet 返回的一组现有条目。



```
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。这些角色定义对 SCOM 数据的访问权限的性质。例如，只读权限 SCOM 操作员看不到“管理”窗格，无法发现或管理规则、计算机或帐户。SCOM 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，Director 管理员将无法执行以下操作。

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：

```
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：

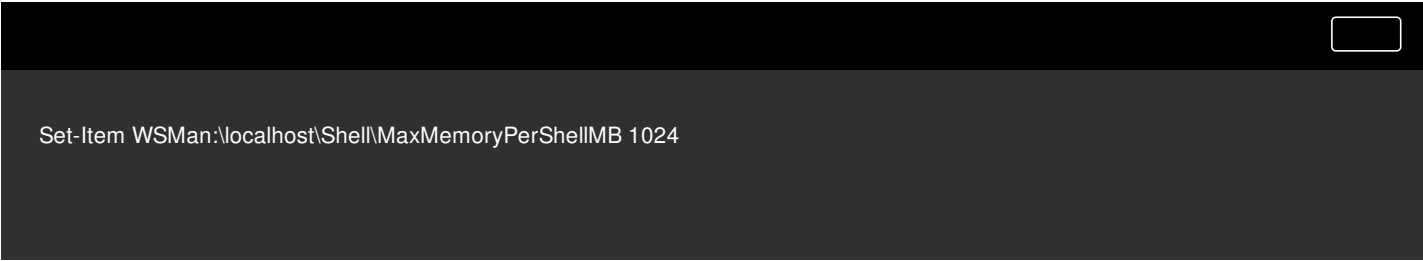
```
Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20
```

c. 修改 MaxMemoryPerShellMB：

在 CLI 中：

```
winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}
```

在 PS 中：



```
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：HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

注册表项：LocalAccountTokenFilterPolicy

类型：DWord

值：1

警告

注册表编辑不当可能会导致严重问题，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。

委派管理和 Director

Mar 17, 2016

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，可以为管理员指派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

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：

- 用于登录 Director 的 Delivery Controller 权限。

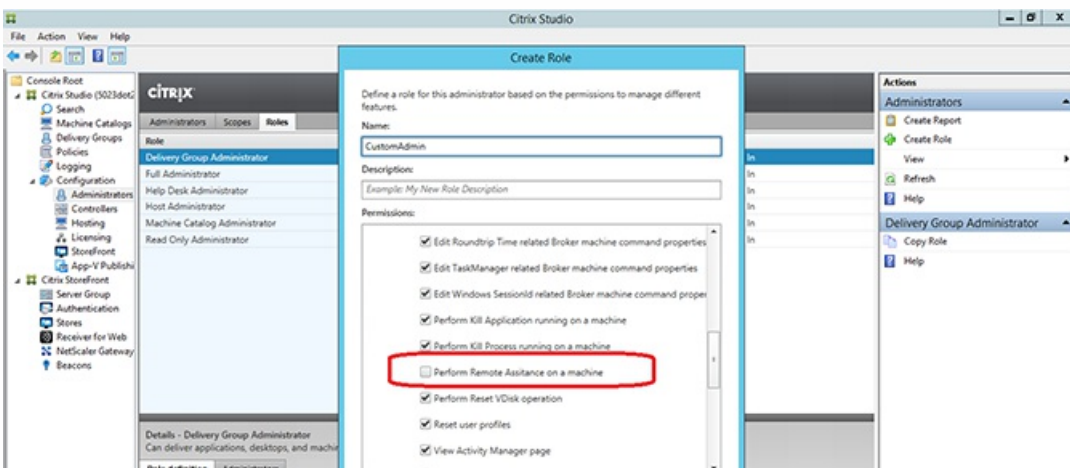
- 用于查看与 Director 中的交付组相关的数据的交付组权限。

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

在此示例中，重影（在计算机上执行远程协助）关闭。



另外，从其他组件的权限列表中，考虑选择以下权限：

- 从交付组：
 - 使用交付组成员身份启用/禁用计算机的维护模式
 - 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

安全 Director 部署

May 12, 2016

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 要求在请求筛选中使用以下文件扩展名：

- .aspx
- .css
- .html
- .js
- .png

Director 要求在请求筛选中使用以下 HTTP 谓词。可以不允许使用未列出的谓词。

- GET
- POST
- HEAD

Director 不需要以下各项：

- ISAPI 筛选器
- ISAPI 扩展
- CGI 程序
- FastCGI 程序

Important

- 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。

Director 中的证书：

- 要使用 HTTPS，可以配置并使用可信证书。

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 使用安全套接字层 (SSL) 和传输层安全性 (TLS) 协议来提供强大的数据加密。

可以使用 TLS Relay 来确保 Director 与 XenApp/XenDesktop 服务器之间的数据流量安全。有关详细信息，请参阅博客文章 [Securing Citrix Director: OData Interface through TLS](#)（通过 TLS 确保 Citrix Director: OData 接口安全）。

Citrix 建议使用 NetScaler Gateway 和 HTTPS 来确保 Director 与用户设备之间的通信安全。要使用 HTTPS，Director 要求将托管身份验证服务的 Microsoft Internet Information Services (IIS) 实例配置为支持 HTTPS。如果没有合适的 IIS 配置，Director 将使用 HTTP 进行通信。Citrix 强烈建议您不要在生产环境中启用指向 Director 的不安全的用户连接。

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，则这些 Web 应用程序中存在的任何安全风险可能会潜在地降低 Director 部署的安全性。如果环境中需要更程度的安全隔离，Citrix 建议您在单独的 Web 域中部署 Director。

为 XenDesktop 7 之前版本的 VDA 配置权限

Mar 17, 2016

如果用户在其设备上安装了 XenDesktop 7 之前的 VDA 版本，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\DesktopDirector 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。

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 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

配置 HDX Insight

Mar 17, 2016

注意：此功能的可用性取决于组织的许可证和管理员权限。

HDX Insight 将 EdgeSight 网络分析和 EdgeSight Performance Management 与 Director 相集成：

- EdgeSight 网络分析利用 HDX Insight 来提供应用程序和桌面的网络上下文视图。使用此功能，Director 可对其部署中的 ICA 通信进行高级分析。
- EdgeSight Performance Management 可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 可为 Director 提供更多信息：

- 趋势页可以显示对整个部署的应用程序、桌面和用户的延迟和带宽影响。
- 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。

在 Director 上配置 EdgeSight 网络分析功能

EdgeSight 可通过利用 NetScaler HDX Insight 提供网络分析功能，以向 Citrix 应用程序和桌面的管理员提供对可能导致网络性能不佳的问题进行故障排除和关联的功能。

必须在 Director 中安装并配置 NetScaler Insight Center，才能启用 EdgeSight 网络分析。Insight Center 是一种虚拟机（设备），可从 Citrix.com 下载。通过使用 EdgeSight 网络分析，Director 可以传送和收集与部署相关的信息。这些信息可在 HDX Insight 中进行利用，这让 HDX Insight 可以对客户端和后端 Citrix 基础结构之间的 Citrix ICA 协议进行可靠分析。

1. 在安装 Director 的服务器上，在 C:\inetpub\wwwroot\Director\tools 中找到 DirectorConfig 命令行工具，并在命令行提示窗口中使用参数 /confignetscaler 运行该工具。
2. 系统弹出提示时，请按提示配置 NetScaler Insight Center 计算机名称（FQDN 或 IP 地址）、用户名、密码和 HTTP 或 HTTPS 连接类型。
3. 要验证更改，请先注销，然后再重新登录。

对用户问题进行故障排除

Mar 17, 2016

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。
- 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

用户的问题	相应的建议：
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
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。

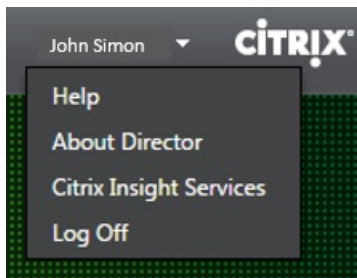
搜索结果中也包括当前未使用计算机或未分配给计算机的用户。

- 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、姓名或显示名称）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。

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 Diagnosis 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 Citrix Insight Services (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](#)。

重影用户

Mar 17, 2016

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。
 - 要执行会话监控，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。

向用户发送消息

Mar 17, 2016

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。

诊断用户登录问题

Mar 17, 2016

请按照以下通用步骤进行操作：

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. 让用户注销然后重新登录，以便您检查登录时长数据。此面板通常在大约 3 分钟后更新，这一时间可能会更长，具体取决于完成登录所需的时间。
3. 检查登录过程的各个阶段：
 - **代理** - 决定向用户分配哪个桌面所用的时间。
 - **VM 启动** - 启动桌面所用的时间。
 - **HDX 连接** - 建立 HDX 连接所用的时间（具体取决于网络情况）。
 - **GPO** - 应用组策略对象所用的时间。
 - **登录脚本** - 脚本所用的时间。
 - **配置文件加载** - 加载用户配置文件所用的时间。
 - **交互式会话** - 建立交互式用户会话所用的时间。

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。

提示：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。

故障排除提示：检查异常差异，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：
 - 安装了新的应用程序。
 - 发生了操作系统更新。
 - 更改了配置。
- 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。

解决应用程序故障

Mar 17, 2016

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（如添加补丁或进行其他更新），请将计算机置于维护模式并将问题上报给相应的管理员。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。

还原桌面连接

Mar 17, 2016

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
请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。

还原会话

Mar 17, 2016

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 Virtual Delivery Agent (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信息。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。

运行 HDX 通道系统报告

Mar 17, 2016

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信息，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。

重置 Personal vDisk

Mar 17, 2016

警告：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。

重置用户配置文件

Mar 17, 2016

警告：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。

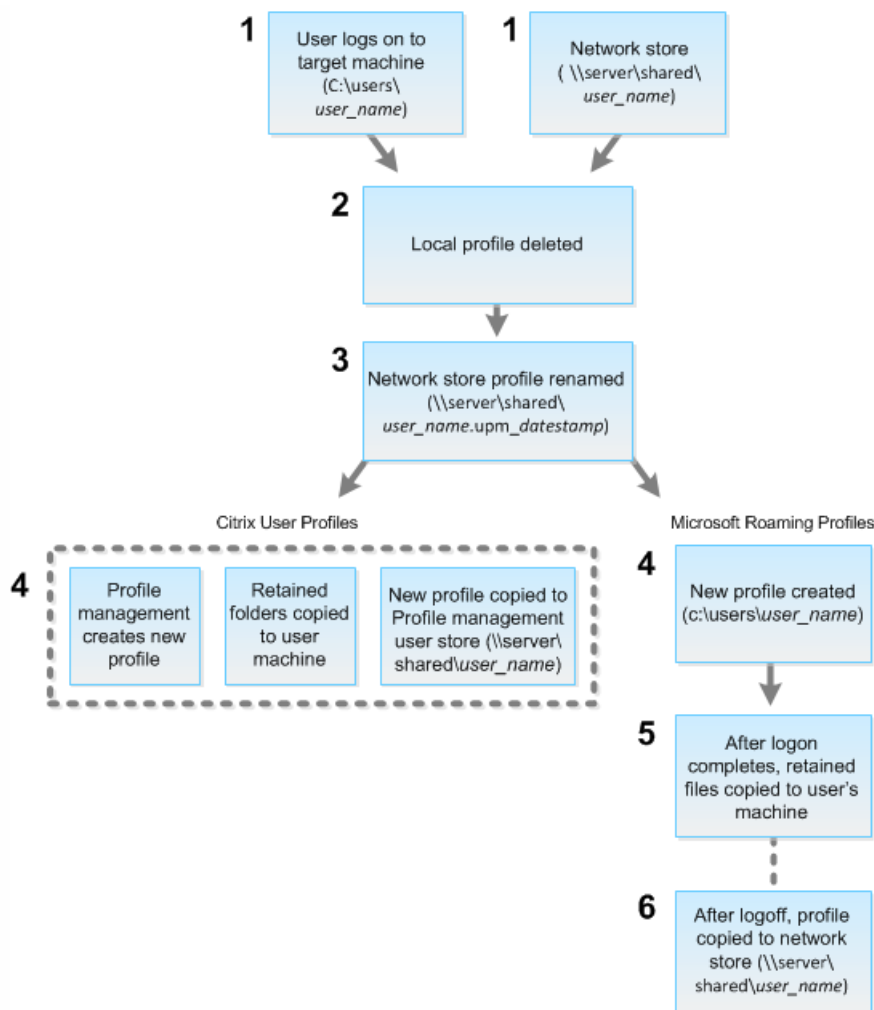
如果配置文件未能成功重置（例如，用户无法成功重新登录计算机或部分文件已丢失），您必须手动还原原始配置文件。用户配置文件中的文件夹（及其文件）将保存并复制到新配置文件中。将按照所列顺序复制这些文件：

- 桌面
- Cookies
- 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。

用户下次登录时，此图会显示发生的处理过程。



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。

SDK 和 API

Mar 17, 2016

本版本提供多种 SDK 和 API。

XenApp 和 XenDesktop SDK : XenApp 和 XenDesktop 建立在多个 Microsoft Windows PowerShell 3.0 管理单元的基础上，它允许您执行通过 Citrix Studio 控制台可以完成的任务，以及一些只使用 Studio 无法完成的任务。

有关详细信息，请参阅 [Citrix Developer](#)。

Citrix 组策略 SDK : Citrix 组策略 SDK 可用来显示和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，请参阅下文[组策略 SDK](#) 部分。

Monitor Service OData API : 可以使用 Monitor Service OData API 执行以下操作：

- 分析历史趋势以便进行未来规划
- 对连接失败和计算机故障进行细致的故障排除
- 提取信息以用于其他工具和流程；例如，可以使用 Microsoft Excel 的 PowerPivot 表以不同的方式显示数据
- 基于 API 提供的数据构建自定义用户界面

有关详细信息，请参阅 [Monitor Service OData API](#) 一文。

XenApp 和 XenDesktop SDK

自版本 7.x 开始，XenApp 和 XenDesktop 共享统一的体系结构和管理：FlexCast Management Architecture。这意味着 XenApp 提供了多种之前仅在 XenDesktop 中提供的功能；因此，与常用功能相关的 SDK 元素同样适用于 XenApp 和 XenDesktop，即使命令本身仅引用 XenDesktop 也是如此。

下表概述了 XenApp 和 XenDesktop SDK 的 7.x 版本之间的差别（假定您熟悉 XenDesktop 5 SDK）。

- **全新的高级 SDK** — XenDesktop 7 提供了全新的高级 SDK，使您可以编写脚本、自动化站点创建以及轻松地进行快速维护。高级 SDK 为您免除了很多低级 SDK 的复杂性，这样，您只需运行两个 cmdlet 即可轻松创建一个新站点。
- **全新的低级 SDK** — 为全新的 XenDesktop 7 服务提供了单独的低级 SDK，包括为 Delegated Administration Service (DAS) 提供了增强的专用 SDK，此 SDK 之前在 XenDesktop 5 中是 Broker SDK 的一部分。此外，还提供了用于 Monitor Service、环境测试以及配置日志记录等新功能的 SDK。
- **Windows 服务器操作系统计算机目录和交付组** — 可以使用 XenDesktop 7 SDK 交付托管在服务器操作系统上的具有成本效益的应用程序和桌面。
- **桌面操作系统计算机应用程序** — 桌面操作系统计算机应用程序在 SDK 级别发生了显著变化。如果您具有用于在桌面操作系统上运行应用程序的现有脚本，则必须为 XenDesktop 7 更新这些脚本，因为几乎不进行向后兼容。
- **将设置应用于交付组中的计算机** — 在 XenDesktop 7 中，使用配置插槽，可以将设置应用于特定交付组中的计算机，而非站点中的所有计算机。这样，就可以配置应用于特定交付组的设置。系统提供了多个包含不同类型设置的预定义配置插槽，例如用于 Receiver 或 App-V 发布服务器位置的 StoreFront 地址设置。可以将插槽的一组设置仅应用于某个特定交付组，同时将同一插槽的另一组设置应用于另一交付组。可以使用与特定部署相对应的名称；例如，“销售部门策略”。
- **取代了目录类型** — 在 XenDesktop 7 中，已使用具有单个属性的目录取代了目录类型。但是，为了向后兼容，仍然可以使用采用目录类型的现有脚本，例如单一映像（池）和精简克隆（专用）等等，但是在内部这些目录类型会被转换为属性集。

警告：在可行的情况下，会维护与 XenDesktop 5 目录类型的向后兼容。但是，编写新脚本时，请勿使用目录类型；而是使用单个属性指定目录。

- **取代了桌面对象** — 在 XenDesktop 5 中，桌面对象是 Broker SDK 脚本中使用的 SDK 对象的主要类型之一。桌面对象同时描述了计算机和计算机上的会话。在 XenDesktop 7 中，此对象已被会话对象和计算机对象所取代，这两个对象均已扩展为担任桌面对象的工作。但是，为了向后兼容，仍然可以使用采用了桌面对象的现有脚本。

警告：在可行的情况下，会维护与 XenDesktop 5 的向后兼容。但是，编写新脚本时，请勿使用桌面对象；而是指定会话对象和计算机对象。

SDK 与 Studio 控制台在策略规则方面存在区别。在 SDK 中，授权和分配策略规则是独立的实体；但在控制台中，这些实体不可见，因为它们与交付组无缝合并在一起。此外，SDK 中访问策略规则的限制性更低。

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 3.0 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.ADIIdentity.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。

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:/`）

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。

Monitor Service OData API

Mar 17, 2016

除使用 Citrix Director 控制台显示历史数据外，还可以使用 Monitor Service API 查询数据。您可以使用 API 执行以下操作：

- 分析历史趋势以便进行未来规划
- 对连接失败和计算机故障进行细致的故障排除
- 提取信息以用于其他工具和流程；例如，可以使用 Microsoft Excel 的 PowerPivot 表以不同的方式显示数据
- 基于 API 提供的数据构建自定义用户界面

Monitor Service API 使用开放数据协议 (OData)。此协议是一个用于查询和更新数据的 Web 协议，并基于诸如 HTTP 之类的 Web 技术而构建。有关 OData 协议的详细信息，请参阅 <http://www.odata.org>。

Monitor Service API 在使用 Windows Communication Foundation (WCF) Data Services（在处理和合并期间填充）的 SQL Server 数据库的基础上构建。通过 wsHttpBinding 显示了两个使用 WCF 的端点。基址为 `http://{dc-host}/Citrix/Monitor/OData/v2`。还可以使用 TLS 保护端点；有关详细信息，请参阅[使用 TLS 保护端点安全](#)。

1. 数据端点可显示对数据库实体的直接只读访问权限，并且可以使用 OData 查询语言进行访问。根据过滤和列选择，本端点允许高度灵活的访问。数据 API URI 为 `http://{dc-host}/Citrix/Monitor/OData/v2/Data`。有关访问 Monitor Service 数据的详细信息，请参阅[使用 API 访问数据](#)。
2. 方法端点可显示 Citrix Director 用于检索需要复杂分组和高性能标准的数据的服务操作（例如“控制板”和“趋势”页上的查询）。方法 API URI 为 `http://{dc-host}/Citrix/Monitor/OData/v2/Methods`。方法仅在 Director 本身中使用，因而不供大多数 Citrix 客户使用。所以，此处并未介绍这些方法。

XenApp 和 XenDesktop 7.6 附带的 API 版本提供以下新功能：

- **修补程序清单。** 在 Director 中使用“用户详细信息”视图或“计算机”视图，您会看到计算机上安装的所有 Citrix 修补程序的列表。您可以使用 API 提取此数据并创建自定义报告（例如，整个站点上安装的修补程序的状态）或将其拉到分析引擎中。引入了新类并且扩展了 Machine 类，可支持跟踪控制器和 VDA 上安装的 Citrix 修补程序。
- **匿名会话故障排除。** 会话可作为一组池本地用户帐户运行。API 向 Session 类添加了新属性 IsAnonymous（默认值为 FALSE）。
- **托管应用程序使用率报告。** Director 提供新的容量报告，可显示托管应用程序随时间变化的使用率。API 允许您报告用户会话中运行的每个应用程序实例的详细信息。

以下位置的《API 参考》中完整介绍了所有数据更新：<http://support.citrix.com/help/monitorserviceapi/7.6/>。

本版本已弃用 GetSessionSummary 方法。

使用 API 访问数据

Mar 17, 2016

以下类型的数据可通过 Monitor Service API 获得：

- 与连接故障相关的数据
- 处于故障状态的计算机
- 会话使用情况
- 登录持续时间
- 负载均衡数据
- 应用于计算机的修补程序
- 托管应用程序的使用情况

有关数据对象的完整说明，请访问 <http://blogs.citrix.com/2013/08/27/xendesktop-7-monitor-service-what-data-is-available/>。

要使用 Monitor Service OData API，您必须是 XenApp 或 XenDesktop 管理员。要调用 API，您需要具有只读权限；但是，返回的数据由 XenApp 或 XenDesktop 管理员角色和权限决定。例如，交付组管理员可以调用 Monitor Service API，但他们可以获取的数据由使用 Citrix Studio 设置的交付组访问权限控制。有关 XenApp 或 XenDesktop 管理员角色和权限的详细信息，请参阅[委派管理](#)。

查询数据

Monitor Service API 是一款基于 REST 的 API，可以使用 OData 使用者程序进行访问。OData 使用者程序是占用使用 OData 协议显示的数据的应用程序。从简单的 Web 浏览器到可利用 OData 协议的所有功能的自定义应用程序，OData 使用者程序的复杂程度各不相同。有关 OData 使用者程序的详细信息，请参阅：<http://www.odata.org/ecosystem#consumers>。

每一部分 Monitor Service 数据模型都可访问，并且可根据 URL 过滤。OData 以 URL 格式提供查询语言，可用于从服务检索条目。有关详细信息，请参阅：<http://msdn.microsoft.com/en-us/library/ff478141.aspx>

查询在服务器端进行处理，并且可以使用客户端上的 OData 协议进行进一步过滤。

建模数据分为以下三类：聚合数据（汇总表）、对象（计算机、会话等）的当前状态和日志数据，日志数据实际上是指历史事件（如连接）。

注意：OData 协议不支持枚举；在其位置使用整数。要确定 Monitor Service OData API 返回的值，请参阅 <http://support.citrix.com/help/monitorserviceapi/7.6/>。

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、会话负载均衡详细信息，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，计算精确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。
- 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 Session and Connection 行信息。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。对于未获得使用 Platinum Edition 许可的客户，不管默认整理保留期限如何，均从第 8 天开始整理。Platinum 客户可以将整理保留期限更改为他们所需的保留天数，如未修改，将使用默认值。

采用以下设置控制整理：

设置名称	受影响的整理	默认值 (天)	访问方法
GroomSessionsRetentionDays	Session 和 SessionDetail 记录	对于非 Platinum 用户为 7；对于	Cmdlet (set/get-monitorconfiguration)

设置名称	受影响的整理	Platinum 默认值 为 90 (天)	访问方法
GroomSummariesRetentionDays	DesktopGroupSummary、FailureLogSummary 和 LoadIndexSummary records。聚合数据 - 日粒度。	对于非 Platinum 用户为 7；对于 Platinum 为 90	Cmdlet (set/get-monitorconfiguration)
GroomHourlyRetentionDays	聚合数据 - 小时粒度	32 天	Monitor.Configuration Database Table。请参阅下面的注释。
GroomMinuteRetentionDays	聚合数据 - 分钟粒度	3 天	Monitor.Configuration Database Table。请参阅下面的注释。
GroomFailuresRetentionDays	MachineFailureLog 和 ConnectionFailureLog 记录	对于非 Platinum 用户为 7；对于 Platinum 为 90	Cmdlet (set/get-monitorconfiguration)
GroomLoadIndexesRetentionDays	LoadIndex 记录	对于非 Platinum 用户为 7；对于 Platinum 为 90	Cmdlet (set/get-monitorconfiguration)
GroomDeletedRetentionDays	LifecycleState 状态为“Deleted”的 Machine、Catalog、DesktopGroup 和 Hypervisor 条目。将删除任何相关的 Session、SessionDetail、Summary、Failure 或 LoadIndex 条目。	对于非 Platinum 用户为 7；对于 Platinum 为 90	Cmdlet (set/get-monitorconfiguration)
GroomMachineHotfixHistoryRetentionDays	应用至 VDA 和 Controller 计算机的修补程序	非 Platinum 和 Platinum 用户均为 90	Cmdlet (set/get-monitorconfiguration)

警告：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。

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：
 $1000 \text{ 个交付组} \times 24 \text{ 小时/天} \times 365 \text{ 天/年} \times 2 \text{ 年} = 17,520,000 \text{ 行数据}$ 。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，这些表格经过两年时间将大于 TB 级数据，这将要求使用企业级高端数据库。

使用 TLS 保护端点安全

Mar 17, 2016

本文档介绍了如何使用 TLS 为 Monitor Service OData API 端点提供安全保护。 如果选择使用 TLS，则必须在站点内的所有 Delivery Controller 上配置 TLS。不能同时使用 TLS 和非 TLS。

要使用 TLS 为 Monitor Service 端点提供安全保护，必须执行以下配置。有些步骤需要在每个站点一次性完成，其余步骤则须在站点中托管 Monitor Service 的计算机上执行。各步骤的说明如下所述。

第 1 部分：在系统中注册证书

1. 使用可信证书管理器创建证书。证书必须与您希望用于 OData TLS 的计算机上的端口相关联。
2. 配置 Monitor Service，以使用此端口进行 TLS 通信。操作步骤取决于您的环境及其与证书结合使用的方式。下例说明了如何配置端口 449：

- 将证书与某个端口相关联：
`netsh http add sslcert ipport=0.0.0.0:449 certhash=97bb629e50d556c80528f4991721ad4f28fb74e9 appid='{00000000-0000-0000-0000-000000000000}'`
提示：在 PowerShell 命令窗口中，请务必用单引号引起 appId 中的 GUID（如下所示），否则命令将不起作用。 请注意，在此示例中添加的换行符只是为了方便阅读。

第 2 部分：修改 Monitor Service 的配置设置

1. 在站点中的任意 Delivery Controller 上，运行以下 PowerShell 命令一次。此命令解除了 Monitor Service 在 Configuration Service 中的注册状态。
`asnp citrix.* $serviceGroup = get-configregisteredinstance -servicetype Monitor | Select -First 1 ServiceGroupUid remove-configservicegroup -ServiceGroupUid $serviceGroup.ServiceGroupU`
2. 在站点中的所有 Controller 上执行以下操作：
 - 使用 cmd 提示符查找已安装的 Citrix Monitor 目录（通常位于 C:\Program Files\Citrix\Monitor\Service 中）。在该目录下，运行：
`Citrix.Monitor.Exe -CONFIGUREFIREWALL -ODDataPort 449 -RequireODDataSsl`
 - 运行以下 PowerShell 命令：
`asnp citrix.* (if not already run within this window) get-MonitorServiceInstance | register-ConfigServiceInstance Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-MonitorServiceGro`

示例

Mar 17, 2016

以下示例介绍如何使用 OData API 导出 Monitor Service 数据。

示例 1 - 原始 XML

1. 将每个数据集的 URL 置于正在使用 XenApp 或 XenDesktop 站点的相应管理权限运行的 Web 浏览器中。Citrix 建议使用装有 Advanced Rest Client 加载项的 Chrome 浏览器。
2. 查看来源。

示例 2 - PowerPivot with Excel

这些说明假定您已安装 Microsoft Excel 和 PowerPivot。

打开 Excel（使用 XenApp 或 XenDesktop 站点的相应管理权限运行）。

如果使用的是 Excel 2010：

1. 单击“PowerPivot”选项卡。
2. 单击 PowerPivot 窗口。
3. 单击功能区中的**从数据馈送**。
4. 选择友好的连接名称（例如：XenDesktop Monitoring Data）并输入数据馈送 URL：http://{dc-host}/Citrix/Monitor/OData/v2/Data（如果正在使用 TLS，则输入 https://{dc-host}/Citrix/Monitor/OData/v2/Data）。
5. 单击**下一步**。
6. 选择要导入到 Excel 的表并单击**完成**。这样便可检索到数据。
7. 现在，您可以使用 PowerPivot 查看和分析带有数据透视表和数据透视图的数据。有关详细信息，请参阅 Learning Center：<http://www.microsoft.com/en-us/bi/LearningCenter.aspx>

如果使用的是 Excel 2013：

1. 单击“数据”选项卡。
2. 依次选择“自其他来源”>“来自 OData 数据馈送”
3. 输入数据馈送 URL http://{dc-host}/Citrix/Monitor/OData/v1/Data（如果正在使用 TLS，则输入 https://{dc-host}/Citrix/Monitor/OData/v1/Data）并单击**下一步**。
4. 选择要导入到 Excel 的表并单击**下一步**。
5. 接受默认名称或自定义名称，然后单击**完成**。
6. 选择**仅连接或透视报表**。这样便可检索到数据。
7. 现在，您可以使用 PowerPivot 查看和分析带有数据透视表和数据透视图的数据。有关详细信息，请参阅 Learning Center：<http://www.microsoft.com/en-us/bi/LearningCenter.aspx>

示例 3 - LINQPad

这些说明假定您已安装 LINQPad。

1. 通过 XenApp 或 XenDesktop 站点的相应管理权限运行 LinqPad。
提示：最简便的方法是在 Delivery Controller 上下载、安装并运行。
2. 单击“添加连接”链接。
3. 选择 WCF Data Services 5.1 (OData 3) 并单击**下一步**。

4. 输入数据馈送 URL `http://{dc-host}/Citrix/Monitor/OData/v2/Data`（如果正在使用 TLS，则输入 `https://{dc-host}/Citrix/Monitor/OData/v1/Data`）。如有必要，请输入用户名和密码以访问 Delivery Controller。单击 **OK**（确定）。
5. 现在您可以针对数据馈送运行 LINQ 查询，并根据需要导出数据。例如，在“目录”上单击鼠标右键并选择 **Catalogs.Take(100)**。此操作将返回数据库中前 100 个目录。选择“导出”>“导出到具有格式设置的 Excel”。

有关如何将该 API 用于 LINQPad 的更多实例，请参阅 <http://blogs.citrix.com/2014/01/14/creating-director-custom-reports-for-monitoring-xendesktop/>。