Citrix Virtual Apps and Desktops 7 2106

Contents

Citrix Virtual Apps and Desktops 7 2106 **11**

Citrix Virtual Apps and Desktops 7 2106 **11**

Windows Server 2022 支持 **14**

已修复的问题 **15**

已知问题 **19**

弃用 **24**

系统要求 **32**

技术概述 **40**

Active Directory **49**

数据库 **51**

交付方法 **56**

网络端口 **59**

HDX **60**

自适应传输 **68**

Citrix ICA 虚拟通道 **75**

Citrix Virtual Apps and Desktops 中的双跃点 **84**

安装和配置 **86**

准备安装 **88**

Microsoft System Center Virtual Machine Manager 虚拟化环境 **96**

Citrix Hypervisor 虚拟化环境 **99**

Microsoft System Center Configuration Manager 环境 **100**

VMware 虚拟化环境 **102**

Nutanix 虚拟化环境 **109**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

安装核心组件 **110**

安装 **VDA** **121**

使用命令行安装 **135**

使用脚本安装 **VDA** **147**

使用 **SCCM** 安装 **VDA** **149**

创建站点 **151**

创建计算机目录 **155**

管理计算机目录 **174**

创建交付组 **180**

管理交付组 **184**

创建应用程序组 **204**

管理应用程序组 **210**

Remote PC Access **213**

App-V **225**

发布内容 **237**

服务器 **VDI** **242**

用户个性化层 **243**

删除组件 **261**

升级和迁移 **263**

升级部署 **265**

安全 **282**

安全注意事项和最佳做法 **283**

将 **Citrix Virtual Apps and Desktops** 与 **Citrix Gateway** 集成 **290**

委派管理 **291**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

管理安全密钥 **297**

智能卡 **312**

智能卡部署 **317**

使用智能卡进行直通身份验证和单点登录 **323**

传输层安全性 **(TLS)** **324**

通用打印服务器上的传输层安全性 **(TLS)** **335**

设备 **344**

通用 **USB** 设备 **345**

移动设备和触摸屏设备 **346**

串行端口 **348**

专业键盘 **353**

TWAIN 设备 **354**

网络摄像机 **355**

WIA 设备 **355**

图形 **356**

HDX 3D Pro **357**

适用于 **Windows** 多会话操作系统的 **GPU** 加速 **358**

适用于 **Windows** 单会话操作系统的 **GPU** 加速 **360**

Thinwire **363**

基于文本的会话水印 **368**

多媒体 **370**

音频功能 **372**

浏览器内容重定向 **379**

HDX 视频会议和网络摄像机视频压缩 **388**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

HTML5 多媒体重定向 **391**

Microsoft Teams 的优化 **394**

监视、故障排除和支持 **Microsoft Teams** **416**

Windows Media 重定向 **422**

常规内容重定向 **423**

客户端文件夹重定向 **424**

主机到客户端重定向 **425**

双向内容重定向 **428**

本地应用程序访问和 **URL** 重定向 **429**

通用 **USB** 重定向和客户端驱动器注意事项 **436**

打印 **445**

打印配置示例 **452**

最佳做法、安全注意事项和默认操作 **455**

打印策略和首选项 **456**

预配打印机 **458**

维护打印环境 **464**

策略 **467**

使用策略 **469**

策略模板 **472**

创建策略 **475**

对策略进行比较、设定优先级、建模和故障排除 **480**

默认策略设置 **482**

策略设置参考 **507**

ICA 策略设置 **510**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

客户端自动重新连接策略设置 **518**

音频策略设置 **521**

带宽策略设置 **522**

双向内容重定向策略设置 **527**

浏览器内容重定向策略设置 **527**

客户端传感器策略设置 **534**

桌面 **UI** 策略设置 **534**

最终用户监视策略设置 **536**

增强的桌面体验策略设置 **537**

文件重定向策略设置 **537**

图形策略设置 **541**

缓存策略设置 **546**

Framehawk 策略设置 **546**

保持活动状态策略设置 **547**

本地应用程序访问策略设置 **548**

移动体验策略设置 **548**

多媒体策略设置 **549**

多流连接策略设置 **557**

端口重定向策略设置 **560**

打印策略设置 **562**

客户端打印机策略设置 **564**

驱动程序策略设置 **567**

通用打印服务器策略设置 **569**

通用打印策略设置 **573**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

安全策略设置 **575**

服务器限制策略设置 **576**

会话限制策略设置 **576**

会话可靠性策略设置 **578**

会话水印策略设置 **580**

时区控制策略设置 **582**

TWAIN 设备策略设置 **583**

USB 设备策略设置 **583**

虚拟通道允许列表策略设置 **590**

视频显示策略设置 **591**

移动图像策略设置 **592**

静态图像策略设置 **593**

WebSocket 策略设置 **595**

WIA 设备策略设置 **596**

通过注册表管理的 **HDX** 功能 **596**

负载管理策略设置 **608**

Profile Management 策略设置 **610**

高级策略设置 **610**

基本策略设置 **614**

跨平台策略设置 **617**

文件系统策略设置 **618**

排除策略设置 **619**

同步策略设置 **620**

文件夹重定向策略设置 **622**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

“**AppData (**漫游**)**”策略设置 **622**

“联系人”策略设置 **623**

桌面策略设置 **623**

“文档”策略设置 **624**

“下载”策略设置 **624**

“收藏夹”策略设置 **625**

“链接”策略设置 **625**

“音乐”策略设置 **626**

“图片”策略设置 **627**

“保存的游戏”策略设置 **627**

“开始”菜单策略设置 **628**

“搜索”策略设置 **628**

“视频”策略设置 **629**

“日志”策略设置 **629**

“配置文件处理”策略设置 **633**

“注册表”策略设置 **637**

“流用户配置文件”策略设置 **638**

用户个性化层策略设置 **639**

Virtual Delivery Agent 策略设置 **640**

HDX 3D Pro 策略设置 **642**

监视策略设置 **642**

虚拟 **IP** 策略设置 **645**

使用注册表配置 **COM** 端口和 **LPT** 端口重定向设置 **646**

Connector for Configuration Manager 2012 策略设置 **647**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

管理 **650**

许可 **651**

多类型许可 **655**

许可常见问题解答 **662**

应用程序 **672**

通用 **Windows** 平台应用程序 **681**

区域 **683**

连接和资源 **692**

本地主机缓存 **703**

虚拟 **IP** 和虚拟环回 **712**

Delivery Controller **715**

VDA 注册 **718**

会话 **727**

在 **Studio** 中使用搜索 **732**

标记 **732**

IPv4/IPv6 支持 **740**

用户配置文件 **741**

在系统启动时收集 **Citrix Diagnostic Facility (CDF)** 跟踪信息 **746**

Citrix Insight Services **749**

Citrix Scout **759**

监视 **778**

配置日志记录 **779**

事件日志 **783**

Director **783**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

安装和配置 **788**

高级配置 **790**

配置 **PIV** 智能卡身份验证 **793**

配置网络分析 **797**

委派管理和 **Director** **798**

安全 **Director** 部署 **800**

使用 **Citrix Analytics for Performance** 配置本地站点 **803**

站点分析 **807**

警报和通知 **815**

过滤数据以排除故障 **827**

监视站点的历史趋势 **829**

部署故障排除 **833**

应用程序故障排除 **833**

应用程序探测 **837**

桌面探测 **841**

计算机故障排除 **846**

对用户问题进行故障排除 **852**

诊断会话启动问题 **854**

诊断用户登录问题 **859**

重影用户 **865**

向用户发送消息 **866**

解决应用程序故障 **866**

还原桌面连接 **867**

还原会话 **868**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

运行 **HDX** 通道系统报告 **868**

重置用户配置文件 **869**

录制会话 **872**

功能兼容性列表 **873**

数据粒度和保留 **876**

Citrix Director 故障原因和故障排除 **880**

第三方声明 **893**

SDK 和 **API** **893**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Virtual Apps and Desktops 7 2106

May 6, 2022

Citrix Virtual Apps and Desktops 7 2106

June 29, 2023

关于此版本

此 Citrix Virtual Apps and Desktops 发行版包括新版本的 Windows Virtual Delivery Agent (VDA) 以及多个新版本的核心组件。您可以：

- 安装或升级站点

  请在此版本中使用 ISO 安装或升级核心组件和 VDA。安装或升级到最新版本允许您使用最新功能。

- 在现有站点中安装或升级 **VDA**

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

  将 VDA 升级到此版本（从版本 7.9 或更高版本）后，不需要更新计算机目录的功能级别。**7.9**（或更高版本）值将保留默认功能级别，并对此版本有效。有关详细信息，请参阅 VDA 版本和功能级别。

有关安装和升级说明：

- 如果要构建新站点，请按照安装和配置中的顺序进行操作。
- 如果要升级站点，请参阅升级部署。

Citrix Virtual Apps and Desktops 7 2106

Windows Server 2022 支持

除非另有说明，否则支持 Windows Server 操作系统的组件、功能和技术现在也支持 Windows Server 2022。有关详细信息，请参阅 Windows Server 2022 支持。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

VDA 安装和升级：**Workspace Environment Management (WEM)**

在 VDA 安装程序中，**WEM** 代理页面已更新。在新的 **WEM** 页面上，您首先指出 WEM 部署是本地还是云（服务）。然后，可以提供 WEM 基础结构服务器的地址（用于本地 WEM）或 Cloud Connector（用于 WEM 服务）。有关详细信息，请参阅步骤 7。Workspace Environment Management。

单会话 **VDA** 安装和升级：安装和升级失败时还原

安装或升级单会话 VDA 时，可以启用故障时还原功能。启用此功能后，如果 VDA 安装或升级失败，计算机将返回到还原点。有关详细信息，请参阅安装或升级失败时还原。

VDA 安装：不支持的选项

安装 Windows VDA 时，不再支持 `install_mcsio_driver` 命令行选项。要安装 MCSIO 驱动程序，请使用 `/includeadditional "Citrix MCS IODriver"` 命令行选项，或在 VDA 安装程序的图形界面的其他组件页面上选择 MCSIO 条目。

在维护模式下与计算机断开连接后重新连接会话

以前，当池（随机）单会话桌面 (VDI) 用户在维护模式下断开与计算机的连接时，不允许会话重新连接到池中的任何计算机。在这种情况下，多会话和静态单会话计算机始终允许会话重新连接。

现在，使用 PowerShell，您可以在交付组级别控制在维护模式下的计算机上发生断开连接后是否允许会话重新连接。这适用于组中的所有 VDA（单会话和多会话）。

有关详细信息，请参阅在维护模式下从计算机断开连接时控制会话重新连接。

Virtual Delivery Agent (VDA) 2106

Windows 单会话操作系统和多会话操作系统 VDA 的 2106 版包括以下增强功能。这些项目是本文前面列出的任何 VDA 安装和升级项目的补充。

双向 **URL** 支持更新 **-** 预览版

已为 Google Chrome 和 Microsoft Edge 添加了双向 URL 重定向支持。

浏览器的双向 URL 重定向要求 Citrix Virtual Apps and Desktops 版本 2106 或更高版本、Citrix Workspace 应用程序 2106 或更高版本以及浏览器重定向扩展程序 5.0 版。

有关详细信息，请参阅双向内容重定向策略设置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

为 **Windows** 多会话操作系统启用或禁用 **VDA** 上的“始终提示输入密码”设置

现在可以在 Windows 多会话操作系统计算机上设置注册表项以控制始终提示输入密码 Microsoft 策略设置。有关详细信息，请参阅通过注册表管理的功能列表中的配置自动登录 VDA。

浏览器内容重定向的集成 **Windows** 身份验证支持

浏览器内容重定向现在支持从未加入域的客户端到与 VDA 位于同一域中且配置了集成 Windows 身份验证 (IWA) 的 Web 服务器的单点登录。通过此增强功能，浏览器内容重定向使用您的域用户名和密码对 IWA Web 服务器进行身份验证。有关详细信息，请参阅使用集成 Windows 身份验证进行单点登录。

汇聚连接的代理身份验证支持

现在，您可以将基于计算机的身份验证与协商和 Kerberos 或 NTLM 网络身份验证协议结合使用，通过 HTTP 代理建立汇聚连接。有关详细信息，请参阅代理注意事项。

Remote PC Access 断开连接的会话计时

借助 Remote PC Access，您现在可以配置计时器，以便在用户会话过期后注销用户。如果用户会话在设定的时间内保持断开连接，计时器将注销该用户，以允许其他用户远程访问同一台物理 PC。要启用计时器，必须配置 **Remote PC Access** 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。有关详细信息，请参阅会话限制策略中的 **Remote PC Access** 断开连接的会话计时器。

Citrix Licensing 11.17.2

Citrix Licensing 11.17.2 包含新增功能以及已修复和已知问题。

相关组件

有关相关组件的文档，请参阅：

- Citrix 联合身份验证服务 (FAS)
- Citrix App Layering
- HDX RealTime Optimization Pack
- Linux Virtual Delivery Agent
- Profile Management
- Citrix Provisioning
- Citrix SCOM Management Pack
- 自助服务密码重置

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Session Recording
- StoreFront
- Workspace Environment Management

更多信息

- 有关弃用和删除通知，请参阅弃用。
- 有关 2018 年引入的产品名称和版本号变更的信息，请参阅新名称和版本号。

Windows Server 2022 支持

November 17, 2021

除非另有说明，否则本版本中支持 Windows Server 平台的 Citrix 组件、功能和技术现在也支持 Windows Server 2022。

已知问题

Citrix Virtual Apps and Desktops

- 使用 Skype 时，网络暂时断开连接后，摄像头可能无法正常工作。[HDX-29950]
- VDA 会话内的客户端映射的驱动器上可能会出现红色十字。[HDX-29984]
- 在 VDA 上可能无法正确设置 Windows Ink 笔快捷方式。[HDX-30097]
- 在 Delivery Controller 上设置了“客户端自动重新连接身份验证”策略时，会话无法重新连接。使用“客户端自动重新连接”策略恢复连接时，会话也断开连接。[HDX-32475]
- 在会话漫游之后，客户端映射的驱动器可能无法重新连接到会话。[HDX-32584]
- （仅适用于 Citrix Virtual Apps and Desktops 服务。）从基于付费 Azure 应用商店映像创建的虚拟机创建 MCS 目录时，会出现以下错误：**Creating a virtual machine image from Marketplace image or a custom image sourced from a Marketplace image requires Plan information in the request**（基于应用商店映像或应用商店中提供的自定义映像创建虚拟机映像需要请求中的规划信息）。出现此问题的原因是付费映像需要虚拟机的 Azure 规划描述中缺少的计费机制。[PMCS-18326]
- 无法在各种虚拟机管理程序上重新打开计算机的电源。[PMCS-18325]
- 使用 MCSIO 的预配目标设备不支持 Windows Server 2022 作为 Hyper-V VM。[PVS-8663]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Provisioning

- 使用 Windows 2022 作为虚拟机管理程序时，使用 Citrix Virtual Apps and Desktops 设置向导和流 VM 向导预配映像将无法创建目标设备。[PVS-8504]
- 创建 Windows 2022 系统的映像然后从虚拟磁盘启动将导致 Windows 启动崩溃恢复功能。[PVS-8791]
- 不支持将 Windows 2022 Hyper-V 第 1 代 VM 作为预配目标设备。

Profile Management

- 启用了启用 **Outlook** 的搜索索引漫游功能后，用户在 Microsoft Outlook 中搜索电子邮件时将显示以下错误消息：**Something went wrong and your search couldn't be completed**（出现错误，您的搜索无法完成）。出现此问题的原因是 Profile Management 无法将相关 API 挂接到 Windows 搜索服务。[UPM-3535]

Workspace Environment Management

- 尝试将 Windows Server 2022 配置为筛选条件的匹配结果（将客户端操作系统作为筛选条件类型）时，您会发现匹配结果菜单中缺少 Windows Server 2022。[WEM-14036]

已修复的问题

July 5, 2024

以下问题自 Citrix Virtual Apps and Desktops 7 2103 起已修复：

App-V

- 在 Windows Server 2016 上，在安装了“Citrix Personalization for App-V”组件的情况下将多会话操作系统 VDA 升级到版本 2103 失败，并显示错误消息“Installation of the Citrix Personalization for App-V-VDA failed with error code 1603”（安装 Citrix Personalization for App-V-VDA 失败，错误代码为 1603）。[APPV-383]

  要解决此问题，请执行以下操作：

  1. 升级 VDA 之前，请从当前 VDA 中删除“Citrix Personalization for App-V”组件。
  2. 重新启动计算机。
  3. 将 VDA 升级到版本 2103。
  4. 升级完成后，将“Citrix Personalization for App-V”组件添加到 VDA。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- App-V 包在 VFS 内的可执行文件的名称或路径中或快捷路径中包含特殊字符（例如撇号），可能会导致应用程序启动失败。[APPV-367]

Citrix Provisioning

Citrix Provisioning 2106 文档提供了有关此版本中的更新的具体信息。

Delivery Controller

- 使用特定的第三方应用程序服务将身份验证请求发送到 Delivery Controller 上的 XML 服务时，可能会出现性能问题。

  要启用此修复，请按如下所示设置此注册表项：

  HKEY_LOCAL_MACHINE\Software\Policies\Citrix\DesktopServer

  Name: DisableGetPasswordExpiryInfo

  类型：DWORD

  值：1

  [CVADHELP-15536]

- 在具有高延迟的多区域环境中，尝试将 XenApp 和 XenDesktop 版本 7.15 LTSR CU5 升级到 Citrix Virtual Apps and Desktops 版本 1912 CU1 可能会失败，但存在以下例外：**NullReferenceException**

  [CVADHELP-16236]

- 使用 UPN 凭据登录未代理的 RDP 会话可能会导致出现未捕获的异常。在 1912 LTSR CU2 中，引入了作为 UPN 提供的用户名的名称翻译。由于 RDS 数据结构中施加的限制，用户名被截断会产生错误的用户名，从而导致未捕获的异常。[CVADHELP-16510]

许可

许可证服务器内部版本 35000 文档提供了有关此版本中的更新的具体信息。

Linux VDA

Linux VDA 2106 文档提供了有关此版本中的更新的具体信息。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Microsoft Teams 优化

- HTML5 Video Redirection Service (txHdxWebSocketService) 可能会意外退出。[CVADHELP-17146]
- 在已发布的桌面中在 HDX 优化模式下使用 Microsoft Teams 时，音频通话可能会断开连接。[CVADHELP-17341]
- 在尝试加入通话时，Citrix HDX HTML5 Video Redirection Service (WebSocketService.exe) 可能会意外退出，导致通话失败。[CVADHELP-17424]
- 将 VDA 升级到版本 2103 后，Citrix HDX HTML5 Video Redirection Service (WebSocketService.exe) 可能会意外退出。[CVADHELP-17505]

Profile Management

Profile Management 2106 文档提供了有关此版本中的更新的具体信息。

Session Recording

Session Recording 2106 文档提供了有关此版本中的更新的具体信息。

适用于单会话操作系统的 VDA

键盘

- 当客户端上的克罗地亚语键盘布局映射到 Windows VDA 会话时，某些克罗地亚语键盘组合可能会显示错误的字符。[CVADHELP-16744]

打印

- 尝试从通过适用于 Chrome 的 Citrix Workspace 应用程序启动的会话打印 PDF 文件可能会失败。[CVADHELP-15318]
- 连接到托管的 HDX 会话时，客户端打印机可能无法重定向。[CVADHELP-16279]

会话/连接

- 通过 DisplayPort 将物理显示器连接到使用 NVIDIA 物理 GPU 的 RemotePC 时，显示器可能会显示空白屏幕。[CVADHELP-16022]
- 从启用了触控功能的端点连接到 VDA 版本 1912 时，屏幕键盘可能无法正常工作。在 VDA 上启用了 UAC 的非管理员用户会出现此问题。[CVADHELP-16045]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 尝试使用截图工具截取屏幕截图或执行复杂计算（例如数据透视表）时，可能会遇到性能问题。在 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics 注册表项下将 **CursorShapeChangeMinInterval** 的值设置为 50 时会出现此问题。[CVADHELP-16718]
- 启动会话后，Microsoft Windows 上运行的音频可能会显示无法删除的红色 X。[CVADHELP-16815]
- 启动 VM 托管应用程序，然后尝试从同一 VDA 启动第二个 VM 托管应用程序时，启动可能会失败。计算机目录使用静态分配时会出现此问题。[CVADHELP-16829]
- 使用某些第三方应用程序时，Websocketagent.exe 可能会使用很高比例的 CPU。启用了浏览器内容重定向或 **HTML5** 视频重定向策略时会出现此问题。[CVADHELP-17067]
- 在 VDA 中将 **DPI** 设置为 100% 以外的值时，**DPI** 值可能会重置为 100%。尝试锁定桌面时会出现此问题。[CVADHELP-17276]

系统异常

- VDA 上的 wdica.sys 可能会遇到致命异常，并显示蓝屏。[CVADHELP-16055]

适用于多会话操作系统的 **VDA**

打印

- 尝试从通过适用于 Chrome 的 Citrix Workspace 应用程序启动的会话打印 PDF 文件可能会失败。[CVADHELP-15318]
- 尝试使用 Citrix 通用打印机驱动程序 (UPD) 打印大型 Microsoft Excel 文件时，在正在后台处理 **-** 打印过程中可能会失败。[CVADHELP-16153]

会话**/**连接

- 在某些情况下，Citrix Studio 中显示的 Citrix 产品许可证使用情况与 Citrix License Manager 中显示的许可证使用情况不一致。[CVADHELP-14950]
- 重新连接到会话时，Citrix Audio Redirection Service (CtxAudioSvc) 可能会失败。在 Microsoft Windows 10 版本 2004 及更高版本上运行适用于多会话操作系统的 VDA 时会出现此问题。[CVADHELP-15804]
- 从启用了触控功能的端点连接到 VDA 版本 1912 时，屏幕键盘可能无法正常工作。在 VDA 上启用了 UAC 的非管理员用户会出现此问题。[CVADHELP-16045]
- 尝试使用截图工具截取屏幕截图或执行复杂计算（例如数据透视表）时，可能会遇到性能问题。在 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics 注册表项下将 **CursorShapeChangeMinInterval** 的值设置为 50 时会出现此问题。[CVADHELP-16718]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

系统异常

- VDA 上的 wdica.sys 可能会遇到致命异常，并显示蓝屏。[CVADHELP-16055]

虚拟桌面组件 - 其他

- 尝试在文件名中使用单引号启动可执行文件可能会失败。[CVADHELP-16104]

已知问题

January 4, 2023

备注

- Citrix Virtual Apps and Desktops 7 2106 版本包含以下问题。分开记录的组件和功能具有各自的已知问题文章。
- 如果已知问题有解决方法，则在问题说明后提供。
- 以下警告消息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。

安装和升级

- 将部署升级到此版本时，兼容性检查错误地报告“所需的 Customer Success Services 日期: 2021-08-15”。

  如果您看到此消息，并且您的 Customer Success Services 日期至少是 2021 年 5 月 15 日（2021-05-15）：

  - 如果您使用的是安装程序的图形界面，请继续升级。
  - 如果您使用的是命令行界面，请使用图形界面重新启动安装程序。

- 在包含 WEM 代理并指定 WEM Cloud Connector (`/includeadditional "Citrix WEM Agent"/wem_cloud_connectors "name1, name2"`) 的命令行 VDA 安装中，将安装 WEM 代理，但不处理 WEM Cloud Connector 配置。

  解决方法：在 VDA 安装完成后，运行 WEM 配置实用程序 (`AgentConfigurationUtility setup --cloud --connectors "name1, name2"`)。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

在使用 VDA 安装程序的图形界面或有本地 WEM 部署时，不会出现此问题。

[HDX-32102]

常规

- 从第一个端点断开用户会话，然后从第二个端点（瘦客户端）重新连接到同一个会话时，客户端音频设备可能会在 VDA 中以不正确的顺序列出。

  要启用此修复，请设置以下注册表项：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio

  名称：CleanMappingWhenDisconnect

  类型：DWORD

  值：1

  [CVADHELP-9986]

- 如果在 VDA 上安装 Citrix Workspace 应用程序并升级 VDA，客户端网络摄像机可能无法正确重定向虚拟会话中运行的 32 位应用程序。要解决此问题，请参阅 CTX291350。[CVADHELP-16854]
- 运行建模向导以生成建模结果报告后，Citrix Studio 将停止运行。必须在运行建模报告后重新启动 Studio，才能使用 Citrix Studio。[GP-753]
- 如果启动应用程序栏，然后在适用于 Windows 的 Citrix Workspace 应用程序中打开“连接中心”菜单，应用程序栏不会显示在对其进行托管的服务器下。[HDX-27504]
- 如果使用适用于 Windows 的 Citrix Workspace 应用程序并在垂直位置启动应用程序栏，该应用程序栏将覆盖“开始”菜单或系统时钟托盘。[HDX-27505]
- 如果您尝试将受保护的应用程序添加到收藏夹，则可能会显示此消息：“您的应用程序当前不可用…”单击确定时，将显示此消息：“无法添加应用程序”。切换到收藏夹屏幕后，受保护的应用程序将在此处列出，但无法将其从收藏夹中删除。[WSP-5497]
- 在启用了浏览器内容重定向的 Chrome 浏览器中，当您单击打开新选项卡的链接时，该选项卡可能无法打开。解决方法为，在 **Pop-ups blocked**（阻止了弹出窗口）消息中选择 **Always allow pop-ups and redirects**（始终允许弹出窗口和重定向）。[HDX-23950]
- 安装 Skype for Business Web 应用程序插件后，可能不会枚举网络摄像机，并且 Firefox 上的会议页面可能不会自动刷新。[HDX-13288]
- 从 StoreFront 启动应用程序时，该应用程序可能无法在前台启动，或者该应用程序在前台启动，但可能没有焦点。解决方法：单击任务栏中的图标将应用程序置于前面，或者单击应用程序屏幕中的图标将其置于焦点下。[HDX-10126]
- 连接到新会话、断开连接，然后重新连接到同一个会话时，桌面图标可能会闪烁不定。解决方法：重置用户配置文件，从会话中注销，然后重新登录。[HDX-15926、UPM-1362]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 使用 Windows 10 1809 LTSC 时，VCLibs 依赖项无法安装。[HDX-16754]
- 当用户选择已在主机上聚焦的组合框时，组合框可能无法正确显示。解决方法为，选择另一个 UI 元素，然后选择组合框。[HDX-21671]
- 您已启用本地应用程序访问。如果启动 Windows 2012 R2 VDA 会话，断开连接并重新连接会话，然后启动本地应用程序并将其最大化，则 VDA 任务栏可能会截断应用程序。[HDX-21913]
- 使用完整产品安装程序修改 VDA 安装时，可以通过选择启用 **MCSIO** 写入缓存以实现存储优化选项，将 MCSIO 存储优化添加到安装中。安装将继续进行，而不安装 MCSIO 驱动程序。[HDX-21754]
- 使用通用 USB 重定向将包含鼠标作为子设备的复合 USB 设备重定向到 RDS 会话中时，该设备可能不可用。最常见的此类设备是 Wacom 绘图平板电脑（不非 Wacom 签名板）。解决方法是，登录后在会话中手动启动 icak2meng.exe。我们建议您为 Windows 多会话操作系统 2016 或 2019 （Windows 10 不需要）创建一条自动启动 C:\Program Files\Citrix\HDX\bin\icak2meng.exe 的组策略。请创建该策略以在每个用户登录时在其会话中启动程序。每个用户的会话中只有一个实例运行。不需要解决方法 [HDX-25085]
- 如果在您的网络中配置了 IPv4 和 IPv6 寻址，则当交付组使用仅允许使用 IPv4 地址过滤的 Broker 访问策略规则时，交付组的资源可能无法访问。要确保所有资源筛选按预期运行，请将 Broker 访问策略规则配置为同时包括客户端 IPv4 和 IPv6 地址。[WADA-7776]

  例如，要设置允许通过“直接连接到 StoreFront”和“Citrix Gateway”访问的 IPv4 和 IPv6 地址的规则，请使用 PowerShell，例如：

```
Set-BrokerAccessPolicyRule -Name "Apps_Direct" -
    IncludedClientIPFilterEnabled $True -IncludedClientIPs @("
    10.0.0.1","2001::3")
Set-BrokerAccessPolicyRule -Name "Apps_AG" -
    IncludedClientIPFilterEnabled $True -IncludedClientIPs @("
    10.0.0.1","2001::3")
```

  要确认规则，请使用 PowerShell，例如：

```
Get-BrokerAccessPolicyRule -Name \"Apps\_Direct\" | Select Name,
    IncludedClientIPFilterEnabled,IncludedClientIPs
```

  如果为 IPv4 和 IPv6 地址正确设置了规则，此命令将返回以下内容：

```
Name         IncludedClientIPFilterEnabled IncludedClientIPs
--                   --------------------------- -----------------
Apps_Direct                            True {
10.0.0.1/32, 2001::3/128 }
```

- 从 Microsoft Office 365 Build 16.0.7967 及更高版本的应用程序发布为 Windows Server 2019 主机中的应用程序时，Office 许可证激活失败。Citrix 正在与 Microsoft 合作解决这个 Microsoft 限制。受支持的解决方法为安装 Windows Server 2016 VDA，该 VDA 没有行为不当的 Web 身份验证管理器组件。[LCM-7637]
- 如果配置使用专用许可证服务器，数据掩码不会掩盖许可证服务器。[XAXDTELE-1634]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- `BrokerHostingPowerAction` PowerShell cmdlet 运行后，Studio 日志记录显示屏幕会显示 cmdlet 失败，即使 cmdlet 已成功完成亦如此。解决方法为，检查主机上的结果。[BRK-7002]

Director

- “Citrix Director > 计算机详细信息”上的控制台链接不会在 Microsoft Edge 44 和 Firefox 68 ESR 浏览器中启动计算机控制台。[DIR-8160]
- 如果已升级到 Director 7 1903 或更高版本，但未清除浏览器缓存（未选中禁用缓存复选框），之前创建的自定义报告将丢失。此外，Director 会在自定义报告选项卡上显示`Unexpected Server error`。早期版本与当前版本的 Director 之间的 UI 设计差异会导致出现此问题。要查看早期的自定义报告并创建新报告，请禁用缓存并执行硬刷新。[DIR-7634]

图形

- 用户首次启动分配了 AMD GPU 的 Microsoft Hyper-V 或 Azure 实例上托管的虚拟桌面时，屏幕上会显示灰色边框。要解决此问题，请在远程会话中使用设备管理器禁用并启用 Citrix Indirect Display 驱动程序 (IDD)。[HDX-26222]
- 将策略拖动时查看窗口内容设置为禁止不适用于 ESXi 和 Hyper-V。[HDX-22002]
- 如果您通过 Theora 压缩使用 64 位网络摄像机应用程序启动视频预览，会话可能会崩溃。[HDX-21443]
- Skype 通用 Windows 应用程序 (UWA) 启动时背景为黑色。有时此背景占据客户端的整个屏幕。[HDX-22088]
- 有时，一个应用程序会在后台启动，而另一个应用程序则处于焦点中。因此，本地窗口排序丢失。[HDX-21569]
- 断开 XenDesktop 会话连接后，XenCenter 控制台可能会显示空白屏幕。解决方法：将 CTLR+ALT+DEL 发送到 XenCenter 控制台以显示控制台屏幕。[HDX-17261]
- 当 DPI 在客户端上发生更改且某个会话重新连接后，在 Windows 多会话操作系统 2016 或 2019 上运行该会话期间，DPI 可能不匹配。解决方法：调整会话窗口的大小以匹配 DPI。[HDX-17313]
- 这些问题适用于 AMD 硬件编码。[HDX-20476]：
  - 使用适用于 Windows 的 Citrix Workspace 应用程序时，可能会发生像素化。作为解决方法，请在已安装适用于 Windows 的 Citrix Workspace 应用程序的客户端上执行以下注册表设置：

    HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\GfxRenc
    （32 位）

    HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\M
    （64 位）

    名称：MaxNumRefFrames

    类型：DWORD

    值：5

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - 使用 4K 分辨率时，性能可能不是最优。此问题导致帧速率为每秒仅 7-10 帧。此外，编码时间也会延长。
  - 使用 Selective H.264 图形模式时，视频的前两到五秒可能会出现视频断断续续。RapidFire SDK 不是针对此用例而设计的。

打印

- 在虚拟桌面中选择的通用打印服务器打印机不会在“控制面板”的设备和打印机窗口中显示。但是，当用户在使用应用程序时，可以使用这些打印机。此问题仅出现在 Windows Server 2012、Windows 10 和 Windows 8 上。有关详细信息，请参阅 CTX213540。[HDX-5043、335153]
- 默认打印机在打印对话框窗口中可能不会正确标记。此问题不影响发送到默认打印机的打印作业。[HDX-12755]

第三方问题

- Chrome 仅支持工具栏、选项卡、菜单和 Web 页面周围的按钮的 UI 自动化。由于此 Chrome 问题，自动键盘显示功能可能无法在触控设备上的 Chrome 浏览器中工作。解决方法为，运行 `chrome --force-renderer-accessibility` 或打开新的浏览器选项卡，键入 `chrome://accessibility`，并为特定页面或所有页面启用本机辅助功能 **API** 支持。此外，发布无缝应用程序时，可以使用 `--force-renderer-accessibility` 开关发布 Chrome。[HDX-20858]
- 使用 Surface Pro 和 Surface Book 笔时，Microsoft Windows 10 版本 1809 中的某个问题可能会导致行为略微不稳定。[HDX-17649]
- 使用 Enlightened Data Transport (EDT) 时，Azure 上运行的 VDA 可能会冻结，要求会话重新连接。解决方法：在 Azure 环境中设置 edtMSS=1350 和 OutbufLength=1350。有关详细信息，请参阅 CTX231821。[HDX-12913]
- 在浏览器内容重定向中，使用 YouTube HTML5 视频播放器启动 YouTube 视频后，全屏模式可能不起作用。单击视频右下角的图标，视频不会调整大小，并在页面的整个区域留下黑色背景。解决方法：单击全屏按钮，然后选择影院模式。[HDX-11294]
- 当文件资源管理器 (explorer.exe) 作为应用程序发布在 Windows Server 2019 中时，创建、重命名或删除文件夹后显示内容不会正确刷新。解决方法：创建以下注册表项。[CTX263595]

  `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\EXPLORER.EXE`

  DWORD：DontUseDesktopChangeRouter

  值：1

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

弃用

September 19, 2023

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

弃用和删除

下表显示了已弃用或删除的平台、Citrix 产品和功能。以粗体显示的日期表示此版本的变更。

弃用

已弃用的项目不会立即删除。Citrix 在 Citrix Virtual Apps and Desktops 7 2106 中继续支持这些功能，但会在将来的版本中将其删除。

项目	宣布在版本中弃用	已在版本中删除	备选
将 Citrix Provisioning 目标设备导入到 Citrix Virtual Apps and Desktops 目录中进行管理	1912 LTSR	-	使用 Citrix Provisioning 导出设备向导
用于 Remote PC Access 的 SCCM 集成局域网唤醒选项。	2012		使用独立的局域网唤醒功能。
Citrix SCOM Management Packs for XenApp and XenDesktop、Provisioning Services 和 StoreFront。有关可以监视的产品版本，请参阅 Citrix SCOM Management Pack 文档。	1912		使用 Director 监视和管理您的部署。有关 SCOM EOL 和替代品的详细信息，请参阅 https://support.citrix.com/article/CTX266943。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

项目	宣布在版本中弃用	已在版本中删除	备选
StoreFront 在 Citrix Virtual Apps and Desktops（以前称为 XenApp 和 XenDesktop）和 Citrix Receiver 与 Workspace Hub 之间支持 TLS 1.0 和 TLS 1.1 协议。	7.17		请将 Citrix Receiver 升级到支持 TLS 1.2 协议的 Citrix Workspace 应用程序。有关 Citrix Workspace 应用程序的详细信息，请参阅 https://docs.citrix.com/en-us/citrix-workspace-app。
Mobility SDK/Mobile SDK（来自以前的 Citrix Labs）	7.16		取代为移动体验策略设置，以及托管桌面/应用程序的本机体验。

删除

在 Citrix Virtual Apps and Desktops 中，已删除的项目已被删除或不再受支持。

项目	宣布在版本中弃用	已在版本中删除	备选
Citrix 许可证管理控制台（最后一次包含在 Windows 许可证服务器 11.16.3 Build 30000 中，在 Windows 许可证服器 v11.16.6 Build 31000 中删除）。	2003	2006	使用 Citrix Licensing Manager。
Azure 和 AWS 公有云（包括 AWS 上的 VMware Cloud）连接。	2003	2003	请考虑在 Citrix Cloud 上使用 Virtual Apps and Desktops 服务。
Windows 10 版本 1709 及更高版本支持 Citrix Indirect Display Driver (IDD) 图形适配器。	2003	2003	使用 Citrix Virtual Apps and Desktops 7 1912 LTSR VDA。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

项目	宣布在版本中弃用	已在版本中删除	备选
通过使用 GRID 9 或更早版本的显示驱动程序的 Nvidia GPU (NVENC) 进行硬件编码。	2003	2003	将 GRID 10 显示驱动程序与 Citrix Virtual Apps and Desktops 7 2003 或更高版本的 VDA 结合使用，或者使用 Citrix Virtual Apps and Desktops 7 1912 LTSR VDA。
自助服务密码重置 (SSPR) 功能。	2003	2006	
支持适用于 VDA 和核心服务器组件的版本 4.8 之前的 Microsoft .NET Framework 版本。包括 Delivery Controller、Studio、Director 和 StoreFront。	1912	2003	升级到.NET Framework 版本 4.8。
Windows Server 2012 R2 上的 VDA。	1912	2003	在受支持的操作系统中安装 VDA。
Citrix Virtual Apps and Desktops Premium Edition 的 AppDNA 应用程序迁移组件。	1909	2003	
在 32 位 (x86) 计算机上安装 Studio。	1909	2003	在受支持的 x64 操作系统中安装。
支持无缝应用程序中的 Excel 挂钩。这用于为每个 Microsoft Excel 2010 工作簿创建单独的任务栏图标。	1909	1909	
Windows Server 2012 R2（包括 Service Pack）上的核心服务器组件。包括：Delivery Controller、Studio 和 Director。	1906	2003	在较新的受支持操作系统中安装。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

项目	宣布在版本中弃用	已在版本中删除	备选
在 Microsoft SQL Server 2008 R2、2012 和 2014（包括所有 Service Pack 和版本）支持站点配置数据库、配置日志记录数据库和监视数据库。	1906	2003	在受支持的 Microsoft SQL Server 版本上安装数据库。
在 x86 平台上支持 Windows 10 上的 VDA。	1906	1909*	在受支持的 x64 操作系统上安装 VDA。* 此功能在 Citrix Virtual Apps and Desktops 7 1912 LTSR 中仍受支持。
从 Citrix Virtual Apps and Desktops 安装介质中删除了 Citrix Smart Tools Agent。	1903	1906	
在 StoreFront 中删除了以下生命周期已结束产品的 Delivery Controller 选项：VDI-in-a-Box 和 XenMobile（9.0 或更低版本）。	1903	1903	
Red Hat Enterprise Linux/CentOS 7.5 对 Linux VDA 的支持。	1903	1903	在更高版本的 Red Hat Enterprise Linux 上安装 Linux VDA。
StoreFront 支持用户访问桌面设备站点上的桌面	1811	1912	将 Desktop Lock 用于未加入域的用例。
支持 Framehawk 显示远程技术	1811	1903	使用启用了自适应传输的 Thinwire。
所有 Citrix Virtual Apps and Desktops（以及 XenApp 和 XenDesktop）版本都支持 Citrix Smart Scale。此功能将于 2019 年 5 月 31 日达到生命周期已结束状态。	1808	1906	考虑在 Citrix Cloud 上使用 Virtual Apps and Desktops 服务，以改进电源管理功能。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

项目	宣布在版本中弃用	已在版本中删除	备选
Citrix StoreFront、Citrix VDA、Citrix Studio、Citrix Director 和 Citrix Delivery Controller 支持 Microsoft .NET Framework 4.5.1、4.5.2、4.6、4.6.1、4.6.2 和 4.7。	7.18	1808	升级到.NET Framework 4.7.1 或更高版本。（如果尚未安装.NET Framework 4.7.1，安装程序将自动安装。）
Red Hat Enterprise Linux 7.3 支持 Linux VDA。	7.18	1808	在更高版本的 Red Hat Enterprise Linux 上安装 Linux VDA。
VDA 支持策略设置“自动安装现成的打印机驱动程序”	7.16	7.16	无。仅在早期版本的操作系统（Windows 7、Windows Server 2012 R2 及早期版本）中的 VDA 上支持的策略设置。
在 SUSE Linux Enterprise Server 11 Service Pack 4 上支持 Linux VDA。	7.16	7.16	应在受支持的 SUSE 版本上安装 Linux VDA。
支持在 VDA 上使用 Citrix WDDM 驱动程序	7.16	7.16	Citrix WDDM 驱动程序不再与 VDA 一起安装。
Windows 10 版本 1511 (Threshold 2) 及早期版本的 Windows 单会话操作系统版本（包括 Windows 8.x 和 Windows 7）上的 VDA）（请参阅 https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/）。	7.15 LTSR（和 7.12）	7.16	在 Windows 10 最低版本 1607 (Redstone 1) 或更高版本的 Semi-Annual Channel 上安装单会话操作系统 VDA。如果使用的是 1607 LTSB，我们建议使用 7.15 VDA。请参阅 CTX224843。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

项目	宣布在版本中弃用	已在版本中删除	备选
Windows Server 2008 R2 和 Windows Server 2012（包括 Service Pack）上的 VDA	7.15 LTSR（和 7.12）	7.16	在受支持的操作系统中安装 VDA。
桌面组合重定向（以前称为 DirectX Command Remoting）(DCR)	7.15 LTSR	7.16	使用 Thinwire。
Citrix Receiver for Web 经典体验（“绿色气泡”用户界面）	7.15 LTSR（和 StoreFront 3.12）	1903	Citrix Receiver for Web 统一体验。
Windows Server 2012 和 Windows Server 2008 R2（包括 Service Pack）上的核心组件。包括：Delivery Controller、Studio、Director、StoreFront、许可证服务器和通用打印服务器。	7.15 LTSR	7.18	在受支持的操作系统中安装组件。
Windows Server 2012 和 Windows Server 2008 R2（包括 Service Pack）中的自助服务密码重置 (SSPR) 功能	7.15 LTSR	7.18	在较新的受支持操作系统中安装。
Windows 7、Windows 8 和 Windows 8.1（包括 Service Pack）中的 Studio	7.15 LTSR	7.18	在受支持的操作系统中安装 Studio。
Flash 重定向	7.15 LTSR	1912	创建视频内容为 HTML5 视频。对托管内容使用 HTML5 视频重定向，对公共 Web 站点使用浏览器内容重定向。有关详细信息，请参阅 Flash 重定向生命周期已结束备注。
与 StoreFront 的 Citrix Online 集成（Goto 产品）	7.14（和 StoreFront 3.11）	StoreFront 3.12	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

项目	宣布在版本中弃用	已在版本中删除	备选
以前在 VDA 安装期间创建并添加到 VDA 计算机上的本地管理员组中的用户帐户 CtxAppVCOMAdmin 现在不再创建。此外，也删除了基础“COM”机制。	7.14	7.14	Windows 服务 CtxAppVService 执行相同的功能。它会自动安装并配置，无需执行任何用户交互。
Windows Server 2008（32 位）支持通用打印服务器 UpsServer 组件	7.14	7.14	在较新的受支持操作系统中安装。
Internet Explorer 8 上的 StoreFront 和 Receiver for Web	7.13	7.13	
用于阻止安装 Citrix App-V 组件的 VDA 命令行安装选项 /no_appv	7.13	7.13	应使用命令行安装选项 /exclude “Citrix Personalization for App-V –VDA”。
完整产品安装程序不再在新安装中安装 Citrix.Common.Commands 管理单元，并在升级现有安装时自动将其删除。	7.13	7.13	Citrix.Common.Commands 管理单元提供的一些 PowerShell 命令在 XenApp 6.5 SDK 中仍可用。
*-CtxIcon cmdlet 提供的用于操纵图标数据的部分功能。	7.13	7.13	现在由 Broker Service 中的 *-BrokerIcon cmdlet 提供。
旧 Thinwire 模式	7.12	7.16	使用 Thinwire。如果您要使用 Windows Server 2008 R2 上的旧 Thinwire 模式，请迁移到 Windows Server 2012 R2 或 Windows Server 2016，然后使用 Thinwire。
StoreFront 2.0、2.1、2.5 和 2.5.2 中的原位升级	7.13	7.16	从其中一个版本升级到受支持的更高版本，然后升级到 XenApp 和 XenDesktop 7.16。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

项目	宣布在版本中弃用	已在版本中删除	备选
XenDesktop 5.6 或 5.6 FP1 中的原位升级	7.12	7.16	将 XenDesktop 5.6 或 5.6 FP1 部署迁移到当前 XenDesktop 版本。为此，请先升级到 XenDesktop 7.6 LTSR（包含最新的 CU），然后升级到最新版本的 Citrix Virtual Desktops（以前称为 XenDesktop）或 LTSR 版本。
在 32 位 (x86) 计算机上安装 Delivery Controller、Director、StoreFront 或许可证服务器。	7.12	7.16	在受支持的 x64 操作系统中安装。
连接租用	7.12	7.16	使用本地主机缓存。
Windows XP 上使用的 XenDesktop 5.6。不支持在 Windows XP 中安装 VDA。	7.12	7.16	在受支持的操作系统中安装 VDA。
支持 CloudPlatform 连接	7.12	2003	应使用其他受支持的虚拟机管理程序或云服务。
支持 Azure 经典（也称为 Azure 服务管理）连接	7.12	2003	请考虑在 Citrix Cloud 上使用 Virtual Apps and Desktops 服务。
AppDisk 功能（以及集成到 Studio 中支持该功能的 AppDNA）	7.13	2003	使用 Citrix App Layering。
Personal vDisk 功能	7.15	2006†	使用 Citrix App Layering 用户层或用户个性化层技术。

† 在 Citrix Virtual Apps and Desktops 7 2003 中，Personal vDisk 驱动程序已从 VDA 安装程序中移除。在 Citrix Virtual Apps and Desktops 7 2006 中，Personal vDisk 驱动程序工作流已从 Studio 中删除。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

系统要求

July 5, 2024

简介

本文档中的系统要求适用于此发布版本的产品。将定期进行更新。本文档中未涉及的组件（例如主机系统、Citrix Workspace 应用程序以及 Citrix Provisioning）的系统要求在其各自的文档中进行说明。

请在开始安装之前阅读准备安装一文。

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。

有关全球化信息，请参阅知识中心文章 CTX119253。

对于可以安装在 Windows Server 上的组件和功能，除非另有说明，否则不支持 Nano 服务器安装。只有 Delivery Controller 和 Director 支持服务器核心。

硬件要求

RAM 和磁盘空间值是对计算机上的产品映像、操作系统和其他软件的附加。性能会有所不同，具体取决于您的配置。这包括您使用的功能，以及用户数和其他因素。仅使用最低配置会导致性能缓慢。

下表列出了核心组件的最低要求。

组件	最低
所有核心组件和 StoreFront 都位于一台服务器上，仅供评估使用，不用于生产部署	5 GB RAM
所有核心组件和 StoreFront 都位于一个服务器上，供测试部署或小型的生产环境	12 GB RAM
Delivery Controller（本地主机缓存需要更多磁盘空间）	5 GB RAM、800 MB 硬盘、数据库：请参阅大小调整指南
Studio	1 GB RAM，100 MB 硬盘
Director	2 GB RAM，200 MB 硬盘
StoreFront	2 GB RAM，请参阅 StoreFront 文档获取磁盘建议
许可证服务器	2 GB RAM，请参阅许可文档获取磁盘建议

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

对可提供桌面和应用程序的 **VM** 进行大小调整

由于硬件产品的复杂性和不确定性，无法提供具体的建议，而且每个部署都有各自的独特需求。通常来说，调整 Citrix Virtual Apps VM 的大小是基于硬件而非用户工作负载进行的。例外是 RAM。对于占用更多 RAM 的应用程序，您需要更多 RAM。

相关详细信息：

- Citrix VDI Handbook and Best Practices（Citrix VDI 手册和最佳做法）包含有关调整大小的指导信息。
- Citrix Virtual Apps and Desktops 单服务器可扩展性 探讨了单个物理主机上可支持多少用户或 VM。

Microsoft Visual C++ 2017 Runtime

在已安装 Microsoft Visual C++ 2015 运行时的计算机上安装 Microsoft Visual C++ 2017 运行时可能会导致自动删除 Visual C++ 2015 运行时。这是设计使然。

如果您已安装会自动安装 Visual C++ 2015 运行时的 Citrix 组件，这些组件将继续在安装了 Visual C++ 2017 版本的情况下正常运行。

有关详细信息，请参阅 Microsoft 文章 https://developercommunity.visualstudio.com/content/problem/332815/visual-c-redistributable-2017-install-removes-visu.html。

Delivery Controller

支持的操作系统：

- Windows Server 2022
- Windows Server 2019 Standard Edition 和 Datacenter Edition，包含服务器核心选项
- Windows Server 2016 Standard Edition 和 Datacenter Edition，包含服务器核心选项

要求：

- 如果尚未安装.NET Framework 4.8（或更高版本），该框架将自动安装。
- Microsoft Internet Information Services（自动安装，当前由 Citrix Orchestration Service 在部署中安装的一项功能使用）。
- Windows PowerShell 3.0 或更高版本。
- Microsoft Visual C++ 2017 Runtime（32 位和 64 位）。

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 2019 Express Edition、Standard Edition 和 Enterprise Edition。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- SQL Server 2017 Express Edition、Standard Edition 和 Enterprise Edition。
  - 对于新安装：默认情况下，如果未检测到支持的现有 SQL Server 安装，安装 Controller 时将安装带累积更新 16 的 SQL Server Express 2017。
  - 对于升级，任何现有 SQL Server Express 版本都不会升级。
- SQL Server 2016 SP2，Express Edition、Standard Edition 和 Enterprise Edition。

支持下列数据库高可用性解决方案（SQL Server Express 除外，此版本仅支持独立模式）：

- SQL Server AlwaysOn 故障转移群集实例
- SQL Server AlwaysOn 可用性组（包括 Basic 可用性组）
- SQL Server 数据库镜像

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

本地主机缓存注意事项： Microsoft SQL Server Express LocalDB 是本地主机缓存独立使用的 SQL Server Express 功能。本地主机缓存不需要除 SQL Server Express LocalDB 以外的 SQL Server Express 的任何组件。

- 安装 Controller 时，将安装带累积更新 16 的 Microsoft SQL Server Express LocalDB 2017 以与本地主机缓存功能一起使用。（此安装与针对站点数据库的默认 SQL Server Express 安装不同。）
- 升级 Controller 时，不自动升级现有的 Microsoft SQL Server Express LocalDB 版本。有关替换要求和步骤，请参阅替换 SQL Server Express LocalDB。

更多数据库信息：

- 数据库
- CTX114501 列出了受支持的最新数据库
- 数据库大小调整指南
- 本地主机缓存

Citrix Studio

支持的操作系统：

- Windows Server 2022
- Windows Server 2019 Standard Edition 和 Datacenter Edition
- Windows Server 2016 Standard Edition 和 Datacenter Edition
- Windows 10（仅限 64 位）

要求：

- 如果尚未安装.NET Framework 4.8（或更高版本），该框架将自动安装。
- Microsoft Management Console 3.0（随所有支持的操作系统提供）。
- Windows PowerShell 3.0 或更高版本。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Director

支持的操作系统：

- Windows Server 2022
- Windows Server 2019 Standard Edition 和 Datacenter Edition，包含服务器核心选项
- Windows Server 2016 Standard Edition 和 Datacenter Edition，包含服务器核心选项

要求：

- 如果尚未安装.NET Framework 4.8（或更高版本），该框架将自动安装。
- Microsoft Internet Information Services (IIS) 7.0 和 ASP.NET 2.0。确保 IIS 服务器角色安装了静态内容角色服务。如果尚未安装此软件，系统将提示您插入 Windows Server 安装介质。然后，将为您安装该软件。
- 必须安装 Microsoft .NET Framework 2.0，才能查看安装了 Citrix Director 的计算机上的事件日志。

Citrix Profile Management：

- 确保 Citrix Profile Management 和 Citrix Profile Management WMI 插件安装在 VDA（安装向导中的附加组件页面）上，并且 Citrix Profile Management Service 正在运行，以查看 Director 中的用户配置文件详细信息。

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。Internet Explorer 不支持兼容模式。请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。如果已安装该浏览器，但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。

推荐的用于查看 Director 的最佳屏幕分辨率为 1366 x 1024。

适用于单会话操作系统的 Virtual Delivery Agent (VDA)

支持的操作系统：

- Windows 10（仅限 x64），最低版本 1607。
  - 有关版本支持，请参阅知识中心文章 CTX224843。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - 有关版本 1709 的 Citrix 已知问题，请参阅知识中心文章 CTX229052。

要求：

- 如果尚未安装.NET Framework 4.8（或更高版本），该框架将自动安装。
- Microsoft Visual C++ 2017 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）。此 VDA 在 Windows 10 上支持面向 Citrix Virtual Desktops Remote PC Access 的安全启动。

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 软件后从计算机中删除媒体基础。否则，用户将无法登录到此计算机。在大多数受支持的 Windows 单会话操作系统版本上，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。有关详细信息，请参阅准备安装。

有关 Linux VDA 的信息，请参阅 Linux Virtual Delivery Agent 各文章。

要使用服务器 VDI 功能，可以在受支持的 Windows Server 计算机上使用命令行界面安装适用于 Windows 单会话操作系统的 VDA。有关指导，请参阅服务器 VDI。

有关在 Windows 7 计算机上安装 VDA 的信息，请参阅早期版本的操作系统。

适用于多会话操作系统的 **Virtual Delivery Agent (VDA)**

支持的操作系统：

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

安装程序将自动部署以下要求，这些要求还可以在 Citrix 安装介质上的 **Support** 文件夹中找到：

- 如果尚未安装.NET Framework 4.8（或更高版本），该框架将自动安装。
- Microsoft Visual C++ 2017 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 版本上，通过服务器管理器安装媒体基础功能。有关详细信息，请参阅准备安装。

如果 VDA 上不存在媒体基础，这些多媒体功能将不起作用：

- Windows Media 重定向
- HTML5 视频重定向

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- HDX RealTime 网络摄像机重定向

有关 Linux VDA 的信息，请参阅 Linux Virtual Delivery Agent 各文章。

有关在 Windows Server 2008 R2 计算机上安装 VDA 的信息，请参阅早期版本的操作系统。

主机/虚拟化资源

> 重要：
>
> 如果您正在升级，并且您的当前版本使用 Microsoft Azure、Amazon Web Services 或 Citrix CloudPlatform 连接，请参阅删除不受支持的主机项目中的要求。

支持以下主机/虚拟化资源（按字母顺序列出）。如果适用，则支持以下 *major.minor* 版本，包括这些版本的更新。知识中心文章 CTX131239 包含当前版本信息以及指向已知问题的链接。

某些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。有关详细信息，请参阅相关功能的文档。

Remote PC Access 局域网唤醒功能至少需要 Microsoft System Center Configuration Manager 2012 版。

- **Citrix Hypervisor**（以前称为 **XenServer**）

  CTX131239 包含当前版本信息，以及指向已知问题的链接。

  有关详细信息，请参阅 Citrix Hypervisor 虚拟化环境。

- **Microsoft 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。

  CTX131239 包含当前版本信息，以及指向已知问题的链接。

  有关详细信息，请参阅 Microsoft System Center Virtual Machine Manager 虚拟化环境。

- **Nutanix Acropolis**

  CTX131239 包含当前版本信息，以及指向已知问题的链接。

  有关详细信息，请参阅 Nutanix 虚拟化环境。

- **VMware vSphere (vCenter + ESXi)**

  不支持 vSphere vCenter“链接模式”操作。

  CTX131239 包含当前版本信息，以及指向已知问题的链接。

  有关详细信息，请参阅 VMware 虚拟化环境。

Active Directory 功能级别

支持以下 Active Directory 林和域功能级别：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

HDX

音频

适用于 Windows 的 Citrix Workspace 应用程序和适用于 Linux 13 的 Citrix Workspace 应用程序支持多流 ICA 的 UDP 音频。

适用于 Windows 的 Citrix Workspace 应用程序支持回声消除。

请参阅下文具体的 HDX 功能支持和要求。有关 HDX 功能和 Citrix Workspace 应用程序的详细信息，请参阅功能列表。

HDX Windows Media 交付

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：适用于 Windows 的 Citrix Workspace 应用程序、适用于 iOS 的 Citrix Workspace 应用程序以及适用于 Linux 的 Citrix Workspace 应用程序。

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 https://developer.nvidia.com/cuda/cuda-gpus。

HDX 3D Pro

适用于 Windows 单会话操作系统的 VDA 将在运行时检测是否存在 GPU 硬件。

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：

- GPU 直通功能可用于：
  - Citrix XenServer
  - Nutanix AHV
  - VMware vSphere 和 VMware ESX，此时它称为虚拟直接图形加速 (VDGA)
  - Windows Server 2016 中的 Microsoft Hyper-V，称为离散设备分配 (Discrete Device Assignment, DDA)。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- vGPU 提供以下功能：
  - Citrix Hypervisor
  - Nutanix AHV
  - VMware vSphere

请参阅 https://www.citrix.com/products/xenapp-xendesktop/hdx-3d-pro.html。

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。
- 为了通过使用 NVIDIA GRID API 实现虚拟化图形加速，可以将 HDX 3D Pro 与 GRID 10 驱动程序支持的所有 NVIDIA GRID GPU 结合使用（请参阅 NVIDIA GRID）。NVIDIA GRID 将提供高帧速率，从而实现高度互动的用户体验。
- 数据中心图形平台的 Intel Xeon Processor E3 系列支持虚拟化图形加速。有关详细信息，请参阅https://www.citrix.com/intel和https://www.intel.com/content/www/us/en/servers/data-center-graphics.html。
- AMD FirePro S 系列服务器卡上的 AMD RapidFire 支持虚拟化图形加速。请参阅 AMD 虚拟化解决方案）。

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。
- 对于多显示器访问，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 Workspace 应用程序。

有关详细信息，请参阅 HDX 3D Pro 各文章和 www.citrix.com/xenapp/3d。

通用打印服务器

通用打印服务器由客户端和服务器组件组成。UpsClient 组件包含在 VDA 安装中。UpsServer 组件安装在每台打印服务器上，在用户会话中通过 Citrix 通用打印驱动程序预配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 2022
- Windows Server 2019

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Windows Server 2016

要求：

- Microsoft Visual C++ 2017 Runtime x86 和 x64
- Microsoft .NET Framework 4.8（最低版本）

对于适用于多会话操作系统的 VDA，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器组件软件包。

有关详细信息，请参阅预配打印机。

其他

仅支持 Citrix 许可证服务器 11.16 及更高版本。有关详细信息，请参阅许可。

在本版本中使用 Citrix Provisioning（以前称为 Provisioning Services）时，XenApp and XenDesktop 7.x 生命周期和 Citrix Virtual Apps and Desktops 生命周期中包含版本 7.x。有关版本兼容性的详细信息，请参阅产品列表。

有关支持的 StoreFront 版本, 请参阅 StoreFront 系统要求。

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)。如果单独安装 `CitrixGroupPolicyManagement_x64.msi`（例如，在未安装 Citrix Virtual Apps and Desktops 核心组件的计算机上），相应的计算机上必须安装 Visual Studio 2015 Runtime。有关详细信息，请参阅 Microsoft 文档。

如果要使用 GPMC 编辑域 GPO，请在包含 Delivery Controller 的所有计算机上启用组策略管理功能（在 Windows 服务器管理器中）。

支持多个 NIC。

默认情况下，安装当前的 VDA 时将不安装适用于 Windows 的 Citrix Workspace 应用程序。有关详细信息，请参阅适用于 Windows 的 Citrix Workspace 应用程序文档。

有关受支持的 Microsoft App-V 版本，请参阅 App-V。

有关该功能支持的浏览器信息，请参阅本地应用程序访问。

此版本的 Citrix Virtual Apps and Desktops 至少需要 HDX RealTime Connector 2.9 LTSR。有关详细信息，请参阅 HDX RealTime Optimization Pack 文档。

技术概述

April 3, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Virtual Apps and Desktops 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。

Citrix Virtual Apps and Desktops 允许执行以下操作：

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

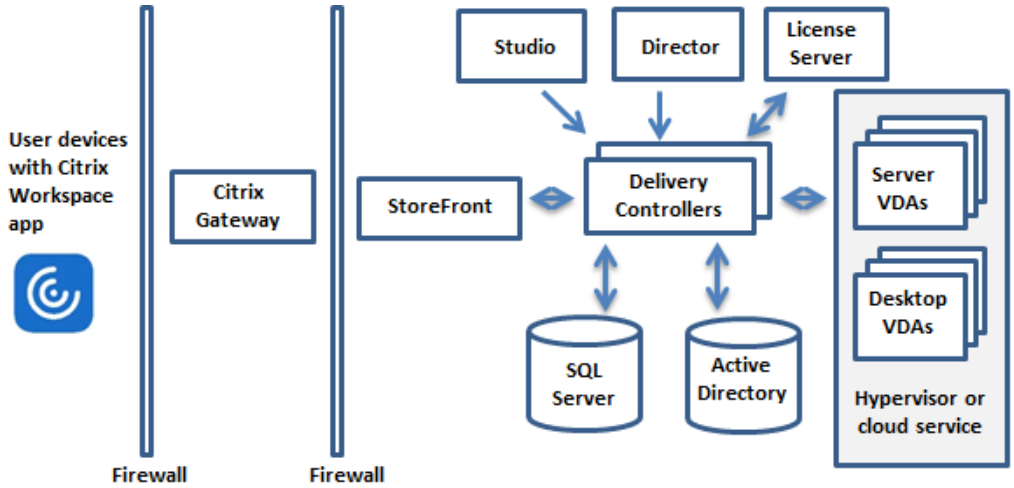
Citrix Virtual Apps and Desktops 共享统一的体系结构 FlexCast Management Architecture (FMA)。FMA 的主要功能是可以通过单个站点和集成预配运行多个版本的 Citrix Virtual Apps 或 Citrix Virtual Desktops。

了解与产品名变更有关的信息。

主要组件

如果您是 Citrix Virtual Apps and Desktops 的新用户，本文将非常有用。如果您当前拥有 6.x 或更低版本的 XenApp 场或者 XenDesktop 5.6 或更低版本的站点，也请参阅 7.x 中的变更。

此图显示了典型部署（称为“站点”）中的主要组件。



Delivery Controller

Delivery Controller 是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，将 Controller 安装在多个服务器上。如果您的部署中包括虚拟机管理程序或其他服务，Controller 服务将与其进行通信，以：

- 分发应用程序和桌面
- 对用户进行身份验证和管理用户访问
- 代理用户与其桌面和应用程序之间的连接。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 优化用户连接
- 对这些连接进行负载平衡。

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

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

来自 Controller 服务的数据存储在站点数据库中。

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

数据库

每个站点至少需要一个 Microsoft SQL Server 数据库，用于存储配置和会话信息。此数据库存储组成 Controller 的服务所收集并管理的数据。在数据中心内安装此数据库，并确保此数据库与 Controller 建立持续型连接。

站点还使用一个配置日志记录数据库和一个监视数据库。默认情况下，这些数据库与站点数据库安装在相同的位置，但您可以对此进行更改。

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。这些计算机提供应用程序或桌面。VDA 使计算机能够向 Controller 注册，Controller 进而允许向用户提供它所托管的计算机和资源。VDA 建立并管理计算机与用户设备之间的连接。VDA 还验证 Citrix 许可证是否对用户或会话可用，并应用为会话配置的策略。

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

“VDA”一词通常用于指代理和安装了该代理的计算机。

VDA 可用于单会话和多会话 Windows 操作系统。适用于多会话 Windows 操作系统的 VDA 允许多个用户同时连接到服务器。适用于单会话 Windows 操作系统的 VDA 每次仅允许一个用户连接到桌面。还可以使用 Linux VDA。

Citrix StoreFront

StoreFront 负责对用户进行身份验证，并管理用户访问的桌面和应用程序的存储。它可以托管企业应用商店，使用户可以自助访问您为其提供的桌面和应用程序。StoreFront 还跟踪用户的应用程序订阅、快捷方式名称以及其他数据。这有助于确保用户在多个设备之间具有一致的体验。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Workspace 应用程序

Citrix Workspace 应用程序安装在用户设备和其他端点（例如虚拟桌面）上，使用户能够快速、安全地自助访问文档、应用程序和桌面。通过 Citrix Workspace 应用程序，可以按需访问 Windows、Web 和软件即服务 (SaaS) 应用程序。对于无法安装设备特定的 Citrix Workspace 应用程序软件的设备，适用于 HTML5 的 Citrix Workspace 应用程序通过与 HTML5 兼容的 Web 浏览器提供了一个连接。

Citrix Studio

Studio 是在其中配置和管理 Citrix Virtual Apps and Desktops 部署的管理控制台。Studio 无需在单独的管理控制台中管理应用程序和桌面的交付。Studio 提供的向导将指导您完成设置环境、创建托管应用程序和桌面的工作负载以及将应用程序和桌面分配给用户的操作。还可以使用 Studio 为站点分配和跟踪 Citrix 许可证。

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

Citrix Director

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

Director 显示：

- 来自 Controller 中的 Broker Service 的实时会话数据，其中包括 Broker Service 从 VDA 中的 Broker Agent 获取的数据。
- 来自 Controller 中的 Monitor Service 的历史站点数据。

Director 使用 Citrix Gateway 设备捕获的 ICA 性能和启发数据来基于数据生成分析信息，然后将其呈现给管理员。

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

Citrix 许可证服务器

许可证服务器管理您的 Citrix 产品许可证。它与 Controller 通信以管理每个用户会话的许可，与 Studio 通信以分配许可证文件。站点必须至少具有一个许可证服务器以存储和管理您的许可证文件。

虚拟机管理程序或其他服务

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Virtual Apps and Desktops 支持各种虚拟机管理程序和其他服务。

虽然许多部署都需要虚拟机管理程序，但您不需要虚拟机管理程序即可提供 Remote PC Access。使用 Provisioning Services (PVS) 预配 VM 时，也不需要虚拟机管理程序。

其他组件

以下组件也可以包含在 Citrix Virtual Apps and Desktops 部署中。有关详细信息，请参阅其文档。

Citrix Provisioning

Citrix Provisioning（以前称为 Provisioning Services）是在某些版本中提供的一个可选组件。它是 MCS 的备选方式，用于预配虚拟机。MCS 创建主映像的副本，PVS 通过流技术将主映像推送到用户设备。PVS 执行此操作时无需使用虚拟机管理程序，因此，您可以使用它来托管物理机。PVS 与 Controller 通信以向用户提供资源。

Citrix Gateway

用户从公司防火墙外部连接时，Citrix Virtual Apps and Desktops 可以使用 Citrix Gateway（以前称为 Access Gateway 和 NetScaler Gateway）技术保护这些与 TLS 的连接的安全性。Citrix Gateway 或 VPX 虚拟设备是在隔离区域 (DMZ) 中部署的 SSL VPN 设备。它通过公司防火墙提供单个安全访问点。

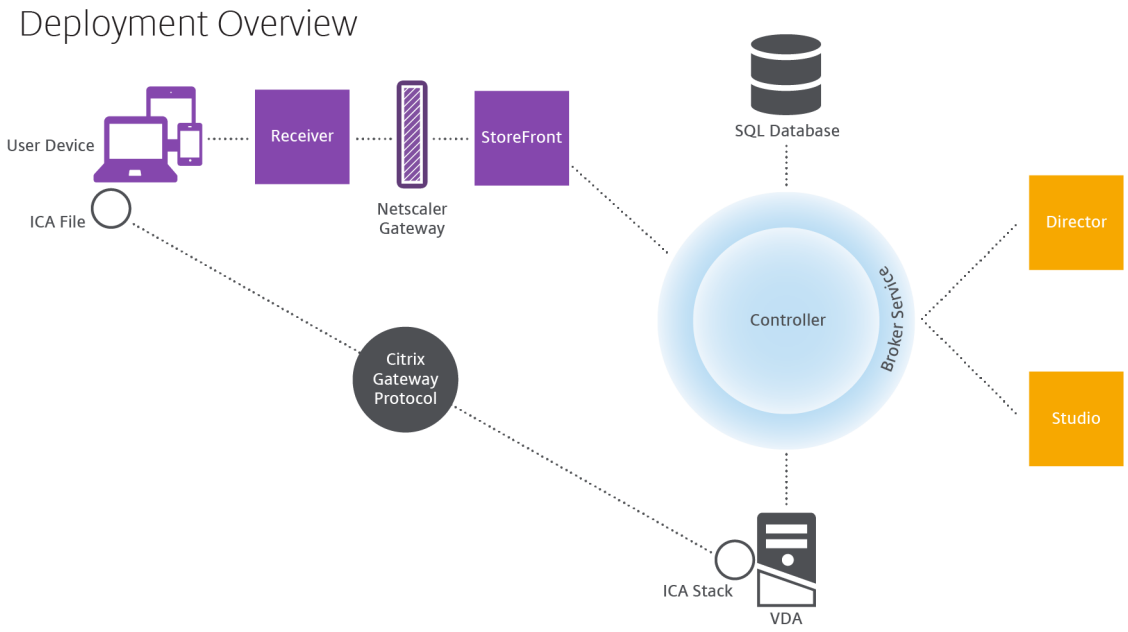
Citrix SD-WAN

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

典型部署的工作原理

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

Controller 由独立的 Windows 服务组成，用于管理资源、应用程序和桌面，并优化和平衡用户连接。每个站点有一个或多个 Controller。由于会话受延迟、带宽和网络可靠性的影响，因此如有可能，请将所有 Controller 放置在同一个 LAN 中。

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 登录时，其凭据将传递到 Controller 上的 Broker Service。然后，Broker Service 将根据为其设置的策略获取配置文件和可用的资源。

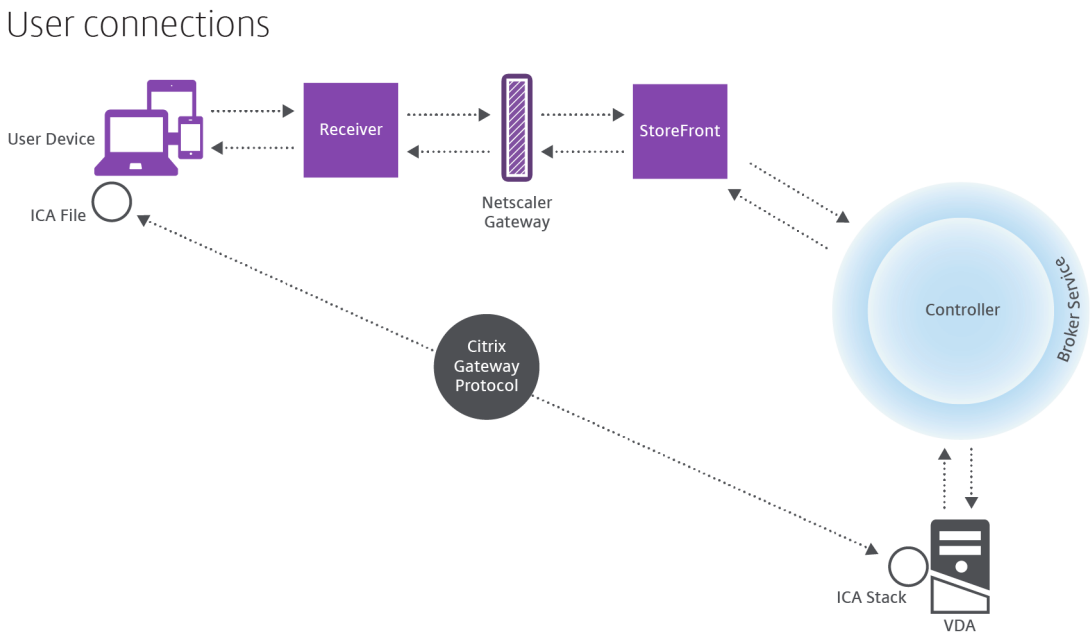
用户连接的处理方式

要启动会话，用户将通过用户设备上安装的 Citrix Workspace 应用程序或 StoreFront Web 站点进行连接。

用户选择所需的物理桌面、虚拟桌面或虚拟应用程序。

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Broker Service 决定允许用户访问的桌面和应用程序。

验证凭据后，有关可用应用程序或桌面的信息将通过 StoreFront-Citrix Workspace 应用程序路径发送回用户。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 随后决定托管特定应用程序或桌面的 VDA。

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

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

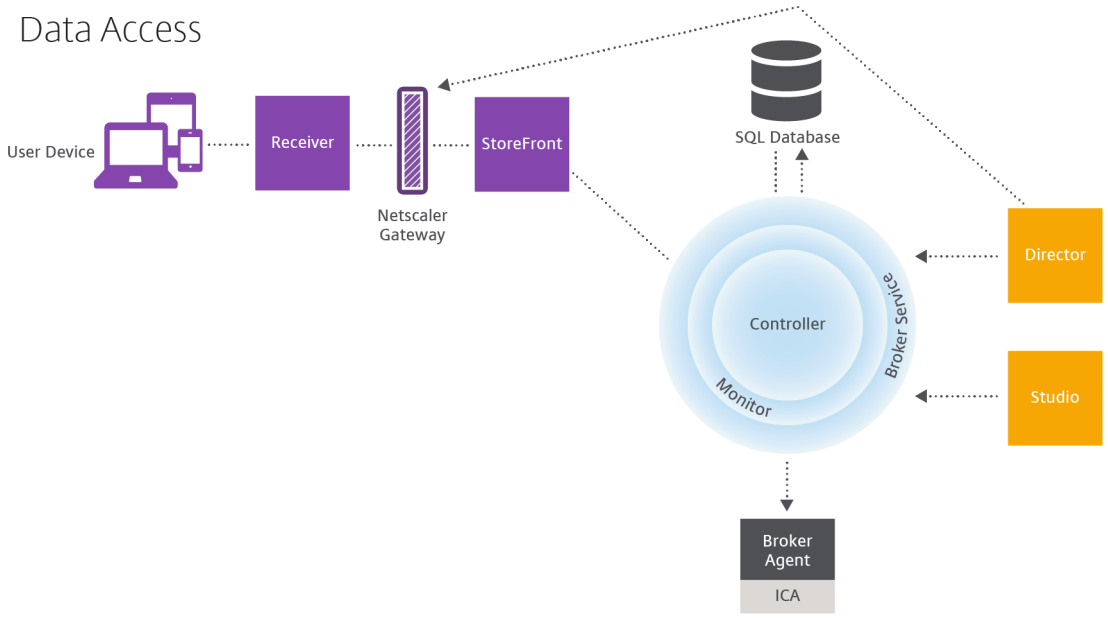
Citrix Workspace 应用程序与 VDA 之间的连接使用 Citrix Gateway 协议 (CGP)。如果连接丢失，通过会话可靠性功能，用户可以重新连接到 VDA，而无需通过管理基础结构重新启动。可以在 Citrix 策略中启用或禁用会话可靠性。

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

数据访问的工作方式

每个 Citrix Virtual Apps and Desktops 会话都将生成 IT 能够通过 Studio 或 Director 访问的数据。通过使用 Studio，管理员可以访问 Broker Agent 中的实时数据，以便管理站点。Director 访问监视数据库中存储的相同数据以及历史数据。它还从 NetScaler Gateway 访问 HDX 数据以便技术支持人员提供支持以及进行故障排除。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

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

Director 还可以访问 Citrix Gateway 以获取与 HDX 数据有关的信息。

交付桌面和应用程序

为计算机目录设置将交付应用程序和桌面的计算机。然后，创建交付组，交付组指定将提供的应用程序和桌面（使用目录中的计算机）以及哪些用户可以访问它们。（可选）之后可以创建应用程序组来管理应用程序的集合。

计算机目录

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

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

有效的计算机类型包括：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 多会话操作系统：具有多会话操作系统的虚拟机或物理计算机。用于交付 Citrix Virtual Apps 发布的应用程序（也称为基于服务器的托管应用程序）和 Citrix Virtual Apps 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。
- 单会话操作系统：配备单会话操作系统的虚拟机或物理机。用于交付 VDI 桌面（运行可以有选择地个性化的单会话操作系统的桌面）、VM 托管应用程序（来自单会话操作系统的应用程序）以及托管的物理桌面。一次仅允许一个用户连接到其中的一台计算机。
- **Remote PC Access**：支持远程用户从任何运行 Citrix Workspace 应用程序的设备访问其物理办公 PC。办公 PC 通过 Citrix Virtual Desktops 部署进行管理，同时要求在允许列表中指定用户设备。

有关详细信息，请参阅 Citrix Virtual Apps and Desktops 映像管理和创建计算机目录。

交付组

交付组指定哪些用户可以访问哪些计算机上的哪些应用程序、桌面或两者。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。可以按照用户所属的 Active Directory 组将其分配到您的交付组，因为 Active Directory 组和交付组是对要求相似的用户进行分组的方式。

每个交付组都可以包含多个目录中的计算机，每个目录可以向多个交付组提供计算机。但是，一台计算机一次只能属于一个交付组。

可以定义交付组中的用户可以访问的资源。例如，要向不同的用户提供不同的应用程序，可以在一个目录的主映像上安装所有应用程序，并在该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，可以配置每个交付组，以交付计算机上安装的不同应用程序子集。

有关详细信息，请参阅创建交付组。

应用程序组

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

有关详细信息，请参阅创建应用程序组。

更多信息

- Citrix Virtual Apps and Desktops 示意图
- 网络端口
- 数据库
- 支持的虚拟机管理程序和其他服务

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Active Directory

January 21, 2022

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

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

本产品支持：

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

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

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

在多林 **Active Directory** 林环境中部署

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 转发器或条件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。请参阅 Microsoft 文档，了解有关此向导的详细信息。

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。使用以下信息将注册表项添加到 VDA 和 Delivery Controller：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 小心：
>
> 注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

在 VDA 上，配置：HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest。

- 名称：SupportMultipleForest
- 类型：REG_DWORD
- 数据：0x00000001 (1)

在所有 Delivery Controller 上，配置：HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\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。

添加了一个注册表项，以避免在 VDA 中不必要地启用 NTLM 身份验证，该身份验证不如 Kerberos 安全。可以使用此注册表项来代替 SupportMultipleForest 注册表项，后者仍可用于向后兼容。

在 VDA 上，配置：HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent。

- 名称：SupportMultipleForestDdcLookup
- 类型：REG_DWORD
- 数据：0x00000001 (1)

此注册表项在允许您在初始注册过程中删除基于 NTLM 的身份验证的双向信任多林环境中执行 DDC 查找。

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 NetBIOS 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 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)。（SID 包含在 Get-BrokerController cmdlet 的结果中。）

如果具有现有外部信任，应对 VDA 做以下更改：

1. 找到文件 Program Files\Citrix\Virtual Desktop Agent\brokeragent.exe.config。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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"` 并将文本更改为 `allowNtlm="true"`。
5. 保存文件。

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

下表列出了支持的信任类型：

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

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

数据库

January 21, 2022

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

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

如果您的站点包含多个区域，请确保主区域始终包含站点数据库。各区域内的 Controller 与该数据库通信。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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（包括 **Basic** 可用性组）：这是 SQL Server 2012 中引入的具有高可用性和灾难恢复能力的企业级解决方案，此方案可以使您最大程度地提高一个或多个数据库的可用性。AlwaysOn 可用性组要求 SQL Server 实例必须驻留在 Windows Server 故障转移群集 (WSFC) 节点上。有关详细信息，请参阅使用 SQL Server 执行 Windows Server 故障转移群集操作。
- **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。与其他解决方案相比，此方法更加昂贵，因为需要在每个数据库服务器上安装完全权限 SQL Server 许可证。不能在镜像环境中使用 SQL Server Express Edition。
- **SQL** 群集化：可以使用 Microsoft 的 SQL 群集化技术，允许一台服务器自动接管另一台故障服务器的任务和职责。但是，该解决方案的设置更为复杂，自动故障转移过程通常比其他备选方案（如 SQL 镜像）更慢。
- 使用虚拟机管理程序的高可用性功能：通过此方法，可以将数据库作为虚拟机进行部署，并使用虚拟机管理程序的高可用性功能。此解决方案的成本比镜像方法要低，因为它使用的是现有虚拟机管理程序软件，您也可以使用 SQL Server Express 版本。但是，其自动故障转移过程比较慢，因为需要花时间为数据库启动新计算机，这样可能会导致为用户提供的服务中断。

本地主机缓存功能是对 SQL Server 高可用性最佳实践的补充。本地主机缓存功能使用户能够连接和重新连接到应用程序和桌面，即使站点数据库不可用时亦如此。有关详细信息，请参阅本地主机缓存。

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，这将允许用户继续访问其桌面和应用程序。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。仅当无法与所有 Controller 进行通信（极少出现）时才使用此功能。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。

在 SQL 群集或 SQL 镜像安装中，不支持在节点上安装控制器。

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。对于概念验证或试验部署，该默认操作通常足以解决问题。但是，SQL Server Express 不支持 Microsoft 高可用性功能。

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

如有需要，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。

对于大多数生产部署以及任何使用 Microsoft 高可用性功能的部署，我们建议您仅使用受支持的非 Express 版 SQL Server。在安装第一个 Controller 的服务器以外的计算机上安装 SQL Server。系统要求列出了受支持的 SQL Server 版本。数据库可以位于一台或多台计算机上。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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上指定数据库名称和地址（位置）。（请参阅数据库地址格式。）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。（请参阅设置数据所需的权限。）

创建站点后，您可以稍后更改配置日志记录和监视数据库的位置。请参阅更改数据库位置。

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。

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伙伴设置为镜像。

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

自动设置

如果您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，Studio 将自动创建数据库，然后为主体数据库和复制数据库应用初始化脚本。

脚本设置

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

1. 在站点创建向导的数据库页面中，选择生成脚本。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。此时站点创建向导将自动停止。稍后返回时，系统会提示您继续创建站点。

然后，数据库管理员创建数据库。每个数据库必须具有以下特征：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 请使用结尾为 `_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，请配置高可用性功能。
- 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。

数据库管理员在 SQLCMD 模式下使用 SQLCMD 命令行实用程序或 SQL Server Management Studio 来执行以下操作：

- 在高可用性 SQL Server 数据库实例上运行每个 `xxx_Replica.sql` 脚本（如果配置了高可用性）
- 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。

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

设置数据库所需的权限

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

操作	用途	服务器角色	数据库角色
创建数据库	创建合适的空数据库	`dbcreator`	
创建架构	创建所有服务特定的架构，并将第一个 Controller 添加到站点	`securityadmin`*	`db_owner`
添加 Controller	将 Controller（除第一个外）添加到站点	`securityadmin`*	`db_owner`
添加 Controller（镜像服务器）	将 Controller 登录信息添加到当前位于镜像数据库的镜像角色中的数据库服务器	`securityadmin`*	
删除 Controller	从站点中删除 Controller	**	`db_owner`
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，但实际上可以将 `securityadmin` 服务器角色视为等同于 `sysadmin` 服务器角色。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

** 从站点中删除 Controller（通过 Desktop Studio，或者使用 Studio 或 SDK 生成的脚本）时，Controller 到数据库服务器的登录信息不会被删除。这是为了避免可能删除同一计算机上除此 Citrix 产品以外的服务正在使用的登录。如果不再需要登录，则必须手动删除登录信息。此操作需要 securityadmin 服务器角色成员资格。

当使用 Studio 执行这些操作时，Studio 用户必须具有明确为相应服务器角色成员的数据库服务器帐户，或者能够提供相应帐户的凭据。

首选数据库权限脚本

在企业环境中，数据库设置包括必须由具有不同角色（权限）的不同团队处理的脚本：securityadmin 或 db_owner。

使用 PowerShell，您现在可以指定首选的数据库权限。（此功能在 Studio 中不可用，该功能仅支持包含所有任务的单个脚本。）

指定非默认值会导致创建单独的脚本。一个脚本包含需要 securityadmin 角色的任务。另一个脚本仅需要 db_owner 权限，并且可以由 Citrix 管理员运行，而无需与数据库管理员联系。

在 get-*DBSchema cmdlet 中，-DatabaseRights 选项具有以下有效值：

- SA：生成用于创建数据库和 Delivery Controller 登录的脚本。这些任务需要 securityadmin 权限。
- DBO：生成一个可在数据库中创建用户角色的脚本、添加登录名，然后创建数据库架构。这些任务需要 db_owner 权限。
- Mixed：（默认）所有任务都在一个脚本中，无论所需权限如何都是如此。

有关详细信息，请参阅 cmdlet 帮助。

数据库地址格式

可以使用以下格式之一指定数据库地址：

- ServerName
- ServerName\InstanceName
- ServerName,PortNumber

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

在创建站点后，您可以更改配置日志记录和监视数据库的位置。（您不能更改站点数据库的位置。）当您更改某个数据库的位置时：

- 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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 新数据库中的第一条日志指示数据库发生更改，但不会标识以前的数据库。

可以在启用强制日志记录功能时更改配置日志记录数据库的位置。

要更改数据库的位置，请执行以下操作：

1. 确保您希望数据库所在的服务器上已安装受支持版本的 Microsoft SQL Server。根据需要设置高可用性功能。
2. 在 Studio 导航窗格中选择配置。
3. 选择要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。如果该操作失败，系统将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。

更多信息

- 数据库大小调整工具。
- 使用 SQL Server 高可用性解决方案时，调整站点数据库大小和配置连接字符串。

交付方法

January 21, 2022

Citrix Virtual Apps and Desktops 提供了各种交付方法。一种交付方法可能无法满足您的所有要求。

简介

选择一种恰当的应用程序交付方法有助于提高可扩展性、改进管理和用户体验。

- 已安装的应用程序：该应用程序属于基础桌面映像的一部分。安装过程涉及复制到映像驱动器的 dll、exe 和其他文件以及注册表修改。有关详细信息，请参阅创建计算机目录。
- 流应用程序 **(Microsoft App-V)** –该应用程序跨网络按需配置并交付到桌面。应用程序文件和注册表设置放置在虚拟桌面上的容器中，与基础操作系统隔离并且相互隔离。此隔离有助于解决兼容性问题。有关详细信息，请参阅 App-V。
- 分层应用程序 **(Citrix App Layering)**：每个层都包含一个应用程序、代理或操作系统。通过集成一个操作系统层、一个平台层（VDA、Citrix Provisioning 代理）以及多个应用程序层，管理员可以轻松创建新的可部署

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

映像。分层简化了现行的维护过程，因为操作系统、代理和应用程序存在于单个层中。更新层时，包含该层的所有已部署的映像将随之更新。有关详细信息，请参阅 Citrix App Layering。

- 托管 **Windows** 应用程序：安装在多用户 Citrix Virtual Apps 主机上并且部署为应用程序（而非桌面）的应用程序。用户从 VDI 桌面或端点设备无缝访问托管 Windows 应用程序，隐藏了应用程序远程运行的事实。有关详细信息，请参阅创建交付组。
- 本地应用程序：部署在端点设备上的应用程序。应用程序界面在用户托管的 VDI 会话中显示，即使在端点上运行亦如此。有关详细信息，请参阅本地应用程序访问和 URL 重定向。
- **Remote PC Access**： Remote PC Access 使员工能够远程访问其物理办公室 PC。用户访问其办公室 PC 时，他们可以访问完成工作所需的所有应用程序、数据和资源。Remote PC Access 无需引入和提供其他工具来满足远程工作需求。有关详细信息，请参阅 Remote PC Access。

对于桌面，请考虑使用已发布的桌面或 VDI 桌面。

Citrix Virtual Apps 发布的应用程序和桌面

使用多会话操作系统计算机交付 Citrix Virtual Apps and Desktops 发布的应用程序和已发布的桌面。

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多个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。用户可以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。
- 托管应用程序集中管理，用户无法修改这些应用程序。这提供了一致、安全且可靠的用户体验。
- 用户必须联机才能访问其应用程序。

用户体验：

- 用户可以通过 StoreFront、其开始菜单或您提供的 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多会话操作系统计算机上。
- 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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 多会话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：

- 多会话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多个应用程序，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。

VM 托管应用程序

使用单会话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具有多个用户。您希望为这些用户提供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正常配合使用或可能与操作系统进行交互的应用程序，例如 Microsoft .NET Framework。这些类型的应用程序最适合在虚拟机上进行托管。

优势和注意事项：

- 可在数据中心内的计算机上安全管理、托管和运行主映像上的应用程序和桌面，从而提供一个更为经济的应用程序交付解决方案。
- 登录后，可以将用户随机分配给交付组内配置为托管相同应用程序的计算机。还可以静态分配单台计算机，以便在每次有单个用户登录时将应用程序交付给该用户。通过静态分配的计算机，用户可以在虚拟机上安装和管理自己的应用程序。
- 单会话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，同时增加用户的数据的存储量。

用户体验：

- 与在多会话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：

- 与多会话操作系统计算机相同，但它们是虚拟单会话操作系统计算机。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

会话管理和分配：

- 单会话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）。

VDI 桌面

使用单会话操作系统计算机交付 Citrix Virtual Apps and Desktops 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已发布的桌面，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。这允许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：

- 随机非永久桌面（又称为池 **VDI** 桌面）：每次用户登录其中一个桌面时，该用户都会连接到从桌面池中选择的桌面。该池基于单个主映像。计算机重新启动时，对桌面所做的更改将全部丢失。
- 静态非永久桌面：首次登录过程中，将从桌面池中为用户分配桌面。（池中的每台计算机都基于一个主映像。）首次使用后，用户每次登录以使用桌面时，该用户都将连接到首次使用时向其分配的同一个桌面。计算机重新启动时，对桌面所做的更改将全部丢失。
- 静态永久桌面：与其他类型的 VDI 桌面不同，用户可以完全对这些桌面进行个性化设置。首次登录过程中，将从桌面池中为用户分配桌面。该用户的后续登录会连接到首次使用时分配的相同桌面。计算机重新启动时，将保留对桌面所做的更改。

网络端口

January 21, 2022

完整的网络端口信息在 Citrix 技术使用的通信端口中提供。

默认情况下，安装 Citrix 组件时，还会更新操作系统的主机防火墙，以与默认网络端口相匹配。

您可能需要以下端口信息：

- 为了遵守法规。
- 如果 Citrix Virtual Apps and Desktops 组件与其他 Citrix 产品或组件之间存在网络防火墙，则可以相应地配置该防火墙。
- 如果使用第三方主机防火墙（例如，反恶意软件安装包附带的防火墙），而非操作系统的主机防火墙。
- 如果更改这些组件上的主机防火墙配置（通常为 Windows 防火墙服务）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 如果将组件功能重新配置为使用不同的端口或端口范围，然后希望禁用或阻止您的配置中未使用的端口。

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

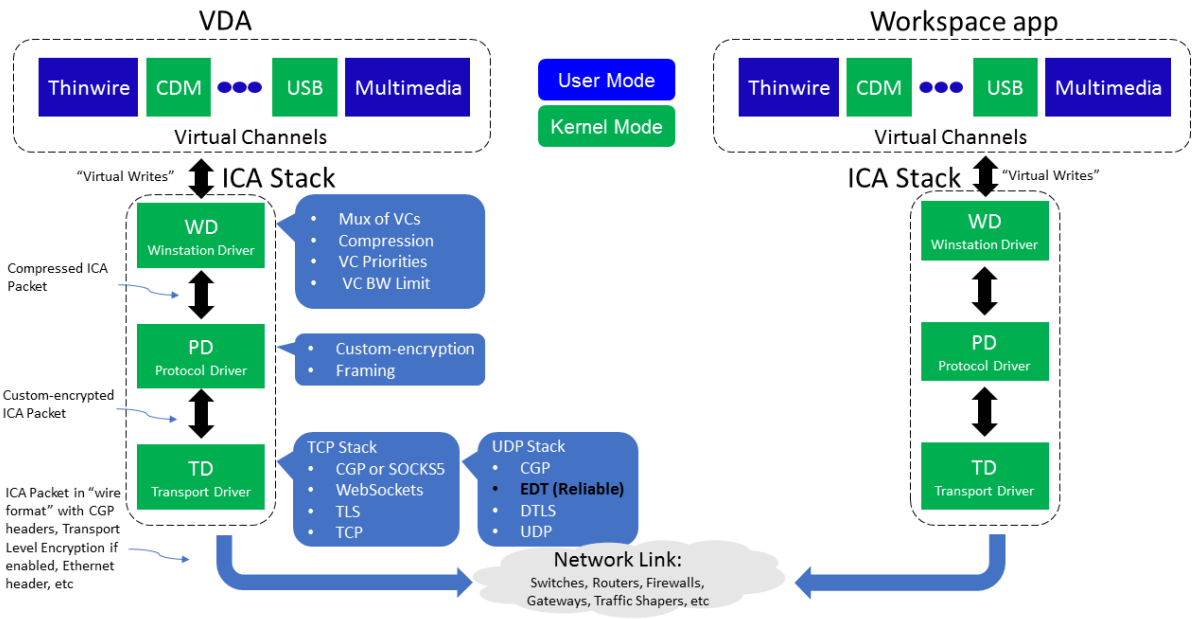
此外，VDA 和 Delivery Controller 上的操作系统需要供自己使用的传入端口。有关详细信息，请参阅 Microsoft Windows 文档。

HDX

July 5, 2024

> 警告：
>
> 注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

Citrix HDX 代表了一系列广泛的技术，可向任何设备上通过任何网络连接的集中式应用程序和桌面用户提供高清晰度的体验。



HDX 围绕三个技术原则设计：

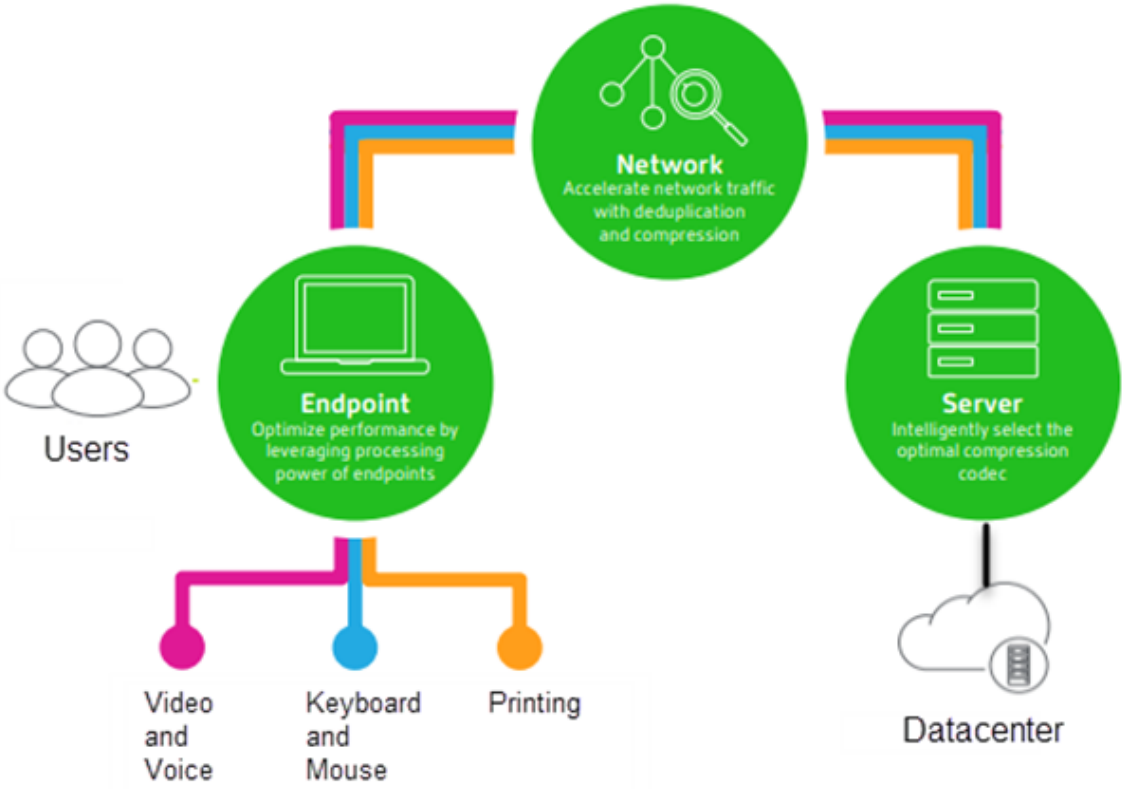
- 智能重定向
- 自适应压缩

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 重复数据删除

这些技术以不同的组合进行应用，优化了 IT 和用户体验，降低了带宽占用量，同时增加了每个托管服务器的用户密度。

- 智能重定向 - 智能重定向检查屏幕活动、应用程序命令、端点设备以及网络和服务器功能，以立即确定呈现应用程序或桌面活动的方式和位置。呈现可以在端点设备或托管服务器上发生。
- 自适应压缩 - 自适应压缩功能允许在瘦网络连接中提供丰富的多媒体显示。HDX 首先评估多个变量，例如，输入、设备和显示内容（文本、视频、语音和多媒体）的类型。HDX 将选择最佳压缩编解码器以及 CPU 和 GPU 使用率的最佳比例。然后根据每个唯一的用户和基础智能地适应环境。这种智能适应是按用户甚至按会话实现的。



- 重复数据删除 - 网络流量的重复数据删除功能减少了在客户端与服务器之间发送的汇总数据。此功能通过利用经常访问的数据（例如位图图形、文档、打印作业以及通过流技术推送的媒体）中的重复模式来实现。缓存这些模式仅允许所做的更改通过网络进行传送，消除了重复的流量。HDX 还支持多媒体流的多播，其中从来源进行的单个传输由多个订阅者在一个位置进行查看，而不是为每个用户建立一对一连接。

有关详细信息，请参阅大幅提高高清晰度用户工作区的生产力。

在设备上

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

工作。

在网络上

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

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

在数据中心中

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

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

HDX Insight

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

可以允许 NetScaler 使用 HDX Insight 虚拟通道移动所有未压缩格式的必需数据点。如果禁用此功能，NetScaler 设备将跨多个虚拟通道解密并解压缩 ICA 通信。使用单个虚拟通道降低了复杂性，增强了可扩展性，并且更具成本效益。

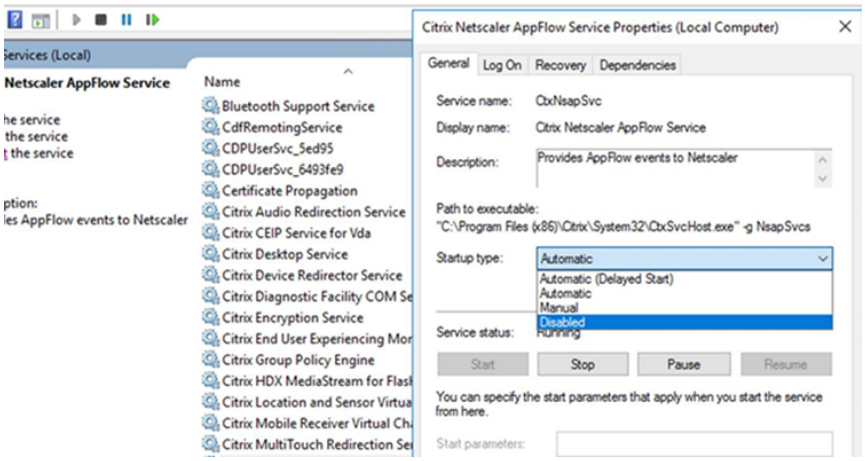
最低要求：

- Citrix Virtual Apps and Desktops 7 v1808
- XenApp 和 XenDesktop 7.17
- NetScaler 版本 12.0 Build 57.x
- 适用于 Windows 的 Citrix Workspace 应用程序 1808
- Citrix Receiver for Windows 4.10
- 适用于 Mac 的 Citrix Workspace 应用程序 1808
- Citrix Receiver for Mac 12.8

启用或禁用 **HDX Insight** 虚拟通道

要禁用此功能，请将 Citrix NetScaler Application Flow 服务属性设置为“已禁用”。要启用此功能，请将此服务设置为“自动”。在任一情况下，我们都建议您在更改这些属性后重新启动服务器计算机。默认情况下，此服务处于启用状态（自动）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



从虚拟桌面体验 **HDX** 功能

- 了解浏览器内容重定向（四个 HDX 多媒体重定向技术之一）如何加快 HTML5 和 WebRTC 多媒体内容的交付：
  1. 下载 Chrome 浏览器扩展程序并将其安装在虚拟桌面上。
  2. 要了解浏览器内容重定向功能是如何向虚拟桌面快速交付多媒体内容的，请在桌面上观看含有 HTML5 视频的 Web 站点（例如 YouTube）上的视频。用户不知道浏览器内容重定向何时运行。要查看是否正在使用浏览器内容重定向，请快速拖动浏览器窗口。您将看到视区与用户界面之间出现延迟或帧失调问题。还可以在 Web 页面上单击鼠标右键，并在菜单中查找关于 **HDX** 浏览器重定向。
- 了解 HDX 如何交付高清晰度音频：
  1. 将 Citrix 客户端配置为采用最高音频质量；请参阅 Citrix Workspace 应用程序文档了解详细信息。
  2. 在您的桌面上使用数字音频播放器（例如 iTunes）播放音乐文件。

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

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

须知：

- 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 多会话操作系统、Windows 单会话操作系统和 Remote PC Access 桌面。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 本内容介绍如何优化用户体验，提高服务器可扩展性或降低带宽要求。有关使用 Citrix 策略和策略设置的信息，请参阅适用于此版本的 Citrix 策略文档。
- 对于包括编辑注册表在内的说明，请注意：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。

客户端自动重新连接和会话可靠性

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

客户端自动重新连接：

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

- 桌面。会话窗口将灰显，并且倒计时器将显示进行重新连接之前的剩余时间。
- 应用程序。会话窗口将关闭并向用户显示一个对话框，其中包含一个显示尝试重新连接之前的剩余时间的倒计时器。

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

重新连接时，断开的会话将使用保存的连接信息重新连接。用户可以正常与应用程序和桌面交互。

默认客户端自动重新连接设置：

- 客户端自动重新连接超时：120 秒
- 客户端自动重新连接：已启用
- 客户端自动重新连接身份验证：已禁用
- 客户端自动重新连接日志记录：已禁用

有关详细信息，请参阅客户端自动重新连接策略设置。

会话可靠性：

会话可靠性将在网络中断时无缝重新连接 ICA 会话。会话可靠性将在设置中指定的时间之后关闭（或断开）用户会话。会话可靠性超时之后，客户端自动重新连接策略设置生效，尝试将用户重新连接到断开连接的会话。启用了会话可靠性时，将向用户发送应用程序和桌面网络中断通知，如下所示：

- 桌面。会话窗口将变为半透明，并且倒计时器将显示进行重新连接之前的剩余时间。
- 应用程序。窗口将变为半透明，并且通知区域中显示连接已中断弹出通知。

会话可靠性处于活动状态时，用户不能与 ICA 会话交互。但是，击键等用户操作在网络中断后会立即缓冲几秒钟时间，并在网络可用时重新传输。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

重新连接时，客户端和服务器将在交换协议的相同位置恢复。会话窗口不再半透明显示，并且将为应用程序显示恰当的通知区域弹出通知。

默认会话可靠性设置

- 会话可靠性超时：180 秒
- 重新连接用户界面不透明度级别：80%
- 会话可靠性连接：已启用
- 会话可靠性端口号：2598

有关详细信息，请参阅会话可靠性策略设置。

启用了客户端自动重新连接和会话可靠性的 **NetScaler**：

如果在服务器上启用了多流和多端口策略，并且满足以下任意或全部条件，客户端自动重新连接将不起作用：

- 会话可靠性在 NetScaler Gateway 上处于禁用状态。
- 故障转移发生在 NetScaler 设备上。
- NetScaler SD-WAN 与 NetScaler Gateway 结合使用。

HDX 自适应吞吐量

HDX 自适应吞吐量可通过调整输出区缓冲智能地调整 ICA 会话的高峰吞吐量。输出缓冲区的数量最初设置为较高的值。这一较高的值允许更快更高效地将数据传输到客户端，尤其是在高延迟网络中。提供更好的交互性、更快的文件传输、更流畅的视频播放、更高的帧速率和分辨率，以提高用户体验。

将持续测量会话交互性以确定 ICA 会话中的数据流是否会对交互性产生不利影响。如果出现这种情况，吞吐量将减少，以降低大量数据流对会话产生的影响并允许恢复交互性。

> 重要：
>
> 通过将此机制从客户端移到 VDA，HDX 自适应吞吐量可以改变输出缓冲区的设置方式，并且不需要任何手动配置。

此功能的要求如下：

- VDA 版本 1811 或更高版本
- 适用于 Windows 的 Workspace 应用程序 1811 或更高版本

提高发送给用户设备的图像质量

下面的视频显示策略设置将控制从虚拟桌面发送到用户设备的图像质量。

- 视觉质量。控制在用户设备上显示的图像的视觉质量：中、高、始终无损、设为无损（默认 = 中）。使用默认设置“中”的实际视频质量取决于可用带宽。
- 目标帧速率。指定每秒从虚拟桌面发送到用户设备的最大帧数（默认 = 30）。对于 CPU 速度较慢的设备，指定较低的值可以改善用户体验。支持的最高每秒帧速率是 60。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 显示内存限制。指定会话的最大视频缓冲区大小，以 KB 为单位（默认 = 65536 KB）。对于需要更高颜色深度和分辨率的连接，可增大该限值。可以计算所需的最大内存。

提高视频会议性能

多个常用视频会议应用程序已优化，可通过多媒体重定向从 Citrix Virtual Apps and Desktops 交付（例如，请参阅 HDX RealTime Optimization Pack）。对于未优化的应用程序，HDX 网络摄像机视频压缩可提高在会话中的视频会议过程中网络摄像机的带宽效率和延迟容忍度。此技术通过一个专用多媒体虚拟通道使用流技术推送网络摄像机通信。与常时等量 HDX Plug-n-Play USB 重定向支持相比，此技术占用的带宽较少，并且可以通过 WAN 连接正常工作。

Citrix Workspace 应用程序用户可以通过选择 Desktop Viewer 麦克风和网络摄像机设置不使用我的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，请通过使用 ICA 策略设置 > USB 设备策略设置下的策略设置禁用 USB 设备重定向。

HDX 网络摄像机视频压缩功能需要启用以下策略设置（默认情况下均已启用）。

- 客户端音频重定向
- 客户端麦克风重定向
- 多媒体会议
- Windows Media 重定向

如果网络摄像机支持硬件编码，默认情况下 HDX 视频压缩功能将采用硬件编码。硬件编码占用的带宽可能高于软件编码。要强制执行软件压缩，请向注册表项 HKCU\Software\Citrix\HdxRealTime 添加以下 DWORD 注册表项值：DeepCompress_ForceSWEncode=1。

网络流量优先级

对于使用支持服务质量的路由器的会话，可以跨多个连接为网络流量分配优先级。可使用四个 TCP 流和两个用户数据报协议 (UDP) 流在用户设备与服务器之间传输 ICA 通信：

- TCP 流 - 实时、交互、后台和批量
- UDP 流 - 语音和 Framehawk 显示远程处理

每个虚拟通道都有一个特定的优先级，并通过相应连接进行传输。可以根据连接所使用的 TCP 端口号分别设置这些通道。

对于安装在 Windows 10、Windows 8 和 Windows 7 计算机上的 Virtual Delivery Agent (VDA)，支持多通道流连接。请与贵公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。

仅当配置了多会话可靠性端口或 CGP 端口时，才支持服务质量。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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 ICA 的 NetScaler Gateway 上进行遍历时，才支持 TLS 连接。在内部企业网络上时，不支持采用 TLS 的多流连接。

要为多流连接设置服务质量，请向策略中添加以下 Citrix 策略设置（有关详细信息，请参阅多流连接策略设置）：

- 多端口策略 - 此设置为跨多个连接的 ICA 通信指定端口，并确定网络优先级。
  - 在“CGP default port priority”（CGP 默认端口优先级）列表中选择优先级。默认情况下，主端口 (2598) 拥有“高”优先级。
  - 根据需要在“CGP port1”（CGP 端口 1）、“CGP port2”（CGP 端口 2）和“CGP port3”（CGP 端口 3）中键入更多 CGP 端口，并标识每个端口的优先级。每个端口必须有唯一的优先级。

  将 VDA 上的防火墙显式地配置为允许其他 TCP 流量。
- 多流计算机设置 - 默认情况下禁用此设置。如果要在环境中使用具有“多流”支持功能的 Citrix NetScaler SD-WAN，则无需配置此设置。如果要使用第三方路由器或旧版 NetScaler SD-WAN 实现所需的服务质量，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。

显示或隐藏远程语言栏

语言栏显示应用程序会话中的首选输入语言。如果启用了此功能（默认设置），则可以在适用于 Windows 的 Citrix Workspace 应用程序中使用高级首选项 **>** 语言栏 UI 显示或隐藏语言栏。通过 VDA 端的注册表设置，可以禁用语言栏功能的客户端控制。如果禁用了此功能，客户端 UI 设置将不生效，并且每位用户的当前设置将决定语言栏的状态。有关详细信息，请参阅改善用户体验。

要从 VDA 禁用语言栏功能的客户端控制，请执行以下操作：

1. 在注册表编辑器中，导航到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI。
2. 创建值为 DWORD 的注册表项 SeamlessFlags，并将其设置为 0x40000。

Unicode 键盘映射

非 Windows Citrix Receiver 使用本地键盘布局 (Unicode)。如果用户更改本地键盘布局和服务器键盘布局（扫描代码），则它们可能不同步，且输出不正确。例如，用户 1 将本地键盘布局从英语更改为德语。然后用户 1 将服务器端键盘更改为德语。即使两个键盘布局都是德语，但它们可能不同步，从而导致字符输出不正确。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

启用或禁用 **Unicode** 键盘布局映射

默认情况下，在 VDA 端上禁用该功能。要启用该功能，请在 VDA 上使用注册表编辑器 regedit 来开启该功能。添加以下注册表项：

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名称：EnableKlMap

类型：DWORD

值：1

要禁用此功能，请将 **EnableKlMap** 设置为 0，或者删除 **CtxKlMap** 项。

启用 **Unicode** 键盘布局映射兼容模式

默认情况下，在服务器端更改键盘布局时，Unicode 键盘布局映射会自动挂接某个 Windows API 以重新加载新的 Unicode 键盘布局映射。一些应用程序无法挂接。为了保持兼容性，您可以将该功能更改为兼容模式以支持这些非挂接的应用程序。添加以下注册表项：

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名称：DisableWindowHook

类型：DWORD

值：1

要使用普通的 Unicode 键盘布局映射，请将 **DisableWindowHook** 设置为 0。

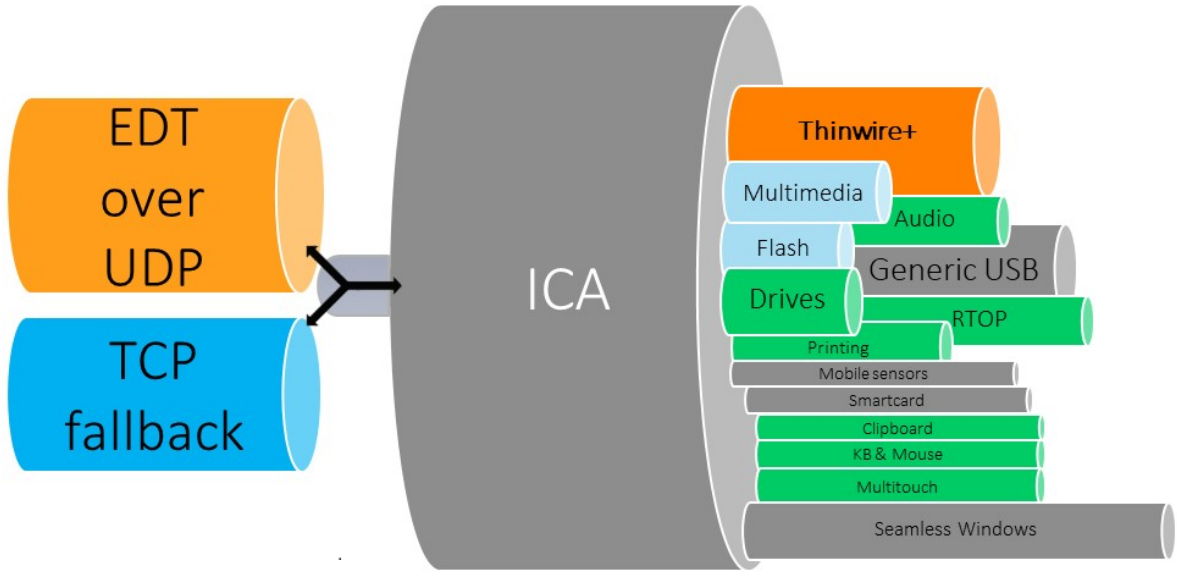
自适应传输

April 4, 2024

自适应传输是 Citrix Virtual Apps and Desktops 中的一种机制，它提供了使用 Enlightened Data Transport (EDT) 作为 ICA 连接的传输协议的功能。当 EDT 不可用时，自适应传输将切换到 TCP。

EDT 是基于用户数据报协议 (UDP) 构建的 Citrix 专有传输协议。它在保持服务器可扩展性的同时，在具有挑战性的长途连接方面提供了出色的用户体验。EDT 提高了不可靠网络中所有 ICA 虚拟通道的数据吞吐量，从而提供更出色、更一致的用户体验。

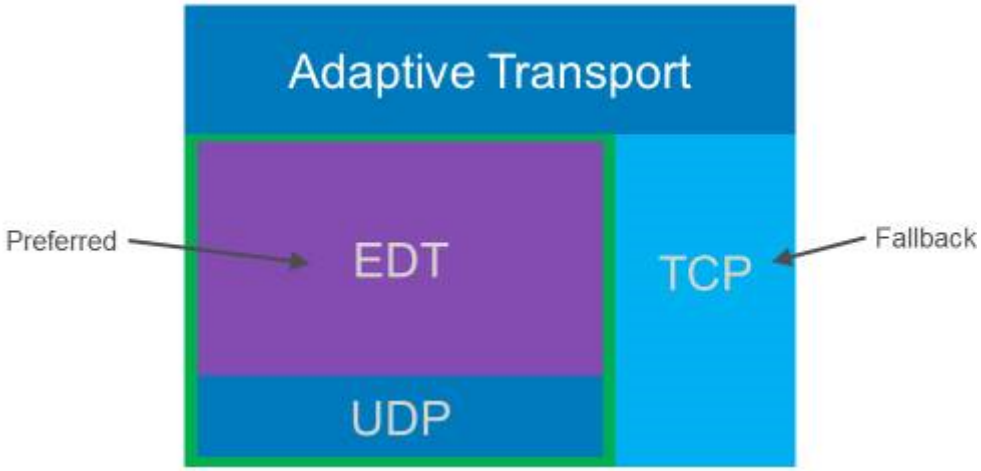
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



自适应传输设置为首选时，EDT 将用作主传输协议，TCP 将用于回退。默认情况下，自适应传输设置为首选。可以将自适应传输设置为诊断模式以进行测试，这仅允许使用 EDT 并禁用回退到 TCP。

使用适用于 Windows、Mac 和 iOS 的 Citrix Workspace 应用程序时，将在初始连接、会话可靠性重新连接和客户端自动重新连接期间并行尝试建立 EDT 和 TCP 连接。如果基础 UDP 传输不可用，必须改为使用 TCP，这样做可以缩短连接时间。如果自适应传输设置为首选，并且使用 TCP 建立连接，自适应传输将继续尝试每五分钟切换到 EDT 一次。

使用适用于 Linux 和 Android 的 Citrix Workspace 应用程序时，将首先尝试建立 EDT 连接。如果连接失败，Citrix Workspace 应用程序将尝试在 EDT 请求超时后使用 TCP 进行连接。



系统要求

下面是使用自适应传输和 EDT 的要求：

- 控制平面

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Citrix Virtual Apps and Desktops 服务
  - Citrix Virtual Apps and Desktops 1912 或更高版本
- Virtual Delivery Agent
  - 版本 1912 或更高版本（推荐 2103 或更高版本）
  - 版本 2012 是将 EDT 与 Citrix Gateway 服务结合使用所需的最低要求
- StoreFront
  - 版本 3.12.x
  - 版本 1912.0.x
- Citrix Workspace 应用程序
  - Windows：版本 1912 或更高版本（推荐 2105 或更高版本）
  - Linux：版本 1912 或更高版本（推荐 2104 或更高版本）
  - Mac：版本 1912 或更高版本（推荐 2108 或更高版本）
  - iOS：Apple App Store 中提供的最新版本
  - Android：Google Play 中提供的最新版本
- Citrix Gateway (ADC)
  - 13.0.52.24 或更高版本
  - 12.1.56.22 或更高版本
- 防火墙（从 VDA 的角度来看）
  - UDP 1494 入站 - 如果禁用了会话可靠性
  - UDP 2598 入站 - 如果启用了会话可靠性
  - UDP 443 入站 - 如果为 ICA 加密 (DTL) 启用了 VDA SSL
  - UDP 443 出站 - 如果使用 Citrix Gateway 服务。有关详细信息，请参阅 Citrix Gateway 服务文档。

注意事项

- 启用会话可靠性以使用 EDT MTU 发现并将 EDT 与 Citrix Gateway 和 Citrix Gateway 服务一起使用。
- 确保已充分设置 EDT MTU 以避免碎片化。否则，在某些情况下，性能可能会受到影响或者会话可能无法启动。有关详细信息，请参阅 EDT MTU 发现部分。
- 有关将 EDT 与 Citrix Gateway 服务结合使用的要求和注意事项的详细信息，请参阅 HDX 自适应传输与 Citrix Gateway 服务对 EDT 的支持。
- 有关支持 EDT 的 Citrix Gateway 配置的详细信息，请参阅配置 Citrix Gateway 以支持 Enlightened Data Transport 和 HDX Insight。
- 当前不支持 IPv6。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

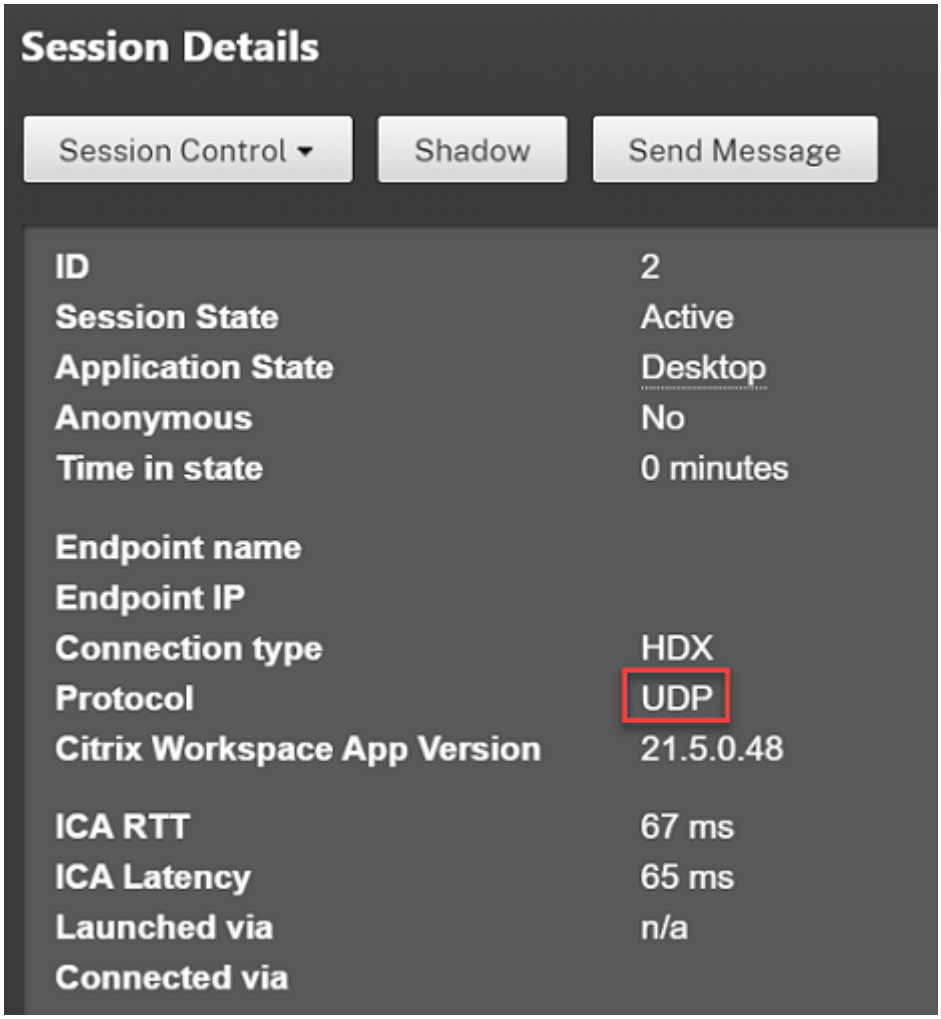
配置

默认情况下启用自适应传输。可以使用 Citrix 策略中的 **HDX** 自适应传输设置配置以下选项。

- 首选。此为默认设置。自适应传输已启用，它使用 EDT 作为首选传输协议，并回退到 TCP。
- 诊断模式。自适应传输已启用，并强制使用 EDT。已禁用回退到 TCP。仅建议对测试和故障排除使用此设置。
- 关。自适应传输已禁用，只有 TCP 用于传输。

要确认 EDT 是否正用作会话的传输协议，可以在 VDA 上使用 Director 或 CtxSession.exe 命令行实用程序。

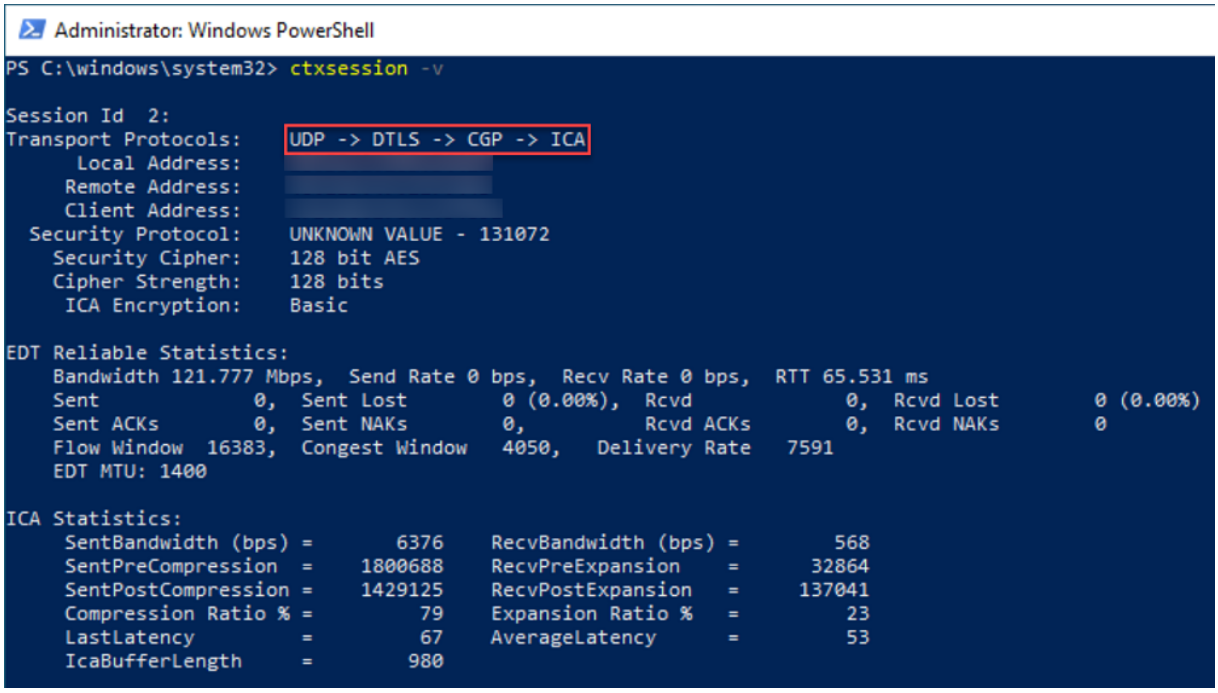
在 Director 中，查找会话并选择详细信息。如果连接类型为 **HDX**，协议为 **UDP**，则表示 EDT 正用作会话的传输协议。如果连接类型为 **RDP**，则表示 ICA 未在使用中，协议将显示“不适用”。有关详细信息，请参阅监视会话。



要使用 CtxSession.exe 实用程序，请在会话中启动命令提示符或 PowerShell 并运行 `ctxsession.exe`。要查看详细的统计信息，请运行 `ctxsession.exe -v`。如果 EDT 正在使用中，传输协议将显示以下内容之一：

- **UDP > ICA**（会话可靠性已禁用）
- **UDP > CGP > ICA**（会话可靠性已启用）
- **UDP > DTL > CGP > ICA**（ICA 是 DTL 加密的端到端）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



EDT MTU 发现

MTU 发现允许 EDT 在建立会话时自动确定最大传输单位 (MTU)。这样做可以防止出现可能会导致性能下降或无法建立会话的 EDT 数据包碎片。

系统要求

- VDA 最低版本 1912（推荐 2103 或更高版本）
- Citrix Workspace 应用程序
  - Windows：版本 1912 或更高版本（推荐 2105 或更高版本）
  - Mac：版本 2108 或更高版本
  - Android：版本 21.5 或更高版本
- Citrix ADC：
  - 13.0.52.24
  - 12.1.56.22
- 必须启用会话可靠性

如果您使用的是不支持此功能的客户端平台或版本，请参阅 CTX231821 以了解有关配置适合您的环境的自定义 EDT MTU 的详细信息。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 重要：
>
> 多流 ICA 不支持 MTU 发现。

控制 **VDA** 上的 **EDT MTU** 发现

默认情况下 MTU 发现处于启用状态。要禁用此功能，请删除 **EDT MTU** 发现注册表值并重新启动 VDA。有关详细信息，请参阅通过注册表管理的 HDX 功能列表中的 EDT MTU 发现设置。

> 警告：
>
> 注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

控制客户端上的 **EDT MTU** 发现

可以通过在 ICA 文件中添加 **MtuDiscovery** 参数，在客户端上有选择地控制 EDT MTU 发现。要禁用此功能，请在应用程序部分下设置以下策略：

```
MtuDiscovery=Off
```

要重新启用此功能，请从 ICA 文件中删除 **MtuDiscovery** 参数。

> 重要：
>
> 要使此 ICA 文件参数正常起作用，请在 VDA 上启用该功能。如果在 VDA 上未启用该功能，ICA 文件参数将不起作用。

丢失容忍模式

> 重要：
>
> - 此功能需要至少使用适用于 Windows 的 Citrix Workspace 应用程序 2002。
> - Citrix Gateway 或 Citrix Gateway Service 不支持丢失容忍模式。此模式仅适用于直接连接。

丢失容忍模式使用 EDT 有损传输协议增强用户通过具有高延迟且会丢失数据包的网络连接的用户体验。

最初，会话是使用 EDT 建立的。如果达到或超过延迟和数据包丢失阈值，适用的虚拟通道将从 EDT 切换到 EDT 有损，同时将其他虚拟通道保留在 EDT 上。如果延迟和数据包丢失降低到阈值以下，适用的虚拟通道将切换回 EDT。

默认阈值为：

- 数据包丢失：5%
- 延迟：300 毫秒（RTT）

默认情况下启用丢失容忍模式。可以使用丢失容忍模式阈值设置禁用该模式或调整数据包丢失和延迟阈值。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

系统要求

- Citrix Virtual Delivery Agent (VDA) 2003
- 适用于 Windows 的 Citrix Workspace 应用程序 2002
- 已启用会话可靠性。有关会话可靠性的详细信息，请参阅会话可靠性策略设置。

已知问题

自适应传输和 EDT 包含以下问题：

- 数据包碎片可能会导致性能下降甚至无法启动会话。可以调整 EDT MTU 以避免出现这种情况。使用 MTU 发现或 CTX231821 中介绍的解决方法。
- 如果启用了 MTU 发现，则从 Windows 客户端启动会话时，可能会出现灰屏或黑屏。要解决此问题，请升级到适用于 Windows 的 Workspace 应用程序 2105 或更高版本或适用于 Windows 的 Workspace 应用程序 1912 CU4 或更高版本。
- 通过 Citrix Gateway 或 Citrix Gateway 服务进行连接时，在 Linux 和 Android 客户端上回退到 TCP 可能会失败。客户端与网关之间成功进行 EDT 协商，并且网关与 VDA 之间的 EDT 协商失败时会发生这种情况。要解决此问题，请升级到适用于 Linux 的 Workspace 应用程序 2104 或更高版本以及适用于 Android 的 Workspace 应用程序 21.5 或更高版本。
- 对于未通过 Citrix Gateway 或 Citrix Gateway 服务的连接，非对称网络路径可能会导致 MTU 发现失败。要解决此问题，请升级到 VDA 版本 2103 或更高版本。[CVADHELP-16654]
- 使用 Citrix Gateway 或 Citrix Gateway 服务时，非对称网络路径可能会导致 MTU 发现失败。这是由于网关上的一个问题导致 EDT 数据包标头中的 “不碎片” (DF) 位无法传播。此问题的修复程序尚不可用。[CGOP-18438]
- 对于通过 DS-Lite 网络连接的用户，MTU 发现可能会失败。当数据包处理已启用时，某些调制解调器无法遵守 DF 位，从而阻止 MTU 发现检测到碎片。在这种情况下，可以使用以下选项：
  - 在用户的调制解调器上禁用数据包处理。
  - 禁用 MTU 发现并使用硬编码的 MTU，如 CTX231821 中所述。
  - 禁用自适应传输以强制会话使用 TCP。如果只有一部分用户受到影响，请考虑在客户端将其禁用，以便其他用户可以继续使用 EDT。

故障排除

为了对自适应传输和 EDT 进行故障排除，我们建议执行以下操作：

1. 彻底检查和验证要求、注意事项和已知问题。
2. 检查 Studio 或 GPO 中是否存在覆盖所需的 **HDX** 自适应传输设置的 Citrix 策略。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. 检查客户端上是否存在覆盖所需的 HDX 自适应传输设置的设置。这可以是 GPO 首选项、使用可选 Workspace 应用程序管理模板配置的设置，或者在注册表或客户端的配置文件中手动配置的 **HDXoverUDP** 设置。
4. 在多会话 VDA 计算机上，确保 UDP 侦听器处于活动状态。在 VDA 计算机中打开命令提示符并运行 `netstat -a -p udp`。有关详细信息，请参阅 How to Confirm HDX Enlightened Data Transport Protocol（如何确认 HDX Enlightened Data Transport 协议）。
5. 绕过 Citrix Gateway 在内部启动直接会话，然后检查正在使用的协议。如果会话使用 EDT，VDA 就可以通过 Citrix Gateway 使用 EDT 进行外部连接。
6. 如果 EDT 适用于直接内部连接而不适用于通过 Citrix Gateway 进行的会话：
   - 确保启用了会话可靠性
   - 确保网关启用了 DTL
7. 检查是否在网络防火墙和 VDA 计算机上运行的防火墙中配置了适当的防火墙规则。
8. 检查用户的连接是否需要非标准 MTU。有效 MTU 低于 1500 字节的连接会导致 EDT 数据包碎片，这反过来可能会影响性能，甚至导致会话启动失败。在使用 VPN、一些 Wi-Fi 接入点和移动网络（例如 4G 和 5G）时，此问题很常见。有关如何解决此问题的信息，请参阅 MTU 发现部分。

与 **Citrix SD-WAN** 的互操作性

Citrix SD-WAN WAN 优化 (WANOP) 提供跨会话的标记化压缩（重复数据删除功能），包括基于 URL 的视频缓存，从而显著降低带宽。如果两个人或多个人在办公室观看同一个客户端提取的视频，或者传输或打印同一个文件或文档的重要部分，则会出现降低情况。此外，通过在分支机构的设备上运行面向 ICA 数据缩减和打印作业压缩的进程，WANOP 将提供 VDA 服务器 CPU 卸载并启用更高的 Citrix Virtual Apps and Desktops 服务器可扩展性。

当前，SD-WAN WANOP 不支持 EDT。但是，如果 SD-WAN WANOP 正在使用中，则无需禁用自适应传输。当用户启动一个在启用了 WANOP 的情况下通过 SD-WAN 进行的会话时，它会自动将该会话设置为使用 TCP 作为传输协议。非 WANOP 会话将尽可能继续使用 EDT。

Citrix ICA 虚拟通道

January 21, 2022

> 警告：
>
> 注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

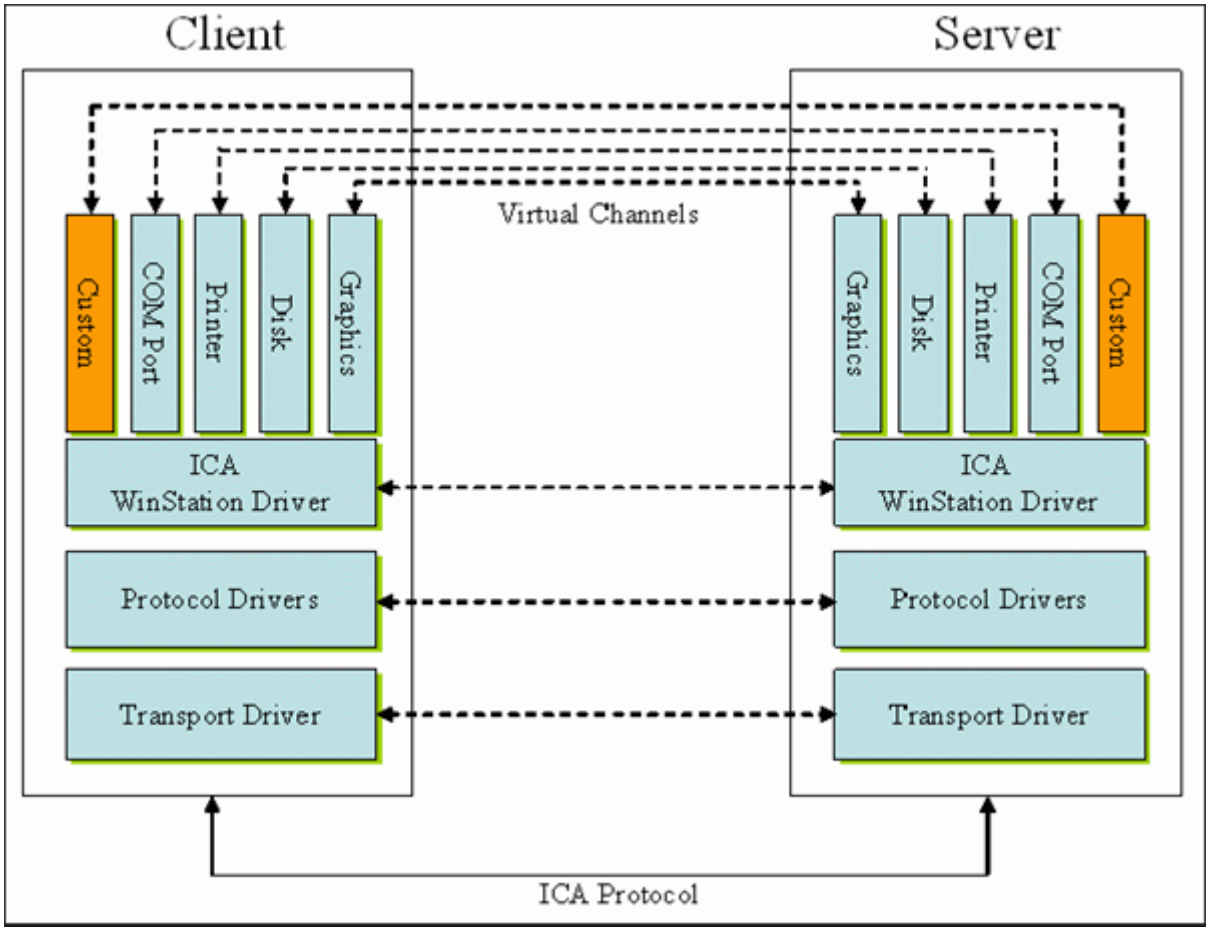
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ICA 虚拟频道是什么

Citrix Workspace 应用程序与 Citrix Virtual Apps and Desktops 服务器之间的大部分功能和通信通过虚拟通道进行。虚拟通道是使用 Citrix Virtual Apps and Desktops 服务器进行远程计算体验的必要组成部分。虚拟通道用于：

- 音频
- COM 端口
- 磁盘
- 图形
- LPT 端口
- 打印机
- 智能卡
- 第三方自定义虚拟通道
- 视频

新虚拟通道有时会随新版本的 Citrix Virtual Apps and Desktops 服务器以及 Citrix Workspace 应用程序产品一起发布，以提供更多功能。



虚拟通道由与服务器端应用程序进行通信的客户端虚拟驱动程序组成。Citrix Virtual Apps and Desktops 随附各种虚拟通道。这些虚拟通道旨在允许客户和第三方供应商通过使用提供的软件开发工具包 (SDK) 之一创建自己的虚拟通

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

道。

虚拟通道提供了一种安全的方式来完成各种任务。例如，正在与客户端设备通信的 Citrix Virtual Apps 服务器上运行的应用程序或与客户端环境通信的应用程序。

在客户端，虚拟通道与虚拟驱动程序相对应。每个虚拟驱动程序都提供一项特定的功能。有些功能是正常操作所必需的，有些功能是可选的。虚拟驱动程序在表示层协议级别运行。通过 Windows 工作站 (WinStation) 协议层提供的多路复用通道可以有多个协议处于活动状态。

以下功能包含在此注册表路径下的 VirtualDriver 注册表值中：

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0`

或

`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0`（适用于 64 位）

- Thinwire3.0（必需）
- ClientDrive
- ClentPrinterQueue
- ClentPrinterPort
- 剪贴板
- ClientComm
- ClientAudio
- LicenseHandler（必需）
- TWI（必需）
- 智能卡
- ICACTL（必需）
- SSPI
- TwainRdr
- UserEXperience
- Vd3d

> 注意：
>
> 可以通过从注册表项中删除其中一个或多个值来禁用特定的客户端功能。例如，如果要删除客户端剪贴板，请删除单词剪贴板。

此列表包含客户端虚拟驱动程序文件及其各自的功能。Citrix Virtual Apps 以及适用于 Windows 的 Citrix Workspace 应用程序使用这些文件。它们采用动态链路库（用户模式）形式，而非 Windows 驱动程序（内核模式）形式，但通用 USB 虚拟通道中描述的通用 USB 除外。

- vd3dn.dll –用于桌面组合重定向的 Direct3D 虚拟通道
- vdcamN.dll –双向音频

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- vdcdm30n.dll –客户端驱动器映射
- vdcom30N.dll - 客户端 COM 端口映射
- vdcpm30N.dll –客户端打印机映射
- vdctln.dll –ICA 控制通道
- vddvc0n.dll –动态虚拟通道
- vdeuemn.dll - 最终用户体验监视
- vdgusbn.dll –通用 USB 虚拟通道
- vdkbhook.dll –透明键直通
- vdlfpn.dll –通过 UDP（例如传输）的 Framehawk 显示通道
- vdmmn.dll –多媒体支持
- vdmrvc.dll –移动 Receiver 虚拟通道
- vdmtchn.dll - 多点触控支持
- vdscardn.dll –智能卡支持
- vdsens.dll –传感器虚拟通道
- vdspl30n.dll –客户端 UPD
- vdsspin.dll –Kerberos
- vdtuin.dll –透明用户界面
- vdtw30n.dll –客户端 Thinwire
- vdtwin.dll –无缝
- vdtwn.dll –Twain

某些虚拟通道被编译成其他文件。例如，剪贴板映射在 wfica32.exe 中可用

64 位兼容性

适用于 Windows 的 Citrix Workspace 应用程序是 64 位兼容的。与大多数编译为 32 位的二进制文件一样，这些客户端文件具有 64 位编译等效文件：

- brapi64.dll
- confmgr.dll
- ctxlogging.dll
- ctxmui.dll
- icaconf.exe
- icaconfs.dll
- icafile.dll
- pnipcn64.dll
- pnsson.dll
- ssoncom.exe
- ssonstub.dll
- vdkbhook64.dll

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

通用 **USB** 虚拟通道

通用 USB 虚拟通道实现使用两内核模式驱动程序和虚拟通道驱动程序 vdgusbn.dll：

- ctxusbm.sys
- ctxusbr.sys

ICA 虚拟通道的工作原理

虚拟通道以多种方式加载。Shell（适用于服务器的 WfShell 和适用于工作站的 PicaShell）会加载一些虚拟通道。某些虚拟通道作为 Windows 服务托管。

Shell 加载的虚拟通道模块，例如：

- EUEM
- Twain
- 剪贴板
- 多媒体
- 无缝会话共享
- 时区

某些通道作为内核模式加载，例如：

- CtxDvcs.sys –动态虚拟通道
- Icausbb.sys –通用 USB 重定向
- Picadm.sys –客户端驱动器映射
- Picaser.sys –COM 端口重定向
- Picapar.sys –LPT 端口重定向

位于服务器端的图形虚拟通道

自 XenApp 7.0 和 XenDesktop7.0 起，`ctxgfx.exe` 将为基于工作站和端点服务器的会话托管图形虚拟通道。`Ctxgfx` 托管与相应驱动程序（`Icardd.dll`，适用于 RDSH，`vdod.dll` 和 `vidd.dll`，适用于工作站）交互的平台特定模块。

对于 XenDesktop 3D Pro 部署，将为 VDA 上的相应 GPU 安装 OEM 图形驱动程序。`Ctxgfx` 加载专用适配器模块以与 OEM 图形驱动程序进行交互。

在 **Windows** 服务中托管专业通道

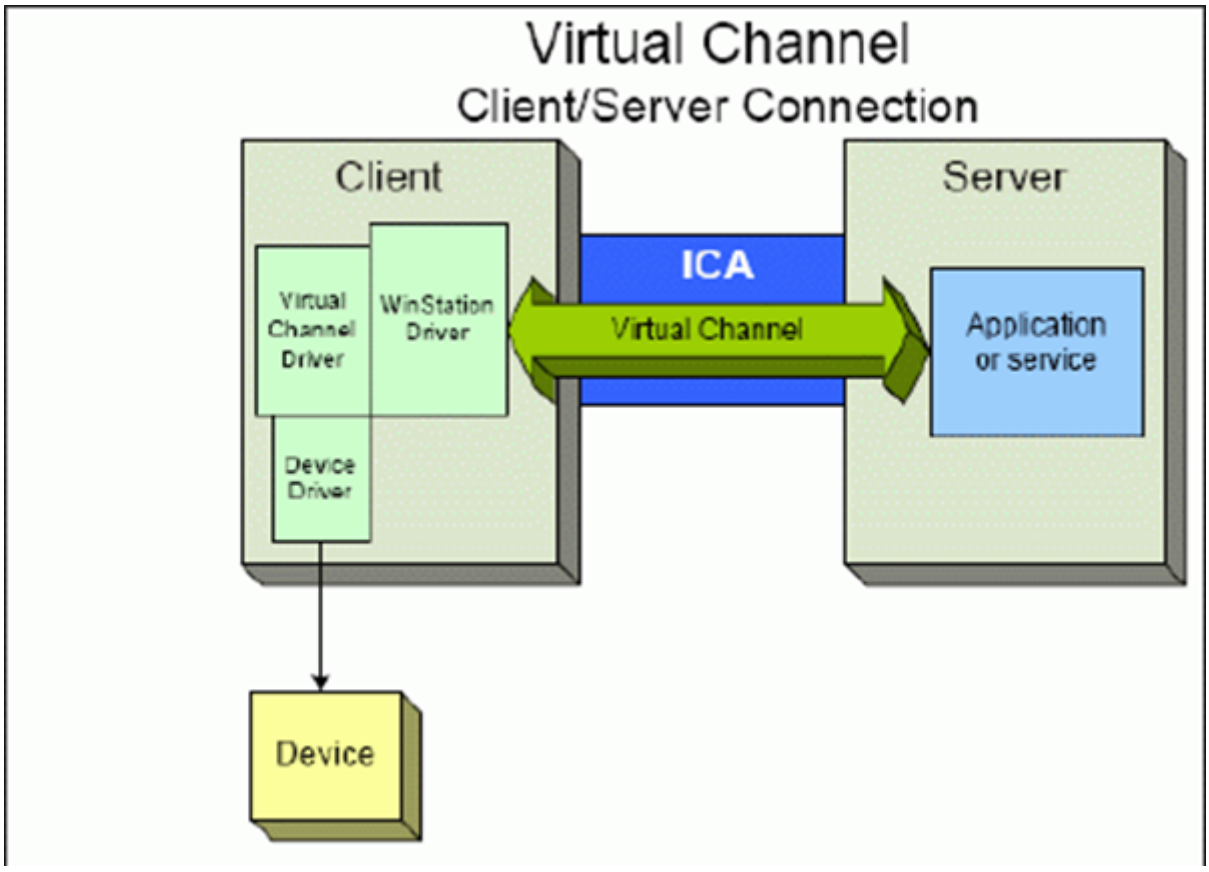
在 Citrix Virtual Apps and Desktops 服务器上，各种通道都将作为 Windows 服务进行托管。此类托管为会话中的多个应用程序和服务器上的多个会话提供一对多语义。此类服务的示例包括：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Citrix Device Redirector Service
- Citrix Dynamic Virtual Channel Service
- Citrix End User Experience Monitoring Service
- Citrix Location and Sensor Virtual Channel Service
- Citrix MultiTouch 重定向服务
- Citrix Print Manager Service
- Citrix Smartcard Service
- Citrix 音频重定向服务（仅限 Citrix Virtual Desktops）

Citrix Virtual Apps 上的音频虚拟通道是使用 Windows 音频服务托管的。

在服务器端，所有客户端虚拟通道都通过 WinStation 驱动程序 Wdica.sys 路由。在客户端，内置于 wfica32.exe 中的相应 WinStation 驱动程序轮询客户端虚拟通道。此示意图说明了虚拟通道客户端与服务器之间的连接。



此概述包含使用虚拟通道的客户端与服务器之间的数据交换。

1. 客户端连接到 Citrix Virtual Apps and Desktops 服务器。客户端将与其支持的虚拟通道的信息传递给服务器。
2. 服务器端应用程序启动，获取虚拟通道的句柄，并有选择地查询与通道有关的其他信息。
3. 客户端虚拟驱动程序和服务器端应用程序使用以下两种方法传递数据：
    - 如果服务器应用程序有要发送到客户端的数据，数据将立即发送到客户端。客户端接收到数据时，WinStation 驱动程序将从 ICA 流中对虚拟通道数据解多路复用，并立即将其传递给客户端虚拟驱动程序。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 如果客户端虚拟驱动程序有要发送到服务器的数据，则在下次 WinStation 驱动程序轮询时将发送数据。服务器接收到数据时，则会排队，直至虚拟通道应用程序读取数据。无法提醒服务器虚拟通道应用程序已收到数据。

4. 当服务器虚拟通道应用程序完成后，将关闭虚拟通道并释放所有分配的资源。

使用虚拟通道 SDK 创建您自己的虚拟通道

> 注意：
>
> Citrix SDK 在 Citrix Developer 门户网站 https://developer.cloud.com 中提供。

使用虚拟通道 SDK 创建虚拟通道需要中间编程知识。使用此方法可提供客户端与服务器之间的主要通信路径。例如，如果要在客户端实现设备（例如扫描仪）的使用，以便与会话中的进程一起使用。

> 注意：
>
> - 虚拟通道 SDK 需要 WFAPI SDK 才能编写虚拟通道的服务器端。
> - 由于 Citrix Virtual Apps and Desktops 的安全性增强，必须指定允许在 ICA 会话中打开哪些虚拟通道。有关详细信息，请参阅虚拟通道允许列表策略设置。

使用 ICA 客户端对象 SDK 创建您自己的虚拟通道

与使用虚拟通道 SDK 相比，使用 ICA 客户端对象 (ICO) 创建虚拟通道更加容易。通过使用 **CreateChannels** 方法在程序中创建一个命名对象来使用 ICO。

> 重要：
>
> 由于自 Citrix Receiver for Windows 10.00 及更高版本（以及适用于 Windows 的 Citrix Workspace 应用程序）起提高了安全性，因此在创建 ICO 虚拟通道时必须执行额外的步骤。

虚拟通道的直通功能

当您在 ICA 会话中使用适用于 Windows 的 Citrix Workspace 应用程序（又称为直通会话）时，Citrix 提供的大多数虚拟通道均以未修改的方式运行。在附加跃点中使用客户端时有一些注意事项。

以下功能在单跃点或多跃点中以相同的方式运行：

- 客户端 COM 端口映射
- 客户端驱动器映射
- 客户端打印机映射
- 客户端 UPD
- 最终用户体验监视

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 通用 USB
- Kerberos
- 多媒体支持
- 智能卡支持
- 透明键直通
- Twain

由于固有的延迟特性以及在每个跃点上执行的压缩、解压缩和渲染等因素，性能可能会受客户端经历的每个附加跃点影响。受影响区域如下：

- 双向音频
- 文件传输
- 通用 USB 重定向
- 无缝
- Thinwire

> 重要：
>
> 默认情况下，由在直通会话中运行的客户端的实例映射的客户端驱动器仅限于连接客户端的客户端驱动器。

Citrix Virtual Desktops 会话与 **Citrix Virtual Apps** 会话之间的虚拟通道的直通功能

当您在 Citrix Virtual Desktops 服务器上的 ICA 会话中使用适用于 Windows 的 Citrix Workspace 应用程序（又称为直通会话）时，Citrix 提供的大多数虚拟通道均以未修改的方式运行。

具体来说，在 Citrix Virtual Desktops 服务器上，有一个运行 **picaPassthruHook** 的 VDA 挂钩。此挂钩使客户端认为自己在 CPS 服务器上运行，并将客户端置于其传统的直通模式。

我们支持以下传统虚拟通道及其功能：

- 客户端
- 客户端 COM 端口映射
- 客户端驱动器映射
- 客户端打印机映射
- 通用 USB（因性能而受到限制）
- 多媒体支持
- 智能卡支持
- SSON
- 透明键直通

安全和 **ICA** 虚拟通道

确保使用安全是规划、开发和实现虚拟通道的重要组成部分。本文档中多次提及特定的安全区域。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

最佳做法

连接和重新连接时打开虚拟通道。注销并断开连接时关闭虚拟通道。

创建使用虚拟通道功能的脚本时，请紧急以下准则。

命名虚拟通道：

最多可以创建 32 个虚拟通道。32 个通道中的 17 个被预留用于特殊目的。

- 虚拟通道名称的长度不得超过 7 个字符。
- 前三个字符为供应商名称预留，后四个字符为通道类型。例如，**CTXAUD** 表示 Citrix 音频虚拟通道。

虚拟通道由七字符（或更短）ASCII 名称引用。在 ICA 协议的一些早期版本中，虚拟通道被编号。这些数字现在根据 ASCII 名称动态分配，使实现更加容易。开发仅供内部使用的虚拟通道代码的用户可以使用任何与现有虚拟通道不冲突的七字符名称。仅使用数字和大小写 ASCII 字符。添加自己的虚拟通道时，请遵循现有的命名约定。有多个预定义的通道。预定义的通道以 OEM 标识符 CTX 开头，仅供 Citrix 使用。

双跃点支持：

虚拟通道	是否支持双跃点?
音频	否
浏览器内容重定向	否
CDM	是
CEIP	否
剪贴板	是
Continuum (MRVC)	否
Control VC	是
HTML5 视频重定向 (v1)	是
键盘、鼠标	是
多点触控	否
NSAPVC	否
打印	是
SensVC	否
智能卡	是
Twain	是
USB VC	是

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

虚拟通道	是否支持双跃点?
使用 USB VC 的 WAYCOM 设备 -K2M	是
网络摄像机视频压缩	是
Windows Media 重定向	是

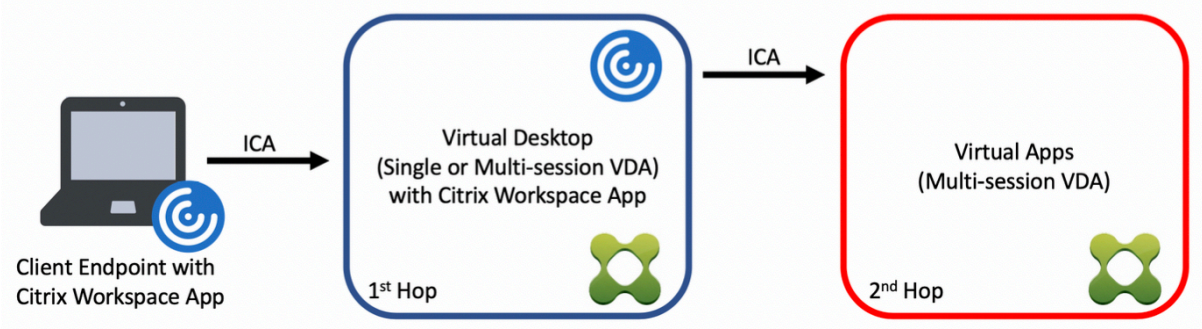
另请参阅

- ICA 虚拟通道 SDK
- Citrix Developer Network 是涉及使用 Citrix SDK 的所有技术资源和论坛的主页。在此网络中，您可以找到 SDK、示例代码和脚本、扩展程序和插件以及 SDK 文档的访问权限。此外，还包括 Citrix Developer Network 论坛，在该论坛中将围绕每个 Citrix SDK 进行技术讨论。

Citrix Virtual Apps and Desktops 中的双跃点

January 21, 2022

在 Citrix 客户端会话的上下文中，术语“双跃点”是指在 Citrix Virtual Desktops 会话中运行的 Citrix Virtual Apps 会话。下图说明了双跃点。



在双跃点场景中，当用户连接到在单会话操作系统 VDA（称为 VDI）或多会话操作系统 VDA（称为已发布的桌面）上运行的 Citrix Virtual Desktops 时，该虚拟桌面被视为第一个跃点。用户连接到虚拟桌面后，可以启动 Citrix Virtual Apps 会话。这被视为第二个跃点。

可以使用双跃点部署模型来支持各种用例。Citrix Virtual Desktops 和 Citrix Virtual Apps 环境由不同实体管理的情况就是一个常见的示例。此方法也可以有效地解决应用程序兼容性问题。

系统要求

所有 Citrix Virtual Apps and Desktops 版本（包括 Citrix Cloud 服务）都支持双跃点。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

第一个跃点必须使用单会话或多会话操作系统 VDA 和 Citrix Workspace 应用程序的受支持的版本。第二个跃点必须使用多会话操作系统 VDA 的受支持的版本。有关支持的版本，请参阅产品列表页面。

为了获得最佳性能和兼容性，Citrix 建议使用与正在使用的 VDA 版本相同或更新的 Citrix 客户端。

在第一个跃点涉及第三方（非 Citrix）虚拟桌面解决方案与 Citrix Virtual Apps 会话结合使用的环境中，支持仅限于 Citrix Virtual Apps 环境。如果出现任何与第三方虚拟桌面相关的问题，包括但不限于 Citrix Workspace 应用程序兼容性、硬件设备重定向和会话性能，Citrix 可以在有限的容量内提供技术支持。作为故障排除的一部分，可能需要位于第一个跃点的 Citrix Virtual Desktops。

双跃点中的 **HDX** 的部署注意事项

通常情况下，双跃点中的每个会话都是唯一的，客户端-服务器功能被隔离到给定的跃点。本部分内容包括需要 Citrix 管理员特别考虑的区域。Citrix 建议客户对所需的 HDX 功能进行彻底测试，以确保用户体验和性能适合给定的环境配置。

图形

在第一个跃点和第二个跃点上使用默认图形设置（选择性编码）。使用 HDX 3D Pro 时，Citrix 强烈建议所有需要图形加速的应用程序在第一个跃点中在本地运行，并使用 VDA 可用的相应 GPU 资源。

延迟

端到端延迟会影响整体用户体验。请注意第一个跃点与第二个跃点之间的额外延迟。这对于硬件设备的重定向尤其重要。

多媒体

服务器端（会话中）音频和视频内容的呈现在第一个跃点中表现最佳。第二个跃点中的视频播放需要在第一个跃点处进行解码和重新编码，从而提高带宽和硬件资源利用率。音频和视频内容必须尽可能限制到第一个跃点。

USB 设备重定向

HDX 包括通用和优化的重定向模式，可支持各种 USB 设备类型。请特别注意每个跃点处使用的模式，并使用下表作为参考，以获得最佳结果。有关通用和优化的重定向模式的详细信息，请参阅通用 USB 设备。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

第一个跃点（VDI 或已发布的桌面）	第二个跃点（虚拟应用程序）	支持说明
已优化	已优化	推荐（基于设备的支持）。例如，USB 大容量存储、TWAIN 扫描仪、网络摄像机、音频。
通用	通用	适用于优化选项不可用的设备。
通用	已优化	虽然在技术上可行，但仍建议您在设备支持可用时跨两个跃点使用优化的模式。
已优化	通用	不支持

> 注意：
>
> 由于 USB 协议固有的干扰，跨跃点的性能可能会下降。功能和结果因特定设备和应用程序要求而异。强烈建议在设备重定向的所有情况下进行验证测试，该测试在双跃点场景中尤其重要。

支持例外

双跃点会话支持大多数 HDX 功能和功能，但以下功能除外：

- 浏览器内容重定向
- 本地应用程序访问
- 适用于 Skype for Business 的 RealTime Optimization Pack
- Microsoft Teams 的优化

安装和配置

December 2, 2022

请在开始执行每个部署步骤之前查看参考文章，以了解部署过程中显示和指定的内容。

请按照下面的顺序部署 Citrix Virtual Apps and Desktops。

准备

查看准备安装，并完成所有必要的任务。

- 与概念、功能、与早期版本之间的差异、系统要求及数据库有关的信息的查找位置。
- 决定要在哪里安装核心组件时的考虑事项。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 权限和 Active Directory 要求。
- 有关可用安装程序、工具和接口的信息。

安装核心组件

安装 Delivery Controller、Citrix Studio、Citrix Director 和 Citrix 许可证服务器。还可以安装 Citrix StoreFront。有关详细信息，请参阅安装核心组件或使用命令行安装。

创建站点

安装核心组件并启动 Studio 后，系统会自动引导您完成创建站点的过程。

安装一个或多个 **Virtual Delivery Agent (VDA)**

在运行 Windows 操作系统的计算机上安装 VDA，在主映像上或直接在每台计算机上安装均可。请参阅安装 VDA 或使用命令行安装。如果要通过 Active Directory 安装 VDA，提供了示例脚本。

对于安装了 Linux 操作系统的计算机，请按照 Linux Virtual Delivery Agent 中的指导进行操作。

对于 Remote PC Access 部署，请在每台办公 PC 上安装适用于单会话操作系统的 VDA。如果只需要核心 VDA 服务，请使用独立的 `VDAWorkstationCoreSetup.exe` 安装程序和现有的电子软件分发 (ESD) 方法。（准备安装中介绍了可用的 VDA 安装程序。）

安装可选组件

如果要使用 Citrix 通用打印服务器，请在您的打印服务器上安装其服务器组件。请参阅安装核心组件或使用命令行安装。

要允许 StoreFront 使用各种身份验证选项（例如 SAML 断言），请安装 Citrix 联合身份验证服务。

要使最终用户能够在更大程度上控制其用户帐户，请安装自助服务密码重置。

（可选）在 Citrix Virtual Apps and Desktops 部署中集成更多 Citrix 组件。

- Citrix Provisioning 是一个可选组件，用于通过流技术将主映像推送到目标设备来预配计算机。
- Citrix Gateway 是一款确保应用程序访问安全的解决方案，为管理员提供应用程序粒度级别的策略和操作控制，从而确保访问应用程序和数据的安全性。
- Citrix SD-WAN 是一套用于优化 WAN 性能的设备。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

创建计算机目录

在 Studio 中创建站点后，系统将引导您完成创建计算机目录的过程。

目录中可以包含物理机或虚拟机 (VM)。虚拟机可以从主映像创建。使用虚拟机管理程序或其他服务提供 VM 时，请先在该主机上创建一个主映像。然后，在创建目录时，请指定该映像，创建 VM 时需要使用该映像。

创建交付组

在 Studio 中创建第一个计算机目录后，系统将引导您完成创建交付组的过程。

交付组指定哪些用户可以访问选定目录中的计算机以及可供这些用户使用的应用程序。

创建应用程序组（可选）

在创建交付组后，您可以选择创建应用程序组。可为在不同交付组之间共享，或由交付组中一个用户子集使用的应用程序创建应用程序组。

准备安装

July 5, 2024

要部署 Citrix Virtual Apps and Desktops，请先安装以下组件。此过程是为向防火墙内的用户交付应用程序和桌面做准备。

- 一个或多个 Delivery Controller
- Citrix Studio
- Citrix Director
- Citrix StoreFront
- Citrix 许可证服务器
- 一个或多个 Citrix Virtual Delivery Agent (VDA)
- 可选组件和技术，例如，通用打印服务器、联合身份验证服务和自助服务密码重置

对于您的防火墙外部的用户，请安装并配置一个附加组件，例如 Citrix Gateway。有关说明，请参阅将 Citrix Virtual Apps and Desktops 与 Citrix Gateway 集成。

如果您的部署中包括 Windows Server 工作负载，请配置 Microsoft RDS 许可证服务器。

可以使用产品 ISO 中的完整产品安装程序部署许多组件和技术。可以使用独立的 VDA 安装程序来安装 VDA。Citrix 下载站点上提供独立的 VDA 安装程序。所有的安装程序都提供图形界面和命令行接口。请参阅安装程序。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

产品 ISO 包含用于在 Active Directory 中安装、升级或删除计算机组的 VDA 的示例脚本。也可以使用脚本来管理 Machine Creation Services (MCS) 和 Citrix Provisioning（以前称为 Provisioning Services）使用的映像。有关详细信息，请参阅使用脚本安装 VDA。

安装之前要查看的信息

- 技术概述：如果您不熟悉该产品及其组件。
- 安全：计划您的部署环境时。
- 已知问题：在此版本中可能会遇到的问题。
- 数据库：了解系统数据库的相关信息以及如何配置这些数据库。在安装 Controller 过程中，可以安装 SQL Server Express 以用作站点数据库。大部分数据库信息都是在安装核心组件之后创建站点时配置的。
- Remote PC Access：如果您要部署一个让您的用户可以远程访问其在办公室的物理机的环境。
- 连接和资源：如果您要使用虚拟机管理程序或其他服务为应用程序和桌面托管或预配 VM。（安装核心组件之后）可以在创建站点时配置第一个连接。请在执行该操作之前随时设置您的虚拟化环境。
- Microsoft System Center Configuration Manager：如果您要使用 ConfigMgr 来管理对应用程序和桌面的访问，或者如果您要将局域网唤醒功能与 Remote PC Access 结合使用。

组件的安装位置

请查看系统要求了解支持的平台、操作系统和版本。必备组件会自动安装，除非另有说明。请参阅 Citrix StoreFront 和 Citrix 许可证服务器文档，了解其支持平台和必备条件。

您可以将核心组件安装在同一服务器或不同服务器上。

- 在一个服务器上安装所有核心组件适用于评估、测试或小型生产部署。
- 为了能够在将来扩展，请考虑在不同的服务器上安装组件。例如，将 Studio 安装在不同于安装了 Controller 的服务器的其他计算机上，您就可以远程管理站点。
- 对于大多数生产部署，建议在单独的服务器上安装核心组件。

  请先安装 Citrix 许可证服务器和许可证，然后再在其他服务器上安装其他组件。
- 要在服务器 CoreOS（例如 Delivery Controller）上安装受支持的组件，必须使用命令行。该操作系统类型不提供图形界面，因此，请在其他位置安装 Studio 和其他工具，然后将其指向 Controller 服务器。

可以在同一服务器上安装 Delivery Controller 和适用于多会话操作系统的 VDA。启动安装程序并选择 Delivery Controller（以及您希望在相应计算机上安装的任何其他核心组件）。然后再次启动安装程序并选择适用于多会话操作系统的 **Virtual Delivery Agent**。

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。保护计算机之间的通信的 Kerberos 基础结构要求同步。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用 Citrix Hypervisor 时，虚拟机的电源状态可能会显示为未知，即使看上去已注册亦如此。要解决此问题，请编辑注册表项 `HostTime` 值以禁用与主机的时间同步：

```
HKEY_LOCAL_MACHINE\Software\Citrix\XenTools\HostTime="Local"

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\XenTools\HostTime="
Local"
```

> 提示：
>
> 默认值为 `HostTime="UTC"`。将此值更改为 UTC 以外的值，例如，`Local`。此更改有效地禁用与主机的时间同步。

CTX216252 中提供了适用于 Windows 10 单会话计算机的优化指导。

不可安装组件的位置：

- 请勿在 Active Directory 域控制器上安装任何组件。
- 不支持在 SQL Server 群集安装或 SQL Server 镜像安装中的节点上安装 Controller，也不支持在运行 Hyper-V 的服务器上安装。

如果您尝试在此产品版本不支持的 Windows 操作系统中安装或升级 VDA，则会显示一条消息，指导您参阅一篇介绍选项的文章。

权限和 **Active Directory** 要求

您必须是正在安装组件的计算机上的域用户和本地管理员。

要使用独立的 VDA 安装程序，必须提升了管理权限或使用以管理员身份运行。

请在开始安装之前配置 Active Directory 域。

- 系统要求列出了受支持的 Active Directory 功能级别。Active Directory 中包含详细信息。
- 必须至少有一个运行 Active Directory 域服务的域控制器。
- 请勿在域控制器上安装任何 Citrix Virtual Apps and Desktops 组件。
- 在 Studio 中指定组织单位名称时，请勿使用正斜杠 (/)。

用于安装 Citrix 许可证服务器的 Windows 用户帐户会自动配置为委派管理完全权限管理员。

有关详细信息：

- 最佳安全做法
- 委派管理
- 有关 Active Directory 配置的 Microsoft 文档

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

安装指导、注意事项和最佳做法

在安装任何组件过程中

- 从完整产品介质安装或升级 Delivery Controller、Studio、Lixense 服务器或 Director 时，如果 Citrix 安装程序检测到计算机上先前安装的 Windows 有重新启动挂起，则安装程序将停止并退出/返回代码 9。系统会提示您重新启动计算机。

  这不是 Citrix 强制进行的重新启动。这是由于之前在计算机上安装了的其他组件而导致。如果发生这种情况，请重新启动计算机，然后再次启动 Citrix 安装程序。

  使用命令行界面时，可以通过在命令中包含 `/no_pending_reboot_check` 选项来阻止检查挂起的重新启动。

- 通常，如果组件有必备条件，安装程序会在它们不存在时部署它们。有些必备条件可能要求重新启动计算机。
- 在安装前、安装期间和安装完毕后创建对象时，为每个对象指定唯一的名称。例如，为网络、组、目录和资源提供唯一名称。
- 如果组件未成功安装，安装将停止并显示一条错误消息。成功安装的组件将会保留。不需要重新安装它们。
- 在安装（或升级）组件时，会自动收集 Citrix Analytics。默认情况下，安装完成时，这些数据会自动上载到 Citrix。此外，在安装组件时，您会自动参加 Citrix 客户体验改善计划 (CEIP)，这会上载匿名数据。

  在安装过程中，您还可以选择参与收集用于维护和故障排除的诊断信息的其他 Citrix 技术。有关这些计划的信息，请参阅 Citrix Insight Services。

- 在安装（或升级）Studio 时，会自动收集 Google Analytics（并在以后上载）。安装 Studio 后，可以使用注册表项 `HKLM\Software\Citrix\DesktopStudio\GAEnabled` 更改此设置。值 **1** 将启用收集和上载，**0** 将禁用收集和上载。
- 如果 VDA 安装失败，MSI 分析器会解析失败 MSI 日志（显示确切的错误代码）。如果是已知问题，该分析器会建议一篇 CTX 文章。该分析器还收集有关失败错误代码的匿名数据。这些数据包含在 CEIP 收集的其他数据中。如果您在 CEIP 中结束注册，则收集的 MSI 分析器数据不再发送到 Citrix。

在安装 **VDA** 过程中

- 安装 VDA 时提供适用于 Windows 的 Citrix Workspace 应用程序，但默认情况下不安装。您或您的用户可以从 Citrix Web 站点下载并安装（以及升级）适用于 Windows 的 Citrix Workspace 应用程序和其他 Citrix Workspace 应用程序。此外，也可以在您的 StoreFront 服务器上提供这些 Citrix Workspace 应用程序。请参阅 StoreFront 文档。
- 默认情况下，在受支持的 Windows 服务器上启用打印后台处理程序服务。如果禁用此服务，则无法成功安装适用于 Windows 多会话操作系统的 VDA，因此，请务必在安装 VDA 之前启用此服务。
- 大多数受支持的 Windows 版本都已附带安装 Microsoft 媒体基础。如果计算机没有媒体基础（例如 N 版本），多项多媒体功能将不安装并且无法运行。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Windows Media 重定向
  - HTML5 视频重定向
  - HDX RealTime 网络摄像机重定向

  您可以在安装媒体基础后确认该限制，或者终止 VDA 安装并在以后重新启动。在图形界面中，此选项在消息中提供。在命令行中，可以使用 `/no_mediafoundation_ack` 选项确认该限制。

- 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。在适用于单会话操作系统的 VDA 上，此组仅适用于 RDP 连接。在适用于多会话操作系统的 VDA 上，此组仅适用于 ICA 和 RDP 连接。
- VDA 必须具有有效的 Controller 地址才能进行通信。否则无法建立会话。您可以在安装 VDA 时指定 Controller 地址，也可以在以后指定。请谨记，必须指定该地址。有关详细信息，请参阅 VDA 注册。

VDA Supportability Tools

每个 VDA 安装程序都包括一个可支持性 MSI，其中包含用于检查 VDA 性能的 Citrix 工具，例如整体运行状况和连接质量。在 VDA 安装程序图形界面的附加组件页面上启用或禁用此 MSI 的安装。在命令行中，可以通过 `/exclude "Citrix Supportability Tools"` 选项禁用安装。

默认情况下，可支持性 MSI 安装在 `c:\Program Files (x86)\Citrix\Supportability Tools\` 中。可以在 VDA 安装程序图形界面的组件页面上更改此位置，也可以通过 `/installdir` 命令行选项进行更改。请记住，更改此位置将更改所有已安装的 VDA 组件的位置，而不仅仅更改可支持性工具的位置。

可支持性 MSI 中的当前工具：

- Citrix Health Assistant：有关详细信息，请参阅 CTX207624。
- VDA 清理实用程序：有关详细信息，请参阅 CTX209255。

如果安装 VDA 时未安装这些工具，CTX 文章中将包含指向当前下载页面的链接。

在安装 **VDA** 之后和过程中重新启动

VDA 安装结束时需要重新启动计算机。默认情况下会自动重新启动。

将 VDA 升级到版本 7.17（或受支持的更高版本），升级过程中将重新启动。此操作不能避免。

为了尽量减少安装 VDA 过程中所需的重新启动次数：

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

如果您未在安装 VDA 之前安装那些必备项：

- 如果您使用图形界面或使用命令行接口但未使用 `/noreboot` 选项，计算机在安装必备项后会自动重新启动。
- 如果您使用命令行接口并使用 `/noreboot` 选项，则必须启动重新启动操作。

将 VDA 升级到版本 7.17 或受支持的更高版本，升级过程中将重新启动。此操作不能避免。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

安装或升级失败时还原

> 注意：
>
> 此功能仅适用于单会话 VDA。

如果单会话 VDA 安装或升级失败，并且启用了“故障时还原”功能，计算机将返回到安装或升级开始之前设置的还原点。

在启用了此功能的情况下开始执行单会话 VDA 安装或升级时，安装程序会在开始实际安装或升级之前创建一个系统还原点。如果 VDA 安装或升级失败，计算机将返回到还原点状态。%temp%/Citrix 文件夹包含部署日志以及有关还原的其他信息。

默认情况下，此功能处于禁用状态。

如果计划启用此功能，请确保没有通过 GPO 设置 (Computer Configuration > Administrative Templates > System > System Restore) 禁用系统还原。

要在安装或升级单会话 VDA 时启用此功能，请执行以下操作：

- 使用 VDA 安装程序的图形界面(例如使用 **Autostart** 或不带任何恢复或静默选项的 XenDesktopVDASetup.exe 命令）时，选中摘要页面上的 **Enable automatic restore if update fails**（如果更新失败，则启用自动还原）复选框。

  如果安装/升级成功完成，则不使用还原点，但会保留。

- 使用 /enablerestore 或 /enablerestorecleanup 选项运行 VDA 安装程序。
  - 如果使用 /enablerestorecleanup 选项，并且安装/升级成功完成，则会自动删除还原点。
  - 如果使用 /enablerestore 选项，并且安装/升级成功完成，则不会使用还原点，但会保留。

安装程序

完整产品安装程序

使用产品 ISO 中提供的完整产品安装程序，您可以：

- 安装、升级或删除核心组件：Delivery Controller、Studio、Director 和许可证服务器。
- 安装或升级 StoreFront。
- 安装或升级适用于单会话或多会话操作系统的 Windows VDA。
- 在您的打印服务器上安装通用打印服务器 UpsServer 组件。
- 安装联合身份验证服务。
- 安装 Session Recording。

要从多会话操作系统为一个用户交付桌面（例如，用于 Web 部署），请使用完整产品安装程序的命令行接口。有关详细信息，请参阅服务器 VDI。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

独立的 **VDA** 安装程序

Citrix 下载页面上提供独立的 VDA 安装程序。（它们不能从产品安装介质中获取。）独立的 VDA 安装程序远小于完整产品 ISO。它们可以更轻松地适应以下部署：

- 使用本地暂存或复制的电子软件分发 (ESD) 软件包
- 具有物理计算机
- 具有远程办公室

默认情况下，自解压独立 VDA 中的文件被解压至 **Temp** 文件夹。解压至 **Temp** 文件夹时所需的计算机上的磁盘空间高于使用完整产品安装程序时所需的磁盘空间。但是，解压至 **Temp** 文件夹的文件在安装完成后会自动被删除。或者，可以使用 `/extract` 命令与绝对路径。

有三个独立的 VDA 安装程序供下载。

VDAServerSetup.exe：

安装适用于多会话操作系统的 VDA。它支持完整产品安装程序适用的所有适用于多会话操作系统的 VDA 选项。

VDAWorkstationSetup.exe：

安装适用于单会话操作系统的 VDA。它支持完整产品安装程序适用的所有适用于单会话操作系统的 VDA 选项。

VDAWorkstationCoreSetup.exe：

安装为 Remote PC Access 部署或核心 VDI 安装优化过的适用于单会话操作系统的 VDA。Remote PC Access 使用物理计算机。核心 VDI 安装是不用作映像的 VM。在此类部署中，它只安装 VDA 连接所需的核心服务。因此，它只支持完整产品安装程序或 `VDAWorkstationSetup.exe` 安装程序适用的选项中的一部分。

此安装程序不安装或包含用于以下项的组件：

- App-V。
- Profile Management。将 Citrix Profile Management 排除在安装之外将影响 Citrix Director 显示内容。有关详细信息，请参阅安装 VDA。
- Machine Identity Service。
- Citrix Supportability Tools。
- Citrix Files for Windows。
- Citrix Files for Outlook。
- Citrix WEM 代理。

`VDAWorkstationCoreSetup.exe` 安装程序不安装或包含适用于 Windows 的 Citrix Workspace 应用程序。

使用 `VDAWorkstationCoreSetup.exe` 相当于使用完整版产品或 `VDAWorkstationSetup` 安装程序安装单会话操作系统 VDA，并且：

- 在图形界面中：选择环境页面上的“Remote PC Access”选项。
- 在命令行接口中：指定 `/remotepc` 选项。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 在命令行界面中：指定 /components vda 和 /exclude "Citrix Personalization for App-V - VDA""Machine Identity Service""Citrix User Profile Management""Citrix User Profile Management WMI Plugin""Citrix Supportability Tools""Citrix Files for Windows""Citrix WEM Agent。

可以在以后运行完整产品安装程序来安装忽略的组件/功能。该操作使您能够安装所有缺少的组件。

VDAWorkstationCoreSetup.exe 安装程序会自动安装浏览器内容重定向 MSI。此自动安装适用于 VDA 2003 及受支持的更高版本。

Citrix 安装返回代码

安装日志以 Citrix 返回代码而不是 Microsoft 值形式包含组件安装结果。

- 0 = Success
- 1 = Failed
- 2 = PartialSuccess
- 3 = PartialSuccessAndRebootNeeded
- 4 = FailureAndRebootNeeded
- 5 = UserCanceled
- 6 = MissingCommandLineArgument
- 7 = NewerVersionFound
- 8 = SuccessRebootNeeded
- 9 = FileLockReboot
- 10 = Aborted
- 11 = FailedMedia
- 12 = FailedLicense
- 13 = FailedPrecheck
- 14 = AbortedPendingRebootCheck
- -1 = Exit

例如，使用 Microsoft System Center Configuration Manager 等工具时，如果安装日志包含返回代码 3，则通过脚本进行的 VDA 安装可能失败。在 VDA 安装程序等待必须启动的重新启动时（例如，在服务器上安装 RDS 角色必备条件后），可能会发生这种情况。只有在安装了所有必备项和选定组件，并且在安装后重新启动计算机后，才会认为 VDA 安装成功。

或者，您可以在 CMD 脚本（返回 Microsoft 退出代码）中打包您的安装，或更改 Configuration Manager 软件包中的成功代码。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

配置适用于 **Windows Server** 工作负载的 **Microsoft RDS** 许可证服务器

此产品在交付 Windows Server 工作负载（例如 Windows 2016）时访问 Windows Server 远程会话功能。这通常需要远程桌面服务客户端访问许可证 (RDS CAL)。VDA 必须能够联系 RDS 许可证服务器以请求 RDS CAL。安装并激活许可证服务器。有关详细信息，请参阅 Microsoft 文档激活远程桌面服务许可证服务器。对于概念证明环境，您可以使用 Microsoft 提供的宽限期。

通过此方法，您可以让此服务应用许可证服务器设置。可以在映像上的 RDS 控制台中配置许可证服务器和每用户模式。还可以使用 Microsoft 组策略设置配置许可证服务器。有关详细信息，请参阅 Microsoft 文档使用客户端访问许可证 (CAL) 许可 RDS 部署。

要使用组策略设置配置 RDS 许可证服务器，请执行以下操作：

1. 在可用计算机上安装远程桌面服务许可证服务器。计算机必须始终可用。Citrix 产品工作负载必须能够访问此许可证服务器。
2. 使用 Microsoft 组策略指定许可证服务器地址和每用户许可模式。有关详细信息，请参阅 Microsoft 文档为 RD 会话主机服务器指定远程桌面许可模式。

Windows 10 工作负载需要适当的 Windows 10 许可证激活。我们建议您按照 Microsoft 文档来激活 Windows 10 工作负载。

Microsoft System Center Virtual Machine Manager 虚拟化环境

January 21, 2022

如果您结合使用 Hyper-V 与 Microsoft System Center Virtual Machine Manager (VMM) 来提供虚拟机，请按本指导操作。

此版本支持系统要求中列出的 VMM 版本。

> 注意：
>
> 不支持混合 Hyper-V 群集（包含运行不同 Hyper-V 版本的服务器）。

可以使用 Citrix Provisioning（以前称为 Provisioning Services）和 Machine Creation Services 预配以下各项：

- 第 1 代支持的桌面或服务器操作系统 VM.
- 第 2 代支持的桌面或服务器操作系统 VM，包括安全启动支持。

安装和配置虚拟机管理程序

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 重要：
>
> 所有 Delivery Controller 必须与 VMM 服务器位于同一个林中。

1. 在服务器上安装 Microsoft Hyper-V Server 和 VMM。
2. 在所有 Controller 上安装 System Center Virtual Machine Manager 控制台。控制台版本必须与管理服务器版本一致。尽管早期版本的控制台可以连接到管理服务器，但是如果版本不同，预配 VDA 将失败。
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。

   > 提示：
   >
   > 使用 VMM 委派管理员时，您需要定义顶层主机组，然后仅向委派管理员授予对此组的完全访问权限。多个主机组需要多个 VMM 委派管理员。为每个主机组配置一个委派管理员。

   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。此配置支持 VM 生命周期管理，例如 VM 创建、更新和删除。

   不支持在运行 Hyper-V 的服务器上安装 Controller。

创建主 **VM**

1. 在主 VM 上安装 VDA，然后选择用于优化桌面的选项以提高性能。
2. 生成主 VM 的快照作为备份。

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 VM 的权限。
4. 在主机详细信息中，选择创建 VM 时将使用的群集或独立主机。

   即使使用单 Hyper-V 主机部署，也请浏览并选择群集或独立主机。

SMB 3 文件共享上的 **MCS**

对于在 SMB 3 文件共享中通过 MCS 为 VM 存储创建的计算机目录，请确保凭据满足以下要求。这些要求可确保来自 Controller 的虚拟机管理程序通信库 (HCL) 的调用成功连接到 SMB 存储：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 Server 使用 VMM 用户凭据执行。

使用 SMB 存储时，请启用从 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)。在 Windows Server 2012 上通过 Hyper-V 对 VMM 2012 SP1 执行此过程。有关详细信息，请参阅 CTX137465。

HCL 使用 `CredSSP` 打开与 Hyper-V 计算机的连接。此功能将 Kerberos 加密的用户凭据传递到 Hyper-V 计算机。远程 Hyper-V 计算机上的会话中的 **PowerShell** 命令使用提供的凭据运行。在这种情况下，使用的是 VMM 用户的凭据，以便与存储的通信命令正常运行。

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 MCS 预配方案（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 VM（并删除对初始主 VM 的依赖）。

  ConvertVirtualHardDisk 位于 root\virtualization\v2 命名空间

  示例：

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)
$result
<!--NeedCopy-->
```

- 创建差异磁盘：从合并主映像时产生的主映像创建差异磁盘。差异磁盘随后将连接到新 VM。

  CreateVirtualHardDisk 位于 root\virtualization\v2 命名空间

  示例：

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.CreateVirtualHardDisk($vhdastext);
$result
<!--NeedCopy-->
```

- 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。

  HCL 通过管理员共享将身份上载到 Hyper-V 计算机。

  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）。

  HCL 删除管理员共享中的文件。

  当 HCL 完成将身份磁盘上载到 Hyper-V 计算机时，远程 PowerShell 会话会将身份磁盘复制到 SMB 存储。然后，它将从 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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 Server 上创建一个仅 VMM 用户有权访问的文件夹（如果尚不存在）。

  Hyper-V 计算机通过 PowerShell 脚本将磁盘从 SMB 存储复制到本地 Hyper-V 存储。此脚本在 PowerShell V3 远程会话中运行。

  HCL 将 Hyper-V 计算机管理员共享中的磁盘读取到内存。

  HCL 删除管理员共享中的文件。

Citrix Hypervisor 虚拟化环境

January 21, 2022

创建与 **Citrix Hypervisor** 的连接

创建与 Citrix Hypervisor（以前称为 XenServer）的连接时，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 Citrix Hypervisor 的通信安全。要使用 HTTPS，必须替换 Citrix Hypervisor 上安装的默认 SSL 证书；请参阅 CTX128656。

如果 Citrix Hypervisor 服务器上已启用高可用性，则可以配置高可用性。Citrix 建议您（从“编辑高可用性”中）选择池中的所有服务器，以便在池主服务器出现故障时能够与 Citrix Hypervisor 服务器进行通信。

如果 Citrix Hypervisor 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。

在一个或多个 Citrix Hypervisor 主机上使用本地存储作为临时数据存储时，请确保池中的每个存储位置都具有唯一的名称。（要在 XenCenter 中更改名称，请右键单击该存储并编辑名称属性。）

可以使用 Citrix Provisioning（以前称为 Provisioning Services）和 Machine Creation Services (MCS) 预配以下各项：

- 支持的桌面或服务器操作系统 VM 的旧版 BIOS。
- 支持的桌面或服务器操作系统 VM 的 UEFI，包括安全启动。

> 注意：
>
> 配置 MCS 时，需要池操作员权限或更高权限。

将 **IntelliCache** 用于 **Citrix Hypervisor** 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取数量。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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 Citrix Hypervisor 中均启用 IntelliCache。

- 安装 Citrix Hypervisor 时，选择 **Enable thin provisioning (Optimized storage for Virtual Desktops)**（启用精简预配 (Virtual Desktops 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 Citrix Hypervisor 文档。
- 在 Citrix Virtual Apps and Desktops 中，默认情况下禁用 IntelliCache。只能在创建 Citrix Hypervisor 连接时更改此设置；之后将无法禁用 IntelliCache。添加 Citrix Hypervisor 连接时：
  - 选择共享作为存储类型。
  - 选中使用 **IntelliCache** 复选框。

使用 **Citrix Hypervisor** 连接创建计算机目录

具有 GPU 功能的计算机需要专用主映像。这些 VM 要求使用支持 GPU 的视频卡驱动程序。应配置支持 GPU 的计算机，以使 VM 与使用 GPU 进行操作的软件结合使用。

1. 在 XenCenter 中，创建一个具有标准 VGA、网络和 vCPU 的 VM。
2. 更新 VM 配置以启用 GPU 使用（直通或 vGPU）。
3. 安装支持的操作系统并启用 RDP。
4. 安装 Citrix VM Tools 和 NVIDIA 驱动程序。
5. 清除虚拟网络计算 (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。

更多信息

- 连接和资源
- 创建计算机目录

Microsoft System Center Configuration Manager 环境

January 21, 2022

通过这些选项，使用 Microsoft System Center Configuration Manager (Configuration Manager) 来管理对应用程序和桌面的访问的站点可以将这种用法扩展到 Citrix Virtual Apps and Desktops：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 使用 SCCM 安装 VDA。
- **Configuration Manager** 唤醒代理功能： Configuration Manager 支持 Remote PC Access 局域网唤醒功能。有关详细信息，请参阅局域网唤醒—SCCM 集成。
- **Citrix Virtual Apps and Desktops** 属性：通过属性，您可以识别 Citrix Virtual Desktops 以便通过 Configuration Manager 进行管理。（在某些版本中，Configuration Manager 使用 Citrix Virtual Apps and Desktops 之前的名称：XenApp 和 XenDesktop。）

属性

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

在 Configuration Manager 中显示的布尔属性会显示为 1 或 0，而非 true 或 false。

这些属性可用于 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、None 和 User（将 IsAssigned 设置为 True）
BrokerSiteName	返回与 HostIdentifier 相同的值
DesktopCatalogName	与桌面关联的计算机目录。
DesktopGroupName	与桌面关联的交付组。
HostIdentifier	返回与 BrokerSiteName 相同的值。
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，在映像上安装应用程序，而非在预配的计算机上安装应用程序。有效值如下：在用作映像的 VM 上为 True。此值在安装期间基于选项而设置，或者在从该映像预配的 VM 上取消选中。
IsVirtualMachine	如果是虚拟机，则为 True；如果是物理机，则为 **false**。
OSChangesPersist	如果桌面操作系统映像在每次重新启动时都重置为清除状态，则为 False，否则为 **true**。
PersistentDataLocation	Configuration Manager 存储永久数据的位置。用户无法访问此位置。
BrokerSiteName, DesktopCatalogName, DesktopGroupName, HostIdentifier	已确定桌面何时向 Controller 中注册。对于尚未完全注册的桌面，这些值为空。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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，名称包括空格或与属性名称略不相同。例如，`BrokerSiteName` 显示为 `Broker Site Name`。

- 配置 Configuration Manager 以便从 Citrix VDA 收集 Citrix WMI 属性
- 使用 Citrix WMI 属性创建基于查询的设备集合
- 根据 Citrix WMI 属性创建全局条件
- 使用全局条件定义应用程序部署类型要求

还可以使用 `Root\ccm_vdi` 命名空间中 Microsoft 类 `CCM_DesktopMachine` 中的 Microsoft 属性。有关详细信息，请参阅 Microsoft 文档。

VMware 虚拟化环境

May 19, 2023

如果您使用 VMware 提供虚拟机，请按照此指导进行操作。

安装 vCenter Server 以及相应的管理工具。（不支持 vSphere vCenter 链接模式操作。）

如果您计划使用 MCS，请勿在 vCenter Server 中禁用数据存储浏览器功能（如 https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2101567 中所述）。禁用了此功能时，MCS 无法正常工作。

可以使用 Citrix Provisioning（以前称为 Provisioning Services）和 Machine Creation Services 预配以下各项：

- 支持的桌面或服务器操作系统 VM 的旧版 BIOS。
- 支持的桌面或服务器操作系统 VM 的 UEFI，包括安全启动。

所需权限

创建 VMware 用户帐户以及一个或多个 VMware 角色。请根据需要分配用户权限的粒度级别来创建这些角色。使用 Citrix Virtual Apps and Desktops 执行操作所需的 vCenter 权限列表定义每个角色的权限。

要向用户授予权限，请在数据中心级别将该用户与角色关联。有关在 vCenter 中设置权限的详细信息，请参阅 VMware 文档。

以下各表显示了 Citrix Virtual Apps and Desktops 操作与所需的最低 VMware 权限之间的映射关系。

> 注意：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 某些 vSphere 版本的权限列表显示名称（特别是用户界面）不同。例如，在 vSphere 6.7 中，用户界面权限为更改内存和更改设置，而非本页上注明的所需权限中所述的设置和内存。

添加连接和资源

SDK	用户界面
System.Anonymous、System.Read 和 System.View	自动添加。可以使用内置的只读角色。

电源管理

SDK	用户界面
VirtualMachine.Interact.PowerOff	虚拟机 > 交互 > 关闭
VirtualMachine.Interact.PowerOn	虚拟机 > 交互 > 打开
VirtualMachine.Interact.Reset	虚拟机 > 交互 > 重置
VirtualMachine.Interact.Suspend	虚拟机 > 交互 > 挂起

预配计算机 **(Machine Creation Services)**

要使用 MCS 预配计算机，必须具备以下权限：

SDK	用户界面
Datastore.AllocateSpace	数据存储 > 分配空间
Datastore.Browse	数据存储 > 浏览数据存储
Datastore.FileManagement	数据存储 > 低级别文件操作
Network.Assign	网络 > 分配网络
Resource.AssignVMToPool	资源 > 将虚拟机分配到资源池
VirtualMachine.Config.AddExistingDisk	虚拟机 > 配置 > 添加现有磁盘
VirtualMachine.Config.AddNewDisk	虚拟机 > 配置 > 添加新磁盘
VirtualMachine.Config.AdvancedConfig	虚拟机 > 配置 > 高级
VirtualMachine.Config.RemoveDisk	虚拟机 > 配置 > 删除磁盘

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SDK	用户界面
VirtualMachine.Config.CPUCount	虚拟机 > 配置 > 更改 CPU 计数
VirtualMachine.Config.Memory	虚拟机 > 配置 > 更改内存
VirtualMachine.Config.Settings	虚拟机 > 配置 > 更改设置
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.CreateFromExisting	虚拟机 > 清单 > 从现有项创建
VirtualMachine.Inventory.Create	虚拟机 > 清单 > 新建
VirtualMachine.Inventory.Delete	虚拟机 > 清单 > 删除
VirtualMachine.Provisioning.Clone	虚拟机 > 预配 > 克隆虚拟机
VirtualMachine.State.CreateSnapshot	vSphere 5.0 Update 2、vSphere 5.1 Update 1 和 vSphere 6.x Update 1：虚拟机 > 状态 > 创建快照； vSphere 5.5：虚拟机 > 快照管理 > 创建快照

映像更新和回滚

SDK	用户界面
Datastore.AllocateSpace	数据存储 > 分配空间
Datastore.Browse	数据存储 > 浏览数据存储
Datastore.FileManagement	数据存储 > 低级别文件操作
Network.Assign	网络 > 分配网络
Resource.AssignVMToPool	资源 > 将虚拟机分配到资源池
VirtualMachine.Config.AddExistingDisk	虚拟机 > 配置 > 添加现有磁盘
VirtualMachine.Config.AddNewDisk	虚拟机 > 配置 > 添加新磁盘
VirtualMachine.Config.AdvancedConfig	虚拟机 > 配置 > 高级
VirtualMachine.Config.RemoveDisk	虚拟机 > 配置 > 删除磁盘
VirtualMachine.Interact.PowerOff	虚拟机 > 交互 > 关闭
VirtualMachine.Interact.PowerOn	虚拟机 > 交互 > 打开

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SDK	用户界面
VirtualMachine.Interact.Reset	虚拟机 > 交互 > 重置
VirtualMachine.Inventory.CreateFromExisting	虚拟机 > 清单 > 从现有项创建
VirtualMachine.Inventory.Create	虚拟机 > 清单 > 新建
VirtualMachine.Inventory.Delete	虚拟机 > 清单 > 删除
VirtualMachine.Provisioning.Clone	虚拟机 > 预配 > 克隆虚拟机

删除预配的计算机

SDK	用户界面
Datastore.Browse	数据存储 > 浏览数据存储
Datastore.FileManagement	数据存储 > 低级别文件操作
VirtualMachine.Config.RemoveDisk	虚拟机 > 配置 > 删除磁盘
VirtualMachine.Interact.PowerOff	虚拟机 > 交互 > 关闭
VirtualMachine.Inventory.Delete	虚拟机 > 清单 > 删除

存储配置文件 **(vSAN)**

要在 vSAN 数据存储上创建目录期间查看、创建或删除存储策略，必须具备以下权限：

SDK	用户界面
storage.Profile 驱动的存储更新	配置文件驱动的存储 > 配置文件驱动的存储更新
storage.Profile 驱动的存储视图	配置文件驱动的存储 > 配置文件驱动的存储视图

标记和自定义属性

标记和自定义属性允许您将元数据附加到在 vSphere 清单中创建的 VM，从而更轻松地搜索和筛选这些对象。要创建、编辑、分配和删除标记或类别，必须具备以下权限：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SDK	用户界面
Tagging.Create	vSphere 标记 > 创建 vSphere 标记
Tagging.Create	vSphere 标记 > 创建 vSphere 标记类别
Tagging.Edit	vSphere 标记 > 编辑 vSphere 标记
Tagging.Edit	vSphere 标记 > 编辑 vSphere 标记类别
Tagging.Delete	vSphere 标记 > 删除 vSphere 标记
Tagging.Delete	vSphere 标记 > 删除 vSphere 标记类别
Tagging.Assign	vSphere 标记 > 分配或取消分配 vSphere 标记
Tagging.Assign	vSphere 标记 > 在对象上分配或取消分配 vSphere 标记
Global.ManageCustomFields	全局 > 管理自定义属性
Global.SetCustomField	全局 > 设置自定义属性

> 注意：
>
> 当 MCS 创建计算机目录时，它会使用特殊的名称标记来标记目标 VM。这些标记将主映像与 MCS 创建的 VM 区分开来，并防止使用 MCS 创建的 VM 进行映像准备。您可以在 vCenter 中通过 `XdProvisioned` 属性的值来识别差异。如果 MCS 创建了 VM，该属性将设置为 **True**。

加密操作

加密操作权限控制谁可以对哪种类型的对象执行哪种类型的加密操作。vSphere Native Key Provider 使用 `Cryptographer.*` 权限。加密操作需要以下最低权限：

SDK	用户界面
Cryptographic operations.Direct Access	权限 > 所有权限 > 加密操作 > 直接访问
Cryptographic operations.Add disk	权限 > 所有权限 > 加密操作 > 添加磁盘
Cryptographic operations.Clone	权限 > 所有权限 > 加密操作 > 克隆
Cryptographic operations.Encrypt	权限 > 所有权限 > 加密操作 > 加密
Cryptographic operations.Encrypt new	权限 > 所有权限 > 加密操作 > 加密新对象

预配计算机 **(Citrix Provisioning)**

所有来自预配计算机 **(Machine Creation Services)** 的权限以及以下各项。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SDK	用户界面
VirtualMachine.Config.AddRemoveDevice	虚拟机 > 配置 > 添加或删除设备
VirtualMachine.Config.CPUCount	虚拟机 > 配置 > 更改 CPU 计数
VirtualMachine.Config.Memory	虚拟机 > 配置 > 内存
VirtualMachine.Config.Settings	虚拟机 > 配置 > 设置
VirtualMachine.Provisioning.CloneTemplate	虚拟机 > 预配 > 克隆模板
VirtualMachine.Provisioning.DeployTemplate	虚拟机 > 预配 > 部署模板

> 注意：
>
> 要通过 Citrix Provisioning 控制台使用 Citrix Virtual Apps and Desktops 设置向导和导出设备向导预配 VM，需要克隆和部署模板的权限。

获取和导入证书

为了保护 vSphere 通信的安全，Citrix 建议您使用 HTTPS，而不使用 HTTP。

HTTPS 需要数字证书。使用由证书颁发机构颁发的符合贵组织的安全策略的数字证书。

如果无法使用证书颁发机构所颁发的数字证书，则可以使用由 VMware 安装的自签名证书。仅当贵组织的安全策略允许时才能使用此方法。在每个 Delivery Controller 中添加 VMware vCenter 证书。

1. 将运行 vCenter Server 的计算机的完全限定域名 (FQDN) 添加到该服务器上的主机文件中，文件位于：%SystemRoot%/WINDOWS/system32/Drivers/etc/。只有当域名系统中尚不存在运行 vCenter Server 的计算机的 FQDN 时，才需要执行此步骤。
2. 使用以下任意三种方法之一获取 vCenter 证书：

   从 **vCenter Server**。

   a) 将 rui.crt 文件从 vCenter Server 复制到 Delivery Controller 上可访问的位置。
   b) 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，请右键单击 Internet Explorer，然后选择以管理员身份运行以下载或安装证书。

   a) 打开 Web 浏览器，与 vCenter Server 建立安全 Web 连接（例如 https://server1.domain1.com)）。
   b) 接受安全警告。
   c) 单击显示证书错误的地址栏。
   d) 查看证书并单击“详细信息”选项卡。
   e) 选择 **Copy to file and export in .CER format**（复制到文件并导出为.CER 格式），并在系统提示时提供名称。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

f) 保存导出的证书。
g) 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** 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。
- 查看证书。

3. 将证书导入到每个 Controller 上的证书存储中。

a) 单击安装证书选项，选择本地计算机，然后单击下一步。
b) 选择将所有的证书都放入下列存储，然后单击浏览。选择受信任人，然后单击确定。单击下一步，然后单击完成。

如果在安装后更改 vSphere 服务器的名称，必须在该服务器上生成新的自签名证书，然后再导入新证书。

配置注意事项

创建主 **VM**：

使用主 VM 在计算机目录中提供用户桌面和应用程序。在虚拟机管理程序上：

1. 在主 VM 上安装 VDA，选择用于优化桌面的选项，这样会提高性能。
2. 生成主 VM 的快照作为备份。

创建连接：

在连接创建向导中执行以下操作：

- 选择 VMware 连接类型。
- 指定 vCenter SDK 接入点的地址。
- 指定先前设置的具有创建 VM 权限的 VMware 用户帐户的凭据。以域/用户名格式指定用户名。

VMware SSL 指纹

VMware SSL 指纹功能无需手动创建与 VMware vSphere 虚拟机管理程序的主机连接。在创建连接之前，不再需要在站点中的 Delivery Controller 与虚拟机管理程序的证书之间手动创建信任关系。

VMware SSL 指纹功能将不受信任的证书的指纹存储在站点数据库中。此配置可确保虚拟机管理程序可以连续地被 Citrix Virtual Apps and Desktops 识别为可信任，即使不是 Controller 识别的亦如此。

在 Studio 中创建 vSphere 主机连接时，可以通过一个对话框查看要连接的计算机的证书。然后，您可以选择是否信任该证书。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nutanix 虚拟化环境

January 21, 2022

在使用 Nutanix Acropolis 向您的 Citrix Virtual Apps and Desktops 部署中提供虚拟机时，请遵循此指导。安装过程中包括以下任务：

- 在您的 Citrix Virtual Apps and Desktops 环境中安装并注册 Nutanix 插件。
- 创建与 Nutanix Acropolis 虚拟机管理程序的连接。
- 创建一个将使用您在 Nutanix 虚拟机管理程序上创建的主映像的快照的计算机目录。

有关详细信息，请参阅 Nutanix 支持门户中提供的“Nutanix Acropolis MCS plug-in Installation Guide”（《Nutanix Acropolis MCS 插件安装指南》）。

安装并注册 Nutanix 插件

完成以下过程以在 Cloud Connector 上安装并注册 Nutanix 插件。使用 Citrix Cloud 中的 **Manage**（管理）功能创建与 Nutanix 虚拟机管理程序的连接。然后创建一个使用您在 Nutanix 环境中创建的主映像的快照的计算机目录。

> 提示：
>
> Citrix 建议您在安装或更新 Nutanix 插件时停止并重新启动 Citrix Host Service、Citrix Broker Service 和 Machine Creation Service。

有关安装 Nutanix 插件的信息，请参阅 Nutanix 文档站点。

创建与 Nutanix 的连接

请参阅创建站点或连接和资源，了解用于创建连接的向导中所有页面的完整信息。

在“站点设置”或“添加连接和资源”向导中的连接页面上，选择 **Nutanix** 连接类型。指定虚拟机管理程序地址和凭据以及连接的名称。在网络页面上，选择用于托管单元的网络。

使用 Nutanix 快照创建计算机目录

此信息用于补充创建计算机目录一文中的指导信息。此信息仅描述特定于 Nutanix 的字段。

您所选的快照是用于在目录中创建 VM 的模板。在创建目录之前，请在 Nutanix 中创建映像和快照。

- 有关主映像的常规信息，请参阅“创建计算机目录”一文。
- 关于用于创建映像和快照的 Nutanix 程序的信息，请参阅 Nutanix 文档。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

操作系统和计算机管理页面不包含 Nutanix 特定的信息。请按照创建计算机目录一文中的指导进行操作。

在容器页面（Nutanix 独有）上，选择 VM 的磁盘所在的容器。

在主映像页面上，选择映像快照。如果需要，使用 Acropolis 控制台重命名快照。如果重命名快照，则重新启动“创建目录”向导以查看刷新的列表。

在虚拟机页面上，指示虚拟 CPU 数量和每个 vCPU 的核心数。

网卡、计算机帐户和摘要页面不包含 Nutanix 特定的信息。请按照创建计算机目录一文中的指导进行操作。

安装核心组件

January 21, 2022

核心组件为 Citrix Delivery Controller、Citrix Studio、Citrix Director 和 Citrix 许可证服务器。

（在 2003 之前的版本中，核心组件包括 Citrix StoreFront。您仍然可以通过单击 **Citrix StoreFront** 磁贴或运行安装介质中的可用命令来安装 StoreFront。）

开始安装之前，请查看本文和准备安装。

本文介绍了安装核心组件时的安装向导顺序。提供了命令行等效命令。有关详细信息，请参阅使用命令行安装。

步骤 **1.** 下载产品软件并启动向导

使用您的 Citrix 帐户凭据访问 Citrix Virtual Apps and Desktops 下载页面。下载产品 ISO 文件。

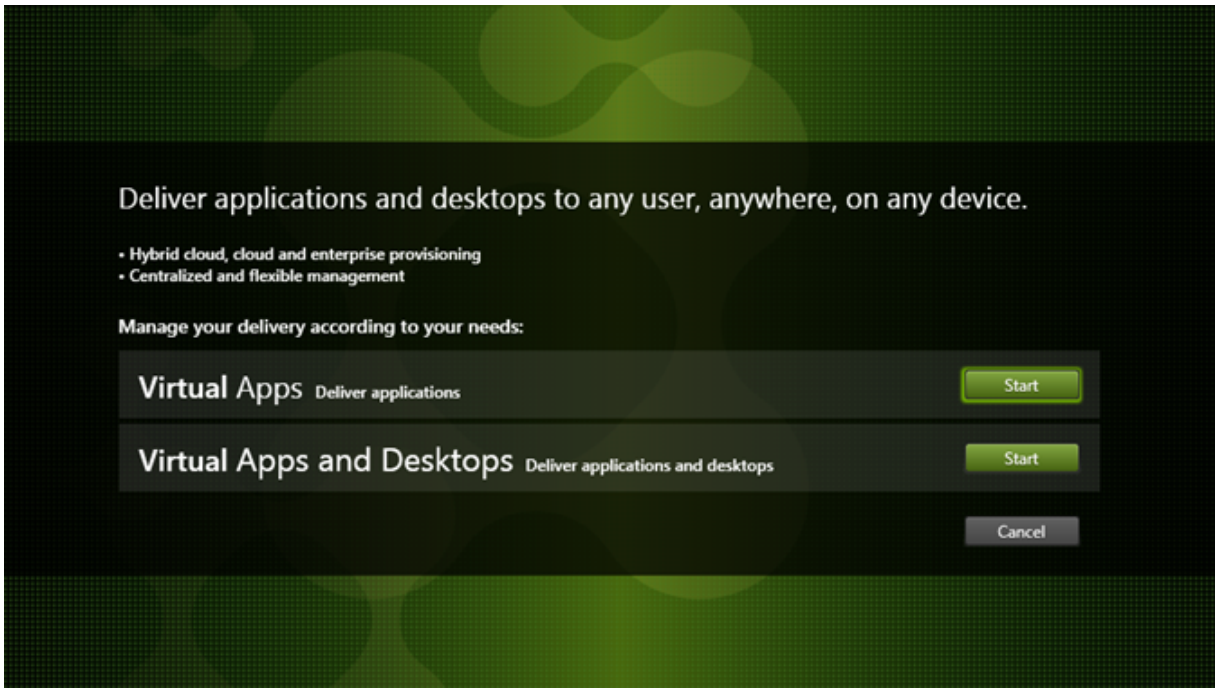
解压文件。或者刻录 ISO 文件的 DVD。

使用本地管理员帐户，登录要在其中安装核心组件的计算机。

在驱动器中插入 DVD 或装载 ISO 文件。如果安装程序未自动启动，请双击 **AutoSelect** 应用程序或装载的驱动器。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

步骤 **2.** 选择要安装的产品



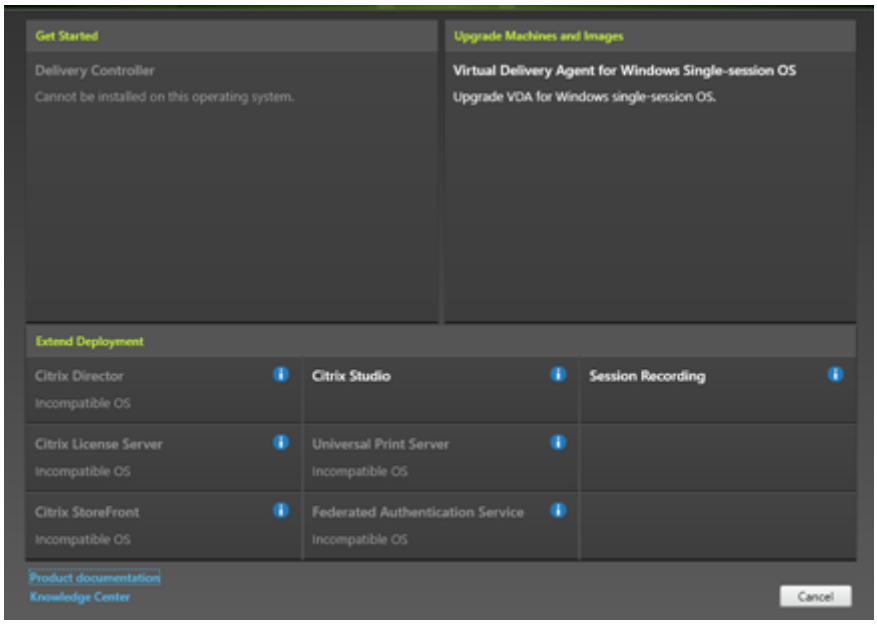
单击产品旁边的开始以安装：Virtual Apps 或 Virtual Apps and Desktops。

（如果计算机上已安装了 Citrix Virtual Apps and Desktops 组件，不会显示此页面。）

命令行选项 /xenapp 用于安装 Citrix Virtual Apps。如果忽略此选项，则安装 Citrix Virtual Apps and Desktops。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

步骤 **3.** 选择要安装的内容



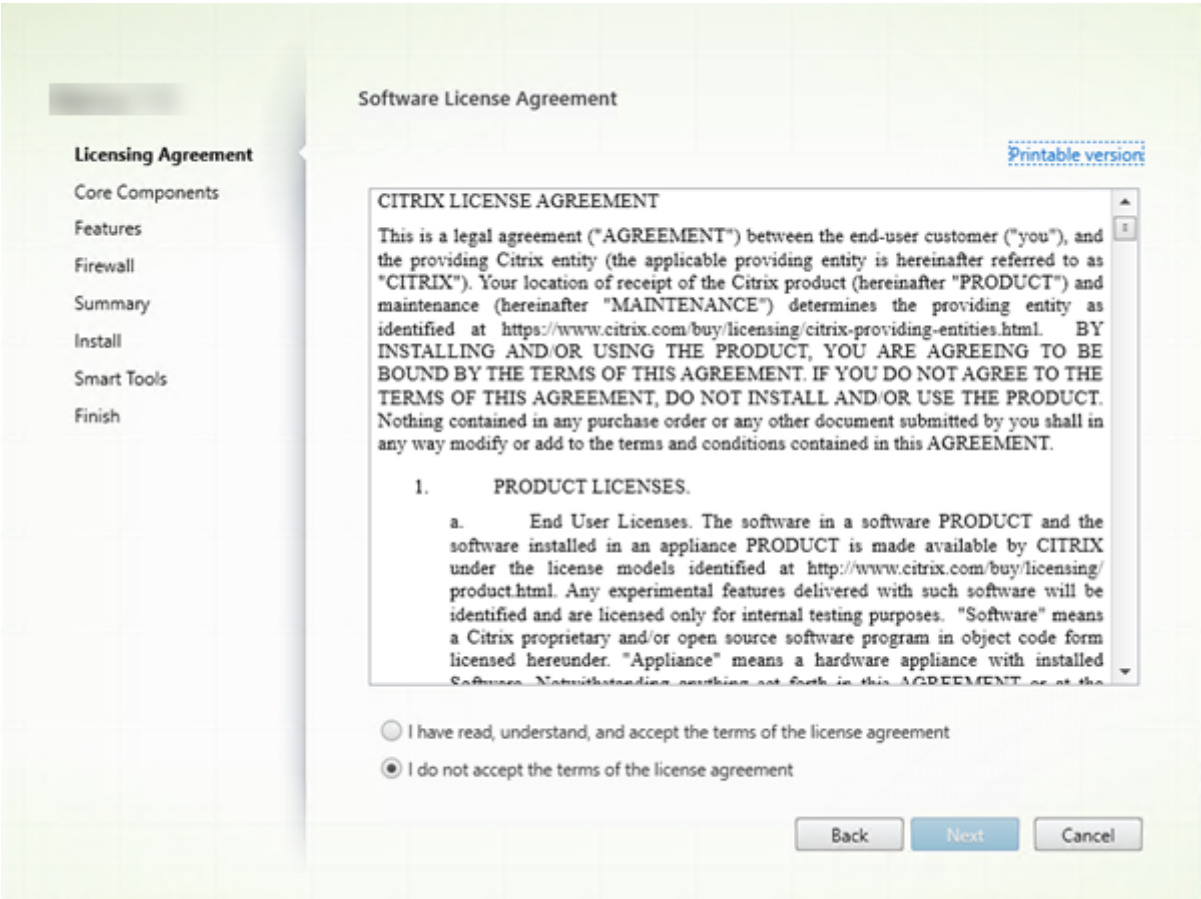
如果刚刚开始安装，请选择 **Delivery Controller**。（在下一页上，您将选择要在此计算机上安装的特定组件。）

如果您已安装 Controller（在此计算机或另一台计算机上）并要安装其他组件，请从扩展部署部分选择相应组件。

命令行选项：`/components`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

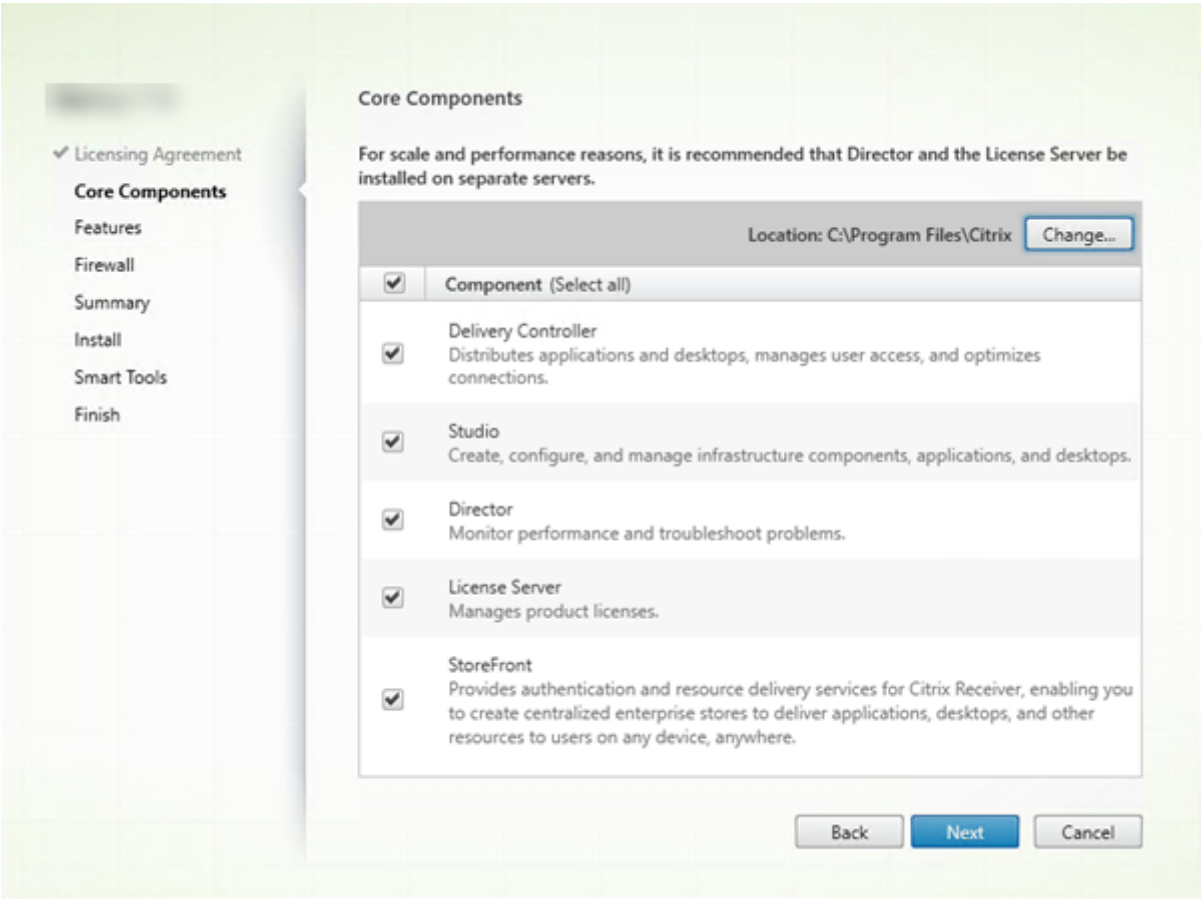
步骤 **4.** 阅读并接受许可协议



在许可协议页面上，阅读许可协议后，指明您已阅读并接受它。然后，单击下一步。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

步骤 **5.** 选择要安装的组件及安装位置



在核心组件页面上：

- 位置：默认情况下，组件安装在 `C:\Program Files\Citrix` 中。该默认设置适用于大多数部署。如果您指定一个不同的位置，它必须具有网络服务的执行权限。
- 组件：默认情况下，所有核心组件对应的复选框都处于选中状态。在一台服务器上安装所有核心组件适用于概念验证、测试或小型生产部署。对于大型生产环境，Citrix 建议在单独的服务器上安装 Director、StoreFront 和许可证服务器。

  > 注意：
  >
  > 如果要在多台服务器上安装组件，请先安装 Citrix 许可证服务器和许可证，然后再在其他服务器上安装其他组件。有关指导，请参阅《Citrix Virtual Apps and Desktops 的许可指南》的“自动安装”部分。

  您选择不在此计算机上安装某个必需的核心组件时，系统会显示图标警报。该警报提醒您安装该组件，尽管不一定在此计算机上。

单击下一步。

命令行选项：`/installdir`、`/components`、`/exclude`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

硬件检查

当您安装或升级 Delivery Controller 时，系统将检查硬件。如果计算机的 RAM 低于建议的内存量 (5 GB)，安装程序会提醒您，这可能会影响站点稳定性。有关详细信息，请参阅硬件要求。

图形界面：将显示一个对话框。

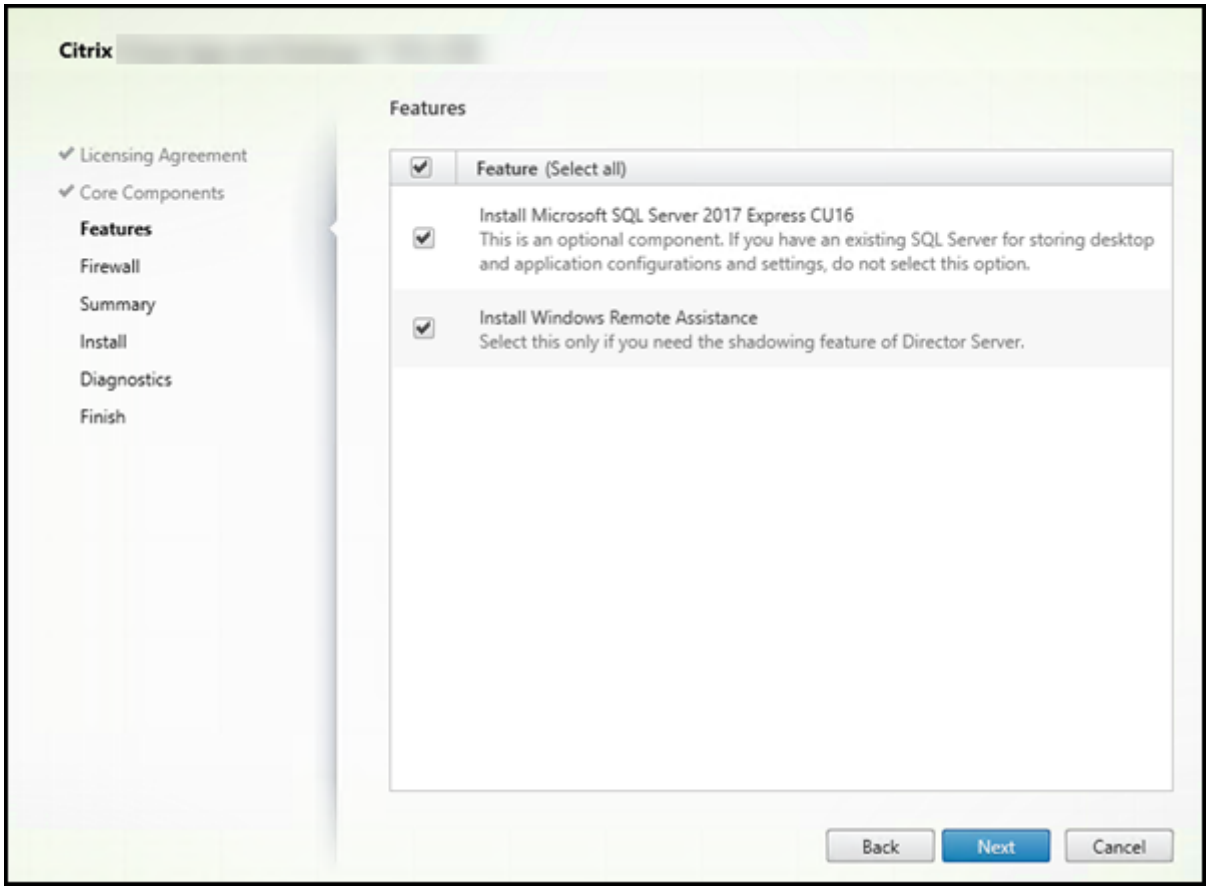
- 建议：单击取消以停止安装。向计算机添加更多 RAM，然后重新启动安装。
- 或者，单击下一步以继续安装。该站点可能存在稳定性问题。

命令行界面：安装/升级结束。安装日志包含一条消息，描述了找到的内容和可用选项。

- 建议：向计算机添加更多 RAM，然后再次运行命令。
- 或者，使用 `/ignore_hw_check_failure` 选项再次运行命令以免出现警告。您的站点可能存在稳定性问题。

升级时，如果操作系统或 SQL Server 版本不再受支持，您也会收到通知。请参阅升级部署。

步骤 6. 启用或禁用功能



在功能页面上：

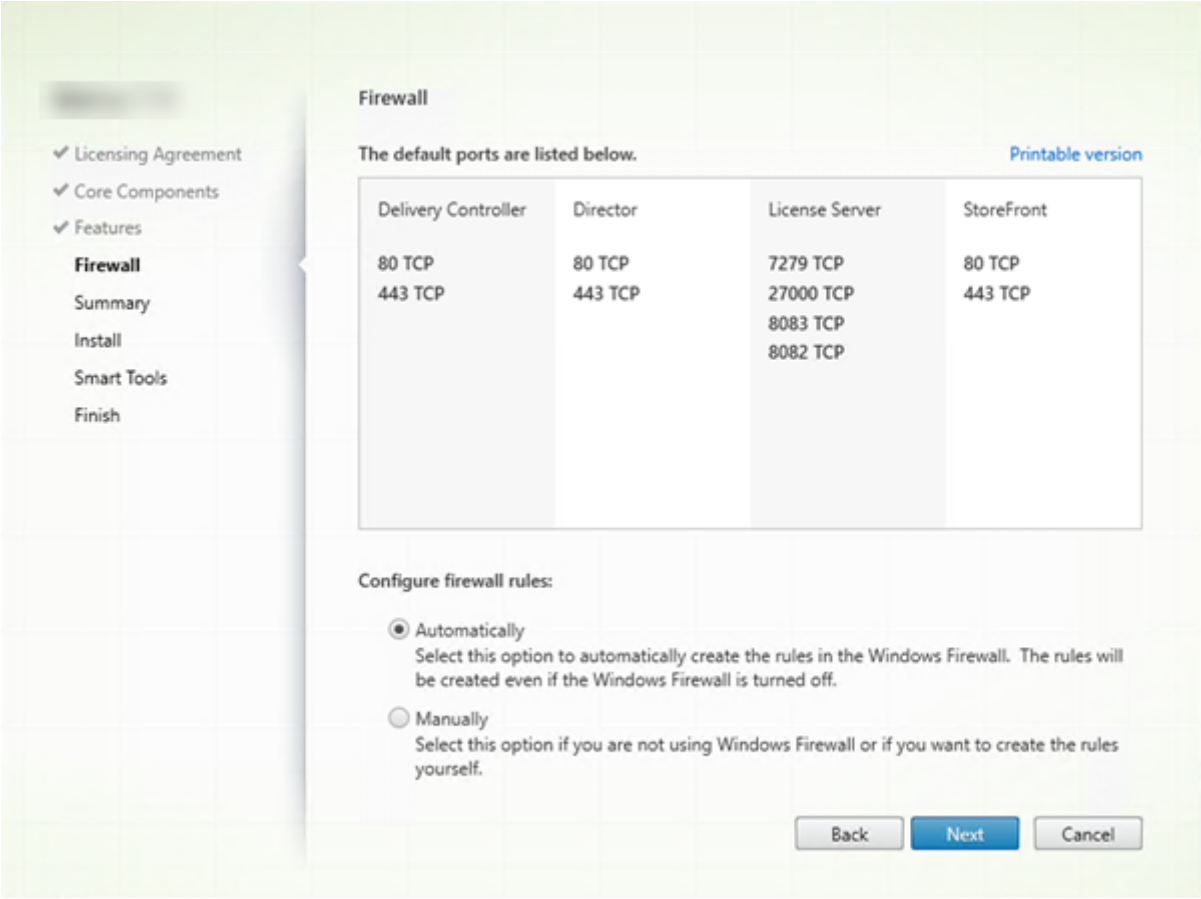
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 选择是否安装 Microsoft SQL Server Express 以用作站点数据库。默认情况下，启用此选择。如果您不熟悉 Citrix Virtual Apps and Desktops 数据库，请查看数据库。
- 安装 Director 时，自动安装 Windows 远程协助。您选择是否在 Windows 远程协助中启用重影以与 Director 用户重影结合使用。启用重影将打开 TCP 端口 3389。默认情况下，启用此功能。该默认设置适用于大多数部署。此功能仅当安装 Director 时才会显示。

单击下一步。

命令行选项：`/nosql`（用于阻止安装）、`/no_remote_assistance`（用于阻止启用）

步骤 **7.** 打开 **Windows** 防火墙端口



默认情况下，如果 Windows 防火墙服务正在运行，那么即使未启用防火墙，防火墙页面上的端口也会自动打开。该默认设置适用于大多数部署。有关端口信息，请参阅网络端口。

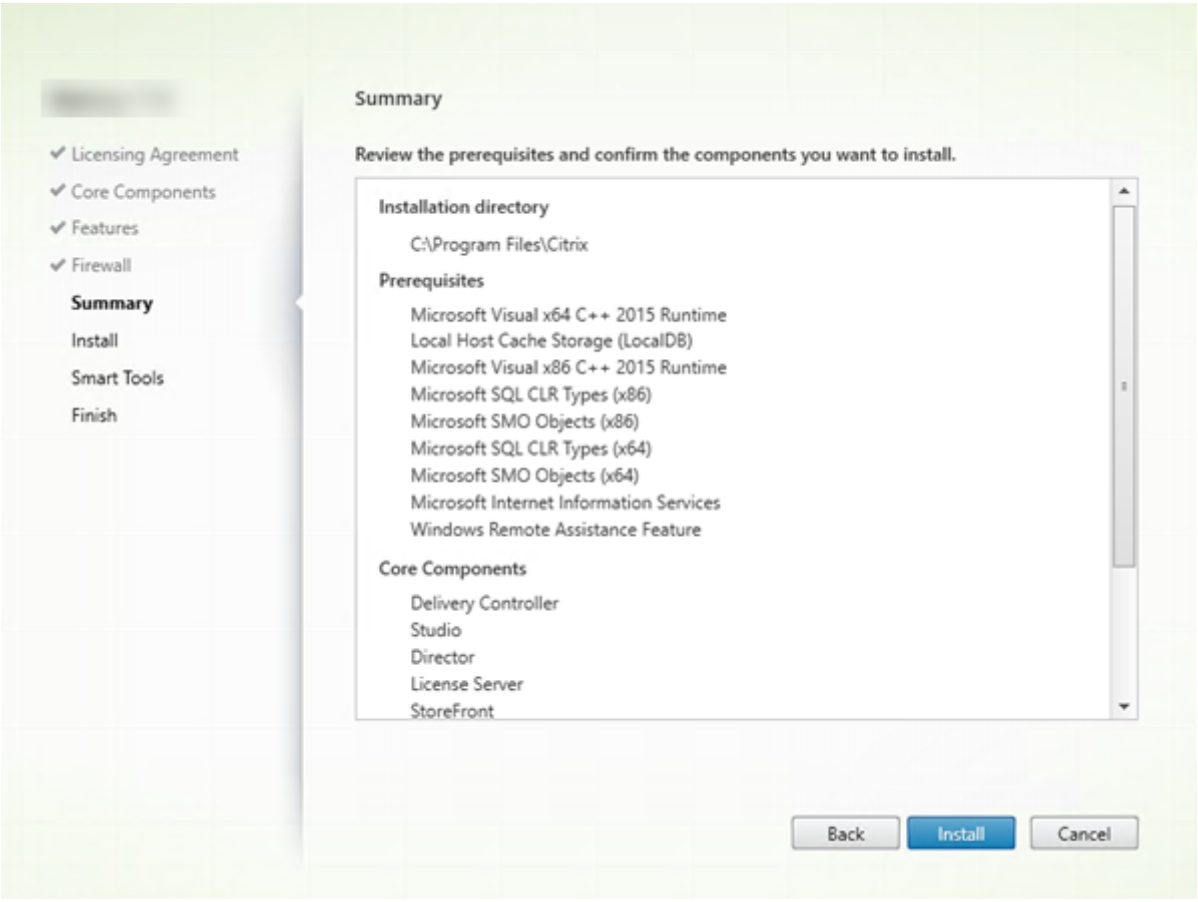
单击下一步。

（图中显示您在此计算机上安装所有核心组件时的端口列表。该类型的安装通常仅用于测试部署。）

命令行选项：`/configure_firewall`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

步骤 **8.** 查看必备条件并确认安装

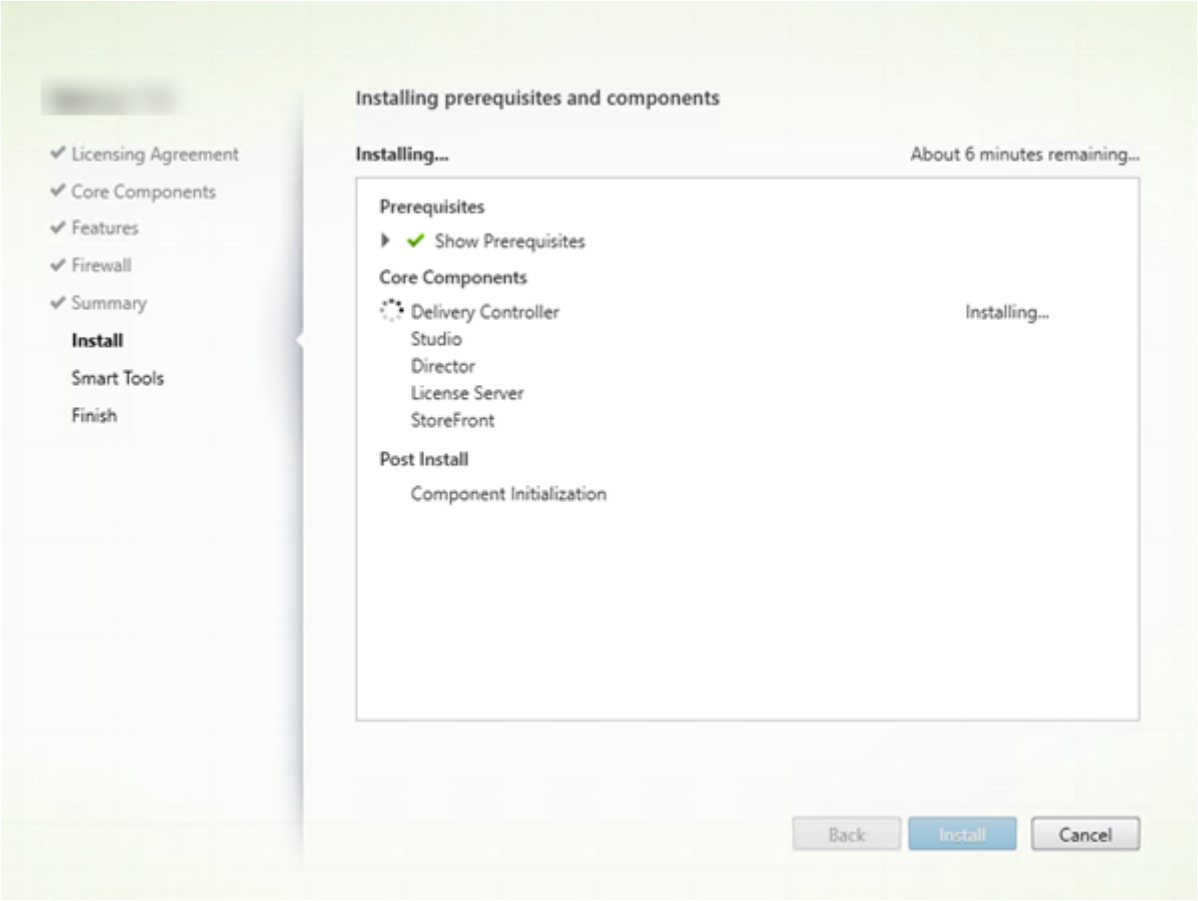


摘要页面上列出将安装的内容。如果需要，可使用返回按钮返回到之前的向导页面并更改选择。

准备好时，单击安装。

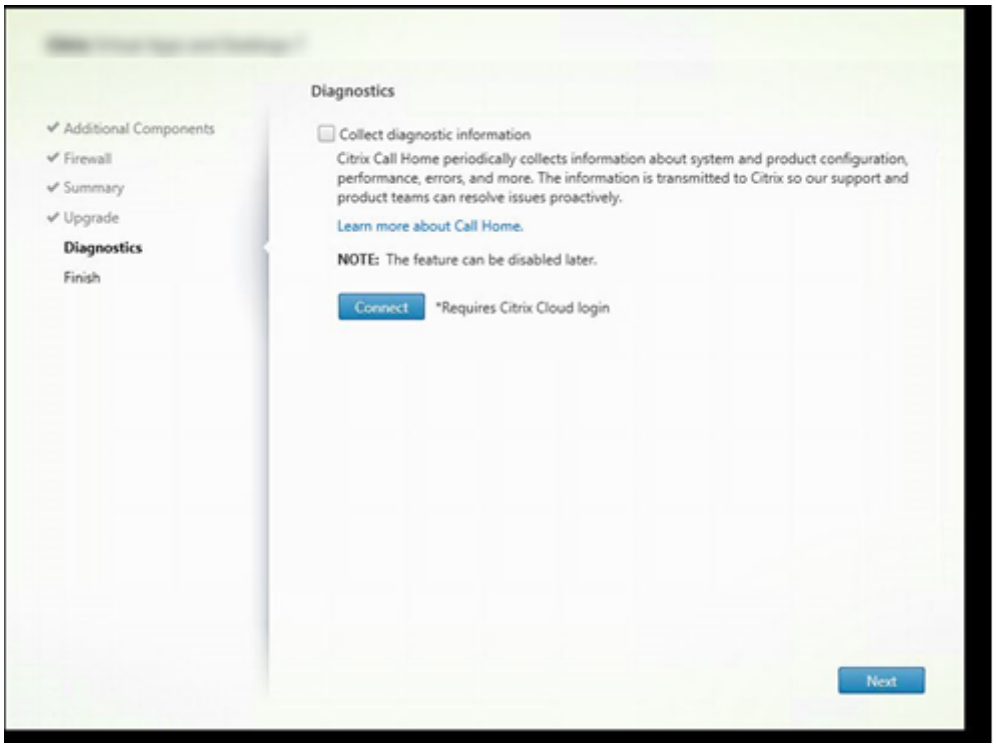
系统将显示安装进度：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

步骤 **9.** 诊断



在诊断页面上，选择是否参与 Citrix Call Home。

使用图形界面安装 Delivery Controller 时，将显示此页面。安装 StoreFront（Controller 除外），向导将显示此页面。如果安装其他核心组件（但不安装 Controller 或 StoreFront），向导将不显示此页面。

在升级过程中，如果已启用 Call Home 或如果安装程序遇到与 Citrix Telemetry Service 有关的错误，则不会显示此页面。

如果您选择参与（默认设置），请单击连接。出现提示时，输入您的 Citrix 帐户凭据。您可以在安装后稍后更改注册选项。

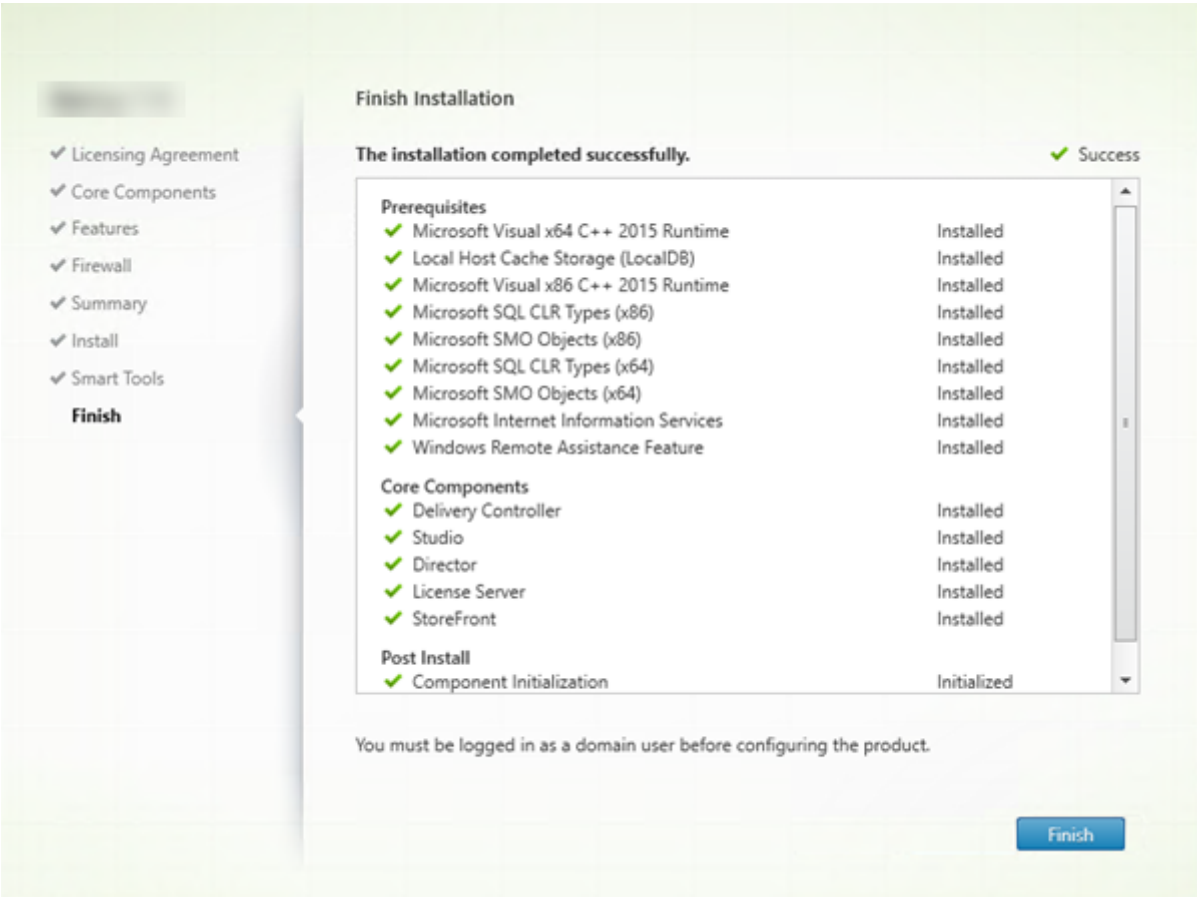
您的凭据通过验证后（或者如果选择不参与），单击下一步。

如果在未先选择收集诊断信息的情况下单击诊断页面上的连接，则在关闭连接到 **Citrix Insight Services** 对话框后，下一步按钮将禁用。您不能移动到下一页。要重新启用下一步按钮，请选择并立即取消选择收集诊断信息。

有关详细信息，请参阅 Call Home。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

步骤 **10.** 完成此安装



完成页面包含带绿色复选标记的所有已成功安装和初始化的必备项和组件。

单击完成。

步骤 **11.** 在其他计算机上安装其余核心组件

如果您在一台计算机上安装了所有核心组件，请继续执行后续步骤。否则，请在其他计算机上运行安装程序以安装其他组件。还可以在其他服务器上安装更多 Controller。

后续步骤

安装了所有必需的组件后，使用 Studio 创建站点。

创建了站点后，安装 VDA。

随时可以使用完整产品安装程序以采用以下组件扩展您的部署：

- 通用打印服务器的服务器组件：在打印服务器上启动安装程序。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. 在扩展部署部分中选择通用打印服务器。
2. 接受许可协议。
3. 在防火墙页面上，默认情况下，如果 Windows 防火墙服务正在运行，那么即使未启用防火墙，也会打开 TCP 端口 7229 和 8080。如果要手动打开这些端口，可以禁用该默认操作。

要通过命令行安装此组件，请参阅用于安装通用打印服务器的命令行选项。

- 联合身份验证服务。
- Session Recording。

安装 VDA

January 21, 2022

> 重要：
>
> 如果要升级，并且您的当前版本安装了 Personal vDisk 或 AppDisk 软件，请参阅删除 PvD、AppDisk 和不受支持的主机。

适用于 Windows 计算机的 VDA 有两种类型：适用于多会话操作系统的 VDA 和适用于单会话操作系统的 VDA。（有关适用于 Linux 计算机的 VDA 的信息，请参阅 Linux Virtual Delivery Agent 文档。）

在开始安装之前，请查看准备安装并完成所有准备任务。

请先安装核心组件，然后再安装 VDA。还可以在安装 VDA 之前创建站点。

本文介绍了安装 VDA 时的安装向导顺序。提供了命令行等效命令。有关详细信息，请参阅使用命令行安装。

步骤 1. 下载产品软件并启动向导

如果您要使用完整产品安装程序：

1. 如果您尚未下载产品 ISO：
   - 使用您的 Citrix 帐户凭据访问 Citrix Virtual Apps and Desktops 下载页面。下载产品 ISO 文件。
   - 解压文件。或者刻录 ISO 文件的 DVD。
2. 在您要安装 VDA 的映像或计算机上使用本地管理员帐户。在驱动器中插入 DVD 或装载 ISO 文件。如果安装程序未自动启动，请双击 **AutoSelect** 应用程序或装载的驱动器。

   此时将启动安装向导。

如果您要使用独立的安装程序：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

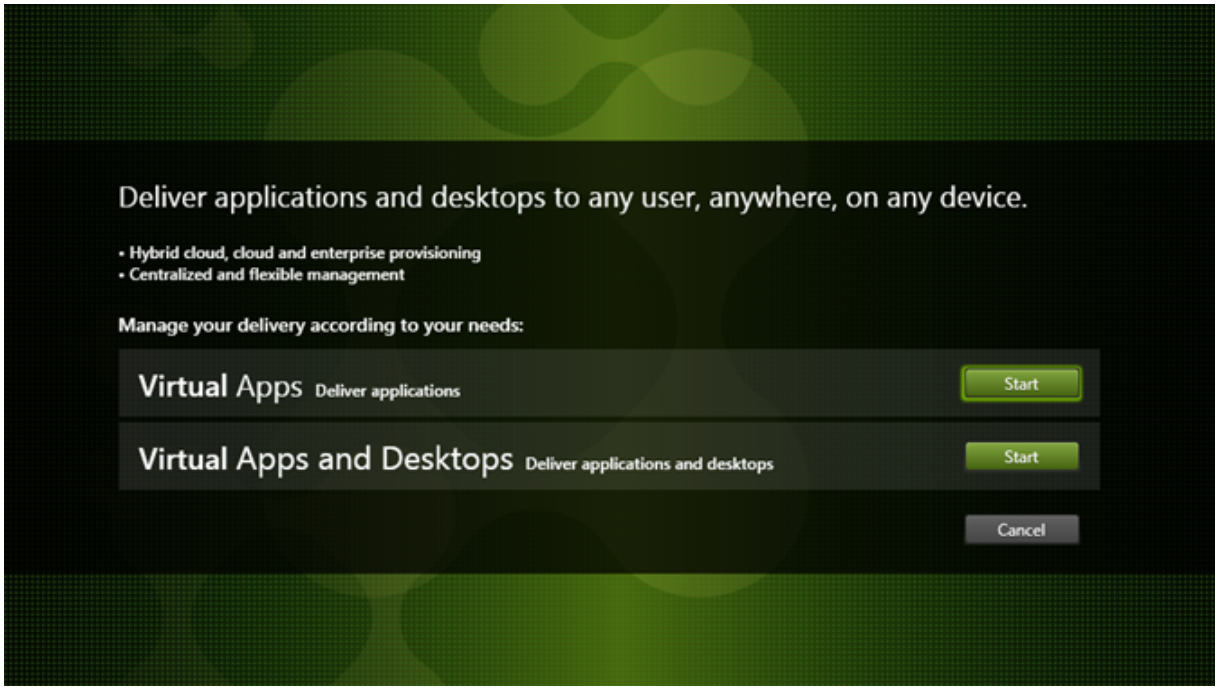
1. 使用您的 Citrix 帐户凭据访问 Citrix Virtual Apps and Desktops 下载页面。下载合适的软件包：

   - `VDAServerSetup.exe`：多会话操作系统 VDA 版本
   - `VDAWorkstationSetup.exe`：单会话操作系统 VDA 版本
   - `VDAWorkstationCoreSetup.exe`：单会话操作系统核心服务 VDA 版本

2. 右键单击软件包，然后选择以管理员身份运行。

   此时将启动安装向导。

步骤 **2.** 选择要安装的产品

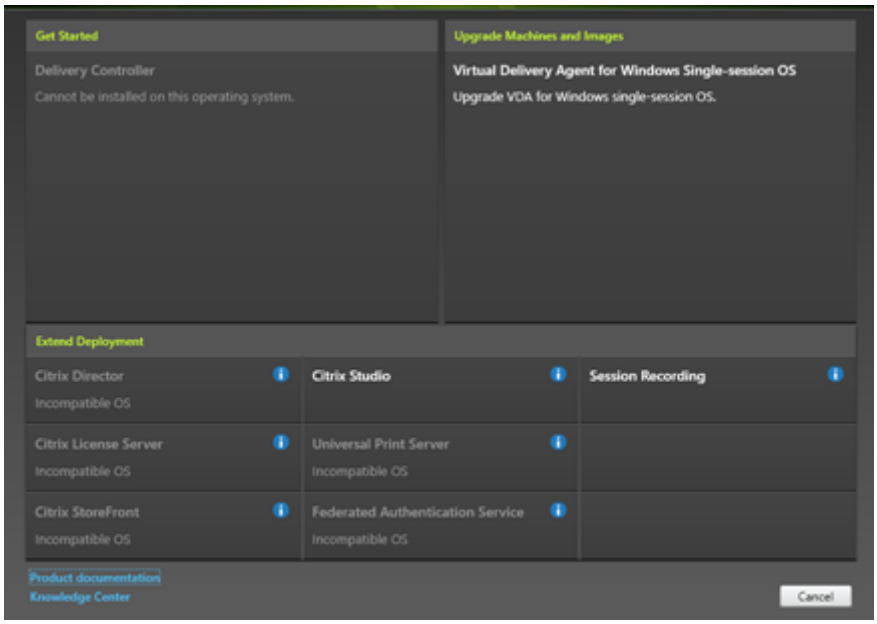


单击产品旁边的开始以安装 Citrix Virtual Apps 或 Citrix Virtual Desktops。（如果计算机上已安装了 Citrix Virtual Apps 或 Citrix Virtual Desktops 组件，不会显示此页面。）

命令行选项 `/xenapp` 用于安装 Citrix Virtual Apps。如果忽略此选项，则安装 Citrix Virtual Desktops。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

步骤 **3.** 选择 **VDA**

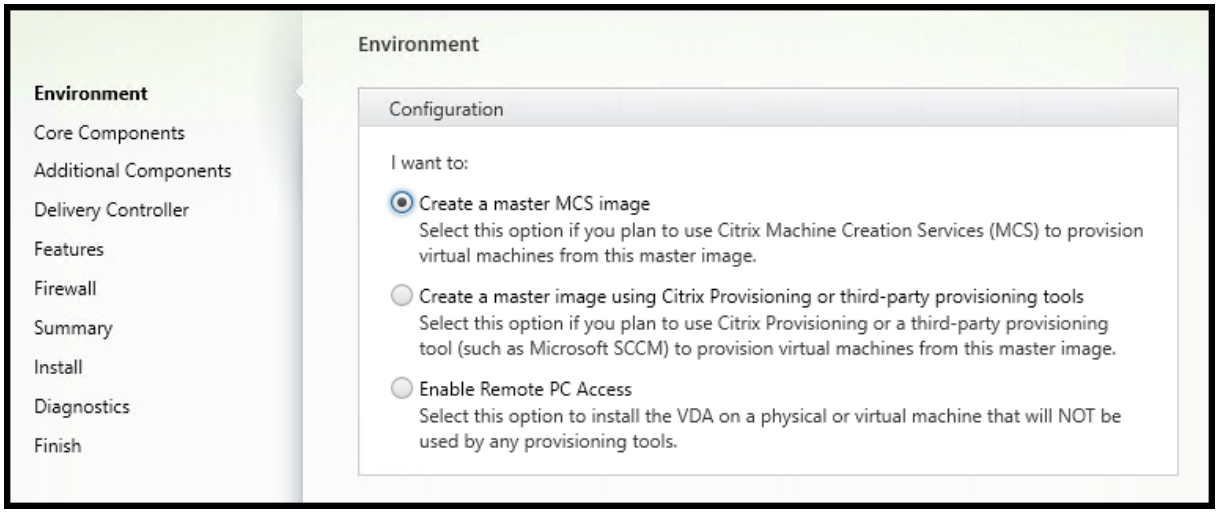


选择 **Virtual Delivery Agent** 条目。安装程序知晓自身是在单会话还是多会话操作系统中运行，因此仅提供恰当的 VDA 类型。

例如，在 Windows Server 2016 计算机上运行安装程序时，会提供适用于多会话操作系统的 VDA 选项。不提供适用于单会话操作系统的 VDA 选项。

如果尝试在此 Citrix Virtual Apps and Desktops 版本不支持的操作系统上安装（或升级到）Windows VDA，则会显示一条消息，指导您浏览关于选项的信息。

步骤 **4.** 指定 **VDA** 的使用方式



在环境页面上，指定您计划如何使用 VDA，以指示是否将此计算机用作映像来预配更多计算机。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

您选择的选项会影响自动安装的 Citrix Provisioning 工具（如果有），以及 VDA 安装程序的其他组件页面上的默认值。

在安装 VDA 时，将自动安装多个 MSI（预配及其他）。阻止其安装的唯一方法是在命令行安装中使用 /exclude 选项。

选择以下方法之一：

- 创建 **MCS** 主映像：如果您计划使用 Machine Creation Services 预配 VM，请选择此选项在 VM 映像上安装 VDA。此选项将安装 Machine Identity Service。这是默认选项。

  命令行选项 /mastermcsimage 或 /masterimage

> 重要：
>
> 安装介质或 ISO 映像必须在本地装载。不支持从网络驱动器挂载 ISO 映像以便安装软件。

- 使用 **Citrix Provisioning** 或第三方预配工具创建主映像：如果您计划使用 Citrix Provisioning 或第三方预配工具（例如 Microsoft System Center Configuration Manager）预配 VM，请选择此选项在 VM 映像上安装 VDA。

  命令行选项：/masterpvsimage

- （仅显示在多会话操作系统计算机上）启用与服务器的中转连接：选择此选项将在将不用作映像来预配其他计算机的物理机或虚拟机上安装 VDA。

  命令行选项：/remotepc

- （仅显示在单会话操作系统计算机上）启用 **Remote PC Access**：选择此选项将在要用于 Remote PC Access 的物理机上安装 VDA。

  命令行选项：/remotepc

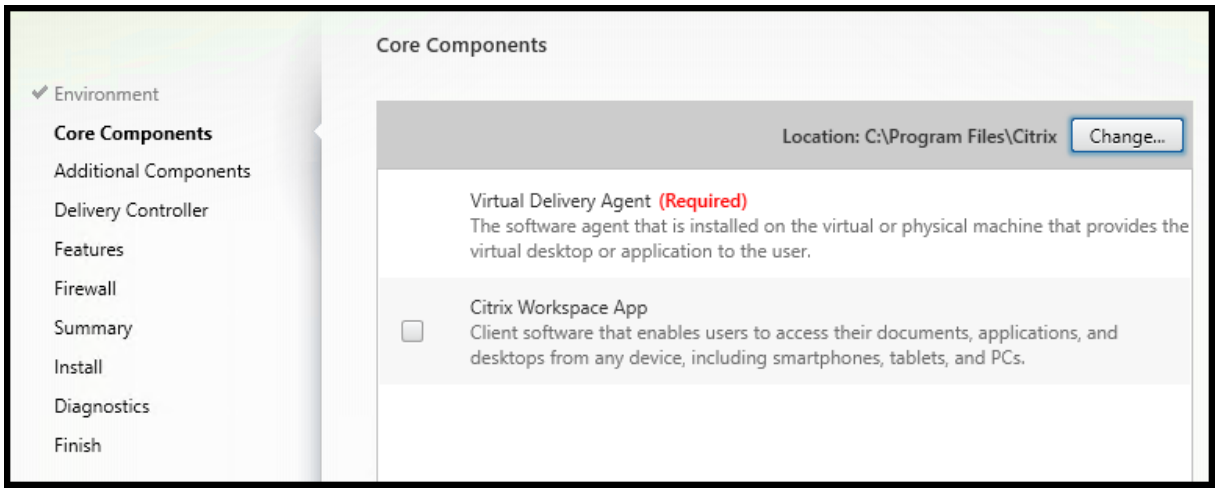
单击下一步。

此页面在以下情况下不显示：

- 如果您升级 VDA
- 如果您使用的是 VDAWorkstationCoreSetup.exe 安装程序

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

步骤 **5.** 选择要安装的组件及安装位置



在核心组件页面上：

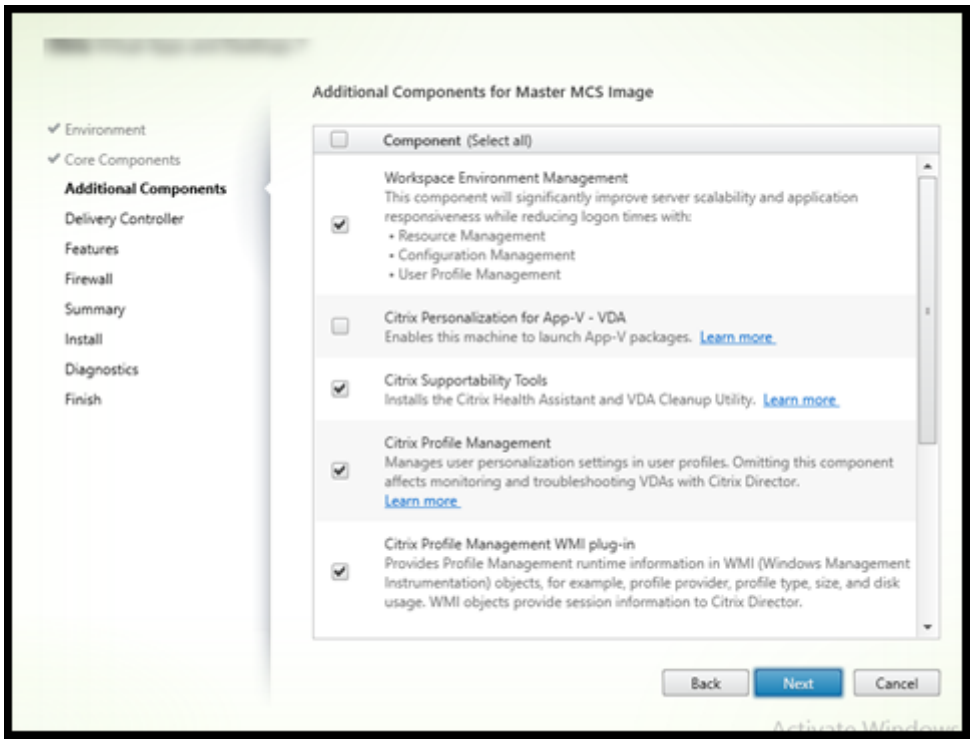
- 位置：默认情况下，组件安装在 `C:\Program Files\Citrix` 中。此默认设置适用于大多数部署。如果您指定一个不同的位置，该位置必须具有网络服务的执行权限。
- 组件：默认情况下，不会随 VDA 安装适用于 Windows 的 Citrix Workspace 应用程序。如果您使用 `VDAWorkstationCoreSetup.exe` 安装程序，则从不安装适用于 Windows 的 Citrix Workspace 应用程序，因此此复选框不显示。

单击下一步。

命令行选项 `/installdir`、`/components vda,plugin` 用于安装 VDA 和适用于 Windows 的 Citrix Workspace 应用程序

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

步骤 **6.** 安装附加组件



附加组件页面包含用于启用或禁用与 VDA 一起安装其他功能和技术的复选框。在命令行安装中，可以使用 `/exclude` 或 `/includeadditional` 选项明确忽略或包含一个或多个可用组件。

下表指出了此页面上各项的默认设置。默认设置取决于您在环境页面上选择的选项。

“附加组件”页面	“环境”页面：选择了“Master image with MCS”（创建 MCS 主映像）或“Master image with Citrix Provisioning”（使用 Citrix Provisioning 或第三方预配工具创建主映像）	“环境”页面：选择了“启用与服务器的中转连接”（适用于多会话操作系统）或“启用 Remote PC Access”（适用于单会话操作系统）
Workspace Environment Management	未选择	未选择
Citrix Personalization for App-V	未选择	未选择
用户个性化层	未选择	不显示，因为它不适用于此用例。
Citrix Supportability Tools	已选择	未选择
Citrix Profile Management	已选择	未选择
Citrix Profile Management WMI 插件	已选择	未选择

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

“附加组件”页面	“环境”页面：选择了“Master image with MCS”（创建 MCS 主映像）或“Master image with Citrix Provisioning”（使用 Citrix Provisioning 或第三方预配工具创建主映像）	“环境”页面：选择了“启用与服务器的中转连接”（适用于多会话操作系统）或“启用 Remote PC Access”（适用于单会话操作系统）
Citrix Files for Windows	未选择	未选择
Citrix Files for Outlook	未选择	未选择
MCSIO write cache for storage optimization（用于存储优化的 MCSIO 写入缓存）	未选择	未选择

此页面在以下情况下不显示：

- 您正在使用 `VDAWorkstationCoreSetup.exe` 安装程序。此外，附加组件的命令行选项对该安装程序无效。
- 您要升级 VDA 并且所有附加组件都已安装。如果已安装部分附加组件，此页面将仅列出未安装的组件。

选中或清除以下复选框：

- **Workspace Environment Management**：如果部署使用 Citrix Workspace Environment Management，请安装此组件。有关详细信息，请参阅 Workspace Environment Management。

  命令行选项 `/includeadditional "Citrix WEM Agent"` 用于启用组件安装，`/exclude "Citrix WEM Agent"` 用于阻止组件安装

- **Citrix Personalization for App-V**：如果使用 Microsoft App-V 包中的应用程序，请安装此组件。有关详细信息，请参阅 App-V。

  命令行选项 `/includeadditional "Citrix Personalization for App-V - VDA "` 用于启用组件安装，`/exclude "Citrix Personalization for App-V - VDA"` 用于阻止组件安装

- **Citrix** 用户个性化层：安装适用于用户个性化层的 MSI。有关详细信息，请参阅用户个性化层。

  仅当在单会话 Windows 10 计算机上安装 VDA 时，此组件才会显示。

  命令行选项 `/includeadditional "User Personalization Layer"` 用于启用组件安装，`/exclude "User Personalization Layer"` 用于阻止组件安装

- **Citrix Supportability Tools**：安装包含 Citrix Supportability Tools（例如 Citrix Health Assistant）的 MSI。

  命令行选项 `/includeadditional "Citrix Supportability Tools"` 用于启用组件安装，`/exclude "Citrix Supportability Tools"` 用于阻止组件安装

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Citrix Profile Management**：此组件用于管理用户配置文件中的用户个性化设置。有关详细信息，请参阅 Profile Management。

  将 Citrix Profile Management 排除在安装之外将影响通过 Citrix Director 对 VDA 执行的监视和故障排除操作。在用户详细信息和端点页面上，个性化面板和登录持续时间面板会出现故障。在控制板和趋势页面上，平均登录持续时间面板仅显示安装了 Profile Management 的计算机的数据。

  即使您使用的是第三方用户配置文件管理解决方案，Citrix 仍建议您安装并运行 Citrix Profile Management Service。不需要启用 Citrix Profile Management Service。

  命令行选项 `/includeadditional "Citrix Profile Management"` 用于启用组件安装，`/exclude "Citrix Profile Management"` 用于阻止组件安装

- **Citrix Profile Management WMI** 插件：此插件在 WMI (Windows Management Instrumentation) 对象中提供 Profile Management 运行时信息（例如，配置文件提供程序、配置文件类型、大小和磁盘使用情况）。WMI 对象向 Director 提供会话信息。

  命令行选项 `/includeadditional "Citrix Profile Management WMI Plugin"` 用于启用组件安装，`/exclude "Citrix Profile Management WMI Plugin"` 用于阻止组件安装

- **Citrix Files for Windows**：用户可以通过此组件连接到其 Citrix Files 帐户。之后，他们可以通过 Windows 文件系统中的一个映射驱动器与 Citrix Files 交互（不需要完全同步其内容）。有关详细信息，请参阅 Content Collaboration。

  命令行选项 `/includeadditional "Citrix Files for Windows"` 用于启用组件安装，`/exclude "Citrix Files for Windows"` 用于阻止组件安装

- **Citrix Files for Outlook**： Citrix Files for Outlook 允许您跳过文件大小限制，并通过 Citrix Files 发送您的附件或电子邮件来增加其安全性。您可以直接在自己的电子邮件中向同事、客户和合作伙伴提供安全的文件上载请求。有关详细信息，请参阅 Content Collaboration。

  命令行选项 `/includeadditional "Citrix Files for Outlook"` 用于启用组件安装，`/exclude "Citrix Files for Outlook"` 用于阻止组件安装

- **MCSIO write cache for storage optimization**（用于存储优化的 MCSIO 写入缓存）：安装 Citrix MCS IO 驱动程序。有关详细信息，请参阅虚拟机管理程序共享的存储和配置临时数据的缓存。

  命令行选项 `/includeadditional "Citrix MCS IODriver"` 用于启用组件安装，`/exclude "Citrix MCS IODriver"` 用于阻止组件安装

步骤 7. Workspace Environment Management

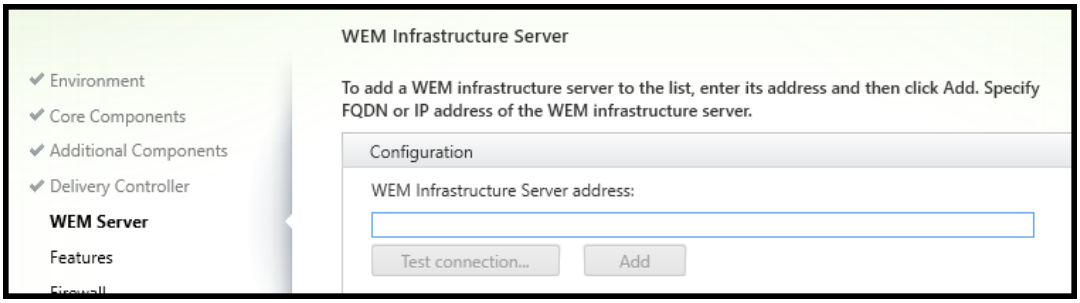
仅当在其他组件页面上启用了相应的复选框时，才显示 **Citrix Workspace Environment Management** (WEM) 页面。

1. 选择是部署 WEM 本地还是 WEM 云（服务）部署。

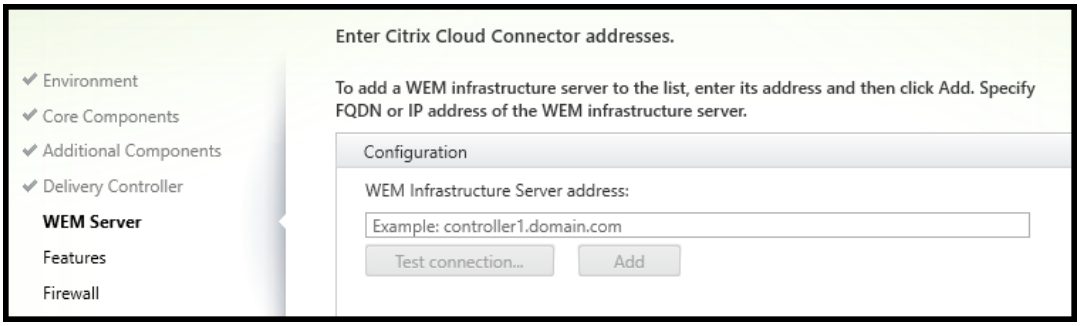
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. 添加 FQDN 或 IP 地址。特殊字符将被忽略。

   - 对于 WEM 本地：WEM 基础结构服务器的地址



   - 对于 WEM 服务：Cloud Connector 的地址



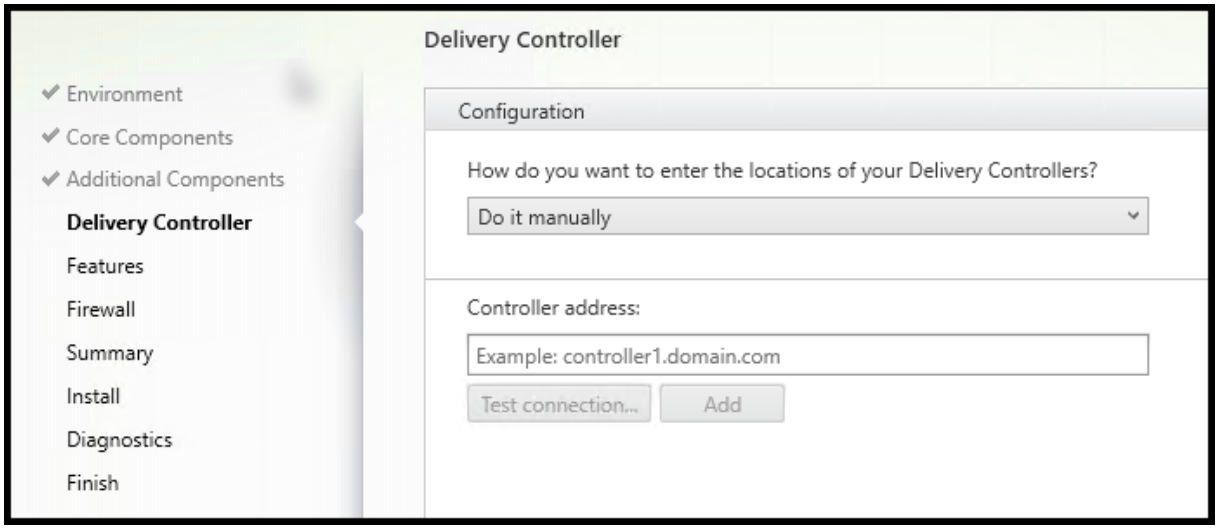
3. 单击测试连接。端口必须在防火墙中打开。
4. 成功进行连接测试后，单击添加。
5. 对于 WEM 服务部署，请为其他 Cloud Connector 重复步骤 2-4。
6. 单击下一步。

命令行选项：`/wem_server`、`/wem_cloud_connectors`

命令行界面中还提供了更多 WEM 代理配置选项。请参阅命令行安装选项。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

步骤 **8. Delivery Controller** 地址



在 **Delivery Controller** 页面上，选择您希望如何输入所安装的 Controller 的地址。Citrix 建议您在安装 VDA 时指定地址（手动操作）。VDA 有了此信息后才能向 Controller 注册。如果 VDA 无法注册，用户无法访问该 VDA 上的应用程序和桌面。

- 手动操作：（默认设置）输入所安装 Controller 的 FQDN，然后单击添加。如果您已安装更多 Controller，请添加其地址。
- 以后 **(**高级**)**：如果选择此选项，向导将要求您确认这是您继续操作之前希望执行的操作。要在以后指定地址，可以重新运行安装程序，或者使用 Citrix 组策略。向导还会在摘要页面上提醒您。
- 从 **Active Directory** 中选择位置：仅当计算机已加入域且用户是域用户时有效。
- 让 **Machine Creation Services** 自动创建：仅当使用 MCS 预配计算机时有效。

单击下一步。如果您选择了以后 **(**高级**)**，系统将提示您确认将在以后指定 Controller 地址。

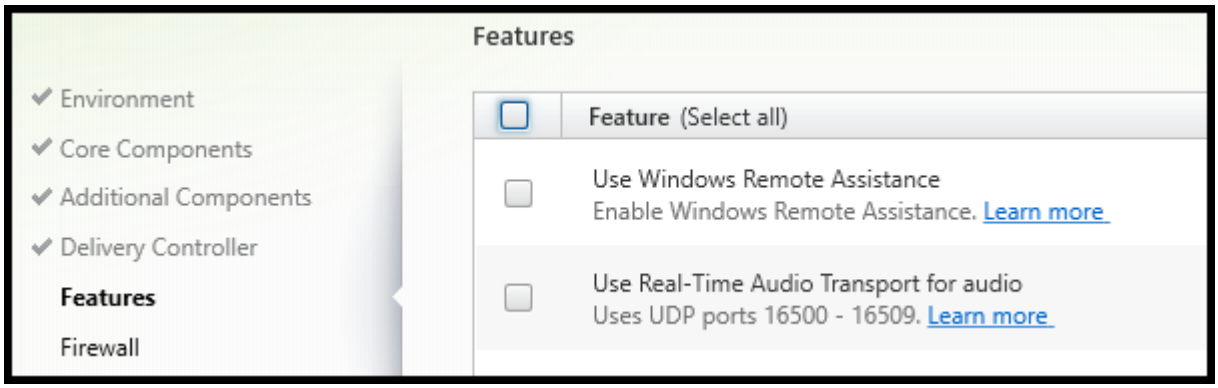
其他注意事项：

- 地址不能包含非字母数字字符。
- 如果在 VDA 安装期间以及在组策略中指定了地址，这些策略设置将覆盖安装过程中提供的设置。
- 需要打开用于与 Controller 进行通信的防火墙端口，才能成功注册 VDA。在向导的防火墙页面上默认启用该操作。
- 在指定 Controller 位置（安装 VDA 期间或之后）之后，可以在添加或删除 Controller 时使用自动更新功能更新 VDA。有关 VDA 如何发现并向 Controller 注册的详细信息，请参阅 VDA 注册。

命令行选项：`/controllers`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

步骤 **9.** 启用或禁用功能



在功能页面上，使用用于启用或禁用要使用的功能的复选框。

- **Use Windows Remote Assistance**（使用 **Windows** 远程协助）：启用此功能后，Windows 远程协助与 Director 的用户重影功能结合使用。Windows 远程协助将在防火墙中打开动态端口。（默认禁用）

  命令行选项：`/enable_remote_assistance`

- 对音频使用实时音频传输：如果在您的网络中广泛使用 VoIP，则启用此功能。该功能可以通过有损网络降低延迟并提高音频恢复能力。它允许使用基于 UDP 的 RTP 传输功能传输音频数据。（默认禁用）

  命令行选项：`/enable_real_time_transport`

如果此页面包含名为 **MCS I/O** 的功能，请勿使用。MCS IO 功能是在附加组件页面上配置的。

单击下一步。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

步骤 **10.** 防火墙端口

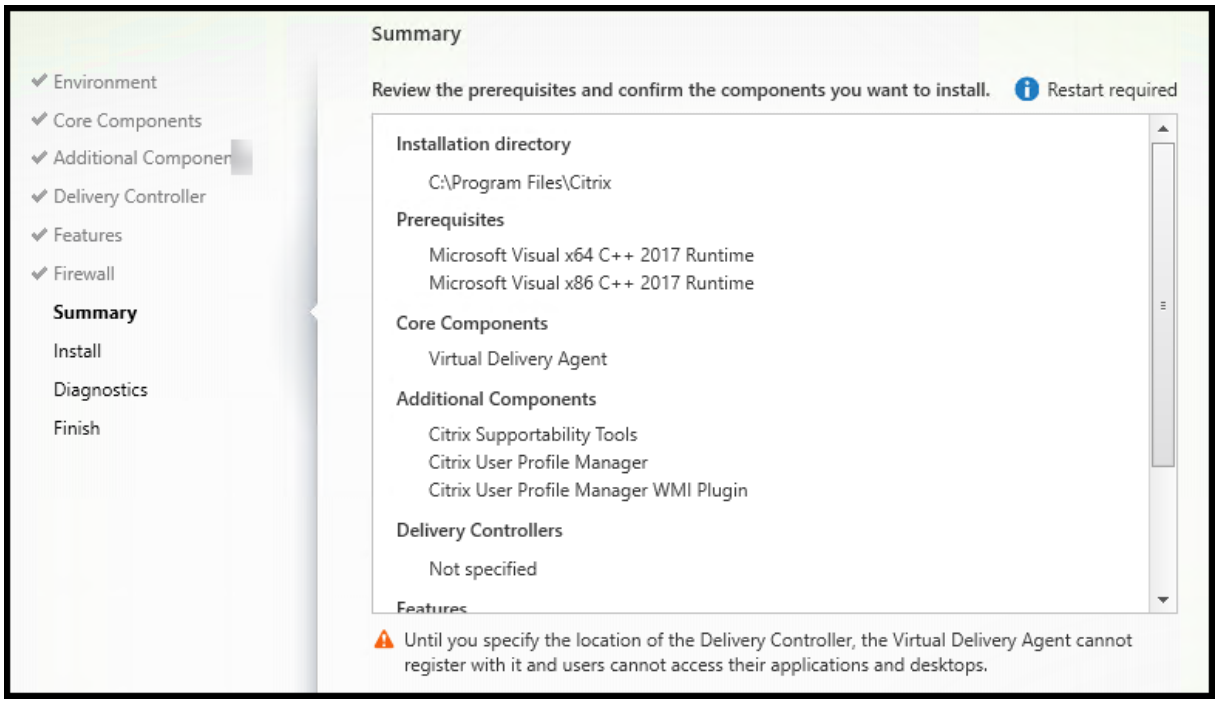
在防火墙页面上，默认情况下，如果 Windows 防火墙服务正在运行，那么即使未启用防火墙，也会自动打开端口。此默认设置适用于大多数部署。有关端口信息，请参阅网络端口。

单击下一步。

命令行选项：`/enable_hdx_ports`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

步骤 **11.** 查看必备条件并确认安装



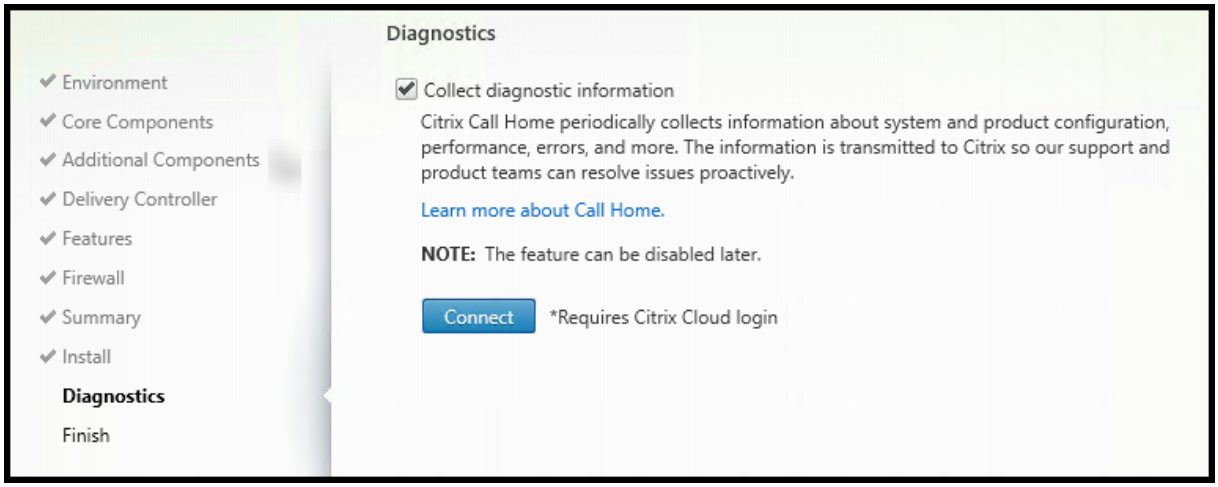
摘要页面上列出将安装的内容。可使用返回按钮返回到之前的向导页面并更改选择。

（仅限单会话 VDA）选中 **Enable automatic restore if update fails**（如果更新失败，则启用自动恢复）复选框以启用失败时还原功能。有关详细信息，请参阅安装或升级失败时还原。

准备好时，单击安装。

如果必备项尚未安装或启用，计算机可能会重新启动一次或多次。请参阅准备安装。

步骤 **12.** 诊断



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

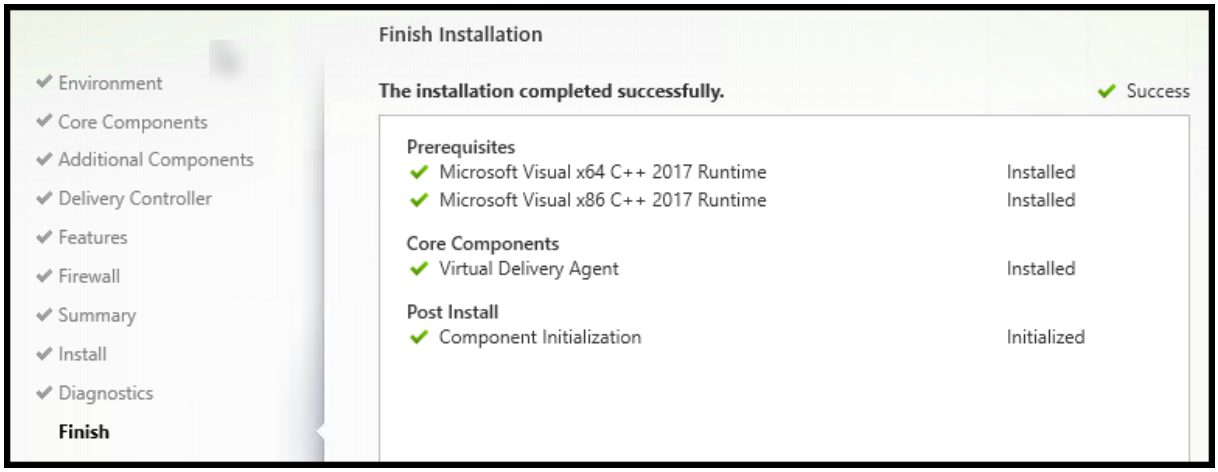
在诊断页面上，选择是否参与 Citrix Call Home。如果您选择参与（默认设置），请单击连接。出现提示时，输入您的 Citrix 帐户凭据。

您的凭据通过验证后（或者如果选择不参与），单击下一步。

使用完整产品安装程序时，如果在未先选择收集诊断信息的情况下单击诊断页面上的连接，则在关闭连接到 **Citrix Insight Services** 对话框后，下一步按钮将禁用。您不能移动到下一页。要重新启用下一步按钮，请选择并立即取消选择收集诊断信息。

有关详细信息，请参阅 Call Home。

步骤 **13.** 完成此安装



完成页面包含带绿色复选标记的所有已成功安装和初始化的必备项和组件。

单击完成。默认情况下，计算机将自动重新启动。尽管您可以禁用此自动重新启动，但在计算机重新启动之前，无法使用 VDA。

后续步骤

重复上述过程在其他计算机或映像上安装 VDA（如果需要）。

安装了所有 VDA 后，启动 Studio。如果您尚未创建站点，Studio 将自动指导您执行该任务。完成后，Studio 将指导您创建计算机目录，然后创建交付组。请参阅：

- 创建站点
- 创建计算机目录
- 创建交付组

Citrix Optimizer

Citrix Optimizer 是适用于 Windows 操作系统的工具，可帮助 Citrix 管理员通过删除和优化各种组件来优化 VDA。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

安装 VDA 并完成最终重新启动后，下载并安装 Citrix Optimizer。请参阅 CTX224676。CTX 文章包含下载软件包以及有关安装和使用 Citrix Optimizer 的说明。

自定义 VDA

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** 或 **Citrix Remote PC Access/VDI Core Services VDA**。然后单击右键并选择更改。
2. 选择自定义 **Virtual Delivery Agent** 设置。安装程序启动时，您可以更改：
   - Controller 地址
   - 向 Controller 注册的 TCP/IP 端口（默认为 80）
   - 是否自动打开 Windows 防火墙端口

故障排除

- 有关 Citrix 如何报告组件安装结果的信息，请参阅 Citrix 安装返回代码。
- 在交付组的 Studio 显示屏幕中，详细信息窗格中的已安装的 **VDA** 版本条目可能不是计算机上安装的版本。计算机的 Windows“程序和功能”将显示实际的 VDA 会话。
- 安装 VDA 后，在向 Delivery Controller 注册之前，无法将应用程序或桌面交付给用户。

  要了解有关 VDA 注册方法以及如何解决注册问题的信息，请参阅 VDA 注册。

使用命令行安装

January 4, 2023

> 重要：
>
> 如果要升级，并且当前版本使用或安装了 Personal vDisk 或 AppDisk 软件，请参阅删除 PvD、应用磁盘和不受支持的主机。

简介

本文适用于在使用 Windows 操作系统的计算机上安装组件。有关适用于 Linux 操作系统的 VDA 的信息，请参阅 Linux Virtual Delivery Agent。

本文介绍如何发出产品安装命令。在开始进行任何安装之前，请查看准备安装。这篇文章提供了可用安装程序的说明。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

要查看命令的执行进度和返回值，您必须是原始管理员或者使用以管理员身份运行。有关详细信息，请参阅 Microsoft 命令文档。

作为对直接使用安装命令的补充，产品 ISO 中提供了示例脚本，用于在 Active Directory 中的计算机上安装、升级或删除 VDA。有关详细信息，请参阅使用脚本安装 VDA。

如果尝试在此 Citrix Virtual Apps and Desktops 版本不支持的 Windows 操作系统版本上安装或升级，则会显示一条消息，指导您参阅与您的选项有关的信息。请参阅早期版本的操作系统。

有关 Citrix 如何报告组件安装结果的信息，请参阅 Citrix 安装返回代码。

使用完整产品安装程序

要访问完整产品安装程序的命令行接口，请执行以下操作：

1. 请从 Citrix 下载产品软件包。需要提供 Citrix 帐户凭据才能访问下载站点。
2. 解压文件。或者刻录 ISO 文件的 DVD。
3. 通过本地管理员帐户，登录要在其中安装组件的服务器。
4. 在驱动器中插入 DVD 或装载 ISO 文件。
5. 从介质上的 `\x64\XenDesktop Setup` 目录中，运行相应的命令。

   要安装核心组件，请执行以下操作：运行 `XenDesktopServerSetup.exe`，并使用安装核心组件的命令行选项中列出的选项。

   要安装 **VDA**，请执行以下操作：运行 `XenDesktopVDASetup.exe`，并使用安装 VDA 的命令行选项中列出的选项。

   要安装 **StoreFront**，请执行以下操作：运行在安装介质上的 `x64 > StoreFront` 文件夹中的 `CitrixStoreFront-x64.exe`。

   要安装通用打印服务器，请执行以下操作：请按照用于安装通用打印服务器的命令行选项中的指导进行操作。

   要安装联合身份验证服务，请执行以下操作： Citrix 建议使用图形界面。

   要安装 **Session Recording**，请执行以下操作：请按照 Sesssion Recording 中的指导进行操作。

用于安装核心组件的命令行选项

使用 `XenDesktopServerSetup.exe` 命令安装核心组件时，以下选项有效。有关选项的更多详细信息，请参阅安装核心组件。

- **/components** *component* [,*component*] …

  要安装或删除的组件的列表（以逗号分隔）。有效值为：

  - `CONTROLLER`: Controller

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - DESKTOPSTUDIO：Studio
  - DESKTOPDIRECTOR：Director
  - LICENSESERVER：Citrix 许可证服务器

  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）。

  （在 2003 之前的版本中，有效值包括 STOREFRONT。对于版本 2003 及更高版本，请使用使用完整产品安装程序中提及的专用 StoreFront 安装命令）。

- **/configure_firewall**

  如果 Windows 防火墙服务正在运行，即使该防火墙并未启用，也会在 Windows 防火墙中打开正在安装的组件使用的所有端口。如果您使用的是第三方防火墙或未使用防火墙，则必须手动打开这些端口。

- **/disableexperiencemetrics**

  防止将安装、升级或删除过程中收集的分析自动上载到 Citrix。

- **/exclude** “*feature*” [,” *feature*”]

  阻止安装一个或多个逗号分隔的功能、服务或技术，其中每项功能、服务或技术两边用直引号引起。有效值为：

  - "Local Host Cache Storage (LocalDB)"：防止安装用于本地主机缓存的数据库。此选项对是否安装 SQL Server Express 以用作站点数据库没有任何影响。

- **/help** 或 **/h**

  显示命令帮助。

- **/ignore_hw_check_failure**

  允许继续安装或升级 Delivery Controller，即使硬件检查失败（例如，由于 RAM 不足）也是如此。有关详细信息，请参阅硬件检查。

- **/ignore_site_test_failure**

  仅在升级 Controller 过程中有效。通常情况下，任何站点测试失败问题都将被忽略，升级继续进行。如果忽略（或者设置为 false），任何站点测试失败都会导致安装程序失败，而不执行升级。默认值：False

  在升级过程中，如果检测到不受支持的 SQL Server 版本，则忽略此选项。有关详细信息，请参阅 SQL Server 版本检查。

- **/installdir *directory***

  用于安装组件的现有空目录。默认为 c:\Program Files\Citrix。

- **/logpath *path***

  日志文件位置。指定的文件夹必须存在。安装程序不会创建它。默认值 = TEMP%\Citrix\XenDesktop Installer

- **/no_remote_assistance**

  仅当安装 Director 时有效。禁用可使用 Windows 远程协助的用户重影功能。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **/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。）

- **/noresume**

  默认情况下，当安装过程中需要计算机重新启动时，安装程序将在重新启动完成后自动继续运行。要覆盖默认值，请指定 /noresume。如果在自动安装过程中必须重新装载介质或者要捕获信息，这将非常有用。

- **/nosql**

  阻止在即将安装 Controller 的服务器上安装 Microsoft SQL Server Express。如果忽略此选项，将安装 SQL Server Express 以用作站点数据库。

  此选项对安装用于本地主机缓存的 SQL Server Express LocalDB 没有任何影响。

- **/quiet** 或 **/passive**

  安装过程中不显示任何用户界面。而只能在 Windows 任务管理器中找到安装过程的证据。如果忽略此选项，将启动图形界面。

- **/remove**

  删除通过 /components 选项指定的核心组件。

- **/removeall**

  删除已安装的所有核心组件。

- **/sendexperiencemetrics**

  将安装、升级或删除过程中收集的分析自动发送到 Citrix。如果忽略此选项（或指定了 /disableexperiencemetrics），分析会在本地收集，但不会自动发送。

- **/tempdir** *directory*

  安装过程中用于保存临时文件的目录。默认路径为：c:\Windows\Temp。

- **/xenapp**

  安装 Citrix Virtual Apps。如果忽略此选项，则安装 Citrix Virtual Apps and Desktops。

核心组件安装示例

以下命令将在服务器上安装 Delivery Controller、Studio、Citrix Licensing 和 SQL Server Express。组件通信所需的防火墙端口会自动打开。

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

以下命令将在服务器上安装 Citrix Virtual Apps Controller、Studio 和 SQL Server Express。组件通信所需的防火墙端口会自动打开。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

使用独立的 **VDA** 安装程序

需要提供 Citrix 帐户凭据才能访问下载站点。必须在开始安装之前提升管理权限，或使用以管理员身份运行。

1. 从 Citrix 下载合适的软件包：

   - 多会话操作系统 Virtual Delivery Agent：`VDAServerSetup.exe`
   - 单会话操作系统 Virtual Delivery Agent：`VDAWorkstationSetup.exe`
   - 单会话操作系统核心服务 Virtual Delivery Agent：`VDAWorkstationCoreSetup.exe`

2. 首先将软件包中的文件提取到一个现有目录，然后运行安装命令，或者只需运行该软件包。

   要在安装之前提取文件，请使用 `/extract` 和绝对路径，例如 `.\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`。该目录必须存在。否则，提取将失败。然后在单独的命令中，使用本文中列出的有效选项运行相应的命令。

   - 对于 `VDAServerSetup_XXXX.exe`，请运行 `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`
   - 对于 `VDAWorkstationCoreSetup_XXXX.exe`，请运行 `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe`
   - 对于 `VDAWorkstationSetup_XXXX.exe`，请运行 `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`

   要运行下载的软件包，请运行其名称：`VDAServerSetup.exe`、`VDAWorkstationSetup.exe` 或 `VDAWorkstationCoreSetup.exe`。请使用本文中列出的有效选项。

如果您熟悉完整产品安装程序：

- 请运行独立的 `VDAServerSetup.exe` 或 `VDAWorkstationSetup.exe` 安装程序，就像它是 `XenDesktopVdaSetup.exe` 命令一样，除了名称不同。
- `VDAWorkstationCoreSetup.exe` 安装程序不同，因为它支持可用于其他安装程序的一部分选项。

用于安装 **VDA** 的命令行选项

以下选项在以下一个或多个命令(安装程序)中有效：`XenDesktopVDASetup.exe`、`VDAWorkstationSetup.exe` 和 `VDAWorkstationCoreSetup.exe`。

有关选项的更多详细信息，请参阅安装 VDA。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **/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`：Virtual Delivery Agent
  - `PLUGINS`：适用于 Windows 的 Citrix Workspace 应用程序

  要安装 VDA 和适用于 Windows 的 Citrix Workspace 应用程序，请指定 `/components vda,plugins`。

  如果忽略此选项，将仅安装 VDA（不安装 Citrix Workspace 应用程序）。

  此选项在使用 `VDAWorkstationCoreSetup.exe` 安装程序时无效。该安装程序不能安装 Citrix Workspace 应用程序。

- **/controllers** "*controller* [*controller*]"

  可与 VDA 通信的 Controller 的 FQDN，以空格分隔并用直引号括起来。请勿同时指定 `/site_guid` 和 `/controllers` 选项。

- **/disableexperiencemetrics**

  防止将安装、升级或删除过程中收集的分析自动上载到 Citrix。

- **/enable_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 VDA 和启用的功能（Windows 远程协助除外）所需的端口。如果使用其他防火墙或未使用防火墙，则必须手动配置防火墙。有关端口信息，请参阅网络端口。

  要打开 HDX 自适应传输功能使用的 UDP 端口，除 `/enable_hdx_ports` 选项外，还请指定此 `/enable_hdx_udp_ports` 选项。

- **/enable_hdx_udp_ports**

  如果检测到 Windows 防火墙服务，即使未启用防火墙，也请在 Windows 防火墙中打开 HDX 自适应传输功能使用的 UDP 端口。如果使用其他防火墙或未使用防火墙，则必须手动配置防火墙。有关端口信息，请参阅网络端口。

  要打开 VDA 使用的附加端口，除 `/enable_hdx_udp_ports` 选项外，还请指定此 `/enable_hdx_ports` 选项。

- **/enable_real_time_transport**

  为音频数据包（实时音频传输）启用或禁用 UDP。启用该功能可提高音频性能。如果希望在检测到 Windows 防火墙服务时自动打开 UDP 端口，请包含 `/enable_hdx_ports` 选项。

- **/enable_remote_assistance**

  在 Windows 远程协助中启用重影功能以与 Director 结合使用。如果指定此选项，Windows 远程协助将在防火墙中打开动态端口。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **/enablerestore** 或 **/enablerestorecleanup**

  （仅对单会话 VDA 有效）启用在 VDA 安装或升级失败时自动返回到还原点。

  如果安装/升级成功完成：

  - `/enablerestorecleanup` 指示安装程序删除还原点。
  - `/enablerestore` 指示安装程序保留还原点，即使未使用亦如此。

  有关详细信息，请参阅安装或升级失败时还原。

- **/exclude** “*component*”[,”*component*”]

  阻止安装一个或多个逗号分隔的可选组件，其中每个组件两边用直引号引起。例如，在不受 MCS 管理的映像上安装或升级 VDA 不需要 Machine Identity Service 组件。有效值为：

  ```
  - Machine Identity Service
  - Citrix Profile Management
  - Citrix Profile Management WMI Plugin
  - Citrix Universal Print Client
  - Citrix Telemetry Service
  - Citrix Personalization for App-V - VDA
  - Citrix Supportability Tools
  - Citrix Files for Windows
  - Citrix Files for Outlook
  - User personalization layer
  - Citrix WEM Agent
  - Citrix MCS IODriver
  ```

  将 Citrix Profile Management 排除在安装 (`/exclude "Citrix Profile Management"`) 之外将影响通过 Citrix Director 对 VDA 执行的监视和故障排除操作。在用户详细信息和端点页面上，“个性化”面板和“登录持续时间”面板会出现故障。在控制板和趋势页面上，“平均登录持续时间”面板仅显示安装了 Profile Management 的计算机的数据。

  即使您使用的是第三方用户配置文件管理解决方案，Citrix 仍建议您安装并运行 Citrix Profile Management Service。不需要启用 Citrix Profile Management Service。

  如果您同时指定 `/exclude` 和 `/includeadditional` 与相同的组件名称，则不安装该组件。

  此选项在使用 `VDAWorkstationCoreSetup.exe` 安装程序时无效。该安装程序会自动排除这些项目中的很多项。

- **/h** 或 **/help**

  显示命令帮助。

- **/includeadditional** “*component*”[,”*component*”]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

包括安装一个或多个逗号分隔的可选组件，其中每个组件两边用直引号引起。创建 Remote PC Access 部署并要安装默认情况下不包含的其他组件时，此选项很有用。有效值为：

```
- Citrix Profile Management
- Citrix Profile Management WMI Plugin
- Citrix Universal Print Client
- Citrix Telemetry Service
- Citrix Personalization for App-V - VDA
- Citrix Supportability Tools
- Citrix Files for Windows
- Citrix Files for Outlook
- User personalization layer
- Citrix WEM Agent
- Citrix MCS IODriver
```

如果您同时指定 /exclude 和 /includeadditional 与相同的组件名称，则不安装该组件。

- **/installdir** *directory*

  用于安装组件的现有空目录。默认为 c:\Program Files\Citrix。

- **/install_mcsio_driver**

  请勿使用。改为使用 /includeadditional "Citrix MCS IODriver" 或 /exclude Citrix MCS IODriver"

- **/logpath** *path*

  日志文件位置。指定的文件夹必须存在。安装程序不会创建它。默认路径为%TEMP%\Citrix\XenDesktop Installer

  此选项在图形界面中不可用。

- **/masterimage**

  仅当在 VM 上安装 VDA 时有效。将 VDA 设置为用于创建其他计算机的映像。此选项相当于 /mastermcsimage。

  此选项在使用 VDAWorkstationCoreSetup.exe 安装程序时无效。

- **/mastermcsimage**

  指定此计算机将与 Machine Creation Services 一起用作映像。此选项相当于 /masterimage。

- **/masterpvsimage**

  指定此计算机将用作映像与 Citrix Provisioning 或第三方预配工具（例如 Microsoft System Center Configuration Manager）一起预配 VM。

- **/no_mediafoundation_ack**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

确认不安装 Microsoft 媒体基础，并且多项 HDX 多媒体功能将不安装并且无法运行。如果忽略此操作，并且不安装媒体基础，VDA 安装将失败。大多数受支持的 Windows 版本都已附带安装 Microsoft 媒体基础，但 N 版本例外。

- **/nodesktopexperience**

  增强的桌面体验功能不再可用。此选项（和策略设置）将被忽略（如果已指定）。

  仅在安装适用于多会话操作系统的 VDA 时有效。阻止启用增强的桌面体验功能。此功能还受增强的桌面体验 Citrix 策略设置的控制。

- **/noreboot**

  防止在安装完成后重新启动。重新启动后，才能使用 VDA。

- **/noresume**

  默认情况下，当安装过程中需要计算机重新启动时，安装程序将在重新启动完成后自动继续运行。要覆盖默认值，请指定 /noresume。如果在自动安装过程中必须重新装载介质或者要捕获信息，这将非常有用。

- **/portnumber** *port*

  仅当指定 /reconfig选项时有效。用于在 VDA 和 Controller 之间进行通信的端口号。先前配置的端口如果不是 80，则会被禁用。

- **/quiet** 或 **/passive**

  安装过程中不显示任何用户界面。只能在 Windows 任务管理器中找到安装和配置过程的证据。如果忽略此选项，将启动图形界面。

- **/reconfigure**

  与 /portnumber、/controllers 或 /enable_hdx_ports 选项结合使用时，自定义先前配置的 VDA 设置。如果指定此选项时未指定 /quiet 选项，将启动用于自定义 VDA 的图形界面。

- **/remotepc**

  仅适用于 Remote PC Access 部署（单会话操作系统）或中转连接（多会话操作系统）。不在单会话操作系统中安装以下组件：

  - Citrix Personalization for App-V
  - Citrix Profile Management
  - Citrix Profile Management WMI 插件
  - Machine Identity Service
  - Citrix Supportability Tools
  - Citrix Files for Windows
  - Citrix Files for Outlook
  - 用户个性化层
  - Citrix WEM 代理
  - Citrix MCS IO write cache for storage optimization（用于存储优化的 Citrix MCS IO 写入缓存）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

此选项在使用 VDAWorkstationCoreSetup.exe 安装程序时无效。该安装程序会自动排除这些组件的安装。

- **/remove**

  删除通过 /components 选项指定的组件。

- **/remove_appdisk_ack**

  授权 VDA 安装程序卸载 AppDisk VDA 插件（如果已安装）。

- **/remove_pvd_ack**

  授权 VDA 安装程序卸载 Personal vDisk（如果已安装）。

- **/removeall**

  删除 VDA。它不会删除 Citrix Workspace 应用程序（如果已安装）。

- **/sendexperiencemetrics**

  将安装、升级或删除过程中收集的分析自动发送到 Citrix。如果忽略此选项（或指定了 /disableexperiencemetrics 选项），分析会在本地收集，但不会自动发送。

- **/servervdi**

  在受支持的 Windows 多会话计算机上安装适用于单会话操作系统的 VDA。在 Windows 多会话计算机上安装适用于多会话操作系统的 VDA 时，请忽略此选项。

  使用此选项前，请参阅服务器 VDI。

  此选项仅用于完整产品 VDA 安装程序。

- **/site_guid** *guid*

  站点 Active Directory 组织单位 (OU) 的全局唯一标识符。使用 Active Directory 进行发现时，该标识符可将虚拟桌面与站点相关联（建议和默认的发现方法为自动更新）。站点 GUID 是 Studio 中显示的站点属性。请勿同时指定 /site_guid 和 /controllers 选项。

- **/tempdir** *directory*

  安装过程中用于保存临时文件的目录。默认路径为：c:\Windows\Temp。

  此选项在图形界面中不可用。

- **/virtualmachine**

  仅当在 VM 上安装 VDA 时有效。通过物理机的安装程序覆盖检测功能，在安装程序中，传递给 VM 的 BIOS 信息将其显示为物理机。

  此选项在图形界面中不可用。

- **/wem_add_firewall_rules**

  添加 WEM 代理防火墙规则。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **/wem_agent_cache_location**

  备用 WEM 代理缓存位置。

- **/wem_agent_port**

  WEM 代理用于与 WEM 基础结构服务器进行通信的端口。

- **/wem_cached_data_sync_port**

  WEM 代理用于将缓存与 WEM 基础结构服务器同步的端口。

- **/wem_cloud_connectors**

  包含 WEM 部署的资源位置中以逗号分隔的 Citrix Cloud Connector 列表。

- **/wem_server**

  WEM 基础结构服务器的 FQDN 或 IP 地址。

VDA 安装示例

使用完整产品安装程序安装 **VDA**:

以下命令将在 VM 上的默认位置安装适用于单会话操作系统的 VDA 和 Citrix Workspace 应用程序。此 VDA 将用作映像，并使用 MCS 预配 VM。VDA 最初与 Controller 一起在 `mydomain` 域中名为 `Contr-Main` 的服务器上注册。VDA 将使用用户个性化层和 Windows 远程协助。

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda
,plugins /controllers "Contr-Main.mydomain.local"/enable_hdx_ports
 /includeadditional "user personalization layer"/mastermcsimage /
enable_remote_assistance
```

使用 **VDAWorkstationCoreSetup** 独立安装程序安装单会话操作系统 **VDA**:

以下命令在单会话操作系统上安装核心服务 VDA，以用于 Remote PC Access 或 VDI 部署。不安装 Citrix Workspace 应用程序和其他非核心服务。将会指定 Controller 的地址，且 Windows 防火墙服务中的端口将自动打开。管理员将处理重新启动。

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.
com"/enable_hdx_ports /noreboot
```

自定义 VDA

安装 VDA 后，可以自定义多项设置。从产品介质上的 `\x64\XenDesktop Setup` 目录，使用用于安装 VDA 的命令行选项中介绍的下列一个或多个选项，运行 `XenDesktopVdaSetup.exe` 命令。

- `/reconfigure`（自定义 VDA 时需要）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- /h 或 /help
- /quiet
- /noreboot
- /controllers
- /portnumber port
- /enable_hdx_ports

VDA 故障排除

- 在交付组的 Studio 显示屏幕中，详细信息窗格中的已安装的 **VDA** 版本条目可能不是计算机上安装的版本。计算机的 Windows“程序和功能”将显示实际的 VDA 会话。
- 安装 VDA 后，在向 Delivery Controller 注册之前，无法将应用程序或桌面交付给用户。

  要了解有关 VDA 注册方法以及如何解决注册问题的信息，请参阅 VDA 注册。

用于安装通用打印服务器的命令行选项

以下选项对 XenDesktopPrintServerSetup.exe 命令有效。

- **/enable_upsserver_port**

软件	文件夹	文件名
Microsoft Visual C++ 2017 Runtime（32 位和 64 位）	支持 **> VcRedist_2017**	vcredist_x64.exe 和vcredist_x86.exe
Citrix 诊断工具	x64 > 虚拟桌面组件	cdf_x64.msi
“通用打印服务器”服务器组件	x64 > 通用打印服务器	UpsServer_x64.msi

如果未指定此选项，安装程序将从图形界面显示防火墙页面。选择自动让安装程序自动添加 Windows 防火墙规则，或者选择手动让管理员手动配置防火墙。

在打印服务器上安装该软件后，请按照预配打印机中的指导配置通用打印服务器。

更多信息

有关 Citrix 如何报告组件安装结果的信息，请参阅 Citrix 安装返回代码。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用脚本安装 VDA

May 19, 2023

> 注意：
>
> Citrix 对针对客户生产环境进行调整的脚本导致出现的问题概不负责。对于任何与安装相关的 Citrix 问题，请使用 Citrix 支持门户开立包含相关安装日志的技术支持案例。

本文适用于在使用 Windows 操作系统的计算机上安装 VDA。有关适用于 Linux 操作系统的 VDA 的信息，请参阅 Linux Virtual Delivery Agent 文档。

安装介质中包含用于在 Active Directory 中安装、升级或删除计算机的 Virtual Delivery Agent (VDA) 的示例脚本。也可以使用脚本来维护 Machine Creation Services 和 Citrix Provisioning（以前称为 Provisioning Services）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。在完整产品 ISO 中，安装命令是 `XenDesktopVdaSetup.exe`，在独立安装程序中，安装命令是 `VDAWorkstationSetup.exe` 或 `VDAServerSetup.exe`。
- 日志记录详细信息存储在本地计算机上。要集中记录结果以供查看和分析，脚本需要对相应网络共享拥有“所有人读/写”访问权限。

要检查运行脚本的结果，请查看中央日志共享。捕获的日志包括脚本日志、安装程序日志及 MSI 安装日志。每次的安装或删除尝试都记录在带时间戳的文件夹中。文件夹标题通过前缀 PASS 或 FAIL 来指示操作结果。您可以使用标准目录搜索工具在中央日志共享中查找失败的安装或删除。这些工具提供了在目标计算机上进行本地搜索的替代方法。

开始执行任何安装之前，请阅读并完成准备安装中的任务。

使用脚本安装或升级 VDA

1. 从安装介质上的 \Support\AdDeploy\ 获取示例脚本 **InstallVDA.bat**。Citrix 建议您先备份原始脚本，再对其进行自定义。
2. 编辑脚本：
   - 指定要安装的 VDA 版本：`SET DESIREDVERSION`。例如，版本 7 可以指定为 7.0。可以在安装介质上的 ProductVersion.txt 文件中找到完整值。但是，无需完全匹配。
   - 指定要在其中调用安装程序的网络共享。指向布局的根目录（树结构的最高点）。脚本运行时会自动调用相应的安装程序版本 (32 位或 64 位)。例如：`SET DEPLOYSHARE=\\fileserver1\share1`。
   - 也可以指定用于存储集中式日志的网络共享位置。例如：`SET LOGSHARE=\\fileserver1\log1`)。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 按照使用命令行安装中的说明指定 VDA 配置选项。默认情况下，脚本中包含 /quiet 和 /noreboot 选项，并且需要这些选项：SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT。

3. 通过组策略启动脚本，将脚本分配给包含您的计算机的 OU。此 OU 应仅包含要安装 VDA 的计算机。重新启动 OU 中的计算机后，脚本在所有这些计算机上运行。VDA 安装在具有支持的操作系统的每台计算机上。

使用脚本删除 **VDA**

1. 从安装介质上的 \Support\AdDeploy\ 获取示例脚本 UninstallVDA.bat。Citrix 建议您先备份原始脚本，再对其进行自定义。
2. 编辑脚本。
   - 指定要删除的 VDA 版本：SET CHECK_VDA_VERSION。例如，版本 7 可以指定为 7.0。可以在安装介质上的 ProductVersion.txt 文件中找到完整值（例如 7.0.0.3018）。但是，无需完全匹配。
   - 也可以指定用于存储集中式日志的网络共享位置。
3. 通过组策略启动脚本，将脚本分配给包含您的计算机的 OU。此 OU 应仅包含要删除 VDA 的计算机。重新启动 OU 中的计算机后，脚本在所有这些计算机上运行。将从每台计算机中删除 VDA。

故障排除

- 脚本将生成说明脚本执行进度的内部日志文件。在开始部署的几秒内，脚本会将 Kickoff_VDA_Startup_Script 日志复制到中央日志共享。您可以确认整个过程正在运行。如果此日志未按预期复制到中央日志共享，请通过检查本地计算机进一步执行故障排除。脚本将两个调试日志文件放在每台计算机上的 %temp% 文件夹中：
  - Kickoff_VDA_Startup_Script_<DateTimeStamp>.log
  - VDA_Install_ProcessLog_<DateTimeStamp>.log

  查看这些日志以确保该脚本：
  - 按预期运行。
  - 正确检测目标操作系统。
  - 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。
- 有关 Citrix 如何报告组件安装结果的信息，请参阅 Citrix 安装返回代码。
- 在交付组的 Studio 显示屏幕中，详细信息窗格中的已安装的 **VDA** 版本条目可能不是计算机上安装的版本。计算机的“程序和功能”将显示实际的 VDA 会话。
- 安装 VDA 后，在向 Delivery Controller 注册之前，无法将应用程序或桌面交付给用户。

  要了解有关 VDA 注册方法以及如何解决注册问题的信息，请参阅 VDA 注册。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用 SCCM 安装 VDA

May 19, 2023

> 注意：
>
> Citrix 对使用适用于客户生产环境的 Microsoft System Center Configuration Manager (SCCM) 等软件分发工具部署 Virtual Delivery Agent (VDA) 导致出现的问题不承担任何责任。对于任何与安装相关的 Citrix 问题，请使用 Citrix 支持门户开立包含相关安装日志的技术支持案例。

概述

VDA 安装分为两个阶段：

- 安装必备项
- 安装 VDA

要使用 Microsoft System Center Configuration Manager (SCCM) 或类似的软件分发工具成功部署 VDA，Citrix 建议您分别处理这些阶段。换句话说，我们建议您首先使用必备项的安装程序安装必备项，然后使用 VDA 安装程序安装 VDA，而非使用 VDA 安装程序同时安装必备项和 VDA。

确定要求和任务序列

必须先在计算机上安装必备项，才能安装 VDA。VDA 必备项因 VDA 版本而异。有关指导，请参阅要安装的 VDA 版本的系统要求：

- Citrix Virtual Apps and Desktops 当前版本
- Citrix Virtual Apps and Desktops 1912 LTSR
- XenApp 和 XenDesktop 7.15 LTSR

同样，安装这些必备项的需求可能因环境而异（例如，取决于目标计算机的操作系统以及计算机已安装的必备项）。在创建脚本或任务序列之前，了解环境的特定要求（例如需要安装哪些必备项）非常重要。然后，您可以正确定义任务序列。

提示：收集此信息的好方法是在环境中的其中一台计算机中手动安装 VDA。此过程将显示在 VDA 安装过程中根据需要确定并安装了哪些必备项。

VDA 必备项的安装文件包含在 Citrix Virtual Apps and Desktops（或 XenApp 和 XenDesktop）版本的安装介质的 **Support** 文件夹下。使用这些文件可确保您安装的是正确的必备项版本。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

重新启动

安装必备项和 VDA 过程中所需的重新启动次数取决于环境。例如，早期软件安装中挂起的更新或重新启动可能需要重新启动。此外，以前被其他进程锁定的文件可能需要更新。

- 在手动安装过程中，确定触发重新启动的必备条件。
- VDA 安装程序中的某些可选组件（例如 Citrix Profile Management、Citrix Files）可能需要重新启动。在手动安装过程中，确定哪些组件安装会触发重新启动。

定义任务序列

确定所有必备项并重新启动后，使用 SCCM 任务排序器完成以下操作：

1. 为安装每个必备项创建单独的 SCCM 作业。这有助于隔离部署过程中出现的任何问题或故障，便于进行故障排除。
2. 创建 VDA 安装作业。在成功安装所有必备项之前，请勿执行此作业。这可以通过以下两种方式之一来完成：
    - 让 SCCM 客户端监视必备项的 GUID 以确定其是否存在。
    - 使 VDA 安装作业依赖于必备项的作业。

SCCM 安装顺序示例

下面是一个示例 SCCM 安装顺序。请记住：您的必备项版本可能会有所不同，具体取决于要安装的 VDA 版本。

1. SCCM JOB1：Microsoft .NET Framework 4.8
2. SCCM JOB2：Microsoft Visual C++ 2017 Runtime（32 位和 64 位）
3. SCCM JOB3：VDA 安装
    a) 根据要求使用相应的 VDA 安装程序命令。添加 `/quiet`、`/noreboot` 和 `/noresume` 选项。（`/noresume` 选项删除了对交互式登录继续安装的依赖关系，从而允许 SCCM 驱动安装过程。）
    b) 注意返回代码。
        - `0`：成功、安装完成、需要重新启动。
        - `3`：成功、安装未完成、需要重新启动。
        - `8`：成功、安装完成、需要重新启动。
    c) 请重新启动计算机。
    d) 如果返回代码为 3，请重复执行步骤 3a。（升级 VDA 时，需要执行额外的重新启动。）

有关返回代码的详细信息，请参阅 Citrix 安装返回代码。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

VDA 安装命令示例

可用的安装选项有所不同，具体取决于使用的安装程序。有关命令行选项详细信息，请参阅以下文章。（提供指向 Citrix Virtual Apps and Desktops 当前版本位置的链接。如果您使用的是 LTSR 产品版本，请参阅相应的 LTSR 文章。）

- 安装 VDA
- 使用命令行安装

Remote PC Access 的安装命令

- 以下命令使用单会话核心 VDA 安装程序（单独的 `VDAWorkstationCoreSetup.exe`）：

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

- 以下命令使用单会话完整 VDA 安装程序（单独的 `VDAWorkstationSetup.exe`）：

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

专用 **VDI** 的安装命令

- 以下命令使用单会话完整 VDA 安装程序（单独的 `VDAWorkstationSetup.exe`）：

  ```
  VDAWorkstationSetup.exe /quiet /components vda /controllers “control.domain.com” /enable_hdx_ports /enable_remote_assistance /noresume /noreboot
  ```

创建站点

January 21, 2022

站点是您为 Citrix Virtual Apps and Desktops 部署提供的名称。它包含 Delivery Controller、其他核心组件、Virtual Delivery Agent (VDA)、主机连接、计算机目录和交付组。在安装核心组件之后创建首个计算机目录和交付组之前创建站点。

如果您的 Controller 安装在 Server Core 上，请使用 Citrix Virtual Apps and Desktops SDK 中的 PowerShell cmdlet 创建站点。

在创建站点时，您将自动注册 Citrix 客户体验改善计划 (CEIP)。CEIP 会收集匿名统计信息和使用情况信息，然后将其发送到 Citrix。大约会在您创建站点七天后将第一个数据包发送到 Citrix。您可以在创建站点之后任何时间更改您

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

的注册。即在 Studio 导航窗格中依次选择配置和产品支持选项卡，并按相应指导进行操作。有关详细信息，请参阅 http://more.citrix.com/XD-CEIP。

创建站点的用户将成为完全权限管理员；有关详细信息，请参阅委派管理。

请在创建站点之前查看本文，以便了解需要什么。

步骤 1. 打开 Studio，然后启动站点创建向导

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。选择该操作。

步骤 2. 站点类型和名称

在简介页面上，选择站点类型：

- 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 导航窗格顶部：**Citrix Studio**（站点名称）。

步骤 3. 数据库

数据库页面包含用于设置站点、监视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。

> 注意：
>
> 如果已配置 SQL Server 始终可用侦听器以用于 TLS 加密，则系统可能会提示您输入具有数据库创建权限的凭据。即使输入有效的管理员凭据，尝试创建数据库仍然会失败。验证 SQL Server 证书的主题备用名称 (SAN) 中是否包含监听程序 DNS 名称。有关详细信息，请参阅 https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover#SSLcertificates。

如果选择安装要用作站点数据库的 SQL Server Express（默认设置），则在安装了该软件后将重新启动。如果选择不安装要用作站点数据库的 SQL Server Express 软件，则不重新启动。

如果不使用默认的 SQL Server Express，请确保在创建站点之前在计算机上安装 SQL Server 软件。系统要求列出了受支持的版本。

如果希望向站点添加多个 Delivery Controller，并且已在其他服务器上安装了 Controller 软件，则可以从此页面添加那些 Controller。如果您还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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

步骤 **4.** 许可

在许可页面上，指定许可证服务器地址，然后指明要使用（安装）的许可证。

- 请以 `name:[port]` 格式指定许可证服务器地址。*name* 必须是 FQDN、NetBIOS 或 IP 地址。建议使用 FQDN。如果忽略端口号，则默认为 27000。单击连接。与许可证服务器成功建立连接之后，才能继续到下一页面。
- 建立连接时，默认选择使用现有许可证。显示屏根据当前安装的许可证列出可配置此产品的兼容产品。
  - 如果要将此产品配置为列出的产品之一（例如，Citrix Virtual Apps Premium 或 Citrix Virtual Desktops Premium），请使用其中一个许可证选择该条目。
  - 如果您已分配并下载用于此产品的许可证（使用 Citrix Manage Licenses Tool），但尚未安装许可证：
    - 单击浏览许可证文件。
    - 在文件资源管理器中，找到并选择您下载的许可证。关联的产品现在显示在站点创建向导的许可页面上。选择要使用的条目。
  - 如果您需要的产品未显示，或者您没有分配和下载的许可证，则可以分配、下载并安装许可证。许可证服务器必须具有 Internet 访问权限，才能执行此操作。您必须拥有所需产品的许可证访问代码。Citrix 将通过电子邮件向您发送该代码。
    - 单击分配和下载。
    - 在分配许可证对话框中，输入 Citrix 发送的许可证访问代码。单击分配许可证。
    - 与新许可证关联的产品将显示在站点创建向导的许可页面上。选择要使用的条目。

    或者，选择使用 **30** 天免费试用版，然后安装许可证。有关详细信息，请参阅 Licensing 文档。

步骤 **5.** 电源管理（仅限 **Remote PC Access**）

请参阅步骤 8. Remote PC Access。

步骤 **6.** 主机连接、网络和存储

如果使用虚拟机管理程序或其他服务上的虚拟机交付应用程序和桌面，则可以选择创建相应主机的第一个连接。也可以为此连接指定存储和网络资源。创建站点后，可以修改此连接和资源，以及创建更多连接。有关详细信息，请参阅管理和资源。

- 有关在连接页面上指定的信息，请参阅连接和资源。
  - 如果不使用虚拟机管理程序或其他服务上的虚拟机（或如果您使用 Studio 管理专用刀片式 PC 上的桌面），请选择连接类型无。
  - 如果要配置 Remote PC Access 站点并计划使用局域网唤醒功能，请选择 **Microsoft System Center Configuration Manager** 类型。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

除了连接类型外，还可以指定是否将使用 Citrix 工具（例如 Machine Creation Services）或其他工具创建 VM。

- 有关在存储和网络页面上指定的信息，请参阅主机存储、存储管理和选择存储。

步骤 **7.** 附加功能

在附加功能页面上，可以选择用于自定义您的站点的功能。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。

- **App-V** 发布：如果使用 App-V 服务器上 Microsoft App-V 包中的应用程序，请选择此功能。提供 App-V 管理服务器的 URL 以及 App-V 发布服务器的 URL 和端口号。

  如果仅使用网络共享位置上 App-V 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。

步骤 **8. Remote PC Access**

有关 Remote PC Access 部署的信息，请参阅 Remote PC Access。

如果使用局域网唤醒功能，在创建站点之前，请在 Microsoft System Center Configuration Manager 上完成配置步骤。有关详细信息，请参阅 Configuration Manager 和 Remote PC Access 局域网唤醒。

创建 Remote PC Access 站点时：

- 如果要使用局域网唤醒功能，请在电源管理页面上指定 Microsoft System Center Configuration Manager 地址、凭据和连接信息。
- 在用户页面上指定用户或用户组。不存在自动添加所有用户的默认操作。另外，在计算机帐户页面上指定计算机帐户（域或 OU）信息。

  要添加用户信息，请单击添加用户。选择用户和用户组，然后单击添加用户。

  要添加计算机帐户信息，请单击添加计算机帐户。选择计算机帐户，然后单击添加计算机帐户。单击添加 **OU**。选择域和组织单位，然后指出是否包含子文件夹中的项目。单击添加 **OU**。

将自动创建名为 `Remote PC User Machine Accounts` 的计算机目录。该目录包含您在站点创建向导中添加的所有计算机帐户。系统会自动创建名为 `Remote PC User Desktops` 的交付组。该组包含您已添加的所有用户和用户组。

步骤 **9.** 摘要

摘要页面上列出了您指定的信息。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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

测试站点配置

要在创建站点后运行测试，请选择导航窗格顶部的 **Citrix Studio** (Site *site-name*)。然后单击中间窗格中的测试站点。可以查看站点测试结果的 HTML 报告。

对于 Windows Server 2016 上安装的 Controller，站点测试功能可能会失败。当本地 SQL Server Express 用于站点数据库而 SQL Server Browser 服务未启动时会失败。为了避免此问题，请完成下列任务。

1. 启用 SQL Server Browser 服务（如有必要），然后启动该服务。
2. 重新启动 SQL Server (SQLEXPRESS) 服务。

当您升级早期部署时，站点测试将自动运行。有关详细信息，请参阅初步站点测试。

故障排除

配置站点后，可以安装 Studio 并通过 MMC 将其添加为远程计算机上的管理单元。如果以后尝试删除该管理单元，MMC 可能停止响应。解决方法：重新启动 MMC。

创建计算机目录

September 19, 2023

> 重要：
>
> 自 Citrix Virtual Apps and Desktops 7 2006 起，如果您的当前部署使用以下任一技术或主机类型，则可以将部署升级到当前版本。只有在删除使用这些技术的项目后才能执行此操作。
>
> - 个人虚拟磁盘 (PvD)
> - AppDisk
> - 公有云主机类型：Amazon Web Services (AWS)、Citrix CloudPlatform、Microsoft Azure Classic、Microsoft Azure Resource Manager
>
> 有关详细信息，请参阅删除 PVD、AppDisk 和不受支持的主机。

简介

物理机或虚拟机的集合作为称为计算机目录的单个实体进行管理。目录中的计算机具有相同类型的操作系统：多会话操作系统或单会话操作系统。包含多会话操作系统计算机的目录可能包含 Windows 计算机或 Linux 计算机，但不能同时包含这二者。

Citrix 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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 提示：
>
> 升级现有部署可启用 Machine Creation Services (MCS) 存储优化 (MCS I/O) 功能，而无需额外的配置。Virtual Delivery Agent (VDA) 和 Delivery Controller 升级处理 MCS I/O 升级。

概述

在您创建 VM 的目录时，要指定如何预配这些 VM。您可以使用 Citrix 工具，例如 Machine Creation Services (MCS) 或 Citrix Provisioning（以前称为 Provisioning Services）。也可以使用您自己的工具来提供计算机。

请注意：

- MCS 支持虚拟机映像中的单个系统磁盘。它忽略附加到该映像的其余数据磁盘。
- 如果使用 Citrix Provisioning 创建计算机，请参阅 Citrix Provisioning 文档以了解相关说明。
- 如果使用 MCS 预配 VM，则需要提供一个主映像（或映像的快照）以在目录中创建完全相同的 VM。创建目录之前，请先使用工具创建并配置主映像。此过程包括在该映像上安装 Virtual Delivery Agent (VDA)。然后在 Studio 中创建计算机目录。选择该映像（或快照），指定要在目录中创建的 VM 数以及配置其他信息。
- 如果您的计算机已可用，您仍必须为那些计算机创建一个或多个计算机目录。
- 如果直接使用 PowerShell SDK 创建目录，可以指定虚拟机管理程序模板 (VMTemplates)，而不是映像或快照。
- 使用模板预配目录被视为一项试验性功能。使用此方法时，虚拟机准备可能会失败。因此，无法使用模板发布目录。

使用 MCS 或 Citrix Provisioning 创建第一个目录时，请使用创建站点时配置的主机连接。之后（创建第一个目录和交付组后），可以更改该连接的信息或创建更多连接。

完成目录创建向导之后，将自动运行测试以确保目录配置正确。测试完成后，可以查看测试报告。通过 Studio 随时运行测试。

> 注意：
>
> MCS 不支持 Windows 10 IoT 核心版和 Windows 10 IoT 企业版。请参阅 Microsoft 站点以了解详细信息。

有关 Citrix Provisioning 工具的技术详细信息，请参阅 Citrix Virtual Apps and Desktops 映像管理。

RDS 许可证检查

在创建包含 Windows 多会话操作系统计算机的计算机目录时，Citrix Studio 当前不会检查是否存在有效的 Microsoft RDS 许可证。要查看适用于 Windows 多会话操作系统计算机的 Microsoft RDS 许可证的状态，请转到 Citrix Director。在计算机详细信息面板中查看 Microsoft RDS 许可证的状态。此面板位于计算机详细信息和用户详细信息页面中。有关详细信息，请参阅 Microsoft RDS 许可证运行状况部分。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

VDA 注册

必须向要在启动代理会话时使用的 Delivery Controller 注册 VDA。未注册的 VDA 会导致无法充分利用原本可用的资源。VDA 无法注册的原因有多种，其中许多都可由管理员进行故障排除。Studio 在目录创建向导中以及在您向交付组中添加了某个目录中的计算机之后，提供故障排除信息。

使用向导添加现有计算机后，计算机帐户名称列表会指示每台计算机是否都适合添加到该目录。将鼠标悬停在每个计算机旁边的图标上，以显示有关该计算机的有用消息。

如果该消息确定存在一台有问题的计算机，请删除该计算机，或者添加计算机。例如，如果一条消息指示可能无法获取有关某台计算机的信息，则添加该计算机。

有关详细信息，请参阅：

- CTX136668，了解 VDA 注册故障排除指导信息
- VDA 版本和功能级别
- VDA 注册方法

MCS 目录创建摘要

此处简要概述您在目录创建向导中提供信息后要执行的默认 MCS 操作。

- 如果选择了主映像（而非快照），则 MCS 会创建快照。
- MCS 创建此快照的完整副本，并将副本放在主机连接中定义的各个存储位置。
- MCS 将计算机添加到 Active Directory，Active Directory 创建唯一身份。
- MCS 创建向导中指定的 VM 数，并为每个 VM 定义两个磁盘。除每个 VM 的两个磁盘外，主映像也存储在相同的存储位置。如果定义了多个存储位置，每个磁盘位置将获得以下磁盘类型：
  - 快照的完整副本，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。此磁盘采用精简预配（前提是主机存储支持）并在必要时增加到主映像的最大大小。每个 VM 获得一个差异磁盘。差异磁盘保存会话期间所做的更改。对于专有桌面，此磁盘为永久磁盘。对于池桌面，每次通过 Delivery Controller 重新启动时都会删除此磁盘并创建一个新磁盘。

或者，在创建 VM 以交付静态桌面时，您可以指定（在目录创建向导的计算机页面上）胖（完整复制）VM 克隆。完整克隆不需要在每个数据存储上保留主映像。每个 VM 均有自己的文件。

MCS 存储注意事项

确定适用于 MCS 的存储解决方案、配置和容量时，需要考虑许多因素。以下信息针对存储容量提供了适当的注意事项：

容量注意事项：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 磁盘

  增量磁盘或差异磁盘在每个 VM 的大多数 MCS 部署中占用的空间量最大。由 MCS 创建的每个 VM 在创建时最少具有 2 个磁盘。

  - Disk0 = 差异磁盘：包含从主基础映像复制时的操作系统。
  - Disk1 = 身份磁盘：16 MB - 包含每个 VM 的 Active Directory 数据。

  随着产品的升级，您可能需要添加更多磁盘，以满足特定用例和功能的占用。例如：

  - MCS 存储优化可为每个 VM 创建写入缓存样式磁盘。
  - MCS 新增了使用完整克隆的功能，而不是前一节中所述的增量磁盘方案。

  虚拟机管理程序功能也可能会进入权衡阶段。例如：

  - Citrix Hypervisor IntelliCache 在本地存储中为每个 Citrix Hypervisor 创建一个读取磁盘。此选项保存在可能保存在共享存储位置的主映像的 IOPS 上。

- 虚拟机管理程序开销

  不同的虚拟机管理程序使用为 VM 创建开销的特定文件。虚拟机管理程序还可以使用存储进行管理和常规日志记录操作。计算空间以包含以下对象的开销：

  - 日志文件
  - 特定于虚拟机管理程序的文件。例如：
    * VMware 会将更多文件添加到 **VM** 存储文件夹中。请参阅 VMware 最佳做法。
    * 计算总虚拟机大小的需求。假设存在一台虚拟机，20 GB 用于虚拟磁盘，16 GB 用于交换文件，100 MB 用于日志文件，总共占用 36.1 GB。
  - XenServer 的快照；VMware 的快照。

- 处理开销

  创建目录、添加计算机以及更新目录会产生独特的存储影响。例如：

  - 初始目录创建要求将基础磁盘的副本复制到每个存储位置。
    * 还要求您临时创建准备 VM。
  - 向目录添加计算机不需要将基础磁盘复制到每个存储位置。目录创建因所选功能而异。
  - 更新目录以在每个存储位置创建额外的基础磁盘。目录更新还会出现临时存储高峰，即目录中的每个 VM 在特定的时间段内都具有 2 个差异磁盘。

更多注意事项：

- **RAM** 大小调整：影响特定虚拟机管理程序文件和磁盘的大小，包括 I/O 优化磁盘、写入缓存和快照文件。
- 精简/密集预配：由于具有精简预配功能，因此首选使用 NFS 存储。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Machine Creation Services (MCS) 存储优化

使用 Machine Creation Service (MCS) 存储优化功能（称为 MCS I/O）：

- 写入缓存容器基于文件，与在 Citrix Provisioning 中找到的功能相同。例如，Citrix Provisioning 写入缓存文件名为 `D:\vdiskdif.vhdx`，MCS I/O 写入缓存文件名为 `D:\mcsdif.vhdx`。
- 通过包括支持写入到写入缓存磁盘的 Windows 故障转储文件来实现诊断功能的改进。
- MCS I/O 保留技术在 *RAM* 中缓存并溢出到硬盘，以提供最优的多层写入缓存解决方案。此功能允许管理员在每个层、RAM 和磁盘中的成本与性能之间进行平衡，以满足所需的工作负载期望。

将写入缓存方法从基于磁盘更新为基于文件需要进行以下更改：

1. MCS I/O 不再支持仅 RAM 缓存。在计算机目录创建期间在 Citrix Studio 中指定磁盘大小。
2. 首次启动 VM 时，将自动创建并格式化 VM 写入缓存磁盘。VM 启动后，写入缓存文件 `mcsdif.vhdx` 将写入到格式化的卷 `MCSWCDisk` 中。
3. 页面文件将重定向到此格式化的卷 `MCSWCDisk`。因此，此磁盘大小将考虑磁盘空间总量。它包括磁盘大小与生成的工作负载之间的增量以及页面文件大小。这通常与 VM RAM 大小相关联。

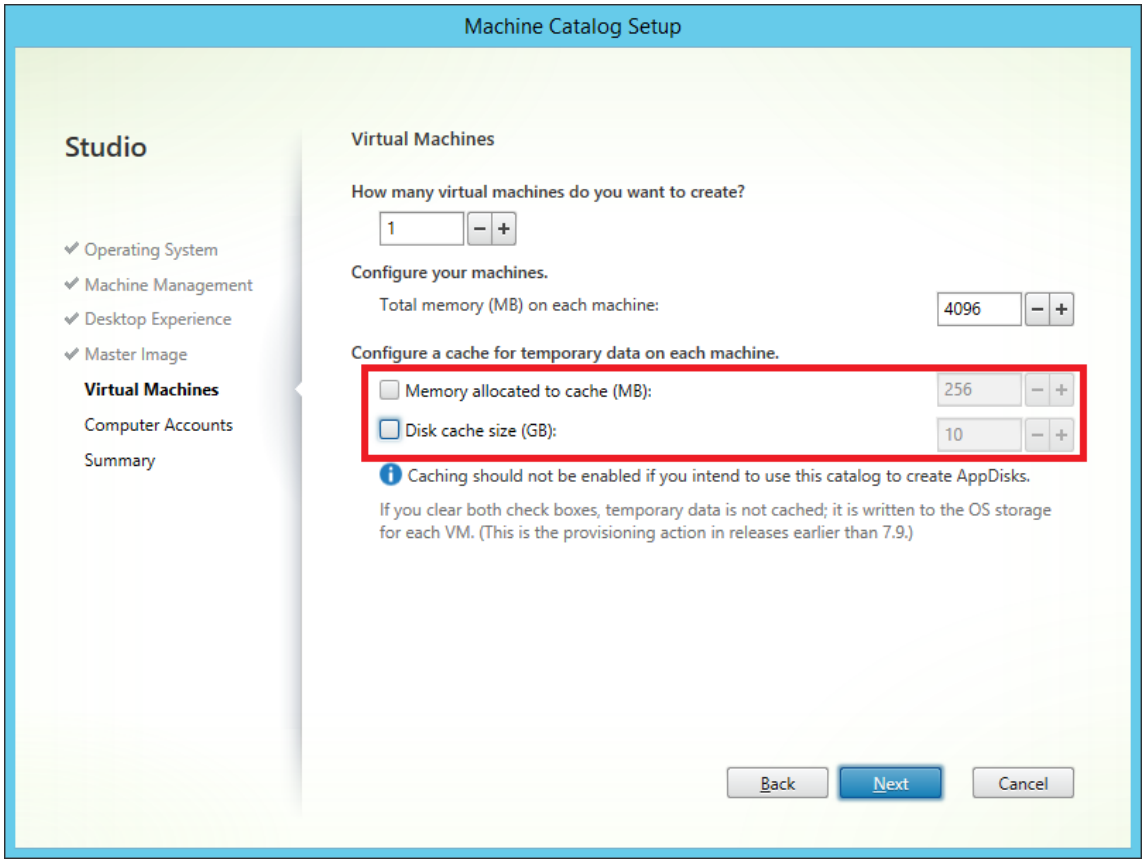
启用 **MCS** 存储优化更新　要启用 MCS I/O 存储优化功能，请将 Delivery Controller 和 VDA 升级到最新版本的 Citrix Virtual Apps and Desktops。

> 注意：
>
> 如果升级启用了 MCS I/O 的现有部署，则无需执行任何其他配置。VDA 和 Delivery Controller 升级处理 MCS I/O 升级。

启用 MCS 存储优化更新时，请注意以下事项：

- 创建计算机目录时，管理员可以配置 RAM 和磁盘大小。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- 将现有计算机目录更新为包含为版本 1903 配置的 VDA 的新 VM 快照会导致出现以下行为：新快照将继续使用现有目录的 MCS I/O 设置来确定 RAM 和磁盘大小。现有原始磁盘已格式化。

> 重要：
>
> Citrix Virtual Apps and Desktops 版本 1903 更改了 MCS 存储优化。此版本支持基于文件的写入缓存技术，提供更好的性能和稳定性。与之前的 Citrix Virtual Apps and Desktops 版本相比，MCS I/O 提供的新功能可能需要更高的写入缓存存储需求。Citrix 建议您重新评估磁盘大小，以确保磁盘有足够的磁盘空间来存储分配的工作流和额外的页面文件大小。页面文件大小通常与系统 RAM 量有关。如果现有目录磁盘大小不足，请创建一个计算机目录并分配较大的写入缓存磁盘。

使用 **PowerShell** 创建具有持久回写式缓存磁盘的目录　要配置具有永久回写式缓存磁盘的目录，请使用 PowerShell 参数 `New-ProvScheme CustomProperties`。此参数支持额外的属性 `PersistWBC`，用于确定 MCS 预配的计算机的回写式缓存磁盘如何保留。仅当指定了 `UseWriteBackCache` 参数时，并且当 `WriteBackCacheDiskSize` 参数设置为指示创建了磁盘时才使用 `PersistWBC` 属性。

在支持 `PersistWBC` 之前在 `CustomProperties` 参数中找到的属性示例包括：

```
1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
    benvaldev5RG3" />
</CustomProperties>
<!--NeedCopy-->
```

使用这些属性时，如果在 CustomProperties 参数中省略这些属性，请考虑其包含默认值。PersistWBC 属性有两个可能的值：**true** 或 **false**。

如果将 PersistWBC 属性设置为 **true**，则当 Citrix Virtual Apps and Desktops 管理员使用 Citrix Studio 关闭计算机时，不会删除回写式缓存磁盘。

如果将 PersistWBC 属性设置为 **false**，则当 Citrix Virtual Apps and Desktops 管理员使用 Citrix Studio 关闭计算机时，将删除回写式缓存磁盘。

> 注意：
>
> 如果省略 PersistWBC 属性，则该属性默认设置为 **false**，并在使用 Citrix Studio 关闭计算机时删除回写式缓存。

例如，使用 CustomProperties 参数将 PersistWBC 设置为 true：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
    benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
</CustomProperties>
<!--NeedCopy-->
```

> 重要：
>
> 只能使用 New-ProvScheme PowerShell cmdlet 设置 PersistWBC 属性。在创建后尝试更改预配方案 CustomProperties 不会影响计算机目录以及计算机关闭时回写式缓存磁盘的持久性。

例如，设置 New-ProvScheme 以在将 PersistWBC 属性设置为 true 时使用回写式缓存：

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
    /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
    XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
    UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
      StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
      /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
      Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
      =`"PersistWBC`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

准备主映像

有关创建连接主机的信息，请参阅连接和资源。

主映像包含操作系统、非虚拟化应用程序、VDA 和其他软件。

须知：

- 主映像可能也称为克隆映像、黄金映像、基础 VM 或基础映像。主机供应商使用不同的术语。
- 使用 Citrix Provisioning 时，可以使用主映像或物理计算机作为主目标设备。Citrix Provisioning 使用与 MCS 不同的术语来表示映像。有关详细信息，请参阅 Citrix Provisioning 文档。
- 确保主机具有足够多的处理器、内存和存储来容纳创建的计算机数。
- 正确配置桌面和应用程序所需的硬盘空间量。因为该值以后不能更改，也不能在计算机目录中更改。
- Remote PC Access 计算机目录不使用主映像。
- 在使用 MCS 时的 Microsoft KMS 激活注意事项：如果您的部署包括采用 XenServer 6.1 或 6.2、vSphere 或 Microsoft System Center Virtual Machine Manager 主机的 7.x VDA，则无需手动重新部署 Microsoft Windows 或 Microsoft Office。

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 Citrix VM 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）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 未虚拟化的第三方应用程序。Citrix 建议对应用程序进行虚拟化。进行虚拟化后，无需在添加或重新配置应用程序后更新主映像，从而降低成本。此外，减少安装的应用程序数量还可以减小主映像硬盘的大小，从而节约存储成本。
- 具有建议设置的 App-V 客户端（如果计划发布 App-V 应用程序）。App-V 客户端可从 Microsoft 获取。
- 使用 MCS 时，如果要本地化 Microsoft Windows，请安装区域设置和语言包。在预配期间，如果已创建快照，则已预配的 VM 使用已安装的区域设置和语言包。

> 重要：
>
> 如果要使用 Citrix Provisioning 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主映像，然后安装操作系统以及所有服务包和更新。指定 vCPU 数。如果使用 PowerShell 创建计算机目录，还可以指定 vCPU 值。使用 Studio 创建目录时不能指定 vCPU 数。配置桌面和应用程序所需的硬盘空间量。因为该值以后不能更改，也不能在目录中更改。
2. 确保硬盘连接在设备位置 0 处。大多数标准主映像模板在默认情况下都会配置此位置，但有些自定义模板可能不配置。
3. 在主映像上安装和配置上面列出的软件。
4. 使用 Citrix Provisioning 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 Citrix Provisioning 文档。
5. 如果未使用 MCS，请将主映像加入到应用程序和桌面所属的域中。确保主映像在创建计算机的主机上可用。如果使用 MCS，则不需要将主映像加入到域中。预配的计算机已加入在目录创建向导中指定的域中。
6. Citrix 建议您创建并命名主映像的快照。如果您在创建目录时指定主映像而非快照，Studio 将创建一个快照。您不能对其进行命名。

使用 **Studio** 创建计算机目录

启动目录创建向导之前，请查看本节内容。

如果要使用主映像，请确保创建目录之前已在此映像上安装 VDA。

在 Studio 中：

- 如果您已创建站点但尚未创建计算机目录，Studio 会指导您进入正确的起始位置以创建目录。
- 如果您已创建目录且希望创建另一目录，请在 **Studio** 导航窗格中选择计算机目录。然后在操作窗格中选择创建计算机目录。

该向导将指导您完成下列项目。根据您所做的选择，您看到的向导页面会有所不同。

操作系统

每个目录都只包含一种类型的计算机。请选择一种。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 多会话操作系统：多会话操作系统目录提供托管共享桌面。计算机可以在受支持的 Windows 或 Linux 操作系统版本上运行，但目录不能同时包含这两种操作系统。（参阅 Linux VDA 文档了解该操作系统的详细信息。）
- 单会话操作系统：单会话操作系统目录提供 VDI 桌面，您可以将这些桌面分配给不同的用户。
- **Remote PC Access**：Remote PC Access 目录为用户提供对其办公室物理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

此页面不会在创建 Remote PC Access 目录时显示。

计算机管理页面指出管理计算机的方式以及用于部署计算机的工具。

选择目录中的计算机是否通过 Studio 进行电源管理。

- 计算机通过 Studio 进行电源管理，例如，VM 或刀片式 PC。仅当您已配置到主机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。

如果您指出计算机是通过 Studio 进行电源管理的，请选择用于创建 VM 的工具。

- **Citrix Machine Creation Services (MCS)**：使用主映像创建和管理虚拟机。MCS 不可用于物理机。
- **Citrix Provisioning**：（以前称为 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 Citrix Provisioning 虚拟磁盘交付桌面和应用程序。

  > 注意：
  >
  > 不再支持此选项。要将 Citrix Provisioning 目标设备导入到 Citrix Virtual Apps and Desktops 目录中，请使用 **Citrix Provisioning** 导出设备向导。

- 其他：用于管理已位于数据中心内的计算机的工具。Citrix 建议您使用 Microsoft System Center Configuration Manager 或其他第三方应用程序，以确保目录中的计算机一致。

桌面类型（桌面体验）

此页面仅在创建包含单会话操作系统计算机的目录时显示。

桌面体验页面确定每次用户登录时发生的情况。选择以下其中之一：

- 用户在每次登录时均会连接至一个新的（随机的）桌面。
- 用户每次登录时连接至同一个（静态）桌面。

如果您选择第二项并使用 MCS 来预配计算机，您可以对如何处理用户对桌面所做的更改进行配置：

- 在本地磁盘上保存用户对桌面的更改。
- 在用户注销时放弃用户更改并清除虚拟桌面。如果您使用的是用户个性化层，请选择此选项。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

主映像

此页面仅在使用 MCS 来创建虚拟机时显示。

在主映像页面上，选择与主机的连接，然后选择之前创建的快照或 VM。如果正在创建第一个目录，唯一可用的连接是您在创建站点时配置的连接。

谨记：

- 使用 MCS 或 Citrix Provisioning 时，请勿在主映像上运行 Sysprep。
- 如果您指定主映像而非快照，Studio 将创建一个快照，但您无法为其命名。

为了能够使用最新的产品功能，请务必在主映像上安装最新的 VDA 版本。请勿更改默认的最小 VDA 选择。但是，如果您必须使用早期 VDA 版本，请参阅 VDA 版本和功能级别。

如果选择的快照或 VM 与您之前在向导中选择的计算机管理技术不兼容，将显示错误消息。

设备集合

此页面仅在使用 Citrix Provisioning 创建 VM 时显示。

设备集合页面显示设备集合和尚未添加至目录的设备。

选择要使用的设备集合。

计算机

此页面不会在创建 Remote PC Access 目录时显示。

此页面的标题取决于您在计算机管理页面上选择的内容：计算机、虚拟机或 **VM** 和用户。

使用 **MCS** 时：

- 指定要创建的虚拟机数。
- 选择每个 VM 将具有的内存量（以 MB 为单位）。
- 创建的每个 VM 都有一个硬盘。其大小在主映像中设置。您不能在目录中更改硬盘大小。
- 如果部署包含多个区域，可以为此目录选择一个区域。
- 如果您正创建静态桌面虚拟机，请选择一个虚拟机复制模式。请参阅虚拟机复制模式。
- 如果您创建的是不使用虚拟磁盘的随机桌面虚拟机，您可以配置一个高速缓存，使其用于每台计算机上的临时数据。请参阅配置用于临时数据的缓存。

使用 **Citrix Provisioning** 时：

设备页面列出了设备集合中您在前面的向导页面中选择的计算机。您无法在此页面上添加或删除计算机。

使用其他工具时：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

添加（或导入一列）Active Directory 计算机帐户名称。在添加/导入了某个虚拟机后可以更改该虚拟机的 Active Directory 帐户名称。如果在桌面体验页面上指定了静态计算机，您可以选择为添加的每个 VM 指定 Active Directory 用户名。

添加或导入名称后，可以使用删除按钮从列表中删除名称，而您仍在此页面上。

使用 **Citrix Provisioning** 或其他工具（而非 **MCS**）时：

每个添加的（或导入的，或来自 Citrix Provisioning 设备集合的）计算机的图标和工具提示都可帮助确定可能不适合添加到目录或者可能无法通过 Delivery Controller 注册的计算机。有关详细信息，请参阅 VDA 版本和功能级别。

虚拟机复制模式

您在计算机页面上指定的复制模式决定 MCS 从主映像创建瘦（快速复制）克隆还是胖（完整复制）克隆。（默认为瘦克隆）

- 使用快速复制克隆以实现更高效的存储用途和更快速的计算机创建。
- 使用完整复制克隆以实现更好的数据恢复和迁移支持，但在创建了计算机之后可能导致更低的 IOPS。

VDA 版本和功能级别

目录的功能级别控制哪些产品功能可用于目录中的计算机。要使用新产品版本中采用的功能，需要使用新的 VDA。通过设置功能级别，该版本（及更高版本，如果功能级别未更改）中采用的所有功能均可用于目录中的计算机。但是，具有早期 VDA 版本的目录中的计算机将无法注册。

计算机（或设备）页面底部附近的菜单允许您选择最低 VDA 级别。这会设定目录的最低功能级别。默认情况下，会针对内部部署选择最新的功能级别。如果您遵循 Citrix 建议，始终安装和升级 VDA 和核心组件至最新版本，则无需更改此选择。但是，如果必须继续使用较早的 VDA 版本，则请选择正确的值。

Citrix Virtual Apps and Desktops 版本可能不包括新 VDA 版本，或者新 VDA 不影响功能级别。在这种情况下，功能级别可能指示 VDA 版本早于已安装或已升级的组件。例如，尽管版本 7.17 包含 7.17 VDA，但默认功能级别（7.9 或更高级别）保持最新版本。因此，安装 7.17 或将组件从 7.9-7.16 升级到 7.17 后，不需要更改默认功能级别。每个版本的新增功能一文都指示默认功能级别的任何更改。

选定的功能级别会影响其上面的计算机列表。在列表中，每个条目附近的工具提示会指示计算机的 VDA 是否与该功能级别下的目录兼容。

如果每台计算机上的 VDA 不符合或超过选定的最低功能级别，则会在页面上弹出消息提示。您可以继续执行本向导。这些计算机可能无法稍后再通过 Controller 来注册。或者，您可以：

- 从列表中删除包含较早 VDA 的计算机，升级它们的 VDA，然后将它们重新添加到目录。
- 选择阻止访问最新的产品功能的较低功能级别。

如果因为错误的计算机类型无法将某台计算机添加到目录，也会弹出消息。例如，尝试将一台服务器添加到单会话操作系统目录，或将一台原本为随机分配创建的单会话操作系统计算机添加到静态计算机的目录中。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 重要：
>
> 在版本 1811 中，添加了一个额外的功能级别：**1811**（或更高版本）。该级别用于与将来的 Citrix Virtual Apps and Desktops 功能结合使用。**7.9**（或更高版本）选项将保留默认值。现在，该默认值对所有部署都有效。
>
> 如果您选择 **1811**（或更高版本），则该目录中的任意早期 VDA 版本将无法通过 Controller 或 Cloud Connector 来注册。但是，如果该目录中仅包含 VDA 版本 1811 或受支持的更高版本，它们将都符合注册条件。这包括为更高版本的 Citrix Virtual Apps and Desktops 版本（包括版本 1903 及当前版本之前的其他 19XX 版本）配置的 VDA 的目录。

配置用于临时数据的缓存

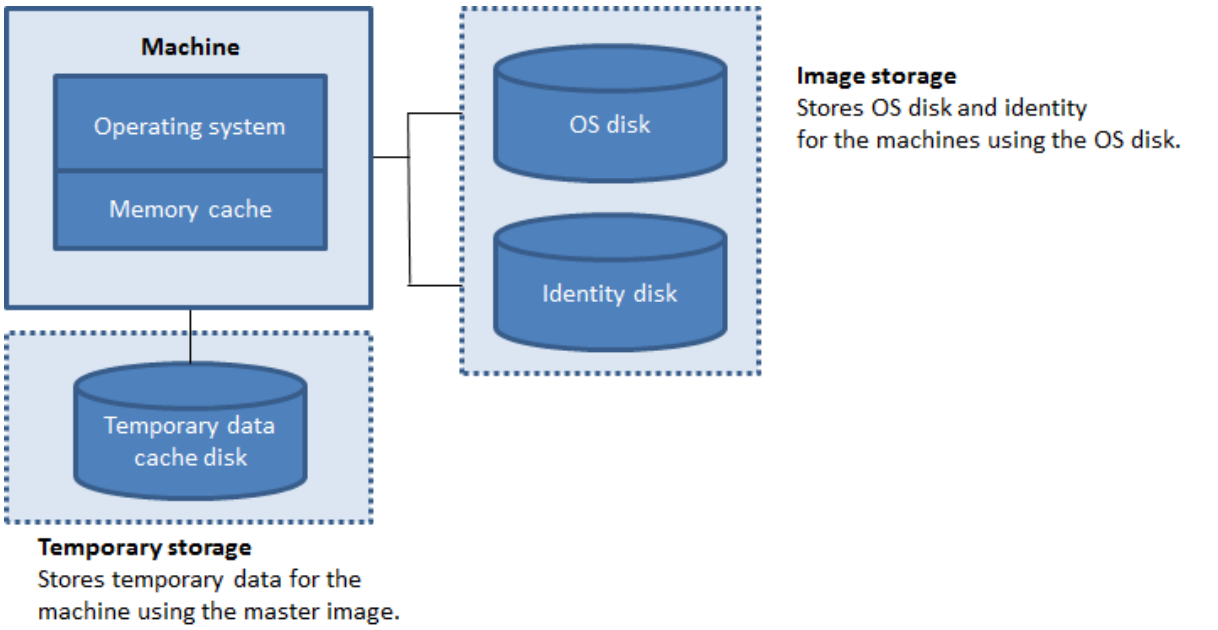
在虚拟机本地缓存临时数据的行为是可选行为。当使用 MCS 管理目录中的合并（而非专用）计算机时，可以在计算机上启用临时数据缓存。如果目录使用一个用于指定临时数据存储的连接，则您可以在创建目录时启用并配置临数据缓存信息。

> 重要：
>
> 此功能需要最新的 MCS I/O 驱动程序。安装或升级 VDA 时可以选择安装此驱动程序。默认情况下，未安装该驱动程序。

在创建目录使用的连接时，可以指定临时数据是使用共享存储还是使用本地存储。有关详细信息，请参阅连接和资源。要为每台计算机上的临时数据配置缓存，可以使用以下两个选项：分配给缓存的内存 **(MB)** 和磁盘缓存大小 **(GB)**。默认情况下，取消选中这两个选项。要启用“分配给缓存的内存 (MB)”选项，请选中“磁盘缓存大小 (GB)”复选框。如果未选中磁盘缓存大小复选框，“分配给缓存的内存”选项将变为灰色。根据连接类型，这些选项的默认值可能会有所差别。通常情况下，默认值对大多数情况来说已足够。但是，请考虑以下各项所需的空间：

- Windows 自己创建的临时数据文件（其中包括 Windows 页面文件）。
- 用户配置文件数据。
- 同步到用户的会话的 ShareFile 数据。
- 可由会话用户，或由可在会话内执行安装的任何应用程序用户创建或复制的数据。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



要为每台计算机上的临时数据配置缓存，请注意以下三种情况：

- 如果不选中“磁盘缓存大小”复选框和“分配给缓存的内存”复选框，则不会缓存临时数据。这些数据会直接写入每个 VM 的其他磁盘（位于操作系统存储中）。（这是版本 7.8 和更早版本中的预配操作。）
- 如果选中了“磁盘缓存大小”复选框，但未选中“分配给缓存的内存”复选框，临时数据将直接写入缓存磁盘，从而仅使用最少量的内存缓存。
- 如果选中了“磁盘缓存大小”复选框和“分配给缓存的内存”复选框，临时数据最初将写入到内存缓存中。当内存缓存达到其配置的限制（分配给缓存的内存值）时，最早的数据将移动到临时数据缓存磁盘。

> 重要：
>
> - 如果磁盘缓存空间已用完，则用户的会话将变得不可用。
> - 此功能在使用 Nutanix 主机连接时不可用。
> - 在创建计算机后，不能在计算机目录中更改缓存值。
>
> 注意：
>
> - 内存缓存是每台计算机上的内存总量的一部分。因此，如果启用“分配给缓存的内存”选项，则可以考虑在每台计算机上增加内存总量。
> - 从其默认值更改磁盘缓存大小可能会影响性能。此大小必须与用户需求以及计算机负载相匹配。

网络接口卡 (NIC)

此页面不会在创建 Remote PC Access 目录时显示。

在网络接口卡页面上，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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

计算机帐户

此页面仅在创建 Remote PC Access 目录时显示。

在计算机帐户页面上，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。

计算机帐户

此页面仅在使用 MCS 创建虚拟机时显示。

目录中的每台计算机都必须具有一个相应的 Active Directory 计算机帐户。在计算机帐户页面上，指示是创建帐户还是使用现有帐户，并指出这些帐户的位置。

- 如果创建帐户，则必须具有在计算机所在的 OU 中创建计算机帐户的权限。

  为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
...
<!--NeedCopy-->
```

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。

对于包含物理计算机或现有计算机的目录，请选择或导入现有帐户。将每台计算机分配给 Active Directory 计算机帐户和用户帐户。

对于使用 Citrix Provisioning 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 Citrix Provisioning 文档。

摘要、名称和描述

在摘要页面上，检查指定的设置。为目录输入名称及说明。此信息显示在 Studio 中。

完成后，单击完成以开始创建目录。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

故障排除

> 重要：
>
> 使用 Citrix Studio 创建计算机目录后，无法再使用 `Get-ProvTask` PowerShell 命令检索与计算机目录创建相关联的任务。此限制是因为，无论目录是否成功创建，Studio 都会在计算机目录创建后删除这些任务。

Citrix 建议收集日志以帮助支持团队提供解决方案。使用 Citrix Provisioning 时，请按照以下过程生成日志文件：

1. 在主映像上，创建值为 1（以“DWORD (32 位) 值”格式）的以下注册表项：`HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`。
2. 关闭主映像并创建快照。
3. 在 Delivery Controller 上运行以下 PowerShell 命令：`Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`。
4. 根据该快照创建一个目录。
5. 当准备 VM 是在虚拟机管理程序上创建的时，请登录并从 C:\ 的根目录下提取以下文件：Image-prep.log 和 PvsVmAgentLog.txt。
6. 关闭计算机，此时将报告失败。
7. 运行以下 PowerShell 命令以重新启用自动关闭映像准备计算机的功能：`Remove-ProvServiceConfigurationD -Name ImageManagementPrep_NoAutoShutdown`。

映像准备问题

由于 MCS 从单个映像创建了许多计算机，因此需要执行一些步骤来确保所有计算机都是唯一的并且正确地获得了许可。映像准备是目录创建过程的一部分。此准备工作可确保已预配的所有计算机都具有唯一的 IP 地址，并将自己作为唯一的实例正确地向 KMS 服务器宣布。在 MCS 中，选择主映像快照后进行映像准备工作。创建副本是为了使目录能够将自身与选定的计算机隔离开来。基于原始 VM 创建准备 VM，但网络连接已断开。断开网络连接可防止与其他计算机发生冲突，同时确保准备好的 VM 仅连接到新的已复制的磁盘。

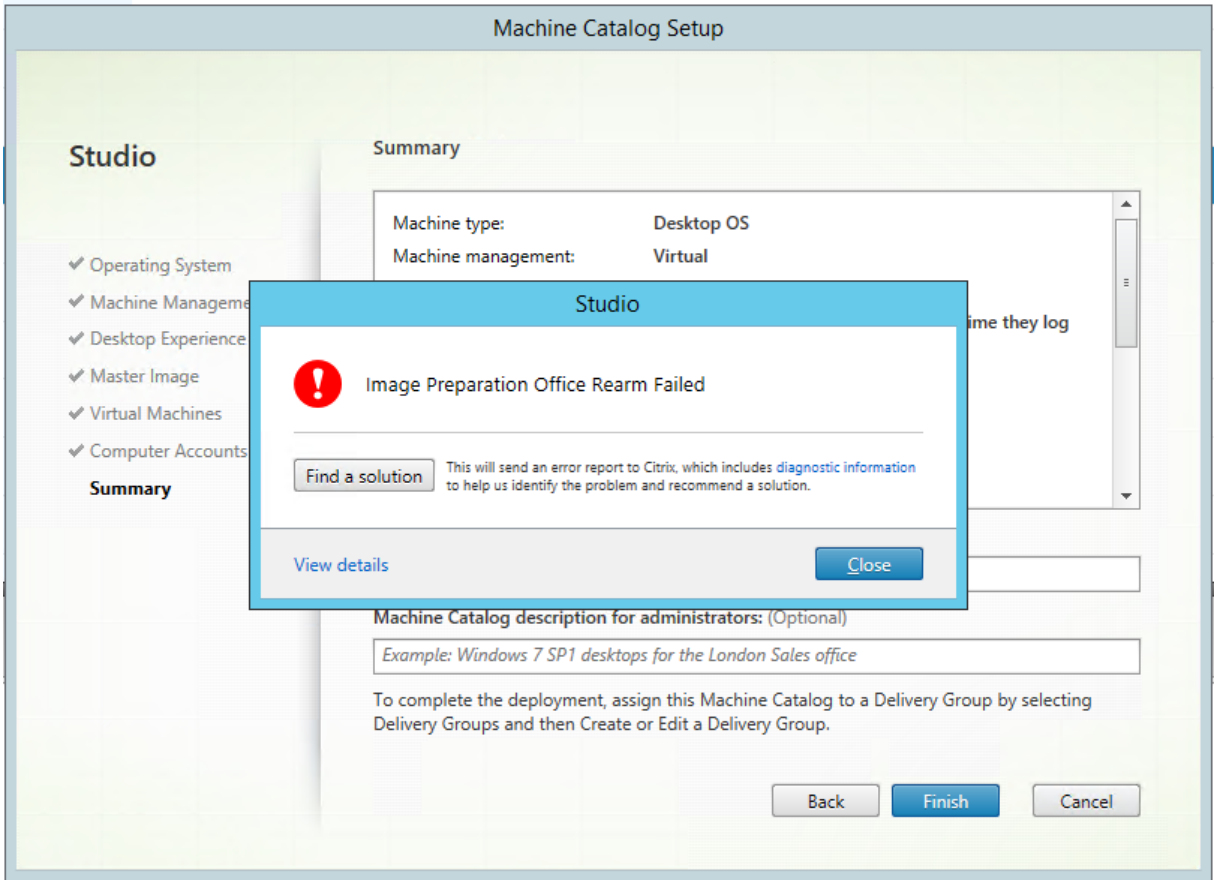
准备好的 VM 附加了一个包含运行映像准备工作所需步骤的小型指令磁盘。这个准备好的 VM 将启动，映像准备过程开始进行。映像准备包括以下过程：

- 启用 DHCP。启用 DHCP 可确保已预配的计算机不会导致 IP 地址冲突。所有网卡上都启用了 DHCP。
- Microsoft Windows KMS 重置。重置 KMS 可确保 Microsoft Windows 正确地获得了许可。重置的操作系统会被调用，以便将其作为新实例正确地报告给 KMS 许可证服务器。
- Microsoft Office KMS 重置（如果安装了 Microsoft Office）。重置 Microsoft Office 可确保任何版本的 Microsoft Office (2010+) 都在其 KMS 服务器上正确注册。调用 Microsoft Office 重置后，它将作为新实例报告给 KMS 许可证服务器。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 提示：
>
> 映像准备过程完成后，将从虚拟机管理程序获取指令磁盘。虚拟机管理程序包含从映像准备过程中收集到的信息。

映像准备阶段可能失败的原因有各种。此时将显示如下所示的失败消息：



下面将讨论这些失败情况。

启用 **DHCP**　这些失败案例是由不支持静态 IP 地址的网卡引起的。例如，早期版本的 Dell SonicWall 网卡。操作失败，因为 SonicWall 卡是防火墙网卡，因此将卡设置为 DHCP 没有意义，因为这仅支持 DHCP。此问题已在 Citrix Virtual Apps and Desktops 的更高版本中修复。但是，如果在其他类型的网卡上看到此问题，应通过论坛或技术支持联系人报告给 Citrix。

> 注意：
>
> 以下示例中的这一 PowerShell 设置应用到 Citrix Virtual Apps and Desktops 站点，因此它会影响对现有目录执行的所有新目录和映像更新。

如果您在其他网卡上遇到此问题，可以通过在 Delivery Controller 上运行 PowerShell 命令来解决：

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
 -Value EnableDHCP
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Microsoft Office 重置、 在 Microsoft Office 重置阶段可能会发生各种 KMS 重置故障。主要故障如下：

- 某些 Microsoft Office 运行时（例如 **Access Runtime**）可以调用 Office 重置，导致其失败。
- 未安装 Microsoft Office 的 KMS 版本。
- 已超过重置计数。

如果错误为误报，则可以通过在 Delivery Controller 上运行以下 PowerShell 命令进行解决：

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
 -Value OfficeRearm
```

Microsoft Windows 重置 在 Microsoft Windows 重置阶段，可能会发生各种 KMS 故障。主要故障如下：

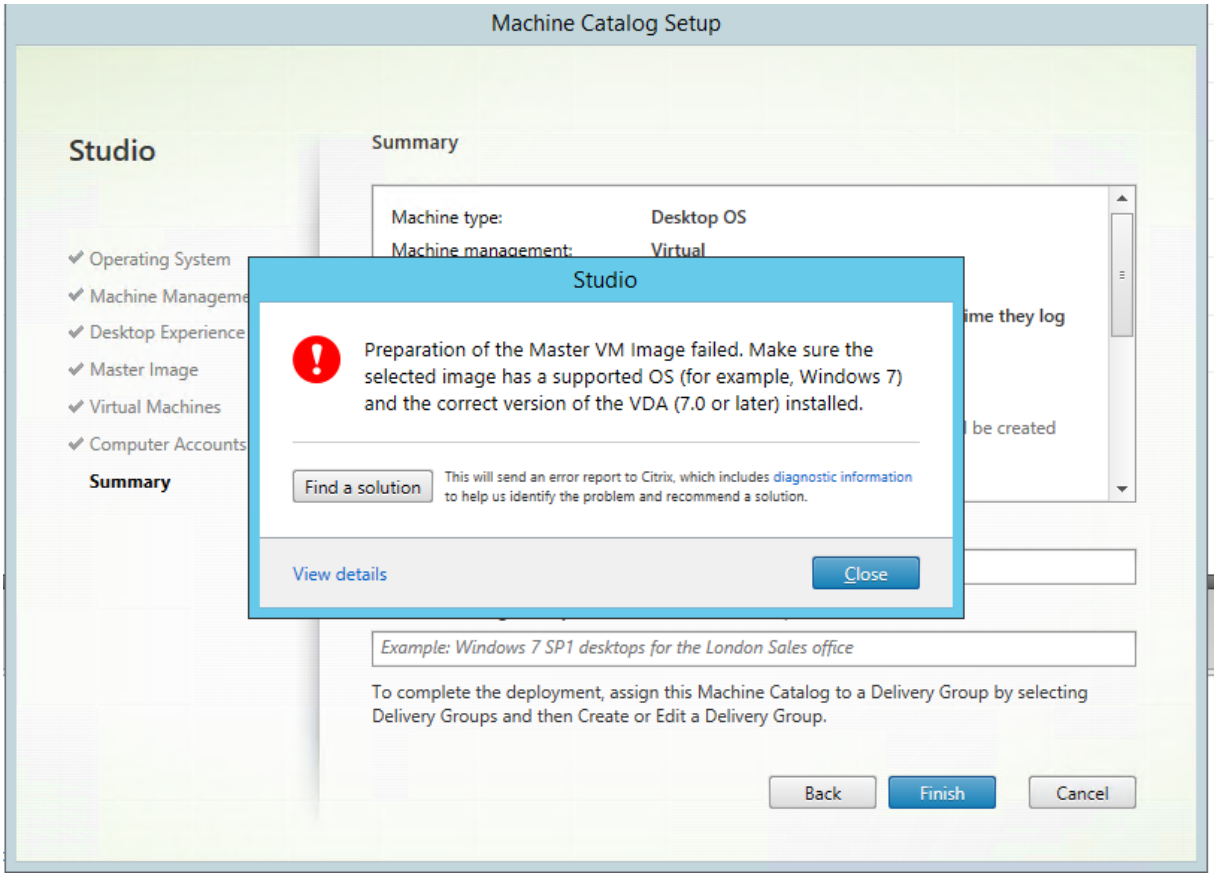
- 安装的 Windows 版本未使用 KMS 激活。例如，使用的是多次激活密钥 (MAK)。
- 已超过重置计数。

如果 Microsoft Windows 的版本正确地获得了许可，则可以通过在 Delivery Controller 上运行以下 PowerShell 命令来清除操作系统重置：

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
 -Value OsRearm
```

完全失败的实例 根据设计，映像准备计算机无法连接到网络，这意味着映像准备阶段有时只能报告完全失败。此失败类型的示例类似于：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



完全失败的主要原因如下：

未安装 **Virtual Delivery Agent (VDA)**，或者安装了 **VDA** 版本 **5.x**　如果主映像上未安装 VDA 7.x，映像准备将在 20 分钟后超时并报告上述错误。这是因为主映像上没有安装软件来运行映像准备阶段并报告成功或失败。要解决此问题，请确保在选定为主映像的快照上安装了 VDA（最低版本为 7）。

DISKPART SAN 策略　由于在主映像上设置了 DISKPART SAN 策略，因此，整个映像准备阶段可能会失败。如果未设置为使映像准备指令磁盘联机，计算机将关闭，映像准备过程将在 20 分钟后报告失败。要在主映像上进行检查，请运行以下命令：

```
C:>; Diskpart.exe
DISKPART>; San
<!--NeedCopy-->
```

此命令将返回当前策略。如果不是 *Online All*（全部联机），请运行以下命令对其进行更改：

```
DISKPART>; San policy=OnlineAll
```

关闭主映像，创建该计算机的快照，然后将其用作基础 MCS 映像。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

如果映像准备过程因其他原因失败　如果映像准备失败且没有明确的失败原因，您可以在创建 MCS 目录时绕过映像准备过程。但是，绕过此过程可能会导致站点上的 KMS 许可和网络连接 (DHCP) 出现问题。使用以下 PowerShell 命令：

```
Set-ProvServiceConfigurationData -Name
    ImageManagementPrep_DoImagePreparation -Value $false
<!--NeedCopy-->
```

请尽可能为 Citrix Support 团队收集日志，并通过论坛或通过技术支持联系人将问题报告给 Citrix。要收集日志，请执行以下操作：

1. 在主映像上，创建值为 1（以“DWORD (32 位) 值”格式）的以下注册表项：`HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`。
2. 关闭主映像并创建快照。在 Delivery Controller 上，启动 PowerShell，然后在加载了 Citrix PowerShell 管理单元的情况下运行 `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`。
3. 根据该快照创建一个目录。
4. 当准备 VM 是在虚拟机管理程序上创建的时，请登录并从 C:\ 的根目录下提取：

```
Image-prep.log
PvsVmAgentLog.txt
<!--NeedCopy-->
```

关闭计算机。此时将报告失败。

运行以下 PowerShell 命令以重新启用映像准备计算机的自动关闭功能：

```
Remove-ProvServiceConfigurationData -Name
ImageManagementPrep_NoAutoShutdown
```

下一步的去向

如果这是创建的第一个目录，Studio 将引导您创建交付组。

管理计算机目录

April 7, 2023

简介

可以在计算机目录中添加或删除计算机、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了最新的操作系统更新。包括防病毒更新、操作系统升级或配置更改。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 包含使用 Machine Creation Services (MCS) 创建的池随机目录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。此方法使您能够有效地更新大量用户计算机。
- 对于使用 Citrix Provisioning 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 Citrix Provisioning 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，请在 Studio 外部管理用户计算机的更新。请使用第三方软件分发工具以单独或集中方式执行此操作。

有关创建和管理与主机虚拟机管理程序的连接的信息，请参阅连接和资源。

> 注意：
>
> MCS 不支持 Windows 10 IoT 核心版和 Windows 10 IoT 企业版。请参阅 Microsoft 站点以了解详细信息。

关于永久实例

在更新使用永久或专用实例创建的 MCS 目录时，为该目录创建的任何新计算机将使用更新后的映像。预先存在的实例将继续使用原始实例。更新映像的过程与更新任何其他类型的目录的方式相同。请注意以下事项：

- 使用永久磁盘目录时，预先存在的计算机不会更新到新的映像，但是添加到该目录中的任何新计算机将使用新映像。
- 对于非永久磁盘目录，下次重置计算机时将更新计算机映像。
- 使用永久计算机目录时，更新映像也将更新使用它的目录实例。
- 对于不会永久存在的目录，如果您希望不同的计算机使用不同的映像，则映像必须位于单独的目录中。

向目录中添加计算机

开始之前：

- 确保虚拟化主机具有足够多的处理器、内存和存储空间来容纳更多的计算机。
- 确保有足够多的未使用 Active Directory 计算机帐户。如果要使用现有帐户，可以添加的计算机数受可用帐户数限制。
- 如果使用 Studio 为更多计算机创建 Active Directory 计算机帐户，必须具有相应的域管理员权限。

向目录中添加计算机：

1. 在 **Studio** 导航窗格中选择计算机目录。
2. 选择计算机目录，然后在操作窗格中选择添加计算机。
3. 选择要添加的虚拟机数。
4. 如果现有 Active Directory 帐户的数量不足，无法容纳要添加的 VM 数量，请选择要在其中创建帐户的域和位置。指定帐户命名方案，并使用井号来表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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。Studio 将管理这些帐户。允许 Studio 重置所有帐户的密码或者指定帐户密码，所有帐户的密码都必须相同。

系统会将计算机创建过程作为后台进程来执行，创建许多计算机时，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，请指示保留、禁用还是删除这些计算机的 Active Directory 帐户。

更改目录说明或更改 **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. 对于 Remote PC Access 目录，请使用电源管理页面更改电源管理设置并选择电源管理连接。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。

将目录移动到其他区域

如果您的部署包含多个区域，可以将某个目录从一个区域移动到另一个区域。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。

删除目录

删除编录之前，请确保：

- 所有用户均已注销且没有仍在运行的已断开连接的会话。
- 该目录中的所有计算机均已打开维护模式，以便无法建立新连接。
- 该目录中的所有计算机均已关闭。
- 该目录不与交付组关联。即，交付组不包含该目录中的计算机。

要删除目录，请执行以下操作：

1. 在 **Studio** 导航窗格中选择计算机目录。
2. 选择一个目录，然后在操作窗格中选择删除计算机目录。
3. 指明是否删除目录中的计算机。如果选择删除计算机，请指示保留、禁用还是删除这些计算机的 Active Directory 计算机帐户。

管理目录中的 **Active Directory** 计算机帐户

要管理计算机目录中的 Active Directory 帐户，可以：

- 从单会话操作系统和多会话操作系统目录中删除 Active Directory 计算机帐户，从而释放未使用的计算机帐户。之后，这些帐户便可用于其他计算机。
- 添加帐户，以便在向此目录添加更多计算机时，有可用的计算机帐户。请勿在 OU 名称中使用正斜杠 (/)。

管理 Active Directory 帐户：

1. 在 **Studio** 导航窗格中选择计算机目录。
2. 选择一个目录，然后在操作窗格中选择管理 **AD** 帐户。
3. 选择是添加还是删除计算机帐户。如果添加帐户，请指定帐户密码的处理方式：重置所有密码还是输入一个适用于所有帐户的密码。

   如果不知道当前的帐户密码，则可能需要重置密码；必须具有重置密码的权限。输入密码时，该密码会在系统导入帐户时发生变化。删除帐户时，请选择在 Active Directory 中保留、禁用还是删除帐户。

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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

更新目录

我们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。回滚或还原目录中的计算机以使用早期版本的主映像。如果用户在部署到其桌面的更新中遇到问题，请执行此任务。这样可以最大限度地减少用户的停机时间。不要对主映像进行删除、移动或重命名。您无法还原目录以进行使用。

对于使用 Citrix Provisioning（以前称为 Provisioning Services）的目录，必须发布新虚拟磁盘才能将更改应用于该目录。有关详细信息，请参阅 Citrix Provisioning 文档。

更新计算机后，计算机将自动重新启动。

更新或创建主映像

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主映像。

1. 在您的虚拟机管理程序中，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. 关闭 VM 的电源。
5. 截取 VM 的快照。为其提供一个能够在 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，但 Citrix 仍建议您使用虚拟机管理程序管理控制台进行创建。然后在 Studio 中选择该快照。执行此过程可以提供有意义的名称和说明，而非自动生成的名称。对于 GPU 主映像，只能通过 Citrix Hypervisor 控制台进行更改。

更新目录

准备并前滚目录中的所有计算机的更新：

1. 在 **Studio** 导航窗格中选择计算机目录。
2. 选择一个目录，然后在操作窗格中选择更新计算机。
3. 在主映像页面上，选择要前滚的主机和映像。
4. 在前滚策略页面上，选择使用新主映像更新计算机目录中计算机的时间：下次关闭时或立即。
5. 确认摘要页面上的信息，然后单击完成。每台计算机都在更新后自动重新启动。

直接使用 PowerShell SDK（而非使用 Studio）更新目录时，请指定虚拟机管理程序模板 (VMTemplates)。将其用作图像或图像快照的替代方法。

前滚策略：

下次关闭时更新映像将立即影响当前未使用的任何计算机，即，没有任何活动用户会话的计算机。正在使用的系统在当前活动会话结束时接收更新。请注意以下事项：

- 在适用的计算机上完成更新之前，无法启动新会话。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 对于单会话操作系统计算机，计算机未在使用或用户未登录时，将立即更新计算机。
- 对于包含子计算机的多会话操作系统，重新引导不会自动发生。必须手动将其关闭并重新启动。

> 提示：
>
> 可以通过主机连接的高级设置来限制要重新引导的计算机数量。使用这些设置可以修改针对给定目录执行的操作；高级设置因虚拟机管理程序而异。

如果选择立即更新映像，请配置分发时间和通知。

- 分发时间：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。内部算法决定该间隔时间内每台计算机的更新时间和重新启动时间。
- 通知：在左侧的通知下拉菜单中，选择是否在更新开始之前在计算机上显示通知消息。默认情况下，不显示任何消息。选择在更新开始前 15 分钟显示消息。或者，选择在初始消息发送后每五分钟重复发送一次消息。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。

回滚更新

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，此过程可能很有必要。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. 按上文前滚操作部分中所述，指定对计算机应用早期主映像的时间。

回滚仅适用于需要还原的计算机。尚未使用新的/更新后的主映像进行更新的计算机不会收到通知消息，也不会被强制注销。

升级目录或还原升级

在将计算机上的 VDA 升级到更新版本之后，可以升级计算机目录。Citrix 建议您将所有 VDA 升级到最新版本，以使其能够访问所有最新的功能。

升级目录之前，请执行以下操作：

- 如果您使用的是 Citrix Provisioning，请升级 VDA 版本。Provisioning 控制台不保留 VDA 版本。Citrix Provisioning 直接与 Citrix Virtual Apps and Desktops 设置向导进行通信，以在创建的目录中设置 VDA 版本。
- 启动升级后的计算机，使其注册到 Controller 中。此过程允许 Studio 确定目录中的计算机是否需要升级。

要升级目录，请执行以下操作：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. 在 **Studio** 导航窗格中选择计算机目录。
2. 选择目录。下部窗格中的详细信息选项卡会显示版本信息。
3. 选择升级目录。如果 Studio 检测到目录需要升级，它会显示一条消息。按照提示进行操作。如果一台或多台计算机无法升级，则消息中会说明原因。Citrix 建议您在升级目录前解决计算机问题，以确保所有计算机均正常运行。

目录升级完成后，您可以通过选择该目录，然后在操作窗格中选择撤消，将计算机还原到其先前的 VDA 版本。

故障排除

- 对于状态为“电源状态未知”的计算机，请参阅 CTX131267 了解指导信息。
- 要修复持续显示未知电源状态的 VM，请参阅如何修复持续显示未知电源状态的 VM。

创建交付组

January 21, 2022

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。稍后，可以更改第一个交付组中的初始设置并创建其他交付组。还有一些功能和设置只能在编辑交付组（而非创建交付组）时进行配置。

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. 如果您创建了站点和计算机目录，但未创建交付组，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，并且希望再创建一个，请选择交付组。在“操作”窗格中选择创建交付组。
2. 此时将启动向导，并打开一个简介页面，您可以在将来启动此向导时不再显示该页面。
3. 该向导随后将引导您完成以下部分中所述的页面。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。

步骤 **1.** 计算机

在计算机页面上，选择一个目录并选择要从该目录中使用的计算机数。

须知：

- 在选定的目录中，必须至少有一台计算机处于未使用状态。
- 可以在多个交付组中指定目录。只能在一个交付组中使用计算机。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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（多会话操作系统、单会话操作系统或 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 建议您使用最新版 VDA 安装或升级所有计算机。根据需要升级目录和交付组。创建交付组时，如果选择安装了不同 VDA 版本的多台计算机，交付组将与最早版本的 VDA 兼容。这就是所谓的组的功能级别。例如，如果其中一台计算机安装了 VDA 7.1，其他计算机安装了当前版本，则组中的所有计算机只能使用 VDA 7.1 中支持的功能。这意味着，在该交付组中可能无法使用需要更高版本的 VDA 的某些功能。
- Remote PC Access 目录中的每台计算机都自动与交付组关联。创建 Remote PC Access 站点时，将自动创建一个名为“Remote PC Access 计算机”的目录和一个名为“Remote PC Access 桌面”的交付组。
- 执行以下兼容性检查：
  - MinimumFunctionalLevel 必须兼容
  - SessionSupport 必须兼容
  - AllocationType 必须与 SingleSession 兼容
  - ProvisioningType‘ 必须兼容
  - PersistChanges 必须与 MCS 和 Citrix Provisioning 兼容
  - RemotePC 目录仅与 RemotePC 目录兼容
  - AppDisk 相关检查

步骤 **2.** 交付类型

只有选择了包含静态（已分配）单会话操作系统计算机的目录后，才会显示此页面。

在交付类型页面上，选择应用程序或桌面。不能同时启用这两者。

如果您是从多会话操作系统或单会话操作系统随机（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。

步骤 **3.** 用户

指定能够使用交付组中的应用程序和桌面的用户和用户组。

指定了用户列表的位置

Active Directory 用户列表在您创建或编辑以下内容时指定：

- 站点的用户访问列表（不通过 Studio 配置）。默认情况下，应用程序授权策略规则包括所有人。有关详细信息，请参阅 PowerShell SDK `BrokerAppEntitlementPolicyRule` cmdlet。
- 应用程序组（如果已配置）。
- 交付组。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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，要将应用程序 A 配置为由特定部门使用，但不过分限制对其他组的访问，请执行以下操作：

- 使用包括所有人的默认应用程序授权策略规则。
- 配置交付组用户列表以允许所有总部用户使用在交付组中指定的任何应用程序。
- （如果已配置应用程序组）配置应用程序组用户列表，以允许行政和财务业务部门的成员访问应用程序 A-L。
- 配置应用程序 A 的属性，使其仅对行政和财务业务部的应收账款业务工作人员可见。

已通过身份验证的用户和未经身份验证的用户

用户类型有两种：已通过身份验证和未经身份验证（后者也称为匿名）。您可以在交付组中配置其中一种类型或这两种类型。

- 已通过身份验证：按名称指定的用户和组成员必须向 StoreFront 或 Citrix Workspace 应用程序提供凭据（例如智能卡或用户名和密码），才能访问应用程序和桌面。对于包含单会话操作系统计算机的交付组，您可以稍后通过编辑交付组来导入用户数据（用户列表）。
- 未经身份验证（匿名）：对于包含多会话操作系统计算机的交付组，可以允许用户访问应用程序和桌面，而不需要向 StoreFront 或 Citrix Workspace 应用程序提供凭据。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凭据。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 Anon*XYZ*，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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

步骤 **4.** 应用程序

须知：

- 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位于 Applications 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。
- 在将某个应用程序添加到多个交付组中时，如果您没有足够的权限来查看所有这些交付组中的该应用程序，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。
- 如果向相同的用户发布两个同名的应用程序，请在 Studio 中更改“应用程序名称 (面向用户)”属性；否则，用户将在 Citrix Workspace 应用程序中看到重复的名称。

单击添加以显示应用程序源。

- 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：位于站点上或网络中的其他位置的应用程序。选择此源会启动一个新页面，您可以在其中键入可执行文件的路径、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，单击确定。
- 现有：先前已添加到站点中的应用程序，可能位于另一个交付组中。当您选择该源时，会打开一个新页面，其中包含已发现的应用程序的列表。添加应用程序，然后单击确定。
- **App-V**：App-V 包中的应用程序。如果选择此源，则会启动一个新页面，您可以在其中选择 App-V 服务器或应用程序库。从生成的显示内容中选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。

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目录中计算机支持的会话类型不兼容。

步骤 **5.** 桌面

此页面的标题取决于计算机页面上选择的目录：

- 如果所选目录包含池计算机，则此页面的标题为桌面。
- 如果所选目录包含已分配的计算机，并且在交付类型页面上指定了“桌面”，则此页面标题为 **Desktop User Assignment**（桌面用户分配）。
- 如果所选目录包含已分配的计算机，并且在交付类型页面上指定了“应用程序”，则此页面的标题为 **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：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 在显示名称和说明字段中，输入要在 Citrix Workspace 应用程序中显示的信息。
- 要向桌面添加标记限制，请选择限制启动带标记的计算机，然后从下拉列表中选择标记。有关详细信息，请参阅标记。
- 启动桌面时，使用单选按钮可启动桌面或分配计算机。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。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）。禁用桌面会停止桌面交付。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。

站点中桌面的最大实例数（仅限 **PowerShell**）

要配置站点中桌面的最大实例数（仅限 PowerShell），请执行以下操作：

- 在 PowerShell 中，使用带 MaxPerEntitlementInstances 参数的相应 BrokerEntitlementPolicyRule cmdlet。例如，以下 cmdlet 修改 `tsvda-desktop` 规则，以将站点中允许的桌面最大并发实例数设置为 2。有两个桌面实例正在运行时，如果第三个订阅者尝试启动桌面，将出现错误。

  ```
  Set-BrokerEntitlementPolicyRule -Name tsvda-desktop -MaxPerEntitlementInst
    2
  ```

- 有关指导，请使用 Get-Help cmdlet。例如，`Get-Help Set-BrokerEntitlementPolicyRule -Parameter MaxPerEntitlementInstances`。

步骤 **6.** 摘要

输入交付组的名称。您也可以（选择）输入说明，该说明显示在 Citrix Workspace 应用程序和 Studio 中。

查看摘要信息，然后单击完成。

管理交付组

November 17, 2022

简介

本文介绍了从管理控制台管理交付组的过程。除了更改在创建组时指定的设置，您还可以配置在创建交付组对您不可用的其他设置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

过程类别包括：常规、用户、计算机和会话。某些任务跨越多个类别。例如，“阻止用户连接到计算机”在计算机类别中进行介绍，但还会影响用户。如果您在一种类别中找不到某项任务，请检查相关的类别。

其他文章还包含相关的信息：

- 应用程序中包含与如何管理交付组中的应用程序有关的信息。
- 管理交付组需要“交付组管理员”内置角色权限。有关详细信息，请参阅委派管理。

常规

- 更改交付类型
- 更改 StoreFront 地址
- 升级交付组
- 管理 Remote PC Access 交付组

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，请从组中删除所有应用程序。

1. 在导航窗格中选择交付组。
2. 选择一个组，然后在“操作”窗格中单击编辑交付组。
3. 在交付类型页面上，选择所需的交付类型。
4. 单击应用以应用所做的任何更改并使窗口保持打开状态。或者，单击确定应用所做的更改并关闭窗口。

更改 **StoreFront** 地址

1. 在导航窗格中选择交付组。
2. 选择一个组，然后在“操作”窗格中单击编辑交付组。
3. 在 **StoreFront** 页面上，选择或添加 StoreFront URL。这些 URL 由交付组中的每台计算机上安装的 Citrix Workspace 应用程序使用。
4. 单击应用以应用所做的任何更改并使窗口保持打开状态。或者，单击确定应用所做的更改并关闭窗口。

也可以通过在导航窗格中选择配置 **> 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 Virtual Delivery Agent (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：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 如果使用 Citrix Provisioning（以前称为 Provisioning Services），请在 Citrix Provisioning 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。此过程将指示控制台交付组中需要升级的内容。
- 如果继续使用早期的 VDA 版本，更新的产品功能将不可用。有关详细信息，请参阅升级文档。

要升级交付组，请执行以下操作：

1. 在导航窗格中选择交付组。
2. 选择一个组，然后在“操作”窗格中单击升级交付组。仅当检测到已升级的 VDA 时才会显示升级交付组操作。

显示内容指示哪些（如果有）计算机无法升级以及原因。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，可以通过选择交付组，然后在操作窗格中单击撤消，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 计算机目录中的某个计算机未分配，则会暂时将该计算机分配给与该目录关联的交付组。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时或用户需要计算机分配时向计算机分配的交付组。值越小，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。请使用 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。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. 在详细信息部分中，单击计算机目录选项卡，然后选择 Remote PC Access 目录。
4. 要添加或还原关联，请单击添加桌面。要删除关联，请单击删除关联。

用户

- 更改用户设置
- 添加或删除用户

更改交付组中的用户设置

此页面的名称显示为用户设置或基本设置。

1. 在导航窗格中选择交付组。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. 选择一个组，然后在“操作”窗格中单击编辑交付组。
3. 在用户设置（或基本设置）页面上，更改下表中的任何设置。
4. 单击应用以应用所做的任何更改并使窗口保持打开状态。或者，单击确定应用所做的更改并关闭窗口。

设置	说明
说明	Citrix Workspace（或 StoreFront）使用的并且用户能够看到的文本。
启用交付组	是否启用交付组。
时区	此交付组的计算机必须所在的时区。该选项列出了站点支持的时区。
启用 Secure ICA	通过用于加密 ICA 协议的 SecureICA 保护与交付组中的计算机之间的通信。默认级别为 128 位。可以使用 SDK 更改该级别。Citrix 建议在遍历公共网络时使用更多加密方法（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，请参阅用户。

1. 在导航窗格中选择交付组。
2. 选择一个组，然后在“操作”窗格中单击编辑交付组。
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。
   - 选中或取消选中该复选框以允许未经身份验证的用户进行访问。
4. 单击应用以应用所做的任何更改并使窗口保持打开状态。或者，单击确定应用所做的更改并关闭窗口。

导入或导出用户列表　对于包含物理单会话操作系统计算机的交付组，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（按任意顺序排列），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. 在导航窗格中选择交付组。
2. 选择一个组，然后在“操作”窗格中单击编辑交付组。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. 在计算机分配页面上，选择导入列表或导出列表，然后浏览到文件位置。
4. 单击应用以应用所做的任何更改并使窗口保持打开状态。或者，单击确定应用所做的更改并关闭窗口。

计算机

- 更改用户的计算机分配情况
- 更改每个用户的最大计算机数
- 更新计算机
- 为桌面添加、更改或删除标记限制
- 删除计算机
- 限制访问计算机
- 阻止用户连接到计算机（维护模式）
- 关闭和重新启动计算机
- 为计算机创建和管理重新启动计划
- 负载托管计算机
- 电源托管计算机

更改为交付组中的用户分配的计算机

可以更改通过 MCS 预配的单会话操作系统计算机的分配。不能更改多会话操作系统计算机或通过 Citrix Provisioning 预配的计算机的分配。

1. 在导航窗格中选择交付组。
2. 选择一个组，然后在“操作”窗格中单击编辑交付组。
3. 在桌面或桌面分配规则页面（页面标题取决于交付组使用的计算机目录的类型）上，指定新用户。
4. 单击应用以应用所做的任何更改并使窗口保持打开状态。或者，单击确定应用所做的更改并关闭窗口。

更改交付组中每个用户的最大计算机数

1. 在导航窗格中选择交付组。
2. 选择一个组，然后在“操作”窗格中单击编辑交付组。
3. 在桌面分配规则页面上，设置“每个用户的最大桌面数”值。
4. 单击应用以应用所做的任何更改并使窗口保持打开状态。或者，单击确定应用所做的更改并关闭窗口。

更新交付组中的计算机

1. 在导航窗格中选择交付组。
2. 选择一个组，然后在“操作”窗格中单击查看计算机。
3. 选择一台计算机，然后在“操作”窗格中单击更新计算机。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

要选择其他映像，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的前滚通知。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（开始更新组中所有计算机的总时间）
- 用户是否收到重新启动通知
- 用户收到的消息

为桌面添加、更改或删除标记限制

添加、更改和删除标记限制可能会对被考虑启动的桌面有意外的影响。请查看标记中的注意事项和警告。

1. 在导航窗格中选择交付组。
2. 选择一个组，然后在“操作”窗格中单击编辑交付组。
3. 在桌面页面上，选择桌面并单击编辑。
4. 要添加标记限制，请选择限制启动带标记的计算机，然后选择标记。
5. 要更改或删除标记限制，可以执行以下操作：
    - 选择一个不同的标记。
    - 通过取消选中限制启动带标记的计算机删除标记限制。
6. 单击应用以应用所做的任何更改并使窗口保持打开状态。或者，单击确定应用所做的更改并关闭窗口。

从交付组中删除计算机

删除某个计算机还会将其从交付组中删除。不会将其从交付组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。

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。请考虑重新创建计算机的映像。

1. 在导航窗格中选择交付组。
2. 选择一个组，然后在“操作”窗格中单击查看计算机。
3. 请确保所有计算机都已关闭。
4. 选择计算机，然后在“操作”窗格中单击从交付组中删除。

此外，也可以通过计算机所采用的连接来删除交付组中的计算机。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

限制对交付组中计算机的访问

无论使用何种方法，为限制访问交付组中的计算机所做的任何更改都将取代以前的设置。您可以：

- 使用委派管理作用域限制管理员的访问权限：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。
- 使用 **SmartAccess** 策略表达式限制用户的访问权限：可使用策略表达式过滤通过 Citrix Gateway 建立的用户连接。

  1. 在导航窗格中选择交付组。
  2. 选择一个组，然后在“操作”窗格中单击编辑交付组。
  3. 在访问策略页面上，选择通过 **NetScaler Gateway** 的连接。
  4. 要选择这些连接中的一部分，请选择满足以下任意过滤器条件的连接。然后定义 Citrix 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 Citrix Gateway 文档。
  5. 单击应用以应用所做的任何更改并使窗口保持打开状态。或者，单击确定应用所做的更改并关闭窗口。

- 通过排除过滤器限制用户的访问权限：可对您在 SDK 中设置的访问策略使用排除过滤器。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，出于安全考虑，可以拒绝对一部分用户或设备进行访问。默认情况下，排除过滤器处于禁用状态。

  例如，企业网络子网中的一个教学实验室，该子网阻止从该实验室访问特定交付组。无论是谁在使用该实验室中的计算机，都请使用以下命令：`Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -`。

  使用星号 (*) 通配符来匹配以相同策略表达式开头的所有标记。例如，如果在一台计算机中添加标记 `VPDesktops_Direct`，在另一台计算机中添加标记 `VPDesktops_Test`，则在 `Set-BrokerAccessPolicy` 脚本中将标记设置为 `VPDesktops_*` 将同时适用于这两台计算机的过滤器。

  如果您是使用 Web 浏览器或者通过在应用商店中启用的 Citrix Workspace 应用程序用户体验功能连接的，则不能使用客户端名称排除过滤器。

禁止用户连接到交付组中的计算机（维护模式）

当您需要临时停止计算机的新连接时，可以针对交付组中的一个或所有计算机打开维护模式。您可能会在应用修补程序或使用管理工具之前执行此操作。

- 当多会话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。
- 当单会话操作系统计算机（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：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. 在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”窗格中单击打开维护模式。

   要为一台计算机打开维护模式，请在“操作”窗格中单击查看计算机。选择计算机，然后在“操作”窗格中单击打开维护模式。
4. 要针对交付组中的一台或所有计算机关闭维护模式，请按照之前的说明操作，但要在“操作”窗格中单击择关闭维护模式。

Windows 远程桌面连接 (RDC) 设置还影响多会话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 未设置为 **Don’t allow connections to this computer**（不允许连接到这台计算机）。**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）。

也可以针对以下计算机打开或关闭维护模式：

- 连接，影响使用该连接的计算机。
- 计算机目录，影响该目录中的计算机。

关闭并在重新启动交付组中的计算机

Remote PC Access 计算机不支持此过程。

1. 在导航窗格中选择交付组。
2. 选择一个组，然后在“操作”窗格中单击查看计算机。
3. 选择计算机，然后在“操作”窗格中单击以下条目之一：
   - 强制关闭：强制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 建议阻止单会话操作系统计算机用户在会话中选择关闭。有关详细信息，请参阅 Microsoft 策略文档。

您也可以关闭并重新启动连接中的计算机。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

在交付组中创建和管理计算机的重新启动计划

重新启动计划指定定期重新启动交付组中的计算机的时间。您可以为交付组创建一个或多个计划。计划会影响：

- 组中的所有计算机。
- 组中的一个或多个（但并非所有）计算机。计算机由应用于计算机的标记识别。这称为标记限制，因为标记会将某个操作限制为仅具有该标记的项目。

例如，假设您的所有计算机都位于一个交付组中。您希望每周重新启动一次所有计算机，并且希望核算团队使用的计算机每天重新启动。要实现这一点，请为所有计算机设置一个计划，并为仅用于核算的计算机设置另一个计划。

计划包括重新启动开始的日期和时间，以及持续时间。

您可以启用或禁用计划。在测试时、特殊间隔期间或在需要之前准备计划时，禁用计划可能非常有用。

不能在管理控制台中使用用于自动开机或关机的计划，只能用于重新启动。

计划重叠　多个计划可以重叠。在上例中，两个计划都会影响核算计算机。这些计算机可能会在星期日重新启动两次。可设计计划规范避免重新启动相同计算机的次数超过需要的次数，但无法保证。

- 如果两个计划的开始时间和持续时间完全一致，则很可能将只重新启动一次计算机。
- 计划在开始时间和持续时间上越不同，越有可能发生多次重新启动。
- 受计划影响的计算机数也会影响重叠的可能性。在该示例中，影响所有计算机的每周计划启动重新启动的速度可能快于核算计算机的每日计划，具体取决于为每个计划指定的持续时间。

有关重新启动计划的深度探讨，请参阅 Reboot schedule internals（重新启动计划内部）。

查看重新启动计划

1. 在导航窗格中选择交付组。
2. 选择一个组，然后在“操作”窗格中单击编辑交付组。
3. 选择重新启动计划页面。

重新启动计划页面包含每个已配置计划的以下信息：

- 计划名称。
- 使用的标记限制（如果有）。
- 计算机重新启动的频率。
- 计算机用户是否收到通知。
- 是否启用计划。

添加（应用）标记　配置使用标记限制的重新启动计划时，请确保将该标记添加到该计划要影响的计算机。在上例中，核算团队使用的每个计算机都应用了标记。有关详细信息，请参阅标记。

虽然您可以将多个标记应用到计算机，但是重新启动计划只能指定一个标记。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. 在导航窗格中选择交付组。
2. 选择包含受计划控制的计算机的组。
3. 单击查看计算机，然后选择要为其添加标记的计算机。
4. 在“操作”窗格中单击管理标记。
5. 如果标记存在，请启用标记名称旁边的复选框。如果标记不存在，请单击创建，然后指定标记名称。创建标记后，启用新建标记名称旁边的复选框。
6. 在管理标记对话框中单击保存。

创建重新启动计划

1. 在导航窗格中选择交付组。
2. 选择一个组，然后在“操作”窗格中单击编辑交付组。
3. 在重新启动计划页面上，单击添加。
4. 在添加重新启动计划页面上：
   - 键入计划名称和描述。
   - 如果您使用的标记限制，请选择该标记。
   - 在重新启动频率中，选择重新启动发生的频率：每日、工作日、周末或每周的特定一天。
   - 使用 24 小时制指定开始重新启动的时间。
   - 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所有受影响计算机的总时长。内部算法确定该间隔内每台计算机的重新启动时间。

     > 注意：
     >
     > 使用 PowerShell 时，还可以选择另一个重新启动持续时间。请参阅耗尽后重新启动。

   - 在向用户发送通知中，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，可以在 Notification frequency（通知频率）中选择在第一次显示消息之后每 5 分钟重复显示此消息一次。默认情况下，该消息不重复显示。
   - 输入通知标题和文本。不存在默认文本。

     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%**。例如：“警告: 您的计算机将在%m% 分钟后自动重新启动。”对于每条重复显示的消息，该值会减去 5 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），每台计算机上均会显示消息。
   - 要启用该计划，请选中该复选框。要禁用该计划，请取消选中该复选框。
5. 单击应用以应用所做的更改并使窗口保持打开状态。或者，单击确定应用所做的更改并关闭窗口。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

耗尽后重新启动　使用 PowerShell 创建或更新计算机重新启动计划（`New-BrokerRebootSchedulev2` 或 `Set-BrokerRebootSchedulev2`）时，可以使用另一个重新启动持续时间值。

使用 `-UseNaturalReboot <Boolean>` 参数启用耗尽后重新启动功能时，将在耗尽所有会话后重新启动所有计算机。到达重新启动时间后，计算机将进入耗尽状态，然后在注销所有会话时重新启动。

包含单会话或多会话计算机的交付组支持此功能。计算机必须进行电源管理。

在本地环境中，仅当使用 PowerShell 时才支持此功能。该功能在 Studio 中不可用。

编辑、删除、启用或禁用重新启动计划

1. 在导航窗格中选择交付组。
2. 选择一个组，然后在“操作”窗格中单击编辑交付组。
3. 在重新启动计划页面上，选中与计划对应的复选框。
    - 要编辑计划，请单击编辑。使用创建重新启动计划中的指南更新计划配置。
    - 要启用或禁用计划，请单击编辑。选中或取消选中启用重新启动计划复选框。
    - 要删除计划，请单击删除。确认删除。删除计划不影响应用于受影响计算机中的计算机的任何标记。

计划的重新启动因数据库中断而延迟

> 注意：
>
> 此功能仅在 PowerShell 中可用。

如果对交付组中的计算机 (VDA) 开始计划的重新启动之前发生站点数据库中断，则重新启动将在中断结束后开始。这可能会产生意想不到的结果。

例如，假设您已安排交付组在非生产时间（从 03:00 开始）重新启动。站点数据库会在计划的重新启动开始前一小时 (02:00) 发生中断。中断将持续六个小时（直到 08:00）。重新启动计划将在 Delivery Controller 和站点数据库之间的连接恢复后开始。VDA 现在在原始计划五小时后重新启动，导致 VDA 在生产时间内重新启动。

为避免出现这种情况，您可以使用 `New-BrokerRebootScheduleV2` 和 `Set-BrokerRebootScheduleV2` cmdlet 的 `MaxOvertimeStartMins` 参数。该值指定重新启动计划可以在计划的开始时间之后多久开始的最大分钟数。

- 如果数据库连接在该时间（计划时间 + `MaxOvertimeStartMins`）内恢复，则将开始重新启动 VDA。
- 如果数据库连接未在该时间内恢复，则 VDA 不会开始重新启动。
- 如果忽略此参数或者此参数的值为零，计划的重新启动将在恢复与数据库的连接时开始，无论中断持续时间如何都是如此。

有关详细信息，请参阅 cmdlet 帮助。此功能仅在 PowerShell 中可用。在 Studio 中配置重新启动计划时，无法设置此值。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

对处于维护模式的计算机执行计划的重新启动

> 注意：
>
> 此功能仅在 PowerShell 中可用。

要指示重新启动计划是否影响处于维护模式的计算机，请将 `IgnoreMaintenanceMode` 选项与 `BrokerRebootScheduleV2` cmdlet 结合使用。

例如，以下 cmdlet 将创建一个计划，用于重新启动处于维护模式的计算机（以及未处于维护模式的计算机）。

```
New-Brokerrebootschedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup
> -IgnoreMaintenanceMode $true
```

以下 cmdlet 修改现有的重新启动计划。

```
Set-Brokerrebootschedulev2 rebootSchedule1 -IgnoreMaintenanceMode
$true
```

有关详细信息，请参阅 cmdlet 帮助。此功能仅在 PowerShell 中可用。

交付组中的负载托管计算机

只能对多会话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，才考虑将多会话操作系统计算机用于负载平衡。
- 服务器负载指数：确定交付多会话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。

  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不可用。

  可以在 Director（监视）、Studio（管理）搜索和 SDK 中监视负载指数。

  在控制台的显示屏幕中，要显示服务器负载指数列（默认处于隐藏状态），请选择一台计算机，右键单击列标题，然后选择选择列。在计算机目录中，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。
- 并发登录容差策略设置：登录服务器的最大并发请求数。（在 XenApp 6.x 版本中，此设置等效于负载限制。）

  所有服务器都等于或高于并发登录容错设置时，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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

交付组中的电源托管计算机

只能对虚拟单会话操作系统计算机进行电源管理，不能对物理机（包括 Remote PC Access 计算机）进行电源管理。具有 GPU 功能的单会话操作系统计算机无法挂起，因此关机操作失败。对于多会话操作系统计算机，您可以创建重新启动计划。

在包含池计算机的交付组中，虚拟单会话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，虚拟单会话操作系统计算机可以：

- 永久分配并且正在使用
- 永久分配并且未连接（但已就绪）
- 未分配并且未连接

在正常使用期间，静态交付组通常既包括永久分配的计算机，也包括未分配的计算机。最初，所有计算机均未分配（创建交付组时手动分配的计算机除外）。当用户连接时，计算机变为永久分配状态。您可以对这些交付组中的未分配计算机进行全面的电源管理，但对永久分配的计算机却只能进行部分管理。

- 池和缓冲区：对于包含未分配计算机的池交付组和静态交付组，池（在这种情况下）是一组保持为开启状态以供用户连接的未分配或临时分配的计算机。用户在登录后将立刻获得计算机。池大小（保持为启动状态的计算机数）可按一天中的具体时刻进行配置。对于静态交付组，请使用 SDK 配置池。

  缓冲区是一组额外的未分配的备用计算机，在池中的计算机数低于阈值时打开。阈值是指交付组大小的百分比。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，或者使用 SDK 调整默认缓冲区大小。

- 电源状态计时器：您可以使用电源状态计时器在用户断开连接指定时间后挂起计算机。例如，在非工作时间，计算机将在用户断开连接至少 10 分钟后自动挂起。

  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，但无法设置池或缓冲区。这些计算机在每个高峰期到来时打开，在每个非高峰期到来时关闭。您无法像处理未分配计算机那样精细控制用来补偿被占用计算机的可用计算机数。

对虚拟单会话操作系统计算机进行电源管理

1. 在导航窗格中选择交付组。
2. 选择一个组，然后在“操作”窗格中单击编辑交付组。
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，单击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. 在高峰时段中，设置每天的高峰时段和非高峰时段。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. 设置工作日高峰时段和非高峰时段的电源状态计时器：在高峰期间 **>** 断开连接时中，指定挂起交付组中任何已断开连接的计算机前的延迟时间（分钟），然后选择挂起。在非高峰期间 **>** 断开连接时中，指定关闭交付组中任何已注销计算机前的延迟时间，然后选择关闭。此计时器不可用于具有随机计算机的交付组。
7. 在对计算机进行电源管理中选择周末，然后配置周末的高峰时段和电源状态计时器。
8. 单击应用以应用所做的任何更改并使窗口保持打开状态。或者，单击确定应用所做的更改并关闭窗口。

使用 SDK 可以执行以下操作：

- 关闭而非挂起计算机以响应电源状态计时器，或者在希望计时器基于注销数而非断开连接数时使用。
- 更改默认的工作日和周末定义。
- 禁用电源管理。请参阅 CTX217289。

对断开连接的会话转换到不同时间段的 **VDI** 计算机进行电源管理

> 重要：
>
> 此增强功能仅适用于具有断开连接的会话的 VDI 计算机。它不适用于具有注销会话的 VDI 计算机。

在早期版本中，转换到需要执行某项操作（断开连接操作为暂停或关闭）的时间段的 VDI 计算机仍保持打开状态。如果计算机在不需要执行任何操作（断开连接操作 = 无）的时间段（高峰时间或非高峰时间）断开连接，则会出现此情况。

自 Citrix Virtual Apps and Desktops 7 1909 起，在指定的断开连接时间过后，计算机将暂停或关闭电源，具体取决于为目标时间段配置的断开连接操作。

例如，可以为 VDI 交付组配置以下电源策略：

- 将 `PeakDisconnectAction` 设置为“无”
- 将 `OffPeakDisconnectAction` 设置为“关闭”
- 将 `OffPeakDisconnectTimeout` 设置为“10”

有关断开连接操作电源策略的详细信息，请参阅https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy和 https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/。

在早期版本中，在高峰时段会话断开连接的 VDI 计算机在从高峰时段过渡到非高峰时段保持打开电源状态。自 Citrix Virtual Apps and Desktops 7 1909 起，`OffPeakDisconnectAction` 和 `OffPeakDisconnectTimeout` 策略操作将在周期转换时应用到 VDI 计算机。因此，计算机在转换为非高峰 10 分钟后关闭电源。

如果要恢复到之前的行为（即，对于从高峰转换到非高峰或从非高峰转换到高峰并且会话断开连接的计算机不采取任何操作），请执行以下操作之一：

- 将 `LegacyPeakTransitionDisconnectedBehaviour` 注册表值设置为 1，相当于启用了先前行为的 *true*。默认情况下，值为 0 或 *false*，在周期转换时触发断开电源策略操作。
  - 路径：`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer`
  - 名称：`LegacyPeakTransitionDisconnectedBehaviour`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - 类型：REG_DWORD
  - 数据：0x00000001 (1)

- 使用 Set-BrokerServiceConfigurationData PowerShell 命令配置设置。例如：

  - PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true

计算机必须满足以下条件，才能在周期转换时对其应用电源策略操作：

- 具有断开连接的会话。
- 没有待处理的电源操作。
- 属于转换到不同时间段的 VDI（单会话）交付组。
- 具有在特定时间段（高峰或非高峰时段）断开连接的会话，并转换到分配了电源操作的时间段。

更改目录中处于打开状态的 **VDA** 的百分比

1. 调整交付组的电源管理部分中桌面组的高峰时段。
2. 记下桌面组名称。
3. 使用管理员权限启动 PowerShell 并运行以下命令。将“桌面组名称”替换为更改了正在运行的 VDA 百分比的桌面组的名称。

   ```
   asnp Citrix*

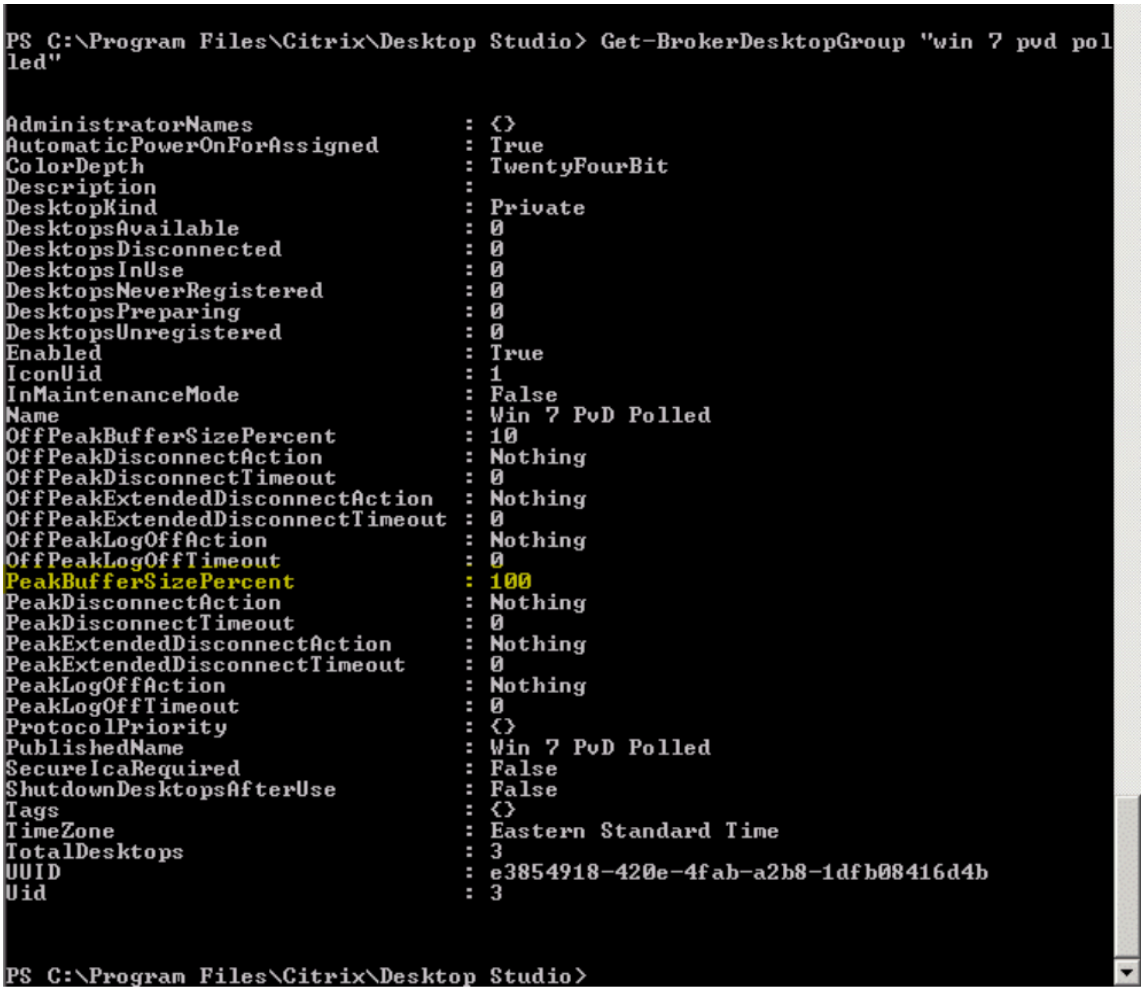
   # Set-BrokerDesktopGroup "Desktop Group Name"-PeakBufferSizePercent
    100
   ```

   值 100 表示所有 VDA 都处于已就绪状态。

4. 通过运行以下命令验证解决方案：

   ```
   #Get-BrokerDesktopGroup "Desktop Group Name"
   ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



可能需要长达一小时时间，更改才能生效。

要在用户注销后关闭 VDA，请输入：

```
# Set-BrokerDesktopGroup "Desktop Group Name"-ShutDownDesktopsAfterUse
 $True
```

要在高峰时段重新启动 VDA，以便其在用户注销后能够随时供用户使用，请输入：

```
# Set-BrokerDesktopGroup "Desktop Group Name"-AutomaticPowerOnForAssignedDurin
 $True
```

会话

- 注销或断开会话，或者向用户发送消息
- 配置会话预启动和会话延迟
- 在维护模式下从计算机断开连接时控制会话重新连接

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

注销会话或断开会话连接

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查看计算机。
3. 在中间窗格中，选择计算机，在操作窗格中选择查看会话，然后选择会话。
    - 或者，在中间窗格中，选择会话选项卡，然后选择一个会话。
4. 要从会话中注销，请在操作窗格中选择注销。会话将关闭，用户将注销。除非已将计算机分配给特定用户，否则该计算机可供其他用户使用。
5. 要断开会话连接，请在操作窗格中选择断开连接。应用程序继续在会话中运行，计算机仍分配给该用户。用户可以重新连接同一计算机。

您可以将单会话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，请参阅已进行电源管理的计算机。

向交付组发送消息

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查看计算机。
3. 在中间窗格中，选择要向其发送消息的计算机。
4. 在操作窗格中，选择查看会话。
5. 在中间窗格中，选择所有会话，然后在操作窗格中选择发送消息。
6. 键入您的消息，然后单击确定。如果需要，可以指定严重性级别。选项包括严重、问题、警告和信息。

或者，也可以使用 Citrix Director 发送消息。有关详细信息，请参阅向用户发送消息。

配置交付组中的会话预启动和会话延迟

只有多会话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，并在会话中的最后一个处于打开状态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适用于多会话操作系统的 VDA（最低版本为 7.6）。
- 这些功能仅在使用适用于 Windows 的 Citrix Workspace 应用程序时受支持，而且还需额外的 Citrix Workspace 应用程序配置。有关说明，请在您所用适用于 Windows 的 Citrix Workspace 应用程序版本对应的产品文档中搜索会话预启动。
- 不支持适用于 HTML5 的 Citrix Workspace 应用程序。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 Workspace 应用程序中注销，会话将结束，且预启动不再应用。
- 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并发许可证，但仅在连接时占用。如果使用用户/设备许可证，许可证将持续使用 90 天。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。此值可以在 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 Workspace 应用程序中配置每天预定时刻的会话预启动。

未使用的预启动会话和延迟会话保持活动状态的时长　如果用户未启动应用程序，可以通过多种方法指定未使用的会话保持活动状态的时长：已配置的超时和服务器负载阈值。您可以配置上述全部项。首先发生的事件会导致未使用的会话结束。

- 超时：配置的超时指定未使用的预启动或延迟会话保持活动状态的分钟数、小时数或天数。如果配置的超时过短，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。

  只能从 SDK (`New`/`Set-BrokerSessionPreLaunch` cmdlet) 启用此超时，不能从管理控制台启用。如果禁用了该超时，它将不会出现在该交付组的控制台显示或编辑交付组页面中。

- 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，它们会自动结束。

  您可以配置两个阈值：交付组中所有服务器的平均百分比负载和交付组中单个服务器的最大百分比负载。超过阈值时，时间最长的预启动或延迟会话将首先结束。其他会话则按分钟间隔逐个结束，直到负载降到阈值之下。超过阈值时，不启动新的预启动会话。

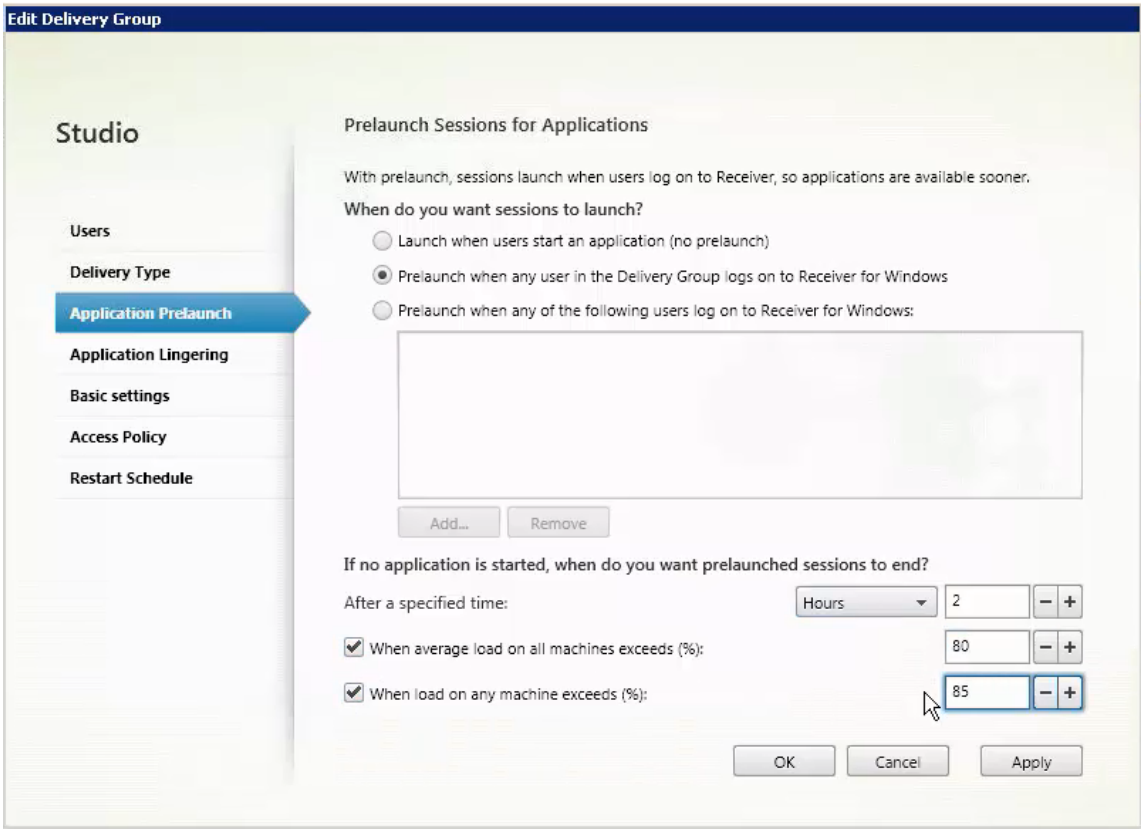
具有 VDA 且未向 Controller 注册的服务器和处于维护模式的服务器被视为全负载。计划外中断会导致预启动和延迟会话自动结束，从而释放容量。

启用会话预启动

1. 在导航窗格中选择交付组。
2. 选择一个组，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。会话预启动功能处于禁用状态。
   - 交付组中的任何用户登录适用于 Windows 的 Citrix Workspace 应用程序时。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 用户和用户组列表中的任何人登录适用于 Windows 的 Citrix Workspace 应用程序时。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。

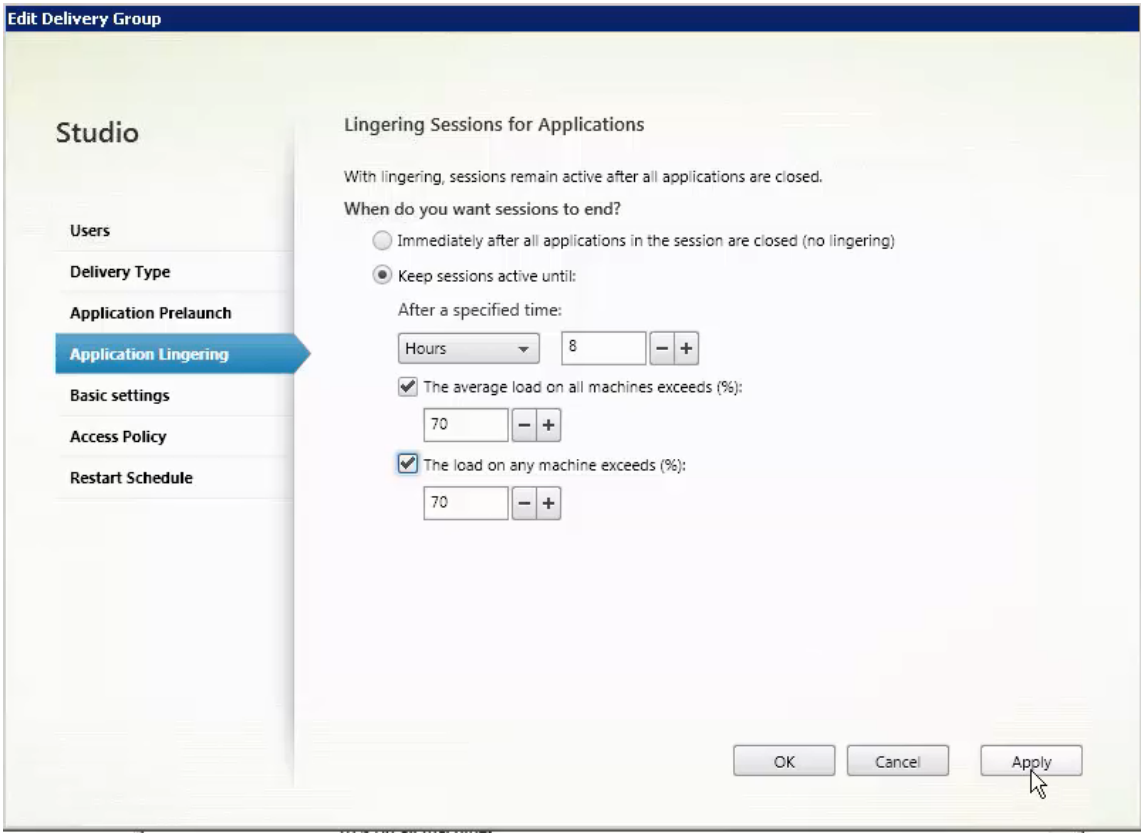
   - 经过指定的时间间隔时。可以更改时间间隔（1-99 天、1-2376 小时或 1-142560 分钟）。
   - 当交付组中所有计算机上的平均负载超过指定百分比 (1-99%) 时。
   - 当交付组中任一计算机上的负载超过指定百分比 (1-99%) 时。

   概述：预启动会话一直保持活动状态，直到下列任一事件发生：用户启动应用程序、经过指定的时间，或者超过指定的负载阈值。

启用会话延迟

1. 在导航窗格中选择交付组。
2. 选择一个组，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，通过选择在此时间之前保持会话处于活动状态来启用会话延迟。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. 如果用户未启动其他应用程序，有几项设置将影响延迟会话保持活动状态的时长。

   - 经过指定的时间间隔时。可以更改时间间隔：1-99 天、1-2376 小时或 1-142560 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。

在维护模式下从计算机断开连接时控制会话重新连接

> 注意：
>
> 此功能仅在 PowerShell 中可用。

可以控制是否允许在维护模式下的计算机上断开连接的会话重新连接到交付组中的计算机。

在版本 2106 之前，不允许在维护模式下与计算机断开连接的单会话池桌面会话重新连接。自版本 2106 起，可以将交付组配置为允许或禁止在维护模式下从计算机断开连接后重新连接（无论 VDA 类型为何）。

创建或编辑交付组（`New-BrokerDesktopGroup`、`Set-BrokerDesktopGroup`）时，请使用 `-AllowReconnectInMaintenanceMode <boolean>` 参数允许或禁止在维护模式下与计算机断开连接的计算机重新连接。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 如果设置为 true，会话可以重新连接到组中的计算机。
- 如果设置为 false，会话无法重新连接到组中的计算机。

默认值：

- 单会话：已禁用
- 多会话：已启用

故障排除

- 启动代理会话时，不会考虑未使用 Delivery Controller 进行注册的 VDA。这样会导致无法充分利用原本可用的资源 VDA 无法注册的原因有多种，其中许多都可由管理员进行故障排除。详细信息显示屏幕在目录创建向导中以及在您向交付组添加了目录之后提供故障排除信息。

  创建交付组后，交付组的详细信息窗格中指示可以注册但未注册的计算机数。例如，一台或多台计算机已打开电源，但未处于维护模式，并且当前未在 Controller 中注册。查看“应注册、但未注册的”计算机时，请查看“详细信息”窗格中的故障排除选项卡，了解可能的原因以及建议的更正措施。

  有关功能级别的消息，请参阅 VDA 版本和功能级别。

  有关 VDA 注册故障排除的信息，请参阅 CTX136668。

- 在交付组的显示屏幕中，“详细信息”窗格中的已安装的 **VDA** 版本可能与计算机上安装的实际版本不同。计算机的 Windows“程序和功能”将显示实际的 VDA 会话。
- 对于状态为电源状态未知的计算机，请参阅 CTX131267 了解指导信息。

创建应用程序组

January 21, 2022

简介

可以借助应用程序组管理应用程序的集合。为跨不同交付组共享的应用程序创建应用程序组。或者，交付组中的用户子集使用的应用程序。应用程序组是可选的；应用程序组提供向多个交付组添加相同应用程序的备选方法。将交付组与多个应用程序组相关联，并将应用程序组与多个交付组相关联。

与使用多个交付组相比，使用应用程序组可以提供应用程序管理和资源控制优势：

- 通过对应用程序及其设置进行逻辑分组，可以作为一个单元来管理这些应用程序。例如，不需要每次向各个交付组中添加（发布）一个相同的应用程序。
- 在应用程序组之间共享会话可以节省占用的资源。在其他情况下，在应用程序组之间禁用会话共享会非常有益。

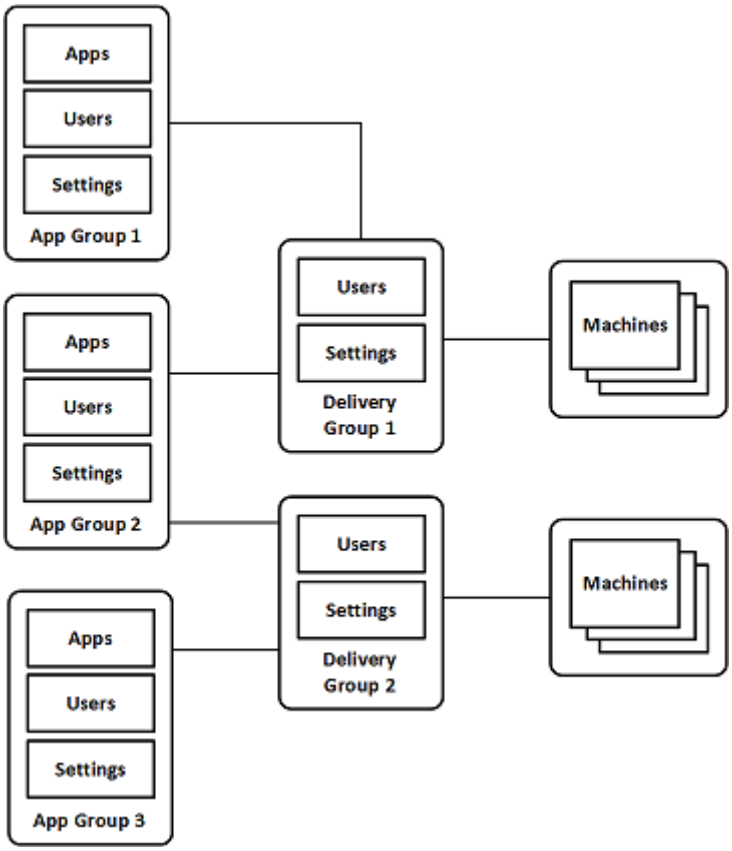
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 可以使用标记限制功能从应用程序组发布应用程序，仅考虑所选交付组中的一部分计算机。通过使用标记限制，可以使用现有计算机来完成多个发布任务，从而节省与部署和管理额外的计算机有关的成本。标记限制可以视为对交付组中的计算机进行划分（或分区）。对交付组中的一部分计算机进行隔离和故障排除时，将应用程序组或桌面与标记限制结合使用很有帮助。

示例配置

示例 **1**：

下图显示了一个包含多个应用程序组的 Citrix Virtual Apps and Desktops 部署：



在此配置中，应用程序被添加到应用程序组中，而非添加到交付组中。交付组指定要使用的计算机。（虽然未显示，但计算机位于计算机目录中。）

应用程序组 1 与交付组 1 相关联。由应用程序组 1 中指定的用户访问应用程序组 1 中的应用程序。只要同时位于交付组 1 的用户列表中，这些组就会显示。此配置遵从的指导原则为：应用程序组的用户列表属于相关联的交付组的用户列表的一部分（限制）。应用程序组 1 中的设置（例如，在应用程序组之间共享应用程序会话、相关联的交付组）适用于该组中的应用程序和用户。交付组 1 中的设置适用于应用程序组 1 和 2 中的用户，因为这些应用程序组已与该交付组相关联。

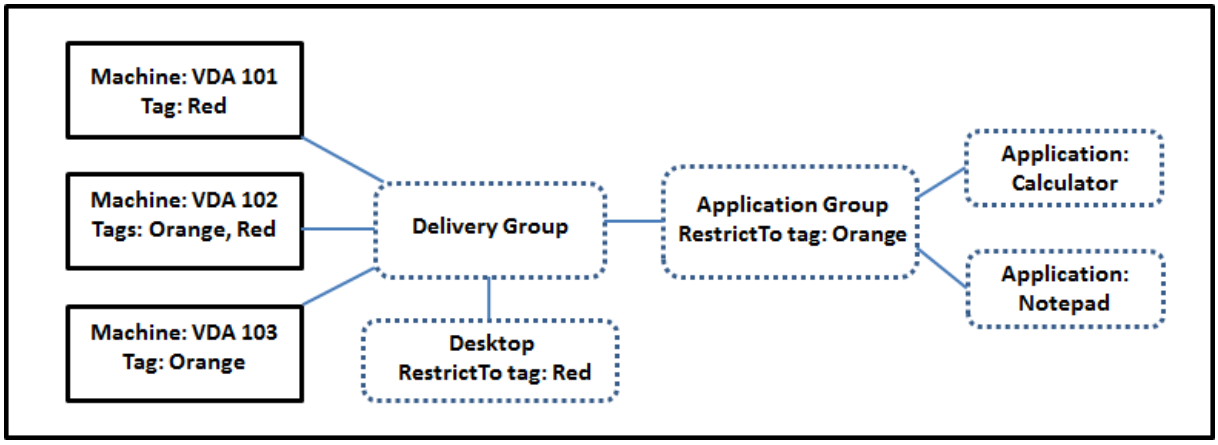
应用程序组 2 与两个交付组 1 和 2 相关联。在应用程序组 2 中为其中的每个交付组分配一个优先级，用于指示启动应用程序时交付组的检查顺序。优先级相等的交付组已实现负载平衡。由应用程序组 2 中指定的用户访问应用程序组 2 中的

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

应用程序。但是，它们还必须显示在交付组 1 和交付组 2 的用户列表中。

示例 **2**：

此简单布局使用标记限制来限制哪些计算机将被考虑用于启动特定的桌面和应用程序。该站点有一个共享交付组、一个发布的桌面以及一个配置了两个应用程序的应用程序组。



已为所有三台计算机 (VDA 101-103) 添加了标记。

创建应用程序组时使用“橙色”标记限制。其每个应用程序仅在该交付组中标记为“橙色”的计算机上、VDA 102 和 103 上启动。

有关在应用程序组中使用标记限制（以及用于桌面）的更全面的示例和指导，请参阅标记。

指导原则和注意事项

Citrix 建议您向应用程序组或交付组中添加应用程序，而不要同时向两者中添加。否则，两种组类型中包含的应用程序的复杂性将增加，使其更加难以管理。

默认情况下，应用程序组处于启用状态。创建应用程序组后，可以编辑该组以更改此设置。请参阅管理应用程序组。

默认情况下，在应用程序组之间共享的应用程序会话处于启用状态。请参阅在应用程序组之间共享会话。

Citrix 建议您将交付组升级到最新版本。此过程需要：

1. 升级交付组中使用的计算机上的 VDA。
2. 升级包含这些计算机的计算机目录。
3. 升级交付组。

有关详细信息，请参阅管理交付组。

您的核心组件的最低版本必须为 7.9，才能使用应用程序组。

创建应用程序组需要交付组管理员内置角色的委派管理权限。有关详细信息，请参阅委派管理。

本文提到将应用程序与多个应用程序组“关联”。它将该操作与从可用源添加该应用程序的实例区分开来。同样，多个交付组与多个应用程序组相关联，而非相互添加或作为对方的组件。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

与应用程序组共享会话

启用了应用程序会话共享时，所有应用程序在同一应用程序会话中启动。这可节省与启动更多应用程序会话关联的成本，并允许使用涉及剪贴板的应用程序功能（例如复制粘贴操作）。但是，在某些情况下，您可以取消选中会话共享。

使用应用程序组时，可以按以下三种方式配置应用程序会话共享，这些方式扩展了仅使用交付组时可用的标准会话共享行为：

- 在应用程序组之间已启用会话共享。
- 仅在同一应用程序组中的应用程序之间启用会话共享。
- 已禁用会话共享。

在应用程序组之间共享会话

可以在应用程序组之间启用应用程序会话共享，也可以禁用它以将应用程序会话共享限制为仅是同一应用程序组中的应用程序。

- 在应用程序组之间启用会话共享非常有用时的示例如下：

  应用程序组 1 包含 Microsoft Office 应用程序，例如 Word 和 Excel。应用程序组 2 包含其他应用程序，例如记事本和计算器，这两个应用程序组都连接到同一个交付组。有权访问这两个应用程序组的用户通过启动 Word 来启动一个应用程序会话，然后启动记事本。如果控制器发现运行 Word 的用户现有会话适合运行记事本，则在现有会话中启动记事本。如果无法从现有会话运行记事本（例如，如果标记限制将运行会话的计算机排除在外），则在合适的计算机上创建一个新会话，而不是使用会话共享。

- 在应用程序组之间禁用会话共享非常有用时的示例如下：

  具有一组与安装在同一台计算机上的其他应用程序互操作性不良的应用程序的配置。例如，同一软件套件的两个不同版本或同一 Web 浏览器的两个不同版本。您不希望某个用户在同一会话中同时启动两个版本。

  为软件套件的每个版本分别创建一个应用程序组，并将软件套件的每个版本对应的应用程序添加到相应的应用程序组中。如果为其中每个应用程序组禁用了在组之间共享会话的功能，在这些组中指定的用户将能够在同一会话中运行同一版本的应用程序。用户仍然可以同时运行其他应用程序，但不能在同一会话中运行。启动版本不同的应用程序的其中一个版本，或者启动未包含在应用程序组中的任何应用程序时，该应用程序将在新会话中启动。

在应用程序组之间共享会话的功能不属于安全沙盒功能。此功能非常复杂，并且无法阻止用户通过其他方式在其会话中启动应用程序（例如，通过 Windows 资源管理器）。

如果计算机已满载，则不会在其中启动新会话。根据需要使用会话共享功能在计算机上的现有会话中启动新应用程序。

只能使预启动的会话可用于已启用应用程序会话共享的应用程序组。（使用会话延迟功能的会话可用于所有应用程序组。）必须在与应用程序组关联的每个交付组中启用和配置这些功能。不能在应用程序组中配置这些功能。

默认情况下，创建应用程序组时，将启用在应用程序组之间共享应用程序会话。创建组时不能更改此设置。创建应用程序组后，可以编辑该组以更改此设置。请参阅管理应用程序组。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

在应用程序组中禁用会话共享

可以阻止在同一应用程序组中的应用程序之间共享应用程序会话。

- 在应用程序组中禁用会话共享非常有用时的示例如下：

  您希望用户在单独的显示器上访问某个应用程序的多个同时进行的全屏会话。

  创建一个应用程序组，并向其添加应用程序。

默认情况下，创建应用程序组时，将启用应用程序会话共享。创建组时不能更改此设置。创建应用程序组后，可以编辑该组以更改此设置。请参阅管理应用程序组。

创建应用程序组

要创建应用程序组，请执行以下操作：

1. 在 Studio 导航窗格中选择应用程序，然后在“操作”窗格中选择创建应用程序组。
2. 此时将启动向导，并打开一个简介页面，您可以在将来启动此向导时不再显示该页面。
3. 该向导将引导您完成以下部分中所述的页面。完成每个页面之后，请单击下一步，直到到达“摘要”页面为止。

步骤 **1.** 交付组

交付组页面列出了所有交付组以及每个组包含的计算机数。

- 兼容的交付组列表中包含可以选择的交付组。兼容的交付组包含随机（非永久分配或静态分配的）多会话或单会话操作系统计算机。
- 不兼容的交付组列表包含无法选择的交付组。每个条目都会解释不兼容的原因，例如，包含静态分配的计算机。

应用程序组可以与包含能够交付应用程序的共享（而非专用）计算机的交付组相关联。

如果满足以下两个条件，您还可以选择包含仅交付桌面的共享计算机的交付组：

- 交付组包含共享计算机，并且是使用 XenDesktop 7.9 之前的版本创建的。
- 您拥有编辑交付组权限。

在提交应用程序组创建向导时，交付组类型将自动转换为“桌面和应用程序”。

虽然您能够创建没有关联交付组的应用程序组（或者能够组织整理应用程序或者用作当前未使用的应用程序的存储），但在至少指定一个交付组之前，不能使用应用程序组来交付应用程序。此外，如果没有指定的交付组，则无法从 **From Start**（从头开始）菜单源将应用程序添加到应用程序组。

所选交付组将指定用于交付应用程序的计算机。请选中要与应用程序组关联的交付组旁边的复选框。

要添加标记限制，请选择限制启动带标记的计算机，然后从下拉列表中选择标记。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

步骤 **2.** 用户

在应用程序组中指定应用程序用户。允许您在上一页面中选择的交付组中的所有用户和用户组，或者从这些交付组中选择特定用户和用户组。如果限制由指定用户使用，则只有在交付组和应用程序组中指定的用户能够访问此组中的应用程序。实际上，应用程序组中的用户列表提供了一个与交付组中的用户列表有关的过滤器。

允许或禁止未经身份验证的用户使用应用程序功能仅在交付组中可用，在应用程序组中不可用。

有关在部署中指定了用户列表的位置的信息，请参阅指定了用户列表的位置。

步骤 **3.** 应用程序

须知：

- 默认情况下，您添加的新应用程序位于 **Applications** 文件夹中。可以指定其他文件夹。如果您尝试添加某个应用程序，但同一文件夹中存在同名应用程序，则系统将提示您重命名要添加的应用程序。如果您同意使用建议的唯一名称，则会使用该新名称添加应用程序。否则，您必须自己先重命名该应用程序，才能添加。有关详细信息，请参阅管理应用程序文件夹。
- 您可以在添加时更改应用程序的属性（设置），或者在以后更改。请参阅更改应用程序属性。如果要向相同的用户发布两个同名应用程序，请在 Studio 中更改应用程序名称 **(**面向用户**)** 属性。否则，用户将在 Citrix Workspace 应用程序中看到重复的名称。
- 如果要将一个应用程序添加到多个应用程序组中，但您没有足够的权限查看所有这些应用程序组中的应用程序，则会产生可见性问题。在这种情况下，可以咨询权限更高的管理员，或者扩展您的作用域，使其包括将应用程序添加到的所有组。

单击下拉菜单中的添加以显示应用程序源。

- 从“开始”菜单：在计算机上发现的位于选定交付组中的应用程序。当您选择该源时，会打开一个新页面，其中包含已发现的应用程序的列表。选中要添加的应用程序的复选框，然后单击确定。

  如果您选择了以下任一项，则不能选择此源：

  - 无关联交付组的应用程序组。
  - 与不包含任何计算机的交付组关联的应用程序组。
  - 不包含任何计算机的交付组。

- 手动定义：位于站点上或网络中的其他位置的应用程序。如果选择此源，则会启动一个新页面，您可以在其中键入可执行文件路径、工作目录、可选命令行参数以及显示给管理员和用户的名称。输入此信息后，单击确定。
- 现有：以前添加到站点的应用程序。当您选择该源时，会打开一个新页面，其中包含已发现的应用程序的列表。选中要添加的应用程序的复选框，然后单击确定。如果站点没有任何应用程序，则无法选择此源。
- **App-V**：App-V 包中的应用程序。如果选择此源，则会启动一个新页面，您可以在其中选择 **App-V** 服务器或应用程序库。从生成的显示内容中，选中要添加的应用程序的复选框，然后单击确定。有关详细信息，请参阅 App-V。如果没有为站点配置 App-V，则无法选择此源（或者此源可能不显示）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

如前所述，如果没有该类型的有效源，则无法选择添加下拉菜单中的某些条目。系统根本不会列出不兼容的源（例如，无法向应用程序组中添加应用程序组，因此，在创建应用程序组时不会列出该源）。

步骤 **4.** 作用域

仅当您以前创建了自定义作用域时才会显示此页面。默认情况下，选中全部作用域。有关详细信息，请参阅委派管理。

步骤 **5.** 摘要

输入应用程序组的名称。还可以（选择性）输入说明。

查看摘要信息，然后单击完成。

管理应用程序组

January 21, 2022

简介

本文介绍如何管理您创建的应用程序组。

有关如何管理应用程序组或交付组中的应用程序的信息（包括如何执行以下操作的信息），请参阅应用程序：

- 在应用程序组中添加或删除应用程序。
- 更改应用程序组关联。

管理应用程序组需要具有交付组管理员内置角色的委派管理权限。有关详细信息，请参阅委派管理。

启用或禁用应用程序组

启用某个应用程序组时，可以提供已添加到该组中的应用程序。禁用某个应用程序组会禁用该组中的每个应用程序。但是，如果这些应用程序同时与其他已启用的应用程序组相关联，则可以从其他相应组中提供这些应用程序。如果已将该应用程序显式添加到与应用程序组关联的交付组中，禁用应用程序组不会影响这些交付组中的应用程序。

应用程序组在创建时即会启用。创建组时不能更改此配置。

1. 在 Studio 导航窗格中选择应用程序。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择编辑应用程序组。
3. 在设置页面上，选中或清除启用应用程序组复选框。
4. 单击应用以使窗口保持打开状态，或单击确定应用更改并关闭窗口。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

在应用程序组之间启用或禁用应用程序会话共享

创建应用程序组时，在应用程序组之间启用会话共享。创建组时不能更改此配置。有关详细信息，请参阅在应用程序组之间共享会话。

1. 在 Studio 导航窗格中选择应用程序。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择编辑应用程序组。
3. 在设置页面上，选中或清除在应用程序组之间启用应用程序会话共享复选框。
4. 单击应用以使窗口保持打开状态，或单击确定应用更改并关闭窗口。

在应用程序组中禁用应用程序会话共享

创建应用程序组时，将默认启用在同一应用程序组中的应用程序之间进行会话共享。如果在应用程序组之间禁用应用程序会话共享，则同一应用程序组中的应用程序之间的会话共享将保持启用状态。

在禁用应用程序组中的应用程序之间的应用程序会话共享的情况下，您可以使用 PowerShell SDK 来配置应用程序组。在某些情况下，此选项是可取的。例如，您可能希望用户在单独的显示器上完整大小的应用程序窗口中启动非无缝应用程序。

在应用程序组中禁用应用程序会话共享时，该组中的每个应用程序都将在新的应用程序会话中启动。如果有一个运行同一个应用程序的已断开连接的合适会话可用，则将其重新连接。例如，当启动记事本时存在已断开连接的会话并且记事本正在运行，该会话将重新连接，而非创建一个会话。有多个已断开连接的合适会话可用时，则以随机但确定性的方式选择其中一个会话进行重新连接。在相同情况下再次出现这种情形时，则选择同一会话，但在其他情况下，会话不一定可预测。

使用 PowerShell SDK 来对某个现有应用程序组中的所有应用程序禁用应用程序会话共享，或创建禁用应用程序会话共享的组。

PowerShell cmdlet 示例

要禁用会话共享，请使用将参数 `SessionSharingEnabled` 设置为 `False` 和将参数 `SingleAppPerSession` 设置为 `True` 的代理 PowerShell cmdlet `New-BrokerApplicationGroup` 或 `Set-BrokerApplicationGro`。

- 例如，创建对应用程序组中的所有应用程序禁用应用程序会话共享的应用程序组：

```
New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -
SingleAppPerSession $True
```

- 例如，在某个现有应用程序组中的所有应用程序之间禁用应用程序会话共享：

```
Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -
SingleAppPerSession $True
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

注意事项

- 要启用 SingleAppPerSession 属性，必须将 SessionSharingEnabled 属性设置为 False。不能同时启用这两个属性。SessionSharingEnabled 参数是指在应用程序组之间共享会话。
- 应用程序会话共享只适用于与应用程序组关联的应用程序，而不是与交付组关联的应用程序。默认情况下，直接与交付组关联的所有应用程序共享会话。
- 如果某个应用程序分配到多个应用程序组，请确保这些组的设置没有冲突。例如，如果一个组的选项设置为 True，另一个组的选项设置为 False，则将导致发生不可预测的行为。

重命名应用程序组

1. 在 Studio 导航窗格中选择应用程序。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择重命名应用程序组。
3. 指定新的唯一名称，然后单击确定。

添加、删除或更改与应用程序组关联的交付组的优先级

应用程序组可以与包含能够交付应用程序的共享（而非专用）计算机的交付组相关联。

如果满足以下两个条件，您还可以选择包含仅交付桌面的共享计算机的交付组：

- 交付组包含共享计算机，并且是使用 7.9 之前的版本创建的。
- 您拥有编辑交付组权限。

提交编辑应用程序组对话框时，交付组类型将自动转换为“桌面和应用程序”。

1. 在 Studio 导航窗格中选择应用程序。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择编辑应用程序组。
3. 选择交付组页面。
4. 要添加交付组，请单击添加。选中可用交付组的复选框。（不能选择不兼容的交付组。）完成选择后，单击确定。
5. 要删除交付组，请选中要删除的组的复选框，然后单击删除。出现提示后，确认删除。
6. 要更改交付组的优先级，请选择交付组的复选框，然后单击编辑优先级。输入优先级（0 = 最高），然后单击确定。
7. 单击应用以应用您所做的任何更改并使窗口保持打开，或单击确定应用更改并关闭窗口。

在应用程序组中添加、更改或删除标记限制

添加、更改和删除标记限制可能会对被考虑用于启动应用程序的计算机有意外的影响。请查看标记中的注意事项和警告。

1. 在 Studio 导航窗格中选择应用程序。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择编辑应用程序组。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. 选择交付组页面。
4. 要添加标记限制，请选择限制启动带标记的计算机，然后从下拉列表中选择标记。
5. 要更改或删除标记限制，请选择一个不同的标记，或者通过清除限制启动带标记的计算机彻底删除标记限制。
6. 单击应用以应用您所做的任何更改并使窗口保持打开，或单击确定应用更改并关闭窗口。

在应用程序组中添加或删除用户

有关用户的详细信息，请参阅创建应用程序组。

1. 在 Studio 导航窗格中选择应用程序。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择编辑应用程序组。
3. 选择用户页面。指出是允许关联交付组中的所有用户使用应用程序组中的应用程序，还是仅允许特定用户和组使用。要添加用户，请单击添加，然后指定要添加的用户。要删除用户，请选择一个或多个用户，然后单击删除。
4. 单击应用以应用您所做的任何更改并使窗口保持打开，或单击确定应用更改并关闭窗口。

更改应用程序组中的作用域

仅当在创建作用域之后，才能更改作用域（不能编辑所有作用域）。有关详细信息，请参阅委派管理。

1. 在 Studio 导航窗格中选择应用程序。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择编辑应用程序组。
3. 选择作用域页面。选中或取消选中某个作用域旁边的复选框。
4. 单击应用以应用您所做的任何更改并使窗口保持打开，或单击确定应用更改并关闭窗口。

删除应用程序组

一个应用程序必须至少与一个交付组或应用程序组相关联。如果删除某个应用程序组会导致一个或多个应用程序不再属于某个组，系统将向您发出警告，指出删除该组还将删除这些应用程序。然后您可以确认或取消删除。

删除应用程序不会将其从原始源中删除。但是，如果您要使其再次可用，必须重新添加。

1. 在 Studio 导航窗格中选择应用程序。
2. 在中间窗格中选择一个应用程序组，然后在“操作”窗格中选择删除组。
3. 出现提示后，确认删除。

Remote PC Access

July 5, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Remote PC Access 是 Citrix Virtual Apps and Desktops 的一项功能，使组织能够轻松地允许员工以安全的方式远程访问企业资源。Citrix 平台允许用户访问其物理办公室 PC，从而使这种安全访问成为可能。如果用户可以访问其办公室 PC，他们可以访问完成工作所需的所有应用程序、数据和资源。Remote PC Access 无需引入和提供其他工具来满足远程工作需求。例如，虚拟桌面或应用程序及其关联的基础架构。

Remote PC Access 使用交付虚拟桌面和应用程序的相同 Citrix Virtual Apps and Desktops 组件。因此，部署和配置 Remote PC Access 的要求和流程与部署 Citrix Virtual Apps and Desktops 以交付虚拟资源所需的要求和流程相同。这种统一性提供了一致且统一的管理体验。用户通过使用 Citrix HDX 交付其办公室 PC 会话，获得最佳用户体验。

该功能由 **Remote PC Access** 类型的、提供以下功能的计算机目录组成：

- 能够通过指定 OU 添加计算机。这种能力有助于批量添加 PC。
- 基于登录到办公室 Windows PC 的用户的自动分配用户。我们支持单用户和多用户分配。

通过使用其他类型的计算机目录，Citrix Virtual Apps and Desktops 可以适应物理 PC 的更多用例。这些用例包括：

- 物理 Linux PC
- 池物理 PC（即随机分配、非专用）

> 备注：
>
> 有关支持的操作系统版本的详细信息，请参阅适用于单会话操作系统的 VDA 和 Linux VDA 的系统要求。
>
> 对于本地部署：Remote PC Access 仅对 Citrix Virtual Apps and Desktops Advanced 或 Premium 许可证有效。会话使用许可证的方式与其他 Citrix Virtual Desktops 会话相同。对于 Citrix Cloud，Remote PC Access 对 Citrix Virtual Apps and Desktops 服务以及 Workspace Premium Plus 有效。

注意事项

虽然适用于 Citrix Virtual Apps and Desktops 的所有技术要求和注意事项通常也适用于 Remote PC Access，但某些要求和注意事项可能与物理 PC 用例更为相关或独占。

> 重要：
>
> Windows 11 物理系统（以及一些运行 Windows 10 的系统）包含基于虚拟化的安全功能，这些功能会导致 VDA 软件错误地将其检测为虚拟机。要减轻此问题，可以使用以下选项：
>
> - 作为 VDA 命令行安装的一部分，请使用“/physicalmachine”选项以及“/remotepc”选项
> - 如果未使用上述选项，请在安装 VDA 后添加以下注册表值 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
>
>   - 名称：ForceEnableRemotePC

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> - 类型：DWORD
> - 数据：1

部署注意事项

在规划 Remote PC Access 的部署时，请做出一些一般性决策。

- 可以将 Remote PC Access 添加到现有的 Citrix Virtual Apps and Desktops 部署。选择此选项之前，请注意以下事项：
  - 当前的 Delivery Controller 或 Cloud Connector 的大小是否适当，能够支持与 Remote PC Access VDA 相关的额外负载？
  - 本地站点数据库和数据库服务器的大小是否适当，能够支持与 Remote PC Access VDA 相关的额外负载？
  - 现有 VDA 和新的 Remote PC Access VDA 是否会超过每个站点支持的最大 VDA 数量？
- 您必须通过自动化过程将 VDA 部署到办公室 PC。下面是可用的选项：
  - 电子软件分发 (Electronic Software Distribution, ESD) 工具，例如 SCCM：使用 SCCM 安装 VDA。
  - 部署脚本：使用脚本安装 VDA。
- 请参阅 Remote PC Access 安全注意事项。

计算机目录注意事项

所需的计算机目录类型取决于用例：

- Remote PC Access
  - Windows 专用 PC
  - Windows 专用多用户 PC。此用例适用于多个用户可以通过不同轮班进行远程访问的物理办公室 PC。
- 单会话操作系统
  - 静态 - 专用 Linux PC
  - 随机 - 池化 Windows 和 Linux PC

确定计算机目录的类型后，请注意以下事项：

- 一台计算机只能同时分配到一个计算机目录。
- 为了便于委派管理，请考虑根据地理位置、部门或任何便于将每个目录的管理委派给相应管理员的其他分组创建计算机目录。
- 选择计算机帐户所在的 OU 时，请选择较低级别的 OU 以获得更大的粒度。如果不需要此类粒度，则可以选择更高级别的 OU。例如，对于银行/主管/出纳，选择出纳以获得更大的粒度。否则，您可以根据要求选择高级职员或银行。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 将 OU 分配到 Remote PC Access 计算机目录后移动或删除 OU 会影响 VDA 关联并导致未来的分配出现问题。因此，请务必相应地制定计划，以便在 Active Directory 更改计划中考虑计算机目录的 OU 分配更新。
- 如果由于 OU 结构，选择 OU 以将计算机添加到计算机目录并不容易，则不必选择任何 OU。之后可以使用 PowerShell 将计算机添加到目录中。如果在交付组中正确地配置了桌面分配，则用户自动分配将继续起作用。GitHub 中提供了将计算机添加到计算机目录以及用户分配的示例脚本。
- 集成局域网唤醒功能仅适用于 **Remote PC Access** 类型计算机目录。

Linux VDA 注意事项

这些注意事项是 Linux VDA 特有的：

- 请仅在非 3D 模式下在物理机上使用 Linux VDA。由于 NVIDIA 驱动程序的限制，当启用了 HDX 3D 模式时，PC 的本地屏幕无法停止，并显示会话的活动。显示此屏幕存在安全风险。
- 请对物理 Linux 计算机使用单会话操作系统类型的计算机目录。
- 自动用户分配不适用于 Linux 计算机。
- 如果用户已在本地登录到其 PC，尝试从 StoreFront 启动 PC 将失败。
- 节能选项不适用于 Linux 计算机。

技术要求和注意事项

本部分内容包含物理 PC 的技术要求和注意事项。

- 不支持以下各项：
  - 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。
  - 双引导计算机。
- 将键盘和鼠标直接连接到 PC。连接到显示器或其他可关闭或断开连接的组件可能会使这些外围设备不可用。如果必须将输入设备连接到显示器等组件上，请勿关闭这些组件。
- 必须将 PC 加入到 Active Directory 域服务域。
- 安全启动功能仅在 Windows 10 上受支持。
- PC 必须具有活动的网络连接。为了提高可靠性和带宽，首选有线连接。
- 如果使用 Wi-Fi，请执行以下操作：
  1. 设置电源设置以保持无线适配器处于打开状态。
  2. 配置无线适配器和网络配置文件，以便在用户登录之前允许自动连接到无线网络。否则，VDA 在用户登录之后才会注册。在用户登录之前，PC 不可用于远程访问。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. 确保可以通过 Wi-Fi 网络访问 Delivery Controller 或 Cloud Connector。

- 可以在便携式计算机上使用 Remote PC Access。确保便携式计算机连接到电源，而非依靠电池运行。配置便携式计算机电源选项以匹配台式机的选项。例如：

  1. 禁用休眠功能。
  2. 禁用睡眠功能。
  3. 将合盖操作设置为不执行任何操作。
  4. 将按下电源按钮的操作设置为关闭。
  5. 禁用显卡和 NIC 节能功能。

- Remote PC Access 在安装了 Windows 10 的 Surface Pro 设备上受支持。请遵循上文提及的便携式计算机的相同准则。

- 如果使用扩展坞，则可以取消停靠和重新停靠便携式计算机。取消停靠便携式计算机时，VDA 将通过 Wi-Fi 在 Delivery Controller 或 Cloud Connector 中重新注册。但是，重新停靠便携式计算机时，VDA 将不切换到使用有线连接，除非断开无线适配器的连接。某些设备提供内置功能，可在建立有线连接时断开无线适配器的连接。其他设备需要自定义解决方案或第三方实用程序才能断开无线适配器的连接。请查看上文提及的 Wi-Fi 注意事项。

  请执行以下操作以便为 Remote PC Access 设备启用停靠和取消停靠：

  1. 在开始菜单中，选择设置 **>** 系统 **>** 电源和睡眠，然后将睡眠设置为从不。
  2. 在设备管理器 **>** 网络适配器 **>** 以太网适配器下，转到电源管理并取消选中允许计算机关闭此设备以节约电源。请务必选中允许此设备唤醒计算机。

- 访问同一办公室 PC 的多个用户在 Citrix Workspace 中可以看到相同的图标。当用户登录到 Citrix Workspace 时，如果其他用户已在使用该资源，该资源将显示为不可用。

- 请在访问办公室 PC 的每个客户端设备（例如，家用 PC）上安装 Citrix Workspace 应用程序。

配置序列

本部分内容概述了如何在使用 **Remote PC Access** 类型的计算机目录时配置 Remote PC Access。有关如何创建其他类型的计算机目录的信息，请参阅创建计算机目录。

1. 仅限本地站点 - 要使用集成的局域网唤醒功能，请配置局域网唤醒中概述的必备项。
2. 如果为 Remote PC Access 创建了新的 Citrix Virtual Apps and Desktops 站点：

   a) 选择 **Remote PC Access** 站点类型。
   b) 在电源管理页面上，为默认 Remote PC Access 计算机目录启用或禁用电源管理。可以稍后通过编辑计算机目录属性来更改此设置。有关配置局域网唤醒功能的详细信息，请参阅局域网唤醒。
   c) 完成用户和计算机帐户页面上的信息。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

完成这些步骤将创建名为 **Remote PC Access** 计算机的计算机目录和名为 **Remote PC Access** 桌面的交付组。

3. 如果添加到现有 Citrix Virtual Apps and Desktops 站点，请执行以下操作：

   a) 创建类型为 **Remote PC Access**（向导的操作系统页面）的计算机目录。有关如何创建计算机目录的详细信息，请参阅创建计算机目录。请确保分配正确的 OU，以便使目标 PC 可用于 Remote PC Access。
   b) 创建交付组以便为用户提供对计算机目录中的 PC 的访问权限。有关如何创建交付组的详细信息，请参阅创建交付组。请确保将交付组分配给包含需要访问其 PC 的用户的 Active Directory 组。

4. 将 VDA 部署到办公室 PC。

   - 我们建议使用单会话操作系统核心 VDA 安装程序 (VDAWorkstationCoreSetup.exe)。
   - 还可以将单会话完整 VDA 安装程序 (VDAWorkstationSetup.exe) 与 `/remotepc` 选项结合使用，该选项可达到与使用核心 VDA 安装程序相同的结果。
   - 请考虑启用 Windows 远程协助，以允许技术支持团队通过 Citrix Director 提供远程支持。要执行此操作，请使用 `/enable_remote_assistance` 选项。有关详细信息，请参阅使用命令行安装。
   - 要能够在 Director 中查看登录持续时间信息，必须使用单会话完整 VDA 安装程序并包含 **Citrix User Profile Management WMI** 插件组件。请使用 `/includeadditional` 选项来包括此组件。有关详细信息，请参阅使用命令行安装。
   - 有关使用 SCCM 部署 VDA 的信息，请参阅使用 SCCM 安装 VDA。
   - 有关通过部署脚本部署 VDA 的信息，请参阅使用脚本安装 VDA。

   成功完成步骤 2 到 4 后，当用户在 PC 上本地登录时，系统会自动将其分配到自己的计算机。

5. 指示用户在其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 Workspace 应用程序。用户可以从 `https://www.citrix.com/downloads/` 或支持的移动设备的应用商店获取 Citrix Workspace 应用程序。

通过注册表管理的功能

> 小心：
>
> 注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

禁用多个用户自动分配

在每个 Delivery Controller 上，添加以下注册表设置：

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- 名称：AllowMultipleRemotePCAssignments
- 类型：DWORD
- 数据：0

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

睡眠模式（最低版本 **7.16**）

要允许 Remote PC Access 计算机进入睡眠模式，请在 VDA 上添加此注册表设置，然后重新启动计算机。重新启动后，将遵从操作系统节能设置。预先配置的空闲计时器过时后，计算机将进入睡眠模式。计算机唤醒后，将在 Delivery Controller 中注册。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名称：DisableRemotePCSleepPreventer
- 类型：DWORD
- 数据：1

会话管理

默认情况下，当本地用户在该计算机上启动会话时（通过按 CTRL+ATL+DEL），远程用户的会话自动断开连接。要阻止此自动操作，请在办公 PC 上添加以下注册表项，然后重新启动计算机。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名称：SasNotification
- 类型：DWORD
- 数据：1

默认情况下，在超时期限内未确认连接消息时，远程用户拥有优先于本地用户的优先权。要配置行为，请使用以下设置：

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名称：RpcaMode
- 类型：DWORD
- 数据：
  - 1 - 如果远程用户没有在指定的超时期限内响应消息 UI，此用户将始终具有优先权。如果未配置此设置，则此行为为默认值。
  - 2 - 本地用户具有优先权。

默认情况下，强制执行 Remote PC Access 模式的超时时间为 30 秒。可以配置此超时，但不要将其设置为低于 30 秒。要配置超时，请使用以下注册表设置：

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- 名称：RpcaTimeout
- 类型：DWORD
- 数据：十进制值格式的超时秒数

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。

注册表更改并重新启动计算机后，如果本地用户在远程用户使用时按 Ctrl+Alt+Del 登录到该 PC，则远程用户会收到提示。该提示询问是允许还是拒绝本地用户的连接。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时进行远程访问。

借助局域网唤醒功能，幻数据包会在 Delivery Controller 指示时直接从 PC 上运行的 VDA 发送到 PC 所在的子网。这允许此功能在不依赖额外的基础结构组件或第三方解决方案的情况下运行，以便传送幻数据包。

局域网唤醒功能不同于传统的基于 SCCM 的局域网唤醒功能。有关基于 SCCM 的局域网唤醒的信息，请参阅 局域网唤醒–SCCM 集成。

系统要求

下面是使用局域网唤醒功能的系统要求：

- 控制平面：
  - Citrix Virtual Apps and Desktops 服务
  - Citrix Virtual Apps and Desktops 2009 或更高版本
- 物理 PC：
  - 2009 或更高版本
  - Windows 10。有关可支持性的详细信息，请参阅 VDA 系统要求。
  - 在 BIOS/UEFI 中启用了局域网唤醒功能
  - 在 Windows 配置内部的网络适配器属性中启用了局域网唤醒

配置局域网唤醒

目前，仅在使用 PowerShell 时支持集成的局域网唤醒的配置。

要配置局域网唤醒，请执行以下操作：

1. 如果您还没有 Remote PC Access 计算机目录，请创建一个目录。
2. 如果您还没有局域网唤醒主机连接，请创建一个连接。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 要使用局域网唤醒功能，如果您具有“Microsoft 配置管理器局域网唤醒”类型的主机连接，请创建一个主机连接。

3. 检索局域网唤醒主机连接的唯一标识符。
4. 将局域网唤醒主机连接与计算机目录相关联。

要创建局域网唤醒主机连接，请执行以下操作：

```
# Load Citrix SnapIns
Add-PSSnapIn -Name "\*citrix\*"

# Provide the name of the Wake on LAN host connection
[string]$connectionName = "Remote PC Access Wake on LAN"

# Create the hypervisor connection
$hypHc = New-Item -Path xdhyp:\Connections `
                -Name $connectionName `
                -HypervisorAddress "N/A" `
                -UserName "woluser" `
                -Password "wolpwd" `
                -ConnectionType Custom `
                -PluginId VdaWOLMachineManagerFactory `
                -CustomProperties "<CustomProperties></CustomProperties
                    >" `
                -Persist

$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
    $hypHc.HypervisorConnectionUid

# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
{

    Start-Sleep -s 5
    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
        $hypHc.HypervisorConnectionUid
 }

<!--NeedCopy-->
```

主机连接准备就绪后，运行以下命令以检索主机连接的唯一标识符：

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
$hypUid = $bhc.Uid
<!--NeedCopy-->
```

检索连接的唯一标识符后，运行以下命令以将连接与 Remote PC Access 计算机目录相关联：

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
    RemotePCHypervisorConnectionUid $hypUid
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

设计注意事项

当您计划在 Remote PC Access 中使用局域网唤醒时，请注意以下事项：

- 多个计算机目录可以使用相同的局域网唤醒主机连接。
- 要使一台 PC 唤醒另一台 PC，两台 PC 必须位于同一子网中，并使用相同的局域网唤醒主机连接。这些 PC 是在相同还是不同的计算机目录中并不重要。
- 将主机连接分配给特定区域。如果您的部署中包含多个区域，则需要在每个区域中使用局域网唤醒主机连接。这同样适用于计算机目录。
- 幻数据包使用全局广播地址 255.255.255.255 进行广播。确保该地址未被阻止。
- 子网中必须至少打开一台 PC（对于每个局域网唤醒连接），才能唤醒该子网中的计算机。

操作注意事项

下面是使用局域网唤醒功能的注意事项：

- VDA 必须至少注册一次，才能使用集成的局域网唤醒功能唤醒 PC。
- 局域网唤醒功能只能用于唤醒 PC。该功能不支持其他电源操作，例如重新启动或关闭。
- 创建局域网唤醒连接后，该功能在 Studio 中可见。但是，不支持在 Studio 中编辑其属性。
- 幻数据包通过以下两种方式之一发送：
  1. 当用户尝试启动到其 PC 的会话并且 VDA 未注册时
  2. 当管理员从 Studio 或 PowerShell 手动发送打开电源命令时
- 由于 Delivery Controller 不知道 PC 的电源状态，因此，Studio 在电源状态下显示不支持。Delivery Controller 使用 VDA 注册状态来确定 PC 是打开还是关闭。

局域网唤醒—**SCCM** 集成

SCCM 集成局域网唤醒是 Remote PC Access 的替代局域网唤醒选项，仅适用于本地 Citrix Virtual Apps and Desktops。

系统要求

下面是使用 SCCM 集成局域网唤醒功能的系统要求：

- Citrix Virtual Apps and Desktops 1912 或更高版本
- 物理 PC：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - VDA 1912 或更高版本
  - Windows 10。有关可支持性的详细信息，请参阅 VDA 系统要求。
  - 在 BIOS/UEFI 中启用了局域网唤醒功能
  - 在 Windows 配置内部的网络适配器属性中启用了局域网唤醒
- System Center Configuration Manager (SCCM) 2012 R2 或更高版本

配置 **SCCM** 集成局域网唤醒

完成以下必备条件：

1. 在组织内配置 SCCM 2012 R2、2016 或 2019。然后将 SCCM 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（或在需要时手动强制运行一个周期）。
2. 要支持唤醒代理，请在 SCCM 中启用该选项。对于组织中使用 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。
3. 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。
4. 在每台 PC 的 BIOS/UEFI 设置中配置局域网唤醒功能。
5. 如果您尚未将 VDA 部署到物理 PC 上，请进行部署。

解决这些必备条件后，请完成以下步骤以允许 Delivery Controller 与 SCCM 通信：

1. 为 SCCM 创建主机连接。有关详细信息，请参阅连接和资源。
   - 选择 **Microsoft Configuration Manager** 局域网唤醒作为连接类型。
   - 输入的凭据必须具有对作用域中的集合的访问权限，并且必须具有远程工具操作员角色。
2. 在 Studio 中选择连接，然后选择编辑连接并单击高级。
3. 选择处理局域网唤醒的相应选项：
   - 如果您使用的是唤醒代理，请选择第一个选项：**Microsoft System Center Configuration Manager** 唤醒代理。
   - 如果您使用的是幻数据包，请选择第二个选项：**Delivery Controller** 传输的局域网唤醒数据包。
     - 选择适当的传输方法：子网定向广播或单播。

创建主机连接后，将连接与 Remote PC Access 目录相关联：

- 如果要创建新的 Remote PC Access 目录，请在目录创建向导的操作系统页面中选择 **Remote PC Access** 作为目录类型，然后从下拉列表中选择相应的连接。
- 要将局域网唤醒添加到现有的 Remote PC Access 目录，请执行以下操作：
  1. 转到 Studio 中的计算机目录节点，选择计算机目录，然后选择编辑计算机目录。
  2. 选择电源管理选项卡，然后选择是以启用计算机目录的电源管理。
  3. 从下拉列表中选择相应的连接，然后单击确定。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

故障排除

显示器擦除不起作用

如果 Windows PC 的本地显示器不是空白，而是存在活动的 HDX 会话（本地显示器显示会话中发生的情况），则可能是由于 GPU 供应商的驱动程序出现问题。要解决此问题，请通过设置以下注册表值为 Citrix Indirect Display 驱动程序 (IDD) 设置比图形卡的供应商驱动程序更高的优先级：

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- 名称：CitrixIDD
- 类型：DWORD
- 数据：3

有关显示适配器优先级和显示器创建的更多详细信息，请参阅知识中心文章 CTX237608。

当您在启用了会话管理通知的计算机上选择 **Ctrl+Alt+Del** 时，会话将断开连接

只有在 VDA 上启用了 Remote PC Access 模式时，**SasNotification** 注册表值控制的会话管理通知才起作用。如果物理 PC 具有 Hyper-V 角色或者启用了任何基于虚拟化的安全功能，该 PC 将报告为虚拟机。如果 VDA 检测到它正在虚拟机上运行，则会自动禁用 Remote PC Access 模式。要启用 Remote PC Access 模式，请添加以下注册表值：

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名称：ForceEnableRemotePC
- 类型：DWORD
- 数据：1

重新启动 PC 以使设置生效。

诊断信息

与 Remote PC Access 有关的诊断信息写入到 Windows 应用程序事件日志中。信息性消息不受限制。错误消息受限制，需删除重复消息。

- 3300（信息性消息）：计算机已添加到目录
- 3301（信息性消息）：计算机已添加到交付组
- 3302（信息性消息）：计算机已分配给用户
- 3303（错误消息）：异常

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

电源管理

如果启用 Remote PC Access 电源管理，子网定向广播可能无法启动与 Controller 不在同一子网上的计算机。如果需要使用子网定向广播跨子网管理电源且不支持 AMT，请尝试使用唤醒代理或“单播”方法。确保在电源管理连接的高级属性中启用了这些设置。

活动的远程会话记录本地触摸屏输入

VDA 启用了 Remote PC Access 模式时，计算机将在活动会话期间忽略本地触摸屏输入。如果物理 PC 具有 Hyper-V 角色或者启用了任何基于虚拟化的安全功能，该 PC 将报告为虚拟机。如果 VDA 检测到它正在虚拟机上运行，则会自动禁用 Remote PC Access 模式。要启用 Remote PC Access 模式，请添加以下注册表设置：

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名称：ForceEnableRemotePC
- 类型：DWORD
- 数据：1

重新启动 PC 以使设置生效。

更多资源

下面是 Remote PC Access 的其他资源：

- 解决方案设计指南：Remote PC Access 设计决策。
- Remote PC Access 体系结构的示例：Citrix Remote PC Access 解决方案的参考体系结构。

App-V

April 8, 2022

结合使用 App-V 与 Citrix Virtual Apps and Desktops

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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

App-V	Citrix Virtual Apps and Desktops Delivery Controller	Citrix Virtual Apps and Desktops VDA
5.0 和 5.0 SP1	XenDesktop 7 至当前版本，XenApp 7.5 至当前版本	7.0 至当前版本
5.0 SP2	XenDesktop 7 至当前版本，XenApp 7.5 至当前版本	7.1 至当前版本
5.0 SP3 和 5.1	XenDesktop 7.6 至当前版本，XenApp 7.6 至当前版本	7.6.300 至当前版本
Windows Server 2016 中的 App-V	XenDesktop 7.12 至当前版本，XenApp 7.12 至当前版本	7.12 至当前版本

App-V 客户端不支持脱机访问应用程序。App-V 集成支持包括针对应用程序使用 SMB 共享。不支持 HTTP 协议。如果您不熟悉 App-V，请参阅 Microsoft 文档。下面概述了本文提及的 App-V 组件：

- 管理服务器。可提供一个中央控制台，用于管理 App-V 基础结构，并向 App-V 桌面客户端和远程桌面服务客户端交付虚拟应用程序。App-V 管理服务器将进行身份验证、发出请求并提供管理员所需的安全性、计量、监视及数据收集功能。服务器使用 Active Directory 和支持工具来管理用户和应用程序。
- 发布服务器。可为 App-V 客户端提供适用于特定用户的应用程序，并托管要通过流技术推送的虚拟应用程序软件包。它从管理服务器提取应用程序包。
- 客户端。检索虚拟应用程序、在客户端上发布应用程序以及在运行时自动设置和管理 Windows 设备上的虚拟环境。您可以在 VDA 上安装 App-V 客户端，用于存储用户特定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 Workspace 应用程序
- 通过 App-V 客户端和 Citrix Workspace 应用程序
- 同时由多个用户在多台设备上启动
- 通过 Citrix StoreFront

应用程序启动时，会实现修改的 App-V 应用程序属性。例如，对于修改过显示名称或具有自定义图标的应用程序，用户启动应用程序时会显示修改内容。在启动应用程序时，也会应用保存在动态配置文件中的应用程序自定义设置。

管理方法

您可以使用通过 App-V Sequencer 创建且位于 App-V 服务器或网络共享上的 App-V 包和动态配置文件。

- **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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

这种管理方法称为双管理，因为访问 App-V 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。在此方法中，管理服务器会处理动态配置文件。使用双管理员管理方法时，Citrix App-V 组件将管理应用程序启动所需的相应发布服务器的注册。这样可确保发布服务器在适当的时间为用户同步。发布服务器使用配置时使用的设置维护软件包生命周期的其他方面（例如登录时刷新和连接组）。

- 网络共享：将软件包和 XML 部署配置文件放置在网络共享上，可以使 Studio 不再依赖于 App-V 服务器和数据库基础结构，降低了开销。（必须在每个 VDA 上安装 Microsoft App-V 客户端。）

  这种管理方法称为单管理员，因为 App-V 包和应用程序仅需使用 Studio 控制台。您可以浏览到网络共享，并从该位置将一个或多个 App-V 软件包添加到站点级应用程序库 [1]。在此方法中，Citrix App-V 组件会在启动应用程序时处理部署配置文件。（用户配置文件不受支持。）使用单管理员管理方法时，Citrix App-V 组件会在主机上管理软件包的生命周期的所有方面。软件包在代理启动时或检测到配置变化（也可以在会话启动时）时添加到计算机中。收到来自 Citrix Workspace 应用程序的启动请求时，软件包首先按需发布给各个用户。

  单管理员还管理满足在 Studio 中做出的隔离组配置定义所需的连接组的生命周期。

  [1] 应用程序库是一个 Citrix 术语，是指用于存储有关 App-V 包的信息的缓存存储库。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。

在这两种管理方法中，如果将 VDA 配置为丢弃用户数据，则必须在下次会话启动时重做发布（或同步）。

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 服务器上或网络共享中的 App-V 包。

> 注意：
>
> 如果同时使用这两种管理方法，并且 App-V 包在两个位置都有动态配置文件，则使用 App-V 服务器中的文件（双管理）。

在 Studio 导航窗格中选择配置 **> App-V** 发布后，系统将显示 App-V 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。选择某个软件包后，详细信息窗格会列出该软件包中的应用程序和快捷方式。

动态配置文件

概述　可以使用动态配置文件自定义 App-V 包，在将动态配置文件应用于此软件包后，可以使用它来更改其特征。例如，您可以使用它们来定义额外的应用程序快捷方式和行为。Citrix App-V 支持两种类型的动态配置文件。在启动应用程序时应用文件设置：

- 部署配置文件可为所有用户提供计算机范围的配置。这些文件应命名为 *<packageFileName>*_DeploymentConfig.xml，并位于与其应用到的 App-V 包相同的文件夹中。单管理和双管理均支持。
- 用户配置文件可提供用户特定的配置，支持针对每个用户对软件包进行自定义设置。单管理支持采用以下格式的用户配置文件：*<packageFileName>*_[UserSID | Username | GroupSID |Group-Name_]UserConfig.xml，并且与其应用到的 App-V 包位于相同的文件夹中。

如果存在面向某个特定包的多个用户配置文件，则将按以下优先级顺序进行应用：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. 用户 SID
2. 用户名
3. AD 组 SID（首先应用找到的第一个 SID）
4. AD 组名称（首先应用找到的第一个组名称）
5. 默认值

例如

```
MyAppVPackage_S-1-5-21-000000001-0000000001-000000001-001_UserConfig.xml
MyAppVPackage_joeblogs_UserConfig.xml
MyAppVPackage_S-1-5-32-547_UserConfig.xml
MyAppVPackage_Power Users_UserConfig.xml
MyAppVPackage_UserConfig.xml
```

> 注意：
>
> 文件名中用户特定的部分也可以在结尾处选择性出现（例如 MyAppVPackage_UserConfig_**joeblogs**.xml）。

动态配置文件位置　在单管理方法中，Citrix App-V 组件仅处理与其 App-V 包位于同一文件夹中的动态配置文件。在启动程序包中的应用程序时，将会重新应用对相应动态配置文件所做的任何更改。如果您的动态配置文件与其软件包位于不同的位置，请使用映射文件将软件包映射到其部署配置文件。

创建映射文件

1. 打开新的文本文件。
2. 对于每个动态配置文件，添加一行，用于使用“<PackageGuid> : 路径”格式指定软件包的路径。

   例如：

   F1f4fd78ef044176aad9082073a0c780 : c:\widows\file\packagedeploy.xml
3. 将此文件另存为 ctxAppVDynamicConfigurations.cfg 并置于此软件包所在文件夹中。每次启动 App-V 包中的应用程序时，都会在与该软件包相同的 UNC 共享的整个目录层次结构中向上递归搜索此文件。

> 注意：
>
> 在包中的某个应用程序处于打开状态的用户会话中，不能对动态部署配置应用所做的更改。如果其他用户（而非当前用户）已打开该软件包中的某个应用程序，则可以将更改应用到动态用户配置文件。

将 **IIS** 配置为使用动态配置文件　根据 UNC 托管软件包使用的相同规则，VDA 上的 Citrix App-V 组件可以使用放置在软件包旁边的 App-V 部署配置文件和用户配置文件。
为此，VDA 组件需要浏览 IIS 目录结构以确定要使用的文件的权限。与 UNC 托管软件包不同，VDA 必须先将配置文件从服务器下载到主机上的临时位置，然后才能在发布中使用。这是一项可选功能，如果未启用目录浏览，则会忽略动态配置文件。

请执行以下步骤以对您的站点启用目录浏览：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. 在 IIS 管理器控制台中，选择 Web 站点节点，然后双击中央窗格中的目录浏览。
2. 单击右侧窗格中的启用，然后选择时间、大小、扩展和日期。（请勿选择“长日期”。）这使 VDA 上的 Citrix App-V 组件能够判断其是应用了最新版本的配置文件，还是需要更新。

隔离组

使用 App-V 单管理方法时，创建隔离组将允许您指定必须在沙盒中运行的互相依赖的应用程序组。该功能与 App-V 连接组相似，但并不完全一致。Citrix 使用“自动”和“显式”作为软件包部署选项，而非 App-V 管理服务器使用的强制和可选软件包术语。

- 用户启动 App-V 应用程序（主应用程序）时，会对隔离组进行搜索以查找其他标记为自动包含的应用程序软件包。这些软件包会自动下载并包含在隔离组中。您不必将其添加到包含主应用程序的交付组中。
- 只有在您已经将某个应用程序显式添加到包含主应用程序的同一个交付组的情况下，被标记为显式包含的隔离组中的该应用程序软件包才会下载。

这样，您可以创建包含各种全局适用于所有用户的自动包含应用程序的隔离组。此外，该组可以包含各种插件和其他（可能具有特定许可限制的）应用程序，您可以将其限制为某一组（通过交付组确定的）用户而无需创建更多的隔离组。

例如，应用程序“app-a”需要使用 JRE 1.7 才可运行。您可以创建一个包含 app-a（具有显式部署类型）和 JRE 1.7（具有自动部署类型）的隔离组。然后，将这些 App-V 包添加到一个或多个交付组中。用户启动 app-a 时，JRE 1.7 会通过它自动部署。

可以将一个应用程序添加到多个 App-V 隔离组。但是，当用户启动该应用程序时，始终会使用该应用程序添加到的首个隔离组。无法对包含该应用程序的其他隔离组进行排序或优先级划分。

对 **App-V** 服务器进行负载平衡

如果使用双管理方法，则支持使用 DNS 轮询对管理服务器和发布服务器进行负载平衡。由于 Studio 需要通过远程 PowerShell 与管理服务器进行通信，因此不支持对 Netscaler、F5（或类似）虚拟 IP 后的管理服务器进行负载平衡。有关详细信息，请参阅此 Citrix 博客文章。

将 **IIS** 配置为托管和通过流技术传输 **App-V** 包

要使 IIS 服务器能够托管和通过流技术传输 App-V 包，请执行以下步骤：

1. 打开 IIS 管理器控制台。有关说明，请参阅https://docs.microsoft.com/en-us/previous-versions/iis/6.0-sdk/ms525920(v%3Dvs.90)。
2. 右键单击要使用的 Web 站点实例，然后选择添加虚拟目录。
3. 键入别名以及您的软件包在网络中物理存储的路径。
4. 双击中央窗格中的 **MIME** 类型，然后右键单击窗口中的任意位置并选择添加。
5. 对于文件扩展名类型 `.appv`，请选择“MIME 类型 `application/app-v`”，然后单击确定。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

将 **HTTP** 流 **App-V** 包导入 **Citrix Virtual Apps and Desktops** 服务

> 注意：
>
> 此功能仅在版本 2009 及更高版本的 Virtual Delivery Agent (VDA) 上受支持。如果将包含 HTTP(S) 路径的 App-V 包中的应用程序添加到功能级别为 2003 或更高版本的交付组中，这些应用程序将发布到 Citrix Virtual Apps and Desktops 服务，但用户无法从 Citrix Cloud 启动，除非 VDA 的版本为 2009 或更高版本。创建交付组中介绍了交付组功能级别。

1. 下载并安装/解压 *CVAD* 远程 *PowerShell SDK* 和 *Citrix App-V* 包发现模块的最新版本。请参阅 Citrix Virtual Apps and Desktops 服务 SDK 和 API。
2. 使用软件包发现模块将 App-V 包从 IIS 服务器导入到 Citrix Virtual Apps and Desktops 服务。例如：

```
Import-Module <Download Directory>\Citrix.Cloud.AppLibrary.Admin.
    v1.psm1
Import-AppVPackageToCloud
 - PackagePath "https://My.AppVServer.net/Packages/Notepad++.appv"
<!--NeedCopy-->
```

3. 登录您的 Citrix Cloud 帐户。
4. 软件包将下载到计算机上的临时位置，您将从该位置提取相关信息并将其上载到 Citrix Virtual Apps and Desktops 服务实例中的应用程序库。

设置

下表概述了使用单管理员管理方法和双管理员管理方法在 Citrix Virtual Apps and Desktops 中使用 App-V 执行的设置任务的顺序。

单管理员	双管理	任务
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 包
X		添加 App-V 隔离组（可选）
X	X	向交付组添加 App-V 应用程序

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

部署 **Microsoft App-V**

有关 App-V 部署说明，请参阅 https://docs.microsoft.com/en-us/microsoft-desktop-optimization-pack/。

（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。

打包和放置

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，请将软件包及其相应的动态配置文件放置在 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，请从 UNC 路径在 App-V 管理服务器上发布软件包。（不支持从 HTTP URL 发布。）

无论软件包是位于 App-V 服务器上还是位于网络共享上，请确保软件包都具有相应的安全权限，以使 Studio 管理员可以访问它们。必须与“已通过身份验证的用户”共享网络共享以确保默认情况下 VDA 和 Studio 具有读取权限。

在 **Studio** 中配置 **App-V** 服务器地址

> 重要：
>
> Citrix 建议在 Controller 上使用 PowerShell cmdlet 指定 App-V 服务器地址（如果这些服务器使用非默认属性值）。有关详细信息，请参阅 SDK 文档。如果要在 Studio 中更改 App-V 服务器地址，您指定的某些服务器连接属性可能会重置为默认值。这些属性在 VDA 上用于连接到 App-V 发布服务器。如果出现此情况，请重新配置服务器上所有已重置的属性的非默认值。

此过程仅适用于双管理方法。

在创建站点期间或创建之后，为双管理方法指定 App-V 管理和发布服务器地址。您可以在创建站点期间或创建之后执行此操作。

在创建站点期间：

- 在向导的 **App-V** 页面上，输入 Microsoft App-V 管理服务器的 URL 以及 App-V 发布服务器的 URL 和端口号。
- 在继续向导之前，请测试此连接。如果测试失败，请参阅下文“故障排除”部分。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

在创建站点之后：

1. 在 Studio 导航窗格中选择配置 **> App-V** 发布。
2. 如果您先前未指定 App-V 服务器地址，请在“操作”窗格中选择添加 **Microsoft** 服务器。
3. 要更改 App-V 服务器地址，请在“操作”窗格中选择编辑 **Microsoft** 服务器。
4. 输入 Microsoft App-V 管理服务器的 URL 以及 App-V 发布服务器的 URL 和端口号。
5. 在关闭此对话框之前，请测试与这些服务器的连接。如果测试失败，请参阅下文“故障排除”部分。

之后，如果要删除指向 App-V 管理和发布服务器的所有链接，并阻止 Studio 从这些服务器中发现 App-V 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。

在 **VDA** 计算机上安装软件

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 客户端可存储用户特定的虚拟应用程序设置，例如各个用户的配置文件中的注册表和文件更改。

App-V 客户端可从 Microsoft 获取。在包含 VDA 的每台计算机上或计算机目录用于创建 VM 的主映像上安装客户端。注意：Windows 10（1607 或更高版本）和 Windows Server 2016 已包括 App-V 客户端。请仅在这些操作系统中，通过运行 PowerShell **Enable-AppV** cmdlet（不带任何参数）来启用 App-V 客户端。**Get-AppVStatus** cmdlet 将检索当前的启用状态。

> 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，则运行 **Set-AppvClientConfiguration -EnablePackageScripts $true**。

Citrix App-V 组件　安装 VDA 时，会默认排除 Citrix App-V 组件软件。

您可以在 VDA 安装过程中控制此默认行为。在图形界面中，选中附加组件页面上的 **Citrix Personalization for App-V - VDA** 复选框。在命令行接口中，使用 **/includeadditional**“**Citrix Personalization for App-V –VDA**”选项。

如果您在 VDA 安装过程中未包括 Citrix App-V 组件，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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

在应用程序库中添加或删除 **App-V** 包

这些过程仅适用于单管理方法。

您必须对包含 App-V 包的网络共享至少具有读取访问权限。

向应用程序库添加 **App-V** 包

1. 在 Studio 导航窗格中选择配置 **> App-V** 发布。
2. 在“操作”窗格中选择添加软件包。
3. 浏览到包含 App-V 包的共享并选择一个或多个软件包。
4. 单击添加。

从应用程序库中删除 **App-V** 包

从应用程序库删除 App-V 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”窗格中选择删除软件包。

添加、编辑或删除 **App-V** 隔离组

添加 **App-V** 隔离组

1. 在 Studio 导航窗格中选择 **App-V** 发布。
2. 在“操作”窗格中选择添加隔离组。
3. 在添加隔离组设置对话框中，键入隔离组的名称和说明。
4. 从“可用软件包”列表中，选择您想要添加到隔离组中应用程序，然后单击右键。选定的应用程序现在应显示在“隔离组中的软件包”列表中。在每个应用程序旁边的部署下拉列表中，选择显式或自动。您也可以使用向上和向下箭头来更改列表中应用程序的顺序。
5. 完成后，单击确定。

编辑 **App-V** 隔离组

1. 在 Studio 导航窗格中选择 **App-V** 发布。
2. 在中间窗格中选择隔离组选项卡，然后选择要编辑的隔离组。
3. 在“操作”窗格中选择编辑隔离组。
4. 在编辑隔离组设置对话框中，更改隔离组名称或说明、添加或删除应用程序、更改其部署类型或更改应用程序顺序。
5. 完成后，单击确定。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

删除 **App-V** 隔离组　删除隔离组不会删除应用程序软件包。只会删除分组。

1. 在 Studio 导航窗格中选择 **App-V** 发布。
2. 在中间窗格中选择隔离组选项卡，然后选择要删除的隔离组。
3. 在“操作”窗格中选择删除隔离组。
4. 确认删除。

向交付组添加 **App-V** 应用程序

以下过程重点介绍如何向交付组添加 App-V 应用程序。有关创建交付组的完整详细信息，请参阅创建交付组。

步骤 **1**：选择您是要创建新的交付组还是要将 App-V 应用程序添加到现有交付组：

要创建包含 App-V 应用程序的交付组，请执行以下操作：

1. 在 Studio 导航窗格中选择交付组。
2. 在“操作”窗格中选择创建交付组。
3. 在一系列向导页面上，指定计算机目录和用户。

要将 App-V 应用程序添加到现有交付组，请执行以下操作：

1. 在 Studio 导航窗格中选择应用程序。
2. 在“操作”窗格中选择添加应用程序。
3. 选择要添加 App-V 应用程序的一个或多个交付组。

步骤 **2**：在向导的应用程序页面上，单击添加下拉列表以显示应用程序源。选择 **App-V**。

步骤 **3**：在添加 **App-V** 应用程序页面上，选择“App-V 源”：App-V 服务器或应用程序库。生成的显示内容包括应用程序名称及其软件包名称和软件包版本。选中要添加的应用程序或应用程序快捷方式旁边的复选框。然后单击确定。

步骤 **4**：完成向导。

须知：

- 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。
- 如果您使用动态配置文件来自定义 App-V 应用程序的属性，则在将其添加到交付组时，这些属性会覆盖您所做的任何更改。
- 如果以后编辑包含 App-V 应用程序的交付组，而该组的交付类型从“桌面和应用程序”更改为“仅限应用程序”，则 App-V 应用程序性能不会发生变化。
- 从交付组中删除以前发布的（单管理员）App-V 包时，Citrix App-V 客户端组件会尝试清理、取消发布和删除单管理员管理方法不再使用的任何包。
- 如果使用混合部署，即包由单管理员管理方法和 App-V 发布服务器提供，由双管理员或其他机制（例如组策略）进行管理，则无法确定哪个（现在可能是冗余的）软件包来自哪个源。在这种情况下，不会尝试清理。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 如果在单个交付组中发布了 100 多个 App-V 应用程序，应用程序可能无法启动。如果是这样，请在相应的绑定元素上使用 MaxReceivedMessageSize 属性来增加 Delivery Controller 和/或 VDA 上的 Broker Agent 配置中的最大应收邮件大小。

故障排除

标有“(双)”的问题只有在使用双管理方法时才会发生。

(双) 在 Studio 导航窗格中选择配置 **> App-V** 发布时出现 PowerShell 连接错误。

- Studio 管理员是否同时是 App-V 服务器管理员？Studio 管理员必须属于 App-V 管理服务器上的“管理员”组才能与之通信。

(双) 在 Studio 中指定 App-V 服务器地址时，测试连接操作返回错误。

- 是否已启动 App-V 服务器？请发送 Ping 命令或检查 IIS 管理器；每个 App-V 服务器均应处于“已启动”或“正在运行”状态。
- 是否已在 App-V 服务器上启用 PowerShell 远程处理？如果未启用，请参阅 https://docs.microsoft.com/en-us/previous-versions/technet-magazine/ff700227(v=msdn.10)。
- Studio 管理员是否同时是 App-V 服务器管理员？Studio 管理员必须属于 App-V 管理服务器上的管理员组才能与之通信。
- 是否已在 App-V 服务器上启用文件共享？在 Windows 资源管理器中或在“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。有关指导，请参阅 http://support.microsoft.com/kb/306541。
- App-V 服务器是否位于 Active Directory 中？

  如果 Studio 计算机与 App-V 服务器分别位于不存在信任关系的不同 Active Directory 域中，请从 Studio 计算机上的 PowerShell 控制台运行 **winrm s winrm/Config/client ‘@(TrustedHosts=”*<App-V server FQDN>*”)’**。

  如果 TrustedHosts 由 GPO 管理，将显示以下错误消息：“*The config setting TrustedHosts cannot be changed because use is controlled by policies.* 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 策略中添加 App-V 服务器名称条目（管理模板 > Windows 组件 > Windows 远程管理 (WinRM) > WinRM 客户端）。

(双) 在将 App-V 应用程序添加到交付组时，发现失败。

- Studio 管理员是否同时是 App-V 管理服务器管理员？Studio 管理员必须属于 App-V 管理服务器上的管理员组才能与之通信。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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://docs.microsoft.com/en-us/previous-versions/technet-magazine/ff700227(v=msdn.10)。
- 软件包是否具有适当的安全权限以供 Studio 管理员访问？

App-V 应用程序只在一个浏览器版本启动。

- 如果发布同一浏览器应用程序的多个排序版本，VDA 上的每个用户一次只能启动该应用程序的一个版本。即使不涉及 Citrix 组件，并且用户从指向不同路径的桌面快捷方式启动排序的版本时，也会出现相同的情况。

  无论用户首先启动哪个浏览器版本，都将决定随后为其运行的浏览器版本。Firefox 检测到自己的第二次启动时，它会首选创建已在运行的进程的实例，而不是创建新进程。其他浏览器的行为方式可能相同。

  您可以通过将命令行参数 **-no-remote** 添加快捷方式的启动命令，以实现在目标 Firefox 浏览器版本中启动应用程序。其他浏览器提供相同或类似的工具。

  > 注意：
  >
  > 必须使用 XenApp 7.17 或更高版本才能利用快捷方式枚举功能。您还必须在该应用程序的两个版本中更改软件包才能获取此双向行为。

App-V 应用程序不启动。

- （双）发布服务器是否正在运行？
- （双）App-V 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 \*` 以显示发布服务器的列表。
- （双）在 App-V 发布服务器上，确保 UserRefreshonLogon 设置为“False”。
- （双）在 App-V 发布服务器上，以管理员身份运行 **Set-AppvPublishingServer** 并将 UserRefreshonLogon 设置为 False。
- VDA 上是否安装了受支持版本的 App-V 客户端？VDA 是否已启用 **enable package scripts**（启用软件包脚本）设置？
- 在包含 App-V 客户端和 VDA 的计算机的“注册表编辑器”(regedit) 中，转到 HKEY_LOCAL_MACHINE\SOFTWARE\Policies 确保 AppVServers 注册表项的值为以下格式：AppVManagementServer+metadata;PublishingServer（例如 `http://xmas-demo-appv.blrstrm.com+0+0+0+1+1+1+0+1;http://xmas-demo-appv.blrstrm.com:8082`）。
- 在包含 App-V 客户端和 VDA 的计算机或主映像上，检查 PowerShell ExecutionPolicy 是否已设置为“RemoteSigned”。Microsoft 提供的 App-V 客户端未进行签名，而此 ExecutionPolicy 允许 PowerShell 运行未签名的本地脚本和 cmdlet。请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) 在“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”。
- 如果出现错误“RegistrationManager.AttemptRegistrationWithSingleDdc: Failed to register”（RegistrationManager.AttemptRegistrationWithSingleDdc: 注册失败），请在相应的绑定元素上使用 MaxRe-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ceivedMessageSize 属性来增加 Delivery Controller 和/或 VDA 上的 Broker Agent 配置中的最大应收邮件大小。

如果这些步骤无法解决问题，则应启用并检查日志。

日志

与 App-V 配置相关的所有日志均位于 C:\CtxAppvLogs 中。应用程序启动日志位于%LOCALAPPDATA%\Citrix\CtxAppvLogs 中。LOCALAPPDATA 会解析为已登录用户的本地文件夹。检查应用程序启动失败的用户的本地文件夹。

要启用 App-V 所使用的 Studio 和 VDA 日志，您必须具有管理员权限。此外，您还需要使用文本编辑器（例如记事本）。

要启用 Studio 日志，请执行以下操作：

1. 创建文件夹 C:\CtxAppvLogs。
2. 转至 C:\Program Files\Citrix\StudioAppVIntegration\SnapIn\Citrix.Appv.Admin.V1。在文本编辑器中打开 CtxAppvCommon.dll.config，然后取消注释以下行：<add key =” LogFileName” value=” C:\CtxAppvLogs\log.txt” />
3. 重新启动 Broker Service 以启动日志记录。

要启用 VDA 日志，请执行以下操作：

1. 创建文件夹 C:\CtxAppvLogs。
2. 转至 C:\Program Files\Citrix\Virtual Desktop Agent。在文本编辑器中打开 CtxAppvCommon.dll.config，然后取消注释以下行：<add key =” LogFileName” value=” C:\CtxAppvLogs\log.txt” />
3. 取消注释以下行并将值字段设置为 1：<add key =” EnableLauncherLogs” value=” 1” />
4. 重新启动计算机以启动日志记录。

发布内容

January 21, 2022

可以发布只是指向资源（例如 Microsoft Word 文档或 Web 链接）的 URL 或 UNC 路径的应用程序。此功能称为已发布的内容。发布内容功能提高了向用户交付内容的灵活性。您可从对应用程序的现有访问控制和管理中受益。还可以指定是使用本地应用程序还是已发布的应用程序打开内容。

在 StoreFront 和 Citrix Workspace 应用程序中，已发布的内容就像其他应用程序一样显示。用户访问这些内容的方式与访问应用程序一样。在客户端上，资源按常规方式打开。

- 如果某个本地安装的应用程序合适，会启动它来打开资源。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 如果定义了文件类型关联，则会启动已发布的应用程序来打开资源。

可使用 PowerShell SDK 发布内容。不能使用 Studio 发布内容。但是，可以在发布了内容后，使用 Studio 编辑应用程序属性。

配置概述和准备

发布内容通过使用 `New-BrokerApplication` cmdlet 与以下主要属性进行。（有关所有 cmdlet 属性的说明，请参阅 cmdlet 帮助。）

```
1 New-BrokerApplication  -ApplicationType PublishedContent -
     CommandLineExecutable location -Name app-name -DesktopGroup delivery
     -group-name
2 <!--NeedCopy-->
```

`ApplicationType` 属性必须为 `PublishedContent`。

`CommandLineExecutable` 属性指定已发布的内容的位置。支持以下格式，字符数上限为 255。

- HTML Web 站点地址（例如 http://www.citrix.com）
- Web 服务器上的文档文件（例如 `https://www.citrix.com/press/pressrelease.doc`）
- FTP 服务器上的目录（例如 `ftp://ftp.citrix.com/code`）
- FTP 服务器上的文档文件（例如 `ftp://ftp.citrix.com/code/Readme.txt`>）
- UNC 目录路径（例如 `file://myServer/myShare or \\\\\myServer\\myShare`）
- UNC 文件路径（例如 `file://myServer/myShare/myFile.asf` 或 `\\myServer\myShare\myFile.asf`）

请确保您有正确的 SDK。

- 对于 Citrix Virtual Apps and Desktops 服务部署，请下载并安装 Citrix Virtual Apps and Desktops 远程 PowerShell SDK。
- 对于本地 Citrix Virtual Apps and Desktops 部署，请使用与 Delivery Controller 一起安装的 PowerShell SDK。要添加一款已发布的内容应用程序，至少使用 7.11 版的 Delivery Controller。

以下过程使用多个示例。在这些示例中：

- 创建了计算机目录。
- 已创建名为 `PublishedContentApps` 的交付组。该组使用该目录中的多会话操作系统计算机。已将 WordPad 应用程序添加到该组。
- 分配了交付组名称、`CommandLineExecutable` 位置和应用程序名称。

入门

在包含 PowerShell SDK 的计算机上打开 PowerShell。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

以下 cmdlet 添加合适的 PowerShell SDK 管理单元，以及分配返回的交付组记录。

```
Add-PsSnapin Citrix\* $dg = Get-BrokerDesktopGroup -Name PublishedContentApps
```

如果要使用 Citrix Virtual Apps and Desktops 服务，请输入您的 Citrix Cloud 凭据进行身份验证。如果有多个客户，请选择一个。

发布 **URL**

分配了位置和应用程序名称后，以下 cmdlet 将 Citrix 主页作为应用程序发布。

```
$citrixUrl = "https://www.citrix.com/"
$appName = "Citrix Home Page"

New-BrokerApplication -ApplicationType PublishedContent -
    CommandLineExecutable $citrixURL -Name $appName -DesktopGroup $dg.
    Uid
<!--NeedCopy-->
```

验证成功：

- 打开 StoreFront 以可以访问 PublishedContentApps 交付组中应用程序的用户身份登录。显示内容包括具有默认图标的新创建的应用程序。要了解自定义图标，请参阅 https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/。
- 单击 **Citrix** 主页应用程序。将在本地运行的默认浏览器实例中启动新选项卡并访问该 URL。

发布位于 **UNC** 路径的资源

在本示例中，管理员已创建了一个名为 `PublishedResources` 的共享。分配了位置和应用程序名称后，以下 cmdlet 在该共享中将 RTF 和 DOCX 文件作为资源发布。

```
$rtfUNC = "\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedRTF.rtf"
$rtfAppName = "PublishedRTF"

New-BrokerApplication -ApplicationType PublishedContent
 -CommandLineExecutable $rtfUNC -Name $rtfAppName
-DesktopGroup $dg.Uid

$docxUNC = "\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx
    "
$docxAppName = "PublishedDOCX"

New-BrokerApplication -ApplicationType PublishedContent
 -CommandLineExecutable $docxUNC -Name $docxAppName
-DesktopGroup $dg.Uid
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

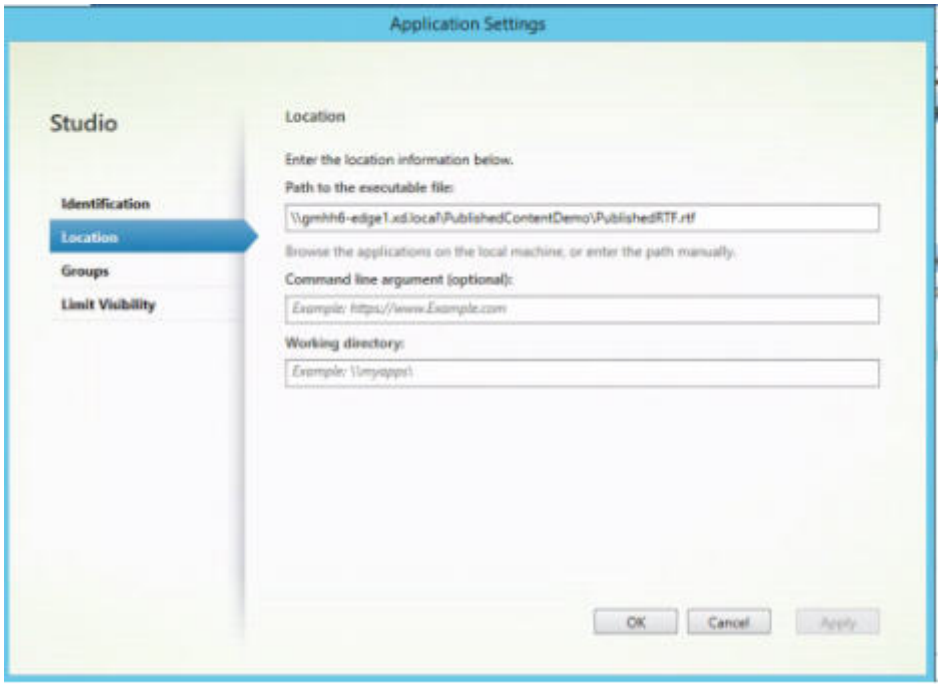
验证成功：

- 刷新 StoreFront 窗口查看新发布的文档。
- 单击 **PublishedRTF** 和 **PublishedDOCX** 应用程序。各文档均在本地运行的 WordPad 中打开。

查看并编辑 **PublishedContent** 应用程序

可使用与其他应用程序类型相同的方法管理已发布的内容。已发布的内容项显示在 Studio 中的应用程序列表中，且可在 Studio 中编辑。

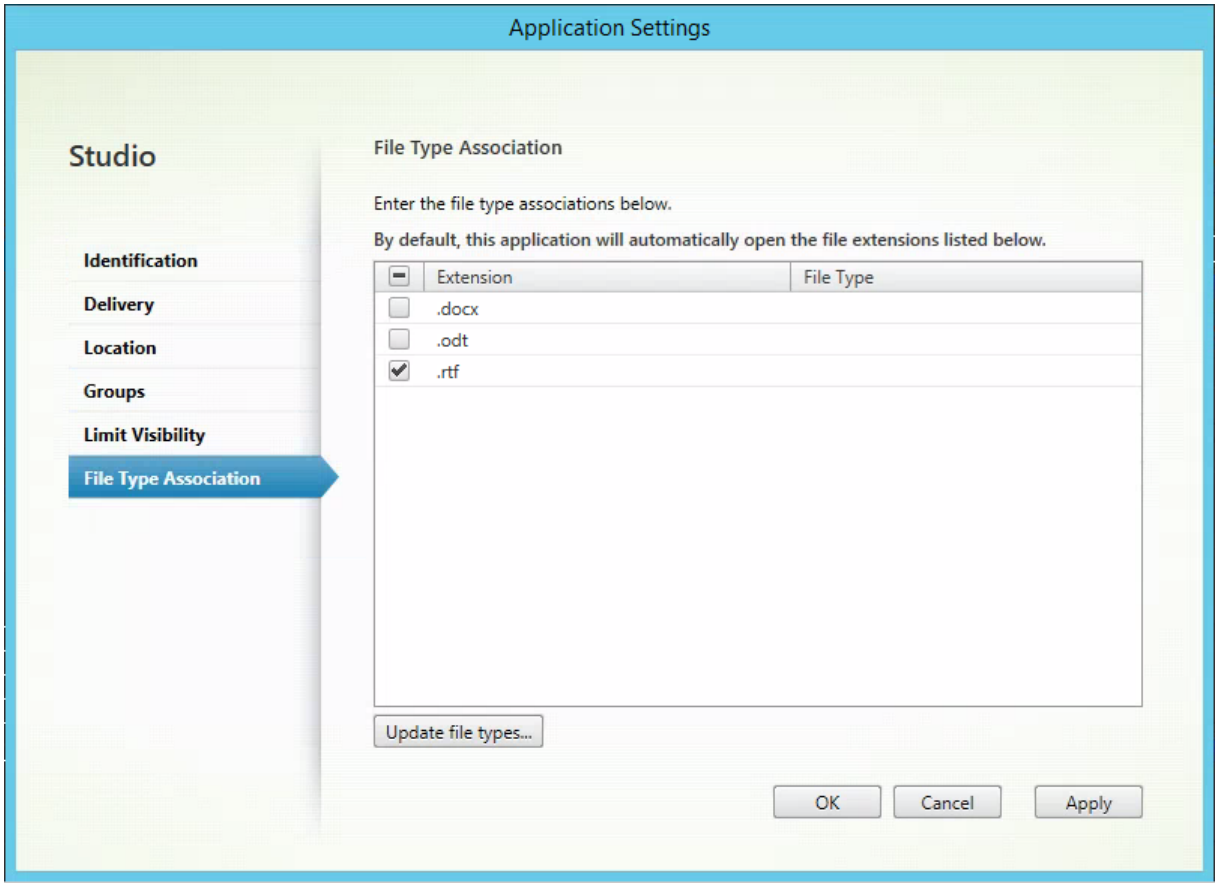
应用程序属性（例如用户可见性、组关联和快捷方式）会应用于已发布的内容。但是，您无法在位置页面上更改命令行参数和工作目录属性。要更改资源，请在该页面上修改可执行文件的路径字段。



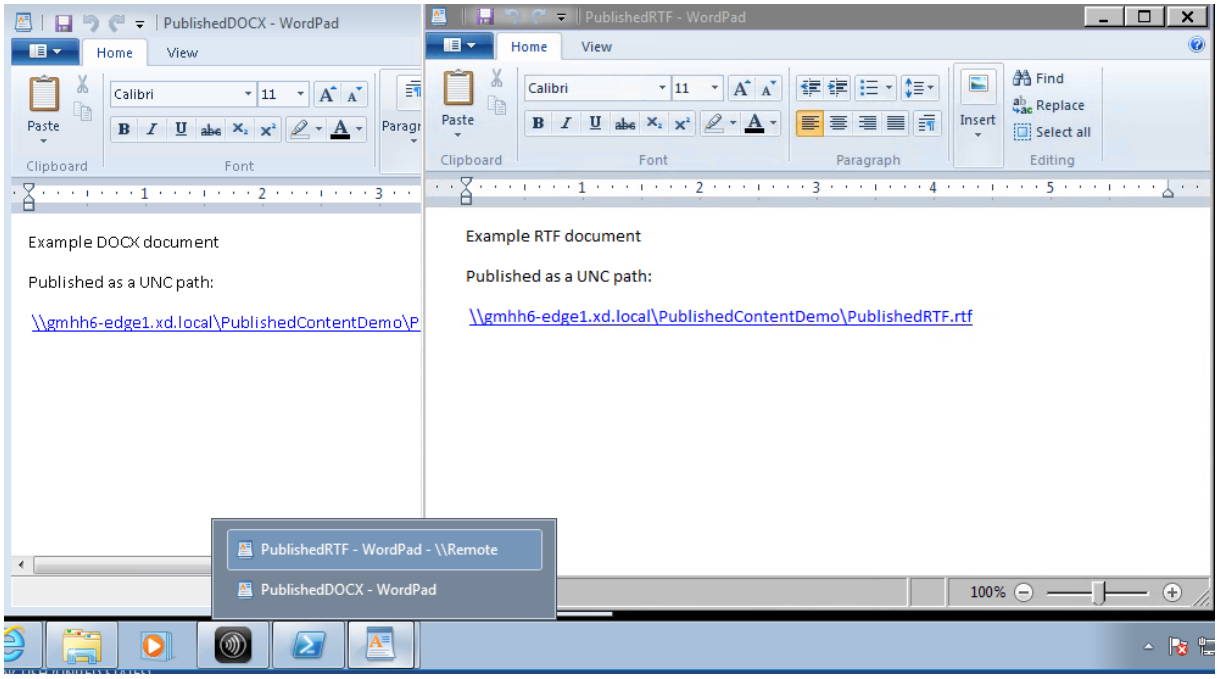
要使用已发布的应用程序打开 `PublishedContent` 应用程序（而非本地应用程序），请编辑已发布的应用程序的文件类型关联属性。在此示例中，已编辑了已发布的 WordPad 应用程序来为.rtf 文件创建文件类型关联。

请先为交付组打开维护模式，然后再编辑文件类型关联。请务必在完成编辑后关闭维护模式。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



刷新 StoreFront 以加载文件类型关联更改，然后单击 **PublishedRTF** 和 **PublishedDOCX** 应用程序。请注意差异。**PublishedDOCX** 仍在本地 WordPad 中打开。但是，由于文件类型关联，**PublishedRTF** 现在在已发布的 WordPad 中打开。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

相关详细信息

- 创建计算机目录
- 创建交付组
- 更改应用程序属性

服务器 VDI

January 21, 2022

通过“服务器 VDI”（虚拟桌面基础结构）功能，可以从服务器操作系统为单个用户交付桌面。

- 企业管理员可以将服务器操作系统作为 VDI 桌面进行交付，这对于工程师和设计师等用户非常有帮助。
- 服务提供商可以从云端提供桌面。这些桌面受 Microsoft 服务提供商许可协议 (SPLA) 约束。

支持：

- 在 Citrix Virtual Apps and Desktops 和 Citrix Virtual Apps and Desktops 服务部署中，Windows Server 2022、Windows Server 2019 和 Windows Server 2016 计算机支持服务器 VDI。
- 所有服务器 VDI 部署都支持用户个性化层技术。
- 要使服务器 VDI 能够与扫描仪等 TWAIN 设备结合使用，必须安装 Windows 服务器桌面体验功能。
- 服务器 VDI 不支持以下功能：
  - 托管应用程序
  - 本地应用程序访问
  - 直接（非代理）桌面连接
  - Remote PC Access

安装和配置服务器 VDI

1. 准备 Windows 服务器以便进行安装。
   - 通过 Windows Server Manager，确保未安装远程桌面服务角色服务。如果先前已安装这些服务，请将其删除。如果安装这些角色服务，VDA 安装将失败。
   - 确保已启用 **Restrict each user to a single session**（限制每个用户只能进行一个会话）属性。在 Windows Server 上，在注册表中编辑端点服务器设置：

     ```
     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer

     DWORD fSingleSessionPerUser = 1
     ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. 使用 Citrix Virtual Apps and Desktops 安装程序的命令行接口在支持的服务器或服务器主映像上安装 VDA，同时指定 /quiet 和 /servervdi 选项。（默认情况下，安装程序的图形界面阻止在服务器操作系统中安装 Windows 单会话操作系统 VDA。使用命令行将替换此行为。）使用以下命令之一：

   - Citrix Virtual Apps and Desktops 部署：
     - XenDesktopVdaSetup.exe /quiet /servervdi
     - VDAWorkstationSetup.exe /quiet /servervdi
   - Citrix Virtual Apps and Desktops 服务部署：
     - VDAWorkstationSetup.exe /quiet /servervdi

   其他选项：

   - 使用 /controllers 指定 Delivery Controller 或 Cloud Connector。
   - 使用 /enable_hdx_ports 在防火墙中打开端口，除非要手动配置防火墙。
   - 如果要在映像上安装 VDA，并使用 MCS 从该映像创建服务器 VM，请使用 /mastermcsimage（或 /masterimage）。
   - 有关所有选项详细信息，请参阅使用命令行安装。

3. 为服务器 VDI 创建计算机目录。在目录创建向导中执行以下操作：

   - 在操作系统页面上，选择单会话操作系统。
   - 在摘要页面上，为管理员指定可明确将其标识为服务器 VDI 的计算机目录名称和说明。在 Studio 中，只能通过该内容来指示目录支持服务器 VDI。

   在 Studio 中使用搜索功能时，服务器 VDI 目录将显示在单会话操作系统计算机选项卡上，即使此 VDA 安装在多会话计算机上亦如此。

4. 创建交付组，并选择您创建的服务器 VDI 目录。

如果在 VDA 安装期间未指定 Delivery Controller 或 Cloud Connector，请务必在之后进行指定。有关详细信息，请参阅 VDA 注册。

用户个性化层

July 5, 2024

Citrix Virtual Apps and Desktops 的用户个性化层功能扩展了非持久性计算机目录的功能，以便跨会话保留用户的数据和本地安装的应用程序。用户个性化层功能由基础 Citrix App Layering 技术提供支持，支持非持久计算机目录中的 Citrix Provisioning 和 Machine Creation Services (MCS)。

在主映像中，将用户个性化层组件与 Virtual Delivery Agent 一起安装。VHD 文件在本地存储用户安装的应用程序。映像上装载的 VHD 充当用户自己的虚拟硬盘驱动器。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 重要：
>
> 可以在 Citrix Virtual Apps and Desktops 中部署用户个性化层，或者使用在映像模板中启用的 App Layering 用户层，但不同时启用两者。请勿在 App Layering 层上安装用户个性化层功能。

此功能取代了 Personal vDisk (PvD)，同时还为非持久性池桌面环境中的用户提供持久的 Workspace 体验。

要部署用户个性化层功能，请使用本文中详细介绍的步骤进行安装和配置。在此之前，该功能不可用。

应用程序支持

除了以下例外，用户个性化层支持用户在桌面上本地安装的所有应用程序。

例外

以下应用程序是例外情况，不支持用户个性化层：

- 企业应用程序，例如 MS Office 和 Visual Studio。
- 修改网络堆栈或硬件的应用程序。示例：VPN 客户端。
- 具有引导级驱动程序的应用程序。示例：病毒扫描仪。
- 使用驱动程序存储的驱动程序的应用程序。示例：打印机驱动程序。

  > 注意：
  >
  > 可以使用 Windows 组策略对象 (GPO) 使打印机可用。

不允许用户在本地安装任何不受支持的应用程序。而是直接在主映像上安装这些应用程序。

需要本地用户或管理员帐户的应用程序

当用户在本地安装应用程序时，应用程序会进入其用户层。如果用户随后添加或编辑本地用户或组，则更改不会在会话之外保留。

> 重要：
>
> 在主映像中添加任何必需的本地用户或组。

要求

用户个性化层功能需要以下组件：

- Citrix Virtual Apps and Desktops 7 1909 或更高版本

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Virtual Delivery Agent (VDA)，版本 1912
- Citrix Provisioning，版本 1909 或更高版本
- Windows 文件共享 (SMB) 或启用了本地 AD 身份验证的 Azure 文件

当操作系统作为单个会话部署时，可以在以下 Windows 版本上部署用户个性化层功能。支持仅限于单个会话中的单个用户。

- Windows 10 Enterprise x64，版本 1607 或更高版本
- Windows 10 多会话（支持 Azure 文件）
- Windows Server 2016（支持 Azure 文件）
- Windows Server 2019（支持 Azure 文件）

对于 Citrix Virtual Apps and Desktops 7，Windows Server 2019、Windows Server 2016v 和 Windows 10 客户端支持在用户个性化层中使用 Azure 文件。

> 注意：
>
> 用户个性化层仅支持作为服务器 VDI 部署。有关部署详细信息，请参阅服务器 VDI 一文。
>
> 用户个性化层每次仅支持每台计算机一个用户，然后必须重新启动计算机才能重置磁盘。不能将用户个性化层用于多会话服务器操作系统，只能用于单会话服务器系统。用户个性化层仅适用于非持久性桌面。

卸载用户个性化层功能（如果已安装）。在安装最新版本之前，请重新启动主映像。

设置文件共享

用户个性化层功能需要 Windows 服务器消息块 (SMB) 存储。要创建 Windows 文件共享，请按照您所在的 Windows 操作系统的常规步骤进行操作。

有关将 Azure 文件与基于 Azure 的目录结合使用的更多信息，请参阅为用户个性化层设置 Azure 文件存储。

建议

请按照本部分中的建议进行成功的用户个性化层部署。

Profile Management 解决方案

用户个性化层存储用户对单个计算机目录映像所做的所有更改。要在多个目录映像中添加漫游配置文件数据等增强功能，Citrix 也建议使用 Profile Management。有关更多详细信息，请参阅 Profile Management 文档。

将 Profile Management 与用户个性化层功能结合使用时，请取消选择在注销时删除用户的信息的功能。可以使用组策略对象 (GPO) 或 Delivery Controller (DDC) 上的策略取消选择删除选项。

有关可用的 Profile Management 策略的详细信息，请参阅 Profile Management 策略描述和默认设置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Microsoft System Center Configuration Manager (SCCM)

如果将 SCCM 与用户个性化层功能结合使用，请按照 Microsoft 的指导原则在 VDI 环境中准备您的映像。有关详细信息，请参阅此 Microsoft TechNet 文章。

用户层大小

用户层是一个精简预配的磁盘，随着磁盘空间的使用而扩展。允许的默认用户层大小为 10 GB，即，我们建议的最小值。

> 注意：
>
> 在安装过程中，如果该值设置为零 (0)，则默认用户层大小设置为 10 GB。

如果要更改用户层大小，可以为用户层大小 Studio 策略输入其他值。请参阅可选：单击“用户层大小 **(GB)**”旁边的选择下的步骤 **5**：创建交付组自定义策略

用于覆盖用户层大小的工具（可选）

通过使用 Windows 工具定义用户层文件共享的配额，可以覆盖用户层大小。

请使用以下 Microsoft 配额工具之一在名为用户的用户层目录上设置硬配额：

- 文件服务器资源管理器 (FSRM)
- 配额管理器

> 注意：
>
> 增加配额会影响新用户层并扩展现有用户层。减少配额仅影响新用户层。现有用户层的大小永远不会减小。

部署用户个性化层

部署用户个性化功能时，可以在 Studio 中定义策略。然后将策略分配给绑定到计算机目录的交付组，该交付组部署了该功能。

如果您保留未设置用户个性化层配置的主映像，服务将处于空闲状态，并且不会干扰创作活动。

如果在主映像中设置了策略，服务将尝试在主映像中运行和装载用户层。主映像将表现出意外的行为和不稳定性。

要部署用户个性化层功能，请按此顺序完成以下步骤：

- 步骤 1：验证 Citrix Virtual Apps and Desktops 环境的可用性。
- 步骤 2：准备您的主映像。
- 步骤 3：创建计算机目录。
- 步骤 4：创建交付组。
- 步骤 5：创建交付组自定义策略。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

步骤 **1**：验证 **Citrix Virtual Apps and Desktops** 环境是否可用

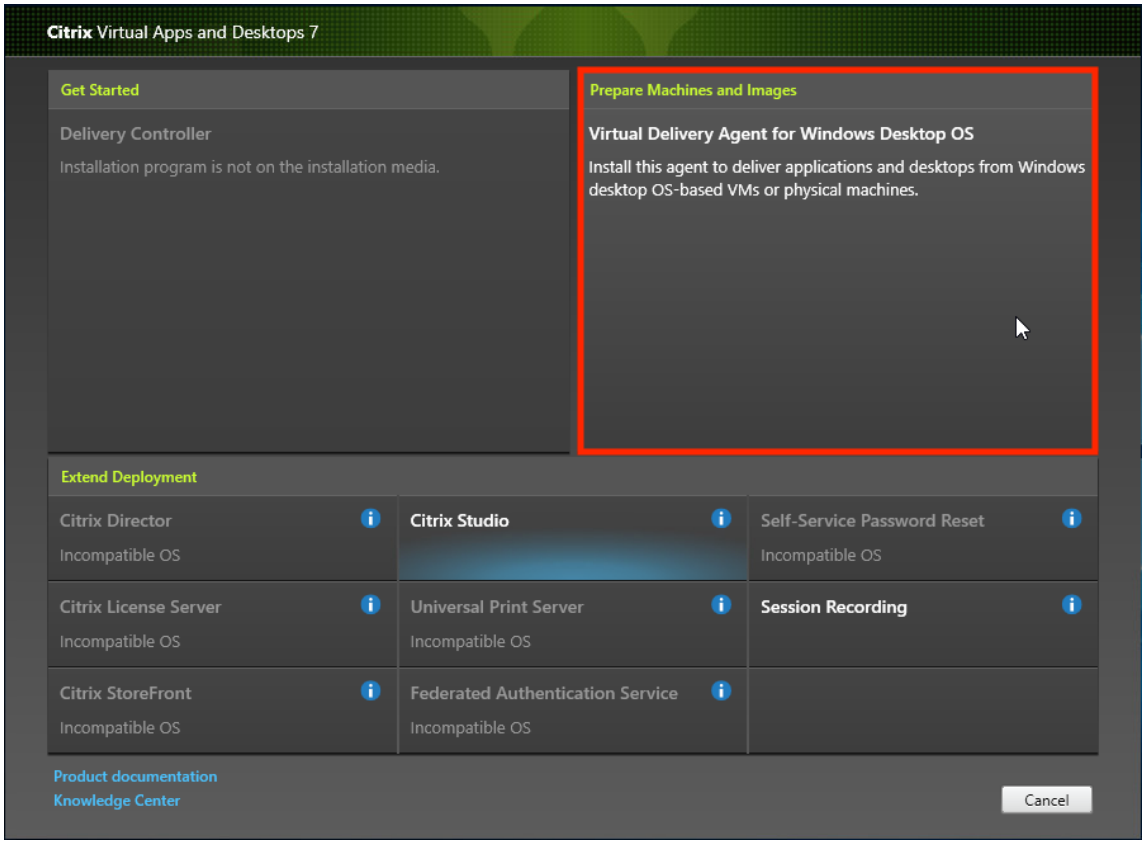
请确保 Citrix Virtual Apps and Desktops 环境可使用这一新增功能。有关设置详细信息，请参阅“安装和配置 Citrix Virtual Apps and Desktops”。

步骤 **2**：准备您的主映像

要准备主映像，请执行以下操作：

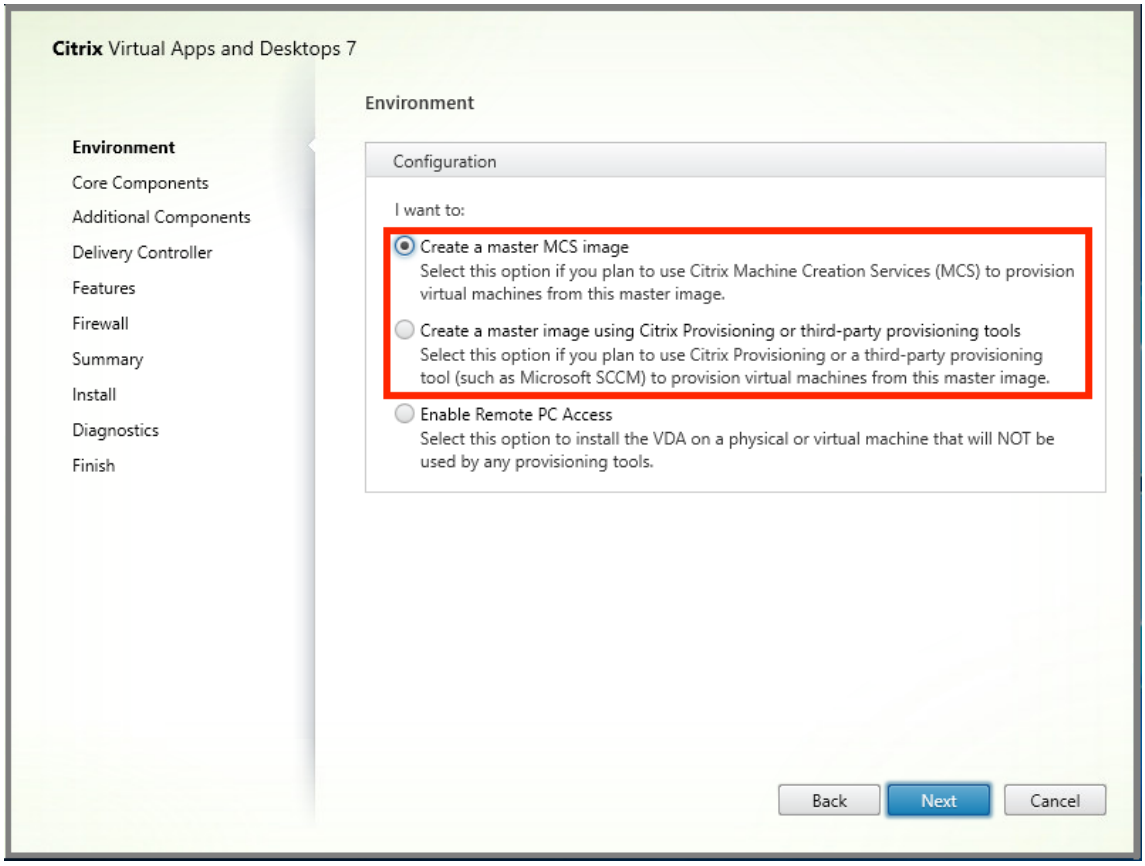
1. 找到主映像。安装贵组织的企业应用程序和用户通常认为有用的任何其他应用程序。
2. 如果要部署服务器 VDI，请按照服务器 VDI 一文中的步骤进行操作。请确保包含可选组件，即用户个性化层。有关详细信息，请参阅用于安装 VDA 的命令行选项。
3. 如果您使用的是 Windows 10，请安装 Virtual Delivery Agent (VDA) 1912。如果已安装较旧版本的 VDA，请先卸载旧版本。安装新版本时，请确保选择并安装可选组件 **Citrix User Personalization Layer**，如下所示：

   a) 单击磁贴 **Virtual Delivery Agent for Windows Desktop OS**：



   a) 环境：选择“创建主 MCS 映像”或“使用 Citrix Provisioning 或第三方预配工具创建主映像”。

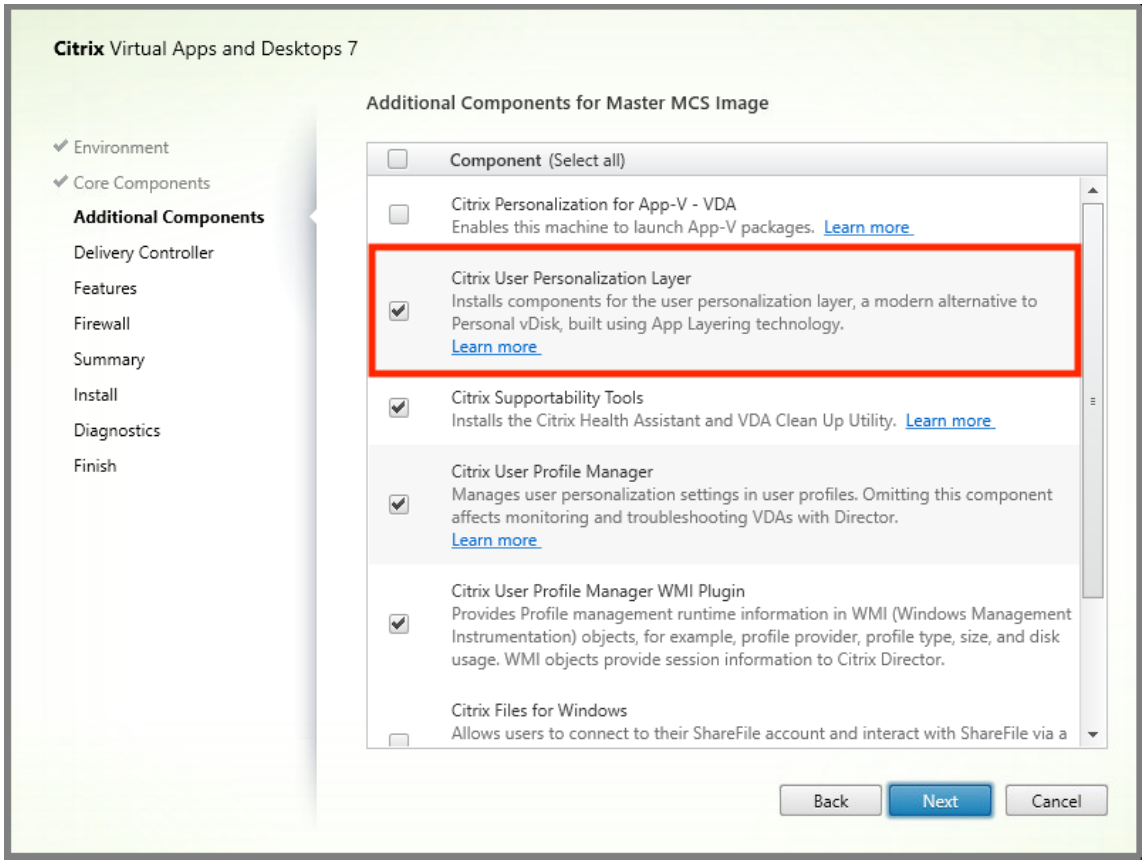
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



a) 核心组件：单击下一步。

b) 其他组件：选中 **Citrix User Personalization Layer**。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



a) 单击其余的安装屏幕，根据需要配置 VDA，然后单击“安装”。映像在安装过程中重新启动一次或多次。

4. 保留 **Windows** 更新处于禁用状态。用户个性化层安装程序将禁用映像上的 Windows 更新。保留更新处于禁用状态。

映像已准备好上载到 Studio 中。

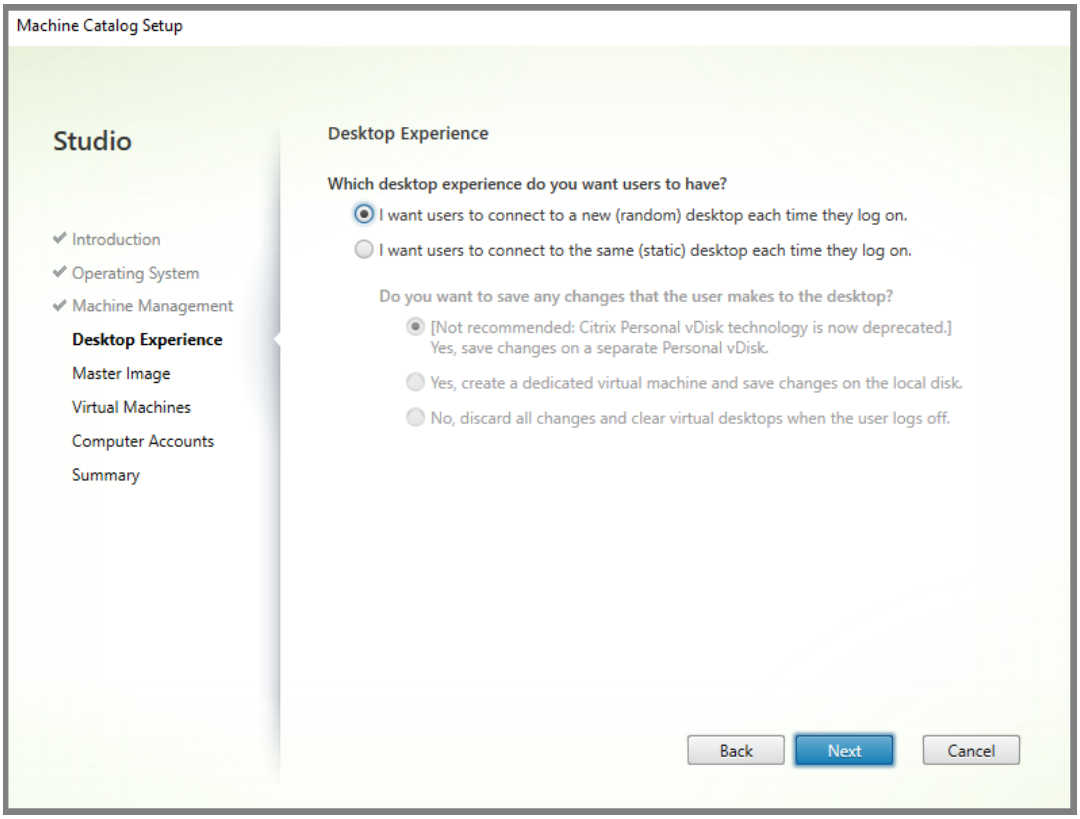
步骤 **3**：创建计算机目录

在 Studio 中，按照步骤创建计算机目录。在目录创建过程中使用以下选项：

1. 选择操作系统并将其设置为单会话操作系统。
2. 选择计算机管理并将其设置为进行电源管理的计算机。例如，虚拟机或刀片式 PC。
3. 选择桌面体验并将其设置为池随机或池静态目录类型，如以下示例中所示：

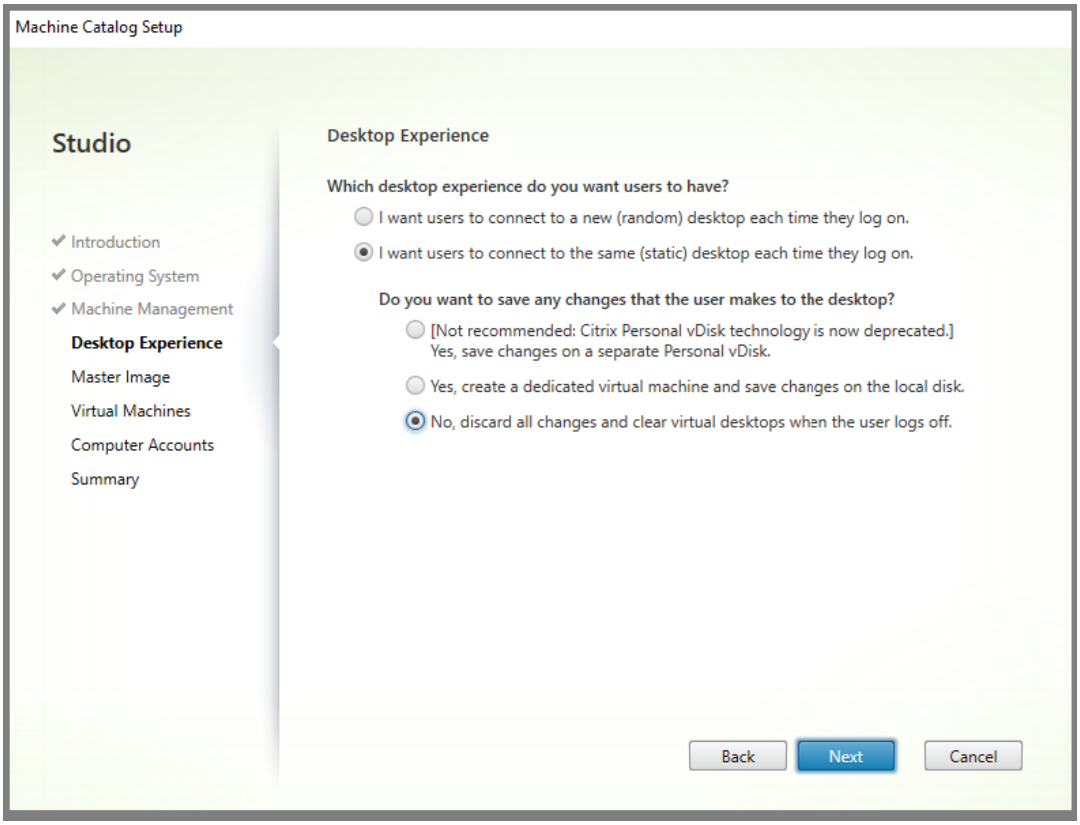
   - 池随机：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- 池静态：如果选择池静态，请将桌面配置为放弃所有更改并在用户注销时清除虚拟桌面，如以下屏幕截图中所示：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> 注意：
>
> 用户个性化层不支持配置为使用 Citrix Personal vDisk 或分配为专用虚拟机的池静态目录。

4. 如果使用的是 MCS，请为在上一部分中创建的映像选择主映像和快照。
5. 根据您的环境的需要配置其余的目录属性。

步骤 **4**：创建交付组

创建和配置交付组，包括您创建的计算机目录中的计算机。有关详细信息，请参阅创建交付组。

步骤 **5**：创建交付组自定义策略

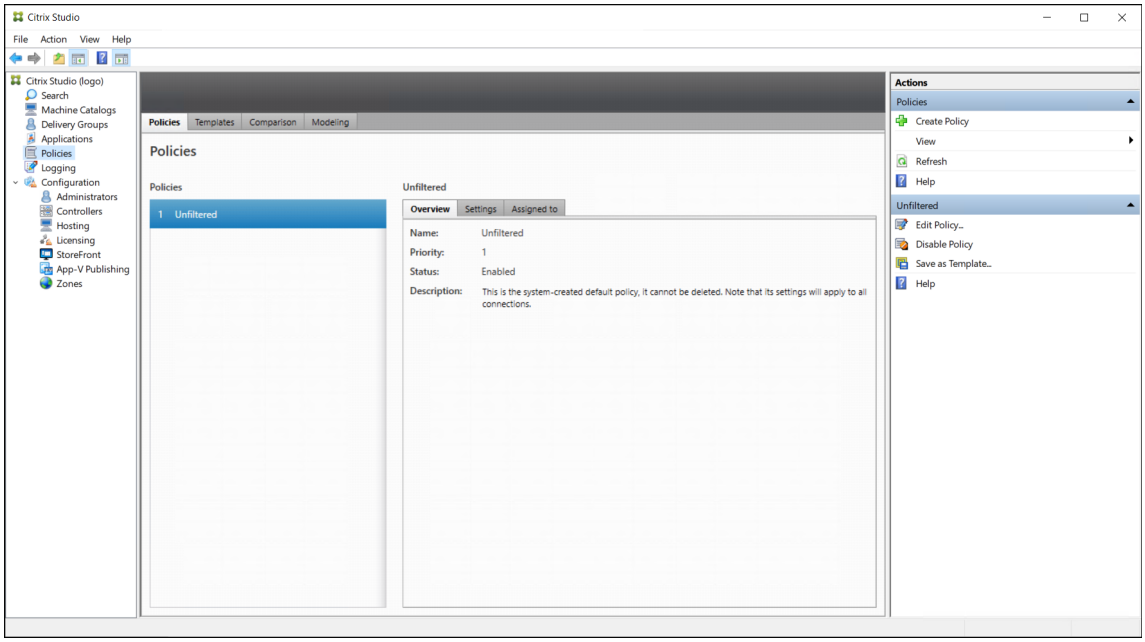
要在 Virtual Delivery Agent 中启用用户层的装载，请使用配置参数指定：

- 在网络上访问用户层的位置。
- 允许用户层磁盘增长的大小。

在 Studio 中将参数定义为自定义 Citrix 策略并将其分配给交付组。

1. 在 Studio 中，在导航窗格中选择“策略”：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

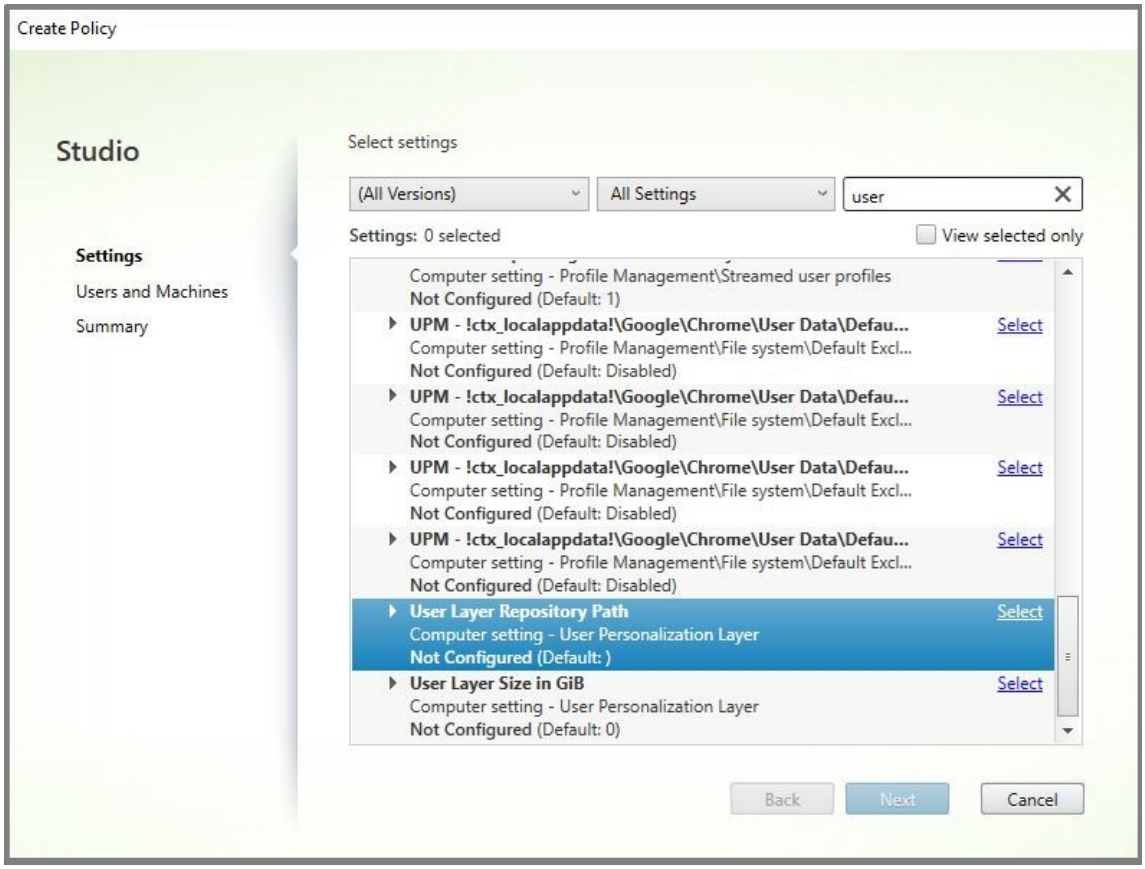


2. 在“操作”窗格中选择“创建策略”。此时将显示创建策略窗口。
3. 在搜索字段中键入“用户层”。可用策略列表中显示以下两个策略：
   - 用户层存储库路径
   - 用户层大小 (GB)

   > 注意：
   >
   > 增加大小会影响新用户层并扩展现有用户层。减小大小仅影响新用户层。现有用户层的大小永远不会减小。

4. 单击“用户层存储库路径”旁边的选择。此时将显示编辑设置窗口。

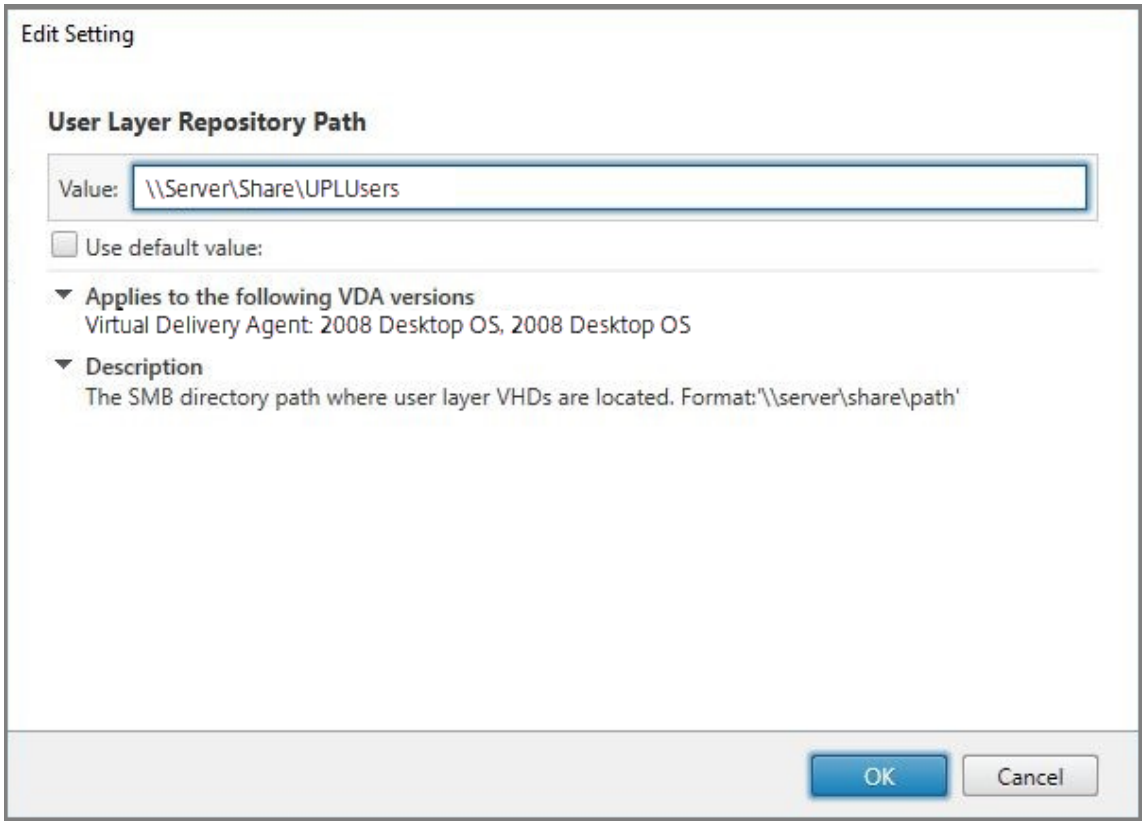
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. 在“值”字段中输入路径，然后单击确定。

   - 路径格式：`\\server-name-or-address\share-name\folder`
   - 路径示例：`\\Server\Share\UPLUsers`
   - 结果路径示例：对于 **CoolCompanyDomain** 中名为 **Alex** 的用户，路径将为：`\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`

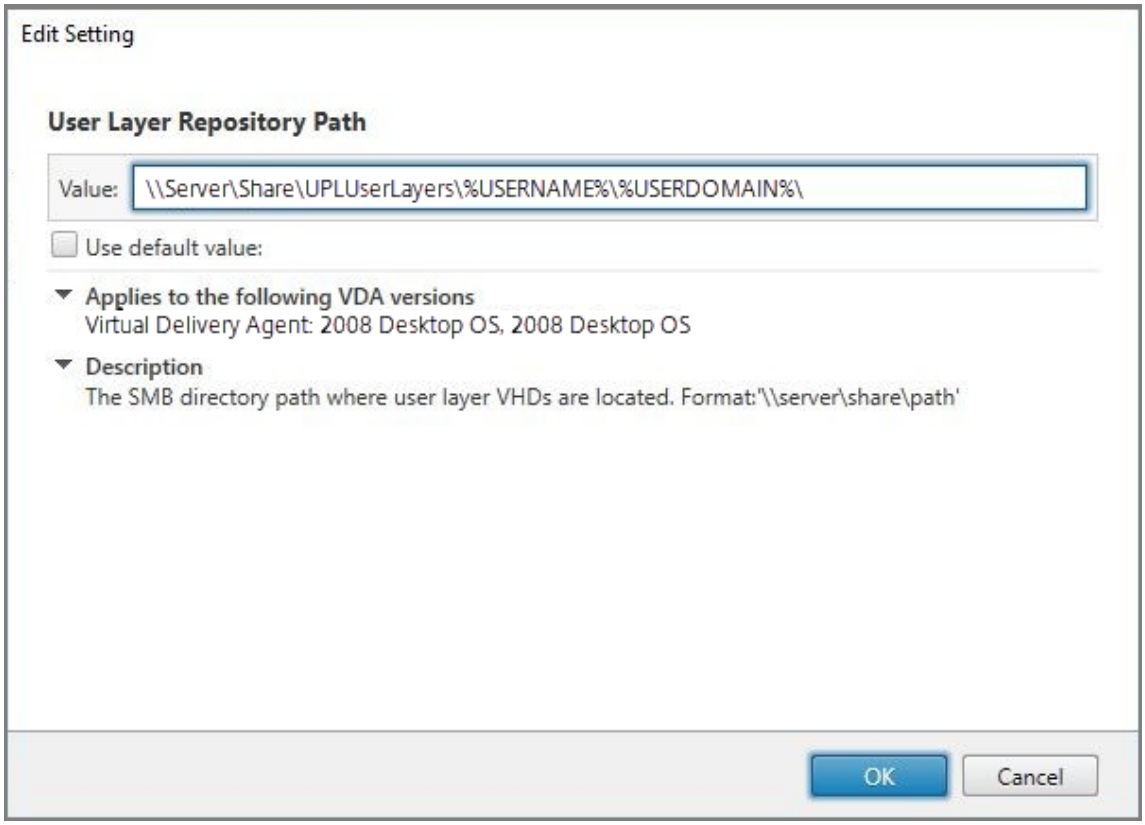
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



可以使用变量 %USERNAME%、%USERDOMAIN% 以及计算机环境变量自定义路径。展开时，这些变量会生成显式路径。

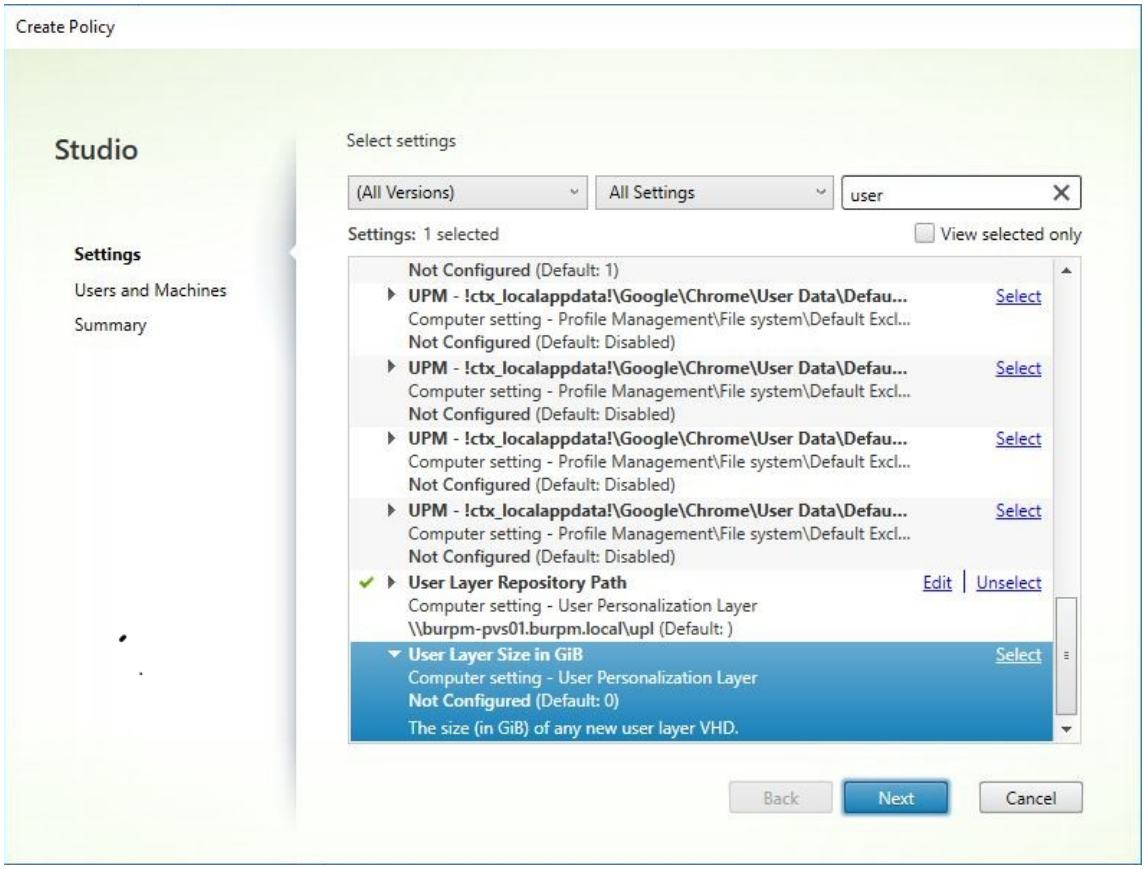
- 路径格式：\\Server-name-or-address\share-name\folder-with-environment-variables
- 路径示例：\\Server\Share\UPLUserLayers\\%USERNAME%\\%USERDOMAIN%
- 结果路径示例：对于 **CoolCompanyDomain** 中名为 **Alex** 的用户，路径将为：\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



6. 可选：单击“用户层大小 (GB)”旁边的选择：

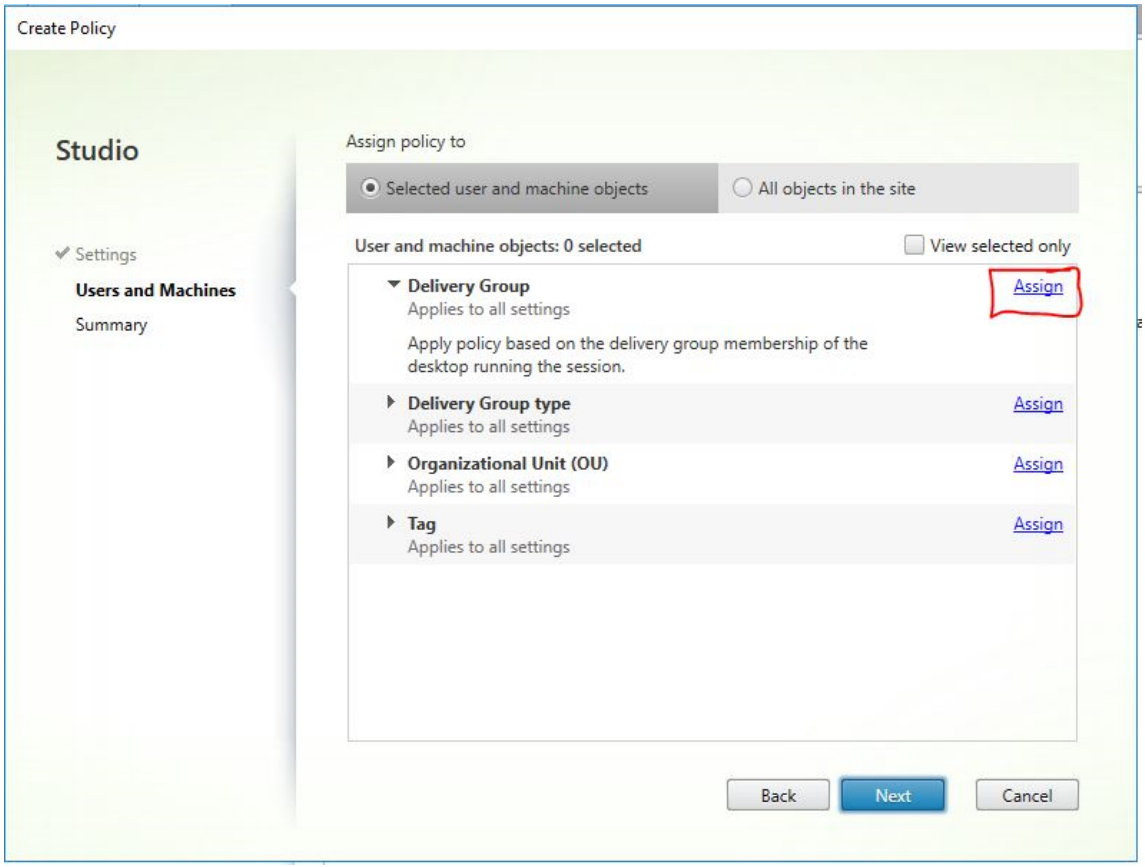
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



此时将显示“编辑设置”窗口。

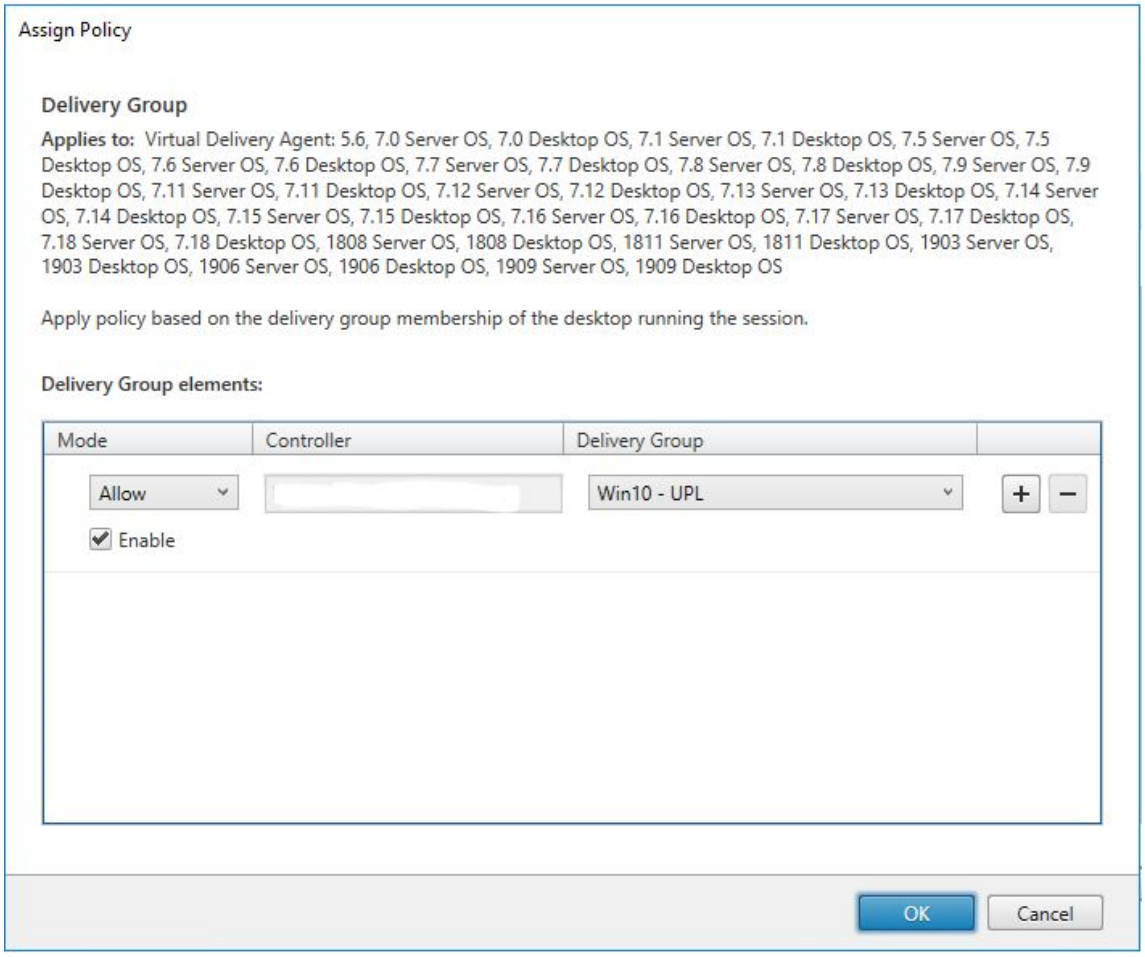
7. 可选：将默认值 **10 GB** 更改为每个用户层可增长的最大大小。单击确定。
8. 单击下一步以配置用户和计算机。单击此图像中突出显示的交付组分配链接：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



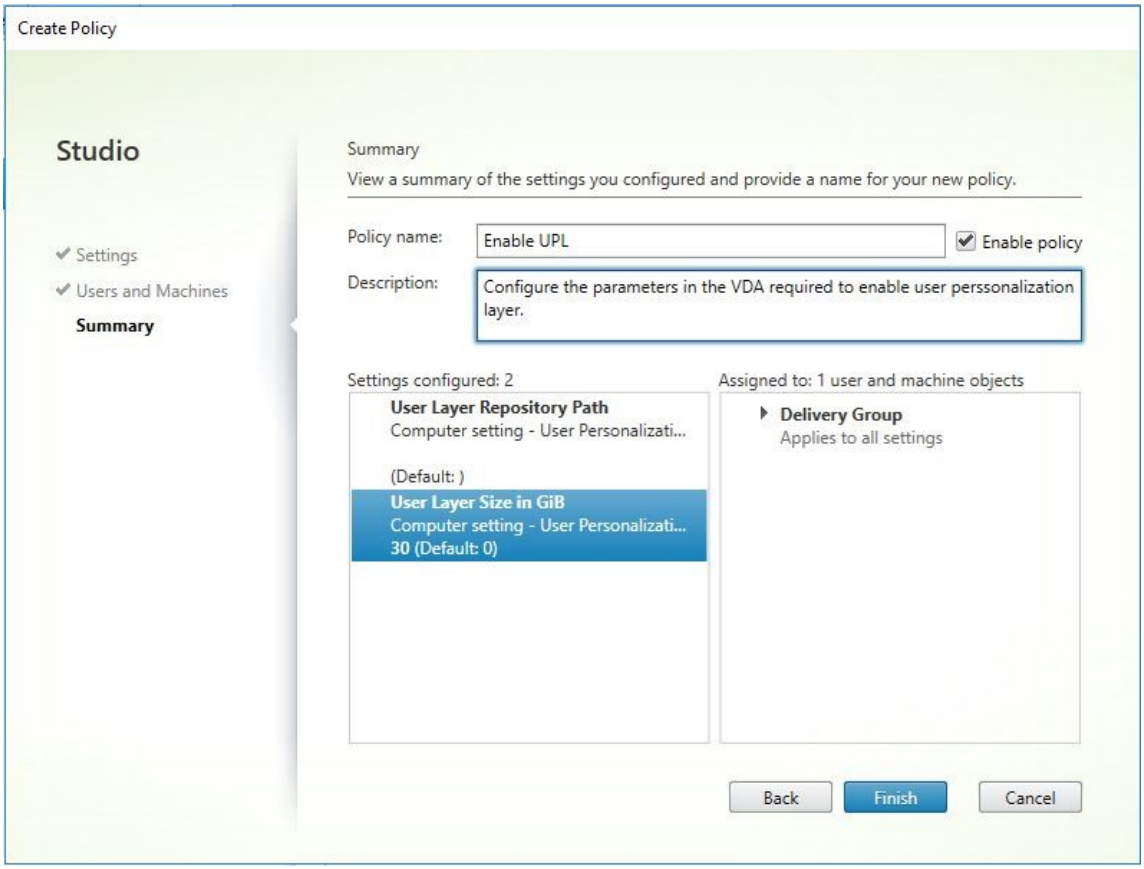
9. 在“交付组”菜单中，选择在上一部分中创建的交付组。单击确定。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



10. 输入策略的名称。单击该复选框以启用该策略，然后单击完成。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



在用户层文件夹上配置安全设置

作为域管理员，您可以为用户层指定多个存储位置。为每个存储位置（包括默认位置）创建 `\Users` 子文件夹。使用以下设置保护每个位置。

设置名称	值	适用对象
创建者/所有者	修改	仅子文件夹和文件
所有者权利	修改	仅子文件夹和文件
用户或组：	创建 Folder/Append Data; Traverse Folder/Execute File; List Folder/Read Data; Read Attributes	仅限选定的文件夹
系统	完全控制	选定的文件夹、子文件夹和文件
域管理员和选定的管理员组	完全控制	选定的文件夹、子文件夹和文件

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

用户层消息

当用户无法访问其用户层时，将收到这些通知消息之一。

- 正在使用的用户层

  ```
  We were unable to attach your user layer because it is in use.
  Any changes you make to application settings or data will not be
  saved. Be sure to save any work to a shared network location.<!--
  NeedCopy-->
  ```

- 用户层不可用

  ```
  We were unable to attach your user layer. Any changes you make to
   application settings or data will not be saved. Be sure to save
  any work to a shared network location.<!--NeedCopy-->
  ```

- 用户注销后无法重置系统

  ```
  This system was not shut down properly. Please log off immediately
   and contact your system administrator.<!--NeedCopy-->
  ```

故障排除时要使用的日志文件

日志文件 ulayersvc.log 包含记录更改的用户个性化层软件的输出。

```
C:\ProgramData\Unidesk\Logs\ulayersvc.log
<!--NeedCopy-->
```

限制

安装和使用用户个性化层功能时，请谨记以下限制。

- 请勿尝试在 App Layering 中的层上部署用户个性化层软件。请在 Citrix Virtual Apps and Desktops 中部署用户个性化层，或者在 App Layering 映像模板中启用用户层，但不同时启用两者。任一过程都会生成所需的用户层。
- 请勿使用持久性计算机目录配置用户个性化层功能。
- 请勿使用会话主机。
- 请勿使用运行新操作系统安装的映像更新计算机目录（甚至是相同版本的 Windows 10）。最佳做法是在创建计算机目录时使用的同一主映像中将更新应用于操作系统。
- 请勿使用启动时间驱动程序，而非任何其他早期启动个性化设置。
- 请勿将 PvD 数据迁移到用户个性化层功能。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 请勿将现有用户层从完整的 App Layering 产品迁移到用户个性化层功能。
- 请勿更改用户层 SMB 路径以访问使用其他主操作系统映像创建的用户层。
- 当用户注销会话然后重新登录时，新会话将在池中的另一台计算机上运行。在 VDI 环境中，Microsoft 软件中心在第一台计算机上将应用程序列出为已安装，但在第二台计算机上将其显示为不可用。

  要了解应用程序的真实状态，请指示用户在“软件中心”中选择该应用程序，然后单击安装。SCCM 随后将状态更新为真实值。
- 在启用了用户个性化层功能的 VDA 中启动后，Software Center 偶尔会立即停止。为了避免出现此问题，请按照 Microsoft 关于 在 XenDesktop VDI 环境中实施 SCCM 的建议进行操作。此外，请确保 `ccmexec` 服务在您启动 Software Center 之前正在运行。
- 在组策略（计算机设置）中，用户层设置会覆盖应用到主映像的设置。因此，使用 GPO 在计算机设置中所做的更改并不总是存在以供用户下一次会话登录使用。

  要解决此问题，请创建一个发出此命令的用户登录脚本：

  ```
  gpupdate /force
  ```

  例如，一个客户将以下命令设置为在每次用户登录时运行：

  ```
  gpudate /Target:Computer /force
  ```

  为获得最佳效果，请在用户登录后直接将更改应用于用户层上的“计算机设置”。

删除组件

January 21, 2022

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。例如，删除 Delivery Controller 时，不会删除 SQL Server 软件和数据库。

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。

有关删除下文未提到的功能的信息，请参阅相应功能的文档。

准备

删除 Controller 之前，请先将其从站点中删除。有关详细信息，请参阅删除 Controller。

先关闭 Studio 和 Director，然后再将其删除。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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，请右键单击 **Citrix Virtual Apps *** 版本 *** 或 ****Citrix Virtual Apps and Desktops *** 版本 ***，然后选择卸载 **。此时将启动安装程序。选择要删除的组件。

  也可以右键单击 **Citrix StoreFront** 并选择 卸载来删除 StoreFront。
- 要删除 VDA，请右键单击 **Citrix Virtual Delivery Agent** 版本，然后选择 卸载。此时将启动安装程序，从中可选择要删除的组件。默认情况下，计算机将在删除后自动重新启动。
- 要删除通用打印服务器，请右键单击 **Citrix** 通用打印服务器，然后选择卸载。

使用命令行删除核心组件

从 `\x64\XenDesktop Setup` 目录中运行 `XenDesktopServerSetup.exe` 命令。

- 要删除一个或多个组件，请指定 `/remove` 和 `/components` 选项。
- 要删除所有组件，请指定 `/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 `\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。例如，要删除 VDA 和 Citrix Workspace 应用程序，请使用 `/remove /components vda,plugin`。
- `/removeall` 选项仅删除 VDA。不会删除 Citrix Workspace 应用程序。

有关命令和参数的详细信息，请参阅使用命令行安装。

默认情况下，计算机将在删除后自动重新启动。

要使用 Active Directory 中的脚本删除 VDA，请参阅使用脚本安装或删除 Virtual Delivery Agent。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

升级和迁移

April 3, 2024

简介

通过升级可以将您的部署更改为 Citrix Virtual Apps and Desktops 7 当前版本 (CR)，而不需要设置新的计算机或站点。这称为原位升级。

通过升级，可以访问您有资格访问的最新功能和技术。升级还可以包含早期版本中的修复、声明和增强功能。

升级概述

1. 开始升级之前，请先查看升级部署一文。这是学习如何准备和实施升级的主要信息源。
2. 完成准备指南。
3. 运行安装程序以升级核心组件。
4. 升级系统数据库和站点。
5. 升级映像上（或直接在计算机上）的 VDA。
6. 升级其他组件。

每个准备和升级步骤都在升级部署中进行详细介绍。

可以升级的版本

Citrix 升级指南中列出了可从中升级的 Citrix Virtual Apps and Desktops（以及 XenApp 和 XenDesktop）版本。

常见问题解答

本部分内容解答有关升级 Citrix Virtual Apps and Desktops 的一些常见问题。

- 升级我的 **Virtual Apps and Desktops** 环境的正确顺序是什么**?**

  有关推荐升级顺序的插图和说明，请参阅升级顺序和升级过程。

- 我的站点有多个 **Delivery Controller**（在不同的区域中）。如果我只升级其中一部分 **Delivery Controller**，会出现什么情况？我是否需要在同一维护时段内升级站点中的每个 **Controller**?

  最佳做法是在同一维护时段内升级所有 Delivery Controller，因为每个 Controller 上的各种服务相互通信。保留不同版本可能会导致出现问题。在维护时段内，我们建议您升级一半 Controller，升级站点，然后升级其余的 Controller。（有关详细信息，请参阅升级过程。）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 我可以直接转至最新版本，还是需要执行增量升级**?**

  除非您要升级到的版本的新增功能一文中明确说明，否则您几乎可以始终升级到最新版本并跳过中间版本。请参阅升级指南。

- 客户是否可以从长期服务版本 **(LTSR)** 环境升级到当前版本**?**

  是。客户无需在长期服务版本上延长一段时间。客户可以根据业务要求和功能将 LTSR 环境移至当前版本。

- 是否允许使用混合版本的组件**?**

  在每个站点中，Citrix 建议将所有组件都升级到相同的版本。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。有关详细信息，请参阅混合环境注意事项。

- 必须多长时间升级一次当前版本**?**

  当前版本在发布日期后的 6 个月达到维护期结束 (EOM)。Citrix 建议客户采用最新的当前版本。当前版本在发布日期后的 18 个月达到生命周期结束 (EOM)。有关详细信息，请参阅当前版本的生命周期。

- 建议升级到 **LTSR** 还是 **CR?**

  当前版本 (CR) 提供最具创新性的最新应用程序、桌面和服务器虚拟化特性和功能。这允许您保持前沿技术和竞争的领先地位。

  长期服务版本 (LTSR) 非常适合于在较长的时间内保留相同基础版本的大型企业生产环境。

  有关详细信息，请参阅服务方案。

- 我是否需要升级我的许可证**?**

  确保当前许可证的日期尚未过期，并且对要升级到的版本有效。请参阅 CTX111618。有关续订的信息，请参阅 Customer Success Services 续订许可证。

- 升级需要多长时间?

  升级部署所需的时间因基础结构和网络而异。因此，我们无法提供确切的时间。

- 最佳做法是什么**?**

  确保您理解并遵循准备指南。

- 支持哪些操作系统**?**

  要升级到的版本的系统要求一文列出了受支持的操作系统。

  如果您的当前部署使用不再受支持的操作系统，请参阅早期版本的操作系统。

- 支持哪些版本的 **VMware vSphere (vCenter + ESXi)?**

  CTX131239 列出了受支持的主机和版本，以及指向已知问题的链接。

- 我的版本何时达到 **EOL?**

  查看产品列表。

- 最新版本的已知问题是什么**?**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Citrix Virtual Apps and Desktops
- StoreFront
- Citrix Provisioning
- Citrix 许可证服务器
- 适用于 Windows 的 Citrix Workspace 应用程序

更多信息

长期服务版本 (LTSR) 部署更新使用累积更新 (CU)。CU 更新 LTSR 的基础组件，每个 CU 包括自己的 Metainstaller。

每个 CU 都具有专用文档。例如，对于 7.15 LTSR，请查看该 LTSR 的新增功能 页面上面向最新 CU 的链接。每个 CU 页面包括受支持的版本信息、说明以及指向 CU 下载软件包的链接。

迁移

迁移到云

可以使用适用于 Citrix Virtual Apps and Desktops 的自动配置工具将本地部署迁移到云中。有关详细信息，请参阅迁移到云。

传统迁移

将数据从早期部署迁移到更新版本。此过程包括安装更新版本的组件和创建新站点，从旧场导出数据，然后将数据导入到新站点。

不支持用于迁移 XenApp 和 XenDesktop 版本或迁移早期 Citrix Virtual Apps and Desktops 版本的工具或脚本。Citrix 升级指南中列出的 Citrix Virtual Apps and Desktops 版本支持升级，本产品文档中对此进行了介绍。

有关早期的 XenApp 6.x 迁移内容，请参阅以下内容。脚本和文章都不受支持或维护。

- XenApp 6.x 版本的开源迁移脚本可从 https://github.com/citrix/xa65migrationtool 获取。Citrix 不支持或维护这些迁移脚本
- 7.x 中的变更
- 将 XenApp 6.5 工作进程升级到新 VDA
- 迁移 XenApp 6.x

升级部署

January 4, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

简介

您可以将某些部署升级为更高版本，而无需事先设置新计算机或站点。此过程称为原位升级。要了解可以升级的 Citrix Virtual Apps and Desktops 版本，请参阅《Citrix 升级指南》。

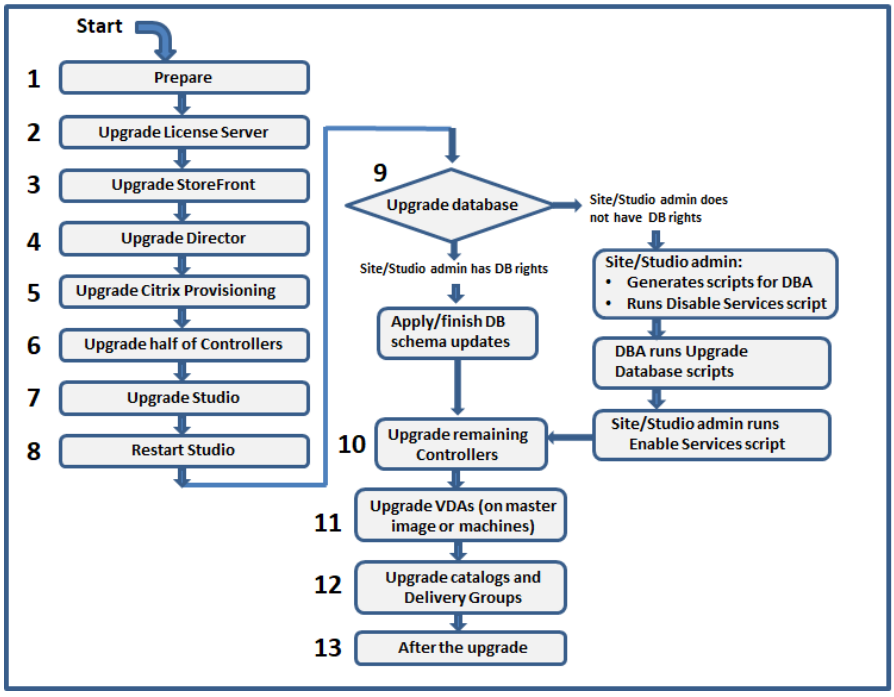
要开始升级，请从新版本运行安装程序以升级以前安装的核心组件、VDA 以及某些其他组件。然后升级数据库和站点。

如果提供了更新版本，则可以升级能够通过完整产品安装程序（和独立的 VDA 安装程序）安装的任何组件。有关不通过完整产品安装程序安装的其他组件（例如 Citrix Provisioning 和 Profile Management），请参阅该组件的文档以了解指导信息。对于主机升级，请参阅相应的文档。

请在开始升级之前查看本文中的所有信息。

升级顺序

下图显示了升级顺序的步骤。升级过程包含示意图中的每个步骤的详细信息。



> 注意：
>
> 为了避免出现故障，必须先升级所有 Delivery Controller 和数据库，然后再执行与预配和交付组相关的任何任务（例如，创建新计算机目录、删除计算机目录、更新交付组中的计算机等）。

升级过程

大多数主要产品组件可以通过在包含组件的计算机上运行产品安装程序来升级。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

如果一台计算机包含多个组件（例如，Studio 和许可证服务器），则该计算机上的所有组件都会升级（如果产品介质包含其软件的较新版本）。

要使用安装程序，请执行以下操作：

- 要运行完整产品安装程序的图形界面，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**。
- 要使用命令行界面，请发出恰当的命令。请参阅使用命令行安装。

步骤 **1**：准备

在开始升级之前，请确保您已准备就绪。阅读并完成任何必要的任务：

- 删除 PVD、应用程序磁盘和不受支持的主机
- 具有 PvD 或 AppDisk 组件的 VDA
- 限制
- 混合环境注意事项
- 早期版本的操作系统
- 准备
- 初步站点测试
- SQL Server 版本检查

步骤 **2**：升级许可证服务器

如果安装中包含 Citrix 许可证服务器软件的新版本，请先升级此组件，然后再升级任何其他组件。

如果您尚不确定许可证服务器是否与新版本兼容，则必须先在许可证服务器上运行安装程序，然后再升级任何其他核心组件。

步骤 **3**：升级 **StoreFront**

如果安装介质包含 StoreFront 软件的新版本，请在包含 StoreFront 服务器的计算机上运行安装程序。

- 在图形界面中，从扩展部署部分选择 **Citrix StoreFront**。
- 在命令行中运行 `CitrixStoreFront-x64.exe`，该命令在 Citrix Virtual Apps and Desktops 安装介质的 `x64` 文件夹中可用。

步骤 **4**：升级 **Director**

如果安装介质包含 Director 软件的新版本，请在包含 Director 的计算机上运行安装程序。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

步骤 **5**：升级 **Citrix Provisioning**

Citrix Provisioning 安装介质与 Citrix Virtual Apps and Desktops 安装介质分开使用。要了解如何安装和升级 Citrix Provisioning 服务器和目标设备软件，请参阅 Citrix Provisioning 产品文档。

步骤 **6**：升级一半 **Delivery Controller**

例如，如果您的站点包含四个 Controller，应在其中两个 Controller 上运行安装程序。

使另一半的 Controller 处于活动状态，以便用户能访问此站点。VDA 可以在其余 Controller 中进行注册。有时，站点容量可能会因可用 Controller 的减少而降低。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，则升级期间该站点将无法正常运行。

初步站点测试在实际升级开始之前在第一个 Controller 上运行。有关详细信息，请参阅初步站点测试。

步骤 **7**：升级 **Studio**

如果尚未升级 Studio（因为它与其他组件位于同一台计算机上），请在包含 Studio 的计算机上运行安装程序。

步骤 **8**：重新启动 **Studio**

重新启动升级的 Studio。升级过程将自动恢复。

步骤 **9**：升级数据库和站点

> 注意：
>
> 为了避免出现故障，必须先升级所有 Delivery Controller 和数据库，然后再执行与预配和交付组相关的任何任务（例如，创建新计算机目录、删除计算机目录、更新交付组中的计算机等）。

请查看准备，了解更新 SQL Server 数据库架构所需的权限。

- 如果您有足够的权限来更新 SQL Server 数据库架构，则可以启动自动数据库升级。继续自动升级数据库和站点。
- 如果您的数据库权限不足，则可以启动使用脚本的手动升级，然后在数据库管理员（拥有所需的权限的用户）的帮助下继续操作。对于手动升级，Studio 用户将生成脚本，然后运行启用和禁用服务的脚本。数据库管理员使用 SQLCMD 实用程序或 SQLCMD 模式下的 SQL Server Management Studio 运行用于更新数据库架构的其他脚本。继续手动升级数据库和站点。
- 如果您有多区域部署并希望自动升级数据库和站点，Citrix 建议应在托管站点的 SQL Server 数据库的同一区域中执行 dbschema 升级。否则，自动升级数据库和站点可能会失败。

Citrix 强烈建议您在升级之前备份数据库。请参阅 CTX135207。数据库升级期间，禁用产品服务。此时，Controller 无法为站点代理任何新连接，因此应认真规划。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

自动升级数据库和站点

1. 启动新升级的 Studio。
2. 指示您希望自动开始站点升级并确认您已准备就绪。

数据库和站点升级将继续进行。

手动升级数据库和站点

1. 启动新升级的 Studio。
2. 指示您要手动升级站点。向导将检查许可证服务器的兼容性并请求确认。
3. 确认您已备份数据库。

   向导会生成并显示脚本以及升级步骤核对表。如果自从升级产品版本后数据库的架构未发生变化，则不生成该脚本。例如，如果日志记录数据库架构未发生变化，则不生成 `UpgradeLoggingDatabase.sql` 脚本。
4. 按照所示顺序运行以下脚本。

   - `DisableServices.ps1`：Studio 用户在 Controller 上运行此 PowerShell 脚本以禁用产品服务。
   - `UpgradeSiteDatabase.sql`：数据库管理员在包含站点数据库的服务器上运行此 SQL 脚本。
   - `UpgradeMonitorDatabase.sql`：数据库管理员在包含 Monitor 数据库的服务器上运行此 SQL 脚本。
   - `UpgradeLoggingDatabase.sql`：数据库管理员在包含配置日志记录数据库的服务器上运行此 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`：Studio 用户在 Controller 上运行此 PowerShell 脚本以启用产品服务。

   数据库升级完成且产品服务启用之后，Studio 会自动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。
5. 完成核对表任务后，单击完成升级。

步骤 **10**：升级其余的 **Delivery Controller**

在新升级的 Studio 的导航窗格中选择 **Citrix Studio** 站点名称。在常规任务选项卡上，选择升级其余的 **Delivery Controller**。

完成升级并确认完成之后，关闭 Studio，然后再重新打开。Studio 可能会提示额外进行一次站点升级，以在站点中注册 Controller 的服务，或者创建区域 ID（如果不存在）。

步骤 **11**：升级 **VDA**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 重要：
>
> 如果要将 VDA 升级到版本 1912 或更高版本，请参阅将 VDA 升级到 1912 或更高版本。

在包含 VDA 的计算机上运行产品安装程序。

如果使用 Machine Creation Services 和主映像创建计算机，请转到您的主机并在主映像上升级 VDA。可以使用任何可用的 VDA 安装程序。

- 有关图形界面指南，请参阅安装 VDA。
- 有关命令行指导，请参阅使用命令行安装。

如果使用 Citrix Provisioning 创建计算机，请参阅 Citrix Provisioning 产品文档了解有关升级的指南。

观看此视频以了解更多：

步骤 **12**：更新计算机目录和交付组

- 更新使用安装了升级的 VDA 的计算机的目录。
- 升级使用安装了升级的 VDA 的计算机的目录。
- 升级使用安装了升级的 VDA 的计算机的交付组。

步骤 **13**：升级完成后

完成升级后，可以测试新升级的站点。在 Studio 的导航窗格中选择 **Citrix Studio** 站点名称。在常规任务选项卡上，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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

如果未启动 SQL Server Browser 服务，则当本地 Microsoft SQL Server Express 用于站点数据库时，对 Windows Server 2016 上的 Controller 执行测试可能会失败。为了避免这种情况，请执行以下操作：

- 启用 SQL Server Browser 服务（如有必要），然后启动该服务。
- 重新启动 SQL Server (SQLEXPRESS) 服务。

升级部署中的其他组件。有关指导，请参阅以下产品文档：

- StoreFront
- AppDNA
- Citrix App Layering
- HDX RealTime Optimization Pack
- Profile Management
- Citrix Provisioning
- Session Recording
- Workspace Environment Management

如果需要使用更高版本替换 Microsoft SQL Server Express LocalDB 软件，请参阅替换 SQL Server Express LocalDB。

删除 **PvD**、**AppDisk** 和不受支持的主机

Citrix Virtual Apps and Desktops 7 当前版本部署中不支持以下技术和主机类型：

- 个人虚拟磁盘 **(PvD)**，用于在目录中存储用户的 VM 旁边的数据。用户个性化层功能现在负责处理用户持久性。
- 用于管理交付组中使用的应用程序的 **AppDisk**。
- 主机类型：Azure Classic、Azure Resource Manager (ARM)、Amazon Web Services (AWS)、Cloud-Platform（原始 Citrix 产品）。
  - 有关此版本中支持的主机类型，请参阅系统要求。
  - 有关可继续使用 ARM 和 AWS 的其他方法的信息，请参阅 CTX270373。

如果您的当前部署使用 PvD 或 AppDisk，或者连接到不受支持的主机类型，则只有在删除使用这些技术的项目后，才能升级到版本 2006（或受支持的更高版本）。

当安装程序检测到一个或多个不受支持的技术或主机类型时，升级将暂停或停止，并显示一条解释性消息。安装程序日志包含详细信息。

为了帮助确保升级成功，请查看并遵循适用的指导以删除不受支持的项目。

- 删除 PvD
- 删除 AppDisk
- 删除不受支持的主机项目

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

即使您未在部署中使用 PvD 或 AppDisk，相关的 MSI 可能已包含在早期的 VDA 安装或升级中。在将 VDA 升级到版本 2006（或受支持的更高版本）之前，必须删除该软件，即使从未使用过该软件亦如此。使用图形界面时，可以为您完成删除操作，也可以在使用 CLI 时包含删除选项。有关详细信息，请参阅升级具有 PVD 或 AppDisk 组件的 VDA。

删除 **PvD**

除非删除配置为使用 PvD 的所有计算机，否则部署升级将无法成功。这会影响目录和交付组。

要从组和目录中删除 PvD，请执行以下操作：

1. 在 Studio 中，如果交付组包含使用 PvD 的目录中的计算机，请从组中删除这些计算机。
2. 在 Studio 中，删除所有目录，这些目录中包含使用 PvD 的计算机。

VDA 升级：部署升级不会检测 VDA 是否安装了 AppDisk 或 PvD 组件。但是，VDA 安装程序会进行检测。有关详细信息，请参阅具有 PvD 或 AppDisk 组件的 VDA。

如果您计划使用 App Layering 而非 PvD，请参阅将 PvD 迁移到 App Layering 以了解有关移动数据的信息。

删除 **AppDisk**

从使用 AppDisk 的所有交付组中删除这些 AppDisk，然后删除 AppDisk 本身之后，部署升级才能继续。

1. 在 Studio 导航窗格中选择交付组。
2. 选择一个组，然后在“操作”窗格中单击管理 **AppDisk**。
3. 单击用于从组中删除 AppDisk 的操作。
4. 对使用 AppDisk 的每个交付组重复执行步骤 2 和 3。
5. 在 Studio 导航窗格中选择 **AppDisk**。
6. 选择一个 AppDisk，然后单击用于删除该 AppDisk 的操作。
7. 对每个 AppDisk 重复执行步骤 5 和 6。

VDA 升级：部署升级不会检测 VDA 是否安装了 AppDisk 或 PvD 组件。但是，VDA 安装程序会进行检测。有关详细信息，请参阅具有 PvD 或 AppDisk 组件的 VDA。

删除不受支持的主机项目

如果站点与不受支持的主机类型（例如 Azure 或 AWS）建立了连接，则无法继续升级到版本 2006（或受支持的更高版本）。在尝试升级之前，请完成以下任务。

在 Studio 中：

- 删除与不受支持的主机的所有连接。
- 如果交付组包含通过不受支持的主机中的主映像创建的目录中的计算机，请从组中删除这些计算机。
- 删除所有目录，这些目录是使用不受支持的主机中的主映像创建的。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

具有 **PvD** 或 **AppDisk** 组件的 **VDA**

如果在 VDA 上安装了启用 PvD 和 AppDisk 技术的组件，删除这些组件之后才能升级该 VDA。

> 注意：
>
> 升级到版本 1912 时，您必须卸载当前 VDA，然后安装新 VDA。在本版本中，系统会询问您是否希望 Citrix 删除组件，然后继续升级。

AppDisk 和 PvD 组件可能已安装在早期 VDA 版本中，即使您从未使用过这些技术亦如此：

- 图形界面：在 VDA 安装程序中，其他组件页面包含 **Citrix AppDisk/Personal vDisk** 选项。默认情况下，7.15 LTSR 和更早的 7.x 版本启用了此选项。因此，如果您接受默认值（或在提供该选项的任何版本中明确启用了该选项），该组件已安装。
- CLI：指定 `/baseimage` 选项已安装的组件。

要执行的操作　如果 VDA 安装程序未检测到当前安装的 VDA 中的 AppDisk 或 PvD 组件，则会像往常一样进行升级。

如果安装程序在当前安装的 VDA 中检测到 AppDisk 或 PvD 组件：

- 图形界面：升级暂停。此时将显示一条消息，询问您是否希望自动删除不受支持的组件。如果单击确定，则会自动删除组件并继续进行升级。
- CLI：为避免命令失败，请在命令中包括以下选项：
  - `/remove_appdisk_ack`
  - `/remove_pvd_ack`

限制

升级存在以下限制：

- 选择性组件安装：如果在安装任何组件或将任何组件升级到新版本时不升级不同计算机上需要升级的其他组件，Studio 将会提醒您。例如，假设一个升级包括新版本的 Controller 和 Studio。您升级 Controller，但您未在安装了 Studio 的计算机上运行安装程序。在您升级 Studio 之前，Studio. 不允许您继续管理站点。

  您不必升级 VDA，但 Citrix 建议升级所有 VDA 以使您能够使用所有可用功能。
- 早期版本或技术预览版：不能从早期版本、技术预览版或预览版本进行升级。
- 早期版本的操作系统中的组件：不能在 Microsoft 或 Citrix 不再支持的操作系统上安装当前 VDA。有关详细信息，请参阅早期版本的操作系统统。
- 混合环境/站点：如果必须继续运行早期版本的站点和当前版本的站点，请参阅混合环境注意事项。
- 产品选择：从早期版本升级时，无需选择或指定在安装过程中设置的产品（Citrix Virtual Apps 或 Citrix Virtual Apps and Desktops）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

混合环境注意事项

升级时，Citrix 建议您升级所有组件和 VDA，以便能够访问您的版本中的所有新增功能和增强功能。

例如，尽管可以在含有早前版本 Controller 的部署中使用当前 VDA，但当前版本中的新增功能可能无法使用。使用非当前版本时，也可能会出现 VDA 注册问题。

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。（这称为功能级别。）默认情况下，此设置指定建议的最低 VDA 版本。对于大多数部署，默认值就足够了。仅当目录包含的 VDA 早于默认值时，才考虑将设置更改为早期版本。不建议在计算机目录中混合使用多个 VDA 版本。

如果目录是使用默认的最低 VDA 版本设置创建的，并且一台或多台计算机安装了默认版本之前的 VDA 版本，这些计算机将无法在 Controller 中注册，并且将无法使用。

有关详细信息，请参阅 VDA 版本和功能级别。

具有不同版本的多个站点

如果您的环境中包含的站点安装了不同的产品版本（例如 XenDesktop 7.18 站点和 Citrix Virtual Apps and Desktops 1909 站点），Citrix 建议使用 StoreFront 来汇总不同产品版本中的应用程序和桌面。有关详细信息，请参阅 StoreFront 文档。

在混合环境中，继续使用与每个发行版对应的 Studio 和 Director 版本，但要确保不同版本安装在单独的计算机上。

早期版本的操作系统

假设您在运行受支持的操作系统 (OS) 版本的计算机上安装了早期版本的组件。现在，您想要使用较新的组件版本，但该组件的当前版本不再支持该操作系统。

例如，假定您在 Windows Server 2008 R2 计算机上安装了服务器 VDA。现在您想要将该 VDA 升级到当前版本，但要升级到的当前版本不支持 Windows Server 2008 R2。

如果您尝试在不再允许使用的操作系统上安装或升级组件，则将显示一条错误消息，例如 “无法在此操作系统上安装”。

这些注意事项适用于升级当前版本和长期服务版本。（它不会影响将 CU 应用到 LTSR 版本。）

请单击以下链接了解支持的操作系统：

- Citrix Virtual Apps and Desktops（当前版本）：
  - Delivery Controller、Studio、Director、VDA、通用打印服务器
  - 联合身份验证服务
  - 对于 StoreFront、自助服务密码重置和 Session Recording，请参阅当前版本的系统要求一文。
- 对于 LTSR，请参阅您的 LTSR 版本和 CU 的组件列表。（请从主 Citrix Virtual Apps and Desktops 产品文档页面中选择您的 LTSR 版本。）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

无效的操作系统

下表列出了不适用于安装/升级当前版本中的组件的早期版本的操作系统。下表指出了列出的每个操作系统支持的最新的有效组件版本，以及安装和升级变得无效的组件版本。

下表中的操作系统包括 Service Pack 和更新。

操作系统	组件/功能	最新的有效版本	不能安装/升级的截至版本
Windows 7 和 Windows 8	VDA	7.15 LTSR	7.16
Windows 7 和 Windows 8	其他安装程序组件	7.17	7.18
1607 之前的 Windows 10 版本	VDA	7.15 LTSR	7.16
Windows 10 x86 版本	VDA	1906.2.0	1909
Windows Server 2008 R2	VDA	7.15 LTSR	7.16
Windows Server 2008 R2	其他安装程序组件	7.17	7.18
Windows Server 2012	VDA	7.15 LTSR	7.16
Windows Server 2012	其他安装程序组件	7.17	7.18
Windows Server 2012 R2	其他安装程序组件 *	1912 LTSR	2003
Windows Server 2012 R2	服务器 VDI	7.15 LTSR	7.16

Windows XP 和 Windows Vista 不适用于任何 7.x 组件或技术。

* 适用于 Delivery Controller、Studio、Director 和 VDA。

可以执行的操作

可以选择的对象。您可以：

- 继续使用当前的操作系统
- 重新创建映像或升级计算机
- 添加新计算机，然后删除旧计算机

继续使用当前的操作系统　这些方法对 VDA 而言是可行的方法。如果您希望继续使用安装了早期版本的操作系统的计算机，可以选择以下选项之一：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 继续使用已安装的组件版本。
- 下载最新的有效组件版本，然后将该组件升级到该版本。（这假设尚未安装最新的有效组件版本。）

例如，您在 Windows 7 SP1 计算机上安装了 7.14 版本的 VDA。Windows 7 操作系统计算机上最新的有效 VDA 版本为 XenApp 和 XenDesktop 7.15 LTSR。可以继续使用 7.14 或下载 7.15 LTSR VDA，然后将您的 VDA 升级到该版本。这些早期版本的 VDA 在包含较新版本的 Delivery Controller 的部署中运行。例如，7.15 LTSR VDA 可以连接到 Citrix Virtual Apps and Desktops 7 1808 Controller。

重新创建映像或升级计算机　这些方法对 VDA 以及其他未安装核心组件（例如 Delivery Controller）的计算机而言是可行的方法。选择以下方法之一：

- 使计算机停止服务（打开维护模式并允许所有会话关闭）后，可以重新创建其映像至受支持的 Windows 操作系统版本，然后安装最新版本的组件。
- 要升级操作系统而不重新创建映像，请先升级操作系统，然后再卸载 Citrix 软件。否则，Citrix 软件将处于不受支持的状态。然后，安装新组件。

添加新计算机，然后删除旧计算机　如果必须升级包含 Delivery Controller 或其他核心组件的计算机上的操作系统，此方法可行。

Citrix 建议站点中的所有 Controller 都具有相同的操作系统。不同的 Controller 的操作系统不同时，以下升级顺序可将时间间隔降至最低。

1. 创建站点中的所有 Delivery Controller 的快照，然后备份站点数据库。
2. 在操作系统受支持的干净服务器上安装新 Delivery Controller。例如，在两台 Windows Server 2016 计算机上安装一个 Controller。
3. 将新 Controller 添加到站点中。
4. 删除对当前版本无效的操作系统中运行的 Controller。例如，删除两台 Windows Server 2008 R2 计算机中的两个 Controller。请按照 Delivery Controller 中有关删除 Controller 的建议进行操作。

准备

开始升级之前，请查看以下信息并完成必要的任务。

> 注意：
>
> 尽管升级 VDA 以后会按照升级顺序进行，最好在开始升级之前选择安装程序并查看该过程，这样您即可知晓预期效果。

选择安装程序和界面

使用产品 ISO 中的完整产品安装程序升级组件。可以使用完整产品安装程序或其中一个独立的 VDA 安装程序来升级 VDA。所有的安装程序都提供图形界面和命令行接口。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

有关详细信息，请参阅安装程序。

安装详情：完成任何准备工作并准备好启动安装程序后，安装一文会显示您将看到的内容（如果使用图形界面）或键入的内容（如果使用命令行接口）。

- 使用图形界面安装/升级核心组件
- 使用命令行安装/升级核心组件
- 使用图形界面安装/升级 VDA
- 使用命令行安装/升级 VDA

如果您最初是使用 `VDAWorkstationCoreSetup.exe` 安装程序安装单会话 VDA，Citrix 建议使用该安装程序对其进行升级。如果使用完整产品 VDA 安装程序或 `VDAWorkstationSetup.exe` 安装程序升级 VDA，可能会安装最初排除的组件，除非在升级中明确将其忽略/排除。

将 VDA 升级到当前版本时，计算机在升级过程中将重新启动。（此要求是 7.17 及更高版本的要求）。此要求不能避免。升级在重新启动后自动继续进行（除非您在命令行中指定了 `/noresume`）。

数据库操作

备份站点数据库、监视数据库和配置日志记录数据库。按照 CTX135207 中的说明进行操作。如果在升级后发现任何问题，可以还原备份。

有关升级不再受支持的 SQL Server 版本的信息，请参阅 SQL Server 版本检查。（这是指用于站点、监视和配置日志记录数据库的 SQL Server。）

Microsoft SQL Server Express LocalDB 会自动安装，以便与本地主机缓存一起使用。如果需要替换早期版本，新版本必须为 SQL Server Express 2017 LocalDB CU16。有关升级组件和站点后使用新版本替换 SQL Server Express LocalDB 的详细信息，请参阅替换 SQL Server Express LocalDB。

确保您的 **Citrix Licensing** 是最新的

有关管理 Citrix Licensing 的综合性概述，请参阅激活、升级和管理 Citrix 许可证。

可以使用完整产品安装程序升级许可证服务器。或者，也可以单独下载和升级许可组件。请参阅升级。

在升级之前，请确保您的 Customer Success Services/软件维护/专享升级服务日期对新产品版本有效。日期必须至少为 2021.05.15。

确保您的 **Citrix** 许可证服务器兼容

确保 Citrix 许可证服务器与新版本兼容。有两种方式实现此要求：

- 在升级任何其他 Citrix 组件之前，请从包含 Delivery Controller 的计算机上的 ISO 布局中运行 `XenDesktopServerSetup.exe` 安装程序。如果存在任何不兼容问题，安装程序会报告该问题并提供解决问题的建议步骤。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 在安装介质上的 XenDesktop Setup 目录中，运行以下命令：.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v。显示内容指示许可证服务器是否兼容。如果许可证服务器不兼容，请升级许可证服务器。

备份所有 **StoreFront** 修改

开始升级之前，如果您对 C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data 中的文件（例如，*default.ica* 和 *usernamepassword.tfrm*）进行了修改，请为每个应用商店备份这些文件。升级后，您可以还原它们以恢复进行的修改。

关闭应用程序和控制台

在开始升级之前，请关闭可能会导致文件锁定的所有程序，其中包括管理控制台和 PowerShell 会话。

重新启动计算机可确保清除任何文件锁定，以及不存在任何未完成的 Windows 更新。

在开始升级之前，请停止并禁用所有第三方监视代理服务。

确保您有合适的权限

除了是域用户以外，您还必须是要升级产品组件的计算机上的本地管理员。

可以自动或手动升级站点数据库和站点。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。

如果 Studio 用户没有这些权限，启动手动数据库升级将生成脚本。Studio 用户从 Studio 运行其中一些脚本。数据库管理员使用 SQL Server Management Studio 等工具运行其他 SQL 脚本。

其他准备任务

- 备份模板并升级虚拟机管理程序（如果需要）
- 完成您的业务连续性计划规定的任何其他准备任务。

初步站点测试

升级 Delivery Controller 和站点时，初步站点测试在实际升级开始之前运行。这些测试将验证：

- 站点数据库可以访问并且已备份
- 与基本 Citrix 服务的连接正常运行
- Citrix 许可证服务器地址可用
- 可以访问配置日志记录数据库

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

测试运行后，可以查看结果报告。然后，可以修复检测到的任何问题并重新运行测试。运行初步站点测试失败，然后解决任何问题都会影响您的站点的运行方式。

包含测试结果的报告是一个与安装日志位于同一目录中的 HTML 文件 (`PreliminarySiteTestResult.html`)。如果该文件不存在，则将创建。如果该文件存在，则会覆盖其内容。

运行测试

- 使用安装程序的图形界面进行升级时，向导将包含一个页面，您可以在该页面中开始测试并显示报告。测试运行并且您已查看报告并解决找到的任何问题后，可以重新运行测试。测试成功完成时，请单击“下一步”以继续执行向导。
- 使用命令行界面进行升级时，测试将自动运行。默认情况下，如果测试失败，将不执行升级。查看报告并解决问题后，请重新运行命令。

Citrix 建议您始终先运行初步站点测试，然后解决所有问题，再继续升级 Controller 和站点。潜在的优势非常值得花费片刻时间来运行测试。但是，您可以忽略这一建议的操作。

- 使用图形界面升级时，可以选择跳过测试并继续升级。
- 从命令行升级时，不能跳过测试。默认情况下，失败的站点测试会导致安装程序失败，而不执行升级。在大多数情况下，如果包括 `/ignore_site_test_failure` 选项，任何测试失败都将被忽略，升级继续进行。（有关例外情况，请参阅 SQL Server 版本检查 。）

升级多个 **Controller** 时

开始在一个 Controller 上升级，然后开始在同一个站点中的另一个 Controller 上升级（在第一个升级完成之前）时：

- 如果已在第一个 Controller 上完成初步站点测试，初步站点测试页面将不在另一个 Controller 上的向导中显示。
- 如果当您在另一个 Controller 上开始升级时第一个 Controller 上的测试正在进行，站点测试页面将在另一个 Controller 上的向导中显示。但是，如果第一个 Controller 上的测试完成，则将仅保留来自第一个 Controller 的测试结果。

与站点的运行状况无关的测试失败问题

- 如果初步站点测试由于内存不足失败，请提供更多可用内存，然后重新运行测试。
- 如果您有升级权限，但未运行站点测试，初步站点测试将失败。要解决此问题，请使用有权运行测试的用户帐户重新运行安装程序。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SQL Server 版本检查

成功的 Citrix Virtual Apps and Desktops 部署需要对站点、监视器和配置日志记录数据库使用受支持的 Microsoft SQL Server 版本。使用不再受支持的 SQL Server 版本升级 Citrix 部署可能会导致出现功能问题，并且站点将不受支持。

要了解要升级到的 Citrix 版本支持哪些 SQL Server 版本，请参阅该版本的系统要求一文。

升级 Controller 时，Citrix 安装程序会检查用于站点、监视器和配置日志记录数据库的当前已安装的 SQL Server 版本。

- 如果检查确定当前安装的 SQL Server 版本不是要升级到的 Citrix 版本中受支持的版本：
  - 图形界面：升级将停止并显示消息。单击我理解，然后单击取消以关闭 Citrix 安装程序。（您无法继续升级。）
  - 命令行界面：命令失败（即使您在命令中包含 `/ignore_db_check_failure` 选项亦如此）。

  升级 SQL Server 版本，然后重新启动 Citrix 升级。
- 如果检查无法确定当前安装的 SQL Server 版本，请查看要升级到的版本中是否支持当前安装的版本（系统要求）。
  - 图形界面：升级将停止并显示消息。
    - 如果支持当前安装的 SQL Server 版本，请单击我理解以关闭该消息，然后单击下一步继续进行 Citrix 升级。
    - 如果不支持当前安装的 SQL Server 版本，请单击我理解以关闭该消息，然后单击取消以结束 Citrix 升级。将 SQL Server 升级到受支持的版本，然后重新启动 Citrix 升级。
  - 命令行界面：命令失败并显示消息。关闭消息后：
    - 如果支持当前安装的 SQL Server 版本，请使用 `/ignore_db_check_failure` 选项重新运行该命令。
    - 如果不支持当前安装的 SQL Server 版本，请将 SQL Server 升级到受支持的版本。重新运行该命令以启动 Citrix 升级。

升级 SQL Server

如果调出新 SQL Server 服务器并迁移站点数据库，则必须更新连接字符串。

如果站点当前为站点数据库使用 SQL Server Express（Citrix 在站点创建过程中自动安装）：

1. 安装最新的 SQL Server Express 版本。
2. 分离数据库。
3. 将数据库附加到新的 SQL Server Express。
4. 迁移连接字符串。

有关详细信息，请参阅配置连接字符串和 Microsoft SQL Server 产品文档。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

替换 SQL Server Express LocalDB

Microsoft SQL Server Express LocalDB 是本地主机缓存独立使用的 SQL Server Express 功能。本地主机缓存不需要除 SQL Server Express LocalDB 以外的 SQL Server Express 的任何组件。

如果您安装了早于 1912 的 Delivery Controller 版本，然后将部署升级到版本 1912 或更高版本，Citrix 不会自动升级 SQL Server Express LocalDB 版本。为什么不？因为您可能具有依赖于 SQL Server Express LocalDB 数据库的非 Citrix 组件。如果您有非 Citrix 组件正在使用 SQL Server Express LocalDB，请确保升级 SQL Server Express LocalDB 不会中断这些组件。要升级（替换）SQL Server Express LocalDB 版本，请按照本部分中的指导进行操作。

- 将 **Delivery Controller** 升级到 **Citrix Virtual Apps and Desktops** 版本 **1912** 或 **2003** 时：升级 SQL Server Express LocalDB 是可选的。本地主机缓存正常运行，不会丢失功能，而无论您是否升级 SQL Server Express LocalDB。我们添加了在对结束支持有疑虑的情况下，从 Microsoft for SQL Server Express LocalDB 2014 移动到更新版本的 SQL Server Express LocalDB 的选项。
- 将 **Delivery Controller** 升级到高于 **2003** 的 **Citrix Virtual Apps and Desktops** 版本时：支持的版本为 SQL Server Express 2017 LocalDB 累积更新 (CU) 16。如果您最初安装了版本 1912 之前的 Delivery Controller，并且自此之后没有用较新版本替换 SQL Server Express LocalDB，则必须立即替换该数据库软件。否则，本地主机缓存将无法正常运行。

您需要什么：

- Citrix Virtual Apps and Desktops 安装介质（针对已升级到的版本）。介质包含 Microsoft SQL Server Express LocalDB 2017 CU 16 的副本。
- 您从 Microsoft 下载的 Windows Sysinternals 工具。

过程：

1. 完成 Citrix Virtual Apps and Desktops 组件、数据库和站点的升级。（这些数据库升级会影响站点、监视和配置日志记录数据库。它们不会影响使用 SQL Server Express LocalDB 的本地主机缓存数据库。）
2. 在 Delivery Controller 上，从 Microsoft 下载 `PsExec`。请参阅 Microsoft 文档 PsExec v2.2。
3. 停止 Citrix High Availability Service。
4. 在命令提示符中，运行 `PsExec` 并切换到网络服务帐户。

   ```
   psexec -i -u "NT AUTHORITY\NETWORK SERVICE"cmd
   ```

   或者，可以使用 `whoami` 确认命令提示符正在以网络服务帐户身份运行。

   ```
   whoami
   nt authority\network service
   ```

5. 移动到包含 SqlLocalDB 的文件夹。

   ```
   cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
   ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. 停止和删除 `CitrixHA` (LocalDB)。

   ```
   SqlLocalDB stop CitrixHA

   SqlLocalDB delete CitrixHA
   ```

7. 删除 `C:\Windows\ServiceProfiles\NetworkService` 中的相关文件。

   ```
   1 HADatabaseName.*
   2 HADatabaseName_log.*
   3 HAImportDatabaseName.*
   4 HAImportDatabaseName_log.*
   5 <!--NeedCopy-->
   ```

   提示：您的部署可能没有 `HAImportDatabaseName.*` 和 `HAImportDatabaseName_log.*`

8. 使用用于删除程序的 Windows 功能从服务器中卸载 SQL Server Express LocalDB 2014。
9. 安装 SQL Server Express LocalDB 2017 CU 16。在 Citrix Virtual Apps and Desktops 安装介质上的 `Support > SQLLocalDB` 文件夹中，双击 `sqllocaldb.msi`。可能会请求重新启动以完成安装。（新的 SQLLocalDB 位于 `C:\Program Files\Microsoft SQL Server\140\Tools\Binn` 中。）
10. 启动 Citrix High Availability Service。
11. 确保在每个 Delivery Controller 上创建本地主机缓存数据库。这确认了如果需要，高可用性服务（辅助 Broker）可以接管。
    - 在 Controller 服务器上，浏览到 `C:\Windows\ServiceProfiles\NetworkService`。
    - 验证 `HaDatabaseName.mdf` 和 `HaDatabaseName_log.ldf` 是否已创建。

安全

November 17, 2021

Citrix Virtual Apps and Desktops 提供设计安全的解决方案，允许您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，Citrix Virtual Apps and Desktops 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。

Citrix Virtual Apps and Desktops 数据中心还提供集中式监视和管理服务，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。

Citrix Virtual Apps and Desktops 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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

通过委派管理员功能，您可以设置管理员角色，以在某个粒度级别控制对 Citrix Virtual Apps and Desktops 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。

Citrix Virtual Apps and Desktops 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 或在最终用户与 Virtual Delivery Agent (VDA) 之间使用传输层安全性 (TLS) 协议来增加 Citrix Virtual Apps 或 Citrix Virtual Desktops 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。

Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps and Desktops 交付的所有资源。这些方法包括：

- 令牌
- 智能卡
- RADIUS
- Kerberos
- 生物识别

Citrix Virtual Desktops 可以与从身份管理到防病毒软件等的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 Citrix Virtual Apps and Desktops 版本。有关这些标准的列表，请转至 https://www.commoncriteriaportal.org/cc/。

安全注意事项和最佳做法

January 20, 2023

> 注意：
>
> 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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

考虑使用特定于平台的反恶意软件。

安装软件时，请安装到提供的默认路径。

- 如果您将软件安装到所提供的默认路径以外的文件位置，请考虑向您的文件位置添加其他安全措施，例如受限权限。

所有网络通信都应该根据您的安全策略进行适当的保护和加密。您可以使用 IPSec 保护 Microsoft Windows 计算机之间的所有通信；有关如何执行此任务的详细信息，请参阅您的操作系统文档。此外，通过 Citrix SecureICA（默认情况下已配置为 128 位加密）保护用户设备和桌面之间的通信。可以在创建或更新交付组时配置 SecureICA。

> 注意：
>
> Citrix SecureICA 是 ICA/HDX 协议的一部分，但它不是像传输层安全性 (TLS) 这样符合标准的网络安全协议。还可以使用 TLS 保护用户设备与桌面之间的网络通信。要配置 TLS，请参阅传输层安全性 (TLS)。

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。

防火墙

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）。

环境中的所有计算机均应使用个人防火墙进行保护。在安装核心组件和 VDA 时，如果检测到 Windows 防火墙服务（即使未启用防火墙），可以选择自动打开组件和功能通信所需的端口。您还可以选择手动配置这些防火墙端口。如果您使用其他防火墙，则必须手动对其进行配置。

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。

> 注意：
>
> TCP 端口 1494 和端口 2598 已用于 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 编号分配机构 (http://www.iana.org/) 正式注册的端口。

应用程序安全性

为防止非管理员用户执行恶意操作，我们建议您为 VDA 主机和本地 Windows 客户端上的安装程序、应用程序、可执行文件和脚本配置 Windows AppLocker 规则。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。有关如何允许用户在使用桌面时查看自己的本地时间的信息，请参阅“管理交付组”一文。
- 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

用户帐户和计算机帐户均需要登录权限。如果授予 Microsoft Windows 权限，登录权限将继续通过常规方法应用于桌面：通过“用户权限分配”配置登录权限，通过“组策略”对成员身份进行分组。

Windows 登录权限包括：本地登录、通过远程桌面服务登录、通过网络登录（从网络中访问此计算机）、作为批处理作业登录以及作为服务登录。

对于计算机帐户，仅授予计算机所需要的登录权限。需要“从网络中访问此计算机”登录权限：

- 在 VDA 上，针对 Delivery Controller 的计算机帐户
- 在 Delivery Controller 上，针对 VDA 的计算机帐户。请参阅基于 Active Directory OU 的控制器发现。
- 在 StoreFront 服务器上，针对位于相同 StoreFront 服务器组的其他服务器的计算机帐户

对于用户帐户，请仅授予用户所需的登录权限。

根据 Microsoft 的规定，默认情况下，“远程桌面用户”组被授予登录权限“允许通过远程桌面服务登录”（在域控制器上除外）。

贵组织的安全策略可能会明确声明应将此组从该登录权限中删除。请考虑使用以下方法：

- 适用于多会话操作系统的 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 Citrix Virtual Apps and Desktops 的其他组件（包括适用于单会话操作系统的 VDA），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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - 如果不通过远程桌面服务管理这些计算机，请考虑在这些计算机上禁用远程桌面服务本身。

虽然可以向登录权限“拒绝通过远程桌面服务登录”中添加用户和组，但通常不建议使用拒绝登录权限。有关详细信息，请参阅 Microsoft 文档。

配置用户权限

Delivery Controller 安装会创建以下 Windows 服务：

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService)：管理虚拟机的 Microsoft Active Directory 计算机帐户。
- Citrix Analytics (NT SERVICE\CitrixAnalytics)：收集由 Citrix 使用的站点配置使用情况信息（如果站点管理员已批准执行此收集）。随后会将此信息提交给 Citrix，以帮助改进产品。
- Citrix App Library (NT SERVICE\CitrixAppLibrary)：支持对 AppDisk、AppDNA 集成进行管理和预配，支持对 App-V 进行管理。
- Citrix Broker Service (NT SERVICE\CitrixBrokerService)：选择对用户可用的虚拟桌面或应用程序。
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging)：记录由管理员对站点执行的所有配置更改和其他状态更改。
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService)：用于共享的配置的站点范围的存储库。
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin)：管理向管理员授予的权限。
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest)：管理其他 Delivery Controller 服务的自检。
- Citrix Host Service (NT SERVICE\CitrixHostService)：存储关于在 Citrix Virtual Apps 或 Citrix Virtual Desktops 部署中使用的虚拟机管理程序基础结构的信息，并提供由控制台用于枚举虚拟机管理程序池中资源的功能。
- Citrix Machine Creation Service (NT SERVICE\CitrixMachineCreationService)：调配桌面虚拟机的创建过程。
- Citrix Monitor Service (NT SERVICE\CitrixMonitor)：收集 Citrix Virtual Apps 或 Citrix Virtual Desktops 的指标、存储历史记录信息，并提供查询界面以用于故障排除和报告工具。
- Citrix Storefront Service (NT SERVICE\ CitrixStorefront)：支持对 StoreFront 进行管理。（它不包含在 StoreFront 组件自身中。）
- Citrix Storefront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService)：支持 StoreFront 的特权管理操作。（它不包含在 StoreFront 组件自身中。）
- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService)：将主站点数据库中的配置数据传播到本地主机缓存。
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService)：在主站点数据库不可用时，选择用户可用的虚拟桌面或应用程序。

Delivery Controller 安装还会创建以下 Windows 服务。随其他 Citrix 组件安装时也会创建这些服务：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc)：支持收集由 Citrix 使用的诊断信息。
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService)：收集由 Citrix 用于执行分析的诊断信息，以使管理员可查看分析结果和建议信息，从而帮助诊断站点中的问题。

Delivery Controller 安装还会创建以下 Windows 服务。这在当前未使用。如果它已启用，请将其禁用。

- Citrix Remote Broker Provider (NT SERVICE\XaXdCloudProxy)

Delivery Controller 安装还会创建以下 Windows 服务。这些在当前未使用，但必须启用。请勿禁用它们。

- Citrix Orchestration Service (NT SERVICE\CitrixOrchestration)
- Citrix Trust Service (NT SERVICE\CitrixTrust)

除 Citrix Storefront Privileged Administration Service 外，这些服务均被授予登录权限“作为服务登录”，以及权限“为进程调整内存配额”、“生成安全审核”和“替换一个进程级令牌”。您不需要更改这些用户权限。这些权限将不由 Delivery Controller 使用，并且已自动禁止。

配置服务设置

除 Citrix Storefront Privileged Administration Service 和 Citrix Telemetry Service 外，在前面的配置用户权限部分中列出的 Delivery Controller Windows 服务被配置为以“网络服务”身份登录。请不要更改这些服务设置。

Citrix Storefront Privileged Administration Service 被配置为登录本地系统 (NT AUTHORITY\SYSTEM)。这是通常无法对服务执行的 Delivery Controller StoreFront 操作所必需的（包括创建 Microsoft IIS 站点）。请勿更改其服务设置。

Citrix Telemetry Service 被配置为以其自己的服务特定身份登录。

可以禁用 Citrix Telemetry Service。除此服务和已禁用的服务外，不要禁用这些 Delivery Controller Windows 服务中的任何其他服务。

配置注册表设置

不再需要在 VDA 文件系统中启用 8.3 文件名和文件夹的创建。可以配置注册表项 **NtfsDisable8dot3NameCreation** 以禁用 8.3 文件名和文件夹的创建。还可以使用 **fsutil.exe behavior set disable8dot3** 命令配置此功能。

部署方案安全含义

您的用户环境可以包含以下两种用户设备之一：不受您的组织管理而完全由用户控制的用户设备；由您的组织管理的用户设备。通常，这两种环境的安全注意事项不同。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。用户将数据存储在桌面上这种做法并不好；数据应该放在文件服务器、数据库服务器，或者可以适当受保护的其他存储库中。

您的桌面环境可能包含各种类型的桌面，例如池桌面和专用桌面。用户不应该将数据存储在用户之间共享的桌面（例如池桌面）上。如果用户将数据存储在专用桌面上，则以后其他用户使用该桌面时应该删除这些数据。

混合版本环境

在一些升级过程中，不可避免地会出现混合版本环境。请遵循最佳做法，尽可能缩短不同版本的 Citrix 组件共同存在的时间。例如，在混合版本环境中，安全策略可能不会统一实施。

> 注意：
>
> 这是其他软件产品的典型特征；使用早期版本的 Active Directory 只能部分向更高版本的 Windows 实施组策略。

以下场景描述了在特定混合版本的 Citrix 环境中会发生的安全问题。使用 Citrix Receiver 1.7 连接到运行 XenApp 和 XenDesktop 7.6 Feature Pack 2 中的 VDA 的虚拟桌面时，在站点中启用了允许在桌面与客户端之间传输文件策略设置，但是无法通过运行 XenApp 和 XenDesktop 7.1 的 Delivery Controller 禁用此策略设置。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和下载文件，这是一个安全问题。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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。

> 小心：
>
> 注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

限制向单个用户执行自动分配：

在站点中的每个 Controller 中，设置以下注册表项：

```
HKEY\_LOCAL\_MACHINE\Software\Citrix|DesktopServer
Name: AllowMultipleRemotePCAssignments
Type: REG_DWORD
Data: 0 = Disable multiple user assignment, 1 = (Default) Enable
    multiple user assignment.
```

如果存在任何现有用户分配，请使用 SDK 命令将其删除，以便接下来 VDA 可以执行单个自动分配。

- 从 VDA 中删除所有已分配的用户：`$machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine`
- 从交付组中删除 VDA：`$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup`

重新启动办公室物理 PC。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

XML 信任

XML 信任设置适用于使用以下对象的部署：

- 本地 StoreFront。
- 不需要密码的订阅者（用户）身份验证技术。此类技术的示例包括域直通、智能卡、SAML 和 Veridium 解决方案。

启用 XML 信任设置允许用户成功进行身份验证，然后启动应用程序。Delivery Controller 信任从 StoreFront 发送的凭据。仅当您已保护 Delivery Controller 与 StoreFront 之间的通信（使用防火墙、IPsec 或其他安全建议）时，才启用此设置。

默认情况下，禁用此设置。

使用 Citrix Virtual Apps and Desktops PowerShell SDK 检查、启用或禁用 XML 信任设置。

- 要检查 XML 信任设置的当前值，请运行 `Get-BrokerSite` 并检查 `TrustRequestsSentToTheXMLServiceP` 的值。
- 要启用 XML 信任，请运行 `Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true`。
- 要禁用 XML 信任，请运行 `Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $false`。

将 Citrix Virtual Apps and Desktops 与 Citrix Gateway 集成

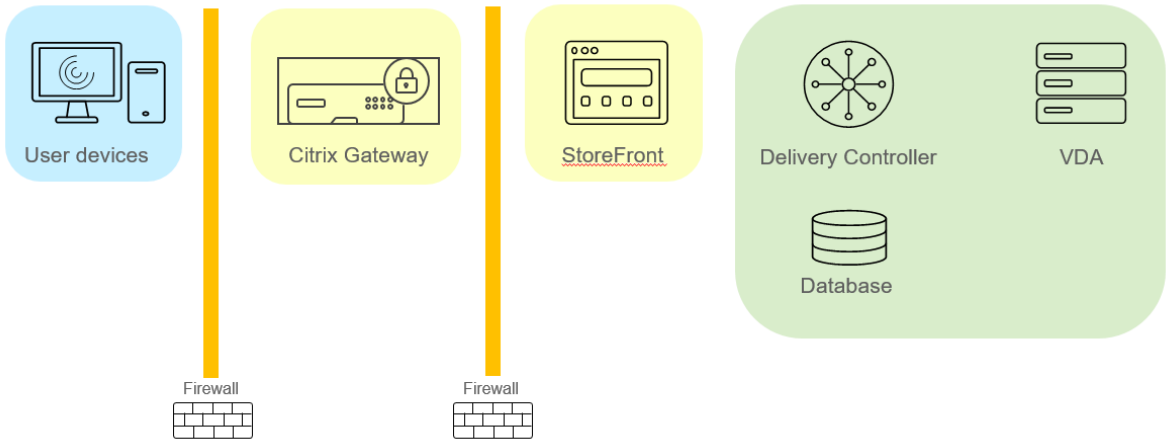
January 21, 2022

要管理对已发布资源和数据的访问，可以部署和配置 StoreFront 服务器。为了进行远程访问，建议在 StoreFront 前面添加 Citrix Gateway。

> 注意：
>
> 有关如何将 Citrix Virtual Apps and Desktops 与 Citrix Gateway 集成的详细配置步骤，请参阅 StoreFront 文档。

下图显示了包括 Citrix Gateway 的简化 Citrix 部署示例。Citrix Gateway 与 StoreFront 通信来保护 Citrix Virtual Apps and Desktops 提供的应用程序和数据。用户设备运行 Citrix Workspace 应用程序来创建安全连接以及访问其应用程序、桌面和文件。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



用户使用 Citrix Gateway 登录并进行身份验证。Citrix Gateway 部署在 DMZ 中并受到保护。配置了双重身份验证。用户会根据用户凭据获得相关的资源和应用程序。应用程序和数据位于相应的服务器上（图中未显示）。安全性敏感应用程序和数据使用单独的服务器。

委派管理

November 17, 2021

“委派管理”模型可以使用角色和基于对象的控制机制灵活地与组织所需的管理活动委派方式相匹配。委派管理可以适应所有规模的部署，并且随着部署复杂性的增加，可以帮助您更细化地配置权限。委派管理基于三个概念：管理员、角色和作用域。

- 管理员：管理员是指由 Active Directory 帐户所标识的一个或一组人。每个管理员均与一个或多个角色和作用域对相关联。
- 角色：角色代表一项工作职能，并且具有定义的关联权限。例如，“交付组管理员”角色具有“创建交付组”和“从交付组中删除桌面”等权限。管理员在一个站点中可以具有多个角色，因此一个人既可以是交付组管理员，又可以是计算机目录管理员。角色可以内置或自定义。

  内置角色包括：

角色	权限
完全权限管理员	可以执行所有任务和操作。完全权限管理员始终与“全部”作用域结合。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

角色	权限
只读权限管理员	可以查看指定作用域内的所有对象及全局信息，但不能更改任何内容。例如，作用域为“伦敦”的只读权限管理员可以查看所有全局对象（例如配置日志记录）和所有伦敦作用域内的对象（例如，伦敦交付组）。但是，该管理员无法查看“纽约”作用域（假设“纽约”作用域和“伦敦”作用域无重叠）中的对象。
技术支持管理员	可以查看交付组，并管理与之关联的会话和计算机。可以查看正在监视的交付组的计算机目录和主机信息。还可以对这些交付组中的计算机执行会话管理和计算机电源管理操作。
计算机目录管理员	可以创建并管理计算机目录，并将计算机预配到这些目录中。可以从虚拟化基础结构、Provisioning Services 和物理机构建计算机目录。此角色可以管理基础映像并安装软件，但不可以向用户分配应用程序或桌面。
交付组管理员	可以交付应用程序、桌面和计算机，还可管理关联的会话。以及应用程序和桌面配置，如策略和电源管理设置。
主机管理员	可以管理主机连接及其关联的资源设置。可以向用户交付计算机、应用程序或桌面。

在某些产品版本中，您可以根据组织的要求创建自定义角色，并可以更细致地委派权限。您可以使用自定义角色按照控制台中操作或任务的粒度来分配权限。

- 作用域：一个作用域代表一个对象集合。作用域用来根据组织的具体情况将对象分组（例如，销售团队使用的交付组集合）。对象可以属于多个作用域；可以将对象视为带有多个作用域的标记。系统提供一个内置的作用域“全部”，其包含全部对象。“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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

管理员	角色	作用域
domain/heidi	只读权限管理员、技术支持管理员	所有销售
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。
- warehouseadmin 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。此外，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”作用域，此作用域无法更改。

默认情况下启用管理员。如果现在要创建管理员，但此人要在之后某个时间才开始履行管理员职责，则禁用管理员可能很有必要。对于已启用的现有管理员，重新组织对象/作用域时，您可能需要禁用多个管理员，当准备启用更新配置时，

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。不会删除角色或作用域。也不会影响配置了该角色/作用域对的任何其他管理员。

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。

- 创建管理员：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，启用新管理员；可以对此进行更改。
- 复制管理员：在中间窗格中选择管理员，然后在“操作”窗格中单击复制管理员。键入或浏览到用户帐户名称。可以选择任何角色/作用域对，然后进行编辑或删除，也可以添加新的角色/作用域对。默认情况下，启用新管理员；可以对此进行更改。
- 编辑管理员：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。
- 删除管理员：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。

上部窗格显示您创建的管理员。选择管理员以在下部窗格中查看其详细信息。警告列指示与管理员关联的角色和作用域对是否包含不可用的角色或作用域。如果关联的角色和作用域对包含不可用的角色或作用域，将显示以下警告消息：

- 关联的角色或作用域不可用
  - 删除与管理员关联的角色和作用域对。

> 重要：
>
> 仅当关联的角色和作用域对包含不可用的角色或作用域或两者时，才会显示警告消息。

要删除与管理员关联的角色和作用域对，请完成以下步骤之一：

- 删除角色和作用域对。
  1. 在操作窗格中，单击编辑管理员。
  2. 在编辑管理员窗口中，选择角色和作用域对，然后单击删除。
  3. 单击确定以退出。
- 删除管理员。
  1. 在操作窗格中，单击删除管理员。
  2. 在 **Studio** 窗口中，单击删除。

创建和管理角色

管理员创建或编辑角色时，可以仅启用自己拥有的权限。这将阻止管理员创建具有超过其当前所拥有的权限的角色，然后将其分配给自己（或编辑已分配的角色）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

角色名称最多可以包含 64 个 Unicode 字符；不能包含反斜线、正斜线、分号、冒号、英镑符号、逗号、星号、问号、等号、左右箭头、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。只有支持自定义角色的版本在“操作”窗格中有相关项。

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。

- 查看角色详细信息：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。
- 创建自定义角色：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。
- 复制角色：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。
- 编辑自定义角色：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。
- 删除自定义角色：在中间窗格中选择角色，然后在“操作”窗格中单击删除角色。出现提示时，确认删除。

创建和管理作用域

创建站点时，唯一可用的作用域是不能删除的“全部”作用域。

可以使用以下过程创建作用域。也可以在创建管理员时创建作用域；每个管理员必须至少与一个角色和作用域对相关联。创建或编辑桌面、计算机目录、应用程序或主机时，可将其添加到现有作用域。如果未将其添加到作用域，则它们仍是“全部”作用域的一部分。

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。（完全权限管理员始终具有“全部”作用域。）计算机、电源操作、桌面和会话不直接作为作用域。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。作用域名称不能包含：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，请确保作用域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。

- 创建作用域：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）。
- 复制作用域：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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 编辑作用域：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。
- 删除作用域：在中间窗格中选择作用域，然后在“操作”窗格中单击删除作用域。出现提示时，确认删除。

创建报告

可以创建两种类型的委派管理报告：

- HTML 报告，此报告将列出与管理员关联的角色/作用域对以及每种对象类型（例如，交付组和计算机目录）的各个权限。通过 Studio 生成此报告。

  要创建此报告，请在 Studio 导航窗格中单击配置 **>** 管理员。在中间窗格中选择“管理员”，然后在“操作”窗格中单击创建报告。

  您还可以在创建、复制或编辑管理员时请求此报告。

- 将所有内置和自定义角色映射到权限的 HTML 或 CSV 报告。通过运行名为 OutputPermissionMapping.ps1 的 PowerShell 脚本生成此报告。

  要运行此脚本，您必须是完全权限管理员、只读权限管理员或具有读取角色权限的自定义管理员。此脚本位于：Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts。

  语法：

  ```
  OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path string] [-AdminAddress string] [-Show] [CommonParameters]
  ```

参数	说明
-Help	显示脚本帮助。
-Csv	指定 CSV 输出。默认值：HTML
-Path string	输出的写入位置。默认值：stdout
-AdminAddress string	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。
CommonParameters	Verbose、Debug、ErrorAction、ErrorVariable、WarningAction、WarningVariable、OutBuffer 和 OutVariable。有关详细信息，请参阅 Microsoft 文档。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

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

管理安全密钥

May 6, 2022

> 注意：
>
> - 必须将此功能与 StoreFront 1912 LTSR CU2 或更高版本结合使用。
> - 只有 Citrix ADC 和 Citrix Gateway 12.1 及更高版本支持安全 XML 功能。

此功能允许您仅允许经批准的 StoreFront 和 Citrix Gateway 计算机与 Citrix Delivery Controller 进行通信。启用此功能后，将阻止不包含该密钥的任何请求。使用此功能可添加额外的安全层，以防止来自内部网络的攻击。

使用此功能的常规工作流程如下：

1. 通过使用 PowerShell SDK 在 Studio 中启用该功能。
2. 在 Studio 中配置各项设置。（使用 Studio 控制台或 PowerShell）。
3. 在 StoreFront 中配置各项设置。（使用 PowerShell）。
4. 在 Citrix ADC 中配置设置。

启用安全密钥功能

默认情况下，该功能处于禁用状态。要将其启用，请使用远程 PowerShell SDK。有关远程 PowerShell SDK 的详细信息，请参阅 SDK 和 API。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

要启用此功能，请执行以下步骤：

1. 运行 Citrix Virtual Apps and Desktops 远程 PowerShell SDK。
2. 在命令窗口中，运行以下命令：

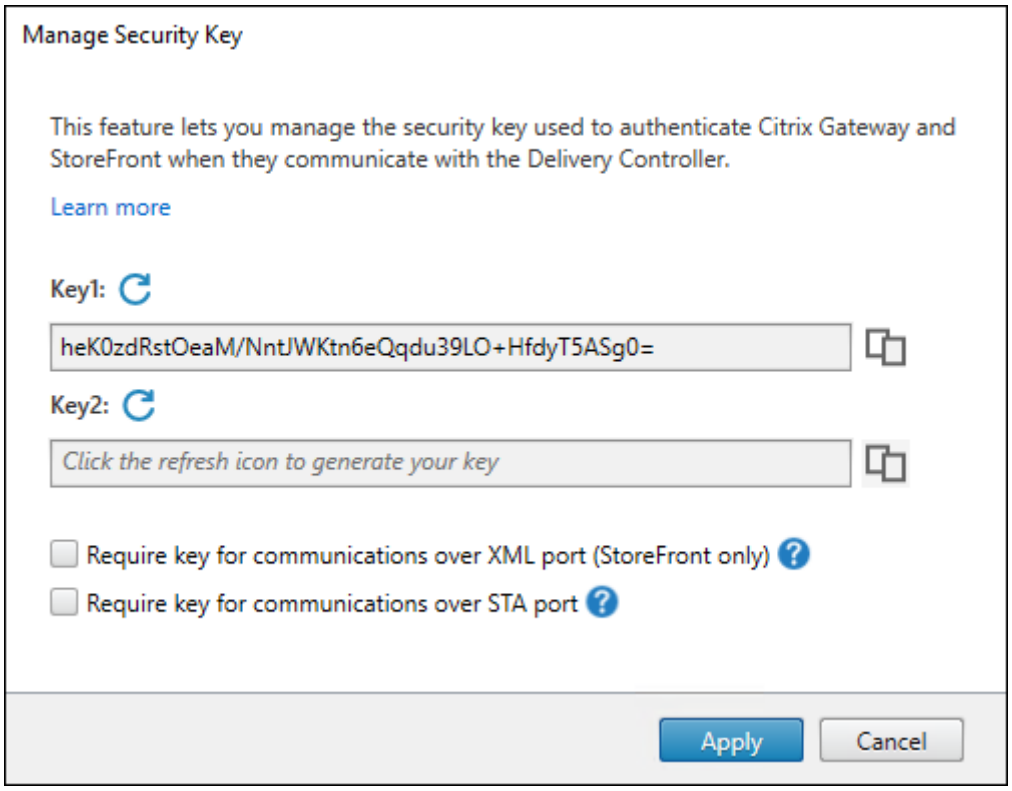
    - `Add-PSSnapIn Citrix*`. 此命令将添加 Citrix 管理单元。
    - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManageme "-Value "True"`

在 **Studio** 中配置各项设置

您可以通过使用 Studio 控制台或 PowerShell 在 Studio 中配置各项设置。

使用 **Studio** 控制台

启用此功能后，导航到 **Studio >** 设置 **>** 管理安全密钥，然后单击编辑。此时将显示管理安全密钥窗口。单击保存以应用所做的更改并退出窗口。



> 重要：
>
> - 有两个密钥可供使用。通过 XML 和 STA 端口进行通信时，您可以使用相同的密钥或不同的密钥。我们建议

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 您一次仅使用一个密钥。未使用的密钥仅用于密钥轮换。
> - 请勿单击刷新图标以更新已在使用的密钥。如果这样做，将会发生服务中断。

单击刷新图标以生成新密钥。

需要密钥才能通过 **XML** 端口进行通信 **(**仅限 **StoreFront)**。如果选择此选项，则需要密钥才能对通过 XML 端口进行的通信执行身份验证。StoreFront 通过此端口与 Citrix Cloud 进行通信。有关更改 XML 端口的信息，请参阅知识中心文章 CTX127945。

需要密钥才能通过 **STA** 端口进行通信。如果选择此选项，则需要密钥才能对通过 STA 端口进行的通信执行身份验证。Citrix Gateway 和 StoreFront 通过此端口与 Citrix Cloud 进行通信。有关更改 STA 端口的信息，请参阅知识中心文章 CTX101988。

应用更改后，单击关闭退出管理安全密钥窗口。

使用 **PowerShell**

以下是相当于 Studio 操作的 PowerShell 步骤。

1. 运行 Citrix Virtual Apps and Desktops 远程 PowerShell SDK。
2. 在命令窗口中，运行以下命令：
   - `Add-PSSnapIn Citrix*`
3. 运行以下命令以生成密钥并设置 Key1：
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. 运行以下命令以生成密钥并设置 Key2：
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`
5. 运行以下一个或两个命令以在对通信进行身份验证时使用密钥：
   - 要对通过 XML 端口进行的通信执行身份验证，请执行以下操作：
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - 要对通过 STA 端口进行的通信执行身份验证，请执行以下操作：
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

有关指导和语法，请参阅 PowerShell 命令帮助。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

在 **StoreFront** 中配置各项设置

在 Studio 中完成配置后，您需要在 StoreFront 中使用 PowerShell 配置相关设置。

在 StoreFront 服务器上，运行以下 PowerShell 命令：

- 要配置通过 XML 端口进行通信所需的密钥，请使用 `Get-STFStoreServie` 和 `Set-STFStoreService` 命令。例如：
  - `PS C:\> Set-STFStoreFarm $farm -Farmtype XenDesktop -Port 80 -TransportType HTTP -Servers <domain name1, domain name2> -XMLValidationEnabled $true -XMLValidationSecret <the key you generated in Studio>`
- 要配置通过 STA 端口进行通信所需的密钥，请使用 `New-STFSecureTicketAuthority` 命令。例如：
  - `PS C:\> $sta = New-STFSecureTicketAuthority -StaUrl <STA URL> -StaValidationEnabled $true -StavalidationSecret <the key you generated in Studio>`

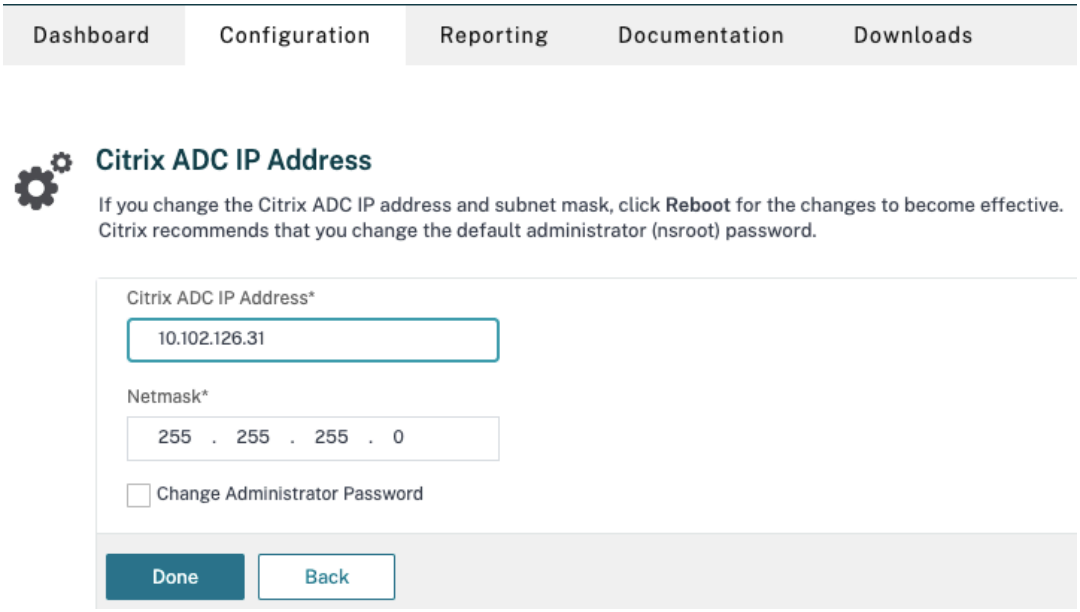
有关指导和语法，请参阅 PowerShell 命令帮助。

在 **Citrix ADC** 中配置设置

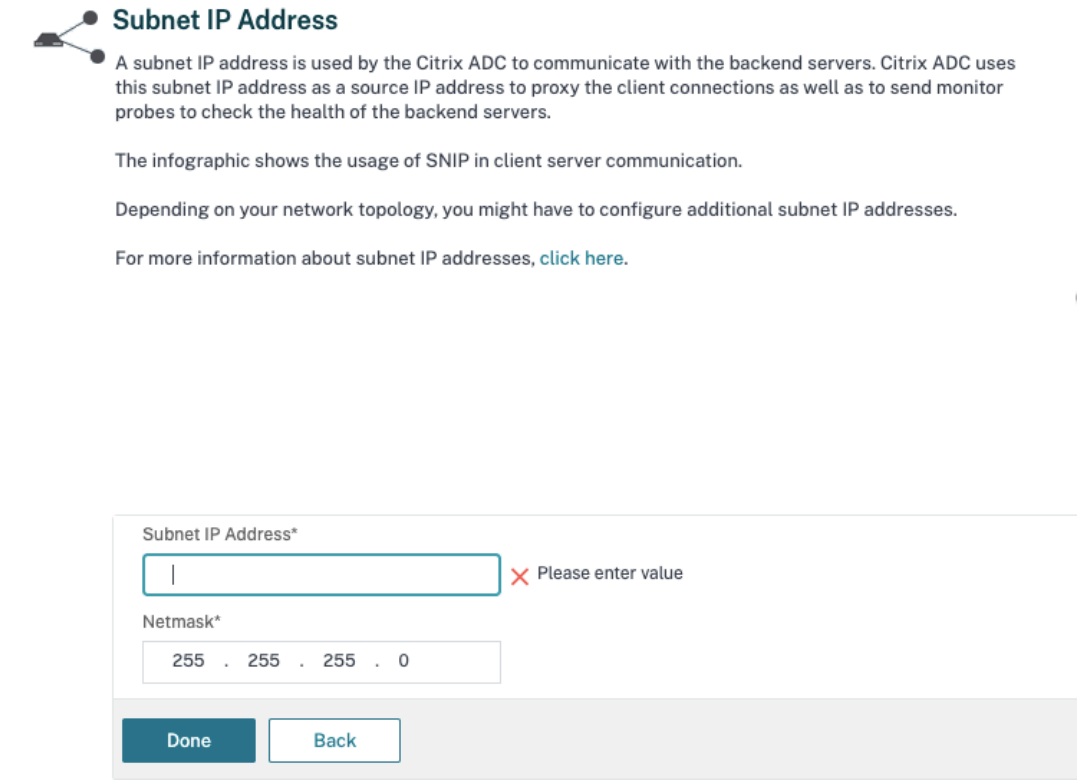
> 注意：
>
> 除非您使用 Citrix ADC 作为网关，否则不需要在 Citrix ADC 中配置此功能。如果使用 Citrix ADC，请按照以下步骤进行操作。

1. 确保以下必备配置已就绪：
   - 配置了以下 Citrix ADC 相关的 IP 地址。
     - 用于访问 Citrix ADC 控制台的 Citrix ADC 管理 IP (NSIP) 地址。有关详细信息，请参阅配置 NSIP 地址。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

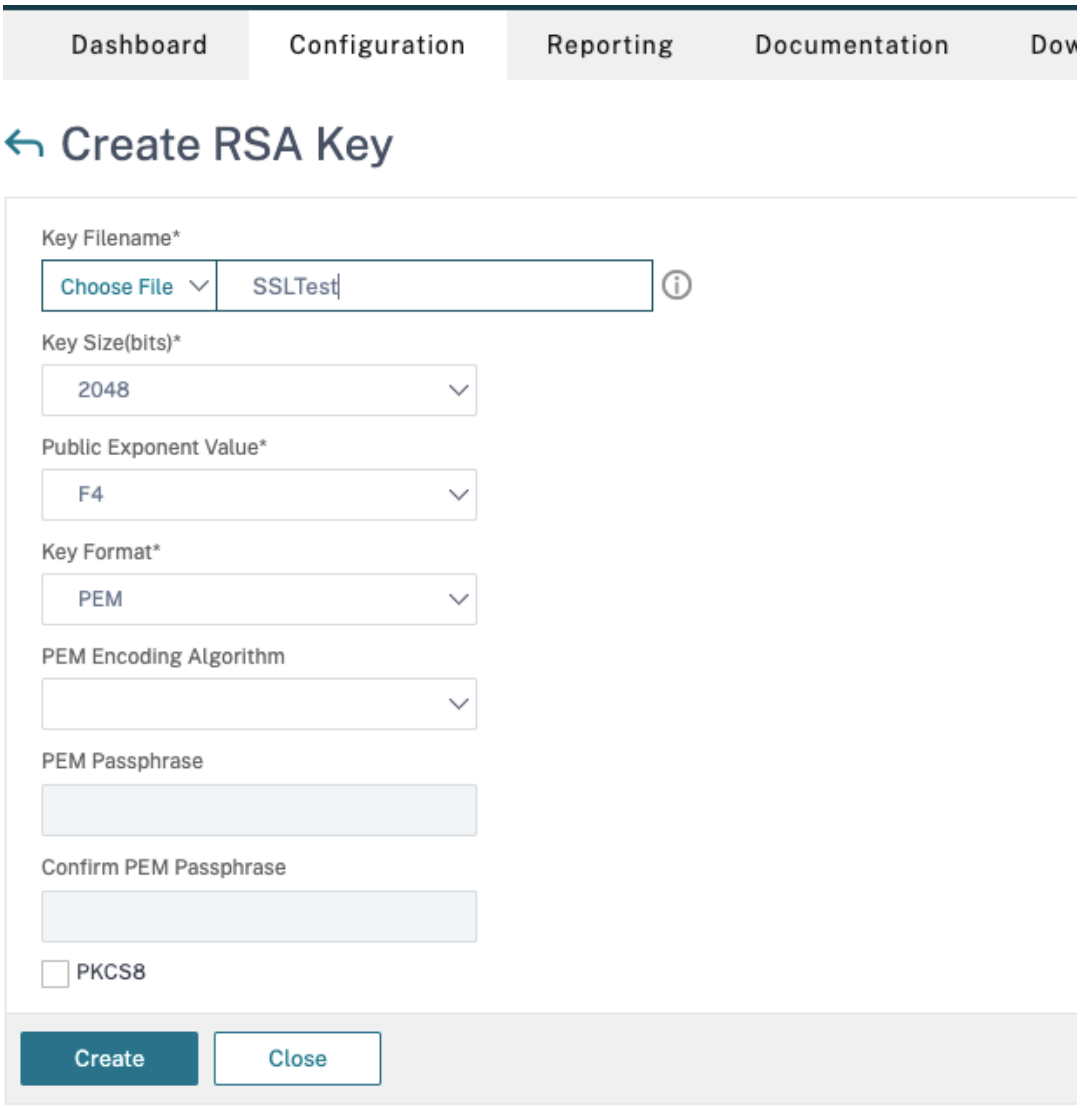


- 子网 IP (SNIP) 地址，用于启用 Citrix ADC 设备与后端服务器之间的通信。有关详细信息，请参阅配置子网 IP 地址。
- Citrix Gateway 虚拟 IP 地址和负载平衡器虚拟 IP 地址，用于登录 ADC 设备以启动会话。有关详细信息，请参阅创建虚拟服务器。



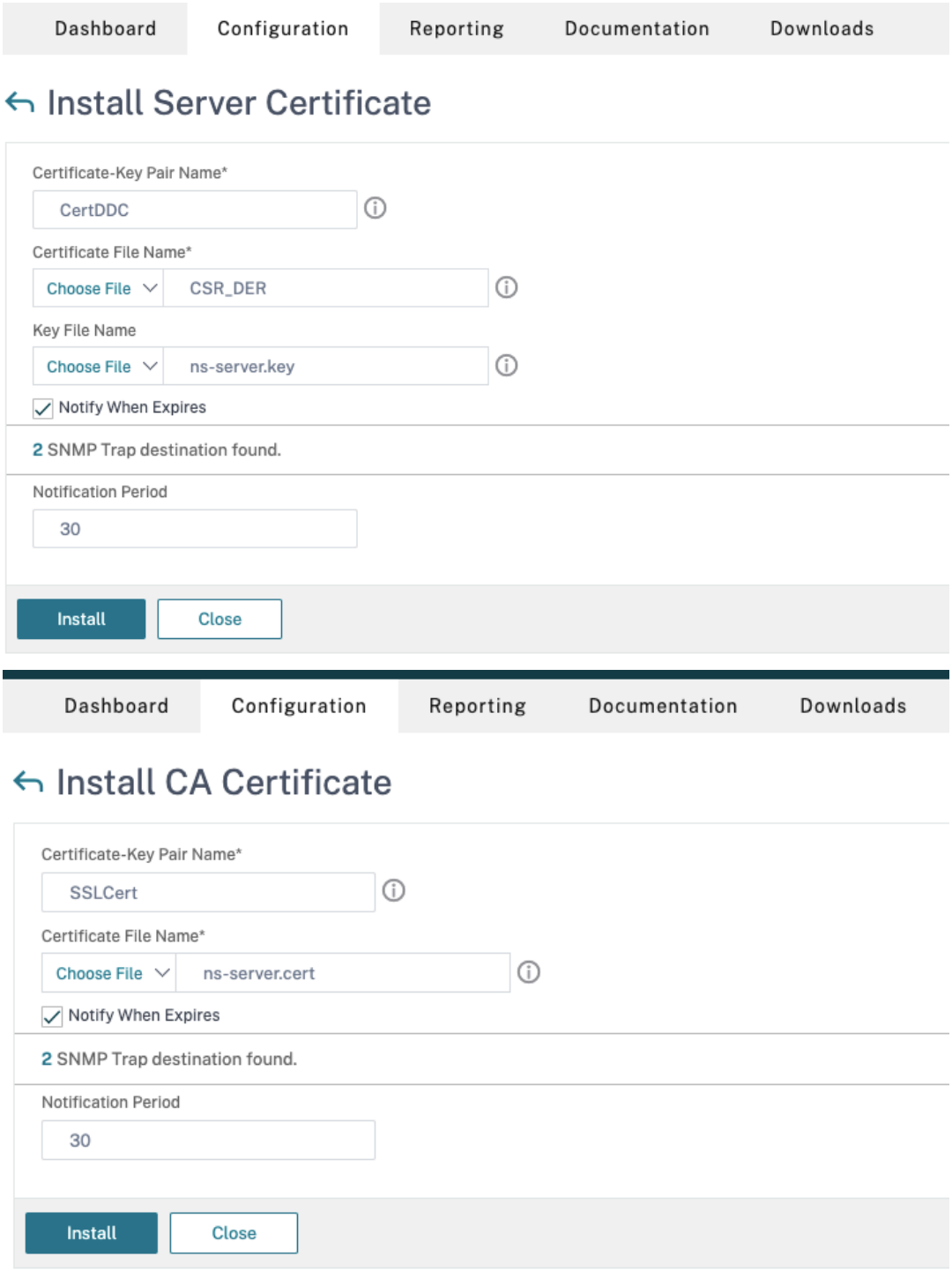
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Citrix ADC 设备中所需的模式和功能已启用。
  - 要启用这些模式，请在 Citrix ADC GUI 中导航到 **System**（系统）**> Settings**（设置）**> Configure Mode**（配置模式）。
  - 要启用这些功能，请在 Citrix ADC GUI 中导航到 **System**（系统）**> Settings**（设置）**> Configure Basic Features**（配置基本功能）。
- 与证书有关的配置已完成。
  - 此时将创建证书签名请求 (CSR)。有关详细信息，请参阅创建证书。



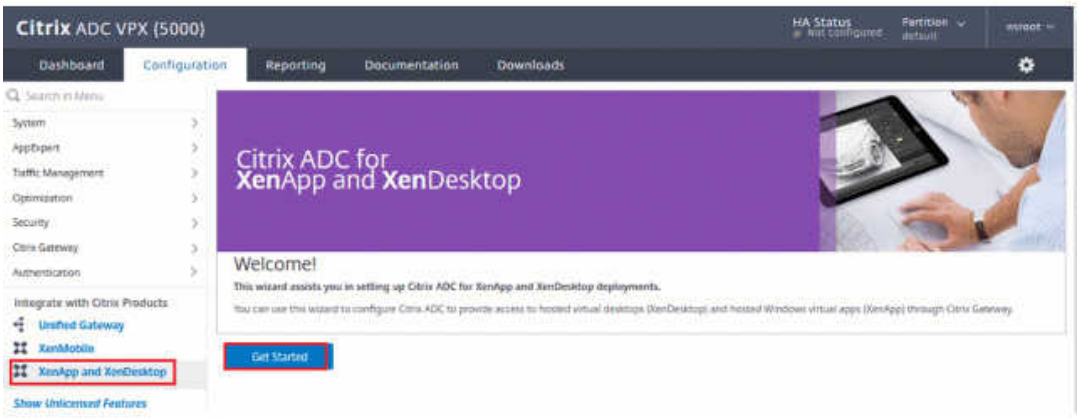
  - 已安装服务器和 CA 证书以及根证书。有关详细信息，请参阅安装、链接和更新。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- 已为 Citrix Virtual Desktops 创建 Citrix Gateway。单击 **Test STA Connectivity**（测试 STA 连接）按钮以确认虚拟服务器处于联机状态，测试连接。有关详细信息，请参阅为 Citrix Virtual Apps and Desktops 设置 Citrix ADC。

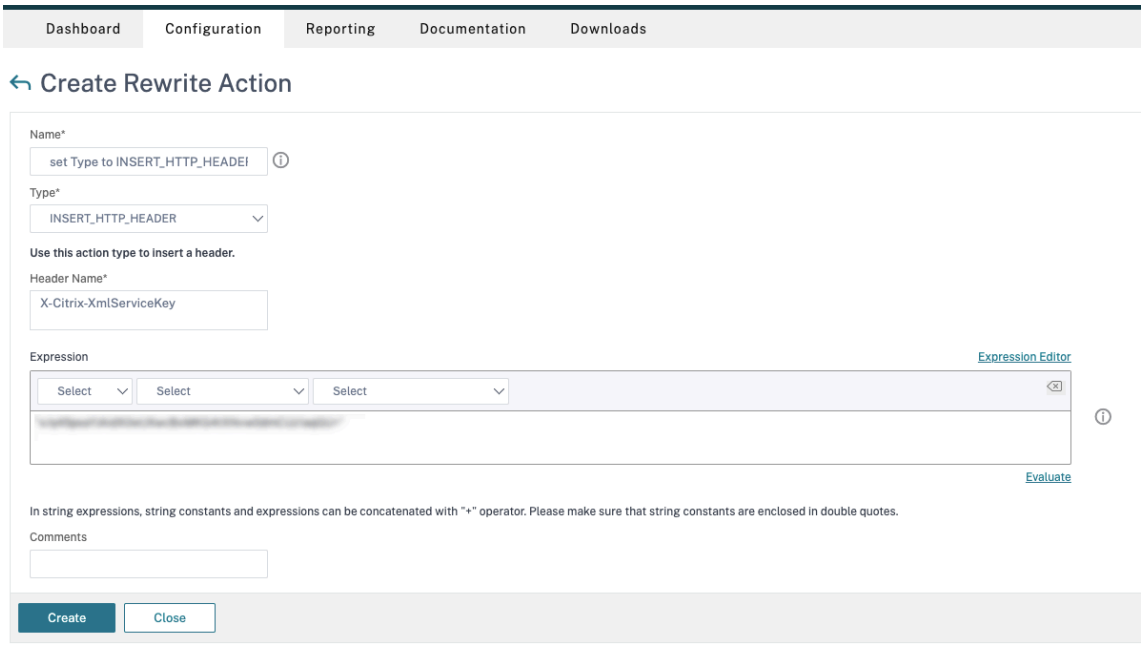
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. 添加重写操作。有关详细信息，请参阅配置重写操作。

   a) 导航到 **AppExpert > Rewrite**（重写）**> Actions**（操作）。

   b) 单击 **Add**（添加）以添加新的重写操作。可以将该操作命名为“set Type to INSERT_HTTP_HEADER”（将“类型”设置为 INSERT_HTTP_HEADER）。

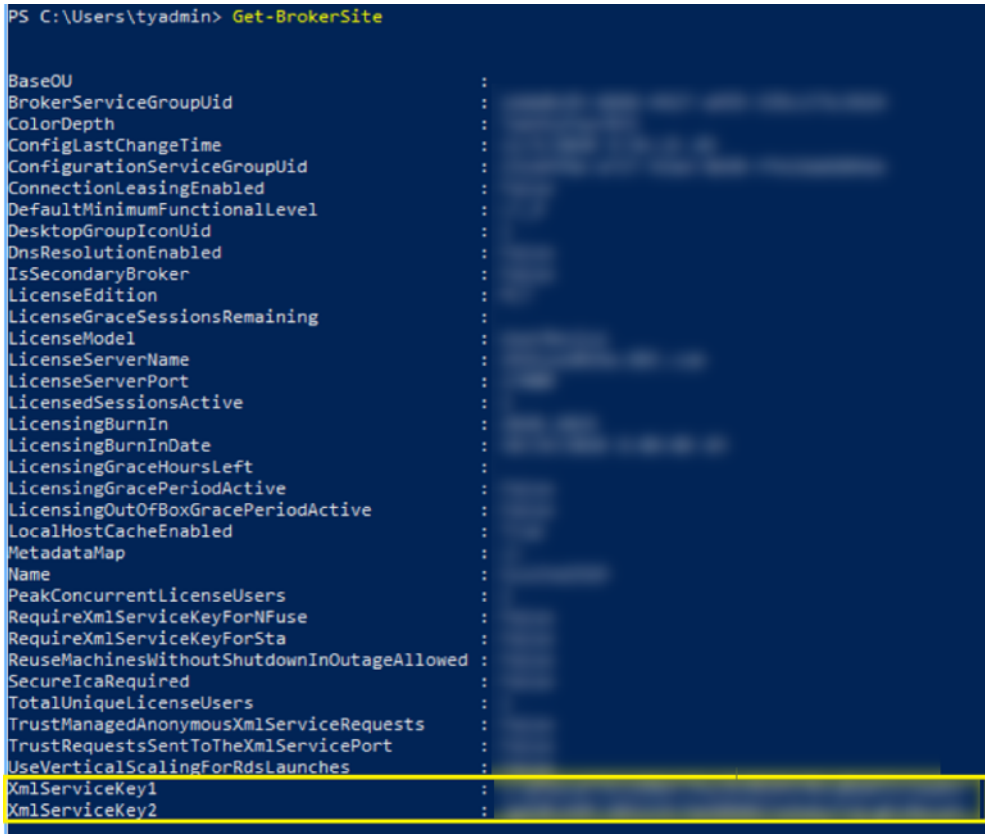


   a) 在 **Type**（类型）中，选择 **INSERT_HTTP_HEADS**。

   b) 在 **Header Name**（标题名称）中，输入 X-Citrix-XmlServiceKey。

   c) 在 **Expression**（表达式）中，使用引号添加 <XmlServiceKey1 value>。可以从 Desktop Delivery Controller 配置中复制 XmlServiceKey1 值。

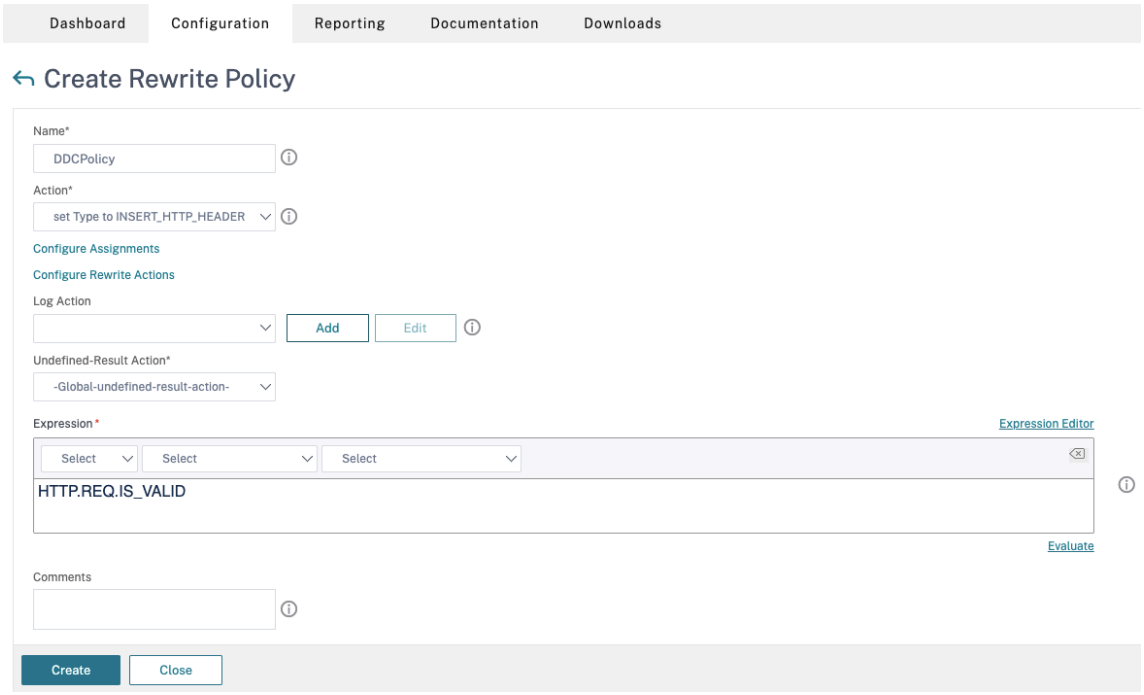
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. 添加重写策略。有关详细信息，请参阅配置重写策略。

   a) 导航到 **AppExpert > Rewrite**（重写）**> Policies**（策略）。

   b) 单击添加添加新策略。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

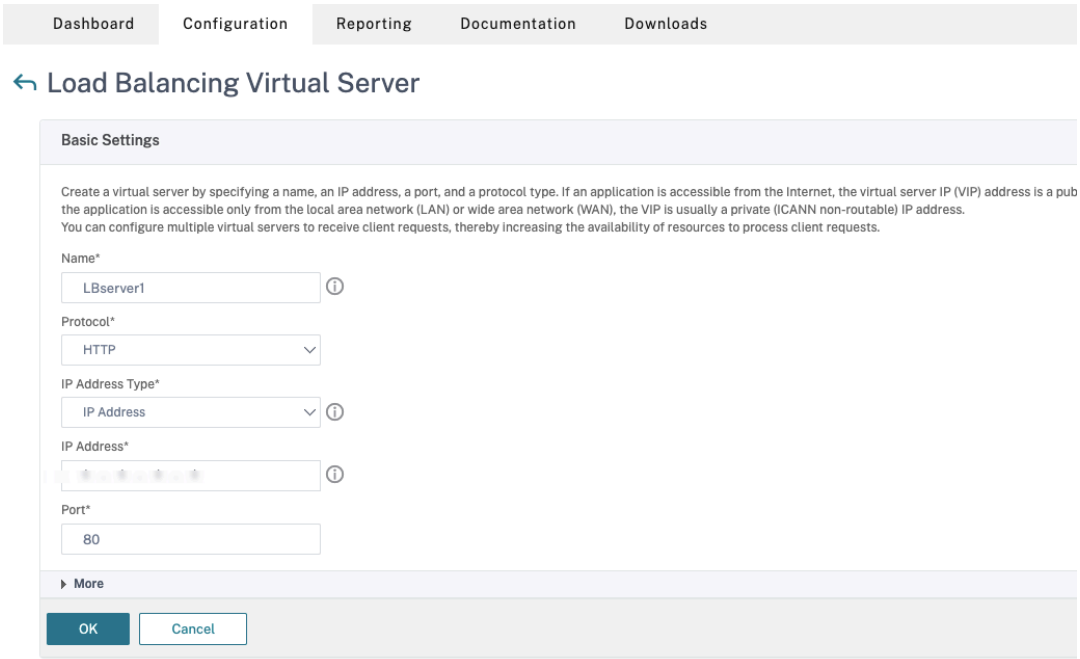
a) 在 **Action**（操作）中，选择在前一步中创建的操作。
b) 在 **Expression**（表达式）中，添加 HTTP.REQ.IS_VALID。
c) 单击确定。

4. 设置负载平衡。必须为每台 STA 服务器配置一个负载平衡虚拟服务器。否则，会话将无法启动。

有关详细信息，请参阅设置基本负载平衡。

a) 创建负载平衡虚拟服务器。

- 导航到 **Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Servers**（服务器）。
- 在 **Virtual Servers**（虚拟服务器）页面中，单击 **Add**（添加）。

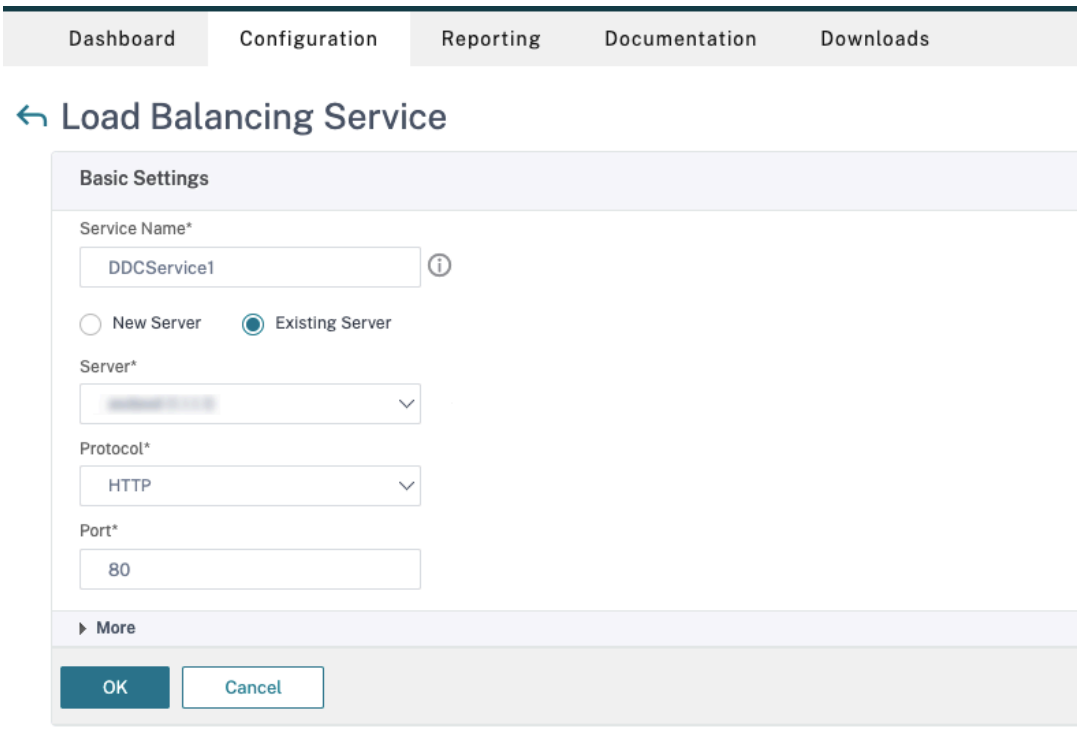


- 在 **Protocol**（协议）中，选择 **HTTP**。
- 添加负载平衡虚拟 IP 地址，然后在 **Port**（端口）中选择 **80**。
- 单击确定。

b) 创建负载平衡服务。

- 导航到 **Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Services**（服务）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

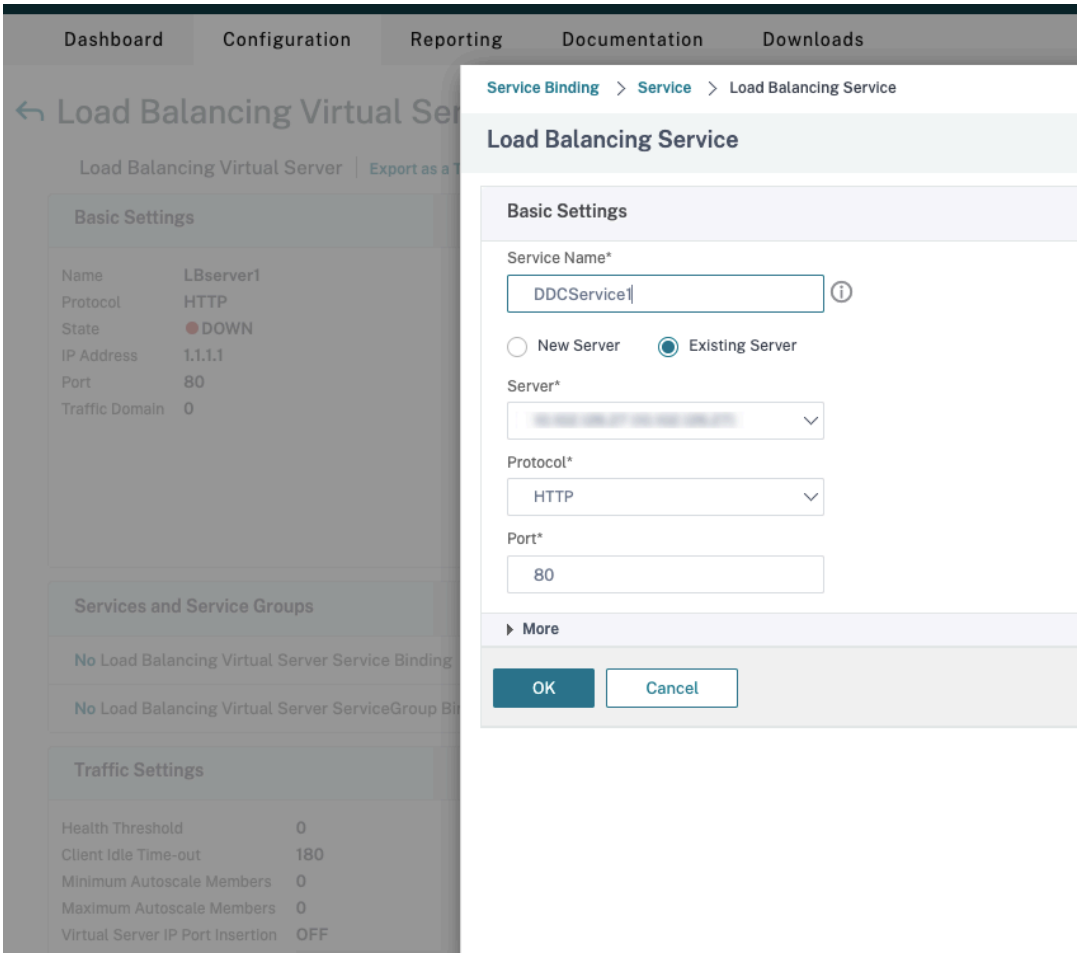


- 在 **Existing Server**（现有服务器）中，选择在上一步中创建的虚拟服务器。
- 在 **Protocol**（协议）中，选择 **HTTP**，然后在 **Port**（端口）中选择 **80**。
- 单击 **OK**（确定），然后单击 **Done**（完成）。

c) 将服务绑定到虚拟服务器。

- 选择之前创建的虚拟服务器，然后单击 **Edit**（编辑）。
- 在 **Services and Service Groups**（服务和服务组）中，单击 **No Load Balancing Virtual Server Service Binding**（无负载平衡虚拟服务器服务绑定）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

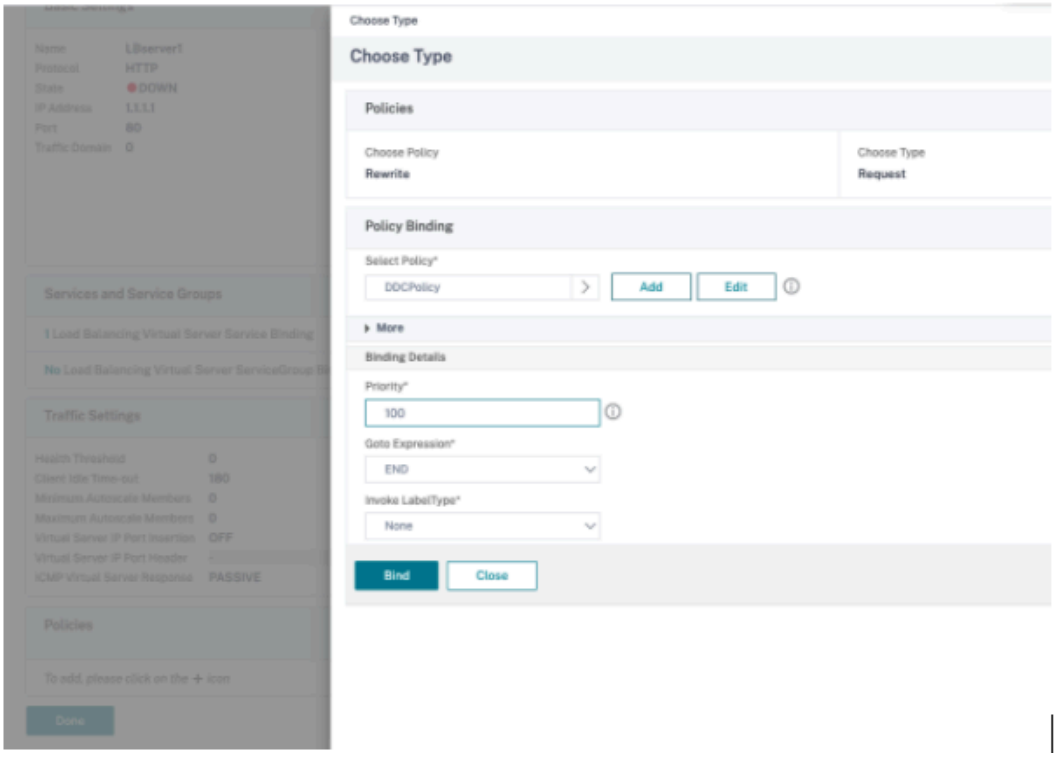


- 在 **Service Binding**（服务绑定）中，选择之前创建的服务。
- 单击 **Bind**（绑定）。

d) 将之前创建的重写策略绑定到虚拟服务器。

- 选择之前创建的虚拟服务器，然后单击 **Edit**（编辑）。
- 在 **Advanced Settings**（高级设置）中，单击 **Policies**（策略），然后在 **Policies**（策略）部分中单击 **+**。

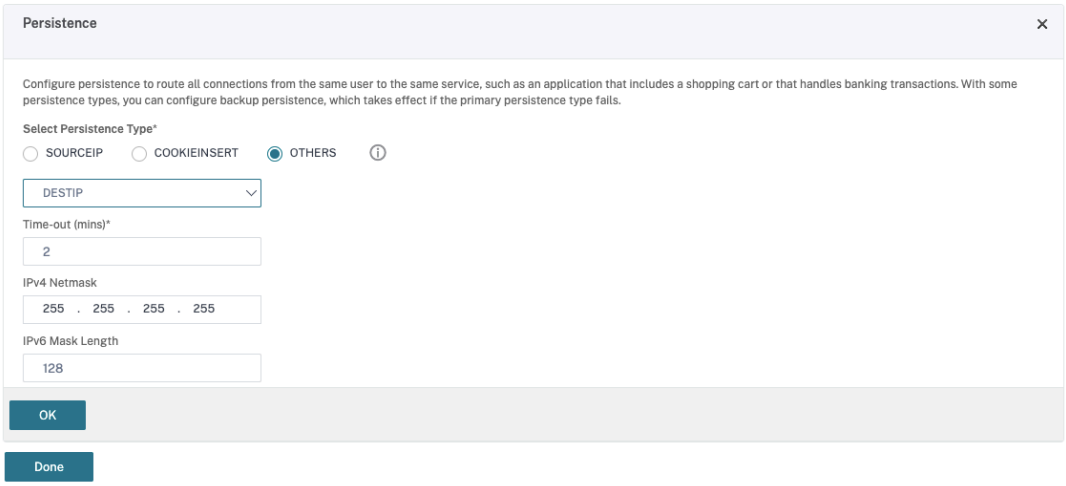
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- 在 **Choose Policy**（选择策略）中，选择 **Rewrite**（重写），然后在 **Choose Type**（选择类型）中选择 **Request**（请求）。
- 单击继续。
- 在 **Select Policy**（选择策略）中，选择之前创建的重写策略。
- 单击 **Bind**（绑定）。
- 单击完成。

e) 如有必要，请为虚拟服务器设置持久性。

- 选择之前创建的虚拟服务器，然后单击 **Edit**（编辑）。
- 在 **Advanced Settings**（高级设置）中，单击 **Persistence**（持久性）。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 选择 **Others**（其他）作为持久性类型。
- 选择 **DESTIP** 以根据虚拟服务器选择的服务的 IP 地址（目标 IP 地址）创建持久性会话
- 在 **IPv4 Netmask**（IPv4 网络掩码）中，添加与 DDC 相同的网络掩码。
- 单击确定。

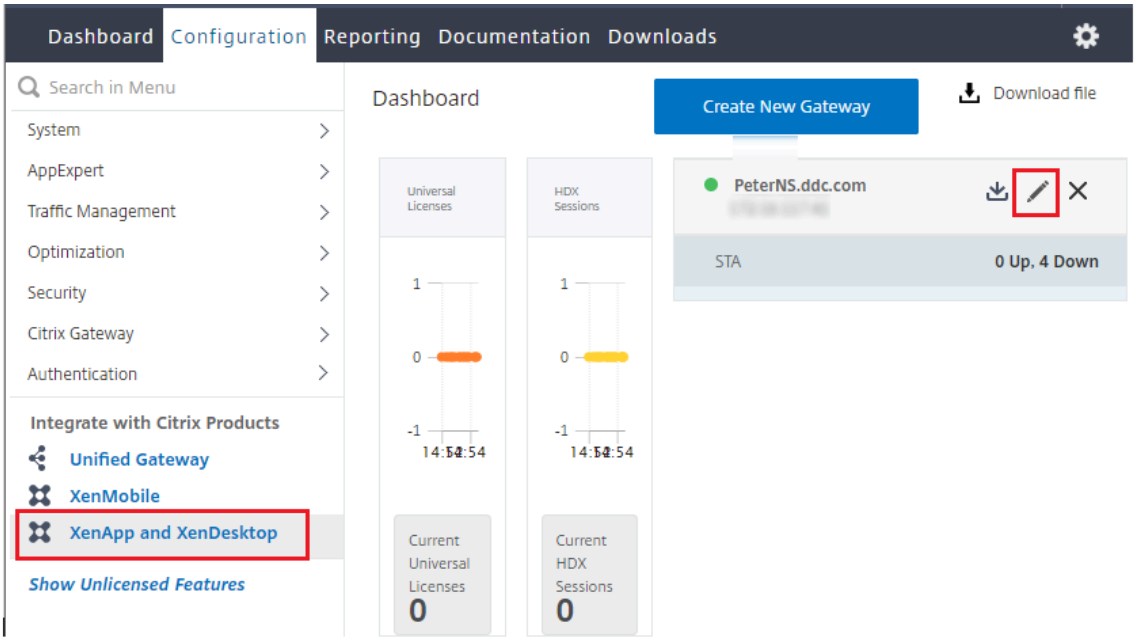
f) 对另一个虚拟服务器也重复这些步骤。

如果 **Citrix ADC** 设备已配置了 **Citrix Virtual Desktops**，配置会发生变化

如果您已经为 Citrix ADC 设备配置了 Citrix Virtual Desktops，则必须进行以下配置更改，才能使用安全 XML 功能。

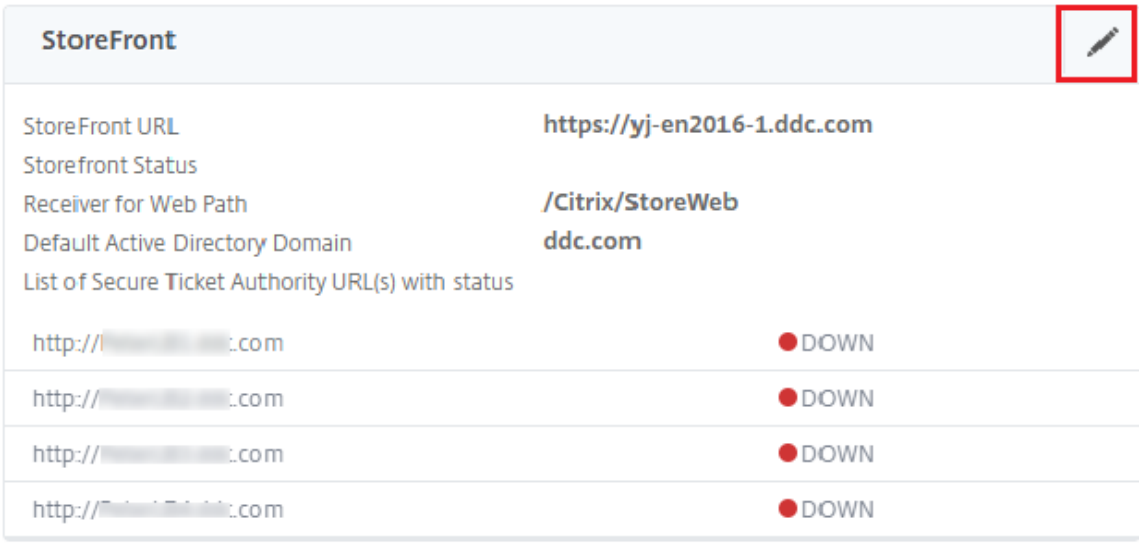
- 在会话启动之前，请更改网关的 **Security Ticket Authority URL**，以使用负载平衡虚拟服务器的 FQDN。
- 确保将 `TrustRequestsSentToTheXmlServicePort` 参数设置为 False。默认情况下，`TrustRequestsSentToTheXmlServicePort` 参数设置为 False。但是，如果客户已经为 Citrix Virtual Desktops 配置了 Citrix ADC，则将 `TrustRequestsSentToTheXmlServicePort` 设置为 True。

1. 在 Citrix ADC GUI 中，导航到 **Configuration**（配置）**> Integrate with Citrix Products**（与 **Citrix** 产品集成），然后单击 **XenApp and XenDesktop**（XenApp 和 XenDesktop）。
2. 选择网关实例，然后单击编辑图标。



3. 在 StoreFront 窗格中，单击编辑图标。

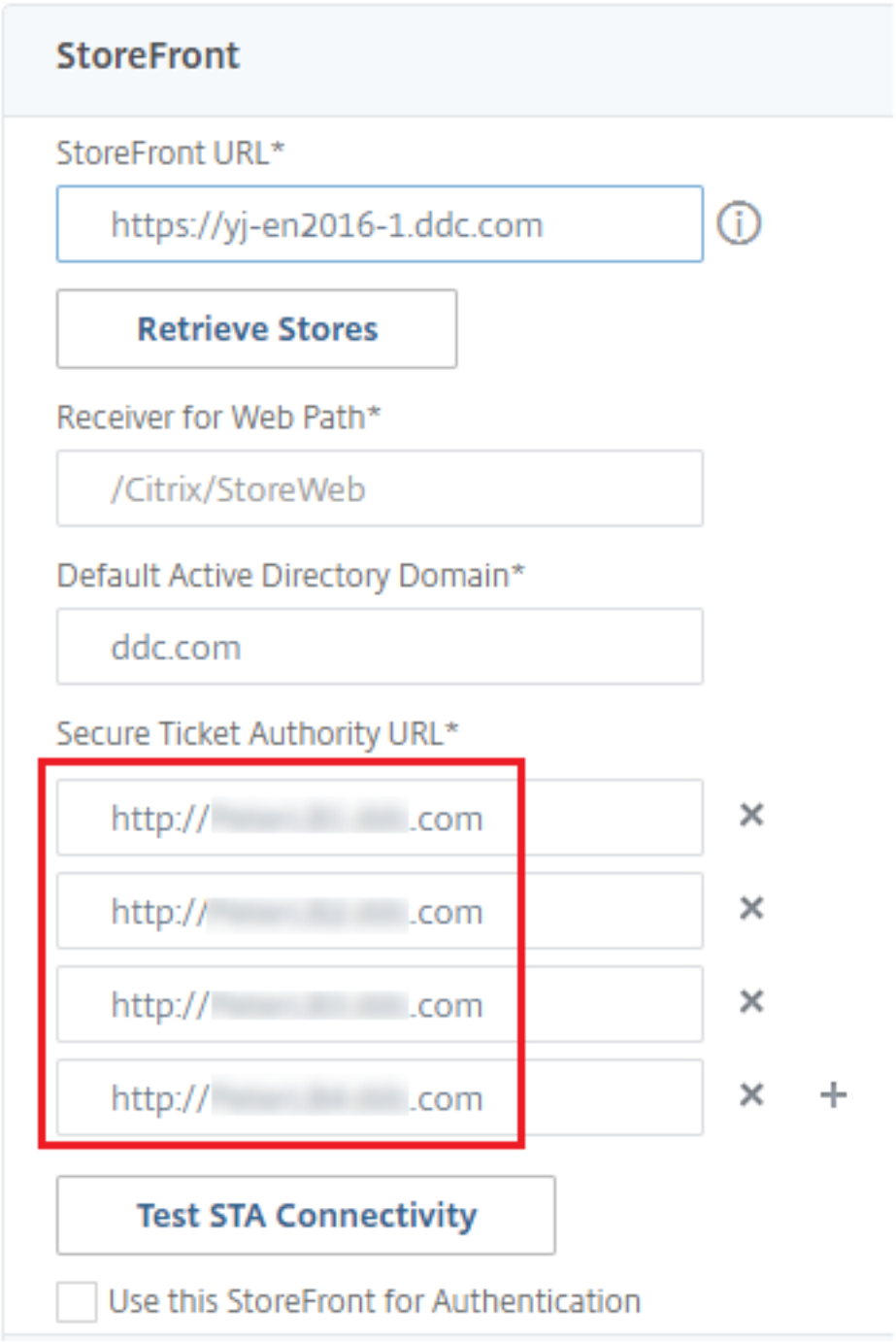
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. 添加 **Secure Ticket Authority URL**。

   - 如果启用了安全 XML 功能，STA URL 必须是负载平衡服务的 URL。
   - 如果禁用了安全 XML 功能，STA URL 必须是 STA（DDC 的地址）的 URL，并且 DDC 上的 TrustRequestsSentToTheXmlServicePort 参数必须设置为 True。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



智能卡

January 21, 2022

根据本文中介绍的指导原则，智能卡以及等效技术均受支持。要对 Citrix Virtual Apps 或 Citrix Virtual Desktops

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用使用智能卡，请完成以下各项：

- 了解贵组织与使用智能卡有关的安全策略。例如，这些策略可能说明如何颁发智能卡，以及用户应该如何保护这些智能卡。在 Citrix Virtual Apps 或 Citrix Virtual Desktops 环境中，可能需要重新评估这些策略的某些方面。
- 确定要与智能卡结合使用的用户设备类型、操作系统和已发布的应用程序。
- 熟悉智能卡技术以及选定智能卡供应商提供的硬件和软件。
- 了解如何在分布式环境中部署数字证书。

> 注意：
>
> 快速智能卡不支持智能卡注册。禁用了快速智能卡时，智能卡注册可能会起作用，但取决于智能卡和中间件的类型。请联系您的智能卡和中间件供应商，了解他们与 Citrix Virtual Apps and Desktops 的集成以及是否支持通过虚拟会话进行智能卡注册。

智能卡类型

企业和使用者智能卡具有相同的尺寸和电连接器，并且适合相同的智能卡读卡器。

供企业使用的智能卡包含数字证书。这些智能卡支持 Windows 登录，并且还可以与应用程序结合使用以进行数字签名以及文档和电子邮件的加密。Citrix Virtual Apps and Desktops 支持这些用法。

供使用者使用的智能卡不包含数字证书，但包含一个共享机密。这些智能卡可以支持付款（例如，签名支付或芯片密码信用卡）。这些智能卡不支持 Windows 登录或典型的 Windows 应用程序。需要对这些智能卡使用专用 Windows 应用程序和适用的软件基础结构（例如，包括与支付卡网络建立连接）。要了解与支持在 Citrix Virtual Apps 或 Citrix Virtual Desktops 上使用这些专用应用程序有关的信息，请联系您的 Citrix 代表。

对于企业智能卡，这些是能够以相似的方式使用的兼容等效物。

- 与智能卡等效的 USB 令牌直接连接到 USB 端口。这些 USB 令牌通常与 U 盘大小相同，但可以像手机中使用的 SIM 卡一样小。这些令牌显示为智能卡与 USB 智能卡读卡器的组合。
- 使用 Windows 受信任的平台模块 (TPM) 的虚拟智能卡显示为智能卡。使用 Citrix Workspace 应用程序（最低版本为 Citrix Receiver 4.3）的 Windows 8 和 Windows 10 支持这些虚拟智能卡。
  - XenApp and XenDesktop 7.6 FP3 之前的 Citrix Virtual Apps and Desktops（以前称为 XenApp 和 XenDesktop）版本不支持虚拟智能卡。
  - 有关虚拟智能卡的详细信息，请参阅虚拟智能卡概览。

  注意：术语“虚拟智能卡”还用于描述存储在用户计算机上的数字证书。这些数字证书严格而言不等同于智能卡。

Citrix Virtual Apps and Desktops 智能卡支持基于 Microsoft 个人计算机/智能卡 (PC/SC) 标准规范。智能卡和智能卡设备必须受底层 Windows 操作系统支持，并且必须获得 Microsoft Windows 硬件质量实验室 (WHQL) 批准，可在运行合格 Windows 操作系统的计算机上使用，这是最低要求。有关硬件 PC/SC 合规性的其他信息，请参阅 Microsoft 文档。其他类型的用户设备可能遵守 PS/SC 标准。有关详细信息，请参阅 Citrix Ready 计划。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

一般情况下，每个供应商的智能卡或等效物都需要独立的设备驱动程序。但是，如果智能卡遵守诸如 NIST 个人身份验证 (PIV) 标准等标准，则可以对一系列智能卡使用单个设备驱动程序。必须将设备驱动程序同时安装在用户设备和 Virtual Delivery Agent (VDA) 上。设备驱动程序通常作为 Citrix 合作伙伴提供的智能卡中间件软件包的一部分提供；智能卡中间件软件包将提供高级功能。此外，还可以将设备驱动程序描述为加密服务提供程序 (CSP)、密钥存储提供程序 (KSP) 或微型驱动程序。

以下适用于 Windows 系统的智能卡和中间件的组合作为各自类型的代表，已经通过 Citrix 的测试。但是，也可以使用其他智能卡和中间件。有关与 Citrix 兼容的智能卡和中间件的详细信息，请参阅 http://www.citrix.com/ready。

中间件	相配的卡
适用于.NET 卡的 Gemalto 微型驱动程序	Gemalto .NET v2+

有关对其他设备类型使用智能卡的信息，请参阅 Citrix Workspace 应用程序文档中与该设备有关的内容。

Remote PC Access

仅在远程访问运行 Windows 10、Windows 8 或 Windows 7 的办公室物理 PC 时支持智能卡。

以下智能卡已通过 Remote PC Access 进行测试：

中间件	相配的卡
Gemalto .NET 微型驱动程序	Gemalto .NET v2+

快速智能卡

快速智能卡是对现有基于 HDX PC/SC 的智能卡重定向的改进。在高延迟 WAN 情况下使用智能卡时，可以提高性能。

默认情况下，在安装了当前支持的 Windows VDA 的主机上启用快速智能卡。要在主机端禁用快速智能卡（例如出于诊断目的），请将“Disable Cryptographic Redirection”（禁用加密重定向）注册表设置设为任意非零值：

```
HKLM\SOFTWARE\Citrix\SmartCard
CryptographicRedirectionDisable (DWORD)
<!--NeedCopy-->
```

在客户端，要启用快速智能卡，请将 SmartCardCryptographicRedirection ICA 参数包含在关联 StoreFront 站点的 *default.ica* 文件中：

```
[WFClient]
SmartCardCryptographicRedirection=On
```

限制：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 只有 Citrix Receiver for Windows 支持快速智能卡。如果在 default.ica 文件中配置了快速智能卡，非适用于 Windows 的 Citrix Receiver 将仍使用现有 PC/SC 重定向。
- 快速智能卡支持的唯一双跃点场景为 ICA 到在两个跃点中启用了快速智能卡的 ICA。由于快速智能卡不支持 ICA 到 RDP 的双跃点场景，因此这些情况下不起作用。
- 快速智能卡不支持下一代加密技术。因此，快速智能卡不支持椭圆曲线加密 (ECC) 智能卡。
- 快速智能卡仅支持只读密钥容器操作。
- 快速智能卡不支持更改智能卡 PIN。

智能卡读卡器类型

智能卡读卡器可能内置在用户设备中，或者单独连接到用户设备（通常通过 USB 或蓝牙进行连接）。支持遵守 USB 芯片/智能卡接口设备 (CCID) 规范的接触式读卡器。这些读卡器包含用户可插入智能卡的插槽或刷槽。Deutsche Kreditwirtschaft (DK) 标准定义了四种类别的接触式读卡器。

- 类别 1 智能卡读卡器最常见，通常仅包含一个插槽。随操作系统提供的标准 CCID 设备驱动程序通常支持类别 1 智能卡读卡器。
- 类别 2 智能卡读卡器还包含一个用户设备无法访问的安全数字小键盘。类别 2 智能卡读卡器可能内置在具有集成的安全数字小键盘的键盘中。要了解与类别 2 智能卡读卡器有关的信息，请联系您的 Citrix 代表；可能需要安装读卡器特有的设备驱动程序，才能启用安全数字小键盘功能。
- 类别 3 智能卡读卡器还包含一个安全显示屏。不支持类别 3 智能卡读卡器。
- 类别 4 智能卡读卡器还包含一个安全的交易模块。不支持类别 4 智能卡读卡器。

> 注意：
>
> 智能卡读卡器类别与 USB 设备类别无关。

智能卡读卡器必须随相应的设备驱动程序一起安装在用户设备上。

有关受支持的智能卡读卡器的信息，请参阅您使用的 Citrix Workspace 应用程序对应的文档。在 Citrix Workspace 应用程序文档中，支持的版本通常在智能卡一文或系统要求一文中列出。

用户体验

智能卡支持功能通过默认启用的特定 ICA/HDX 智能卡虚拟通道集成在 Citrix Virtual Apps and Desktops 中。

重要：请勿对智能卡读卡器使用通用 USB 重定向。该功能默认对智能卡读卡器禁用，如果启用，则不受支持。

在同一个用户设备上可以使用多个智能卡和多个读卡器，但是，如果正在使用直通身份验证，当用户启动虚拟桌面或应用程序时必须仅插入一个智能卡。在应用程序中使用智能卡时（例如，为了实现数字签名或加密功能），可能会出现要求插入智能卡或输入 PIN 的其他提示。同时插入多个智能卡时可能会发生这种情况。

- 当智能卡已插入读卡器中，但仍提示插入智能卡时，应选择取消。
- 如果提示输入 PIN，则应重新输入 PIN。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

您可以使用卡管理系统或供应商实用程序重置 PIN。

> 重要：
>
> 在 Citrix Virtual Apps 或 Citrix Virtual Desktops 会话中，不支持对 Microsoft 远程桌面连接应用程序使用智能卡。这有时称为“双跃点”用法。

部署智能卡之前的准备工作

- 获取智能卡读卡器的设备驱动程序，并将其安装到用户设备。许多智能卡读卡器可以使用 Microsoft 提供的 CCID 设备驱动程序。
- 从智能卡供应商处获取设备驱动程序和加密服务提供程序 (CSP) 软件，然后将其安装在用户设备和虚拟桌面上。驱动程序和 CSP 软件必须与 Citrix Virtual Apps and Desktops 兼容；请查阅供应商的文档以了解兼容性。对于支持并使用微型驱动程序模型的智能卡的虚拟桌面，智能卡微型驱动程序应自动下载，但您也可以从 http://catalog.update.microsoft.com 或从供应商处获取。此外，如果需要 PKCS#11 中间件，请从卡供应商处获取。
- 重要：Citrix 建议您首先在物理计算机上安装并测试驱动程序和 CSP 软件，然后再安装 Citrix 软件。
- 在 Windows 10 上的 Internet Explorer 中，为使用智能卡的用户将 Citrix Receiver for Web URL 添加到可信站点列表中。在 Windows 10 中，Internet Explorer 默认情况下不会针对可信站点采用受保护模式运行。
- 确保正确配置了您的公钥基础结构 (PKI)。包括确保针对 Active Directory 环境正确配置了证书至帐户的映射，并且可以成功执行用户证书验证。
- 确保您的部署符合与智能卡结合使用的其他 Citrix 组件（包括 Citrix Workspace 应用程序和 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 Gateway/Citrix Access Gateway 10.x
  - VDA
  - （对于 Remote PC Access 可选）：Microsoft Exchange Server

支持使用智能卡

步骤 **1.** 根据智能卡颁发策略向用户颁发智能卡。

步骤 **2.** （可选）设置智能卡以使用户能够启用 Remote PC Access。

步骤 **3.** 安装并配置 Delivery Controller 和 StoreFront（如果尚未安装）以实现智能卡远程连接。

步骤 **4.** 启用 StoreFront 以使用智能卡。有关详细信息，请参阅 StoreFront 文档中的配置智能卡身份验证。

步骤 **5.** 启用 Citrix 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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

步骤 **6.** 启用 VDAs 以使用智能卡。

- 确保 VDA 具有必需的应用程序和更新。
- 安装中间件。
- 设置智能卡远程连接功能，在用户设备上的 Citrix Workspace 应用程序与虚拟桌面会话之间启用智能卡数据的通信。

步骤 **7.** 使用户设备（包括加入域的计算机或未加入域的计算机）支持使用智能卡。有关详细信息，请参阅 StoreFront 文档中的配置智能卡身份验证。

- 向设备的密钥库中导入证书颁发机构根证书和颁发的证书颁发机构证书。
- 安装您的供应商提供的智能卡中间件。
- 安装并配置适用于 Windows 的 Citrix Workspace 应用程序，确保通过使用组策略管理控制台来导入 icaclient.adm 并启用智能卡身份验证。

步骤 **8.** 测试部署。使用测试用户的智能卡启动虚拟桌面，来确保已正确配置您的部署。测试所有可能的访问机制（例如，通过 Internet Explorer 和 Citrix Workspace 应用程序访问桌面）。

跟踪智能卡读卡器插入计数

使用智能卡远程处理功能时，您可以使用 SCardGetStatusChange 功能跟踪插入智能卡或从读卡器中删除智能卡的次数。该函数将更新 SCARD_READERSTATE 数据结构的阵列—您监视的每个读取器一个阵列。每个 SCARD_READERSTATE 的 dwEventState 字段的高位字（16 位）都包含读卡器计数。有关详细信息，请参阅 Microsoft 文章 SCardGetStatusChangeA function（SCardGetStatusChangeA 函数）和 SCARD_READERSTATEA structure（SCARD_READERSTATEA 结构）。

默认情况下，读卡器插入计数报告设置处于禁用状态。要启用跟踪，请添加以下注册表项：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

名称：EnableReaderInsertCountReporting

类型：DWORD

值：任何非零值

当会话断开连接时，计数将重置为零。

读卡器插入计数报告与第三方智能卡中间件兼容。

智能卡部署

November 17, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

本产品版本和包含本版本的混合环境支持下列类型的智能卡部署。其他配置可能可以运行，但不受支持。

类型	StoreFront 连接
加入本地域的计算机	直接连接
从加入域的计算机远程访问	通过 Citrix 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 Citrix Gateway 连接
访问桌面设备站点的未加入域的计算机和瘦客户端	通过桌面设备站点连接
通过 XenApp Services URL 访问 StoreFront 的加入域的计算机和瘦客户端	通过 XenApp Services URL 连接

部署类型由智能卡读卡器连接到的用户设备的以下特性定义：

- 设备是否已加入域。
- 设备连接到 StoreFront 的方式。
- 查看虚拟桌面和应用程序使用的软件。

此外，启用智能卡的应用程序（如 Microsoft Word 和 Microsoft Excel）也可在这些部署中使用。这些应用程序允许用户对文档进行数字签名或加密。

双模式身份验证

在其中的每个部署中，如有可能，Receiver 支持双模式身份验证，允许用户在使用智能卡和输入其用户名和密码之间进行选择。如果无法使用智能卡（例如，用户将智能卡遗忘在家中或登录证书已过期），此功能会很有帮助。

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 Citrix Gateway，则用户登录设备后，Receiver for Windows 会提示用户向 Citrix Gateway 进行身份验证。对于加入域的设备和未加入域的设备均是如此。用户可以使用智能卡和 PIN 或使用显式凭据登录 Citrix Gateway。这样，您可以向用户提供用于 Citrix Gateway 登录的双模式身份验证。可以配置从 Citrix Gateway 到 StoreFront 的直通身份验证，并将智能卡用户的凭据验证委派给 Citrix Gateway，这样用户就可以无提示地向 StoreFront 进行身份验证。

多个 **Active Directory** 林注意事项

在 Citrix 环境中，在单个林中支持智能卡。跨林进行智能卡登录要求对所有用户帐户启用直接双向林信任。不支持涉及智能卡的更加复杂的多林部署（即，其中的信任仅为单向信任或具有不同的类型）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。

智能卡移除策略

在产品上设置的智能卡移除策略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。智能卡移除策略通过 Windows 操作系统进行配置，并且也由 Windows 操作系统来处理。

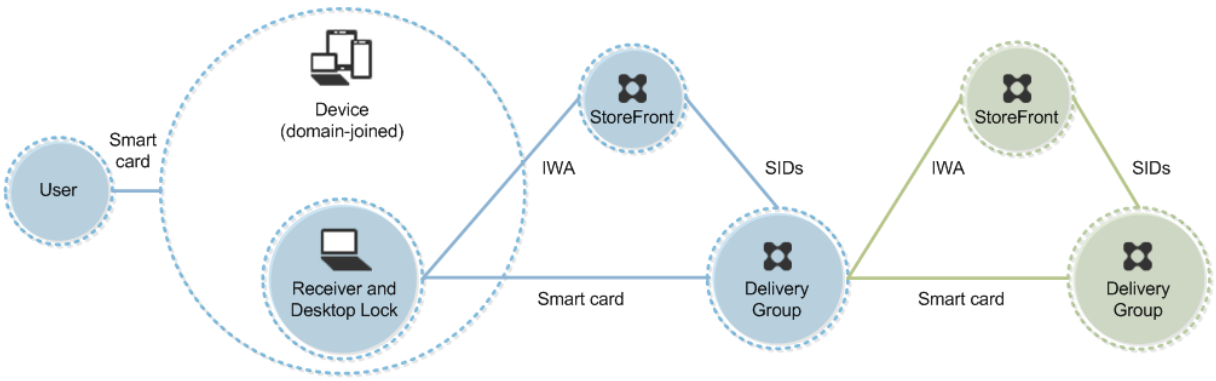
策略设置	桌面行为
无操作	无操作。
锁定工作站	桌面会话断开连接，并锁定虚拟桌面。
强制注销	将强制用户注销。如果网络连接已断开，并启用了此设置，则此会话可能会注销，用户可能会丢失数据。
如果是远程终端服务会话，则断开连接	会话断开连接，并锁定虚拟桌面。

证书吊销检查

如果启用证书吊销检查，并且用户将具有无效证书的智能卡插入读卡器，用户将无法对与该证书相关的桌面或应用程序进行身份验证或访问。例如，如果使用无效证书进行电子邮件解密，电子邮件将保持加密状态。如果卡上的其他证书（例如，用于身份验证的证书）仍有效，这些功能将仍有效。

部署示例：加入域的计算机

此部署涉及运行 Desktop Viewer 并直接连接到 StoreFront 的已加入域的用户设备。



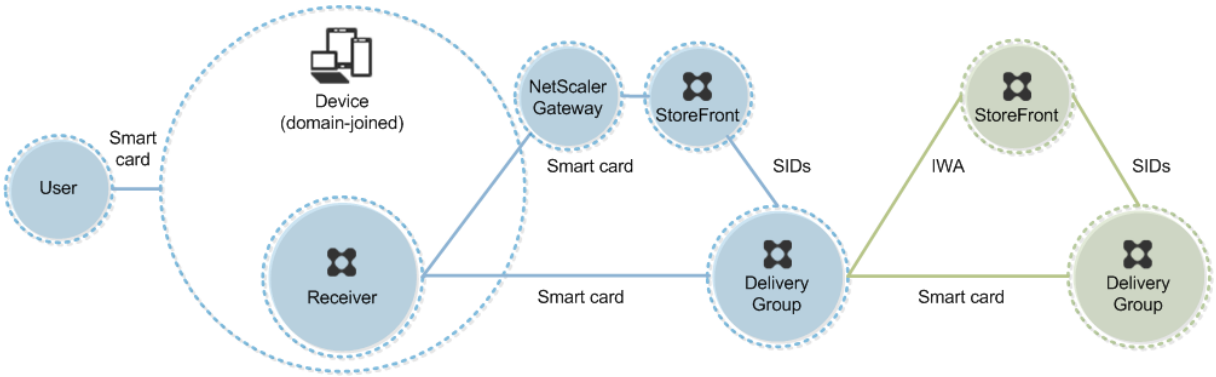
用户使用智能卡和 PIN 登录设备。Receiver 使用集成 Windows 身份验证 (IWA) 向 StoreFront 服务器进行用户身份验证。StoreFront 将用户安全标识符 (SID) 传递到 Citrix Virtual Apps 或 Citrix Virtual Desktops。当用户启动虚拟桌面或应用程序时，系统不会提示用户重新输入 PIN，因为 Receiver 上已配置单点登录功能。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。

部署示例：从加入域的计算机进行远程访问

此部署涉及运行 Desktop Viewer 并通过 Citrix Gateway/Access Gateway 连接到 StoreFront 的已加入域的用户设备。



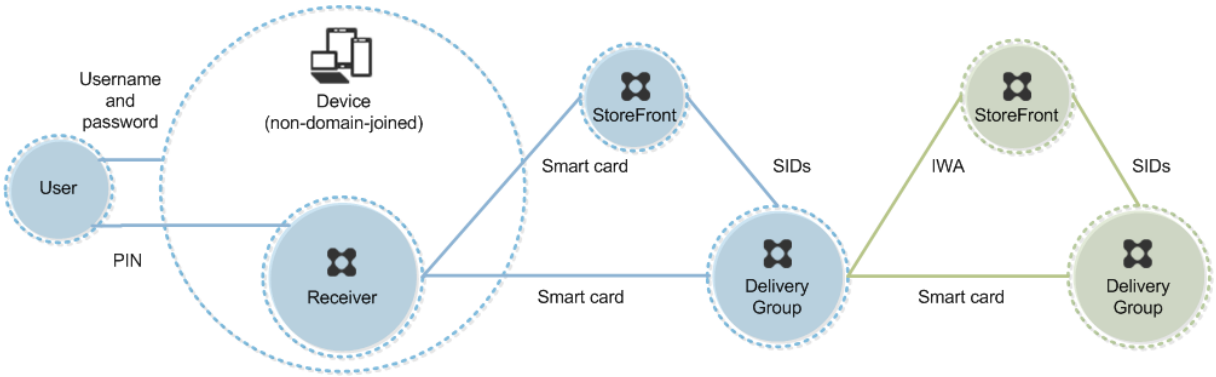
用户使用智能卡和 PIN 登录设备，然后重新登录 Citrix Gateway/Access Gateway。第二次登录可以使用智能卡和 PIN，也可以使用用户名和密码，因为在此部署中 Receiver 允许双模式身份验证。

用户将自动登录 StoreFront，将用户安全标识符 (SID) 传递到 Citrix Virtual Apps 或 Citrix Virtual Desktops。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。

部署示例：未加入域的计算机

此部署涉及运行 Desktop Viewer 并直接连接到 StoreFront 的未加入域的用户设备。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

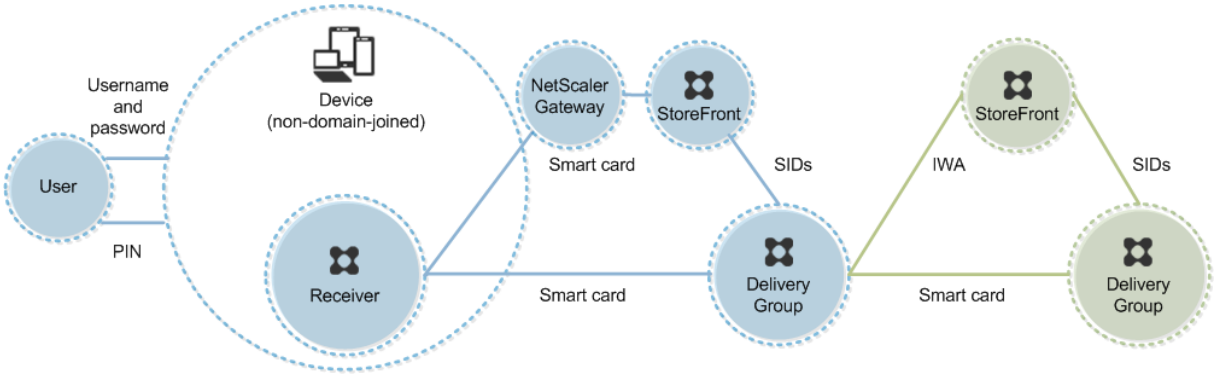
用户登录设备。通常情况下，用户需要输入用户名和密码，但由于此设备未加入域，因此此登录的凭据是可选的。因为在此部署中可使用双模式身份验证，因此 Receiver 会提示用户输入智能卡和 PIN，或使用用户名和密码。然后 Receiver 对 StoreFront 进行身份验证。

StoreFront 将用户安全标识符 (SID) 传递到 Citrix Virtual Apps 或 Citrix Virtual Desktops。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 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。

部署示例：从未加入域的计算机进行远程访问

此部署涉及运行 Desktop Viewer 并直接连接到 StoreFront 的未加入域的用户设备。



用户登录设备。通常情况下，用户需要输入用户名和密码，但由于此设备未加入域，因此此登录的凭据是可选的。因为在此部署中可使用双模式身份验证，因此 Receiver 会提示用户输入智能卡和 PIN，或使用用户名和密码。然后 Receiver 对 StoreFront 进行身份验证。

StoreFront 将用户安全标识符 (SID) 传递到 Citrix Virtual Apps 或 Citrix Virtual Desktops。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。

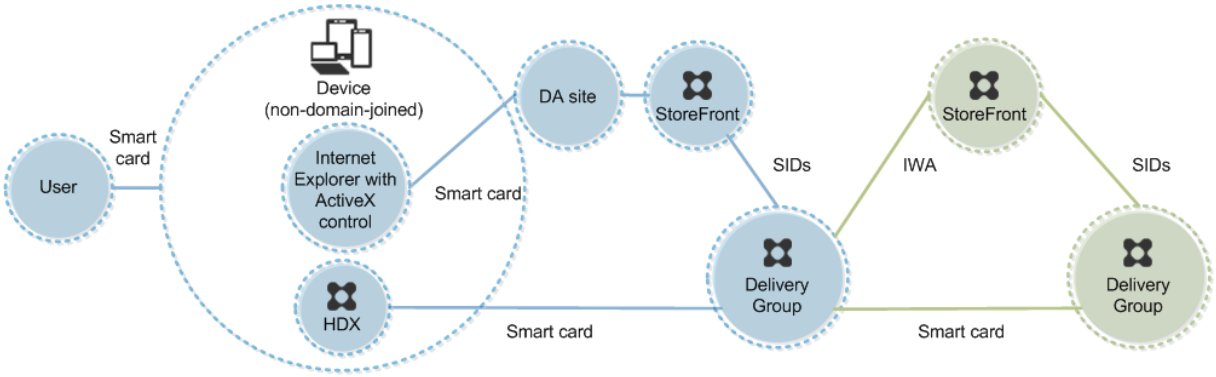
通过添加第二台 StoreFront 服务器和托管应用程序的服务器，此部署可以扩展到双跳。虚拟桌面的 Receiverd 对第二台 StoreFront 服务器进行身份验证。第二次连接时，可以使用任何身份验证方法。第一个跃点显示的配置可在第二个跃点中重新使用，或仅能在第二个跃点中使用。

部署示例：未加入域的计算机和瘦客户端访问桌面设备站点

此部署涉及运行 Desktop Lock，并通过桌面设备站点连接到 StoreFront 的未加入域的用户设备。

Desktop Lock 是随 Citrix Virtual Apps、Citrix Virtual Desktops 和 VDI-in-a-Box 发布的独立组件。它是 Desktop Viewer 的替代项，主要是针对重新设计用途的 Windows 计算机和 Windows 瘦客户端而设计的。Desktop Lock 取代了这些用户设备中的 Windows shell 和任务管理器，以阻止用户访问基础设备。通过使用 Desktop Lock，用户可以访问 Windows Server 计算机桌面和 Windows 桌面计算机桌面。可以选择安装 Desktop Lock。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



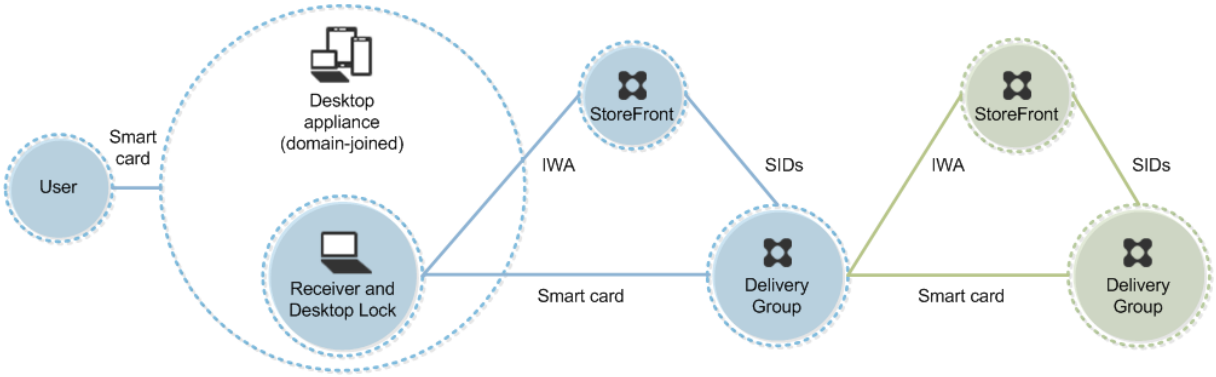
用户使用智能卡登录设备。如果 Desktop Lock 正在设备上运行，该设备配置为通过在 Kiosk 模式下运行的 Internet Explorer 启动桌面设备站点。该站点上的 ActiveX 控件会提示用户输入 PIN，然后将其发送到 StoreFront。StoreFront 将用户安全标识符 (SID) 传递到 Citrix Virtual Apps 或 Citrix Virtual Desktops。分配的桌面组列表（按字母顺序）中的第一个可用桌面将启动。

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。

部署示例：加入域的计算机和瘦客户端通过 **XenApp Services URL** 访问 **StoreFront**

此部署涉及运行 Desktop Lock，并通过 XenApp Services URL 连接到 StoreFront 的加入域的用户设备。

Desktop Lock 是随 Citrix Virtual Apps、Citrix Virtual Desktops 和 VDI-in-a-Box 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 Citrix Virtual Apps 或 Citrix Virtual Desktops。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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

November 17, 2021

直通身份验证

运行 Windows 10、Windows 8 和 Windows 7 SP1 Enterprise Edition 和 Professional Edition 的用户设备支持使用智能卡对虚拟桌面进行直通身份验证。

运行 Windows Server 2016、Windows Server 2012 R2、Windows Server 2012 和 Windows Server 2008 R2 SP1 的服务器支持使用智能卡对托管应用程序进行直通身份验证。

要使用智能卡对托管应用程序进行直通身份验证，请确保在配置使用智能卡进行直通身份验证作为站点的身份验证方法时启用 Kerberos。

注意：使用智能卡进行直通身份验证的可用性取决于许多因素，包括但不限于以下因素：

- 贵组织关于直通身份验证的安全策略。
- 中间件类型和配置。
- 智能卡读卡器类型。
- 中间件 PIN 缓存策略。

Citrix StoreFront 上已配置使用智能卡进行直通身份验证。有关详细信息，请参阅 StoreFront 文档。

单点登录

单点登录是一项 Citrix 功能，用于实现对虚拟桌面和应用程序启动的直通身份验证。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 Citrix 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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 Virtual Delivery Agent (VDA)，则会显示一个 Windows 磁贴，表示以前的成功身份验证模式，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)

January 21, 2022

Citrix Virtual Apps and Desktops 支持对组件之间基于 TCP 的连接使用传输层安全性 (TLS) 协议。Citrix Virtual Apps and Desktops 还可通过使用自适应传输，支持对基于 UDP 的 ICA/HDX 连接使用数据报传输层安全性 (DTLS) 协议。

TLS 和 DTLS 相似，并且都支持相同的数字证书。将 Citrix Virtual Apps 或 Citrix Virtual Desktops 站点配置为使用 TLS 也会将其配置为使用 DTLS。过程如下；除非另有说明，否则，这些步骤对于 TLS 和 DTLS 是通用的：

- 获取服务器证书并在所有 Delivery Controller 上安装和注册，并使用 TLS 证书配置端口。有关详细信息，请参阅在 Controller 上安装 TLS 服务器证书。

  （可选）可以更改 Controller 用于侦听 HTTP 和 HTTPS 流量的端口。

- 通过完成以下任务在 Citrix Workspace 应用程序和 Virtual Delivery Agent (VDA) 之间启用 TLS 连接：

  - 在安装 VDA 的计算机上配置 TLS。（为方便起见，后面将安装了 VDA 的计算机简称为 VDA。）有关常规信息，请参阅 VDA 上的 TLS 设置。强烈建议使用 Citrix 提供的 PowerShell 脚本来配置 TLS/DTLS。有关详细信息，请参阅使用 PowerShell 脚本在 VDA 上配置 TLS。但是，如果要手动配置 TLS/DTLS，请参阅在 VDA 上手动配置 TLS。
  - 通过在 Studio 中运行一组 PowerShell cmdlet，在包含 VDA 的交付组中配置 TLS。有关详细信息，请参阅在交付组上配置 TLS。

    要求和注意事项：

    * 在用户和 VDA 之间启用 TLS 连接仅对 XenApp 7.6 和 XenDesktop 7.6 及后续受支持的版本有效。
    * 在安装组件、创建站点、创建计算机目录和创建交付组之后，在交付组中和 VDA 上配置 TLS。
    * 要在交付组中配置 TLS，必须具有更改 Controller 访问规则的权限。完全权限管理员具有此权限。
    * 要在 VDA 上配置 TLS，必须是安装 VDA 的计算机上的 Windows 管理员。
    * 在通过 Machine Creation Services 或 Provisioning Services 置备的池 VDA 中，VDA 计算机映像会在重新启动时重置，从而导致以前的 TLS 设置丢失。请在每次重新启动 VDA 后运行 PowerShell 脚本以重新配置 TLS 设置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 警告：
>
> 有关涉及在 Windows 注册表中操作的任务 - 注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

有关为站点数据库启用 TLS 的信息，请参阅 CTX137556。

在 **Controller** 上安装 **TLS** 服务器证书

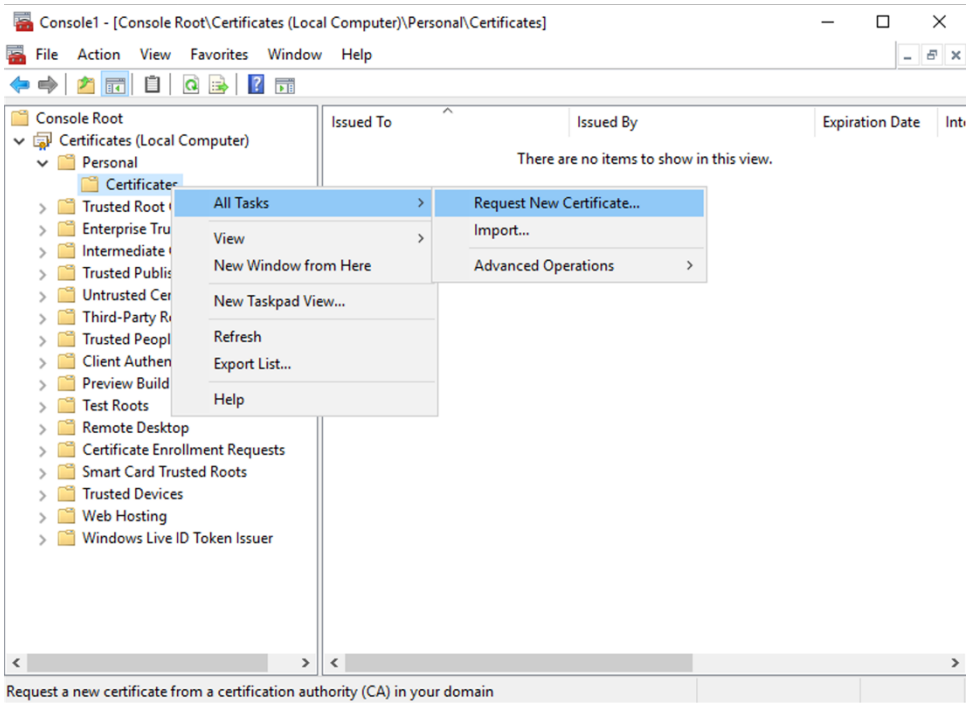
对于 HTTPS，XML Service 通过使用服务器证书而非客户端证书来支持 TLS 功能。本部分内容介绍如何在 Delivery Controller 中获取和安装 TLS 证书。同样的步骤可以应用到 Cloud Connector 以加密 STA 和 XML 流量。

有各种不同类型的证书颁发机构以及从这些机构请求证书的方法，本文介绍了 Microsoft 证书颁发机构。Microsoft 证书颁发机构需要发布证书模板以便进行服务器身份验证。

如果 Microsoft 证书颁发机构集成到 Active Directory 域或 Delivery Controller 加入到的可信林中，则可以从证书 MMC 管理单元证书注册向导获取证书。

请求和安装证书

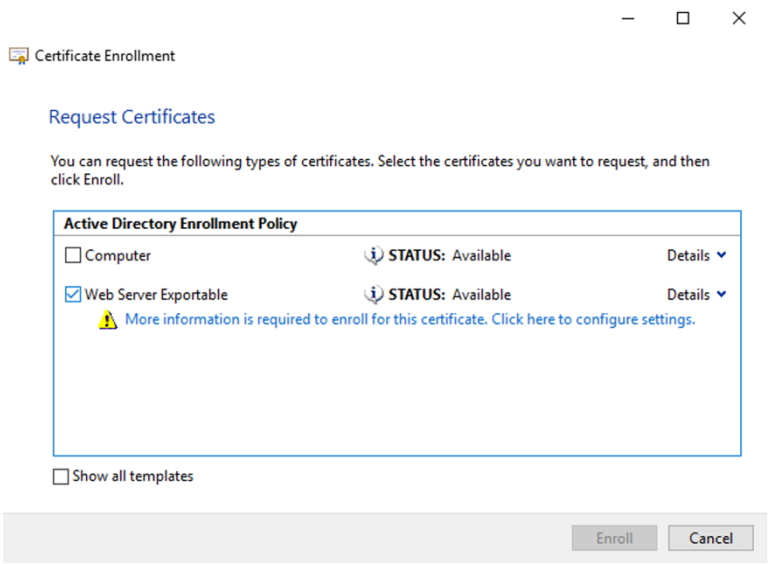
1. 在 Delivery Controller 上，打开 MMC 控制台并添加“证书”管理单元。出现提示时，选择“计算机帐户”。
2. 展开个人 **>** 证书，然后使用所有任务 **>** 申请新证书上下文菜单命令。



3. 单击下一步开始，然后单击下一步以确认您正在从 Active Directory 注册中获取证书。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

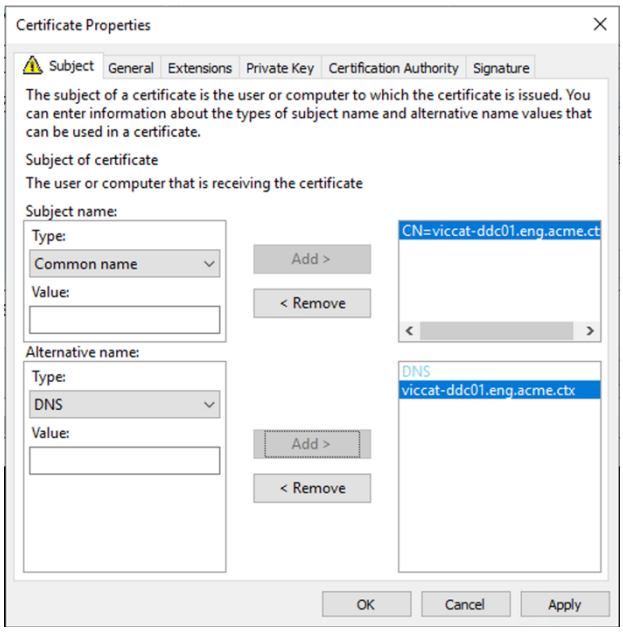
4. 选择服务器身份验证证书的模板。如果模板已设置为自动提供“使用者”的值，您可以单击注册，而不提供更多详细信息。



5. 要提供证书模板的更多详细信息，请单击详细信息箭头按钮并配置以下设置：

   使用者名称：选择公用名并添加 Delivery Controller 的 FQDN。

   备用名称：选择 DNS 并添加 Delivery Controller 的 FQDN。



配置 **SSL/TLS** 侦听器端口

1. 以计算机管理员身份打开 PowerShell 命令窗口。
2. 运行以下命令以获取 Broker Service 应用程序 GUID：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
New-PSDrive -Name HKCR -PSProvider Registry -Root
    HKEY_CLASSES_ROOT

$Service_Guid = Get-ChildItem HKCR:\Installer\Products -Recurse -
    Ea 0 | Where-Object {
  $key = $\_; $\_.GetValueNames() | ForEach-Object {
  $key.GetValue($\_)  }
  | Where-Object {
  $\_ -like 'Citrix Broker Service'  }
   }
  | Select-Object Name

$Service_Guid.Name -match "[A-Z0-9]*$"

$Guid = $Matches[0]

[GUID]$Formatted_Guid = $Guid

Remove-PSDrive -Name HKCR

Write-Host "Broker Service Application GUID: $($Formatted_Guid)" -
    ForegroundColor Yellow
<!--NeedCopy-->
```

3. 在同一 PowerShell 窗口中运行以下命令以获取之前安装的证书的指纹：

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

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-
    Object {
 $_.Subject -match ("CN=" + $HostName) }
 ).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $($HostName): $(
    $Thumbprint)" -Foreground Yellow
<!--NeedCopy-->
```

4. 在同一 PowerShell 窗口中运行以下命令，以配置 Broker Service SSL/TLS 端口并使用证书进行加密：

```
$IPV4_Address = Test-Connection -ComputerName $HostName -Count 1
    | Select-Object -ExpandProperty IPV4Address

$IPPort = "$($IPV4_Address):443"

$SSLxml = "http add sslcert ipport=$IPPort certhash=$Thumbprint
    appid={
 $Formatted_Guid }
 "

$SSLxml | netsh

. netsh http show sslcert
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

正确配置后，最后一个命令 `.netsh http show sslcert` 的输出显示监听器正在使用正确的 `IP:port`，并且 `Application ID` 与 Broker Service 应用程序 GUID 匹配。

如果服务器信任 Delivery Controller 上安装的证书，您现在可以将 StoreFront Delivery Controller 和 Citrix Gateway STA 绑定配置为使用 HTTPS 而非 HTTP。

> 注意：
>
> 如果在 Windows Server 2016 上安装了 Controller，同时在 Windows Server 2012 R2 上安装了 StoreFront，则需要对该 Controller 进行配置更改，以更改 TLS 密码套件的顺序。具有其他 Windows Server 版本组合的 Controller 和 StoreFront 不需要此配置更改。

密码套件顺序列表必须包括 `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` 或 `TLS_ECDHE_RSA_WITH_AES_` 密码套件（或两者）；并且这些密码套件必须位于任何 `TLS_DHE_` 密码套件之前。

1. 使用 Microsoft 组策略编辑器，浏览至计算机配置 **>** 管理模板 **>** 网络 **> SSL** 配置设置。
2. 编辑策略“SSL 密码套件顺序”。默认情况下，此策略设置为“未配置”。将此策略设置为已启用。
3. 按正确的顺序安排套件，删除任何不需要使用的密码套件。

确保 `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` 或 `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` 位于任何 `TLS_DHE_` 密码套件之前。

在 Microsoft MSDN 上，另请参阅 Prioritizing Schannel Cipher Suites（Schannel 密码套件优先级划分）。

更改 HTTP 或 HTTPS 端口

默认情况下，Controller 上的 XML Service 在端口 80 上侦听 HTTP 流量，在端口 443 上侦听 HTTPS 流量。尽管可以使用非默认端口，但请注意：将 Controller 暴露在不受信任的网络上存在安全风险。部署独立 StoreFront 服务器比更改默认值更可取。

要更改 Controller 使用的默认 HTTP 或 HTTPS 端口，请从 Studio 运行以下命令：

```
BrokerService.exe -WIPORT \<http-port> -WISSLPORT \<https-port>
```

其中，`<http-port>` 是用于 HTTP 流量的端口号，`<https-port>` 是用于 HTTPS 流量的端口号。

> 注意：
>
> 更改端口后，Studio 可能会显示关于许可证兼容性和升级的消息。要解决此问题，请使用以下 PowerShell cmdlet 序列重新注册服务实例：

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding
    XML_HTTPS |
Unregister-ConfigRegisteredServiceInstance
Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |
Register-ConfigServiceInstance
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

仅会强制执行 **HTTPS** 流量

如果希望 XML Service 忽略默认端口上的 HTTP 流量，请在 Controller 上的 HKLM\Software\Citrix\DesktopServer\ 中创建以下注册表设置，然后重新启动 Broker Service。

要忽略 HTTP 流量，请创建 DWORD XmlServicesEnableNonSsl 并将其设置为 0。

提供了一个能够创建的用于忽略 HTTPS 流量的相应注册表 DWORD 值：DWORD XmlServicesEnableSsl。请确保未将其设置为 0。

VDA 上的 **TLS** 设置

交付组不能既包含已配置 TLS 的 VDA 又包含未配置 TLS 的 VDA。为交付组配置 TLS 时，确保已经为该交付组中的所有 VDA 配置 TLS

在 VDA 上配置 TLS 时，已安装 TLS 证书上的权限会被更改，向 ICA Service 授予读取证书私钥的权限，并向 ICA Service 告知以下信息：

- 证书存储中用于 **TLS** 的证书。
- 用于 **TLS** 连接的 **TCP** 端口号。

  必须将 Windows 防火墙（如果启用）配置为允许此 TCP 端口上的传入连接。使用 PowerShell 脚本时会完成此配置。
- 允许哪些版本的 **TLS** 协议。

  > 重要：
  >
  > Citrix 建议您查看您的 SSLv3 使用情况，并在适当的情况下重新配置那些部署以删除对 SSLv3 的支持。请参阅 CTX200238。

  支持的 TLS 协议版本遵循以下层次结构（从最低到最高）：SSL 3.0、TLS 1.0、TLS 1.1 和 TLS 1.2。指定允许的最低版本；将允许使用此版本或更高版本的所有协议连接。

  例如，如果指定 TLS 1.1 作为最低版本，则允许 TLS 1.1 和 TLS 1.2 协议连接。如果指定 SSL 3.0 作为最低版本，则允许所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。

  DTLS 1.0 对应于 TLS 1.1，DTLS 1.2 对应于 TLS 1.2。
- 允许哪些 **TLS** 密码套件。

  密码套件选择用于连接的加密。客户端和 VDA 可以支持不同的密码套件组。客户端（Citrix Workspace 应用程序或 StoreFront）连接并发送支持的 TLS 密码套件列表，VDA 将客户端的密码套件之一与其自己的配置密码套件列表中的密码套件之一进行匹配，并接受连接。如果没有匹配的密码套件，VDA 将拒绝连接。

  VDA 支持三组密码套件（也称为合规性模式）：GOV(ernment)、COM(mercial) 及 ALL。可接受的密码套件还取决于 Windows FIPS 模式；有关 Windows FIPS 模式的信息，请参阅 http://support.microsoft.com/kb/811833。下表列出了每组中的密码套件：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

TLS/DTLS 密码套件	ALL	COM	GOV	ALL	COM	GOV
FIPS 模式	关	关	关	开	开	开
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*	X			X		X
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	X			X		X
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	X			X	X	

* 在 Windows Server 2012 R2 中不受支持。

> 注意：
>
> VDA 不支持 DHE 密码套件(例如 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384、TLS_DHE_RSA_WITH_AES_256_CBC
> TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 和 TLS_DHE_RSA_WITH_AES_128_CBC_SHA)。如果 Windows 选择了这些密码套件，Receiver 可能不会使用。
>
> 如果您使用的是 Citrix Gateway，请参阅 Citrix ADC 文档，以了解有关后端通信的密码套件支持信息。有关 TLS 密码套件支持的信息，请参阅 Citrix ADC 设备上可用的密码。有关 DTLS 密码套件支持的信息，请参阅 DTLS 密码支持。

使用 **PowerShell** 脚本在 **VDA** 上配置 **TLS**

在证书存储的本地计算机 > 个人 > 证书区域中安装 TLS 证书。如果该位置有多个证书，请向 PowerShell 脚本提供证书的指纹。

> 注意：
>
> 自 XenApp 和 XenDesktop 7.16 LTSR 起，PowerShell 脚本会根据 VDA 的 FQDN 查找正确的证书。如果该 VDA FQDN 只有一个证书，则不需要提供指纹。

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* > *Tools* > *SslSupport* 文件夹中。

启用了 TLS 时，将禁用 DHE 密码套件。ECDHE 密码套件不受影响。

如果启用 TLS，则该脚本会对指定的 TCP 端口禁用所有现有 Windows 防火墙规则。然后添加一个新规则，允许 ICA Service 只接受 TLS TCP 和 UDP 端口上的传入连接。它还对以下各项禁用 Windows 防火墙规则：

- Citrix ICA（默认：1494）
- Citrix CGP（默认：2598）
- Citrix WebSocket（默认：8008）

其结果是，用户只能使用 TLS 或 DTLS 进行连接。如果不使用 TLS 或 DTLS，则他们不能使用 ICA/HDX、已启用会话可靠性的 ICA/HDX 或采用 WebSocket 的 HDX。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 通过 UDP 协议的 ICA/HDX 音频实时传输或 ICA/HDX Framehawk 不支持 DTLS。

请参阅网络端口。

此脚本包含以下语法描述以及额外的示例；可以使用 Notepad++ 等工具查看此信息。

> 重要：
>
> 指定 Enable 或 Disable 参数以及 CertificateThumbPrint 参数。其他参数为可选参数。

语　法　`Enable-VdaSSL { -Enable | -Disable } -CertificateThumbPrint "<thumbprint>"[-SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite"\<suite>"]`

参数	说明
启用	在 VDA 上安装并启用 TLS 侦听器。此参数或 Disable 参数为必需参数。
禁用	在 VDA 上禁用 TLS 侦听器。此参数或 Enable 参数为必需参数。如果指定此参数，其他参数均无效。
CertificateThumbPrint “”	证书存储中 TLS 证书的指纹，两边用引号引起。脚本使用指定的指纹来选择要使用的证书。如果忽略此参数，则会选择错误的证书。
SSLPort	TLS 端口。默认值：443
SSLMinVersion “”	最低 TLS 协议版本，两边用引号引起。有效值：“TLS_1.0”（默认值）、“TLS_1.1”和“TLS_1.2”。
SSLCipherSuite “”	TLS 密码套件，两边用引号引起。有效值：”GOV”、”COM”和“ALL”（默认值）。

示例　以下脚本安装并启用 TLS 协议版本值。指纹（在此示例中以 12345678987654321 表示）用于选择要使用的证书。

```
Enable-VdaSSL -Enable -CertificateThumbPrint "12345678987654321"
```

以下脚本安装并启用 TLS 侦听器，指定 TLS 端口 400、GOV 密码套件和最低 TLS 1.2 协议值。指纹（在此示例中以 12345678987654321 表示）用于选择要使用的证书。

```
Enable-VdaSSL -Enable
-CertificateThumbPrint "12345678987654321"
-SSLPort 400 -SSLMinVersion "TLS_1.2"
-SSLCipherSuite "All"
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

以下脚本在 VDA 上禁用 TLS 侦听器。

```
Enable-VdaSSL -Disable
```

在 **VDA** 上手动配置 **TLS**

在 VDA 上手动配置 TLS 时，可以向各个 VDA 上的相应服务授予对 TLS 证书私钥的一般读取权限：NT SERVICE\PorticaService（适用于 Windows 单会话操作系统的 VDA）或者 NT SERVICE\TermService（适用于 Windows 多会话操作系统的 VDA）。在安装 VDA 的计算机上：

步骤 **1.** 启动 Microsoft 管理控制台 (MMC)：“开始”>“运行”> mmc.exe。

步骤 **2.** 将证书管理单元添加到 MMC：

1. 选择文件 > 添加/删除管理单元。
2. 选择证书，然后单击添加。
3. 收到“该管理单元将始终为下列帐户管理证书:”提示时，选择“计算机帐户”，然后单击“下一步”。
4. 收到“请选择需要这个管理单元管理的计算机”提示时，选择“本地计算机”，然后单击“完成”。

步骤 **3.** 在证书 (本地计算机) > 个人 > 证书下，在证书上单击鼠标右键，然后选择所有任务 > 管理私钥。

步骤 **4.** 访问控制列表编辑器显示“(友好名称) 私钥的权限”，其中，(友好名称) 是 TLS 证书的名称。添加以下其中一项服务并向其授予读取权限：

- 对于适用于 Windows 单会话操作系统的 VDA，“PORTICASERVICE”
- 对于适用于 Windows 多会话操作系统的 VDA，“TERMSERVICE”

步骤 **5.** 双击已安装的 TLS 证书。在证书对话框中，选择详细信息选项卡，然后滚动到底部。单击指纹。

步骤 **6.** 运行 regedit 并转至 HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd。

1. 编辑 SSL 指纹注册表项并将 TLS 证书的指纹值复制到此二进制值中。可以忽略编辑二进制值对话框中的未知项（如‘0000’和特殊字符），这样是安全的。
2. 编辑 SSLEnabled 注册表项并将 DWORD 值更改为 1。（之后要禁用 SSL，请将 DWORD 值更改为 0。）
3. 如果要更改默认设置（可选），请在相同注册表路径中使用以下值：

   SSLPort DWORD –SSL 端口号。默认值：443。

   SSLMinVersion DWORD –1 = SSL 3.0、2 = TLS 1.0、3 = TLS 1.1、4 = TLS 1.2。默认值：2 (TLS 1.0)。

   SSLCipherSuite DWORD –1 = GOV、2 = COM、3 = ALL。默认值：3 (ALL)。

步骤 **7.** 如果 TLS TCP 和 UDP 端口不是默认值 443，请确保这些端口在 Windows 防火墙中处于打开状态。（在 Windows 防火墙中创建入站规则时，请确保其属性已选中“允许连接”或“启用”条目）。

步骤 **8.** 确保没有其他应用程序或服务（如 IIS）正在使用 TLS TCP 端口。

步骤 **9.** 对于适用于 Windows 多会话操作系统的 VDA，请重新启动计算机以使更改生效。（无需重新启动包含适用于 Windows 单会话操作系统的 VDA 的计算机）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 重要：
>
> VDA 在 Windows Server 2012 R2、Windows Server 2016 或者 Windows 10 Anniversary Edition 或支持的更高版本上时，需要执行额外的步骤。此影响来自 Citrix Receiver for Windows（版本 4.6 到 4.9）、适用于 HTML5 的 Citrix Workspace 应用程序以及适用于 Chrome 的 Citrix Workspace 应用程序的连接。其中也包括使用 Citrix Gateway 的连接。
>
> 对于使用 Citrix Gateway 的所有连接以及所有 VDA 版本（如果在 Citrix Gateway 与 VDA 之间配置了 TLS），也需要执行此步骤。这影响所有 Citrix Receiver 版本。

在 VDA（Windows Server 2012 R2、Windows Server 2016、Windows 10 Anniversary Edition 或更高版本）上，使用组策略编辑器，转到“计算机配置”>“策略”>“管理模板”>“网络”>“SSL 配置设置”>“SSL 密码套件顺序”。选择以下顺序：

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

> 注意：
>
> 前六项还指定椭圆曲线 P384 或 P256。请确保未选择 “curve25519”。FIPS 模式不会阻止使用 “curve25519”。

配置了此组策略设置时，VDA 将仅选择同时显示在两个列表中的密码套件：组策略列表和选定合规性模式列表（COM、GOV 或 ALL）。该密码套件还必须显示在客户端（Citrix Workspace 应用程序或 StoreFront）发送的列表中。

此组策略配置还会影响 VDA 上的其他 TLS 应用程序和服务。如果您的应用程序要求使用特定的密码套件，您可能需要将它们添加到此组策略列表中。

> 重要：
>
> 尽管组策略更改一旦应用便会显示，但对 TLS 配置的组策略更改只有在重新启动操作系统后才会生效。因此，对于池桌面，请将对 TLS 配置的组策略更改应用于基础映像。

在交付组上配置 **TLS**

为包含已配置 TLS 连接的 VDA 的每个交付组完成此过程。

1. 从 Studio，打开 PowerShell 控制台。
2. 运行 **asnp Citrix.*** 以加载 Citrix 产品 cmdlet。
3. 运行 **Get-BrokerAccessPolicyRule -DesktopGroupName ‘*<delivery-group-name>*’ | Set-BrokerAccessPolicyRule -HdxSslEnabled $true**。
4. 运行 **Set-BrokerSite -DnsResolutionEnabled $true**。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

故障排除

如果出现连接错误，请检查 VDA 上的系统事件日志。

使用适用于 Windows 的 Citrix Workspace 应用程序时，如果收到指示 TLS 错误的连接错误，请禁用 Desktop Viewer，然后重新尝试连接。尽管连接仍失败，但可能会提供基本 TLS 问题的解释。例如，您在从证书颁发机构申请证书时指定了错误的模板。

大多数使用 HDX 自适应传输的配置在使用 DTLS 时能够成功运行，包括使用最新版本的 Citrix Workspace 应用程序、Citrix Gateway 和 VDA 的配置。某些在 Citrix Workspace 应用程序与 Citrix Gateway 之间使用 DTLS 的配置以及在 Citrix Gateway 与 VDA 之间使用 DTLS 的配置都需要额外的操作。

在以下情况下需要额外的操作：

- Citrix Receiver 版本支持 HDX 自适应传输和 DTLS：Receiver for Windows（4.7、4.8、4.9）、Receiver for Mac（12.5、12.6、12.7）、Receiver for iOS（7.2、7.3.x）或 Receiver for Linux (13.7)

并且以下任一情况也适用：

- Citrix Gateway 版本支持通过 DTLS 传输到 VDA，但 VDA 版本不支持 DTLS（版本 7.15 或更低版本），
- VDA 版本支持 DTLS（版本 7.16 或更高版本），但 Citrix Gateway 版本不支持通过 DTLS 传输到 VDA。

要避免来自 Citrix Receiver 的连接失败，请执行以下操作之一：

- 将 Citrix Receiver 更新到 Receiver for Windows 4.10 或更高版本、Receiver for Mac 12.8 或更高版本或者 Receiver for iOS 7.5 或更高版本；或
- 将 Citrix Gateway 更新到支持通过 DTLS 传输到 VDA 的版本；或
- 将 VDA 更新到版本 7.16 或更高版本；或
- 在 VDA 上禁用 DTLS；或
- 禁用 HDX 自适应传输。

> 注意：
>
> 适用于 Receiver for Linux 的更新尚未提供。Receiver for Android（版本 3.12.3）不支持 HDX 自适应传输以及通过 Citrix Gateway 的 DTLS，因此不受影响。
>
> 要在 VDA 上禁用 DTLS，请将 VDA 防火墙配置修改为禁用 UDP 端口 443。请参阅网络端口。

Controller 与 VDA 之间的通信

Windows Communication Framework (WCF) 消息级保护会保护 Controller 与 VDA 之间的通信。不需要进行使用 TLS 的额外传输层保护。WCF 配置使用 Kerberos 在 Controller 与 VDA 之间进行相互身份验证。加密使用处于 CBC 模式的带 256 位密钥的 AES。消息完整性使用 SHA-1。

根据 Microsoft，WCF 所使用的安全协议符合 OASIS（结构化信息标准促进组织）标准，包括 WS-SecurityPolicy 1.2。此外，Microsoft 还申明，WCF 支持安全策略 1.2 中列出的所有算法套件。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Controller 和 VDA 间的通信使用 basic256 算法套件，该套件的算法如上所述。

TLS 和 **HTML5** 视频重定向以及浏览器内容重定向

可以使用 HTML5 视频重定向和浏览器内容重定向来重定向 HTTPS Web 站点。注入到这些 Web 站点的 JavaScript 必须与 VDA 上运行的 Citrix HDX HTML5 视频重定向服务建立 TLS 连接。为了实现此功能，HTML5 视频重定向服务将在 VDA 上的证书存储中生成两个自定义证书。停止此服务将删除证书。

HTML5 视频重定向策略默认处于禁用状态。

浏览器内容重定向默认处于启用状态。

有关 HTML5 视频重定向的详细信息，请参阅多媒体策略设置。

通用打印服务器上的传输层安全性 **(TLS)**

January 21, 2022

Virtual Delivery Agent (VDA) 与通用打印服务器之间的基于 TCP 的连接支持传输层安全性 (TLS) 协议。

> 警告：
>
> 有关涉及在 Windows 注册表中操作的任务 - 注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

VDA 与通用打印服务器之间的打印连接类型

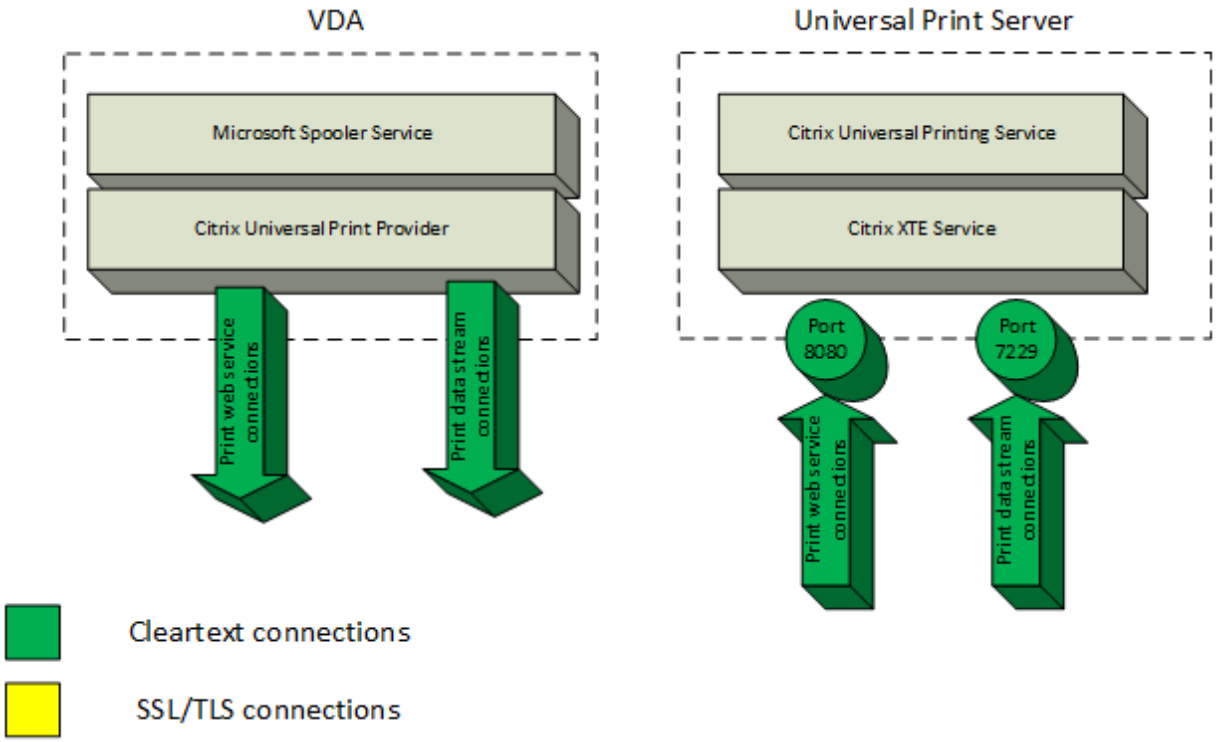
明文连接

以下与打印相关的连接来自 VDA，并连接到通用打印服务器上的端口。仅当 **SSL** 已启用策略设置设为已禁用（默认设置）时，才会建立这些连接。

- 明文打印 Web 服务连接（TCP 端口 8080）
- 明文打印数据流 (CGP) 连接（TCP 端口 7229）

Microsoft 支持文章 Windows 的服务概述和网络端口要求描述了 Microsoft Windows 打印后台处理程序服务使用的端口。本文档中的 SSL/TLS 设置不适用于 Windows 打印后台处理程序服务建立的 NETBIOS 和 RPC 连接。如果通用打印服务器启用策略设置设为已启用并回退到 **Windows** 的本机远程打印，VDA 将使用 Windows 网络打印提供程序 (win32spl.dll) 作为回退。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

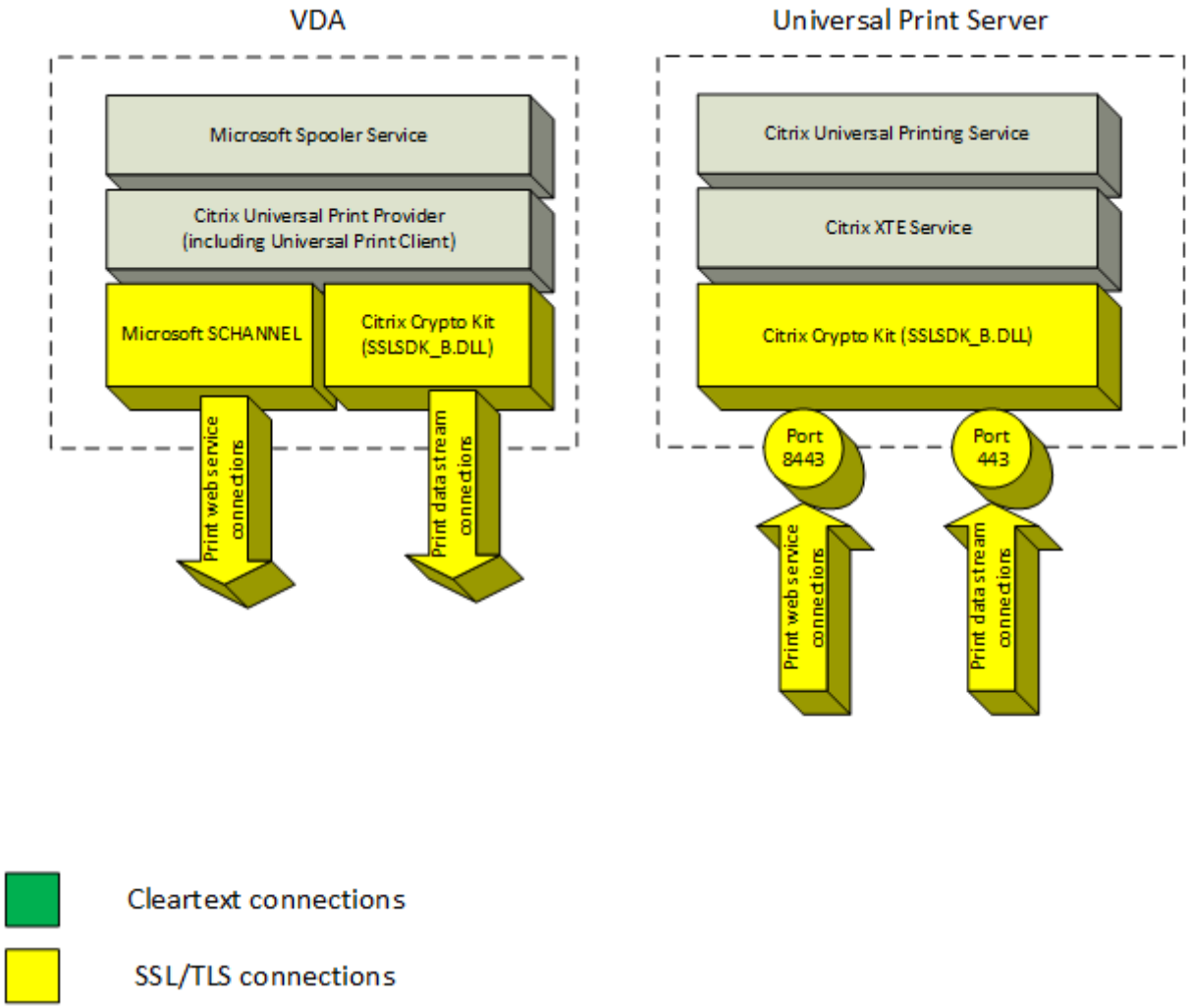


加密连接

这些与打印相关的连接来自 VDA，并连接到通用打印服务器上的端口。仅当 **SSL** 已启用策略设置设为已启用时，才会建立这些连接。

- 加密的打印 Web 服务连接（TCP 端口 8443）
- 加密的打印数据流 (CGP) 连接（TCP 端口 443）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



SSL/TLS 客户端配置

VDA 作为 SSL/TLS 客户端运行。

使用 Microsoft 组策略和注册表可配置用于加密的打印 Web 服务连接（TCP 端口 8443）的 Microsoft SCHANNEL SSP。Microsoft 支持文章 TLS 注册表设置描述了 Microsoft SCHANNEL SSP 的注册表设置。

在 VDA（Windows Server 2016 或 Windows 10）上，使用组策略编辑器转到计算机配置 **>** 管理模板 **>** 网络 **> SSL** 配置设置 **> SSL** 密码套件顺序。选择以下顺序：

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 配置此组策略设置后，仅当连接出现在两个 SSL 密码套件列表中时，VDA 才为加密的打印 Web 服务连接（默认端口：8443）选择密码套件：
>
> - 组策略 SSL 密码套件顺序列表
> - 与所选 SSL 密码套件策略设置（COM、GOV 或 ALL）对应的列表
>
> 此组策略配置还会影响 VDA 上的其他 TLS 应用程序和服务。如果您的应用程序要求使用特定的密码套件，可能需要将其添加到此组策略密码套件顺序列表中。
>
> 重要：
>
> 对 TLS 配置的组策略更改只有在重新启动操作系统后才会生效。
>
> 使用 Citrix 策略为加密的打印数据流 (CGP) 连接（TCP 端口 443）配置 SSL/TLS 设置。

SSL/TLS 服务器配置

通用打印服务器作为 SSL/TLS 服务器运行。

使用 `Enable-UpsSsl.ps1` PowerShell 脚本配置 SSL/TLS 设置。

在通用打印服务器上安装 **TLS** 服务器证书

对于 HTTPS，通用打印服务器通过使用服务器证书来支持 TLS 功能。不使用客户端证书。使用 Microsoft Active Directory 证书服务或其他证书颁发机构为通用打印服务器申请证书。

使用 Microsoft Active Directory 证书服务注册/申请证书时，请谨记以下注意事项：

1. 将证书放置在本地计算机个人证书存储中。
2. 将证书的使用者可分辨名称（使用者 DN）的公用名属性设置为通用打印服务器的完全限定域名 (FQDN)。请在证书模板中指定此设置。
3. 将用于生成证书请求和私钥的加密服务提供程序 (CSP) 设置为 **Microsoft** 增强型 **RSA** 和 **AES** 加密提供程序 **(**加密**)**。请在证书模板中指定此设置。
4. 将密钥大小至少设置为 2048 位。请在证书模板中指定此设置。

在通用打印服务器上配置 **SSL**

通用打印服务器上的 XTE 服务侦听传入连接。启用了 SSL 时，该服务器作为 SSL 服务器运行。传入连接有两种类型：打印 Web 服务连接（包含打印命令）和打印数据流连接（包含打印作业）。可以对这些连接启用 SSL。SSL 保护这些连接的保密性和完整性。默认情况下，SSL 处于禁用状态。

用于配置 SSL 的 PowerShell 脚本位于安装介质中，文件名如下：`\Support\Tools\SslSupport\Enable-UpsSsl.ps1`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

在通用打印服务器上配置侦听端口号

下面是 XTE 服务的默认端口：

- 明文打印 Web 服务 (HTTP) TCP 端口：8080
- 明文打印数据流 (CGP) 连接 TCP 端口：7229
- 加密的打印 Web 服务 (HTTPS) 连接 TCP 端口：8443
- 加密的打印数据流 (CGP) TCP 端口：443

要更改通用打印服务器上的 XTE 服务使用的端口，请以管理员身份在 PowerShell 中运行以下命令（请参阅后面的部分，以了解使用 Enable-UpsSsl.ps1 PowerShell 脚本的说明）：

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>` 或 `Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`
3. `Start-Service CitrixXTEServer`

通用打印服务器上的 **TLS** 设置

如果您在负载平衡的配置中有多个通用打印服务器，请确保在所有通用打印服务器上一致地配置 TLS 设置。

在通用打印服务器上配置 TLS 时，已安装 TLS 证书上的权限会被更改，向通用打印服务授予读取证书私钥的权限，并向通用打印服务告知以下信息：

- 证书存储中用于 TLS 的证书。
- 用于 TLS 连接的 TCP 端口号。

必须将 Windows 防火墙（如果启用）配置为允许这些 TCP 端口上的传入连接。使用 Enable-UpsSsl.ps1 PowerShell 脚本时会完成此配置。

- 允许哪些版本的 TLS 协议。

通用打印服务器支持 TLS 协议版本 1.2、1.1 和 1.0。指定允许的最低版本。

默认 TLS 协议版本为 1.2。

- 允许哪些 TLS 密码套件。

密码套件选择用于连接的加密算法。VDA 和通用打印服务器可以支持不同的密码套件组。VDA 连接并发送支持的 TLS 密码套件列表时，通用打印服务器将客户端的密码套件之一与其自己的配置密码套件列表中的密码套件之一进行匹配，并接受连接。如果没有匹配的密码套件，通用打印服务器将拒绝连接。

对于 OPEN、FIPS 和 SP800-52 本机加密套件模式，通用打印服务器支持以下名为 GOV(ernment)、COM(mercial) 和 ALL 的密码套件集。可接受的密码套件还取决于 **SSL FIPS** 模式策略设置和 Windows FIPS 模式。有关 Windows FIPS 模式的信息，请参阅此 Microsoft 支持文章。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

密码套件（按优先级降序排列）	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_AES256_GCM_SHA384			X	X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_SHA384			X	X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_SHA		X		X	X		X	X	

使用 **PowerShell** 脚本在通用打印服务器上配置 **TLS**

在证书存储的本地计算机 **>** 个人 **>** 证书区域中安装 TLS 证书。如果该位置有多个证书，请向 `Enable-UpsSsl.ps1` PowerShell 脚本提供证书的指纹。

> 注意：
>
> PowerShell 脚本根据通用打印服务器的 FQDN 查找正确的证书。仅当通用打印服务器 FQDN 只有一个证书时，您才不需要提供证书指纹。

`Enable-UpsSsl.ps1` 脚本启用或禁用从 VDA 到通用打印服务器的 TLS 连接。此脚本位于安装介质上的 **Support > Tools > SslSupport** 文件夹中。

如果启用 TLS，则该脚本会对通用打印服务器的 TCP 端口禁用所有现有 Windows 防火墙规则。然后添加新规则，这些规则允许 XTE 服务只接受 TLS TCP 和 UDP 端口上的传入连接。它还对以下各项禁用 Windows 防火墙规则：

- 明文打印 Web 服务连接（默认端口：8080）
- 明文打印数据流 (CGP) 连接（默认端口：7229）

其效果为，VDA 只能在使用 TLS 时建立这些连接。

> 注意：
>
> 启用 TLS 不会影响来自 VDA 并转至通用打印服务器的 Windows 打印后台处理程序 RPC/SMB 连接。
>
> 重要：
>
> 指定启用或禁用作为第一个参数。如果本地计算机个人证书存储中只有一个证书具有通用打印服务器的 FQDN，“证书指纹”参数将为可选参数。其他参数为可选参数。

语法

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
Enable-UpsSSL.ps1 -Enable [-HTTPPort <port>] [-CGPPort <port>] [-
    HTTPSPort <port>] [-CGPSSLPort <port>] [-SSLMinVersion <version>] [-
    SSLCipherSuite <name>] [-CertificateThumbprint <thumbprint>] [-
    FIPSMode <Boolean>] [-ComplianceMode <mode>]
Enable-UpsSSL.ps1 -Disable [-HTTPPort <portnum>] [-CGPPort <portnum>]
```

参数	说明
启用	在 XTE 服务器上启用 SSL/TLS。此参数或 Disable 参数为必需参数。
禁用	在 XTE 服务器上禁用 SSL/TLS。此参数或 Enable 参数为必需参数。
CertificateThumbprint "<thumbprint>"	本地计算机个人证书存储中 TLS 证书的指纹，两边用引号引起。脚本使用指定的指纹来选择要使用的证书。
HTTPPort <port>	明文打印 Web 服务 (HTTP/SOAP) 端口。默认值：8080
CGPPort <port>	明文打印数据流 (CGP) 端口默认值：7229
HTTPSPort <port>	加密的打印 Web 服务 (HTTPS/SOAP) 端口。默认值：8443
CGPSSLPort <port>	加密的打印数据流 (CGP) 端口。默认值：443
SSLMinVersion "<version>"	最低 TLS 协议版本，两边用引号引起。有效值：TLS_1.0、TLS_1.1 和 TLS_1.2。默认值：TLS_1.2。
SSLCipherSuite “<name>”	TLS 密码套件包的名称，两边用引号引起。有效值：GOV、COM 和 ALL（默认值）。
FIPSMode <Boolean>	在 XTE 服务器上启用或禁用 FIPS 140 模式。有效值：$true 将启用 FIPS 140 模式，$false 将禁用 FIPS 140 模式。

示例

以下脚本将启用 TLS。指纹（在此示例中以 12345678987654321 表示）用于选择要使用的证书。

```
Enable-UpsSsl.ps1 -Enable -CertificateThumbprint "12345678987654321"
```

以下脚本将禁用 TLS。

```
Enable-UpsSsl.ps1 -Disable
```

配置 **FIPS** 模式

启用美国联邦信息处理标准 (FIPS) 模式可确保仅将 FIPS 140 兼容的加密用于通用打印服务器加密的连接。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

在客户端配置 FIPS 模式之前，在服务器上配置 FIPS 模式。

请查询 Microsoft 的文档站点，了解有关启用/禁用 Windows FIPS 模式的信息。

在客户端上启用 **FIPS** 模式

在 Delivery Controller 上，运行 Citrix Studio，并将 **SSL FIPS** 模式 Citrix 策略设置设为已启用。启用 Citrix 策略。

请在每个 VDA 上执行以下操作：

1. 启用 Windows FIPS 模式。
2. 重新启动 VDA。

在服务器上启用 **FIPS** 模式

请在每个通用打印服务器上执行以下操作：

1. 启用 Windows FIPS 模式。
2. 以管理员身份运行此 PowerShell 命令：`stop-service CitrixXTEServer, UpSvc`
3. 运行带有 `-Enable -FIPSMode $true` 参数的 `Enable-UpsSsl.ps1` 脚本：
4. 重新启动通用打印服务器。

在客户端上禁用 **FIPS** 模式

在 Delivery Controller 上，运行 Citrix Studio，并将 **SSL FIPS** 模式 Citrix 策略设置设为已禁用。启用 Citrix 策略。还可以删除 **SSL FIPS** 模式 Citrix 策略设置。

请在每个 VDA 上执行以下操作：

1. 禁用 Windows FIPS 模式。
2. 重新启动 VDA。

在服务器上禁用 **FIPS** 模式

请在每个通用打印服务器上执行以下操作：

1. 禁用 Windows FIPS 模式。
2. 以管理员身份运行此 PowerShell 命令：`stop-service CitrixXTEServer, UpSvc`
3. 运行带有 `-Enable -FIPSMode $false` 参数的 `Enable-UpsSsl.ps1` 脚本：
4. 重新启动通用打印服务器。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

配置 **SSL/TLS** 协议版本

默认 SSL/TLS 协议版本为 TLS 1.2。TLS 1.2 是唯一推荐用于生产使用的 SSL/TLS 协议版本。为了进行故障排除，可能需要在非生产环境中临时更改 SSL/TLS 协议版本。

通用打印服务器不支持 SSL 2.0 和 SSL 3.0。

在服务器上设置 **SSL/TLS** 协议版本

请在每个通用打印服务器上执行以下操作：

1. 以管理员身份运行此 PowerShell 命令：`stop-service CitrixXTEServer, UpSvc`
2. 运行带有 `-Enable -SSLMinVersion` 版本参数的 `Enable-UpsSsl.ps1` 脚本。请记住在完成测试后将其设置回 TLS 1.2。
3. 重新启动通用打印服务器。

在客户端上设置 **SSL/TLS** 协议版本

请在每个 VDA 上执行以下操作：

1. 在 Delivery Controller 上，将 **SSL** 协议版本策略设置设为所需的协议版本，并启用该策略。
2. Microsoft 支持文章 TLS 注册表设置描述了 Microsoft SCHANNEL SSP 的注册表设置。使用注册表设置启用客户端 **TLS 1.0**、**TLS 1.1** 或 **TLS 1.2**。

   > 重要：
   >
   > 请谨记在完成测试后将注册表设置还原为原始值。

3. 重新启动 VDA。

故障排除

如果出现连接错误，请检查通用打印服务器上的 C:\Program Files (x86)\Citrix\XTE\logs\error.log 日志文件。

如果 SSL/TLS 握手失败，此日志文件中将显示来自客户端的 **SSL** 握手失败错误消息。如果 VDA 和通用打印服务器上的 SSL/TLS 协议版本不匹配，可能会出现此类故障。

在下面包含通用打印服务器主机名的策略设置中使用通用打印服务器 FQDN：

- 会话打印机
- 打印机分配
- 用于负载平衡的通用打印服务器

确保通用打印服务器和 VDA 上的系统时钟（日期、时间和时区）正确无误。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

设备

January 21, 2022

HDX 可以在任何设备、任何位置提供高清晰度的用户体验。“设备”部分中的文章介绍了以下设备：

- 通用 USB 设备
- 移动设备和触摸屏设备
- 串行设备
- 专业键盘
- TWAIN 设备
- 网络摄像机
- WIA 设备

优化的 **USB** 设备与通用 **USB** 设备

优化的 USB 设备是指 Citrix Workspace 应用程序对其提供特定支持的设备。例如，能够使用 HDX 多媒体虚拟通道重定向网络摄像机。通用设备是指 Citrix Workspace 应用程序中不提供特定支持的 USB 设备。

默认情况下，通用 USB 重定向无法重定向具有优化的虚拟通道支持的 USB 设备，除非将其置于通用模式。

一般情况下，使用处于优化模式的 USB 设备所获得的性能优于处于通用模式的 USB 设备。但是，有时处于优化模式的 USB 设备不具备完整功能。可能需要切换到通用模式以获取对其功能的完全访问权限。

借助 USB 大容量存储设备，可以使用客户端驱动器映射和/或通用 USB 重定向，均由 Citrix 策略进行控制。主要的区别为：

如果同时启用了通用 USB 重定向和客户端驱动器映射策略，并且在会话启动之前或之后插入了大容量存储设备，则将使用客户端驱动器映射对其进行重定向。

满足以下条件时，将使用通用 USB 重定向对大容量存储设备进行重定向：

- 同时启用了通用 USB 重定向和客户端驱动器映射策略。
- 设备配置为自动重定向。
- 大容量存储设备在会话启动之前或之后插入。

有关详细信息，请参阅 http://support.citrix.com/article/CTX123015。

功能	客户端驱动器映射	通用 USB 重定向
默认已启用	是	否
可配置只读访问权限	是	否

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

功能	客户端驱动器映射	通用 USB 重定向
加密的设备访问	是，如果在虚拟会话中访问设备之前解锁加密。	仅限 Citrix Virtual Desktops

在多个显示器中使用混合 DPI

Citrix Virtual Apps and Desktops 环境不支持在两个显示器之间使用不同的 DPI。您可以使用 Windows 的“控制面板”>“显示”选项来验证 DPI（% 缩放）。如果使用的是 Windows 8.1 或 Windows 10 客户端设备，请通过在 Windows 的“控制面板”>“显示”选项中启用让我选择一个适合我的所有显示器的缩放级别来相应地配置显示器。有关详细信息，请参阅知识中心文章 CTX201696。

映射的客户端驱动器

为了安全起见，用户登录到 Citrix Virtual Apps and Desktops 时，默认情况下服务器会映射客户端驱动器，但不具有用户运行权限。要使用户能够运行映射的客户端驱动器上的可执行文件，可通过编辑服务器上的注册表来覆盖此默认设置。有关注册表设置的信息，请参阅通过注册表管理的功能列表中的映射的客户端驱动器。

Citrix Virtual Apps and Desktops 7 2006 是包含此注册表位置的第一个版本。早期版本的 Citrix Virtual Apps and Desktops 使用了不同的注册表位置。

通用 USB 设备

July 5, 2024

HDX 技术为最常用的 USB 设备提供了优化的支持。这些设备包括：

- 显示器
- 鼠标
- 键盘
- IP 语音电话
- 耳机
- 网络摄像机
- 扫描仪
- 摄像头
- 打印机
- 驱动器
- 智能卡读卡器

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 手写板
- 签名板

优化的支持可提供改进的用户体验和通过 WAN 实现的更高性能和带宽效率。通常情况下，优化的支持即是最佳选择，尤其对于存在高延迟的环境或对安全性极为敏感的环境更是如此。

HDX 技术为没有优化的支持的特殊设备或优化的支持不适用的场合提供通用 **USB** 重定向。有关通用 USB 重定向的详细信息，请参阅通用 USB 重定向。

有关 USB 设备和适用于 Windows 的 Citrix Workspace 应用程序的详细信息，请参阅配置复合 USB 设备重定向和 [配置 USB 支持]。(/en-us/citrix-workspace-app-for-windows/configure/config-xdesktop/config-usb-support.html)

移动设备和触摸屏设备

September 8, 2022

适用于使用 **Windows Continuum** 的触摸屏设备的平板电脑模式

Continuum 是 Windows 10 的一项功能，可以满足客户端设备的使用需要。自 VDA 7.16 版和 Citrix Receiver for Windows 4.10 版起，我们提供了此版本的 Continuum 支持（包括动态更改模式的功能）。

Windows 10 VDA 可以在启用触控的客户端上检测是否存在键盘或鼠标，如果存在，则将客户端置于桌面模式。如果没有键盘或鼠标，则 Windows 10 VDA 将客户端置于平板电脑/手机模式。在连接和重新连接时进行此检测。在动态连接或分离键盘或鼠标时也会进行此检测。

默认情况下启用该功能。要禁用此版本的功能，请编辑“ICA 策略设置”一文中介绍的平板电脑模式切换策略设置。

对于 XenApp 7.14 和 7.15 LTSR 以及 XenDesktop 7.14 和 7.15 LTSR 中包含的功能版本，请使用注册表设置禁用该功能。有关详细信息，请参阅适用于触摸屏设备的平板电脑模式。

平板电脑模式提供了更适于触摸屏的用户界面：

- 稍大的按钮。
- 开始屏幕和您启动的任何应用程序都以全屏模式打开。
- 任务栏包含返回按钮。
- 从任务栏中删除的图标。

您可以访问文件资源管理器。

桌面模式可提供传统的用户界面，您可以像使用 PC 与键盘和鼠标一样进行交互。

平板电脑模式要求最低版本为 XenServer 7.2。XenServer 7.2 与 Citrix Virtual Desktops VDA 集成，并更改虚拟机管理程序以便为二合一设备启用虚拟固件设置。Windows 10 根据此更新的 BIOS 在虚拟机上加载 GPIO 驱动程序。它用于在虚拟机中在平板电脑和桌面模式之间切换。有关详细信息，请参阅 XenServer 7.2 发行说明。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

适用于 HTML5 的 Citrix Workspace 应用程序（简易版）不支持 Windows Continuum 功能。

运行 XenServer CLI 命令可在便携式计算机/平板电脑之间切换：

xe vm-param-set uuid=<VM_UUID> platform:acpi_laptop_slate=1

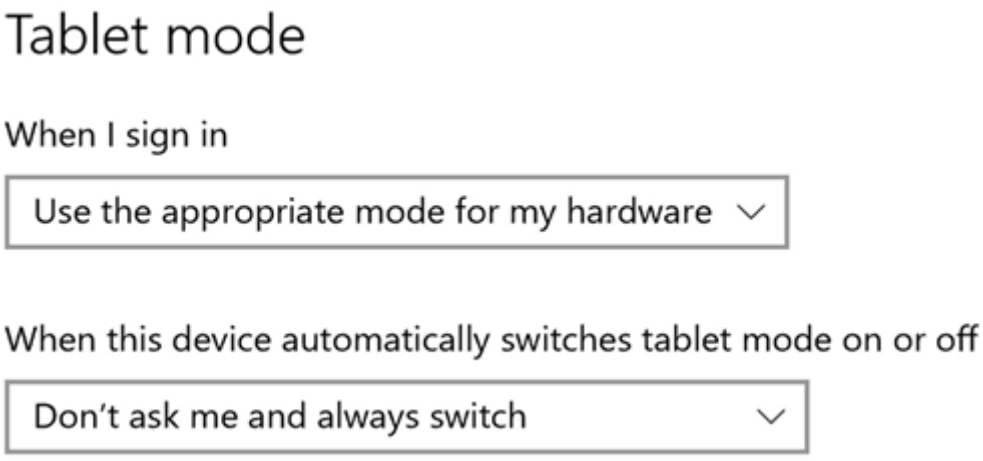
> 重要：
>
> 更新元数据设置后更新现有计算机目录的基础映像不会影响以前置备的任何虚拟机。更改 XenServer VM 基础映像后，请创建一个目录，选择基础映像，然后预配新的 Machine Creation Services (MCS) 计算机。

启动会话之前的准备工作：

我们建议您在启动会话之前先在 VDA 上导航到 **Settings**（设置）**> System**（系统）**> Tablet Mode**（平板电脑模式），然后从下拉菜单中设置以下选项：

- Use the appropriate mode for my hardware（为我的硬件使用合适的模式）
- Don’t ask me and always switch（不再询问并始终切换）

如果您未在启动会话之前设置这些选项，请在启动会话后设置这些选项并重新启动 VDA。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Microsoft Surface Pro 和 Surface Book 笔

我们支持在基于 Windows Ink 的应用程序中使用标准笔功能。此功能要求使用在 Microsoft Window 10 版本 1809（最低版本）上运行的 Virtual Delivery Agent 以及使用适用于 Windows 的 Citrix Workspace 应用程序版本 1902（最低版本）的客户端设备。支持包括指向、擦除、笔压力、蓝牙信号以及取决于操作系统固件和笔型号的其他功能。例如，笔压力可高达 4096 个等级。默认情况下启用此功能。

要获取 Windows Ink 和笔功能的演示，请单击此图形：

系统要求

- Citrix Virtual Apps and Desktops 最低版本 1903
- 适用于 Windows 的 Citrix Workspace 应用程序最低版本 1902
- Microsoft Windows 10 最低版本 1809

要禁用或启用此功能，请参阅通过注册表管理的功能列表中的 Microsoft Surface Pro 和 Surface Book 笔。

串行端口

January 21, 2022

最新的 PC 没有内置串行 (COM) 端口。可以通过 USB 转换器轻松添加这些端口。适合串行端口的应用程序通常涉及传感器、控制器、旧检查读取器、板等。某些 USB 虚拟 COM 端口设备使用供应商特定的驱动程序来代替 Windows 提供的驱动程序 (usbser.sys)。这些驱动程序允许您强制使用 USB 设备的虚拟 COM 端口，以便其即使连接到不同的 USB 插槽也不会发生变化。可以通过从设备管理器 **>** 端口 **(COM** 和 **LPT) >** 属性或从控制设备的应用程序完成此操作。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

通过客户端 COM 端口映射，在虚拟会话期间将能够使用连接到用户的端点上的 COM 端口的设备。可以像使用任何其他网络映射一样使用这些映射。

对于每个 COM 端口，操作系统中的驱动程序将分配一个符号链接名称，例如 COM1 和 COM2。然后，应用程序将使用该链接访问端口。

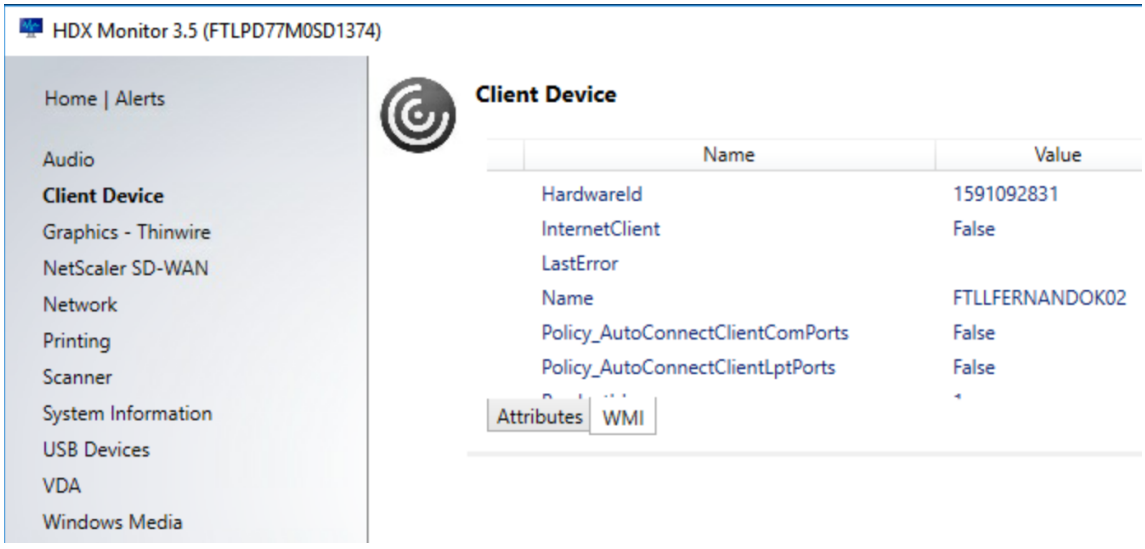
> 重要：
>
> 由于设备可以使用 USB 直接连接到端点，因此并不意味着可以使用通用 USB 重定向功能对其进行重定向。某些 USB 设备功能的运行方式与虚拟 COM 端口相似，应用程序可以通过与物理串行端口相同的方式进行访问。操作系统可以将 COM 端口抽象化并将其视为类似于文件共享的对象。虚拟 COM 的两个公共协议为 CDC ACM 或 MCT。通过 RS-485 端口连接时，应用程序可能完全不运行。请获取一个 RS-485 转 RS232 转换器以将 RS-485 用作 COM 端口。
>
> 重要：
>
> 仅当连接到客户端工作站上的 COM1 或 COM2 时，某些应用程序才能一致地识别设备（例如，签名板）。

将客户端 **COM** 端口映射到服务器 **COM** 端口

可以通过以下三种方式将客户端 COM 端口映射到 Citrix 会话：

- Studio 策略。有关策略的详细信息，请参阅端口重定向策略设置。
- VDA 命令提示窗口。
- 远程桌面（端点服务）配置工具。

1. 启用客户端 **COM** 端口重定向和自动连接客户端 **COM** 端口 **Studio** 策略。应用后，某些信息将在 HDX Monitor 中提供。



2. 如果自动连接客户端 **COM** 端口无法映射该端口，则可以手动映射该端口或使用登录脚本。登录到 VDA，然后在命令提示窗口中键入：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

NET USE COMX: \\CLIENT\COMZ:

或

NET USE COMX: \\CLIENT\CLIENTPORT:COMZ:

X 为 VDA 上的 COM 端口号（端口 1 到 9 可用于映射）。**Z** 为要映射的客户端 COM 端口号。

要确认操作是否成功，请在 VDA 命令提示窗口中键入 **NET USE**。显示的列表中将包含映射的驱动器、LPT 端口和映射的 COM 端口。

```
C:\Windows\system32>net use
New connections will be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
             COM3      \\Client\COM3:            Citrix Client Network
```

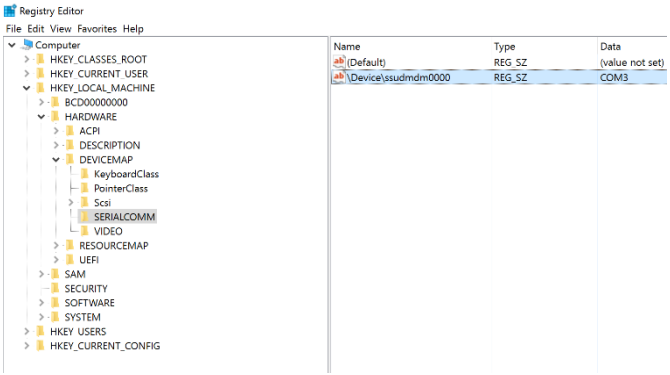
3. 要在虚拟桌面或应用程序中使用此 COM 端口，请安装您的用户设备应用程序并将其指向映射的 COM 端口名称。例如，如果将客户端上的 COM1 映射到服务器上的 COM3，请在会话期间在 VDA 中安装您的 COM 端口设备应用程序并将其指向 COM3。使用此映射 COM 端口时，就如同在使用用户设备上的 COM 端口一样。

> 重要：
>
> COM 端口映射与 TAPI 不兼容。不能将 Windows 电话应用程序编程接口 (TAPI) 设备映射到客户端 COM 端口。TAPI 定义应用程序为数据、传真和语音通话控制电话功能的标准方式。TAPI 管理信号发送，包括拨号、应答和结束通话。此外，还管理呼叫保留、呼叫转接和电话会议等补充服务。

故障排除

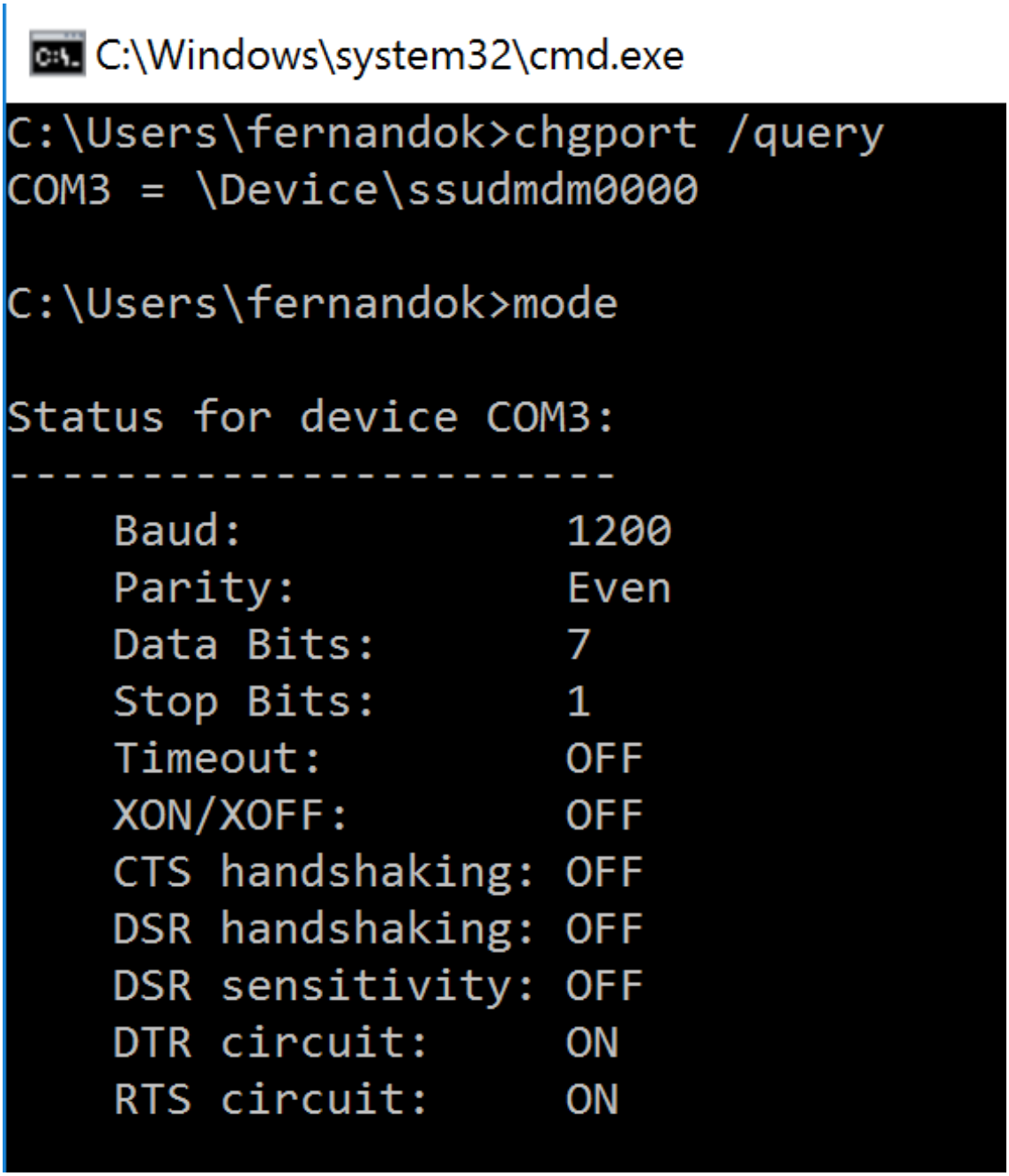
1. 请确保您能够直接从端点访问该设备，不需要通过 Citrix。端口未映射到 VDA 时，您将不连接到 Citrix 会话。请按照设备附带的任何故障排除说明进行操作，并先确认其在本地运行。

   设备连接到串行 COM 端口时，将在此处显示的配置单元中创建一个注册表项：



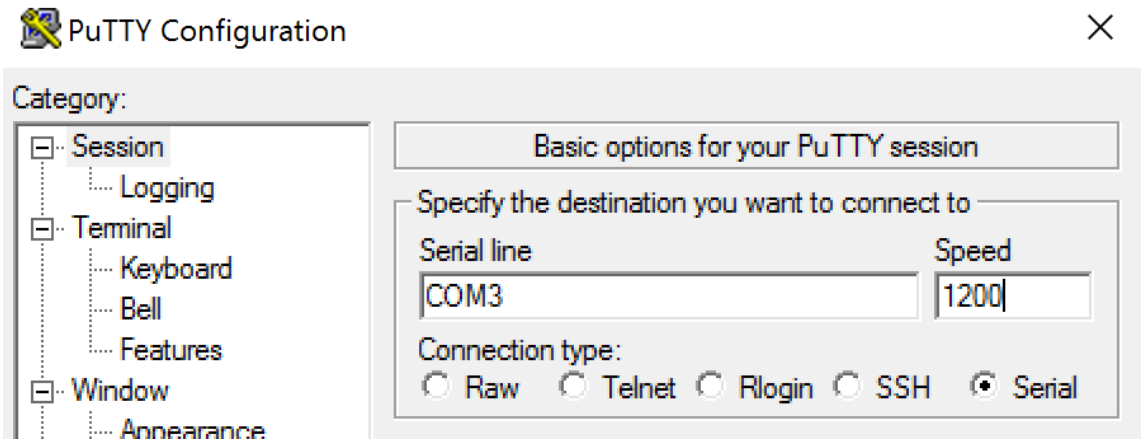
   还可以在命令提示窗口中通过运行 **chgport /query** 查找此信息。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



如果设备的故障排除说明未提供，请尝试打开 PuTTY 会话。选择 **Session**（会话）并在 **Serial line**（串行线）中指定 COM 端口。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



可以在本地命令窗口中运行 **MODE**。输出可能会显示正在使用的 COM 端口以及波特/奇偶校验/数据位数/停止位数，您的 PuTTY 会话中需要这些信息。如果 PuTTY 连接成功，请按 **Enter** 键查看来自设备的反馈。无论您键入哪些字符，都可能会在屏幕上重复出现或被响应。如果此步骤不成功，您将无法从虚拟会话中访问该设备。

2. 将本地 COM 端口映射到 VDA（使用策略或 **NET USE COMX: \\CLIENT\COMZ:**），并重复执行上一个步骤中相同的 PuTTY 过程，但这一次从 VDA PuTTY 执行。如果 PuTTY 无法显示错误 **Unable to open connection to COM1. Unable to open serial port**（无法打开与 COM1 的连接。无法打开串行端口），则表示另一个设备可能正在使用 COM1。

3. 运行 **chgport /query**。如果 VDA 上的内置 Windows 串行驱动程序自动将 \Device\Serial0 分配给 VDA 的 COM1 端口，请执行以下操作：
   A. 在 VDA 上打开 CMD 并键入 **NET USE**。

   B. 删除 VDA 上的任何现有映射（例如，COM1）。

   NET USE COM1 /DELETE

   C. 将设备映射到 VDA。

   NET USE COM1: \\CLIENT\COM3:

   D. 将 VDA 上的应用程序指向 COM3。

   最后，请尝试将您的本地 COM 端口（例如，COM3）映射到 VDA 上的其他 COM 端口（非 COM1，例如 COM3）。请确保您的应用程序指向该端口：
   NET USE COM3: \\CLIENT\COM3

4. 如果您现在看到映射的端口，则表示 PuTTY 正在运行，但不传递数据，它可能是一个争用条件。应用程序可能会在其映射之前连接并打开该端口，将其锁定以阻止其映射。请尝试以下操作之一：

   - 打开相同服务器上发布的第二个应用程序。等待几秒钟时间以便端口完成映射，然后打开尝试使用该端口的真正应用程序。
   - 在 Active Directory 而非 Studio 中从组策略编辑器启用 COM 端口重定向策略。这些策略为客户端 **COM** 端口重定向和自动连接客户端 **COM** 端口。可能会先处理通过这种方式应用的策略，然后再处理

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Studio 策略，以保证映射 COM 端口。Citrix 策略将推送到 VDA 并存储在以下位置：
`HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`

- 要为用户使用此登录脚本而非发布应用程序，请发布一个.bat 脚本，该脚本首先删除 VDA 上的任何映射、重新映射虚拟 COM 端口，然后再启动该应用程序：

```
@echo off
NET USE COM1 /delete
NET USE COM2 /delete
NET USE COM1: \\CLIENT\COM1:
NET USE COM2: \\CLIENT\COM2:
MODE COM1: BAUD=1200（或所需的任何值）
MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1（或所需的任何值）
START C:\Program Files\< 软件路径 >\\软件路径 >
```

5. 如非绝对必要，请勿使用 Sysinternals 发布的进程监视程序。在 VDA 上运行此工具时，请查找并过滤 COM3、picaser.sys、CdmRedirector 等对象，特别是 <your_app>.exe。所有错误都可能会显示为“访问被拒绝”或类似的错误。

专业键盘

July 5, 2024

Bloomberg 键盘

> 警告：
>
> 注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

Citrix Virtual Apps and Desktops 支持 Bloomberg 4 型 Starboard 键盘（以及更早的 3 型键盘）。此键盘允许财务部门的客户使用键盘的特殊功能来访问财务市场数据并快速执行交易。

此键盘与 KVM 开关盒兼容，可以在以下两种模式下工作：

- PC（一根 USB 电缆，不带任何 KVM）
- KVM 模式（两根 USB 电缆，其中一根穿过 KVM）

> 重要：
>
> 我们建议您仅在一个会话中使用 Bloomberg 键盘。我们不建议在多个并发会话（一个客户端举行多个会话）中使用该键盘。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Bloomberg 键盘 4 是在一个物理外壳中包含四个 USB 设备的 USB 组合设备。

- 键盘。
- 指纹读取器。
- 带有用于增大和降低音量以及对扬声器和麦克风进行静音的按键的音频设备。此设备包括板载扬声器、麦克风以及麦克风和耳机插孔。
- 用于将所有这些设备连接到系统的 USB 集线器。

要求：

- 适用于 Windows 的 Citrix Workspace 应用程序连接到的会话必须支持 USB 设备。
- 支持 Bloomberg 键盘 3 型和 4 型的适用于 Windows 的 Citrix Workspace 应用程序 1808 或 Citrix Receiver for Windows 4.8（最低版本）。
- 对 4 型使用 KVM 模式（两根 USB 电缆，其中一根穿过 KVM）的适用于 Windows 的 Citrix Workspace 应用程序 1808 或 Citrix Receiver for Windows 4.12（最低版本）。

有关在适用于 Windows 的 Citrix Workspace 应用程序上配置 Bloomberg 键盘的信息，请参阅配置 Bloomberg 键盘。

要启用 Bloomberg 键盘支持，请参阅通过注册表管理的功能列表中的 Bloomberg 键盘。

确认支持：

要确定是否在 Citrix Workspace 应用程序中启用了 Bloomberg 键盘支持，请检查 Desktop Viewer 是否正确报告 Bloomberg 键盘的设备。

桌面场景：

打开 Desktop Viewer。如果启用了对 Bloomberg 键盘的支持，Desktop Viewer 将在 USB 图标下显示三个设备：

- Bloomberg 指纹扫描仪
- Bloomberg 键盘功能
- Bloomberg LP 键盘 2013

仅限无缝应用程序的场景：

从 Citrix Workspace 应用程序通知区域图标中打开连接中心菜单。如果启用了对 Bloomberg 键盘的支持，设备菜单中将显示三个设备。

针对其中每个设备的复选标记指示其远程连接到会话。

TWAIN 设备

January 21, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

要求

- 扫描仪必须兼容 TWAIN。
- 在本地设备上安装 TWAIN 驱动程序。不需要安装在服务器上。
- 在本地连接扫描仪（例如，通过 USB）。
- 确保扫描仪使用本地 TWAIN 驱动程序，而非 Windows 图像采集服务。
- 确保所有限制 ICA 会话内部带宽的策略都未应用到用于测试的用户帐户。例如，客户端 USB 重定向带宽限制。

有关策略设置的信息，请参阅 TWAIN 设备策略设置。

网络摄像机

January 21, 2022

高清网络摄像机流技术推送

在虚拟会话中运行的视频会议应用程序可以使用网络摄像机。服务器上的应用程序将根据支持的格式类型选择网络摄像机格式和分辨率。会话开始时，客户端将网络摄像机信息发送到服务器。从视频会议应用程序中选择网络摄像机。如果网络摄像机和应用程序都支持高清晰度呈现，则应用程序将使用高清晰度分辨率。我们支持高达 1920x1080 的网络摄像机分辨率。

此功能需要 Citrix Receiver for Windows 最低版本 4.10。有关支持 HDX 网络摄像机重定向的 Citrix Workspace 应用程序平台的列表，请参阅 Citrix Workspace 应用程序功能列表。

有关高清晰度网络摄像机流技术推送的详细信息，请参阅 HDX 视频会议和网络摄像机视频压缩。

可以使用注册表项禁用和启用该功能，然后配置特定的分辨率。有关信息，请参阅通过注册表管理的功能列表中的高清网络摄像机流技术推送和高清网络摄像机分辨率。

WIA 设备

January 21, 2022

要求

- 扫描仪必须符合 WIA 标准。
- 在本地设备上安装 WIA 驱动程序。不需要安装在服务器上。
- 在本地连接扫描仪（例如，通过 USB）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 确保扫描仪使用本地 Windows 图像采集服务，而非 TWAIN 驱动程序。
- 确保所有限制 ICA 会话内部带宽的策略都未应用到用于测试的用户帐户。例如，客户端 USB 重定向带宽限制。

Windows 图像采集应用程序允许列表

允许列表允许您控制 VDA 上的哪些应用程序可以访问 Windows 图像采集扫描仪重定向。注册表编辑器在包含 Windows 图像采集的每个 VDA 上使用允许列表设置中的输入。默认情况下，任何应用程序都无权访问 Windows 图像采集。

要调整面向 VDA 上的应用程序的 Windows 图像采集，请参阅通过注册表管理的功能列表中的 Windows 图像采集应用程序允许列表设置。

有关策略设置的信息，请参阅 WIA 设备策略设置。

图形

January 21, 2022

Citrix HDX 图形包括一套广泛的图形加速和编码技术，用于优化从 Citrix Virtual Apps and Desktops 进行的丰富图形应用程序的交付。使用图形密集型虚拟应用程序远程工作时，图形技术提供的体验与使用物理桌面时相同。

您可以使用软件或硬件进行图形呈现。软件呈现需要名为软件光栅器的第三方库。例如，Windows 包括适用于基于 DirectX 的图形的 WARP 光栅器。有时，您可能希望使用备用软件呈现器。硬件呈现（硬件加速）需要图形处理器 (GPU)。

HDX 图形提供已针对常见用例优化的默认编码配置。使用 Citrix 策略时，IT 管理员还可以配置各种与图形有关的设置，以满足不同的要求和提供所需的用户体验。

Thinwire

Thinwire 是 Citrix Virtual Apps and Desktops 中使用的 Citrix 默认显示远程处理技术。

显示远程处理技术允许一台计算机上生成的图形传输（通常跨网络）到另一台计算机上进行显示。图形是由于用户输入（例如，按键或鼠标操作）而生成。

HDX 3D Pro

借助 Citrix Virtual Apps and Desktops 中的 HDX 3D Pro 功能，可以交付通过使用图形处理器 (GPU) 进行硬件加速实现最佳性能的桌面和应用程序。这些应用程序包括基于 OpenGL 和 DirectX 的 3D 专业图形应用程序。标准 VDA 仅支持 DirectX 的 GPU 加速。

适用于 **Windows** 单会话操作系统的 **GPU** 加速

通过 HDX 3D Pro，可在单会话操作系统计算机上随托管桌面或应用程序交付图形密集型应用程序。HDX 3D Pro 支持物理主机计算机（包括桌面、刀片式服务器和机架工作站）以及 XenServer、vSphere 和 Hyper-V（仅限直通）虚拟机管理程序提供的 GPU 直通和 GPU 虚拟化技术。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

利用 GPU 直通功能，可以创建对专用图形处理硬件具有独占访问权限的 VM。可以在虚拟机管理程序上安装多个 GPU，并将 VM 一对一地分配给每个 GPU。

利用 GPU 虚拟化技术，多个虚拟机可以直接访问单个物理 GPU 的图形处理功能。

适用于 **Windows** 多会话操作系统的 **GPU** 加速

通过 HDX 3D Pro，在 Windows 多会话操作系统会话中运行的图形密集型应用程序可以在服务器图形处理器 (GPU) 上呈现。通过将 OpenGL、DirectX、Direct3D 和 Windows Presentation Foundation (WPF) 呈现移至服务器 GPU，图形呈现不会降低服务器 CPU 的速率。服务器还能够处理更多图形，因为工作负载在 CPU 和 GPU 之间进行了拆分。

Framehawk

> 重要：
>
> 截至 Citrix Virtual Apps and Desktops 7 1903，不再支持 Framehawk。请改为使用启用了自适应传输的 Thinwire。

Framehawk 是适用于移动工作人员的显示远程处理技术，主要针对宽带无线连接（Wi-Fi 和 4G/LTE 蜂窝网络）。Framehawk 克服了光谱干扰和多径传播等挑战，为虚拟应用和桌面用户提供了流畅的交互式用户体验。

基于文本的会话水印

基于文本的会话水印有助于威慑和启用跟踪数据盗窃功能。这一可跟踪的信息在会话桌面上显示，对使用相机和屏幕截图盗取数据的数据盗窃行为具有威慑作用。可以指定一层文本水印。该水印可以在整个会话屏幕上显示，但不会改变原始文档的内容。基于文本的会话水印需要 VDA 支持。

相关信息

- HDX 3D Pro
- 适用于 Windows 单会话操作系统的 GPU 加速
- 适用于 Windows 多会话操作系统的 GPU 加速
- Framehawk
- Thinwire
- 基于文本的会话水印

HDX 3D Pro

January 21, 2022

借助 Citrix Virtual Apps and Desktops 中的 HDX 3D Pro 功能，可以交付通过使用图形处理器 (GPU) 进行硬件加速实现最佳性能的桌面和应用程序。这些应用程序包括基于 OpenGL 和 DirectX 的 3D 专业图形应用程序。标准 VDA 仅支持 DirectX 的 GPU 加速。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

有关 HDX 3D Pro 策略设置，请参阅针对 3D 图形工作负载优化。

所有受支持的 Citrix Workspace 应用程序都可以使用 3D 图形。为了在具有复杂 3D 工作负载、高分辨率显示器、多显示器配置和高帧速率应用程序时获得最佳性能，我们建议使用最新版本的适用于 Windows 的 Citrix Workspace 应用程序和适用于 Linux 的 Citrix Workspace 应用程序。有关受支持的 Citrix Workspace 应用程序版本的详细信息，请参阅 Citrix Workspace 应用程序的生命周期里程碑。

三维专业应用程序示例包括：

- 计算机辅助设计、制造和工程处理 (CAD/CAM/CAE) 应用程序
- 地理信息系统 (GIS) 软件
- 用于医学成像的图形存档与通信系统 (PACS)
- 使用最新 OpenGL、DirectX、NVIDIA CUDA、OpenCL 和 WebGL 版本的应用程序
- 使用 NVIDIA 统一计算设备架构 (CUDA) GPU 实现并行计算的计算密集型非图形应用程序

HDX 3D Pro 在任何带宽条件下均可提供最佳用户体验：

- 在 WAN 连接条件下：通过带宽低至 1.5 Mbps 的 WAN 连接提供交互式用户体验。
- 在 LAN 连接条件下：提供等同于使用 LAN 连接的本地桌面的用户体验。

  可以将图形处理转移到数据中心进行集中管理，从而以简单的用户设备代替复杂且昂贵的工作站。

HDX 3D Pro 为 Windows 单会话操作系统计算机和 Windows 多会话操作系统计算机提供 GPU 加速。有关详细信息，请参阅适用于 Windows 单会话操作系统的 GPU 加速和适用于 Windows 多会话操作系统的 GPU 加速。

HDX 3D Pro 与以下虚拟机管理程序提供的 GPU 直通和 GPU 虚拟化技术兼容，也与裸机兼容：

- Citrix Hypervisor
  - 使用 NVIDIA GRID、AMD 和 Intel GVT-d 实现的 GPU 直通
  - 使用 NVIDIA GRID、AMD 和 Intel GVT-g 实现的 GPU 虚拟化
  - 有关硬件兼容性，请参阅 Hypervisor 硬件兼容性列表。

使用 HDX Monitor 工具可以验证 HDX 虚拟化技术的操作和配置，并可以对 HDX 问题进行诊断和故障排除。要下载此工具并了解其详细信息，请参阅 https://taas.citrix.com/hdx/download/。

适用于 **Windows** 多会话操作系统的 **GPU** 加速

January 21, 2022

通过 HDX 3D Pro，在 Windows 多会话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，图形呈现不会降低服务器的 CPU 速率。服务器还能够处理更多图形，因为工作负载在 CPU 和 GPU 之间进行了拆分。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

由于 Windows Server 是多用户操作系统，因此多个用户可以共享由 Citrix Virtual Apps 访问的 GPU，而无需 GPU 虚拟化 (vGPU)。

有关涉及到编辑注册表的过程，请注意：注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

GPU Sharing

GPU 共享使 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。

按照虚拟机管理程序和 GPU 供应商的要求，可以在完全直通或虚拟 GPU (vGPU) 模式下将 GPU 分配给 Windows Server 虚拟机。还支持在物理 Windows Server 计算机上进行裸机部署。

GPU 共享不依赖任何特定的图形卡。

- 对于虚拟机，请选择与正在使用的虚拟机管理程序兼容的图形卡。有关 Citrix Hypervisor 硬件兼容性列表，请参阅 Hypervisor 硬件兼容性列表。
- 在裸机上运行时，建议使用操作系统启用的一个显示适配器。如果在硬件上安装了多个 GPU，请仅保留一个 GPU，并使用 Device Manager 禁用其余的 GPU。

使用 GPU Sharing 的可扩展性取决于多个因素：

- 正在运行的应用程序
- 占用的视频 RAM 量
- 图形卡的处理能力

一些应用程序处理视频 RAM 短缺的能力要优于其他应用程序。如果硬件过载，可能会出现不稳定或图形卡驱动程序崩溃。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。有关 GPU-Z，请访问 http://www.techpowerup.com/gpuz/。

- 访问 NVIDIA GPU 和 Intel Iris Pro 图形处理器的高性能视频编码器。策略设置（默认启用）控制此功能，并允许使用硬件编码进行 H.264 编码（如果可用）。如果此类硬件不可用，VDA 会回退到使用软件视频编解码器的基于 CPU 的编码。有关详细信息，请参阅图形策略设置。

DirectX、Direct3D 和 WPF 呈现

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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 及更高版本上，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 及更高版本上的 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设置。
- 要能够使用服务器的 GPU 呈现 WPF 应用程序，请在运行 Windows 多会话操作系统会话的服务器的注册表中创建设置。有关注册表设置的信息，请参阅通过注册表管理的功能列表中的 Windows Presentation Foundation (WPF) 呈现。

面向 **CUDA** 或 **OpenCL** 应用程序的 **GPU** 加速功能

默认禁用在用户会话中运行的 CUDA 或 OpenCL 应用程序的 GPU 加速功能。

要使用 CUDA 加速 POC 功能，请启用注册表设置。有关信息，请参阅通过注册表管理的功能列表中的面向 CUDA 或 OpenCL 应用程序的 GPU 加速功能。

适用于 **Windows** 单会话操作系统的 **GPU** 加速

April 7, 2023

通过 HDX 3D Pro，可在单会话操作系统计算机上随托管桌面或应用程序交付图形密集型应用程序。HDX 3D Pro 支持物理主机计算机（包括桌面、刀片式服务器和机架工作站）以及 Citrix Hypervisor、vSphere、Nutanix 和 Hyper-V（仅限直通）虚拟机管理程序提供的 GPU 直通和 GPU 虚拟化技术。

HDX 3D Pro 提供以下功能：

- 基于 H.264 或基于 H.265 的自适应深度压缩，用于实现最佳的 WAN 和无线性能。HDX 3D Pro 使用基于 CPU 的全屏 H.264 压缩作为编码的默认压缩技术。对支持 NVENC 的 NVIDIA、Intel 和 AMD 卡使用采用 H.264 的硬件编码。对支持 NVENC 的 NVIDIA 卡使用采用 H.265 的硬件编码。
- 专用的无损压缩选项。HDX 3D Pro 还提供基于 CPU 的无损编解码器，可支持需要在像素级完美呈现图形的应用程序，例如医学成像。建议仅针对特殊用例使用真正的无损压缩，因为这种压缩方式占用更多网络和处理资源。

  使用无损压缩时：

  - 无损指示器（一个通知区域图标）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无损构建时，此图标很有用。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，请右键单击切换到像素完美或使用快捷键 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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 HKEY_LOCAL_MACHINE\SOFTWARE\Citri
  下配置一个新注册表设置。
  - 名称：HKEY_LOCAL_MACHINE_HotKey，类型：字符串
  - 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。
  - 例如：
    - 对于 F10，设置 K=0x79
    - 对于 Ctrl + F10，设置 C=1、K=0x79
    - 对于 Alt + A、设置 A=1、K=a 或 A=1、K=A 或 K=A、A=1
    - 对于 Ctrl + Alt + 5，设置 C=1、A=1、K=5 或 A=1、K=5、C=1
    - 对于 Ctrl + Shift + F5，设置 A=1、S=1、K=0x74

> 小心：
>
> 注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

- 多显示器和高分辨率显示器支持。对于单会话操作系统计算机，HDX 3D Pro 支持用户设备最多使用 4 个显示器。用户可以采用任意配置安排自己的显示器，并且可以混合使用分辨率和方向各不相同的显示器。显示器的数量受主机计算机 GPU 功能、用户设备以及可用带宽限制。HDX 3D Pro 支持所有显示器分辨率，并仅受主机计算机上 GPU 的功能限制。
- 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 vGPU 体系结构。HDX 3D Pro 支持 NVIDIA vGPU 卡。有关信息，请参阅 NVIDIA vGPU，了解 GPU 直通和 GPU 共享。NVIDIA vGPU 允许多个 VM 使用在非虚拟操作系统中部署的相同 NVIDIA 图形驱动程序同时直接访问单个物理 GPU。
- 支持使用虚拟直接图形加速 (vDGA) 的 VMware vSphere 和 VMware ESX —可针对 RDS 和 VDI 工作负载将 HDX 3D Pro 与 vDGA 结合使用。
- 支持使用 NVIDIA GRID vGPU 和 AMD MxGPU 的 VMware vSphere/ESX。
- 对使用 Windows Server 2016 中离散设备分配的 Microsoft HyperV 的支持。
- 对具有 Intel Xeon Processor E3 系列的数据中心图形的支持。HDX 3D Pro 支持多显示器（最多 3 个）、控制台消隐、自定义分辨率和受支持的 Intel 处理器系列的高帧速率功能。有关详细信息，请参阅http://www.citrix.com/intel和http://www.intel.com/content/www/us/en/servers/data-center-graphics.html。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

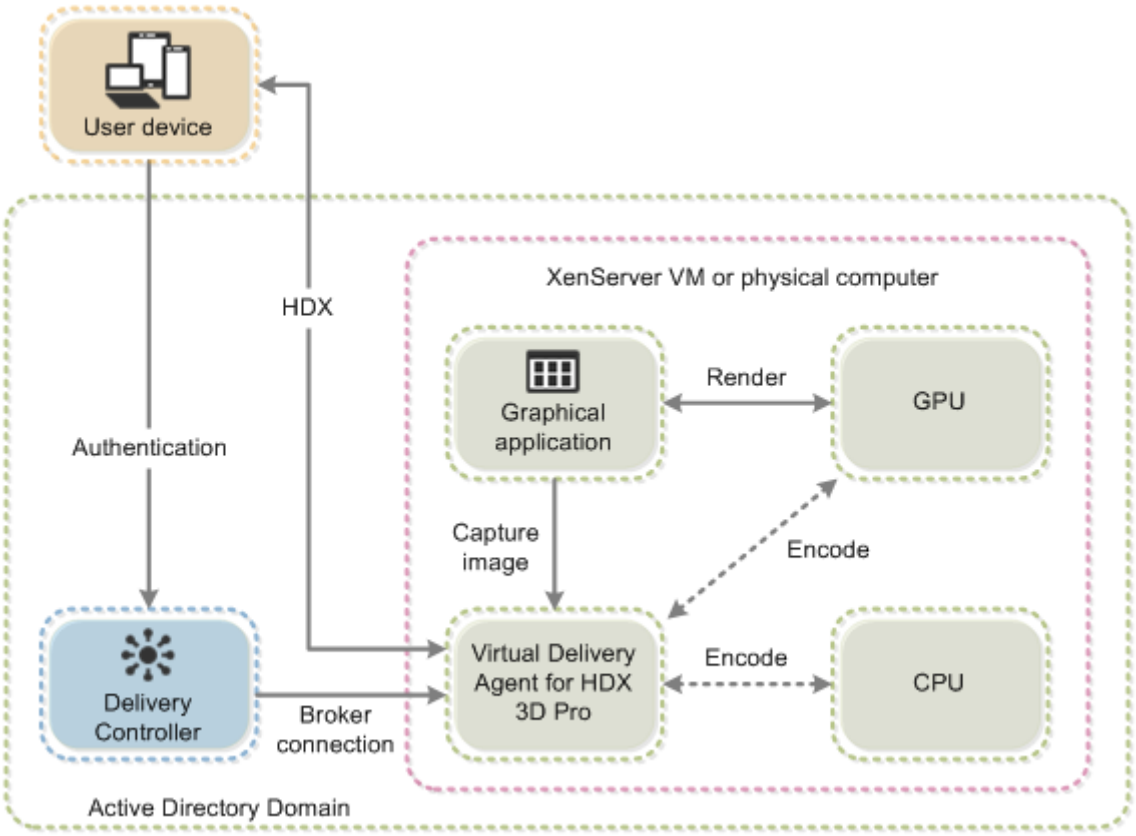
- AMD FirePro S 系列服务器卡支持 AMD RapidFire。HDX 3D Pro 支持多显示器（最多 6 个）、控制台消隐、自定义分辨率和高帧速率功能。注意：针对 AMD MxGPU（GPU 虚拟化）的 HDX 3D Pro 支持仅适用于 VMware vSphere vGPU。GPU 直通支持 Citrix Hypervisor 和 Hyper-V。有关详细信息，请参阅 AMD 虚拟化解决方案。
- 访问适用于 NVIDIA GPU、AMD GPU 和 Intel Iris Pro 图形处理器的高性能视频编码器。策略设置（默认情况下启用）控制此功能。此功能允许使用硬件编码进行 H.264 编码（如果可用）。如果此类硬件不可用，VDA 会回退到使用软件视频编解码器的基于 CPU 的编码。有关详细信息，请参阅图形策略设置。

如下图所示：

- 当用户登录到 Citrix Workspace 应用程序并访问虚拟应用程序或桌面时，Controller 将对用户进行身份验证。然后，Controller 与 VDA for HDX 3D Pro 联系，以代理与托管图形应用程序的计算机的连接。

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在主机计算机与用户设备之间传输。此传输是通过 Citrix Workspace 应用程序与 VDA for HDX 3D Pro 之间的直接 HDX 连接完成的。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

优化 **HDX 3D Pro** 用户体验

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。这样做会导致用户会话期间不稳定。

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 Workspace 应用程序 - 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），我们建议您使用总会话带宽限制策略设置，以限制每位用户可用的带宽。使用此设置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，我们建议您将通用 USB 重定向虚拟通道的优先级提高到 0。有关如何更改虚拟通道优先级的信息，请参阅知识中心文章 CTX128190。

Thinwire

January 21, 2022

简介

Thinwire 是 Citrix HDX 技术的一部分，是 Citrix Virtual Apps and Desktops 中使用的 Citrix 默认显示远程处理技术。

显示远程处理技术允许一台计算机上生成的图形传输（通常跨网络）到另一台计算机上进行显示。

成功的显示远程处理解决方案提供与本地 PC 类似的高度互动用户体验。Thinwire 通过使用一系列复杂有效的图像分析和压缩技术实现此体验。Thinwire 最大程度地实现了服务器可扩展性，且占用的带宽少于其他显示远程处理技术。

由于这种平衡，Thinwire 满足最一般的业务用例，并用作 Citrix Virtual Apps and Desktops 中的默认显示远程处理技术。

HDX 3D Pro

在其默认配置中，Thinwire 可以提供 3D 或高度交互的图形，并使用图形处理器 (GPU)（如果存在）。但是，我们建议您在存在 GPU 时使用针对 **3D** 图形工作负载优化或视觉质量 **>** 无损构建策略来启用 HDX 3D Pro 模式。这些策略将

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Thinwire 配置为使用视频编解码器（H.264 或 H.265）来使用硬件加速对整个屏幕进行编码（如果存在 GPU）。这样做可以在 3D 专业图形方面提供更加流畅的体验。有关详细信息，请参阅 H.264 无损构建、HDX 3D Pro 和适用于 Windows 单会话操作系统的 GPU 加速。

要求

Thinwire 已经过优化，适用于最新的操作系统，包括 Windows Server 2012 R2、Windows Server 2016、Windows Server 2019、Windows 7 和 Windows 10。对于 Windows Server 2008 R2，建议使用旧图形模式。使用内置 Citrix 策略模板、“服务器高度可扩展性 - 旧版操作系统”和“针对广域网优化 - 旧版操作系统”为这些用例提供 Citrix 建议的策略设置组合。

> 注意：
>
> 此版本不支持旧版图形模式。为了在结合使用 XenApp 7.15 LTSR、XenDesktop 7.15 LTSR 和早期 VDA 版本与 Windows 7 和 Windows 2008 R2 时向后兼容而包括此项。

- 在 Citrix Virtual Apps and Desktops 7 1808 或更高版本与 XenApp and XenDesktop 7.6 FP3 及更高版本中的 VDA 版本上提供了驱动 Thinwire 行为的策略设置使用视频编解码器进行压缩。在 Citrix Virtual Apps and Desktops 7 1808 或更高版本与 XenApp and XenDesktop 7.9 及更高版本中的 VDA 版本上，偏好时使用视频编解码器选项是默认设置。
- 所有 Citrix Workspace 应用程序都支持 Thinwire。某些 Citrix Workspace 应用程序可能支持其他 Citrix Workspace 应用程序不支持的 Thinwire 功能，例如，为了降低带宽使用量的 8 位或 16 位图形。此类功能支持由 Citrix Workspace 应用程序自动协商。
- 在多显示器或高分辨率情况下，Thinwire 使用较多的服务器资源（CPU、内存）。可以调整 Thinwire 使用的资源量，但可能会导致带宽使用量增加。
- 在低带宽或高延迟情况下，请考虑启用 8 位或 16 位图形来提高交互性。视觉质量可能会受影响，尤其是使用 8 位颜色深度时。

编码方法

Thinwire 可以在两种不同的编码模式下运行，具体取决于策略和客户端功能：

- Thinwire 全屏 H.264 或 H.265
- 使用选择性 H.264 或 H.265 的 Thinwire

旧 GDI 远程处理使用 XPDM 远程处理驱动程序，而非 Thinwire 位图编码器。

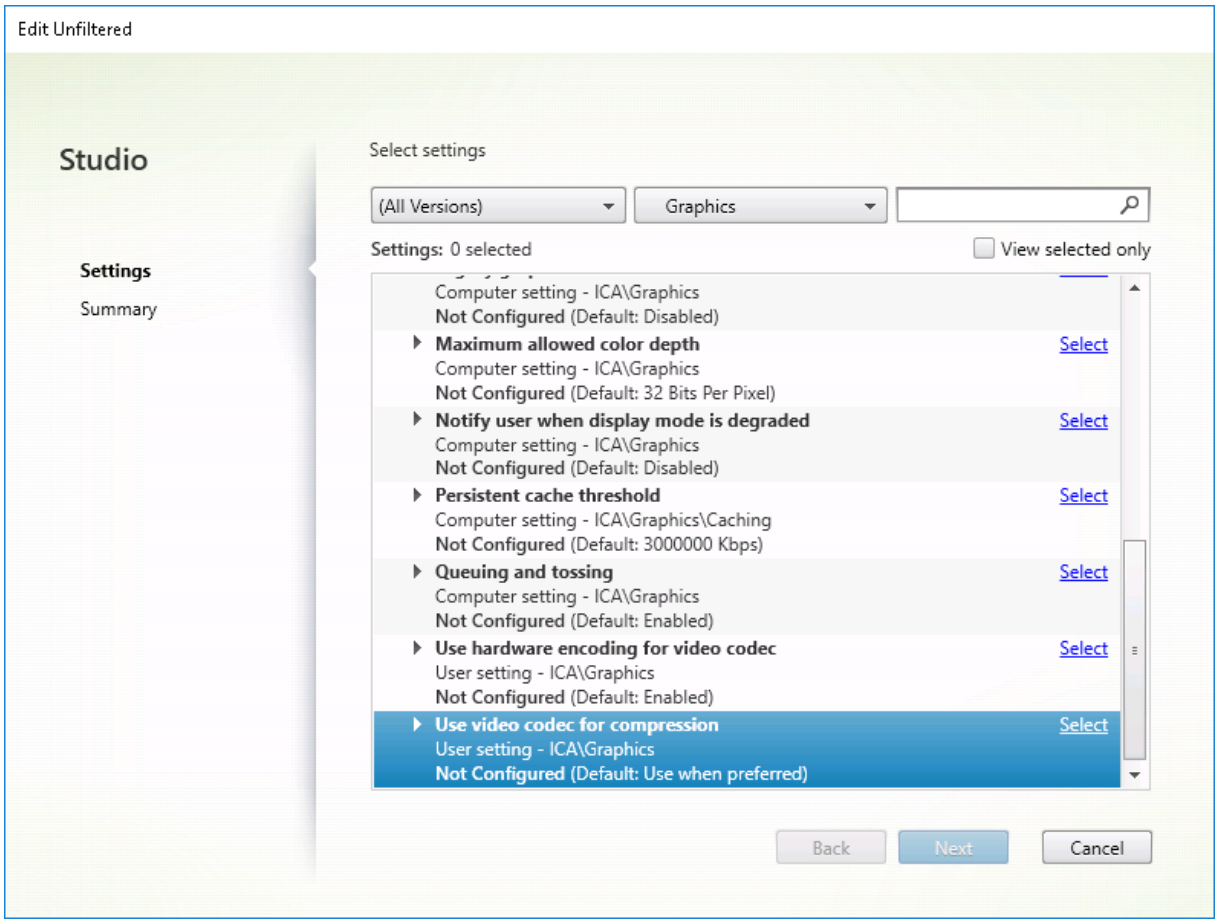
配置

Thinwire 是默认显示远程处理技术。

以下“图形”策略设置会设置默认设置，并提供适用于不同用例的备选设置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 使用视频编解码器进行压缩
  - 偏好时使用视频编解码器。此为默认设置。无需执行其他配置。将此设置保持为默认设置可确保为所有 Citrix 连接选择 Thinwire，且 Thinwire 已针对典型桌面工作负载在可扩展性、带宽和卓越图像质量方面经过优化，这在功能上等同于针对主动变化的区域。
- 此策略设置中的其他选项会继续将 Thinwire 与其他技术结合使用以应对不同的用例。例如：
  - 针对主动变化的区域。Thinwire 中的自适应显示技术可识别移动图像（视频、动态 3D），并只在图像移动的屏幕部分使用 H.264 或 H.265。
  - 针对整个屏幕。为 Thinwire 提供全屏 H.264 或 H.265，以在大量使用 3D 图形的情况下针对改进用户体验和带宽使用情况进行优化。使用 H.264 4:2:0 时（禁用视觉无损策略），最终图像不是完美的像素（无损），可能不适合某些情况。在此类情况下，请考虑改为使用 H.264 无损构建。



某些其他策略设置（包括以下视觉显示策略设置）可以用于对显示远程处理技术的性能进行完善：Thinwire 支持其中的所有功能。

- 简单图形的首选颜色深度
- 目标帧速率
- 视觉质量

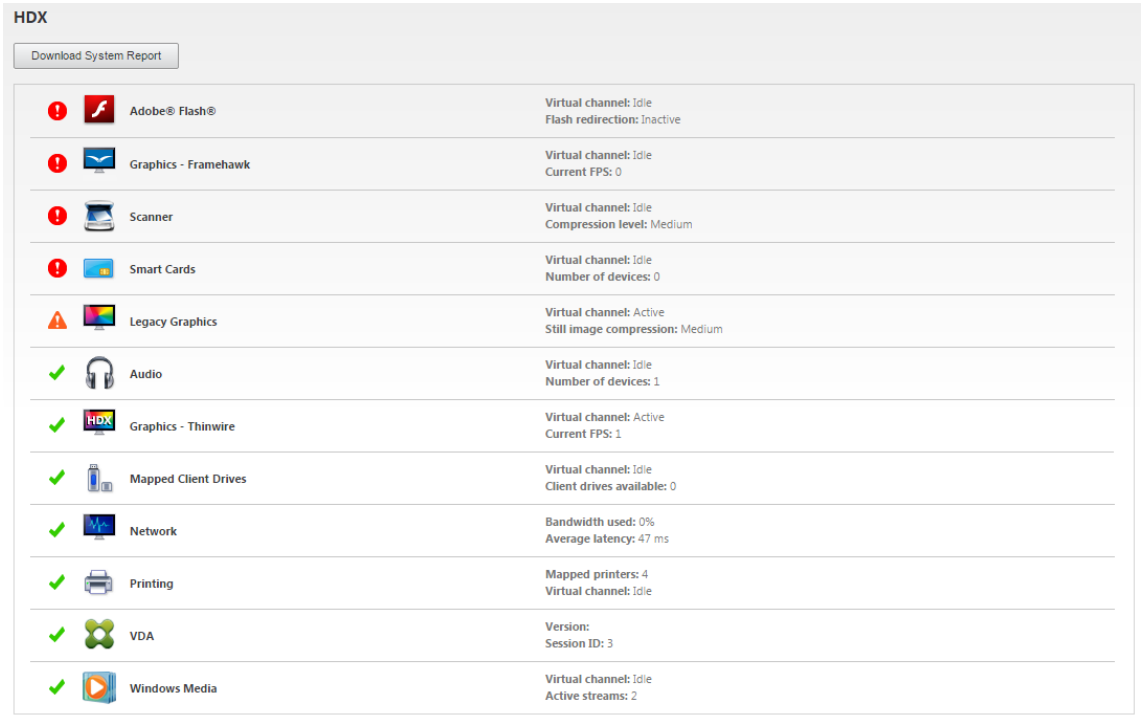
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

要获得适用于不同业务用例的 Citrix 建议策略设置组合，请使用内置 Citrix 策略模板。服务器高度可扩展性和超高清晰度用户体验模板都结合使用 Thinwire 与符合您的组织的优先级要求和您的用户的期望的最优策略设置组合。

监视 **Thinwire**

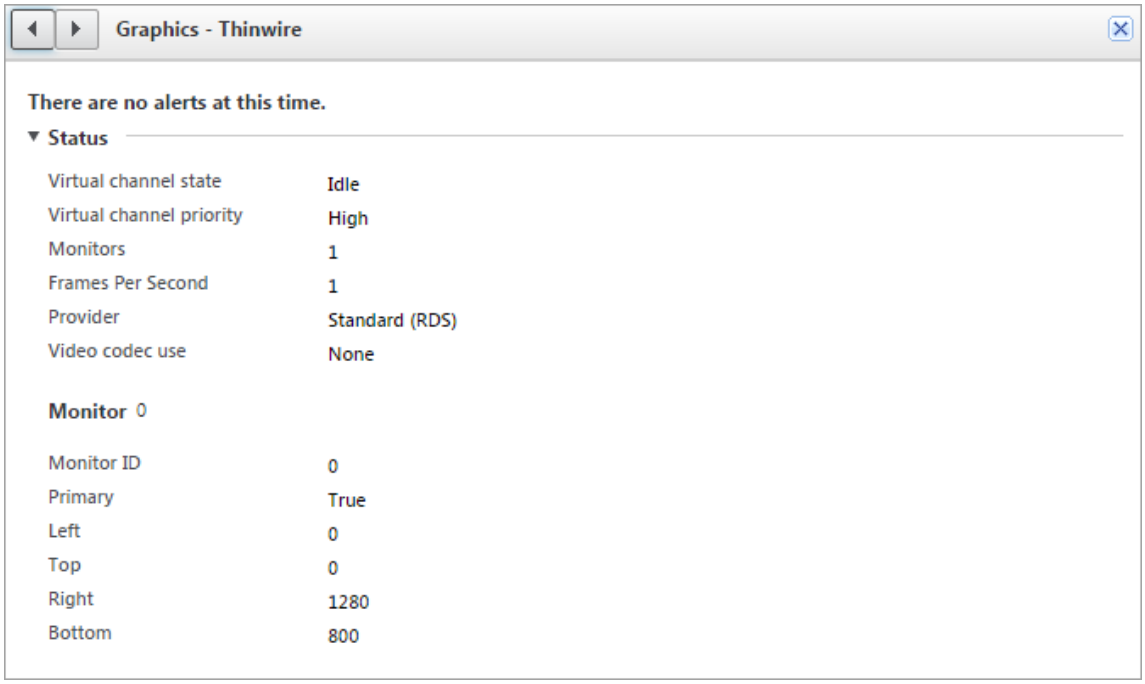
您可以从 Citrix Director 监视 Thinwire 的使用情况和性能。HDX 虚拟通道详细信息视图包含有助于对任何会话中的 Thinwire 进行监视和故障排除的有用信息。要查看 Thinwire 相关的指标，请执行以下操作：

1. 在 Director 中，搜索用户、计算机或端点，打开一个活动会话并单击详细信息。也可以选择过滤器 > 会话 > 所有会话，打开一个活动会话并单击详细信息。
2. 向下滚动到 **HDX** 面板。



3. 选择图形 **- Thinwire**。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



无损压缩编解码器 (MDRLE)

在典型桌面会话中，大多数图像都是简单图形或文本区域。Thinwire 确定这些区域的位置，并使用 2DRLE 编解码器选择这些区域进行无损编码。在 Citrix Workspace 应用程序客户端，这些元素通过 Citrix Workspace 应用程序端的 2DRLE 解码器进行解码，以便显示会话。

在 XenApp 和 XenDesktop 7.17 中，我们增加了一个压缩比更高的 MDRLE 编码器，该编码器在典型桌面会话中占用的带宽低于 2DRLE 编解码器。这一新编解码器不会影响服务器的可扩展性。

带宽较低，通常意味着会话交互性会有所改进（通常在共享链路或约束链路中），并且成本降低。例如，对于典型办公类工作负载，使用 MDRLE 编解码器时的预期带宽占用量大约比使用 XenApp 和 XenDesktop 7.15 LTSR 时低 10–15%。

MDRLE 编解码器不需要任何配置。如果 Citrix Workspace 应用程序支持 MDRLE 解码，VDA 将使用 VDA MDRLE 编码和 Citrix Workspace 应用程序 MDRLE 解码。如果 Citrix Workspace 应用程序不支持 MDRLE 解码，VDA 将自动回退到 2DRLE 编码。

MDRLE 要求：

- Citrix Virtual Apps and Desktops 最低版本 7 1808 VDA
- XenApp 和 XenDesktop 最低版本 7.17 VDA
- 适用于 Windows 的 Citrix Workspace 应用程序最低版本 1808
- Citrix Receiver for Windows：最低版本 4.11

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

渐进式模式

Citrix Virtual Apps and Desktops 1808 引入了渐进式模式，默认情况下启用该模式。在受限的网络条件下（默认值：带宽 < 2 Mbps，或者延迟 > 200 毫秒），Thinwire 增加了文本和静态影像的压缩，以改善屏幕活动期间的交互性。然后，当屏幕活动停止时，大量压缩的文本和图像会以随机块的方式逐渐锐化。通过这种方式进行压缩和锐化可提高整体交互性，但它降低了缓存效率并增加了带宽使用率。

自 Citrix Virtual Apps and Desktops 1906 起，默认情况下将禁用渐进式模式。我们现在使用不同的方法。静止图像的质量现在基于网络条件，并在每个视觉质量设置预定义的最小值到最大值之间浮动。由于没有明确的锐化步骤，Thinwire 可优化映像交付并保持缓存效率，同时提供渐进式模式的几乎所有优势。

更改渐进式模式行为

可以通过注册表项更改渐进式模式的状态。有关信息，请参阅通过注册表管理的功能列表中的渐进式模式。

H.264 设为无损

无损构建是一种特殊的 Thinwire 配置，可优化图形交付以实现交互性和最终图像质量。可以通过将视觉质量策略设置为无损构建来启用此设置。

“无损构建”在屏幕活动期间使用 H.264（或 H.265）压缩屏幕，在活动停止时锐化为完美像素（无损）。H.264（或 H.265）图像质量可根据可用资源进行调整，以保持最佳帧速率。锐化步骤逐渐执行，如果用户在锐化开始后不久开始屏幕活动，则将立即响应。例如，选择一个模型并进行旋转。

H.264 无损构建提供全屏 H.264 或 H.265 的所有优势（包括硬件加速），但具有最终的保证无损屏幕的额外优势。这对于需要最终像素完美映像的 3D 类型工作负载至关重要。例如，操作医学图像。此外，H.264 无损构建使用比全屏 H.264 4:4:4 更少的资源。因此，使用无损构建通常会导致帧速率高于视觉无损 H.264 4:4:4。

> 注意：
>
> 除视觉质量策略外，还会将使用视频编解码器策略设置为偏好时使用（默认值）或针对主动变化的区域。通过将使用视频编解码器策略设置为不使用视频编解码器，您可以恢复到非 H.264“无损构建”。这会导致移动图像使用 JPEG 而非 H.264（或 H.265）进行编码。

基于文本的会话水印

January 21, 2022

基于文本的会话水印有助于威慑和启用跟踪数据盗窃功能。这一可跟踪的信息在会话桌面上显示，对使用相机和屏幕截图盗取数据的数据盗窃行为具有威慑作用。可以指定一层文本水印，该水印将在整个会话屏幕上显示，但不会改变原始文档的内容。基于文本的会话水印需要 VDA 支持。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 重要：
>
> 基于文本的会话水印不属于安全功能。此解决方案不能完全阻止数据盗窃，但可以提供一定级别的威慑作用和可跟踪性。虽然我们不保证使用此功能时信息完全可跟踪，但是我们建议您将此功能与其他安全解决方案结合使用（如果适用）。

会话水印属于文本，不适用于向用户提供的会话。会话水印中包含用于跟踪数据盗窃的信息。最重要的数据是在其中创建了屏幕图像的当前会话的登录用户的身份。为了更有效地跟踪数据泄漏，请包括服务器或客户端 Internet 协议地址以及连接时间等其他信息。

要调整用户体验，请使用会话水印策略设置配置屏幕上的放置位置和水印外观。

要求：

Virtual Delivery Agent：

多会话操作系统 7.17
单会话操作系统 7.17

限制：

- 会话水印在使用本地应用程序访问、Windows Media 重定向、MediaStream、浏览器内容重定向和 HTML5 视频重定向的会话中不受支持。要使用会话水印，请务必禁用这些功能。
- 如果会话在全屏硬件加速模式（全屏 H.264 或 H.265 编码）下运行，会话水印将不受支持，并且不显示。
- 如果设置了这些 HDX 策略，水印设置将不生效，并且水印不在会话显示屏幕中显示。

使用视频编解码器的硬件编码设置为已启用
使用视频编解码器进行压缩设置为针对整个屏幕

- 如果设置了这些 HDX 策略，行为将不确定，并且水印可能不会显示。

  使用视频编解码器的硬件编码设置为已启用
  使用视频编解码器进行压缩设置为偏好时使用视频编解码器

  为确保水印能够显示，请将使用视频编解码器的硬件编码设置为已禁用，或者将使用视频编解码器进行压缩设置为针对主动变化的区域或不使用视频编解码器。

- 会话水印仅支持 Thinwire 图形模式。
- 如果使用 Session Recording，录制的会话将不包括水印。
- 如果使用 Windows 远程协助，则不显示水印。
- 如果用户按 **Print Screen** 键捕获屏幕，在 VDA 端捕获的屏幕将不包括水印。我们建议您采取措施来避免复制捕获的图像。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

多媒体

November 17, 2021

HDX 技术堆栈支持通过两种互补的方法来交付多媒体应用程序：

- 服务器端呈现多媒体交付
- 客户端呈现多媒体重定向

此策略可确保您能够在将服务器可扩展性增加至最大以降低每个用户的成本时交付全部多媒体格式，并提供优异的用户体验。

使用服务器呈现的多媒体交付时，音频和视频内容将通过应用程序解码并在 Citrix Virtual Apps and Desktops 服务器上呈现。该内容随后被压缩并通过 ICA 协议交付到用户设备上的 Citrix Workspace 应用程序。此方法提供的与各种应用程序和媒体格式的兼容率最高。由于视频处理属于计算密集型操作，因此，服务器呈现的多媒体交付将大大受益于板载硬件加速。例如，对 DirectX 视频加速 (DXVA) 的支持将通过在单独的硬件中执行 H.264 解码来卸载 CPU 的负载。Intel Quick Sync、AMD RapidFire 和 NVIDIA NVENC 技术提供硬件加速的 H.264 编码。

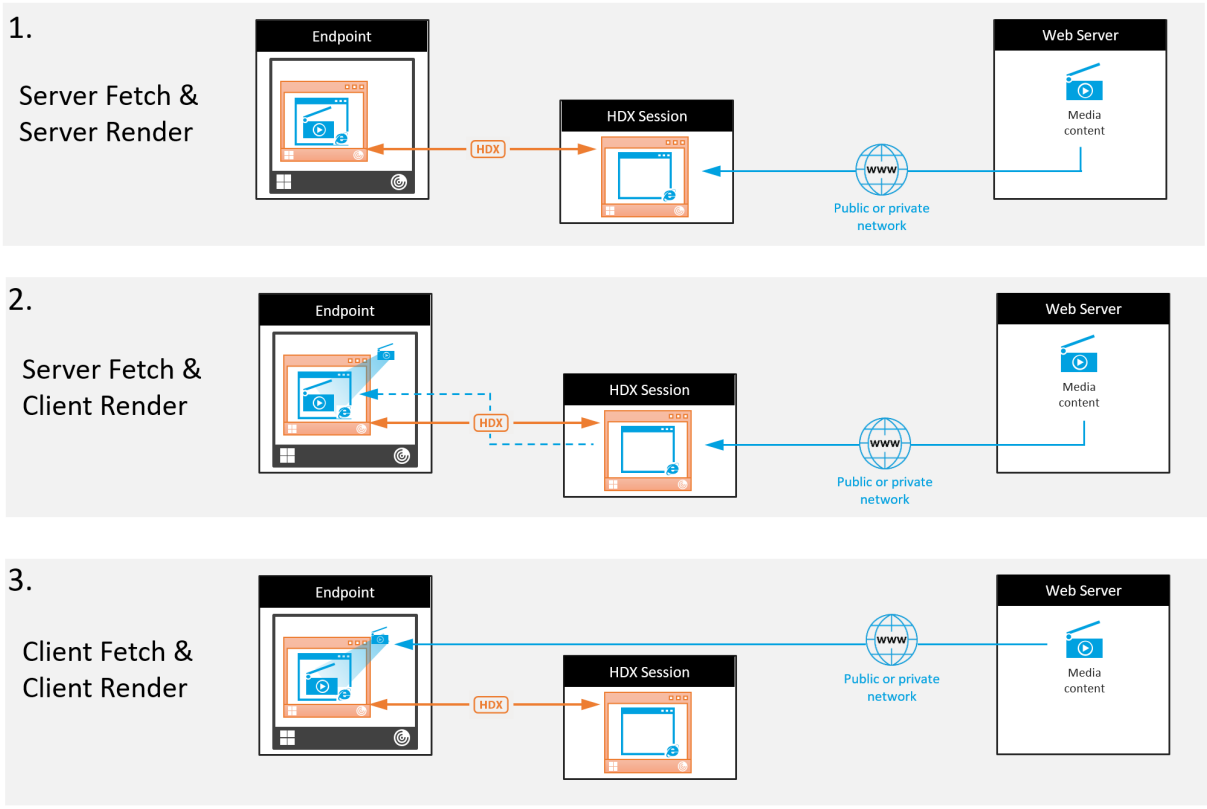
由于大多数服务器不对视频压缩提供任何硬件加速，因此，如果所有视频处理都在服务器 CPU 上完成，服务器可扩展性将受到负面影响。可以通过将多种多媒体格式重定向到用户设备以进行本地呈现来保持高服务器可扩展性。

- Windows Media 重定向针对许多种通常与 Windows Media Player 关联的媒体格式来卸载服务器的负载。
- HTML5 视频变得非常盛行，Citrix 为这种类型的内容引入了重定向技术。我们建议使用 HTML5、HLS、DASH 或 WebRTC 对 Web 站点进行浏览器内容重定向。
- 可以对多媒体内容应用常规访问重定向技术“主机到客户端重定向”和“本地应用程序访问”。

如果未配置重定向，同时使用这些技术时，HDX 将执行服务器端呈现。
如果配置了重定向，HDX 将使用服务器提取和客户端呈现，或者客户端提取和客户端呈现。如果这些方法失败，HDX 将根据需要回退到服务器端呈现，并且遵从“回退防护”策略。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

示例场景



场景 **1**。（服务器提取和服务器呈现）：

1. 服务器从其来源提取媒体文件，进行解码，然后将内容提供给音频设备或显示设备。
2. 服务器分别从显示设备或音频设备提取提供的图像或声音。
3. 服务器有选择地对其进行压缩，然后将其传输到客户端。

此方法的 CPU 成本和带宽成本都非常高（如果提取的图像/声音未有效压缩），并且服务器可用性非常低。

Thinwire 和音频虚拟通道采用此方法。此方法的优势是降低了客户端的硬件和软件要求。使用此方法时，解码在服务器上进行，并且适用于许多种设备和格式。

方案 **2.** （服务器提取和客户端呈现）：

此方法依赖在解码之前截获媒体内容并将其提供给音频设备或显示设备的能力。压缩后的音频/视频内容改为发送到客户端，之后将在客户端上对其进行本地解码和呈现。此方法的优势是卸载到客户端设备，缩短了服务器上的 CPU 周期。

但是，此方法还额外引入了一些针对客户端的硬件和软件要求。客户端必须能够解码可能会接收到的每种格式。

方案 **3.** （客户端提取和客户端呈现）：

此方法依赖在从其来源提取之前截获媒体内容 URL 的能力。URL 将被发送到客户端，并且媒体内容将在客户端本地提取、解码和呈现。此方法从概念上讲非常简单。其优势是缩短了服务器上的 CPU 周期并且节省了带宽，因为服务器仅发送控制命令。但是，媒体内容并非始终可由客户端访问。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

框架和平台：

单会话操作系统（Windows、Mac OS X 和 Linux）提供允许更加快速地部署多媒体应用程序的多媒体框架。下表列出了部分较为常见的多媒体框架。每种框架都将媒体处理划分为多个阶段，并使用基于管道的体系结构。

Framework	平台
DirectShow	Windows（98 及更高版本）
媒体基础	Windows（Vista 及更高版本）
Gstreamer	Linux
Quicktime	Mac OS X

媒体重定向技术的双跃点支持

	客户端重定向	否
	浏览器内容重定向	否
	HDX 网络摄像机重定向	是
	HTML5 视频重定向	是
	Windows Media 重定向	是

音频功能

June 29, 2023

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依赖项，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：
>
> 我们建议使用用户数据报协议 (UDP) 而非 TCP 来传输音频。只有 Windows Virtual Delivery Agent (VDA) 支持通过 UDP 传输音频。
>
> 使用 DTLS 的 UDP 音频加密仅在 Citrix Gateway 与 Citrix Workspace 应用程序之间可用。因此，有时使用 TCP 传输可能更为可取。TCP 支持从 VDA 到 Citrix Workspace 应用程序的端到端 TLS 加密。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

音频质量

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，使用 TCP 传输时，音频质量策略设置设为“高 - 高清晰度音频”。使用 UDP 传输（推荐）时，此策略设置为“中 - 语音优化”。高清晰度音频设置提供高保真立体声音频，但占用的带宽高于其他质量设置。对于未优化的语音聊天或视频聊天应用程序（例如软件电话），请勿使用此音频质量。原因是此音频质量可能会在不适用于实时通信的音频路径中引入延迟。我们建议对实时音频使用语音优化策略设置，而无论选定的传输协议为何。

带宽受限时（例如卫星连接或拨号连接），将音频质量降低至低将占用可行的最低带宽。在这种情况下，请为使用低带宽连接的用户创建单独的策略，以便不会对使用高带宽连接的用户产生不利影响。

有关设置的详细信息，请参阅音频策略设置。请务必在用户设备上启用“客户端音频设置”。

音频播放和录制件带宽指南：

- 高品质（默认）
  - 比特率：约 100 kbps（最小值为 75 kbps，最大值为 175 kbps）用于播放/约 70 kbps 用于麦克风捕获
  - 声道数量：2（立体声）用于播放，1（单声道）用于麦克风捕获
  - 频率：44100 Hz
  - 位深度：16 位
- 中等质量（推荐用于 VoIP）
  - 比特率：约 16 kbps（最小值为 20 kbps，最大值为 40 kbps）用于播放，约 16 kbps 用于麦克风捕获
  - 通道数量：1（单声道）用于播放和捕获
  - 频率：16000 Hz（宽带）
  - 位深度：16 位
- 低质量
  - 比特率：约 11 kbps（最小值为 10 kbps，最大值为 25 kbps）用于播放，约 11 kbps 用于麦克风捕获
  - 通道数量：1（单声道）用于播放和捕获
  - 频率：8000 Hz（窄带）
  - 位深度：16 位

客户端音频重定向

要允许用户在用户设备上通过扬声器或其他音频设备，接收来自服务器上应用程序的音频，请将客户端音频重定向设置保留为允许。这是默认值。

客户端音频映射会造成服务器及网络的负载过大。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“客户端音频设置”。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

客户端麦克风重定向

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，请将客户端麦克风重定向设置保留为其默认值（允许）。

出于安全考虑，当不受用户信任的服务器尝试访问麦克风时，用户设备会向其用户发出警报。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 Workspace 应用程序上禁用此警报。

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“客户端音频设置”。

音频即插即用

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，启用此设置。音频即插即用功能可识别音频设备。这些设备即使是在启动了用户会话之后才插入，也能够被识别。

此设置仅适用于 Windows 多会话操作系统计算机。

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和音频重定向带宽限制百分比

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“客户端音频设置”。

通过 **UDP** 协议的音频实时传输和音频 **UDP** 端口范围

默认情况下，“通过用户数据报协议 (UDP) 的音频实时传输”设置为“允许”（如果在安装时选择）。它将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。如果发生网络拥堵或数据包丢失，我们建议为音频配置 UDP/RTP 协议，以确保可能的最佳用户体验。对于软件电话应用程序等任意实时音频，首选使用 UDP 音频而不是 EDT。UDP 允许在不重新传输的情况下存在数据包丢失，从而确保不会对数据包丢失率较高的连接增加任何延迟。

> 重要：
>
> 如果未安装 Citrix Gateway，则不加密通过 UDP 传输的音频数据。如果 Citrix Gateway 配置为访问 Citrix Virtual Apps and Desktops 资源，则端点设备与 Citrix 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 Windows 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，范围为 16500 到 16509。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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“客户端音频设置”。

通过 UDP 传输音频需要 Windows VDA。有关 Linux VDA 上支持的策略，请参阅策略支持列表。

用户设备的音频设置策略

1. 按照配置组策略对象管理模板进行操作，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 Workspace >** 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。请使用选定的选项启用音频重定向。
   - 已禁用。禁用音频重定向。
4. 如果选择启用，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 Citrix Gateway 使用 UDP 音频，请选择 **Allow Real-Time Transport Through gateway**（允许通过网关实时传输）。为 Citrix Gateway 配置 DTLS。有关详细信息，请参阅本文。

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，请使用 StoreFront 中的 default.ica 属性启用 UDP 音频。例如，针对自带设备或家用计算机。

1. 在 StoreFront 计算机上，使用编辑器（例如记事本）打开 C:\inetpub\wwwroot\Citrix\<Store Name>\App_Data\default.ica。
2. 在 [Application] 部分下创建以下条目。

```
; This text enables Real-Time Transport

EnableRtpAudio=true

; This text allows Real-Time Transport Through gateway

EnableUDPThroughGateway=true

; This text sets audio quality to Medium

AudioBandwidthLimit=1

; UDP Port range

RtpAudioLowestPort=16500

RtpAudioHighestPort=16509
```

如果您通过编辑 default.ica 启用用户数据报协议 (UDP) 音频，UDP 音频将对使用该存储的所有用户启用。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

在多媒体会议期间避免产生回声

用户参与音频或视频会议时可能会听到回声。通常当扬声器和麦克风彼此间距离太近的时候会产生回声。因此，我们建议您在音频和视频会议中使用耳机。

HDX 提供了一个回声消除选项（默认情况下处于启用状态），可以将任何回声降低到最小。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。请确保这些设备相互之间的距离适中。

您可以更改注册表设置以禁用回声消除功能。有关信息，请参阅通过注册表管理的功能列表中的在多媒体会议期间避免产生回声。

软件电话

软件电话是指用作电话界面的软件。可以使用软件电话通过 Internet 从计算机或其他智能设备进行通话。使用软件电话时，可以拨打电话号码以及使用屏幕执行与电话有关的其他功能。

Citrix Virtual Apps and Desktops 支持使用多种备用方法来提供软件电话。

- 控制模式。托管的软件电话控制物理电话机。在此模式下，所有音频流量都不通过 Citrix Virtual Apps and Desktops 服务器。
- **HDX RealTime** 优化的软件电话支持（推荐）。媒体引擎在用户设备上运行，并且 IP 语音流量对端传输。例如，请参阅：
  - Microsoft Teams 的 HDX 优化
  - HDX RealTime Optimization Pack，优化了 Microsoft Skype for Business 的交付。
  - Cisco Jabber Softphone for VDI（以前称为 VXME）
  - 适用于 VDI 的 Cisco Webex Meetings
  - Avaya VDI Equinox（以前称为 VDI Communicator）
  - 缩放 VDI 插件
  - Genesys PureEngage Cloud
  - Nuance Dragon PowerMic 听写设备
- 本地应用程序访问。这是一项 Citrix Virtual Apps and Desktops 功能，允许软件电话等应用程序在 Windows 用户设备上本地运行。Windows 用户设备尚未显示与其虚拟/已发布的桌面无缝集成。此功能会将所有音频处理卸载到用户设备。有关详细信息，请参阅本地应用程序访问和 URL 重定向。
- **HDX RealTime** 通用软件电话支持。通过 ICA 的 IP 语音。

通用软件电话支持

通用软件电话支持功能允许您在数据中心中的 XenApp 或 XenDesktop 上托管未经修改的软件电话。音频流量通过 Citrix ICA 协议（最好使用 UDP/RTP）传输到运行 Citrix Workspace 应用程序的用户设备。

通用软件电话支持是 HDX RealTime 的一项功能。此软件电话交付方法在以下情况下特别有用：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 优化后的用于交付软件电话的解决方案不可用，并且用户未登录能够使用本地应用程序访问的 Windows 设备。
- 优化后的软件电话交付所需的媒体引擎尚在用户设备上安装，或者该引擎不适用于用户设备上运行的操作系统版本。在这种情况下，通用 HDX RealTime 可提供重要的回退解决方案。

使用 Citrix Virtual Apps and Desktops 时有两个软件电话交付注意事项：

- 如何将软件电话应用程序交付到虚拟/已发布的桌面。
- 如何将音频传输到用户的耳机、麦克风和扬声器或者 USB 电话机，以及如何从这些设备传输音频。

Citrix Virtual Apps and Desktops 包括多种支持通用软件电话交付的技术：

- 针对语音优化的编解码器，实现了实时音频和带宽的快速编码。
- 低延迟音频堆栈。
- 服务器端抖动缓冲区，用于在网络延迟波动时使音频趋于平稳。
- 面向服务质量的数据包标记（DSCP 和 WMM）。
  - 面向 RTP 数据包的 DSCP 标记（第 3 层）
  - 面向 Wi-Fi 的 WMM 标记

适用于 Windows、Linux、Chrome 和 Mac 的各 Citrix Workspace 应用程序版本也具备 IP 语音功能。适用于 Windows 的 Citrix Workspace 应用程序提供以下功能：

- 客户端抖动缓冲区 - 即使在网络延迟波动时也能确保音频平稳传输。
- 回声消除 - 允许声音在未使用耳机的工作人员的麦克风与扬声器之间的距离内大幅波动。
- 音频即插即用 - 在启动会话之前不需要插入音频设备。可以随时插入这些设备。
- 音频设备路由 - 用户可以通过耳机的声音路径将铃声直接传输到扬声器。
- 多流 ICA - 启用通过网络完成的、基于服务质量的灵活路由。
- ICA 支持四股 TCP 数据流和两股 UDP 数据流。其中一股 UDP 数据流支持通过 RTP 传输的实时音频。

有关 Citrix Workspace 应用程序功能的汇总，请参阅 Citrix Receiver 功能列表。

系统配置建议

客户端硬件和软件：
要提供最佳音频质量，我们建议您安装最新版本的 Citrix Workspace 应用程序，并使用具有回声消除 (AEC) 功能的优质耳机。适用于 Windows 的 Citrix Workspace 应用程序、适用于 Linux 的 Citrix Workspace 应用程序和适用于 Mac 的 Citrix Workspace 应用程序的各版本均支持 IP 语音。此外，Dell Wyse 提供对 ThinOS (WTOS) 的 IP 语音支持。

CPU 注意事项：
请监视 VDA 上的 CPU 使用率以确定是否有必要向每个虚拟机分配两个虚拟 CPU。实时语音和视频属于数据密集型数据。配置两个虚拟 CPU 可以缩短线程切换延迟。因此，我们建议您在 Citrix Virtual Desktops VDI 环境中配置两个 vCPU。

配置两个虚拟 CPU 并不一定意味着将物理 CPU 的数量增加两倍，因为物理 CPU 可以跨会话共享。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Gateway Protocol (CGP) 也会增加 CPU 占用量，该协议用于会话可靠性功能。在高质量的网络连接中，您可以在 VDA 中禁用此功能以降低 CPU 占用量。在功能强大的服务器上，可能没有必要执行上述任何步骤。

UDP 音频：
通过 UDP 传输的音频对网络拥挤和数据包丢失情况的容忍力非常强。我们建议您在可用时使用 UDP 来代替 TCP。

LAN/WAN 配置：
正确的网络配置对提供优质的实时音频质量非常重要。通常情况下，必须配置虚拟 LAN (VLAN)，因为过量的广播数据包会引入抖动。启用了 IPv6 的设备可能会生成许多广播数据包。如果不需要 IPv6 支持，可以在这些设备上禁用 IPv6。请进行配置以支持服务质量。

使用 *WAN* 连接时的设置：
可以通过 LAN 和 WAN 连接使用语音聊天。在 WAN 连接中，音频质量取决于连接中的延迟、数据包丢失和抖动。如果在 WAN 连接中向用户提供软件电话，我们建议您在数据中心与远程办公室之间使用 NetScaler SD-WAN。这样可以维护高服务质量。NetScaler SD-WAN 支持多流 ICA，包括 UDP。此外，对于单个 TCP 数据流，可以区分各种 ICA 虚拟通道的优先级，以确保高优先级的实时音频数据受到优先处理。

使用 Director 或 HDX Monitor 验证您的 HDX 配置。

远程用户连接：
Citrix Gateway 支持 DTLS，以在本机提供 UDP/RTP 流量（在 TCP 中无封装）。
双向打开防火墙，以便 UDP 流量通过端口 443 传输。

编解码器选择和带宽占用量：
我们建议在用户设备与数据中心中的 VDA 之间使用语音优化编解码器设置（也称为“中”质量音频）。在 VDA 平台与 IP-PBX 之间，软件电话使用编解码器的配置和协商结果。例如：

- G711 提供出色的语音质量，但带宽要求为每个通话 80 kbps 到 100 kbps（基于网络第 2 层开销）。
- G729 提供出色的语音质量，但带宽要求为每个通话 30 kbps 到 40 kbps（基于网络第 2 层开销）。

向虚拟桌面交付软件电话应用程序

可以通过两种方法向 XenDesktop 虚拟桌面交付软件电话：

- 可以在虚拟桌面映像中安装该应用程序。
- 可以使用 Microsoft App-V 通过流技术将该应用程序推送到虚拟桌面。此方法具有易管理的优势，因为虚拟桌面映像保持得非常整洁。通过流技术推送到虚拟桌面后，该应用程序将在该环境中运行，就像按常规方式安装一样。并非所有应用程序都与 App-V 兼容。

向用户设备传输音频以及从用户设备传输音频

通用 HDX RealTime 支持两种向用户设备传输音频以及从用户设备传输音频的方法：

- **Citrix** 音频虚拟通道。我们通常建议使用 Citrix 音频虚拟通道，因为它是专门针对音频传输而设计的。
- 通用 **USB** 重定向。如果用户设备位于连接回 Citrix Virtual Apps and Desktops 服务器的 LAN 或类似 LAN 的连接中，则支持带按钮或显示屏（或两者）的音频设备、人体学接口设备 (HID)。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix 音频虚拟通道

双向 Citrix 音频虚拟通道 (CTXCAM) 允许音频通过网络有效传输。通用 HDX RealTime 接收来自用户的耳机或麦克风的音频，并对其进行压缩。然后，通过 ICA 将其发送到虚拟桌面上的软件电话应用程序。类似地，软件电话的音频输出将被压缩，并在另一个方向发送到用户的耳机或扬声器。此压缩与软件电话本身使用的压缩无关（例如 G.729 或 G.711）。此压缩是使用针对语音优化的编解码器完成的（“中”质量）。其特性对 IP 语音而言非常完美。此编解码器的特性是编码时间非常快，并且最高仅占用大约 56 千位/秒的网络带宽（每个方向 28 Kbps）。必须在 Studio 控制台中明确选择此编解码器，因为这不是默认音频编解码器。默认编解码器为高清音频编解码器（“高”质量）。此编解码器非常适用于高保真立体声声道，但与针对语音优化的编解码器相比，其编码速度较慢。

通用 ***USB*** 重定向

Citrix 通用 USB 重定向技术（CTXGUSB 虚拟通道）提供通用的远程连接 USB 设备的方法，包括复合设备（音频加 HID）以及常时等量 USB 设备。此方法仅限于通过 LAN 连接的用户。原因是 USB 协议通常对网络延迟非常敏感，并且需要占用大量的网络带宽。常时等量 USB 重定向在使用部分软件电话时非常适用。此重定向提供出色的语音质量和低延迟。但是，Citrix 音频虚拟通道是首选，因为该通道已针对音频流量优化。主要的例外情况发生在使用带按钮的音频设备时。例如，连接到通过 LAN 连接到数据中心的用户设备的 USB 电话。在这种情况下，通用 USB 重定向通过将信号发送回软件电话来支持电话机或耳机上用于控制功能的按钮。对于在设备上本地使用的按钮而言，这并不是问题。

限制

在您的客户端上安装音频设备，启用音频重定向，然后启动 RDS 会话。音频文件可能无法播放，并显示一条错误消息。

解决方法：在 RDS 计算机上添加注册表项，然后重新启动计算机。有关信息，请参阅通过注册表管理的功能列表中的音频限制。

浏览器内容重定向

January 21, 2022

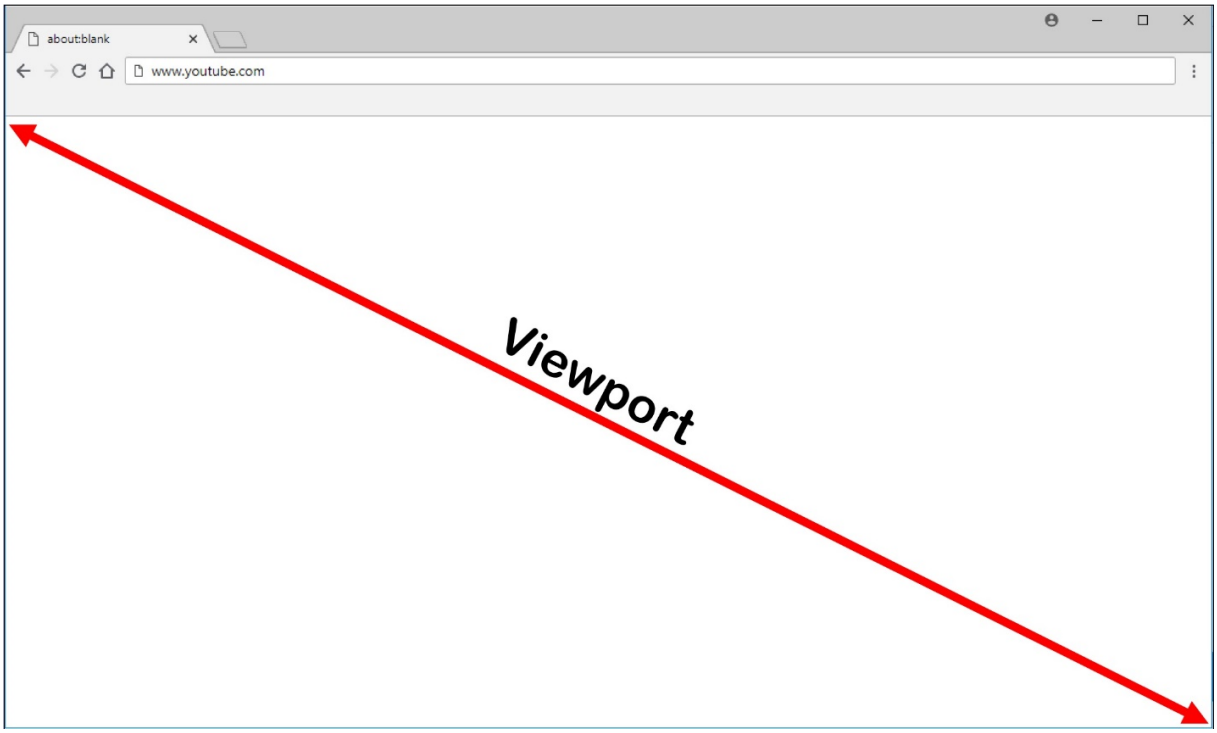
浏览器内容重定向会阻止在 VDA 端呈现允许列表中的 Web 页面。此功能使用适用于 Windows 的 Citrix Workspace 应用程序或适用于 Linux 的 Citrix Workspace 应用程序在客户端实例化相应的呈现引擎，该引擎会从 URL 提取 HTTP 和 HTTPS 内容。

> 注意：
>
> 可以使用阻止列表指定要重定向到 VDA 端（以及不在客户端重定向）的 Web 页面。

此叠加 Web 布局引擎在端点设备上运行，而非在 VDA 上运行，并且使用端点 CPU、GPU、RAM 和网络。

只有浏览器视口会进行重定向。视口是浏览器中显示内容的矩形区域。视口不包含地址栏、收藏夹工具栏、状态栏等内容。这些项目位于用户界面中，仍在 VDA 中的浏览器上运行。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



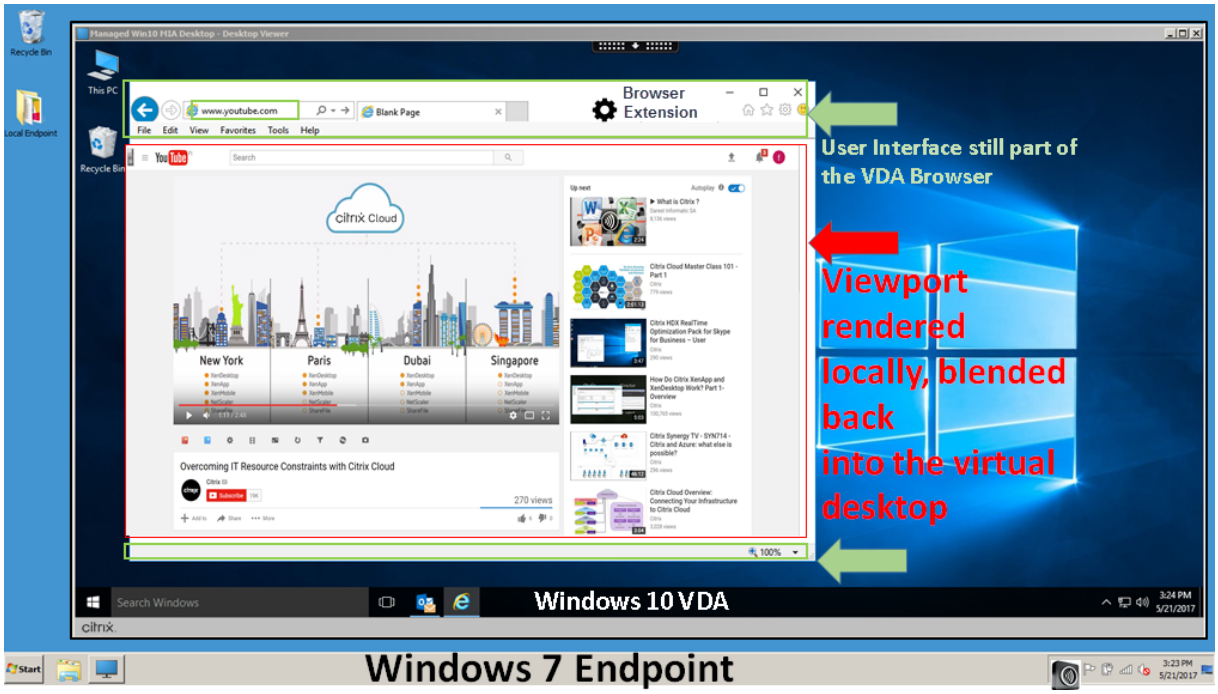
1. 配置用于指定包含可重定向的允许列表中的 URL 的访问控制列表或禁用了特定 URL 路径重定向的阻止列表中的 Studio 策略。为了使 VDA 上的浏览器检测用户正在导航到的 URL 与允许列表匹配还是与阻止列表不匹配，某个浏览器扩展将执行比较。适用于 Internet Explorer 11 的浏览器扩展程序 (BHO) 包含在安装介质中并自动安装。对于 Chrome，浏览器扩展程序在 Chrome 网上应用店中提供，可以使用组策略和 ADMX 文件进行部署。Chrome 扩展程序基于每个用户安装。不需要更新黄金映像即可添加或删除扩展程序。
2. 如果在允许列表中找到了一个匹配项（例如 `https://www.mycompany.com/`），并且没有与阻止列表中的 URL 匹配的项（例如 `https://www.mycompany.com/engineering`），虚拟通道 (CTXCSB) 将指示 Citrix Workspace 应用程序需要重定向并中继该 URL。然后，Citrix Workspace 应用程序会实例化一个本地呈现引擎并显示此 Web 站点。
3. 之后，Citrix Workspace 应用程序会将此 Web 站点无缝融入虚拟桌面浏览器内容区域中。

徽标的颜色指定 Chrome 扩展程序的状态。其颜色为以下三种颜色之一：

- 绿色：活动并连接。
- 灰色：在当前选项卡上不活动/空闲。
- 红色：已损坏/不运行。

可以使用扩展程序菜单中的选项来调试日志记录。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



下面是 Citrix Workspace 应用程序提取内容的方式的几种情况：

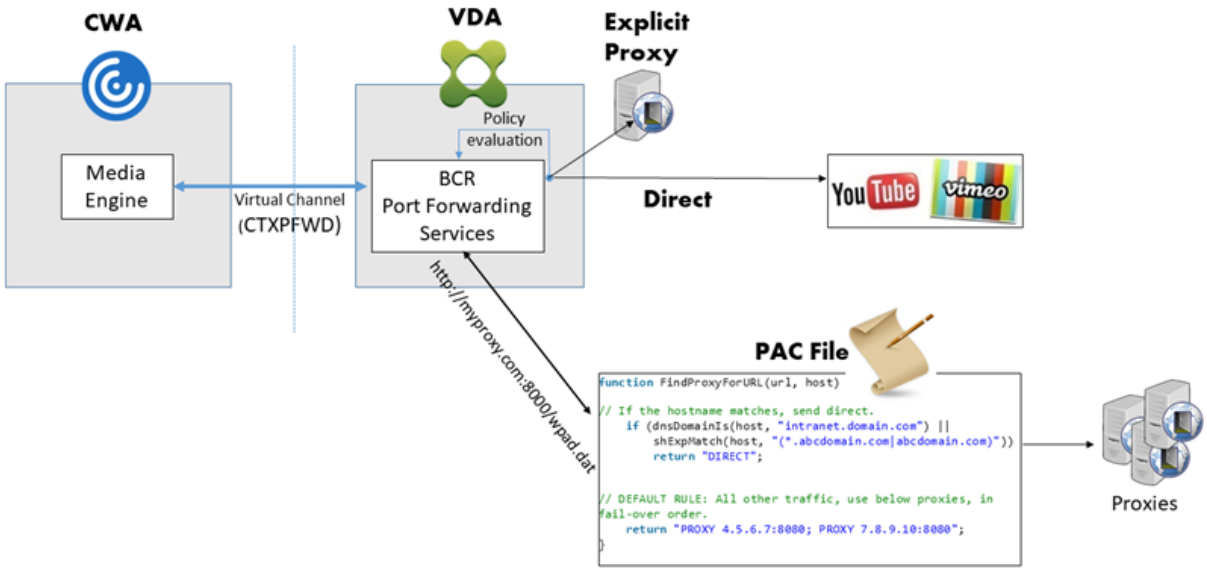
- 服务器提取和服务器呈现：由于没有将站点添加到允许列表或重定向失败，因此没有重定向。我们将回退到在 VDA 上呈现 Web 页面，并使用 Thinwire 来远程显示图形。使用策略来控制回退行为。VDA 上的 CPU、RAM 和带宽占用量较高。
- 服务器提取和客户端呈现：Citrix Workspace 应用程序使用虚拟通道 (CTXPFWD) 通过 VDA 连接 Web 服务器并从中提取内容。如果客户端无法访问 Internet，则此选项很有用（例如瘦客户端）。VDA 上的 CPU 和 RAM 占用量较低，但在 ICA 虚拟通道上占用带宽。

  此方案有三种操作模式。术语代理是指 VDA 为获取 Internet 访问权限而访问的代理设备。

  可选择的策略选项：

  - 显式代理 - 如果您的数据中心中有单个显式代理。
  - 直接或透明 - 如果您没有代理，或者您使用透明代理。
  - PAC 文件 - 如果您依赖 PAC 文件，以便 VDA 中的浏览器可以自动选择适当的代理服务器来获取指定的 URL。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

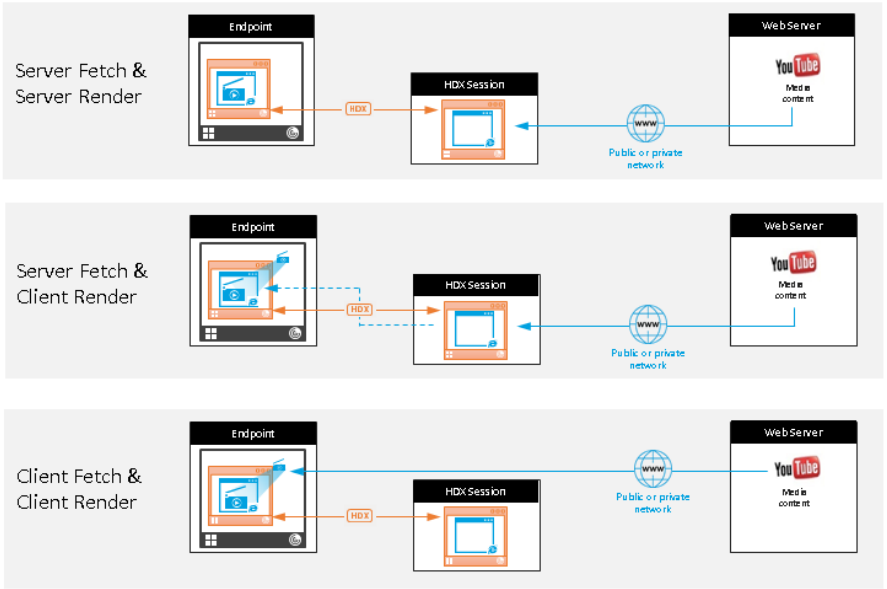


- 客户端提取和客户端呈现：由于 Citrix Workspace 应用程序直接连接 Web 服务器，因此需要访问 Internet。在此情况下，会从 XenApp 和 XenDesktop 站点卸载所有网络、CPU 和 RAM 使用量。

  优势：

  - 更出色的最终用户体验（自适应比特率 (ABR)）
  - 降低了 VDA 资源使用量 (CPU/RAM/IO)
  - 降低了带宽占用量

Redirection scenarios



Benefits:

- Better end user experience (Adaptive Bit Rate (ABR))
- Reduced VDA resource usage (CPU/RAM/IO)
- Reduced bandwidth consumption

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

回退机制：

客户端重定向有时可能会失败。例如，如果客户端计算机无法直接访问 Internet，则可能会向 VDA 返回一条错误响应。在这种情况下，VDA 上的浏览器可以在服务器上重新加载并呈现页面。

可以使用现有 **Windows Media** 回退预防策略禁止服务器呈现视频元素。请将此策略设置为仅在客户端上播放所有内容或仅在客户端上播放客户端可访问的内容。如果客户端重定向失败，这些设置将阻止视频元素在服务器上播放。仅当启用了浏览器内容重定向，并且访问控制列表策略中包含回退的 URL 时，此策略才生效。URL 不能位于阻止列表策略中。

系统要求：

Windows 端点：

- Windows 10
- 适用于 Windows 的 Citrix Workspace 应用程序 1809 或更高版本

> 注意：
>
> 适用于 Windows 的 Citrix Workspace 应用程序 1912 LTSR 以及 Citrix Workspace 应用程序 1912 LTSR 的所有累积更新均不支持浏览器内容重定向。

Linux 端点：

- 适用于 Linux 的 Citrix Workspace 应用程序 1808 或更高版本
- 瘦客户端端点必须包括 WebKitGTK+

Citrix Virtual Apps and Desktops 7 1808 或更高版本以及 XenApp 和 XenDesktop 7.15 CU5 或更高版本：

- VDA 操作系统：Windows 10（最低版本 1607）、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019
- VDA 上的浏览器：
  - Google Chrome v66 或更高版本（Chrome 要求安装用户端点上适用于 Windows 的 Citrix Workspace 应用程序 1809 或更高版本、Citrix Virtual Apps and Desktops 7 1808 VDA 或更高版本以及浏览器内容重定向扩展程序）
  - Internet Explorer 11，并配置以下选项：
    - 在 **Internet** 选项 > 高级 **>** 安全下，取消选中增强保护模式
    - 在 **Internet** 选项 **>** 高级 **>** 浏览下，选中启用第三方浏览器扩展

故障排除

有关故障排除信息，请参阅知识中心文章 https://support.citrix.com/article/CTX230052。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

浏览器内容重定向 **Chrome** 扩展程序

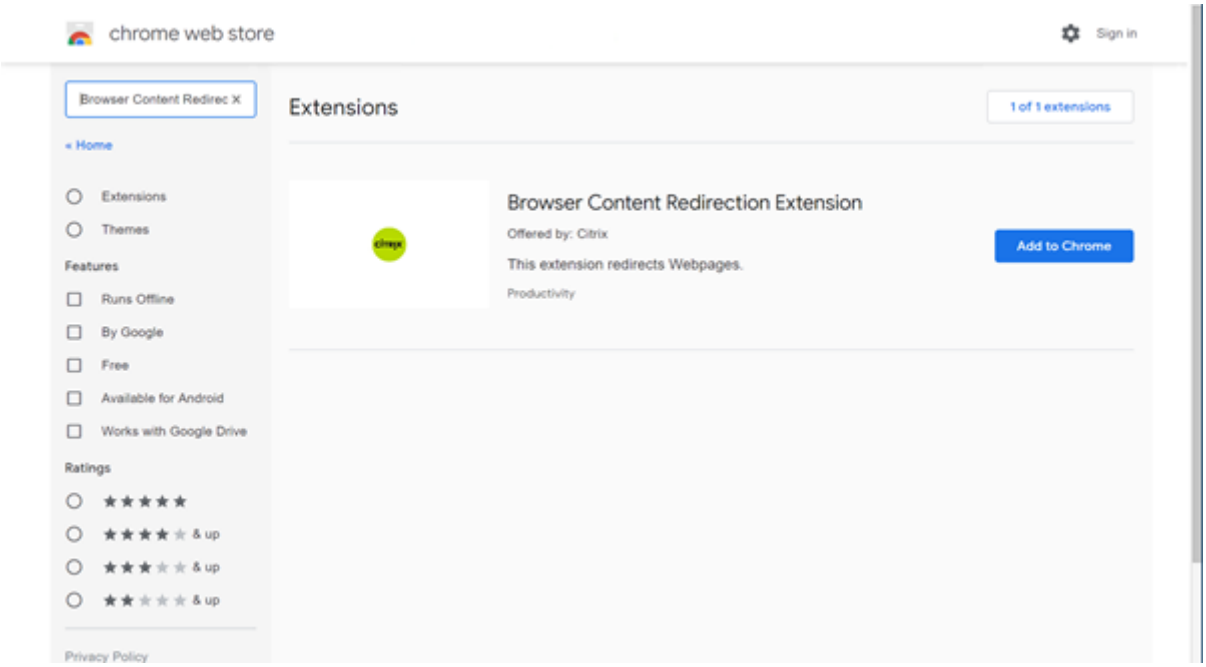
要在 Chrome 中使用浏览器内容重定向，请从 Chrome 网上应用店中添加浏览器内容重定向扩展程序。在 Citrix Virtual Apps and Desktops 环境中单击添加到 **Chrome**。

用户的客户端计算机中不需要此扩展程序，仅在 VDA 中需要。

系统要求

- Chrome v66 或更高版本
- 浏览器内容重定向扩展程序
- Citrix Virtual Apps and Desktops 7 1808 或更高版本
- 适用于 Windows 的 Citrix Workspace 应用程序 1809 或更高版本

> 注意：
>
> 适用于 Windows 的 Citrix Workspace 应用程序 1912 LTSR 以及 Citrix Workspace 应用程序 1912 LTSR 的所有累积更新均不支持浏览器内容重定向。



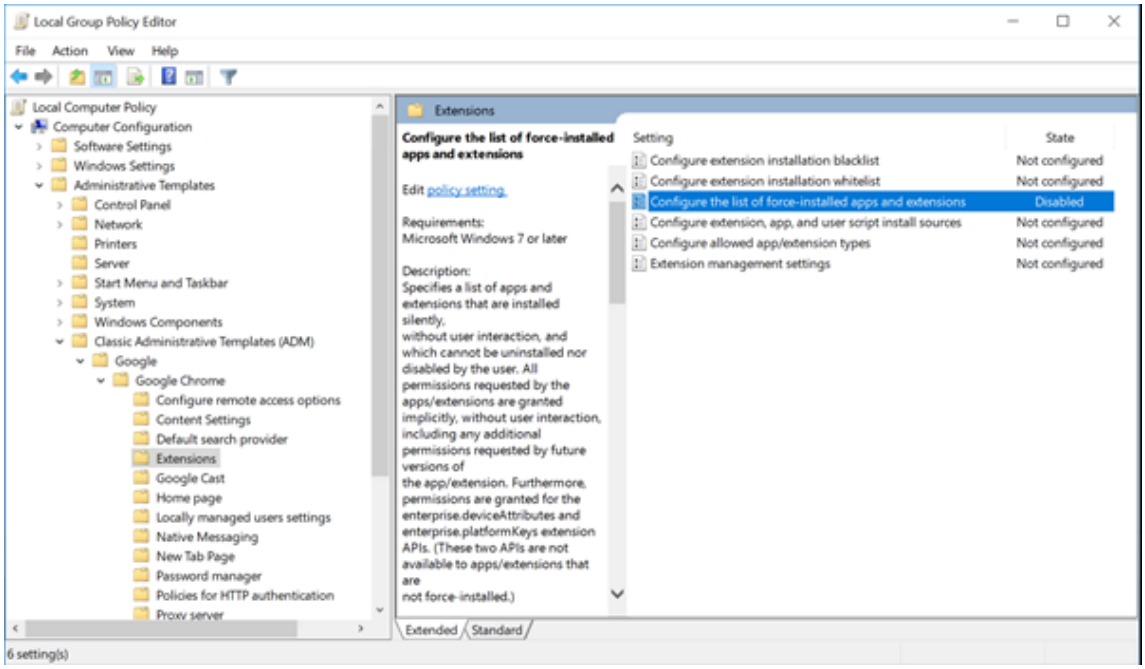
此方法适用于单个用户。要将扩展程序部署到贵组织中的一大组用户，请使用组策略部署该扩展程序。

使用组策略部署扩展程序

1. 将 Google Chrome ADMX 文件导入到您的环境中。有关下载策略模板并在组策略编辑器中安装和配置这些模板的信息，请参阅在托管 PC 上设置 Chrome 浏览器策略。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

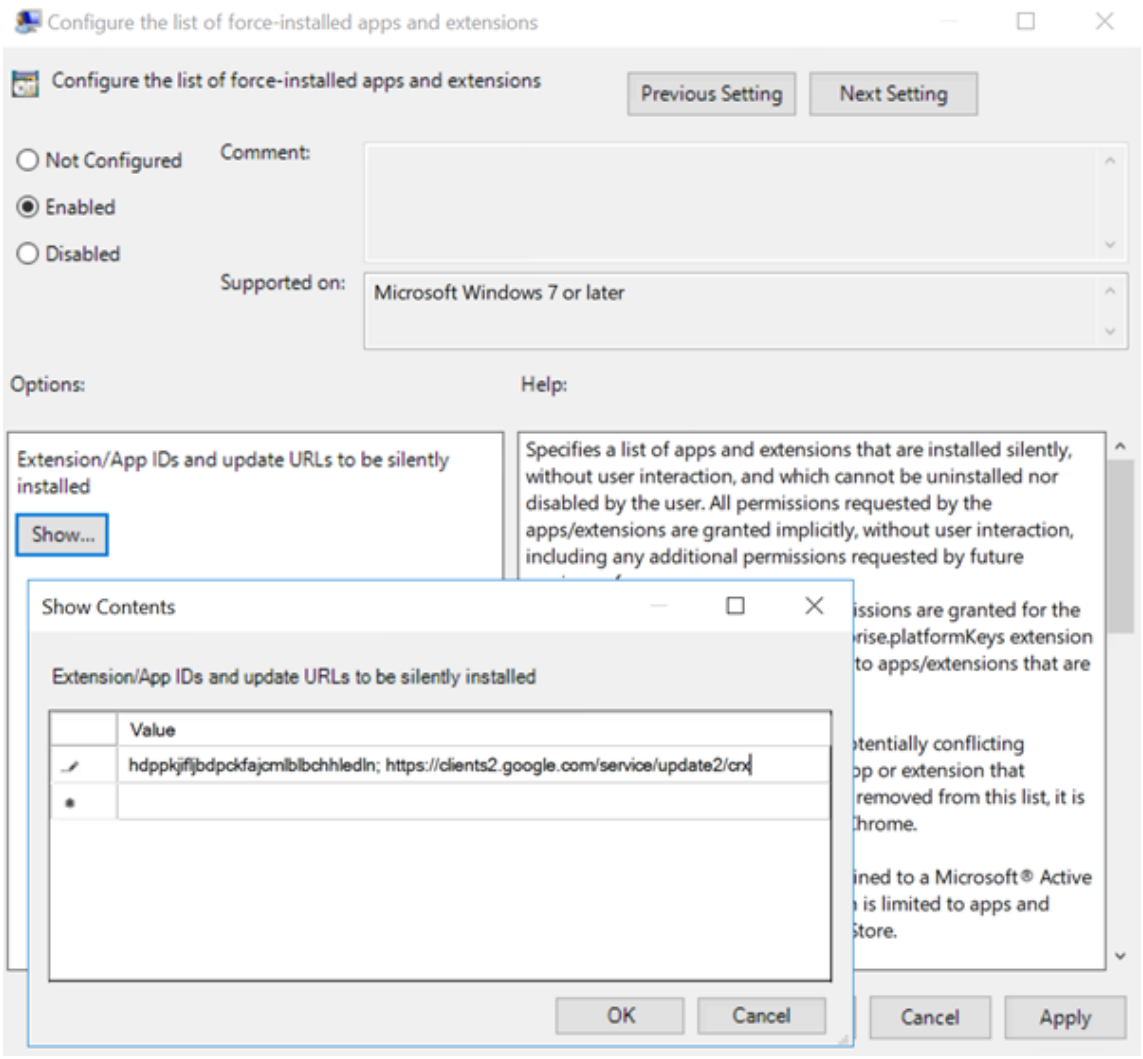
2. 打开组策略管理控制台，转至用户配置 \ 管理模板 \ 经典管理模板 **(ADM) \ Google \ Google Chrome ** 扩展程序。启用 **Configure the list of force-installed apps and extensions**（配置强制安装的应用程序和扩展程序列表）设置。



3. 单击显示，键入以下字符串，该字符串与扩展程序 ID 相对应。更新浏览器内容重定向扩展程序的 URL。

```
hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. 应用设置并执行 **gpudate** 刷新后，用户将自动接收扩展程序。如果在用户的会话中启动了 Chrome 浏览器，则扩展程序已应用并且无法将其删除。

   扩展程序的所有更新都将通过在设置中指定的更新 URL 自动安装在用户的计算机上。

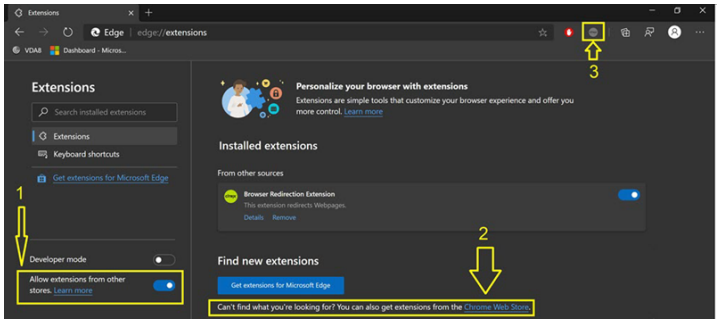
   如果 **Configure the list of force-installed apps and extensions**（配置强制安装的应用程序和扩展程序列表）设置为 **Disabled**（已禁用），扩展程序将自动从 Chrome 中删除（针对所有用户）。

浏览器内容重定向 **Edge Chromium** 扩展程序

要在 Edge 中安装浏览器内容重定向扩展程序，请确保您安装了 **83.0.478.37** 或更高版本的 Edge 浏览器。

1. 单击菜单中的扩展选项，然后打开 **Allow extensions from other stores**（允许来自其他应用商店的扩展）。
2. 单击 **Chrome** 网上应用店链接，扩展程序将显示在右上角的栏中。
   有关 Microsoft Edge 扩展的详细信息，请参阅扩展。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



浏览器内容重定向和 DPI

在用户的计算机上使用浏览器内容重定向时，如果 DPI（缩放）设置为超过 100% 的任何设置，重定向的浏览器内容屏幕将错误地显示。为避免出现此问题，请不要在使用浏览器内容重定向时设置 DPI。避免此问题的另一种方法是，通过在用户的计算机上创建注册表项来禁用适用于 Chrome 的浏览器内容重定向 GPU 加速。有关信息，请参阅通过注册表管理的功能列表中的浏览器内容重定向和 DPI。

使用集成 Windows 身份验证进行单点登录

浏览器内容重定向增强了叠加功能，以使用协商方案对与 VDA 位于同一域中且配置了集成 Windows 身份验证 (IWA) 的 Web 服务器进行身份验证。

默认情况下，浏览器内容重定向使用基本身份验证方案，该方案要求用户在每次访问 Web 服务器时使用其 VDA 凭据进行身份验证。对于单点登录，您可以启用浏览器内容重定向集成 **Windows** 身份验证支持策略设置，也可以在 VDA 上创建注册表项。

在启用单点登录之前，请完成以下操作：

- 将 Kerberos 基础结构配置为针对根据主机名构建的服务主体名称 (SPN) 发出票证。例如，HTTP/serverhostname.com。
- 对于服务器提取：在服务器提取模式下使用浏览器内容重定向时，请确保在 VDA 上正确配置了 DNS。
- 对于客户端提取：在客户端提取模式下使用浏览器内容重定向时，请确保在客户端设备上正确配置了 DNS，并且允许从叠加到 Web 服务器 IP 地址的 TCP 连接。

要使用浏览器内容重定向策略配置单点登录，请参阅浏览器内容重定向集成 Windows 身份验证支持设置。

或者，您可以通过在 VDA 上添加注册表项来启用到 Web 服务器的单点登录。有关信息，请参阅通过注册表管理的功能列表中的使用集成 Windows 身份验证进行单点登录，以实现浏览器内容重定向。

用户代理请求标头

用户代理标头有助于识别从浏览器内容重定向发送的 HTTP 请求。配置代理和防火墙规则时，此设置会非常有用。例如，如果服务器阻止从浏览器内容重定向发送的请求，则可以创建包含用户代理标头的规则以绕过某些要求。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

只有 Windows 设备支持用户代理请求标头。

默认情况下，用户代理请求标头字符串处于禁用状态。要为客户端呈现的内容启用用户代理标头，请使用注册表编辑器。有关信息，请参阅通过注册表管理的功能列表中的用户代理请求标头。

HDX 视频会议和网络摄像机视频压缩

January 21, 2022

> 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。

虚拟会话中运行的应用程序可以通过使用 HDX 网络摄像机视频压缩或 HDX 即插即用通用 USB 重定向来使用网络摄像机。可使用 **Citrix Workspace** 应用程序 **>** 首选项 **>** 设备在模式之间切换。Citrix 建议始终尽可能使用 HDX 网络摄像机视频压缩功能。仅当 HDX 视频压缩存在应用程序兼容性问题时或需要网络摄像机的高级本机功能时，才建议使用 HDX 通用 USB 重定向。为了获得更好的性能，Citrix 建议 Virtual Delivery Agent 至少有两个虚拟 CPU。

要阻止用户切换 HDX 网络摄像机视频压缩功能，请通过使用 **ICA** 策略设置 **> USB** 设备策略设置下的策略设置禁用 USB 设备重定向。Citrix Workspace 应用程序用户可以通过选择 Desktop Viewer 麦克风和网络摄像机设置不使用我的麦克风或网络摄像机来覆盖默认行为。

HDX 网络摄像机视频压缩

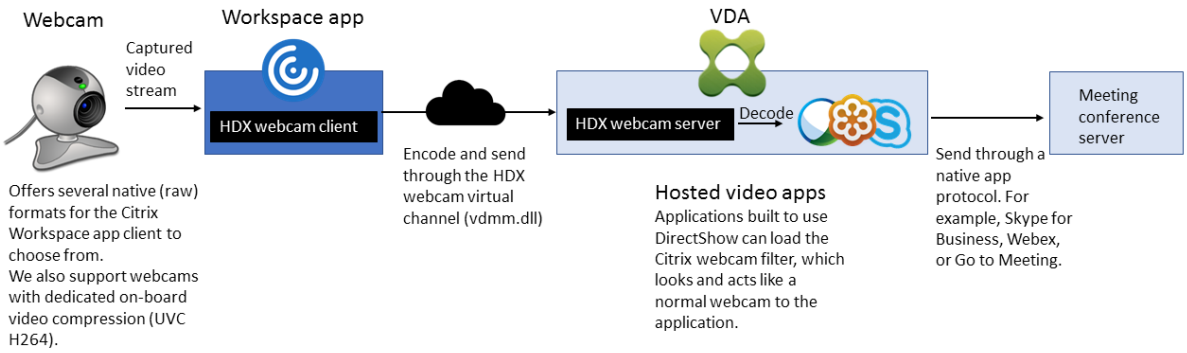
HDX 网络摄像机视频压缩也称为优化网络摄像机模式。这种类型的网络摄像机视频压缩将 H.264 视频直接发送到在虚拟会话中运行的视频会议应用程序。为了优化 VDA 资源，HDX 网络摄像机压缩不会对网络摄像机视频进行编码、转码和解码。默认情况下启用此功能。

要禁用从服务器到视频会议应用程序的直接视频流，请在 VDA 上将注册表项设置为 0。有关信息，请参阅通过注册表管理的功能列表中的网络摄像机视频压缩。

如果禁用适用于通过流技术推送视频资源的默认功能，HDX 网络摄像机视频压缩将使用属于客户端操作系统的多媒体框架技术截获来自捕获设备的视频，并对其进行转码和压缩。捕获设备的制造商提供插入操作系统内核流技术推送体系结构的驱动程序。

客户端处理与网络摄像机的通信。之后，客户端仅将视频发送到可以正确显示它的服务器。服务器不能直接与网络摄像机通信，但其集成可在您的桌面中为您提供相同的体验。Workspace 应用程序会压缩视频以节省带宽，并在 WAN 场景中提高恢复能力。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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）。

- 多媒体会议
- Windows Media 重定向

如果网络摄像机支持硬件编码，默认情况下 HDX 视频压缩功能将采用硬件编码。硬件编码占用的带宽可能高于软件编码。要强制执行软件压缩，请在客户端上编辑注册表项。有关信息，请参阅通过注册表管理的功能列表中的网络摄像机软件压缩。

HDX 网络摄像机视频压缩要求

HDX 网络摄像机视频压缩支持以下版本的 Citrix Workspace 应用程序：

平台	处理器
适用于 Windows 的 Citrix Workspace 应用程序	适用于 Windows 的 Citrix Workspace 应用程序支持 XenApp 和 XenDesktop 7.17 及更高版本上面向 32 位和 64 位应用程序的网络摄像机视频压缩。在早期版本中，适用于 Windows 的 Citrix Workspace 应用程序仅支持 32 位应用程序。
适用于 Mac 的 Citrix Workspace 应用程序	适用于 Mac 的 Citrix Workspace 应用程序 2006 或更高版本支持 XenApp 和 XenDesktop 7.17 及更高版本上面向 64 位应用程序的网络摄像机视频压缩。在早期版本中，适用于 Mac 的 Citrix Workspace 应用程序仅支持 32 位应用程序。
适用于 Linux 的 Citrix Workspace 应用程序	适用于 Linux 的 Citrix Workspace 应用程序仅支持虚拟桌面上的 32 位应用程序。
适用于 Chrome 的 Citrix Workspace 应用程序	由于某些 ARM Chromebook 不支持 H.264 编码，因此，只有 32 位应用程序可以使用优化的 HDX 网络摄像机视频压缩。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

基于 Media Foundation 的视频应用程序在 Windows 8.x 或更高版本以及 Windows Server 2012 R2 及更高版本上支持 HDX 网络摄像机视频重定向。有关详细信息，请参阅知识中心文章 CTX132764。

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可降低客户端的 CPU 使用率。
- 对于 HDX 网络摄像机视频压缩，请将摄像机制造商提供的网络摄像机驱动程序安装在客户端上（如果可能）。服务器上不需要安装设备驱动程序。

不同的网络摄像机提供不同的帧速率，并具有不同级别的亮度和对比度。调整网络摄像机的对比度可以显著降低上行流量。Citrix 使用以下网络摄像机进行初始功能验证：

- Microsoft LifeCam VX 模型（2000、3000、5000、7000）
- Creative Live! Cam Optia Pro
- Logitech QuickCam Messenger
- Logitech C600、C920
- HP Deluxe Webcam

要调整首选视频帧速率，请在客户端上编辑注册表项。有关信息，请参阅通过注册表管理的功能列表中的网络摄像机视频压缩帧速率。

高清网络摄像机流技术推送

服务器上的视频会议应用程序将根据支持的格式类型选择网络摄像机格式和分辨率。会话开始时，客户端将网络摄像机信息发送到服务器。从应用程序中选择一个网络摄像机。如果网络摄像机和视频会议应用程序支持高清晰度呈现，则应用程序将使用高清晰度分辨率。我们支持高达 1920x1080 的网络摄像机分辨率。

此功能需要适用于 Windows 的 Citrix Workspace 应用程序最低版本 1808 或 Citrix Receiver for Windows 最低版本 4.10。

可以使用注册表项来禁用和启用此功能。有关信息，请参阅通过注册表管理的功能列表中的高清网络摄像机流技术推送。

如果媒体类型协商失败，HDX 将回退到默认分辨率 352x288 CIF。可以使用客户端上的注册表项来配置默认分辨率。确保摄像头支持指定的分辨率。有关信息，请参阅通过注册表管理的功能列表中的高清网络摄像机分辨率。

与即插即用通用 USB 重定向相比，HDX 网络摄像机视频压缩占用的带宽显著降低，并且可以在 WAN 连接条件下很好地运行。要调整带宽，请在客户端上设置注册表项。有关信息，请参阅通过注册表管理的功能列表中的高清网络摄像机带宽。

输入以 bps 为单位的值。如果未指定带宽，视频会议应用程序将默认使用 350000 bps。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

HDX 即插即用通用 USB 重定向

HDX 即插即用通用 USB 重定向（常时等量）也称为通用网络摄像机模式。HDX 即插即用通用 USB 重定向的优势在于您不需要在瘦客户端/端点上安装驱动程序。USB 协议栈进行了虚拟化，以便插入本地客户端的任何内容都会发送到远程 VM。远程桌面的行为就像您在本机将其插入一样。Windows 桌面处理与硬件的所有交互，并且运用即插即用逻辑来查找正确的驱动程序。如果服务器上存在驱动程序，则大多数网络摄像机都可以正常使用，并且可以通过 ICA 使用。通用网络摄像机模式会占用相当多的带宽（许多 Mbps），这是因为在网络中使用 USB 协议发送未压缩的视频。

HTML5 多媒体重定向

January 21, 2022

HTML5 多媒体重定向扩展了 HDX MediaStream 的多媒体重定向功能，将 HTML5 音频和视频包括进来。由于多媒体内容联机分发（尤其是向移动设备）的增长，浏览器行业开发了更有效的音频和视频呈现方式。

Flash 曾是标准，但它需要插件、不能在所有设备上运行，并且在移动设备上运行时电池使用量较高。YouTube 和 Netflix 等公司以及 Mozilla、Google 和 Microsoft 的更高浏览器版本正在转向 HTML5，使其成为新的标准。

与专有插件相比，基于 HTML5 的多媒体具有多个优势，包括：

- 与公司无关的标准 (W3C)
- 简化了数字版权管理 (DRM) 工作流
- 提高了性能，且没有由插件引起的安全问题

HTTP 渐进式下载

HTTP 渐进式下载是支持 HTML5 的基于 HTTP 的伪流技术推送方法。在渐进式下载中，浏览器在从 HTTP Web 服务器下载单个文件（以单一质量编码）的同时播放该文件。视频接收后存储在驱动器上并从驱动器播放。如果重新观看视频，浏览器可以从缓存中加载视频。

有关渐进式下载的示例，请参阅 HTML5 视频重定向测试页面。要检查 Web 页面中的视频元素以及在 HTML5 视频标记中查找来源（mp4 容器格式），请使用您的浏览器中的开发人员工具：

HTML5 与 Flash 比较

功能	HTML5	Flash
需要专有播放器	否	是
在移动设备上运行	是	一些

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

功能	HTML5	Flash
在不同平台上的运行速度	高	慢
受 iOS 支持	是	否
资源使用情况	较少	更多
加载速度更快	是	否

要求

我们仅对 mp4 格式的渐进式下载支持重定向。我们不支持 WebM 和自适应比特率流推送技术（如 DASH/HLS）。

我们支持以下对象，并使用策略对其进行控制。有关详细信息，请参阅多媒体策略设置。

- 服务器端呈现
- 服务器提取客户端呈现
- 客户端提取和呈现

Citrix Workspace 应用程序和 Citrix Receiver 最低版本：

- 适用于 Windows 的 Citrix Workspace 应用程序 1808
- Citrix Receiver for Windows 4.5
- 适用于 Linux 的 Citrix Workspace 应用程序 1808
- Citrix Receiver for Linux 13.5

最低 VDA 浏览器版本	Windows 操作系统版本/内部版本/SP
Internet Explorer 11.0	Windows 10 x86 (1607 RS1) 和 x64 (1607 RS1)；Windows 7 x86 和 x64；Windows Server 2016 RTM 14393 (1607)；Windows Server 2012 R2
Firefox 47 手动向 Firefox 证书存储添加证书或配置 Firefox 从 Windows 可信证书存储中搜索证书。有关详细信息，请参阅https://wiki.mozilla.org/CA:AddRootToFirefox。	Windows 10 x86 (1607 RS1) 和 x64 (1607 RS1)；Windows 7 x86 和 x64；Windows Server 2016 RTM 14393 (1607)；Windows Server 2012 R2
Chrome 51	Windows 10 x86 (1607 RS1) 和 x64 (1607 RS1)；Windows 7 x86 和 x64；Windows Server 2016 RTM 14393 (1607)；Windows Server 2012 R2

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

HTML5 视频重定向解决方案的组成部分

- **HdxVideo.js** - 在 Web 站点上截获视频命令的 JavaScript 挂钩。HdxVideo.js 使用安全 WebSocket (SSL/TLS) 与 WebSocketService 通信。
- **WebSocket SSL** 证书
  - 对于 CA（根）：**Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX In-Product CA)
    位置：证书 **(**本地计算机**) >** 可信根证书颁发机构 **>** 证书。
  - 对于最终实体（叶）：**Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX Service)
    位置：证书 **(**本地计算机**) >** 个人 **>** 证书。
- **WebSocketService.exe** - 在本地系统上运行，并执行 SSL 终止和用户会话映射。TLS 安全 WebSocket 侦听 127.0.0.1 端口 9001。
- **WebSocketAgent.exe** - 在用户会话中运行，并根据 WebSocketService 命令的指示呈现视频。

如何启用 HTML5 视频重定向?

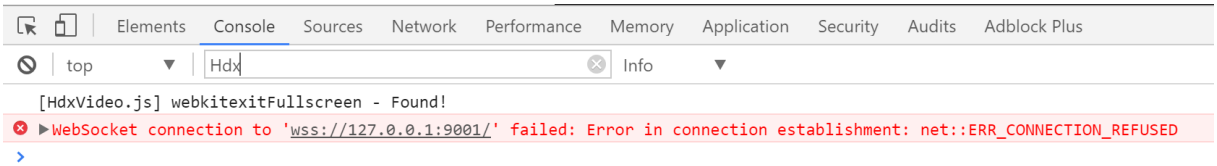
在此版本中，此功能仅用于受控 Web 页面。它要求将 HdxVideo.js JavaScript（包含在 Citrix Virtual Apps and Desktops 安装介质中）添加到提供 HTML5 多媒体内容的 Web 页面。例如，内部培训站点上的视频。

youtube.com 等基于技术（例如 HTTP Live Streaming (HLS) 和 Dynamic Adaptive Streaming over HTTP (DASH)）的 Web 站点不受支持。

有关详细信息，请参阅多媒体策略设置。

故障排除提示

Web 页面尝试运行 HdxVideo.js 时可能出现错误。如果 JavaScript 无法加载，则 HTML5 重定向机制将失败。请通过在您的浏览器的开发人员工具窗口检查控制台，确保不存在与 HdxVideo.js 有关的错误。例如：



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Microsoft Teams 的优化

March 14, 2023

> 重要：
>
> 适用于 Windows 的 Workspace 应用程序 2009.6 和适用于 Linux 的 Workspace 应用程序 2009 中的 WebRTC 媒体引擎已从 HdxTeams.exe 重命名为 HdxRtcEngine.exe

Citrix 使用 Citrix Virtual Apps and Desktops 和 Citrix Workspace 应用程序为基于桌面的 Microsoft Teams（1.2.00.31357 或更高版本）提供优化。默认情况下，我们将所有必要的组件绑定到 Citrix Workspace 应用程序和 Virtual Delivery Agent (VDA) 中。

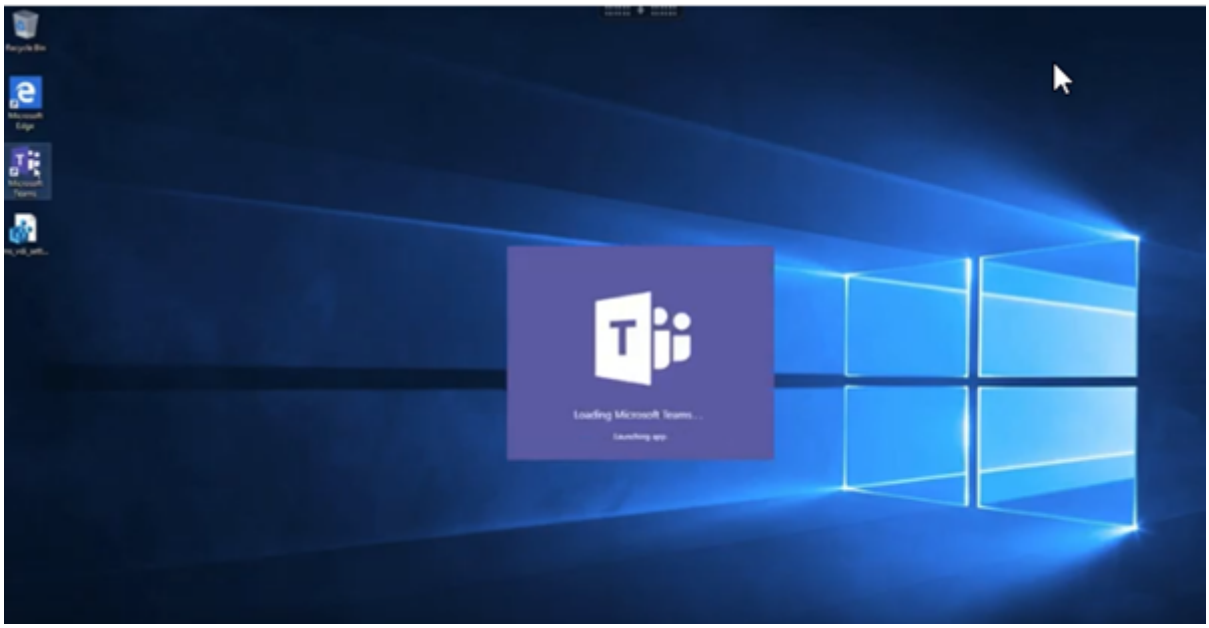
我们针对 Microsoft Teams 的优化包含一个 VDA 端 HDX 服务和 API，用于与 Microsoft Teams 托管的应用程序进行交互以接收命令。这些组件将向 Citrix Workspace 应用程序端媒体引擎打开控制虚拟通道 (CTXMTOP)。端点在本地解码并呈现多媒体，将 Citrix Workspace 应用程序窗口移回托管的 Microsoft Teams 应用程序中。

身份验证和发出信号在本地发生在 Microsoft Teams 托管的应用程序上，就像其他 Microsoft Teams 服务（例如聊天或协作）一样。音频/视频重定向不会对其产生影响。

CTXMTOP 是一个命令和控制虚拟通道。这意味着在 Citrix Workspace 应用程序与 VDA 之间不交换媒体。

仅客户端提取/客户端呈现可用。

此视频演示让您了解 Microsoft Teams 如何在 Citrix 虚拟环境中工作。



Microsoft Teams 安装

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 我们建议先安装 VDA，然后在黄金映像中安装 Microsoft Teams。需要采用此安装顺序，才能使 **ALLUSER=1** 标志生效。如果您先在虚拟机中安装了 Microsoft Teams 再安装 VDA，请卸载并重新安装 Microsoft Teams。如果您使用的是 App Layering，请参阅面向 App Layering 了解更多详细信息。

我们建议您遵循 Microsoft Teams 计算机范围的安装准则，并避免使用在 `AppData` 中安装 Microsoft Teams 的.exe 安装程序。而是通过使用命令行中的 **ALLUSER=1** 标志来安装 `C:\Program Files (x86)\Microsoft\Teams`。

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1 ALLUSERS=1
```

此示例还使用 **ALLUSERS=1** 参数。设置此参数时，Teams 计算机范围内的安装程序将显示在“控制面板”的程序和功能中，以及计算机的所有用户的 Windows 设置的应用程序和功能中。如果所有用户都有管理员凭据，则可以卸载 Microsoft Teams。

了解 **ALLUSERS=1** 与 **ALLUSER=1** 之间的区别非常重要。可以在非 VDI 和 VDI 环境中使用 **ALLUSERS=1** 参数。请仅在 VDI 环境中使用 **ALLUSERS=1** 参数以指定每计算机安装。

在 **ALLUSER=1** 模式下，只要有新版本，Microsoft Teams 应用程序就不会自动更新。我们建议对非持久性环境应用此模式，例如，Windows Server 或 Windows 10 随机/池目录中的托管共享应用程序或桌面。有关详细信息，请参阅使用 MSI 安装 Microsoft Teams（VDI 安装部分）。

假设您有 Windows 10 专用的永久 VDI 环境。您希望 Microsoft Teams 应用程序自动更新，并希望 Microsoft Teams 在 `Appdata/Local` 下执行每用户安装。在这种情况下，请使用 `.exe` 安装程序或不带 **ALLUSER=1** 的 MSI。

面向 App Layering

如果使用 Citrix App Layering 管理不同层中的 VDA 和 Microsoft Teams 安装，请在使用 **ALLUSER=1** 安装 Microsoft Teams 之前在 Windows 中部署此注册表项。有关信息，请参阅通过注册表管理的功能列表中的借助 Citrix App Layering 优化 Microsoft Teams。

Profile Management 建议

我们建议在 Windows Server 和池 VDI Windows 10 环境中使用计算机范围内的安装程序。

当 **ALLUSER=1** 标志从命令行（计算机范围内的安装程序）传递到 MSI 时，Microsoft Teams 应用程序将安装在 `C:\Program Files (x86)` 下 (~300 MB)。该应用程序将 `AppData\Local\Microsoft\TeamsMeetingAddin` 用于日志，将 `AppData\Roaming\Microsoft\Teams` (~600-700 MB) 用于用户特定的配置、缓存用户界面中的元素等等。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 重要：
>
> 如果您没有通过 **ALLUSER=1** 标志，MSI 会将 Teams.exe 安装程序和 `setup.json` 置于 `C:\Program Files (x86)\Teams Installer` 下。注册表项 (TeamsMachineInstaller) 将添加到以下位置：`HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
>
> 后续用户登录将改为触发 **AppData** 中的最终安装。

计算机范围内的安装程序

下面是通过在 Windows Server 2016 64 位 VM 上安装 Microsoft Teams 计算机范围内的安装程序创建的文件夹、桌面快捷方式和注册表示例：

文件夹：

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

桌面快捷方式：

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

注册表：

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

建议

- 我们建议通过删除 Microsoft Teams 注册表项来禁用自动启动。这样做可以防止同时发生许多登录（例如，在工作日开始时）增加 VM 的 CPU。
- 如果虚拟桌面没有 GPU/vGPU，我们建议在 Microsoft Teams 的设置中设置禁用 **GPU** 硬件加速以提高性能。此设置 (`"disableGpu":true`) 存储在 `desktop-config.json` 中的 `%Appdata%\Microsoft\Teams` 中。可以使用登录脚本编辑该文件并将值设置为 **true**。
- 如果使用 Citrix Workspace Environment Management (WEM)，请启用 **CPU Spikes Protection**（CPU 峰值保护）来管理 Microsoft Teams 的处理器消耗。

每用户安装程序

使用 `.exe` 安装程序时，安装过程会有所差别。所有文件都放置在 AppData 中。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

文件夹：

- C:\Users\<username>\AppData\Local\Microsoft\Teams
- C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin
- C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin
- C:\Users\<username>\AppData\Local\SquirrelTemp
- C:\Users\<username>\AppData\Roaming\Microsoft\Teams

桌面快捷方式：

```
C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --
processStart "Teams.exe"
```

注册表：

```
HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

最佳做法

最佳做法建议取决于用例场景。

使用具有非持久性设置的 Microsoft Teams 需要配置文件缓存管理器来实现高效的 Microsoft Teams 运行时数据同步。使用配置文件缓存管理器时，将在用户会话期间缓存适当的用户特定信息（例如，用户数据、配置文件和设置）。同步以下两个文件夹中的数据：

- C:\Users\<username>\AppData\Local\Microsoft\IdentityCache
- C:\Users\<username>\AppData\Roaming\Microsoft\Teams

非持久性设置的 **Microsoft Teams** 缓存内容排除列表　从 Microsoft Teams 缓存文件夹 %AppData%/Microsoft/Teams 中排除以下项目。排除这些项目有助于减少用户缓存大小，从而进一步优化非持久性设置。

排除列表 - 文件

- Roaming\Microsoft\Teams* .txt

排除列表 - 目录

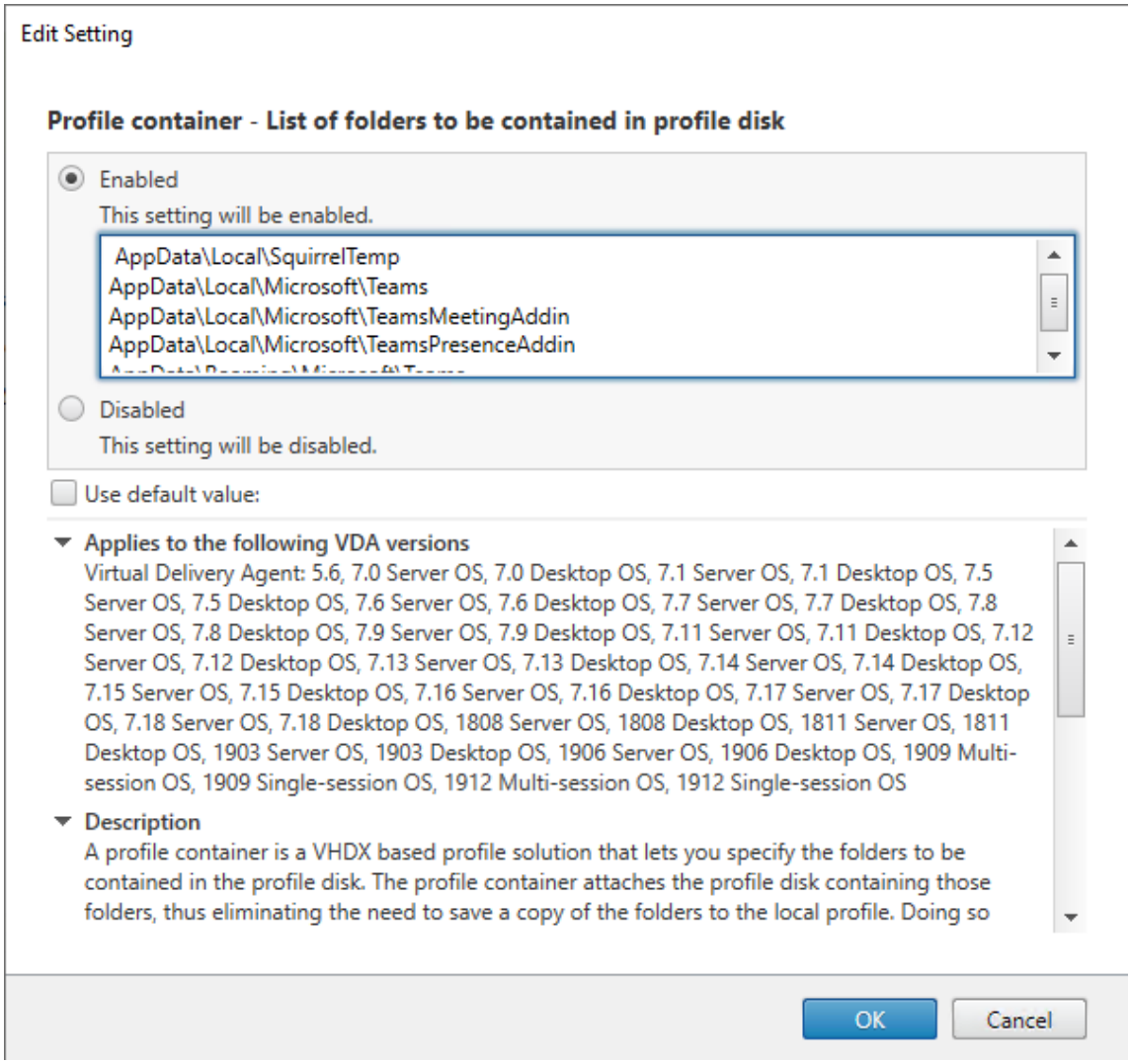
- Roaming\Microsoft\Teams\Logs
- Roaming\Microsoft\Teams\media-stack
- Roaming\Microsoft\Teams\Service Worker\CacheStorage
- Roaming\Microsoft\Teams\Application Cache
- Roaming\Microsoft\Teams\Cache
- Roaming\Microsoft\Teams\GPUCache
- Roaming\Microsoft\Teams\meeting-addin\Cache（对于 Outlook 中缺少加载项的问题至关重要）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

用例：单会话场景　在这种情况下，最终用户一次在一个位置使用 Microsoft Teams。他们不需要同时在两个 Windows 会话中运行 Microsoft Teams。例如，在常见的虚拟桌面部署中，每个用户被分配有一个桌面，Microsoft Teams 作为一个应用程序在虚拟桌面中部署。

我们建议启用 Citrix Profile 容器并将每用户安装程序中列出的每用户目录重定向到该容器中。

1. 在黄金映像中部署 Microsoft Teams 计算机范围内的安装程序 (**ALLUSER=1**)。
2. 启用 Citrix Profile Management 并使用适当的权限设置用户配置文件存储。
3. 启用以下 Profile Management 策略设置：文件系统 **>** 同步 **>** 配置文件容器 **-** 要包含在配置文件磁盘中的文件夹列表。



将所有每用户目录列入此配置中。也可以使用 Citrix Workspace Environment Management (WEM) 服务配置这些设置。

4. 将这些设置应用到正确的交付组。
5. 登录以验证部署。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

系统要求

推荐的最低版本 **- Delivery Controller (DDC) 1906.2**

如果您使用的是早期版本，请参阅启用 Microsoft Teams 的优化：

支持的操作系统：

- Windows Server 2019、2016、2012 R2 Standard Edition 和 Datacenter Edition，包含服务器核心选项

最低版本 **- Virtual Delivery Agent (VDA) 1906.2**

支持的操作系统：

- Windows 10 64 位，版本为 1607 及更高版本。（不支持 VM 托管应用程序）。
- Windows Server 2019、2016 和 2012 R2（Standard Edition 和 Datacenter Edition）。

要求：

- BCR_x64.msi - 包含 Microsoft Teams 优化代码并从 GUI 自动启动的 MSI。如果使用命令行界面进行 VDA 安装，请不要将其排除。

推荐的版本 **-** 适用于 **Windows** 的 **Citrix Workspace** 应用程序的最新 **CR** 和最低版本 **-** 适用于 **Windows** 的 **Citrix Workspace** 应用程序 **1907**

- Windows 8 和 10（32 位和 64 位版本，包括嵌入式版本）（对 Windows 7 的支持已在版本 2006 时停止）
- Windows 10 IoT Enterprise 2016 LTSB (v1607) 和 2019 LTSC (v1809)
- 支持的处理器 (CPU) 体系结构：x86 和 x64（不支持 ARM）
- 端点要求：大约 2.2–2.4 GHz 双核 CPU，可在点对点视频会议通话期间支持 720p HD 分辨率。
- 具有较低基础速度（大约 1.5 GHz）的双核或四核 CPU，配备 Intel Turbo Boost 或 AMD Turbo Core，可提升至至少 2.4 GHz。
- 通过验证的 HP 瘦客户端：t630/t640、t730/t740、mt44/mt45。
- 通过验证的 Dell 瘦客户端：5070、5470 Mobile TC。
- 经过验证的 10ZiG 瘦客户端：4510 和 5810q。
- 有关通过验证的端点的完整列表，请参阅瘦客户端。
- Citrix Workspace 应用程序至少需要 600 MB 可用磁盘空间和 1 GB RAM。
- Microsoft .NET Framework 最低要求为版本 4.6.2。如果系统中不存在，Citrix Workspace 应用程序会自动下载并安装.NET Framework。

管理员可以通过更改 Teams 优化策略来启用/禁用在优化模式下启动的 Microsoft Teams。在 Citrix Workspace 应用程序中以优化模式启动的用户无法选择禁用 Microsoft Teams。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

最低版本 **-** 适用于 **Linux** 的 **Citrix Workspace** 应用程序 **2006**

有关详细信息，请参阅 2006 中的新增功能中的 *Microsoft Teams* 优化。

软件：

- GStreamer 1.0 或更高版本或 Cairo 2
- libc++-9.0 或更高版本
- libgdk 3.22 或更高版本
- OpenSSL 1.1.1d
- x64 Linux 发行版

硬件：

- 最低 1.8 GHz 双核 CPU，可在点对点视频会议通话期间支持 720p HD 分辨率
- 双核或四核 CPU，基本速度为 1.8 GHz，并采用至少为 2.9 GHz 的高速英特尔睿频加速技术

有关通过验证的端点的完整列表，请参阅瘦客户端。

有关详细信息，请参阅安装 Citrix Workspace 应用程序所需的必备条件。

可以禁用 Teams 优化，在 `/opt/Citrix/ICAClient/config/module.ini` 文件中将字段 VDWEBRTC 的值更新为 Off。默认值为 VDWEBRTC=On。执行更新后，重新启动会话。（需要 root 用户权限）。

最低版本 **-** 适用于 **Mac** 的 **Citrix Workspace** 应用程序 **2012**

支持的操作系统：

- macOS Catalina (10.15)。
- macOS Big Sur 11.0.1 或更高版本。

支持的功能：

- 音频
- 视频
- 屏幕共享优化（传入和传出）

> 注意：
>
> Citrix Viewer 应用程序需要访问 MacOS“安全性与隐私”首选项，才能使屏幕共享正常工作。用户可以在苹果菜单 **>** 系统偏好设置 **>** 安全性与隐私 **>** 隐私选项卡 **>** 屏幕录制中选择 **Citrix Viewer** 来配置此首选项。

如果用户具有 Citrix Workspace 应用程序 2012 或更高版本以及 macOS 10.15，则默认情况下，Microsoft Teams 优化会起作用。

如果要禁用 Microsoft Teams 优化，请在端点中运行以下命令并重新启动 Workspace 应用程序：

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

最低版本 **-** 适用于 **ChromeOS** 的 **Citrix Workspace** 应用程序 **2105.5**

支持的功能：

- 音频
- 视频
- 屏幕共享优化（传入和传出）- 默认处于禁用状态。有关如何将其打开的说明，请参阅这些设置。

功能列表和版本支持

功能	Windows CR	Windows 1912 LTSR（及 CU1-CU4）	Windows 1912 CU5（或更高版本）	Mac	Linux	ChromeOS
音频/视频 (P2P 和会议)	1907	是	是	2009	2004	2106
屏幕共享	1907	是	是	2012	2006	2106 (1)
i. 屏幕指示器红色边框	2002	是	是	2012	2006	X
ii. 将捕获限制为 Desktop Viewer	2009.5	X	是	2012	2006	X
iii. 多显示器	2106 (2)	X	X	2106	2106	X
DTMF	2102	X	是 (5)	2101	2101	X
代理服务器支持	2012 (3)	X	是 (3) (5)	2104 (4)	2101 (4)	X

1. 默认处于禁用状态，需要管理员启用。
2. 仅限全屏模式下的 CD 查看器。Shift+F2 不受支持。
3. 协商/Kerberos、NTLM、基本和摘要式。还支持 Pac 文件。
4. 仅限匿名。
5. 仅限在 Windows 10 客户端操作系统上。

启用 **Microsoft Teams** 优化

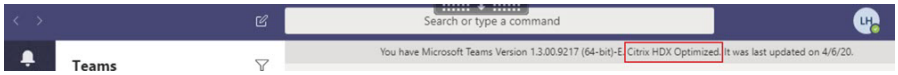
要为 Microsoft Teams 启用优化，请使用 Microsoft Teams 重定向策略中介绍的“管理”控制台策略。默认情况下它处于开状态。除启用此策略外，HDX 还会进行检查，以验证 Citrix Workspace 应用程序的版本至少是所需的最低版本。如果启用了此策略并且支持 Citrix Workspace 应用程序的版本，

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

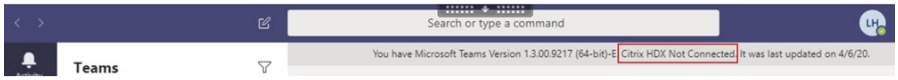
HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport 将在 VDA 上自动设置为 **1**。Microsoft Teams 读取在 VDI 模式下加载的密钥。

> 注意：
>
> 如果您对“管理”控制台 (Studio) 中没有可用策略的较旧控制器版本（例如，7.15 版）使用 1906.2 或更高版本的 VDA，您的 VDA 仍可以进行优化。默认情况下，在 VDA 中启用“Microsoft Teams 的 HDX 优化”。

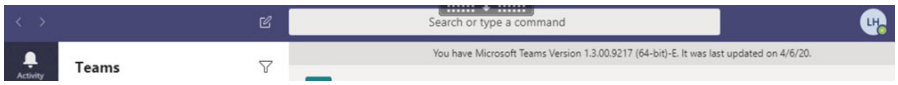
如果单击关于 **>** 版本，则会显示 **Citrix HDX Optimized**（Citrix HDX 已优化）图例：



如果您看到 **Citrix HDX** 未连接，Citrix API 将加载到 Microsoft Teams 中。加载 API 是迈向重定向的第一步。但是堆栈的后面部分存在错误。此错误很可能发生在 VDA 服务或 Citrix Workspace 应用程序中。



如果您没有看到任何图例，Microsoft Teams 无法加载 Citrix API。请通过右键单击通知区域图标并重新启动来退出 Microsoft Teams。请确保“管理”控制台策略未设置为禁止，并且 Citrix Workspace 应用程序版本受支持。



网络要求

Microsoft Teams 依赖 Office 365 中的媒体处理器服务器进行会议或多方呼叫。Microsoft Teams 依赖于 Office 365 传输中继处理以下场景：

- 点对点通话中的两个对端没有直接连接
- 参与者没有直接连接到媒体处理器。

因此，对端与 Office 365 云之间的网络运行状况决定通话的性能。

我们建议您对环境进行评估，以确定可能会影响整个云语音和视频部署的任何风险和要求。
使用 Skype for Business 网络评估工具来测试您的网络是否已准备好使用 Microsoft Teams。有关支持信息，请参阅支持。

实时协议 **(RTP)** 流量的关键网络建议汇总

- 尽可能直接从分支机构连接到 Office 365 网络。
- 如果必须在分支机构使用以下任何内容，请确保 RTP/UDP Teams 流量不受阻碍。HdxTeams.exe 不支持在端点上配置的显式代理。
  - 绕过代理服务器

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - 网络 SSL 拦截
  - 深度包检测设备
  - VPN 发夹（如有可能，使用拆分通道）

- 规划并提供足够的带宽。
- 检查每个分支机构的网络连接性和质量。

Workspace 应用程序（HdxTeams.exe 或 HdxRtcEngine.exe）中的 WebRTC 媒体引擎对卸载到客户端的多媒体数据流使用安全实时传输协议 (SRTP)。SRTP 通过使用对称密钥（128 位）加密媒体和控制消息，并在计数器模式下使用 AES 加密密码，为 RTP 提供机密性和身份验证。

建议使用以下指标来保证正面的用户体验：

指标	端点到 Office 365
延迟（单向）	< 50 毫秒
延迟 (RTT)	< 100 毫秒
Packet Loss（数据包丢失）	在任何 15 秒时间间隔内 < 1%
数据包到达间抖动	在任何 15 秒时间间隔内 <30 毫秒

有关详细信息，请参阅为 Microsoft Teams 准备贵组织的网络。

在带宽要求方面，Microsoft Teams 的优化可以使用对音频 (OPUS/G.722/PCM G711) 和视频 (H264) 使用各种编解码器。

在通话建立过程中，对端使用会话描述协议 (SDP) 请求应答来协商这些编解码器。
Citrix 对每位用户的最低建议如下：

类型	Bandwidth（带宽）	编解码器
音频（单向）	大约 90 kbps	G.722
音频（单向）	大约 60 kbps	Opus*
视频（单向）	大约 700 kbps	H264 360p @ 30 fps 16:9
屏幕共享	大约 300 kbps	H264 1080p @ 15 fps

* Opus 支持恒定和可变比特率编码，范围为 6 kbps 到 510 kbps。

Opus 是两个优化的 VDI 用户之间的点对点通话的首选编解码器。

G.722 和 H264 是加入会议的 VDI 用户的首选编解码器。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

代理服务器

请注意以下事项，具体取决于代理的位置：

- VDA 上的代理配置：

  如果在 VDA 中配置了显式代理服务器并通过代理将连接路由到 localhost，重定向将失败。要正确配置代理服务器，必须在 **Internet** 选项 **>** 连接 **>** 局域网设置 **>** 代理服务器中选择对于本地地址不使用代理服务器设置，然后确保不使用 `127.0.0.1:9002`。

  如果使用 PAC 文件，对于 `wss://127.0.0.1:9002`，PAC 文件中的 VDA 代理配置脚本必须返回 **DIRECT**。如果没有，优化将失败。要确保脚本返回 **DIRECT**，请使用 `shExpMatch(url, "wss://127.0.0.1:9002/*")`。

- Citrix Workspace 应用程序上的代理配置：

  如果分支机构配置为通过代理访问 Internet，这些版本支持代理服务器：

  - 适用于 Windows 的 Citrix Workspace 应用程序 2012（协商/Kerberos、NTLM、Basic 和 Digest。还支持 Pac 文件）
  - 适用于 Windows 的 Citrix Workspace 应用程序 1912 CU5（协商/Kerberos、NTLM、Basic 和 Digest。还支持 Pac 文件）
  - 适用于 Linux 的 Citrix Workspace 应用程序 2101 版（匿名身份验证）
  - 适用于 Mac 的 Citrix Workspace 应用程序 2104 版本（匿名身份验证）

安装了 Citrix Workspace 应用程序的早期版本的客户端设备无法读取代理配置。这些设备将流量直接发送到 Office 365 TURN 服务器。

> 重要：
>
> 验证客户端设备是否可以连接到 DNS 服务器以执行 DNS 解析。客户端设备必须能够解析三个 Microsoft Teams TURN 服务器的 FQDN：`worldaz.turn.teams.microsoft.com`、`usaz.turn.teams.microsoft.com` 和 `euaz.turn.teams.microsoft.com`。

通话建立和媒体流路径

如有可能，Citrix Workspace 应用程序（HdxTeams.exe 或 HdxRtcEngine.exe）中的 HDX WebRTC 媒体引擎会尝试在点对点通话中通过用户数据报协议 (UDP) 建立直接网络安全实时传输协议 (SRTP) 连接。如果 UDP 端口被阻止，Media Engine 将回退到 TCP 443。

HDX Media Engine 支持 ICE、Session Traversal Utilities for NAT (STUN) 和 Traversal Using Relays around NAT (TURN) 进行候选发现和建立连接。

请注意，这意味着端点必须能够执行 DNS 解析。

假设两个对等方之间或对等方与会议服务器之间没有直接路径，例如用户是否加入多方通话或会议。HdxTeams.exe 使用 Office 365 中的 Microsoft Teams 传输中继服务器访问其他对等节方或媒体处理器（用于举办会议）。用户的客

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

户端计算机必须具有两个 Office 365 子网 IP 地址范围和 4 个 UDP 端口的访问权限。有关详细信息，请参阅通话设置中的体系结构图和 Office 365 URL 和 IP 地址范围 ID 11

ID	类别	地址	目标端口
11	需要优化	13.107.64.0/18、52.112.0.0/14、52.120.0.0/14	**UDP**：3478、3479、3480、3481 **TCP**：443（回退）

这些范围包含传输中继和媒体处理器。

Microsoft Teams T 传输中继提供 STUN 和 TUN 功能，但它们不是 ICE 端点。此外，Microsoft Teams 传输中继不会终止媒体，也不会执行任何转码。当它们将流量转发到其他对端或媒体处理器时，可以将 TCP（如果 HdxTeams.exe 使用 TCP）桥接到 UDP。

Workspace 应用程序 WebRTC 媒体引擎在 Office 365 云中联系距离最近的 Microsoft Teams 传输中继。每天引擎使用任意广播 IP 和端口 3478—3481 UDP（每个工作负载使用不同的 UDP 端口，尽管会发生多路复用）或 443 TCP TLSv1.2 进行回退。通话质量取决于基础网络协议。由于始终推荐 UDP 而非 TCP，因此，我们建议将您的网络设计为适应分支机构中的 UDP 流量。

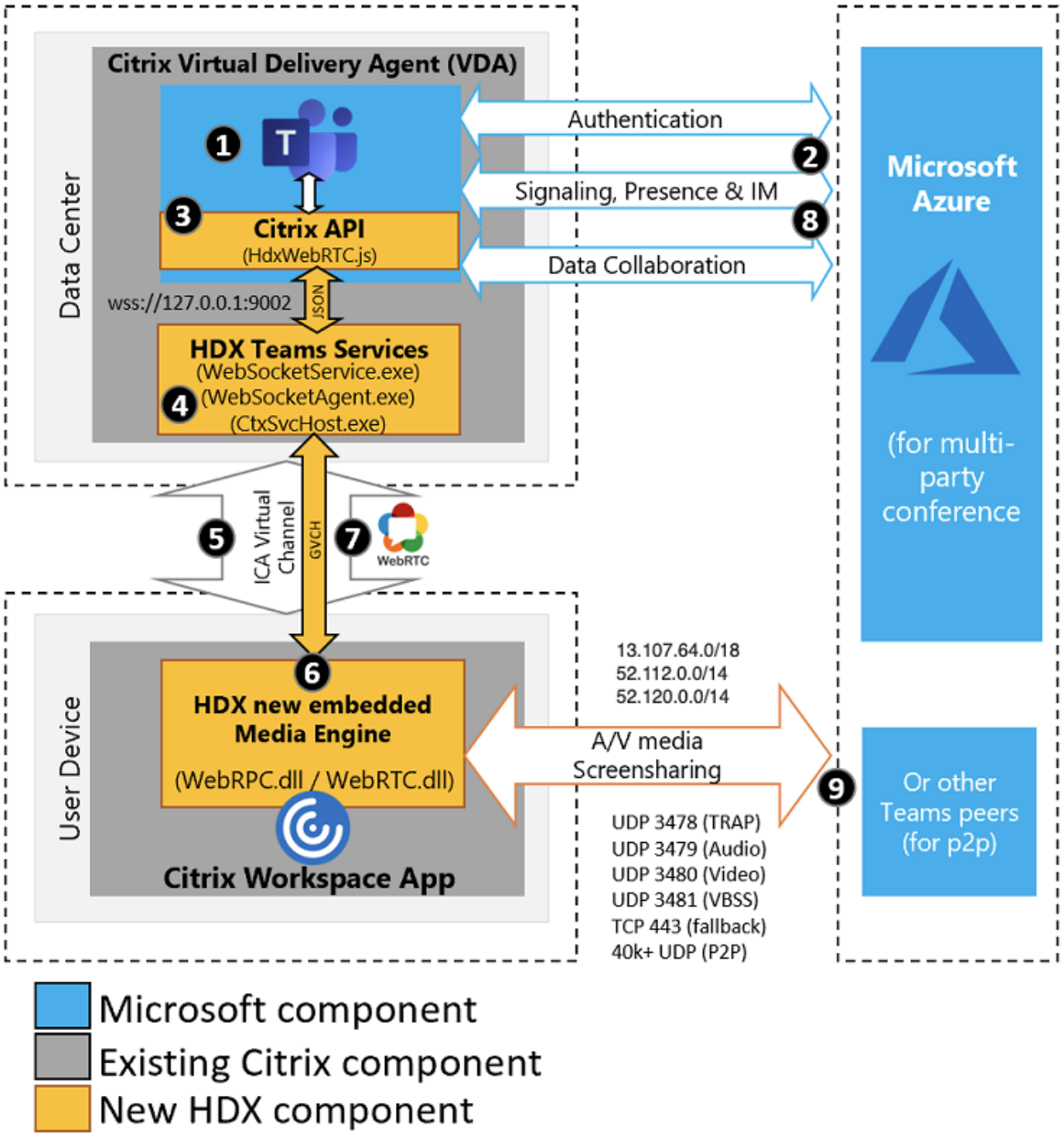
如果 Microsoft Teams 是在优化模式下加载的并且 HdxTeams.exe 在端点上运行，则 ICE 失败可能会导致呼叫设置失败或单程音频/视频。当呼叫无法完成或媒体流不是全双工时，请先检查端点上的 **Wireshark** 跟踪。有关 ICE 候选人收集过程的详细信息，请参阅支持部分中的“收集日志”。

> 注意：
>
> 如果端点无法访问 Internet，则当用户位于同一 LAN 上时，可能仍然可以进行点对点呼叫。会议失败。在这种情况下，通话设置开始之前有 30 秒的超时。

呼叫设置

请使用此体系结构示意图作为调用流序列的可视参考。示意图中显示了相应的步骤。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



体系结构

1. 启动 Microsoft Teams。
2. Microsoft Teams 向 O365 进行身份验证。租户策略被向下推送到 Microsoft Teams 客户端，并将相关 TURN 和信号通道信息中继到应用程序。
3. Teams 检测到其正在 VDA 中运行，并对 Citrix JavaScript API 进行 API 调用。
4. Microsoft Teams 中的 Citrix JavaScript 将打开一个与在 VDA 上运行的 WebSocketService.exe 的安全 WebSocket 连接，这会在用户会话内部生成 WebSocketAgent.exe。
5. WebSocketAgent.exe 通过调用到 Citrix HDX Teams Redirection Service (CtxSvcHost.exe) 来实例化通用虚拟通道。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. Citrix Workspace 应用程序的 wfica32.exe (HDX Engine) 产生一个名为 HdxTeams.exe 或 HdxRtcEngine.exe 的新进程，这是用于 Microsoft Teams 优化的新 WebRTC 引擎。
7. Citrix 媒体引擎和 Teams.exe 有一个双向虚拟通道路径，可以开始处理多媒体请求。

   ——用户呼叫——

8. 对端 **A** 单击呼叫按钮。Teams.exe 与 Office 365 中的 Microsoft Teams 服务通信，通过对等方 **B** 建立端到端信号路径。Microsoft Teams 向 HdxTeams 询问一系列受支持的呼叫参数（编解码器、分辨率等，称为会话描述协议 (SDP) 提议）。然后使用指向 Office 365 中的 Microsoft Teams 服务的信令路径中继这些呼叫参数，并从该位置传输到另一个对等方。
9. SDP 提议/应答（单通协商）通过信号通道进行，ICE 连接性检查（NAT 和使用 STUN 绑定请求的防火墙遍历）完成。然后，安全实时传输协议 (SRTP) 媒体直接在 HdxTeams.exe 与其他对端（或 Office 365 会议服务器，如果是会议）之间流动。

Microsoft Phone 系统

Phone System 是 Microsoft 的技术，在 Office 365 云中对 Microsoft Teams 启用呼叫控制和 PBX。Microsoft Teams 的优化使用 Office 365 通话套餐或直接路由支持 Phone System。使用直接路由，您可以直接将自己支持的会话边界控制器连接到 Microsoft Phone System，而无需任何额外的本地软件。
支持通话队列、转接、转移、保持、静音和继续通话。

DTMF:

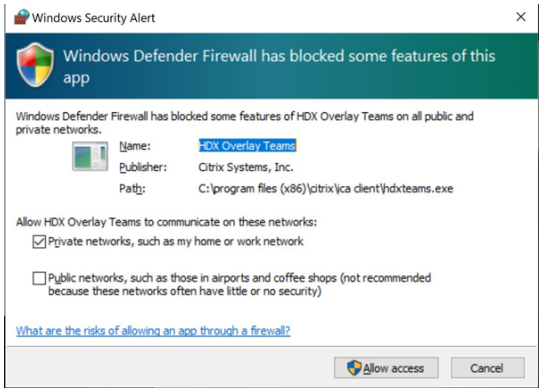
这些版本的 Citrix Workspace 应用程序（或更高版本）支持双音多频 (Dual tone multi frequency, DTMF)：

- 适用于 Windows 的 Citrix Workspace 应用程序版本 2102
- 适用于 Windows 的 Citrix Workspace 应用程序 LTSR 1912 CU5
- 适用于 Linux 的 Citrix Workspace 应用程序 2101
- 适用于 Mac 的 Citrix Workspace 应用程序 2101

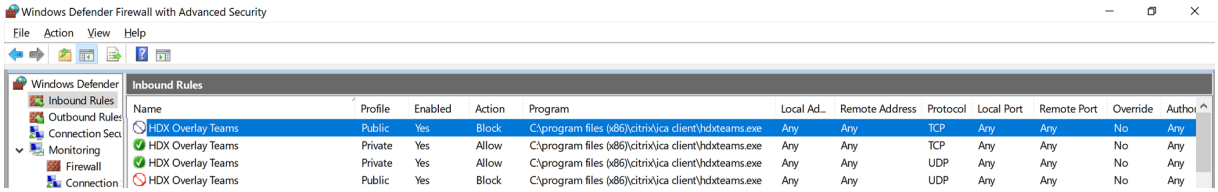
防火墙注意事项

当用户首次使用 Microsoft Teams 客户端启动优化的呼叫时，他们可能会注意到 **Windows** 防火墙设置的警告。警告要求用户允许 HdxTeams.exe 或 HdxRtcEngine.exe (HDX Overlay Teams) 的通信。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



在 **Windows Defender** 防火墙 **>** 高级安全控制台的入站规则下添加了以下四个条目。如有需要，可以应用更严格的规则。



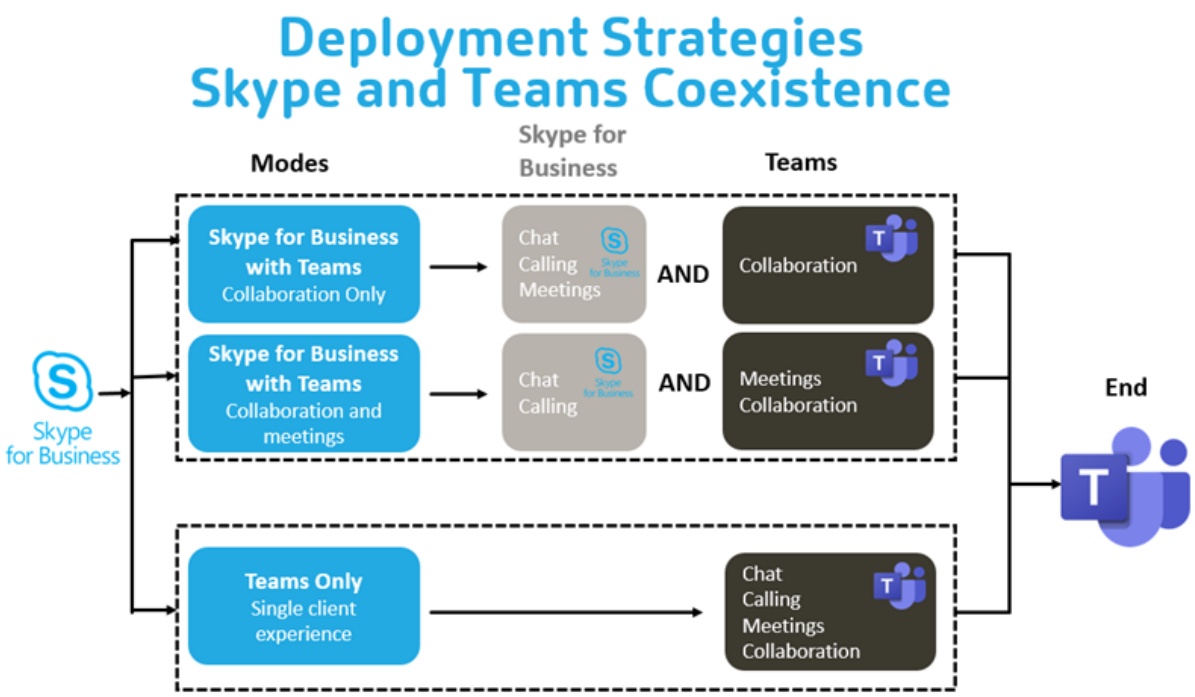
Microsoft Teams 和 **Skype for Business** 同时存在

可以并行部署 Microsoft Teams 和 Skype for Business，作为两个具有重叠功能的独立解决方案。
有关详细信息，请参阅了解 Microsoft Teams 和 Skype for Business 的共存与互操作性。

适用于 Microsoft Teams 多媒体引擎的 Citrix RealTime Optimization Pack 和 HDX 优化随后遵守您的环境中设置的配置。示例包括岛屿模式、Skype for Business 与 Microsoft Teams 协作，以及 Skype for Business 与 Microsoft Teams 协作和会议。

此时只能向单个应用程序授予外围设备访问权限。例如，通话期间 RealTime Media Engine 访问网络摄像头会在通话期间锁定成像设备。松开设备后，它将可用于 Microsoft Teams。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Citrix SD-WAN：针对 **Microsoft Teams** 的优化网络连接

最佳音频和视频质量要求具有低延迟、低抖动和低数据包丢失的 Office 365 云的网络连接。在进入 Internet 之前，将 Microsoft Teams 音频-视频 RTP 流量从分支机构位置的 Citrix Workspace 应用程序用户到数据中心可能会增加过多的延迟。这也可能会导致 WAN 链接上出现拥堵 Citrix SD-WAN 按照 Microsoft Office 365 网络连接性原则优化 Microsoft Teams 的连接性。Citrix SD-WAN 使用基于 Microsoft REST 的 Office 365 IP 地址和 Web 服务以及近似 DNS 来识别、分类和引导 Microsoft Teams 的流量。

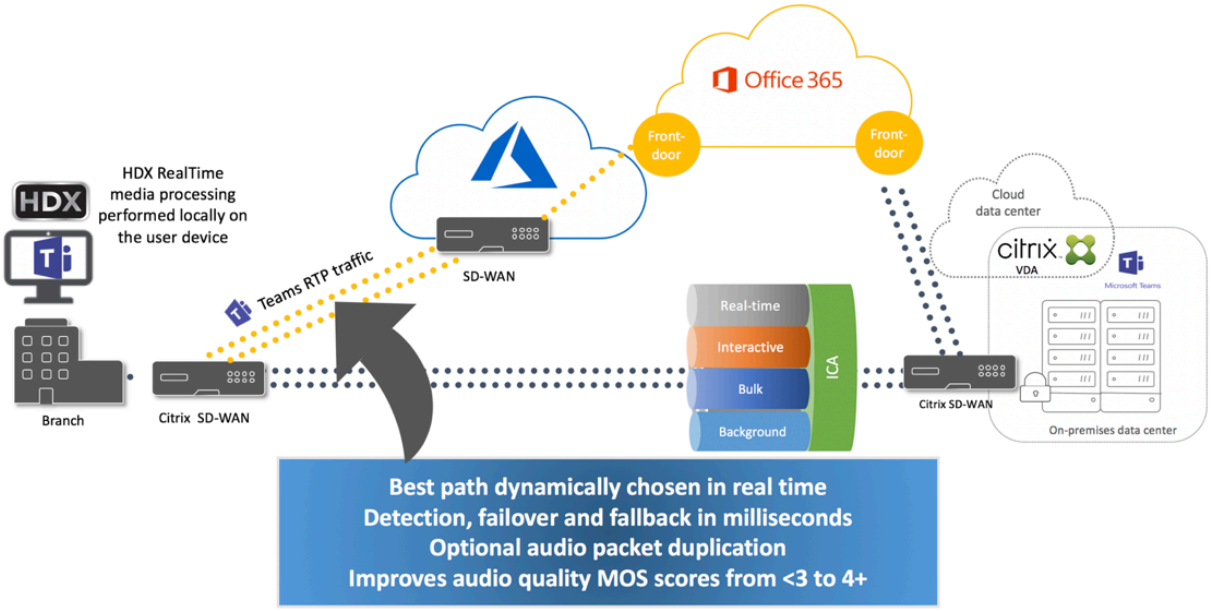
许多地区的企业宽带 Internet 连接都会受到间歇性数据包丢失、过度抖动和中断的影响。

Citrix SD-WAN 提供了两种解决方案，以便在网络运行状况变化或降低时保持 Microsoft Teams 音频-视频质量。

- 如果使用 Microsoft Azure，则在 Azure VNET 中部署的 Citrix SD-WAN 虚拟设备 (VPX) 可提供高级连接优化。这些优化包括无缝链路故障转移和音频数据包竞赛。
- Citrix SD-WAN 客户可以通过 Citrix Cloud 直接服务连接到 Office 365。此服务为所有受 Internet 限制的流量提供可靠和安全交付。

如果分支机构 Internet 连接的质量无需担心，通过将 Microsoft Teams 流量直接从 Citrix SD-WAN 分支机构转向最近的 Office 365 前门，可能足以最大限度地减少延迟。有关详细信息，请参阅 Citrix SD-WAN Office 365 优化。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Microsoft Teams 中的库视图和活动扬声器

Microsoft Teams 支持 **Gallery**（库）、**Large gallery**（大型库）和 **Together mode**（共聚模式）布局。

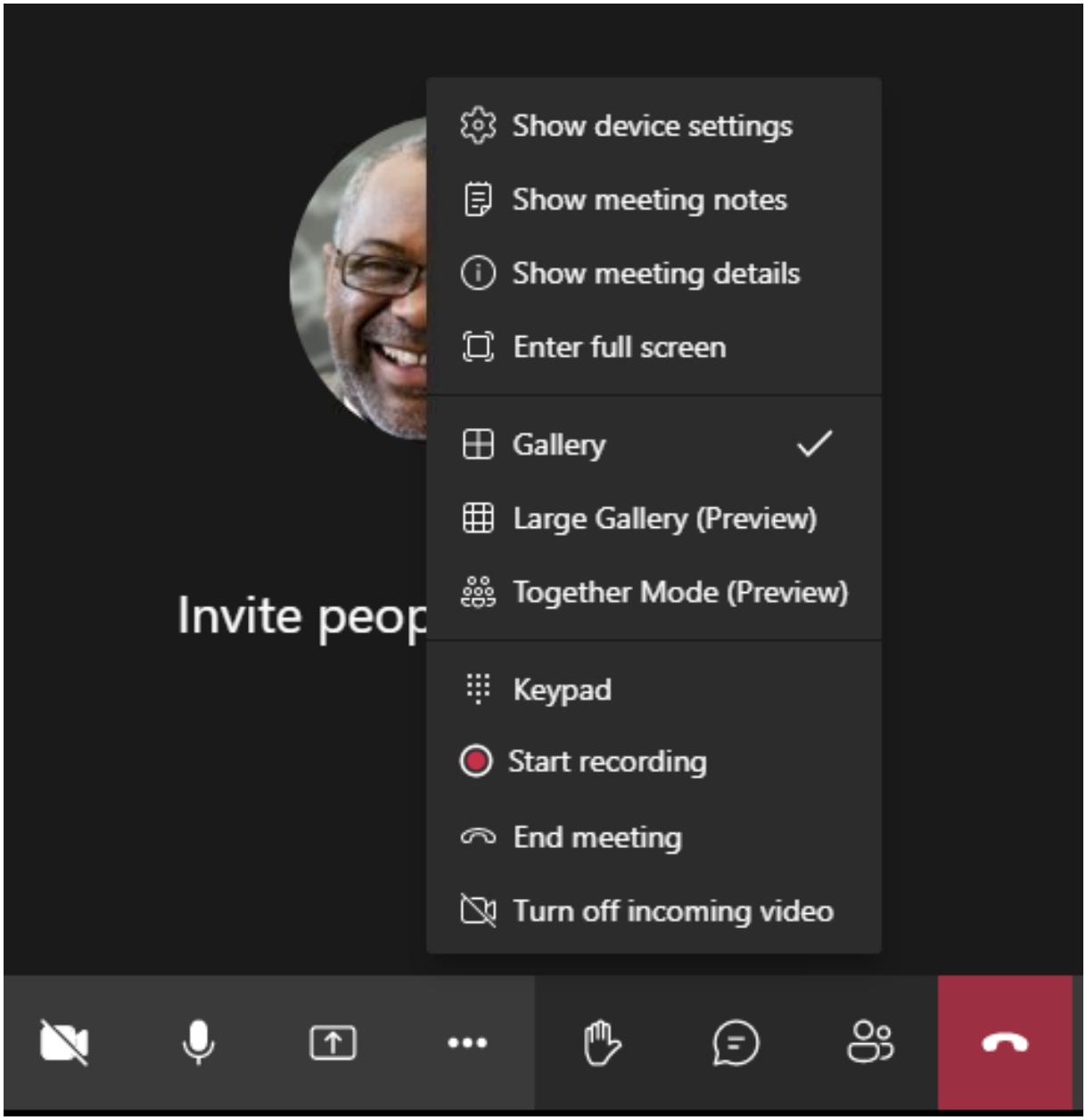
Microsoft Teams 显示一个 2x2 网格，其中包含四名参与者的视频流（称为库）。在这种情况下，Teams 将 4 个视频流发送到客户端设备进行解码。当共享视频的参与者超过四位时，屏幕上只会显示最后四位最活跃的发言者。

Microsoft Teams 还提供了具有一个高达 7x7 的网格的大型库视图。因此，Microsoft Teams 会议服务器会合成单个视频源并将其发送到客户端设备进行解码，从而降低 CPU 消耗。这个单一的列表式源可能还包括用户的自我预览视频。

最后，Microsoft Teams 支持共聚模式，这是新会议体验的一部分。Teams 使用 AI 细分技术以数字方式将参与者置于共享背景中，将所有参与者都放在同一个大会堂中。

用户可以在电话会议期间通过在省略号菜单中选择 **Gallery**（库）、**Large gallery**（大型库）或 **Together mode**（共聚模式）布局来控制这些模式。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



支持视频纵横比约束（适用于 Windows 的 CWA 2102、适用于 Linux 的 CWA 2106、适用于 MAC 的 CWA 2106 或更高版本）：

- **Fill to frame**（填充到框架）选项在“Gallery/Large Gallery View”（库/大型库视图）中可用。此选项裁剪视频大小以适应子窗口的大小。另一方面，**Fit to frame**（适合框架）在视频两侧显示黑色条（信箱），因此不会裁剪。

Microsoft Teams 中的屏幕共享

Microsoft Teams 依赖于基于视频的屏幕共享 (VBSS)，有效地对正在与 H264 等视频编解码器共享的桌面进行编码，并创建高清晰度流。通过 HDX 优化，传入屏幕共享被视为视频流。因此，如果您正在进行视频通话，而其他对等方开

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

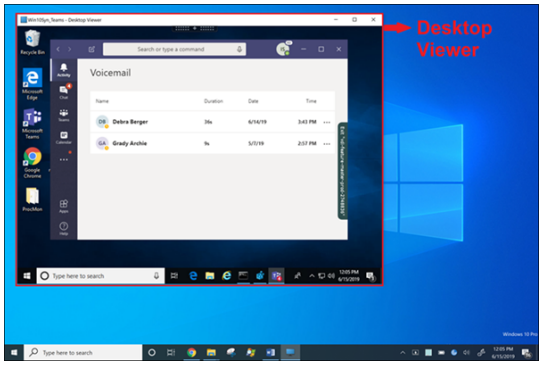
始共享桌面，则原始网络摄像机视频源将暂停。相反，将显示屏幕共享视频源。然后，对端必须手动恢复网络摄像机共享。

传出屏幕共享也进行了优化，并卸载到 Citrix Workspace 应用程序（1907 或更高版本）。在这种情况下，每天引擎捕获并仅传输 Citrix Desktop Viewer (CDViewer.exe) 窗口。如果要共享在客户端计算机上运行的本地应用程序，可以将其叠加在 CDViewer 上，并且也可以将其捕获。

适用于 Windows 的 Citrix Workspace 应用程序 2009.6 会执行窗口的本机位图捕获，因此不会捕获重叠窗口。

多显示器：如果 Desktop Viewer (CDViewer.exe) 处于全屏模式并跨越多显示器设置，Citrix Workspace 应用程序 2106 或更高版本（Windows/Linux/Mac）将允许屏幕选择器选择要共享的监视器。
如果禁用 Desktop Viewer（可以通过编辑.ica 文件模板或 StoreFront web.config）或者如果正在使用 Desktop Lock，多显示器选择功能在屏幕选择器中将不可用。SHIFT+F2 热键与多显示器屏幕共享不兼容。

在 2106 之前的 Workspace 应用程序版本中，仅共享主监视器。用户必须将虚拟桌面中的应用程序拖动到主显示器，以便通话中的其他对端查看该应用程序。

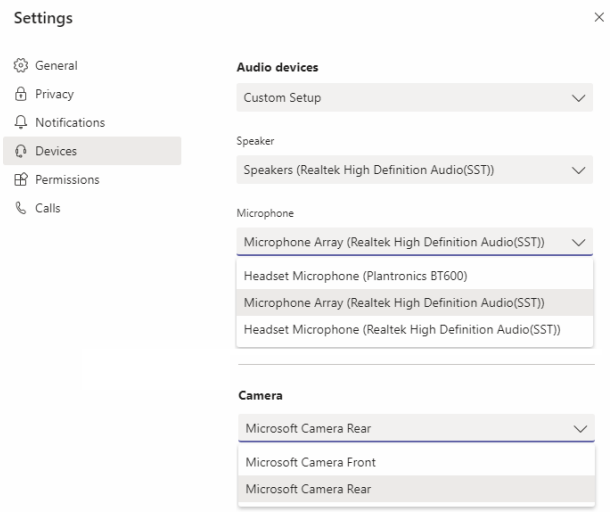


> 注意：
>
> 如果要将 Microsoft Teams 发布为独立的无缝应用程序，屏幕共享会捕获 Citrix Workspace 应用程序最低版本 1909 中物理端点的本地桌面。

Microsoft Teams 中的外围设备

当 Microsoft Teams 的优化处于活动状态时，Citrix Workspace 应用程序将访问外围设备（耳机、麦克风、相机、扬声器等）。然后在 Microsoft Teams UI（设置 **>** 设备）中正确列出外围设备。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Microsoft Teams 不直接访问这些设备。相反，它依赖 Workspace 应用程序 WebRTC 媒体引擎来获取、捕获和处理媒体。Microsoft Teams 列出了供用户选择的设备。

建议：

- 具有内置回声消除功能的 Microsoft Teams 认证的耳机。在具有多个外围设备的设置中，如果麦克风和扬声器位于不同的设备，则可能会出现回声。例如，带有内置麦克风的网络摄像机和带扬声器的显示器。使用外部扬声器时，请尽可能远离麦克风和可能将声音折射到麦克风的任何表面。
- Microsoft Teams 认证的相机，但 Skype for Business 认证的外围设备与 Microsoft Teams 兼容。
- Citrix Workspace 应用程序媒体引擎无法利用 CPU 卸载与执行板载 H.264 编码 -UVC 1.1 和 1.5 的网络摄像机。

> 注意：
>
> 适用于 Windows 的 Workspace 应用程序 2009.6 现在可以获取具有 24 位音频格式或频率高于 96 kHz 的外围设备。
>
> HdxTeams.exe（在适用于 Windows 的 Workspace 应用程序 2009 或更高版本中）仅支持以下特定的音频设备格式（通道、位深度和采样率）：
>
> - 播放设备：最多 2 个通道，16 位，频率高达 96000 Hz
> - 录制设备：多达 4 个通道，16 位，频率高达 96000 Hz
>
> 即使一个扬声器或麦克风与预期设置不匹配，Teams 中的设备枚举也会失败，并且设置 **>** 设备下显示无。
>
> **HdxTeams.exe** 中的 **Webrpc** 日志显示以下类型的信息：
>
> ```
> Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing
> ...
> Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't
> create audio module!
> ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 解决方法：禁用特定设备或：
>
> 1. 打开声音控制面板 (mmsys.cpl)。
> 2. 选择播放或录制设备。
> 3. 转到属性 > 高级，然后将设置更改为支持的模式。

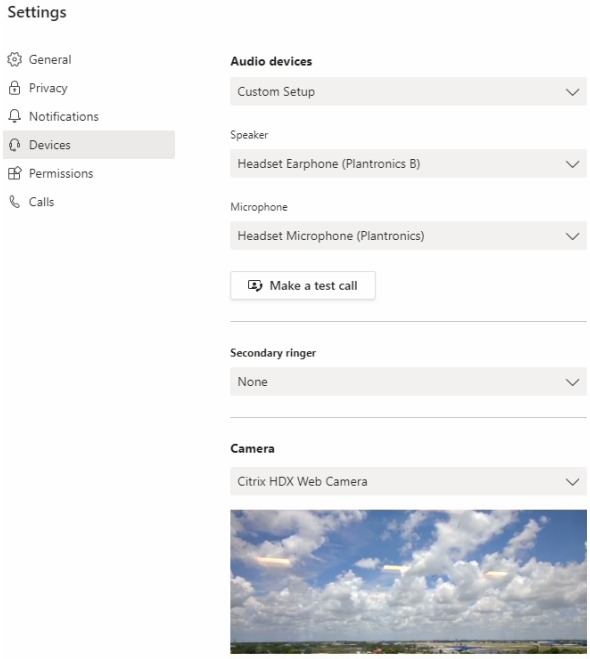
回退模式

如果 Microsoft Teams 无法在优化的 VDI 模式下加载（在“Teams”/“关于”/“版本”中显示“Citrix HDX 未连接”），VDA 将回退到旧版 HDX 技术，例如网络摄像机重定向以及客户端音频和麦克风重定向。如果您使用的是不支持 Teams 优化的 Workspace 应用程序版本/平台操作系统，则不应用回退注册表项。
在回退模式下，外围设备映射到 VDA。外围设备在 Microsoft Teams 应用程序中显示，就像它们在本地连接到虚拟桌面一样。

现在，您可以通过在 VDA 中设置注册表项来精确控制回退机制。有关信息，请参阅通过注册表管理的功能列表中的 Microsoft Teams 回退模式。

此功能需要 Teams 版本 1.3.0.13565 或更高版本。

在查看 Teams 中的设置 > 设备选项卡时，要确定您处于优化模式还是未优化模式，主要的区别是网络摄像机名称。如果 Microsoft Teams 在未优化模式下加载，旧版 HDX 技术将启动。网络摄像机名称具有 **Citrix HDX** 后缀，如下图所示。与优化模式相比，扬声器和麦克风设备名称可能略有不同（或被截断）。



使用旧版 HDX 技术时，Microsoft Teams 不会将音频、视频和屏幕共享处理卸载到端点的 Citrix Workspace 应用程序 WebRTC 媒体引擎。相反，HDX 技术使用服务器端呈现。打开视频时，预计 VDA 上的 CPU 消耗很高。实时音频性能可能不是最佳的。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

已知限制

Citrix 限制

Citrix Workspace 应用程序的限制：

- HID 按钮 - 不支持接听呼叫和结束通话。支持调高和调低音量。
- 备用铃声（**Teams >** 设置 **>** 设备）不受支持。
- Microsoft Teams 管理中心中的 QoS 设置不适用于 VDI 用户。
- Citrix Workspace 应用程序的应用程序保护附加功能可防止出站屏幕共享，并阻止传入屏幕共享和视频。

VDA 的限制：

- 将 Citrix Workspace 应用程序的“高 DPI”设置配置为是时，如果显示器的 DPI 缩放系数设置为高于 100%，则重定向的视频窗口不会显示在恰当的位置。

Citrix Workspace 应用程序和 VDA 的限制：

- 传出屏幕共享：不支持应用程序共享。
- 只能使用客户端计算机上（而非 VDA 上）的音量栏控制优化的通话的音量。

Microsoft 限制

- 不支持用于模糊或自定义背景的选项。
- 不支持 3x3 库视图。Microsoft Teams 依赖项 - 联系 Microsoft，了解何时可以期待 3x3 网格。
- 与 Skype for Business 的互操作性仅限于音频通话，没有视频模式。
- 传入和传出视频流的最大分辨率为 720p。Microsoft Teams 依赖项—联系 Microsoft，了解何时可以期待 1080p。
- 不支持 PSTN 呼叫回铃音。
- 不支持适用于直接路由的媒体旁路。
- 仅支持来自传入摄像机或屏幕共享流的一个视频流。当有一个传入屏幕共享时，将显示该屏幕共享，而非显示主扬声器的视频。
- 不支持广播和现场活动策划人和主持人角色。与会者角色受支持但未优化（而是在 VDA 上呈现）。
- 不支持 Microsoft Teams 中的放大和缩小功能。

Citrix 和 **Microsoft** 限制

- 执行屏幕共享时，包括系统音频选项不可用。
- 不支持弹出式聊天（也称为多窗口聊天或新会议体验）。
- VDI 参与者支持分组讨论会议室。如果组织者是 VDI 用户，Microsoft Teams 将不支持分组讨论会议室。
- 授予控制权和获取控制权：在屏幕共享或应用程序共享会话期间不受支持. 仅在 PowerPoint 共享会话期间受支持。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 不支持 E911 和基于位置的路由。

其他信息

- 监视、故障排除和支持 Microsoft Teams
- 将 Teams 桌面应用程序部署到 VM
- 使用 MSI 安装 Microsoft Teams（VDI 安装部分）
- 瘦客户端
- Skype for Business 网络评估工具
- 了解 Microsoft Teams 和 Skype for Business 的共存与互操作性

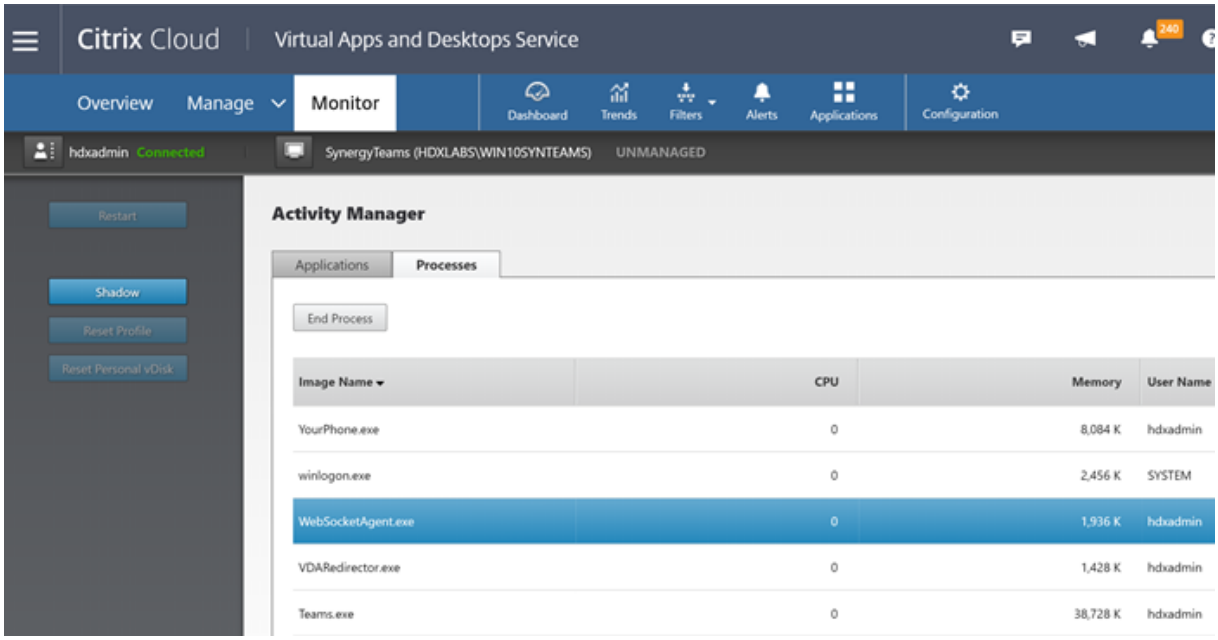
监视、故障排除和支持 **Microsoft Teams**

January 21, 2022

监视 **Teams**

本部分提供了使用 HDX 监视 Microsoft Teams 优化的指南。

如果用户在优化模式下运行并且 `HdxTeams.exe` 或 `HdxRtcEngine.exe` 正在客户端计算机上运行，则 VDA 中存在一个名为 `WebSocketAgent.exe` 的进程正在会话中运行。使用 Director 中的活动管理器查看应用程序。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用 VDA 最低版本 1912，可以使用 Citrix HDX Monitor（最低版本 3.11）监视活动的 Teams 呼叫。Citrix Virtual Apps and Desktops 产品 ISO 包含文件夹 `layout\image-full\Support\HDX Monitor` 中的最新 `hdxmonitor.msi`。

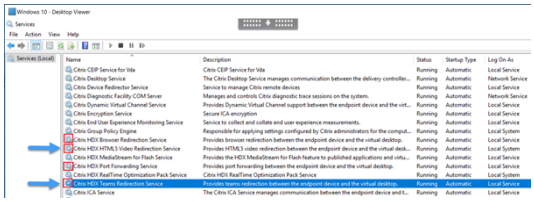
有关详细信息，请参阅知识中心文章 CTX253754 中的监视。

故障排除

本部分内容提供故障排除提示，解决您在使用 Microsoft Teams 优化时可能遇到的问题。有关详细信息，请参阅 CTX253754。

在 **Virtual Delivery Agent** 上

BCR_x64.msi 安装四个服务。只有两个服务负责 VDA 中的 Microsoft Teams 重定向。

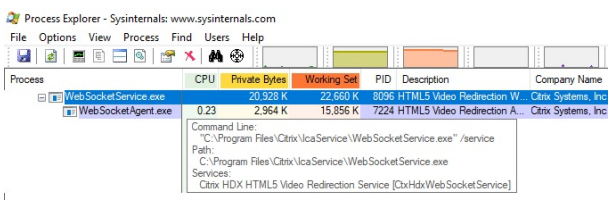


- **Citrix HDX Teams** 重定向服务建立 Microsoft Teams 中使用的虚拟通道。该服务依赖于 CtxSvcHost.exe。
- **Citrix HDX HTML5** 视频重定向服务作为 WebSocketService.exe 在 127.0.0.1:9002 TCP 上侦听。WebSocketService.exe 执行两项主要功能：

  i. 安全 **WebSocket** 的 **TLS** 终止接收来自 vdiCitrixPeerConnection.js 的安全 WebSocket 连接，这是 Microsoft Teams 应用程序中的一个组件。您可以使用进程监视器对其进行跟踪。有关证书的详细信息，请参阅 Controller 与 VDA 之间的通信下的“TLS 和 HTML5 视频重定向以及浏览器内容重定向”部分。

  一些防病毒和桌面安全软件会干扰 `WebSocketService.exe` 及其证书的正常运行。虽然 Citrix HDX HTML5 Video Redirection 服务 (Citrix HDX HTML5 Video Redirection) 可能正在 `services.msc` 控制台中运行，但 localhost `127.0.0.1:9002` TCP 套接字从未处于侦听模式，如 netstat 中所示。尝试重新启动服务会导致其挂起（“正在停止…”）。确保为 `WebSocketService.exe` 流程应用正确的排除项。

  ii. 用户会话映射。当 Microsoft Teams 应用程序启动时，WebSocketService.exe 将在 VDA 中的用户会话中启动 WebSocketAgent.exe 进程。WebSocketService.exe 作为 LocalSystem 帐户在会话 0 中运行。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

可以使用 `netstat` 来检查 VDA 中的 WebSocketService.exe 服务是否处于主动侦听状态。

从提升的命令提示符窗口运行 `netstat -anob -p tcp`:

```
 TCP    127.0.0.1:9001         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
 TCP    127.0.0.1:9002         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
```

在成功连接时，状态将更改为“已建立”:

```
 TCP    127.0.0.1:9002         127.0.0.1:58069        ESTABLISHED     8096
[WebSocketService.exe]
 TCP    127.0.0.1:58069        127.0.0.1:9002         ESTABLISHED     748
[Teams.exe]
```

> 重要:
>
> WebSocketService.exe 在两个 TCP 套接字中侦听，即 127.0.0.1:9001 和 127.0.0.1:9002。端口 9001 用于浏览器内容重定向和 HTML5 视频重定向。端口 9002 用于 Microsoft Teams 重定向。确保 VDA 的 Windows 操作系统中没有任何可能会阻止 Teams.exe 和 WebSocketService.exe 之间直接进行通信的代理配置。有时，当您在 Internet Explorer 11（**Internet** 选项 **>** 连接 **>** 局域网设置 **>** 代理服务器）中配置显式代理时，可能会通过已分配的代理服务器进行连接。确认使用手动和显式代理设置时是否选中对于本地地址不使用代理服务器。

服务位置和说明

服务	Windows Server OS 中可执行文件的路径	登录身份	说明
Citrix HTML5 视频重定向服务	“C:\Program Files (x86)\Citrix\System32\WebSocketService.exe” /service	本地系统帐户	通过在虚拟桌面与端点设备之间执行媒体重定向所需的初始框架提供了多个 HDX 多媒体服务。
Citrix HDX 浏览器重定向服务	“C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe” -g BrowserRedirSvcs	此帐户（本地服务）	在端点设备与虚拟桌面之间提供浏览器内容重定向。
Citrix 端口转发服务	“C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe” -g PortFwdSvcs	此帐户（本地服务）	在端点设备与虚拟桌面之间为浏览器内容重定向提供端口转发。
Citrix HDX Teams 重定向服务	“C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe” -g TeamsSvcs	本地系统帐户	在端点设备与虚拟桌面之间提供 Microsoft Teams 重定向。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Workspace 应用程序

在用户的端点上，适用于 Windows 的 Citrix Workspace 应用程序将实例化名为 HdxTeams.exe 或 HdxRtcEngine.exe 的新服务。当 Microsoft Teams 在 VDA 中启动并且用户尝试在自助预览中调用或访问外围设备时会执行此操作。如果您没有看到此服务，请检查以下内容：

1. 确保您至少安装了适用于 Windows 的 Workspace 应用程序版本 1905。您是否在 Workspace 应用程序安装路径中看到 HdxTeams.exe 或 HdxRtcEngine.exe 和 webrpc.dll 二进制文件？
2. 如果验证了步骤 1，请执行以下操作以检查 HdxTeams.exe 或 HdxRtcEngine.exe 是否正在启动。
    a) 在 VDA 上退出 Microsoft Teams。
    b) 在 VDA 上启动 services.msc。
    c) 停止 Citrix HDX Teams 重定向服务。
    d) 断开 ICA 会话的连接。
    e) 连接 ICA 会话。
    f) 启动 Citrix HDX Teams 重定向服务。
    g) 重新启动 Citrix HDX HTML5 视频重定向服务。
    h) 在 VDA 启动 Microsoft Teams。
3. 如果您仍然没有看到正在客户端端点上启动的 HdxTeams.exe 或 HdxRtcEngine.exe，请执行以下操作：
    a) 重新启动 VDA。
    b) 重新启动客户端端点。

支持

Citrix 和 Microsoft 联合支持使用 Microsoft Teams 优化从 Citrix Virtual Apps and Desktops 交付 Microsoft Teams。这种联合支持是两家公司密切合作的结果。如果您有有效的支持合同，并且遇到此解决方案的问题，请与您怀疑其代码导致该问题的供应商打开支持票证。也就是说，Teams 有关的问题请联系 Microsoft，优化组件有关的问题请联系 Citrix。
Citrix 或 Microsoft 会收到票证、对问题进行分级并根据需要上报。您无需联系每个公司的支持团队。

遇到问题时，我们建议您在 Teams UI 中单击帮助 **>** 报告问题。Citrix 与 Microsoft 之间自动共享 VDA 端日志，以更快地解决技术问题。

收集日志

HDX 媒体引擎日志可以在用户的计算机（而非 VDA）上找到。如果出现任何问题，请务必将日志附加到您的支持案例中。

Windows 日志：

可以在%TEMP% 下的 **HDXTeams** 文件夹（AppData/Local/Temp/HDXTeams 或 AppData/Local/Temp/HdxRtcEngine）中找到 Windows 日志。查找名为 webrpc_Day_Month_timestamp_Year.txt 的.txt 文件。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

如果您使用的是较新版本的 Citrix Workspace 应用程序（例如 Citrix Workspace 应用程序 2009.5 或更高版本），请将日志存储在 AppData\Local\Temp\HdxRtcEngine 中。

每个会话都会为日志创建单独的文件夹。

Mac 日志：

1. VDWEBRTC 日志 - 记录虚拟通道的执行情况。

   位置：/Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt

2. HdxRtcEngine 日志 - 记录 HdxRtcEngine 上进程的执行情况。

   位置：$TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log

   HdxRtcEngine 日志默认处于启用状态。

Linux 日志：

可以在 /tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/ 目录中找到 Linux 日志。

建立通话时，需要以下四个 ICE 阶段：

- 候选收集
- 候选交换
- 连接性检查（STUN 绑定请求）
- 候选提升

在 HdxTeams.exe/HdxRtcEngine.exe 日志中，以下条目是相关互动式连接建立 (ICE) 条目。这些条目是为成功设置通话而必须存在的（请参阅此用于收集阶段的示例代码段）：

```
1  RPCStubs Info: -> device id = \\?\display#int3470#4&1835d135&0&uid13424
       #{
2   65e8773d-8f56-11d0-a3b9-00a0c9223196 }
3   {
4   bf89b5a5-61f7-4127-a279-e187013d7caf }
5    label = Microsoft Camera Front groupId =
6
7  webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1
8  webrtcapi.RTCPeerConnection Info: setLocalDescription.
9  >>> begin:sdp
10 [...]
11
12 webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
       HaveLocalOffer
13
14 webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
       Gathering
15
16 [...]
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
>>> begin:sdp
candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
    generation 0 ufrag oVk6 network-id 1
<<< end:sdp
[…]
>>> begin:sdp
candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay
    raddr 73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1
    network-cost 10
<<< end:sdp
[…]
>>> begin:sdp
candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx
    raddr 10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id
    1
<<< end:sdp
[…]

webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
    Complete webrtcapi.RTCPeerConnection Info: setRemoteDescription.
>>> begin:sdp
[…]

webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
    HaveRemotelOffer

<!--NeedCopy-->
```

如果有多个 ICE 候选，则首选顺序为：

1. host
2. 对端反向
3. 服务器反向
4. 传输中继

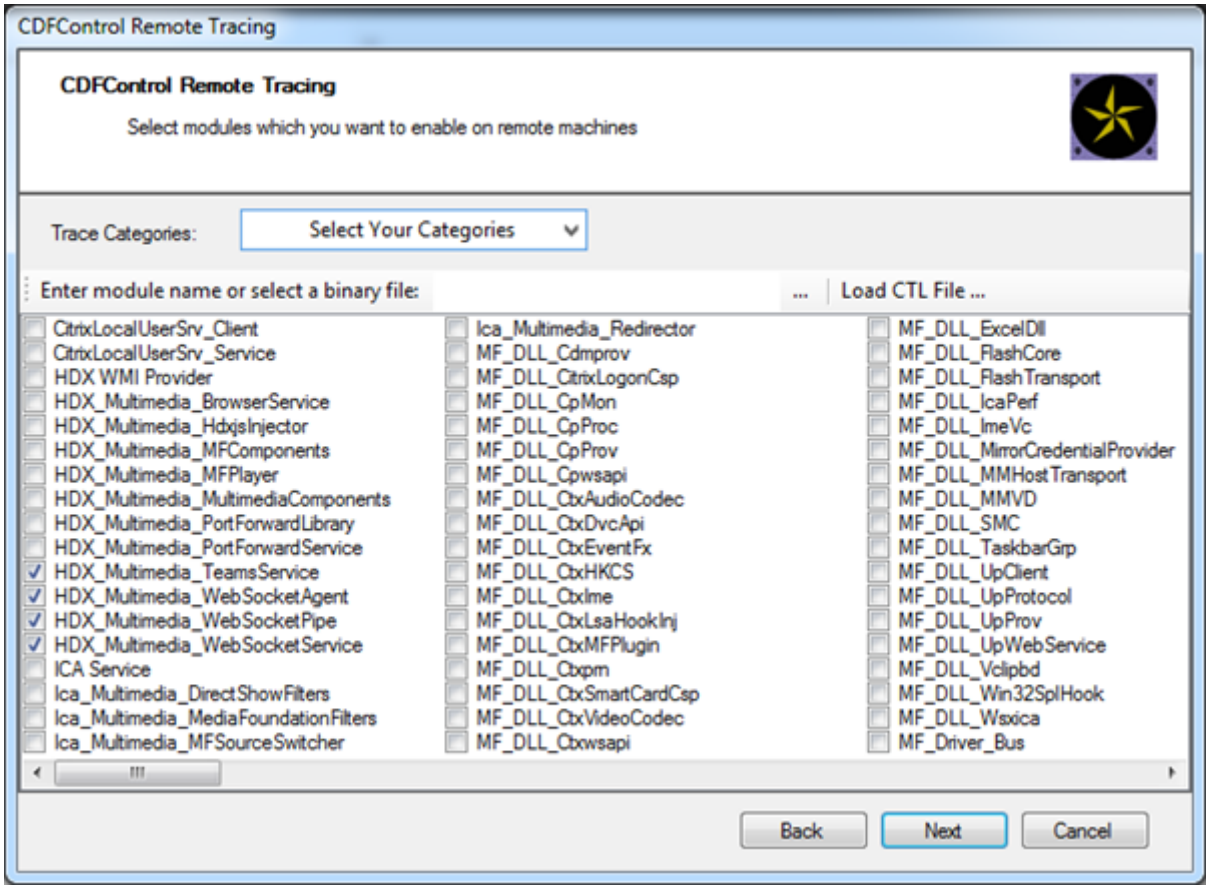
如果您遇到问题并且可以持续重现该问题，我们建议您在 Teams 中单击帮助 **>** 报告问题。如果您通过 Microsoft 开立了一个案例，Citrix 与微软之间将共享日志以解决技术问题。

在联系 Citrix 支持部门之前捕获 CDF 跟踪也非常有益。有关详细信息，请参阅知识中心文章 CDFcontrol。

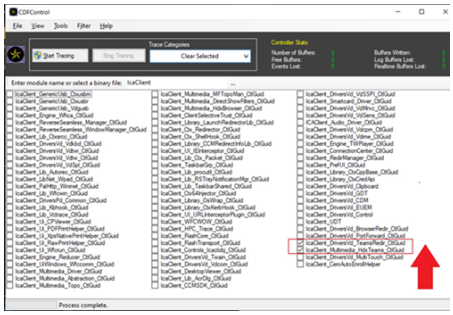
有关收集 CDF 跟踪信息的建议，请参阅知识中心文章收集 CDF 跟踪信息的建议。

VDA 端 **CDF** 跟踪 **-** 启用以下 **CDF** 跟踪提供程序：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Workspace 应用程序端 **CDF** 跟踪 **-** 启用以下 **CDF** 跟踪提供程序：



- IcaClient_DriversVd_TeamsRedir（可选）
- IcaClient_Multimedia_HdxTeams（需要 Citrix Workspace 应用程序 2012 年或更高版本）

Windows Media 重定向

January 21, 2022

Windows Media 重定向控制和优化服务器向用户交付流音频和视频的方式。Windows Media 重定向通过在客户

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

端设备而非服务器上播放媒体运行时文件来降低播放多媒体文件时的带宽要求。Windows Media 重定向可提升虚拟 Windows 桌面上运行的 Windows Media Player 以及兼容播放器的性能。

如果不满足 Windows Media 客户端内容提取的要求，媒体交付将自动使用服务器端提取。此方法对用户而言是透明的。您可以使用 Citrix Scout 从 HostMMTransport.dll 执行 Citrix Diagnosis Facility (CDF) 跟踪，以确定使用的方法。有关详细信息，请参阅 Citrix Scout。

Windows Media 重定向在主机服务器上截获媒体管道，捕获本机压缩格式的媒体数据，然后将内容重定向到客户端设备。客户端设备随后重新创建媒体管道以解压缩并呈现从主机服务器接收的媒体数据。Windows Media 重定向在运行 Windows 操作系统的客户端设备上正常运行。这些设备具有所需的多媒体框架以重新构建媒体渠道，就像它已经存在于主机服务器上一样。Linux 客户端使用相同的开源媒体框架来重新构建媒体管道。

策略设置 **Windows Media** 重定向控制此功能，并且默认设置为允许。通常情况下，此设置可将从服务器上呈现的音频和视频的质量提高到一个可与客户端设备上本地播放的音频和视频的质量相提并论的级别。在极少数情况下，使用 Windows Media 重定向播放媒体的效果比使用基本 ICA 压缩和常规音频所呈现的效果差。您可以通过向策略中添加 **Windows Media** 重定向设置并将其值设置为禁止来禁用此功能。

有关策略设置的详细信息，请参阅多媒体策略设置。

限制：

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

常规内容重定向

January 21, 2022

内容重定向功能允许您控制用户是使用在服务器上发布的应用程序来访问信息，还是使用用户设备上本地运行的应用程序来访问信息。

客户端文件夹重定向

客户端文件夹重定向改变了在主机端会话中访问客户端文件的方式。

- 当仅在服务器上启用客户端驱动器映射时，客户端满载的卷会作为通用命名约定 (UNC) 链接自动映射到会话中。
- 如果您在服务器上启用客户端文件夹重定向，同时用户也在 Windows 桌面设备上配置了客户端文件夹重定向，将重定向用户指定的部分本地卷。

主机到客户端重定向

请考虑对特定的不常见用例使用主机到客户端重定向。通常情况下，其他形式的内容重定向可能会更好。我们仅支持在多会话操作系统 VDA（而非单会话操作系统 VDA）上使用此种类型的重定向。

本地应用程序访问和 URL 重定向

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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桌面环境中。这样做不会将其从一台计算机更改到另一台计算机。

HDX 技术为没有任何优化的支持的特殊设备或优化的支持不适用的场合提供通用 **USB** 重定向。

客户端文件夹重定向

January 21, 2022

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。如果您仅在服务器上启用了客户端驱动器映射，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。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在会话内部显示为 UNC 链接。即，不显示为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 单会话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 Workspace 应用程序中。

要求：

对于服务器：

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

对于客户端：

- Windows 10 32 位和 64 位版本（最低版本 1607）
- Windows 8.1，32 位和 64 位版本（包括 Embedded Edition）
- Windows 7，32 位和 64 位版本（包括 Embedded Edition）

要在服务器上启用客户端文件夹重定向，请参阅通过注册表管理的功能列表中的客户端文件夹重定向。

在用户设备上，指定要重定向的文件夹：

1. 确保安装了最新版本的 Citrix Workspace 应用程序。
2. 从 Citrix Workspace 应用程序安装目录启动 CtxCFRUI.exe。
3. 选择自定义单选按钮，然后添加、编辑或删除文件夹。
4. 断开连接然后重新连接会话，以使设置生效。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

主机到客户端重定向

January 21, 2022

主机到客户端重定向允许使用用户端点设备上的相应应用程序打开作为超链接嵌入在 Citrix 会话上运行的应用程序中的 URL。主机到客户端重定向的一些常见用例包括：

- Citrix 服务器无法通过 Internet 或网络访问源的情况下的 Web 站点的重定向。
- 出于安全性、性能、兼容性或可扩展性的原因而不需要在 Citrix 会话内运行 Web 浏览器时的 Web 站点的重定向。
- Citrix 服务器上未安装打开 URL 所需的应用程序时特定 URL 类型的重定向。

主机到客户端重定向不适用于您在 Web 页面上访问的 URL，也不适用于在 Citrix 会话中运行的 Web 浏览器的地址栏中键入的 URL。有关 Web 浏览器中的 URL 的重定向，请参阅双向 URL 重定向或浏览器内容重定向。

系统要求

- 多会话操作系统 VDA
- 支持的客户端：
  - 适用于 Windows 的 Citrix Workspace 应用程序
  - 适用于 Mac 的 Citrix Workspace 应用程序
  - 适用于 Linux 的 Citrix Workspace 应用程序
  - 适用于 HTML5 的 Citrix Workspace 应用程序
  - 适用于 Chrome 的 Citrix Workspace 应用程序

客户端设备必须安装并配置应用程序以处理 URL 类型的重定向。

配置

请使用主机到客户端重定向 Citrix 策略启用此功能。默认情况下，主机到客户端重定向处于禁用状态。启用主机到客户端重定向策略后，Citrix Launcher 应用程序将向 Windows 服务器注册，以确保其可以拦截 URL 并将其发送到客户端设备。

然后，您必须将 Windows 组策略配置为使用 Citrix Launcher 作为面向所需 URL 类型的默认应用程序。在 Citrix 服务器 VDA 上，创建 ServerFTAdefaultPolicy.xml 文件并插入以下 XML 代码。

```
<?xml version="1.0" encoding="UTF-8"?>

<DefaultAssociations>

<Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="
    ServerFTA" />
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
6
7  <Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName=
       "ServerFTA" />
8
9  </DefaultAssociations>
10 <!--NeedCopy-->
```

在组策略管理控制台中，转到计算机配置 **>** 管理模板 **> Windows** 组件 **>** 文件资源管理器 **>** 设置默认关联配置文件，然后保存您的 ServerFTAdefaultPolicy.xml 文件。

> 注意：
>
> 如果 Citrix 服务器没有组策略设置，Windows 会提示用户选择用于打开 URL 的应用程序。

默认情况下，我们支持以下 URL 类型的重定向：

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

要在重定向列表中包含其他标准或自定义 URL 类型，请在之前引用的 ServerFTAdefaultPolicy.xml 文件中创建一个新的关联标识符行。例如：

```
<Association Identifier="ftp"ProgId="ServerFTAHTML"ApplicationName="
ServerFTA"/>

<Association Identifier="mailto"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>

<Association Identifier="customtype1"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>

<Association Identifier="customtype2"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>
```

向列表中添加 URL 类型还需要配置客户端。在 Windows 客户端上创建以下注册表项和值。

> 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。

- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- 值名称：ExtraURLProtocols
- 值类型：REG_SZ

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 值数据：指定所需的 URL 类型，用分号分隔。在 URL 的授权部分之前包括所有内容。例如：`ftp://;mailto:;customtype1://;custometype2://`

可以添加仅适用于 Windows 客户端的 URL 类型。缺少上述注册表设置的客户端拒绝重定向回 Citrix 会话。客户端必须安装并配置应用程序以处理指定的 URL 类型。

要从默认重定向列表中删除 URL 类型，请在服务器 VDA 上创建以下注册表项和值。

- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 值名称：DisableServerFTA
- 值类型：DWORD
- 值数据：1
- 值名称：NoRedirectClasses
- 值类型：REG_MULTI_SZ
- 值数据：指定值的任意组合：`http`、`https`、`rtsp`、`rtspu`、`pnm` 或 `mms`。在单独的行中输入多个值。例如：

```
http
https
rtsp
```

要为一组特定的 Web 站点启用主机到客户端重定向，请在服务器 VDA 上创建一个注册表项和值。

- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 值名称：ValidSites
- 值类型：REG_MULTI_SZ
- 数据：指定完全限定域名 (FQDN) 的任意组合。在单独的行中键入多个 FQDN。仅包括 FQDN，没有协议（`http://` 或 `https://`）。FQDN 只能在最左侧位置包含星号 (*) 作为通配符。这匹配一层域，与 RFC 6125 中的规则一致。例如：

```
www.exmaple.com
*.example.com
```

> 注意：
>
> 不能将注册表项 **ValidSites** 与注册表项 **DisableServerFTA** 和 **NoRedirectClasses** 结合使用。

服务器 **VDA** 默认浏览器配置

如本部分所述启用主机到客户端重定向将取代服务器 VDA 上之前的任何默认浏览器配置。如果未重定向 Web URL，Citrix Launcher 会将 URL 传递到在注册表项 `command_backup` 中配置的浏览器。默认情况下，该注册表项指

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

向 Internet Explorer，但您可以将其修改为包含指向不同浏览器的路径。有关详细信息，请参阅通过注册表管理的功能列表中的服务器 VDA 默认浏览器配置。

双向内容重定向

July 5, 2024

双向内容重定向允许在 Citrix VDA 会话与客户端端点之间双向转发 Web 浏览器中的 HTTP 或 HTTPS URL 或者嵌入到应用程序中的 HTTP 或 HTTPS URL。在 Citrix 会话中运行的浏览器中输入的 URL 可以使用客户端的默认浏览器打开。相反，在客户端上运行的浏览器中输入的 URL 可以通过已发布的应用程序或桌面在 Citrix 会话中打开。双向内容重定向的一些常见用例包括：

- 在起始浏览器无法通过网络访问源的情况下重定向 Web URL。
- 出于浏览器兼容性和安全原因重定向 Web URL。
- 不希望在 Citrix 会话或客户端上运行 Web 浏览器时重定向应用程序中嵌入的 Web URL。

系统要求

- 单会话或多会话操作系统 VDA
- 适用于 Windows 的 Citrix Workspace 应用程序

浏览器：

- Internet Explorer 11
- 带 Citrix Browser Redirection Extension 的 Google Chrome（可在 Google Chrome 网上应用店中购买）
- 带 Citrix Browser Redirection Extension 的 Microsoft Edge (Chromium)（可在 Google Chrome 网上应用店中购买）

配置

必须在 VDA 和客户端上使用 Citrix 策略启用双向内容重定向，重定向才能正常运行。默认情况下，双向内容重定向处于禁用状态。

有关 VDA 配置，请参阅 ICA 策略设置中的双向内容重定向。

有关客户端配置，请参阅适用于 Windows 的 Citrix Workspace 应用程序文档中的双向内容重定向。

必须使用显示的命令注册浏览器扩展程序。根据需要在 VDA 和客户端上根据正在使用的浏览器运行命令。

要在 VDA 上注册浏览器扩展程序，请打开命令提示符。然后，使用所需的浏览器选项运行 `%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe`，如显示的示例所示：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regIE
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regChrome
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regEdge
```

要在所有可用的浏览器上注册扩展程序，请运行：

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regall
```

要取消注册浏览器扩展程序，请使用显示的示例中所示的 /unreg<browser> 选项：

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /unregIE
```

要在客户端上注册浏览器扩展程序，请打开命令提示符，然后使用与显示的示例相同的选项运行 %ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe。

> 注意：
>
> register 命令会使 Chrome 和 Edge 浏览器在首次启动时提示用户启用 Citrix Browser Redirection Extension。也可以从 Google Chrome 网上应用店手动安装该浏览器扩展程序。

其他注意事项

- 浏览器要求和配置仅适用于启动重定向的浏览器。不考虑支持在重定向成功后打开 URL 的目标浏览器。将 URL 从 VDA 重定向到客户端时，只有 VDA 上需要支持的浏览器配置。相反，将 URL 从客户端重定向到 VDA 时，只有客户端上需要支持的浏览器配置。重定向的 URL 将移交给在目标计算机（客户端或 VDA）上配置的默认浏览器，具体取决于方向。不需要在 VDA 和客户端上使用相同的浏览器类型。
- 请检查重定向规则不会导致出现循环配置。例如，VDA 策略设置为重定向 https://www.citrix.com，而客户端策略设置为重定向同一 URL，从而导致无限循环。
- 仅支持 HTTP/HTTPS 协议 URL。不支持 URL 缩短程序。
- 客户端到 VDA 重定向要求使用管理员权限安装 Windows 客户端。
- 如果目标浏览器已打开，重定向的 URL 将在新选项卡中打开。否则，URL 将在新浏览器窗口中打开。
- 启用了本地应用程序访问 (LAA) 后，双向内容重定向不起作用。

本地应用程序访问和 **URL** 重定向

April 8, 2022

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，而无需从一个桌面切换到另一个桌面。利用本地应用程序访问，您可以：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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。
- 当应用程序独立于虚拟桌面托管时，请避免使用双跃点延迟。通过在用户的 Windows 设备上放置已发布应用程序的快捷方式来执行此操作。
- 使用如下应用程序：
  - 视频会议软件，例如 GoToMeeting。
  - 尚未虚拟化的特殊或利基应用程序。
  - 采用其他方式时会将大量数据从用户设备传输到服务器再返回用户设备的应用程序和外围设备。例如 DVD 刻录机或 TV 调谐器。

在 Citrix Virtual Apps and Desktops 中，托管的桌面会话使用 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 阻止列表）。如果导航至未列入阻止列表的 URL，则此 URL 会再次在桌面会话中打开。

URL 重定向仅适用于桌面会话，不适用于应用程序会话。唯一可用于应用程序会话的重定向功能是主机到客户端的内容重定向，它是服务器 FTA（文件类型关联）重定向的一种类型。此 FTA 可将某些协议（例如 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。没有任何 URL 阻止列表或允许列表支持。

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 Citrix Virtual Apps and Desktops 服务器到用户的计算机
- 在启动（而非重定向）它们的环境中呈现

要指定特定 Web 站点中内容的重定向路径，请在 Virtual Delivery Agent 上配置 URL 允许列表和 URL 阻止列表。这些名单包含多字符串注册表项，用于指定 URL 重定向策略设置。有关详细信息，请参阅本地应用程序访问策略设置。

URL 可在 VDA 上呈现，但存在以下例外情况：

- 地理/区域设置信息—需要区域设置信息的 Web 站点，如 msn.com 或 news.google.com（根据地理信息打开特定于某个国家/地区的页面）。例如，如果从位于英国的数据中心预配 VDA，而客户端从印度进行连接，用户期望看到 in.msn.com。但用户将看到 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。此功能重定向包含其他媒体类型（例如 Silverlight）的站点此过程在安全的环境中进行。也就是说，管理员批准的 URL 在客户端上运行，而其余 URL 将重定向到 VDA。

除 URL 重定向外，还可以使用 FTA 重定向。FTA 在会话中遇到文件时会启动本地应用程序。如果启动本地应用程序，则该应用程序必须具有此文件的访问权限才能将其打开。因此，只能使用本地应用程序打开位于网络共享或客户端驱动器（使用客户端驱动器映射）上的文件。例如，当打开 PDF 文件时，如果 PDF 阅读器是本地应用程序，则文件使用 PDF 阅读器打开。由于本地应用程序可以直接访问文件，因此，无需通过 ICA 网络传输文件，即可打开此文件。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

要求、注意事项和限制

我们支持在面向适用于 Windows 多会话操作系统的 VDA 和适用于 Windows 单会话操作系统的 VDA 的有效操作系统上使用本地应用程序访问。本地应用程序访问要求使用适用于 Windows 的 Citrix Workspace 应用程序版本 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：
  - 如果在窗口模式下运行或未覆盖所有显示器的虚拟桌面上使用本地应用程序访问，用户体验可能会非常混乱。
  - 多个显示器—最大化一个显示器时，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。即使后续的应用程序通常在其他显示器上启动，也会出现这种默认情况。
  - 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：
  - 驱动器盘符可能会使用户感到困惑，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。这些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。
  - 本地应用程序访问将复制 VDA 上的本地应用程序的属性（例如客户端桌面上和“开始”菜单中的快捷方式）。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。即，将 32 位本地应用程序与 64 位本地应用程序编组在一起。
  - 不能使用 COM 启动应用程序。例如，如果从 Office 应用程序中单击嵌入式 Office 文档，则检测不到进程启动，且本地应用程序集成失败。
- 用户从一个虚拟桌面会话内部启动另一个虚拟桌面的双跳场景不受支持。
- URL 重定向仅支持显式 URL（即，出现在浏览器的地址栏中或使用浏览器内的导航找到的 URL，具体取决于浏览器）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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。
- 如果将允许本地应用程序访问策略设置设为启用，则不支持浏览器内容重定向。默认情况下，禁止本地应用程序访问。

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，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 Workspace 应用程序，请执行以下操作：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 在本地客户端计算机上安装 Citrix Workspace 应用程序。可以在 Citrix Workspace 应用程序安装期间启用这两项功能，也可以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已启用。还可以为 URL 重定向配置 URL 允许列表和阻止列表策略设置。有关详细信息，请参阅本地应用程序访问策略设置。

启用本地应用程序访问和 **URL** 重定向

要为所有本地应用程序启用本地应用程序访问，请执行以下步骤：

1. 启动 Citrix Studio。
   - 对于本地部署，请从开始菜单中打开 **Citrix Studio**。
   - 对于云服务部署，请转到 **Citrix Cloud > Virtual Apps and Desktops** 服务 **>** 管理选项卡。
2. 在 Studio 导航窗格中，单击策略。
3. 在“操作”窗格中，单击创建策略。
4. 在“创建策略”窗口中，在搜索框中键入“允许本地应用程序访问”，然后单击选择。
5. 在“编辑设置”窗口中，选择允许。默认情况下，禁止允许本地应用程序访问策略。允许此设置时，VDA 允许最终用户决定是否在会话中启用已发布的应用程序和本地应用程序访问的快捷方式。（禁用此设置时，已发布的应用程序和本地应用程序访问的快捷方式不适用于 VDA。）此策略设置适用于整台计算机，URL 重定向策略也是如此。
6. 在“创建策略”窗口中，在搜索框中键入“URL 重定向允许列表”，然后单击选择。URL 重定向允许列表指定要在远程会话的默认浏览器中打开的 URL。
7. 在“编辑设置”窗口中，单击添加以添加 URL，然后单击确定。
8. 在“创建策略”窗口中，在搜索框中键入“URL 重定向阻止列表”，然后单击选择。URL 重定向阻止列表指定重定向到端点上运行的默认浏览器的 URL。
9. 在“编辑设置”窗口中，单击添加以添加 URL，然后单击确定。
10. 在“设置”页面上，单击下一步。
11. 在“用户和计算机”页面上，将策略分配给适用的交付组，然后单击下一步。
12. 在“摘要”页面上，查看设置，然后单击完成。

要在 Citrix Workspace 应用程序安装过程中为所有本地应用程序启用 URL 重定向，请按以下步骤进行操作：

1. 在安装 Citrix Workspace 应用程序时为计算机上的所有用户启用 URL 重定向。这样还会注册 URL 重定向所需的浏览器加载项。
2. 在命令提示窗口中，使用以下选项之一运行相应的命令以安装 Citrix Workspace 应用程序：
   - 对于 CitrixReceiver.exe，请使用 `/ALLOW_CLIENTHOSTEDAPPSURL=1`。
   - 对于 CitrixReceiverWeb.exe，请使用 `/ALLOW_CLIENTHOSTEDAPPSURL=1`。

使用组策略编辑器启用本地应用程序访问模板

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> - 在使用组策略编辑器启用本地应用程序访问模板之前，请将 receiver.admx/adml 模板文件添加到本地 GPO 中。有关详细信息，请参阅配置组策略对象管理模板。
> - 仅当您将 CitrixBase.admx/CitrixBase.adml 添加到%systemroot%\policyDefinitions 文件夹时，管理模板 **> Citrix** 组件 **> Citrix Workspace** 文件夹中的本地 GPO 中才会有适用于 Windows 的 Citrix Workspace 应用程序模板文件。

要使用组策略编辑器启用本地应用程序访问模板，请执行以下步骤：

1. 运行 **gpedit.msc**。
2. 转至计算机配置 **>** 管理模板 **>** 经典管理模板 **(ADM) > Citrix** 组件 **> Citrix Workspace >** 用户体验。
3. 单击本地应用程序访问设置。
4. 选择启用，然后选择允许 **URL** 重定向。对于 URL 重定向，请使用本文结尾的注册浏览器加载项部分中所述的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

可以使用注册表编辑器或 PowerShell SDK 提供对已发布应用程序的访问权限。

对于注册表编辑器，请参阅通过注册表管理的功能列表中的面向已发布应用程序的本地应用访问。

要使用 PowerShell SDK，请执行以下操作：

1. 在运行 Delivery Controller 的计算机上打开 PowerShell。
2. 输入以下命令：`set-configsitemetadata -name "studio_clientHostedAppsEnabled "-value "true"`。

要在云服务部署中访问添加本地应用程序访问应用程序，请使用 Citrix Virtual Apps and Desktops 远程 PowerShell SDK。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 远程 PowerShell SDK。

1. 下载安装程序：

   https://download.apps.cloud.com/CitrixPoshSdk.exe

2. 运行以下命令：

   a) `asnp citrix.*`
   b) `Get-XdAuthentication`

3. 输入以下命令：`set-configsitemetadata -name “studio_clientHostedAppsEnabled” -value “true”`。

完成上述适用的步骤后，请按照以下步骤继续操作。

1. 从开始菜单中打开 **Citrix Studio**。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. 在 Studio 导航窗格中，单击应用程序。
3. 在中上部的窗格中，右键单击空白区域，然后从上下文菜单中选择添加本地应用程序访问应用程序。还可以单击“操作”窗格中的添加本地应用程序访问应用程序。要在“操作”窗格中显示“添加本地应用程序访问应用程序”选项，请单击刷新。
4. 发布本地应用程序访问应用程序。
    - 此时将启动“添加应用程序”向导，并打开一个“简介”页面，您可以在将来启动此向导时不再显示该页面。
    - 该向导将引导您访问“组”、“位置”、“标识”、“应用程序”和“摘要”页面，如下所述。完成每个页面之后，请单击下一步，直到到达“摘要”页面为止。
    - 在“组”页面上，选择一个或多个要添加新应用程序的交付组，然后单击下一步。
    - 在“位置”页面上，键入用户的本地计算机上的应用程序的完整可执行文件路径，然后键入应用程序所在的文件夹的路径。Citrix 建议您使用系统环境变量路径；例如，%ProgramFiles(x86)%\Internet Explorer\iexplore.exe。
    - 在“标识”页面上，接受默认值或键入所需的信息，然后单击下一步。
    - 在“交付”页面上，配置通过何种方式将此应用程序交付给用户，然后单击下一步。可以为所选应用程序指定图标。还可以指定虚拟桌面上的本地应用程序的快捷方式是否显示在“开始”菜单、桌面或二者上。
    - 在“摘要”页面上，查看设置，然后单击完成以退出本地应用程序访问向导。

注册浏览器加载项

> 注意：
>
> 使用 /ALLOW_CLIENTHOSTEDAPPSURL=1 选项从命令行安装 Citrix Workspace 应用程序时，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，<*browser*> 为 Internet Explorer、Firefox、Chrome 或“全部”。

例如，以下命令在运行 Citrix Workspace 应用程序的设备上注册 Internet Explorer 加载项。

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

以下命令在 Windows 多会话操作系统 VDA 上注册所有加载项。

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

浏览器间的 **URL** 拦截

- 默认情况下，Internet Explorer 重定向指定的 URL。如果该 URL 不在阻止列表中，但浏览器或 Web 站点将其重定向到其他 URL，则最终的 URL 不会被重定向。即使该 URL 在阻止列表中，也不会被重定向。

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允许或阻止安装加载项。请允许加载项，以便功能正常运行。

- 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。禁用了扩展时，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。

配置在注销和断开连接时本地应用程序的行为

> 注意：
>
> 如果未执行以下步骤来配置这些设置，则默认情况下，当用户从虚拟桌面注销或断开连接时，本地应用程序将继续运行。重新连接后，如果本地应用程序在虚拟桌面中可用，则将重新集成。

要配置注销和断开连接时的本地应用程序行为，请参阅通过注册表管理的功能列表中的注销和断开连接时本地应用程序的行为。

通用 **USB** 重定向和客户端驱动器注意事项

July 5, 2024

HDX 技术为最常用的 USB 设备提供了优化的支持。优化的支持可提供改进的用户体验和通过 WAN 实现的更高性能和带宽效率。通常情况下，优化的支持即是最佳选择，尤其对于存在高延迟的环境或对安全性极为敏感的环境更是如此。

HDX 技术为没有优化的支持的特殊设备或优化的支持不适用的场合提供通用 **USB** 重定向，例如：

- USB 设备具有更多不属于优化的支持的高级功能，例如具有更多按钮的鼠标或网络摄像机。
- 用户需要不属于优化的支持的功能。
- USB 设备属于专业化设备，诸如测试和测量设备或工业控制器。
- 某个应用程序需要直接访问该设备作为一个 USB 设备。
- 该 USB 设备仅具有一个可用的 Windows 驱动程序。例如，某个智能卡读卡器可能没有可用于适用于 Android 的 Citrix Workspace 应用程序的驱动程序。
- 该版本的 Citrix Workspace 应用程序没有为这种类型的 USB 设备提供任何优化的支持。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。

> 重要：
>
> - 通用 USB 重定向可以与优化的支持一起使用。如果启用了通用 USB 重定向，请同时针对通用 USB 重定向和优化的支持配置 Citrix USB 设备策略设置。
> - 客户端 USB 设备优化规则中的 Citrix 策略设置是针对通用 USB 重定向的特定设置，适用于某种特定的 USB 设备。而不适用于此处所述的优化的支持。

USB 设备的性能注意事项

使用通用 USB 重定向时，对于某些类型的 USB 设备而言，网络延迟和带宽会影响用户体验和 USB 设备操作。例如，对时间极为敏感的设备可能无法在高延迟低带宽的链路上正常工作。可能的情况下可转而使用优化的支持。

某些 USB 设备需要高带宽才能使用，例如，3D 鼠标（与通常也需要使用高带宽的 3D 应用程序一起使用）。如果无法增加带宽，您也许能够通过使用带宽策略设置来调整其他组件的带宽使用情况，从而缓解该问题。有关详细信息，请参阅客户端 USB 设备重定向的带宽策略设置和多流连接策略设置。

USB 设备的安全注意事项

某些 USB 设备本质上属于安全敏感型设备，例如智能卡读卡器、指纹读取器和电子签名板。诸如 USB 存储设备等其他 USB 设备可能会用于传输敏感的数据。

USB 设备经常用于散布恶意软件。Citrix Workspace 应用程序和 Citrix Virtual Apps and Desktops 的配置可减少这些 USB 设备所带来的风险，但不会彻底消除风险。无论是否使用通用 USB 重定向或优化的支持，这种情况均适用。

> 重要：
>
> 对于安全敏感型设备和数据，请始终使用 TLS 或 IPsec 来保护 HDX 连接。
>
> 仅对您需要的 USB 设备启用支持。同时配置通用 USB 重定向和优化的支持来满足这种需求。
>
> 向用户提供安全使用 USB 设备的指导：
>
> - 仅使用从可信来源获取的 USB 设备。
> - 请勿单独将 USB 设备遗留在开放式环境中，例如，网吧中的闪存驱动器。
> - 讲解在多台计算机中使用一个 USB 设备的风险。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

通用 **USB** 重定向的兼容性

通用 USB 重定向支持 USB 2.0 及更早的设备。通用 USB 重定向还支持连接到 USB 2.0 或 USB 3.0 端口的 USB 3.0 设备。通用 USB 重定向不支持 USB 3.0 中引入的 USB 功能，诸如超高速。

以下 Citrix Workspace 应用程序支持通用 USB 重定向：

- 适用于 Windows 的 Citrix Workspace 应用程序，请参阅配置应用程序交付。
- 适用于 Mac 的 Citrix Workspace 应用程序，请参阅适用于 Mac 的 Citrix Workspace 应用程序。
- 适用于 Linux 的 Citrix Workspace 应用程序，请参阅优化。
- 适用于 Chrome OS 的 Citrix Workspace 应用程序，请参阅适用于 Chrome 的 Citrix Workspace 应用程序。

有关 Citrix Workspace 应用程序版本，请参阅 Citrix Workspace 应用程序功能列表。

如果您使用的是早期版本的 Citrix Workspace 应用程序，请参阅 Citrix Workspace 应用程序文档以确认是否支持通用 USB 重定向。请参阅 Citrix Workspace 应用程序文档以了解有关受支持的 USB 设备类型的任何限制。

从适用于单会话操作系统的 VDA 7.6 版至当前版本运行的桌面会话支持通用 USB 重定向。

从适用于多会话操作系统的 VDA 7.6 版至当前版本运行的桌面会话支持通用 USB 重定向，但具有以下限制：

- VDA 必须运行 Windows Server 2012 R2 或 Windows Server 2016。
- USB 设备驱动程序必须完全兼容适用于 VDA OS (Windows 2012 R2) 的远程桌面会话主机 (RDSH)，包括完整的虚拟化支持。

某些类型的 USB 设备不受通用 USB 重定向的支持，因为重定向这些设备不会有任何益处：

- USB 调制解调器。
- USB 网络适配器。
- USB 集线器。连接到 USB 集线器的 USB 设备被单独处理。
- USB 虚拟 COM 端口。使用 COM 端口重定向而非通用 USB 重定向。

有关已完成通用 USB 重定向测试的 USB 设备的信息，请参阅 Citrix Ready Marketplace。某些 USB 设备在使用通用 USB 重定向时无法正确操作。

配置通用 **USB** 重定向

可以控制并分别配置哪些类型的 USB 设备可以使用通用 USB 重定向：

- 在 VDA 上，使用 Citrix 策略设置。有关详细信息，请参阅策略设置参考中的客户端驱动器和用户设备的重定向和 USB 设备策略设置
- 在 Citrix Workspace 应用程序中，使用依赖于 Citrix Workspace 应用程序的机制。例如，管理模板控制用于配置适用于 Windows 的 Citrix Workspace 应用程序的注册表设置。默认情况下，会允许某些类型的 USB 设备使用 USB 重定向功能，而拒绝其他类型的 USB 设备使用。有关详细信息，请参阅适用于 Windows 的 Citrix Workspace 应用程序文档中的配置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

这种单独配置提供了灵活性。例如：

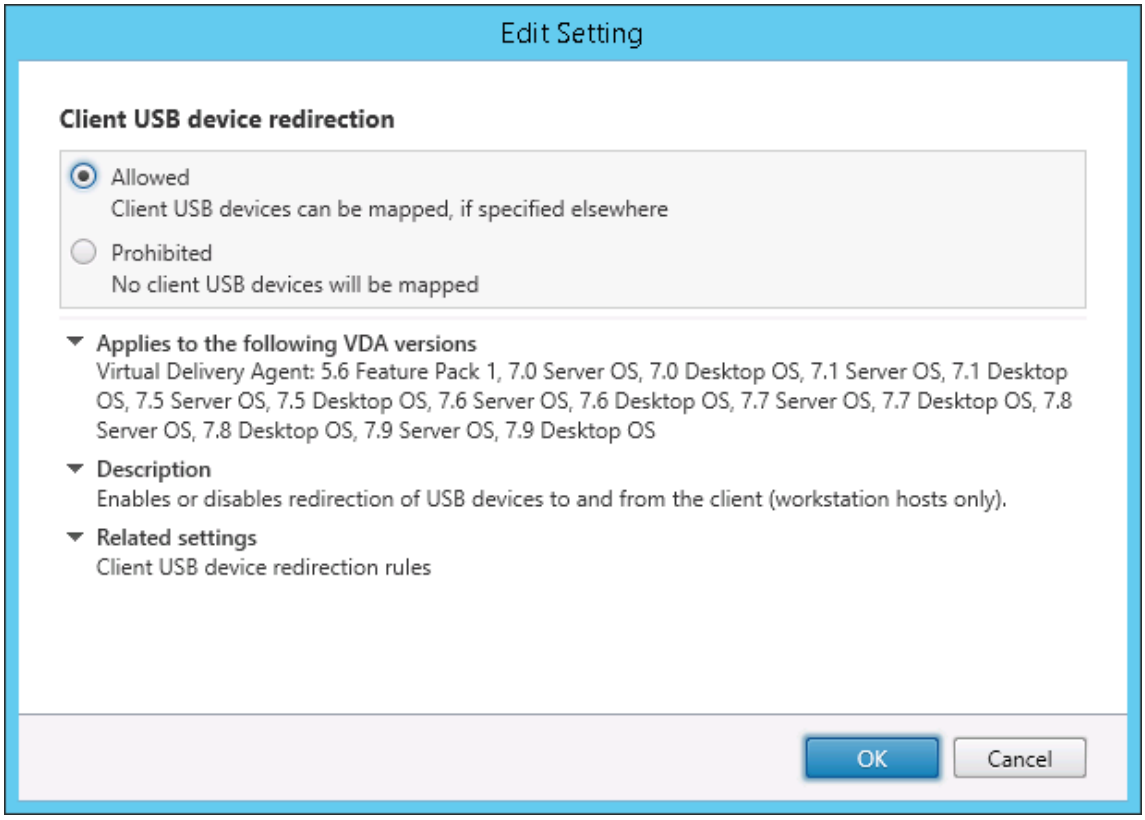
- 如果两个不同的组织或部门负责 Citrix Workspace 应用程序和 VDA，他们可以单独执行控制。当一个组织中的用户访问另一个组织中的应用程序时，此配置适用。
- Citrix 策略设置可以控制仅允许特定用户或某些仅通过 LAN（而不是通过 Citrix Gateway）进行连接的用户使用的 USB 设备。

启用通用 **USB** 重定向

要启用通用 USB 重定向，并且不需要用户手动进行重定向，请配置 Citrix 策略设置和 Citrix Workspace 应用程序连接首选项。

在 Citrix 策略设置中：

1. 向策略中添加客户端 USB 设备重定向，并将其值设置为允许。

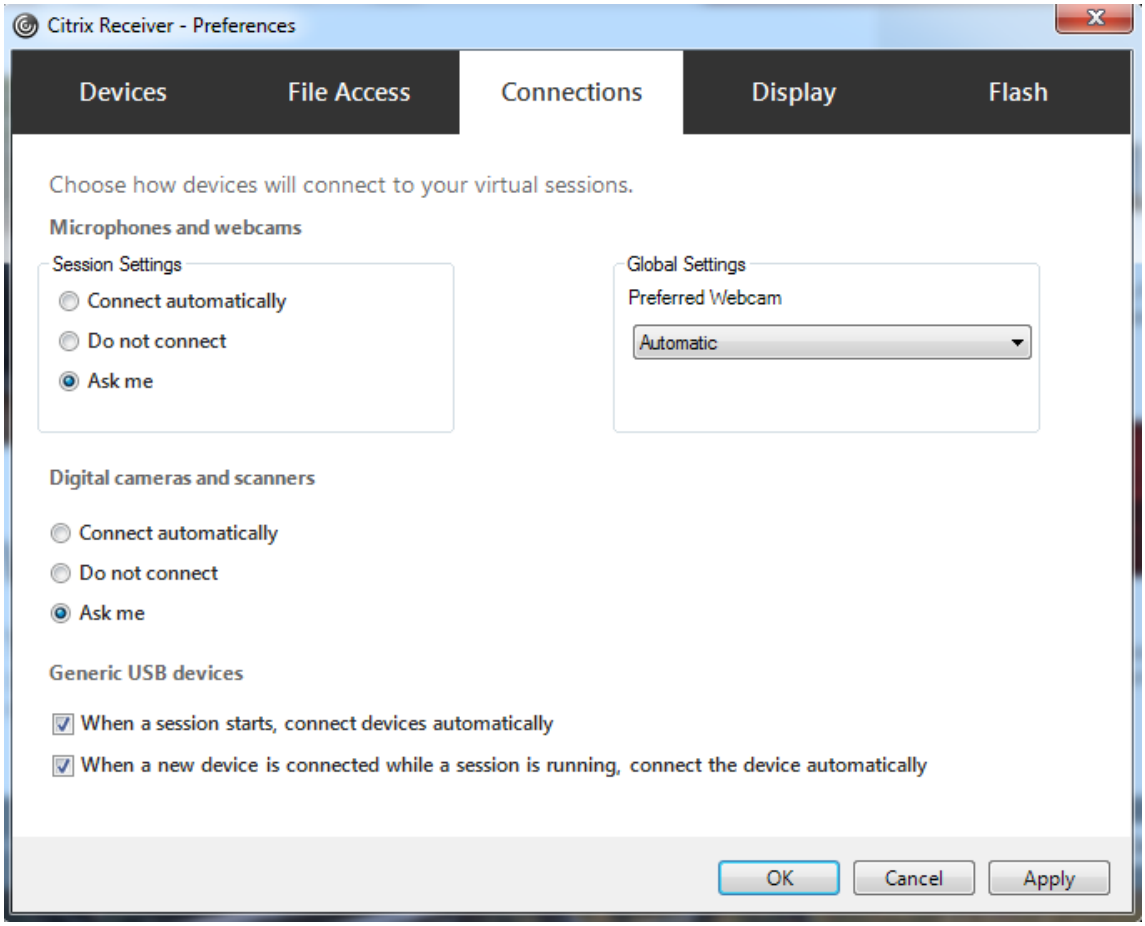


2. （可选）要更新可进行重定向的 USB 设备的列表，请向策略中添加客户端 USB 设备重定向规则设置并指定 USB 策略规则。

   在 Citrix Workspace 应用程序中：

3. 指定自动连接设备而无需手动重定向。您可以使用管理模板或在适用于 **Windows** 的 **Citrix Workspace** 应用程序 **>** 首选项 **>** 连接中完成此操作。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



如果已在上一步中为 VDA 指定了 USB 策略规则，请为 Citrix Workspace 应用程序指定相同的策略规则。

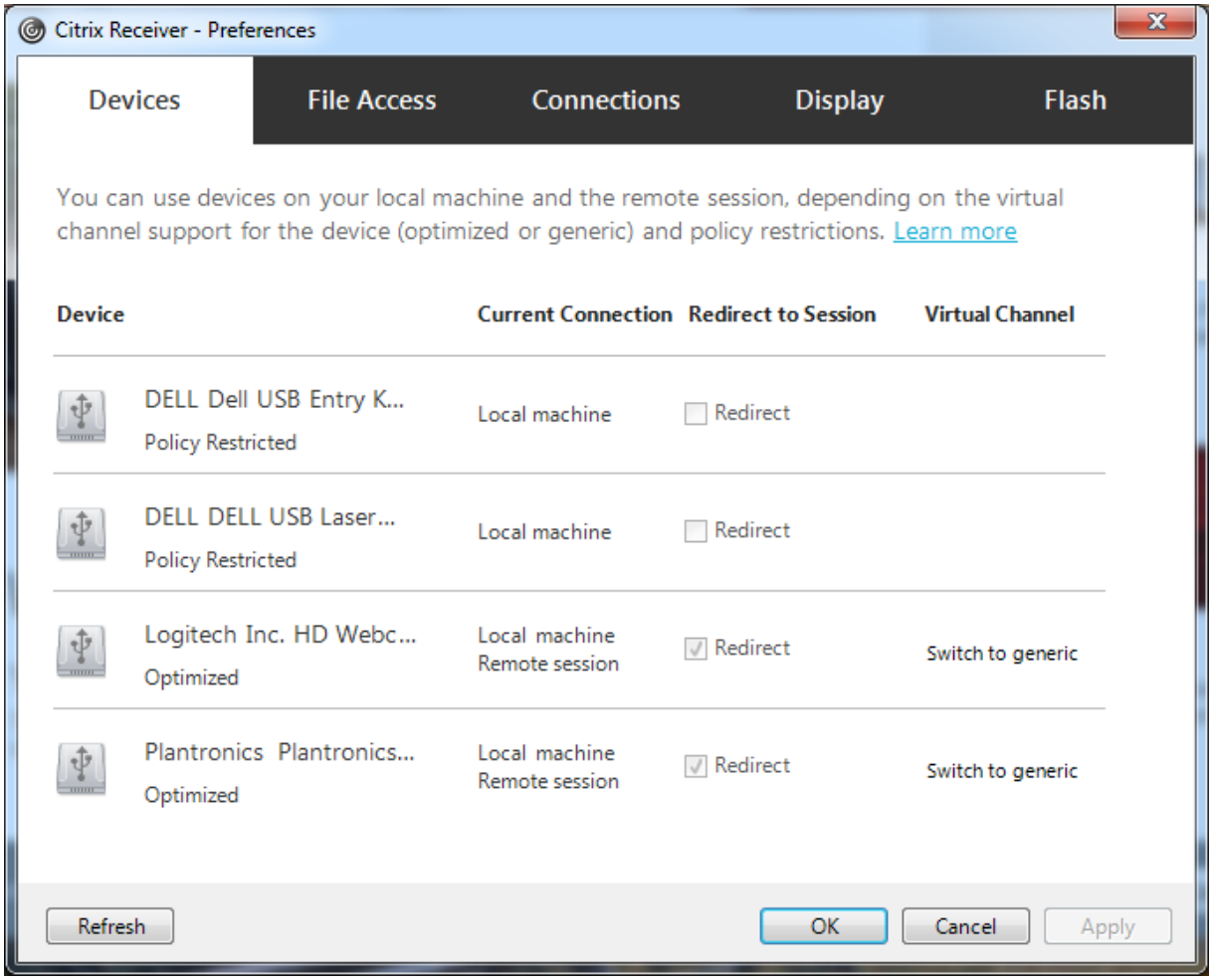
对于瘦客户端，请向制造商咨询有关 USB 支持以及任何所需配置的详细信息。

配置适用于通用 **USB** 重定向的 **USB** 设备的类型

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。不存在连接栏时，也会自动重定向 USB 设备。

用户可以明确地对未自动重定向的设备执行重定向操作，方法是从 USB 设备列表中选择这些设备。有关详细信息，请参阅适用于 Windows 的 Citrix Workspace 应用程序用户帮助文章在 Desktop Viewer 中显示设备。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



要使用通用 USB 重定向而非优化的支持，您可以：

- 在 Citrix Workspace 应用程序中，手动选择 USB 设备以使用通用 USB 重定向，从“首选项”对话框的“设备”选项卡中选择切换到通用。
- 通过配置 USB 设备类型的自动重定向（例如，AutoRedirectStorage=1）并将 USB 用户首选项设置设为自动连接 USB 设备，可以自动选择 USB 设备以使用通用 USB 重定向。有关详细信息，请参阅配置 USB 设备的自动重定向。

> 注意：
>
> 仅在某个网络摄像机被发现与 HDX 多媒体重定向不兼容时，才能配置通用 USB 重定向以与该网络摄像机一同使用。

要阻止列出或重定向 USB 设备，可以为 Citrix Workspace 应用程序和 VDA 指定设备规则。

对于通用 USB 重定向，至少需要了解 USB 设备类别和子类别。并非所有的 USB 设备都会使用其明显的 USB 设备类别和子类别。例如：

- 笔类设备使用鼠标设备类别。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 智能卡读卡器可以使用供应商定义的或 HID 设备类别。

要想实现更为精确的控制，您需要了解供应商 ID、产品 ID 和版本 ID。您可以从设备供应商处获取这些信息。

> 重要：
>
> 恶意的 USB 设备可能会呈现出某些不符合其预期用途的 USB 设备特征。设备规则并非为了防止这种行为。

通过指定 USB 设备重定向规则，可以控制用于通用 USB 重定向的 USB 设备，以覆盖默认 USB 策略规则。

Citrix Virtual Apps and Desktops 服务：

- 在大多数情况下，将下载 Citrix 组策略管理控制台 MSI (`CitrixGroupPolicyManagement_x64.msi`) 并将其安装在您的 Active Directory 系统中，然后管理 AD 组策略。（请勿在 VDA 上安装 MSI。）
- 对于适用于 Windows 的 Citrix Workspace 应用程序，请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)，因此您可以通过 Active Directory 组策略更改用户设备：dvd root `\os\lang\Support\Configuration\icaclient_usb.adm`

本地 Citrix Virtual Apps and Desktops：

- 对于 VDA，请通过组策略规则为多会话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：
  - x64：dvd root `\os\lang\x64\Citrix Policy\CitrixGroupPolicyManagement_x64.msi`
  - x86：dvd root `\os\lang\x86\Citrix Policy\CitrixGroupPolicyManagement_x86.msi`
- 对于适用于 Windows 的 Citrix Workspace 应用程序，请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)，因此您可以通过 Active Directory 组策略更改用户设备：dvd root `\os\lang\Support\Configuration\icaclient_usb.adm`

> 警告：
>
> 注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

产品默认规则存储在 HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\GenericUSB 中。请勿编辑这些产品默认规则，相反，请将其用作创建管理员覆盖规则的指南，本文后面的部分将对此进行解释说明。GPO 覆盖规则将在产品默认规则之前进行评估。

管理员覆盖规则存储在 HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRules 中。GPO 策略规则的格式为 **{Allow: | Deny:}**，后接一组以空格分隔的 *tag=value* 表达式。

支持以下标记：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

标记	说明
VID	设备描述符中的供应商 ID
PID	设备描述符中的产品 ID
REL	设备描述符中的版本 ID
类	设备描述符或接口描述符中的类；请参阅 USB Web 站点 http://www.usb.org/ 了解可用的 USB 类代码
子类	设备描述符或接口描述符中的子类
端口	设备描述符或接口描述符中的协议

创建策略规则时，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。

> 注意：
>
> 如果使用 ADM 模板文件，则必须在一行中创建规则（以分号分隔的列表）。

示例：

- 以下示例显示了一个用于供应商和产品标识符的 USB 策略规则，由管理员定义：

```
Allow: VID=046D PID=C626 # 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。

使用适用于 Windows 的 Citrix Workspace 应用程序时，以下情况适用：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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。

适合 **USB** 大容量存储设备的安全控制

为 USB 大容量存储设备提供了优化支持。此支持是 Citrix Virtual Apps and Desktops 客户端驱动器映射的一部分。用户登录时，用户设备上的驱动器将自动映射至虚拟桌面上的驱动器盘符。这些驱动器显示为具有映射的驱动器盘符的共享文件夹。要配置客户端驱动器映射，请使用客户端可移动驱动器设置。此设置位于 ICA 策略设置的文件重定向策略设置部分。

借助 USB 大容量存储设备，可以使用客户端驱动器映射或通用 USB 重定向，或者两者。使用 Citrix 策略对其进行控制。主要的区别为：

功能	客户端驱动器映射	通用 USB 重定向
默认已启用	是	否
可配置只读访问权限	是	否
加密的设备访问	是，如果在访问设备前解锁加密	是
BitLocker To Go 设备	否	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 重定向和客户端驱动器映射策略，并且在会话启动之前或之后插入了大容量存储设备，则将使用客户端驱动器映射对其进行重定向。如果同时启用了通用 USB 重定向和客户端驱动器映射策略，设备配置为自动重定向，并且在会话启动之前或之后插入了大容量存储设备，则将使用通用 USB 重定向对其进行重定向。有关详细信息，请参阅知识中心文章 CTX123015。

> 注意：
>
> 低带宽连接（例如 50 Kbps）条件下支持 USB 重定向。但是，复制大型文件不起作用。

通过客户端驱动器映射控制文件访问

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。

要防止用户添加或更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。将此设置添加到某个策略中时，请确保“客户端驱动器重定向”设置设为允许，并且也已添加到该策略中。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

打印

January 21, 2022

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. 选择打印机预配方法，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。

打印概念

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：

- 可用的打印机预配类型
- 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。

打印过程

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预配。
- 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预配、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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

打印机预配

在会话中启用打印机的过程称为预配。打印机预配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。

最常用的打印机预配方法有：

- 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，您可以使用多会话操作系统计算机上的单个驱动程序以允许从任何设备进行网络打印。

Citrix 建议针对远程打印服务器的情况使用 Citrix 通用打印服务器。通用打印服务器通过网络以经过优化和压缩的格式传输打印作业，从而最大程度地减少网络使用，并改善用户体验。

通用打印服务器功能包含以下组件：

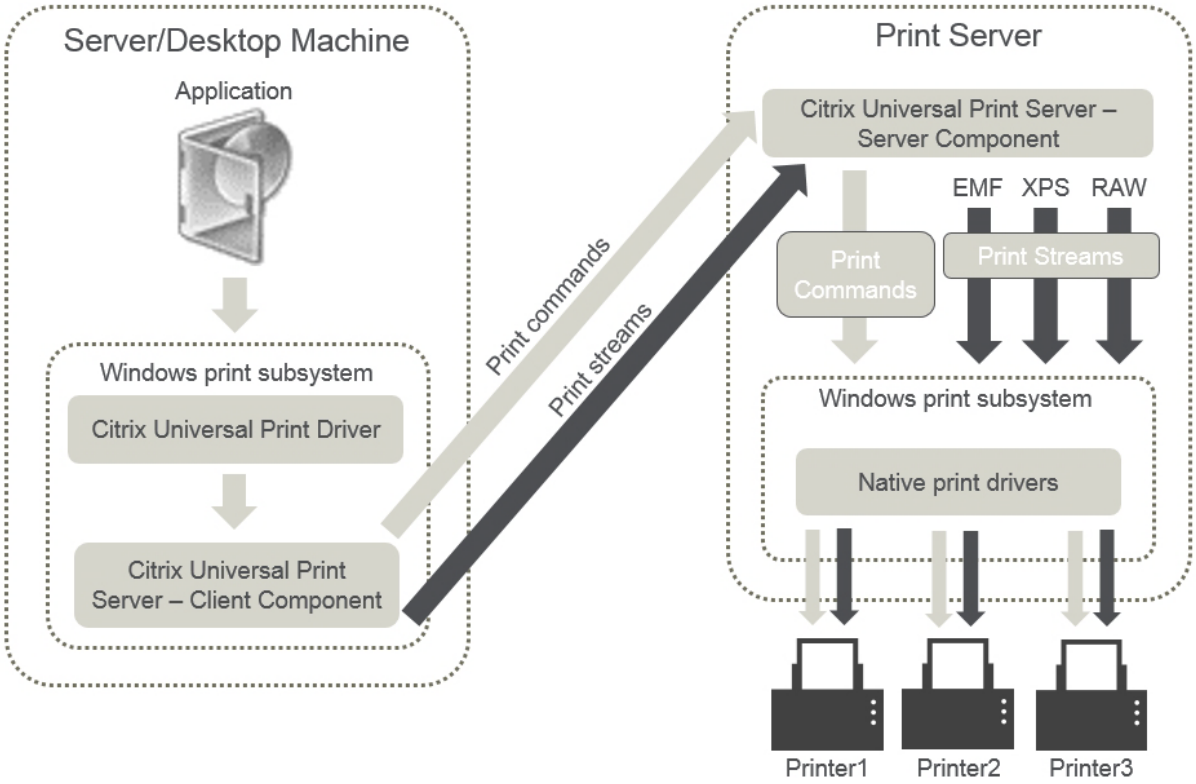
客户端组件 **UPClient** - 在预配会话网络打印机并且使用通用打印驱动程序的每台多会话操作系统计算机上启用通用打印客户端。

服务器组件 **UPServer** - 在预配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（无论会话打印机是否集中预配）。

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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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。

- 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，多会话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多会话操作系统计算机添加驱动程序。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

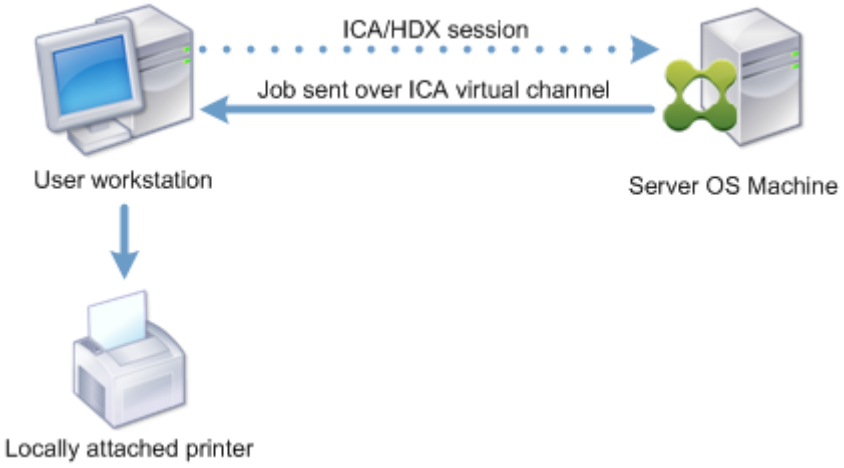
打印作业路由

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。后台处理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

系统将作业从多会话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

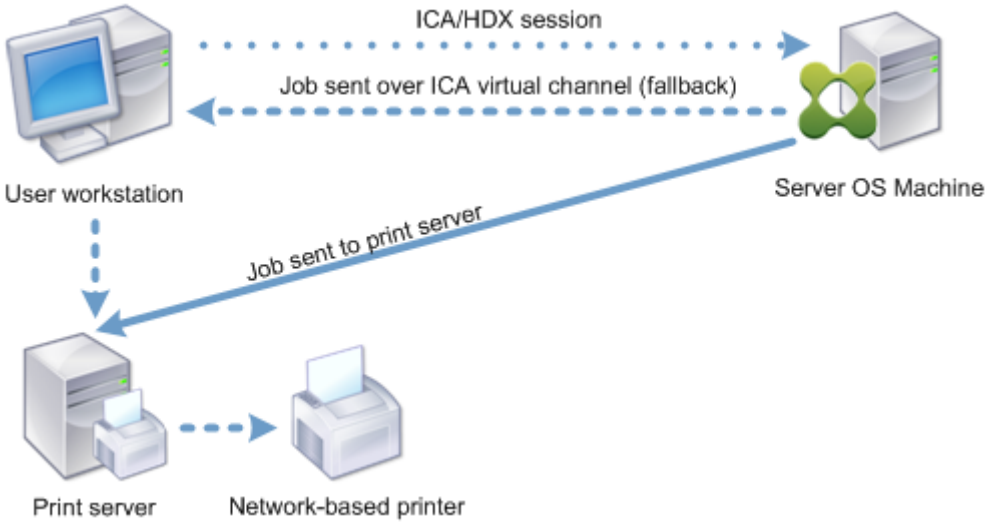
默认情况下，发往网络打印机的所有打印作业都会从多会话操作系统计算机通过网络直接路由到打印服务器。但是在以下情形中，打印作业会自动通过 ICA 连接进行路由：

- 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多会话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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



打印驱动程序管理

Citrix 通用打印机驱动程序 (UPD) 是独立于设备的打印驱动程序，与大多数打印机兼容。Citrix UPD 由两个组件构成：

服务器组件。Citrix UPD 作为 Citrix Virtual Apps and Desktops VDA 安装的一部分安装。VDA 将以下驱动程序与 Citrix UPD 一起安装：“Citrix 通用打印机”（EMF 驱动程序）和“Citrix XPS 通用打印机”（XPS 驱动程序）。

Name	Processor	Type
Citrix Universal Printer	x64	Type 3 - User Mode
Citrix XPS Universal Printer	x64	Type 3 - User Mode

VDA 安装程序不再提供用于控制通用打印服务器 PDF 打印机驱动程序安装的选项。该 PDF 打印机驱动程序现在始终自动安装。升级到 7.17 VDA（或受支持的更高版本）时，以前安装的任何 Citrix PDF 打印机驱动程序都将自动删除并替换为最新版本。

启动打印作业时，驱动程序记录应用程序的输出，且不做任何修改地发送到端点设备。

客户端组件。Citrix UPD 作为 Citrix Workspace 应用程序安装的一部分安装。Citrix UPD 提取 Citrix Virtual Apps and Desktops 会话的传入打印数据流。然后将打印流转发到使用设备特定的打印机驱动程序呈现打印作业的本地打印子系统。

Citrix UPD 支持以下打印格式：

- 增强的图元文件格式 (**EMF**)，默认值。EMF 是 32 位版本的 Windows 图元文件 (WMF) 格式。EMF 驱动程序只能由基于 Windows 的客户端使用。
- XML 纸张规范 (**XPS**)。XPS 驱动程序使用 XML 创建独立于平台的“电子文件”，其格式与 Adobe PDF 格式类似。
- 打印机命令语言（**PCL5c** 和 **PCL4**）。PCL 是 Hewlett-Packard 最初为喷墨式打印机开发的打印协议。它用于打印基本文本和图形，在 HP LaserJet 和多功能外围设备上广受支持。

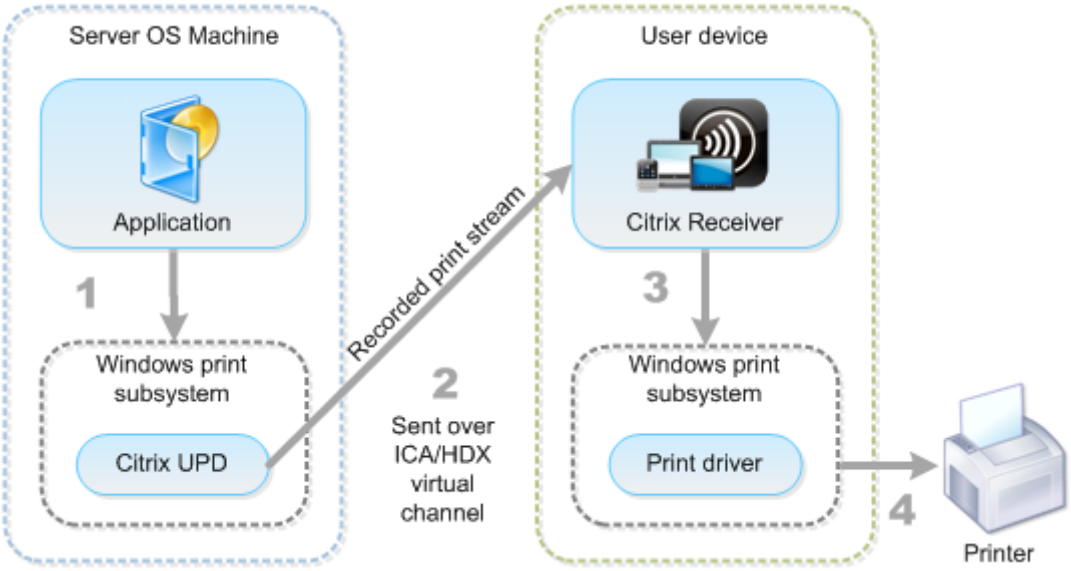
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- PostScript (**PS**)。PostScript 是可以用于打印文本和矢量图形的计算机语言。该驱动程序在低价打印机和多功能外围设备上广泛使用。

PCL 和 PS 驱动程序最适用于使用基于非 Windows 的设备（例如 Mac 或 UNIX 客户端）的场合。可以使用通用驱动程序优先级策略设置来更改 Citrix UPD 尝试使用驱动程序的顺序。

Citrix UDP（EMF 和 XPS 驱动程序）支持高级打印功能，例如，装订和纸张来源选择。这些功能在本机驱动程序使用 Microsoft 打印功能技术允许其可用时才可用。本机驱动程序应在打印功能 XML 中使用标准化的打印架构关键字。如果使用非标准关键字，则高级打印功能将不能通过 Citrix 通用打印驱动程序使用。

下图显示了通用打印驱动程序组件和本地连接到设备的打印机的典型工作流。

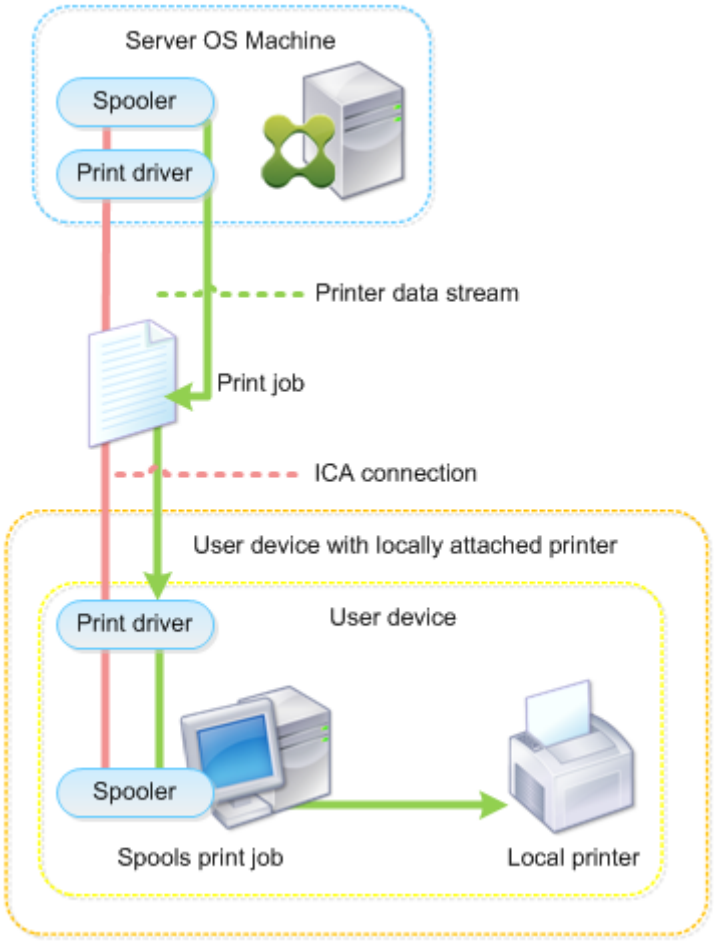


规划驱动程序管理策略时，请确定支持的驱动程序类型：通用打印驱动程序、设备特定的驱动程序或者两者。如果支持标准驱动程序，您必须确定：

在自动创建打印机期间，如果系统检测到有新的本地打印机连接至用户设备，即会在多会话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，多会话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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- 要支持的驱动程序类型。
- 当多会话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。

相关内容

- 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
- 预配打印机
- 维护打印环境

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

打印配置示例

November 17, 2021

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。

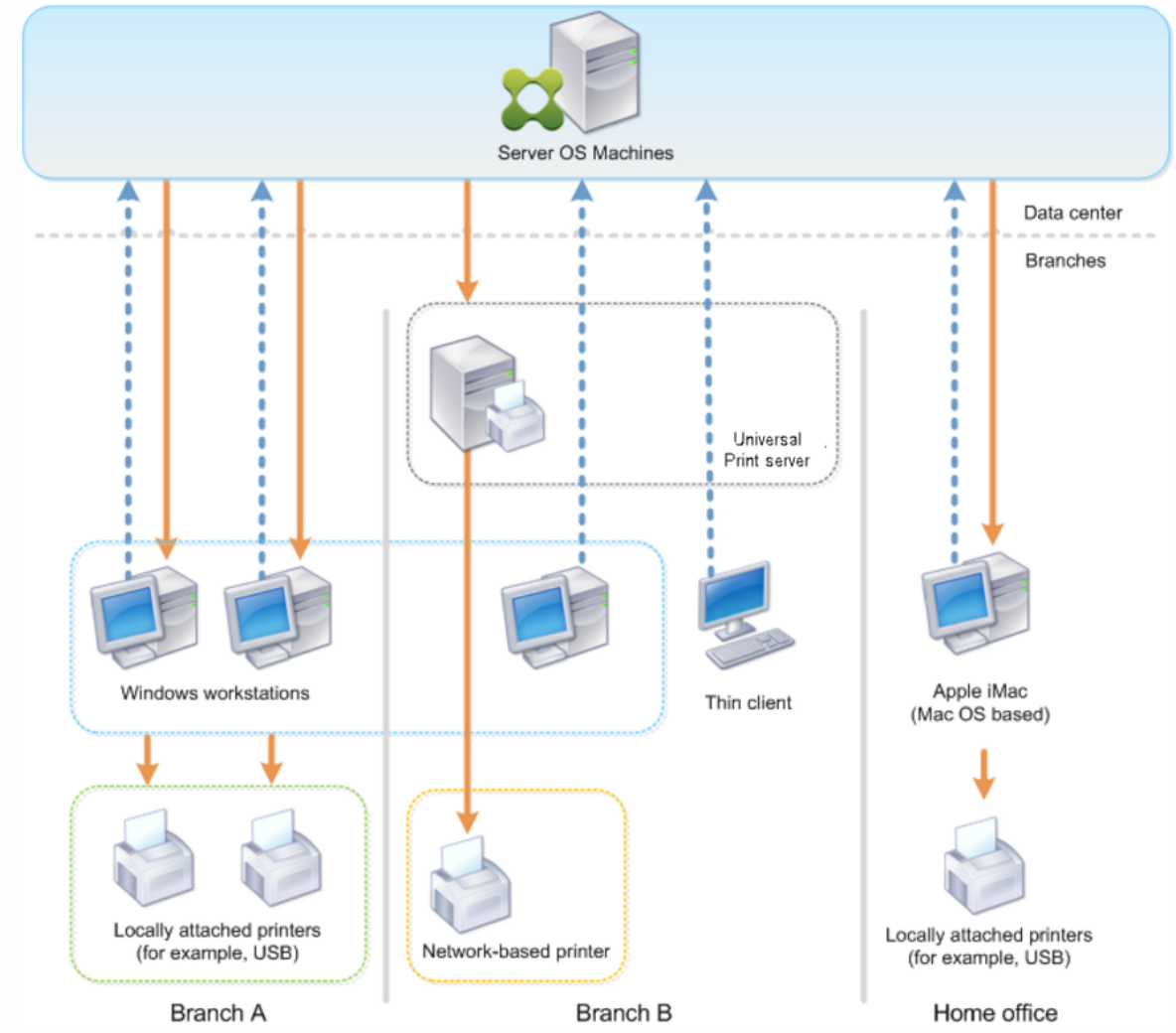
在设计打印配置时，应尽量为会话中的用户提供与从本地用户设备打印时相同的体验。

打印部署示例

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，具有几个 Windows 工作站。每个用户工作站都有一个本地连接的专用打印机。
- 分支机构 **B** - 大型分支机构，具有瘦客户端和基于 Windows 的工作站。为了提高效率，此分支机构的用户共享基于网络的打印机（每个楼层一台）。位于分支机构内部的基于 Windows 的打印服务器管理着打印队列。
- 公司总部 - 公司总部，具有基于 Mac 操作系统的用户设备，可访问公司的 Citrix 基础结构。用户设备具有本地连接的打印机。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



以下部分介绍了可最大程度地降低环境复杂性并简化其管理的配置。

自动创建的客户端打印机和 **Citrix** 通用打印机驱动程序

在分支机构 A 中，所有用户在基于 Windows 的工作站上工作，因此将使用自动创建的客户端打印机和通用打印机驱动程序。这些技术具有以下优势：

- 性能 - 打印作业通过 ICA 打印通道交付，这样可以压缩打印数据，从而节省带宽。

  为了确保打印大型文档的单个用户不会降低其他用户的会话性能，配置了一个 Citrix 策略以指定最大打印带宽。

  备选解决方案为利用多流 ICA 连接，在此连接中，打印流量在单独的低优先级 TCP 连接中进行传输。多流 ICA 适用于不在 WAN 连接上实施服务质量 (QoS) 时使用。

- 灵活性 - 使用 Citrix 通用打印机驱动程序，可确保还可以从虚拟桌面或应用程序会话使用连接到客户端的所有打印机，而无需在数据中心中集成新打印机驱动程序。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix 通用打印服务器

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。

自动创建的客户端打印机和 **Citrix** 通用打印机驱动程序

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。

部署摘要

概括而言，部署示例如下所示进行配置：

- 未在多会话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，单会话操作系统计算机将直接连接到打印服务器。所需的唯一配置是启用通用打印服务器组件。
- 对分支机构 B 的每个楼层配置会话打印机策略，并应用于相应楼层的所有瘦客户端。
- 对分支机构 B 实施 QoS，以确保卓越的用户体验。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

最佳做法、安全注意事项和默认操作

November 17, 2021

最佳做法

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。
- 最大程度减少多会话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端点服务测试，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，以便该驱动程序已经过 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。

安全注意事项

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。

默认打印操作

默认情况下，如果未配置任何策略规则，打印行为如下所述：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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多会话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多会话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。
- 在 VDA 7.16 及更高版本中，Citrix 策略设置“自动安装现有的打印机驱动程序”不会对 Windows 8 及更高版本的 Windows 操作系统版本产生任何影响，因为 V3 现有的打印机驱动程序不包括在操作系统中。
- 在 7.16 之前的 VDA 中，系统使用 Windows 版本的打印机驱动程序（如果该驱动程序在多会话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

Always-On 日志记录功能对 VDA 上的打印服务器和打印子系统可用。

要将日志整理为 ZIP 文件，以便通过电子邮件发送，或者要将日志自动上载到 Citrix Insight Services，请使用 **Start-TelemetryUpload** PowerShell cmdlet。

打印策略和首选项

January 21, 2022

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：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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，Citrix Workspace 应用程序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）或在多会话操作系统计算机上的用户配置文件中存储或保留打印机属性。如果用户在会话期间更改打印机属性，这些更改会在计算机上的用户配置文件中进行更新。下次用户登录或重新连接时，用户设备会继承这些保留的设置。即，用户必须注销并重新登录，用户设备上的打印机属性更改才会影响当前会话。

打印首选项保存位置

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（即在多会话操作系统计算机上），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。
- 在多会话操作系统计算机上 - 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。

用户打印首选项的层级

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，系统会将存储在多会话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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

保存用户打印首选项

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，则会自动回退到多会话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。

预配打印机

January 21, 2022

Citrix 通用打印服务器

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 定义的与设备无关的公共设置。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，该驱动程序是多会话操作系统计算机上的单个驱动程序，允许从任何设备（包括瘦客户端和平板电脑）进行本地打印或网络打印。

要将通用打印服务器与 Windows 本机驱动程序结合使用，请启用通用打印服务器。默认情况下，如果 Windows 本机驱动程序可用，请使用 Windows 本机驱动程序。否则，将使用通用打印驱动程序。要指定对该行为的更改，例如仅使用 Windows 本机驱动程序或仅使用通用打印驱动程序，请更新通用打印驱动程序使用策略设置。

安装通用打印服务器

要使用通用打印服务器，请按安装文档中所述在打印服务器上安装 UpsServer 组件并进行配置。有关详细信息，请参阅安装核心组件和使用命令行安装。

对于希望单独部署通用打印客户端组件的环境（例如采用 **XenApp 6.5**），请执行以下操作：

1. 下载适用于 Windows 单会话操作系统或 Windows 多会话操作系统的 Citrix Virtual Apps and Desktops Virtual Delivery Agent (VDA) 独立软件包。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. 根据使用命令行安装中介绍的命令行说明提取 VDA。
3. 从 \Image-Full\Support\VcRedist_2013_RTM 安装必备决条件：
    - Vcredist_x64 / vcredist_x86
        - 对于 32 位部署，仅运行 x86，对于 64 位部署，两个均运行。
4. 从 \Image-Full\x64\Virtual Desktop Components 或 \Image-Full\x86\Virtual Desktop Components 安装 cdf 必备项。
    - 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 中查找通用打印客户端组件。
6. 解压并启动组件的 MSI 以安装通用打印客户端组件。
7. 安装通用打印客户端组件后需要重新启动。

退出针对通用打印服务器的 **CEIP**

在安装通用打印服务器时，您会自动注册 Citrix 客户体验改善计划 (CEIP)。在安装日期和时间后的七日时将首次上载数据。

要退出 CEIP，请编辑注册表项 **HKLM\Software\Citrix\Universal Print Server\CEIPEnabled**，并将 **DWORD** 值设置为 **0**。

要重新加入，请将 DWORD 值设置为 1。

小心：注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

有关详细信息，请参阅 Citrix Insight Services。

配置通用打印服务器

使用以下 Citrix 策略设置配置通用打印服务器。有关详细信息，请参阅屏幕上的策略设置帮助。

- 启用通用打印服务器。默认情况下禁用通用打印服务器。启用通用打印服务器时，需要选择是否在通用打印服务器不可用时使用 Windows 打印提供程序。启用通用打印服务器之后，用户可以通过 Windows 打印提供程序和 Citrix 提供程序界面添加和枚举网络打印机。
- 通用打印服务器打印数据流 **(CGP)** 端口。指定由通用打印服务器打印数据流 CGP（通用网关协议）侦听器使用的 TCP 端口号。默认为 **7229**。
- 通用打印服务器 **Web** 服务 **(HTTP/SOAP)** 端口。指定由通用打印服务器侦听器使用的 TCP 端口号，用以侦听传入的 HTTP/SOAP 请求。默认值为 **8080**。

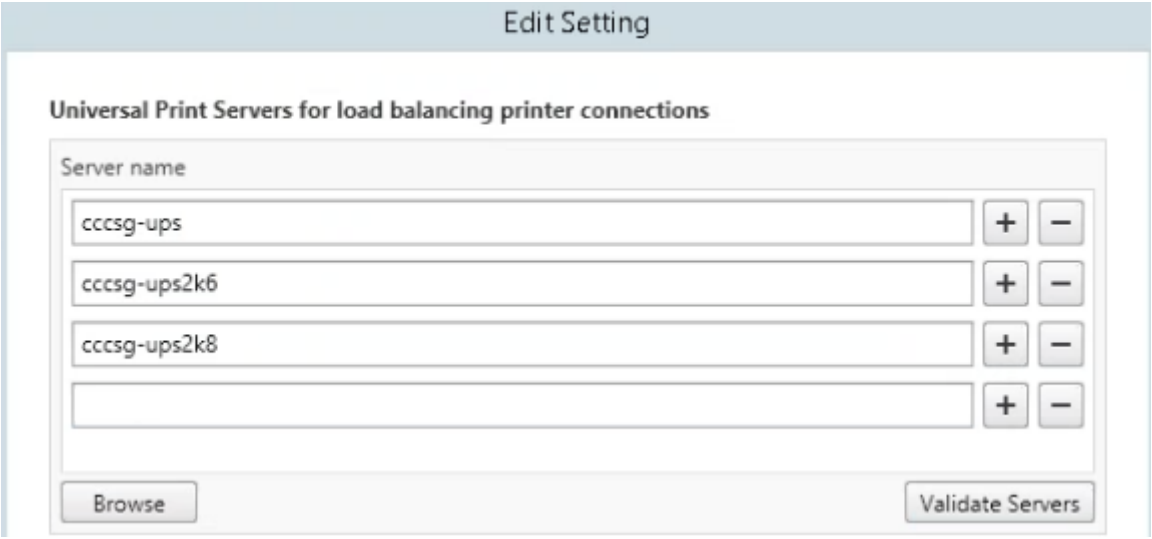
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

要更改通用打印服务器与 Citrix Virtual Apps and Desktops 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:<portnumber>

此端口号必须与 Studio 中的 HDX 策略“通用打印服务器 Web 服务 (HTTP/SOAP) 端口”匹配。

- 通用打印服务器打印流输入带宽限制 **(kbps)**。指定使用 CGP 从每个打印作业向通用打印服务器交付打印数据时的传输速率上限 (kbps)。默认为 0（无限制）。
- 用于负载平衡的通用打印服务器。此设置列出了在评估其他 Citrix 打印策略设置后，用于对会话启动时建立的打印机连接执行负载平衡的通用打印服务器。为了优化打印机创建时间，Citrix 建议所有打印服务器具有相同的共享打印机集合。



- 通用打印服务器停止运行阈值。指定负载平衡器应等待不可用的打印服务器恢复的时长，在此之后负载平衡器将该服务器确定为永久脱机，并将其负载重新分配到其他可用的打印服务器。默认值是 180（秒）。

在 Delivery Controller 上修改打印策略后，可能需要几分钟时间来向 VDA 应用策略更改。

与其他策略设置的交互 - 通用打印服务器支持其他 Citrix 打印策略设置并如下表所述与之交互。下表中提供的信息基于以下假设：已启用通用打印服务器策略设置，已安装通用打印服务器组件，并已应用策略设置。

策略设置	交互
客户端打印机重定向，自动创建客户端打印机	启用通用打印服务器之后，将使用通用打印驱动程序（而非本机驱动程序）创建客户端网络打印机。用户看到的打印机名称与先前相同。
会话打印机	使用 Citrix 通用打印服务器解决方案时，将保留通用打印驱动程序策略设置。

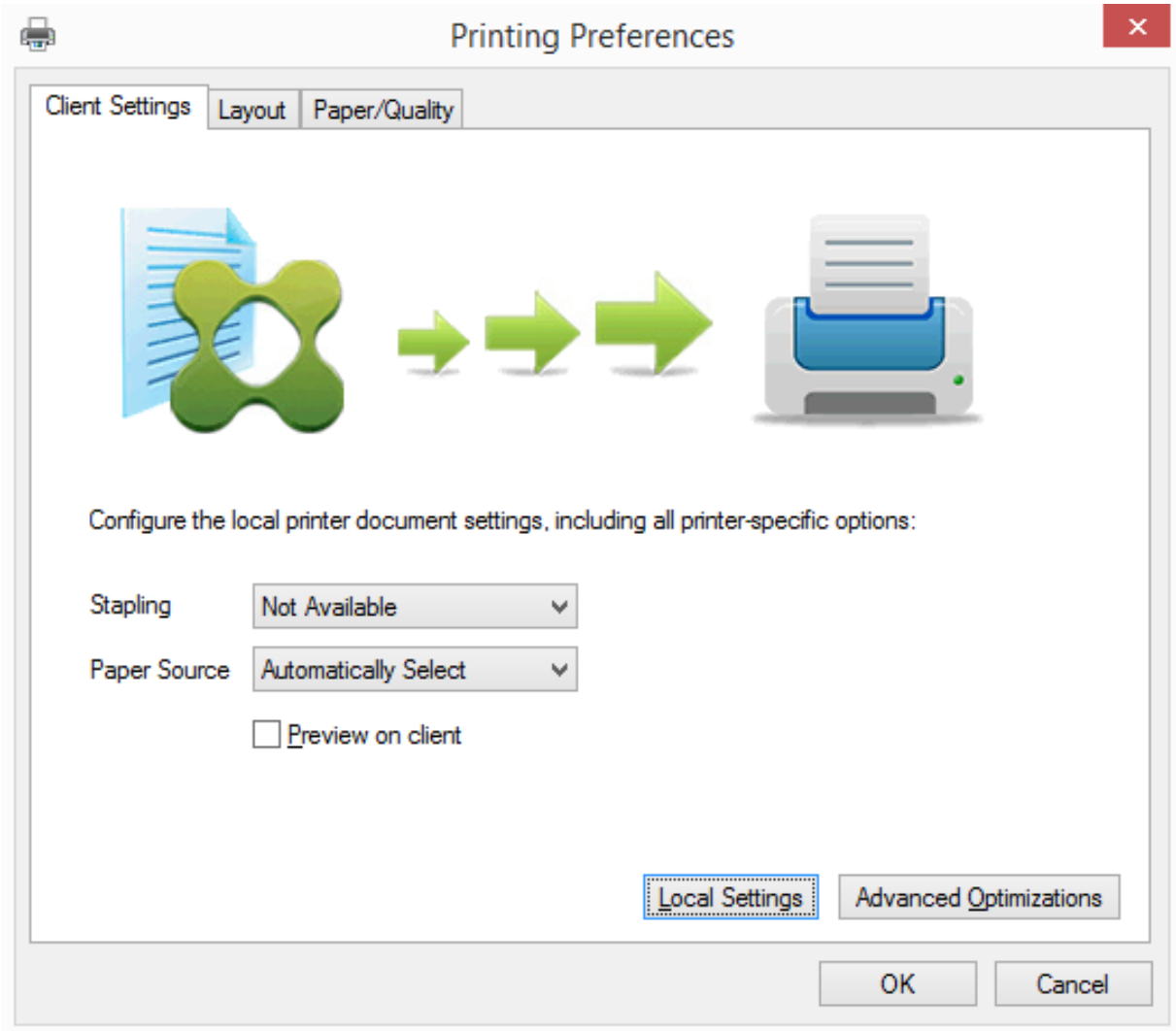
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

与打印服务器的直接连接	启用通用打印服务器并将通用打印驱动程序使用策略设置配置为仅使用通用打印时，可使用通用打印驱动程序在打印服务器上创建直接网络打印机连接。
UPD 首选项	支持 EMF 和 XPS 驱动程序。

对用户界面的影响 - 通用打印服务器使用的 Citrix 通用打印驱动程序会禁用以下用户界面控件：

- “打印机属性”对话框中的“本地打印机设置”按钮
- “文档属性”对话框中的“本地打印机设置”和“在客户端上预览”按钮

Citrix 通用打印驱动程序（EMF 和 XPS 驱动程序）支持高级打印功能，例如，装订和纸张来源。用户可以从自定义 UPD 打印对话框中选择“装订”或“纸张来源”选项（如果映射到会话中的 UPD 的客户端或网络打印机支持这些功能）。



要设置非标准打印机设置（例如，装订和安全 PIN），请在客户的 UPD 打印对话框中，为使用 Citrix UPD EMF 或 XPS

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

驱动程序的任何客户端映射的打印机选择本地设置。映射的打印机的打印首选项对话框显示在客户端上会话之外（允许用户更改任何打印机选项），并且打印文档时，修改后的打印机设置用于活动会话中。

这些功能在本机驱动程序使用 Microsoft 打印功能技术允许其可用时才可用。本机驱动程序应在打印功能 XML 中使用标准化的打印架构关键字。如果使用非标准关键字，则高级打印功能将不能通过 Citrix 通用打印驱动程序使用。

使用通用打印服务器时，Citrix 打印提供程序的“添加打印机”向导与 Windows 打印提供程序的“添加打印机”向导相同，但有以下几点不同：

- 按名称或地址添加打印机时，可以提供打印服务器的 HTTP/SOAP 端口号。该端口号将成为打印机名称的一部分并出现在名称显示中。
- 如果 Citrix 通用打印驱动程序使用策略设置指定必须使用通用打印，则选择打印机时将显示通用打印驱动程序名称。Windows 打印提供程序无法使用通用打印驱动程序。

Citrix Print Provider 不支持客户端呈现。

有关通用打印服务器的详细信息，请参阅 CTX200328。

自动创建的客户端打印机

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 Citrix 通用打印机，这样可以大大降低资源使用情况并降低用户登录次数。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 Workspace 应用程序。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 Workspace 应用程序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 - 与设备无关的打印机驱动程序。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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 通用打印预览首选项。指定是否使用自动创建的打印机或一般通用打印机的打印预览功能。
- 通用打印 EMF 处理模式。控制在 Windows 用户设备上处理 EMF 后台打印文件的方法。默认情况下，系统将 EMF 记录直接后台打印到打印机中。借助直接后台打印到打印机中的方式，后台处理程序可以更快地处理记录，且使用的 CPU 资源更少。

有关更多策略，请参阅优化打印性能。要更改默认设置（例如纸张大小、打印质量、色彩、双面打印和份数），请参阅 CTX113148。

在用户设备中自动创建打印机 - 默认情况下，在会话开始时，系统会在用户设备上自动创建所有打印机。您可以控制为用户置备的打印机类型（如果有），并阻止自动创建。

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）。

将网络打印机分配给用户

默认情况下，会话开始时会在用户设备上自动创建网络打印机。系统使您能够通过指定要在每个会话中创建的网络打印机，减少枚举或映射的网络打印机数量。这类打印机称为会话打印机。

您可以按 IP 地址过滤会话打印机策略以提供邻近打印。通过邻近打印，指定 IP 地址范围内的用户可以自动访问该范围内存在的网络打印设备。邻近打印由 Citrix 通用打印服务器提供，并且不需要进行本节所述的配置。

邻近打印可能涉及以下情况：

- 内部公司网络与为用户自动指定 IP 地址的 DHCP 服务器一起运行。
- 公司内的所有部门均具有唯一的指定 IP 地址范围。
- 网络打印机存在于每个部门的 IP 地址范围内。

如果配置了邻近打印，则员工从一个部门转移到另一个部门时，无需进行其他打印设备配置。只要用户设备在新部门的 IP 地址范围内得以识别，即对该范围内的所有网络打印机具有访问权限。

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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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端点服务或 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，这不需要此处所述的配置。

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

January 21, 2022

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

管理打印机驱动程序

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多会话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：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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，以确保多会话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。

优化打印性能

要优化打印性能，请使用通用打印服务器和通用打印驱动程序。以下策略可控制打印优化和压缩：

- 通用打印优化默认值。指定在为会话创建通用打印机时所使用的通用打印机默认设置：
  - 所需图像质量指定应用到通用打印的默认图像压缩限制。默认情况下，启用标准质量，这意味着用户只能使用标准或降低质量的压缩级别来打印图像。
  - 启用超级压缩用于启用或禁用在超出由“所需图像质量”所设置的压缩级别上减少带宽，而不降低图像质量。默认情况下，禁用超级压缩功能。
  - 图像与字体缓存设置指定是否缓存在打印流中多次出现的图像和字体，以确保每个唯一的图像或字体只发送给打印机一次。默认情况下，将缓存嵌入式图像和字体。
  - 允许非管理员修改这些设置指定用户是否可以更改会话内的默认打印优化设置。默认情况下，不允许用户更改默认打印优化设置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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多会话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 - 当文件从多会话操作系统计算机打印到用户打印机时，其他虚拟通道（例如视频）可能会因为争用带宽而导致性能下降，特别是当用户通过速度较慢的网络访问服务器时。为避免出现此类性能下降，可以限制用户打印所用的带宽。通过限制打印的数据传输速率，可将 HDX 数据流中的更多带宽用于视频、按键以及鼠标数据的传输。

> 重要：
>
> 打印机带宽限制始终会强制执行，即使其他通道处于不使用状态时也是如此。

可使用以下 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，请在每台多会话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。

负载平衡通用打印服务器

可以通过向负载平衡解决方案添加更多打印服务器来扩展通用打印服务器解决方案。不存在单一故障点，因为每个 VDA 都具有自己的负载平衡器，用于将印刷负载分配到所有打印服务器。

可使用策略设置用于负载平衡的通用打印服务器和通用打印服务器停止运行阈值在负载平衡解决方案中的所有打印服务器上分配打印负载。

如果某打印服务器发生意外故障，则每个 VDA 中的负载平衡器的故障转移机制会将该故障打印服务器上已分配的打印机连接自动重新分配给其他可用打印服务器，使得所有现有会话和传入会话正常工作，而不会影响用户体验，并且不需要管理员立即进行干预。

管理员可以使用一组性能计数器来监视已进行负载平衡的打印服务器的活动，以便在 VDA 中跟踪以下项：

- VDA 上的负载平衡打印服务器及其状态（可用、不可用）的列表
- 每个打印服务器所接受的打印机连接数

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 每个打印服务器上的失败打印机连接数
- 每个打印服务器上的活动打印机连接数
- 每个打印服务器上的挂起打印机连接数

显示和管理打印队列

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
客户端打印机（连接到用户设备的打印机）	客户端打印途径	已启用 UAC 打开：位于 Microsoft 管理控制台中的打印管理单元；已启用 UAC 关闭：Windows 8 之前的版本：控制面板，Windows 8：打印管理单元
网络打印机（网络打印服务器上的打印机）	网络打印途径	已启用 UAC 打开：打印服务器 > 位于 Microsoft 管理控制台中的打印管理单元；已启用 UAC 关闭：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	已启用 UAC 打开：打印服务器 > 位于 Microsoft 管理控制台中的打印管理单元；已启用 UAC 关闭：Windows 8 之前的版本：控制面板，Windows 8：打印管理单元
本地网络服务器打印机（来自网络打印服务器且已添加到多会话操作系统计算机）	网络打印途径	已启用 UAC 打开：打印服务器 > 控制面板；已启用 UAC 关闭：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。

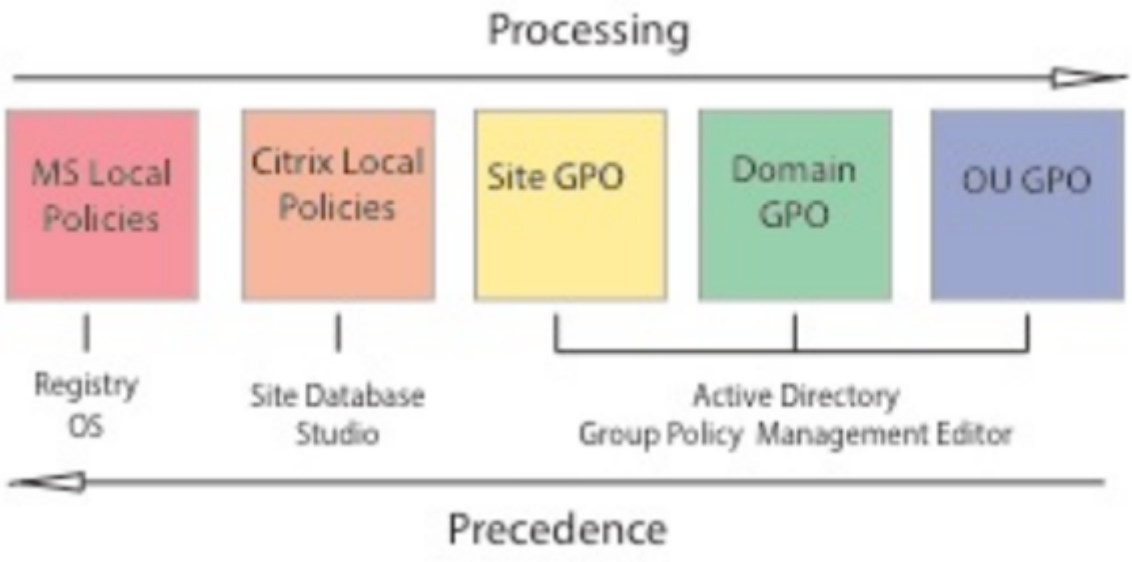
策略

November 17, 2021

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。如果您未明确分配策略，设置将应用于所有连接。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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 本地策略都在 Citrix Studio 控制台中创建和管理，并存储在站点数据库中。组策略使用 Microsoft 组策略管理控制台 (GPMC) 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，二者可能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 Citrix Workspace 应用程序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。之后将其应用于端点设备的注册表和托管资源的计算机。
7. 最终用户从资源注销。最终用户和端点设备的 Citrix 策略不再起作用。
8. 最终用户注销用户设备，从而释放 GPO 用户策略。
9. 最终用户关闭设备，从而释放 GPO 计算机策略。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

为一组用户、设备和计算机创建策略时，有些成员可能会有其他要求，并且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：
> 我们不支持在同一个 GPO 中混合使用 Windows 策略和 Citrix 策略。

使用策略

May 6, 2022

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 Broker 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：
>
> 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：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. 组织单位
2. 域级 GPO
3. 站点级 GPO
4. XenApp 或 XenDesktop 站点 GPO（存储在站点数据库中）
5. 本地 GPO

例如，Citrix 管理员使用 Studio 创建了一个策略（策略 A），用于为公司的销售员工启用客户端文件重定向。同时，另一名管理员使用组策略编辑器也创建了一个策略（策略 B），用于为销售员工禁用客户端文件重定向。当销售员工登录到虚拟桌面时，将应用策略 B 而忽略策略 A，因为策略 B 在域级别处理，而策略 A 在 XenApp 或 XenDesktop 站点 GPO 级别处理。

但是，当用户启动 ICA 或远程桌面协议 (RDP) 会话时，Citrix 会话设置将覆盖在 Active Directory 策略中或使用远程桌面会话主机配置进行配置的相同设置。这包括与典型的 RDP 客户端连接设置相关的设置（例如桌面墙纸、菜单动画以及拖动时查看窗口内容）。

使用多个策略时，可以向包含冲突设置的策略分配优先级，请参阅对策略进行比较、设定优先级、建模和故障排除了解详细信息。

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。

> 注意：
>
> 要打开 Citrix 组策略建模向导，请导航到策略 **>** 建模选项卡，然后在操作窗格中单击启动建模向导。在 Citrix Cloud 中托管的 Studio 中，建模选项卡不可用。

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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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（策略分配到的用户和计算机对象）。有关详细信息，请参阅创建策略。
  - 模板选项卡列出 Citrix 提供的模板和您创建的自定义模板。选择模板时，右侧的选项卡显示：说明（要使用此模板的原因）和设置（已配置设置的列表）。有关详细信息，请参阅策略模板。
  - 利用比较选项卡，您可以将某个策略或模板中的设置与其他策略或模板中的设置进行比较。例如，您可能希望验证设置值以确保符合最佳做法。有关详细信息，请参阅对策略进行比较、设定优先级、建模和故障排除。
  - 从建模选项卡，可以利用 Citrix 策略模拟连接场景。有关详细信息，请参阅对策略进行比较、设定优先级、建模和故障排除。

    > 注意：
    >
    > 在 Citrix Cloud 中托管的 Studio 中，建模选项卡不可用。

  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，便与所使用的模板无关。您可以使用新策略的说明字段来跟踪所使用的源模板。

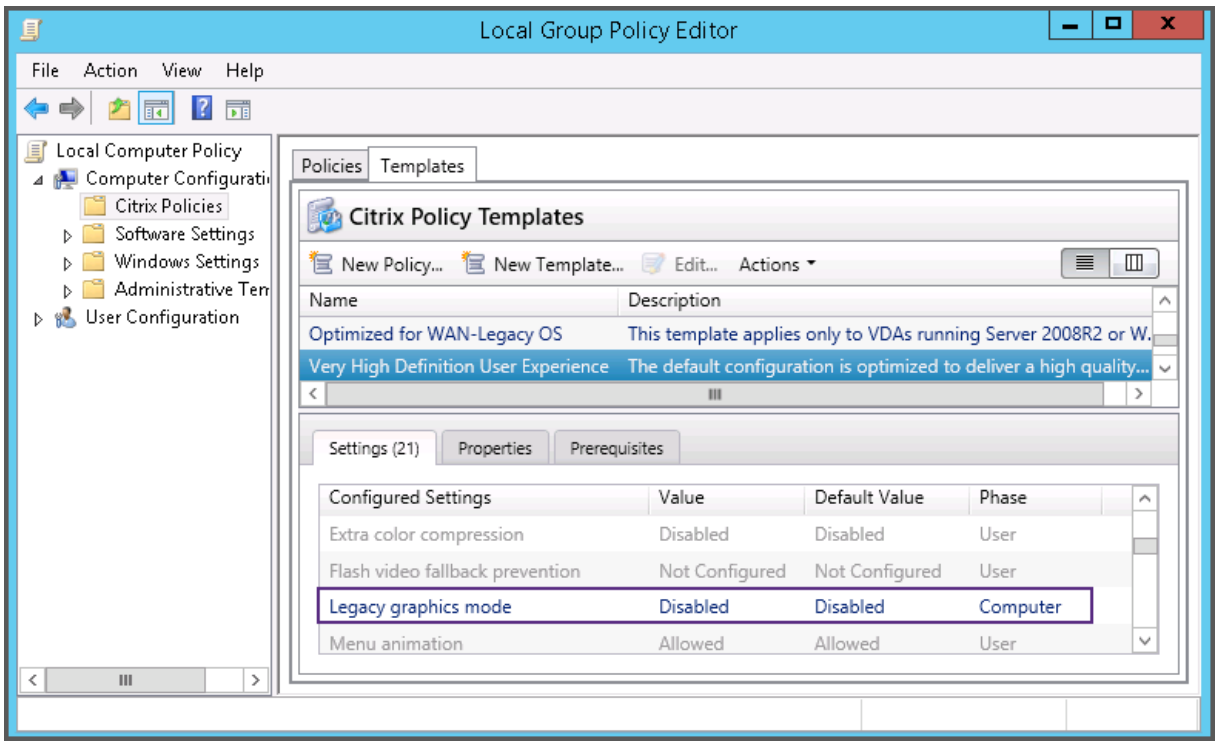
在 Studio 中，策略和模板显示在单个列表中，不管它们是否包含用户、计算机或两种设置类型，并且可以使用用户和计算机过滤器进行应用。

在组策略编辑器中，计算机和用户设置必须单独应用，即使是通过包含两种设置类型的模板创建也是如此。在此示例中，选择使用计算机配置中的超高清晰度用户体验：

- 旧图形模式是用于通过此模板创建的策略的计算机设置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 6, 2022

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 支持或可信第三方传递策略的方法。

策略模板可以导入和导出。

有关使用模板创建策略时的注意事项，请参阅知识库文章 CTX202330。

内置 **Citrix** 模板

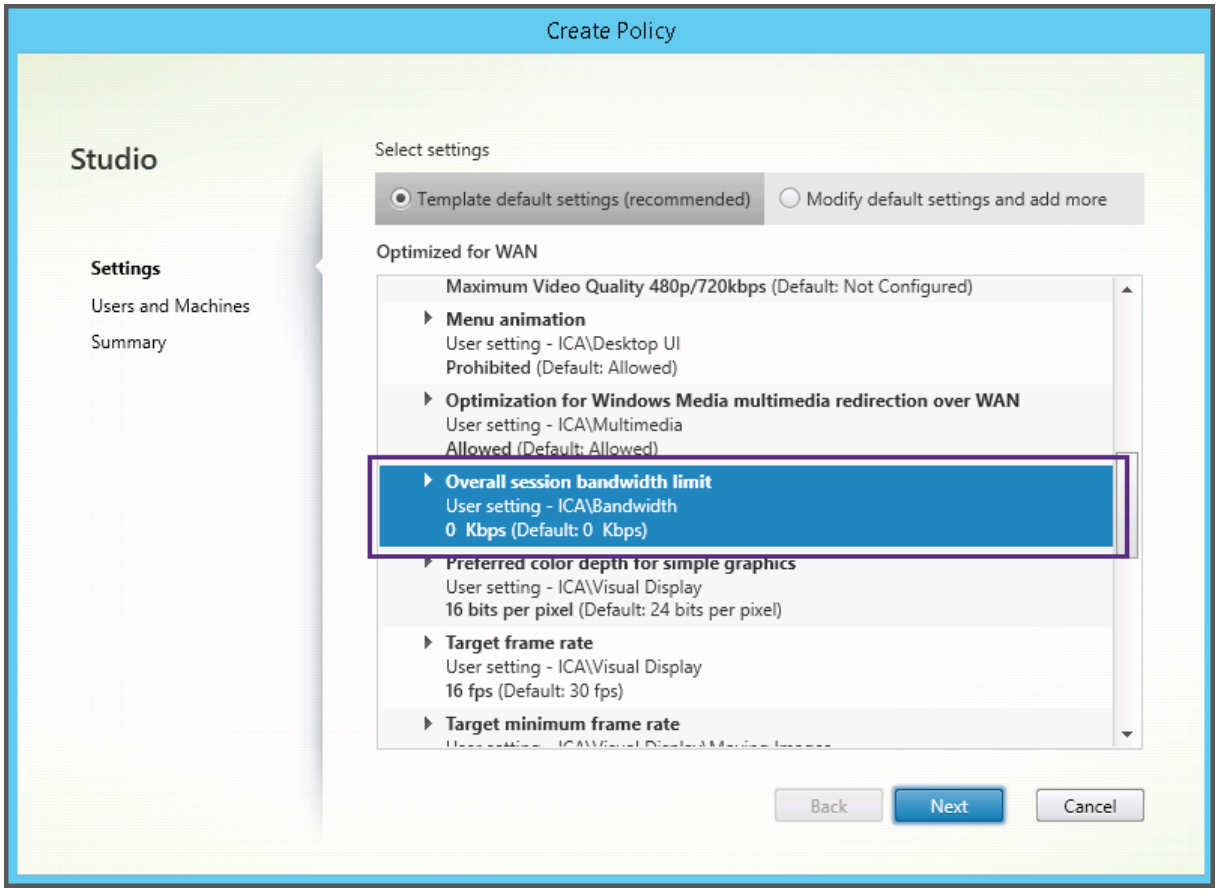
以下策略模板可用：

- 超高清晰度用户体验。此模板强制实施尽可能实现最佳用户体验的默认设置。在按照优先级顺序处理多个策略的场景中使用此模板。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 高服务器可扩展性。应用此模板可节约服务器资源。此模板可以平衡用户体验和服务器可扩展性。它可以提供良好的用户体验，同时增加单个服务器上可以托管的用户数。此模板不使用视频编解码器压缩图像，并阻止服务器端进行多媒体呈现。
- 高服务器可扩展性-旧版操作系统。此高服务器可扩展性模板仅适用于运行 Windows Server 2008 R2 或 Windows 7 及更早版本的 VDA。此模板依靠对这些操作系统较为有效的旧图形模式。
- 针对 **NetScaler SD-WAN** 优化。对在具有 NetScaler SD-WAN 的分支机构工作的用户应用此模板以优化 Citrix Virtual Desktops 的交付。(NetScaler SD-WAN 是 CloudBridge 的新名称)。
- **WAN** 优化。此模板旨在用于满足以下条件的任务型工作人员：位于使用共享 WAN 连接的分支结构或采用低带宽连接的远程位置，访问具有简单图形用户界面并且包含很少多媒体内容的应用程序。此模板通过降低视频播放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 Citrix Virtual Apps and Desktops 中默认启用的功能。此模板中包含用于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 加速的设置。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。

尽管我们建议使用内置 Citrix 模板的默认设置，但有些设置没有具体的建议值。例如，WAN 优化模板中的总会话带宽限制。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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

性”和“WAN 优化”模板，请使用这些模版的旧版操作系统版本（如果适用）。

> 注意：
>
> Citrix 负责创建和更新内置模板。您无法修改或删除这些模板。

使用 **Studio** 创建和管理模板

要基于模板创建模板，请执行以下操作：

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。删除任何不属于的现有设置。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。

要基于策略创建模板，请执行以下操作：

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。删除任何不属于的现有设置。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。选择合适的操作。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

任务	说明
基于现有策略创建模板	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 Citrix Virtual Apps and Desktops 站点的数据库。这意味着 Windows 管理权限负责控制策略模板文件，而非由站点的委派管理角色和作用域进行控制。

因此，站点中具有只读权限的管理员可以创建模板。但是，由于模板是本地文件，因此不对环境做任何更改。

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

September 8, 2022

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 组策略的相同条件。

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策略。

创建策略时，可以将策略模板中的设置作为基础并根据需要自定义设置，也可以不使用模板，然后添加所需的全部设置。

在 Citrix Studio 中，除非明确选中了启用策略复选框，否则创建的新策略会设置为“已禁用”。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。有时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来限制该设置的配置。这样将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，可以将其分配给某些用户和计算机对象。根据特定条件或规则将该策略应用于连接。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。

> 注意：
>
> 策略分配也称为策略过滤器。有关其他信息，请参阅以下主题：
>
> - 创建、修改或删除策略的过滤器
> - 如何应用过滤器？

下表列出了可用的分配：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 - 将策略应用于使用 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。访问条件 - 要使用的终点分析策略或会话策略的名称。
NetScaler SD-WAN	是否通过 NetScaler SD-WAN 启动用户会话。注意：您只能向策略中添加一个 NetScaler SD-WAN 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。注意：“专用桌面”和“共享桌面过滤器”选项仅适用于 Citrix Virtual Apps and Desktops 7.x。有关详细信息，请参阅 CTX219153。
组织单位 (OU)	组织单位。
标记	标记。注意：将此策略应用到所有带标记的计算机。不包括应用程序标记。
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 OU 包含名为 Sales-US 的 GPO，该 GPO 包含美国销售团

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

队的所有成员。该 Sales-US GPO 是使用包含多项用户策略设置的“未过滤”策略进行配置的。美国的销售经理登录到站点时，“未过滤”策略中的设置会自动应用到会话，因为该用户属于 Sales-US GPO 的成员。

分配的模式决定策略是否仅应用到符合所有分配条件的连接。如果将模式设置为允许（默认设置），策略将仅应用到符合分配条件的连接。如果将模式设置为拒绝，将在连接不符合分配条件时应用策略。下例说明了存在多个分配时分配模式对 Citrix 策略的影响。

- 示例：模式不同但类型相同的分配 - 如果策略中包含两个类型相同的分配，其中一个设置为“允许”，一个设置为“拒绝”，假设连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。模式设置为“允许”。
  - 分配 B 指定销售经理的帐户。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 是用于指定销售组的用户分配。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）。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 是用于指定销售组的用户分配。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。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. 通过选择以下选项之一指定应用策略的方式：

   - 分配给所选用户和计算机对象并选择要应用策略的用户和计算机对象。
   - 分配给站点中的所有对象以将策略应用到站点中的所有用户和计算机对象。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。如果您过后必须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。如果您过后必须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。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。向策略中添加多个过滤器时，必须满足所有过滤条件才能应用该策略。
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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

任务	说明
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

November 17, 2021

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，为获得增强的安全性，您可能需要对经常使用高度敏感数据的用户组设置限制。还可以创建一个这样的策略：它可以阻止用户在其本地客户端驱动器上保存敏感文件。但是，如果用户组中的某些人员确实需要访问其本地驱动器，则可以仅针对此类用户创建另一个策略。然后，您可以对这两个策略分级或设定两个策略的优先级，以控制哪个策略的优先顺序较高。

使用多个策略时，需要确定如何设定策略的优先级、如何创建例外情况，以及如何在策略冲突时查看有效的策略。

通常情况下，策略会覆盖针对整个站点、特定 Delivery Controller 或在用户设备上配置的相似设置。此原则的唯一例外情况是安全性。环境中的最高加密设置（包含操作系统及限制性最强的重影设置）通常会覆盖其他设置和策略。

Citrix 策略会与您在操作系统中设置的策略进行交互。在 Citrix 环境中，Citrix 设置会覆盖在 Active Directory 策略中配置的相同设置或使用远程桌面会话主机配置的相同设置。这包括与典型的远程桌面协议 (RDP) 客户端连接设置相关的设置（例如桌面墙纸、菜单动画以及拖动时查看窗口内容）。某些策略设置（例如 Secure ICA）必须与操作系统中的设置匹配。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必须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，当单会话操作系统 VDA 连接到多会话操作系统 VDA 时，Citrix 策略将像在用户设备上一样在单会话操作系统 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单会话操作系统 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，您可能需要验证设置值以确保遵从最佳做法。您可能还希望将策略或模板中的设置与 Citrix 提供的默认设置进行比较。

1. 在 Studio 导航窗格中选择策略。
2. 单击“比较”选项卡，然后单击“选择”。
3. 选择要比较的策略或模板。要同时比较默认值，请选中与默认设置进行比较复选框。
4. 单击比较后，已配置的设置按列显示。
5. 要查看所有设置，请选择显示所有设置。要返回到默认视图，请选择显示常规设置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。设置根据优先级以及设置的条件进行合并。例如，该设置是禁用还是启用。任何已禁用的设置都会覆盖等级较低的已启用设置。未配置的策略设置会被忽略，而且不会覆盖等级较低的设置的设置。

1. 在 Studio 导航窗格中选择策略。确保选择“策略”选项卡。
2. 选择一个策略。
3. 在“操作”窗格中，选择较低优先级或较高优先级。

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.*。模式设置为“允许”
- 分配 B 为用户分配，指定特定的用户帐户。模式设置为“拒绝”。

该策略适用于使用分配 A 中指定范围内的 IP 地址登录到站点的所有用户。但是，该策略不适用于使用分配 B 中指定的用户帐户登录到站点的用户，即使为该用户的计算机分配的 IP 地址在分配 A 中指定的范围内。

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这些对象（包括 Citrix 策略）应用到特定的用户和控制器。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 (gpmc.msc)，在树状窗格中的 Citrix 组策略建模上单击鼠标右键，然后选择 Citrix 组策略建模向导。

按照向导中的说明，选择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

January 21, 2022

以下各表列出了策略设置、其默认值以及设置应用到的 Virtual Delivery Agent (VDA) 版本。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ICA

名称	默认设置	VDA
自适应传输	关。偏好时使用	VDA 7.13–7.15；VDA 7.16 至当前版本
客户端剪贴板重定向	允许	VDA 的所有版本
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
桌面启动	禁止	适用于多会话操作系统的 VDA 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	适用于多会话操作系统的 VDA 7 至当前版本
将剪贴板客户端限制为会话传输大小	已禁用	VDA 2009
将剪贴板会话限制为客户端传输大小	已禁用	VDA 2009
丢失容忍模式	允许	VDA 2003。注意：丢失容忍模式尚不可用。本版本的 VDA 将在可用时向其提供支持。
丢失容忍阈值	当丢失容忍模式可用时：数据包丢失：5%，延迟：300 毫秒 (RTT)	VDA 2003 至当前版本
汇聚协议	已禁用	仅适用于通过 Citrix Cloud 建立的 HDX 会话。
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
平板电脑模式切换	已启用	VDA 7.16 至当前版本；对于 VDA 7.14 和 7.15 LTSR，请使用注册表配置此设置。
虚拟通道允许列表	已禁用	VDA 2006

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

名称	默认设置	VDA

ICA/音频

名称	默认设置	VDA
音频即插即用	允许	适用于多会话操作系统的 VDA 7 至当前版本
音频质量	高 - 高清晰度音频	VDA 的所有版本
客户端音频重定向	允许	VDA 的所有版本
客户端麦克风重定向	允许	VDA 的所有版本

ICA/客户端自动重新连接

名称	默认设置	VDA
通过 UDP 协议的音频实时传输	允许	VDA 的所有版本
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
客户端自动重新连接超时	120 秒	VDA 7.13 至当前版本
重新连接用户界面透明度级别	80%	VDA 7.13 至当前版本

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、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

名称	默认设置	VDA
客户端 USB 设备重定向带宽限制百分比	0	VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 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 7.0 至 7.8 版本，使用注册表配置此设置
COM 端口重定向带宽限制百分比	0	VDA 的所有版本；对于 VDA 7.0 至 7.8 版本，使用注册表配置此设置
文件重定向带宽限制	0 Kbps	VDA 的所有版本
文件重定向带宽限制百分比	0	VDA 的所有版本
HDX MediaStream 多媒体加速带宽限制	0 Kbps	VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 和适用于单会话操作系统的 VDA 7 至当前版本的适用于多会话操作系统的 VDA 和适用于单会话操作系统的 VDA
HDX MediaStream 多媒体加速带宽限制百分比	0	VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本
LPT 端口重定向带宽限制	0 Kbps	VDA 的所有版本；对于 VDA 7.0 至 7.8 版本，使用注册表配置此设置
LPT 端口重定向带宽限制百分比	0	VDA 的所有版本；对于 VDA 7.0 至 7.8 版本，使用注册表配置此设置
总会话带宽限制	0 Kbps	VDA 的所有版本
打印机重定向带宽限制	0 Kbps	VDA 的所有版本
打印机重定向带宽限制百分比	0	VDA 的所有版本
TWAIN 设备重定向带宽限制	0 Kbps	VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 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、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本

ICA/双向内容重定向

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

名称	默认设置	VDA
允许双向内容重定向	禁止	VDA 7.13 至当前版本
允许重定向到客户端的 URL	empty	VDA 7.13 至当前版本
允许重定向到 VDA 的 URL	empty	VDA 7.13 至当前版本
客户端到主机 (VDA) 和客户端到客户端双向内容重定向		使用 Citrix Workspace 应用程序组策略对象管理模板

ICA/浏览器内容重定向

名称	默认设置	VDA
浏览器内容重定向	允许	VDA 7.16 至当前版本
浏览器内容重定向 ACL 配置	`https://www.youtube.com/*`	VDA 7.16 至当前版本
浏览器内容重定向集成 Windows 身份验证支持	禁止	VDA 2106 至当前版本
浏览器内容重定向代理配置	empty	VDA 7.16 至当前版本
浏览器内容重定向服务器提取 Web 代理身份验证	禁止	VDA 2012 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、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本

ICA/桌面 **UI**

名称	默认设置	VDA
桌面组合重定向	已禁用（7.6 FP3 至当前版本）；已启用（5.6 至 7.6 FP2）	VDA 5.6、适用于单会话操作系统的 VDA 7 到 7.15

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

名称	默认设置	VDA
桌面组合重定向图形质量	中	VDA 5.6、适用于单会话操作系统的 VDA 7 到 7.15
桌面墙纸	允许	VDA 的所有版本
菜单动画	允许	VDA 的所有版本
拖动时查看窗口内容	允许	VDA 的所有版本

ICA/最终用户监视

名称	默认设置	VDA
ICA 往返行程计算	已启用	VDA 的所有版本
ICA 往返行程计算间隔	15 秒	VDA 的所有版本
空闲连接的 ICA 往返行程计算	已禁用	VDA 的所有版本

ICA/增强的桌面体验

名称	默认设置	VDA
增强的桌面体验	允许	适用于多会话操作系统的 VDA 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

名称	默认设置	VDA
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	适用于多会话操作系统的 VDA 7 至当前版本
保留客户端驱动器盘符	已禁用	VDA 5、5.5、5.6 FP1、适用于单会话操作系统的 VDA 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、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本
特殊文件夹重定向	允许	仅限 Web Interface 部署；适用于多会话操作系统的 VDA 7 至当前版本
使用异步写入	已禁用	VDA 的所有版本

ICA/图形

名称	默认设置	VDA
允许视觉无损压缩	已禁用	VDA 7.6 至当前版本
显示内存限制	65536 Kb	VDA 5、5.5、5.6 FP1、适用于单会话操作系统的 VDA 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、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本
图像缓存	已启用	VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本
旧图形模式	已禁用	适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 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	适用于多会话操作系统的 VDA 7 至当前版本
针对 3D 图形工作负载优化	已禁用	VDA 7.17 至当前版本
排队与丢弃	已启用	VDA 的所有版本
使用视频编解码器进行压缩	偏好时使用视频编解码器	VDA 7.6 FP3 至当前版本

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

名称	默认设置	VDA
使用视频编解码器的硬件编码	已启用	VDA 7.11 至当前版本

ICA/图形**/**缓存

名称	默认设置	VDA
永久性缓存阈值	3000000 bps	适用于多会话操作系统的 VDA 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	32243324	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	适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

名称	默认设置	VDA
URL 重定向阻止列表	未指定任何站点	适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本
URL 重定向允许列表	未指定任何站点	适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 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、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本
启动经过触控优化的桌面	允许	VDA 5.6 FP1、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本此设置已禁用，不适用于 Windows 10 和 Windows Server 2016 计算机。
远程控制组合框	禁止	VDA 5.6 FP1、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本

ICA/多媒体

名称	默认设置	VDA
HTML5 视频重定向	禁止	VDA 7.12 至当前版本
限制视频质量	未配置	适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本
Microsoft Teams 重定向	允许	适用于多会话操作系统的 VDA 1906 至当前版本、适用于单会话操作系统的 VDA 1906 至当前版本
多媒体会议	允许	VDA 的所有版本

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

名称	默认设置	VDA
优化通过 WAN 进行的 Windows Media 多媒体重定向	允许	适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本
使用 GPU 优化通过 WAN 进行的 Windows Media 多媒体重定向	禁止	适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本
Windows Media 回退预防	未配置	VDA 7.6 FP3 至当前版本
Windows Media 客户端内容提取	允许	适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 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 至当前版本
Windows Media 重定向缓冲区大小的使用	已禁用	VDA 5、5.5、5.6 FP1 至当前版本

ICA/多流连接

名称	默认设置	VDA
通过 UDP 传输音频	允许	适用于多会话操作系统的 VDA 7 至当前版本
音频 UDP 端口范围	16500、16509	VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 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、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本
多流计算机设置	已禁用	VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本
多流用户设置	已禁用	VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本
多流虚拟通道流分配设置	有关默认流分配，请参阅多流虚拟通道分配设置	VDA 2003

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 7.0 至 7.8 版本，使用注册表配置此设置
自动连接客户端 LPT 端口	已禁用	VDA 的所有版本；对于 VDA 7.0 至 7.8 版本，使用注册表配置此设置
客户端 COM 端口重定向	禁止	VDA 的所有版本；对于 VDA 7.0 至 7.8 版本，使用注册表配置此设置
客户端 LPT 端口重定向	禁止	VDA 的所有版本；对于 VDA 7.0 至 7.8 版本，使用注册表配置此设置

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 5.6
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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

名称	默认设置	VDA
打印机属性保留	仅当未保存在客户端时才保留在配置文件中	VDA 的所有版本
保留和恢复的客户端打印机	允许	VDA 5、5.5、5.6 FP1

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
通用驱动程序优先级	EMF、XPS、PCL5c、PCL4、PS	VDA 的所有版本
通用打印驱动程序用法	仅当请求的驱动程序不可用时才使用通用打印	VDA 的所有版本

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 (kbps)	0	VDA 的所有版本
通用打印服务器 Web 服务 (HTTP/SOAP) 端口	8080	VDA 的所有版本
用于负载平衡的通用打印服务器		VDA 7.9 版至最新版本
通用打印服务器停止运行阈值	180（秒）	VDA 7.9 版至最新版本

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

名称	默认设置	VDA
通用打印图像压缩限制	最佳质量 (无损压缩)	VDA 的所有版本
通用打印优化默认值	图像压缩：所需图像质量 = 标准质量，启用超级压缩 = False；图像和字体缓存：允许缓存嵌入的图像 = True；允许非管理员修改这些设置 = False；	VDA 的所有版本
通用打印预览首选项	不对自动创建的打印机或一般通用打印机使用打印预览	VDA 的所有版本
通用打印的打印质量限制	无限制	VDA 的所有版本

ICA/安全性

名称	默认设置	VDA
SecureICA 最低加密级别	基本	适用于多会话操作系统的 VDA 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	适用于多会话操作系统的 VDA 7 至当前版本

ICA/会话限制

名称	默认设置	VDA
断开会话计时器	已禁用	VDA 5、5.5、5.6 FP1、适用于单会话操作系统的 VDA 7 至当前版本
Remote PC Access 断开连接的会话计时	已禁用	适用于单会话操作系统的 VDA 7 至当前版本
断开会话计时器间隔	1440 分钟	VDA 5、5.5、5.6 FP1、适用于单会话操作系统的 VDA 7 至当前版本

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

名称	默认设置	VDA
会话连接计时器	已禁用	VDA 5、5.5、5.6 FP1、适用于单会话操作系统的 VDA 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、适用于单会话操作系统的 VDA 7 至当前版本
会话空闲计时器	已启用	VDA 5、5.5、5.6 FP1、适用于单会话操作系统的 VDA 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、适用于单会话操作系统的 VDA 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
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	适用于多会话操作系统的 VDA 7 至当前版本
在会话断开连接或注销时还原单会话操作系统时区	已启用	当前 VDA 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

名称	默认设置	VDA
客户端 TWAIN 设备重定向	允许	VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本
TWAIN 压缩级别	中	VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 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	已启用（VDA 7.6 FP3 至当前版本）；已禁用（VDA 7.11 至当前版本）；默认情况下，不指定任何规则	VDA 7.6 FP3 至当前版本
客户端 USB 设备重定向	禁止	VDA 的所有版本
客户端 USB 设备重定向规则	未指定任何规则	VDA 的所有版本
客户端 USB 即插即用设备重定向	允许	适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 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	适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本

ICA/视频显示**/**移动图像

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

名称	默认设置	VDA
最低图像质量	标准	VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本
移动图像压缩	已启用	VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本
渐进式压缩级别	无	VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本
渐进式压缩阈值	2,147,483,647 Kbps	VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本
目标最低帧速率	10 fps	VDA 5.5、5.6 FP1、适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 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	2,147,483,647 Kbps	VDA 的所有版本

ICA/WebSockets

名称	默认设置	VDA
WebSocket 连接	禁止	适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

名称	默认设置	VDA
WebSocket 端口号	8008	适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本
WebSocket 可信源服务器列表	通配符 * 用于信任所有 Receiver for Web URL	适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本

负载管理

名称	默认设置	VDA
并发登录容错	2	适用于多会话操作系统的 VDA 7 至当前版本
CPU 使用率	已禁用	适用于多会话操作系统的 VDA 7 至当前版本
排除 CPU 使用率的进程优先级	低于正常或低	适用于多会话操作系统的 VDA 7 至当前版本
磁盘使用情况	已禁用	适用于多会话操作系统的 VDA 7 至当前版本
最大会话数	250	适用于多会话操作系统的 VDA 7 至当前版本
内存使用率	已禁用	适用于多会话操作系统的 VDA 7 至当前版本
内存使用基础负载	零负载：768 MB	适用于多会话操作系统的 VDA 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Profile Management/基本设置

名称	默认设置	VDA
主动回写	已禁用	VDA 的所有版本
启用 Profile Management	已禁用	VDA 的所有版本
排除的组	已禁用。处理所有用户组的成员。	VDA 的所有版本
脱机配置文件支持	已禁用	VDA 的所有版本
用户存储路径	Windows	VDA 的所有版本
处理本地管理员登录	已禁用	VDA 的所有版本
处理的组	已禁用。处理所有用户组的成员。	VDA 的所有版本

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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
要镜像的文件夹	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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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”的重定向位置	内容将重定向到在“下载”路径策略设置中指定的 UNC 路径	VDA 的所有版本

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

名称	默认设置	VDA
“搜索”路径	已禁用。未指定任何位置。	VDA 的所有版本
“搜索”的重定向设置	内容将重定向到在“搜索”路径策略设置中指定的 UNC 路径	VDA 的所有版本

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
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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

名称	默认设置	VDA
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
登录及注销时的策略值	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
删除缓存的配置文件之前的延迟	0	VDA 的所有版本
Delete locally cached profiles on logoff（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。在用户首次登录的设备上，会通过默认用户配置文件创建新用户配置文件。	VDA 的所有版本
模板配置文件覆盖本地配置文件	已禁用	VDA 的所有版本
模板配置文件覆盖漫游配置文件	已禁用	VDA 的所有版本
模板配置文件用作所有登录的 Citrix 强制配置文件	已禁用	VDA 的所有版本

Profile Management/注册表

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

名称	默认设置	VDA
排除列表	已禁用。用户注销时，将处理 HKCU 配置单元中的所有注册表项。	VDA 的所有版本
包含列表	已禁用。用户注销时，将处理 HKCU 配置单元中的所有注册表项。	VDA 的所有版本

Profile Management/流用户配置文件

名称	默认设置	VDA
总是缓存	已禁用	VDA 的所有版本
总是缓存的大小	0 Mb	VDA 的所有版本
Profile Streaming	已禁用	VDA 的所有版本
流用户配置文件组	已禁用。正常情况下，将处理 OU 内的所有用户配置文件。	VDA 的所有版本
挂起区域锁定文件超时 (天数)	1 天	VDA 的所有版本

Receiver

名称	默认设置	VDA
StoreFront 帐户列表	未指定任何存储	适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本

用户个性化层

名称	默认设置	VDA
用户层存储库路径	已禁用。未指定任何路径。	VDA 19.12 及更高版本
用户层大小 (GB)	10 GB。用户层是精简预配的磁盘，可扩展到设置的大小。用户层的大小永远不会减小。	版本 19.12 或更高版本

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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	适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本
控制器注册端口	80	VDA 的所有版本
控制器 SID	未指定任何 SID	VDA 的所有版本
控制器	未指定任何控制器	VDA 的所有版本
启用控制器自动更新	已启用	适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本
仅使用 IPv6 控制器注册	已禁用	适用于多会话操作系统的 VDA 7 至当前版本、适用于单会话操作系统的 VDA 7 至当前版本
站点 GUID	未指定任何 GUID	VDA 的所有版本

Virtual Delivery Agent/HDX 3D Pro

名称	默认设置	VDA
启用无损	已启用	VDA 5.5、5.6 FP1
HDX 3D Pro 质量设置		VDA 5.5、5.6 FP1

Virtual Delivery Agent/监视

名称	默认设置	VDA
启用进程监视	已禁用	VDA 7.11 至当前版本
启用资源监视	已启用	VDA 7.11 至当前版本

虚拟 IP

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

策略设置参考

November 17, 2021

“策略”包含强制执行策略时应用的设置。本部分中的说明还会指出要启用某项功能是否需要更多设置或与某项设置相似的更多设置。

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。

所有策略设置的完整列表将以.CHM（编译后的 HTML）格式和.CSV 格式提供。这些文件位于安装了代理 (Delivery Controller) 的服务器上的 `\program files\citrix\grouppolicy` 文件夹中。您也可以通过单击此处下载最新版本的策略设置。

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”

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

要限制用于以下项目的带宽	使用此策略设置
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	“打印机重定向带宽限制”或“打印机重定向带宽限制百分比”
TWAIN 设备（例如照相机或扫描仪）	“TWAIN 设备重定向带宽限制”或“TWAIN 设备重定向带宽限制百分比”
USB 设备	“客户端 USB 设备重定向带宽限制”或“客户端 USB 设备重定向带宽限制百分比”

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”
控制在会话中可否使用用户的本地 CD、DVD 或蓝光驱动器	“客户端光盘驱动器”和“客户端驱动器重定向”
控制在会话中可否使用用户的本地可移动驱动器	“客户端可移动驱动器”和“客户端驱动器重定向”
控制在会话中可否使用用户的 TWAIN 设备（如扫描仪和相机），并控制图像数据传输的压缩	客户端 TWAIN 设备重定向；TWAIN 压缩重定向
控制在会话中可否使用 USB 设备	“客户端 USB 设备重定向”和“客户端 USB 设备重定向规则”
提高通过 WAN 将文件写入和复制到客户端磁盘的速度	使用异步写入

内容重定向

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

> 重要：
>
> Flash 策略保留仅允许具有较旧 VDA 的客户使用较新的控制器（例如，版本为 1912 的控制器）并仍然使用 Flash。此 VDA 版本不支持 Flash。

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
控制在会话中访问时 Web 站点可否显示 Flash 内容	Flash 服务器端内容提取 URL 列表；Flash URL 兼容性列表；Flash 视频回退预防策略设置；Flash 视频回退预防错误 *.swf
控制服务器端呈现的视频的压缩	使用视频编解码器进行压缩；使用视频编解码器的硬件编码
控制 HTML5 多媒体 Web 内容向用户的交付	HTML5 视频重定向

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	多流（计算机和用户设置）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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
控制客户端还是服务器处理打印请求	直接连接到打印服务器
控制用户可否访问连接到其用户设备的打印机	客户端打印机重定向
控制自动创建客户端和网络打印机时的本机 Windows 驱动程序的安装	自动安装现成的打印机驱动程序
控制何时使用通用打印机驱动程序	通用打印驱动程序用法
根据漫游用户会话信息选择打印机	默认打印机
平衡通用打印服务器的负载并设置故障转移阈值	用于负载平衡的通用打印服务器；通用打印服务器停止运行阈值

> 注意：
>
> 在桌面或应用程序会话中不能使用策略来启用屏幕保护程序。如果用户需要启用屏幕保护程序，可以在用户设备上实现。

ICA 策略设置

June 29, 2023

自适应传输

此设置允许或阻止基于 EDT 的数据传输作为主要方式以及回退到 TCP。

默认情况下，启用自适应传输（首选），以及尽可能使用 EDT，并启用回退到 TCP。如果已禁用，而您希望将其启用，请按照此过程进行操作。

1. 在 Studio 中，启用策略设置“HDX 自适应传输”。我们还建议您不要将此功能作为站点中所有对象的通用策略来启用。
2. 要启用该策略设置，请将值设置为首选，然后单击确定。

首选。尽可能使用基于 EDT 的自适应传输，并回退到 TCP。

诊断模式。强制启用 EDT，并禁用回退到 TCP。我们建议此设置仅用于故障排除。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

关。强制启用 TCP，并禁用 EDT。

有关详细信息，请参阅自适应传输。

应用程序启动等待超时

此设置指定会话等待第一个应用程序启动的等待超时值（毫秒）。如果应用程序的启动超过此时间段，会话将结束。

您可以选择默认时间（10,000 毫秒），也可以指定一个数字（毫秒）。

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。

允许此设置之后，配置剪贴板在客户端连接中可以占用的最大允许带宽量。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。

客户端剪贴板写入允许的格式

限制客户端剪贴板写入设置设为已启用时，不能与客户端端点共享主机剪贴板数据。可以使用此设置来允许与客户端端点剪贴板共享特定数据格式。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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

以下自定义格式是在 XenApp 和 XenDesktop 及 Citrix Virtual Apps and Desktops 中预定义的格式：

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- CFX_FILE

HTML 格式默认处于禁用状态。启用该功能：

- 请务必将客户端剪贴板重定向设置为允许。
- 请务必将限制客户端剪贴板写入设置为已启用。
- 在客户端剪贴板写入允许的格式中为 **CF_HTML**（以及希望支持的任何其他格式）添加相应的条目。

您可以添加更多自定义格式。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。

> 注意
>
> 启用 HTML 格式剪贴板复制支持 (CF_HTML) 会将所有脚本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 文件并执行时，这些脚本才处于活动状态。

将剪贴板客户端限制为会话传输大小

此设置指定在单个剪切和粘贴操作期间用户可以从客户端端点传输到虚拟会话的剪贴板数据的最大大小。

要限制剪贴板传输大小，请启用将剪贴板会话限制为客户端传输大小设置。然后，在大小限制字段中，输入一个以千字节为单位的值，以定义本地剪贴板与会话之间的数据传输大小。

默认情况下，此设置处于禁用状态，并且对客户端到会话的传输没有限制。

将剪贴板会话限制为客户端传输大小

此设置指定在单个剪切和粘贴操作期间用户可以从虚拟会话传输到客户端端点的剪贴板数据的最大大小。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

要限制剪贴板传输大小，请启用将剪贴板会话限制为客户端传输大小设置。然后，在大小限制字段中，输入一个以千字节为单位的值，以定义会话与本地剪贴板之间的数据传输大小。

默认情况下，此设置处于禁用状态，并且对到客户端的会话传输没有限制。

限制客户端剪贴板写入

如果将其设置为允许，则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。可以使用此设置来允许与会话剪贴板共享特定数据格式。

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

以下自定义格式是在 XenApp 和 XenDesktop 及 Citrix Virtual Apps and Desktops 中预定义的格式：

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

HTML 格式默认处于禁用状态。启用该功能：

- 请务必将客户端剪贴板重定向设置为允许。
- 请务必将限制会话剪贴板写入设置为已启用。
- 在会话剪贴板写入允许的格式中为 **CF_HTML**（以及希望支持的任何其他格式）添加相应的条目。

您可以添加更多自定义格式。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。

> 注意：
>
> 启用 HTML 格式剪贴板复制支持 (CF_HTML) 会将所有脚本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 文件并执行时，这些脚本才处于活动状态。

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。无论是否启用此设置，这些用户都可以连接到 VDA。此设置对不在 VDA 直接访问用户组中的非管理用户没有影响。无论是否启用此设置，这些用户都无法连接到 VDA。

FIDO2 重定向

此设置启用或禁用 FIDO2 重定向。FIDO2 重定向使用户能够利用虚拟机中的本地端点 FIDO2 组件。用户可以在安装了 TPM 2.0 和 Windows Hello 的设备上使用 FIDO2 安全密钥或集成的生物特征在其虚拟会话中进行身份验证。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

当此设置为允许时，用户可以使用本地端点功能执行 FIDO2 身份验证。默认情况下，此设置设为允许。

还可以通过配置以下注册表项在客户端端点上启用或禁用 FIDO2 重定向：

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\

名称：FIDO2

类型：REG_DWORD

值：1

将值设置为 0 可禁用该功能，将值设置为 1 可将其启用。默认情况下，该功能处于启用状态。

> 小心：
>
> 注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

ICA 侦听器连接超时

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 120,000 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 Workspace 应用程序或插件上更改该端口号。

键盘和输入法编辑器 **(IME)**

此设置启用或禁用动态键盘布局同步、输入法编辑器 (IME)、Unicode 键盘布局映射，并隐藏或显示键盘布局切换通知对话框消息。

1. 在 Studio 中，选择键盘和 **IME**。
2. 选择客户端键盘布局同步和 **IME** 改进功能以控制 VDA 中的动态键盘布局同步和通用客户端输入法编辑器 (IME) 功能。您可以配置：

   已禁用 - 动态键盘布局同步和通用客户端输入法编辑器 (IME)。

   支持动态客户端键盘布局同步 - 启用动态键盘布局同步。

   支持动态客户端键盘布局同步和 **IME** 改进功能 - 支持动态键盘布局同步和通用客户端输入法编辑器 (IME)。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. 选择启用 **Unicode** 键盘布局映射以启用或禁用 Unicode 键盘映射。
4. 选择隐藏键盘布局开关弹出消息框，以控制是否显示指明用户在更改客户端键盘布局时正在同步键盘布局的消息。如果您阻止显示消息，则用户需要在键入内容之前稍等片刻，以避免输入错误的字符。

默认设置：

- 客户端键盘布局同步和 **IME** 改进功能
  - 在 Windows Server 2016 和 Windows Server 2019 中禁用。
  - 在 Windows Server 2012 和 Windows 2010 中支持动态客户端键盘布局同步和 IME 改进功能。
- 禁用 **Unicode** 键盘布局映射
- 显示键盘布局开关弹出消息框

此策略替换策略设置的说明部分中列出的注册表设置。

注销检查器启动延迟

此设置指定注销检查器启动的延迟持续时间。使用此策略可设置客户端会话在断开连接之前等待的时间（秒）。

此设置还会增加用户从服务器注销所花时间。

丢失容忍模式

> 重要：
>
> - 此功能需要至少使用适用于 Windows 的 Citrix Workspace 应用程序 2002。本版本的 VDA 将在可用时向其提供支持。
> - Citrix Gateway 或 Citrix Gateway Service 不支持丢失容忍模式。此模式仅适用于直接连接。

此设置启用或禁用丢失容忍模式。

默认情况下，丢失容忍模式设置为允许。

如果允许，当数据包丢失和延迟超过阈值时将进入该模式。可以使用丢失容忍阈值策略设置阈值。

有关详细信息，请参阅丢失容忍模式。

丢失容忍阈值

丢失容忍模式可用时，此设置指定会话切换到丢失容忍模式的网络指标阈值。

默认阈值为：

- 数据包丢失：5%

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 延迟：300 毫秒（RTT）

有关详细信息，请参阅丢失容忍模式。

汇聚协议

此设置更改了使用 Citrix Gateway 服务时 HDX 会话代理的方式。启用后，HDX 流量不再通过 Citrix Cloud Connector 传输。相反，VDA 将与 Citrix Gateway 服务直接建立出站连接（从而增强 Cloud Connector 可扩展性）。

> 重要：
>
> 此功能由 Citrix Cloud 中的功能切换和 HDX 策略设置控制。Citrix Cloud 功能切换默认处于启用状态，而 HDX 设置默认处于禁用状态。HDX 设置仅影响通过 Citrix Gateway 服务建立的 HDX 会话。此设置对直接在客户端与 VDA 之间或通过本地 Citrix Gateway 建立的会话没有任何影响。

有关信息，请参阅回绝协议。

汇聚代理配置

此设置允许您配置显式代理以便与汇聚协议一起使用。如果使用透明代理，则无需启用此设置。

默认情况下，禁用此设置。

禁用后，VDA 在尝试与 Gateway Service 建立汇聚连接时不会通过任何非透明代理路由出站流量。

启用后，VDA 将尝试通过在此设置中定义的代理与 Gateway Service 建立汇聚连接。

VDA 支持使用 HTTP 和 SOCKS5 代理建立汇聚连接。要将 VDA 配置为使用代理建立汇聚连接，必须启用此设置并指定代理的地址或者 PAC 文件的路径。例如：

- 代理地址：`http://<URL or IP>:<port>` 或 `socks5://<URL or IP>:<port>`
- PAC 文件：`http://<URL or IP>/<path>/<filename>.pac`

  VDA 版本 2103 是使用 PAC 文件进行代理配置的受支持的最低版本。有关 SOCKS5 代理的 PAC 文件架构的详细信息，请参阅代理配置。

> 注意：
>
> 只有 SOCKS5 代理支持通过 EDT 进行数据传输。对于 HTTP 代理，请使用 TCP 作为 ICA 的传输协议。

有关详细信息，请参阅 Rendezvous 协议。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。

平板电脑模式切换策略设置

平板电脑模式切换优化了 VDA 上的应用商店应用程序、Win32 应用程序和 Windows Shell 的外观和行为。这是通过在从手机和平板电脑等小型设备或任何启用了触控功能的设备连接时自动将虚拟桌面切换到平板电脑模式来实现的。

如果禁用此策略，则 VDA 处于用户设置的模式，并始终保持相同的模式，无论客户端属于何种类型。

客户端自动重新连接策略设置

November 17, 2021

“客户端自动重新连接”部分包含用于控制会话自动重新连接的策略设置。

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。

对于 Citrix Receiver for Windows 4.7 及更高版本以及 Citrix Workspace 应用程序 1808 及更高版本，客户端自动重新连接仅使用 Citrix Studio 中的策略设置。在 Studio 中这些策略的更新会将客户端自动重新连接从服务器同步到客户端。使用旧版本的 Citrix Receiver for Windows 时，要配置客户端自动重新连接，请使用 Studio 策略并更改注册表或 default.ica 文件。

如果允许客户端自动重新连接，则当连接断开时，用户将可以从中断处继续执行原来的工作。自动重新连接会检测连接断开情形，然后将用户重新连接到其会话。

如果不使用包含会话 ID 和凭据的密钥的 Citrix Workspace 应用程序 Cookie，自动重新连接可能会导致启动新会话。也就是说，不重新连接到现有会话。如果 Cookie 已过期（例如因为重新连接延迟，或者必须重新输入凭据），则不使用该 Cookie。如果用户有意断开连接，则不触发客户端自动重新连接。

重新连接过程中，会话窗口将显示为灰色。倒计时器显示重新连接会话之前的剩余时间。会话超时时将断开连接。

对于应用程序会话，允许自动重新连接时，通知区域中将显示一个倒计时器，指定重新连接会话之前的剩余时间。Citrix Workspace 应用程序将一直尝试重新连接会话，直到重新连接成功或者用户取消重新连接尝试为止。

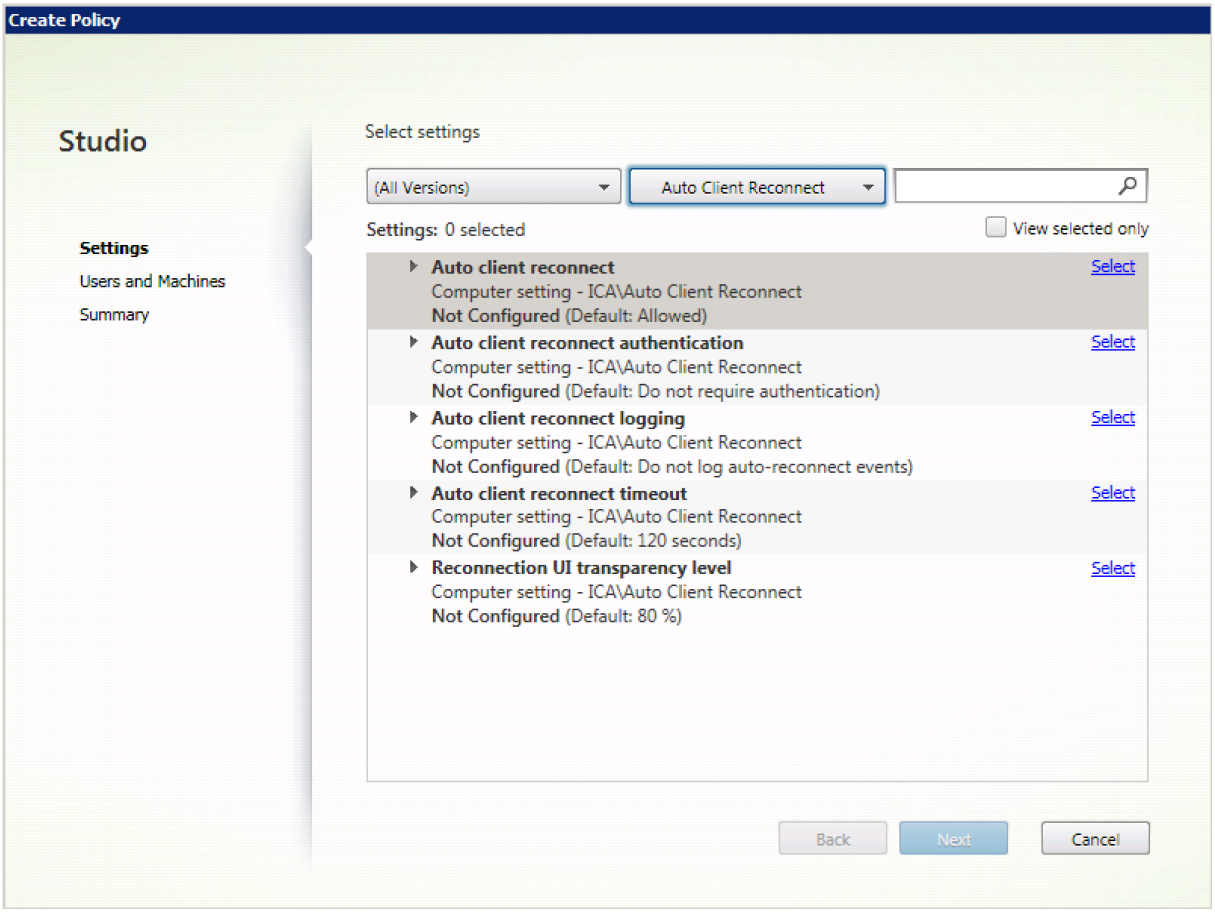
对于用户会话，允许自动重新连接时，Citrix Workspace 应用程序将在指定时间段内尝试重新连接会话，除非重新连接成功或者用户取消了重新连接尝试。默认情况下，此时间段为两分钟。要更改此时间期限，请编辑策略。

默认情况下，允许客户端自动重新连接。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

要禁用客户端自动重新连接，请执行以下操作：

1. 启动 Citrix Studio。
2. 打开客户端自动重新连接策略。
3. 将策略设置为禁止。



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。

在用户最初登录时，其凭据将加密并存储在内存中，并创建一个包含加密密钥的 cookie。Cookie 将发送到 Citrix Workspace 应用程序。配置此设置后，将不使用 Cookie。而是在 Citrix Workspace 应用程序尝试自动重新连接时，向用户显示一个对话框，要求输入凭据。

默认情况下，无需进行身份验证。

要更改客户端自动重新连接身份验证，请执行以下操作：

1. 启动 Citrix Studio。
2. 打开客户端自动重新连接身份验证策略。
3. 启用或禁用身份验证。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. 选择 **OK**（确定）。

客户端自动重新连接日志记录

此设置启用或禁用在事件日志中记录客户端自动重新连接。

启用日志记录后，服务器系统日志将捕获与成功或失败的自动重新连接事件有关的信息。站点并不会提供所有服务器的重新连接事件组合日志。

默认情况下，禁用日志记录。

要更改客户端自动重新连接日志记录，请执行以下操作：

1. 启动 Citrix Studio。
2. 打开客户端自动重新连接日志记录策略。
3. 启用或禁用日志记录。
4. 选择 **OK**（确定）。

客户端自动重新连接超时

默认情况下，客户端自动重新连接超时设置为 120 秒，可配置的最大客户端自动重新连接超时值为 300 秒。

要更改客户端自动重新连接超时，请执行以下操作：

1. 启动 Citrix Studio。
2. 打开客户端自动重新连接超时策略。
3. 编辑超时值。
4. 选择 **OK**（确定）。

重新连接用户界面透明度级别

可以使用 Studio 策略配置会话可靠性重新连接过程中应用到 XenApp 或 XenDesktop 会话窗口的不透明度级别。

默认情况下，重新连接用户界面透明度设置为 80%。

要更改重新连接用户界面不透明度级别，请执行以下操作：

1. 启动 Citrix Studio。
2. 打开重新连接 **UI** 透明度级别策略。
3. 编辑值。
4. 选择 **OK**（确定）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

音频策略设置

November 17, 2021

“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** 协议的音频实时传输

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 多会话操作系统计算机。

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高可压缩到 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 IP 语音质量无法满足需要，请确保将“通过 UDP 协议的音频实时传输”策略设置为“允许”。

  现在，“通过 UDP 进行实时传输 (RTP)”仅在选中此音频质量时受支持。即使在以下情况下交付媒体应用程序，也可以使用此音频质量：网络连接不畅，例如网速低（低于 512 Kbps）；网络拥堵且有数据包丢失。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 多会话操作系统计算机上，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 Workspace 应用程序上禁用警报。

在 Windows 多会话操作系统计算机上，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

January 21, 2022

“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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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）。

如果为此设置和音频重定向带宽限制百分比设置都输入了一个值，则应用最严格的设置（较低的值）。

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，则应用最严格的设置（较低的值）。

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，将应用最严格的设置（较低的值）。

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，将应用最严格的设置（较低的值）。

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，则应用最严格的设置（较低的值）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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，则应用最严格的设置（较低的值）。

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 7.0 到 7.8，请使用注册表配置此设置；请参阅使用注册表配置 COM 端口和 LPT 端口重定向设置。

此设置指定在客户端连接中访问 COM 端口时允许使用的最大带宽 (Kbps)。如果为此设置输入一个值，并为 COM 端口重定向带宽限制百分比设置输入一个值，则应用最严格的设置（较低的值）。

COM 端口重定向带宽限制百分比

注意：对于 Virtual Delivery Agent 7.0 到 7.8，请使用注册表配置此设置；请参阅使用注册表配置 COM 端口和 LPT 端口重定向设置。

此设置指定在客户端连接中访问 COM 端口时允许使用的最大带宽（占总会话带宽的百分比）。

默认情况下，未指定最大值（零）

如果为此设置输入一个值，并为 COM 端口重定向带宽限制设置输入一个值，则应用最严格的设置（较低的值）。

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）。

如果为此设置和文件重定向带宽限制百分比设置都输入了一个值，则应用最严格的设置（较低的值）。

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，则应用最严格的设置（较低的值）。

如果配置此设置，还必须配置总会话带宽限制设置，后者用于指定客户端会话可用的带宽总量。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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，最严格的设置（较低的值）将生效。

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百分比”设置都输入值，最严格的设置（较低的值）将生效。

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 7.0 到 7.8，请使用注册表配置此设置；请参阅使用注册表配置 COM 端口和 LPT 端口重定向设置。

此设置指定在单个用户会话中使用 LPT 端口的打印作业允许使用的最大带宽 (Kbps)。

默认情况下，未指定最大值（零）。

如果为此设置输入一个值，并为 LPT 端口重定向带宽限制百分比设置输入一个值，则应用最严格的设置（较低的值）。

LPT 端口重定向带宽限制百分比

注意：对于 Virtual Delivery Agent 7.0 到 7.8，请使用注册表配置此设置；请参阅使用注册表配置 COM 端口和 LPT 端口重定向设置。

此设置指定在单个客户端会话中使用 LPT 端口的打印作业的带宽限制（占总会话带宽的百分比）。

默认情况下，未指定最大值（零）。

如果为此设置输入一个值，并为 LPT 端口重定向带宽限制设置输入一个值，则应用最严格的设置（较低的值）。

如果配置此设置，还必须配置总会话带宽限制设置，后者用于指定客户端会话可用的带宽总量。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 20 Mbps (20000 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，则应用最严格的设置（较低的值）。

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，则应用最严格的设置（较低的值）。

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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

双向内容重定向策略设置

January 21, 2022

双向内容重定向部分包含用于启用或禁用客户端到主机和主机到客户端 URL 重定向的策略设置。

服务器策略是在 Studio 中设置的。客户端策略在 Citrix Workspace 应用程序组策略对象管理模板中设置。

Citrix 为客户端到 URL 重定向提供主机到客户端重定向和本地应用程序访问。但是，我们建议您对加入域的 Windows 客户端使用双向内容重定向。

允许双向内容重定向

请将此策略设置为允许以启用服务器 (VDA) 与客户端之间的重定向。默认情况下，该策略设置为禁止。

使用允许重定向到客户端的 **URL** 策略配置用于 VDA 到客户端重定向的 URL 列表。

> 注意：
>
> 要允许重定向，必须在客户端上使用双向内容重定向策略设置此策略。

允许重定向到客户端的 **URL**

指定允许双向内容重定向时要在客户端上打开的 URL 列表。

分号 (;) 是分隔符。星号 (*) 可用作通配符。例如：

```
*.xyz.com;https://www.example.com
```

浏览器内容重定向策略设置

January 21, 2022

“浏览器内容重定向”部分包含用于配置此功能的策略设置。

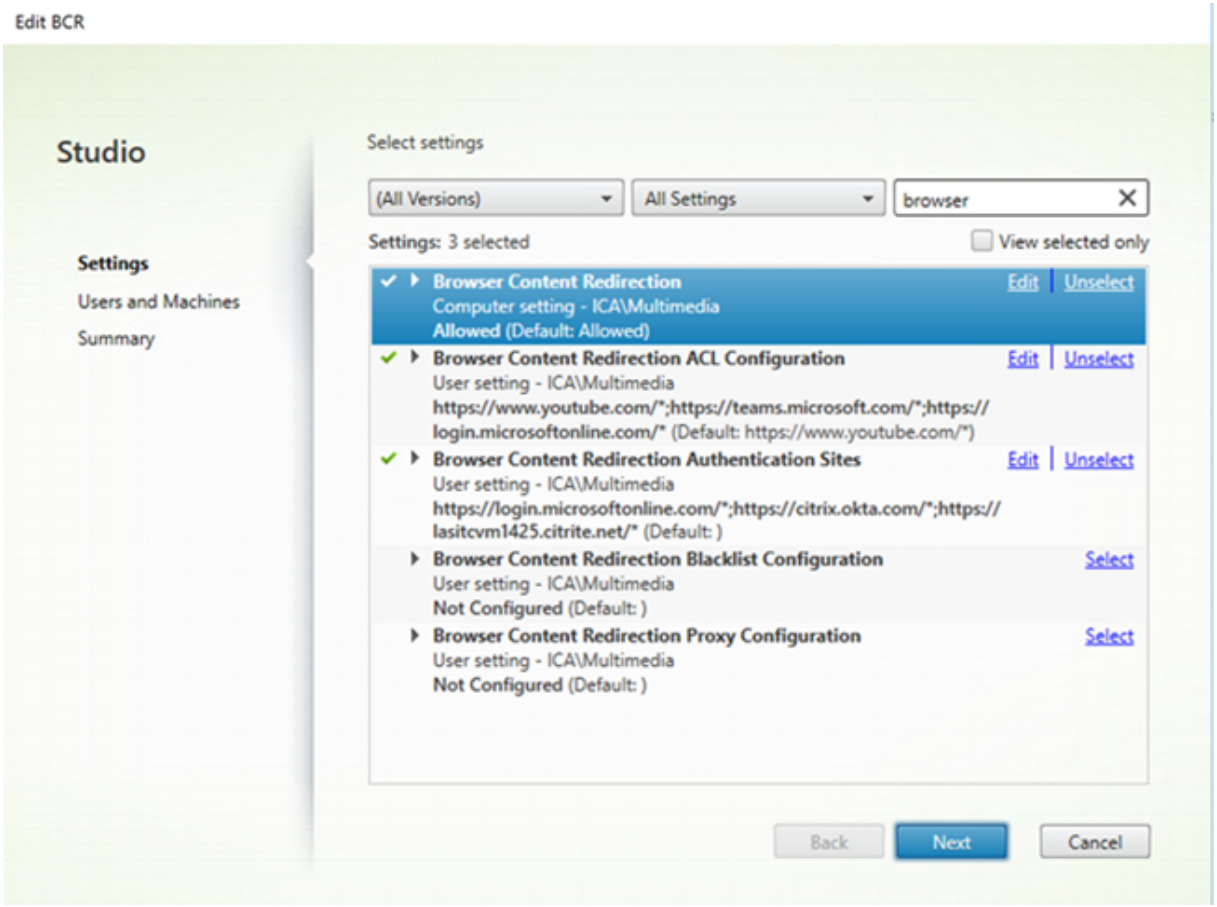
浏览器内容重定向功能用于控制并优化 Citrix Virtual Apps and Desktops 为向用户提供任何 Web 浏览器内容（例如 HTML5）的方式。只有浏览器中显示有内容的可见区域会进行重定向。

HTML5 视频重定向和浏览器内容重定向是相互独立的功能。此功能不需要设置 HTML5 视频重定向策略即可运行，但浏览器内容重定向将使用 Citrix HDX HTML5 视频重定向服务。有关详细信息，请参阅浏览器内容重定向。

策略设置：

以下策略设置适用于 Citrix Studio 中的浏览器内容重定向功能。可以在 VDA 上使用注册表项覆盖这些策略，但注册表项为可选。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



TLS 和浏览器内容重定向

可以使用浏览器内容重定向来重定向 HTTPS Web 站点。注入到这些 Web 站点的 JavaScript 必须与 VDA 上运行的 Citrix HDX HTML5 视频重定向服务 (WebSocketService.exe) 建立 TLS 连接。为了实现此重定向并维护 Web 页面的 TLS 完整性，Citrix HDX HTML5 视频重定向服务将在 VDA 上的证书存储中生成两个自定义证书。

HdxVideo.js 使用 Secure Web 套接字与 VDA 上运行的 WebSocketService.exe 进行通信。此过程在本地系统中运行，并执行 SSL 终止和用户会话映射。

WebSocketService.exe 在 127.0.0.1 端口 9001 上进行侦听。

浏览器内容重定向

默认情况下，Citrix Workspace 应用程序将尝试进行客户端提取和客户端呈现。如果客户端提取和客户端呈现失败，则尝试进行服务器端呈现。如果您同时启用了浏览器内容重定向代理配置策略，则 Citrix Workspace 应用程序将仅尝试进行服务器提取和客户端呈现。

默认情况下，此设置设为允许。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

浏览器内容重定向集成 **Windows** 社分验证支持设置

浏览器内容重定向启用使用协商方案进行身份验证的叠加。此增强功能提供了对与 VDA 位于同一域中且配置了集成 Windows 身份验证 (IWA) 的 Web 服务器的单点登录。

如果设置为允许，浏览器内容重定向叠加将使用用户的 VDA 凭据获取协商票证。然后，用户通过单点登录向 Web 服务器进行身份验证。

如果设置为禁止，浏览器内容重定向叠加不会请求 VDA 提供协商票证。用户使用基本身份验证方法向 Web 服务器进行身份验证，该方法要求用户在每次访问 Web 服务器时输入 VDA 凭据。

默认情况下，此设置为“禁止”。

浏览器内容重定向服务器提取 **Web** 代理身份验证设置

此设置通过下游 Web 代理路由来自叠加层的 HTTP 流量。下游 Web 代理通过协商身份验证方案使用 VDA 用户的域凭据对 HTTP 流量进行授权和身份验证。

必须使用“浏览器内容重定向代理配置”策略在 PAC 文件中为服务器提取模式配置浏览器内容重定向。在 PAC 脚本中，提供通过下游 Web 代理路由叠加流量的说明。然后将下游 Web 代理配置为通过协商身份验证方案对 VDA 用户进行身份验证。

如果设置为允许，Web 代理将以 407 协商质询进行响应，其中包含代理身份验证**:** 协商标题。然后，浏览器内容重定向将使用 VDA 用户的域凭据获取 Kerberos 服务票证，并将服务票证包含在对 Web 代理的后续请求中。

如果设置为禁止，浏览器内容重定向将代理叠加层与 Web 代理之间的所有 TCP 流量而不会产生干扰。叠加使用基本身份验证凭据或任何其他可用凭据向 Web 代理进行身份验证。

默认情况下，此设置为“禁止”。

浏览器内容重定向访问控制列表 **(ACL)** 策略设置

使用此设置可配置能够使用浏览器内容重定向或者被拒绝访问浏览器内容重定向的 URL 的访问控制列表 (ACL)。

获得授权的 URL 是指内容将重定向到客户端的允许列表中的 URL。

允许使用通配符 *，但在 URL 的协议或域地址部分中不允许使用此通配符。

允许：`http://www.xyz.com/index.html`、`https://www.xyz.com/*`、`http://www.xyz.com/*videos*`

不允许：`http://*.xyz.com/`

可以通过在 URL 中指定路径来实现更好的粒度。例如，如果指定 `https://www.xyz.com/sports/index.html`，则只重定向 index.html 页面。

默认情况下，此设置设为 `https://www.youtube.com/*`

有关详细信息，请参阅知识中心文章 CTX238236。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

浏览器内容重定向身份验证站点

可使用此设置来配置 URL 列表。通过使用浏览器内容重定向功能进行重定向的站点使用该列表对用户进行身份验证。此设置指定在离开允许列表中的 URL 时浏览器内容重定向保持活动状态（重定向）的 URL。

经典场景是依赖身份提供程序 (IdP) 进行身份验证的 Web 站点。例如，Web 站点 `www.xyz.com` 必须重定向到端点，但由第三方 IdP（如 Okta (`www.xyz.okta.com`)）处理身份验证部分。管理员使用浏览器内容重定向 ACL 配置策略将 `www.xyz.com` 添加到允许列表，然后使用浏览器内容重定向身份验证站点将 `www.xyz.okta.com` 添加到允许列表。

有关详细信息，请参阅知识中心文章 CTX238236。

浏览器内容重定向阻止列表设置

此设置与浏览器内容重定向 ACL 配置设置结合使用。如果 URL 存在于浏览器内容重定向 ACL 配置设置和阻止列表配置设置中，阻止列表配置将具有更高的优先级，并且不重定向 URL 的浏览器内容。

未经授权的 **URL**：指定浏览器内容不重定向到客户端，但在服务器上呈现的阻止列表中的 URL。

允许使用通配符 *，但在 URL 的协议或域地址部分中不允许使用此通配符。

允许：`http://www.xyz.com/index.html`、`https://www.xyz.com/*`、`http://www.xyz.com/*videos*`

不允许：`http://*.xyz.com/`

可以通过在 URL 中指定路径来实现更好的粒度。例如，如果指定 `https://www.xyz.com/sports/index.html`，阻止列表中只有 index.html。

浏览器内容重定向代理设置

此设置用于为 VDA 上的浏览器内容重定向的代理设置提供配置选项。如果已使用有效的代理地址和端口号、PAC/WPAD URL 或直接/透明设置启用此设置，Citrix Workspace 应用程序将仅尝试进行服务器提取和客户端呈现。

如果已禁用或未配置此设置并使用默认值，则 Citrix Workspace 应用程序将尝试进行客户端提取和客户端呈现。

默认情况下，此设置为“禁止”。

显式代理允许的模式：

```
http://\<hostname/ip address\>:\<port\>
```

示例：

```
http://proxy.example.citrix.com:80
http://10.10.10.10:8080
```

PAC/WPAD 文件允许的模式：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

`http://<hostname/ip address>:<port>/<path>/<Proxy.pac>`

示例：`http://wpad.myproxy.com:30/configuration/pac/Proxy.pac`

`https://<hostname/ip address>:<port>/<path>/<wpad.dat>`

示例：`http://10.10.10.10/configuration/pac/wpad.dat`

直接或透明代理允许的模式：

在策略文本框中键入单词 **DIRECT**。

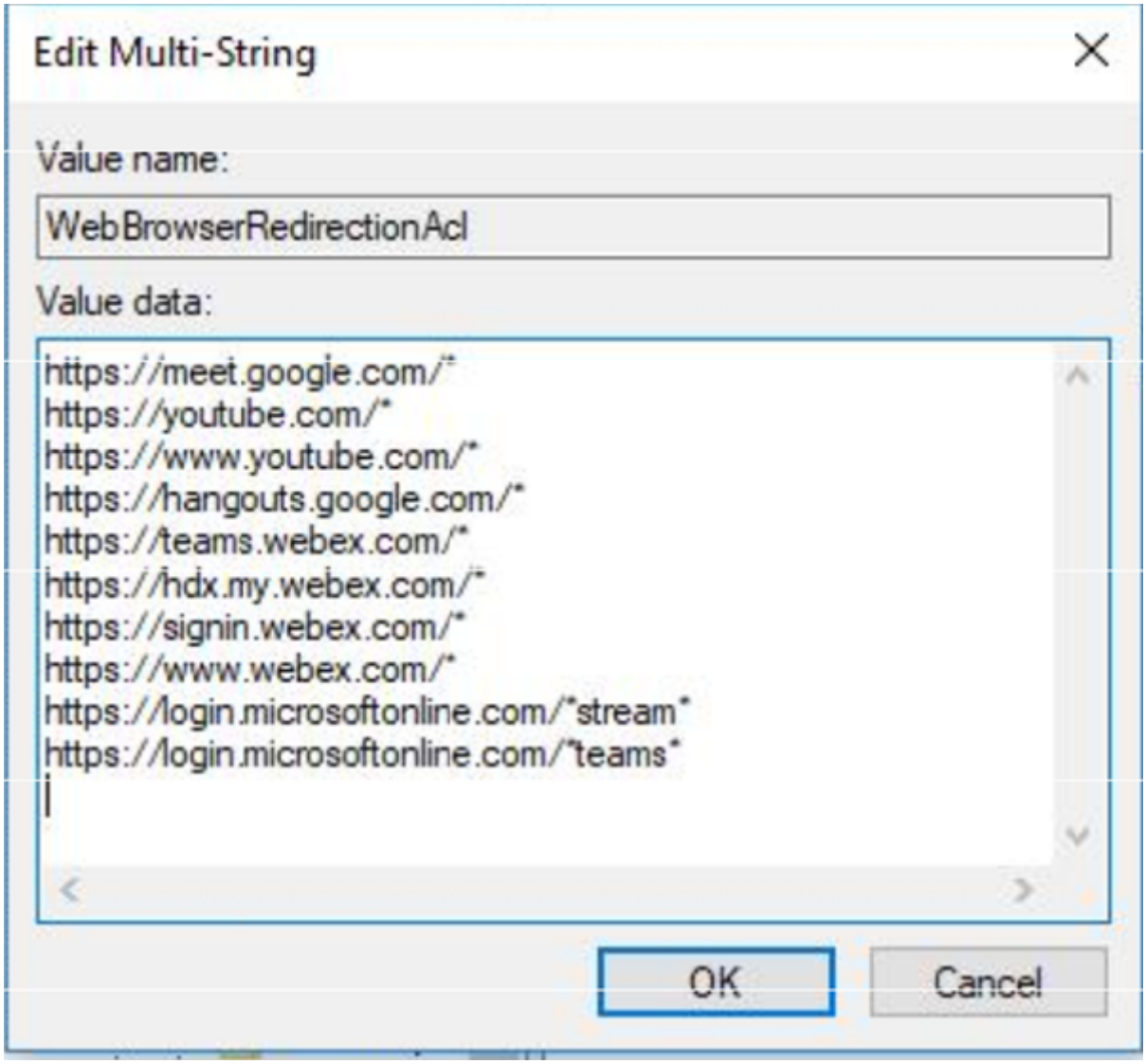
浏览器内容重定向注册表项覆盖

> 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。
>
> 用于策略设置的注册表覆盖选项：

`\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream`

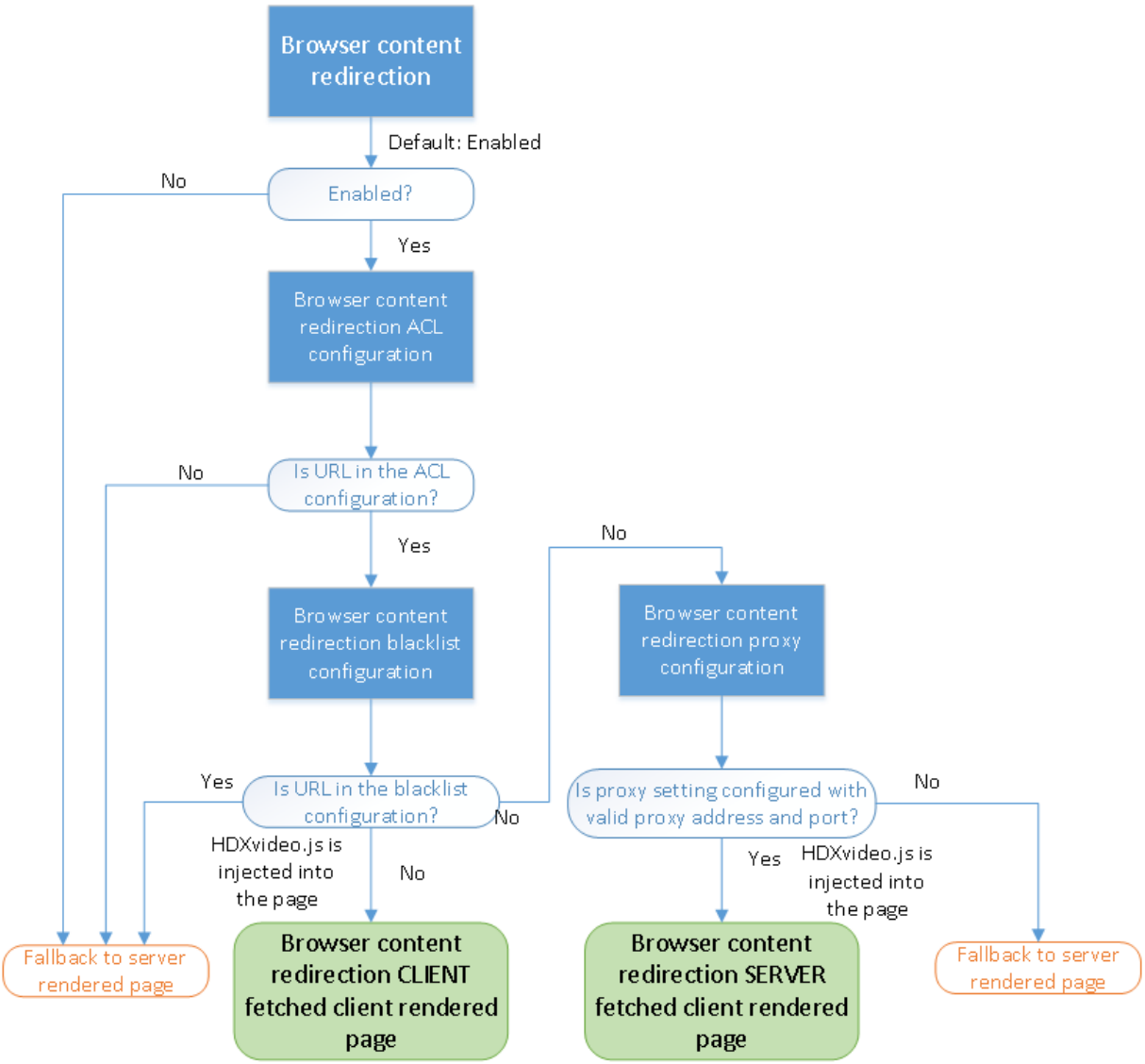
名称	类型	值
WebBrowserRedirection	DWORD	1 = 允许，0 = 禁止
WebBrowserRedirectionAcl	REG_MULTI_SZ	
WebBrowserRedirectionAuthenticationMethod	REG_MULTI_SZ	
WebBrowserRedirectionProxyAddress	REG_SZ	`http://myproxy.citrix.com:8080` 或 `http://10.10.10.10:8888`
WebBrowserRedirectionBlacklist	REG_MULTI_SZ	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

用于浏览器内容重定向的 **HDXVideo.js** 注入



HdxVideo.js 是使用浏览器内容重定向 Chrome 扩展程序或 Internet Explorer 浏览器帮助程序对象 (BHO) 在 Web 页面上注入的。BHO 是 Internet Explorer 的插件模型。它为浏览器 API 提供了挂钩，并可使插件访问页面的文档对象模型 (DOM) 以控制导航。

BHO 可决定是否在给定页面上注入 HdxVideo.js。此决策建立在上文流程图中所示的管理策略的基础之上。

在决定注入 JavaScript 并将浏览器内容重定向到客户端后，VDA 上 Internet Explorer 浏览器中的 Web 页面将被清空。将 **document.body.innerHTML** 设置为空将删除 VDA 上的 Web 页面的完整正文。此时，页面已准备好，可发送到客户端以显示在客户端上的叠加浏览器 (Hdxbrowser.exe) 中。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

客户端传感器策略设置

November 17, 2021

“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 Workspace 应用程序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：

- 确保启用了位置功能的应用程序不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 Workspace 应用程序不缓存位置数据。）
- 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，强制使用安全连接（例如，使用 TLS 或 VPN）。将 Citrix Workspace 应用程序连接到可信服务器。
- 注意征求使用定位服务方面的法律意见。

桌面 **UI** 策略设置

November 17, 2021

“桌面 UI”部分包含的策略设置可控制视觉效果（例如桌面墙纸、菜单动画以及拖放图像）以管理客户端连接占用的带宽。限制带宽使用量可以改善 WAN 上的应用程序性能。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 重要：
>
> 在此版本中，我们不支持旧图形模式和桌面组合重定向 (DCR)。仅为了在结合使用 XenApp 7.15 LTSR、XenDesktop 7.15 LTSR 和早期 VDA 版本与 Windows 7 和 Windows 2008 R2 时向后兼容而包括此策略。

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，禁用桌面组合重定向。

要取消选中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已禁用。

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。

默认值为“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。

要取消选中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。

如果此策略设置设为允许，并且启用了菜单动画 Microsoft 个人首选项设置，则会在桌面上启用菜单动画。

> 注意：
>
> 对菜单动画 Microsoft 个人首选项设置所做的更改会影响桌面。如果将桌面设置为在会话结束时放弃更改，启用了菜单动画的用户在后续会话中可能没有菜单动画。对于需要菜单动画的用户，请在桌面的主映像中启用

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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。

最终用户监视策略设置

November 17, 2021

“最终用户监控”部分包含用于测量会话流量的策略设置。

ICA 往返行程计算

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 往返行程计算间隔

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** 往返行程计算

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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

增强的桌面体验策略设置

November 17, 2021

“增强的桌面体验”策略设置在看起来像本地 Windows 7 桌面的服务器操作系统中运行会话。

默认情况下，此设置为允许。

如果虚拟桌面上存在具有 Windows Classic 主题的用户配置文件，此策略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。

如果在具有活动用户会话的虚拟桌面上禁用该策略，在 Windows 7 和 Windows Classic 桌面上这些会话的界面将不一致。为避免出现这一不一致性问题，请务必在更改此策略设置后重新启动虚拟桌面。然后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。客户端和服务器操作系统的配置文件有所差别。当用户在两种类型之间移动时，跨两种类型共享漫游配置文件可能会导致配置文件属性不一致。

文件重定向策略设置

November 17, 2021

“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，请务必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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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。

> 注意：
>
> 客户端驱动器重定向策略设置不适用于使用通用 USB 重定向映射到会话的驱动器。

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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 媒体服务器 (MMS)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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盘符。

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更改映射的客户端驱动器上的文件或文件夹。

默认情况下，可以更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，并设置为“允许”。

特殊文件夹重定向

此设置允许或阻止 Citrix Workspace 应用程序和 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 Workspace 应用程序指定的任何相关设置。

要定义哪些用户可以使用特殊文件夹重定向，请选择允许，并将此设置包括在对您希望具有此功能的用户执行过滤的策略中。此设置将覆盖所有其他特殊文件夹重定向设置。

由于特殊文件夹重定向必须与用户设备交互，因此，禁止用户访问文件或将文件保存到本地硬盘驱动器的策略设置，也会禁止用户使用特殊文件夹重定向。

将此设置添加到策略中时，请确保“客户端固定驱动器”设置存在，并设置为允许。

使用异步写入

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 WAN 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。如果出现这种未定义的状态，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。

我们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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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，并设置为“允许”。如果禁用此设置，将不执行异步写入。

图形策略设置

January 21, 2022

“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。

允许视觉无损压缩

此设置允许为图像使用视觉无损压缩，而不是真正无损的压缩。相比于真正无损的压缩，视觉无损功能可提高性能，但会产生视觉上不易察觉的轻微损失。此设置可更改“视觉质量设置”值的使用方式。

默认情况下，禁用此设置。

图形状态指示器

此设置将图形状态指示器配置为在用户会话中运行。此指示器允许用户查看正在使用的图形模式的详细信息，包括图形提供程序、编码器、硬件编码、图像质量、渐进式显示状态和无损文本。

默认情况下，图形状态指示器处于禁用状态。此设置将替代无损指示器。早期版本的 Citrix Virtual Apps and Desktops 则会启用无损指示器。

由于 **Microsoft** 免打扰时间而限制：

启用图形状态指示器后，用户首次登录 Citrix Virtual Apps and Desktops 时可能会出现问题。四个小时后，状态指示器图标将显示在通知区域中。

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。

指定会话的最大视频缓冲区大小 (KB)。指定一个介于 128 到 4,194,303 之间的量 (KB)。最大值 4,194,303 不会限制显示内存。默认情况下，显示内存为 65536 KB。如果为连接使用更高的颜色深度和分辨率，则需要更多内存。在传统图形模式下，如果达到内存限制，则显示质量会根据“显示模式降级首选项”设置的情况而降级。

对于需要更高颜色深度和分辨率的连接，可增大该限值。使用如下公式计算所需的最大内存：

内存深度 (字节) = (颜色深度 (bpp) / 8) x (垂直分辨率 (像素)) x (水平分辨率 (像素))。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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) x (600) x (800) = 1920000 字节，从而得出显示内存限制为 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

在以下情况下，此设置启用或禁用无缝窗口的显示：

- 窗口切换-
- 三维窗口切换
- 任务栏预览
- Windows 预览

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。
Windows 预览	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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。该设置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 - 不支持。仅限向后兼容

> 重要：
>
> 在此版本中，我们不支持旧图形模式和桌面组合重定向 (DCR)。仅为了在结合使用 XenApp 7.15 LTSR、XenDesktop 7.15 LTSR 和早期 VDA 版本与 Windows 7 和 Windows 2008 R2 时向后兼容而包括此策略。

此设置禁用丰富的图形体验。使用此设置可还原为旧版图形体验，降低了使用 WAN 或移动连接时占用的带宽。XenApp 和 XenDesktop 7.13 中引入的带宽降低功能导致此模式过时。

默认情况下，禁用此设置，并向用户提供丰富的图形体验。

旧图形模式在 Windows 7 和 Windows Server 2008 R2 VDA 中受支持。

旧图形模式在 Windows 8.x、10 或 Windows Server 2012、2012 R2 和 2016 中不受支持。

有关在 XenApp 和 XenDesktop 7.6 FP3 或更高版本中优化图形模式和策略的详细信息，请参阅 CTX202687。

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单会话操作系统 VDA（例如 Windows 8），此设置无影响。对于使用 WDDM 驱动程序的 Windows 多会话操作系统 VDA（例如 Windows Server 2012 R2），此设置可能会阻止用户连接到 VDA。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。

针对 **3D** 图形工作负载优化

此设置配置最适合图形密集型工作负载的相应默认设置。可为工作负载集中于图形密集型应用程序的用户启用此设置。仅在会话可以使用 GPU 的情况下应用此策略。显式覆盖由此策略设置的默认设置的其他任何设置具有更高的优先级。

默认情况下，禁止优化 3D 图形工作负载。

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。

此设置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。

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。选中针对整个屏幕时，视频编解码器将用作所有项的默认编解码器。选中针对主动变化的区域时，视频编解码器将用于屏幕上存在不断变化的区域，其他数据将使用静态图像压缩和位图缓存。视频解码在端点上不可用时，或者当您指定了不使用视频编解码器时，将同时使用静态图像压缩和位图缓存。选择偏好时使用时，系统会基于各种因素进行选择。结果可能会因版本而异，因为选择方法已得以增强。

选择偏好时使用可允许系统尽可能为当前场景选择适合的设置。

选择针对整个屏幕以针对改进用户体验和带宽使用情况进行优化，尤其是在大量使用服务器端呈现的视频和 3D 图形的情况下。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

选择针对主动变化的区域以针对改善视频性能（尤其是低带宽的性能）进行优化，同时维持静态和缓慢变化的内容的可扩展性。多显示器部署中支持此设置。

选择不使用视频编解码器以针对服务器 CPU 负载和改善不大量使用服务器端呈现的视频或其他图形密集型应用程序的情况进行优化。

默认设置为偏好时使用。

使用视频的硬件编码

此设置允许使用图形硬件（如果可用）并采用视频编解码器来压缩屏幕元素。如果此类硬件不可用，VDA 会回退到使用软件视频编解码器的基于 CPU 的编码。

此策略设置的默认选项为启用。

支持使用多个显示器。

任何支持视频解码的 Citrix Workspace 应用程序均可随硬件编码一起使用。

NVIDIA

对于 NVIDIA GRID GPU，适用于多会话操作系统和单会话操作系统的 VDA 支持硬件编码。

NVIDIA GPU 必须支持 NVENC 硬件编码。请参阅 NVIDIA 视频编解码器 SDK 获取受支持的 GPU 列表。

NVIDIA GRID 要求使用 3.1 或更高版本的驱动程序。NVIDIA Quadro 要求使用 362.56 或更高版本的驱动程序。Citrix 推荐使用 NVIDIA Release R361 分支版中的驱动程序。

无损文本与 NVENC 硬件编码不兼容。如果启用了无损文本，则无损文本优先于 NVENC 硬件编码。

支持针对主动变化的区域选择性地使用 H.264 硬件编解码器。

支持视觉无损 (YUV 4:4:4) 压缩。视觉无损（图形策略设置，允许视觉无损压缩）要求使用 Citrix Workspace 应用程序 1808 或更高版本或者 Citrix Receiver for Windows 4.5 或更高版本。

Intel

对于 Intel Iris Pro 图形处理器，适用于单会话操作系统和多会话操作系统的 VDA 支持硬件编码。

支持 Intel Broadwell 处理器系列及更高系列中的 Intel Iris Pro 图形处理器。Intel Remote Displays SDK 版本 1.0 是必需的，可以从 Intel Web 站点 Remote Displays SDK 进行下载。

仅当为整个屏幕设置了“视频编解码器”策略并禁用了针对 **3D** 图形工作负载优化时才支持无损文本。

不支持视觉无损 (YUV 4:4:4)。

Intel 编码器在最多有八个编码会话时（例如，使用八台显示器的一个用户或各使用一台显示器的八个用户）可提供良好的用户体验。如果需要的编码会话超过八个，请检查虚拟机连接的显示器数量。为了保持良好的用户体验，管理员可以决定按每个用户或每台计算机配置此策略设置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

AMD

对于 AMD，适用于单会话操作系统的 VDA 支持硬件编码。

AMD GPU 必须支持 RapidFire SDK。例如，AMD Radeon Pro 或 FirePro GPU。

为了使编码正常工作，请安装最新的 AMD 驱动程序。您可以 https://www.amd.com/en/support 从下载这些驱动程序。

无损文本与 AMD 硬件编码不兼容。如果启用了无损文本，则无损文本优先于 AMD 硬件编码。

支持针对主动变化的区域选择性地使用 H.264 硬件编解码器。

缓存策略设置

November 17, 2021

本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。

永久性缓存阈值

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。

此设置将位图缓存在用户设备的硬盘驱动器上，从而使之前会话中经常使用的大型图像可重复使用。

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

January 21, 2022

> 重要：
>
> 截至 Citrix Virtual Apps and Desktops 7 1903，不再支持 Framehawk。请改为使用启用了自适应传输的 Thinwire。

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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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，它还可以使用比其他图形模式更多的服务器资源和带宽。

默认情况下，禁用 Framehawk 显示通道。

Framehawk 显示通道端口范围

此策略设置指定 VDA 用于与用户设备交换 Framehawk 显示通道数据的 UDP 端口范围（格式为最低端口号, 最高端口号）。VDA 会尝试使用每个端口，从最低端口号开始，后面每次尝试都增加端口号。端口处理入站和出站通信。

默认情况下，端口范围为 3224,3324。

保持活动状态策略设置

November 17, 2021

“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 保持活动状态消息

此设置允许或禁止定期发送 ICA 保持活动状态消息。

默认情况下，不发送 ICA 保持活动状态消息。

启用此设置可防止中断的连接被断开连接。如果服务器检测不到活动，此设置可防止远程桌面服务 (RDS) 断开会话连接。服务器将每隔几秒钟发送一次保持活动状态消息，以检测会话是否处于活动状态。如果会话不再处于活动状态，服务器会将该会话标记为已断开连接。

ICA 保持活动状态在使用会话可靠性时将无效。请仅为不使用会话可靠性的连接配置 ICA 保持活动状态。

相关策略设置：会话可靠性连接。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

本地应用程序访问策略设置

November 17, 2021

“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。

如果将允许本地应用程序访问策略设置设为启用，则不支持浏览器内容重定向，且客户端通知区域的电池状态不会显示在桌面会话中。

默认情况下，允许本地应用程序访问处于禁用状态。

URL 重定向阻止列表

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。这些 Web 站点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 重定向允许列表

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

November 17, 2021

“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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

启动经过触控优化的桌面

此设置已禁用，不适用于 Windows 10 或 Windows Server 2016 计算机。

此设置通过允许或禁止使用为平板电脑设备优化的触控友好界面，控制 Citrix Workspace 应用程序的整体界面行为。

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，用户可以将适用于 iOS 的 Citrix Workspace 应用程序会话设置更改为使用 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

January 21, 2022

“多媒体”部分包含用于管理用户会话中的流 HTML5 和 Windows 音频和视频的策略设置。

> 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。

多媒体策略

默认情况下，在 Delivery Controller 上设置的所有多媒体策略都存储在以下注册表项中：

计算机策略：

HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies

用户策略：

HKEY_LOCAL_MACHINE\Software\Policies\Citrix{用户会话 ID}\User\MultimediaPolicies

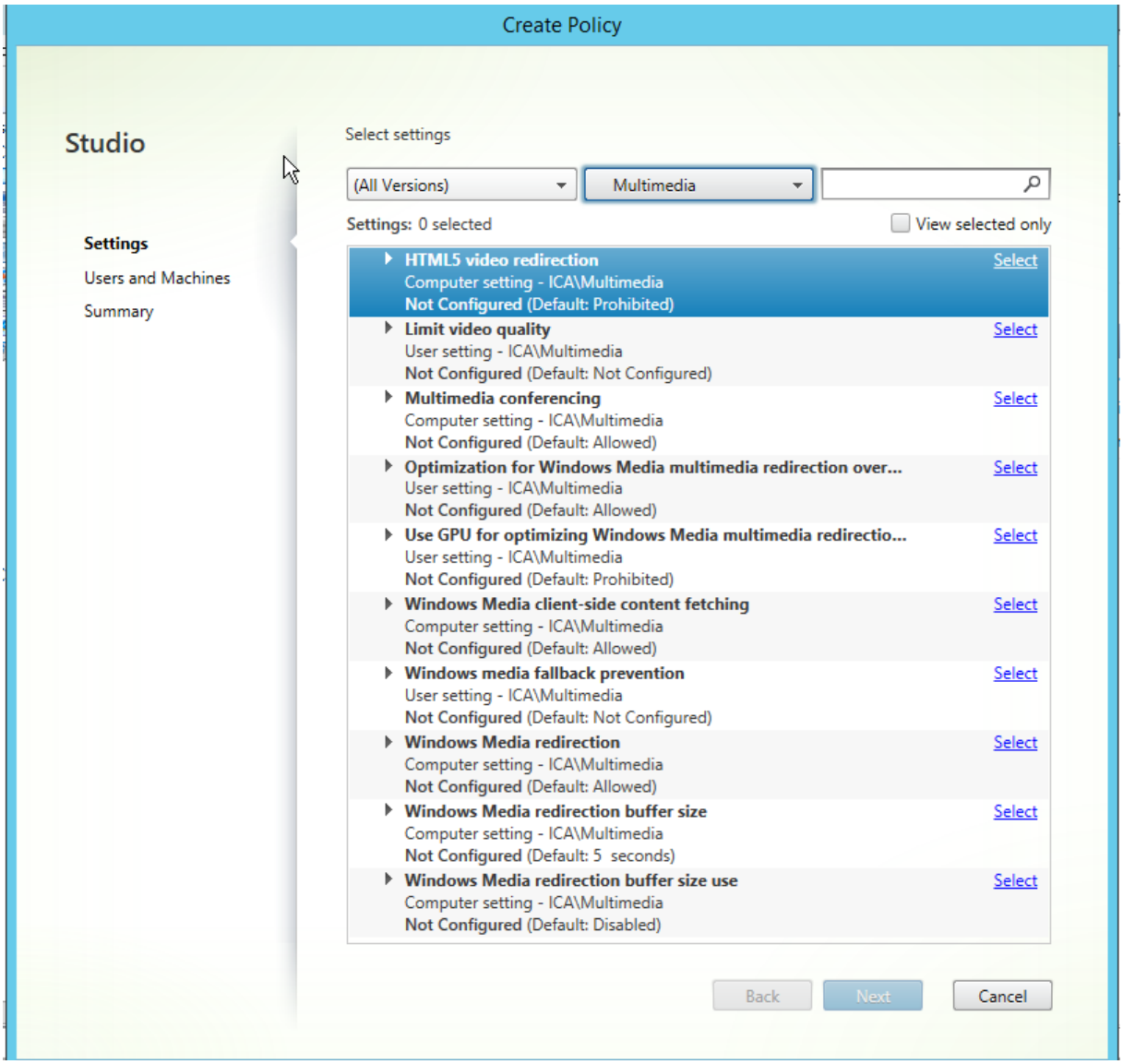
要查找当前的用户会话 ID，请在 Windows 命令行中发出 **qwinsta** 命令。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

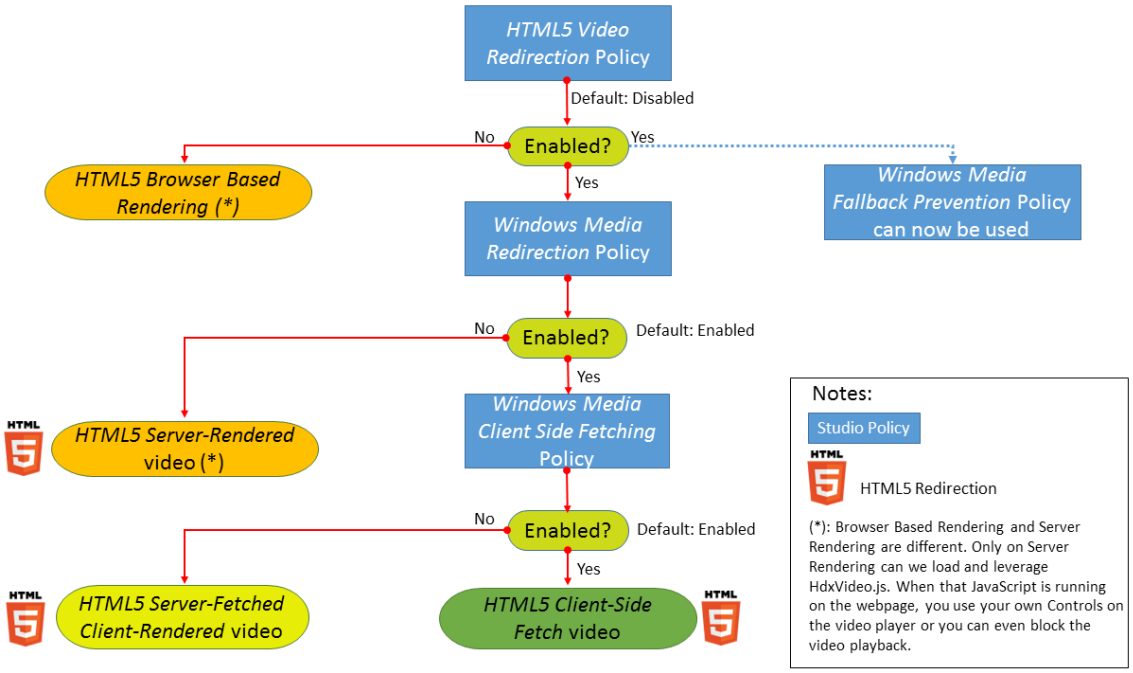
HTML5 视频重定向

控制和优化 Citrix Virtual Apps and Desktops 服务器向用户交付 HTML5 多媒体 Web 内容的方式。

默认情况下，禁用此设置。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



在此版本中，此功能仅用于受控 Web 页面。它要求向提供 HTML5 多媒体内容（例如，内部培训站点上的视频）的 Web 页面添加 JavaScript。

配置 HTML5 视频重定向：

1. 将文件 **HdxVideo.js** 从 VDA 安装上的%Program Files%/Citrix/ICA Service/HTML5 Video Redirection 复制到您的内部 Web 页面位置。
2. 将此行插入您的 Web 页面（如果您的 Web 页面有其他脚本，请将 **HdxVideo.js** 放在那些脚本之前）：
   ```
   <script src="HdxVideo.js"type="text/javascript"\></script>
   ```

注意：如果 HdxVideo.js 与您的 Web 页面不在同一位置，请使用 **src** 属性指定其完整路径。

如果未将 JavaScript 添加到您的受控 Web 页面且用户播放 HTML5 视频，则 Citrix Virtual Apps and Desktops 将默认进行服务器端呈现。

为了能够重定向 HTML5 视频，请允许 ***Windows Media*** 重定向。要进行服务器提取客户端呈现，必需此策略，要进行客户端提取，需要此策略（进而还要求允许 *Windows Media* 客户端内容提取）。

Microsoft Edge 不支持此功能。

HdxVideo.js 会将浏览器 HTML5 播放器控件替换为自己的控件。要检查 HTML5 视频重定向策略是否在某个特定 Web 站点上生效，请将播放器控件与禁止 **HTML5** 视频重定向策略的情况进行比较：

（允许该策略时的 Citrix 自定义控件）

（禁止或未配置该策略时的原始 Web 页面控件）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

支持以下视频控制功能：

- 播放
- 暂停
- 搜寻
- 重复
- 音频
- 全屏

您可以在 https://www.citrix.com/virtualization/hdx/html5-redirect.html 上查看 HTML5 视频重定向测试页面。

TLS、HTML5 视频重定向和浏览器内容重定向

可以使用 HTML5 视频重定向从 HTTPS Web 站点重定向视频，或者使用浏览器内容重定向重定向整个 Web 站点。注入到这些 Web 站点的 JavaScript 必须与 VDA 上运行的 Citrix HDX HTML5 视频重定向服务 (WebSocketService.exe) 建立 TLS 连接。为了实现此重定向并维护 Web 页面的 TLS 完整性，Citrix HDX HTML5 视频重定向服务将在 VDA 上的证书存储中生成两个自定义证书。

HdxVideo.js 使用安全的 WebSocket 与 VDA 上运行的 WebSocketService.exe 进行通信。此过程以本地系统帐户运行，并执行 SSL 终止和用户会话映射。

WebSocketService.exe 在 127.0.0.1 端口 9001 上进行侦听。

限制视频质量

此设置仅适用于 Windows Media，而不适用于 HTML5。它要求您启用优化通过 **WAN** 进行的 **Windows Media** 多媒体重定向。

此设置指定 HDX 连接允许使用的最大视频质量级别。配置后，最大视频质量将限制为指定值，确保在环境中保持多媒体服务质量 (QoS)。

默认情况下未配置此设置。

要限制允许使用的最大视频质量级别，请选择以下任一选项：

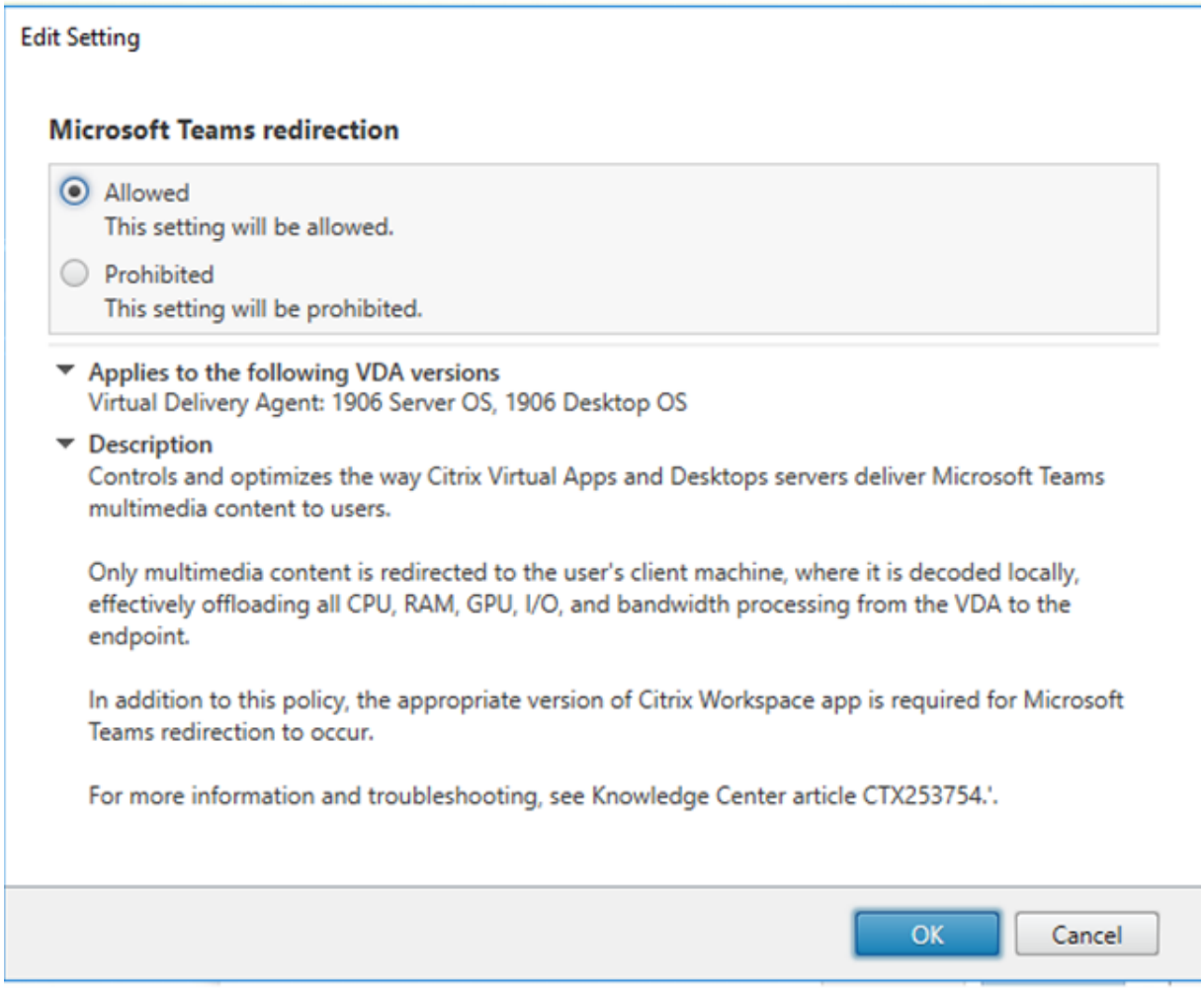
- 1080p/8.5mbps
- 720p/4.0mbps
- 480p/720kbps
- 380p/400kbps
- 240p/200kbps

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

在同一台服务器上同时播放多个视频会消耗大量资源，并且会影响服务器的可扩展性。

Microsoft Teams 重定向

此设置启用基于 HDX 技术的 Microsoft Teams 优化。



如果启用了此策略，并且您使用的是 Citrix Workspace 应用程序的受支持版本，则在 VDA 上将此注册表项设置为 **1**。Microsoft Teams 应用程序读取要在 VDI 模式下加载的密钥。

请注意，不需要手动设置注册表项。

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

名称：MSTeamsRedirSupport

值：DWORD（1 - 开，0 - 关）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 如果使用的是版本 1906.2 或更高版本的 VDA 与较旧的 Controller 版本（例如，版本 7.15）（Studio 中没有可用的策略），则默认情况下，HDX 优化在 VDA 中处于启用状态。如果 Workspace 应用程序版本为 1907 或更高版本，Teams 将在优化模式下启动。有关混合 7.15 LTSR Controller 和 CR VDA 时的注意事项的信息，请参阅知识中心文章 CTX205549。
>
> 在这种情况下，要为特定用户禁用此功能，可以使用组策略将登录脚本应用到用户的组织单位来覆盖注册表设置。

默认情况下，启用 Microsoft Teams 重定向。

多媒体会议

此设置允许或阻止视频会议应用程序使用优化的网络摄像机重定向技术。

默认情况下，允许视频会议支持。

将此设置添加到某个策略时，请确保 Windows Media 重定向设置存在，并且设置为允许（默认设置）。

使用多媒体会议时，请确保满足以下条件：

- 在客户端上安装了制造商为用于多媒体会议的网络摄像机提供的驱动程序。
- 先将网络摄像机连接到用户设备，然后再启动视频会议会话。服务器在任何给定的时间只使用一个已安装的网络摄像机。如果用户设备上安装了多个网络摄像机，服务器会依次尝试使用每个网络摄像机，直至成功创建视频会议会话。

使用通用 USB 重定向对网络摄像机进行重定向时，不需要此策略。在这种情况下，请在 VDA 上安装网络摄像机驱动程序。

优化通过 **WAN** 进行的 **Windows Media** 多媒体重定向

此设置仅适用于 Windows Media，而不适用于 HTML5。该设置支持实时多媒体代码转换，允许在状况不佳的网络中通过流技术将音频和视频媒体推送到移动设备，并利用改善通过 WAN 交付 Windows Media 内容的方式增强了用户体验。

默认情况下，已优化通过 WAN 的 Windows Media 内容交付。

将此设置添加到策略时，请确保 **Windows Media** 重定向设置存在，且设置为允许。

启用此设置后，将根据需要自动部署实时多媒体代码转换以启用媒体流，因此即使在恶劣的网络条件下也可以提供无缝用户体验。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用 **GPU** 优化通过 **WAN** 进行的 **Windows Media** 多媒体重定向

此设置仅适用于 Windows Media，并支持在 Virtual Delivery Agent (VDA) 上的图形处理器 (GPU) 中执行实时多媒体代码转换。这会改善服务器可扩展性。仅在 VDA 具有支持硬件加速的 GPU 时，GPU 代码转换才可用。否则，代码转换将回退到 CPU。

注意：只有 NVIDIA GPU 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“优化通过 WAN 进行的 Windows Media 多媒体重定向”设置存在，且设置为允许。

Windows Media 回退预防

此设置适用于浏览器内容重定向、HTML5 和 Windows Media。为使其支持 HTML5，请将 **HTML5** 视频重定向策略设置为允许。

管理员可以使用 Windows Media 回退预防策略设置指定向用户交付流内容时尝试使用的方法。

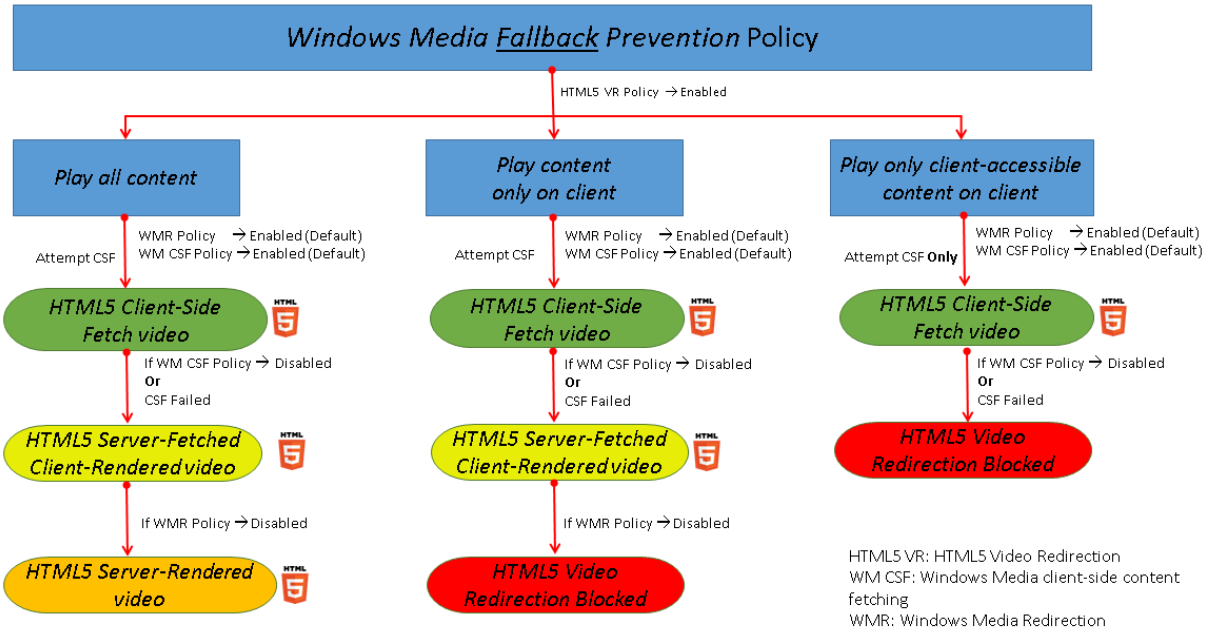
默认情况下未配置此设置。该设置设为“未配置”时，行为与播放所有内容相同。

要配置此设置，请选择以下选项之一：

- 播放所有内容。尝试执行客户端内容提取，然后执行 Windows Media 重定向。如果不成功，则在服务器上播放内容。
- 仅在客户端上播放所有内容。尝试执行客户端提取，然后执行 Windows Media 重定向。如果不成功，则不播放内容。
- 仅在客户端上播放客户端可访问的内容。仅尝试执行客户端提取。如果不成功，则不播放内容。

内容不播放时，播放器窗口会显示错误消息“由于缺少资源，因此公司阻止了该视频”（默认持续时间为 5 秒）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



可以通过 VDA 上的以下注册表项自定义此错误消息的持续时间。如果该注册表项不存在，持续时间将默认为 5 秒。

注册表路径因 VDA 的体系结构而异：

\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream

或

\HKLM\SOFTWARE\Citrix\HdxMediastream

注册表项：

名称：VideoLoadManagementErrDuration

类型：DWORD

范围： 1 - 最大 DWORD 限制（默认值 = 5）

单位：秒

Windows Media 客户端内容提取

此设置适用于 HTML5 和 Windows Media。该设置支持用户设备能够通过流技术直接从 Internet 或 Intranet 上的源提供程序推送多媒体文件，而非通过 XenApp 或 XenDesktop 主机服务器推送。

默认情况下，此设置设为允许。允许此设置后，可将对媒体的任何处理过程从主机服务器转到用户设备，提高了网络使用和服务器可扩展性。此外，还不需要在用户设备上安装 Microsoft DirectShow 或媒体基础等高级多媒体框架。用户设备只需要从 URL 播放文件的能力

将此设置添加到策略时，请确保 **Windows Media** 重定向设置存在，且设置为允许。如果禁用 **Windows Media** 重定向，也会禁用通过流技术将多媒体文件直接从源提供程序推送到用户设备。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Windows Media 重定向

此设置适用于 HTML5 和 Windows Media，并可控制和优化服务器向用户交付流音频和视频的方式。

默认情况下，此设置设为允许。对于 HTML5，如果策略 **HTML5** 视频重定向为禁止，此设置将无法生效。

允许此设置后，可将服务器上呈现的音频和视频质量提高到一个级别，可与用户设备上本地播放的音频和视频质量相媲美。服务器会将多媒体以原始压缩格式通过流技术推送到客户端，并允许用户设备解压缩和呈现该媒体。

Windows Media 重定向可优化使用编解码器编码的多媒体文件，这些编解码器遵循 Microsoft DirectShow、DirectX 媒体对象 (DMO) 和媒体基础标准。要播放给定的多媒体文件，用户设备上必须存在与多媒体文件的编码格式兼容的编解码器。

默认情况下，在 Citrix Workspace 应用程序上音频处于禁用状态。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 Workspace 应用程序界面上自行打开音频的权限。

仅当使用 Windows Media 重定向播放媒体的效果比使用基本 ICA 压缩和常规音频所呈现的效果差时，才选择已禁止。这种情况很少见，但在带宽较低的情况下可能会发生。例如，当播放关键帧的频率较低低的媒体时。

Windows Media 重定向缓冲区大小

此设置是一个旧设置，不适用于 HTML5。

此设置为多媒体加速指定 1 到 10 秒的缓冲区大小。

默认情况下，缓冲区大小为 5 秒。

Windows Media 重定向缓冲区大小的使用

此设置是一个旧设置，不适用于 HTML5。

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

January 21, 2022

“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 连接的服务质量优先级顺序。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 如果启用“多流连接”策略，则不支持 MTU 发现。

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，允许在服务器上通过 UDP 传输音频。

启用后，此设置在服务器上打开一个 UDP 端口以支持配置为使用“通过 UDP 实时传输音频”的所有连接。

音频 **UDP** 端口范围

此设置指定 Virtual Delivery Agent (VDA) 用于与用户设备交换音频数据包数据的端口号范围（最小端口号, 最大端口号）。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，也无法更改其优先级。

配置此设置时，请重新启动服务器。只有启用了多流计算机设置策略设置时，此设置才会生效。

多流计算机设置

此设置在服务器上启用或禁用“多流”功能。

默认情况下，禁用“多流”功能。如果使用 Citrix SD-WAN 或第三方路由器实现所需的服务质量，请配置多流计算机策略。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

如果启用“多流”，则不支持 MTU 发现（自适应传输的一项功能）。

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。如果使用 Citrix SD-WAN 或第三方路由器实现所需的服务质量，请配置多流用户设置。

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。

多流虚拟通道分配设置

此设置指定多流使用过程中虚拟通道要分配到的 ICA 流。

如果未配置这些设置，虚拟通道将保留在其默认流中。要将虚拟通道分配给 ICA 流，请从虚拟通道名称旁边的流编号列表中选择所需的流编号（0、1、2、3）。

如果环境中存在正在使用的自定义虚拟通道，请单击添加，在虚拟通道下的文本框中指定虚拟通道名称，然后从其旁边的流编号 列表中选择所需的流编号。指定的名称必须是实际的虚拟通道名称，不能是友好名称。例如，请指定 CTXSBR，而非指定 Citrix Browser Acceleration。

仅当您启用了多流计算机设置时，这些设置才能生效。

默认情况下，虚拟通道及其流分配如下：

- AppFlow：2
- 音频：0
- 浏览器内容重定向：2
- 客户端 COM 端口映射：3
- 客户端驱动器映射：2
- 客户端打印机映射：3
- 剪贴板：2
- CTXDND：1（注意：这支持在 Citrix 会话与本地端点之间拖放文件，请参阅 Citrix Virtual Apps and Desktops 7 2012 新增功能

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- DVC 插件（静态 VC 名称基于 DVC 插件友好名称自动生成，或者管理员进行分配）：2
- 最终用户体验监视：1
- 文件传输 (HTML5 Receiver)：2
- 通用数据传输：2
- ICA 控制：1
- 输入法编辑器：1
- 旧版客户端打印机映射 (COM1)：1、3
- 旧版客户端打印机映射 (COM2)：2、3
- 旧版客户端打印机映射 (LPT1)：1、3
- 旧版客户端打印机映射 (LPT2)：2、3
- 许可证管理：1
- Microsoft Teams/WebRTC 重定向：1
- 移动 Receiver：1
- 多点触控：1
- 端口转发：2
- 远程音频和视频扩展 (RAVE)：2
- 无缝（透明窗口集成）：1
- 传感器和位置：1
- 智能卡：1
- Thinwire 图形：1
- 透明 UI 集成/登录状态：2
- TWAIN 重定向：2
- USB：2
- 零延迟字体和键盘：2
- 零延迟数据通道：2

有关虚拟通道分配和优先级的详细信息，请参阅知识中心文章 CTX131001。

端口重定向策略设置

January 21, 2022

端口重定向部分包含用于客户端 LPT 和 COM 端口映射的策略设置。

对于 **7.0** 之前的 Virtual Delivery Agent 版本，请使用以下策略设置来配置端口重定向。对于 VDA 版本 **7.0** 至 **7.8**，请使用注册表来配置这些设置；请参阅使用注册表配置 COM 端口和 LPT 端口重定向设置。对于 VDA **7.9** 版本，请使用以下策略设置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

自动连接客户端 **COM** 端口

此设置启用或禁用用户登录到站点时用户设备上 COM 端口的自动连接。

默认情况下，不自动连接客户端 COM 端口。

自动连接客户端 **LPT** 端口

此设置启用或禁用用户登录到站点时用户设备上 LPT 端口的自动连接。

默认情况下，不自动连接客户端 LPT 端口。

客户端 **COM** 端口重定向

此设置允许或阻止访问用户设备上的 COM 端口。

默认情况下，禁止 COM 端口重定向。

下列策略设置为相关设置：

- COM 端口重定向带宽限制
- COM 端口重定向带宽限制百分比

客户端 **LPT** 端口重定向

此设置允许或阻止访问用户设备上的 LPT 端口。

默认情况下，禁止 LPT 端口重定向。

只有将打印作业发送至 LPT 端口（而非发送至用户设备上的打印对象）的旧版应用程序才可使用 LPT 端口。目前大多数应用程序都可将打印作业发送至打印机对象。只有用于托管打印至 LPT 端口的旧版应用程序的服务器，才有必要使用此策略设置。

请注意，虽然客户端 COM 端口重定向是双向的，但是在 ICA 会话中仅会输出 LPT 端口，并重定向到 \\client\LPT1 和 \\client\LPT2。

下列策略设置为相关设置：

- LPT 端口重定向带宽限制
- LPT 端口重定向带宽限制百分比

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

打印策略设置

November 17, 2021

“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 Server 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 **Printer assignments**（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打印机，请选择“不调整”。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Server 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。在 ICA/HDX 会话内部，Citrix 打印管理器服务 (CpSvc.exe) 在会话登录期间为在会话打印机策略设置中指定的每台网络打印机创建网络打印机连接。它会在会话注销期间删除打印机。默认情况下，不指定任何打印机。

在会话打印机策略设置中，网络打印机可以驻留在 Windows 打印服务器或 Citrix 通用打印服务器上。

- **Windows** 打印服务器：共享一个或多个网络打印机。此服务器还具有使用网络打印机所需的本机打印机驱动程序。
- 通用打印服务器：安装了 Citrix 通用打印服务器软件的 Windows 打印服务器。

使用 Windows 打印服务器时，Citrix 打印管理器服务将使用本机打印机驱动程序创建网络打印机连接。Citrix Virtual Apps 服务器必须安装本机打印机驱动程序。

使用 Citrix 通用打印服务器时，Citrix 打印管理器服务将使用本机打印机驱动程序、Citrix 通用打印机驱动程序或 Citrix 通用 XPS 打印机驱动程序创建网络打印机连接。您使用的驱动程序由“通用打印驱动程序用法”策略设置进行控制。

所有 Windows 打印机驱动程序当前都属于 v3 或 v4 驱动程序版本。有关详细信息，请参阅支持 Microsoft V3 和 V4 打印机驱动程序体系结构。

要添加会话打印机并验证其是否显示在会话中，请完成以下过程：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. 在 Citrix Studio 中，导航到策略选项卡。
2. 在编辑策略对话框中启用会话打印策略。
3. 在策略中，添加会话打印机。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。会话打印机必须显示在列表中。
4. 设置策略后，已发布的应用程序可能不会显示会话打印机。由于 Citrix Virtual Apps 服务器缺少打印机驱动程序，或者策略已创建但未启用，可能会出现此问题。

   > 注意：
   >
   > 如果 Citrix Virtual Apps 服务器上尚未安装打印机驱动程序，您可能会遇到会话打印机中最常见的错误，即管理员忘记在 Citrix Virtual Apps 服务器上安装打印机驱动程序。

5. 启动已发布的桌面，并在设备和打印机 **>** 控制面板中手动添加会话打印机。
6. 如果此操作失败，请调查 Citrix Virtual Apps 服务器与打印服务器之间的通信。请考虑使用 RDP 运行测试。

等待创建打印机

以不同的方式启用此功能，具体取决于其适用于 Citrix Virtual Desktops 还是 Citrix Virtual Apps。使用 Delivery Controller 上的策略在 Citrix Virtual Desktops 上启用此功能。使用 Delivery Controller 上的 PowerShell cmdlet 在 Citrix Virtual Apps 上启用此功能。

等待创建打印机（服务器桌面）：

此设置允许连接到会话时出现延迟，以便可以自动创建客户端重定向的打印机。

默认情况下不发生连接延迟。

等待创建打印机 **(Citrix Virtual Apps)**：

设置以下 PowerShell cmdlet 将允许连接到在服务器桌面上创建的虚拟应用程序时出现延迟，以便可以自动创建客户端重定向的打印机。

```
Set-BrokerApplication -Name <VirualAppName> -WaitForPrinterCreation
$true
```

默认情况下不发生连接延迟。

客户端打印机策略设置

November 17, 2021

“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）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

自动创建客户端打印机

此设置指定自动创建的客户端打印机。此设置可覆盖默认的客户端打印机自动创建设置。

默认情况下，所有客户端打印机都是自动创建的。

仅当客户端打印机重定向设置存在，且设置为允许时，此设置才能生效。

将此设置添加到策略时，请选择一个选项：

- 自动创建所有客户端打印机可在用户设备上自动创建所有打印机。
- 仅自动创建客户端的默认打印机仅自动创建选择作为用户设备上的默认打印机的打印机。
- 仅自动创建本地 **(**非网络**)** 客户端打印机将仅自动创建通过 LPT、COM、USB、TCP/IP 或其他本地端口直接连接到用户设备的打印机。
- 不自动创建客户端打印机在用户登录时关闭所有客户端打印机的自动创建功能。选择此选项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

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：

- 通用打印驱动程序用法
- 通用驱动程序优先级

自动创建 **PDF** 通用打印机

此设置为使用适用于 Windows 的 Citrix Workspace 应用程序（从 VDA 7.19 开始）、适用于 HTML5 的 Citrix Workspace 应用程序或适用于 Chrome 的 Citrix Workspace 应用程序的会话启用或禁用 Citrix PDF 打印机的自动创建。

默认情况下，不会自动创建 Citrix PDF 打印机。

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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

选择旧版打印机名称以使用旧式客户端打印机名称，并保留与产品的 XenApp 和 XenDesktop 版本中存在的旧版打印机名称的向后兼容性。您可以将此选项与产品的当前 Citrix Virtual Apps and Desktops 版本结合使用。旧版打印机名称示例：“Client/clientname#/HPLaserJet 4”。此选项不够安全。

在从适用于 HTML5 的 Citrix Workspace 应用程序启动的会话中使用 Citrix PDF 打印机时，请将客户端打印机名称设置设为默认设置或选择标准打印机名称。如果选择旧版打印机名称，则适用于 HTML5 的 Citrix Workspace 应用程序不支持“Citrix PDF 打印机”选项。

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。

此设置配置为从自动创建的客户端打印机列表中排除 Microsoft OneNote 和 XPS Document Writer。

定义驱动程序替代规则时，可以允许或禁止使用指定的驱动程序创建打印机。此外，可以允许创建的打印机仅使用通用打印驱动程序。驱动程序替换将覆盖或映射用户设备提供的打印机驱动程序名称，从而替换服务器上的等效驱动程序。这样可使服务器应用程序有权访问与服务器具有相同驱动程序，但驱动程序名称不同的客户端打印机。

可以添加驱动程序映射，编辑现有映射，覆盖映射的自定义设置，删除映射或更改驱动程序条目在列表中的顺序。添加映射时，请输入客户端打印机驱动程序名称，然后选择要替换的服务器驱动程序。

打印机属性保留

此设置指定是否存储打印机属性以及打印机属性的存储位置。

默认情况下，系统会决定是将打印机属性存储在用户设备上（如果有），还是存储在用户配置文件中。

将此设置添加到策略时，请选择一个选项：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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）。Citrix Virtual Apps 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。

Citrix PDF 通用打印机驱动程序

通过 Citrix PDF 通用打印机驱动程序，用户可以打印使用托管应用程序或使用 Citrix Virtual Apps and Desktops 提供的虚拟桌面上运行的应用程序打开的文档。当用户选择 **Citrix PDF** 打印机选项时，驱动程序会将该文件转换为 PDF 并将该 PDF 传输至本地设备。随后 PDF 会打开以从本地连接的打印机进行查看和打印。PDF 是 Citrix 通用打印支持的格式之一（EMF 和 XPS 也是）。
可以使用 Citrix 策略启用、配置 PDF 打印机以及将其设置为默认值。适用于 Windows、Chrome 和 HTML5 的 Citrix Workspace 应用程序用户可使用 **Citrix PDF** 打印机选项。

> 注意：
>
> Windows 端点需要 PDF 查看器。客户端必须具有在 Windows 上注册了文件类型关联的应用程序，才能打开 PDF 文件。

驱动程序策略设置

November 17, 2021

“驱动程序”部分包含与打印机驱动程序有关的策略设置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

自动安装现成的打印机驱动程序

> 注意
>
> 在此版本中，此策略不支持 VDA。

此设置启用或禁用从 Windows 现成驱动程序集或从使用 pnputil.exe /a 在主机上暂存的驱动程序软件包来自动安装打印机驱动程序。

默认情况下，会根据需要安装这些驱动程序。

通用驱动程序优先级

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。

通用打印驱动程序用法

此设置指定何时使用通用打印。

默认情况下，仅当请求的驱动程序不可用时才使用通用打印。

通用打印使用一般打印机驱动程序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机计算机上管理驱动程序的负担。通用打印驱动程序的可用性取决于用户设备、主机和打印服务器软件的功能。在某些配置中，通用打印可能不可用。

将此设置添加到策略时，请选择一个选项：

- 仅使用特定于打印机型号的驱动程序指定客户端打印机仅使用在登录时自动创建的特定于打印机型号的标准驱动程序。如果请求的驱动程序不可用，将无法自动创建客户端打印机。
- 仅使用通用打印指定不使用特定于型号的标准驱动程序。仅使用通用打印驱动程序创建打印机。
- 仅当请求的驱动程序不可用时才使用通用打印使用标准的特定于打印机型号的驱动程序来创建打印机（如果这些驱动程序可用）。如果该驱动程序在服务器上不可用，则使用合适的通用驱动程序自动创建客户端打印机。
- 仅当通用打印不可用时才使用打印机型号专用的驱动程序在通用打印驱动程序可用时将使用此驱动程序如果该驱动程序在服务器上不可用，则使用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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

通用打印服务器策略设置

November 17, 2021

“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。

SSL 密码套件

此设置指定通用打印客户端用于加密打印数据流 (CGP) 连接的一组 SSL/TLS 密码套件。

要控制通用打印客户端用于加密的打印 Web 服务 (HTTPS/SOAP) 连接的密码套件包，请参阅 [SCHANNEL]。

默认值：ALL

此设置具有以下值：ALL、COM 或 GOV。

每个值对应的密码套件如下所示：

ALL:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

COM:

TLS_ECDHE_RSA_AES128_CBC_SHA

GOV:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

SSL 合规模式

此设置指定与通用打印客户端用于加密的打印数据流 (CGP) 连接使用的 NIST Special Publication 800-52 的合规性级别。

默认值：无。

此设置具有以下值：

无。

加密的打印数据流 (CGP) 连接使用默认合规模式。

SP800-52。

加密的打印数据流 (CGP) 连接使用 NIST Special Publication 800-52 合规模式。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SSL 已启用

此设置指定通用打印客户端是否对打印数据流 (CGP) 连接和 Web 服务 (HTTP/SOAP) 连接使用 SSL/TLS。

将通用打印服务器启用设置为已启用并回退到 **Windows** 的本机远程打印时，回退连接将由 Microsoft Windows 网络打印提供程序建立。此设置不影响这些回退连接。

默认值：已禁用

此设置具有以下值：

已启用。

通用打印客户端使用 SSL/TLS 连接到通用打印服务器。

已禁用。

通用打印客户端使用 SSL/TLS 连接到通用打印服务器。

SSL FIPS 模式

此设置指定通用打印客户端对打印数据流 (CGP) 连接使用的 SSL/TLS 加密模块是否将在 FIPS 模式下运行。

默认值：已禁用

此设置具有以下值：

已启用。

FIPS 模式已打开。

已禁用。

FIPS 模式已关闭。

SSL 协议版本

此设置指定通用打印客户端使用的 SSL/TLS 协议版本。

默认值：ALL

此设置具有以下值：

ALL。

使用 TLS 版本 1.0、1.1 或 1.2。

TLSv1。

使用 TLS 版本 1.0。

TLSv1.1。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用 TLS 1.1 版本。

TLSv1.2。

使用 TLS 版本 1.2。

SSL 通用打印服务器的加密打印数据流 **(CGP)** 端口

此设置指定通用打印服务器的加密打印数据流 (CGP) 端口的 TCP 端口号。此端口接收打印作业的数据。

默认值：443

SSL 通用打印服务器的加密 **Web** 服务 **(HTTPS/SOAP)** 端口

此设置指定通用打印服务器的加密 Web 服务 (HTTPS/SOAP) 端口的 TCP 端口号。此端口接收打印命令的数据。

默认值：8443

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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

通用打印服务器打印流输入带宽限制 **(kbps)**

此设置指定每个打印作业使用 CGP 向通用打印服务器传输打印数据的速率上限值 (Kbps)。此策略设置适用于包含托管应用程序的虚拟桌面或服务器的 OU。

默认值为 0，表示不指定上边界。

通用打印服务器 **Web** 服务 **(HTTP/SOAP)** 端口

此设置用于指定通用打印服务器的 Web 服务 (HTTP/SOAP) 侦听器所使用的 TCP 端口号。通用打印服务器是一个可选组件，允许将 Citrix 通用打印驱动程序用于网络打印场景。在使用通用打印服务器时，打印命令将从 Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps and Desktops 上的 VDA。此外，还必须更改通用打印服务器上的默认端口。

默认情况下，此端口号设置为 8080。

有效端口号必须在 0 到 65535 范围内。

用于负载平衡的通用打印服务器

此设置列出了在评估其他 Citrix 打印策略设置后，用于对会话启动时建立的打印机连接执行负载平衡的通用打印服务器。为了优化打印机创建时间，Citrix 建议所有打印服务器具有相同的共享打印机集合。对于可添加以用于负载平衡的打印服务器数量而言，没有上限。

此设置还可实现打印服务器故障转移检测和打印机连接恢复。将定期检查打印服务器的可用性。如果检测到某服务器发生故障，会从负载平衡方案中删除该服务器，并在其他可用的打印服务器中重新分配该服务器上的打印机连接。发生故障的打印服务器在恢复后将重新加入负载平衡方案。

单击验证服务器，检查每个服务器是否为打印服务器，服务器列表是否不包含重复的服务器名称，以及是否所有服务器都已安装一组相同的共享打印机。此操作可能需要一些时间。

通用打印服务器停止运行阈值

此设置指定负载平衡器应在多长时间内等待不可用的打印服务器恢复，在此之后负载平衡器将该服务器确定为永久脱机，并将其负载重新分配到其他可用的打印服务器。

默认情况下，此阈值设置为 180（秒）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

通用打印策略设置

November 17, 2021

“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 记录直接后台打印到打印机中。

将此设置添加到策略时，请选择一个选项：

- 为打印机重新处理 EMF 强制重新处理 EMF 后台打印文件，并通过用户设备上的 GDI 子系统发送。可以将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，请选择一个选项：

- 无压缩
- 最佳质量 (无损压缩)
- 高质量
- 标准质量
- 降低质量 (最大压缩)

将该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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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，启用标准质量，这意味着用户只能使用标准或降低质量的压缩级别来打印图像。
- 启用超级压缩用于启用或禁用在超出由“所需图像质量”所设置的压缩级别上减少带宽，而不降低图像质量。默认情况下，禁用超级压缩功能。
- 图像与字体缓存设置指定是否缓存在打印流中多次出现的图像和字体，以确保每个唯一的图像或字体只发送给打印机一次。默认情况下，将缓存嵌入式图像和字体。请注意，只有在用户设备支持此行为时，这些设置才适用。
- 允许非管理员修改这些设置指定用户是否可以更改会话内的默认打印优化设置。默认情况下，不允许用户更改默认打印优化设置。

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，请选择一个选项：

- 不对自动创建的打印机或一般通用打印机使用打印预览
- 仅对自动创建的打印机使用打印预览
- 仅对一般通用打印机使用打印预览
- 对自动创建的打印机和一般通用打印机均使用打印预览

通用打印的打印质量限制

此设置指定在会话中生成打印输出时可用的最高分辨率 (dpi)。

默认情况下，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，请选择一个选项：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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

November 17, 2021

“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 Citrix Virtual Apps and Desktops 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”，会话数据将使用“RC5 (128 位)”加密进行加密。如果没有为交付组选择“启用安全 ICA”，会话数据将通过基本加密进行加密。

将此设置添加到策略时，请选择一个选项：

- 基本可使用一种非 RC5 算法加密客户端连接。它保护数据流使之不能被直接读取，但可以解密。默认情况下，服务器对客户端-服务器通信流使用基本加密。
- 仅限 RC5 (128 位) 登录使用 RC5 128 位加密来加密登录数据，使用基本加密来加密客户端连接。
- RC5 (40 位) 使用 RC5 40 位加密来加密客户端连接。
- RC5 (56 位) 使用 RC5 56 位加密来加密客户端连接。
- RC5 (128 位) 使用 RC5 128 位加密来加密客户端连接。

为客户端-服务器加密指定的设置可能会与您的环境和 Windows 操作系统中的任何其他加密设置进行交互。如果在服务器或用户设备上设置了优先级更高的加密级别，则您为已发布的资源指定的设置可能会被覆盖。

您可以为特定用户提高加密级别，以进一步加强其通信安全和消息的完整性。如果某项策略需要更高的加密级别，则使用较低加密级别的 Citrix Receiver 将被拒绝连接。

SecureICA 不执行身份验证，也不检查数据完整性。要为站点提供端到端加密，请将 SecureICA 与 TLS 加密一起使用。

SecureICA 不使用符合 FIPS 标准的算法。如果这样会带来问题，请将服务器和 Citrix Receiver 配置为避免使用 SecureICA。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SecureICA 使用 RFC 2040 中介绍的 RC5 块密码来保密。块大小为 64 位（32 位字单位的倍数）。密钥长度为 128 位。循环次数为 12。

创建会话时会协商 RC5 块加密的密钥。使用 Diffie-Hellman 算法进行协商。此协商使用 Diffie-Hellman 公共参数，这些参数在安装 Virtual Delivery Agent 时存储在 Windows 注册表中。公共参数不是机密参数。Diffie-Hellman 协商的结果是一个私钥，从中派生出 RC5 块加密的会话密钥。单独的会话密钥用于用户登录和数据传输；单独的会话密钥用于进出 Virtual Delivery Agent 的流量。因此，每个会话有四个会话密钥。不存储密钥和会话密钥。RC5 块加密的初始化向量也是从密钥派生的。

服务器限制策略设置

November 17, 2021

“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

此设置确定在用户未输入任何内容的情况下，用户会话可以保持不中断的时长（毫秒）。

默认情况下，空闲连接不会断开连接（服务器空闲计时器间隔 = 0）。Citrix 建议将此值最小设置为 60000 毫秒（60 秒）。

要显示该策略，请选择多个版本，取消选中“单会话操作系统版本”，然后选择服务器限制。

> 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。Citrix 策略设置不控制此 Microsoft 对话框消息。有关详细信息，请参阅 http://support.citrix.com/article/CTX118618。

会话限制策略设置

November 17, 2021

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长。

> 重要：
>
> 本文中描述的设置不适用于运行多会话 VDA 的计算机。有关为运行多会话 VDA 的计算机配置会话时间限制的详细信息，请参阅 Microsoft 知识库 - 会话时间限制。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

断开会话计时器

此设置将启用或禁用计时器，计时器指定断开连接的锁定桌面在会话注销之前保持锁定状态的时长。如果启用此计时器，则断开连接的会话将在计时器超时时注销。

默认情况下，断开连接的会话不注销。

Remote PC Access 断开连接的会话计时

此设置启用或禁用在计时器到期后注销断开连接的用户会话的计时器。如果启用此设置，请使用断开连接的会话计时器间隔设置指定在注销用户会话之前，断开连接的桌面可以保持锁定状态的分钟数。

默认情况下，禁用此设置。

断开会话计时器间隔

此设置用于指定断开连接的锁定桌面在注销会话前可保持锁定状态的时间长度（分钟）。

默认情况下，此时间期限为 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。如果启用此计时器，则会话将在计时器超时时断开连接或注销。Microsoft 达到时间限制时终止会话设置确定会话的下一状态。

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

此设置将启用或禁用计时器，计时器指定在没有用户输入的情况下用户设备与桌面之间维持不间断连接的时长。此计时器超时后，会话将处于断开连接状态，并且断开会话计时器适用。如果断开会话计时器处于禁用状态，会话将不注销。

默认情况下，启用此计时器。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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保持不中断的时间长度（分钟）。

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

November 17, 2021

会话可靠性部分包含用于管理会话可靠性连接的策略设置。

会话可靠性连接

此设置允许或阻止会话在失去网络连接期间保持打开状态。会话可靠性与客户端自动重新连接一起允许用户在从网络中断恢复时自动重新连接到其 Citrix Workspace 应用程序会话。默认情况下，会话可靠性为“允许”。

在 Citrix Workspace 应用程序 1808 及更高版本和 Citrix Receiver for Windows 4.7 及更高版本中，Studio 中的设置将在客户端上强制执行。客户端上的 Citrix Receiver 组策略对象将被 Studio 策略覆盖。对 Studio 中这些策略的更新会将会话可靠性从服务器同步到客户端。

> 注意：
>
> - Citrix Receiver for Windows 4.7 及更高版本以及适用于 Windows 的 Citrix Workspace 应用程序 - 在 Studio 中设置策略。
> - 版本低于 4.7 的 Citrix Receiver for Windows - 在 Studio 和客户端上的 Citrix Receiver 组策略对象模板中设置策略，以使行为保持一致。

会话可靠性使会话在网络连接中断时保持活动状态并显示在用户的屏幕上。用户仍然可以看到他们正在使用的应用程序，直至网络连接恢复。

会话可靠性可使会话在服务器上保持活动状态。为了指示连接已断开，用户显示变为不透明。用户在连接中断期间可能会看到冻结的会话，在网络连接恢复后可以继续与应用程序交互。会话可靠性可重新连接用户而不提示进行重新身份验证。

如果您同时使用了会话可靠性和客户端自动重新连接，这两项功能将按顺序发挥作用。会话可靠性将在会话可靠性超时设置中指定的时间之后关闭（或断开）用户会话。之后，客户端自动重新连接策略设置生效，尝试将用户重新连接到断开连接的会话。

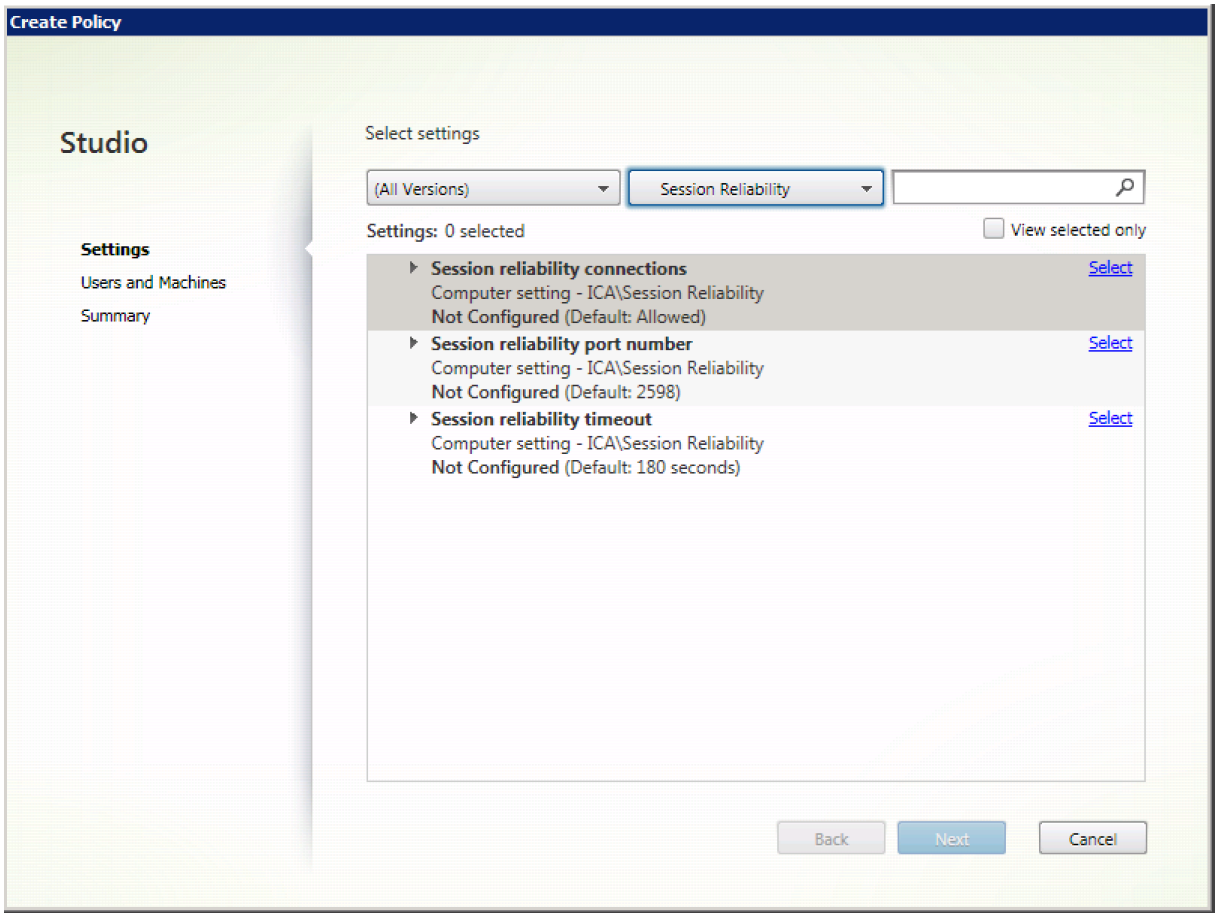
默认情况下，会话可靠性为“允许”。

要禁用会话可靠性，请执行以下操作：

1. 启动 Citrix Studio。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. 打开会话可靠性连接策略。
3. 将策略设置为禁止。



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。

要更改会话可靠性端口号，请执行以下操作：

1. 启动 Citrix Studio。
2. 打开会话可靠性端口号策略。
3. 编辑端口号。
4. 单击确定。

会话可靠性超时

此设置指定会话可靠性代理等待用户重新连接的时间长度（以秒为单位），达到该时间后将允许会话断开连接。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

尽管您可以延长会话保持打开状态的时间长度，此功能是提供方便，它不会提示用户重新进行身份验证。会话打开的时间越长，用户让设备置于无人看管状态并使其会被未经授权的用户访问的可能性越高。

默认情况下，此超时设置为 180 秒或 3 分钟。

更改会话可靠性超时：

1. 启动 Citrix Studio。
2. 打开会话可靠性超时策略。
3. 编辑超时值。
4. 单击确定。

会话水印策略设置

November 17, 2021

“会话水印”部分包含用于配置此功能的策略设置。
启用此功能会导致 VDA 计算机的网络带宽和 CPU 占用量大大增加。我们建议您根据可用的硬件资源为选定的 VDA 计算机配置会话水印。

> 重要
>
> “启用会话水印”设置将使其他水印策略设置生效。为实现更加出色的用户体验，启用的水印文本项目数请不要超过两个。

启用会话水印

启用了此设置时，会话显示屏幕上将覆盖一层显示会话特定信息的不透明文本水印。其他水印设置取决于此设置的启用。

默认情况下，会话水印处于禁用状态。

包括客户端 **IP** 地址

启用了此设置时，会话将显示当前的客户端 IP 地址作为水印。

默认情况下，“包括客户端 IP 地址”处于禁用状态。

包括连接时间

启用了此设置时，会话水印将显示连接时间。格式为 yyyy/mm/dd hh:mm。显示的时间取决于系统时钟和时区。

默认情况下，“包括连接时间”处于禁用状态。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

包括登录用户名

启用了此设置时，会话将显示当前的登录用户名作为水印。显示格式为 USERNAME@DOMAINNAME。我们建议用户名最多包含 20 个字符。用户名超过 20 个字符时，可能会出现字符字体过小或截断问题，并降低水印的有效性。

默认情况下，“包括登录用户名”处于启用状态。

包括 **VDA** 主机名

启用了此设置时，会话将显示当前 ICA 会话的 VDA 主机名作为水印。

默认情况下，“包括 VDA 主机名”处于启用状态。

包括 **VDA IP** 地址

启用了此设置时，会话将显示当前 ICA 会话的 VDA IP 地址作为水印。

默认情况下，“包括 VDA IP 地址”处于禁用状态。

会话水印样式

此设置控制您显示单个水印文本标签还是多个标签。请从值下拉菜单中选择多个或单个。

多个将在会话中显示 5 个水印标签。其中 1 个标签在中心显示，另外 4 个在边角显示。

单个将在会话中心显示 1 个水印标签。

默认情况下，“会话水印样式”设置为“多个”。

水印自定义文本

此设置指定要在会话水印中显示的自定义文本字符串（例如，公司名称）。配置了非空字符串时，将在一个新行中显示该文本，后跟在水印中启用的其他信息。
水印自定义文本最多包含 25 个 Unicode 字符。如果配置了更长的字符串，该字符串将被截断到 25 个字符。

不存在默认文本。

水印透明度

可以指定介于 0 到 100 之间的水印透明度。指定的值越大，水印越不透明。

默认情况下，值为 17。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

时区控制策略设置

November 17, 2021

“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。

在会话断开连接或注销时还原桌面操作系统时区

此设置确定用户断开连接或注销时，单会话操作系统 VDA 的时区设置是否还原到计算机的原始时区。如果启用此设置，VDA 会在用户断开连接或注销时将计算机的时区还原到其原始设置。要使此设置生效，请将使用客户端的本地时间设置为使用客户端时区。

默认情况下，此设置处于启用状态。

使用客户端本地时间

此设置确定用户会话的时区设置。选项包括用户会话的时区（服务器时区）或用户设备的时区（客户端时区）。

默认情况下，使用用户会话的时区。

要使此设置生效，请在组策略编辑器中启用允许时区重定向设置。该设置位于本地计算机策略 > 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 > 设备和资源重定向中。

如果您在运行服务器操作系统的计算机上使用单会话 VDA（以前称为“工作站 VDA”），请将本地用户权限更改时区配置为所有人。可以在本地计算机策略 > 计算机配置 > **Windows** 设置 > 安全设置 > 本地策略 > 用户权限分配中找到此用户权限。

> 注意：
>
> 在单会话操作系统中，用户包含在用户权限分配更改时区中，尽管不在多会话操作系统中也是如此。在多会话操作系统中，时区使用以下组策略进行同步：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\设备和资源重定向\允许时区重定向。当“服务器”不在多会话操作系统 VDA（使用 `/ServerVDI` 命令安装）中的“远程桌面会话主机”中时，此策略不适用。在多会话操作系统中，默认设计为用户没有更改时区的本地权限。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

TWAIN 设备策略设置

November 17, 2021

“TWAIN 设备”部分包含的策略设置与以下内容相关：映射客户端 TWAIN 设备（例如数码相机或扫描仪），优化从服务器到客户端的图像传输。

> 注意：
>
> TWAIN 2.0 支持 Citrix Receiver for Windows 4.5。

客户端 TWAIN 设备重定向

TWAIN 设备使用 TWAIN 协议与服务器托管的图像处理应用程序进行通信。

此设置允许或阻止用户访问用户设备上的 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

November 17, 2021

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，主机将检查 **USB** 策略设置是否允许此设备。如果不允许此设备，主机则检查此设备的客户端 **USB** 设备优化规则。如果未指定任何规则，则不会优化设备。对于签名设备，建议使用捕获模式 (04)。对于其他因更高延迟而降级性能的设备，管理员可以启用交互模式 (02)。请参阅本文中的表格中的可用模式说明。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

须知

- 如果要使用 Wacom 签名板和平板电脑，建议您禁用屏幕保护程序。本部分结尾将介绍如何禁用屏幕保护程序。
- 安装 Citrix Virtual Apps and Desktops 策略时已经预配置了对优化 Wacom STU 签名板和平板电脑系列产品的支持。
- 签名设备在整个 Citrix Virtual Apps and Desktops 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更多软件。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。请将这些设备连接到客户端上的 USB 主机控制器，以便在 Citrix Virtual Desktops 会话内部重定向。

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	类为 **03** 的输入设备支持优化模式。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，四位十六进制数。
PID	设备描述符中的产品 ID，四位十六进制数。
REV	设备描述符中的修订版 ID，四位十六进制数。
类	设备描述符或接口描述符中的类。
子类	设备描述符或接口描述符中的子类。
端口	设备描述符或接口描述符中的协议。

示例

Mode=00000004 VID=067B PID=1230 class=03 # 输入设备在捕获模式下运行

Mode=00000002 VID=067B PID=1230 class=03 # 输入设备在交互模式下运行（默认）

Mode=00000001 VID=067B 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=067B PID=1230 # 设备设置优化已禁用（默认）

Mode=00000200 VID=067B PID=1230 # 设备设置优化已启用

为 **Wacom** 签名板设备禁用屏幕保护程序

对于使用 Wacom 签名板和平板电脑的情况，Citrix 建议您按如下所示禁用屏幕保护程序：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**，选择您的型号对应的选项卡。
4. 选择 **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），然后选择 **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“Allow”规则，则该设备会远程连接到虚拟桌面。如果第一个匹配项是一条“Deny”规则，则该设备只能连接本地桌面。如果未找到匹配项，则使用默认规则。

策略规则的格式为 {Allow: | Deny:} 后接一组以空格分隔的 tag=value 表达式。支持以下标记：

标记名称	说明
VID	设备描述符中的供应商 ID
PID	设备描述符中的产品 ID
REL	设备描述符中的版本 ID
类	设备描述符或接口描述符中的类
子类	设备描述符或接口描述符中的子类
端口	设备描述符或接口描述符中的协议

创建策略规则时，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=067B_。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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=067B PID=0007 # 其他行业，其他闪存驱动器
- 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。

配置 **USB** 设备的自动重定向

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。

> 注意：
>
> 在 Receiver for Windows 4.2 中，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。在早期版本的 Citrix Receiver for Windows 中，在桌面设备模式下或在具有虚拟机 (VM) 托管应用程序的情况下操作时，也会自动对 USB 设备执行重定向操作。

重定向所有 USB 设备并非始终是最佳做法。用户可以明确重定向不会自动重定向的 USB 设备列表中的设备。要阻止列出或重定向 USB 设备，请使用客户端端点或 Virtual Desktop Agent (VDA) 上的 DeviceRules。有关更多详细信息，请参阅管理指南。

> 小心：
>
> “注册表编辑器”使用不当会导致出现严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

USB 设备自动重定向的用户首选项设置

策略：

1. 打开本地组策略编辑器并转至管理模板 **> Citrix** 组件 **> Citrix Receiver >** 远程连接客户端设备 **>** 通用 **USB** 远程连接。
2. 打开新 **USB** 设备，选择已启用，然后单击确定。
3. 打开现有 **USB** 设备，选择已启用，然后单击确定。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Receiver：

1. 转至 **Citrix Receiver** 首选项 **>** 连接。
2. 请务必选择以下选项：
    - 会话启动时，自动连接设备
    - 会话运行过程中连接新设备时，自动连接该设备。
3. 单击确定。

所有注册表项和策略变更都应用到 Windows 客户端设备。

普通 **USB** 打印机重定向

普通 USB 打印机的最佳解决方案是使用专用通用打印机驱动程序和虚拟通道执行打印。默认情况下，普通 USB 打印机不会自动重定向。

普通打印机使用启发式方法进行检测，并且预计具有（例如）扫描功能的高级打印机可能需要使用 USB 支持进行重定向才能完全正常工作。

请使用以下注册表配置是否自动重定向普通打印机：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名称：AutoRedirectPrinters

类型：DWORD

数据：00000000

默认值为 0（不自动重定向）。将值更改为大于值的任何数值都将启用 USB 支持以重定向普通 USB 打印机。

还可以将 Active Directory 策略部署到此注册表项，并覆盖非策略值（如果两者都存在）：

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名称：AutoRedirectAudio

类型：DWORD

数据：00000000

普通音频设备重定向

与普通打印机类似，最佳用户体验是使用 ICA 的专用音频虚拟通道来发送普通音频设备中的音频数据实现的。但是，您可能需要使用 USB 支持来重定向某些专业设备。启发式方法用于确定哪些设备属于普通音频设备。

请在客户端端点上使用此注册表来配置是否自动重定向普通音频设备：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

名称：AutoRedirectAudio

类型：DWORD

数据：00000000

默认值设置为 0（不自动重定向）。将值更改为非零值会通过 USB 支持重定向普通 USB 音频设备。

可以使用 Active Directory 策略将此值部署到注册表项并覆盖非策略值（如果两者都存在）：

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名称：AutoRedirectVideo

类型：DWORD

数据：00000000

普通存储设备（大容量存储设备）重定向

对于普通存储设备，将使用专用虚拟通道（例如同时执行优化的客户端驱动器映射）来实现最佳用户体验。除了简单的读取或写入文件外，要执行某些特殊任务（例如刻录 CD/DVD 或访问加密的文件系统设备），该设备可能仍需要使用通用 USB 支持进行重定向。

启发式方法用于确定哪些设备属于普通存储设备。请使用以下注册表项配置是否自动重定向普通存储设备：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名称：AutoRedirectStorage

类型：DWORD

数据：00000000

默认值设置为 0（不自动重定向）。将值更改为非零值会通过通用 USB 支持重定向普通 USB 存储设备。

还可以使用 Active Directory 策略将此值部署到以下注册表项并覆盖非策略值（如果两者都存在）：

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名称：AutoRedirectStorage

类型：DWORD

数据：00000000

> 注意：
>
> 如果使用通用 USB 支持，则无法配置对普通存储设备的只读访问权限，如果使用 CDM，则可以配置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用硬件加密重定向的 **U** 盘

使用硬件加密的 U 盘通常由加密的存储分区和第二个用于解锁加密分区的实用程序的实用程序分区组成。对于 U 盘设备，将使用同时执行优化的专用客户端驱动器映射/动态 U 盘映射 HDX 虚拟通道来实现最佳用户体验。

通用 USB 重定向是非 Windows 客户端（例如，Linux 客户端）和客户对客户端上的本地功能具有受限（锁定）用户访问权限的客户端所必需的。通用 USB 重定向可以将不使用硬件加密的任何 USB 存储设备同时重定向到单会话操作系统和多会话操作系统 VDA 会话中。

在 Citrix Virtual Apps and Desktops 7 1808 之前，无法通过任何有用的方法将使用硬件加密的 U 盘重定向到单会话操作系统或多会话操作系统 VDA 会话中。Citrix Virtual Apps and Desktops 7 1808 中引入的新增强功能支持将使用硬件加密的 U 盘通过通用 USB 重定向重定向到单会话操作系统和多会话操作系统 VDA 会话中。
重定向设备后，其驱动器不会出现在本地客户端上。因此，如果需要解锁驱动器，请在会话中执行该操作。此功能需要安装 Windows 更新 KB4074590。

普通静止图像设备（扫描仪和数码相机）

对于普通静止图像设备，将使用同时执行优化的专用虚拟通道（例如 TWAIN 虚拟通道）来实现最佳用户体验。这些设备必须遵循行业标准。如果设备不合规，或者如果设备未基于原始意图使用，通用 USB 重定向可能会是使用该设备的唯一方法。启发式方法用于确定哪些设备属于静止图像设备。

请使用以下注册表项配置是否自动重定向普通静止图像设备：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名称：AutoRedirectImage

类型：DWORD

数据：00000000

默认值设置为 0（不自动重定向）。将值更改为非零值会通过通用 USB 重定向普通 USB 静止图像设备。

还可以使用 Active Directory 策略将此值部署到此注册表项并覆盖非策略值（如果两者都存在）：

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名称：AutoRedirectImage

类型：DWORD

数据：00000000

设备特定的设置

用于选择 Citrix 可优化设备（例如打印机、音频设备、视频设备、存储设备和静止图像设备）的启发式方法并不一定始终符合您的预期。您可能希望控制上文未列出的设备的自动重定向。可以在设备特定的基础之上控制自动重定向。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

例如，不需要使用 USB 支持重定向 DemoTech 2000 条码读取器。该读取器具有 12AB 供应商标识符和 5678 产品标识符。可以在设备管理器中找到这些十六进制数。

要防止此设备被自动重定向，请创建此设备特定的注册表项：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名称：AutoRedirect

类型：DWORD

数据：00000000

值 0 将阻止自动重定向该设备。非零值指示必须将该设备视为进行自动重定向（取决于用户首选项）。供应商与产品标识符之间存在一个空格字符。

还可以使用 Active Directory 策略将此值部署到此注册表项。如果两者都存在，则会覆盖非策略值：

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名称：AutoRedirect

类型：DWORD

数据：00000000

设备特定的 AutoRedirect 设置的优先级高于上文所述的更加常规的 AutoRedirectXXX 值。Citrix 优化的设备的默认启发式方法可能会将某个设备误解为通用设备。因此，请将设备特定的 AutoRedirect 值设置为 1 以自动将其重定向。

虚拟通道允许列表策略设置

January 21, 2022

虚拟通道允许列表策略设置允许使用允许列表，该列表指定允许在 ICA 会话中打开哪些虚拟通道。

禁用后，将允许所有虚拟通道。

启用后，仅允许 Citrix 虚拟通道。

要使用自定义或第三方虚拟通道，请将虚拟通道添加到列表中。要将虚拟通道添加到列表中，请输入虚拟通道名称，后跟逗号，然后输入访问该虚拟通道的进程的路径。可以列出更多可执行路径，并且路径用逗号分隔。

例如，

```
CTXCVC1,C:\VC1\vchost.exe
CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe
```

默认情况下，虚拟通道允许列表处于禁用状态。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

如果您使用的是适用于 Skype for Business 的 HDX RealTime Optimization Pack，请将虚拟通道添加到允许列表中。有关详细信息，请参阅 HDX RealTime Optimization Pack 文档。

> 重要：
>
> 启用虚拟频道允许列表策略设置后，文本框中会自动显示已禁用文本。要使功能生效，必须删除文本已禁用。如果没有正在使用的自定义虚拟通道，请将该文本框留空。如果使用自定义虚拟通道，请添加所需的信息。
>
> 必须重新启动 VDA 计算机才能使设置生效。

有关虚拟通道的详细信息，请参阅 ICA 虚拟通道。

视频显示策略设置

January 21, 2022

“视频显示”部分中包含用于控制从虚拟桌面发送到用户设备的图像质量的策略设置。

简单图形的首选颜色深度

此策略设置在 VDA 版本 7.6 FP3 及更高版本中提供。8 位选项在 VDA 版本 7.12 及更高版本中提供。

使用此设置，可以降低通过网络发送简单图形时使用的颜色深度。降低到 8 位/像素或 16 位/像素可能会提高使用低带宽连接时的响应能力，但会略微降低图像质量。使用视频编解码器进行压缩策略设置设置为“针对整个屏幕”时，不支持 8 位颜色深度。

默认的首选颜色深度是 24 位/像素。

如果在 VDA 版本 7.11 及更低版本上应用 8 位设置，VDA 将回退至 24 位（默认）颜色深度。

目标帧速率

此设置指定每秒从虚拟桌面发送到用户设备的最大帧数。

默认情况下，最大值为 30 帧/秒。

设置一个较高的每秒帧数值（例如 30）可改进用户体验，但需要占用更多带宽。减小每秒帧数值（例如 10）可将服务器可扩展性提高至最高水平，但用户体验将非常差。对于 CPU 速度较慢的用户设备，指定较低的值可以改善用户体验。

支持的最高每秒帧速率是 60。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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，此设置为“中”。

要指定图像质量，请选择下列选项之一：

- 低 - 建议对可以降低视觉质量以实现交互的带宽受限网络使用
- 中 - 在大多数用例中可提供最佳性能和最高带宽效率
- 高 - 如果需要视觉无损图像质量，建议采用此设置
- 设为无损 - 在高网络活动期间将有损图像发送到用户设备，以及在网络活动减少后将无损图像发送到用户设备。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 - 保留图像数据非常重要时，请选择“始终无损”以确保绝不会将有损数据发送到用户设备。例如，显示不允许有质量损失的 X 光图像时。

移动图像策略设置

November 17, 2021

“移动图像”部分包含使您能够删除或更改动态图像的压缩的设置。

最低图像质量

注意：对于 Virtual Delivery Agent 7.x，仅当启用旧图形模式策略设置时，才会应用此策略设置。

此设置指定自适应显示功能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”。

移动图像压缩

此设置指定是否启用自适应显示功能。自适应显示功能将根据可用带宽自动调整视频和幻灯片播放时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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

渐进式压缩级别

注意：对于 Virtual Delivery Agent 7.x，仅当启用旧图形模式策略设置时，才会应用此策略设置。

此设置提供的图像的初始显示细节较少但速度更快。

默认情况下，不应用任何渐进式压缩。

细节更丰富的图像（由常规有损压缩设置定义）在可用时显示。使用“很高”或“超高”压缩可改善需要占用大量带宽的图形（例如照片）的查看速度。

要使渐进式压缩生效，其压缩级别必须高于有损压缩级别设置。

注意：提高与渐进式压缩相关联的压缩级别，还会提高客户端连接上动态图像的交互性。动态图像（例如旋转的三维模型）的质量在图像停止动作前会暂时降低，之后会应用标准有损压缩设置。

下列策略设置为相关设置：

- 渐进式压缩阈值
- 渐进式超级压缩

渐进式压缩阈值

注意：对于 Virtual Delivery Agent 7.x，仅当启用旧图形模式策略设置时，才会应用此策略设置。

此设置表示应用渐进式压缩的连接的最大带宽 (Kbps)。此设置仅适用于低于此带宽的客户端连接。

默认情况下，该阈值为 2147483647 Kbps。

下列策略设置为相关设置：

- 渐进式压缩阈值
- 渐进式超级压缩

目标最低帧速率

此设置为动态图像指定了低带宽条件下，系统尝试保持的最低每秒帧速率。

默认情况下设置为 10 fps。

对于版本 7.0 至 7.6 的 VDA，此设置仅在启用旧图形模式时应用。对于版本为 7.6 FP1 及更高版本的 VDA，此设置在禁用或启用旧图形模式时均可以应用。

静态图像策略设置

November 17, 2021

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

“静态图像”部分包含使您能够删除或更改静态图像的压缩的设置。

额外颜色压缩

此设置允许或禁止当通过带宽受限制的客户端连接交付图像时，这些图像使用额外颜色压缩，从而以降低显示图像质量的方式来提高响应能力。

默认情况下，禁用额外颜色压缩。

启用后，则只有当客户端连接带宽低于额外颜色压缩阈值的值时，才会应用额外颜色压缩。如果客户端连接带宽高于该阈值，或者选择了已禁用，则不会应用额外颜色压缩。

额外颜色压缩阈值

注意：对于 Virtual Delivery Agent 7.x，仅当启用旧图形模式策略设置时，才会应用此策略设置。

此设置表示连接的最大带宽 (Kbps)，如果低于该带宽，则会应用额外颜色压缩。如果客户端连接带宽低于设置的值，则会应用额外颜色压缩（如果启用）。

默认情况下，该阈值为 8192 Kbps。

超级压缩

注意：对于 Virtual Delivery Agent 7.x，仅当启用旧图形模式策略设置时，才会应用此策略设置。

此设置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，禁用超级压缩功能。

如果启用超级压缩，它会应用到所有有损压缩设置。这种压缩在 Citrix Workspace 应用程序上受支持，但对其他插件不起作用。

下列策略设置为相关设置：

- 渐进式压缩级别
- 渐进式压缩阈值

有损压缩级别

注意：对于 Virtual Delivery Agent 7.x，仅当启用旧图形模式策略设置时，才会应用此策略设置。

此设置控制通过带宽受限的客户端连接交付的图像上所用的有损压缩程度。在此类情况下，显示未压缩的图像速度会很慢。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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，请使用高压缩。当保留图像数据非常重要（例如显示不允许有质量损失的 X 光图像时），您可能不希望使用有损压缩。

相关策略设置：有损压缩阈值

有损压缩阈值

注意：对于 Virtual Delivery Agent 7.x，仅当启用旧图形模式策略设置时，才会应用此策略设置。

此设置表示应用有损压缩的连接的最大带宽 (Kbps)。

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

November 17, 2021

WebSocket 部分包含用于使用适用于 HTML5 的 Citrix Workspace 应用程序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，从而提高安全性并减少开销。此功能在不打开多个 HTTP 连接的情况下执行此操作。

WebSocket 连接

此设置允许或禁止 WebSocket 连接。

默认情况下，禁止 WebSocket 连接。

WebSocket 端口号

此设置可识别传入的 WebSocket 连接的端口。

默认情况下，此值为 8008。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

WebSocket 可信源服务器列表

此设置提供了一个逗号分隔的可信原始服务器列表，通常是适用于 Web 的 Citrix Workspace 应用程序，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 * 用于信任所有适用于 Web 的 Citrix Workspace 应用程序 URL。

如果您选择在列表中键入地址，请使用以下语法：

< 协议 >://< 主机的完全限定的域名 >:[端口]
协议必须是 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。
主机的完全限定的域名 > 协议 >

WIA 设备策略设置

January 21, 2022

“WIA 设备”部分包含使用 Windows 图像采集 (WIA) 管理扫描程序重定向的策略设置。

WIA 重定向

WIA 设备（例如数码相机和扫描仪）通过使用 WIA 框架与服务器托管的图像处理应用程序进行通信。此设置允许或禁止用户访问用户设备上的 WIA 设备。默认情况下，禁止 WIA 重定向。

有关符合 WIA 标准的设备的信息，请参阅 WIA 设备。

通过注册表管理的 **HDX** 功能

January 21, 2022

> 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。

要打开注册表编辑器，请在服务器上运行 `regedit.exe`。然后导航到注册表项以添加或编辑设置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

设备

Bloomberg 键盘

Citrix Virtual Apps and Desktops 支持 Bloomberg 4 型和 3 型 Starboard 键盘。默认情况下，对增强的 Bloomberg 键盘的支持处于禁用状态。

要启用对 Bloomberg 键盘的支持，请在开始连接之前在客户端计算机上设置以下注册表值：

- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB
- 值名称：EnableBloombergHID
- 值类型：DWORD
- 值数据：0 = 禁用，1 = 启用

有关详细信息，请参阅 Bloomberg 键盘。

映射的客户端驱动器

为了安全起见，用户登录到 Citrix Virtual Apps and Desktops 时，默认情况下服务器会映射客户端驱动器，但不具有用户运行权限。要使用户能够运行映射的客户端驱动器上的可执行文件，可通过编辑服务器上的注册表来覆盖此默认设置。

要允许访问，请编辑以下注册表值（如果 **CDMSettings** 不存在，请创建）：

- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\CDMSettings
- 值名称：ExecuteFromMappedDrive
- 值类型：DWORD
- 值数据：1 = 允许权限，0 = 拒绝映射的驱动器的权限

此更改对编辑注册表后连接的会话有效。

有关详细信息，请参阅映射的客户端驱动器。

Microsoft Surface Pro 和 Surface Book 笔

Citrix Virtual Apps and Desktops 支持在基于 Windows InK 的应用程序中使用标准笔功能默认情况下，启用此功能。

要禁用或启用此功能，请设置以下注册表值：

- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent\PenApi
- 值名称：DisablePen
- 值类型：DWORD
- 值数据：1 = 禁用，0 = 启用

有关详细信息，请参阅 Microsoft Surface Pro 和 Surface Book 笔。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Windows 图像采集应用程序允许列表

此设置允许您控制 VDA 上的哪些应用程序可以访问 Windows 图像采集扫描程序重定向。

默认情况下，任何应用程序都无权访问 Windows 图像采集。

要调整 VDA 上的应用程序的 Windows 图像采集，请创建以下注册表设置：

- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix
- 值名称：WIAAllowedProcesses

  选择并右键单击 **WIAAllowedProcesses**。选择新建 **>** 多字符串值，然后将新值重命名为 **AllowProcesses**。
- 值数据：输入可以访问 Windows 图像采集的每个应用程序的完整路径和进程名称。在新行中提供每个应用程序。

对此设置所做的任何更改都将在您下次在 VDA 上启动会话时生效。

常规

配置自动登录 **VDA**

此设置允许您在 Windows 10 单会话操作系统和多会话操作系统 VDA 上启用或禁用始终提示输入密码 Microsoft 策略设置。

如果启用了始终提示输入密码，用户在启动远程会话时必须在 VDA 上输入凭据。如果禁用此设置，用户将自动连接到远程会话，而不在 VDA 上提供凭据。

默认情况下，Microsoft 策略设置处于禁用状态。要启用或禁用始终提示输入密码设置，请在 VDA 上设置以下注册表值：

- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Portica
- 值名称：AutoLogon
- 值类型：DWORD
- 值数据：
  - 1 - 禁用 Microsoft 策略设置，并允许用户自动登录远程会话。
  - 0 - 启用 Microsoft 策略设置，并在用户启动远程会话时提示用户提供凭据。

禁用超时警告

默认情况下，具有非活动会话或空闲会话的用户在会话自动断开连接前两分钟收到警告消息。

此设置禁用和删除在 Windows 2004 或更高版本的多会话操作系统中达到空闲会话超时限制的用户的警告消息。要删除警告，请在 VDA 上设置以下注册表值：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 注册表项:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\ICA-CGP
- 值名称：fEnableTimeoutWarning
- 值类型：DWORD
- 值数据：1 = 禁用警告消息，0 = 启用警告消息

要显示警告消息，请删除注册表值或将其设置为 0。

EDT MTU 发现

MTU 发现允许 EDT 在建立会话时自动确定最大传输单位 (MTU)。这样做可以防止出现可能会导致性能下降或无法建立会话的 EDT 数据包碎片。

默认情况下，启用此设置。要禁用 EDT MTU 发现，请删除以下注册表值并重新启动 VDA。

- 注册表项:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd
- 值名称：MtuDiscovery
- 值类型：DWORD
- 值数据：00000001

此设置在计算机范围内适用，影响从受支持的客户端连接的所有会话。

常规内容重定向

为主机到客户端重定向添加 **URL** 类型

默认情况下，我们支持以下 URL 类型的重定向：HTTP、HTTPS、RTSP、RTSPU、PNM 和 MMS。通过在 Windows 客户端上创建以下注册表项和值，可以将 URL 类型添加到列表中。

- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- 值名称：ExtraURLProtocols
- 值类型：REG_SZ
- 值数据：指定所需的 URL 类型，用分号分隔。在 URL 的授权部分之前包括所有内容。例如：
  `ftp://;mailto:;customtype1://;custometype2://`

可以添加仅适用于 Windows 客户端的 URL 类型。缺少此注册表设置的客户端拒绝重定向回 Citrix 会话。客户端必须安装并配置应用程序以处理指定的 URL 类型。

有关详细信息，请参阅主机到客户端重定向。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。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。

要在服务器上启用客户端文件夹重定向，请设置以下注册表值：

- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection
- 值名称：CFROnlyModeAvailable
- 值类型：DWORD
- 值数据：1

有关详细信息，请参阅客户端文件夹重定向。

面向一组特定 **Web** 站点的主机到客户端重定向

要为一组特定的 Web 站点启用主机到客户端重定向，请在服务器 VDA 上设置以下注册表值。

- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 值名称：ValidSites
- 值类型：REG_MULTI_SZ
- 数据：指定完全限定域名 (FQDN) 的任意组合。在单独的行中键入多个 FQDN。仅包括 FQDN，没有协议 (`http://` 或 `https://`)。FQDN 只能在最左侧位置包含星号 (*) 作为通配符。这匹配一层域，与 RFC 6125 中的规则一致。例如：

```
www.example.com
*.example.com
```

有关详细信息，请参阅主机到客户端重定向。

注销和断开连接时本地应用程序的行为

默认情况下，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。重新连接后，如果本地应用程序在虚拟桌面中可用，则将重新集成。要在注销和断开连接时配置本地应用程序行为，请在托管桌面中设置以下注册表值：

- 注册表项:HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies
- 值名称：会话状态
- 值类型：DWORD
- 值数据：
  - 1 - 当用户从虚拟桌面注销或断开连接时，本地应用程序继续运行。一旦重新建立连接，如果本地应用程序在虚拟桌面中可用，将重新集成。
  - 3 - 当用户从虚拟桌面注销或断开连接时，本地应用程序关闭。

有关详细信息，请参阅本地应用程序访问和 URL 重定向。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

从主机到客户端重定向的默认列表中删除 **URL** 类型

要从默认重定向列表中删除 URL 类型，请在服务器 VDA 上创建以下注册表项和值。

- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 值名称：DisableServerFTA
- 值类型：DWORD
- 值数据：1
- 值名称：NoRedirectClasses
- 值类型：REG_MULTI_SZ
- 值数据：指定值的任意组合：`http`、`https`、`rtsp`、`rtspu`、`pnm` 或 `mms`。在单独的行中输入多个值。例如：

```
http
https
rtsp
```

有关详细信息，请参阅主机到客户端重定向。

服务器 **VDA** 默认浏览器配置

可以启用主机到客户端重定向以取代服务器 VDA 上的任何默认浏览器配置。如果未重定向 Web URL，Citrix Launcher 会将 URL 传递到在注册表项 `command_backup` 中配置的浏览器。默认情况下，该注册表项指向 Internet Explorer，但您可以将其修改为包含指向不同浏览器的路径。

- Internet Explorer（默认）
  - 注册表项：HKEY_CLASSES_ROOT\http\shell\open\command_backup
  - 值名称：Default
  - 值类型：REG_SZ
  - 值数据：`"c:\program files\internet explorer\iexplore.exe"%1`
  - 注册表项：HKEY_CLASSES_ROOT\https\shell\open\command_backup‘
  - 值名称：Default
  - 值类型：REG_SZ
  - 值数据：`"c:\program files\internet explorer\iexplore.exe"%1`
- Google Chrome

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - 注册表项：HKEY_CLASSES_ROOT\http\shell\open\command_backup
  - 值名称：Default
  - 值类型：REG_SZ
  - 值数据："C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"%1
  - 注册表项：HKEY_CLASSES_ROOT\https\shell\open\command_backup
  - 值名称：Default
  - 值类型：REG_SZ
  - 值数据："C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"%1

- Microsoft Edge
  - 注册表项：HKEY_CLASSES_ROOT\http\shell\open\command_backup
  - 值名称：Default
  - 值类型：REG_SZ
  - 值数据："C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe"%1
  - 注册表项：HKEY_CLASSES_ROOT\https\shell\open\command_backup
  - 值名称：Default
  - 值类型：REG_SZ
  - 值数据："C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe"%1

面向已发布应用程序的本地应用访问

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，而无需从一个桌面切换到另一个桌面。要提供对已发布应用程序的访问权限，请在服务器上设置以下注册表值：

- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio
- 值名称：ClientHostedAppsEnabled
- 值类型：DWORD
- 值数据：1 = 启用，0 = 禁用

有关详细信息，请参阅本地应用程序访问和 URL 重定向。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

图形

面向 **CUDA** 或 **OpenCL** 应用程序的 **GPU** 加速功能

默认禁用在用户会话中运行的 CUDA 或 OpenCL 应用程序的 GPU 加速功能。

要使用 CUDA 加速 POC 功能，请启用以下注册表设置：

- 注册表项:HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper
- 值名称：CUDA
- 值类型：DWORD
- 值数据：00000001

要使用 OpenCL 加速 POC 功能，请启用以下注册表设置：

- 注册表项:HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper
- 值名称：OpenCL
- 值类型：DWORD
- 值数据：00000001

有关详细信息，请参阅适用于 Windows 多会话操作系统的 GPU 加速

渐进式模式

默认情况下，渐进式模式处于禁用状态。可以通过以下注册表值更改渐进式模式的状态：

- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- 值类型：REG_DWORD
- 值名称：ProgressiveDisplay
- 值数据：
  - 0 = 始终关闭（禁用渐进式模式。此值为默认值。）
  - 1 = 自动（根据网络条件切换。）
  - 2 = 始终开启

有关详细信息，请参阅渐进式模式。

Windows Presentation Foundation (WPF) 呈现

通过 HDX 3D Pro，在 Windows 多会话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 Windows Presentation Foundation (WPF) 呈现移到服务器的 GPU 上，图形呈现不会降低服务器的 CPU 速率。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

要能够使用服务器的 GPU 呈现 WPF 应用程序，请在运行 Windows 多会话操作系统的服务器的注册表中创建以下设置：

- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432\Citrix\CtxHook\AppInit_Dlls\Multiple Monitor Hook
- 值名称：EnableWPFHook
- 值类型：DWORD
- 值数据：00000001

有关详细信息，请参阅适用于 Windows 多会话操作系统的 GPU 加速。

多媒体

在多媒体会议期间避免产生回声

Citrix Virtual Apps and Desktops 提供了回声消除选项，可最大限度地减少任何回声。默认情况下启用此功能。要禁用回声消除，可以更改以下注册表设置之一：

- 注册表项：
  - 32 位：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\
  - 64 位：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Adva
- 值名称：EchoCancellation
- 值类型：DWORD
- 值数据：False

有关详细信息，请参阅音频功能。

音频限制

在客户端上安装音频设备、启用音频重定向并启动 RDS 会话后，音频文件可能无法播放音频。解决方法：在 RDS 计算机上添加以下注册表项，然后重新启动计算机：

- 注册表项：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig
- 值名称：EnableSvchostMitigationPolicy
- 值类型：DWORD
- 值数据：0

有关详细信息，请参阅音频功能。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

浏览器内容重定向和 **DPI**

在用户的计算机上使用浏览器内容重定向时，如果 DPI（缩放）设置为超过 100% 的任何设置，重定向的浏览器内容屏幕将错误地显示。为避免出现此问题，请通过在用户的计算机上创建以下注册表值来禁用 Chrome 的浏览器内容重定向 GPU 加速：

- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream
- 值名称：GPU
- 值类型：DWORD
- 值数据：0

有关详细信息，请参阅浏览器内容重定向和 DPI。

高清网络摄像机流技术推送

服务器上的视频会议应用程序将根据支持的格式类型选择网络摄像机格式和分辨率。Citrix Virtual Apps and Desktops 支持高达 1920x1080 的网络摄像机分辨率。要禁用和启用高清网络摄像机流技术推送，请添加以下注册表值：

- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDXRealTime
- 值名称：Enable_HighDefWebcam
- 值类型：DWORD
- 值数据：
  - 0 = 禁用高清网络摄像机流技术推送
  - 1 = 启用高清网络摄像机流技术推送

高清网络摄像机分辨率

如果媒体类型协商失败，HDX 将回退到默认分辨率 352x288 CIF。可以使用客户端上的注册表项来配置默认分辨率。在设置以下注册表项之前，请确保相机支持指定的分辨率。

- 注册表项：HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- 宽度
  - 值名称：DefaultWidth
  - 值类型：DWORD
  - 值数据：所需的十进制宽度（例如 1280）
- 高度
  - 值名称：DefaultHeight
  - 值类型：DWORD
  - 值数据：所需的十进制高度（例如 720）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

高清网络摄像机带宽

与即插即用通用 USB 重定向相比，HDX 网络摄像机视频压缩占用的带宽较少，并且可以在 WAN 连接条件下很好地运行。要调整带宽，请在客户端上设置以下注册表值：

- 注册表项：HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- 值名称：TargetBitrate
- 值类型：DWORD
- 值数据：350000

输入以 bps 为单位的值。如果未指定带宽，视频会议应用程序将默认使用 350000 bps。

有关详细信息，请参阅 HDX 网络摄像机视频压缩。

Microsoft Teams 回退模式

如果 Microsoft Teams 无法在优化的 VDI 模式下加载（在“Teams”/“关于”/“版本”中显示“Citrix HDX 未连接”），VDA 将回退到旧版 HDX 技术，例如网络摄像机重定向以及客户端音频和麦克风重定向。= 如果您使用的是不支持 Microsoft Teams 优化的 Workspace 应用程序版本/平台操作系统，则不应用回退注册表项。

要控制回退机制，请在 VDA 上设置以下注册表值之一：

- 注册表项（只需要一个）：
  - 计算机设置： HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams
  - 用户设置： HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Teams
- 值名称：DisableFallback
- 值类型：DWORD
- 值数据：1 = 禁用回退模式，2 = 仅启用音频

如果该值不存在或设置为 0，则启用回退模式。此功能需要 Microsoft Teams 版本 1.3.0.13565 或更高版本。有关详细信息，请参阅 Microsoft Teams 优化。

借助 Citrix App Layering 优化 Microsoft Teams

如果使用 Citrix App Layering 管理不同层中的 VDA 和 Microsoft Teams 安装，请在使用 **ALLUSER**=1 安装 Microsoft Teams 之前在 Windows 中部署此注册表项。

创建名为 **PortICA** 的空注册表项，然后保留默认值名称、类型和数据。

- 注册表编辑器 32 位版本的密钥: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA
- 注册表编辑器 64 位版本的密钥：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA

有关详细信息，请参阅 Microsoft Teams 优化。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用集成 **Windows** 身份验证进行单点登录，以实现浏览器内容重定向

此设置提供对与 VDA 位于同一域中且配置了集成 Windows 身份验证 (IWA) 的 Web 服务器的单点登录。要启用单点登录，请将以下注册表值设置为 1：

- 注册表项：
  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream

  或

  - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\HdxMediastream
- 值名称：WebBrowserRedirectionIwaSupport
- 值类型：DWORD
- 值数据：1

有关详细信息，请参阅使用集成 Windows 身份验证进行单点登录。

用户代理请求标头

用户代理标头有助于识别从浏览器内容重定向发送的 HTTP 请求。配置代理和防火墙规则时，此设置会非常有用。例如，如果服务器阻止从浏览器内容重定向发送的请求，则可以创建包含用户代理标头的规则以绕过某些要求。只有 Windows 设备支持用户代理请求标头。

默认情况下，用户代理请求标头字符串处于禁用状态。要为客户端呈现的内容启用用户代理标头，请使用注册表编辑器。

在每个适用于 Windows 的 Citrix Workspace 应用程序客户端上，设置下面其中一项注册表设置：

- 注册表项：
  - 32 位：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStream
  - 64 位：HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream
- 名称名称：EnableCefUserAgentString
- 值类型：DWORD
- 值数据：1

添加注册表值后，用户代理标头将包含 CitrixBCR/2102.1 文本，其中 2102.1 为适用于 Windows 的 Citrix Workspace 应用程序版本。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

网络摄像机软件压缩

如果网络摄像机支持硬件编码，默认情况下 HDX 视频压缩功能将采用硬件编码。硬件编码占用的带宽可能高于软件编码。要强制执行软件压缩，请在客户端上添加以下值：

- 注册表项：HKEY_CURRENT_USER\SOFTWARE\Citrix\HdxRealTime
- 值名称：DeepCompress_ForceSWEncode
- 值类型：DWORD
- 值数据：1

有关详细信息，请参阅 HDX 网络摄像机视频压缩。

网络摄像机视频压缩

HDX 网络摄像机视频压缩将 H.264 视频直接发送到在虚拟会话中运行的视频会议应用程序。为了优化 VDA 资源，HDX 网络摄像机压缩不会对网络摄像机视频进行编码、转码和解码。默认情况下启用此功能。

要禁用从服务器到视频会议应用程序的直接视频流，请在 VDA 中设置以下注册表值。

- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime
- 值名称：OfferH264ToApp
- 值类型：DWORD
- 值数据：0

有关详细信息，请参阅 HDX 网络摄像机视频压缩。

网络摄像机视频压缩缩帧率

要调整首选视频帧速率，请在客户端上编辑以下注册表值：

- 注册表项：HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- 值名称：FramesPerSecond
- 值类型：DWORD
- 值数据：15

如果网络摄像机不支持指定的帧速率，应用程序将默认使用 15 FPS。

有关详细信息，请参阅 HDX 网络摄像机视频压缩。

负载管理策略设置

January 21, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

“负载管理”部分包含用于在交付 Windows 多会话操作系统计算机的服务器之间启用和配置负载管理的策略设置。

有关计算负载评估器指数的信息，请参阅 CTX202150。

并发登录容错

此设置指定服务器可以接受的最大并发登录数。

默认情况下，此范围设置为 2。

启用了此设置时，负载平衡功能将尝试避免服务器 VDA 上同时出现多个指定的活动登录。但是，该限制并不严格执行。要执行该限制（导致超出指定数量的并发登录失败），请创建以下注册表项：

> HKLM\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit
> 类型：DWORD
> 值：1

CPU 使用率

此设置指定服务器报告满负载时的 CPU 使用率，以百分比表示。启用时，服务器报告满负载的默认值是 90%。

默认情况下，此设置处于禁用状态，负载计算中不包括 CPU 使用率。

排除 **CPU** 使用率的进程优先级

> 注意：
>
> 在计算机由 Workspace Environment Management 管理的情况下，使用此设置以及 CPU 优先级设置可能会产生意想不到的结果。如果选择使用 CPU 优先级设置，我们建议您禁用此设置。

此设置指定从 CPU 使用率负载指数中排除进程 CPU 使用率时的优先级。

默认情况下，此参数设置为低于正常或低。

磁盘使用情况

此设置指定服务器报告 75% 满负载时的磁盘队列长度。启用时，磁盘队列长度的默认值为 8。

默认情况下，此设置处于禁用状态，负载计算中不包括磁盘使用情况。

最大会话数

此设置指定服务器可以托管的最大会话数。启用时，服务器可托管最大会话数的默认设置为 250。

默认情况下，此设置处于启用状态。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

内存使用率

此设置指定服务器报告满负载时的内存使用率，以百分比表示。启用时，服务器报告满负载的默认值是 90%。

默认情况下，此设置处于禁用状态，负载计算中不包括内存使用率。

内存使用基础负载

此设置指定基本操作系统内存使用空间的近似值，并定义服务器被视为零负载时的内存使用空间（以 MB 为单位）。

默认情况下，将其设置为 768 MB。

Profile Management 策略设置

January 21, 2022

本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。

有关其他信息（例如等效.ini 文件设置的名称和策略设置需要的 Profile Management 版本），请参阅 Profile Management 策略。

高级策略设置

January 21, 2022

访问锁定文件的重试次数

设置尝试访问锁定文件的重试次数。

如果禁用了此策略，则将使用默认值重试五次。如果未在此处配置此策略，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，则将使用默认值。

注销时处理 **Internet Cookie** 文件

某些部署会保留未被 Index.dat 文件引用的多余 Internet Cookie。持续浏览后保留在文件系统中的多余 Cookie 可能会导致配置文件膨胀。启用该策略可强制处理 Index.dat，并强制删除多余的 Cookie。该策略会延长注销时间，因此，仅当您遇到此问题时才能启用该设置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

如果未在此处配置此策略，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，则将不处理 Index.dat。

禁用自动配置

Profile Management 将检查所有 Citrix Virtual Desktops 环境，例如，检查是否存在个人虚拟磁盘，以及配置相应的组策略。只会调整处于未配置状态的 Profile Management 策略，因此将会保留您所做的任何自定义设置。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 Citrix Virtual Apps 或其他环境中无法使用。

您可以将自动配置视为可根据运行时的环境自动配置默认策略设置的动态配置检查器。这样就无需手动配置设置。运行时环境包括：

- Windows 操作系统
- Windows 操作系统版本
- 存在 Citrix Virtual Desktops
- 存在个人虚拟磁盘

如果环境发生变化，自动配置可能会更改以下策略：

- 主动回写
- 总是缓存
- Delete locally cached profiles on logoff（注销时删除本地缓存的配置文件）
- 删除缓存的配置文件之前的延迟
- Profile Streaming

有关不同操作系统中的策略的默认状态，请参见下表：

	多会话操作系统	单会话操作系统
主动回写	已启用	*Disabled*（已禁用）（如果正在使用 Personal vDisk）；否则将启用。
总是缓存	已禁用	*Disabled*（已禁用）（如果正在使用 Personal vDisk）；否则将启用。
Delete locally cached profiles on logoff（注销时删除本地缓存的配置文件）	已启用	*Disabled*（已禁用）（如果正在使用 Personal vDisk 或如果已分配 Citrix Virtual Desktops 或如果未安装 Citrix Virtual Desktops）；否则将启用。
删除缓存的配置文件之前的延迟	0 秒	60 秒（如果用户进行的更改不是永久性的）；否则为 0 秒。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

	多会话操作系统	单会话操作系统
Profile Streaming	已启用	*Disabled*（已禁用）（如果正在使用 Personal vDisk）；否则将启用。

但是，禁用了自动配置后，上述所有策略都将默认设置为禁用。

> 重要：
>
> Personal vDisk 已弃用。有关详细信息，请参阅删除 PVD、AppDisk 和不受支持的主机。

自 Profile Management 1909 起，您可以通过 Windows 10（1607 及更高版本）和 Windows Server 2016 及更高版本上的“开始”菜单获得改进的体验。此改进功能是通过自动配置以下策略来实现的：

- 在“要镜像的文件夹”中添加“Appdata\Local\Microsoft\Windows\Caches”和“Appdata\Local\Packages”
- 在“要同步的文件”中添加“Appdata\Local\Microsoft\Windows\UsrClass.Dat*”

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，则将启动自动配置，若环境更改，Profile Management 设置可能也会更改。

遇到问题时注销用户

如果已禁用或未配置该策略，将会在遇到问题（例如，用户存储不可用）时为用户提供一个临时配置文件。如果已启用该策略，将会显示一条错误消息，并注销用户。此设置可以简化对问题进行故障排除的过程。

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。

客户体验改善计划

默认情况下，系统会启用“客户体验改善计划”，以通过发送匿名统计信息和使用情况信息来帮助改进 Citrix 产品的质量和性能。

如果未在此处配置此设置，则将使用.ini 文件中的值。

启用 **Outlook** 的搜索索引漫游

通过自动漫游 Outlook 搜索数据以及用户配置文件，实现基于用户的 Outlook 搜索体验。这需要用户存储中具有额外空间来存储 Outlook 的搜索索引。

您必须注销后重新登录，才能使此策略生效。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Outlook 搜索索引数据库 **-** 备份和还原

此设置配置在启用了“启用 Outlook 的搜索索引漫游”时 Profile Management 在登录过程中执行的操作。

如果启用此设置，Profile Management 会在每次登录时成功装载数据库时保存搜索索引数据库的备份。Profile Management 将备份视为搜索索引数据库的状态良好的副本。尝试装载搜索索引数据库由于数据库损坏而失败时，Profile Management 会自动将搜索索引数据库还原到最后一个已知良好的副本。

> 注意：
>
> Profile Management 在成功保存新备份后删除之前保存的备份。备份会占用 VHDX 文件的可用存储空间。

为配置文件容器启用多会话回写功能

在多会话场景中为配置文件容器启用回写功能。如果已启用，所有会话中的更改都会回写到配置文件容器。否则，仅保存第一个会话中的更改，因为配置文件容器中只有第一个会话处于读取/写入模式。自 Citrix Profile Management 2103 起支持 Citrix Profile Management 配置文件容器。自 Citrix Profile Management 2003 起支持 FSLogix 配置文件容器。

要将此策略用于 FSLogix 配置文件容器，请确保满足以下必备条件：

- FSLogix 配置文件容器功能已安装并启用。
- 在 FSLogix 中，配置文件类型设置为 **Try for read-write profile and fallback to read-only**（针对读写配置文件尝试，并回退到只读）。

复制用户存储

除了 **Path to user store**（用户存储路径）策略指定的路径外，您还可以在每次登录和注销时将用户存储复制到多个路径。要同步到会话期间修改的用户存储文件和文件夹，请启用主动回写。此功能当前不支持完整的容器解决方案。启用此策略可以增加系统 I/O，并且可能延长注销时间。

启用对用户存储的基于凭据的访问

默认情况下，Citrix Profile Management 模拟当前用户访问用户存储。因此，它要求当前用户具有直接访问用户存储的权限。如果您不希望 Profile Management 在访问用户存储时模拟当前用户，请启用此功能。可以将用户存储放置在当前用户无权访问的存储库（例如 Azure 文件）中。

要确保 Profile Management 能够访问用户存储，请将配置文件存储服务器的凭据保存在 Workspace Environment Management (WEM) 或 Windows 凭据管理器中。我们建议您使用 Workspace Environment Management 来消除为运行 Profile Management 的每台计算机配置相同凭据的需要。如果使用 Windows 凭据管理器，请使用本地系统帐户安全地保存凭据。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 要确保保留 NTFS 权限，必须将整个配置文件放置在配置文件容器中。

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，默认处于禁用状态。则

基本策略设置

November 17, 2021

本部分包含与 Profile Management 基本配置有关的策略设置。

启用 **Profile Management**

默认情况下，为便于部署，Profile Management 不处理登录或注销。要启用 Profile Management，必须先执行其他所有设置任务并测试 Citrix 用户配置文件在环境中的执行情况。

如果未在此处配置此策略，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 Profile Management 不会以任何方式处理 Windows 用户配置文件。

处理的组

可以使用计算机本地组和域组（本地、全局和通用）。必须使用以下格式指定域组：域名\组名。

如果此处配置了该策略，Profile Management 将只处理这些用户组的成员。如果禁用此策略，Profile Management 将处理所有用户。如果未在此处配置此策略，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，则将处理所有用户组的成员。

排除的组

可以使用计算机本地组和域组（本地组、全局组和通用组）以禁止处理特定用户配置文件。按“域名\组名”格式指定域组。

如果此处配置了此设置，Profile Management 将排除这些用户组的成员。如果已禁用此设置，Profile Management 将不会排除任何用户。如果未在此处配置此设置，则将使用.ini 文件中的值。如果未在此处也未在.ini 文件中配置此设置，则不会排除任何组的成员。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

处理本地管理员登录

指定是否处理 BUILTIN\Administrators 组成员的登录。如果此策略已禁用，或者未在多会话操作系统（例如 Citrix Virtual Apps 环境）中进行配置，Profile Management 将假定必须处理以域用户而不是本地管理员身份进行的登录。在单会话操作系统（例如 Citrix Virtual Desktops 环境）中，会处理以本地管理员身份进行的登录。此策略允许具有本地管理员权限的域用户（通常是具有分配的虚拟桌面的 Citrix Virtual Desktops 用户），跳过任何处理过程、登录以及对出现 Profile Management 问题的桌面进行故障排除。

注意：域用户的登录可能受到组成员身份所造成的各种限制的约束，这样通常可以确保符合产品许可的要求。
如果禁用了此策略，Profile Management 将不处理本地管理员的登录。如果未在此处配置此策略，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，则不处理管理员。

用户存储路径

可以设置用于保存用户设置（注册表更改和同步文件）的目录（用户存储）路径。

路径可以是：

- 相对路径。此路径必须是相对于主目录的路径（主目录通常配置为 Active Directory 中用户的 #homeDirectory# 属性）。
- 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。

可以对此策略使用以下类型的变量：

- 百分号括起的系统环境变量（例如%ProfVer%）。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 变量产品文档。

请勿使用其他用户环境变量（%username% 和 %userdomain% 除外）。也可以创建自定义属性，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$%USERNAME%.%USERDOMAIN%!CTX_OSNAME!!CTX_OSBITNESS! 可能会扩展为 \server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64

重要：无论使用哪种属性或变量，均请确认此策略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$\JohnSmith.Finance\Win8x64\UPM_Profile 中，应将用户存储路径设置为 \server\profiles$\JohnSmith.Finance\Win8x64（而非 \UPM_Profile 子文件夹）。

有关如何使用变量指定用户存储路径的详细信息，请参阅以下主题：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 在多个文件服务器上共享 Citrix 用户配置文件
- 在 OU 内和跨 OU 管理配置文件
- Profile Management 的高可用性和灾难恢复

如果用户存储路径已禁用，用户设置将保存在主目录的 Windows 子目录中。

如果禁用该策略，会将用户设置保存在主目录的 Windows 子目录中。如果未在此处配置此策略，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，则将使用主驱动器上的 Windows 目录。

迁移用户存储

指定之前保存用户设置（注册表更改和同步的文件）的文件夹的路径（之前使用的用户存储路径）。

如果配置了此设置，存储在之前的用户存储中的用户设置将迁移到在“用户存储路径”策略中指定的当前用户存储。

该路径可以是绝对 UNC 路径，也可以是相对于主目录的路径。

在这两种情况下，可以使用以下类型的变量：以一对百分号括起的系统环境变量，以及以一对井号括起的 Active Directory 用户对象的属性。

示例：

- 文件夹 `Windows\\%ProfileVer%` 存储用户存储的 `Windows\W2K3` 子文件夹中的用户设置（如果%ProfileVer% 是解析为 W2K3 的系统环境变量）。
- `\\server\share\\#SAMAccountName#` 将用户设置存储到 UNC 路径 `\\server\share\<JohnSmith>` 中（如果 `#SAMAccountName#` 解析为当前用户 JohnSmith）。

在该路径中，您可以使用除 %`username`% 和 %`userdomain`% 以外的用户环境变量。

如果禁用此设置，用户设置将保存在当前用户存储中。

如果未在此处配置此设置，则将使用.ini 文件中的相应设置。

如果未在此处也未在.ini 文件中配置此设置，用户设置将保存在当前用户存储中。

主动回写

可以在会话过程中、注销之前将修改的文件或文件夹（但不包括注册表项）同步到用户存储。

如果未在此处配置此策略，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，则将处于启用状态。

脱机配置文件支持

此策略使配置文件能够尽早与用户存储进行同步。该策略适用于使用便携式计算机或移动设备的漫游用户。当网络连接断开时，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，其上的配置文件仍然会保持不变。移动设备用户开始工作时，其配置文件将在本地更新，并最终在重新建立网络连接时与用户存储进行同步。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

如果未在此处配置此策略，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，则将禁用脱机配置文件。

主动回写注册表

将此策略与“主动回写”结合使用。可以在会话过程中将修改的注册表项同步到用户存储。

如果未在此处配置此设置，则将使用.ini 文件中的值。

如果未在此处或.ini 文件中配置此设置，则将禁用主动回写注册表。

脱机配置文件支持

启用脱机配置文件功能。此功能适用于断开网络的计算机，通常是笔记本电脑或移动设备，而不是服务器或台式机。

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，则将禁用脱机配置文件支持。

跨平台策略设置

November 17, 2021

本部分包含与配置 Profile Management 跨平台设置功能有关的策略设置。

启用跨平台设置

默认情况下，为便于部署，会禁用跨平台设置。通过启用该策略可启动处理，但仅在对此功能进行彻底的规划和测试之后。

如果未在此处配置此策略，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，则将不应用任何跨平台设置。

跨平台设置用户组

输入一个或多个 Windows 用户组。例如，可以使用该策略仅处理来自测试用户组的配置文件。如果配置了此策略，Profile Management 的跨平台设置功能将仅处理这些用户组的成员。如果未禁用此策略，该功能将处理由处理的组策略指定的所有用户。

如果未在此处配置此策略，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，则将处理所有用户组。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

跨平台定义路径

确定从下载软件包中复制的定义文件所在的网络位置。此路径必须是一个 UNC 路径。用户必须对此位置具有读取权限，而管理员必须对其具有写入权限。此位置必须是一个服务器消息块 (Server Message Block, SMB) 或通用 Internet 文件系统 (Common Internet File System, CIFS) 文件共享。

如果未在此处配置此策略，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，则将不应用任何跨平台设置。

跨平台设置存储路径

设置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。用户必须对此区域具有写入权限。该路径可以是绝对 UNC 路径，也可以是相对于主目录的路径。

此区域是多个平台共享的配置文件数据所在的用户存储的公共区域。用户必须对此区域具有写入权限。该路径可以是绝对 UNC 路径，也可以是相对于主目录的路径。可以与用户存储路径使用相同的变量。

如果禁用该策略，则将使用路径 Windows\PM_CP。如果未在此处配置此策略，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，则将使用默认值。

创建跨平台设置的来源

如果在平台的 OU 中启用此策略，则指定该平台为基础平台。此策略可将数据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。您必须决定使用哪个平台的配置文件数据来生成跨平台设置存储。此平台称为基础平台。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，则除非您禁用该策略，否则 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 或多个用户或计算机对象中启用此策略，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，此策略处于“已启用”状态。

文件系统策略设置

November 17, 2021

本部分包含的策略用于设置用户配置文件中的哪些文件和目录在安装了配置文件的系统与用户存储之间进行同步。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

排除策略设置

November 17, 2021

本部分包含的策略设置用于配置将用户配置文件中的哪些文件和目录从同步过程中排除。

排除列表 - 文件

同步期间忽略的文件的列表。文件名必须为与用户配置文件 (%USERPROFILE%) 相对的路径。允许使用通配符，但应递归应用。

示例：

- Desktop\Desktop.ini 将忽略 Desktop 文件夹中的文件 Desktop.ini
- %USERPROFILE%*.tmp 将忽略整个配置文件中扩展名为.tmp 的所有文件
- AppData\Roaming\MyApp*.tmp 将忽略其中一部分配置文件中扩展名为.tmp 的所有文件

如果禁用此策略，将不会排除任何文件。如果未在此处配置此策略，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，则不会排除任何文件。

启用默认排除列表 - 目录

同步过程中将忽略默认目录列表。使用此策略可指定 GPO 排除目录，不需要手动填充。

如果禁用了此策略，Profile Management 默认将不排除任何目录。如果未在此处配置此策略，Profile Management 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，Profile Management 默认将不排除任何目录。

排除列表 - 目录

同步期间忽略的文件夹的列表。必须将文件夹名称指定为与用户配置文件 (%USERPROFILE%) 相对的路径。

示例：

- 输入 Desktop 将忽略用户配置文件中的 Desktop 文件夹

如果禁用此策略，将不会排除任何文件夹。如果未在此处配置此策略，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，则不会排除任何文件夹。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

登录排除项检查

此设置配置 Profile Management 在用户存储中的配置文件包含被排除的文件或文件夹时需要执行的操作。

如果此设置处于禁用状态或者设置为默认值“登录时同步排除的文件或文件夹”，Profile Management 将在用户登录时将这些排除的文件或文件夹从用户存储同步到本地配置文件。

如果此设置设为“登录时忽略排除的文件或文件夹”，Profile Management 将在用户登录时忽略用户存储中被排除的文件或文件夹。

如果此设置设为“登录时删除排除的文件或文件夹”，Profile Management 将在用户登录时删除用户存储中被排除的文件或文件夹。

如果未在此处配置此设置，则将使用.ini 文件中的值。

如果未在此处或.ini 文件中配置此设置，则会在用户登录时将排除的文件或文件夹从用户存储同步到本地配置文件。

大型文件处理 **-** 要以符号链接方式创建的文件

为了提高登录性能并处理大型文件，请创建符号链接而不是复制此列表中的文件。

可以在引用文件的策略中使用通配符；例如 `!ctx_localappdata!\Microsoft\Outlook\*.OST`。

要处理 Microsoft Outlook 的脱机文件夹文件 (`*.ost`)，请确保不要为 Profile Management 排除 **Outlook** 文件夹。

不能同时在多个会话中访问这些文件。

同步策略设置

November 17, 2021

同步部分包含的策略设置用于指定将在安装配置文件的系统与用户存储之间同步用户配置文件中的哪些文件和文件夹。

同步的目录

Profile Management 在安装了 Profile Management 的系统与用户存储之间，同步每个用户的完整配置文件。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。

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）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

禁用此策略与启用此策略并配置空列表具有相同的效果。

如果未在此处配置此策略，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，则将仅对用户配置文件中没有排除的文件夹进行同步。

同步的文件

Profile Management 在安装了 Profile Management 的系统与用户存储之间，同步每个用户的完整配置文件。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。

此策略可用于包括下列排除的文件夹中的文件。该列表中的路径必须是相对于用户配置文件的路径。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

禁用此策略与启用此策略并配置空列表具有相同的效果。

如果未在此处配置此策略，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，则将仅会对用户配置文件中没有排除的文件夹进行同步。

要镜像的文件夹

此策略可以帮助解决与任何事务性文件夹（也称为引用文件夹）有关的问题。该文件夹包含相互依赖的文件，即其中一个文件会引用其他文件。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。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。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将被最后一次更新覆盖，导致配置文件更改丢失。

例如，考虑一下用户浏览 Internet 时 Index.dat 如何引用 Cookie。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，前提是配置了主动回写功能），第二个会话中的 cookie 必须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 覆盖这些 cookie。因此，Index.dat 将保持最新。

如果未在此处配置此策略，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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

加快文件夹镜像速度

启用此策略和 **Folders to mirror**（要镜像的文件夹）策略后，Profile Management 将镜像的文件夹存储在基于 vHDX 的虚拟磁盘上。它会在登录期间附加虚拟磁盘，并在注销时将其分离。启用此策略无需在用户存储与本地配置文件之间复制文件夹，并加快文件夹镜像速度。

文件夹重定向策略设置

November 17, 2021

本部分包含的策略设置用于指定是否将经常出现在配置文件中的文件夹重定向到共享网络位置。

授予管理员访问权限

此设置使管理员可以访问用户重定向的文件夹的内容。

> 注意：
>
> 此设置可向对域具有完整且不受限制的访问权限的管理员授予相应权限。

默认情况下，此设置处于禁用状态，用户被授予独占访问其重定向文件夹内容的权限。

包含域名

此设置允许将 %`userdomain`% 环境变量包含在为重定向文件夹指定的 UNC 路径中。

默认情况下，此设置处于禁用状态，%`userdomain`% 环境变量不包括在为重定向文件夹指定的 UNC 路径中。

“**AppData (**漫游**)**”策略设置

November 17, 2021

本部分包含将 **AppData(Roaming)** 文件夹的内容重定向到共享网络位置的策略设置。

“**AppData(**漫游**)**”路径

此设置指定 **AppData(Roaming)** 文件夹的内容将重定向到的网络位置。

默认情况下，此设置处于禁用状态，不指定任何位置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

“**AppData (**漫游**)**”的重定向设置

此设置指定如何重定向 **AppData(Roaming)** 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

November 17, 2021

本部分包含将联系人文件夹的内容重定向到共享网络位置的策略设置。

“联系人”路径

此设置指定联系人文件夹的内容将重定向到的网络位置。

默认情况下，此设置处于禁用状态，不指定任何位置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“联系人”的重定向设置

此设置指定如何重定向联系人文件夹的内容。

默认情况下，内容重定向到 UNC 路径。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

桌面策略设置

November 17, 2021

本部分包含用于将 `Desktop` 文件夹的内容重定向到共享网络位置的策略设置。

“桌面”路径

此设置指定桌面文件夹的内容将重定向到的网络位置。

默认情况下，此设置处于禁用状态，不指定任何位置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

“桌面”的重定向设置

此设置指定如何重定向桌面文件夹的内容。

默认情况下，内容重定向到 UNC 路径。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“文档”策略设置

November 17, 2021

本部分包含将文档文件夹的内容重定向到共享网络位置的策略设置。

“文档”路径

此设置指定文档文件夹中的文件将重定向到的网络位置。

默认情况下，此设置处于禁用状态，不指定任何位置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

必须启用文档路径设置，以将文件重定向到文档文件夹，同时将文件重定向到音乐、图形和视频文件夹。

“文档”的重定向设置

此设置指定如何重定向文档文件夹的内容。

默认情况下，内容重定向到 UNC 路径。

要控制如何重定向文档文件夹的内容，请选择以下选项之一：

- 重定向到以下 UNC 路径。将内容重定向到“文档”路径策略设置中指定的 UNC 路径。
- 重定向到用户的主目录。将内容重定向到用户主目录，通常配置为 Active Directory 中用户的 #homeDirectory# 属性。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“下载”策略设置

November 17, 2021

本部分包含将下载文件夹的内容重定向到共享网络位置的策略设置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

“下载”路径

此设置指定下载文件夹中的文件将重定向到的网络位置。

默认情况下，此设置处于禁用状态，不指定任何位置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“下载”的重定向位置

此设置指定如何重定向下载文件夹的内容。

默认情况下，内容重定向到 UNC 路径。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“收藏夹”策略设置

November 17, 2021

本部分包含将收藏夹文件夹的内容重定向到共享网络位置的策略设置。

“收藏夹”路径

此设置指定收藏夹文件夹的内容将重定向到的网络位置。

默认情况下，此设置处于禁用状态，不指定任何位置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“收藏夹”的重定向设置

此设置指定如何重定向收藏夹文件夹。

默认情况下，内容重定向到 UNC 路径。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“链接”策略设置

November 17, 2021

本部分包含将链接文件夹的内容重定向到共享网络位置的策略设置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

“链接”路径

此设置指定链接文件夹的内容将重定向到的网络位置。

默认情况下，此设置处于禁用状态，不指定任何位置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“链接”的重定向设置

此设置指定如何重定向链接文件夹的内容。

默认情况下，内容重定向到 UNC 路径。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“音乐”策略设置

November 17, 2021

本部分包含将音乐文件夹的内容重定向到共享网络位置的策略设置。

“音乐”路径

此设置指定音乐文件夹的内容将重定向到的网络位置。

默认情况下，此设置处于禁用状态，不指定任何位置。

如果未在此处配置此设置，Profile Management 将不会重定向指定文件夹。

“音乐”的重定向设置

此设置指定如何重定向音乐文件夹的内容。

默认情况下，内容重定向到 UNC 路径。

要控制如何重定向音乐文件夹的内容，请选择以下选项之一：

- 重定向到以下 UNC 路径。将内容重定向到“音乐”路径策略设置中指定的 UNC 路径。
- 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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

“图片”策略设置

November 17, 2021

本部分包含将图片文件夹的内容重定向到共享网络位置的策略设置。

“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

November 17, 2021

本部分包含将保存的游戏文件夹的内容重定向到共享网络位置的策略设置。

“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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

“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。

“开始”菜单策略设置

November 17, 2021

本部分包含将开始菜单文件夹的内容重定向到共享网络位置的策略设置。

“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。

“搜索”策略设置

November 17, 2021

本部分包含将搜索文件夹的内容重定向到共享网络位置的策略设置。

“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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

“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。

“视频”策略设置

November 17, 2021

本部分包含将视频文件夹的内容重定向到共享网络位置的策略设置。

“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

November 17, 2021

本部分包含的策略设置用于配置 Profile Management 日志记录。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

文件系统操作

此设置启用或禁用对文件系统中执行的操作进行详细日志记录。

默认情况下，禁用此设置。

启用此设置时，请确保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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

日志文件最大大小

此设置指定 Profile Management 日志文件的最大允许大小（以字节为单位）。

默认情况下，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，则将使用默认值。

日志文件路径

此设置指定用于保存 Profile Management 日志文件的备用路径。

默认情况下,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，但可能会产生大量网络流量，对日志文件来说可能不适合。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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

登录及注销时的策略值

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

此设置启用或禁用在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

November 17, 2021

本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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

删除缓存的配置文件之前的延迟

此设置指定注销时 Profile Management 在删除本地缓存的配置文件之前的可选延迟时间（分钟）。

值为 0 时会在注销过程结束时立即删除配置文件。Profile Management 每分钟检查一次注销，因此值为 60 可确保在用户注销后一到两分钟内删除配置文件（取决于最后一次检查的时间）。如果已知注销期间进程会使文件或用户注册表配置单元处于打开状态，延长延迟时间将很有用。对于大型配置文件，这种做法还可以加快注销速度。

默认情况下，此参数设置为 0，Profile Management 会立即删除本地缓存的配置文件。

启用此设置时，请确保注销时删除本地缓存的配置文件也处于启用状态。

如果未在此处配置此设置，则将使用.ini 文件中的值。

如果在此处和.ini 文件中均未配置此设置，则会立即删除配置文件。

Delete locally cached profiles on logoff（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 建议您为端点服务器启用此设置。

默认情况下，此设置处于禁用状态，用户注销后，将继续保留用户本地配置文件缓存。

如果未在此处配置此设置，则将使用.ini 文件中的值。

如果该设置没有在此配置，也不在 INI 文件中，则不会删除缓存的配置文件。

本地配置文件冲突处理

If you enable the Citrix Personalization for App-V - VDA check box 在既存在用户存储中的用户配置文件，又存在本地 Windows 用户配置文件（非 Citrix 用户配置文件）的情况下，此设置用于配置 Profile Management 的行为。

默认情况下，Profile Management 将使用本地 Windows 配置文件，但不通过任何方式更改该配置文件。

要控制 Profile Management 的行为，请选择以下选项之一：

- Use local profile（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。
- Delete local profile（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。
- Rename local profile（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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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
- 本地
- 漫游
- 无（已禁用）

如果选择无，系统将使用现有 Windows 机制创建配置文件，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。

自动迁移现有应用程序配置文件

此设置将启用或禁用跨不同操作系统自动迁移现有应用程序配置文件。应用程序配置文件包括 AppData 文件夹中的应用程序数据以及 HKEY_CURRENT_USER\SOFTWARE 下的注册表项。如果您希望跨不同操作系统迁移应用程序配置文件，此设置会非常有用。

例如，假设您将操作系统 (OS) 从 Windows 10 版本 1803 升级到 Windows 10 版本 1809。如果启用此设置，Profile Management 会在每个用户首次登录时自动将现有应用程序设置迁移到 Windows 10 版本 1809。因此，将迁移 AppData 文件夹中的应用程序数据以及 HKEY_CURRENT_USER\SOFTWARE 下的注册表项。

如果存在多个现有应用程序配置文件，Profile Management 将按以下优先级顺序执行迁移：

1. 相同操作系统类型的配置文件（单会话操作系统到单会话操作系统和多会话操作系统到多会话操作系统）。
2. 相同 Windows 操作系统系列的配置文件；例如，Windows 10 到 Windows 10，或者 Windows Server 2016 到 Windows Server 2016。
3. 早期版本的操作系统的配置文件；例如，Windows 7 到 Windows 10，或 Windows Server 2012 到 Windows 2016。
4. 最新操作系统的配置文件。

注意：必须通过在用户存储路径中包含变量!CTX_OSNAME! 来指定操作系统的短名称。这样将允许 Profile Management 查找现有应用程序配置文件。

如果未在此处配置此设置，则将使用.ini 文件中的设置。

如果未在此处也未在.ini 文件中配置此设置，默认处于禁用状态。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

模板配置文件的路径

此设置指定希望 Profile Management 用来创建用户配置文件的模板配置文件的路径。

指定的路径必须为文件夹的完整路径，其中包含 NTUSER.DAT 注册表文件以及模板配置文件所需的其他任何其他文件夹和文件。

注意：请勿在路径中包括 NTUSER.DAT。例如，对于文件 \\myservername\myprofiles\template\ntuser.dat，应将路径设置为 \\myservername\myprofiles\template。

应使用绝对路径，绝对路径可以是 UNC 路径，也可以是本地计算机上的路径。例如，可以使用后者指定永久存在于 Citrix Provisioning Services 映像中的模板配置文件。不支持相对路径。

注意：此设置不支持扩展 Active Directory 属性、系统环境变量或 %USERNAME% 和 %USERDOMAIN% 变量。

默认情况下，此设置处于禁用状态，系统将根据用户首次登录的设备上的默认用户配置文件创建新用户配置文件。

如果未在此处配置此设置，则将使用.ini 文件中的值。

如果未在此处也未在.ini 文件中配置此设置，则不使用任何模板。

模板配置文件覆盖本地配置文件

此设置允许在创建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用户配置文件时所使用的本地配置文件。

如果未在此处配置此设置，则将使用.ini 文件中的值。

如果未在此处也未在.ini 文件中配置此设置，则不使用任何模板。

模板配置文件覆盖漫游配置文件

此设置可在创建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。

如果未在此处也未在.ini 文件中配置此设置，则不使用任何模板。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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用户配置文件时使用的默认配置文件。

默认情况下，此设置处于禁用状态，系统将根据用户首次登录的设备上的默认用户配置文件创建新用户配置文件。

如果未在此处配置此设置，则将使用.ini 文件中的值。

如果未在此处也未在.ini 文件中配置此设置，则不使用任何模板。

“注册表”策略设置

November 17, 2021

本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

注销时忽略的 HKCU 配置单元中的注册表项列表。

示例：Software\Policies

如果禁用此策略，则不会排除任何注册表项。如果未在此处配置此策略，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，则不会排除任何注册表项。

包含列表

注销时处理的 HKCU 配置单元中的注册表项列表。

示例：Software\Adobe。

如果启用此策略，将仅处理此列表中的项。如果禁用此策略，将处理整个 HKCU 配置单元。如果未在此处配置此策略，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，则将处理整个 HKCU。

启用默认排除列表 **- Profile Management 5.5**

HKCU 配置单元中未同步到用户的配置文件的默认注册表项列表。使用此策略可指定 GPO 排除文件，不需要手动填充。

如果禁用了此策略，Profile Management 默认将不排除任何注册表项。如果未在此处配置此策略，Profile Management 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，Profile Management 默认将不排除任何注册表项。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

NTUSER.DAT 备份

启用 NTUSER.DAT 的上次已知的良好副本的备份并在出现损坏时回滚。

如果未在此处配置此策略，Profile Management 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，Profile Management 将不备份 NTUSER.DAT。

“流用户配置文件”策略设置

January 21, 2022

本部分包含的策略设置用于指定 Profile Management 处理流用户配置文件的方式。

总是缓存

此设置指定 Profile Management 在用户登录后是否立即缓存流文件。在用户登录后缓存文件可以节省网络带宽，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，此值设置为 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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。

启用 **Profile Streaming** 排除

启用 Profile Streaming 排除后，Profile Management 不会对排除列表中的文件夹执行流操作，用户登录时，所有文件夹会立即从用户存储中提取到本地计算机。

有关详细信息，请参阅通过流技术推送用户配置文件。

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，则将使用默认值。

用户个性化层策略设置

January 21, 2022

要在 Virtual Delivery Agent 中启用用户层的装载，请使用配置参数指定：

- 在网络上访问用户层的位置。
- 任何新用户层磁盘可以增加的大小。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

为此，这两个策略将显示在可用策略列表中：

- 用户层存储库路径 - 在“值”字段中输入格式为“\服务器名称或地址\文件夹名称”的路径。
- 用户层大小 (GB) - 默认用户层大小 10 GB 是我们建议的最小值。用户层是精简预配的磁盘，随着空间的使用而扩展到设置的大小。用户层的大小永远不会减小。

> 注意：
>
> 增加用户层大小会影响新用户层并扩展现有用户层。减小层大小仅影响新用户层。现有用户层的大小永远不会减小。

有关详细信息，请参阅用户个性化层。

Virtual Delivery Agent 策略设置

November 17, 2021

Virtual Delivery Agent (VDA) 部分包含的策略设置可以控制 VDA 与站点控制器之间的通信。

重要：如果没有使用自动更新功能，VDA 需要使用这些设置提供的信息向 Delivery Controller 注册。由于此信息是进行注册所必需的信息，因此，除非在 VDA 安装期间提供了此信息，否则必须使用组策略编辑器配置下列设置：

- 控制器注册 IPv6 网络掩码
- 控制器注册端口
- 控制器 SID
- 控制器
- 仅使用 IPv6 控制器注册
- 站点 GUID

控制器注册 IPv6 网络掩码

此策略设置允许管理员将 VDA 限制为仅在首选的子网（而非全局 IP，如果已注册）中使用。此设置指定 VDA 要注册的 IPv6 地址和网络。VDA 将仅在与指定网络掩码匹配的第一个地址上进行注册。仅当启用仅使用 IPv6 控制器注册策略设置时，此设置才有效。

默认情况下，此设置为空。

控制器注册端口

仅当禁用启用控制器自动更新设置时，才使用此设置。

此设置指定 VDA 向控制器注册时所用的 TCP/IP 端口号（如果使用基于注册表的注册方式）。

默认情况下，此端口号设置为 80。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

HDX 3D Pro 策略设置

November 17, 2021

HDX 3D Pro 部分包含用于为用户启用和配置图像质量配置工具的策略设置。该工具使用户能够实时调整图像质量与响应速度之间的平衡点，从而优化对可用带宽的使用情况。

启用无损

此设置指定用户是否能够使用图像质量配置工具启用和禁用无损压缩功能。默认情况下，用户可以选择启用无损压缩功能。

用户启用无损压缩功能后，图像质量将自动设置为在图像配置工具中可用的最大值。默认情况下，可以根据用户设备和主机计算机的功能，使用基于 GPU 或 CPU 的压缩。

HDX 3D Pro 质量设置

此设置指定图像质量配置工具中用于定义用户可用的图像质量调整范围的最小值和最大值。

可以指定 0 到 100 之间（包括 0 和 100）的图像质量值。最大值必须大于或等于最小值。

监视策略设置

January 21, 2022

“监视”部分包含用于进程、资源监视和应用程序故障监视的策略设置。

这些策略的作用域可以根据站点、交付组、交付组类型、组织单位和标记进行定义。

用于进程和资源监视的策略

CPU、内存和进程的每个数据点均通过 VDA 收集，并存储在监视数据库中。发送来自 VDA 的数据点会消耗网络带宽，存储这些数据点会占用监视数据库中的大量空间。如果您不想监视某一特定作用域（例如，特定的交付组或组织单位）的资源数据或/和进程数据，建议您禁用此策略。

启用进程监视

启用此设置以通过 VDA 监视计算机上运行的进程。诸如 CPU 和内存使用等统计信息会发送至 Monitoring Service。该统计信息用于 Director 中的实时通知和历史报告。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

此设置默认情况下为禁用。

启用资源监视

启用此设置以通过 VDA 监视计算机上的关键性能计数器。统计信息（例如 CPU 和内存数据、IOPS 和磁盘延迟数据）会发送至 Monitoring Service。该统计信息用于 Director 中的实时通知和历史报告。

此设置默认情况下为启用。

可扩展性

CPU 和内存数据每隔 5 分钟从每个 VDA 推送到数据库一次。流程数据（如果已启用）每隔 10 分钟推送到数据库一次。IOPS 和磁盘延迟数据按 1 小时间隔推送至数据库。

CPU 和内存数据

默认情况下，CPU 和内存数据处于启用状态。数据保留期限值如下（Platinum 许可证）：

数据粒度	天数
5 分钟数据	1 天
10 分钟数据	7 天
小时数据	30 天
日数据	90 天

IOPS 和磁盘延迟数据

默认情况下，IOPS 和磁盘延迟数据处于已启用状态。数据保留期限值如下（Platinum 许可证）：

数据粒度	天数
小时数据	3 天
日数据	90 天

根据数据保留期限设置，大约需要 276 KB 的磁盘空间即可存储一个 VDA 一年时间的 CPU、内存、IOPS 和磁盘延迟数据。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

计算机数	所需的大约存储
1	276 KB
1K	270 MB
40K	10.6 GB

进程数据

默认情况下，进程数据处于已禁用状态。建议根据需要对一部分计算机启用进程数据。进程数据的默认数据保留设置如下：

数据粒度	天数
10 分钟数据	1 天
小时数据	7 天

如果进程数据已启用，在使用默认保留设置的情况下，进程数据在为期一年的时间内每 VDA 会消耗大约 1.5 MB，每端点服务 VDA (TS VDA) 会消耗大约 3 MB。

计算机数	VDA 所需的大约存储	TS VDA 所需的大约存储
1	1.5 MB	3 MB
1K	1.5 GB	3 GB

> 注意：
>
> 之前提供的数字不包括索引空间。同时，所有计算为近似计算，根据部署的不同而有所不同。

可选配置

您可以修改默认保留期限设置以满足您的需求。但是，这会占用额外的存储空间。通过启用以下设置，您可以获得更高的进程利用率数据准确性。可以启用的配置为：

EnableMinuteLevelGranularityProcessUtilization

EnableDayLevelGranularityProcessUtilization

这些配置可以通过 Monitoring PowerShell cmdlet 来启用：Set-MonitorConfiguration

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

应用程序故障监视策略

默认情况下，应用程序故障选项卡仅显示多会话操作系统 VDA 中的应用程序故障。可以通过以下监视策略修改应用程序故障监视的设置：

启用应用程序故障的监视

使用此设置可配置应用程序故障监视，以监视应用程序错误或故障（崩溃和未处理的异常），或者监视两者。
通过将值设置为无禁用应用程序故障监视。
此设置的默认值为“仅限应用程序故障”。

在单会话操作系统 **VDA** 上启用应用程序故障的监视

默认情况下，仅监视多会话操作系统 VDA 上托管的应用程序中的故障。要监视单会话操作系统 VDA，请将此策略设置为允许。
此设置的默认值为禁止。

从故障监视中排除的应用程序列表

指定不监视其故障的应用程序的列表。
此列表默认为空。

存储计划提示

组策略。如果您对监视资源数据或进程数据不感兴趣，可以使用组策略来关闭两者或其中之一。有关详细信息，请参阅创建策略的“组策略”部分。

数据整理。可以对默认的数据保留设置进行修改，以尽早整理数据并释放存储空间。有关整理设置的详细信息，请参阅使用 API 访问数据中的数据粒度和保留。

虚拟 **IP** 策略设置

November 17, 2021

> 重要：
>
> Windows 10 Enterprise 多会话不支持远程桌面 IP 虚拟化（虚拟 IP），我们不支持 Windows 10 Enterprise 多会话上的虚拟 IP 或虚拟环回。

“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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

January 21, 2022

在 VDA 版本 7.0 到 7.8 中，COM 端口和 LPT 端口设置只能使用注册表进行配置。对于 7.0 之前的 VDA 版本和 VDA 7.9 及更高版本，这些设置可以在 Studio 中进行配置。有关详细信息，请参阅端口重定向策略设置和带宽策略设置。

用于 COM 端口和 LPT 端口重定向的策略设置位于 VDA 映像或计算机上的 HKLM\Software\Citrix\GroupPolicy\Defaults\Depre 下方。

要启用 COM 端口和 LPT 端口重定向，请添加类型为 REG_DWORD 的新注册表项，如下所示：

小心：注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

注册表项	说明	允许使用的值
AllowComPortRedirection	允许或禁止使用 COM 端口重定向	1（允许）或 0（禁止）
LimitComBw	COM 端口重定向通道的带宽限制	数值
LimitComBWPercent	COM 端口重定向通道的带宽限制（占总会话带宽的百分比）	0 到 100 之间的数值
AutoConnectClientComPorts	从用户设备自动连接 COM 端口	1（允许）或 0（禁止）
AllowLptPortRedirection	允许或禁止使用 LPT 端口重定向	1（允许）或 0（禁止）
LimitLptBw	LPT 端口重定向通道的带宽限制	数值
LimitLptBwPercent	LPT 端口重定向通道的带宽限制（占总会话带宽的百分比）	0 到 100 之间的数值
AutoConnectClientLptPorts	从用户设备自动连接 LPT 端口	1（允许）或 0（禁止）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

配置这些设置后，请更改您的计算机目录，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

November 17, 2021

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 管理的多会话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。对于手动管理的单会话操作系统目录，使用 Configuration Manager 通知用户。对于由 Provisioning Services 管理的单会话操作系统目录，使用 Provisioning Services 通知用户。

警告频率时间间隔

此设置定义将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 0–999 之间的可选参数。
- hh 为介于 0–23 之间的小时数。
- mm 为介于 0–59 之间的分钟数。
- ss 是介于 0–59 之间的秒数。

默认情况下，时间间隔设置为 1 小时 (01:00:00)。

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} 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。）

警告消息框标题

此设置包含显示给用户的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）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

警告时间段

此设置定义在维护前多久首次显示警告消息。

时间使用 ddd.hh:mm:ss 格式进行设置，其中：

- ddd 代表天数，是介于 0–999 之间的可选参数。
- hh 为介于 0–23 之间的小时数。
- mm 为介于 0–59 之间的分钟数。
- ss 是介于 0–59 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 0–999 之间的可选参数。
- hh 为介于 0–23 之间的小时数。
- mm 为介于 0–59 之间的分钟数。
- ss 是介于 0–59 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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

默认情况下，此消息中包含以下内容：“{TIMESTAMP} 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。）

强制注销消息文本框标题

此设置包含强制注销消息的标题栏的可编辑文本。

默认情况下，标题为：“Notification From IT Staff”（来自 IT 人员的通知）

托管映像模式

Connector Agent 将自动检测其是在 Provisioning Services 还是 MCS 管理的计算机克隆上运行。该 Agent 会阻止 Configuration Manager 在托管映像克隆上更新，并自动在目录的主映像上安装更新。

更新主映像后，请使用 Studio 调配 MCS 目录克隆的重新启动行为。在 Configuration Manager 维护时段，Connector Agent 将自动调配 PVS 目录克隆的重新启动行为。要覆盖此行为以便软件由 Configuration Manager 安装在目录克隆上，请将托管映像模式更改为已禁用。

重新启动消息框正文文本

此设置包含可编辑的消息文本，用于在服务器即将重新启动时通知用户。

默认情况下，消息为：“The server is currently going offline for maintenance.”（服务器当前即将脱机进行维护。）

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 0–999 之间的可选参数。
- hh 为介于 0–23 之间的小时数。
- mm 为介于 0–59 之间的分钟数。
- ss 是介于 0–59 之间的秒数。

默认情况下，常规时间间隔设置为 5 分钟 (00:05:00)。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

管理

January 21, 2022

管理 Citrix Virtual Apps and Desktops 站点涵盖各种项目和任务。

许可

创建站点时，需要与 Citrix 许可证服务器建立有效连接。之后，可以从 Studio 完成各种许可任务，包括添加许可证、更改许可证类型或模式以及管理许可证管理员。还可以从 Studio 访问许可证管理控制台。

应用程序

管理交付组和应用程序组（可选）中的应用程序。

区域

在地理位置分散的部署中，可以使用区域使应用程序和桌面距离用户更近，这样可以改善性能。安装和配置站点时，所有 Controller、计算机目录和主机连接位于一个主要区域中。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，可以指定任何新创建的计算机目录、主机连接或添加的 Controller 将位于哪个区域。还可以在区域之间移动项目。

连接和资源

如果要使用虚拟机管理程序或其他服务托管向用户交付应用程序和桌面的计算机，应在创建站点时创建与该虚拟机管理程序或其他服务的第一个连接。该连接的存储和网络详细信息组成了其资源。之后，可以更改此连接及其资源并创建更多连接。您还可以管理使用已配置连接的计算机。

本地主机缓存

本地主机缓存允许在 Delivery Controller 与站点数据库之间的连接失败时站点中的连接代理操作继续执行。

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的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 通信的应用程序配置为使用 localhost 范围之内的唯一虚拟环回地址。

Delivery Controller

本文包含在站点中添加和删除 Controller 时的考虑事项和过程。此外还介绍如何将 Controller 移至另一个区域或站点，以及如何将 VDA 移至另一个站点。

向 Controller 中注册 VDA

VDA 必须向 Controller 注册（建立通信）才能帮助交付应用程序和桌面。可以按多种方式指定 Controller 地址，本文对这些方式进行了介绍。在站点中添加、移动和删除 Controller 时，VDA 及时具有最新信息至关重要。

会话

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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 会话可靠性
- 客户端自动重新连接
- ICA 保持活动状态
- 工作区控制
- 会话漫游

在 **Studio** 中使用搜索

如果希望在 Studio 中查看有关计算机、会话、计算机目录、应用程序或交付组的信息，可使用灵活的搜索功能。

标记

使用标签来识别各个项目，例如计算机、应用程序、组和策略。然后，您可以定制特定操作以应用于带有特定标记的项目。

IPv4/IPv6

Citrix Virtual Apps and Desktops 支持纯 IPv4 部署、纯 IPv6 部署，以及使用重叠 IPv4 和 IPv6 网络的双协议栈部署。本文介绍并举例说明这些部署。本文还介绍控制使用 IPv4 还是 IPv6 的 Citrix 策略设置。

用户配置文件

默认情况下，安装 VDA 会自动安装 Citrix Profile Management。如果您使用此配置文件解决方案，请查看本文以获取常规信息。有关详细信息，请参阅 Profile Management 文档。

收集 Citrix Diagnostic Facility (CDF) 跟踪信息

CDFControl 实用程序是一个事件跟踪控制器或使用方，用来捕获各种 Citrix 跟踪提供程序中显示的 Citrix Diagnostic Facility (CDF) 跟踪消息。此实用程序用来对相关的复杂 Citrix 问题进行故障排除、解析过滤器支持以及收集性能数据。

Citrix Insight Services

Citrix Insight Services (CIS) 是用于性能监测、遥测以及生成业务洞察的 Citrix 平台。

Citrix Scout

Citrix Scout 会收集诊断信息并运行运行状况检查。您可以使用在 Citrix Virtual Apps and Desktops 部署中进行主动维护的结果。Citrix 通过 Citrix Insight Services 提供诊断收集信息的综合的自动分析。您还可以使用 Scout 自己或在 Citrix Support 的指导下对问题进行故障排除。

许可

September 8, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> Studio 和 Director 支持以下版本的 Citrix 许可证服务器虚拟设备：
>
> - v11.16.3.0_29500
> - v11.14.0.1_19800
>
> 确保在支持的 VPX 版本上启用 Citrix Licensing Manager。

有关 Citrix 本地订阅许可证的信息，请参阅年度零售许可证和有期限的零售许可证的 Citrix 本地订阅。

如果许可证服务器与 Studio 位于相同的域内或位于可信域内，则可以通过 Studio 管理和跟踪许可。有关其他许可任务的信息，请参阅许可文档和多类型许可。

您必须是完全权限许可证管理员才能完成本文中介绍的任务（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
Citrix Virtual Apps	Premium、Advanced、Standard	并发
Citrix Virtual Desktops	Premium、Advanced、Standard	用户/设备和并发

有关详细信息，请参阅并发许可证和用户/设备许可证。

支持的当前版本 (CR) 和长期服务版本 (LTSR)

有关受支持的当前版本 (CR)、长期服务版本 (LTSR) 和最低兼容 LS 版本的信息，请参阅 Citrix Virtual Apps and Desktops 当前版本文档。

> 重要：
>
> 许可证服务器 VPX 已弃用，不会收到任何进一步的维护或安全修复。建议使用 11.16.6 或以前版本的许可证服务器 VPX 的客户尽快迁移到最新版本的 Windows 许可证服务器。

查看许可证信息

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。

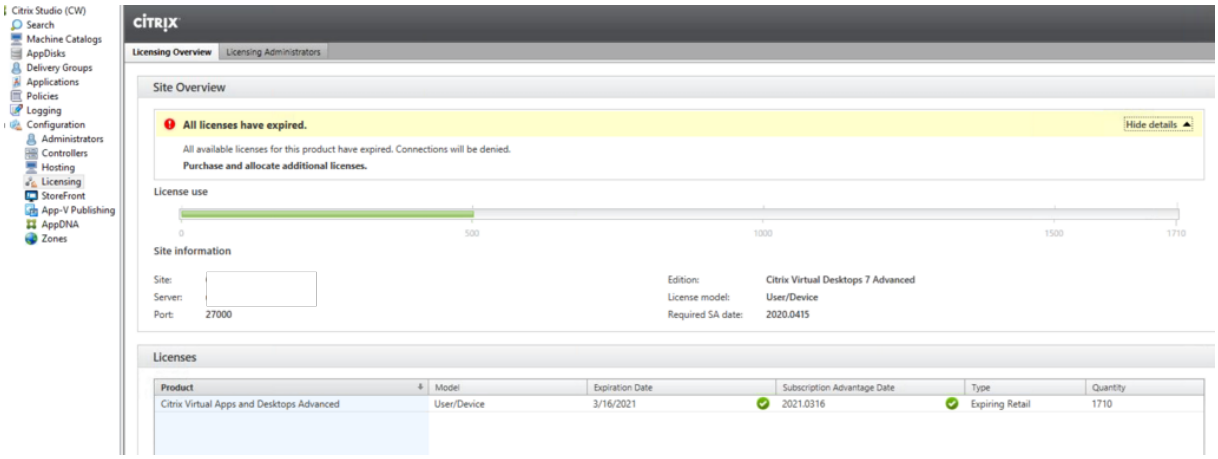
确保站点的许可设置（包括产品类型、许可证版本和许可模式）与您配置的许可证服务器使用的许可证相匹配。否则，您可能必须下载或分配现有许可证以匹配站点的许可证设置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

查看许可证到期警报

Citrix Studio 从 Citrix 许可证服务器中查询许可证文件过期日期。如果许可证文件即将过期或已过期，管理员会收到警报。

您可以在 Studio 用户界面中看到这些警报。下图显示了 Citrix Studio UI 上显示的许可证到期警报。



使用 **Studio** 从 **Citrix** 下载并安装许可证

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，该代码将在购买或续订许可证后在 Citrix 发送的电子邮件中提供。
4. 选择产品并选择分配许可证。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“我的帐户”。

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)。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。

> 注意：
>
> 在 Citrix Studio 中使用的许可证之间切换时（例如，在 Advanced 与 Premium 之间或者反向），更改可能需要 5 分钟才能显示在 Citrix Director 中。

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。

更改许可管理员的权限或删除许可管理员

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，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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

更改许可管理员组的权限或删除许可管理员组

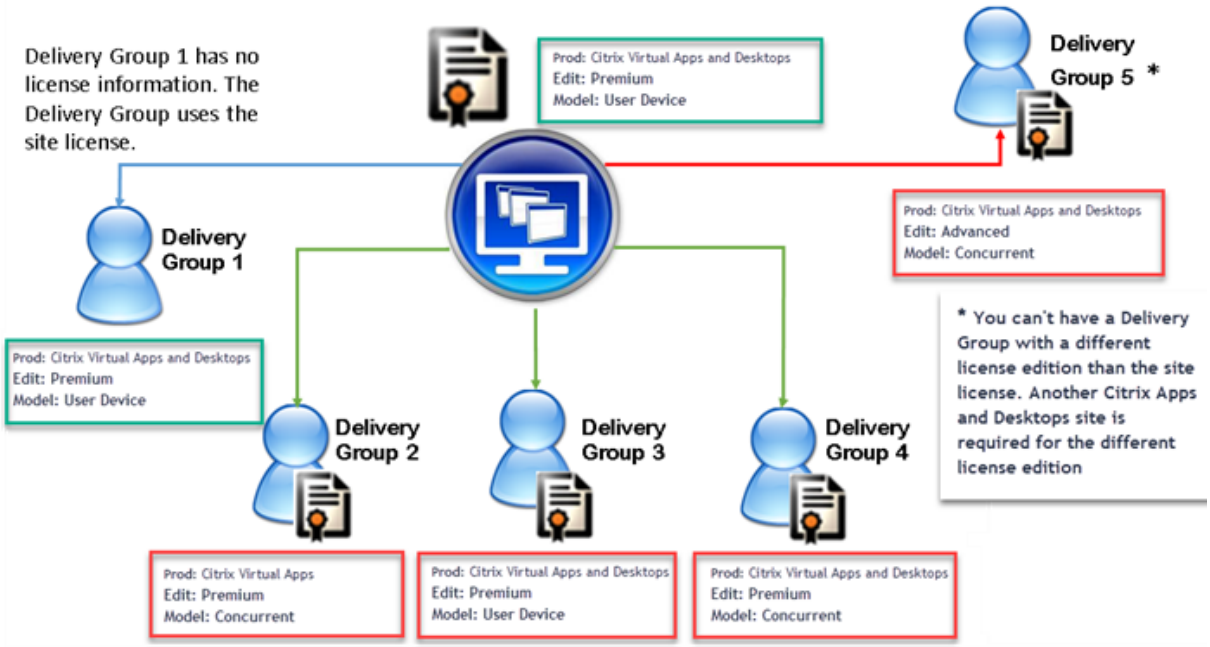
1. 在 Studio 导航窗格中选择配置 **>** 许可。
2. 在中间窗格中选择“许可管理员”选项卡，然后选择管理员组。
3. 在“操作”窗格中选择编辑许可管理员组或删除许可管理员组。

多类型许可

January 21, 2022

多类型许可支持在单个 Citrix Virtual Apps and Desktops 站点上为交付组使用不同的许可证类型。类型是产品 ID（XDT 或 MPS）和模式（UserDevice 或 Concurrent）的一种组合。交付组必须使用在站点级别配置的相同产品版本（PLT/Premium 或 ENT/Advanced）。希望为 Citrix Virtual Apps and Desktops 部署配置多类型许可时，请注意本文末尾的特殊注意事项。

如果未配置多类型许可，则仅当为独立站点配置时才能使用不同的许可证类型。交付组使用站点许可证。有关配置多类型许可时的重要通知限制，请参阅特殊注意事项。



要确定使用不同许可证类型的交付组，请使用以下 Broker PowerShell cmdlet：

- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

要安装许可证，请使用：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Citrix Studio
- Citrix Licensing Manager
- citrix.com.cn

Customer Success Services 日期是每个许可证文件以及每个产品和模式特有的。以不同方式设置的交付组的 Customer Success Services 日期可能会不同。

许可证兼容性列表

此表详细介绍了旧产品名称、新产品名称和关联的功能名称。四个兼容性列指定了哪些产品和许可模式组合适用于多类型许可。CCU 和 CCS 表示并发许可证，UD 表示用户/设备许可证。

Old Name	New Name	Feature	Multi-type licensing compatibility			
			STD	ADV	ENT	PLT
Citrix XenApp Standard	Citrix XenApp Standard	MPS_STD_CCU	X			
Citrix XenApp Advanced	Citrix Virtual Apps Standard	MPS_ADV_CCU		X		
Citrix XenApp Enterprise	Citrix Virtual Apps Advanced	MPS_ENT_CCU			X	
Citrix XenApp Platinum	Citrix Virtual Apps Premium	MPS_PLT_CCU				X
Citrix XenApp Advanced	Citrix Virtual Apps Standard	MPS_ADV_CCU		X		
Citrix XenDesktop VDI Edition (XDT-U)	Citrix Virtual Desktops Standard- Per User/Device	XDT_STD_UD	X			
Citrix XenDesktop VDI Edition (XDT-C)	Citrix Virtual Desktops Standard - Concurrent	XDT_STD_CCS	X			
Citrix XenDesktop Enterprise Edition (XDT-C)	Citrix Virtual Apps and Desktops Advanced - Concurrent	XDT_ENT_CCS			X	
Citrix XenDesktop Enterprise Edition (XDT-U)	Citrix Virtual Apps and Desktops Advanced - Per User/Device	XDT_ENT_UD			X	
Citrix XenDesktop Platinum Edition (XDT-C)	Citrix Virtual Apps and Desktops Premium - Concurrent	XDT_PLT_CCS				X
Citrix XenDesktop Platinum Edition (XDT-U)	Citrix Virtual Apps and Desktops Premium - Per User/Device	XDT_PLT_UD				X

Broker PowerShell SDK

DesktopGroup 对象具有以下两个属性，您可以使用关联的 New-BrokerDesktopGroup 和 Set-BrokerDesktopGroup cmdlet 进行控制。

名称	值	限制
LicenseModel	用于指定组的许可模式的参数 (Concurrent 或 UserDevice)。如果未指定，则使用站点范围的许可模式。	如果禁用功能切换，尝试设置属性将失败。
ProductCode	指定组的许可产品 ID 的文本字符串 XDT（表示 Citrix Virtual Desktops）或 MPS（表示 Citrix Virtual Apps)。如果未指定，则使用站点范围的产品代码。	如果禁用功能切换，尝试设置属性将失败。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

有关 LicenseModel 和 ProductCode 的详细信息，请参阅 about_Broker_Licensing。

New-BrokerDesktopGroup

创建桌面组以便对多组桌面的代理进行管理。有关此 cmdlet 的详细信息，请参阅https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/。

Set-BrokerDesktopGroup

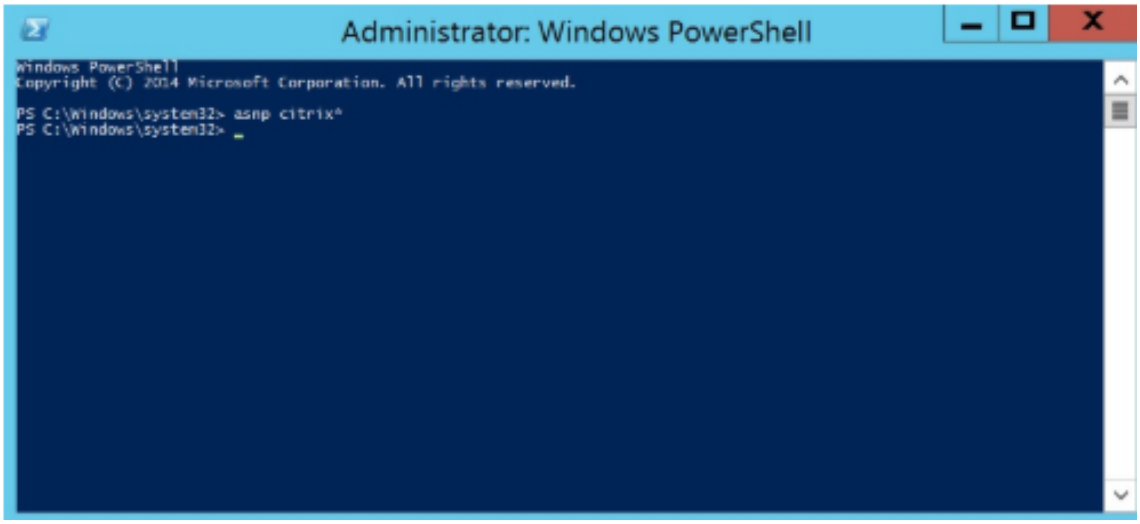
禁用或启用现有 Broker 桌面组或更改其设置。有关此 cmdlet 的详细信息，请参阅 https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/

Get-BrokerDesktopGroup

检索匹配指定条件的桌面组。Get-BrokerDesktopGroup cmdlet 的输出包括组的 **ProductCode** 和 **LicenseModel** 属性。如果未使用 New-BrokerDesktopGroup 或 Set-BrokerDesktopGroup 设置这些属性，则返回空值。如果为空，则使用站点范围的许可模式和产品代码。有关此 cmdlet 的详细信息，请参阅https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/。

按照交付组配置不同的许可证产品和型号

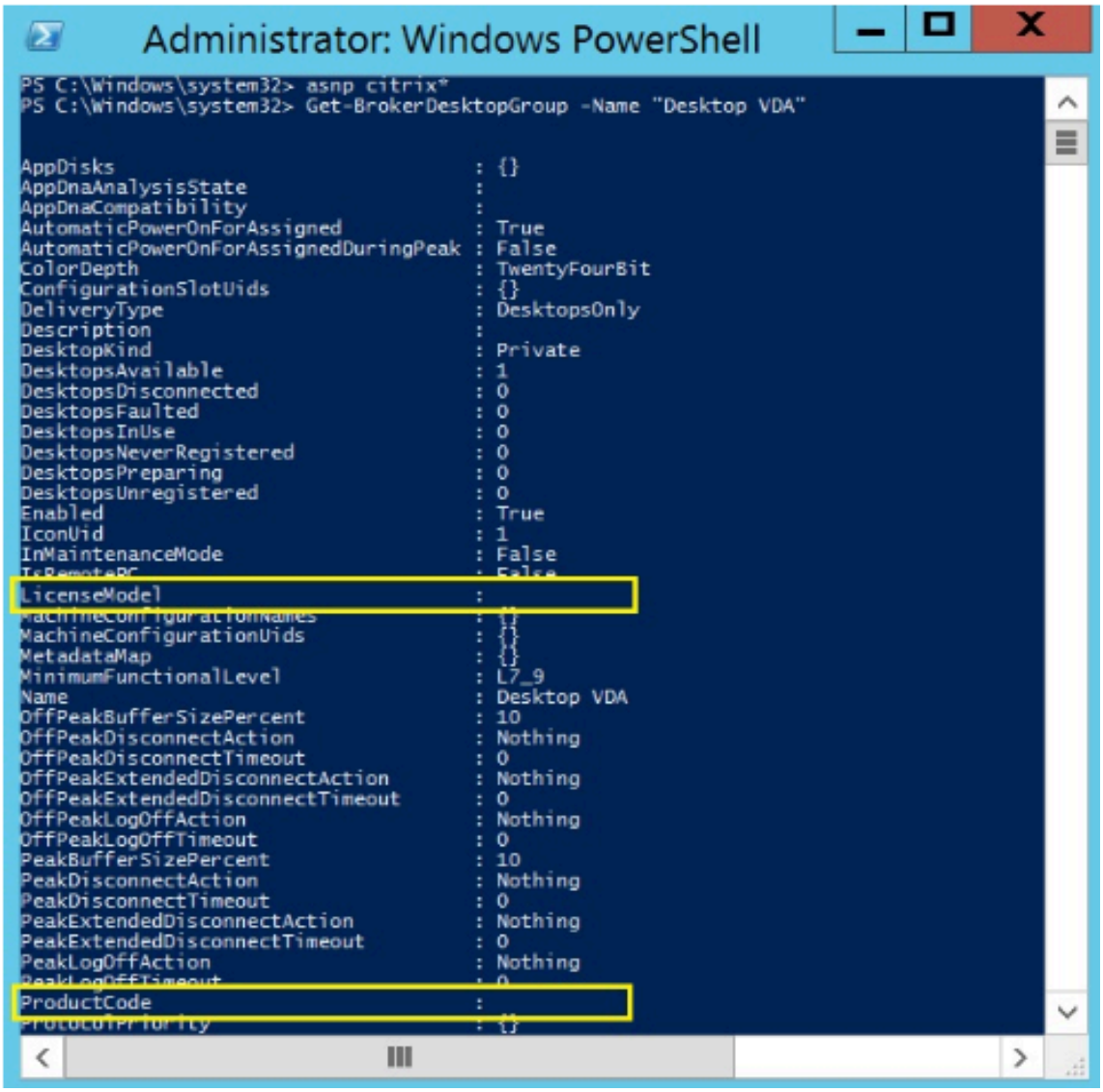
1. 使用管理权限打开 PowerShell 并添加 Citrix 管理单元。



2. 运行命令 **Get-BrokerDesktopGroup** –**Name** “**DeliveryGroupName**”以查看当前许可证配置。查找 **LicenseModel** 和 **ProductCode** 参数。如果以前未配置过以下参数，则它们可能为空。

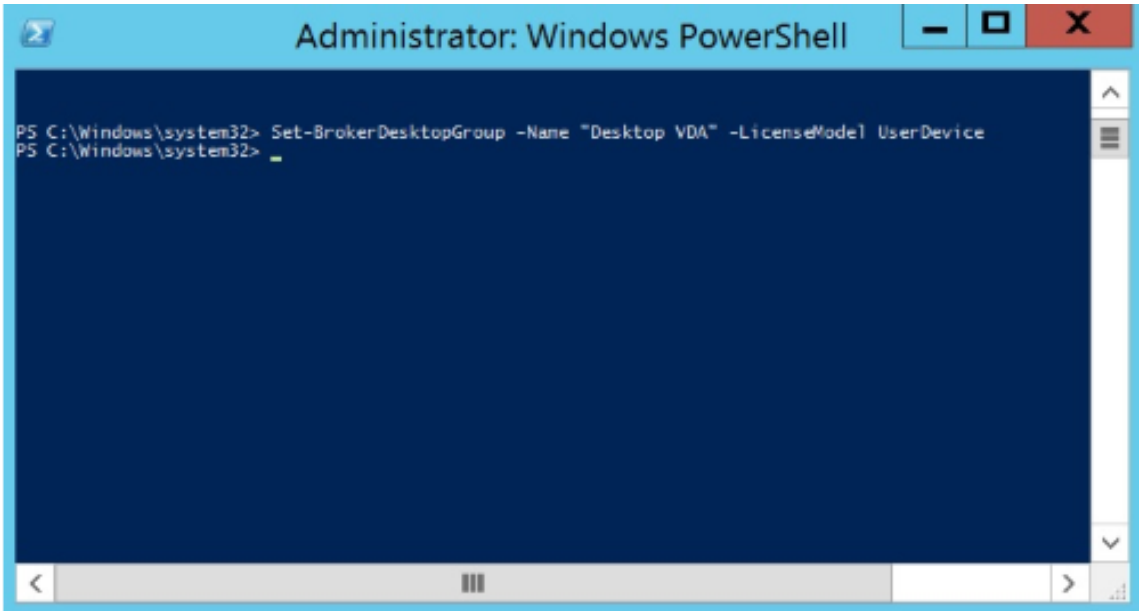
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 如果交付组未设置许可证信息，则默认为站点级别站点许可证。

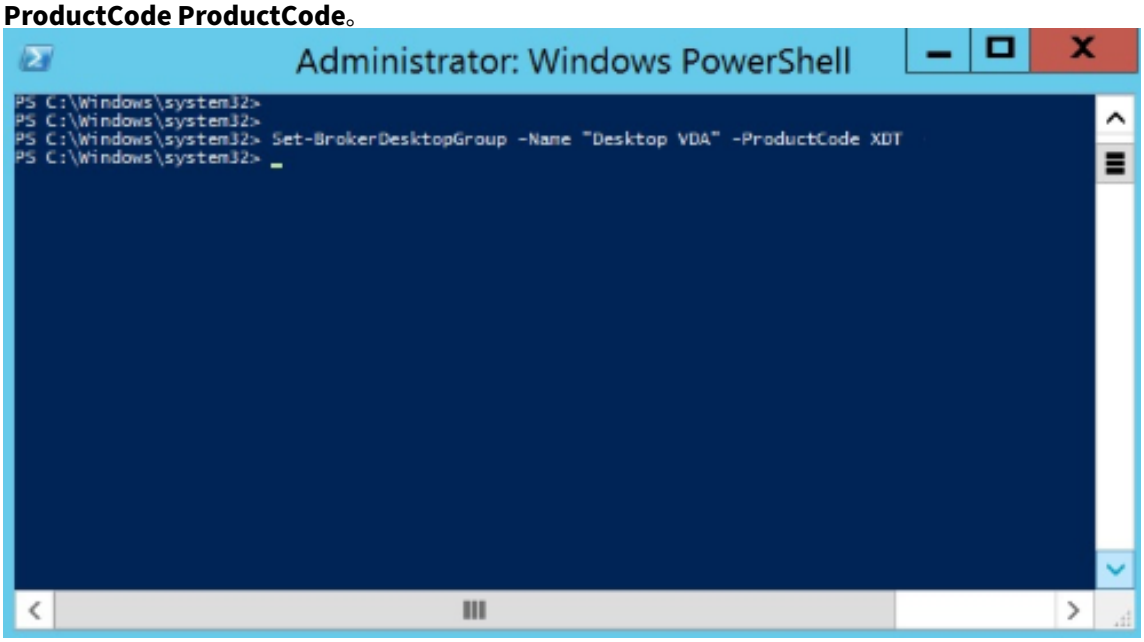


3. 请通过运行以下命令来更改许可模式：**Set-BrokerDesktopGroup -Name "DeliveryGroupName" -LicenseModel LicenseModel**。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



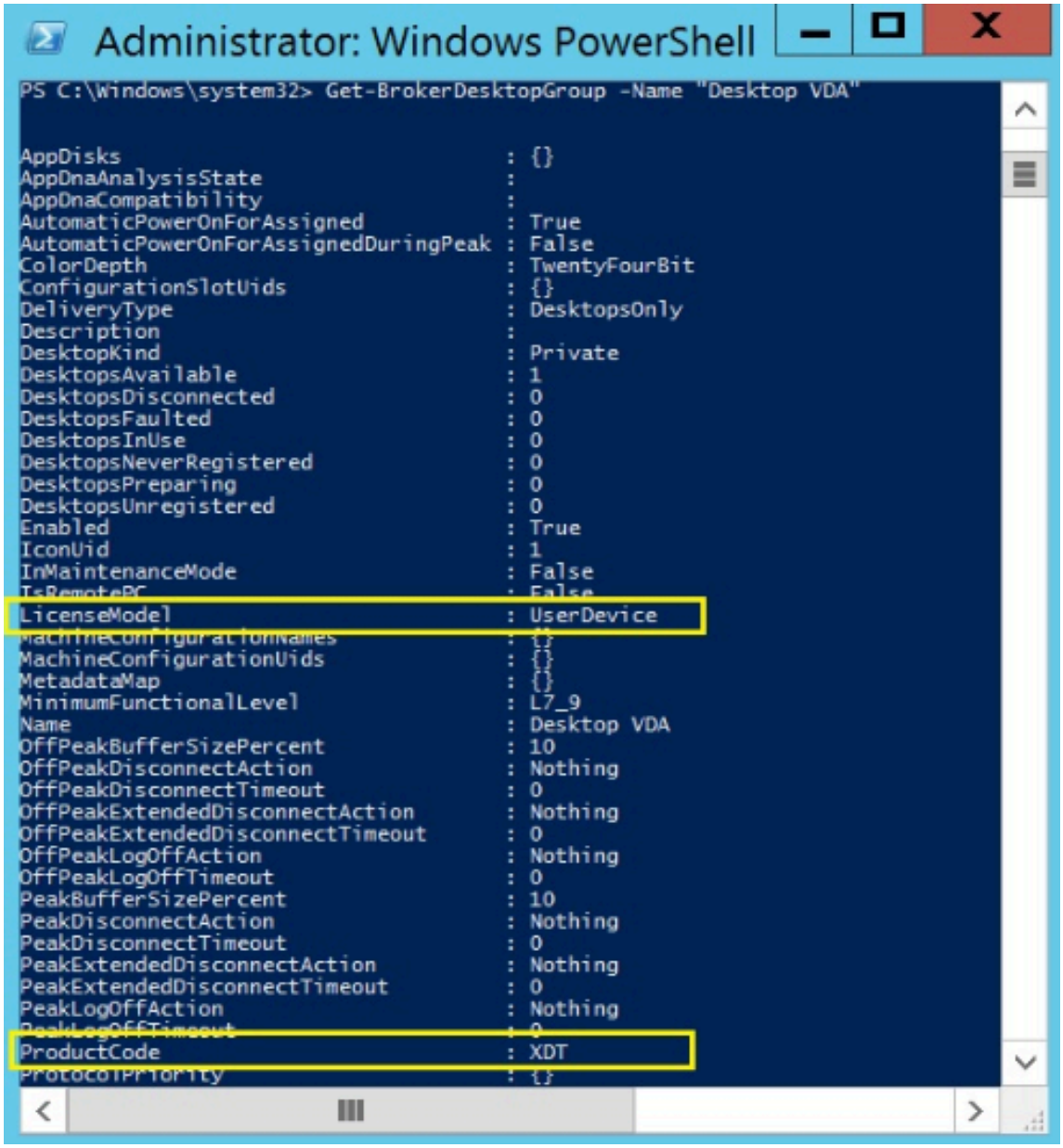
4. 请通过运行以下命令来更改许可证产品：**Set-BrokerDesktopGroup -Name "DeliveryGroupName" -ProductCode ProductCode**。



5. 输入命令 **Get-BrokerDesktopGroup -Name "DeliveryGroupName"** 以验证所做的更改。

> 注意：
>
> 您不能混合和匹配同一站点中的版本。例如，Premium 和 Advanced 许可证。如果您拥有不同版本的许可证，则需要多个站点。

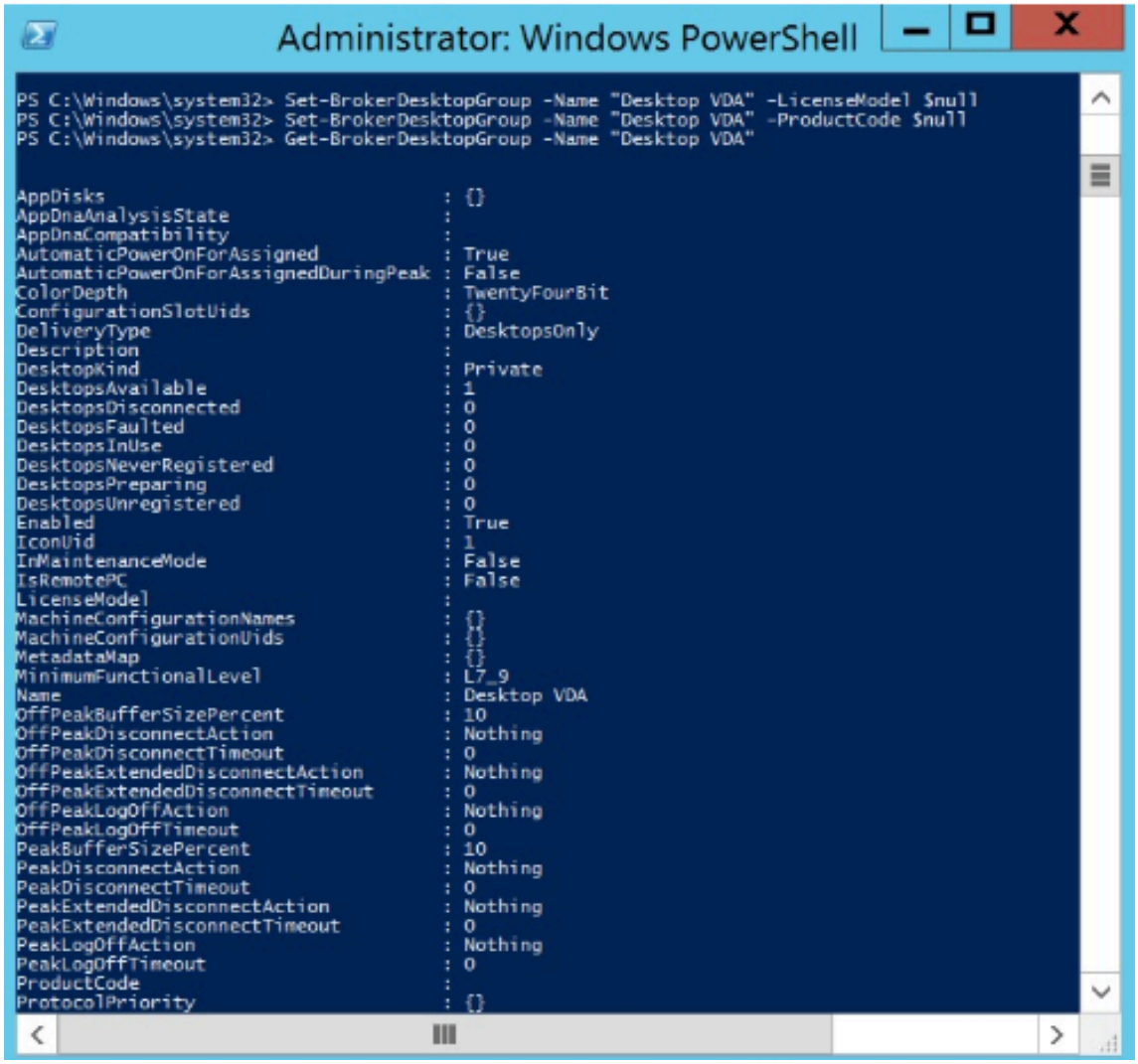
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



6. 请运行之前步骤中所述的相同 **Set-BrokerDesktopGroup** 命令来删除许可证配置，并将值设置为 **$null**。

> 注意：
>
> Studio 不显示每个交付组的许可证配置。使用 PowerShell 查看当前配置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



示例

此 PowerShell cmdlet 示例说明如何为两个现有交付组设置多类型许可，然后创建并设置第三个交付组。

要查看与交付组关联的许可产品和许可模式，请使用 **Get-BrokerDesktopGroup** PowerShell cmdlet。

1. 为第一个交付组设置 XenApp 和 Concurrent。

   Set-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Apps Premium Concurrent” -ProductCode MPS -LicenseModel Concurrent

2. 为第二个交付组设置 XenDesktop 和 Concurrent。

   Set-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Desktops Premium Concurrent” -ProductCode XDT -LicenseModel Concurrent

3. 创建第三个交付组并为其设置 XenDesktop 和 UserDevice。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

New-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Desktops Premium UserDevice” -PublishedName “MyDesktop” -DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

特殊注意事项

多类型许可与常规 Citrix Virtual Apps and Desktops 许可的功能不同。

对于配置为使用与站点配置不同的类型的交付组，Director 或 Studio 没有发出警报和通知：

- 临近许可证限制时没有任何信息，不会触发补充宽限期，也不存在补充宽限期到期。
- 特定组出现问题时不显示任何通知。

为多类型许可证配置的交付组仅使用该许可证类型，在完全使用时不会回退到站点配置。

尽管 Citrix Virtual Apps Standard 和 Citrix Virtual Desktops Standard 许可证版本名称只是这些许可证都是 Standard 版本，但其版本不同。多类型许可不适用于 Citrix Virtual Apps Standard 和 Citrix Virtual Desktop Standard 许可证。

许可常见问题解答

April 3, 2024

> 注意：
>
> - 有关与 COVID-19 大流行病有关的业务连续性资源，请参阅 CTX27055。
> - 有关维护业务连续性的常规信息，请参阅业务连续性 - 按需。
> - 有关当前 Citrix 许可证服务器的详细信息，请参阅许可。

Citrix Licensing

我可以通过何种方式获取我的许可证文件?

我们会使用电子邮件发送许可证访问代码。使用许可证访问代码生成许可证文件的方法有三种：

- citrix.com 上的“我的帐户”页面中的“管理许可证”工具箱
- Citrix Studio 负责分配您的购买，许可证文件将自动安装在 Citrix 许可证服务器上。
- Citrix 许可证服务器中的 Citrix Licensing Manager 负责分配您的购买并安装许可证文件。

有关详细信息，请参阅 Citrix Licensing 文档中的许可和 Citrix Virtual Apps and Desktops 文档中的许可。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix 许可使用哪些 **TCP** 端口**?**

- 许可证服务器端口号为 27000
- 供应商守护程序端口号为 7279
- 管理控制台 Web 端口为 8082
- Web Services for Licensing 端口为 8083

Citrix 许可证服务器是什么**?**

Citrix 许可证服务器是实现许可证跨网络共享的系统。有关详细信息，请参阅 Licensing 操作概述。

我是否可以将 **Citrix** 许可证服务器虚拟化或集群化**?**

是。您可以将 Citrix 许可证服务器虚拟化或群集化。有关详细信息，请参阅群集许可证服务器。

如果我对 **Citrix** 许可证服务器进行虚拟化，我有哪些好处**?**

对 Citrix 许可证服务器进行虚拟化可提供冗余解决方案。该解决方案允许在多个物理服务器之间移动，而无需停机。

如果我对 **Citrix** 许可证服务器进行虚拟化，是否需要考虑任何限制**?**

不能。

Citrix 许可证服务器是否管理我的 **Citrix Virtual Apps and Desktops** 部署的所有许可证**?**

Citrix 许可证服务器管理您为 Citrix Virtual Apps and Desktops 接收的所有许可证，但与 Citrix Gateway 一起使用的 Premium Edition 许可证除外。根据那些面向安全性的网络设备的需要内置到网络设备的许可证服务器管理这些许可证。

Citrix Licensing Manager 是什么**?**

Citrix Licensing Manager 支持从安装了 Citrix Licensing Manager 的许可证服务器下载和分配许可证文件。Citrix Licensing Manager 是推荐使用的许可证服务器管理方法，可实现以下功能：

- 在 Citrix Cloud 注册许可证服务器的短代码和轻松删除注册。
- 配置用户帐户和组帐户。
- 使用控制板显示已安装、使用中、已过期和可用的许可证以及 Customer Success Services 日期。
- 导出许可证使用数据以用于报告中。
- 配置历史使用数据保留期限。默认数据保留期限为 180 天。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 简化了使用许可证访问代码或下载的文件在许可证服务器上安装许可证文件的过程。
- 启用和禁用补充宽限期。
- 配置客户体验改善计划 (CEIP) 和 Call Home。
- 自动或手动检查 Customer Success Services 续订许可证并向您发出通知，或者在找到许可证时自动安装。
- 通知您许可证服务器的状态 - 缺少启动许可证、时间问题、上载程序故障。
- 修改以下端口：
  - 许可证服务器（默认值 27000）
  - 供应商守护程序（默认值 7279）
  - Web Services for Licensing（默认值 8083）

有关详细信息，请参阅 Citrix Licensing Manager。

Citrix 许可证管理控制台在什么位置**?**

许可证管理控制台不再受支持，并且已从许可证服务器版本 11.16.6 中删除。我们建议您使用 CCitrix Licensing Manager。

只要许可证服务器与 Studio 位于相同的域内或位于可信域内，您就可以使用 Studio 管理和跟踪许可。

有关详细信息，请参阅 Citrix Licensing Manager。

许可证分配期限是多久**?**

许可证分配期限是将 Citrix Virtual Apps and Desktops 许可证分配给用户或设备的术语。默认的许可证分配期限为 90 天。

我如何知晓我的组织购买了多少个许可证**?**

所有购买的许可证都可以随时（全天候）查看和访问 https://www.citrix.com 上我的帐户页面上的安全管理许可证工具箱。

我如何知晓在任何时候正在使用多少许可证**?**

Citrix Licensing Manager 和 Studio 提供有关实时许可证使用的详细信息。

许可证服务器灾难恢复和维护

有关许可证服务器的灾难恢复和维护的信息，请参阅 Citrix Licensing 文档中的灾难恢复和维护。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Virtual Apps and Desktops 许可

Citrix Virtual Apps and Desktops 如何获得许可?

Citrix Virtual Apps and Desktops 许可提供用户/设备和并发许可证模式。

用户/设备：

灵活的用户/设备模式与以下内容保持一致：

- 企业范围的桌面使用情况。
- 基础 Microsoft 桌面虚拟化许可。
- 用户只需偶尔访问其虚拟桌面和应用程序的客户的并发许可。

用户/设备许可允许用户从无限数量的设备访问其虚拟桌面和应用程序。设备许可证允许用户从单个设备访问无限次访问其虚拟桌面和应用程序。此方法为您提供了最大的灵活性，并提高了与 Microsoft 桌面虚拟化许可的一致性。

> 重要：
>
> 您无法手动将许可证分配给用户或设备。许可证服务器或云服务负责分配许可证。使用用户/设备许可，一旦分配许可证，直到 90 天不活动后才能将其分配给其他用户。

并发：

并发许可证允许任何用户和任何设备一次连接到无限数量的虚拟应用程序和桌面。许可证仅在活动会话期间使用。如果会话断开连接或终止，许可证将签回到池中。

有关用户/设备许可的详细信息，请参阅用户/设备许可证，有关并发许可证的详细信息，请参阅并发许可证。

是否可以在购买许可证之前试用 Citrix Virtual Apps and Desktops?

是。可以下载 Citrix Virtual Apps and Desktops 软件并在试用模式下运行。试用模式允许您在本地使用 Citrix Virtual Apps and Desktops 30 天，建立 10 个连接，无需许可证。

适用于 Citrix Cloud 的 Citrix Virtual Apps and Desktops 服务可根据批准进行试用服务。请咨询您的 Citrix 代表以了解更多详细信息。

Citrix 如何为 Citrix Virtual Apps and Desktops 定义并发性?

Citrix Virtual Apps and Desktops 并发模式允许任何用户和任何设备一次连接到无限数量的虚拟应用程序和桌面。许可证仅在活动会话期间使用。如果会话断开连接或终止，许可证将签回到池中以重新发放。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

我是否可以在公用许可证服务器上部署多个版本的 **Citrix Virtual Apps and Desktops** 许可证**?**

是。许可证服务器同时管理 Citrix Virtual Apps and Desktops 的许可证。我们建议您安装最新版本的许可证服务器。如果不确定许可证服务器版本是否为最新版本，请通过将您的版本号与 Citrix 下载站点上的版本号进行比较来进行验证。

单个站点是否可以同时使用 **Citrix Virtual Apps** 和 **Citrix Virtual Apps and Desktops** 许可证**?**

根据版本的不同，单个 Citrix Virtual Apps 或 Citrix Virtual Apps and Desktops 站点可以支持两种许可模式 - 用户/设备模式或并发模式。单个 Citrix Virtual Apps 或 Citrix Virtual Apps and Desktops 站点只能支持一个版本。有关详细信息，请参阅多类型许可。

支持多类型许可的最低版本为 XenApp 和 XenDesktop 7.15 长期服务版本 (LTSR) 以及 Citrix Virtual Apps and Desktops 7 1808。

如果我在许可证服务器上安装了 **Citrix Virtual Apps and Desktops** 用户**/**设许可证备或 **Citrix Virtual Apps and Desktops** 并发许可证，是否可以选择 **Citrix Virtual Apps** 并发模式作为产品模式**?**

如果您将 Citrix Virtual Apps 用作 Citrix Virtual Apps and Desktops Advanced 或 Premium Edition 的功能，则 Citrix Virtual Apps 许可模式将与 Citrix Virtual Apps and Desktops 的 Advanced 或 Premium Edition 相同。如果您已购买 Citrix Virtual Apps and Desktops，请将您的许可配置为 Citrix Virtual Apps and Desktops，即使您仅计划使用 Citrix Virtual Apps 功能亦如此。仅当您在许可证服务器上安装了 Citrix Virtual Apps 并发独立许可证时，才选择 Citrix Virtual Apps 作为产品模式。

每个 **Citrix Virtual Apps** 和 **Citrix Virtual Apps and Desktops** 版本都包含哪些产品组件**?**

有关按版本列出的完整功能列表，请参阅 Citrix Virtual Apps and Desktops 功能。

我如何根据 **Citrix Virtual Apps and Desktops EULA** 授权 **Citrix Virtual Desktops** 环境**?**

要根据 Citrix Virtual Apps and Desktops EULA 在用户/设备或并发许可模式下部署 Citrix Virtual Apps and Desktops，请将许可证文件应用到许可证服务器。然后，许可证服务器将控制和监视许可证合规性。我们建议您根据购买的产品配置您的产品。例如，如果您购买 Citrix Virtual Apps and Desktops Premium，但仅希望使用 Citrix Virtual Apps 功能，请将产品配置为 Citrix Virtual Apps and Desktops 以满足合规性。有关详细信息，请参阅产品许可证合规中心。

我如何根据 **Citrix Virtual Apps EULA** 授权 **Citrix Virtual Apps** 环境**?**

要根据 Citrix Virtual Apps EULA 在并发许可模式下部署 Citrix Virtual Apps，请将许可证文件应用到许可证服务器。然后，许可证服务器将控制和监视许可证合规性。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Virtual Apps and Desktops 服务选项是否有许可要求：长期服务版本 **(LTSR)** 或当前版本 **(CR)?**

Citrix Virtual Apps and Desktops 服务选项（例如长期服务版本）是 Customer Success Services 计划的一个优势。您必须拥有有效的 Customer Success Services 才能享受 LTSR 的优势。有关详细信息，请参阅 Citrix Virtual Apps、[Citrix Virtual Apps and Desktops 和 Citrix Hypervisor 服务选项。

Secure Browser 标准服务共用时间的工作原理是什么**?**

当您购买至少 25 个服务用户时，您将获得 5000 小时的服务使用权限，这些权限跨所有用户共用。后续购买用户权限不会增加共用小时权利。要增加服务小时的权利，请购买附加包。

我可以将 **Remote PC Access** 与 **CCU** 许可证结合使用吗**?**

是。

有关 Remote PC Access 的信息，请参阅 Remote PC Access。

用户或设备许可证

Citrix 如何向用户**/**设备许可模式下的用户分配许可证**?**

使用用户/设备许可模式，许可证服务器将许可证分配给唯一的用户 ID。它允许单个用户从无数个设备建立无数个连接。如果用户连接到桌面或设备，则用户需要分配给该用户一个许可证才能访问虚拟桌面或应用程序。许可证服务器或云服务负责分配该许可证。您无法手动分配这些许可证。许可证分配给用户，而非共享设备。一旦分配许可证，直到 90 天不活动后才能将其分配给其他用户。

Citrix 如何在用户**/**设备许可模式下定义已获得许可的设备**?**

已获得许可的设备需要唯一的端点设备 ID。在用户/设备模式下，设备是您授权任何个人用于访问 Citrix Virtual Apps and Desktops 实例的任何设备。对于共享设备，单个 Citrix Virtual Apps and Desktops 用户/设备许可证可以支持共享该设备的多个用户。例如，共享设备可以是教室工作站或医院中的临床工作站。

我是否可以将我的 **Citrix Virtual Desktops Standard Edition** 并发许可证转换为用户**/**设备模式**?**

您无法将 Citrix Virtual Desktops Standard Edition 并发许可证转换为 Citrix Virtual Desktops Standard Edition 用户/设备许可证。同样，无法将 Citrix Virtual Desktops Standard Edition 用户/设备许可证转换为 Citrix Virtual Desktops Standard Edition 并发许可证。

如果您拥有 Citrix Virtual Desktops Standard Edition 并发许可证，并且希望使用用户/设备许可证模式，请升级到 Citrix Virtual Apps and Desktops Advanced 或 Premium Edition。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

原术语	至 Standard 并发	至 Standard 用户/设备	至 Advanced 用户/设备	至 Premium 用户/设备
Citrix Virtual Desktops Standard Edition 并发许可证	不适用	不允许将并发许可证转换为用户/设备许可证	您无法转换许可证模式，但可以升级到 Citrix Virtual Apps and Desktops Advanced 或 Premium Edition。	您无法转换许可证模式，但可以升级到 Citrix Virtual Apps and Desktops Advanced 或 Premium Edition。
Citrix Virtual Desktops Standard Edition 用户/设备许可证	不允许将用户设备许可证转换为并发许可证	不适用	不适用	不适用

并发许可与用户/设备许可的工作原理有何不同?

我们基于并发设备连接进行并发许可。仅当设备建立了活动连接时才使用并发许可证。连接结束后，并发许可证将返回到许可证池以便立即使用。我们建议偶尔使用此许可模式。用户/设备许可证将租用一段时间，在租约到期之前不可用于其他用户。

在用户/设备模式下，我们是否可以将许可证分配给同一企业中的用户和设备?

是。这两种类型都可以存在于同一企业中。许可证服务器根据使用情况以最佳方式将许可证分配给用户或设备。您无法手动分配这些许可证。

我如何确定要许可的用户或设备数量?

请评估用例要求以确定恰当的许可证数量。用户/设备许可允许从无限数量的设备访问无线数量的虚拟桌面和虚拟应用程序。并发许可允许无限制地从无限数量的用户可以使用的单个设备访问无限数量的虚拟桌面和虚拟应用程序。请考虑以下公式：

```
(Number of total users) - (number of users that only access exclusively
 with shared devices) + (number shared devices) = total number of licenses to buy.

For example, there are 1000 total users at the hospital. If 700 of them access only
Citrix Virtual Desktops from 300 shared devices in the hospital, the number of
licenses to purchase is 1000 - 700 + 300 = 600 licenses.
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

在用户/设备模式下，获得许可的用户可用于连接到我的环境的最大设备数量是多少?

每个获得许可的用户都有权使用无限数量的已连接设备或脱机设备。

在用户/设备模式下，可以访问获得许可的设备的最大用户数量是多少?

每个获得许可的设备都可以为组织内无限数量的用户提供服务。

在用户/设备模式下，获得许可的用户在任何指定的时间都可以使用的虚拟桌面或 **Secure Browser Web** 应用程序的最大数量是多少?

每个获得许可的用户都可以连接到无限数量的虚拟桌面或 Web 应用程序。

我是否可以购买 **Citrix Virtual Apps and Desktops** 许可证，以增加现有 **Citrix Virtual Apps and Desktops** 环境中的获得许可的用户/设备数量?

是。您可以购买 Citrix Virtual Apps and Desktops 许可证，以增加现有 Citrix Virtual Apps and Desktops 环境中获得许可的用户/设备的数量。

我如何释放授权的用户/设备许可证?

要释放授权用户/设备的分配，请根据 EULA 条款使用 `udadmin` 实用程序。然后，许可证服务器将许可证分配给下一个相应的用户/设备。

如果我超出购买的用户/设备许可证计数，会发生什么情况?

用户/设备许可证包括 10% 的透支许可证，这是在生成许可证时包含的。透支许可证也包含在已安装的许可证计数中。如果使用高峰超过包括透支在内的安装计数，则拒绝更多用户访问。购买并部署新许可证才能为更多用户启用访问权限。

如果所有许可证都在使用（包括许可证透支），补充宽限期可实现与产品的不受限连接。补充宽限期让您有时间确定您为什么超过最大许可证计数，以及购买更多许可证而不会干扰您的用户。此宽限期持续 15 天或持续到您安装了更多的零售许可证，以其中较早者为准。有关详细信息，请参阅补充宽限期。

Director 将显示宽限期状态。有关详细信息，请参阅 Director 控制板上的面板。

获得许可的用户在任何指定的时间都可以使用的虚拟应用程序的最大数量是多少?

每个获得许可的用户都可以连接到无限数量的虚拟应用程序。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

如果获得许可的用户离开我的组织，会发生什么情况**?**

当现有获得许可的用户离开贵组织时，您可以在不通知 Citrix 的情况下释放离开的用户的许可证。使用 udadmin 实用程序释放许可证。如果您不释放许可证，许可证服务器会在不活动 90 天后自动释放任何许可证。此信息受 EULA 中指定的条款约束。

如果获得许可的用户长时间缺席，会发生什么情况**?**

如果现有的获得许可的用户长时间缺席，您可以在不通知 Citrix 的情况下释放许可证，以便可以重新分配许可证。使用 udadmin 实用程序释放许可证。

如果我们更换我的组织中的获得许可的设备，会发生什么情况**?**

如果您更换了现有的获得许可的设备，则可以在不通知 Citrix 的情况下释放许可证，以便可以重新分配许可证。使用 udadmin 实用程序释放许可证。

如果获得许可的设备长时间停止使用，会发生什么情况**?**

如果现有的获得许可的设备在相当长的一段时间内不提供服务，您可以在不通知 Citrix 的情况下释放许可证，以便可以重新分配许可证。使用 udadmin 实用程序释放许可证。如果您不释放许可证，许可证服务器会在不活动 90 天后自动释放任何许可证。此信息受 EULA 中指定的条款约束。

我是否可以将用户许可证转换为设备许可证，并在将许可证分配给设备或用户后再转换回来**?**

是。此更改会自动发生。许可证服务器根据使用模式将许可证分配给用户或设备。如果使用模式发生变化，许可证服务器可能会根据新的使用情况转换分配。许可证服务器始终以最经济的方式为客户分配许可证。此外，许可证服务器还监视许可证，以便在 90 天分配期之后识别未使用的许可证。可以将 90 天分配期后识别为未使用的许可证重新分配给其他用户或设备。

并发许可证

在并发模式下，获得许可的 **Citrix Virtual Apps and Desktops** 用户在任何指定的时间都可以使用的虚拟桌面的最大数量是多少**?**

端点可以为许多用户提供服务，并允许建立不限数量的连接。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

我是否可以将早期版本的 **Citrix Virtual Apps and Desktops** 以及新用户/设备或并发许可证部署到单个许可证服务器**?**

是。您可以继续使用相同的许可证服务器来支持用户/设备或并发许可部署。

我是否可以将并发许可证和用户/设备或并发许可证部署到单个许可证服务器**?**

是。您可以继续使用相同的许可证服务器来支持并发和用户/设备或并发许可部署。

Citrix Virtual Apps and Desktops Advanced 和 **Premium Edition** 是否包括 **Citrix Virtual Apps** 并发许可证**?**

Citrix Virtual Apps and Desktops Advanced 和 Premium 用户/设备许可证包括并发 Citrix Virtual Apps 许可证，仅用于实现兼容性。这些并发许可证仅用于与用户/设备许可证不兼容的早期产品版本。仅允许在以下版本中使用用户/设备许可证中包含的并发兼容性许可证：早于 6.5 的 XenApp 版本和早于 5.0 Service Pack 1 的 XenDesktop 版本。

如果我超出购买的并发许可证计数，会发生什么情况**?**

如果所有许可证都在使用，补充宽限期将允许无限制地连接到产品。补充宽限期让您有时间确定您为什么超过最大许可证计数，以及购买更多许可证而不会干扰您的用户。此宽限期持续 15 天或持续到您安装了更多的零售许可证，以其中较早者为准。有关详细信息，请参阅补充宽限期。

Director 将显示宽限期状态。有关详细信息，请参阅 Director 控制板上的面板。

透支许可证

我如何获得透支许可证**?**

支持用户/设备、用户或设备许可模式的产品（Citrix Cloud 除外）包括许可证透支功能，使您能够使用有限数量的额外许可证以防止访问被拒绝。我们提供任何透支功能是为了方便，而不是作为许可证权利。并发许可证和服务器许可证不包含透支功能。使用的任何透支许可证都必须在首次使用后 30 天内购买，但使用期限不限于 30 天。Citrix 保留删除新产品版本中的任何透支功能的权利。有关详细信息，请参阅许可证透支。

我可以如何识别许可证透支**?**

您可以在 Citrix Licensing Manager 中查看使用情况信息，包括透支的许可证数量。Studio 还包含透支使用信息。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用透支许可证时会发生什么情况?

从已安装的许可证中分配许可证，以启用对 Citrix Virtual Apps and Desktops 环境的访问。此透支许可证提供与您的其他许可证相同的访问权限和功能。

当我的透支许可证被占用时，我可以收到警报吗?

目前，当透支许可证被占用时，不提供特定的警报。

可以占用透支许可证多长时间?

在首次使用后 30 天内购买任何透支许可证。

其他产品特定的许可信息

- Citrix ADC
- Citrix Cloud
- Citrix Endpoint Management
- Citrix Gateway
- Citrix Hypervisor
- Citrix Licensing

应用程序

July 5, 2024

简介

如果您的部署仅使用交付组（而不使用应用程序组），则将应用程序添加到交付组。如果您也具有应用程序组，通常请改为将应用程序添加到应用程序组。本指导信息提供更轻松的管理过程。应用程序必须始终至少属于一个交付组或应用程序组。

在“添加应用程序”向导中，您可以选择一个或多个交付组或应用程序组，但不能同时选择两者。虽然您可在之后更改应用程序的组关联（例如，将应用程序从应用程序组移动到交付组），但是建议不要增加此复杂性。应使应用程序保持在一个类型的组中。

如果要将一个应用程序关联到多个组，但您没有足够权限来查看所有这些组中的应用程序，则会产生可见性问题。在这种情况下，可以咨询权限更高的管理员，或者扩展您的作用域，以包括要与应用程序关联的所有组。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

如果您向同一用户发布两个同名（可能来自不同组）的应用程序，请在 Studio 中更改 `Application name (for user)` 属性。否则，用户将在 Citrix Workspace 应用程序中看到重复的名称。

您可以在添加时更改应用程序的属性（设置），或者在以后更改。还可以在添加应用程序使或在此之后更改用于放置应用程序的应用程序文件夹。

有关详细信息，请参阅：

- 创建交付组
- 创建应用程序组
- 标记

添加应用程序

可以在创建交付组或应用程序组时添加应用程序。这些过程在创建交付组和创建应用程序组中详细介绍。以下过程描述如何在您创建组之后添加应用程序。

须知：

- 无法向 Remote PC Access 交付组中添加应用程序。
- 不能使用“添加应用程序”向导从交付组或应用程序组中删除应用程序。必须单独执行该操作。

要添加一个或多个应用程序，请执行以下操作：

1. 在 Studio 导航窗格中选择应用程序，然后在“操作”窗格中选择添加应用程序。
2. 此时将启动“添加应用程序”向导，并打开一个简介页面，您可以在将来启动此向导时不再显示该页面。
3. 该向导将引导您访问组、应用程序和摘要页面。完成每个页面之后，请单击下一步，直到到达摘要页面为止。

用于替代步骤 1 的方法（如果要将应用程序添加到单个交付组或应用程序组）：

- 要将应用程序只添加到一个交付组，请执行以下操作：在步骤 1 中，在 Studio 导航窗格中选择交付组，在中间窗格中选择一个交付组，然后在“操作”窗格中选择添加应用程序。该向导不会显示组页面。
- 要只将应用程序添加到一个应用程序组，请执行以下操作：在步骤 1 中，在 Studio 导航窗格中选择应用程序，在中间窗格中选择一个应用程序组，然后在“操作”窗格中应用程序组的名称下选择添加应用程序条目。该向导不会显示组页面。

“组”页面

此页面列出了站点中的所有交付组。如果您还创建了应用程序组，则该页面将列出应用程序组和交付组。您可从其中任何一个组进行选择，但不能同时从这两个组中选择。即，不能同时将应用程序添加到应用程序组和交付组。总体而言，如果您使用的是应用程序组，请将应用程序添加到应用程序组而非交付组。

添加应用程序时，请选中至少一个交付组（或应用程序组，如果可用）旁边的复选框。每个应用程序都必须始终至少与一个组关联。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

“应用程序”页面

单击添加以显示应用程序源。

- 从“开始”菜单：在计算机上发现的位于选定交付组中的应用程序。当您选择该源时，会打开一个新页面，其中包含已发现的应用程序的列表。选中要添加的应用程序的复选框，然后单击确定。

  在下列情况下不能选择此源：(1) 您选择的应用程序组不与交付组关联，(2) 选择的应用程序组与不包含任何计算机的交付组关联，或者 (3) 选择的交付组不包含任何计算机。

- 手动定义：位于站点上或网络中的其他位置的应用程序。选择此源时，将启动一个新页面。请输入可执行文件的路径、工作目录、可选命令行参数以及管理员和用户的显示名称。输入此信息后，单击确定。

- 现有：以前添加到站点的应用程序。当您选择该源时，会打开一个新页面，其中包含已发现的应用程序的列表。选中要添加的应用程序的复选框，然后单击确定。

  如果站点没有任何应用程序，则无法选择此源。

- **App-V**：App-V 包中的应用程序。如果选择此源，则会启动一个新页面，您可以在其中选择 App-V 服务器或应用程序库。从生成的显示内容中，选中要添加的应用程序的复选框，然后单击确定。有关详细信息，请参阅 App-V。

  如果没有为站点配置 App-V 则无法选择此源。

- 应用程序组：应用程序组。当您选择该源时，会打开一个新页面，其中包含应用程序组的列表。（虽然显示内容也会列出各个组中的应用程序，但是您只能选择组，而不能选择单个应用程序。）此时将添加选定组中的所有当前和将来的应用程序。选中要添加的应用程序组的复选框，然后单击确定。

  在下列情况中不能选择此源：(1) 没有应用程序组，或 (2) 所选交付组不支持应用程序组（例如，含静态分配的计算机的交付组）。

如果不存在该类型的有效源，则添加列表中的一些源无法选择（如表中所示）。该列表中不包括不兼容的源（例如，您不能将应用程序组添加到应用程序组）。无法选择已添加到您所选择的组的应用程序。

可以在此页面中更改应用程序的属性（设置），或在以后进行此更改。

默认情况下，添加的应用程序将放置在名为 `Applications` 的应用程序文件夹中。可从该页面中更改应用程序，或在以后执行此更改。如果您尝试添加某个应用程序，但同一文件夹中存在同名应用程序，系统将提示您重命名要添加的应用程序。您可以接受或拒绝系统所提供的新名称，然后重命名应用程序或选择不同的文件夹。例如，如果 **Applications** 文件夹中已经存在 `app`，而您尝试将另一个名为 `app` 的应用程序添加到该文件夹，则将提供新名称 `app_1`。

“摘要”页面

如果要添加 10 个或更少的应用程序，则它们的名称会列在要添加的应用程序中。如果要添加超过 10 个的应用程序，应指定总数。

查看摘要信息，然后单击完成。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

更改应用程序的组关联

添加应用程序后，可以更改与应用程序关联的交付组和应用程序组。

可以将应用程序拖动到其他组。可使用此操作代替在“操作”窗格中使用命令的操作。

如果应用程序与多个交付组或应用程序组相关联，则可以使用组优先级指定对多个组进行检查以发现应用程序的顺序。默认情况下，所有组都具有优先级 0（最高优先级）。将对具有相同优先级的组进行负载平衡。

可将应用程序与交付组（其中包含共享（非专用）的可提供应用程序的计算机）。还可以选择包含仅用于交付桌面的共享计算机的交付组，前提如下：(1) 交付组包含共享计算机，并且是通过 7.9 之前的 XenDesktop 7.x 版本创建的，(2) 您具有“Edit delivery group”权限。在提交属性对话框时，“交付组”类型将自动转换为“desktops and applications”。

1. 在 Studio 导航窗格中选择应用程序，然后在中间窗格中选择应用程序。
2. 在“操作”窗格中选择属性。
3. 选择组页面。
    - 要添加组，请单击添加并选择应用程序组或交付组。（如果尚未创建任何应用程序组，则唯一条目为交付组。）然后选择一个或多个可用的组。无法选择不兼容的，或已与应用程序关联的应用程序。
    - 要删除组，请选择一个或多个组，然后单击删除。如果删除组关联会导致应用程序不再与任何组关联，则系统会提醒您，指出该应用程序将被删除。
    - 要更改某个组的优先级，请选择该组，然后单击编辑优先级。选择一个优先级值，然后单击确定。
4. 完成操作后，单击应用以应用您执行的更改并保持打开窗口，或单击确定应用更改并关闭窗口。

复制、启用/禁用、重命名或删除应用程序

以下操作可用：

- 复制：您可能希望复制应用程序以创建具有不同参数或属性的不同版本。复制应用程序时，应用程序会通过唯一的后缀自动重命名并放置在与原始应用程序相邻的位置。您可能还需要复制应用程序并将其添加到不同的组。（复制后，可通过最简单的拖动方法来移动应用程序。）
- 启用或禁用：启用和禁用应用程序的操作与启用和禁用交付组或应用程序组的操作不同。
- 重命名：一次只能重新命名一个应用程序。如果您尝试重命名某个应用程序，但同一文件夹或组中存在同名应用程序，系统将提示您指定一个不同的名称。
- 删除：如果删除应用程序，会将其从关联的交付组和应用程序组中删除，但不会从最初用于添加此应用程序的源中删除。删除应用程序的过程与从交付组或应用程序组中删除应用程序的过程不同。

要复制、启用、禁用、重命名或删除应用程序，请执行以下操作：

1. 在 Studio 导航窗格中选择应用程序。
2. 在中间窗格中选择一个或多个应用程序，然后在“操作”窗格中选择相应的任务。
3. 在系统提示时，确认所做操作。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

从交付组中删除应用程序

应用程序必须至少关联（或属于）一个交付组或应用程序组。如果您尝试从交付组删除某个应用程序，将删除该应用程序与任何交付组或应用程序组的关联。如果继续操作，您会收到通知，指出应用程序将被删除。当发生这种情况时，如果要交付应用程序，则必须再次从有效源添加中应用程序。

1. 在 Studio 导航窗格中选择交付组。
2. 选择交付组。在中下部分的窗格中，在应用程序选项卡，选择要删除的应用程序。
3. 在“操作”窗格中选择删除应用程序。
4. 确认删除。

从应用程序组中删除应用程序

应用程序必须至少属于一个交付组或应用程序组。如果您尝试从应用程序组中删除某个应用程序，则将导致该应用程序不再属于任何组。如果继续操作，您会收到通知，指出该应用程序将被删除。当发生这种情况时，如果要交付应用程序，则必须再次从有效源添加中应用程序。

1. 在 Studio 导航窗格中选择应用程序。
2. 在中间窗格中选择应用程序组，然后选择一个或多个应用程序。
3. 在“操作”窗格中选择从应用程序组中删除。
4. 确认删除。

更改应用程序属性

一次只能更改一个应用程序的属性。

要更改应用程序的属性，请执行以下操作：

1. 在 Studio 导航窗格中选择应用程序。
2. 选择一个应用程序，然后在“操作”窗格中选择编辑应用程序属性。
3. 选择包含要更改的属性的页面。
4. 完成后，单击应用以应用您执行的所有更改并保持打开窗口，或者单击确定应用更改并关闭窗口。

在下面的列表中，页面在括号中显示。

属性	页面
Citrix Workspace 应用程序中用于显示应用程序的类别/文件夹	交付
命令行参数；请参阅将参数传递到已发布的应用程序	位置
其中包含可用应用程序的交付组和应用程序组	组

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

属性	页面
说明	标识
文件名扩展名和文件类型关联：将由应用程序自动打开的扩展名	文件类型关联
图标	交付
StoreFront 的关键字	标识
限制；请参阅配置应用程序限制	交付
名称：向用户和管理员显示的名称	标识
可执行文件的路径；请参阅将参数传递到已发布的应用程序	位置
用户桌面上的快捷方式：启用或禁用	交付
可见性：限制哪些用户可以看到 Citrix Workspace 应用程序中的应用程序。仍然可以启动不可见的应用程序。要使其不可用且不可见，请将其添加到其他组。	限制可见性
工作目录	位置

在当前的应用程序用户从其会话中注销之前，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，应用程序限制可用于管理资源密集型应用程序的同时运行的实例数。该限制有助于维持服务器性能并阻止服务恶化。

此功能限制 Controller 代理的应用程序启动的数量（例如，从 Citrix Workspace 应用程序和 StoreFront），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 处于中断模式时，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。有多种应用程序限制设置。可以配置任何或全部设置。

- 交付组中的所有用户运行的最大并发应用程序实例数。
- 交付组中的每个用户运行一个应用程序实例。
- 每台计算机的最大并发应用程序实例数（仅限 PowerShell）。

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。如果配置了多个限制，达到第一限制时会报告错误。

使用应用程序限制的示例：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 同时运行的最大实例数限制：在交付组中，可以将同时运行的最大应用程序 Alpha 实例数配置为 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。Alpha 不启动，因为这将超出所配置的同时运行的应用程序实例数限制 (15)。
- “每个用户运行一个实例”应用程序限制：在另一个交付组中，您为应用程序 Beta 启用了每个用户运行一个实例选项。用户 Tony 成功启动了应用程序 Beta。当天晚些时候，当该应用程序仍在 Tony 的会话中运行时，他尝试启动 Beta 的另一个实例。此时将生成一条错误消息，并且 Beta 不启动，因为这将超出一个用户运行一个实例的限制。
- 同时运行的最大实例数和“每个用户运行一个实例”限制：在另一个交付组中，可以为应用程序 Delta 配置同时运行的最大实例数 10，并启用每个用户运行一个实例选项。以后，当该交付组中的 10 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。Delta 不启动。如果当前 10 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。
- 每台计算机同时运行的最大实例数以及使用标记限制：应用程序 Charlie 具有许可和性能要求，这些要求规定了在特定服务器上可以同时运行的实例数。这些要求还规定了在站点中的所有服务器上可以同时运行的实例数。

  每台计算机的应用程序实例数限制会影响站点中的任何服务器（不只是某个特定交付组中的计算机）。假设您的站点有三台服务器。对于应用程序 Charlie，您可以将每台计算机的应用程序实例数限制配置为 2。因此，在站点范围内允许启动不超过六个应用程序 Charlie 实例。（即在三台服务器中的每台服务器上不能超过两个 Charlie 实例。）

  要将应用程序的使用仅限制到交付组中的某些计算机（除了限制站点范围内的所有计算机上的实例之外），请执行以下操作：

  - 对这些计算机使用标记功能。
  - 为该应用程序配置每台计算机的最大实例数限制。

如果应用程序通过除 Controller 代理以外的其他方法启动（例如，当 Controller 处于中断模式时），并且超出了配置的限制，用户将无法启动更多实例，直至其关闭足够的实例以便不再超出限制为止。超出该限制的实例不会强制关闭。它们将被允许继续运行，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。

要配置每个交付组的最大实例数限制和每个用户运行一个实例限制，请执行以下操作：

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，选择以下选项之一。

   - 允许不受限制地使用应用程序。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最大实例数

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 限制每个用户运行一个应用程序实例

4. 单击确定以应用所做的更改并关闭对话框，或单击应用以应用所做的更改并使对话框保持打开。

要配置每台计算机的最大实例数限制（仅限 PowerShell），请执行以下操作：

- 在 PowerShell（对于 Citrix Cloud 部署，使用远程 PowerShell SDK，或对于本地部署，使用 PowerShell SDK）中，输入带有 `MaxPerMachineInstances` 参数的相应 `BrokerApplication` cmdlet。
- 有关指导，请使用 `Get-Help` cmdlet。例如：

```
Get-Help Set-BrokerApplication -Parameter MaxPerMachineInstances
```

将参数传递到已发布的应用程序

使用某个应用程序属性的位置页面输入命令行，并将参数传递到已发布的应用程序。

将已发布的应用程序与文件类型相关联时，符号 “%*”（双引号中含百分号和星号）会附加在应用程序命令行的末尾。这些符号充当传递给用户设备的参数的占位符。

如果已发布的应用程序在应该启动时没有启动，请确认其命令行包含的符号是否正确。默认情况下，在附加符号 “%*” 时会验证用户设备提供的参数。对于使用用户设备提供的自定义参数的已发布应用程序，在命令行后面附加 “%**” 符号将跳过命令行验证。如果您在应用程序的命令行中看不到这些符号，请手动进行添加。

如果可执行文件的路径包含带空格的目录名称（例如 “C:\Program Files”），请使用双引号引起应用程序的命令行，以指示空格属于该命令行。要执行此操作，请使用双引号引起该路径，并使用另一个双引号引起 %* 符号。应确保在路径的右引号与 %* 符号的左引号之间留有一个空格。

例如：已发布的应用程序 Windows Media Player 的命令行为：

```
“C:\Program Files\Windows Media Player\mplayer1.exe” “%*”
```

管理应用程序文件夹

默认情况下，添加到交付组中的新应用程序将放置在名为应用程序的文件夹中。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：

- 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。
- 文件夹不必包含应用程序。允许使用空文件夹。
- 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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 您必须具有View Applications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Edit Application Properties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。或者，也可以使用右键菜单或拖动项目。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，请在 Studio 导航窗格中选择应用程序。请按下列指导进行操作。

- 查看所有文件夹（不包括嵌套文件夹）：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），请执行以下操作：选择 **Applications** 文件夹。要将新文件夹置于 **Applications** 之外的其他现有文件夹下，请选择该文件夹。然后，在“操作”窗格中选择创建文件夹。请输入名称。
- 移动文件夹：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。（最简便的移动文件夹的方法是拖动文件夹。）
- 重命名文件夹：选择该文件夹，然后在“操作”窗格中选择重命名文件夹。请输入名称。
- 删除文件夹：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。删除应用程序同时会从交付组中删除应用程序分配。不会将其从计算机中删除。
- 将应用程序移至某个文件夹：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。

在创建交付组或应用程序组时，您还可以将要添加的应用程序放置在应用程序页面的文件夹中。默认情况下，添加的应用程序位于 **Applications** 文件夹中。单击更改以选择或创建文件夹。

控制已发布的桌面上的应用程序的本地启动

用户从已发布的桌面内部启动已发布的应用程序时，可以控制该应用程序在该桌面会话中启动，还是作为已发布的应用程序启动。Citrix Workspace 应用程序在 VDA 上的 Windows 注册表中搜索应用程序的安装路径，如果存在，则启动该应用程序的本地实例。否则，将启动该应用程序的托管实例。如果您启动的应用程序未安装在 VDA 上，则会启动托管应用程序。有关详细信息，请参阅 vPenter 启动。

在 PowerShell（在 Citrix Cloud 部署中使用远程 PowerShell SDK 或在本地部署中使用 PowerShell SDK）中，可以更改此操作。

在 New-Broker 应用程序或 Set-BrokerApplication cmdlet 中，使用 LocalLaunchDisabled 选项。例如：

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

默认情况下，此选项的值为 false (-LocalLaunchDisabled $false)。从已发布的桌面内部启动已发布的应用程序时，该应用程序将在该桌面会话中启动。

如果将选项的值设置为 true (-LocalLaunchDisabled $true)，则会启动已发布的应用程序。这将额外创建一个从已发布的桌面（使用适用于 Windows 的 Citrix Workspace 应用程序）到已发布的应用程序的单独会话。

要求和限制：

- 应用程序的 ApplicationType 值必须为 HostedOnDesktop。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 此选项仅通相应的过 PowerShell SDK 提供。此选项当前不在 Studio 图形界面中提供。
- 此选项要求的最低版本：StoreFront 3.14、Citrix Receiver for Windows 4.11 和 Delivery Controller 7.17。

通用 **Windows** 平台应用程序

January 24, 2023

有关通用 Windows 平台 (UWP) 应用程序的信息，请参阅以下 Microsoft 文档：

- 通用 Windows 平台 (UWP) 应用程序是什么?
- Windows Package Manager

要求和限制

Citrix Virtual Apps and Desktops 支持在以下 Windows 计算机上使用 UWP 应用程序和 VDA：

- Windows 10 及更高版本
- Windows Server 2016 及更高版本

这些 VDA 的版本至少应为 7.11。

以下 Citrix Virtual Apps and Desktops 功能在使用 UWP 应用程序时不受支持或受到限制：

- 不支持文件类型关联。
- 不支持本地应用程序访问。
- 动态预览：如果会话中运行的应用程序重叠，该预览会显示默认图标。动态预览所使用的 Win32 API 不受 UWP 应用程序支持。
- 操作中心远程处理：UWP 应用程序可以使用操作中心来显示会话中的消息。这些消息目前未重定向到端点，无法向用户显示。

不支持从同一服务器启动 UWP 应用程序和非 UWP 应用程序。而是将 UWP 应用程序和非 UWP 应用程序放置在单独的交付组或应用程序组中。

由于计算机上安装的所有 UWP 应用程序都是枚举的，因此 Citrix 建议禁用用户对 Windows 应用商店的访问权限。这防止一个用户安装的 UWP 应用程序被另一个用户访问。

在旁加载过程中，UWP 应用程序将安装在计算机上，且可由其他用户使用。当其他用户启动该应用程序时，该应用程序即已安装，操作系统更新其 AppX 数据库以指示该用户“已安装”。

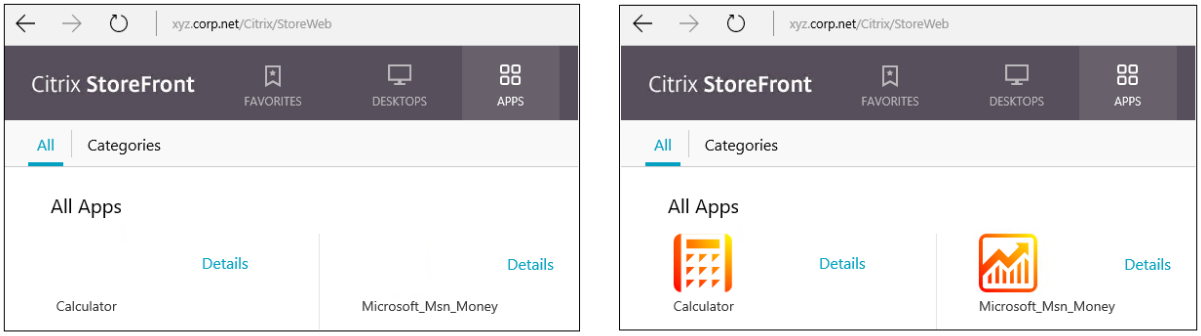
从在固定或无缝窗口中启动的已发布 UWP 应用程序启动的正常注销可能会阻止 VDA 会话关闭并强制注销用户。发生这种情况时，VDA 会话中剩余的多个进程会阻止其正常关闭。要解决此问题，请确定哪个进程在阻止 VDA 会话关闭，然后将其添加到“LogoffCheckSysModules”注册表项值中，并按照 CTX891671 中的指导进行操作。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

UWP 应用程序的应用程序显示名称和说明可能不具有正确的名称。在将这些应用程序添加到交付组时编辑并更正这些属性。

检查已知问题了解任何其他问题。

当前，多个 UWP 应用程序具有启用了透明度的白色图标，这导致在 StoreFront 显示屏的白色背景下看不见图标。要避免此问题，您可以更改背景。例如，在 StoreFront 计算机上，编辑文件 `C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css`。在文件末尾，添加 `.storeapp-icon { background-image: radial-gradient( circle at top right, yellow, red ); }`。以下图形阐释了该示例前后变化的情况。



在 Windows Server 2016 及更高版本中，服务器管理器也可能会在启动 UWP 应用程序时启动。为防止出现这种情况，请禁止服务器管理器在使用 `HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon` 注册表项登录期间自动启动。有关详细信息，请参阅 https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/。

安装和发布 **UWP** 应用程序

默认情况下已启用对 UWP 应用程序的支持。

要在 VDA 上安装一个或多个 UWP 应用程序（或一个主映像），请使用以下方法之一：

- 通过适用于企业的 Windows 应用商店完成离线安装，使用诸如 Deployment Image Servicing and Management (DISM) 等工具将应用程序部署至桌面映像。有关详细信息，请参阅 Windows Package Manager。
- 旁加载应用程序。有关详细信息，请参阅 Windows 客户端设备中的旁加载业务线 (LOB) 应用程序。
- 请直接从适用于企业的 Windows 应用商店为每个目标用户安装 UWP 应用程序。

要在 Citrix Virtual Apps 或 Citrix Virtual Desktops 中添加（发布）一个或多个 UWP 应用程序，请执行以下操作：

1. 在计算机上安装了 UWP 应用程序之后，将 UWP 应用程序添加到交付组或应用程序组。您可以在创建一个组时执行此操作，或稍后执行。在应用程序页面上的添加菜单中，选择从“开始”菜单。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. 显示应用程序列表时，选择要发布的 UWP 应用程序。
3. 继续执行向导或关闭编辑对话框。

有关使用用户配置文件管理器 (UPM) 时的其他配置要求的信息，请参阅 Windows 应用程序 - Microsoft Store。

要禁止在 VDA 上使用 UWP 应用程序，请在 HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle 中添加注册表设置 **EnableUWASeamlessSupport** 并将其设为 **0**。

卸载 **UWP** 应用程序

使用诸如 Remove-AppXPackage 等命令卸载 UWP 应用程序时，仅可由管理员卸载该项目。要从可能已经启动和使用该应用程序的用户的计算机上删除应用程序，请在每台计算机上运行删除命令。无法通过一条命令从所有用户的计算机上卸载 AppX 软件包。

区域

January 21, 2022

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 Citrix Virtual Apps 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更多站点的成本。

  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 以实现冗余并具有恢复能力，但并非必须安装一个或多个 Controller。

  站点中配置的 Controller 数会影响某些操作（例如，向站点自身添加新 Controller）的性能。为了避免此问题，建议将您的 Citrix Virtual Apps 或 Citrix Virtual Desktops 站点中的区域数限制在 50 以内。

  区域的网络延迟超过 250 毫秒 RTT 时，我们建议您部署多个站点来代替区域。

在本文中，术语“本地”是指正在讨论的区域。例如，“VDA 注册到本地 Controller 中”是指 VDA 注册到 VDA 所在的区域中的 Controller。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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、云或云中的可用区域使用卫星区域。

主要区域：

主区域的默认名称为“Primary”。此区域中包含 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 Citrix Gateway。始终将站点数据库保留在主要区域中。

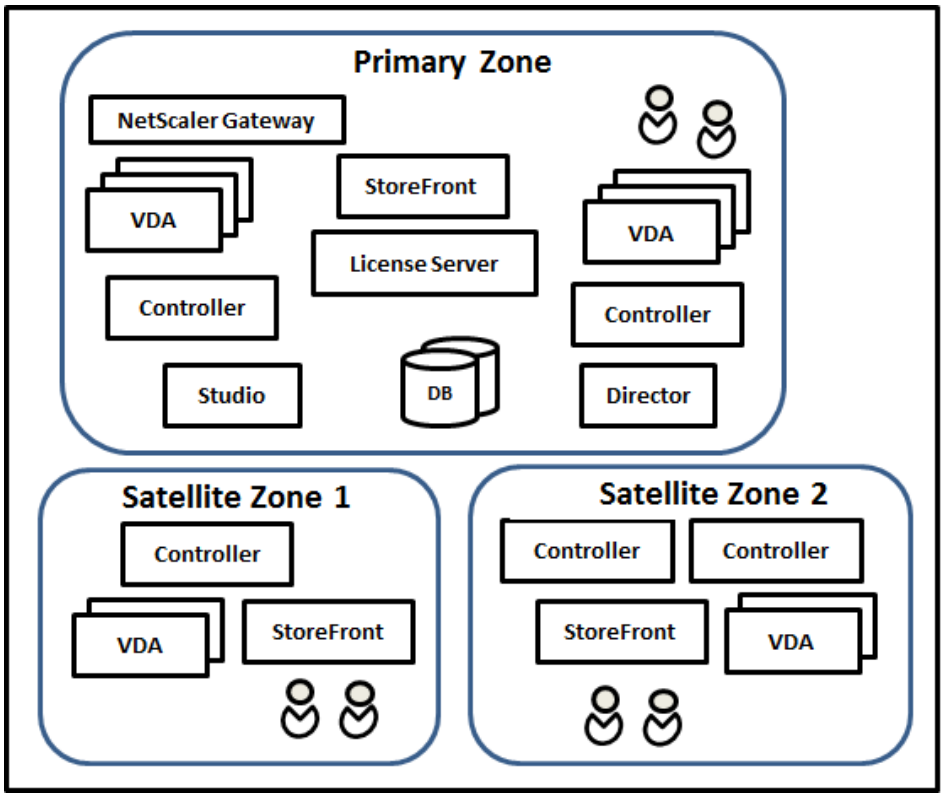
主区域应至少具有两个 Controller 以实现冗余。主要区域可以具有与数据库和基础结构紧密配对的应用程序的 VDA。

卫星区域：

一个卫星区域包含一个或多个 VDA、Controller、StoreFront 服务器和 Citrix 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，用于预配和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其他服务连接与其关联。（请确保使用该连接的所有目录都位于相同的区域。）

站点可以包含不同配置的卫星区域，具体取决于您的独特需求和环境。下图显示了一个主要区域以及卫星区域的示例。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

在该图中：

- 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 Citrix 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 与主要区域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，本地主机缓存功能将允许该卫星区域中的 Controller 继续中转与该区域中的 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。
- 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 将尝试向主要区域中的 Controller 注册。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。（将某个目录移动到另一个区域时，请确保此区域以及包含关联主机连接的区域的连接状况良好。如果带宽有限或者存在高延迟现象，请将主机连接移动到包含关联计算机目录的相同区域。）

如果主要区域中的所有 Controller 都出现故障：

- Studio 无法连接到站点。
- 无法与主要区域中的 VDA 建立连接。
- 站点性能将下降，直至主要区域中的 Controller 可用。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

对于包含版本 7.7 之前的 VDA 的站点：

- 卫星区域中的 VDA 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 随机注册到主要区域或本地区域中的 Controller。（最低版本为 7.7 的 VDA 首先选择本地区域。）

区域首选项

要使用区域首选项功能，您必须至少使用 StoreFront 3.7 和 Citrix Gateway 11.0-65.x。

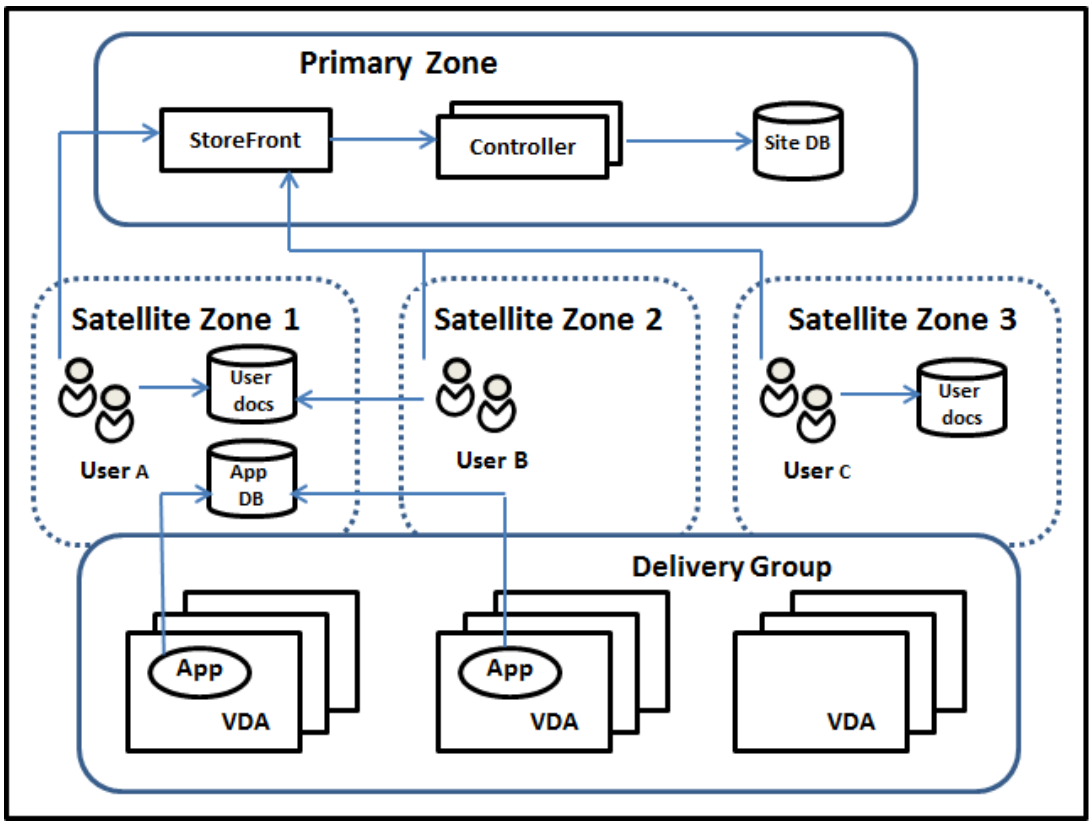
在多个区域的站点中，区域首选项功能为管理员提供更多的灵活性来控制哪些 VDA 可用于启动一款应用程序或桌面。

区域首选项的工作方式

有三种形式的区域首选项。您可能更喜欢使用特定区域中的 VDA，基于：

- 应用程序数据的存储位置。这称为应用程序的主区域。
- 用户的主区域数据的位置，例如配置文件或主区域共享。这称为用户的主区域。
- 用户的当前位置（Citrix Workspace 应用程序正在运行的位置）。这称为用户位置。

下图显示了多区域配置示例。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

在此示例中，VDA 分布在三个卫星区域中，但都处在同一个交付组中。因此，Broker 可以选择针对用户启动请求使用哪个 VDA。此示例指示用户可以运行其 Citrix Workspace 应用程序端点的几个位置：

- 用户 A 使用卫星区域 1 中安装了 Citrix Workspace 应用程序的设备。
- 用户 B 使用卫星区域 2 中的设备。
- 用户的文档可以存储在不同的位置。
  - 用户 A 和 B 使用卫星区域 1 中的共享。
  - 用户 C 使用来自卫星区域 C 的共享。
  - 其中一个已发布的应用程序使用位于卫星区域 1 中的数据库。

您可以通过为用户或应用程序配置一个主区域的方法将其与某个区域关联。然后，Delivery Controller 中的 Broker 会使用这些关联来帮助选择将会在其中启动会话的区域（如果资源可用）。您可以：

- 通过向某个区域添加用户的方法来为用户配置主区域。
- 通过编辑应用程序属性来为某个应用程序配置主区域。

一名用户或一个应用程序一次只能有一个主区域。（在由于用户组成员身份而出现多个区域成员身份时，可能会出现用户的例外；请参阅“其他注意事项”部分。但是，即使在这种情况下，Broker 只能使用一个主区域。）

尽管可以配置用户和应用程序的区域首选项，Broker 一次启动只能选择一个首选的区域。选择首选区域的默认优先次序为应用程序主区域 > 用户主区域 > 用户位置。您可以限制顺序；请参阅定制区域首选项。用户启动应用程序时：

- 如果该应用程序具有一个已配置的区域关联（一个应用程序主区域），那么首选的区域就是该应用程序的主区域。
- 如果该应用程序不具有配置的区域关联，但用户具有配置的区域关联（用户主区域），则首选的区域为该用户的主区域。
- 如果应用程序和用户都没有配置的区域关联，则首选区域为用户正运行 Citrix Workspace 应用程序实例的区域（用户位置）。如果该区域未定义，则使用随机的 VDA 和区域选择。负载平衡适用于首先区域中的所有 VDA。如果没有首选区域，负载平衡适用于交付组中所有 VDA。

定制区域首选项

配置（或删除）某个用户或应用程序的主区域时，也可以进一步限制如何使用区域偏好。

- 强制用户主区域使用：在交付组中，可以指定会话在用户的主区域（如果已配置）中启动，如果主区域没有可用资源，则不会故障转移到另一区域。在您必须避免在多个区域间复制大型配置文件或数据文件而带来的风险时，这一限制会很有用。换而言之，您宁可拒绝一次会话启动，也不愿在不同的区域中启动会话。
- 强制应用程序主区域使用：同样，配置某个应用程序的主区域时，可以指示仅在该区域启动应用程序，且在应用程序的主区域中资源不可用时不会故障转移到另一个区域。
- 无应用程序主区域，且忽略配置的用户主区域：如果不指定某个应用程序的主区域，还可以指示在启动该应用程序时不考虑配置的任何用户区域。例如，您可能希望用户使用用户位置区域首选项在设备附近的 VDA 上运行应用程序，即使某些用户可能具有不同的主区域亦如此。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

首选区域如何影响会话使用

用户启动一个应用程序或桌面时，Broker 希望使用首选的区域，而不是使用现有的会话。

如果启动应用程序或桌面的用户已经具有一个适合被启动资源的会话（例如，可以使用某个应用程序的会话共享，或一个已经在运行被启动资源的会话），但该会话正在不同于该用户/应用程序首选区域的区域中的 VDA 上运行，那么系统可能会创建新的会话。这满足了在正确的区域中启动的需求（如果具有可用的容量），而无需重新连接到该用户会话要求的较不理想区域中的会话。

要防止出现无法访问的孤立会话，允许对现有的断开连接的会话进行重新连接，即便它们处在非首选的区域中也是如此。

可满足一次启动的会话的理想顺序为：

1. 重新连接到首选区域中的现有会话。
2. 重新连接到不同于首选区域的区域中已断开连接的现有会话。
3. 在首选区域中启动新的会话。
4. 重新连接到不同于首选区域的区域中的现有已连接会话。
5. 在不同于首选区域的区域中启用一个新的会话。

其他区域首选项注意事项

- 如果您配置一个用户组（例如安全组）的主区域，该组的用户（通过直接或间接成员身份）关联到指定的区域。但是，用户可以是多个安全组的成员，因此可能具有通过其他组成员关系配置的不同主区域。在这种情况下，可能无法清晰确定该用户的主区域。

如果用户具有一个不通过组成员身份获得的已配置主区域，该区域将用于区域首选项。任何通过组成员身份获得的区域关联将被忽略。

如果该用户具有多个仅通过组成员身份获得的不同区域关联，则 Broker 会在这些区域中进行随机选择。Broker 完成选择之后，该区域将用于后续的会话启动，直到用户的组成员身份变更为止。

- 用户位置区域首选项要求由用来连接设备的 Citrix Gateway 来检测端点设备上的 Citrix Workspace 应用程序。必须对 Citrix Gateway 进行配置，以将 IP 地址范围与特定区域关联，同时必须通过 StoreFront 将已发现的区域标识传递到 Controller。

有关区域首选项的详细信息，请参阅 Zone preference internals（区域首选项内部）。

注意事项、要求和最佳做法

- 您可以将以下项目放置在一个区域中：Controller、计算机目录、主机连接、用户和应用程序。如果某个目录使用主机连接，请确保该目录和连接都位于相同的区域中。（但是，如果低延迟、高带宽连接可用，则可以位于不同的区域中。）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 如果将多个项目放置在一个卫星区域中，会影响站点与这些项目以及与跟它们相关的其他对象的交互方式。
  - 将 Controller 放置在一个卫星区域中时，假定这些计算机与同一区域中的虚拟机管理程序和 VDA 的（本地）连接情况良好。那么，在处理这些虚拟机管理程序和 VDA 计算机时，优先使用该卫星区域中的 Controller，而不是主要区域中的 Controller。
  - 某个虚拟机管理程序连接放置在一个卫星区域中时，假定通过该虚拟机管理程序连接管理的所有虚拟机管理程序也都位于该卫星区域中。那么，通过该虚拟机管理程序连接进行通信时，优先使用该卫星区域中的 Controller，而不是主要区域中的 Controller。
  - 某个计算机目录放置在一个卫星区域中时，假定该目录中的所有 VDA 计算机都位于该卫星区域中。首次注册了各个 VDA 后，并且激活了 Controller 列表自动更新机制后，尝试向站点注册时，优先使用本地 Controller，而不是主要区域中的 Controller。
  - Citrix Gateway 实例也可以与区域关联。对于此处所述的其他元素，这是在 StoreFront 最佳 HDX 路由配置中完成的，而不是在站点配置中完成的。某个 Citrix Gateway 与某个区域关联后，使用与该区域中的 VDA 计算机的 HDX 连接时，优先使用该 Citrix Gateway。
- 创建生产站点，然后创建第一个目录和交付组时，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。（如果您创建一个空站点，主要区域最初将仅包含 Controller。您可以在创建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。
- 始终将站点数据库保留在主要区域中。
- 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。这种灵活性允许您将在近距离内处于最佳运行状态的项目分隔开来。例如，将某个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。在区域之间移动项目之前，请考虑预料之外的潜在影响。请保持目录与其使用的主机连接位于相同的区域中，或者位于连接信号良好的区域中（例如，通过低延迟、高带宽网络建立连接）。
- 要实现最佳性能，请仅在主要区域中安装 Studio 和 Director。如果希望另一个 Studio 实例位于卫星区域中（例如，如果主要区域变得不可用，包含 Controller 的某个卫星区域将用作故障转移区域），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，请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 Citrix Gateway，即使您能够对该区域内部的连接使用 Citrix Gateway 也是如此。
- 谨记：要使用区域首选项功能，您必须至少使用 StoreFront 3.7 和 Citrix Gateway 11.0-65.x。

连接质量限制

卫星区域中的 Controller 直接执行与站点数据库的 SQL 交互。这对卫星区域与包含站点数据库的主要区域之间的链接的质量造成了一些限制。具体限制与该卫星区域中部署的 VDA 数和那些 VDA 上的用户会话数相关。因此，与具有大量

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

VDA 和会话数的卫星区域相比，只有少量 VDA 和会话数的卫星区域在与数据库的连接质量较差时也可以正常运行。

有关详细信息，请参阅延迟和 SQL 阻塞查询改进功能。

延迟对中转性能的影响

尽管区域允许用户使用延迟较高的链接，假定有一个本地 Broker，额外的延迟不可避免地会影响最终用户体验。对于用户执行的大多数操作，他们体验到的慢速是由卫星区域中的 Controller 与站点数据库之间的往返造成的。

对于启动应用程序，会话中转过程识别合适的 VDA 来向其发送会话启动请求时，会发生额外的延迟。

创建和管理区域

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，要将目录从一个区域移动到另一个区域，必须对该目录具有编辑权限。有关详细信息，请参阅委派管理。

如果使用 **Citrix Provisioning**：Citrix Provisioning 控制台不知道区域，因此，Citrix 建议使用 Studio 为卫星区域创建目录。在 Studio 中创建目录，并指定正确的卫星区域。因此，可以使用 Citrix Provisioning 控制台在该目录中预配计算机。（如果使用 Citrix Provisioning 向导创建目录，该目录将放置在主区域中。稍后您将不得不使用 Studio 将其移动到卫星区域。）

创建区域

1. 在 Studio 导航窗格中选择配置 **>** 区域。
2. 在“操作”窗格中选择创建区域。
3. 输入该区域的名称和说明（可选）。该名称在站点中必须唯一。
4. 选择要放置在新区域中的项目。可以过滤或搜索要从中选择项目的列表。也可以创建空区域；不需要选择任何项目。
5. 单击保存。

作为此方法的备选方法，可以在 Studio 中选择一个或多个项目，然后在“操作”窗格中选择创建区域。

更改区域名称或说明

1. 在 Studio 导航窗格中选择配置 **>** 区域。
2. 在中间窗格中选择一个区域，然后在“操作”窗格中选择编辑区域。
3. 更改区域名称、说明或两者。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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

将项目从一个区域移动到另一个区域

1. 在 Studio 导航窗格中选择配置 **>** 区域。
2. 在中间窗格中选择一个区域，然后选择一个或多个项目。
3. 将项目拖动到目标区域，或者在“操作”窗格中选择移动项目，然后指定要将项目移动到的区域。

此时将显示一条列出所选项目的确认消息，并询问您是否确实要移动全部项目。

谨记：如果目录使用连接到虚拟机管理程序或其他服务的主机连接，则该目录和连接位于相同的区域中。否则，性能可能会受到影响。如果移动一个项目，请同时移动另一个。

删除区域

区域必须不包含任何内容才能将其删除。不能删除主要区域。

1. 在 Studio 导航窗格中选择配置 **>** 区域。
2. 在中间窗格中选择一个区域。
3. 在“操作”窗格中选择删除区域。如果该区域不为空（包含项目），系统会要求您选择要移动这些项目的区域。
4. 确认删除。

添加用户的主区域

配置用户的主区域也称为将用户添加到区域。

1. 在 Studio 导航窗格中选择配置 **>** 区域，然后在中间窗格中选择一个区域。
2. 在“操作”窗格中选择将用户添加到区域。
3. 在将用户添加到区域对话框中，单击添加，然后选择要添加到该区域的用户和用户组。如果您指定已经具有主区域的用户，则会显示一条消息，提供两个选择：是 = 仅添加您指定的没有主区域的用户；否 = 返回用户选择对话框。
4. 单击确定。

对于具有已配置主区域的用户，您可能需要仅从他们的主区域启动会话：

1. 创建或编辑交付组。
2. 在用户页面上，选中如果已配置，则会话必须在用户的主区域中启动复选框。

由该交付组中用户启动的所有会话必须在用户的主区域中从计算机启动。如果交付组中的用户不具有已配置的主区域，此设置无效。

删除用户的主区域

此步骤也称为从区域中删除用户。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. 在 Studio 导航窗格中选择配置 **>** 区域，然后在中间窗格中选择一个区域。
2. 在“操作”窗格中选择从区域中删除用户。
3. 在将用户添加到区域对话框中，单击删除，然后选择要从该区域中删除的用户和用户组。此操作仅从该区域中删除用户；这些用户仍保留在他们所属的交付组和应用程序组。
4. 系统提示时确认删除。

管理应用程序的主区域

配置应用程序的主区域也称为将应用程序添加到区域。默认情况下，在多区域环境中，应用程序不具有主区域。

应用程序的主区域在该应用程序的属性中指定。可以在将应用程序添加到组时配置应用程序属性，也可以稍后配置。

- 在创建交付组、创建应用程序组或将应用程序添加到现有组时，请在向导的应用程序页面上选择属性。
- 要在添加应用程序后更改应用程序的属性，请在 Studio 导航窗格中选择应用程序。选择一个应用程序，然后在“操作”窗格中选择编辑应用程序属性。

在应用程序的属性/设置的区域页面上：

- 如果您想要该应用程序具有一个主区域：
  - 选择使用选定的区域来决定单选按钮，然后选择该区域。
  - 如果您希望该应用程序仅从选定的区域（不从任何其他区域）中启动，请选中该区域选择下方的复选框。
- 如果您不希望该应用程序具有一个主区域：
  - 选择请勿配置主区域单选按钮。
  - 如果您不希望 Broker 在启动该应用程序时考虑任何配置的用户区域，请选中该单选按钮下方的复选框。在这种情况下，既不会使用应用程序也不会使用用户主区域来确定此应用程序的启动位置。

包括指定区域在内的其他操作

创建至少一个卫星区域后，您可以在添加主机连接或创建目录时指定一个区域。

通常情况下，主要区域为默认区域。使用 Machine Creation Services 创建目录时，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

January 21, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 重要：
>
> 自 Citrix Virtual Apps and Desktops 7 2006 起，如果您的当前部署使用以下任一技术或主机类型，则只有在删除使用这些技术的项目后，才能将部署升级到当前版本。
>
> - 个人虚拟磁盘 (PvD)
> - AppDisk
> - 公有云主机类型：Amazon Web Services (AWS)、Citrix CloudPlatform、Microsoft Azure Classic、Microsoft Azure Resource Manager
>
> 有关详细信息，请参阅删除 PVD、AppDisk 和不受支持的主机。

简介

在创建站点时，可以选择性创建与托管资源的第一个连接。之后，可以更改该连接并创建其他连接。配置连接包括从受支持的虚拟机管理程序中选择连接类型，以及为该连接从资源中选择的存储和网络。

只读权限管理员可以查看连接和资源详细信息。您必须是完全权限管理员才能执行连接和资源管理任务。有关详细信息，请参阅委派管理。

与连接类型有关的信息的查找位置

可以使用受支持的虚拟化平台托管和管理 Citrix Virtual Apps 或 Citrix Virtual Desktops 环境中的计算机。系统要求一文列出了支持的类型。

有关详细信息，请参阅以下来源：

- **Citrix Hypervisor**（以前称为 **XenServer**）：
  - Citrix Hypervisor 虚拟化环境。
  - Citrix Hypervisor 文档。
- **Nutanix Acropolis**：
  - Nutanix 虚拟化环境。
  - Nutanix 文档。
- **VMware**：
  - VMware 虚拟化环境。
  - VMware 产品文档。
- **Microsoft Hyper-V**：
  - Microsoft System Center Virtual Machine Manager 虚拟化环境一文。
  - Microsoft 文档。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

主机存储

某个存储产品由支持的虚拟机管理程序托管时，则支持该存储产品。Citrix 支持将帮助这些存储产品供应商对问题进行故障排除并予以解决，以及根据需要在知识中心中记录这些问题。

预配计算机时，数据将按类型分类：

- 操作系统数据，其中包括主映像。
- 临时数据。此数据包括写入 MCS 预配计算机的非持久性数据、Windows 页面文件、用户配置文件数据，以及与 ShareFile 同步的任何数据。计算机每次重新启动时将丢弃该数据。

为每种数据类型提供独立的存储可以降低每个存储设备上的负载并提高性能，从而充分利用主机的可用资源。此外，这样还允许对不同的数据类型使用适当的存储。因为对某些数据而言，永久性和恢复能力比其他方面更加重要。

存储可以是虚拟机管理程序的共享存储（位于中央位置，与所有主机使用的任何主机分隔开来），也可以是其本地存储。例如，中央共享存储可以是一个或多个 Windows Server 2012 群集化存储卷（无论是否包含附加存储），也可以是存储供应商提供的设备。中央存储还可以提供自己的优化设置，例如，虚拟机管理程序存储控制路径以及通过合作伙伴插件直接访问。

在本地存储临时数据可避免必须遍历网络才能访问共享存储的问题。它还可以降低共享存储设备上的负载。共享存储的成本更高，因此，在本地存储数据可以降低费用。这些优势必须与虚拟机管理程序服务器上充足的存储空间的可用性进行权衡。

创建连接时，可以选择以下两种存储管理方法之一：虚拟机管理程序共享的存储或虚拟机管理程序的本地存储。

在一个或多个 Citrix Hypervisor 主机上使用本地存储作为临时数据存储时，请确保池中的每个存储位置都具有唯一的名称。（要在 XenCenter 中更改名称，请右键单击该存储并编辑名称属性。）

虚拟机管理程序共享的存储

虚拟机管理程序共享的存储方法存储需要长期存储在中央位置的数据，提供中央备份和管理。该存储容纳操作系统磁盘。

选择此方法时，可以选择是否对临时计算机数据使用本地存储（位于相同的虚拟机管理程序池中的服务器上）。此方法不需要永久存在或恢复能力不需要与共享存储中的数据相同（称为临时数据缓存）。本地磁盘有助于降低传输到主操作系统存储的流量。此磁盘在每次计算机重新启动后清除。此磁盘通过直写内存缓存进行访问。如果为临时数据使用本地存储，预配的 VDA 将绑定到特定的虚拟机管理程序主机。如果该主机出现故障，VM 将无法启动。

例外：使用群集存储卷 (Clustered Storage Volumes, CSV) 时，Microsoft System Center Virtual Machine Manager 不允许在本地存储中创建临时数据缓存磁盘。

创建连接以在本地存储临时数据，然后为每个 VM 的缓存磁盘大小和内存大小启用和配置非默认值。默认值是根据连接类型定制的，满足大多数情况下的需求。有关详细信息，请参阅创建计算机目录。

虚拟机管理程序还可以通过磁盘映像的读取缓存在本地提供优化技术。例如，Citrix Hypervisor 提供 IntelliCache，这可以减少传输到中央存储的网络流量。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

虚拟机管理程序的本地存储

虚拟机管理程序的本地存储在虚拟机管理程序上本地存储数据。使用此方法，主映像和其他操作系统数据将传输到站点中的虚拟机管理程序。此过程适用于初始计算机创建和将来的映像更新。此过程会导致管理网络中存在大量流量。映像传输也很耗时，并且映像对每个主机可用的时间也不同。

创建连接和资源

创建站点时，可以选择性创建第一个连接。站点创建向导包含以下各部分中介绍的与连接相关的页面。

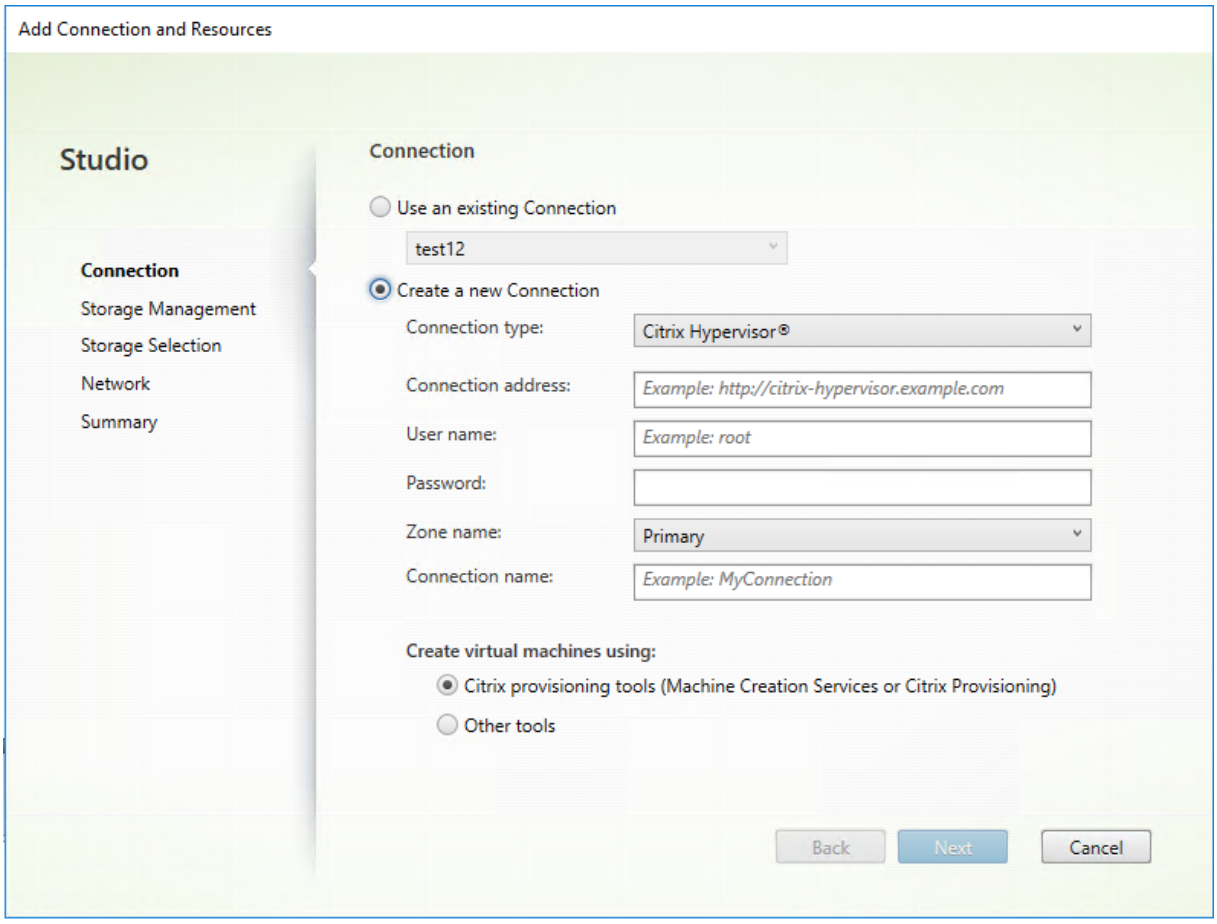
如果要在创建站点后创建连接，请从步骤 1 开始操作。

> 重要：
>
> 创建连接之前，主机资源（存储和网络）必须可用。

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. 该向导将引导您完成以下页面（具体的页面内容取决于所选连接类型）。完成每一页之后，请单击下一步，直到到达摘要页为止。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

连接

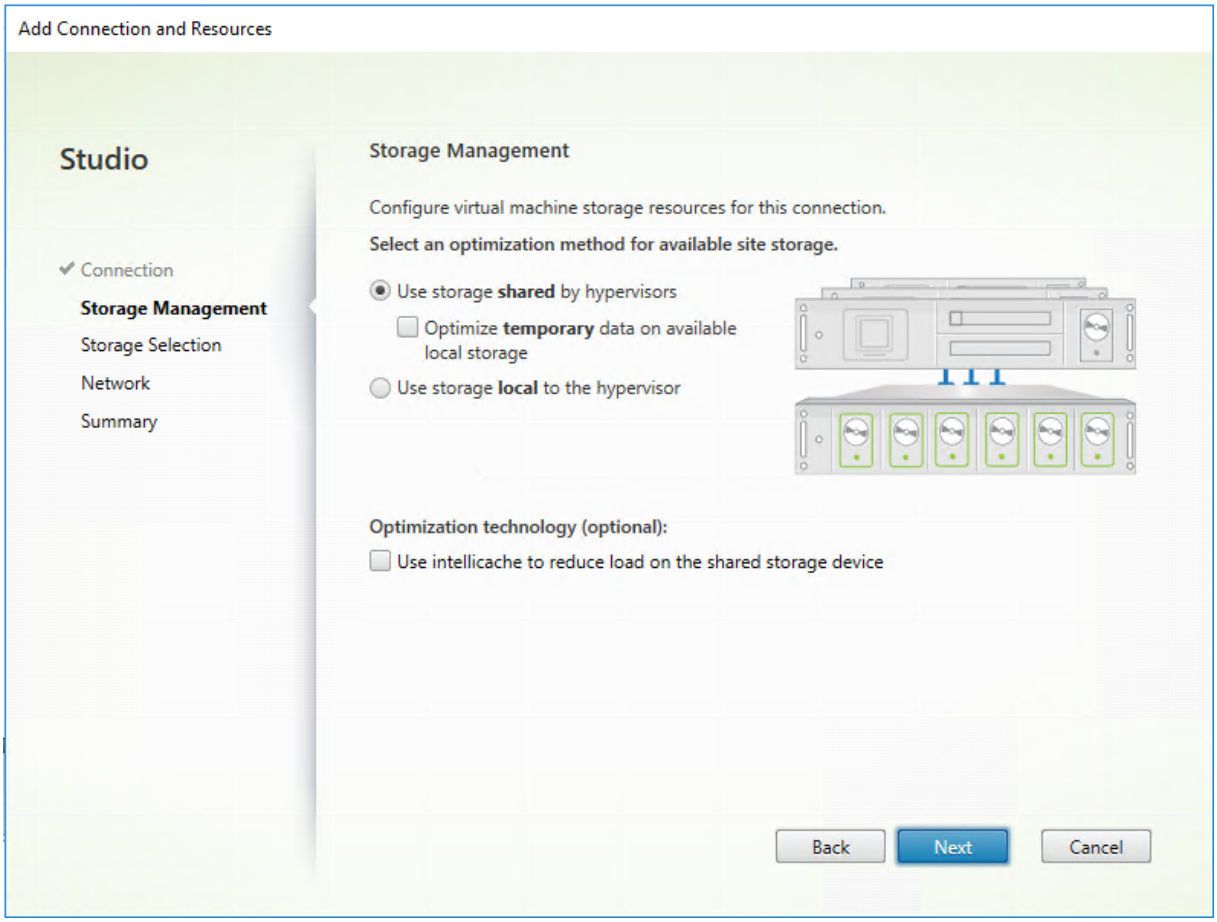


在连接页面上：

- 要创建一个连接，请选择创建新连接。要基于与现有连接相同的主机配置创建一个连接，请选择使用现有连接，然后选择相关连接。
- 在连接类型字段中选择要使用的虚拟机管理程序。
- 连接地址和凭据字段因所选连接类型而异。输入请求的信息。
- 输入连接名称。此名称将在 Studio 中显示。
- 选择用于创建虚拟机的工具：Studio 工具（例如，Machine Creation Services 或 Citrix Provisioning）或其他工具。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

管理存储



有关存储管理类型和方法的信息，请参阅主机存储。

如果要配置与 Hyper-V 或 VMware 主机的连接，请浏览到群集名称并选择一个名称。其他连接类型不需要群集名称。

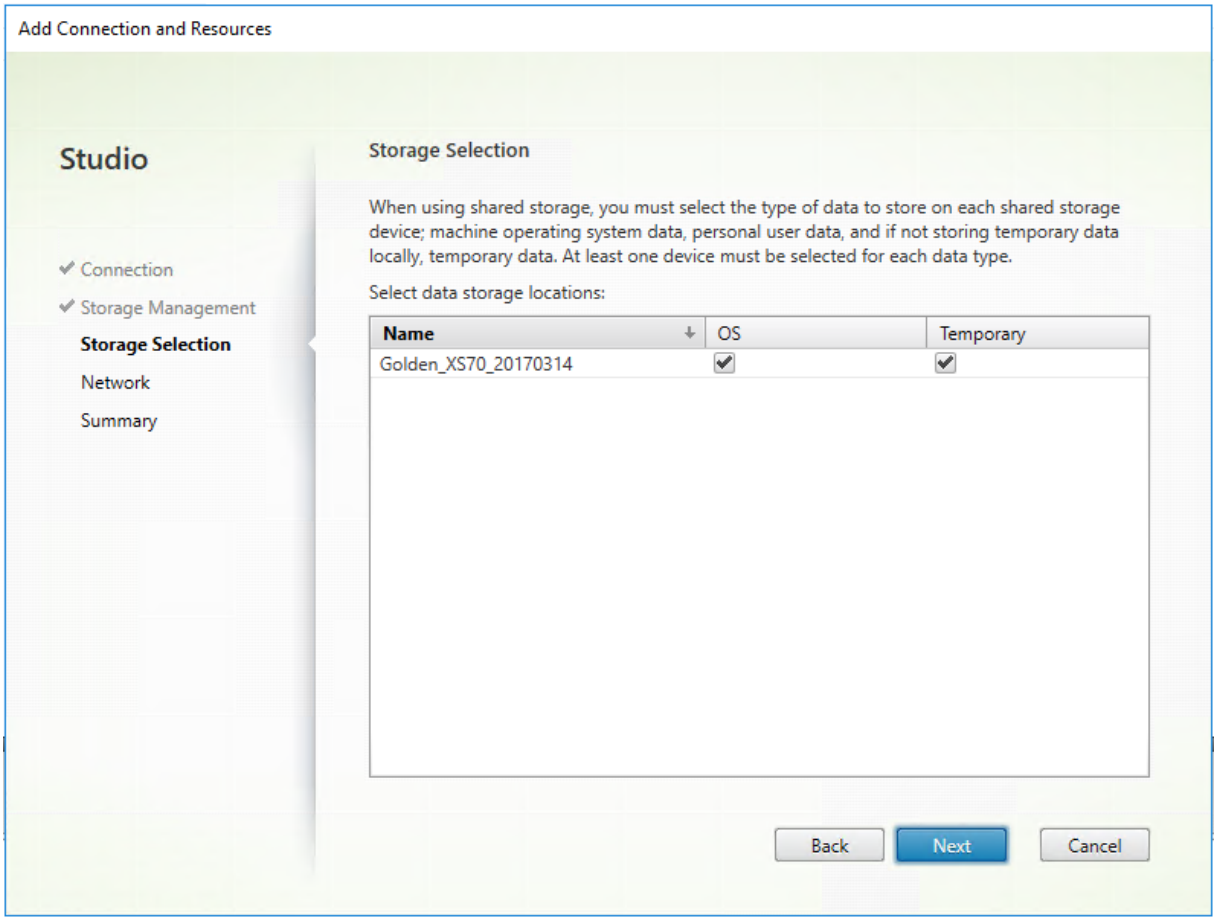
选择存储管理方法：虚拟机管理程序共享的存储或虚拟机管理程序的本地存储。

- 如果选择虚拟机管理程序共享的存储，请指出是否要在可用的本地存储上保存临时数据。（可以在使用此连接的计算机目录中指定非默认临时存储大小。）例外：使用群集存储卷 (CSV) 时，Microsoft System Center Virtual Machine Manager 不允许在本地存储中创建临时数据缓存磁盘。在 Studio 中配置该存储管理设置失败。

如果使用 Citrix Hypervisor 池中的共享存储，请指出是否要使用 IntelliCache 来降低共享存储设备上的负载。请参阅将 IntelliCache 用于 Citrix Hypervisor 连接。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

存储选择



有关存储选择的详细信息，请参阅主机存储。

请至少为每种可用的数据类型选择一个主机存储设备。在上一页面中选择的存储管理方法将影响此页面上可供选择的数据类型。请至少为每种受支持的数据类型选择一个存储设备，才能继续进入向导中的下一页面。

如果已选择由虚拟机管理程序共享的存储并在上一页中启用了 **Optimize temporary data on available local storage**（优化可用本地存储中的临时数据），则选择存储页面的下半部分将包含更多配置选项。您可以选择要用于存储临时数据的本地存储设备。

系统会显示当前选择的存储设备数量（在上图中，显示“已选择 1 个存储设备”）。将鼠标悬停在该条目上时，将显示选定的设备名称。

1. 单击选择更改要使用的存储设备。
2. 在选择存储对话框中，选中或取消选中存储设备复选框，然后单击确定。

网络

在网络页面中，输入资源的名称。此名称在 Studio 中显示，以表示与连接关联的存储和网络组合。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

选择 VM 使用的一个或多个网络。

摘要

在摘要页面上，检查所做的选择。完成后，单击完成。

谨记：如果在本地存储临时数据，则可以在创建包含使用此连接的计算机的计算机目录时为临时数据配置非默认值。请参阅创建计算机目录。

编辑连接设置

请勿使用此过程来重命名连接或创建连接。这些连接属于不同的操作。仅当当前主机具有新地址时才更改地址。向其他计算机输入地址会破坏连接的计算机目录。

无法更改连接的 **GPU** 设置，因为访问此资源的计算机目录必须使用特定于 GPU 的正确主映像。创建连接。

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，请按照面向可用设置的指导进行操作。
4. 完成后，单击应用以应用您执行的所有更改并保持打开窗口，或者单击确定应用更改并关闭窗口。

连接属性页面：

- 要更改连接地址和凭据，请选择编辑设置，然后输入新信息。
- 要为 Citrix Hypervisor 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 Citrix Hypervisor 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（与 Remote PC Access 集合使用），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最大电源操作数。在电源管理设置允许同时启动的计算机过多或过少时，这些设置非常有用。每种连接类型具有适用于大多数情况的特定默认值，不应更改。
- 同步操作 **(**所有类型**)** 设置指定两个值：一个是可在此连接上同时发生的最大绝对值，另一个是占使用此连接的所有计算机的最大百分比。必须同时指定绝对值和百分比值。实际应用的限值低于这些值。

  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
- 在连接选项字段中输入信息时，请遵循 Citrix 技术支持代表或明确的文档说明的指导。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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，也可以针对单台计算机打开或关闭维护模式。此外，还可以为计算机目录或交付组中的计算机打开或关闭维护模式。

删除连接

如果删除连接，会导致大量计算机被删除，并会导致数据丢失。请确保受影响计算机上的用户数据已经备份，或者已不再需要。

删除连接之前，请确保：

- 所有用户都已从该连接上所存储的计算机中注销。
- 没有仍在运行的已断开连接的用户会话。
- 已为池计算机和专用计算机打开维护模式。
- 关闭连接使用的计算机目录中的所有计算机。

删除计算机目录引用的连接时，该目录会变为不可用。如果有目录引用此连接，可以选择删除该目录。删除目录前，请确保其他连接未使用此目录。

1. 在 **Studio** 导航窗格中选择配置 **>** 托管。
2. 选择连接，然后在操作窗格中选择删除连接。
3. 如果此连接上存储了计算机，系统会询问您是否删除这些计算机。如果要将其删除，请指定应对关联的 Active Directory 计算机帐户执行的操作。

重命名或测试连接

1. 在 **Studio** 导航窗格中选择配置 **>** 托管。
2. 选择连接，然后在操作窗格中选择重命名连接或测试连接。

查看连接上的计算机详细信息

1. 在 **Studio** 导航窗格中选择配置 **>** 托管。
2. 选择连接，然后在操作窗格中选择查看计算机。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

上方窗格列出通过此连接访问的计算机。选择某台计算机可在下方窗格查看其详细信息。对于打开的会话，还会提供会话详细信息。

使用搜索功能可快速查找计算机。从窗口顶部的列表中选择保存的搜索，或者创建搜索。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. 选择一个连接，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。某些操作不可用，具体取决于计算机状态和连接主机类型。

操作	说明
启动	启动计算机（如果计算机关闭或挂起）。
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，则桌面仍保持当前状态。
启用维护模式	暂时停止与计算机的连接。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。）
从交付组中移除	从交付组中移除某台计算机不会从交付组使用的计算机目录中删除该计算机。仅当计算机未连接任何用户时，才能将其移除。在移除计算机时，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，用户将不再拥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阻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，可能面临更新未完成计算机就已关机的风险。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

编辑存储

可以显示用于存储使用连接的 VM 的操作系统和临时数据的服务器的状态。还可以指定用于每种数据类型的存储的服务器。

1. 在 **Studio** 导航窗格中选择配置 **>** 托管。
2. 选择相应连接，然后在操作窗格中选择编辑存储。
3. 在左侧窗格中，选择数据类型：操作系统或临时数据。
4. 选中或取消选中所选数据类型的一个或多个存储设备对应的复选框。
5. 单击确定。

列表中的每个存储设备都包含其名称和存储状态。有效存储状态值如下：

- 使用中：存储正用于创建计算机。
- 被取代：存储正仅用于现有计算机。不会将新计算机添加到此存储中。
- 未在使用中：存储未用于创建计算机。

如果取消选中当前处于使用中状态的设备对应的复选框，其状态将更改为被取代。现有计算机将继续使用该存储设备（并且可以向其中写入数据），因此，即使在该位置停止用于创建计算机后，该位置也有可能会满载。

删除、重命名或测试资源

1. 在 **Studio** 导航窗格中选择配置 **>** 托管。
2. 选择资源，然后在操作窗格的删除资源、重命名资源或测试资源中选择相应的条目。

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：确定在用户未输入任何内容的情况下，用户设备与虚拟桌面之间的连接可以保持不中断的时长。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长。使用断开连接的会话计时器和断开连接的会话计时器间隔策略设置。

如果更新其中任何一项设置，请确保部署中的设置一致。

有关详细信息，请参阅策略设置文档。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

本地主机缓存

May 19, 2023

为确保 Citrix Virtual Apps and Desktops 站点数据库始终可用，Citrix 建议按照 Microsoft 的高可用性最佳做法开始部署容错 SQL Server。（有关支持的 SQL Server 高可用性功能，请参阅数据库。）但是，网络问题和中断会导致用户无法连接到其应用程序或桌面。

本地主机缓存功能允许在发生中断时，站点中的连接代理操作能够继续。本地 Citrix 环境中的 Delivery Controller 与站点数据库之间的连接失败时会出现中断。在站点数据库无法访问达 90 秒时，将使用本地主机缓存。

截至 XenApp and XenDesktop 7.16，连接租用功能（早期版本中的高可用性功能的前身）已从产品中删除，并且不再可用。

数据内容

本地主机缓存包含以下信息（主数据库中的一部分信息）：

- 为其分配了访问对从站点发布的资源的权限的用户和组的身份。
- 当前正在使用或最近使用了站点中已发布资源的用户的身份。
- 站点中配置的 VDA 计算机（包括 Remote PC Access 计算机）的身份。
- 主动使用 Citrix Receiver 计算机连接到已发布的资源的客户端的标识（名称和 IP 地址）。

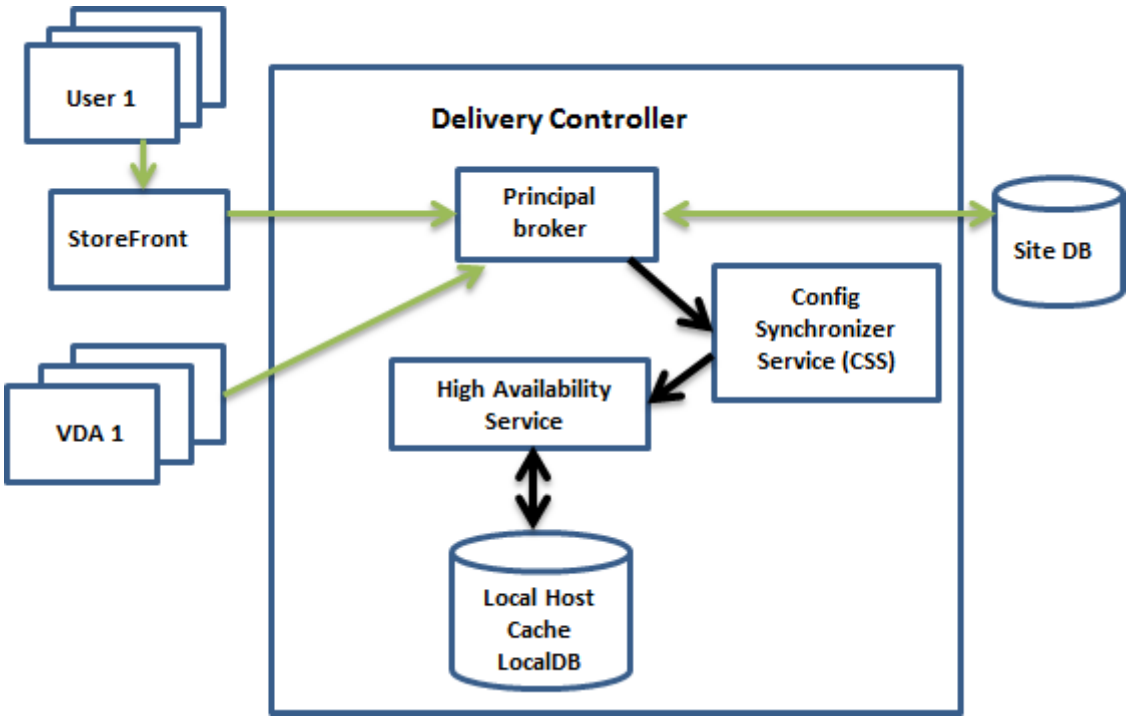
此外，它还包含主数据库不可用时建立且当前处于活动状态的连接的信息：

- Citrix Receiver 执行的任何客户端计算机端点分析的结果。
- 站点涉及的基础结构计算机（例如 NetScaler Gateway 和 StoreFront 服务器）的标识。
- 用户进行的最近活动的日期和时间以及类型。

工作原理

下图说明了正常操作过程中本地主机缓存组件和通信路径。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



正常操作过程中

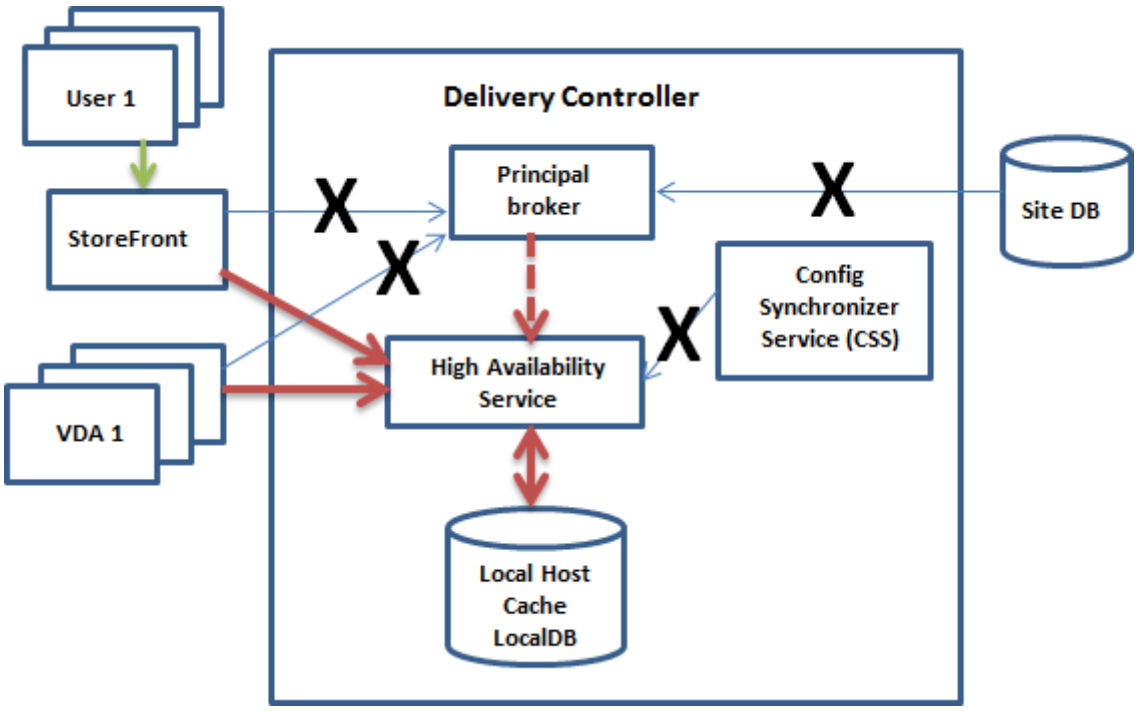
- Connector 上的主 *Broker* (Citrix Broker Service) 接受来自 StoreFront 的连接请求。Broker 与站点数据库进行通信，以便使用已注册到 Controller 的 VDA 连接用户。
- Citrix Config Synchronizer Service (CSS) 大约每隔 1 分钟与 Broker 核对一次，以查看是否做出了任何更改。这些更改可能是管理员发起的更改（例如，更改交付组属性）或系统操作（例如，计算机分配）。
- 如果自上次检查后更改了配置，CSS 会将信息同步（复制）到 Connector 上的辅助 Broker。（辅助 Broker 也称为高可用性服务。）

  所有配置数据都会被复制，而不仅仅是自上次核对后更改的项目。CSS 将配置数据导入到 Controller 上的 Microsoft SQL Server Express LocalDB 数据库中。此数据库称为本地主机缓存数据库。CSS 确保本地主机缓存数据库中的信息与站点数据库中的信息一致。每次同步时，都会重新创建本地主机缓存数据库。

  当您安装 Connector 时，Microsoft SQL Server Express LocalDB（由本地主机缓存数据库使用）会自动安装。（在从命令行安装 Controller 时，可以禁止此安装。）本地主机缓存数据库不能在 Controller 之间共享。您不需要备份本地主机缓存数据库。每次检测到配置更改时都会重新创建此数据库。
- 如果自上次检查后没有进行任何更改，则不复制数据。

下图说明了主 Broker 失去与站点数据库的联系时（中断开始）通信路径的变化。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



中断过程中

当中断开始时：

- 辅助代理开始侦听并处理连接请求。
- 中断开始时，辅助代理没有当前的 VDA 注册数据，但当 VDA 与其通信时，就会立即触发注册过程。在该过程中，辅助 Broker 还获取有关该 VDA 的当前会话信息。
- 在辅助 Broker 处理连接的同时，Broker 主体将继续监视连接。恢复连接时，代理主体将指示辅助代理停止侦听连接信息，并且代理主体将继续执行代理操作。下次 VDA 与代理主体通信时，将触发注册过程。辅助代理将删除上一次中断中剩余的任何 VDA 注册。了解部署中是否发生配置变更时，CSS 将继续同步信息。

在同步期间发生中断这种不太可能发生的事件中，会丢弃当前导入，并使用已知的最后一个配置。

事件日志提供有关同步和中断的信息。

对中断模式下的操作没有时间限制。

标准模式与中断模式之间的转换不影响现有会话。它只影响新会话的启动。

您还可以有意触发中断。有关执行此操作的原因和方法的详细信息，请参阅强制中断。

具有多个 **Controller** 的站点

除了其他任务外，CSS 还定期向辅助 Broker 提供有关区域中所有 Controller 的信息。（如果您的部署中没有多个区域，则此操作影响站点中的所有 Controller。）有了那些信息，每个辅助 Broker 都可以了解该区域中的其他 Controller 上运行的所有对等辅助 Broker。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

辅助 Broker 在单独的通道中相互通信。如果发生中断，这些 Broker 将使用正在其中运行的计算机的按字母顺序排列的 FQDN 名称列表来确定（选择）哪个辅助 Broker 将在区域中代理操作。在中断期间，所有 VDA 向选定的辅助 Broker 注册。区域中的非选定辅助 Broker 将主动拒绝传入连接和 VDA 注册请求。

如果在中断期间某个选定的辅助代理出现故障，则将选择另一个辅助代理来接管，并且 VDA 将在新选定的辅助代理中重新注册。

在中断期间，如果重新启动某个 Controller：

- 如果该 Controller 不是选定的 Broker，则无法重新启动。
- 如果该 Controller 是选定的 Broker，此时选择另一个 Controller，这会导致 VDA 进行注册。重新启动的 Controller 开启后，它会自动接管代理，这会导致 VDA 再次注册。在这种情况下，在注册期间，性能会受影响。

如果在正常操作期间关闭某个 Controller，然后在中断期间将其开启，如果该 Controller 被选为 Broker，则无法在该 Controller 上使用本地主机缓存。

事件日志提供有关选择的信息。

中断期间不可用的功能以及其他差异

对中断模式下的操作没有时间限制。但是，Citrix 建议尽快恢复连接。

中断过程中：

- 您不能使用 Studio。
- 您对 PowerShell SDK 具有优先的访问权限。
  - 必须首先：
    - 添加值为 1 的注册表项 `EnableCssTestMode`：`New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
    - 使用端口 89：`Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ContollerDNSName, DesktopGroupName, RegistrationState`
  - 运行这些命令后，您可以访问：
    - 所有 `Get-Broker*` cmdlet。
    - 电源管理 cmdlet `New-BrokerHostingPowerAction`、`Set-BrokerHostingPowerAction` 和 `Remove-BrokerHostingPowerAction`。
- 无法从 Host Service 获取虚拟机管理程序凭据。所有计算机都处于未知电源状态，因此无法发出任何电源操作。但是，已打开电源的主机上的 VM 可以用于连接请求。
- 仅当在正常操作过程中发生了分配时，才可以使用分配的计算机。在中断期间不能执行新分配。
- 不能自动注册和配置 Remote PC Access 计算机。但是，正常操作过程中注册和配置的计算机可以使用。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 如果资源在不同的区域中，服务器托管的应用程序和桌面用户使用的会话可能超过其配置的会话限制。
- 用户只能从包含当前处于活动状态的/选定的二级 Broker 的区域中已注册的 VDA 启动应用程序和桌面。断电期间不支持跨区域启动（从一个区域中的二级 Broker 到另一个区域中的 VDA）。
- 如果对交付组中的 VDA 开始计划的重新启动之前发生站点数据库中断，则重新启动将在中断结束后开始。这可能会产生意想不到的结果。有关更多详细信息，请参阅计划的重新启动因数据库中断而延迟。
- 无法配置区域首选项。如果已配置，会话启动时将不考虑首选项。
- 会话启动不支持使用标签来指定区域的标记限制。配置了此类标记限制并启用了 StoreFront 应用商店的高级运行状况检查选项后，会话可能会间歇性无法启动。

应用程序和桌面支持

本地主机缓存支持服务器托管的应用程序和桌面以及静态（已分配）桌面。

本地主机缓存支持池交付组中的桌面 VDA，如下所示：

- 默认情况下，发生中断时，启用了 `ShutdownDesktopsAfterUse` 属性的池交付组（通过 MCS 或 Citrix Provisioning 创建）中进行电源管理的桌面 VDA 将被置于维护模式。您可以更改此默认值，以允许在中断期间使用这些桌面。

  但是，中断期间您无法依赖电源管理。（正常操作恢复后，电源管理恢复。）此外，由于这些桌面未重新启动，它们可能包含前一个用户的数据。

- 要覆盖默认行为，必须在站点范围内启用并针对受影响的每个交付组启用。运行以下 PowerShell cmdlet。

  站点范围：

  ```
  Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
  ```

  对于每个受影响的交付组，请运行以下 PowerShell 命令：

  ```
  Set-BrokerDesktopGroup -Name "name"-ReuseMachinesWithoutShutdownInOutage
   $true
  ```

  在站点和交付组中启用此功能不会影响配置的 `ShutdownDesktopsAfterUse` 属性在正常操作期间的作用方式。

RAM 大小注意事项

LocalDB 服务可以使用大约 1.2 GB 的 RAM（每个数据库缓存最多 1 GB，另加 200 MB 用于运行 SQL Server Express LocalDB）。如果中断持续较长时间，且发生了很多登录（例如，12 个小时内 10K 用户），则辅助 Broker 最多可以使用 1 GB 的 RAM。这些内存要求是 Controller 的正常 RAM 要求之外的要求，因此您可能需要增加 RAM 总容量。

如果您对站点数据库使用 SQL Server Express 安装，则服务器将有两个 sqlserver.exe 进程。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

CPU 核心和套接字配置注意事项

Controller 的 CPU 配置，尤其是可用于 SQL Server Express LocalDB 的核心数，直接影响本地主机缓存性能，甚至比内存分配还要严重。仅在数据库不可访问且辅助 Broker 处于活动状态时，在中断期间观察此 CPU 开销。

虽然 LocalDB 可以使用多个核心（最多 4 个），但只能使用一个套接字。添加多个套接字不会提高性能（例如，每个有 4 个套接字和 1 个核心）。相反，Citrix 建议结合使用多个套接字和多个核心。在 Citrix 测试中，2x3（2 个套接字，3 个核心）配置提供的性能优于 4x1 和 6x1 配置。

存储注意事项

由于在中断期间用户访问资源，LocalDB 会增长。例如，在以每秒 10 次登录运行的登录/注销测试期间，数据库以每 2-3 分钟 1 MB 的速度增长。在正常操作恢复时，将重新创建本地数据库并返还空间。但是，安装了 LocalDB 的驱动器上必须有足够的空间，以允许在中断期间数据库增长。在中断期间，本地主机缓存中还会发生更多 I/O 操作：大约每秒 3 MB 的写入操作，以及数十万次读取操作。

性能注意事项

在中断期间，一个二级 Broker 处理所有连接，因此，在正常操作过程中在多个 Controller 之间进行负载平衡的站点（或区域）中，选定的二级 Broker 需要处理的请求数可能远高于中断期间的正常数。因此，CPU 需求会比较高。站点（区域）中的每个辅助 Broker 都必须能够处理本地主机缓存数据库和所有受影响的 VDA 造成的额外负载，因为在中断期间选择的反映这个月 Broker 可能会发生变化。

VDI 限制：

- 在单区域 VDI 部署中，中断期间最多可以有效处理 10,000 个 VDA。
- 在多区域 VDI 部署中，中断期间在每个区域中最多可以有效处理 10,000 个 VDA，在站点中最多可以处理 40,000 个 VDA。例如，在中断期间，可以有效处理以下站点之一：
  - 具有四个区域的站点，每个区域包含 10,000 个 VDA。
  - 具有七个区域的站点，一个区域包含 10,000 个 VDA，另外六个区域每个包含 5,000 个 VDA。

在中断期间，站点内的负载管理会受到影响。负载评估器（尤其是会话计数规则）会超额。

在所有 VDA 向 Broker 中注册的这段时间，该 Broker 可能没有与当前会话有关的完整信息。因此，在该时间间隔内的用户连接请求会导致启动新会话，即使有可能重新连接到现有会话也是如此。此时间间隔（在此期间，在重新注册过程中，“新”二级 Broker 从所有 VDA 获取会话信息）无法避免。在该过渡时间间隔内，中断开始时已连接的会话不受影响，但新会话和会话重新连接可能会受影响。

每当 VDA 必须注册时，都会出现此时间间隔：

- 中断开始：从主 Broker 迁移到辅助 Broker 时。
- 中断期间辅助 Broker 出现故障：从出现故障的辅助代理迁移到新选定的辅助代理时。
- 从中断恢复：正常操作恢复且主 Broker 恢复控制时。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

可以通过降低 Citrix Broker Protocol 的 `HeartbeatPeriodMs` 注册表值（默认为 600000 毫秒，即 10 分钟）来缩短该时间间隔。此检测信号值是 VDA 执行 ping 操作的时间间隔的两倍，因此，默认值将导致 ping 操作每隔 5 分钟执行一次。

例如，以下命令将检测信号更改为 5 分钟（300000 毫秒），这将导致 ping 操作每隔 2.5 分钟执行一次：

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name
HeartbeatPeriodMs -PropertyType DWORD -Value 300000
```

更改检测信号值时请务必小心谨慎。增大频率会导致处于标准模式和中断模式时 Controller 上的负载增加。

无论 VDA 注册的速度有多快，都无法完全消除该时间间隔。

在二级 Broker 之间同步所需的时间会随对象（例如 VDA、应用程序、组）数增加。例如，同步 5000 个 VDA 可能需要 10 分钟或更长时间来完成。

XenApp 6.x 各版本中的差异

尽管此本地主机缓存实施与 XenApp 6.x 及更早 XenApp 版本中的本地主机缓存功能的名称相同，但进行了显著的改进。此实施更强大且不易损坏。维护要求降低到最小，例如，不再需要定期运行 `dsmaint` 命令。此本地主机缓存在技术上是完全不同的实现。

管理本地主机缓存

要使本地主机缓存正确工作，每个 Controller 上的 PowerShell 执行策略都必须设置为 RemoteSigned、Unrestricted 或 Bypass。

SQL Server Express LocalDB

在安装 Controller 或从低于 7.9 的版本升级 Controller 时，会自动安装本地主机缓存使用的 Microsoft SQL Server Express LocalDB 软件。只有辅助 Broker 与此数据库进行通信。不能使用 PowerShell cmdlet 更改与此数据库有关的任何内容。LocalDB 不能在多个 Controller 之间共享。

无论是否启用本地主机缓存，都会安装 SQL Server Express LocalDB 数据库软件。

要阻止其安装，请使用 `XenDesktopServerSetup.exe` 命令安装或升级 Controller，并包含 `/exclude "Local Host Cache Storage (LocalDB)"` 选项。但是，请注意，没有数据库时，无法使用本地主机缓存功能，并且不能将不同的数据库用于辅助 Broker。

安装此 LocalDB 数据库对您是否安装 SQL Server Express 以用作站点数据库没有影响。

有关将较早的 SQL Server Express LocalDB 版本替换为较新版本的信息，请参阅替换 SQL Server Express LocalDB。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

产品安装和升级后的默认设置

在全新安装 Citrix Virtual Apps and Desktops（最低版本 7.16）过程中，启用本地主机缓存。

升级（到 7.16 版或更高版本）后，如果整个部署中的 VDA 数量低于 10000，则将启用本地主机缓存。

启用和禁用本地主机缓存

- 要启用本地主机缓存，请输入：

  ```
  Set-BrokerSite -LocalHostCacheEnabled $true
  ```

  要确定是否已启用本地主机缓存，请输入 `Get-BrokerSite`。检查 `LocalHostCacheEnabled` 属性是否为 `True`。

- 要禁用本地主机缓存，请输入：

  ```
  Set-BrokerSite -LocalHostCacheEnabled $false
  ```

谨记：截至 XenApp and XenDesktop 7.16，连接租用（自版本 7.6 起提供的本地主机缓存功能之前的功能）已从产品中删除，并且不再可用。

验证本地主机缓存是否正在运行

要验证本地主机缓存是否已设置并正常运行，请执行以下操作：

- 确保同步导入成功完成。检查事件日志。
- 确保在每个 Delivery Controller 上创建 SQL Server Express LocalDB 数据库。这证实，如果需要，辅助 Broker 可以接管。
  - 在 Delivery Controller 服务器上，浏览到 `C:\Windows\ServiceProfiles\NetworkService`。
  - 验证 `HaDatabaseName.mdf` 和 `HaDatabaseName_log.ldf` 是否已创建。
- 在 Delivery Controller 上强制中断。验证本地主机缓存是否正常运行后，请记住将所有 Controller 重置回普通模式。这可能大约需要 15 分钟。

事件日志

事件日志记录何时发生同步和中断。在事件查看器日志中，中断模式称为高可用性模式。*

Config Synchronizer Service:

在正常操作期间，当 CSS 使用本地主机缓存代理将配置数据导入到本地主机缓存数据库时，可能会发生以下事件。

- 503：Citrix Config Sync Service 收到更新的配置。此事件指示同步过程的开始。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 504：Citrix Config Sync Service 导入了更新的配置。配置导入已成功完成。
- 505：Citrix Config Sync Service 导入失败。配置导入未成功完成。如果以前的成功配置可用，发生中断时将使用该配置。但是，它将在当前配置中过期。如果以前的配置都不可用，服务将无法在中断期间参与会话中转。在这种情况下，请参阅故障排除部分，并与 Citrix 支持部门联系。
- 507：Citrix Config Sync Service 放弃了导入，因为系统处于中断模式，并且正在使用本地主机缓存代理进行代理。服务收到了新的配置，但导入被放弃，因为发生中断。这是预期的行为。
- 510: No Configuration Service configuration data received from primary Configuration Service.（510: 未从主 Configuration Service 收到任何 Configuration Service 配置数据。）
- 517: There was a problem communicating with the primary Broker.（517: 与主 Broker 通信时出现问题。）
- 518: Config Sync 脚本已中止，因为次要 Broker (高可用性服务) 未在运行。

High Availability Service:

此服务又称为本地主机缓存代理。

- 3502: 发生中断，本地主机缓存代理正在执行代理操作。
- 3503：已解决中断并已恢复正常操作。
- 3504：指示选择哪个本地主机缓存代理，以及参与选择的其他本地主机缓存代理。

强制中断

您可能希望有意强制中断。

- 如果您的网络反复开启和关闭。在网络问题解决之前强制中断网络可以防止持续在正常模式与中断模式之间转换（并且会导致频繁出现 VDA 注册风暴）。
- 要测试灾难恢复计划。
- 帮助确保本地主机缓存正常运行。
- 更换或维修站点数据库服务器时。

要强制中断，请编辑包含 Delivery Controller 的每个服务器的注册表。在 `HKLM\Software\Citrix\DesktopServer\LHC` 中，创建 `OutageModeForced` 作为 `REG_DWORD` 并将其设置为 1。此设置指示本地主机缓存代理进入中断模式，而无论数据库的状态为何。将该值设置为 0 将使本地主机缓存代理退出中断模式。

要验证事件，请监视 `C:\ProgramData\Citrix\WorkspaceCloud\Logs\Plugins\HighAvailabilityService` 中的 `Current_HighAvailabilityService` 日志文件。

故障排除

向本地主机缓存数据库的同步导入失败并且发布了 505 事件时，可以使用多个故障排除工具。

CDF 跟踪：包含 `ConfigSyncServer` 和 BrokerLHC‘ 模块的选项。那些选项与其他 Broker 模块一起可能会确定问题。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

报告：如果同步导入失败，可以生成报告。此报告在导致出错的对象所在的位置停止。此报告功能影响同步速度，因此，Citrix 建议在不使用时禁用它。

要启用并生成 CSS 跟踪报告，请输入以下命令：

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -PropertyType DWORD -Value 1
```

HTML 报告发布在 `C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.html` 上。

生成报告后，输入以下命令以禁用报告功能：

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```

导出 **Broker** 配置：提供准确的配置以用于调试目的。

```
Export-BrokerConfiguration | Out-File <file-pathname>
```

例如，`Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`。

虚拟 IP 和虚拟环回

January 21, 2022

> 重要：
>
> Windows 10 Enterprise 多会话不支持远程桌面 IP 虚拟化（虚拟 IP），我们不支持 Windows 10 Enterprise 多会话上的虚拟 IP 或虚拟环回。

Windows Server 2016 计算机支持虚拟 IP 和虚拟环回功能。这些功能不适用于 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的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、身份验证或其他需要唯一 IP 地址或环回地址的目的。其他应用程序可能会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，因为该端口正在使用中。要使这些应用程序能够在 Citrix Virtual Apps 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 Server 上启用并配置此功能。（不需要 Citrix 策略设置。）
- 要使用 Citrix 虚拟环回，请在 Citrix 策略中配置两项设置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

虚拟 IP

在 Windows Server 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 Citrix Virtual Apps 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的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的 IP 地址和端口以及哪些进程名称正在打开这些端口。
4. 配置任何打开服务器的 IP 地址（0.0.0.0 或 127.0.0.1）的进程。
5. 为确保应用程序不会在其他端口上打开相同的 IP 地址，请启动该应用程序的另一个实例。

Microsoft 远程桌面 (RD) IP 虚拟化的工作方式

- 必须在 Microsoft 服务器上启用虚拟 IP 地址。

  例如，在 Windows Server 2016 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，该会话会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`、`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，应用程序只能看到要使用的正确 IP 地址。应用程序试图侦听 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）。应用程序打开的任何源连接都来自绑定到该应用程序的 IP 地址。

在返回地址的函数（如 `GetAddrInfo()`，Windows 策略进行控制）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。有关 Windows 策略的详细信息，请参阅 Windows Server 中的 RDS IP 虚拟化。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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，禁用此设置。此功能仅适用于虚拟 IP 虚拟环回程序列表策略设置指定的应用程序。
- 虚拟 IP 虚拟环回程序列表。此策略设置指定使用虚拟 IP 环回功能的应用程序。此设置仅在启用了虚拟 IP 环回支持策略设置时有效。

相关功能

可以使用以下注册表设置来确保虚拟环回的优先级高于虚拟 IP。此功能称为首选环回。但是，操作时请注意以下事项：

- 仅当同时启用了虚拟 IP 和虚拟环回时才使用首选环回。否则，您可能会收到意外的结果。
- 注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

在应用程序所在的服务器运行注册表。

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP
- 名称：PreferLoopback，类型：REG_DWORD，数据：1
- 名称：PreferLoopbackProcesses，类型：REG_MULTI_SZ，数据：< 进程列表 > 进程列表 >

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Delivery Controller

August 2, 2022

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：生产站点始终至少拥有两个位于不同物理服务器上的 Controller，这是最佳做法。如果一个 Controller 出现故障，其他的 Controller 可以管理连接和站点。
- 可扩展性：随着站点活动的增加，Controller 上的 CPU 使用率将会提高，数据库活动也会增加。更多的 Controller 使您能够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 与主要区域中的站点数据库通信。

> 重要：
>
> 请勿在配置站点后更改 Controller 的计算机名称或域成员身份。

VDA 如何向 Controller 注册

VDA 必须首先向站点的 Delivery Controller 注册（建立连接），然后该 VDA 才可以使用。有关 VDA 注册的信息，请参阅向 Controller 注册 VDA。

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。

在 SQL 群集或 SQL 镜像安装中，不支持在节点上安装控制器。

将 Delivery Controller 添加到站点时，请务必将该计算机的登录凭据添加到用于实现高可用性的任何副本 SQL Server 中。

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，请在运行脚本之前启用 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。该 cmdlet 可确保已在要镜像的连接字符串中设置故障转移合作伙伴。

在添加、删除或移动 Controller 后：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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。无法将安装了此软件的早期版本的 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. 如果您尚未创建站点，请启动 Studio。系统会提示您创建站点。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。

   如果计划生成用于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**

从站点中删除 Controller 不会卸载 Citrix 软件或任何其他组件。该操作将从数据库中删除 Controller，这样它就不能再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。如果不再需要登录，则必须手动删除登录信息。删除登录需要 `securityadmin` 服务器角色权限。

> 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。如果要在短时间内删除 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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**。如果您没有正确的数据库权限，则可以生成一个脚本，该脚本允许具有这些权限的人员（例如数据库管理员）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 Citrix Provisioning 预配的或者 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) 预配的 VDA 从一个站点移动到另一个站点。MCS 不支持将 VDA 检查的 ListOfDDC 更改为向 Controller 注册。使用 MCS 预配的 VDA 始终检查与创建这些 VDA 时的站点关联的 ListOfDDC。

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，指定站点 2 中某个控制器的 FQDN（DNS 条目）。

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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。站点 1 中在其中注册了 VDA 的 Controller 不在站点 2 中的 Controller 所发送的列表中。因此，VDA 将重新注册，在站点 2 列表中的 Controller 中进行选择。从此时开始，VDA 会从站点 2 中自动更新信息。

有关如何使用组策略编辑器的信息，请参阅 Citrix 策略文档。

VDA 注册

January 21, 2022

简介

> 注意：
>
> 在本地环境中，VDA 注册到 Delivery Controller。在 Citrix Cloud 服务环境中，VDA 注册到 Cloud Connector。在混合环境中，某些 VDA 注册到 Delivery Controller，而其他 VDA 注册到 Cloud Connector。

VDA 必须先向站点中的一个或多个 Controller 或 Cloud Connector 注册（建立连接），然后该 VDA 才可以使用。VDA 通过检查名为 `ListofDDCs` 的列表来查找控制器或连接器。VDA 上的 `ListOfDDCs` 包含将该 VDA 指向站点中的 Controller 或 Cloud Connector 的 DNS 条目。为实现负载平衡，VDA 会自动在列表中的所有 Controller 或 Cloud Connector 之间分发连接。

为什么 VDA 注册如此重要?

- 从安全角度而言，注册是一种敏感操作。您将在 Controller 或 Cloud Connector 与 VDA 之间建立连接。对于此类敏感操作，如果所有情况未达到良好状态，预期行为是拒绝连接。您将有效地建立两个单独的通信通道：VDA 至 Controller 或 Cloud Connector 和 Controller 或 Cloud Connector 至 VDA。连接使用 Kerberos，因此不允许存在时间同步和域成员身份问题。Kerberos 使用服务主体名称 (SPN)，因此您不能使用负载平衡的 IP\主机名。
- 添加和删除 Controller 或 Cloud Connector 后，如果 VDA 没有准确的 Controller（或 Cloud Connector）最新信息，VDA 可能会拒绝未列出的 Controller 或 Cloud Connector 代理的会话启动。无效的项会使虚拟桌面系统软件的启动发生延迟。VDA 不会接受来自未知的不可信 Controller 或 Cloud Connector 的连接。

除了 `ListofDDCs` 之外，`ListOfSIDs`（安全 ID）也可以指示 `ListofDDCs` 中的哪些计算机可信。`ListofSIDs` 可用于降低 Active Directory 上的负载或避免来自受感染 DNS 服务器的潜在安全威胁。有关详细信息，请参阅 ListOfSIDs。

如果 `ListofDDCs` 指定多个 Controller 或 Cloud Connector，VDA 将尝试以随机顺序连接这些 Controller 或 Cloud Connector。在本地部署中，`ListofDDCs` 还可以包含 Controller 组。VDA 将尝试连接组中的每个 Controller，然后转向 `ListofDDCs` 中的其他项。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Virtual Apps and Desktops 会在 VDA 安装期间自动测试与配置的 Controller 或 Cloud Connector 的连接。如果无法访问 Controller 或 Cloud Connector，会显示错误。如果您忽略无法访问 Controller 或 Cloud Connector 的警告（或者在 VDA 安装期间您不指定 Controller 或 Cloud Connector 地址时），系统会显示消息提醒您。

Controller 或 **Cloud Connector** 地址配置方法

管理员将选择 VDA 首次注册（初始注册）时使用的配置方法。在首次注册期间，会在 VDA 上创建永久性缓存。在后续注册期间，除非检测到配置更改，否则 VDA 将从此本地缓存中检索 Controller 或 Cloud Connector 列表。

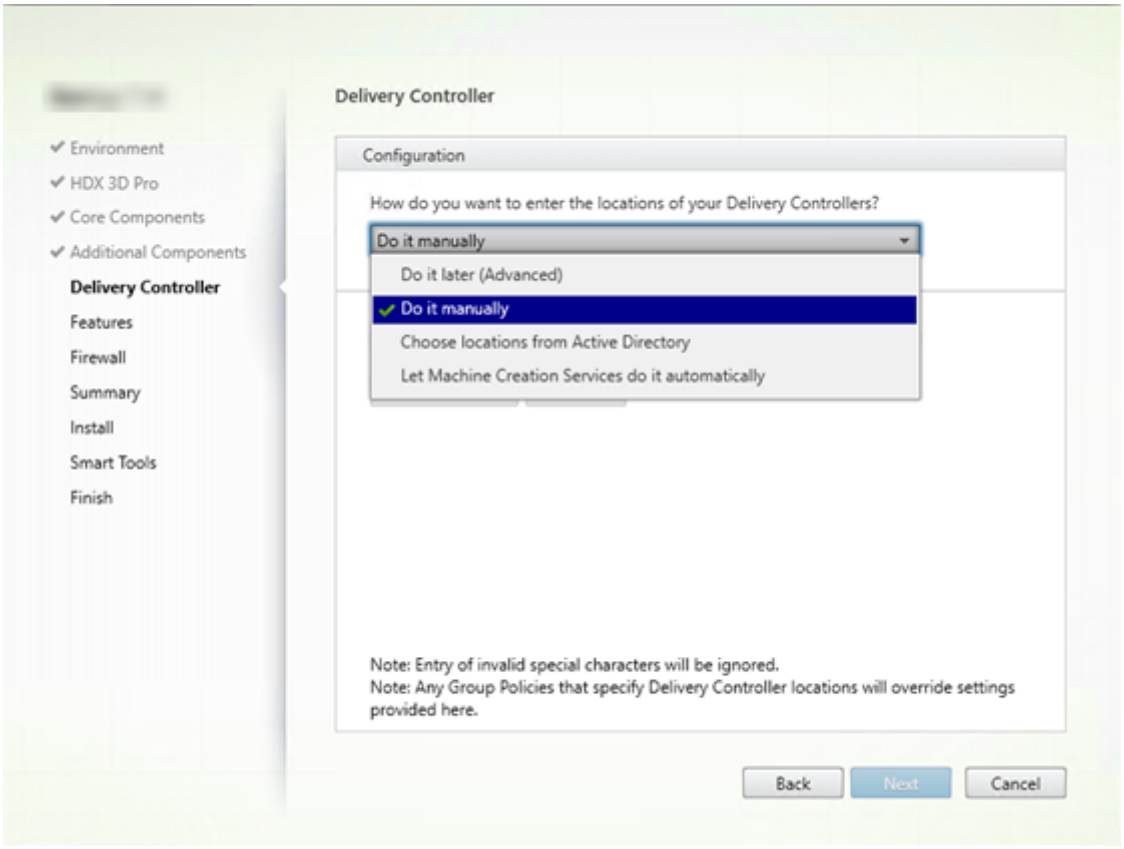
在后续注册期间检索该列表的最简单的方法是使用自动更新功能。默认情况下启用自动更新。有关详细信息，请参阅自动更新。

在 VDA 上配置 Controller 或 Cloud Connector 地址的方法有多种。

- 基于策略（LGPO 或 GPO）
- 基于注册表（手动、组策略首选项 (GPP)、在 VDA 安装期间指定）
- 基于 Active Directory OU（旧 OU 发现）
- 基于 MCS (personality.ini)

首次注册方法在安装 VDA 时指定。（如果禁用自动更新，则在 VDA 安装期间选择的方法将用于后续注册。）

下图显示了 VDA 安装向导的 **Delivery Controller** 页面。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

基于策略 **(LGPO\GPO)**

Citrix 建议 VDA 首次注册时使用 GPO。它的优先级最高。（尽管列出的自动更新的优先级最高，但仅在首次注册之后使用自动更新。）基于策略的注册具有使用组策略进行配置的集中优势。

要指定此方法，请完成以下两个步骤：

- 在 VDA 安装向导中的 **Delivery Controller** 页面上，选择以后 **(**高级**)**。该向导会多次提醒您指定 Controller 地址，即使您在 VDA 安装期间不指定它们也是如此。（VDA 注册非常重要!）
- 可以在 “Virtual Delivery Agent Settings > Controllers” 设置中通过 Citrix 策略启用或禁用基于策略的 VDA 注册。（如果安全性是您的首要任务，请使用 Virtual Delivery Agent Settings > Controller SIDs 设置。）

此设置存储在 HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs) 下。

基于注册表

要指定此方法，请完成以下步骤之一：

- 在 VDA 安装向导中的 **Delivery Controller** 页面上，选择手动操作。然后输入所安装 Controller 的 FQDN，并单击添加。如果您已安装更多 Controller，请添加其地址。
- 对于命令行 VDA 安装，请使用 /controllers 选项并指定所安装 Controller 或 Cloud Connector 的 FQDN。

此信息存储在注册表项 HKLM\Software\Citrix\VirtualDesktopAgent 或 HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent 下的注册表值 ListOfDDCs 中。

还可以手动配置此注册表项或使用组策略首选项 (GPP)。此方法可能优于基于策略的方法（例如，如果您要对不同的 Controller 或 Cloud Connector 进行有条件的处理，如：对名称以 XDW-001- 开头的计算机使用 XDC-001）。

更新 ListOfDDCs 注册表项，该注册表项用于列出站点中所有 Controller 或 Cloud Connector 的 FQDN。（此注册表项相当于 Active Directory 站点 OU。）

HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)

如果 HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent 注册表位置包含这两个注册表项 ListOfDDCs 和 FarmGUID，则 ListOfDDCs 用于 Controller 或 Cloud Connector 发现。如果在 VDA 安装过程中指定了站点 OU，则存在 FarmGUID。（这可能用于旧部署中。）

（可选）更新 ListOfSIDs 注册表项（有关详细信息，请参阅 ListOfSIDs）：

HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)

谨记：如果您还通过 Citrix 策略启用基于策略的 VDA 注册，这将会覆盖您在 VDA 安装期间指定的设置，因为该方法的优先级更高。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

基于 **Active Directory OU**（旧）

支持此方法主要是为了向后兼容，建议不要使用此方法。如果您仍在使用此方法，Citrix 建议改为其他方法。

要指定此方法，请完成以下两个步骤：

- 在 VDA 安装向导中的 **Delivery Controller** 页面上，选择从 **Active Directory** 中选择位置。
- 使用 `Set-ADControllerDiscovery.ps1` 脚本（在每个 Controller 上都可用）。此外，在每个 VDA 上配置 `FarmGuid` 注册表项以指向正确的 OU。可以使用组策略配置此设置。

有关详细信息，请参阅基于 Active Directory OU 的发现。

基于 **MCS**

如果您计划只使用 MCS 来预配 VM，可以指示 MCS 设置 Controller 或 Cloud Connector 列表。此功能可进行自动更新。创建目录时，MCS 会在初始预配期间将 Controller 或 Cloud Connector 列表注入到 `Personality.ini` 文件中。自动更新会使该列表保持最新状态。

建议不要将此方法用于大型环境中。在下列情况下，可以使用此方法：

- 小型环境
- 不会在站点之间移动 VDA
- 只使用 MCS 预配 VM
- 您不想使用组策略

要指定此方法，请在 VDA 安装向导中的 **Delivery Controller** 页面上，选择 **Let Machine Creation Services do it**（让 Machine Creation Services 完成）。

审查和建议

最佳做法：

- 首次注册时使用组策略注册方法。
- 使用自动更新（默认情况下启用）使 Controller 列表保持最新。
- 在多区域部署中，首次配置时使用组策略（至少有两个 Controller 或 Cloud Connector）。将 VDA 指向其区域中的本地 Controller 或 Cloud Connector。使用自动更新使其保持最新。自动更新会自动优化卫星区域中 VDA 的 `ListofDDCs`。
- 在某个控制器不可用时，在 `ListOfDDCs` 注册表项中列出多个以空格分隔的控制器可防止出现注册问题。例如：

```
DDC7x.xd.local DDC7xHA.xd.local

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
32-bit: HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\
    ListOfDDCs

HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\
    ListOfDDCs (REG_SZ)
<!--NeedCopy-->
```

- 请确保 ListofDDCs 下列出的所有值都映射到有效的完全限定域名，以防止出现启动注册延迟问题。

自动更新

默认情况下启用自动更新（在 XenApp 和 XenDesktop 7.6 中引入）。这是使 VDA 注册保持最新的最有效方法。尽管不用于首次注册，但在首次注册时，自动更新软件会下载 ListofDDCs 并将其存储在 VDA 上的永久性缓存中。此过程将针对每个 VDA 执行。此缓存中还保存计算机策略信息，这样可以确保在重新启动后保留策略设置。

使用 MCS 或 Citrix Provisioning 预配计算机时支持自动更新，但 Citrix Provisioning 服务器端缓存除外。服务器端缓存不是常见的情况，因为没有用于自动更新缓存的持久存储。

要指定此方法，请执行以下操作：

- 通过包含设置“Virtual Delivery Agent Settings > Enable auto update of Controllers”的 Citrix 策略启用或禁用自动更新。默认情况下，启用此设置。

工作原理：

- 每次 VDA 重新注册时（例如，重新启动计算机后），都会更新缓存。此外，每个 Controller 或 Cloud Connector 每 90 分钟检查一次站点数据库。如果自上次检查后添加或删除了 Controller 或 Cloud Connector，或者如果发生了影响 VDA 注册的策略更改，Controller 或 Cloud Connector 会向其注册的 VDA 发送更新列表，并更新缓存。VDA 接受来自其最新缓存列表中所有 Controller 或 Cloud Connector 的连接。
- 如果 VDA 接收的列表不包括其注册的 Controller 或 Cloud Connector（即，已从站点中删除该 Controller 或 Cloud Connector），VDA 将从 ListofDDCs 中选择 Controller 或 Cloud Connector 并重新注册。

示例：

- 某个部署包含三个 Controller：A、B 和 C。VDA 向 Controller B 注册（该 Controller 在 VDA 安装期间指定）。
- 之后，将 D 和 E 两个 Controller 添加到站点中。在 90 分钟内，VDA 收到更新的列表，然后接受来自 Controller A、B、C、D 和 E 的连接。（在重新启动 VDA 之前，负载不会平均分布到所有 Controller。）
- 再之后，Controller B 移至另一个站点。在 90 分钟内，原始站点中的 VDA 收到更新的列表，因为自上次检查后 Controller 已发生更改。最初已向 Controller B 注册的 VDA（该 Controller 已不在列表中）将从当前列表（A、C、D 和 E）中选择 Controller 并重新注册。

在一个多区域部署中，卫星区域中的自动更新会先自动缓存所有本地 Controller。主要区域中的所有 Controller 都缓存在备份组中。如果卫星区域中无本地 Controller 可用，将尝试向主要区域中的 Controller 注册。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

如下例所示，缓存文件包含主机名和安全 ID 列表 (ListofSIDs)。VDA 不会查询 SID，这会降低 Active Directory 负载。

```
<?xml version="1.0"?>
<ListOfDDcsListIfSids xmlns="http://schemas.datacontract.org/2004/07/Citrix.Cds.BrokerAgent" xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
  - <_x003C_GroupsOfDDCs_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
      - <d2p1:ArrayOfstring>
          <d2p1:string>CTX-XDC-002.zugec.lan</d2p1:string>
          <d2p1:string>CTX-XDC-001.zugec.lan</d2p1:string>
        </d2p1:ArrayOfstring>
    </_x003C_GroupsOfDDCs_x003E_k__BackingField>
  - <_x003C_ListOfDDCs_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
      <d2p1:string>CTX-XDC-002.zugec.lan</d2p1:string>
      <d2p1:string>CTX-XDC-001.zugec.lan</d2p1:string>
    </_x003C_ListOfDDCs_x003E_k__BackingField>
  - <_x003C_ListOfSids_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
      <d2p1:string>S-1-5-21-726903571-3621260514-849154371-1119</d2p1:string>
      <d2p1:string>S-1-5-21-726903571-3621260514-849154371-1126</d2p1:string>
    </_x003C_ListOfSids_x003E_k__BackingField>
    <_x003C_NonAutoListOfDDCsMethod_x003E_k__BackingField>RegistryBasedFarm</_x003C_NonAutoListOfDDCsMethod_x003E_k__BackingField>
    <_x003C_NonAutoListOfDDCsOrOu_x003E_k__BackingField>CTX-XDC-002.zugec.lan</_x003C_NonAutoListOfDDCsOrOu_x003E_k__BackingField>
</ListOfDDcsListIfSids>
```

可以使用 WMI 调用来检索缓存文件。但是，它存储在只有 SYSTEM 帐户可读的位置中。

> 重要：
>
> 提供此信息只是供参考。请勿修改此文件。如果修改此文件或文件夹，会导致配置不受支持。

```
Get-WmiObject -Namespace "Root\Citrix\DesktopInformation" -Class "Citrix_VirtualDesktopInfo" -Property "PersistentDataLocation"
```

如果出于安全原因（不同于降低 Active Directory 负载）需要手动配置 ListofSIDs，不能使用自动更新功能。有关详细信息，请参阅 ListOfSIDs。

自动更新优先级例外情况

尽管通常情况下，在所有 VDA 注册方法中自动更新的优先级最高，它会覆盖其他方法的设置，仍有一个例外情况。缓存中的 NonAutoListOfDDCs 元素指定 VDA 首次配置方法。自动更新会监视此信息。如果首次注册方法更改，则注册过程会跳过自动更新，并使用配置的优先级次高的方法。将 VDA 移至另一个站点时（例如，在灾难恢复期间），此过程很有用。

配置注意事项

查看常见的 VDA 注册配置。

这是一个嵌入式视频。单击链接观看视频

查看 VDA 注册步骤。

这是一个嵌入式视频。单击链接观看视频

配置可能会影响 VDA 注册的项目时，请考虑以下事项。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Controller 或 **Cloud Connector** 地址

无论使用哪种方法指定 Controller 或 Cloud Connector，Citrix 都建议使用 FQDN 地址。IP 地址并不视为可信配置，因为与 DNS 记录相比，IP 更容易受影响。如果手动填充 `ListofSIDs`，可以在 `ListofDDCs` 中使用 IP。但是，仍建议使用 FQDN。

负载平衡

如前所述，VDA 会自动在 `ListofDDCs` 中的所有 Controller 或 Cloud Connector 之间分发连接。Citrix 代理协议 (CBP) 中内置了故障转移和负载平衡功能。如果在配置中指定多个 Controller 或 Cloud Connector，需要时，注册会自动在这些 Controller 或 Cloud Connector 之间进行故障转移。由于自动更新功能，会自动为所有 VDA 进行故障转移。

出于安全原因，不能使用网络负载平衡器（例如 Citrix ADC）。VDA 注册使用 Kerberos 双向身份验证，在这种验证中，客户端 (VDA) 必须向服务 (Controller) 证明其身份。但是，Controller 或 Cloud Connector 必须向 VDA 证明其身份。这意味着 VDA 和 Controller 或 Cloud Connector 同时用作服务器和客户端。如本文开头所述，有两种通信通道：VDA 到 Controller/Cloud Connector 和 Controller/Cloud Connector 到 VDA。

此过程中的组件称为服务主体名称 (SPN)，它作为属性存储在 Active Directory 计算机对象中。VDA 连接到 Controller 或 Cloud Connector 时，它必须指定要与谁通信。此地址为 SPN。如果使用负载平衡的 IP，则 Kerberos 双向身份验证会正确识别该 IP 不属于预期的 Controller 或 Cloud Connector。

有关详细信息，请参阅：

- Kerberos 简介
- 使用 Kerberos 的双向身份验证

自动更新替代 **CNAME**

自动更新功能替代了 XenApp 和 XenDesktop 7.x 之前版本中的 CNAME（DNS 别名）功能。从 XenApp 和 XenDesktop 7 开始，禁用 CNAME 功能。使用自动更新替代 CNAME。（如果必须使用 CNAME，请参阅 CTX137960。为了持续使用 DNS 别名，请勿同时使用自动更新和 CNAME。）

Controller/Cloud Connector 组

在有些情况下，您可能希望按组处理 Controller 或 Cloud Connector，一个组作为首选组，其他组用于在该组中所有 Controller/Cloud Connector 发生故障时进行故障转移。请注意，Controller 或 Cloud Connector 是随机从列表中选择的，因此，分组可以有助于实施优先使用。

这些组用于在单个站点（而非多个站点）中使用。

使用括号指定 Controller/Cloud Connector 组。例如，有四个 Controller（两个主要，两个备份），分组方式可以如下：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

(XDC-001.cdz.lan XDC-002.cdz.lan)(XDC-003.cdz.lan XDC-004.cdz.lan)

在此示例中，先处理第一个组（001 和 002）中的 Controller。如果都出现故障，则处理第二个组中的 Controller (003 和 004)。

对于 XenDesktop 7.0 或更高版本，需要执行一个额外的步骤才能使用注册组功能。需要从 Citrix Studio 中禁用启用控制器自动更新策略。

ListOfSIDs

VDA 可以访问以进行注册的 Controller 列表是 ListofDDCs。VDA 还必须知道信任哪些 Controller；VDA 不会自动信任 ListofDDCs 中的 Controller。ListofSIDs（安全 ID）用于标识可信 Controller。VDA 仅向可信 Controller 尝试注册。

在大多数环境中，会自动基于 ListofDDCs 生成 ListofSIDs。可以使用 CDF 跟踪来读取 ListofSIDs。

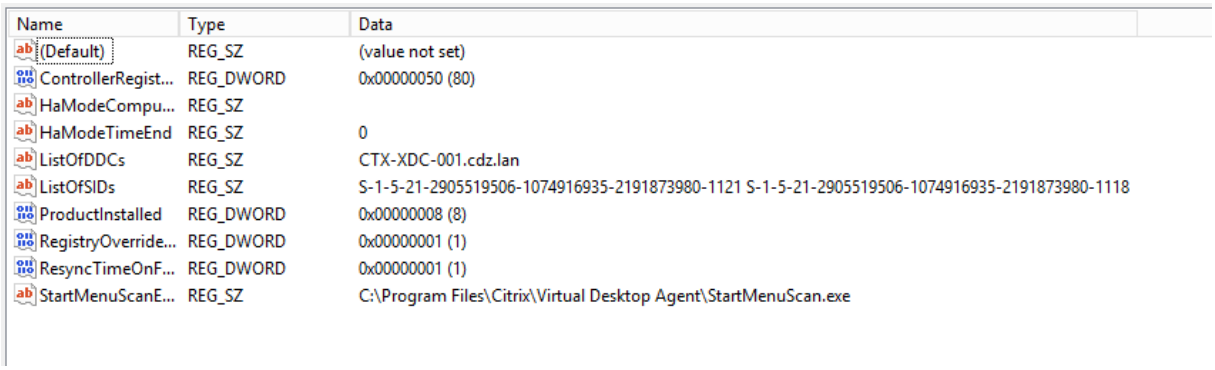
通常，无需手动修改 ListofSIDs。存在几种例外情况。由于有了较新的技术，前两种例外情况已不存在。

- **Controller** 使用单独的角色：在 XenApp 和 XenDesktop 7.7 中引入区域之前，仅当一部分 Controller 用于注册时手动配置 ListofSIDs。例如，如果使用 XDC-001 和 XDC-002 作为 XML Broker，使用 XDC-003 和 XDC-004 进行 VDA 注册，则在 ListofSIDs 中指定所有 Controller，在 ListofDDCs 中指定 XDC-003 和 XDC-004。这不是典型配置或建议的配置。请勿在较新的环境中使用。而是改用区域。
- 降低 **Active Directory** 负载：在 XenApp 和 XenDesktop 7.6 中引入自动更新功能之前，使用 ListofSIDs 来降低域控制器上的负载。通过预填充 ListofSIDs，可以跳过从 DNS 名称到 SID 的解析。但是，有了自动更新功能后，不再需要执行此操作，因为此永久性缓存中包含 SID。Citrix 建议使自动更新功能保持启用状态。
- 安全性：在一些受到高度保护的环境中，手动配置了可信 Controller 的 SID 以避免来自受感染 DNS 服务器的潜在安全威胁。但是，如果禁用了该策略，则必须禁用自动更新功能。否则，将使用永久性缓存中的配置。

因此，除非有特殊原因，否则请勿修改 ListofSIDs。

如果必须修改 ListofSIDs，请在 HKLM\Software\Citrix\VirtualDesktopAgent 下创建一个名为 ListOfSIDs （REG_SZ）的注册表项。值为可信 SID 列表，如果有多个，用空格分隔开。

在以下示例中，一个 Controller 用于 VDA 注册 (ListofDDCs)，两个 Controller 用于代理 (List OfSIDs)。



Name	Type	Data
(Default)	REG_SZ	(value not set)
ControllerRegist...	REG_DWORD	0x00000050 (80)
HaModeCompu...	REG_SZ	
HaModeTimeEnd	REG_SZ	0
ListOfDDCs	REG_SZ	CTX-XDC-001.cdz.lan
ListOfSIDs	REG_SZ	S-1-5-21-2905519506-1074916935-2191873980-1121 S-1-5-21-2905519506-1074916935-2191873980-1118
ProductInstalled	REG_DWORD	0x00000008 (8)
RegistryOverride...	REG_DWORD	0x00000001 (1)
ResyncTimeOnF...	REG_DWORD	0x00000001 (1)
StartMenuScanE...	REG_SZ	C:\Program Files\Citrix\Virtual Desktop Agent\StartMenuScan.exe

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

在 **VDA** 注册期间搜索 **Controller**

当 VDA 尝试注册时，Broker 代理首先在本地域中执行 DNS 查找，以确保可以访问指定的 Controller。

如果初始查找找不到 Controller，Broker 代理可以在 AD 中启动回退自上而下查询。该查询将搜索所有域，并经常重复。如果 Controller 地址无效（例如，管理员在安装 VDA 时输入了不正确的 FQDN），该查询的活动可能会导致域控制器上的分布式拒绝服务 (DDoS) 条件。

下面的注册表项控制在初始搜索期间找不到 Controller 时 Broker 代理是否使用回退自上而下查询。

`HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`

- 名称：`DisableDdcWildcardNameLookup`
- 类型：`DWORD`
- 值：`1`（默认值）或 `0`

如果设置为 `1`，则将禁用回退搜索。如果 Controller 的初始搜索失败，Broker 代理将停止查找。此为默认设置。
如果设置为 `0`，则启用回退搜索。如果 Controller 的初始搜索失败，则启动回退自上而下搜索。

VDA 注册问题故障排除

如前所述，必须向要在启动代理会话时考虑使用的 Delivery Controller 或 Cloud Connector 注册 VDA。未注册的 VDA 会导致无法充分利用原本可用的资源。VDA 无法注册的原因有多种，其中许多都可由管理员进行故障排除。Studio 在目录创建向导中，以及在您创建了交付组之后，提供故障排除信息。

- 在计算机目录创建期间发现问题：在目录创建向导中，添加现有计算机之后，计算机帐户名称列表会指示每台计算机是否都适合添加到该目录。将鼠标悬停在每个计算机旁边的图标上，以显示有关该计算机的有用消息。

  如果该消息确定存在一台有问题的计算机，您可以删除该计算机（使用删除按钮），也可以添加计算机。例如，如果一条消息指示未获取有关某台计算机的信息（可能因为该计算机始终未注册），您可能会选择添加计算机。

  目录的功能级别控制哪些产品功能可用于目录中的计算机。要使用新产品版本中采用的功能，可能需要使用新 VDA。通过设置功能级别，该版本（及更高版本，如果功能级别未更改）中采用的所有功能均可用于目录中的计算机。但是，具有早期 VDA 版本的目录中的计算机将无法注册。

- 在创建了交付组之后发现问题：创建了交付组之后，Studio 会显示与该组关联的计算机的详细信息。

  交付组的详细信息窗格中指示应该注册但未注册的计算机数。即，可能存在一台或多台已开启且不是处于维护模式但当前未向 Controller 注册的计算机。查看“应注册、但未注册的”计算机时，请查看“详细信息”窗格中的故障排除选项卡，了解可能的原因以及建议的更正措施。

有关 **VDA** 注册故障排除的详细信息

- 有关功能级别的详细信息，请参阅 VDA 版本和功能级别。
- 有关 VDA 注册故障排除的详细信息，请参阅 CTX136668。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 还可以使用 Citrix Scout 运行状况检查对 VDA 注册和会话启动进行故障排除。有关详细信息，请参阅关于运行状况检查。

会话

March 14, 2023

维护会话处于活动状态对于提供最佳用户体验至关重要。如果由于网络不稳定、网络延迟变化无常以及无线设备的覆盖范围受限等因素而使连接断开，会令用户感到沮丧。对于许多移动工作人员（例如医护人员）而言，在设备之间快速移动以及在每次登录时访问相同的应用程序是需要优先考虑的事项。

本文所述的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之间快速、轻松漫游的能力。

还可以使用户注销会话、断开会话连接以及配置会话预启动和延迟，请参阅管理交付组。

会话可靠性

会话可靠性使会话在网络连接中断时保持活动状态并显示在用户的屏幕上。用户仍然可以看到他们正在使用的应用程序，直至网络连接恢复。

此功能对于使用无线连接的移动用户尤为有用。例如，使用无线连接的用户进入铁路隧道后将暂时失去连接。通常，会话会断开连接并从用户屏幕上消失，然后该用户必须重新连接到已断开连接的会话。会话可靠性可使会话在计算机上保持活动状态。为指示连接已断开，用户的显示内容将冻结，且光标变成一个旋转的沙漏，直至用户到达隧道的另一端后恢复连接。用户在连接中断期间可继续访问显示内容，在网络连接恢复后可继续与应用程序交互。会话可靠性可重新连接用户而不提示进行重新身份验证。

Citrix Workspace 应用程序用户无法覆盖 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 Citrix 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，但是此功能的主要目的是为用户提供方便。因此，它不会提示用户重新进行身份验证。如果延长会话保持打开状态的时间长度，用户可能会因感到不耐烦而离开用户设备的几率会增加。这些操作可能会使未经授权的用户能够访问会话。
- 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。
- 要防止用户重新连接到中断的会话而不必重新进行身份验证，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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Workspace 应用程序可以检测到 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 Workspace 应用程序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 Workspace 应用程序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设置（其中 `seconds` 为秒数，超过此时间后，不再尝试重新连接会话）。

```
HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds ; DWORD;<seconds>
```

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 Workspace 应用程序自动重新连接。
- 客户端自动重新连接身份验证：允许或禁止自动重新连接后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。每台服务器都将重新连接事件的信息存储在自己的系统日志中。站点并不会提供所有服务器的重新连接事件组合日志。

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。当用户最初登录时，服务器会加密用户凭据并将其存储在内存中。服务器还会创建包含加密密钥的 cookie 并将其发送到 Citrix Workspace 应用程序。Citrix Workspace 应用程序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。

如果您启用了“客户端自动重新连接身份验证”设置，则不使用 cookie。而是在 Citrix Workspace 应用程序尝试自动重新连接时，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 文件对适用于 Windows 的 Citrix Workspace 应用程序禁用客户端自动重新连接。有关详细信息，请参阅您的适用于 Windows 的 Citrix Workspace 应用程序版本的文档。

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”，如上文所述。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 连接指 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）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 Workspace 应用程序进行重新连接。
- 可将连接配置为对中断或超时的连接重置或注销会话。重置会话时，尝试重新连接将启动新会话。而非将用户还原到正在使用的应用程序中的同一位置，应用程序将重新启动。
- 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 Workspace 应用程序或插件提交错误的身份验证信息，自动重新连接会失败。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。启用后，如果服务器未检测到任何活动，此功能将阻止远程桌面服务断开该会话的连接。不活动示例包括不更改时钟、不移动鼠标、不更新屏幕。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。

> 重要：
>
> 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 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：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 登录：默认情况下，工作区控制让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。如果您的漫游用户必须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将用户从 StoreFront 和所有活动会话中注销，也可以仅从 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，而无需与每个桌面和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 Workspace 应用程序用户。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）映射是根据用户登录到会话所使用的客户端设备来应用的。例如，医护人员从急诊室的设备注销，然后登录到 X 射线实验室的工作站。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。分配给应用程序的打印机和其他资源通常也会继续。

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，此会议需要使用打印机。

- 启用了会话漫游时，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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 禁用了会话漫游时，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。或者，还可以指定 LeasingBehavior 属性。

对于桌面会话：

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

对于应用程序会话：

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

其中，`value` 可以是以下值之一：

- **Always**：会话始终漫游，不管所使用的客户端设备以及会话是已连接还是已断开连接。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。相反，将启动一个新会话。
- **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**（仅允许每个用户运行一个应用程序实例）的影响。

- 如果禁用会话漫游，则会禁用“Allow only one instance …”（仅允许每个用户运行…）应用程序限制。
- 如果启用“Allow only one instance …”（仅允许每个用户运行…）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。

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`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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。

此设置仅适用于包含桌面 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

November 17, 2021

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。

   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）可显示搜索属性菜单。可以通过从菜单中的属性构建表达式来执行高级搜索。

可加快搜索速度的提示：

- 要在显示画面中显示作为搜索和排序依据的其他特性，请在任意列上单击鼠标右键，然后选择选择列。
- 要查找已连接到计算机的用户设备，请使用客户端 **(IP)** 和是，然后输入设备的 IP 地址。
- 要查找活动会话，请使用会话状态、是和已连接。
- 要列出交付组中的所有计算机，请在导航窗格中选择交付组，再选择相应组，然后在“操作”窗格中选择查看计算机。

标记

January 21, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

简介

标记是指用于标识计算机、应用程序、桌面、交付组、应用程序组和策略等项目的字符串。创建标记并将其添加到项目后，就可以定制某些操作，以便仅应用于具有指定标记的项目。

- 在 Studio 中定制搜索显示内容。

  例如，要仅显示已针对测试人员优化的应用程序，可创建名为“测试”的标记，然后将其添加（应用）到那些应用程序。现在就可以使用标记“测试”过滤 Studio 搜索。

- 从交付组中的应用程序组或特定桌面发布应用程序，仅考虑所选交付组中的一部分计算机。这称为标记限制。

  通过使用标记限制，可以使用现有计算机来完成多个发布任务，从而节省与部署和管理更多计算机有关的成本。标记限制可以视为对交付组中的计算机进行划分（或分区）。其功能类似于 XenApp 7.x 之前版本中的工作组，但不完全一样。

  对交付组中的一部分计算机进行隔离和故障排除时，将应用程序组或桌面与标记限制结合使用很有用。

- 为交付组中的一部分计算机安排定期重新启动。

  通过对计算机使用标记限制，您可以使用新的 PowerShell cmdlet 为交付组中的一部分计算机配置多个重新启动计划。有关示例和详细信息，请参阅管理交付组。

- 对交付组中的一部分计算机、交付组类型或具有（或没有）指定标记的 OU 定制 Citrix 策略的应用（分配）。

  例如，如果您只想将 Citrix 策略应用于功能更强大的工作站，可为那些计算机添加名为“功能强大”的标记。然后，在“创建策略”向导中的分配策略页面上，选择该标记和启用复选框。您也可以为交付组添加标记，然后将 Citrix 策略应用于该组。有关详细信息，请参阅创建策略。

可以将标记应用于：

- 计算机
- 应用程序
- 计算机目录（仅限 PowerShell；请参阅计算机目录上的标记）
- 交付组
- 应用程序组

可以在 Studio 中创建或编辑以下项时配置标记限制：

- 共享交付组中的桌面
- 应用程序组

用于桌面或应用程序组的标记限制

标记限制涉及多个步骤：

- 创建标记，然后将其添加（应用）到计算机。

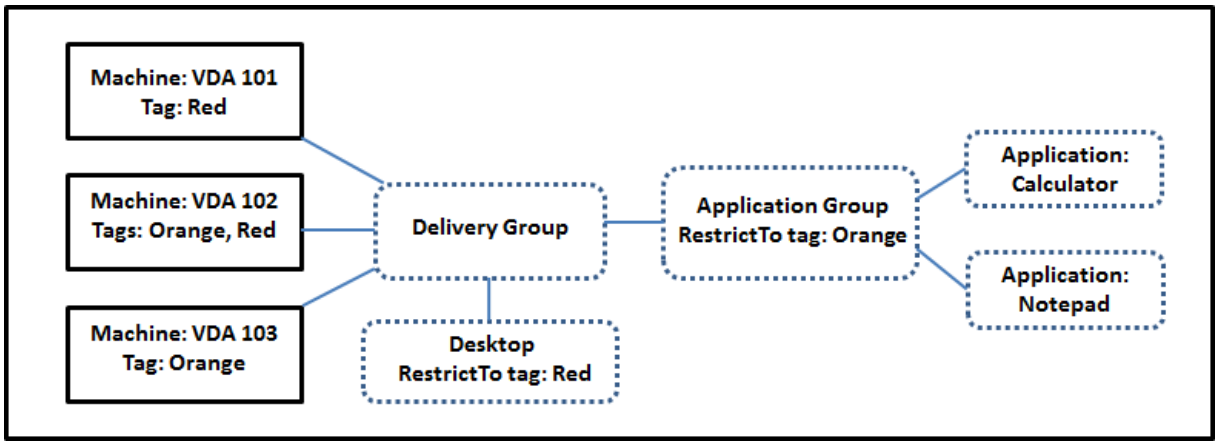
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 使用标记限制创建或编辑组（即，“限制启动带标记 x 的计算机”）。

标记限制延长了 Broker 计算机选择过程。Broker 从受限于访问策略、配置的用户列表、区域首选项、启动就绪情况以及标记限制（如果存在）的关联交付组中选择计算机。对于应用程序，Broker 按优先级顺序回退到其他交付组，对考虑的每个交付组应用相同的计算机选择规则。

示例 **1**：简单布局

此示例介绍一个简单布局，它使用标记限制来限制哪些计算机被考虑用于启动特定的桌面和应用程序。该站点有一个共享交付组、一个发布的桌面以及一个配置了两个应用程序的应用程序组。



- 已为所有三台计算机 (VDA 101-103) 添加了标记。
- 共享交付组中的桌面是使用名为“Red”的标记限制创建的。只能在该交付组中具有标记“Red”的计算机（VDA 101 和 102）上启动桌面。
- 应用程序组创建时使用了“Orange”标记限制，因此它的所有应用程序（Calculator 和 Notepad）只能在该交付组中具有标记“Orange”的计算机（VDA 102 和 103）上启动。

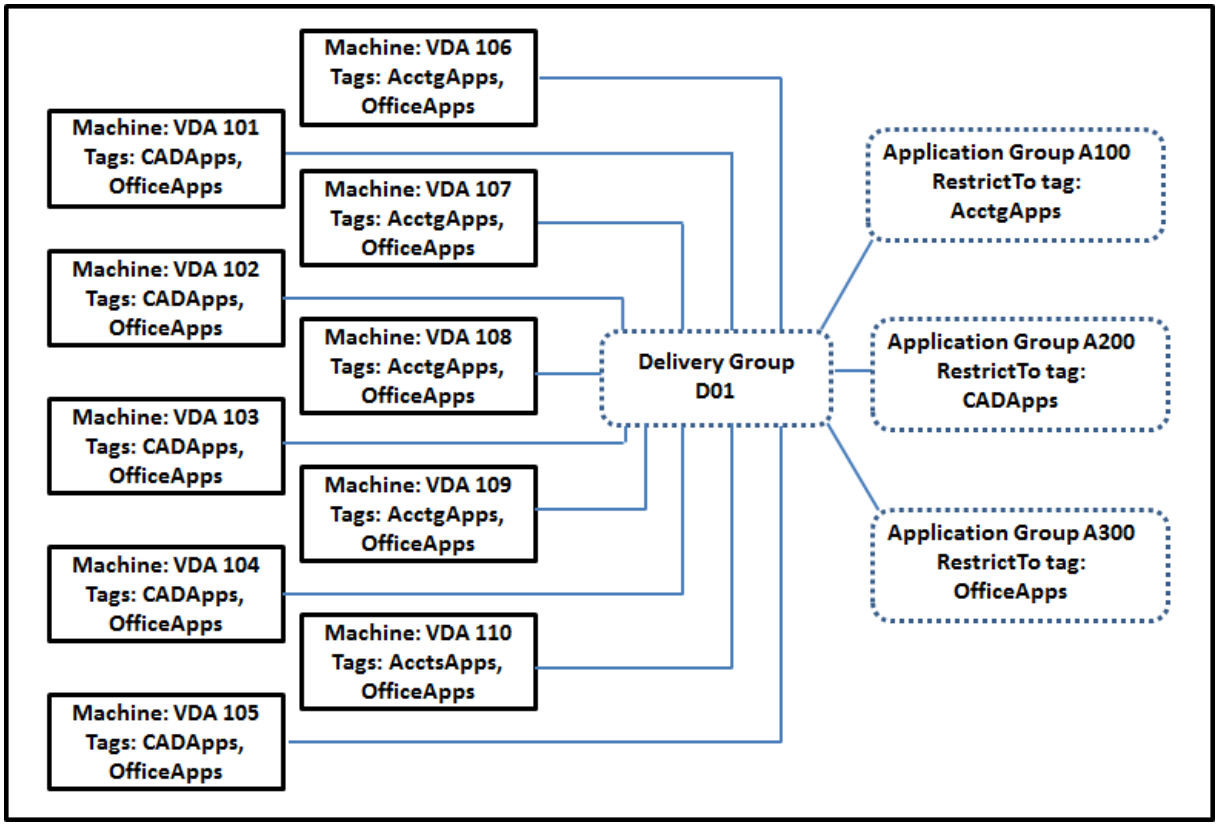
计算机 VDA 102 有两个标记（Red 和 Orange），因此该计算机可以被考虑用于启动应用程序和桌面。

示例 **2**：较复杂的布局

此示例包含创建时使用了标记限制的多个应用程序组。这样，相比仅使用交付组时，可以使用更少的计算机来交付更多应用程序。

如何配置示例 2 介绍了用于创建和应用标记以及之后配置此示例中的标记限制的步骤。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



此示例使用 10 台计算机 (VDA 101-110)、一个交付组 (D01) 和三个应用程序组（A100、A200 和 A300）。通过将标记应用于每台计算机，然后在创建每个应用程序组时指定标记限制：

- 组中的核算用户可以访问五台计算机 (VDA 101–105) 上他们所需的应用程序。
- 组中的 CAD 设计师可以访问五台计算机 (VDA 106-110) 上他们所需的应用程序。
- 组中需要 Office 应用程序的用户可以访问 10 台计算机 (VDA 101-110) 上的 Office 应用程序。

只使用 10 台计算机，并且只有一个交付组。单独使用交付组（不使用应用程序组）需要的计算机数可能是使用应用程序组时的两倍，因为一台计算机只能属于一个交付组。

管理标记和标记限制

标记是通过 Studio 中的管理标记操作来创建、添加（应用）、编辑以及从选定项目删除。

（例外情况：用于策略分配的标记是通过 Studio 中的管理标记操作来创建、编辑以及删除的。但是，标记是在创建策略时应用（分配）的。请参阅创建策略了解详细信息。）

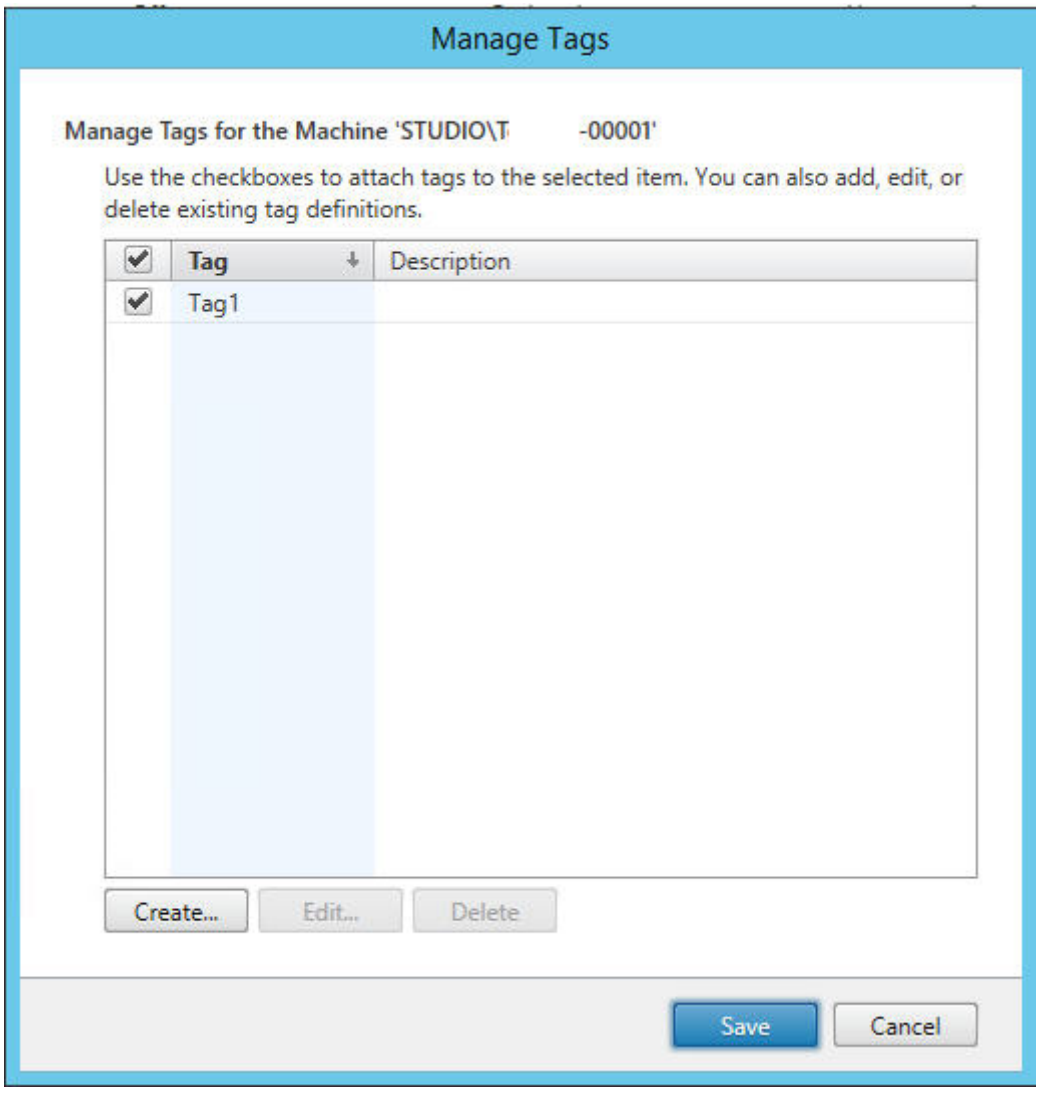
标记限制是当您在交付组中创建或编辑桌面时以及当您创建和编辑应用程序组时配置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用 **Studio** 中的“管理标记”对话框

在 Studio 中，选择要应用标记的项目（一台或多台计算机、应用程序、桌面、交付组或应用程序组），然后在“操作”窗格中选择管理标记。此对话框将列出在站点中创建的所有标记，而不仅限于为所选项目创建的标记。

- 包含复选标记的复选框表示标记已经添加到选定项目。（在下方屏幕截图中，选定计算机应用了名为“Tag1”的标记。）
- 如果您选择了多个项目，则包含连字符的复选框表示部分（而非所有）选定项目添加了标记。



可以从管理标记对话框中执行以下操作。请务必查看使用标记时的注意事项。

- 要创建标记，请执行以下操作：

  单击创建。输入名称和说明。标记名称必须是唯一的，并且不区分大小写。然后单击确定。（创建标记不会自动将其应用于您选择的任何项目。请使用复选框应用标记。）

- 要添加（应用）一个或多个标记，请执行以下操作：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

启用标记名称旁边的复选框。如果您选择了多个项目，且标记旁边的复选框包含一个连字符（表示部分（而非所有）选定项目已经应用了标记），将其更改为复选标记将影响所有选定的计算机。

如果您尝试将标记添加到一台或多台计算机，并且该标记正在用作一个应用程序组中的限制，系统会警告您该操作会导致那些计算机可以用于启动。如果这是您希望得到的结果，请继续。

- 要删除一个或多个标记，请执行以下操作：

  清除标记名称旁边的复选框。如果您选择了多个项目，且标记旁边的复选框包含一个连字符（表示部分（而非所有）选定项目已经应用了标记），清除复选框将从所有选定的计算机中删除标记。

  如果您尝试从正在将某个标记用作限制的计算机删除该标记，系统会警告您该操作会影响将被考虑用于启动的那些计算机。如果这是您希望得到的结果，请继续。

- 要编辑标记，请执行以下操作：

  选择一个标记，然后单击编辑。输入新名称、说明或两者。一次只能编辑一个标记。

- 要删除一个或多个标记，请执行以下操作：

  选择标记，然后单击删除。删除标记对话框将显示当前使用所选标记的项目数（例如，“2 台计算机”）。单击项目可显示详细信息。例如，单击“2 台计算机”项目将显示应用了标记的两台计算机的名称。确认是否要删除标记。

  不能使用 Studio 删除用作限制的标记。首先，编辑应用程序组并删除标记限制或选择一个不同的标记。

在“管理标记”对话框中完成时，单击保存。

要查看某台计算机是否应用了任何标记，请在导航窗格中选择交付组。在中间窗格中选择一个交付组，然后在“操作”窗格中选择查看计算机。在中间窗格中选择一台计算机，然后在详细信息窗格中选择标记选项卡。

管理标记限制

配置标记限制是一个多步骤过程：首先创建标记，并将其添加/应用到计算机。然后，将限制添加到应用程序组或桌面。

- 要创建和应用标记，请执行以下操作：

  使用上文所述的管理标记操作来创建标记，然后将其添加（应用）到将受标记限制影响的计算机。

- 要将标记限制添加到应用程序组，请执行以下操作：

  创建或编辑应用程序组。在交付组页面上，选择限制启动带标记的计算机，然后从列表中选择标记。

- 要更改或删除应用程序组上的标记限制，请执行以下操作：

  编辑组。在交付组页面上，从列表中选择一个不同的标记，或通过清除限制启动带标记的计算机彻底删除标记限制。

- 要将标记限制添加到桌面，请执行以下操作：

  创建或编辑交付组。在桌面页面上，单击添加或编辑。在“添加桌面”对话框中，选择限制启动带标记的计算机，然后从菜单中选择标记。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 要更改或删除交付组上的标记限制，请执行以下操作：

  编辑组。在“桌面”页面上，单击编辑。在对话框中，从列表中选择一个不同的标记，或通过清除限制启动带标记的计算机彻底删除标记限制。

使用标记时的注意事项

应用于项目的标记可以用于不同的目的，因此请注意，添加和删除标记可能会有意外的影响。可以使用标记对 Studio 搜索字段中的计算机显示排序。配置应用程序组或桌面时，可以使用相同的标记作为限制。该标记将考虑启动的对象限制为指定交付组中具有该标记的计算机。

在将某个标记配置为桌面或应用程序组的标记限制之后，当您尝试向计算机中添加该标记时，系统将显示警告。添加该标记可能会使计算机可用于启动其他应用程序或桌面。如果这是您希望得到的结果，请继续。如果不是，您可以取消操作。

例如，假设您创建一个具有“Red”标记限制的应用程序组。然后，您在该应用程序组使用的相同交付组中添加多个其他计算机。如果您之后尝试将“Red”标记添加到那些计算机，Studio 将显示与此类似的消息：“标记“Red”已用作以下应用程序组上的限制。添加此标记可能会使选定的计算机可用于启动此应用程序组中的应用程序。”您随后可以确认或取消向这些附加计算机添加该标记。

同样，如果某个应用程序组使用标记限制启动，Studio 会警告您不能删除该标记，直到您删除作为限制的该标记。（如果您已被允许删除用作应用程序组中的限制的标记，那可能会导致允许应用程序在与该应用程序组关联的交付组中的所有计算机上启动。）如果标记正在用作桌面启动的限制，适用相同的禁止删除标记做法。编辑交付组中的应用程序组或桌面以删除相应标记限制后，可以删除标记。

所有计算机不能有相同的应用程序集合。用户可能属于多个应用程序组，每个组都有不同的标记限制和属于交付组的不同或重叠计算机集合。下表列出了如何决定计算机考虑范围。

应用程序已添加到以下应用程序组时	选定交付组中的这些计算机被考虑用于启动
没有标记限制的一个应用程序组	任何计算机。
具有标记限制 A 的一个应用程序组	应用了标记 A 的计算机。
两个应用程序组，一个具有标记限制 A，另一个具有标记限制 B	同时具有标记 A 和标记 B 的计算机。如果不存在，则是具有标记 A 或标记 B 的计算机。
两个应用程序组，一个具有标记限制 A，另一个没有标记限制	具有标记 A 的计算机。如果不存在，则是任何计算机

如果您在计算机重新启动计划中使用了标记限制，则影响标记应用或限制的任何更改都将影响下一个计算机重新启动周期。但不会影响进行更改时正在进行的任何重新启动周期。

如何配置示例 **2**

以下顺序显示了创建和应用标记以及之后为第二个示例中说明的应用程序组配置标记限制的步骤。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

VDA 和应用程序已经安装在计算机上，且已创建交付组。

创建标记并将其应用于计算机：

1. 在 Studio 中，选择交付组 D01，然后在“操作”窗格中选择查看计算机。
2. 选择计算机 VDA 101-105，然后在“操作”窗格中选择管理标记。
3. 在“管理标记”对话框中，单击创建，然后创建名为 CADApps 的标记。单击确定。
4. 重新单击创建，并创建名为 OfficeApps 的标记。单击确定。
5. 仍在管理标记对话框中时，通过启用每个标记名称（CADApps 和 OfficeApps）旁边的复选框将新创建的标记添加（应用）到选定的计算机。完成后，关闭对话框。
6. 选择交付组 D01，然后在“操作”窗格中选择查看计算机。
7. 选择计算机 VDA 106-110，然后在“操作”窗格中选择管理标记。
8. 在管理标记对话框中，单击创建。创建一个名为 AcctgApps 的标记。单击确定。
9. 通过单击每个标记的名称旁边的复选框将新创建的 AcctgApps 标记和 OfficeApps 标记应用到选定的计算机，然后关闭该对话框。

创建具有标记限制的应用程序组。

1. 在 Studio 的导航窗格中，选择应用程序，然后在“操作”窗格中选择创建应用程序组。“创建应用程序组”向导将启动。
2. 在向导的交付组页面上，选择交付组 D01。选择限制启动带标记的计算机，然后从列表中选择 AcctgApps 标记。
3. 完成向导，同时指定核算用户和核算应用程序。（添加应用程序时，请选择从“开始”菜单来源，这将搜索具有 AcctgApps 标记的计算机上的应用程序。）在摘要页面上，为组命名 A100。
4. 重复上述步骤以创建应用程序组 A200，同时指定具有 CADApps 标记的计算机，以及合适的用户和应用程序。
5. 重复这些步骤以创建应用程序组 A300，同时指定具有 OfficeApps 标记的计算机，以及合适的用户和应用程序。

计算机目录上的标记

您可以在计算机目录上使用标记。创建标记，然后将其应用于目录的整体顺序与之前所述的相同。但是，仅支持通过 PowerShell 界面将标记应用于目录。您不能使用 Studio 将标记应用于目录或从目录中删除标记。在 Studio 中显示的目录不会指明是否应用了标记。

摘要：您可以使用 Studio 或 PowerShell 来创建或删除要用于目录的标记。使用 PowerShell 将标记应用到目录。

以下是将标记与目录结合使用的一些示例：

- 交付组包含多个目录中的计算机，但您希望某个操作（如重新启动计划）仅影响特定目录中的计算机。将标记应用于该目录即可实现该目标。
- 在应用程序组中，您希望将应用程序会话限制为特定目录中的计算机。将标记应用于该目录即可实现该目标。

受影响的 PowerShell cmdlet：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 您可以将目录对象传递给 cmdlet，如 `Add-BrokerTag` 和 `Remove-BrokerTag`。
- `Get-BrokerTagUsage` 显示包含标记的目录数。
- `Get-BrokerCatalog` 具有一个名为 `Tags` 的属性。

例如，以下 cmdlet 会将名为 `fy2018` 的标记添加到名为 `acctg`:
`Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018` 的目录中。（此标记之前是使用 Studio 或 PowerShell 创建的。）

有关更多指导和语法，请参阅 PowerShell cmdlet 帮助。

更多信息

博客文章：How to assign desktops to specific servers（如何向特定服务器分配桌面）。

IPv4/IPv6 支持

November 17, 2021

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。

以下组件仅支持 IPv4。所有其他产品都支持 IPv4 和 IPv6。

- Citrix Provisioning
- Citrix Hypervisor
- 不由仅使用 **IPv6** 控制器注册策略设置控制的 Virtual Delivery Agent (VDA)

IPv6 通信通过与 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。

  此策略设置可控制 VDA 向 Delivery Controller 注册时所用的地址格式：

  启用后，VDA 将注册到 Controller 并使用按以下优先级选择的单个 IPv6 地址与其进行通信：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。此为默认值。

  如果团队经常使用 IPv6 网络，请根据已启用仅使用 **IPv6** 控制器注册策略设置的映像或组织单位 (OU) 为这些用户发布桌面和应用程序。

  如果团队经常使用 IPv4 网络，请根据已禁用仅使用 **IPv6** 控制器注册策略设置的映像或 OU 为这些用户发布桌面和应用程序。

- 定义 **IPv6** 网络掩码的从属设置：控制器注册 IPv6 网络掩码。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 要注册的网络。VDA 将仅在与指定网络掩码匹配的第一个地址上进行注册。

仅当启用了仅使用 **IPv6** 控制器注册策略设置时，此设置才有效。默认值 = 空字符串

部署注意事项

如果您的环境同时包含 IPv4 和 IPv6 网络，请为仅使用 IPv4 的客户端和可以访问 IPv6 网络的客户端创建单独的交付组配置。考虑使用命名、手动分配 Active Directory 组或 SmartAccess 过滤器来区分用户。

如果连接在 IPv6 网络上启动，然后尝试从仅具有 IPv4 访问权限的客户端再次进行连接，则会话重新连接可能会失败。

用户配置文件

January 21, 2022

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 Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps and Desktops 策略，应与他们合作以确保他们可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 Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps and Desktops 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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 调整的策略如下表中所示。此功能将保留任何非默认策略设置，且不会将其覆盖。有关各策略的详细信息，请参阅 Profile Management 文档。创建配置文件的计算机类型会影响调整的策略。主要因素为计算机属于静态计算机还是预先置备的计算机，以及这些计算机是由多个用户共享还是专门仅供一个用户使用。

静态系统具有某些类型的本地存储，这些本地存储中的内容在关闭系统时有望继续存在。静态系统可能会采用 SAN 等存储技术来提供本地磁盘模拟。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。预配技术通常为 Citrix Provisioning 或 Machine Creation Services（或第三方的等效技术）。预配的系统有时具有静态本地存储。这些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 创建的静态本地存储的单会话操作系统计算机、具有通过 VDI-in-a-Box 创建的静态存储的桌面、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 创建的多会话操作系统计算机
- 预配的专用计算机 - 例如，具有静态分配但没有通过 Citrix Provisioning 创建的静态存储的单会话操作系统计算机
- 预配的共享计算机 - 例如，具有通过 Citrix Provisioning 创建的随机分配的单会话操作系统计算机、没有通过 VDI-in-a-Box 创建的静态存储的桌面

以下 Profile Management 策略设置是针对不同的计算机类型建议的指导原则。这些设置在大多数情况下能够正常发挥作用，但根据部署要求，您可能希望使用与之有所差别的设置。

> 重要：
>
> 注销时删除本地缓存的配置文件、**Profile Streaming** 和总是缓存是自动配置功能强制使用的策略。手动调整其他策略。

静态计算机

策略	静态专用计算机	静态共享计算机
Delete locally cached profiles on logoff（注销时删除本地缓存的配置文件）	已禁用	已启用
Profile Streaming	已禁用	已启用
总是缓存	已启用（注意 1）	已禁用（注意 2）
主动回写	已禁用	已禁用（注意 3）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

策略	静态专用计算机	静态共享计算机
处理本地管理员登录	已启用	已禁用（注意 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
Delete locally cached profiles on logoff（注销时删除本地缓存的配置文件）	已禁用（注意 5）	已启用
Profile Streaming	已启用	已启用
总是缓存	已禁用（注意 6）	已禁用
主动回写	已启用	已启用
处理本地管理员登录	已启用	已启用（注意 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. 禁用主动回写，但在 Citrix Virtual Apps 服务器之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。此设置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 Citrix Virtual Apps and Desktops 服务器之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。文件夹重定向将减少配置文件大小并缩短加载时间，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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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。

仅使用 Citrix 策略或 Active Directory 组策略对象配置文件夹重定向，请勿同时使用二者。同时使用这两个策略引擎来配置文件夹重定向可能会导致出现意外行为。

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，即高级文件夹重定向。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。此方法将分隔每个操作系统上的开始菜单文件夹及其内容，从而确保为用户提供一致的体验。

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。如果未正确使用文件夹重定向，则可能会导致不可预知的行为。

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

该部署包含在 Windows 10 桌面和应用程序上运行的应用程序（包括各个版本的 Microsoft Outlook 和 Internet Explorer），包括由 Windows Server 2019 提供的其他版本的 Outlook 和 Internet Explorer。您已为这两个操作系统设置两个交付组。用户希望在这两个版本的两个应用程序中访问同一组联系人和收藏夹。

重要：以下决策和建议适用于所述的操作系统和部署。在您的组织中，您选择重定向的文件夹以及决定是否共享这些文件夹取决于您的特定部署所独有的各种因素。

- 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	是否已在 Windows 10 中执行重定向?	是否已在 Windows Server 2019 中执行重定向?
我的文档	是	是
应用程序数据	否	否

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

文件夹	是否已在 Windows 10 中执行重定向?	是否已在 Windows Server 2019 中执行重定向?
通讯录	是	是
桌面	是	否
下载	否	否
收藏夹	是	是
链接	是	否
我的音乐	是	是
我的图片	是	是
我的视频	是	是
搜索	是	否
保存的游戏	否	否
“开始”菜单	是	否

- 对于共享的重定向文件夹：
  - 在分析由不同版本的 Outlook 和 Internet Explorer 保存的数据结构后，您认为可以安全共享联系人和收藏夹文件夹。
  - 您已知晓，我的文档、我的音乐、我的图片和我的视频文件夹的结构在各个操作系统中都是标准的。因此，可以将这些文件夹安全存储在每个交付组的同一网络位置。
- 对于非共享的重定向文件夹：
  - 您不在 Windows Server 交付组中重定向桌面、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这两个操作系统中是不同的。因此无法共享。
  - 要确保可以预测这些非共享数据的行为，只能在 Windows 10 交付组中重定向这类数据。用户在日常工作中使用 Windows 10 的频率更高。用户仅偶尔访问 Windows Server 提供的应用程序。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 10 计算机而非 Windows Server 计算机，则可能非常有用。
- 对于非重定向的文件夹：
  - 您不希望使存储用户下载文件的服务器变得混乱，因此您选择不重定向“下载”文件夹
  - 来自单独应用程序的数据可能导致兼容性和性能问题，因此您决定不重定向“应用程序数据”文件夹

有关文件夹重定向的信息，请参阅文件夹重定向、脱机文件和漫游用户配置文件概述。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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将配合使用。确保未排除已重定向的文件夹，这样 Profile Management 就可以在您稍后决定不重定向它们时将其移回配置文件的文件夹结构中，并保持数据完整性。有关排除的详细信息，请参阅包含和排除项目。

在系统启动时收集 **Citrix Diagnostic Facility (CDF)** 跟踪信息

November 17, 2021

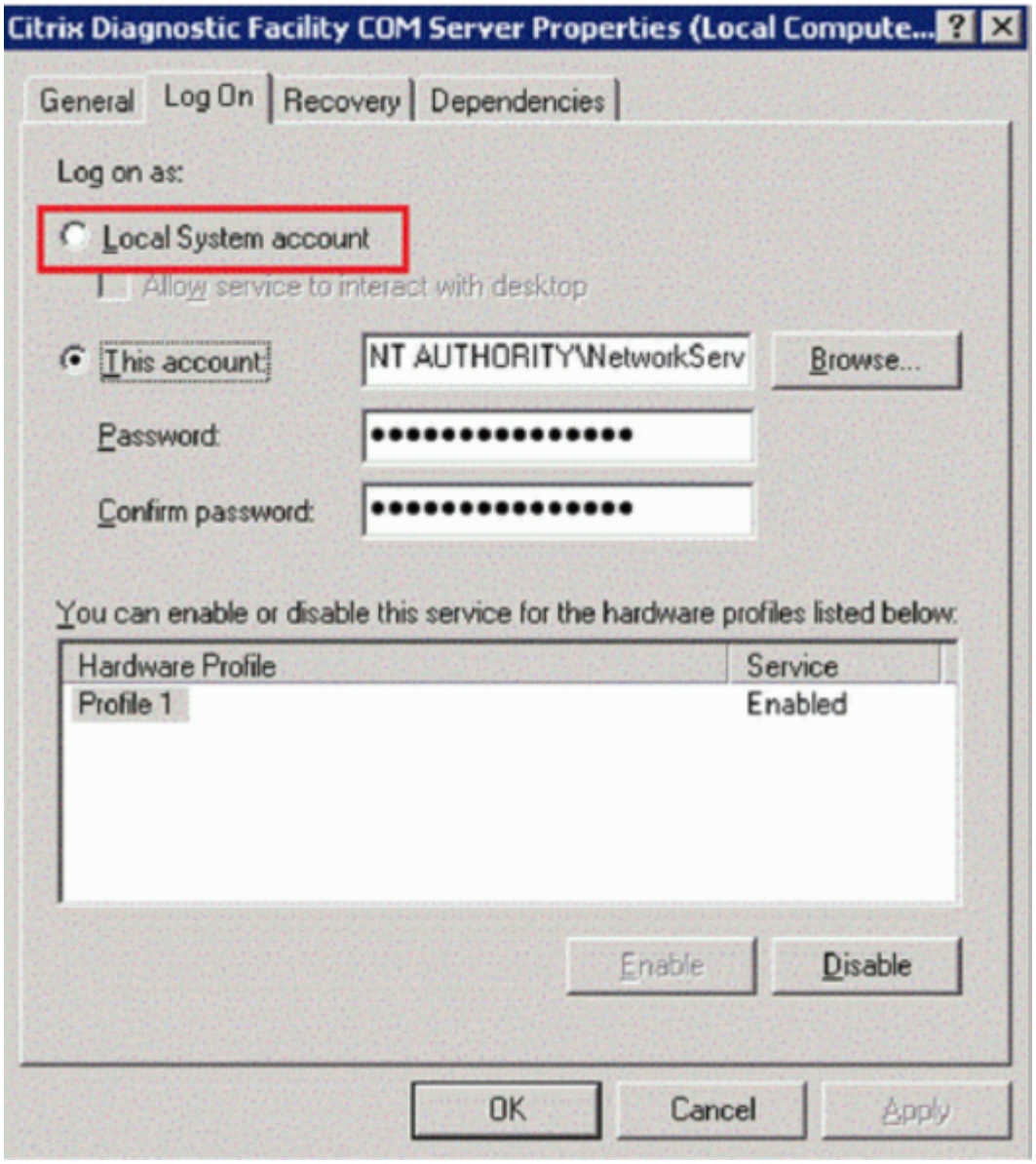
CDFControl 实用程序是一个事件跟踪控制器或使用方，用来捕获各种 Citrix 跟踪提供程序中显示的 Citrix Diagnostic Facility (CDF) 跟踪消息。此实用程序用来对相关的复杂 Citrix 问题进行故障排除、解析过滤器支持以及收集性能数据。要下载 CDFControl 实用程序，请参阅 CTX111961。

使用本地系统帐户

要使用 CDF COM 服务器服务的本地系统帐户，请完成以下步骤：

1. 在开始菜单中单击运行。
2. 在对话框中键入 `services.msc`，然后单击确定
3. 选择 **Citrix Diagnostics Facility COM** 服务器服务，然后选择属性。
4. 单击登录选项卡并启用本地系统帐户。然后单击确定。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



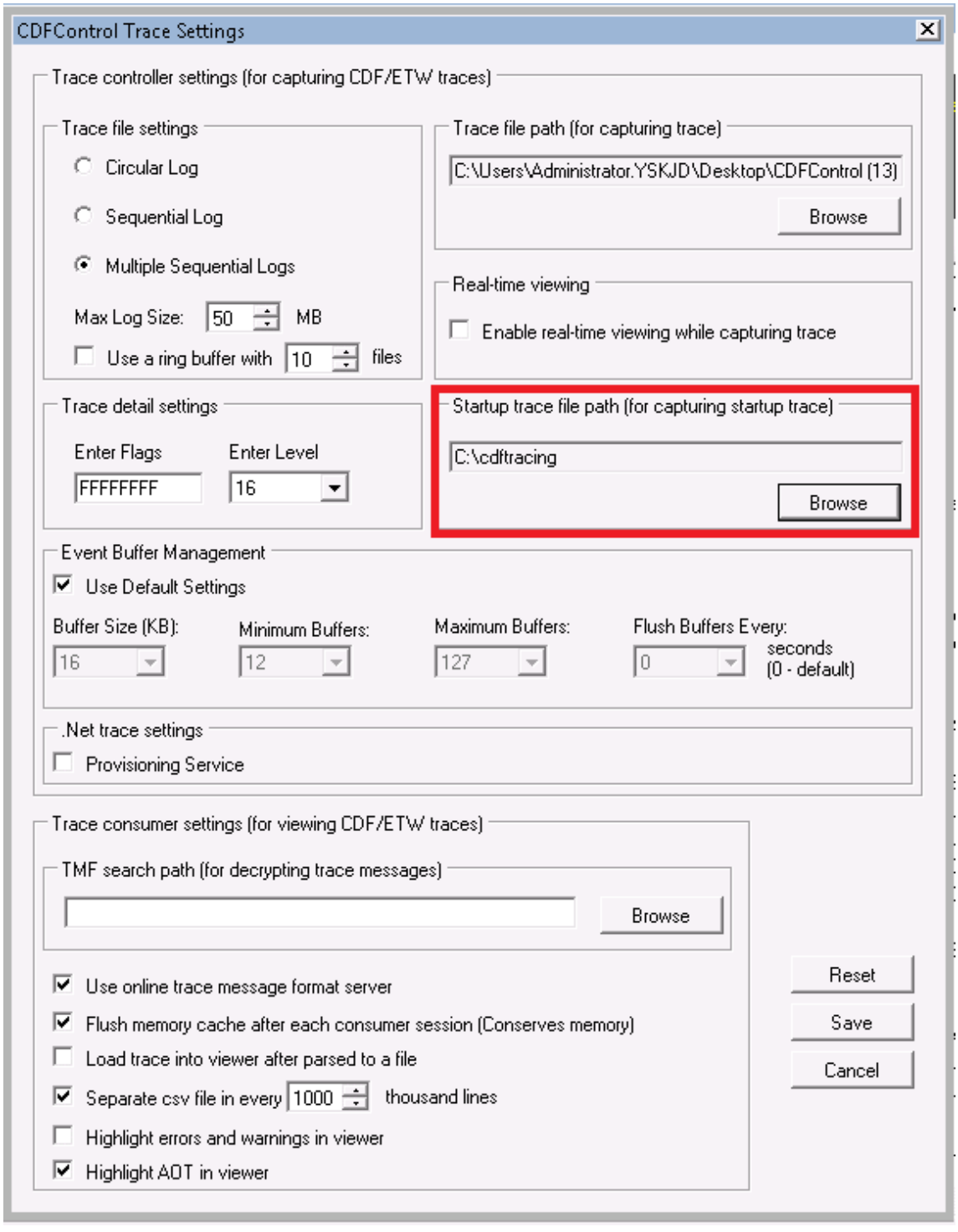
5. 重新启动服务。

在系统启动时收集跟踪信息

使用以下过程在系统启动时收集 CDF 跟踪。您需要管理员权限。

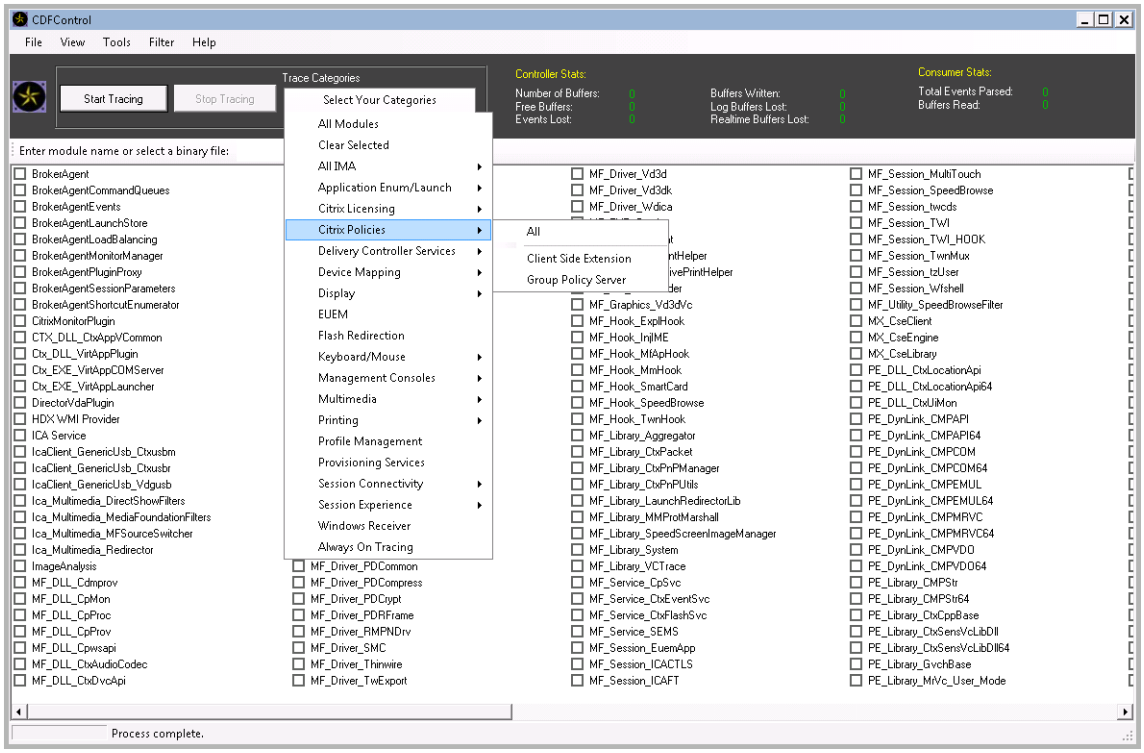
1. 启动 **CDFControl** 并从 **Tools**（工具）菜单中选择 **Options**（选项）。
2. 在 **Startup trace file path for capturing startup trace**（用于捕获启动跟踪信息的启动跟踪文件路径）部分中指定跟踪文件路径。然后单击 **Save**（保存）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. 根据 Citrix 技术支持的建议选择 **Trace Categories**（跟踪类别）。（在以下示例中，选择了 **Citrix** 策略。该选择只是一个示例。我们建议您针对要进行故障排除的特定问题启用提供程序。）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. 选择启动跟踪，然后从工具菜单中选择启用。

   选择 **Enable**（启用）后，动画栏将开始滚动。此活动不会影响该过程。继续执行下一个步骤。

5. 启用 **Startup Tracing**（启动跟踪）后，关闭 **CDFControl utility**（CDFControl 实用程序）并重新启动系统。

6. 启动 **CDFControl** 实用程序。系统重新启动并出现错误后，通过从工具菜单中选择启动跟踪，然后单击禁用来禁用启动跟踪。

7. 停止 **Citrix Diagnostics Facility COM** 服务器服务。

8. 重复步骤 1 和 2，收集跟踪日志文件 (.etl) 以进行分析。

9. 启动 **Citrix Diagnostics Facility COM** 服务器服务。

Citrix Insight Services

July 5, 2024

Citrix Insight Services (CIS) 是用于性能监测、遥测以及生成业务洞察的 Citrix 平台。通过其性能监测和遥测功能，技术用户（客户、合作伙伴和工程师）就可以自行诊断和修复问题并优化其环境。有关 CIS 及其工作原理的最新详细信息，请访问 https://cis.citrix.com（需要 Citrix 帐户凭据）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

上载到 Citrix 的所有信息均用于故障排除和诊断目的，以及提高产品的质量、可靠性和性能，对这些信息的使用将遵循以下策略：

- Citrix Insight Services 策略，网址为 https://cis.citrix.com/legal
- Citrix 隐私政策，网址为 https://www.cloud.com/privacy-policy

此 Citrix Virtual Apps and Desktops 版本支持以下技术。

- Citrix Virtual Apps and Desktops 安装和升级分析
- Citrix 客户体验改善计划 (CEIP)
- Citrix Call Home
- Citrix Scout

除了（以及不同于）CIS 和 Citrix Analytics 之外：在安装（或升级）Studio 时，会自动收集 Google Analytics（并在以后上载）。安装 Studio 后，可以使用注册表项 HKLM\Software\Citrix\DesktopStudio\GAEnabled 更改此设置。值 1 将启用收集和上载，0 将禁用收集和上载。

安装和升级分析

当您使用完整产品安装程序部署或升级 Citrix Virtual Apps and Desktops 组件时，将在安装/升级组件的计算机上收集和存储有关安装过程的匿名信息。这些数据用于帮助 Citrix 改善其客户的安装体验。

该信息以本地方式存储在%ProgramData%\Citrix\CTQs 下面。

在完整产品安装程序的图形界面和命令行接口中，默认启用自动上载该数据。

- 可以在注册表设置中更改该默认值。如果在安装/升级之前更改注册表设置，则将在使用完整产品安装程序时使用该值。
- 如果使用命令行接口进行安装/升级，可以通过在命令中指定选项来覆盖该默认设置。

控制自动上载：

- 控制自动上载安装/升级分析数据的注册表设置（默认值为 1）：
  - 位置：HKLM:\Software\Citrix\MetaInstall
  - 名称：SendExperienceMetrics
  - 值：0 = 禁用，1 = 启用
- 使用 PowerShell 时，以下 cmdlet 禁用自动上载安装/升级分析数据：

```
1  New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
       SendExperienceMetrics -PropertyType DWORD -Value 0
2  <!--NeedCopy-->
```

- 要在 XenDesktopServerSetup.exe 或 XenDesktopVDASetup.exe 命令中禁用自动上载，请包含 /disableexperiencemetrics 选项。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

要在 XenDesktopServerSetup.exe 或 XenDesktopVDASetup.exe 命令中启用自动上载，请包含 /sendexperiencemetrics 选项。

Citrix 客户体验改善计划

当您参与 Citrix 客户体验改善计划 (CEIP) 时，将向 Citrix 发送匿名的统计数据和使用情况信息，帮助 Citrix 提高 Citrix 产品的质量和性能。有关详细信息，请参阅 https://more.citrix.com/XD-CEIP。

创建或升级站点期间注册

（安装了第一个 Delivery Controller 后）在创建站点时，您会自动在 CEIP 中注册。大约会在您创建站点七天后上载第一个数据包。您可以在创建站点后随时停止参与。即在 Studio 导航窗格中选择配置节点（产品支持选项卡），并按指导信息进行操作。

升级 Citrix Virtual Apps and Desktops 部署时：

- 如果从不支持 CEIP 的版本升级，系统将询问您是否要参与此计划。
- 如果从支持 CEIP 的版本升级，且已启用计划参与功能，则将在升级后的站点中启用 CEIP。
- 如果从支持 CEIP 的版本升级，且已禁用计划参与功能，则将在升级后的站点中禁用 CEIP。
- 如果从支持 CEIP 的版本升级，且计划参与情况未知，则系统会询问您是否要参与计划。

所收集的信息是匿名的，因此在上载到 Citrix Insight Services 之后无法查看。

安装 VDA 时注册

默认情况下，安装 Windows VDA 时您会自动在 CEIP 中注册。可以在注册表设置中更改此默认设置。如果在安装 VDA 之前更改注册表设置，则将使用该值。

控制 CEIP 中的自动注册的注册表设置（默认值为 1）：

位置：HKLM: \Software\Citrix\Telemetry\CEIP
名称：已启用
值：0 = 已禁用，1 = 已启用

默认情况下，Enabled 属性隐藏在注册表中。当它保持未指定时，启用自动上载功能。

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

```
1 New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name
     Enabled -PropertyType DWORD -Value 0
2 <!--NeedCopy-->
```

收集的运行时数据点会定期写入文件作为输出文件夹（默认为%programdata%/Citrix/VdaCeip）。

大约在您安装 VDA 七天后第一次上载数据。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

安装其他产品和组件时注册

您也可以在安装相关 Citrix 产品、组件和技术（如 Citrix Provisioning、AppDNA、Citrix 许可证服务器、适用于 Windows 的 Citrix Workspace 应用程序、通用打印服务器和 Session Recording）时参与 CEIP。请参阅这些产品、组件和技术的文档，以了解有关其安装和计划参与过程的默认设置的详细信息。

Citrix Call Home

在安装 Citrix Virtual Apps and Desktops 中的某些组件和功能时，您可以选择是否参与 Citrix Call Home。Call Home 会收集诊断数据，然后定期将包含该数据的遥测包直接上载到 Citrix Insight Services（在默认端口 443 上通过 HTTPS）以进行分析和故障排除。

在 Citrix Virtual Apps and Desktops 中，Call Home 作为一个后台服务以名称 Citrix Telemetry Service 运行。有关详细信息，请参阅 https://more.citrix.com/XD-CALLHOME。

Citrix Scout 中也提供 Call Home 计划功能。有关详细信息，请参阅 Citrix Scout。

收集内容

Citrix 诊断工具 (CDF) 将跟踪可用于执行故障排除的日志信息。Call Home 将收集 CDF 跟踪信息子集，此信息有助于排除常见故障，例如 VDA 注册和应用程序/桌面启动。此技术称为“始终启用跟踪”(AOT)。AOT 日志保存在磁盘的 C:\Users\CitrixTelemetryService\Appdata\Local\CitrixAOT 中。

Call Home 不会收集任何其他 Windows 事件跟踪 (ETW) 信息，也无法在经过配置后执行此类操作。

Call Home 还会收集其他一些信息，如：

- 由 Citrix Virtual Apps and Desktops 在 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix` 下创建的注册表项。
- Citrix 命名空间下的 Windows Management Instrumentation (WMI) 信息。
- 正在运行的进程列表。
- Citrix 进程的存储于%PROGRAM DATA%\Citrix\CDF 中的故障转储。
- 安装和升级信息。这可以包括完整产品 Metainstaller 日志、失败的 MSI 日志、MSI 日志分析器的输出、StoreFront 日志、许可兼容性检查日志以及初步站点升级测试的结果。

在收集跟踪信息时将压缩此信息。Citrix Telemetry Service 最多保留 10 MB 压缩后的近期跟踪信息，最长时间期限为 8 天。

- 通过压缩数据，Call Home 可在 VDA 中占用较少的空间。
- 跟踪信息保留在内存中，以避免在置备的计算机上发生 IOPS。
- 跟踪缓冲区采用循环机制在内存中保留跟踪信息。

Call Home 将收集 Call Home 关键数据点中列出的关键数据点。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

配置和管理摘要

可以在使用完整产品安装向导期间注册 Call Home，也可在以后使用 PowerShell cmdlet 进行此注册。您注册后，默认情况下，会在当地时间每个星期日大约凌晨 3:00 收集诊断信息并上载到 Citrix。上载将从指定的时间开始在两小时的时间间隔内随机进行。这意味着使用默认计划执行的上载操作会在凌晨 3:00 和 5:00 之间发生。

如果您不想根据计划上载诊断信息（或者如果您希望更改计划），可以使用 PowerShell cmdlet 手动收集和上载诊断信息或将其存储在本地。

在注册按计划的 Call Home 上载时，以及手动向 Citrix 上载诊断信息时，必须提供 Citrix 帐户或 Citrix Cloud 凭据。Citrix 会将凭据更换为用于标识客户以及上载数据的上载令牌。凭据不会被保存。

上载时，系统会向与 Citrix 帐户关联的地址发送一封电子邮件。

如果在安装组件时启用了 Call Home，可以稍后将其禁用。

必备条件

- 计算机必须运行 PowerShell 3.0 或更高版本。
- 计算机上必须运行 Citrix Telemetry Service。
- 系统变量 `PSModulePath` 必须设置为 Telemetry 的安装路径，例如 C:\Program Files\Citrix\Telemetry Service\。

在组件安装期间启用 **Call Home**

在安装或升级 **VDA** 期间：在完整产品安装程序中使用图形用户界面安装或升级 Virtual Delivery Agent 时，系统会询问您是否希望参与 Call Home。有两种选择：

- 参与 Call Home。
- 不参与 Call Home。

如果您是升级 VDA 且以前注册了 Call Home，则不会显示该向导页面。

在安装或升级 **Controller** 期间：使用图形用户界面安装或升级 Delivery Controller 时，系统会询问您是否希望参与 Call Home。有三个选项：

安装 Controller 时，如果服务器具有应用了策略设置“作为服务登录”的 Active Directory GPO，您将无法在安装向导中的 Call Home 页面上配置信息。有关详细信息，请参阅 CTX218094。

如果您要升级 Controller 并且以前注册了 Call Home，系统不会要求您参与。

PowerShell cmdlet

PowerShell 可帮助提供全面的语法，包括对并用于这些常见情况的 cmdlet 和参数的说明。

要使用代理服务器进行上载，请参阅配置代理服务器。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 启用按计划上载：诊断收集信息会自动上载到 Citrix。如果没有为自定义计划输入其他 cmdlet，则会使用默认的计划。

```
$cred = Get-Credential
Enable-CitrixCallHome -Credential $cred
<!--NeedCopy-->
```

  要确认已启用按计划上载，请输入 Get-CitrixCallHomeGet-CitrixCallHome。如果已启用，则返回 IsEnabled=True 和 IsMasterImage=False。

- 为从主映像创建的计算机启用按计划上载：通过在主映像中启用按计划上载，无需对计算机目录中创建的每台计算机进行配置。

```
Enable-CitrixCallHome -Credential $cred -MasterImage
```

  要确认已启用按计划上载功能，请输入 **Get-CitrixCallHome**。如果已启用，则返回 IsEnabled=True 和 IsMasterImage=True。

- 创建自定义计划：为诊断收集和上载创建每天或每周计划。

```
$timespan = New-TimeSpan - Hours hours -Minutes minutes
Set-CitrixCallHomeSchedule - TimeOfDay $timespan - DayOfWeek day
    -UploadFrequency {
Daily|Weekly }

<!--NeedCopy-->
```

示例：

以下 cmdlet 会创建一个在每天晚上 10:20 打包并上载数据的计划。Hours 参数采用 24 小时制时间。当 UploadFrequency 参数值为 Daily 时，将忽略 DayOfWeek 参数（如果已指定）。

```
$timespan - New-TimeSpan - Hours 22 - Minutes 20
Set-CitrixCallHomeSchedule - TimeOfDay $timespan -UploadFrequency Daily
<!--NeedCopy-->
```

要确认计划，请输入 Get-CitrixCallHomeSchedule。在上面的示例中，将返回 StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency=Daily。

以下 cmdlet 会创建一个计划，在每个星期三晚上 10:20 上载数据。

```
$timespan - New-TimeSpan - Hours 22 - Minutes 20
Set-CitrixCallHomeSchedule - TimeOfDay $timespan - DayOfWeek Wed -
    UploadFrequency Weekly
<!--NeedCopy-->
```

要确认计划，请输入 Get-CitrixCallHomeSchedule。在上面的示例中，将返回 StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

禁用 **Call Home**

您可以使用 PowerShell cmdlet 或通过 Citrix Scout 禁用 Call Home。

即使禁用了 Call Home 按计划上载，系统也会收集 AOT 日志并将其存储到磁盘中。（禁用按计划上载时，AOT 日志不会自动上载到 Citrix。）您可以禁用 AOT 日志的收集和本地存储。

通过 PowerShell 禁用 Call Home　运行以下 cmdlet 后，诊断数据将不会自动上载到 Citrix。（您仍可使用 Citrix Scout 或遥测 PowerShell cmdlet 上载诊断数据。）

```
Disable-CitrixCallHome
```

要确认 Call Home 是否处于禁用状态，请输入 `Get-CitrixCallHome`。如果已禁用，则返回 `IsEnabled=False` 和 `IsMasterImage=False`。

使用 Citrix Scout 禁用收集计划　要使用 Citrix Scout 禁用诊断信息收集计划，请按照计划收集中的指导操作。在步骤 3 中，单击关以取消选定计算机的计划。

禁用 AOT 日志的收集　运行以下 cmdlet（将 `Enabled` 字段会设置为 **`false`**）后，将不会收集 AOT 日志。

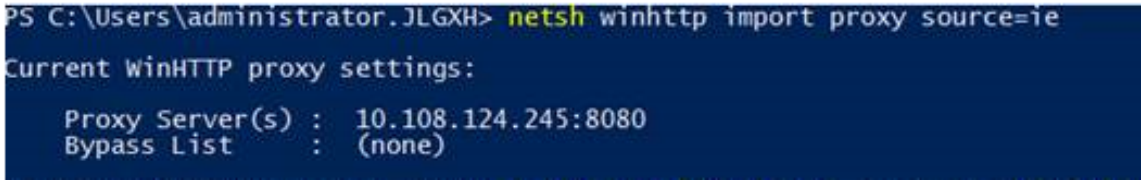
```
Enable-CitrixTrace -Listen '{ "trace" :{ "enabled" :false, "persistDirectory" : "C:\Users\Public" ," maxSizeBytes" :1000000, "sliceDurationSeconds" :300 } } '
```

`Listen` 参数包含 JSON 格式的参数。

配置代理服务器以完成 **Call Home** 上载

在启用了 Call Home 的计算机上完成以下任务。以下过程中的示例图中包含服务器地址和端口 10.158.139.37:3128。您的信息将会不同。

1. 在您的浏览器中添加代理服务器信息。在 Internet Explorer 中，依次选择 **Internet** 选项 **>** 连接 **>** 局域网设置。选择为 **LAN** 使用代理服务器并输入代理服务器地址和端口号。
2. 在 PowerShell 中，运行 `netsh winhttp import proxy source=ie`。



3. 使用文本编辑器，编辑 TelemetryService.exe 配置文件，该文件位于 C:\Program Files\Citrix\Telemetry Service 中。添加红框中显示的信息。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. 重新启动 Telemetry Service。

在 PowerShell 中运行 Call Home cmdlet。

手动收集和上载诊断信息

可以使用 CIS Web 站点向 CIS 上载诊断信息包。也可以使用 PowerShell cmdlet 收集诊断信息并将其上载到 CIS。

要使用 CIS Web 站点上载包，请执行以下操作：

1. 使用 Citrix 帐户凭据登录到 Citrix Insight Services。
2. 选择 **My Workspace**（我的工作区）。
3. 选择运行状况检查，然后导航至您数据所在的位置。

CIS 支持多个用于管理数据上载操作的 PowerShell cmdlet。本文档介绍了用于两种常见情况的 cmdlet：

- 使用 `Start-CitrixCallHomeUpload` cmdlet 手动收集诊断信息包并将其上载到 CIS。（信息包不在本地保存。）
- 使用 `Start-CitrixCallHomeUpload` cmdlet 手动收集数据，并在本地存储诊断信息包。这使您能够预览数据。以后，请使用 `Send-CitrixCallHomeBundle` cmdlet 手动将该包的副本上载到 CIS。（您最初保存的数据仍会在本地保留。）

PowerShell 可帮助提供全面的语法，包括对并用于这些常见情况的 cmdlet 和参数的说明。

当您输入一个 cmdlet 以将数据上载到 CIS 时，系统会提示您确认此上载。如果在上载完成之前 cmdlet 超时，请在系统事件日志中检查上载操作的状态。如果服务已在执行上载操作，则上载请求可能会被拒绝。

收集数据并向 **CIS** 上载包：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath
    string] [-Description string] [-IncidentTime string] [-SRNumber
    string] [-Name string] [-UploadHeader string] [-AppendHeaders string
    ] [-Collect string] [<CommonParameters>]
<!--NeedCopy-->
```

收集数据并将其保存在本地：

```
Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
    Description string] [-IncidentTime string] [-SRNumber string] [-Name
     string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
    strings] [<CommonParameters>]
<!--NeedCopy-->
```

以下参数有效：

- **Credential**：指示上载至 CIS。
- **InputPath**：要包括在包内的 zip 文件的位置。这可能是 Citrix 支持部门要求提供的一个附加文件。请务必包括“.zip”扩展名。
- **OutputPath**：将用于保存诊断信息的位置。在本地保存 Call Home 数据时，此参数是必需的。
- **Description** 和 **Incident Time**：有关上载的自由格式的信息。
- **SRNumber**： Citrix 技术支持事件编号。
- **Name**：用于标识包的名称。
- **UploadHeader**： JSON 格式的字符串，用于指定上载到 CIS 的上载标头。
- **AppendHeaders**： JSON 格式的字符串，用于指定上载到 CIS 的附加标头。
- 收集：JSON 格式的字符串，用于指定要收集或忽略的数据，采用 { ‘collector’ :{ ‘enabled’ :Boolean}} 格式，其中 Boolean 为 true 或 false。
  有效的 collector 值为：
  - ‘wmi’
  - ‘process’
  - ‘registry
  - ‘crashreport’
  - ‘trace’
  - ‘file’
  - ‘msi’
  - ‘localdata’
  - ‘sitedata’
  - ‘sfb’

  默认情况下，会启用除 ‘sfb’ 之外的所有收集器。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

‘sfb’ 收集器经过专门设计，可根据需求用于诊断 Skype for Business 问题。除 ‘enabled’ 参数以外，’sfb’ 收集器支持使用 ‘account’ 和 ‘accounts’ 参数来指定目标用户。使用以下一种形式：

- “-Collect “{ ‘sfb’ :{ ‘account’ :’ domain\\user1’ }}”
- “-Collect “{ ‘sfb’ :{ ‘accounts’ :[‘domain\\\user1’ , ‘domain\\\user2’]}}”

- 常用参数：请参阅 PowerShell 帮助。

上载以前在本地保存的数据：

```
Send-CitrixCallHomeBundle -Credential <PSCredentia\> -Path string [<
CommonParameters>]
```

Path 参数指定以前保存的包的位置。

示例：

以下 cmdlet 会请求将 Call Home 数据上载（不包括从 WMI 收集器获取的数据）到 CIS。此数据（在下午 2:30 记录）与 Citrix Provisioning VDA 的失败注册相关，对应的 Citrix 支持案例编号为 123456。除了 Call Home 数据外，会将文件 “c:\Diagnostics\ExtraData.zip” 包含到上载包中。

```
C:\PS>Start-CitrixCallHomeUpload -InputPath "c:\Diagnostics\ExtraData.
    zip" -Description "Registration failures with Citrix Provisioning
    VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name "
    RegistrationFailure-021812016" -Collect "{
 'wmi':{
 'enabled':false }
  }
 " -UploadHeader "{
 'key1':'value1' }
 " -AppendHeaders "{
 'key2':'value2' }
 "
<!--NeedCopy-->
```

以下 cmdlet 可保存与 Citrix 支持案例编号 223344 相关的 Call Home 数据（在早上 8:15 记录）。该数据将保存在网络共享上的 mydata.zip 文件中。除 Call Home 数据外，还会将文件 “c:\Diagnostics\ExtraData.zip” 包含到保存的包中。

```
C:\PS>Start-CitrixCallHomeUpload -OutputPath \mynetwork\myshare\mydata.
    zip -InputPath "c:\Diagnostics\ExtraData.zip" -Description "
    Diagnostics for incident number 223344" -IncidentTime "8:15" -
    SRNumber 223344
<!--NeedCopy-->
```

以下 cmdlet 可上载以前保存的数据包。

```
$cred=Get-Credential
C:\PS>Send-CitrixCallHomeBundle  -Credential $cred -Path \mynetwork\
    myshare\mydata.zip
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Scout

January 21, 2022

简介

Citrix Scout 会收集诊断信息并运行运行状况检查。可以使用结果来维护您的 Citrix Virtual Apps and Desktops 部署。Citrix 通过 Citrix Insight Services 提供诊断收集信息的综合的自动分析。您还可以使用 Scout 自己或在 Citrix Support 的指导下对问题进行故障排除。

可以将收集文件上载到 Citrix 以供分析以及获取 Citrix 支持提供的指导。也可以将收集信息保存在本地供自己查看，以及以后将收集文件上载到 Citrix 以供分析。

Scout 提供以下程序：

- 收集：在站点中所选计算机上运行一次性诊断信息收集。然后，可以将文件上载到 Citrix 或将其保存在本地。
- 跟踪和重现：在所选计算机上启动手动跟踪。然后，在这些计算机上重新创建问题。重现问题后，将停止跟踪。Scout 随后会收集其他诊断信息并将文件上载到 Citrix，或保存在本地。
- 计划安排：安排在所选计算机上在每天或每周的指定时间执行诊断信息收集。文件将自动上载到 Citrix。
- 运行状况检查：运行检查以衡量站点及其组件的运行状况和可用性。您可以对 Delivery Controller、Virtual Delivery Agent (VDA)、StoreFront 服务器和 Citrix 许可证服务器运行运行状况检查。如果在检查过程中发现问题，Scout 会提供详细报告。每次 Scout 启动时，都会检查更新后的运行状况检查脚本。如果新版本可用，Scout 会自动下载这些脚本，以便下次运行运行状况检查时使用。

> 注意：
>
> 跟踪和重现、计划和运行状况检查过程当前不适用于 Linux VDA。

本文所述图形界面是使用 Scout 的主要方式。也可以使用 PowerShell 配置一次性或计划的诊断信息收集和上载。请参阅 Call Home。

Scout 运行位置：

- 在本地部署中，从 Delivery Controller 运行 Scout 以捕获诊断信息或对一个或多个 Virtual Delivery Agent (VDA)、Delivery Controller、StoreFront 服务器和许可证服务器运行检查。还可以从 VDA 运行 Scout 来收集本地诊断信息。
- 在使用 Citrix Virtual Apps and Desktops 服务的 Citrix Cloud 环境中，从 VDA 运行 Scout 来收集本地诊断信息。

Scout 应用程序的日志存储在 `C:\ProgramData\Citrix\TelemetryService\ScoutUI.log` 中。此文件可用于进行故障排除。

查看 Citrix Scout 的演示。

这是一个嵌入式视频。单击链接观看视频

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

收集内容

Scout 收集的诊断信息包括 Citrix Diagnostic Facility (CDF) 跟踪日志文件。还包括称为 AlwaysOn 跟踪 (AOT) 的一部分 CDF 跟踪。对常见问题（例如，VDA 注册和应用程序/桌面启动）进行故障排除时，AOT 信息很有用。系统不会收集任何其他 Windows 事件跟踪 (ETW) 信息。

收集包括：

- 由 Citrix Virtual Apps and Desktops 在 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix` 下创建的注册表项。
- 位于 **Citrix** 命名空间下的 Windows Management Instrumentation (WMI) 信息。
- 运行的进程。
- Citrix 进程的存储于%PROGRAMDATA%\Citrix\CDF 中的故障转储。
- CSV 格式的 Citrix 策略信息。
- 安装和升级信息。收集可能包括完整的产品 Metainstaller 日志、失败的 MSI 日志、MSI 日志分析器的输出、StoreFront 日志、许可兼容性检查日志以及初步站点升级测试的结果。

关于跟踪信息：

- 跟踪信息会在收集时进行压缩处理，以便在计算机上占用较少空间。
- 在每台计算机上，Citrix Telemetry Service 将保留压缩后的近期跟踪信息，最长保留时间期限为 8 天。
- 从 Citrix Virtual Apps and Desktops 7 1808 开始，AOT 跟踪信息默认保存到本地磁盘。（在早期版本中，跟踪保存在内存中。）默认路径 = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`。
- 从 Citrix Virtual Apps and Desktops 7 1811 开始，保存到网络共享的 AOT 跟踪信息是通过其他诊断程序进行收集的。
- 可以使用 `Enable-CitrixTrace` cmdlet 或 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry DefaultListen` 注册表字符串修改最大大小（默认值为 10 MB）和切片持续时间。
- 在文件达到 `MaxSize` 的 10% 之前，跟踪信息将附加到该文件。

有关 Scout 收集的数据点列表，请参阅 Call Home 关键数据点。

Scout 配置

Scout 可以配置为在 Linux VDA 上运行。有关 Linux VDA 和遥测的详细信息，请参阅与 Citrix Telemetry Service 集成

Linux VDA 可能会自动更改 `ctxtelemetry` 套接字端口或遥测服务的端口。如果是这样，则必须手动配置端口。

1. 导航至 C:\Program Files\Citrix\Telemetry Service
2. 打开 ScoutUI.exe.config 文件。
3. 将 LinuxVDATelemetryServicePort 或 LinuxVDATelemetryWakeupPort 的值更改为在 Linux VDA 上配置的值：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- `<add key="LinuxVDATelemetryServicePort"value="7502"/>`
- `<add key="LinuxVDATelemetryWakeupPort"value="7503"/>`

1. 保存所做的更改并关闭该文件。
2. 再次打开 Scout 以确保其加载最新的配置。

关于运行状况检查

运行状况检查数据存储在 `C:\ProgramData\Citrix\TelemetryService\` 下的文件夹中。

站点运行状况检查

站点运行状况检查包含在 Environment Test Service 中，这些检查可对 FlexCast Management Architecture (FMA) 服务进行全面评估。除了检查服务可用性外，这些检查还会查找其他运行状况指标，例如数据库连接。

站点运行状况检查在 Delivery Controller 上运行。根据站点的大小，这些检查可能需要长达一小时才能完成。

Delivery Controller 配置检查　作为站点运行状况检查的一部分。根据 Citrix 对 Virtual Apps and Desktops 站点提出的建议，Delivery Controller 配置检查会验证是否存在以下问题：

- 一个或多个 Delivery Controller 处于故障状态。
- 站点中只有一个 Delivery Controller。
- Delivery Controller 具有不同版本。

除了满足运行状况检查的权限和要求之外，Delivery Controller 配置检查还要求：

- 至少有一个 Controller 已开机。
- Broker Service 正在 Controller 上运行。
- 从 Controller 到站点数据库的连接正常工作。

VDA 运行状况检查

VDA 运行状况检查确定常见 VDA 注册、会话启动和时区重定向问题的可能的根本原因。

要在 VDA 上进行注册，Scout 会检查：

- VDA 软件安装
- VDA 计算机域成员身份
- VDA 通信端口可用性
- VDA 服务状态
- Windows 防火墙配置
- 与 Controller 通信

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 与 Controller 进行时间同步
- VDA 注册状态

对于 VDA 上的会话启动，Scout 将检查：

- 会话启动通信端口可用性
- 会话启动服务状态
- 会话启动 Windows 防火墙配置
- VDA 远程桌面服务客户端访问许可证
- VDA 应用程序启动路径

要在 VDA 上进行时区重定向，Scout 会检查：

- Windows 修补程序安装
- Citrix 修补程序安装
- Microsoft 组策略设置
- Citrix 组策略设置

对于 VDA 上的 Profile Management ，Scout 将检查：

- 虚拟机管理程序检测
- 预配检测
- Citrix Virtual Apps and Desktops
- Personal vDisk 配置
- 用户存储
- Profile Management Service 状态检测
- Winlogon.exe 挂钩测试

要对 Profile Management 运行检查，必须在 VDA 上安装并启用 Profile Management。有关 Profile Management 配置检查的详细信息，请参阅知识中心文章 CTX132805。

StoreFront 运行状况检查

StoreFront 检查会验证：

- Citrix Default Domain Service 正在运行
- Citrix Credential Wallet 服务正在运行
- 从 StoreFront 服务器到 Active Directory 端口 88 的连接
- 从 StoreFront 服务器到 Active Directory 端口 389 的连接
- 基本 URL 具有有效的 FQDN
- 可以从基本 URL 中检索正确的 IP 地址
- IIS 应用程序池正在使用.NET 4.0
- 证书是否已绑定到主机 URL 的 SSL 端口

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 证书链是否完成
- 证书是否已过期
- 证书是否即将到期（30 天内）

许可证服务器检查

许可证服务器检查会验证：

- 与 Delivery Controller 的许可证服务器连接
- 许可证服务器防火墙远程访问状态
- Citrix Licensing 服务状态
- 许可证服务器宽限期状态
- 许可证服务器端口连接
- Citrix 供应商守护程序 (CITRIX) 是否正在运行
- 系统时钟是否同步
- Citrix Licensing service 是否在本地服务帐户下运行
- 存在 `CITRIX.opt` 文件
- Customer Success Services 资格日期
- Citrix 许可证服务器更新
- 许可证服务器证书是否位于 Delivery Controller 的受信任根存储中

除了满足运行状况检查的权限和要求之外，许可证服务器还必须加入域。否则，将无法发现许可证服务器。

运行运行状况检查

运行状况检查过程包括选择计算机、启动检查，然后查看结果报告。

1. 启动 Scout。从计算机的开始菜单中，选择 **Citrix > Citrix Scout**。在打开的页面上，单击运行状况检查。
2. 选择计算机。单击查找计算机以发现计算机。选择计算机页面将列出在站点中发现的所有 VDA、Delivery Controller 和许可证服务器。可以按计算机名称过滤显示内容。选中要从中收集诊断信息的每台计算机旁边的复选框，然后单击继续。

   要添加其他组件类型（例如 StoreFront 服务器和 VDA 计算机），请参阅手动添加计算机和导入 VDA 计算机。无法手动添加 Citrix Provisioning 服务器或许可证服务器。

   Scout 将自动在选择的每台计算机上启动验证测试，以确保计算机满足验证测试中所列的条件。如果验证失败，系统将在状态列中发布一条消息，并取消选中相应计算机的复选框。您可以执行下列操作之一：

   - 解决问题，然后重新选中相应计算机的复选框。这将触发重试验证测试。
   - 跳过相应的计算机（让其复选框处于取消选中状态）。系统不会为该计算机运行运行状况检查。

   验证测试完成后，单击继续。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. 在所选计算机上运行运行状况检查。摘要列出了运行测试的所有计算机（您选择的通过验证测试的计算机）。单击开始检查。

   检查期间和检查后：

   - 状态列指示计算机的当前检查状态。
   - 要停止所有正在进行的检查，请单击页面右下角的停止检查。（不能取消单个计算机的运行状况检查，只能取消所有选定计算机的运行状况检查。系统将保留已完成检查的计算机中的信息。
   - 完成所有选定计算机的检查时，右下角的停止检查按钮将变为完成。
   - 如果检查失败，可以在操作列中单击重试。
   - 如果检查完成时未发现任何问题，操作列将为空。
   - 如果检查发现问题，请单击查看详细信息以显示结果。
   - 完成所有选定计算机的检查后，请勿单击返回。（如果执行此操作，检查结果将丢失。）

4. 检查完成时，单击完成返回到 Scout 的打开页面。

运行状况检查结果

对于生成报告的 Citrix 检查，报告包含：

- 生成结果报告的时间和日期
- 已检查的计算机
- 检查在目标计算机上查找的条件

权限和要求

权限：

- 要收集诊断信息，请执行以下操作：
  - 您必须是要从中收集诊断信息的每台计算机的本地管理员和域用户。
  - 必须对每台计算机上的 LocalAppData 目录具有写入权限。
- 要运行运行状况检查，请执行以下操作：
  - 您必须是域用户组的成员。
  - 您必须是具有完全权限的管理员或具有站点只读权限和运行环境测试权限的自定义角色。
  - 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`。注意：其他脚本执行权限也可以起作用。
- 启动 Scout 时使用以管理员身份运行。

对于要从中收集诊断信息或运行运行状况检查的每台计算机：

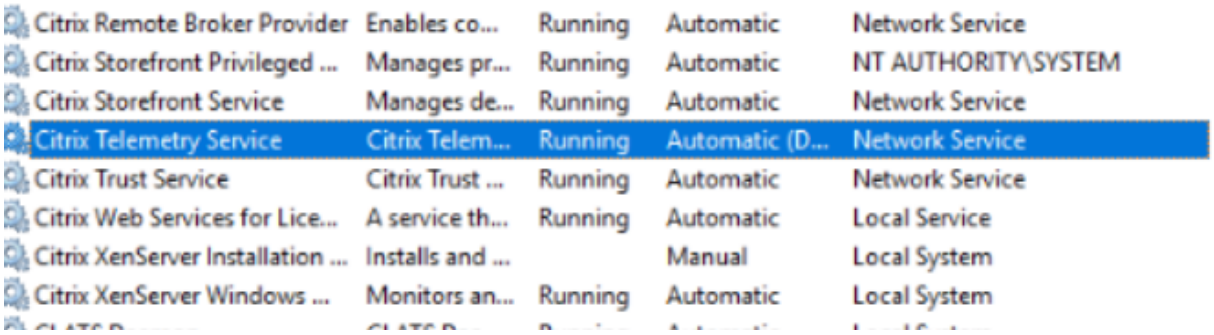
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Scout 必须能够与计算机通信。
- 必须打开文件和打印机共享。
- 必须启用 PSRemoting 和 WinRM。计算机还必须运行 PowerShell 3.0 或更高版本。
- 计算机上必须运行 Citrix Telemetry Service。
- 必须在计算机上启用 Windows Management Infrastructure (WMI) 访问权限。
- 要设置收集诊断信息的计划，计算机必须运行兼容的 Scout 版本。

请勿在路径名中指定的用户名中使用美元符号 ($)。这会阻止收集诊断信息。

Scout 将在所选计算机上运行验证测试，以确保满足上述要求。

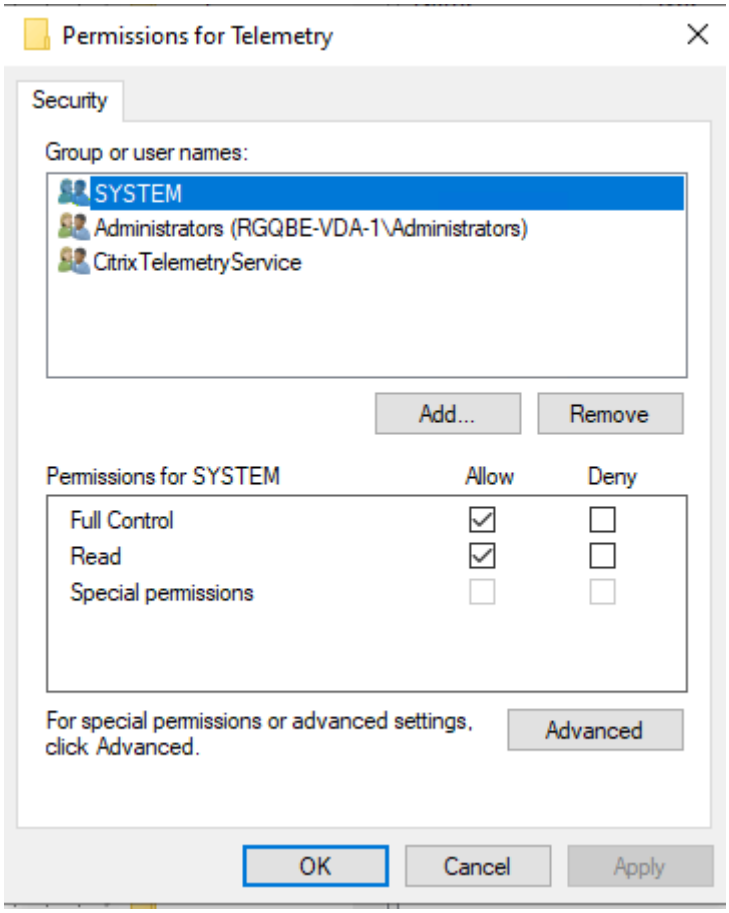
适用于 Windows 的 Telemetry Service 在网络服务上运行。



AOT 跟踪文件夹保存在 `C:\ProgramData\Citrix\TelemetryService\CitrixAOT` 中。

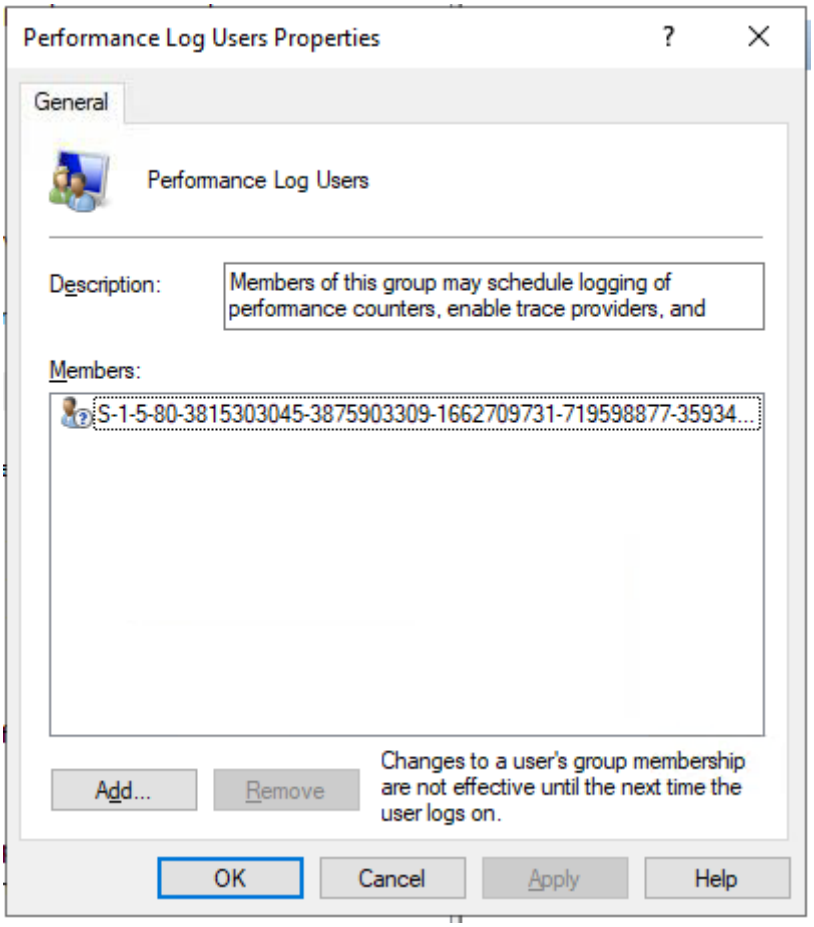
只有管理员组、系统和 Telemetry Service SID 中的用户有权访问 `HKEYLOCALMACHINE:SOFTWARE\Citrix\Telemetry` 注册表。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



在卸载 Telemetry Service 后，Telemetry Service SID 保留在性能日志用户组中，但您可以手动将其删除。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



验证测试

在开始收集诊断信息或执行运行状况检查之前，验证测试将针对选定的每台计算机自动运行。这些测试将确保满足这些要求。如果某台计算机的测试失败，Scout 将显示一条消息，提供建议的更正措施。

- **Scout** 无法访问此计算机 - 请确保：
  - 计算机已打开电源。
  - 网络连接正确运行。（这可以包括验证您的防火墙是否已正确配置。）
  - 已打开文件和打印机共享。请参阅 Microsoft 文档以了解相关说明。
- 启用 **PSRemoting** 和 **WinRM** - 可以同时启用 PowerShell 远程处理和 WinRM。使用以管理员身份运行，运行 `Enable-PSRemoting` cmdlet。有关详细信息，请参阅 Microsoft 帮助中的 cmdlet。
- **Scout** 要求 **PowerShell 3.0 (**最低版本**)** - 在计算机上安装 PowerShell 3.0（或更高版本），然后启用 PowerShell 远程处理。
- 无法访问此计算机上的 **LocalAppData** 目录 - 确保帐户对计算机上的 LocalAppData 目录具有写入权限。
- 找不到 **Citrix Telemetry Service** - 确保已在计算机上安装并启动 Citrix Telemetry Service。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 无法获取时间安排计划 - 将计算机（最低）升级到 XenApp 和 XenDesktop 7.14。
- **WMI** 未在计算机上运行 - 确保启用 Windows Management Instrumentation (WMI) 访问。
- 阻止 **WMI** 连接 - 在 Windows 防火墙服务中启用 WMI。
- 需要更新版本的 **Citrix Telemetry Service** -（仅针对“收集”、“跟踪和重现”检查版本。）升级计算机上的 Telemetry Service 版本（请参阅安装和升级）。如果不升级服务，则该计算机将不包含在收集或跟踪和重现操作中。
- **Scout** 无法连接到此计算机上的 **systemd** 套接字 - 请确保：
  - 端口 7503 处于打开状态。验证系统 systemd ctxtelemetry.socket 是否正在侦听计算机上的端口 7503。如果更改了 ctxtelemetry.socket porthas，端口可能会有所不同。请参阅 Scout 配置以调整端口。
  - 网络连接正确运行。（这可能包括验证您的防火墙是否已正确配置。）
- 在此计算机上未启动 **Linux VDA Telemetry Service** - 请确保：
  - 端口 7502 处于打开状态。验证是否已在计算机上安装并启动 Linux VDA Telemetry Service。如果遥测服务端口已更改，端口可能会有所不同。请参阅 Scout 配置以调整端口。
  - 网络连接正确运行。（这可能包括验证您的防火墙是否已正确配置。）

版本兼容性

此版本的 Scout (3.x) 要在 Citrix Virtual Apps and Desktops（最低 XenApp 和 XenDesktop 7.14）和 VDA 上运行。

XenApp 和 XenDesktop 7.14 之前的版本随附早期版本的 Scout。有关早期版本的信息，请参阅 CTX130147。

如果将 7.14 之前的 Controller 或 VDA 升级到版本 7.14（或受支持的更高版本），早期版本的 Scout 会替换为当前版本。

功能	Scout 2.23	Scout 3.0
支持 Citrix Virtual Apps and Desktops（以及 XenApp 和 XenDesktop 7.14 到 7.18）	是	是
支持 XenDesktop 5.x、7.1–7.13	是	否
支持 XenApp 6.x、7.5 至 7.13	是	否
与产品一起提供	7.1–7.13	自 7.14 起
可以从 CTX 文章中下载	是	否
捕获 CDF 跟踪	是	是

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

功能	Scout 2.23	Scout 3.0
捕获 AlwaysOn 跟踪 (AOT)	否	是
允许收集诊断数据	一次最多 10 台计算机（默认）	无限制（受资源可用性约束）
允许诊断数据发送到 Citrix	是	是
允许诊断数据保存在本地	是	是
支持 Citrix Cloud 凭据	否	是
支持 Citrix 凭据	是	是
支持使用代理服务器进行上载	是	是
调整计划	不适用	是
脚本支持	命令行（仅限本地 Controller）	使用 Call Home cmdlet 的 PowerShell（安装了 Telemetry Service 的任何计算机）
运行状况检查	否	是

安装和升级

默认情况下，安装或升级 VDA 或 Controller 时，Scout 会自动作为 Citrix Telemetry Service 的一部分进行安装或升级。

如果在安装 VDA 时忽略 Citrix Telemetry Service，或稍后删除该服务，请从 Citrix Virtual Apps and Desktops 安装介质上的 `x64\Virtual Desktop Components` 或 `x86\Virtual Desktop Components` 文件夹运行 `TelemetryServiceInstaller_xx.msi`。

选择收集或跟踪和重现操作时，系统会通知您计算机是否运行较旧版本的 Citrix Telemetry Service。Citrix 建议使用最新受支持的版本。如果不升级该计算机上的 Telemetry Service，该服务将不包含在收集或跟踪和重现操作中。要升级 Telemetry Service，请使用与安装该服务相同的过程。

上载授权

如果您计划将诊断收集信息上载到 Citrix，必须有 Citrix 或 Citrix Cloud 帐户。（这些是访问 Citrix 下载或访问 Citrix Cloud 控制中心时使用的凭据。）验证了您的帐户凭据后，系统会发出令牌。

- 如果您使用 Citrix 帐户进行身份验证，则发出令牌的过程不可见。您只需输入您的帐户凭据。Citrix 验证凭据后，您可以继续使用 Scout 向导。
- 如果您使用 Citrix Cloud 帐户进行身份验证，则单击链接访问 Citrix Cloud（在您的默认浏览器中使用 HTTPS）。输入您的 Citrix Cloud 凭据后，将显示令牌。请将令牌复制并粘贴到 Scout 中。然后您就可以在 Scout 向导中继续操作。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

令牌存储在运行 Scout 的计算机本地。要允许下次使用该令牌，请运行收集或跟踪和重现，然后选中存储令牌并在将来跳过此步骤复选框。

您每次在 Scout 的打开页面上选择计划时都必须重新授权。创建或更改计划时不能使用存储的令牌。

使用代理进行上载

如果要使用代理服务器将收集信息上载到 Citrix，可以指示 Scout 使用为浏览器的“Internet 属性”配置的代理设置。或者，您可以指定代理服务器的 IP 地址和端口号。

查找计算机

对于收集、跟踪和重现以及计划过程，Scout 会列出其自动发现的 Controller 和 VDA。

从 Delivery Controller 运行 Scout Health Check 时，单击查找计算机可发现计算机，包括 Delivery Controller、VDA、许可证服务器和 StoreFront 服务器。

从加入了域的计算机（不是 Delivery Controller）运行 Scout 运行状况检查时，Scout 无法自动发现计算机。您需要手动添加计算机或导入 VDA 计算机。

手动添加计算机

Scout 列出其发现的 Controller 和 VDA 后，您可以在部署中手动添加其他计算机，如 StoreFront 服务器、许可证服务器和 Citrix Provisioning 服务器。

运行运行状况检查时：

- 系统会自动发现域中的 Citrix 许可证服务器。无法手动添加许可证服务器。
- 运行状况检查当前不支持 Citrix Provisioning 服务器。

在列出发现的计算机的任何 Scout 页面上，单击 **+** 添加计算机。键入要添加的计算机的 FQDN，然后单击继续。根据需要重复以上操作以添加其他计算机。（虽然输入 DNS 别名而不是 FQDN 可能会显示有效，但运行状况检查可能会失败。）

手动添加的计算机始终显示在计算机列表的顶部，位于发现的计算机上方。

识别手动添加的计算机的简单方法是相应行右端有红色删除按钮。只有手动添加的计算机才有该按钮。发现的计算机没有该按钮。

要删除手动添加的计算机，请单击相应行右端的红色按钮。确认删除。重复以上操作以删除其他手动添加的计算机。

Scout 会记住手动添加的计算机，直到您将其删除。关闭再重新打开 Scout 时，列表顶部仍会列出手动添加的计算机。

在 StoreFront 服务器上使用跟踪和重现时，不会收集 CDF 跟踪信息。但会收集所有其他跟踪信息。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

导入 **VDA** 计算机

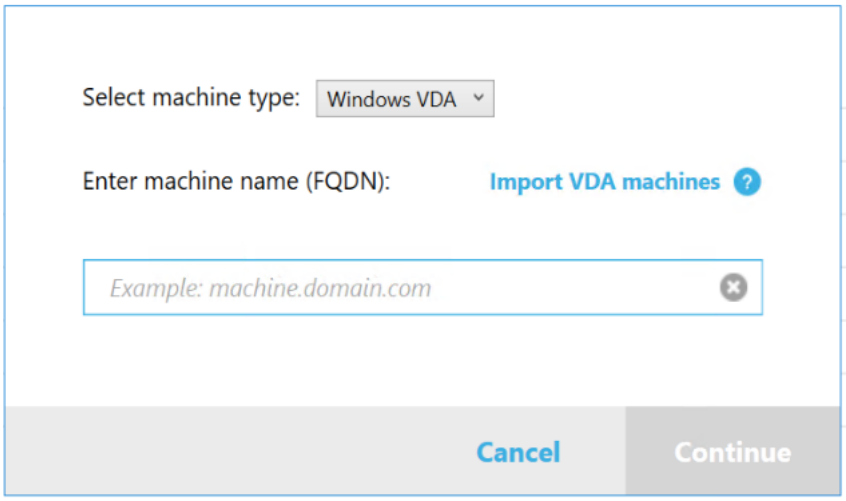
运行运行状况检查时，可以在部署中导入 VDA 计算机。

1. 在 Delivery Controller 或 Connector 上，使用 PowerShell 命令生成计算机列表文件。在 Connector 上，必须输入 Citrix 凭据并在弹出对话框中选择客户。

   ```
   Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList
   .txt
   ```

2. 将 machineList.txt 文件复制到要启动 Scout 运行状况检查并且加入了域的计算机。
3. 在“Scout 运行状况检查”页面上，单击添加计算机。
4. 选择 **Windows VDA** 计算机类型。
5. 单击导入 **VDA** 计算机。
6. 选择 machineList.txt 文件。
7. 单击打开。

导入的 VDA 计算机将在“Scout 运行状况检查”页面上列出。



收集诊断信息

收集过程包括选择计算机、开始收集诊断信息以及将包含收集信息的文件上载到 Citrix 或将其保存在本地。

1. 启动 Scout。从计算机的开始菜单中，选择 **Citrix > Citrix Scout**。在打开的页面上，单击收集。
2. 选择计算机。

   - 在 Controller 上，选择计算机页面上会列出站点中的所有 VDA 和 Controller。可以按计算机名称过滤显示内容。要手动添加其他计算机（例如 StoreFront 或 Citrix Provisioning 服务器），请参阅手动添加计算机。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 在其他组件（例如 VDA 服务器）上，选择计算机页面仅列出本地计算机。不支持手动添加计算机。

选中要从中收集诊断信息的每台计算机旁边的复选框，然后单击继续。

Scout 将自动在选择的每台计算机上启动验证测试，确保计算机满足验证测试中所列的条件。如果验证失败，将在状态列中发布一条消息，且取消选中相应计算机的复选框。您可以执行下列操作之一：

- 解决问题，然后重新选中相应计算机的复选框。这将触发重试验证测试。
- 跳过相应的计算机（让其复选框处于取消选中状态）。系统将不会从该计算机收集诊断信息。

验证测试完成后，单击继续。

3. 收集诊断信息。摘要中列出从中收集诊断信息的所有计算机（您选择的通过验证测试的计算机）。单击开始收集。

   在收集期间：

   - 状态列指示计算机的当前收集状态。
   - 要停止单台计算机上正在进行的收集，请在该计算机对应的操作列中单击取消。
   - 要停止所有正在进行的收集，请单击页面右下角的停止收集。系统会保留已完成收集的计算机中的诊断信息。要恢复收集，请在每台计算机对应的操作列中单击重试。
   - 完成所有选定计算机的收集时，右下角的停止收集按钮将变为继续。
   - 要再次收集诊断信息，请单击该计算机对应的操作列中的 重新收集。较新的收集信息将覆盖较早的收集信息。
   - 如果收集失败，可以在操作列中单击重试。仅成功完成的收集信息会上载或保存。
   - 在所有选定计算机完成收集后，请勿单击返回。（如果单击“返回”，收集的信息将丢失。）

   收集完成时，单击继续。

4. 保存或上载收集信息。选择是将文件上载到 Citrix，还是将其保存在本地计算机上。

   如果选择立即上载该文件，请继续执行步骤 5。

   如果选择在本地保存该文件：

   - 此时将显示 Windows 保存对话框。导航到所需位置。
   - 完成本地保存时，将显示文件的路径名并提供链接。您可以查看该文件。您可以稍后将文件上载到 Citrix。请参阅 CTX136396。

   单击完成返回 Scout 的打开页面。在此过程中，不需要完成任何进一步的步骤。

5. 为上载验证身份及（可选）指定代理。有关详情，请参阅上载授权。

   - 如果您没有通过 Scout 进行身份验证，请继续执行此步骤。
   - 如果您已通过 Scout 完成身份验证，则将默认使用存储的授权令牌。如果这是您想要执行此操作，请选择此选项并单击继续。系统不会提示您为此收集提供凭据。继续执行步骤 6。
   - 如果您之前已通过身份验证，但希望重新授权并获取新令牌，请单击更改/重新授权并继续执行此步骤。

   选择您要使用 Citrix 凭据还是 Citrix Cloud 凭据对上载进行身份验证。单击继续。仅当您不使用存储的令牌时才会显示凭据页面。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

在凭据页面上：

- 如果要使用代理服务器进行文件上载，请单击配置代理。可以指示 Scout 使用为浏览器的 Internet 属性配置的代理设置。或者，可以输入代理服务器的 IP 地址和端口号。关闭代理对话框。
- 对于 Citrix Cloud 帐户，请单击生成令牌。您的默认浏览器将启动并打开显示令牌的 Citrix Cloud 页面。请将令牌复制并粘贴到 Scout 页面中。
- 对于 Citrix 帐户，请输入您的凭据。

完成后，请单击继续。

6. 输入有关上载的信息。

   - 名称字段将包含所收集诊断信息的文件的默认名称。尽管您可以更改该名称，但这对于大多数收集来说足够了。（如果您删除默认名称，并使名称字段留空，系统将使用默认名称。）
   - （可选）指定 8 位数的 Citrix 支持案例号。
   - 在可选的说明字段中，描述问题并指示问题的发生时间（如果适用）。

   完成时，单击开始上载。

   在上载期间，页面左下部分会显示已完成的上载百分比近似值。要取消正在进行的上载，请单击停止上载。

   上载完成时，将显示其位置的 URL 并提供链接。您可以访问该链接前往 Citrix 位置查看上载的分析情况，也可以复制该链接。

   单击完成返回 Scout 的打开页面。

跟踪和重现

跟踪和重现过程包括选择计算机、启动跟踪、重现问题、完成诊断收集，以及将文件上载到 Citrix 或将其保存在本地。

此过程与标准收集过程类似。但是，您可以在计算机上开始跟踪，然后在这些计算机上重现问题。所有诊断集合都包括 AOT 跟踪信息。此过程添加 CDF 跟踪以帮助进行故障排除。

1. 启动 Scout。从计算机的开始菜单中，选择 **Citrix > Citrix Scout**。在打开的页面上，单击跟踪和重现。
2. 选择计算机。选择计算机页面上会列出站点中的所有 VDA 和 Controller。可以按计算机名称过滤显示内容。选中要从中收集跟踪和诊断信息的每台计算机旁边的复选框。然后单击继续。

   要手动添加其他计算机（例如 StoreFront 或 Citrix Provisioning 服务器），请参阅手动添加计算机。

   Scout 将自动在选择的每台计算机上启动验证测试，以确保计算机满足验证测试中所列的条件。如果某台计算机的验证失败，将在状态列中发布一条消息，且取消选中该计算机的复选框。您可以执行下列操作之一：

   - 解决问题，然后重新选中相应计算机的复选框。这将触发重试验证测试。
   - 跳过相应的计算机（让其复选框处于取消选中状态）。系统不会从该计算机收集诊断和跟踪信息。

   验证测试完成后，单击继续。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. 启动跟踪。摘要中列出从中收集跟踪信息的所有计算机。单击 **Start Tracing**（开始跟踪）。

   在一台或多台选定的计算机上，重现遇到的问题。在您执行该操作时，跟踪收集操作继续进行。完成问题重现后，在 Scout 中单击继续。这将停止跟踪。

   停止跟踪后，请指示是否在跟踪期间重现了问题。

4. 从计算机收集诊断信息。单击开始收集。在收集期间：

   - 状态列指示计算机的当前收集状态。
   - 要停止单台计算机上正在进行的收集，请在该计算机对应的操作列中单击取消。
   - 要停止所有正在进行的收集，请单击页面右下角的停止收集。系统会保留已完成收集的计算机中的诊断信息。要恢复收集，请在每台计算机对应的操作列中单击重试。
   - 完成所有选定计算机的收集时，右下角的停止收集按钮将变为继续。
   - 要再次从计算机收集诊断信息，请单击该计算机的操作列中的重新收集。较新的收集信息将覆盖较早的收集信息。
   - 如果收集失败，可以在操作列中单击重试。仅成功完成的收集信息会上载或保存。
   - 在所有选定计算机完成收集后，请勿单击返回。（如果单击“返回”，收集的信息将丢失。）

   收集完成时，单击继续。

5. 保存或上载收集信息。选择是将文件上载到 Citrix，还是将其保存在本地。

   如果选择立即上载该文件，请继续执行步骤 6。

   如果选择在本地保存该文件：

   - 此时将显示 Windows 保存对话框。选择所需位置。
   - 完成本地保存时，将显示文件的路径名并提供链接。您可以查看该文件。谨记：您可以在以后从 Citrix 上载该文件；请参阅 CTX136396 了解 Citrix Insight Services。

   单击完成返回 Scout 的打开页面。在此过程中，不需要完成任何进一步的步骤。

6. 为上载验证身份及（可选）指定代理。有关此过程的详细信息，请查看上载授权。

   - 如果您没有通过 Scout 进行身份验证，请继续执行此步骤。
   - 如果您已通过 Scout 完成身份验证，则将默认使用存储的授权令牌。如果这是您想要执行的操作，请选择此选项并单击继续。系统不会提示您为此收集提供凭据。继续执行步骤 7。
   - 如果您之前已通过身份验证，但希望重新授权并获取新令牌，请单击更改/重新授权并继续执行此步骤。

   选择您要使用 Citrix 凭据还是 Citrix Cloud 凭据对上载进行身份验证。单击继续。仅当您不使用存储的令牌时才会显示凭据页面。

   在凭据页面上：

   - 如果要使用代理服务器进行文件上载，请单击配置代理。可以指示 Scout 使用为浏览器的 Internet 属性配置的代理设置。或者，可以输入代理服务器的 IP 地址和端口号。关闭代理对话框。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 对于 Citrix Cloud 帐户，请单击生成令牌。您的默认浏览器将启动并打开显示令牌的 Citrix Cloud 页面。请将令牌复制并粘贴到 Scout 页面中。
- 对于 Citrix 帐户，请输入您的凭据。

完成后，请单击继续。

7. 提供有关上载的信息。

   输入上载详细信息：

   - 名称字段将包含所收集诊断信息的文件的默认名称。尽管您可以更改该名称，但这对于大多数收集来说足够了。（如果您删除默认名称，并使名称字段留空，系统将使用默认名称。）
   - （可选）指定 8 位数的 Citrix 支持案例号。
   - 在可选的说明字段中，描述问题并指示问题的发生时间（如果适用）。

   完成时，单击开始上载。

   在上载期间，页面左下部分显示已完成的上载百分比近似值。要取消正在进行的上载，请单击停止上载。

   上载完成时，将显示其位置的 URL 并提供链接。您可以访问该链接前往 Citrix 位置查看上载的分析情况，也可以复制该链接。

   单击完成返回 Scout 的打开页面。

计划收集

> 注意：
>
> 您目前可以计划收集，但不能计划运行状况检查。

计划过程包括选择计算机以及设置或取消计划。计划的收集信息会自动上载到 Citrix。（您可以使用 PowerShell 界面在本地保存计划的收集信息。请参阅 Citrix Call Home。）

1. 启动 Scout。从计算机的“开始”菜单中，选择 **Citrix > Citrix Scout**。在打开的页面上，单击计划。
2. 选择计算机。系统将列出站点中的所有 VDA 和 Controller。可以按计算机名称过滤显示内容。

   当您使用图形界面安装 VDA 和 Controller 时，如果您设置了 Call Home 计划（请参阅 Citrix Call Home），Scout 默认情况下会显示这些设置。可以使用此版本的 Scout 首次开始计划的收集，也可以更改以前配置的计划。

   尽管您在组件安装期间基于每台计算机启用/禁用了 Call Home，但在 Scout 中配置的计划会影响您选择的所有计算机。

   选中要从中收集诊断信息的每台计算机旁边的复选框，然后单击继续。

   要手动添加其他计算机（例如 StoreFront 或 Citrix Provisioning 服务器），请参阅手动添加计算机。

   Scout 将自动在选择的每台计算机上启动验证测试，以确保计算机满足验证测试中的条件。如果某台计算机的验证失败，将在状态列中发布一条消息，且取消选中该计算机的复选框。您可以执行下列操作之一：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 解决问题，然后重新选中相应计算机的复选框。这将触发重试验证测试。
- 跳过相应的计算机（让其复选框处于取消选中状态）。不会从该计算机收集诊断（或跟踪）信息。

验证测试完成后，单击继续。

摘要页面上列出应用计划的计算机。单击继续。

3. 设置计划。指示要何时收集诊断信息。谨记：计划会影响所有选定计算机。

   - 要为选定计算机配置每周计划，请单击每周。选择星期几。输入开始收集信息的时间（24 小时制）。
   - 要为选定计算机配置每天计划，请单击每天。输入开始收集信息的时间（24 小时制）。
   - 要为选定计算机取消现有计划（且不替换为其他计划），请单击关闭。这将取消之前为这些计算机配置的任何计划。

   单击继续。

4. 为上载验证身份及（可选）指定代理。有关此过程的详细信息，请查看上载授权。谨记：使用 Scout 计划时，不能使用存储的令牌进行身份验证。

   选择您要使用 Citrix 凭据还是 Citrix Cloud 凭据对上载进行身份验证。单击继续。

   在凭据页面上：

   - 如果要使用代理服务器进行文件上载，请单击配置代理。可以指示 Scout 使用为浏览器的 Internet 属性配置的代理设置。或者，可以输入代理服务器的 IP 地址和端口号。关闭代理对话框。
   - 对于 Citrix Cloud 帐户，请单击生成令牌。您的默认浏览器将启动并打开显示令牌的 Citrix Cloud 页面。请将令牌复制并粘贴到 Scout 页面中。
   - 对于 Citrix 帐户，请输入您的凭据。

   完成后，请单击继续。

   查看配置的计划。单击完成返回 Scout 的打开页面。

   在收集期间，每个选定计算机的 Windows 应用程序日志都包含有关收集和上载的条目。

数据屏蔽

使用 Citrix Scout 收集的诊断信息可能包含安全敏感信息。Citrix Scout 数据屏蔽功能允许您在将诊断文件中的敏感数据上载到 Citrix 之前屏蔽这些数据。

Scout 数据屏蔽功能配置为屏蔽 IP 地址、计算机名称、域名、用户名、虚拟机管理程序名称、交付组名称、目录名称、应用程序名称和 SID。

> 注意：
>
> CDF 跟踪是加密的，无法屏蔽。
>
> Linux VDA 日志压缩为 `.tar.gz2` 格式，无法屏蔽。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

收集新诊断信息并执行数据屏蔽

要使用 Citrix Scout 数据屏蔽功能，请从命令行启动 Scout。

1. 在 Windows 中，以管理员身份打开命令提示符。
2. 转到 Scout 的安装目录：`cd C:\Program Files\Citrix\Telemetry Service`。
3. 启动 Scout：`ScoutUI.exe datamasking`。
4. 单击收集或跟踪和重现以收集诊断信息。
5. 收集完成后，选择启用数据屏蔽。默认情况下启用此选项。
6. 配置数据屏蔽。可以使用默认规则或者自定义规则。
7. 选择上载还是保存诊断收集信息。

    - 如果选择将收集的诊断信息上载到 **Citrix**，则会将屏蔽的诊断文件上载到 Citrix。
    - 如果选择在您的本地计算机上保存收集的诊断信息，原始诊断和屏蔽的诊断都将保存到指定位置。

对现有诊断信息执行数据屏蔽

1. 在 Windows 中，以管理员身份打开命令提示符。
2. 转到 Scout 的安装目录：`cd C:\Program Files\Citrix\Telemetry Service`。
3. 在数据屏蔽模式下直接启动 Scout：`ScoutUI.exe datamasking filePath`。
4. 选择“启用数据屏蔽”以继续。默认情况下启用此选项。
5. 配置数据屏蔽。可以使用默认规则运行数据屏蔽或者自定义规则。
6. 选择上载还是保存诊断收集信息。

    - 如果选择将收集的诊断信息上载到 **Citrix**，则会将屏蔽的诊断文件上载到 Citrix。
    - 如果选择在您的本地计算机上保存收集的诊断信息，原始诊断和屏蔽的诊断都将保存到指定位置。

屏蔽的数据文件和映射文件位置

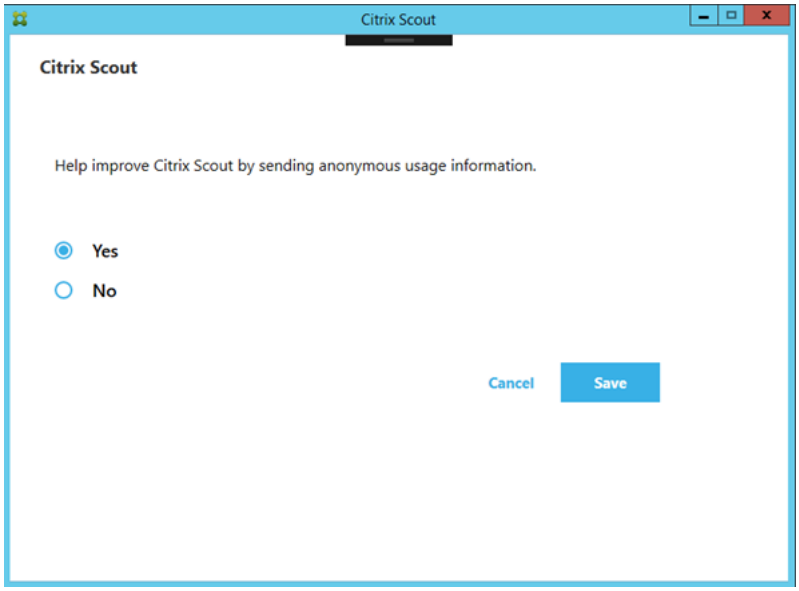
上载或保存诊断收集信息后，单击链接以打开原始诊断信息和屏蔽的诊断信息，然后打开映射信息文件。

使用数据收集

使用 Scout 时，Citrix 会使用 Google Analytics 来收集匿名使用数据，用于将来的产品功能和改进。默认情况下，数据收集处于启用状态。

要更改使用情况数据收集和上载，请单击 Scout UI 中的设置齿轮。然后，您可以选择是否发送信息，方法是选择是或否，然后单击保存。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



监视

January 21, 2022

管理员和技术支持人员可以使用各种功能和工具监视 Citrix Virtual Apps and Desktops 站点。使用这些工具，您可以监视：

- 用户会话和会话使用情况
- 登录性能
- 连接和计算机，包括失败情况
- 负载评估
- 历史趋势
- 基础结构

Citrix Director

Director 是一款实时 Web 工具，您可以利用此工具进行监视和排除故障以及为最终用户执行支持任务。

有关详细信息，请参阅 Director 各文章。

配置日志记录

利用配置日志记录功能，管理员可以跟踪对站点所做的管理更改。配置日志记录可以帮助管理员诊断和排除配置更改后出现的问题，辅助进行变更管理和跟踪配置，并报告管理活动。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

您可以从 Studio 查看和生成关于已记录信息的报告。还可以在 Director 中使用 Trend View 查看记录的项目，以提供配置更改通知。此功能对不具有 Studio 访问权限的管理员很有用。

Trends View 提供一段时间内的配置更改历史数据，使管理员可以访问对站点所做的更改、更改时间和执行更改的人员，以便查找问题的原因。此视图将配置信息细分为三个类别：

- 连接失败
- 出现故障的单会话计算机
- 出现故障的多会话计算机

有关如何启用和配置“配置日志记录”的详细信息，请参阅配置日志记录。Director 各文章介绍了如何通过该工具查看记录的信息。

事件日志

Citrix Virtual Apps and Desktops 中的服务记录发生的事件。事件日志可以用于对操作进行监视和故障排除。

有关详细信息，请参阅事件日志。各功能文章可能也包含某些事件信息。

配置日志记录

January 21, 2022

配置日志记录是用于捕获针对数据库的站点配置更改和管理活动的一项功能。默认情况下启用该功能。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并进行故障排除。日志提供浏览路径记录。
- 协助更改管理和跟踪配置。
- 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。可以按日期范围和全文搜索结果过滤显示的配置日志。如果启用强制日志记录，可以阻止进行配置更改，除非这些更改可以记入日志。只要具有适当的权限，即可删除配置日志中的条目。您无法使用配置日志记录功能编辑日志内容。

配置日志记录使用 PowerShell SDK 和 Configuration Logging Service。Configuration Logging Service 在站点中的每个 Controller 上运行。如果某个 Controller 出现故障，另一个 Controller 上的服务将自动处理日志记录请求。

默认情况下，启用配置日志记录功能，它使用在您创建站点时所创建的数据库（站点配置数据库）。可以为数据库指定不同的位置。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，用英语创建的日志将以英语显示，而无论阅读器的区域设置为何。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

记录的内容

通过 Studio、Director 和 PowerShell 脚本启动的配置更改和管理活动都在记录范围之内。记录的配置更改包括对以下项目的处理（创建、编辑、删除和分配）：

- 计算机目录
- 交付组（包括更改电源管理设置）
- 管理员角色和作用域
- 主机资源和连接
- 通过 Studio 管理的 Citrix 策略

记录的管理更改示例包括：

- 虚拟机或用户桌面的电源管理
- Studio 或 Director 向用户发送消息

以下操作不在记录范围之内：

- 自动操作，如虚拟机的池管理启动。
- 通过组策略管理控制台 (GPMC) 实施的策略操作；使用 Microsoft 工具查看这些操作的日志。
- 通过注册表、直接访问数据库或从 Studio、Director 或 PowerShell 以外的来源进行的更改。
- 初始化部署后，配置日志记录从在 Configuration Service 中注册首个 Configuration Logging Service 实例时开始可用。因此，早期阶段的配置不会写入日志（例如，获取和应用数据库架构以及初始化虚拟机管理程序期间的配置）。

管理配置日志记录

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。

不支持配置日志记录的产品版本在 Studio 中没有日志记录节点。

启用和禁用配置日志记录以及强制日志记录

默认情况下，启用配置日志记录，禁用强制日志记录。

1. 在 Studio 导航窗格中选择日志记录。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。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。如果先前已启用日志记录，现有的日志仍然可通过 PowerShell SDK 进行读取。

   要启用强制日志记录，请选择阻止在数据库不可用时更改站点配置。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。仅当启用了配置日志记录（即选择了启用时），才能启用强制日志记录。如果 Configuration Logging Service 出现故障，并且未使用高可用性，则会使用强制日志记录。在这种情况下，将不会执行通常会记入日志的操作。

   要禁用强制日志记录，请选择允许在数据库不可用时更改站点配置。即使无法访问配置日志记录数据库，也允许进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

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。请参阅数据库地址格式了解有效的格式。
6. 要允许 Studio 创建数据库，请单击确定。出现提示时，单击确定，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。如果该操作失败，系统将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，并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指出发生了数据库更改，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 的中上部窗格中将列出 Studio 和 Director 创建的高级别操作。高级别操作会导致出现一个或多个服务和 SDK 调用，这些是低级别操作。在上部的窗格中选择一项高级别操作时，下部的窗格将显示低级别操作。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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，中心窗格将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。您可以：

- 按列标题对显示的内容进行排序。
- 通过指定一个一天的时间间隔，或者在搜索框中输入文本，对显示的内容进行过滤。要在使用搜索后返回到标准显示，请清除搜索框中的文本。

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（名为 MyReport）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。
- 浏览到要保存报告的位置。

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。完全权限管理员角色具有此权限。自定义角色必须具有在“其他权限”类别中选择的“只读”或“管理”权限。

  要在删除配置日志记录数据之前为其创建备份，自定义角色还必须具有在“日志记录权限”类别中选择的“只读”或“管理”权限。

- **SQL Server** 数据库：必须具备拥有可从数据库中删除记录权限的 SQL Server 登录帐户。有两种方式实现此要求：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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个角色成员：`ConfigurationLoggingSchema_ROL` 或 `dbowner`。

  有关详细信息，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。

事件日志

November 17, 2021

以下文章列出并介绍了 Citrix Virtual Apps and Desktops 中的服务可以记录的事件。

此信息不全面。读者应检查各功能文章了解其他事件信息。

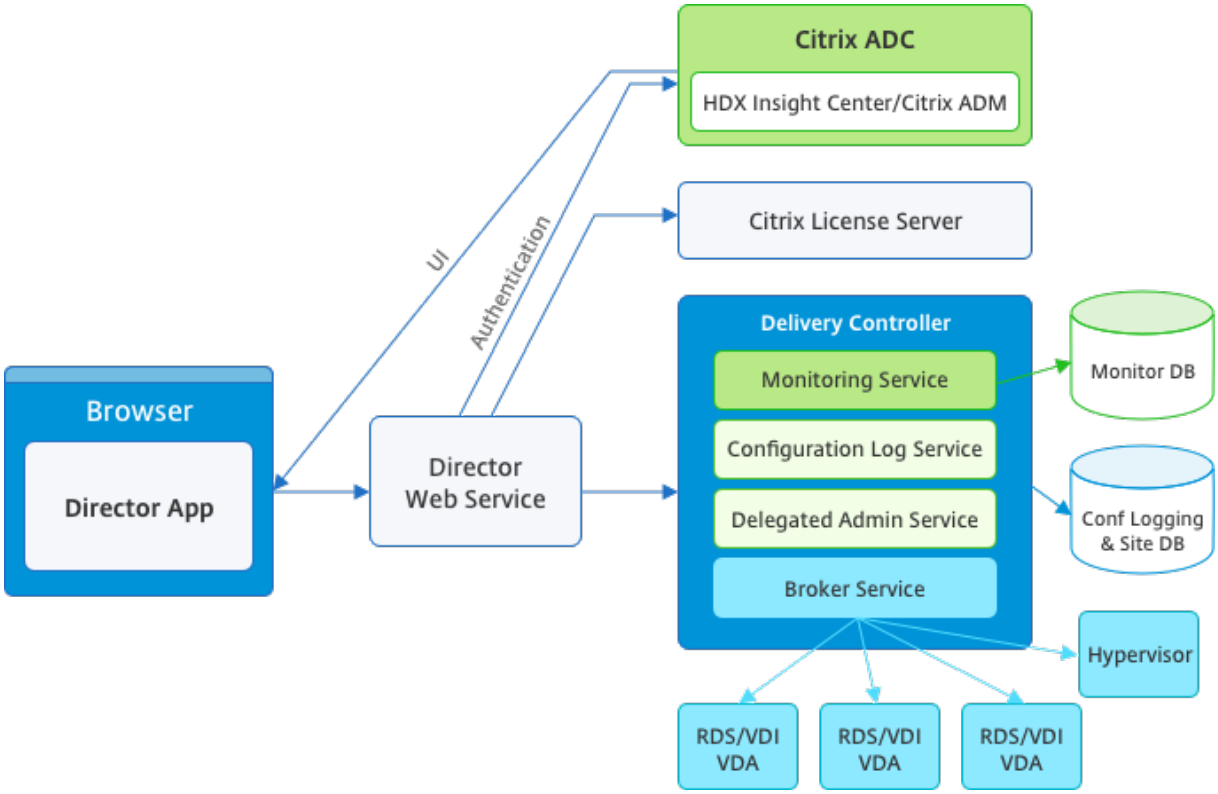
- Citrix Broker Service 事件
- Citrix FMA Service SDK 事件
- Citrix Configuration Service 事件
- Citrix Delegated Administration Service 事件

Director

July 5, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Director 是适用于 Citrix Virtual Apps and Desktops 的监视和故障排除控制台。



Director 可以访问：

- 使用集成了 Analytics、Performance Manager 和 Network Inspector 的统一控制台访问来自 Broker Agent 的实时数据。以下分析由 Citrix ADM 提供技术支持，以确定由于 Citrix Virtual Apps 或 Citrix Virtual Desktops 环境中的网络造成的瓶颈：
  - 运行状况和容量保证的性能管理
  - 历史趋势和网络分析
- 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 Citrix ADM 来自 Citrix Gateway 的 ICA 数据。
  - 可以了解 Citrix Virtual Apps 或 Citrix Virtual Desktops 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 Citrix Virtual Desktops 7 Director 监视工具集成。

Director 使用故障排除控制板。此控制板提供对 Citrix Virtual Apps 或 Citrix Virtual Desktops 站点的实时和历史运行状况监视。利用此功能，您可以实时查看故障，更好地了解最终用户的体验。

有关 Director 功能与 Delivery Controller (DC)、VDA 以及任何其他依赖组件的兼容性的详细信息，请参阅功能兼容性列表。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 在近期披露了 Meltdown 和 Spectre 推理执行边信道漏洞的背景下，Citrix 建议您安装相关缓解修补程序。这些修补程序可能会影响 SQL Server 的性能。有关详细信息，请参阅 Microsoft 支持文章保护 SQL Server 免受 Spectre 和 Meltdown 边信道漏洞的攻击。Citrix 建议您测试规模，并在生产环境中实施修补程序之前规划您的工作负载。

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。有关安装和配置 Director 的特定信息，请参阅安装和配置 Director。

登录 **Director**

Director Web 站点位于 https 或 `http://<Server FQDN>/Director`。

如果多站点部署中的一个站点出现故障，在尝试连接到该故障站点时，登录所需的时间会稍长。

在 **Director** 中使用 **PIV** 智能卡身份验证

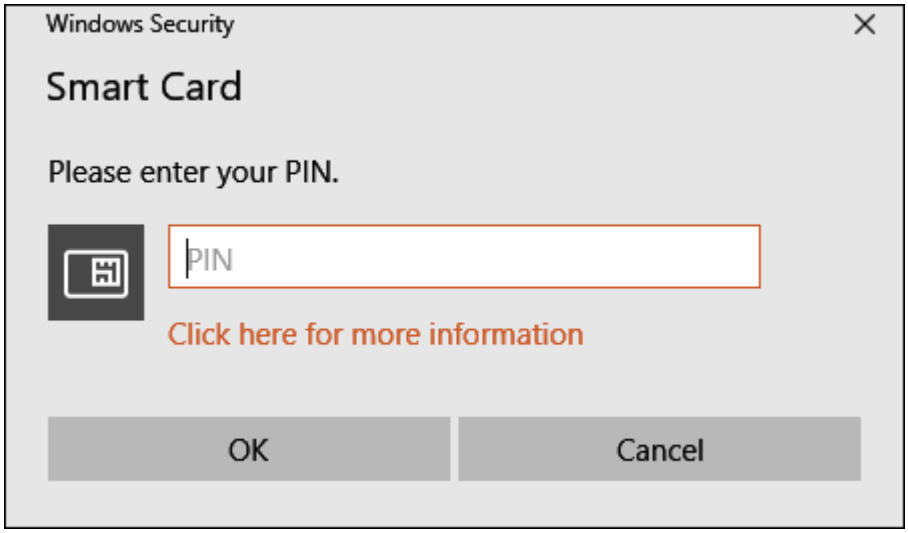
Director 现在支持通过基于智能卡身份验证的个人身份验证 (PIV) 进行登录。此功能对使用基于智能卡的身份验证进行访问控制的组织和政府机构非常有用。
智能卡身份验证要求在 Director 服务器上和 Active Directory 中执行特定配置。配置步骤在配置 PIV 智能卡身份验证中进行详细说明。

> 注意：
>
> 智能卡身份验证仅支持来自相同 Active Directory 域的用户。

执行所需的配置后，可以使用智能卡登录 Director：

1. 将您的智能卡插入到智能卡读卡器中。
2. 打开浏览器并转至 Director URL `https://<directorfqdn>/Director`。
3. 从显示的列表中选择一个有效的用户证书。
4. 输入您的智能卡令牌。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



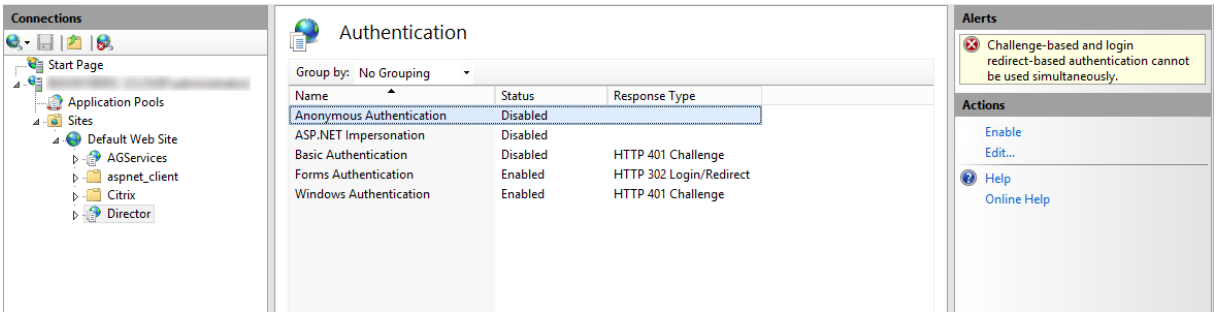
5. 进行身份验证后，无需在 Director 登录页面上键入额外的凭据即可访问 Director。

将 **Director** 与集成 **Windows** 身份验证结合使用

通过集成 Windows 身份验证 (IWA)，加入了域的用户可以获得直接访问 Director 的权限，而不需要重新在 Director 登录页面上键入其凭据。使用集成 Windows 身份验证和 Director 的必备条件如下：

- 在托管 Director 的 IIS Web 站点上启用集成 Windows 身份验证。安装 Director 时，启用匿名和表单身份验证。要支持集成 Windows 身份验证和 Director，请禁用匿名身份验证并启用 Windows 身份验证。对于非域用户的身份验证，表单身份验证仍必须设置为“已启用”。

  1. 启动 IIS 管理器。
  2. 转至站点 > 默认 **Web** 站点 > **Director**。
  3. 选择身份验证。
  4. 右键单击匿名身份验证，然后选择禁用。
  5. 右键单击 **Windows** 身份验证，然后选择启用。



- 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，则仅需要进行配置。

  1. 在 Active Directory 计算机上，打开 Active Directory 管理控制台。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. 在 Active Directory 管理控制台中，导航到域名 > 计算机。选择 Director 计算机。
3. 单击鼠标右键并选择属性。
4. 在“属性”中，选择委派选项卡。
5. 选择选项信任此计算机来委派任何服务 **(**仅 **Kerberos)**。

- 用于访问 Director 的浏览器必须支持集成 Windows 身份验证。在 Firefox 和 Chrome 中，可能需要执行额外的配置步骤。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。

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。

有关 Director 中的各种角色及其权限的详细信息，请参阅委派管理和 Director

Google Analytics 执行的使用数据收集

Director Service 会在安装 Director 后开始使用 Google Analytics 匿名收集使用数据。收集有关“趋势”页面的使用情况及其 OData API 调用分析有关的统计信息。Analytics 收集符合 Citrix 隐私政策。默认情况下，安装 Director 时启用数据收集。

要退出 Google Analytics 数据收集，请在安装了 Director 的计算机上编辑注册表项。如果该注册表项不存在，请创建并将其设置为所需的值。请在更改注册表项值后刷新 Director 实例。

小心：注册表编辑器使用不当会导致出现严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。Citrix 建议您先备份 Windows 注册表，然后再更改。

位置：HKEY_LOCAL_MACHINE\Software\Citrix\Director

名称：DisableGoogleAnalytics

值：0 = 已启用（默认值），1 = 已禁用

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

可以使用以下 PowerShell cmdlet 禁用 Google Analytics 执行的数据收集：

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director

New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
    DisableGoogleAnalytics -PropertyType DWORD -Value 1
```

新增功能指南

Director 包含产品内指南，该指南使用 Pendo 深入介绍了当前版本的 Director 中发布的新增功能。快速概览再加上相应的产品内消息可帮助您了解产品中的新增功能。

要退出此功能，请按照下面的说明在安装了 Director 的计算机上编辑注册表项。如果该注册表项不存在，请创建并将其设置为所需的值。请在更改注册表项值后刷新 Director 实例。

> 小心：
>
> “注册表编辑器”使用不当会导致出现严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。Citrix 建议您先备份 Windows 注册表，然后再更改。

位置：HKEY_LOCAL_MACHINE\Software\Citrix\Director

名称：DisableGuidedHelp

值：0 = 已启用（默认值），1 = 已禁用

可以使用以下 PowerShell cmdlet 禁用产品内指南：

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director

New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
    -PropertyType DWORD -Value 1
```

安装和配置

January 21, 2022

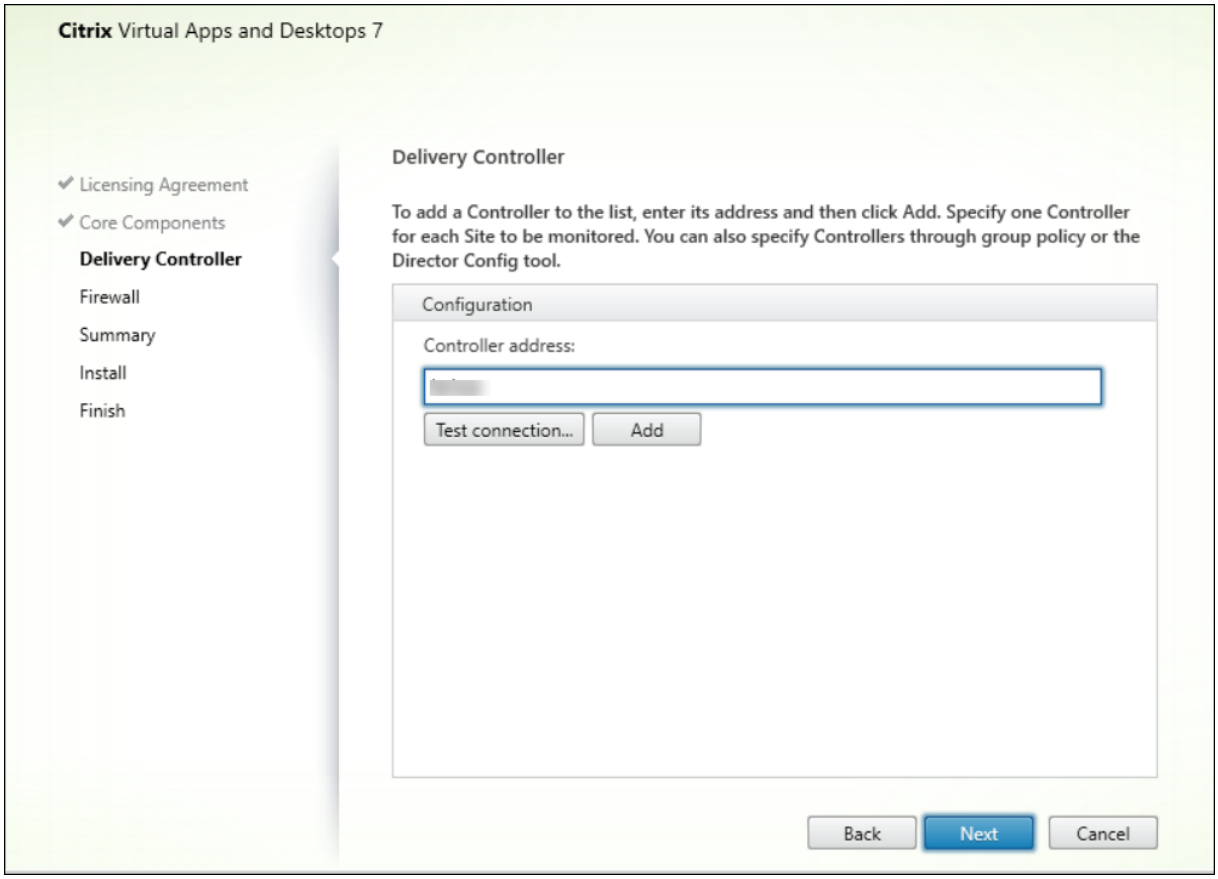
安装 **Director**

使用 Citrix Virtual Apps and Desktops 完整产品 ISO 安装程序安装 Director，该安装程序将检查必备项，安装任何缺少的组件，设置 Director Web 站点，以及执行基本配置。有关必备项和其他详细信息，请参阅此版本的系统要求文档。此版本的 Director 与 6.5 版之前的 Virtual Apps 部署或 7 版之前的 Virtual Desktops 部署不兼容。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

安装程序提供的默认配置可处理典型部署。如果在安装期间未安装 Director，请使用 ISO 安装程序添加 Director。要添加任何其他组件，请重新运行 ISO 安装程序并选择要安装的组件。有关使用 ISO 安装程序的信息，请参阅安装文档中的安装核心组件。Citrix 建议仅使用完整产品 ISO 安装程序进行安装，而不是使用.MSI 文件。

当 Director 安装在 Controller 上时，将自动配置 localhost 作为服务器地址，并且默认情况下，Director 将与本地 Controller 进行通信。要在 Controller 的远程专用服务器上安装 Director，系统将提示您输入 Controller 的 FQDN 或 IP 地址。



> 注意：
>
> 单击添加可添加要监视的 Controller。

默认情况下，Director 与指定的 Controller 进行通信。仅为监视的每个站点指定一个 Controller 地址。Director 将自动发现同一站点中的所有其他 Controller，并且如果您指定的 Controller 出现故障，则将回退到其他 Controller。

> 注意：
>
> Director 无法在 Controller 之间平衡负载。

为确保浏览器与 Web 服务器之间的通信安全，Citrix 建议您在托管 Director 的 IIS Web 站点上实施 TLS。有关说明，请参阅 Microsoft IIS 文档。无需对 Director 执行任何配置即可启用 TLS。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

部署和配置 **Director**

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。

> 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，请仅允许使用 HTTPS（而不是 HTTP）建立 Director 连接。某些工具可以读取 HTTP（未加密）网络数据包中的纯文本用户名和密码，这会对用户造成潜在安全风险。

配置权限

要登录 Director，具有 Director 权限的管理员必须是 Active Directory 域用户并且必须具有以下权限：

- 对要搜索的所有 Active Directory 林的读取权限（请参阅高级配置）
- 配置的委派管理员角色（请参阅委派管理和 Director）。
- 要重影用户，必须使用适用于 Windows 远程协助的 Microsoft 组策略来配置管理员。此外：
  - 安装 VDA 时，确保在所有用户设备（默认处于选中状态）上启用 Windows 远程协助功能。
  - 在服务器上安装 Director 时，确保已安装 Windows 远程协助（默认处于选中状态）。但默认情况下服务器上禁用此功能。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（CTX127388：如何为 Desktop Director 启用远程协助）。

高级配置

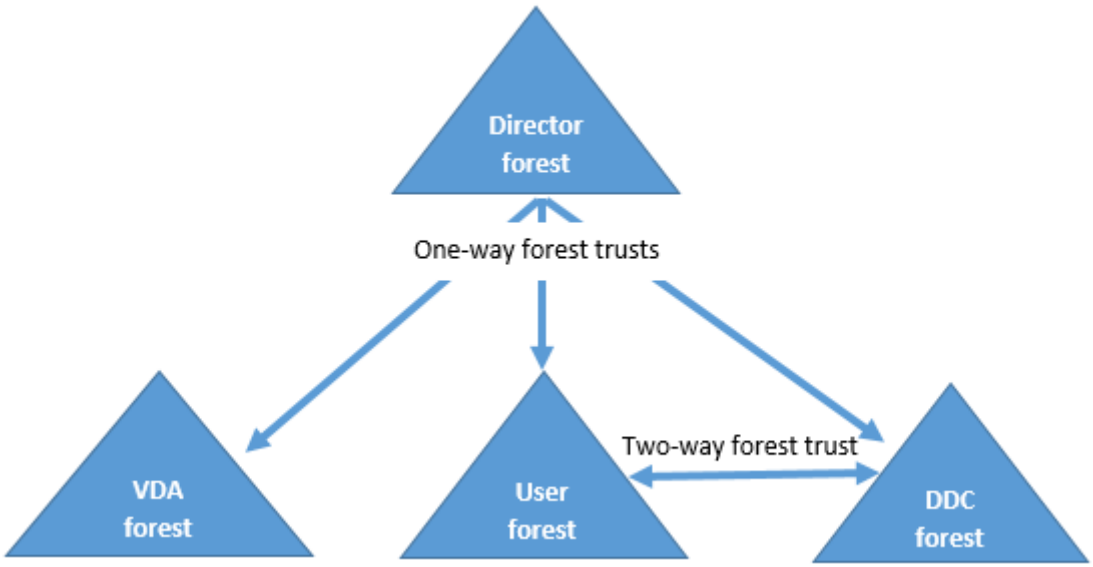
November 17, 2021

Director 可支持跨越一个林配置的多林环境，其中用户、Delivery Controller (DC)、VDA 和 Director 均位于不同的林中。这要求在这些林中和配置设置中正确设置信任关系。

多林环境中的建议配置

建议的配置要求在这些林中使用整个域身份验证创建传出和传入林信任关系。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



通过 Director 中的信任关系，您可以对位于不同林的用户会话、VDA 和 Delivery Controller 中出现的问题进行故障排除。

Director 支持多个林所需的高级配置通过 Internet Information Services (IIS) 管理器中定义的设置进行控制。

> 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。
5. 单击添加以添加新设置。

Director 使用 Active Directory 搜索用户并查找更多用户和计算机信息。默认情况下，Director 搜索：

- 管理员帐户所属的域或林。
- Director Web 服务器所属的域或林（如果不相同）。

Director 将尝试使用 Active Directory 全局目录在林级别执行搜索。如果您没有相应的权限，无法在林级别执行搜索，则仅搜索域。

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。在 IIS 管理器中将以下应用程序设置配置到 Director Web 站点：

```
Connector.ActiveDirectory.Domains = (user),(server)
```

值属性“user”和“server”分别代表 Director user（管理员）和 Director server 所在的域。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

要使用户能够从额外的域或林中进行搜索，请将该域的名称添加到列表中，如下例中所示：

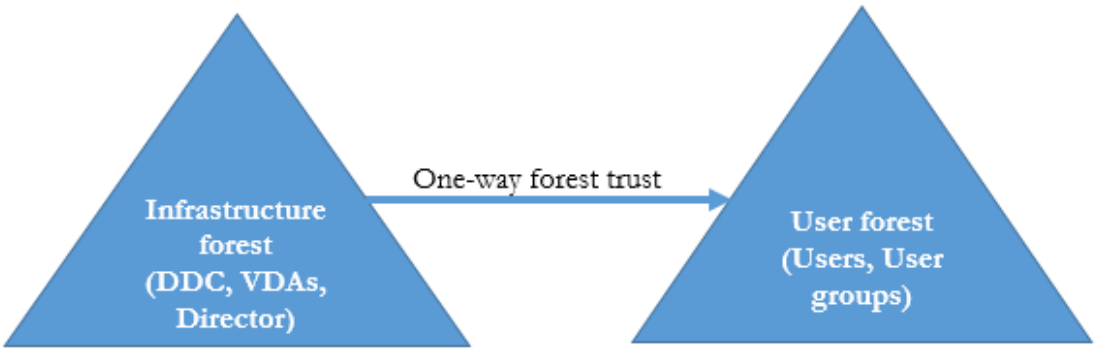
```
Connector.ActiveDirectory.Domains = (user),(server),\<domain1\>,\<
    domain2\>
```

对于列表中的每个域，Director 将尝试在林级别执行搜索。如果您没有相应的权限，无法在林级别执行搜索，则仅搜索域。

域本地组配置

大多数 Citrix Service Provider (CSP) 在基础结构林中具有由 VDA、DC 和 Director 组成的相似环境设置。用户或用户组记录属于客户林。从基础结构林到客户林存在单向传出信任。

CSP 管理员通常在基础结构林中创建一个域本地组，并将客户林中的用户或用户组添加到此域本地组。



与此类似，Director 可以支持多林设置，以及可以监视使用域本地组配置的用户会话。

1. 在 IIS 管理器中将以下应用程序设置添加到 Director Web 站点：

   ```
   Connector.ActiveDirectory.DomainLocalGroupSearch= true Connector.
       ActiveDirectory

   DomainLocalGroupSearchDomains= \<domain1\>,\<domain2\>
   ```

   <domain1><domain2> 是域本地组所在的林的名称。

2. 将域本地组分配到 Citrix Studio 中的交付组。
3. 重新启动 IIS 并再次登录 Director 以使更改生效。现在，Director 可以监视并显示这些用户的会话。

向 **Director** 中添加站点

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：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
<!--NeedCopy-->
```

SiteAController 和 SiteBController 为两个不同站点中的 Delivery Controller 的地址。

在活动管理器中禁止显示运行中的应用程序

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都查看此信息。对于委派管理员角色，完全权限管理员、交付组管理员和技术支持管理员均可以查看此信息。

为保护用户及其正在运行的应用程序的隐私，您可以禁止应用程序选项卡以列出正在运行的应用程序。

> 警告：
>
> 注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 不保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

1. 在 VDA 上，修改位于 HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed 的注册表项。默认情况下，该注册表项设置为 1。将值更改为 0，这表示信息不是从 VDA 中收集的，因此不在活动管理器中显示。
2. 在安装了 Director 的服务器上，修改用于控制正在运行的应用程序可见性的设置。默认情况下，该值为 true，表示允许应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，请进行上述两项更改，以确保在活动管理器中不显示这些数据。

配置 PIV 智能卡身份验证

January 21, 2022

本文列出了在 Director 服务器上和 Active Directory 中启用智能卡身份验证功能所需的配置。

> 注意：
>
> 智能卡身份验证仅支持来自相同 Active Directory 域的用户。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Director 服务器配置

请在 Director 服务器上执行以下配置步骤：

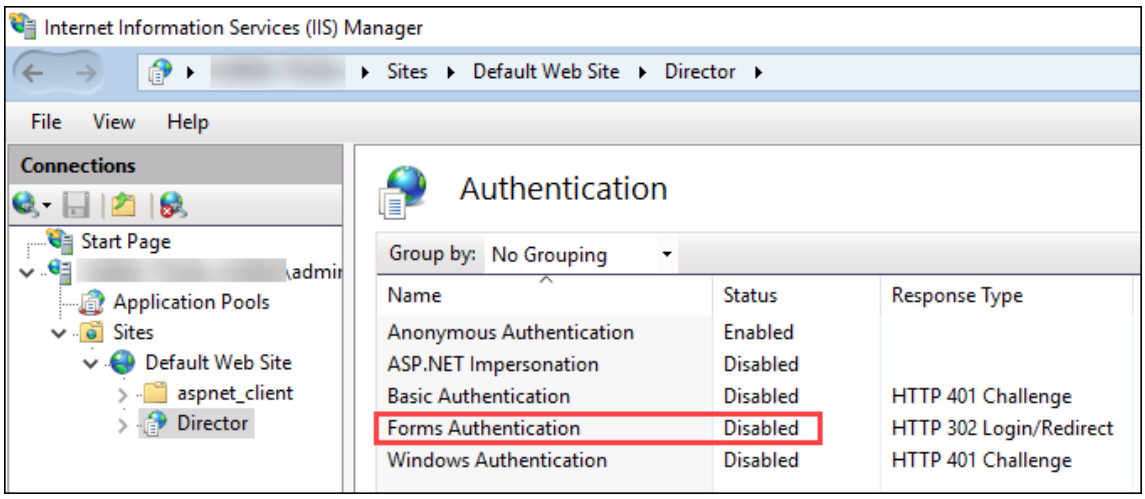
1. 安装和启用客户端证书映射身份验证。请按照 Microsoft 文档 Client Certificate Mapping Authentication（客户端证书映射身份验证）中的 **Client Certificate Mapping authentication using Active Directory**（使用 Active Directory 的客户端证书映射身份验证）。
2. 在 Director 站点上禁用表单身份验证。

   启动 IIS 管理器。

   转至站点 > 默认 **Web** 站点 > **Director**。

   选择身份验证。

   右键单击表单身份验证，然后选择禁用。



3. 将 Director URL 配置为使用更安全的 https 协议（而非 HTTP）进行客户端证书身份验证。

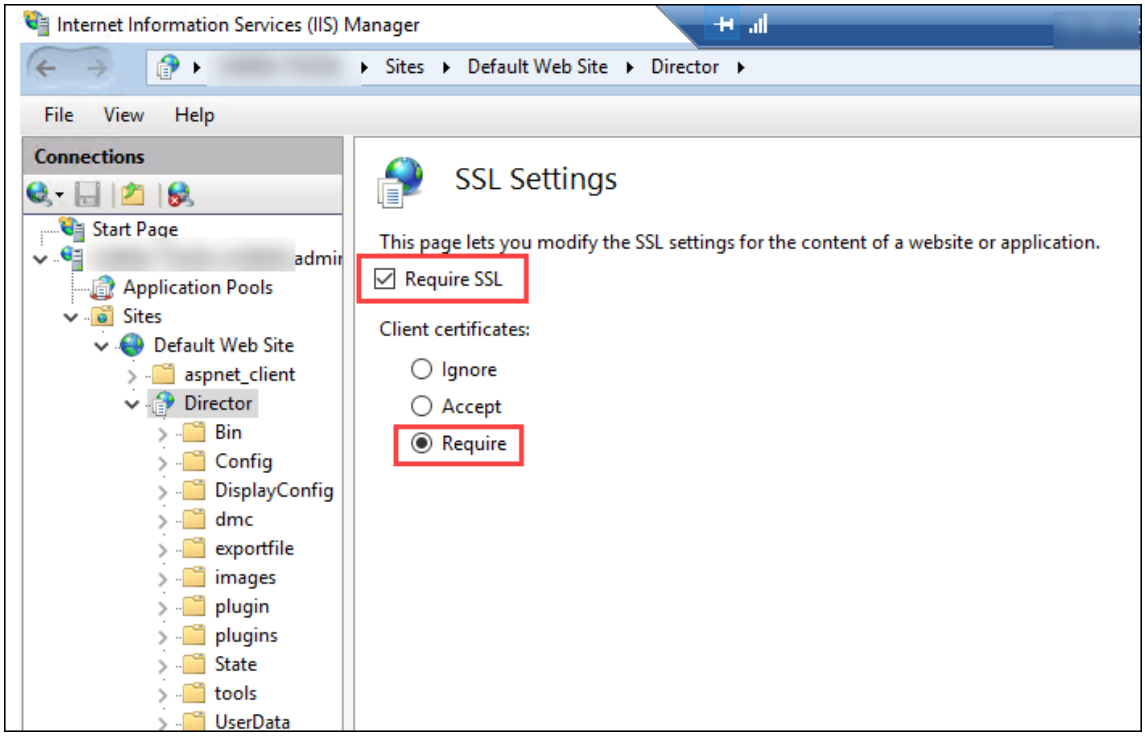
   a) 启动 IIS 管理器。

   b) 转至站点 > 默认 **Web** 站点 > **Director**。

   c) 选择 **SSL** 设置。

   d) 选择需要 **SSL** 和客户端证书 > 需要。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. 更新 web.config。使用文本编辑器打开 web.config 文件（在 c:\inetpub\wwwroot\Director 中提供）。

在 <system.webServer> 父元素下，添加以下代码段作为第一个子元素：

```
<defaultDocument>
   <files>
       <add value="LogOn.aspx"/>
   </files>
</defaultDocument>
```

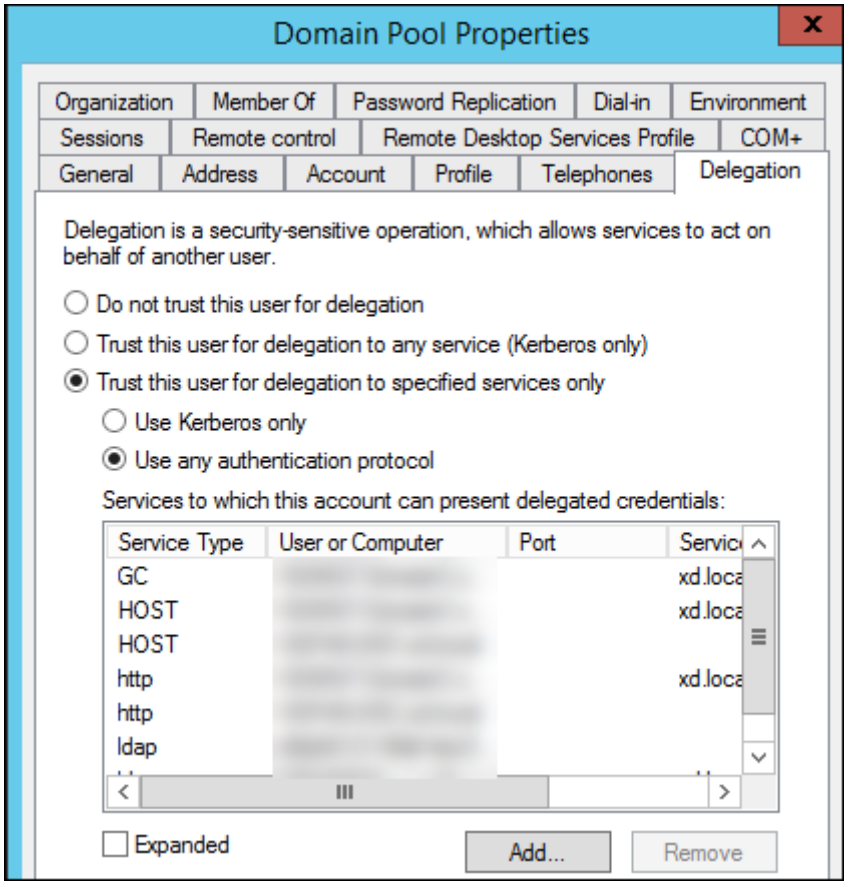
Active Directory 配置

默认情况下，Director 应用程序使用应用程序池标识属性运行。智能卡身份验证要求 Director 应用程序标识必须在服务主机上具有可信计算基 (TCB) 权限的委派。

Citrix 建议您为应用程序池标识创建一个单独的服务帐户。根据 MSDN Microsoft 文章 Protocol Transition with Constrained Delegation Technical Supplement（通过约束委派技术进行的协议转换增补）中的说明创建服务帐户并分配 TCB 权限。

将新创建的服务帐户分配给 Director 应用程序池。下图显示了示例服务帐户 Domain Pool 的属性对话框。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



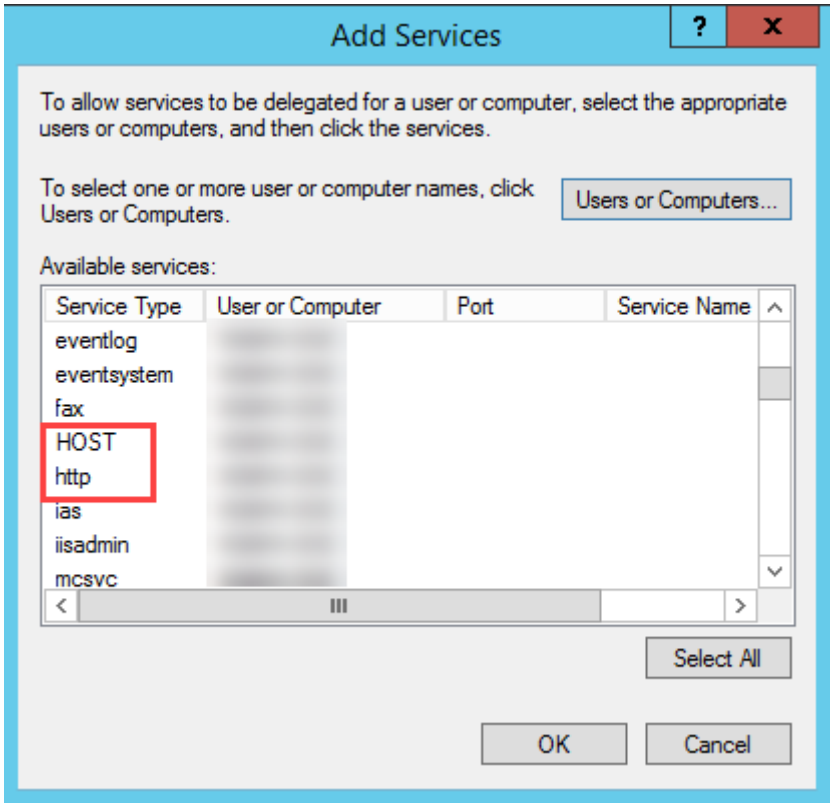
请为此帐户配置以下服务：

- Delivery Controller：HOST、HTTP
- Director：HOST、HTTP
- Active Directory：GC、LDAP

要进行配置，请

1. 在用户帐户属性对话框中，单击添加。
2. 在添加服务对话框中，单击“用户或计算机”。
3. 选择 Delivery Controller 主机名。
4. 从可用服务列表中，选择“HOST”和 HTTP 服务类型。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



同样，请为 **Director** 和 **Active Directory** 主机添加服务类型。

Firefox 浏览器配置

要使用 Firefox 浏览器，请安装 OpenSC 0.17.0 中提供的 PIV 驱动程序。有关安装和配置说明，请参阅 Installing OpenSC PKCS#11 Module in Firefox, Step by Step（在 Firefox 中逐步安装 OpenSC PKCS#11 模块）。
有关在 Director 中使用智能卡身份验证功能的信息，请参阅“Director”一文中的在 Director 中使用基于 PIV 的智能卡身份验证部分。

配置网络分析

April 7, 2023

> 注意：
> 此功能的可用性取决于组织的许可证和管理员权限。

Director 与 Citrix ADM 集成可提供网络分析和性能管理：

- 网络分析使用 Citrix ADM 提供的 HDX Insight 报告来提供网络的应用程序和桌面上下文视图。借助此功能，Director 为您的部署中的 ICA 通信提供高级分析。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 性能管理提供历史保留和趋势报告。通过历史数据保留与实时评估，可以创建趋势报告，其中包括容量趋势和运行状况趋势。

在 Director 中启用此功能后，HDX Insight 报告可为 Director 提供更多信息：

- “趋势”页面中的“网络”选项卡显示对整个部署中的应用程序、桌面和用户产生的延迟和带宽影响。
- 用户详细信息页可以显示特定于某个特殊用户会话的延迟和带宽信息。

限制：

- 在“趋势”视图中，不会针对早于版本 7 的 VDA 收集 HDX 连接登录数据。对于更早版本的 VDA，图表数据将显示为 0。

要启用网络分析，必须在 Director 中安装并配置 Citrix ADM。Director 要求 Citrix ADM 版本 11.1 Build 49.16 或更高版本。MAS 是在 Citrix XenServer 中运行的虚拟设备。通过使用网络分析，Director 可以传送和收集与部署相关的信息。

有关详细信息，请参阅 Citrix ADM 文档。

> 注意：
> Citrix NetScaler Insight Center 已于 2018 年 5 月 15 日结束其维护。请参阅 Citrix Product Matrix（Citrix 产品列表）。将 Director 与 Citrix ADM 集成以进行网络分析。要将 NetScaler Insight Center 迁移至 Citrix ADM，请参阅从 NetScaler Insight Center 迁移至 Citrix ADM。

1. 在安装了 Director 的服务器上，在 C:\inetpub\wwwroot\Director\tools 中找到 DirectorConfig 命令行工具，并在命令提示窗口中使用参数 /confignetscaler 运行该工具。
2. 系统提示时，请输入 Citrix ADM 计算机名称（FQDN 或 IP 地址）、用户名、密码、HTTPS 连接类型（优先级高于 HTTP），然后选择 Citrix ADM 集成。
3. 要验证更改，请先注销，然后再重新登录。

委派管理和 **Director**

January 21, 2022

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，请参阅委派管理一文。

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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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和全局信息。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。可以对单会话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。无法对多会话操作系统计算机使用电源控制选项。
计算机目录管理员	只能访问“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：

- Delivery Controller 登录 Director 的权限 - 至少需要管理员节点中的只读权限
- 用于查看与 Director 中的交付组相关的数据的交付组权限 - 至少需要只读权限

此外，还可以通过复制现有角色创建自定义角色，并包括不同视图的额外权限。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。

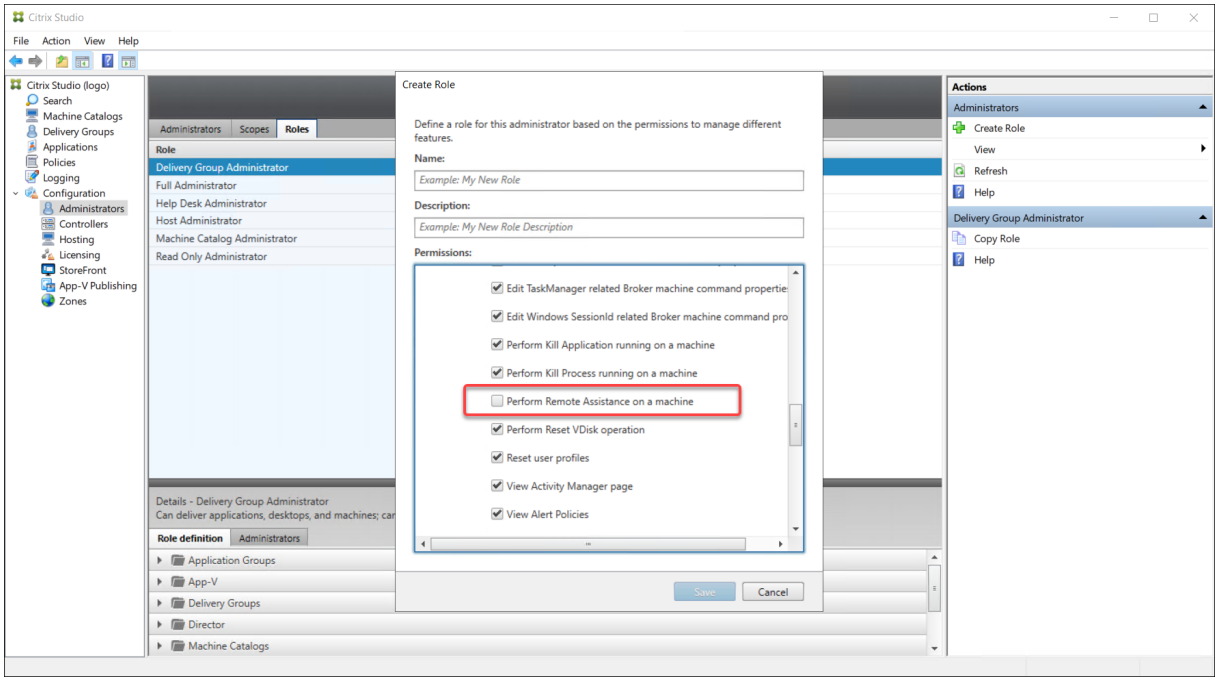
为自定义角色选择 Director 权限，包括：

- 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
- 重置用户配置文件
- 查看“客户端详细信息”页面

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 查看控制板页
- 查看“过滤器”页面
- 查看“计算机详细信息”页面
- 查看“趋势”页面
- 查看“用户详细信息”页面

在此示例中，重影（在计算机上执行远程协助）关闭。



某种权限可以对其他权限具有依赖关系，以在用户界面上变得适用。例如，选择在计算机上执行终止应用程序的操作权限将仅在角色具有权限的面板中启用结束应用程序功能。可以选择以下面板权限：

- 查看“过滤器”页面
- 查看“用户详细信息”页面
- 查看“计算机详细信息”页面
- 查看“客户端详细信息”页面

另外，从其他组件的权限列表中，请考虑选择交付组中的以下权限：

- 使用交付组成员身份启用/禁用计算机的维护模式。
- 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

January 21, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。

配置 Microsoft Internet Information Services (IIS)

可以配置具有受限 IIS 配置的 Director。

文件扩展名

可以不允许使用未列出的文件扩展名。

Director 要求在请求过滤中使用以下文件扩展名：

- .aspx
- .css
- .html
- .js
- .png
- .svc
- .png
- .json
- .woff
- .woff2
- .ttf

Director 要求在请求过滤中使用以下 HTTP 谓词。可以不允许使用未列出的谓词。

- GET
- POST
- HEAD

Director 不需要以下各项：

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

> 重要：
>
> - Director 要求完全信任。请勿将全局.NET 信任级别设置为“高”或更低。
> - Director 维护独立的应用程序池。要修改 Director 的设置，请选择 Director 站点并进行修改。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

配置用户权限

安装 Director 后，将向其应用程序池授予以下权限：

- 作为服务登录登录权限
- 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权限。

所提到的权限和特权是创建应用程序池时的正常安装行为。

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 通信

在生产环境中，请使用 Internet 协议安全性 (IPsec) 或 HTTPS 协议来确保在 Director 与您的服务器之间传输的数据的安全。

IPsec 是 Internet 协议的一组标准扩展，可提供经过身份验证和加密的通信，并且可以实现数据完整性和重播保护功能。由于 IPsec 是一个网络层协议集，因此无需任何修改即可将其用于更高级别的协议。HTTPS 使用传输层安全性 (TLS) 协议提供强大的数据加密。

> 注意：
>
> - Citrix 强烈建议您限制对内联网网络中的 Director 控制台的访问。
> - Citrix 强烈建议您不要在生产环境中启用指向 Director 的不安全连接。
> - 来自 Director 的安全连接需要为每个连接单独配置。
> - 不建议使用 SSL 协议。请改为使用更安全的 TLS 协议。
> - 使用 TLS（而非 IPsec）保护与 Citrix ADC 的通信安全。

要保护 Director 与 Citrix Virtual Apps and Desktops 服务器之间的通信安全（以实现监视和报告功能），请参阅 Data Access Security（数据访问安全性）。

要保护 Director 与 Citrix ADC 之间的通信安全（针对 Citrix Insight），请参阅配置网络分析。

要保护 Director 与许可证服务器之间的通信安全，请参阅保护许可证管理控制台。

Director 安全隔离

可以在与 Director 相同的 Web 域（域名和端口）中部署任何 Web 应用程序。但是，这些 Web 应用程序中的任何安全风险都可能会降低 Director 部署的安全性。如果环境中需要更大程度的安全隔离，Citrix 建议您在单独的 Web 域中部署 Director。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

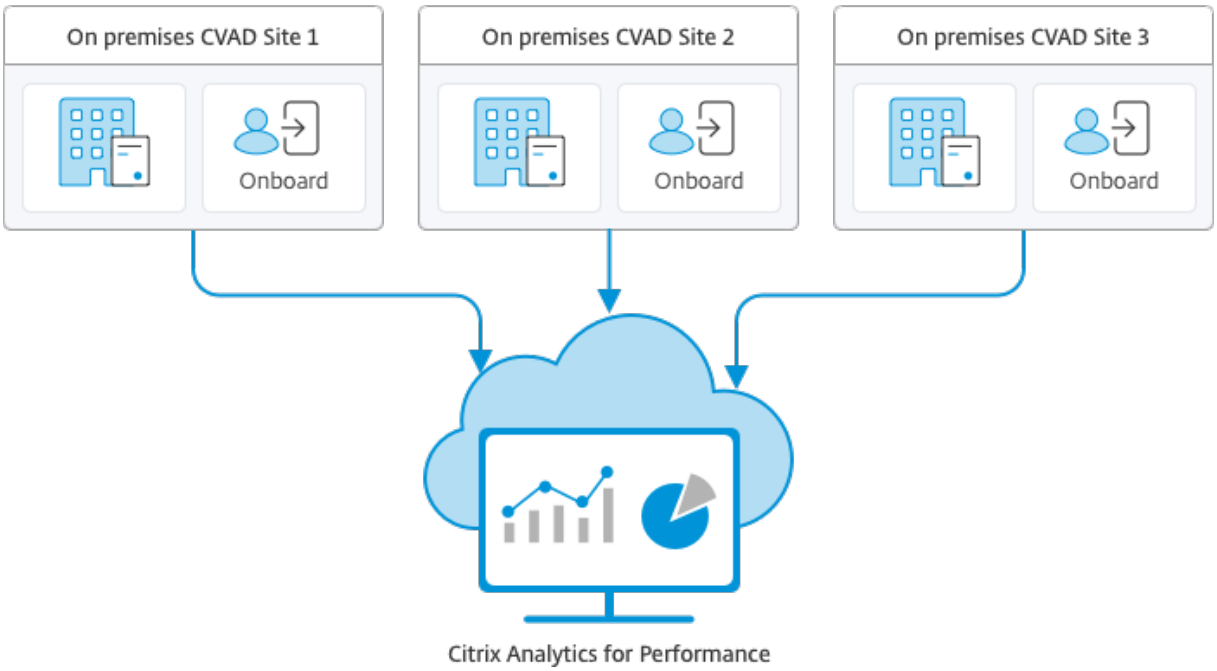
使用 **Citrix Analytics for Performance** 配置本地站点

October 12, 2022

Citrix Analytics for Performance (Performance Analytics) 是 Citrix Analytics Cloud Service 提供的综合性能监视解决方案。Performance Analytics 提供基于性能指标构建的高级见解和分析。Performance Analytics 可帮助您监视和查看贵组织中的一个或多个 Citrix Virtual Apps and Desktops 站点的使用情况和性能指标。

有关 Performance Analytics 的详细信息，请参阅 Performance Analytics 文章。

可以将性能数据从您的站点发送到 Citrix Cloud 上的 Citrix Analytics for Performance，以利用其高级性能分析功能。要查看和使用 Performance Analytics，必须首先从 **Director** 中的分析选项卡使用 Citrix Analytics for Performance 配置您的本地站点。



Performance Analytics 以安全的方式访问数据，并且不会将数据从 Citrix Cloud 传输到本地环境。

必备条件

无需安装新组件即可从 Director 配置 Citrix Analytics for Performance。确保满足以下要求：

- 您的 Delivery Controller 和 Director 在版本 1909 或更高版本中提供。有关详细信息，请参阅功能兼容性列表。
- 只有完全权限管理员才能访问分析选项卡以执行此配置。
- 为了使 Performance Analytics 能够访问性能指标，所有 Delivery Controlle 和安装了 Director 的计算机上都可以访问出站 Internet。具体而言，确保以下 URL 的可访问性：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Citrix 键注册：https://*.citrixnetworkapi.net/
  - Citrix Cloud：https://*.citrixworkspacesapi.net/
  - Citrix Analytics：https://*.cloud.com/
  - Microsoft Azure：https://*.windows.net/

  如果 Delivery Controller 和 Director 计算机位于 Intranet 中，并且通过代理服务器进行出站 Internet 访问，请确保以下各项：

- 代理服务器必须允许使用上述 URL 列表。
- 在 Director web.config 和 citrix.monitor.exe.config 文件中添加以下配置：

```
<system.net>
    <defaultProxy>
        <proxy  usesystemdefault = "false"  proxyaddress = "http
            ://<your_proxyserver_address>:80" bypassonlocal = "
            true"  />
    </defaultProxy>
</system.net>  -  Director web.config 位于安装了 Director 的计算
    机上的 `C:\inetpub\wwwroot\Director\web.config` 下。  -
    citrix.monitor.exe.config 位于安装了 Delivery Controller 的计
    算机上的 `C:\Program Files\Citrix\Monitor\Service\Citrix.
    Monitor.exe.Config` 下。
```

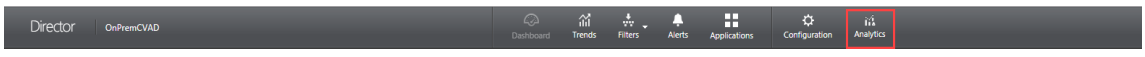
  此设置由 Microsoft 在 IIS 上提供。有关详细信息，请参阅 https://docs.microsoft.com/en-us/dotnet/framework/network-programming/proxy-configuration。
  配置文件中的 **defaultproxy** 字段控制 Director 和 Monitor Service 的出站访问。Performance Analytics 的配置以及与其进行的通信需要将 **defaultproxy** 字段设置为 **true**。实际上，策略可能会将此字段设置为 false。在这种情况下，您必须手动将字段设置为 true。在进行更改之前备份配置文件。重新启动 Delivery Controller 上的监视服务以便影响所做的更改。

- 您拥有 Citrix Analytics for Performance 的活动 Citrix Cloud 授权。
- Citrix Cloud 帐户是具有产品注册体验权限的管理员帐户。有关管理员权限的详细信息，请参阅修改管理员权限。

配置步骤

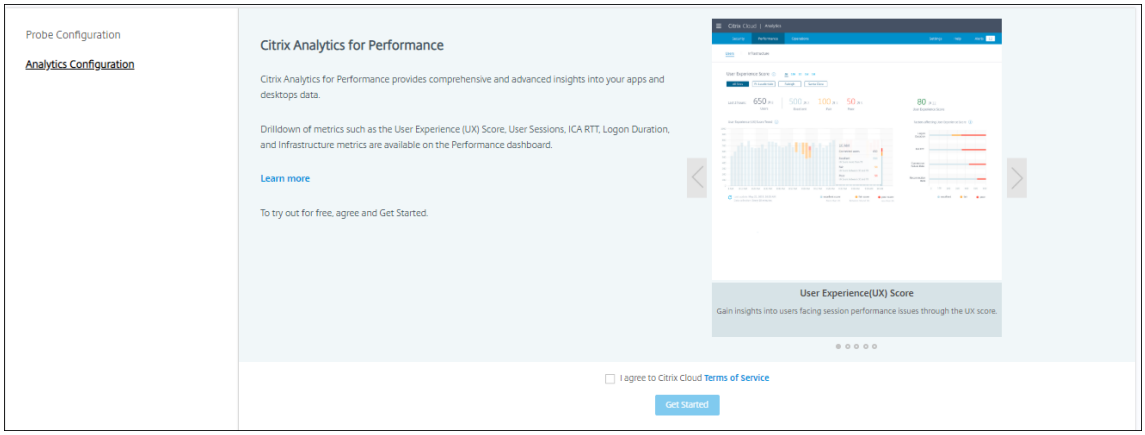
验证必备条件后，请执行以下操作：

1. 以完全权限管理员身份登录 Director，然后选择要使用 Performance Analytics 进行配置的站点。
2. 单击分析选项卡。此时将显示配置页面。

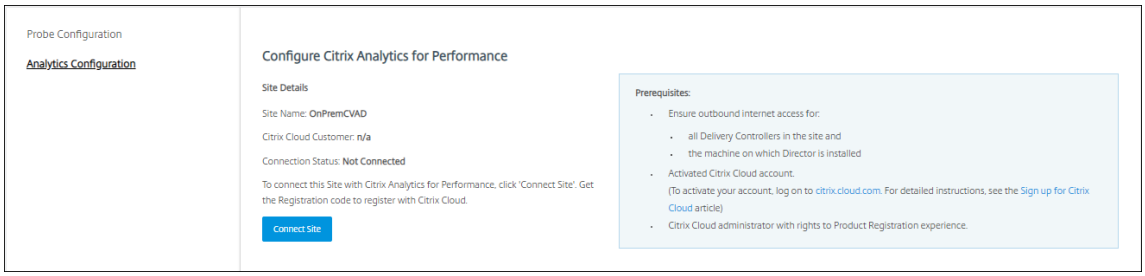


3. 查看步骤，选择服务条款，然后单击开始。

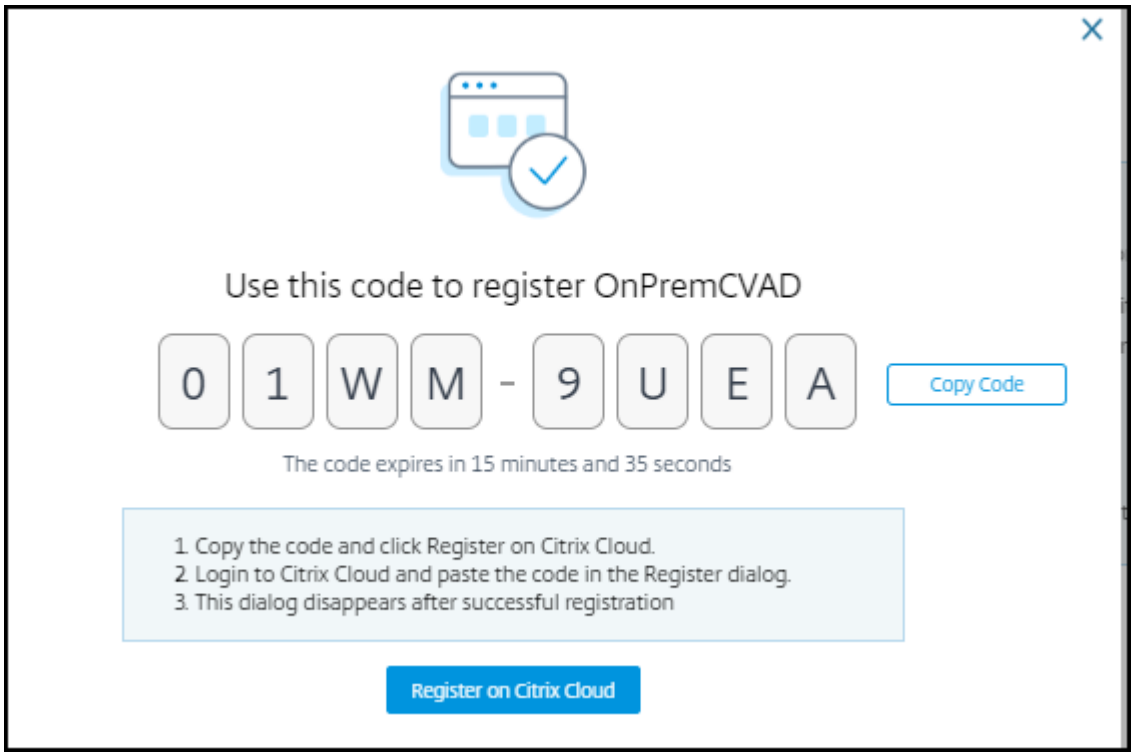
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. 查看必备条件并确保满足这些条件。查看站点详细信息。
5. 单击连接站点以启动配置过程。



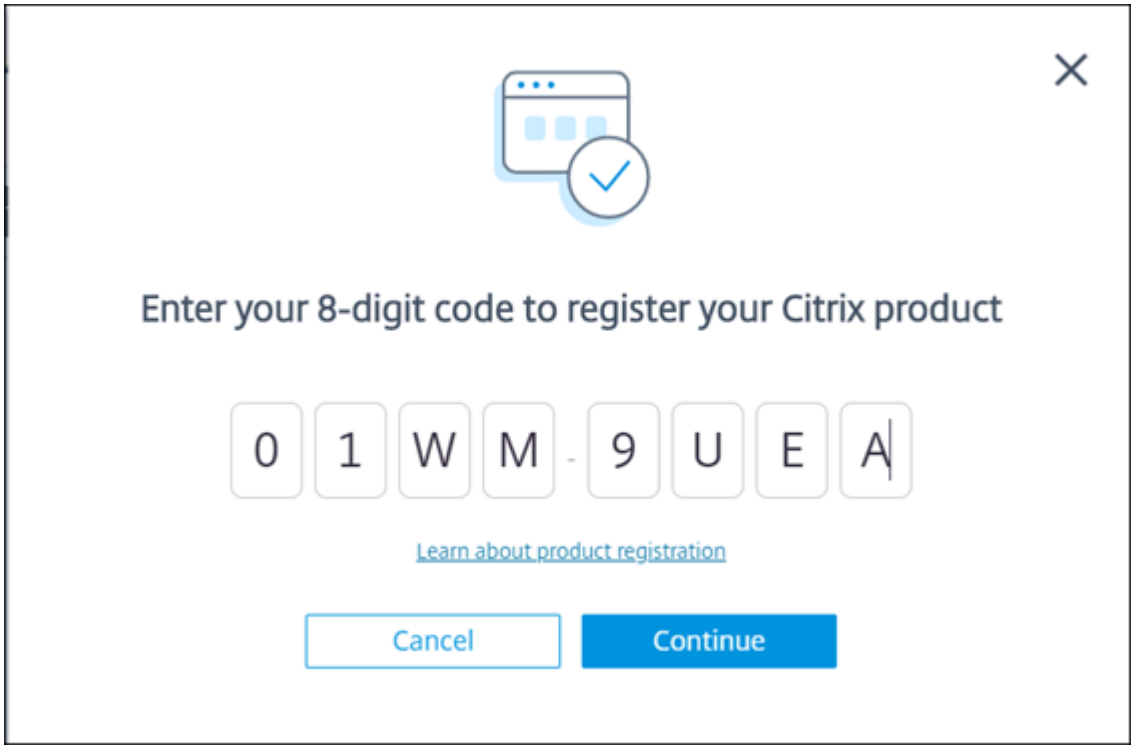
6. 将生成一个唯一的 8 位数注册代码，用于在 Citrix Cloud 中注册此站点。



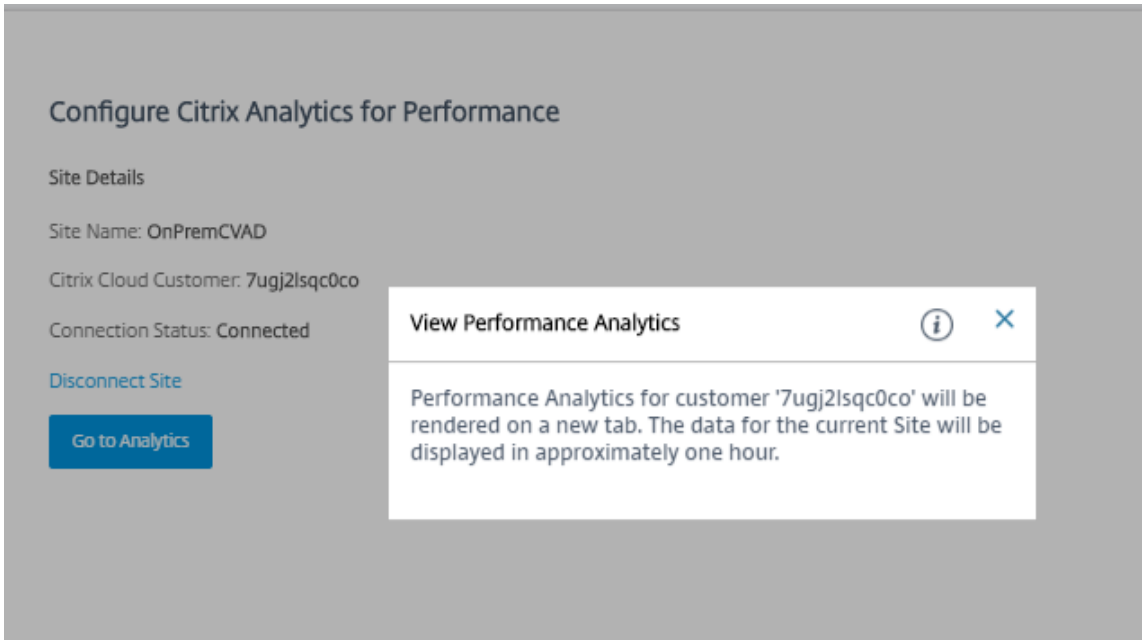
7. 单击复制代码复制代码，然后单击在 **Citrix Cloud** 上注册。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

8. 您将被重定向到 Citrix Cloud 中的注册 URL。使用 Citrix Cloud 凭据登录并选择您的客户。
9. 将复制的注册代码粘贴到 Citrix Cloud 中的“产品注册”页面。单击继续进行注册。查看注册详细信息并单击注册。

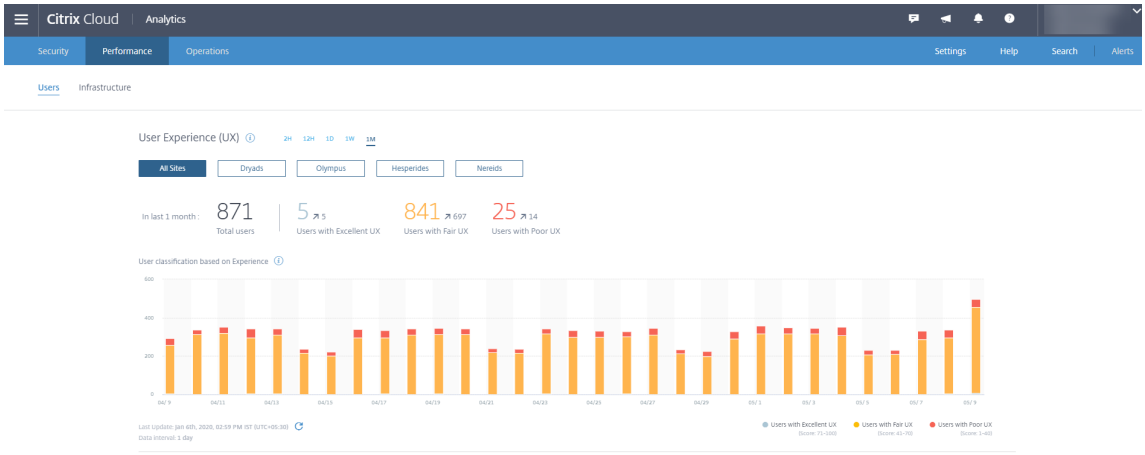


10. 您的本地站点将注册到 Citrix Cloud。现在，在 **Director** 中，单击 **Analytics** 选项卡中的转至 **Analytics**。



11. Performance Analytics 在浏览器的新选项卡中打开。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



如果 Citrix Cloud 会话已过期，您可能会被重定向到 Citrix.com 或 My Citrix 帐户登录页面。

12. 要在 Performance Analytics 中注册多个站点，请从 Director 对每个站点重复上述配置步骤。所有已配置的站点的指标都显示在 Performance Analytics 控制板上。

    如果每个站点上运行了多个 Director 实例，请从任意一个 Director 实例进行配置。连接到站点的所有其他 Director 实例将在配置过程完成后的下次刷新时更新。

13. 要断开站点与 Citrix Cloud 的连接，请单击断开连接站点。此选项将删除现有配置。

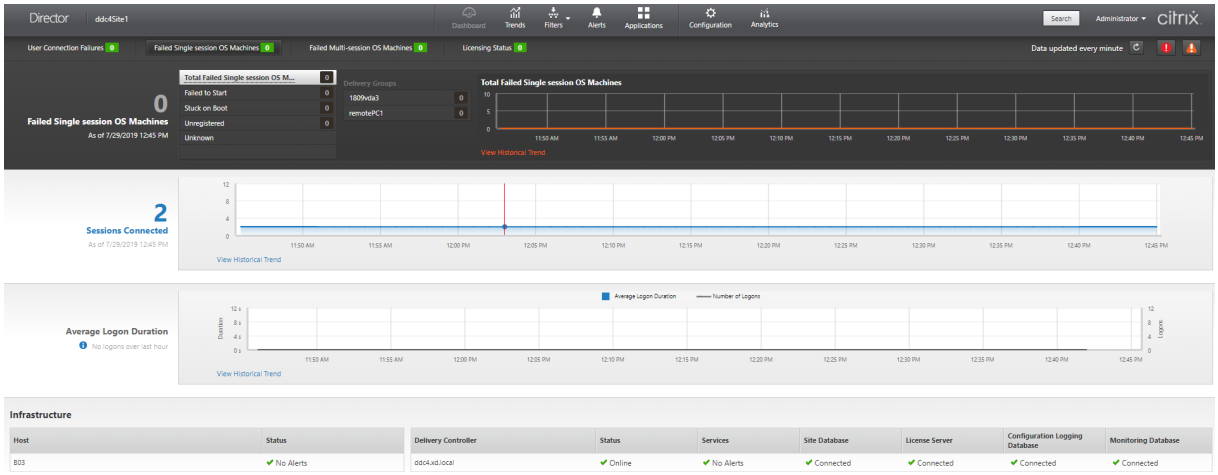
    > 备注：
    >
    > 首次配置站点时，站点中的事件可能需要一段时间（大约一个小时）才能完成处理；导致 Performance Analytics 控制板上的指标显示出现延迟。此后，事件定期刷新。
    >
    > 断开连接后，旧帐户中的数据传输将继续一段时间，直到传输新帐户中的事件。在数据传输停止后大约一小时内，与旧帐户相关的分析仍然显示在 Performance Analytics 控制板上。
    >
    > Citrix Analytics 服务的授权到期后，最多需要一天时间才能停止向 Performance Analytics 发送站点指标。

站点分析

January 21, 2022

如果您具有完全权限管理员权限，在打开 Director 时，控制板将提供一个集中位置来监视站点的运行状况和使用情况。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



如果当前未出现失败情况且在过去 60 分钟内没有出现失败情况，则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。

Director 控制板上的面板

用户连接失败次数

过去 60 分钟内的连接失败次数。单击总数旁的类别可以查看这种失败类型的指标。在相邻的表中，该数量将按交付组进行细分。连接失败包括达到应用程序限制导致的失败。有关应用程序限制的详细信息，请参阅应用程序。

出现故障的单会话操作系统计算机或出现故障的多会话操作系统计算机

按照交付组细分的过去 60 分钟内出现的所有故障。按类型（包括无法启动、引导时卡住以及未注册）细分的故障。对于多会话操作系统计算机，出现故障的计算机还包括达到最大负载的计算机。

许可状态

许可证服务器警报显示许可证服务器发送的警报以及解决警报所需执行的操作。需要许可证服务器 11.12.1 或更高版本。Delivery Controller 警报显示向 Controller 显示的以及 Controller 发送的许可状态的详细信息。需要适用于 XenApp 7.6 或 XenDesktop 7.6 或更高版本的 Controller。可以在 Studio 中设置警报的阈值。在 **Delivery Controller** > 详细信息 > 产品版本 > **PLT** 中显示的许可状态指示 **Premium**，而非 **Platinum**。

宽限期状态

Director 显示以下宽限状态之一。此信息从 Delivery Controller 中提取。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. 不活动：不在任何类型的宽限期内。正常的许可限制适用。
2. 开箱即用宽限期：指向没有许可证的许可证服务器时，新安装后的前 30 天内有 10 个连接。
3. 补充宽限期：使用所有许可证时，将为业务连续性提供 15 天的宽限期，直到添加新许可证或减少使用量。在补充宽限期内允许无限次连接。用户不受影响。在补充宽限期到期或重置之前，无法消除 Director 中显示的警告。
4. 紧急宽限期：当许可证服务器无法访问或在代理连接时无法获取许可证信息时生效。紧急宽限期的有效期为 30 天。用户不受影响。在许可证服务器可访问之前，无法消除 Director 中显示的错误。
5. 宽限期已过期：紧急宽限期或补充宽限期已过期。

有关详细信息，请参阅许可证透支和补充宽限期。

已连接的会话

过去 60 分钟内所有交付组中已连接的会话。

平均登录持续时间

过去 60 分钟的登录数据。左侧的大数值表示该小时内的平均登录持续时间。此平均值中不包括 XenDesktop 7.0 之前版本的 VDA 的登录数据。有关详细信息，请参阅诊断用户登录问题。

基础结构

列出站点的基础结构–主机和 Controller。对于 Citrix Hypervisor 或 VMware 中的基础结构，可以查看性能警报。例如，可以将 XenCenter 配置为在某个托管服务器或虚拟机的 CPU、网络 I/O 或磁盘 I/O 超过特定阈值时生成性能警报。默认情况下，警报重复时间间隔是 60 分钟，但您也可以配置此时间间隔。有关详细信息，请参阅 Citrix Hypervisor 产品文档中的“XenCenter 性能警报”。

> 注意：
>
> 如果未显示某特定指标的图标，则表明您所使用的主机类型不支持该指标。例如，不提供 System Center Virtual Machine Manager (SCVMM) 主机、AWS 和 CloudStack 的运行状况信息。

继续使用以下选项（在以下部分中介绍了这些选项）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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

监视会话

如果会话断开连接，它将继续处于活动状态，其应用程序仍会运行，但用户设备将不再与该服务器通信。

操作	说明
查看用户当前连接的计算机或会话	在“活动管理器”和“用户详细信息”视图中，查看用户当前连接的计算机或会话，以及该用户有权访问的所有计算机和会话的列表。要访问此列表，请单击用户标题栏中的会话切换程序图标。有关详细信息，请参阅还原会话。
查看所有交付组中的已连接会话总数	从控制板的已连接的会话窗格中，查看过去 60 分钟内所有交付组中的已连接会话总数。然后单击较大的总数，以打开“过滤器”视图，您可在其中根据所选交付组以及各个交付组的范围和使用情况显示图形会话数据。
结束空闲会话	“会话过滤器”视图中显示与所有活动会话相关的数据。根据关联用户、交付组、会话状态和大于阈值时间段的空闲时间来过滤会话。从过滤的列表中，选择要注销或断开连接的会话。有关详细信息，请参阅应用程序故障排除。
查看更长时间段内的数据	在“趋势”视图中，选择会话选项卡，深入了解更长时间内已连接和已断开连接的会话的更具体的使用数据（即过去 60 分钟之前的会话总数）。要查看此信息，请单击查看历史趋势。

> 注意：
>
> 如果用户设备运行的是旧版的 Virtual Delivery Agent (VDA)，例如版本 7 以前的 VDA 或 Linux VDA，Director 将无法显示有关会话的完整信息。相反，它会显示指出信息不可用的消息。

桌面分配规则限制：

通过 Citrix Studio，可以将不同用户或用户组的多条桌面分配规则 (DAR) 分配给交付组中的单个 VDA。StoreFront 将根据已登录用户的 DAR 显示已分配的桌面（包含相应的显示名称）。但是，Director 不支持 DAR，而是使用交付组名称显示已分配的桌面，与已登录的用户无关。因此，不能在 Director 中将特定桌面映射到某个计算机。

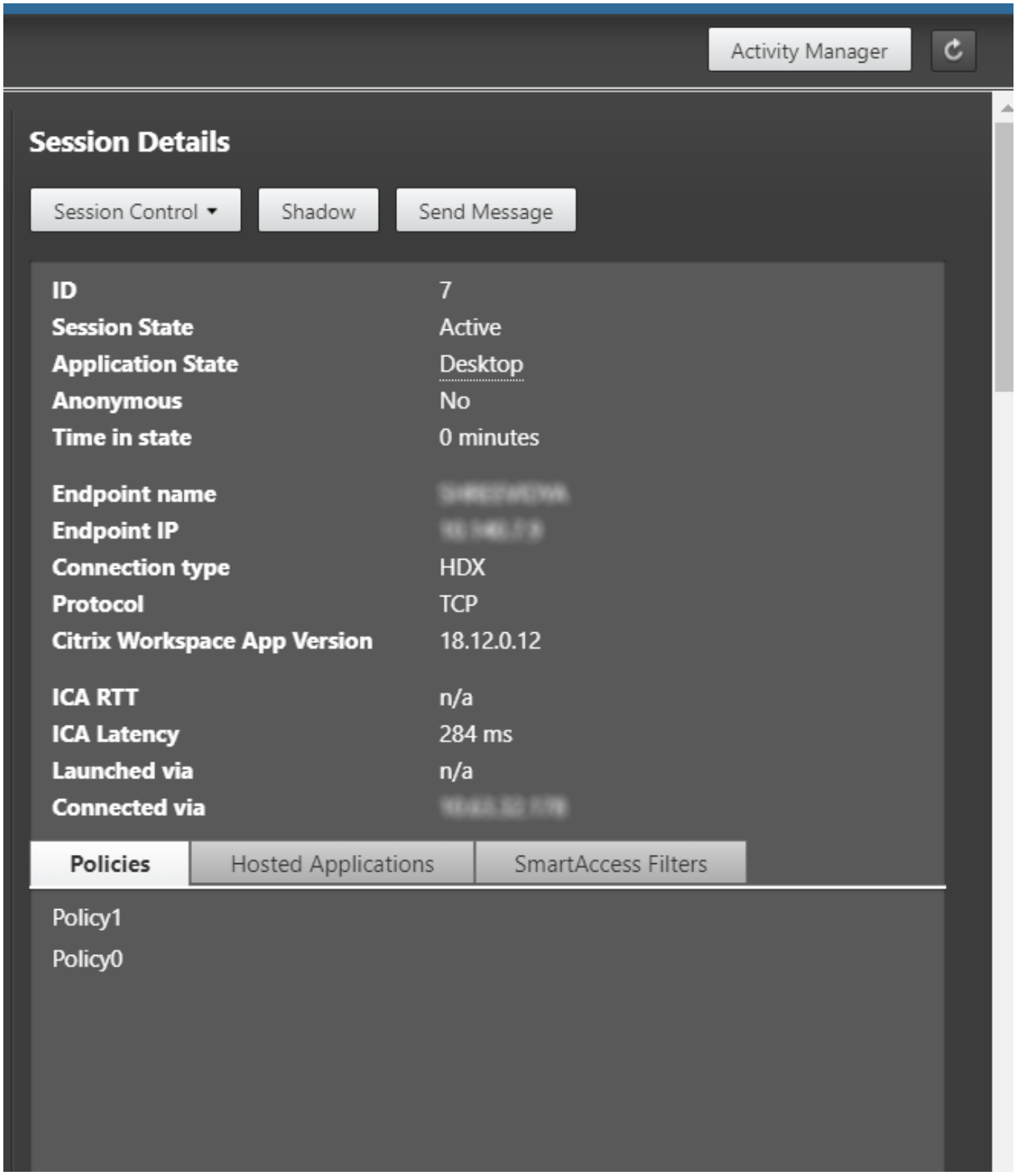
可以使用以下 PowerShell 命令将 StoreFront 中显示的已分配桌面映射到在 Director 中显示的交付组名称：

```
Get-BrokerDesktopGroup | Where-Object {
  \$\_.Uid -eq \(Get-BrokerAssignmentPolicyRule | Where-Object {
  \$\_.PublishedName -eq \"\<Name on StoreFront\>\"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

会话传输协议

在会话详细信息面板中查看用于当前会话的 HDX 连接类型的传输协议。对于在 VDA 7.13 版或更高版本上启动的会话，提供此信息。



- 对于 **HDX** 连接类型：
  - 如果 EDT 用于 HDX 连接，协议显示为 **UDP**。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - 如果 TCP 用于 HDX 连接，协议显示为 **TCP**。

- 对于 **RDP** 连接类型，协议显示为不适用。

配置了自适应传输时，会话传输协议根据网络状况在 EDT（基于 UDP）与 TCP 之间动态切换。如果无法使用 EDT 建立 HDX 会话，则回退到 TCP 协议。

有关自适应传输配置的详细信息，请参阅自适应传输。

导出报告

您可以导出趋势数据以生成常规使用情况和容量管理报告。导出操作支持 PDF、Excel 和 CSV 报告格式。PDF 和 Excel 格式的报告包含以图表和表格表示的趋势。CSV 格式的报告包含表格数据，这种数据可以通过处理生成视图或进行存档。

要导出报告，请执行以下操作：

1. 转至趋势选项卡。
2. 设置过滤条件和时间段并单击应用。趋势图形和表格填充有数据。
3. 单击导出并输入报告的名称和格式。

Director 会根据您选择的过滤条件生成报告。如果更改了过滤条件，请单击应用，然后再单击导出。

> 注意：
>
> 导出大量的数据时，会导致 Director 服务器、Delivery Controller 和 SQL Server 中内存和 CPU 消耗大幅增加。支持的并发导出操作数和可以导出的数据量被设置为默认限制，以实现最佳的导出性能。

支持的导出限制

导出的 PDF 和 Excel 格式的报告包含满足选定过滤条件的完整图表。但是，超出对表格中的行数或记录数设置的默认限制的所有报告格式的表格数据都将被截断。默认的受支持记录数根据报告格式确定。

您可以通过在 Internet Information Services (IIS) 中配置 Director 应用程序设置的方法来更改默认限制。

报告格式	默认的受支持记录数	**Director** 应用程序设置中的字段	最大的受支持记录数
PDF	500	UI.ExportPdfDrilldownLimit	5000
Excel	100000	UI.ExportExcelDrilldownLimit	1000000
CSV	100000（在会话选项卡中为 10000000）	UI.ExportCsvDrilldownLimit	10000000

要更改可以导出的记录数的限制，请执行以下操作：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. 打开 IIS 管理器控制台。
2. 转到默认 Web 站点下的 Director Web 站点。
3. 双击应用程序设置。
4. 根据需要编辑或添加 UI.ExportPdfDrilldownLimit、UI.ExportExcelDrilldownLimit 或 UI.ExportCsvDrilldownLimit 字段的设置。

在“应用程序设置”中添加这些字段值将覆盖默认值。

> 警告：
>
> 如果将字段值设置为高于支持的最大记录数，可能会影响导出性能，因此不建议这样操作。

错误处理

本节介绍有关处理在导出操作过程中可能遇到的错误的信息。

- **Director** 超时

此错误出现的原因可能是网络问题，或者与 Director 服务器或 Monitor Service 的高资源使用率有关。

默认的超时持续时间为 100 秒。要增加 Director Service 的超时持续时间，请在 Internet Information Services (IIS) 的 Director 应用程序设置中，设置 **Connector.DataServiceContext.Timeout** 字段的值：

1. 打开 IIS 管理器控制台。
2. 转到默认 Web 站点下的 Director Web 站点。
3. 双击应用程序设置。
4. 编辑 **Connector.DataServiceContext.Timeout** 的值。

- 显示器超时

此错误出现的原因可能是网络问题，或者与 Monitor Service 或 SQL Server 的高资源使用率有关。

要增加 Monitor Service 的超时持续时间，请在 Delivery Controller 上运行以下 PowerShell 命令：

```
asnp Citrix.*
Get-MonitorConfiguration
Set-MonitorConfiguration -MonitorQueryTimeoutSeconds <timeout value>
```

- 正在进行最大并发导出或预览操作

Director 支持一个导出或预览实例。如果遇到正在进行最大并发导出或预览操作错误，请稍后再尝试下一个导出操作。

虽然可以增加并发导出或预览操作数，但 Director 的性能会受到影响，因此不建议这样做：

1. 打开 IIS 管理器控制台。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. 转到默认 Web 站点下的 Director Web 站点。
3. 双击应用程序设置。
4. 编辑 **UI.ConcurrentExportLimit** 的值。

- **Director** 中的磁盘空间不足

每个导出操作最多需要 Windows Temp 文件夹提供 2 GB 的硬盘空间。清理空间后再尝试导出，或者在 Director 服务器上添加更多的硬盘空间。

监视修补程序

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。

控制用户计算机电源状态

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。这些选项适用于单会话操作系统计算机，但可能不适用于多会话操作系统计算机。

> 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。所有正在运行的进程都将单独停止。
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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

命令	功能
继续	恢复挂起的 VM 并还原其原始运行状态。
启动	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。

阻止与计算机连接

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，指示此桌面不可用。无法进行新连接，直到您禁用维护模式。

应用程序分析

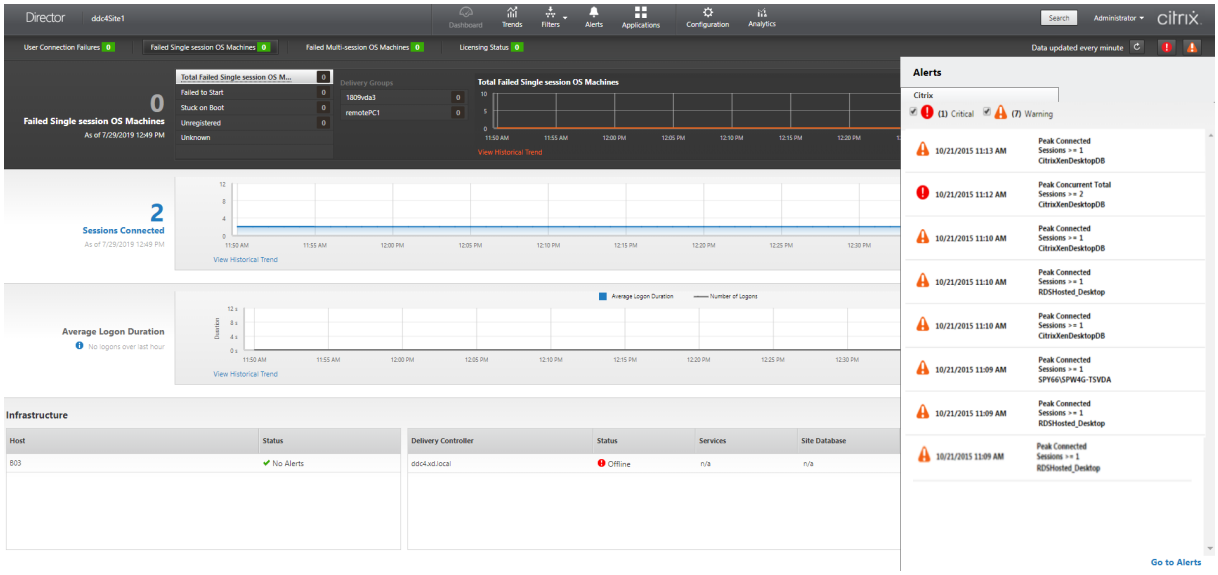
应用程序选项卡中有一个综合视图显示基于应用程序的分析，这些分析有助于高效地分析和管理应用程序性能。您可以获得有关站点上发布的所有应用程序的运行状况和使用情况信息的宝贵洞察数据。它将显示诸如探测结果、每个应用程序的实例数等指标，以及与已发布的应用程序关联的故障和错误。有关详细信息，请参阅对应用程序进行故障排除中的应用程序分析部分。

警报和通知

April 18, 2023

警报在 Director 中的控制板上以及其他高级别视图中显示，带有警告和严重警报符号。警报适用于获得 **Premium** 许可的站点。警报每分钟自动更新一次；也可以根据需要更新警报。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

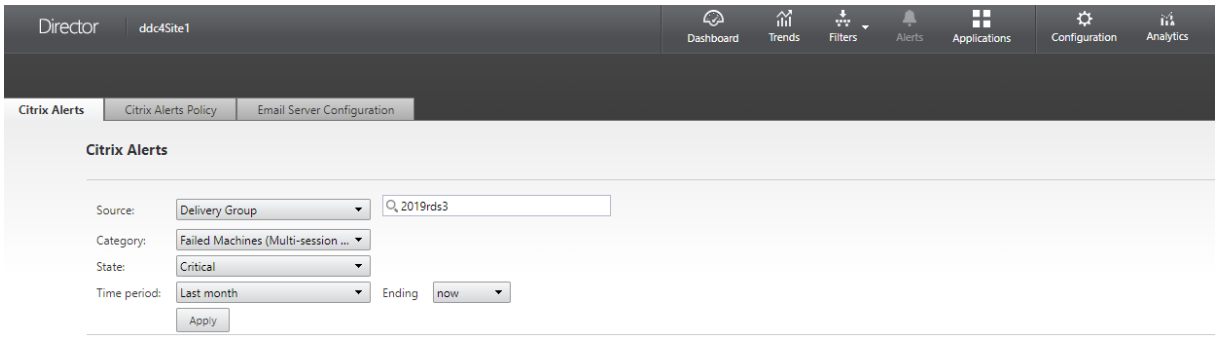


警告警报（琥珀色三角形）指示已达到或超过条件的警告阈值。

严重警报（红色圆形）显示已达到或超过条件的严重阈值。

可以查看警报的更多详细信息，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，上个月中针对特定交付组的出现故障的多会话操作系统计算机，或针对特定用户的所有警报。有关详细信息，请参阅导出报告。



Citrix 警报

Citrix 警报是指在 Director 中监视且源自 Citrix 组件的警报。可以在 Director 内部的警报 > **Citrix** 警报策略中配置 Citrix 警报。作为配置的一部分，可以设置要在警报超出所设置的阈值时通过电子邮件向个人和组发送的通知。有关设置 Citrix 警报的详细信息，请参阅创建警报策略。

> 注意：
>
> 确保您的防火墙、代理或 Microsoft Exchange Server 不会阻止电子邮件警报。

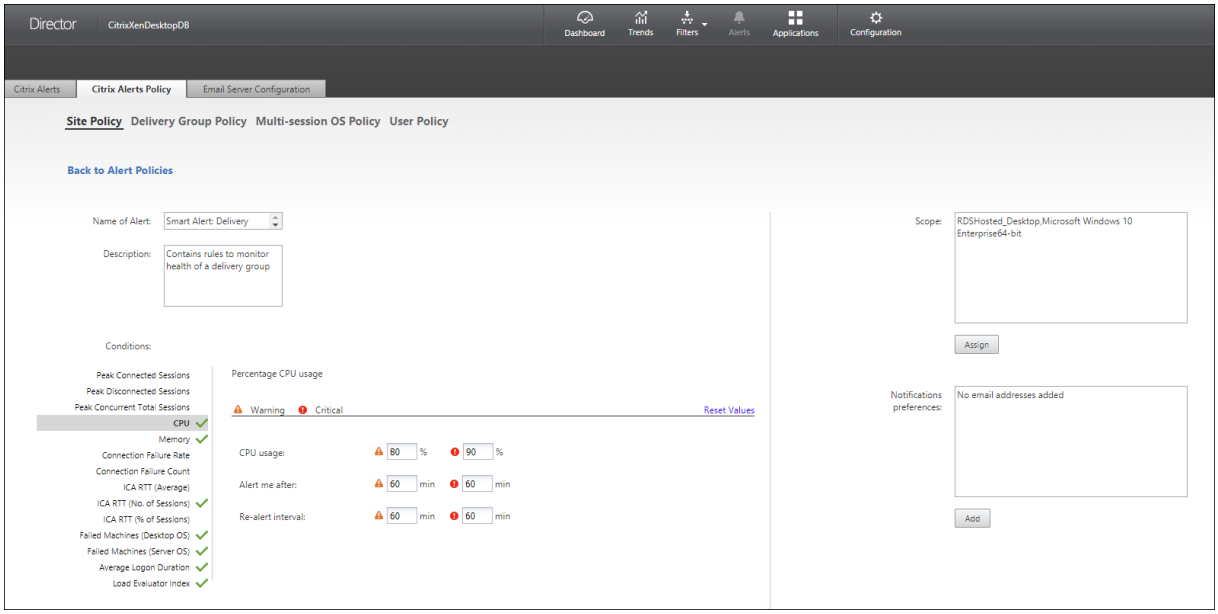
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

智能警报策略

一组具有预定义阈值的内置警报策略适用于交付组和多会话操作系统 VDA 作用域。此功能需要 Delivery Controller 7.18 版或更高版本。可以在警报 > **Citrix** 警报策略中修改内置警报策略的阈值参数。
当在站点中至少定义了一个警报目标（一个交付组或一个多会话操作系统 VDA）时，将创建这些策略。此外，这些内置警报会被自动添加到新的交付组或多会话操作系统 VDA。

升级 Director 以及您的站点时，将执行早期 Director 实例中的警报策略。仅当监视数据库中不存在任何相应的警报规则时，才创建内置警报策略。

有关内置警报策略的阈值，请参阅警报策略条件部分。



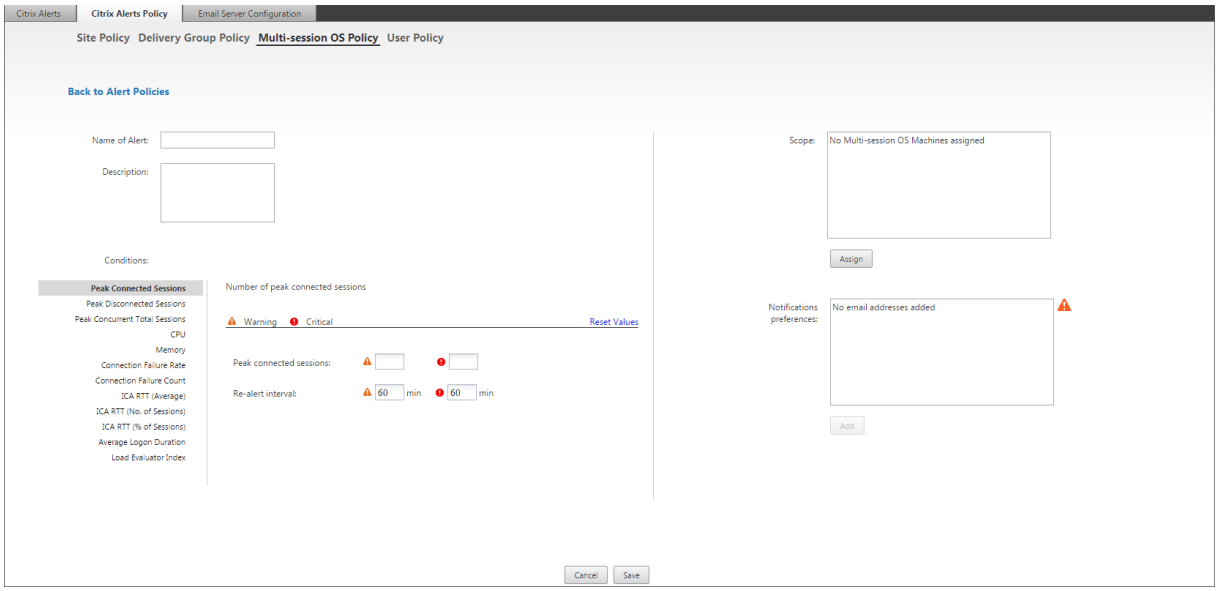
SCOM 警报

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，请参阅配置 SCOM 警报集成部分。

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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

创建警报策略



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，然后选择策略，例如“多会话操作系统策略”。
2. 单击创建。
3. 命名并描述该策略，然后设置触发警报时必须满足的条件。例如，指定“最大已连接会话数”、“最大已断开会话数”和“最大并发会话总数”对应的警告和严重警报数。警告值不得大于严重警报值。有关详细信息，请参阅警报策略条件。
4. 设置重新发出警报的时间间隔。如果仍满足警报的条件，则在达到此时间间隔时会再次出发警报，如果在警报策略中设置了此时间间隔，则会生成电子邮件通知。已消除的警报在达到重新发出警报的时间间隔时不生成电子邮件通知。
5. 设置作用域。例如，为特定交付组进行设置。
6. 在“通知”首选项中，指定触发警报时应通过电子邮件向哪些用户发送通知。必须在电子邮件服务器配置选项卡中指定电子邮件服务器，才能在“警报策略”中设置电子邮件通知首选项。
7. 单击保存。

创建一条包含在作用域中定义的 20 个或更多交付组的策略大约需要 30 秒才能完成配置。此时将显示一个微调器。

如果为最多 20 个不同的交付组创建 50 多个策略（共 1000 个交付组目标），可能会导致响应时间增加（超过 5 秒）。

将包含活动会话的计算机从一个交付组移至另一个交付组可能会触发使用计算机参数定义的错误交付组警报。

警报策略条件

下文介绍了警报类别、用于缓解警报的建议操作以及内置策略条件（如果已定义）。内置警报策略是针对 60 分钟警报和重新警报时间间隔定义的。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

最大已连接会话数

- 查看 Director 的“会话趋势”视图，获取最大已连接会话数。
- 检查以确保容量足以容纳会话负载。
- 根据需要添加新计算机

最大已断开会话数

- 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

- 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

CPU

CPU 使用率百分比指示 VDA 上的整体 CPU 占用量，包括进程的整体 CPU 占用量。可以从相应 VDA 的计算机详细信息页面更加深入地了解各个进程的 CPU 利用率。

- 转至计算机详细信息 **>** 查看历史利用率 **>** 排名前 **10** 的进程，确定占用 CPU 的进程。确保启用进程监视策略以启动进程级别的资源使用情况统计信息的收集。
- 必要时结束进程。
- 结束进程会导致未保存的数据丢失。
- 如果一切均正常工作，请以后再添加其他 CPU 资源。

  > 注意：
  >
  > 在具有 VDA 的计算机上，默认允许使用启用资源监视策略设置，以监视 CPU 和内存性能计数器。如果禁用此策略设置，则不会触发 CPU 和内存状况警报。有关详细信息，请参阅监视策略设置。

  智能策略条件：

  - 作用域：交付组、多会话操作系统作用域
  - 阈值：警告 - 80%、严重 - 90%

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

内存

内存使用率百分比指示 VDA 上的整体内存消耗量，包括进程的整体内存消耗量。可以从相应 VDA 的计算机详细信息页面更加深入地了解各个进程的内存利用率。

- 转至计算机详细信息 **>** 查看历史利用率 **>** 排名前 **10** 的进程，确定占用内存的进程。确保启用进程监视策略以启动进程级别的资源使用情况统计信息的收集。
- 必要时结束进程。
- 结束进程会导致未保存的数据丢失。
- 如果一切均正常工作，请以后再添加其他内存。

  > 注意：
  >
  > 在具有 VDA 的计算机上，默认允许使用启用资源监视策略设置，以监视 CPU 和内存性能计数器。如果禁用此策略设置，则不会触发 CPU 和内存状况警报。有关详细信息，请参阅监视策略设置。

  智能策略条件：

  - 作用域：交付组、多会话操作系统作用域
  - 阈值：警告 - 80%、严重 - 90%

连接失败率

过去一小时内连接失败的百分比。

- 根据失败总次数除以尝试连接的总次数计算得来。
- 检查 Director 的“连接失败趋势”视图，了解配置日志中记录的事件。
- 确定桌面或应用程序是否可访问。

连接失败次数

过去一小时内连接失败的次数。

- 检查 Director 的“连接失败趋势”视图，了解配置日志中记录的事件。
- 确定桌面或应用程序是否可访问。

ICA RTT（平均值）

平均 ICA 往返时间。

- 检查 Citrix ADM 获取 ICA RTT 中的故障信息以确定根本原因。有关详细信息，请参阅 Citrix ADM 文档。
- 如果 Citrix ADM 不可用，请检查“Director 用户详细信息”视图以获取 ICA RTT 和延迟信息，并确定是网络问题还是应用程序或桌面问题。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ICA RTT（会话数）

超过 ICA 往返时间阈值的会话数。

- 检查 Citrix ADM 以获取具有高 ICA RTT 的会话数。有关详细信息，请参阅 Citrix ADM 文档。
- 如果 Citrix ADM 不可用，请与网络团队协作共同确定根本原因。

  智能策略条件：

  - 作用域：交付组、多会话操作系统作用域
  - 阈值：警告 - 300 毫秒（5 个或更多会话）、严重 - 400 毫秒（10 个或更多会话）

ICA RTT（会话百分比）

超过平均 ICA 往返时间的会话百分比。

- 检查 Citrix ADM 以获取具有高 ICA RTT 的会话数。有关详细信息，请参阅 Citrix ADM 文档。
- 如果 Citrix ADM 不可用，请与网络团队协作共同确定根本原因。

ICA RTT（用户）

应用于由指定用户启动的会话的 ICA 往返时间。如果 ICA RTT 高于至少一个会话中的阈值，则会触发该警报。

出现故障的计算机（单会话操作系统）

出现故障的单会话操作系统计算机数。可能会因多种原因而出现故障，如在 Director 的“控制板”和“过滤器”视图中所示。

- 请运行 Citrix Scout 诊断以确定根本原因。有关详细信息，请参阅对用户问题进行故障排除。

  智能策略条件：

  - 作用域：交付组作用域
  - 阈值：警告 - 1、严重 - 2

出现故障的计算机数（多会话操作系统）

出现故障的多会话操作系统计算机数。可能会因多种原因而出现故障，如在 Director 的“控制板”和“过滤器”视图中所示。

- 请运行 Citrix Scout 诊断以确定根本原因。

  智能策略条件：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - 作用域：交付组、多会话操作系统作用域
  - 阈值：警告 - 1、严重 - 2

平均登录持续时间

过去一小时内的平均登录持续时间。

- 查看 Director 的“控制板”，获取与登录持续时间有关的最新指标。大量用户在短时间内登录会延长登录持续时间。
- 请查看登录的基准时间和中断时间，以缩小原因范围。有关详细信息，请参阅诊断用户登录问题

  智能策略条件：

  - 作用域：交付组、多会话操作系统作用域
  - 阈值：警告 - 45 秒、严重 - 60 秒

登录持续时间（用户）

过去一小时内发生的指定用户的登录的登录持续时间。

负载评估器指数

过去 5 分钟内负载评估器指数的值。

- 查看 Director 中可能具有峰值负载（最大负载）的多会话操作系统计算机。查看“控制板”（失败）和“趋势负载评估器指数”报告。

  智能策略条件：

  - 作用域：交付组、多会话操作系统作用域
  - 阈值：警告 - 80%、严重 - 90%

虚拟机管理程序警报监视

Director 会显示警报以监视虚拟机管理程序的运行状况。来自 Citrix Hypervisor 和 VMware vSphere 的警报可以帮助监视虚拟机管理程序参数和状态。还可以监视与虚拟机管理程序的连接状态以在群集或主机池重新启动或不可用时提供警报。

要接收虚拟机管理程序警报，请确保在 Citrix Studio 中创建宿主连接。有关详细信息，请参阅连接和资源。仅监视这些连接以获取虚拟机管理程序警报。下表介绍虚拟机管理程序警报的各种参数和状态。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

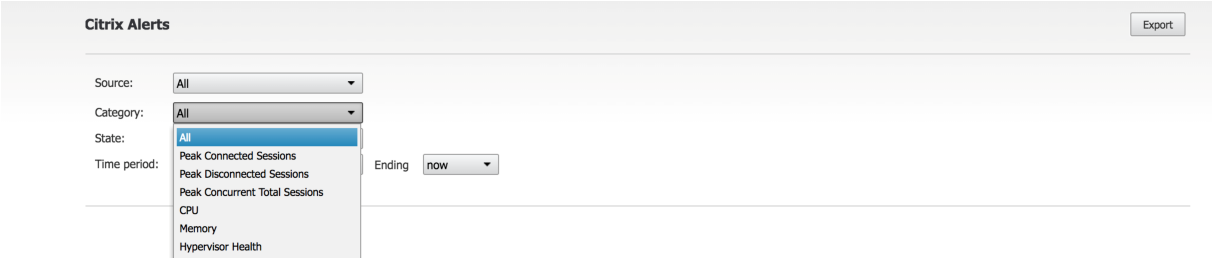
警报	支持的虚拟机管理程序	触发者	条件	配置
CPU 使用率	Citrix Hypervisor、VMware vSphere	虚拟机管理程序	已达到或超过 CPU 使用率警报阈值	必须在虚拟机管理程序中配置警报阈值。
内存使用率	Citrix Hypervisor、VMware vSphere	虚拟机管理程序	已达到或超过内存使用率警报阈值	必须在虚拟机管理程序中配置警报阈值。
网络使用情况	Citrix Hypervisor、VMware vSphere	虚拟机管理程序	已达到或超过网络使用情况警报阈值	必须在虚拟机管理程序中配置警报阈值。
磁盘使用情况	VMware vSphere	虚拟机管理程序	已达到或超过磁盘使用情况警报阈值	必须在虚拟机管理程序中配置警报阈值。
主机连接或电源状态	VMware vSphere	虚拟机管理程序	虚拟机管理程序主机已重新启动或不可用	在 VMware vSphere 中预先生成警报。不需要任何其他配置。
虚拟机管理程序连接不可用	Citrix Hypervisor、VMware vSphere	Delivery Controller	与虚拟机管理程序（池或群集）的连接已断开或已关闭或重新启动。只要连接不可用，就会每小时生成一次该警报。	警报是在 Delivery Controller 中预先生成的。不需要任何其他配置。

> 注意：
>
> 有关配置警报的详细信息，请参阅 Citrix XenCenter 警报或 VMware vCenter 警报。

可以在 **Citrix** 警报策略 **>** 站点策略 **>** 虚拟机管理程序运行状况下配置电子邮件通知首选项。只能从虚拟机管理程序而非从 Director 配置、编辑、禁用或删除虚拟机管理程序警报策略的阈值条件。但是，修改电子邮件首选项和消除警报可以通过在 Director 中完成。

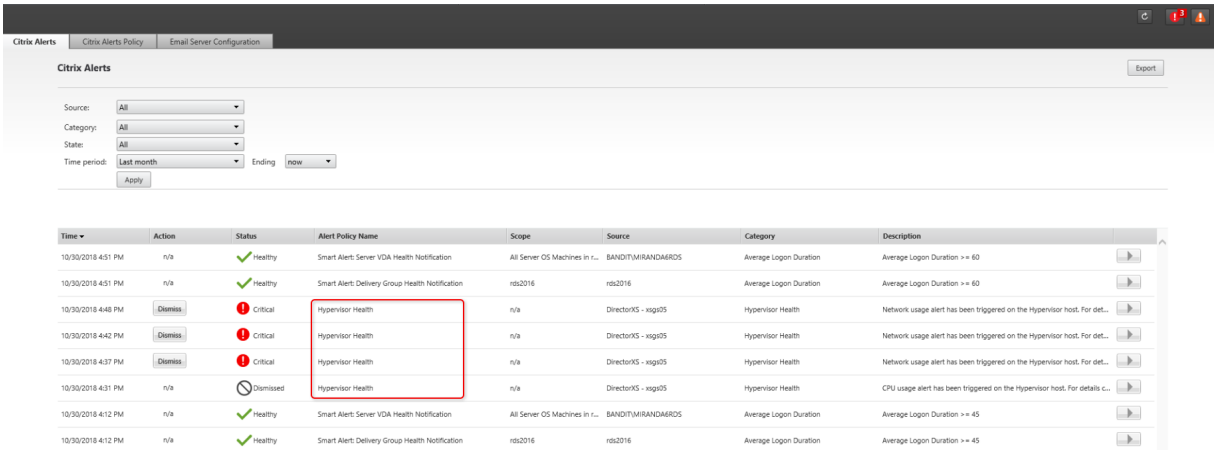
> 重要：
>
> - 由虚拟机管理程序触发的警报将在 Director 中进行提取和显示。但是，对虚拟机管理程序警报的生命周期/状态所做的更改不会反映在 Director 中。
> - 在虚拟机管理程序控制台中处于正常状态或被消除或禁用的警报继续显示在 Director 中且必须显式消除。
> - 在 Director 中被消除的警报不会在虚拟机管理程序控制台中自动消除。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



添加了称为虚拟机管理程序运行状况的新警报类别，以仅过滤虚拟机管理程序警报。达到或超过阈值后，将显示这些警报。虚拟机管理程序警报可以为：

- 临界 - 达到或超过虚拟机管理程序警报策略的临界阈值
- 警告 - 达到或超过虚拟机管理程序警报策略的警告阈值
- 消除 - 不再显示为活动警报的警报



此功能需要 Delivery Controller 版本 7 1811 或更高版本。如果将较早版本的 Director 与站点 7 1811 或更高版本结合使用，则仅显示虚拟机管理程序警报计数。要查看警报，必须升级 Director。

配置 **SCOM** 警报集成

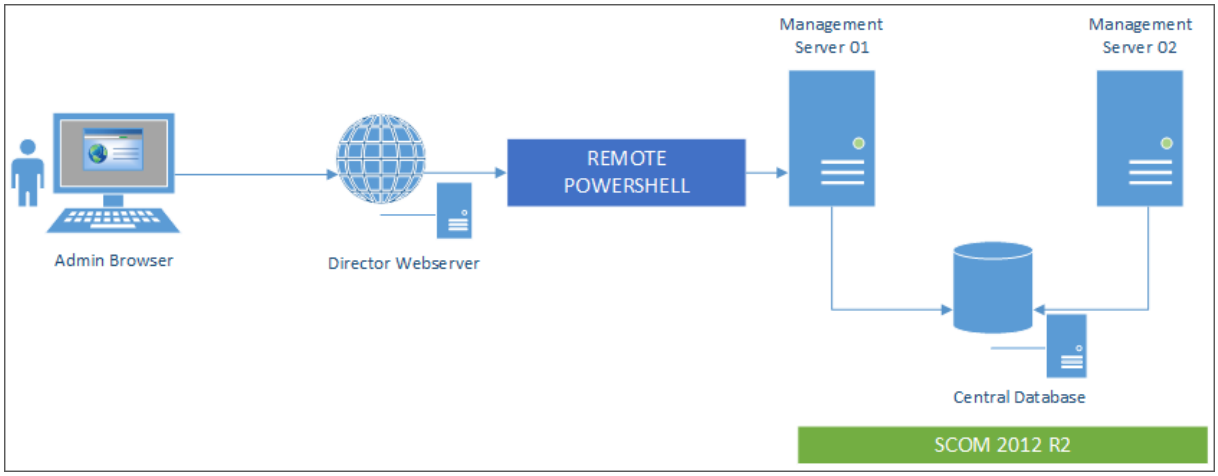
SCOM 与 Director 的集成允许您在 Director 中的“控制板”以及其他高级别视图中查看来自 SCOM 的警报信息。

SCOM 警报与 Citrix 警报一起在屏幕上显示。可以从边栏中的“SCOM”选项卡访问并深入查看 SCOM 警报。

可以查看长达过去一个月内的历史警报、排序、过滤以及将过滤的信息导出为 CSV、Excel 和 PDF 报告格式。有关详细信息，请参阅导出报告。

SCOM 集成使用远程 PowerShell 3.0 或更高版本查询 SCOM 管理服务器中的数据，并维护用户的 Director 会话中的持续型运行空间连接。Director 和 SCOM 服务器必须具有相同的 PowerShell 版本。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



SCOM 集成的要求如下：

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager
- PowerShell 3.0 或更高版本（Director 和 SCOM 服务器上安装的 PowerShell 版本必须一致）
- 四核 CPU，16 GB RAM（建议）
- 必须在 Director web.config 文件中配置 SCOM 的主管理服务器。可以使用 DirectorConfig 工具进行配置。

Citrix 建议将 Director 管理员帐户配置为 SCOM 操作员角色，以便能够在 Director 中检索完整的警报信息。如果不可能，则可以使用 DirectorConfig 工具在 web.config 文件中配置 SCOM 管理员帐户。

Citrix 进一步建议您为每个 SCOM 管理服务器配置的 Director 管理员数量不要超过 10 个以确保性能最佳。

在 Director 服务器上执行以下操作：

1. 键入 **Enable-PSRemoting** 以启用 PowerShell 远程处理。
2. 将 SCOM 管理服务器添加到 TrustedHosts 列表中。打开 PowerShell 提示符并执行以下命令：
   - 获取 TrustedHosts 的当前列表

     Get-Item WSMAN:\localhost\Client\TrustedHosts
   - 将 SCOM 管理服务器的 FQDN 添加到 TrustedHosts 列表中。\< 旧值\> 表示 Get-Item cmdlet 返回的一组现有条目。

     Set-Item WSMAN:\localhost\Client\TrustedHosts -Value “\<FQDN SCOM 管理服务器\>,\< 旧值\>”
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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。有四种类别的 SCOM 操作员角色可用来定义对 SCOM 数据的访问性质。例如，具有只读权限的角色看不到“管理”窗格，无法发现或管理规则、计算机或帐户。操作员角色属于完全权限管理员角色。

> 注意：
>
> 如果将 Director 管理员分配给非操作员角色，以下操作将不可用：
>
> - 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端管理服务器。
> - 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，可以在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<!--NeedCopy-->
```

b) 修改 MaxShellsPerUser：

在 CLI 中：

```
winrm set winrm/config/winrs @{ MaxShellsPerUser="20"} <!--NeedCopy-->
```

在 PS 中：

“‘Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20

```
1.  修改 MaxMemoryPerShellMB：

    在 CLI 中：
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.
```

```
4
5       ```winrm set winrm/config/winrs @{
6    MaxMemoryPerShellMB="1024" }
7    <!--NeedCopy-->
```

```
1  在 PS 中：
```

```
Set-Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 1024<!--
NeedCopy-->
```

5. 要确保 SCOM 集成在混合域环境中运行，请设置以下注册表项。

路径：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

注册表项：LocalAccountTokenFilterPolicy

类型：DWord

值：1

小心：注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

设置 SCOM 集成后，系统可能会显示消息“无法获取最新的 SCOM 警报。有关详细信息，请查看 Director 服务器事件日志。”服务器事件日志将帮助您确定并更正问题。原因可能包括：

- Director 或 SCOM 计算机上的网络连接断开。
- SCOM 服务不可用或太忙，无法响应。
- 由于所配置的用户的权限发生变化，授权失败。
- 处理 SCOM 数据时 Director 中出现错误。
- Director 与 SCOM 服务器之间的 PowerShell 版本不一致。

过滤数据以排除故障

January 21, 2022

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，还可以跨所有交付组创建计算机、连接、会话和应用程序实例的自定义过滤视图。

1. 选择视图：
    - 计算机。选择“单会话操作系统计算机”或“多会话操作系统计算机”。这些视图显示了已配置计算机的数量。“多会话操作系统计算机”选项卡还包括负载评估器指数，如果将鼠标悬停在链接上，则会指示性能计数器的分布情况和会话计数的工具提示。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 会话。还可以从“会话”视图中查看会话计数。空闲时间度量值用于确定空闲时间超过阈值时间段的会话。
- 连接。按不同时间段显示的过滤连接，包括过去 60 分钟、过去 24 小时或过去 7 天。
- 应用程序实例。此视图显示服务器和单会话操作系统的 VDA 上所有应用程序实例的属性。会话空闲时间度量值可用于多会话操作系统的 VDA 上的应用程序实例。

> 注意：
>
> 如果您已在 Windows 10 1809 计算机上安装的 VDA 上启动桌面会话，Director 中的活动管理器有时可能会将 Microsoft Edge 和 Office 显示为主动运行的应用程序，而它们实际上仅在后台运行。

2. 对于过滤依据，请选择条件。
3. 根据需要，对每个视图使用其他选项卡以完成过滤。
4. 根据需要，选择额外的列以执行进一步的故障排除。
5. 保存并命名过滤器。
6. 要从多台 Director 服务器访问过滤器，请将过滤器存储在可从那些服务器访问的共享文件夹中：
   - Director 服务器上的帐户对该共享文件夹必须具有修改权限。
   - 必须对 Director 服务器进行配置以便访问该共享文件夹。要进行配置，请运行 **IIS** 管理器。在 **Sites**（站点）**> Default Web Site**（默认 **Web** 站点）**> Director > Application Settings**（应用程序设置）中，修改 **Service.UserSettingsPath** 设置以反映共享文件夹的 UNC 路径。
7. 以后要打开过滤器，请从过滤器菜单中选择过滤器类型（计算机、会话、连接或应用程序实例），然后选择保存的过滤器。
8. 单击导出将数据导出到 CSV 格式的文件。最多可以导出包含 100000 条记录的数据。此功能在 Delivery Controller 版本 1808 及更高版本中提供。
9. 如果需要，对于计算机视图或连接视图，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。
10. 在计算机视图和连接视图中，单击故障计算机或失败连接的故障原因以获取有关故障的详细说明以及排除故障的建议操作。Citrix Director 7.12 Failure Reasons Troubleshooting Guide（《Citrix Director 7.12 故障原因排除指南》）中提供了计算机故障和连接失败的故障/失败原因和建议的操作。
11. 在计算机视图中，单击计算机名称链接转到相应的计算机详细信息页面。此页面显示计算机的详细信息、提供电源控制、显示 CPU、内存、磁盘监视以及 GPU 监视图。此外，单击查看历史利用率可查看计算机的资源利用率趋势。有关详细信息，请参阅计算机故障排除。
12. 在应用程序实例视图中，可根据大于某个阈值时间段的空闲时间进行排序或过滤。选择要结束的空闲应用程序实例。注销或断开连接应用程序实例会结束在同一会话中的所有活动应用程序实例。有关详细信息，请参阅应用程序故障排除。如果 Director、Delivery Controller 和 VDA 是 7.13 版或更高版本，则提供应用程序实例过滤页面和会话过滤页面上的空闲时间度量值。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
> 通过 Citrix Studio，可以将不同用户或用户组的多条桌面分配规则 (DAR) 分配给交付组中的单个 VDA。StoreFront 将根据已登录用户的 DAR 显示已分配的桌面（包含相应的显示名称）。但是，Director 不支持 DAR，而是使用交付组名称显示已分配的桌面，与已登录的用户无关。因此，不能在 Director 中将特定桌面映射到某个计算机。要将在 StoreFront 中显示的已分配桌面映射到在 Director 中显示的交付组名称，请使用以下 PowerShell 命令：

```
Get-BrokerDesktopGroup | Where-Object {
  $\_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
  $\_.PublishedName -eq "<Name on StoreFront>"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
<!--NeedCopy-->
```

监视站点的历史趋势

January 21, 2022

“趋势”视图可访问每个站点的历史趋势信息以获取以下参数：

- 会话
- 连接失败
- 计算机故障
- 登录性能
- 负载评估
- 容量管理
- 计算机使用情况
- 资源利用率
- 每个站点的网络分析。

要查找此信息，请单击趋势菜单。

借助放大逐级浏览功能，您可以通过放大时间段（单击图中的数据点）和逐级浏览来导航浏览趋势图，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哪些人员或哪些方面。

要更改每个图形的默认作用域，请对数据应用其他过滤器。

选择需要历史趋势信息的时间段。时间段可用性取决于您的 Director 部署，如下所示：

- 在获得 Premium 许可的站点中，最多可以提供去年（365 天）的趋势报告。
- 在获得 Advanced 许可的站点中，最多可以提供上个月（31 天）的趋势报告。
- 在未获得 Premium 许可和未获得 Advanced 许可的站点中，最多可以提供过去 7 天的趋势报告。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> - 在所有 Director 部署中，时间段设置为“上个月”（截至目前）或更短的时间时，会话、故障和登录性能趋势信息以图形和表格的形式提供。选择时间段“上个月”（带有自定义结束日期）或“去年”时，趋势信息将以图形的形式提供，而不是表格。
> - Monitor Service 的整理保留期限值控制趋势数据的可用性。数据粒度和保留中提供了默认值。获得 Premium 许可的站点上的客户可以将整理保留期限更改为他们所需的保留天数。
> - IIS 管理器中的以下参数控制可供选择的自定义结束日期的范围，并且可以自定义。但是，选定日期的数据可用性取决于要衡量的特定指标的整理保留期限设置。

参数	默认值
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

可用趋势

查看会话的趋势：在会话选项卡中，选择交付组和时间段以查看有关并发会话计数的更多详细信息。

会话自动重新连接列显示会话中自动重新连接的数量。会话可靠性或客户端自动重新连接策略生效时，将启用“自动重新连接”。端点上出现网络中断时，以下策略将生效：

- 会话可靠性生效（默认 3 分钟），其中 Citrix Receiver 或 Citrix Workspace 应用程序尝试连接到 VDA。
- “客户端自动重新连接”在客户端尝试连接到 VDA 的 3 到 5 分钟之间生效。

这两个重新连接操作将被捕获并显示给用户。重新连接发生后，此信息最多需要 5 分钟才能显示在 Director UI 上。

自动重新连接信息可帮助您查看网络连接中断并对其进行故障排除，还可分析具有无缝体验的网络。您可以查看过滤器中选定的特定交付组或时间段的重新连接数。深入分析提供了安装 Workspace 应用程序的计算机的会话可靠性或客户端自动重新连接、时间戳、端点 IP 和端点名称等附加信息。

默认情况下，日志按事件时间戳降序排序。此功能适用于 Windows 的 Citrix Workspace 应用程序、适用于 Mac 的 Citrix Workspace 应用程序、Citrix Receiverfor Windows 和 Citrix Receiver for Mac。此功能需要 Delivery Controller 版本 7 1906 或更高版本以及 VDA 1906 或更高版本。

有关会话重新连接的详细信息，请参阅会话。

有关策略的详细信息，请参阅客户端自动重新连接策略设置和会话可靠性策略设置。

有时，由于以下原因，自动重新连接数据可能不会显示在 Director 中：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Workspace 应用程序不向 VDA 发送自动重新连接数据。
- VDA 不向监视服务发送数据。
- Delivery Controller 丢弃 VDA 负载，因为它们可能没有相应的会话。

> 注意：
>
> 有时，如果设置了某些 Citrix Gateway 策略，可能无法正确获取客户端 IP 地址。

查看连接失败的趋势：在“故障”选项卡中，选择连接、计算机类型、故障类型、交付组和时间段，以查看包含有关站点中用户连接失败的更多详细信息的图形。

查看计算机故障的趋势：在单会话操作系统计算机故障选项卡或“多会话操作系统计算机”选项卡中，选择故障类型、交付组和时间段，以查看包含有关站点中计算机故障的更多详细信息的图形。

查看登录性能的趋势：在登录性能选项卡中，选择交付组和时间段，以查看包含有关站点中用户登录次数的持续时间以及登录次数是否影响性能的更多详细信息的图形。此视图还显示各个登录时期的平均持续时间，例如代理持续时间和 VM 启动时间。
此数据专用于用户登录，不包括尝试从已断开连接的会话重新连接的用户。
图形下面的表格显示了按用户会话列出的登录持续时间。您可以选择要显示的列，并按任何列对报告进行排序。
有关详细信息，请参阅诊断用户登录问题

查看负载评估的趋势：在负载评估器指数选项卡中，查看包含有关在多会话操作系统计算机之间分布的负载的更多详细信息的图形。此图形的筛选器选项包括交付组或交付组中的多会话操作系统计算机、多会话操作系统计算机（仅在选择了交付组中的多会话操作系统计算机时可用）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。
在容量管理选项卡中，选择托管应用程序使用情况选项卡，选择“交付组”和时间段，以查看显示一个最大并发使用情况的图形和一个显示基于应用程序的使用情况的表格。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。

查看单会话和多会话操作系统使用情况：“趋势”视图按站点和交付组显示单会话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多会话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，选择单会话操作系统计算机或“多会话操作系统计算机”以获取 VM 使用情况的实时视图，以便能够快速评估您的站点的容量需求。
单会话操作系统可用性 - 根据可用性显示整个站点或特定交付组的单会话操作系统计算机 (VDI) 的当前状态。
多会话操作系统可用性 - 根据可用性显示整个站点或特定交付组的多会话操作系统计算机的当前状态。

> 注意：
> “可用计数器”中显示的计算机数包括处于维护模式的计算机。

查看资源利用率：在资源利用率选项卡中，选择单会话操作系统计算机或多会话操作系统计算机以获取有关每个 VDI 计算机的 CPU 和内存使用情况以及 IOPS 和磁盘延迟的历史趋势数据分析，从而更好地实现容量规划。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

此功能需要 Delivery Controller 和 VDA **7.11** 或更高版本。
图形会显示平均 CPU、平均内存、平均 IOPS、磁盘延迟和峰值并发会话的数据。您可以深入了解计算机，查看 CPU 占用排名前 10 的进程的数据和图表。可按交付组和时间段过滤。提供过去 2 小时、24 小时、7 天、上个月和上一年的 CPU、内存使用情况和峰值并发会话图形。提供过去 24 小时、上个月和上一年的平均 IOPS 和磁盘延迟图形。

> 注意：
>
> - 必须将监视策略设置启用进程监视设置为允许以在“历史计算机利用率”页面上“排名前 10 的进程”表中收集并显示数据。默认情况下，该策略设置为禁止。默认情况下会收集所有资源利用率数据。可以使用启用资源监视策略设置禁用此设置。图形下方的表格显示每台计算机的资源利用率数据。有关详细信息，请参阅监视策略设置。
> - 平均 IOPS 显示的是每日平均值。峰值 IOPS 的计算方式为取选定时间范围的 IOPS 平均值的最高值。(IOPS 平均值是在 VDA 上一个小时中收集的每小时 IOPS 平均值。)

查看网络分析数据：此功能的可用性取决于组织的许可证和管理员权限。此功能需要 Delivery Controller **7.11** 或更高版本。

在网络选项卡中，监视您的网络分析，其中提供网络的用户、应用程序和桌面上下文视图。利用此功能，Director 通过 Citrix ADM 中的 HDX Insight 报告为您的部署中的 ICA 通信提供高级分析。有关详细信息，请参阅配置网络分析。

查看应用程序故障：应用程序故障选项卡会显示与 VDA 上已发布的应用程序关联的故障。

此功能需要 Delivery Controller 和 VDA **7.15** 或更高版本。支持运行 Windows Vista 及更高版本的单会话操作系统 VDA 以及运行 Windows Server 2008 及更高版本的多会话操作系统 VDA。
有关详细信息，请参阅历史应用程序故障监视。

默认情况下，仅显示来自多会话操作系统 VDA 的应用程序故障。可以使用“监视”策略设置应用程序故障的监视。有关详细信息，请参阅监视策略设置。

查看应用程序探测结果：“应用程序探测结果”选项卡显示已在“配置”页面中为探测配置的应用程序的探测结果。在此将记录发生应用程序启动失败过程中的启动阶段。

此功能需要 Delivery Controller 和 VDA **7.18** 或更高版本。有关详细信息，请参阅应用程序探测。

创建自定义报告：“自定义报告”选项卡中提供一个用户界面，用于以表格形式生成包含来自监视数据库的实时数据和历史数据的自定义报告。

此功能需要 Delivery Controller **7.12** 或更高版本。

从以前保存的自定义报告查询列表中，可以单击运行并下载来导出 CSV 格式的报告、单击复制 **OData** 来复制和共享对应的 OData 查询，或单击编辑来编辑查询。
可以根据计算机、连接、会话或应用程序实例创建新的自定义报告查询。根据字段（例如，计算机、交付组或时间段）指定过滤条件。指定您的自定义报告中所需的其他列。预览显示报告数据示例。保存自定义报告查询会将其添加到保存的查询列表中。

可以根据复制的 OData 查询创建新的自定义报告查询。为此，请选择 OData 查询选项，并粘贴复制的 OData 查询。可以保存结果查询供以后执行。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
> 使用 OData 查询生成的“Preview and Export”（预览和导出）报告中的列名未本地化，而是以英语显示。

图表上的旗帜图标表示此特定时间范围内的重要事件或操作。将鼠标悬停在旗帜上并单击时，可列出事件或操作。

> 注意：
>
> - 对于版本 7 之前的 VDA 版本，不会收集 HDX 连接登录数据。对于更早版本的 VDA，图表数据将显示为 0。
> - 可以在 Director 的“趋势”过滤器中选择在 Citrix Studio 中删除的交付组，直至清除与其相关的数据。选择已删除的交付组将显示未保留的可用数据的图表。但是，这些表格不显示数据。
> - 将包含活动会话的计算机从一个交付组移至另一个交付组会导致新交付组的资源利用率和负载评估器指数表格显示从新交付组和旧交付组合并的指标。

部署故障排除

November 17, 2021

作为技术支持管理员，您可以搜索报告问题的用户并显示与该用户关联的会话或应用程序的详细信息。同样，可以搜索被报告出现问题的计算机或端点。可以通过监视相关指标并执行合适的操作快速解决问题。

可用操作包括：

- 结束无响应的应用程序或进程
- 重影用户计算机上的操作
- 注销无响应的会话
- 重新启动计算机
- 将计算机置于维护模式
- 重置用户配置文件

应用程序故障排除

January 21, 2022

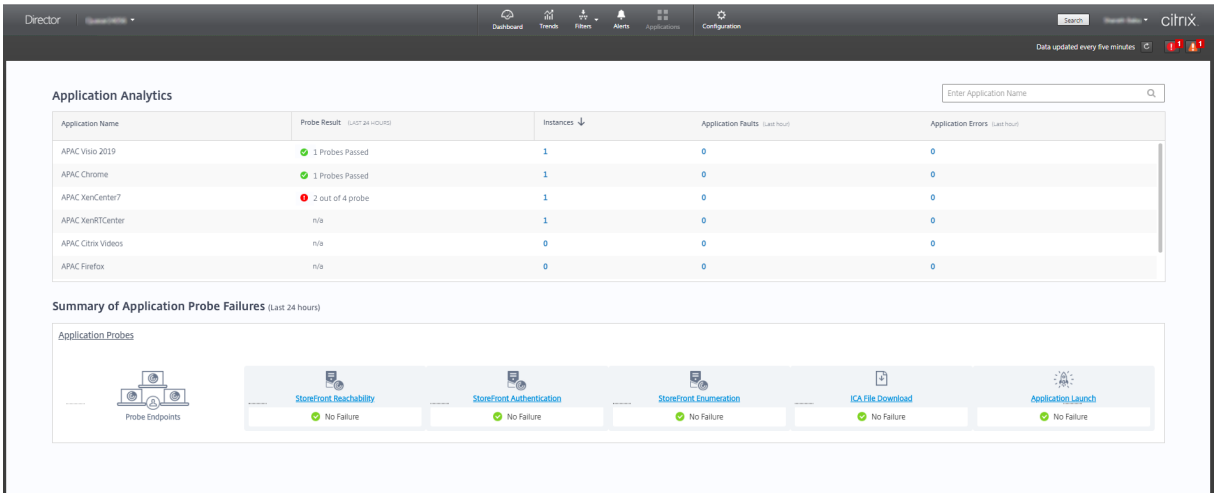
应用程序分析

应用程序视图中有一个综合视图显示基于应用程序的分析，这些分析有助于高效地分析和管理应用程序性能。您可以获得有关站点上发布的所有应用程序的运行状况和使用情况信息的宝贵洞察数据。默认视图有助于识别排在前面的运行的

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

应用程序。

此功能需要 Delivery Controller 7.16 或更高版本和 VDA 7.15 或更高版本。



探测结果列显示过去 24 小时内运行的应用程序探测的结果。单击探测结果链接可在趋势 > 应用程序探测结果页面中查看更多详细信息。有关如何配置应用程序探测的更多详细信息，请参阅应用程序探测。

实例列显示应用程序的使用情况。它指示当前正在运行的应用程序实例数（包括连接的实例和断开连接的实例）。要进一步进行故障排除，请单击实例字段以查看相应的应用程序实例过滤器页面。在此，可以选择要注销或断开连接的应用程序实例。

> 注意：
>
> 对于自定义作用域管理员，Director 不显示在应用程序组下创建的应用程序实例。您必须是完全权限管理员，才能查看所有应用程序实例。有关详细信息，请参阅知识中心文章 CTX256001。

可通过应用程序故障和应用程序错误列来监视站点中已发布的应用程序的运行状况。这些列显示在过去一小时内启动相应应用程序时发生的故障和错误总数。单击应用程序故障或应用程序错误字段以在趋势 > 应用程序故障页面上查看与选定应用程序对应的故障详细信息。

应用程序失败策略设置控制故障和错误的可用性和显示。有关策略及如何修改它们的详细信息，请参阅监视策略设置中的应用程序故障监视策略。

实时应用程序监视

可以使用空闲时间指标对应用程序和会话进行故障排除以确定空闲时间超过特定时间限制的实例。

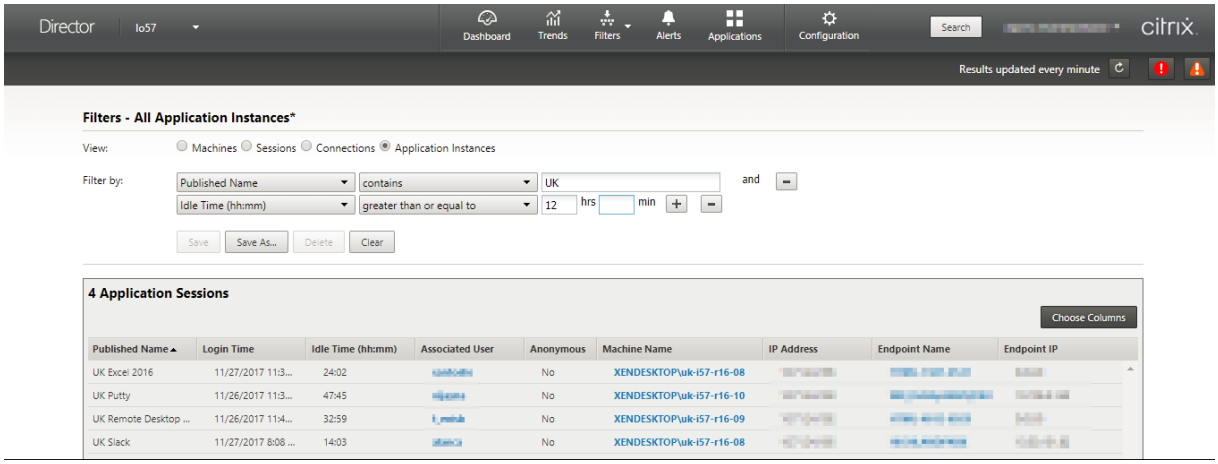
基于应用程序的故障排除的典型用例是在卫生保健部门，在此部门中，员工将共享应用程序许可证。在此部门中，必须结束空闲会话和应用程序实例才能清除 Citrix Virtual Apps and Desktops 环境、重新配置性能较差的服务器或者维护和升级应用程序。

应用程序实例过滤器页面将列出服务器和单会话操作系统的 VDA 上的所有应用程序实例。对于已至少空闲 10 分钟且在多会话操作系统的 VDA 上的应用程序实例，系统将显示关联的空闲时间度量值。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 所有许可证版本的站点上都提供应用程序实例指标。

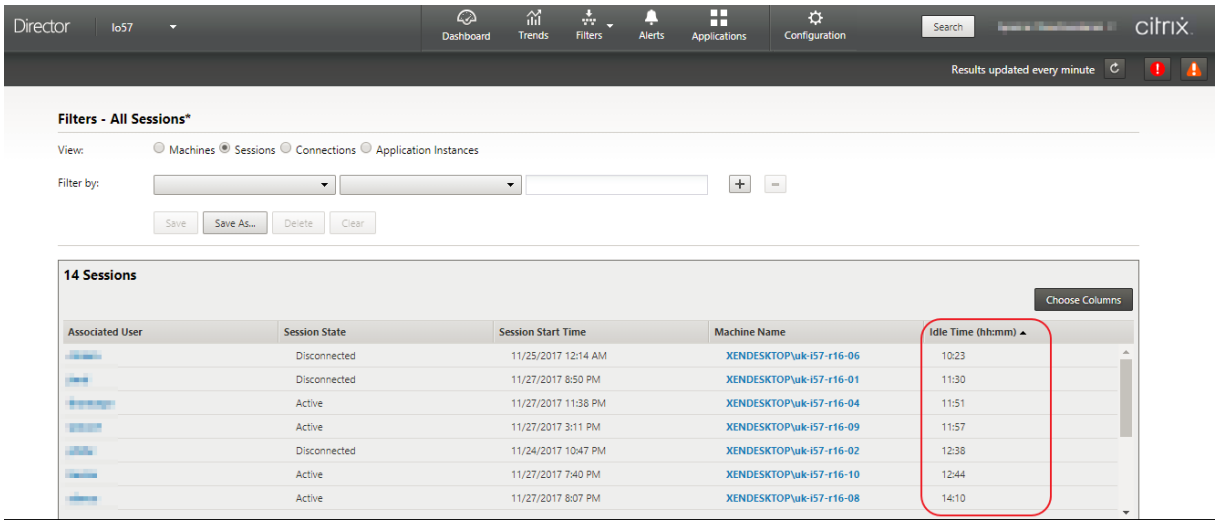
使用此信息可确定空闲时间超过特定时间段的应用程序实例并根据需要注销或断开其连接。为此，请选择过滤器 **>** 应用程序实例，然后选择预先保存的过滤器或选择所有应用程序实例并创建您自己的过滤器。



下面是一个过滤器的示例。对于过滤依据条件，请选择（应用程序的）发布的名称和空闲时间。然后，将空闲时间设置为大于或等于特定时间限制并保存该过滤器以供重复使用。从过滤的列表中，选择应用程序实例。选择用于发送消息的选项，或者从会话控制下拉菜单中，选择注销或断开连接，以结束实例。

> 注意：
>
> 注销或断开应用程序实例注销或断开当前会话连接可结束属于同一会话的所有应用程序实例。

可以使用会话状态和会话空闲时间指标确定会话过滤器页面中的空闲会话。可按空闲时间列进行排序或定义一个过滤器以确定空闲时间超过特定时间限制的会话。系统将列出已至少空闲 10 分钟且在多会话操作系统的 VDA 上的会话的空闲时间。



会话或应用程序实例处于以下状态时空闲时间将显示为不适用

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 空闲时间未超过 10 分钟，
- 是在单会话操作系统中启动的，或者
- 是在运行 7.12 或早期版本的 VDA 上启动的。

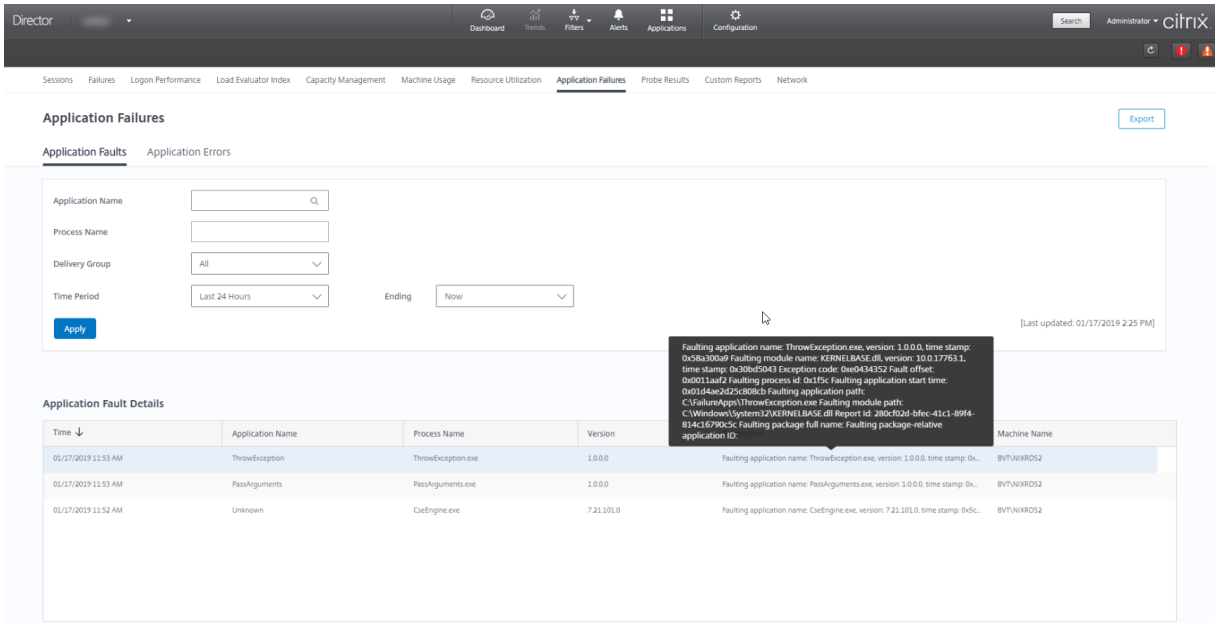
历史应用程序故障监视

趋势 -> 应用程序故障选项卡显示与 VDA 上已发布的应用程序关联的故障。

对于获得 Premium 和 Advanced 许可的站点，可以获取过去 2 小时、24 小时、7 天和 1 个月内的应用程序故障趋势。对于其他许可证类型，可以获取过去 2 小时、24 小时和 7 天内的应用程序故障趋势。记录到事件查看器中的来源为“应用程序错误”的应用程序故障将被监视。单击导出可生成 CSV、Excel 或 PDF 格式的报告

对于获得 Premium 和未获得 Premium 许可的站点，应用程序故障监视的整理保留期限设置 GroomApplicationErrorsRetentionDays 和 GroomApplicationFaultsRetentionDays 默认设置为 1 天。可以使用以下 PowerShell 命令更改此设置：

```
PowerShell command Set-MonitorConfiguration -\<setting name\> \<value \> <!--NeedCopy-->
```



根据故障的严重性，这些故障显示为应用程序故障或应用程序错误。“应用程序故障”选项卡显示与功能或数据的丢失有关的故障。“应用程序错误”指示不直接相关的问题；这些错误表示可能会导致将来出现问题的条件。

可以根据已发布的应用程序名称、进程名称或交付组以及时间段对故障进行过滤。下表显示了故障或错误代码以及故障的简短说明。详细的故障说明以工具提示的方式显示。

> 注意：
>
> 无法推断出相应的应用程序名称时，“已发布的应用程序名称”显示为“未知”。已启动的应用程序在桌面会话中出现故障时，或者该应用程序由于依赖的可执行文件导致的未处理的异常而出现故障时，通常会出现此问题。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

默认情况下，系统仅监视在多会话操作系统 VDA 上托管的应用程序是否出现故障。可以通过以下监视组策略修改监视设置：“启用应用程序故障的监视”、“在单会话操作系统 VDA 上启用应用程序故障的监视”以及“从故障监视中排除的应用程序列表”。有关详细信息，请参阅“监视策略设置”中的应用程序故障监视策略。

趋势 > 应用程序探测结果页面显示过去 24 小时和过去 7 天内在站点中运行的应用程序探测的结果。有关如何配置应用程序探测的更多详细信息，请参阅应用程序探测。

应用程序探测

July 5, 2024

应用程序探测会自动执行检查在站点中发布的 Citrix Virtual Apps 的运行状况的过程。应用程序探测结果可以在 Director 中获取。

要求：

- Delivery Controller 运行版本 7.18 或更高版本。
- 运行探测代理的端点计算机是指安装了 Citrix Receiver for Windows 4.8 或更高版本或者适用于 Windows 的 Citrix Workspace 应用程序（以前称为 Citrix Receiver for Windows）版本 1808 或更高版本的 Windows 计算机。适用于统一 Windows 平台 (UWP) 的 Workspace 应用程序不受支持。
- Director 和 StoreFront 支持基于表单的默认身份验证。

运行应用程序探测所需的用户帐户/权限：

- 要在每个端点计算机上进行探测的唯一 StoreFront 用户。StoreFront 用户不必是管理员；可以在非管理员上下文中运行探测。
- 具有 Windows 管理员权限的用户帐户，以在端点计算机上安装并配置 Citrix Probe Agent
- 完全权限管理员用户帐户或具有以下权限的自定义角色。重复使用现有的用户帐户进行应用程序探测可能会从用户的活动会话中注销。
  - 交付组权限：
    - 只读
  - Director 权限：
    - 创建\编辑\删除警报电子邮件服务器配置 - 如果尚未配置电子邮件服务器
    - 创建\编辑\删除探测配置
    - 查看“配置”页面
    - 查看“趋势”页面

配置应用程序探测

可以安排应用程序探测在非高峰时段跨多个地理区域运行。综合的探测结果有助于在用户遇到与应用程序、托管计算机或连接有关的问题之前对这些问题进行故障排除。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Probe Agent 版本 2103 支持站点聚合。可以从聚合站点枚举和启动应用程序和桌面。配置探测代理时，请选择 已启用 **Workspace (StoreFront)** 站点聚合选项以启用聚合站点中的应用程序和桌面的枚举。支持以下站点的组合：

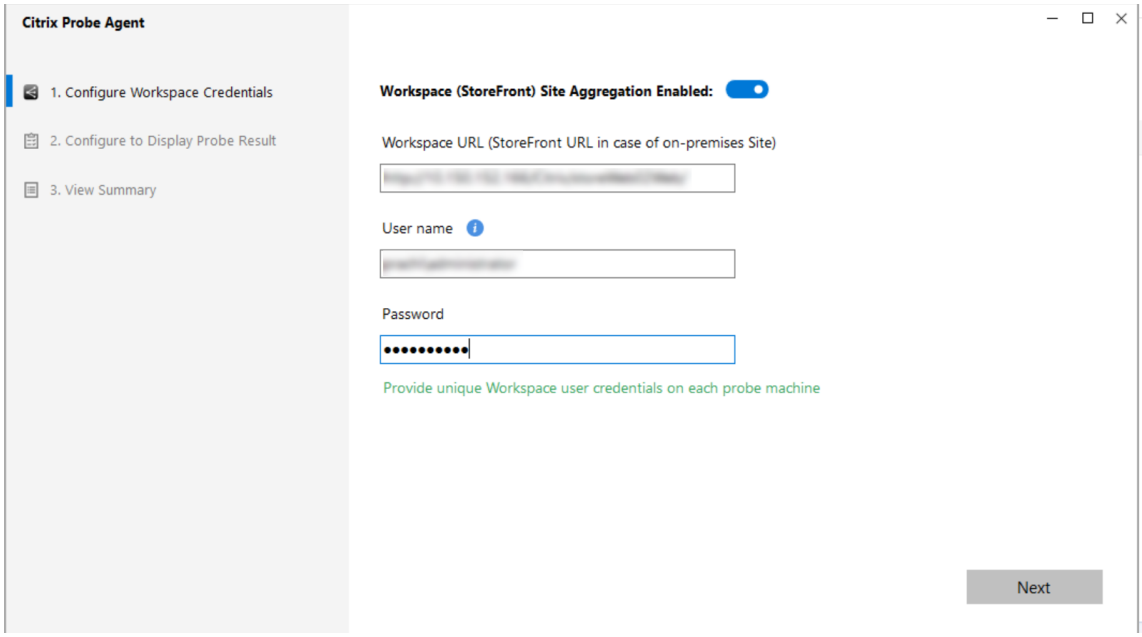
- 具有一个 StoreFront URL 的多个本地站点。
- 具有 StoreFront 或 Workspace URL 的本地和云站点。
- 具有一个 Workspace URL 的多个云站点。

> 注意：
>
> 必须创建单独的管理员或用户才能配置只能访问一个站点的探测。

步骤 1：安装和配置 Citrix Probe Agent

Citrix Probe Agent 是用于模拟用户通过 StoreFront 执行的实际应用程序启动的 Windows 可执行文件。Citrix Probe Agent 测试应用程序启动（如在 Director 中所配置），并将报告结果返回到 Director。

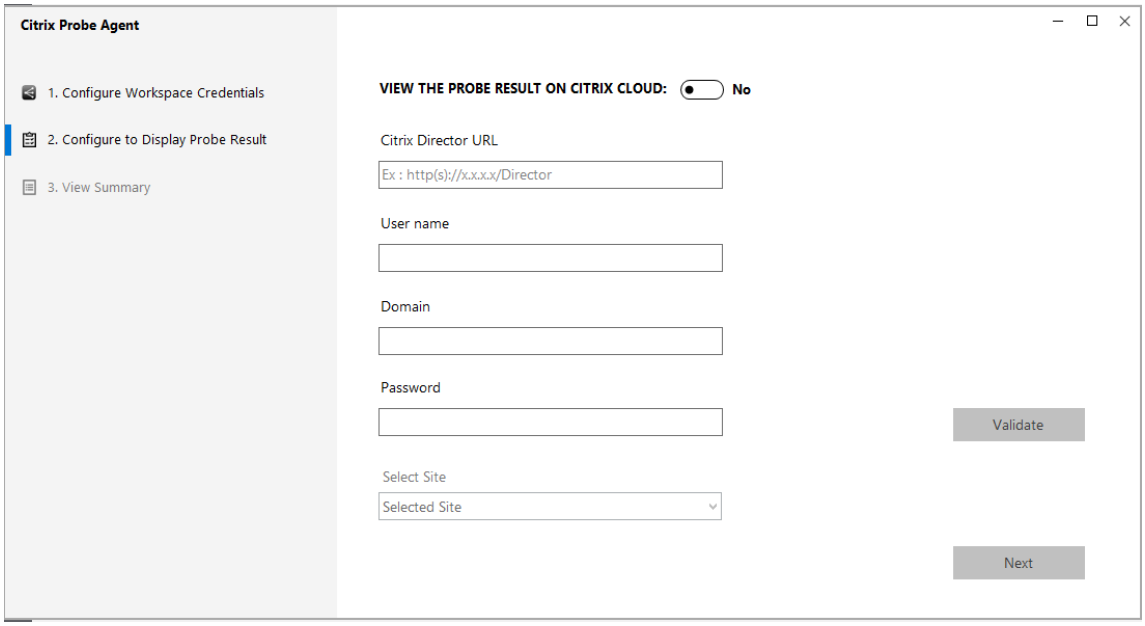
1. 确定要从其中运行应用程序探测的端点计算机。
2. 具有管理权限的用户可以在端点计算机上安装并配置 Citrix Probe Agent。在此处下载 Citrix Probe Agent 可执行文件：https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. 启动代理并配置您的 StoreFront Receiver for Web 凭据。在每个端点计算机上配置唯一的 StoreFront 用户。凭据将加密并安全地存储。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 要访问从外部网络探测的站点，请在“StoreFront URL”字段中键入 Citrix Gateway 的登录 URL。Citrix Gateway 会自动将该请求路由到相应的站点 StoreFront URL。此功能适用于 Citrix Gateway 版本 12.1 或更高版本（RfWebUI 主题），以及 Delivery Controller 1811 及更高版本。

4. 在配置为显示探测结果选项卡中，输入您的 Director 凭据，然后单击验证。



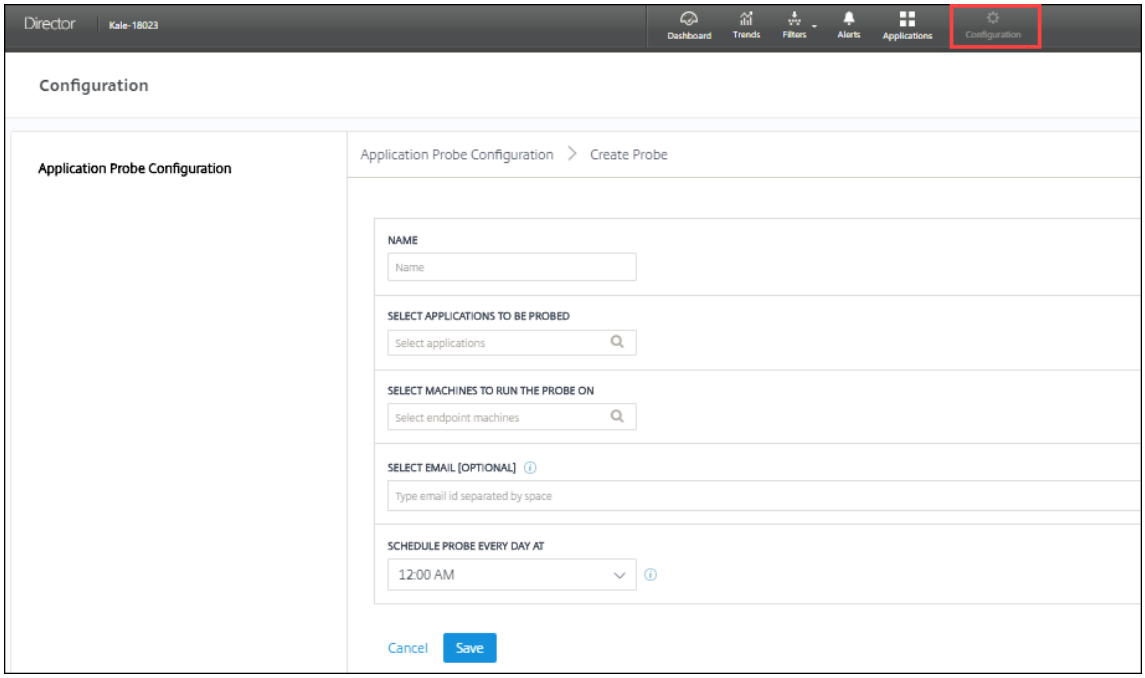
5. 选择您的站点，然后单击下一步。

步骤 **2**：在 **Director** 中配置应用程序探测

1. 转至配置 > 应用程序探测配置。
2. 创建探测并选择：
   - 要探测的应用程序，
   - 必须在其上运行探测的端点计算机，
   - 失败探测结果发送到的电子邮件地址（在警报 -> 电子邮件服务器配置中配置电子邮件服务器），以及
   - 每天必须运行探测的时间（根据端点计算机的本地时区）。

   在 Director 中完成配置后，代理在准备好开始探测之前需要 10 分钟时间。然后，代理将自下一个小时开始运行配置的探测。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



步骤 **3**：执行探测

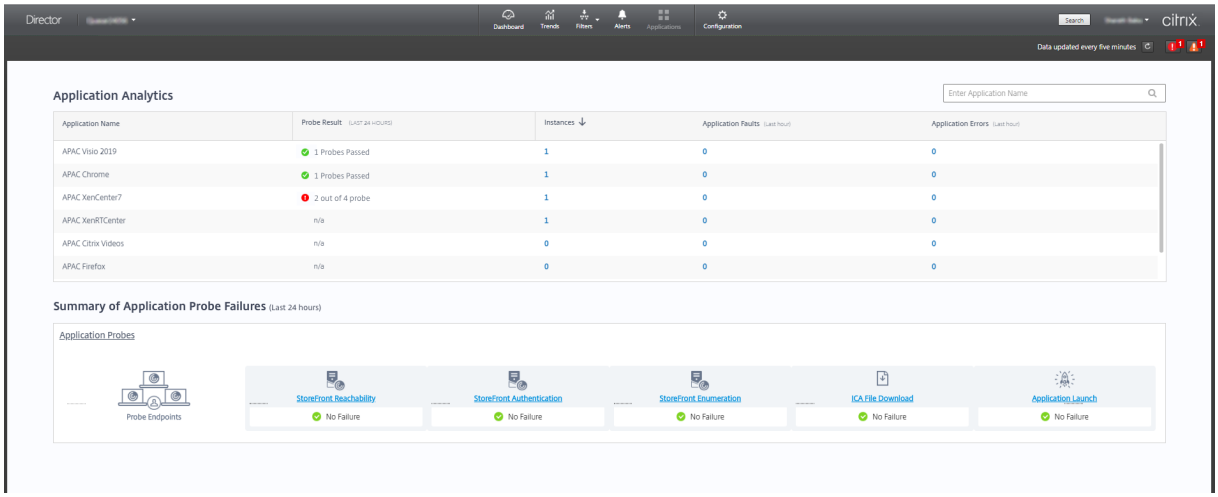
代理根据其定期从 Director 中提取的探测配置运行应用程序探测。代理使用 StoreFront 连续启动选定的应用程序。代理通过监视数据库将报告结果返回到 Director。失败情况在以下五个特定阶段报告：

- **StoreFront** 可访问性 - 配置的 StoreFront URL 无法访问。
- **StoreFront** 身份验证 - 配置的 StoreFront 凭据无效。
- **StoreFront** 枚举 - StoreFront 枚举应用程序列表不包含要探测的应用程序。
- **ICA** 下载 - ICA 文件不可用。
- 应用程序启动 - 无法启动应用程序。

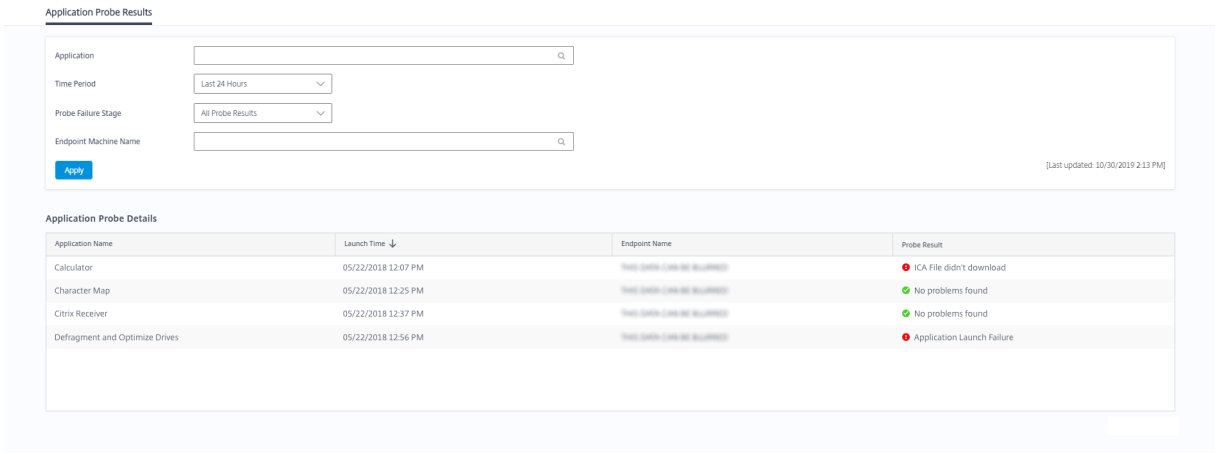
步骤 **4**：查看探测结果

可以在应用程序页面中查看最新的探测结果。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



要进一步进行故障排除，请在趋势 > 应用程序探测结果页面中单击探测结果链接以查看更多详细信息。



在此页面上提供过去 24 小时或过去 7 天的时间内的整理后的探测结果数据。可以看到探测失败的阶段。可以对特定应用程序、探测失败阶段或端点计算机的表格进行过滤。

桌面探测

July 5, 2024

桌面探测会自动执行检查在站点中发布的 Citrix Virtual Desktops 的运行状况的过程。桌面探测结果可以在 Director 中获取。

在 Director 的“配置”页面中，配置要探测的桌面、要在其上运行探测的端点计算机以及探测时间。该代理测试使用 StoreFront 的选定桌面的启动，并向 Director 报告返回的结果。探测结果在 Director UI 中显示–过去 24 小时的数据在“应用程序”页面中显示，历史探测数据在趋势 **>** 探测结果 **>** 桌面探测结果页面中显示。此处，您可以看到出现探测故障时的阶段 - StoreFront 可访问性、StoreFront 身份验证、StoreFront 枚举、ICA 下载或桌面启动。故障报告将发送到配置的电子邮件地址。可以安排桌面探测在非高峰时段跨多个地理区域运行。综合的结果有助于在用户遇到与

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

预配的桌面、托管计算机或连接有关的问题之前主动对这些问题进行故障排除。桌面探测适用于获得 Premium 许可的站点。此功能需要 Delivery Controller 版本 7 1906 或更高版本以及 Probe Agent 1903 或更高版本。

要求：

- Delivery Controller 运行版本 1906 或更高版本。
- 运行探测代理的端点计算机是指安装了 Citrix Receiver for Windows 4.8 或更高版本或者适用于 Windows 的 Citrix Workspace 应用程序（以前称为 Citrix Receiver for Windows）版本 1906 或更高版本的 Windows 计算机。适用于统一 Windows 平台 (UWP) 的 Workspace 应用程序不受支持。
- Director 和 StoreFront 支持基于表单的默认身份验证。

运行桌面探测所需的用户帐户或权限：

- 要在每个端点计算机上进行探测的唯一 StoreFront 用户。StoreFront 用户不必是管理员；可以在非管理员上下文中运行探测。
- 具有 Windows 管理员权限的用户帐户，以在端点计算机上安装并配置 Citrix Probe Agent
- 完全权限管理员用户帐户或具有以下权限的自定义角色。重复使用普通用户帐户进行桌面探测可能会从用户的活动会话中注销。
  - 交付组权限：
    - 只读
  - Director 权限：
    - 创建、编辑、删除警报电子邮件服务器配置 - 如果尚未配置电子邮件服务器
    - 创建、编辑、删除探测配置
    - 查看“配置”页面
    - 查看“趋势”页面

配置桌面探测

可以安排桌面探测在非高峰时段跨多个地理区域运行。综合的探测结果有助于在用户遇到与桌面、托管计算机或连接有关的问题之前对这些问题进行故障排除。

Citrix Probe Agent 版本 2103 支持站点聚合。可以从聚合站点枚举和启动应用程序和桌面。配置探测代理时，请选择 已启用 **Workspace (StoreFront)** 站点聚合选项以启用聚合站点中的应用程序和桌面的枚举。支持以下站点的组合：

- 具有一个 StoreFront URL 的多个本地站点。
- 具有 StoreFront 或 Workspace URL 的本地和云站点。
- 具有一个 Workspace URL 的多个云站点。

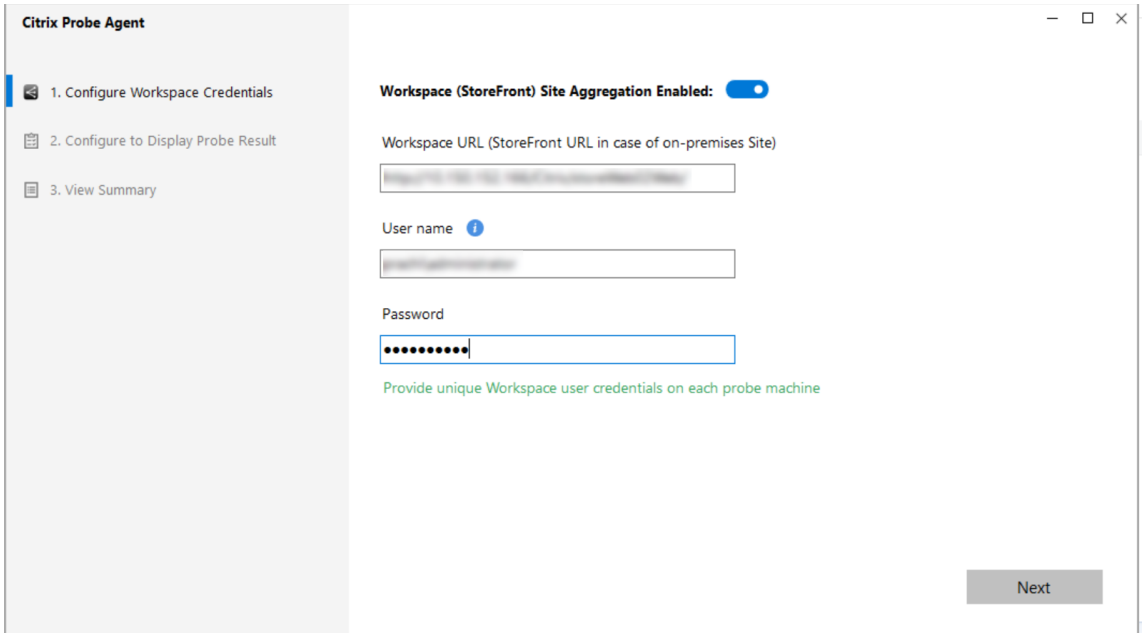
> 注意：
>
> 必须创建单独的管理员或用户才能配置只能访问一个站点的探测。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

步骤 **1**：安装和配置 **Citrix Probe Agent**

Citrix Probe Agent 是用于模拟用户通过 StoreFront 执行的实际桌面启动的 Windows 可执行文件。Citrix Probe Agent 测试桌面启动（如在 Director 中所配置），并将报告结果返回到 Director。

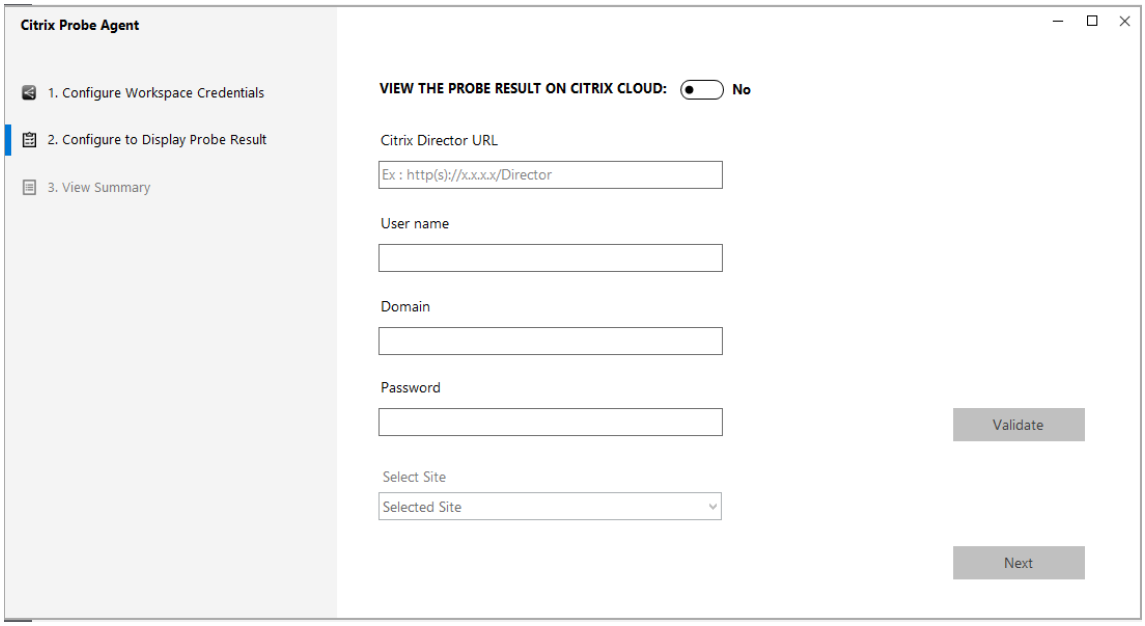
1. 确定要从其中运行桌面探测的端点计算机。
2. 具有管理权限的用户可以在端点计算机上安装并配置 Citrix Probe Agent。在此处下载 Citrix Probe Agent 可执行文件：https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. 启动代理并配置您的 StoreFront Receiver for Web 凭据。在每个端点计算机上配置唯一的 StoreFront 用户。凭据将加密并安全地存储。



> 注意：
>
> - 要访问从外部网络探测到的站点，请在“StoreFront URL”字段中键入 Citrix Gateway 登录页面 URL。Citrix Gateway 会自动将该请求路由到相应的站点 StoreFront URL。此功能适用于 Citrix Gateway 版本 12.1 或更高版本，以及 Delivery Controller 1811 或更高版本。
> - 必须为配置的唯一 StoreFront 用户启用交互式登录。

4. 在配置为显示探测结果选项卡中，输入您的 Director 凭据，然后单击验证。

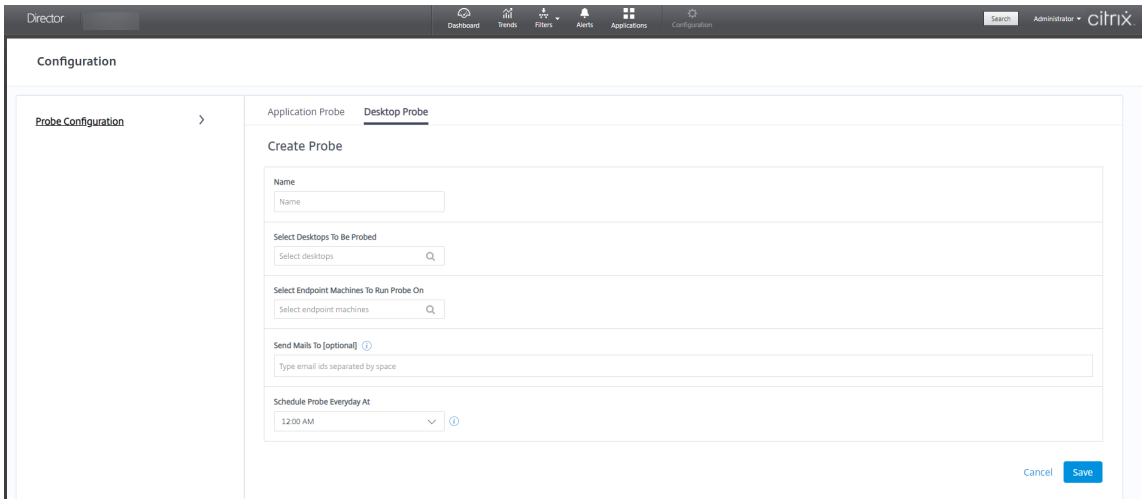
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. 选择您的站点，然后单击下一步。

步骤 **2**：在 **Director** 中配置桌面探测

1. 转至配置 > 桌面探测配置。
2. 要创建探测，请输入详细信息并单击保存。



> 注意：
>
> 在警报 > 电子邮件服务器配置中配置您的电子邮件服务器。

完成桌面探测配置后，代理在准备好开始探测之前需要 10 分钟时间。然后，代理将自下一个小时开始运行配置的探测。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

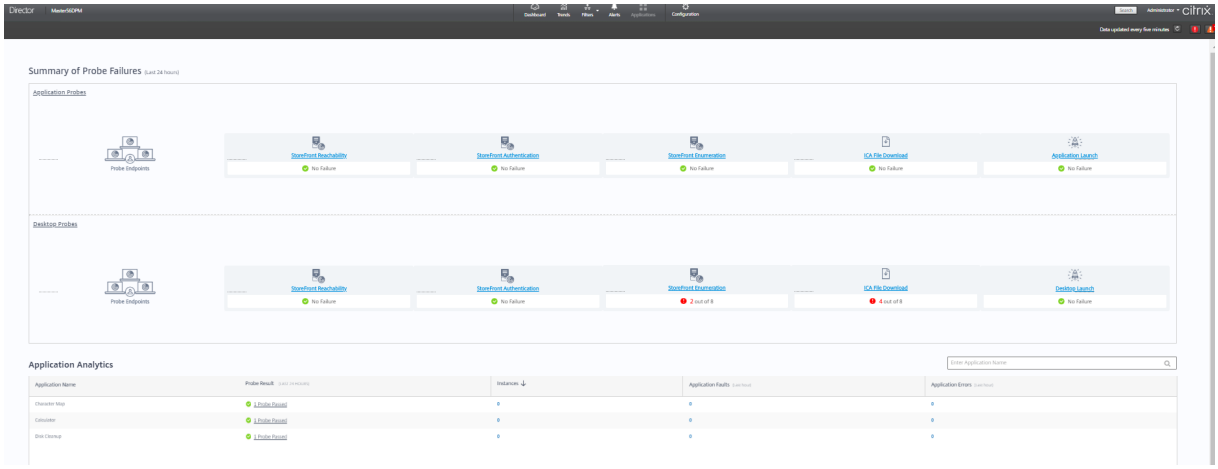
步骤 **3**：执行探测

代理根据其定期从 Director 中提取的探测配置运行桌面探测。代理使用 StoreFront 连续启动选定的桌面。代理通过监视数据库将报告结果返回到 Director。失败情况在以下五个特定阶段报告：

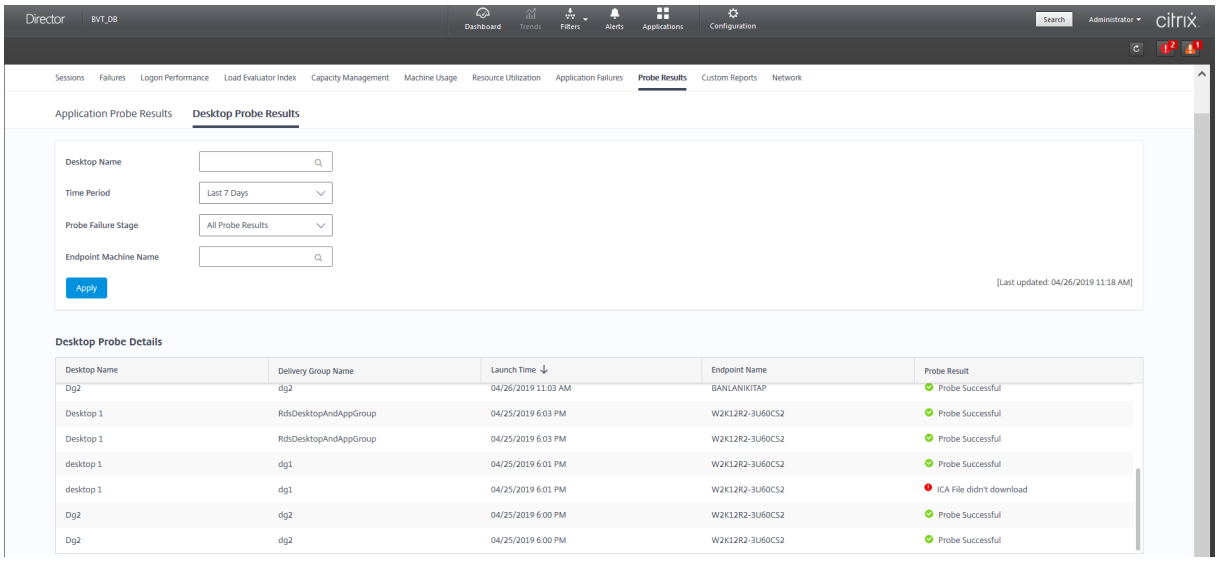
- **StoreFront** 可访问性 - 配置的 StoreFront URL 无法访问。
- **StoreFront** 身份验证 - 配置的 StoreFront 凭据无效。
- **StoreFront** 枚举 - StoreFront 枚举桌面列表不包含要探测的桌面。
- **ICA** 下载 - ICA 文件不可用。
- 桌面启动–桌面无法启动。

步骤 **4**：查看探测结果

可以在桌面页面中查看最新的探测结果。



要进一步进行故障排除，请在趋势 > 探测结果 > 桌面探测结果页面中单击探测结果链接以查看更多详细信息。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

在此页面上提供过去 24 小时或过去 7 天的时间内的整理后的探测结果数据。可以看到探测失败的阶段。可以对特定桌面、探测失败阶段或端点计算机的表格进行过滤。

计算机故障排除

January 21, 2022

> 注意：
>
> **Citrix Health Assistant** 是用于对未注册的 VDA 中的配置问题进行故障排除的工具。此工具自动执行多项运行状况检查，以确定 VDA 注册失败以及会话启动和时区重定向配置中的问题的可能的根本原因。知识中心文章 Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch（Citrix Health Assistant - 对 VDA 注册和会话启动进行故障排除）中包含 **Citrix Health Assistant** 工具下载和使用说明。

Director 控制台中的过滤器 **>** 计算机视图将显示在站点中配置的计算机。“多会话操作系统计算机”选项卡包括负载评估器指数，如果将鼠标悬停在链接上，则会指示性能计数器的分布情况和会话计数的工具提示。

单击故障计算机的故障原因列可获取有关故障的详细说明以及排除故障的建议操作。Citrix Director 7.12 Failure Reasons Troubleshooting Guide（《Citrix Director 7.12 故障原因排除指南》）中提供了计算机故障和连接失败的故障/失败原因和建议的操作。

单击计算机名称链接可转到计算机详细信息页面。

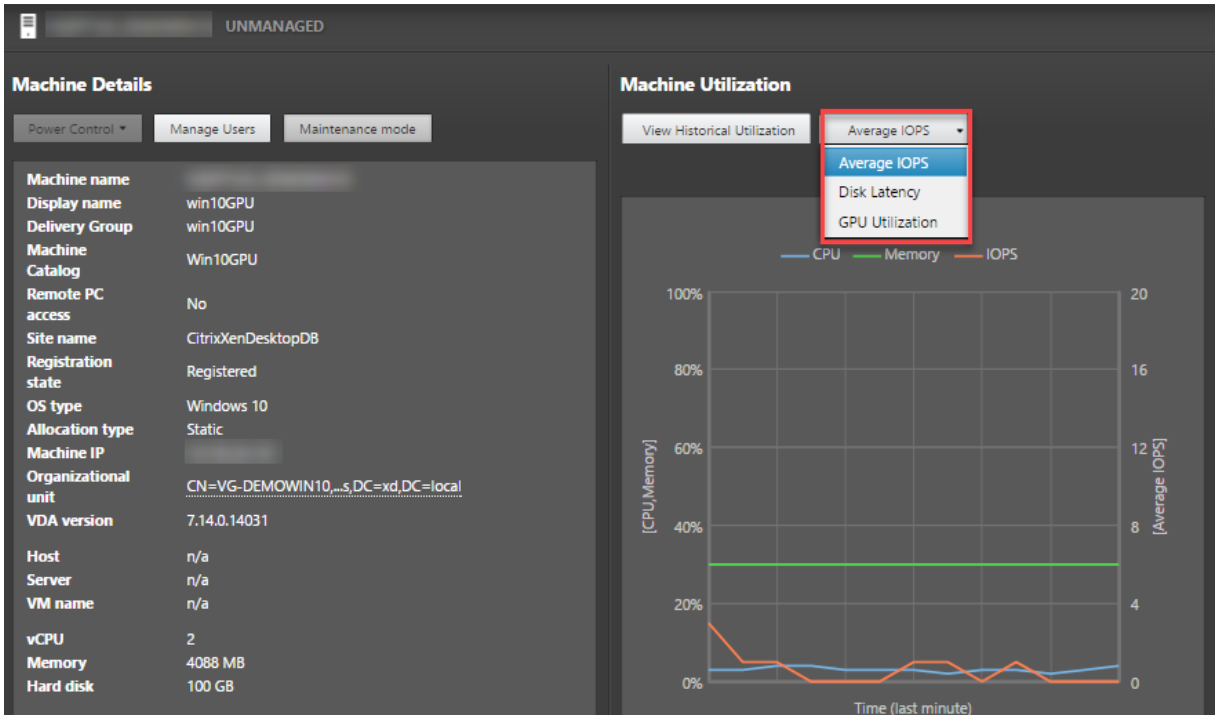
“计算机详细信息”页面列出计算机详细信息、基础结构详细信息和计算机上应用的修补程序的详细信息。

基于计算机的实时资源利用率

计算机利用率面板提供显示 CPU 和内存实时利用率的图形。此外，对于具有 Delivery Controller 和 VDA **7.14** 或更高版本的站点，还提供磁盘和 GPU 监视图。

磁盘监视图、平均 IOPS 和磁盘延迟是重要的性能指标，可帮助您监视与 VDA 磁盘有关的问题并对其进行故障排除。平均 IOPS 图显示磁盘的平均读写次数。选择磁盘延迟可查看请求数据与从磁盘返回数据之间的延迟图（以毫秒为单位）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



选择 **GPU** 利用率可查看 GPU、GPU 内存以及编码器和解码器的利用率百分比，从而对服务器或单会话操作系统 VDA 上的 GPU 相关问题进行故障排除。仅对运行配备了 NVIDIA Tesla M60 GPU 的 64 位 Windows 的 VDA 和运行显示驱动程序 369.17 版或更高版本的 VDA 提供 GPU 利用率图。

VDA 必须启用了 HDX 3D Pro 才能实现 GPU 加速。有关详细信息，请参阅适用于 Windows 单会话操作系统的 GPU 加速和适用于 Windows 多会话操作系统的 GPU 加速。

VDA 访问多个 GPU 时，利用率图将显示从各个 GPU 收集的 GPU 指标的平均值。GPU 指标是针对整个 VDA 收集，而不是针对各个进程收集。

基于计算机的历史资源利用率

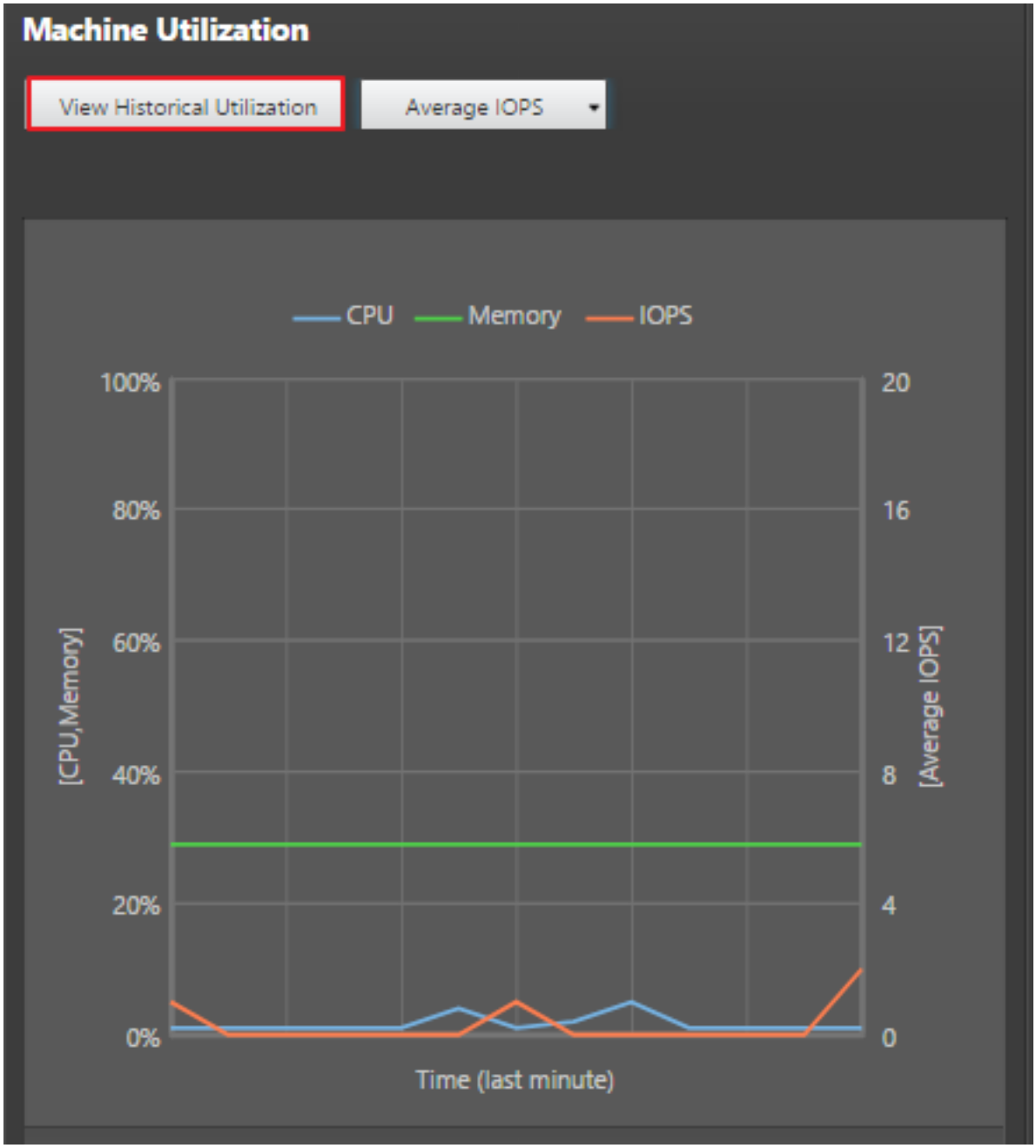
在计算机利用率面板中，单击查看历史利用率可查看选定计算机上资源的历史使用情况。

利用率图包括 CPU、内存、最大并发会话数、平均 IOPS 和磁盘延迟的关键性能计数器。

> 注意：
>
> 必须将监视策略设置启用进程监视设置为“允许”以在“历史计算机利用率”页面上“排名前 10 的进程”表中收集并显示数据。默认情况下禁止收集。

默认情况下会收集 CPU 和内存利用率、平均 IOPS 和磁盘延迟数据。可以使用启用资源监视策略设置禁用收集。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

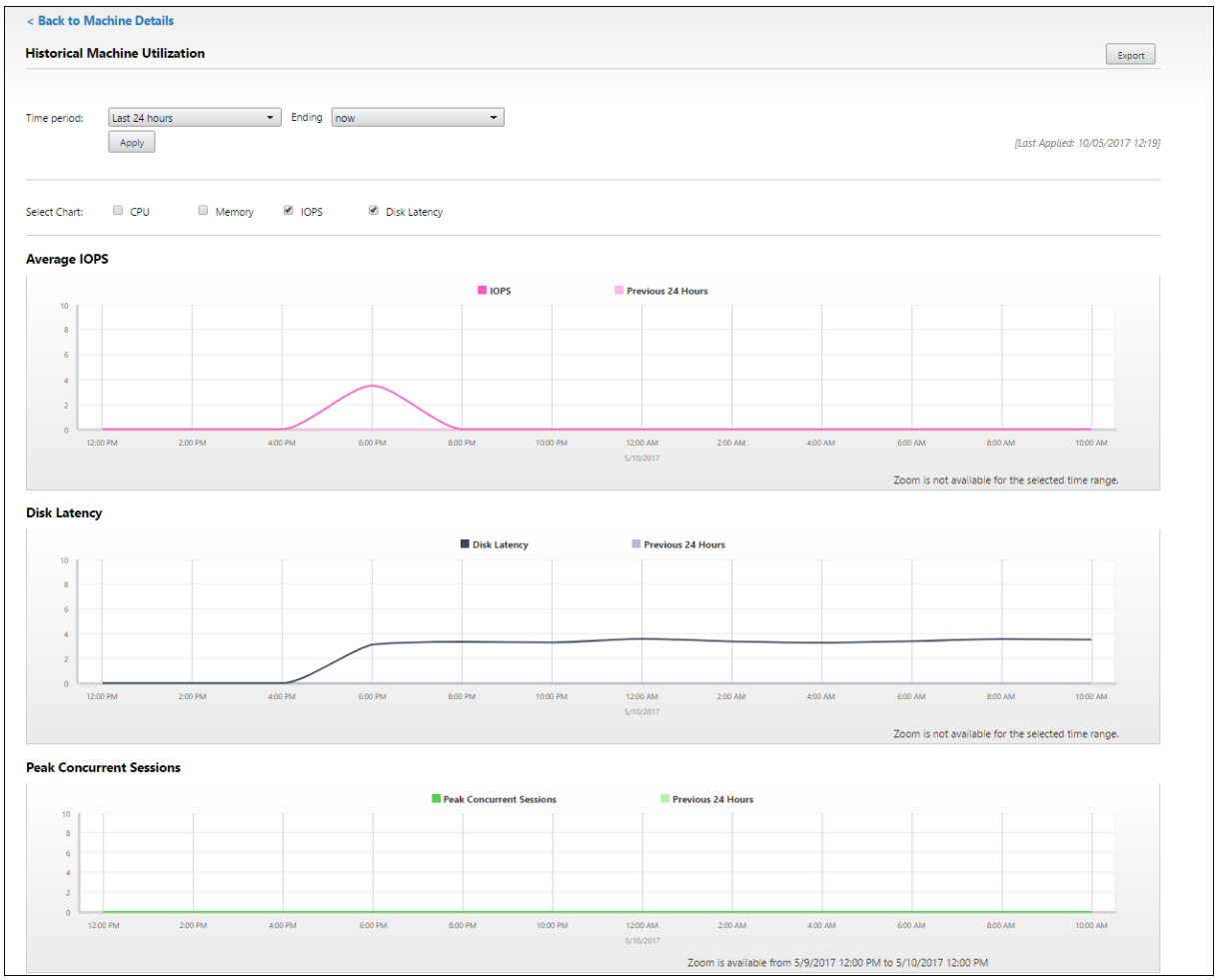


1. 在计算机详细信息视图的计算机利用率面板中，选择查看历史利用率。
2. 在历史计算机利用率页面中，设置时间段以查看过去 2 小时、24 小时、7 天、上个月或上一年的使用情况。

   > 注意：
   >
   > 仅提供过去 24 小时、上个月和去年截止到现在的平均 IOPS 和磁盘延迟使用数据。不支持自定义结束时间。

3. 单击应用并选择所需图形。
4. 将鼠标悬停在图形的不同部分，以查看选定时间段的详细信息。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



例如，如果您选择过去 **2** 小时，则基准期将为选定时间范围前的 2 小时。查看过去 2 小时和基准时间内的 CPU、内存和会话趋势。如果选择上个月，则基准期为上个月。选择可查看上个月和基准时间内的平均 IOPS 和磁盘延迟。

1. 单击导出可导出所选时间段的资源利用率数据。有关详细信息，请参阅“监视部署”中的导出报告部分。
2. 在图形下方，表中列出了基于 CPU 或内存利用率排名前 10 的进程。您可以按照任何列进行排序，其中显示有选定时间范围内的应用程序名称、用户名、会话 ID、平均 CPU 、峰值 CPU、平均内存以及峰值内存。IOPS 和磁盘延迟列不能排序。

   > 注意：
   >
   > 系统进程的会话 ID 将显示为 0000。

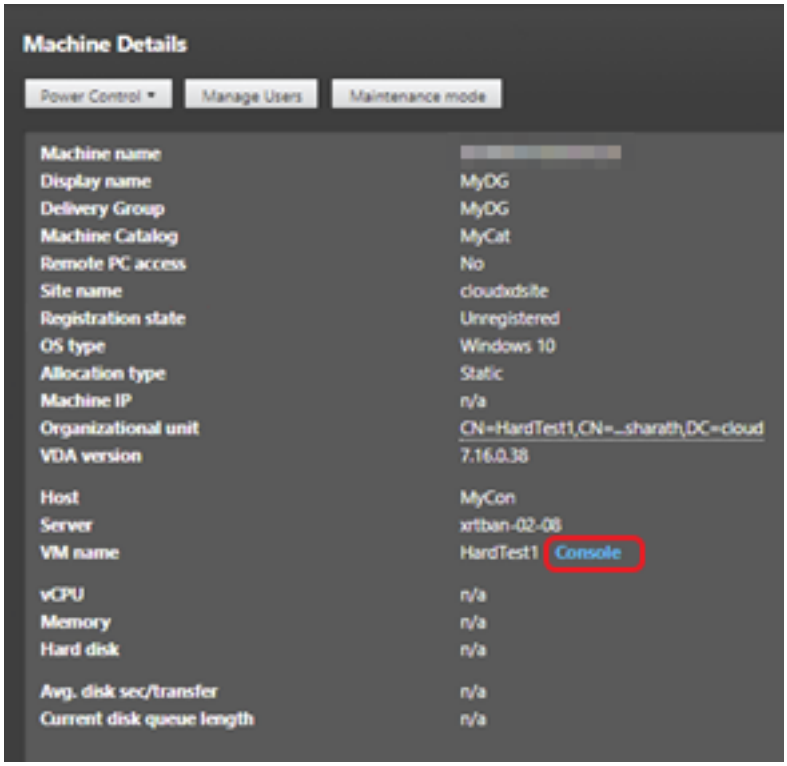
3. 要查看特定进程的资源消耗的历史趋势，请进一步查看排名前 10 的进程中的任何一个。

计算机控制台访问

您可以直接从 Director 访问在 XenServer 7.3 版及更高版本上托管的单会话和多会话操作系统计算机的控制台。这样，您不需要 XenCenter 即可对 XenServer 托管的 VDA 上出现的问题进行故障排除。要使此功能可用：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 需要 Delivery Controller 7.16 或更高版本。
- 托管计算机的 XenServer 的版本必须为 7.3 或更高版本，并且必须可从 Director UI 访问。



要对计算机进行故障排除，请单击相应的“计算机详细信息”面板中的控制台链接。使用您提供的主机凭据进行身份验证后，计算机控制台将使用 noVNC（基于 Web 的 VNC 客户端）在独立的选项卡中打开。您现在可以通过键盘和鼠标访问控制台。

> 注意：
>
> - 此功能在 Internet Explorer 11 中不受支持。
> - 如果计算机控制台上的鼠标指针未对齐，请参阅 CTX230727 了解修复此问题的步骤。
> - Director 在新选项卡中启动控制台访问，确保您的浏览器设置允许弹出窗口。
> - 出于安全原因，Citrix 建议您在浏览器中安装 SSL 证书。

Microsoft RDS 许可证运行状况

您可以在计算机详细信息的“计算机详细信息”面板和多会话操作系统计算机的用户详细信息页面中查看 Microsoft RDS 许可证的状态。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

将显示以下消息之一：

- 许可证可用
- 未正确配置（警告）
- 许可证错误（错误）
- 不兼容的 VDA 版本（错误）

> 注意：
>
> 具有有效许可证且在宽限期内的计算机的 RDS 许可证运行状态将显示绿色的许可证可用消息。在过期之前续订许可证。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

有关警告和错误消息，请将鼠标悬停在信息图标上方以查看下表中提供的其他信息。

消息类型	Director 中的消息
错误	适用于 VDA 7.16 及更高版本。
错误	不允许建立新 RDS 连接。
错误	RDS 许可已超出其宽限期。
错误	使用“每设备客户端访问”许可类型时，没有为所需的操作系统级别配置许可证服务器。
错误	使用“每设备客户端访问”许可类型时，配置的许可证服务器与 RDS 主机操作系统级别不兼容。
警告	在 Citrix Virtual Apps and Desktops 部署中，个人端点服务器不是有效的 RDS 许可类型。
警告	“用于管理的远程桌面”在 Citrix Virtual Apps and Desktops 部署中不是有效的许可类型。
警告	未配置 RDS 许可类型。
警告	使用“每用户客户端访问”RDS 许可类型时，无法访问域控制器或许可证服务器。
警告	使用“每设备客户端访问”许可类型时，无法确定客户端设备许可证，因为无法访问所需操作系统级别的许可证服务器。

> 注意：
>
> 此功能仅适用于 Microsoft RDS CAL（客户端访问许可证）。

对用户问题进行故障排除

January 21, 2022

使用 Director 的技术支持视图（活动管理器页面）查看用户相关信息：

- 检查与用户登录、连接和应用程序相关的详细信息。
- 重影用户计算机。
- 录制 ICA 会话。
- 执行下表中建议的操作对问题进行故障排除，并将其上报给相应的管理员。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

故障排除提示

用户问题	建议
登录时间过长，或者间歇或重复性地出现登录失败。	诊断用户登录问题
会话启动时间过长，或者间歇或重复性地出现会话启动失败问题	诊断会话启动问题
应用程序运行缓慢或无响应	解决应用程序故障
连接失败	还原桌面连接
会话执行缓慢或不响应	还原会话
录制会话	录制会话
视频加载缓慢或画质差	运行 HDX 通道系统报告

> 注意：
> 为确保计算机不处于维护模式，请从“用户详细信息”视图查看“计算机详细信息”面板。

搜索提示

当您在“搜索”字段中键入用户名称时，Director 会在 Active Directory 中跨所有配置为支持 Director 的站点搜索用户。

在“搜索”字段中输入多用户计算机名称时，Director 显示特定计算机的计算机详细信息。

在“搜索”字段中输入端点名称时，Director 使用连接到指定端点的未经身份验证（匿名）的会话和经过身份验证的会话，从而对未经身份验证的会话进行故障排除。请确保端点名称唯一以启用对未经身份验证的会话进行故障排除。

搜索结果中也包括当前未使用计算机或未分配给计算机的用户。

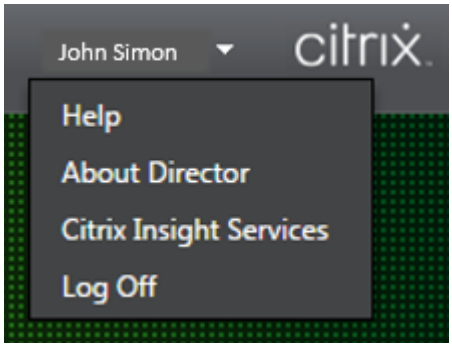
- 搜索时不区分大小写。
- 不完整的输入会产生一个可能匹配的列表。
- 您键入一个由两部分构成且中间以空格分隔的名称（用户名、姓名或显示名称）的几个字母后，搜索结果中将包含与这两个字符串均匹配的条目。例如，如果您键入 jo rob，搜索结果中可能包括“John Robertson”或 Robert, Jones 等字符串。

要返回登录页面，请单击 **Director** 徽标。

访问 **Citrix Insight Services**

您可以从 Director 的用户下拉列表中访问 Citrix Insight Services (CIS) 以获得其他诊断见解。CIS 中的数据来自 Call Home 和 Citrix Scout 等。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



将故障排除信息上载给 **Citrix** 技术支持

从单个 Delivery Controller 或 VDA 运行 Citrix Scout 可捕获关键数据点和 Citrix Diagnostics Facility (CDF) 跟踪以对所选计算机进行故障排除。Scout 提供将数据安全地上载到 CIS 平台以帮助 Citrix 技术支持进行故障排除的功能。Citrix 技术支持使用 CIS 平台可缩短解决客户报告的问题所需的时间。

Scout 随 Citrix Virtual Apps and Desktops 组件一起安装。安装或升级到 Citrix Virtual Apps and Desktops 时，Scout 显示在 Windows 的“开始”菜单或“开始”屏幕上，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。

诊断会话启动问题

July 5, 2024

除了诊断用户登录问题部分中提到的登录进程各阶段外，Director 还显示会话启动持续时间。这在用户详细信息页面和计算机详细信息页面上分为 Workspace 应用程序会话启动和 VDA 会话启动持续时间。这两个持续时间进一步包含各个阶段，其启动持续时间也会显示。此数据可帮助您了解会话启动持续时间过长的问题并对其进行故障排除。此外，会话启动中涉及的每个阶段的持续时间有助于解决与各个阶段相关联的问题。例如，如果驱动器映射时间较长，则可以检查是否在 GPO 或脚本中正确映射了所有有效的驱动器。此功能仅在 Delivery Controller 版本 7 1906 和更高版本以及 VDA 1903 和更高版本中提供。

必备条件

确保满足以下必备条件才能显示会话启动持续时间数据：

- Delivery Controller 7 1906 或更高版本。
- VDA 1903 或更高版本。
- Citrix End User Experience Monitoring (EUEM) 服务必须在 VDA 上运行。

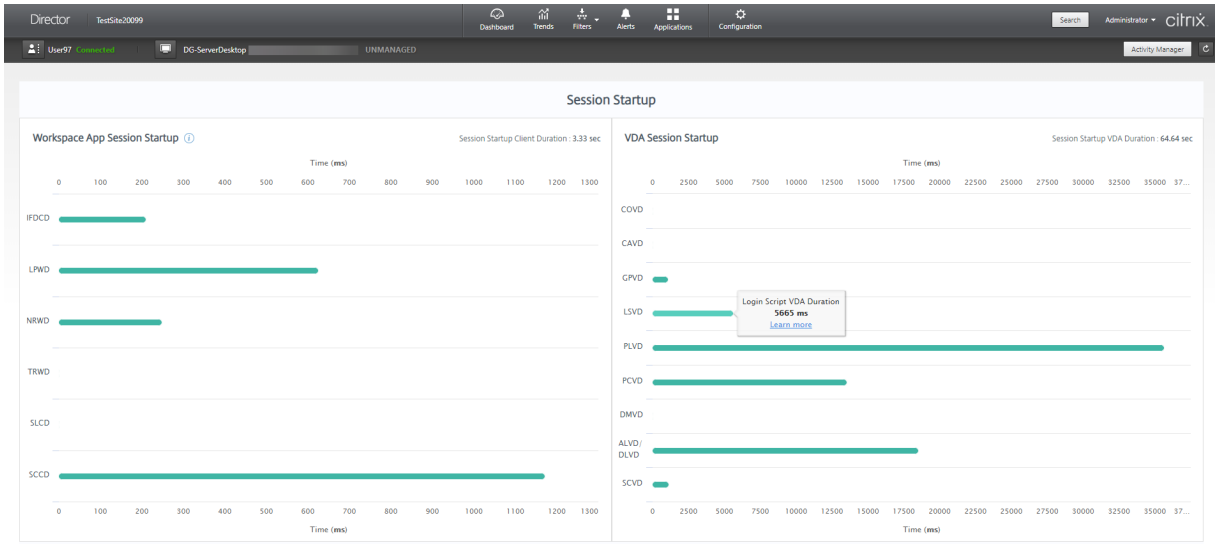
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

限制

当 Director 显示会话启动持续时间数据时，将适用以下限制。

- 会话启动持续时间仅适用于 HDX 会话。
- 对于从 iOS 和 Android 操作系统启动会话，只有 VDA 启动持续时间可用。
- 只有在从浏览器启动过程中检测到 Workspace 应用程序时，ICA 文件下载持续时间 (IFDCD) 才可用。
- 对于从 Mac 操作系统启动会话，IFDCD 仅适用于 Workspace 应用程序 1902 或更高版本。
- 对于从 Windows 操作系统启动会话，IFDCD 可用于 Workspace 应用程序 1902 及更高版本。对于早期版本，仅针对从检测到 Workspace 应用程序的浏览器进行的应用程序启动显示 IFDCD。

> 备注：
>
> - 如果在满足必备条件后会话启动持续时间显示时遇到问题，请查看 Director 服务器和 VDA 日志，如 CTX130320 中所述。
>
> 对于共享会话（在同一会话中启动的多个应用程序），将显示针对最新连接或最新应用程序启动的 Workspace 应用程序启动指标。
> - VDA 会话启动中的某些指标不适用于重新连接。在这种情况下，将显示一条消息。



Workspace 应用程序会话启动阶段

会话启动客户端持续时间 **(SSCD)**

当此指标较高时，它表示客户端问题导致较长的开始时间。查看后续指标以确定问题的可能根本原因。SSCD 开始尽可能接近请求的时间（鼠标单击）。在客户端设备与 VDA 之间建立 ICA 连接时，它将结束。在共享会话的情况下，此持续时间要小得多，因为不会产生与创建到服务器的新连接相关的设置成本。在下一级别，有几个详细的指标可用。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ICA 文件下载持续时间

这是客户端从服务器下载 ICA 文件所需的时间。整个过程如下：

1. 用户单击 Workspace 应用程序中的资源（应用程序或桌面）。
2. 用户的请求将通过 Citrix Gateway(如果已配置)发送到 StoreFront，后者将请求发送到 Delivery Controller。
3. Delivery Controller 查找请求可用的计算机，并将计算机信息和其他详细信息发送到 StoreFront。此外，StoreFront 请求并接收来自 Secure Ticket Authority 的一次性票证。
4. StoreFront 会生成一个 ICA 文件并通过 Citrix Gateway（如果已配置）将其发送给用户。

IFDCD 代表完成过程（步骤 1–4）所需的时间。客户端接收到 ICA 文件时，IFDCD 持续时间停止计数。

LPWD 是过程的 StoreFront 组件。

如果 IFDCD 很高（但 LPWD 正常），则启动的服务器端处理成功，但客户端设备与 StoreFront 之间存在通信问题。这是两台计算机之间的网络问题引起的。因此，您可以先解决潜在的网络问题。

启动页面 **Web** 服务器持续时间 **(LPWD)**

这是处理 StoreFront 上的启动页面 (launch.aspx) 所需的时间。如果 LPWD 很高，StoreFront 可能会出现瓶颈。

可能的原因包括：

- StoreFront 上的高负载。尝试通过检查 Internet Information Services (IIS) 日志和监视工具、任务管理器、性能监视器等来识别减速的原因。
- StoreFront 与其他组件（例如 Delivery Controller）进行通信时遇到问题。检查 StoreFront 与 Delivery Controller 之间的网络连接是否缓慢，或者某些 Delivery Controller 已关闭或过载。

名称解析 **Web** 服务器持续时间 **(NRWD)**

这是 Delivery Controller 将已发布的应用程序/桌面的名称解析为 VDA 计算机 IP 地址所花费的时间。

此指标较高时，表示 Delivery Controller 需要很长时间才能将已发布的应用程序的名称解析为 IP 地址。

可能的原因包括客户端上的问题、Delivery Controller 的问题（例如 Delivery Controller 过载）或它们之间的网络链接问题。

票证响应 **Web** 服务器持续时间 **(TRWD)**

此持续时间表示从 Secure Ticket Authority (STA) 服务器或 Delivery Controller 获取票证所需的时间（如有必要）。当此持续时间较长时，它指示 STA 服务器或 Delivery Controller 过载。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

会话查找客户端持续时间 **(SLCD)**

此持续时间表示查询每个会话以托管请求的已发布应用程序所需的时间。在客户端上执行检查，以确定现有会话是否能够处理应用程序启动请求。使用的方法取决于会话是新会话还是共享会话。

会话创建客户端持续时间 **(SCCD)**

此持续时间表示创建会话所需的时间，从启动 wfica32.exe（或类似的等效文件）到建立连接的时间。

VDA 会话启动阶段

会话启动 **VDA** 持续时间 **(SSVD)**

此持续时间是高级服务器端连接启动指标，包含 VDA 执行整个启动操作所需的时间。此指标较高时，表示存在增加会话开始时间的 VDA 问题。这包括在 VDA 上执行整个启动操作花费的时间。

凭据获取 **VDA** 持续时间 **(COVD)**

VDA 获取用户凭据所花费的时间。

如果用户未能及时提供凭据，此持续时间可能会人为地增加。因此，它不包括在 VDA 启动持续时间中。只有当使用手动登录并显示服务器端凭据对话框（或者在登录开始前显示合法通知）时，此时间才可能很重要。

凭据身份验证 **VDA** 持续时间 **(CAVD)**

这是 VDA 根据身份验证提供程序验证用户凭据所花费的时间。它们可以是 Kerberos、Active Directory 或安全支持提供程序接口 (SSPI)。

组策略 **VDA** 持续时间 **(GPVD)**

此持续时间是在登录期间应用组策略对象所花费的时间。

登录脚本执行 **VDA** 持续时间 **(LSVD)**

这是 VDA 运行用户的登录脚本所需的时间。

考虑使用户或组的登录脚本异步。考虑优化任何应用程序兼容性脚本或改用环境变量。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

配置文件加载 **VDA** 持续时间 **(PLVD)**

这是 VDA 加载用户的配置文件所需的时间。

如果此持续时间较长，请考虑您的用户配置文件配置。漫游配置文件大小和位置会导致会话启动速度缓慢。当用户登录到启用了端点服务漫游配置文件和主文件夹的会话时，漫游配置文件内容和对该文件夹的访问将在登录过程中映射。这需要额外的资源。有时，这可能会占用大量 CPU。您可以考虑将端点服务主文件夹和重定向的个人文件夹结合使用，以缓解此问题。通常，请考虑使用 Citrix Profile Management 来管理 Citrix 环境中的用户配置文件。如果您使用 Citrix Profile Management 且登录时间缓慢，请检查防病毒软件是否阻止 Citrix Profile Management 工具。

打印机创建 **VDA** 持续时间 **(PCVD)**

这是 VDA 同步映射用户的客户端打印机所需的时间。如果配置设置为异步执行打印机创建，则不会为 PCVD 记录任何值，因为它不会影响会话启动的完成。

在映射打印机上花费的时间过长通常是打印机自动创建策略设置的结果。用户客户端设备上本地添加的打印机数量和打印配置会直接影响会话启动时间。会话启动时，Citrix Virtual Apps and Desktops 必须在客户端设备上创建每个本地映射的打印机。请考虑重新配置打印策略，以减少创建的打印机数量，特别是在用户拥有许多本地打印机时。为此，请在 Delivery Controller 和 Citrix Virtual Apps and Desktops 中编辑“打印机自动创建”策略。

驱动器映射 **VDA** 持续时间 **(DMVD)**

这是 VDA 映射用户的客户端驱动器、设备和端口所花费的时间。

确保您的基本策略包含禁用未使用的虚拟通道的设置。例如，音频或 COM 端口映射，以优化 ICA 协议并提高整体会话性能。

应用程序/桌面启动 **VDA** 持续时间 **(ALVD/DLVD)**

此阶段是 Userinit 和 Shell 持续时间的组合。当用户登录到 Windows 计算机时，winlogon 将运行 Userinit.exe。Usernit.exe 运行登录脚本、重新建立网络连接，然后启动 Explorer.exe。Userinit 表示 userinit.exe 启动到虚拟桌面或应用程序的用户界面启动之间的持续时间。Shell 持续时间是指用户界面初始化到用户收到键盘和鼠标控制权的时间之间的时间。

会话创建 **VDA** 持续时间 **(SCVD)**

此时间包括 VDA 上的会话创建时间中的任何杂项延迟。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

诊断用户登录问题

January 21, 2022

使用“登录持续时间”数据解决用户登录问题。

仅测量使用 HDX 与桌面或应用程序建立的初始连接的登录持续时间。此数据不包括尝试与远程桌面协议建立连接或从断开的会话重新连接的用户。具体而言，当用户最初使用非 HDX 协议建立连接，然后使用 HDX 重新连接时，不测量登录持续时间。

在“用户详细信息”视图中，持续时间显示为数字值。在此数值下，将显示登录时间以及登录过程各阶段的图表。

当用户登录到 Citrix Virtual Apps and Desktops 时，Monitor Service 会跟踪登录过程的各个阶段。这些阶段从用户从 Citrix Workspace 应用程序连接的时间开始到桌面可以使用的时间结束。

左侧的大数字是总登录时间。计算方法为：将建立连接和从 Delivery Controller 获得桌面所用的时间与执行身份验证和登录虚拟桌面所用的时间相结合。持续时间信息显示为秒（或秒的小数部分）。

必备条件

请确保满足以下必备条件以显示登录持续时间数据和深入分析信息：

1. 在 VDA 上安装 **Citrix User Profile Manager** 和 **Citrix User Profile Manager WMI** 插件。
2. 确保 Citrix Profile Management 服务正在运行。
3. 对于 XenApp 和 XenDesktop 站点 7.15 及更早版本，请禁用 GPO 设置不处理旧的运行列表。
4. 必须启用审核流程跟踪以对交互式会话进行深入分析。
5. 要对 GPO 进行深入分析，请增加组策略运行日志的大小。

> 备注：
>
> - 仅在默认 Windows Shell (explorer.exe) 上而非自定义 Shell 上支持登录持续时间。
> - 仅当 **Citrix User Profile Manager** 和 **Citrix User Profile Manager WMI** 插件在 Remote PC Access 安装过程中作为额外的组件安装时，Remote PC Access 的登录持续时间才可用。有关详细信息，请参阅 Remote PC Access 配置和顺序注意事项中的步骤 4。

用于解决用户登录问题的步骤

1. 在用户详细信息视图中，使用“登录持续时间”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。
   - 如果用户已登录，“登录持续时间”面板会显示用户登录当前会话所用的时间。
2. 检查登录过程中的各个阶段。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

登录过程阶段

正在代理

在决定向用户分配哪个桌面时所用的时间。

VM 启动

如果会话需要启动计算机，VM 启动时间为启动虚拟机所用的时间。

HDX 连接

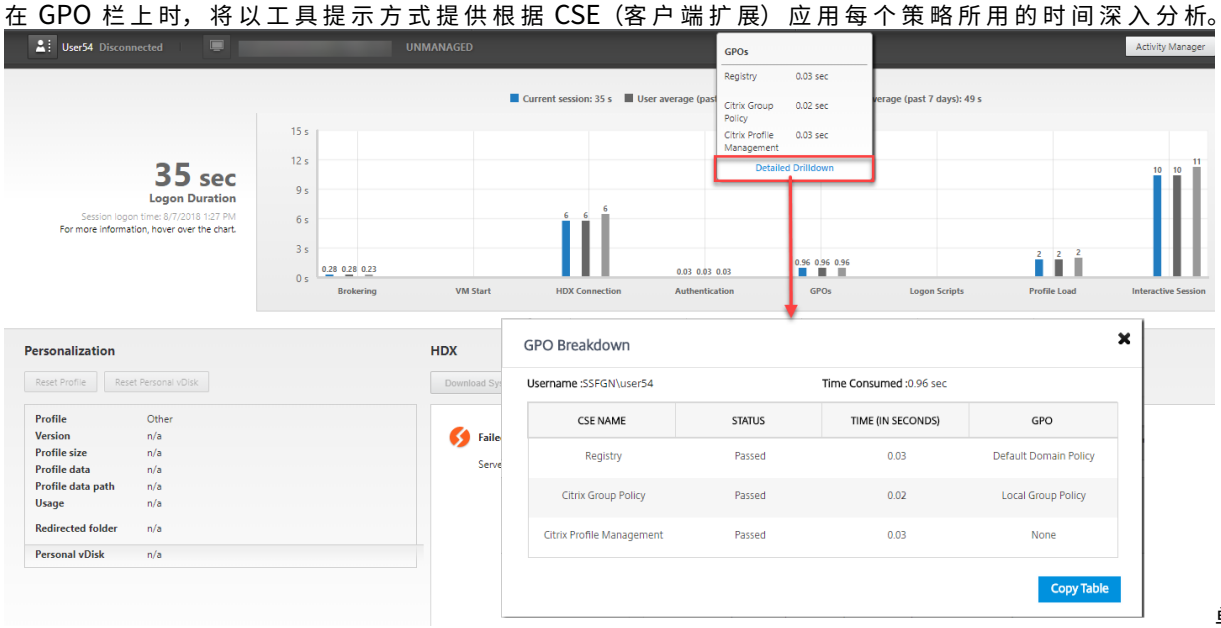
在设置从客户端到虚拟机的 HDX 连接期间需执行的步骤所用的时间。

身份验证

完成远程会话的身份验证所用的时间。

GPO

如果在虚拟机上启用了组策略设置，则为登录过程中应用组策略对象所用的时间。将鼠标悬停在 GPO 栏上时，将以工具提示方式提供根据 CSE（客户端扩展）应用每个策略所用的时间深入分析。



单击详细的深入分析可查看包含策略状态与相应的 GPO 名称的表格。深入分析中的持续时间仅表示 CSE 处理时间，不计入总 GPO 时间。您可以复制深入分析表格以进一步排除故障或用于报告中。可从事件查看器日志中检索策略的 GPO 时间。根据为操作日志分配的内存（默认大小为 4 MB），这些日志可能会被覆盖。有关增加操作日志的日志大小的详细信息，请参阅 Microsoft TechNet 文章 Configuring the Event Logs（配置事件日志）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

登录脚本

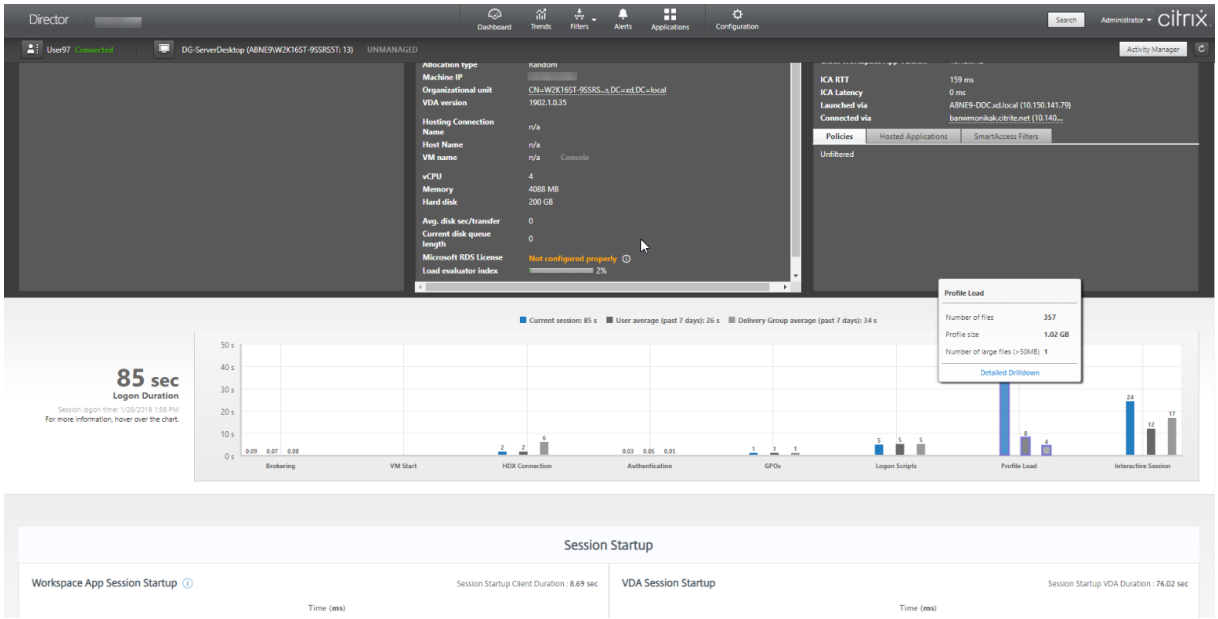
如果为会话配置了登录脚本，则指运行登录脚本所用的时间。

配置文件加载

如果为用户或虚拟机配置了配置文件设置，则为加载配置文件所用的时间。

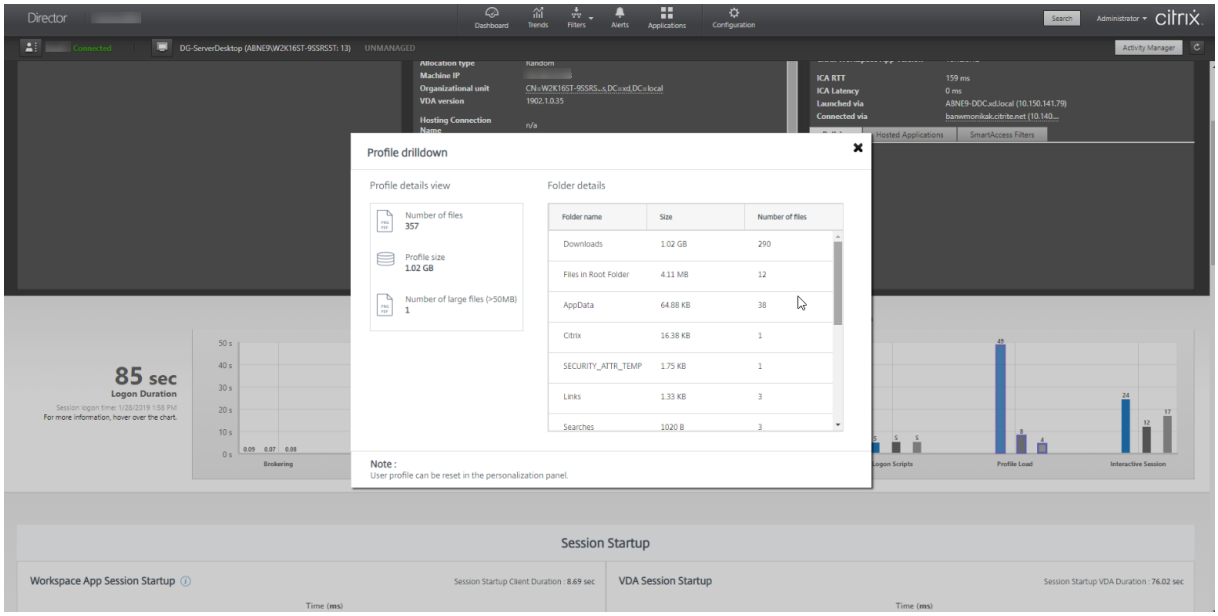
如果配置了 Citrix Profile Management，配置文件加载栏将包括 Citrix Profile Management 处理用户配置文件所需的时间。此信息可帮助管理员解决高配置文件加载持续时间的问题。配置 Profile Management 后，配置文件加载栏将显示增加的持续时间。这种增加是由此增强功能引起的，并不反映性能下降问题。此增强功能在 VDA 1903 或更高版本中可用。

将鼠标悬停在配置文件加载条上将显示工具提示，即显示当前会话的用户配置文件详细信息。



单击详细的深入分析以进一步深入分析配置文件根文件夹（例如，C:/Users/username）中的各个文件夹、其大小和文件数量（包括嵌套文件夹中的文件）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



配置文件深入分析功能仅在 Delivery Controller 版本 7 1811 或更高版本以及 VDA 1811 或更高版本中提供。使用配置文件深入分析信息，可以解决与配置文件加载时间较长有关的时间。您可以：

- 重置用户配置文件
- 删除不必要的大型文件以优化配置文件
- 减少文件数量以降低网络负载
- 使用 Profile Streaming

默认情况下，配置文件根目录中的所有文件夹都将显示明细。要隐藏文件夹名称，请编辑 VDA 计算机上的注册表值：

> 警告：
>
> 注册表添加和编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 不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，在 HKEY_LOCAL_MACHINE\Software\Citrix\Director 中添加新的注册表值 **ProfileFolderNameHidden**\
2. 将值设置为 1。此值必须是 DWORD（32 位）值。文件夹名称可见性现在处于禁用状态。
3. 要使文件夹名称再次可见，请将值设置为 0。

> 注意：
> 可以使用 GPO 或 PowerShell 命令在多个计算机上应用对注册表值所做的更改。有关使用 GPO 部署注册表更改的详细信息，请参阅博客。

其他信息

- 配置文件深入分析不考虑重定向的文件夹。
- 根文件夹中的 NTUser.dat 文件可能对最终用户不可见。但是，这些文件包含在配置文件深入分析中，且会显示在根文件夹中的文件列表中。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 配置文件明细中不包括 AppData 文件夹中的一些隐藏文件。
- 由于存在某些 Windows 限制，文件数和配置文件大小数据可能与“个性化”面板中的数据不匹配。

交互式会话

这是在加载用户配置文件后向用户“移交”键盘和鼠标控制权所用的时间。它通常是登录过程的所有阶段的最长持续时间，其计算公式如下：交互式会话持续时间 **=** 桌面就绪事件时间戳（**VDA** 上的 **EventId 1000**）**-** 用户配置文件加载的事件时间戳（**VDA** 上的 **EventId 2**）。交互式会话有三个子阶段：Pre-userinit、Userinit 和 Shell。将鼠标悬停在交互式会话上可查看显示以下内容的工具提示：

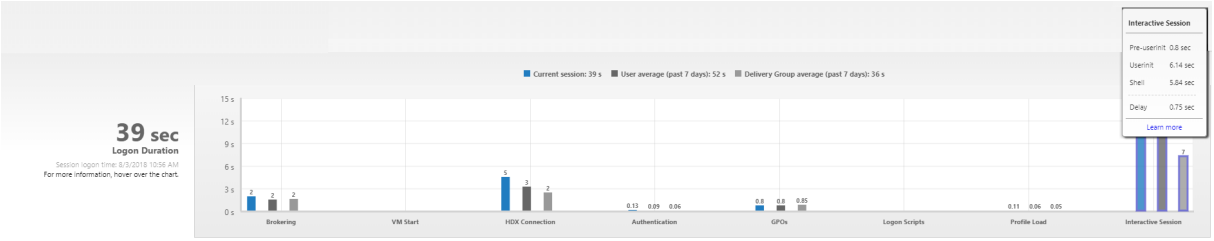
- 子阶段
- 每个子阶段所用的时间
- 这些子阶段之间的总累积时间延迟
- 指向文档的链接。

> 注意：
>
> 此功能在 VDA 1811 及更高版本中提供。如果您在低于 7.18 的站点上启动了会话，然后升级到 7.18 或更高版本，则会显示“由于服务器错误，深入分析不可用”消息。但是，如果您在升级后启动会话，则不会显示错误消息。

要查看每个子阶段的持续时间，请在 VM (VDA) 上启用审核进程跟踪。审核进程跟踪处于禁用状态（默认）时，将显示 Pre-userinit 的持续时间以及 Userinit 和 Shell 的总持续时间。您可以通过组策略对象 (GPO) 启用审核进程跟踪，如下所示：

1. 使用 GPO 编辑器创建一个 GPO 并对其进行编辑。
2. 转至计算机配置 **>** **Windows** 设置 **>** 安全设置 **>** 本地策略 **>** 审核策略。
3. 在右侧窗格中，双击审核进程跟踪。
4. 选择成功，然后单击“确定”。
5. 将此 GPO 应用于所需的 VDA 或组。

有关审核进程跟踪以及对其进行启用或禁用的详细信息，请参阅 Microsoft 文档中的审核进程跟踪。



“用户详细信息”视图中的“登录持续时间”面板。

- 交互式会话 **- Pre-userinit**：与组策略对象和脚本重叠的交互式会话的片段。可以通过优化 GPO 和脚本缩短此子阶段。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 交互式会话 **- Userinit:** 当用户登录 Windows 计算机时，Winlogon 将运行 Userinit.exe。Userinit.exe 运行登录脚本，重新建立网络连接，然后启动 Explorer.exe（Windows 用户界面）。交互式会话的此子阶段表示 Userinit.exe 启动到虚拟桌面或应用程序的用户界面启动之间的持续时间。
- 交互式会话 **- Shell:** 在上一阶段，Userinit 开始初始化 Windows 用户界面。Shell 子阶段将捕获用户界面初始化到用户收到键盘和鼠标控制权之间的持续时间。
- 延迟：这是 **Pre-userinit** 和 **Userinit** 子阶段与 **Userinit** 和 **Shell** 子阶段之间的累积时间延迟。

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更多处理，这可能会导致登录持续时间大于阶段总和。
总登录时间不包括 ICA 空闲时间，即应用程序的 ICA 文件下载与 ICA 文件启动之间的时间。
要在应用程序启动时自动打开 ICA 文件，请对浏览器进行配置以在下载 ICA 文件时自动启动 ICA 文件。有关详细信息，请参阅 CTX804493。

> 注意：
> “登录持续时间”图形会显示各登录阶段（秒）。任何小于一秒的持续时间值都将显示为次秒值。大于一秒的值将四舍五入为最接近的 0.5 秒值。此图形可将最大 y 轴值显示为 200 秒。任何大于 200 秒的值都显示为实际值，位于栏上方。

故障排除提示

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持续时间以及最近七天此交付组中所有用户的平均持续时间进行比较。

如有必要请进行上报。例如，如果 VM 启动速度缓慢，可能是虚拟机管理程序存在问题，因此您可以将问题上报给虚拟机管理程序管理员。或者，如果代理速度缓慢，您可以将该问题上报给站点管理员，让其检查 Delivery Controller 上的负载平衡情况。

检查异常的差异，其中包括：

- 缺少（当前）登录栏
- 当前持续时间与此用户平均持续时间之间存在很大差异。原因包括：
  - 已安装新应用程序。
  - 发生操作系统更新。
  - 更改了配置。
  - 用户配置文件很大。在这种情况下，“配置文件加载”值很大。
- 用户的登录次数（当前持续时间和平均持续时间）与交付组平均持续时间之间存在很大差异。

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，例如 VM 启动或代理方面的问题。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

重影用户

January 21, 2022

在 Director 中，使用重影用户功能直接在用户的虚拟机或会话中进行查看或操作。可以重影 Windows 和 Linux VDA。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。

Director 在新选项卡中启动重影，应更新您的浏览器设置以允许来自 Director URL 的弹出窗口。

从用户详细信息视图访问重影功能。选择用户会话，然后在“活动管理器”视图或“会话详细信息”面板中单击重影。

重影 **Linux VDA**

重影适用于运行 RHEL 7.3 或 Ubuntu 16.04 Linux 发行版的 Linux VDA 7.16 版及更高版本。

> 注意：
>
> - 必须可从 Director UI 访问 VDA，才能使用重影。因此，仅当 Linux VDA 与 Director 客户端在同一 Intranet 中时，才能对其使用重影。
> - Director 使用 FQDN 连接到目标 Linux VDA。确保 Director 客户端可以解析 Linux VDA 的 FQDN。
> - VDA 必须安装了 python websockify 和 x11vnc 软件包。
> - 与 VDA 的 noVNC 连接使用 WebSocket 协议。默认情况下，使用 **ws://** WebSocket 协议。出于安全原因，Citrix 建议您使用安全 **wss://** 协议。在每个 Director 客户端和 Linux VDA 上安装 SSL 证书。

按照会话重影中的说明为 VDA 配置重影。

1. 单击重影后，重影连接将初始化，并且用户设备上将显示确认提示。
2. 指示用户单击是启动计算机或会话共享。
3. 管理员只能查看重影的会话。

重影 **Windows VDA**

可使用 Windows 远程协助重影 Windows VDA 会话。在安装 VDA 时，启用用户 **Windows** 远程协助功能。有关详细信息，请参阅启用或禁用功能。

1. 单击重影后，重影连接将初始化，并且将显示一个对话框，提示您打开或保存.msrc 事件文件。
2. 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。
3. 指示用户单击是启动计算机或会话共享。
4. 要执行更多控制操作，请要求用户共享键盘和鼠标控制。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

简化用于重影的 **Microsoft Internet Explorer** 浏览器

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

November 17, 2021

在 Director 中，向连接到一台或多台计算机的用户发送消息。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。该消息将显示在用户的计算机中。

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。

解决应用程序故障

November 17, 2021

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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

对于多会话操作系统计算机和单会话操作系统计算机，系统将列出与每个断开连接的会话对应的应用程序。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	选择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	如果您拥有所需的权限，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”，此操作仅适用于单会话操作系统计算机。或者，在“计算机详细信息”视图中，使用电源控制项重新启动或关闭计算机。指示用户再次登录，以便您重新检查应用程序。对于多会话操作系统计算机，重新启动选项不可用。而是需要用户注销，然后再重新登录。
将计算机置于维护模式	如果计算机的映像需要维护（如安装修补程序或其他更新），请将计算机置于维护模式。在“计算机详细信息”视图中，单击详细信息，然后打开维护模式选项。上报给相应的管理员。

还原桌面连接

November 17, 2021

从 Director 的用户标题栏检查当前计算机的用户连接状态。

如果桌面连接失败，将会显示导致连接失败的错误，以帮助您确定如何进行故障排除。

操作	说明
确保计算机未处于维护模式	请确保在用户详细信息页面上已关闭维护模式。
重新启动用户的计算机	选择计算机，然后单击重新启动。如果用户的计算机没有响应或无法连接，请使用此选项。例如，当计算机使用的 CPU 资源量异常高时，这可能会使 CPU 无法使用。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

还原会话

November 17, 2021

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多会话操作系统计算机。对于非代理会话，则禁用此选项。
从用户的会话注销	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。也可以重影该用户，以便更加密切地监视此会话。

运行 **HDX** 通道系统报告

November 17, 2021

在用户详细信息视图的 **HDX** 面板中，检查用户计算机上 HDX 通道的状态。只有在用户计算机使用 HDX 连接时，才可使用此面板。

如果出现了一条指示当前无法获取信息的消息，请等待一分钟以便页面进行刷新，或选择刷新按钮。HDX 数据更新时间比其他数据更新时间稍长。

单击错误或警告图标，以了解更多信息。

> 提示：
>
> 可以在同一对话框中，通过单击标题栏左角的向左和向右箭头，查看其他通道的相关信息。

HDX 通道系统报告主要供 Citrix 技术支持用来进行进一步的故障排除。

1. 在 HDX 面板中，单击下载系统报告。
2. 可以查看或保存.xml 报告文件。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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。

重置用户配置文件

November 17, 2021

> 小心：
>
> 重置配置文件后，用户的文件夹和文件将保存并复制到新配置文件中。但是，大多数用户配置文件数据都会被删除（例如，重置注册表，应用程序设置可能会被删除）。

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. 指示用户重新登录。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。

上述步骤假定您使用的是 Citrix Virtual Desktops（桌面 VDA）。如果您使用的是 Citrix Virtual Desktops（服务器 VDA），则需要登录平台才能执行配置文件重置。用户随后需要注销，然后重新登录才能完成配置文件重置。

如果配置文件未能成功重置（例如，用户无法成功重新登录计算机或部分文件已丢失），您必须手动还原原始配置文件。

用户配置文件中的文件夹（及其文件）将保存并复制到新配置文件中。将按照所列顺序复制这些文件：

- 桌面
- cookie
- 收藏夹
- 文档
- 图片
- 音乐
- 视频

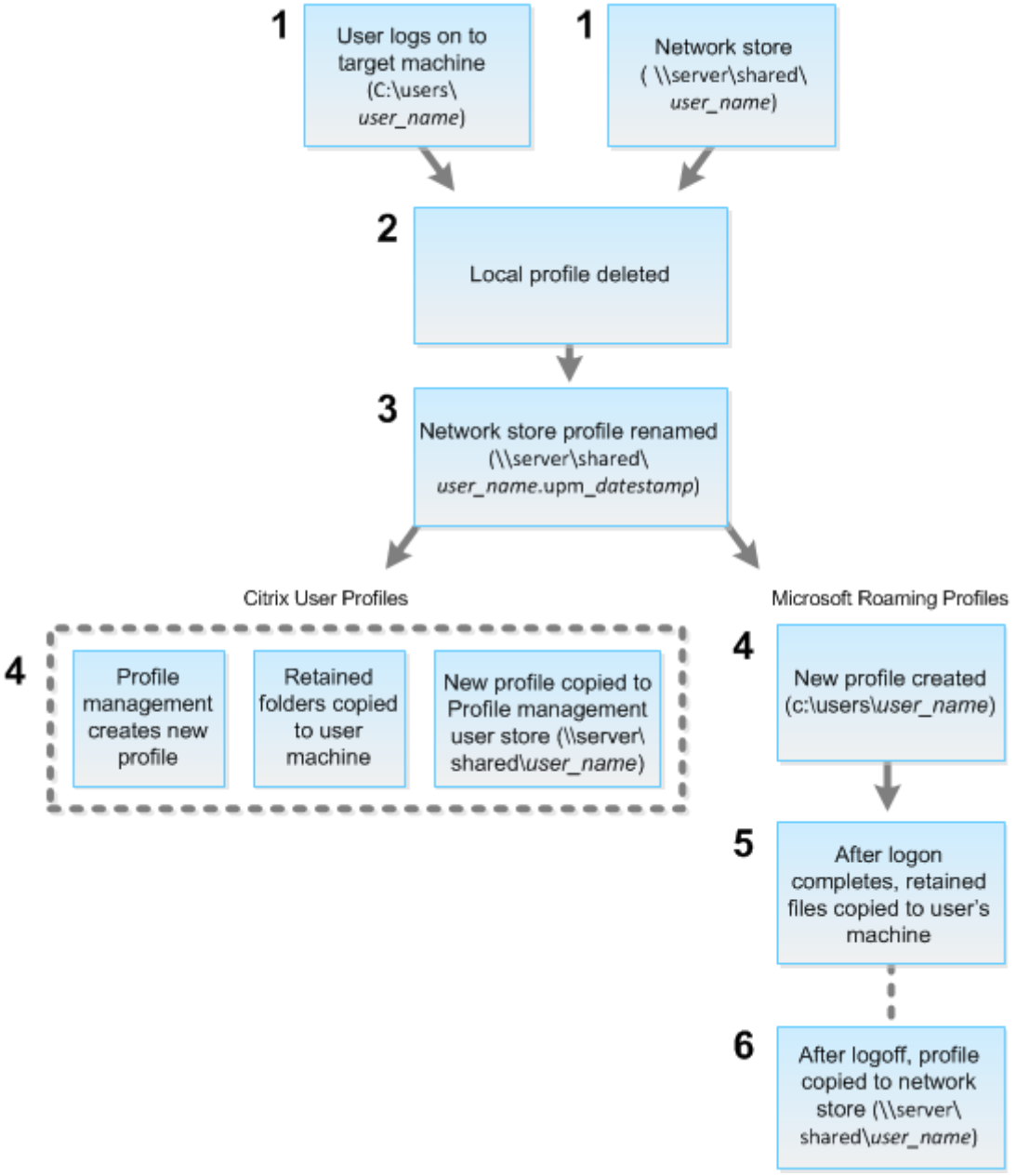
> 注意：
>
> 在 Windows 8 或更高版本中，重置配置文件时不会复制 Cookie。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

如何处理重置配置文件

所有 Citrix 用户配置文件或 Microsoft 漫游配置文件均可重置。在用户注销并且您选择重置命令（在 Director 中或使用 PowerShell SDK）后，Director 首先识别正在使用的用户配置文件并发出相应的重置命令。Director 通过 Profile Management 接收信息，包括有关配置文件大小、类型和登录时间的信息。

下图显示了重置用户配置文件时用户登录后的过程。



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）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. 如果存在本地配置文件，则会将其删除。
2. 重命名网络配置文件。
3. 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，使用 Profile Management 导入规则创建新配置文件。文件夹被复制回网络配置文件，用户可以正常登录。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。如有必要，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，Windows 将创建一个新配置文件，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。

重置失败后手动还原配置文件

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. 使用原始配置文件名称重命名存档的文件夹。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。

使用 **PowerShell SDK** 重置配置文件

可以使用 Broker PowerShell SDK 重置配置文件。

New-BrokerMachineCommand

创建排队等待传递给特定用户、会话或计算机的命令。有关此 cmdlet 的详细信息，请参阅https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerMachineCommand/。

示例

有关如何使用 PowerShell cmdlet 重置配置文件的详细信息，请参阅以下示例：

重置 Profile Management 配置文件

- 假设您要重置 user1 的配置文件。使用 New-BrokerMachineCommand PowerShell 命令。例如：

```
- New-BrokerMachineCommand -Category UserProfileManager -CommandName
  "ResetUpmProfile"-DesktopGroups 1 -CommandData $byteArray -
  SendTrigger logon -user domain1\user1
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 重要：
>
> `CommandData $byteArray` 必须使用以下格式：`<SID>[,<backup path>]`。如果未提供备份路径，Profile Management 将生成按当前日期和时间命名的备份文件夹。

重置 Windows 漫游配置文件

- 假设您要重置 user1 的漫游配置文件。使用 New-BrokerMachineCommand PowerShell 命令。例如：

```
- New-BrokerMachineCommand -Category UserProfileManager -CommandName
  "ResetRoamingProfile"-DesktopGroups 1 -CommandData $byteArray
  -SendTrigger logon -user domain1\user1
```

录制会话

January 21, 2022

在 Director 中，可以使用用户详细信息和计算机详细信息中的 Session Recording 控件录制 ICA 会话。**Premium** 站点上的客户可以使用此功能。

要使用 DirectorConfig 工具在 Director 中配置 Session Recording，请参阅创建和激活录制策略中的将 **Director** 配置为使用 **Session Recording Server** 部分。
仅当已登录的用户具有修改 Session Recording 策略的权限时，Session Recording 控件才会在 Director 中可用。可以在 Session Recording Authorization 控制台上设置此权限，如创建和激活录制策略中所述。

> 注意：
> 通过 Director 或 Session Recording 策略控制台对 Session Recording 设置所做的更改自后续的 ICA 会话开始生效。

Director 中的 **Session Recording** 控件

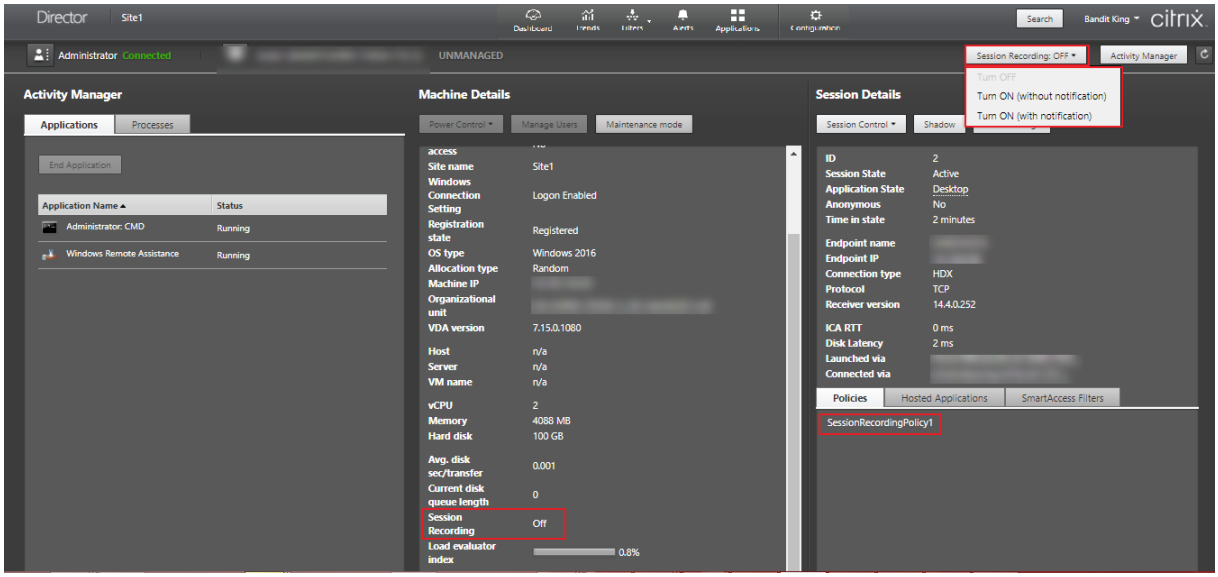
可以在活动管理器或用户详细信息屏幕中为特定用户启用 Session Recording。将在受支持的所有服务器上针对特定用户录制后续会话。

您可以：

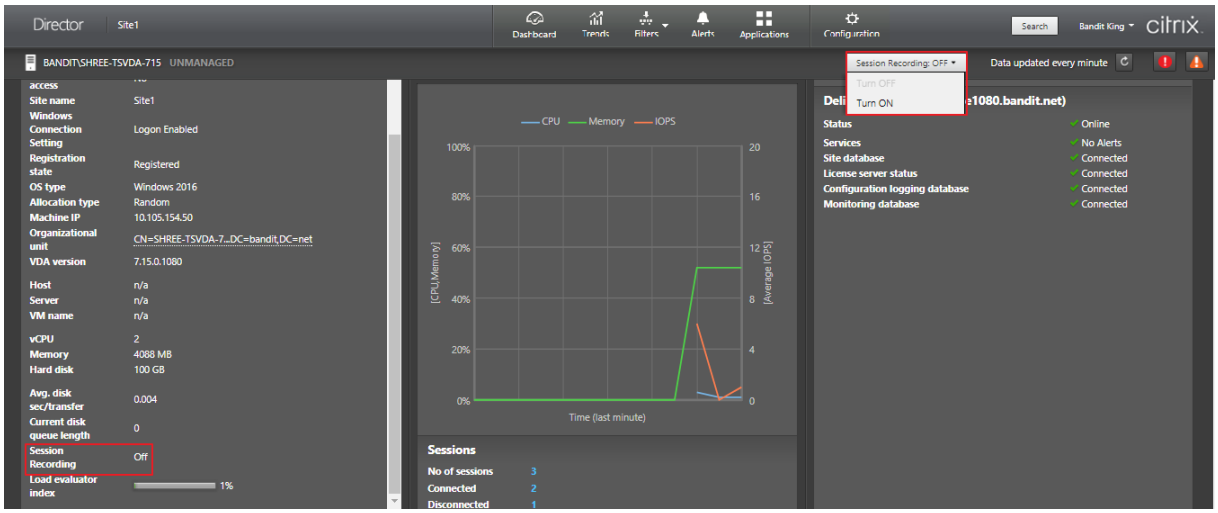
- 打开 (并通知) - 用户登录 ICA 会话时会收到将录制会话的通知。
- 打开（但不通知）- 无提示录制会话，不通知用户。
- 关闭 - 对用户禁用会话录制。

策略面板显示活动 Session Recording 策略的名称。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



可以从“计算机详细信息”页面为特定计算机启用 Session Recording。该计算机上的后续会话将被录制。计算机详细信息面板显示该计算机的 Session Recording 策略状态。



功能兼容性列表

August 2, 2022

Citrix Director 7 2106 与以下版本兼容：

- Citrix Virtual Apps and Desktops 7 2103 及更高版本
- Citrix Virtual Apps and Desktops 7 1912 LTSR

在每个站点中，尽管可以在早期版本的 Delivery Controller 中使用 Director，但是可能无法使用最新版本的 Director 中的所有功能。Citrix 建议使用相同版本的 Director、Delivery Controller 和 VDA。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 升级 Delivery Controller 后，系统将在您打开 Studio 时提示您升级站点。有关详细信息，请参阅升级部署中的升级顺序部分。

在 Director 升级后第一次登录时，将在配置的站点上执行版本检查。如果有任何站点运行的 Controller 版本低于 Director 的版本，则 Director 控制台上会显示一条消息，建议进行站点升级。此外，只要站点的版本低于 Director 的版本，Director 控制板中便会一直显示通知，指示这一不匹配的情况。

> 注意：
>
> Citrix Director 的早期版本不显示应用到在最新版本的 VDA 上运行的用户会话的策略。Citrix Director 1912 及更早版本不显示应用到在 VDA 2003 及更高版本上运行的用户会话的策略。使用 Citrix Director 2003 及更高版本查看这些策略。

下面列出了最低版本的 Delivery Controller (DC)、VDA 和许可版本所需的其他依赖组件中可用的特定 Director 功能。

Director 版本	功能	依赖组件 - 所需的最低版本	版本
1909	使用 Citrix Analytics for Performance 配置本地站点	DC 7 1906 和 VDA 1906	全部
1906	会话自动重新连接	DC 7 1906 和 VDA 1906	全部
1906	会话启动持续时间	DC 7 1906 和 VDA 1903	全部
1906	桌面探测	DC 7 1906 和 Citrix Probe Agent 1903	Premium
7.9 及更高版本	配置文件加载过程中 Citrix Profile Management 的持续时间	VDA 1903	全部
1811	配置文件深入分析	DC 7 1811 和 VDA 1811	全部
1811	虚拟机管理程序警报监视	DC 7 1811	Premium
1811	应用程序探测	DC 7 1811 和 Citrix Application Probe Agent 1811	Premium
1811	Microsoft RDS 许可证运行状况	DC 7 1811 和 VDA 7.16	全部
1811	显示关键 RTOP 数据	DC 7 1811 和 VDA 1808	Premium
1808	导出过滤器数据	DC 7 1808	全部

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Director 版本	功能	依赖组件 - 所需的最低版本	版本
1808	交互式会话深入分析	DC 7 1808 和 VDA 1808	全部
1808	GPO 深入分析	DC 7 1808 和 VDA 1808	全部
1808	使用 OData API 时可用的计算机历史数据	DC 7 1808	全部
7.18	应用程序探测	DC 7.18	Premium（以前称为 Platinum）
7.18	智能警报策略	DC 7.18	Premium（以前称为 Platinum）
7.18	Health Assistant 链接	无	全部
7.18	交互式会话深入分析	无	全部
7.17	PIV 智能卡身份验证	无	全部
7.16	应用程序分析	DC 7.16 和 VDA 7.15	全部
7.16	OData API V.4	DC 7.16	全部
7.16	重影 Linux VDA 用户	VDA 7.16	全部
7.16	域本地组支持	无	全部
7.16	计算机控制台访问	DC 7.16	全部
7.15	应用程序故障监视	DC 7.15 和 VDA 7.15	全部
7.14	以应用程序为中心的故障排除	DC 7.13 和 VDA 7.13	全部
7.14	磁盘监视	DC 7.14 和 VDA 7.14	全部
7.14	GPU 监视	DC 7.14 和 VDA 7.14	全部
7.13	“会话详细信息”面板上的传输协议	DC 7.x 和 VDA 7.13	全部
7.12	用户友好的连接和计算机故障说明	DC 7.12 和 VDA 7.x	全部
7.12	提高了 Enterprise Edition 中历史数据的可用性	DC 7.12 和 VDA 7.x	Enterprise
7.12	自定义报告	DC 7.12 和 VDA 7.x	Premium（以前称为 Platinum）
7.11	资源利用率报告	DC 7.11 和 VDA 7.11	全部

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Director 版本	功能	依赖组件 - 所需的最低版本	版本
7.11	针对 CPU、内存和 ICA RTT 条件扩展了警报	DC 7.11 和 VDA 7.11	Premium（以前称为 Platinum）
7.11	导出报告改进	DC 7.11 和 VDA 7.x	全部
7.11	与 Citrix ADM 集成	DC 7.11、VDA 7.x 和 MAS 11.1 Build 49.16	Premium（以前称为 Platinum）
7.9	登录持续时间细分	DC 7.9 和 VDA 7.x	全部
7.7	主动监视和警告	DC 7.7 和 VDA 7.x	Premium（以前称为 Platinum）
7.7	SCOM 集成	DC 7.7、VDA 7.x、SCOM 2012 R2 和 PowerShell 3.0	Premium（以前称为 Platinum）
7.7	Windows 身份验证集成	DC 7.x 和 VDA 7.x	全部
7.7	单会话和多会话操作系统使用情况	DC 7.7 和 VDA 7.x	Premium（以前称为 Platinum）
7.6.300	支持 Framehawk 虚拟通道	DC 7.6 和 VDA 7.6	全部
7.6.200	Session Recording 集成	DC 7.6 和 VDA 7.x	Premium（以前称为 Platinum）
7	HDX Insight 集成	DC 7.6、VDA 7.x 和 Citrix ADM	Premium（以前称为 Platinum）

数据粒度和保留

November 17, 2021

数据值聚合

Monitor Service 收集各种数据，其中包括用户会话使用情况、用户登录性能详细信息、会话负载平衡详细信息，以及连接和计算机故障信息。根据其类别，数据以不同的方式聚合。了解使用 OData Method API 提供的数据值的聚合是解释数据的关键。例如：

- 一段时间内发生的连接的会话故障和计算机故障。因此它们显示为一段时间内的最大值。
- 登录持续时间是时间长度的度量，因此它们显示为一段时间内的平均值。
- 登录计数和连接失败次数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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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，该分钟内的所有会话（无论它们是否重叠）都被视为并发。时间间隔的大小非常小，以致计算精度所涉及的性能开销不值得增加。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。

关联汇总表和原始数据

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。
- 原始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任何数据。尽管存在这些部分时间间隔的原始数据，但绝不会汇总这些原始数据。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。如上一部分内容中所述，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，但是原始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原始数据时，必须考虑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。在连接高可用性期间，当前连接的汇总数据计数会存在误差，但是会话实例仍在原始数据中运行。
- 数据保留期限。汇总表中的数据保留整理计划不同于原始事件数据的计划。由于数据已从汇总表或原始表格加以整理，因此可能会有所缺失。不同粒度的汇总数据的保留期限可能也有所差异。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特定粒度，未接收到某个粒度的数据并不表示在同一时间段内不存在更高粒度的数据。
- 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。

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 - 使用每分钟粒度。
- 0 < T <= 30 天 - 使用每小时粒度。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- T > 31 天 - 使用每天粒度。

非来源于聚合数据的请求数据来源于原始会话和连接信息。此数据往往增长很快，因此具有自己的整理设置。通过整理可确保仅长期保留相关数据。整理功能可以确保实现更好的性能，同时维护报告所需的粒度。获得 Premium 许可的站点上的客户可以将整理保留期限更改为他们所需的保留天数，否则将使用默认值。

要访问设置，请在 Delivery Controller 上运行以下 PowerShell 命令：

```
asnp Citrix.*
 Get-MonitorConfiguration
 Set-MonitorConfiguration -<setting name> <value>
<!--NeedCopy-->
```

	设置名称	受影响的整理	Premium 默认值（天）	非 Premium 默认值（天）
1	GroomSessionsRetentionDays	会话终止后的会话和连接记录保留期限	90	7
2	GroomFailuresRetentionDays	MachineFailureLog 和 ConnectionFailureLog 记录	90	7
3	GroomLoadIndexesRetentionDays	LoadIndex 记录	90	7
4	GroomDeletedRetentionDays	LifecycleState 为“Deleted”的 Machine、Catalog、DesktopGroup 和 Hypervisor 实体。此设置还将删除任何相关的 Session、SessionDetail、Summary、Failure 或 LoadIndex 记录。	90	7

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

	设置名称	受影响的整理	Premium 默认值（天）	非 Premium 默认值（天）
5	GroomSummariesRetentionDays	DesktopGroupSummary、FailureLog-Summary 和 LoadIndex-Summary 记录。聚合数据 - 日粒度。	90	7
6	GroomMachineHotfixLogRetentionDays	应用至 VDA 和 Controller 计算机的修补程序	90	90
7	GroomMinuteRetentionDays	聚合数据 - 分钟粒度	3	3
8	GroomHourlyRetentionDays	聚合数据 - 小时粒度	32	7
9	GroomApplicationInstanceRetentionDays	应用程序实例历史记录	90	0
10	GroomNotificationRetentionDays	通知日志记录	90	
11	GroomResourceUsageRawDataRetentionDays	资源利用率数据 - 原始数据	1	1
12	GroomResourceUsageMinuteDataRetentionDays	资源利用率汇总数据 - 分钟粒度	7	7
13	GroomResourceUsageHourlyDataRetentionDays	资源利用率汇总数据 - 小时粒度	30	7
14	GroomResourceUsageDayDataRetentionDays	资源利用率汇总数据 - 天粒度	90	7
15	GroomProcessUsageRawDataRetentionDays	进程利用率数据 - 原始数据	1	1
16	GroomProcessUsageMinuteDataRetentionDays	进程利用率数据 - 分钟粒度	3	3
17	GroomProcessUsageHourlyDataRetentionDays	进程利用率数据 - 小时粒度	7	7
18	GroomProcessUsageDayDataRetentionDays	进程利用率数据 - 天粒度	30	7
19	GroomSessionMetrics-DataRetentionDays	会话指标数据	1	1
20	GroomMachineMetrics-DataRetentionDays	计算机指标数据	3	3
21	GroomMachineMetrics-SummaryDataRetentionDays	计算机指标汇总数据	90	7

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

	设置名称	受影响的整理	Premium 默认值（天）	非 Premium 默认值（天）
22	GroomApplicationInstanceRetentionDays	应用程序实例数据	1	1
23	GroomApplicationUsageRetentionDays	应用程序使用数据	1	1

> 小心：
>
> 修改 Monitor Service 数据库上的值需要重新启动此服务才能使新值生效。建议仅在 Citrix 技术支持人员的指导下修改 Monitor Service 数据库。

设置 GroomProcessUsageRawDataRetentionDays、GroomResourceUsageRawDataRetentionDays 和 GroomSessionMetricsDataRetentionDays 限制到其默认值 1，而 GroomProcessUsageMinuteDataRetentionDays 限制到期默认值 3。用于设置这些值的 PowerShell 命令已被禁用，因为进程使用数据增长速度较快。
此外，基于许可证的保留设置如下所示：

- **Premium** 许可的站点 **-** 所有设置的整理保留期限为 1000 天（Citrix 建议 365 天）。
- 获得了 **Advanced** 许可的站点 **-** 所有设置的整理保留期限都限制为 31 天。
- 所有其他站点 **-** 所有设置的整理保留期限都限制为 7 天。

例外：

- 只能在获得 Premium 许可的站点中设置 GroomApplicationInstanceRetentionDays。
- GroomApplicationErrorsRetentionDays 和 GroomApplicationFaultsRetentionDays 在获得 Premium 许可的站点中被限制为 31 天。

长期保留数据会对表格大小产生以下影响：

- 小时数据。如果允许小时粒度的数据在数据库中最多保留两年，具有 1000 个交付组的站点将导致数据库按以下方式增长：

  1000 个交付组 x 24 小时/天 x 365 天/年 x 2 年 = 17,520,000 行数据。聚合表中存在如此巨大的数据量对性能的影响是非常显著的。如果从此表格提取控制板数据，将需要使用大型数据库服务器。数据量过大可能会对性能造成巨大影响。

- 会话和事件数据。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），此数据的增长速度很快。例如，经过两年时间，这些表格中收集的数据将超过 1 TB，这将要求使用企业级高端数据库。

Citrix Director 故障原因和故障排除

July 5, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

下表介绍了各种故障类别、原因以及解决问题所需采取的措施。有关详细信息，请参阅枚举、错误代码和说明。

连接失败错误

类别	原因	问题	操作
不适用	[0] 未知。此错误代码未映射。	监视服务无法根据代理服务共享的信息确定报告的启动或连接失败的原因。	在控制器上收集 CDF 日志并联系 Citrix 技术支持。
[0] 无	[1] 无	无	不适用
[2] MachineFailure	[2] SessionPreparation	从 Delivery Controller 向 VDA 发送的会话准备请求失败。可能的原因：Controller 和 VDA 之间的通信问题、Broker Service 在创建准备请求过程中遇到的问题，或导致 VDA 不接受请求的网络问题。	有关导致 Controller 与 VDA 之间的通信问题的常见问题，请参阅知识中心文章在 Citrix Virtual Apps and Desktops 中对 Virtual Desktop Agent 在 Delivery Controller 中的注册进行故障排除中列出的故障排除步骤。
[2] MachineFailure	[3] RegistrationTimeout	VDA 已打开，但尝试在 Delivery Controller 中注册时发生超时。	确认 Citrix Broker Service 是否正在 Delivery Controller 上运行，以及 Desktop Service 是否正在 VDA 上运行。如果停止，则将启动每一个。
[1] ClientConnection-Failure	[4] ConnectionTimeout	准备好 VDA 以启动会话之后客户端未连接到 VDA。会话已被成功代理，但等待客户端连接到 VDA 时发生超时。可能的原因：防火墙设置、网络中断或阻止远程连接的设置。	查看 Director 控制台，了解客户端当前是否具有活动连接，这意味着所有用户都不受影响。如果不存在会话，请查看客户端和 VDA 上的事件日志中是否记录了任何错误消息。解决客户端与 VDA 之间的网络连接存在的任何问题。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

类别	原因	问题	操作
[4] NoLicensesAvailable	[5] 许可	许可请求失败。可能的原因：许可证数量不足或许可证服务器已关闭 30 天以上。	确认许可证服务器是否已联机且可访问。请解决与许可证服务器有关的所有网络连接问题或重新启动许可证服务器（如果可能出现故障）。确认环境中是否具有足够的许可证，并根据需要分配更多许可证。
[1] ClientConnection-Failure	[6] 票据处理	创建票据期间出现故障，指出客户端与 VDA 的连接与代理的请求不匹配。启动请求票据是通过 Broker 准备的，在 ICA 文件中提供。当用户尝试启动会话时，VDA 将通过 Broker 验证 ICA 文件中的启动票据。可能的原因：ICA 文件损坏或用户正在尝试建立未经授权的连接。	根据在交付组中定义的用户组确认用户是否有权访问应用程序或桌面。指示用户重新启动应用程序或桌面以确定这是否是一次性问题。如果此问题再次出现，请查看客户端设备事件日志中记录的错误消息。验证用户正在尝试连接到的 VDA 是否已注册。如果未注册，请检查 VDA 上的事件日志并解决与注册有关的所有问题。
[1] ClientConnection-Failure	[7] 其他	在客户端最初联系 VDA 之后、完成连接顺序之前已将会话报告为从 VDA 终止。	确认会话是否在启动之前被用户终止。尝试重新启动会话，如果问题仍然存在，请收集 CDF 日志并联系 Citrix 技术支持。
[1] ClientConnection-Failure	[8] GeneralFail	会话无法启动。可能的原因：已请求执行代理的启动，但 Broker 仍在启动或初始化，或启动的代理阶段出现内部错误。	确认 Citrix Broker Service 是否正在运行并重新尝试启动会话。
[5] 配置	[9] MaintenanceMode	VDA 或 VDA 所属的交付组是在维护模式下设置的。	确定是否需要维护模式。如果不需要，请在有问题的交付组或计算机上禁用维护模式，并指示用户尝试重新连接。
[5] 配置	[10] ApplicationDisabled	最终用户无法访问该应用程序，因为它已被管理员禁用。	如果应用程序可供生产使用，请启用该应用程序并指示用户重新连接。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

类别	原因	问题	操作
[4] NoLicensesAvailable	[11] LicenseFeature Refused	正在使用的功能不在现有许可证的涵盖范围内。	联系 Citrix 销售代表，确认现有 Citrix Virtual Apps and Desktops 许可证版本和类型涵盖的功能。
[3] NoCapacityAvailable	[13] SessionLimitReached	所有 VDA 都在使用中，没有容量来托管更多会话。可能的原因：所有 VDA 都在使用中（针对单会话操作系统 VDA），或所有 VDA 都已达到所配置的最大允许并发会话数（针对多会话操作系统 VDA）。	确认是否存在处于维护模式的任何 VDA。如果不需要释放更多容量，请禁用维护模式。考虑增加 Citrix 策略设置中最大会话数的值，以允许每个服务器 VDA 上运行更多会话。考虑添加更多多会话操作系统 VDA。考虑添加更多单会话操作系统 VDA。
[5] 配置	[14] DisallowedProtocol	不允许使用 ICA 和 RDP 协议。	在 Delivery Controller 上运行 **Get-BrokerAccessPolicyRule PowerShell** 命令并验证 **AllowedProtocols** 值是否列出了所需的所有协议。仅当存在配置错误时才会出现此问题。
[5] 配置	[15] ResourceUnavailable	用户尝试连接的应用程序或桌面不可用。此应用程序或桌面可能不存在，或者没有可用于运行此应用程序或桌面的 VDA。可能的原因：应用程序或桌面未发布，或托管应用程序或桌面的 VDA 已达最大负载，或应用程序或桌面是在维护模式下设置的。	确认应用程序或桌面是否仍处于已发布状态，以及 VDA 是否未处于维护模式。确定多会话操作系统 VDA 是否处于满载状态。如果满载，请预配更多多会话操作系统 VDA。确认是否存在可供连接的单会话操作系统 VDA。如有需要，请预配更多单会话操作系统 VDA。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

类别	原因	问题	操作
[5] 配置	[16] ActiveSessionReconnectDisabled	ICA 会话处于活动状态，并且连接到不同的端点。但是，由于活动会话重新连接已禁用，因此，客户端无法连接到活动会话。	在 Delivery Controller 上，确认活动会话重新连接是否已启用。确认注册表中 **HKEY_LOCAL_MACHINE\Software** 下的 **DisableActiveSessionReconnect** 的值是否设置为 0。
[2] MachineFailure	[17] NoSessionToReconnect	客户端尝试重新连接到特定会话，但该会话已终止。	重新尝试执行工作区控制重新连接。
[2] MachineFailure	[18] SpinUpFailed	无法为会话启动打开 VDA 的电源。这是虚拟机管理程序报告的问题。	如果计算机仍处于关闭状态，请尝试从 Citrix Studio 启动计算机。如果失败，请查看虚拟机管理程序的连接性和权限。如果 VDA 是 PVS 预配的计算机，请在 PVS 控制台中确认该计算机是否正在运行。如果未运行，请验证是否已为该计算机分配虚拟磁盘，然后登录虚拟机管理程序以重置 VM。
[2] MachineFailure	[19] 被拒绝	Delivery Controller 向 VDA 发送了准备建立来自最终用户的连接请求，但 VDA 主动拒绝了该请求。	通过 ping 确认 Delivery Controller 是否能够成功与 VDA 通信。如果不成功，请解决所有防火墙或网络路由问题。
[2] MachineFailure	[20] ConfigurationSetFailure	Delivery Controller 在会话启动过程中未向 VDA 发送所需的配置数据，例如，策略设置和会话信息。可能的原因：Controller 和 VDA 之间的通信问题、创建配置设置请求时 Broker Service 遇到的问题，或导致 VDA 不接受请求的网络问题。	-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

类别	原因	问题	操作
[3] NoCapacityAvailable	[21] MaxTotalInstance-sExceeded	已达到应用程序的实例数上限。不能在 VDA 上打开更多应用程序实例。此问题与应用程序限制功能有关。	如果许可允许，请考虑将应用程序设置将同时运行的实例数限制为增大到更大的值。
[3] NoCapacityAvailable	[22] MaxPerUserIn-stancesExceeded	用户正在尝试打开某个应用程序的多个实例，但该应用程序配置为仅允许每个用户打开应用程序的一个实例。此问题与应用程序限制功能有关。	默认情况下，仅允许每个用户使用一个应用程序实例。如果要求每个用户运行多个实例，请考虑取消选中应用程序设置中的限制每个用户一个实例设置。
[1] ClientConnection-Failure	[23] Communication error	Delivery Controller 尝试向 VDA 发送信息 (例如，准备建立连接请求)，但通信尝试期间出现错误。此问题可能是由于网络中断导致的。	如果已启动，请在 VDA 上重新启动桌面服务以重新启动注册过程并验证 VDA 是否已成功注册。请通过应用程序事件日志中的详细信息确认为 VDA 配置的 Delivery Controller 是否准确无误。
[3] NoCapacityAvailable	[100] NoMachineAvailable Monitoring service converts [12] NoDesktopAvailable to this error code.	所分配的用于启动会话的 VDA 处于无效状态或者不可用。可能的原因：VDA 的电源状态未知或不可用、VDA 自最后一个用户的会话结束之后未重新启动、会话共享已禁用，但当前会话需要启用该功能，或 VDA 已从交付组或站点中删除。	验证 VDA 是否在交付组中。如果没有，请将其添加到相应的交付组中。确认注册的 VDA 数量是否充足且处于已就绪状态，能够启动用户请求的已发布共享桌面或应用程序。确认托管 VDA 的虚拟机管理程序是否未处于维护模式。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

类别	原因	问题	操作
[2] MachineFailure	[101] MachineNotFunctional. Monitoring service converts [12] NoDesktopAvailable to this error code.	VDA 无法运行。可能的原因：VDA 已从交付组中删除、VDA 未注册、VDA 电源状态不可用或 VDA 遇到内部问题。	验证 VDA 是否在交付组中。如果没有，请将其添加到相应的交付组中。验证 VDA 在 Citrix Studio 中是否显示为已打开电源。如果多台计算机的电源状态未知，请解决与虚拟机管理程序连接或主机故障有关的任何问题。确认托管 VDA 的虚拟机管理程序是否未处于维护模式。解决这些问题后，重新启动 VDA。

计算机故障类型

错误代码	错误代码 ID	问题	操作
未知	-	-	-
未注册	3	-	-
MaxCapacity	4	虚拟机管理程序上的负载指数已达到其最大容量。	确保所有虚拟机管理程序都已启动。向虚拟机管理程序中添加更多容量。添加更多虚拟机管理程序。
StuckOnBoot	2	VM 未完成其启动顺序，并且不与虚拟机管理程序通信。	确保 VM 已在虚拟机管理程序上成功启动。检查 VM 上的其他消息，例如操作系统问题。确保已在 VM 上安装虚拟机管理程序工具。确保已在 VM 上安装 VDA。
FailedToStart	1	尝试在虚拟机管理程序上启动时 VM 遇到问题。	查看虚拟机管理程序日志。
无	0	-	-

计算机取消注册原因（故障类型为“未注册”或“未知”时适用）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

错误代码	错误代码 ID	问题	操作
AgentShutdown	0	VDA 出现正常关机。	如果根据现有的电源管理策略，您不希望 VDA 关闭，请打开 VDA 的电源。查看事件日志中记录的任何错误。
AgentSuspended	1	VDA 处于休眠或睡眠模式。	使 VDA 退出休眠模式。考虑通过电源设置对 Citrix Virtual Apps and Desktops VDA 禁用休眠。
IncompatibleVersion	100	由于 Citrix 协议版本不匹配，VDA 无法与 Delivery Controller 通信。	调整 VDA 与 Delivery Controller 的版本，使其保持一致。
AgentAddressResolutionFailed	101	Delivery Controller 无法解析 VDA 的 IP 地址。	验证 AD 中是否存在 VDA 计算机帐户。如果没有，请创建。验证 DNS 中 VDA 的名称和 IP 地址是否准确。如果没有，请纠正。如果普遍存在，请验证 Delivery Controller 上的 DNS。通过运行 `nslookup` 命令从 Controller 验证 DNS 解析。
	101	Delivery Controller 无法解析 VDA 的 IP 地址。	验证 AD 中是否存在 VDA 计算机帐户。如果没有，请创建。验证 DNS 中 VDA 的名称和 IP 地址是否准确。如果没有，请纠正。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

错误代码	错误代码 ID	问题	操作
AgentNotContactable	102	Delivery Controller 与 VDA 之间出现通信问题。	使用 ping 验证 Delivery Controller 是否可以与 VDA 成功通信。如果没有，请解决任何防火墙或网络问题。有关导致 Controller 与 VDA 之间的通信问题的常见问题，请参阅知识中心文章在 Citrix Virtual Apps and Desktops 中对 Virtual Desktop Agent 在 Delivery Controller 中的注册进行故障排除 (CTX136668) 中列出的故障排除步骤。
	102	Delivery Controller 与 VDA 之间出现通信问题。	有关导致 Controller 与 VDA 之间的通信问题的常见问题，请参阅知识中心文章在 Citrix Virtual Apps and Desktops 中对 Virtual Desktop Agent 在 Delivery Controller 中的注册进行故障排除 (CTX136668) 中列出的故障排除步骤。联系 Citrix 技术支持。
AgentWrongActiveDirectoryOU	103	发生了 Active Directory 发现错误配置。在 VDA 注册表中配置的站点特定的 OU (其中，站点控制器信息存储在 AD 中) 适用于不同的站点。	确保 Active Directory 配置正确无误，或者检查注册表设置。
EmptyRegistrationRequest	104	从 VDA 发送到 Delivery Controller 的注册请求为空。这可能是由于损坏的 VDA 软件安装导致的。	重新启动 VDA 上的 Desktop Service 以重新启动注册过程，并通过应用程序事件日志确认 VDA 是否已正确注册。
MissingRegistrationCapabilities	105	VDA 版本与 Delivery Controller 不兼容。	升级 VDA，或者删除 VDA 并重新安装。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

错误代码	错误代码 ID	问题	操作
MissingAgentVersion	106	VDA 版本与 Delivery Controller 不兼容。	如果此问题影响所有计算机，请重新安装 VDA 软件。
InconsistentRegistrationCapabilities	107	VDA 无法向 Broker 传达自己的功能。这可能是由于 VDA 与 Delivery Controller 版本之间的不兼容导致的。注册功能（因版本而异）是使用与注册请求不匹配的格式表示的。	调整 VDA 与 Delivery Controller 的版本，使其保持一致。
NotLicensedForFeature	108	您正在尝试使用的功能未获许可。	检查您的 Citrix Licensing 版本，或者删除 VDA 并重新安装。
	108	您正在尝试使用的功能未获许可。	联系 Citrix 技术支持。
UnsupportedCredentialSecurity 版本	109	VDA 与 Delivery Controller 使用的加密机制不同。	调整 VDA 与 Delivery Controller 的版本，使其保持一致。
InvalidRegistrationRequest	110	VDA 向 Broker 发出了注册请求，但请求的内容已损坏或无效。	有关导致 Controller 与 VDA 之间的通信问题的常见问题，请参阅知识中心文章在 Citrix Virtual Apps and Desktops 中对 Virtual Desktop Agent 在 Delivery Controller 中的注册进行故障排除 (CTX136668) 中列出的故障排除步骤。
SingleMultiSessionMismatch	111	VDA 的操作系统类型与计算机目录或交付组不兼容。	将 VDA 添加到正确的计算机目录类型或包含安装了相同操作系统的计算机的交付组。
FunctionalLevelTooLowForCatalog	112	为计算机目录设置的 VDA 功能级别高于所安装的 VDA 版本。	确认 VDA 的计算机目录功能级别是否与 VDA 的功能级别匹配。升级或降级计算机目录以匹配 VDA 的计算机目录。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

错误代码	错误代码 ID	问题	操作
FunctionalLevelTooLowForDesktopGroup	102	为交付组设置的 VDA 功能级别高于所安装的 VDA 版本。	确认 VDA 的交付组功能级别是否与 VDA 的功能级别匹配。升级或降级计算机目录以匹配 VDA 的计算机目录。
PowerOff	200	VDA 未正常关闭。	如果假定 VDA 已启动，请尝试从 Citrix Studio 中启动 VDA，并验证其是否能够正确启动并注册。任何启动或注册问题故障排除。备份后检查 VDA 上的事件日志，以帮助确定关闭的根本原因。
AgentRejectedSettingsUpdate	203	已更改或更新 Citrix 策略等设置，但向 VDA 发送更新时出错。如果更新与所安装的 VDA 版本不兼容，则可能会出现此问题。	根据需要升级 VDA。检查 VDA 版本是否支持应用的更新。
SessionPrepareFailure	206	Broker 未完成 VDA 上正在运行的会话的审核。	如果普遍存在，请重新启动 Delivery Controller 上的 Citrix Broker Service。
	206	Broker 未完成 VDA 上正在运行的会话的审核。	联系 Citrix 技术支持。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

错误代码	错误代码 ID	问题	操作
ContactLost	207	Delivery Controller 与 VDA 断开连接。这可能是由网络中断造成的。	确认 Citrix Broker Service 是否正在 Delivery Controller 上运行，以及 Desktop Service 是否正在 VDA 上运行。如果停止，则将启动每一个。如果已启动，请在 VDA 上重新启动桌面服务以重新启动注册过程并验证 VDA 是否已成功注册。请通过应用程序事件日志中的详细信息确认为 VDA 配置的 Delivery Controller 是否准确无误。使用 ping 验证 Delivery Controller 是否可以与 VDA 成功通信。如果没有，请解决任何防火墙或网络问题。
	207	Delivery Controller 与 VDA 断开连接。这可能是由网络中断造成的。	验证 Desktop Service 是否正在 VDA 上运行。如果已停止，请启动。
BrokerRegistrationLimitReached	201	Delivery Controller 已达到允许所配置的 VDA 同时在其中注册的最大数量。默认情况下，Delivery Controller 允许 10000 个并发 VDA 注册。	考虑向站点中添加 Delivery Controller 或者创建一个新站点。还可以通过 **HKEY_LOCAL_MACHINE\Software** 注册表项增加允许在 Delivery Controller 中同时注册的 VDA 数量。有关详细信息，请参阅知识中心文章 Citrix Virtual Apps and Desktops 使用的注册表项 (CTX117446)。对于 Controller 而言，增加此数字可能需要更多的 CPU 和内存资源。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

错误代码	错误代码 ID	问题	操作
SettingsCreationFailure	208	Broker 未构建一组要发送到 VDA 的设置和配置。如果 Broker 无法收集数据，注册将失败，VDA 将取消注册。	检查 Delivery Controller 上的事件日志中是否记录了任何错误。如果日志中未明确记录某个特定问题，请重新启动 Broker Service。重新启动 Broker Service 后，重新启动受影响的 VDA 上的 Desktop Service，并确认这些 VDA 是否已成功注册。
	208	Broker 未构建一组要发送到 VDA 的设置和配置。如果 Broker 无法收集数据，注册将失败，VDA 将取消注册。	重新启动受影响的 VDA 上的 Desktop Service，并确认这些 VDA 是否已成功注册。联系 Citrix 技术支持。
SendSettingsFailure	204	Broker 未向 VDA 发送设置和配置数据。如果 Broker 能够收集但无法发送数据，注册将失败。	如果限制到单个 VDA，请重新启动 VDA 上的 Desktop Service 以强制重新注册，并通过应用程序事件日志验证 VDA 是否已成功注册。请解决发现的所有错误。有关导致 Controller 与 VDA 之间的通信问题的常见问题，请参阅知识中心文章在 Citrix Virtual Apps and Desktops 中对 Virtual Desktop Agent 在 Delivery Controller 中的注册进行故障排除 (CTX136668) 中列出的故障排除步骤。
AgentRequested	2	出现未知错误。	联系 Citrix 技术支持。
DesktopRestart	201	出现未知错误。	联系 Citrix 技术支持。
DesktopRemoved	202	出现未知错误。	联系 Citrix 技术支持。
SessionAuditFailure	205	出现未知错误。	联系 Citrix 技术支持。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

错误代码	错误代码 ID	问题	操作
UnknownError	300	出现未知错误。	联系 Citrix 技术支持。
RegistrationStateMismatch	302	出现未知错误。	联系 Citrix 技术支持。
未知	-	出现未知错误。	联系 Citrix 技术支持。

第三方声明

November 17, 2021

本版本的 Citrix Virtual Apps and Desktops 可能包含根据在以下文档中定义的条款获得使用许可的第三方软件：

- Citrix Virtual Apps and Desktops 第三方声明（PDF 下载）
- 面向 FlexNet Publisher 2017 (11.15.0.0) 的非商用软件披露（PDF 下载）
- FlexNet Publisher 文档补充：FlexNet Publisher 11.15.0 中使用的第三方软件和开源软件

SDK 和 API

January 21, 2022

此版本提供多种 SDK 和 API。有关详细信息，请参阅开发人员文档。在该文档中，可以访问以下对象的编程信息：

- Delivery Controller
- Monitor Service OData
- StoreFront

Citrix Group Policy SDK 可用来显示并配置组策略设置和过滤器。它使用 PowerShell 提供程序创建与计算机和用户的设置及过滤器相对应的虚拟驱动器。提供程序以 New-PSDrive 扩展的形式显示。要使用组策略 SDK，必须安装 Studio 或 Citrix Virtual Apps and Desktops SDK。有关详细信息，请参阅 Group Policy SDK。

Delivery Controller SDK

SDK 由多个 PowerShell 管理单元组成，在安装 Delivery Controller 或 Studio 时，安装向导会自动安装这些管理单元。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Citrix Virtual Apps 或 Citrix Virtual Desktops，但 Citrix 建议，对于常规操作，应创建具有相应权限的 Citrix 管理员，而不要使用本地管理员帐户。

访问并运行 cmdlet：

1. 在 PowerShell 中启动 shell：打开 Studio，选择 **PowerShell** 选项卡，然后单击启动 **PowerShell**。
2. 要在脚本内使用 SDK cmdlet，应在 PowerShell 中设置执行策略。有关 PowerShell 执行策略的详细信息，请参阅 Microsoft 文档。

   > 注意：
   >
   > 当前 SDK 可同时作为 PowerShell 管理单元和 PowerShell 模块进行安装。
   >
   > 通过添加模块功能，您可以使用此 SDK 的 cmdlet，而不使用如前所述的 `Add-PSSnapin`（或 `asnp`）cmdlet。
   >
   > 对于仅作为管理单元安装的关联组件的 SDK（如 Citrix Licensing、Citrix Provisioning 和 StoreFront），使用它们的 cmdlet 仍然需要如前所述的 `Add-PSSnapin`（或 `asnp`）。
   >
   > 如果要通过管理单元使用此 SDK，请继续执行下一步。

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 单元属于版本 1。Citrix Virtual Apps and Desktops 以及早期版本的 XenDesktop 7 管理单元属于版本 2。例如，要安装 Citrix Virtual Apps and Desktops 管理单元，请键入 `Add-PSSnapin Citrix.ADIdentity.Admin.V2`。要导入所有 cmdlet，请键入：`Add-PSSnapin Citrix.*.Admin.V*`

添加管理单元后，可以访问 cmdlet 及其关联的帮助。

要查看当前的 Citrix Virtual Apps and Desktops PowerShell cmdlet 帮助，请执行以下操作：

1. 在 PowerShell 控制台中，添加 Citrix 管理单元：`Add -PSSnapin Citrix.*.Admin.V*`。
2. 请按照 Windows PowerShell ISE 中的说明进行操作。

Group Policy SDK

要使用组策略 SDK，必须安装 Studio 或 Citrix Virtual Apps and Desktops 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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Monitor Service OData

监视 API 允许使用版本为 3 或 4 的 OData API 访问 Monitor Service 数据。可以根据从 Monitor Service 数据中查询的数据创建自定义监视和报告控制板。OData V.4 基于 ASP.NET Web API，并且支持聚合查询。有关详细信息，请参阅 Monitor Service OData API。

© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).