



# Citrix DaaS

Contents

概述	10
新增功能	18
已知问题	93
弃用	94
系统要求	97
限制	102
技术安全性概述	105
<b>Citrix 托管 Azure 的技术安全性概述</b>	<b>112</b>
交付方法	122
入门：规划和构建部署	125
注册 <b>Citrix DaaS</b>	132
适用于 <b>Windows 365</b> 的 <b>Citrix HDX</b>	135
适用于 <b>Amazon WorkSpaces Core</b> 的 <b>Citrix DaaS</b> （预览版）	135
适用于 <b>Google Cloud</b> 的 <b>Citrix DaaS</b>	148
使用 <b>DaaS</b> 入门指南（预览版）	148
计算机标识	161
已加入 <b>Active Directory</b>	163
已加入 <b>Azure Active Directory</b>	163
<b>Microsoft Intune</b>	166
已加入混合 <b>Azure Active Directory</b>	167
未加入域	170
设置资源位置	172
<b>AWS</b> 虚拟化环境	175



<b>Google Cloud</b> 虚拟化环境	<b>181</b>
<b>HPE Moonshot</b> 虚拟化环境（预览版）	<b>187</b>
<b>Microsoft Azure Resource Manager</b> 虚拟化环境	<b>188</b>
<b>Microsoft System Center Virtual Machine Manager</b> 虚拟化环境	<b>189</b>
<b>Nutanix</b> 虚拟化环境	<b>191</b>
<b>Nutanix</b> 云和合作伙伴解决方案	<b>192</b>
<b>VMware</b> 虚拟化环境	<b>194</b>
<b>VMware</b> 云和合作伙伴解决方案	<b>194</b>
<b>XenServer</b> 虚拟化环境	<b>218</b>
<b>Cloud Connector</b> 的大小和规模注意事项	<b>219</b>
安装 <b>VDA</b>	<b>226</b>
使用命令行安装 <b>VDA</b>	<b>244</b>
创建和管理连接和资源	<b>251</b>
与 <b>AWS</b> 的连接	<b>262</b>
与 <b>Google Cloud</b> 环境的连接	<b>277</b>
连接到 <b>HPE Moonshot</b> （预览版）	<b>290</b>
与 <b>Microsoft Azure</b> 的连接	<b>293</b>
与 <b>Microsoft System Center Virtual Machine Manager</b> 的连接	<b>314</b>
与 <b>Nutanix</b> 的连接	<b>315</b>
与 <b>Nutanix</b> 云和合作伙伴解决方案的连接	<b>316</b>
与 <b>VMware</b> 的连接	<b>318</b>
与 <b>VMware</b> 云和合作伙伴解决方案的连接	<b>325</b>
连接到 <b>XenServer</b>	<b>326</b>
创建计算机目录	<b>328</b>

创建 <b>AWS</b> 目录	351
创建 <b>Google</b> 云端平台目录	361
创建 <b>HPE Moonshot</b> 计算机目录（预览版）	380
创建 <b>Microsoft Azure</b> 目录	381
创建 <b>Microsoft System Center Virtual Machine Manager</b> 目录	473
创建 <b>Nutanix</b> 目录	476
创建 <b>VMware</b> 目录	477
创建 <b>XenServer</b> 目录	481
创建不同加入类型的目录	484
创建加入了 <b>Azure Active Directory</b> 的目录	485
创建支持 <b>Microsoft Intune</b> 的目录	494
创建加入了混合 <b>Azure Active Directory</b> 的目录	496
创建未加入域的目录	498
管理计算机目录	499
管理 <b>AWS</b> 目录	536
管理 <b>Google</b> 云端平台目录	541
管理 <b>HPE Moonshot</b> 目录（预览版）	547
管理 <b>Microsoft Azure</b> 目录	548
管理 <b>Microsoft System Center Virtual Machine Manager</b> 目录	563
管理 <b>VMware</b> 目录	564
管理 <b>XenServer</b> 目录	567
电源管理	569
对 <b>AWS VM</b> 进行电源管理	570
对 <b>Azure VM</b> 进行电源管理	573

安全策略	586
安全组	586
安全启动	587
加密功能	588
快速部署	589
快速部署入门	593
使用快速部署创建目录	595
在快速部署中管理目录	605
快速部署中的 <b>Azure</b> 订阅	615
快速部署中的映像	621
快速部署中的网络连接	630
快速部署中的用户和身份验证	646
快速部署中的 <b>Remote PC Access</b>	652
在快速部署中进行监视	660
快速部署中的故障排除	666
快速部署参考	669
创建交付组	678
管理交付组	686
创建应用程序组	709
管理应用程序组	715
<b>Remote PC Access</b>	720
删除组件	731
用户个性化层	732
升级 <b>VDAs</b>	749

将配置迁移到 <b>Citrix Cloud</b>	<b>763</b>
从本地迁移到云	<b>777</b>
将多个站点合并到一个站点中	<b>780</b>
从云迁移到云	<b>787</b>
自动配置工具 <b>cmdlet</b>	<b>790</b>
自动配置故障排除及其他信息	<b>813</b>
使用 <b>Image Portability Service</b> 在资源位置之间迁移工作负载	<b>820</b>
打印	<b>838</b>
策略	<b>839</b>
使用策略	<b>841</b>
策略模板	<b>843</b>
创建策略	<b>847</b>
策略集（预览版）	<b>852</b>
对策略进行优先排序、建模、比较和故障排除	<b>855</b>
<b>HDX 概述</b>	<b>858</b>
<b>Citrix ICA</b> 虚拟通道	<b>867</b>
<b>Citrix DaaS</b> 中的双跃点	<b>876</b>
<b>HDX 传输</b>	<b>878</b>
自适应传输	<b>878</b>
<b>Rendezvous</b> 协议	<b>885</b>
<b>Rendezvous V1</b>	<b>886</b>
<b>Rendezvous V2</b>	<b>889</b>
<b>HDX Direct</b> （预览版）	<b>894</b>
<b>NAT</b> 兼容性	<b>900</b>

故障排除	901
设备	904
客户端驱动器映射 (CDM)	905
通用 USB 设备	906
支持移动和触摸屏客户端设备	907
串行端口	911
专业键盘	916
<b>TWAIN 设备</b>	<b>918</b>
网络摄像机	918
<b>WIA 设备</b>	<b>918</b>
图形	919
<b>HDX 3D Pro</b>	<b>921</b>
适用于 <b>Windows</b> 多会话操作系统的 <b>GPU</b> 加速	922
适用于 <b>Windows</b> 单会话操作系统的 <b>GPU</b> 加速	923
<b>Thinwire</b>	<b>927</b>
基于文本的会话水印	932
多媒体	933
音频功能	935
浏览器内容重定向	942
<b>HDX</b> 视频会议和网络摄像机视频压缩	<b>950</b>
<b>HTML5</b> 多媒体重定向	<b>953</b>
<b>Microsoft Teams</b> 的优化	<b>956</b>
<b>Windows Media</b> 重定向	<b>990</b>
常规内容重定向	<b>991</b>

客户端文件夹重定向	991
双向内容重定向配置	992
主机到客户端重定向	994
双向内容重定向	997
本地应用程序访问和 <b>URL</b> 重定向	1000
通用 <b>USB</b> 重定向和客户端驱动器注意事项	1006
管理	1015
自适应访问	1016
<b>Device Posture</b>	1017
自适应身份验证服务	1017
基于用户网络位置的自适应访问	1017
应用程序包	1027
<b>AutoScale</b>	1037
开始使用 <b>Autoscale</b>	1038
基于计划和基于负载的设置	1044
动态会话超时	1063
自动缩放带标记的计算机（云突发）	1065
动态预配计算机	1072
用户注销通知（以前是强制用户注销）	1077
分析 <b>AutoScale</b> 设置的有效性	1080
<b>Broker PowerShell SDK</b> 命令	1082
<b>Cloud Health Check</b>	1085
配置日志记录	1119
委派管理	1124

完整配置界面的主页	1139
许可证	1142
多类型许可	1143
平衡计算机负载	1147
本地主机缓存	1148
使用搜索监视和管理计算机和会话	1158
计算机操作和列	1163
会话操作和列	1173
管理安全密钥	1176
会话恢复设置	1191
标记	1197
时区设置	1206
对 <b>VDA</b> 注册和会话启动问题进行故障排除	1207
用户访问	1209
虚拟 <b>IP</b> 和虚拟环回	1212
区域	1215
<b>Monitor</b>	1224
站点分析	1225
警报和通知	1232
过滤数据以排除故障	1241
监视站点的历史趋势	1243
监视 <b>Autoscale</b> 托管的计算机	1247
部署故障排除	1249
应用程序故障排除	1249

应用程序探测	1252
桌面探测	1257
计算机故障排除	1261
对用户问题进行故障排除	1269
诊断会话启动问题	1273
诊断用户登录问题	1277
重影用户	1282
向用户发送消息	1283
解决应用程序故障	1284
还原桌面连接	1285
还原会话	1286
运行 <b>HDX</b> 通道系统报告	1286
重置用户配置文件	1287
录制会话	1290
功能兼容性列表	1292
委派管理和监视	1295
数据粒度和保留	1298
会话启动诊断	1301
适用于 <b>Citrix Service Provider</b> 的 <b>Citrix DaaS</b>	1345
<b>Citrix Gateway</b> 服务	1352
<b>SDK 和 API</b>	1352



### 概述

March 30, 2024

### 简介

Citrix DaaS 是一项提供应用和桌面虚拟化的服务，允许 IT 人员控制本地或云端托管的虚拟机、应用和安全，同时为任何设备提供随时随地的访问。最终用户可以独立于设备的操作系统和界面使用应用程序和桌面。

通过 Citrix DaaS，您可以向任何设备交付安全的虚拟应用程序和桌面，而将大多数安装、设置和升级工作留给 Citrix 处理。您负责在任何设备上交付最佳用户体验的同时维护对应用程序、策略和用户的完全控制。

Citrix DaaS 允许您在混合部署中一起管理本地数据中心和公有云工作负载。您可以连接到公有云 Microsoft Azure、Amazon Web Services (AWS) 和 Google Cloud 以及本地虚拟机管理程序，例如 XenServer、Microsoft Hyper-V、Nutanix AHV 和 VMware vSphere。通过混合云、多云方法，您可以灵活地在全球不同的资源位置部署不同的应用程序。

Citrix DaaS 提供了多种交付应用程序和桌面的方法。

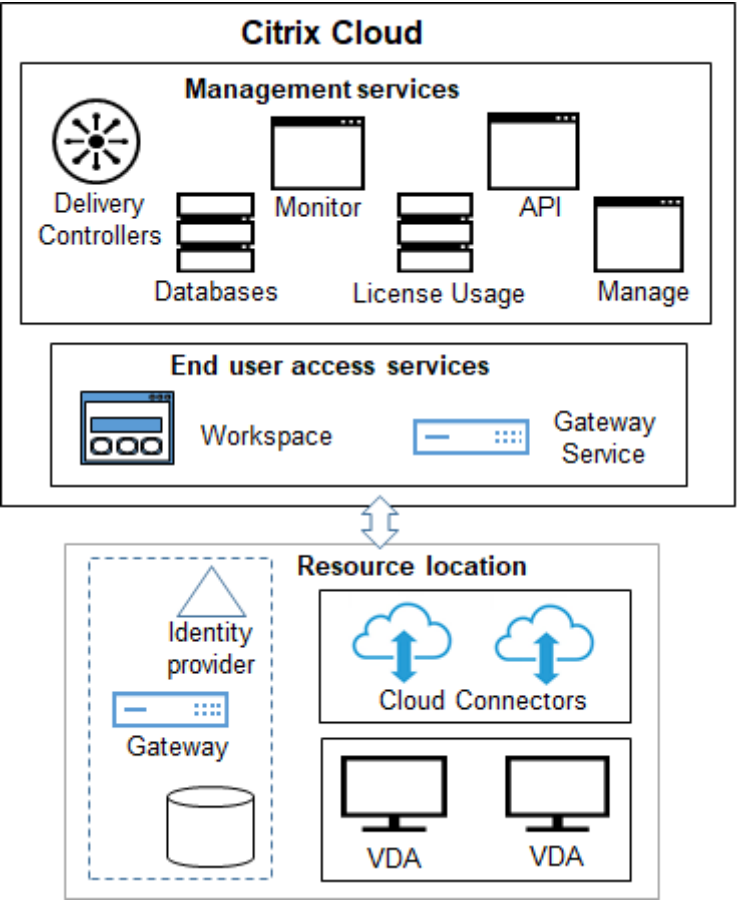
- [交付方法](#)介绍了主要的方法，包括用例和优势/劣势。
- [交付模型](#)列出了更多选择，还提供了 VDI 模型比较。

Citrix 托管的 Azure 进一步简化了虚拟应用程序和桌面的部署。借助 Citrix 托管 Azure，Citrix 还可以管理 Azure 工作负载的托管。

[了解有关使用此服务的优势的更多信息。](#)

### 站点概览

下图显示了 Citrix 管理员在 Citrix DaaS 生产部署（也称为站点）中使用的服务和组件。



如图所示，Citrix 负责管理 Citrix Cloud 中的用户访问和管理服务及组件。您交付给用户的应用程序和桌面位于一个或多个资源位置中的多台计算机上。在 Citrix DaaS 部署中，资源位置中包含访问层和资源层中的组件。每个资源位置都被视为一个区域。

如果您最近从 Citrix Virtual Apps and Desktops 迁移，则会看到 Citrix DaaS 消除了本地部署中所需的大多数组件设置工作。

### Citrix 管理的组件和服务

- **Delivery Controller**: Citrix DaaS 提供了对应用程序和桌面进行负载平衡、对用户进行身份验证、代理或优先处理直接来自云的连接的功能，而无需管理 Delivery Controller，就像管理 Citrix Virtual Apps and Desktops 一样。
- **数据库**: 站点配置、监视和配置日志记录数据由云服务进行存储，从而消除了本地 Citrix Virtual Apps and Desktops 产品的 SQL 数据库要求。
- **许可**: 管理许可证并提供使用情况统计信息。
- **管理界面**: 请参阅管理界面。许多任务也可在[服务 API](#) 中提供。

- **Monitor** 界面：通过 [Monitor](#) 界面，IT 支持人员和技术支持人员可以在问题变严重之前监视环境以及对问题进行故障排除，并且可以为最终用户执行支持任务。显示内容包括：

- 来自 Controller 中的 Broker Service 的实时会话数据，其中包括 Virtual Deliver Agent (VDA) 中的 Broker Agent 中的数据。
- 来自 Controller 中的 Monitor Service 的历史数据。
- 与 HDX 流量（又称为 ICA 流量）有关的数据。

- **Cloud Connector**：Cloud Connector 是 Citrix Cloud 中的组件与资源位置中的组件之间的通信通道。在资源位置中，Cloud Connector 用作 Citrix Cloud 中的 Delivery Controller 的代理。

每个资源位置至少包含一个 Cloud Connector。为了实现冗余，建议您使用两个或更多 Cloud Connector。

- 使用完整配置预配计算机时，请先从 Citrix Cloud 控制台安装 Cloud Connector。有关详细信息，请参阅 [Cloud Connector](#)。
- 使用快速部署来预配 Azure 计算机时，Citrix 将在创建目录时为您创建资源位置和 Cloud Connector。

安装 Cloud Connector 后，Citrix 将对其进行管理和更新。客户处理的唯一任务是 Cloud Connector Windows 更新和修补。

## 管理接口

从 Citrix DaaS 的管理选项卡中，您可以选择以下接口。

## 完整配置

在管理 > 完整配置界面中，可以执行以下操作：

- 从 [主页](#) 概述您的 Citrix DaaS 部署和最新功能。
- [创建与主机的连接](#) 并进行管理。
- [创建](#) 和 [管理](#) 包含您交付给用户的应用程序和桌面的计算机的目录。
- [创建](#) 和 [管理](#) 交付组（以及应用程序组，可选）。
- 创建和管理 [Citrix 策略](#)，这些策略会影响 HDX 技术和功能的使用与行为，以及站点级管理。这包括会话、自适应传输、设备、图形、多媒体、内容重定向和 VDA 的策略设置。
- 自定义 [委派管理](#) 以创建基于角色且具有特定授权范围的管理员。
- 管理 [Autoscale](#) 功能，以主动对交付应用程序和桌面的计算机进行电源管理。
- [平衡计算机负载](#)
- 对 VDA [运行状况检查](#) 以识别潜在问题并修复建议。
- [显示配置日志内容](#) 以查看配置更改和其他管理活动的发生时间以及发起人。

## 快速部署

在管理 > 快速部署界面中，您可以轻松部署和管理使用 Citrix 托管 Azure 订阅或自己的 Azure 订阅的 Microsoft Azure 工作负载。有关详细信息，请参阅[快速部署](#)和 Citrix 托管的 Azure。在快速部署中，您可以：

- [创建和管理](#)目录。
- [创建并自定义](#)映像，可以是来自各种 Citrix 准备的映像，也可以来自从 Azure 订阅导入的映像。

有关详细信息，请参阅[快速部署](#)。

## Environment Management

通过 **Environment Management** 界面，您可以使用智能资源管理和 Profile Management 技术提供最佳性能、桌面登录和应用程序响应时间。有关详细信息，请参阅 [Workspace Environment Management](#)。

## 客户管理的组件和技术

- **Citrix Gateway**：用户从公司防火墙外部连接时，Citrix DaaS 可以使用 Citrix 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 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 在 Citrix Cloud 中安装和管理 Citrix Gateway 服务。还可以选择在资源位置中安装 Citrix Gateway。

- **Active Directory**：Active Directory 用于身份验证和授权。它对用户进行身份验证，并确保其能够访问适当的资源。订阅者的身份定义了他们在 Citrix Cloud 中可以访问的服务。此身份来自从资源位置中的域提供的 Active Directory 域帐户。
- **身份提供程序 (IdP)**：IdP 是用户身份的最终授权。支持的 IdP 包括：本地 Active Directory、Active Directory + 令牌、Azure Active Directory、Citrix Gateway 和 Okta。有关详细信息，请参阅：
  - [Workspace 身份](#)
  - [身份识别和访问管理](#)

- **Virtual Delivery Agent (VDA)**：提供资源（应用程序和桌面）的每个物理机或虚拟机都必须在其上安装 Citrix VDA。VDA 建立并管理安装了 VDA 的计算机与用户设备之间的连接，并应用为会话配置的策略。

VDA 使用资源位置中的 Cloud Connector 作为代理，向 Delivery Controller 注册。

有几种 VDA 类型可供选择：

- 适用于 Windows 多会话操作系统的 VDA 允许多个用户同时连接到计算机。此 VDA 类型通常安装在 Windows 服务器上。
- 适用于 Windows 单会话操作系统的 VDA 允许一个用户一次连接到一台计算机。此 VDA 类型通常用于 VDI。

此 VDA 类型的核心版本可与 Remote PC Access 功能一起使用。它包含完整单会话 VDA 中的一部分功能。

- Linux VDA 支持基于 RHEL、CentOS、SUSE 或 Ubuntu 发行版的虚拟应用程序和桌面。

在本服务的文档中，“VDA”通常是指代理和安装了代理的计算机。

- 虚拟机管理程序和云服务：在大多数生产站点中，您向用户提供（发布）的应用程序和桌面实例（工作负载）都由[受支持的虚拟机管理程序或云服务](#)进行“托管”。（通常情况下，Remote PC Access 功能用于物理机。因此，它不使用虚拟机管理程序或云服务进行计算机预配。）
  - 使用完整配置界面时，您可以创建与受支持的主机虚拟机管理程序或云服务的连接。然后，在完整配置中，您可以使用映像（通过该主机创建）来创建包含应用程序和桌面实例的计算机目录。然后您将创建一个交付组。Citrix 提供了许多工具来简化和促进这些会话主机的构建和维护方式。
  - 使用快速部署交付 Azure 工作负载时，只需创建目录即可。尽管您可以在创建目录时使用自己的 Azure 订阅，但是使用 Citrix 托管的 Azure 订阅也无需管理主机。

您发布的应用程序和桌面实例可以在本地、托管在公有云中或同时托管在本地和公有云中。

- **Citrix StoreFront:** [Citrix StoreFront](#) 是云托管的 Citrix Workspace 的前代产品。它用作访问应用程序和桌面的 Web 界面。

可以选择在多个资源位置中安装 StoreFront 服务器。具有本地存储有助于在网络中断期间交付应用程序和桌面。[本地主机缓存](#)功能要求在每个资源位置中有一个由客户管理的 StoreFront。

请参阅[用户访问](#)，了解在服务环境中使用 StoreFront 的注意事项。

## 您配置的用于交付桌面和应用程序的对象

可以配置以下项目以在生产环境中交付应用程序和桌面。

- 主机连接：主机连接（上文已提及）有助于启用控制平面 (Citrix Cloud) 中的组件与资源位置中的 VDA 之间的通信。连接规格包括：
  - 用于访问主机的地址和凭据
  - 要使用的存储方法以及用于存储的计算机
  - VM 可以使用的网络

请记住：使用快速部署时，您不必创建连接。如果您使用 Citrix 托管的 Azure，Citrix 也会管理该托管。

- 目录：在完整配置和 Monitor 界面中，目录称为“计算机目录”。  
目录是具有相同操作系统类型的虚拟机或物理机的集合（例如，Windows 多会话、Ubuntu 单会话）。

When creating a catalog, you usually use an image, which is also known as a template. (Remote PC Access catalogs usually contain physical machines, so no image is needed.)

- When using Quick Deploy, Citrix provides several Citrix prepared images you can use to create your own customized images. Or, you can import images from your own Azure subscription.
- When using Full Configuration to create VMs using a supported host type, the image usually must be created and reside on a host machine. When creating the catalog, you provide the path to that image.

Regardless of where the image resides, you can install applications on the image, if you want those apps on all machines created from that image (and don't want to virtualize those apps).

After the image is ready, you create the catalog.

- For VMs, MCS creates the machines and the catalog.
- For Remote PC Access, MCS simply creates the catalog, because the physical machines already exist.

For more information about MCS, see [Image management](#).

- 交付组：交付组指定：

- 目录中的一台或多台计算机。
- 允许访问这些计算机的用户。
- 用户可以通过 **Workspace** 访问的应用程序和桌面。

使用快速部署时，系统会自动创建交付组。（它仅出现在完整配置界面中。）

- 应用程序组：应用程序组允许您管理应用程序的集合。可为在不同交付组之间共享的应用程序或由交付组中的部分用户使用的应用程序创建应用程序组。应用程序组是可选的。

## Citrix 托管 Azure

Citrix 托管 Azure 是多个 Citrix DaaS 版本中提供的选项。使用 Citrix 托管 Azure 可简化 Azure 中 Virtual Apps and Desktops 的部署。Citrix 负责管理托管 Azure 工作负载的基础结构。

借助 Citrix 托管 Azure，您可以获得专用 Citrix 托管 Azure 订阅和资源位置。在该 Azure 订阅中，您可以创建 VM 的目录。您可以：

- 从各种受支持的版本部署单会话和多会话 Windows 操作系统计算机或 Linux 操作系统计算机。
- 从精选区域的计算类型和存储选项精选列表中进行选择。
- 在这些计算机上预配持久或非持久工作负载。
- 从安装了最新 VDA 的几个 Citrix 提供的映像中进行选择。然后，在 Citrix 界面中，您可以从该模板构建自己的映像，然后对其进行自定义。还可以从您自己的 Azure 订阅导入和使用映像。

即使 Citrix 负责管理 Azure 容量，但如果您想通过自己的 Azure 订阅与现有资源进行通信，也可以使用 Azure VNet 对等连接资源。还可以使用 Citrix SD-WAN 直接连接到本地资源。

有关使用 Citrix 托管的 Azure 时的安全性和职责的信息，请参阅 [Citrix 托管的 Azure 的技术安全概述](#)。

### 订购 Citrix 托管 Azure

必须订阅受支持的 Citrix 服务产品，然后订购 Citrix 托管 Azure 消费基金，才能获得 Citrix 托管 Azure 订阅。可以通过 Citrix 或从 Azure 应用商店订购 Citrix DaaS 和消费基金。

以下服务产品支持 Citrix 托管 Azure：

- Citrix Workspace Premium Plus
- Citrix DaaS, Advanced、Advanced Plus 和 Premium Edition
- Citrix DaaS Standard for Azure 版本

有关详细信息，请参阅[注册 Citrix DaaS](#)。

### Citrix 托管 Azure 权益摘要

使用 Citrix 托管 Azure 具有以下多种优势：

- 获得混合云优势的最快速径。
- 减轻基础结构的 IT 管理负载。提供管理体验，让 IT 在没有管理和维护挑战的情况下掌控 IT。
- 使您能够快速扩展工作解决方案。
- 提供由 Citrix 管理和维护的单独 Azure 订阅。这将活动与您的其他 Azure 订阅隔离开来。
- 您保留使用自己的 Azure 订阅创建和管理工作负载的灵活性。您的部署可能包括使用 Citrix 托管 Azure 订阅的工作负载，以及使用自己（客户管理的）Azure 订阅的工作负载。
- 使用真正的基于消费的基础结构即服务 (IaaS) 模型。
- 有几种技术可用于创建与自己的本地网络的连接（例如 Azure VNet 对等互连和 SD-WAN）。这允许您的用户访问网络的资源，例如文件服务器。

通过此服务部署和管理 Citrix 托管的 Azure 将使用[快速部署](#)管理界面。

有关详细信息，请联系您的 Citrix 代表。

向用户交付应用程序和桌面

### Citrix Workspace

订阅者（用户）通过 Citrix Workspace 访问其桌面和应用程序。

安装并配置 Citrix DaaS 后，您将获得一个 Workspace URL 链接。Workspace URL 在两个位置发布：

- 在 Citrix Cloud 控制台中，从左上角的菜单中选择 **Workspace** 配置。“访问”选项卡包含 Workspace URL。
- 在 Citrix DaaS 欢迎页面中，Workspace URL 将显示在页面底部。

测试 Workspace URL 链接并与您的订阅者（用户）共享，以向其授予对应用程序和桌面的访问权限。您的订阅者无需任何额外的配置即可访问 Workspace URL。

可以从 Citrix Cloud 配置工作区。

- 指定与 Citrix Workspace 集成的服务。
- 自定义您的订阅者用来访问其工作区的 URL。
- 自定义订阅者的工作区外观，例如徽标、颜色和首选项。
- 指定订阅者如何对其工作区进行身份验证，例如使用 Active Directory 或 Azure Active Directory。
- 指定您的订阅者使用的资源位置的外部连接。

有关详细信息，请参阅 [Citrix Workspace](#)。

### Citrix Workspace 应用程序

在用户端，Citrix Workspace 应用程序安装在用户设备和其他端点上，例如虚拟桌面。通过 Citrix Workspace 应用程序，用户能够安全地从任何设备（包括智能手机、平板电脑和 PC）自助访问文档、应用程序和桌面。通过 Citrix 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 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 Workspace 应用程序适用于各种操作系统。有关详细信息，请参阅 [Citrix Workspace 应用程序](#)。

### 服务级别协议

Citrix DaaS 设计为使用行业最佳做法来实现云规模以及服务的高度可用性。

有关 Citrix 对 Citrix Cloud 服务的可用性的承诺的完整详细信息，请参阅[服务级别协议](#)。

可以在 <https://status.cloud.com> 上针对此目标持续监视性能。

### 限制

此服务级别目标的计算将不包括以下原因导致的可用性断开情况：

- 客户未能遵从 <https://docs.citrix.com> 上的产品文档中记录的 Citrix DaaS 的配置要求。
- 非 Citrix 管理的任何组件导致的可用性断开情况，包括但不限于客户控制的物理机和虚拟机、客户安装和维护的操作系统及软件、客户安装和控制的网络连接设备或其他硬件；客户定义和控制的安全设置、组策略以及其他配置策略；公有云提供商故障、Internet 服务提供上故障或超出 Citrix 控制的其他故障。
- 由于超出 Citrix 控制的原因导致的服务中断，包括自然灾害、战争或恐怖袭击、政府操作。



### 更多信息

- [Citrix DaaS 示意图](#)
- [Citrix DaaS 参考体系结构和部署方法](#)
- [技术安全性概述](#)
- [网络端口](#)
- [第三方声明](#)
- [系统要求](#)
- [功能](#)
  - [HDX 技术简介](#)，以及有关[设备](#)、[图形](#)和[多媒体](#)的详细信息。
  - [Remote PC Access](#)：允许用户从任意位置远程登录到办公室中的物理 PC。可以从完整配置或快速部署配置 Remote PC Access。
  - [发布内容](#)：发布仅作为资源的 URL 或 UNC 路径的应用程序。
  - [服务器 VDI](#)：从单个用户的服务器操作系统交付桌面。
- 有关 Citrix DaaS Standard for Azure，请参阅[其专用产品文档](#)。
- 要了解 Citrix DaaS 产品和版本中的功能可用性，请参阅 [Citrix DaaS 功能列表](#)。
- Citrix Cloud Learning 系列提供教育课程，帮助您启动并运行 Citrix Cloud 及其服务。可以按顺序查看所有模块，包括从简介到规划和构建服务的所有内容。还可以在模块中选择单个模块或特定于任务的区段。请参阅 [Cloud Learning 系列](#)。

### 入门

要了解如何设置部署，请从[规划和构建部署](#)开始。该摘要将指导您完成此过程中的主要步骤，并提供了指向更多信息和详细过程的链接。

### 新增功能

March 30, 2024

Citrix 的目标是在推出了新增功能和产品更新时向 Citrix DaaS 客户提供。新版本会带来更多的价值，应立即将更新告知客户。Citrix DaaS 的滚动更新大约每三周发布一次。

对您而言，此过程是透明的。初始更新仅应用于 Citrix 内部站点，然后逐步应用于客户环境。以分阶段的递增方式提供更新有助于确保产品质量并最大程度地保证可用性。

有关云规模和服务可用性方面的 Endpoint Management 服务级别目标的详细信息，请参阅[服务级别协议](#)。要监视服务中断情况和计划内维护，请参阅“[服务运行状况](#)”控制板。

## Virtual Delivery Agent (VDA)

适用于 Windows 计算机的 VDA 通常与 Citrix Virtual Apps and Desktops 产品同时发布。

- 有关新增 VDA 和 HDX 功能的信息，请参阅当前 Citrix Virtual Apps and Desktops 产品的[新增功能](#)和[已知问题](#)文章。
- 有关不再受支持的 VDA 平台和功能的信息，请参阅[弃用](#)。该文章还包括未来版本不支持的平台和功能（例如哪些操作系统支持 VDA 安装）。

### 重要：

如果 VDA 上曾安装过 Personal vDisk (PvD) 组件，则无法将该 VDA 升级到 1912 LTSR 或更高版本。要使用新 VDA，必须卸载当前 VDA，然后安装新 VDA。（即使您安装了 PvD 但从未使用，此指导也适用。）有关详细信息，请参阅[如果 VDA 安装了 Personal vDisk](#)。

## 2024 年 3 月

简化了计算机目录的子网更新。以前，要更改计算机目录的子网设置，必须将其删除并重新创建。使用此功能，您现在可以通过编辑目录来实现相同的功能。请注意，只有在目录下创建的新虚拟机才会位于新关联的子网上。此增强功能减少了对目录删除和相关任务的需求。有关详细信息，请参阅[编辑目录](#)。

完整配置：支持使用计算机配置文件更新更多 **Azure VM** 设置。有了完整配置，您现在可以通过计算机配置文件更新由 MCS 配置的 Azure VM 的更多设置，其中包括：

- 计算机规模
- 许可证类型
- 可用性区域
- 专用主机组 ID

更新计算机配置文件后，“完整配置”会将当前设置与新设置进行比较。如果存在差异，系统将提示您确认要申请哪个。这种设计可确保透明、高效地更新 VM 设置。

完整配置：支持更改 **MCS** 配置的 **Azure** 虚拟机的回写缓存属性。对于使用计算机创建服务 (MCS) 置备的 Azure VM，您现在可以使用完整配置更改其回写缓存 (WBC) 属性，例如 磁盘缓存大小、内存缓存大小和启用存储成本节省金额。此外，当您为这些虚拟机选择新的计算机大小或计算机配置文件时，完整配置会验证 WBC 设置以防止冲突，例如超过新选择的内存限制。如果发生冲突，系统将提示您重新配置 WBC 设置。

## 2024 年 2 月

从 **Workspace** 界面暂停虚拟机。现在，您可以通过 Workspace 用户界面暂停具有活动会话的永久虚拟机。此增强功能提供以下好处：

- 从上次停下的地方恢复系统。

- 与停止的已解除分配的计算机相比，启动时间更短。
- 性价比高且节能。
- 使用 AutoScale 功能进行高效的资源分配。

新 **Machine Creation Services (MCS)** 存储优化 (**MCSIO**) 支持：现在，当您为 MCS 配置准备映像时，您可以选择 Image Portability Service 添加或删除 MCSIO。

有关更多信息，请参阅[自动配置 VDA](#)。

探测器概述增强功能：探测指标和探测失败阶段的摘要现可在“探测”>“概述”页面中找到。“探测指标”显示计划的运行、失败的运行、跳过的运行和成功的运行次数。故障阶段的图形表示有助于分析大多数故障发生的阶段。此信息有助于快速对探测结果进行故障排除。有关详细信息，请参阅[应用程序和桌面探测](#)一文。

计算机目录页面上的映像信息。现在，您可以通过计算机目录的模板属性查看以下映像信息：

- 操作系统
- Machine Identity Service
- Machine Creation Services 存储
- 用于 Azure 部署的 `pagefile.sys` 的文件路径

此增强功能使映像信息更加清晰，并确保管理员将有关计算机目录的所有信息集中在一个地方。

对 **VDA** 注册令牌管理的全面配置支持。基于令牌的 VDA 注册可减少 Cloud Connector 的负载并减少潜在的故障点，非常适合使用非 Citrix Provisioning 技术准备计算机的用例。借助完整配置，您现在可以为非 Citrix 配置的 VDA 生成和管理注册令牌，从而简化基于注册令牌的部署。有关更多信息，请参阅[生成和管理注册令牌](#)。

**PowerShell** 日志记录。在完整配置中，您现在可以查看与您的日常用户界面操作相对应的 PowerShell 命令。此功能可帮助您深入了解底层 PowerShell 命令以供学习。要查看 PowerShell 日志，请转到日志记录 > **PowerShell**。有关详细信息，请参阅[配置日志记录](#)。

使用完整配置为单会话池 **VDA** 启用本地主机缓存 (**LHC**)。默认情况下，使用 MCS 或 Citrix Provisioning 置备的单会话池 VDA 在 LHC 模式下不可用。使用完整配置，您现在可以针对每个交付组覆盖此默认行为，从而使这些 VDA 在 LHC 期间可用于新连接。有关详细信息，请参阅[创建交付组和管理交付组](#)。

**Citrix Hypervisor** 在“完整配置”中更名为 **XenServer**。根据我们的品牌重塑战略，我们已将完整配置内的所有 Citrix Hypervisor 实例更新为 XenServer。

端到端网络跳跃视图。端到端网络跳转视图是加强 Citrix Monitor 故障排除工作流程的下一步。用户详细信息 > 会话性能 > 会话拓扑部分提供了连接的 HDX 会话的端到端网络跃点视图的直观表示。会话中路径有助于了解会话路径中涉及的组件及其元数据、组件之间的链接以及在 VDA 上发布的应用程序。会话拓扑有助于数据流动，以及识别可能会带来性能问题的特定跃点。

此外，当会话处于连接状态时，还会显示会话的 ICA 延迟和 ICA RTT 测量值。有关详细信息，请参阅[“端到端网络跃点”视图](#)。

使用主映像的磁盘加密 **ID (DES ID)** 对目录虚拟机的所有磁盘进行加密。以前，在 Azure 环境中，MCS 计算机目录的磁盘加密 ID (DES ID) 源自计算机配置文件或自定义属性。使用此功能，计算机目录还可以从主映像派生 DES ID，以加密目录中的 VMS 的所有磁盘。

更新 **MCS** 标签以在迁移后检测孤立资源。当您从本地配置迁移到云站点，或者从云配置迁移到另一个云站点时，由于站点 ID 标签过旧，无法正确检测到孤立资源。借助此功能，您可以使用 PowerShell 命令在迁移后更新永久目录的 MCS 站点 ID 标记，以便正确检测孤立资源。目前，此功能适用于 Azure。有关更多信息，请参阅[更新 MCS 标签以在迁移后检测孤立资源](#)。

在创建 **MCS** 计算机目录之前验证配置。借助此功能，您现在可以在使用 `New-ProvScheme` 命令中的 `-validate` 参数创建 MCS 计算机目录之前验证配置设置。使用该参数运行此 PowerShell 命令后，如果使用了错误的参数或某个参数与其他参数发生冲突，则会收到相应的错误消息。然后，您可以使用错误消息来解决问题，并使用 PowerShell 成功创建 MCS 计算机目录。

目前，此功能适用于 Azure、GCP 和 VMware 虚拟化环境。有关更多信息，请参阅[在创建 MCS 计算机目录之前验证配置](#)。

支持将标签从计算机配置文件源复制到 **AWS** 中的虚拟机。借助此功能，在 AWS 虚拟化环境中，您可以将计算机配置文件中指定的网卡和磁盘（身份磁盘、回写缓存磁盘和操作系统磁盘）上的标签复制到 MCS 计算机目录中新创建的虚拟机。可以在任何计算机配置文件源（AWS EC2 实例或 AWS 启动模板版本）中指定这些标记。此功能适用于永久计算机目录和非永久计算机目录和 VM。有关详细信息，请参阅[复制 VM 上的标记](#)。

**SCVMM** 支持计算机配置文件。。借助此功能，您现在可以使用计算机配置文件在 System Center Virtual Machine Manager (SCVMM) 环境中创建和更新 MCS 计算机目录。还可以启用嵌套的虚拟化和 vTPM。有关详细信息，请参阅[使用计算机配置文件创建目录](#)。

**Azure** 支持将现成 **VM** 与 **MCS** 配合使用。Azure 现成 VM 允许您利用 Azure 未使用的计算容量，从而节省大量成本。但是，由于其逐出策略，Azure 现成 VM 仅适用于某些非关键应用程序和桌面。

借助此功能，您可以使用计算机配置文件（VM 或模板规范）创建 Azure 现成 VM 的 MCS 计算机目录。可以更新现有目录以将 Azure 现成 VM 作为新创建的 VM，或者切换到使用标准 Azure VM。也可以将现有 VM 更新为 Azure 现成 VM。有关详细信息，请参阅[使用 Azure 现成 VM 创建目录](#)。

支持从计算机配置文件中捕获诊断设置。在 Azure 环境中，MCS 现在支持在创建或更新 MCS 计算机目录或更新现有 VM 时从计算机配置文件中捕获 VM 和 NIC 上的诊断设置。因此，通过这种实现，诊断数据可以无缝传输到指定的 Azure 目标端点，例如日志分析工作区或事件中心，以进行深入分析和可视化。有关详细信息，请参阅[从计算机配置文件中捕获 VM 和 NIC 上的诊断设置](#)。

**MCS** 支持管理计算机目录的不同版本。借助此功能，您可以使用 PowerShell 命令管理计算机目录的配置版本。每次使用 `Set-ProvScheme` 更改配置都会生成新的配置版本。您可以：

- 查看版本列表。
- 使用任何先前版本更新计算机目录。
- 如果虚拟机未使用某个版本，请手动删除该版本。
- 更改计算机目录要保留的最大版本数。

有关详细信息，请参阅[管理计算机目录的版本](#)。

在单会话和共享桌面 **VDA** 上发布 **App-V**、**MSIX** 和 **MSIX** 应用程序附加打包的应用程序。现在，您可以在单会话和共享桌面 VDA 上访问打包的应用程序，例如 App-V、MSIX 和 MSIX 应用附加。此增强功能可确保打包的应用程序在您

登录时随时可用。此功能有助于更加快速地启动打包的应用程序，并通过使其更接近访问本地安装的应用程序来显著改善您的体验。有关详细信息，请参阅[在单会话或共享桌面 VDA 上发布打包的应用程序](#)。

回放直播和录制的会话：Citrix Monitor 现在支持播放使用 Session Recording 服务录制的录制和实时用户会话。您可以快速了解用户在重播中遇到的与会话相关的问题。借助此功能，您可以随时在 Monitor 控制台中访问录制文件以及与会话相关的指标。它有助于将在录制件中发现的问题与性能指标关联起来。它消除了跨多个 Session Recording Server 搜索录制文件或者寻找用于查看录制文件的第三方应用程序的要求。

此功能需要 VDA 和 Session Recording Server 版本 2308 或更高版本。

Monitor 将录制文件存储在集中存储库中，并在会话选择器模式中显示它们。**Sessions with recordings**（包含录制文件的会话）链接显示在过去 24 小时或过去 2 天内处于活动状态的会话录制文件。使用 Citrix Session Recording 播放服务器在新选项卡上播放录制文件。

有关详细信息，请参阅[录制会话](#)。

**Microsoft Teams 优化：**Monitor 显示 Microsoft Teams 可用的 HDX 优化的状态。可以在用户详细信息页面 > 会话详细信息面板中查看新的 **Microsoft Teams** 优化。只有当 Microsoft Teams 作为已发布的应用程序运行或在已发布的桌面中运行时，Monitor 才会显示 Microsoft Teams 的优化状态。此增强功能使管理员能够查看用户报告的 Microsoft Teams 上的会话性能问题，从而能够进行故障排除。有关详细信息，请参阅[对用户问题进行故障排除](#)。

用户界面改进：Citrix Monitor 用户界面现已焕然一新，外观新颖。经过改进的全新用户界面提供了更轻松的导航和更优质的数据表示方式。改进后的体验非常直观，旨在轻松理解监视 Citrix 会话以及对其进行故障排除所需的数据。

最佳屏幕分辨率：查看 Citrix Monitor 的推荐最佳屏幕分辨率已更新为 1440 x 1024。

## 2024 年 1 月

增强的双向内容重定向配置 以前，配置双向内容重定向涉及管理三种不同的策略：允许双向内容重定向、允许将 URL 重定向到 VDA 和允许将 URL 重定向到客户端。这些策略需要在服务器端（在 **DaaS > 完整配置** 中配置）和客户端（通过组策略配置）进行配置。从本版本开始，我们将所有三项策略合并为一个统一的策略。它不仅简化和增强了配置过程，而且消除了对客户端配置的要求。有关更多信息，请参阅[双向内容重定向配置](#)。

支持从“搜索”节点的“会话”选项卡重新启动和关闭单会话计算机。在搜索节点的会话选项卡上，您现在可以搜索处于不健康状态的用户会话，并在同一选项卡中无缝重启或关闭关联的单会话计算机。此功能提高了效率，可以在单个界面内对已确定的会话问题立即采取操作。

支持从“完整配置”访问全球应用程序配置服务。我们在完整配置界面中提供了操作项目，可将您链接到全球应用程序配置服务。通过此集成，您可以通过完整配置轻松访问全局应用程序配置，以管理最终用户设置。

要从“完整配置”访问此服务，您有两种选择：

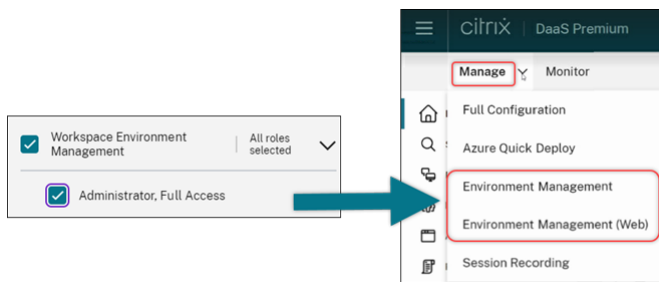
- 选择 **StoreFront** 节点，单击服务器记录，然后在操作栏中选择“配置客户机设置”。
- 选择“策略”节点，然后在操作栏中选择“配置客户端设置”。

支持使用完整配置管理 **Citrix Cloud** 管理的交付组的用户分配。作为我们计划将用户分配管理从云库迁移到完整配置的一部分，您现在可以通过完整配置管理 Citrix Cloud 托管交付组的用户分配。要完成此任务，请在完整配置 > 交付

组中编辑目标交付组，并通过以下菜单之一指定允许使用桌面或应用程序的用户：桌面（或桌面分配规则）或应用程序分配规则。有关详细信息，请参阅[管理交付组](#)。

在一个门户中进行的更新可与另一个门户无缝同步，从而确保两个门户之间的更新一致。

将 **WEM** 控制台访问权限限制为 **WEM** 完全访问管理员角色。我们为 Workspace Environment Management (WEM) 控制台启用了访问控制，以防止未经授权的进入。现在，只有拥有 **Workspace Environment Management** 完全访问权限管理员角色的用户才能使用 **DaaS > 管理访问 WEM 控制台**。



完整配置：**Azure** 目录支持从主映像继承 **DES** 设置。以前，完整配置仅根据计算机配置文件设置 Azure 目录的默认 DES 设置。我们现在已经扩展了这项功能。通过此增强，在以下情况下，完整配置直接基于主映像设置 Azure 目录的默认 DES 设置：

- 如果未选择计算机配置文件
- 如果配置文件指定了平台管理密钥 (PMK)

有关详细信息，请参阅在“完整配置”界面中的[使用 Azure Resource Manager 镜像创建计算机目录](#)。

增强搜索：更多过滤器可提高精度。我们增强了搜索节点上的搜索功能，加入了两个新的筛选条件，即区域和配置类型，以提高精度并提高可用性。

完整配置：支持为 **GCP** 计算机目录选择 **Google Cloud** 计算机类型。借助此功能，管理员可以灵活地为配置的 GCP 虚拟机选择所需的内存和处理器配置，对其进行定制以满足特定的操作要求。有关更多信息，请参阅[使用“完整配置”界面创建计算机目录](#)。

支持全球和区域客户管理的加密密钥 (**CMEK**)，用于配置 **GCP VM**。现在，您可以使用全球和区域性 CMEK 密钥来配置任何配置项目中的虚拟机。此增强功能为配置虚拟机和提高虚拟机安全性提供了更大的密钥选择灵活性。

## 2023 年 12 月

### 新增功能和增强功能

发送消息进度。现在，您可以在“**Monitor**”>“过滤器”中查看“发送消息”操作的进度。此操作有助于向您站点上的所有连接会话发送批量消息。操作进度以百分比显示。操作完成后，系统将显示已发送的消息数量和失败的消息数量。管理大型网站时，发送消息状态很有用。它有助于了解是否需要将消息重新发送给某些用户。如果计算机未注册或会话出现故障，则发送消息可能会失败。有关“发送消息”的更多信息，请参阅[向用户发送消息](#)。

通过 **Citrix Gateway** 通过域凭据和多重身份验证支持 **Citrix Probe Agent** 身份验证。



用于应用程序和桌面探测的 Citrix Probe Agent 现在支持通过 Citrix Gateway 使用域凭据和多因素身份验证进行身份验证。此功能有助于在通过 Citrix Gateway 连接到 StoreFront 的计算机上运行探测代理。Monitor 上提供的全面探测结果有助于在用户体验与应用程序、托管计算机或连接相关的问题之前对其进行故障排除。只有配置了 LDAP 和使用单一登录架构的本地 OTP 的 Citrix Gateway 才支持使用多重身份验证的 Citrix Gateway。有关详细信息，请参阅[应用程序和桌面探测](#)

重新设计了访问策略用户界面，以实现更灵活的资源访问控制。我们重新设计了编辑交付组 > 访问策略用户界面，让您在管理交付组的资源访问时更加灵活。以下是新设计提供的主要功能：

- 支持添加策略。现在，您可以添加访问策略，根据用户连接的属性限制资源访问权限。策略可以包含两种类型的标准：
  - 包含标准。允许您指定允许访问交付组的用户连接。
  - 排除标准。允许您指定禁止访问交付组的用户连接。
- 扩展了过滤器支持。现在，您可以使用一系列 SmartAccess 过滤器定义包含和排除标准。这些过滤器包括 Workspace 过滤器（例如 `Citrix.Workspace.UsingDomain` 和 `Citrix-Via-Workspace`）以及用于基于网络位置的自适应访问的过滤器。
- 匹配所含条件的所有逻辑支持。新逻辑使您能够在为交付组指定允许的用户连接时实现较高的精度和控制力。

有关更多信息，请参阅[限制对交付组中资源的访问权限](#)。

## 2023 年 11 月

### 新增功能和增强功能

支持使用“完整配置”界面创建 **Citrix Provisioning** 目录。要创建 Citrix Provisioning 目录，您必须使用 Citrix Virtual Apps and Desktops 安装向导。借助此功能，您现在可以使用“完整配置”界面和 PowerShell 创建 Citrix Provisioning 目录。

此实现为您提供了以下优势：

- 用于管理 MCS 和 Citrix Provisioning 目录的单一统一控制台。
- 为 Citrix Provisioning 目录提供新功能，例如身份管理解决方案、按需预配等。

目前，此功能仅适用于 Azure 工作负载。有关详细信息，请参阅在 [Citrix Studio 中创建 Citrix Provisioning 目录](#)。

介绍搜索应用程序组。我们已经在“应用程序”节点中引入了应用程序组的搜索功能。借助此增强功能，您现在可以直接在任何应用程序文件夹中搜索应用程序组。有关更多信息，请参阅[搜索应用程序组](#)。

修改了配置限制。下表描述了为提高性能和提供成本效益而对 DaaS 配置限制所做的修改。

资源	旧上限	新上限
Active Directory 域	85	100

资源	旧上限	新上限
目录	1000	2000
交付组	1000	2000
资源位置	85	100
资源位置 -> 会话总数	20,000	25,000

有关详细信息，请参阅 [限制](#)。

用于在电源重启期间保留 **VM** 和系统磁盘的单个选项。现在，在 Azure 上启动现有 VM 的速度比启动新 VM 更快，因此电源重启时保留 VM 是一种更有效的选择。为了应对这一变化，我们将跨电源周期保留 **VM** 和电源重启期间保留系统磁盘这两个选项合并为一个选项 **Retain VM and system disk during power cycles**（在电源重启期间保留 VM 和系统磁盘）。这意味着，当您选择此选项通过保留系统磁盘来减少虚拟机重启时间时，您的虚拟机也会被保留。

完整配置中的新功能可根据计算机配置文件中的“主机加密”属性筛选计算机大小（特定于 **Azure VM**）。在 Azure 计算机目录创建或管理期间选择了启用主机加密的计算机配置文件后，将仅显示支持此功能的计算机大小。

将备份和还原操作限制为完全管理员角色。我们增强了对备份和还原操作的访问控制。现在，只有具有完全管理员角色的用户才能访问备份 + 还原节点，从而防止未经授权的操作。

搜索节点的数据缓存。我们已经为 Citrix DaaS 搜索节点引入了数据缓存。此增强功能提高了搜索性能，以下列出了简化日常任务的用例：

- 首次检索搜索结果后快速显示搜索结果。
- 在向外导航并返回搜索节点后保留分页结果。

计算机目录页面上的映像信息。现在，您可以通过计算机目录的模板属性查看以下映像信息：

- 操作系统
- Machine Identity Service
- Machine Creation Services 存储
- Azure 部署的 `pagefile.sys` 的文件路径。

此增强功能使映像信息更加清晰，并确保管理员将有关计算机目录的所有信息集中在一个地方。

支持固定搜索过滤器。为了提供快速的搜索体验，“完整配置”允许工具固定搜索过滤器。过滤器固定功能允许您在页面上访问常用的搜索过滤器。此增强功能可在以下节点的搜索面板中使用：

- 搜索
- 计算机目录
- 交付组
- 应用程序

有关详细信息，请在“完整配置”管理界面中使用“搜索”。



支持将元数据与配置日志相关联。使用此增强功能，您现在可以通过在高级操作上关联 `name-value` 对将元数据附加到配置日志中。有关详细信息，请参阅 [将元数据与配置日志关联](#)。

忽略带有特定标签的孤立资源。在 Azure 环境中，标记了所有 Citrix 标签的客户管理资源被检测为孤立资源。使用此功能，如果您为该资源添加另一个值为 `true` 的标签 `CitrixDetectIgnore`，则在检测孤立资源时会忽略该资源。

**SCCM 重复 GUID 问题的解决方案。**使用 MCS 创建多个 VM 后，由于 GUID 重复，System Center Configuration Manager (SCCM) 在其控制台上仅显示一个 VM。现在，通过在映像准备中添加一个步骤解决了此问题。此步骤删除主映像中的现有证书和 GUID 信息。默认情况下，此步骤处于启用状态。

修复活跃计算机帐户的身份信息。借助此功能，您可以重置存在身份相关问题的活动计算机帐户的身份信息。可以选择仅重置计算机密码和信任密钥，也可以重置身份磁盘的所有配置。此实现同时适用于永久和非永久计算机目录。目前，只有 Azure 和 VMware 虚拟化环境支持该功能。有关详细信息，请参阅 [修复活动计算机帐户的身份信息](#)。

对与计算机配置文件关联的主机信息进行加密。在 Azure 环境中，通过此功能，您现在可以使用 PowerShell 命令知晓是否在主机上为计算机配置文件输入（VM 或模板规范）启用了加密。有关详细信息，请参阅 [从计算机配置文件中检索主机加密信息](#)。

修复混合 **Azure AD** 加入计算机身份的用户证书。使用此功能，您可以使用 PowerShell 命令修复混合 Azure AD 加入计算机身份的用户证书（如果这些身份损坏或过期）。有关详细信息，请参阅[创建加入了混合 Azure Active Directory 的目录](#)。

加入了混合 **Azure AD** 的计算机目录支持证书过期警告。现在，“完整配置”可在已加入混合 Azure AD 的计算机目录上提前一个月发出用户证书到期警告。此增强功能旨在降低因证书过期而导致服务中断的风险。要查看详细信息和建议的操作，请转到计算机目录节点，选择计算机目录，然后单击故障排除选项卡。

可以运行 `Get-ProvScheme` 命令来获取与加入了混合 Azure AD 的计算机目录的用户证书过期日期有关的信息。

支持 **Azure 机密 VM**（预览版）。Azure 机密计算虚拟机确保您的虚拟桌面在内存中经过加密并在使用中受到保护。有了此功能，您现在可以使用 MCS 创建包含 Azure 机密 VM 的目录。必须使用计算机配置文件工作流程来创建此类目录。您可以将 VM 和 ARM 模板规范用作计算机配置文件输入。有关详细信息，请参阅 [Azure 机密 VM（预览版）](#)。

支持在 **AWS** 环境中将非基于计算机配置文件的计算机目录转换为基于计算机配置文件的计算机目录。在 AWS 环境中，您现在可以使用 VM 或启动模板作为计算机配置文件输入，以将非基于计算机配置文件的计算机目录转换为基于计算机配置文件的计算机目录。添加到目录中的新 VM 从计算机配置文件中获取属性值。有关详细信息，请参阅[将非基于计算机配置文件的计算机目录转换为基于计算机配置文件的计算机目录](#)。

支持 **Citrix** 管理的 **HPE Moonshot** 插件（预览版）。以前，您使用 Hewlett Packard Enterprise (HPE) 维护的 HPE 管理的 Moonshot 插件 (HPE Moonshot Machine Manager) 在 HPE Moonshot 机箱上执行电源管理操作。该插件基于旧版 API，这使 MCS 基础结构项目变得困难。借助此功能，推出了 Citrix 管理的 HPE Moonshot 插件 (HPE Moonshot)。使用此插件，您可以使用完整配置界面和 PowerShell 命令与 HPE Moonshot 机箱建立连接、创建目录以及对目录中的计算机进行电源管理。有关详细信息，请参阅：

- [HPE Moonshot 虚拟化环境（预览版）](#)
- [与 HPE Moonshot 的连接（预览版）](#)

- [创建 HPE Moonshot 计算机目录（预览版）](#)
- [管理 HPE Moonshot 目录（预览版）](#)

能够更改内存和磁盘缓存的大小。使用此功能，您现在可以使用 PowerShell 命令更改回写缓存（启用 MCSIO 时）的内存和磁盘缓存大小，而无需创建新的计算机目录。此实现可帮助您获取适合您的业务需求的优化缓存配置。此功能适用于：

- GCP 和 Microsoft Azure 环境，以及
- 启用了 MCSIO 的非永久目录

有关详细信息，请参阅 [更改现有计算机目录上的缓存配置](#)。

支持创建客户管理的启用加密密钥的目录。在 Azure 环境中，您现在可以使用完整配置界面和 PowerShell 命令创建启用了客户管理的加密密钥 (CMEK) 的 Citrix Provisioning 目录。有关详细信息，请参阅 [创建客户管理的启用加密密钥的目录](#)。

能够复制 **Azure** 中所有资源的标签。借助此功能，在 Azure 环境中，您现在可以将计算机配置文件中指定的标签复制到所有资源，例如新虚拟机或现有 VM 的多个 NIC 和磁盘（操作系统磁盘、身份磁盘和回写缓存磁盘）。

计算机配置文件来源可以是 VM 或 ARM 模板规范。有关详细信息，请参阅 [在所有资源上复制标签](#)。

计算机暂停后，会话状态更新为已断开连接。以前，在您暂停虚拟机后，会话仍显示为“活动”。通过此增强功能，在您暂停虚拟机后，关联会话的状态现在显示为“已断开连接”。

支持创建支持休眠的 **AWS** 虚拟机。现在，您可以在 AWS 环境中创建支持 VM 休眠的计算机目录，从而提高部署的整体成本效益。如果关联的计算机配置文件支持此功能，则还可以编辑目录以包括支持休眠的虚拟机。有关详细信息，请参阅 [对 AWS VM 进行电源管理](#)。

支持在交付组级别配置负载平衡方法（预览版）。此功能允许您在交付组级别选择垂直负载平衡方法。使用此功能，在下一台计算机开机之前，每台计算机都与最大负载指数对齐。AutoScale 和垂直负载平衡决定下一台计算机的开机时间。此功能可最大限度地提高每台计算机的利用率，并节省公有云中的成本。此功能为管理计算机的负载平衡策略提供了更大的灵活性。

您可以将交付组配置为继承站点级设置中的负载平衡方法，也可以替换站点级负载平衡方法，改为选择垂直或水平负载平衡方法之一。有关详细信息，请参阅 [步骤 2. 负载平衡](#)。

在 **Azure** 中支持休眠的 **VM**（预览版）。在 Azure 环境中，您可以创建支持休眠的 MCS 计算机目录。使用此功能，您可以挂起 VM，然后在用户再次登录时重新连接到 VM 的先前状态。有关详细信息，请参阅 [创建支持休眠的 VM（预览版）](#)。

**DaaS 入门指南**。我们发布了一份新指南，旨在为新手和有经验的管理员简化和简化 DaaS 的部署和配置。它具有以下主要优点：

- 易于上手。本指南采用基于问卷调查的分步方法，帮助新管理员快速设置部署。整个指南中的上下文帮助信息有助于理解基本概念和术语。
- 简化复杂的配置。本指南包括适用的预配置设置，并提供对完整配置用户界面的访问以进行高级设置。经验丰富的管理员可以将其用作更复杂配置的基础。

有关详细信息，请参阅[使用 DaaS 入门指南](#)。

使用完整配置为回写缓存磁盘分配驱动器号。以前，只能使用 PowerShell cmdlet 为回写缓存磁盘分配特定的驱动器号。现在，您可以使用“完整配置”完成相同的任务。有关详细信息，请参阅[创建计算机目录](#)。

支持使用完整配置更改各种 **Azure** 计算机属性。对于 Machine Creation Services 提供的 Azure 计算机，您现在可以使用完整配置更改以下属性设置：

- 存储类型
- 专用主机组
- Azure Compute Gallery 设置

当您更改其中任何设置时，“完整配置”会自动识别相关设置，并提供自动同步或提示消息，要求您重新选择相关设置。此功能可确保关联设置的一致更改，防止潜在的配置错误。有关详细信息，请参阅[编辑目录](#)。

使用现有身份池为 **MCS** 配置的计算机创建身份。在创建已加入 AD 的目录或使用完整配置向其中添加计算机时，您现在可以使用现有的身份池来分配计算机身份。此功能允许您在多个目录中应用一致的计算机帐户命名方案。有关详细信息，请参阅[计算机标识](#)。

会话拓扑。会话拓扑视图是增强 Monitor 中故障排除工作流程的下一步。会话拓扑视图提供了连接的 HDX 会话的会话中路径的可视化表示。您可以从“用户详细信息”>“会话性能”访问拓扑视图。

连接到 HDX 的会话的会话拓扑视图显示会话路径中涉及的组件及其元数据、组件之间的链接以及 VDA 上发布的应用程序。此外，当会话处于连接状态时，还会显示会话的 ICA 延迟和 ICA RTT 测量值。

使用会话拓扑视图来了解会话数据流经的组件，并确定可能带来性能问题的特定跃点。有关详细信息，请参阅[会话拓扑](#)。

## 2023 年 10 月

### 新增功能和增强功能

使用历史使用情况优化您的 **AutoScale** 设置。一个名为 **AutoScale Insights** 的全新 AutoScale 设置选项卡提供了一个全面的图表，可以直观地比较 AutoScale 设置和前一周的计算机使用数据。通过此图表，您可以深入了解 AutoScale 设置的有效性：

- 性价比不高。由于过度配置容量，存在财务浪费。
- 用户体验不佳。由于容量配置不足，用户体验受到负面影响。
- 在用户体验和成本之间取得良好的平衡。预置的容量与历史使用量一致。

有关详细信息，请参阅[分析 AutoScale 设置的有效性](#)。

多个 **NIC** 支持 **Azure** 虚拟机。使用完整配置，您现在可以创建具有多个 NIC 的 Azure 虚拟机。虚拟机的最大 NIC 数由计算机大小设置决定，而其实际允许的 NIC 数量由计算机配置文件设置定义。有关详细信息，请参阅[创建计算机目录](#)。

要使用 PowerShell 命令创建或更新每个虚拟机有多个 NIC 的目录，请参阅[创建或更新包含每个 VM 多个 NIC 的目录](#)。

会话性能指标的趋势。Monitor 引入了新的“用户详细信息”>“会话性能”选项卡，该选项卡增强了故障排除工作流程，首先能够关联实时指标以识别用户会话中的问题。会话体验现在包含会话指标的趋势，例如 ICARTT、ICA 延迟、每秒帧数、可用的输出带宽和占用的输出带宽。此功能有助于在单个视图中关联多个性能指标来缩短解决问题的平均时间。有关详细信息，请参阅[用户问题](#)文章。

在创建/编辑策略的设置页面上支持 **VDA** 版本。作为创建策略的一部分，在配置设置时，系统会提供查看设置类型的选项。您可以查看以下设置类型：

- 所有设置 - 查看所有 VDA 版本的所有设置
- 仅限当前设置 - 仅查看当前 VDA 版本的设置
- 仅限旧版设置 - 仅查看已弃用的 VDA 版本的设置

有关详细信息，请参阅 [创建策略](#)

限制仅支持 **Active Directory** 帐户的应用程序可见性。限制应用程序可见性的功能仅适用于 Active Directory 用户帐户，而不适用于 Azure Active Directory 和 Okta 帐户。请注意，为了帮助实现此功能，在应用程序设置工作流程中，在“选择用户或组”页面上，“选择身份类型”字段中的 **Azure Active Directory** 和 **Okta** 选项已禁用。

新的用户界面选项，用于仅从 **Citrix** 站点数据库中删除虚拟机记录。当由于无法访问的虚拟机管理程序而导致目录和虚拟机删除失败时，您现在可以选择仅从 Citrix 站点数据库中删除虚拟机记录，使主机上的虚拟机保持不变。有关详细信息，请参阅 [删除目录](#)。

支持为非 **MCS** 配置的计算机创建空计算机目录。现在，创建空计算机目录可以扩展到非 MCS 配置的计算机，包括：

- 使用 Machine Creation Services 以外的技术调配的虚拟机或刀片机。
- 物理机不是由 Citrix DaaS 管理的电源
- Remote PC Access 计算机

使用此功能，您现在可以创建计算机目录，而无需在创建目录期间向其中添加计算机。

图像刷新增强功能。以前，刷新图像时，无论是否选择了树中的特定节点，都会更新图像树中的所有图像。在最新的增强功能中，如果您选择了节点，则仅刷新此节点中的图像。此增强功能可确保更有针对性的刷新过程，从而显著提高图像刷新速度。此外，现在您可以通过按住 CTRL 键并单击该节点来清除图像树中的选定节点。有关详细信息，请参阅 [主映像](#)。

峰值 **AutoScale** 指定 **PowerOn**。当永久桌面已开机但仍未使用或没有用户登录时，管理员可以定义等待执行操作（例如不执行任何操作、暂停或关闭）的时间。

对于已分配的计算机，如果计算机已开机，但在高峰时段开始后的设定时间内仍未连接到该计算机，则可以在交付组级别添加策略以关闭计算机。

对于已分配的计算机，如果计算机处于还原状态，但会话在高峰时段开始后的设定时间内仍未连接到该计算机，则可以在交付组级别添加策略以暂停计算机。

如果最终用户处于 PTO 或尚未登录，或者公司的周末很长，则此功能非常有用，则可以设置等待时间和要采取的计算机断开连接操作，以帮助降低 Azure 的使用成本。有关详细信息，请参阅[单会话操作系统随机交付组](#)和[单会话操作系统静态交付组](#)。

监视多个 **Citrix DaaS** 实例（预览版）。现在，您可以使用 Citrix Monitor 监视多个 Citrix DaaS 实例中的问题并对其进行故障排除。Citrix DaaS 允许客户使用中心和分支模型聚合多个服务实例。使用此配置，管理员可以从单个 Monitor 控制台对所有已配置的 DaaS 实例执行帮助台搜索。有关将分支服务实例聚合到中心所需的配置的更多信息，请参阅[聚合多个 Citrix Virtual Apps and Desktops 服务实例](#)。Monitor 支持在单个 DaaS 租户（中心）下聚合多达四个 DaaS 租户（分支）。

要对所有 DaaS 租户进行统一监视，请使用中心和分支实例的双向枚举。有关详细信息，请参阅[跨多个 DaaS 实例的聚合搜索（预览版）](#)。

支持 **vSAN 8.0**。您现在可以使用 MCS 在 vSAN 8.0 环境中预配 VM。

在已配置的虚拟机上保留 **NIC** 设置。以前，主映像的 NIC 设置不会保留在已预配的 VM 中。例如，如果您对主映像配置了 DNS 设置，则已预配的 VM 不会保留主映像的已配置 DNS 设置。借助此功能，已预配的 VM 现在可以保留主映像的 NIC 设置。即使在更新 Windows 之后，这些设置仍会保留。如果您通过安装 MCS 主映像部署了 Hyper-V 的计算机上执行 VDA 版本 2308 或更高版本的全新安装，则会自动安装过滤驱动程序。但是，当前，如果您从旧版本的 VDA（低于 2308 的版本）升级并想要安装过滤器驱动程序，则在升级 VDA 时，必须在“其他组件”页面上选中“**Citrix HyperV 过滤器驱动程序**”复选框。有关详细信息，请参阅[安装其他组件](#)。

此功能适用于：

- Hyper-V VM（包括 Azure 和 SCVMM）
- 持久和非持久 MCS 计算机目录
- 含有 MCSIO 的非永久性 MCS 计算机目录
- 含有多个 NIC 的主映像

检测孤立的 **Azure** 资源。借助此功能，您现在可以检测 Azure 部署中的孤立资源，从而实现高效的资源管理。确定孤立资源后，您可以进一步进行操作，从而提高生产率以及降低成本。有关详细信息，请参阅[检测部署中的孤立 Azure 资源](#)。

新映像更新状态。在完全配置中监视目录的图像更新状态时，除了现有状态已完全更新、部分更新和待更新之外，您现在还可以查看新的准备映像状态。有关详细信息，请参阅[更改主映像](#)。

用于创建自动标记（预览）的 **PowerShell** 命令。有了这个功能，您现在可以使用 PowerShell 命令自动创建标签。有关详细信息，请参阅[自动标记](#)。

向用户或交付组显示通知标志。在创建或修改策略并配置设置时，如果禁用了所有交付组，则系统会显示一条警告：-此筛选器中的所有元素均未启用。如果启用了至少一个交付组，则系统不会显示警告标志。有关详细信息，请参阅[策略设置](#)。



## 2023 年 9 月

### 新增功能和增强功能

用于管理本地主机缓存 (LHC) 的 **PowerShell** 命令。您现在可以使用 PowerShell 命令在 Citrix Cloud Connector 上管理 LHC。有关详细信息，请参阅[本地主机缓存 PowerShell 命令](#)。

支持创建空的计算机目录。在完整配置中，您现在无需立即创建虚拟机即可创建计算机目录。借助此功能，您可以将虚拟机的创建推迟到后端主机准备就绪或虚拟机配置完成之后，从而在创建目录时获得更大的灵活性。目前，此功能仅适用于由 Machine Creation Services 配置的目录。有关详细信息，请参阅[创建计算机目录](#)。

主节点的数据缓存。我们已经为 Citrix DaaS 主页节点引入了数据缓存。此增强功能通过缩短您导航到“主页”节点时的页面加载时间来改善用户体验。

应用程序的搜索增强功能。我们改进了“应用程序”节点中的搜索功能，使其与“搜索”节点中引入的新设计保持一致。这项新功能可改善您的应用程序搜索体验，并在 DaaS 之间保持一致的搜索体验。筛选表达式中的关键字“应用程序名称”已重命名为“名称”，同时保留其原始含义。有关详细信息，请参阅[在“完整配置”管理界面中使用搜索](#)。

增强的范围管理：在文件夹视图中显示对象。在范围创建和管理页面上，计算机目录、交付组和应用程序组现在以文件夹结构显示，这些文件夹结构与 DaaS 中的管理保持一致。此文件夹视图简化了为范围创建和管理选择对象的过程，使您的选择更加直观和直观。有关详细信息，请参阅[创建和管理作用域](#)。

移除了“将用户管理留给 **Citrix Cloud**”选项。在管理 > 完整配置中创建交付组时，在用户页面上，将删除对此选项的支持。对于通过 Citrix Cloud 处理用户分配的交付组，请继续在 Citrix Cloud 库中管理用户分配。

移除了 **Azure** 德国版选项。随着 Microsoft Cloud Deutschland 于 2021 年 10 月 29 日关闭，我们已从主机连接创建页面中删除了 **Azure Germany** 选项。

完整配置中的主动服务警报。警报分为两个级别：显示在“主页”（旗帜图标）中的站点范围警报，以及每个区域的“故障排除”选项卡上显示的区域相关警报。目前，此功能会主动向您发出警告和警报，以确保您的本地主机缓存和区域配置正确，以便在发生中断时，本地主机缓存可以正常工作，并且您的用户不会受到影响。有关详细信息，请参阅[服务运行状况警报](#) 和 [区域](#)。

## 2023 年 8 月

### 新增功能和增强功能

完整配置：支持使用计算机配置文件配置 **AWS** 和 **GCP** 虚拟机。使用 Machine Creation Services (MCS) 配置 AWS 或 GCP 虚拟机时，您现在可以选择现有虚拟机作为计算机配置文件，让目录中的虚拟机继承所选虚拟机的设置。

- 对于 GCP 虚拟机，继承的设置包括磁盘加密 ID、计算机大小、存储类型和区域。
- 对于 AWS 虚拟机，继承的设置因阶段而异：
  - 创建目录期间：计算机大小、租赁类型、安全组 and NIC 数量。
  - 目录编辑期间：计算机大小和安全组。

有关详细信息，请参阅[创建计算机目录](#)。

在计算机目录和交付组节点中引入搜索功能。现在，您可以直接在计算机目录和交付组节点中搜索和定位计算机目录和交付组。这些节点中的搜索功能提供与搜索节点相同的界面，从而提供跨 DaaS 的无缝搜索体验。有关详细信息，请参阅在[“完整配置”管理界面中使用搜索](#)。

使用 **Device Posture** 在会话启动诊断中查看端点设备状态。Monitor 中的“会话启动诊断”功能有助于缩小会话故障发生的确切组件和阶段。这有助于确定会话启动失败的确切原因并采取建议的措施。

下一步是全面检查会话启动序列中涉及的所有组件，您现在可以查看端点设备扫描结果。在组件列表中单击端点设备将显示设备状态扫描状态。Device Posture Service 根据管理员定义的策略扫描端点设备的合规性。

确保设备状态服务已按照 [Device Posture](#) 一文中所述配置了 DaaS。Device Posture 记录的错误在 [Device Posture 错误日志](#) 中介绍。

有关详细信息，请参阅[诊断会话启动失败的步骤](#)

完整配置中的新选项，用于通过 **Citrix Cloud Connector** 将 API 请求路由到 **Azure** 和 **GCP**。以前，向 Azure 和 GCP 发出的 API 请求只能通过公共端点进行路由。借助“完整配置”>“添加连接和资源”中的新选项，您现在可以通过 Citrix Cloud Connector 路由它们来选择更安全的方法。有关详细信息，请参阅[使用完整配置创建服务主体和连接](#)。

搜索和筛选增强功能。为了改善您的搜索体验，我们进行了以下改进：

- 简化搜索：现在，在没有筛选条件的情况下执行搜索会删除搜索推荐，从而提供简洁明了的搜索体验。
- **AND/OR** 运算符更新：过滤器面板中现在提供了“匹配全部（AND 运算符）”和“匹配任意（OR 运算符）”选项，只需单击过滤器图标即可访问。
- 简化的过滤器配置：现在，您可以使用过滤器面板无缝指定和应用多个过滤器。
- 更简洁的界面：移除了“过滤器固定”功能，减少了用户界面的混乱，让您的搜索体验更加直观。
- 快速添加过滤器：应用过滤器后，您现在可以使用加号快速再添加一个过滤器。
- 删除已保存的筛选器集：现在，您可以直接在搜索菜单中轻松删除已保存的筛选器集，而无需导航到“管理过滤器集”。

有关详细信息，请参阅在[“完整配置”管理界面中使用搜索](#)。

**VDA** 升级支持 **Azure** 快速部署创建的计算机目录。使用完整配置，您现在可以为通过 Azure 快速部署创建的计算机目录启用 **VDA** 升级，然后对它们执行升级 **VDA** 以进行即时升级或计划升级。有关详细信息，请参阅[使用完整配置界面升级 VDA](#)。

能够在 **SCVMM** 中在 **MCS** 创建的计算机目录中重置永久虚拟机的操作系统磁盘。您现在可以使用 PowerShell 命令 [Reset-ProvVMDisk](#) 在 MCS 创建的计算机目录中重置永久性 VM 的操作系统磁盘。该功能自动执行重置操作系统磁盘的过程。例如，它有助于将 VM 重置为使用 MCS 创建的永久开发桌面目录的初始状态。目前，此功能适用于 Azure、Citrix Hypervisor、SCVMM 和 VMware 虚拟化环境。有关使用 PowerShell 命令重置操作系统磁盘的详细信息，请参阅[重置操作系统磁盘](#)。

更新单个 **VM** 的属性。现在，您可以使用 PowerShell 命令更新永久性 MCS 计算机目录中各个 VM 的属性。此实现可以帮助您高效地管理各个 VM，而无需更新整个计算机目录。目前，此功能仅适用于 Azure 环境。有关详细信息，请参阅[更新各个 VM 的属性](#)。

限制托管磁盘的上载和下载。根据 Azure 政策，您不能使用同一个磁盘访问对象同时上载或下载五个以上的磁盘或快照。使用此功能，如果您符合以下条件，则不会强制执行五次并发上载或下载的限制：

- 在 [ProxyHypervisorTrafficThroughConnector](#) 中配置 [CustomProperties](#)，然后
- 请勿将 Azure 策略配置为自动为每个新磁盘创建磁盘访问权限以使用专用端点。

支持为 **MCS I/O** 回写式缓存磁盘分配特定的驱动器盘符。以前，Windows 操作系统会自动为 MCS I/O 回写式缓存磁盘分配一个驱动器盘符。使用此功能，您现在可以为 MCS I/O 回写缓存磁盘分配特定的驱动器号。此实现可帮助您避免所使用的任何应用程序的驱动器盘符与 MCS I/O 回写缓存磁盘的驱动器盘符发生冲突。此功能仅适用于 Windows 操作系统。有关详细信息，请参阅[MCS I/O 写回缓存磁盘分配特定的驱动器盘符](#)。

在 **Citrix Hypervisor** 中支持计算机配置文件。在 Citrix Hypervisor 中，您现在可以使用计算机配置文件创建 MCS 计算机目录。计算机配置文件输入的来源为 VM。计算机配置文件会从 VM 模板中捕获硬件属性并将其应用于目录中新配置的 VM。有关详细信息，请参阅[使用计算机配置文件创建计算机目录](#)。

失败后重试创建目录。当目录创建失败时，您现在可以重试创建目录。为确保成功创建，请检查故障排除信息并解决问题。该信息描述了发现的问题并提供了解决这些问题的建议。故障目录标有错误图标。要查看详细信息，请转到每个目录的故障排除选项卡。有关详细信息，请参阅[管理计算机目录](#)。

管理配置集的权限。为了更精确地控制 WEM 配置集管理，我们在计算机目录权限集中引入了一种名为“管理配置集”的新权限。此权限向可以执行诸如绑定或解除绑定配置集以及切换到其他目录配置集等任务的用户授予独占访问权限。有关详细信息，请参阅[管理目录的配置集](#)。

“完整配置”中的新选项，用于清理已加入的 **Azure AD** 的陈旧设备。我们在“完整配置”中引入了一个选项，以简化 Citrix DaaS 中过时的加入了 Azure AD 的设备的清理工作。以前，必须运行自定义 PowerShell 脚本才能执行任务。启用此选项可授予主机连接自动清理过时的加入了 Azure AD 的设备的权限。有关详细信息，请参阅[Azure 主机连接](#)。

使用完整配置 **Monitor** 目录的映像更新状态。现在，您可以使用新列“映像更新”来监视非持久性计算机目录的映像更新状态。此列指示目录的映像是否已完全更新、已部分更新还是待更新。

要在“计算机目录”表中显示该列，请执行以下步骤：

1. 在“计算机目录”节点中，选择操作栏上的“要显示的列”图标。
2. 选择 计算机目录 > 映像状态。
3. 单击保存。

显示“映像更新”列可能会降低控制台性能。我们建议仅在必要时才显示它。

为 **GCP** 管理的流量提供安全的环境。有了这个功能，您现在只能允许 Google 私密访问您的 Google Cloud 项目。这种实现增强了处理敏感数据的安全性。为此，请在部署 Citrix Cloud 时在 [CustomProperties](#) 中添加 [ProxyHypervisorTrafficThroughConnector](#)。如果您使用的是专用工作人员池，请将 [UsePrivateWorkerPool](#) 加入到 [CustomProperties](#) 中。有关详细信息，请参阅[GCP 管理的流量创建安全环境](#)。



## 2023 年 7 月

### 新增功能和增强功能

支持在 **Azure** 上获取孤立资源列表。在 Azure 环境中，您现在可以获得由 MCS 创建但不再被 MCS 使用的孤立资源列表。此功能有助于避免额外费用。有关详细信息，请参阅[检索孤立资源列表](#)。

支持使用完整配置创建永久性多会话计算机。在创建多会话计算机目录时，您现在可以指定是否将其永久化。对于永久性多会话计算机，请记住，用户对桌面所做的更改会被保存，可供所有授权用户访问。有关详细信息，请参阅[创建计算机目录](#)。

“完整配置”中的新功能，用于筛选 **AWS AMI** 清单。在创建 AWS 目录期间选择计算机模板时，您现在可以使用以下搜索条件筛选目标模板的 AWS AMI 清单：

- 映像名称
- 映像 ID
- 映像标记

向下滚动列表时，计算机模板列表会动态加载——最初加载了 25 个项目，滚动时会加载更多项目。

支持删除 **Azure AD** 设备。使用此功能，通过为服务主体分配云设备管理员角色并修改托管连接的自定义属性，可以持续删除陈旧的 Azure AD 设备。如果不删除 Azure 陈旧的 AD 设备，则相应的非持久 VM 将保持初始化状态，直到您手动将其从 Azure AD 门户中移除。有关详细信息，请参阅[创建 Azure Active Directory 加入的目录](#)。

支持 **AWS** 环境中的计算机配置文件。当您在 AWS 中使用 Machine Creation Services (MCS) 创建目录以预配计算机时，您现在可以使用计算机配置文件从 EC2 实例 (VM) 中捕获硬件属性或启动模板版本并将其应用到已预配的计算机。例如，捕获的属性可以包括 EBS 卷属性、实例类型、EBS 优化和其他支持的 AWS 配置。编辑目录时，可以通过提供不同的 VM 或启动模板来更改已预配计算机的计算机配置文件。有关详细信息，请参阅[使用计算机配置文件创建目录](#)。

搜索结果的导出限制从 **10000** 个扩大到 **30000** 个。我们扩大了搜索结果的导出限制。以前限制为 10000 个项目，现在最多可以将 30000 个项目导出为 CSV 文件。有关详细信息，请参阅[将搜索结果导出为 CSV 文件](#)。

映像刷新选项。在为计算机目录选择主映像时，现在可以使用右上角的刷新选项快速获取最新的主映像列表。请注意，刷新选项不适用于 AWS 目录。此外，还为 Azure 目录中的计算机配置文件和主机组提供了刷新选项。

## 2023 年 6 月

### 新增功能和增强功能

支持从 **GCP** 中的计算机配置文件输入中获取自定义属性。以前，在 GCP 环境中，在使用计算机配置文件输入创建 MCS 计算机目录时，必须明确指定自定义属性。该操作迫使人们付出额外的努力。有了这个功能，您现在可以在不明确定义的情况下派生以下自定义属性：

- [ServiceOffering](#)

- [CryptoKeyId](#)
- [CatalogZones](#)
- [Storage](#)

当您运行 [New-ProvScheme](#) 和 [Set-ProvScheme](#) 命令但未明确指定自定义属性时，将从计算机配置文件输入中派生这些属性的值。

例如，除非您在 [New-ProvScheme](#) 命令中指定 [ServiceOffering](#)，否则会将计算机配置文件的计算机类型 [New-ProvScheme -MachineProfile](#) 写入预配方案的 [ServiceOffering](#) 属性。如果您运行 [Set-ProvVMScheme](#) 两次，最新的命令将生效。

在 **AWS** 环境中删除标记。以前，带有 [ForgetVM](#) 参数的 [Remove-ProvVM](#) 和 [Remove-ProvScheme](#) PowerShell 命令会从 Citrix 数据库中删除虚拟机和计算机目录。但是，这些命令并未删除标记。您必须单独管理未从所有资源中完全删除的 VM 和计算机目录。有了这个功能，您可以使用：

- 带 [ForgetVM](#) 参数的 [Remove-ProvVM](#) 从单个虚拟机或计算机目录中的虚拟机列表中删除虚拟机和标签。
- 使用 [ForgetVM](#) 参数的 [Remove-ProvScheme](#) 从 Citrix 数据库中删除计算机目录，从计算机目录中删除资源。

此实现有助于：

- 识别泄露的资源
- 消除了维护不需要的资源的额外成本

此功能仅适用于永久 VM。有关详细信息，请参阅 [移除标签](#)。

能够获取与 **MCS** 计算机目录相关的历史错误和警告。以前，您只会收到与计算机目录关联的最新警告和错误。使用此功能，您现在可以获取 MCS 计算机目录的历史警告和错误列表。此列表可帮助您了解 MCS 计算机目录中的任何问题并修复这些问题。

有关详细信息，请参阅[检索与目录关联的警告和错误](#)。

**Citrix** 在 **Google Cloud** 中提高了性能，从而增加了容量。Citrix 现在可以在单个 Google Cloud 项目中支持包含多达 3000 个 VDA 的目录。此更新同时为预配和电源管理操作带来了性能改进。

能够在 **Google Cloud** 和 **AWS** 环境中重置 **MCS** 创建的计算机目录中永久虚拟机的操作系统磁盘。您现在可以使用 PowerShell 命令 [Reset-ProvVMDisk](#) 在 MCS 创建的计算机目录中重置永久性 VM 的操作系统磁盘。该功能自动执行重置操作系统磁盘的过程。例如，它有助于将 VM 重置为使用 MCS 创建的永久开发桌面目录的初始状态。目前，此功能适用于 AWS、Azure、Citrix Hypervisor、Google Cloud 和 VMware 虚拟化环境。有关使用 PowerShell 命令重置操作系统磁盘的详细信息，请参阅[重置操作系统磁盘](#)。

支持在 **GCP** 中更改现有目录和现有虚拟机的磁盘相关自定义属性。以前，在 GCP 环境中，只有在创建了 MCS 计算机目录时才能添加自定义属性。使用此功能，您现在可以更改现有目录和目录中的现有 VM 的以下磁盘相关自定义属性。

- [PersistOSDisk](#)
- [PersistWBC](#)
- [StorageType](#)

- [IdentityDiskStorageType](#)
- [WbcDiskStorageType](#)

即使在创建目录之后，此实现也可以帮助您为不同的磁盘选择不同的存储类型，从而平衡与不同存储类型相关的定价。有关详细信息，请参阅[更改现有目录的磁盘相关自定义属性](#)。

动态会话超时支持已扩展到 **VDA 版本 2203 LTSR CU3** 或更高版本。对于单会话操作系统交付组，此功能现在适用于版本 2206 CR 或更高版本或 2203 LTSR CU3 或更高版本的 VDA。有关详细信息，请参阅[动态会话录制](#)。

改进了“完整配置”中的主机连接创建体验。选择资源位置后，连接类型 下拉列表现在会显示所有 Citrix 支持的虚拟机管理程序和云服务，它们的可用性取决于：

- 对于没有可访问的 Cloud Connector 的资源位置，只有支持无连接器部署的虚拟机管理程序和云服务可用。
- 对于具有可访问的 Cloud Connector 的资源位置，只有在这些连接器上正确安装了插件的虚拟机管理程序和云服务才可用。

有关详细信息，请参阅[创建和管理连接](#)。

在 **VDA** 升级中选择其他组件。现在，您可以选择在升级 VDA 时升级或安装哪些附加组件。有关详细信息，请参阅 [为 VDA 配置自动升级](#)。

**重要：**

要使用附加组件功能，请确保您的 VDA Upgrade Agent 为 7.34 或更高版本，该版本包含在 VDA 安装程序版本 2206 或更高版本中。

完整配置现在可根据计算机配置文件预配置 **Azure** 计算机的某些设置。在配置 Azure 虚拟机时，“完整配置”现在会根据选定的计算机配置文件预配置以下设置：

- 主机组
- 磁盘加密设置
- 可用性区域
- 许可证类型

支持 **AWS** 实例休眠。现在，您可以启动 AWS 实例，根据需要进行设置并休眠它们。休眠过程存储实例的内存状态及其私有和弹性 IP 地址，使其能够从中断的地方继续运行。有关创建支持休眠的虚拟机的更多信息，请参阅[实例休眠](#)。

支持优化 **AWS** 限制。现在，您可以开启和关闭 AWS 目录中的大量计算机，而不会遇到节流问题。当发送到 AWS 的请求数量超过服务器可以处理的请求数时，就会出现限制问题。此功能通过减少批量开启和关闭计算机电源的 AWS 调用次数来提高效率。它还显著缩短了永久目录中打开和关闭计算机的电源所花费的时间。

**Azure** 托管流量的安全环境。以前，您依靠公共互联网让 Azure 端点与环境中的资源进行交互。结果，由于访问了公共互联网，安全问题引起了人们的关注。借助此功能，MCS 使网络流量能够通过环境中的 Citrix Cloud Connector 进行路由。这使得环境安全，因为现在所有 Azure 托管流量都来自您自己的环境。为此，请在 [CustomProperties](#) 中添加 [ProxyHypervisorTrafficThroughConnector](#)。有关详细信息，请参阅[为 Azure 托管流量创建安全环境](#)。

设置自定义属性后，可以将 Azure 策略配置为拥有 Azure 托管磁盘的专用磁盘访问权限。

支持使用 **Azure Monitor** 代理配置目录虚拟机。Azure Monitor 代理 (AMA) 收集 Monitor 数据并将其提供给 Azure Monitor。使用此功能，您可以预置将 AMA 作为扩展程序安装的 MCS 计算机目录 VM（永久和非永久）。此实现通过在监视数据中唯一识别 VM 来实现监视。有关 AMA 的详细信息，请参阅 [Azure Monitor Agent overview](#) (Azure Monitor 代理概述)。

目前，MCS 仅支持面向此功能的计算机配置文件工作流程。有关配置启用了 AMA 的计算机目录虚拟机的更多信息，请参阅 [预配安装了 Azure Monitor 代理的目录虚拟机](#)。

启用 **MCS** 目录的重启时间表。以前，您可以通过等待下次重新启动或触发所有 VM 的立即重新启动来安排映像更新。使用此功能，您现在可以为要在所需日期和时间触发的目录创建一个一次性重新启动计划，以促进 MCS 映像更新。要创建重新启动计划，请使用 `BrokerCatalogRebootSchedule` 命令。有关详细信息，请参阅 [更改主映像](#)。

在 **Azure** 快速部署中管理过期的客户端密钥。在 Azure Quick Deploy 中，您现在可以在客户端密钥过期时随时了解警报，并轻松更新警报以确保持续访问 Azure 资源。有关详细信息，请参阅 [更新过期的客户端机密](#)。

## 2023 年 5 月

### 新增功能和增强功能

搜索增强功能。此功能增强了过滤器的视觉效果和交互性，为您带来更好的搜索体验。有关详细信息，请参阅在 [“完整配置”管理界面中使用搜索](#)。

新的用户排除策略允许您定义未重定向到用户层的目录路径。用户排除适用于用户个性化层 (UPL)，但不适用于会话主持人。Logoff.txt 现在包含所有活跃用户排除项。有关详细信息，请参阅 [用户个性化层](#)。

支持更新 **MCS** 计算机目录中添加的新 **VM** 的硬件版本。在 VMware 环境中，您现在可以使用计算机配置文件源更新现有 MCS 计算机目录中新添加的 VM 的硬件版本。您无需创建新的计算机目录即可更新添加到目录中的虚拟机的硬件版本。必须使用计算机配置文件工作流程才能使用此功能。

支持筛选 **AWS** 虚拟机实例。以前，当您使用 AWS 虚拟机实例作为计算机配置文件输入来创建 MCS 计算机目录时，由于计算机配置文件输入无效，该目录有时无法正常创建或运行。借助此功能，您现在可以列出可用作有效计算机配置文件虚拟机的 AWS 虚拟机实例。要执行此操作，请使用 `Get-HypInventoryItem` 命令。有关详细信息，请参阅 [筛选虚拟机实例](#)。

支持在 **Azure** 环境中将非基于计算机配置文件的计算机目录转换为基于计算机配置文件的计算机目录。在 Azure 环境中，您现在可以使用虚拟机或模板规范作为计算机配置文件输入，将非基于计算机配置文件的计算机目录转换为基于计算机配置文件的计算机目录。除非被明确的自定义属性覆盖，否则添加到目录中的现有 VM 和新 VM 将从计算机配置文件中获取属性值。有关详细信息，请参阅 [将非基于计算机配置文件的计算机目录转换为基于计算机配置文件的计算机目录](#)。

在 **Azure** 环境中支持对托管磁盘进行双重加密。在 Azure 环境中，您现在可以创建具有双重加密的 MCS 计算机目录。双重加密是指平台端加密（默认）和客户管理的加密 (CMEK)。因此，如果您是高度安全敏感的客户，并且担心与任何加密算法、实现或密钥泄露相关的风险，则可以选择这种双重加密。永久操作系统和数据磁盘、快照和映像均使用双重加密进行静态加密。有关详细信息，请参阅 [托管磁盘上的双重加密](#)。

在 **VMware** 中支持计算机配置文件。在 VMware 环境中，您现在可以使用计算机配置文件创建 MCS 计算机目录。计算机配置文件输入的来源为 VMware 模板。计算机配置文件从 VMware 模板中捕获硬件属性并将其应用到目录中新配置的 VM。有关详细信息，请参阅[使用计算机配置文件创建计算机目录](#)。

能够在 **Azure** 和 **Citrix Hypervisor** 中重置 **MCS** 创建的计算机目录中永久虚拟机的操作系统磁盘。您现在可以使用 PowerShell 命令 **Reset-ProvVMDisk** 在 MCS 创建的计算机目录中重置永久性 VM 的操作系统磁盘。该功能自动执行重置操作系统磁盘的过程。例如，它有助于将 VM 重置为使用 MCS 创建的永久开发桌面目录的初始状态。目前，此功能适用于 Azure、Citrix Hypervisor 和 VMware 虚拟化环境。有关使用 PowerShell 命令重置操作系统磁盘的详细信息，请参阅[重置操作系统磁盘](#)。

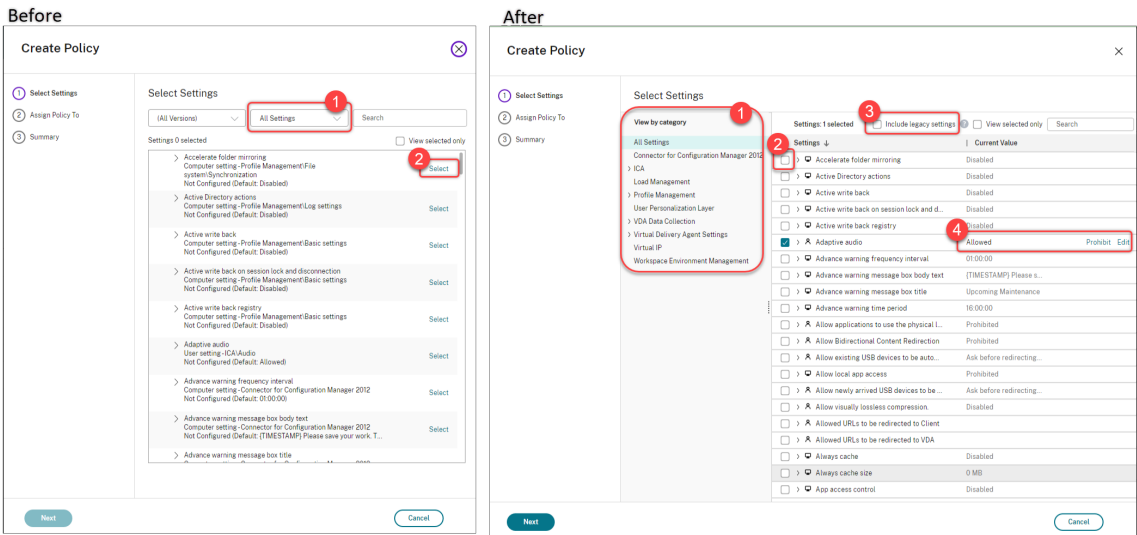
改进了主机连接创建体验。现在，在创建主机连接时，您可以获得以下信息：

- 所有 Citrix 支持的虚拟机管理程序插件列表，包括第三方插件
- 虚拟机管理程序插件的可用性。如果可用性状态为 false，则可能的原因可能是未安装 Cloud Connector

此功能可帮助您正确设置资源位置，从而创建主机连接。有关详细信息，请参阅 [步骤 1. 连接](#)。

策略节点的用户体验得到改进。为了改善用户体验并提高策略管理的效率，我们对“完整配置”>“策略”节点进行了以下改进：

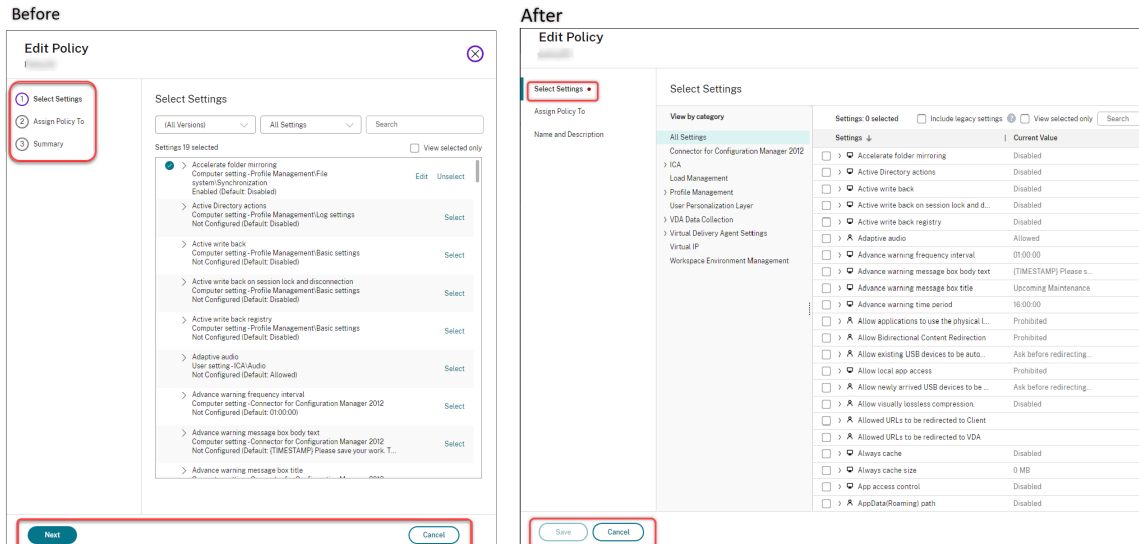
- “创建策略”和“创建模板”操作的新 UI 设计：
  - 策略设置的可扩展文件夹视图。在“选择设置”页面上，所有设置都按类别显示在可展开的树视图中，这样可以更轻松找到设置。
  - 要选择设置，只需单击复选框而不是使用 选择 按钮。
  - 默认情况下，旧版设置处于隐藏状态，因此仅显示最相关的设置。如果需要旧版设置，请选择包括旧版设置。
  - 在布尔值设置旁边添加了一个操作按钮，使您能够直接在设置列表中更改其值。



- 编辑策略操作的新用户界面设计：



- 导航菜单已更新为无序列表。现在，列表中的每个项目都在其页面上包含一个保存按钮。使用这种新设计，您可以保存对项目所做的更改，而无需浏览导航菜单中的所有项目。这些改进功能使策略管理更加高效和简化。
- 导航项目旁边出现红点表示设置错误。



- 拖动以重新确定策略的优先级。在优先级列表中，您现在可以通过将策略拖动到所需位置来更改策略的优先级。

关闭 **AutoScale** 的强制用户注销功能的新选项。现在，“管理 **AutoScale**” > “用户注销通知” 页面上提供了一个名为“既不通知也不强制用户注销”的新选项。选择该选项后，AutoScale 既不会强制用户注销处于排水状态的计算机，也不会通知用户注销并登录到另一台计算机。有关详细信息，请参阅 [用户注销通知](#)。

能够重启 **Windows 365** 云电脑。您现在可以使用 Citrix DaaS 重启 [Windows 365 云电脑](#)。

更多会话详情。当您在“完整配置” > “搜索” > “会话”中查看会话时，会话视图（位于下部窗格中）现在包含更多会话详细信息，可帮助您进行故障排除和识别客户端问题：

- 重新连接时间。会话在断开连接后重新连接的时间。
- 客户平台。用于启动会话的平台。
- 客户端版本。用于启动会话的客户端平台版本。
- 远程主机 IP。托管 Citrix Workspace 的远程主机的 IP 地址。

支持重命名虚拟机的 **Azure AD** 安全组。对于通过 Citrix DaaS 添加到 Azure AD 安全组的虚拟机，您现在可以使用完整配置 > 编辑计算机目录重命名安全组。保存更改后会进行重命名。

计算机帐户的默认域选择。创建目录时，默认情况下会为计算机帐户选择资源（连接）所在的域。

能够显示 **Azure AD** 分配的安全组以供 **VM** 加入。在完整配置中，当您创建加入了 Azure Active Directory 的 VM 时，以成员身份加入已分配的安全组选项现已可用，允许您将 VM 所在的 Azure AD 安全组添加到分配的安全组中。有关详细信息，请参阅[使用 Azure Resource Manager 映像创建计算机目录](#)。

支持更改网络以进行连接。在完整配置中，您现在可以更改网络以进行连接。如果网络正在使用，则无法取消与连接的关联。有关详细信息，请参阅[编辑网络](#)。

能够在 **Azure** 环境中删除标签。以前，带有 **ForgetVM** 参数的 **Remove-ProvVM** 和 **Remove-ProvScheme** PowerShell 命令会从 Citrix 数据库中删除虚拟机和计算机目录。但是，这些命令并没有从资源中删除标记。您必须单独管理未从所有资源中完全删除的虚拟机和计算机目录。有了这个功能，您可以使用：

- 带 **ForgetVM** 参数的 **Remove-ProvVM**，用于从单个 VM 或计算机目录中的 VM 列表中删除在资源上创建的 VM 和标记。
- 带 **ForgetVM** 参数的 **Remove-ProvScheme**，用于从 Citrix 数据库中删除计算机目录，以及在整个计算机目录中的资源上创建的标记。

此实现有助于识别由 MCS 创建但不再由 MCS 使用的孤立资源。

此功能仅适用于永久 VM。有关详细信息，请参阅 [移除标签](#)。

故障计算机警报。Director 的主动通知和警报功能得以增强，根据交付组中故障计算机的百分比添加了新的警报，即故障计算机（百分比）。新的警报条件允许您将警报阈值配置为交付组中的故障计算机的百分比。有关详细信息，请参阅“警报”一文中的[故障计算机](#)部分。

## 2023 年 4 月

### 新增功能和增强功能

使用 **Image Portability Service** 中的 **Citrix Provisioning** 在特定的云平台上发布。使用 Image Portability Service 在 AWS、Azure 和 Google Cloud 中发布的特定工作流程现已可用。此外，Azure 和联网所需的权限已更新。有关更多详细信息，请参阅 [将工作负载迁移到公有云](#)。

支持识别计算机为何处于维护模式。以前，PowerShell 是确定计算机为何处于维护模式的唯一选择。您现在可以在完整配置中实现这一点：

1. 使用“[搜索](#)”找到计算机。
2. 在下部窗格的“详细信息”选项卡上选中“维护原因”。或者将鼠标悬停在“维护模式”列上。可能会出现以下信息：
  - 由管理员：由管理员进入维护模式。
  - 最大注册失败次数：当计算机超过允许的最大注册尝试次数时，进入维护模式。

此外，现在还提供了“维护原因”过滤器。您可以用它来识别目标计算机。

该功能对于管理员在维护模式下对计算机问题进行故障排除非常有用。

使用变量通知用户注销前的剩余时间。强制用户注销时，您现在可以使用 **%s%** 或 **%m%** 作为变量在通知消息中指示指定的时间。要以秒为单位表示时间，请使用 **%s%**。要以分钟为单位表示时间，请使用 **%m%**。有关详细信息，请参阅 [用户注销通知](#)。

支持在存储类型更改失败时自定义开机行为。开机时，由于 Azure 出现故障，托管磁盘的存储类型可能无法更改为所需类型。以前，在这些情况下，VM 将保持关闭状态并向您发送故障消息。使用此功能，您可以选择在存储无法还原到其配

置的类型时打开 VM 的电源，也可以选择保持 VM 处于关闭状态。有关详细信息，请参阅[自定义存储类型更改失败时的开机行为](#)。

支持 **MAK** 激活。现在，您可以使用通过多次激活密钥 (MAK) 激活的 VM 预配永久性计算机目录和非永久性计算机目录。MCS 现在还可以借助此功能与预配的 VM 通信。此实现有助于在不丢失激活次数的情况下激活 Windows 系统。有关详细信息，请参阅[批量许可激活](#)。

支持主机上的 **Azure** 磁盘加密。通过此功能，您现在可以创建具有主机加密功能的 MCS 计算机目录。目前，MCS 仅支持面向此功能的计算机配置文件工作流程。您可以使用 VM 或模板规范作为计算机配置文件的输入。有关详细信息，请参阅[Azure 磁盘主机加密](#)。

在此类型的加密中，托管 VM 的服务器对数据进行加密，加密的数据随后会流经 Azure 存储服务器。因此，这种加密方法会对数据进行端到端加密。有关详细信息，请参阅[Encryption at host - End-to-end encryption for your VM data](#)（主机加密 - VM 数据的端到端加密）。

支持 **GCP** 实例模板作为计算机配置文件的输入。使用此功能，您现在可以选择 GCP 实例模板作为计算机配置文件的输入。实例模板是 GCP 中的轻型资源，因此非常经济实惠。要执行此操作，请使用 PowerShell 命令。有关通过选择 GCP 实例模板来使用 PowerShell 命令创建和更新计算机目录的详细信息，请参阅[使用计算机配置文件作为实例模板创建计算机目录](#)。

支持修改 **Azure AD** 动态安全组名称。您可以从 Azure 门户中修改或删除 Azure AD 动态安全组名称。此操作可使 Azure AD 动态安全组名称与与计算机目录关联的动态安全组不同步。使用此功能，您现在可以修改与计算机目录关联的 Azure AD 动态安全组名称。

此修改可帮助您使存储在 Azure AD 身份池对象中的 Azure AD 动态安全组信息与 Azure 门户中存储的信息保持一致。有关详细信息，请参阅[修改 Azure AD 动态安全组名称](#)。

在 **GCP** 中添加了所需的权限。现在添加了执行以下操作所需的权限：

- 创建主机连接
- 对虚拟机进行电源管理
- 预配目录

有关详细信息，请参阅[关于 GCP 权限](#)。

凭据处理。为了增强安全性，默认情况下，与 VDA 不在同一域中的用户的凭据不会转发到云端。当满足以下所有条件时，登录尝试会失败：

- 用户所在的域与 VDA 不同
- 域之间不存在信任
- StoreFront 与 VDA 安装在同一个域中

以前，在这种情况下，用户无法通过 StoreFront 进行身份验证。因此，Cloud Connector 将用户凭据转发到云端，以便将身份验证请求路由到该用户的正确目的地。如果需要，仍然可以配置此行为。有关详细信息，请参阅 DaaS PowerShell SDK 中 [Set-Brokersite](#) 的 [CredentialForwardingToCloudAllowed](#) 参数。



## 2023 年 3 月

### 新增功能和增强功能

支持为管理员配置角色和作用域。Citrix Cloud 现在在为管理员配置访问权限时支持更灵活性和自定义。以前，您只能选择预定义的角色和作用域对。使用此增强功能，您可以选择一个角色，然后将其与您选择的作用域配对。

有关详细信息，请参阅[为管理员配置自定义访问权限](#)。

支持在现有分配的安全组下创建动态安全组。以前，您可以为计算机目录创建 Azure AD 动态安全组。使用此功能，您还可以在现有 Azure AD 分配的安全组下添加 Azure AD 动态安全组。可执行以下操作：

- 获取安全组信息。
- 获取从本地 AD 服务器同步的所有 Azure AD 分配的安全组或可分配 Azure AD 角色的已分配安全组。
- 获取所有 Azure AD 动态安全组。
- 将 Azure AD 动态安全组添加为已分配 Azure AD 的组的成员。
- 删除 Azure AD 动态安全组和计算机目录时，删除 Azure AD 动态安全组与 Azure AD 分配的安全组之间的成员资格。

有关详细信息，请参阅[在现有 Azure AD 分配的安全组下创建 Azure AD 动态安全组](#)。

支持加入了 **Azure AD** 的虚拟机的 **Azure AD** 动态安全组。Citrix 现在在创建 MCS 计算机目录时支持目录的动态安全组。动态安全组规则根据计算机目录的命名方案将目录中的虚拟机置于动态安全组中。当您想通过 Azure Active Directory (Azure AD) 管理虚拟机时，这很有用。当您想要应用条件访问策略或者通过使用 Azure AD 动态安全组筛选 VM 来分发来自 Intune 的应用程序时，这也非常有用。删除目录时，动态安全组也会被删除。有关详细信息，请参阅[Azure Active Directory 动态安全组](#)。

有关使用动态安全组的许可证要求的更多信息，请参阅 Microsoft 文档在[Azure Active Directory 中创建或更新动态组](#)。

支持通过完整配置将虚拟机添加到 **Azure AD** 安全组。创建加入 Azure AD 的虚拟机时，现在可以使用一个名为 **Azure AD** 安全组的选项。该选项允许您根据虚拟机的命名方案将虚拟机添加到 Azure AD 安全组。有关详细信息，请参阅[创建 Microsoft Azure 目录](#)。

支持在 **Azure** 环境中关闭时将现有 **VM** 的存储类型更改为较低的存储层。在 Azure 环境中，现在可以在关闭 VM 时将现有 VM 的存储类型更改为较低的层级，从而节省存储成本。为此，请使用 StorageTypeAtShutdown 自定义属性。有关详细信息，请参阅[在关闭时将现有 VM 的存储类型更改为较低的存储层](#)。

支持在创建虚拟机时允许使用安全标识符。以前，在使用配置方案指定的配置创建新虚拟机时，无法向 NewProvVM 命令添加安全标识符 (ADAccountSid)。使用此功能，您现在可以在创建新虚拟机时添加参数 ADAccountSid 以唯一标识计算机。有关详细信息，请参阅[在创建虚拟机时添加 SID](#)。

能够获得与 **MCS** 目录相关的警告。以前，您没有收到任何表明您的计算机目录存在问题的信息。使用此功能，您现在可以收到警告，以了解您的 MCS 目录存在的问题并修复这些问题。

与错误不同，警告不会导致启动的配置任务失败。

要获得警告，请使用 PowerShell 命令。有关详细信息，请参阅[检索与目录关联的警告](#)。

用于连接的共享租户。现在，您可以通过订阅连接来添加共享 Azure Compute Gallery 的租户和订阅。因此，在创建或更新目录时，您可以从这些租户和订阅中选择共享映像。有关详细信息，请参阅[编辑连接设置](#)。

删除了对更改 **Azure** 目录操作系统类型的支持。更改目录映像时，仅显示与正在使用的映像具有相同操作系统类型的映像。有了这项增强功能，Citrix DaaS 不再支持在创建目录后更改 Azure 目录的操作系统类型，例如从 Windows 操作系统类型更改为 Linux，反之亦然。

## 2023 年 2 月

### 新增功能和增强功能

支持在不同的 **Azure** 租户之间共享映像。以前，在 Azure 环境中，只能使用 Azure Compute Gallery 与共享订阅共享映像。使用此功能，您现在可以在 Azure Compute Gallery 中选择属于不同租户中不同共享订阅的映像来创建和更新 MCS 目录。有关详细信息，请参阅[在 Azure 租户之间共享映像](#)。

策略建模。策略建模功能现已正式发布。您可以模拟策略以进行规划和测试。有关详细信息，请参阅[使用策略建模向导](#)。

能够开启或关闭预览功能。在“完整配置”>“主页”中，作为具有完全访问权限的 Citrix Cloud 管理员，您现在无需联系 Citrix 即可开启或关闭预览功能。有关详细信息，请参阅[完整配置界面的主页](#)。

使用用户名搜索会话诊断。如果您没有事务 ID，则此功能允许使用以用户名开头的会话启动诊断。如果最终用户尚未捕获事务 ID，此功能对于帮助台管理员对失败的会话进行分类特别有用。

您可以搜索用户名，然后从用户在过去 48 小时内尝试启动的失败会话列表中选择要分类的会话。会话启动诊断页面显示失败会话的详细信息。它列出了发生故障的确切组件和阶段。有关详细信息，请参阅[会话启动诊断](#)一文。

使用 **Secure Private Access** 部署安全的 **Web** 和 **SaaS** 应用程序。在“完整配置”>“应用程序”>“应用程序”选项卡上，操作栏中现在有一个新选项“添加 **Web/SaaS** 应用程序”。该选项允许您使用 Secure Private Access 来部署安全的 Web 和 SaaS 应用程序。Citrix Secure Private Access 为远程用户使用零信任方法访问基于 Web、SaaS 和客户端服务器的应用程序提供了一种简单、灵活的方式。它支持单点登录 Web 和 SaaS 应用程序，以及精细的安全控制，例如水印和复制/粘贴控件，以及其他安全功能。借助 Citrix Secure Private Access，您可以将所有虚拟化和非虚拟化应用程序合并到一个地方，并增强用户的用户体验。请参阅[Citrix Secure Private Access](#)。

在特定时间段内筛选日志内容。现在，“完整配置”>“日志”>“事件”中的持续时间列表中提供了一个新选项“自定义”。使用它来指定要筛选搜索的事件时段。有关详细信息，请参阅[配置日志记录](#)。

**AutoScale** 的更新。我们更新了“当 **AutoScale** 开始开启带标记的计算机时控制”选项，使其易于理解。该选项根据未标记计算机剩余容量的百分比控制 AutoScale 何时开始打开已标记计算机的电源。当百分比降至阈值以下（默认值为 10%）时，AutoScale 开始打开带标记的计算机的电源。当百分比超过阈值时，AutoScale 进入关机模式。有关详细信息，请参阅[带有 AutoScale 标记的计算机（云爆发）](#)。

**App Protection** 策略。现在，您可以在创建或编辑交付组时启用 App Protection。该功能为客户端会话提供反键盘记录和防屏幕捕获功能。有关详细信息，请参阅[创建交付组和管理交付组](#)。

适用于 **AMD GPU** 的实时 **GPU** 利用率。您现在可以在 Monitor 中看到 AMD Radeon Instinct MI25 GPU 和 AMD EPYC 7V12(Rome) CPU 的 GPU 利用率。Monitor 已经支持 NVIDIA Tesla M60 GPU。“GPU 利用率”显示的图表中包含 GPU、GPU 内存以及编码器和解码器的实时利用率百分比，从而对多会话和单会话操作系统 VDA 上的 GPU 相关问题进行故障排除。AMD GPU 利用率图表仅适用于运行 64 位 Windows 和 Citrix Virtual Apps and Desktops 7 2212 或更高版本的 VDA。有关详细信息，请参阅 [GPU 利用率](#)。

支持在 **Azure** 中安排配置更新。在 Azure 环境中，您现在可以使用 PowerShell 命令 [Schedule-ProvVMUpdate](#) 为 MCS 预配的现有计算机的配置更新安排时段。在安排的时段内打开电源或重新启动都会对计算机应用安排的预配方案更新。也可以使用 [Cancel-ProvVMUpdate](#) 在计划的时间之前取消配置更新。

可以计划和取消以下对象的配置更新：

- 单个或多个 VM
- 整个目录

有关详细信息，请参阅[计划配置更新](#)。

支持直接从 **Google Cloud Marketplace** 使用 **Citrix Ready** 的示意图。现在，您可以在 Google Cloud Marketplace 上浏览和选择 Citrix 提供的映像来创建 MCS 目录。目前，MCS 仅支持面向此功能的计算机配置文件工作流程。有关详细信息，请参阅 [Google Cloud Marketplace](#)。

在 **SCVMM** 主机连接中限制主机组范围。以前，主机连接到 SCVMM 需要管理员配置单个顶层主机组。这意味着管理员可以查看单个顶层主机组下的所有主机组、群集或主机。使用此功能，在单个 SCVMM 管理不同数据中心的多群集的大型部署中，您现在可以限制管理员的主机组范围。为此，您可以使用 Microsoft System Center Virtual Machine Manager (VMM) 控制台中的委派管理员角色来选择管理员必须有权访问的主机组。有关详细信息，请参阅[安装和配置虚拟机管理程序](#)。

支持 **Azure** 中的区域冗余存储。以前，MCS 仅提供本地冗余存储。借助此功能，区域冗余存储现在是 Azure 中的一个选项，允许您根据要使用的冗余类型选择存储类型。区域冗余存储可跨多个可用性区域复制 Azure 托管磁盘，这允许您利用其他区域的冗余从一个区域的故障中恢复。有关详细信息，请参阅[启用区域冗余存储](#)。

## 2023 年 1 月

### 新增功能和增强功能

**VM** 关闭时可选择将存储磁盘降级为标准 **HDD**。创建或更新 Azure 目录时，磁盘设置页面上现在提供了一个新选项启用节约存储成本。该选项通过将存储磁盘降级为标准 HDD，并在 VM 关闭时降级为回写式缓存磁盘来节省存储成本。VM 在重新启动时切换到其原始设置。有关详细信息，请参阅[创建 Microsoft Azure 目录](#)。

支持在“完整配置”中配置会话漫游。以前，PowerShell 是您为应用程序和桌面配置会话漫游的唯一选择。现在，您可以在“完整配置”中执行此操作。有关详细信息，请参阅[管理交付组](#)。

重命名了一些操作以更好地与其实际含义保持一致。我们在“完整配置”>“计算机目录”和“完整配置”>“交付组”中重命名了以下操作。执行这些操作的工作流程保持不变。

- 更新计算机重命名为更改主映像

- 回滚计算机更新重命名为回滚主映像
- 升级目录重命名为更改功能级别
- 升级交付组重命名为更改功能级别
- 撤消升级目录重命名为撤消功能级别更改
- 撤消升级交付组已重命名为撤消功能级别更改

支持使用文件夹组织应用程序组。现在，您可以创建嵌套文件夹来组织应用程序组以便于访问。有关详细信息，请参阅[使用文件夹组织应用程序组](#)。

增强了交付组的限制。以前，在限制交付组使用应用程序或桌面时，只能指定允许在交付组中使用应用程序或桌面的用户和用户组。现在，您还可以添加要屏蔽的用户和用户组。当您一组用户添加到允许列表中，同时想要在允许列表中屏蔽一部分用户时，此增强功能很有用。有关详细信息，请参阅[创建交付组](#)。

从 **Monitor** 访问“**Citrix Analytics for Performance** - 会话详细信息”。来自 Citrix Analytics for Performance 的“会话详细信息”页面现已集成到 Monitor 中。在 Monitor 的“会话”页面中单击“查看会话时间表”，以在 Monitor 中查看 Citrix Analytics for Performance 的“会话详细信息”页面。这要求您拥有有效的 Citrix Analytics for Performance 权限。会话详细信息适用于在 Citrix Analytics for Performance 中归类为“优秀”、“一般”或“差”的会话。

您可以查看最近三天的会话体验趋势以及影响体验的因素。此信息补充了 Monitor 中提供的实时数据，帮助台管理员在解决与会话体验相关的问题时会使用这些数据。

有关详细信息，请参阅[网站分析](#) 文章。

在“完整配置”中删除非永久 **VM** 或其计算机目录时，会将其从虚拟机管理程序或云服务中删除。现在，在虚拟机管理程序或云服务中保留虚拟机的选项仅适用于永久虚拟机。有关详细信息，请参阅[管理计算机目录](#)。

## 2022 年 12 月

### 新增功能和增强功能

支持创建以下主 **VM**：加入了 **Azure AD**、加入了混合 **Azure AD**、目录启用了 **Microsoft Intune** 并且加入了 **Azure AD**。现在，您可以创建以下主 VM：加入了 Azure AD、加入了混合 Azure AD、目录启用了 Microsoft Intune 并且加入了 Azure AD、加入了混合 Azure AD 以及未加入域。如果要通过 Microsoft Intune 管理主 VM，请使用 VDA 版本 2212 或更高版本，并且在创建或更新计算机目录时不要跳过映像准备工作。

有关计算机标识的详细信息，请参阅[加入了 Azure Active Directory、Microsoft Intune 和加入了混合 Azure Active Directory](#)。

**MCS** 支持在不访问虚拟机管理程序的情况下删除 **VM** 对象。现在，您无需访问虚拟机管理程序即可在 MCS 中删除 VM 对象。删除虚拟机或配置方案时，MCS 需要移除标记，这样就不会再跟踪或识别资源。以前，如果无法访问虚拟机管理程序，则会忽略标记删除失败。使用此功能，如果在使用 **Remove-ProvVM** 命令时无法访问虚拟机管理程序，则删除标记将失败，但是通过使用 **PurgeDBOnly** 选项，您仍然可以从数据库中删除 VM 资源对象。有关详细信息，请参阅[删除没有虚拟机管理程序访问权限的计算机](#)。

## 2022 年 11 月

### 新增功能和增强功能

支持交付 **MSIX** 和 **MSIX** 应用程序附加应用程序。在 完整配置 > 应用程序包中，您现在可以上载 MSIX 和 MSIX 应用程序将打包的应用程序附加到 Citrix Cloud，然后将其交付给您的用户。有关详细信息，请参阅[应用程序包](#)。

提示输入不支持的 **VDA** 版本和功能级别。现在，“完整配置”界面会提醒您有关不受支持的 VDA 版本和功能级别。为避免潜在问题：

- 如果计算机运行不支持的 VDA 版本，系统会提示您升级到支持的版本。
- 如果不支持目录或交付组的功能级别，系统会提示您将其设置为更高的级别。

提示：

VDA 受 [Citrix Virtual Apps and Desktops 的 CR 和 LTSR 生命周期覆盖](#)。

对主映像进行注释的功能扩展到目录创建。在“完整配置”中创建 MCS 目录时，您现在可以为其主映像添加注释。有关详细信息，请参阅 [主映像](#)。

支持通过“完整配置”导出桌面分配数据。在查看单会话操作系统交付组的桌面分配时，您现在可以将任务数据导出到 CSV 文件中以供审核。为此，请在 完整配置 > 交付组中选择这样的交付组，转到 桌面 选项卡，然后单击选项卡左上角的 导出。

所有“应用程序”和“应用程序文件夹”选项卡合并为一个。在“完整配置”>“应用程序”中，“所有应用程序 和 应用程序文件夹”选项卡已合并到一个选项卡“应用程序”中。此更改统一了“完整配置”节点上文件夹视图管理的用户体验。

支持在 **Azure** 环境中关闭 **VM** 时将存储类型更改为较低层。在 Azure 环境中，您现在可以在关闭 VM 时将托管磁盘的存储类型切换到较低的层来节省存储成本。为此，请使用 [StorageTypeAtShutdown](#) 自定义属性。关闭 VM 时，磁盘的存储类型更改为较低层（如 [StorageTypeAtShutdown](#) 自定义属性中所指定）。打开 VM 的电源后，存储类型将更改回原始存储类型（如 [StorageType](#) 或 [WBCDiskStorageType](#) 自定义属性中所指定）。有关详细信息，请参阅[关闭 VM 时将存储类型更改为较低的层](#)。

筛选器视图中的更新。Monitor 中的“过滤器”页面已更新，包括单独的“已保存”和“默认”筛选器列表，以便更好地显示和访问筛选器。您可以从计算机、会话、连接或应用程序实例中选择视图。然后，您可以从“已保存筛选器”或“默认筛选器”列表选择一个筛选器，以查看筛选后的数据列表。您可以使用下拉列表来细化筛选条件或编辑现有标准。您可以将过滤器保存在“已保存的筛选器”列表中。有关详细信息，请参阅[过滤器](#)一文。

能够在 **MCS** 创建的计算机目录中重置永久虚拟机的操作系统磁盘。在 VMware 虚拟化环境中，您现在可以使用 PowerShell 命令 [Reset-ProvVMDisk](#) 在 MCS 创建的计算机目录中重置永久性 VM 的操作系统磁盘。该功能自动执行重置操作系统磁盘的过程。例如，它有助于将 VM 重置为使用 MCS 创建的永久开发桌面目录的初始状态。

有关使用 PowerShell 命令重置操作系统磁盘的更多信息，请参阅[重置操作系统磁盘](#)。

支持在 **Azure** 环境中更新 **MCS** 置备的计算机的计算机配置文件和其他自定义属性。以前，在 Azure 环境中，您可以使用 [Request-ProvVMUpdate](#) 更新 MCS 置备计算机的 [ServiceOffering](#) 自定义属性。现在，您还可以更新计算机配置文件和以下自定义属性：



- [StorageType](#)
- [WBCDiskStorageType](#)
- [IdentityDiskStorageType](#)
- [LicenseType](#)
- [DedicatedHostGroupId](#)
- [PersistWBC](#)
- [PersistOsDisk](#)
- [PersistVm](#)

有关详细信息，请参阅[将预配的计算机更新为当前预配方案状态](#)。

支持 **GCP** 中的计算机配置文件。当您创建目录以在 Google 云端平台 (GCP) 环境中使用 Machine Creation Services (MCS) 预配计算机时，现在可以使用计算机配置文件从虚拟机捕获硬件属性并将其应用到目录中新预配的虚拟机。不使用 [MachineProfile](#) 参数时，将从主映像 VM 或快照中捕获硬件属性。

计算机配置文件在 Linux 和 Windows 操作系统中均可使用。

有关如何使用计算机配置文件创建计算机目录的信息，请参阅[使用计算机配置文件创建计算机目录](#)。

支持在 **GCP** 环境中更新 **MCS** 配置的计算机。在 GCP 环境中，[Set-ProvScheme](#) 更改模板（预配方案），并且不影响现有计算机。现在，您可以使用 PowerShell 命令 [Request-ProvVMUpdate](#) 将当前的预配方案应用到现有计算机（或一组计算机）。目前，在 GCP 中，此功能支持的属性更新是计算机配置文件。有关详细信息，请参阅[使用 PowerShell 更新已预配的计算机](#)。

## 2022 年 10 月

### 新增功能和增强功能

支持同时使用计算机配置文件和主机组。使用 Azure Resource Manager 主映像创建目录时，现在可以同时使用计算机配置文件和主机组。这在您想要使用 trusted Launch 来提高安全性，同时在专用主机上运行计算机的情况下很有用。有关详细信息，请参阅 [Microsoft Azure Resource Manager 虚拟化环境](#)。

支持使用文件夹组织交付组。现在，您可以创建文件夹树来组织交付组以便于访问。有关详细信息，请参阅 [使用文件夹整理交付组](#)。

支持通过“完整配置”为计算机安排一次性重新启动。现在，当您为交付组创建重新启动计划时，可以使用新选项一次。使用此选项，您可以安排交付组中的计算机在指定的日期和时间重新启动一次。有关详细信息，请参阅[创建重新启动计划](#)。

高级探测调度。现在可以通过 Monitor 改进应用程序和桌面探测器的调度。使用此功能，可以将 Citrix Probe Agent 配置为在一周中的特定日期运行探测任务，并在白天按指定的间隔重复执行探测任务。这允许您安排单个探测任务在一天和一周的特定时间重复。现在，您可以使用设置为在适当时间定期运行的探测器来主动检查站点运行状况。此功能简化了 Monitor 中的探头设置和管理。有关详细信息，请参阅[应用程序和桌面探测](#)。

## 2022 年 9 月

### 新增功能和增强功能

旧版本的 **Remote PowerShell SDK** 现已过时。如果您使用的是已过时的版本，SDK 将停止运行，并且您会看到一条错误消息，提示您下载当前版本。如果发生这种情况，请从 [Citrix 网站](#) 下载最新的 Remote PowerShell SDK。

在 **Azure** 中受信任启动的计算机目录。在 Azure 环境中，您可以创建启用受信任启动的计算机目录，并使用虚拟机清单的 **SupportsTrustedLaunch** 属性来确定支持受信任启动的虚拟机大小。

受信任启动是提高第 2 代 VM 安全性的无缝方式。受信任启动可防范高级和持续攻击技术。有关详细信息，请参阅[支持受信任启动的计算机目录](#)。

支持识别由 **MCS** 创建的 **Microsoft System Center Virtual Machine Manager** 资源。您现在可以使用标记识别 MCS 创建的 Microsoft System Center Virtual Machine Manager (SCVMM) 资源。有关 MCS 向资源添加的标记的详细信息，请参阅[识别 MCS 创建的资源](#)。

支持识别由 **MCS** 创建的 **VMware** 资源。现在，您可以使用标记识别 MCS 创建的 VMware 资源。有关 MCS 向资源添加的标记的详细信息，请参阅[识别 MCS 创建的资源](#)。

支持优化 **AWS** 工作区限制。现在，您可以在 AWS Workspace 中打开和关闭大量计算机的电源，而不会遇到限制问题。当发送到 AWS Workspace 的请求数量超过服务器可以处理的请求数量时，就会出现限制问题。因此，Citrix 现在将多个请求分组为一个请求，然后再将其发送到 AWS Workspace SDK。

在主页中查看计算机数量时能够检查计算机的详细信息。在 主页中按可用性状态查看计算机计数时，现在可以单击某个状态以查看处于该状态的计算机的详细信息。有关详细信息，请参阅[完整配置界面的主页](#)。

支持在同一 **Azure** 租户中使用来自不同订阅的映像创建计算机目录。以前，在 Azure 环境中，您只能在订阅中选择一个映像来创建计算机目录。使用此功能，您现在可以在 Azure Compute Gallery（以前称为“共享映像库”）中选择属于其他共享订阅的映像来创建和更新 MCS 目录。

有关创建目录的更多信息，请参阅[使用 Azure Resource Manager 映像创建计算机目录](#)。

有关与同一租户中的另一个服务主体共享映像的信息，请参阅[与同一租户中的另一个服务主体共享映像](#)。

有关用于从其他订阅中选择映像的 PowerShell 命令的信息，请参阅[使用 PowerShell 从不同的订阅中选择映像](#)。

有关 Azure Compute Gallery 的更多信息，请参阅[Azure 共享映像库](#)。

## 2022 年 8 月

### 新增功能和增强功能

支持识别由 **MCS** 创建的 **Citrix** 虚拟机管理程序资源。现在，您可以使用标记标识由 MCS 创建的 Citrix 虚拟机管理程序资源。有关 MCS 向资源添加的标记的详细信息，请参阅[识别 MCS 创建的资源](#)。

支持同时使用主机组和 **Azure** 可用性区域。在 Azure 环境中，现在有一项飞行前检查，以根据自定义属性和主机组区域中指定的 Azure 可用性区域来评估计算机目录的创建是否成功。如果可用性区域自定义属性与主机组的区域不匹配，目录创建将失败。

主机组是表示专用主机的集合的资源。专用主机是指提供托管一个或多个虚拟机的物理服务器的服务。

Azure 可用性区域是每个 Azure 区域中物理上独立的位置，可以容忍本地故障。

有关导致计算机目录创建成功或失败的可用性区域和主机组区域的各种组合的详细信息，请参阅 [同时使用主机组和 Azure 可用性区域](#)。

支持在 **VMware** 中更新计算机目录的文件夹 ID。在 VMware 虚拟化环境中，您现在可以使用 `Set-ProvScheme` 中的自定义属性 `FolderID` 来更新 MCS 计算机目录的文件夹 ID。更新文件夹 ID 后创建的 VM 将在此新文件夹 ID 下创建。如果未在 `CustomProperties` 中指定此属性，则会在主映像所在的文件夹下创建 VM。有关更新文件夹 ID 的详细信息，请参阅[更新计算机目录的文件夹 ID](#)。

时区设置。现在，您可以使用日期和时间设置配置界面的 日期和时间 格式，以满足您的偏好。有关详细信息，请参阅 [时区设置](#)。

**Image Portability Service (IPS)** 现在支持 **Amazon Web Services (AWS)**。通过配置 AWS 所需的权限和组件，可以将 IPS 工作流程用于 AWS 帐户。有关更多详细信息，请参阅[将工作负载迁移到公有云](#)。

在 **Azure** 环境中准备映像期间设置页面文件。在 Azure 环境中，您现在可以避免页面文件位置的潜在混淆。为此，MCS 现在可以在映像准备期间创建预配方案时确定页面文件的位置。此计算基于某些规则。临时操作系统磁盘 (EOS) 和 MCS I/O 等功能具有自己的预期页面文件位置，并且彼此独占。此外，如果将映像准备与预配方案创建分离，则 MCS 会正确地确定页面文件的位置。有关页面文件位置的详细信息，请参阅[页面文件位置](#)。

支持在 **Azure** 环境中更新页面文件设置。在 Azure 环境中创建目录时，现在可以使用 PowerShell 命令指定页面文件设置，包括其位置和大小。这将覆盖 MCS 确定的页面文件设置。您可以通过运行具有以下自定义属性的 `New-ProvScheme` 命令来执行此操作：

- `PageFileDiskDriveLetterOverride`：页面文件位置磁盘驱动器盘符
- `InitialPageFileSizeInMB`：初始页面文件大小，以 MB 为单位
- `MaxPageFileSizeInMB`：最大页面文件大小，以 MB 为单位

有关更新页面文件设置的详细信息，请参阅[更新页面文件设置](#)。

主页更新。“入门”小组件现在有了新的外观和感觉。主页的其他更新包括：

- 右上角新增的“刷新”和“帮助”图标。
- 可点击的资源计数，提供对相关资源页面的快速访问。
- 增强了“不喜欢”图标。如果您不喜欢某个推荐，该推荐会消失。如果您不喜欢推荐小部件，则该小组件将消失。

有关详细信息，请参阅[主页](#)。

支持启用 **Azure VM** 扩展。使用 ARM 模板规范作为计算机配置文件创建计算机目录时，您现在可以将 Azure VM 扩展添加到目录中的 VM，查看支持的扩展列表以及删除已添加的扩展。Azure VM 扩展是在 Azure VM 上提供部署后配置和自动化任务的小型应用程序。例如，如果 VM 需要安装软件、防病毒保护或需要在其内部运行脚本，则可以使用 VM 扩展。有关如何启用 Azure VM 扩展的详细信息，请参阅[使用 PowerShell 启用 Azure VM 扩展](#)。



对临时操作系统磁盘的受信任启动支持。现在，您可以在具有受信任启动的 Windows 上使用临时操作系统磁盘创建预配方案。受信任启动是提高第 2 代 VM 安全性的无缝方式。它结合了可以独立启用的技术，例如安全启动和可信平台模块 (vTPM) 的虚拟化版本，从而防止高级和持续攻击技术。有关创建计算机目录的详细信息，请参阅[使用 Azure Resource Manager 映像创建计算机目录](#)。

## 2022 年 7 月

### 新增功能和增强功能

单会话操作系统计算机的动态会话超时。动态会话超时现在支持单会话操作系统计算机。需要具有至少一个 2206 或更高版本的 VDA 的交付组。请确保这些 VDA 已在 Citrix Cloud 中至少注册过一次。有关详细信息，请转到[动态会话超时](#)。

在 **AutoScale** 中发送注销提醒而不强制用户注销。AutoScale 中的 用户注销通知（以前称为“强制用户注销”）中现在提供了一项新功能。该功能允许您向用户发送注销提醒，而无需强制他们注销。这样做可以避免因强制用户注销会话而导致的潜在数据丢失。有关详细信息，请参阅[用户注销通知](#)。

在 **Azure** 中创建 **Linux VM** 目录时能够设置 **Linux** 操作系统许可证类型。使用完整配置界面，您现在可以在 Azure 中创建 Linux VM 目录时选择 Linux 操作系统许可证类型。自带 Linux 许可证有两种选择：Red Hat 企业 Linux 和 SUSE Linux 企业服务器。有关详细信息，请参阅[使用 Azure Resource Manager 映像创建计算机目录](#)。

增强了完整配置中的搜索体验。“搜索”节点提供了以下新增功能和增强功能：

- 能够导出搜索结果。您现在可以导出搜索结果。为此，请单击右上角的导出图标。
- 新的过滤器可用。现在可以使用一个名为“待定电源操作”的过滤器。使用筛选器来细化您的搜索。
- 对某些项目的“不包含”搜索支持。计算机名称和标记等项目现在支持“不包含”搜索条件。
- 支持在添加滤镜时搜索对象。为以下对象添加筛选器时，您现在可以搜索它们：连接、计算机目录、交付组、应用程序组和标记。

有关详细信息，请参阅在[“完整配置”管理界面中使用搜索](#)。

支持 **VMware** 存储配置文件。使用 vSAN 数据存储上的主映像创建计算机目录时，现在可以将存储策略（如 RAID-1 或 RAID-5 信息）从主映像复制到创建的目标设备。对于现有目录，即使您更新了目录，存储策略也将保持不变。

支持 **RestrictedKrbHost SPN** 注册。现在，所有 Citrix MCS 创建的计算机帐户都已使用 **RestrictedKrbHost** 服务主体名称 (SPN) 进行注册。这样可以避免在 MCS 创建计算机帐户后运行 **setspn** 命令为其注册 SPN 的要求。

完全配置的应用程序包，用于交付 **Microsoft** 打包的应用程序。App-V 节点已重命名为应用程序包，并重新设计以容纳更多类型的 Microsoft 打包应用程序。以前，您必须使用发现模块将 App-V 打包的应用程序添加到您的环境中以进行交付。现在，您可以使用“应用程序包”节点在一个位置添加和交付应用程序。有关详细信息，请参阅[应用程序包](#)。

支持将 **ARM** 模板规范用作计算机配置文件。以前，只能将 VM 用作计算机配置文件。现在，在创建 Azure 计算机目录时，也可以将 ARM 模板规范用作计算机配置文件。此功能允许您利用 Azure ARM 模板功能，例如版本控制。为确保所

选规范配置正确且包含必需的配置，我们对其进行验证。如果验证失败，系统会提示您选择其他计算机配置文件。有关详细信息，请参阅[使用 Azure Resource Manager 映像创建计算机目录](#)。

支持验证 **ARM** 模板规范。现在，您可以验证 ARM 模板规范，以确保它可以用作计算机配置文件来创建计算机目录。有两种方法可以验证 ARM 模板规范：

- 使用完整配置管理界面。
- 使用 PowerShell 命令。

有关验证 ARM 模板规范的详细信息，请参阅 [使用 Azure Resource Manager 映像创建计算机目录](#)。

## 2022 年 6 月

### 新增功能和增强功能

对单会话操作系统计算机的重新启动计划支持。以前，重新启动计划功能仅适用于多会话操作系统计算机。它现在也可用于单会话操作系统计算机。现在，您可以为包含单会话操作系统计算机的交付组创建重新启动计划。有关详细信息，请参阅 [为交付组中的计算机创建和管理重新启动计划](#)。

用于执行用户名预检查的选项。现在，当您输入域凭据时，“检查名称”选项可用。使用选项，您可以检查用户名是有效还是唯一。例如，在以下情况下，该选项很有用：

- 多个域中存在相同的用户名。系统会提示您选择所需的用户。
- 您记不起域名。可以在不指定域名的情况下输入用户名。如果检查通过，则会自动填充域名。

有关详细信息，请参阅 [域凭据](#)。

能够更改现有配置方案的网络设置。现在，您可以更改现有置备方案的网络设置，以便在新子网中创建新的 VM。使用 `Set-ProvScheme` 命令中的 `-NetworkMapping` 参数更改网络设置。只有方案中新置备的 VM 才具有新的子网设置。您还必须确保子网位于同一个托管单元下。有关详细信息，请参阅 [更改现有置备方案的网络设置](#)。

检索 **Azure VM**、托管磁盘、快照、**Azure VHD** 和 **ARM** 模板的区域名称信息。现在，您可以显示 Azure VM、托管磁盘、快照、Azure VHD 和 ARM 模板的区域名称信息。分配计算机目录后，将为主映像上的资源显示此信息。有关详细信息，请参阅 [检索 Azure VM、托管磁盘、快照、Azure VHD 和 ARM 模板的区域名称信息](#)。

能够在 **Azure** 环境中使用计算机配置文件属性值。在使用计算机配置文件创建 Azure 目录时，现在可以从 ARM 模板规范或 VM 中设置属性值（以用作计算机配置文件为准），前提是这些值未在自定义属性中明确定义。受此功能影响的属性如下：

- 可用性区域
- 专用主机组 ID
- 磁盘加密集 ID
- 操作系统类型
- 许可证类型
- 服务方案

- 存储类型

如果计算机配置文件中缺少某些属性，并且未在自定义属性中定义，则在适用的情况下将使用这些属性的默认值。有关详细信息，请参阅[使用计算机配置文件属性值](#)。

扩展了对 **VDA** 升级的支持。使用完整配置界面，您现在可以升级 MCS 置备的持久性计算机。您可以按目录或每台计算机升级它们。有关详细信息，请参阅 [使用完整配置界面升级 VDA](#)。

**Citrix Cloud Japan** 和 **Citrix Cloud Government** 控制平面中的 **Citrix Probe Agent** Citrix Probe Agent 现在支持 Citrix Cloud Japan 和 Citrix Cloud Government 控制平面上托管的站点。要在这些平面中使用探测代理，请将路径 “\HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region” 中的注册表值设置为 2，对于政府区域，将路径中的注册表值设置为 3。Citrix Probe Agent 可自动检查站点中发布的虚拟应用程序和桌面的运行状况。有关详细信息，请参阅[应用程序和桌面探测](#)。

自定义用于 **VDA** 和 **Cloud Connector** 之间通信的端口。现在，您可以根据特定的安全要求自定义 VDA 用于与 Cloud Connector 通信的端口。如果您的安全团队不允许打开默认端口（端口 80）或者默认端口已在使用中，则此功能非常有用。有关详细信息，请参阅 [自定义用于与 Cloud Connector 通信的端口](#)。

支持使用文件夹组织计算机目录。现在，您可以创建嵌套文件夹来组织计算机目录，以便于访问。有关详细信息，请参阅 [使用文件夹组织目录](#)。

支持 **SCVMM 2022**。Citrix DaaS 现在支持 Microsoft System Center Virtual Machine Manager (SCVMM) 2022。SCVMM 提供了一系列服务，包括维护部署 VM 所需的资源。有关 SCVMM 2022 中支持的新增功能的详细信息，请参阅 [What's new in System Center Virtual Machine Manager](#) (System Center Virtual Machine Manager 中的新增功能)。

支持在 **AWS** 上配置最大并发预配置操作参数。Citrix DaaS 现在支持 `MaximumConcurrentProvisioningOperation` 作为 AWS 上的 MCS 的可配置自定义属性。`MaximumConcurrentProvisioningOperations` 是用于确定可以同时创建或删除的 VM 数量的属性。虽然默认情况下 MCS 最多支持 100 个并发置备操作，但您现在可以输入 PowerShell 命令来自定义此值。您可以输入 1 到 1000 之间的范围。将此属性设置为您的首选值允许您控制在创建或删除 VM 时可以执行的并行任务数。有关配置最大并发置备操作数的详细信息，请参阅 [主机连接默认值](#)。

## 2022 年 5 月

### 新增功能和增强功能

增强了会话启动诊断。Citrix DaaS 现在支持详细的会话启动失败诊断。现在，您可以查看会话启动序列中涉及的组件。上次生成的错误代码出现故障的组件将突出显示。这有助于确定会话启动失败的确切原因并采取建议的措施。

“事务详细信息” 面板扩展了“事务”页面，该面板包含指示错误发生情况的组件列表。单击组件名称将显示“组件详细信息”和“上次已知故障详细信息”。此时将显示“失败原因”和“错误代码”。单击“了解更多”链接将显示有关[错误代码](#)的特定代码，其中包含详细说明和建议的操作。有关详细信息，请参阅[会话诊断](#)。

支持在 **Remote PowerShell SDK** 中使用 **Set-ProvServiceConfigurationData** 现在，您可以使用 Remote PowerShell SDK 运行 `Set-ProvServiceConfigurationData` 来对所有适用的参数进行设置。您也可

以使用此命令在映像准备期间跳过启用 DHCP。以下是 `Set-ProvServiceConfigurationData` 支持的设置列表：

- 更改映像准备超时：`Set-ProvServiceConfigurationData -Name "ImageManagementPrep_ProcTimeout -value 60`
- 跳过启用 DHCP：`Set-ProvServiceConfigurationData -Name ImageManagementPrep_ExcludedSteps -Value EnableDHCP`
- 跳过 Microsoft Windows KMS 重置：`Set-ProvServiceConfigurationData -Name ImageManagementPrep_ExcludedSteps -Value OsRearm`
- 跳过 Microsoft Office KMS 重置：  
`Set-ProvServiceConfigurationData -Name ImageManagementPrep_ExcludedSteps -Value OfficeRearm`
- 禁用准备 VM 自动关闭：  
`Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value true`
- 禁用域注入：  
`Set-ProvServiceConfigurationData -Name DisableDomainInjection -Value true`

能够在使用 **PowerShell** 命令创建 **Linux** 计算机目录时设置 **Linux** 许可证类型。使用 PowerShell 命令，您可以在创建 Linux 计算机目录时设置 Linux 许可证类型。自带 Linux 许可证有两种选择：RHEL\_BYOS 和 SLES\_BYOS。该设置默认为 Azure Linux 许可。有关详细信息，请参阅[使用 Azure Resource Manager 映像创建计算机目录](#)。

支持识别由 **MCS** 创建的所有 **Azure** 资源。现在，您可以使用名为 `provschemeID` 的标记识别由 MCS 创建的所有 Azure 资源，例如映像、ID 磁盘、操作系统磁盘、NIC、VM 等，这些资源与 ProvScheme 关联。有关 MCS 向资源添加的标记的详细信息，请参阅[识别 MCS 创建的资源](#)。

通过 **SCVMM** 支持 **Azure** 堆栈 **HCI** 预配。MCS 现在通过 Microsoft System Center Virtual Machine Manager (SCVMM) 支持 Azure Stack HCI 预配。您可以使用包括 SCVMM 在内的现有工具管理 Azure 堆栈 HCI 群集。有关详细信息，请参阅[Microsoft System Center Virtual Machine Manager 虚拟化环境](#)。

支持手动添加非 **Active Directory** 用户。使用完整配置管理界面，现在可以在为目录添加非 Active Directory 用户时输入以分号分隔的用户名列表。添加驻留在不同目录中的用户时，请考虑该格式。例如，如果用户在 Active Directory 中，则直接输入姓名。如果没有，请按以下格式输入名称：`<identity provider>:<user name>`。示例：`AzureAD:username`。有关详细信息，请参阅[创建计算机目录](#)。

## 2022 年 4 月

### 新增功能和增强功能

完整配置界面的主页。完整配置现在有一个主页，该主页提供了 Citrix DaaS 部署和工作负载的概述，以及可帮助您从订阅中获得最大收益的信息。该页面由以下部分组成：

- 服务概述。概述您的 Citrix DaaS 部署和工作负载。
- 建议。推荐订阅中提供的功能并收集您的反馈。
- 新增功能。显示最新功能。
- 预览功能。显示当前处于预览状态的功能。
- 入门。显示指导您完成初始设置的步骤。

有关详细信息，请参阅[主页](#)。

显示目录创建和更新的进度。“完整配置”现在可让您随时了解目录创建和更新的最新信息。您可以获得创建和更新过程的概览、查看已执行步骤的历史记录以及监视当前步骤的进度和运行时间。有关详细信息，请参阅[开始创建目录](#)。

根据所选区域显示可用的虚拟机管理程序和云服务。在“完全配置”中，创建托管连接时，您需要先选择一个区域，然后才能选择连接类型。连接类型下拉列表显示该区域可用的虚拟机管理程序和云服务。以前，为确保连接类型列表显示所需的虚拟机管理程序或云服务，您必须在每个区域中安装其插件。有了这个新的配置序列，您现在只能在所需的区域中安装插件。

您还可以使用 PowerShell 命令获取选定区域中可用的虚拟机管理程序插件列表。有关详细信息，请参阅[创建连接和资源](#)。

在完全配置中支持加入非本地 **AD** 的用户。在将用户分配到已置备的桌面或应用程序、交付组或应用程序组的界面中提供了一个新字段“选择身份类型”。通过该字段，您现在可以从 Citrix Cloud 连接的以下任何身份提供商中选择用户帐户：

- Active Directory
- Azure Active Directory
- Okta

能够拒绝 **Google Cloud Platform (GCP)** 和 **Azure** 环境中的无效自定义属性。现在，如果自定义属性设置为 **New-ProvScheme** 且 **Set-ProvScheme** 不生效，则可以避免潜在的混淆。如果您指定了一个或多个不存在的自定义属性，则会收到一条错误消息。有关详细信息，请参阅[关于设置自定义属性的重要注意事项](#)。

支持创建已加入 **Azure Active Directory** 的计算机。在完整配置中，当您创建目录时，已加入 **Azure Active Directory** 的标识类型现在可以在计算机标识中使用。使用该标识类型，您可以使用 MCS 创建加入到 Azure Active Directory 的计算机。您还有一个额外的选项，在 **Microsoft Intune** 中注册计算机，以便在 Microsoft Intune 中注册计算机进行管理。

有关创建已加入 Azure Active Directory 的目录的信息，请参阅[创建计算机目录](#)。有关与 Azure Active Directory 加入相关的要求和注意事项的信息，请参阅[已加入 Azure Active Directory](#)。

支持创建已加入混合 **Azure Active Directory** 的计算机。在完整配置中，当您创建目录时，已加入混合 **Azure Active Directory** 标识类型现在可以在计算机标识中使用。使用该标识类型，您可以使用 MCS 创建已加入混合 Azure Active Directory 的计算机。这些计算机归某个组织所有，并使用属于该组织的 Active Directory 域服务帐户登录。

有关创建已加入混合 Azure Active Directory 的目录的信息，请参阅[创建计算机目录](#)。有关与已加入混合 Azure Active Directory 相关的要求和注意事项的信息，请参阅[已加入混合 Azure Active Directory](#)。



快照的 **Azure** 受信任启动支持。除了映像之外，Azure 受信任的启动现在也可用于快照。如果您选择启用了受信任启动的快照，则必须使用计算机配置文件。此外，必须选择启用了受信任启动的计算机配置文件。有关详细信息，请参阅 [Microsoft Azure Resource Manager 云环境](#)。

导出计算机。现在，您可以将计算机 目录设置向导的计算机 \*\* 页面上列出的计算机导出为 CSV 文件，以便在将计算机批量添加到目录时用作模板。有关详细信息，请参阅 [从目录导出计算机](#)。

用于访问 **Workspace Environment Management Web** 控制台的选项。现在，“管理”选项卡的菜单中提供了“环境 管理 (Web)”选项。该选项将带您进入新的基于 Web 的 Workspace Environment Management 控制台。要访问旧版控制台，请使用 **Environment Management**。我们正在将全套功能从旧版控制台迁移到 Web 控制台。Web 控制台的响应速度通常比传统控制台快。有关详细信息，请参阅 [Workspace Environment Management 服务](#)。

能够管理 **ProvScheme** 参数。使用 MCS 创建目录时，如果在计算机目录创建期间在不受支持的虚拟机管理程序中设置 **New-ProvScheme** 参数，或者在创建计算机目录后更新 **Set-ProvScheme** 参数，则会出现错误。有关详细信息，请参阅[创建计算机目录](#)。

增加了资源位置限制。现在，单会话 VDA 和多会话 VDA 的资源位置限制分别提高到 10000 和 1000。有关详细信息，请参阅 [限制](#)。

支持在耗尽所有会话后重新启动非电源管理的计算机。Citrix DaaS 现在允许您在所有会话从计算机中耗尽后为未进行电源管理的计算机创建重新启动计划。在“完全配置”界面中，选择“耗尽所有会话后重新启动所有计算机”作为重新启动持续时间。有关详细信息，请参阅[创建重新启动计划](#)。

支持升级 **VDA** 计算机（预览版）。使用完整配置界面，您现在可以为 Citrix DaaS 部署升级 VDA 计算机。您可以按目录或每台计算机升级它们。该功能适用于不是使用 MCS 创建的计算机（例如，物理机）。有关详细信息，请参阅 [使用完整配置界面升级 VDA](#)。

停机期间计算机不会关闭。Citrix DaaS 现在可防止虚拟机在计算机所在的区域中断时被 Broker 关闭。中断结束后，计算机将自动可用于连接。中断后，您无需执行任何操作即可使计算机可用。

会话启动诊断。Citrix DaaS 现在支持增强的会话启动失败诊断。使用来自 Citrix Monitor（即 Citrix Director 服务）的 Citrix Workspace 应用程序生成的 32 位 (8-4-4-4-12) 事务 ID 缩小到出现问题的确切组件和阶段，然后应用建议的操作来解决问题。有关详细信息，请参阅[会话启动诊断](#)。

访问会话录制服务的选项。现在，“管理”选项卡的菜单中提供了“会话录制”选项。Session Recording 服务的引入提供了对策略、播放和服务器配置的集中管理。它提供了一个统一的入口点来管理和观察整个组织中的分布式对象，从而减轻了 IT 管理员的负担。有关详细信息，请参阅 [Session Recording 服务（预览版）](#)。

更名为 **Citrix Virtual Apps and Desktops** 服务。**Citrix Virtual Apps and Desktops** 服务已重命名为 **Citrix DaaS**。有关名称变更的详细信息，请参阅[我们博客上的公告](#)。

Citrix Virtual Apps and Desktops 服务的以下产品已重命名。

- **Citrix Virtual Apps** 服务 **Advanced** 已重命名为 **Citrix DaaS Advanced**。
- **Citrix Virtual Apps** 服务 **Premium** 已重命名为 **Citrix DaaS Premium**。
- **Citrix Virtual Desktops** 服务已重命名为 **Citrix DaaS Advanced Plus**。

- **Citrix Virtual Apps and Desktops 服务 Advanced** 已重命名为 **Citrix DaaS Advanced Plus**。
- **Citrix Virtual Apps and Desktops 服务 Premium** 现已作为 **Citrix DaaS Premium** 和 **Citrix DaaS Premium Plus** 提供。
- 适用于 **Azure** 的 **Citrix Virtual Apps and Desktops Standard** 已重命名为 **Citrix DaaS Standard for Azure**。
- 适用于 **Google Cloud** 的 **Citrix Virtual Apps and Desktops Standard** 已重命名为适用于 **Google Cloud** 的 **Citrix DaaS Standard**。
- 适用于 **Google Cloud** 的 **Citrix Virtual Apps and Desktops Premium** 已重命名为适用于 **Google Cloud** 的 **Citrix DaaS Premium**。

在我们的产品及其文档中实现此转换是一个正在进行的过程。感谢您在此转换期间耐心等待。

- 产品 UI、产品中内容以及产品文档中的图像和说明将在未来几周内更新。
- 某些项目（例如命令和 MSI）可能会继续保留以前的名称，以防止损坏客户的现有脚本。
- 相关产品文档以及从此产品文档链接的其他资源（例如视频和博客文章）可能仍包含以前的名称。

**注意：**

本地 **Citrix Virtual Apps and Desktops** 产品名称保持不变。

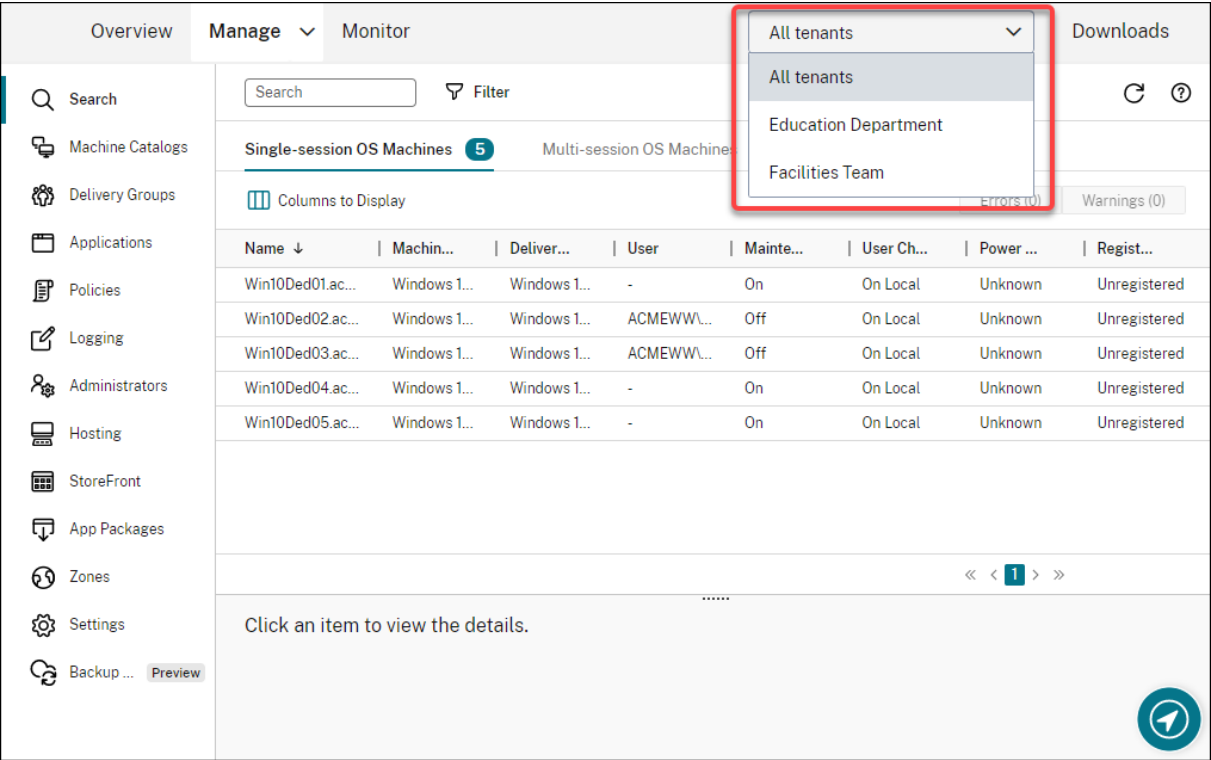
完整配置中的租户支持。现在，您可以在单个 Citrix DaaS 实例中创建配置分区。可以通过在管理员 > 作用域中创建租户作用域并将相关配置对象（例如计算机目录和交付组）与这些租户关联来实现这一目标。因此，具有租户访问权限的管理员只能管理与租户关联的对象。例如，如果您的组织执行以下操作，则此功能非常有用：

- 有不同的业务孤岛（独立的部门或独立的 IT 管理团队）或
- 具有多个本地站点，并希望在单个 Citrix DaaS 实例中保持相同的设置。

此外，“完整配置”界面还允许您按名称筛选租户客户。默认情况下，界面显示有关所有租户的信息。

此功能同时适用于 Citrix Service Provider (CSP) 和非 CSP。CSP 环境中的接口基本上与非 CSP 环境中的接口相同，只是用于创建租户的方法除外。

- CSP 将租户客户加入 Citrix DaaS，然后配置管理员对 Citrix DaaS 的访问权限。有关详细信息，请参阅[适用于 Citrix Service Provider 的 Citrix DaaS](#)。
- 非 CSP 通过首先创建作用域，然后为各自的管理员配置自定义访问权限来创建租户客户。有关详细信息，请参阅[创建和管理作用域](#)。



**AutoScale** 的更新。我们使用刀片样式更新了 **AutoScale**，为您带来更好的用户体验。配置设置的工作流程保持不变。  
**AutoScale** 的其他更新包括：

- 将限制 **AutoScale** 重命名为自动缩放已标记的计算机，使其易于理解。
- 添加了一个新选项控制 **AutoScale** 何时开始打开已标记的计算机的电源。该选项允许您根据未标记计算机的使用情况控制 **AutoScale** 何时开始打开带标记的计算机的电源。

有关自动缩放带标记的计算机的详细信息，请参阅 [AutoScale 标记的计算机](#)。

许可证有效性检查。现在，“完全配置”界面会自动检查主机连接正在使用的许可证的有效性。如果主机连接的许可证无效，则会将其置于维护模式。因此，您无法执行某些操作，例如编辑连接和关闭维护模式。例如，在以下情况下，许可证将失效：

- 许可证已过期。在这种情况下，请联系您的 Citrix 销售代表续订或购买新许可证。
- 许可证已从许可证服务器中删除。

应用到“计算机目录”和“策略”节点的刀片样式。刀片样式现在应用到“完整配置”的所有节点。

支持在 **Azure** 环境中更新 **MCS** 预配的计算机。**Set-ProvScheme** 更改了模板（预配方案），不会影响现有计算机。现在，您可以使用 **Request-ProvVMUpdate** 命令将当前的预配方案应用到现有计算机（或一组计算机）。目前，此功能支持的属性更新为 **ServiceOffering**。有关详细信息，请参阅[将预配的计算机更新为当前预配方案状态](#)。



## 2022 年 3 月

### 新增功能和增强功能

**Google Cloud Marketplace** 上提供了适用于 **Google Cloud** 的 **Citrix Virtual Apps and Desktops**。适用于 Google Cloud 的 Citrix Virtual Apps and Desktops Premium 现在可以在 Google Cloud Marketplace 上购买。适用于 Google Cloud 的 Citrix Virtual Apps and Desktops Premium 在 Google Cloud 上运行 Citrix Virtual Apps and Desktops 服务控制平面。

**Azure** 受信任启动支持。Azure 受信任启动现在可用于完整配置管理界面。如果您选择启用了受信任启动的映像，则必须使用计算机配置文件。此外，必须选择启用了受信任启动的计算机配置文件。有关详细信息，请参阅 [Microsoft Azure Resource Manager 云环境](#)。

在“完整配置”中，刀片样式应用到另外三个节点中的向导。这些节点为 **Search**（搜索）、**Delivery Groups**（交付组）和 **Applications**（应用程序）。

**Image Portability Service (IPS)** 已正式发布。IPS 简化了跨平台映像的管理。此功能对于管理本地资源位置与公有云之间的映像非常有用。Citrix Virtual Apps and Desktops REST API 可用于自动管理 Citrix Virtual Apps and Desktops 站点中的资源。有关详细信息，请参阅[将工作负载迁移到公有云](#)。

## 2022 年 2 月

### 新增功能和增强功能

**Azure** 权限。满足安全要求以及将风险降至最低需要两组权限。

- 最低权限：这组权限提供了更好的安全控制。但是，需要额外权限的新功能将因使用最低权限而失败。
- 常规权限：这组权限不会阻止您获得新的增强权益。

有关详细信息，请参阅[关于 Azure 权限](#)。

支持使用 **VM** 的临时磁盘在 **Azure** 环境中托管回写缓存磁盘。我们在 **Manage**（管理）> **Full Configuration**（完整配置）界面的 **Machine Catalog Setup**（计算机目录设置）> **Disk Settings**（磁盘设置）页面中添加了一个选项 **Use non-persistent write-back cache disk**（使用非永久回写式缓存磁盘）。如果您不希望回写式缓存磁盘为已预配的 VM 保留，请选择该选项。选择该选项后，如果临时磁盘有足够的空间，我们将使用虚拟机的临时磁盘来托管回写缓存磁盘。这样做可以降低您的成本。有关详细信息，请参阅 [Microsoft Azure Resource Manager 云环境](#)。

**AWS** 主机连接默认设置的更新。AWS 主机连接默认设置值会更新为更高的值，并且很可能与所有 AWS 云平台设置相同。这有助于在 AWS 云环境中创建主机连接，而无需根据个人设置评估和配置默认设置值。有关详细信息，请参阅[主机连接默认值](#)。

添加了在 **GCP** 环境中对不同存储层的支持。现在，您可以在 GCP 环境中提供以下自定义属性，以设置连接到新创建的 VM 的磁盘的存储类型：

- StorageType

- IdentityDiskStorageType
- WBCDiskStorageType

有关详细信息，请参阅 [Citrix Virtual Apps and Desktops 服务 SDK](#)。

创建 **Azure** 虚拟机目录后更改某些虚拟机设置。现在，使用“完整配置”管理界面，您可以在创建目录后更改以下设置：

- 计算机规模
- 可用性区域
- 计算机配置文件
- Windows 许可证

为此，请在计算机目录节点上选择目录，然后在操作栏中选择编辑计算机目录。有关详细信息，请参阅[编辑目录](#)。

支持将 **Azure** 临时操作系统磁盘存储在缓存磁盘或临时磁盘上。Citrix Virtual Apps and Desktops 服务现在允许您将 Azure 临时操作系统磁盘存储在启用了 Azure 的虚拟机的缓存磁盘或临时磁盘上。此功能对于需要的 SSD 磁盘的性能高于标准 HDD 磁盘的 Azure 环境非常有用。有关详细信息，请参阅 [Microsoft Azure Resource Manager 云环境](#)。

支持 **AWS** 上的 **Nutanix Clusters**。Citrix Virtual Apps and Desktops 服务支持 AWS 上的 Nutanix Clusters。Nutanix Clusters 简化了应用程序在私有云或多个公有云上的运行方式。有关详细信息，请参阅 [AWS 上的 Nutanix Clusters](#)。

支持 **Amazon Web Services (AWS)** 上的 **VMware** 云。借助 Amazon Web Services (AWS) 上的 VMware 云，您可以将基于 VMware 的本地 Citrix 工作负载迁移到 AWS 云，将核心 Citrix Virtual Apps and Desktops 环境迁移到 Citrix Virtual Apps and Desktops 服务。有关详细信息，请参阅 [Amazon Web Services \(AWS\) 上的 VMware 云](#)。

支持为在 **Google Cloud Platform (GCP)** 上运行的计算机配置回写式缓存磁盘。在“完整配置”管理界面中，在 GCP 上预配计算机时，您现在可以配置以下回写式缓存磁盘设置：

- 磁盘大小
- 分配给缓存的内存
- 磁盘存储类型
- 磁盘持久性

有关详细信息，请参阅 [Google Cloud Platform 虚拟化环境](#)一文中的[创建计算机目录](#)。

## 2022 年 1 月

### 新增功能和增强功能

支持 **AWS** 上的 **Nutanix Clusters**。Citrix Virtual Apps and Desktops 服务现在支持 AWS 上的 Nutanix Clusters。此支持提供的功能与 Nutanix 本地群集相同。仅支持单个群集 *Prism Element*。有关详细信息，请参阅 [Nutanix 虚拟化环境](#)。

**Cloud Health Check** 中可用的新功能。Cloud Health Check 已更新为新版本，其功能包括：

- 自动修复。Cloud Health Check 现在支持自动检测和修复在运行该软件的计算机上发现的某些问题。现在有了结果报告，向您显示采取了哪些具体措施。有关详细信息，请参阅[自动修复](#)。
- 命令行支持。现在可以从命令行运行 Cloud Health Check。有关详细信息，请参阅[在命令行中运行 Cloud Health Check](#)。
- **Citrix Universal Injection Driver** 状态。Cloud Health Check 现在显示 Citrix UVI 驱动程序的状态，并具有 Citrix UVI 驱动程序的相关事件日志检查。
- 会话启动注册表检查。Cloud Health Check 现在会检查会话启动注册表设置。
- 更新检查报告。对于具有多个检查点的选中项目，最终检查报告现在会列出所有经过验证的检查，以显示在运行状况检查期间执行了哪些操作。

有关详细信息，请参阅 [Cloud Health Check](#)。

使用“完整配置”对 **VDA** 注册和会话启动问题进行故障排除。使用“完整配置”管理界面，您现在可以运行判定 VDA 的运行状况的检查。VDA 运行状况检查确定常见 VDA 注册和会话启动问题的可能的原因。您可以单独运行运行状况检查，也可以分批运行。有关详细信息，请参阅 [VDA 运行状况检查](#)。

能够为现有连接指定 **Azure** 机密过期日期。使用“完整配置”管理界面，您现在可以指定应用程序机密过期的日期。有关如何查看机密过期日期的指导，请参阅 [Microsoft Azure Resource Manager 云环境](#)。使用此功能时，请注意以下区别：

- 对于在 Azure 中手动创建的服务主体，可以在编辑连接 > 连接属性页面上直接编辑到期日期。
- 对于代表您首次编辑通过“完整配置”创建的服务主体的过期日期，请转到编辑连接 > 编辑设置 > 使用现有。可以在编辑连接 > 连接属性页面上进行后续编辑。

用于添加管理员的按钮。我们在 **Full Configuration** (完整配置) > **Administrators** (管理员) > **Administrators** (管理员) 选项卡中添加了 **Add Administrator** (添加管理员) 按钮。通过该按钮可以快速转到 **Identity and Access Management** (身份识别和访问管理) > **Administrators** (管理员)，您可以在其中添加(邀请)管理员。有关详细信息，请参阅[添加管理员](#)。

“完整配置”中向导的全新外观。为了给您带来更好的用户体验，我们更新了以下节点中的向导，添加了新样式(包括颜色、字体和其他格式更改)：**Administrators** (管理员)、**Hosting** (托管)、**StoreFront**、**App Packages** (应用程序软件包)、**Zones** (区域) 和 **Settings** (设置)。新向导出现在刀片视图中，视区更宽，可以显示更多内容。配置设置的工作流程保持不变。

支持在 **Google Cloud Platform (GCP)** 上运行的计算机启用 **MCS I/O** 时保留系统磁盘。在“完整配置”管理界面中，在 GCP 上预配计算机时，您现在可以在启用 MCS 存储优化 (MCS I/O) 后，在电源重新启动期间保留系统磁盘。有关详细信息，请参阅[启用 MCS 存储优化更新](#)。

支持从 **Amazon Web Services (AWS)** 上的 **EBS** 直接上载或下载。AWS 现在提供了 API，允许直接创建包含所需内容的 EBS 卷。现在，您可以使用该 API 来消除创建目录和添加 VM 时对卷工作线程的要求。有关此功能所需的 AWS 权限的信息，请参阅 [Amazon Web Services 云环境](#)。

能够识别 **MCS** 创建的 **Amazon Web Services (AWS)** 资源。我们添加了一个名为 `CitrixProvisioningSchemeID` 的新标记来标识 MCS 创建的 AWS 资源。有关详细信息，请参阅[识别 MCS 创建的资源](#)。

能够配置对“管理”和“监视”的访问权限。现在，“完整配置”管理界面为您提供了其他选项，用于控制是否向自定义角色授予对管理和监视的访问权限。有关详细信息，请参阅[创建和管理角色](#)。

## 2021 年 12 月

### 新增功能和增强功能

支持 **Google Cloud VMware Engine**。该平台现在允许您将基于 VMware 的本地 Citrix 工作负载迁移到 Google Cloud，将核心 Citrix Virtual Apps and Desktops 环境迁移到 Citrix Virtual Apps and Desktops 服务。有关详细信息，请参阅[Google Cloud Platform \(GCP\) VMware Engine 支持](#)。

能够在指定命名方案时指定帐户名称的开头。此版本在“完整配置”管理界面的 **Machine Catalog Setup**（计算机目录设置）> **Machine Identities**（计算机标识）页面中引入了一个选项。此选项允许您指定帐户名称开头的数字或字母，从而可以更好地控制目录创建期间计算机帐户的命名方式。有关详细信息，请参阅[计算机标识](#)。

支持创建 **Nutanix AHV XI** 和 **Nutanix AHV Prism Central (PC)** 连接。在“完整配置”管理界面中，您现在可以创建 Nutanix AHV XI 和 Nutanix AHV PC 连接。有关详细信息，请参阅[Nutanix 虚拟化环境](#)。

支持在 **GCP** 上预配 **VM** 时选择操作系统磁盘的存储类型。在“完整配置”管理界面中，在 GCP 上置备 VM 时，您现在可以选择操作系统磁盘的存储类型。计算机目录设置 > 存储页面上的可用存储选项包括标准永久性磁盘、平衡的永久性磁盘和 **SSD** 永久性磁盘。有关详细信息，请参阅[创建计算机目录](#)。

“完整配置”管理界面现在支持 **Azure** 临时磁盘。以前，PowerShell 是创建使用临时操作系统磁盘的计算机的唯一选择。现在，我们将选项 **Azure** 临时操作系统磁盘添加到计算机目录设置 > 存储和许可证类型页面中。如果要使用 VM 的本地磁盘托管操作系统磁盘，请选择该选项。有关详细信息，请参阅[使用 Azure Resource Manager 映像创建计算机目录](#)。

保护 **Machine Creation Services (MCS)** 托管的资源不被意外删除。现在，您可以通过应用为 VM 启用的 GCP `deletionProtection` 标志来保护 Google 云端平台 (GCP) 上的 MCS 托管资源。使用 `compute.instances.setDeletionProtection` 权限或 IAM 计算管理员角色，您可以重置该标志以允许删除资源。此功能同时适用于持久性和非持久性目录。有关详细信息，请参阅[防止意外删除计算机](#)。

## 2021 年 11 月

### 新增功能和增强功能

更新计算机时对映像进行注释。在“完整配置”管理界面中，您现在可以通过在更新 MCS 创建的目录时添加注释来为映像添加注释。每次更新目录时，无论是否添加注释，都会创建一个与注释相关的条目。如果您在未添加注释的情况下更新目录，该条目将显示为空 (-)。要查看映像的注释历史记录，请选择目录，在下方窗格中单击模板属性，然后单击查看附注历史记录。有关详细信息，请参阅[更新目录](#)。

多类型许可支持。“完整配置”管理界面现在支持多类型许可，允许您指定希望站点使用的许可证权利（您的 Citrix Virtual Apps and Desktops 服务产品的部署）或交付组。

- 在站点级别，当用户在其设备上启动应用程序或桌面时，您可以决定在整个站点范围内使用的许可证。选定的许可证适用于所有交付组，但配置了不同许可证的交付组除外。
- 在交付组级别，您可以确定希望交付组使用哪个许可证，享受多类型许可的灵活性和优势。

有关详细信息，请参阅[多类型许可](#)。

支持显示 **Azure** 应用商店购买计划信息。在“完整配置”管理界面中，创建计算机目录时，现在可以查看源自 Azure 应用商店映像的主映像的购买计划信息。

## 2021 年 10 月

### 新增功能和增强功能

能够更新持久性 **MCS** 目录。我们在“完整配置”管理界面中为持久性 MCS 目录引入了更新计算机选项。该选项允许您管理目录使用的映像或模板。更新持久性目录时，请注意以下事项：只有以后添加到目录中的计算机才会使用新映像或模板创建。我们不会将更新发布到目录中的现有计算机。有关详细信息，请参阅[更新目录](#)。

用于在 **Azure** 专用主机上预配 **VM** 的选项。我们已将选项使用主机组添加到“完整配置”管理界面的计算机目录设置 > 主映像页面中。该选项允许您指定在 Azure 环境中预配 VM 时要使用的主机组。有关详细信息，请参阅[使用 Azure Resource Manager 映像创建计算机目录](#)。

通过在重启电源时保留预配的虚拟机来提高性能。我们在“完整配置”管理界面的计算机目录设置 > 磁盘设置页面中添加了一项设置，即跨电源周期保留 **VM**。该设置允许您在 Azure 环境中重启电源时保留预配的 VM。有关详细信息，请参阅[MCS 存储优化](#)。或者，可以使用 PowerShell 配置该功能。有关详细信息，请参阅[重新启动电源时保留已置备的虚拟机](#)。

将计算机目录绑定到 **Workspace Environment Management** 配置集。创建计算机目录时，现在可以将其绑定到 Workspace Environment Management 配置集。这样，您就可以使用 Workspace Environment Management 服务为用户提供可能的最佳工作区体验。还可以选择在创建目录后绑定目录。有关详细信息，请参阅[创建计算机目录和管理计算机目录](#)。

## 2021 年 9 月

### 新增功能和增强功能

为映像更新添加信息性描述。现在，您可以添加与计算机目录的映像更新有关的更改的信息性描述。此功能对于希望在更新目录使用的映像（例如安装的 Office 365）时添加描述性标记的管理员非常有用。使用 PowerShell 命令，您可以创建和查看这些消息。有关详细信息，请参阅[向映像中添加描述](#)。

**Azure VMware 解决方案 (AVS)** 集成。Citrix Virtual Apps and Desktops 服务支持 AVS，即 Azure VMware 解决方案。AVS 提供包含 Azure 创建的 vSphere 群集的云基础结构。利用 Citrix Virtual Apps and Desktops 服务使

用 AVS 预配 VDA 工作负载的方式与在本地环境中使用 vSphere 的方式相同。有关详细信息，请参阅 [Azure VMware 解决方案集成](#)。

多个目录的同一资源组。现在，您可以使用同一资源组在 Citrix Virtual Apps and Desktops 服务中更新和创建目录。此过程：

- 适用于包含一个或多个计算机目录的任何资源组。
- 支持不是由 Machine Creation Services 创建的资源组。
- 创建 VM 和关联的资源。
- 删除 VM 或目录时删除资源组中的资源。

有关详细信息，请参阅 [Azure 资源组](#)。

检索 **Azure VM**、快照、操作系统磁盘和库映像定义的信息。可以显示 Azure VM、操作系统磁盘、快照和库映像定义的信息。分配计算机目录时，将为主映像上的资源显示此信息。使用此功能可以查看和选择 Linux 或 Windows 映像。有关详细信息，请参阅 [检索 Azure VM、快照、操作系统磁盘和库映像定义的信息](#)。

自动配置的新更新。自动配置已更新为新版本，其功能包括：

- Machine Creation Services (MCS) 支持 - 自动配置现在支持 MCS 目录。有关详细信息，请参阅 [了解迁移 Machine Creation Services 预配的目录](#)。

自动配置的其他更新包括：

- 通过在导出期间使用本地区域的名称预填充 ZoneMapping.yml 文件以及在备份时使用云资源位置来增强区域支持。
- StoreFront 已成为顶层可管理组件。在此之前，StoreFront 是作为交付组的一部分进行管理的。这种分离更好地促进了站点合并。
- 已将 **AddMachinesOnly** 更改为 **MergeMachines** 以匹配当前和新合并选项的模式。
- 添加了在使用支持 cmdlet 时创建和更新 CustomerInfo.yml 时使用 SecurityClient.csv 文件导入 ClientId 和密钥的功能。
- 添加了用户区域首选项迁移。
- 修复了对 Japanese Control Plane 的支持。
- 其他修复和改进功能。

从 [Citrix 下载](#) 下载自动配置。有关自动配置的详细信息，请参阅 [将配置迁移到 Citrix Cloud](#)。

重新启动计划随附更多计划选项。“完整配置”管理界面现在可为您提供额外选项来控制何时执行计划的重新启动。除了每日重复的重新启动计划之外，您还可以设置每周和每月重复模式。有关详细信息，请参阅 [创建重新启动计划](#)。

保留会降低性能的自定义列。以前，在“完整配置”管理界面的搜索节点上，刷新浏览器窗口或注销控制台然后再登录之后，降低性能的自定义列消失了。现在，您可以控制是否保留这些自定义列。有关详细信息，请参阅在“完整配置”管理界面中使用搜索。

使用自动配置工具进行备份和还原。我们向“完整配置”管理界面添加了一个备份和还原节点。该节点汇总了与自动配置工具相关的所有资源，包括以下相关信息：



- 使用单个命令计划 Citrix Virtual Apps and Desktops 配置的自动备份
- 根据需要从以前的备份中还原
- 精细地执行备份和还原
- 支持其他用例

有关详细信息，请参阅[自动配置](#)文档。

支持未加入域的目录。我们已将标识类型未加入域添加到“完整配置”管理界面的计算机目录设置 > 计算机标识页面中。使用该标识类型，您可以使用 MCS 创建未加入任何域的计算机。有关详细信息，请参阅[创建计算机目录](#)。

支持使用计算机配置文件。我们已将选项使用计算机配置文件添加到“完整配置”管理界面的计算机目录设置 > 主映像页面中。通过该选项，您可以指定在 Azure 环境中创建 VM 时希望 VM 从哪个计算机配置文件继承配置。然后，目录中的 VM 可以从选定的计算机配置文件继承配置。配置示例包括：

- 加速的网络连接
- 启动诊断
- 主机磁盘缓存（与操作系统和 MCSIO 磁盘有关）
- 计算机大小（除非另有说明）
- 置于 VM 上的标记

有关详细信息，请参阅[使用 Azure Resource Manager 映像创建计算机目录](#)。

支持 **Windows Server 2022**。至少需要 VDA 2106。

## 2021 年 8 月

### 新增功能和增强功能

将可排序的项目数量从 **500** 个扩大到 **5000** 个。在“完整配置”管理界面的“搜索”节点上，您现在可以按任何列标题对多达 5000 个项目进行排序。当项目数量超过 5000 时，使用筛选条件将项目数量减少到 5000 个或更少，以便启用排序。有关详细信息，请参阅在[“完整配置”管理界面中使用搜索](#)。

支持其他 **Azure** 存储类型。现在，您可以使用 MCS 为 Azure 环境中的虚拟机选择不同的存储类型。有关详细信息，请参阅[存储类型](#)。

支持选择回写式缓存磁盘的存储类型。在“完整配置”管理界面中，创建 MCS 目录时，您现在可以选择回写式缓存磁盘的存储类型。可用的存储类型包括：高级 SSD、标准 SSD 和标准 HDD。有关详细信息，请参阅[创建计算机目录](#)。

关闭挂起的计算机。在管理 > 完整配置界面中，我们向单会话操作系统交付组的“管理 AutoScale”用户界面的基于负载的设置页面中添加了选项如果在 **(分钟)** 内没有重新连接。选择暂停后，该选项将变得可用，允许您指定何时关闭挂起的计算机。已挂起的计算机在断开连接的用户重新连接时仍可用，但不适用于新用户。关闭计算机使其再次可用于处理所有工作负载。有关详细信息，请参阅[AutoScale](#)。

扩展了对使用 **CSV** 文件将计算机批量添加到目录的支持。在管理 > 完整配置界面中，您现在可以使用 CSV 文件将数据中心中已存在的计算机批量添加到对这些计算机进行电源管理的目录中。有关详细信息，请参阅[创建计算机目录](#)和[管理计算机目录](#)。

## 2021 年 7 月

### 新增功能和增强功能

配置日志记录。在管理 > 完整配置中，日志记录用户界面已更改。下面三个选项卡组成了该界面：

- 事件（以前为配置日志记录）。通过此选项卡，您可以跟踪配置更改和管理活动。
- 任务。此选项卡允许您查看与计算机目录操作有关的任务。
- **API**。通过此选项卡，您可以查看在特定时间段内发出的 REST API 请求。

有关详细信息，请参阅[配置日志记录](#)。

**AutoScale** 现在为您提供动态会话超时选项。您可以为高峰和非高峰使用时间配置断开连接和空闲会话超时，以实现更快的计算机终止和节省成本。有关详细信息，请参阅[动态会话录制](#)。

支持 **Google Cloud Platform (GCP)** 客户托管加密密钥 (**CMEK**)。您现在可以将 Google 的 CMEK 与 MCS 目录一起使用。CMEK 可以更好地控制用于加密 Google Cloud 项目中的数据的数据的密钥。有关详细信息，请参阅[客户管理的加密密钥 \(CMEK\)](#)。要配置此功能，请参阅[使用客户托管加密密钥 \(CMEK\)](#)。此功能在管理 > 完整配置界面的计算机目录设置 > 磁盘设置页面上提供。

注意：

此功能可作为预览版使用。

对“管理”选项卡的更新。我们更新了管理选项卡菜单中的选项：

- 完整配置：以前，此选项将您带到旧版控制台。现在系统会将您引导至新的、基于 Web 的控制台 (Web Studio)。基于 Web 的控制台与旧版控制台具有完全奇偶校验，并包括多项增强功能。我们建议您立即开始使用。
- 旧版配置：此选项将引导您进入旧版控制台，该控制台计划于 2021 年 9 月移除。之后，完整配置将是唯一可以访问所有配置和管理操作的界面。

**Web Studio** 现在支持为 **Remote PC Access** 目录选择电源管理连接。以前，您可以使用 Studio 创建与资源位置的局域网唤醒主机连接（选择 **Remote PC** 局域网唤醒作为连接类型）。但是，PowerShell 是将该连接与 Remote PC Access 目录关联的唯一选择。您现在可以使用 Studio 来实现这一目标。有关详细信息，请参阅在[“完整配置”界面中配置局域网唤醒](#)。

## 2021 年 6 月

### 新增功能和增强功能

访问 **Azure** 共享映像库映像。创建计算机目录时，您现在可以从“主映像”屏幕上的 Azure 共享映像库访问映像。有关详细信息，请参阅[访问 Azure 共享映像库中的映像](#)。

在 **Google Cloud Platform (GCP)** 上支持屏蔽虚拟机。可以在 GCP 上预配受防护的虚拟机。一组安全控制措施强化了受防护的虚拟机，这些控制措施使用安全引导、虚拟可信平台模块、UEFI 固件和完整性监视等高级平台安全功能提供计算引擎实例的可验证的完整性。有关详细信息，请参阅[屏蔽 VM](#)。



强制传输 **HTTPS** 或 **HTTP**。使用注册表设置通过 [XML Service](#) 强制传输 **HTTPS** 或 **HTTP** 流量。

始终将标准 **SSD** 用于身份磁盘，以降低 **Azure** 环境中的成本。计算机目录对身份磁盘使用标准 **SSD** 存储类型。**Azure** 标准 **SSD** 是经济高效的存储方案，该方案已针对在较低的 IOPS 级别需要性能一致的工作负载而优化。有关存储类型的详细信息，请参阅 [Azure Resource Manager](#) 主映像。

注意：

有关 **Azure** 托管磁盘定价的详细信息，请参阅 [Managed Disks pricing](#)（托管磁盘定价）。

**Web Studio** 中提供的新增功能。以下功能现在仅在基于 **Web** 的控制台中可用：

- **Studio** 现在支持对 **Azure** 进行身份验证以创建服务主体。现在，您可以通过向 **Azure** 进行身份验证来建立与 **Azure** 的主机连接以创建服务主体。此支持消除了 **Studio** 中创建连接之前在 **Azure** 订阅中手动创建服务主体的必要性。有关详细信息，请参阅 [Microsoft Azure Resource Manager 虚拟化环境](#)。
- **Studio** 现在支持克隆现有的计算机目录。此功能使您能够克隆现有计算机目录以用作新计算机目录的模板，这样将无需从头开始创建类似的目录。克隆目录时，无法更改与操作系统和计算机管理关联的设置。克隆的目录从原始目录继承这些设置。有关详细信息，请参阅 [克隆目录](#)。
- 现在，**Studio** 导航窗格中有一个名为“设置”的新节点。设置节点允许您配置应用到整个站点（**Citrix Virtual Apps and Desktops** 服务产品的部署）的设置。可以使用以下设置：
  - 平衡多会话目录的负载。选择满足您需求的负载平衡选项。此设置适用于所有目录。以前，您可以通过单击控制台右上角的齿轮图标来访问此功能。有关详细信息，请参阅 [平衡计算机负载](#)。
- **Studio** 中增强的搜索体验。此版本增强了您的 **Studio** 搜索体验。使用过滤器执行高级搜索时，添加过滤器窗口将在前台显示，使背景视图保持不变。有关详细信息，请参阅在“完整配置”管理界面中使用搜索。
- 能够在 **MCS** 中暂停和恢复 **Google Cloud VM**。现在，您可以像处理任何 **VM** 一样在 **MCS** 中暂停和恢复 **Google Cloud VM**。有关详细信息，请参阅 [管理交付组](#)。要启用此功能，请在 **Google Cloud** 服务帐户中设置 `compute.instances.suspend` 和 `compute.instances.resume` 权限。计算管理员角色随附这些权限。

在 **Citrix Virtual Apps and Desktops** 中，还可以使用 `New-BrokerHostingPowerAction PowerShell` 命令暂停和恢复 **VM**。有关详细信息，请参阅 [New-Brokerhostingpoweraction](#)。

**Google Cloud** 对可以暂停的实例的类型和配置实施了一些限制。有关详细信息，请参阅在 **Google Cloud** 站点上的 [Suspending and resuming an instance](#)（暂停和恢复实例）。

## 2021 年 5 月

### 新增功能和增强功能

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](#)。

所有 **Citrix Virtual Apps and Desktops** 服务版本中的应用程序探测和桌面探测支持。除了现有的 **Premium Edition** 支持之外，**Citrix Virtual Apps Advanced Service** 和 **Citrix Virtual Apps and Desktops Advanced Service** 版本现已提供应用程序探测和桌面探测。

**Web Studio** 中提供的新增功能。以下功能现在仅在基于 Web 的控制台中可用：

- **Studio** 现在支持选择 **Azure** 可用性区域。以前，PowerShell 是您将计算机预配到 Azure 环境中的特定可用性区域的唯一选择。使用 Studio 创建计算机目录时，您现在可以选择要预配计算机的一个或多个可用性区域。如果未指定区域，Machine Creation Services (MCS) 允许 Azure 将计算机放置在区域内。如果指定了多个区域，MCS 会在这些区域之间随机分配计算机。有关详细信息，请参阅[将计算机预配到指定的可用性区域中](#)。

**Azure** 临时磁盘。Citrix Virtual Apps and Desktops 服务支持 Azure 临时磁盘。临时磁盘允许您重新调整缓存磁盘的用途，以便为启用了 Azure 的虚拟机存储操作系统磁盘。此功能对于需要的 SSD 磁盘的性能高于标准 HDD 磁盘的 Azure 环境非常有用。

**注意：**

永久目录不支持临时操作系统磁盘。此外，使用此功能时，请考虑额外的性能磁盘会产生额外的成本。它有利于重复使用缓存磁盘来存储操作系统磁盘，而不用为额外的托管磁盘付费。

临时操作系统磁盘要求您的预配方案使用托管磁盘和共享映像库。有关详细信息，请参阅[Azure 临时磁盘](#)。

提高了 **Azure** 上 **MCS** 托管 **VDA** 的性能。Citrix Virtual Apps and Desktops 服务可提高 Azure 上使用 Machine Creation Services (MCS) 管理的 VDA 的性能。此增强功能会将托管连接的绝对同步操作的默认值更改为 500，托管连接的每分钟最大新操作数更改为 2000。利用此增强功能无需手动配置任务。有关详细信息，请参阅[Azure 限制](#)。

**Cloud Health Check** 中提供的新功能。Cloud Health Check 已更新为新版本，其功能包括：

- 自动发现 **VDA** 计算机。Cloud Health Check 现在可以从 Citrix Virtual Apps and Desktops 服务部署中自动发现和检索 VDA。有关详细信息，请参阅[检索 VDA 计算机](#)。
- 计划运行状况检查。Cloud Health Check 现在允许您设置执行定期运行状况检查的计划。有关详细信息，请参阅[Cloud Health Check 计划程序](#)。
- **Cloud Health Check** 版本信息。现在，您可以检查您使用的是哪个版本的 Cloud Health Check。要查看版本信息，请单击 Cloud Health Check 主窗口右上角的齿轮图标。
- 自动修复。Cloud Health Check 现在支持自动检测和修复在运行该软件的计算机上发现的某些问题。有关详细信息，请参阅[自动修复](#)。

**注意：**

自动修复可作为预览版提供。

## 2021 年 4 月

### 新增功能和增强功能

使用 **AWS API** 重新获取动态实例。Citrix Virtual Apps and Desktops 服务现在会查询 AWS 以动态检索实例类型。此功能无需为希望使用超出 Citrix Virtual Apps and Desktops 服务中定义的计算机大小限制的客户创建自定义 `InstanceTypes.xml` 文件。此信息以前由 `InstanceTypes.xml` 文件提供。为了方便对可用 AWS 实例类型的动态访问，用户必须更新其服务主体的权限以包含 `ec2:DescribeInstanceTypes` 权限。为了支持选择不更新其服务主体权限的客户的向后兼容性，请使用 `InstanceTypes.xml` 中列出的 AWS 实例类型。此过程会在 MCS CDF 日志中生成警告消息。

注意：

Citrix Studio 不显示 CDF 日志中包含的警告消息。

有关权限的详细信息，请参阅[定义 IAM 权限](#)和[关于 AWS 权限](#)。

**Web Studio** 中提供的新增功能。以下功能现在仅在基于 Web 的控制台中可用：

- **Studio** 现在会显示您所在时区的日期和时间。以前，Studio 仅根据系统时钟和时区显示日期和时间。当您将鼠标指针悬停在事件项上时，Studio 现在支持显示当地时区的日期和时间。时间用 UTC 表示。

对没有临时存储的 **Azure VM** 提供 **MCS I/O** 支持。MCS I/O 现在支持为没有临时磁盘或未附加存储的 VM 创建计算机目录。有了这种支持：

- 在没有临时存储的情况下，从源 VM 中检索快照（托管磁盘）。计算机目录中的 VM 没有临时存储。
- 快照（托管磁盘）是从具有临时存储的源 VM 中检索的。计算机目录中的 VM 具有临时存储。

有关详细信息，请参阅[Machine Creation Services \(MCS\) 存储优化](#)

**Web Studio** 中提供的新增功能。以下功能现在仅在基于 Web 的控制台中可用：

- 强制注销。AutoScale 现在允许您在达到既定的宽限期时强制注销计算机上的现有会话，从而使计算机符合关闭条件。这样做使 AutoScale 能够更快地关闭计算机，从而降低成本。您可以在用户注销之前向用户发送通知。有关详细信息，请参阅[AutoScale](#)。

自动配置的新更新。自动配置已更新为新版本，其功能包括：

- 合并多个站点 - 可以将多个站点合并到一个站点中，同时使用前缀和后缀避免名称冲突。有关详细信息，请参阅[将多个站点合并到一个站点中](#)。
- 站点激活 - 可以选择本地部署还是云部署控制资源，例如重新启动计划和电源方案。有关详细信息，请参阅[激活站点](#)。

自动配置的其他更新包括：

- 迁移管理员角色和作用域的能力。

- **Quiet** 参数，用于选择 cmdlet 来禁止控制台日志记录。
- **SecurityFileFolder** 参数，允许将 CvadAcSecurity.yml 文件放置在需要身份验证的安全网络文件共享中。
- 能够按计算机目录和交付组中的计算机名称进行筛选。
- 改进了组件选择参数以使用 switch 参数方法，无需在组件名称之后添加 **\$true**。
- 一个新 cmdlet (**New-CvadAcZipInfoForSupport**)，用于将要发送给 Citrix 以获得支持的所有日志文件压缩到 zip 文件中。

从 [Citrix 下载](#) 下载自动配置。有关自动配置的详细信息，请参阅[迁移到云](#)。

在整个电源周期内保留 **GCP** 实例。关闭电源时，不再删除非持久性 Google Cloud Platform (GCP) 实例。相反，实例会在整个电源周期内保留。关闭非持久性实例的电源时，操作系统磁盘将被分离并删除。当实例打开电源时，操作系统磁盘将从基础磁盘重新创建，然后附加到现有实例。

支持 **Azure Gen2** 映像。现在，您可以使用 Gen2 快照或 Gen2 托管磁盘配置 Gen2 VM 目录，以提高启动时间性能。有关详细信息，请参阅[创建计算机目录](#)。Azure Gen2 映像支持以下操作系统：

- Windows Server 2019、2016、2012 和 2012 R2
- Windows 10

注意：

不支持使用 Gen1 快照或托管磁盘创建 Gen2 计算机目录。同样，也不支持使用 Gen2 快照或托管磁盘创建 Gen1 计算机目录。有关详细信息，请参阅[支持 Azure 上的第 2 代 VM](#)。

禁用表存储帐户。在 Azure 上预配 VDA 时，Machine Creation Services (MCS) 不再为使用托管磁盘的目录创建表存储帐户。有关详细信息，请参阅[Azure 表存储](#)。

消除存储帐户中的锁定。使用托管磁盘在 Azure 中创建目录时，不再创建存储帐户。为现有目录创建的存储帐户保持不变。此更改仅适用于托管磁盘。对于非托管磁盘，现有行为没有变化。Machine Creation Services (MCS) 将继续创建存储帐户和锁定。

**Web Studio** 中提供的新增功能。以下功能现在仅在基于 Web 的控制台中可用：

- 使用客户管理的加密密钥加密计算机上的数据。Studio 现在将名为客户管理的加密密钥的设置添加到计算机目录设置 > 磁盘设置页面。该设置允许您选择是否加密要在目录中预配的计算机上的数据。有关详细信息，请参阅[客户管理的加密密钥](#)。
- **Studio** 现在支持将 **AutoScale** 限制到带标记的计算机。以前，您必须使用 PowerShell 将 AutoScale 限制到交付组中的某些计算机。您现在也可以使用 Studio。有关详细信息，请参阅[将 AutoScale 限制到交付组中的某些计算机](#)。

## 2021 年 3 月

### 新增功能和增强功能

**Azure 专用主机。** Azure 专用主机允许您在单个客户专用的硬件上预配虚拟机。在使用专用主机时，Azure 可确保您的虚拟机是该主机上唯一运行的计算机。这为客户提供了更多的控制和可见性，从而确保满足其法规或内部安全要求。使用 `HostGroupId` 参数时，需要在托管单元所在区域中预配置的 Azure 主机组。此外，需要 Azure 自动放置功能。有关详细信息，请参阅 [Azure 专用主机](#)。

#### 提示：

使用 Azure 专用主机时，选择 **Azure** 可用性区域不起作用。虚拟机通过 Azure 自动放置过程进行放置。

支持 **Azure** 服务器端加密。Citrix Virtual Apps and Desktops 服务支持 Azure 托管磁盘的客户管理的加密密钥。通过此支持，您可以使用自己的加密密钥对计算机目录的托管磁盘进行加密，从而管理组织和合规性要求。有关详细信息，请参阅 [Azure 服务器端加密](#)。

将计算机预配到 **Azure** 上的指定可用性区域中。您现在可以将计算机预配到 Azure 环境中的特定可用性区域中。借助此功能：

- 可以在 Azure 上指定一个或多个可用性区域。如果提供了多个区域，计算机名义上将平均分布在所有提供的区域中。
- 虚拟机和相应磁盘将放置在指定的区域（或多个区域）中。
- 可以浏览可用性区域以查找给定的服务产品或地区。使用 PowerShell 命令显示有效的可用性区域。使用 `Get-Item` 查看服务产品清单项目。

有关详细信息，请参阅[将计算机预配到 Azure 上指定的可用性区域中](#)。

**Web Studio** 中提供的新增功能。以下功能现在仅在基于 Web 的控制台中可用：

- **Studio** 现在支持将应用程序与自定义图标关联。以前，您必须使用 PowerShell 添加自定义图标以用于已发布的应用程序。现在您也可以使用 Studio 来做到这一点。有关详细信息，请参阅[管理应用程序组](#)。
- **Studio** 现在支持将标记应用到计算机目录。以前，您可以使用 Studio 创建或删除用于目录的标记。但是，必须使用 PowerShell 将标记应用到目录。现在，您还可以像处理交付组一样，使用 Studio 将标记应用到目录或在目录中应用或删除标记。有关详细信息，请参阅[将标记应用到计算机目录](#)。
- **Studio** 现在支持在“水平负载平衡”与“垂直负载平衡”模式之间切换。以前，PowerShell 是您在水平负载平衡与垂直负载平衡模式之间切换的唯一选择。Studio 现在让您可以更灵活地控制如何平衡多会话操作系统计算机的负载。有关详细信息，请参阅[平衡计算机负载](#)。
- **Studio** 现在支持将处于维护模式的计算机纳入重新启动计划。以前，PowerShell 是您为处于维护模式的计算机配置计划重新启动的唯一选择。现在，您还可以使用 Studio 来控制是否将这些计算机包括在重新启动计划中。有关详细信息，请参阅[创建重新启动计划](#)。
- **Studio** 现在支持为 **Remote PC Access** 配置局域网唤醒。以前，您必须使用 PowerShell 为 Remote PC Access 配置局域网唤醒。现在，您还可以使用 Studio 来配置该功能。有关详细信息，请参阅[配置局域网唤醒](#)。

- **Studio** 现在支持应用 **AWS** 实例属性和标记运行资源。创建目录以使用 MCS 在 AWS 中预配计算机时，可以指定是否将 IAM 角色和标记属性应用到这些计算机。还可以指定是否将计算机标记应用到运行资源。您有以下两个选项：

- 将计算机模板属性应用到虚拟机
- 将计算机标记应用到运行资源

有关详细信息，请参阅[应用 AWS 实例属性和标记运行资源](#)。

**Azure** 共享映像库。Citrix Virtual Apps and Desktops 服务支持 Azure 共享映像库作为 Azure 中 MCS 预配的计算机的已发布的映像的存储库。管理员可以选择在库中存储映像，以加快创建和提取操作系统磁盘的速度。此过程缩短了非永久 VM 的启动和应用程序启动时间。有关此功能的详细信息，请参阅[Azure 共享映像库](#)。

注意：

共享映像库功能与托管磁盘兼容。它不适用于旧版计算机目录。

存储桶在与计算机目录相同的 **Google Cloud Platform** 区域中创建。在早期版本中，MCS 在预配过程中创建了临时存储桶，作为磁盘上载过程的一部分。这些存储桶跨越多个区域，其中 **Google** 定义为包含两个或多个地理位置的大型地理区域。无论目录在何处预配，这些临时存储桶的地理位置都位于美国。现在，MCS 将在您预配目录的同一区域创建存储桶。存储桶不再是临时存储桶；在您完成预配过程后，它们仍保留在 Google Cloud Platform 项目中。将来的预配操作将使用现有存储桶（如果该区域中存在存储桶）。如果指定区域中不存在新存储桶，则会创建一个新存储桶。

## 2021 年 2 月

### 新增功能和增强功能

支持 **Azure Gen2** 映像。您现在可以在 Azure 环境中使用 Gen2 VM 预配托管磁盘，以提高启动时间性能。支持以下操作系统：

- Windows Server 2019、2016、2012 和 2012 R2
- Windows 10

注意：

有了这种支持，将仅支持一部分 VM。例如，某些 VM 可以是 Gen1 和 Gen2 类型，而其他 VM 只能是 Gen1。有关详细信息，请参阅[支持 Azure 上的第 2 代 VM](#)。

计算机重新启动计划。Citrix Studio 现在将名为耗尽会话后重新启动所有计算机的选项添加到重新启动持续时间菜单中。该选项允许您选择是否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，并在注销所有会话时重新启动。有关详细信息，请参阅[创建重新启动计划](#)。

**Web Studio** 中提供的新增功能。以下功能现在仅在基于 Web 的控制台中可用：

- **Studio** 现在支持使用 **CSV** 文件将计算机批量添加到目录中。通过此功能，您可以使用 CSV 文件执行以下操作：



- 将计算机批量添加到不通过 Studio 进行电源管理的多会话或单会话操作系统目录中。
- 将计算机批量添加到 Remote PC Access 目录中。以前，您必须选择 OU 才能将计算机批量添加到 Remote PC Access 目录中。但是，在有 OU 结构限制的情况下，这样做并不容易。通过该功能，您可以更加灵活地批量添加计算机。只能添加计算机（用于用户自动分配）或将计算机与用户分配一起添加。

有关详细信息，请参阅[创建计算机目录](#)和[管理计算机目录](#)。

- 对 **Citrix** 托管 **Azure** 的扩展支持。[Citrix 托管 Azure](#) 现已在以下 Citrix Virtual Apps and Desktops 服务版本中提供：Standard for Azure、Advanced、Premium 和 Workspace Premium Plus。
- 支持将主映像放置在 **Azure** 共享映像库中。Studio 现在为您提供了将主映像放置在 Azure 共享映像库 (SIG) 中的选项。SIG 是用于管理和共享映像的存储库。它可以让您在整个组织中使用映像。我们建议您在创建大型非持久性计算机目录时将主映像存储在 SIG 中，因为这样做可以更快地重置 VDA 操作系统磁盘。有关详细信息，请参阅[Microsoft Azure Resource Manager 虚拟化环境](#)。
- 在 **Azure** 中保留 **MCS** 计算机目录的系统磁盘。Studio 现在允许您控制是否在电源重新启动期间为 VDA 保留系统磁盘。通常情况下，系统磁盘在关机时删除，并在启动时重新创建。这样可以确保磁盘始终处于干净状态，但会导致 VM 重新启动时间更长。如果系统写入操作重定向到缓存并回写到缓存磁盘，系统磁盘将保持不变。为避免不必要的磁盘重复创建，请使用计算机目录设置 > 磁盘设置页面上的电源重新启动期间保留系统磁盘选项。启用该选项可缩短 VM 的重新启动时间，但会增加存储成本。在环境包含具有敏感重新启动时间的工作负载的情况下，该选项会非常有用。有关详细信息，请参阅[MCS 存储优化](#)。
- **Studio** 现在支持使用永久回写式缓存磁盘创建 **MCS** 计算机目录。以前，PowerShell 是您创建具有永久性回写式缓存磁盘的目录的唯一选择。现在，您可以使用 Studio 来控制是否在创建目录时为 Azure 中预配的 VM 永久保留回写式缓存磁盘。如果禁用，则会在每次电源重新启动期间删除回写式缓存磁盘以节省存储成本，导致重定向到磁盘的所有数据都丢失。要保留该数据，请启用计算机目录设置 > 磁盘设置页面上的使用永久回写式缓存磁盘选项。有关详细信息，请参阅[MCS 存储优化](#)。

支持使用 **StoreFront** 为 **Citrix Virtual Apps and Desktops** 服务提供 **App Protection**。有关详细信息，请参阅[App Protection](#)。

## 2021 年 1 月

**Web Studio** 中提供的新增功能。以下功能现在仅在基于 Web 的控制台中可用：

- **Studio** 现在支持将应用程序与自定义图标关联。以前，您必须使用 PowerShell 添加自定义图标以用于已发布的应用程序。现在您也可以使用 Studio 来做到这一点。有关详细信息，请参阅[管理应用程序组](#)。
- **Studio** 现在支持将标记应用到计算机目录。以前，您可以使用 Studio 创建或删除用于目录的标记。但是，必须使用 PowerShell 将标记应用到目录。现在，您还可以像处理交付组一样，使用 Studio 将标记应用到目录或在目录中应用或删除标记。有关详细信息，请参阅[将标记应用到计算机目录](#)。
- **Studio** 现在支持在“水平负载平衡”与“垂直负载平衡”模式之间切换。以前，PowerShell 是您在水平负载平衡与垂直负载平衡模式之间切换的唯一选择。Studio 现在让您可以更灵活地控制如何平衡多会话操作系统计算机的负载。有关详细信息，请参阅[平衡计算机负载](#)。



- **Studio** 现在支持将处于维护模式的计算机纳入重新启动计划。以前，PowerShell 是您为处于维护模式的计算机配置计划重新启动的唯一选择。现在，您还可以使用 Studio 来控制是否将这些计算机包括在重新启动计划中。有关详细信息，请参阅[创建重新启动计划](#)。
- **Studio** 现在支持为 **Remote PC Access** 配置局域网唤醒。以前，您必须使用 PowerShell 为 Remote PC Access 配置局域网唤醒。现在，您还可以使用 Studio 来配置该功能。有关详细信息，请参阅[配置局域网唤醒](#)。
- **Studio** 现在支持应用 **AWS** 实例属性和标记运行资源。创建目录以使用 MCS 在 AWS 中预配计算机时，可以指定是否将 IAM 角色和标记属性应用到这些计算机。还可以指定是否将计算机标记应用到运行资源。您有以下两个选项：

- 将计算机模板属性应用到虚拟机
- 将计算机标记应用到运行资源

有关详细信息，请参阅[应用 AWS 实例属性和标记运行资源](#)。

- **AWS 专用主机**。Citrix Studio 现在计算机目录设置 > 安全页面中添加了一个名为使用专用主机的选项。此设置适用于需要您使用专用主机的许可限制或安全要求的部署。使用专用主机，您可以拥有整个物理主机，并按小时计费。拥有该主机可让您在该主机允许的情况下启动尽可能多的 EC2 实例，而无需支付额外的费用。有关详细信息，请参阅[AWS 租赁](#)。
- **Studio** 现在支持立即运行重新启动计划。Studio 现在允许您立即运行重新启动计划以重新启动计划中的所有适用计算机。有关详细信息，请参阅[立即运行重新启动计划](#)。
- **AutoScale**。AutoScale 提供了以下新增功能和增强功能：
  - **Studio** 现在支持显示处于耗尽状态的计算机。以前，PowerShell 是您识别处于耗尽状态的计算机的唯一选项。现在，您可以使用 Studio 来识别处于耗尽状态的计算机。有关详细信息，请参阅[显示处于耗尽状态的计算机](#)。
  - **Studio** 现在支持按 30 分钟的粒度级别为 **VDI** 交付组定义高峰时间。以前，您必须使用 PowerShell 按 30 分钟的粒度级别为 VDI 交付组定义计划中包含的天数的高峰时间。现在您也可以使用 Studio 来做到这一点。此支持允许您单独设置一天中每半小时在 VDI 交付组中运行的计算机的最小数量。

**Azure** 共享映像库。Citrix Virtual Apps and Desktops 服务支持 Azure 共享映像库作为 Azure 中 MCS 预配的计算机的已发布的映像的存储库。管理员可以选择在库中存储映像，以加快从主映像创建和提取操作系统磁盘的速度。此过程缩短了非永久 VM 的启动和应用程序启动时间。

该库包含以下三个元素：

- 库。映像存储在此处。MCS 为每个计算机目录创建一个库。
- 库映像定义。此定义包括有关主映像的信息（操作系统类型和状态、Azure 区域）。MCS 为目录创建的每个主映像创建一个映像定义。
- 库映像版本。共享映像库中的每个映像可以有多个版本，每个版本可以在不同的区域中有多个副本。每个副本都是主映像的完整副本。Citrix Virtual Apps and Desktops 服务始终为每个映像创建一个 Standard\_LRS 映像版本（版本 1.0.0），并在目录区域中创建相应数量的副本。此配置基于目录中的计算机数、配置的副本比率以及配置的副本最大值。

注意：

共享映像库功能仅适用于托管磁盘。它不适用于旧版计算机目录。

有关此功能的详细信息，请参阅[配置共享映像库](#)。

存储桶在与计算机目录相同的 **Google Cloud Platform** 区域中创建。在早期版本中，MCS 在预配过程中创建了临时存储桶，作为磁盘上载过程的一部分。这些存储桶跨越多个区域，其中 **Google** 定义为包含两个或多个地理位置的大型地理区域。无论目录在何处预配，这些临时存储桶的地理位置都位于美国。现在，MCS 将在您预配目录的同一区域创建存储桶。存储桶不再是临时存储桶；在您完成预配过程后，它们仍保留在 Google Cloud Platform 项目中。将来的预配操作将使用现有的存储桶。如果该区域中存在存储桶，或者如果指定区域中不存在新存储桶，则会创建一个新存储桶。

**PowerShell** 选项，该选项默认设置为在中断期间重复使用池 **VDA**。默认情况下，新 PowerShell 命令选项 (**-DefaultReuseMachinesWithoutShutdownInOutage**) 扩展了重复使用中断期间未关闭的池桌面 VDA 的功能。请参阅[应用程序和桌面支持](#)。

**Google Cloud Platform** 按需预配。Citrix Virtual Apps and Desktops 服务更新了 Google Cloud Platform (GCP) 预配计算机目录的方式。创建计算机目录时，不会在 GCP 中创建相应的计算机实例，并且电源状态设置为关。计算机不是在创建目录时预配的，而是在第一次打开计算机电源时预配的。例如，创建目录后，VM 电源状态将设置为关：

Search

▼

Saved searches

Single-session OS Machines (0)

Multi-session OS Machines (1)

Sessions (0)

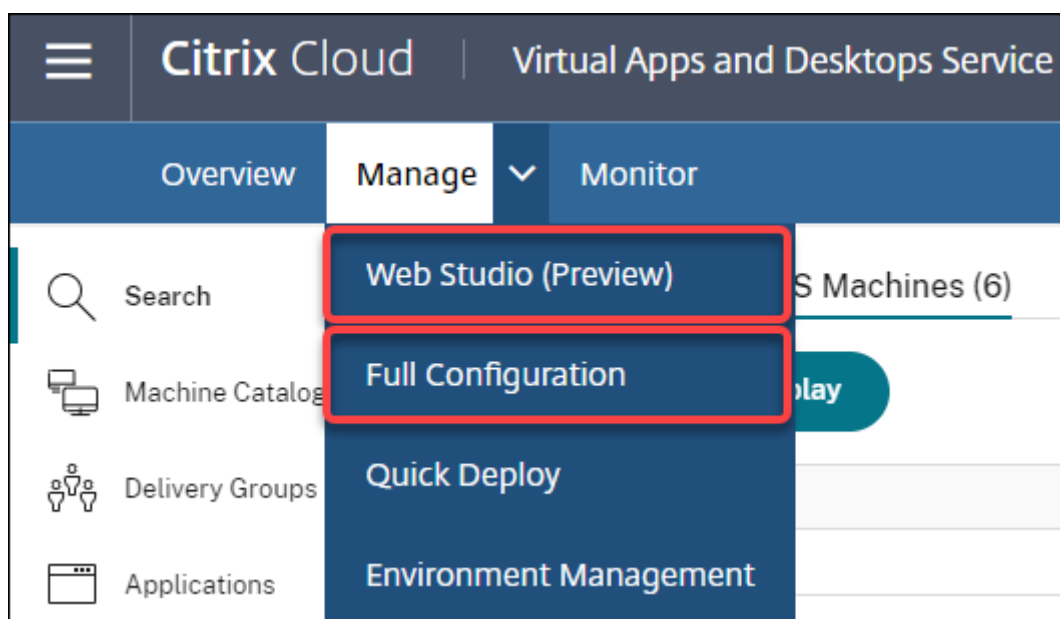
Name	Machine Catalog	Delivery Group	Maintenance Mode	Persist User Changes	Power State	Registration State	Session Count
scale1ma-01.mcs-gcp-local	scale1cat	-	Off	Discard	Off	Unregistered	0

2020 年 12 月

新增功能和增强功能

**Web Studio** 可作为预览版提供。新的基于 Web 的控制台现已推出。我们正在将 Studio 的完整功能集从旧版控制台迁移到全新的、基于 Web 的控制台。基于 Web 的控制台通常比旧版控制台的响应速度更快。默认情况下，您会自动登录到基于 Web 的控制台。可以在管理选项卡中在基于 Web 的控制台与旧版控制台之间轻松切换，以执行配置或站点管理任务。单击管理旁边的向下箭头，然后选择一个选项：

- **Web Studio**（预览版）。带您进入全新的基于 Web 的控制台。
- 完整配置。带您进入旧版控制台。



以下功能仅在基于 Web 的控制台中可用：

- 面向 **Azure** 的标准 **SSD** 磁盘类型支持。Studio 现在增加了对标准 SSD 磁盘类型的支持。Azure 标准 SSD 是经济高效的存储方案，该方案已针对在较低的 IOPS 级别需要性能一致的工作负载而优化。有关详细信息，请参阅[使用 Azure Resource Manager 主映像创建计算机目录](#)。
- **Studio** 现在支持为静态 **VDI** 交付组配置关机延迟。以前，您只能通过 PowerShell SDK 为静态 VDI 交付组配置关机延迟。Studio 现在允许您在 AutoScale 用户界面中为静态 VDI 交付组配置关机延迟。有关详细信息，请参阅[AutoScale](#)。

## 2020 年 10 月

### 新增功能和增强功能

关闭多个虚拟机管理程序警报。Citrix Monitor 现在支持自动消除时间在一天以上的虚拟机管理程序警报。有关详细信息，请参阅[虚拟机管理程序警报监视](#)。

删除外部 IP 地址。不再需要用于在 Google Cloud Platform (GCP) 中准备已预配的映像的临时虚拟机上的外部 IP 地址。此外部 IP 地址使临时虚拟机能够访问 Google 公共 API 以完成预配过程。

启用专用 Google 访问权限才能允许 VM 直接从子网访问 Google 公共 API。有关详细信息，请参阅[启用 Google 专用访问权限](#)。

新模型解决了如何管理计算机标识的问题。计算机目录中使用的计算机标识已使用 Active Directory 进行管理和维护。MCS 创建的所有计算机现在都将加入 Active Directory。新的 Citrix Virtual Apps and Desktops 服务模型解决了如何管理计算机标识的问题。此模型允许使用工作组或未加入域的计算机创建计算机目录。

提示：

此功能支持为未加入域的计算机添加到 Citrix Cloud 的新身份服务 FMA 信任。

MCS 与新的 FMA 信任服务进行通信以完成身份管理。身份信息作为一对 GUID 和私钥对（而非 Active Directory 使用的域 SID 和计算机帐户密码范例）存储在身份磁盘中。使用未加入域的计算机的 VDA 使用此 GUID 和私钥组合进行 Broker 注册。有关详细信息，请参阅[配置对未加入域的目录的支持](#)。

对 **Azure** 托管磁盘使用直接上载。此版本允许您在 Azure 环境中创建托管磁盘时使用直接上载。此功能降低了与额外的存储帐户相关的成本。在将 VHD 转换为托管磁盘之前，您不再需要将其存储到存储帐户中。此外，直接上载消除了将空托管磁盘附加到虚拟机的需要。通过直接上载到 Azure 托管磁盘，您将能够直接复制本地 VHD 以用作托管磁盘，从而简化了工作流程。支持的托管磁盘包括标准 HDD、标准 SSD 和高级 SSD。

有关此功能的详细信息，请参阅 Microsoft Azure [博客](#)。

有关 Azure 托管磁盘的详细信息，请参阅[文档页面](#)。

**Azure** 中的单个资源组。现在，您可以创建和使用单个 Azure 资源组来更新和创建 Citrix Virtual Apps and Desktops 中的目录。此增强功能同时适用于完整作用域和窄作用域服务主体。

删除了以前每个 Azure 资源组每 800 个托管磁盘包含 240 个 VM 的限制。对每个 Azure 资源组的虚拟机、托管磁盘、快照和映像数量不再有限制。

有关详细信息，请参阅 [Microsoft Azure Resource Manager 虚拟化环境](#)。

## 2020 年 9 月

### 新增功能和增强功能

快速部署。新的[快速部署](#)功能取代了早期的 Azure 快速部署。新增功能提供了一种通过 Microsoft Azure 快速入门使用 Citrix Virtual Apps and Desktops 服务的方法。可以使用快速部署来交付桌面和应用程序以及配置 Remote PC Access。

会话管理员（内置角色）。Citrix Studio 现在添加了一个名为会话管理员的新内置角色。该角色允许管理员在 **Monitor** 选项卡的过滤器页面上查看交付组并管理其关联的会话和计算机。使用此功能，您可以通过与其在组织中的角色相一致的方式配置现有管理员或您邀请的管理员的访问权限。有关内置角色的详细信息，请参阅[内置角色和作用域](#)。有关如何将内置角色分配给管理员的信息，请参阅[委派管理和监视](#)。

要更加精细地控制对与会话和计算机相关的过滤器页面的访问，请创建一个自定义角色并为 Director 对象选择以下选项之一：查看过滤器页面 - 仅限计算机，查看过滤器页面 - 仅限会话。有关创建自定义角色的信息，请参阅[创建和管理角色](#)。

支持新的计算机类型。在为计算机目录配置高级磁盘时，此版本增加了对 NV v4 和 DA v4 系列 AMD 计算机的支持。有关详细信息，请参阅[创建交付组](#)。

## 2020 年 8 月

### 新增功能和增强功能

中断期间对 **Remote PowerShell SDK** 的有限访问。以前，您可能无法在中断期间使用 PowerShell 命令。现在，本地主机缓存允许在中断期间对 Remote PowerShell SDK 进行有限访问。请参阅[中断期间不可用的内容](#)。

支持两个新的 **Citrix Virtual Apps and Desktops** 服务版本。Citrix Monitor 现在支持两个新的 Citrix Virtual Apps and Desktops 服务版本，即 **Citrix Virtual Apps Advanced Service** 和 **Citrix Virtual Apps and Desktops Advanced Service**。有关详细信息，请参阅 Citrix Monitor [功能兼容性列表](#)。

支持 **Google Cloud Platform** 中的共享虚拟私有云 (VPC)。Citrix Virtual Apps and Desktops 服务支持 Google Cloud Platform 上的共享 VPC 作为主机资源。可以使用 Machine Creation Services (MCS) 在共享 VPC 中预配计算机，并使用 Citrix Studio 对这些计算机进行管理。有关共享 VPC 的信息，请参阅[共享虚拟私有云](#)。

对 **Google Cloud Platform** 的区域选择支持。Citrix Virtual Apps and Desktops 服务支持 Google Cloud Platform 上的区域选择。此功能允许管理员在一个区域内指定一个或多个区域以进行目录创建。

对于单租户类型的 VM，区域选择将使管理员能够跨自己选择的区域放置单租户节点。对于非唯一租户 VM，区域选择提供了在其选择的区域之间确切地放置 VM 的功能，从而提供了设计部署的灵活性。有关配置信息，请参阅[启用区域选择](#)。

此外：

- 唯一租赁提供对唯一租户节点的独占访问权限，该节点是专用于托管项目的 VM 的物理计算引擎服务器。这些节点允许您在同一个硬件上将虚拟机组合在一起，或者将虚拟机与其他项目的虚拟机分开。
- 唯一租户节点可以帮助您满足自带许可证 (BYOL) 场景的专用硬件要求。它们还使您能够遵守网络访问控制策略、安全性和隐私要求（例如 HIPAA）。

#### 注意：

唯一租赁是在 Google Cloud 上使用 Windows 10 VDI 部署的唯一途径。服务器 VDI 还支持此方法。有关唯一租赁的详细描述可在 [Google 文档站点](#) 上找到。

改进了 **Azure** 系统磁盘的引导性能。本版本支持在启用了 MCSIO 时使用 Azure 的 Citrix Cloud 实施的改进引导性能。有了此支持，您可以保留系统磁盘。这具有以下优势：

- VM 和应用程序现在可以引导和启动，其性能类似于向黄金映像提供服务的方式。
- 减少 API 配额消耗，删除和创建系统磁盘，以及删除 VM 时导致的状态转换延迟。

例如，请使用 `New-ProvScheme` 命令中的 PowerShell `PersistOSDisk` 自定义属性配置此功能。

```
1 -CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com
   /2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
   />
```

```
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
  Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
  benvaldev5RG3" />
5 <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
  />
6 </CustomProperties>'
7 <!--NeedCopy-->
```

有关更多配置信息，请参阅[提高启动性能](#)。

## 2020 年 7 月

### 新增功能和增强功能

支持对“过滤器”页面的粒度、基于角色的访问。现在，在创建自定义角色时，Citrix Studio 提供了对 **Monitor >** 过滤器页面的访问权限的更精细的控制。具体而言，您可以为自定义角色分配查看计算机、会话、连接和应用程序实例的任意组合的权限。下面是创建角色窗口中的 **Director** 对象的另外四个选项：

- “查过滤器”页面 - 仅限应用程序实例
- “查看过滤器”页面 - 仅限连接
- “查看过滤器”页面 - 仅限计算机
- “查看过滤器”页面 - 仅限会话

有关创建角色的信息，请参阅[创建和管理角色](#)。

对分配的 **VDI** 计算机的关机延迟支持（仅限 **PowerShell**）。在早期版本中，关机延迟仅适用于未分配的计算机。从本版本起，关机延迟同时适用于已分配和未分配的计算机。有关详细信息，请参阅[AutoScale 如何管理计算机电源](#)。

支持 **Windows** 客户端许可证。Citrix Virtual Apps and Desktops 服务现在支持使用 Windows 客户端许可证在 Azure 中预配 VM。要在 Azure 中运行 Windows 10 VM，请验证您与 Microsoft 签订的批量许可协议是否符合此使用条件。有关详细信息，请参阅[使用 Azure Resource Manager 主映像创建计算机目录](#)。

## 2020 年 5 月

### 新增功能和增强功能

计算机重新启动计划。现在，您可以指示重新启动计划是否影响处于维护模式的计算机。此功能仅在 PowerShell 中可用。有关详细信息，请参阅[对处于维护模式的计算机执行计划的重新启动](#)。

资源可用性。现在，您可以在中断期间确保资源可用性，而无需在每个区域（资源位置）中发布资源。有关详细信息，请参阅[资源可用性](#)。



## 2020 年 4 月

### 新增功能和增强功能

**VDI** 交付组的增强计划粒度（仅限 **PowerShell**）。AutoScale 现在支持按 30 分钟的粒度级别定义计划中包含的天数的高峰时间。可以单独设置一天中每半小时在 VDI 交付组中运行的计算机的最小数量。此外，AutoScale 现在可以每半小时而非每小时增加或降低 VDI 交付组中已打开电源的计算机数量。有关详细信息，请参阅 [Broker PowerShell SDK 命令](#)。

**MTU** 发现。Citrix 协议 Enlightened Data Transport (EDT) 现在具有 MTU 发现功能。MTU 发现允许 EDT 自动确定和设置会话的有效负载大小。通过此功能，ICA 会话可以根据具有非标准最大传输单元 (MTU) 或最大分段大小 (MSS) 要求的网络进行调整。调整功能可避免出现数据包碎片，这可能会导致性能降低或无法建立 ICA 会话。此更新需要至少使用适用于 Windows 的 Citrix Workspace 应用程序 1911。如果使用 Citrix Gateway，则所需的 Citrix ADC 固件版本最低为 13.0.52.24 或 12.1.56.22。有关详细信息，请参阅 [EDT MTU 发现](#)。

## 2020 年 3 月

### 新增功能和增强功能

**PVS** 目标设备指标。Citrix Monitor 现在在“计算机详细信息”页面上提供 PVS 目标设备衡量指标面板。使用面板可查看单会话和多会话操作系统计算机的 Provisioning 目标设备的状态。此面板上提供了网络、启动和缓存的几个衡量指标。这些指标可帮助您监视 PVS 目标设备并对其进行故障排除，以确保其已启动并且正在运行。有关详细信息，请参阅 [PVS 目标设备指标](#)。

**AWS** 实例属性捕获。MCS 现在从从中获取 AMI 的实例中读取属性，并将计算机的 IAM 角色和标记应用于为给定目录预配的计算机。使用此可选功能时，目录创建过程会查找选定的 AMI 源实例，读取一组有限的属性。然后，这些属性将存储在 AWS 启动模板中，该模板用于为该目录预配计算机。目录中的任何计算机都会继承捕获的实例属性。有关详细信息，请参阅 [AWS 实例属性捕获](#)。

**AWS** 运行资源标记。此版本引入了一个选项，用于在预配期间标记 Citrix 组件创建的资源。每个标记都表示一个由客户定义的密钥和一个可选值组成的标记，可提高您管理、搜索和筛选资源的能力。有关详细信息，请参阅 [AWS 运行资源标记](#)。

**Azure** 存储中的安全传输。Machine Creation Services (MCS) 为 Azure Resource Manager 环境中由 MCS 预配的目录创建的存储帐户提供了增强功能。此增强功能会自动启用安全传输所需的属性。此选项仅允许来自安全连接的帐户请求，从而增强了存储帐户的安全性。有关详细信息，请参阅 Microsoft 站点上的[需要安全传输以确保安全连接](#)。

在 Azure 中创建存储帐户时启用安全传输所需的属性：



Create storage account

Basics

Advanced

Tags

Review + create

SECURITY

Secure transfer required ⓘ

Disabled

Enabled

VIRTUAL NETWORKS

Allow access from

All networks

Selected network

ⓘ All networks will be able to access this storage account. [Learn more](#)

DATA LAKE STORAGE GEN2 (PREVIEW)

Hierarchical namespace ⓘ

Disabled

Enabled

Review + create

Previous

Next : Tags >

支持 **Azure SSD** 托管磁盘。Machine Creation Services (MCS) 支持 Azure 虚拟机的标准 SSD 托管磁盘。与 HDD 磁盘相比，此磁盘类型提供了一致的性能，并且提供了更好的可用性。有关详细信息，请参阅 [Standard SSD Disks for Azure Virtual machine workloads](#)（适用于 Azure 虚拟机工作负载的标准 SSD 磁盘）。

使用 `New-ProvScheme` 命令或 `Set-ProvScheme` 命令中的 `PowerShell StorageAccountType` 自定义属性配置此功能：

```
1 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" /><Property xsi:type="StringProperty" Name="StorageAccountType" Value="StandardSSD_LRS" /><Property xsi:type="StringProperty" Value="Windows_Server" />
2 <!--NeedCopy-->
```

注意：

此功能仅在使用托管磁盘时可用，即，自定义属性 `UseManagedDisks` 设置为 **true**。对于非托管磁盘，仅支持标准 HDD 和高级 SSD。

## 2020 年 1 月

### 新增功能和增强功能

**Citrix Studio** 中的语言栏。自本版本起，Citrix Studio 提供了一个语言栏，以帮助进行正确的键盘映射。

- 如果 Citrix Cloud 的语言或浏览器的显示语言设置为英语或日语，则不会显示语言栏。
- 如果 Citrix Cloud 的语言或浏览器的显示语言设置为德语、西班牙语或法语，语言栏在您登录 Citrix Studio 后显示。语言栏列表中有两种语言选项。请选择与浏览器最顶部的语言匹配的选项。

提示：

- 1 - Settings that you configure **for** the language bar might not take effect. In **this case**, log out and log back on.
- 2 - You might fail to input certain symbols and localized characters by using the language bar. To resolve the issue, you need to configure the language of Citrix Cloud, the display language of your browser, and the local keyboard layout. For more information, see Knowledge Center article [CTX310743] (<https://support.citrix.com/article/CTX310743>).

重新启动计划的最大延迟计时器（仅限 **PowerShell**）。如果由于站点数据库中断而未开始交付组中计算机的计划重新启动，则可以指定超过计划的启动时间后需等待的时间。如果在此间隔内还原了数据库连接，则重新启动将开始。如果在此间隔内未恢复连接，则重新启动不会开始。有关详细信息，请参阅[计划的重新启动因数据库中断而延迟](#)。

垂直负载平衡（仅限 **PowerShell**）。以前，该服务对所有 RDS 启动使用水平负载平衡，这会将传入负载分配给负载最小的 RDS 计算机。这仍然是默认行为。现在，您可以使用 PowerShell 将垂直负载平衡作为站点范围的设置启用。

启用垂直负载平衡时，Broker 将传入负载分配给未达到高水印的负载最多的计算机。这将使现有计算机饱和，然后再转移到新计算机。当用户断开连接并释放现有计算机时，将为这些计算机分配新负载。

默认情况下，启用水平负载平衡。为查看、启用或禁用垂直负载平衡，`Get-BrokerSite` 和 `Set-BrokerSite` cmdlet 现在支持 `UseVerticalScalingForRdsLaunches` 设置。有关详细信息，请参阅[交付组中的负载托管计算机](#)。

## 2019 年 12 月

### 新增功能和增强功能

面向 **Citrix Service Providers (CSP)** 的服务。CSP 现在可以将租户客户登录到 Virtual Apps and Desktops 服务，配置客户管理员对服务的访问权限，以及使用联盟域向客户的用户提供共享或专用工作区。有关详细信息，请参阅[面向 Citrix Service Provider 的 Citrix Virtual Apps and Desktops 服务](#)。

支持确定计算机处于维护模式的原因（仅限 **PowerShell**）。使用 PowerShell，您现在可以确定计算机处于维护模式的原因。为此，请使用参数 `-MaintenanceModeReason`。该功能对于管理员在维护模式下对计算机问题进行

故障排除非常有用。有关详细信息，请参阅 <https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/Broker/Get-BrokerMachine/>。

**AutoScale**。AutoScale 现在提供动态创建计算机以及将其删除的功能。可以使用 PowerShell 脚本来利用该功能。该脚本可帮助您根据当前负载条件动态增加或减少交付组中的计算机数量。有关详细信息，请参阅[通过 AutoScale 动态预配计算机](#)。

## 2019 年 11 月

### 新增功能和增强功能

**GroomStartHour**。Monitor 现在支持 **GroomStartHour**，这是一种新配置，可帮助管理员确定整理应开始运行的一天中的时间。有关详细信息，请参阅 [Citrix Virtual Apps and Desktops SDK 文档](#)。

**OData** 分页。Monitor 现在支持 **OData** 分页。所有 OData v4 端点每页最多返回 100 条记录，其中包含指向响应中接下来 100 条记录的链接。有关详细信息，请参阅[使用 Citrix Cloud 中的 OData v4 端点访问 Monitor Service 数据](#)。

## 2019 年 10 月

### 新增功能和增强功能

**App-V**。App-V 功能现在在 Citrix Cloud 中提供。可以在 Citrix Cloud 配置中以单管理员模式或双管理员模式将 App-V 包添加到 Delivery Controller 中。[Citrix 下载](#) 中提供的 *Virtual Apps and Desktops Service App-V* 包发现模块允许您导入 App-V 包并注册 Microsoft App-V 服务器。其中包含的应用程序随后可供用户使用。此 PowerShell 模块允许您使用 DNS URL 注册 Microsoft App-V 管理和发布服务器，从而避免使用其实际计算机 URL 注册负载均衡机制后的服务器。有关详细信息，请参阅[适用于 App-V 包和服务器的 Citrix Virtual Apps and Desktops 服务发现模块](#)。

**Google Cloud Platform**。Citrix Virtual Apps and Desktops 服务现在增加了对使用 Machine Creation Services (MCS) 在 Google Cloud Platform (GCP) 上预配计算机的支持。有关详细信息，请参阅 [Google Cloud Platform 虚拟化环境](#)。

## 2019 年 9 月

### 新增功能和增强功能

**VDA 对 Azure 虚拟桌面的支持**。有关支持的操作系统和 VDA 版本，请参阅 [Azure 虚拟桌面环境中的 VDA](#)。

增强的电源策略。在早期版本中，过渡到需要执行某项操作（断开连接操作 = “挂起”或“关闭”）的时间段的 VDI 计算机保持开启状态。如果计算机在不需要任何操作（断开连接操作 = “无”）的时间段（高峰或非高峰时段）断开连接，就会发生这种情况。

自本版本起，在指定的断开连接时间过后，AutoScale 将暂停或关闭计算机电源，具体取决于为目标时间段配置的断开连接操作。有关详细信息，请参阅[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](#)。

计算机目录：标记。您现在可以使用 PowerShell 将标记应用于计算机目录。有关详细信息，请参阅[将标记应用到计算机目录](#)。

会话启动持续时间。Monitor 现在显示会话启动持续时间，分为 Workspace 应用程序会话启动时间段和 VDA 会话启动时间段。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。此功能在 VDA 1903 或更高版本中可用。有关详细信息，请参阅[诊断会话启动问题](#)。

## 2019 年 8 月

### 新增功能和增强功能

会话自动重新连接。“趋势”选项卡上的“会话”页面现在包含与自动重新连接次数有关的信息。“会话可靠性”或“客户端自动重新连接”策略生效时，将尝试自动重新连接。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。

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。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 Receiver for Windows 和 Citrix Receiver for Mac。此功能需要 VDA 1906 或更高版本。有关详细信息，请参阅：

- [会话](#)
- [客户端自动重新连接策略设置](#)
- [会话可靠性策略设置](#)
- [会话自动重新连接](#)

## 2019 年 7 月

### 新增功能和增强功能

配置日志记录。现在，您可以使用 Remote PowerShell SDK 定期删除配置日志记录数据库内容。有关详细信息，请参阅[计划定期删除数据](#)。

**AutoScale**。AutoScale 现在提供仅管理交付组中计算机子集的灵活性。此功能在云爆发用例中非常有用，在此类用例中，您希望在基于云的资源满足其他需求（即工作负载爆发）之前使用本地资源处理工作负载。有关详细信息，请参阅[将 AutoScale 限制到交付组中的某些计算机](#)。

本地应用程序访问和 **URL** 重定向。Citrix Studio 现在允许您使用 PowerShell SDK 将“添加本地应用程序访问应用程序”选项添加到站点的 Studio 用户界面。有关详细信息，请参阅[仅提供对已发布应用程序的访问](#)。

操作系统名称更改。创建计算机目录 > 计算机目录设置 > 操作系统和监视页面上的操作系统名称已更改：

- 多会话操作系统（以前称为“服务器操作系统”）：多会话操作系统计算机目录为大规模部署标准化的 Windows 多会话操作系统或 Linux 操作系统计算机提供托管的共享桌面。
- 单会话操作系统（以前称为桌面操作系统）：单会话操作系统计算机目录提供的 VDI 桌面是各种用户的理想选择。

配置文件加载过程中 **Citrix Profile Management** 的持续时间。Monitor 现在包括登录持续时间图表的配置文件加载栏中的配置文件处理持续时间。这是 Citrix Profile Management 处理用户配置文件的持续时间。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，使其具有更高的准确性。此增强功能在 VDA 1903 及更高版本中可用。有关详细信息，请参阅[配置文件加载](#)。

桌面探测。桌面探测是 Citrix Virtual Apps and Desktops 服务的一项功能。此功能自动执行在站点上发布的虚拟桌面的运行状况检查，这样可以改进用户体验。要启动桌面探测，请在一个或多个端点上安装并配置 Citrix Probe Agent。桌面探测适用于获得 Premium 许可的站点。此功能需要 Citrix Probe Agent 1903 或更高版本。有关详细信息，请参阅[应用程序和桌面探测](#)。

注意：

Citrix Probe Agent 现在支持 TLS 1.2。

## 2019 年 6 月

### 新增功能和增强功能

通过标记限制。标记是指用于标识计算机、应用程序、桌面、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。有关详细信息，请参阅[应用程序组](#)和[标记](#)。

电子邮件通知。Citrix Virtual Apps and Desktops 服务直接发送与警报和探测有关的电子邮件通知。这样将无需配置 SMTP 电子邮件服务器。默认情况下，通知首选项框处于启用状态，Citrix Cloud 将向通知首选项部分中提供的电子邮件地址发送警报通知。确保电子邮件地址 [donotreplynotifications@citrix.com](mailto:donotreplynotifications@citrix.com) 在您的电子邮件设置中列入白名单。

## 2019 年 5 月

### 新增功能和增强功能

**AutoScale**。AutoScale 是 Citrix Virtual Apps and Desktops 服务一项功能，可提供一致的高性能解决方案，以主动管理您的计算机的电源。它旨在平衡成本和用户体验。AutoScale 将弃用的 Smart Scale 技术集成到 Studio 电源管理解决方案中。有关详细信息，请参阅[AutoScale](#)。可以从 **Monitor** 选项卡上的“趋势”页面监视 AutoScale 托管的计算机的指标。有关详细信息，请参阅[监视 AutoScale 托管的计算机](#)。

## 2019 年 2 月

### 新增功能和增强功能

虚拟机管理程序警报监视。来自 Citrix Hypervisor 和 VMware vSphere 的警报现在显示在监视 > 警报选项卡上，以帮助监视以下虚拟机管理程序运行状况的状态/参数：

- CPU 使用率
- 内存使用率
- 网络使用情况
- 虚拟机管理程序连接不可用
- 磁盘使用情况（仅限 vSphere）
- 主机连接或电源状态（仅限 vSphere）

有关详细信息，请参阅[警报和通知](#)中的“虚拟机管理程序警报监视”部分。

通过早期 **TLS** 版本进行的通信。为了提高服务的安全性，Citrix 将自 2019 年 3 月 15 日起阻止通过传输层安全性 (TLS) 1.0 和 1.1 进行的任何通信，仅允许 TLS 1.2 通信。有关详细信息，请参阅[TLS 版本](#)。有关全面的指导，请参阅[CTX247067](#)。

应用程序组。可以借助应用程序组管理应用程序的集合。可为在不同交付组之间共享的应用程序或由交付组中的部分用户使用的应用程序创建应用程序组。有关详细信息，请参阅[创建应用程序组](#)。

登录性能 - 配置文件深入分析。**Monitor** 中用户详细信息页面上的登录持续时间面板现在包括与登录过程的配置文件加载阶段深入分析有关的信息。配置文件深入分析为当前会话提供有关用户配置文件的有用信息，这些信息可帮助管理员对高配置文件加载问题进行故障排除。将显示与以下用户配置文件信息有关的工具提示：

- 文件数量
- 配置文件大小
- 大型文件的数量

详细的深入分析可提供各个文件夹、其大小和文件数量的信息。此功能在 VDA 1811 及更高版本中提供。有关详细信息，请参阅[诊断用户登录问题](#)。

**Microsoft RDS** 许可证运行状况。Monitor 在“计算机详细信息”的计算机详细信息面板和服务器操作系统计算机的“用户详细信息”页面中显示的 Microsoft RDS（远程桌面服务）许可证状态。将针对许可证状态显示相应的消息。您可以将鼠标悬停在信息图标上方以查看更多详细信息。有关详细信息，请参阅[对计算机进行故障排除](#)中的“Microsoft RDS 许可证运行状况”部分。

应用程序探测。此功能可自动评估站点中发布的虚拟应用程序的运行状况。

要启动应用程序探测，请执行以下操作：

- 在一台或多台终端计算机上，安装 Citrix Application Probe Agent
- 使用 Citrix Workspace 和 Citrix Virtual Apps and Desktops 服务的凭据配置 Citrix Application Probe Agent。

- 在 Citrix Virtual Apps and Desktops 服务的监视 > 配置中配置要探测的应用程序、要在其上运行探测的端点计算机以及计划的探测时间。

代理通过 Citrix Workspace 测试所选应用程序的启动，并在 Citrix Virtual Apps and Desktops 服务的监视选项卡上报告探测结果：

- 应用程序页面-过去 24 小时的数据和“趋势” > “应用程序探测结果”页面
- 历史探测数据以及发生探测故障时的阶段 - Workspace 可访问性、Workspace 身份验证、Workspace 枚举、ICA 下载或应用程序启动

故障报告通过电子邮件发送到配置的电子邮件地址。可以安排应用程序探测在非高峰时间跨多个地理位置运行。通过这种方式，您可以在用户遇到与预配的应用程序、托管计算机或连接有关的问题之前使用这些结果主动对这些问题进行故障排除。有关详细信息，请参阅[应用程序和桌面探测](#)。

## 2019 年 1 月

### 新增功能和增强功能

具有自定义作用域的委派管理。监视功能现在支持内置委派管理员角色的自定义作用域。有关可用于监视的内置角色以及如何分配这些角色的详细信息，请参阅[委派管理员角色](#)。

## 2018 年 12 月

### 新增功能和增强功能

Citrix 将阻止通过传输层安全性 (TLS) 1.0 和 1.1 进行的通信的日期已从 2018 年 12 月 31 日更改为 2019 年 1 月 31 日。有关详细信息，请参阅[弃用 TLS 版本](#)。

## 2018 年 11 月

### 新增功能和增强功能

使用 **OData API** 提供的计算机历史数据：包含计算机分析的历史数据现在可通过 OData API 获取。此数据是按小时收集的，累积每天的数据。

- 已打开电源的计算机（电源托管计算机）的数量
- 已注册的计算机数量
- 处于维护模式的计算机数量
- 计算机总数



此数据汇聚了监视服务运行期间的数据。有关 OData API 的用法及示例的详细信息，请参阅 [Citrix Monitor Service 7 1808](#)。数据库架构在 [Monitor Service 架构](#) 中提供。

**登录性能 - 交互式会话深入查看：**用户和会话详细信息视图中的登录持续时间面板中包含与登录过程的交互式会话阶段有关的信息。三个子阶段（**Pre-userinit**、**Userinit** 和 **Shell**）的每个子阶段所需的时间在交互式会话栏中显示为一个工具提示。这将提供此登录阶段的更精细的故障排除和修正。此外，还提供子阶段与指向文档的链接之间的累积延迟时间。此功能在 Delivery Controller 版本 7 1808 及更高版本中提供。交互式会话明细栏仅显示当前会话的持续时间。有关详细信息，请参阅[诊断用户登录问题](#)。

**登录性能 - GPO 深入查看：**用户和会话详细信息视图中的登录持续时间面板中包含 GPO（组策略对象）持续时间。这是登录过程中在虚拟机上应用 GPO 所需的总时间。您现在可以看到按照 CSE（客户端扩展）应用的每个策略的明细在 GPO 栏中以工具提示的形式显示。对于每个策略应用程序，明细将显示状态和所需的时间。这一附加信息简化了涉及高 GPO 持续时间的故障排除和修正过程。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。此功能在 Delivery Controller 版本 7 1808 及更高版本中提供。有关详细信息，请参阅[诊断用户登录问题](#)。

## 修复

监视过程中保存的自定义报告查询在执行云升级后不可用。[DNA-23420]

## 2018 年 10 月

### 新增功能和增强功能

**应用程序：**每台计算机的限制。您现在可以限制每台计算机的应用程序实例数。此限制适用于站点中的所有计算机。此限制是面向交付组中的所有用户的现有应用程序限制以及每个用户的限制的补充。此功能仅通过 PowerShell 提供，不在 Studio 中提供。有关详细信息，请参阅[配置应用程序限制](#)。

**Windows Server 2019。**现在，您可以在 Windows Server 2019 计算机上安装适用于多会话操作系统的 VDA（以前称为适用于服务器操作系统的 VDA），如[系统要求](#)中所述。

## 2018 年 9 月

### 新增功能和增强功能

**委派管理。**如果具有委派管理权限，则可以根据您的所有管理员在贵组织中的角色来配置其所需的访问权限。有关详细信息，请参阅[委派管理](#)。监视功能支持内置角色的分配。内置角色可以全面使用。有关用于监视的内置角色以及如何分配这些角色的详细信息，请参阅[委派管理员角色](#)。

**配置日志记录。**利用配置日志记录功能，管理员可以跟踪配置更改和管理活动。有关详细信息，请参阅[配置日志记录](#)。

现在已启用以前禁用的 Remote PowerShell SDK 中的多个 PowerShell cmdlet，以便与配置日志记录结合使用：

- Log:GetLowLevelOperation
- Log:GetHighLevelOperation
- Log:GetSummary
- Log:GetDataStore
- Log:ExportReport

本地主机缓存。本地主机缓存现已完全可用。本地主机缓存功能允许在资源位置中的 Cloud Connector 无法与 Citrix Cloud 通信时继续执行连接代理操作。有关详细信息，请参阅[本地主机缓存](#)。

**Citrix Provisioning。**要预配 VDA，您现在可以使用 Citrix Provisioning 或现有的 Machine Creation Services。有关特定于云环境的 Citrix Provisioning 的信息，请参阅[Citrix Provisioning 由 Citrix Cloud 进行管理](#)。

## 修复

在早期版本中，如果使用 Azure 按需预配，关闭电源时将删除所有 VM。现在将仅删除池 VM。关闭电源时不删除静态（专用）VM。

## 2018 年 8 月

- 新产品名

如果您已作为 Citrix 客户或合作伙伴一段时间，您会注意到在我们的产品和此产品文档中出现的新名称。如果您是此 Citrix 产品的新用户，可能会看到某个产品或组件的不同名称。

新的产品和组件名称源于扩展的 Citrix 产品组合和云策略。本产品文档中的文章使用以下名称。

- **Citrix Virtual Apps and Desktops:** Citrix Virtual Apps and Desktops 以云服务和本地产品的方式提供虚拟应用程序和桌面解决方案，使员工能够随时随地在任何设备上自由地工作，同时降低了 IT 成本。从任何云提供 Windows、Linux、Web 和 SaaS 应用程序或完整的虚拟桌面：共有云、本地云或混合云。Virtual Apps and Desktops 以前称为 XenApp 和 XenDesktop。
- **Citrix Workspace** 应用程序：Citrix Workspace 应用程序集成了现有的 Citrix Receiver 技术以及其他 Citrix Workspace 客户端技术。此产品已增强，能够提供更多功能，以向最终用户提供统一的上下文体验，在此产品中，用户可以与所有工作应用程序、文件以及必须最好地完成工作所需的设备进行交互。有关详细信息，请参阅此 博客文章。
- **Citrix SD-WAN:** NetScaler SD-WAN 是一项至关重要的技术，面向我们通过云技术转换其分支机构网络和 WAN 的客户和合作伙伴，现已更名为 Citrix SD-WAN。
- **Citrix Secure Web Gateway:** 随着 Citrix Networking 产品组合的扩展，我们很自豪能够提供强大的 Citrix Secure Web Gateway 服务，以前称为 NetScaler Secure Web Gateway。
- **Citrix Gateway:** 我们的功能强大的 NetScaler Unified Gateway，允许您用来安全地对必须最好地完成工作所需的应用程序和数据进行上下文访问，现已更名为 Citrix Gateway。
- **Citrix Content Collaboration** 和适用于 **Windows** 的 **Citrix Files:** ShareFile 的高级访问、协作、工作流、权限管理和集成功能现已在我们安全、上下文集成 Citrix Workspace 的 Citrix Content

Collaboration 组件集中提供。通过 Citrix Files for Windows，您可以直接通过映射的驱动器来访问 Content Collaboration 文件，从而提供本机 Windows 资源管理器体验。

- **Citrix Hypervisor**: XenServer 提供的面向虚拟化基础结构的技术，在 XenProject 虚拟机管理程序的基础上构建，现已更名为 Citrix Hypervisor。

下面是简要概述：

新名称	旧名称
Citrix Virtual Apps and Desktops	XenApp 和 XenDesktop
Citrix Workspace 应用程序	集成了 Citrix Receiver 和大量的增强功能
Citrix SD-WAN	NetScaler SD-WAN
Citrix Secure Web Gateway	NetScaler Secure Web Gateway
Citrix Gateway	NetScaler Unified Gateway
Citrix Content Collaboration	ShareFile
Citrix Files for Windows	ShareFile Desktop App、ShareFile Sync、ShareFile Drive Mapper
Citrix Hypervisor	XenServer
Citrix Provisioning	Citrix Provisioning Services

在我们的产品及其文档中实现此转换是一个正在进行的过程。

- 产品中的内容可能仍包含以前的名称。例如，您可能会在控制台文本、消息以及目录/文件名中看到早期的名称实例。
- 某些项目（例如命令和 MSI）可能会继续保留以前的名称，以防止损坏客户的现有脚本。
- 相关产品文档以及从此产品的文档链接的其他资源（例如视频和博客文章）可能仍包含以前的名称。
- 对于 Citrix Hypervisor：新名称自 2018 年 9 月起在 Citrix Web 站点和信息性产品资料中使用。您还会在某些 Citrix 产品（例如 Citrix Virtual Apps and Desktops）的管理员控制台中看到新名称。XenServer 产品版本和技术文档资料将继续使用 XenServer 7.x，直至 2019 年初。

感谢您在此转换期间耐心等待。

有关新名称的更多详细信息，请参阅 <https://www.citrix.com/about/citrix-product-guide/>。

#### • 产品和组件版本号变更

Citrix 安装和管理大多数 Citrix Virtual Apps and Desktops 组件，因此您不必担心这些版本号。但是，您可能在安装 Cloud Connector 以及在资源位置中安装或升级 VDA 时看到版本号。

Citrix Virtual Apps and Desktops 产品和组件版本号按以下格式显示：**YYMM.c.m.b**

- YYMM = 发布产品或组件时的年份和月份。例如，2018 年 9 月的发行版显示为 1809。

- c = 当月的 Citrix Cloud 版本号。
- m = 维护版本（如果适用）。
- b = 内部版本号。此字段仅在组件的“关于”页面上以及用于删除或更改程序的操作系统功能中显示。

例如，**Citrix Virtual Apps and Desktops 1809.1.0** 表示该组件是在 2018 年 9 月发布的。它与当月的 Citrix Cloud 发行版 1 相关联，并且不是维护版本。某些显示内容仅显示版本的年份和月份：例如，**Citrix Virtual Apps and Desktops 1809**。

在早期版本（7.18 及更早版本）中，版本号的显示格式如下：7.version，其中，version 每个版本增加 1。例如，XenApp and XenDesktop 7.17 之后的 VDA 版本为 7.18。早期版本（7.18 及更早版本）不使用新编号格式进行更新。

- 弃用 **TLS** 版本。为了提高 Citrix Virtual Apps and Desktops 服务的安全性，Citrix 将阻止通过传输层安全性 (TLS) 1.0 和 1.1 进行的任何通信，自 2018 年 12 月 31 日起生效。有关详细信息，请参阅 [弃用 TLS 版本](#)。
- **Google Cloud Platform** 虚拟化环境。Citrix Virtual Apps and Desktops 服务支持在 Google Cloud Platform (GCP) 上手动关闭并打开 Virtual Apps and Desktops VM 的功能。有关详细信息，请参阅 [Google Cloud Platform 虚拟化环境](#)。

## 2018 年 7 月

- 导出过滤器数据。您现在可以将 **Monitor** > 过滤器选项卡中的实时监视数据导出到 CSV 格式的文件中。导出功能在“计算机”、“会话”、“连接”和“应用程序实例”过滤器页面中提供。可以选择一个预定义的自定义过滤器或选择恰当的过滤条件，在表格中选择所需的列，然后导出数据。最多可以导出包含 100000 条记录的数据。导出的 CSV 文件提供实时数据的综合视图，有助于简化大型数据集的分析。

## 2018 年 6 月

- **Azure Resource Manager** 连接。在 Studio 连接创建向导中，连接页面上的 Azure 环境选择包括所有对您的 Azure 订阅有效的 Azure 云。Azure 美国政府云和 Azure 德国云的通用版本取代了早期版本中这两种环境的预览版本。

## 2018 年 5 月

- **Azure** 快速部署。当您的资源位置使用 Azure Resource Manager 计算机交付应用程序和桌面时，现在可以选择一种部署方法：
  - 完整配置：这一现有的方法使用 Studio 管理控制台，该控制台将引导您完成创建计算机目录，然后创建交付组的过程。
  - Azure 快速部署：这一新选项提供了一个更简单的界面，可以更快地部署应用程序和桌面。

- **Citrix Health Assistant** 链接。“监视”控制台中未注册的计算机的“计算机详细信息”页面现在包含 **Health Assistant** 按钮。目前，该按钮链接到[计算机故障排除](#)一文和知识中心文章 [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)，可以从中下载该工具。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，以确定常见 VDA 注册、会话启动和时区重定向配置问题的可能的根本原因。
- 交互式会话深入分析。在监视控制台中，用户详细信息视图 > 登录持续时间面板现在包括与登录过程的交互式会话阶段有关的信息。为了提供此登录阶段更精细的故障排除和修正，交互式会话现在包含三个子阶段：**Pre-userinit**、**Userinit** 和 **Shell**。在本版本中，将鼠标悬停在交互式会话上将显示一个显示子阶段以及指向文档的链接的工具提示。有关各子阶段的说明以及如何提高每个阶段的性能说明，请参阅[诊断用户登录问题](#)。

## 2018 年 3 月

- 应用程序实例预测（预览版功能）。这是第一个基于预测分析的监视功能。预测资源使用模式对于管理员在每种资源上组织资源和所需许可证数量非常重要。应用程序实例预测功能指示随着时间的推移，每个站点或交付组可能启动的托管应用程序实例的数量。基于使用现有历史数据创建的数据模型的机器学习算法用于进行预测。容差级别表示预测质量。

有关详细信息，请参阅 Director 中的[应用程序实例预测](#)。请在 [Citrix Cloud 论坛](#)中提交关于此功能的实用性和可用性的反馈。

- 交付组 **API** - 预览版

交付组 API 预览版提供了一组 REST API，您可以使用这些 API 自动管理交付组。可以在 Citrix Cloud API 文档（网址为 <https://developer.cloud.com/>）中查看和试用完整的可用 API 集。

- **Web Studio** 身份验证

Citrix Cloud 上的服务管理控制台现在使用持有者令牌对客户进行身份验证。对交付组 REST API 的访问进行身份验证需要持有者令牌。

- 使用 **OData** 版本 4 API 访问 **Monitor Service** 数据（预览版功能）

可以使用 OData V.4 端点基于 Monitor Service 数据创建自定义监视和报告控制板。OData V.4 基于 ASP .Net Web API，支持聚合查询。请使用 Citrix Cloud 用户名和持有者令牌通过 V4 端点访问数据。有关详细信息和示例，请参阅[使用 Citrix Cloud 中的 OData v4 端点访问 Monitor Service 数据](#)。

在 [Citrix Cloud 论坛](#)中分享您对此功能的实用性的反馈意见。

## 修复

- 可以重命名、移动和删除应用程序文件夹。[#STUD-2376]

## 2018 年 1 月

- **RDS** 许可证检查。现在创建包含 Windows Server OS 计算机的计算机目录时，会进行 RDS 许可证自动检查。发现的任何 RDS 许可证问题都会显示，以便您可以采取适当的步骤来防止服务出现中断。有关详细信息，请参阅[创建计算机目录](#)。
- 从 **Monitor** 访问计算机控制台。Monitor 中的“计算机详细信息”面板现在提供访问 XenServer 虚拟机管理程序 7.3 上托管的计算机的控制台的功能。您现在可以在 VDA 中直接从 Monitor 对问题进行故障排除。有关详细信息，请参阅“计算机故障排除”中的[计算机控制台访问](#)。

## 2017 年 12 月

### 新增功能和增强功能

- **Citrix Workspace**。Citrix Workspace 现已对新 XenApp and XenDesktop Service 客户可用。有关详细信息，请参阅[Workspace 配置](#)。
- 应用程序分析。现在可以使用 **Monitor** > 应用程序选项卡上的新“应用程序分析”页面高效地分析和监视应用程序的性能。该页面提供了在您的站点上发布的所有应用程序的运行状况和使用情况的综合视图。它显示一些指标（例如，每个应用程序的实例数），以及与已发布的应用程序关联的故障和错误。此功能需要 VDA 版本 7.15 或更高版本。  
  
有关详细信息，请参阅 Monitor 中的[应用程序分析](#)部分。

## 2017 年 11 月

### 新增功能和增强功能

- 本地主机缓存。本地主机缓存功能允许在资源位置中的 Cloud Connector 无法与 Citrix Cloud 通信时继续执行连接代理操作。有关详细信息，请参阅[本地主机缓存](#)。
- **Azure** 托管磁盘。Azure 托管磁盘功能现在默认由 Azure Resource Manager 环境中 MCS 预配的 VM 使用。或者，您也可以使用常规存储帐户。有关详细信息，请参阅[Microsoft Azure Resource Manager 虚拟化环境](#)。
- 技术支持管理员。管理 Citrix Cloud 客户帐户的服务管理员时，您现在可以使用一个新选项，即：技术支持管理员。技术支持管理员可以访问该服务中的监视功能。有关详细信息，请参阅[管理](#)。

### 修复

- 您现在可以使用服务管理控制台向导创建 Remote PC Access 计算机目录。在早期版本中，必须使用 PowerShell cmdlet 才能创建目录（如 [CTX220737](#) 文档中所述）。其次，必须返回到管理控制台才能创建交付组。现在，您可以在管理控制台中依次创建目录和交付组。
- MCS 创建的目录可以使用现有 Active Directory 计算机帐户。[#DNA-24566]
- 监视部署时，在排序后的趋势 > 会话表中滚动将显示准确的结果。[DNA-51257]



## 更多信息

- [已知问题](#)。
- 有关服务中包含的第三方软件的信息，请参阅[第三方声明](#)。

## 已知问题

March 5, 2024

Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）存在以下已知问题：

- 在使用完整配置界面创建与 Azure 的主机连接时，如果选择启用加入了 **Azure AD** 的设备管理或单击连接详细信息页面上的创建服务主体，然后单击下一步，则可能会出现错误。要解决此问题，请在浏览器中允许第三方 Cookie。[STUD-24463]
- 在 AWS 上托管的 VMware 环境中，如果主映像已启用 vTPM，则创建 MCS 计算机目录将失败。有关 VMware 支持，请参阅[获取支持](#)。[PMCS-37603]
- 如果 Pendo URL <https://citrix-cloud-content.customer.pendo.io/> 被屏蔽，监视器屏幕可能无法加载。  
[DIR-18482]
- 如果您在 Remote PowerShell SDK 中运行带 **XDHyp:\** 的命令，就会出现错误。要解决此问题，请执行以下操作：
  1. 运行带 **Hyp** 的命令。例如：**Get-HypServiceStatus**
  2. 运行带 **XDHyp:\** 的命令。例如：**Get-ChildItem XDHyp:\Connections\**  
[BRK-13723]
- 在 2209 版中更改 Citrix DaaS 体系结构后，Windows 桌面和在此版本之前部署的应用程序的默认图标已更改为通用 PC 桌面图标。此更改仅适用于指向默认图标的桌面和应用程序。如果您想将图标更改回 Windows 应用程序的默认图标，请使用 Remote PowerShell SDK 运行以下脚本：  
**Get-BrokerApplication -IconUid 1 | Set-BrokerApplication -IconUid 0。**
- 在“管理”>“完整配置”中，尝试更改 Azure 目录的操作系统类型失败并显示错误消息。即使您使用 PowerShell，也不再支持更改 Azure 目录的操作系统类型。[STUD-19819]
- 在 Microsoft Azure 环境中，同时启用 Azure 临时操作系统磁盘和 MCS I/O 无法创建计算机目录。但是，对于现有计算机目录，您仍然可以更新计算机目录、添加或删除 VM 以及删除计算机目录。[PMCS-21698]
- “平均 IOPS”、“会话控制”和“电源控制”按钮的下拉箭头图标可能不会显示在用户详细信息和计算机详细信息页面上。但是，该功能可以正常工作。要查看菜单上的所有项目，请单击该按钮上的任意位置。[DIR-11875]



- 如果使用 Azure AD 域服务：Workspace（或 StoreFront）登录 UPN 必须包含启用 Azure AD 域服务时指定的域名。登录不能为您创建的自定义域使用 UPN，即使该自定义域被指定为主域亦如此。
- 部署到 Azure 并创建启用了写回缓存功能并且主映像上安装的 VDA 为 1811 或更低版本的 MCS 目录版本 7.9 或更高版本时，会发生错误。此外，您将无法创建与适用于 Microsoft Azure 的 Personal vDisk 有关的任何对象。解决方法是选择其他目录版本部署到 Azure，或禁用回写缓存。要在创建目录时禁用回写缓存，请清除“计算机”页面上的“分配给缓存的内存”和“磁盘缓存大小”复选框。
- 监视 > 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]
- 当您尝试在 Workspace 应用程序 Web 或桌面上使用“重启”选项时，“重新启动”对话框永远不会关闭也永远不会报告成功。虚拟机管理程序显示计算机已关闭但尚未启动。解决方法是，一段时间后，用户可以关闭“重新启动”对话框并启动桌面，桌面必须启动。[BRK-5564]

要了解与当前 VDA 有关的问题，请参阅[已知问题](#)。

弃用

March 5, 2024

本文将提前通知您正在逐步淘汰的 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）功能，以便您能够及时做出业务决策。Citrix 将监视客户使用情况和反馈以确定功能的退出时间。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。

注意：

Citrix Virtual Apps and Desktops 的弃用和删除在其各自的[弃用](#)文章中介绍。

弃用和删除

下面的列表显示了已弃用或已删除的 Citrix DaaS 功能。

已弃用的项目不会立即删除。Citrix 继续支持这些项目，但会在将来的版本中将其删除。

在 Citrix DaaS 中，已删除的项目已被删除或不再受支持。粗体显示的日期表示最新更新。

项目	在发行版中宣布弃用	版本中已删除的功能	备选
支持将回写缓存配置为仅包含磁盘缓存而不包含内存缓存	2024 年 2 月		使用内存缓存大小配置选项并给出非零大小。

项目	在发行版中宣布弃用	版本中已删除的功能	备选
支持在按需配置功能之前创建的 Azure 目录（“旧版”目录）	2024 年 2 月		重新创建 Azure 旧版目录虚拟机。这些目录是按需配置的，有助于节省存储成本。
支持适用于 System Center Configuration Manager 的 Citrix Connector 3.1	2023 年 12 月		手动更新映像或应用程序。
支持在与创建目录的区域不同的区域中使用主映像	2023 年 12 月		使用 Azure 计算库将主映像复制到所需区域。
为 AWS 批量工作者提供支持	2023 年 11 月		使用直接磁盘上传和下载。请参阅 <a href="#">直接磁盘上传和下载</a> 。
支持在创建交付组时使用 <code>Leave user management to Citrix Cloud</code>	2023 年 9 月	2023 年 9 月	
支持在 AWS 环境中使用的 <code>AwsCaptureInstanceProperties</code>	2023 年 8 月		使用计算机配置文件。请参阅 <a href="#">使用计算机配置文件创建目录</a> 。
支持 VMware vSphere 6.7		2023 年 6 月	<a href="#">对 VMware vSphere 使用更高的版本</a> 。
<code>Schedule-ProvVMUpdate</code> PowerShell 命令	2023 年 4 月		使用 <code>Set-ProvVMUpdateTimeWindow</code> 命令。
<code>Request-ProvVMUpdate</code> PowerShell 命令	2023 年 4 月		使用带 <code>-StartsNow</code> 和 <code>-DurationInMinutes -1</code> 参数的 <code>Set-ProvVMUpdateTimeWindow</code> 命令。
<code>Cancel-ProvVMUpdate</code> PowerShell 命令	2023 年 4 月		使用 <code>Clear-ProvVMUpdateTimeWindow</code> 命令。

项目	在发行版中宣布弃用	版本中已删除的功能	备选
<a href="#">New-ProvScheme</a> 命令中使用的 <a href="#">DedicatedTenancy</a> 参数	2023 年 3 月		使用 <a href="#">TenancyType</a> 参数。
用于在 Azure 环境中创建 VM 的非托管磁盘	2022 年 6 月		
支持四个 AWS 特定命令： <a href="#">Revoke-HypSecurityGroupIngress</a> 、 <a href="#">Revoke-HypSecurityGroupEgress</a> 、 <a href="#">Grant-HypSecuritygroupegress</a> 和 <a href="#">Grant-HypSecurityGroupIngress</a>	2022 年 5 月		
在 Azure 环境中使用的 <a href="#">StorageAccountType</a> 参数	2022 年 4 月		使用 <a href="#">StorageType</a> 。
旧版控制台（基于 MMC 的控制台）	2021 年 7 月	2021 年 11 月	使用管理 > 完整配置可以访问所有配置和管理操作。
Azure 快速部署	2020 年 9 月		使用 <a href="#">快速部署</a> 。
能够导入 Citrix Provisioning 目标设备以在 Citrix Studio 中创建目录。	2020 年 8 月	2021 年 2 月	使用 Citrix Provisioning 导出设备向导可将 Citrix Provisioning VM 推送到 Delivery Controller/MCS 中，以便创建目录。请参阅 <a href="#">导出设备向导</a> 。

## 系统要求

March 5, 2024

### 简介

本文档中未涉及的组件（例如 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。

由于硬件产品的复杂性和不确定性，无法提供具体的用于交付桌面和应用程序的 VM 的大小建议。每个部署都有独特的需求。通常，虚拟机的大小是基于硬件而不是用户工作负载（RAM 除外；消耗更多内存的应用程序需要更多 RAM。）[Citrix Tech Zone](#) 包含有关 VDA 规模调整的最新指南。

#### 重要提示：

本文中提到的 VDA 版本受 Citrix 产品生命周期的约束。有关详细信息，请参阅 Citrix Web 站点上的[产品列表](#)。

有关在 Citrix DaaS 上使用 LTSR VDA 的更多信息，请参阅 [CTX205549](#)。

谨记：在 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）部署中，您无需安装或管理核心组件（Delivery Controller、站点数据库或者管理和监视控制台）。有关 Virtual Delivery Agent (VDA) 安装指南，请参阅：

- [安装 VDA](#)
- [使用命令行安装 VDA](#)。

## Cloud Connector

有关详细信息，请参阅 [Cloud Connector 技术详细信息](#)。

## Azure 环境中的 VDA

支持的操作系统：

- Windows 11 多会话
- Windows 11 单会话
- Windows 10 多会话
- Windows 10 单会话
- Windows Server 2022（至少需要 VDA 2106）
- Windows Server 2019
- Windows Server 2016

支持所有尚未达到生命周期终止的 VDA 与 Citrix DaaS 一起使用。对于 LTSR VDA，我们建议将其与最新的累积更新一起使用。有关 VDA 生命周期的更多信息，请参阅 [Citrix 产品矩阵](#)。

只有 VDA 1912（及更高版本的 CU）支持 Windows Server 2012 R2。

Windows Server 需要 [Microsoft RDS 许可](#)。

有关 Azure 虚拟桌面的信息，请参阅 Microsoft [文档](#)。

## 适用于单会话操作系统的 VDA

以下信息适用于最新的 VDA 版本。

支持的操作系统：

- Windows 11
- Windows 10
  - 有关版本支持，请参阅 [CTX224843](#)。该文章还包含指向与受支持的 Windows 版本有关的 Citrix 已知问题的链接。
  - Windows 10 不支持桌面组合重定向和旧图形模式。

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++ 2015-2019 可再发行软件包。
  - 如果计算机包含该运行时的早期版本（例如 2015-2017），Citrix 安装程序将对其进行升级。
  - 如果计算机包含的版本早于 2015，Citrix 将并行安装较新的版本。

Remote PC Access 使用此 VDA（您可将其安装在办公室物理 PC 上）。此 VDA 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，多媒体加速功能将不安装且无法运行。请勿在安装 Citrix 软件后从计算机中删除媒体基础。否则，用户将无法登录此计算机。在大多数受支持的 Windows 桌面操作系统版本上，已经安装了媒体基础支持，不能将其删除。但是，N 个版本不包括某些媒体相关技术。您可以从 Microsoft 或第三方获取该软件。

更多信息：

- 有关 Linux VDA 信息，请参阅 [Linux Virtual Delivery Agent](#) 产品文档。
- 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单会话 VDA。有关指导，请参阅 [服务器 VDI](#)。
- 有关在较旧的计算机上安装 VDA 的信息，请参阅 [早期操作系统](#)。
- 另请参阅 Azure 虚拟桌面环境中的 VDA。

## 适用于多会话操作系统的 **VDA**

以下信息适用于最新的 VDA 版本。

支持的操作系统：

- Windows Server 2022（至少需要 VDA 2106）
- Windows Server 2019 Standard Edition 和 Datacenter Edition
- Windows Server 2016 Standard Edition 和 Datacenter Edition
- Windows 11
- Windows 10 (64 位) 所有支持的版本

安装程序将自动部署以下要求：

- 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++ 2015-2019 可再发行软件包。
  - 如果计算机包含该运行时的早期版本（例如 2015-2017），Citrix 安装程序将对其进行升级。
  - 如果计算机包含的版本早于 2015，Citrix 将并行安装较新的版本。

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。这将触发重新启动操作。

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，多媒体加速功能将不安装且无法运行。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。但是，N 个版本不包括某些媒体相关技术。您可以从 Microsoft 或第三方获取该软件。

如果 VDA 上不存在媒体基础，这些多媒体功能将不起作用：

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

更多信息：

- 有关 Linux VDA 的信息，请参阅 [Linux Virtual Delivery Agent](#) 各文章。
- 有关在不再支持的 Windows 操作系统上安装 VDA 的信息，请参阅 [早期版本的操作系统](#)。
- 另请参阅 Azure 虚拟桌面环境中的 VDA。

## 主机/虚拟化资源

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。[CTX131239](#) 包含最新虚拟机管理程序版本信息，以及已知问题的链接。

- **Amazon Web Services (AWS)**

- 可以在支持的 Windows 服务器操作系统上预配应用程序和桌面。
- 不支持 Amazon Relational Database Service (RDS)。

有关详细信息，请参阅 [AWS 云环境](#)。

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

[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 [XenServer 虚拟化环境](#)。

- **Google** 云端平台

有关详细信息，请参阅 [Google Cloud 环境](#) 和 [Google Cloud 上的 Citrix DaaS 入门](#)。

- **Microsoft Azure Resource Manager**

有关详细信息，请参阅 [Microsoft Azure Resource Manager 云环境](#)。

- **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](#)。

- **AWS 上的 VMware 云**

[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 [Amazon Web Services \(AWS\) 上的 VMware 云](#)。

- **Azure VMware 解决方案 (AVS)**

[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 [Azure VMware 解决方案 \(AVS\) 集成](#)。

- **Google Cloud VMware Engine**

[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 [Google Cloud VMware Engine](#)。

- **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](#)。

注意：

不得在任何 Citrix DDC 或 StoreFront 服务器上安装 VDA 软件。VDA 必须是独立的系统。仅当开发概念验证或仅向管理员发布 Studio 管理员控制台时，才允许在单个 VM 上安装多个组件。在这种情况下，您必须确保非管理员用户无权访问 DDC/StoreFront 虚拟机。

## Active Directory 功能级别

支持以下 Active Directory 林和域功能级别：

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

有关 Active Directory 的详细信息，请参阅[加入了 Active Directory](#)。

## HDX 技术

有关特定的 HDX 功能支持和要求，请参阅 [HDX](#)。

## 通用打印服务器

通用打印服务器由客户端和服务组件组成。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 2019
- Windows Server 2016

要求：

- Microsoft .NET Framework 4.8（最低版本）
- Microsoft Visual C++ 2015-2022 可再发行软件包。
  - 如果计算机包含该运行时的早期版本（例如 2015-2017），Citrix 安装程序将对其进行升级。
  - 如果计算机包含的版本早于 2015，Citrix 将并行安装较新的版本。

对于多会话 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组件软件包。

有关详细信息，请参阅[预配打印机](#)。

### 服务连接性

有关 Internet 连接信息，请参阅[系统和连接要求](#)。该信息包括大多数 Citrix Cloud 服务常见的要求以及 [Citrix DaaS 特定的要求](#)。

### 其他

- 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)。安装了 [CitrixGroupPolicyManagement\\_x64.msi](#) 的计算机必须安装 Visual Studio 2015 运行时。有关详细信息，请参阅 Microsoft 文档。
- 本产品支持 PowerShell 版本 3 至 5。
- 对于可以安装在 Windows Server 上的产品组件和功能，除非特别注明，否则不支持 Server Core 和 Nano Server 安装。
- 有关部署中的资源限制的详细信息，请参阅[限制](#)。
- 有关支持的 StoreFront 版本，请参阅 [StoreFront 系统要求](#)。
- 有关全球化信息，请参阅 [CTX119253](#)。
- 有关 Citrix DaaS 使用的端口的信息，请参阅 [Citrix 技术使用的通信端口](#)。
- 有关使用“快速部署”管理界面时的要求的信息，请参阅[要求](#)。

### 限制

December 18, 2023

本文中的值指示单个 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）实例的限制。这些限制已经 Citrix 进行了广泛测试，建议使用这些限制以获得最佳的最终用户和管理员体验。这些是软限制，在技术上没有强制执行（每个资源位置的 VDA 总数除外）。当并发用户数超过 125,000 个时，Citrix 可以扩展并组合多个 Citrix DaaS 实例，以提供任意规模的统一体验。

本文中的信息将随时更新。请经常返回查看以获取更新。如果您当前有发布的限制无法满足的要求，请尽早联系您的 Citrix 代表寻求帮助。

### 配置限制

如果策略超出限制，Citrix 建议使用 [Workspace Environment Management 服务](#)或 [Active Directory 组策略对象 \(GPO\)](#)。

资源	限制
Active Directory 域	100
应用程序文件夹	1,000
应用程序组	250
应用程序	5,000
目录	2,000
交付组	2,000
主机连接	200
资源位置	100
“管理”控制台（完整配置）策略	200
标记	10,000
VDA	100,000

资源位置限制

下表列出了每个资源位置的限制。

如果您的要求超出这些限制，Citrix 建议使用其他资源位置。

资源	限制
VDA 总数（硬限制）	10,000
会话总数	25,000
Active Directory 域	1
主机连接	40

Citrix Cloud 连接器被分配到资源位置，并将工作负载链接到 Citrix DaaS。有关 Cloud Connector 限制的信息，请参阅 [Cloud Connector 的大小和规模注意事项](#)。

资源调配限制

下表中的配置限制是 Citrix 为单个公共提供商订阅推荐的最大配置限制。

您可能会达到公有云供应商设置的较低级别的配额限制。在此类情况下，请联系供应商以提高您的订阅配额。对于大型部署，Citrix 建议使用中心辐射模型，其中 VDA 分布在多个订阅和主机连接中。

有关详细信息，请参阅以下参考体系结构：

- [AWS 上的 Citrix DaaS](#)
- [Google Cloud 上的 Citrix 虚拟化](#)
- [Azure 上的 Citrix DaaS](#)

资源	限制
每个区域每个 Amazon Web Services 帐户的 VDA	1,500
每个 Google 云端平台项目的 VDA	3,000
每个区域每个 Microsoft Azure 订阅的 VDA	5,000

注意：

Citrix 建议使用这些限制。

使用限制

有关管理员角色以及这些角色之间的差异的信息，请参阅：

- [“管理” > “完整配置” 管理员](#)
- [Monitor \(Director\) 管理员](#)

资源	限制
并发监视 (Director) 完全权限管理员	40
并发监视 (Director) 技术支持管理员	200
并发监视 (Director) 会话管理员	50
并发管理（完整配置）云管理员	100
并发管理（完整配置）技术支持管理员	60
并发最终用户	125,000
发布给单个用户的资源	250
每分钟会话启动次数	3,000

- 监视器（Director 器）支持在单个租户（集线器）下聚合多达四个 Citrix DaaS 租户（分支）。
- 中心实例的技术支持管理员可以根据特定实例的委派管理配置，监视来自所有聚合实例（集线器和分支）的用户、计算机、端点和事务并对其进行故障排除。
- 每个 Citrix DaaS 实例的并发管理员数量与使用限制表相同。

限制变更日志

下表跟踪配置限制的修改：

日期	资源	说明
2023 年 11 月 22 日	Active Directory 域	上限从 85 提高到 100。
	目录	上限从 1000 提高到 2000。
	交付组	上限从 1000 提高到 2000。
	资源位置	上限从 85 提高到 100。
	资源位置 -> 会话总数	上限从 20000 提高到 25000。
2023 年 12 月 7 日	预配限制 -> 每个区域每个 Microsoft Azure 订阅的 VDA	上限从 2500 提高到 5000。

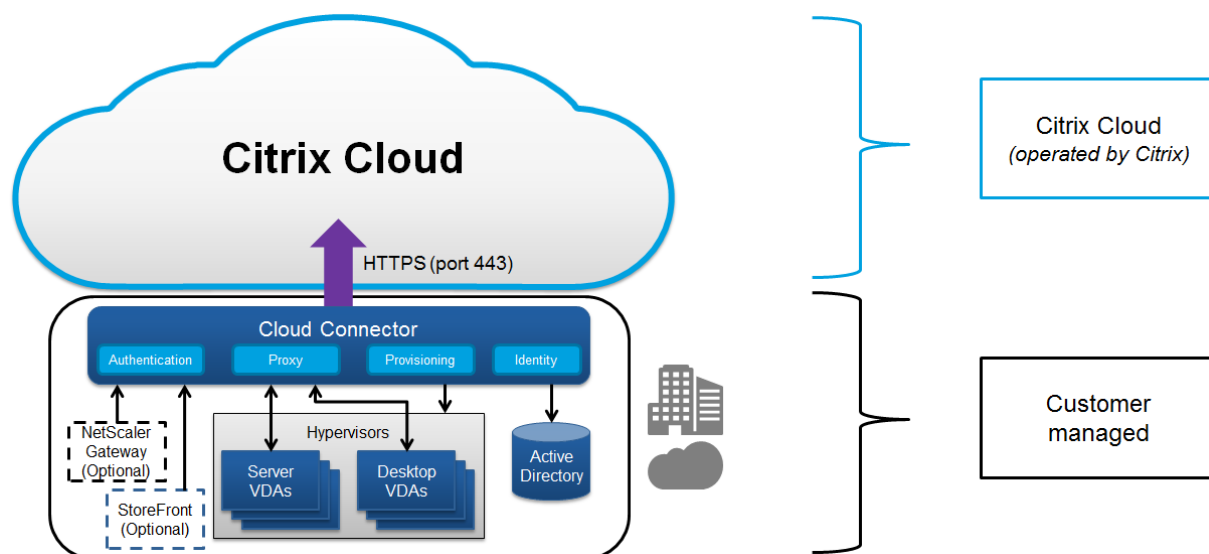
技术安全性概述

September 1, 2023

安全性概述

本文档适用于 Citrix Cloud 中托管的 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）。此信息包括 Citrix Virtual Apps Essentials 和 Citrix Virtual Desktops Essentials。

Citrix Cloud 管理 Citrix DaaS 环境的控制平面操作。控制面板包括 Delivery Controller、管理控制台、SQL 数据库、许可证服务器以及（可选）StoreFront 和 Citrix Gateway（以前称为 NetScaler Gateway）。托管应用程序和桌面的 Virtual Delivery Agent (VDA) 在客户选择的数据中心（云或本地）中仍处于客户的控制之下。这些组件使用名为 Citrix Cloud Connector 的代理连接到云服务。如果客户选择使用 Citrix Workspace，则同时可以选择使用 Citrix Gateway 服务来代替在其数据中心的运行 Citrix Gateway。下图说明了 Citrix DaaS 及其安全边界。



### 基于 **Citrix Cloud** 的合规性

截至 2021 年 1 月，尚未针对 Citrix SOC 2（类型 1 或 2）、ISO 27001、HIPAA 或其他云合规性要求评估 Citrix 托管 Azure 容量与各种 Citrix DaaS 版本以及 Workspace Premium Plus 的使用情况。请访问 [Citrix Trust Center](#) 了解有关 Citrix Cloud 认证的详细信息，并经常返回查看以获取更新。

### 数据流

Citrix DaaS 不托管 VDA，因此，预配所需的客户应用程序数据和映像将始终在客户设置中托管。控制平面有权访问元数据，例如用户名、计算机名称和应用程序快捷方式，但限制从控制平面访问客户的知识产权。

云与客户本地之间的数据流动使用安全的 TLS 连接通过端口 443 进行。

### 数据隔离

Citrix DaaS 仅存储代理和监视客户应用程序和桌面所需的元数据。敏感信息（包括映像、用户配置文件和其他应用程序数据）仍保留在客户本地，或者保留在其公有云供应商的订阅中。

### 服务版本

Citrix DaaS 的功能因版本而异。例如，Citrix Virtual Apps Essentials 仅支持 Citrix Gateway 服务和 Citrix Workspace。请查阅产品文档，了解与支持的功能有关的更多信息。

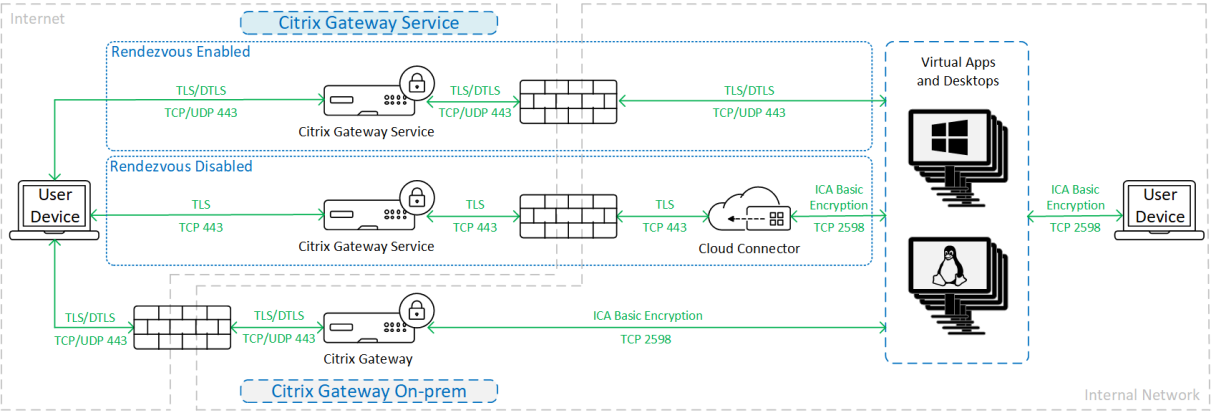
ICA 安全

Citrix DaaS 提供了多种选项来保护传输中的 ICA 流量。下面是可用的选项：

- 基本加密：默认设置。
- **SecureICA**：允许使用 RC5（128 位）加密对会话数据进行加密。
- **VDA TLS/DTL**：允许使用使用 TLS/DTL 的网络级加密。
- 汇聚协议：仅在使用 Citrix Gateway 服务时可用。使用汇聚协议时，ICA 会话使用 TLS/DTL 进行端到端加密。

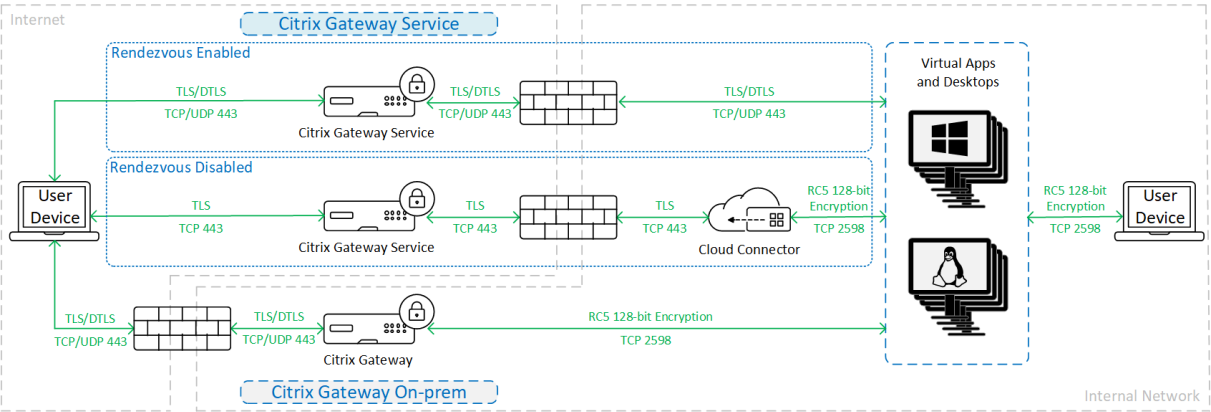
基本加密

使用基本加密时，将对流量进行加密，如下图所示。



SecureICA

使用 SecureICA 时，流量将被加密，如下图所示。



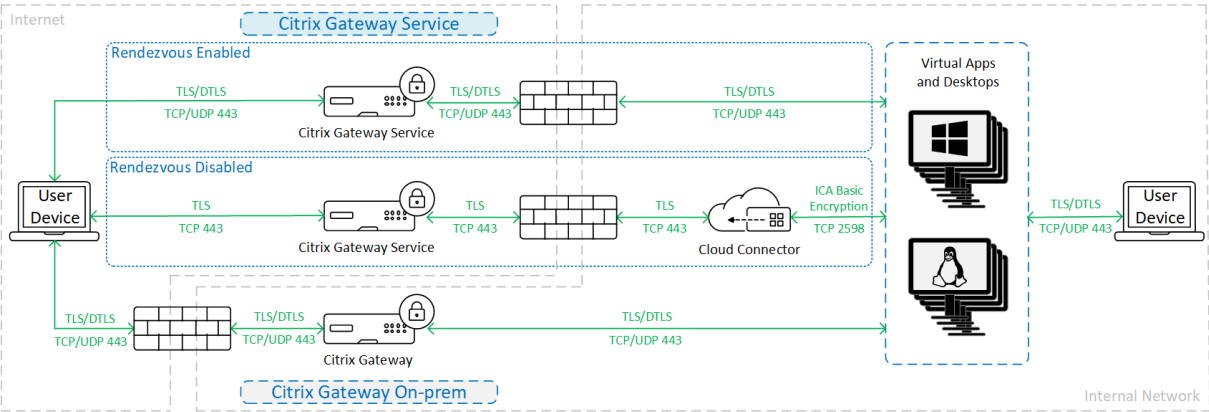
注意：

使用适用于 HTML5 的 Workspace 应用程序时，不支持 SecureICA。



VDA TLS/DTL

使用 VDA TLS/DTL 加密时，流量将被加密，如下图所示。



注意：

在没有汇聚的情况下使用网关服务时，VDA 与 Cloud Connector 之间的流量不会进行 TLS 加密，因为 Cloud Connector 不支持使用网络级加密连接到 VDA。

更多资源

有关 ICA 安全选项以及如何配置这些选项的详细信息，请参阅：

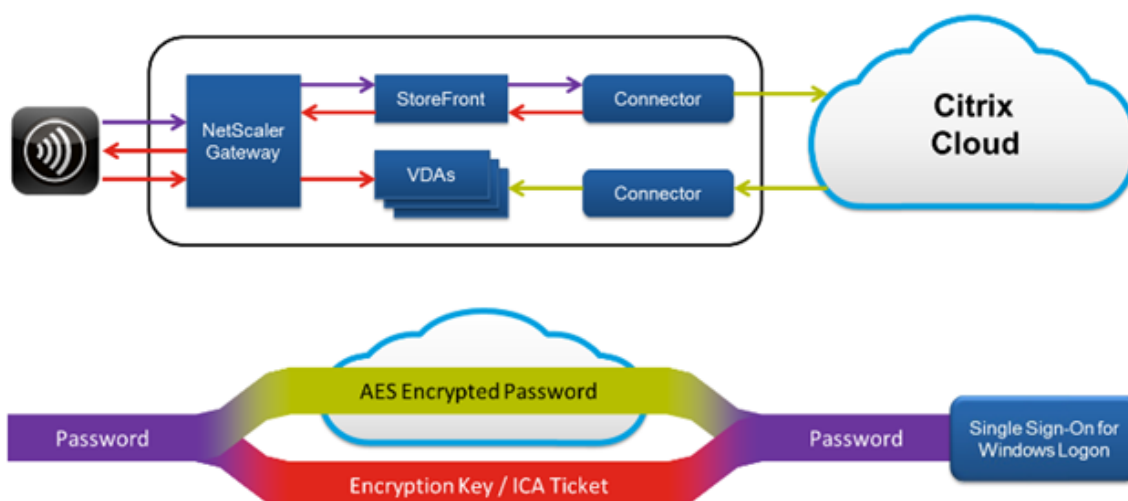
- SecureICA: [安全策略设置](#)
- VDA TLS/DTLS: [传输层安全性](#)
- 汇聚协议: [汇聚协议](#)

凭据处理

Citrix DaaS 处理四种类型的凭据：

- 用户凭据：使用客户管理的 StoreFront 时，Cloud Connector 使用使用 AES-256 加密方法以及为每次启动生成的随机一次性密钥加密用户凭据。此密钥永远不会传递到云，并且仅返回到 Citrix Workspace 应用程序。Citrix Workspace 应用程序之后会将此密钥传递到 VDA，以在会话启动过程中解密用户密码，从而实现单点登录体验。下图显示了该流程。

默认情况下，不会跨不可信域边界转发用户凭证。如果将 VDA 和 StoreFront 安装在一个域中，而另一个域中的用户尝试连接到 VDA，则除非在两个域之间建立信任，否则登录尝试会失败。您可以使用 DaaS PowerShell SDK 禁用此行为并允许在不可信域之间转发证书。有关详细信息，请参阅 [Set-Brokersite](#)。



- 管理员凭据：管理员针对 Citrix Cloud 进行身份验证。身份验证将生成一个一次性签名的 JSON Web 令牌 (JWT)，管理员通过该令牌将能够访问 Citrix DaaS。
- 虚拟机管理程序密码：需要密码进行身份验证的本地虚拟机管理程序具有管理员生成的、在云中的 SQL 数据库中直接存储并加密的密码。Citrix 负责管理对等密钥，以确保虚拟机管理程序仅对通过了身份验证的进程可用。
- Active Directory (AD) 凭据：Machine Creation Services 使用 Cloud Connector 在客户的 AD 中创建计算机帐户。由于 Cloud Connector 的计算机帐户仅对 AD 具有读取访问权限，因此，每次执行计算机创建或删除操作时，系统都会提示管理员输入凭据。这些凭据仅存储在内存中，并且仅用于单个预配事件。

## 部署注意事项

Citrix 建议用户查阅已发布的最佳做法文档，了解在其环境中部署 Citrix Gateway 应用程序和 VDA 的相关信息。

## Citrix Cloud Connector 网络访问要求

Citrix Cloud Connector 仅需要传输至 Internet 的端口 443 出站流量，并且可以托管在 HTTP 代理后面。

- 在 Citrix Cloud 中为 HTTPS 使用的通信为 TLS。（请参阅弃用 TLS 版本。）
- 在内部网络中，Cloud Connector 需要访问以下组件才能使用 Citrix DaaS：
  - VDA：端口 80，入站和出站，以及 1494 和 2598 入站（如果使用 Citrix Gateway 服务）
  - StoreFront 服务器：端口 80，入站。
  - Citrix Gateway，如果配置为 STA：端口 80，入站。
  - Active Directory 域控制器
  - 虚拟机管理程序：仅限出站。有关特定端口，请参阅[Citrix 技术使用的通信端口](#)。

VDA 与 Cloud Connector 之间的流量使用 Kerberos 消息级安全性进行加密。

## 客户管理的 **StoreFront**

客户管理的 StoreFront 为部署体系结构提供更多安全配置选项以及更大的灵活性，包括本地维护用户凭据的功能。StoreFront 可以托管在 Citrix Gateway 后面，以提供安全的远程访问、执行多重身份验证以及添加其他安全功能。

## **Citrix Gateway** 服务

如果使用 Citrix Gateway 服务，则不需要再在客户数据中心中部署 Citrix Gateway。

有关详细信息，请参阅 [Citrix Gateway 服务](#)。

Cloud Connector 与 Citrix Cloud 之间的所有 TLS 连接都从 Cloud Connector 启动到 Citrix Cloud。不需要任何入站防火墙端口映射。

## **XML** 信任

此设置在“完整配置”>“设置”>“启用 **XML** 信任”中可用，默认情况下处于禁用状态。或者，你可以使用 Citrix DaaS Remote PowerShell SDK 来管理 XML 信任。

XML 信任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 信任将允许用户成功进行身份验证，然后启动应用程序。Cloud Connector 信任从 StoreFront 发送的凭据。仅当您已保护 Citrix Cloud Connector 与 StoreFront 之间的通信（使用防火墙、IPsec 或其他安全建议）时，才启用 XML 信任。

默认情况下，禁用此设置。

使用 Citrix DaaS 远程 PowerShell SDK 管理 XML 信任。

- 要检查 XML 信任的当前值，请运行 `Get-BrokerSite` 并检查 `TrustRequestsSentToTheXMLServicePort` 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`

## 强制传输 **HTTPS** 或 **HTTP** 流量

要通过 XML Service 强制传输 HTTPS 或 HTTP 流量，请在每个 Cloud Connector 上配置以下注册表值集之一。

配置设置后，在每个 Cloud Connector 上重新启动 Remote Broker Provider Service。

在 `HKLM\Software\Citrix\DesktopServer\` 中：

- 要强制传输 HTTPS（忽略 HTTP）流量，请执行以下操作：将 `XmlServicesEnableSsl` 设置为 1，将 `XmlServicesEnableNonSsl` 设置为 0。
- 要强制传输 HTTP（忽略 HTTPS）流量，请执行以下操作：将 `XmlServicesEnableNonSsl` 设置为 1，将 `XmlServicesEnableSsl` 设置为 0。

弃用 **TLS** 版本

为了提高 Citrix DaaS 的安全性，Citrix 已自 2019 年 3 月 15 日起开始阻止通过传输层安全性 (TLS) 1.0 和 1.1 进行的任何通信。

从 Citrix Cloud Connector 到 Citrix Cloud 服务的所有连接都需要 TLS 1.2。

为确保从用户设备成功连接到 Citrix Workspace，已安装的 Citrix Receiver 版本必须等于或高于以下版本。

Receiver	版本
Windows	4.2.1000
Mac	12.0
Linux	13.2
Android	3.7
iOS	7.0
Chrome/HTML5	最新版本（浏览器必须支持 TLS 1.2）

要升级到最新的 Citrix Receiver 版本，请转到 <https://www.citrix.com/products/receiver/>。

或者，升级到使用 TLS 1.2 的 [Citrix Workspace 应用程序](#)。要下载 Citrix Workspace 应用程序，请转到 <https://www.citrix.com/downloads/workspace-app/>。

如果您必须继续使用 TLS 1.0 或 1.1（例如，使用基于较早版本的 Receiver for Linux 的瘦客户端），请在您的资源位置中安装 StoreFront。然后，请让所有 Citrix Receiver 都指向它。

更多信息

以下资源包含安全信息：

- [Citrix 托管 Azure 的技术安全性概述](#)。
- [Citrix 安全站点](#)。

- [安全性和合规性信息](#)：安全性和合规性中心包含安全公告，可帮助您随时了解最新消息。该中心还包含关于标准和认证的文档，这些标准和认证对维护安全、合规的 IT 环境非常重要。
- [《适用于 Citrix Cloud 平台的安全部署指南》](#)：本指南概述了使用 Citrix Cloud 时的安全性最佳做法并介绍了 Citrix Cloud 收集和管理的信息。本指南还包含指向有关 Citrix Cloud Connector 的综合性信息的链接。
- [系统和连接要求](#)。
- [安全注意事项和最佳做法](#)。
- [智能卡](#)。
- [传输层安全性 \(TLS\)](#)。

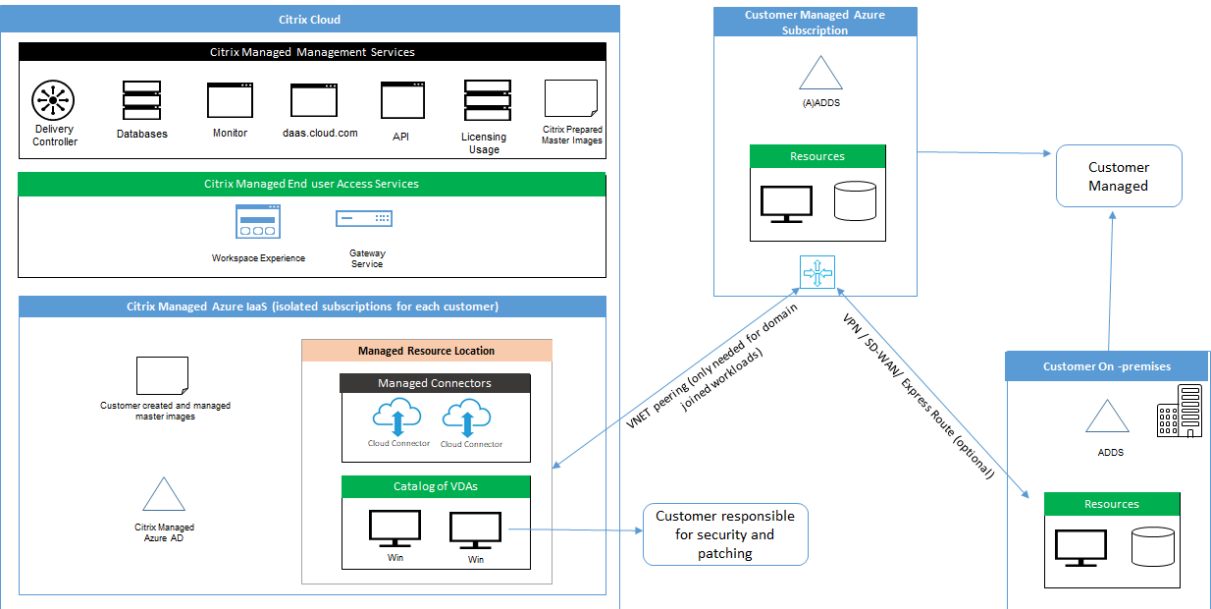
注意：

本文档的目的是向读者提供 Citrix Cloud 的安全功能的简介和概述，以及针对确保 Citrix Cloud 安全来定义 Citrix 与客户之间的职责划分。其目的不是用作 Citrix Cloud 或其任何组件或服务的配置和管理指导手册。

## Citrix 托管 Azure 的技术安全性概述

April 11, 2023

下图显示了使用 Citrix 托管 Azure 的 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）部署中的组件。此示例使用 vNet 对等连接。



使用 Citrix 托管 Azure，交付桌面和应用程序的客户的 Virtual Delivery Agent (VDA) 以及 Citrix Cloud Connector 将部署到 Citrix 托管的 Azure 订阅和租户中。

### 基于 **Citrix Cloud** 的合规性

截至 2021 年 1 月，尚未针对 Citrix SOC 2（类型 1 或 2）、ISO 27001、HIPAA 或其他云合规性要求评估 Citrix 托管 Azure 容量与各种 Citrix DaaS 版本以及 Workspace Premium Plus 的使用情况。请访问 [Citrix Trust Center](#) 了解有关 Citrix Cloud 认证的详细信息，并经常返回查看以获取更新。

### **Citrix** 的职责

#### 适用于未加入域的目录的 **Citrix Cloud Connector**

使用 Citrix 托管 Azure 订阅时，Citrix DaaS 在每个资源位置中至少部署两个 Cloud Connector。如果某些目录与同一客户的其他目录位于同一个区域中，这些目录可能会共享资源位置。

Citrix 负责对未加入域的目录 Cloud Connector 执行以下安全操作：

- 应用操作系统更新和安全补丁
- 安装和维护防病毒软件
- 应用 Cloud Connector 软件更新

客户无权访问 Cloud Connector。因此，Citrix 对未加入域的目录 Cloud Connector 的性能负全部责任。

### **Azure** 订阅和 **Azure Active Directory**

Citrix 负责为客户创建的 Azure 订阅和 Azure Active Directory (AAD) 的安全性。Citrix 确保租户隔离，因此，每个客户都有自己的 Azure 订阅和 AAD，并防止不同租户之间的交谈。Citrix 还限制 AAD 仅访问 Citrix DaaS 和 Citrix 运营人员。Citrix 对每个客户的 Azure 订阅的访问权限都将被审核。

使用未加入域的目录的客户可以使用 Citrix 托管的 AAD 作为 Citrix Workspace 的身份验证方式。对于这些客户，Citrix 在 Citrix 托管的 AAD 中创建有限权限的用户帐户。但是，客户的用户和管理员都无法对 Citrix 托管的 AAD 执行任何操作。如果这些客户选择改为使用自己的 AAD，他们对其安全负全部责任。

### 虚拟网络和基础结构

在客户的 Citrix 托管 Azure 订阅中，Citrix 创建了用于隔离资源位置的虚拟网络。在这些网络中，Citrix 除了存储帐户、密钥保管库和其他 Azure 资源之外，还为 VDA、Cloud Connector 和映像构建器计算机创建虚拟机。Citrix 与 Microsoft 合作，负责包括虚拟网络防火墙在内的虚拟网络的安全。

Citrix 确保将默认 Azure 防火墙策略（网络安全组）配置为限制对 vNet 对等连接和 SD-WAN 连接中的网络接口的访问。这通常可以控制到 VDA 和 Cloud Connector 的传入流量。有关详细信息，请参阅：

- Azure vNet 对等连接的防火墙策略
- SD-WAN 连接的防火墙策略

客户无法更改此默认防火墙策略，但可以在 Citrix 创建的 VDA 计算机上部署额外的防火墙规则；例如，为了部分限制出站流量。在 Citrix 创建的 VDA 计算机上安装虚拟专用网络客户端或其他能够绕过防火墙规则的软件的客户应对可能产生的任何安全风险负责。

使用 Citrix DaaS 中的映像构建器创建和自定义新计算机映像时，端口 3389-3390 将在 Citrix 托管的 VNet 中暂时打开，以便客户可以 RDP 到包含新计算机映像的计算机以对其进行自定义。

### 使用 **Azure vNet** 对等连接时的 **Citrix** 职责

为了使 Citrix DaaS 中的 VDA 与本地域控制器、文件共享或其他 Intranet 资源联系，Citrix DaaS 提供了 VNet 对等互连工作流作为连接选项。客户的 Citrix 托管虚拟网络与客户管理的 Azure 虚拟网络对等互连。客户管理的虚拟网络可以使用客户选择的云到本地连接解决方案（例如 Azure ExpressRoute 或 IPsec 通道）实现与客户的本地资源的连接。

Citrix 对 VNet 对等互连的责任仅限于支持工作流程和相关 Azure 资源配置，以便在 Citrix 与客户管理的 VNet 之间建立对等互连关系。

**Azure vNet** 对等连接的防火墙策略 Citrix 为使用 VNet 对等连接的入站和出站流量打开或关闭以下端口。

### 使用未加入域的计算机的 **Citrix** 托管 **VNet**

- 入站规则
  - 允许端口 80、443、1494 和 2598 从 VDA 到 Cloud Connector 的入站，以及从 Cloud Connector 到 VDA 的入站。
  - 允许端口 49152-65535 从监视器重影功能使用的 IP 范围入站到 VDA。请参阅 [Citrix 技术使用的通信端口](#)。
  - 拒绝所有其他入站。这包括从 VDA 到 VDA 的 VNET 内流量，以及 VDA 到 Cloud Connector 的 VNET 内流量。
- 出站规则
  - 允许所有流量出站。

### 使用加入域的计算机的 **Citrix** 托管 **VNet**

- 入站规则：
  - 允许端口 80、443、1494 和 2598 从 VDA 到 Cloud Connector 的入站，以及从 Cloud Connector 到 VDA 的入站。
  - 允许端口 49152-65535 从监视器重影功能使用的 IP 范围入站到 VDA。请参阅 [Citrix 技术使用的通信端口](#)。



- 拒绝所有其他入站。这包括从 VDA 到 VDA 的 VNET 内流量，以及 VDA 到 Cloud Connector 的 VNET 内流量。
- 出站规则
  - 允许所有流量出站。

#### 具有加入域的计算机的客户管理的 **VNet**

- 客户有责任正确配置其 VNet。这包括打开以下端口以加入域。
- 入站规则：
  - 允许从客户端 IP 中的 443、1494、2598 入站以进行内部启动。
  - 允许从 Citrix VNet 中的 53、88、123、135-139、389、445、636 入站（客户指定的 IP 范围）。
  - 允许使用代理配置打开的端口上的入站。
  - 客户创建的其他规则。
- 出站规则：
  - 允许在 443、1494、2598 出站到 Citrix VNet（客户指定的 IP 范围）进行内部启动。
  - 客户创建的其他规则。

#### 使用 **SD-WAN** 连接时的 **Citrix** 职责

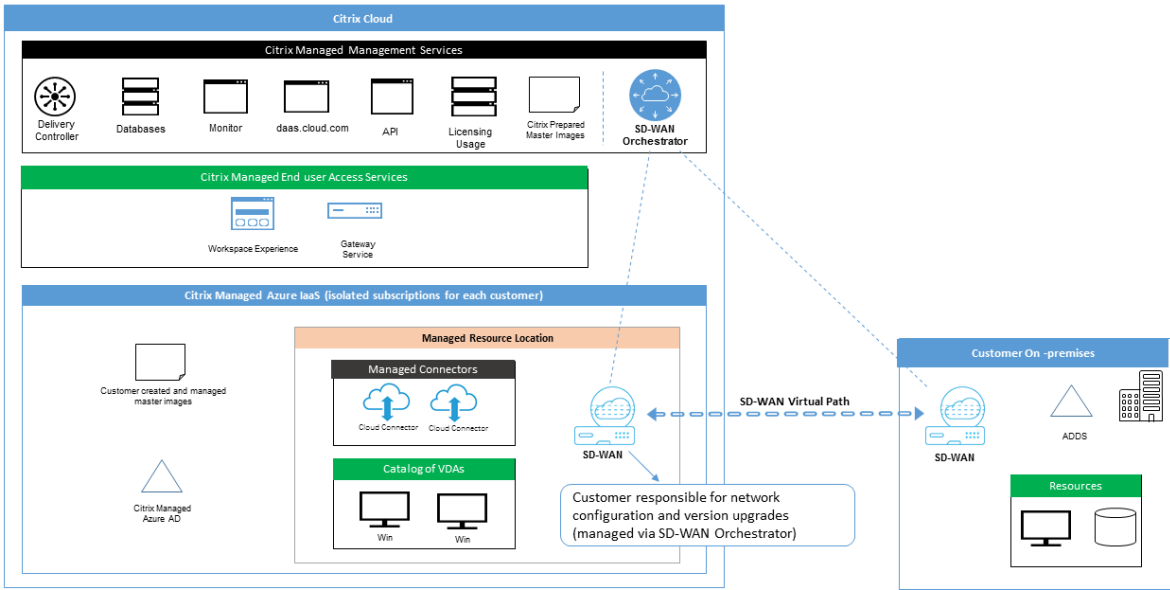
Citrix 支持一种完全自动部署虚拟 Citrix SD-WAN 实例的方式，以启用 Citrix DaaS 与本地资源之间的连接。与 vNet 对等互连相比，Citrix SD-WAN 连接有多项优势，包括：

VDA 到数据中心和 VDA 到分支机构 (ICA) 连接的高可靠性和安全性。

- 具有先进的 QoS 功能和 VoIP 优化，为办公室工作人员提供最佳终端用户体验。
- 内置功能，可以检查、确定优先级和报告 Citrix HDX 网络流量和其他应用程序的使用情况。

Citrix 要求希望利用 Citrix DaaS 的 SD-WAN 连接的客户使用 SD-WAN Orchestrator 来管理其 Citrix SD-WAN 网络。

下图显示了使用 Citrix 托管 Azure 订阅和 SD-WAN 连接的 Citrix DaaS 部署中添加的组件。



适用于 Citrix DaaS 的 Citrix SD-WAN 部署与 Citrix SD-WAN 的标准 Azure 部署配置类似。有关详细信息，请参阅在 [Azure 上部署 Citrix SD-WAN Standard Edition 实例](#)。在高可用性配置中，带有 Azure 负载均衡器的 SD-WAN 实例的活动/备用对作为包含 VDA 和 Cloud Connector 的子网与 Internet 之间的网关进行部署。在非高可用性配置中，只有一个 SD-WAN 实例作为网关部署。虚拟 SD-WAN 设备的网络接口是从拆分为两个子网的单独小地址范围中分配的地址。

配置 SD-WAN 连接时，Citrix 对上述托管桌面的网络连接配置进行了一些更改。特别是，来自 VNet 的所有传出流量（包括到 Internet 目标位置的流量）都是通过云 SD-WAN 实例路由的。SD-WAN 实例还配置为 Citrix 托管的 VNet 的 DNS 服务器。

对虚拟 SD-WAN 实例的管理访问权限需要管理员登录名和密码。SD-WAN 的每个实例都分配了一个独特的随机安全密码，可供 SD-WAN 管理员通过 SD-WAN Orchestrator UI、虚拟设备管理 UI 和 CLI 进行远程登录和故障排除。

与其他租户特定的资源一样，部署在特定客户 VNet 中的虚拟 SD-WAN 实例与所有其他 VNet 完全隔离。

当客户启用 Citrix SD-WAN 连接时，Citrix 会自动执行与 Citrix DaaS 一起使用的虚拟 SD-WAN 实例的初始部署，维护基础 Azure 资源（虚拟机、负载均衡器等），为虚拟 SD-WAN 实例的初始配置提供安全高效的即开即用默认设置，并通过 SD-WAN Orchestrator 启用持续维护和故障排除。Citrix 还采取合理的措施来执行 SD-WAN 网络配置的自动验证、检查已知的安全风险并通过 SD-WAN Orchestrator 显示相应的警报。

**SD-WAN 连接的防火墙策略** Citrix 使用 Azure 防火墙策略（网络安全组）和公用 IP 地址分配来限制对虚拟 SD-WAN 设备的网络接口的访问：

- 只有 WAN 和管理接口分配了公用 IP 地址，并允许与 Internet 建立出站连接。
- 作为 Citrix 托管的 VNet 的网关的局域网接口只允许与同一 VNet 上的虚拟机交换网络流量。

- WAN 接口将入站流量限制到 UDP 端口 4980 (Citrix SD-WAN 用于虚拟路径连接)，并拒绝向 VNet 传输出站流量。
- 管理端口允许传输到端口 443 (HTTPS) 和 22 (SSH) 的入站流量。
- 高可用性接口仅允许相互交换控制流量。

### 基础结构的访问权限

Citrix 可以访问客户的 Citrix 托管基础结构 (Cloud Connector) 来执行某些管理任务，例如收集日志 (包括 Windows 事件查看器) 和重新启动服务，而无需通知客户。Citrix 负责安全可靠地执行这些任务，对客户产生的影响最小。Citrix 还负责确保安全可靠地检索、传输和处理任何日志文件。无法以这种方式访问客户 VDA。

### 未加入域的目录的备份

Citrix 不负责执行未加入域的目录的备份。

### 计算机映像的备份

Citrix 负责备份上载到 Citrix DaaS 的任何计算机映像，包括使用映像构建器创建的映像。Citrix 为这些映像使用本地冗余存储。

### 未加入域的目录的堡垒

如有必要，Citrix 运营人员可以创建堡垒来访问客户的 Citrix 托管 Azure 订阅，以便诊断和修复客户问题，这可能是在客户意识到问题之前完成的。Citrix 不需要客户同意即可创建堡垒。Citrix 创建堡垒时，Citrix 会为堡垒创建一个强大的随机生成的密码，并限制 RDP 对 Citrix NAT IP 地址的访问。不再需要堡垒时，Citrix 将处置该堡垒，密码不再有效。该堡垒 (及其随附的 RDP 访问规则) 将在操作完成时处置。Citrix 只能通过堡垒访问客户的未加入域的 Cloud Connector。Citrix 没有用于登录未加入域的 VDA 或已加入域的 Cloud Connector 和 VDA 的密码。

### 使用故障排除工具时的防火墙策略

当客户请求创建堡垒计算机进行故障排除时，将对 Citrix 托管的 VNet 进行以下安全组修改：

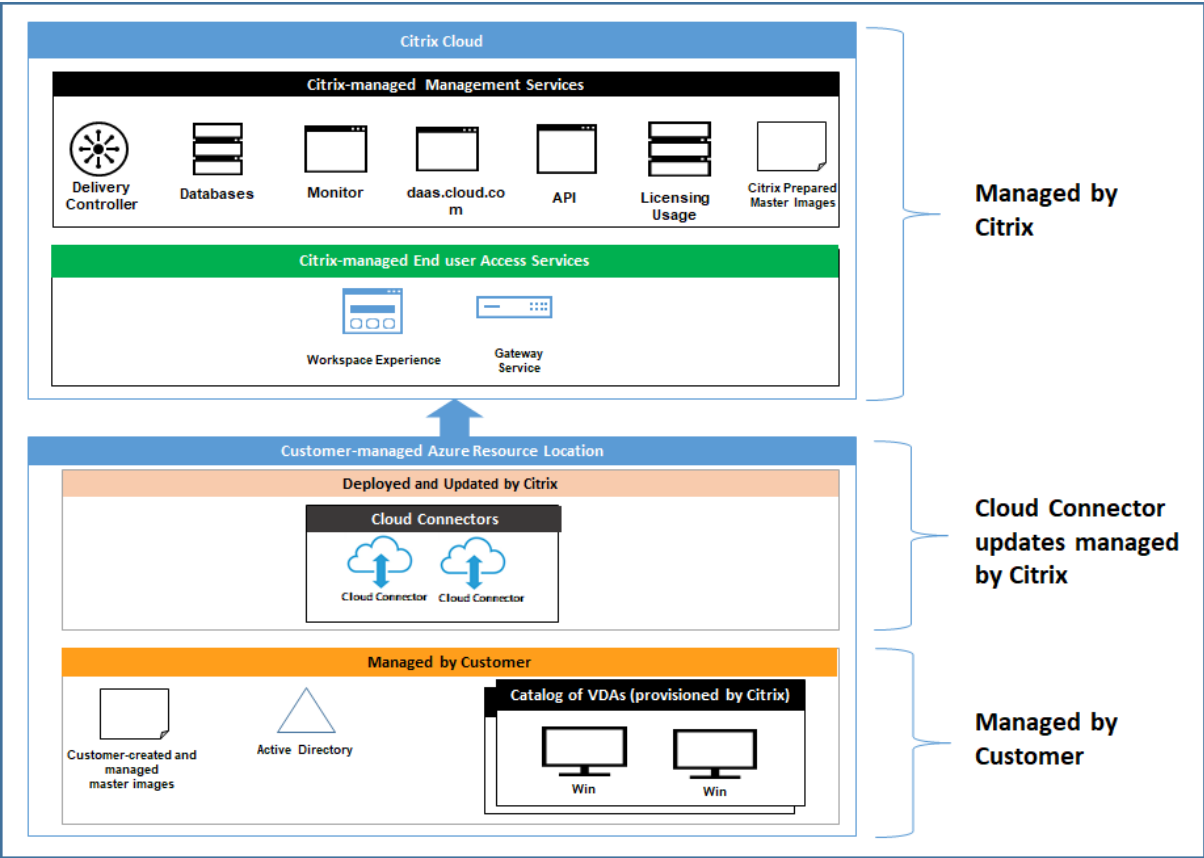
- 暂时允许从客户指定的 IP 范围到堡垒的 3389 入站。
- 暂时允许从堡垒 IP 地址到 VNet (VDA 和 Cloud Connector) 中的任何地址的 3389 入站。
- 继续阻止 Cloud Connector、VDA 和其他 VDA 之间的 RDP 访问。

当客户启用 RDP 访问以进行故障排除时，将对 Citrix 托管的 VNet 进行以下安全组修改：

- 暂时允许从客户指定的 IP 范围到 VNet (VDA 和 Cloud Connector) 中的任何地址的 3389 入站。
- 继续阻止 Cloud Connector、VDA 和其他 VDA 之间的 RDP 访问。

客户管理的订阅

对于客户管理的订阅，Citrix 在部署 Azure 资源期间遵守上述职责。部署之后，上述所有内容都属于客户的职责，因为客户是 Azure 订阅的所有者。



客户的职责

**VDA** 和计算机映像

客户负责 VDA 计算机上安装的软件的所有方面，包括：

- 操作系统更新和安全补丁
- 防病毒软件和反恶意软件
- VDA 软件更新和安全补丁
- 其他软件防火墙规则（尤其是出站流量）
- 按照 Citrix [安全注意事项和最佳做法](#) 进行操作

Citrix 提供了一个准备好的映像，该映像目的是作为起点。客户可以将此映像用于概念证明或演示目的，或者作为构建自己的计算机映像的基础。Citrix 不保证这一准备好的映像的安全性。Citrix 将尝试使准备好的映像上的操作系统和 VDA 软件保持最新状态，并将这些映像上启用 Windows Defender。

### 使用 **vNet** 对等互连时客户的职责

客户必须打开在具有加入域的计算机的客户管理的 VNet 中指定的所有端口。

配置 VNet 对等互连后，客户负责自己的虚拟网络及其与本地资源的连接的安全。客户还负责来自 Citrix 托管的对等互连虚拟网络的传入流量的安全。Citrix 不采取任何措施来阻止从 Citrix 托管的虚拟网络传输到客户的本地资源的流量。

客户可以通过以下选项限制传入流量：

- 为 Citrix 托管的虚拟网络提供一个 IP 块，该 IP 块不在客户的本地网络或客户管理的已连接虚拟网络中的其他地方使用。这对于 vNet 对等互连是必需的。
- 在客户的虚拟网络和本地网络中添加 Azure 网络安全组和防火墙，以阻止或限制来自 Citrix 托管的 IP 块的流量。
- 针对 Citrix 托管的 IP 块，在客户的虚拟网络和本地网络中部署诸如入侵防御系统、软件防火墙和行为分析引擎等措施。

### 使用 **SD-WAN** 连接时客户的职责

配置 SD-WAN 连接后，客户可以完全灵活地根据其网络要求配置与 Citrix DaaS 一起使用的虚拟 SD-WAN 实例，但为确保在 Citrix 托管的 VNet 中正确运行 SD-WAN 所需的一些因素除外。客户的职责包括：

- 设计和配置路由和防火墙规则，包括 DNS 和 Internet 流量突破规则。
- 维护 SD-WAN 网络配置。
- 监视网络的运行状态。
- 及时部署 Citrix SD-WAN 软件更新或安全修复。由于客户网络上的所有 Citrix SD-WAN 实例都必须运行同一版本的 SD-WAN 软件，因此，对 Citrix DaaS SD-WAN 实例的更新后的软件版本的部署需要由客户根据其网络维护计划和限制条件来管理。

SD-WAN 路由和防火墙规则配置不正确，或者 SD-WAN 管理密码管理不当，可能会对 Citrix DaaS 中的虚拟资源以及通过 Citrix SD-WAN 虚拟路径访问的本地资源造成安全风险。另一个可能的安全风险来自于没有将 Citrix SD-WAN 软件更新到最新的可用修补程序版本。虽然 SD-WAN Orchestrator 和其他 Citrix Cloud 服务提供了应对此类风险的手段，但客户最终负责确保虚拟 SD-WAN 实例配置得当。

### 代理

客户可以选择是否使用代理传输来自 VDA 的出站流量。如果使用代理，客户应负责：

- 在 VDA 计算机映像上配置代理设置，或者如果 VDA 已加入域，则使用 Active Directory 组策略。
- 代理的维护和安全。

不允许代理与 Citrix Cloud Connector 或其他 Citrix 托管的基础结构一起使用。

### 目录恢复能力

Citrix 提供了三种类型的目录，具有不同的恢复能力级别：

- **静态**：每个用户都分配给单个 VDA。此目录类型不提供高可用性。如果用户的 VDA 关闭，则必须将其放置在新的 VDA 上才能恢复。Azure 为单实例 VM 提供 99.5% 的 SLA。客户仍然可以备份用户配置文件，但是对 VDA 所做的任何自定义（例如安装程序或配置 Windows）都将丢失。
- **随机**：启动时，每个用户都随机分配给服务器 VDA。此目录类型通过冗余提供高可用性。如果 VDA 关闭，则不会丢失任何信息，因为用户的配置文件位于其他位置。
- **Windows 10 多会话**：此目录类型的运行方式与随机类型相同，但使用 Windows 10 工作站 VDA 而非服务器 VDA。

### 已加入域的目录的备份

如果客户使用带 VNet 对等互连的已加入域的目录，则客户负责备份其用户配置文件。Citrix 建议客户配置本地文件共享并在 Active Directory 或 VDA 上设置策略，以便从这些文件共享中提取用户配置文件。客户负责这些文件共享的备份和可用性。

### 灾难恢复

如果 Azure 数据丢失，Citrix 将尽可能多地恢复 Citrix 托管的 Azure 订阅中的资源。Citrix 将尝试恢复 Cloud Connector 和 VDA。如果 Citrix 无法成功恢复这些项目，则客户应负责创建新目录。Citrix 假定计算机映像已备份，客户已备份其用户配置文件，从而允许重新构建目录。

如果丢失整个 Azure 区域，客户应负责在新区域中重新构建客户管理的虚拟网络，并在 Citrix DaaS 中创建新的 VNet 对等互连或新的 SD-WAN 实例。

## Citrix 和客户共享的职责

### 适用于已加入域的目录的 **Citrix Cloud Connector**

Citrix DaaS 在每个资源位置中至少部署两个 Cloud Connector。如果某些目录与同一客户的其他目录位于同一区域、VNet 对等互连和域中，这些目录可能会共享资源位置。Citrix 将客户的已加入域的 Cloud Connector 配置为映像上的以下默认安全设置：

- 操作系统更新和安全补丁
- 防病毒软件
- Cloud Connector 软件更新

客户通常无权访问 Cloud Connector。但是，他们可以通过执行目录故障排除步骤和使用域凭据登录来获取访问权限。客户对通过堡垒登录时所做的任何更改负责。

客户还可以通过 Active Directory 组策略控制加入域的 Cloud Connector。客户有责任确保适用于 Cloud Connector 的组策略安全且合理。例如，如果客户选择使用组策略禁用操作系统更新，客户将负责在 Cloud Connector 上执行操作系统更新。客户还可以选择使用组策略来实施比 Cloud Connector 默认设置更严格的安全性，例如通过安装不同的防病毒软件。一般来说，Citrix 建议客户将 Cloud Connector 放置在自己的 Active Directory 组织单位中，而不配置任何策略，因为这将确保 Citrix 使用的默认值可以毫无问题地应用。

## 故障排除

如果客户遇到 Citrix DaaS 中出现目录问题，可以选择两种故障排除方案：使用堡垒和启用 RDP 访问。这两种方案都会给客户带来安全风险。在使用这些方案之前，客户必须了解此风险并同意承担此风险。

Citrix 负责打开和关闭必要的端口以执行故障排除操作，并限制在这些操作期间可以访问的计算机。

通过堡垒或 RDP 访问，执行操作的活动用户将负责所访问的计算机的安全。如果客户通过 RDP 访问 VDA 或 Cloud Connector 但意外感染了病毒，则由客户负责。如果 Citrix 支持人员访问这些计算机，这些人员将有责任安全执行操作。本文档的其他部分涵盖了对访问堡垒或部署中的其他计算机的任何人暴露的任何漏洞的责任（例如，客户有责任向允许列表中添加 IP 范围，Citrix 有责任正确实施 IP 范围）。

在这两种情况下，Citrix 都负责正确创建防火墙例外以允许传输 RDP 流量。Citrix 还负责在客户处置堡垒或通过 Citrix DaaS 终止 RDP 访问权限后撤销这些例外情况。

**堡垒** Citrix 可能会在客户的 Citrix 托管订阅内在客户的 Citrix 托管虚拟网络中创建堡垒，以主动诊断和修复问题（无需客户通知）或响应客户提出的问题。堡垒是指客户可以通过 RDP 访问，然后用于通过 RDP 访问 VDA 和 Cloud Connector（适用于已加入域的目录）以收集日志、重新启动服务或执行其他管理任务的计算机。默认情况下，创建堡垒会打开外部防火墙规则以允许 RDP 流量从客户指定的 IP 地址范围传输到堡垒计算机。它还打开了内部防火墙规则以允许通过 RDP 访问 Cloud Connector 和 VDA。打开这些规则会带来很大的安全风险。

客户负责提供用于本地 Windows 帐户的强密码。客户还负责提供允许 RDP 访问堡垒的外部 IP 地址范围。如果客户选择不提供 IP 范围（允许任何人尝试执行 RDP 访问），则客户应对恶意 IP 地址试图执行的任何访问负责。

客户还负责在故障排除完成后删除堡垒。堡垒主机暴露了额外的攻击面，因此 Citrix 会在计算机打开电源八 (8) 小时后自动关闭计算机。但是，Citrix 永远不会自动删除堡垒。如果客户选择长时间使用堡垒，他们将负责修补和更新堡垒。Citrix 建议仅使用几天堡垒，然后将其删除。如果客户希望使用最新的堡垒，则可以删除当前堡垒，然后创建一个新堡垒，这将预配一台安装了最新的安全修补程序的新计算机。

**RDP 访问** 对于已加入域的目录，如果客户的 VNet 对等互连功能正常，客户可以允许 RDP 从对等互连 VNet 访问其 Citrix 托管 VNet。如果客户使用此选项，则客户负责通过 VNet 对等互连访问 VDA 和 Cloud Connector。可以指定源 IP 地址范围，以便可以进一步限制 RDP 访问，即使是在客户的内部网络中亦如此。客户需要使用域凭证才能登录这些计算机。如果客户正在与 Citrix 技术支持合作解决问题，客户可能需要与支持人员共享这些凭证。问题解决后，客户应负责禁用 RDP 访问权限。保持从客户的对等互连或本地网络进行 RDP 访问处于打开状态会带来安全风险。



### 域凭据

如果客户选择使用已加入域的目录，客户应负责向 Citrix DaaS 提供域帐户（用户名和密码），并有权将计算机加入域。在提供域凭证时，客户有责任遵守以下安全原则：

- 可审核：应专门为 Citrix DaaS 使用情况创建帐户，以便轻松审核帐户的用途。
- 作用域：帐户只需要将计算机加入域的权限。它不应是完全权限域管理员。
- 安全：应在帐户上放置强密码。

Citrix 负责将此域帐户安全存储在客户的 Citrix 托管 Azure 订阅中的 Azure 密钥保管库中。只有在操作需要域帐户密码时才能检索该帐户。

### 更多信息

相关信息，请参阅：

- [适用于 Citrix Cloud 平台的安全部署指南](#)：Citrix Cloud 平台的安全信息。
- [技术安全性概述](#)：Citrix DaaS 的安全信息
- [第三方声明](#)

### 交付方法

April 11, 2023

一种交付方法可能无法满足您的所有要求。

可以考虑使用多种应用程序交付方法。选择恰当的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。此操作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（例如 VDA）以及多个应用程序层，管理员可以轻松创建新的可部署映像。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。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](#)。

对于桌面，可以考虑使用 Citrix Virtual Apps 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 发布的应用程序和发布的桌面。

用例：

- 您希望使用基于服务器的经济实惠的交付，以便最大程度地减少向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。
- 托管应用程序集中进行管理且用户无法修改应用程序，从而提供一致、安全、可靠的用户体验。
- 用户必须联机才能访问其应用程序。

用户体验：

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

处理、托管和交付应用程序：

- 应用程序处理在托管计算机（而非用户设备）上执行。托管计算机可以是物理机，也可以是虚拟机。
- 应用程序和桌面驻留在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。
- 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，并且该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来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完美配合使用或可能与操作系统进行交互的应用程序，例如 Microsoft .NET Framework。这些类型的应用程序最适合在虚拟机上进行托管。

优势和注意事项：

- 可以在数据中心中的计算机上安全管理、托管和运行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，同时增加用户的个人虚拟磁盘的存储量。

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。

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）。操作系统将每个应用程序视为一个新会话。
- 在交付组中，已登录的用户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 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 Citrix Virtual Apps 发布的桌面，但是不要求其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映像。）首次使用后，用户每次登录以使用其中一个桌面时，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。

## Remote PC Access

Remote PC Access 是 Citrix DaaS（以前称为 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 DaaS 组件。因此，部署和配置 Remote PC Access 的要求和流程与部署 Citrix DaaS 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。

有关详细信息，请参阅 [Remote PC Access](#)。

## 入门：规划和构建部署

March 30, 2024

如果您不熟悉 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）所使用的组件、术语和对象，请参阅 [Citrix DaaS](#)。

要了解客户旅程视角，请转到 [Citrix Success Center](#)。成功中心为 Citrix 之旅的五个关键阶段提供指导：规划、构建、推出、管理和优化。

- Success Center 信息是本产品文档的重要合作伙伴。
- Success Center 文章和指南提供了基于解决方案的广泛视角。它们还包含指向本产品文档中特定于服务的详细信息的链接。

如果要从 Citrix Virtual Apps and Desktops 部署进行迁移，请参阅[迁移到云](#)。

### 重要：

为确保您获得有关 Citrix Cloud 和您订阅的 Citrix 服务的重要信息，请确保您能够接收所有电子邮件通知。

在 Citrix Cloud 控制台的右上角，展开客户名称和 OrgID 字段右侧的菜单。选择帐户设置。在我的个人资料选项卡上，选择电子邮件通知部分中的所有条目。

## 如何使用本文

要设置 Citrix DaaS 部署，请完成下面概述的任务。提供了指向每个任务的详细信息的链接。

开始部署之前，请检查整个过程，这样您会知晓预期结果。本文还链接到其他有用的信息来源。

### 注意：

如果您计划使用快速部署界面预配 Microsoft Azure 计算机，请按照[快速部署入门](#)中的设置指南进行操作。

## 规划和准备

使用 Success Center [Plan](#)（规划）指南可帮助确定目标、定义用例和业务目标、识别潜在风险以及创建项目计划。

在 Citrix Tech Zone 文档中，请参阅[此服务的分步概念证明指南](#)。

## 注册

[注册](#)一个 Citrix 帐户并申请 Citrix DaaS 演示版。

## 设置资源位置

资源位置包含向用户交付应用程序和桌面所需的资源。创建资源位置使 DaaS 能够使用这些资源。要了解有关资源位置的详细信息，请参阅[连接到 Citrix Cloud](#)。

在创建计算机之前，必须将资源位置连接到 DaaS：

- 加入域的计算机要求您在资源位置中安装 Cloud Connector。在这种情况下，您可以：
  - [创建加入了 Active Directory 的本地目录](#)
  - [创建加入了 Azure Active Directory 的目录](#)

- 创建加入了 [Azure Active Directory](#) 的混合目录

为了实现高可用性，我们建议您在每个资源位置安装两个 Cloud Connector。请参阅 [Cloud Connector 安装](#)。

更多信息：

- [资源位置和 Cloud Connector 是什么？](#)
- [有关安装 Cloud Connector 的视频：](#)



- 未加入域的计算机不需要 Cloud Connector，但需要您启用 Rendezvous V2。Rendezvous 协议允许 VDA 绕过 Cloud Connector 直接安全地与 DaaS 连接。请参阅 [Rendezvous V2](#)。在这种情况下，您可以：

- [创建未加入域的目录](#)

如果您正在使用[快速部署](#)界面来预配 Azure VM，Citrix 将为您创建资源位置和 Cloud Connector。

### 创建与资源位置的连接

添加资源位置和 Cloud Connector 后，请使用 Citrix DaaS 的“完整配置”界面[创建连接](#)，该连接指向资源位置。

在以下任何一种情况下，此步骤都不是必需执行的：

- 您正在构建简单的概念证明部署
- 您正在使用[快速部署](#)界面来预配 Azure VM。

更多信息：

- [主机是什么？](#)
- [主机连接是什么？](#)

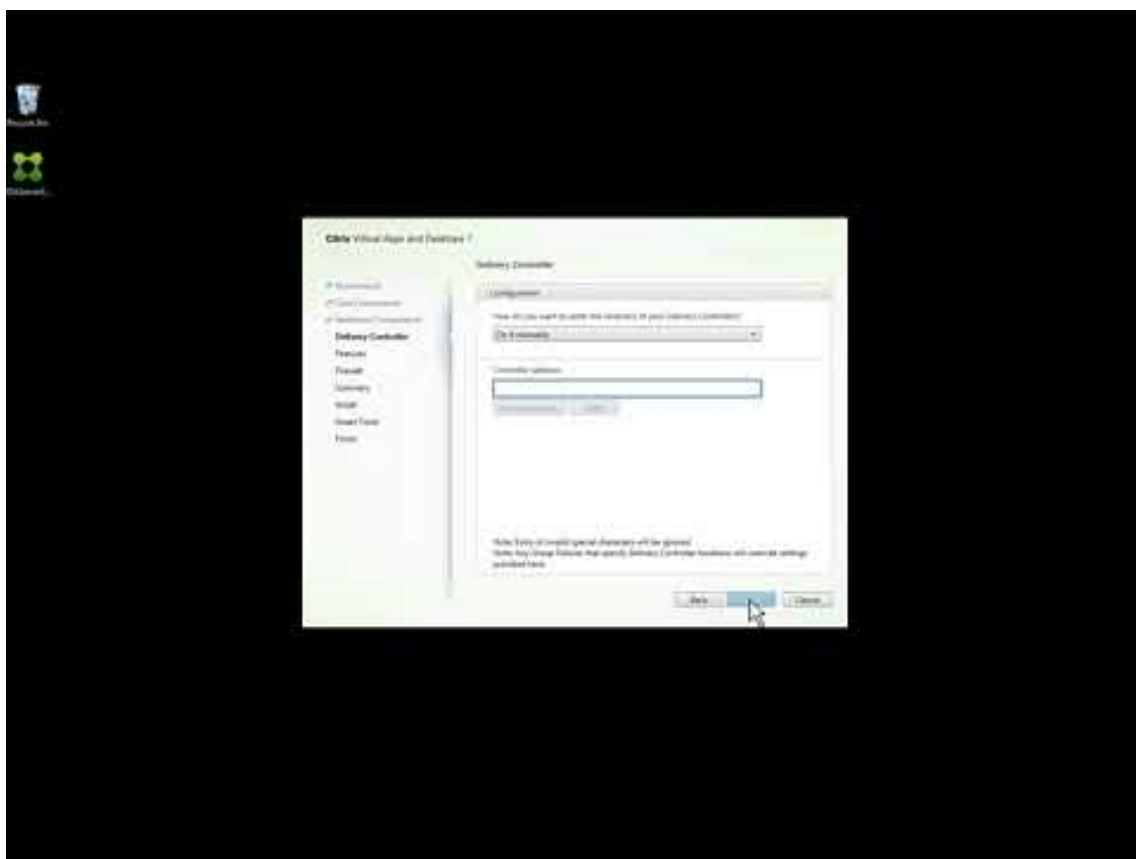
## 安装 VDA

用于向用户交付应用程序和桌面的每台计算机上都必须安装 Citrix Virtual Delivery Agent (VDA)。

- 对于简单的概念证明部署，请在一台计算机上下载并安装 VDA。
- 如果要使用映像预配 VM，请在映像上安装 VDA。
- 对于 [Remote PC Access](#) 部署，请在每台物理办公 PC 上安装适用于单会话操作系统的 VDA 的核心版本。

操作方法和更多信息：

- [VDA 是什么？](#)
- [安装准备和说明](#)
- [命令行 VDA 安装](#)
- 有关下载和安装 VDA 的视频：



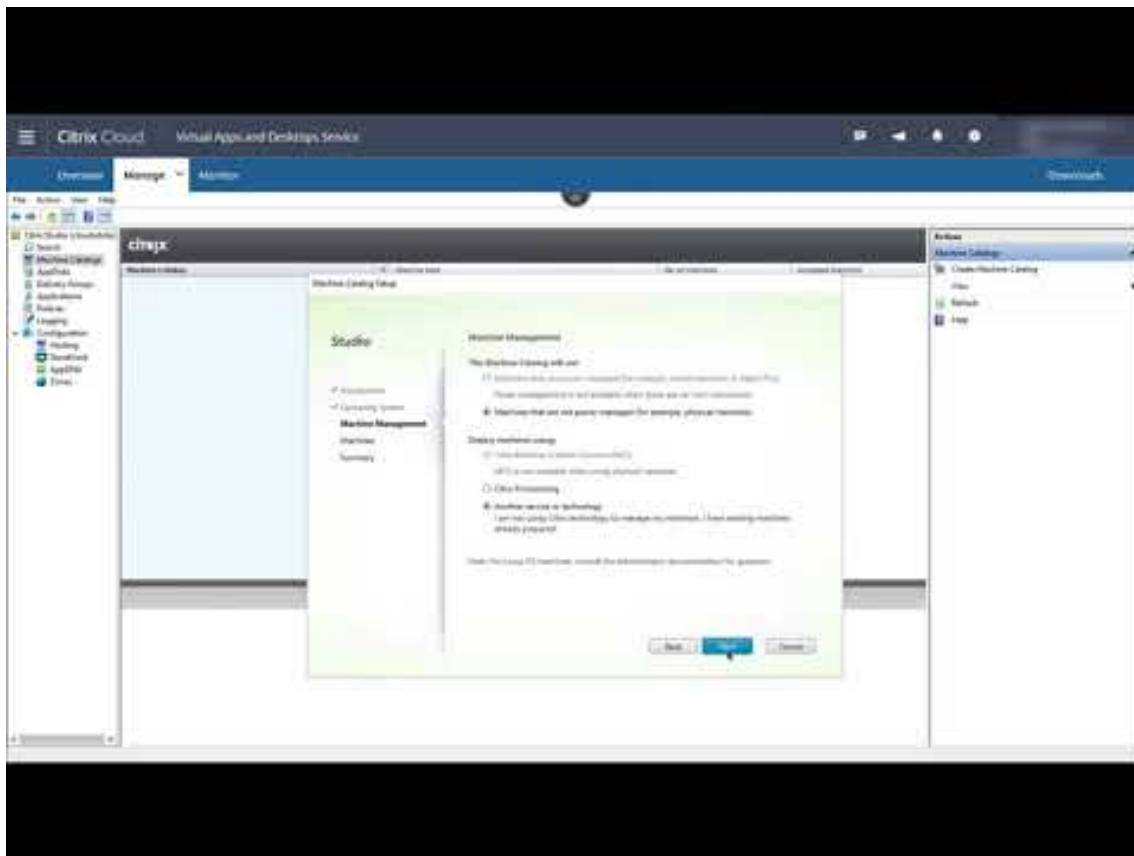
## 创建目录

创建与您的资源位置的连接后（如果需要），即可创建目录。如果您使用的是“完整配置”界面，工作流将自动引导您进入此步骤。

操作方法和更多信息：



- [目录是什么？](#)
- [创建目录](#)
- 使用[快速部署](#)界面部署包含 Azure VM 的目录。
- 关于使用完整配置管理界面创建目录的视频：



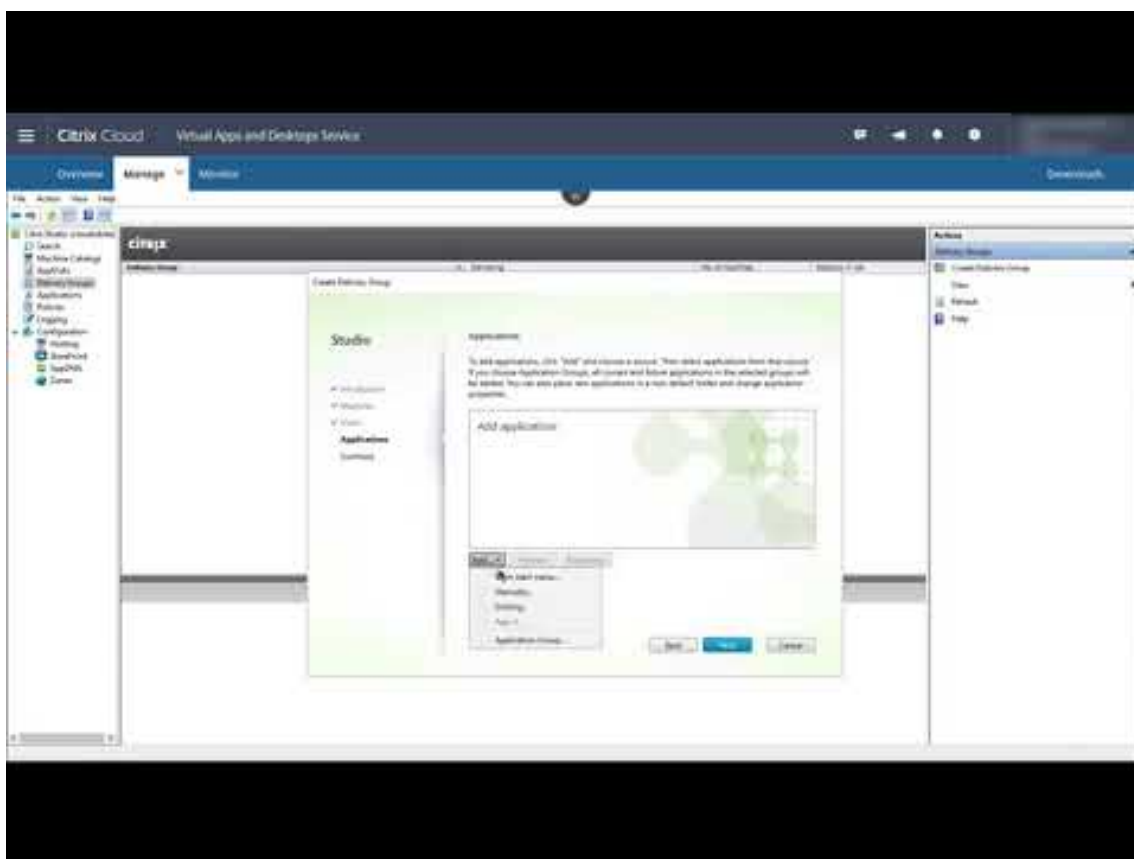
## 创建交付组

创建第一个目录后，管理工作流将引导您创建交付组。

如果您使用[快速部署](#)界面来预配 Azure VM，则没有必要执行此步骤。

操作方法和更多信息：

- [交付组是什么？](#)
- [创建交付组](#)
- 有关如何创建交付组的视频：



## 部署其他组件和技术

完成上述设置 Citrix DaaS 部署的任务后，请按照 Citrix Success Center 的 [Build](#)（构建）区域中的指导进行操作。可以在 Citrix 解决方案中找到有关预配和配置其他组件和技术的信息，例如：

- [Citrix 策略](#)
- [StoreFront](#)
- [App Layering](#)
- [Workspace Environment Management \(WEM\) Service](#)
- [Citrix Gateway 服务](#)
- [区域](#)
- [联合身份验证服务 \(FAS\)](#)

完成适用于您的配置的其他任务。例如，如果您计划交付 Windows Server 工作负载，请[配置 Microsoft RDS 许可证服务器](#)。

## 启动应用程序和桌面

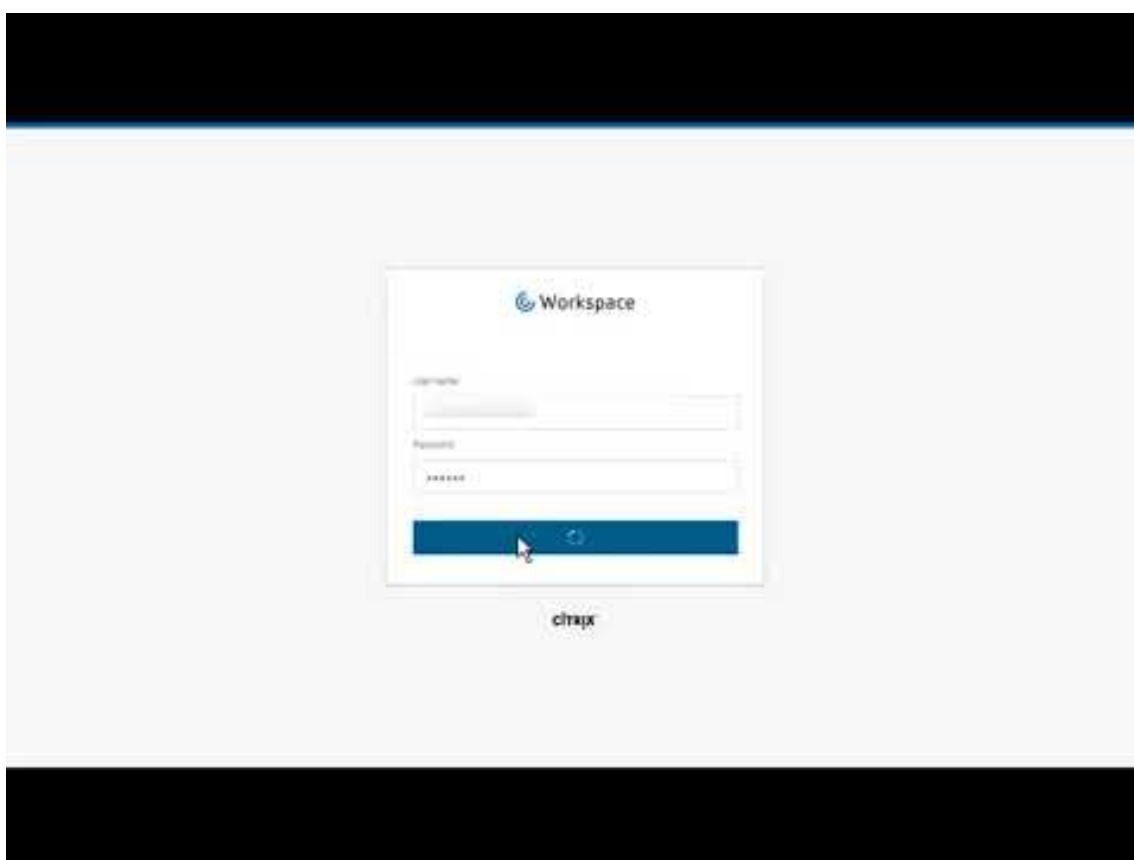
配置部署后，将自动进行发布。您配置的应用程序和桌面可供其 Citrix Workspace 中的用户使用。用户只需导航到其 Workspace URL 并选择一个应用程序或桌面，该应用程序或桌面将立即启动。

将 [Workspace URL 发送给用户](#)。您可以在两个位置找到 Workspace URL：

- 在 Citrix Cloud 控制台中，从左上角的菜单中选择工作区配置。“访问”选项卡包含工作区 URL。
- 在 Citrix DaaS 概述页面中，工作区 URL 将显示在靠近页面底部的位置。

更多信息：

- 有关用户如何从其工作区启动应用程序和桌面的视频：



更多信息

Citrix Cloud Learning 系列提供按照您的路径组织整理的教育课程：

- 如果您不熟悉 Citrix DaaS，请参阅 [New to Citrix DaaS Learning Path](#)（首次使用 Citrix DaaS 学习路径）。
- 如果要从 Citrix Virtual Apps and Desktops 部署进行迁移，请参阅[将 Citrix DaaS 迁移到 Citrix Cloud 学习路径](#)。

## 注册 **Citrix DaaS**

November 16, 2023

### 简介

可以通过 Citrix 或 Azure 应用商店订阅 Citrix DaaS。

如果您计划使用 [Citrix 托管 Azure](#)，则还可以通过 Citrix 或 Azure 应用商店订购 Citrix Azure Consumption Fund。

- 通过 Citrix 订购时，可以同时订购 Citrix DaaS 和 Citrix Azure Consumption Fund。
- 通过 Azure 应用商店订购时，请先订购 Citrix DaaS。然后，可以为 Citrix Azure Consumption Fund 下另一个订单。

如果您现在只订购 Citrix DaaS，稍后可以通过 Azure 应用商店或 Citrix 帐户代表订购 Citrix Azure Consumption Fund。

### 演示版和试用版

您可以通过 Citrix 根据请求评估 Citrix DaaS。在试用版中，您可以转换为付费服务订阅。

在试用期间，可以选择使用 Citrix 托管 Azure 订阅来建立目录、映像和网络连接。如果您在转换为付费订阅时有 Citrix 托管的资源，则必须购买消费量或删除这些 Citrix 托管的资源。如果您不购买消费量，这些资源将自动删除，这可能会影响用户。

### 如果您当前订阅了 **Citrix DaaS** 服务

通常情况下，Citrix Cloud 帐户仅允许您一次为每个 Citrix OrgID 订阅其中一项 Citrix DaaS 的服务（或一个版本）。例如，您可以订阅 Citrix DaaS Premium Edition 或 Citrix DaaS for Azure，但不能同时订阅两者。

如果您当前订阅了 Citrix DaaS 并想订阅此服务，则有两种选择：

- 使用其他 Citrix Cloud 帐户 (OrgID) 订阅此服务。
- 取消您已经拥有的 Citrix DaaS，然后订购此服务。有关停用说明，请参阅 [CTX239027](#)。

### 通过 **Citrix** 订购

可以通过 Citrix Citrix Cloud 或通过 Citrix 帐户代表订购此服务（以及 Citrix Azure Consumption Fund）。

通过 Citrix Cloud：

- 按照[注册 Citrix Cloud](#) 中的指南获取 Citrix Cloud 帐户和组织 ID。
- 可以申请 Citrix DaaS 演示版。在 Citrix DaaS 磁贴中，单击 **Request Demo**（申请演示版）。提供请求的信息。

Citrix 代表将与您联系，讨论您的要求、环境和计划。您将被授权参加管理员演示版或概念证明试用版的权限，具体取决于我们代表的评估结果。有关详细信息，请参阅[Citrix Cloud 服务试用版](#)。

获得试用授权后，Citrix Cloud 控制台中的 Citrix DaaS 磁贴上的文本将变为管理。

### 通过 **Azure** 应用商店订购

可以通过 Azure 应用商店订购以下 Citrix 产品/服务：

- 适用于 Azure 的 Citrix
- Citrix DaaS Advanced Edition
- Citrix DaaS Premium Edition
- Workspace Premium Plus

如果您计划在 Microsoft Azure 上托管 Citrix Virtual Apps and Desktops 工作负载，并希望使用[Citrix 托管 Azure](#) 订阅，请在订购 Citrix DaaS 或 Workspace Premium Plus 后订购 Citrix Azure Consumption Fund。

使用 Citrix Azure Consumption Fund，您需要按月收取消费费用，这可能会因您选择的托管资源和使用时间而有所不同。可以通过 Citrix Cloud 查看消费量使用情况。

来自 Azure 应用商店：

- 不能将 Citrix DaaS 和消费基金合并在一个订单中。
- Citrix Azure Consumption Fund 的订购过程基本上与订购 Citrix DaaS 相同，但您必须先前订购了 Citrix DaaS。

### 通过 **Azure** 应用商店订购的要求

- 您的 Citrix Cloud 帐户的组织 ID。
  - 如果您有 Citrix Cloud 帐户，但不知道组织 ID，请查看 Citrix Cloud 控制台的右上角。或者，查看您在创建帐户时收到的电子邮件。
  - 如果您没有 Citrix Cloud 帐户，请按照[注册 Citrix Cloud](#) 中的指南进行操作。
- 该帐户中的 Azure 帐户和至少一个 Azure 订阅。

### 通过 **Azure** 应用商店订购的过程

按照此过程通过 Azure 应用商店订购 Citrix DaaS 或 Workspace Premium Plus。（如果要使用 Citrix 托管的 Azure，请在订购 Citrix DaaS 后再下一个 Citrix Azure Consumption Fund 的订单。）

1. 使用 Azure 帐户凭据登录到 [Azure 应用商店](#)。
2. 搜索然后导航到要订购的 Citrix 产品。
3. 选择立即获取。
4. 在 **One more thing**（另一个操作）消息中，填写所需的信息，启用同意复选框，然后选择继续。
5. 查看包含有关产品、计划、定价和使用情况的信息的选项卡。准备就绪后，选择一个计划（如果有多个计划），然后选择设置 + 订阅。
6. 在基本选项卡上：
  - 订阅：表示您选择的计划。
  - 资源组：选择或创建资源组。
  - 名称：输入订阅订单的名称，以便稍后轻松识别。
  - 计划信息根据账单期限显示所选计划的价格。要更改计划期限，请选择更改计划。选择你想要的期限，然后选择更改计划。
7. 在 **Review + subscribe**（检查 + 订阅）选项卡上，查看联系人信息，然后根据需要进行更新。检查基本订阅信息。选择订阅。
8. 在 **Subscription in progress**（订阅进行中）页面上，选择 **Configure account now**（立即配置帐户）。（如果按钮处于禁用状态，请稍候。）您被转至 Citrix 激活页面。
9. 在激活页面上：
  - 使用登录链接登录 Citrix Cloud。成功登录将自动填充组织 ID 字段。
  - 数量：输入用户数量。（初始订单必须至少为 25。）此时将显示预估价格。
  - 同意条款和条件，然后选择激活订单。

#### 通过 **Azure** 应用商店订购后

预配服务时，Citrix 会向您发送电子邮件。预配可能需要一段时间。如果您在第二天之前没有收到电子邮件，请联系 [Citrix 支持](#)。收到 Citrix 发送的电子邮件时，即可开始使用 Citrix DaaS。

Citrix Azure Consumption Fund 订单的履行不需要太多时间。当 Citrix 收到有关订单的通知时，Citrix DaaS 控制台会出现一条横幅，表示将为您准备 Citrix 托管的 Azure 订阅。

请勿在 Azure 中删除 Citrix DaaS 资源。删除该资源将取消您的订阅。

#### 通过 **Google Cloud Marketplace** 订购

您可以通过 Google Cloud Marketplace 订购以下 Citrix 产品：

- Citrix DaaS Standard for Google Cloud
- Citrix DaaS Premium for Google Cloud

要通过 Google Cloud Marketplace 订购，您需要以下物品：

- 您的 Citrix Cloud 帐户的组织 ID。
  - 如果您有 Citrix Cloud 帐户，但不知道组织 ID，请查看 Citrix Cloud 控制台的右上角。或者，查看您在创建帐户时收到的电子邮件。
  - 如果您没有 Citrix Cloud 帐户，请按照[注册 Citrix Cloud](#) 中的指南进行操作。
- 一个 Google Cloud 帐户以及该帐户中至少有一个 Google Cloud 订阅。

要下订单，请执行以下操作：

1. 登录 [Google Cloud Marketplace](#)
2. 请按照 [Citrix DaaS for Google Cloud](#) 页面上的说明进行购买。

预配服务时，Citrix 会向您发送电子邮件。预配可能需要一段时间。如果您在第二天之前没有收到电子邮件，请联系 [Citrix 支持](#)。收到 Citrix 发送的电子邮件时，即可开始使用 Citrix DaaS。

请勿删除 Google Cloud 中的 Citrix DaaS 资源。删除该资源将取消您的订阅。

接下来做什么

订单完成后，继续执行[规划和构建部署](#)中的后续步骤。

例如：

- 如果尚未设置虚拟机管理程序、云服务或 Active Directory，请参阅[设置资源位置](#)。
- 如果已设置您的主机环境和 Active Directory，请参阅[创建连接](#)。

## 适用于 **Windows 365** 的 **Citrix HDX**

December 1, 2022

适用于 Windows 365 的 Citrix HDX Plus 允许您将 Citrix Cloud 与 Windows 365 集成，使用 Citrix HDX 技术来获得增强和更安全的 Windows 365 云电脑体验，此外还有其他 Citrix Cloud 服务以增强可管理性。

有关更多信息，请参阅[适用于 Windows 365 的 Citrix HDX Plus](#)

## 适用于 **Amazon WorkSpaces Core** 的 **Citrix DaaS**（预览版）

March 30, 2024



该预览版仅用于使用开发或测试工作负载进行评估。您不得将其用于生产工作负载。您不得将预览用于任何关键、生产或其他重要代码、数据或其他内容。

AWS 可能会自行决定或根据参与者的反馈在预览期内和之后更改预览的功能。预览功能、特性和文档在预览期间可能会发生变化，可能与任何公开版本不同。

尽管 AWS 不为此预览版收费，但您应承担与预览一起使用的其他 AWS 服务产生的费用。标准定价适用于您使用这些 AWS 服务。

您不得使用预览来处理或存储 PII 或其他敏感数据或信息。

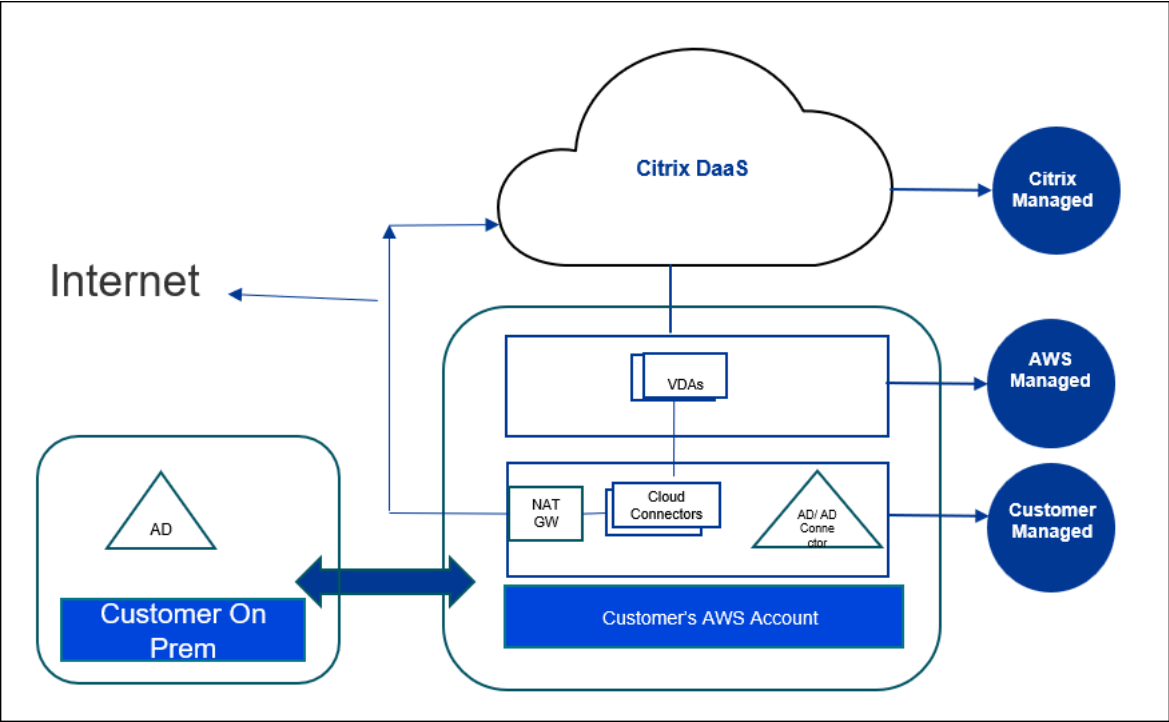
此预览版未经过 HIPAA 身份验证，也未经过身份验证，无法在美国或国际上处理或存储医疗数据或信息。

如果您在使用此预览版时使用来自第三方医院、患者或医疗保健机构的任何数据，请确保在允许这些第三方使用之前获得所有必要的同意。

简介

本文介绍如何使用 Citrix 为 Amazon WorkSpaces Core 准备和创建部署。Amazon WorkSpaces Core 位于 Amazon Web Services (AWS) 中。

下面是使用 Citrix DaaS 实现 AWS 及其管理的示例：



### 关于此预览

- 如需本预览期间的支持，请在美国东海岸工作时间内联系您的 Citrix 客户代表。请勿联系 Citrix 支持或 AWS 支持部门。
- 要在此预览期间管理 Citrix 环境，请仅使用 Citrix DaaS 中的管理控制台。此预览版期间不支持 Citrix 或 AWS API。（Citrix 欢迎您就将来要使用的 API 提供反馈。）

### 准备和创建部署

快速部署界面中的部署清单包含指向过程 1-5 的链接。

1. [在开始之前](#)，请先完成 Citrix Cloud 和 AWS 中的必备条件。
2. 在 Citrix Cloud 中[创建资源位置](#)。（此过程也作为必备条件包括在内。）
3. [连接您的 AWS 帐户](#)。此过程启用权限，这样 Citrix DaaS 就可以连接到 AWS。
4. [创建目录连接](#)。此过程配置允许访问您组织的 Active Directory 的连接。
5. [导入映像](#)。此过程使您能够为用户创建桌面体验。
6. [创建部署](#)。此过程指定了要部署的计算机以及可以通过 Citrix Workspace 访问这些计算机的用户。

### 开始之前的准备工作

在开始准备和创建部署之前，请确保您已完成以下任务。

有一个例外：在 Citrix Cloud 中创建资源位置被列为必备条件。这也是部署清单中的第一个程序。因此，如果您将资源位置创建为必备条件的一部分，请跳过清单序列中的该过程。同样，如果您之前没有完成该程序，请在清单中完成该程序。

### 在 **Citrix Cloud** 中完成的前提条件

- [创建 Citrix Cloud 帐户](#)并订阅 Citrix DaaS。您的 Citrix 代表可以帮助解决这个问题。您的代表还会为您启用此预览功能。
- [创建 Citrix Cloud 资源位置](#)。（此过程也在“快速部署”界面中进行了链接。）

### 在 **AWS** 中完成的必备条件

- 创建非生产 AWS 用户帐户。该帐户必须有：
  - Citrix API 客户端的角色权限。
  - 编程访问权限。有关更多信息，请参阅 [AWS 帐户编程访问权限](#)。
  - 创建 workspaces\_DefaultRole 角色。有关更多信息，请参阅[创建 workspaces\\_DefaultRole 角色](#)。
- 在 Active Directory 中：

- 使用 AD 连接器选项存储和管理信息。有关更多详细信息，请参阅 [AD 连接器](#)。
  - 创建一个 OU，在其中创建 VM。该 OU 必须有 Citrix 策略才能与 Cloud Connector 和 Citrix Cloud 进行通信。有关详细信息，请参阅“参考”部分。
  - 为 Citrix Cloud Connector 配置设置组策略：
    1. 从 [Citrix 下载站点](#) 下载由 Citrix 提供的最新组策略管理控制台 (CitrixGroupPolicyManagement\_64.msi)。
    2. 安装 MSI (该计算机必须安装 Visual Studio 2015 运行时)。然后创建包含 [控制器策略设置](#) 的 [Citrix 策略](#)。该设置指定 Cloud Connector 地址。
  - 创建或使用现有的 NAT 网关。有关更多信息，请参阅 [NAT 网关](#)。
  - 创建或使用一个或多个现有安全组，允许 Citrix Cloud Connector 与已部署的虚拟机进行通信。有关更多信息，请参阅 [使用安全组控制流向 AWS 资源的流量](#)。
  - 打开 AWS 支持票证，在您的帐户上启用 BYOL。要开始使用，请联系您的 AWS 帐户经理或销售代表，或联系 AWS 支持中心。您的联系人将验证并启用 BYOL。有关更多信息，请参阅 [使用 Amazon WorkSpaces 控制台为您的帐户启用 BYOL 的 BYOL](#)。
- 注意：

BYOL 目前不支持 Windows 10 N 和 Windows 11 N 版本。
- 使用 Citrix DaaS for Amazon WorkSpaces Core 功能将自动启用 AWS WorkSpaces Core 中的自带协议 (BYOP) 功能。
  - 为将要创建的桌面拥有足够的 Windows 10 许可证。有关更多信息，请参阅 [自带 Windows 桌面许可证](#)。

## 一般准备

在开始之前，请先查看每个程序。好处：这将有助于轻松完成流程。

## 创建资源位置

您可以在 Citrix Cloud 中创建资源位置。

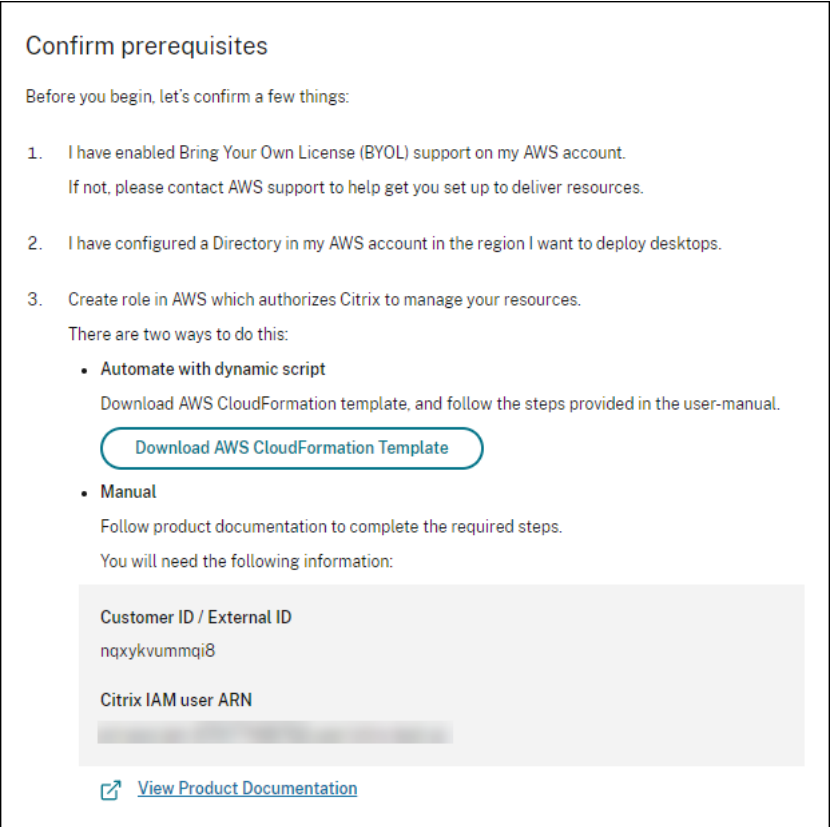
- 资源位置包含两个或更多与 Citrix Cloud 通信的 Cloud Connector。您安装 Cloud Connector 的服务器必须位于 EC2 VPC 中，已加入域并且具有 Internet 连接。Cloud Connector 必须与您计划使用的目录位于同一 VPC 中。
- 有关 Cloud Connector 的更多信息，请参阅 [Citrix Cloud Connector](#) 以及如何对其进行配置。
- 资源位置也可以包含您的 Active Directory 服务器。有关更多信息，请参阅 [将 Active Directory 连接到 Citrix Cloud](#)。

连接您的 **AWS** 帐户

此过程允许 Citrix DaaS 连接到 AWS 的权限。

要为 AWS WorkSpaces Core 创建 AssumeRole，请按照以下步骤操作：

1. 在 Citrix DaaS 中，在“管理” > “快速部署” > “帐户” 下，单击“连接帐户”。
2. 在“连接 **AWS** 帐户”页面的“确认前提条件”下，单击“下载 **AWS CloudFormation** 模板”。下载模板后，单击“下一步”。



1. 要上载模板，请参阅为 [AWS Workspace Core 集成创建 AssumeRole](#)。
2. 在身份验证帐户页面中，添加在角色 **ID** 字段中生成的 **Amazon Resource Name (ARN)**，在名称字段中提供名称，然后单击“下一步”。“选择区域”页面打开。

角色 **ID** 对应角色的 ARN，该角色将授权 Citrix 管理资源。通过导航到 **IAM > 角色**，可以在 AWS 管理控制台 中找到角色 ID。

如果您使用的是 **CloudFormation** 脚本，请导航到 CloudFormation 并单击用于创建角色的相应堆栈。导航到资源选项卡，然后单击带有 LogicalID **CitrixAssumeRole** 的资源。

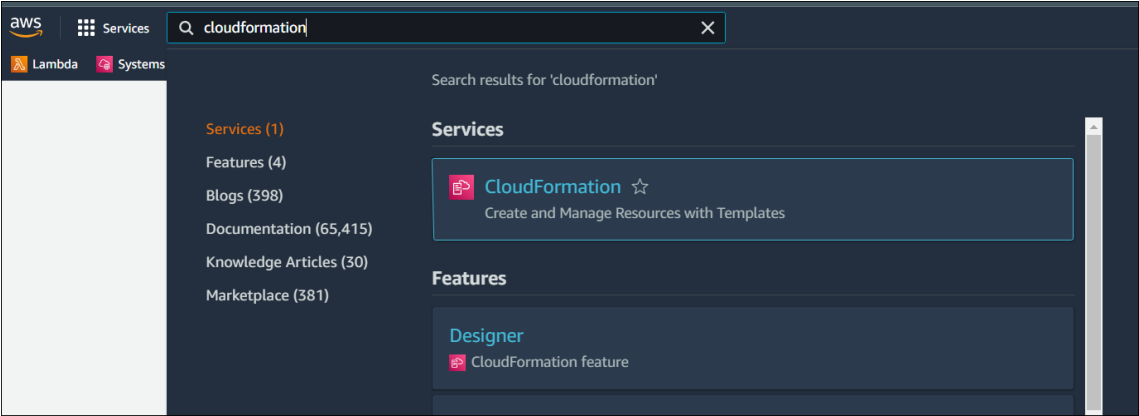
注意：

您不能为同一 AWS 帐户连接同一区域的两个帐户。

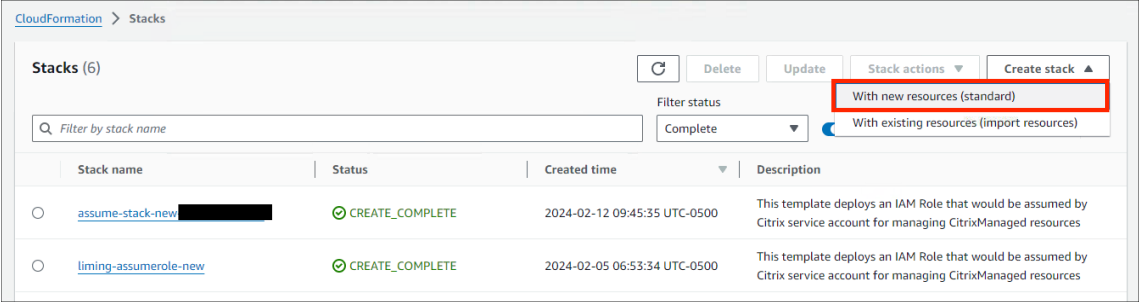
3. 在选择区域页面中，选择要部署桌面的区域，然后单击下一步。
4. 在配置 **BYOL** 支持页面中，要配置 BYOL 支持，需要连接到安全 Amazon 网络的管理网络接口。选择要搜索的 IP 地址范围用作该接口。然后选择“显示可用的 CIDR 块”。如果 CIDR 区块在所搜索范围内可用，请选择一个可用的 CIDR 块。当您成功选择搜索地址范围和可用的 CIDR 块时，将显示一条确认消息。单击下一步。
5. 在“摘要”页面中，查看您指定的信息。您可以返回到之前的页面。完成后，单击“完成”。  
连接过程可能需要几个小时才能完成。

为 **AWS Workspace Core** 集成创建 **AssumeRole**

1. 在浏览器窗口中，打开 **Amazon Web Services Web** 站点并登录。
2. 在“搜索”字段中，键入 **cloudformation** 并按 **Enter**。



3. 在服务下选择 **CloudFormation**。堆栈窗口打开。



4. 单击右上角的创建堆栈 > 使用新资源（标准）。创建堆栈窗口打开。
  - a) 在“必备条件-准备模板”下，选择“模板准备就绪”。
  - b) 在“指定模板”下，单击“上传模板文件” > “选择文件”，然后单击“下一步”。将打开“指定堆栈详细信息”窗格。
5. 在指定堆栈详细信息窗格中，提供堆栈名称和 **AssumeRoleName**，然后单击下一步。配置堆栈选项 窗格打开。

CloudFormation > Stacks > Create stack

Step 1  
Specify template

Step 2  
Specify stack details

Step 3  
Configure stack options

Step 4  
Review

### Specify stack details

Stack name

Stack name

zl-assumerole-stack

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

AssumeRoleName

The name of the IAM role for Connector EC2 instance

zlrole-demo

Cancel

Previous

Next

注意：

- 在配置堆栈选项窗格中，选择保留成功配置的资源选项。此选项保留成功配置资源的状态。下次堆栈操作时，将删除没有上次已知稳定状态的资源。

CloudFormation > Stacks > Create stack

Step 1  
Specify template

Step 2  
Specify stack details

Step 3  
Configure stack options

Step 4  
Review

### Configure stack options

Tags

You can specify tags (key-value pairs) to apply to resources in your stack. You can add up to 50 unique tags for each stack. [Learn more](#)

Key

Value

Remove

Add tag

Permissions

Choose an IAM role to explicitly define how CloudFormation can create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses permissions based on your user credentials. [Learn more](#)

IAM role - optional

Choose the IAM role for CloudFormation to use for all operations performed on the stack.

iamRoleName

Remove

Stack failure options

Behavior on provisioning failure

Specify the roll back behavior for a stack failure. [Learn more](#)

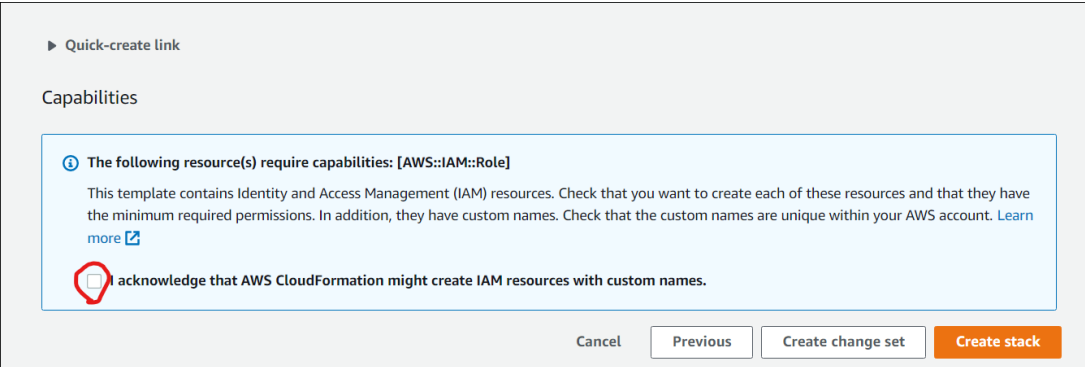
☐ Roll back all stack resources

Roll back the stack to the last known stable state.

☒ Preserve successfully provisioned resources

Preserves the state of successfully provisioned resources, while rolling back failed resources to the last known stable state. Resources without a last known stable state will be deleted upon the next stack operation.

- 在“功能”弹出窗口中，选中“我确认 **AWS CloudFormation** 可能会使用自定义名称创建 **IAM** 资源”复选框，然后单击“创建堆栈”。



堆栈创建最后可能会失败，因为已经创建了 **workspace\_DefaultRole**。这不会影响 **AssumeRole** 的创建。

- 1. 事件选项卡显示创建的堆栈的状态。
- 2. 在资源选项卡中，选择与创建的 **AssumeRole** 对应的物理 ID。

Stack info	Events	Resources	Outputs	Parameters	Template	Change sets
Resources (4)						
<input type="text" value="Search resources"/>						
Logical ID	Physical ID	Type	Status	Status reason	Module	
CitrixAssumeRole	<a href="#">citrix-drole-demo</a>	AWS::IAM::Role	CREATE_COMPLETE	-	-	
ConnectorInstanceProfile	<a href="#">citrix-drole-demo-connector</a>	AWS::IAM::InstanceProfile	CREATE_COMPLETE	-	-	
ConnectorInstanceRole	<a href="#">citrix-drole-demo-connector</a>	AWS::IAM::Role	CREATE_COMPLETE	-	-	
WorkspacesDefaultRole	-	AWS::IAM::Role	CREATE_FAILED	workspaces_DefaultRole already exists	-	

- 3. 摘要窗格显示生成的 **Amazon Resource Name (ARN)**。

Role created with Cloudformation template for reading parameter store / secrets manager

Summary

Creation date

February 05, 2024, 06:53 (UTC-05:00)

Last activity

3 days ago

ARN

arn:aws:iam::[redacted]:role/citrix-[redacted]assumerole-new

Maximum session duration

1 hour

- 4. 继续执行“[连接 AWS 帐户](#)”中第 4 步中的过程

创建目录连接

此过程创建了一个允许访问您组织的 Active Directory 的连接。

必备条件：

- 包含两个 Cloud Connector 的资源位置。
- 一个安全组。
- 您的 Active Directory 中的一个 OU。

有关必备条件的详细信息，请参阅[在开始之前](#)。

您可以从以下两个位置之一开始此过程：



- “入门” 清单上的链接。
- 在 DaaS 管理控制台中，选择左侧窗格中的“快速部署”，“**Amazon WorkSpaces Core**”部分下的“目录连接”。然后选择“创建目录连接”。

按照创建目录连接顺序进行操作：

1. 确认必备条件：如果您已完成必备条件，请单击“下一步”。
2. 连接目录：选择资源位置、帐户和目录。（所选帐户必须至少有一个目录。）
  - 选择要在其中部署台式机的两个子网。子网必须位于相应的可用区内。
  - 为此连接指定一个友好名称。
  - 完成后，单击“下一步”。
3. 虚拟机设置：您选择的设置适用于使用此目录连接的所有虚拟机。
  - 所选的 OU 必须与 Citrix 组策略所针对的 OU 相匹配。
  - 选择一个安全组。
  - 指明是否要向分配给 VM 的每位用户授予管理员权限。

## 导入映像

此过程使您能够为用户创建桌面体验。

导入映像的必备条件：

- 必须是 EC2 映像。
- 必须安装 Citrix Virtual Delivery Agent (VDA)。
- 必须为 BYOL 做好准备。BYOL 脚本可在以下网址获得：[BYOLChecker.zip](#)。

要导入映像，请按照以下步骤操作：

1. 确认必备条件：完成必备条件步骤后，单击“下一步”。（如果您尚未为 BYOL 准备镜像，则可以从此页面下载脚本。）有关更多信息，请参阅[要求](#)。
2. 选择映像并为映像提供一个友好的名称。选择帐户 AMI 并添加描述。单击下一步。“摘要”页面打开。
3. 在“摘要”页面中，查看您提供的信息。验证后，选择“导入映像”。

注意：

导入映像可能需要几个小时。

## 导入映像时集成 **Microsoft Office 2019** 映像

要在导入映像时集成 Microsoft Office 2019 映像，请执行以下操作：

1. 在 **Web Studio > 快速部署** 中，单击“映像”。

2. 在“我的映像”中，单击“导入映像”。
3. 在“导入映像” > “必备条件”中，单击“下一步：选择映像”。
4. 在“导入映像” > “选择映像”中：
  - 从“帐户”下拉列表选择一个帐户。
  - 从 **AMI** 下拉列表选择一个 AMI。
  - 在“名称”字段中输入映像的名称。
  - 在映像中选择包括 **Microsoft Office 2019 Professional Plus**。
  - 在“描述”字段中输入描述。
5. 在“导入映像” > “选择映像”中，单击“下一步：摘要”。
6. 在“选择映像” > “摘要”中，确保 **Microsoft Office 2019** 显示“已选定”。
7. 在“我的映像”中，单击“导入映像”。

在导入操作完成之前，最近部署的映像的状态显示正在导入。
8. 在“我的映像”中，选择最近部署的映像，然后单击“查看详情”。
9. 在详细信息面板中，**Microsoft Office 2019** 字段显示已包含。

注意：

只有以下版本的操作系统兼容：

- Windows 10 版本 21H2 (2021 年 12 月更新)
- Windows 10 版本 22H2 (2022 年 11 月更新)
- Windows 10 Enterprise LTSC 2019 (1809) (1809)
- Windows 10 Enterprise LTSC 2021 (21H2) (21H2)
- Windows 11 版本 22H2 (2022 年 10 月发布)

## 创建部署

部署是一组桌面，用户可以从 Citrix Workspace 访问这些桌面。此过程指定了要部署为桌面的虚拟机的特征，以及哪些 AD 用户可以使用它们。

### 必备条件

完成[准备和创建部署](#)中列出的所有步骤。

1. 在 **Web Studio** > 快速部署中，单击 **Amazon Web Services** 列中的部署。单击“创建部署”。
2. 名称和连接：输入这组计算机的友好名称。其名称必须唯一。选择目录连接，然后单击“下一步：映像和性能”。
3. 映像和性能：选择计算机的操作系统和计算机性能。指定根卷和用户卷的默认大小。

启动该组中的桌面后，您无法更改卷大小。因此，请指定您认为需要的最大尺寸。您还可以在下一页上为每个用户指定这些大小。单击“下一步：用户”。
4. 用户：搜索并选择允许访问桌面的用户。

如果要为用户自定义卷大小，请选择“编辑用户和根卷大小”，然后指定大小。单击“下一步：摘要”。
5. 摘要：查看您提供的信息，然后单击“创建部署”。

## 集成 **Microsoft 365 Windows** 应用程序

要集成 Microsoft 365 应用程序，请参阅 [Microsoft 365 应用程序企业版现已在 Amazon WorkSpaces 服务中提供](#)和 [Microsoft 365 自带许可证 \(BYOL\)](#)。

### 管理部署中的计算机

除了[管理计算机目录](#)中描述的计算机管理功能外，对于某些操作，您还可以从部署中选择要管理的计算机。

要管理部署中的计算机，请执行以下操作：

1. 在 **Web Studio** > 快速部署中，选择部署。
2. 在“部署”窗格中，选择包含要管理的计算机的部署。
3. 单击“查看详细信息”。
4. 在部署详细信息窗格中，选择要管理的计算机。
5. 从显示的操作中，选择要在计算机上执行的操作：
  - 单击“编辑卷大小”以更改计算机的音量大小。
  - 单击“删除”将计算机从部署和 AWS 中删除。如果计算机位于交付组中，则只有在维护模式下才能将其删除。
  - 单击“打开/关闭维护模式”以打开计算机的维护模式（如果已关闭）或关闭（如果已打开）。

### 参考

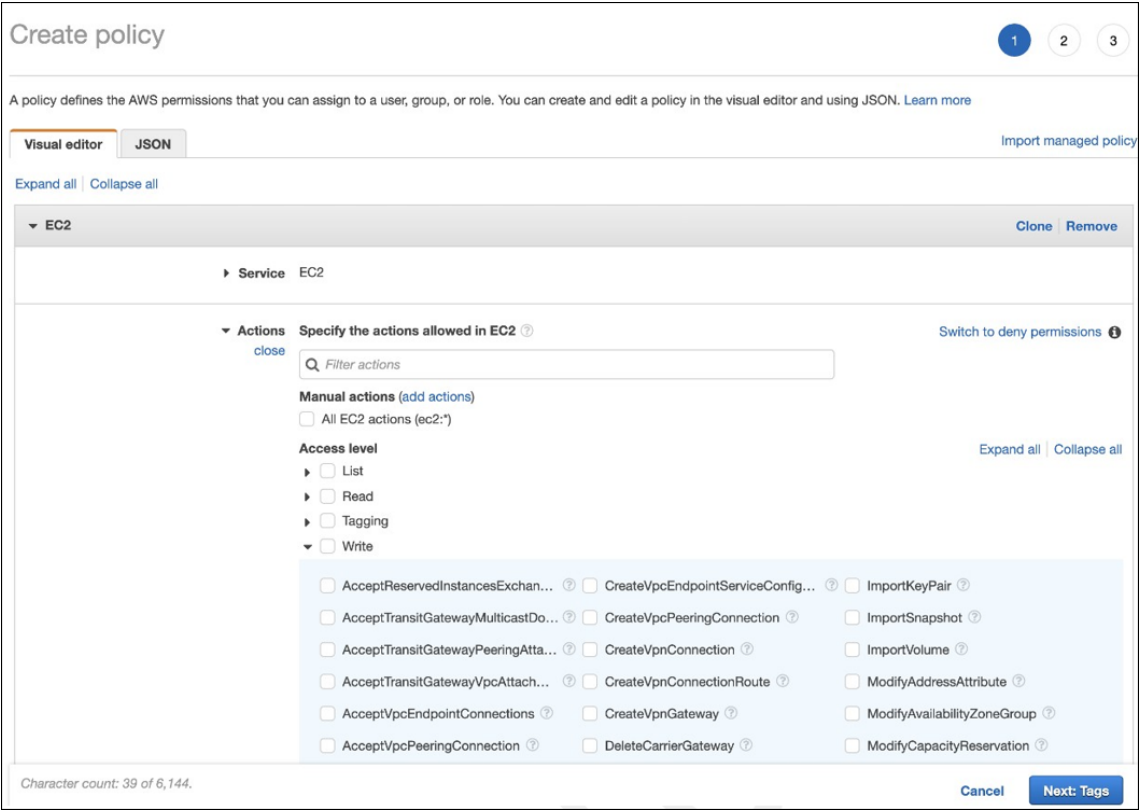
#### **AWS** 帐户编程访问权限

AWS 用户帐户必须具有一定的编程访问权限才能对 AWS 资源层进行 API 调用。编程访问会创建访问密钥 ID 和私有访问密钥。

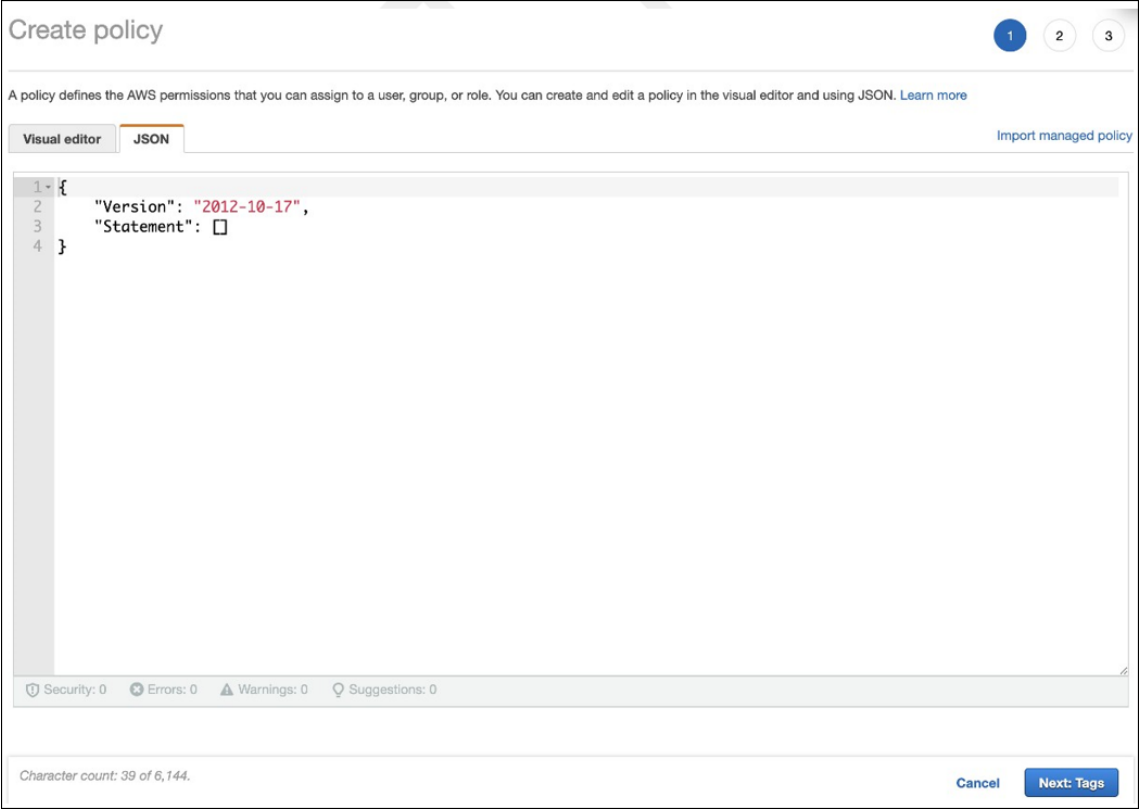
您可以在 [IAM 控制台](#) 中创建包含这些权限的策略。如下图所示，您可以使用可视化编辑器（逐一添加权限）或 JSON（添加下面的代码片段）。

有关更多信息，请参阅[在您的 AWS 帐户中创建 IAM 用户](#)。

- 在可视化编辑器选项卡上，逐一添加权限。



- 在 **JSON** 选项卡上，添加下图后面显示的片段。



## 所需的权限

```

1  {
2
3      "Version": "2012-10-17",
4      "Statement": [
5          {
6
7              "Sid": "VisualEditor0",
8              "Effect": "Allow",
9              "Action": [
10                 "workdocs:DeregisterDirectory",
11                 "workdocs:RegisterDirectory",
12                 "workdocs:AddUserToGroup",
13                 "ec2:ImportInstance",
14                 "ec2:DescribeImages",
15                 "ec2:CreateKeyPair",
16                 "ec2:DescribeKeyPairs",
17                 "ec2:ModifyImageAttribute",
18                 "ec2:DescribeVpcs",
19                 "ec2:DescribeSubnets",
20                 "ec2:RunInstances",
21                 "ec2:DescribeSecurityGroups",
22                 "ec2:CreateTags",
23                 "ec2:DescribeRouteTables",
24                 "ec2:DescribeInternetGateways",
25                 "ec2:CreateSecurityGroup",
26                 "ec2:DescribeInstanceTypes",
27                 "servicequotas:ListServices",
28                 "servicequotas:GetRequestedServiceQuotaChange",
29                 "servicequotas:ListTagsForResource",
30                 "servicequotas:GetServiceQuota",
31                 "servicequotas:
32                     GetAssociationForServiceQuotaTemplate",
33                 "servicequotas:ListAWSDefaultServiceQuotas",
34                 "servicequotas:ListServiceQuotas",
35                 "servicequotas:
36                     GetAWSDefaultServiceQuota",
37                 "servicequotas:
38                     GetServiceQuotaIncreaseRequestFromTemplate",
39                 "servicequotas:
40                     ListServiceQuotaIncreaseRequestsInTemplate",
41                 "servicequotas:
42                     ListRequestedServiceQuotaChangeHistory",
43                 "servicequotas:
44                     ListRequestedServiceQuotaChangeHistoryByQuota",
45                 "sts:DecodeAuthorizationMessage",
46                 "ds:*",
47                 "workspaces:*",
48                 "iam:GetRole",
49                 "iam:GetContextKeysForPrincipalPolicy",
50                 "iam:SimulatePrincipalPolicy"
51             ],
52             "Resource": "*"
53         }
54     ]
55 }

```

```
48         }
49
50     ]
51 }
52
53 <!--NeedCopy-->
```

## 适用于 Google Cloud 的 Citrix DaaS

November 11, 2022

适用于 Google Cloud 的 Citrix DaaS 使您能够使用 Citrix DaaS 的完整配置管理界面部署 Google Cloud 桌面和应用程序。适用于 Google Cloud 的 Citrix DaaS 有标准版和高级版两种版本。

有关支持的功能的信息，请参阅 [Citrix Virtual Apps and Desktops 功能列表](#)。

您可以从 Google Cloud [市场订购适用于 Google Cloud 的 Citrix DaaS](#)。

订购 Citrix DaaS 后，请登录 Citrix Cloud。在左上角的菜单中，选择我的服务 > **DaaS**。

请按照产品文档中的设置指南进行操作。使用“完整配置”界面，您可以创建连接、目录和交付组，就像在其他产品版本中使用该界面一样。（这些版本当前没有快速部署管理界面。）

“完整配置”界面中的某些显示可能与文档中的显示不同。例如，在适用于 Google Cloud 的 Citrix Virtual Apps and Desktops 版本中创建连接时，可用的连接类型包括受支持的虚拟机管理程序和 Google Cloud。其他云服务不可用。

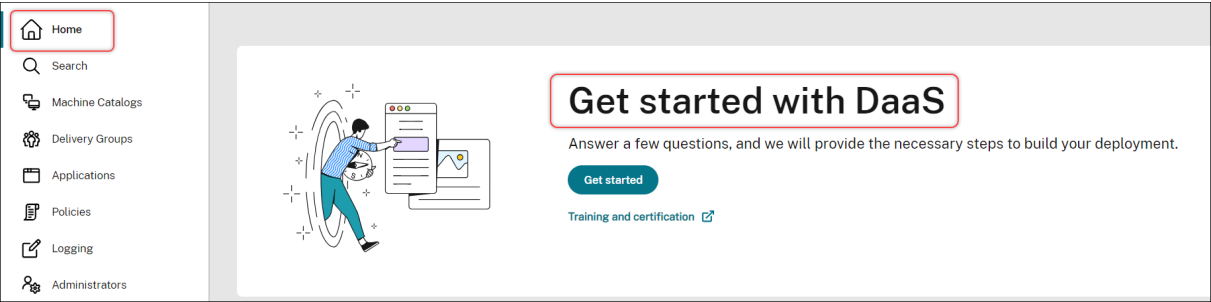
同样，请使用产品文档中适用于受支持的虚拟机管理程序和 Google Cloud 的信息。

有关在 Google Cloud 上部署和配置 Citrix DaaS 的分步说明，请参阅此 Citrix Tech Zone 文章：[Citrix virtualization on Google Cloud](#)（Google Cloud 上的 Citrix 虚拟化）。本文介绍了如何定义部署体系结构、准备 Google Cloud 项目、配置网络服务和部署 Active Directory。

## 使用 **DaaS** 入门指南（预览版）

February 9, 2024

DaaS 入门指南简化并简化了新手和经验丰富的管理员的 DaaS 部署流程。使用该指南，您可以通过回答一系列问题来快速设置 DaaS 部署。



本文将引导您完成设置五种典型的 DaaS 部署场景的过程。

优势

使用本指南的好处包括：

- 易于上手。本指南通过以调查问卷为主导的分步工作流程将基本部署步骤联系起来。如果您是新管理员，则可以通过情境帮助快速设置部署，同时学习概念和术语。
- 简化复杂的配置。本指南在必要时提供预先配置的设置，并允许访问完整配置用户界面进行高级配置。如果您是一位经验丰富的管理员，您可以使用该指南作为复杂配置的起点。

支持的部署方案

本指南为以下场景提供了快速部署：

要交付什么？	计算机已经存在了吗？	计算机类型	备注
虚拟应用程序和桌面	否	虚拟机（由 DaaS 预配）	电源管理
虚拟应用程序和桌面	是	虚拟机或刀片 PC	电源管理
虚拟应用程序和桌面	是	物理机或虚拟机	未进行电源管理
办公室 PC	是	物理机	电源管理
办公室 PC	是	物理机	未进行电源管理

有关详细说明，请参阅以下部分：

- 从头开始交付应用程序和桌面（电源管理）
- 使用现有计算机交付应用程序和桌面（电源管理）
- 使用现有计算机（非电源管理）交付应用程序和桌面
- 交付办公室 PC（电源管理）
- 交付办公室 PC（非电源管理）



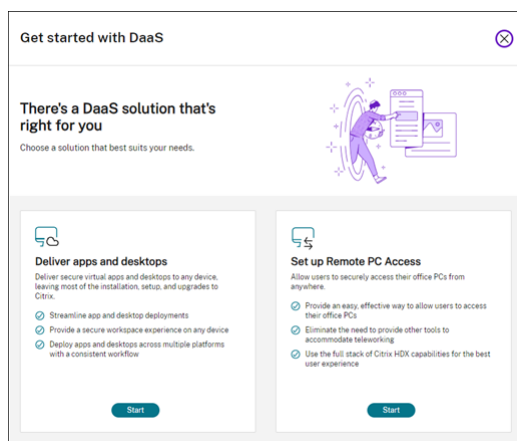
## 术语

以下是 DaaS 的特定术语：

- 资源位置。包含向用户交付应用程序和桌面所需的资源。
- 主机连接。将 DaaS 连接到资源位置的主机（虚拟机管理程序或云服务）。要在主机上创建和管理计算机或对现有计算机进行电源管理时，需要创建主机连接。
- 主映像。用作在主机上复制虚拟机的模板。它包括操作系统、应用程序、Virtual Delivery Agent (VDA) 和其他软件。
- 计算机目录。收集相同的计算机。它们可以是虚拟的，也可以是物理的，具体取决于您的需求。您可以创建计算机目录以在主机上创建配置相同的计算机，也可以将计算机导入 DaaS 进行管理。
- 交付组。包含来自计算机目录的计算机。此外，它还指定哪些用户可以使用这些计算机以及这些用户可以使用哪些应用程序和桌面。
- 计算机配置文件。指定虚拟机的属性。目录中的虚拟机可以继承计算机配置文件的属性。

## 访问指南

1. 转到 **DaaS >** 主页。
2. 找到 **DaaS** 入门。
3. 单击“开始”以启动部署流程。



注意：

您可以随时单击“关闭”退出该进程，指南会自动保存您的设置。要继续配置，请单击“继续”。要重新开始，请单击“重新开始”。

## 从头开始交付应用程序和桌面（电源管理）

本节指导您完成创建虚拟机以及使用虚拟机交付应用程序和桌面的部署过程。

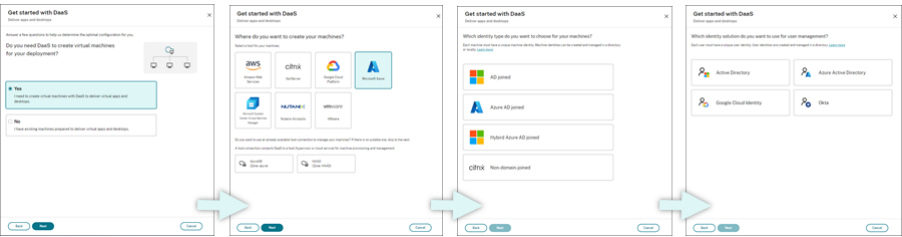
必备条件

在开始之前，您需要：

- 从 Citrix Cloud 连接到目标身份提供商  
有关更多信息，请参阅 [身份提供商](#) 中的相应部分。
- 角色：完全权限管理员或云管理员
- 目标虚拟机管理程序或云服务所需的权限。  
有关更多信息，请参阅 [创建和管理连接](#) 中的相应部分。
- 用于创建 VM 帐户的管理员凭据

准备

回答屏幕上的问题以完成以下基础结构级别的设置。有关详细信息，请参阅下表。

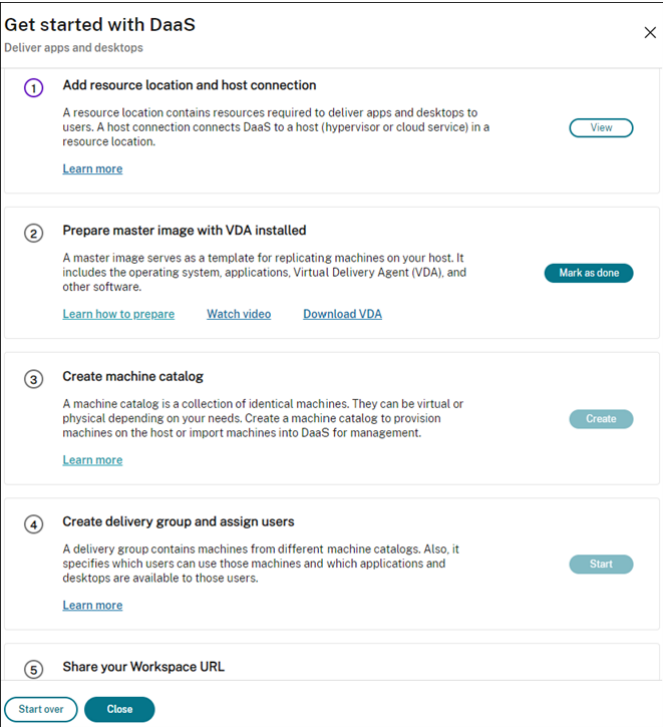


#	设置	说明
1	指定是否需要创建 VM	选择是。
2	选择主机类型	为您的部署选择主机类型。  选项：AWS、XenServer（前身为 Citrix Hypervisor）、Google 云端平台、Microsoft Azure、Microsoft System Center Virtual Machine Manager、Nutanix Acropolis 和 VMware
3	选择计算机标识类型	为计算机管理选择身份类型。  选项：已加入 AD、已加入 Azure AD、已加入混合 Azure AD 和未加入域
4	选择用户身份类型	为用户管理选择身份类型。

#	设置	说明
		选项：Active Directory、Azure Active Directory、Google Cloud Identity 和 Okta

部署步骤

完成基础结构级别设置后，特定于该部署方案的步骤如下所示。



按照屏幕上的说明完成设置。

**步骤 1：**添加资源位置和主机连接 通过安装 Cloud Connector 来设置您的资源位置，并在该位置配置与虚拟机管理程序或云服务的连接。

- 命名资源位置。
- 在至少两台 Windows Server 计算机上下载并安装 Cloud Connector。
- 检测安装的 Cloud Connector。
- 为资源位置添加和配置主机连接。连接的详细设置包括：
  - 连接详细信息，例如连接地址、用户名和密码。
  - 存储资源

- 网络资源

注意：

DaaS 通过这些连接在主机上创建和管理虚拟机。创建计算机目录时必须指定连接。

**步骤 2：**为您的计算机准备主映像 在资源位置的 VM 上准备主映像。有关更多信息，请参阅[在虚拟机管理程序或云服务上准备主映像](#)。

**步骤 3：**创建计算机目录 创建计算机目录以在主机上创建一组配置相同的计算机。详细步骤如下所示：

1. 命名目录。

2. 选择计算机类型。

选项：多会话、单会话静态（个人桌面）和单会话随机（池桌面）。

3. 选择主机连接。

选项来自您在步骤 1 中为资源位置配置的所有主机连接。

4. 选择主映像。

5. 选择计算机配置文件。

注意：

计算机配置文件支持目前可用于 Azure、GCP 和 AWS 云服务，GCP 可以选择使用计算机配置文件。

6. 设置要创建多少台计算机。

7. 设置计算机身份。

默认情况下，显示您在准备阶段选择的计算机身份类型。为虚拟机提供所需的身份设置，例如域、组织单位和命名方案。

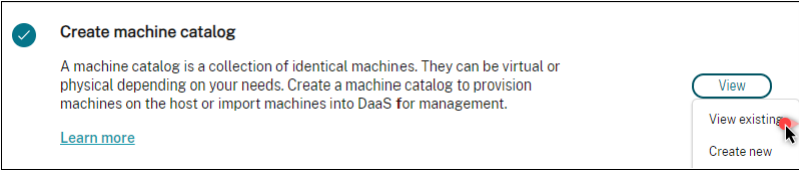
8. 输入创建计算机所需的管理员凭据。

9. 单击创建。

提示：

只有在您提供所有必需的设置后，“创建”按钮才可用。

要查看目录创建进度，请选择查看 > 查看现有。



**步骤 4：创建交付组并分配用户**

提示：

在创建交付组之前，请查看现有目录以确保已成功创建至少一个目录。否则，您将无法创建交付组。

创建交付组包括以下子任务：

- 将 VM 添加到组中
  - 将用户分配到组
  - 指定要向分配的用户提供哪些应用程序和桌面
1. 为组命名。
  2. 通过选择计算机目录并指定该组有多少虚拟机可用，将计算机添加到组中。
  3. 为该组指定可用的应用程序和桌面：
    - 要从所选目录中正在运行的计算机中添加应用程序，请单击新增 > 从“开始”菜单。
    - 要添加部署在网络共享上的应用程序，请单击“新增” > “手动”，然后提供所需的设置，例如路径、工作目录等。
    - （仅在多会话操作系统计算机上可见）对于桌面交付，请选中“启用桌面交付”。
  4. 在此组中添加可以访问应用程序和桌面的用户。

**第 5 步：**与用户共享 **Workspace URL** 转到 Workspace 配置 > 访问，然后与用户共享 Workspace URL

**使用现有计算机交付应用程序和桌面（电源管理）**

本节指导您完成使用现有计算机（电源管理）交付应用程序和桌面的部署过程。

**必备条件**

在开始之前，您需要：

- 从 Citrix Cloud 连接到目标身份提供商  
有关更多信息，请参阅 [身份提供商](#) 中的相应部分。
- 角色：完全权限管理员或云管理员

**准备**

回答屏幕上的问题以完成以下基础结构级别的设置。

#	设置	说明
1	指定是否需要创建 VM	选择“否”。
2	选择是否需要电源管理	选择进行电源管理的计算机 (例如，虚拟机或刀片式 <b>PC</b> )。
3	选择主机平台	选择现有计算机所在的主机平台。  选项：AWS、Citrix、Google 云端平台、Microsoft Azure、Microsoft System Center Virtual Machine Manager、Nutanix Acropolis 和 VMware
4	选择用户身份类型	为用户管理选择身份类型。  选项：Active Directory、Azure Active Directory、Google Cloud Identity 和 Okta

部署步骤

完成基础结构级别设置后，将显示特定于该部署方案的步骤。按照屏幕上的说明完成设置。

**步骤 1：**添加资源位置和主机连接 通过安装 Cloud Connector 来设置您的资源位置，并在您的位置配置与虚拟机管理程序或云服务的连接。

- 1. 命名资源位置。
- 2. 在至少两台 Windows Server 计算机上下载并安装 Cloud Connector。
- 3. 检测安装的 Cloud Connector。
- 4. 为资源位置添加和配置主机连接。连接设置的示例包括连接地址、用户名和密码。

注意：

DaaS 通过连接管理资源位置中的计算机。将计算机导入目录时，您需要指定连接。

**步骤 2：**创建计算机目录 创建计算机目录并将您的计算机导入其中。

- 1. 命名目录
- 2. 选择计算机类型。  
  
选项：多会话、单会话静态（个人桌面）和单会话随机（池桌面）。
- 3. 选择资源位置。

4. 将计算机导入目录。

计算机按主机连接进行组织。选择主机连接来导入关联计算机。

5. 单击创建。

**步骤 3：**创建交付组并分配用户 要创建交付组，您必须：

- 将 VM 添加到组中
  - 将用户分配到组
  - 指定要向分配的用户提供哪些应用程序和桌面
1. 为组命名。
  2. 根据需要选择计算机目录，然后指定交付组有多少台计算机可用。
  3. 为该组指定可用的应用程序和桌面：
    - 要从所选目录中正在运行的计算机中添加应用程序，请单击新增 > 从“开始”菜单。
    - 要添加部署在网络共享上的应用程序，请单击“新增” > “手动”，然后提供所需的设置，例如路径、工作目录等。
    - （仅在多会话操作系统计算机上可见）对于桌面交付，请选中“启用桌面交付”。
  4. 将用户添加到组中。

**步骤 4：**与用户共享 **Workspace URL** 转到 **Workspace** 配置 > 访问，然后与用户共享 Workspace URL。

## 使用现有计算机（非电源管理）交付应用程序和桌面

本节指导您完成使用现有计算机（非电源管理）交付应用程序和桌面的部署过程。

### 必备条件

在开始之前，您需要：

- 从 Citrix Cloud 连接到目标身份提供商  
有关更多信息，请参阅[身份提供商](#)中的相应部分
- 角色：完全权限管理员或云管理员

### 准备

回答屏幕上的问题以完成以下基础结构级别的设置。



#	设置	说明
1	指定是否需要创建 VM	选择“否”。
2	选择是否需要电源管理	选择 不受电源管理的计算机（例如，物理机）。
3	选择用户身份类型	为用户管理选择身份类型。  选项：Active Directory、Azure Active Directory、Google Cloud Identity 和 Okta

部署步骤

完成基础结构级别设置后，将显示特定于该部署方案的步骤。按照屏幕上的说明完成设置。

**步骤 1：添加资源位置** 通过安装 Cloud Connector 来设置您的资源位置。

1. 命名资源位置。
2. 在至少两台 Windows Server 计算机上下载并安装 Cloud Connector。
3. 检测安装的 Cloud Connector。

注意：

只有当您想要对计算机进行电源管理时，才需要创建主机连接。

**步骤 2：创建计算机目录** 创建计算机目录并将您的计算机导入其中。

1. 命名目录
2. 选择计算机类型。  
  
选项：多会话、单会话静态（个人桌面）和单会话随机（池桌面）。
3. 选择资源位置。
4. 将计算机导入目录。  
  
要简化计算机搜索，请使用部分计算机名称和目录选择。
5. 单击创建。

**步骤 3：创建交付组并分配用户** 要创建交付组，您必须：

- 将 VM 添加到组中

- 将用户分配到组
  - 指定要向分配的用户提供哪些应用程序和桌面
1. 为组命名。
  2. 根据需要选择计算机目录，然后指定交付组有多少台计算机可用。
  3. 为该组指定可用的应用程序和桌面：
    - 要从所选目录中正在运行的计算机中添加应用程序，请单击新增 > 从“开始”菜单。
    - 要添加部署在网络共享上的应用程序，请单击“新增” > “手动”，然后提供所需的设置，例如路径、工作目录等。
    - （仅在多会话操作系统计算机上可见）对于桌面交付，请选中“启用桌面交付”。
  4. 将用户添加到组中。

**步骤 4：**与用户共享 **Workspace URL** 转到 **Workspace** 配置 > 访问，然后与用户共享 Workspace URL。

交付办公室 **PC**（电源管理）

本节指导您完成交付办公室 PC（电源管理）的部署过程。

必备条件

在开始之前，您需要：

- PC 的计算机名称。
  - 每台 PC 上都安装了 Citrix Virtual Delivery Agent (VDA)。（此步骤可以在创建目录后完成。）
- 有关更多信息，请参阅[下载 VDA](#)。

准备

回答屏幕上的问题以完成以下基础结构级别的设置。

#	步骤	说明
1	选择计算机分配类型。	选择计算机的分配方式。  选项：静态自动分配、静态预分配和随机池未分配
2	确定是否允许用户打开计算机电源	选择“我希望远程用户自己开机”。
3	选择用户身份类型	为用户管理选择身份类型。

#	步骤	说明
		选项: Active Directory、Azure Active Directory、Google Cloud Identity 和 Okta

部署步骤

完成基础结构级别设置后，将显示特定于该部署方案的步骤。按照屏幕上的说明完成设置。

**步骤 1:** 添加资源位置和主机连接 通过安装 Cloud Connector 来设置资源位置，然后添加 “**Remote PC** 局域网唤醒” 类型的连接。

- 命名资源位置。
- 在至少两台 Windows Server 计算机上下载并安装 Cloud Connector。
- 检测安装的 Cloud Connector。
- 单击“新增”以添加连接：
  - 选择资源位置（区域）。
  - 在“连接类型”中选择 “**Remote PC** 局域网唤醒”。
  - 输入连接的名称。

注意：

DaaS 通过配置的连接对计算机进行电源管理。在为电源管理计算机创建 Remote PC Access 目录时，必须配置 “**Remote PC** 局域网唤醒” 类型的连接。

**步骤 2:** 创建 **Remote PC Access** 目录 创建计算机目录并将您的办公室 PC 导入其中。

- 命名目录
- 选择资源位置。
- 选择计算机分配类型。默认情况下，显示您在准备阶段选择的类型。
- 选择“局域网唤醒”连接。选项是您为所选位置配置的 “**Remote PC** 局域网唤醒” 类型的连接。
- 导入您的计算机。
- 单击创建。

**步骤 3:** 创建交付组并分配用户 创建交付组以对要交付的计算机进行分组，并指定谁可以访问这些计算机。

- 为组命名。
- 根据需要选择计算机目录。只显示 “**Remote PC Access**” 目录。
- 将用户分配到组。

**步骤 4:** 与用户共享 **Workspace URL** 转到 **Workspace** 配置 > 访问，然后与用户共享 Workspace URL。

交付办公室 **PC**（非电源管理）

本节指导您完成交付办公室 PC（非电源管理）的部署过程。

必备条件

在开始之前，您需要：

- PC 的计算机名称。
- 每台 PC 上都安装了 Citrix Virtual Delivery Agent (VDA)。（此步骤可以在创建目录后完成。）

有关更多信息，请参阅[下载 VDA](#)。

准备

回答屏幕上的问题以完成以下基础结构级别的设置。

#	设置	说明
1	选择计算机分配类型。	选择计算机的分配方式。  选项：静态自动分配、静态预分配和随机池未分配
2	确定是否允许用户打开计算机电源	继续清除“我希望远程用户自己开机”。
3	选择用户身份类型	为用户管理选择身份类型。  选项：Active Directory、Azure Active Directory、Google Cloud Identity 和 Okta

部署步骤

完成基础结构级别设置后，将显示特定于该部署方案的步骤。按照屏幕上的说明完成设置。

**步骤 1:** 添加资源位置 通过安装 Cloud Connector 来设置您的资源位置。

1. 命名资源位置。
2. 在至少两台 Windows Server 计算机上下载并安装 Cloud Connector。
3. 检测安装的 Cloud Connector。

**注意：**

只有当您想要对计算机进行电源管理时，才需要创建主机连接。

**步骤 2：创建 Remote PC Access 目录** 创建目录并将您的办公室 PC 导入其中。

- 1. 命名目录
- 2. 选择资源位置。
- 3. 选择分配类型。默认情况下，显示您在准备阶段选择的类型。
- 4. 导入您的计算机。
- 5. 单击创建。

**步骤 3：创建交付组并分配用户** 为要交付的计算机创建交付组，并指定谁可以访问它们。

- 1. 为组命名。
- 2. 根据需要选择计算机目录。只显示 “Remote PC Access” 目录。
- 3. 为组分配用户。

**步骤 4：与用户共享 Workspace URL** 转到 Workspace 配置 > 访问，然后与用户共享 Workspace URL。

计算机标识

October 26, 2023

每台计算机都必须具有唯一的计算机标识，也称为计算机帐户。可以在本地计算机或目录中创建和管理计算机标识，例如本地 Active Directory (AD) 或 Azure AD。Citrix 支持在加入了 Active Directory、加入了 Azure Active Directory、加入了混合 Azure Active Directory 或未加入域的计算机上托管虚拟应用程序和桌面。

计算机身份类型

支持以下计算机标识类型。

计算机身份类型	说明
已加入 AD	标识是在本地 Active Directory 中创建和管理的。置备的计算机使用分配的计算机标识加入本地 Active Directory。

计算机身份类型	说明
已加入 Azure AD	身份是在 Azure AD 中创建和管理的。置备的计算机使用分配的计算机标识加入到 Azure AD。不支持将 VM 导入 Citrix DaaS。
已加入混合 Azure AD	身份在本地 Active Directory 中创建，并通过 Azure AD Connect 与 Azure AD 同步。置备的计算机将加入本地 Active Directory 和 Azure AD。然后，这些计算机将加入混合 Azure AD。要导入加入混合 Azure AD 的虚拟机，Citrix DaaS 会将该虚拟机视为加入了 Active Directory 的虚拟机。
未加入域	身份是在本地计算机中创建和管理的。不支持将 VM 导入 Citrix DaaS。

支持的配置

下面是每种场景支持的配置的详细信息。

支持的基础结构

计算机标识	Citrix DaaS	Citrix Workspace	Citrix StoreFront	Citrix Gateway 服务	Citrix Gateway
已加入 AD	是	是	是	是	是
已加入 Azure AD	是	是	否	是	否
已加入混合 Azure AD	是	是	是	是	是
未加入域	是	是	是	是	是

注意

使用 StoreFront 时，本地主机缓存和服务连续性均不适用于非域加入的会话主机。

支持的 **Workspace** 身份验证身份提供程序

计算机标识	Azure Active Directory	Active Directory	Active Directory 和令牌	Okta	SAML	Citrix Gateway	自适应身份 验证
已加入 AD	是	是	是	是	是	是	是
已加入 Azure AD	是	否	否	否	否	否	否
已加入混合 Azure AD	是	是	是	是	是	是	是
未加入域	是	是	是	是	是	是	是

### 已加入 Active Directory

July 3, 2023

标识是在本地 Active Directory 中创建和管理的。置备的计算机使用分配的计算机标识加入本地 Active Directory。有关林和域支持的功能级别的更多信息，请参阅 [Active Directory 功能级别](#)。

有关如何使用 Citrix DaaS 创建 Active Directory (AD) 加入目录的信息，请参阅 [创建计算机目录](#)。

### 已加入 Azure Active Directory

August 14, 2023

除了 Citrix DaaS 系统要求部分中概述的要求外，本文还介绍了使用 Citrix DaaS 创建 Azure Active Directory (AAD) 加入目录的要求。

#### 要求

- 控制平面：参阅[支持的配置](#)
- VDA 类型：单会话（仅限桌面）或多会话（应用程序和桌面）
- VDA 版本：2203 或更高版本
- 配置类型：Machine Creation Services (MCS)、使用计算机配置文件工作流的持久和非持续
- 分配类型：专用和池
- 托管平台：仅限 Azure
- 必须启用 Rendezvous V2



## 限制

- 不支持服务连续性。
- 不支持单点登录到虚拟桌面。用户在登录桌面时必须手动输入凭据。
- 不支持在虚拟桌面中使用 Windows Hello 进行登录。目前仅支持用户名和密码。如果用户尝试使用任何 Windows Hello 方法登录，则他们会收到一条错误消息，指出他们不是代理用户，并且会话已断开连接。关联的方法包括 PIN、FIDO2 密钥、MFA 等。
- 仅支持 Microsoft Azure Resource Manager 云环境。
- 首次启动虚拟桌面会话时，Windows 登录屏幕可能会显示上次登录的用户的登录提示，但无法选择切换到其他用户。用户必须等到登录超时并且出现桌面的锁定屏幕，然后单击锁定屏幕以再次显示登录屏幕。此时，用户可以选择“其他用户”并输入其凭据。当计算机处于非持久状态时，每个新会话都会出现这种行为。

## 注意事项

### 映像配置

- 请考虑使用 [Citrix Optimizer](#) 工具优化 Windows 映像。

## Azure AD 已加入

- 考虑禁用 Windows Hello，这样用户在登录虚拟桌面时就不会被提示进行设置。如果您使用的是 VDA 2209 或更高版本，则会自动完成。对于早期版本，您可以通过以下两种方式之一执行此操作：
  - 组策略或本地策略
    - ★ 导航到计算机配置 > 管理模板 > **Windows 组件** > **Windows Hello 企业版**。
    - ★ 将使用 **Windows Hello 企业版** 设置为：
      - 已禁用，或者
      - 已启用，然后选择 **Do not start Windows Hello provisioning after sign-in**（登录后不启动 Windows Hello 预配）。
  - Microsoft Intune
    - ★ 创建用于禁用 Windows Hello 企业版的设备配置文件。请参阅 [Microsoft 文档](#) 了解详细信息。
    - ★ 目前，Microsoft 仅支持静态计算机的 Intune 注册，这意味着您无法使用 Intune 管理非静态计算机。
- 必须授予用户在 Azure 中的显式访问权限，才能使用其 AAD 凭据登录计算机。这可以通过在资源组级别添加角色分配来实现：
  1. 登录 Azure 门户。
  2. 选择资源组。

3. 单击虚拟桌面工作负载所在的资源组。
4. 选择 访问控制 (**IAM**)。
5. 单击 **Add role assignment** (添加角色分配)。
6. 搜索 **Virtual Machine User Login** (虚拟机用户登录)，在列表中将其选中，然后单击下一步。
7. 选择 **User, group, or service principal** (用户、组或服务主体)。
8. 单击 **Select members** (选择成员)，然后选择要提供虚拟桌面访问权限的用户和组。
9. 单击 **Select** (选择)。
10. 单击 **Review + assign** (检查 + 分配)。
11. 再次单击 **Review + assign** (检查 + 分配)。

注意：

如果选择让 MCS 为虚拟桌面创建资源组，则可以在创建计算机目录后添加此角色分配。

- 主 VM 可以已加入 Azure AD，也可以未加入域。此功能需要 VDA 版本 2212 或更高版本。

## VDA 安装和配置

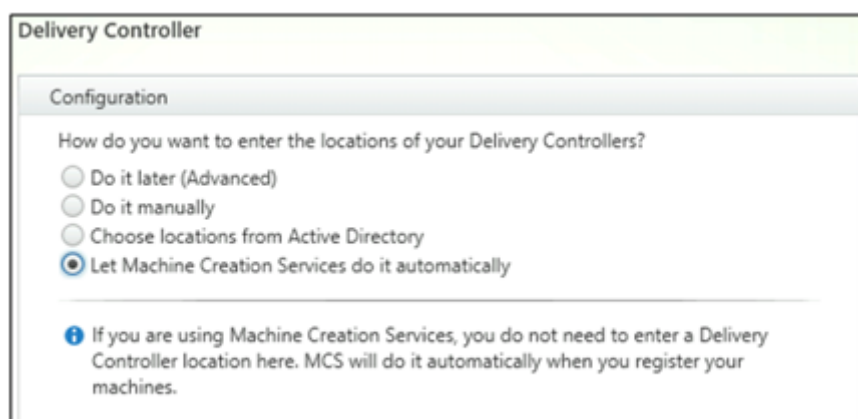
请按照安装 VDA 的步骤进行操作：

1. 请务必在安装向导中选择以下选项：
  - 在“环境”页面中，选择创建主 **MCS** 映像。



(Azure AD 配置 1)

- 在“Delivery Controller”页面中，选择让 **Machine Creation Services** 自动创建。



(Azure AD 配置 2)

2. 安装 VDA 后，添加以下注册表值：

- 注册表项：HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
- 值类型：DWORD
- 值名称：GctRegistration
- 值数据：1

3. 对于基于 Windows 11 22H2 的主虚拟机，在主 VM 中创建计划任务，该任务在系统启动时使用系统帐户执行以下命令。只有 VDA 版本 2212 或更早版本才需要在主虚拟机中安排任务的任务。

```
1 reg ADD HKLM\Software\AzureAD\VirtualDesktop /v Provider /t REG_SZ
   /d Citrix /f
2 <!--NeedCopy-->
```

4. 如果您将主虚拟机加入到 Azure AD，然后通过 `dsregcmd` 实用程序手动删除加入，请确保 HKLM\Software\Microsoft\Windows Azure\CurrentVersion\AADLoginForWindowsExtension 下 `AADLoginForWindowsExtensionJoined` 的值为零。

下一步的去向

资源位置和主机连接可用后，请继续创建计算机目录。有关创建已加入 Azure Active Directory 的计算机目录的详细信息，请参阅[创建已加入 Azure Active Directory 的目录](#)。

## Microsoft Intune

March 5, 2024

除了 Citrix DaaS 系统要求部分中概述的要求外，本文还介绍了使用 Citrix DaaS 创建支持 Microsoft Intune 的目录的要求。

Microsoft Intune 是一项基于云的服务，专注于移动设备管理 (MDM) 和移动应用程序管理 (MAM)。您可以控制组织设备的使用方式，包括手机、平板电脑和笔记本电脑。有关更多信息，请参阅 [Microsoft Intune](#)。设备必须满足最低系统要求。有关更多信息，请参阅 Microsoft 文档 [Intune 中支持的操作系统和浏览器](#)。

Microsoft Intune 通过使用 Azure AD 的功能来工作。

**重要提示：**

在启用此功能之前，请验证您的 Azure 环境是否符合使用 Microsoft Intune 的许可要求。有关详细信息，请参阅 Microsoft 文档：<https://docs.microsoft.com/en-us/mem/intune/fundamentals/licenses>。如果您没有相应的 Intune 许可证，请不要启用该功能。

## 要求

- 控制平面：Citrix DaaS
- VDA 类型：单会话操作系统 VDA
- VDA 版本：2203 或更高版本
- 预配类型：Machine Creation Services (MCS) 持续，仅使用计算机配置文件工作流程
- 任务类型：专用

## 限制

- 仅支持单会话 Azure AD 加入的永久虚拟机。
- 仅支持使用用户凭据或具有共同管理功能的设备凭据加入永久 VM 的单会话混合 Azure AD。有关详细信息，请参阅[使用组策略自动注册 Windows 设备](#)。
- 创建或更新计算机目录时，请勿跳过映像准备工作。

## 注意事项

- 创建用于禁用 Windows Hello 企业版的设备配置文件。
- 如果 Microsoft Intune 必须管理主 VM，请使用 VDA 版本 2212 或更高版本。

## 下一步的去向

有关创建启用 Microsoft Intune 的目录的信息，请参阅[创建启用了 Microsoft Intune 的目录](#)。

## 已加入混合 **Azure Active Directory**

April 11, 2023

除了 Citrix DaaS 系统要求部分中概述的要求外，本文还介绍了使用 Citrix DaaS 创建混合 Azure Active Directory (HAAD) 加入目录的要求。

已加入 Azure AD 的混合计算机使用本地 AD 作为身份验证提供程序。您可以将它们分配给本地 AD 中的域用户或组。要启用 Azure AD 无缝 SSO 体验，您需要将域用户同步到 Azure AD。

### 注意：

联合身份基础架构和托管身份基础架构均支持加入 Azure AD 的混合 VM。

## 要求

- 控制平面：参阅[支持的配置](#)
- VDA 类型：单会话（仅限桌面）或多会话（应用程序和桌面）
- VDA 版本：2212 或更高版本
- 配置类型：Machine Creation Services (MCS)、持久和非持久
- 分配类型：专用和池
- 托管平台：任何虚拟机管理程序或云服务

## 限制

- 如果使用 Citrix 联合身份验证服务 (FAS)，则单点登录将定向到本地 AD 而不是 Azure AD。在这种情况下，建议配置基于 Azure AD 证书的身份验证，以便在用户登录时生成主刷新令牌 (PRT)，这有助于在会话中单点登录到 Azure AD 资源。否则，PRT 将不存在，Azure AD 资源的 SSO 也将不起作用。有关使用 Citrix 联合身份验证服务 (FAS) 实现对混合加入的 VDA 的 Azure AD 单点登录 (SSO) 的信息，请参阅[混合加入的 VDA](#)。
- 在创建或更新计算机目录时，请勿跳过映像准备工作。如果要跳过映像准备工作，请确保主 VM 未加入 Azure AD 或者未加入混合 Azure AD。

## 注意事项

- 创建已加入混合 Azure Active Directory 的计算机需要目标域中的 **Write userCertificate** 权限。请确保在创建目录期间输入具有该权限的管理员的凭据。
- 混合 Azure AD 加入过程由 Citrix 管理。您需要在主 VM 中禁用由 Windows 控制的 **autoWorkplaceJoin** 功能，如下所示。只有在 VDA 版本 2212 或更早版本中才需要手动禁用 **autoWorkplaceJoin**。
  1. 运行 **gpedit.msc**。
  2. 导航到 **计算机配置 > 管理模板 > Windows 组件 > 设备注册**。
  3. 将“将加入域的计算机注册为设备”设置为“已禁用”。
- 选择在创建计算机标识时配置为与 Azure AD 同步的组织单位 (OU)。

- 对于基于 Windows 11 22H2 的主虚拟机，在主虚拟机中创建计划任务，该任务在系统启动时使用系统帐户执行以下命令。只有 VDA 版本 2212 或更早版本才需要在主虚拟机中安排任务的任务。

```
1 $VirtualDesktopKeyPath = 'HKLM:\Software\AzureAD\VirtualDesktop'
2 $WorkplaceJoinKeyPath = 'HKLM:\SOFTWARE\Policies\Microsoft\
   Windows\WorkplaceJoin'
3 $MaxCount = 60
4
5 for ($count = 1; $count -le $MaxCount; $count++)
6 {
7
8     if ((Test-Path -Path $VirtualDesktopKeyPath) -eq $true)
9     {
10
11         $provider = (Get-Item -Path $VirtualDesktopKeyPath).GetValue(
12             "Provider", $null)
13         if ($provider -eq 'Citrix')
14         {
15             break;
16         }
17
18         if ($provider -eq 1)
19         {
20
21             Set-ItemProperty -Path $VirtualDesktopKeyPath -Name "
22                 Provider" -Value "Citrix" -Force
23             Set-ItemProperty -Path $WorkplaceJoinKeyPath -Name "
24                 autoWorkplaceJoin" -Value 1 -Force
25             Start-Sleep 5
26             dsregcmd /join
27             break
28         }
29     }
30
31     Start-Sleep 1
32 }
33
34
35 <!--NeedCopy-->
```

## 下一步的去向

有关创建已加入混合 Azure Active Directory 的目录的详细信息，请参阅[创建已加入混合 Azure Active Directory 的目录](#)。

## 未加入域

November 16, 2023

除了 Citrix DaaS 系统要求部分中概述的要求外，本文还介绍了使用 Citrix DaaS 创建未加入域的目录的要求。

### 要求

- 控制平面：参阅[支持的配置](#)
- VDA 类型：单会话（仅限桌面）或多会话（应用程序和桌面）
- VDA 版本：2203 或更高版本
- 配置类型：Machine Creation Services (MCS)、持久和非持久
- 分配类型：专用和池
- 托管平台：MCS 支持的所有平台
- 必须启用 Rendezvous V2
- Cloud Connector：仅当您计划在本地虚拟机管理程序上预置计算机或要在 Workspace 中使用 Active Directory 作为身份提供商时才需要。

### 限制

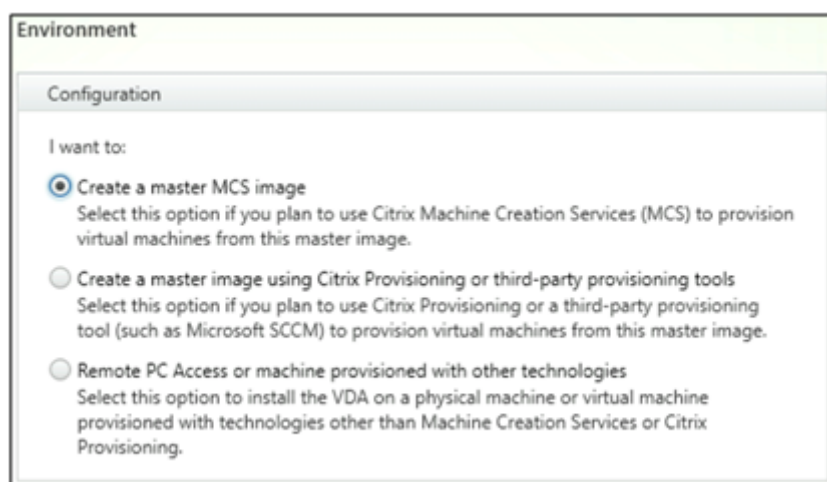
- 不支持服务连续性。
- 每当我们使用多会话非域加入 VDA 时，本地用户的个人资料数据都不会被保留，会在注销时被删除。

## VDA 安装和配置

请按照安装 VDA 的步骤进行操作：

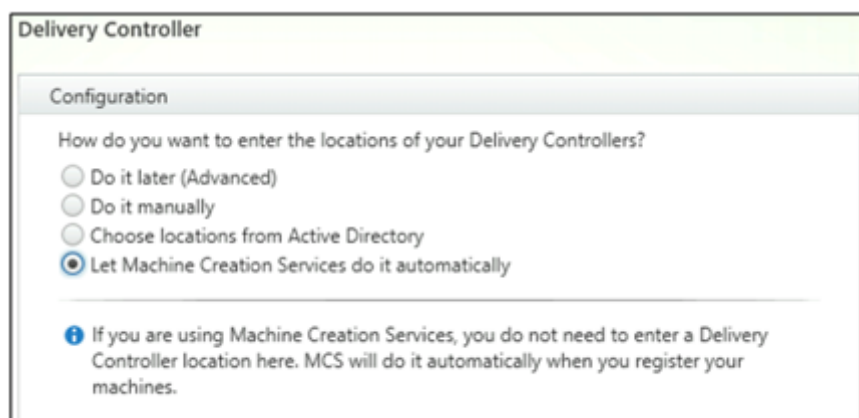
1. 请务必在安装向导中选择以下选项：
  - 在“环境”页面中，选择创建主 **MCS** 映像。





(Azure AD 配置 1)

- 在“Delivery Controller”页面中，选择让 **Machine Creation Services** 自动创建。



(Azure AD 配置 2)

2. 安装 VDA 后，添加以下注册表值：

- 注册表项：HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
- 值类型：DWORD
- 值名称：GctRegistration
- 值数据：1

下一步的去向

资源位置和主机连接可用后，请继续创建计算机目录。有关创建未加入域的计算机目录的更多信息，请参阅 [创建未加入域的目录](#)。

## 设置资源位置

January 23, 2024

资源位置中包含向用户交付应用程序和桌面所需的资源。您可以管理来自 Citrix Cloud 的资源。资源通常包括：

- 虚拟机管理程序或云服务，称为主机，包括：
  - Active Directory 域控制器
  - 虚拟交付代理 (VDA)：VDA 安装在向用户交付应用程序和桌面的计算机上。
  - Citrix Gateway（可选）：要启用对提供给用户的应用程序和桌面的安全外部访问，请向资源位置中添加一个 Citrix Gateway VPX 设备。然后，设置 Citrix Gateway。
  - Citrix StoreFront 服务器。
  - 每个资源位置都必须包含一个 Citrix Cloud Connector，才能与 Citrix Cloud 通信。建议每个资源位置至少使用两个 Cloud Connector。

区域与资源位置等效。创建资源位置并安装 Cloud Connector 时，将自动为您创建一个区域。有关详细信息，请参阅[区域](#)。

要了解有关资源类型的详细信息，请参阅[连接到 Citrix Cloud](#)。

## 主机要求

在其中配置虚拟机的虚拟机管理程序或云服务需要独特的权限或设置。

- 如果虚拟机管理程序或云服务需要虚拟网络，请按照其文档中的指南进行操作。
- 为要添加到资源位置的计算机创建相应的虚拟专用云 (VPC)（适用于 AWS 或 GCP）或虚拟网络 (VNET)（适用于 Azure）。
- 创建适当的规则来保护虚拟网络中计算机之间的入站和出站流量。例如，在使用 AWS 时，请确保 VPC 的安全组配置了相应的规则，这样只有您指定的 IP 地址才能访问 VPC 中的计算机。

支持以下主机类型：

- Amazon Web Services (AWS) 虚拟化环境
- XenServer 虚拟化环境
- Google 云端平台虚拟化环境
- Microsoft Azure Resource Manager 虚拟化环境
- Microsoft System Center Virtual Machine Manager 虚拟化环境
- Nutanix 虚拟化环境
- Nutanix 云和合作伙伴解决方案
- VMware 虚拟化环境
- VMware 云和合作伙伴解决方案

## Active Directory

配置 Windows 服务器，安装 Active Directory 域服务 (AD DS)，并将其升级为域控制器。有关指导，请参阅关于 [Active Directory 域服务概述](#) 有关的 Microsoft 文档。

重要注意事项如下：

- 必须至少有一个域控制器运行 Active Directory 域服务。
- 不要在域控制器上安装任何 Citrix 组件。

有关详细信息，请参阅：

- [Active Directory 功能级别](#)
- Citrix Cloud 中的[身份和访问管理](#)。
- [将 Active Directory 连接到 Citrix Cloud](#)
- [将 Connector Appliance 与 Active Directory 配合使用的部署方案](#)

## Cloud Connector

Cloud Connector 是 Citrix Cloud 提供的一组服务，允许在 VDA、StoreFront 和基于云的 Delivery Controller 之间进行通信。可以交互式安装 Cloud Connector，也可以从命令行安装。

有关 Cloud Connector 的更多信息，请参阅：

- [Citrix Cloud Connector](#)
- [技术详细信息](#)
- [代理和防火墙配置](#)
- [Installation](#)
- [Connector 更新](#)

大小和规模注意事项

- 在评估 Citrix DaaS 以确定规模和可扩展性时，请考虑所有组件。
- 研究和测试 Cloud Connector 和 StoreFront 的配置，以满足您的特定需求。
- 缩小计算机大小会对系统性能产生负面影响。

[Cloud Connector 的大小和规模注意事项](#)一文包括：

- 尺寸和规模测试信息
- 测试的最大容量
- Cloud Connector 计算机配置的最佳实践建议

## 添加资源类型

1. 登录 [Citrix Cloud](#)。
2. 在右上角的菜单中，选择资源位置。
3. 选择 **+** 资源位置以添加资源位置。
4. 输入资源位置的名称，然后单击“保存”。有关命名注意事项的信息，请参阅[名称限制](#)。
5. 在新资源位置下，选择 **+ Cloud Connector**。
6. 在您拥有 Citrix DaaS 资源的域中的至少两台服务器上下载并安装 Cloud Connector 软件。
  - 在安装过程中，选择您在前面的步骤中创建的资源位置。
  - 安装后，Citrix Cloud 将服务器添加到资源位置，并注册安装了 Cloud Connector 的域。
7. 验证注册的域是否处于活动状态：
  - 在 Citrix Cloud 菜单中，选择 **Identity Access Management**（身份访问管理）。
  - 选择域。此时将显示部署了 Cloud Connector 的域列表。
  - 找到您在 Citrix DaaS 中使用的域。活动域在域条目左侧显示并且带有一个绿条。

如果您的域名没有可视指示器，则该域处于未使用状态。如果在计算机目录设置期间指定了未使用的域，目录创建将失败。为确保计算机目录设置没有错误，请按照激活未使用的域中的步骤进行操作。

有关详细信息，请参阅 [CTX473009: DaaS Catalog Creation Wizard: “Internal Server Error” when creating adding new machine accounts](#) (CTX473009: DaaS 目录创建向导：创建添加新计算机帐户时出现“内部服务器错误”)。

## 激活未使用的域名

1. 在 **Domain**（域）选项卡的 **Identity and Access Management**（身份识别和访问管理）中，选择 **Show Unused Domains**（显示未使用的域）。选择此选项后，标签将更改为 **Hide Unused Domains**（隐藏未使用的域）。
2. 在列表中找到未使用的域。未使用的域名在域条目左侧显示一个灰色条，在右侧显示一个单选省略号菜单。
3. 选择省略号菜单，然后选择“使用域”。灰色条变为绿色，省略号菜单更改为 **Disable**（禁用）。

## 下一步的去向

- 要进行简单的概念验证部署，请在指定用于向用户交付应用程序或桌面的计算机上[安装 VDA](#)。
- 要为特定主机类型设置资源位置，请执行以下操作：
  - [AWS 虚拟化环境](#)
  - [Google Cloud 虚拟化环境](#)

- [Microsoft Azure Resource Manager 虚拟化环境](#)
  - [Microsoft System Center Virtual Machine Manager 虚拟化环境](#)
  - [Nutanix 虚拟化环境](#)
  - [Nutanix 云和合作伙伴解决方案](#)
  - [VMware 虚拟化环境](#)
  - [VMware 云和合作伙伴解决方案](#)
  - [XenServer 虚拟化环境](#)
- 要进行全面部署，请[创建和管理与资源位置](#)的连接和资源。
  - [查看安装和配置过程中的所有步骤](#)

## AWS 虚拟化环境

March 30, 2024

本文介绍如何将您的 AWS 帐户设置为可用于 Citrix DaaS 的资源位置。

资源位置包括基本组件集，非常适用于不需要资源跨多个可用性区域传播的概念证明或其他部署。

完成本文中的任务时，您的资源位置包括以下组件：

- 单个可用性区域中具有公用子网和专用子网的虚拟私有云 (VPC)。
- 一个同时作为 Active Directory 域控制器和 DNS 服务器运行的实例，位于 VPC 的专用子网中。
- 安装了 Citrix Cloud Connector 的两个加入了域的实例，位于 VPC 的专用子网中。
- 用作堡垒主机的实例，位于 VPC 的公用子网中。此实例用于启动与专用子网中的实例的 RDP 连接以实现管理目的。完成设置资源位置后，可以关闭此实例，以便其不再易于访问。必须管理专用子网中的其他实例（例如 VDA 实例）时，可以重新启动堡垒主机实例。

完成任务后，您可以安装 VDA、置备计算机、创建计算机目录和创建交付组。

### 任务概述

设置具有公用子网和专用子网的虚拟私有云 (**VPC**)。当您完成此任务后，AWS 将在公有子网中部署具有弹性 IP 地址的 NAT 网关。这使得专用子网中的实例能够访问 Internet。公用子网中的实例可由入站公共流量访问，但专用子网中的实例不可访问。

配置安全组。安全组用作控制 VPC 中的实例的流量的虚拟防火墙。您负责向安全组中添加允许公共子网中的实例与专用子网中的实例进行通信的规则。您还可以将这些安全组与 VPC 中的每个实例关联起来。

创建 **DHCP** 选项集。默认提供 Amazon VPC、DHCP 和 DNS 服务，这会影响您在 Active Directory 域控制器上配置 DNS 的方式。Amazon 的 DHCP 无法禁用，并且 Amazon 的 DNS 只能用于公共 DNS 解析，而不能用于 Active

Directory 名称解析。要指定通过 DHCP 传递给实例的域和名称服务器，请创建 DHCP 选项集。该选项集将为您的 VPC 中的所有实例分配 Active Directory 域后缀并指定 DNS 服务器。要确保主机 (A) 和反向查找 (PTR) 记录在实例加入域时自动注册，请为要添加到专用子网中的每个实例配置网络适配器属性。

向 **VPC** 添加堡垒主机、域控制器和 **Cloud Connector**。通过堡垒主机，您可以登录专用子网中的实例来设置域、将实例加入域并安装 Cloud Connector。

## 任务 1：设置 VPC

1. 在 AWS 管理控制台中，选择 **VPC**。
2. 在 VPC 控制面板中，选择创建 **VPC**。
3. 选择 **VPC** 及更多。
4. 在 NAT 网关 (\$) 下，选择 **In 1 AZ** 或 **1 per AZ**。
5. 在 DNS 选项下，保持“启用 **DNS** 主机名”处于选中状态。
6. 选择创建 **VPC**。AWS 将创建公用子网和专用子网、Internet 网关、路由表和默认安全组。

### 注意：

在 AWS 控制台中更改 AWS 虚拟私有云 (VPC) 的名称会中断 Citrix Cloud 中的现有托管单元。托管单元损坏时，您将无法创建新目录，也无法将计算机添加到现有目录。来自已知问题：PMCS-7701

## 任务 2：配置安全组

此任务将为您的 VPC 创建并配置以下安全组：

- 与您的公有子网中的实例关联的公共安全组。
- 与您的专用子网中的实例关联的专用安全组。

要创建安全组，请执行以下操作：

1. 在 VPC 控制面板中，选择安全组。
2. 为公共安全组创建安全组。选择创建安全组，然后输入组的名称标记和说明。在“VPC”中，选择之前创建的 VPC。选择是，创建。

### 配置公用安全组

1. 在安全组列表中，选择“Public security group”（公用安全组）。
2. 选择入站规则选项卡，然后选择“编辑”以创建以下规则：

类型	源
所有流量	选择 “Private security group”（专用安全组）。
所有流量	选择 “Public security group”（公用安全组）。
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0
80 (HTTP)	0.0.0.0/0
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (Session Reliability) (2598（会话可靠性）)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. 完成后，选择保存。
4. 选择出站规则选项卡，然后选择编辑以创建以下规则。

类型	目标
所有流量	选择 “Private security group”（专用安全组）。
所有流量	0.0.0.0/0
ICMP	0.0.0.0/0

5. 完成后，选择保存。

配置专用安全组

1. 在安全组列表中，选择 “Private security group”（专用安全组）。
2. 如果您尚未设置来自公共安全组的流量，则必须设置 TCP 端口。选择入站规则选项卡，然后选择编辑以创建以下规则：

类型	源
所有流量	选择 “Private security group”（专用安全组）。
所有流量	选择 “Public security group”（公用安全组）。
ICMP	选择 “Public security group”（公用安全组）。



类型	源
TCP 53 (DNS)	选择 “Public security group”（公用安全组）。
UDP 53 (DNS)	选择 “Public security group”（公用安全组）。
80 (HTTP)	选择 “Public security group”（公用安全组）。
TCP 135	选择 “Public security group”（公用安全组）。
TCP 389	选择 “Public security group”（公用安全组）。
UDP 389	选择 “Public security group”（公用安全组）。
443 (HTTPS)	选择 “Public security group”（公用安全组）。
TCP 1494 (ICA/HDX)	选择 “Public security group”（公用安全组）。
TCP 2598 (Session Reliability) (TCP 2598（会话可靠性）)	选择 “Public security group”（公用安全组）。
3389 (RDP)	选择 “Public security group”（公用安全组）。
TCP 49152–65535	选择 “Public security group”（公用安全组）。

- 3. 完成后，选择 “保存”。
- 4. 选择出站规则选项卡，然后选择编辑以创建以下规则。

类型	目标
所有流量	选择 “Private security group”（专用安全组）。
所有流量	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53 (DNS)	0.0.0.0/0

- 5. 完成后，选择保存。

任务 3：启动实例

执行以下步骤创建四个 EC2 实例并解密 Amazon 生成的默认管理员密码：

- 1. 在 AWS 管理控制台中，选择 **EC2**。
- 2. 在 EC2 控制面板中，选择 **Launch Instance**（启动实例）。
- 3. 选择 Windows Server 计算机映像和实例类型。

4. 在配置实例详细信息页面上，输入实例的名称，然后选择您之前设置的 VPC。
5. 在 **Subnet**（子网）中，为每个实例做以下选择：
  - 堡垒主机：选择公有子网
  - 域控制器和连接器：选择专用子网
6. 在 **Auto-assign Public IP address**（自动分配公用 IP 地址）中，为每个实例做以下选择：
  - 堡垒主机：选择启用
  - 域控制器和连接器：选择“使用默认设置”或“禁用”
7. 在网络接口中，为域控制器和 Cloud Connector 实例输入专用子网 IP 范围内的主 IP 地址。
8. 如有必要，在添加存储页面上修改磁盘大小。
9. 在标签实例页面上，输入每个实例的友好名称。
10. 在“配置安全组”页面上，选择“选择现有安全组”，然后为每个实例进行以下选择：
  - Bastion host（堡垒主机）：选择“Public security group”（公用安全组）。
  - Domain controller and Cloud Connectors（域控制器和 Cloud Connector）：选择“Private security group”（专用安全组）。
11. 检查所做的选择，然后选择 **Launch**（启动）。
12. 创建新密钥对或选择现有密钥对。如果您创建了新的密钥对，请下载您的私钥（**.pem**）文件并将其保存在安全的地方。获取实例的默认管理员密码时，必须提供您的私钥。
13. 选择启动实例。选择“查看实例”以显示您的实例列表。请等到新启动的实例通过所有状态检查后再进行访问。
14. 获取每个实例的默认管理员密码。
  - a) 在实例列表中，选择实例，然后选择 **Connect**（连接）。
  - b) 转到 **RDP** 客户端 选项卡，选择获取密码，并在出现提示时上载您的私钥（**.pem**）文件。
  - c) 选择“解密密码”以获取人类可读的密码。AWS 将显示默认密码。
15. 重复步骤 2 中的所有步骤，直到创建了四个实例：
  - 您的公有子网中的一个堡垒主机实例
  - 您的专用子网中有三个实例可用作：
    - 一个作为域控制器
    - 两个作为 Cloud Connector

#### 任务 4：创建 **DHCP** 选项集

1. 在 VPC 控制面板中，选择 **DHCP Options Sets**（DHCP 选项集）。
2. 输入以下信息：

- **Name tag** (名称标记): 为选项集输入一个友好名称。
- **域名**: 输入配置域控制器实例时使用的完全限定域名。
- **域名服务器**: 输入您分配给域控制器实例的专用 IP 地址和字符串 **AmazonProvidedDNS**, 用逗号分隔。
- **NTP servers** (NTP 服务器): 将此字段留空。
- **NetBIOS 域名服务器**: 输入域控制器实例的专用 IP 地址。
- **NetBIOS node type** (NetBIOS 节点类型): 输入 **2**。

3. 选择是, 创建。

4. 将新选项集与您的 VPC 相关联:

- a) 在 VPC 控制面板中, 选择 **Your VPCs** (您的 VPC), 然后选择之前设置的 VPC。
- b) 依次选择 **Actions** (操作) > **Edit DHCP Options Set** (编辑 DHCP 选项集)。
- c) 出现提示时, 选择您创建的新集合, 然后选择“保存”。

## 任务 5: 配置实例

1. 使用 RDP 客户端连接到堡垒主机实例的公用 IP 地址。系统提示时, 输入管理员帐户的凭据。

2. 在堡垒主机实例中, 启动远程桌面连接并连接到要配置的实例的专用 IP 地址。系统提示时, 输入实例的管理员凭据。

3. 为专用子网中的所有实例配置 DNS 设置:

- a) 依次选择开始 > 控制面板 > 网络和 **Internet** > 网络和共享中心 > 更改适配器设置。双击显示的网络连接。
- b) 选择属性 > **Internet 协议版本 4 (TCP/IPv4)** > 属性。
- c) 选择高级 > **DNS**。确保启用以下设置, 然后选择“确定”:
  - 在 **DNS** 中注册此连接的地址
  - 在 **DNS** 注册中使用此连接的 **DNS** 后缀

4. 配置域控制器:

- a) 使用服务器管理器, 添加具有所有默认功能的 Active Directory 域服务角色。
- b) 将该实例升级为域控制器。提升过程中, 启用 DNS 并使用创建 DHCP 选项集时指定的域名。系统提示时, 重新启动实例。

5. 配置第一个 Cloud Connector:

- a) 将实例加入到域中, 并在系统提示时重新启动。在堡垒主机实例中, 使用 RDP 重新连接到实例。
- b) 登录 Citrix Cloud。在左上角的菜单中, 选择 **Resource Locations** (资源位置)。
- c) 下载 Cloud Connector。
- d) 系统提示时, 运行 `cwconnector.exe` 文件并提供您的 Citrix Cloud 凭据。按照向导提示操作。

- e) 完成后，选择“刷新”以显示“资源位置”页面。注册 Cloud Connector 时，实例将在页面上显示。
6. 重复这些步骤，配置 Cloud Connector 以配置第二个 Cloud Connector。
7. 将 IAM 策略附加到 Cloud Connector，通过基于角色的授权支持 AWS 托管连接。您必须将相同的 IAM 策略附加到资源位置中的所有 Cloud Connector。有关 AWS 权限的信息，请参阅[所需的 AWS 权限](#)。

#### 下一步的去向

- 要进行简单的概念验证部署，请在指定用于向用户交付应用程序或桌面的计算机上[安装 VDA](#)。
- 有关创建和管理连接的信息，请参阅[与 AWS 的连接](#)。
- [查看安装和配置过程中的所有步骤](#)

#### 更多信息

- [创建和管理连接和资源](#)
- [创建计算机目录](#)

## Google Cloud 虚拟化环境

March 30, 2024

Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）允许您在 Google Cloud 上预配和管理计算机。

#### 要求

- Citrix Cloud 帐户：这些功能仅在 Citrix Cloud 中可用。
- Citrix DaaS 订阅。有关详细信息，请参阅[入门](#)。
- Google Cloud 项目。该项目存储与计算机目录关联的所有计算资源。它可以是现有项目或新项目。
- 在您的 Google Cloud 项目中启用四个 API。有关详细信息，请参阅[启用 Google Cloud API](#)。
- Google Cloud 服务帐户。此服务帐户对 Google Cloud 进行身份验证，以启用对项目的访问权限。有关详细信息，请参阅[配置和更新服务帐号](#)。
- 启用 Google 专用访问权限。有关详细信息，请参阅[Enable-private-google-access](#)。

## Google Cloud 项目

Google Cloud 项目基本上有两种类型：

- 预配项目：在这种情况下，当前管理员帐户拥有项目中已预配的计算机。此项目也称为本地项目。

- 共享 VPC 项目：在预配项目中创建的计算机使用共享 VPC 项目中的 VPC 的项目。用于配置项目的管理员帐户在此项目中的权限有限，具体而言，只有使用 VPC 的权限。

## 服务端点 URL

您必须有权访问以下 URL：

- <https://oauth2.googleapis.com>
- <https://cloudresourcemanager.googleapis.com>
- <https://compute.googleapis.com>
- <https://storage.googleapis.com>
- <https://cloudbuild.googleapis.com>

## 启用 Google Cloud API

要通过 Citrix DaaS 完整配置界面使用 Google Cloud 功能，请在您的 Google Cloud 项目中启用以下 API：

- 计算引擎 API
- 云资源管理器 API
- 身份识别和访问管理 (IAM) API
- 云构建 API

在 Google Cloud 控制台中，完成以下步骤：

1. 在左上角的菜单中，选择 **API 和服务** > 已启用的 **API 和服务**。
2. 在“已启用 **API 和服务**”屏幕上，确保已启用计算引擎 API。如果没有，请按照以下步骤操作：
  - a) 导航到 **APIs and Services (API 和服务) > Library (库)**。
  - b) 在搜索框中，键入 *Compute Engine* (计算引擎)。
  - c) 从搜索结果中，选择 **Compute Engine API** (计算引擎 API)。
  - d) 在 **Compute Engine API** (计算引擎 API) 页面上，选择 **Enable** (启用)。
3. 启用云资源管理器 API。
  - a) 导航到 **APIs and Services (API 和服务) > Library (库)**。
  - b) 在搜索框中，键入 *Cloud Resource Manager* (云资源管理器)。
  - c) 在搜索结果中，选择 **Cloud Resource Manager API** (云资源管理器 API)。
  - d) 在 **Cloud Resource Manager API** (云资源管理器 API) 页面中，选择 **Enable** (启用)。此时将显示 API 的状态。
4. 同样，启用身份和访问管理 (**IAM**) API 和 **Cloud Build API** 以及云密钥管理服务 (**KMS**) API。

也可以使用 Google Cloud Shell 启用 API。为此，您需要：

1. 打开 Google 控制台并加载 Cloud Shell。
2. 在 Cloud Shell 中运行以下四个命令：
  - `gcloud services enable compute.googleapis.com`
  - `gcloud services enable cloudresourcemanager.googleapis.com`
  - `gcloud services enable iam.googleapis.com`
  - `gcloud services enable cloudbuild.googleapis.com`
  - `gcloud services enable cloudkms.googleapis.com`
3. 当 Cloud Shell 提示时，单击“授权”。

## 配置和更新服务帐户

Citrix Cloud 在 Google Cloud 项目中使用三个独立的服务帐户：

- **Citrix Cloud 服务帐户**：此服务帐户允许 Citrix Cloud 访问 Google 项目、预配和管理计算机。Google Cloud 帐户使用 Google Cloud 生成的[密钥](#)对 Citrix Cloud 进行身份验证。

您必须按照此处的说明手动创建此服务帐户。有关更多信息，请参见[创建 Citrix Cloud 服务帐户](#)。

可以使用电子邮件地址识别此服务帐户。例如，`<my-service-account>@<project-id>.iam.gserviceaccount.com`。

- **Cloud Build Service Account** (Cloud Build 服务帐户)：启用 [Enable Google Cloud APIs](#) (启用 Google Cloud API) 中提到的所有 API 后，系统会自动预配此服务帐户。要查看所有自动创建的服务帐号，请在 **Google Cloud** 控制台中导航到 **IAM 和管理 > IAM**，然后选中“包括 **Google** 提供的角色授权”复选框。

可以通过以 **Project ID** (项目 ID) 和 **cloudbuild** 一词开头的电子邮件地址来识别此服务帐户。例如，`<project-id>@cloudbuild.gserviceaccount.com`

验证服务帐号是否已被授予以下角色。如果您必须添加角色，请按照[向 Cloud Build 服务帐户添加角色](#)中概述的步骤进行操作。

- 云构建服务帐户
  - 计算实例管理员
  - 服务帐户用户
- **云计算服务帐户**：激活计算 API 后，Google Cloud 会将此服务帐户添加到在 Google Cloud 中创建的实例中。此帐户具有 IAM 基本编辑角色来执行操作。但是，如果您删除默认权限以获得更精细的控制，则必须添加需要以下权限的存储管理员角色：
    - `resourcemanager.projects.get`
    - `storage.objects.create`
    - `storage.objects.get`
    - `storage.objects.list`

您可以通过以项目 **ID** 开头的电子邮件地址和 **compute** 一词来识别此服务帐户。例如，`<project-id>-compute@developer.gserviceaccount.com`。

注意：

2024 年 4 月 29 日，GCP 将对 Cloud Build 的默认行为和新项目中服务帐号的使用进行更改。因此，您将看到本文的更改。但是，您的现有谷歌项目和 Citrix 目录不受 GCP 此次变更的影响。有关更多信息，请参阅 [Cloud Build 服务帐户变更](#)。

## 创建 Citrix Cloud 服务帐户

要创建 Citrix Cloud 服务帐户，请执行以下步骤：

1. 在 Google Cloud 控制台中，导航至 **IAM & Admin** (IAM 和管理员) > **Service accounts** (服务帐户)。
2. 在 **Service accounts** (服务帐户) 页面上，选择 **CREATE SERVICE ACCOUNT** (创建服务帐户)。
3. 在创建服务帐户页面上，输入所需信息，然后选择创建并继续。
4. 在“授予此服务帐户项目访问权限”页面上，单击“选择角色”下拉菜单并选择所需的角色。如果要添加更多角色，请单击 **+ADD ANOTHER ROLE** (+ 添加其他角色)。

每个帐户（个人或服务）都具有定义项目管理的各种角色。向此服务帐户授予以下角色：

```
1 - Compute Admin
2 - Storage Admin
3 - Cloud Build Editor
4 - Service Account User
5 - Cloud Datastore User
6 - Cloud KMS Crypto Operator
7
8 The Cloud KMS Crypto Operator requires the following permissions:
9
10 - cloudkms.cryptoKeys.get
11 - cloudkms.cryptoKeys.list
12 - cloudkms.keyRings.get
13 - cloudkms.keyRings.list
14
15 > **Note:**
16 >
17 > Enable all the APIs to get the complete list of roles available while
    creating a new service account.
```

1. 单击继续
2. 在 **Grant users access to this service account** (授予用户对此服务帐户的访问权限) 页面上，添加用户或组以授予其在此服务帐户中执行操作的权限。
3. 单击完成。
4. 导航到 IAM 主控制台。
5. 识别创建的服务帐户。
6. 验证角色是否已成功分配。

注意事项：

创建服务帐户时，请注意以下事项：

- **Grant this service account access to project**（授予此服务帐户对项目的访问权限）和 **Grant users access to this service account**（授予用户对此服务帐户的访问权限）的步骤是可选的。如果选择跳过这些可选配置步骤，新创建的服务账号不会显示在 **IAM & Admin**（IAM 和管理）> **IAM** 页面中。
- 要显示与服务帐户关联的角色，请在不跳过可选步骤的情况下添加角色。此过程可确保为配置的服务帐户显示角色。

**Citrix Cloud** 服务帐户密钥 在 Citrix DaaS 中创建连接需要 Citrix Cloud 服务帐户密钥。密钥包含在凭据文件 (.json) 中。创建密钥后，文件会自动下载并保存到下载文件夹。创建密钥时，请务必将密钥类型设置为 JSON。否则，Citrix 的“完整配置”界面无法进行解析。

要创建服务帐户密钥，请导航到 **IAM** 和管理 > 服务帐户，然后单击 Citrix Cloud 服务帐户的电子邮件地址。切换到密钥选项卡，然后选择添加密钥 > 创建新密钥。确保选择 **JSON** 作为密钥类型。

提示：

使用 Google Cloud 控制台中的 **Service accounts**（服务帐户）页面创建密钥。出于安全考虑，我们建议您定期更改密钥。通过编辑现有 Google Cloud 连接，可以向 Citrix Virtual Apps and Desktops 应用程序提供新密钥。

#### 向 **Citrix Cloud** 服务帐户添加角色

要向 Citrix Cloud 服务帐户添加角色，请执行以下操作：

1. 在 Google Cloud 控制台中，导航至 **IAM & Admin**（IAM 和管理员）> **IAM**。
2. 在 **IAM > PERMISSIONS**（权限）页面上，找到您创建的服务帐户，该帐户可通过电子邮件地址进行识别。  
例如，<my-service-account>@<project-id>.iam.gserviceaccount.com
3. 选择铅笔图标以编辑对服务帐户主体的访问权限。
4. 在所选主体选项的 **Edit access to “project-id”**（编辑对 project-id 的访问权限）页面上，选择 **ADD ANOTHER ROLE**（添加另一个角色）将以下角色逐个添加到您的服务帐户，然后选择 **SAVE**（保存）。

#### 向 **Cloud Build** 服务帐户添加角色

要向 Cloud Build 服务帐户添加角色，请执行以下操作：

1. 在 Google Cloud 控制台中，导航至 **IAM & Admin**（IAM 和管理员）> **IAM**。



2. 在 **IAM** 页面上，找到 Cloud Build 服务帐户，该帐户可以使用以 **Project ID**（项目 ID）和 **cloudbuild** 一词开头的电子邮件地址进行识别。

例如，<project-id>@cloudbuild.gserviceaccount.com

3. 选择铅笔图标以编辑 Cloud Build 帐户角色。
4. 在所选主体选项的 **Edit access to “project-id”**（编辑对 project-id 的访问权限）页面上，选择 **ADD ANOTHER ROLE**（添加另一个角色）将以下角色逐个添加到您的 Cloud Build 服务帐户，然后选择 **SAVE**（保存）。

注意：

启用所有 API 以获取完整的角色列表。

## 存储权限和存储桶管理

Citrix DaaS 改进了报告 [Google Cloud 服务](#) 的云生成失败的过程。此服务在 Google Cloud 上运行生成过程。Citrix DaaS 会创建一个名为 `citrix-mcs-cloud-build-logs-{ region } -{ 5 random characters }` 的存储桶，Google Cloud 服务将在其中捕获生成日志信息。在此存储桶上设置了一个选项，用于在 30 天后删除内容。此过程要求用于连接的服务帐户将 Google Cloud 权限设置为 `storage.buckets.update`。如果服务帐户没有此权限，Citrix DaaS 将忽略错误并继续执行目录创建过程。如果没有此权限，生成日志的大小会增加，需要手动清理。

## 启用 Google 专用访问权限

当 VM 缺少分配给其网络接口的外部 IP 地址时，数据包仅发送到其他内部 IP 地址目标。启用专用访问时，VM 将连接到 Google API 和相关服务使用的外部 IP 地址集。

注意：

无论是否启用了专用 Google 访问权限，所有具有或没有公用 IP 地址的 VM 都必须能够访问 Google 公用 API，尤其是在环境中安装了第三方网络连接设备的情况下。

要确保子网中的 VM 能够在没有公用 IP 地址的情况下访问 Google API 以进行 MCS 预配，请执行以下操作：

1. 在 Google Cloud 中，访问 **VPC network configuration**（VPC 网络配置）。
2. 在当前项目的“子网”选项卡中确定所使用的子网或 Citrix 环境。
3. 点击子网的名称并启用 **Google** 私有访问权限。

有关详细信息，请参阅[配置专用 Google 访问权限](#)。

重要：

如果您的网络配置为防止虚拟机访问互联网，请确保您的组织承担与为虚拟机连接的子网启用 Google 专用访问权限相关的风险。

### 下一步的去向

- 要进行简单的概念验证部署，请在指定用于向用户交付应用程序或桌面的计算机上[安装 VDA](#)。
- 要创建和管理连接，请参阅[连接到 Google Cloud 环境](#)。
- [查看安装和配置过程中的所有步骤](#)。

### 更多信息

- [创建和管理连接和资源](#)
- [创建计算机目录](#)

## HPE Moonshot 虚拟化环境（预览版）

January 23, 2024

Citrix DaaS 通过位于 DaaS 控制平面中的 Citrix 管理的 HPE Moonshot 插件来管理您的 HPE Moonshot 工作负载。使用此插件，您可以创建与 HPE Moonshot 机箱的连接、创建目录以及对目录中的计算机进行电源管理。

### 要求

在 **DaaS > 主页 > 预览功能** 中启用功能开关 **moonshotpluginenabled**。

### 关键步骤

1. 设置您的 HPE 环境。
2. 与 HPE Moonshot 机箱建立连接。

#### 注意：

启用功能切换后，将自动安装 Citrix 管理的 HPE Moonshot 插件。因此，您可以使用 Citrix 管理的 Moonshot 插件来继续使用现有计算机目录，而不是 HPE 管理的 HPE Moonshot 插件。

3. 创建计算机目录。

注意：

在创建目录之前，请确保拥有一个或多个 HPE Moonshot 盒式服务器节点，并在这些节点上安装 VDA。  
您可以将 HPE Moonshot 机箱视为虚拟机管理程序，将盒式服务器视为 VM。

4. 创建交付组。
5. 将其余非托管的 HPE Moonshot 节点迁移到托管目录或交付组。

#### 下一步的去向

- 对于简单的概念证明部署，请在要向用户交付应用程序或桌面的计算机上[安装 VDA](#)。
- 有关创建和管理连接的信息，请参阅[连接到 HPE Moonshot](#)。
- [查看安装和配置过程中的所有步骤](#)。

#### 更多信息

- [创建和管理连接和资源](#)
- [创建计算机目录](#)

## Microsoft Azure Resource Manager 虚拟化环境

January 23, 2024

在使用 Microsoft Azure Resource Manager 在 Citrix DaaS 部署中配置虚拟机时，请熟悉以下内容：

- [Microsoft Entra ID 是什么？](#)
- [将 Microsoft Entra ID 与应用程序集成入门指南](#)
- [Microsoft Entra ID 中的应用程序和服务主体对象](#)

要设置 Microsoft Azure Resource Manager，请参阅[设置资源位置](#)。

#### 下一步的去向

- 要进行简单的概念验证部署，请在指定用于向用户交付应用程序或桌面的计算机上[安装 VDA](#)。
- 要创建和管理连接，请参阅[与 Microsoft Azure 的连接](#)。
- [查看安装和配置过程中的所有步骤](#)。

## 更多信息

- [创建和管理连接和资源](#)
- [创建计算机目录](#)
- [CTX219211](#): 设置 Microsoft Azure Active Directory 帐户
- [CTX219243](#): 对 Azure 订阅授予 XenApp 和 XenDesktop 访问权限
- [CTX219271](#): 使用站点到站点 VPN 部署混合云

## Microsoft System Center Virtual Machine Manager 虚拟化环境

January 23, 2024

如果您将 Hyper-V 与 Microsoft System Center Virtual Machine Manager (VMM) 结合使用以提供虚拟机，请遵循此指南。

有关受支持的 VMM 版本的列表，请参阅[系统要求](#)。

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

- 第 1 代桌面或服务器操作系统 VM
- 第 2 代 Windows Server 2016、Windows Server 2019、Windows Server 2022、Windows 10 和 Windows 11 虚拟机（带或不带安全启动）

### 安装和配置虚拟机管理程序

在服务器上安装 Microsoft Hyper-V 角色和 VMM。

验证以下帐户信息：

在管理 > 完整配置中，您在创建连接时指定的帐户必须是相关 Hyper-V 计算机的 VMM 管理员或 VMM 委派的管理员。如果此帐户在 VMM 中仅具有委派管理员角色，则在连接创建过程中，存储数据不会在“完整配置”界面中列出。

您的用户帐户还必须是每个 Hyper-V Server 上的管理员本地安全组的成员，才能支持 VM 生命周期管理（例如 VM 创建、更新和删除）。

在单个 SCVMM 管理不同数据中心的多群集的大型部署中，您可以限制管理员的主机组范围。

要限制主机组范围，请在 Microsoft System Center Virtual Machine Manager (VMM) 控制台使用委派的管理员角色。

1. 在创建用户角色向导中，选择架构管理员（委派管理员）作为用户角色。
2. 在 **Members**（成员）中，在 Active Directory 中添加要用作委派管理员的用户帐户。

3. 在 **Scope**（作用域）中，选择您希望委派管理员有权访问的主机组。
4. 使用委派管理员用户凭据创建新的“运行身份”帐户。稍后使用这些凭据创建虚拟机管理程序连接。请勿使用主管理员角色帐户。

## 安装 VMM 控制台

在具有 Citrix Cloud Connector 的每台服务器上安装系统中心虚拟机管理器控制台。

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。

## 通过 SCVMM 进行 Azure Stack HCI 预配

Azure Stack HCI 是一种超融合基础结构 (HCI) 群集解决方案，可在混合本地环境中托管虚拟化的 Windows 和 Linux 工作负载及其存储。

Azure 混合服务通过基于云的监视、站点恢复和 VM 备份等功能增强了群集功能。您还可以在 Azure 门户中集中查看所有 Azure Stack HCI 部署。

## 将 Azure Stack HCI 与 SCVMM 集成

要将 Azure Stack HCI 与 SCVMM 集成，您需要先创建 Azure Stack HCI 群集，然后将该群集与 SCVMM 集成。

1. 要创建 Azure Stack HCI 群集并将其注册到 Azure，请参阅 Microsoft 文档[将 Azure Stack HCI 连接到 Azure](#)。
2. 要将 Azure Stack HCI 群集与 SCVMM 集成，请执行以下操作：
  - a) 登录准备托管 SCVMM 服务器的计算机并安装 SCVMM 2019 UR3 或更高版本。

注意：  
在 Cloud Connector 虚拟机中安装 SCVMM 2019 UR3 或更高版本的管理员控制台。
  - b) 在 VMM 控制台的设置页面中，创建一个运行方式帐户。
  - c) 在 SCVMM 服务器中使用管理权限运行以下 PowerShell 命令，将 Azure Stack HCI 群集添加为主机：

```
1 $runAsAccountName = 'Admin'
2 $runAsAccount = Get-SCRunAsAccount -Name $runAsAccountName
3 $hostGroupName = 'All Hosts'
4 $hostGroup = Get-SCVMHostGroup -Name $hostGroupName
5 $hostCluster = 'FQDN of Azure Stack HCI cluster'
6 Add-SCVMHostCluster -Name $hostCluster -RunAsynchronously -
  VMHostGroup
```

```
7 $hostGroup -Credential $runAsAccount -RemoteConnectEnabled  
   $true  
8 <!--NeedCopy-->
```

d) 现在，您可以在 VMM 控制台中查看 Azure Stack HCI 群集以及节点。

e) 在完整配置界面中创建 SCVMM 托管连接。

#### 下一步的去向

- 要进行简单的概念验证部署，请在指定用于向用户交付应用程序或桌面的计算机上[安装 VDA](#)。
- 有关创建和管理连接的信息，请参阅[与 Microsoft System Center Virtual Machine Manager 的连接](#)。
- [查看安装和配置过程中的所有步骤](#)。

#### 更多信息

- [创建和管理连接和资源](#)
- [创建计算机目录](#)

## Nutanix 虚拟化环境

February 9, 2024

使用 Nutanix Acropolis 在 Citrix DaaS 部署中提供虚拟机时，请遵循本指南。安装过程包括在 Citrix DaaS 环境中安装和注册 Nutanix 插件的任务。

有关 Nutanix Acropolis MCS 插件安装指南的更多信息，请访问 [Nutanix 支持门户](#)。

#### 重要提示：

在所有 Cloud Connector 上安装 Nutanix 插件，Citrix DaaS 必须创建到具有 Nutanix 虚拟机管理程序的资源位置的主机连接。

#### 安装并注册 Nutanix 插件

完成在所有 Cloud Connector 上安装和注册 Nutanix 插件的程序。使用 Citrix Cloud 中的 **Manage**（管理）> **Full Configuration**（完整配置）功能创建与 Nutanix 的连接。

有关安装 Nutanix 插件的信息，请参阅 [Nutanix 文档站点](#)。

有关如何设置 Nutanix 虚拟环境的详细信息，请参阅在 [Citrix Cloud 中添加资源类型或激活未使用的域](#)。

## 下一步的去向

- 要进行简单的概念验证部署，请在指定用于向用户交付应用程序或桌面的计算机上[安装 VDA](#)。
- 要创建和管理连接，请参阅[与 Nutanix 的连接](#)。
- [查看安装和配置过程中的所有步骤](#)。

## 更多信息

- [创建和管理连接和资源](#)
- [创建计算机目录](#)

## Nutanix 云和合作伙伴解决方案

January 23, 2024

Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）支持以下 Nutanix 云和合作伙伴解决方案：

- AWS 上的 Nutanix Cloud Clusters

### AWS 上的 Nutanix Cloud Clusters

Citrix DaaS 支持 AWS 上的 Nutanix Cloud Clusters。Nutanix 群集简化了应用程序在私有云或多个公有云上的运行方式。有关 AWS 上的 Nutanix Cloud Clusters 的详细信息，请参阅 [Nutanix Cloud Clusters on AWS Deployment and User Guide](#)（《AWS 上的 Nutanix Cloud Clusters 部署和用户指南》）。

提示：

此支持提供的功能与 Nutanix 本地群集相同。仅支持一个群集，即 *Prism Element*。有关详细信息，请参阅[此处](#)。

## 要求

您需要以下帐户才能在 AWS 上使用 Nutanix Clusters：

- 一个 Nutanix 帐户
- 具有以下权限的 AWS 帐户：
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

## 创建 **Nutanix** 群集

要创建 Nutanix 群集，请执行以下操作：

1. 登录您的 Nutanix 帐户。
2. 找到 **Nutanix cluster** (Nutanix 群集) 选项，然后单击 **Launch** (启动)。**Nutanix Console** (Nutanix 控制台) 将打开。有关详细信息，请参阅 [Get Started with Nutanix Cluster on AWS](#) (AWS 上的 Nutanix 群集入门)。
3. 选择创建新 **VPC**。

群集创建过程可能会失败，并出现以下错误：

- 群集无法在给定时限内创建。删除群集。
- 主机 Nutanix 群集 - 节点 XXXXXXXXXXXX: Instance i-xxxxxxxxxxxxx: disable network interface source/dest check error.
- 主机 Nutanix 群集 - 节点 XXXXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxx network interface info.

如果群集无法创建，那么：

- 尝试在其他区域重新创建一个群集。
- 在重试之前，请务必删除 Nutanix CloudFormation 堆栈 (CFS)。

除了其他资源外，Nutanix CFS 还创建了：

- 1 个名为 *Nutanix Cluster xxxxxxxxxxxx* 10.0.0.0/16 的 VPC
- 2 个子网 10.0.128.0/24 和 10.0.129.0/24
- 1 Internet 网关
- 1 个 NAT 网关

创建群集后，检索 **Nutanix Prism** 的地址：

1. 转至 **Nutanix Console** (Nutanix 控制台)。
2. 在控制台的右上角，将鼠标悬停在启动 **Prism Element** 链接上并复制 URL。

## 下一步的去向

- 要进行简单的概念验证部署，请在指定用于向用户交付应用程序或桌面的计算机上[安装 VDA](#)。
- 有关创建和管理连接的信息，请参阅[连接到 Nutanix 云和合作伙伴解决方案](#)。
- [查看安装和配置过程中的所有步骤](#)。

## 更多信息

- [创建和管理连接和资源](#)



- [创建计算机目录](#)

## VMware 虚拟化环境

January 23, 2024

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。）

注意：

不支持 vSphere vCenter “链接模式”操作。

如果您计划使用 Machine Creation Services (MCS)，请勿按照[禁用 vCenter Server 数据存储浏览器](#)中所述在 vCenter Server 中禁用数据存储浏览器功能。如果禁用此功能，MCS 无法正常工作。

要设置您的 VMware 虚拟化环境，请参阅在[Citrix Cloud 中添加资源类型或激活未使用的域](#)。

### 下一步的去向

- 要进行简单的概念验证部署，请在指定用于向用户交付应用程序或桌面的计算机上[安装 VDA](#)。
- 有关创建和管理连接的信息，请参阅[与 VMware 的连接](#)。
- [查看安装和配置过程中的所有步骤](#)。

### 更多信息

- [创建和管理连接和资源](#)
- [创建计算机目录](#)

## VMware 云和合作伙伴解决方案

January 23, 2024

Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）支持以下 VMware 云和合作伙伴解决方案：

- Azure VMware 解决方案 (AVS)
- Google Cloud VMware Engine
- Amazon Web Services (AWS) 上的 VMware 云

使用 Citrix DaaS 将基于 VMware 的本地 Citrix 工作负载迁移到相应的 VMware 合作伙伴解决方案。

## Azure VMware 解决方案 (AVS) 集成

Citrix DaaS 支持 [AVS](#)。AVS 提供包含由 Azure 基础结构创建的 vSphere 群集的云基础结构。利用 DaaS 使用 AVS 来配置 VDA 工作负载，就像在本地环境中使用 vSphere 一样。

### 设置 AVS 群集

要允许 Citrix DaaS 使用 AVS，请在 Azure 中执行以下步骤：

- 申请主机配额
- 注册 [Microsoft.AVS](#) 资源提供商
- 验证网络规划清单
- 网络清单
- 创建 AVS 私有云
- 访问 AVS 私有云
- 在 Azure 中为 VMware 私有云配置网络连接
- 为 AVS 配置 DHCP
- 在 AVS 中添加网络分段
- 验证 AVS 环境

为 **Azure** 企业协议客户申请主机配额 在 Azure 门户的帮助 + 支持页面中，选择新建支持请求，并包含以下信息：

- 问题类型：技术
- 订阅：选择您的订阅
- 服务：所有服务 > **Azure VMware 解决方案**
- 资源：一般问题
- 摘要：需要容量
- 问题类型：容量管理问题
- 问题子类型：客户请求增加主机配额/容量

在支持票证的说明中，在详细信息选项卡中包含以下信息：

- POC 或生产
- 区域名称
- 主机数量
- 任何其他详细信息

注意：

AVS 至少需要三台主机，建议您使用 N+1 台主机的冗余。

指定支持票证的详细信息后，选择查看 + 创建以将申请提交到 Azure。

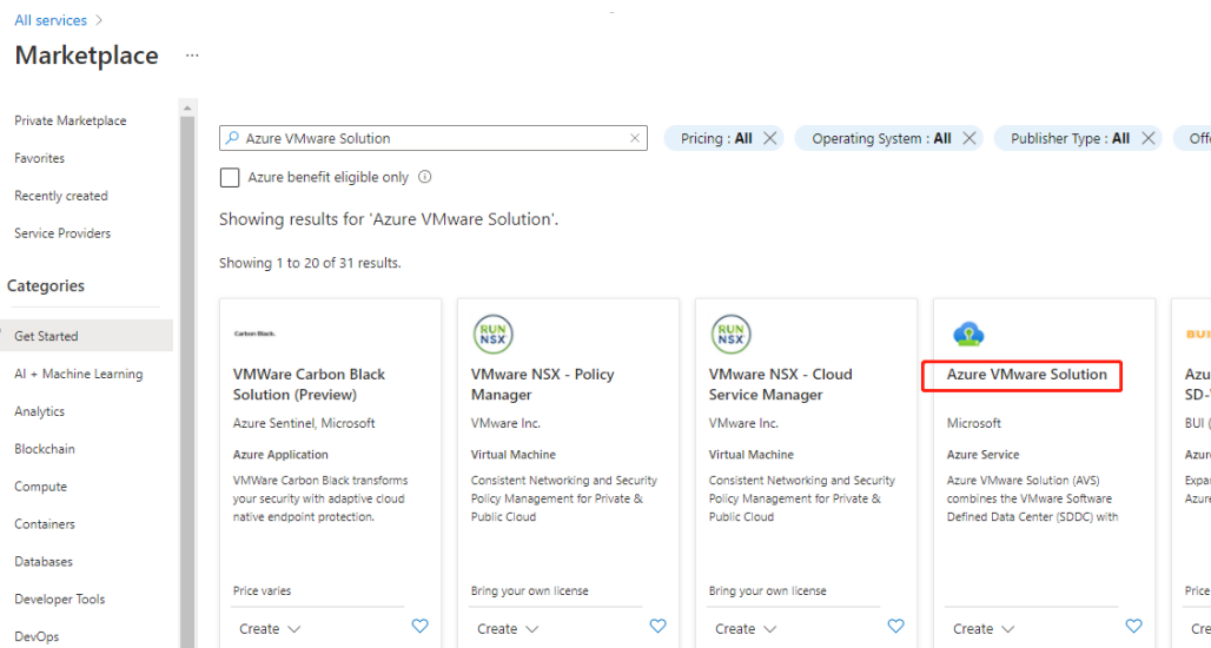
注册 **Microsoft.AVS** 资源提供程序 申请主机配额后，注册资源提供程序：

- 1. 登录 Azure 门户。
- 2. 在 Azure 门户菜单中，选择所有服务。
- 3. 在所有服务菜单中，输入订阅，然后选择订阅。
- 4. 从订阅列表中选择订阅。
- 5. 选择资源提供程序，然后在搜索栏中输入 **Microsoft.AVS**。
- 6. 如果资源提供程序未注册，请选择注册。

网络连接注意事项 AVS 提供需要特定网络地址范围和防火墙端口的网络连接服务。有关详细信息，请参阅 [Azure VMware 解决方案的网络规划清单](#)。

创建 **AVS** 私有云 在考虑了环境的网络要求之后，创建 ASV 私有云：

- 1. 登录 Azure 门户。
- 2. 选择创建新资源。
- 3. 在搜索应用商店文本框中，键入 *Azure VMware* 解决方案，然后从列表中选择 **Azure VMware** 解决方案。



在 **Azure VMware** 解决方案窗口中：

- 1. 选择创建。
- 2. 转到“基础知识”选项卡。
- 3. 使用下表中的信息输入字段的值：

字段	值
订阅	选择您计划用于部署的订阅。Azure 订阅中的所有资源一起计费。
资源组	为您的私有云选择资源组。Azure 资源组是在其中部署和管理 Azure 资源的逻辑容器。或者，您可以为私有云创建一个新资源组。
位置	选择一个位置，例如美国东部。这是您在规划阶段定义的区域。
资源名称	提供 Azure VMware 解决方案私有云的名称。
主机的大小	根据需要选择尺寸。
主机数量	显示为私有云群集分配的主机数。默认值为 3，部署后可以增大或减小该值。
专用云的地址块	为私有云提供 IP 地址块。CIDR 代表私有云管理网络，将用于群集管理服务，例如 vCenter Server 和 NSX-T Manager。请使用 /22 地址空间，例如 10.175.0.0/22。该地址应是唯一的，不得与其他 Azure 虚拟网络和本地网络重叠。

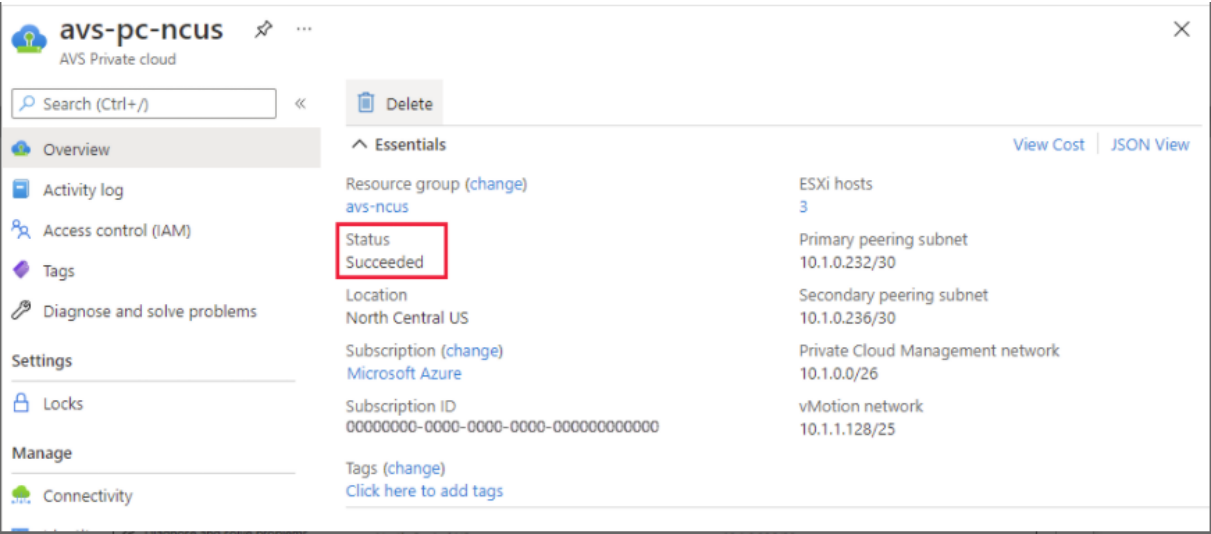
在创建私有云屏幕中：

1. 在“位置”字段中，选择拥有 AVS 的区域。资源组区域与 AVS 区域相同。
2. 在“主机大小”字段中，根据需要选择大小。
3. 在“专用云地址块”字段中指定 IP 地址。例如，10.15.0.0/22。
4. 选择审阅 + 创建。
5. 审阅信息后，单击创建。

提示：

创建私有云可能需要 3–4 个小时。向群集添加单个主机可能需要 30–45 分钟。

验证部署是否成功。导航到您创建的资源组并选择您的专用云。状态为成功后，部署即完成。



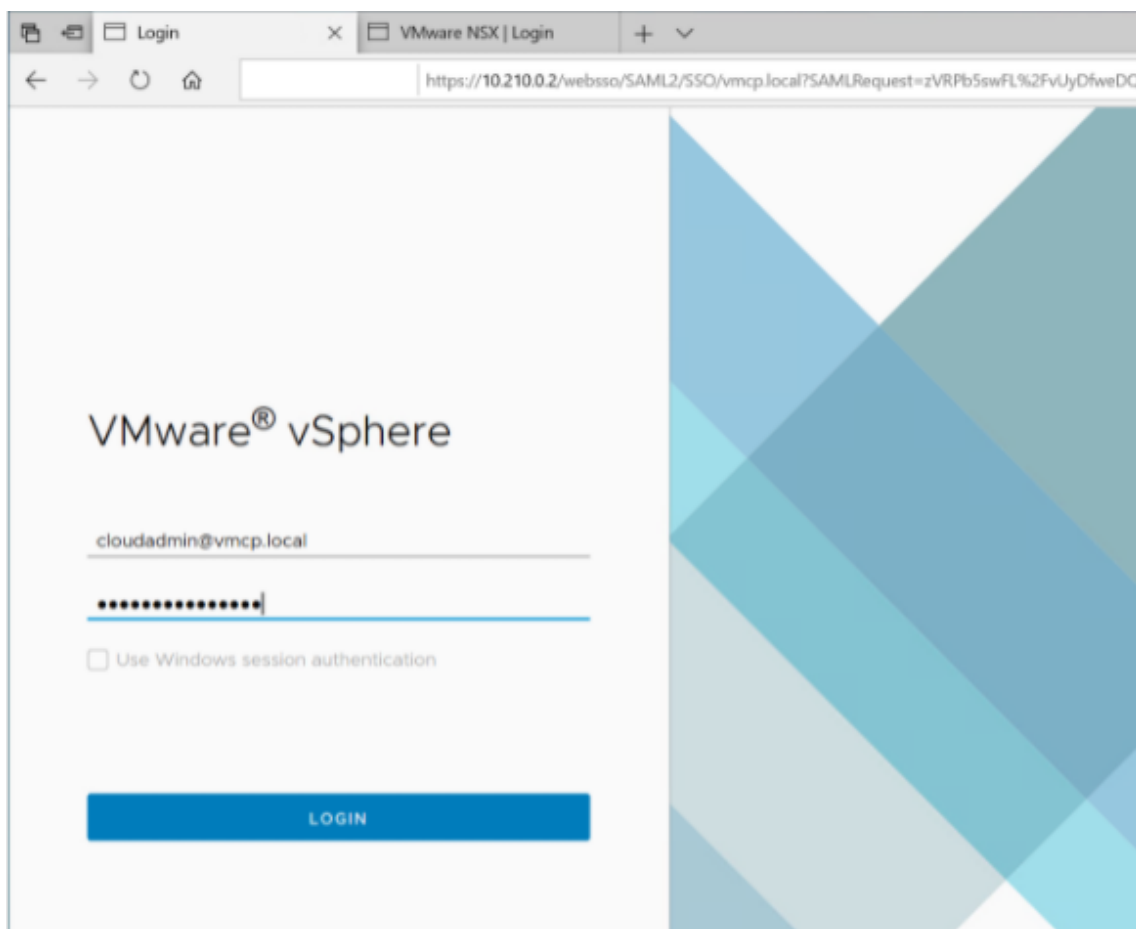
访问 **AVS** 私有云 创建私有云后，请创建一个 Windows VM 并连接到私有云的本地 vCenter。

创建新的 **Windows** 虚拟机

1. 在资源组中，选择 + 添加，然后搜索并选择 **Microsoft Windows 10/11** 或 **Windows Server 2016/2019**。
2. 输入所需的信息，然后选择审阅 + 创建。
3. 验证通过后，选择创建以启动虚拟机创建过程。

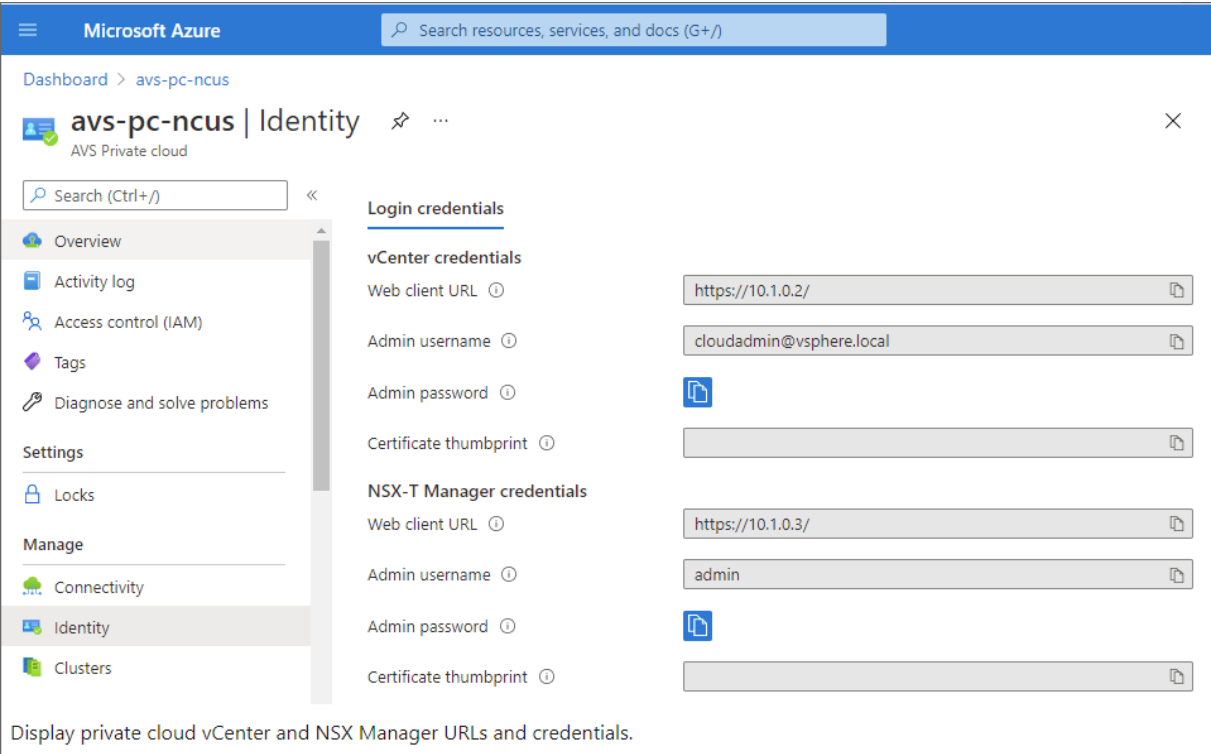
连接到私有云的本地 **vCenter**

1. 以云管理员身份使用 **VMware vCenter SSO** 登录 **vSphere Client**。



2. 在 Azure 门户中，选择您的私有云，然后选择管理 > 身份。

此时将显示私有云 vCenter 和 NSX-T Manager 的 URL 和用户凭据：



确认 URL 和用户凭据后：

1. 导航到您在前面的步骤中创建的虚拟机并连接到该虚拟机。
2. 在 Windows VM 中，打开浏览器，然后在两个浏览器选项卡中导航到 vCenter 和 NSX-T Manager URL。在 vCenter 选项卡中，输入上一步中的 `cloudadmin@vmcp.local` 用户凭据。

在 **Azure** 中为 **VMware** 私有云配置网络连接 访问 ASV 私有云后，通过创建虚拟网络和网关来配置网络连接。

#### 创建虚拟网络

1. 登录 Azure 门户。
2. 导航到之前创建的资源组。
3. 选择 + 添加以定义新资源。
4. 在搜索应用商店文本框中，键入虚拟网络。查找虚拟网络资源并将其选中。
5. 在虚拟网络页面上，选择创建为私有云设置虚拟网络。
6. 在创建虚拟网络页面上，输入虚拟网络的详细信息。
7. 在基本选项卡上，输入虚拟网络的名称，选择相应的区域，然后单击下一步：**IP** 地址。
8. 在 **IP** 地址选项卡上的 IPv4 地址空间下，输入先前创建的地址。

重要：

使用与您创建私有云时使用的地址空间不重叠的地址。

进入地址空间后：

1. 选择 **+** 添加子网。
2. 在添加子网页面上，为子网指定名称和适当的地址范围。
3. 单击添加。
4. 选择审阅 **+** 创建。
5. 验证信息，然后单击创建。部署完成后，虚拟网络将显示在资源组中。

创建虚拟网络网关    创建虚拟网络后，创建虚拟网络网关。

1. 在资源组中，选择 **+** 添加以添加新资源。
2. 在搜索应用商店文本框中，键入虚拟网络网关。查找虚拟网络资源并将其选中。
3. 在虚拟网络网关页面上，单击创建。
4. 在创建虚拟网络网关页面的基本选项卡上，为字段提供值。
5. 单击查看 **+** 创建。



Home > Resource groups > AVS > Create a resource > Virtual network gateway >

# Create virtual network gateway ...

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*

cc-lab-xac-cp1-ca-aakash.mathai@citrix.com

Resource group ⓘ

AVS (derived from virtual network's resource group)

Instance details

Name \*

AVS\_gateway

Region \*

Southeast Asia

Gateway type \* ⓘ

☐ VPN

☒ ExpressRoute

SKU \* ⓘ

Standard

Virtual network \* ⓘ

AVS\_vNet

Create virtual network

ⓘ Only virtual networks in the currently selected subscription and region are listed.

Gateway subnet address range \* ⓘ

10.16.1.0/24

10.16.1.0 - 10.16.1.255 (256 addresses)

Public IP address

Public IP address \* ⓘ

☒ Create new

☐ Use existing

Public IP address name \*

AVSPprivateCloudgatewayIP

Public IP address SKU

Basic

Assignment

☒ Dynamic

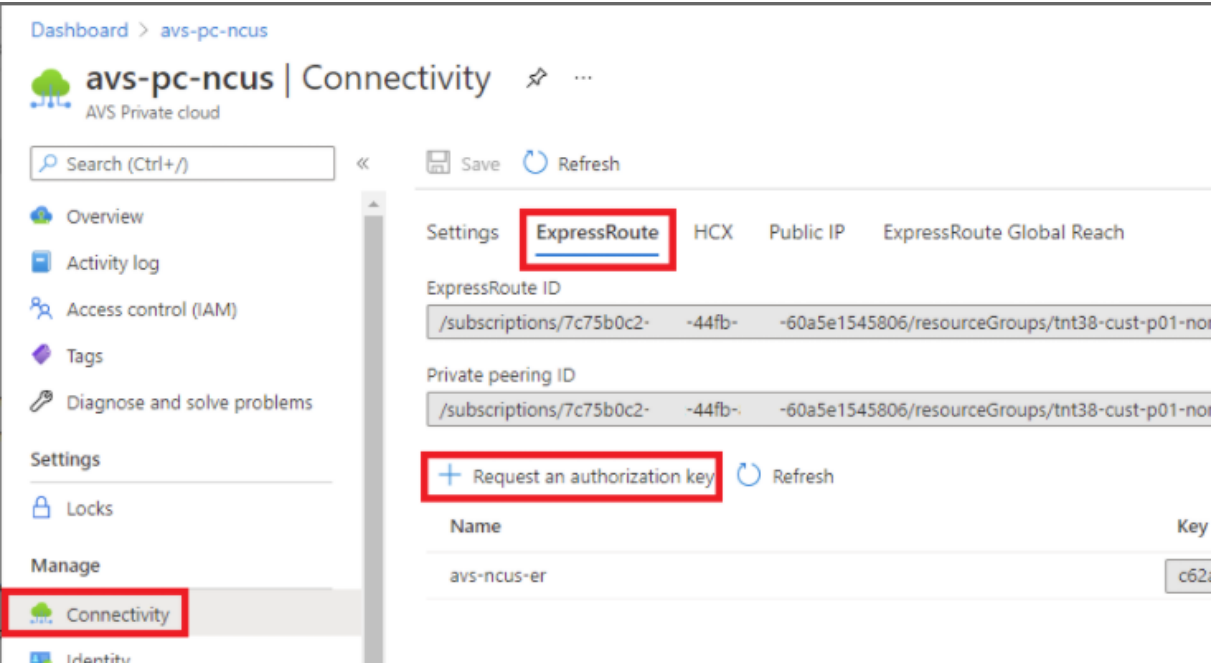
☐ Static

查看虚拟网络网关配置后，单击创建以部署虚拟网络网关。

部署完成后，将 **ExpressRoute** 连接连接到包含您的 Azure AVS 私有云的虚拟网络网关。

将 **ExpressRoute** 连接到虚拟网络网关 部署虚拟网络网关后，在该网关与您的 Azure AVS 私有云之间添加连接：

1. 申请 ExpressRoute 授权密钥。
2. 在 Azure 门户中，导航到 **Azure VMware Solution private cloud**（Azure VMware 解决方案私有云）。  
选择管理 > 连接 > **ExpressRoute**，然后选择 **+ Request an authorization key**（+ 申请授权密钥）。



申请授权密钥后：

1. 键入注册表项的名称，然后单击创建。创建密钥可能需要大约 30 秒钟。创建后，新密钥将出现在私有云的授权密钥列表中。
2. 复制授权密钥和 **ExpressRoute ID**。您需要这些信息来完成对等互连过程。授权密钥会在一段时间后消失，因此请在出现时复制。
3. 导航到您计划使用的虚拟网络网关，然后选择连接 > + 添加。
4. 在添加连接页面上，为字段提供值，然后选择确定。

Home > Microsoft.VirtualNetworkGateway-20210611150456 > AVS\_gateway >

## Add connection

AVS\_gateway

**i** Ensure that the ExpressRoute associated with this authorization is provisioned by the provider before redeeming the authorization.

Name \*

azure\_to\_avs\_ncus ✓

Connection type ⓘ

ExpressRoute ▼

☒ Redeem authorization ⓘ

\*Virtual network gateway ⓘ

AVS\_gateway 🔒

Authorization key \*

..... ✓

Peer circuit URI \*

..... ✓

☐ FastPath ⓘ

Subscription ⓘ

..... ▼

Resource group ⓘ

..... ▼

Location ⓘ

Southeast Asia ▼

OK

authorization key

ExpressRoute ID

在 ExpressRoute 电路与虚拟网络之间建立连接：

+ Add ↻ Refresh

🔍 Search connections

Name	↑↓ Status	↑↓ Connection type	↑↓ Peer
azure_to_aws_ncus	Succeeded	ExpressRoute	tnt47-cust-p01-southeastasia-er

为 **Azure VMware** 解决方案配置 **DHCP** 将 ExpressRoute 连接到虚拟网关后，请配置 DHCP。

使用 **NSX-T** 托管 **DHCP** 服务器 在 NSX-T 管理器中：

- 1. 选择 **Networking**（网络连接）> **DHCP**，然后选择 **Add Server**（添加服务器）。
- 2. 为 **Server Type**（服务器类型）选择 **DHCP**，提供服务器名称和 IP 地址。
- 3. 单击保存。
- 4. 选择 **Tier 1 Gateways**（第 1 层网关），选择第一层网关上的垂直省略号，然后选择编辑。
- 5. 选择 **No IP Allocation Set**（无 IP 分配集）以添加子网。
- 6. 选择 **Type**（类型）为 **DHCP Local Server**（DHCP 本地服务器）。
- 7. 对于 **DHCP Server**（DHCP 服务器），请选择 **Default DHCP**（默认 DHCP），然后单击 **Save**（保存）。
- 8. 再次单击 **Save**（保存），然后选择 **Close Editing**（关闭编辑）。

ADD SERVER

Filter by Name, Path or more

Server Type	Server Name	Server IP Address	Lease Time (seconds)	Edge Cluster	Where Used	Tags
DHCP Server	DHCP	10.16.100.1/24	86400	TNT47-CLSTR		Tag Sco...

Format is CIDR e.g 10.1.1.1/24

Max 30 allowed. Click (+) to save.

SAVE CANCEL

在 **Azure VMware** 解决方案中添加网络分段 设置 DHCP 后，添加一个网段。

要添加网段，请在 NSX-T Manager 中选择 **Networking**（网络连接）> **Segments**（网段），然后单击 **Add Segment**（添加网段）。

vm NSX-T

Home Networking Security Inventory Plan & Troubleshoot System Advanced Networking & Security

Network Overview

Connectivity

Tier-0 Gateways

Tier-1 Gateways

Segments

Network Services

SEGMENTS

SEGMENT PROFILES

ADD SEGMENT

	Segment Name	Connected Gateway & Type
>	TNT47-HCX-UPLINK	TNT47-T1   Tier1 - Flexible
>	TNT47-T0-PRIVATE01-LS	None - Flexible
>	TNT47-T0-PRIVATE02-LS	None - Flexible

在 **Segments profile**（网段配置文件）屏幕中：

- 1. 输入网段的名称。
- 2. 选择 **Tier-1 Gateway (TNTxx-T1)**（第 1 层网关 (TNTxx-T1)）为 **Connected Gateway**（已连接的网关），然后将 **Type**（类型）保留为 **Flexible**（灵活）。
- 3. 选择预先配置的叠加 **Transport Zone(TNTxx-OVERLAY-TZ)**（传输区域 (TNTxx-OVERLAY-TZ)）。
- 4. 单击 **Set Subnets**（设置子网）。

ENTS

SEGMENT PROFILES

EXPAND ALL

Filter by Name, Path o

Segment Name	Connected Gateway & Type	Subnets
Is01	TNT47-T1Flexible	Set Subnets

Segment needs to have either Subnets or VPN defined, or both.

L2 VPN

You have no L2 VPN sessions for this Gateway. For that, go to [VPN Services](#) . Note that for L2 sessions to work, you also need IP Sec session defined.

Transport Zone

TNT47-OVERLAY-TZ | Overlay

VPN Tunnel ID

VLAN

Enter List of VLANs

Connectivity

NOTE - Before further configurations can be done, fill out mandatory fields above ( \* ), click 'Save' below.

PORTS

SEGMENT PROFILES

SAVE

CANCEL

1:1

在 **Subnets**（子网）部分中：

- 1. 输入网关 IP 地址。
- 2. 选择添加。

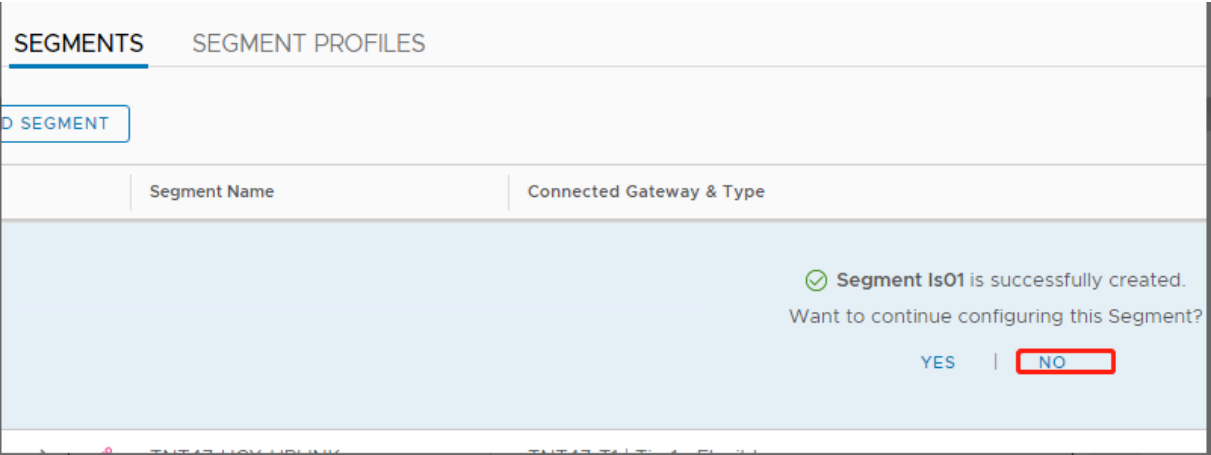
重要：

此网段 IP 地址必须属于 Azure 网关 IP 地址 10.15.0.0/22。

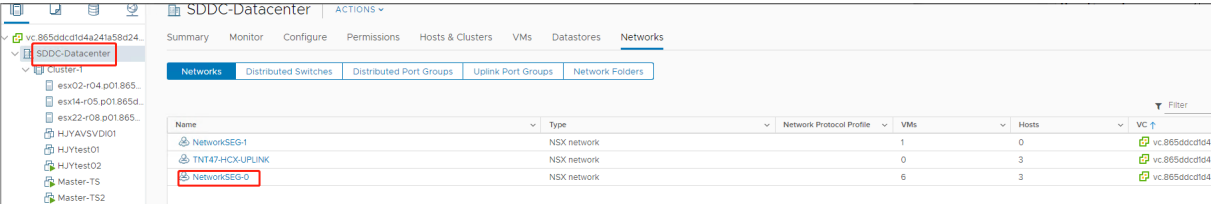
DHCP 范围必须属于分段 IP 地址：

<input type="checkbox"/> Segment name ↑↓	Connected gateway ↑↓	Gateway IP ↑↓	DHCP range ↑↓	Port/VIF ↑↓	State ↑↓
<input type="checkbox"/> NetworkSEG-0	TNT47-T1	10.15.4.1/24	10.15.4.100-10.15.4.200	6	<div>SUCCESS</div>

选择 **No**（否）将拒绝用于继续配置网段的选项：



在 vCenter 中，选择网络连接 > **SDDC** 数据中心：



验证 **AVS** 环境    为 AVS 专用云设置资源位置并安装一对云连接器。

在 **Citrix Studio** 中创建 **AVS** 连接

1. 在 vCenter 中创建一台计算机并在计算机中安装一对 Cloud Connector。请参阅[配置实例](#)。
2. 在管理 > 完整配置中，选择左侧窗格中的“托管”。
3. 选择托管节点，然后单击添加连接和资源。
4. 在 **Connection**（连接）屏幕上，选择 **Create a new Connection**（创建新连接），然后选择以下详细信息：

The screenshot shows the 'Add Connection and Resources' window. On the left, a sidebar lists steps: 1 Connection, 2 Storage Management, 3 Storage Selection, 4 Network, 5 Scopes, and 6 Summary. The main area is titled 'Connection'. It has two radio buttons: 'Use an existing connection' (unselected) and 'Create a new connection' (selected). Below the radio buttons, there are several fields: 'Zone' (dropdown menu showing 'Azure-VMware RL'), 'Connection type' (dropdown menu showing 'VMware vSphere®'), 'Connection address' (text input showing 'https://10.15.0.2/'), 'User name' (text input showing 'cloudadmin@vsphere.local'), 'Password' (password field with dots), and 'Connection name' (text input showing 'AVS'). There is a link 'Learn about user permissions' above the user name field. At the bottom, there is a section 'Create virtual machines using:' with two radio buttons: 'Citrix provisioning tools (Machine Creation Services or Citrix Provisioning)' (selected) and 'Other tools' (unselected). At the very bottom, there are 'Next' and 'Cancel' buttons.

- a) 选择连接类型为 **VMware vSphere**。
- b) 在 **Connection address**（连接地址）中，输入 vCenter 专用 IP 地址。
- c) 输入 vCenter 凭据。
- d) 输入连接名称。
- e) 选择用于创建虚拟机的工具。

- 5. 在网络屏幕上，选择在 NSX-T 服务器中创建的子网。
- 6. 完成向导。

**Google Cloud VMware Engine**

借助 Citrix DaaS，您可以将基于 VMware 的本地 Citrix 工作负载迁移到 Google Cloud VMware Engine。

**配置 Google Cloud VMware Engine**

以下过程介绍了如何在 Google Cloud VMware Engine 上获取和设置群集。

**访问 VMware Engine 门户**

- 1. 在 **Google Cloud Console**（Google Cloud 控制台）中，单击导航菜单。
- 2. 在计算部分中，单击 **VMware Engine** 以在新浏览器选项卡中打开 VMware Engine。

创建第一个私有云的要求 您必须有权访问 Google Cloud VMware Engine、可用的 VMware Engine 节点配额以及适当的 IAM 角色。在继续创建专用云之前，请设置以下要求：

1. 请求 API 访问权限和节点配额。有关详细信息，请参阅[请求 API 访问权限和配额](#)。
  2. 请注意要用于 VMware 管理设备和 HCX 部署网络的地址范围。有关详细信息，请参阅[网络连接要求](#)。
- 注意：

HCX 部署仅适用于 IP 计划版本 1.0。
3. 获取 VMware Engine Service 管理 IAM 角色。

创建您的第一个私有云

1. 访问 VMware Engine 门户。
2. 在 VMware Engine 主页上，单击 **Create a private cloud**（创建私有云）。列出了托管位置和硬件节点类型。
3. 选择私有云的节点数。至少需要三个节点。
4. 输入 VMware 管理网络的无类别域际路由 (Classless Inter-Domain Routing, CIDR) 范围。
5. 输入 HCX 部署网络的 CIDR 范围。

重要：

- CIDR 范围不得与任何本地子网或云子网重叠。CIDR 范围必须为 /27 或更高。
- HCX 部署仅适用于 IP 计划版本 1.0。

6. 选择检查 + 创建。
7. 检查设置。要更改任何设置，请单击 **Back**（上一步）。
8. 单击 **Create**（创建）开始创建私有云。

在 VMware Engine 创建您的新私有云时，它会部署多个 VMware 组件，并为私有云中的群集设置初始 Autoscale 策略。创建私有云可能需要 30 分钟到 2 小时。预配完成后，您会收到一封电子邮件。

设置 **Google Cloud VMware Engine VPN** 网关 要建立与 Google Cloud VMware Engine 的初始连接，您可以使用 VPN 网关。这是一个基于 OpenVPN 的客户端 VPN，您可以用来连接到 VMware Software Defined Data Center (SDDC) vCenter 并进行所需的任何初始配置。

在部署 VPN 网关之前，请为部署 SDDC 的区域配置 **Edge** 服务范围。为此，您需要：

1. 登录 **Google Cloud VMware Engine** 门户，然后转到 **Network**（网络）> **Regional Settings**（区域设置）。单击 **Add Region**（添加区域）。
2. 选择部署了 SDDC 的区域，然后启用 **Internet Access**（Internet 访问权限）和 **Public IP Service**（公共 IP 服务）。



3. 提供规划期间记录的边缘服务范围，然后单击 **Submit** (提交)。启用这些服务需要 10 到 15 分钟。

完成后，边缘服务将在“Regional Settings”（区域设置）页面上显示为 **Enabled**（已启用）。启用这些设置允许将公用 IP 分配给您的 SDDC，这是部署 VPN 网关的必要条件。

#### 部署 VPN 网关

1. 在 **Google Cloud VMware Engine** 门户中，转到 **Network**（网络）> **VPN Gateways**（VPN 网关）。单击 **Create New VPN Gateway**（创建新 VPN 网关）。
2. 提供规划期间保留的 VPN 网关和客户端子网的名称。VPN 的位置必须与专用云区域相同。单击下一步。
3. 选择要授予 VPN 访问权限的用户。单击下一步。
4. 指定必须可通过 VPN 访问的网络。单击下一步。
5. 此时将显示摘要屏幕。验证所做的选择，然后单击 **Submit** (提交) 以创建 VPN 网关。此时将显示“VPN Gateways”（VPN 网关）页面，其中新 VPN 网关的状态为 **Creating**（正在创建）。
6. 状态变为 **Operational**（可操作）后，单击新的 VPN 网关。
7. 单击 **Download my VPN configuration**（下载我的 VPN 配置）以下载一个 ZIP 文件，其中包含 VPN 网关的预配置的 OpenVPN 配置文件。提供用于通过 UDP/1194 和 TCP/443 进行连接的配置文件。选择您的首选选项并将其导入到 OpenVPN 中，然后进行连接。
8. 转到 **Resources**（资源），然后选择您的 SDDC。

#### 连接 VPN

1. 请通过 VPN 网关设置在本地网络与私有云之间建立点对点连接。请参阅设置 Google Cloud VMware Engine VPN 网关。
2. 上载在设置 Google Cloud VMware Engine VPN 网关中下载的 VPN 配置。
3. 导入到您的 VPN 客户端，例如 OpenVPN Connect 接。

有关详细信息，请参阅[使用 VPN 进行连接](#)。

#### 创建第一个子网

从 **VMware Engine** 门户访问 **NSX-T Manager** 创建子网过程发生在 NSX-T 中，您可以通过 VMware Engine 访问该子网。要访问 NSX-T Manager，请执行以下操作。

1. 登录 **Google Cloud VMware Engine** 门户。
2. 在主导航栏中，转到 **Resources**（资源）。
3. 单击与要在其中创建子网的私有云对应的 **Private cloud name**（私有云名称）。
4. 在私有云的详细信息页面上，单击 **vSphere Management Network**（vSphere 管理网络）选项卡。
5. 单击与 NSX-T Manager 对应的 **FQDN**。

6. 出现提示时，输入您的登录凭据。如果您已设置 vIDM 并将其连接到标识源（例如 Active Directory），请改用标识源凭据。

提醒：

可以从私有云详细信息页面检索生成的凭据。

为子网设置 **DHCP** 服务 在创建子网之前，请先设置 DHCP 服务：

在 NSX-T 管理器中：

1. 转到 **Networking**（网络连接）> **DHCP**。网络连接控制板显示 DHCP 服务创建了一个第 0 层网关和一个第 1 层网关。
2. 要开始配置 DHCP 服务器，请单击 **Add Server**（添加服务器）。
3. 为 **Server Type**（服务器类型）选择 **DHCP**，提供服务器名称和 IP 地址。
4. 单击 **Save**（保存）以创建 DHCP 服务。

执行以下操作以将此 DHCP 服务附加到相关的第 1 层网关。DHCP 服务已预配默认第 1 层网关：

1. 选择 **Tier 1 Gateways**（第 1 层网关），选择第一层网关上的垂直省略号，然后选择编辑。
2. 在 **IP Address Management**（IP 地址管理）字段中，选择 **No IP Allocation Set**（无 IP 分配集）。
3. 选择 **Type**（类型）为 **DHCP Local Server**（DHCP 本地服务器）。
4. 选择为 **DHCP Server**（DHCP 服务器）创建的 DHCP 服务器。
5. 单击保存。
6. 单击 **Close Editing**（关闭编辑）。

现在，您可以在 NSX-T 中创建网段。有关 NSX-T 中的 DHCP 的详细信息，请参阅 [VMware documentation for DHCP](#)（适用于 DHCP 的 VMware 文档）。

在 **NSX-T** 中创建网段 对于工作负载 VM，您可以为私有云创建子网作为 NSX-T 网段：

1. 在 NSX-T Manager 中，转到 **Networking**（网络连接）> **Segments**（区段）。
2. 单击 **Add Segment**（添加区段）。
3. 输入网段的名称。
4. 选择 **Tier-1**（第 1 层）为 **Connected Gateway**（已连接的网关），然后将“Type”（类型）保留为 **Flexible**（灵活）。
5. 单击 **Set Subnets**（设置子网）。
6. 单击添加子网。
7. 在 **Gateway IP/Prefix Length**（网关 IP/前缀长度）中输入子网范围。指定子网范围，最后一个二进制八位数为 **.1**。例如，**10.12.2.1/24**。
8. 指定 DHCP 范围，然后单击 **ADD**（添加）。
9. 在 **Transport Zone**（传输区域）中，从下拉列表中选择 **TZ-OVERLAY**。
10. 单击保存。现在，您可以在创建 VM 时在 vCenter 中选择此网段。

在给定区域中，使用专用服务访问权限，您最多可以设置 100 条从 VMware Engine 到 VPC 网络的唯一路由。例如，这包括私有云管理 IP 地址范围、NSX-T 工作负载网段和 HCX 网络 IP 地址范围。此限制包括该区域中的所有私有云。

注意：

存在一个 Google Cloud 配置问题，因此您需要多次配置 DHCP 范围设置。因此，请务必在配置 Google Cloud 后配置 DHCP 范围设置。单击 **EDIT DHCP CONFIG**（编辑 DHCP 配置）以配置 DHCP 范围。

Network Overview

Network Topology

Connectivity

Tier-0 Gateways

Tier-1 Gateways

Segments

Network Services

VPN

NAT

Load Balancing

Forwarding Policies

ADD SEGMENT

EXPAND

Segment Name	Connected Gateway	Transport Zone	Subnets	Ports
segmentC1	Tier1   Tier1	TZ-OVERLAY	10.20.8.1/23 CIDR e.g. 10.22.12.2/23 Gateway CIDR IPv6 CIDR e.g. fc7e:f206:db42::1/48	1
<div>EDIT DHCP CONFIG</div> <div>DELETE DHCP CONFIG</div>				
Segment needs to have either Subnets or VPN defined, or both.				
L2 VPN	You have no L2 VPN sessions for this Gateway. For that, go to <a href="#">VPN Services</a> . Note that for L2 sessions to work, you also need			VPN Tunnel ID

Set DHCP Config

Segment segmentC1

IPV4 Gateway10.20.8.1/23

#DHCP Ranges

IPV6 GatewayNot Set

#DHCP Ranges

DHCP Type \*

Gateway DHCP Server

DHCP Profiledhcp

IPv4 Server

IPv6 Server

Settings

Options

DHCP Config

Enabled

DHCP Server Address

10.20.6.1/23

DHCP Ranges

99 Maximum | Format 172.16.14.10-172.16.14.100 or 172.16.14.0/24 | Please verify that IP addresses in this range are not in range to avoid duplicate IP address allocation

10.20.8.10-10.20.8.200

Belong to subnet CIDR

Enter DHCP Ranges

Lease Time (seconds)

86400

DNS Servers

在 Citrix Studio 中创建 Google Cloud VMware 连接

- 1. 在 vCenter 中创建一台计算机并在计算机中安装一对 Cloud Connector。请参阅[配置实例](#)。
- 2. 启动 Citrix Studio。
- 3. 选择托管节点，然后单击添加连接和资源。

4. 在 **Connection**（连接）屏幕上，选择 **Create a new Connection**（创建新连接），然后选择以下详细信息：

**Add Connection and Resources**

1 Connection

2 Storage Manageme...

3 Storage Selection

4 Network

5 Scopes

6 Summary

Create a new connection

Connection type: VMware vSphere®

Connection address: https://10.129.0.6/sdk

[Learn about user permissions](#)

User name: CloudOwner@gve.local

Password: .....

Zone name: VMware-GCP

Connection name: VMware-GCP1

Create virtual machines using:

☒ Citrix provisioning tools (Machine Creation Services or Citrix Provisioning)

Next

Cancel

- 选择连接类型为 **VMware vSphere**。
  - 在 **Connection address**（连接地址）中，输入 vCenter 专用 IP 地址。
  - 输入 vCenter 凭据。
  - 输入连接名称。
  - 选择用于创建虚拟机的工具。
5. 在网络屏幕上，选择在 NSX-T 服务器中创建的子网。
6. 完成向导。

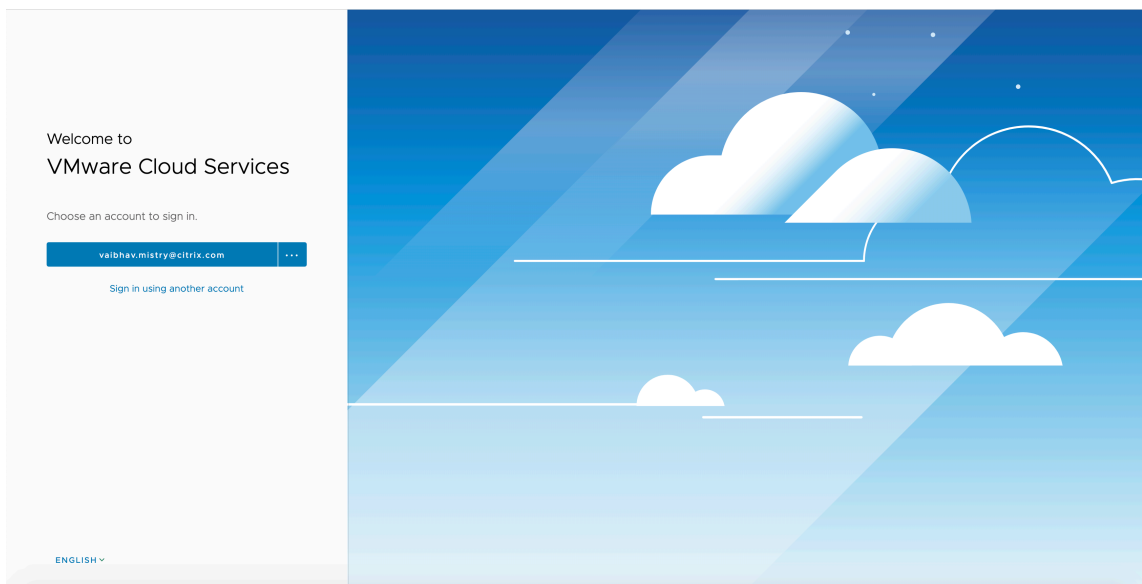
## Amazon Web Services (AWS) 上的 VMware 云

借助 Amazon Web Services (AWS) 上的 VMware 云，您可以将基于 VMware 的本地 Citrix 工作负载迁移到 AWS 云，将核心 Citrix Virtual Apps and Desktops 环境迁移到 Citrix DaaS。

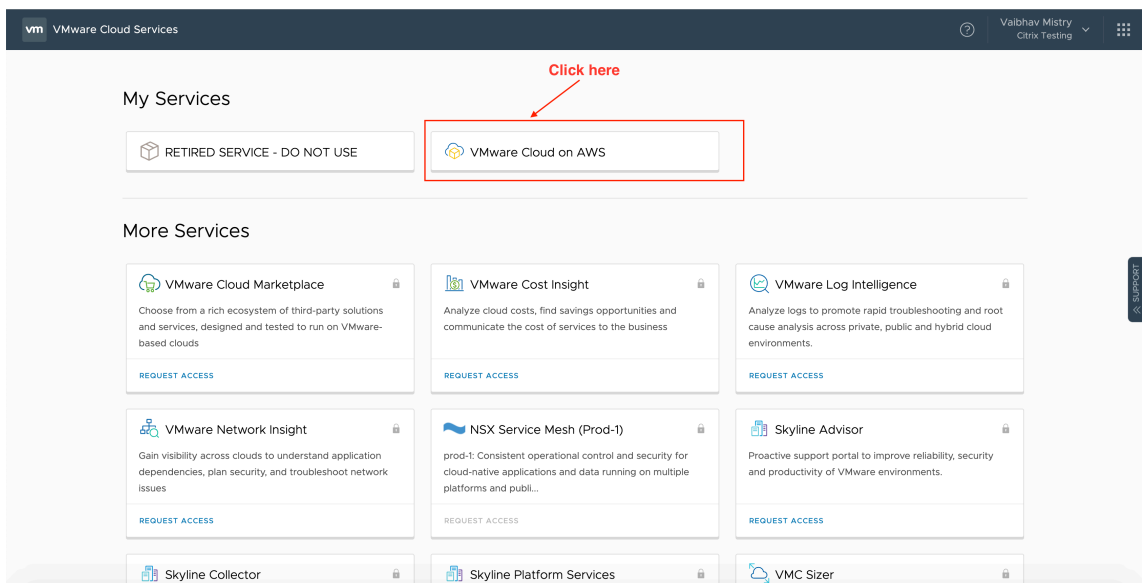
本文介绍了在 AWS 上设置 VMware 云的过程。

访问 **VMware** 云环境

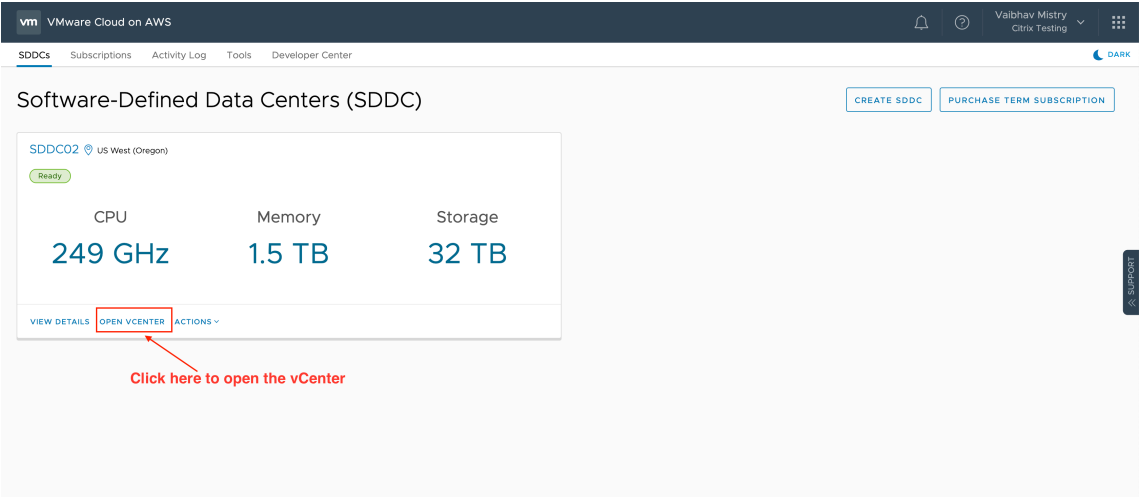
- 使用 URL <https://console.cloud.vmware.com/> 登录 VMware 云服务。



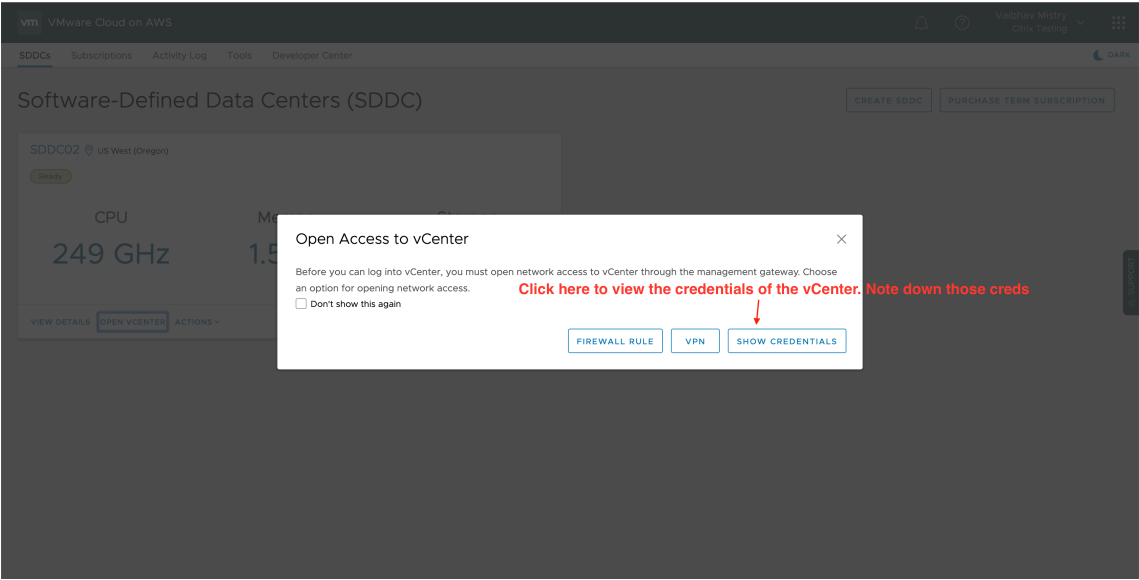
2. 单击 **AWS** 上的 **VMware** 云。此时将显示 “Software-Defined Data Centers (SDDC)”（软件定义的数据中心 (SDDC)）页面。



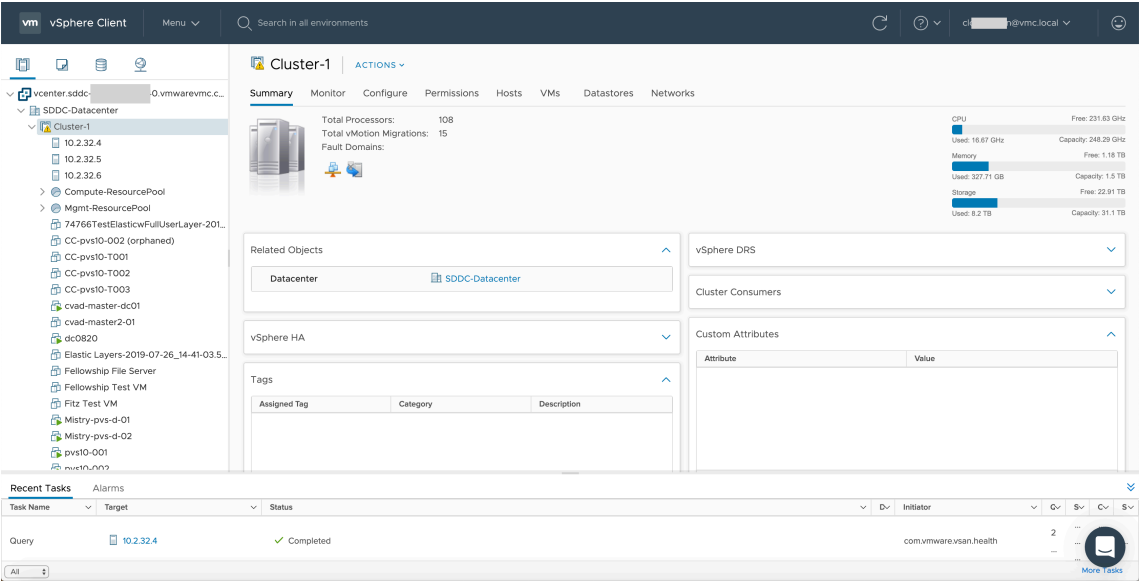
3. 单击 **OPEN VCENTER**（打开 Vcenter），然后单击 **SHOW CREDENTIALS**（显示凭据）。请记住这些凭据以供以后使用。



(打开 vCenter)



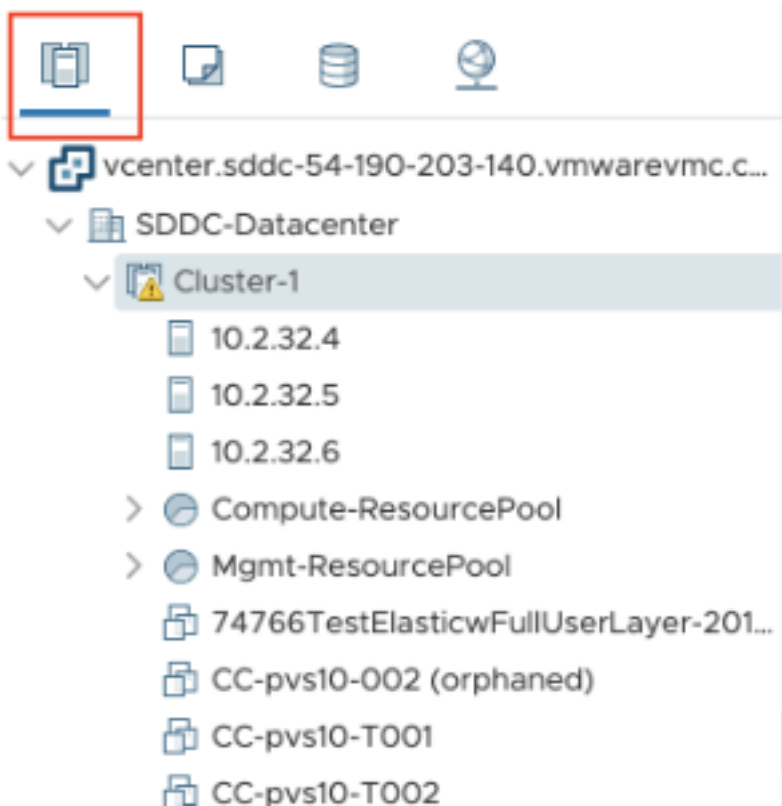
4. 打开 Web 浏览器，然后输入 vSphere Web Client 的 URL。
5. 按照说明输入凭据，然后单击 **Login**（登录）。vSphere 客户端 Web 页面与本地环境类似。



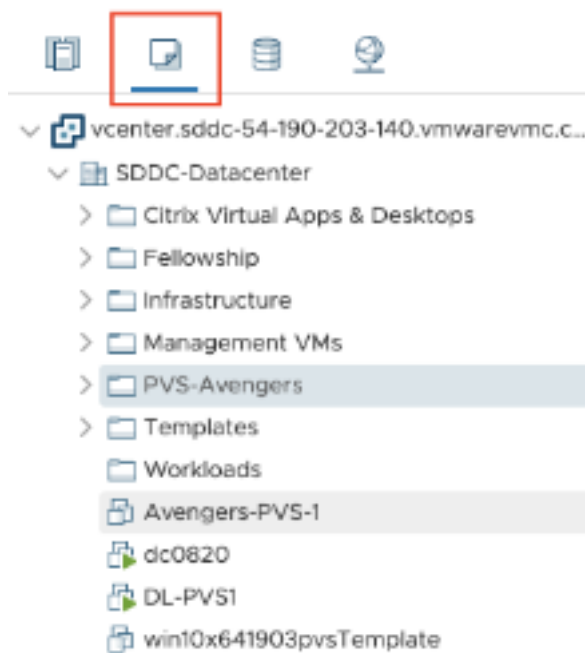
关于 **VMware** 云环境

vSphere 客户端 Web 页面上有四个视图。

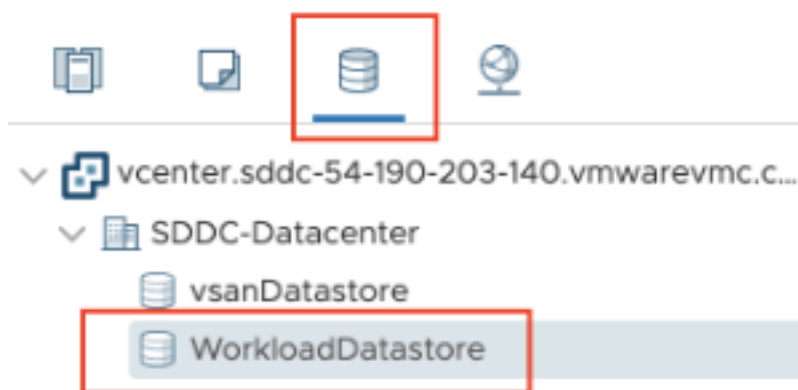
- 主机和群集视图：您无法创建新群集，但云管理员可以创建多个资源池。



- VM 和模板视图：云管理员可以创建许多文件夹。



- 存储视图：在 Citrix Studio 中添加托管单元时选择 **WorkloadDatastore** 存储，因为您只能访问工作负载数据存储服务。



**VMC customers have access to  
Only WorkloadDatastore**



- 网络视图：VMware 云网络和不透明网络的图标有所差别。



设置群集后，请参阅 [VMware 虚拟化环境](#) 以添加连接和资源。

#### 下一步的去向

- 要进行简单的概念验证部署，请在指定用于向用户交付应用程序或桌面的计算机上[安装 VDA](#)。
- 有关创建和管理连接的信息，请参阅[与 VMware 云和合作伙伴解决方案的连接](#)。
- [查看安装和配置过程中的所有步骤](#)。

#### 更多信息

- [创建和管理连接和资源](#)
- [创建计算机目录](#)

## XenServer 虚拟化环境

January 23, 2024

XenServer 可简化您的运营管理，同时确保密集型工作负载的高清用户体验。

要设置您的 XenServer，请参阅[添加资源类型](#)。

#### 下一步的去向

- 要进行简单的概念验证部署，请在指定用于向用户交付应用程序或桌面的计算机上[安装 VDA](#)。
- 有关创建和管理连接的信息，请参阅[与 XenServer 的连接](#)。
- [查看安装和配置过程中的所有步骤](#)。

## 更多信息

- [创建和管理连接和资源](#)
- [创建计算机目录](#)

## Cloud Connector 的大小和规模注意事项

January 23, 2024

在评估 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）以确定规模和可扩展性时，请考虑所有组件。根据您的特定要求研究和测试 Citrix Cloud Connector 和 StoreFront 的配置。如果没有足够的资源来调整规模和可扩展性，则会对部署的性能产生负面影响。

### 注意：

- 除了 Citrix DaaS 之外，这些建议还适用于 [Citrix DaaS Standard for Azure](#)。
- 本文中给出的测试和建议是帮助您开始测试的指南。我们建议您在环境中进行测试，以验证连接器大小是否正确。

本文详细介绍了已测试的最大容量以及针对 Cloud Connector 计算机配置的最佳实践建议。对配置有 StoreFront 和本地主机缓存 (LHC) 的部署进行了测试。

所提供的信息适用于每个资源位置都包含 VDI 工作负载或 RDS 工作负载的部署。对于同时包含 VDI 和 RDS 混合工作负载的资源位置，请联系 Citrix 咨询服务。

Cloud Connector 通过以下方式将您的工作负载链接到 Citrix DaaS：

- 为 VDA 和 Citrix DaaS 之间的通信提供代理
- 为 Citrix DaaS 与 Active Directory (AD) 和虚拟机管理程序之间的通信提供代理
- 在包含 StoreFront 服务器的部署中，Cloud Connector 在云中断期间充当临时会话代理，为用户提供持续的资源访问权限

请务必正确调整 Cloud Connector 的大小和配置，以满足您的特定需求。

每组云连接器都分配给一个资源位置（也称为区域）。资源位置是一种逻辑分隔，用于指定哪些资源与这组 Cloud Connector 进行通信。每个域至少需要一个资源位置才能与 Active Directory (AD) 进行通信。

每个计算机目录和托管连接都分配到一个资源位置。

对于具有多个资源位置的部署，请将计算机目录和 VDA 分配给资源位置，以优化 LHC 在中断期间代理连接的能力。有关创建和管理资源位置的更多信息，请参阅 [连接到 Citrix Cloud](#)。要获得最佳性能，请在与 VDA、AD 服务器和虚拟机管理程序的低延迟连接上配置 Cloud Connector。

### 推荐的处理器和存储

要获得与这些测试中类似的性能，请使用支持 SHA 扩展的现代处理器。SHA 扩展减少了 CPU 的加密负载。推荐的处理器包括：

- 高级微设备 (AMD) Zen 和更新的处理器
- Intel Ice Lake 和更新的处理器

推荐的处理器可以高效运行。您可以使用较旧的处理器，但是，这可能会导致更高的 CPU 负载。我们建议增加 vCPU 数量以抵消这种行为。

本文中描述的测试是使用 AMD EPYC 和 Intel Cascade Lake 处理器执行的。

Cloud Connector 在与云通信时具有沉重的加密负载。使用具有 SHA 扩展的处理器 Cloud Connector 的 CPU 负载较低，这表现为 Windows Local Security Authority Subsystem Service (LSASS) 的 CPU 使用率降低。

Citrix 建议使用具有足够每秒 I/O 操作 (IOPS) 的现代存储，特别是对于使用 LHC 的部署。建议使用固态硬盘 (SSD)，但不需要高级云存储层。Cloud Connector 运行数据库的小型副本的 LHC 场景需要更高的 IOPS。该数据库会定期更新站点配置更改，并在 Citrix Cloud 中断时为资源位置提供代理功能。

### 本地主机缓存的推荐计算配置

当 Cloud Connector 无法与 Citrix Cloud 通信时，本地主机缓存 (LHC) 将允许部署中的连接代理操作继续，从而提高可用性。

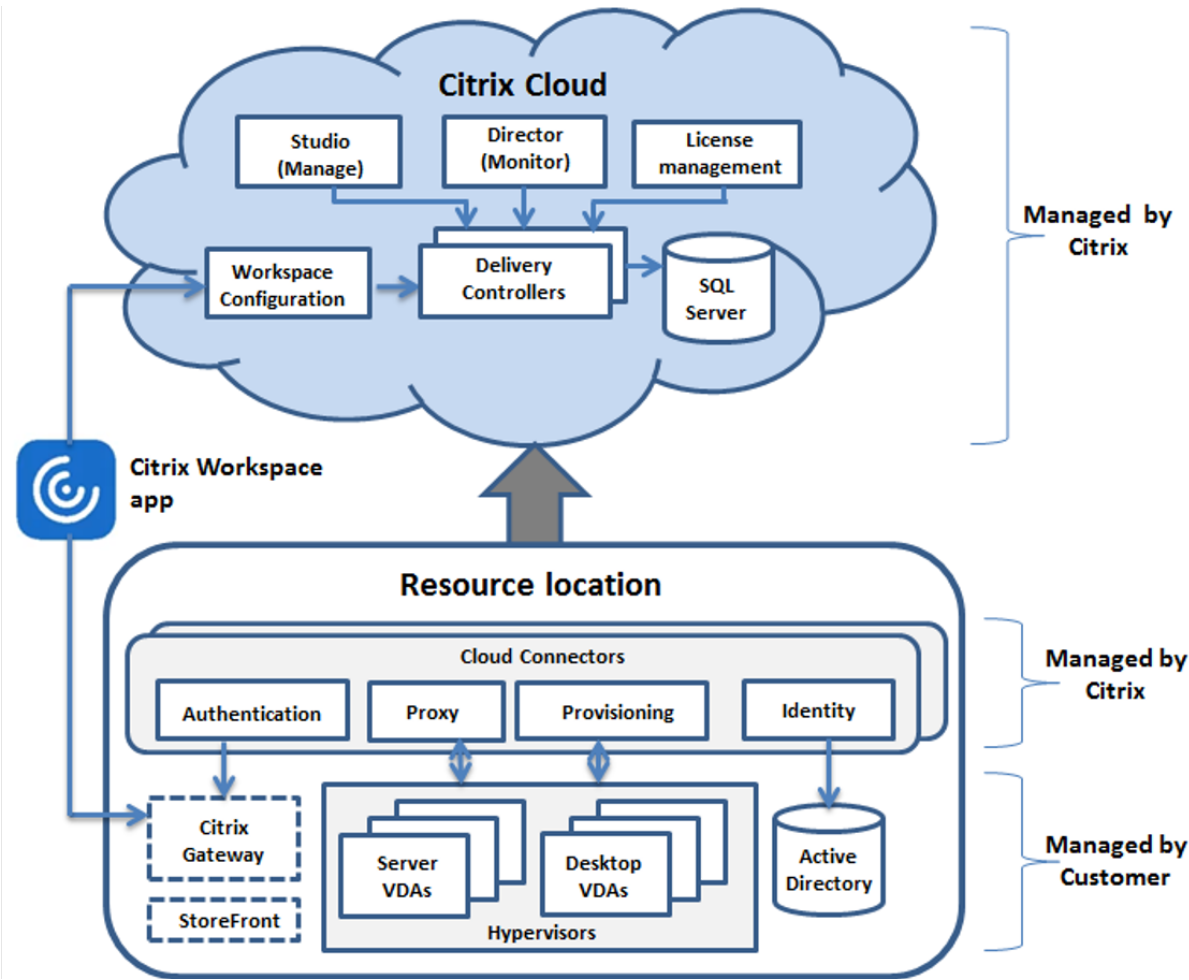
Cloud Connector 运行 Microsoft SQL Express Server LocalDB，它会在您安装 Cloud Connector 时自动安装。Cloud Connector 的 CPU 配置，尤其是 SQL Express Server LocalDB 可用的内核数量，直接影响 LHC 性能。SQL Server Express Server LocalDB 可用的 CPU 内核数量对 LHC 性能的影响甚至超过内存分配。只有在无法访问 Citrix DaaS 且大型强子对撞机代理处于活动状态时，在 LHC 模式下才会观察到此 CPU 开销。对于任何使用 LHC 的部署，Citrix 建议每个插槽四个内核，每个 Cloud Connector 至少有四个 CPU 内核。有关为 SQL Express Server LocalDB 配置计算资源的信息，请参阅[各版本的 SQL Server 计算容量限制](#)。

如果 SQL Express Server LocalDB 可用的计算资源配置错误，则配置同步时间可能会增加，中断期间的性能可能会降低。在某些虚拟化环境中，计算容量可能取决于逻辑处理器的数量，而不是 CPU 内核的数量。

### 测试结果摘要

本摘要中的所有结果均基于本文详细部分中配置的测试环境的结果。此处显示的结果是针对单个资源位置的。不同的系统配置可能会产生不同的结果。

此图以图形方式概述了经测试的配置。



此表提供了调整资源位置规模的快速指南。10k 是单个资源位置的最大值。有关资源位置限制的信息，请参阅[限制](#)。

注意：  
超过限制可能会在中断期间导致连接和性能问题。因此，您不得超过建议的限制，因为这可能会导致 VDA 未注册。

结果基于 Citrix 内部测试。所描述的配置在不同的工作负载下进行了测试，包括高速会话启动测试和注册风暴。

	中	大型	最高
VDA	1000 VDI 或 250 RDS	5000 VDI 或 500 RDS	10000 VDI 或 1000 RDS
托管连接	20	40	40
用于连接器的 <b>CPU</b>	4 vCPU	4 vCPU	8 vCPU
连接器存储器	6 GB	8 GB	10 GB

## 测试方法

进行了测试，以增加负载并测量环境组件的性能。通过收集性能数据和程序计时（例如登录时间和注册时间）来监视组件。有时，会使用专有的 Citrix 仿真工具来模拟 VDA 和会话。这些工具旨在通过与传统 VDA 和会话相同的方式使用 Citrix 组件，而无需满足托管实际会话和 VDA 的相同资源要求。针对使用 Citrix StoreFront 的场景，在云代理和 LHC 模式下进行了测试。

本文中针对 Cloud Connector 大小调整的建议基于从这些测试中收集的数据。

运行了以下测试：

- 会话登录/启动风暴：模拟大容量登录周期的测试。
- **VDA** 注册风暴：模拟大容量 VDA 注册周期的测试。例如，遵循升级周期或在云代理模式和本地主机缓存模式之间过渡。
- **VDA** 电源动作风暴：模拟大量 VDA 电源动作的测试。

## 测试场景和条件

这些测试是在配置了 LHC 的情况下进行的。有关使用 LHC 的更多信息，请参阅 [本地主机缓存](#) 一文。LHC 需要本地 StoreFront 服务器。有关 StoreFront 的详细信息，请参阅 [StoreFront 产品文档](#)。

StoreFront 配置建议：

- 如果您有多个资源位置使用一个 StoreFront 服务器或服务器组，请为 StoreFront 应用商店启用高级运行状况检查选项。请参阅本地主机缓存一文中的 [StoreFront 要求](#)。
- 要获得更高的会话启动率，请使用 StoreFront 服务器组。请参阅 StoreFront 产品文档中的[配置服务器组](#)。

测试条件：

- CPU 和内存要求仅适用于基本操作系统和 Citrix 服务。第三方应用和服务可能需要额外的资源。
- VDA 是运行 Citrix Virtual Delivery Agent 的任何虚拟机或物理机。
- 测试仅使用 Windows VDA 执行。
- 所有测试的 VDA 均使用 Citrix DaaS 进行电源管理。
- 测试了 1000 到 10000 个 VDI 和 250—1000 个 RDS 服务器的工作负载，具有 1000-20000 个会话。
- 对每个资源位置的 RDS 会话进行了多达 20,000 次测试。
- 测试是在正常运行和中断期间使用一个 Cloud Connector 进行的。Citrix 建议使用至少两个云连接器以实现高可用性。在中断模式下，只有一个连接器用于 VDA 注册和代理。
- 测试是使用配置了 Intel Cascade Lake 处理器的 Cloud Connector 进行的。
- 会话是通过单个 Citrix StoreFront 服务器启动的。
- LHC 停机时会启动在机器重新注册后进行的测试。

RDS 会话计数只是一个建议，而不是限制。在您的环境中测试您自己的 RDS 会话限制。

注意：  
对于 RDS 而言，会话计数和启动速率比 VDA 计数更重要。

中等工作负载

这些工作负载使用 4 个 vCPU 和 6 GB 内存进行了测试。

测试工作负载	站点状况	VDA 注册时间	注册 CPU 和 内存使用情况	启动测试长度	会话启动 CPU 和内存 使用情况	启动速率
1000 VDI	联机	5 分钟	CPU 最大值 = 36%, CPU 平均 = 33%, 最大内存 = 5.3 GB	2 分钟	CPU 最大值 = 29%, CPU 平均 = 27%, 最大内存 = 3.7 GB	每分钟 500
1000 VDI	中断	4 分钟	CPU 最大值 = 11%, CPU 平均 = 10%, 最大内存 = 4.5 GB	2 分钟	CPU 最大值 = 42%, CPU 平均 = 28%, 最大内存 = 4.0 GB	每分钟 500
250 RDS, 5000 个会话	联机	3 分钟	CPU 最大值 = 14%, CPU 平均 = 4%, 最大内存 = 3.5 GB	9 分钟	CPU 最大值 = 46%, CPU 平均 = 21%, 最大内存 = 3.7 GB	每分钟 555
250 RDS, 5000 个会话	中断	3 分钟	CPU 最大值 = 15%, CPU 平均值 = 5%, 最大 内存 = 3.7	9 分钟	CPU 最大值 = 51%, CPU 平均 = 32%, 最大内存 = 4.2 GB	每分钟 555

大型工作负载

这些工作负载使用 4 个 vCPU 和 8 GB 内存进行了测试。

测试工作负载	站点状况	VDA 注册时间	注册 CPU 和 内存使用情况	启动测试长度	会话启动 CPU 和内存 使用情况	启动速率
5000 VDI	联机	3—4 分钟	CPU 最大值 = 45%, CPU 平均 = 25%, 最大内 存 = 7.0 GB	5 分钟	CPU 最大值 = 75%, CPU 平均 = 55%, 最大内 存 = 7.0 GB	每分钟 1000
5000 VDI	中断	4—6 分钟	CPU 最大值 = 15%, CPU 平均 = 5%, 最大内存 = 7.5 GB	5 分钟	CPU 最大值 = 45%, CPU 平均 = 40%, 最大内 存 = 7.5 GB	每分钟 1000
500 RDS, 10000 个会 话	联机	3 分钟	CPU 最大值 = 45%, CPU 平均 = 25%, 最大内 存 = 7.0 GB	10 分钟	CPU 最大值 = 75%, CPU 平均 = 55%, 最大内 存 = 7.0 GB	每分钟 1000
500 RDS, 10000 个会 话	中断	3 分钟	CPU 最大值 = 15%, CPU 平均 = 5%, 最 大内存 = 7.5	10 分钟	CPU 最大值 = 45%, CPU 平均 = 40%, 最大内 存 = 7.5 GB	每分钟 1000

最大工作负载

这些工作负载使用 8 个 vCPU 和 10 GB 内存进行了测试。

测试工作负载	站点状况	VDA 注册时间	注册 CPU 和 内存使用情况	启动测试长度	会话启动 CPU 和内存 使用情况	启动速率
10000 VDI	联机	3—4 分钟	CPU 最大值 = 85%, CPU 平均 = 10%, 最大内存 = 8.5 GB	7 分钟	CPU 最大值 = 66%, CPU 平均 = 28%, 最大内存 = 7.0 GB	每分钟 1400

测试工作负载	站点状况	VDA 注册时间	注册 CPU 和		会话启动	
			内存使用情况	启动测试长度	CPU 和内存使用情况	启动速率
10000 VDI	中断	4—5 分钟	CPU 最大值 = 90%, CPU 平均 = 17%, 最大内存 = 8.2 GB	5 分钟	CPU 最大值 = 90%, CPU 平均 = 45%, 最大内存 = 8.5 GB	每分钟 2000
1000 RDS, 20000 个会话	联机	1—2 分钟	CPU 最大值 = 60%, CPU 平均 = 20%, 最大内存 = 8.6 GB	17 分钟	CPU 最大值 = 66%, 平均 CPU = 25%, 最大内存 = 6.8 GB	每分钟 1200
1000 RDS, 20000 个会话	中断	3—4 分钟	CPU 最大值 = 22%, CPU 平均 = 10%, 最大内存 = 8.5	21 分钟	CPU 最大值 = 90%, CPU 平均 = 50%, 最大内存 = 7.5 GB	每分钟 1000

注意：

此处显示的工作负载是针对一个资源位置推荐的最大工作负载。要支持更大的工作负载，请添加更多资源位置。

配置同步资源使用情况

配置同步过程使 Cloud Connector 与 Citrix DaaS 保持同步。更新会自动发送到 Cloud Connector，以确保 Cloud Connector 准备好在发生中断时接管代理。配置同步会更新 LHC 数据库 SQL Express Server LocalDB。该过程将数据导入临时数据库，然后在导入后切换到该数据库。这样可以确保始终有一个 LHC 数据库可以接管。

将数据导入临时数据库时，CPU、内存和磁盘使用量会暂时增加。

测试结果：

- 数据导入时间：7—10 分钟
- CPU 使用率：
  - 最大值 = 25%
  - 平均值 = 15%
- 内存使用情况：
  - 最大值 = 9 GB
  - 将大约 2 GB 增加到 3 GB



- 磁盘使用情况：
  - 4 MB/s 磁盘读取峰值
  - 18 MB/s 磁盘写入峰值
  - 下载和写入 xml 配置文件期间 70 MB/s 的磁盘写入峰值
  - 导入完成时出现 4 MB/s 磁盘读取峰值
- **LHC** 数据库大小：
  - 400—500 MB 数据库文件
  - 200—300 MB 日志数据库

测试条件：

- 已在 8 vCPU AMD EPYC 上进行测试
- 导入的站点配置数据库适用于站点范围内总共有 80,000 个 VDA 和 300,000 个用户（三班制，每个 100,000 个用户）的环境
- 在具有 10,000 VDI 的资源位置测试了数据导入时间

其他资源使用注意事项：

- 在导入过程中，将下载完整的站点配置数据。此下载可能会导致内存峰值，具体取决于站点大小。
- 经过测试的站点总共使用了大约 800 MB 的数据库和数据库日志文件。在配置同步期间，将复制这些文件，最大组合大小约为 1600 MB。确保您的 Cloud Connector 有足够的磁盘空间来存放重复的文件。如果磁盘已满，配置同步过程将失败。

## 安装 **VDA**

February 9, 2024

### 简介

本文开头介绍了 Windows VDA 和可用的 VDA 安装程序。本文的其余部分介绍了 VDA 安装向导中的步骤。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 VDA](#)。

有关 Linux VDA 的信息，请参阅[Linux Virtual Delivery Agent](#)。

查看 VDA 简介。



## 安装注意事项

[Citrix DaaS](#) 一文介绍了 VDA 的定义及其用途。下面是更多信息。

- **分析数据收集**：当安装或升级组件时，会自动收集分析数据。默认情况下，安装完成时，这些数据会自动上载到 Citrix。此外，当您安装组件时，您会自动注册 [Citrix 客户体验改善计划 \(CEIP\)](#)，该计划上载匿名数据。此外，在安装或升级期间，您可以有机会在 Call Home 中注册。

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，该分析程序会建议阅读一篇 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。

有关这些计划的信息，请参阅 [Citrix Insight Services](#)。

- **Citrix Workspace 应用程序**：安装 VDA 时默认不安装适用于 Windows 的 Citrix Workspace 应用程序。可以从 Citrix Web 站点下载并安装或升级适用于 Windows 的 Citrix Workspace 应用程序和其他 Citrix Workspace 应用程序。此外，也可以在 Workspace 或 StoreFront 服务器上提供这些 Citrix Workspace 应用程序。
- **打印后台处理程序服务**：必须启用 Microsoft 打印后台处理程序服务。如果禁用了该服务，则无法成功安装 VDA。
- **Microsoft 媒体基础**：大多数受支持的 Windows 版本都已附带安装媒体基础。如果要安装 VDA 的计算机上未安装 Microsoft 媒体基础（例如 N 版本），多项多媒体功能将不安装且无法运行。
  - Flash 重定向

- 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。

- 本地用户组：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。对于单会话操作系统 VDA，此组仅适用于 RDP 连接。在多会话操作系统 VDA 上，此组仅适用于 ICA 和 RDP 连接。
- **Cloud Connector** 地址要求：VDA 必须至少带有一个用来进行通信的有效 Cloud Connector 地址（在相同的资源位置中）。否则无法建立会话。可以在安装 VDA 时指定 Cloud Connector 地址。有关用来指定可以在其中注册 VDA 的 Cloud Connector 地址的其他方法的信息，请参阅 [VDA 注册](#)。
- 操作系统注意事项：
  - 请查看[系统要求](#)了解支持的平台、操作系统和版本。
  - 确保每个操作系统都维护最新的更新。
  - 确保 VDA 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。
  - [CTX216252](#) 中提供了面向 Windows 10 计算机的优化指导。
  - 如果您尝试在该 VDA 版本不支持的操作系统上安装（或升级到）Windows VDA，则会显示一条介绍您的选项的消息。例如，如果您尝试在较旧的 Windows 计算机上安装最新的 VDA，则会有一条消息引导您前往 [CTX139030](#)。有关详细信息，请参阅[早期版本的操作系统](#)。
- 已安装 **MSI**：安装 VDA 时会自动安装多个 MSI。可以在图形界面的其他组件页面上或使用 CLI 中的 `/exclude` 选项阻止安装某些 MSI。对于其他人来说，防止安装的唯一方法是使用 `/exclude` CLI 选项。
- 已加入域：在安装 VDA 软件之前，请确保计算机已加入域。

## 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，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。

## VDA 安装过程中重新启动

VDA 安装结束时需要重新启动计算机。默认情况下会自动重新启动。

为了尽量减少安装 VDA 过程中所需的其他重新启动次数：

- 请务必在开始安装 VDA 之前安装受支持的 Microsoft .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。

每次重新启动后，VDA 安装将继续进行。如果要从命令行进行安装，可以通过 `/noresume` 选项阻止自动恢复。

将 VDA 升级到版本 7.17 或受支持的更高版本时，升级过程中将重新启动。本次重新启动是不可避免的。

## 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。

## VDA 安装程序

可以直接从 Citrix Cloud 控制台下载 VDA 安装程序。

默认情况下，自解压安装程序中的文件被解压至 **Temp** 文件夹。解压至 **Temp** 文件夹的文件在安装完成后会自动删除。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** 安装多会话操作系统 VDA。

**VDAWorkstationSetup.exe** 安装单会话操作系统 VDA。

**VDAWorkstationCoreSetup.exe** 安装为 Remote PC Access 部署或核心 VDI 安装优化过的单会话操作系统 VDA。Remote PC Access 使用物理计算机。核心 VDI 安装是不用作映像的 VM。此安装程序仅部署 VDA 连接所需的核​​心服务。因此，此安装程序仅支持 VDAWorkstationSetup 安装程序适用的一部分选项。

当前版本的这一安装程序不安装或不包含用于执行以下操作的组件：

- App-V。
- Profile Management。将 Citrix Profile Management 排除在安装之外将影响监视器的显示内容。
- Machine Identity Service。
- 适用于 Windows 的 Citrix Workspace 应用程序。
- Citrix Supportability Tools。
- Citrix Files for Windows。
- Citrix Files for Outlook。
- MCSIO write cache for storage optimization（用于存储优化的 MCSIO 写入缓存）。

此安装程序不安装或包含适用于 Windows 的 Citrix Workspace 应用程序。

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

使用 **VDAWorkstationCoreSetup.exe** 相当于使用 **VDAWorkstationSetup.exe** 安装程序安装单会话操作系统 VDA，并且：

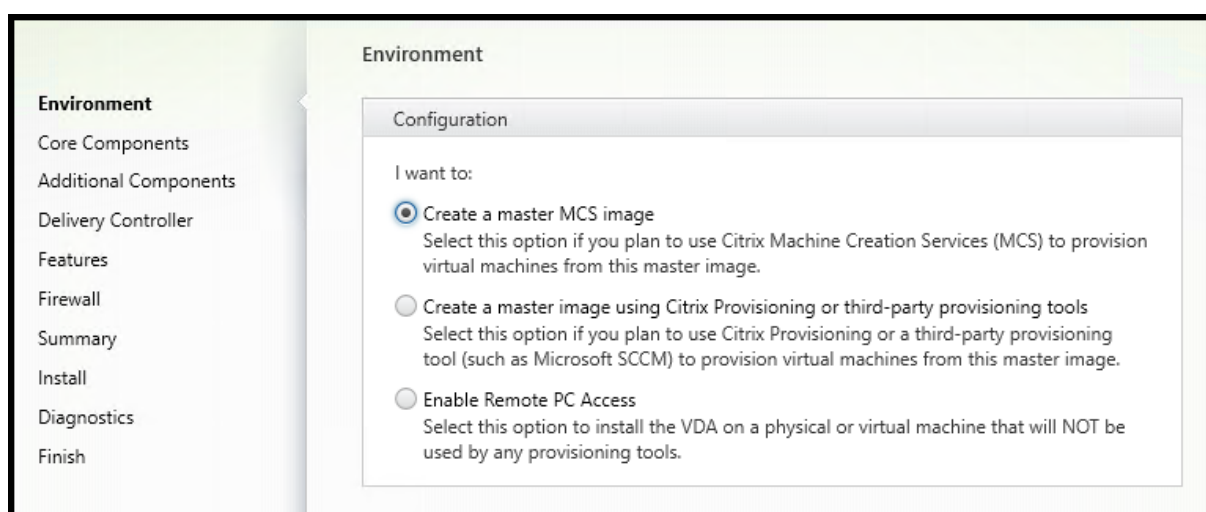
- 在图形界面中：选择环境页面上的 **Remote PC Access** 选项。
- 在命令行界面中：指定 `/remotepc` 选项。
- 在命令行界面中：指定 `/components vda` 和 `/exclude "Citrix Personalization for App-V - VDA""Personal vDisk""Machine Identity Service""Citrix Profile Management""Citrix Profile Management WMI Plugin""Citrix Supportability Tools""Citrix Files for Windows""Citrix Files for Outlook""Citrix MCS IODriver"`。

如果使用 **VDAWorkstationCoreSetup.exe** 安装程序安装 VDA，以后使用 **VDAWorkstationSetup.exe** 安装程序升级该 VDA，则可以有选择地安装忽略的组件和功能。

**步骤 1. 下载产品软件并启动向导**

1. 在要安装 VDA 的计算机上，登录到 [Citrix Cloud](#)。
2. 在左上角的菜单中，在我的服务列表中选择 Citrix DaaS。
3. 在右侧，单击 **Downloads**（下载）并选择 **Download VDA**（下载 VDA）。系统会将您重定向到 VDA 下载页面。找到所需的 VDA 安装程序，然后选择 **Download File**（下载文件）。
4. 下载完成后，右键单击该文件并选择以管理员身份运行。此时将启动安装向导。

作为对步骤 1-3 的替代步骤，您可以直接从 [Citrix 下载页面](#) 下载 VDA。

**步骤 2. 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计算机。您选择的选项会影响自动安装哪些 Citrix 配置工具（如果有），以及 VDA 安装程序的“其他组件”页面上的默认值。

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`

- 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），请选择此选项在 VM 映像上安装 VDA。对于以前已预配的从 Citrix Provisioning 读/写磁盘引导的 VM，请使用此选项。

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：选择此选项可在将不用作映像的物理机或虚拟机上安装 VDA。

命令行选项： `/remotepc`

- (仅显示在多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。

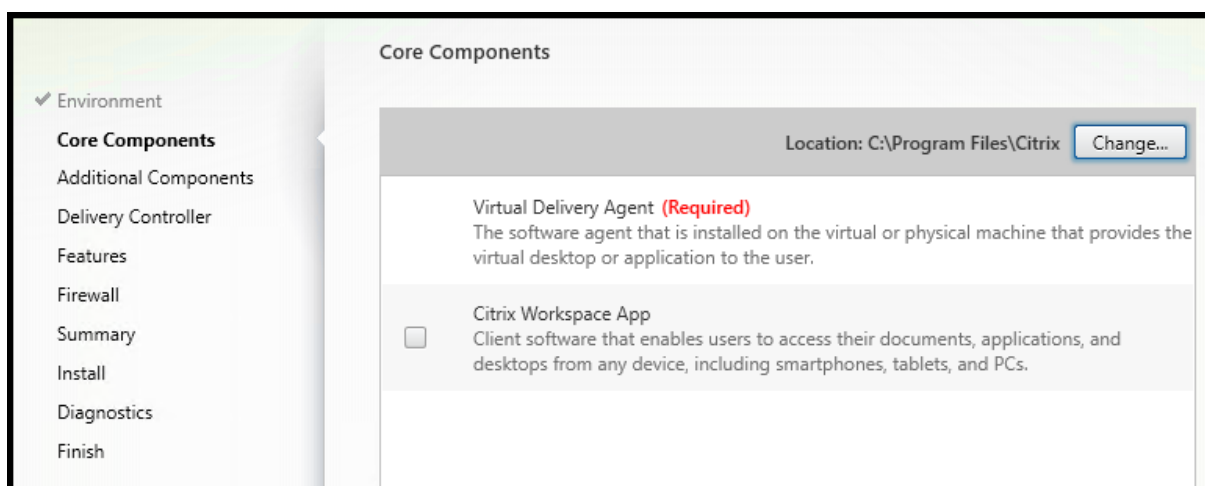
命令行选项: `/remotepc`

选择下一步。

此页面在以下情况下不显示:

- 升级 VDA 时。
- 使用 `VDAWorkstationCoreSetup.exe` 安装程序时。

### 步骤 3. 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。

命令行选项: `/installdir`

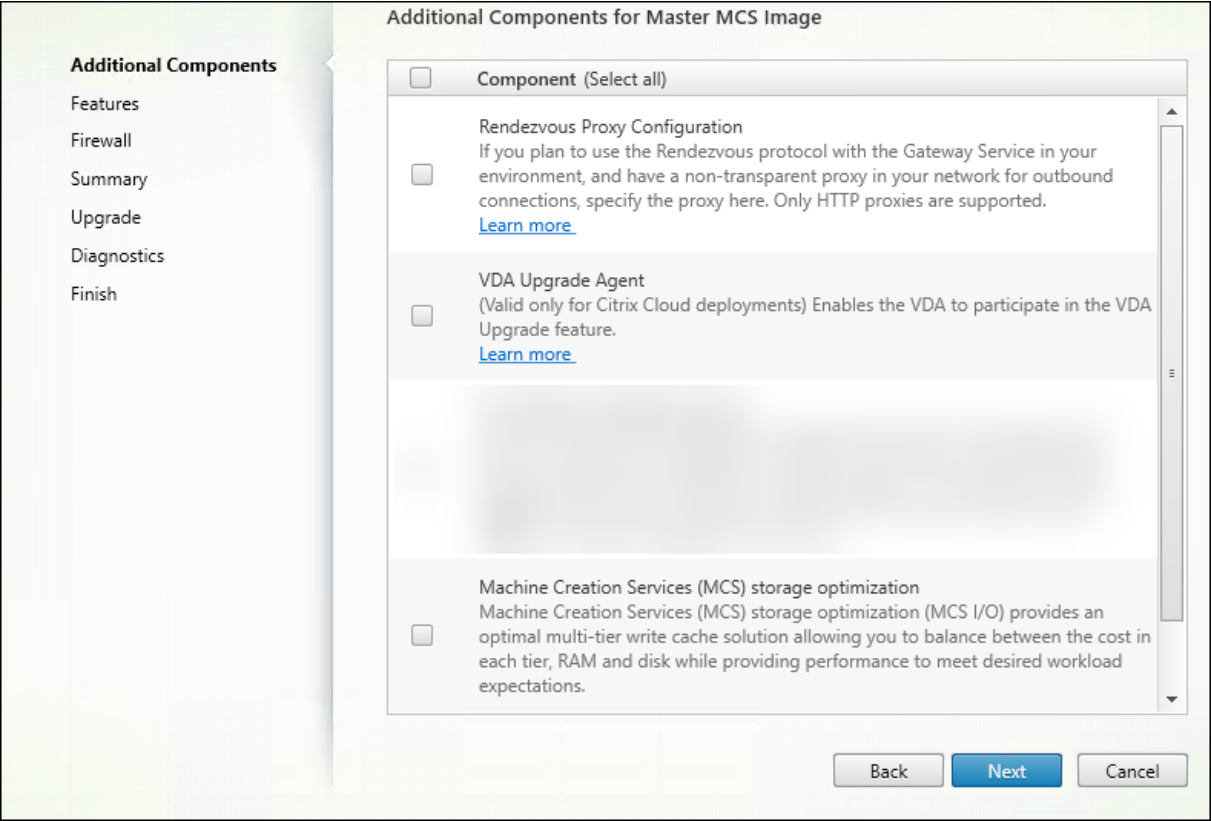
- 组件: 默认情况下, 不会随 VDA 安装适用于 Windows 的 Citrix Workspace 应用程序。如果您使用 `VDAWorkstationCoreSetup.exe` 安装程序, 则从不安装适用于 Windows 的 Citrix Workspace 应用程序, 因此此复选框不显示。

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

选择下一步。



步骤 4. 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）	
Citrix Personalization for App-V 用户个性化层	未选择	未选择	未选择	不显示，因为它不适用于此用例
Citrix Supportability Tools	已选择	已选择	未选择	
Citrix Profile Management	已选择	已选择	未选择	
Citrix Profile Management WMI 插件	已选择	已选择	未选择	



“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 VDA 升级代理	未选择	未选择
Citrix 备份和还原	未选择	未选择
Citrix Files for Windows	未选择	未选择
Citrix Files for Outlook	未选择	未选择
Machine Creation Services (MCS) 存储优化	未选择	未选择
Rendezvous 协议配置	未选择	未选择

此页面在以下情况下不显示：

- 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。
- 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。

组件列表可以包括：

- **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 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

- **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在 Citrix Cloud 中对 VDA 执行的监视和故障排除操作。

- 在监视选项卡的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

- **VDA 升级代理**：（仅适用于 Citrix DaaS 部署。）使 VDA 能够参与 [VDA 升级功能](#)。您可以使用该功能立即或按计划的时间从管理控制台升级目录的 VDA。如果未安装此代理，则可以通过在计算机上运行 VDA 安装程序来升级 VDA。

命令行选项 `/includeadditional "Citrix VDA Upgrade Agent"` 用于启用组件安装，`/exclude "Citrix VDA Upgrade Agent"` 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 文件系统中的映射驱动器与 Citrix Files 交互，不需要完全同步其内容。

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**：此组件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。可以直接在您的电子邮件中提供安全的文件上传请求。有关详细信息，请参阅 [Citrix Files for Outlook](#)。

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

- **Machine Creation Services (MCS) 存储优化**：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

- **Rendezvous 代理配置**：如果计划在环境中将 Rendezvous 协议与 Citrix Gateway 服务结合使用，并且您的网络中有用于出站连接的非透明代理，请安装此组件。仅支持 HTTP 代理。

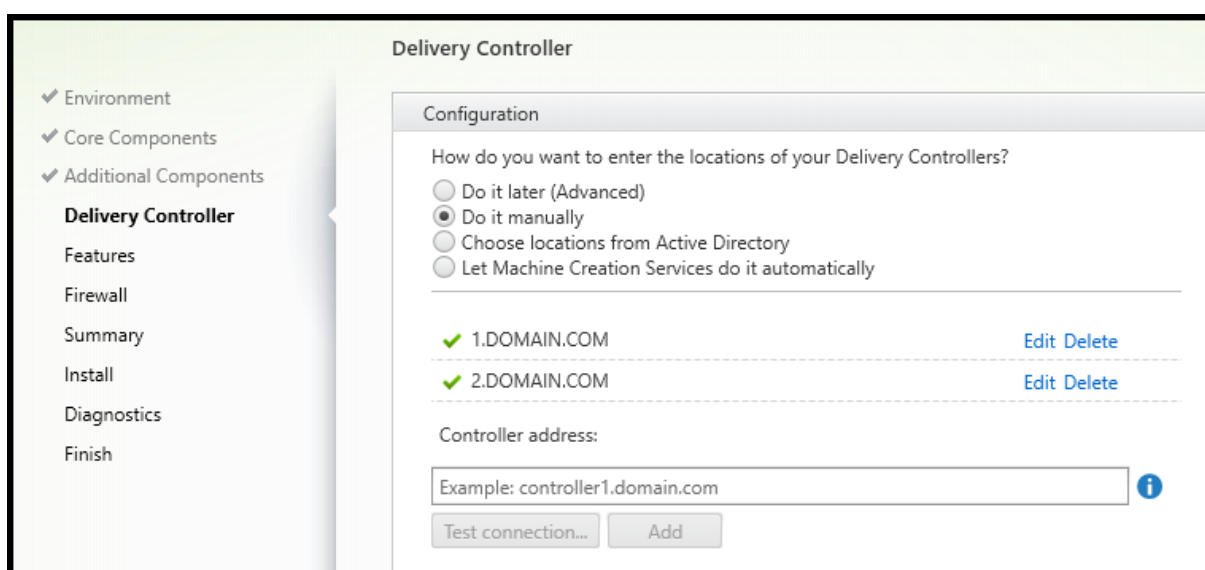
如果安装此组件，请在 **Rendezvous** 代理配置页面上指定代理的地址或 PAC 文件路径。有关功能详细信息，请参阅 [Rendezvous 协议](#)。

命令行选项 `/includeadditional "Citrix Rendezvous V2"` 用于启用组件安装，`/exclude "Citrix Rendezvous V2"` 用于阻止组件安装

- **Citrix** 备份和还原：如果 VDA 安装或升级失败，则此组件可以将计算机恢复到安装或升级之前完成的备份。

命令行选项 `/includeadditional "Citrix Backup and Restore"` 用于启用组件安装，`/exclude "Citrix Backup and Restore"` 用于阻止组件安装。

## 步骤 5. Cloud Connector 地址



在 **Delivery Controller** 页面上，选择手动操作。输入已安装的 Cloud Connector 的 DNS 名称，然后选择添加。如果您在资源位置中安装了其他 Cloud Connector，请添加其 DNS 名称。

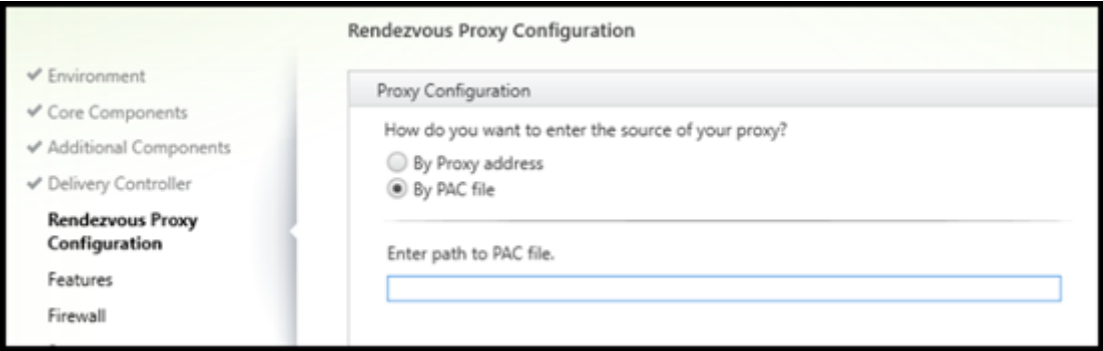
选择下一步。

注意事项：

- 地址只能包含字母数字字符。
- 需要打开用于与 Cloud Connector 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。

命令行选项： `/controllers`

步骤 6. Rendezvous 代理配置



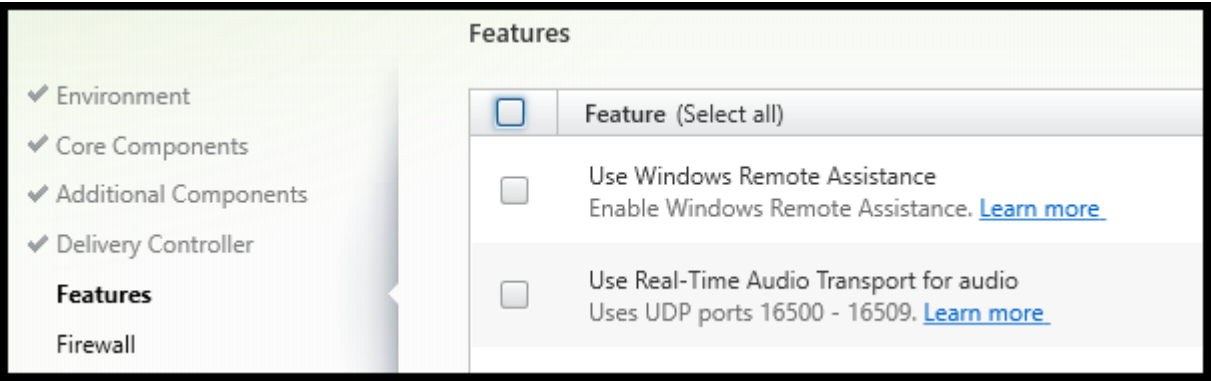
仅当在其他组件页面上启用了 **Rendezvous** 代理配置复选框时，才会显示 **Rendezvous** 代理配置页面。

1. 选择按代理地址还是 PAC 文件路径指定代理源。
2. 指定代理地址或 PAC 文件路径。
  - 代理地址格式: `http://<url-or-ip>:<port>`
  - PAC 文件格式: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

必须打开代理端口的防火墙才能成功进行连接测试。如果无法与代理建立连接，则可以选择是否继续安装 VDA。

命令行选项: `/proxyconfig`

步骤 7. 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 Citrix Cloud 中的 Director 组件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

- 使用屏幕共享：启用后，屏幕共享使用的端口将在 Windows 防火墙中打开。（默认禁用）

命令行选项：/enable\_ss\_ports

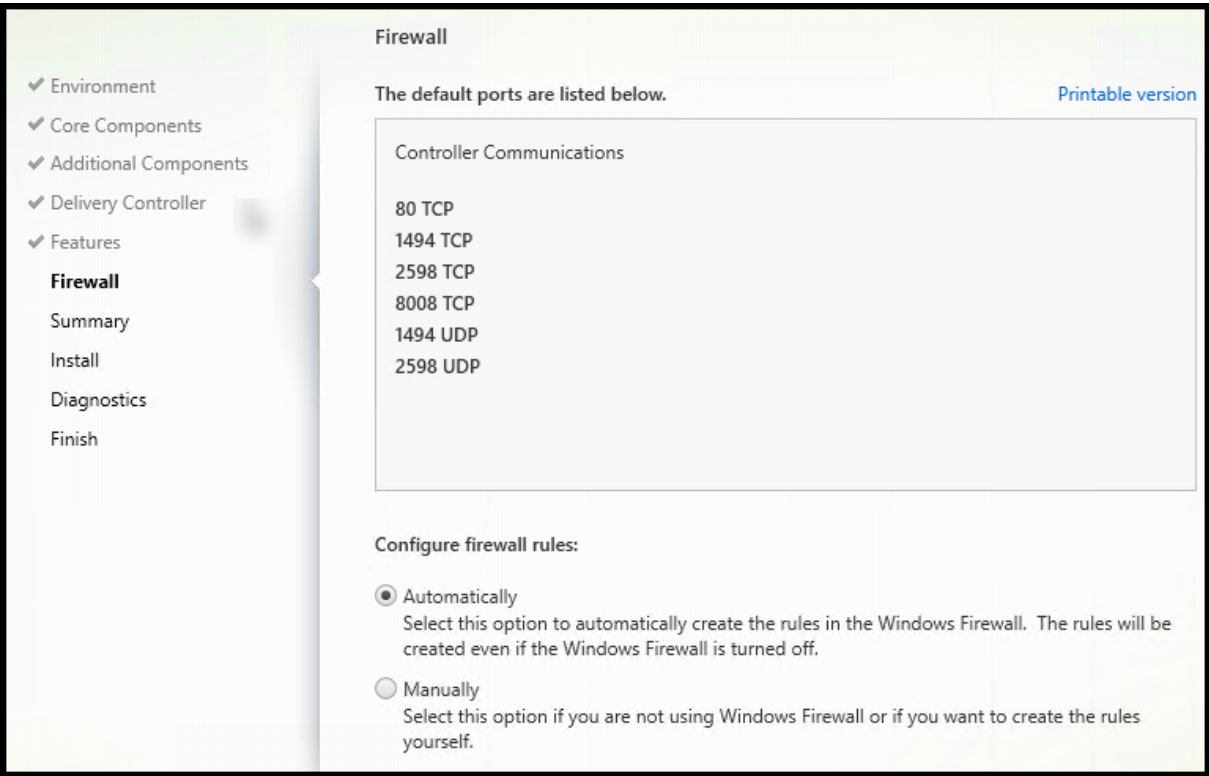
- 此 **VDA** 是否安装在云中的虚拟机上：此设置可帮助 Citrix 正确识别本地部署和服务 (Citrix Cloud) VDA 部署的资源位置，以实现遥测目的。此功能对客户端的利用率没有影响。如果您的部署使用 Citrix DaaS，请启用此设置。（默认禁用）

命令行选项：/xendesktopcloud

选择下一步。

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。

步骤 8. 防火墙端口



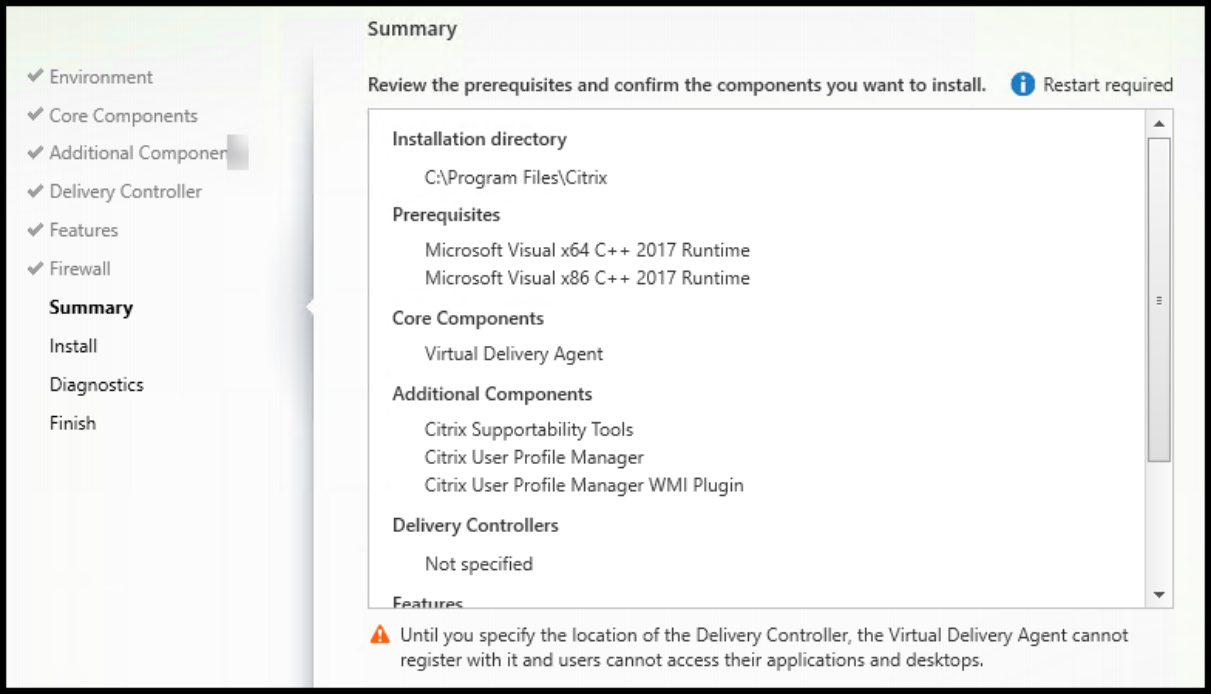
防火墙页面指示 VDA 和 Cloud Connector 用于相互通信的端口。默认情况下，如果 Windows 防火墙服务正在运行，那么即使未启用防火墙，这些端口也会自动打开。此默认设置适用于大多数部署。

有关端口信息，请参阅[网络端口](#)。

选择下一步。

命令行选项: `/enable_hdx_ports`

步骤 9. 查看必备条件并确认安装

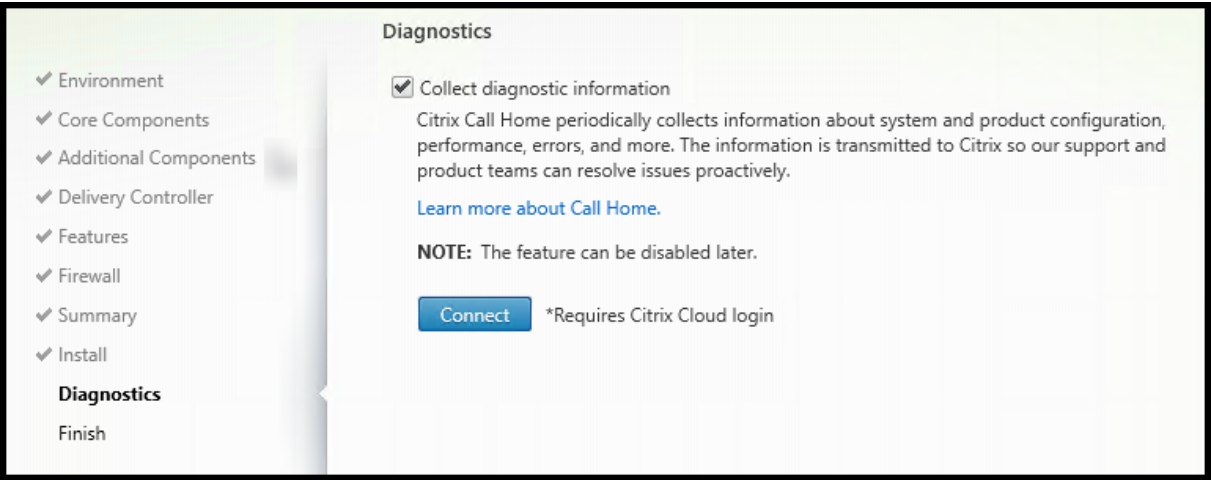


摘要页面上列出将安装的内容。如果需要，可以返回到之前的向导页面并更改选择。

(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，选择安装。

步骤 10. 诊断

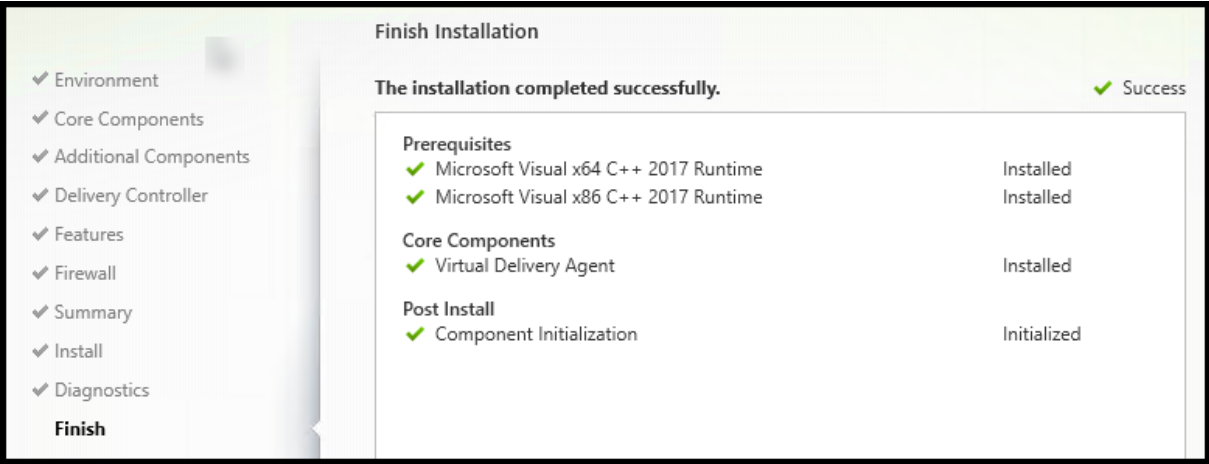


在诊断页面上，选择是否参与 Citrix Call Home。如果您选择参与（默认设置），请选择连接。出现提示时，输入您的 Citrix 帐户凭据。

您的凭据通过验证后（或者如果选择不参与），选择下一步。

有关详细信息，请参阅 [Call Home](#)。

步骤 **11**. 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。

选择完成。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。

如果要在单独的计算机而非映像上安装 VDA，请重复执行上述步骤以根据需要在其他计算机上安装 VDA。

故障排除

在交付组的管理 > 完整配置显示屏幕中，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。

**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。

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**

以后，要自定义已安装的 VDA（或更改其信息），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，更改任何可用的设置。

### 自定义用于与 **Cloud Connector** 通信的端口

您可以根据自己的特定安全要求自定义 VDA 用于与 Cloud Connector 通信的端口。如果您的安全团队不允许打开默认端口（端口 80）或者默认端口已在使用中，则此功能非常有用。

要自定义端口，请完成以下步骤：

1. 在 Citrix Cloud Connector 上添加控制器端口号。
2. 在 VDA 上添加 VDA 端口号。

### 在 **Citrix Cloud Connector** 上添加控制器端口号

转到 Citrix Cloud Connector 并运行以下两个 PowerShell 命令：

- `PS C:\> & 'C:\Program Files\Citrix\XaXdCloudProxy\XaXdCloudProxy.exe'-VdaPort <port number>`
- `PS C:\> & 'C:\Program Files\Citrix\Broker\Service\HighAvailabilityService.exe'-VdaPort <port number> -ConfigureFirewall`

示例：

- `PS C:\> & 'C:\Program Files\Citrix\XaXdCloudProxy\XaXdCloudProxy.exe'-VdaPort 18000`
- `PS C:\> & 'C:\Program Files\Citrix\Broker\Service\HighAvailabilityService.exe'-VdaPort 18000 -ConfigureFirewall`

自定义端口时，请考虑以下事项：

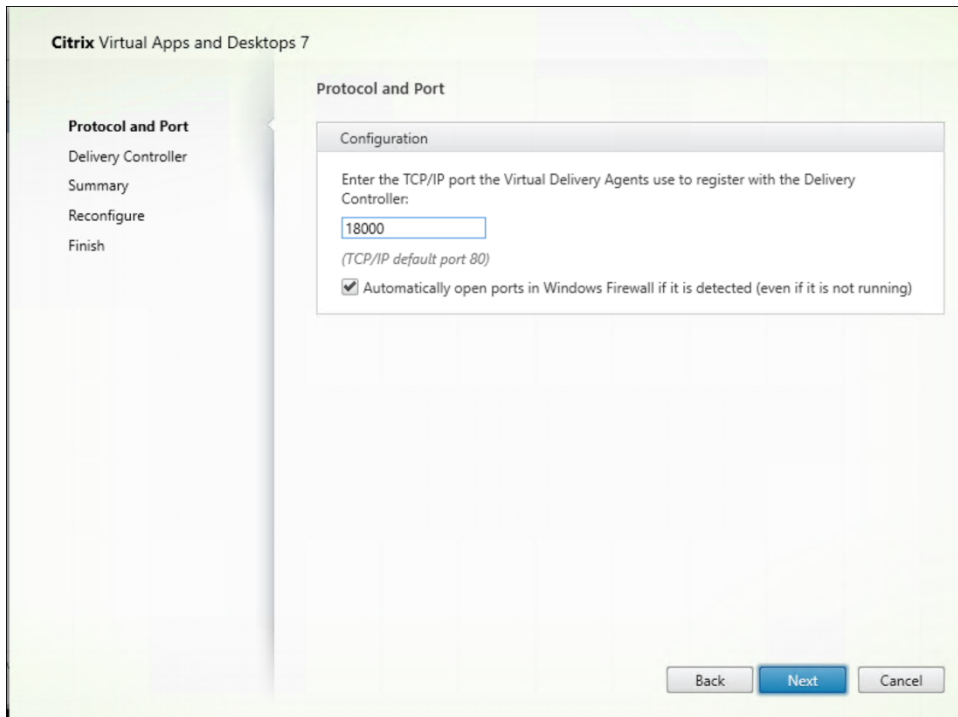
- 必须在两个命令中使用相同的端口号。
- 您必须在所有 *Citrix Cloud Connector* 上运行这两个命令。
- 要成功与 Cloud Connector 通信，请确保所有 VDA 使用相同的端口号。
- 您配置的端口在连接器更新期间仍然存在。

### 在 **VDA** 上添加 **VDA** 端口号

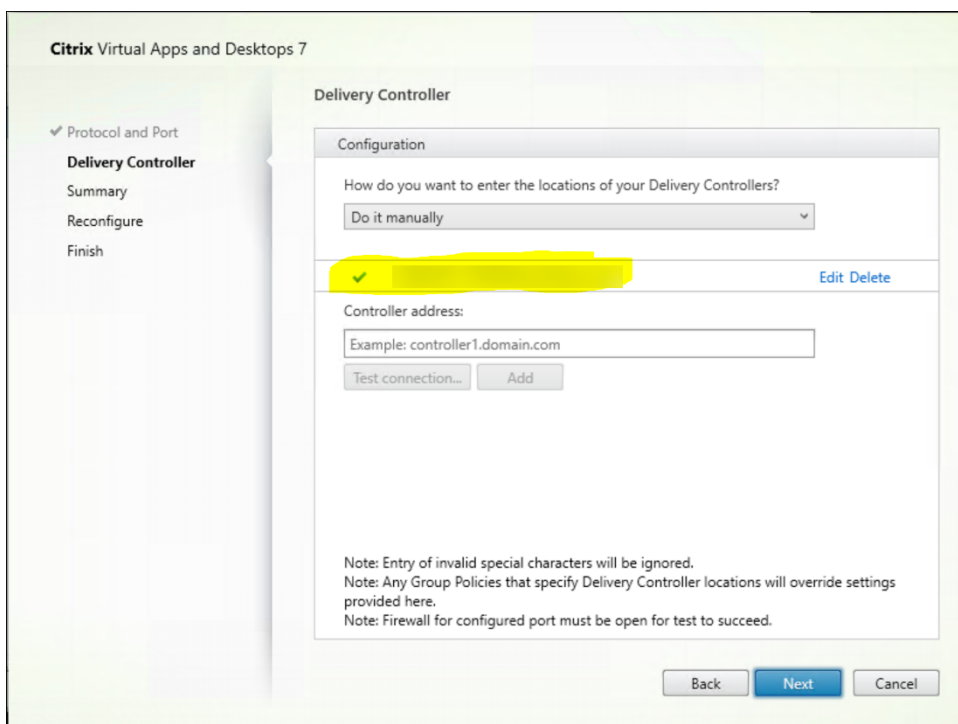
使用默认设置安装 VDA 并按如下方式进行配置。如果已安装 VDA，请继续执行以下步骤。



1. 在VDA上,打开位于C:\Program Files\Citrix\XenDesktopVdaSetup\XenDesktopVdaSetup.exe 的 **XenDesktopVdaSetup.exe**。
2. 在“协议和端口”页面上,添加自定义端口号。



3. 在 **Delivery Controller** 页面上, 输入控制器的 FQDN。



4. 单击“下一步”继续执行向导以完成配置。

然后成功地重新配置端口号。

注意：

在测试 Controller 连接时，您可能会看到以下错误消息：在上找不到正在 < 您输入的 Controller="" 地址=""> 上运行的 Controller 实例。如果地址正确，则可以取消该消息。您输入的 >

## 故障排除

要检查自定义端口的配置是否正确，请转到 Cloud Connector 并执行以下故障排除步骤：

1. 验证以下两个注册表项是否存在。

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\XaXdCloudProxyPersist

名称：CustomVDAPortNumber

类型：REG\_DWORD

数据：18000

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\XaXdCloudProxyPersist

名称：CustomVDAPortNumberHA

类型：REG\_DWORD

数据：18000

2. 运行以下命令创建.txt 文件。

- `netsh http show urlacl > <filepath>.txt`

示例：

- `netsh http show urlacl > c:\reservations.txt`

3. 打开.txt 文件并检查以下四个 URL 以验证是否使用了正确的端口。

- `http://+:18000/Citrix/CdsController/IRegistrar/`
- `http://+:18000/Citrix/CdsController/ITicketing/`
- `http://+:18000/Citrix/CdsController/IDynamicDataSink/`
- `http://+:18000/Citrix/CdsController/INotifyBroker/`

4. 验证是否创建了以下两个防火墙规则，并且所需的端口已打开。

- Citrix XaXdProxy
- Citrix Broker Service (TCP-In)

## 其他信息

- 安装 VDA 后，可以使用 [Cloud Health Check](#) 来检查站点及其组件的运行状况和可用性。

下一步的去向

[创建计算机目录。](#)

要查看整个配置过程，请参阅[规划和构建部署](#)。

## 使用命令行安装 **VDA**

September 1, 2023

### 简介

本文适用于在使用 Windows 操作系统的计算机上安装、升级和自定义 Virtual Delivery Agent (VDA)。

本文介绍如何发出 VDA 安装命令。开始安装之前，请查看[安装 VDA](#) 以了解与安装注意事项、安装程序以及您在安装过程中指定的内容有关的信息。

### 从命令行安装 **VDA**

要安装 VDA（并查看命令执行进度和返回值），必须具有更高的管理权限或使用以管理员身份运行。

1. 在要安装 VDA 的计算机上，登录 [Citrix Cloud](#)。
2. 在左上角的菜单中，选择我的服务 > **DaaS**。
3. 在右上角，单击 **Downloads**（下载）并选择 **Download VDA**（下载 VDA）。您被重定向到 [VDA 下载页面](#)。找到所需的 VDA 安装程序，然后单击“下载文件”。
4. 下载完成后，运行其名称。请使用本文中介绍的选项。
  - 对于多会话操作系统 Virtual Delivery Agent，请运行 `VDAServerSetup.exe`
  - 对于单会话操作系统 Virtual Delivery Agent，请运行 `VDAWorkstationSetup.exe`
  - 对于单会话操作系统核心服务 Virtual Delivery Agent，请运行 `VDAWorkstationCoreSetup.exe`

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`

#### 用于安装 **VDA** 的命令行选项

以下选项在一个或多个命令中有效：`VDAServerSetup.exe`、`VDAWorkstationSetup.exe` 和 `VDAWorkstationCoreSetup.exe`。

- **/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
- 插件：适用于 Windows 的 Citrix Workspace 应用程序

要安装 VDA 和 Citrix Workspace 应用程序，请指定 `/components vda,plugins`。

如果省略 `plugins` 选项，则仅安装 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 Citrix Cloud Connector 的 FQDN，以空格分隔并用直引号引起。请勿同时指定 `/site_guid` 和 `/controllers` 选项。

- **/disableexperiencemetrics**

防止将安装、升级或删除过程中收集的分析自动上载到 Citrix。

- **/enable\_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 `/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 自适应传输功能需要的 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 使用的端口, 除 `/enable_hdx_udp_ports` 选项外, 还请指定 `/enable_hdx_ports` 选项。

- **`/enable_real_time_transport`**

为音频数据包 (实时音频传输) 启用或禁用 UDP。启用该功能可提高音频性能。如果希望在检测到 Windows 防火墙服务时自动打开 UDP 端口, 请包含 `/enable_hdx_ports` 选项。

- **`/enable_remote_assistance`**

在 Windows 远程协助中启用重影功能以与监视功能结合使用。如果指定此选项, Windows 远程协助将在防火墙中打开动态端口。

- **`/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, 即使还原点未使用。

有关详细信息, 请参阅[安装或升级失败时还原](#)。

- **`/enable_ss_ports`**

如果检测到 Windows 防火墙服务, 即使未启用防火墙, 也请在 Windows 防火墙中打开屏幕共享所需的端口。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。

- **`/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 MCS 托管的映像上安装或升级 VDA 需要 Machine Identity Service 组件。有效值为:

- Machine Identity Service
- Citrix Profile Management
- Citrix Profile Management WMI 插件
- Citrix Personalization for App-V - VDA
- Citrix Supportability Tools
- Citrix MCS IODriver
- Citrix VDA 升级代理
- Citrix Rendezvous V2

将 Citrix Profile Management 排除在安装之外 (`/exclude "Citrix Profile Management"`) 将影响从监视选显卡对 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“登录时长”面板失败。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。

如果您计划使用 MCS 预配 VM，请勿排除 Machine Identity Service。

如果您使用相同的组件名称同时指定 `/exclude` 和 `/includeadditional`，则不会安装该组件。

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” ] ...**

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。组件名称区分大小写。

创建 Remote PC Access 部署并要安装默认情况下不包含的组件时，此选项很有用。有效值为：

- Citrix Profile Management
- Citrix Profile Management WMI 插件
- Citrix Personalization for App-V - VDA
- Citrix Supportability Tools
- Citrix MCS IODriver
- Citrix VDA 升级代理
- Citrix Rendezvous V2
- 用户个性化层
- Citrix Web Socket VDA 注册工具

如果您使用相同的组件名称同时指定 `/exclude` 和 `/includeadditional`，则不会安装该组件。

- **`/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。相反，请使用 `/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**

指定此计算机将作为映像与 Citrix Provisioning 或第三方预配工具（例如 Microsoft System Center Configuration Manager）结合使用。

- **/no\_mediafoundation\_ack**

确认不安装 Microsoft 媒体基础，并且多项 HDX 多媒体功能将不安装并且无法运行。如果忽略此操作，并且不安装媒体基础，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**

仅在安装多会话操作系统 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。

- **/proxyconfig** “地址或 PAC 文件路径”

仅当命令包含 [/includeadditional "Citrix Rendezvous V2"](#) 时才有效。与 Rendezvous 协议一起使用的代理的地址或 PAC 文件路径。有关功能详细信息，请参阅 [Rendezvous 协议](#)。

- 代理地址格式：[http://<url-or-ip>:<port>](#)
- PAC 文件格式：[http://<url-or-ip>:<port>/<path>/<filename>.pac](#)

- **/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）。

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\_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）。

- **/remove**

删除通过 `/components` 选项指定的组件。

- **/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 服务器上安装单会话操作系统 VDA。在 Windows 服务器上安装多会话 VDA 时，请忽略此选项。使用此选项前，请参阅[服务器 VDI](#)。

- **/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 是在管理 > 完整配置中显示的站点属性。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。

- **/xendesktopcloud**

表示 VDA 已安装在 Citrix DaaS (Citrix Cloud) 部署中。



## 示例：安装 **VDA**

- 在多会话操作系统上安装 **VDA**。以下命令将在多会话操作系统中安装 VDA。

```
VDASetup.exe /quiet /controllers "Contr-East.domain.com"/  
enable_hdx_ports /masterimage
```

VDA 将用作映像。

- 安装多会话操作系统 **VDA** 或单会话操作系统 **VDA**。以下命令安装多会话操作系统 VDA 或单会话操作系统 VDA。

```
VDASetup_XXXX.exe /quiet /controllers "ddc1.abc.com",  
"ddc2.abc.com"/enable_hdx_ports /enable_Remote_Assistance /  
enable_real_time_transport /enable_ss_ports /noreboot
```

用逗号分隔每个 Delivery Controller FQDN。请注意，XXXX 代表 VDA 版本。

- 在单会话操作系统上安装核心服务 **VDA**。以下命令在单个会话操作系统上安装核心服务 VDA，用于 Remote PC Access 或 VDA 部署。

```
VDAWorkstationCoreSetup.exe /quiet /controllers "Contr-East.  
domain.com"/enable_hdx_ports /noreboot
```

不安装 Citrix Workspace 应用程序和其他非核心服务。指定了 Cloud Connector 的地址，并自动打开 Windows 防火墙服务中的端口。管理员负责处理重新启动。

## 使用命令行自定义 **VDA**

安装 VDA 后，可以自定义多项设置。使用下面的一个或多个选项运行 `XenDesktopVDASetup.exe`。

- `/reconfigure` (自定义 VDA 时需要)
- `/h` 或 `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

## 下一步的去向

- [创建计算机目录](#)
- 要查看整个配置过程，请参阅[规划和构建部署](#)。

## 创建和管理连接和资源

February 20, 2024

### 简介

配置连接包括从支持的虚拟机管理程序和云服务列表中选择连接类型，并为该连接选择适当的存储和网络资源。

注意：

您必须具有完全管理员权限才能执行与连接和资源管理相关的任务。

与连接类型有关的信息的查找位置

[系统要求](#)提供了支持的虚拟机管理程序和云服务版本的列表，以及每台特定主机的文章链接。

### 主机存储

如果存储产品可以通过支持的虚拟机管理程序进行管理，则支持该存储产品。Citrix 支持仅帮助存储产品供应商排除和解决问题，并在必要时在知识中心记录这些问题和解决方案。

预配计算机时，数据将按类型分类：

- 操作系统 (OS)：包括映像
- 临时数据：包括写入 MCS 配置的计算机的所有非持久数据、Windows 页面文件以及与 ShareFile 同步的所有数据。计算机每次重新启动时将丢弃该数据。如果基础映像包含用户个人资料数据，则这些数据将保持不变。如果使用集中式用户配置文件解决方案，则用户配置文件数据将与外部配置文件存储同步。每次计算机重启时，本地缓存的用户配置文件数据将被丢弃。

为不同类型的数据分配不同的存储资源可以最大限度地减少系统负载，并增强每台存储设备上的 IOPS（每秒输入/输出操作数）性能。这种战略分配使主机的可用资源得到最佳利用。此外，它允许根据每种数据类型的特定需求选择最合适的存储介质，例如提高某些类型数据的持久性或弹性。

- 共享和本地存储选项：存储资源可以集中化，即与任何主机分开并由所有主机使用，也可以本地化到特定的虚拟机管理程序。集中式选项包括 Windows 群集共享卷（可能有也可能没有额外的附加存储）或存储供应商提供的设备。集中式存储解决方案可能会提供高级优化功能，例如，特定于虚拟机管理程序的存储控制路径和直接插件访问。
- 本地存储的好处和权衡取舍：在本地存储临时数据可避免进入网络访问共享存储，从而减少共享资源上的 IOPS 负载。虽然集中式存储可能更昂贵，但使用本地存储可能是一种经济实惠的选择。但是，可以根据虚拟机管理程序服务器上是否有足够的存储来权衡这些好处。

## 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）。此数据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。这称为临时数据缓存。本地磁盘有助于降低传输到主操作系统存储的流量。此磁盘在每次计算机重新启动后清除。此磁盘通过直写内存缓存进行访问。请记住，如果为临时数据使用本地存储，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：如果使用群集存储卷 (Clustered Storage Volumes, CSV)，Microsoft System Center Virtual Machine Manager 则不允许在本地存储上创建临时数据缓存磁盘。

如果您在本地存储临时数据，则可以在创建使用该连接的计算机目录时为每个虚拟机的缓存磁盘和内存大小启用和配置非默认值。但是，默认值取决于连接类型，在大多数情况下已经足够了。

虚拟机管理程序还可以通过在本地对磁盘映像进行内存读取缓存来提供优化技术。例如，XenServer 提供 IntelliCache 这样还可以降低传输到中央存储的网络流量。

## 虚拟机管理程序的本地存储

虚拟机管理程序的本地存储在虚拟机管理程序上本地存储数据。使用此方法时，映像和其他操作系统数据将被传输到在站点中使用的所有虚拟机管理程序，用于初始计算机创建和将来的映像更新。这会导致管理网络中存在大量流量。映像传输也很耗时，并且映像对每个主机可用的时间也不同。

## 创建连接和资源

### 重要提示：

创建连接之前，您的资源位置中的主机资源（存储和网络）必须可用。

1. 登录 Citrix Cloud。
2. 导航到左上角的菜单并选择我的服务 > **DaaS**。
3. 在管理 > 完整配置中，选择左侧窗格中的托管。
4. 在操作栏中单击“添加连接和资源”。
5. 该向导将引导您完成以下步骤中描述的配置过程。特定页面内容取决于所选连接类型。完成每个页面上的步骤后，选择“下一步”，直到到达“摘要”页面。

### 注意：

向导中每个页面的内容因您选择的连接类型而异。

步骤 1. 连接

1 Connection

2 Region

3 Network

4 Scopes

5 Summary

Connection

Use an existing connection

BingTest

Create a new connection

Zone name:

Connection type:

Google Cloud Platform

Service account key:

Import key...

Service account ID:

Connection name:

Create virtual machines using:

Citrix provisioning tools (Machine Creation Services or Citrix Provisioning)

Other tools

Next

Cancel

7

在连接页面上：

- 要创建一个新的连接，请选择创建新连接。要基于与现有连接相同的主机配置创建连接，请选择“使用现有连接”，然后选择相关的连接。
- 在区域名称字段中选择一个区域。选项是您配置的所有资源位置。
- 在 连接类型 字段中选择虚拟机管理程序或云服务。这些选项包括所有 Citrix 支持的虚拟机管理程序和云服务：
  - 对于没有可访问的 Cloud Connector 的资源位置，只有支持无连接器部署的虚拟机管理程序和云服务可用。
  - 对于具有可访问的 Cloud Connector 的资源位置，只有在这些连接器上正确安装了插件的虚拟机管理程序和云服务才可用。

或者，您可以使用 PowerShell 命令 `Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable] false` 或 `true` 来获取可用虚拟机管理程序和云服务的列表。

- 输入连接名称。此名称出现在主机显示屏中。
- 选择工具来创建虚拟机。

注意：

连接页面上的信息因您使用的主机或连接类型而异。例如，使用 Azure Resource Manager 时，可以使用现有服务主体或者创建一个新主体。有关详细信息，请参阅[与 Microsoft Azure 的连接](#)。

步骤 2. 管理存储

Add Connection and Resources

1 Connection

2 Storage Management

3 Storage Selection

4 Network

5 Summary

Storage Management

Configure virtual machine storage resources for this connection.

Select a cluster:

Browse

Select an optimization method for available site storage.

☒ Use storage shared by hypervisors

☐ Optimize temporary data on available local storage

☐ Use storage local to the hypervisor

Back

Next

Cancel

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。

有关详细信息，请参阅虚拟机管理程序共享的存储空间和虚拟机管理程序的本地存储。

如果您在 XenServer 池上使用共享存储，请指明是否要使用 IntelliCache 来减少共享存储设备上的负载。请参阅[将 IntelliCache 用于 XenServer 连接](#)。

步骤 3. 存储选择

✓ Connection

✓ Storage Management

③ Storage Selection

④ Network

⑤ Summary

Add Connection and Resources

Storage Selection

When using local storage, you must select the type of data to store on each local storage device; machine operating system data, temporary data, and if not storing personal user data remotely, personal user data. At least one device must be selected for each data type.

Select data storage locations:

Name ↓	OS	Temporary
Library1 on [redacted]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Local storage on [redacted]	<input type="checkbox"/>	<input type="checkbox"/>
System32 on [redacted]	<input type="checkbox"/>	<input type="checkbox"/>
Users on [redacted]	<input type="checkbox"/>	<input type="checkbox"/>

Back

Next

Cancel

有关存储选择的详细信息，请参阅主机存储。

请至少为每种可用的数据类型选择一个主机存储设备。在上一页面中选择的存储管理方法将影响此页面上可供选择的数据类型。必须至少为每种受支持的数据类型选择一个存储设备，才能继续进入向导中的下一页面。

如果您选择“使用虚拟机管理程序共享的存储”，然后在“存储管理”页面上选择“优化可用本地存储上的临时数据”，则可以在存储选择页面上获得更多配置选项。例如，您可以选择使用哪些本地存储设备（在同一个虚拟机管理程序池中）存储临时数据。

系统会显示当前选择的存储设备数量（在图中，显示“已选择 1 个存储设备”）。将鼠标悬停在该条目上时，将显示所选设备的名称（除非未配置任何设备）。

1. 选择选择更改要使用的存储设备。
2. 在“选择存储”对话框中，选中或清除“存储设备”复选框，然后选择“确定”。

步骤 4. 地理区域

注意：

区域页面仅针对某些主机类型显示。

区域选择指明虚拟机的部署位置。实际上，请选择一个靠近用户将在其中访问其应用程序的区域。

步骤 5. 网络

输入资源的名称。此名称在管理控制台中显示，以表示与连接关联的存储和网络组合。

选择 VM 要使用的一个或多个网络。

某些连接类型（例如 Azure Resource Manager）还将列出 VM 要使用的子网。请选择一个或多个子网。

## 步骤 6. 总结

查看您的选择。如果要进行更改，请返回之前的向导页面。完成检查后，请选择完成。

### 注意：

- 如果您在本地存储临时数据，则在创建包含使用此连接的计算机的目录时，可以为临时数据存储配置非默认值。
- 不显示完全访问权限管理员的作用域。有关详细信息，请参阅[管理员、角色和作用域](#)。

## 编辑连接设置

您不能使用此过程来：

- 重命名连接或创建新连接。
- 更改连接的 GPU 设置。访问此资源的目录必须使用相应的 GPU 专用图像。因此，如果要更改 GCP 设置，请创建新连接，而不是编辑现有连接。

## 编辑连接

1. 在管理 > 完整配置中，选择左侧窗格中的托管。
2. 选择连接，然后在操作栏中选择“编辑连接”。
3. 使用“连接属性”页面更改连接地址和凭据。仅当当前主机具有新地址时才更改地址。向另一台计算机输入地址会中断连接的计算机目录。

- 选择编辑设置…，然后输入新信息。
- 要为 XenServer 连接指定高可用性服务器，请选择编辑服务器…，然后选择服务器。Citrix 建议选择池中的所有服务器，以便在池主服务器出现故障时允许与 XenServer 实现通信。

### 注意：

如果您使用的是 HTTPS，想要配置高可用性服务器，请不要为池中的所有服务器安装通配符证书。每台服务器都需要单独的证书。有关详细信息，请参阅[创建与 XenServer 的连接](#)。

4. 使用“高级”页面编辑设置，以指定每个主机连接的最大同步操作（或并发计算机）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。通常情况下，它们不需要更改。

- 同步操作 **(所有类型)** 和同步个人虚拟磁盘清单更新设置指定两个值：一个是可在此连接上同时发生的最大绝对值，另一个是占使用此连接的所有计算机的最大百分比。必须同时指定绝对值和百分比值。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
- 仅在 Citrix 支持代表的指导下在连接选项中输入信息。

5. 使用“范围”页面为该主机选择一个或多个作用域。

注意：

不显示完全访问权限管理员的作用域。根据定义，这些管理员可以访问所有客户管理的 Citrix Cloud 和订阅的服务对象。

有关详细信息，请参阅[管理员、角色和作用域](#)。

6. 使用“共享租户”页面添加通过此连接订阅共享 Azure Compute Gallery 的租户和订阅。

- a) 输入与此连接关联的应用程序的应用程序密钥。借助这些信息，您就可以向 Azure 进行身份验证。我们建议您定期更改密钥以确保安全。
- b) 添加共享租户和订阅。您最多可以添加八个共享租户。对于每个租户，您最多可以添加八个订阅。

7. 单击“保存并应用”以应用您所做的任何更改并保持窗口处于打开状态，或选择“确定”以应用更改并关闭窗口。

## 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. 在管理 > 完整配置中，选择左侧窗格中的托管。
2. 选择连接。要打开维护模式，请在操作栏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。

您也可以为单台计算机开启或关闭维护模式。可以为计算机目录或交付组中的计算机打开或关闭维护模式。

## 删除连接

小心：

如果删除连接，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. 在管理 > 完整配置中，选择左侧窗格中的托管。
2. 选择连接，然后在操作栏中选择删除连接。
3. 如果此连接上存储了计算机，系统会询问您是否删除这些计算机。如果要将其删除，请指定应对关联的 Active Directory 计算机帐户执行的操作。

### 重命名连接

1. 在管理 > 完整配置中，选择左侧窗格中的托管。
2. 选择连接，然后选择“重命名连接”。

### 测试连接

1. 在管理 > 完整配置中，选择左侧窗格中的托管。
2. 选择连接，然后选择“测试连接”。

### 查看连接上的计算机详细信息

1. 在管理 > 完整配置中，选择左侧窗格中的托管。
2. 选择连接，然后在操作栏中选择查看计算机。

上方窗格列出通过此连接访问的计算机。选择某台计算机可在下方窗格查看其详细信息。对于打开的会话，还会提供会话详细信息。

使用搜索功能可快速查找计算机。从窗口顶部的列表中选择保存的搜索，或者创建新的搜索。可以通过键入完整或部分计算机名称进行搜索，也可以构建表达式进行高级搜索。要生成表达式，请选择“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. 在管理 > 完整配置中，选择左侧窗格中的托管。
2. 选择一个连接，然后在操作栏中选择“查看计算机”。
3. 在操作栏中选择以下选项之一。某些操作可能不可用，具体取决于计算机状态和连接主机类型。

- 启动：启动计算机（如果计算机已关闭或挂起）。
- 挂起：不关闭但暂停计算机并刷新计算机列表。
- 关闭：请求关闭操作系统。
- 强制关闭：强行关闭计算机并刷新计算机列表。
- 重新启动：请求关闭操作系统，然后再次启动计算机。如果操作系统无法关闭，则桌面仍保持当前状态。
- 启用维护模式：暂时停止连接到计算机。在此状态下用户无法连接计算机。如果已经连接用户，则维护模式会在其注销后生效。（还可以为通过某个连接进行访问的所有计算机打开或关闭维护模式，请参阅上文。）
- 从交付组中删除：将计算机从交付组中删除并不会将其从交付组使用的计算机目录中删除。仅当计算机未连接任何用户时，才能将其移除。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，用户将不再具有访问该计算机的权限，该计算机将从计算机目录中删除。删除计算机之前，应确保所有用户数据都已备份，或者不再需要这些数据。仅当计算机未连接任何用户时，才能将其删除。在删除计算机时，可打开维护模式暂时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，则会关闭电源。如果 Windows 尝试在关闭期间安装更新，可能面临在更新完成前计算机关机的风险。

## 编辑存储

您可以显示用于存储使用连接的虚拟机的操作系统、临时和个人 (PvD) 数据的服务器的状态。还可以指定用于每种数据类型的存储的服务器。

1. 在管理 > 完整配置中，选择左侧窗格中的托管。
2. 选择相应连接，然后在操作栏中选择编辑存储。
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. 选择确定。

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。未向此存储中添加任何新计算机。
- 未使用：存储未用于创建计算机。

如果清除当前正在使用的设备的复选框，则其状态将更改为“已取代”。现有计算机将继续使用该存储设备（并且可以向其写入数据）。因此，即使在停止用于创建计算机之后，该位置也可能会变为满载。

## 检测孤立的 **Azure** 资源

孤立资源是系统中存在的未使用资源，它们可能会导致不必要的开支。

此功能允许您在云站点的主机中检测孤立的 **Azure** 资源。

按照 Citrix DaaS 上的步骤进行操作：

1. 在管理 > 完整配置中，选择左侧窗格中的托管。
2. 选择一个连接，然后在操作栏中选择“检测孤立资源”。**Detect Orphaned Resources**（检测孤立资源）对话框显示孤立资源报告。
3. 要查看孤立资源报告，请选择查看报告。

或者，您可以使用 PowerShell 检测孤立的 Azure 资源。有关详细信息，请参阅[检索孤立资源列表](#)。

要了解孤立资源背后的原因并了解如何进一步继续操作，请参阅[Efficiently manage Orphaned Azure resources with Citrix](#)（使用 Citrix 高效管理孤立的 Azure 资源）。

## 连接计时器

可以使用 Citrix 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：确定在注销会话之前，断开连接、锁定的虚拟桌面可以保持锁定状态的时间。使用断开连接的会话计时器和断开连接的会话计时器间隔策略设置。

如果更新其中任何一项设置，请确保部署中的设置一致。

有关详细信息，请参阅策略设置文档。

## 编辑资源网络

您可以更改网络以进行连接。请执行以下操作：

1. 转到管理 > 完整配置 > 托管。
2. 选择连接下的目标资源，然后在操作栏中选择“编辑网络”。
3. 选择一个或多个网络供虚拟机使用。
4. 单击“保存”保存更改并退出。

## 删除、重命名或测试资源

1. 在管理 > 完整配置中，选择左侧窗格中的托管。
2. 选择连接下的目标资源，然后在操作栏中选择相应的条目：
  - 删除资源
  - 重命名资源
  - 测试资源

## 检索孤立资源列表

您可以获得由 MCS 创建但 MCS 不再跟踪的孤立资源列表。这当前适用于 Azure 环境。要获取列表，您可以使用 PowerShell 命令。可以使用连接进行筛选。

注意：

如果正在进行任何预配或映像更新，PowerShell 命令将被拒绝。

## 限制

- 只有内置的完全权限管理员或云管理角色管理员用户才能运行 PowerShell 命令并获取孤立资源列表。
- 为避免错误识别孤立资源，在筛选孤立资源时不要打开虚拟机的电源。
- 如果工作量可能很大，则将大约 2,000 条记录显示为孤立记录。

## 显示孤立资源列表

### 显示孤立资源列表

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*`。
3. 运行以下命令：
  - a) 获取连接 UID。连接 uid 是 HypervisorConnectionUid 属性的值。

```
1 Get-ChildItem xdhyp:\connections | where {  
2   $_.PluginId -like 'Azure*' }  
3 "  
4 <!--NeedCopy-->
```

- b) 获取孤立资源列表。

```
1 get-provorphanedresource  
2 -HypervisorConnectionUid <connection uid>  
3 <!--NeedCopy-->
```

## 显示订阅 ID 中的孤立资源列表

要显示订阅 ID 中的孤立资源列表，请执行以下操作：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*`。
3. 运行以下命令：

- a) 使用订阅 ID 查找连接 UID。连接 uid 是 HypervisorConnectionUid 属性的值。

```
1 Get-ChildItem xdhyp:\connections | where {
2     $_.CustomProperties -match '<subscriptionId>' }
3
4 <!--NeedCopy-->
```

- b) 获取孤立资源列表。

```
1 get-provorphanedresource -HypervisorConnectionUid <connection
   uid>
2 <!--NeedCopy-->
```

注意：

在删除之前，请仔细检查资源。

## 下一步的去向

- 有关与特定主机类型的连接的信息，请参阅：
  - [与 AWS 的连接](#)
  - [与 Google Cloud 环境的连接](#)
  - [与 Microsoft Azure 的连接](#)
  - [与 Microsoft System Center Virtual Machine Manager 的连接](#)
  - [与 Nutanix 的连接](#)
  - [与 Nutanix 云和合作伙伴解决方案的连接](#)
  - [与 VMware 的连接](#)
  - [与 VMware 云和合作伙伴解决方案的连接](#)
  - [连接到 XenServer](#)

如果您正在执行初始部署过程，请[创建计算机目录](#)。

## 与 **AWS** 的连接

March 5, 2024

[创建和管理连接和资源](#)介绍了用于创建连接的向导。以下信息涵盖了特定于 AWS 云环境的详细信息。

注意：

在创建与 AWS 的连接之前，您需要先完成将 AWS 设置为资源位置。请参阅 [AWS 虚拟化环境](#)。

创建连接

从“完整配置”界面创建连接时：

- 必须提供 API 密钥和密钥值。可以先从 AWS 中导出包含这些值的密钥文件，然后再导入。此外，还必须提供地理区域、可用性区域、VPC 名称、子网地址、域名、安全组名称和凭据。
- root AWS 帐户的凭据文件（从 AWS 控制台检索）的格式与为标准 AWS 用户下载的凭据文件的格式不同。因此，Citrix DaaS 无法使用该文件填充 API 密钥和密钥字段。请务必使用 AWS Identity Access Management (IAM) 凭据文件。

注意：

创建连接后，尝试更新 API 密钥和密钥可能会失败。要解决此问题，请检查您的代理服务器或防火墙限制，并确保以下地址可访问：[https://\\*.amazonaws.com](https://*.amazonaws.com)。

限制

如果您在 AWS 控制台中更改 AWS 虚拟私有云 (VPC) 的名称，则 Citrix Cloud 中的现有托管单元会中断。托管单元损坏时，您将无法创建新目录，也无法将计算机添加到现有目录。要解决此问题，请将 AWS VPC 的名称改回原来的名称。

主机连接默认值

在 AWS 云环境的完整配置界面中创建主机连接时，将显示以下默认值：

选项	绝对值	百分比
同步操作 (所有类型)	125	100
每分钟最大新操作数	150	不适用
最大并发预配操作数	100	不适用

默认情况下，MCS 最多支持 100 个并发预配操作。

您可以通过访问“编辑连接”屏幕上的 Citrix Studio 高级 部分来配置这些值：

Edit Connection

citrix-demet-rba

Connection Properties

Advanced

Scopes

Advanced

Use these settings to specify a maximum number of simultaneous actions (or concurrent machines) per hosting connection. For simultaneous actions, specify both settings. The lower value overrides the higher value. [Learn more](#)

Simultaneous actions (all types): ?

Absolute

Percentage (%)

125

100

Maximum new actions per minute:

75

Connection options:

Use this setting only when Citrix Technical Support or the product documentation makes the recommendation.

或者，您可以使用 Remote PowerShell SDK 为每个环境设置最佳设置的最大并发操作数。

使用 PowerShell 自定义属性 `MaximumConcurrentProvisioningOperations` 指定并发 AWS 预配置操作的最大数量。

配置之前：

- 确保您已经安装了适用于云的 PowerShell SDK。
- 了解 `MaximumConcurrentProvisioningOperations` 的默认值是 100。

要自定义 `MaximumConcurrentProvisioningOperations` 值，请执行以下步骤：

1. 打开 **PowerShell** 窗口。
  2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
  3. 输入 `cd xdhyp:\Connections\`。
  4. 输入 `dir` 以列出连接。
  5. 更改或初始化自定义属性字符串：
    - 如果“自定义属性”字符串具有值，请将“自定义属性”复制到记事本中。接下来，将 `MaximumConcurrentProvisioningOperations` 属性更改为首选值。您可以输入介于 1—1000 范围内的值。
- 例如，`<Property xsi:type="IntProperty" Name="MaximumConcurrentProvisioningOperations" Value="xyz"/>`。

- 如果“自定义属性”字符串为空/空,则必须通过为架构和 `MaximumConcurrentProvisioningOperations` 属性输入正确的语法来初始化该字符串。

6. 在 **PowerShell** 窗口中, 粘贴记事本中修改过的自定义属性, 并为修改后的自定义属性分配一个变量。如果您初始化了自定义属性, 请在语法后面添加以下几行:

```
$customProperties = '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><Property xsi:type="IntProperty" Name="MaximumConcurrentProvisioningOperations" Value="100"/></CustomProperties>'
```

此字符串将 `MaximumConcurrentProvisioningOperations` 属性设置为 100。在“自定义属性”字符串中, 必须将 `MaximumConcurrentProvisioningOperations` 属性设置为符合需要的值。

7. 输入 `Get-XDAuthentication`, 这会提示您输入凭据。
8. 运行 `$cred = Get-Credential`, 这可能会提示您仅输入密码 (或名称和密码)。还可能会提示您输入应用程序 ID 和关联密钥。对于使用基于角色的身份验证的连接, `role_based_auth` 既是名称又是密码。否则, 请输入 AWS API ID 和密钥。
9. 运行 `set-item -PSPath 'XDHyp:\Connections<connection-name>' -CustomProperties $customProperties -username $cred.username -Securepassword $cred.password`。必须将 <连接名称> 设置为连接的名称。
10. 输入 `dir` 以验证更新的 CustomProperties 字符串。

## 服务端点 URL

### 标准区域服务端点 URL

使用 MCS 时, 会添加一个带有 API 密钥和 API 机密的新 AWS 连接。借助这些信息以及经过身份验证的帐户, MCS 使用 AWS DescribeRegions EC2 API 调用向 AWS 查询支持的区域。查询是使用通用 EC2 服务端点 URL <https://ec2.amazonaws.com/> 进行的。请使用 MCS 从支持的区域列表中选择用于连接的区域。系统会自动为区域选择首选的 AWS 服务端点 URL。但是, 在创建服务端点 URL 之后, 您将无法再设置或修改该 URL。

### 非标准服务端点 URL

在某些情况下, 您可能不需要使用为连接自动选择的 AWS 服务端点 URL。对于此类情况, 您可以使用 Citrix Cloud SDK 和 PowerShell 创建具有非标准服务端点 URL 的连接。例如, 要使用服务端点 URL <https://ec2.cn-north-1.amazonaws.com.cn> 创建连接, 请执行以下操作:

1. 设置 AWS 托管的 Cloud Connector 并确保其具有连接性。



2. 运行以下 PowerShell 命令以查看 Cloud Connector 的列表。

```
1 PS C:> asnp citrix.*
2 PS C:> Get-XDAAuthentication
3 PS C:> Get-ConfigEdgeServer
4 <!--NeedCopy-->
```

3. 从新创建的 Cloud Connector 中找到 ZoneUid，然后将其输入到以下 PowerShell 命令中。用相应的值替换斜体项目。

```
PS C:\> $hyp= New-Item -Path xdhyp:\Connections -ZoneUidZoneUid-
Name "My New Connection" -ConnectionType "AWS"-HypervisorAddress @
("https://ec2.cn-north-1.amazonaws.com.cn")-UserName "APIkey" "-
PasswordAPI Secret" -Persist
PS C:\> New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hyp. HypervisorConnectionUid
```

4. 刷新完整配置 > 托管选项卡以验证 EC2 连接是否已创建。
5. 使用新连接添加资源位置。

## 定义 IAM 权限

使用本部分中的信息定义 AWS 上的 Citrix DaaS 的 IAM 权限。Amazon 的 IAM 服务允许帐户拥有多个用户，这些用户可以进一步组织到组中。这些用户可以拥有不同的权限来控制其执行与帐户关联的操作的能力。有关 IAM 权限的更多信息，请参阅 [IAM JSON 策略参考](#)。

要将 IAM 权限策略应用到新用户组，请执行以下操作：

1. 登录 AWS 管理控制台，然后从下拉列表中选择 **IAM service** (IAM 服务)。
2. 选择 **Create a New Group of Users** (创建新用户组)。
3. 键入新用户组的名称，然后选择 **Continue** (继续)。
4. 在权限页面上，选择自定义策略，然后选择选择。
5. 键入权限策略的名称。
6. 在“策略文档”部分中，输入相关权限。

输入策略信息后，选择“继续”以完成 IAM 权限策略对用户组的应用。租中的用户仅被授予执行 Citrix DaaS 所需操作的权限。

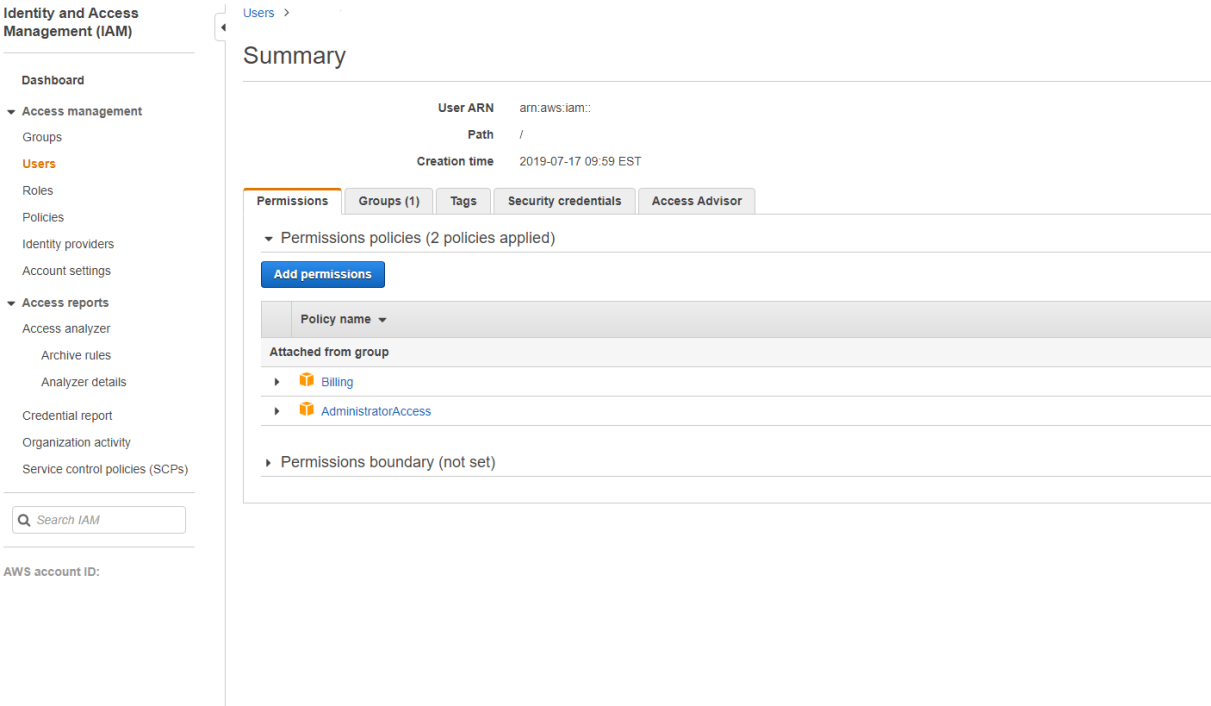
### 重要提示：

使用以下示例中提供的策略文本列出 Citrix DaaS 在 AWS 帐户内执行操作时使用的操作，而不将这些操作限制在特定资源上。Citrix 建议您将该示例用于测试目的。对于生产环境，您可以选择添加对资源的进一步限制。

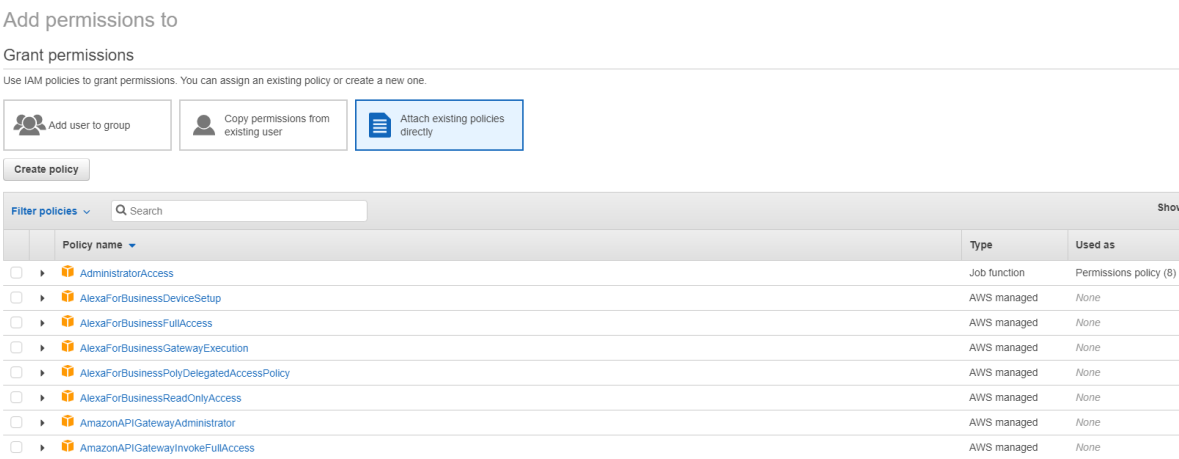
添加 IAM 权限

在 AWS 管理控制台的 IAM 部分添加权限：

- 1. 在摘要面板中，选择权限选项卡。
- 2. 选择添加权限。



在将权限添加到屏幕中，授予权限：



在 JSON 选项卡中使用以下内容作为示例：

Create policy

12

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editorJSON

Import managed policy

1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "VisualEditor0",  
6       "Effect": "Allow",  
7       "Action": [  
8          "ec2:CreateTags",  
9          "ec2:DeleteTags",  
10         "ec2:DescribeTags",  
11         "ec2:PutObjectTagging",  
12         "ec2:PutBucketTagging"  
13       ],  
14       "Resource": "\*"  
15     },  
16     {  
17       "Sid": "VisualEditor1",  
18       "Effect": "Allow",  
19       "Action": "iam:PassRole",  
20       "Resource": "arn:aws:iam::\*:role/\*"  
21     }  
22   ]  
23 }  
24

Character count: 304 of 6,144.

CancelReview policy

提示：

所示的 JSON 示例可能不包括针对您的环境的所有权限。有关详细信息，请参阅[关于 AWS 权限](#)。

所需的 **AWS** 权限

本部分包含 AWS 权限的完整列表。使用本节中给出的全套权限以使该功能正常运行。

注意：

只有 **role\_based\_auth** 才需要 *iam:PassRole* 权限。

创建主机连接

使用从 AWS 获取的信息添加新的主机连接。

```
1 {  
2  
3   "Version": "2012-10-17",  
4   "Statement": [  
5     {  
6  
7       "Action": [  
8          "ec2:DescribeAvailabilityZones",
```

```
9         "ec2:DescribeImages",
10        "ec2:DescribeInstances",
11        "ec2:DescribeInstanceTypes",
12        "ec2:DescribeSecurityGroups",
13        "ec2:DescribeSubnets",
14        "ec2:DescribeVpcs"
15    ],
16    "Effect": "Allow",
17    "Resource": "*"
18  }
19
20  ]
21  }
22
23  <!--NeedCopy-->
```

## VM 的电源管理

计算机实例已打开或关闭电源。

```
1  {
2
3    "Version": "2012-10-17",
4    "Statement": [
5      {
6
7        "Action": [
8          "ec2:AttachVolume",
9          "ec2:CreateVolume",
10         "ec2>DeleteVolume",
11         "ec2:DescribeInstances",
12         "ec2:DescribeVolumes",
13         "ec2:DetachVolume",
14         "ec2:StartInstances",
15         "ec2:StopInstances"
16       ],
17       "Effect": "Allow",
18       "Resource": "*"
19     }
20   ]
21 }
22
23
24 <!--NeedCopy-->
```

## 创建、更新或删除 VM

使用预配为 AWS 实例的 VM 创建、更新或删除计算机目录。

```

1  {
2
3      "Version": "2012-10-17",
4      "Statement": [
5          {
6
7              "Action": [
8                  "ec2:AttachVolume",
9                  "ec2:AssociateIamInstanceProfile",
10                 "ec2:AuthorizeSecurityGroupEgress",
11                 "ec2:AuthorizeSecurityGroupIngress",
12                 "ec2:CreateImage",
13                 "ec2:CreateLaunchTemplate",
14                 "ec2:CreateSecurityGroup",
15                 "ec2:CreateTags",
16                 "ec2:CreateVolume",
17                 "ec2>DeleteVolume",
18                 "ec2:DescribeAccountAttributes",
19                 "ec2:DescribeAvailabilityZones",
20                 "ec2:DescribeIamInstanceProfileAssociations",
21                 "ec2:DescribeImages",
22                 "ec2:DescribeInstances",
23                 "ec2:DescribeInstanceTypes",
24                 "ec2:DescribeLaunchTemplates",
25                 "ec2:DescribeLaunchTemplateVersions",
26                 "ec2:DescribeNetworkInterfaces",
27                 "ec2:DescribeRegions",
28                 "ec2:DescribeSecurityGroups",
29                 "ec2:DescribeSnapshots",
30                 "ec2:DescribeSubnets",
31                 "ec2:DescribeTags",
32                 "ec2:DescribeSpotInstanceRequests",
33                 "ec2:DescribeInstanceCreditSpecifications",
34                 "ec2:DescribeInstanceAttribute",
35
36                 "ec2:GetLaunchTemplateData",
37                 "ec2:DescribeVolumes",
38                 "ec2:DescribeVpcs",
39                 "ec2:DetachVolume",
40                 "ec2:DisassociateIamInstanceProfile",
41                 "ec2:RunInstances",
42                 "ec2:StartInstances",
43                 "ec2:StopInstances",
44                 "ec2:TerminateInstances"
45             ],
46             "Effect": "Allow",
47             "Resource": "*"
48         }
49     ],
50     {
51
52         "Action": [
53             "ec2:AuthorizeSecurityGroupEgress",

```

```

54         "ec2:AuthorizeSecurityGroupIngress",
55         "ec2:CreateSecurityGroup",
56         "ec2>DeleteSecurityGroup",
57         "ec2:RevokeSecurityGroupEgress",
58         "ec2:RevokeSecurityGroupIngress"
59     ],
60     "Effect": "Allow",
61     "Resource": "*"
62 },
63 ,
64 {
65     "Action": [
66         "s3:CreateBucket",
67         "s3>DeleteBucket",
68         "s3:PutBucketAcl",
69         "s3:PutBucketTagging",
70         "s3:PutObject",
71         "s3:GetObject",
72         "s3>DeleteObject",
73         "s3:PutObjectTagging"
74     ],
75     "Effect": "Allow",
76     "Resource": "arn:aws:s3:::citrix*"
77 },
78 ,
79 {
80     "Action": [
81         "ebs:StartSnapshot",
82         "ebs:GetSnapshotBlock",
83         "ebs:PutSnapshotBlock",
84         "ebs:CompleteSnapshot",
85         "ebs:ListSnapshotBlocks",
86         "ebs:ListChangedBlocks",
87         "ec2:CreateSnapshot"
88     ],
89     "Effect": "Allow",
90     "Resource": "*"
91 },
92 ],
93 }
94 ]
95 }
96 }
97
98 <!--NeedCopy-->

```

**注意：**

- 只有在目录创建期间必须为准备 VM 创建隔离安全组时，才需要与 SecurityGroups 相关的 EC2 部分。完成此操作后，不需要这些权限。

**直接上载和下载磁盘** 直接上载磁盘不再需要满足预配计算机目录的卷工作线程要求，改为使用 AWS 提供的公共 API。此功能降低了与额外的存储帐户相关的成本以及维护卷工作线程操作的复杂性。

注意：

对卷工作线程的支持已过时。

必须将以下权限添加到策略中：

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DescribeLaunchTemplates`

重要提示：

- 您可以将新虚拟机添加到现有计算机目录中，而无需任何卷工作线程资源，例如卷工作线程 AMI 和卷工作线程虚拟机。
- 如果您删除以前使用过任何卷工作线程的现有目录，则所有与卷工作线程相关的对象都将被删除。

### 已创建的卷的 **EBS** 加密

如果 AMI 已加密，或者 EBS 配置为加密所有新卷，EBS 可以自动加密新创建的卷。但是，要实现该功能，IAM 策略中必须包含以下权限。

```
1 {
2
3     "Version": "2012-10-17",
4     "Statement": [
5         {
6
7             "Effect": "Allow",
8             "Action": [
9                 "kms:CreateGrant",
10                "kms:Decrypt",
11                "kms:DescribeKey",
12                "kms:GenerateDataKeyWithoutPlainText",
13                "kms:GenerateDataKey",
14                "kms:ReEncryptTo",
15                "kms:ReEncryptFrom"
16            ],
17             "Resource": "*"
18         }
19     ]
20 }
```

```

20     ]
21   }
22
23   <!--NeedCopy-->

```

注意：

用户可自行决定是否包含资源和条件块，从而将权限限制到特定密钥。例如，具有以下条件的 **KMS** 权限：

```

1  {
2
3    "Version": "2012-10-17",
4    "Statement": [
5      {
6
7        "Effect": "Allow",
8        "Action": [
9          "kms:CreateGrant",
10         "kms:Decrypt",
11         "kms:DescribeKey",
12         "kms:GenerateDataKeyWithoutPlainText",
13         "kms:GenerateDataKey",
14         "kms:ReEncryptTo",
15         "kms:ReEncryptFrom"
16       ],
17       "Resource": [
18         "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123-456d-a12b-a123b4cd56ef"
19       ],
20       "Condition": {
21
22         "Bool": {
23
24           "kms:GrantIsForAWSResource": true
25         }
26       }
27     }
28   }
29
30 ]
31 }
32
33
34 <!--NeedCopy-->

```

以下密钥策略声明是允许帐户使用 IAM 策略委派对 KMS 密钥的所有操作 (kms: \*) 的权限所必需的 KMS 密钥的完整默认密钥策略。

```

1  {
2
3    "Sid": "Enable IAM policies",
4    "Effect": "Allow",
5    "Principal": {

```



```

6
7  "AWS": "arn:aws:iam::111122223333:root"
8  }
9  ,
10 "Action": "kms:",
11 "Resource": ""
12 }
13
14 <!--NeedCopy-->

```

有关详细信息，请参阅 [AWS 密钥管理服务官方文档](#)。

### 基于 IAM 角色的身份验证

添加了以下权限以支持基于角色的身份验证。

```

1  {
2
3      "Version": "2012-10-17",
4      "Statement": [
5          {
6
7              "Effect": "Allow",
8              "Action": "iam:PassRole",
9              "Resource": "arn:aws:iam::\*:role/*"
10         }
11     ]
12 }
13
14
15 <!--NeedCopy-->

```

### 最低 IAM 权限策略

以下 JSON 可用于当前支持的所有功能。可以使用此策略创建主机连接、创建、更新或删除 VM 以及进行电源管理。可以按照定义 IAM 权限部分中的说明将策略应用到用户，也可以通过 **role\_based\_auth** 安全密钥和密钥使用基于角色的身份验证。

#### 重要：

要使用 **role\_based\_auth**，请在设置 Cloud Connector 时首先在 Cloud Connector ec2 实例上配置所需的 IAM 角色。使用 Citrix Studio 添加托管连接并为身份验证密钥和机密提供 role\_based\_auth。具有这些设置的托管连接之后将使用基于角色的身份验证。

```

1  {
2
3      "Version": "2012-10-17",
4      "Statement": [

```

```
5      {
6
7          "Action": [
8              "ec2:AttachVolume",
9              "ec2:AssociateIamInstanceProfile",
10             "ec2:AuthorizeSecurityGroupEgress",
11             "ec2:AuthorizeSecurityGroupIngress",
12             "ec2:CreateImage",
13             "ec2:CreateLaunchTemplate",
14             "ec2:CreateNetworkInterface",
15             "ec2:CreateTags",
16             "ec2:CreateVolume",
17             "ec2>DeleteLaunchTemplate",
18             "ec2>DeleteNetworkInterface",
19             "ec2>DeleteSecurityGroup",
20             "ec2>DeleteSnapshot",
21             "ec2>DeleteTags",
22             "ec2>DeleteVolume",
23             "ec2:DeregisterImage",
24             "ec2:DescribeAccountAttributes",
25             "ec2:DescribeAvailabilityZones",
26             "ec2:DescribeIamInstanceProfileAssociations",
27             "ec2:DescribeImages",
28             "ec2:DescribeInstances",
29             "ec2:DescribeInstanceTypes",
30             "ec2:DescribeLaunchTemplates",
31             "ec2:DescribeLaunchTemplateVersions",
32             "ec2:DescribeNetworkInterfaces",
33             "ec2:DescribeRegions",
34             "ec2:DescribeSecurityGroups",
35             "ec2:DescribeSnapshots",
36             "ec2:DescribeSubnets",
37             "ec2:DescribeTags",
38             "ec2:DescribeSpotInstanceRequests",
39             "ec2:DescribeInstanceCreditSpecifications",
40             "ec2:DescribeInstanceAttribute",
41             "ec2:GetLaunchTemplateData",
42             "ec2:DescribeVolumes",
43             "ec2:DescribeVpcs",
44             "ec2:DetachVolume",
45             "ec2:DisassociateIamInstanceProfile",
46             "ec2:RebootInstances",
47             "ec2:RunInstances",
48             "ec2:StartInstances",
49             "ec2:StopInstances",
50             "ec2:TerminateInstances"
51         ],
52         "Effect": "Allow",
53         "Resource": "*"
54     },
55     {
56
57
```

```

58         "Action": [
59             "ec2:AuthorizeSecurityGroupEgress",
60             "ec2:AuthorizeSecurityGroupIngress",
61             "ec2:CreateSecurityGroup",
62             "ec2>DeleteSecurityGroup",
63             "ec2:RevokeSecurityGroupEgress",
64             "ec2:RevokeSecurityGroupIngress"
65         ],
66         "Effect": "Allow",
67         "Resource": "*"
68     },
69     ,
70     {
71         "Action": [
72             "s3:CreateBucket",
73             "s3>DeleteBucket",
74             "s3>DeleteObject",
75             "s3:GetObject",
76             "s3:PutBucketAcl",
77             "s3:PutObject",
78             "s3:PutBucketTagging",
79             "s3:PutObjectTagging"
80         ],
81         "Effect": "Allow",
82         "Resource": "arn:aws:s3:::citrix*"
83     },
84     ,
85     {
86         "Action": [
87             "ebs:StartSnapshot",
88             "ebs:GetSnapshotBlock",
89             "ebs:PutSnapshotBlock",
90             "ebs:CompleteSnapshot",
91             "ebs:ListSnapshotBlocks",
92             "ebs:ListChangedBlocks",
93             "ec2:CreateSnapshot"
94         ],
95         "Effect": "Allow",
96         "Resource": "*"
97     },
98     ,
99     {
100         "Effect": "Allow",
101         "Action": [
102             "kms:CreateGrant",
103             "kms:Decrypt",
104             "kms:DescribeKey",
105             "kms:GenerateDataKeyWithoutPlainText",
106             "kms:GenerateDataKey",
107             "kms:ReEncryptTo",

```

```
111         "kms:ReEncryptFrom"
112     ],
113     "Resource": "*"
114 }
115 ,
116 {
117     "Effect": "Allow",
118     "Action": "iam:PassRole",
119     "Resource": "arn:aws:iam::*:role/*"
120 }
121 ]
122 }
123 ]
124 }
125
126 <!--NeedCopy-->
```

注意：

- 只有在目录创建期间必须为准备 VM 创建隔离安全组时，才需要与 SecurityGroups 相关的 EC2 部分。完成此操作后，不需要这些权限。
- 只有在使用 EBS 卷加密时才需要 KMS 部分。
- 只有 **role\_based\_auth** 需要 **iam:PassRole** 权限部分。
- 根据您的要求和环境，可以添加特定的资源级权限，而非完全访问权限。有关更多详细信息，请参阅 AWS 文档 [Demystifying EC2 Resource-Level Permissions](#)（揭开 EC2 资源级权限的神秘面纱）和 [Access management for AWS resources](#)（AWS 资源访问管理）。
- 仅在使用卷工作线程方法时才使用 **ec2:CreateNetworkInterface** 和 **ec2:DeleteNetworkInterface** 权限。

### 下一步的去向

- 如果您处于初始部署过程中，请参阅[创建计算机目录](#)。
- 有关 AWS 的特定信息，请参阅[创建 AWS 目录](#)。

### 更多信息

- [创建和管理连接和资源](#)
- [AWS 虚拟化环境](#)

## 与 Google Cloud 环境的连接

January 23, 2024

[创建和管理连接和资源](#)介绍了用于创建连接的向导。以下信息涵盖了特定于 Google Cloud 环境的详细信息。

注意：

在创建与 Google Cloud 环境的连接之前，需要先完成将 Google Cloud 帐户设置为资源位置的过程。查看 [Google Cloud 虚拟化环境](#)。

## 添加连接

在完整配置界面中，按照[创建和管理连接和资源](#)中的指导进行操作。以下说明将指导您完成设置托管连接的过程：

1. 在管理 > 完整配置中，选择左侧窗格中的托管。
2. 在操作栏中选择添加连接和资源。
3. 在连接页面上，选择创建新连接和 **Citrix Provisioning** 工具，然后选择下一步。
  - 区域名称。选择您希望主机资源驻留的区域（等同于资源位置）。当您创建资源位置并向其中添加 Cloud Connector 时，会自动创建区域。有关详细信息，请参阅[区域](#)。
  - 连接类型。从菜单中选择 **Google** 云端平台。
  - 服务帐户密钥。导入您的 Google 凭据文件 (.json) 中包含的密钥。您可以粘贴凭据文件中的密钥，也可以浏览到凭据文件。要粘贴密钥，请执行以下操作：
    - a) 找到您的凭据文件
    - b) 使用记事本（或任何文本编辑器）打开文件
    - c) 复制内容。
    - d) 返回“连接”页面，选择“添加密钥”，粘贴内容，然后选择“完成”。
  - 服务帐户 ID。该字段会自动填充来自服务帐户密钥的信息。
  - 连接名称。键入连接的名称。
  - 通过 **Citrix Cloud Connector** 路由流量。要通过可用的 Citrix Cloud Connector 路由 API 请求，请选中此复选框。您也可以选中“启用 **Google Cloud Build** 以使用专用池”复选框以获得额外的安全保障。

或者，您可以使用 PowerShell 启用此功能。有关详细信息，请参阅[为 GCP 管理的流量创建安全的环境](#)。
4. 在区域页面上，从菜单中选择项目名称，选择包含要使用的资源的区域，然后选择下一步。

注意：

仅当您的部署中有活动的 Citrix Cloud Connector 时，此选项才可用。目前，Connector Appliance 不支持此功能。

- 使用创建虚拟机。选择创建虚拟机的方法。

5. 在网络网络上，键入资源的名称，从菜单中选择虚拟网络，选择子集，然后选择下一步。资源名称可帮助您识别此区域和网络的组合名称后面附加了 *(Shared)* 后缀的虚拟网络表示共享 VPC。如果您为共享 VPC 配置了子网级别的 IAM 角色，则子网列表中仅显示共享 VPC 的特定子网。

注意：

- 资源名称可以包含 1-64 个字符，不能仅包含空格或字符 \ / ; : # . \* ? = < > | [ ] { } " ' ( ) ' )。

6. 在摘要页面上，确认信息，然后选择完成退出添加连接和资源窗口。

创建连接和资源后，将列出您创建的连接和资源。要配置连接，请选择该连接，然后选择操作栏中的适用选项。

同样，可以删除、重命名或测试在连接下创建的资源。为此，请选择连接下的资源，然后选择操作栏中的适用选项。

## 为 GCP 托管流量创建安全的环境

您只能允许 Google 私密访问您的 Google Cloud 项目。这种实现增强了处理敏感数据的安全性。为此，您需要：

1. 在要执行 VPC 服务控制的 VPC 中安装 Cloud Connector。有关详细信息，请参阅 [VPC 服务控制](#)。
2. 如果是 Citrix Cloud 部署，则可以在 [CustomProperties](#) 中添加 [ProxyHypervisorTrafficThroughCon](#)。如果您使用的是专用工作人员池，请将 [UsePrivateWorkerPool](#) 加入到 [CustomProperties](#) 中。有关专用工作人员池的信息，请参阅 [专用池概述](#)。

注意：

目前，Connector Appliance 不支持此功能。

## 为 GCP 管理的流量创建安全环境的要求

为 GCP 托管流量创建安全环境的要求如下：

- 更新自定义属性时，请确保托管连接处于维护模式。
- 要使用专用工作程序池，需要进行以下更改：
  - 对于 Citrix Cloud 服务帐户，请添加以下 IAM 角色：
    - ★ 云构建服务帐户
    - ★ 计算实例管理员
    - ★ 服务帐户用户
    - ★ 服务帐户令牌创建者
    - ★ Cloud Build WorkerPool 所有者
  - 在用于创建托管连接的同一项目中创建 Citrix Cloud 服务帐户。

- 按照 [DNS 配置](#) 中所述为 `private.googleapis.com` 和 `gcr.io` 设置 DNS 区域。

Zone details

EDIT

ADD NETWORKS

DELETE ZONE

googleapis-com-private

DNS namegoogleapis.com.

TypePrivate

RECORD SETS

IN USE BY

ADD STANDARD

ADD WITH ROUTING POLICY

DELETE RECORD SETS

REFRESH

Filter

Filter record sets

<input type="checkbox"/>	DNS name ↑	Type	TTL (seconds)	Routing policy		
<input type="checkbox"/>	*.googleapis.com.	CNAME	300	Default	▼	✎
<input type="checkbox"/>	googleapis.com.	NS	21600	Default	▼	✎
<input type="checkbox"/>	googleapis.com.	SOA	21600	Default	▼	✎
<input type="checkbox"/>	private.googleapis.com.	A	300	Default	▼	✎

Zone details

EDIT

ADD NETWORKS

DELETE ZONE

gcr

DNS namegcr.io.

TypePrivate

RECORD SETS

IN USE BY

ADD STANDARD

ADD WITH ROUTING POLICY

DELETE RECORD SETS

REFRESH

Filter

Filter record sets

<input type="checkbox"/>	DNS name ↑	Type	TTL (seconds)	Routing policy		
<input type="checkbox"/>	*.gcr.io.	CNAME	300	Default	▼	✎
<input type="checkbox"/>	gcr.io.	SOA	21600	Default	▼	✎
<input type="checkbox"/>	gcr.io.	NS	21600	Default	▼	✎
<input type="checkbox"/>	gcr.io.	A	300	Default	▼	✎

- 设置专用网络地址转换 (NAT) 或使用专用服务连接。有关详细信息，请参阅[通过端点访问 Google API](#)。

Private Service Connect

CONNECTED ENDPOINTS

PUBLISHED SERVICES

Private Service Connect lets you connect privately and securely to Services. [Learn more](#)

Connections

Accepted

Rejected

Pending

Closed

1 in total

1

0

0

0

Endpoints

CONNECT ENDPOINT

Filter

Enter property name or value

<input type="checkbox"/>	Endpoint ↑	Status	PSC Connection ID	Target	Network	Region	IP address	Namespace
<input type="checkbox"/>	connectendpoint	Accepted	42924925526780928	All Google APIs	plm-vpc		10.8.172.0	goog-psc-plm-vpc-8514753636491831765

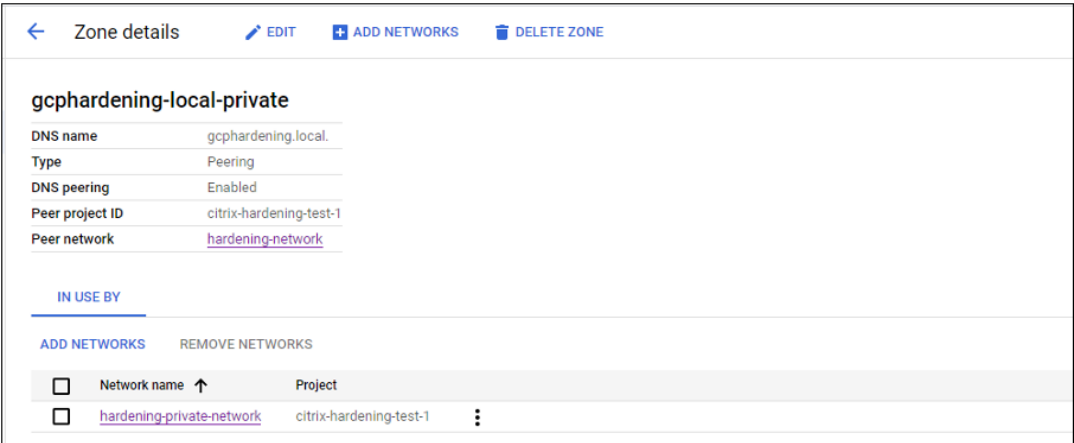
Load balancer endpoints

Filter

Enter property name or value

Load balancer ↑	Type	Number of NEGs	Network	Region	IP addresses
No rows to display					

- 如果使用对等 VPC，请创建一个与对等 VPC 对等的 Cloud DNS 区域。有关详细信息，请参阅[创建对等区域](#)。



- 在 VPC 服务控制中，设置出口规则以便 API 与 VM 可以与 Internet 通信。入口规则为选填。例如：

```
1 Egress Rule 1
2 From:
3 Identities:ANY_IDENTITY
4 To:
5 Projects =
6 All projects
7 Service =
8 Service name: All services
9 <!--NeedCopy-->
```

启用代理

要启用代理，请在主机连接上设置自定义属性，如下所示：

1. 从 Delivery Controller 主机打开 PowerShell 窗口或使用远程 PowerShell SDK。有关远程 PowerShell SDK 的详细信息，请参阅 [SDK](#) 和 [API](#)。
2. 运行以下命令：
  - a) `Add-PSSnapin citrix*`
  - b) `cd XDHyp:\Connections\`
  - c) `dir`
3. 将连接中的 `CustomProperties` 复制到记事本。
4. 按如下方式附加属性设置：
  - 如果是云部署（使用公共池）：将属性设置 `<Property xsi:type="StringProperty" Name="ProxyHypervisorTrafficThroughConnector" Value="True"/>` 附加到 `CustomProperties` 以启用代理。例如：

```
1 <CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema
  -instance" xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation">
```



```

2   <Property xsi:type="StringProperty" Name="
    ProxyHypervisorTrafficThroughConnector" Value="True"/>
3   </CustomProperties>
4   <!--NeedCopy-->

```

允许在 VPC 服务外围使用 Cloud Build 服务帐户的入口规则。例如：

```

1   Ingress Rule 1
2   From:
3   Identities:
4   <ProjectID>@cloudbuild.gserviceaccount.com
5   Source > All sources allowed
6   To:
7   Projects =
8   All projects
9   Services =
10  Service name: All services
11  <!--NeedCopy-->

```

有关 VPC 服务边界的信息，请参阅[服务外围详细信息和配置](#)。

- 如果是云部署中的专用工作线程池，请将属性设置 `<Property xsi:type="StringProperty" Name="ProxyHypervisorTrafficThroughConnector" Value="True"/>` 和 `<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool" Value="True"/>` 附加到 CustomProperties 以启用代理。例如：

```

1   <CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema
    -instance" xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation">
2   <Property xsi:type="StringProperty" Name="
    ProxyHypervisorTrafficThroughConnector" Value="True"/>
3   <Property xsi:type="StringProperty" Name="
    UsePrivateWorkerPool" Value="True"/>
4   </CustomProperties>
5   <!--NeedCopy-->

```

5. 在 PowerShell 窗口中，为修改后的自定义属性分配一个变量。例如：  
`$customProperty = '<CustomProperties...</CustomProperties>'。`
6. 运行 `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"`。
7. 运行 `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"`。
8. 运行 `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText -Force`。
9. 运行以下命令更新现有的主机连接：

```
1 Set-Item -PassThru -Path @('XDHyp:\Connections\\<ENTER YOUR  
   CONNECTION NAME HERE>') -SecurePassword $securePassword -  
   UserName $gcpServiceAccount -CustomProperties $customProperty  
2 <!--NeedCopy-->
```

## 所需的 GCP 权限

本部分包含 GCP 权限的完整列表。使用本部分中给出的完整权限集以使该功能正常运行。

### 创建主机连接

- 预配项目中的 Citrix Cloud Service 帐户所需的最低权限：

```
1 compute.instanceTemplates.list  
2 compute.instances.list  
3 compute.networks.list  
4 compute.projects.get  
5 compute.regions.list  
6 compute.subnetworks.list  
7 compute.zones.list  
8 resourcemanager.projects.get  
9 <!--NeedCopy-->
```

下列 Google 定义的角色具有上面列出的权限：

- 计算管理员
  - 云数据存储用户
- 共享 VPC 项目中 Citrix Cloud Service 帐户的共享 VPC 所需的额外权限：

```
1 compute.networks.list  
2 compute.subnetworks.list  
3 resourcemanager.projects.get  
4 <!--NeedCopy-->
```

下列 Google 定义的角色具有上面列出的权限：

- 计算网络用户

## VM 的电源管理

如果是仅限电源管理的目录，则在 Provisioning 项目中 Citrix Cloud 服务帐户所需的最低权限：

```
1 compute.instanceTemplates.list  
2 compute.instances.list  
3 compute.instances.get  
4 compute.instances.reset
```

```
5 compute.instances.resume
6 compute.instances.start
7 compute.instances.stop
8 compute.instances.suspend
9 compute.networks.list
10 compute.projects.get
11 compute.regions.list
12 compute.subnetworks.list
13 compute.zones.list
14 resourceManager.projects.get
15 compute.zoneOperations.get
16 <!--NeedCopy-->
```

下列 Google 定义的角色具有上面列出的权限：

- 计算管理员
- 云数据存储用户

#### 创建、更新或删除 **VM**

- 预配项目中的 Citrix Cloud Service 帐户所需的最低权限：

```
1 cloudbuild.builds.create
2 cloudbuild.builds.get
3 cloudbuild.builds.list
4 compute.acceleratorTypes.list
5 compute.diskTypes.get
6 compute.diskTypes.list
7 compute.disks.create
8 compute.disks.createSnapshot
9 compute.disks.delete
10 compute.disks.get
11 compute.disks.list
12 compute.disks.setLabels
13 compute.disks.use
14 compute.disks.useReadOnly
15 compute.firewalls.create
16 compute.firewalls.delete
17 compute.firewalls.list
18 compute.globalOperations.get
19 compute.images.create
20 compute.images.delete
21 compute.images.get
22 compute.images.list
23 compute.images.setLabels
24 compute.images.useReadOnly
25 compute.instanceTemplates.create
26 compute.instanceTemplates.delete
27 compute.instanceTemplates.get
28 compute.instanceTemplates.list
29 compute.instanceTemplates.useReadOnly
```

```
30 compute.instances.attachDisk
31 compute.instances.create
32 compute.instances.delete
33 compute.instances.detachDisk
34 compute.instances.get
35 compute.instances.list
36 compute.instances.reset
37 compute.instances.resume
38 compute.instances.setDeletionProtection
39 compute.instances.setLabels
40 compute.instances.setMetadata
41 compute.instances.setServiceAccount
42 compute.instances.setTags
43 compute.instances.start
44 compute.instances.stop
45 compute.instances.suspend
46 compute.machineTypes.get
47 compute.machineTypes.list
48 compute.networks.list
49 compute.networks.updatePolicy
50 compute.nodeGroups.list
51 compute.nodeTemplates.get
52 compute.projects.get
53 compute.regions.list
54 compute.snapshots.create
55 compute.snapshots.delete
56 compute.snapshots.list
57 compute.snapshots.get
58 compute.snapshots.setLabels
59 compute.snapshots.useReadOnly
60 compute.subnetworks.get
61 compute.subnetworks.list
62 compute.subnetworks.use
63 compute.zoneOperations.get
64 compute.zoneOperations.list
65 compute.zones.get
66 compute.zones.list
67 iam.serviceAccounts.actAs
68 resourcemanager.projects.get
69 storage.buckets.create
70 storage.buckets.delete
71 storage.buckets.get
72 storage.buckets.list
73 storage.buckets.update
74 storage.objects.create
75 storage.objects.delete
76 storage.objects.get
77 storage.objects.list
78 compute.networks.get
79 compute.resourcePolicies.use
80
81 <!--NeedCopy-->
```

下列 Google 定义的角色具有上面列出的权限：

- 计算管理员
  - 存储管理员
  - 云构建编辑者
  - 服务帐户用户
  - 云数据存储用户
- 共享 VPC 项目中的 Citrix Cloud Service 帐户的共享 VPC 需要额外的权限，才能使用共享 VPC 项目中的 VPC 和子网创建托管单元：

```
1  compute.firewalls.list
2  compute.networks.list
3  compute.projects.get
4  compute.regions.list
5  compute.subnetworks.get
6  compute.subnetworks.list
7  compute.subnetworks.use
8  compute.zones.list
9  resourcemanager.projects.get
10 <!--NeedCopy-->
```

下列 Google 定义的角色具有上面列出的权限：

- 计算网络用户
  - 云数据存储用户
- 将准备说明磁盘下载到 MCS 时，Google Cloud Build Service 要求的预配项目中的 Cloud Build Service 帐户所需的最低权限：

```
1  compute.disks.create
2  compute.disks.delete
3  compute.disks.get
4  compute.disks.list
5  compute.disks.setLabels
6  compute.disks.use
7  compute.disks.useReadOnly
8  compute.images.get
9  compute.images.list
10 compute.images.useReadOnly
11 compute.instances.create
12 compute.instances.delete
13 compute.instances.get
14 compute.instances.getSerialPortOutput
15 compute.instances.list
16 compute.instances.setLabels
17 compute.instances.setMetadata
18 compute.instances.setServiceAccount
19 compute.machineTypes.list
20 compute.networks.get
21 compute.networks.list
```

```
22 compute.projects.get
23 compute.subnetworks.list
24 compute.subnetworks.use
25 compute.subnetworks.useExternalIp
26 compute.zoneOperations.get
27 compute.zones.list
28 iam.serviceAccounts.actAs
29 logging.logEntries.create
30 pubsub.topics.publish
31 resourcemanager.projects.get
32 source.repos.get
33 source.repos.list
34 storage.buckets.create
35 storage.buckets.get
36 storage.buckets.list
37 storage.objects.create
38 storage.objects.delete
39 storage.objects.get
40 storage.objects.list
41 <!--NeedCopy-->
```

下列 Google 定义的角色具有上面列出的权限：

- 云构建服务帐户
  - 计算实例管理员
  - 服务帐户用户
- 将准备说明磁盘下载到 MCS 时，Google Cloud Build Service 要求的预配项目中 Cloud Compute Service 帐户所需的最低权限：

```
1 resourcemanager.projects.get
2 storage.objects.create
3 storage.objects.get
4 storage.objects.list
5 <!--NeedCopy-->
```

下列 Google 定义的角色具有上面列出的权限：

- 计算网络用户
  - 存储帐户用户
  - 云数据存储用户
- 将准备说明磁盘下载到 MCS 时，Google Cloud Build 服务要求在预配项目中为 Cloud Build Service 帐户提供共享 VPC 所需的额外权限：

```
1 compute.firewalls.list
2 compute.networks.list
3 compute.subnetworks.list
4 compute.subnetworks.use
5 resourcemanager.projects.get
6 <!--NeedCopy-->
```

下列 Google 定义的角色具有上面列出的权限：

- 计算网络用户
  - 存储帐户用户
  - 云数据存储用户
- 预配项目中 Citrix Cloud Service 帐户的云密钥管理服务 (KMS) 所需的其他权限：

```
1 cloudkms.cryptoKeys.get
2 cloudkms.cryptoKeys.list
3 cloudkms.keyRings.get
4 cloudkms.keyRings.list
5 <!--NeedCopy-->
```

下列 Google 定义的角色具有上面列出的权限：

- 计算 KMS 查看器

#### 一般权限

下面是预配项目中 Citrix Cloud Service 帐户对 MCS 中支持的所有功能的权限。这些权限提供了未来的最佳兼容性：

```
1 resourceManager.projects.get
2 cloudbuild.builds.create
3 cloudbuild.builds.get
4 cloudbuild.builds.list
5 compute.acceleratorTypes.list
6 compute.diskTypes.get
7 compute.diskTypes.list
8 compute.disks.create
9 compute.disks.createSnapshot
10 compute.disks.delete
11 compute.disks.get
12 compute.disks.setLabels
13 compute.disks.use
14 compute.disks.useReadOnly
15 compute.firewalls.create
16 compute.firewalls.delete
17 compute.firewalls.list
18 compute.globalOperations.get
19 compute.images.create
20 compute.images.delete
21 compute.images.get
22 compute.images.list
23 compute.images.setLabels
24 compute.images.useReadOnly
25 compute.instanceTemplates.create
26 compute.instanceTemplates.delete
27 compute.instanceTemplates.get
28 compute.instanceTemplates.list
```

```
29 compute.instanceTemplates.useReadOnly
30 compute.instances.attachDisk
31 compute.instances.create
32 compute.instances.delete
33 compute.instances.detachDisk
34 compute.instances.get
35 compute.instances.list
36 compute.instances.reset
37 compute.instances.resume
38 compute.instances.setDeletionProtection
39 compute.instances.setLabels
40 compute.instances.setMetadata
41 compute.instances.setTags
42 compute.instances.start
43 compute.instances.stop
44 compute.instances.suspend
45 compute.instances.update
46 compute.instances.updateAccessConfig
47 compute.instances.updateDisplayDevice
48 compute.instances.updateSecurity
49 compute.instances.updateShieldedInstanceConfig
50 compute.instances.updateShieldedVmConfig
51 compute.machineTypes.get
52 compute.machineTypes.list
53 compute.networks.list
54 compute.networks.updatePolicy
55 compute.nodeGroups.list
56 compute.nodeTemplates.get
57 compute.projects.get
58 compute.regions.list
59 compute.snapshots.create
60 compute.snapshots.delete
61 compute.snapshots.list
62 compute.snapshots.get
63 compute.snapshots.setLabels
64 compute.snapshots.useReadOnly
65 compute.subnetworks.get
66 compute.subnetworks.list
67 compute.subnetworks.use
68 compute.subnetworks.useExternalIp
69 compute.zoneOperations.get
70 compute.zoneOperations.list
71 compute.zones.get
72 compute.zones.list
73 resourceManager.projects.get
74 storage.buckets.create
75 storage.buckets.delete
76 storage.buckets.get
77 storage.buckets.list
78 storage.buckets.update
79 storage.objects.create
80 storage.objects.delete
81 storage.objects.get
```



```
82 storage.objects.list
83 cloudkms.cryptoKeys.get
84 cloudkms.cryptoKeys.list
85 cloudkms.keyRings.get
86 cloudkms.keyRings.list
87 compute.disks.list
88 compute.instances.setServiceAccount
89 compute.networks.get
90 compute.networks.use
91 compute.networks.useExternalIp
92 iam.serviceAccounts.actAs
93 compute.resourcePolicies.use
94 <!--NeedCopy-->
```

### 下一步的去向

- 如果您处于初始部署过程中，请参阅[创建计算机目录](#)。
- 有关 Google 云端平台 (GCP) 的特定信息，请参阅[创建 Google 云端平台目录](#)。

### 更多信息

- [创建和管理连接和资源](#)
- [Google Cloud 虚拟化环境](#)。

## 连接到 **HPE Moonshot**（预览版）

January 23, 2024

[创建和管理连接和资源](#)介绍了用于创建连接的向导。以下信息涵盖了 HPE Moonshot 的特定详细信息。

#### 注意：

在创建与 HPE Moonshot 的连接之前，您需要先完成 HPE 帐户的设置。请参阅 [HPE Moonshot 虚拟化环境](#)。

### 创建连接

您可以使用以下方法创建与 HPE Moonshot 的连接：

- 完整配置界面
- PowerShell 命令

### 使用完整配置界面创建连接

1. 在添加连接和资源页面中，选择 **HPE Moonshot** 作为 连接类型。
2. 输入您的 Moonshot iLO Chassis Manager 的连接地址。可以使用 IP 地址、主机名或 FQDN 作为地址。
3. 输入您的机箱管理凭据和友好的连接名称。

当出现以下任一情况时，连接设置将停止：

- DaaS 收到一个由 CA 签名的公共证书，但出现错误：出现一条错误消息。按照屏幕上的说明修复问题。否则，您将无法继续创建连接。
- DaaS 会收到 CA 签名的私有证书。出现警告页面。将收到的指纹与服务器的指纹进行比较，以了解证书的有效性。如果有效，请选择“信任证书”，然后单击“确定”继续创建连接。然后，DaaS 将信任证书并存储指纹以供将来验证。

### 使用 PowerShell 命令创建连接

使用 PowerShell 命令创建连接时，请提供以下信息：

- IP：HPE 服务器 IP 地址
- 用户名：HPE 用户名
- 密码：HPE 密码

例如：

```
1 New-Item -ConnectionType "Custom" -HypervisorAddress $IP -Metadata @{
2   "Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false" }
3   -Path @("XDHyp:\Connections$connectionName") -Persist -PluginId "
    HPMoonshotFactory" -Scope @() -SecurePassword $Password -UserName
    $UserName -sslthumbprint $SslThumbprint New-
    BrokerHypervisorConnection -HypHypervisorConnectionUid
    $HypervisorConnectionID
4 <!--NeedCopy-->
```

注意：

`sslthumbprint` 参数仅对私有 CA 签名的证书是必需的。

### 证书和指纹验证

要成功建立与 **HPE Moonshot** 的连接，证书不得有错误且指纹必须具有正确的值。以下是与证书和指纹验证相关的用例：

- CA 签名的公共证书有错误。未成功创建连接。查看错误详情并解决问题。
- 由 CA 签名的公共证书，没有错误。连接已成功创建，`SslThumbprints` 值为 **Null**。

- 由 CA 签名的私有证书，没有错误和 `sslthumbprint` 值。连接已成功创建，`SslThumbprints` 值正确。
- CA 签名的私有证书，指纹值不正确。未成功创建连接。
- 由 CA 签名的私有证书，没有错误。连接已成功创建。创建连接时 `SslThumbprints` 为 **Null**。`SslThumbprints` 值由站点服务更新为某个值。

管理连接

本节详细介绍了如何管理连接：

- 使用完整配置界面修复证书问题
- 使用 PowerShell 命令更新指纹值

修复证书问题

出现证书问题时，DaaS 会阻止 HPE Moonshot 连接，从而使您无法在关联的 HPE Moonshot 节点上交付和管理工作负载。您将在 主机 连接列表中的连接旁边看到一个错误图标。有关具体问题和解决方案，请参阅下表。

问题	解决方案
CA 签名的公共证书出现证书错误	单击连接并选择“故障排除”选项卡。查看错误详细信息并解决问题。
收到的证书是 CA 签名的私有证书或已过期。	编辑主机连接以更新证书指纹。详细步骤： <ol style="list-style-type: none"><li>1. 选择连接，然后单击“编辑连接”。</li><li>1. 在“连接属性”页面上，单击“编辑设置”。</li><li>1. 输入连接到 HPE Moonshot 机箱的密码，然后单击“保存”。</li><li>1. 在出现的“警告”页面上，将收到的指纹与服务器的指纹进行比较，以了解证书的有效性。</li><li>1. 如果它们相同，请选择“信任证书”，然后单击“确定”。</li></ol>

更新指纹值

创建连接后，您可以使用 `Set-Item` PowerShell 命令更新连接的指纹值。例如，运行以下命令：

1. 获取连接的连接详细信息。例如：

```
1 Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
2 <!--NeedCopy-->
```

2. 更新指纹值。例如：

```
1 Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
  Administrator -SslThumbprint
  xxxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
2 <!--NeedCopy-->
```

3. 检查更新的指纹值。例如：

```
1 Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
2 <!--NeedCopy-->
```

注意：

如果您在 `Set-Item` 命令中提供的指纹值不正确，更新将失败。

## 下一步的去向

- 如果您处于初始部署过程中，请参阅[创建计算机目录](#)。
- 有关 HPE Moonshot 的特定信息，请参阅[创建 HPE Moonshot 计算机目录](#)。

## 更多信息

- [创建和管理连接和资源](#)
- [HPE Moonshot 虚拟化环境](#)

## 与 Microsoft Azure 的连接

March 30, 2024

[创建和管理连接和资源](#)介绍了用于创建连接的向导。以下信息涵盖了特定于 Azure Resource Manager 云环境的详细信息。

注意：

在创建与 Microsoft Azure 的连接之前，必须先将 Azure 帐户设置为资源位置。请参阅 [Microsoft Azure Resource Manager 虚拟化环境](#)。

## 创建服务主体和连接

在创建连接之前，必须设置连接用来访问 Azure 资源的服务主体。您可以通过两种方式创建连接：

- 使用完整配置同时创建服务主体和连接
- 使用先前创建的服务主体创建连接

本节向您展示如何完成以下任务：

- 使用完整配置创建服务主体和连接
- 使用 PowerShell 创建服务主体
- 在 Azure 中获取应用程序机密
- 使用现有服务主体创建连接

## 注意事项

在开始之前，请注意以下注意事项：

- Citrix 建议使用具有贡献者角色的服务主体。但是，请参阅最低权限部分以获取最低权限列表。
- 在创建第一个连接时，Azure 会提示您为其授予必要的权限。对于将来的连接，您仍然必须进行身份验证，但是 Azure 会记住您以前同意的情况，并且不会再显示提示。
- 用于身份验证的帐户必须是订阅的协管理员。
- 用于身份验证的帐户必须是订阅的目录的成员。需要注意两种类型的帐户：“工作或学校”和“个人 Microsoft 帐户”。有关详细信息，请参阅 [CTX219211](#)。
- 虽然可以通过将现有 Microsoft 帐户添加为订阅目录的成员来使用该帐户，但如果以前已为用户授予对其中一个目录的资源的来宾访问权限，则可能会出现复杂情况。在这种情况下，他们可能在目录中有一个不会授予其必要权限的占位符条目，并会返回错误。

通过从目录中删除资源并将其明确添加回来纠正这个问题。但是，请谨慎使用此选项，因为它会对该帐户可以访问的其他资源产生意想不到的影响。

- 有一个已知问题，即某些帐户实际上是成员时，会被检测为目录来宾。此类配置通常发生在较旧的目录帐户中。解决方法：向目录中添加一个帐户，该帐户采用适当的成员身份值。
- 资源组只是资源的容器，它们可以包含来自自己所在区域以外的区域的资源。如果您希望资源组的区域中显示的资源可用，这可能会引起混淆。
- 请确保您的网络和子网足够大，可以容纳您需要的计算机数量。这需要一些先见之明，但 Microsoft 会帮助您指定合适的值，并提供有关地址空间容量的指导。

## 使用完整配置创建服务主体和连接

**重要：**

此功能尚不适用于 Azure 中国订阅。

使用完整配置，您可以在单个工作流程中创建服务主体和连接。服务主体为连接提供对 Azure 资源的访问权限。向 Azure 进行身份验证以创建服务主体时，应用程序将在 Azure 中注册。为注册的应用程序创建了密钥（称为客户端机密或应用程序机密）。注册的应用程序（在本例中为连接）使用客户端机密对 Azure AD 进行身份验证。

在开始之前，请确保您已满足以下必备条件：

- 在订阅的 Azure Active Directory 租户中具有一个用户帐户。
- Azure AD 用户帐户也是您希望用来预配资源的 Azure 订阅的协管理员。
- 您拥有全局管理员、应用程序管理员或应用程序开发者权限以进行身份验证。创建主机连接后，可以撤销权限。有关角色的详细信息，请参阅 [Azure AD 内置角色](#)。

使用添加连接和资源向导一起创建服务主体和连接：

1. 在连接页面上，选择创建新连接、**Microsoft Azure** 连接类型和您的 Azure 环境。
2. 选择可以使用哪些工具来创建虚拟机，然后选择下一步。
3. 在“连接详细信息”页面上，创建服务主体并按如下方式设置连接名称：
  - a) 要授予自动清理过时的加入了 Azure AD 的设备的连接权限，请选择“启用加入了 **Azure AD** 的设备管理”。如果您想通过此连接创建加入了 Azure AD 的计算机，我们建议您选择此选项。有关详细信息，请参阅启用加入了 Azure AD 的设备管理。
  - b) 输入 Azure 订阅 ID 和连接的名称。输入订阅 ID 后，将启用新建按钮。

**注意：**

连接名称可以包含 1-64 个字符，不能仅包含空格或字符 \ / ; : # . \* ? = < > | [ ] { } " ' ( ) '。

- a) 选择新建，然后输入 Azure Active Directory 帐户用户名和密码。
- b) 选择登录。
- c) 选择“接受”以授予 Citrix DaaS 列出的权限。Azure 创建了一个服务主体，允许 Citrix DaaS 代表指定用户管理 Azure 资源。
- d) 选择“接受”后，您将返回到“连接详细信息”页面。

**注意：**

成功对 Azure 进行身份验证后，新建和使用现有按钮将消失。连接成功文本显示时带有绿色复选标记，表示成功连接到 Azure 订阅。

- e) 要通过 Citrix Cloud Connector 将 API 请求路由到 Azure，请选中“通过 **Citrix Cloud Connector** 路由流量”复选框。

或者，您可以使用 PowerShell 启用此功能。有关详细信息，请参阅 [为 Azure 管理的流量创建安全的环境](#)。

注意：

仅当您的部署中有活动的 Citrix Cloud Connector 时，此选项才可用。目前，Connector Appliance 不支持此功能。

f) 选择下一步。

注意：

在成功对 Azure 进行身份验证并同意授予所需的权限之后，才能进入下一页。

4. 按如下方式配置连接的资源：

- 在区域页面上，选择一个区域。
- 在网络页面上，执行以下操作：
  - 键入 1-64 字符的资源名称以帮助确定区域和网络组合。资源名称不能仅包含空格或字符 \ / ; : # . \* ? = < > | [ ] { } " ' ( ) ' 。
  - 选择一个虚拟网络/资源组对。（如果您有多个具有相同名称的虚拟网络，将网络名称与资源组配对可提供唯一的组合。）如果您在上一个页面上选择的区域不具有任何虚拟网络，请返回到该页面并选择一个具有虚拟网络的区域。

5. 在摘要页面上，查看设置的摘要，然后选择完成以完成您的设置。

查看应用程序 ID 创建某个连接后，可以查看该连接用于访问 Azure 资源的应用程序 ID。

在添加连接和资源列表中，选择连接以查看详细信息。“详细信息”选项卡显示应用程序 ID。

1027azure

Details

Troubleshoot

Connection

Name:

1027azure

Subscription ID:

75b42f4d-8471-4230-a800-ba2791650a99

Application ID:

69875a0f-1400-4230-b843-01d74ae12ba6

Scopes:

All

Tenants:

-

Maintenance Mode:

Off

Secret expiration date:

-

使用 PowerShell 创建服务主体

要使用 PowerShell 创建服务主体，请连接到 Azure Resource Manager 订阅并使用以下部分中提供的 PowerShell cmdlet。

请务必准备好以下项目：

- **SubscriptionId**: 您希望预配 VDA 的订阅的 Azure Resource Manager **SubscriptionID**。
- **ActiveDirectoryID**: 您在 Azure AD 中注册的应用程序的租户 ID。
- **ApplicationName**: 要在 Azure AD 中创建的应用程序的名称。

详细步骤如下所示:

1. 连接到您的 Azure Resource Manager 订阅。

```
Connect-AzAccount
```

2. 选择您要创建服务主体的 Azure Resource Manager 订阅。

```
Get-AzSubscription -SubscriptionId $subscriptionId | Select-AzSubscription
```

3. 在您的 AD 租户中创建应用程序。

```
$AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
```

4. 创建服务主体。

```
New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
```

5. 向服务主体分配角色。

```
New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName $AzureADApplication.AppId -scope /subscriptions/$SubscriptionId
```

6. 在 PowerShell 控制台的输出窗口中, 记下 ApplicationId。请在创建主机连接时提供该 ID。

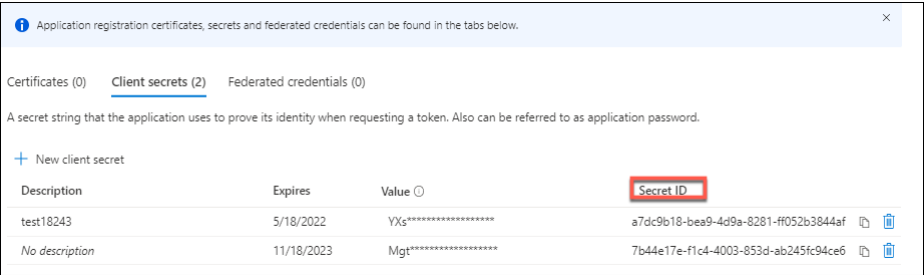
在 **Azure** 中获取应用程序机密

要使用现有服务主体创建连接, 必须先在 Azure 门户中获取服务主体的应用程序 ID 和密钥。

详细步骤如下所示:

1. 从“完整配置”界面或使用 PowerShell 获取应用程序 **ID**。
2. 登录 Azure 门户。
3. 在 Azure 中, 选择 **Azure Active Directory**。
4. 从 Azure AD 中的应用程序注册中, 选择您的应用程序。
5. 转到证书和密钥。
6. 单击“客户端密钥”。





使用现有服务主体创建连接

如果您已经有服务主体，则可以使用它使用完整配置来创建连接。

确保准备好以下项目：

- SubscriptionId
  - ActiveDirectoryID（租户 ID）
  - 应用程序 ID
  - 应用程序机密
  - 机密过期日期
- 有关详细信息，请参阅获取应用程序机密。

详细步骤如下所示：

在添加连接和资源向导中，执行以下操作：

1. 在连接页面上，选择创建新连接、**Microsoft Azure** 连接类型和您的 Azure 环境。
2. 选择可以使用哪些工具来创建虚拟机，然后选择下一步。
3. 在连接详细信息页面上，输入 Azure 订阅 ID 和连接的名称。

注意：

连接名称可以包含 1-64 个字符，不能仅包含空格或字符 \ / ; : # . \* ? = < > | [ ] { } " ' ( ) '。

4. 选择使用现有。在现有服务主体详细信息窗口中，输入现有服务主体的以下设置。输入详细信息后，将会启用保存按钮。选择保存。除非提供有效的详细信息，否则无法跳过此页面。
  - 订阅 ID。输入您的 Azure 订阅 ID。要获取您的订阅 ID，请登录 Azure 门户并导航到订阅 > 概述。
  - **Active Directory ID**（租户 ID）。输入您在 Azure AD 中注册的应用程序的目录（租户）ID。
  - 应用程序 ID。输入您在 Azure AD 中注册的应用程序的应用程序（客户端）ID。
  - 应用程序机密。输入密钥（客户端机密）。注册的应用程序使用密钥向 Azure AD 进行身份验证。出于安全考虑，我们建议您定期更改密钥。请务必保存密钥，因为以后将无法检索密钥。

- 机密过期日期。输入应用程序机密的过期日期。在密钥到期之前，您会在控制台上收到警报。但是，如果密钥过期，您会收到错误。

注意：

出于安全考虑，有效期从现在起不得超过两年。

- 身份验证 **URL**。此字段是自动填充的，不可编辑。
- 管理 **URL**。此字段是自动填充的，不可编辑。
- 存储后缀。此字段是自动填充的，不可编辑。

在 Azure 中创建 MCS 目录需要访问以下端点。访问这些端点可优化您的网络与 Azure 门户及其服务之间的连接。

- 身份验证 URL: <https://login.microsoftonline.com/>
- 管理 URL: <https://management.azure.com/>。这是 Azure Resource Manager 提供程序 API 的请求 URL。管理端点取决于环境。例如，对于 Azure Global 为 <https://management.azure.com/>，对于 Azure 美国政府为 <https://management.usgovcloudapi.net/>。
- 存储后缀: [https://\\*.core.windows.net/](https://*.core.windows.net/)。此 (\*) 是存储后缀的通配符。例如，<https://demo.table.core.windows.net/>。

5. 选择“保存”后，您将返回到“连接详细信息”页面。选择下一步进入下一页。

6. 按如下方式配置连接的资源：

- 在区域页面上，选择一个区域。
- 在网络页面上，执行以下操作：
  - 键入 1-64 字符的资源名称以帮助确定区域和网络组合。资源名称不能仅包含空格或字符 `\ / ; : # . * ? = < > | [ ] { } " ' ( ) ' .`。
  - 选择一个虚拟网络/资源组对。（如果您有多个具有相同名称的虚拟网络，将网络名称与资源组配对可提供唯一的组合。）如果您在上一个页面上选择的区域不具有任何虚拟网络，请返回到该页面并选择一个具有虚拟网络的区域。

7. 在摘要页面上，查看设置的摘要，然后选择完成以完成您的设置。

## 管理服务主体和连接

本部分内容详细介绍了如何管理服务主体和连接：

- 配置 Azure 限制设置
- 启用加入了 Azure AD 的设备管理
- 在 Azure 中启用映像共享
- 使用完整配置将共享租户添加到连接中
- 使用 PowerShell 实现映像共享

- 为 Azure 管理的流量创建安全的环境
- 管理应用程序机密和机密过期日期

配置 **Azure** 限制设置

Azure Resource Manager 限制订阅和租户的请求，从而根据定义的限制路由流量，根据提供商的特定需求量身定制。请参阅 Microsoft 站点上的[限制 Resource Manager 请求](#)，了解详细信息。订阅和租户存在限制，在这些情况下，管理许多计算机可能会成问题。例如，包含许多计算机的订阅可能会遇到与电源操作有关的性能问题。

提示：  
有关详细信息，请参阅[使用 Machine Creation Services 提高 Azure 性能](#)。

为了帮助缓解这些问题，Citrix DaaS 允许您删除 MCS 内部限制，以使用 Azure 中的更多可用请求配额。

我们建议在大型订阅（例如，包含 1,000 个 VM 的订阅）中打开或关闭 VM 的电源时采用以下最佳设置：

- 绝对同时操作：500
- 每分钟最大新操作数：2000
- 操作的最大并发数：500

使用“完整配置”界面为给定主机连接配置 Azure 操作：

1. 在管理 > 完整配置中，选择左侧窗格中的托管。
2. 选择与 Azure 有关的连接以对其进行编辑。
3. 在编辑连接向导中，选择高级。
4. 在高级页面上，使用配置选项指定同时操作的数量、每分钟执行的最大新操作数以及任何其他连接选项。

默认情况下，MCS 最多支持 500 个并发操作。或者，您可以使用 Remote PowerShell SDK 设置最大并发操作数。

使用 **PowerShell** 属性 `MaximumConcurrentProvisioningOperations` 可指定并发 Azure 预配操作的最大数量。使用此属性时，请注意：

- `MaximumConcurrentProvisioningOperations` 的默认值为 500。
- 使用 PowerShell 命令 `Set-item` 配置 `MaximumConcurrentProvisioningOperations` 参数。

## 启用加入了 **Azure AD** 的设备管理

在 Azure 中加入过时的 Azure AD 设备可能会阻止新计算机加入 Azure AD，从而导致它们无法正常工作。为避免潜在问题，您可以授予连接权限来管理加入了 Azure AD 的设备。有了这个权限，连接就可以自动清理过时的加入了 Azure AD 的设备。

### 注意：

删除计算机或计算机目录时，无法从 Azure AD 中删除已加入 Azure AD 的设备。

1. 从“管理” > “完整配置”中，在左侧窗格中选择主机。
2. 选择连接，然后在操作栏中选择编辑连接。
3. 从左侧窗格中选择“连接属性”。
4. 在出现的“连接属性”页面上，执行以下步骤：
  - a) 选择“启用加入了 **Azure AD** 的设备管理”。
  - b) 单击保存。
  - c) 在出现的 Azure 登录窗口中，输入您的订阅密码，然后单击“登录”。

登录完成后，您将返回到托管连接和资源列表。单击列表中的连接，然后单击底部窗格中的“详细信息”选项卡。您可以看到加入了 **Azure AD** 的设备管理字段显示已启用。

使用完整配置启用 Azure AD 加入设备管理时，无论选择哪种主机连接创建方法（新建或使用现有连接），都必须使用 Azure AD 进行身份验证。Azure AD 内置云设备管理员角色已分配给服务主体。要采用 Azure AD 加入设备管理的最低权限，可以手动从服务主体中删除云设备管理员角色的分配，然后创建一个仅包含最低权限的 Azure AD 自定义角色并将其分配给服务主体。

### 注意：

- Azure AD 加入设备管理的最低权限是 Azure AD 权限，而不是 Azure Resource Manager 权限。它们不能显式分配给服务主体。您必须在 Azure AD 中创建一个包含这些权限的自定义角色并将其分配给服务主体。有关详细信息，请参阅[在 Azure Active Directory 中创建和分配自定义角色](#)。
- 要在 Azure AD 中创建定制角色，您需要 Azure AD Premium P1 或 P2 许可证。

## 在 **Azure** 中启用映像共享

创建或更新计算机目录时，可以选择来自不同的 Azure 租户和订阅的共享映像（通过 Azure Compute Gallery 共享）。要允许在租户内部或租户之间共享映像，必须在 Azure 中进行必要的设置：

- 在租户内（跨订阅）共享映像
- 在租户之间共享映像

在租户内（跨订阅）共享映像 要在 Azure Compute Gallery 中选择属于其他订阅的映像，必须与该订阅的服务主体 (SPN) 共享该映像。

例如，如果存在服务主体 (SPN 1)，则在 Studio 中将其配置为：

服务主体：SPN 1

订阅：订阅 1

租户：租户 1

映像处于不同的订阅中，在 Studio 中将其配置为：

订阅：订阅 2

租户：租户 1

如果您想与订阅 1 (SPN 1) 共享订阅 2 中的镜像，请转到订阅 2，然后与 SPN1 共享资源组。

必须使用 Azure 基于角色的访问控制 (RBAC) 与其他 SPN 共享映像。Azure RBAC 是用于管理 Azure 资源访问权限的授权系统。有关 Azure RBAC 的详细信息，请参阅 Microsoft 文档 [What is Azure role-based access control \(Azure RBAC\)](#) (什么是 Azure 基于角色的访问控制 (Azure RBAC))。要授予访问权限，您可以使用贡献者角色向资源组范围内的服务主体分配角色。要分配 Azure 角色，您必须拥有 `Microsoft.Authorization/roleAssignments/write` 权限，例如用户访问管理员或所有者。有关与其他 SPN 共享映像的详细信息，请参阅 Microsoft 文档 [Assign Azure roles using the Azure portal](#) (使用 Azure 门户分配 Azure 角色)。

在租户之间共享映像 要使用 Azure Compute Gallery 在租户之间共享映像，请创建应用程序注册。

例如，如果有两个租户（租户 1 和租户 2），并且您想与租户 1 共享您的映像库，那么：

1. 为租户 1 创建应用程序注册。有关详细信息，请参阅[创建应用程序注册](#)。
2. 通过使用浏览器请求登录，授予租户 2 对应用程序的访问权限。将 `Tenant2 ID` 替换为租户 1 的租户 ID。将 `Application (client) ID` 替换为您创建的应用程序注册的应用程序 ID。完成替换后，将 URL 粘贴到浏览器中，然后按照登录提示登录到租户 2。例如：

```
1 https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?  
   client_id=<Application (client) ID>&response_type=code&  
   redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F  
2 <!--NeedCopy-->
```

有关详细信息，请参阅[向租户 2 授予访问权限](#)。

3. 授予应用程序对租户 2 资源组的访问权限。以租户 2 身份登录，为应用程序提供对包含库映像的资源组的注册访问权限。有关详细信息，请参阅[对跨租户的请求进行身份验证](#)。

使用“完整配置”向连接添加共享租户

在完整配置界面中创建或更新计算机目录时，可以选择来自不同 Azure 租户和订阅的共享映像（通过 Azure Compute Gallery 共享）。该功能要求您为关联的主机连接提供共享租户和订阅信息。

注意：

确保已在 Azure 中配置了必要的设置，以允许在租户之间共享映像。有关详细信息，请参阅在租户之间共享映像。

请完成以下步骤以建立连接：

1. 在管理 > 完整配置中，选择左侧窗格中的托管。
2. 选择连接，然后在操作栏中选择编辑连接。

3. 在共享租户中，执行以下操作：
  - a) 提供与连接的订阅关联的应用程序 ID 和应用程序机密。DaaS 使用此信息向 Azure AD 进行身份验证。
  - b) 通过订阅连接添加共享 Azure Compute Gallery 的租户和订阅。最多可以为每个租户添加八个共享租户和八个订阅。
4. 完成后，选择应用以应用您所做的更改并使窗口保持打开，或者选择确定应用更改并关闭窗口。

### 使用 PowerShell 实现映像共享

本部分内容将指导您完成使用 PowerShell 共享映像的过程：

- 从其他订阅中选择一个映像
- 使用共享租户 ID 更新托管连接自定义属性
- 从其他租户中选择一个映像

从其他订阅中选择一个映像 可以在 Azure Compute Gallery 中选择属于同一 Azure 租户中不同共享订阅的映像，以使用 PowerShell 命令创建和更新 MCS 目录。

1. 在托管单元根文件夹中，Citrix 创建了一个名为 `sharedsubscription` 的新共享订阅文件夹。
2. 列出租户中的所有共享订阅。

```
1 Get-ChildItem -Path "XDhyp:\HostingUnits\azres\sharedsubscription.  
  folder"  
2 <!--NeedCopy-->
```

3. 选择一个共享订阅，然后列出该共享订阅的所有共享资源组。

```
1 Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123  
  .sharedsubscription"  
2 <!--NeedCopy-->
```

4. 选择一个资源组，然后列出该资源组的所有库。

```
1 Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123  
  .sharedsubscription\ xyz.resourcegroup"  
2 <!--NeedCopy-->
```

5. 选择一个库，然后列出该库的所有映像定义。

```
1 Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123  
  .sharedsubscription\xyz.resourcegroup\testgallery.gallery"  
2 <!--NeedCopy-->
```

6. 选择一个映像定义，然后列出该映像定义的所有映像版本。

```
1 Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123  
  .sharedsubscription\xyz.resourcegroup\sigtestdef.  
  imagedefinition"  
2 <!--NeedCopy-->
```

7. 使用以下元素创建和更新 MCS 目录：

- 资源组
- 库
- 库映像定义
- 库映像版本

有关如何使用 Remote PowerShell SDK 创建目录的信息，请参阅 <https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>。

使用共享租户 ID 更新托管连接自定义属性 执行 `Set-Item` 以使用共享租户 ID 和订阅 ID 来更新托管连接自定义属性。在 `CustomProperties` 中添加属性 `SharedTenants`。`Shared Tenants` 的格式为：

```
1 [{  
2   "Tenant": "94367291-119e-457c-bc10-25337231f7bd", "Subscriptions": ["7  
    bb42f40-8d7f-4230-a920-be2781f6d5d9"] }  
3   , {
```

```

4   "Tenant": "50e83564-c4e5-4209-b43d-815c45659564", "Subscriptions": [ "06
    ab8944-6a88-47ee-a975-43dd491a37d0" ] }
5   ]
6   <!--NeedCopy-->

```

例如：

```

1   Set-Item -CustomProperties "<CustomProperties xmlns=`"http://schemas.
    citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
    /2001/XMLSchema-instance`">
2   <Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`" Value=`"
    123`" />
3   <Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`" Value
    =`"https://management.azure.com/" />
4   <Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
    Value=`"https://login.microsoftonline.com/" />
5   <Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`" Value=`"
    core.windows.net`" />
6   <Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`
    " />
7   <Property xsi:type=`"StringProperty`" Name=`"SharedTenants`" Value=`"[
    {
8     'Tenant': '123abc', 'Subscriptions': ['345', '567'] }
9   ]`" />
10  </CustomProperties>"
11  -LiteralPath @"(XDHyp:\Connections\azure)" -PassThru -UserName "
    advc345" -SecurePassword
12  $psd
13  <!--NeedCopy-->

```

注意：

您可以添加多个租户。每个租户可以有多个订阅。

从不同的租户中选择映像 可以在 Azure Compute Gallery 中选择属于不同 Azure 租户的映像，以使用 PowerShell 命令创建和更新 MCS 目录。

1. 在托管单元根文件夹中，Citrix 创建了一个名为 `sharedsubscription` 的新共享订阅文件夹。
2. 列出所有共享的订阅。

```

1   Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
2   <!--NeedCopy-->

```

3. 选择一个共享订阅，然后列出该共享订阅的所有共享资源组。

```

1   Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription
2   <!--NeedCopy-->

```

4. 选择一个资源组，然后列出该资源组的所有库。



```
1 Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.  
  sharedsubscription\ xyz.resourcegroup  
2 <!--NeedCopy-->
```

5. 选择一个库，然后列出该库的所有映像定义。

```
1 Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.  
  sharedsubscription\xyz.resourcegroup\efg.gallery  
2 <!--NeedCopy-->
```

6. 选择一个映像定义，然后列出该映像定义的所有映像版本。

```
1 Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.  
  sharedsubscription\xyz.resourcegroup\efg.gallery\hij.  
  imagedefinition  
2 <!--NeedCopy-->
```

7. 使用以下元素创建和更新 MCS 目录：

- 资源组
- 库
- 库映像定义
- 库映像版本

有关如何使用 Remote PowerShell SDK 创建目录的信息，请参阅 <https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>。

为 **Azure** 管理的流量创建安全的环境

MCS 允许通过环境中的 Cloud Connector 路由网络流量（从 Citrix Cloud 到 Azure 虚拟机管理程序的 API 调用）。此实现可帮助您锁定 Azure 订阅，以允许来自特定 IP 地址的网络流量。为此，请在 **CustomProperties** 中添加 **ProxyHypervisorTrafficThroughConnector**。设置自定义属性后，可以将 Azure 策略配置为拥有 Azure 托管磁盘的专用磁盘访问权限。

如果您将 Azure 策略配置为自动为每个新磁盘创建磁盘访问权限以使用私有端点，则不能使用与 Azure 强制执行的相同磁盘访问对象同时上载或下载五个以上的磁盘或快照。如果您在资源组级别配置 Azure 策略，则此限制适用于每个计算机目录；如果您在订阅级别配置 Azure 策略，则适用于所有计算机目录。

如果您未将 Azure 策略配置为自动为每个新磁盘创建磁盘访问权限以使用私有端点，则不会强制执行五次并发操作的限制。

注意：

目前，Connector Appliance 不支持此功能。有关与此功能相关的 Azure 限制，请参阅[使用 Azure 私有链接限制托管磁盘的导入/导出访问权限](#)。

启用代理 要启用代理，请在主机连接上设置自定义属性，如下所示：

1. 使用 Remote PowerShell SDK 打开 PowerShell 窗口。有关详细信息，请参阅 <https://docs.citrix.com/en-us/citrix-daas/sdk-api.html#citrix-virtual-apps-and-desktops-remote-powershell-sdk/>。
2. 运行以下命令：

```
1 Add-PSSnapin citrix*.
2 cd XDHyp:\Connections\
3 dir
4 <!--NeedCopy-->
```

3. 将连接中的 CustomProperties 复制到记事本并将属性设置 `<Property xsi:type="StringProperty" Name="ProxyHypervisorTrafficThroughConnector" Value="True"/>` 附加到 CustomProperties 以启用代理。例如：

```
1 <CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-
  instance" xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation">
2 <Property xsi:type="StringProperty" Name="SubscriptionId" Value="
  4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx" />
3 <Property xsi:type="StringProperty" Name="ManagementEndpoint"
  Value="https://management.azure.com/" />
4 <Property xsi:type="StringProperty" Name="AuthenticationAuthority"
  Value="https://login.microsoftonline.com/" />
5 <Property xsi:type="StringProperty" Name="StorageSuffix" Value="
  core.windows.net" />
6 <Property xsi:type="StringProperty" Name="TenantId" Value="5cxxxxx
  -9xxx-4xxx-8xxx-dffe3efdxxxx" />
7 <Property xsi:type="StringProperty" Name="
  ProxyHypervisorTrafficThroughConnector" Value="True" />
8 </CustomProperties>
9 <!--NeedCopy-->
```

4. 在 PowerShell 窗口中，为修改后的自定义属性分配一个变量。例如：

```
1 $customProperty = '<CustomProperties xmlns:xsi="http://www.w3.org
  /2001/XMLSchema-instance" xmlns="http://schemas.citrix.com
  /2014/xd/machinecreation">
2 <Property xsi:type="StringProperty" Name="SubscriptionId" Value
  ="4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx" />
3 <Property xsi:type="StringProperty" Name="ManagementEndpoint"
  Value="https://management.azure.com/" />
4 <Property xsi:type="StringProperty" Name="AuthenticationAuthority"
  Value="https://login.microsoftonline.com/" />
5 <Property xsi:type="StringProperty" Name="StorageSuffix" Value="
  core.windows.net" />
6 <Property xsi:type="StringProperty" Name="TenantId" Value="5cxxxxx
  -9xxx-4xxx-8xxx-dffe3efdxxxx" />
7 <Property xsi:type="StringProperty" Name="
  ProxyHypervisorTrafficThroughConnector" Value="True" />
8 </CustomProperties>'
9 <!--NeedCopy-->
```

5. 运行 `$cred = Get-Credential`。如果出现提示，请提供连接凭据。凭据是 Azure 应用程序 ID 和密钥。
6. 运行 `Set-Item -PSPath XDHyp:\Connections\<Connection_Name> -CustomProperties $customProperty -username $cred.username -Securepassword $cred.password`。

**重要：**

如果您收到一条提示缺失 `SubscriptionId` 的消息，请将自定义属性中的所有双引号 ( `"` ) 替换为反引号，然后是双引号 ( `"` )。例如：

```

1 <CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-
  instance" xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation">
2 <Property xsi:type="StringProperty" Name="SubscriptionId"
  Value="4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx" />
3 <Property xsi:type="StringProperty" Name="ManagementEndpoint"
  Value="https://management.azure.com/" />
4 <Property xsi:type="StringProperty" Name="
  AuthenticationAuthority" Value="https://login.microsoftonline
  .com/" />
5 <Property xsi:type="StringProperty" Name="StorageSuffix" Value
  ="core.windows.net" />
6 <Property xsi:type="StringProperty" Name="TenantId" Value="5
  cxxxxx-9xxx-4xxx-8xxx-dffe3efdxxxx" />
7 <Property xsi:type="StringProperty" Name="
  ProxyHypervisorTrafficThroughConnector" Value="True" />
8 </CustomProperties>
9 <!--NeedCopy-->

```

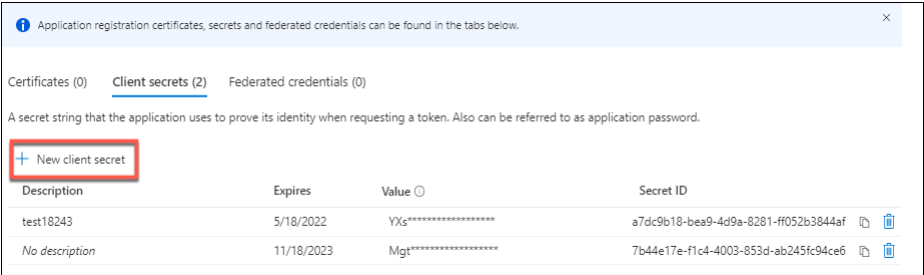
7. 运行 `dir` 以验证更新的 `CustomProperties` 设置。

## 管理应用程序机密和机密过期日期

请务必在密钥到期之前更改连接的应用程序密钥。在密钥到期之前，您会在“完整配置”界面上收到警报。

在 **Azure** 中创建应用程序密钥 可以通过 Azure 门户为连接创建应用程序机密。

1. 选择 **Azure Active Directory**。
2. 从 Azure AD 中的应用程序注册中，选择您的应用程序。
3. 转到证书和密钥。
4. 单击“客户端密钥” > “新建客户端密钥”。



5. 提供密码的说明并指定持续时间。完成后，选择“添加”。

注意：

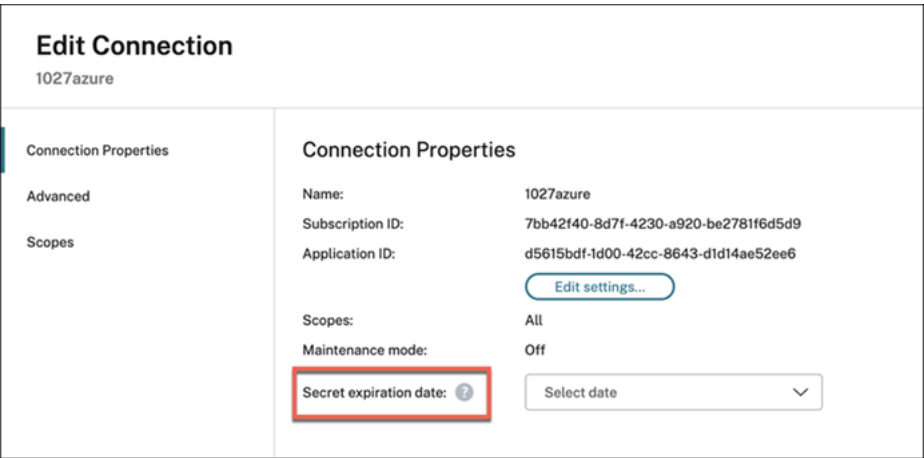
请务必保存客户端密钥，因为您以后将无法检索该密钥。

6. 复制客户端密钥值和到期日期。

7. 在“完整配置”界面中，编辑相应的连接，并将应用程序密钥和密钥到期日期字段中的内容替换为您复制的值。

**更改密钥到期日期** 您可以使用完整配置界面添加或修改正在使用的应用程序密钥的到期日期。

1. 在“添加连接和资源”向导中，右键单击连接，然后单击“编辑连接”。
2. 在“连接属性”页上，单击“密钥到期日期”以添加或修改正在使用的应用程序密钥的过期日期。



## 所需的 **Azure** 权限

本节详细介绍了 Azure 所需的最低权限和一般权限。

### 最低权限

最低权限可提供更好的安全控制。但是，如果仅提供最低权限，则需要额外权限的新功能将失败。本节按操作列出最低权限。

创建主机连接 使用从 Azure 获得的信息添加主机连接。

```
1 "Microsoft.Network/virtualNetworks/read",
2 "Microsoft.Compute/virtualMachines/read",
3 "Microsoft.Compute/disks/read",
4 <!--NeedCopy-->
```

VM 的电源管理 打开或关闭计算机实例的电源。

```
1 "Microsoft.Compute/virtualMachines/read",
2 "Microsoft.Resources/subscriptions/resourceGroups/read",
3 "Microsoft.Compute/virtualMachines/deallocate/action",
4 "Microsoft.Compute/virtualMachines/start/action",
5 "Microsoft.Compute/virtualMachines/restart/action",
6 <!--NeedCopy-->
```

创建、更新或删除 VM 创建计算机目录，然后添加、删除、更新计算机和删除计算机目录。

以下是主映像是托管磁盘或与主机连接位于同一区域的快照时所需的最低权限列表。

```
1 "Microsoft.Resources/subscriptions/resourceGroups/read",
2 "Microsoft.Resources/deployments/validate/action",
3 "Microsoft.Compute/virtualMachines/read",
4 "Microsoft.Compute/virtualMachines/write",
5 "Microsoft.Compute/virtualMachines/delete",
6 "Microsoft.Compute/virtualMachines/deallocate/action",
7 "Microsoft.Compute/snapshots/read",
8 "Microsoft.Compute/snapshots/write",
9 "Microsoft.Compute/snapshots/delete",
10 "Microsoft.Compute/snapshots/beginGetAccess/action",
11 "Microsoft.Compute/snapshots/endGetAccess/action",
12 "Microsoft.Compute/disks/read",
13 "Microsoft.Compute/disks/write",
14 "Microsoft.Compute/disks/delete",
15 "Microsoft.Compute/disks/beginGetAccess/action",
16 "Microsoft.Compute/disks/endGetAccess/action",
17 "Microsoft.Network/virtualNetworks/read",
18 "Microsoft.Network/virtualNetworks/subnets/join/action",
19 "Microsoft.Network/virtualNetworks/subnets/read",
20 "Microsoft.Network/networkSecurityGroups/read",
21 "Microsoft.Network/networkSecurityGroups/write",
22 "Microsoft.Network/networkSecurityGroups/delete",
23 "Microsoft.Network/networkSecurityGroups/join/action",
24 "Microsoft.Network/networkInterfaces/read",
25 "Microsoft.Network/networkInterfaces/write",
26 "Microsoft.Network/networkInterfaces/delete",
27 "Microsoft.Network/networkInterfaces/join/action",
28 <!--NeedCopy-->
```

您需要根据以下功能的最低权限获得下列额外的权限：

- 如果主映像是与主机连接位于同一区域的存储帐户中的 VHD:

```
1 "Microsoft.Storage/storageAccounts/read",
2 "Microsoft.Storage/storageAccounts/listKeys/action",
3 <!--NeedCopy-->
```

- 如果主映像是 Azure Compute Gallery (以前为共享映像库) 中的 ImageVersion:

```
1 "Microsoft.Compute/galleries/read",
2 "Microsoft.Compute/galleries/images/read",
3 "Microsoft.Compute/galleries/images/versions/read",
4 <!--NeedCopy-->
```

- 如果主映像是托管磁盘、快照或 VHD 位于与主机连接区域不同的区域:

```
1 "Microsoft.Storage/storageAccounts/read",
2 "Microsoft.Storage/storageAccounts/listKeys/action",
3 "Microsoft.Storage/storageAccounts/write",
4 "Microsoft.Storage/storageAccounts/delete",
5 <!--NeedCopy-->
```

- 如果您使用 Citrix 管理的资源组:

```
1 "Microsoft.Resources/subscriptions/resourceGroups/write",
2 "Microsoft.Resources/subscriptions/resourceGroups/delete",
3 <!--NeedCopy-->
```

- 如果您将主映像放在 Azure Compute Gallery (以前为共享映像库) 中:

```
1 "Microsoft.Compute/galleries/write",
2 "Microsoft.Compute/galleries/images/write",
3 "Microsoft.Compute/galleries/images/versions/write",
4 "Microsoft.Compute/galleries/read",
5 "Microsoft.Compute/galleries/images/read",
6 "Microsoft.Compute/galleries/images/versions/read",
7 "Microsoft.Compute/galleries/delete",
8 "Microsoft.Compute/galleries/images/delete",
9 "Microsoft.Compute/galleries/images/versions/delete",
10 <!--NeedCopy-->
```

- 如果您使用 Azure 专用主机支持:

```
1 "Microsoft.Compute/hostGroups/read",
2 "Microsoft.Compute/hostGroups/write",
3 "Microsoft.Compute/hostGroups/hosts/read",
4 <!--NeedCopy-->
```

- 如果您将服务器端加密 (SSE) 与客户托管密钥 (CMK) 结合使用:

```
1 "Microsoft.Compute/diskEncryptionSets/read",
2 <!--NeedCopy-->
```

- 如果您使用 ARM 模板 (计算机配置文件) 部署 VM:

```

1 "Microsoft.Resources/deployments/write",
2 "Microsoft.Resources/deployments/operationstatuses/read",
3 "Microsoft.Resources/deployments/read",
4 "Microsoft.Resources/deployments/delete",
5 <!--NeedCopy-->

```

- 如果使用 Azure 模板规范作为计算机配置文件：

```

1 "Microsoft.Resources/templateSpecs/read",
2 "Microsoft.Resources/templateSpecs/versions/read",
3 <!--NeedCopy-->

```

创建、更新和删除包含非托管磁盘的计算机 下面是主映像为 VHD 并使用管理员提供的资源组时所需的最低权限列表：

```

1 "Microsoft.Resources/subscriptions/resourceGroups/read",
2 "Microsoft.Storage/storageAccounts/delete",
3 "Microsoft.Storage/storageAccounts/listKeys/action",
4 "Microsoft.Storage/storageAccounts/read",
5 "Microsoft.Storage/storageAccounts/write",
6 "Microsoft.Compute/virtualMachines/deallocate/action",
7 "Microsoft.Compute/virtualMachines/delete",
8 "Microsoft.Compute/virtualMachines/read",
9 "Microsoft.Compute/virtualMachines/write",
10 "Microsoft.Resources/deployments/validate/action",
11 "Microsoft.Network/networkInterfaces/delete",
12 "Microsoft.Network/networkInterfaces/join/action",
13 "Microsoft.Network/networkInterfaces/read",
14 "Microsoft.Network/networkInterfaces/write",
15 "Microsoft.Network/networkSecurityGroups/delete",
16 "Microsoft.Network/networkSecurityGroups/join/action",
17 "Microsoft.Network/networkSecurityGroups/read",
18 "Microsoft.Network/networkSecurityGroups/write",
19 "Microsoft.Network/virtualNetworks/subnets/read",
20 "Microsoft.Network/virtualNetworks/read",
21 "Microsoft.Network/virtualNetworks/subnets/join/action",
22 <!--NeedCopy-->

```

管理已加入 **Azure AD** 的设备 以下是管理 Azure AD 已加入 Azure 的设备所需的最低权限列表：

```

1 microsoft.directory/devices/standard/read
2 microsoft.directory/devices/delete
3 <!--NeedCopy-->

```

#### 一般权限

贡献者角色拥有管理所有资源的完全访问权限。这组权限不会阻止您获取新功能。



以下权限集提供了将来的最佳兼容性，尽管它包含的权限超过了当前功能集所需的权限亦如此：

```
1 "Microsoft.Compute/diskEncryptionSets/read",
2 "Microsoft.Compute/disks/beginGetAccess/action",
3 "Microsoft.Compute/disks/delete",
4 "Microsoft.Compute/disks/endGetAccess/action",
5 "Microsoft.Compute/disks/read",
6 "Microsoft.Compute/disks/write",
7 "Microsoft.Compute/galleries/delete",
8 "Microsoft.Compute/galleries/images/delete",
9 "Microsoft.Compute/galleries/images/read",
10 "Microsoft.Compute/galleries/images/versions/delete",
11 "Microsoft.Compute/galleries/images/versions/read",
12 "Microsoft.Compute/galleries/images/versions/write",
13 "Microsoft.Compute/galleries/images/write",
14 "Microsoft.Compute/galleries/read",
15 "Microsoft.Compute/galleries/write",
16 "Microsoft.Compute/hostGroups/hosts/read",
17 "Microsoft.Compute/hostGroups/read",
18 "Microsoft.Compute/hostGroups/write",
19 "Microsoft.Compute/snapshots/beginGetAccess/action",
20 "Microsoft.Compute/snapshots/delete",
21 "Microsoft.Compute/snapshots/endGetAccess/action",
22 "Microsoft.Compute/snapshots/read",
23 "Microsoft.Compute/snapshots/write",
24 "Microsoft.Compute/virtualMachines/deallocate/action",
25 "Microsoft.Compute/virtualMachines/delete",
26 "Microsoft.Compute/virtualMachines/read",
27 "Microsoft.Compute/virtualMachines/restart/action",
28 "Microsoft.Compute/virtualMachines/start/action",
29 "Microsoft.Compute/virtualMachines/write",
30 "Microsoft.Network/networkInterfaces/delete",
31 "Microsoft.Network/networkInterfaces/join/action",
32 "Microsoft.Network/networkInterfaces/read",
33 "Microsoft.Network/networkInterfaces/write",
34 "Microsoft.Network/networkSecurityGroups/delete",
35 "Microsoft.Network/networkSecurityGroups/join/action",
36 "Microsoft.Network/networkSecurityGroups/read",
37 "Microsoft.Network/networkSecurityGroups/write",
38 "Microsoft.Network/virtualNetworks/subnets/read",
39 "Microsoft.Network/virtualNetworks/read",
40 "Microsoft.Network/virtualNetworks/subnets/join/action",
41 "Microsoft.Resources/deployments/operationstatuses/read",
42 "Microsoft.Resources/deployments/read",
43 "Microsoft.Resources/deployments/validate/action",
44 "Microsoft.Resources/deployments/write",
45 "Microsoft.Resources/deployments/delete",
46 "Microsoft.Resources/subscriptions/resourceGroups/read",
47 "Microsoft.Resources/subscriptions/resourceGroups/write",
48 "Microsoft.Resources/subscriptions/resourceGroups/delete",
49 "Microsoft.Storage/storageAccounts/delete",
50 "Microsoft.Storage/storageAccounts/listKeys/action",
51 "Microsoft.Storage/storageAccounts/read",
52 "Microsoft.Storage/storageAccounts/write",
```



```
53 "Microsoft.Resources/templateSpecs/read",  
54 "Microsoft.Resources/templateSpecs/versions/read",  
55 <!--NeedCopy-->
```

**Azure AD 权限** 如果您创建 Azure AD 加入的计算机目录，那么当您启用 Azure AD 加入的设备管理时，MCS 将负责管理 Azure AD 设备。Azure AD 内置的云设备管理员角色提供了最佳的兼容性，尽管它包含的权限确实超过了当前功能集所需的权限。

#### 下一步的去向

- 如果您处于初始部署过程中，请参阅[创建计算机目录](#)。
- 有关 Azure 的特定信息，请参阅[创建 Microsoft Azure 目录](#)。

#### 更多信息

- [创建和管理连接和资源](#)
- [Microsoft Azure Resource Manager 虚拟化环境](#)

## 与 Microsoft System Center Virtual Machine Manager 的连接

January 23, 2024

[创建和管理连接和资源](#)介绍了用于创建连接的向导。以下信息涵盖了特定于 Microsoft System Center Virtual Machine Manager (VMM) 的详细信息。

#### 注意：

在创建与 VMM 的连接之前，您需要先完成将 VMM 设置为资源位置。请参阅[Microsoft System Center Virtual Machine Manager 虚拟化环境](#)。

#### 创建连接

如果您的 VM 是使用 MCS 预配的，请在连接创建向导中执行以下操作：

- 以主机服务器的完全限定的域名格式输入地址。
- 输入您之前设置的管理员帐户的凭据。此帐户必须具有创建新 VM 的权限。
- 在“主机详细信息”对话框中，选择创建 VM 时将使用的群集或独立主机。

重要

即使使用单 Hyper-V 主机部署，也请浏览群集或独立主机。

## 下一步的去向

- 如果您处于初始部署过程中，请参阅[创建计算机目录](#)。
- 要在 SMB 3 文件共享上使用 MCS 创建计算机目录，请参阅[创建 Microsoft System Center 虚拟机管理器目录](#)。

## 更多信息

- [创建和管理连接和资源](#)
- [Microsoft System Center Virtual Machine Manager 虚拟化环境](#)。

## 与 Nutanix 的连接

January 23, 2024

[创建和管理连接和资源](#)介绍了用于创建连接的向导。以下信息涵盖了特定于 Nutanix 的详细信息。

注意：

在创建与 Nutanix 的连接之前，需要先完成将 Nutanix 帐户设置为资源位置的过程。请参阅[Nutanix 虚拟化环境](#)。

## 创建与 Nutanix 的连接

以下信息是对[创建和管理连接](#)中的指南的补充。要创建 Nutanix 连接，请按照该文章中的常规指导进行操作，并注意 Nutanix 特定的详细信息。

在添加连接和资源向导中的连接页面上选择 **Nutanix** 连接类型，然后指定地址和凭据以及连接名称。在网络页面上，选择用于托管单元的网络。

以下连接类型可供选择：**Nutanix AHV**、**Nutanix AHV DRaaS** 和 **Nutanix AHV PC**。

- 对于 **Nutanix AHV**，请指定 Prism Element (PE) 群集地址和凭据。
- 对于 **Nutanix AHV PC**，请指定虚拟机管理程序地址和凭据。

注意：

目前，连接类型 **Nutanix AHV PC** 仅用于在 Azure 上创建与 Nutanix Cloud Clusters (NC2) 的连接。  
此外，计算机目录只能托管在 Azure 连接上的 NC2 中的单个群集上。

- 对于 **Nutanix AHV DRaaS**，请指定您的地址和用户名，然后导入 Nutanix DRaaS 凭据文件中包含的公钥和私钥（.pem）。（公钥和私钥由 Nutanix DRaaS 管理员在 Nutanix DRaaS 云中生成。）
  - 要导入密钥，请找到您的凭据文件，使用记事本（或任何文本编辑器）打开该文件，然后复制内容。之后，请返回到连接页面，选择导入密钥，粘贴内容，然后选择保存。

注意：请勿更改凭据内容或其格式。

提示：

如果您使用 Nutanix AHV (Prism Element) 作为资源部署计算机，请选择虚拟机磁盘所在的容器。

## 下一步的去向

- 如果您处于初始部署过程中，请参阅[创建计算机目录](#)。
- 有关 Nutanix 的具体信息，请参阅[创建 Nutanix 目录](#)。

## 更多信息

- [创建和管理连接和资源](#)
- [Nutanix 虚拟化环境](#)
- [Nutanix 云和合作伙伴解决方案](#)

## 与 Nutanix 云和合作伙伴解决方案的连接

January 23, 2024

[创建和管理连接和资源](#)介绍了用于创建连接的向导。以下信息涵盖了特定于 Nutanix 云和合作伙伴解决方案的详细信息。

Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）支持以下 Nutanix 云和合作伙伴解决方案：

- AWS 上的 Nutanix Cloud Clusters

注意：

- 在创建与 Nutanix 云和合作伙伴解决方案的连接之前，必须先完成对应帐户作为资源位置的设置。请参阅[Nutanix 云和合作伙伴解决方案](#)。

- 有关在云端设置 Nutanix 的最新信息，请关注 [Nutanix 最新指南](#)。

## 连接到 Nutanix Prism

创建 Nutanix 群集后，连接到 Nutanix Prism。

要连接到 Nutanix Prism，请执行以下操作：

1. 在 10.0.129.0/24 子网中创建堡垒 VM。
2. RDP 进入堡垒 VM，请转到您在上一节中复制的 **Prism Element** 的 URL。
3. 使用默认凭据登录：`admin:nutanix/4u`。请谨记更改密码。

## 在 Nutanix 群集上创建 VM

连接到 **Nutanix Prism** 后，在 [Nutanix 群集中创建 VM](#)。

如果 VM 需要 **Internet** 访问权限

1. 前往 AWS 控制台。
2. 在与 Nutanix CFS 创建的子网相同的 VPC 中创建一个新子网 10.0.130.0/24。
3. 在此子网的路由表中添加一条路由，将所有 none 本地流量定向到上述 NAT 网关。
4. RDP 进入堡垒 VM，请转到您在上一节中复制的 **Prism Element** 的 URL 并登录。
5. 添加新网络。转到设置 > 网络配置 > 创建子网。使用 AWS 中使用的相同子网 10.0.130.0/24。
6. 在该新子网中创建所有 VM（AD、CC、VDA 等）。

如果 VM 不需要 **Internet** 访问权限

1. RDP 进入堡垒 VM，请转到您在上一节中复制的 **Prism Element** 的 URL 并登录。
2. 添加新网络。转到设置 > 网络配置 > 创建子网。使用子网 10.0.129.0/24。
3. 在该子网中创建所有 VM（AD、CC、VDA 等）。

提示：

确保 VM 中的时间和时区信息设置正确。对于 AD 来说尤其如此。

## 创建主机连接

1. 在管理 > 完整配置中，选择左侧窗格中的托管。
2. 单击“添加连接和资源”。
3. 在连接屏幕上，选择新建连接，然后在连接地址中输入 `https://xxx.xxx.xxx.xxx:9440`。
4. 按照 UI 完成向导。

### 注意：

所有连接器虚拟机都必须安装 Nutanix 插件才能在 Citrix Studio 中使用 Nutanix 选项，即使插件未在 Nutanix 区域中使用。

### 下一步的去向

- 如果您处于初始部署过程中，请参阅[创建计算机目录](#)。
- 有关 Nutanix 的具体信息，请参阅[创建 Nutanix 目录](#)。

### 更多信息

- [创建和管理连接和资源](#)
- [Nutanix 虚拟化环境](#)
- [Nutanix 云和合作伙伴解决方案](#)

## 与 VMware 的连接

March 5, 2024

[创建和管理连接和资源](#)介绍了用于创建连接的向导。以下信息涵盖了特定于 VMware 虚拟化环境的详细信息。

### 注意：

在创建与 VMware 的连接之前，需要先完成将 VMware 帐户设置为资源位置的过程。请参阅[VMware 虚拟化环境](#)。

### 所需的权限

创建一个 VMware 用户帐户和一个或多个 VMware 角色，该角色具有本文中列出的一组或全部权限。角色的创建基于用户随时请求各种 Citrix DaaS 操作的权限所需的特定粒度级别。要在任何时候授予用户特定的权限，请至少在数据中心级别将其与相应的角色相关联。

下表显示了 Citrix DaaS 操作与 VMware 所需的最低权限之间的映射。

### 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 &gt; 交互 &gt; 关闭

VirtualMachine.Interact.PowerOn

虚拟机 &gt; 交互 &gt; 打开

VirtualMachine.Interact.Reset

虚拟机 &gt; 交互 &gt; 重置

VirtualMachine.Interact.Suspend

虚拟机 &gt; 交互 &gt; 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 &gt; 分配空间

Datastore.Browse

数据存储 &gt; 浏览数据存储

Datastore.FileManagement

数据存储 &gt; 低级别文件操作

Network.Assign

网络 &gt; 分配网络

Resource.AssignVMToPool

资源 &gt; 将虚拟机分配到资源池

VirtualMachine.Config.AddExistingDisk

虚拟机 &gt; 配置 &gt; 添加现有磁盘

VirtualMachine.Config.AddNewDisk

虚拟机 &gt; 配置 &gt; 添加新磁盘

VirtualMachine.Config.AdvancedConfig

虚拟机 &gt; 配置 &gt; 高级

VirtualMachine.Config.RemoveDisk

虚拟机 &gt; 配置 &gt; 删除磁盘

VirtualMachine.Config.CPUCount

虚拟机 &gt; 配置 &gt; 更改 CPU 计数

VirtualMachine.Config.Memory

虚拟机 &gt; 配置 &gt; 更改内存

VirtualMachine.Config.Settings

虚拟机 &gt; 配置 &gt; 更改设置

VirtualMachine.Interact.PowerOff

虚拟机 &gt; 交互 &gt; 关闭

SDK	用户界面
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, 更新 2, vSphere 5.1, 更新 1, 以及 vSphere 6.x, 更新 1: 虚拟机 > 状态 > 创建快照; vSphere 5.5: 虚拟机 > 快照管理 > 创建快照; vSphere 8.0: 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
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

SDK	用户界面
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 驱动存储更新	配置文件驱动存储 > 配置文件驱动的存储更新。对于 vSphere 8：虚拟机存储策略 > 更新虚拟机存储策略
storage.Profile 驱动存储视图	配置文件驱动存储 > 配置文件驱动的存储视图。对于 vSphere 8：虚拟机存储策略 > 查看虚拟机存储策略

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：

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



SDK	用户界面
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：

注意：

使用配备 vTPM 的 VM 创建 MCS 计算机目录需要这些权限。

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
Cryptographic operations.Decrypt	权限 > 所有权限 > 加密操作 > 解密
Cryptographic operations.Migrate	权限 > 所有权限 > 加密操作 > 迁移

SDK	用户界面
Cryptographic operations.Read KMS 信息	权限 > 所有权限 > 加密操作 > 读取 KMS 信息

预配计算机 (Citrix Provisioning)

要通过 Citrix Provisioning 控制台使用 Citrix Virtual Apps and Desktops 安装向导和导出设备向导置虚拟机，则需要这些权限才能克隆和部署模板。在创建主机连接时设置权限。  
您需要来自预配计算机 (Machine Creation Services) 的所有权限以及以下权限。

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
vApp.Export	vApp > 导出

注意：  
**vApp.Export** 对使用计算机配置文件创建 MCS 计算机目录是必需的。

保护与 VMware 环境的连接

使用 [HTTPS/SSL](#) 与 vCenter 的连接需要 Citrix DaaS 信任该连接。

有两种选择：

- (推荐) Citrix DaaS 数据库安装了 SSL 指纹。每个 Cloud Connector 上的 Citrix DaaS 都使用此指纹来信任与 vCenter 的连接。
- (备选) 每个 Cloud Connector 都信任 vCenter 证书，Cloud Connector 上的服务会重复使用这种信任。这种信任可能来自：
  - vCenter 证书，由证书颁发机构颁发并受 Windows 信任，从而在 Windows 与 vCenter 之间建立信任。
  - 在 Windows 上安装了 vCenter 证书，从而在 Windows 和 vCenter.OT 之间建立了信任

注意：

VMware Cloud 及其合作伙伴解决方案不需要 vCenter 证书和 VMware SSL 指纹。

## VMware SSL 指纹

VMware SSL 指纹功能解决了一个在与 VMware vSphere 虚拟机管理程序建立主机连接时经常报告的错误。以前，管理员必须在创建连接之前在站点中 Citrix 托管的 Delivery Controller 和虚拟机管理程序证书之间手动创建信任关系。VMware SSL 指纹功能取消了该手动要求：不可信证书的指纹存储在站点数据库中，这样 Citrix DaaS（即使控制者不是）也能持续将虚拟机管理程序识别为可信。

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。

稍后可以使用 PowerShell SDK `Set-Item -LiteralPath "<FullPath_to_connection>"-username $cred.username -Securepassword $cred.password -SslThumbprint "<New ThumbPrint>"-hypervisorAddress <vcenter URL>` 更新 VMware SSL 指纹。

提示：

证书指纹必须用大写字母书写。

## 获取和导入证书

为了保护 vSphere 通信的安全，Citrix 建议您使用 HTTPS，而不使用 HTTP。HTTPS 需要数字证书。Citrix 建议您根据贵组织的安全策略使用由证书颁发机构所颁发的数字证书。

如果无法使用证书颁发机构所颁发的数字证书，而您组织的安全策略允许使用数字证书，则可以使用由 VMware 安装的自签名证书。在每个 Cloud Connector 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，该文件位于 %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 Cloud Connector 上可访问的位置。
- b) 在 Cloud Connector 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：如果您使用的是 Internet Explorer，则必须右键单击 Internet Explorer，然后选择以管理员身份运行才能下载或安装证书，具体取决于您的用户帐户。

- 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) 单击“证书无效”，然后单击“详细信息”选项卡。
- e) 单击“导出”。
- 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：

- 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。

3. 将证书导入到每个 Cloud Connector 上的证书存储中。

- a) 单击安装证书，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。在受支持的更高版本中：选中受信任人，然后单击确定。单击下一步，然后单击完成。

#### 重要提示：

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。

#### 下一步的去向

- 如果您处于初始部署过程中，请参阅[创建计算机目录](#)。
- 有关 VMware 的特定信息，请参阅[创建 VMware 目录](#)。

#### 更多信息

- [创建和管理连接和资源](#)
- [VMware 虚拟化环境](#)。
- [VMware 云和合作伙伴解决方案](#)

### 与 VMware 云和合作伙伴解决方案的连接

January 23, 2024

设置 [Azure VMware 解决方案 \(AVS\) 群集](#)、[Google Cloud VMware Engine](#) 和 [AWS 上的 VMware 云](#) 后，创建连接。有关创建连接的信息，请参阅[与 VMware 虚拟化环境的连接](#)。

## 下一步的去向

- 如果您处于初始部署过程中，请参阅[创建计算机目录](#)。
- 有关 VMware 的特定信息，请参阅[创建 VMware 目录](#)。

## 更多信息

- [创建和管理连接和资源](#)
- [VMware 虚拟化环境](#)。
- [VMware 云和合作伙伴解决方案](#)

## 连接到 XenServer

March 5, 2024

[创建和管理连接和资源](#)提供了使用向导创建连接的详细说明。在建立与 XenServer（前身为 Citrix Hypervisor）的连接之前，需要先完成将 XenServer 设置为主机。请参阅在 [Citrix Cloud 中添加资源类型或激活未使用的域](#)。

### 创建与 XenServer 的连接

创建与 XenServer 的连接时，必须为虚拟机超级管理员（VM 电源管理员）或更高级别的用户提供凭据。

Citrix 建议使用 HTTPS 确保与 XenServer 的通信安全。要使用 HTTPS，必须替换安装在 XenServer 上的默认 TLS 证书。有关详细信息，请参阅[在服务器上安装 TLS 证书](#)。

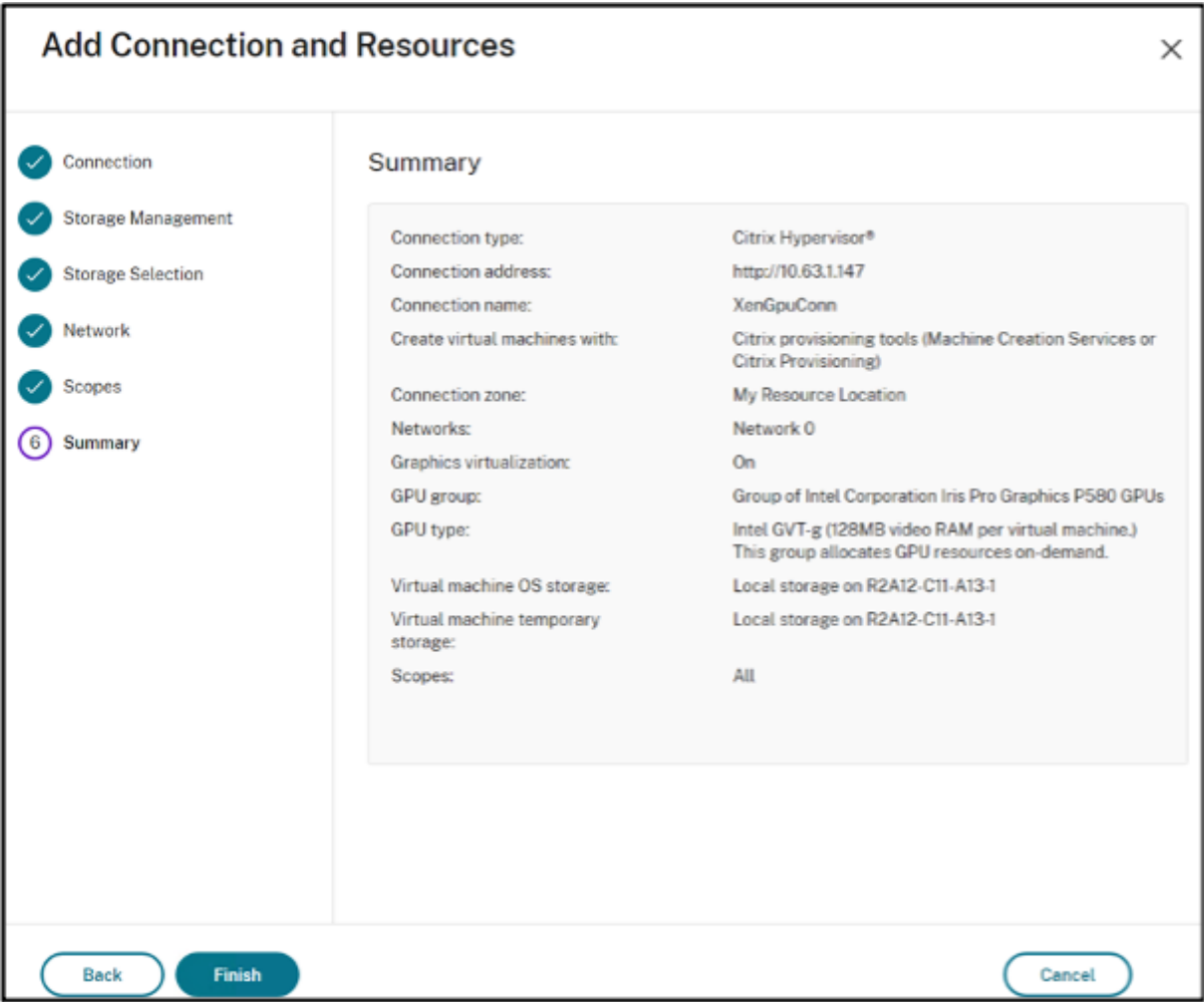
如果在 XenServer 服务器上启用了高可用性，则可以对其进行配置。Citrix 建议您选择池中的所有服务器（从“编辑高可用性”中），以便在池主服务器出现故障时允许与 XenServer 服务器进行通信。

#### 注意：

如果您使用的是 HTTPS，想要配置高可用性服务器，请不要为池中的所有服务器安装通配符证书。每台服务器都需要单独的证书。

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

如果您连接到支持 vGPU 的 XenServer，则可以在创建连接的向导的摘要页面中验证 GPU 组和 GPU 类型。



### 将 **IntelliCache** 用于 **XenServer** 连接

通过使用 IntelliCache，托管的 VDI 部署将更节省成本，因为您可以将共享存储与本地存储结合使用。这会提高性能并降低网络流量。本地存储对共享存储的主映像进行缓存，从而减少了共享存储上的读操作数量。对于共享桌面，对不同磁盘写入的内容将写入到主机上的本地存储而不是共享存储中。

重要注意事项如下：

- 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确保尽可能快的数据传输。

要使用 IntelliCache，请按详细说明启用 IntelliCache：

- 安装 XenServer 时，选择“启用精简预配”。有关从本地媒体安装 XenServer 主机的信息，请参阅[安装 XenServer 主机](#)。Citrix 不支持混合服务器池，有些服务器启用了 IntelliCache，有些服务器未启用 IntelliCache。

- 在 Citrix DaaS 中，IntelliCache 默认处于禁用状态。只有在创建 XenServer 连接时才能更改设置。以后不能禁用 IntelliCache。创建 XenServer 连接时：
  - 选择共享作为存储类型。
  - 选中使用 **IntelliCache** 复选框。

有关详细信息，请参阅 [IntelliCache](#)。

## 下一步的去向

- 如果您处于初始部署过程中，请参阅[创建计算机目录](#)。
- 有关 XenServer 的特定信息，请参阅[创建 XenServer 目录](#)。

## 更多信息

- [创建和管理连接和资源](#)
- [XenServer 虚拟化环境](#)

## 创建计算机目录

March 5, 2024

### 注意：

本文介绍了如何使用“完整配置”界面创建目录。如果使用“快速部署”来创建 Azure 资源，请按照[使用快速部署创建目录](#)中的指导进行操作。

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。在计算机目录中，所有计算机共享一个共同的操作系统类型，可以是多会话操作系统或单会话操作系统，例如基于 Windows 或 Linux 的系统。

管理 > 完整配置界面可指导您创建第一个计算机目录。创建第一个计算机目录后，您可以创建第一个交付组。之后，您可以更改所创建的目录，也可以创建更多目录。

## 概述

在您创建 VM 的目录时，要指定如何预配这些 VM。可以使用 Machine Creation Services (MCS)。也可以使用您自己的工具来提供计算机。

- 如果使用 MCS 预配 VM，则需要提供一个映像（或快照）以在目录中创建完全相同的 VM。在创建目录之前，必须首次设置与所选虚拟机管理程序或云服务的托管连接，然后必须在同一虚拟机管理程序或服务上创建和配置主映像。配置主映像需要执行诸如必要时加入域、安装所需的驱动程序、要发布的应用程序以及在映像上部署 Virtual Delivery Agent (VDA) 等任务。
- 创建主映像后，您可以在“管理”>“完整配置”界面中创建计算机目录。选择该映像（或某个映像的快照），指定要在目录中创建的 VM 数以及配置其他信息。
- 如果您的计算机已经可用，则仍必须创建一个或多个计算机目录才能将这些虚拟机导入到目录中。

使用 MCS 创建第一个目录时，需要指定之前创建的托管单元。托管单元为您创建虚拟机提供资源配置。稍后（在创建第一个目录和交付组之后），您可以更改有关该托管单元或其父主机连接的信息，或者创建更多连接和托管单元。

如果 Cloud Connector 无法正常运行，MCS 配置操作（例如目录更新）需要比平时更长的时间，并且管理界面的性能会显著下降。

## RDS 许可证检查

创建包含 Windows 多会话操作系统计算机的计算机目录时，会自动检查是否存在有效的 Microsoft RDS 许可证。在目录中搜索已开机并注册的计算机以进行检查。

- 如果找不到已开机并注册的计算机，则会显示警告，说明无法执行 RDS 许可检查。
- 如果找到计算机并检测到错误，则显示 > 完整配置会显示针对包含检测到的问题的目录的警告消息。要从某个目录中删除 RDS 许可证警告（使其不再出现在显示中），请选择该目录。选择删除 **RDS** 许可证警告。出现提示时，确认操作。

## VDA 注册

必须向要在启动代理会话时考虑使用的 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。可能无法注册 VDA 的原因有很多，您可以对其中许多原因进行故障排除。故障排除信息在目录创建向导中提供，以及在您向交付组添加了目录之后提供。

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，如果一条消息表明无法获得有关计算机的信息（可能是因为它从未注册过），则无论如何您都可以选择添加该计算机。

有关 VDA 注册故障排除的详细信息，请参阅 [CTX136668](#)。

## MCS 目录创建摘要

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。

- 如果您选择图像（而不是快照），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所有存储位置。
- 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。除了每个 VM 的两个磁盘外，快照或主映像的完整副本也存储在同一个存储位置。如果定义了多个存储位置，每个磁盘位置将获得以下磁盘类型：
  - 快照的完整副本（如上所述），该副本为只读且在所创建的 VM 之间共享。
  - 唯一的 16 MB 身份磁盘，为每个 VM 提供唯一身份。每个 VM 获得身份磁盘。
  - 唯一的差异磁盘，用于存储对 VM 执行的写操作。此磁盘采用精简预配（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 都有一个不同的磁盘。差异磁盘保存会话期间所做的更改。对于专有桌面，此磁盘为永久磁盘。对于池桌面，每次重新启动时会删除此磁盘并创建一个新磁盘。

或者，在创建 VM 以交付静态桌面时，您可以指定（在目录创建向导的计算机页面上）胖（完整复制）VM 克隆。完整克隆不需要在每个数据存储上保留主映像。每个 VM 均有自己的文件。

## 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：

- 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：从基础主映像复制时包含操作系统。
- 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：

- [XenServer IntelliCache](#) 在本地存储器上为每台 XenServer 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。计算空间以包括以下方面的开销：

- [日志文件](#)
- 虚拟机管理程序特定的文件。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。

## Machine Creation Services (MCS) 存储优化

Machine Creation Services (MCS) 存储优化功能也被称为 MCS I/O。该功能仅在 Azure、GCP、XenServer、VMware 和 SCVMM 上可用。

- 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 DaaS。

**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。

有关为回写式缓存磁盘分配驱动器号的信息，请参阅为 MCS I/O 回写式缓存磁盘分配特定的驱动器号。

**在虚拟机管理程序或云服务上准备主映像**

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。主机供应商和云服务提供商可能会使用不同的术语。
- 确保虚拟机管理程序或云服务具有足够多的处理器、内存和存储来容纳创建的计算机数。
- 正确配置桌面和应用程序所需的硬盘空间量。因为该值以后不能更改，也不能在计算机目录中更改。
- Remote PC Access 计算机目录不使用主映像。
- 在使用 MCS 时的 Microsoft KMS 激活注意事项：如果您的部署包括采用 XenServer 6.1 或 6.2、vSphere 或 Microsoft System Center Virtual Machine Manager 主机的 7.x VDA，则无需手动重新部署 Microsoft Windows 或 Microsoft Office。

**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 建议安装最新版本的 VDA 以允许访问最新功能。在主映像上安装 VDA 失败会导致目录创建失败。
- 所需的第三方工具（例如防病毒软件或电子软件分发代理）。使用适合用户和计算机类型的设置配置服务（如更新功能）。
- 未虚拟化的第三方应用程序。Citrix 建议对应用程序进行虚拟化。进行虚拟化后，无需在添加或重新配置应用程序后更新主映像，从而降低成本。此外，减少安装的应用程序数量还可以减小主映像硬盘的大小，从而节约存储成本。
- 具有建议设置的 App-V 客户端（如果计划发布 App-V 应用程序）。App-V 客户端可从 Microsoft 获取。
- 使用 MCS 时，如果要本地化 Microsoft Windows，请安装区域设置和语言包。在预配期间，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。

**重要提示：**

如果要使用 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。从管理 > 完整配置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. 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。
5. Citrix 建议您创建并命名主映像的快照，以便以后能识别该快照。如果您在创建目录时指定主映像而非快照，管理界面将创建一个快照，但您无法对其进行命名。

## 批量许可激活

MCS 支持批量许可激活，以自动执行和管理 Windows 操作系统和 Microsoft Office 的激活。MCS 支持的批量许可激活的三种模式如下：

- 密钥管理服务 (KMS)
- 基于 Active Directory 的激活 (ADBA)
- 多次激活密钥 (MAK)

创建计算机目录后，可以更改激活设置。

### 密钥管理服务 (KMS)

KMS 是一种不需要专用系统的轻型服务，可以轻松地将其他服务托管在提供其他服务的系统中。Citrix 支持的所有 Windows 版本都支持此功能。在准备映像期间，MCS 会重置 Microsoft Windows 和 Microsoft Office KMS。您可以通过运行 [Set-Provserviceconfigurationdata](#) 命令跳过重置。有关映像准备期间 Microsoft Windows KMS Rearm 和 Microsoft Office KMS Rearm 的详细信息，请参阅 [Machine Creation Services: Image Preparation Overview and Fault-Finding](#) (Machine Creation Services: 映像准备概述和故障查找)。有关 KMS 激活的详细信息，请参阅 [Activate using Key Management Service](#) (使用密钥管理服务进行激活)。

#### 注意：

运行 [Set-Provserviceconfigurationdata](#) 命令后创建的所有计算机目录的设置都与命令中提供的设置相同。

### 基于 Active Directory 的激活 (ADBA)

ADBA 使您能够通过其域连接激活计算机。计算机在加入域时立即激活。只要这些计算机保持加入域并与域联系，就会保持激活状态。除 Windows Server 2022 外，Citrix 支持的所有 Windows 版本都支持此功能。有关基于 Active Directory 的激活的详细信息，请参阅 [Activate using Active Directory-based activation](#) (使用基于 Active Directory 的激活执行激活)。

## 多次激活密钥 (MAK)

MAK 是一种在 Microsoft 服务器的帮助下激活音量和对 Windows 系统进行身份验证的方法。您必须从 Microsoft 购买 MAK 密钥，该密钥分配了固定数量的激活次数。每次激活 Windows 系统时，激活次数都会减少。有两种激活系统的方法：

- 联机激活：如果您要激活的 Windows 系统具有 Internet 访问权限，系统会在安装产品密钥时自动激活 Windows。此过程将相应的 MAK 的激活次数减少 1。
- 脱机激活：如果 Windows 系统无法连接到 Internet 进行联机激活，MCS 会从 Microsoft 服务器获取确认 ID 和安装 ID 以激活 Windows 系统。这种激活方式对非持久性计算机目录非常有用。

### 关键要求

- Delivery Controller 必须具有 Internet 访问权限。
- 如果要更新的新映像的 MAK 密钥与原始映像的 MAK 密钥不同，则创建新目录。
- 在主映像上安装 MAK 密钥。有关在 Windows 系统中安装 MAK 密钥的步骤，请参阅[部署 MAK 激活](#)。
- 如果您未使用映像准备，请：
  1. 在 `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation` 下添加注册表 DWORD 值 `Manual`。
  2. 将值设置为 1。

**激活次数** 要查看 MAK 密钥的剩余激活次数或者查看 VM 是否正在消耗两次或更多次激活，请使用批量激活管理工具 (VAMT)。请参阅[安装 VAMT](#)。

**使用 MAK 激活 Windows 系统** 要使用 MAK 激活 Windows 系统，请执行以下操作：

1. 在主映像上安装产品密钥。此步骤消耗一个激活次数。
2. 创建 MCS 计算机目录。
3. 如果您未使用映像准备，请：
  - a) 在 `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation` 下添加注册表 DWORD 值 `Manual`。
  - b) 将值设置为 1。

此方法禁用联机激活选项。

4. 向计算机目录中添加 VM。

5. 打开 VM 的电源。
6. 根据联机激活还是脱机激活，Windows 系统会被激活。
  - 如果联机激活，则会在安装产品密钥后激活 Windows 系统。
  - 如果激活处于脱机状态，MCS 将与预配的 VM 进行通信以获取 Windows 系统的激活状态。然后，MCS 从 Microsoft 服务器检索确认 ID 和安装 ID。这些 ID 用于激活 Windows 系统。

**故障排除** 如果未使用已安装的 MAK 密钥激活已预配的 VM，请在 PowerShell 窗口中运行 `Get-ProvVM` 或 `Get-ProvScheme` 命令。

- `Get-ProvScheme` 命令：请查看最新主映像中与 MCS 计算机目录关联的参数 `WindowsActivationType`。
- `Get-ProvVM` 命令。请参阅参数 `WindowsActivationType`、`WindowsActivationStatus`、`WindowsActivationStatusErrorCode` 和 `WindowsActivationStatusError`。

可以检查错误并验证解决问题的步骤。

## 使用完整配置界面创建计算机目录

创建目录之前，请执行以下操作：

- 确保您已创建与虚拟机管理程序、云服务以及托管您的计算机的其他资源的连接。
- 如果您创建了用于置备计算机的主映像。确保您已在该主映像上安装了 VDA。

### 注意：

当您使用云服务或虚拟机管理程序托管虚拟机时，目录创建向导可能会包含特定于该主机的额外页面。例如，使用 Azure Resource Manager 主映像时，目录创建向导将包含一个存储和许可证类型页面。有关特定于主机的信息，请参阅[下一步去向](#)中提及的特定文章。

## 启动目录创建向导

1. 登录 [Citrix Cloud](#)。在左上角的菜单中，选择我的服务 > **DaaS**。
2. 选择管理。
3. 如果这是正在创建的第一个目录，则系统会引导您选择正确的目录（例如“设置计算机并创建计算机目录以运行应用程序和桌面”）。目录创建向导将打开。
4. 如果您已经创建了一个目录并且想要创建另一个目录，请按照以下步骤操作：
  - a) 在管理 > 完整配置中，选择左窗格中的计算机目录。
  - b) 要使用文件夹组织目录，请在默认的 计算机目录 文件夹下创建文件夹。有关详细信息，请参阅[创建目录文件夹](#)。

- c) 选择要在其中创建目录的文件夹，然后单击创建计算机目录。目录创建向导将打开。

该向导将引导您浏览以下部分中描述的页面。根据您所做的选择以及使用的（与主机的）连接，您看到的页面可能会有所不同。[主机/虚拟化资源](#)列出了受支持的主机类型的信息源。

### 选择计算机类型

每个目录只能包含一种操作系统类型的计算机。在“计算机类型”页面上选择以下选项之一：

- 多会话操作系统：多会话操作系统目录提供托管共享桌面。这些计算机可以运行 Windows 或 Linux 操作系统的支持版本，但该目录不能同时包含 Windows 和 Linux 操作系统。
- 单会话操作系统：单会话操作系统目录提供可分配给不同用户的 VDI 桌面。
- **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。

### 选择计算机管理选项

注意：

如果您在“计算机类型”页面上选择“**Remote PC Access**”，则不会出现“计算机管理”页面。

计算机管理页面显示了计算机的管理方式以及您要用于部署计算机的工具。

选择其中一个选项以指明必须如何通过完整配置界面对计算机进行电源管理：

- 电源管理的计算机（例如，虚拟机或刀片式计算机）：只有当您已经配置了与虚拟机管理程序或云服务的[连接](#)时，此选项才可用。
- 计算机不受电源管理（例如，物理机）

如果选择电源管理的计算机（例如，虚拟机或刀片式计算机）选项，则选择一个工具来创建虚拟机：

- **Citrix Machine Creation Services (MCS)**：使用主映像创建和管理虚拟机。云环境中的计算机目录使用 MCS。MCS 不可用于物理机。
- 其他服务或技术：一种用于管理数据中心中已有计算机的工具。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。

注意：

对于 Linux 操作系统计算机，请参阅[使用 Machine Creation Services \(MCS\) 创建 Linux VDA](#)。

### 选择桌面体验

**注意：**

桌面体验页面上的选项因您在计算机类型页面上选择的计算机类型而异。

- 对于多会话操作系统计算机，用户每次登录时都会被分配一个随机桌面。您可以在“桌面体验”页面上获得以下选项：
  - 将更改保存到托管虚拟桌面的计算机的本地磁盘上：持久
  - 用户注销时丢弃所有更改并清除虚拟桌面：非持久

**注意：**

对于永久性多会话计算机，将保存用户对桌面所做的更改，供所有授权用户访问。

- 对于单会话操作系统计算机，您可以在桌面体验页面上获得以下选项：
  - 用户每次登录时都连接到新的（随机）桌面。
  - 用户每次登录时都连接到同一（静态）桌面。

您可以进一步决定用户在注销后所做的更改是保存还是放弃。

**选择一张图片****注意：**

- 仅当您在计算机管理页面上选择 **Citrix Machine Creation Services (MCS)** 时，才会显示此页面。
- 此页面上的可用选项因虚拟机管理程序或云服务而异。

按照以下步骤完成页面上的设置：

1. 为计算机目录选择映像类型，然后选择映像。有两种类型的映像可用：

- 主映像：作为主映像创建的快照或 VM。在目录创建之初，它会自动进行映像准备。如果需要，您可以为所选映像添加注释。

**注意：**

1 - 在您使用 MCS 时，请勿在主映像上运行 Sysprep。

- 如果您指定主映像而非快照，管理界面将创建一个快照，但您无法对其进行命名。
- 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。
- 要更新图像节点内的图像，请在树中将其选中，然后单击右上角的“刷新”选项。如果您未选择任何图像节点，则单击“刷新”会更新树中的所有图像。要清除树中的选定节点，请按住 **CTRL** 键 然后单击该节点。

- 准备好的映像：经过映像准备的映像，可以直接用于虚拟机创建。选择准备好的映像而不是主映像来创建目录可确保更快、更可靠地创建计算机目录，并简化映像生命周期管理。



有关映像准备的更多信息，请参阅 [Machine Creation Services: 映像准备概述和故障排除](#)。

2. 要从计算机配置文件继承虚拟机设置，请选择“使用计算机配置文件”，然后选择用作计算机配置文件的 VM 或 ARM 模板规范（特定于 Azure）。

注意：

目前，使用计算机配置文件仅限于 Azure、AWS 和 GCP 虚拟机。

3. 为目录选择最低功能级别。要使用最新的产品功能，请确保主映像安装了最新的 VDA 版本。

## 配置计算机

注意：

- 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、虚拟机或计算机和用户。
- 如果您在“计算机类型”页面上选择“**Remote PC Access**”，则不会显示此页面。
- 您可以创建一个空目录，这意味着该目录中不包含任何计算机。
- 使用 **MCS** 创建计算机时：
  - 指定要创建的虚拟机数。如果您不想创建任何内容，请输入 **0**（零）。稍后，要为空目录创建虚拟机，可以执行 添加计算机。
  - 选择每个 VM 将具有的内存量（以 MB 为单位）。

重要提示：

创建的每个 VM 都有一个硬盘。硬盘的大小在主映像中进行设置；您不能在目录中更改硬盘大小。
  - 如果您在“桌面体验”页面上指明用户对静态桌面的更改应保存在单独的个人虚拟磁盘上，则以 GB 为单位指定虚拟磁盘大小和驱动器号。
  - 如果您的部署使用多个区域（资源位置），则可以为此目录选择一个区域。
  - 如果您要创建静态桌面虚拟机，请选择虚拟机复制模式。请参阅虚拟机复制模式。
  - 如果您要创建随机的非持久桌面虚拟机，则可以为此计算机上的临时数据启用和配置回写缓存，以提高 I/O 性能。有关详细信息，请参阅配置临时数据的缓存。
- 使用其他工具装备计算机时：

添加（或导入计算机帐户名列表）。添加或导入 VM 后，可以更改其帐户名。如果您在“桌面体验”页面上指定了静态计算机，则可以选择指定用于添加的每个 VM 的用户名。

提示：

要添加用户，您可以浏览到这些用户或手动输入以分号分隔的用户名列表。如果用户在 Active Directory

中，请直接输入名称。如果没有，请按以下格式输入名称：<identity provider>:<user name>。示例：AzureAD:username。

添加或导入姓名后，您可以使用“删除”按钮从列表中删除姓名，而您仍在此向导页面上。

- 使用其他工具（不是 **MCS**）时：

每个添加的（或导入的）计算机的图标和工具提示有助于确定那些可能不适合添加到目录，或可能无法通过 Cloud Connector 注册的计算机。

**虚拟机复制模式** 您在计算机页面上指定的复制模式决定了 MCS 是从主映像创建精简（快速复制）还是复制（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。

**配置用于临时数据的缓存** 使用 MCS 管理目录中的随机非持续计算机时，可以为计算机启用回写缓存以提高 I/O 性能。

回写缓存被称为 MCSIO。有关详细信息，请参阅 [这篇博客文章](#)。

**必备条件** 要启用回写缓存，目录必须满足以下要求：

- 使用指定临时数据存储空间的连接。有关详细信息，请参阅[连接和资源](#)。
- VDA 必须至少为 7.9 版本并安装最新的 MCSIO 驱动程序。

注意：

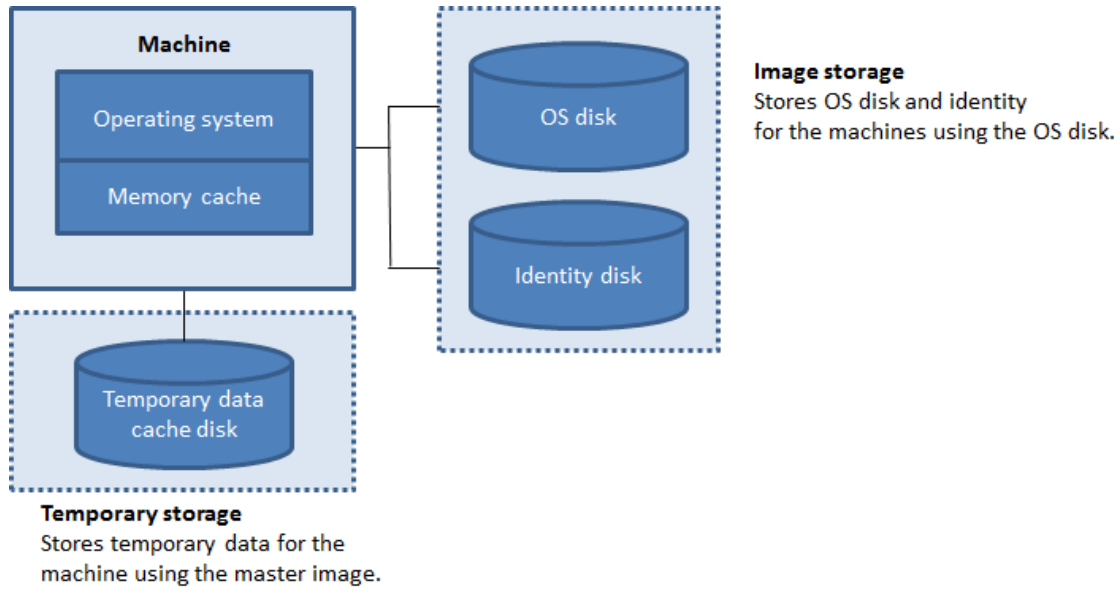
安装或升级 VDA 时可以选择安装此驱动程序。默认情况下，该驱动程序未安装。

- 要启用磁盘缓存的驱动器号分配，虚拟机必须满足以下额外要求：
  - 操作系统：Windows
  - VDA 版本：2305 或更高版本

#### 注意事项

- 回写式缓存位于内存缓存和磁盘缓存中。默认情况下，它们的默认值因连接类型而异。通常，默认值足以满足大多数情况的要求；但是，请考虑下列各项所需的空間：
  - 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。



- 如果启用“内存缓存大小 **(MB)** (推荐)”复选框，则临时数据最初会写入内存缓存。当内存缓存达到其配置限制时，最旧的数据将移至临时数据缓存磁盘。
- 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“内存缓存大小 **(MB)** (推荐)”复选框，请考虑增加每台计算机的内存总量。
- 如果保持“内存缓存大小 **(MB)** (推荐)”复选框处于清除状态，则使用最少的内存将临时数据直接写入磁盘缓存。
- 将 磁盘缓存大小 **(GB)** 更改为默认值会影响性能。此大小必须与用户需求以及计算机负载相匹配。

**重要提示：**

如果磁盘缓存空间已用完，则用户的会话将变得不可用。

如果清除“磁盘缓存大小”复选框，则不会创建任何缓存磁盘。在这种情况下，请指定分配给缓存的内存值，该值足以保留所有临时数据。此操作仅在可将大量 RAM 分配给每个 VM 时才可行。

如果清除这两个复选框，则不会缓存临时数据。这些数据会写入每个 VM 的其他磁盘（位于操作系统存储中）。（这是在早于 7.9 的版本中执行的预配操作）。

如果要使用此目录创建 AppDisk，请勿启用缓存。

在创建缓存值后，不能在计算机目录中更改此值。

**使用 CSV 文件批量添加计算机** 如果使用完整配置管理界面，则可以使用 CSV 文件批量添加计算机。该功能适用于除了通过 MCS 创建的目录之外的所有目录。

使用 CSV 文件批量添加计算机的常规工作流程如下：

1. 在计算机页面上，选择添加 **CSV** 文件。此时将显示批量添加计算机窗口。

2. 选择下载 **CSV** 模板。
3. 填写模板文件。
4. 拖动或浏览到该文件进行上载。
5. 选择验证可对您的导入执行验证检查。
6. 选择导入完成操作。

有关 CSV 文件注意事项的信息，请参阅[使用 CSV 文件添加计算机时的注意事项](#)。

您也可以在同一“计算机”页面上从目录中导出计算机。然后，在批量添加计算机时，可以将计算机的导出 CSV 用作模板。要导出计算机，请执行以下操作：

1. 在“计算机”页面上，选择“导出到 **CSV** 文件”。将下载包含计算机列表的 CSV 文件。
2. 打开 CSV 文件以根据需要添加或编辑计算机。要使用保存的 CSV 文件批量添加计算机，请参阅上一节 [使用 CSV 文件批量添加计算机](#)。

注意：

- 此功能不适用于“Remote PC Access”目录。
- 仅支持在相同类型的目录之间导出和导入 CSV 文件中的计算机。

## 为计算机配置 NIC

如果在“计算机类型”页面上选择“**Remote PC Access**”，则不会出现 **NIC** 页面。

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。

## 添加计算机帐户

注意：

只有在“计算机类型”页面上选择“**Remote PC Access**”时，才会显示此页面“计算机帐户”。

添加 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。

还可以使用 CSV 文件批量添加计算机。此操作的常规工作流程如下：

1. 在计算机帐户页面上，选择添加 **CSV** 文件。此时将显示批量添加计算机窗口。
2. 选择下载 **CSV** 模板。
3. 填写模板文件。
4. 拖动或浏览到该文件进行上载。

5. 选择验证可对您的导入执行验证检查。
6. 选择导入完成操作。

有关 CSV 文件注意事项的信息，请参阅[使用 CSV 文件添加计算机时的注意事项](#)。

为目录中的计算机配置身份

注意：

- 只有当您未在“计算机类型”页面上选择“**Remote PC Access**”，也没有在“计算机管理”页面上选择 **Citrix Machine Creation Services (MCS)** 时，才会显示“计算机身份”页面。

目录中的每台计算机必须具有唯一的标识。此页面允许您为目录中的计算机配置标识。在预配之后，这些计算机将加入到标识中。创建目录后无法更改标识类型。

在此页面上配置设置的一般工作流程如下：

1. 从列表中选择标识。
2. 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（域）。

您可以选择以下选项之一：

- 本地 **Active Directory**：由组织拥有并使用属于该组织的 Active Directory 帐户登录的计算机。它们存在于本地。

注意：

默认情况下，资源（连接）所在的域处于选中状态。

- 已加入 **Azure AD**：计算机归组织所有，使用属于该组织的 Azure Active Directory 帐户登录。它们只存在于云中。有关要求、限制和注意事项的信息，请参阅[已加入 Azure Active Directory](#)。

注意：

此选项要求主映像满足操作系统必备条件。有关详细信息，请参阅 Microsoft 文档[加入了 Microsoft Entra 的设备](#)。

- 已加入混合 **Azure Active Directory**。某个组织拥有并使用属于该组织的 Active Directory 域服务帐户登录的计算机。它们存在于云端和本地。有关要求、限制和注意事项的信息，请参阅[加入了混合 Azure Active Directory](#)。

注意：

- 在使用混合 Azure Active Directory 加入之前，请确保您的 Azure 环境满足必备条件。请参阅[配置 Microsoft Entra 混合加入](#)。

- 此选项要求主映像满足操作系统必备条件。有关详细信息，请参阅[已加入 Microsoft Entra 混合的设备](#)。

- 未加入域。未加入任何域的计算机。有关要求和限制的信息，请参阅[未加入域](#)。

重要提示：

- 如果选择本地 **Active Directory** 或已加入混合 **Azure Active Directory** 作为标识类型，则目录中的每台计算机都必须具有相应的 Active Directory 计算机帐户。
- 未加入域的标识类型需要 1811 或更高版本的 VDA 作为该目录的最低功能级别。要使其可用，请更新最低功能级别。
- 已加入 **Azure Active Directory** 和已加入混合 **Azure Active Directory** 的身份类型要求将 VDA 版本 2203 或更高版本作为目录的最低功能级别。要使其可用，请更新最低功能级别。

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。目录中的每台计算机必须具有唯一的名称。为要创建的计算机指定帐户命名方案。有关详细信息，请参阅[计算机帐户命名方案](#)。

注意：

确保 OU 名称不使用正斜杠 (/)。

如果您使用现有帐户，请浏览到这些帐户或单击“导入”并指定一个包含帐户名的 **.csv** 文件。导入的文件内容必须使用以下格式：**[ADComputerAccount] ADcomputeraccountname.domain**

确保所有要添加的计算机都有足够的帐户。“完整配置”界面管理这些帐户。因此，请允许界面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。

对于包含物理机或现有计算机的目录，选择或导入现有帐户，并将每台计算机同时分配给 Active Directory 计算机帐户和用户帐户。

**计算机帐户命名方案** 目录中的每台计算机必须具有唯一的名称。创建目录时，必须指定计算机帐户命名方案。使用通配符（哈希标记）作为名称中出现的连续数字或字母的占位符。

指定命名方案时，请考虑以下几点：

- 允许的最大字符数为 15。
- 命名方案必须包含至少一个通配符。必须将所有通配符放置在一起。
- 全名（包括通配符）必须至少包含 2 个但不超过 15 个字符。它必须至少包含一个非数字字符和一个 #（通配符）字符。
- 名称不得包含空格或以下任何字符：, ~ ! @ ' \$ % ^ & . ( ) } { \ / \* ? " < > | = + [ ] ; : \_ " .。
- 名称不能以连字符 (-) 结尾。
- 角色数量随着计算机帐户数量的增加而增加。例如，如果您使用“veryverylong#”架构创建 1,000 个计算机帐户，则最后创建的帐户名 (veryverylong1000) 包含 16 个字符，超过了允许的最大字符数。

您可以指明顺序值是数字 (0-9) 还是字母 (A-Z)。

- **0-9**. 如果选中，指定的通配符将解析为连续数字。

注意：

如果只有一个通配符 (#)，帐户名称将以 1 开头。如果有两个通配符，帐户名称将以 01 开头。如果有三个通配符，帐户名称将以 001 开头，依此类推。

- **A-Z**. 如果选中，指定的通配符将解析为连续字母。

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 等的帐户。

或者，您可以指定帐户名称的开头。

- 如果选择 **0-9**，则从指定的数字开始按顺序命名帐户。根据您在前面的字段中使用的通配符数量，输入一个或多个数字。例如，如果使用两个通配符，请输入两位或更多数字。
- 如果选择 **A-Z**，帐户将从指定的字母开始按顺序命名。输入一个或多个字母，具体取决于您在前面的字段中使用的通配符数量。例如，如果使用两个通配符，请输入两个或更多字母。

#### 添加域名凭据

选择“输入凭据”，然后输入有权在目标 Active Directory 域中执行帐户操作的管理员的凭据。

请使用检查名称选项检查用户名是否有效或唯一。例如，在以下情况下，该选项很有用：

- 多个域中存在相同的用户名。系统会提示您选择所需的用户。
- 您记不起域名。可以在不指定域名的情况下输入用户名。如果检查通过，则会自动填充域名。

注意：

如果您在计算机标识中选择的标识类型为已加入混合 **Azure Active Directory**，您输入的凭据必须已获得 **Write userCertificate** 权限。

#### 选择 **Workspace Environment Management** 配置集（可选）

仅当您使用 Citrix DaaS 的 Advanced 或 Premium 版本时，**WEM** 页面才会出现。

选择要将目录绑定到的 Workspace Environment Management (WEM) 配置集。配置集是用于组织一组 WEM 配置的逻辑容器。通过将目录绑定到配置集，您可以使用 WEM 为用户提供可能的最佳工作区体验。

重要提示：

- 必须先设置 WEM 服务部署，才能将目录绑定到配置集。登录 Citrix Cloud，然后启动 WEM 服务。有关详细信息，请参阅 [Workspace Environment Management 服务入门](#)。
- 如果您已经在使用 WEM，则您要置备的目录中的计算机可能已经存在于配置集中。例如，通过 Active Directory。在这种情况下，我们建议您始终使用 Active Directory 来执行配置并跳过此配置。

如果选定的配置集不包含与 WEM 的基本配置有关的设置，则会显示以下选项：

- 将基本设置应用到配置集。此选项允许您通过将基本设置应用到配置集来快速开始使用 WEM。基本设置包括 CPU 峰值保护、自动防止 CPU 峰值和智能 CPU 优化。要查看基本设置，请单击此处链接。要进行修改，请使用 WEM 控制台。

### 升级 VDA（可选）

#### 重要提示：

- 为确保平稳升级，在将 VDA 升级到 CR 或 LTSR CU 版本之前，请确保满足必备条件并查看已知问题。请参阅[使用完整配置界面升级 VDA](#)。
- 将 LTSR VDA 升级到 LTSR 累积更新 (CU) 版本时，请确保在 VDA 上运行的 VDA 升级代理版本为 7.36.0.7 或更高版本。有关详细信息，请参阅[使用完整配置界面升级 VDA](#)。

此功能适用于以下计算机类型：

- MCS 预配的持久性计算机。在目录创建过程中，您可以使用计算机管理页面上的 **Citrix Machine Creation Services** 进行部署。
- 不是使用 MCS 创建的计算机（例如，物理机）。在创建目录期间，您可以使用计算机管理页面上的其他服务或技术进行部署。

有关这两个选项的详细信息，请参阅计算机管理。

在“VDA 升级”页面上，选择要升级到的 VDA 版本。如果指定，则目录中安装了 VDA Upgrade Agent 的 VDA 可以立即升级到所选版本，也可以按计划时间升级。

#### 注意：

- 此功能仅支持升级到最新的 VDA。创建 VDA 升级计划或升级 VDA 的时间决定了 VDA 的最新版本。
- 配置 VDA 升级设置后，“VDA 升级”字段最多可能需要 15 分钟才能反映最新状态。要显示 VDA 升级列，请单击右上角的要显示的列图标，选择 计算机目录 > VDA 升级，然后单击 保存。

### 选择适合您部署的 VDA 路径：

#### 重要提示：

只要从早期版本切换到更高版本，就可以在 CR VDA 和 LTSR VDA 之间切换。您无法从更高版本切换到较早的版本，因为这被视为降级。例如，您无法从 2212 CR 降级到 2203 LTSR（任何 CU），但可以从 2112 CR 升级到 2203 LTSR（任何 CU）。

- 最新的 **CR VDA**。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。
- 最新的 **LTSR VDA**。对于希望长时间保持相同基本版本的大型企业生产环境，建议使用长期服务版本 (LTSR)。

创建目录后，您可以根据需要升级 VDA。有关详细信息，请参阅[升级 VDA](#)。

如果要稍后启用 VDA 升级，则可以在创建目录后通过编辑目录返回到此页面。有关详细信息，请参阅[通过编辑目录配置 VDA 升级设置](#)。



## 查看设置

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“完整配置”管理界面中。

完成后，选择完成以开始创建目录。

在计算机目录中，显示的新目录带有内联进度条。

要查看创建进度的详细信息，请执行以下操作：

1. 将鼠标悬停在计算机目录上。
2. 在出现的工具提示中，单击查看详细信息。

此时将出现分步操作进度图，您可以在其中看到以下内容：

- 步骤的历史记录
- 当前步骤的进度和运行时间
- 剩余步骤

## 使用 **PowerShell** 命令创建 **MCS** 计算机目录

您也可以使用 PowerShell 命令创建 MCS 计算机目录。有关详细信息，请参阅：

- [SDK 和 API](#)
- [使用 Remote PowerShell SDK 管理 Citrix DaaS](#)
- [创建目录](#)

## 为 **MCS I/O** 回写式缓存磁盘分配特定的驱动器号

您可以为 MCS I/O 回写式缓存磁盘分配特定的驱动器号。此实现可帮助您避免所使用的任何应用程序的驱动器盘符与 MCS I/O 回写缓存磁盘的驱动器盘符发生冲突。为此，可以使用 PowerShell 命令。支持的虚拟机管理程序是 Azure、GCP、VMware、SCVMM 和 XenServer。

注意：

此功能需要 VDA 版本 2305 或更高版本。

## 限制

- 仅适用于 Windows 操作系统
- 适用于回写缓存磁盘的驱动器盘符：[E](#) 到 [Z](#)
- 当 Azure 临时磁盘用作回写式缓存磁盘时不适用
- 仅在创建新的计算机目录时适用

为回写式缓存磁盘分配驱动器号 要为回写缓存磁盘分配驱动器盘符，请执行以下操作：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*`。
3. 创建标识池（如果尚未创建）。有关信息，请参阅[创建目录](#)。
4. 使用带有属性 `WriteBackCacheDriveLetter` 的命令 `New-ProvScheme` 创建预配方案。例如：

```

1 New-ProvScheme -CleanOnBoot `
2 -HostingUnitName "<name>" `
3 -IdentityPoolName $schemeName `
4 -ProvisioningSchemeName $schemeName `
5 -InitialBatchSizeHint 1 `
6 -UseWriteBackCache -WriteBackCacheDiskSize 127 -
   WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `
7 -MasterImageVM "XDHyp:\HostingUnits<name>\image.folder\abcd-
   resources.resourcegroup\
   MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxxx2130aa145ec77.
   manageddisk" `
8 -NetworkMapping @{
9   "0"="XDHyp:\HostingUnits\name\virtualprivatecloud.folder\East US.
   region\virtualprivatecloud.folder\abcd-resources.resourcegroup
   \abcd-resources-vnet.virtualprivatecloud\default.network" }
10 `
11 -ServiceOffering "XDHyp:\HostingUnits\<name>\serviceoffering.
   folder\Standard_D2s_v5.serviceoffering" `
12 -CustomProperties '<CustomProperties xmlns="http://schemas.citrix.
   com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
13   <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
   true" />
14   <Property xsi:type="StringProperty" Name="OsType" Value="Windows"
   />
15   <Property xsi:type="StringProperty" Name="StorageType" Value="
   Premium_LRS"/>
16   <Property xsi:type="StringProperty" Name="PersistWBC" Value="false
   " />
17   <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="
   false" />
18   <Property xsi:type="StringProperty" Name="PersistVm" Value="false"
   />
19   <Property xsi:type="StringProperty" Name="WBCDiskStorageType"
   Value="Premium_LRS" />
20   <Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value
   ="false" />
21   <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   abcd-group1" />
22   <Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client" />
23   <Property xsi:type="StringProperty" Name="SchemaVersion" Value="2"
   />
24 </CustomProperties>'

```

```
25 <!--NeedCopy-->
```

5. 完成目录的创建。

关于设置自定义属性的重要注意事项

必须在 GCP 和 Azure 环境中的 `New-ProvScheme` 和 `Set-ProvScheme` 处正确设置自定义属性。如果您指定了一个或多个不存在的自定义属性，则会收到以下错误消息，并且命令无法运行。

`Invalid property found: <invalid property>. Ensure that the CustomProperties parameter supports the property.`

关于设置 **ProvScheme** 参数的重要注意事项

使用 MCS 创建目录时，如果出现以下情况，则会出现错误：

- 创建计算机目录时，在不受支持的虚拟机管理程序中设置以下 `New-ProvScheme` 参数：

参数	受支持的虚拟机管理程序
<code>UseWriteBackCache</code>	VMware
	Hyper-V
	XenServer
	Azure
	GCP
<code>DedicatedTenancy</code>	Azure
	GCP
	AWS
<code>TenancyType</code>	Azure
	GCP
	AWS
<code>UseFullDiskCloneProvisioning</code>	VMware
	Hyper-V
	XenServer

- 创建计算机目录后，请更新以下 `Set-ProvScheme` 参数：

- `CleanOnBoot`
- `UseWriteBackCache`
- `DedicatedTenancy`
- `TenancyType`
- `UseFullDiskCloneProvisioning`

在创建虚拟机时添加 **SID**

在创建新虚拟机时，您可以添加参数 `ADAccountSid` 以唯一地标识计算机。

为此，您需要：

1. 使用支持的身份类型创建目录。
2. 使用 `NewProvVM` 将计算机添加到目录中。例如：

```
1 New-ProvVM -ProvisioningSchemeName "name" -ADAccountSid @"SID "  
   ) -RunAsynchronously  
2 <!--NeedCopy-->
```

但是，您不能为计算机预配以下对象：

- 不在目录标识池中的 AD 帐户
- 未处于可用状态的 AD 帐户

在创建 **MCS** 计算机目录之前验证配置

您可以使用 `New-ProvScheme` 命令中的参数 `-validate` 在创建 MCS 计算机目录之前验证配置设置。使用该参数运行此 PowerShell 命令后，如果使用了错误的参数或某个参数与其他参数发生冲突，则会收到相应的错误消息。然后，您可以使用错误消息来解决问题，并使用 PowerShell 成功创建 MCS 计算机目录。目前，此功能适用于 Azure、GCP 和 VMware 虚拟化环境。

注意：

验证时，不得创建实际的 MCS 计算机目录。必须使用命令的结果来修复错误，然后成功创建目录。因此，在运行 `New-ProvScheme` 命令时，使用虚假的身份池名称。

要验证配置，请执行以下步骤：

1. 从 Delivery Controller 主机上打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 运行 `New-ProvScheme` 命令并使用参数 `-validate`。提供虚假的身份池名称以使该命令生效。例如，

```

1 $result =New-ProvScheme -CleanOnBoot -HostingUnitName "vSanRg" -
  IdentityPoolName "mptmpcatalogdemo" -InitialBatchSizeHint 1 -
  MasterImageVM "XDHyp:\HostingUnits\vSanRg\Windows19MasterImage.
  vm\Citrix_XD_NonMachineProfileWin19Machines.snapshot" -
  NetworkMapping @{
2   "0"="XDHyp:\HostingUnits\vSanRg\VM Network.network" }
3   -ProvisioningSchemeName "MachineProfileW10Machines" -Scope @()
4   -VMCpuCount 2 -VM
5   MemoryMB 6143 -MachineProfile "XDHyp:\HostingUnits\vSanRg\TRW-
  Win11-tpm-BL-TEMPLATE.template" -TenancyType Shared -
  FunctionalLevel "L7_20" -Validate
6 $result.TerminatingError | Format-List -Property *
7 <!--NeedCopy-->

```

错误消息：

```

1 ErrorData      : {
2   [[ValidationFailureCount, xxx], [InvalidMemoryValue, The memory
  size provided 6143 must be a multiple of 4 MB and must be
  greater than or equal to 4 MB.], [InconsistentGuestOsSetting,
  The GuestOs setting - windows9_64Guest of the selected machine
  profile does not match with the setting -
  windows2019srv_64Guest of master image. Please select a
  machine profile that matches the GuestOs setting of the master
  image.], [InconsistentVtpmSetting, The vTPM setting of the
  selected machine profile does not match with the selected
  master image. Please select a machine profile that matches the
  vTPM setting of the master image.], [
  InconsistentFirmwareSetting, The firmware setting - efi of the
  selected machine profile does not match with the setting -
  bios of master image. Please select a machine profile that
  matches the firmware setting of the master image ErrorId
  : ValidationFailure
3 ErrorMessage   : ValidationFailure
4 Operation      : ValidatingInputs
5 <!--NeedCopy-->

```

4. 验证配置设置后，您可以创建具有真实身份池名称和正确参数的 MCS 计算机目录。

下一步的去向

有关创建特定虚拟机管理程序目录的信息，请参阅：

- [创建 AWS 目录](#)
- [创建 Google 云端平台目录](#)
- [创建 Microsoft Azure 目录](#)
- [创建 Microsoft System Center Virtual Machine Manager 目录](#)
- [创建 Nutanix 目录](#)
- [创建 VMware 目录](#)

- [创建 XenServer 目录](#)

如果这是创建的第一个目录，系统将引导您[创建交付组](#)。

要查看整个配置过程，请参阅[规划和构建部署](#)。

您可以使用完整配置界面和 PowerShell 创建 Citrix Provisioning 目录。

此实现为您提供了以下优点：

- 用于管理 MCS 和 Citrix Provisioning 目录的单一统一控制台。
- 为 Citrix Provisioning 目录提供新功能，例如身份管理解决方案、按需预配等。

目前，此功能仅适用于 Azure 工作负载。有关详细信息，请参阅在 [Citrix Studio 中创建 Citrix Provisioning 目录](#)。

#### 更多信息

- [Citrix Virtual Apps and Desktops 映像管理](#)
- [创建和管理连接和资源](#)
- [创建已加入目录的计算机身份](#)
- [管理计算机目录](#)

## 创建 **AWS** 目录

March 5, 2024

[创建计算机目录](#)介绍了用于创建计算机目录的向导。以下信息涵盖了特定于 AWS 虚拟化环境的详细信息。

#### 注意：

在创建 AWS 目录之前，您需要完成创建与 AWS 的连接。请参阅[与 AWS 的连接](#)。

#### 映像准备期间的网络设置

在映像准备期间，将在原始 VM 的基础上创建准备虚拟机 (VM)。此准备 VM 已与网络断开连接。为了断开网络与准备 VM 的连接，需要创建一个网络安全组以拒绝所有入站和出站流量。此网络安全组会持续存在并可重复使用。网络安全组的名称为 `Citrix.XenDesktop.IsolationGroup-GUID`，其中 GUID 是随机生成的。

#### **AWS** 租赁

AWS 提供以下租赁选项：共享租赁（默认类型）和专用租赁。共享租赁意味着来自不同客户的多个 Amazon EC2 实例可能位于同一个物理硬件上。专用租赁意味着您的 EC2 实例仅与已部署的其他实例一起在硬件上运行。其他客户不使用同一个硬件。

可以使用完整配置界面或 PowerShell 通过 MCS 预配 AWS 专用主机。

向 **AWS** 主机进行配置的要求

- 导入的 BYOL（自带许可）映像 (AMI)。通过专用主机，使用并管理您的现有许可证。
- 分配了具有足够利用率的专用主机，可满足预配请求。
- 启用自动放置。

使用“完整配置”界面配置 **AWS** 专用主机租赁

使用 MCS 创建用于在 AWS 中预配计算机的目录时，计算机目录设置 > 安全页面提供了以下选项：

- 使用共享硬件。此设置适合大多数部署。多个客户共享几个硬件，即使他们之间没有互动亦如此。使用共享硬件是运行 Amazon EC2 实例的最便宜的选择。
- 使用专用主机。Amazon EC2 专用主机是具有完全专用的 EC2 实例容量的物理服务器，允许您按套接字或 VM 使用现有软件许可证。专用主机具有基于实例类型的预设利用率。例如，针对 C4 大型实例类型分配的一个专用主机最多运行 16 个实例。请参阅 [AWS 站点](#) 以了解详细信息。
- 使用专用实例。此设置更适合具有特定安全性或合规性要求的部署。使用专用实例，您仍然可以享受将主机与其他 AWS 客户分开的好处，但无需为整个主机付费。您无需担心主机的容量，但需要为实例支付更高的费率。

此设置适用于需要您使用专用主机的许可限制或安全要求的部署。使用专用主机，您可以拥有整个物理主机，并按小时计费。拥有该主机可让您在该主机允许的情况下启动尽可能多的 EC2 实例，而无需支付额外的费用。

注意：

如果没有正在进行的目录创建或映像更新任务，则可以删除任何可用的准备身份磁盘。

使用 **PowerShell** 配置 **AWS** 专用主机租赁

或者，您可以通过 PowerShell 预配 AWS 专用主机。使用参数 `TenancyType` 设置为 `Host` 的 `New-ProvScheme` cmdlet。请参阅 [Citrix 开发人员文档](#) 以了解详细信息。

捕获 **AWS** 实例属性

当您在 AWS 中创建目录以使用 Machine Creation Services (MCS) 预配计算机时，您可以选择一个 AMI 来表示该目录的主映像。在该 AMI 中，MCS 使用磁盘的快照。

提示：

您必须拥有与 AMI 关联的 VM，才能使用 AWS 实例属性捕获功能。

**MCS** 从获取 **AMI** 的实例中读取属性，并将计算机的身份访问管理 (IAM) 角色和标签应用于为给定目录配置的计算机。使用此可选功能时，目录创建过程会查找选定的 AMI 源实例，读取一组有限的属性。然后，这些属性将存储在 AWS 启动模板中，该模板用于为该目录预配计算机。目录中的任何计算机都会继承捕获的实例属性。

捕获的属性包括：

- IAM 角色：适用于预置实例。
- 标签：应用于预置的实例、其磁盘和 NIC。这些标记应用到临时 Citrix 资源，包括：S3 存储桶和对象、AMI、快照和启动模板。

提示：

临时 Citrix 资源的标记是可选的，可使用自定义属性 `AwsOperationalResourcesTagging` 进行配置。要成功应用标记并创建带有操作资源标记的 AWS 目录，请不要删除用于创建 AMI 映像的 EC2 实例。

### 捕获 **AWS** 实例属性

在为 AWS 托管连接创建预配方案时，可以通过指定自定义属性 `AwsCaptureInstanceProperties` 来使用此功能：

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true"  
...<standard provscheme parameters
```

请参阅 [Citrix 开发人员文档](#) 以了解详细信息。

注意：

`AwsCaptureInstanceProperties` 已被弃用。

### 标记 **AWS** 运行资源

Amazon Machine Image (AMI) 表示用于在 Amazon 云环境中创建虚拟机的一种虚拟设备，通常称为 EC2。可以使用 AMI 部署使用 EC2 环境的服务。创建目录以使用适用于 AWS 的 MCS 预配计算机时，可以选择 **AMI** 作为该目录的黄金映像。

重要提示：

使用运行资源标记需要通过捕获实例属性和启动模板来创建目录。

要创建 AWS 目录，必须首先为希望成为黄金映像的实例创建 AMI。MCS 从该实例读取标记并将其合并到启动模板中。然后，启动模板标记将应用于在 AWS 环境中创建的所有 Citrix 资源，包括：

- 虚拟机
- VM 磁盘
- VM 网络接口
- S3 存储桶



- S3 对象
- 启动模板
- AMI

在“完整配置”界面中应用 **AWS** 实例属性并标记操作资源

在创建目录以使用 MCS 在 AWS 中预配计算机时，可以控制是否将 IAM 角色和标记属性应用到这些计算机。还可以控制是否将计算机标记应用到运行资源。您有以下两个选项：

Machine Catalog Setup

Machine Type

Machine Management

Machine Template

Virtual Machines

Security

NICs

Machine Identities

Domain Credentials

Scopes

WEM (Optional)

Summary

Machine Template

Select the machine template that the virtual machines will be based upon.

Name ↓	Description
<input type="radio"/> Bastion-06082015-1609 (ami-837893e8)	Bastion dated 06/08/2015 at 16:09
<input type="radio"/> Bastion-Onpremises-testing-v1 (ami-f80d6...)	CDF control added, xdttesting.net certs added
<input type="radio"/> Bastion-Onpremises-testing-v2 (ami-c40b7...)	Added License and updated Netscaler_Confi...
<input type="radio"/> Bastion-Onpremises-testing-v3 (ami-047a...)	Fixing License updating script
<input type="radio"/> Bastion-RingDot5-V1 (ami-f259cf9a)	Replaced Lib and NS file from prev version
<input type="radio"/> Bastion-RingDot5-V2 (ami-380f9950)	Making correction in configure script
<input type="radio"/> Bastion-RingDot5-V3 (ami-f61a8b9e)	Removed DomainC LB Server
<input type="radio"/> Bastion-RingDot5-V4 (ami-825cc4ea)	New Windows Instance with NSCERT for Xe...
<input type="radio"/> Bastion-RingDot5-V5 (ami-663ba30e)	Added Certs for prod, test and staging. Adde...
<input type="radio"/> Bastion-RingDot6-V1 (ami-14e9917c)	Added BYOL changes
<input type="radio"/> Bastion-RZ-v4 (ami-443e192c)	The Bastion AMI used for AWS RZ creation
<input type="radio"/> Before Cloud Broker (ami-0e60fb66)	Image before testing the cloud broker on a s...
<input type="radio"/> CentOS Linux 7 x86_64 HVM EBS ENA 18...	CentOS Linux 7 x86_64 HVM EBS ENA 1803...
<input type="radio"/> CentOS Linux 7 x86_64 HVM EBS ENA 18...	CentOS Linux 7 x86_64 HVM EBS ENA 1804...
<input type="radio"/> CentOS Linux 7 x86_64 HVM EBS ENA 19...	CentOS Linux 7 x86_64 HVM EBS ENA 1901...

Select the minimum functional level for this catalog: 1811 (or later)

To register with delivery groups that reference this catalog, machines require the selected version of the VDA or later. [Learn more](#)

☒ Apply machine template properties to virtual machines

☐ Apply machine tags to operational resources

Back

Next

Cancel

- 将计算机模板属性应用到虚拟机
  - 控制是否将与所选计算机模板关联的 IAM 角色和标记属性应用到此目录中的虚拟机。
- 将计算机标记应用到运行资源
  - 控制是否将计算机标记应用到在 AWS 环境中创建的每个项目，以便于预配计算机。运行资源是作为目录创建的副产品创建的。它们包括临时资源和永久性资源，例如准备 VM 实例和 AMI。

## 使用 **PowerShell** 标记操作资源

要使用 PowerShell 标记资源，请执行以下操作：

1. 从 DDC 主机打开 PowerShell 窗口。
2. 运行命令 `asnp citrix` 以加载 Citrix 特定的 PowerShell 模块。

要为已配置的虚拟机标记资源，请使用自定义属性 `AwsOperationalResourcesTagging`。此属性的语法为：

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,  
true; AwsOperationalResourcesTagging,true" ...<standard provscheme  
parameters>
```

## 使用 **PowerShell** 创建基于计算机配置文件的计算机目录

您可以使用计算机配置文件从 EC2 实例 (VM) 捕获硬件属性，或者启动模板版本并将其应用于已配置的计算机。例如，捕获的属性可以包括 EBS 卷属性、实例类型、EBS 优化和其他支持的 AWS 配置。

您可以使用 AWS EC2 实例 (VM) 或 AWS 启动模板版本作为计算机配置文件输入。

注意：

EBS 卷属性仅源自计算机配置文件。

## 重要注意事项

创建 MCS 计算机目录时的重要注意事项：

- 如果您在 `New-ProvScheme` 和 `Set-ProvScheme` 命令中添加计算机硬件属性参数，则参数中提供的值将覆盖计算机配置文件中的值。
- 如果您将 `AwsCaptureInstanceProperties` 设置为 **true**，但未设置 `MachineProfile` 属性，则仅捕获 IAM 角色和标记。
- 您不能同时设置 `AwsCaptureInstanceProperties` 和 `MachineProfile`。

\*\* 注意：

`AwsCaptureInstanceProperties` 已被弃用。

- 必须明确提供以下属性的值：
  - `TenancyType`
  - 安全组
  - ENI 或虚拟网络

- 仅当启用了 `AwsCaptureInstanceProperties` 或者指定了计算机配置文件时才能启用 `AwsOperationalResourcesTagging`。

创建 MCS 计算机目录后的重要考虑因素是：

- 您无法将目录从基于计算机配置文件的目录更改为基于非计算机配置文件的目录。

使用计算机配置文件创建计算机目录

要使用计算机配置文件创建计算机目录，请执行以下操作：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 创建标识池（如果尚未创建）。例如，

```
1 New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
  Domain abcdf -NamingSchemeType Numeric
2 <!--NeedCopy-->
```

4. 运行 `New-ProvScheme` 命令。例如：

```
1 New-ProvScheme -ProvisioningSchemeName demet-test-1
2 -HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1
3 -IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4
4 -CleanOnBoot
5 -MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-
  demet-ami.0 (ami-0ca813xxxxxx061ef).template'
6 -MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-east-
  1a.availabilityzone\machine-profile-instance i (i-0xxxxxxx).
  vm'
7 <!--NeedCopy-->
```

5. 完成目录的创建。有关详细信息，请参阅[创建目录](#)。

更新计算机配置文件

要更新最初使用计算机配置文件置备的目录上的计算机配置文件，请执行以下操作：

1. 运行 `Set-ProvScheme` 命令。例如，

```
1 Set-ProvScheme `
2 -ProvisioningSchemeUid "<ID" `
3 -MachineProfile "XDHyp:\HostingUnits\abc\us-east-1a.
  availabilityzone\citrix-cvad-machineprofile-instance (i-0
  xxxxxxxx).vm"
4 <!--NeedCopy-->
```

## 使用 **PowerShell** 创建包含启动模板版本的目录

您可以使用启动模板版本作为计算机配置文件输入来创建 MCS 计算机目录。还可以将计算机配置文件目录的输入从 VM 更新为启动模板版本，以及从启动模板版本更新到 VM。

在 AWS EC2 控制台上，您可以提供启动模板的实例配置信息以及版本号。当您在创建或更新计算机目录时将启动模板版本指定为计算机配置文件输入时，该启动模板版本中的属性将复制到已预配的 VDA VM 中。

以下属性可以使用计算机配置文件输入来提供，也可以在 **New-ProvScheme** 或 **Set-ProvScheme** 命令中作为参数明确提供。如果这些属性是在 **New-ProvScheme** 或 **Set-ProvScheme** 命令中提供的，它们将优先于这些属性的计算机配置文件值。

- 服务方案
- 网络
- 安全组
- 租赁类型

### 注意：

如果未在计算机配置文件启动模板中提供服务产品，也未将其作为 **New-ProvScheme** 命令中的参数提供，则会出现相应的错误。

要使用启动模板版本作为计算机配置文件输入来创建目录，请执行以下操作：

1. 打开 **PowerShell** 窗口。
2. 运行 **asnp citrix\*** 以加载 Citrix 特定的 PowerShell 模块。
3. 获取启动模板的启动模板版本列表。例如：

```
1 XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate>
   ls | Select FullPath
2 <!--NeedCopy-->
```

4. 创建标识池（如果未创建）。例如：

```
1 New-AcctIdentityPool `
2 -IdentityPoolName "abc11" `
3 -NamingScheme "abc1-##" `
4 -NamingSchemeType Numeric `
5 -Domain "citrix-xxxxxx.local" `
6 -ZoneUid "xxxxxxxx" `
7 <!--NeedCopy-->
```

5. 使用启动模板版本作为计算机配置文件输入来创建预配方案。例如：

```
1 New-ProvScheme `
2 -ProvisioningSchemeName "MPLT1" `
3 -HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `
4 -IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxxx" `
```

```

5 -MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-
  persistent-vda-win2022 (ami-0axxxxxxxxxxx).template" `
6 -CleanOnBoot `
7 -MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
  (lt-01xxxx).launchtemplate\lt-01xxxx (1).
  launchtemplateversion"
8 <!--NeedCopy-->

```

还可以覆盖服务产品、安全组、租赁和网络等参数。例如：

```

1 New-ProvScheme `
2 -ProvisioningSchemeName "MPLT1" `
3 -HostingUnitUid " c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `
4 -IdentityPoolUid " bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxxx" `
5 -MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-
  persistent-vda-win2022 (ami-0axxxxxxxxxxx).template" `
6 -CleanOnBoot `
7 -MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
  (lt-01xxxx).launchtemplate\lt-01xxxx (1).launchtemplateversion"
8 -ServiceOffering "XDHyp:\HostingUnits\xxxd-ue1a\T3 Large Instance.
  serviceoffering"
9 <!--NeedCopy-->

```

6. 将供应方案注册为经纪人目录。例如：

```

1 New-BrokerCatalog -Name "MPLT1" `
2 -AllocationType Random `
3 -Description "Machine profile catalog" `
4 -ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxxx `
5 -ProvisioningType Mcs `
6 -SessionSupport MultiSession `
7 -PersistUserChanges Discard
8 <!--NeedCopy-->

```

7. 完成目录的创建。有关详细信息，请参阅[创建目录](#)。

## 更新计算机配置文件源

还可以将计算机配置文件目录的输入从 VM 更新为启动模板版本，以及从启动模板版本更新到 VM。例如：

- 要将计算机配置文件目录的输入从 VM 更新为启动模板版本，请执行以下操作：

```

1 Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
2 -MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
  (lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxxx (1).
  launchtemplateversion"
3 <!--NeedCopy-->

```

- 要将计算机配置文件目录的输入从启动模板版本更新为 VM，请执行以下操作：

```
1 Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
2 -MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-east-1a.
   availabilityzone\apollo-non-persistent-vda-win2022-2 (i-08
   xxxxxxxxx).vm"
3 <!--NeedCopy-->
```

## 复制 VM 上的标记

可以将计算机配置文件中指定的 NIC 和磁盘（身份磁盘、回写式缓存磁盘和操作系统磁盘）上的标记复制到 MCS 计算机目录中新创建的 VM。可以在任何计算机配置文件源（AWS VM 实例或 AWS 启动模板版本）中指定这些标记。此功能适用于永久计算机目录和非永久计算机目录和 VM。

### 注意：

- 在 AWS EC2 控制台上，您无法在启动模板版本资源标签下看到标签网络接口值。但是，您可以运行 PowerShell 命令 `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` 来查看标记规范。
- 如果计算机配置文件源（VM 或启动模板版本）有两个网络接口（eni-1 和 eni-2），并且 eni-1 的标记为 t1，eni-2 的标记为 t2，则 VM 将获得这两个网络接口的标记。

## 使用 PowerShell 筛选虚拟机实例

您用作计算机配置文件 VM 的 AWS 虚拟机实例必须兼容计算机目录才能正常创建和运行。要列出可用作计算机配置文件输入虚拟机的 AWS 虚拟机实例，您可以使用 `Get-HypInventoryItem` 命令。该命令可以分页和筛选托管单元上可用的虚拟机清单。

分页：

**Get-HypInventoryItem** 支持两种分页模式：

- 分页模式使用 `-MaxRecords` 和 `-Skip` 参数返回项目集：
  - `-MaxRecords`：默认值为 **1**。此参数控制要退回的项目数量。
  - `-Skip`：默认值为 **0**。此参数控制从虚拟机管理程序中的列表的绝对开头（或绝对结尾）跳过的项目数量。
- 滚动模式使用 `-MaxRecords`、`-ForwardDirection` 和 `-ContinuationToken` 参数来允许滚动记录：
  - `-ForwardDirection`：默认值为 **True**。此参数与 `-MaxRecords` 一起使用，以返回下一组匹配记录或前一组匹配记录。
  - `-ContinuationToken`：返回紧随其后（如果 `ForwardDirection` 设置为 **false**，则在其前面）的项目，但不包括 `ContinuationToken` 中给出的项目。

分页示例：

- 返回名称排在最后的计算机模板的单条记录。AdditionalData 字段包括 TotalItemsCount 和 TotalFilteredItemsCount:

```
1 Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
   -ResourceType template
2 <!--NeedCopy-->
```

- 要返回名称排在最后的计算机模板的 10 条记录，请执行以下操作：

```
1 Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
   -ResourceType template -MaxRecords 10 | select Name
2 <!--NeedCopy-->
```

- 要返回以排在最前面的名称结尾的记录数组，请执行以下操作：

```
1 Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
   -ResourceType template -ForwardDirection $False -MaxRecords 10
   | select Name
2 <!--NeedCopy-->
```

- 要返回从与给定 ContinuationToken 关联的计算机模板开始的记录数组，请执行以下操作：

```
1 Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
   -ResourceType template -ContinuationToken "ami-07xxxxxxxxxx" -
   MaxRecords 10
2 <!--NeedCopy-->
```

#### 筛选：

筛选功能支持以下其他可选参数。可以将这些参数与分页选项结合使用。

- **-ContainsName "my\_name"**：如果给定字符串与 AMI 名称的一部分相匹配，则 AMI 将包含在 Get 结果中。例如：

```
1 Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
   -ResourceType template -MaxRecords 100 -ContainName 'apollo'
   | select Name
2 <!--NeedCopy-->
```

- **-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" } '**：如果 AMI 至少具有其中一个标记，Get 该标记将包含在结果中。例如：

```
1 Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
   -ResourceType template -MaxRecords 100 -Tags '{
2 "opex owner": "Not tagged" }
3 ' | select Name
4 <!--NeedCopy-->
```

注意：

支持两个标记值。未标记的标记值匹配标记列表中没有给定标记的项目。无论标记的值为何，所有值标记

值都会匹配具有该标记的项目。否则，仅当项目带标记且值等于过滤器中给出的值时才会进行匹配。

- `-Id "ami-0a2d913927e0352f3"`: 如果 AMI 与给定的 ID 相匹配，则会将其包含在 `Get` 结果中。
- 例如：

```
1 Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
  -ResourceType template -Id ami-xxxxxxxxxxxxx
2 <!--NeedCopy-->
```

根据 **AdditionalData** 参数进行筛选：

**AdditionalData** 筛选参数根据模板或 VM 的功能、服务产品或 **AdditionalData** 中的任何属性列出模板或 VM。

例如：

```
1 (Get-HypInventoryItem -ResourceType "launchtemplateversion" -
  LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200).
  AdditionalData
2 <!--NeedCopy-->
```

也可以添加一个 `-Warn` 参数来指明不兼容的 VM。VM 中包含一个名为警告的 **AdditionalData** 字段。例如：

```
1 (Get-HypInventoryItem -ResourceType "launchtemplateversion" -
  LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami
  -015xxxxxxxxxx" -Warn $true).AdditionalData
2 <!--NeedCopy-->
```

下一步的去向

- 如果这是创建的第一个目录，系统将引导您[创建交付组](#)。
- 要查看整个配置过程，请参阅[规划和构建部署](#)。
- 要管理目录，请参阅[管理计算机目录](#)和[管理 AWS 目录](#)。

更多信息

- [创建和管理连接和资源](#)
- [与 AWS 的连接](#)
- [创建计算机目录](#)

## 创建 Google 云端平台目录

February 9, 2024

[创建计算机目录](#)介绍了用于创建计算机目录的向导。以下信息涵盖了特定于 Google Cloud 环境的详细信息。



注意：

在创建 Google 云端平台 (GCP) 目录之前，您需要完成创建与 GCP 的连接。请参阅[与 Google Cloud 环境的连接](#)。

## 准备主 VM 实例和永久磁盘

提示：

永久磁盘是虚拟磁盘的 Google Cloud 术语。

要准备主 VM 实例，请使用与您计划的计算机目录中克隆的 VDA 实例所需的配置匹配的属性创建和配置 VM 实例。配置不仅适用于实例大小和类型。它还包括实例属性，例如元数据、标记、GPU 分配、网络标记和服务帐户属性。

作为控制过程的一部分，MCS 使用您的主 VM 实例创建 Google Cloud 实例模板。然后，实例模板将用于创建组成计算机目录的克隆 VDA 实例。克隆的实例继承创建实例模板的所基于的主 VM 实例的属性（VPC、子网和永久磁盘属性除外）。

根据具体情况配置主 VM 实例的属性后，启动实例，然后为实例准备永久磁盘。

我们建议您手动创建磁盘的快照。这样做可以使用有意义的命名约定来跟踪版本，为您提供更多选项来管理早期版本的主映像，并节省创建计算机目录的时间。如果您不创建自己的快照，MCS 会为您创建一个临时快照（在预配过程结束时删除该快照）。

## 启用区域选择

Citrix DaaS 支持区域选择。通过区域选择，您可以指定要在其中创建 VM 的区域。通过区域选择，管理员可以在其选择的区域之间放置唯一的租户节点。必须在 Google Cloud 上完成以下操作，才能配置唯一租赁：

- 保留 Google Cloud 唯一租户节点
- 创建 VDA 主映像

## 保留 Google Cloud 唯一租户节点

要预留单租户节点，请参阅 [Google Cloud 文档](#)。

重要提示：

节点模板用于指示节点组中预留的系统的性能特征。这些特征包括 vGPU 的数量、分配给节点的内存量以及用于在节点上创建的计算机的计算机类型。有关详细信息，请参阅 [Google Cloud 文档](#)。

## 创建 VDA 主映像

要在唯一租户节点上成功部署计算机，您需要在创建主 VM 映像时执行额外的步骤。Google Cloud 上的计算机实例具有名为节点关联性标签的属性。用作部署到唯一租户节点的目录的主映像的实例需要一个与目标节点组名称匹配的节点关联性标签。为实现这一目标，请记住以下几点：

- 对于新实例，请在创建实例时在 Google Cloud 控制台中设置标签。有关详细信息，请参阅[创建实例时设置节点关联性标签](#)。
- 对于现有实例，请使用 **gcloud** 命令行设置标签。有关详细信息，请参阅[为现有实例设置节点关联性标签](#)。

### 注意：

如果您打算将唯一租赁与共享 VPC 结合使用，请参阅[共享虚拟私有云](#)。

**创建实例时设置节点关联性标签** 要设置节点关联性标签，请执行以下操作：

1. 在 Google Cloud 控制台中，导航到 **Compute Engine**（计算引擎）> **VM instances**（VM 实例）。
2. 在 **VM instances**（VM 实例）页面上，选择 **Create instance**（创建实例）。
3. 在 **Instance creation**（实例创建）页面上，键入或配置所需的信息，然后选择 **management, security, disks, networking, sole tenancy**（管理、安全性、磁盘、网络连接、唯一租户）以打开设置面板。
4. 在 **Sole tenancy**（唯一租赁）选项卡上，选择 **Browse**（浏览）以查看当前项目中的可用节点组。此时将显示 **Sole-tenant node**（唯一租户节点）页面，其中显示可用节点组的列表。
5. 在 **Sole-tenant node**（唯一租户节点）页面上，从列表中选择适用的节点组，然后选择 **Select**（选择）以返回到 **Sole tenancy**（唯一租赁）选项卡。节点关联性标签字段将使用您选择的信息进行填充。此设置可确保从实例创建的计算机目录将部署到选定的节点组。
6. 选择创建以创建实例。

**为现有实例设置节点关联性标签** 要设置节点关联性标签，请执行以下操作：

1. 在 Google Cloud Shell 终端窗口中，使用 `gcloud compute instances` 命令设置节点关联性标签。在 **gcloud** 命令中包含以下信息：
  - **VM** 的名称。例如，使用名为 `s*2019-vda-base` 的现有 VM。\*
  - 节点组的名称。使用之前创建的节点组名称。例如，`mh-sole-tenant-node-group-1`。
  - 实例所在的区域。例如，VM 位于 `*us-east-1b*` `zone` 中。

例如，在终端窗口中键入以下命令：

- `gcloud compute instances set-scheduling "s2019-vda-base"--node-group="mh-sole-tenant-node-group-1"--zone="us-east1-b"`

有关 `gcloud compute instances` 命令的详细信息，请参阅 Google 开发人员工具文档，网址为 <https://cloud.google.com/sdk/gcloud/reference/beta/compute/instances/set-scheduling>。

2. 导航到实例的 **VM instance details**（VM 实例详细信息）页面，并验证 **Node Affinities**（节点关联）字段是否填充了标签。

## 创建计算机目录

注意：

请在创建计算机目录之前创建您的资源。配置计算机目录时，请使用 Google Cloud 建立的命名约定。有关详细信息，请参阅[存储桶和对象命名指南](#)。

可以通过两种方式创建计算机目录：

- 完整配置界面
- PowerShell。请参阅[创建目录](#)。有关如何使用 PowerShell 实现特定功能的信息，请参阅[使用 PowerShell](#)

### 使用完整配置界面创建计算机目录

请按照[创建计算机目录](#)中的指导进行操作。下面的说明是 Google Cloud 目录独有的。

1. 在管理 > 完整配置中，选择左窗格中的计算机目录。
2. 然后在操作栏中选择创建计算机目录。
3. 在计算机类型页面上，选择多会话操作系统，然后选择下一步。Citrix DaaS 还支持单会话操作系统。
4. 在计算机管理页面上，选择进行电源管理的计算机和 **Citrix Machine Creation Services** 选项，然后选择下一步。如果有多种资源，请从菜单中选择一种资源。
5. 在“映像”页面上，根据需要完成这些步骤，然后单击“下一步”。

a) 选择快照或 VM 作为主映像。如果要使用唯一租赁功能，请务必选择已正确配置节点组属性的映像。请参阅[启用区域选择](#)。

b) 要使用现有虚拟机作为计算机配置文件，请选择使用计算机配置文件，然后选择虚拟机。

注意：

当前，该目录中的 VM 从计算机配置文件中继承磁盘加密 ID、计算机大小、存储类型和区域设置。

c) 为目录选择最低功能级别。

6. 在存储页面上，选择用于容纳此计算机目录的操作系统的存储类型。下面每种存储方案都有独特的价格和性能特征。身份磁盘始终使用区域标准永久性磁盘创建。

- 标准永久性磁盘

- 平衡的永久磁盘
- SSD 永久性磁盘

如需详细了解 Google Cloud 存储选项，请参阅[存储选项](#)。

7. 在虚拟机页面上，指定要创建的虚拟机数量，查看虚拟机的详细规格，选择 Google Cloud 计算机类型，然后选择下一步。如果将唯一租户节点组用于计算机目录，请确保仅选择预留的唯一租户节点可用的区域。请参阅[启用区域选择](#)。

8. 在磁盘设置页面上，可以配置以下设置：

- 选择是否启用回写式缓存。启用回写式缓存后，您可以执行以下操作：
  - 配置用于缓存临时数据的磁盘和 RAM 的大小。有关详细信息，请参阅[配置临时数据的缓存](#)。
  - 选择回写式缓存磁盘的存储类型。以下存储选项可用于回写式缓存磁盘：
    - ★ 标准永久性磁盘
    - ★ 平衡的永久磁盘
    - ★ SSD 永久性磁盘

如需详细了解 Google Cloud 存储选项，请参阅[存储选项](#)。

- 选择回写式缓存磁盘的类型。
  - ★ 使用非永久回写式缓存磁盘。如果选中此选项，回写式缓存磁盘不会为已预配的 VM 保留。在电源重启期间，磁盘将被删除，重定向到磁盘的所有数据都将丢失。
  - ★ 使用永久回写式缓存磁盘。如果选中此选项，回写式缓存磁盘将为已预配的 VM 保留。启用此选项会增加存储成本。
- 启用 MCS 存储优化 (MCS I/O) 后，可以选择是否在电源重启期间为 VDA 保留系统磁盘。有关详细信息，请参阅[启用 MCS 存储优化更新](#)。
- 选择是否使用自己的密钥来保护磁盘内容。要使用该功能，您必须首先创建自己的客户管理的加密密钥 (CMEK)。有关详细信息，请参阅[使用客户管理的加密密钥 \(CMEK\)](#)。

注意：

它仅在管理 > 完整配置界面中可用。

创建密钥后，可以从列表中选择其中一个密钥。创建目录后无法更改注册表项。Google Cloud 不支持在现有的永久磁盘或映像中轮换密钥。因此，在预配目录之后，该目录将与密钥的特定版本绑定。如果该密钥处于禁用状态或被销毁，则在重新启用或恢复密钥之前，使用该密钥加密的实例和磁盘将无法使用。

9. 在计算机标识页面上，选择一个 Active Directory 帐户，然后选择下一步。

- 如果选择创建新的 **Active Directory** 帐户，请选择一个域，然后输入表示在 Active Directory 中创建的已预配的 VM 计算机帐户的命名方案的字符序列。帐户命名方案可以包含 1-64 个字符，不能包含空格，也不能包含非 ASCII 字符或特殊字符。

- 如果选择使用现有的 **Active Directory** 帐户，请选择浏览以导航到所选计算机的现有 Active Directory 计算机帐户。
10. 在域凭据页面上，选择输入凭据，键入用户名和密码，选择保存，然后选择下一步。
    - 键入的凭据必须具有执行 Active Directory 帐户操作的权限。
  11. 在作用域页面上，选择计算机目录的作用域，然后选择下一步。
    - 可以选择可选作用域或选择自定义作用域以根据需要自定义作用域。
  12. 在摘要页面上，确认信息，指定目录的名称，然后选择完成。

注意：

目录名称可以包含 1-39 个字符，不能仅包含空格或字符 \ / ; : # . \* ? = < > | [ ] { } " ' ( ) ' ) 。

完成计算机目录创建可能需要很长时间。完成后，系统将列出目录。可以验证计算机是否在 Google Cloud 控制台中的目标节点组上创建。

## 导入手动创建的 Google Cloud 计算机

通过此功能，您可以：

- 将手动创建的 Google Cloud 多会话操作系统计算机导入到 Citrix DaaS 目录中。
- 从 Citrix DaaS 目录中移除手动创建的 Google Cloud 多会话操作系统计算机。
- 使用现有 Citrix DaaS 电源管理功能对 Google Cloud Windows 多会话操作系统计算机进行电源管理。例如，为这些计算机设置重新启动计划。

此功能不需要更改现有 Citrix DaaS 的配置工作流程，也不需要移除任何现有功能。

建议您使用 MCS 在 Citrix DaaS 的完整配置界面中置备计算机，而不是导入手动创建的 Google Cloud 计算机。

## 共享虚拟私有云

共享虚拟私有云 (VPC) 包括一个主机项目（可以从中使用共享子网）以及一个或多个使用该资源的服务项目。共享 VPC 是较大规模安装的理想选项，因为它们可以集中控制、使用和管理共享的企业 Google Cloud 资源。有关详细信息，请参阅 [Google 文档站点](#)。

使用此功能，Machine Creation Services (MCS) 可以支持预配和管理部署到共享 VPC 的计算机目录。这种支持在功能上等同于当前在本地 VPC 中提供的支持，在两个方面有所差别：

- 必须向用于创建主机连接的服务帐户授予额外权限。此过程允许 MCS 访问和使用共享 VPC 资源。请参阅“需要新权限”。

- 必须创建两条防火墙规则，每条规则分别用于入口和出口。这些防火墙规则将在映像控制过程中使用。请参阅防火墙规则。

有关配置共享 VPC 的信息，请参阅配置共享 VPC。

#### 需要新权限

创建主机连接时，需要具有特定权限的 Google Cloud 服务帐户。必须向用于创建基于共享 VPC 的主机连接的任何服务帐户授予这些额外的权限。

##### 提示：

这些额外的权限对于 Citrix DaaS 来说并不陌生。它们用来促进本地 VPC 的实施。对于共享 VPC，这些额外的权限允许访问其他共享 VPC 资源。

为了支持共享 VPC，必须向与主机连接关联的服务帐户授予最多四个额外权限：

- **compute.firewalls.list** - 此权限是强制性的。它允许 MCS 检索共享 VPC 上存在的防火墙规则的列表。
- **compute.networks.list** - 此权限是强制性的。它允许 MCS 识别服务帐户可用的共享 VPC 网络。
- **compute.subnetworks.list** - 此权限是可选的，具体取决于您使用 VPC 的方式。它允许 MCS 识别可见的共享 VPC 中的子网。使用本地 VPC 时已需要此权限，但也必须在共享 VPC 主机项目中进行分配。
- **compute.subnetworks.use** - 此权限是可选的，具体取决于您使用 VPC 的方式。必须在预配的计算机目录中使用子网资源。使用本地 VPC 已需要此权限，但也必须在共享 VPC 主机项目中进行分配。

使用这些权限时，请考虑根据用于创建计算机目录的权限类型有不同的方法：

- 项目级别权限：
  - 允许访问主机项目中的所有共享 VPC。
  - 需要权限 `compute.subnetworks.list` 且 `compute.subnetworks.use` 必须分配给服务帐号。
- 子网级别权限：
  - 允许访问共享 VPC 中的特定子网。
  - 权限 `compute.subnetworks.list` 和 `compute.subnetworks.use` 是子网级别分配的固有权限，因此无需直接分配给服务帐号。

请选择符合贵组织需求和安全标准的方式。

##### 提示：

有关项目级别权限和子网级权限之间差异的更多信息，请参阅[服务项目管理员](#)。

## 防火墙规则

在准备计算机目录期间，将准备计算机映像作为目录的主映像系统磁盘。发生此过程时，磁盘将临时连接到虚拟机。此 VM 必须在隔离的环境中运行，以阻止所有入站和出站网络流量。这是通过一对 deny-all 防火墙规则实现的：一条规则用于入口流量，一条规则用于出口流量。使用 Google Cloud 本地 VCP 时，MCS 会在本地网络中创建此防火墙，并将其应用到计算机以进行控制。控制操作完成后，将从映像中删除防火墙规则。

我们建议您将使用共享 VPC 所需的新权限的数量保持在最低限度。共享 VPC 是更高级别的企业资源，通常具有更严格的安全协议。因此，在共享 VPC 资源的主机项目中创建一对防火墙规则，一条用于入口，一条用于出口。请为其分配最高优先级。使用以下值将新目标标记应用到这些规则中的每一个规则：

`citrix-provisioning-quarantine-firewall`

创建或更新计算机目录时，MCS 会搜索包含此目标标记的防火墙规则。然后，它会检查规则的正确性，并将其应用到用于准备目录的主映像的计算机。如果未找到防火墙规则，或者找到规则，但规则或其优先级不正确，则会出现类似以下内容的消息：

```
"Unable to find valid INGRESS and EGRESS quarantine firewall rules
for VPC <name> in project <project>. "Please ensure you have created
'deny all' firewall rules with the network tag 'citrix-provisioning-
quarantine-firewall' and proper priority." "Refer to Citrix Documentation
for details."
```

## 配置共享 VPC

在 Citrix DaaS 的“完整配置”界面中添加共享 VPC 作为主机连接之前，请完成以下步骤，以将您计划预配的项目中的服务帐户添加到：

1. 创建 IAM 角色。
2. 向宿主项目 IAM 角色添加服务帐户。
3. 将云构建服务帐户添加到共享 VPC。
4. 创建防火墙规则。

创建 IAM 角色 确定角色的访问级别：

- 项目级别访问权限，或
- 使用子网级别访问的更受限制的模型。

**IAM** 角色的项目级别的访问权限。对于项目级别的 IAM 角色，包括以下权限：

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use



要创建项目级别的 IAM 角色，请执行以下操作：

1. 在 Google 云控制台中，导航至 **IAM & Admin** (IAM 和管理员) > **Roles** (角色)。
2. 在角色页面上，选择创建角色。
3. 在 **Create Role** (创建角色) 页面上，指定角色名称。选择添加权限。
  - a) 在 **Add permissions** (添加权限) 页面上，单独向角色添加权限。要添加权限，请在筛选器表字段中键入权限的名称。选择权限，然后选择添加。
  - b) 选择创建。

子网级别的 IAM 角色。此角色将在选择 **CREATE ROLE** (创建角色) 后省略添加权限 `compute.subnetworks.list` 和 `compute.subnetworks.use`。对于此 IAM 访问级别，权限 `compute.firewalls.list` 和 `compute.networks.list` 必须应用到新角色。

要创建子网级别的 IAM 角色，请执行以下操作：

1. 在 Google Cloud 控制台中，导航到 **VPC network** (VPC 网络) > **Shared VPC** (共享 VPC)。此时将显示 **Shared VPC** (共享 VPC) 页面，其中显示主机项目所包含的共享 VPC 网络的子网。
2. 在 **Shared VPC** (共享 VPC) 页面上，选择要访问的子网。
3. 在右上角，选择 **ADD MEMBER** (添加成员) 以添加服务帐户。
4. 在 **Add members** (添加成员) 页面上，完成以下步骤：
  - a) 在 **New members** (新成员) 字段中，键入服务帐户的名称，然后在菜单中选择您的服务帐户。
  - b) 选择 **Select a role** (选择角色) 字段，然后单击 **Compute Network User** (计算网络用户)。
  - c) 选择保存。
5. 在 Google Cloud 控制台中，导航到 **IAM & Admin** (IAM 和管理员) > **Roles** (角色)。
6. 在角色页面上，选择创建角色。
7. 在 **Create Role** (创建角色) 页面上，指定角色名称。选择添加权限。
  - a) 在 **Add permissions** (添加权限) 页面上，单独向角色添加权限。要添加权限，请在筛选器表字段中键入权限的名称。选择权限，然后选择添加。
  - b) 选择创建。

将服务帐户添加到主机项目 IAM 角色 创建 IAM 角色后，请执行以下步骤以便为主机项目添加服务帐户：

1. 在 Google Cloud 控制台中，导航到主机项目，然后导航到 **IAM & Admin** (IAM 和管理员) > **IAM**。
2. 在 **IAM** 页面上，选择 **ADD** (添加) 以添加服务帐户。
3. 在 **Add members** (添加成员) 页面上：
  - a) 在 **New members** (新成员) 字段中，键入服务帐户的名称，然后在菜单中选择您的服务帐户。
  - b) 选择一个角色字段，键入您创建的 IAM 角色，然后选择菜单中的角色。
  - c) 选择保存。

现在已为主机项目配置服务帐户。



将云构建服务帐户添加到共享 **VPC** 每个 Google Cloud 订阅都有一个服务帐户，该帐户以项目 ID 命名，后跟 `cloudbuild.gserviceaccount`。例如: `705794712345@cloudbuild.gserviceaccount`。

您可以通过在 Google Cloud 控制台中导航到云端概览 > 控制面板来确定项目的项目 ID 号。项目 ID 和项目编号显示在项目控制面板项目信息卡上：

请执行以下步骤以将云构建服务帐户添加到共享 VPC：

1. 在 Google Cloud 控制台中，导航到主机项目，然后导航到 **IAM & Admin**（IAM 和管理员）> **IAM**。
2. 在 **Permissions**（权限）页面上，选择 **ADD**（添加）以添加帐户。
3. 在 **Add members**（添加成员）页面上，完成以下步骤：
  - a) 在 **New members**（新成员）字段中，键入云构建服务帐户的名称，然后在菜单中选择您的服务帐户。
  - b) 选择选择角色字段，键入 **Computer Network User**，然后在菜单中选择角色。
  - c) 选择保存。

**创建防火墙规则** 作为映像控制过程的一部分，MCS 会复制选定的计算机映像，并使用该映像为目录准备主映像系统磁盘。在映像控制过程中，MCS 将磁盘附加到临时虚拟机，然后该虚拟机将运行准备脚本。此 VM 必须在隔离的环境中运行，以禁止所有入站和出站网络流量。

要创建隔离环境，MCS 需要两个 *deny all*（全部拒绝）防火墙规则（入口规则和出口规则）。因此，在主机项目中创建两个防火墙规则（入口和出口），如下所示：

1. 在 Google Cloud 控制台中，导航到主机项目，然后导航到 **VPC network**（VPX 网络）> **Firewall**（防火墙）。
2. 在 **Firewall**（防火墙）页面上，选择 **CREATE FIREWALL RULE**（创建防火墙规则）。
3. 在 **Create a firewall rule**（创建防火墙规则）页面上，完成以下操作：
  - 名称。键入规则的名称。
  - **Network**（网络）。选择入口防火墙规则应用到的共享 VPC 网络。
  - **Priority**（优先级）。值越小，规则的优先级就越高。我们建议使用较小的值（例如 10）。
  - **Direction of traffic**（流量方向）。选择 **Ingress**（入口）。
  - **Action on match**（针对匹配项的操作）。选择 **Deny**（拒绝）。
  - **Targets**（目标）。使用默认的 **Specified target tags**（指定的目标标记）。
  - **Target tags**（目标标记）。键入 `citrix-provisioning-quarantine-firewall`。
  - **Source filter**（源筛选器）。使用默认的 **IP ranges**（IP 范围）。
  - **Source IP ranges**（源 IP 范围）。键入匹配所有流量的范围。键入 `0.0.0.0/0`。
  - **Protocols and ports**（协议和端口）。选择 **Deny all**（全部拒绝）。
4. 选择创建以创建规则。
5. 重复这些步骤以创建另一条规则。对于 **Direction of traffic**（流量方向），请选择 **Egress**（出口）。

## 使用客户管理的加密密钥 (CMEK)

可以将客户管理的加密密钥 (CMEK) 用于 MCS 目录。使用此功能时，您将 Google Cloud Key Management Service [CryptoKey Encrypter/Decrypter](#) 角色分配给 Compute Engine Service Agent。Citrix DaaS 帐户在存储密钥的项目中必须具有正确的权限。请参阅为 Citrix DaaS 帐户分配权限。有关详细信息，请参阅[使用 Cloud KMS 密钥帮助保护资源](#)。

您的 Compute Engine Service Agent 的格式如下：[service-`<Project \_Number>`@compute-system.iam.gserviceaccount.com](#)。此表单与默认的 Compute Engine Service 帐户不同。

### 注意：

此 Compute Engine Service 帐户可能不会显示在 Google 控制台 **IAM** 权限显示屏中。在这种情况下，请按照[使用 Cloud KMS 密钥帮助保护资源](#)中所述使用 `gcloud` 命令。

## 向 Citrix DaaS 帐户分配权限

Google Cloud KMS 权限可以通过多种方式进行配置。可以提供项目级 KMS 权限或资源级 KMS 权限。有关详细信息，请参阅[权限和角色](#)。

**项目级别 KMS 权限** 一种选择是向 Citrix DaaS 帐户提供项目级权限以浏览 Cloud KMS 资源。为此，请创建一个自定义角色，然后添加以下权限：

- [cloudkms.keyRings.list](#)
- [cloudkms.keyRings.get](#)
- [cloudkms.cryptokeys.list](#)
- [cloudkms.cryptokeys.get](#)

将此自定义角色分配给 Citrix DaaS 帐户。这允许您浏览清单中相关项目中的区域密钥。

**资源级 KMS 权限** 对于另一个选项（资源级权限），请在 Google Cloud 控制台中浏览到用于 MCS 预配的 [cryptoKey](#)。将 Citrix DaaS 帐户添加到您用于目录预配的密钥链或密钥中。

### 提示：

使用此选项，您无法浏览清单中的项目的区域密钥，因为 Citrix DaaS 帐户对 Cloud KMS 资源没有项目级列表权限。但是，您仍然可以通过在 **ProvScheme** 自定义属性中指定正确的 [cryptoKeyId](#) 来使用 CMEK 预置目录。请参阅[使用自定义属性使用 CMEK 创建目录](#)。

## 轮换客户管理的密钥

Google Cloud 不支持在现有的永久磁盘或映像中轮换密钥。一旦计算机预配完毕，它将与创建时使用的密钥版本绑定在一起。但是，可以创建密钥的新版本，新密钥用于在使用新主映像更新目录时创建的新预配的计算机或资源。

关于密钥链的重要注意事项 无法重命名或删除密钥链。此外，对其进行配置时可能会产生不可预见的费用。删除或移除密钥链时，Google Cloud 会显示一条错误消息：

```
1 Sorry, you can't delete or rename keys or key rings. We were concerned
  about the security implications of allowing multiple keys or key
  versions over time to have the same resource name, so we decided to
  make names immutable. (And you can't delete them, because we wouldn't
  be able to do a true deletion--there would still have to be a
  tombstone tracking that this name had been used and couldn't be
  reused).
2 We're aware that this can make things untidy, but we have no immediate
  plans to change this.
3 If you want to avoid getting billed for a key or otherwise make it
  unavailable, you can do so by deleting all the key versions; neither
  keys nor key rings are billed for, just the active key versions
  within the keys.
4 <!--NeedCopy-->
```

提示：

有关详细信息，请参阅[从控制台编辑或删除密钥链](#)。

## 统一存储桶级别访问兼容性

Citrix DaaS 与 Google Cloud 上的统一存储桶级别访问控制策略兼容。此功能增强了 IAM 策略的使用，该策略向服务帐户授予权限，以允许操作资源，包括存储桶。通过统一存储桶级别访问控制，Citrix DaaS 允许您使用访问控制列表 (ACL) 来控制对存储桶或存储在其中的对象的访问。有关 Google 云端平台统一存储桶级别访问的概述信息，请参阅[统一存储桶级别访问](#)。有关配置信息，请参阅[要求统一存储桶级别访问](#)。

## 使用 PowerShell

本部分内容详细介绍了如何使用 PowerShell 执行以下任务：

- 创建具有永久回写式缓存磁盘的目录
- 使用 MCSIO 提高启动性能
- 使用自定义属性使用 CMEK 创建目录
- 使用计算机配置文件创建计算机目录
- 使用计算机配置文件作为实例模板创建计算机目录
- 使用屏蔽虚拟机创建目录

## 创建具有永久回写式缓存磁盘的目录

要使用永久回写式缓存磁盘配置目录，请使用 PowerShell 命令 `New-ProvScheme CustomProperties`。

### 提示：

请仅将 PowerShell 参数 `New-ProvScheme CustomProperties` 用于基于云的托管连接。如果您想使用永久回写式缓存磁盘为本地解决方案（例如 XenServer）预配计算机，则不需要 PowerShell，因为该磁盘会自动保存。

此命令支持一个额外的属性 `PersistWBC`，用于确定 MCS 配置的计算机的回写式缓存磁盘的保存方式。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。

### 注意：

此行为同时适用于 Azure 和 GCP，在重启电源时，默认 MCSIO 回写式缓存磁盘将删除并重新创建。可以选择保留该磁盘，以避免删除和重新创建 MCSIO 回写式缓存磁盘。

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">
2   <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
3   <Property xsi:type="StringProperty" Name="StorageAccountType" Value="Premium_LRS" />
4   <Property xsi:type="StringProperty" Name="ResourceGroups" Value="benva1dev5RG3" />
5 </CustomProperties>
6 <!--NeedCopy-->
```

### 注意：

此示例仅适用于 Azure。GCP 环境中的属性会有所差别。

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**。

当 Citrix DaaS 管理员从管理界面关闭计算机时，将 `PersistWBC` 属性设置为 **true** 不会删除回写式缓存磁盘。

当 Citrix DaaS 管理员从管理界面关闭计算机时，将 `PersistWBC` 属性设置为 **false** 会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**，并在从管理界面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**：

```

1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
  instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
  />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
  Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
  benvaldev5RG3" />
5 <Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
6 </CustomProperties>
7 <!--NeedCopy-->

```

**重要提示：**

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：

```

1 New-ProvScheme
2 -CleanOnBoot
3 -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=`"
  StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
  /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
  Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
  =`"PersistWBC`" Value=`"true`" /></CustomProperties>"
4 -HostingUnitName "adSubnetScale1"
5 -IdentityPoolName "BV-WBC1-CAT1"
6 -MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
  GoldImages.resourcegroup\W10MCSI0-01
  _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
7 -NetworkMapping @{
8   "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
  CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
  adSubnetScale1.network" }
9
10 -ProvisioningSchemeName "BV-WBC1-CAT1"
11 -ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
  folder\Standard_D2s_v3.serviceoffering"
12 -UseWriteBackCache
13 -WriteBackCacheDiskSize 127
14 -WriteBackCacheMemorySize 256
15 <!--NeedCopy-->

```

使用 **MCSIO** 提高启动性能

启用 MCSIO 后, 可以提高 Azure 和 GCP 托管磁盘的引导性能。请使用 **New-ProvScheme** 命令中的 PowerShell **PersistOSDisk** 自定义属性配置此功能。与 **New-ProvScheme** 关联的选项包括:

```

1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
  instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
  />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
  Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="Resource<!--NeedCopy-->
5 <!--NeedCopy-->
6 <!--NeedCopy-->Groups" Value="benvaldev5RG3" />
7 <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
  />
8 </CustomProperties>
9 <!--NeedCopy-->

```

要启用此功能, 请将 **PersistOSDisk** 自定义属性设置为 **true**。例如:

```

1 New-ProvScheme
2 -CleanOnBoot
3 -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=`"
  StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
  /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
  Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
  =`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
4 -HostingUnitName "adSubnetScale1"
5 -IdentityPoolName "BV-WBC1-CAT1"
6 -MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
  GoldImages.resourcegroup\W10MCSIO-01
  _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
7 -NetworkMapping @{
8   "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
  CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
  adSubnetScale1.network" }
9
10 -ProvisioningSchemeName "BV-WBC1-CAT1"
11 -ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
  folder\Standard_D2s_v3.serviceoffering"
12 -UseWriteBackCache
13 -WriteBackCacheDiskSize 127
14 -WriteBackCacheMemorySize 256
15 <!--NeedCopy-->

```

## 使用自定义属性使用 **CMEK** 创建目录

通过 PowerShell 创建预配方案时，请在 `ProvScheme CustomProperties` 中指定 `CryptoKeyId` 属性。例如：

```
1 '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
2   <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="<
3     yourCryptoKeyId>" />
4 </CustomProperties>'
```

必须按以下格式指定 `cryptoKeyId`：

`projectId:location:keyRingName:cryptoKeyName`

例如，如果您想在区域 `us-east1` 和 ID 为 `my-example-project-1` 的项目中的密钥链 `my-example-key-ring` 中使用密钥 `my-example-key`，您的 `ProvScheme` 自定义设置将类似于：

```
1 '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
2   <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
3     example-project-1:us-east1:my-example-key-ring:my-example-key"
4   />
5 </CustomProperties>'
```

与此预配方案相关的所有 MCS 预配磁盘和映像都使用此客户管理的加密密钥。

### 提示：

如果使用全局密钥，客户属性位置必须指出 `global` 而非区域名称，在上面的示例中为 `us-east1`。  
例如：`<Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-example-project-1:global:my-example-key-ring:my-example-key"/>`。

## 使用计算机配置文件创建计算机目录

创建目录以使用 Machine Creation Services (MCS) 预配计算机时，可以使用计算机配置文件从虚拟机捕获硬件属性并将其应用到目录中新预配的 VM。不使用 `MachineProfile` 参数时，将从主映像 VM 或快照中捕获硬件属性。您明确定义的某些属性（例如 `StorageType`、`CatalogZones` 和 `CryptoKeyId`）在计算机配置文件中会被忽略。

- 要使用计算机配置文件创建目录，请使用 `New-ProvScheme` 命令。例如，`New-ProvScheme -MachineProfile "path to VM"`。如果未指定 `MachineProfile` 参数，则从主映像 VM 捕获硬件属性。



- 要使用新的计算机配置文件更新目录，请使用 `Set-ProvScheme` 命令。例如，`Set-ProvScheme -MachineProfile "path to new VM"`。此命令不会更改目录中现有 VM 的计算机配置文件。只有添加到目录中的新创建的 VM 才具有新的计算机配置文件。
- 您也可以更新主映像，但是，更新主映像时，不会更新硬件属性。如果要更新硬件属性，则需要使用 `Set-ProvScheme` 命令更新计算机配置文件。这些更改仅适用于目录中的新计算机。要更新现有计算机的硬件属性，可以使用带 `-StartsNow` 和 `-DurationInMinutes -1` 参数的 `Set-ProvVMUpdateTimeWindow` 命令。

注意：

- `StartsNow` 表示计划的开始时间为当前时间。
- `DurationInMinutes` 负数（例如 -1）表示计划的时间范围没有上限。

### 使用计算机配置文件作为实例模板创建计算机目录

您可以选择 GCP 实例模板作为计算机配置文件的输入。实例模板是 GCP 中的轻型资源，因此非常经济实惠。

#### 使用计算机配置文件作为实例模板创建新计算机目录

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 使用以下命令在 GCP 项目中查找实例模板：

```
1 cd XDHyp:\HostingUnits<HostingUnitName>\instanceTemplates.folder
2 <!--NeedCopy-->
```

4. 通过 `NewProvScheme` 命令使用计算机配置文件作为实例模板创建新的计算机目录：

```
1 New-ProvScheme -ProvisioningSchemeName <CatalogName> -
  HostingUnitName <HostingUnitName> -IdentityPoolName <identity
  pool name> -MasterImageVM
2 XDHyp:\HostingUnits<HostingUnitName>\Base.vm\Base.snapshot -
  MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
  instanceTemplates.folder\mytemplate.template
3 <!--NeedCopy-->
```

有关 `New-ProvScheme` 命令的详细信息，请参阅 <https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/>。

5. 使用 PowerShell 命令完成计算机目录的创建。

#### 更新计算机目录以使用实例模板作为计算机配置文件

1. 打开 PowerShell 窗口。



2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 请运行以下命令：

```
1 Set-ProvScheme -ProvisioningSchemeName <CatalogName> -  
  MachineProfile XDHyp:\HostingUnits<HostingUnitName>\  
  instanceTemplates.folder<TemplateName>.template  
2 <!--NeedCopy-->
```

有关 Set-ProvScheme 命令的信息，请参阅 <https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/>。

### 使用屏蔽虚拟机创建目录

可以创建具有受保护的 VM 属性的 MCS 计算机目录。一组安全控制措施强化了受保护的虚拟机，这些控制措施使用安全引导、虚拟可信平台模块、UEFI 固件和完整性监视等高级平台安全功能提供计算引擎实例的可验证的完整性。

MCS 支持使用计算机配置文件工作流程创建目录。如果使用计算机配置文件工作流程，必须启用 VM 实例的受保护的 VM 属性。然后，您可以使用此 VM 实例作为计算机配置文件输入。

### 使用屏蔽虚拟机创建 **MCS** 计算机目录

1. 在 Google Cloud 控制台中启用 VM 实例的受保护的 VM 选项。请参阅[快速入门：启用安全强化型 VM 选项](#)。
2. 使用虚拟机实例创建包含计算机配置文件工作流程的 MCS 计算机目录。
  - a) 打开 PowerShell 窗口
  - b) 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
  - c) 创建标识池（如果尚未创建）。
  - d) 运行 `New-ProvScheme` 命令。例如：

```
1 New-ProvScheme -ProvisioningSchemeName <catalog-name>  
2 -HostingUnitName gcp-hostint-unit  
3 -MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-  
  vda.vm  
4 -MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-  
  machine.vm  
5 <!--NeedCopy-->
```

3. 完成计算机目录的创建。

### 使用新的计算机配置文件更新计算机目录

1. 运行 `Set-ProvScheme` 命令。例如：

```

1 Set-ProvScheme -ProvisioningSchemeName <catalog-name>
2 -MasterImageVM XDHyp:\HostingUnits<hostin-unit>\catalog-vda.vm
3 -MachineProfile "DHyp:\HostingUnits<hostin-unit>\catalog-machine.
   vm
4 <!--NeedCopy-->

```

要将在 `Set-ProvScheme` 中所做的更改应用到现有 VM，请运行 `Set-ProvVMUpdateTimeWindow` 命令。

1. 运行 `Set-ProvVMUpdateTimeWindow` 命令。例如：

```

1 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
   VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
2 <!--NeedCopy-->

```

2. 重新启动 VM。

## Google Cloud Marketplace

可以在 Google Cloud Marketplace 上浏览和选择 Citrix 提供的映像来创建计算机目录。目前，MCS 仅支持面向此功能的计算机配置文件工作流程。

要通过 Google Cloud Marketplace 搜索 Citrix VDA VM 产品，请转至 <https://console.cloud.google.com/marketplace/>。

可以使用自定义映像或 Google Cloud Marketplace 上的 Citrix Ready 映像来更新计算机目录的映像。

注意：

如果计算机配置文件不包含存储类型信息，则该值来自自定义属性。

支持的 Google Cloud Marketplace 映像如下：

- Windows 2019 单会话
- Windows 2019 多会话
- Ubuntu

使用 Citrix Ready 映像作为创建计算机目录的源示例：

```

1 New-ProvScheme -ProvisioningSchemeName GCPCatalog \
2 -HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \
3 -MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
   win2019-single-vda-v20220819.publicimage \
4 -MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
5 <!--NeedCopy-->

```

## 下一步的去向

- 如果这是创建的第一个目录，系统将引导您[创建交付组](#)。
- 要查看整个配置过程，请参阅[规划和构建部署](#)。
- 要管理目录，请参阅[管理计算机目录](#)和[管理 Google 云端平台目录](#)。

## 更多信息

- [创建和管理连接和资源](#)
- [与 Google Cloud 环境的连接](#)
- [创建计算机目录](#)

## 创建 **HPE Moonshot** 计算机目录（预览版）

January 23, 2024

[创建计算机目录](#)介绍了用于创建计算机目录的向导。以下信息涵盖了特定于 HPE Moonshot 环境的详细信息。

### 注意：

- 创建与 HPE Moonshot 的连接
- 确保有一个或多个 HPE Moonshot 节点可用，并在这些节点上安装 VDA。
- 有关创建初始 HPE Moonshot 磁带映像的信息，请参阅 [《在 Moonshot 上部署操作系统用户指南》](#)。

您可以使用以下方法创建 HPE Moonshot 计算机目录：

- 完整配置界面
- PowerShell 命令

### 使用完整配置界面创建计算机目录

在“计算机目录设置”向导中：

1. 在操作系统页面上，选择多会话操作系统或单会话操作系统。
2. 在“计算机管理”页面上，选择“受电源管理的计算机”和“其他服务或技术”。
3. 在 虚拟机 页面上，添加计算机及其 Active Directory 计算机帐户。您可以执行以下任一操作：
  - 单击“添加计算机”以手动添加计算机。将出现“选择虚拟机”窗口。扩展您之前创建的 HPE Moonshot 机箱连接，然后选择要添加的节点 (VM)。然后添加关联的计算机帐户名。

- 单击“添加 **CSV** 文件”以批量添加计算机。有关使用 CSV 文件添加计算机的信息，请参阅 [使用 CSV 文件将计算机批量添加到目录](#)。

范围和摘要页面不包含 HPE Moonshot 的特定信息。

## 使用 **PowerShell** 命令创建计算机目录

运行 **New-BrokerCatalog** 和 **New-BrokerMachine** PowerShell 命令以创建代理目录并将计算机导入代理目录。

例如：

```
1 New-BrokerCatalog -AdminAddress "localhost:19097" -AdminClientIP "
  103.14.252.249" -AllocationType "Random" -IsRemotePC $False -
  MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "
  BurMC" -PersistUserChanges "OnLocal" -ProvisioningType "Manual" -
  Scope @() -SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc
  -4578-bc07-bcf2a82d1463"
2 New-BrokerMachine -AdminAddress "localhost:19097" -AdminClientIP "
  103.14.252.249" -CatalogUid 3 -HostedMachineId "c10n1" -
  HypervisorConnectionUid 4 -IsReserved $False -MachineName "S
  -1-5-21-2589939477-3963209805-1860259709-1121"
3 <!--NeedCopy-->
```

## 下一步的去向

- 如果这是创建的第一个目录，系统将引导您[创建交付组](#)。
- 要查看整个配置过程，请参阅[规划和构建部署](#)。
- 要管理目录，请参阅[管理计算机目录](#)和[管理 HPE Moonshot 目录](#)。

## 更多信息

- [创建和管理连接和资源](#)
- [连接到 HPE Moonshot](#)
- [创建计算机目录](#)

## 创建 **Microsoft Azure** 目录

March 30, 2024

[创建计算机目录](#)介绍了用于创建计算机目录的向导。以下信息涵盖了特定于 Microsoft Azure Resource Manager 云环境的详细信息。

注意：

在创建 Microsoft Azure 目录之前，您需要完成创建与 Microsoft Azure 的连接。请参阅[与 Microsoft Azure 的连接](#)。

## 创建计算机目录

可以通过两种方式创建计算机目录：

- 完整配置界面。
- PowerShell。请参阅[创建目录](#)。有关如何使用 PowerShell 实现特定功能的信息，请参阅[使用 PowerShell](#)。

在完整配置界面中使用 **Azure Resource Manager** 映像创建计算机目录

此信息用于补充[创建计算机目录](#)中的指导信息。

映像可以是磁盘、快照或 Azure Compute Gallery 中用于在计算机目录中创建 VM 的映像定义的映像版本。

创建计算机目录之前，请在 Azure Resource Manager 中创建一个映像。

注意：

- 不建议使用非托管磁盘置备 VM。
- 不支持使用与在主机连接中配置的区域不同的主映像。使用 Azure Compute Gallery 将主映像复制到所需区域。

在映像准备期间，将在原始 VM 的基础上创建准备虚拟机 (VM)。此准备 VM 已与网络断开连接。为了断开网络与准备 VM 的连接，需要创建一个网络安全组以拒绝所有入站和出站流量。每个目录自动创建一次网络安全组。网络安全组的名称为 **Citrix-Deny-All-a3pgu-GUID**，其中 GUID 是随机生成的。例如，**Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1**。

在计算机目录创建向导中，执行以下操作：

1. 计算机类型和计算机管理页面不包含 Azure 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。
2. 在映像页面上，选择要用作目录中所有计算机的主映像的映像。此时将出现选择映像向导。请按照以下步骤选择图片：
  - a) (仅适用于使用租户内部或租户间共享映像配置的连接) 选择映像所在的订阅。
  - b) 选择资源组。
  - c) 导航到 Azure 托管磁盘、Azure Compute Gallery 或 Azure 映像版本。

选择映像时，请注意以下事项：

- 验证映像上是否安装了 Citrix VDA。
- 如果选择连接到虚拟机的磁盘，则必须先关闭虚拟机，然后才能继续执行下一步。

## 注意：

- 与在目录中创建计算机的连接（主机）对应的订阅用绿点表示。其他订阅是指那些与该订阅共享了 Azure Compute Gallery 的订阅。在这些订阅中，仅显示共享映像。有关如何配置共享订阅的信息，请参阅[在租户内（跨订阅）共享映像](#)和[在租户之间共享映像](#)。
- 您可以在 Windows 上使用具有受信任启动功能的临时操作系统磁盘创建预配方案。当您选择具有受信任启动功能的映像时，必须选择启用了 vTPM 的具有受信任启动功能的计算机配置文件。要使用临时操作系统磁盘创建计算机目录，请参阅[如何使用临时操作系统磁盘创建计算机](#)。
- 当映像复制正在进行时，您可以继续选择映像作为主映像并完成设置。但是，在复制映像时创建目录可能需要更长时间才能完成。MCS 要求复制在目录创建开始的一小时内完成。如果复制超时，目录创建将失败。您可以在 Azure 中验证复制状态。请在复制仍处于挂起状态或在复制完成后重试。
- 您可以使用 Gen2 映像来预配 Gen2 VM 目录，以缩短启动时间。但是，不支持使用 Gen1 映像创建 Gen2 计算机目录。同样，也不支持使用 Gen2 映像创建 Gen1 计算机目录。此外，没有版本信息的任何旧映像都是 Gen1 映像。

选择是否希望目录中的 VM 继承计算机配置文件中的配置。默认情况下，使用计算机配置文件（对于 **Azure Active Directory** 是必需的）复选框处于选中状态。单击选择计算机配置文件，从资源组列表中浏览到 VM 或 ARM 模板规范。

VM 可以从计算机配置文件中继承的配置示例包括：

- 加速的网络连接
- 启动诊断
- 主机磁盘缓存（与操作系统和 MCSIO 磁盘有关）
- 计算机大小（除非另有说明）
- 置于 VM 上的标记

## 注意：

- 在 Azure 中为计算机目录选择主映像时，计算机配置文件将根据您选择的主映像进行筛选。例如，计算机配置文件根据主映像的 Windows 操作系统、安全类型、休眠支持和磁盘加密 ID 进行筛选。
- 选择启用了受信任启动的映像或快照时，必须使用安全类型设置为“受信任启动”的计算机配置文件。然后，您可以通过在计算机配置文件中指定其值来启用或禁用 SecureBoot 和 vTPM。有关 Azure 可信启动的信息，请参阅 <https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch>。

验证 ARM 模板规范，确保其是否能够用作计算机配置文件来创建计算机目录。有关创建 Azure 模板规范的信息，请参阅[创建 Azure 模板规范](#)。

有两种方法可以验证 ARM 模板规范：

- 从资源组列表中选择 ARM 模板规范后，单击下一步。如果 ARM 模板规范有错误，则会出现错误消息。
- 运行以下 PowerShell 命令之一：

- Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>
- Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>

例如：

```
1 Test-ProvInventoryItem -HostingUnitName "we-vdi0101-d-vnet" -
  InventoryPath machineprofile.folder/vdi01-d-rg.
  resourcegroup/VDD-templ-spec.templatespec/1.5.
  templatespecversion
2 <!--NeedCopy-->
```

创建目录后，可以查看映像从计算机配置文件继承的配置。在计算机目录节点上，选择目录以在下方的窗格中查看其详细信息。然后，单击模板属性选项卡以查看计算机配置文件属性。标记部分最多显示三个标记。要查看放置在 VM 上的所有标记，请单击查看全部。

如果您希望 MCS 在 Azure 专用主机上预置虚拟机，请启用“使用主机组”复选框，然后从列表选择一个主机组。主机组是表示专用主机的集合的资源。专用主机是指提供托管一个或多个虚拟机的物理服务器的服务。您的服务器专用于您的 Azure 订阅，不与其他订阅者共享。使用专用主机时，Azure 会确保您的 VM 是该主机上唯一运行的计算机。此功能适用于必须满足法规或内部安全要求的场景。要详细了解主机组及其使用注意事项，请参阅在 Azure 专用主机上预配虚拟机。

重要：

- 仅显示启用了 Azure 自动放置功能的主机组。
- 使用主机组会更改向导中后面提供的虚拟机页面。该页面上仅显示选定主机组包含的计算机大小。此外，可用性区域是自动选择的，不可供选择。

### 3. 只有当您使用 Azure Resource Manager 映像时，才会显示存储和许可证类型页面。

可以将以下存储类型用于计算机目录：

- **Premium SSD**。提供适用于具有 I/O 密集型工作负载的 VM 的高性能、低延迟磁盘存储方案。
- **标准 SSD**。提供经济高效的存储方案，该方案适用于在较低的 IOPS 级别需要性能一致的工作负载。
- **标准 HDD**。提供适用于运行延迟不敏感的工作负载的 VM 的可靠、低成本的磁盘存储方案。
- **Azure 临时操作系统磁盘**。提供经济高效的、重复使用 VM 的本地磁盘来托管操作系统磁盘的存储方案。或者，您可以使用 PowerShell 创建使用临时操作系统磁盘的计算机。有关详细信息，请参阅 [Azure 临时磁盘](#)。使用临时操作系统磁盘时，请考虑以下几点：
  - 无法同时启用 Azure 临时操作系统磁盘和 MCS I/O。
  - 必须选择大小不超过 VM 的缓存磁盘或临时磁盘大小的映像，才能更新使用临时操作系统磁盘的计算机。
  - 您无法使用稍后在向导中提供的电源重启期间保留 **VM** 和系统磁盘选项。

注意：

无论您选择哪种存储类型，身份磁盘始终使用标准 SSD 创建。

该存储类型决定在向导的虚拟机页面上提供哪些计算机大小。MCS 将高级磁盘和标准磁盘配置为使用本地冗余存储 (LRS)。LRS 在单个数据中心中创建您的磁盘数据的多个同步副本。Azure 临时操作系统磁盘使用 VM 的本地磁盘来存储操作系统。有关 Azure 存储类型和存储复制的详细信息，请参阅以下内容：

- [Azure 存储简介](#)
- [Azure 高级存储：专为高性能而设计](#)
- [Azure 存储冗余](#)

选择是使用现有的 Windows 许可证还是 Linux 许可证：

- Windows 许可证：通过将 Windows 许可证和 Windows 映像（Azure 平台支持映像或自定义映像）结合使用，您可以在 Azure 中以更低的成本运行 Windows VM。许可证有两种类型：
  - **Windows Server** 许可证。支持使用 Windows Server 许可证或 Azure Windows Server 许可证，以允许使用 Azure Hybrid Benefits。有关详细信息，请参阅 <https://azure.microsoft.com/en-us/pricing/hybrid-benefit/>。Azure Hybrid Benefits 将在 Azure 中运行 VM 的成本降低到基本计算费率，从而免除了源自 Azure 库的额外 Windows Server 许可证的费用。
  - **Windows** 客户端许可证。支持在 Azure 中使用 Windows 10 和 Windows 11 许可证，以允许您在 Azure 中运行 Windows 10 和 Windows 11 VM，而无需额外的许可证。有关详细信息，请参阅 [客户端访问许可证和管理许可证](#)。
- Linux 许可证：使用自带订阅 (BYOS) Linux 许可证，您无需为软件付费。BYOS 费用仅包括计算硬件费用。许可证有两种类型：
  - **RHEL\_BYOS**：要成功使用 RHEL\_BYOS 类型，请在您的 Azure 订阅中启用 Red Hat Cloud Access。
  - **SLES\_BYOS**：SLES 的 BYOS 版本包括 SUSE 提供的支持。

请参阅以下内容：

- [验证 Windows 许可证](#)
- [配置 Linux 许可证](#)

请参阅以下文档以了解许可证类型及其好处：

- <https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet>
- <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux>



Azure Compute Gallery 是用于管理和共享映像的存储库。它可以让您在整个组织中使用映像。我们建议您在创建大型非持久性计算机目录时将映像存储在 Azure Compute Gallery 中，因为这样做可以更快地重置 VDA 操作系统磁盘。选择在 **Azure Compute Gallery** 中放置准备好的映像后，将出现 **Azure Compute Gallery** 设置部分，允许您指定更多 Azure Compute Gallery 设置：

- 虚拟机与映像副本的比率。用于指定希望 Azure 保留的虚拟机与映像副本的比率。默认情况下，Azure 为每 40 个非持久性计算机保留一个映像副本。对于持久性计算机，该数字默认为 1000。
- 最大副本计数。允许您指定希望 Azure 保留的最大映像副本数。默认值为 10。

有关 Azure Compute Gallery 的信息，请参阅 [Azure Compute Gallery](#)。

4. 在虚拟机页面上，指明要创建的虚拟机数量和计算机大小。创建目录后，可以通过编辑目录来更改计算机大小。
5. **NIC** 页面不包含 Azure 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。
6. 在磁盘设置页面上，选择是否启用回写式缓存。启用了 MCS 存储优化功能后，可以在创建目录时配置以下设置。这些设置适用于 Azure 和 GCP 环境。

启用回写式缓存后，您可以执行以下操作：

- 配置用于缓存临时数据的磁盘和 RAM 的大小。有关详细信息，请参阅[配置临时数据的缓存](#)。
- 选择回写式缓存磁盘的存储类型。以下存储选项可用于回写式缓存磁盘：
  - 高级 SSD
  - 标准 SSD
  - 标准 HDD
- 选择是否要为已预配的 VM 保留回写式缓存磁盘。选择启用回写式缓存以使这些选项可用。默认情况下，选中使用非永久回写式缓存磁盘。
- 选择回写式缓存磁盘的类型。
  - 使用非永久回写式缓存磁盘。如果选中此选项，则会在电源重启期间删除回写式缓存磁盘。重定向到该磁盘的任何数据都将丢失。如果 VM 的临时磁盘有足够的空间，它将用于托管回写式缓存磁盘以降低成本。创建目录后，可以检查已预配的计算机是否使用临时磁盘。为此，请单击目录并验证模板属性选项卡上的信息。如果使用临时磁盘，您将看到非永久回写式缓存磁盘，其值为是（使用 **VM** 的临时磁盘）。否则，您将看到非永久回写式缓存磁盘，其值为否（不使用 **VM** 的临时磁盘）。
  - 使用永久回写式缓存磁盘。如果选中此选项，回写式缓存磁盘将为已预配的 VM 保留。启用此选项会增加存储成本。
- 选择是否在电源重启期间为 VDA 保留 VM 和系统磁盘。

在电源重启期间保留 **VM** 和系统磁盘。当您选择“启用回写式缓存”时可用。默认情况下，VM 和系统磁盘会在关机时删除，并在启动时重新创建。如果要缩短 VM 重新启动时间，请选择此选项。请记住，启用此选项还会增加存储成本。

- 选择是否启用存储成本节约。如果已启用，则可以在 VM 关闭时将存储磁盘降级为标准 HDD，从而节省存储成本。VM 在重新启动时切换到其原始设置。该选项同时适用于存储和回写式缓存磁盘。或者，也可以使用 PowerShell。请参阅[关闭 VM 时将存储类型更改为较低的层](#)。

注意：

在 VM 关闭期间，Microsoft 对更改存储类型施加了限制。Microsoft 将来也有可能阻止更改存储类型。有关详细信息，请参阅这篇 [Microsoft 文章](#)。

- 选择是否加密该目录中计算机上的数据以及使用哪个加密密钥。使用客户管理密钥 (CMK) 进行服务器端加密允许您在托管磁盘级别管理加密并保护目录中计算机上的数据。默认设置继承自计算机配置文件或主映像，配置文件优先：
  - 如果您使用带有 CMK 的计算机配置文件，则会自动选择“使用以下密钥加密每台计算机上的数据”选项，默认为计算机配置文件中的密钥。
  - 如果您使用带有平台管理密钥 (PMK) 的计算机配置文件并且主映像已加密 CMK，则会自动选择使用以下密钥加密每台计算机上的数据选项，默认为主映像中的密钥。
  - 如果您未使用计算机配置文件且主映像已加密 CMK，则会自动选择使用以下密钥加密每台计算机上的数据选项，默认为主映像中的密钥。

有关详细信息，请参阅 Azure 服务器端加密。

7. 在资源组页面上，选择是创建资源组还是使用现有组。

- 如果选择创建资源组，请选择下一步。
- 如果选择使用现有资源组，请从可用的预配资源组列表中选择组。

注意：

请选择足够的组以容纳您要在目录中创建的计算机。如果选择太少，系统将显示一条消息。如果您计划以后向目录添加更多 VM，则您可能希望选择的数量多于所需的最低数量。创建目录后，无法向目录添加更多资源组。

有关详细信息，请参阅 Azure 资源组。

8. 在计算机标识页面上，选择标识类型并为该目录中的计算机配置标识。如果您选择 VM 为已加入 **Azure Active Directory**，则可以将其添加到 Azure AD 安全组。详细步骤如下所示：

- a) 在标识类型字段中，选择已加入 **Azure Active Directory**。此时将显示 **Azure AD 安全组 (可选)** 选项。
- b) 单击 **Azure AD 安全组: 新建**。
- c) 输入组名称，然后单击创建。
- d) 请按照屏幕上的说明登录 Azure。

如果 Azure 中不存在组名称，则会出现绿色图标。否则，将显示一条错误消息，要求您输入新名称。
- e) 要将安全组添加到已分配的安全组，请选择“以成员身份加入已分配的安全组”，然后单击“选择组”以选择要加入的已分配组。
- f) 输入虚拟机的计算机帐户命名方案。

创建目录后，Citrix DaaS 代表您访问 Azure 并为该组创建安全组和动态成员身份规则。根据该规则，使用在此目录中指定的命名方案的 VM 将自动添加到安全组中。

将使用不同命名方案的 VM 添加到此目录需要您登录 Azure。然后，Citrix DaaS 可以访问 Azure 并根据新命名方案创建动态成员身份规则。

删除此目录时，从 Azure 中删除安全组还需要登录 Azure。

注意：

要在创建目录后重命名 Azure AD 安全组，请编辑目录并从左侧导航栏转到 **Azure AD** 安全组。Azure AD 安全组的名称不得包含以下字符：@ "\ / ; : # . \* ? = < > | [ ] ( )'。

- 域凭据和摘要页面不包含 Azure 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。

完成向导。

## 创建 Azure 模板规范

您可以在 Azure 门户中创建 Azure 模板规范，然后在 完整配置 界面和 PowerShell 命令中使用它来创建或更新 MCS 计算机目录。

要为现有 VM 创建 Azure 模板规范，请执行以下操作：

1. 转至 Azure 门户。选择一个资源组，然后选择 VM 和网络接口。在顶部的 ... 菜单中，单击导出模板。
2. 如果要为目录预配创建模板规范，请清除包括参数复选框。
3. 单击添加到库以便稍后修改模板规范。
4. 在导入模板页面上，输入所需信息，例如名称、订阅、资源组、位置和版本。单击下一步：编辑模板。
5. 如果要预配目录，还需要将网络接口作为独立资源。因此，必须删除在模板规范中指定的任何 `dependsOn`。  
例如：

```
1  "dependsOn": [  
2  "[resourceId('Microsoft.Network/networkInterfaces', 'tnic937')]"  
3  ],  
4  <!--NeedCopy-->
```

6. 创建检查 + 创建并创建模板规范。
7. 在模板规格页面上，验证您创建的模板规范。单击模板规范。在左侧面板上，单击版本。
8. 可以通过单击创建新版本来创建新版本。指定新版本号，更改当前的模板规范，然后单击检查 + 创建以创建模板规范的新版本。

可以使用以下 PowerShell 命令获取有关模板规范和模板版本的信息：

- 要获取有关模板规范的信息，请运行：

```
1 get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.  
  resourcegroup\bggTemplateSpec.templatespec  
2 <!--NeedCopy-->
```

- 要获取有关模板规范版本的信息，请运行：

```
1 get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.  
  resourcegroup\bggTemplateSpec.templatespec\bgg1.0.  
  templatespecversion  
2 <!--NeedCopy-->
```

在创建或更新目录时使用模板规范

可以使用模板规范作为计算机配置文件输入来创建或更新 MCS 计算机目录。为此，您可以使用“完整配置”界面或 PowerShell 命令。

- 使用完整配置界面：请参阅在完整配置界面中使用 Azure Resource Manager 映像创建计算机目录。
- 对于 PowerShell：请参阅使用 PowerShell 创建或更新目录时使用模板规范

将计算机预配到指定的可用性区域中

可以将计算机预配到 Azure 环境中的特定可用性区域中。可以使用“完整配置”界面或 PowerShell 来实现这一目标。

注意：

如果未指定任何区域，MCS 将允许 Azure 将计算机放置在区域内。如果指定了多个区域，MCS 会在这些区域之间随机分配计算机。

在完整配置界面中配置可用性区域

创建计算机目录时，可以指定要预配计算机的可用性区域。在虚拟机页面上，选择要在其中创建计算机的一个或多个可用性区域。

没有可用性区域的原因有两个：区域没有可用性区域或选定的计算机大小不可用。

有关使用 PowerShell 命令进行配置的信息，请参阅使用 PowerShell 配置可用性区域。

## Azure 临时磁盘

[Azure 临时磁盘](#) 允许您重新调整缓存磁盘或临时磁盘的用途，以便为启用了 Azure 的虚拟机存储操作系统磁盘。此功能对于需要的 SSD 磁盘的性能高于标准 HDD 磁盘的 Azure 环境非常有用。有关使用 Azure 临时磁盘创建目录的信息，请参阅使用 Azure 临时磁盘创建目录。

注意：

永久目录不支持临时操作系统磁盘。

临时操作系统磁盘要求您的配置方案使用托管磁盘和 Azure Compute Gallery。有关详细信息，请参阅 [Azure 共享映像库](#)。

#### 存储临时操作系统临时磁盘

您可以选择将临时操作系统磁盘存储在 VM 临时磁盘或资源磁盘上。通过此功能，您可以将临时操作系统磁盘用于没有缓存或缓存不足的 VM。此类 VM 具有用于存储临时操作系统磁盘的临时磁盘或资源磁盘，例如 [Ddv4](#)。

请注意以下事项：

- 临时磁盘存储在 VM 缓存磁盘或 VM 临时（资源）磁盘中。除非缓存磁盘的大小不足以容纳操作系统磁盘的内容，否则缓存磁盘优先于临时磁盘。
- 对于更新，如果新映像大于缓存磁盘但小于临时磁盘，则会导致将临时操作系统磁盘替换为 VM 的临时磁盘。

#### Azure 临时磁盘和 Machine Creation Services (MCS) 存储优化 (MCS I/O)

无法同时启用 Azure 临时操作系统磁盘和 MCS I/O。

重要注意事项如下：

- 您无法创建同时启用了临时操作系统磁盘和 MCS I/O 的计算机目录。
- 在“计算机目录设置”向导中，如果在“存储和许可证类型”页面上选择 **Azure** 临时操作系统磁盘，则在“磁盘设置”页面上将无法获得回写缓存 磁盘设置 选项。

Machine Catalog Setup

✕

Machine Type

Machine Management

Desktop Experience

Master Image

Storage and License Types

Virtual Machines

NICs

Disk Settings

Resource Group

Machine Identities

Domain Credentials

Scopes

WEM (Optional)

Summary

Storage and License Types

Select the type of storage to use for this machine catalog. MCS configures premium and standard disks to use Locally Redundant Storage (LRS). LRS makes multiple synchronous copies of your disk data within a single data center. The storage type you select affects the machine sizes offered later in this wizard.

☐ Premium SSD (supports I/O-intensive workloads with significantly high throughput and low latency)

☐ Standard SSD

☐ Standard HDD

☒ Azure ephemeral OS disk

You can use Windows volume licenses to provision VMs in Azure at the base compute rate. To verify that your volume licensing agreement with Microsoft qualifies for the Azure base compute rate, consult Microsoft.

☒ Use my Windows Client licenses

☐ Use my Windows Server licenses

☐ Use Azure Windows Server licenses

☒ Place image in Azure Shared Image Gallery

?

Azure Shared Image Gallery settings

Ratio of virtual machines to image replicas:

1000

⬆

⬆

?

Maximum replica count:

10

⬆

⬆

?

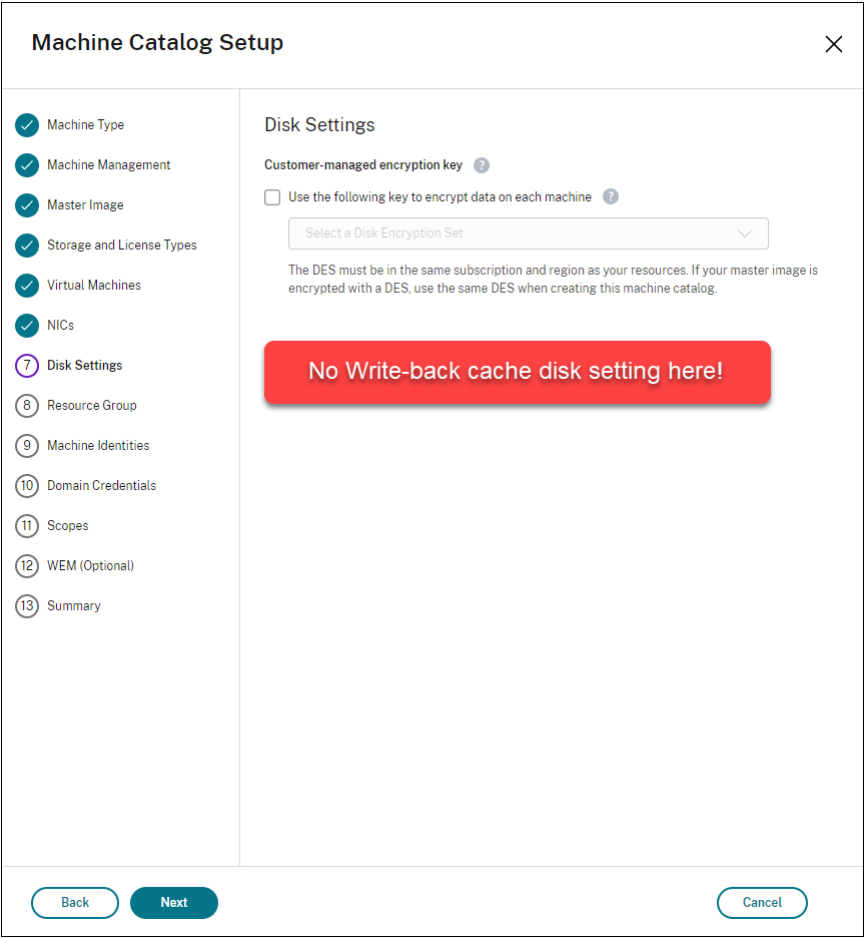
Back

Next

Cancel

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

391



- PowerShell 参数 (`UseWriteBackCache` 和 `UseEphemeralOsDisk`) 在 `New-ProvScheme` 或 `Set-ProvScheme` 中设置为 **true** 失败并显示正确的错误消息。
- 对于在启用了这两种功能的情况下创建的现有计算机目录，您仍然可以：
  - 更新计算机目录。
  - 添加或删除 VM。
  - 删除计算机目录。

## Azure Compute Gallery

使用 Azure Compute Gallery（前身为共享映像库）作为 Azure 中已配置的 MCS 计算机的已发布映像存储库。可以在该库中存储已发布的映像，以加快操作系统磁盘的创建和水化速度，从而缩短非永久 VM 的启动和应用程序启动时间。Azure Compute Gallery 包含以下三个元素：

- 库：映像存储在此位置。MCS 为每个计算机目录创建一个库。
- 库映像定义：此定义包括有关已发布的映像的信息（操作系统类型和状态、Azure 区域）。MCS 为目录创建的每个映像创建一个映像定义。

- 图库图像版本：Azure Compute Gallery 中的每个图像可以有多个版本，每个版本可以在不同的区域有多个副本。每个副本都是已发布的映像的完整副本。Citrix DaaS 根据目录中的计算机数量、配置的副本比率和配置的副本最大值，为每个映像创建一个 Standard\_LRS 映像版本（1.0.0 版），该版本在目录所在区域中具有恰当的副本数量。

注意：

Azure Compute Gallery 功能仅与托管磁盘兼容。它不适用于旧版计算机目录。

有关详细信息，请参阅 [Azure 共享映像库概述](#)。

### 从 Azure Compute Gallery 访问映像

选择用于创建计算机目录的映像时，可以选择在 Azure Compute Gallery 中创建的映像。这些映像显示在“计算机目录设置”向导的“映像”页面的映像列表中。

要显示这些图片，您必须：

1. 设置 Citrix DaaS。
2. 连接到 [Azure Resource Manager](#)。
3. 在 Azure 门户中，创建资源组。有关详细信息，请参阅[使用门户创建 Azure 共享映像库](#)。
4. 在资源组中，创建 Azure Compute Gallery。
5. 在 Azure Compute Gallery 中，创建映像定义。
6. 在映像定义中，创建映像版本。

有关配置 Azure Compute Gallery 的信息，请参阅[配置 Azure Compute Gallery](#)。

### Azure 临时磁盘有资格使用回写式缓存磁盘的条件

仅当满足以下所有条件时，才能将 Azure 临时磁盘用作回写式缓存磁盘：

- 回写式缓存磁盘必须非永久，因为 Azure 临时磁盘不适合静态数据。
- 所选 Azure VM 大小必须包含临时磁盘。
- 不需要启用临时操作系统磁盘。
- 接受以将回写式缓存文件放置在 Azure 临时磁盘上。
- Azure 临时磁盘大小必须大于（回写式缓存磁盘大小 + 页面文件的预留空间 + 1 GB 缓冲区空间）的总大小。

### 非永久回写式缓存磁盘场景

下表描述了在创建计算机目录时使用临时磁盘进行回写式缓存的三种不同场景。



场景	结果
使用临时磁盘进行回写式缓存的所有条件都得到满足。	WBC 文件 <code>mcsdif.vhdx</code> 放置在临时磁盘上。
临时磁盘空间不足，无法使用回写式缓存。	将创建一个 VHD 磁盘 “MCSWCDisk”，并将 WBC 文件 <code>mcsdif.vhdx</code> 放置在此磁盘上。
临时磁盘有足够的空间来使用回写缓存，但将 <code>UseTempDiskForWBC</code> 设置为 <code>false</code> 。	将创建一个 VHD 磁盘 “MCSWCDisk”，并将 WBC 文件 <code>mcsdif.vhdx</code> 放置在此磁盘上。

请参阅以下 PowerShell 主题：

- 使用非永久回写式缓存磁盘创建计算机目录
- 使用永久回写式缓存磁盘创建计算机目录

**Azure 服务器端加密**

Citrix DaaS 通过 Azure 密钥保管库支持 Azure 托管磁盘的客户托管加密密钥。通过此支持，您可以使用自己的加密密钥对计算机目录的托管磁盘进行加密，从而管理组织和合规性要求。有关详细信息，请参阅 [Azure 磁盘存储的服务器端加密](#)。

对托管磁盘使用此功能时：

- 要更改磁盘加密时使用的密钥，请更改 `DiskEncryptionSet` 中的当前密钥。与该 `DiskEncryptionSet` 关联的所有资源都将更改为使用新密钥加密。
- 禁用或删除密钥时，任何具有使用该密钥的磁盘的 VM 都会自动关闭。关闭后，除非再次启用该密钥或分配新密钥，否则 VM 将无法使用。使用该密钥的任何目录都无法打开，也无法向其中添加 VM。

使用客户管理的加密密钥时的重要注意事项

使用此功能时请注意以下事项：

- 与客户管理的密钥（Azure 密钥保管库、磁盘加密集、VM、磁盘和快照）相关的所有资源都必须位于同一订阅和区域中。
- 启用客户管理的加密密钥后，以后无法将其禁用。如果要禁用或删除客户管理的加密密钥，请将所有数据复制到不使用客户管理的加密密钥的其他托管磁盘。
- 使用服务器端加密和客户托管的密钥从加密的自定义映像创建的磁盘必须使用相同的客户管理的密钥进行加密。这些磁盘必须位于同一个订阅中。
- 使用服务器端加密和客户管理的密钥加密的磁盘创建的快照必须使用相同的客户管理的密钥进行加密。
- 使用客户管理的密钥加密的磁盘、快照和映像无法移动到其他资源组和订阅。

- 当前或之前使用 Azure 磁盘加密进行加密的托管磁盘不能使用客户管理的密钥进行加密。
- 有关每个区域的磁盘加密集的限制，请参阅 [Microsoft 站点](#)。

注意：

有关配置 Azure 服务器端加密的信息，请参阅[快速入门：使用 Azure 门户创建密钥保管库](#)。

### Azure 客户管理的加密密钥

创建计算机目录时，可以选择是否加密在目录中预配的计算机上的数据。通过使用客户管理的加密密钥的服务器端加密，您可以在托管磁盘级别管理加密，并保护目录中的计算机上的数据。磁盘加密集 (Disk Encryption Set, DES) 表示客户管理的密钥。要使用此功能，必须首先在 Azure 中创建 DES。DES 采用以下格式：

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryption`

从列表中选择 DES。所选择的 DES 必须与您的资源位于相同的订阅和区域。如果使用 DES 加密了映像，请在创建计算机目录时使用相同的 DES。创建目录后无法更改 DES。

如果使用加密密钥创建目录，然后在 Azure 中禁用相应的 DES，则无法再打开目录中的计算机的电源或者向其中添加计算机。

请参阅使用客户管理的密钥创建计算机目录。

### Azure 磁盘主机加密

可以创建具有主机加密功能的 MCS 计算机目录。目前，MCS 仅支持面向此功能的计算机配置文件工作流程。您可以使用 VM 或模板规范作为计算机配置文件的输入。

此加密方法不会通过 Azure 存储对数据进行加密。托管 VM 的服务器对数据进行加密，加密的数据随后会流经 Azure 存储服务器。因此，这种加密方法会对数据进行端到端加密。

限制：

主机上的 Azure 磁盘加密是：

- 并非所有 Azure 计算机大小都支持
- 与 Azure 磁盘加密不兼容

有关详细信息，请参阅：

- 创建具有主机加密功能的计算机目录。
- 从计算机配置文件中检索主机加密信息

## 托管磁盘上的双重加密

可以创建具有双重加密的计算机目录。使用此功能创建的任何目录都会同时使用平台和客户管理的密钥对所有磁盘服务器端进行加密。您拥有并维护 Azure Key Vault、加密密钥和磁盘加密集 (DES)。

双重加密是指平台端加密（默认）和客户管理的加密 (CMEK)。因此，如果您是高度安全敏感的客户，并且担心与任何加密算法、实现或密钥泄露相关的风险，则可以选择这种双重加密。永久操作系统和数据磁盘、快照和映像均使用双重加密进行静态加密。

### 注意：

- 您可以使用完整配置界面和 PowerShell 命令创建和更新采用双重加密的计算机目录。
- 可以使用非基于计算机配置文件的工作流程或基于计算机配置文件的工作流程来创建或更新具有双重加密的计算机目录。
- 如果您使用非基于计算机配置文件的工作流程来创建计算机目录，则可以重复使用存储的 [DiskEncryptionSetId](#)。
- 如果使用计算机配置文件，则可以使用 VM 或模板规范作为计算机配置文件输入。

### 限制

- 超级磁盘或 Premium SSD v2 磁盘不支持双重加密。
- 非托管磁盘不支持双重加密。
- 如果您禁用与目录关联的磁盘加密集密钥，则该目录的虚拟机将被禁用。
- 与客户管理的密钥（Azure 密钥保管库、磁盘加密集、VM、磁盘和快照）相关的所有资源都必须位于同一订阅和区域中。
- 每个订阅每个区域最多只能创建 50 个磁盘加密集。
- 无法使用其他 [DiskEncryptionSetId](#) 更新已包含 [DiskEncryptionSetId](#) 的计算机目录。

请参阅以下 PowerShell 主题：

- 使用双重加密创建计算机目录
- 将未加密的目录转换为使用双重加密
- 验证目录是否经过双重加密

## Azure 资源组

Azure 预配资源组提供了一种预配向用户提供应用程序和桌面的 VM 的方法。您可以创建 MCS 计算机目录时添加现有的空 Azure 资源组，也可以创建新资源组。有关 Azure 资源组的信息，请参阅 [Microsoft 文档](#)。

Azure 资源组使用情况

每个 Azure 资源组的虚拟机、托管磁盘、快照和映像数量都没有限制。（删除了每个 Azure 资源组每 800 个托管磁盘包含 240 个 VM 的限制。）

- 使用完整作用域服务主体创建计算机目录时，MCS 仅创建一个 Azure 资源组，并为目录使用该资源组。
- 使用窄作用域服务主体创建计算机目录时，必须为目录提供一个空的、预先创建的 Azure 资源组。

Azure 应用商店

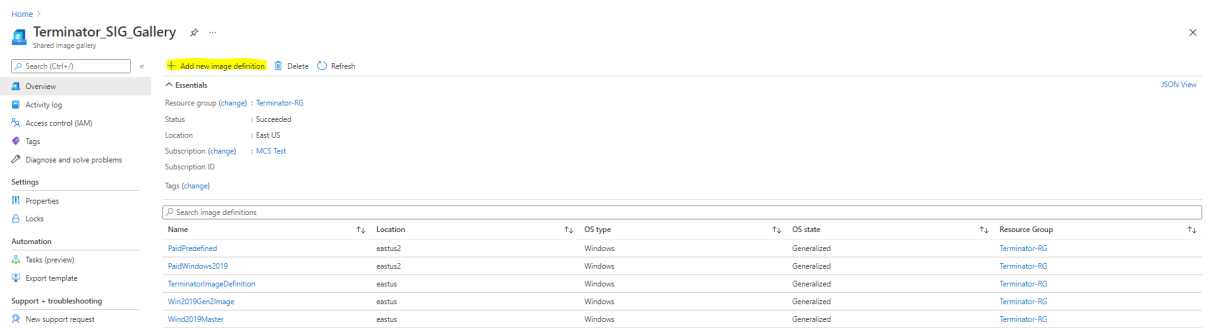
Citrix DaaS 支持在 Azure 上使用包含计划信息的主映像来创建计算机目录。有关详细信息，请参阅 [Microsoft Azure 应用商店](#)。

提示：

在 Azure 应用商店中找到的某些映像（例如标准 Windows Server 映像）不会附加计划信息。Citrix DaaS 功能适用于付费映像。

确保在 Azure Compute Gallery 中创建的映像包含 Azure 计划信息

使用本节中的步骤在完整配置界面中查看 Azure Compute Gallery 映像。这些映像可以选择用于主映像。要将映像放入 Azure Compute Gallery，请在库中创建映像定义。



在发布选项页面中，验证购买计划信息。

购买计划信息字段最初为空。请使用用于映像的购买计划信息填充这些字段。未能填充购买计划信息会导致计算机目录进程失败。

Microsoft Azure

Search resources, services, and docs (Ctrl+J)

Home > PaidPredefined (Terminator.SIG.Gallery/PaidPredefined) > Terminator.SIG.Gallery >

Add new image definition to shared image gallery

BasicVersionPublishing optionsTagsReview + create

Provide additional metadata about the image, including recommended VM specifications, and links to release notes and privacy policies.

Publishing meta data

EULA link

Description

Release notes URI

Privacy URI

Purchase plan name

Purchase plan publisher name

Purchase plan product name

VM deployment

Provide recommendations for VM specifications for this image. These recommendations are informational only, and do not constrain VM specification.

Recommended VM vCPUs

Recommended VM memory

Excluded disk types

Image definition end of life date

Review + createPreviousNext: Tags >

确认购买计划信息后，在定义中创建一个映像版本。这用作主映像。单击添加版本：

Home > Terminator.SIG.Gallery >

PaidPredefined (Terminator.SIG.Gallery/PaidPredefined)

Image definition

Search (Ctrl+J)

+ Create VM + Create VMSS Delete Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Image versions

Configuration

Properties

Locks

Automation

Tasks (preview)

Export template

Support + troubleshooting

New support request

Essentials

Resource group (change) : Terminator-RG

Location (change) : East US 2

Subscription (change) : MCS Test

Subscription ID :

Status : Succeeded

Tags (change) :

Shared image gallery : Terminator.SIG.Gallery

Operating system : Windows

Operating system state : Generalized

Publisher : Offer : SKU : PaidPublisher2 : PaidOffer2 : PaidSKU2

JSON View

PropertiesGet startedImage versions

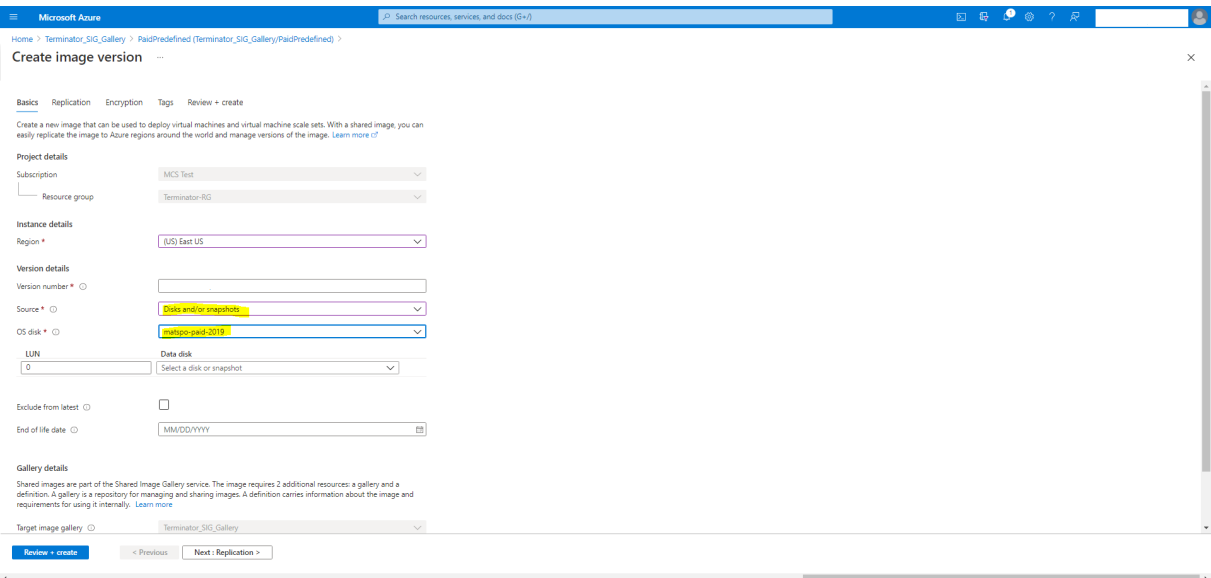
Filter by number...

Showing 1 of 1 image versions

Add versionDelete

Number	Provisioning State	Published date	Target regions	Replication status	Create VM from version
1.0.0	Succeeded	7/7/2021, 2:13:04 PM	East US	Completed	Create VM

在版本详细信息部分中，选择映像快照或托管磁盘作为源：



预配安装了 **Azure Monitor** 代理的目录 **VM**

Azure Monitor 是一项服务，可用于收集、分析和处理来自 Azure 和本地环境的遥测数据。

Azure Monitor 代理 (AMA) 从虚拟机等计算资源收集监视数据，并将数据交付给 Azure Monitor。它目前支持收集事件日志、系统日志和性能指标，并将其发送到 Azure Monitor 指标和 Azure Monitor 日志数据源。

要通过唯一标识监视数据中的 VM 来启用监视，您可以预配安装了 AMA 作为扩展程序的 MCS 计算机目录的 VM。

要求

- 权限：请确保您拥有[关于 Azure 权限](#)中指定的最低 Azure 权限以及以下使用 Azure Monitor 的权限：
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`
  - `Microsoft.Insights/dataCollectionRuleAssociations/write`
  - `Microsoft.Insights/DataCollectionRules/Read`
- 数据收集规则：在 Azure 门户中设置数据收集规则。有关设置 DCR 的信息，请参阅[创建数据收集规则](#)。DCR 是特定于平台的（Windows 或 Linux）。请务必根据所需平台创建 DCR。  
AMA 使用数据收集规则 (DCR) 来管理 VM 等资源与数据源（例如 Azure Monitor 指标和 Azure Monitor 日志）之间的映射。
- 默认工作区：在 Azure 门户中创建工作区。有关创建工作区的信息，请参阅[创建日志分析工作区](#)。当您收集日志和数据时，信息存储在工作区中。工作区具有唯一的工作区 ID 和资源 ID。对于给定的资源组，工作区名称必须唯一。创建工作区后，请配置数据源和解决方案以将其数据存储在在工作区中。

- 将 Monitor 扩展程序列入白名单: 扩展程序 `AzureMonitorWindowsAgent` 和 `AzureMonitorLinuxAgent` 是 Citrix 定义的白名单扩展程序。要查看列入白名单的扩展列表, 请使用 PowerShell 命令 `Get-ProvMetadataConfiguration`。
- 主映像: Microsoft 建议在使用现有计算机创建新计算机之前从现有计算机中删除扩展程序。如果不删除扩展程序, 可能会导致出现剩余文件和意外行为。有关详细信息, 请参阅[如果 VM 是从现有 VM 重新创建的](#)。

有关使用 PowerShell 创建启用 AMA 的目录的信息, 请参阅[配置启用 AMA 的目录虚拟机](#)。

## Azure 机密 VM (预览版)

Azure 机密计算虚拟机确保您的虚拟桌面在内存中经过加密并在使用中受到保护。

您可以使用 MCS 创建包含 Azure 机密 VM 的目录。必须使用计算机配置文件工作流程来创建此类目录。您可以将 VM 和 ARM 模板规范用作计算机配置文件输入。

### 机密 VM 的重要注意事项

支持的虚拟机大小和使用机密 VM 创建计算机目录的重要注意事项如下:

- 支持的 VM 大小: 机密 VM 支持以下 VM 大小:
  - DCasv5 系列
  - DCadsv5 系列
  - ECasv5 系列
  - ECadsv5 系列
- 使用机密 VM 创建计算机目录。
  - 您可以使用完整配置界面和 PowerShell 命令创建包含 Azure 机密 VM 的计算机目录。
  - 必须使用基于计算机配置文件的工作流程来创建包含 Azure 机密 VM 的计算机目录。您可以使用 VM 或模板规格作为计算机配置文件输入。
  - 必须使用相同的机密安全类型启用主映像和计算机配置文件输入。安全类型是:
    - \* VMGuestStateOnly: 仅加密了 VM 来宾状态的机密 VM
    - \* DiskWithVMGuestState: 机密 VM, 操作系统磁盘和 VM 来宾状态均使用平台管理密钥或客户管理密钥进行加密。普通操作系统磁盘和临时操作系统磁盘均可加密。
  - 您可以使用 `AdditionalData` 参数获取各种资源类型的机密 VM 信息, 例如托管磁盘、快照、Azure Compute Gallery 映像、VM 和 ARM 模板规范。例如:

```
1 PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork
   \image.folder\username-dev-testing-rg.resourcegroup\
   username-dev-tsvda.vm).AdditionalData
2 <!--NeedCopy-->
```

其他数据字段是：

- ★ DiskSecurityType
- ★ ConfidentialVMDiskEncryptionSetId
- ★ DiskSecurityProfiles

要获取计算机大小的机密计算属性，请运行以下命令：  
`(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

附加数据字段是 `ConfidentialComputingType`。

- 您不能将主映像或计算机配置文件从机密安全类型更改为非机密安全类型，或从非机密安全类型更改为机密安全类型。
- 对于任何不正确的配置，您都会收到相应的错误消息。

### 使用机密 **VM** 创建计算机目录

1. 创建启用机密 VM 的主映像。请参阅 Azure 门户中的[快速入门：使用 ARM 模板部署机密 VM](#)和[快速入门：在 AMD 上创建机密 VM](#)以创建主 VM。
2. 使用主 VM 作为计算机配置文件或创建 Azure 模板规范。有关创建模板规范的信息，请参阅[创建 Azure 模板规范](#)。
3. 使用完整配置界面或 PowerShell 命令创建基于计算机配置文件的计算机目录。

注意：

确保使用相同的机密安全类型启用主映像和计算机配置文件输入。

### 使用 **PowerShell**

本部分内容详细介绍了如何使用 PowerShell 执行以下任务：

- 使用 [PowerShell](#) 在创建或更新目录时使用模板规范
- 启用 [Azure 虚拟机扩展](#)
- 支持受信任启动的计算机目录
- 使用计算机配置文件属性值
- 使用 [PowerShell](#) 配置可用性区域
- 在 [Azure 专用主机](#)上配置 VM
- 配置存储类型
- 启用区域冗余存储
- 从计算机配置文件中捕获 VM 和 NIC 上的诊断设置
- 验证 Windows 许可证



- [配置 Linux 许可证](#)
- [使用 Azure 临时磁盘创建计算机目录](#)
- [配置 Azure Compute Gallery](#)
- [创建或更新每个 VM 有多个 NIC 的目录](#)
- [使用非永久回写式缓存磁盘创建计算机目录](#)
- [使用永久回写式缓存磁盘创建计算机目录](#)
- [使用 MCSIO 提高启动性能](#)
- [使用客户管理的加密密钥创建计算机目录](#)
- [创建具有主机加密功能的计算机目录](#)
- [使用双重加密创建计算机目录](#)
- [页面文件位置](#)
- [更新页面文件设置](#)
- [配置启用 AMA 的目录虚拟机](#)
- [使用 Azure 现成 VM 创建目录](#)
- [复制所有资源上的标记](#)

### 使用 **PowerShell** 在创建或更新目录时使用模板规范

可以使用模板规范作为计算机配置文件输入来创建或更新 MCS 计算机目录。为此，您可以使用“完整配置”界面或 PowerShell 命令。

有关完整配置界面，请参阅在完整配置界面中使用 Azure Resource Manager 映像创建计算机目录。

使用 PowerShell 命令：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*`。
3. 创建或更新目录。

- 要创建目录，请执行以下操作：

- a) 对作为计算机配置文件输入的模板规范使用 `New-ProvScheme` 命令。例如：

```
1 New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/  
  image.folder/fgthj.resourcegroup/nab-ws-  
  vda_OsDisk_1_xxxxxxxxxxa.manageddisk"  
2 MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.  
  folder/fgthj.resourcegroup/test.templatespec/V1.  
  templatespecversion"  
3 -ProvisioningSchemeName <String>  
4 -HostingUnitName <String>  
5 -IdentityPoolName <String>  
6 [-ServiceOffering <String>][-CustomProperties <String>]  
7 [<CommonParameters>]  
8 <!--NeedCopy-->
```

- b) 完成目录的创建。

- 要更新目录，请对作为计算机配置文件输入的模板规范使用 `Set-ProvScheme` 命令。例如：

```
1 Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
   Us.region/vm.folder/MasterDisk.vm'
2 MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.
   folder/fgthj.resourcegroup/testing.templatespec/V1.
   templatespecversion'
3 [-ProvisioningSchemeName] <String>
4 [-CustomProperties <String>][--ServiceOffering <String>] [--
   PassThru]
5 [<CommonParameters>]
6 <!--NeedCopy-->
```

## 启用 **Azure** 虚拟机扩展

选择 ARM 模板规范后，运行以下 PowerShell 命令以使用 Azure VM 扩展：

- 要查看支持的 Azure VM 扩展列表，请执行以下操作：`Get-ProvMetadataConfiguration`
- 要添加更多 VM 扩展，请执行以下操作：`Add-ProvMetadataConfiguration`。例如，`Add-ProvMetadataConfiguration -PluginType "AzureRM"-ConfigurationName "Extension"-ConfigurationValue "CustomScriptExtension"`

如果您尝试添加以下任一项，命令将失败并显示错误消息：

- Citrix 定义的扩展名。
  - 现有的用户定义扩展。
  - 不支持的配置密钥。目前，支持的配置密钥是 `Extension`。
- 要从列表中删除扩展名，请执行以下操作：`Remove-ProvMetadataConfiguration`。您可以移除已添加的扩展。

## 支持受信任启动的计算机目录

要使用受信任启动成功创建计算机目录，请使用：

- 具有受信任启动功能的计算机配置文件
- 支持受信任启动的 VM 大小
- 支持受信任启动的 Windows VM 版本。目前，Windows 10、Windows 11、2016、2019 和 2022 支持受信任启动。

### 重要：

MCS 支持使用启用了受信任启动的 VM 创建新目录。但是，要更新现有的永久目录和现有的 VM，必须使用 Azure

门户。无法更新非永久目录的受信任启动。有关详细信息，请参阅 Microsoft 文档 [Enable Trusted launch on existing Azure VMs](#)（在现有 Azure VM 上启用受信任启动）。

要查看 Citrix DaaS 提供的清单项目，并确定虚拟机大小是否支持可信启动，请运行以下命令：

1. 打开 PowerShell 窗口。
2. 运行 **asnp citrix\*** 以加载特定于 Citrix 的 PowerShell 模块。
3. 运行以下命令：

```
1 $s = (ls XDHyp:\HostingUnits<name of hosting unit>\serviceoffering
   .folder"<VM size>".serviceoffering)
2 <!--NeedCopy-->
```

4. 运行 `$s | select -ExpandProperty Additionaldata`
5. 检查 `SupportsTrustedLaunch` 属性的值。

- 如果 `SupportsTrustedLaunch` 设置为 **True**，则 VM 大小支持受信任启动。
- 如果 `SupportsTrustedLaunch` 设置为 **False**，则 VM 大小不支持受信任启动。

根据 Azure 的 PowerShell，您可以使用以下命令来确定支持受信任启动的 VM 大小：

```
1 (Get-AzComputeResourceSku | where {
2   $_.Locations.Contains($region) -and ($_.Name -eq "<VM size>") }
3 ) [0].Capabilities
4 <!--NeedCopy-->
```

以下示例描述了运行 Azure PowerShell 命令后虚拟机大小是否支持可信启动。

- 示例 1：如果 Azure VM 仅支持第 1 代，则该 VM 不支持受信任启动。因此，运行 Azure PowerShell 命令后不会显示 `TrustedLaunchDisabled` 功能。
- 示例 2：如果 Azure VM 仅支持第 2 代，并且 `TrustedLaunchDisabled` 功能设置为 **True**，则受信任启动不支持第 2 代 VM 大小。
- 示例 3：如果 Azure VM 仅支持第 2 代，并且在运行 PowerShell 命令后未显示 `TrustedLaunchDisabled` 功能，则受信任启动时支持第 2 代 VM 大小。

有关 Azure 虚拟机受信任启动的详细信息，请参阅 Microsoft 文档 [Trusted launch for Azure virtual machines](#) (Azure 虚拟机的受信任启动)。

#### 使用受信任启动功能创建计算机目录

1. 创建启用了受信任启动的主映像。请参阅 Microsoft 文档 [Trusted launch VM Images](#)（受信任启动 VM 映像）。
2. 创建安全类型为受信任启动虚拟机的 VM 或模板规范。有关创建 VM 或模板规范的详细信息，请参阅 Microsoft 文档 [Deploy a trusted launch VM](#)（部署受信任启动 VM）。

3. 使用“完整配置”界面或 PowerShell 创建计算机目录。

- 如果要使用“完整配置”界面，请参阅在“完整配置”界面中使用 Azure Resource Manager 映像创建计算机目录。
- 如果要使用 PowerShell 命令，请使用带有 VM 或模板规范的 New-ProvScheme 命令作为计算机配置文件输入。有关创建目录的命令的完整列表，请参阅创建目录。

使用 VM 作为计算机配置文件输入的 New-ProvScheme 示例：

```
1 New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
  IdentityPoolName "name" -InitialBatchSizeHint 1
2 -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
  resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
3 -MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.
  folder<def.resourcegroup><machine profile vm.vm>"
4 -ProvisioningSchemeName <String>
5 -HostingUnitName <String>
6 -IdentityPoolName <String>
7 [-ServiceOffering <String>][-CustomProperties <String>]
8 [<CommonParameters>]
9 <!--NeedCopy-->
```

使用模板规范作为计算机配置文件输入的 New-ProvScheme 示例：

```
1 New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
  IdentityPoolName "name" -InitialBatchSizeHint 1
2 -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
  resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
3 MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
  folder/fgthj.resourcegroup/test.templatespec/V1.
  templatespecversion"
4 -ProvisioningSchemeName <String>
5 -HostingUnitName <String>
6 -IdentityPoolName <String>
7 [-ServiceOffering <String>][-CustomProperties <String>]
8 [<CommonParameters>]
9 <!--NeedCopy-->
```

使用受信任启动创建计算机目录时出错

在以下情况下使用受信任启动创建计算机目录时，您会遇到相应的错误：

场景	错误
如果您在创建非托管目录时选择了计算机配置文件	MachineProfileNotSupportedForUnmanagedCata

场景	错误
如果您在创建以非托管磁盘作为主映像的目录时选择支持受信任启动的计算机配置文件	<code>SecurityTypeNotSupportedForUnmanagedDisk</code>
如果您在使用以受信任启动作为安全类型的主映像源创建托管目录时未选择计算机配置文件	<code>MachineProfileNotFoundForTrustedLaunchMasterImage</code>
如果您选择安全类型与主映像的安全类型不同的计算机配置文件	<code>SecurityTypeConflictBetweenMasterImageAndMachineProfile</code>
如果您选择的 VM 大小不支持受信任启动，但在创建目录时使用支持受信任启动的主映像	<code>MachineSizeNotSupportTrustedLaunch</code>

使用计算机配置文件属性值

计算机目录使用在自定义属性中定义的以下属性：

- 可用性区域
- 专用主机组 ID
- 磁盘加密 ID
- 操作系统类型
- 许可证类型
- 存储类型

如果未显式定义这些自定义属性，则从 ARM 模板规范或 VM（以用作计算机配置文件为准）中设置属性值。此外，如果未指定 `ServiceOffering`，则从计算机配置文件进行设置。

注意：

如果计算机配置文件中缺少某些属性，并且未在自定义属性中定义，则在适用的情况下将使用这些属性的默认值。

以下部分描述了 `CustomProperties` 从 `MachineProfile` 派生定义的所有属性或值时 `New-ProvScheme` 和 `Set-ProvScheme` 下的某些方案。

- `New-ProvScheme` 方案
  - `MachineProfile` 具有所有属性，但未定义 `CustomProperties`。示例:

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"
```

以下值被设置为目录的自定义属性：

```
1 Get-ProvScheme | select CustomProperties
```

```

2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<mpA-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
    -value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
    "<mpA-value>"/>
6  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
    " Value="<mpA-value>"/>
7  <Property xsi:type="StringProperty" Name="
    DedicatedHostGroupId" Value="<mpA-value>"/>
8  <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
    value>"/>
9  </CustomProperties>
10 <!--NeedCopy-->

```

- MachineProfile 有一些属性，但未定义 CustomProperties。示例：MachineProfile 只有 LicenseType 和 OSType。

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"
```

以下值被设置为目录的自定义属性：

```

1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
    -value>"/>
4  <Property xsi:type="StringProperty" Name="LicenseType" Value=
    "<mpA-value>"/>
5  </CustomProperties>
6  <!--NeedCopy-->

```

- MachineProfile 和 CustomProperties 定义了所有属性。示例：

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
$CustomPropertiesA
```

自定义属性优先。以下值被设置为目录的自定义属性：

```

1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<CustomPropertiesA-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
    CustomPropertiesA-value>"/>

```

```

5 <Property xsi:type="StringProperty" Name="LicenseType" Value=
  "<CustomPropertiesA-value>"/>
6 <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
  " Value="<CustomPropertiesA-value>"/>
7 <Property xsi:type="StringProperty" Name="
  DedicatedHostGroupId" Value="<CustomPropertiesA-value>"/>
8 <Property xsi:type="StringProperty" Name="Zones" Value="<
  CustomPropertiesA-value>"/>
9 </CustomProperties>
10 <!--NeedCopy-->

```

- 有些属性在 MachineProfile 中定义，有些属性在 CustomProperties 中定义。示例：

- \* CustomProperties 定义 LicenseType 和 StorageAccountType
- \* MachineProfile 定义 LicenseType、OsType 和区域

```

New-ProvScheme -MachineProfile "XDHy:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
$CustomPropertiesA

```

以下值被设置为目录的自定义属性：

```

1 Get-ProvScheme | select CustomProperties
2 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/
  XMLSchema-instance">
3 <Property xsi:type="StringProperty" Name="StorageAccountType"
  Value="<CustomPropertiesA-value>"/>
4 <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
  -value>"/>
5 <Property xsi:type="StringProperty" Name="LicenseType" Value=
  "<CustomPropertiesA-value>"/>
6 <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
  value>"/>
7 </CustomProperties>
8 <!--NeedCopy-->

```

- 有些属性在 MachineProfile 中定义，有些属性在 CustomProperties 中定义。此外，未定义 ServiceOffering。示例：

- \* CustomProperties 定义 StorageType
- \* MachineProfile 定义 LicenseType

```

1 New-ProvScheme -MachineProfile "XDHy:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"
2 -ServiceOffering "XDHy:\HostingUnits\azureunit\
  serviceoffering.folder<explicit-machine-size>.
  serviceoffering"
3 <!--NeedCopy-->

```

以下值被设置为目录的自定义属性：

```

1 Get-ProvScheme | select ServiceOffering
2 serviceoffering.folder<explicit-machine-size>.serviceoffering
3
4 Get-ProvScheme | select CustomProperties
5 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
6   <Property xsi:type="StringProperty" Name="StorageAccountType"
   Value="explicit-storage-type"/>
7   <Property xsi:type="StringProperty" Name="LicenseType" Value=
   "value-from-machineprofile"/>
8 </CustomProperties>
9 <!--NeedCopy-->

```

- 如果 OsType 既不在 CustomProperties 中，也不在 MachineProfile 中，那么：

- ★ 该值将从主映像中读取。
- ★ 如果主映像是非托管磁盘，则 OsType 设置为 Windows。示例：

```

New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"-MasterImageVM
"XDHyp:\HostingUnits\azureunit\image.folder\linux-master-
image.manageddisk"

```

主映像中的值将写入自定义属性，在本例中为 Linux。

```

1 Get-ProvScheme | select CustomProperties
2 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
3   <Property xsi:type="StringProperty" Name="OSType" Value="
   Linux"/>
4 </CustomProperties>
5 <!--NeedCopy-->

```

#### • Set-ProvScheme 方案

- 包含以下对象的现有目录：

- ★ StorageAccountType 和 OsType 的 CustomProperties
- ★ 用于定义区域的 MachineProfile mpA.vm

- 更新：

- ★ 用于定义 StorageAccountType 的 MachineProfile mpB.vm
- ★ 用于定义 LicenseType 和 OsType 的一组新自定义属性 \$CustomPropertiesB

```

Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpB.vm"-CustomProperties
$CustomPropertiesB

```



以下值被设置为目录的自定义属性：

```

1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
   Value="<mpB-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
   CustomPropertiesB-value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
   "<CustomPropertiesB-value>"/>
6  </CustomProperties>
7  <!--NeedCopy-->

```

- 包含以下对象的现有目录：
  - \* `StorageAccountType`和 `OsType` 的 `CustomProperties`
  - \* 用于定义 `StorageAccountType` 和 `LicenseType` 的 `MachineProfile mpA.vm`
- 更新：
  - \* 用于定义 `StorageAccountType` 和 `OsType` 的一组新自定义属性 `$CustomPropertiesB`。

`Set-ProvScheme -CustomProperties $CustomPropertiesB`

以下值被设置为目录的自定义属性：

```

1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
   Value="<CustomPropertiesB-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
   CustomPropertiesB-value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
   "<mp-A-value>"/>
6  </CustomProperties>
7  <!--NeedCopy-->

```

- 包含以下对象的现有目录：
  - \* `StorageAccountType`和 `OsType` 的 `CustomProperties`
  - \* 用于定义区域的 `MachineProfile mpA.vm`
- 更新：
  - \* 用于定义 `StorageAccountType` 和 `LicenseType` 的 `MachineProfile mpB.vm`
  - \* 未指定 `ServiceOffering`

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit  
 \machineprofile.folder\azure.resourcegroup\mpB.vm"`

以下值被设置为目录的自定义属性：

```

1  Get-ProvScheme | select ServiceOffering
2  serviceoffering.folder<value-from-machineprofile>.
   serviceoffering
3
4  Get-ProvScheme | select CustomProperties
5  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
6  <Property xsi:type="StringProperty" Name="StorageAccountType"
   Value="<mpB-value>"/>
7  <Property xsi:type="StringProperty" Name="OSType" Value="<
   prior-CustomProperties-value>"/>
8  <Property xsi:type="StringProperty" Name="LicenseType" Value=
   "<mpB-value>"/>
9  </CustomProperties>
10 <!--NeedCopy-->

```

## 使用 PowerShell 配置可用性区域

使用 PowerShell，您可以使用 `Get-Item` 查看 Citrix DaaS 产品清单项目。例如，要查看美国东部地区 `Standard_B1ls` 服务产品，请执行以下操作：

```

1  $serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-
   name\East US.region\serviceoffering.folder\Standard_B1ls.
   serviceoffering"
2  <!--NeedCopy-->

```

要查看区域，请使用该项目的 `AdditionalData` 参数：

`$serviceOffering.AdditionalData`

如果未指定可用性区域，计算机的预配方式没有任何变化。

要通过 PowerShell 配置可用性区域，请使用随 `New-ProvScheme` 操作提供的区域自定义属性。区域属性定义了要在其中预配计算机的可用性区域列表。这些区域可以包括一个或多个可用性区域。例如，`<Property xsi:type="StringProperty" Name="Zones" Value="1, 3"/>` 对于区域 1 和 3。

使用 `Set-ProvScheme` 命令可更新预配方案的区域。

如果提供的区域无效，则不会更新预配方案，并且会显示一条错误消息，提供有关如何修复无效命令的说明。

提示：

如果指定了无效的自定义属性，则不会更新预配方案，并显示相关的错误消息。

同时使用主机组和 **Azure** 可用性区域的结果

根据自定义属性和主机组区域中指定的可用性区域，进行预先检查以评估计算机目录的创建是否成功。如果可用性区域自定义属性与主机组的区域不匹配，目录创建将失败。

有关通过 PowerShell 配置可用性区域的信息，请参阅[通过 PowerShell 配置可用性区域](#)。

有关 Azure 专用主机的信息，请参阅[Azure 专用主机](#)。

下表描述了可用性区域和主机组区域的各种组合，以及哪些组合会导致计算机目录的创建成功或失败。

主机组区域	自定义属性中的可用性区域	计算机目录创建结果
已指定。例如，主机组位于区域 1 中	未指定	成功。计算机在主机组的区域中创建
已指定。例如，主机组位于区域 1 中	与主机组区域相同的区域。例如，自定义属性中的区域设置为 1	成功。计算机在区域 1 中创建
已指定。例如，主机组位于区域 1 中	与主机组区域不同。例如，自定义属性中的 zone 设置为 2	由于指定的可用性区域与主机组的区域不匹配，因此，目录创建失败并在实施前检查期间出现相关错误
已指定。例如，主机组位于区域 1 中	指定了多个区域。例如，自定义属性中的区域设置为 1,2 或 2,3	由于指定的可用性区域与主机组的区域不匹配，因此，目录创建失败并在实施前检查期间出现相关错误
未指定。例如，主机组的区域是 <b>None</b>	未指定	由于指定的可用性区域与主机组的区域匹配（即没有区域），因此目录创建成功。计算机不是在任何区域中创建的
未指定。例如，主机组的区域是 <b>None</b>	已指定。例如，自定义属性中的区域设置为一个或多个区域	由于指定的可用性区域与主机组的区域不匹配，因此目录创建失败并会在预检检查期间出现相关错误

在 **Azure** 专用主机上配置 **VM**

可以使用 MCS 在 Azure 专用主机上预配 VM。在 Azure 专用主机上预配 VM 之前：

- 创建主机组。
- 在该主机组中创建主机。
- 确保有足够的主机容量用于创建目录和虚拟机。

可以创建具有通过以下 PowerShell 脚本定义的主机租赁的计算机目录：

```
1 New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
  xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi
  ="http://www.w3.org/2001/XMLSchema-instance">
```

```

2   <Property xsi:type="StringProperty" Name="HostGroupId" Value="
      myResourceGroup/myHostGroup" />
3   ...other Custom Properties...
4   </CustomProperties>
5   <!--NeedCopy-->

```

使用 MCS 在 Azure 专用主机上预配虚拟机时，请注意：

- 专用主机是目录属性，一旦创建了目录，则无法进行更改。Azure 当前不支持专用租赁。
- 使用 `HostGroupId` 参数时，需要在托管单元所在区域中预配置的 Azure 主机组。
- Azure 自动放置是必需的。此功能请求加载与主机组关联的订阅。有关详细信息，请参阅在 [Azure 专用主机上设置 VM 规模 - 公共预览版](#)。如果未启用自动放置，MCS 在目录创建过程中会引发错误。

## 配置存储类型

为 Azure 环境中使用 MCS 的虚拟机选择不同的存储类型。对于目标 VM，MCS 支持：

- 操作系统磁盘：高级 SSD、SSD 或 HDD
- 回写缓存磁盘：高级 SSD、SSD 或 HDD

使用这些存储类型时，请注意以下事项：

- 确保您的 VM 支持选定的存储类型。
- 如果您的配置使用 Azure 临时磁盘，则无法获得回写式缓存磁盘设置的选项。

提示：

`StorageType` 已针对操作系统类型和存储帐户进行了配置。`WBCKDiskStorageType` 已针对写回式缓存存储类型进行了配置。对于常见目录，`StorageType` 是必需的。如果未配置 `WBCKDiskStorageType`，则会将 `StorageType` 用作 `WBCKDiskStorageType` 的默认值。

如果未配置 `WBCKDiskStorageType`，则会将 `StorageType` 用作 `WBCKDiskStorageType` 的默认值

## 为 VM 配置存储类型

要为虚拟机配置存储类型，请使用 `New-ProvScheme` 中的 `StorageType` 参数。要将现有目录中 `StorageType` 参数的值更新为支持的存储类型之一，请使用 `Set-ProvScheme` 命令。

下面是预配方案中的一组示例 `CustomProperties` 参数：

```

1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
      <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
        machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
        instance">
2   <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />

```

```

3 <Property xsi:type="StringProperty" Name="StorageType" Value="
  Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="LicenseType" Value="
  Windows_Client" />
5 </CustomProperties>'
6 <!--NeedCopy-->

```

## 启用区域冗余存储

在创建目录期间，您可以选择区域冗余存储。它跨多个可用性区域同步复制您的 Azure 托管磁盘，这允许您利用其他区域中的冗余从一个区域中的故障中恢复。

可以在存储类型自定义属性中指定 **Premium\_ZRS** 和 **StandardSSD\_ZRS**。可以使用现有的自定义属性或通过 **MachineProfile** 模板设置 ZRS 存储。带 **-StartsNow** 和 **-DurationInMinutes -1** 参数的 **Set-ProvVMUpdateTimeWindow** 命令也支持 ZRS 存储。您可以将现有虚拟机从 LRS 更改为 ZRS 存储。

### 注意：

- **StartsNow** 表示计划的开始时间为当前时间。
- **DurationInMinutes** 负数（例如-1）表示计划的时间范围没有上限。

### 限制：

- 仅支持托管磁盘
- 仅支持高级和标准固态驱动器 (SSD)
- 不支持 **StorageTypeAtShutdown**
- 仅在某些地区可用。
- 大规模创建 ZRS 磁盘时，Azure 的性能会下降。因此，首次打开电源时，请小批量打开计算机（一次少于 300 台计算机）

## 将区域冗余存储设置为磁盘存储类型

您可以在初始目录创建期间选择区域冗余存储，也可以更新现有目录中的存储类型。

## 使用 PowerShell 命令选择区域冗余存储

使用 **New-ProvScheme** PowerShell 命令在 Azure 中创建新目录时，请使用 **Standard\_ZRS** 作为 **StorageAccountType** 中的值。

例如：

```

1 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
  StandardSSD_ZRS" />
2 <!--NeedCopy-->

```

设置此值时，它将由动态 API 进行验证，以确定该值是否可以正确使用。如果 ZRS 的使用对您的目录无效，则可能会出现以下异常：

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: StorageTypeAtShutdown 自定义属性不能用于 ZRS 存储。
- **StorageAccountTypeNotSupportedInRegion**: 如果您尝试在不支持 ZRS 的 Azure 区域中使用 ZRS 存储，则会出现此异常。
- **ZrsRequiresManagedDisks**: 区域冗余存储只能用于托管磁盘。

可以使用以下自定义属性设置磁盘存储类型：

- [StorageType](#)
- [WBCDiskStorageType](#)
- [IdentityDiskStorageType](#)

注意：

在创建目录期间，如果未设置自定义属性，则将使用计算机配置文件的操作系统磁盘 [StorageType](#)。

## 从计算机配置文件中捕获 VM 和 NIC 上的诊断设置

在创建计算机目录、更新现有计算机目录和更新现有 VM 过程中，可以从计算机配置文件中捕获 VM 和 NIC 上的诊断设置。

可以创建 VM 或模板规范作为计算机配置文件来源。

### 关键步骤

1. 在 Azure 中设置所需的 ID。必须在模板规范中提供这些 ID。
  - 存储帐户
  - 日志分析工作区
  - 采用标准分层定价的事件中心命名空间
2. 创建计算机配置文件源。
3. 创建新计算机目录、更新现有目录或更新现有 VM。

## 在 Azure 中设置所需的 ID

在 Azure 中设置以下选项之一：

- 存储帐户
- 日志分析工作区
- 采用标准分层定价的事件中心命名空间

**设置存储帐户** 在 Azure 中创建标准存储帐户。在模板规范中，将存储帐户的完整资源 ID 指定为 `storageAccountId`。

将 VM 设置为将数据记录到存储帐户后，可以在 `insights-metrics-pt1m` 容器下找到数据。

**设置日志分析工作区** 创建日志分析工作区。在模板规范中，将日志分析工作区的完整资源 ID 作为工作区 ID。

将 VM 设置为将数据记录到工作区后，即可在 Azure 中的“Logs”（日志）下查询数据。可以在 Azure 中的“Logs”（日志）下运行以下命令，以显示资源记录的所有指标的计数：

‘AzureMetrics

| summarize Count=count() by ResourceId# 创建 Microsoft Azure 目录

[创建计算机目录](#)介绍了用于创建计算机目录的向导。以下信息涵盖了特定于 Microsoft Azure Resource Manager 云环境的详细信息。

注意：

在创建 Microsoft Azure 目录之前，您需要完成创建与 Microsoft Azure 的连接。请参阅[与 Microsoft Azure 的连接](#)。

## 创建计算机目录

可以通过两种方式创建计算机目录：

- 完整配置界面。
- PowerShell。请参阅[创建目录](#)。有关如何使用 PowerShell 实现特定功能的信息，请参阅使用 PowerShell。

在完整配置界面中使用 **Azure Resource Manager** 映像创建计算机目录

此信息用于补充[创建计算机目录](#)中的指导信息。

映像可以是磁盘、快照或 Azure Compute Gallery 中用于在计算机目录中创建 VM 的映像定义的映像版本。

创建计算机目录之前，请在 Azure Resource Manager 中创建一个映像。

注意：

- 不建议使用非托管磁盘置备 VM。
- 不支持使用与在主机连接中配置的区域不同的主映像。使用 Azure Compute Gallery 将主映像复制到所需区域。

在映像准备期间，将在原始 VM 的基础上创建准备虚拟机 (VM)。此准备 VM 已与网络断开连接。为了断开网络与准备 VM 的连接，需要创建一个网络安全组以拒绝所有入站和出站流量。每个目录自动创建一次网络安全组。网络安全组的名称为 `<!JEKYLL@5180@0>`，其中 GUID 是随机生成的。例如，`<!JEKYLL@5180@1>`。

在计算机目录创建向导中，执行以下操作：

1. 计算机类型和计算机管理页面不包含 Azure 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。
2. 在映像页面上，选择要用作目录中所有计算机的主映像的映像。此时将出现选择映像向导。请按照以下步骤选择图片：

- a) (仅适用于使用租户内部或租户间共享映像配置的连接) 选择映像所在的订阅。
- b) 选择资源组。
- c) 导航到 Azure 托管磁盘、Azure Compute Gallery 或 Azure 映像版本。

选择映像时，请注意以下事项：

- 验证映像上是否安装了 Citrix VDA。
- 如果选择连接到虚拟机的磁盘，则必须先关闭虚拟机，然后才能继续执行下一步。

注意：

- 与在目录中创建计算机的连接（主机）对应的订阅用绿点表示。其他订阅是指那些与该订阅共享了 Azure Compute Gallery 的订阅。在这些订阅中，仅显示共享映像。有关如何配置共享订阅的信息，请参阅[在租户内（跨订阅）共享映像](#)和[在租户之间共享映像](#)。
- 您可以在 Windows 上使用具有受信任启动功能的临时操作系统磁盘创建预配方案。当您选择具有受信任启动功能的映像时，必须选择启用了 vTPM 的具有受信任启动功能的计算机配置文件。要使用临时操作系统磁盘创建计算机目录，请参阅[如何使用临时操作系统磁盘创建计算机](#)。
- 当映像复制正在进行时，您可以继续选择映像作为主映像并完成设置。但是，在复制映像时创建目录可能需要更长时间才能完成。MCS 要求复制在目录创建开始的一小时内完成。如果复制超时，目录创建将失败。您可以在 Azure 中验证复制状态。请在复制仍处于挂起状态或在复制完成后重试。
- 您可以使用 Gen2 映像来预配 Gen2 VM 目录，以缩短启动时间。但是，不支持使用 Gen1 映像创建 Gen2 计算机目录。同样，也不支持使用 Gen2 映像创建 Gen1 计算机目录。此外，没有版本信息的任何旧映像都是 Gen1 映像。

选择是否希望目录中的 VM 继承计算机配置文件中的配置。默认情况下，使用计算机配置文件 **(对于 Azure Active Directory 是必需的)** 复选框处于选中状态。单击选择计算机配置文件，从资源组列表中浏览到 VM 或 ARM 模板规范。

VM 可以从计算机配置文件中继承的配置示例包括：

- 加速的网络连接
- 启动诊断
- 主机磁盘缓存（与操作系统和 MCSIO 磁盘有关）
- 计算机大小（除非另有说明）
- 置于 VM 上的标记

注意：

- 在 Azure 中为计算机目录选择主映像时，计算机配置文件将根据您选择的主映像进行筛选。例如，计算机配置文件根据主映像的 Windows 操作系统、安全类型、休眠支持和磁盘加密 ID 进行筛选。



- 选择启用了受信任启动的映像或快照时，必须使用安全类型设置为“受信任启动”的计算机配置文件。然后，您可以通过在计算机配置文件中指定其值来启用或禁用 SecureBoot 和 vTPM。有关 Azure 可信启动的信息，请参阅 <https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch>。

验证 ARM 模板规范，确保其是否能够用作计算机配置文件来创建计算机目录。有关创建 Azure 模板规范的信息，请参阅 [创建 Azure 模板规范](#)。

有两种方法可以验证 ARM 模板规范：

- 从资源组列表中选择 ARM 模板规范后，单击下一步。如果 ARM 模板规范有错误，则会出现错误消息。
- 运行以下 PowerShell 命令之一：
  - <!JEKYLL@5180@2>
  - <!JEKYLL@5180@3>

例如：

<!JEKYLL@5180@4>

创建目录后，可以查看映像从计算机配置文件继承的配置。在计算机目录节点上，选择目录以在下方的窗格中查看其详细信息。然后，单击模板属性选项卡以查看计算机配置文件属性。标记部分最多显示三个标记。要查看放置在 VM 上的所有标记，请单击查看全部。

如果您希望 MCS 在 Azure 专用主机上预置虚拟机，请启用“使用主机组”复选框，然后从列表选择一个主机组。主机组是表示专用主机的集合的资源。专用主机是指提供托管一个或多个虚拟机的物理服务器的服务。您的服务器专用于您的 Azure 订阅，不与其他订阅者共享。使用专用主机时，Azure 会确保您的 VM 是该主机上唯一运行的计算机。此功能适用于必须满足法规或内部安全要求的场景。要详细了解主机组及其使用注意事项，请参阅在 Azure 专用主机上预配虚拟机。

重要：

- 仅显示启用了 Azure 自动放置功能的主机组。
- 使用主机组会更改向导中后面提供的虚拟机页面。该页面上仅显示选定主机组包含的计算机大小。此外，可用性区域是自动选择的，不可供选择。

### 3. 只有当您使用 Azure Resource Manager 映像时，才会显示存储和许可证类型页面。

可以将以下存储类型用于计算机目录：

- **Premium SSD**。提供适用于具有 I/O 密集型工作负载的 VM 的高性能、低延迟磁盘存储方案。
- **标准 SSD**。提供经济高效的存储方案，该方案适用于在较低的 IOPS 级别需要性能一致的工作负载。
- **标准 HDD**。提供适用于运行延迟不敏感的工作负载的 VM 的可靠、低成本的磁盘存储方案。
- **Azure 临时操作系统磁盘**。提供经济高效的、重复使用 VM 的本地磁盘来托管操作系统磁盘的存储方案。或者，您可以使用 PowerShell 创建使用临时操作系统磁盘的计算机。有关详细信息，请参阅 [Azure 临时磁盘](#)。使用临时操作系统磁盘时，请考虑以下几点：

- 无法同时启用 Azure 临时操作系统磁盘和 MCS I/O。
- 必须选择大小不超过 VM 的缓存磁盘或临时磁盘大小的映像，才能更新使用临时操作系统磁盘的计算机。
- 您无法使用稍后在向导中提供的电源重启期间保留 **VM** 和系统磁盘选项。

注意：

无论您选择哪种存储类型，身份磁盘始终使用标准 SSD 创建。

该存储类型决定在向导的虚拟机页面上提供哪些计算机大小。MCS 将高级磁盘和标准磁盘配置为使用本地冗余存储 (LRS)。LRS 在单个数据中心中创建您的磁盘数据的多个同步副本。Azure 临时操作系统磁盘使用 VM 的本地磁盘来存储操作系统。有关 Azure 存储类型和存储复制的详细信息，请参阅以下内容：

- [Azure 存储简介](#)
- [Azure 高级存储：专为高性能而设计](#)
- [Azure 存储冗余](#)

选择是使用现有的 Windows 许可证还是 Linux 许可证：

- Windows 许可证：通过将 Windows 许可证和 Windows 映像（Azure 平台支持映像或自定义映像）结合使用，您可以在 Azure 中以更低的成本运行 Windows VM。许可证有两种类型：
  - **Windows Server** 许可证。支持使用 Windows Server 许可证或 Azure Windows Server 许可证，以允许使用 Azure Hybrid Benefits。有关详细信息，请参阅 <https://azure.microsoft.com/en-us/pricing/hybrid-benefit/>。Azure Hybrid Benefits 将在 Azure 中运行 VM 的成本降低到基本计算费率，从而免除了源自 Azure 库的额外 Windows Server 许可证的费用。
  - **Windows** 客户端许可证。支持在 Azure 中使用 Windows 10 和 Windows 11 许可证，以允许您在 Azure 中运行 Windows 10 和 Windows 11 VM，而无需额外的许可证。有关详细信息，请参阅 [客户端访问许可证和管理许可证](#)。
- Linux 许可证：使用自带订阅 (BYOS) Linux 许可证，您无需为软件付费。BYOS 费用仅包括计算硬件费用。许可证有两种类型：
  - **RHEL\_BYOS**：要成功使用 RHEL\_BYOS 类型，请在您的 Azure 订阅中启用 Red Hat Cloud Access。
  - **SLES\_BYOS**：SLES 的 BYOS 版本包括 SUSE 提供的支持。

请参阅以下内容：

- [验证 Windows 许可证](#)
- [配置 Linux 许可证](#)

请参阅以下文档以了解许可证类型及其好处：

- <https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet>

- <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux>

Azure Compute Gallery 是用于管理和共享映像的存储库。它可以让您在整个组织中使用映像。我们建议您在创建大型非持久性计算机目录时将映像存储在 Azure Compute Gallery 中，因为这样做可以更快地重置 VDA 操作系统磁盘。选择在 **Azure Compute Gallery** 中放置准备好的映像后，将出现 **Azure Compute Gallery** 设置部分，允许您指定更多 Azure Compute Gallery 设置：

- 虚拟机与映像副本的比率。用于指定希望 Azure 保留的虚拟机与映像副本的比率。默认情况下，Azure 为每 40 个非持久性计算机保留一个映像副本。对于持久性计算机，该数字默认为 1000。
- 最大副本计数。允许您指定希望 Azure 保留的最大映像副本数。默认值为 10。

有关 Azure Compute Gallery 的信息，请参阅 Azure Compute Gallery。

4. 在虚拟机页面上，指明要创建的虚拟机数量和计算机大小。创建目录后，可以通过编辑目录来更改计算机大小。
5. **NIC** 页面不包含 Azure 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。
6. 在磁盘设置页面上，选择是否启用回写式缓存。启用了 MCS 存储优化功能后，可以在创建目录时配置以下设置。这些设置适用于 Azure 和 GCP 环境。

启用回写式缓存后，您可以执行以下操作：

- 配置用于缓存临时数据的磁盘和 RAM 的大小。有关详细信息，请参阅[配置临时数据的缓存](#)。
- 选择回写式缓存磁盘的存储类型。以下存储选项可用于回写式缓存磁盘：
  - 高级 SSD
  - 标准 SSD
  - 标准 HDD
- 选择是否要为已预配的 VM 保留回写式缓存磁盘。选择启用回写式缓存以使这些选项可用。默认情况下，选中使用非永久回写式缓存磁盘。
  - 使用非永久回写式缓存磁盘。如果选中此选项，则会在电源重启期间删除回写式缓存磁盘。重定向到该磁盘的任何数据都将丢失。如果 VM 的临时磁盘有足够的空间，它将用于托管回写式缓存磁盘以降低成本。创建目录后，可以检查已预配的计算机是否使用临时磁盘。为此，请单击目录并验证模板属性选项卡上的信息。如果使用临时磁盘，您将看到非永久回写式缓存磁盘，其值为是（使用 **VM** 的临时磁盘）。否则，您将看到非永久回写式缓存磁盘，其值为否（不使用 **VM** 的临时磁盘）。
  - 使用永久回写式缓存磁盘。如果选中此选项，回写式缓存磁盘将为已预配的 VM 保留。启用此选项会增加存储成本。
- 选择是否在电源重启期间为 VDA 保留 VM 和系统磁盘。

在电源重启期间保留 **VM** 和系统磁盘。当您选择“启用回写式缓存”时可用。默认情况下，VM 和系统磁盘会在关机时删除，并在启动时重新创建。如果要缩短 VM 重新启动时间，请选择此选项。请记住，启用此选项还会增加存储成本。

- 选择是否启用存储成本节约。如果已启用，则可以在 VM 关闭时将存储磁盘降级为标准 HDD，从而节省存储成本。VM 在重新启动时切换到其原始设置。该选项同时适用于存储和回写式缓存磁盘。或者，也可以使用 PowerShell。请参阅[关闭 VM 时将存储类型更改为较低的层](#)。

注意：

在 VM 关闭期间，Microsoft 对更改存储类型施加了限制。Microsoft 将来也有可能会阻止更改存储类型。有关详细信息，请参阅这篇 [Microsoft 文章](#)。

- 选择是否加密该目录中计算机上的数据以及使用哪个加密密钥。使用客户管理密钥 (CMK) 进行服务器端加密允许您在托管磁盘级别管理加密并保护目录中计算机上的数据。默认设置继承自计算机配置文件或主映像，配置文件优先：
  - 如果您使用带有 CMK 的计算机配置文件，则会自动选择“使用以下密钥加密每台计算机上的数据”选项，默认为计算机配置文件中的密钥。
  - 如果您使用带有平台管理密钥 (PMK) 的计算机配置文件并且主映像已加密 CMK，则会自动选择使用以下密钥加密每台计算机上的数据选项，默认为主映像中的密钥。
  - 如果您未使用计算机配置文件且主映像已加密 CMK，则会自动选择使用以下密钥加密每台计算机上的数据选项，默认为主映像中的密钥。

有关详细信息，请参阅 Azure 服务器端加密。

7. 在资源组页面上，选择是创建资源组还是使用现有组。

- 如果选择创建资源组，请选择下一步。
- 如果选择使用现有资源组，请从可用的预配资源组列表中选择组。

注意：

请选择足够的组以容纳您要在目录中创建的计算机。如果选择太少，系统将显示一条消息。如果您计划以后向目录添加更多 VM，则您可能希望选择的数量多于所需的最低数量。创建目录后，无法向目录添加更多资源组。

有关详细信息，请参阅 Azure 资源组。

8. 在计算机标识页面上，选择标识类型并为该目录中的计算机配置标识。如果您选择 VM 为已加入 **Azure Active Directory**，则可以将其添加到 Azure AD 安全组。详细步骤如下所示：

- a) 在标识类型字段中，选择已加入 **Azure Active Directory**。此时将显示 **Azure AD 安全组 (可选)** 选项。
- b) 单击 **Azure AD 安全组: 新建**。
- c) 输入组名称，然后单击创建。
- d) 请按照屏幕上的说明登录 Azure。

如果 Azure 中不存在组名称，则会出现绿色图标。否则，将显示一条错误消息，要求您输入新名称。
- e) 要将安全组添加到已分配的安全组，请选择“以成员身份加入已分配的安全组”，然后单击“选择组”以选择要加入的已分配组。
- f) 输入虚拟机的计算机帐户命名方案。

创建目录后，Citrix DaaS 代表您访问 Azure 并为该组创建安全组和动态成员身份规则。根据该规则，使用在此目录中指定的命名方案的 VM 将自动添加到安全组中。

将使用不同命名方案的 VM 添加到此目录需要您登录 Azure。然后，Citrix DaaS 可以访问 Azure 并根据新命名方案创建动态成员身份规则。

删除此目录时，从 Azure 中删除安全组还需要登录 Azure。

注意：

要在创建目录后重命名 Azure AD 安全组，请编辑目录并从左侧导航栏转到 **Azure AD** 安全组。Azure AD 安全组的名称不得包含以下字符：<!JEKYLL@5180@5>。

- 域凭据和摘要页面不包含 Azure 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。

完成向导。

## 创建 **Azure** 模板规范

您可以在 Azure 门户中创建 Azure 模板规范，然后在 完整配置 界面和 PowerShell 命令中使用它来创建或更新 MCS 计算机目录。

要为现有 VM 创建 Azure 模板规范，请执行以下操作：

1. 转至 Azure 门户。选择一个资源组，然后选择 VM 和网络接口。在顶部的 ... 菜单中，单击导出模板。
2. 如果要为目录预配创建模板规范，请清除包括参数复选框。
3. 单击添加到库以便稍后修改模板规范。
4. 在导入模板页面上，输入所需信息，例如名称、订阅、资源组、位置和版本。单击下一步：编辑模板。
5. 如果要预配目录，还需要将网络接口作为独立资源。因此，必须删除在模板规范中指定的任何 <!JEKYLL@5180@6>。例如：  
  
<!JEKYLL@5180@7>
6. 创建检查 + 创建并创建模板规范。
7. 在模板规格页面上，验证您创建的模板规范。单击模板规范。在左侧面板上，单击版本。
8. 可以通过单击创建新版本来创建新版本。指定新版本号，更改当前的模板规范，然后单击检查 + 创建以创建模板规范的新版本。

可以使用以下 PowerShell 命令获取有关模板规范和模板版本的信息：

- 要获取有关模板规范的信息，请运行：  
  
<!JEKYLL@5180@8>
- 要获取有关模板规范版本的信息，请运行：  
  
<!JEKYLL@5180@9>

在创建或更新目录时使用模板规范

可以使用模板规范作为计算机配置文件输入来创建或更新 MCS 计算机目录。为此，您可以使用“完整配置”界面或 PowerShell 命令。

- 使用完整配置界面：请参阅在完整配置界面中使用 Azure Resource Manager 映像创建计算机目录。
- 对于 PowerShell：请参阅使用 PowerShell 创建或更新目录时使用模板规范

将计算机预配到指定的可用性区域中

可以将计算机预配到 Azure 环境中的特定可用性区域中。可以使用“完整配置”界面或 PowerShell 来实现这一目标。

注意：

如果未指定任何区域，MCS 将允许 Azure 将计算机放置在区域内。如果指定了多个区域，MCS 会在这些区域之间随机分配计算机。

在完整配置界面中配置可用性区域

创建计算机目录时，可以指定要预配计算机的可用性区域。在虚拟机页面上，选择要在其中创建计算机的一个或多个可用性区域。

没有可用性区域的原因有两个：区域没有可用性区域或选定的计算机大小不可用。

有关使用 PowerShell 命令进行配置的信息，请参阅使用 PowerShell 配置可用性区域。

## Azure 临时磁盘

[Azure 临时磁盘](#)允许您重新调整缓存磁盘或临时磁盘的用途，以便为启用了 Azure 的虚拟机存储操作系统磁盘。此功能对于需要的 SSD 磁盘的性能高于标准 HDD 磁盘的 Azure 环境非常有用。有关使用 Azure 临时磁盘创建目录的信息，请参阅使用 Azure 临时磁盘创建目录。

注意：

永久目录不支持临时操作系统磁盘。

临时操作系统磁盘要求您的配置方案使用托管磁盘和 Azure Compute Gallery。有关详细信息，请参阅 [Azure 共享映像库](#)。

#### 存储临时操作系统临时磁盘

您可以选择将临时操作系统磁盘存储在 VM 临时磁盘或资源磁盘上。通过此功能，您可以将临时操作系统磁盘用于没有缓存或缓存不足的 VM。此类 VM 具有用于存储临时操作系统磁盘的临时磁盘或资源磁盘，例如 <!JEKYLL@5180@10>。

请注意以下事项：

- 临时磁盘存储在 VM 缓存磁盘或 VM 临时（资源）磁盘中。除非缓存磁盘的大小不足以容纳操作系统磁盘的内容，否则缓存磁盘优先于临时磁盘。
- 对于更新，如果新映像大于缓存磁盘但小于临时磁盘，则会导致将临时操作系统磁盘替换为 VM 的临时磁盘。

#### Azure 临时磁盘和 Machine Creation Services (MCS) 存储优化 (MCS I/O)

无法同时启用 Azure 临时操作系统磁盘和 MCS I/O。

重要注意事项如下：

- 您无法创建同时启用了临时操作系统磁盘和 MCS I/O 的计算机目录。
- 在“计算机目录设置”向导中，如果在“存储和许可证类型”页面上选择 **Azure** 临时操作系统磁盘，则在“磁盘设置”页面上将无法获得回写缓存 磁盘设置 选项。

Machine Catalog Setup

✕

✓ Machine Type

✓ Machine Management

✓ Desktop Experience

✓ Master Image

5 Storage and License Types

6 Virtual Machines

7 NICs

8 Disk Settings

9 Resource Group

10 Machine Identities

11 Domain Credentials

12 Scopes

13 WEM (Optional)

14 Summary

Storage and License Types

Select the type of storage to use for this machine catalog. MCS configures premium and standard disks to use Locally Redundant Storage (LRS). LRS makes multiple synchronous copies of your disk data within a single data center. The storage type you select affects the machine sizes offered later in this wizard.

☐ Premium SSD (supports I/O-intensive workloads with significantly high throughput and low latency)

☐ Standard SSD

☐ Standard HDD

☒ Azure ephemeral OS disk

You can use Windows volume licenses to provision VMs in Azure at the base compute rate. To verify that your volume licensing agreement with Microsoft qualifies for the Azure base compute rate, consult Microsoft.

☒ Use my Windows Client licenses

☐ Use my Windows Server licenses

☐ Use Azure Windows Server licenses

☒ Place image in Azure Shared Image Gallery 

?

Azure Shared Image Gallery settings

Ratio of virtual machines to image replicas:

1000

⬆ ⬇ ⬆

?

Maximum replica count:

10

⬆ ⬇ ⬆

?

Back

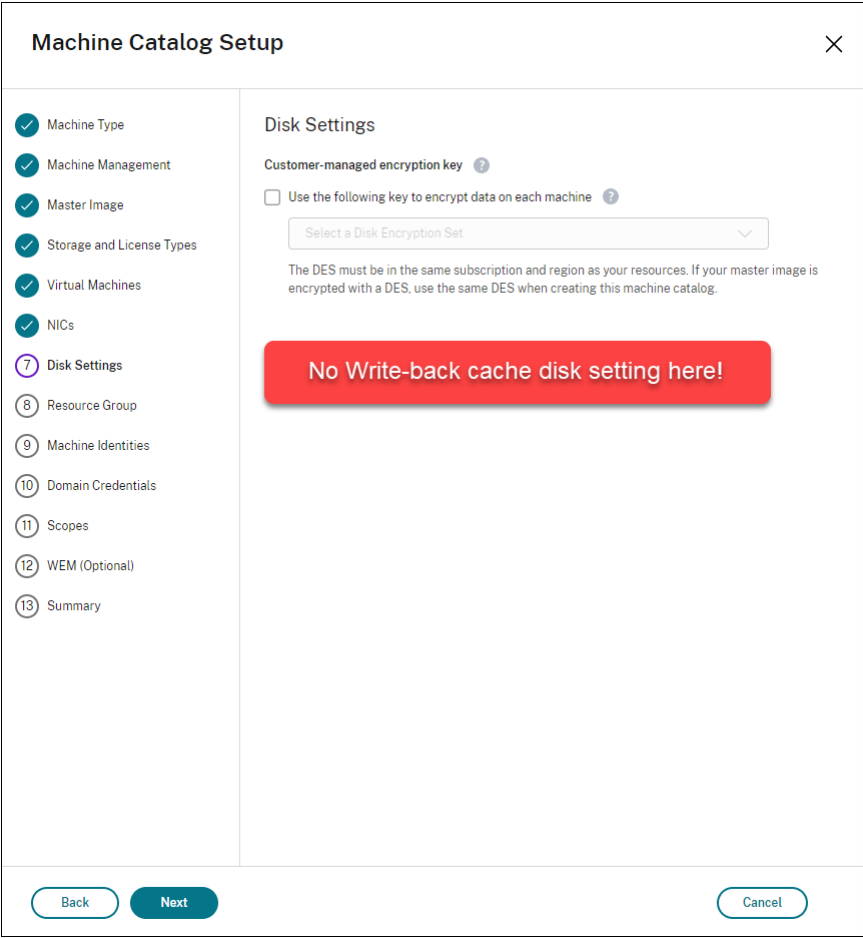
Next

Cancel

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

425





- PowerShell 参数 (<!JEKYLL@5180@11> 和 <!JEKYLL@5180@12>) 在 <!JEKYLL@5180@13> 或 <!JEKYLL@5180@14> 中设置为 **true** 失败并显示正确的错误消息。
- 对于在启用了这两种功能的情况下创建的现有计算机目录，您仍然可以：
  - 更新计算机目录。
  - 添加或删除 VM。
  - 删除计算机目录。

## Azure Compute Gallery

使用 Azure Compute Gallery（前身为共享映像库）作为 Azure 中已配置的 MCS 计算机的已发布映像存储库。可以在该库中存储已发布的映像，以加快操作系统磁盘的创建和水化速度，从而缩短非永久 VM 的启动和应用程序启动时间。Azure Compute Gallery 包含以下三个元素：

- 库：映像存储在此位置。MCS 为每个计算机目录创建一个库。
- 库映像定义：此定义包括有关已发布的映像的信息（操作系统类型和状态、Azure 区域）。MCS 为目录创建的每个映像创建一个映像定义。

- 图库图像版本：Azure Compute Gallery 中的每个图像可以有多个版本，每个版本可以在不同的区域有多个副本。每个副本都是已发布的映像的完整副本。Citrix DaaS 根据目录中的计算机数量、配置的副本比率和配置的副本最大值，为每个映像创建一个 Standard\_LRS 映像版本（1.0.0 版），该版本在目录所在区域中具有恰当的副本数量。

注意：

Azure Compute Gallery 功能仅与托管磁盘兼容。它不适用于旧版计算机目录。

有关详细信息，请参阅 [Azure 共享映像库概述](#)。

### 从 Azure Compute Gallery 访问映像

选择用于创建计算机目录的映像时，可以选择在 Azure Compute Gallery 中创建的映像。这些映像显示在“计算机目录设置”向导的“映像”页面的映像列表中。

要显示这些图片，您必须：

1. 设置 Citrix DaaS。
2. 连接到 [Azure Resource Manager](#)。
3. 在 Azure 门户中，创建资源组。有关详细信息，请参阅[使用门户创建 Azure 共享映像库](#)。
4. 在资源组中，创建 Azure Compute Gallery。
5. 在 Azure Compute Gallery 中，创建映像定义。
6. 在映像定义中，创建映像版本。

有关配置 Azure Compute Gallery 的信息，请参阅[配置 Azure Compute Gallery](#)。

### Azure 临时磁盘有资格使用回写式缓存磁盘的条件

仅当满足以下所有条件时，才能将 Azure 临时磁盘用作回写式缓存磁盘：

- 回写式缓存磁盘必须非永久，因为 Azure 临时磁盘不适合静态数据。
- 所选 Azure VM 大小必须包含临时磁盘。
- 不需要启用临时操作系统磁盘。
- 接受以将回写式缓存文件放置在 Azure 临时磁盘上。
- Azure 临时磁盘大小必须大于（回写式缓存磁盘大小 + 页面文件的预留空间 + 1 GB 缓冲区空间）的总大小。

### 非永久回写式缓存磁盘场景

下表描述了在创建计算机目录时使用临时磁盘进行回写式缓存的三种不同场景。

场景	结果
使用临时磁盘进行回写式缓存的所有条件都得到满足。	WBC 文件 <!JEKYLL@5180@15> 放置在临时磁盘上。
临时磁盘空间不足，无法使用回写式缓存。	将创建一个 VHD 磁盘 “MCSWCDisk”，并将 WBC 文件 <!JEKYLL@5180@16> 放置在此磁盘上。
临时磁盘有足够的空间来使用回写缓存，但将 <!JEKYLL@5180@17> 设置为 false。	将创建一个 VHD 磁盘 “MCSWCDisk”，并将 WBC 文件 <!JEKYLL@5180@18> 放置在此磁盘上。

请参阅以下 PowerShell 主题：

- 使用非永久回写式缓存磁盘创建计算机目录
- 使用永久回写式缓存磁盘创建计算机目录

**Azure 服务器端加密**

Citrix DaaS 通过 Azure 密钥保管库支持 Azure 托管磁盘的客户托管加密密钥。通过此支持，您可以使用自己的加密密钥对计算机目录的托管磁盘进行加密，从而管理组织和合规性要求。有关详细信息，请参阅 [Azure 磁盘存储的服务器端加密](#)。

对托管磁盘使用此功能时：

- 要更改磁盘加密时使用的密钥，请更改 <!JEKYLL@5180@19> 中的当前密钥。与该 <!JEKYLL@5180@20> 关联的所有资源都将更改为使用新密钥加密。
- 禁用或删除密钥时，任何具有使用该密钥的磁盘的 VM 都会自动关闭。关闭后，除非再次启用该密钥或分配新密钥，否则 VM 将无法使用。使用该密钥的任何目录都无法打开，也无法向其中添加 VM。

**使用客户管理的加密密钥时的重要注意事项**

使用此功能时请注意以下事项：

- 与客户管理的密钥（Azure 密钥保管库、磁盘加密集、VM、磁盘和快照）相关的所有资源都必须位于同一订阅和区域中。
- 启用客户管理的加密密钥后，以后无法将其禁用。如果要禁用或删除客户管理的加密密钥，请将所有数据复制到不使用客户管理的加密密钥的其他托管磁盘。
- 使用服务器端加密和客户托管的密钥从加密的自定义映像创建的磁盘必须使用相同的客户管理的密钥进行加密。这些磁盘必须位于同一个订阅中。
- 使用服务器端加密和客户管理的密钥加密的磁盘创建的快照必须使用相同的客户管理的密钥进行加密。
- 使用客户管理的密钥加密的磁盘、快照和映像无法移动到其他资源组和订阅。

- 当前或之前使用 Azure 磁盘加密进行加密的托管磁盘不能使用客户管理的密钥进行加密。
- 有关每个区域的磁盘加密集的限制，请参阅 [Microsoft 站点](#)。

注意：

有关配置 Azure 服务器端加密的信息，请参阅[快速入门：使用 Azure 门户创建密钥保管库](#)。

### Azure 客户管理的加密密钥

创建计算机目录时，可以选择是否加密在目录中预配的计算机上的数据。通过使用客户管理的加密密钥的服务器端加密，您可以在托管磁盘级别管理加密，并保护目录中的计算机上的数据。磁盘加密集 (Disk Encryption Set, DES) 表示客户管理的密钥。要使用此功能，必须首先在 Azure 中创建 DES。DES 采用以下格式：

- <!JEKYLL@5180@21>

从列表中选择 DES。所选择的 DES 必须与您的资源位于相同的订阅和区域。如果使用 DES 加密了映像，请在创建计算机目录时使用相同的 DES。创建目录后无法更改 DES。

如果使用加密密钥创建目录，然后在 Azure 中禁用相应的 DES，则无法再打开目录中的计算机的电源或者向其中添加计算机。

请参阅使用客户管理的密钥创建计算机目录。

### Azure 磁盘主机加密

可以创建具有主机加密功能的 MCS 计算机目录。目前，MCS 仅支持面向此功能的计算机配置文件工作流程。您可以使用 VM 或模板规范作为计算机配置文件的输入。

此加密方法不会通过 Azure 存储对数据进行加密。托管 VM 的服务器对数据进行加密，加密的数据随后会流经 Azure 存储服务器。因此，这种加密方法会对数据进行端到端加密。

限制：

主机上的 Azure 磁盘加密是：

- 并非所有 Azure 计算机大小都支持
- 与 Azure 磁盘加密不兼容

有关详细信息，请参阅：

- 创建具有主机加密功能的计算机目录。
- 从计算机配置文件中检索主机加密信息

## 托管磁盘上的双重加密

可以创建具有双重加密的计算机目录。使用此功能创建的任何目录都会同时使用平台和客户管理的密钥对所有磁盘服务器端进行加密。您拥有并维护 Azure Key Vault、加密密钥和磁盘加密集 (DES)。

双重加密是指平台端加密（默认）和客户管理的加密 (CMEK)。因此，如果您是高度安全敏感的客户，并且担心与任何加密算法、实现或密钥泄露相关的风险，则可以选择这种双重加密。永久操作系统和数据磁盘、快照和映像均使用双重加密进行静态加密。

### 注意：

- 您可以使用完整配置界面和 PowerShell 命令创建和更新采用双重加密的计算机目录。
- 可以使用非基于计算机配置文件的工作流程或基于计算机配置文件的工作流程来创建或更新具有双重加密的计算机目录。
- 如果您使用非基于计算机配置文件的工作流程来创建计算机目录，则可以重复使用存储的 <!JEKYLL@5180@22>。
- 如果使用计算机配置文件，则可以使用 VM 或模板规范作为计算机配置文件输入。

## 限制

- 超级磁盘或 Premium SSD v2 磁盘不支持双重加密。
- 非托管磁盘不支持双重加密。
- 如果您禁用与目录关联的磁盘加密集密钥，则该目录的虚拟机将被禁用。
- 与客户管理的密钥（Azure 密钥保管库、磁盘加密集、VM、磁盘和快照）相关的所有资源都必须位于同一订阅和区域中。
- 每个订阅每个区域最多只能创建 50 个磁盘加密集。
- 无法使用其他 <!JEKYLL@5180@23> 更新已包含 <!JEKYLL@5180@24> 的计算机目录。

请参阅以下 PowerShell 主题：

- 使用双重加密创建计算机目录
- 将未加密的目录转换为使用双重加密
- 验证目录是否经过双重加密

## Azure 资源组

Azure 预配资源组提供了一种预配向用户提供应用程序和桌面的 VM 的方法。您可以创建 MCS 计算机目录时添加现有的空 Azure 资源组，也可以创建新资源组。有关 Azure 资源组的信息，请参阅 [Microsoft 文档](#)。

Azure 资源组使用情况

每个 Azure 资源组的虚拟机、托管磁盘、快照和映像数量都没有限制。（删除了每个 Azure 资源组每 800 个托管磁盘包含 240 个 VM 的限制。）

- 使用完整作用域服务主体创建计算机目录时，MCS 仅创建一个 Azure 资源组，并为目录使用该资源组。
- 使用窄作用域服务主体创建计算机目录时，必须为目录提供一个空的、预先创建的 Azure 资源组。

Azure 应用商店

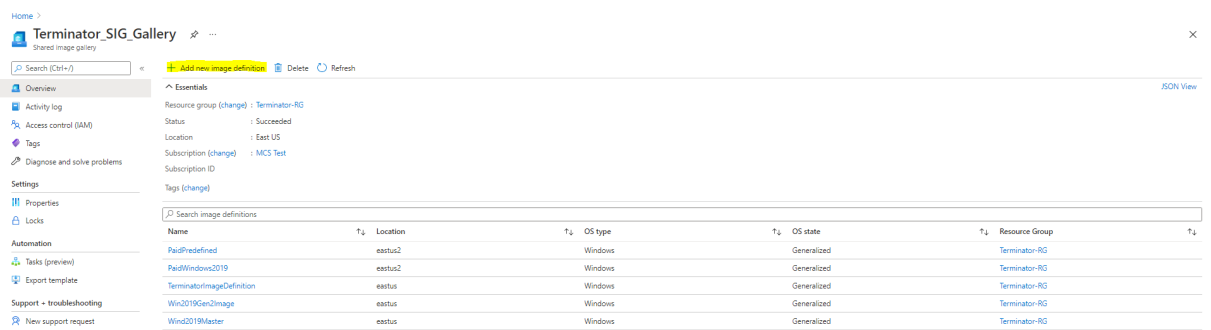
Citrix DaaS 支持在 Azure 上使用包含计划信息的主映像来创建计算机目录。有关详细信息，请参阅 [Microsoft Azure 应用商店](#)。

提示：

在 Azure 应用商店中找到的某些映像（例如标准 Windows Server 映像）不会附加计划信息。Citrix DaaS 功能适用于付费映像。

确保在 Azure Compute Gallery 中创建的映像包含 Azure 计划信息

使用本节中的步骤在完整配置界面中查看 Azure Compute Gallery 映像。这些映像可以选择用于主映像。要将映像放入 Azure Compute Gallery，请在库中创建映像定义。



在发布选项页面中，验证购买计划信息。

购买计划信息字段最初为空。请使用用于映像的购买计划信息填充这些字段。未能填充购买计划信息会导致计算机目录进程失败。

Microsoft Azure

Search resources, services, and docs (Ctrl+J)

Home > PaidPredefined (Terminator\_SIG\_Gallery/PaidPredefined) > Terminator\_SIG\_Gallery >

Add new image definition to shared image gallery

BasicVersionPublishing optionsTagsReview + create

Provide additional metadata about the image, including recommended VM specifications, and links to release notes and privacy policies.

Publishing meta data

EULA link

Description

Release notes URI

Privacy URI

Purchase plan name

Purchase plan publisher name

Purchase plan product name

VM deployment

Provide recommendations for VM specifications for this image. These recommendations are informational only, and do not constrain VM specification.

Recommended VM vCPUs

Recommended VM memory

Excluded disk types

Image definition end of life date

Review + createPreviousNext: Tags >

确认购买计划信息后，在定义中创建一个映像版本。这用作主映像。单击添加版本：

Home > Terminator\_SIG\_Gallery >

PaidPredefined (Terminator\_SIG\_Gallery/PaidPredefined)

Image definition

Search (Ctrl+J)

+ Create VM + Create VMSS Delete Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Image versions

Configuration

Properties

Locks

Automation

Tasks (preview)

Export template

Support + troubleshooting

New support request

Essentials

Resource group (change) : Terminator-RG

Location (change) : East US 2

Subscription (change) : MCS Test

Subscription ID :

Status : Succeeded

Tags (change) :

Shared image gallery : Terminator\_SIG\_Gallery

Operating system : Windows

Operating system state : Generalized

Publisher : Offer : SKU : PaidPublisher2 : PaidOffer2 : PaidSKU2

JSON View

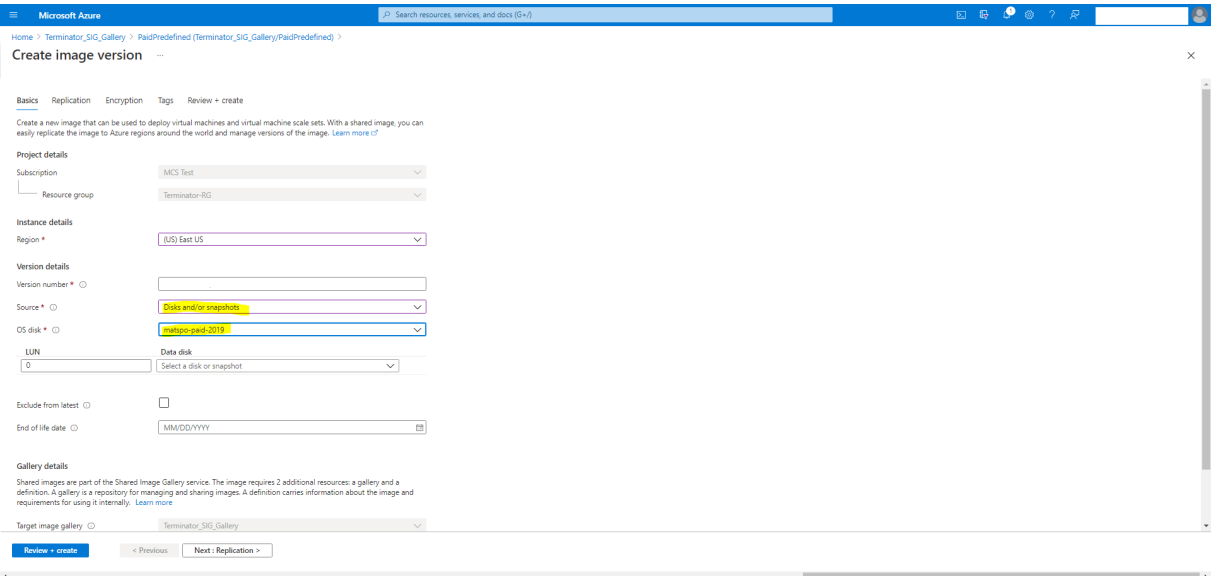
PropertiesGet startedImage versions

Filter by number... Showing 1 of 1 image versions

Add versionDelete

Number	Provisioning State	Published date	Target regions	Replication status	Create VM from version
1.0.0	Succeeded	7/7/2021, 2:13:04 PM	East US	Completed	Create VM

在版本详细信息部分中，选择映像快照或托管磁盘作为源：



预配安装了 **Azure Monitor** 代理的目录 **VM**

Azure Monitor 是一项服务，可用于收集、分析和处理来自 Azure 和本地环境的遥测数据。

Azure Monitor 代理 (AMA) 从虚拟机等计算资源收集监视数据，并将数据交付给 Azure Monitor。它目前支持收集事件日志、系统日志和性能指标，并将其发送到 Azure Monitor 指标和 Azure Monitor 日志数据源。

要通过唯一标识监视数据中的 VM 来启用监视，您可以预配安装了 AMA 作为扩展程序的 MCS 计算机目录的 VM。

要求

- 权限：请确保您拥有[关于 Azure 权限](#)中指定的最低 Azure 权限以及以下使用 Azure Monitor 的权限：
  - <!JEKYLL@5180@25>
  - <!JEKYLL@5180@26>
  - <!JEKYLL@5180@27>
  - <!JEKYLL@5180@28>
  - <!JEKYLL@5180@29>
- 数据收集规则：在 Azure 门户中设置数据收集规则。有关设置 DCR 的信息，请参阅[创建数据收集规则](#)。DCR 是特定于平台的（Windows 或 Linux）。请务必根据所需平台创建 DCR。  
AMA 使用数据收集规则 (DCR) 来管理 VM 等资源与数据源（例如 Azure Monitor 指标和 Azure Monitor 日志）之间的映射。
- 默认工作区：在 Azure 门户中创建工作区。有关创建工作区的信息，请参阅[创建日志分析工作区](#)。当您收集日志和数据时，信息存储在工作区中。工作区具有唯一的工作区 ID 和资源 ID。对于给定的资源组，工作区名称必须唯一。创建工作区后，请配置数据源和解决方案以将其数据存储在在工作区中。



- 将 Monitor 扩展程序列入白名单：扩展程序 <!JEKYLL@5180@30> 和 <!JEKYLL@5180@31> 是 Citrix 定义在白名单扩展程序。要查看列入白名单的扩展列表，请使用 PowerShell 命令 <!JEKYLL@5180@32>。
- 主映像：Microsoft 建议在使用现有计算机创建新计算机之前从现有计算机中删除扩展程序。如果不删除扩展程序，可能会导致出现剩余文件和意外行为。有关详细信息，请参阅[如果 VM 是从现有 VM 重新创建的](#)。

有关使用 PowerShell 创建启用 AMA 的目录的信息，请参阅配置启用 AMA 的目录虚拟机。

## Azure 机密 VM（预览版）

Azure 机密计算虚拟机确保您的虚拟桌面在内存中经过加密并在使用中受到保护。

您可以使用 MCS 创建包含 Azure 机密 VM 的目录。必须使用计算机配置文件工作流程来创建此类目录。您可以将 VM 和 ARM 模板规范用作计算机配置文件输入。

### 机密 VM 的重要注意事项

支持的虚拟机大小和使用机密 VM 创建计算机目录的重要注意事项如下：

- 支持的 VM 大小：机密 VM 支持以下 VM 大小：
  - DCasv5 系列
  - DCadsv5 系列
  - ECasv5 系列
  - ECadsv5 系列
- 使用机密 VM 创建计算机目录。
  - 您可以使用完整配置界面和 PowerShell 命令创建包含 Azure 机密 VM 的计算机目录。
  - 必须使用基于计算机配置文件的工作流程来创建包含 Azure 机密 VM 的计算机目录。您可以使用 VM 或模板规格作为计算机配置文件输入。
  - 必须使用相同的机密安全类型启用主映像和计算机配置文件输入。安全类型是：
    - ★ VMGuestStateOnly：仅加密了 VM 来宾状态的机密 VM
    - ★ DiskWithVMGuestState：机密 VM，操作系统磁盘和 VM 来宾状态均使用平台管理密钥或客户管理密钥进行加密。普通操作系统磁盘和临时操作系统磁盘均可加密。
  - 您可以使用 AdditionalData 参数获取各种资源类型的机密 VM 信息，例如托管磁盘、快照、Azure Compute Gallery 映像、VM 和 ARM 模板规范。例如：

<!JEKYLL@5180@33>

其他数据字段是：

- ★ DiskSecurityType

- ★ ConfidentialVMDiskEncryptionSetId
- ★ DiskSecurityProfiles

要获取计算机大小的机密计算属性，请运行以下命令：<!JEKYLL@5180@34>

附加数据字段是 <!JEKYLL@5180@35>。

- 您不能将主映像或计算机配置文件从机密安全类型更改为非机密安全类型，或从非机密安全类型更改为机密安全类型。
- 对于任何不正确的配置，您都会收到相应的错误消息。

### 使用机密 **VM** 创建计算机目录

1. 创建启用机密 VM 的主映像。请参阅 Azure 门户中的[快速入门：使用 ARM 模板部署机密 VM](#)和[快速入门：在 AMD 上创建机密 VM](#)以创建主 VM。
2. 使用主 VM 作为计算机配置文件或创建 Azure 模板规范。有关创建模板规范的信息，请参阅[创建 Azure 模板规范](#)。
3. 使用完整配置界面或 PowerShell 命令创建基于计算机配置文件的计算机目录。

注意：

确保使用相同的机密安全类型启用主映像和计算机配置文件输入。

### 使用 **PowerShell**

本部分内容详细介绍了如何使用 PowerShell 执行以下任务：

- [使用 PowerShell 在创建或更新目录时使用模板规范](#)
- [启用 Azure 虚拟机扩展](#)
- [支持受信任启动的计算机目录](#)
- [使用计算机配置文件属性值](#)
- [使用 PowerShell 配置可用性区域](#)
- [在 Azure 专用主机上配置 VM](#)
- [配置存储类型](#)
- [启用区域冗余存储](#)
- [从计算机配置文件中捕获 VM 和 NIC 上的诊断设置](#)
- [验证 Windows 许可证](#)
- [配置 Linux 许可证](#)
- [使用 Azure 临时磁盘创建计算机目录](#)
- [配置 Azure Compute Gallery](#)
- [创建或更新每个 VM 有多个 NIC 的目录](#)
- [使用非永久回写式缓存磁盘创建计算机目录](#)

- [使用永久回写式缓存磁盘创建计算机目录](#)
- [使用 MCSIO 提高启动性能](#)
- [使用客户管理的加密密钥创建计算机目录](#)
- [创建具有主机加密功能的计算机目录](#)
- [使用双重加密创建计算机目录](#)
- [页面文件位置](#)
- [更新页面文件设置](#)
- [配置启用 AMA 的目录虚拟机](#)
- [使用 Azure 现成 VM 创建目录](#)
- [复制所有资源上的标记](#)

使用 **PowerShell** 在创建或更新目录时使用模板规范

可以使用模板规范作为计算机配置文件输入来创建或更新 MCS 计算机目录。为此，您可以使用“完整配置”界面或 PowerShell 命令。

有关完整配置界面，请参阅在完整配置界面中使用 Azure Resource Manager 映像创建计算机目录。

使用 PowerShell 命令：

1. 打开 **PowerShell** 窗口。
2. 运行 <!JEKYLL@5180@36>。
3. 创建或更新目录。
  - 要创建目录，请执行以下操作：
    - a) 对作为计算机配置文件输入的模板规范使用 <!JEKYLL@5180@37> 命令。例如：  
<!JEKYLL@5180@38>
    - b) 完成目录的创建。
  - 要更新目录，请对作为计算机配置文件输入的模板规范使用 <!JEKYLL@5180@39> 命令。例如：  
<!JEKYLL@5180@40>

启用 **Azure** 虚拟机扩展

选择 ARM 模板规范后，运行以下 PowerShell 命令以使用 Azure VM 扩展：

- 要查看支持的 Azure VM 扩展列表，请执行以下操作：<!JEKYLL@5180@41>
- 要添加更多 VM 扩展，请执行以下操作：<!JEKYLL@5180@42>。例如，<!JEKYLL@5180@43>

如果您尝试添加以下任一项，命令将失败并显示错误消息：

- Citrix 定义的扩展名。
- 现有的用户定义扩展。

- 不支持的配置密钥。目前，支持的配置密钥是 <!JEKYLL@5180@44>。
- 要从列表中删除扩展名，请执行以下操作：<!JEKYLL@5180@45>。您可以移除已添加的扩展。

## 支持受信任启动的计算机目录

要使用受信任启动成功创建计算机目录，请使用：

- 具有受信任启动功能的计算机配置文件
- 支持受信任启动的 VM 大小
- 支持受信任启动的 Windows VM 版本。目前，Windows 10、Windows 11、2016、2019 和 2022 支持受信任启动。

### 重要：

MCS 支持使用启用了受信任启动的 VM 创建新目录。但是，要更新现有的永久目录和现有的 VM，必须使用 Azure 门户。无法更新非永久目录的受信任启动。有关详细信息，请参阅 Microsoft 文档 [Enable Trusted launch on existing Azure VMs](#)（在现有 Azure VM 上启用受信任启动）。

要查看 Citrix DaaS 提供的清单项目，并确定虚拟机大小是否支持可信启动，请运行以下命令：

1. 打开 PowerShell 窗口。
2. 运行 **asnp citrix\*** 以加载特定于 Citrix 的 PowerShell 模块。
3. 运行以下命令：  
  
<!JEKYLL@5180@46>  
  
4. 运行 <!JEKYLL@5180@47>  
  
5. 检查 <!JEKYLL@5180@48> 属性的值。
  - 如果 <!JEKYLL@5180@49> 设置为 **True**，则 VM 大小支持受信任启动。
  - 如果 <!JEKYLL@5180@50> 设置为 **False**，则 VM 大小不支持受信任启动。

根据 Azure 的 PowerShell，您可以使用以下命令来确定支持受信任启动的 VM 大小：

<!JEKYLL@5180@51>

以下示例描述了运行 Azure PowerShell 命令后虚拟机大小是否支持可信启动。

- 示例 1：如果 Azure VM 仅支持第 1 代，则该 VM 不支持受信任启动。因此，运行 Azure PowerShell 命令后不会显示 <!JEKYLL@5180@52> 功能。
- 示例 2：如果 Azure VM 仅支持第 2 代，并且 <!JEKYLL@5180@53> 功能设置为 **True**，则受信任启动不支持第 2 代 VM 大小。
- 示例 3：如果 Azure VM 仅支持第 2 代，并且在运行 PowerShell 命令后未显示 <!JEKYLL@5180@54> 功能，则受信任启动时支持第 2 代 VM 大小。

有关 Azure 虚拟机受信任启动的详细信息，请参阅 Microsoft 文档 [Trusted launch for Azure virtual machines](#) (Azure 虚拟机的受信任启动)。

使用受信任启动功能创建计算机目录

1. 创建启用了受信任启动的主映像。请参阅 Microsoft 文档 [Trusted launch VM Images](#) (受信任启动 VM 映像)。
2. 创建安全类型为受信任启动虚拟机的 VM 或模板规范。有关创建 VM 或模板规范的详细信息，请参阅 Microsoft 文档 [Deploy a trusted launch VM](#) (部署受信任启动 VM)。
3. 使用“完整配置”界面或 PowerShell 创建计算机目录。
  - 如果要使用“完整配置”界面，请参阅在“完整配置”界面中使用 [Azure Resource Manager 映像创建计算机目录](#)。
  - 如果要使用 PowerShell 命令，请使用带有 VM 或模板规范的 `<!JEKYLL@5180@55>` 命令作为计算机配置文件输入。有关创建目录的命令的完整列表，请参阅[创建目录](#)。

使用 VM 作为计算机配置文件输入的 `<!JEKYLL@5180@56>` 示例：

`<!JEKYLL@5180@57>`

使用模板规范作为计算机配置文件输入的 `<!JEKYLL@5180@58>` 示例：

`<!JEKYLL@5180@59>`

使用受信任启动创建计算机目录时出错

在以下情况下使用受信任启动创建计算机目录时，您会遇到相应的错误：

场景	错误
如果您在创建非托管目录时选择了计算机配置文件	<code>&lt;!JEKYLL@5180@60&gt;</code>
如果您在创建以非托管磁盘作为主映像的目录时选择支持受信任启动的计算机配置文件	<code>&lt;!JEKYLL@5180@61&gt;</code>
如果您在使用以受信任启动作为安全类型的主映像源创建托管目录时未选择计算机配置文件	<code>&lt;!JEKYLL@5180@62&gt;</code>
如果您选择安全类型与主映像的安全类型不同的计算机配置文件	<code>&lt;!JEKYLL@5180@63&gt;</code>
如果您选择的 VM 大小不支持受信任启动，但在创建目录时使用支持受信任启动的主映像	<code>&lt;!JEKYLL@5180@64&gt;</code>

## 使用计算机配置文件属性值

计算机目录使用在自定义属性中定义的以下属性：

- 可用性区域
- 专用主机组 ID
- 磁盘加密集 ID
- 操作系统类型
- 许可证类型
- 存储类型

如果未显式定义这些自定义属性，则从 ARM 模板规范或 VM（以用作计算机配置文件为准）中设置属性值。此外，如果未指定 `<!JEKYLL@5180@65>`，则从计算机配置文件进行设置。

### 注意：

如果计算机配置文件中缺少某些属性，并且未在自定义属性中定义，则在适用的情况下将使用这些属性的默认值。

以下部分描述了 `<!JEKYLL@5180@66>` 从 MachineProfile 派生定义的所有属性或值时 `<!JEKYLL@5180@67>` 和 `<!JEKYLL@5180@68>` 下的某些方案。

- New-ProvScheme 方案
  - MachineProfile 具有所有属性，但未定义 CustomProperties。示例：  
`<!JEKYLL@5180@69>`  
以下值被设置为目录的自定义属性：  
`<!JEKYLL@5180@70>`
  - MachineProfile 有一些属性，但未定义 CustomProperties。示例：MachineProfile 只有 License-Type 和 OsType。  
`<!JEKYLL@5180@71>`  
以下值被设置为目录的自定义属性：  
`<!JEKYLL@5180@72>`
  - MachineProfile 和 CustomProperties 定义了所有属性。示例：  
`<!JEKYLL@5180@73>`  
自定义属性优先。以下值被设置为目录的自定义属性：  
`<!JEKYLL@5180@74>`
  - 有些属性在 MachineProfile 中定义，有些属性在 CustomProperties 中定义。示例：
    - \* CustomProperties 定义 LicenseType 和 StorageAccountType

- ★ MachineProfile 定义 LicenseType、OsType 和区域

<!JEKYLL@5180@75>

以下值被设置为目录的自定义属性：

<!JEKYLL@5180@76>

- 有些属性在 MachineProfile 中定义，有些属性在 CustomProperties 中定义。此外，未定义 ServiceOffering。示例：

- ★ CustomProperties 定义 StorageType

- ★ MachineProfile 定义 LicenseType

<!JEKYLL@5180@77>

以下值被设置为目录的自定义属性：

<!JEKYLL@5180@78>

- 如果 OsType 既不在 CustomProperties 中，也不在 MachineProfile 中，那么：

- ★ 该值将从主映像中读取。

- ★ 如果主映像是非托管磁盘，则 OsType 设置为 Windows。示例：

<!JEKYLL@5180@79>

主映像中的值将写入自定义属性，在本例中为 Linux。

<!JEKYLL@5180@80>

- Set-ProvScheme 方案

- 包含以下对象的现有目录：

- ★ <!JEKYLL@5180@81> 和 OsType 的 CustomProperties

- ★ 用于定义区域的 MachineProfile <!JEKYLL@5180@82>

- 更新：

- ★ 用于定义 StorageAccountType 的 MachineProfile mpB.vm

- ★ 用于定义 LicenseType 和 OsType 的一组新自定义属性 \$CustomPropertiesB

<!JEKYLL@5180@83>

以下值被设置为目录的自定义属性：

<!JEKYLL@5180@84>

- 包含以下对象的现有目录：

- ★ <!JEKYLL@5180@85> 和 OsType 的 CustomProperties

- ★ 用于定义 StorageAccountType 和 LicenseType 的 MachineProfile <!JEKYLL@5180@86>

- 更新:

- \* 用于定义 StorageAccountType 和 OsType 的一组新自定义属性 \$CustomPropertiesB。

<!JEKYLL@5180@87>

以下值被设置为目录的自定义属性:

<!JEKYLL@5180@88>

- 包含以下对象的现有目录:

- \* <!JEKYLL@5180@89> 和 OsType 的 CustomProperties
  - \* 用于定义区域的 MachineProfile <!JEKYLL@5180@90>

- 更新:

- \* 用于定义 StorageAccountType 和 LicenseType 的 MachineProfile mpB.vm
  - \* 未指定 <!JEKYLL@5180@91>

<!JEKYLL@5180@92>

以下值被设置为目录的自定义属性:

<!JEKYLL@5180@93>

## 使用 **PowerShell** 配置可用性区域

使用 PowerShell, 您可以使用 <!JEKYLL@5180@94> 查看 Citrix DaaS 产品清单项目。例如, 要查看美国东部地区 <!JEKYLL@5180@95> 服务产品, 请执行以下操作:

<!JEKYLL@5180@96>

要查看区域, 请使用该项目的 <!JEKYLL@5180@97> 参数:

<!JEKYLL@5180@98>

如果未指定可用性区域, 计算机的预配方式没有任何变化。

要通过 PowerShell 配置可用性区域, 请使用随 <!JEKYLL@5180@99> 操作提供的区域自定义属性。区域属性定义了要在其中预配计算机的可用性区域列表。这些区域可以包括一个或多个可用性区域。例如, <!JEKYLL@5180@100> 对于区域 1 和 3。

使用 <!JEKYLL@5180@101> 命令可更新预配方案的区域。

如果提供的区域无效, 则不会更新预配方案, 并且会显示一条错误消息, 提供有关如何修复无效命令的说明。

**提示:**

如果指定了无效的自定义属性, 则不会更新预配方案, 并显示相关的错误消息。



同时使用主机组和 **Azure** 可用性区域的结果

根据自定义属性和主机组区域中指定的可用性区域，进行预先检查以评估计算机目录的创建是否成功。如果可用性区域自定义属性与主机组的区域不匹配，目录创建将失败。

有关通过 PowerShell 配置可用性区域的信息，请参阅[通过 PowerShell 配置可用性区域](#)。

有关 Azure 专用主机的信息，请参阅[Azure 专用主机](#)。

下表描述了可用性区域和主机组区域的各种组合，以及哪些组合会导致计算机目录的创建成功或失败。

主机组区域	自定义属性中的可用性区域	计算机目录创建结果
已指定。例如，主机组位于区域 1 中	未指定	成功。计算机在主机组的区域中创建
已指定。例如，主机组位于区域 1 中	与主机组区域相同的区域。例如，自定义属性中的区域设置为 1	成功。计算机在区域 1 中创建
已指定。例如，主机组位于区域 1 中	与主机组区域不同。例如，自定义属性中的 zone 设置为 2	由于指定的可用性区域与主机组的区域不匹配，因此，目录创建失败并在实施前检查期间出现相关错误
已指定。例如，主机组位于区域 1 中	指定了多个区域。例如，自定义属性中的区域设置为 1,2 或 2,3	由于指定的可用性区域与主机组的区域不匹配，因此，目录创建失败并在实施前检查期间出现相关错误
未指定。例如，主机组的区域是 <!JEKYLL@5180@102>	未指定	由于指定的可用性区域与主机组的区域匹配（即没有区域），因此目录创建成功。计算机不是在任何区域中创建的
未指定。例如，主机组的区域是 <!JEKYLL@5180@103>	已指定。例如，自定义属性中的区域设置为一个或多个区域	由于指定的可用性区域与主机组的区域不匹配，因此目录创建失败并会在预检检查期间出现相关错误

在 **Azure** 专用主机上配置 VM

可以使用 MCS 在 Azure 专用主机上预配 VM。在 Azure 专用主机上预配 VM 之前：

- 创建主机组。
- 在该主机组中创建主机。
- 确保有足够的主机容量用于创建目录和虚拟机。

可以创建具有通过以下 PowerShell 脚本定义的主机租赁的计算机目录：

<!JEKYLL@5180@104>

使用 MCS 在 Azure 专用主机上预配虚拟机时，请注意：

- 专用主机是目录属性，一旦创建了目录，则无法进行更改。Azure 当前不支持专用租赁。
- 使用 `<!JEKYLL@5180@105>` 参数时，需要在托管单元所在区域中预配置的 Azure 主机组。
- Azure 自动放置是必需的。此功能请求加载与主机组关联的订阅。有关详细信息，请参阅[在 Azure 专用主机上设置 VM 规模 - 公共预览版](#)。如果未启用自动放置，MCS 在目录创建过程中会引发错误。

## 配置存储类型

为 Azure 环境中使用 MCS 的虚拟机选择不同的存储类型。对于目标 VM，MCS 支持：

- 操作系统磁盘：高级 SSD、SSD 或 HDD
- 回写缓存磁盘：高级 SSD、SSD 或 HDD

使用这些存储类型时，请注意以下事项：

- 确保您的 VM 支持选定的存储类型。
- 如果您的配置使用 Azure 临时磁盘，则无法获得回写式缓存磁盘设置的选项。

提示：

`<!JEKYLL@5180@106>` 已针对操作系统类型和存储帐户进行了配置。`<!JEKYLL@5180@107>` 已针对写回式缓存存储类型进行了配置。对于常见目录，`<!JEKYLL@5180@108>` 是必需的。如果未配置 `<!JEKYLL@5180@109>`，则会将 `<!JEKYLL@5180@110>` 用作 `<!JEKYLL@5180@111>` 的默认值。

如果未配置 `WBCDiskStorageType`，则会将 `StorageType` 用作 `WBCDiskStorageType` 的默认值

## 为 VM 配置存储类型

要为虚拟机配置存储类型，请使用 `<!JEKYLL@5180@112>` 中的 `<!JEKYLL@5180@113>` 参数。要将现有目录中 `<!JEKYLL@5180@114>` 参数的值更新为支持的存储类型之一，请使用 `<!JEKYLL@5180@115>` 命令。

下面是预配方案中的一组示例 `<!JEKYLL@5180@116>` 参数：

`<!JEKYLL@5180@117>`

## 启用区域冗余存储

在创建目录期间，您可以选择区域冗余存储。它跨多个可用性区域同步复制您的 Azure 托管磁盘，这允许您利用其他区域中的冗余从一个区域中的故障中恢复。

可以在存储类型自定义属性中指定 **Premium\_ZRS** 和 **StandardSSD\_ZRS**。可以使用现有的自定义属性或通过 **MachineProfile** 模板设置 ZRS 存储。带 `<!JEKYLL@5180@118>` 和 `<!JEKYLL@5180@119>` 参数的 `<!JEKYLL@5180@120>` 命令也支持 ZRS 存储。您可以将现有虚拟机从 LRS 更改为 ZRS 存储。

**注意：**

- <!JEKYLL@5180@121> 表示计划的开始时间为当前时间。
- <!JEKYLL@5180@122> 负数（例如-1）表示计划的时间范围没有上限。

**限制：**

- 仅支持托管磁盘
- 仅支持高级和标准固态驱动器 (SSD)
- 不支持 <!JEKYLL@5180@123>
- 仅在某些地区可用。
- 大规模创建 ZRS 磁盘时，Azure 的性能会下降。因此，首次打开电源时，请小批量打开计算机（一次少于 300 台计算机）

将区域冗余存储设置为磁盘存储类型

您可以在初始目录创建期间选择区域冗余存储，也可以更新现有目录中的存储类型。

使用 **PowerShell** 命令选择区域冗余存储

使用 <!JEKYLL@5180@124> PowerShell 命令在 Azure 中创建新目录时，请使用 <!JEKYLL@5180@125> 作为 <!JEKYLL@5180@126> 中的值。

例如：

<!JEKYLL@5180@127>

设置此值时，它将由动态 API 进行验证，以确定该值是否可以正确使用。如果 ZRS 的使用对您的目录无效，则可能会出现以下异常：

- **StorageTypeAtShutdownNotSupportedForZrsDisks**：StorageTypeAtShutdown 自定义属性不能用于 ZRS 存储。
- **StorageAccountTypeNotSupportedInRegion**：如果您尝试在不支持 ZRS 的 Azure 区域中使用 ZRS 存储，则会出现此异常。
- **ZrsRequiresManagedDisks**：区域冗余存储只能用于托管磁盘。

可以使用以下自定义属性设置磁盘存储类型：

- <!JEKYLL@5180@128>
- <!JEKYLL@5180@129>
- <!JEKYLL@5180@130>

注意：

在创建目录期间，如果未设置自定义属性，则将使用计算机配置文件的操作系统磁盘 <!JEKYLL@5180@131>。

## 从计算机配置文件中捕获 VM 和 NIC 上的诊断设置

在创建计算机目录、更新现有计算机目录和更新现有 VM 过程中，可以从计算机配置文件中捕获 VM 和 NIC 上的诊断设置。

可以创建 VM 或模板规范作为计算机配置文件来源。

### 关键步骤

1. 在 Azure 中设置所需的 ID。必须在模板规范中提供这些 ID。
  - 存储帐户
  - 日志分析工作区
  - 采用标准分层定价的事件中心命名空间
2. 创建计算机配置文件源。
3. 创建新计算机目录、更新现有目录或更新现有 VM。

### 在 Azure 中设置所需的 ID

在 Azure 中设置以下选项之一：

- 存储帐户
- 日志分析工作区
- 采用标准分层定价的事件中心命名空间

**设置存储帐户** 在 Azure 中创建标准存储帐户。在模板规范中，将存储帐户的完整资源 ID 指定为 <!JEKYLL@5180@132>。

将 VM 设置为将数据记录到存储帐户后，可以在 <!JEKYLL@5180@133> 容器下找到数据。

**设置日志分析工作区** 创建日志分析工作区。在模板规范中，将日志分析工作区的完整资源 ID 作为工作区 ID。

将 VM 设置为将数据记录到工作区后，即可在 Azure 中的“Logs”（日志）下查询数据。可以在 Azure 中的“Logs”（日志）下运行以下命令，以显示资源记录的所有指标的计数：

‘AzureMetrics

设置事件中心 要在 Azure 门户中设置事件中心，请执行以下操作：

1. 使用标准分层定价创建事件中心命名空间。
2. 在命名空间下创建事件中心。
3. 导航到事件中心下的 **Capture**（捕获）。打开开关，使用 Avro 输出类型进行捕获。
4. 在现有存储帐户中创建一个新容器来捕获日志。
5. 在模板规范中，请按以下格式指定 `eventHubAuthorizationRuleId:/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`
6. 指定事件中心的名称。

一旦 VM 设置为将数据记录到事件中心，数据就会捕获到配置的存储容器中。

#### 创建计算机配置文件源

可以创建 VM 或模板规范作为计算机配置文件来源。

使用诊断设置创建基于 **VM** 的计算机配置文件 如果您想创建 VM 作为计算机配置文件，请先在模板 VM 自身中设置诊断设置。可以参考 Microsoft 文档 [Diagnostic settings in Azure Monitor](#)（Azure Monitor 中的诊断设置）中提供的详细说明。

可以运行以下命令来验证现在是否存在与 VM 或 NIC 关联的诊断设置：

```
1 az monitor diagnostic-settings list --resource-group matspo --resource
  matspo-tog-cc2659 --resource-type microsoft.network/
  networkInterfaces
2 <!--NeedCopy-->
```

```
1 az monitor diagnostic-settings list --resource-group matspo --resource
  matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
2 <!--NeedCopy-->
```

使用诊断设置创建基于模板规范的计算机配置文件 如果您想使用启用了诊断设置的 VM 并将其导出到 ARM 模板规范中，则这些设置不会自动包含在模板中。必须在 ARM 模板中手动添加或修改诊断设置。

但是，如果您想使用 VM 作为计算机配置文件，MCS 可确保准确捕获关键诊断设置并将其应用到 MCS 目录中的资源。

1. 创建用于定义 VM 和 NIC 的标准模板规范。
2. 根据规范添加其他资源来部署诊断设置：[Microsoft.Insights diagnosticSettings](#)。对于作用域，请按名称引用模板中带有部分 ID 的 VM 或 NIC。例如，要在模板规范中创建附加到名为 test-VM 的 VM 的诊断设置，请将作用域指定为：

```
1 "scope": "microsoft.compute/virtualMachines/test-VM",
2 <!--NeedCopy-->
```

3. 使用模板规范作为计算机配置文件来源。

使用诊断设置创建或更新目录

创建计算机配置文件源后，您现在可以使用 `New-ProvScheme` 命令创建计算机目录，使用 `Set-ProvScheme` 命令更新现有计算机目录，使用 `Request-ProvVMUpdate` 命令更新现有 VM。

### 验证 **Windows** 许可证

您可以通过运行以下 PowerShell 命令来验证已预配的 VM 是否正在利用许可权益：`Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`。

- 对于 Windows Server 许可证类型，请验证许可证类型是否为 **Windows\_Server**。更多说明，请访问 <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/>。
- 对于 Windows 客户端许可证类型，请验证许可证类型是否为 **Windows\_Client**。更多说明，请访问 <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/>。

或者，您可以使用 `Get-ProvScheme` PowerShell SDK 来执行验证。例如：`Get-ProvScheme -ProvisioningSchemeName "My Azure Catalog"`。有关此 cmdlet 的详细信息，请参阅 <https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/>。

### 配置 **Linux** 许可证

使用自带订阅 (BYOS) Linux 许可证，您无需为软件付费。BYOS 费用仅包括计算硬件费用。许可证有两种类型：

- **RHEL\_BYOS**：要成功使用 RHEL\_BYOS 类型，请在您的 Azure 订阅中启用 Red Hat Cloud Access。
- **SLES\_BYOS**：SLES 的 BYOS 版本包括 SUSE 提供的支持。

可以在 `New-ProvScheme` 和 `Set-ProvScheme` 处将 `LicenseType` 值设置为 Linux 选项。

在 `New-ProvScheme` 处将 `LicenseType` 设置为 RHEL\_BYOS 的示例：

```
1 New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "azureCatalog" -
  RunAsynchronously -Scope @() -SecurityGroup @() -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="StringProperty" Name="
```

```

        StorageAccountType" Value="StandardSSD_LRS" /><Property xsi:type="
        StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /><Property
        xsi:type="StringProperty" Name="OsType" Value="Linux" /><Property
        xsi:type="StringProperty" Name="LicenseType" Value="RHEL_BYOS" /></
        CustomProperties>'
2 <!--NeedCopy-->

```

在 `Set-ProvScheme` 处将 `LicenseType` 设置为 `SLES_BYOS` 的示例：

```

1 Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -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="StringProperty" Name="
  StorageAccountType" Value="StandardSSD_LRS" /><Property xsi:type="
  StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /><Property
  xsi:type="StringProperty" Name="OsType" Value="Linux" /><Property
  xsi:type="StringProperty" Name="LicenseType" Value="SLES_BYOS" /></
  CustomProperties>'
2 <!--NeedCopy-->

```

注意：

如果 `LicenseType` 值为空，则默认值为 Azure Windows Server 许可证或 Azure Linux 许可证，具体取决于 `OsType` 的值。

将 `LicenseType` 设置为空的示例：

```

1 Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -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="StringProperty" Name="
  StorageAccountType" Value="StandardSSD_LRS" /><Property xsi:type="
  StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /><Property
  xsi:type="StringProperty" Name="OsType" Value="Linux" /></
  CustomProperties>'
2 <!--NeedCopy-->

```

## 使用 **Azure** 临时磁盘创建计算机目录

要使用 `New-ProvScheme` 预配临时操作系统磁盘，请注意以下限制：

- 用于目录的 VM 大小必须支持临时操作系统磁盘。
- 与 VM 大小关联的缓存磁盘或临时磁盘的大小必须大于或等于操作系统磁盘的大小。
- 临时磁盘大小必须大于缓存磁盘大小。

在以下情况下，还要考虑这些限制因素：

- 创建配置方案

- 修改配置方案
- 更新映像

要使用临时磁盘，必须在运行 `New-ProvScheme` 时将自定义属性 `UseEphemeralOsDisk` 设置为 **true**。

注意：

如果自定义属性 `UseEphemeralOsDisk` 设置为 **false** 或未指定值，则所有预配的 VDA 将继续使用预配的操作系统磁盘。

下面是要在预配方案中使用的自定义属性的示例集：

```
1  "CustomProperties": [  
2      {  
3  
4          "Name": "UseManagedDisks",  
5          "Value": "true"  
6      }  
7  ,  
8      {  
9  
10         "Name": "StorageType",  
11         "Value": "Standard_LRS"  
12     }  
13  ,  
14     {  
15  
16         "Name": "UseSharedImageGallery",  
17         "Value": "true"  
18     }  
19  ,  
20     {  
21  
22         "Name": "SharedImageGalleryReplicaRatio",  
23         "Value": "40"  
24     }  
25  ,  
26     {  
27  
28         "Name": "SharedImageGalleryReplicaMaximum",  
29         "Value": "10"  
30     }  
31  ,  
32     {  
33  
34         "Name": "LicenseType",  
35         "Value": "Windows_Server"  
36     }  
37  ,  
38     {  
39  
40         "Name": "UseEphemeralOsDisk",  
41         "Value": "true"
```



```

42         }
43
44     ],
45     <!--NeedCopy-->

```

为现有目录配置临时磁盘

要为现有目录配置 Azure 临时操作系统磁盘，请使用 `Set-ProvScheme` 中的 `UseEphemeralOsDisk` 参数。将 `UseEphemeralOsDisk` 参数的值设置为 **true**。

注意：

要使用此功能，还必须启用参数 `UseManagedDisks` 和 `UseSharedImageGallery`。

例如：

```

1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties <
   CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
2   <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
   />
3   <Property xsi:type="StringProperty" Name="UseSharedImageGallery" Value=
   "true" />
4   <Property xsi:type="StringProperty" Name="UseEphemeralOsDisk" Value="
   true" />
5 </CustomProperties>'
6 <!--NeedCopy-->

```

## 配置 Azure Compute Gallery

使用 `New-ProvScheme` 命令创建支持 Azure Compute Gallery 的配置方案。使用 `Set-ProvScheme` 命令为预配方案启用或禁用此功能，并更改副本比率和副本最大值。

为支持 Azure Compute Gallery 功能，在配置方案中添加了三个自定义属性：

### UseSharedImageGallery

- 定义是否使用 Azure Compute Gallery 来存储已发布的映像。如果设置为 **True**，则映像存储为 Azure Compute Gallery 映像，否则映像将存储为快照。
- 有效值为 **True** 和 **False**。
- 如果未定义属性，则默认值为 **False**。

### SharedImageGalleryReplicaRatio

- 定义计算机与库映像版本副本的比率。
- 有效值为大于 0 的整数。

- 如果未定义该属性，则将使用默认值。永久操作系统磁盘的默认值为 1000，非永久操作系统磁盘的默认值为 40。

### SharedImageGalleryReplicaMaximum

- 定义每个库映像版本的最大副本数。
- 有效值为大于 0 的整数。
- 如果未定义该属性，则默认值为 10。
- Azure 当前支持多达 10 个库映像单个版本的副本。如果将属性设置为大于 Azure 支持的值，MCS 将尝试使用指定值。Azure 将生成一个错误，MCS 日志之后将当前副本计数保持不变。

#### 提示：

使用 Azure Compute Gallery 存储 MCS 已配置目录的已发布映像时，MCS 会根据目录中的计算机数量、副本比率和副本最大值来设置图库映像版本副本数。副本计数的计算方法如下：将目录中的计算机数除以副本比率（四舍五入到最接近的整数值），然后将该值最高限定到最大副本计数。例如，副本比率为 20，最大值为 5，0—20 台计算机将创建 1 个副本，21—40 台将创建 2 个副本，41—60 台将创建 3 个副本，61—80 台将创建 4 个副本，81 台以上将创建 5 个副本。

#### 用例：更新 **Azure Compute Gallery** 副本比率和副本最大值

现有计算机目录使用 Azure Compute Gallery。使用 **Set-ProvScheme** 命令更新目录中的所有现有计算机以及将来任何计算机的自定义属性：

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '  
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/  
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-  
    instance"> <Property xsi:type="StringProperty" Name="StorageType"  
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="  
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"  
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="  
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <  
    Property xsi:type="IntProperty" Name="  
    SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
2 <!--NeedCopy-->
```

#### 用例：将快照目录转换为 **Azure Compute Gallery** 目录

对于此用例：

1. 在 **UseSharedImageGallery** 标志设置为 **True** 的情况下运行 **Set-ProvScheme**。（可选）包括 **SharedImageGalleryReplicaRatio** 和 **SharedImageGalleryReplicaMaximum** 属性。
2. 更新目录。
3. 关闭并打开计算机电源以强制更新。

例如：

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '  
  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/  
  machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-  
  instance"> <Property xsi:type="StringProperty" Name="StorageType"  
  Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="  
  UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"  
  Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="  
  IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <  
  Property xsi:type="IntProperty" Name="  
  SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'  
2 <!--NeedCopy-->
```

提示：

参数 `SharedImageGalleryReplicaRatio` 和 `SharedImageGalleryReplicaMaximum` 不是必需的。`Set-ProvScheme` 命令完成后，Azure Compute Gallery 映像尚未创建。将目录配置为使用库后，下一个目录更新操作会将已发布的映像存储在库中。目录更新命令创建库、库映像和映像版本。关闭并打开计算机会对其进行更新，此时副本计数将在适当的情况下更新。从那时起，将使用 Azure Compute Gallery 映像重置所有现有的非永久性计算机，所有新置备的计算机均使用该映像创建。旧快照会在几个小时内自动清理。

用例：将 **Azure Compute Gallery** 目录转换为快照目录

对于此用例：

1. 在 `UseSharedImageGallery` 标志设置为 **False** 或未定义的情况下运行 `Set-ProvScheme`。
2. 更新目录。
3. 关闭并打开计算机电源以强制更新。

例如：

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '  
  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/  
  machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-  
  instance"> <Property xsi:type="StringProperty" Name="StorageType"  
  Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="  
  UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"  
  Name="UseSharedImageGallery" Value="False"/></CustomProperties>'  
2 <!--NeedCopy-->
```

提示：

与从快照更新到 Azure Compute Gallery 目录不同，每台计算机的自定义数据尚未更新以反映新的自定义属性。运行以下命令以查看原始 Azure Compute Gallery 自定义属性：`Get-ProvVm -ProvisioningSchemeName catalog-name`。`Set-ProvScheme` 命令完成后，尚未创建映像快照。将目录配置为不使用库后，下一个目录更新操作将已发布的映像存储为快照。自此以后，所有现有的非

持久计算机都将使用快照重置，并且所有新预配的计算机都是基于该快照创建的。关闭并打开计算机会对其进行更新，此时自定义计算机数据将更新以反映 `UseSharedImageGallery` 设置为 **False**。旧的 Azure Compute Gallery 资源（库、映像和版本）会在几个小时内自动清除。

### 创建或更新每个 VM 有多个 NIC 的目录

MCS 支持每个 VM 多个 NIC。您可以将虚拟机上的多个 NIC 关联到多个子网，但是，这些子网必须位于同一个虚拟网络 (VNet) 中。您可以使用 PowerShell 命令来：

- 在 VM 上创建包含多个 NIC 的目录
- 更新现有目录配置以在虚拟机上拥有多个 NIC，以便新创建的 VM 具有多个 NIC
- 更新现有 VM 以拥有多个 NIC

您可以创建或更新非基于计算机配置文件的计算机目录和基于计算机配置文件的计算机目录，以便在虚拟机上拥有多个 NIC。目前，对于基于计算机配置文件的计算机目录，只能拥有与计算机配置文件源中指定的 NIC 数量相同。

诸如加速网络和网络安全组之类的属性源自计算机配置文件源。

注意：

虚拟机大小必须支持相同数量的 NIC 和相应的加速网络，否则会出现错误。

您可以检索与所选 VM 大小关联的最大 NIC 数量。当您使用 `AdditionalData` 参数运行 PowerShell `get-item` 命令时，名为 `MaxNetworkInterfaces` 的 PowerShell 属性会显示最大网卡数。

### 检索最大 NIC 数量

要检索最大网卡数，请执行以下操作：

1. 从 Delivery Controller 主机打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 运行 `Get-ChildItem -Path "XDHyp:\Connections\abc-connection\East US .region\serviceoffering.folder"` 以列出所有可用的虚拟机大小。
4. 运行 `get-item -Path "XDHyp:\Connections\abc-connection\East US .region\serviceoffering.folder\Standard_M416ms_v2.serviceoffering".AdditionalData`
5. 检查 `MaxNetworkInterfaces` 以了解 NIC 的最大数量。

### 在 VM 上创建包含多个 NIC 的目录

要在 VM 上创建包含多个 NIC 的目录，请执行以下操作：

1. 从 Delivery Controller 主机上打开 PowerShell 窗口。

2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 创建标识池（如果尚未创建）。
4. 创建配置方案：

- 如果创建非基于计算机配置文件的计算机目录，请运行带 `NetworkMappings` 参数的 `New-ProvScheme` 命令。您可以向参数 `NetworkMappings` 添加多个子网。例如：

```
1 New-ProvScheme -NetworkMappings @{
2   "0"="subnetpath1";"1"="subnetpath1" }
3
4 <!--NeedCopy-->
```

- 如果创建基于计算机配置文件的计算机目录：
  - a) 在 Azure 中创建虚拟机以拥有多个 NIC。有关信息，请参阅[创建和管理具有多个 NIC 的 Windows 虚拟机](#)。您也可以创建新的 VM，然后在 Azure 门户的网络页面中连接网络接口。
  - b) 使用虚拟机作为计算机配置文件输入运行 `New-ProvScheme` 命令。

注意：

创建基于计算机配置文件的计算机目录时，`NetworkMappings` 的数量必须与计算机配置文件的 `NetworkInterfaceCount` 数量相同。可以从 `Get-item -Path "machine profile path"` 的 `AdditionalData` 中检索 `NetworkInterfaceCount`。

5. 完成目录的创建。

## 更新目录以在虚拟机上拥有多个 NIC

要更新目录以在虚拟机上拥有多个 NIC，请执行以下操作：

1. 从 Delivery Controller 主机打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 更新配置方案：
  - 如果创建的不是基于计算机配置文件的计算机目录，请运行带 `NetworkMappings` 参数的 `Set-ProvScheme` 命令。您可以向参数 `NetworkMappings` 中添加多个子网。例如：

```
1 Set-ProvScheme -NetworkMappings @{
2   "0"="subnetpath1";"1"="subnetpath1" }
3
4 <!--NeedCopy-->
```

- 如果根据计算机配置文件创建计算机目录：
  - a) 在 Azure 中创建虚拟机以拥有多个 NIC。有关信息，请参阅[创建和管理具有多个 NIC 的 Windows 虚拟机](#)。
  - b) 使用虚拟机作为计算机配置文件输入运行 `Set-ProvScheme` 命令。

## 更新现有 VM 以在虚拟机上拥有多个 NIC

您还可以使用 `Set-ProvVMUpdateTimeWindow` 更新现有虚拟机，也可以在更新时间窗口内对现有虚拟机执行电源重启。有关更新现有 VM 的更多信息，请参阅[将已预配的计算机更新到当前的配置方案状态](#)。

## 使用非永久回写式缓存磁盘创建计算机目录

要配置具有非永久回写式缓存磁盘的目录，请使用 PowerShell 参数 `New-ProvScheme CustomProperties`。自定义属性包括：

- **UseTempDiskForWBC**。此属性指示您是否接受使用 Azure 临时存储来存储回写式缓存文件。如果要临时磁盘用作回写式缓存磁盘，则必须在运行 `New-ProvScheme` 时将其配置为 `true`。如果未指定此属性，则默认情况下将参数设置为 `False`。

例如，使用 `CustomProperties` 参数将 `UseTempDiskForWBC` 设置为 `true`：

```
1 -CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-instance"> `
2 <Property xsi:type="StringProperty" Name="PersistWBC" Value="false" /> `
3 <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false" /> `
4 <Property xsi:type="StringProperty" Name="PersistVm" Value="false" /> `
5 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="Premium_LRS" /> `
6 <Property xsi:type="StringProperty" Name="WBCDiskStorageType" Value="Premium_LRS" /> `
7 <Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" /> `
8 <Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="true" /> `
9 </CustomProperties>'
10 <!--NeedCopy-->
```

### 注意：

提交计算机目录以使用 Azure 本地临时存储作为回写式缓存文件后，以后无法更改为使用 VHD。

## 使用永久回写式缓存磁盘创建计算机目录

要使用永久回写缓存磁盘配置目录，请使用 PowerShell 参数 `New-ProvScheme CustomProperties`。

### 提示：

请仅将 PowerShell 参数 `New-ProvScheme CustomProperties` 用于基于云的托管连接。如果您

想使用永久回写式缓存磁盘为本地解决方案（例如 XenServer）预配计算机，则不需要 PowerShell，因为该磁盘会自动保存。

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。

注意：

此行为同时适用于 Azure 和 GCP，在重启电源时，默认 MCSIO 回写式缓存磁盘将删除并重新创建。可以选择保留该磁盘，以避免删除和重新创建 MCSIO 回写式缓存磁盘。

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">
2   <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
3   <Property xsi:type="StringProperty" Name="StorageAccountType" Value="Premium_LRS" />
4   <Property xsi:type="StringProperty" Name="ResourceGroups" Value="benva1dev5RG3" />
5 </CustomProperties>
6 <!--NeedCopy-->
```

注意：

此示例仅适用于 Azure。在 GCP 环境中，这些属性是不同的。

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**。

当 Citrix DaaS 管理员从管理界面关闭计算机时，将 `PersistWBC` 属性设置为 **true** 不会删除回写式缓存磁盘。

当 Citrix DaaS 管理员从管理界面关闭计算机时，将 `PersistWBC` 属性设置为 **false** 会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**，并在从管理界面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：

```
1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
2   <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
3   <Property xsi:type="StringProperty" Name="StorageAccountType" Value="Premium_LRS" />
```



```

4 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
    benvaldev5RG3" />
5 <Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
6 </CustomProperties>
7 <!--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：

```

1 New-ProvScheme
2 -CleanOnBoot
3 -CustomProperties "<CustomProperties xmlns='http://schemas.citrix.com
    /2014/xd/machinecreation' xmlns:xsi='http://www.w3.org/2001/
    XMLSchema-instance'">
4 <Property xsi:type='StringProperty' Name='UseManagedDisks' Value='
    true' />
5 <Property xsi:type='StringProperty' Name='StorageAccountType' Value
    ='Premium_LRS' />
6 <Property xsi:type='StringProperty' Name='ResourceGroups' Value='
    benvaldev5RG3' />
7 <Property xsi:type='StringProperty' Name='PersistWBC' Value='true'
    />
8 </CustomProperties>"
9 -HostingUnitName "adSubnetScale1"
10 -IdentityPoolName "BV-WBC1-CAT1"
11 -MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
    GoldImages.resourcegroup\W10MCSI0-01
    _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
12 -NetworkMapping @{
13     "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }
14
15 -ProvisioningSchemeName "BV-WBC1-CAT1"
16 -ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
    folder\Standard_D2s_v3.serviceoffering"
17 -UseWriteBackCache
18 -WriteBackCacheDiskSize 127
19 -WriteBackCacheMemorySize 256
20 <!--NeedCopy-->

```

**使用 MCSIO 提高启动性能**

启用 MCSIO 后，可以提高 Azure 和 GCP 托管磁盘的引导性能。请使用 **New-ProvScheme** 命令中的 PowerShell **PersistOSDisk** 自定义属性配置此功能。与 **New-ProvScheme** 关联的选项包括：



```

1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
  instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
  />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
  Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
  benvaldev5RG3" />
5 <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
  />
6 </CustomProperties>
7 <!--NeedCopy-->

```

要启用此功能，请将 **PersistOsDisk** 自定义属性设置为 **true**。例如：

```

1 New-ProvScheme
2 -CleanOnBoot
3 -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=`"
  StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
  /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
  Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
  =`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
4 -HostingUnitName "adSubnetScale1"
5 -IdentityPoolName "BV-WBC1-CAT1"
6 -MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
  GoldImages.resourcegroup\W10MCSI0-01
  _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
7 -NetworkMapping @{
8   "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
  CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
  adSubnetScale1.network" }
9
10 -ProvisioningSchemeName "BV-WBC1-CAT1"
11 -ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
  folder\Standard_D2s_v3.serviceoffering"
12 -UseWriteBackCache
13 -WriteBackCacheDiskSize 127
14 -WriteBackCacheMemorySize 256
15 <!--NeedCopy-->

```

使用客户管理的加密密钥创建计算机目录

如果要使用 PowerShell 命令创建计算机目录，其中加密密钥是客户管理的密钥，请执行以下操作：

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。

3. 输入 `cd xdhyp:/`。
4. 输入 `cd .\HostingUnits\(your hosting unit)`。
5. 输入 `cd diskencryptionset.folder`。
6. 输入 `dir` 以获取磁盘加密集列表。
7. 复制磁盘加密集的 ID。
8. 创建包含磁盘加密集的 ID 的自定义属性字符串。例如：

```

1 $customProperties = "<CustomProperties xmlns='http://schemas.
  citrix.com/2014/xd/machinecreation' xmlns:xsi='http://www.w3.
  org/2001/XMLSchema-instance'">
2 <Property xsi:type='StringProperty' Name='persistWBC' Value='
  False' />
3 <Property xsi:type='StringProperty' Name='PersistOsDisk' Value
  ='false' />
4 <Property xsi:type='StringProperty' Name='UseManagedDisks'
  Value='true' />
5 <Property xsi:type='StringProperty' Name='DiskEncryptionSetId'
  Value='/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxxx/
  resourceGroups/abc/providers/Microsoft.Compute/
  diskEncryptionSets/abc-des' />
6 </CustomProperties>
7 <!--NeedCopy-->

```

9. 创建标识池（如果尚未创建）。例如：

```

1 New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
  Domain def.local -NamingSchemeType Numeric
2 <!--NeedCopy-->

```

10. 运行 `New-ProvScheme` 命令：例如：

```

1 New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
  IdentityPoolName "name" -InitialBatchSizeHint 1
2 -MasterImageVM "XDHyp:\HostingUnits\azure-res2\image.folder\def.
  resourcegroup\def.snapshot"
3 -NetworkMapping @{
4   "0"="XDHyp:\HostingUnits\azure-res2\virtualprivatecloud.folder\
  def.resourcegroup\def-vnet.virtualprivatecloud\subnet1.network
  " }
5
6 -ProvisioningSchemeName "name"
7 -ServiceOffering "XDHyp:\HostingUnits\azure-res2\serviceoffering.
  folder\Standard_DS2_v2.serviceoffering"
8 -MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.folder<
  def.resourcegroup><machine profile vm.vm>"
9 -CustomProperties $customProperties
10 <!--NeedCopy-->

```

11. 完成计算机目录的创建。

## 创建具有主机加密功能的计算机目录

### 创建具有主机加密功能的计算机目录

1. 检查订阅是否启用了主机加密功能。为此，请参阅<https://learn.microsoft.com/en-us/rest/api/resources/features/get?tabs=HTTP/>。如果未启用，则必须为订阅启用该功能。有关为您的订阅启用该功能的信息，请参阅 <https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/>。
2. 检查特定 Azure VM 大小是否支持主机加密。要执行此操作，请在 PowerShell 窗口中运行以下任一命令：

```
1 PS XDHyp:\Connections<your connection>\east us.region\  
   serviceoffering.folder>  
2 <!--NeedCopy-->
```

```
1 PS XDHyp:\HostingUnits<your hosting unit>\serviceoffering.folder>  
2 <!--NeedCopy-->
```

3. 在 Azure 门户中创建虚拟机或模板规范，作为计算机配置文件的输入，启用主机加密。
  - 如果要创建 VM，请选择支持主机加密功能的 VM 大小。创建 VM 后，VM 属性 **Encryption at host**（主机加密）处于启用状态。
  - 如果要使用模板规范，请在 `securityProfile` 内部将参数 `Encryption at Host` 指定为 **true**。
4. 通过选择 VM 或模板规范，使用计算机配置文件工作流程创建 MCS 计算机目录。
  - 操作系统磁盘/数据磁盘：通过客户管理的密钥和平台管理的密钥进行加密
  - 临时操作系统磁盘：仅通过平台管理的密钥进行加密
  - 缓存磁盘：通过客户管理的密钥和平台管理的密钥进行加密

您可以使用完整配置界面或运行 PowerShell 命令来创建计算机目录。

### 从计算机配置文件中检索主机加密信息

运行带有 `AdditionalData` 参数的 PowerShell 命令时，可以从计算机配置文件中检索主机加密信息。如果 `EncryptionAtHost` 参数设置为 **True**，则表示已为计算机配置文件启用主机加密。

例如：当计算机配置文件输入为 VM 时，请运行以下命令：

```
1 (get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.  
   resourcegroup\def.vm).AdditionalData  
2 <!--NeedCopy-->
```

例如：当计算机配置文件输入是模板规范时，运行以下命令：

```
1 (get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.  
   resourcegroup\def_templatespec.templatespec\EncryptionAtHost.  
   templatespecversion).AdditionalData  
2 <!--NeedCopy-->
```

## 使用双重加密创建计算机目录

您可以使用完整配置界面和 PowerShell 命令创建和更新采用双重加密的计算机目录。

有关如何使用双重加密创建计算机目录的详细步骤如下：

1. 使用平台管理的密钥和客户管理的密钥创建 Azure Key Vault 和 DES。有关如何创建 Azure 密钥保管库和 DES 的信息，请参阅[使用 Azure 门户为托管磁盘启用静态双重加密](#)。
2. 要浏览主机连接中可用的磁盘加密集，请执行以下操作：

- a) 打开 **PowerShell** 窗口。
- b) 运行以下 PowerShell 命令：
  - i. `asnp citrix*`
  - ii. `cd xdhyp:`
  - iii. `cd HostingUnits`
  - iv. `cd YourHostingUnitName` (ex. `azure-east`)
  - v. `cd diskencryptionset.folder`
  - vi. `dir`

可以使用 `DiskEncryptionSet` 的 ID 通过自定义属性创建或更新目录。

3. 如果您想使用计算机配置文件工作流程，请创建 VM 或模板规范作为计算机配置文件输入。
  - 如果您想使用 VM 作为计算机配置文件输入：
    - a) 在 Azure 门户中创建 VM。
    - b) 导航到磁盘 > 密钥管理，直接使用任何 `DiskEncryptionSetID` 加密 VM。
  - 如果您想使用模板规范作为计算机配置文件输入：
    - a) 在模板中的 `properties>storageProfile>osDisk>managedDisk` 下，添加 `diskEncryptionSet` 参数并添加双重加密 DES 的 ID。
4. 然后，创建计算机目录。
  - 如果使用完整配置界面，除了[创建计算机目录](#)中的步骤外，还要执行以下任一操作。
    - 如果您不使用基于计算机配置文件的工作流程，请在磁盘设置页面上，选择使用以下密钥加密每台计算机上的数据。然后，从下拉列表中选择您的双重加密 DES。继续创建目录。
    - 如果使用计算机配置文件工作流程，请在映像页面上，选择主映像（或准备好的映像）和计算机配置文件。确保计算机配置文件的属性中包含磁盘加密集 ID。

在目录中创建的所有计算机都通过与您选择的 DES 关联的密钥进行双重加密。

- 如果使用 PowerShell 命令，请执行以下操作之一：
  - 如果不使用基于计算机配置文件的工作流程，请在 `New-ProvScheme` 命令中添加自定义属性 `DiskEncryptionSetId`。例如：

```
1 New-ProvScheme -CleanOnBoot -CustomProperties '<
    CustomProperties xmlns="http://schemas.citrix.com/2014/
    xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks"
    Value="true" />
3 <Property xsi:type="StringProperty" Name="
    StorageAccountType" Value="Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="
    DiskEncryptionSetId" Value="/subscriptions/12345678-
    xxxx-1234-1234-123456789012/resourceGroups/Sample-RG/
    providers/Microsoft.Compute/diskEncryptionSets/
    SampleEncryptionSet" />
5 </CustomProperties>'
6 -HostingUnitName "Redacted"
7 -IdentityPoolName "Redacted"
8 -InitialBatchSizeHint 1
9 -MasterImageVM "Redacted"
10 -NetworkMapping @{
11 "0"="Redacted" }
12
13 -ProvisioningSchemeName "Redacted"
14 -ServiceOffering "Redacted"
15 <!--NeedCopy-->
```

- 如果使用基于计算机配置文件的工作流程，请在 `New-ProvScheme` 命令中使用计算机配置文件输入。例如：

```
1 New-ProvScheme -CleanOnBoot
2 -HostingUnitName azure-east
3 -IdentityPoolName aio-ip
4 -InitialBatchSizeHint 1
5 -MasterImageVM XDHyp:\HostingUnits\azure-east\image.folder
    \abc.resourcegroup\fgb-vda-snapshot.snapshot
6 -NetworkMapping @{
7 "0"="XDHyp:\HostingUnits\azure-east\virtualprivatecloud.
    folder\apa-resourceGroup.resourcegroup\apa-
    resourceGroup-vnet.virtualprivatecloud\default.network"
    }
8
9 -ProvisioningSchemeName aio-test
10 -MachineProfile XDHyp:\HostingUnits\azure-east\
    machineprofile.folder\abc.resourcegroup\abx-mp.
    templatespec\1.0.0.templatespecversion
11 <!--NeedCopy-->
```

使用 Remote PowerShell SDK 完成目录的创建。有关如何使用 Remote PowerShell SDK 创建目录的信息，请参阅 <https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>。在目录中创建的所有计算机均使用与您选择的 DES 关联的密钥进行双重加密。

将未加密的目录转换为使用双重加密

只有在计算机目录之前未加密的情况下，才能更新计算机目录的加密类型（使用自定义属性或计算机配置文件）。

- 如果不使用基于计算机配置文件的工作流程，请在 `Set-ProvScheme` 命令中添加自定义属性 `DiskEncryptionSetId`。例如：

```
1 Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
2 -CustomProperties '<CustomProperties xmlns="http://schemas.citrix
   .com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org
   /2001/XMLSchema-instance">
3   <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
   Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
   resourceGroups/Sample-RG/providers/Microsoft.Compute/
   diskEncryptionSets/SampleEncryptionSet" />
4 </CustomProperties>'
5 <!--NeedCopy-->
```

- 如果使用基于计算机配置文件的工作流程，请在 `Set-ProvScheme` 命令中使用计算机配置文件输入。例如：

```
1 Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
   XDHy:\HostingUnits\azure-east\machineprofile.folder\aelx.
   resourcegroup\elx-mp.templatespec\1.0.0.templatespecversion
2 <!--NeedCopy-->
```

成功后，您在目录中添加的所有新 VM 都将使用与您选择的 DES 关联的密钥进行双重加密。

验证目录是否经过双重加密

- 在完整配置界面中：

1. 导航到计算机目录。
2. 选择要验证的目录。单击屏幕底部附近的模板属性选项卡。
3. 在 **Azure** 详细信息下，验证磁盘加密集中的磁盘加密 ID。如果目录的 DES ID 为空，则目录未加密。
4. 在 Azure 门户中，验证与 DES ID 关联的 DES 的加密类型是否为平台管理的密钥和客户管理的密钥。

- 使用 PowerShell 命令：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。

3. 使用 `Get-ProvScheme` 可获取您的计算机目录信息。例如：

```
1 Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
2 <!--NeedCopy-->
```

4. 检索计算机目录的 DES ID 自定义属性。例如：

```
1 <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
  Value="/subscriptions
    /12345678-1234-1234-1234-123456789012/resourceGroups/Sample
    -RG/providers/Microsoft.Compute/diskEncryptionSets/
    SampleEncryptionSet" />
2 <!--NeedCopy-->
```

5. 在 Azure 门户中，验证与 DES ID 关联的 DES 的加密类型是否为平台管理的密钥和客户管理的密钥。

页面文件位置

在 Azure 环境中，页面文件位置是在首次创建 VM 时设置的。页面文件设置的格式为：页面文件位置 [最小大小] [最大大小]（以 MB 为单位的大小）。有关详细信息，请参阅[如何确定适当的页面文件大小](#)。

在映像准备过程中，当您创建预配方案时，MCS 会根据特定规则确定页面文件的位置。创建预配方案后，您不能：

- 更改 VM 大小
- 更新计算机配置文件
- 更改 EOS 和 MCS I/O 属性

页面文件位置确定

EOS 和 MCS I/O 等功能有自己的预期页面文件位置，并且是相互独有的。下表显示了每个功能的预期页面文件位置：

功能	预期页面文件位置
EOS	操作系统磁盘
MCS I/O	首先是 Azure 临时磁盘，否则写回缓存磁盘

注意：

即使将映像准备与预配方案创建分离，MCS 也会正确地确定页面文件的位置。默认页面文件位置位于操作系统磁盘上。

页面文件设置场景

下表描述了映像准备和预配方案更新期间页面文件设置的一些可能情形：

在	场景	结果
映像准备	您可以在临时磁盘上设置源映像页面文件，而在预配方案中指定的 VM 大小没有临时磁盘	页面文件放置在操作系统上
映像准备	可以在操作系统磁盘上设置源映像页面文件，而在预配方案中指定的 VM 大小具有临时磁盘	页面文件放置在临时磁盘上
映像准备	可以在临时磁盘上设置源映像页面文件，并在预配方案中启用临时操作系统磁盘	页面文件放置在操作系统磁盘上
预配方案更新	您尝试更新预配方案。原来的 VM 大小有一个临时磁盘，而目标 VM 没有临时磁盘	拒绝带错误消息的更改
预配方案更新	您尝试更新预配方案。原始 VM 大小没有临时磁盘，而目标 VM 有临时磁盘	拒绝带错误消息的更改

更新页面文件设置

使用 PowerShell 命令，您可以指定页面文件设置，包括位置和大小。这将覆盖 MCS 确定的页面文件设置。您可以通过在创建计算机目录期间运行以下 `New-ProvScheme` 命令来完成此操作。

注意：

即使您在主映像上手动配置页面文件，虚拟机的页面文件设置也设置为系统管理。您只能使用 PowerShell 命令创建具有定制页面文件设置的计算机目录。

```
1 New-ProvScheme -CleanOnBoot `
2 -HostingUnitName "zijinnet" `
3 -IdentityPoolName "PageFileSettingExample" `
4 -ProvisioningSchemeName "PageFileSettingExample" `
5 -InitialBatchSizeHint 1 `
6 -MasterImageVM "XDHyp:\HostingUnits\zijinnet\image.folder\neal-
    zijincloud-resources.resourcegroup\
    CustomWin10VDA_0sDisk_1_9473d7c8a6174b2c8284c7d3efeea88f.manageddisk
    " `
7 -NetworkMapping @{
8   "0"="XDHyp:\HostingUnits\zijinnet\virtualprivatecloud.folder\East US.
    region\virtualprivatecloud.folder\neal-zijincloud-resources.
    resourcegroup\neal-zijincloud-resources-vnet.virtualprivatecloud\
    default.network" }
9 `
10 -ServiceOffering "XDHyp:\HostingUnits\zijinnet\serviceoffering.folder\
    Standard_B2ms.serviceoffering" `
```



```

11 -CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com
    /2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
    XMLSchema-instance"> `
12 <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
    "/> `
13 <Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
14 <Property xsi:type="StringProperty" Name="
    PageFileDiskDriveLetterOverride" Value="d"/> `
15 <Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
    Value="2048"/> `
16 <Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value
    ="8196"/> `
17 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS"/> `
18 <Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client"/> `
19 </CustomProperties>'
20 <!--NeedCopy-->

```

有关如何使用 Remote PowerShell SDK 创建目录的信息，请参阅[使用 PowerShell 创建目录](#)。

限制：

- 只有在通过运行 **New-ProvScheme** 命令创建预配方案时，才能更新页面文件设置。以后无法更改页面文件设置。
- 您必须在 **New-ProvScheme** 命令中提供所有自定义属性（“PageFileDiskDriveLetterOverride”、“InitialPageFileSizeInMB”和“MaxPageFileSizeInMB”），或者不提供任何自定义属性。
- Citrix Studio 不支持此功能。
- 初始页面文件大小必须介于 16 MB 到 16777216 MB 之间。
- 最大页面文件大小必须大于或等于初始页面文件大小且小于 16777216 MB。
- 您可以同时将初始页面文件大小和最大页面文件大小设置为零。

配置启用 **AMA** 的目录虚拟机

#### 1. 设置计算机配置文件模板。

- 如果您想使用 VM 作为计算机配置文件模板：
  - a) 在 Azure 门户上创建 VM。
  - b) 打开 VM 的电源。
  - c) 将 VM 添加到资源下的数据收集规则中。这会调用模板 VM 上的代理安装。

注意：

如果必须创建 Linux 目录，请设置一台 Linux 计算机。

- 如果您想使用模板规范作为计算机配置文件模板：
  - a) 设置模板规范。

b) 将以下扩展程序和数据收集规则关联添加到生成的模板规范中：

```

1  {
2
3  "type": "Microsoft.Compute/virtualMachines/extensions",
4  "apiVersion": "2022-03-01",
5  "name": "<vm-name>/AzureMonitorWindowsAgent",
6  "dependsOn": [
7      "Microsoft.Compute/virtualMachines/<vm-name>"
8  ],
9  "location": "<azure-region>",
10 "properties": {
11
12     "publisher": "Microsoft.Azure.Monitor",
13     "type": "AzureMonitorWindowsAgent",
14     "typeHandlerVersion": "1.0",
15     "autoUpgradeMinorVersion": true,
16     "enableAutomaticUpgrade": true
17 }
18
19 }
20 ,
21 {
22
23     "type": "Microsoft.Insights/
24         dataCollectionRuleAssociations",
25     "apiVersion": "2021-11-01",
26     "name": "<associatio-name>",
27     "scope": "Microsoft.Compute/virtualMachines/<vm-name>",
28     "dependsOn": [
29         "Microsoft.Compute/virtualMachines/<vm-name>",
30         "Microsoft.Compute/virtualMachines/<vm-name>/extensions
31         /AzureMonitorWindowsAgent"
32     ],
33     "properties": {
34
35         "description": "Association of data collection rule.
36             Deleting this association will break the data
37             collection for this Arc server.",
38         "dataCollectionRuleId": "/subscriptions/<azure-
39             subscription>/resourcegroups/<azure-resource-group>
40             /providers/microsoft.insights/datacollectionrules
41             /<azure-data-collection-rule>"
42     }
43 }
44
45 }
46
47 <!--NeedCopy-->

```

注意：

如果您使用 Microsoft Sentinel 数据连接器设置了数据收集规则，则只需按照与常规 DCR 关联相

同的方式在模板规范中添加 `dataCollectionRuleAssociation` 即可。然后，目录虚拟机可以显示在 Sentinel DCR 中，AMA 将安装在这些 VM 上。有关创建数据收集规则的最佳做法的信息，请参阅在 [Azure Monitor 中创建和管理数据收集规则的最佳做法](#)。

## 2. 创建或更新现有的 MCS 计算机目录。

- 要创建新 MCS 目录，请执行以下操作：

- a) 在“完整配置”界面中选择该 VM 或模板规范作为计算机配置文件。
- b) 继续执行后续步骤以创建目录。

- 要更新现有 MCS 目录，请使用以下 PowerShell 命令。在这种情况下，只有新虚拟机才能获得更新的计算机配置文件模板。

```
1 Set-ProvScheme -ProvisioningSchemeName "name"
2 -MachineProfile "XDHyp:\HostingUnits\Unit1\machineprofile.
   folder\abc.resourcegroup\ab-machine-profile.vm"
3 <!--NeedCopy-->
```

- 要使用更新的计算机配置文件模板更新现有虚拟机，请运行 `Set-ProvScheme`，然后运行 `Set-ProvVMUpdateTimeWindow`：

```
1 Set-ProvScheme -ProvisioningSchemeName "name" -MachineProfile
   "XDHyp:\HostingUnits\Unit1\machineprofile.folder\abc.
   resourcegroup\ab-machine-profile.vm"
2 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
   -StartsNow -DurationInMinutes -1
3 <!--NeedCopy-->
```

## 3. 打开目录 VM 的电源。

4. 前往 Azure 门户，检查监视器扩展程序是否安装在虚拟机上，虚拟机是否显示在 DCR 的资源下。几分钟后，监视数据将显示在 Azure Monitor 上。

## 故障排除

有关 Azure Monitor 代理的故障排除指南中的信息，请参阅以下内容：

- <https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/>
- <https://learn.microsoft.com/en-us/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/>

## 使用 Azure 现成 VM 创建目录

Azure 现成 VM 允许您利用 Azure 未使用的计算容量，从而节省大量成本。但是，分配 Azure Spot 虚拟机的能力取决于当前的容量和价格。因此，Azure 可能会逐出您的正在运行的 VM，无法创建 VM，或者无法按照 [Eviction policy](#)

(逐出策略) 打开 VM 的电源。因此，Azure 现成 VM 适用于某些非关键应用程序和桌面。有关详细信息，请参阅 [Use Azure Spot Virtual Machines](#) (使用 Azure 现成虚拟机)。

#### 限制

- Azure 现成 VM 不支持所有 VM 大小。有关详细信息，请参阅[限制](#)。

可以运行以下 PowerShell 命令来检查 VM 大小是否支持现成 VM。如果 VM 大小支持现成 VM，则 `SupportsSpotVM` 设置为 **True**。

```
1 (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\serviceoffering.  
   folder\Standard_D2ds_v4.serviceoffering"). AdditionalData  
2 <!--NeedCopy-->
```

- 目前，Azure 现成 VM 不支持休眠。

#### 要求

为 Azure 现成 VM 目录创建计算机配置文件源 (VM 或模板规范) 时，必须选择 Azure 现成实例 (如果使用 VM) 或者将 `priority` 设置为 `Spot` (如果使用模板规范)。

#### 使用 Azure 现成 VM 创建目录的步骤

##### 1. 创建计算机配置文件源 (VM 或启动模板)。

- 要使用 Azure 门户创建 VM，请参阅[使用 Azure 门户部署 Azure Spot 虚拟机](#)。
- 要创建模板规范，请在模板规范中的 **resources > type: Microsoft.Compute/virtualMachines > properties** 下添加以下属性。例如：

```
1 "priority": "Spot",  
2 "evictionPolicy": "Deallocate",  
3 "billingProfile": {  
4  
5   "maxPrice": 0.01  
6 }  
7  
8 <!--NeedCopy-->
```

#### 注意：

- 逐出策略可以是 **Deallocate** (取消分配) 或 **Delete** (删除)。
  - 对于非永久 VM，MCS 始终将逐出策略设置为 **Delete** (删除)。如果 VM 已逐出，则会将其与所有非永久磁盘 (例如，操作系统磁盘) 一起删除。不会删除任何永久磁盘 (例如，身份磁盘)。但是，如果目录类型为永久或者自定义属性 `PersistOsDisk` 设置为 “True”，操作系统磁盘

将具有永久。同样，如果将自定义属性 **PersistWbc** 设置为 **True**，WBC 磁盘将具有永久。

- 对于永久 VM，MCS 始终将逐出策略设置为“Deallocate”（取消分配）。如果 VM 已逐出，它将被取消分配。未对磁盘进行任何更改。
- 最高价格是您愿意每小时支付的价格。如果您使用的是 **Capacity Only**（仅限容量），此值将为 **-1**。最高价格只能为 null、-1 或大于零的十进制数。有关详细信息，请参阅 [Pricing](#)（定价）。

2. 可以运行以下 PowerShell 命令来检查计算机配置文件是否启用了 Azure 现成 VM。如果 **SpotEnabled** 参数设置为 **True** 且 **SpotEvictionPolicy** 设置为 **Deallocate**（取消分配）或 **Delete**（删除），则计算机配置文件启用了 Azure 现成 VM。例如，

- 如果计算机配置文件源为 VM，请运行以下命令：

```
1 (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
   .folder\fifthcolumn.resourcegroup\kb-spot-delete.vm").
   AdditionalData
2 <!--NeedCopy-->
```

- 如果计算机配置文件源为模板规范，请运行以下命令：

```
1 (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
   .folder\fifthcolumn.resourcegroup\fc-aeh-templatespec.
   templatespec\14.0.0-spot-delete.templatespecversion").
   AdditionalData
2 <!--NeedCopy-->
```

3. 使用计算机配置文件通过 **New-ProvScheme** PowerShell 命令创建计算机目录。

可以使用 **Set-ProvScheme** 命令更新目录。也可以使用 PowerShell 命令 **Set-ProvVmUpdateTimeWindow** 更新现有 VM。计算机配置文件将在下次打开电源时更新。

#### 正在运行的 **Azure** 现成 **VM** 上的逐出

如果计算容量不可用或者每小时价格高于配置的最高价格，Azure 会逐出正在运行的现成 VM。默认情况下，您不会收到逐出通知。VM 只会冻结并且 VM 会被逐出。Microsoft 建议使用计划事件来监视逐出。请参阅 [Continuously monitor for eviction](#)（持续监视逐出）。您还可以在 VM 内部运行脚本，以便在逐出之前收到通知。例如，Microsoft 在 Python [ScheduledEvents.cs](#) 中有一个投票脚本。

#### 故障排除

- 可以使用 **Get-ProvVM** 命令在预配的 VM 的 customMachineData 中查看现成 VM 属性。如果优先级字段设置为 **Spot**（现成虚拟机），则将使用现成虚拟机。
- 可以在 Azure 门户中检查 VM 是否在使用现成虚拟机：

1. 在 Azure 门户中查找 VM。

2. 转到 **Overview**（概述）页面。
3. 向下滚动到底部并找到 **Azure Spot**（Azure 现成虚拟机）部分。
  - 如果未使用现成虚拟机，则此字段为空。
  - 如果正在使用现成 VM，则会设置 **Azure Spot**（Azure 现成虚拟机）和 **Azure Spot eviction policy**（Azure 现成虚拟机逐出策略）字段。
1. 可以在“配置”页面上查看 VM 的计费配置文件或每小时最高价格。

### 复制所有资源上的标记

可以将计算机配置文件中指定的标记复制到所有资源，例如新 VM 或计算机目录中的现有 VM 的多个 NIC 和磁盘（操作系统磁盘、身份磁盘和回写式缓存磁盘）。计算机配置文件来源可以是 VM 或 ARM 模板规范。

注意：

必须在标记上添加策略（请参阅[为标记合规性分配策略定义](#)）或者在计算机配置文件源中添加标记以保留资源上的被标记。

### 必备条件

创建计算机配置文件源（VM 或 ARM 模板规范），以便在 VM、磁盘和该 VM 的 NIC 上添加标记。

- 如果您想将 VM 作为计算机配置文件输入，请在 VM 和 Azure 门户中的所有资源上应用标记。请参阅 [Apply tags with Azure portal](#)（使用 Azure 门户应用标记）。
- 如果您想将 ARM 模板规范作为计算机配置文件输入，请在每个资源下添加以下标记块。

```
1  "tags": {  
2  
3  "TagC": "Value3"  
4  }  
5  ,  
6  <!--NeedCopy-->
```

注意：

模板规范中最多可以有一个磁盘和至少一个 NIC。

### 将标记复制到新计算机目录中的 VM 的资源

1. 使用 VM 或 ARM 模板规范作为计算机配置文件输入来创建非永久目录或永久目录。
2. 将 VM 添加到目录中并打开电源。您必须看到在计算机配置文件中指定的标记复制到该 VM 的相应资源。

**注意：**

如果在计算机配置文件中提供的 NIC 数量与您希望 VM 使用的 NIC 数量不匹配，则会出现错误。

**修改现有 VM 的资源上的标记**

1. 使用所有资源上的标记创建计算机配置文件。
2. 使用更新后的计算机配置文件更新现有计算机目录。例如：

```
1 Set-ProvScheme -ProvisioningSchemeName <YourCatalogName> -  
  MachineProfile <PathToYourMachineProfile>  
2 <!--NeedCopy-->
```

3. 关闭要对其应用更新的 VM。
4. 申请 VM 的预定更新。例如：

```
1 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <  
  YourCatalogName> -VMName machine1 -StartsNow -  
  DurationInMinutes -1  
2 <!--NeedCopy-->
```

5. 打开 VM。
6. 您必须看到在计算机配置文件中指定的标记复制到相应的资源。

**注意：**

如果在计算机配置文件中提供的 NIC 数量与在 `Set-ProvScheme` 中提供的 NIC 数量不匹配，则会出现错误。

**下一步的去向**

- 如果这是创建的第一个目录，系统将引导您[创建交付组](#)。
- 要查看整个配置过程，请参阅[规划和构建部署](#)。
- 要管理目录，请参阅[管理计算机目录](#)和[管理 Microsoft Azure 目录](#)。

**更多信息**

- [创建和管理连接和资源](#)
- [与 Microsoft Azure Resource Manager 的连接](#)
- [创建计算机目录](#)

## 创建 Microsoft System Center Virtual Machine Manager 目录

February 20, 2024

[创建计算机目录](#)介绍了用于创建计算机目录的向导。以下信息涵盖了特定于 Microsoft System Center Virtual Machine Manager (VMM) 虚拟化环境的详细信息。

注意：

在创建 VMM 目录之前，您需要完成创建与 VMM 的连接。请参阅[与 Microsoft System Center Virtual Machine Manager 的连接](#)。

### 创建主 VM

- 在主 VM 上安装 VDA，然后选择用于优化桌面的选项。这样会提高性能。
- 生成主 VM 的快照作为备份。
- 创建虚拟桌面。

### SMB 3 文件共享上的 MCS

对于在虚拟机存储的 SMB 3 文件共享上使用 MCS 创建的计算机目录，凭据必须满足以下要求，才能确保来自 XenServer 通信库 (HCL) 的呼叫成功连接到 SMB 存储。

- VMM 用户凭据必须包含对 SMB 存储的完全读取写入权限。
- 虚拟机生命周期事件期间的存储虚拟磁盘操作通过 Hyper-V 服务器使用 VMM 用户凭据执行。

有关 SMB 3 的详细信息，请参阅[在 Windows Server 中使用 SMB 3 协议共享文件概述](#)。

在 Windows Server 2012 上同时使用 VMM 2012 SP1 和 Hyper-V 时：使用 SMB 作为存储时，启用 Cloud Connector 到单个 Hyper-V 计算机的身份验证凭据安全支持提供程序 (CredSSP)。有关详细信息，请参阅 [CTX137465](#)。

使用标准 PowerShell V3 远程会话时，Cloud Connector 中的 HCL 将使用 CredSSP 打开与 Hyper-V 计算机的连接。此功能可将 Kerberos 加密的用户凭据传递到 Hyper-V 计算机，并在使用所提供的凭据（本例中指 VMM 用户的凭据）运行的远程 Hyper-V 计算机上的此会话中传递 PowerShell 命令，以便存储的通信命令正确运行。

以下任务使用 HCL 中的 PowerShell 脚本。这些脚本随后将被发送到 Hyper-V 计算机以在 SMB 3.0 存储中使用。

合并主映像：主映像可创建新的 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新 VM（并删除对初始主 VM 的依赖）。

ConvertVirtualHardDisk 位于 root\virtualization\v2 命名空间

示例：



```
1 $ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
2 $result = $ims.ConvertVirtualHardDisk($diskName, $vhdaText)
3 $result
4 <!--NeedCopy-->
```

创建差异磁盘：根据合并映像生成的映像创建差异磁盘。然后将差异磁盘连接到新虚拟机。

CreateVirtualHardDisk 位于 root\virtualization\v2 命名空间

示例：

```
1 $ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
2 $result = $ims.CreateVirtualHardDisk($vhdaText);
3 $result
4 <!--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 Cloud Connector 中读取磁盘，因此 HCL 必须首先通过 Hyper-V 计算机复制身份磁盘，如下所述。

1. HCL 通过管理员共享将身份上载到 Hyper-V 计算机。
2. Hyper-V 计算机通过 PowerShell 远程会话中运行的 PowerShell 脚本将磁盘复制到 SMB 存储。  
将在 Hyper-V 计算机上创建一个文件夹，此文件夹的权限已锁定，仅 VMM 用户有权访问（通过远程 PowerShell 连接）。
3. HCL 删除管理员共享中的文件。
4. 当 HCL 完成向 Hyper-V 计算机的身份磁盘上载后，远程 PowerShell 会话会将身份磁盘复制到 SMB 存储，然后将其从 Hyper-V 计算机中删除。

如果删除标识磁盘文件夹，则会重新创建该文件夹，以供重复使用。

下载身份磁盘：与上载一样，身份磁盘通过 Hyper-V 计算机传递到 HCL。以下过程将在 Hyper-V 服务器上创建一个仅具有 VMM 用户权限的文件夹（如果尚不存在）。

1. HyperV 计算机使用在 PowerShell V3 远程会话中运行的 PowerShell 脚本将磁盘从 SMB 存储复制到本地 Hyper-V 存储。
2. HCL 将 Hyper-V 计算机管理员共享中的磁盘读取到内存。
3. HCL 删除管理员共享中的文件。

### 使用计算机配置文件创建目录

可以使用计算机配置文件在 System Center Virtual Machine Manager (SCVMM) 环境中创建和更新 MCS 计算机目录。还可以启用嵌套的虚拟化和 vTPM。

## 重要注意事项

- 主映像只能是快照，不能是 VM。
- 您只能使用 VM 作为计算机配置文件源。
- 可以从 Hyper-V 控制台配置 vTPM，而非从 SCVMM 控制台配置 vTPM。
- 如果主映像启用了 vTPM，则必须在计算机配置文件源上启用 vTPM。
- vTPM 仅在第 2 代计算机上受支持。
- 如果单独提供，以下参数将覆盖在计算机配置文件中捕获的值：
  - VMcpuCount
  - VMmemoryMB
  - 磁盘存储
- 可以使用 `Set-ProvScheme` 命令更新现有目录。

## 使用计算机配置文件创建目录的步骤

1. 创建 VM 作为计算机配置文件源。有关详细信息，请参阅 [Provision virtual machines in the VMM fabric](#)（在 VMM 构造中预配虚拟机）。一旦选择 **Generation**（代系）就无法更改。
  - 如果要启用嵌套虚拟化，请在 **Select Source**（选择源）页面上选中 **Enable Nested Virtualization**（启用嵌套虚拟化）复选框。
  - 如果要启用 vTPM，则在创建 VM 后，登录 Hyper-V 主机，在 **Hyper-V Manager**（Hyper-V 管理器）下找到您的 VM。右键单击 VM，然后转到 **Settings**（设置）。在 **Security**（安全）下，选中 **Enable Trusted Platform Module**（启用可信平台模块）复选框。
2. 打开 **PowerShell** 窗口。
3. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
4. 创建 Broker 目录。此目录由即将创建的计算机进行填充。
5. 创建标识池。标识池将用作为即将创建的计算机而创建的 AD 帐户的容器。
6. 使用计算机配置文件创建预配方案。例如：

```
1 New-ProvScheme -HostingUnitName "<hostingunit name>"
2 -IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1<
  path to the checkpoint/snapshot>"
3 -ProvisioningSchemeName "<catalogname>" -MachineProfile "XDHyp:<
  path to the machine profile VM>"
4 <!--NeedCopy-->
```

7. 通过预配方案的唯一 ID 更新 Broker 目录。

8. 创建 VM 并将其添加到目录中。

可以使用 Set-ProvScheme 命令更新现有目录。例如：

```
1 Set-ProvScheme -ProvisioningSchemeName "<catalogname>" -MachineProfile  
   "XDHyp:<path to the machine profile VM>"  
2 <!--NeedCopy-->
```

下一步的去向

- 如果这是创建的第一个目录，系统将引导您[创建交付组](#)。
- 要查看整个配置过程，请参阅[规划和构建部署](#)。
- 要管理目录，请参阅[管理计算机目录](#)和[管理 Microsoft System Center Virtual Machine Manager 目录](#)。

更多信息

- [创建和管理连接和资源](#)
- [与 Microsoft System Center Virtual Machine Manager 的连接](#)
- [创建计算机目录](#)

## 创建 **Nutanix** 目录

February 9, 2024

[创建计算机目录](#)介绍了用于创建计算机目录的向导。以下信息涵盖了特定于 Nutanix 虚拟化环境的详细信息。

注意：

在创建 Nutanix 目录之前，您需要完成创建与 Nutanix 的连接。请参阅[与 Nutanix 的连接](#)。

### 使用 **Nutanix** 快照创建计算机目录

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。有关详细信息，请参阅 [Nutanix 文档](#)。

在目录创建向导中执行以下操作：

- 操作系统和计算机管理页面不包含 Nutanix 特定的信息。
- 容器或群集和容器页面是 Nutanix 所特有的。
  - 如果使用 Nutanix AHV XI 作为资源来部署计算机，请在容器页面上选择要放置 VM 身份磁盘的容器。

- 如果使用 Nutanix AHV Prism Central (PC) 作为资源部署计算机，您会看到群集和容器页面。选择用于部署 VM 的群集，然后选择容器。
- 在映像页面上，选择映像快照。如果需要，请使用 Acropolis 控制台重命名快照。如果重命名快照，请重新启动目录创建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。
- 在 **NIC** 页面上，选择 NIC 类型以筛选关联的网络。此选项仅适用于 Nutanix AHV PC 连接。有两种 NIC 类型：**VLAN** 和覆盖。选择主映像包含的一个或多个 NIC，然后为每个 NIC 选择关联的虚拟网络。
- 计算机标识、域凭据、作用域和摘要页面不包含 Nutanix 特定的信息。

## 限制

使用 Nutanix 主机连接（特别是 Nutanix AHV 插件 2.7.1 和 Nutanix AHV 插件 2.5.1）创建 MCS 目录时，已配置虚拟机的硬盘大小会错误地显示在完整配置界面上。

- Nutanix AHV 插件 2.7.1：显示的大小（1 GB）比实际存储大小小得多。
- Nutanix AHV 插件 2.5.1：显示的大小（32 GB）比实际存储大小小得多。

但是，如果主映像虚拟机是虚拟机中的快照，则可以按设计运行。

## 下一步的去向

- 如果这是创建的第一个目录，系统将引导您[创建交付组](#)。
- 要查看整个配置过程，请参阅[规划和构建部署](#)。
- 要管理目录，请参阅[管理计算机目录](#)。

## 更多信息

- [创建和管理连接和资源](#)
- [与 Nutanix 的连接](#)
- [与 Nutanix 云和合作伙伴解决方案的连接](#)
- [创建计算机目录](#)

## 创建 VMware 目录

January 23, 2024

[创建计算机目录](#)介绍了用于创建计算机目录的向导。

注意：

在创建 VMware 目录之前，您需要完成创建与 VMware 的连接。请参阅[与 VMware 的连接](#)。

### 使用计算机配置文件创建计算机目录

可以使用计算机配置文件创建 MCS 计算机目录。计算机配置文件输入的来源为 VMware 模板。计算机配置文件从 VMware 模板中捕获硬件属性并将其应用到目录中新配置的 VM。

注意：

- 主映像输入（快照）和计算机配置文件输入（VMware 模板）必须同时启用 vTPM 或者同时禁用 vTPM。此规则同时适用于 [New-ProvScheme](#) 和 [Set-ProvScheme](#)。
- 如果主映像启用了 vTPM，则 VMware 模板只能来自与主映像相同的 VM 来源。
- 加密的存储策略仅支持完整克隆。

计算机配置文件中的 VMware 模板必须存在于目录生命周期内，才能向目录预配 VM。如果没有 VMware 模板，则无法预配新 VM。删除 VMware 模板时，必须使用 [Set-ProvScheme](#) 命令提供新模板。

- MCS 捕获 VMware 模板的属性。您可以使用 [Get-Provscheme](#) 命令创建引用 VMware 模板存储属性的新 VMware 模板。
- 或者，如果存在计算机目录和已配置的虚拟机，则也可以使用 MCS 配置的计算机来创建新的 VMware 模板。

根据不同的操作系统，您可以创建具有不同配置的计算机目录：

- 如果在主映像上安装 Windows 11，则需要为主映像启用 vTPM。因此，作为计算机配置文件来源的 VMware 模板必须附加 vTPM。
- 如果 Windows 10 安装在未连接 vTPM 的主映像上，则可以使用非 vTPM VMware 模板创建计算机目录作为计算机配置文件源。

还有另一种配置，您可以使用完整复制磁盘模式创建计算机目录，并将计算机配置文件模板应用到加密的存储策略。

要使用以计算机配置文件作为输入的 PowerShell 命令创建计算机目录，请执行以下操作：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 运行以下命令：
  - 要创建一个附加 vTPM 的 VMware 模板作为计算机配置文件输入源并安装 windows11 主映像的计算机目录，请执行以下操作：

```
1 $identityPool = New-AcctIdentityPool
2 -IdentityPoolName "<string>"
3 -NamingScheme "<string>-###"
4 -NamingSchemeType Numeric
```

```

5 -Domain "<domain name>"
6 -ZoneUid "<Uid>" -Scope @()
7 <!--NeedCopy-->

```

```

1 $provScheme =New-ProvScheme -CleanOnBoot
2 -HostingUnitName "vSanRg"
3 -IdentityPoolName "<string>"
4 -InitialBatchSizeHint 1
5 -MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
   snapshot name>.snapshot"
6 -NetworkMapping @{
7 "0"="XDHyp:\HostingUnits<hosting unit name>\\<network name>.
   network" }
8
9 -ProvisioningSchemeName "<string>"
10 -Scope @() -VMCpuCount 4 -VMMemoryMB 6144
11 -MachineProfile "XDHyp:\HostingUnits<hosting unit name><
   template name>.template"
12 -TenancyType Shared
13 -FunctionalLevel "L7_20"
14 <!--NeedCopy-->

```

```

1 $catalog = New-BrokerCatalog
2 -AllocationType "Static"
3 -PersistUserChanges "OnLocal"
4 -Description "<string>" -IsRemotePC $False
5 -MinimumFunctionalLevel 'L7_9' -Name "<catalog name>" -
   ProvisioningType 'MCS'
6 -Scope @() -SessionSupport "SingleSession"
7 -ZoneUid "<Uid>"
8 <!--NeedCopy-->

```

```

1 Set-BrokerCatalog -Name "<string>"
2 -ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
3 <!--NeedCopy-->

```

- 要使用非 vTPM VMware 模板作为计算机配置文件源和 Windows10 安装的主映像创建计算机目录，请执行以下操作：

```

1 $identityPool = New-AcctIdentityPool
2 -IdentityPoolName "<string>"
3 -NamingScheme "<string>-###"
4 -NamingSchemeType Numeric
5 -Domain "<domain name>"
6 -ZoneUid "<Uid>" -Scope @()
7 <!--NeedCopy-->

```

```

1 $provScheme =New-ProvScheme -CleanOnBoot
2 -HostingUnitName "<string>"
3 -IdentityPoolName "<string>"
4 -InitialBatchSizeHint 1
5 -MasterImageVM "XDHyp:\HostingUnits<hosting unit name><

```

```

        snapshot name>.snapshot"
6  -NetworkMapping @{
7  "0"="XDHyp:\HostingUnits<hosting unit name>\\<string>.network
   " }
8
9  -ProvisioningSchemeName "<string>" -Scope @() -VMCpuCount 4
   -VMMemoryMB 8192
10 -MachineProfile "XDHyp:\HostingUnits<hosting unit name><
    template name>.template"
11 -TenancyType Shared -FunctionalLevel "L7_20"
12 <!--NeedCopy-->

```

```

1  $catalog = New-BrokerCatalog
2  -AllocationType "Static"
3  -PersistUserChanges "OnLocal" -Description "<string>" -
   IsRemotePC $False
4  -MinimumFunctionalLevel 'L7_9' -Name "<string>" -
   ProvisioningType 'MCS' -Scope @() -SessionSupport "
   SingleSession" -ZoneUid "<Uid"
5  <!--NeedCopy-->

```

```

1  Set-BrokerCatalog -Name "<string>"
2  -ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
3  <!--NeedCopy-->

```

- 要使用完整复制磁盘模式创建计算机目录，并应用加密存储策略的计算机配置文件模板，请执行以下操作：

```

1  $identityPool = New-AcctIdentityPool
2  -IdentityPoolName "<string>"
3  -NamingScheme "<string>-###"
4  -NamingSchemeType Numeric
5  -Domain "<domain name>"
6  -ZoneUid "<Uid>" -Scope @()
7  <!--NeedCopy-->

```

```

1  $provScheme =New-ProvScheme
2  -HostingUnitName "<string>"
3  -IdentityPoolName "<string>" -InitialBatchSizeHint 1
4  -MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
    snapshot name>.snapshot"
5  -NetworkMapping @{
6  "0"="XDHyp:\HostingUnits<hosting unit name>\\<string>.network
   " }
7
8  -ProvisioningSchemeName "<string>" -Scope @() -VMCpuCount 4
   -VMMemoryMB 8192
9  -MachineProfile "XDHyp:\HostingUnits<hosting unit name><
    template name>.template"
10 -TenancyType Shared -FunctionalLevel "L7_20"
11 -UseFullDiskCloneProvisioning
12 <!--NeedCopy-->

```

```

1 $catalog = New-BrokerCatalog
2 -AllocationType "Static"
3 -PersistUserChanges "OnLocal"
4 -Description "<string>"
5 -IsRemotePC $False
6 -MinimumFunctionalLevel 'L7_9' -Name "<string>" -
   ProvisioningType 'MCS' -Scope @()
7 -SessionSupport "SingleSession" -ZoneUid "<Uid>"
8 <!--NeedCopy-->

```

```

1 Set-BrokerCatalog -Name "<string>"
2 -ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
3 <!--NeedCopy-->

```

- 要更新计算机配置文件，请使用 `Set-ProvScheme` 命令。例如：

```

1 Set-ProvScheme -ProvisioningSchemeName 'name' -
   IdentityPoolName 'name' -MachineProfile 'XDHyp:\
   HostingUnits<hosting unit name><template name>.template
2 <!--NeedCopy-->

```

## 故障排除

如果目录创建失败，请参阅 [CTX294978](#)。

## 下一步的去向

- 如果这是创建的第一个目录，系统将引导您[创建交付组](#)。
- 要查看整个配置过程，请参阅[规划和构建部署](#)。
- 要管理目录，请参阅[管理计算机目录](#)和[管理 VMware 目录](#)。

## 更多信息

- [创建和管理连接和资源](#)
- [与 VMware 的连接](#)
- [与 VMware 云和合作伙伴解决方案的连接](#)
- [创建计算机目录](#)

## 创建 XenServer 目录

March 5, 2024



[创建计算机目录](#)介绍了用于创建计算机目录的向导。以下信息涵盖了特定于 XenServer（前身为 Citrix Hypervisor）虚拟化环境的详细信息。

注意：

在创建 XenServer 目录之前，需要完成创建与 XenServer 的连接。参阅[连接到 XenServer](#)。

## 使用支持 GPU 的 XenServer 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. 关闭虚拟网络计算 (Virtual Network Computing, VNC) 管理控制台以优化性能，然后重新启动 VM。
6. 系统将提示您使用 RDP。使用 RDP 安装 VDA，然后重新启动 VM。
7. 或者，创建 VM 的一个快照作为其他 GPU 主映像的基线模板。
8. 使用 RDP，安装在 XenCenter 中配置并使用 GPU 功能的客户特定应用程序。

## 使用 PowerShell 创建基于计算机配置文件的计算机目录

创建目录以使用 MCS 预配计算机时，可以使用计算机配置文件从虚拟机捕获硬件属性并将其应用到目录中新预配的 VM。如果不使用 `MachineProfile` 参数，将从主映像 VM 或快照中捕获硬件属性。

注意：

当前，您只能使用快照作为计算机配置文件输入。

您可以显式配置以下参数以覆盖计算机配置文件输入中的参数值：

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

## 使用计算机配置文件创建目录

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*`。
3. 创建标识池。标识池是要创建的 VM 的 Active Directory (AD) 帐户的容器。例如：

```

1 New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -
  IdentityPoolName "ExampleIdentityPool" -NamingScheme "abc1-##"
  -NamingSchemeType "Numeric" -Scope @() -ZoneUid "xxxxxxx"
2 <!--NeedCopy-->

```

4. 在 Active Directory 中，创建所需的 AD 计算机帐户。

```

1 $password = "password123" | ConvertTo-SecureString -AsPlainText -
  Force
2 New-AcctADAccount -IdentityPoolName "ExampleIdentityPool" -Count
  10 -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
3 Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
  -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
4 <!--NeedCopy-->

```

5. 运行 New-ProvScheme 命令以创建目录。例如：

```

1 New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
  -IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
  -CustomProperties '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
  true" />
3 </CustomProperties>'
4 -MasterImageVM "XDHyp:\HostingUnits\ExampleHostingUnit\ExampleVDA.
  vm\ExampleVDA.snapshot" -ProvisioningSchemeName "ExampleCatalog
  " -Scope @() -SecurityGroup @()
5 -MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
  ExampleMachineProfile.vm\ExampleSnapshot.snapshot"
6 <!--NeedCopy-->

```

6. 将预配方案注册为代理目录。例如：

```

1 $ConfigZone = Get-ConfigZone | Where-Object {
2   $_.Name -eq "xxxxxx" }
3
4 New-BrokerCatalog -Name "MPLT1" -AllocationType Random -
  Description "Machine profile catalog" -ProvisioningSchemeId
  fe7df345-244e-4xxxx-xxxxxxxxxx -ProvisioningType Mcs -
  SessionSupport MultiSession -PersistUserChanges Discard -
  ZoneUid ($ConfigZone.Uid)
5 <!--NeedCopy-->

```

7. 将 VM 添加到目录中。

使用新的计算机配置文件更新目录

注意：

- 在此情况下，[Set-ProvScheme](#) 命令不会更改目录中现有 VM 的计算机配置文件。只有添加到目录中的新创建的 VM 才具有新的计算机配置文件。
- 无法将基于计算机配置文件的计算机目录转换为基于非计算机配置文件的计算机目录。

要使用新计算机配置文件更新目录，请执行以下操作：

1. 运行 [Set-ProvScheme](#) 命令。例如：

```
1 Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -  
MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\  
ExampleMachineProfileVm.vm\ExampleMachineProfileSnapshot.  
snapshot"  
2 <!--NeedCopy-->
```

有关 [Set-ProvScheme](#) 命令的详细信息，请参阅 [Set-ProvScheme](#)。

#### 下一步的去向

- 如果这是创建的第一个目录，系统将引导您[创建交付组](#)。
- 要查看整个配置过程，请参阅[规划和构建部署](#)。
- 要管理目录，请参阅[管理计算机目录](#)和[管理 XenServer 目录](#)。

#### 更多信息

- [创建和管理连接和资源](#)
- [与 XenServer 的连接](#)
- [创建计算机目录](#)

#### 创建不同加入类型的目录

July 3, 2023

使用 MCS，您可以将计算机预配为未加入域、已加入本地 AD、已加入 Azure AD 或已加入混合 Azure AD。

有关如何在“完全配置”界面中配置计算机标识的信息，请参阅 [创建计算机目录](#)。

有关如何创建加入目录的计算机身份的具体信息，请参阅以下内容：

- [创建加入了 Azure Active Directory 的目录](#)
- [创建支持 Microsoft Intune 的目录](#)
- [创建已加入混合 Azure Active Directory 的目录](#)
- [创建未加入域的目录](#)

## 创建加入了 **Azure Active Directory** 的目录

February 9, 2024

本文介绍如何使用 Citrix DaaS 创建 Azure Active Directory (AD) 加入的目录。

有关要求、限制和注意事项的信息，请参阅[已加入 Azure Active Directory](#)。

在创建计算机目录之前，需要满足以下条件：

### 1. 新资源位置

- 导航到 Citrix Cloud 管理员 UI > 左上角的汉堡菜单 > **Resource Locations** (资源位置)。
- 单击 **+** 资源位置。
- 输入新资源位置的名称，然后单击保存。

### 2. 创建主机连接。有关详细信息，请参阅[创建和管理连接](#)部分。在 Azure 上部署计算机时，请参阅[连接到 Azure Resource Manager](#)。

### 3. 要持续删除陈旧的 Azure AD 设备并允许新设备加入 Azure AD，可以将云设备管理员角色分配给配置服务主体。如果不删除 Azure 陈旧的 AD 设备，则相应的非持久性 VM 将保持初始化状态，直到您手动将其从 Azure AD 门户中移除。为此，请[使用完整配置接口启用加入了 Azure AD 的设备对主机连接的管理](#)，或者执行以下步骤：

- a) 登录 Azure 门户并导航到 **Azure Active Directory** > 角色和管理员。
- b) 搜索云设备管理员内置角色，然后单击“添加分配”，将该角色分配给托管连接所用应用程序的服务主体。
- c) 使用 Citrix Remote PowerShell SDK 运行以下命令以获取现有 **CustomProperties** 的主机连接。`${ HostingConnectionName }` 是指托管连接的名称。

i. 打开 **PowerShell** 窗口。

ii. 运行 `asnp citrix*` 以加载 Citrix 特定的 **PowerShell** 模块。

iii. 运行以下命令以获取托管连接的现有自定义属性。

```
1 (Get-Item -LiteralPath XDHyp:\Connections${
2   HostingConnectionName }
3   ).CustomProperties
4 <!--NeedCopy-->
```

iv. 将连接中的 CustomProperties 复制到记事本并附加属性设置 `<Property xsi:type="StringProperty" Name="AzureAdDeviceManagement" Value="true" />`。

v. 在 **PowerShell** 窗口中，为修改后的定制属性分配一个变量。例如，`$UpdatedCustomProperties = ' <CustomProperties ...</CustomProperties>'`。

vi. 将自定义属性设置回托管连接：

```
1 Set-Item -LiteralPath XDHyp:\Connections${
2   HostingConnectionName }
3   -CustomProperties ${
4     UpdatedCustomProperties }
5   -ZoneUid ${
6     ZoneUid }
7
8 <!--NeedCopy-->
```

- vii. 运行命令 (`Get-Item -LiteralPath XDHyp:\Connections\${ HostingConnectionName } ).CustomProperties` 以验证更新的自定义属性设置。

您可以使用完整配置界面或 **PowerShell** 创建加入了 Azure AD 的目录。

### 使用“完整配置”界面

以下信息用于补充[创建计算机目录](#)中的指导信息。若要创建加入了 Azure AD 的目录，请遵循该文章中的一般指导，注意特定于加入了 Azure AD 的目录的详细信息。

在目录创建向导中执行以下操作：

1. 在“映像”页面上：
  - 选择 2106 或更高版本作为功能级别。
  - 选择“使用计算机配置文件”，然后从列表中选择相应的计算机。
2. 在“计算机标识”页面上，选择“已加入 **Azure Active Directory**”。创建的计算机归某个组织所有，并使用属于该组织的 Azure AD 帐户登录。它们只存在于云中。

#### 注意：

- 已加入 **Azure Active Directory** 标识类型要求将 2106 或更高版本作为目录的最低功能级别。
- 计算机已加入与主机连接绑定到的租户关联的 Azure AD 域。

3. 必须授予用户在 Azure 中的显式访问权限，才能使用其 AAD 凭据登录计算机。有关更多详细信息，请参阅[已加入 Azure Active Directory](#) 部分。

### 使用 PowerShell

以下是 **PowerShell** 步骤，等效于“完整配置”中的操作。有关如何使用 Remote PowerShell SDK 创建目录的信息，请参阅 <https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>。

本地 AD 加入目录和加入 Azure AD 的目录之间的区别在于身份池的创建和置备方案。

要为加入了 Azure AD 的目录创建身份池，请执行以下操作：

```

1 New-AcctIdentityPool -AllowUnicode -IdentityType="AzureAD" -
  WorkgroupMachine -IdentityPoolName "AzureADJoinedCatalog" -
  NamingScheme "AzureAD-VM-##" -NamingSchemeType "Numeric" -Scope @()
  -ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
2 <!--NeedCopy-->

```

要为加入 Azure AD 的目录创建置备方案，需要在 New-ProvScheme 中使用 **MachineProfile** 参数：

```

1 New-ProvScheme -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='\"
  StringProperty\"' Name='\"StorageType\"' Value='\"StandardSSD_LRS\"' /><
  Property xsi:type='\"StringProperty\"' Name='\"LicenseType\"' Value='\"
  Windows_Server\"' /></CustomProperties>" -HostingUnitName "
  AzureResource" -IdentityPoolName "AzureADJoinedCatalog" -
  InitialBatchSizeHint 1 -MachineProfile "XDHyp:\HostingUnits\
  AzureResource\image.folder\azuread-rg.resourcegroup\MasterVDA.vm" -
  MasterImageVM "XDHyp:\HostingUnits\AzureResource\image.folder\
  azuread-rg.resourcegroup\azuread-
  small_0sDisk_1_5fb42fadf7ff460bb301ee0d56ea30da.manageddisk" -
  NetworkMapping @{
2   "0"="XDHyp:\HostingUnits\AzureResource\virtualprivatecloud.folder\East
    US.region\virtualprivatecloud.folder\azuread-rg.resourcegroup\
    azuread-vnet.virtualprivatecloud\Test_VNET.network" }
3   -ProvisioningSchemeName "AzureADJoinedCatalog" -RunAsynchronously -
    Scope @() -SecurityGroup @() -ServiceOffering "XDHyp:\HostingUnits
    \AzureResource\serviceoffering.folder\Standard_DS1_v2.
    serviceoffering"
4 <!--NeedCopy-->

```

用于创建 Azure AD 联接目录的所有其他命令与用于传统本地 AD 联接目录的命令相同。

### 查看 **Azure AD** 加入过程的状态

在“完整配置”界面中，当交付组中加入了 Azure AD 的计算机处于开机状态时，Azure AD 加入进程的状态将可见。要查看状态，请使用[搜索](#)来标识这些计算机，然后在下部窗格的详细信息选项卡上为每台选中计算机标识。计算机标识中可能显示以下信息：

- 已加入 Azure AD
- 尚未加入 Azure AD

#### 注意：

如果计算机未能处于 Azure AD 加入状态，则它们不会向 Delivery Controller 注册。它们的注册状态显示为初始化。

此外，使用完整配置界面，您可以了解计算机不可用的原因。为此，请单击搜索节点上的计算机，在下部窗格的详细信息选项卡上选中注册，然后阅读工具提示以获取其他信息。

## 交付组

有关详细信息，请参阅 [创建交付组](#) 部分。

## 启用 Rendezvous

创建交付组后，您可以启用 Rendezvous。有关详细信息，请参阅 [Rendezvous V2](#)。

## 故障排除

如果计算机无法加入 Azure AD，请执行以下操作：

- 检查是否为计算机启用了系统分配的托管身份。MCS 配置的计算机必须自动启用此功能。如果没有系统分配托管身份，Azure AD 加入过程将失败。如果未为 MCS 配置的计算机启用系统分配的托管身份，则可能的原因是：
  - 与预配方案关联的身份池的 `IdentityType` 未设置为 `AzureAD`。可以通过运行 `Get-AcctIdentityPool` 来验证这一点。
- 对于使用具有 VDA 版本 2206 或更早版本的主映像的目录，请检查计算机的 **AADLoginForWindows** 扩展程序的配置状态。如果 **AADLoginForWindows** 扩展程序不存在，可能的原因如下：
  - 与预配方案关联的身份池的 `IdentityType` 未设置为 `AzureAD`。可以通过运行 `Get-AcctIdentityPool` 来验证这一点。
  - **AADLoginForWindows** 扩展程序的安装被 Azure 策略阻止。
- 要对 **AADLoginForWindows** 扩展程序配置失败进行故障排除，您可以在 MCS 配置的计算机上查看 `C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.ActiveDirectory.AADLoginForWindows` 下的日志。

### 注意：

使用 VDA 版本 2209 或更高版本的主映像时，MCS 不依赖 `AADLoginForWindows` 扩展将虚拟机加入 Azure AD。在这种情况下，`AADLoginForWindows` 扩展程序不会安装在 MCS 预配的计算机上。因此，无法收集 `AADLoginForWindows` 扩展程序预配日志。

- 通过在 MCS 配置的计算机上运行 `dsregcmd /status` 命令来检查 Azure AD 加入状态和调试日志。
- 在“应用程序和服务日志” > “**Microsoft**” > “**Windows**” > “用户设备注册”下查看 Windows 事件日志。
- 运行 `Get-Item -LiteralPath XDHyp:\Connections\${ HostingConnectionName }` 时检查 Azure AD 设备管理配置是否正确。

确保以下各项的值：

- `CustomProperties` 中的属性 `AzureAdDeviceManagement` 为 **true**

- 元数据中的 `Citrix_MCS_AzureAdDeviceManagement_PermissionGranted` 属性为 **true**

如果 `Citrix_MCS_AzureAdDeviceManagement_PermissionGranted` 为 **false**，则表示托管连接所使用的应用程序的 `ServicePrincipal` 没有获得足够的权限来执行 Azure AD 设备管理。要解决此问题，请为 `ServicePrincipal` 分配云设备管理员角色。

## Azure Active Directory 动态安全组

动态组规则根据计算机目录的命名方案将目录中的 VM 置于动态安全组中。

如果计算机目录的命名方案是 Test###（其中，# 表示数字），Citrix 会在动态安全组中创建动态成员资格规则 `^Test[0-9]{3}$`。现在，如果 Citrix 创建的 VM 的名称介于 Test001 到 Test999 之间，则该虚拟机将包含在动态安全组中。

### 注意：

如果您手动创建的虚拟机的名称介于 Test001 到 Test999 之间，则该虚拟机也包含在动态安全组中。这是动态安全组的局限性之一。

当您想通过 Azure Active Directory (Azure AD) 管理 VM 时，动态安全组功能很有用。当您想要应用条件访问策略或者通过使用 Azure AD 动态安全组筛选 VM 来分发来自 Intune 的应用程序时，这也非常有用。

您可以使用 **PowerShell** 命令来：

- 使用 Azure AD 动态安全组创建计算机目录
- 为 Azure AD 目录启用安全组功能
- 删除已加入 Azure AD 的设备安全组的计算机目录

### 重要提示：

- 要使用 Azure AD 动态安全组创建计算机目录、将计算机添加到目录并删除计算机目录，必须拥有 Azure AD 访问令牌。有关获取 Azure AD 访问令牌的信息，请参阅 <https://docs.microsoft.com/en-us/graph/graph-explorer/graph-explorer-features#consent-to-permissions/>。
- 要在 Azure AD 中申请访问令牌，Citrix 请求 Microsoft Graph API 的 **Group.ReadWrite.All** 权限。拥有租户范围管理员同意权限的 Azure AD 用户可以授予 Microsoft Graph API 的 **Group.ReadWrite.All** 权限。有关如何向 Azure Active Directory (Azure AD) 中的应用程序授予租户范围的管理员同意的信息，请参阅 Microsoft 文档 <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent/>。

## 使用 Azure AD 动态安全组创建计算机目录

1. 在基于 Web 的控制台的计算机目录设置用户界面中，在“计算机身份”页面上，选择已加入 **Azure Active Directory**。



2. 登录 Azure AD。
3. 获取 MS Graph API 的访问令牌。运行 **PowerShell** 命令时,使用此访问令牌作为 `$AzureADAccessToken` 参数 de 值。
4. 运行以下命令以验证租户中是否存在动态安全组名称。

```
1 Get-AcctAzureADSecurityGroup
2 - AccessToken $AzureADAccessToken
3 - Name "SecurityGroupName"
4 <!--NeedCopy-->
```

5. 使用租户 ID、访问令牌和动态安全组创建计算机目录。运行以下命令使用创建带 `IdentityType=AzureAD` 的 `IdentityPool`,然后在 Azure 中创建动态安全组。

```
1 New-AcctIdentityPool
2 -AllowUnicode
3 -IdentityPoolName "SecurityGroupCatalog"
4 -NamingScheme "SG-VM-###"
5 -NamingSchemeType "Numeric" -Scope @()
6 -ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
7 -WorkgroupMachine
8 -IdentityType "AzureAD"
9 -DeviceManagementType "None"
10 -AzureADTenantId 620387bb-9167-4bdd-8435-e3dccc58369e
11 -AzureADSecurityGroupName "SecurityGroupName"
12 -AzureADAccessToken $AzureADAccessToken
13 <!--NeedCopy-->
```

## 为 **Azure AD** 目录启用安全组功能

您可以为在未启用动态安全组功能的情况下创建的 Azure AD 目录启用动态安全功能。为此,您需要:

1. 手动创建新的动态安全组。您也可以重用现有的动态安全组。
2. 登录 Azure AD,获取 MS Graph API 的访问令牌。运行 **PowerShell** 命令时,使用此访问令牌作为 `$AzureADAccessToken` 参数 de 值。

注意:

有关 Azure AD 用户所需权限的信息,请参阅 <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent#prerequisites/>。

3. 运行以下命令将身份池连接到创建的 Azure AD 动态安全组。

```
1 Set-AcctIdentityPool
2 -IdentityPoolName "SecurityGroupCatalog"
3 -AzureADTenantId 620387bb-9167-4bdd-8435-e3dccc58369e
4 -AzureADSecurityGroupNam "ExistingSecurityGroupName"
5 -AzureADAccessToken $AzureADAccessToken
6 <!--NeedCopy-->
```

如果您更新命名方案，Citrix 会将命名方案更新为新的成员资格规则。如果您删除目录，则会删除成员资格规则，而不是安全组。

删除已加入 **Azure AD** 的设备安全组的计算机目录

删除计算机目录时，已加入 Azure AD 的设备安全组也会被删除。

要删除 Azure AD 动态安全组，请执行以下操作：

1. 登录 Azure AD。
2. 获取 MS Graph API 的访问令牌。运行 **PowerShell** 命令时，使用此访问令牌作为 `$AzureADAccessToken` 参数的值。
3. 请运行以下命令：

```
1 Remove-AcctIdentityPool
2 -IdentityPoolName "SecurityGroupCatalog"
3 -AzureADAccessToken $AzureADAccessToken
4 <!--NeedCopy-->
```

在现有 **Azure AD** 分配的安全组下创建 **Azure AD** 动态安全组

您可以在现有 Azure AD 分配的安全组下创建 Azure AD 动态安全组。可执行以下操作：

- 获取安全组信息。
- 获取从本地 AD 服务器同步的所有 Azure AD 分配的安全组或可分配 Azure AD 角色的已分配安全组。
- 获取所有 Azure AD 动态安全组。
- 将 Azure AD 动态安全组添加为已分配 Azure AD 的组的成员。
- 删除 Azure AD 动态安全组和计算机目录时，删除 Azure AD 动态安全组与 Azure AD 分配的安全组之间的成员资格。

当任何操作失败时，您还可以看到明确的错误消息。

要求：

运行 **PowerShell** 命令时，您必须拥有 MS Graph API 的访问令牌。

要获取访问令牌，请执行以下操作：

1. 打开 [Microsoft Graph 资源管理器](#) 并登录 Azure AD。
2. 确保您同意 **Group.ReadWrite.All** 和 **GroupMember.ReadWrite.All** 权限。
3. 从 Microsoft Graph 资源管理器获取访问令牌。在运行 **PowerShell** 命令时使用此访问令牌。

要按组 ID 获取安全组信息，请执行以下操作：

1. 获取访问令牌。

2. 从 Azure 门户中查找组对象 ID。
3. 在 **PowerShell** 控制台中运行以下 **PowerShell** 命令：

```
1 Get-AcctAzureADSecurityGroup
2 -AccessToken <token> -GroupId <GroupUId>
3 <!--NeedCopy-->
```

要按组显示名称获取安全组，请执行以下操作：

1. 获取访问令牌。
2. 在 **PowerShell** 控制台中运行以下 **PowerShell** 命令：

```
1 Get-AcctAzureADSecurityGroup
2 -AccessToken <token>
3 -Name <TargetGroupDisplayName>
4 <!--NeedCopy-->
```

要获取显示名称包含子字符串的安全组，请执行以下操作：

1. 获取访问令牌。
2. 在 **PowerShell** 控制台中运行以下 **PowerShell** 命令：

```
1 Get-AcctAzureADSecurityGroup
2 -AccessToken <token>
3 -SearchString <displayNameSubString>
4 <!--NeedCopy-->
```

要获取从本地 AD 服务器同步的所有 Azure AD 分配的安全组或可分配 Azure AD 角色的已分配安全组，请执行以下操作：

1. 获取访问令牌。
2. 在 **PowerShell** 控制台中运行以下 **PowerShell** 命令：

```
1 Get-AcctAzureADSecurityGroup
2 -AccessToken <token>
3 -Assigned true
4 <!--NeedCopy-->
```

要获取所有 Azure AD 动态安全组，请执行以下操作：

1. 获取访问令牌。
2. 在 **PowerShell** 控制台中运行以下 **PowerShell** 命令：

```
1 Get-AcctAzureADSecurityGroup
2 -AccessToken <token>
3 -Dynamic true
4 <!--NeedCopy-->
```

要获得具有最大记录数的 Azure AD 分配的安全组，请执行以下操作：

1. 获取访问令牌。
2. 在 **PowerShell** 控制台中运行以下 **PowerShell** 命令：

```
1 Get-AcctAzureADSecurityGroup
2 -AccessToken <token>
3 -Assigned true
4 -MaxRecordCount 10
5 <!--NeedCopy-->
```

要将 Azure AD 动态安全组添加为 Azure AD 分配的安全组的成员，请执行以下操作：

1. 获取访问令牌。
2. 在 **PowerShell** 控制台中运行以下 **PowerShell** 命令：

```
1 Add-AcctAzureADSecurityGroupMember
2 -AccessToken <token>
3 -GroupId <ASG-Id>
4 -RefGroupId <DSG-Id>
5 <!--NeedCopy-->
```

要获得 Azure AD 分配的安全组成员，请执行以下操作：

1. 获取访问令牌。
2. 在 **PowerShell** 控制台中运行以下 **PowerShell** 命令：

```
1 Get-AcctAzureADSecurityGroupMember
2 -AccessToken <token>
3 -GroupId <ASG-Id>
4 <!--NeedCopy-->
```

注意：

`Get-AcctAzureADSecurityGroupMember` 在 Azure AD 分配的安全组下，仅为您提供安全组类型的直接成员。

要在删除 Azure AD 动态安全组和计算机目录时删除 Azure AD 动态安全组与 Azure AD 分配的安全组之间的成员资格，请执行以下操作：

1. 获取访问令牌。
2. 在 **PowerShell** 控制台中运行以下 **PowerShell** 命令：

```
1 Remove-AcctIdentityPool
2 -IdentityPoolName "SecurityGroupCatalog"
3 -AzureADAccessToken $AzureADAccessToken
4 <!--NeedCopy-->
```

## 修改 **Azure AD** 动态安全组名称

可以修改与计算机目录关联的 Azure AD 动态安全组名称。此修改使存储在 Azure AD 身份池对象中的安全组信息与 Azure 门户中存储的信息保持一致。

注意：

Azure AD 动态安全组不包括从本地 AD 和 Office 365 组等其他组类型同步的安全组。

您可以使用完整配置界面和 **PowerShell** 命令修改 Azure AD 动态安全组名称。

要使用 **PowerShell** 修改 Azure AD 动态安全组名称，请执行以下操作：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 **PowerShell** 模块。
3. 运行命令 `Set-AcctIdentityPool -AzureAdSecurityGroupName [DSG-Name]`。

如果无法修改 Azure AD 动态安全组名称，则会收到相应的错误消息。

## 创建支持 **Microsoft Intune** 的目录

January 23, 2024

本文介绍如何使用 Citrix DaaS 创建启用 Microsoft Intune 的目录。您可以使用完整配置界面或 PowerShell 来启用 Microsoft Intune。

有关要求、限制和注意事项的信息，请参阅 [Microsoft Intune](#)。

### 使用“完整配置”界面

以下信息用于补充[创建计算机目录](#)中的指导信息。此功能要求在目录创建期间在计算机标识中选择已加入 **Azure Active Directory**。请遵循该文章中的一般指导，注意此功能的特定细节。

在目录创建向导中执行以下操作：

- 在“计算机身份”页面上，选择“已加入 **Azure Active Directory**”，然后选择“在 **Microsoft Intune** 中注册计算机”如果启用，请在 Microsoft Intune 中注册计算机以进行管理。

### 使用 **PowerShell**

以下是 PowerShell 步骤，等效于“完整配置”中的操作。

要使用远程 PowerShell SDK 在 Microsoft Intune 中注册计算机，请使用 `New-AcctIdentityPool` 中的 `DeviceManagementType` 参数。此功能要求目录已加入 Azure AD，并且 Azure AD 拥有正确的 Microsoft Intune 许可证。例如：

```
1 New-AcctIdentityPool -AllowUnicode -DeviceManagementType "Intune"  
   IdentityType="AzureAD" -WorkgroupMachine -IdentityPoolName "  
   AzureADJoinedCatalog" -NamingScheme "AzureAD-VM-##" -  
   NamingSchemeType "Numeric" -Scope @() -ZoneUid "81291221-d2f2-49d2-  
   ab12-bae5bbd0df05"  
2 <!--NeedCopy-->
```

## 故障排除

如果计算机无法在 Microsoft Intune 中注册，请执行以下操作：

- 检查 MCS 配置的计算机是否已加入 Azure AD。如果计算机未加入 Azure AD，则无法在 Microsoft Intune 中注册。有关 Azure AD 加入问题的故障排除，请参阅 <https://docs.citrix.com/en-us/citrix-daas/install-configure/create-machine-identities-joined-catalogs/create-azure-ad-joined-catalogs.html>。
- 检查是否为您的 Azure AD 租户分配了相应的 Intune 许可证。有关 Microsoft Intune 的许可要求，请参阅 <https://learn.microsoft.com/en-us/mem/intune/fundamentals/licenses>。
- 对于使用具有 VDA 版本 2206 或更早版本的主映像的目录，请检查计算机的 **AADLoginForWindows** 扩展程序的配置状态。如果 **AADLoginForWindows** 扩展程序不存在，可能的原因如下：
  - 与配置方案关联的身份池的 `IdentityType` 未设置为 `AzureAD`，或者 `DeviceManagementType` 未设置为 `Intune`。可以通过运行 `Get-AcctIdentityPool` 来验证这一点。
  - **AADLoginForWindows** 扩展程序的安装被 Azure 策略阻止。
- 要对 **AADLoginForWindows** 扩展程序配置失败进行故障排除，您可以在 MCS 已配置的计算机上查看 `C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.ActiveDirectory.AADLoginForWindows` 下的日志。

### 注意：

使用 VDA 版本 2209 或更高版本的主映像时，MCS 不依赖 **AADLoginForWindows** 扩展程序将 VM 加入 Azure AD 并注册到 Microsoft Intune。在这种情况下，**AADLoginForWindows** 扩展程序不会安装在 MCS 预配的计算机上。因此，无法收集 **AADLoginForWindows** 扩展程序预配日志。

- 在“应用程序和服务日志” > “**Microsoft**” > “**Windows**” > “**DeviceManagement-Enterprise-Diagnostics-Provider**” 下查看 Windows 事件日志。

## 创建加入了混合 **Azure Active Directory** 的目录

December 6, 2023

本文介绍如何使用 Citrix DaaS 创建已加入混合 Azure Active Directory (AD) 的目录。

您可以使用完整配置界面或 PowerShell 创建加入了 Azure AD 的目录。

有关要求、限制和注意事项的信息，请参阅[已加入混合 Azure Active Directory](#)。

### 使用“完整配置”界面

以下信息用于补充[创建计算机目录](#)中的指导信息。要创建加入了混合 Azure AD 的目录，请遵循该文章中的常规指南，注意加入了混合 Azure AD 的目录特定的详细信息。

在目录创建向导中执行以下操作：

- 在计算机标识页面上，选择加入了混合 **Azure Active Directory**。创建的计算机归某个组织所有，并使用属于该组织的 Active Directory 域服务帐户登录。它们存在于云端和本地。

#### 注意：

如果您选择加入了混合 **Azure Active Directory** 作为标识类型，则目录中的每台计算机都必须具有相应的 AD 计算机帐户。

### 使用 **PowerShell**

以下是 PowerShell 步骤，等效于“完整配置”中的操作。有关如何使用远程 PowerShell SDK 创建目录的信息，请参阅<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>。

本地加入了 AD 的目录与加入了混合 Azure AD 的目录之间的区别在于标识池和计算机帐户的创建。

要创建标识池以及加入了混合 Azure AD 的目录的帐户，请执行以下操作：

```
1 New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -
   Domain "corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -
   NamingScheme "HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU "CN=
   AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-d2f2-49
   d2-ab12-bae5bbd0df05"
2 New-AcctADAccount -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
   -ADUserName "corp\admin1" -ADPassword $password
3 Set-AcctADAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -
   All -ADUserName "corp\admin1" -ADPassword $password
4 <!--NeedCopy-->
```

注意：

`$password` 是具有写入权限的 AD 用户帐户的匹配密码。

用于创建加入了混合 Azure AD 的目录的所有其他命令与加入了传统本地 AD 的目录的命令相同。

### 查看混合 Azure AD 加入进程的状态

在“完整配置”界面中，在交付组中已加入混合 Azure AD 的计算机处于开机状态时，已加入混合 Azure AD 的进程的状态将可见。要查看状态，请使用[搜索](#)来标识这些计算机，然后在下部窗格的详细信息选项卡上为每台选中计算机标识。以下信息可能出现在计算机标识中：

- 已加入混合 Azure AD
- 尚未加入 Azure AD

注意：

- 当计算机最初开机时，您可能会遇到混合 Azure AD 加入延迟的情况。这是由默认的计算机标识同步时间间隔（Azure AD Connect 为 30 分钟）引起的。只有在通过 Azure AD Connect 将计算机标识同步到 Azure AD 之后，计算机才处于加入了混合 Azure AD 状态。
- 如果计算机无法进入已加入混合 Azure AD 状态，则不会在 Delivery Controller 中注册。其注册状态显示为初始化。

此外，使用完整配置界面，您可以了解计算机不可用的原因。为此，请单击搜索节点上的计算机，在下部窗格的详细信息选项卡上选中注册，然后阅读工具提示以获取其他信息。

### 故障排除

如果计算机无法加入混合 Azure AD，请执行以下操作：

- 检查计算机帐户是否已通过 Microsoft Azure AD 门户同步到 Azure AD。如果已同步，则会出现尚未加入 **Azure AD**，表示待注册状态。

要将计算机帐户同步到 Azure AD，请确保：

- 计算机帐户位于配置为与 Azure AD 同步的 OU 中。没有 **userCertificate** 属性的计算机帐户不会同步到 Azure AD，即使它们位于配置为同步的 OU 中亦如此。
- **userCertificate** 属性填充到计算机帐户中。使用 Active Directory Explorer 查看该属性。
- 创建计算机帐户后，Azure AD Connect 必须至少同步过一次。如果未同步，请在 Azure AD Connect 计算机的 PowerShell 控制台中手动运行 `Start-ADSyncSyncCycle -PolicyType Delta` 命令以触发即时同步。



- 通过查询 **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix** 下 **DeviceKey-PairRestored** 的值，检查混合 Azure AD 加入的 Citrix 托管设备密钥对是否已正确推送到计算机。

验证该值是否为 1。如果不是，可能的原因如下：

- 与预配方案关联的标识池的 **IdentityType** 未设置为 **HybridAzureAD**。可以通过运行 **Get-AcctIdentityPool** 来验证这一点。
  - 未使用与计算机目录相同的预配方案预配计算机。
  - 计算机未加入本地域。加入的本地域是混合 Azure AD 加入的必备条件。
- 通过在 MCS 预配的计算机上运行 **dsregcmd /status /debug** 命令来检查诊断消息。
    - 如果混合 Azure AD 加入成功，**AzureAdJoined** 和 **DomainJoined** 在命令行输出中为 **YES**。
    - 如果不成功，请参阅 Microsoft 文档来解决以下问题：<https://docs.microsoft.com/en-us/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current>。
    - 如果您收到错误消息“服务器消息：在设备上找不到用户证书，ID 为：xxxxxxxxxxxx-xxxxxxxxxxxxxxxxxxxxxxxx”，则运行以下 PowerShell 命令来修复用户证书：

```
1 Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
   UserCertificate
2 <!--NeedCopy-->
```

有关用户证书问题的更多信息，请参阅 [CTX566696](#)。

## 创建未加入域的目录

November 3, 2022

本文介绍如何使用 Citrix DaaS 创建未加入域的目录。

有关要求、限制和注意事项的信息，请参阅[未加入域](#)。

在创建计算机目录之前，需要满足以下条件：

### 1. 新资源位置

- 导航到 Citrix Cloud 管理员 UI > 左上角的汉堡菜单 > **Resource Locations**（资源位置）。
- 单击 **+** 资源位置。
- 输入新资源位置的名称，然后单击保存。

### 2. 创建主机连接。有关详细信息，请参阅[创建和管理连接](#)部分。

使用 Citrix DaaS，您可以基于工作组或未加入域的计算机创建目录。创建未加入域的计算机取决于帐户身份池的创建方式。帐户身份池是 MCS 用于在目录预配期间创建和跟踪计算机名称的机制。

您可以使用完整配置界面或 PowerShell 创建未加入域的目录。

## 使用“完整配置”界面

以下信息用于补充[创建计算机目录](#)中的指导信息。要创建未加入域的目录，请遵循该文章中的一般指导，注意特定于未加入域的目录的详细信息。

在目录创建向导中执行以下操作：

- 在“计算机标识”页面上，选择“未加入域”。创建的计算机未加入任何域。

### 注意：

未加入域的标识类型需要 1811 或更高版本的 VDA 作为该目录的最低功能级别。要使其可用，请在必要时更新最低功能级别。

## 使用 PowerShell

以下是相当于完全配置中的操作的 PowerShell 步骤。

您可以使用远程 PowerShell SDK 为未加入域的目录创建身份池。

例如，在以前的版本中，所有 Active Directory 字段都是在一个实例中提供的：

```
1 New-AcctIdentityPool -AllowUnicode -Domain "corp.local" -  
   IdentityPoolName "NonDomainJoinedCatalog" -NamingScheme "NDJ-VM-###"  
   -NamingSchemeType "Numeric" -OU "CN=Computers,DC=corp,DC=local" -  
   Scope @() -ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"  
2 <!--NeedCopy-->
```

MCS 现在使用新的 PowerShell 参数 **WorkgroupMachine** 和 **IdentityType** 为未加入域的目录创建身份池。使用与上面相同的示例，这些参数无需指定所有特定于 AD 的参数，包括域管理员凭据：

```
1 New-AcctIdentityPool -AllowUnicode -IdentityType "Workgroup" -  
   WorkgroupMachine -IdentityPoolName "NonDomainJoinedCatalog" -  
   NamingScheme "NDJ-VM-###" -NamingSchemeType "Numeric" -Scope @() -  
   ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"  
2 <!--NeedCopy-->
```

用于创建未加入域的目录的所有其他命令与传统的内部部署 Active Directory 加入目录的命令相同。

## 管理计算机目录

March 31, 2024

### 注意：

本文介绍如何使用完整配置界面和 PowerShell 命令管理目录。如果您使用“快速部署”界面创建了目录，并继

续使用该界面管理目录，然后按照[在快速部署中管理目录](#)进行操作。

## 简介

可以在计算机目录中添加或删除计算机，以及重命名、更改说明或管理目录的 Active Directory 计算机帐户。

目录维护还可以包括的任务包括确保每台计算机都安装最新的操作系统更新、防病毒软件更新、操作系统升级或配置更改。

- 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映像，然后更新计算机来维护计算机。此方法可让您有效地更新大量用户计算机。
- 对于包含永久分配的静态计算机的目录，您可以管理这些目录当前使用的映像或模板，但只能使用新映像或模板创建以后添加到目录中的计算机。
- 对于 Remote PC Access 目录，您可以在“完整配置”管理界面之外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的方式执行此操作。

有关创建和管理与主机虚拟机管理程序和云服务的连接的信息，请参阅[创建和管理连接和资源](#)。

### 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

更新包含永久性计算机的 MCS 目录的主映像时，添加到该目录的任何新计算机都将使用更新后的映像。现有计算机继续使用原始主映像。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。
- 对于非永久性磁盘目录，只有在 Studio 或 PowerShell 中重新启动计算机时，下次才会更新计算机映像。如果从 Studio 外部的虚拟机管理程序重新启动计算机，则不会重置磁盘。
- 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。

## 管理计算机目录

可以通过两种方式管理计算机目录：

- 使用完整配置界面
- 使用 PowerShell

使用完整配置界面

本节详细介绍了如何使用完整配置界面管理目录：

- 查看目录详细信息
- [向目录中添加计算机](#)
- [从目录中删除计算机](#)
- [编辑目录](#)
- [重命名目录](#)
- [删除目录](#)
- [管理目录中的 Active Directory 计算机帐户](#)
- [更改目录的主映像](#)
- [更改功能级别或撤消更改](#)
- [克隆目录](#)
- [使用文件夹整理目录](#)
- [为 VDA 配置自动升级](#)
- [管理目录的配置集](#)
- [重试创建目录](#)
- (仅限非 Citrix 预置的 VDA) 生成和管理注册令牌

查看目录详细信息

1. 使用搜索功能查找特定的计算机目录。有关说明，请参阅[搜索实例](#)。
2. 根据需要从搜索结果中选择一个目录。
3. 有关目录列的描述，请参阅下表。
4. 单击底部详细信息窗格中的选项卡，了解有关此目录的更多信息。

列	说明
计算机目录	<p>目录的名称和分配类型。分配类型包括：</p> <ul style="list-style-type: none"><li>• 随机：目录中的计算机随机分配给用户。</li><li>• 永久：目录中的计算机永久分配给用户。</li></ul>
计算机类型	<p>目录中计算机支持的会话类型。可能的值包括：</p> <ul style="list-style-type: none"><li>• 操作系统类型：多会话操作系统（虚拟）；用户数据：丢弃。</li><li>• 操作系统类型：多会话操作系统（虚拟）；用户数据：在本地磁盘上</li><li>• 操作系统类型：单会话操作系统 (Remote PC Access)</li></ul>

列	说明
	<ul style="list-style-type: none"><li>操作系统类型：单会话操作系统（虚拟）；用户数据：丢弃</li><li>操作系统类型：单会话操作系统（虚拟）；用户数据：在本地磁盘上</li></ul>
计算机数量	目录中的计算机数量和配置方法。可能的配置方法包括：Machine Creation Services（MCS 计算机）、手动和 Citrix Provisioning 服务。
分配的数量	目录中分配给交付组的计算机数量。
文件夹	目录在计算机目录树中的位置。它显示目录所在文件夹的名称（包括尾部的反斜杠），或者 -（如果目录位于根级别）。
VDA 升级	VDA 升级状态。可能的值包括：未配置、已计划、可用和最新。
映像状态	目录的映像更新状态。仅适用于非永久性计算机目录。可能的值包括：完全更新、部分更新、待更新、准备中

向目录中添加计算机

开始之前：

- 确保虚拟化主机（虚拟机管理程序或云服务提供程序）具有足够多的处理器、内存和存储空间来容纳更多的计算机。
- 确保有足够多的未使用 Active Directory 计算机帐户。如果要使用现有帐户，可以添加的计算机数受可用帐户数限制。
- 如果使用“完整配置”管理界面为更多计算机创建 Active Directory 计算机帐户，必须具有相应的域管理员权限。

提示：

如果用于将计算机添加到计算机目录的 Citrix DaaS 帐户的 AD 权限受限，请在登录到…中添加您打算使用的所有 Cloud Connector 屏幕。

向目录中添加计算机：

1. 在管理 > 完整配置中，选择左窗格中的计算机目录。
2. 选择计算机目录，然后在操作栏中选择添加计算机。
3. 在虚拟机页面上，选择要添加的虚拟机数量。
4. 在“计算机身份”页面上，按如下方式配置设置：

- 从列表中选择标识。
- 如果适用，请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（域）。

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。

如果您使用现有 Active Directory 帐户，请浏览到这些帐户或选择“导入”并指定一个包含帐户名的 .csv 文件。确保所有要添加的计算机都有足够的帐户。“完整配置”界面管理这些帐户。允许界面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。

- 如果其他目录使用此身份池，则无法使用完整配置将其更改为其他池。改用 **Set-ProvScheme** PowerShell cmdlet。有关详细信息，请参阅 [Citrix Virtual Apps and Desktops SDK 文档](#)。
- 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。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。
- 或者，您可以指定帐户名称的开头。

指定帐户名称的开头时，请注意以下情况：如果起始数字或字母已被使用，则创建的第一个帐户将使用最近的未使用数字或字母命名。

请参阅管理计算机名称的序列号，通过 PowerShell 命令自定义使用 MCS 部署的计算机的序列号。

5. 在域凭据页面上，选择输入凭据，然后输入具有足够权限的用户凭据以创建计算机帐户。

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“完整配置”管理界面，计算机创建也会继续进行。

#### 使用 CSV 文件将计算机批量添加到目录

可以使用 CSV 文件批量添加计算机。该功能适用于所有目录，但通过 MCS 置备的目录除外。

要将计算机批量添加到目录中，请完成以下步骤：

1. 在管理 > 完整配置中，选择左窗格中的计算机目录。
2. 选择计算机目录，然后在操作栏中选择添加计算机。此时将显示添加计算机窗口。
3. 选择添加 CSV 文件。此时将显示批量添加计算机窗口。
4. 选择下载 CSV 模板。
5. 填写模板文件。
6. 拖动或浏览到该文件进行上载。
7. 选择验证可对导入执行验证检查。
8. 选择导入以完成该过程。

#### 使用 CSV 文件添加计算机时的注意事项

## 注意：

- 对于非 Active Directory 用户，必须按以下格式键入其名称：<identity provider>:<user name>。示例：AzureAD:username。
- VM 名称区分大小写。输入 VM 路径时，请确保正确输入了 VM 名称。

编辑 CSV 模板文件时，请谨记以下几点：

- 通过该功能，您可以更加灵活地通过 CSV 文件批量添加计算机。在该文件中，您可以仅添加计算机（用于用户自动分配）或将计算机与用户分配一起添加。请按以下格式键入数据：

- 对于计算机帐户和用户名 (samName) 对：

- \* Domain\ComputerName1, Domain\Username1
- \* Domain\ComputerName2, Domain\Username1;Domain\Username2
- \* Domain\ComputerName3, AzureAD:username

- 仅适用于计算机帐户：

- \* Domain\ComputerName1
- \* Domain\ComputerName2

- 对于 VM 和用户名对：

- \* XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName1.vm,Domain\ComputerName1
- \* XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName2.vm,Domain\ComputerName2

- 仅适用于 VM：

- \* XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName1.vm,Domain\ComputerName1
- \* XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName2.vm,Domain\ComputerName2

例如：

XDHyp:\Connections\xpace-scale\East US.region\vm.folder\wsvdaV3-2.vm

其中，

- \* **xpace-scale** 是 ConnectionName：您在 完整配置 > 托管 > 添加连接和资源中输入的连接的名称。有关详细信息，请参阅 [创建连接和资源](#)。
- \* **East US.region** 是 RegionName：扩展名为 **.region** 的区域的名称。
- \* **wsvdaV3-2.vm** 是 VMName：扩展名为 **.vm** 的虚拟机的名称。

- 文件可以包含的最大计算机数为 1000。要导入 1000 多台计算机，请将其分布在不同的文件中，然后逐个导入这些文件。我们建议您导入的计算机数不超过 1000。否则，目录创建可能需要很长时间才能完成。

您也可以在同一“添加计算机”页面上从目录中导出计算机。然后，在批量添加计算机时，可以将计算机的导出 CSV 用作模板。要导出计算机，请执行以下操作：

1. 在管理 > 完整配置中，选择左窗格中的计算机目录。
2. 选择计算机目录，然后在操作栏中选择添加计算机。此时将显示添加计算机窗口。
3. 选择 导出到 **CSV** 文件。将下载包含计算机列表的 CSV 文件。
4. 打开 CSV 文件以根据需要添加或编辑计算机。要使用保存的 CSV 文件批量添加计算机，请参阅上一节 使用 CSV 文件将计算机批量添加到目录。

注意：

- 此功能不适用于 Remote PC Access 和 MCS 配置的目录。
- 仅支持在相同类型的目录之间导出和导入 CSV 文件中的计算机。

## 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。
- 计算机已关闭电源。

从目录中删除计算机：

1. 在管理 > 完整配置中，选择左窗格中的计算机目录。
2. 选择一个目录，然后在操作栏中选择查看计算机。
3. 选择一个或多个计算机，然后在操作栏中选择删除。
4. 如果您要从目录中删除永久计算机，请选择是将其从虚拟机管理程序还是云服务中删除。如果您选择删除它们，请注明是保留、禁用还是删除他们的 Active Directory 帐户。

从 Azure Resource Manager 目录中删除永久计算机时，即使您选择保留这些计算机和关联资源组，也会从 Azure 中删除它们。

当您从目录中删除非永久性计算机时，它们会自动从虚拟机管理程序或云服务中删除。

## 编辑目录

1. 在管理 > 完整配置中，选择左窗格中的计算机目录。
2. 选择一个目录，然后在操作栏中选择编辑计算机目录。
3. 在作用域页面上，更改作用域。
4. 在 **NIC** 页面上，执行以下操作：
  - 要更改 NIC 的子网映射，请从“关联网”字段中选择一个网络。
  - 要添加子网映射，请选择添加 **NIC**，从“关联网”字段中选择一个网络，然后选择“保存”。



只有那些存在于与目录关联的主机中的子网才会出现在“关联网”字段中。

在没有计算机配置文件的情况下，只能将 NIC 添加到 Azure 计算机目录中。

注意：

- 对于 AWS 计算机目录，您不能将同一个子网映射到多个 NIC。
- 对于带有计算机配置文件的计算机目录，目录上的 NIC 数量必须等于计算机配置文件上的 NIC 数量。
- IBM Cloud 虚拟机管理程序不支持此功能。
- 只有 Nutanix 虚拟机管理程序的 Nutanix Prism Element 支持此功能。

5. 在 **VDA** 升级页面上，更改或选择要升级到的 VDA 版本。有关详细信息，请参阅 [VDA 升级](#)。

6. 您可能会看到其他页面，具体取决于目录类型。

对于使用 Azure Resource Manager 映像创建的目录，以下页面可见。请记住，您所做的更改仅适用于稍后添加到目录的计算机。现有计算机保持不变。

- 在虚拟机页面上，更改要在其中创建计算机的计算机大小和可用性区域。

注意：

- 仅显示目录支持的计算机大小。
- 如有必要，请选择仅显示在其他计算机目录中使用的计算机规模以筛选计算机大小列表。

- 在计算机配置文件页面上，选择是使用计算机配置文件还是更改计算机配置文件。
- （仅当目录配置了专用组主机时）在 专用主机组 页面上，选择是否更改主机组。
- 在“存储和许可类型”页面上，选择是否更改存储类型、许可类型和 Azure 电脑库设置（仅在使用“将准备好的图像放入 **Azure** 图库”时可用）。

注意：

如果新选择的设置不支持当前的计算机大小，则会出现一个警告对话框，通知您更改该设置将重置计算机大小设置。如果您选择继续，虚拟机 菜单旁边会出现一个红点，提示您选择新的计算机大小。

有关页面上可用的设置的详细信息，请参阅[使用 Azure Resource Manager 映像创建计算机目录](#)。

对于 Remote PC Access 目录，以下页面可见：

- 在电源管理页面上，更改电源管理设置以及选择电源管理连接。
- 在组织单位页面上，添加或删除 Active Directory OU。

7. 在说明页面上，更改目录说明。

8. 单击“应用”以应用所做的更改，然后单击“保存”退出。

## 重命名目录

1. 在管理 > 完整配置中，选择左窗格中的计算机目录。
2. 选择一个目录，然后在操作栏中选择重命名计算机目录。
3. 输入新名称。

## 删除目录

删除编录之前，请确保：

- 所有用户均已注销，没有正在运行已断开连接的会话。
- 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。
- 该目录未与交付组关联。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. 在管理 > 完整配置中，选择左窗格中的计算机目录。
2. 选择一个目录，然后在操作栏中选择删除计算机目录。
3. 如果目录包含永久计算机，请指明是从虚拟机管理程序还是云服务中删除这些计算机。如果您选择这样做，请选择是保留、禁用还是删除他们的 Active Directory 计算机帐户。
4. 如有必要，请选择“隐藏进度”以在后台运行删除。

注意：

- 删除 Azure Resource Manager 目录时，关联的计算机和资源组将从 Azure 中删除，即使您选择保留它们也是如此。
- 当您删除包含非永久计算机的目录时，这些计算机将从虚拟机管理程序或云服务中删除。
- 如果在删除目录期间无法访问虚拟机管理程序或云服务，则目录和虚拟机删除都会失败。如果需要，您可以选择仅从 Citrix 站点数据库中删除 VM 记录。为此，请在“计算机目录”节点中选择 计算机目录，然后执行“故障排除”选项卡上显示的删除操作。请记住，此操作会使主机上的虚拟机保持不变。

## 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：

- 从单会话和多会话目录中删除 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. 在管理 > 完整配置中，选择左窗格中的计算机目录。

2. 选择一个目录，然后在操作栏中选择管理 **AD** 帐户。
3. 选择是添加还是删除计算机帐户。如果添加帐户，请指定帐户密码的处理方式：重置所有密码还是输入一个适用于所有帐户的密码。

如果不知道当前的帐户密码，则可能需要重置密码；必须具有重置密码的权限。如果输入密码，该密码会在系统导入帐户时发生变化。如果删除某个帐户，请选择要在 Active Directory 中保留、禁用还是删除该帐户。

还可以指示从目录中删除计算机或删除目录时要保留、禁用还是删除 Active Directory 帐户。

## 更改目录的主映像

我们建议您在更改目录的主映像之前保存映像的副本或快照。数据库会保留每个计算机目录中使用映像的历史记录。如果用户在部署到其桌面的新映像时遇到问题，则可以将其回滚到以前的版本，从而最大限度地减少用户停机时间。不要对映像进行删除、移动或重命名。否则，您将无法回滚主映像。

### 重要：

更改永久目录的主映像时，请考虑以下几点：只有稍后添加到目录的计算机才会使用新映像创建。我们不会将新映像发布到目录中的现有计算机上。

更新计算机后，计算机将自动重新启动。

## 更新或创建映像

在更改目录的主映像之前，请通过更新现有映像或创建映像在主虚拟机管理程序上准备新映像。

1. 在您的虚拟机管理程序或云服务提供程序上，创建当前 VM 的快照并为该快照提供一个有意义的名称。此快照可用于回滚主映像。
2. 如有需要，请打开映像的电源并登录。
3. 安装更新或对映像做任何必要的更改。
4. 如果映像使用个人虚拟磁盘，请更新清单。
5. 关闭 VM 的电源。
6. 拍摄 VM 的快照，为快照指定一个有意义的名称，以便在更改主映像时识别。

### 注意：

尽管您可以使用管理界面创建快照，但我们建议您使用虚拟机管理程序管理控制台创建快照，然后在完整配置管理界面中选择该快照。使用此方法可以提供有意义的名称及说明，而非自动生成的名称。对于 GPU 映像，只能通过 XenServer 的 XenCenter 控制台进行更改。

## 更改主映像

要向目录中的所有计算机推出新的主映像，请执行以下操作：

1. 在管理 > 完整配置中，选择左窗格中的计算机目录。
2. 选择一个目录，然后在操作栏中选择更改主映像。
3. 在映像页面上，选择要推出的主机和映像。

提示：

对于 MCS 创建的目录，可以通过为映像添加注释来对其映像进行注释。注释最多可以包含 500 个字符。每次更改主映像时，无论您是否添加注释，都会创建与注释相关的条目。如果您在未添加注释的情况下更新目录，该条目将显示为空 (-)。要查看映像的注释历史记录，请选择目录，在下方窗格中单击模板属性，然后单击查看附注历史记录。

4. 在回滚策略页面上，选择何时使用新映像更改计算机目录中的计算机：下次关闭时或立即更改。

注意：

前滚策略页面不适用于永久 VM，因为部署仅适用于非永久 VM。

5. 确认摘要页面上的信息，然后选择完成。每台计算机都在更新后自动重新启动。

要跟踪更新进度，请在 计算机目录 中找到目录，以查看内联进度条和分步进度图。对于非永久目录，您可以通过“图像更新”列跟踪其 图像更新 状态，包括 已完全更新、部分更新、待更新和 准备图片。

提示：

要显示“映像更新”列，请在操作栏中选择“要显示的列”图标，选择“计算机目录” > “映像状态”，然后单击“保存”。

如果要使用 PowerShell SDK 更新目录，可以指定一个虚拟机管理程序模板 (VM Templates)，作为映像或映像的快照的替换选项。

## 前滚策略

下次关机时更改映像将立即影响当前未使用的任何计算机，即没有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。

注意：

部署策略仅适用于非永久 VM。

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。
- 对于单会话计算机，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。

**回滚主映像**

推出更新后的映像或新映像后，可以将其回滚。如果新更新的计算机出现问题，可能有必要进行回滚。回滚时，目录中的计算机将回滚到上一个工作映像。需要较新映像的任何新功能将不再可用。与前滚一样，回滚计算机也需要重新启动。

1. 在管理 > 完整配置中，选择左窗格中的计算机目录。
2. 选择目录，然后在操作栏中选择“回滚主映像”。
3. 按前滚操作所述，指定对计算机应用早期映像的时间。

回滚仅适用于需要还原的计算机。对于尚未更改为新映像或更新映像的计算机（例如，用户未注销的计算机），用户不会收到通知消息，也不会被强制注销。

要跟踪回滚进度，请在 计算机目录中找到该目录，以查看内联进度条和分步进度图。

在某些情况下无法回滚，包括以下情况。（回滚主映像选项不可见）。

- 您没有回滚权限。
- 该目录不是使用 MCS 创建的。
- 该目录是使用操作系统磁盘的映像创建的。
- 用于创建该目录的快照已损坏。
- 用户对该目录中的计算机进行的更改不会保留。
- 该目录中的计算机处于运行状态。

**更改功能级别或撤消更改**

将计算机上的 VDA 升级到新版本后，更改计算机目录的功能级别。我们建议将所有 VDA 升级到最新版本，以访问所有最新功能。

在更改计算机目录的功能级别之前：

- 启动升级后的计算机，以便它们在 Citrix DaaS 中注册。这样，管理界面便可以确定目录中的计算机是否需要升级。

要更改目录的功能级别，请执行以下操作：

1. 在管理 > 完整配置中，选择左窗格中的计算机目录。
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“更改功能级别”。如果管理界面检测到目录需要更改功能级别，则会显示一条消息。按照提示进行操作。如果一台或多台计算机无法更改，则会显示一条消息说明原因。确保所有计算机都能正常运行。我们建议您在单击“更改”之前解决这些问题。

目录升级完成后，您可以选择目录，然后在操作栏中选择“撤消功能级别更改”，将计算机还原为其先前的 VDA 版本。

## 克隆目录

在克隆目录之前，请注意以下事项：

- 无法更改与[操作系统](#)和[计算机管理](#)关联的设置。克隆的目录从原始目录继承这些设置。
- 克隆目录可能需要一些时间才能完成。如有必要，请选择隐藏进度以在后台运行克隆。
- 克隆的目录继承了原始目录的名称，并带有后缀 [Copy](#)。可以更改此名称。请参阅[重命名目录](#)。
- 克隆完成后，请务必将克隆的目录分配给交付组。
- 您可以通过克隆来创建空目录。在目录克隆期间，您可以将 MCS 配置的目录的计算机数量设置为零，而对于非 MCS 配置的目录，可以不添加任何计算机。

1. 在管理 > 完整配置中，选择左窗格中的计算机目录。
2. 选择一个目录，然后在操作栏中选择克隆。
3. 在克隆选定的计算机目录窗口中，查看克隆的目录的设置并配置适用的设置。选择下一步进入下一页。
4. 在摘要页面上，查看设置的摘要，然后选择完成开始克隆。
5. 如有必要，请选择隐藏进度以在后台运行克隆。

## 使用文件夹整理目录

可以创建文件夹来整理目录以便于轻松访问。例如，您可以按映像类型或组织结构来组织目录。

### 必需的角色

默认情况下，您需要具有以下内置角色才能创建和管理目录文件夹：云管理员、完全权限管理员或计算机目录管理员。如有必要，您可以自定义用于创建和管理目录文件夹的角色。有关详细信息，请参阅 [必需权限](#)。

## 创建目录文件夹

在开始之前，请先计划如何整理您的目录。请注意以下事项：

- 最多可以嵌套五级深度的文件夹（不包括默认的根本文件夹）。
- 目录文件夹可以包含目录和子文件夹。
- 完全配置 中的所有节点（例如 计算机目录 和 应用程序 节点）在后端共享一个文件夹树。为避免在重命名或移动文件夹时与其他节点发生名称冲突，我们建议您为不同节点中的第一级文件夹指定不同的名称。

要创建目录文件夹，请执行以下步骤：

1. 在管理 > 完整配置中，选择左窗格中的计算机目录。
2. 在文件夹层次结构中，选择一个文件夹，然后在操作栏中选择创建文件夹。

3. 输入新文件夹的名称，然后单击完成。

提示：

如果您在非预期位置创建文件夹，则可以将其拖动到正确的位置。

移动目录

可以在文件夹之间移动目录。详细步骤如下所示：

1. 在管理 > 完整配置中，选择左窗格中的计算机目录。
2. 按文件夹查看目录。也可以打开文件夹层次结构上方的查看全部以一次查看所有目录。
3. 右键单击某个目录，然后选择移动计算机目录。
4. 选择要将目录移动到的文件夹，然后单击完成。

提示：

可以将目录拖到某个文件夹。

管理目录文件夹

可以删除、重命名和移动目录文件夹。

仅当文件夹及其子文件夹不包含目录时，才能删除该文件夹。

要管理文件夹，请执行以下步骤：

1. 在管理 > 完整配置中，选择左窗格中的计算机目录。
2. 在文件夹层次结构中，选择一个文件夹，然后根据需要在 操作 栏中选择一个操作：
  - 要重命名文件夹，请选择重命名文件夹。
  - 要删除文件夹，请选择删除文件夹。
  - 要移动文件夹，请选择移动文件夹。
3. 按照屏幕上的说明完成其余步骤。

所需的权限

下表列出了对目录文件夹执行操作所需的权限。

操作	所需的权限
创建目录文件夹	创建计算机目录文件夹
删除目录文件夹	移除计算机目录文件夹

操作	所需的权限
移动目录文件夹	移动计算机目录文件夹
重命名目录文件夹	编辑计算机目录文件夹
将目录移至文件夹	编辑计算机目录文件夹和编辑计算机目录属性

为 **VDA** 配置自动升级

重要：

- 为确保平稳升级，在将 VDA 升级到 CR 或 LTSR CU 版本之前，请确保满足必备条件并查看已知问题。请参阅[使用完整配置界面升级 VDA](#)。
- 将 LTSR VDA 升级到 LTSR 累积更新 (CU) 版本时，请确保在 VDA 上运行的 VDA 升级代理版本为 7.36.0.7 或更高版本。有关详细信息，请参阅[使用完整配置界面升级 VDA](#)。
- 只要从早期版本切换到更高版本，就可以在 CR VDA 和 LTSR VDA 之间切换。您无法从更高版本切换到较早的版本，因为这被视为降级。例如，您无法从 2212 CR 降级到 2203 LTSR（任何 CU），但可以从 2112 CR 升级到 2203 LTSR（任何 CU）。
- 也可以使用 PowerShell 升级 VDA。请参阅[使用 PowerShell 升级 VDA](#)。

使用该功能，您可以执行以下操作：

- 逐个目录升级 VDA
- 编辑或取消计划的 VDA 升级
- 在创建目录后配置 VDA 升级设置
- 以每台计算机为单位升级 VDA

注意：

- 计划目录的 VDA 升级时，只有安装了 VDA 升级代理的目录中的 VDA 才能升级。
- 当计算机处于维护模式或在计算机上运行会话时，升级 VDA 将失败。

支持的计算机类型

此功能适用于以下计算机类型：

- MCS 配置的永久计算机（[已加入 AD](#)、[已加入 Azure AD](#) 和[未加入域](#)）。在目录创建过程中，您可以使用计算机管理页面上的 **Citrix Machine Creation Services** 进行部署。
- [Remote PC Access](#) 计算机
- [适用于 Windows 365 计算机的 Citrix HDX Plus](#)
- 其他使用非 Citrix 预配服务或技术预配的永久性计算机。在目录创建过程中，您可以使用“计算机管理”页面上的其他服务或技术，将这些计算机添加到 **DaaS** 中进行管理。



有关 **Citrix Machine Creation Services** 和其他服务或技术选项的详细信息，请参阅[计算机管理](#)。

注意：

对于 MCS 配置的计算机，仅支持静态永久性计算机。不支持随机计算机，即使它们是永久性的。

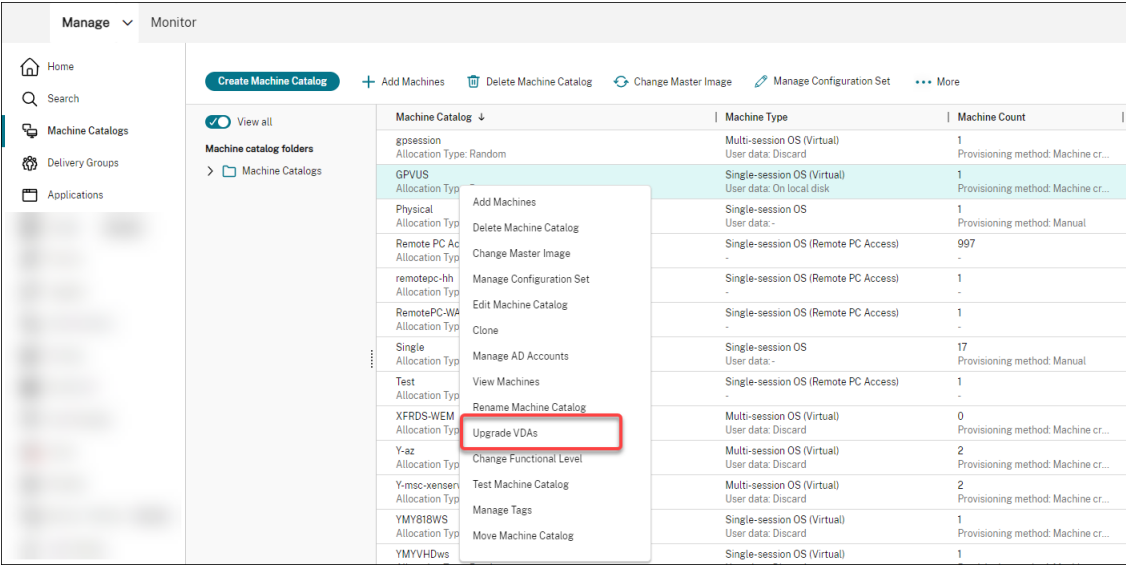
逐个目录升级 **VDA**

注意：

在为目录安排 VDA 升级时，请注意，该目录中的所有计算机都将包含在升级范围内。因此，我们建议在启动升级之前备份这些计算机。

为目录启用 VDA 升级后，您可以立即升级目录中的 VDA 或计划目录的升级。为此，请按照以下步骤操作：

1. 在管理 > 完整配置中，选择计算机目录。
2. 选择目录，然后从上下文菜单或操作栏中 升级 **VDA**。（右键单击可显示上下文菜单。）出现 VDA 升级窗口。



3. 选择是否升级部署中的其他组件。除了升级之外，您还可以选择安装某些组件。如果某个组件需要配置，则必须单击“配置”按钮并配置该组件的设置才能继续。配置完成后，您可以单击“编辑”来更改配置。

重要：

- 要使用附加组件功能，请确保您的 VDA Upgrade Agent 为 7.34 或更高版本，该版本包含在 VDA 安装程序版本 2206 或更高版本中。

注意：

- 如果您选择不升级组件，则该组件在您的部署中将保持不变。
- 有关其他组件的完整列表，请参阅[安装 VDA](#)。

1

Additional Components

2

Features

3

Schedule

4

Additional Components

Upgrade VDAs in the catalog immediately or schedule VDA upgrades for the catalog. Choose whether install additional components and enable features as part of the upgrade process. [Learn more](#)

To use this feature, ensure that the VDA Upgrade Agent is version 7.34 or later (available with the VDA installer version 2206 or later).

Specify whether to upgrade the following components in your deployment.

Components

↓

✓

Citrix Profile Management

Manages user personalization settings in user profiles. Omitting this component affects monitoring and troubleshooting VDAs with Citrix Director.

✓

Citrix Profile Management WMI Plug-in

Provides Profile Management runtime information in WMI (Windows Management Instrumentation) objects, for example, profile provider, profile type, size, and disk usage. WMI Objects provide session information to Citrix Director.

✓

Machine Identity Service

Citrix Machine Identity Service Agent.

Specify whether to install the following components along with the upgrade.

Components

↓

Citrix MCS IO Driver

Citrix MCS IO Driver Component.

Citrix Personalization for App-V - VDA

Enables the VDA to launch App-V packages.

Citrix Rendezvous V2

Citrix Rendezvous V2 allows VDAs to bypass the Citrix Cloud Connectors to connect directly and securely with Citrix Cloud Control plane when using the Citrix Gateway Service.

User Personalization Layer

Installs Components for the user personalization layer, a modern alternative to Personal vDisk, built using App Layering technology.

4. 单击下一步。

5. 选择是否启用任何列出的功能。单击下一步。

注意：

默认情况下，“启用还原清理”复选框处于选中状态。我们建议启用还原功能。启用该功能后，将在升级开始之前创建系统还原点。成功安装 VDA 后，还原点将被删除。有关详细信息，请参阅 [安装或升级失败时还原](#)。

✓

Additional Components

2

Features

3

Schedule

4

Features

Specify whether to enable the following features in your deployment. [Learn more](#)

Features

↓

Enable HDX Ports

Opens ports in the Windows firewall required by the VDA and enabled features (except Windows Remote Assistance), if the Windows Firewall Service is detected, even if the firewall is not enabled. If you are using a different firewall or no firewall, you must configure the firewall manually.

Enable HDX UDP ports

Opens UDP ports in the Windows firewall that HDX adaptive transport uses, if the Windows Firewall Service is detected, even if the firewall is not enabled. If you are using a different firewall or no firewall, you must configure the firewall manually.

Enable Real Time transport

Enables or disables use of UDP for audio packets (RealTime Audio Transport for audio). Enabling this feature can improve audio performance.

Enable Remote assistance

Enables the shadowing feature in Windows Remote Assistance for use with Director. If you specify this option, Windows Remote Assistance opens the dynamic ports in the firewall.

Enable Restore

Enables automatic return to the restore point, if the VDA install or upgrade fails. If the install/upgrade completes successfully, EnableRestore instructs the installer to retain the restore point, even though it was not used.

✓

Enable restore cleanup

Enables automatic return to the restore point, if the VDA install or upgrade fails. If the install/upgrade completes successfully, EnableRestoreCleanup instructs the installer to remove the restore point.

Enable Screen Sharing Ports

Opens ports in the Windows Firewall that are required for screen sharing, if the Windows Firewall Service is detected, even if the firewall is not enabled. If you are using a different firewall or no firewall, you must configure the firewall manually.

6. 选择是立即升级 VDA 还是按计划时间升级 VDA。

- 要立即升级 VDA，请选择 立即升级，然后指定持续时间。

持续时间是以小时为单位的时间，在此时间之后 VDA 升级服务停止启动其他升级。正在进行的升级将运行

至完成。在此期间，当 VDA 符合条件时，DaaS 会开始升级（例如，不再有活动会话）。

必须升级的 VDA 越多，持续时间越长。我们建议选择较大的值（例如 12 小时）。否则，可能仍会有 VDA 无法在此窗口内升级 DaaS，具体取决于 VDA 的数量。

- 要计划升级，请选择 稍后 升级，然后指定升级的时间。

您只能为接下来的七天安排升级。您计划的升级仅适用于目录中当前的计算机。如果您稍后向目录中添加了计算机，但也希望对其进行升级，请取消计划的升级，然后重新创建计划。

7. 单击下一步。

8. 在“摘要”页面上查看您的选择，然后单击“完成”以应用您的设置并退出窗口。

注意：

- 只有在为目录启用 VDA 升级后，升级 **VDA** 选项才可用。要启用 VDA 升级，请[编辑目录](#)。
- 在推出升级时，目录中的所有计算机都将置于维护模式。升级最多可能需要 30 分钟才能开始，并且只会在指定的时间段内执行。

在 计算机目录 节点上，“**VDA 升级**”列提供了目录的 VDA 升级信息。可能会出现以下信息：

提示：

要显示 **VDA** 升级列，请在操作栏中选择要显示的列，选择计算机目录 > **VDA 升级**，然后单击保存。

- 可用：有新的 VDA 版本可用。
- 已计划：已计划 VDA 升级。
- 未配置：未为目录启用 VDA 升级时显示。
- 最新：目录的 VDA 是最新的。
- 未知：无法获取 VDA 升级所需的信息。有多种可能的原因：
  - VDA 在升级期间正在使用。
  - 正在进行的升级数量达到了 500 的最大限制。
  - 在升级期间，[VDA 升级代理](#)没有响应。确保代理在 VDA 上运行并且可以与 Citrix DaaS 通信。
  - 无法执行升级验证检查。请参阅[VDA 升级要求](#)。

您还可以查看目录的 VDA 升级状态。为此，请单击目录，然后在“详细信息”选项卡上查看 **VDA** 升级状态 信息。可能会出现以下信息：

- 未计划：您已为目录启用 VDA 升级，但尚未设置升级计划。
- 已计划：您已为目录创建了升级计划。例如，如果将计划设置为 09:00 PM, December 14, 2030 开始，则会显示如下信息：December 14, 2030 09:00 PM UTC 的计划。
- 进行中：VDA 升级已启动。
- 已取消：您已取消计划的升级。
- 失败：目录包含一台或多台 VDA 升级未成功的计算机。
- 成功：目录中的所有 VDA 均已成功升级。

您还可以使用针对目录的建议操作对 VDA 升级问题进行故障排除。为此，请单击目录，然后转到“故障排除”选项卡。

要快速细化到具有特定 VDA 升级状态的目录，可以使用筛选器。有关详细信息，请参阅在“完整配置”管理界面中使用搜索。

请注意以下事项：

- **VDA** 升级或 **VDA** 升级状态过滤器仅可用于以下过滤器：名称和计算机目录。
- 使用 **VDA** 升级或 **VDA** 升级状态过滤器时，右上角的错误和警告将变为不可用。

### 编辑或取消计划的 **VDA** 升级

为目录安排升级后，您可能需要编辑或取消计划的升级。为此，请按照以下步骤操作：

1. 在管理 > 完整配置中，选择计算机目录。
2. 选择目录，然后在操作栏中选择编辑计划的 **VDA** 升级。将出现“编辑 VDA 升级”窗口，显示有关已安装的 VDA 版本和要升级到的 VDA 版本的信息。
3. 选择是编辑还是取消计划的升级。
  - 要取消升级，请单击“取消计划的升级”。请记住：取消计划的升级不会强制停止正在进行的升级。
4. 单击“完成”退出窗口。

### 通过编辑目录配置 **VDA** 升级设置

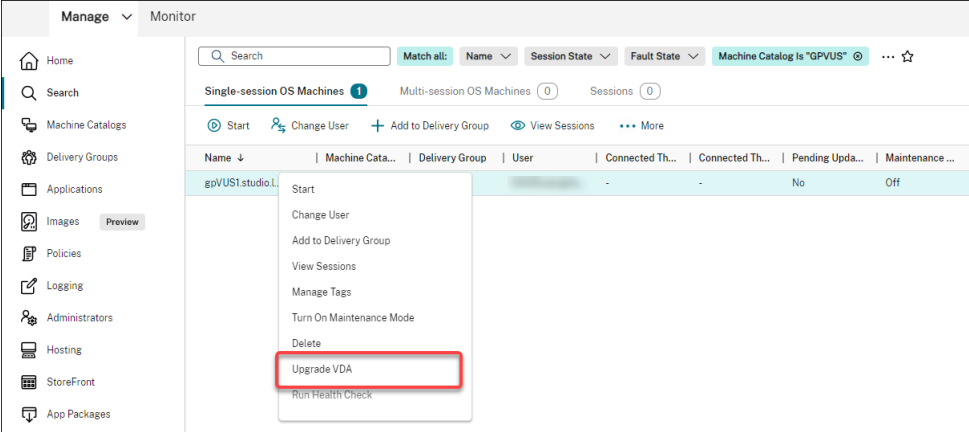
创建目录后，可以通过编辑目录来配置 VDA 升级设置。在开始编辑之前，请考虑以下事项：

- 验证目录中的所有计算机是否都在同一 VDA (CR 或 LTSR) 轨道上。否则，某些 VDA 升级将失败。例如，如果您选择最新 **LTSR VDA**，则 CR VDA 升级将失败。
- 目录中某些计算机的升级可能已经开始。您无法修改已在进行的升级。正在进行的升级仍在继续。那些尚未启动的版本将升级到指定版本。

以每台计算机为单位升级 **VDA**

为目录启用 VDA 升级后，您可以逐个或批量升级该目录的 VDA。为此，请按照以下步骤操作：

1. 从“管理” > “完整配置”中，选择“搜索”。
2. 选择一台或多台计算机，然后从上下文菜单或操作栏中升级 **VDA**。（右键单击可显示上下文菜单。）



注意：

- 要使“升级 **VDA**”选项可用，请确保已为选定计算机所在的目录启用 VDA 升级，并且这些计算机安装了 VDA 升级代理。要为其启用 VDA 升级，请编辑目录。
- 在推出升级时，计算机将被置于维护模式。升级最多可能需要 30 分钟才能开始。
- 如果您选择的计算机包含 VDA 升级不可用或升级处于挂起状态（已计划、正在进行或等待升级）的计算机，我们将跳过这些计算机的升级。

在“搜索”节点上，可以添加“**VDA** 升级”列。有关如何添加自定义列的信息，请参阅 [自定义要显示的列](#)。该列很有用。它为计算机提供了 VDA 升级信息。可能会出现以下信息：

- 可用：有新的 VDA 版本可用。
- 已计划：已计划 VDA 升级。
- 未配置：未为计算机启用 VDA 升级时显示。
- 最新：VDA 是最新的。
- 未知：尚无有关 VDA 升级的信息。

您还可以查看计算机的 VDA 升级状态。为此，请单击计算机，然后在“详细信息”选项卡上查看 **VDA** 升级状态 信息。可能会出现以下信息：

- 未知：无法获取 VDA 升级所需的信息。有多种可能的原因：
  - VDA 在升级期间正在使用。
  - 正在进行的升级数量达到了 500 的最大限制。
  - 在升级期间，[VDA 升级代理](#)没有响应。确保代理在 VDA 上运行并且可以与 Citrix DaaS 通信。
  - 无法执行升级验证检查。请参阅 [VDA 升级要求](#)。

- 已计划：您已设置升级计划。例如，如果将计划设置为 09:00 PM, December 14, 2030 开始，则会显示如下信息：December 14, 2030 09:00 PM UTC 的计划。
- 等待升级：计算机处于维护模式，等待升级。（请确保用户已注销会话，以便升级可以继续。）
- 进行中：VDA 升级已启动。
- 升级失败：尝试升级 VDA 失败。
- 验证失败：尝试验证 VDA 升级设置失败。
- 已取消：计算机的升级已被取消。
- 成功：VDA 已成功升级。

您还可以使用针对计算机的建议操作对 VDA 升级问题进行故障排除。为此，请单击计算机，然后转到“故障排除”选项卡。

要快速深入查看具有特定 VDA 升级状态的计算机，可以使用过滤器。有关详细信息，请参阅在“完整配置”管理界面中使用搜索。请注意以下事项：

- **VDA 升级或 VDA 升级状态过滤器**仅可用于以下过滤器：名称和计算机目录。
- 使用 **VDA 升级或 VDA 升级状态过滤器**时，右上角的错误和警告将变为不可用。

## 管理目录的配置集

在开始之前，请确保已设置 WEM 服务部署。有关详细信息，请参阅 [Workspace Environment Management 服务入门](#)。

### 注意：

默认情况下，如果您具有云管理员、完全访问权限管理员或计算机目录管理员角色，则可以管理目录的配置集。如有必要，您可以通过向角色授予“管理配置集”权限来允许他们管理配置集。

## 将目录绑定到配置集

### 重要：

如果您的 Citrix DaaS 和 WEM 服务实例不在同一区域中，则无法将目录绑定到配置集。在这种情况下，请将您的 WEM 服务迁移到与 Citrix DaaS 相同的区域。

要将目录绑定到配置集，请执行以下步骤：

1. 在管理 > 完整配置中，选择计算机目录。
2. 选择计算机目录，然后在操作栏中选择管理配置集。此时将显示管理配置集窗口。
3. 选择要将目录绑定到的 WEM 配置集。

### 注意：

如果选定的配置集不包含与 WEM 的基本配置相关的设置，则会出现将基本设置应用到配置集选项。我们

建议您选择用于将基本设置应用到配置集的选项。

4. 单击保存以保存更改。

## 切换到其他配置集

要切换到目录的其他配置集，请执行以下步骤：

1. 在管理 > 完整配置中，选择计算机目录。
2. 选择计算机目录，然后在操作栏中选择管理配置集。此时将显示管理配置集窗口。
3. 选择要将目录绑定到的其他 WEM 配置集。
4. 单击保存以保存更改。

## 从配置集取消绑定目录

要从配置集解除目录的绑定，请执行以下步骤：

1. 在管理 > 完整配置中，选择计算机目录。
2. 选择计算机目录，然后在操作栏中选择管理配置集。此时将显示管理配置集窗口。
3. 单击所选配置集右侧的 X 图标。
4. 单击保存以保存更改。

## 重试创建目录

注意：

此功能仅适用于 MCS 目录。

故障目录标有错误图标。要查看详细信息，请转到每个目录的故障排除选项卡。在重试创建目录之前，请注意以下注意事项：

- 请先查看故障排除信息并解决问题。该信息描述了发现的问题并提供了解决这些问题的建议。
- 无法更改与[操作系统](#)和[计算机管理](#)关联的设置。该目录继承了原始目录中的这些设置。
- 创作可能需要一些时间才能完成。如有必要，请选择隐藏进度以在后台运行创作。

要重试创建目录，请执行以下操作：

1. 在管理 > 完整配置中，选择左窗格中的计算机目录。
2. 选择目录，然后转到其“故障排除”选项卡。
3. 单击“重试”超链接重试创建目录。
4. 在出现的向导中，根据需要更改设置。如果无需进行更改，则可以直接转到“摘要”页面。
5. 完成后，选择“完成”开始创建。

(仅限非 Citrix 预置的 VDA) 生成和管理注册令牌

在决定为非 Citrix 置备的计算机启用基于令牌的注册后，必须首先根据每个计算机目录生成令牌，然后与 VDA 安装管理员共享。

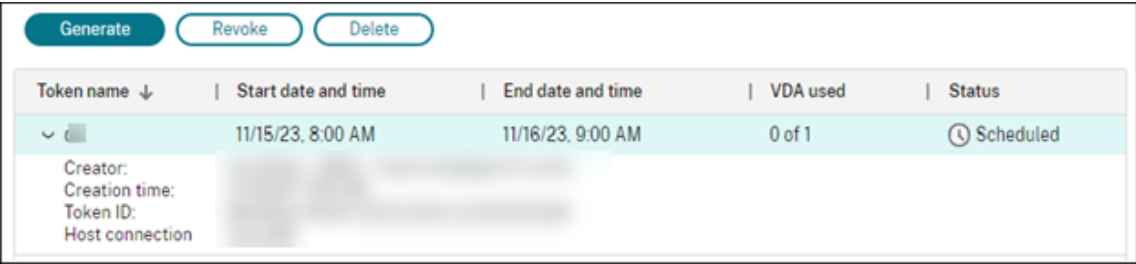
注册令牌具有以下特点：

- 注册范围：1—100 台 VDA 计算机
- 有效期：1 小时至 14 天

要使用完整配置为目录生成令牌，请执行以下步骤：

1. 在“完整配置” > “计算机目录”中，找到非 MCS 配置的目录，该目录的“计算机数量”列中显示了“预配方法：手动”。
2. 右键单击目录，然后选择“管理注册令牌”。
3. 在出现的生成注册令牌页面上，提供以下令牌信息：
  - 键入令牌的名称。
  - 输入其有效期。期限必须从一小时到十四天不等。该令牌仅在指定时间段内有效。
  - (可选) 选择主机连接，对使用令牌注册的 VDA 进行电源管理。选项包括该目录区域下的所有主机连接。
  - 输入令牌使用限制 (介于 1—100 之间)。
4. 单击 **Generate** (生成)。
5. 在出现的“成功生成令牌”窗口中，复制令牌并将其保存在安全的地方，或单击“下载”将其下载到“下载”文件夹。

令牌记录出现在令牌列表中。



<div>Generate Revoke Delete</div>				
Token name ↓	Start date and time	End date and time	VDA used	Status
▼ [icon]	11/15/23, 8:00 AM	11/16/23, 9:00 AM	0 of 1	🕒 Scheduled
Creator: Creation time: Token ID: Host connection				

6. 与 VDA 安装管理员共享令牌。

有关如何在计算机上安装 VDA 和令牌的更多信息，请参阅[安装 VDA](#)。

管理令牌

您可以通过两种方式撤消令牌并使其不可用于 VDA 注册：

- 撤销：撤销令牌，但将其保留在列表中以用于记录目的。
- 删除：撤消令牌并将其从列表中删除。



注意：

过期的令牌将在 14 天内自动删除。

## 使用 PowerShell

本部分内容详细介绍了如何使用 PowerShell 管理目录：

- [使用 PowerShell 检查 VDA 升级状态和 VDA 版本](#)
- [管理计算机名称的序列号](#)
- [启用一次性重新启动计划](#)
- [向映像中添加描述](#)
- [重置操作系统磁盘](#)
- [修复活跃计算机帐户的身份信息](#)
- [更改现有计算机目录的网络设置](#)
- [管理计算机目录的版本](#)
- [更改现有计算机目录的缓存配置](#)
- [将非基于计算机配置文件的计算机目录转换为基于计算机配置文件的计算机目录](#)
- [检索与目录关联的警告和错误](#)
- [删除没有虚拟机管理程序访问权限的计算机](#)

### 使用 PowerShell 检查 VDA 升级状态和 VDA 版本

使用 `Get-VusCatalog` PowerShell 命令检查 VDA 升级状态。假设目录名称为 `wuhanTestMC1`。可以在命令提示符下键入以下内容：

- `PS C:\> Get-VusCatalog -Name wuhanTestMC1`

```
PS C:\Users\hanw> Get-VusCatalog -Name wuhanTestMC1

CancelledUpgrades      : 0
DurationInHours        : 8
FailedUpgrades         : 0
InProgressUpgrades     : 0
LastStateChangeInUtc   : 4/22/2022 7:52:51 AM
MaxConcurrentUpgrades  : 100
Name                   : wuhanTestMC1
ProvisioningType        : MCS
ScheduledTimeInUtc     : 4/22/2022 7:20:56 AM
SecurityCheckFailedUpgrades : 0
SessionSupport         : SingleSession
StateId                : UpgradeSuccessful
SuccessfulUpgrades     : 1
TotalMachines          : 1
Uid                    : 12
UpgradeState           : UpgradeAvailable
UpgradeType            : CR
UpgradeVersion         : 2112.0.0.32068
Uuid                   : 339e7bce-271b-4c37-9a1c-bce287008b65
```

在此示例中，UpgradeState 为 UpgradeAvailable，表示已为目录启用 VDA 升级。StateId 为 UpgradeSuccessful，表示该目录已成功升级到 2112.0.0.32068 (UpgradeVersion)。

使用 Get-BrokerMachine PowerShell 命令获取当前 VDA 版本。

```

SessionProtocol           :
SessionSecureIcaActive    :
SessionSmartAccessTags    :
SessionStartTime          :
SessionState              :
SessionStateChangeTime    :
SessionSupport            : MultiSession
SessionType               :
SessionUid                :
SessionUserName           :
SessionUserSID            :
SessionsEstablished        : 0
SessionsPending           : 0
SummaryState              : Unregistered
SupportedPowerActions     : {}
Tags                      : {}
UUID                      : 9c0c4623-a4dc-44f9-ae4b-54c86cc76a7f
Uid                       : 4
VMToolsState              : NotPresent
WillShutdownAfterUse      : False
WillShutdownAfterUseReason : None
WindowsConnectionSetting  : LogonEnabled
ZoneHealthy               : False
ZoneName                  : My Resource Location
ZoneUid                   : ae0366c2-3001-459d-89ff-0b159c9d436d

AgentVersion              : 2112.0.0.32068 ←
AllocationType            : Static
ApplicationsInUse         : {}
AssignedClientName        :
AssignedIPAddress         :
AssignedUserSIDs          : {}
AssociatedTenantId        :
AssociatedUserFullNames   : {}
AssociatedUserNames       : {}
AssociatedUserSIDs        : {}
AssociatedUserUPNs        : {}
AzureADJoinedMode         : NotAadJoined
BrowserName               :
Capabilities               : {}
CatalogName               : wuhanTestMC1
CatalogUUID               : 339e7bce-271b-4c37-9a1c-bce287008b65
CatalogUid                : 12
CbpVersion                :
ColorDepth                :
ControllerDNSName         :
DNSName                   : wuhanVUSTest02.WHCloud.Internal
DeliveryType              :
Description                :
DesktopConditions          : {}

```

使用 `Get-VusAvailableVdaVersion` PowerShell 命令获取最新的 VDA 版本。

```
PS C:\Users\hanw> Get-VusAvailableVdaVersion
```

```

UpgradeType  Version
-----
CR  2203.0.0.33220
LTSR 2203.0.0.33220

```

## 管理计算机名称的序列号

要通过 PowerShell 命令自定义使用 MCS 部署的计算机的序列号，请执行以下操作：

1. 以管理员身份在 Delivery Controller 上打开 PowerShell。
2. 运行命令 `asnp citrix*` 加载 Citrix 模块。
3. 运行以下命令检查目录身份池的起始次数：

```
1 Get-AcctIdentityPool -IdentityPoolName xxx
2 <!--NeedCopy-->
```

`IdentityPoolName` 是目录的名称。

4. 如果要将此计数设置为其他值，请运行以下命令并将 `StartCount` 指定为 X：

```
1 Set-AcctIdentityPool -IdentityPoolName xxx -StartCount X
2 <!--NeedCopy-->
```

5. 将计算机添加到目录中，以便按所需数量创建计算机。
6. 创建计算机后，运行以下命令将其设置回原始值 Y：

```
1 Set-AcctIdentityPool -IdentityPoolName xxx -StartCount Y
2 <!--NeedCopy-->
```

## 启用一次性重启计划

如果要使用 PowerShell 启用一次性重新启动计划，请使用以下 `BrokerCatalogRebootSchedule` PowerShell 命令创建、修改和删除重新启动计划：

- `Get-BrokerCatalogRebootSchedule`
- `New-BrokerCatalogRebootSchedule`
- `Set-BrokerCatalogRebootSchedule`
- `Remove-BrokerCatalogRebootSchedule`
- `Rename-BrokerCatalogRebootSchedule`

示例：

- 为目录中名为 **BankTellers** 的 VM 创建重新启动计划，该计划将于 2022 年 2 月 3 日凌晨 2 点到凌晨 4 点之间开始。

```
1 New-BrokerCatalogRebootSchedule -Name BankTellers
2 -CatalogName BankTellers
3 -StartDate "2022-02-03"
4 -StartTime "02:00"
5 -Enabled $true
6 -RebootDuration 120
```

```
7 <!--NeedCopy-->
```

- 为目录中 UID 为 17 的 VM 创建重新启动计划，该计划将于 2022 年 2 月 3 日凌晨 1 点到凌晨 5 点之间开始。在重启前十分钟，每个 VM 都设置为在每个用户会话中显示一个消息框，标题为：警告：重启待定以及消息保存您的工作。

```
1 New-BrokerCatalogRebootSchedule
2 -Name 'Update reboot'
3 -CatalogUid 17
4 -StartDate "2022-02-03"
5 -StartTime "01:00" -Enabled $true -RebootDuration 240
6 -WarningTitle "WARNING: Reboot pending"
7 -WarningMessage "Save your work" -WarningDuration 10
8 <!--NeedCopy-->
```

- 要重命名目录，请重新启动名为“旧名称改为新名称”的时间表。

```
1 Rename-BrokerCatalogRebootSchedule -Name "Old Name" -NewName "New
   Name"
2 <!--NeedCopy-->
```

- 显示 UID 为 1 的所有目录重新启动计划，然后将 UID 为 1 的目录重新启动计划重命名为新名称。

```
1 Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
   BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
2 <!--NeedCopy-->
```

- 将名为会计的目录重启计划设置为在每台 VM 重启前十分钟显示标题为“警告：待重启”的消息，以及消息“保存您的工作”。该消息出现在该 VM 上的每个用户会话中。

```
1 Set-BrokerCatalogRebootSchedule -Name Accounting
2 -WarningMessage "Save your work"
3 -WarningDuration 10 -WarningTitle "WARNING: Reboot pending"
4 <!--NeedCopy-->
```

- 显示所有已禁用的重新启动计划，然后启用所有已禁用的重新启动计划。

```
1 Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
   BrokerCatalogRebootSchedule -Enabled $true
2 <!--NeedCopy-->
```

- 使用 UID 17 设置目录重启时间表以显示以下消息：在每个 VM 重启前的十五、十和五分钟内，在 %m% 分钟内重新启动。

```
1 Set-BrokerCatalogRebootSchedule 17 -WarningMessage "Rebooting in
   %m% minutes." -WarningDuration 15 -WarningRepeatInterval 5
2 <!--NeedCopy-->
```

- 为名为 **MyCatalog** 的目录配置时区。

```
1 Set-BrokerCatalog -Name "MyCatalog" -TimeZone <TimeZone>
```

```
2 <!--NeedCopy-->
```

## 向映像中添加描述

可以添加与计算机目录的映像更新有关的更改的信息性描述。在创建目录时或更新目录的现有主映像时，可以使用此功能添加描述。还可以显示目录中的每个主映像的信息。此功能对于希望在更新目录使用的主映像（例如安装的 *Office 365*）时添加描述性标记的管理员非常有用。使用以下命令添加或查看映像说明：

- **NewProvScheme**。新参数 **masterImageNote** 允许您向映像中添加注释。例如：

```
1 C:\PS>New-ProvScheme -ProvisioningSchemeName XenPS -HostingUnitName
   XenHu -IdentityPoolName idPool1 -MasterImageVM XDHyp:\HostingUnits\
   XenHU\Base.vm\Base.snapshot -MasterImageNote "Office365 installed"
2 <!--NeedCopy-->
```

- **Publish-ProvMasterVMImage**。使用此参数可发布注释。例如：

```
1 C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName MyScheme -
   MasterImageVM XDHyp:\HostingUnits\HostUnit1\RhoneCC_baseXP.vm\base.
   snapshot -MasterImageNote "Visual Studio 2019 installed"
2 <!--NeedCopy-->
```

- **Get-ProvSchemeMasterVMImageHistory**。显示每个映像的信息。例如：

```
1 C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
   MyScheme -Showall
2
3 VMImageHistoryUid : 3cba3a75-89cd-4868-989b-27feb378fec5
4
5 ProvisioningSchemeUid : 7585f0de-192e-4847-a6d8-22713c3a2f42
6
7 ProvisioningSchemeName : MyScheme
8
9 MasterImageVM : /Base.vm/base.snapshot
10
11 Date : 17/05/2021 09:27:50
12
13 MasterImageNote : Office365 installed
14 <!--NeedCopy-->
```

## 重置操作系统磁盘

使用 PowerShell 命令 **Reset-ProvVMDisk** 在 MCS 创建的计算机目录中重置永久性 VM 的操作系统磁盘。目前，此功能适用于 Azure、Google Cloud、SCVMM、VMware 和 XenServer 虚拟化环境。

要成功运行 PowerShell 命令，请确保：

- 目标 VM 位于永久 MCS 目录中。
- MCS 计算机目录运行正常。这意味着资源预配方案和主机存在，并且预配方案有正确的条目。
- 虚拟机管理程序未处于维护模式。
- 目标 VM 已关闭电源并处于维护模式。

请执行以下步骤以重置操作系统磁盘：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载特定于 Citrix 的 PowerShell 模块。
3. 使用以下任一方式运行 PowerShell 命令 `Reset-ProvVMDisk`：

- 将 VM 列表指定为以逗号分隔的列表，然后在每个 VM 上执行重置：

```
1 Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc", "def") -OS
2 <!--NeedCopy-->
```

- 将 VM 列表指定为 `Get-ProvVM` 命令的输出，然后在每个 VM 上执行重置：

```
1 (Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk "abc" -OS
2 <!--NeedCopy-->
```

- 按名称指定单个 VM：

```
1 Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
2 <!--NeedCopy-->
```

- 为 `Get-ProvVM` 命令返回的每个 VM 创建单独的重置任务。这种方法效率较低，因为每个任务都将执行相同的冗余检查，例如虚拟机管理程序功能检查、每个 VM 的连接检查。

```
1 Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk - ProvisioningSchemeName "xxx" -OS
2 <!--NeedCopy-->
```

4. 出现确认提示，其中列出了要重置的 VM 以及一条警告消息，提示这是不可恢复的操作。如果您没有提供答案并按 **Enter** 键，则不会采取进一步的操作。

可以运行 PowerShell 命令 `-WhatIf` 来打印其要执行的操作，然后在不执行该操作的情况下退出。

也可以使用以下方法之一绕过确认提示：

- 提供 `-Force` 参数：

```
1 Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS -Force
2 <!--NeedCopy-->
```

- 提供 `-Confirm:$false` 参数：

```
1 Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"  
  -OS -Confirm:$false  
2 <!--NeedCopy-->
```

- 在运行 `Reset-ProvVMDisk` 之前，请将 `$ConfirmPreference` 更改为“无”：

```
1 PS C:\Windows\system32> $ConfirmPreference= 'None'  
2 PS C:\Windows\system32> $ConfirmPreference  
3 None  
4 PS C:\Windows\system32> Reset-ProvVMDisk -  
  ProvisioningSchemeName "xxx" -VMName "abc" -OS  
5 <!--NeedCopy-->
```

注意：

在重置过程完成之前，请勿使虚拟机退出维护模式或开启 VM。

5. 运行 `Get-ProvTask` 以获取 `Reset-ProvVMDisk` 命令返回的任务的状态。

## 修复活跃计算机帐户的身份信息

可以重置存在身份相关问题的活动计算机帐户的身份信息。可以选择仅重置计算机密码和信任密钥，也可以重置身份磁盘的所有配置。此实现同时适用于永久和非永久 MCS 计算机目录。

注意：

目前，只有 Azure 和 VMware 虚拟化环境支持该功能。

## 条件

请务必满足以下条件才能成功重置身份磁盘：

- 关闭 VM 并将其设置为维护模式
- 请勿在 PowerShell 命令中包含参数 `-OS`

## 重置身份信息

要重置身份信息，请执行以下操作：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 重置身份信息。



- 要仅重置计算机密码和信任密钥，请按以下顺序运行以下命令：

```
1 Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
   PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
   $password -Target IdentityInfo
2 <!--NeedCopy-->
```

该命令中使用的参数的说明如下：

- **IdentityAccountName**：必须修复的身份帐户的名称。
- **PrivilegedUserName**：对身份提供商（AD 或 Azure AD）具有写入权限的用户帐户。
- **PrivilegedUserPassword**：PrivilegedUserName 的密码。
- **Target**：修复操作的目标。可以是 IdentityInfo 来修复帐户密码/信任密钥，也可以是用户证书来修复加入混合 Azure AD 的计算机身份的用户证书属性。

```
1 Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name>
   > -Identity -ResetIdentityInfo
2 <!--NeedCopy-->
```

**ResetIdentityInfo** 参数重置以下内容：

- 密码和信任密钥：如果 VM 加入了 AD 域（仅适用于 Citrix DaaS）
- 仅限信任密钥：如果 VM 未加入 AD 域（仅适用于 Citrix DaaS）
- 仅限密码：如果 VM 加入了 AD 域（仅适用于 Citrix Virtual Apps and Desktops）

- 要重置身份磁盘的所有配置，请按以下顺序运行以下命令：

```
1 Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
   PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
   $password -Target IdentityInfo
2 <!--NeedCopy-->
```

```
1 Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>
   -Identity
2 <!--NeedCopy-->
```

4. 键入 **y** 确认操作。也可以使用 **-Force** 参数跳过确认提示。例如：

```
1 Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name> -
   Identity -Force
2 <!--NeedCopy-->
```

5. 运行 **Get-ProvVM -ProvisioningSchemeName <name> -VMName <name>** 以检查更新后的身份磁盘设置。必须更新身份磁盘的属性（例如 **IdentityDiskId**）。**StorageId** 和 **IdentityDiskIndex** 不得更改。

## 更改现有计算机目录的网络设置

您可以更改现有计算机目录的网络设置，以便在新的子网上创建新的虚拟机。使用 `Set-ProvScheme` 命令中的 `-NetworkMapping` 参数更改网络设置。

要更改现有预配方案的网络设置，请执行以下操作：

1. 在 PowerShell 窗口中，运行命令 `asnp citrix*` 以加载 PowerShell 模块。
2. 运行 `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` 以获取要更改的网络路径。
3. 为新的网络设置分配一个变量。例如：

```
1 $NewNetworkMap = @{
2   "0"= "XDHYP:\HostingUnits\MyNetworks\Network 0.network" }
3
4 <!--NeedCopy-->
```

4. 运行 `Set-ProvScheme -ProvisioningSchemeName "name"-NetworkMapping $NewNetworkMap`。
5. 运行 `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` 以验证现有预配方案的新网络设置。

## 管理计算机目录的版本

使用 `Set-ProvScheme` 命令更新 MCS 计算机目录时，当前配置将另存为版本。然后，您可以使用 PowerShell 命令管理计算机目录的各种版本。您可以：

- 查看计算机目录的版本列表
- 使用任意早期版本更新计算机目录
- 在该计算机目录的 VM 未使用某个版本时手动删除该版本
- 更改计算机目录保留的最大版本数量（默认值为 99）

版本包含计算机目录的以下信息：

- VMCpuCount
- VMMemoryMB
- CustomProperties
- ServiceOffering
- MachineProfile
- NetworkMapping
- 安全组

运行以下命令（以示例形式提供）来管理计算机目录的各种版本。

- 要查看计算机目录的各种版本的配置详细信息，请执行以下操作：

```
1 Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
2 <!--NeedCopy-->
```

- 要查看计算机目录的特定版本的配置详细信息，请执行以下操作：

```
1 Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -
  Version 2
2 <!--NeedCopy-->
```

- 要查看与计算机目录关联的版本总数，请执行以下操作：

““

(Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).Count

- 要使用任意早期版本更新计算机目录，请执行以下操作：

```
1 Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
2 <!--NeedCopy-->
```

- 要在该计算机目录的 VM 未使用某个版本时手动删除该版本，请执行以下操作：

```
1 Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -
  Version 3
2 <!--NeedCopy-->
```

- 设置计算机目录保留的最大版本数量（默认值为 99）。此设置适用于所有目录。例如，在这种情况下，所有 MCS 预配的目录最多保留 15 个版本。

```
1 Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions" -
  Value 15
2 <!--NeedCopy-->
```

如果版本数量达到最大版本数，则如果计算机目录中的任何 VM 正在使用较旧的版本，则无法创建新版本。在这种情况下，请执行以下操作之一：

- 增加计算机目录保留的最大版本数量的上限。
- 更新一些较旧的版本上的 VM，以便这些较旧的版本不再被任何 VM 引用，并且可以将其删除。

### 更改现有计算机目录的缓存配置

在启用了 MCSIO 的情况下创建非永久目录后，您可以使用 `Set-ProvScheme` 命令修改以下参数：

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

此功能当前适用于：

- GCP 和 Microsoft Azure 环境，以及
- 启用了 MCSIO 的非永久目录

## 要求

修改缓存配置的要求如下：

- 更新到 VDA 的最新版本（2308 或更高版本）。
- 为现有的计算机目录启用参数 `UseWriteBackCache`。使用 `New-ProvScheme` 创建启用了 `UseWriteBackCache` 的计算机目录。例如：

```
1 New-ProvScheme -ProvisioningSchemeName $CatalogName -
   HostingUnitUid $HostingUnitUid `
2 -IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `
3 -MasterImageVM $MasterImage `
4 -ServiceOffering $ServiceOffering `
5 -NetworkMap $NetworkMap `
6 -SecurityGroup $SecurityGroup `
7 -UseWriteBackCache -WriteBackCacheDiskSize 8
8 <!--NeedCopy-->
```

## 更改缓存配置

运行 `Set-ProvScheme` 命令。例如：

```
1 Set-ProvScheme -ProvisioningSchemeName $provScheme.
   ProvisioningSchemeName -WriteBackCacheDiskSize 8 -
   WriteBackCacheMemorySize 128
2 <!--NeedCopy-->
```

### 注意：

- `WriteBackCacheDiskSize` 的值必须大于零，因为至少需要 1 GB 的缓存磁盘存储空间。
- `WriteBackCacheMemorySize` 的值必须小于计算机目录内存大小。
- 这些更改仅影响更改后添加到目录中的新 VM。现有虚拟机不受这些更改的影响。

## 将基于非计算机配置文件的计算机目录转换为基于计算机配置文件的计算机目录

您可以使用虚拟机、模板规范（如果是 Azure）或启动模板（以 AWS 为例）作为计算机配置文件输入，将非基于计算机配置文件的计算机目录转换为基于计算机配置文件的计算机目录。添加到目录中的新 VM 从计算机配置文件中获取属性值。

**注意：**

基于计算机配置文件的现有计算机目录无法更改为非基于计算机配置文件的计算机目录。

为此，您需要：

1. 创建包含 VM 但不包含计算机配置文件的永久或非永久计算机目录。
2. 打开 **PowerShell** 窗口。
3. 运行 **Set-ProvScheme** 命令以将计算机配置文件中的属性值应用到添加到计算机目录中的新 VM。例如：

- 对于 Azure：

```
1 Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx  
  -MachineProfile XDHyp:\HostingUnits<HostingUnitName>\  
    machineprofile.folder<ResourceGroupName><TemplateSpecName>  
    <<VersionName>  
2 <!--NeedCopy-->
```

- 以 AWS 为例：

```
1 Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx  
  -MachineProfile "XDHyp:\HostingUnits<hosting-unit><launch-  
    template>.launchtemplate<launch-template-version>.  
    launchtemplateversion"  
2 <!--NeedCopy-->
```

### 检索与目录关联的警告和错误

可以获取历史错误和警告，以了解您的 MCS 计算机目录中的问题并修复这些问题。

使用 PowerShell 命令，您可以：

- 获取错误或警告列表
- 将警告状态从新更改为已确认
- 删除错误或警告

要运行 PowerShell 命令，请执行以下操作：

1. 打开 PowerShell 窗口。
2. 运行 **asnp citrix\*** 以加载 Citrix 特定的 PowerShell 模块。

要获取错误和警告列表，请执行以下操作：

运行 **Get-ProvOperationEvent** 命令。

- 不带参数：获取所有错误和警告
- 使用 **LinkedObjectType** 和 **LinkedObjectId** 参数：获取与特定预配方案关联的所有错误和警告

- 使用 `EventId` 参数：获取与此事件 ID 匹配的特定错误或警告
- 使用 `Filter` 参数：通过自定义过滤器获取错误或警告

要将错误或警告的状态从新更改为已确认，请执行以下操作：

运行 `Confirm-ProvOperationEvent` 命令。

- 使用 `EventId` 参数：设置与此事件 ID 匹配的特定错误或警告的状态。可以作为 `Get-ProvOperationEvent` 命令的输出获取特定错误或警告的 `EventId`
- 使用 `LinkedObjectType` 和 `LinkedObjectId` 参数：设置与特定预配方案关联的所有错误和警告的状态
- 使用 `All` 参数：将所有错误和警告的状态设置为已确认

要删除错误或警告，请执行以下操作：

运行 `Remove-ProvOperationEvent` 命令。

- 使用 `EventId` 参数：删除与此事件 ID 匹配的特定错误或警告。可以作为 `Get-ProvOperationEvent` 命令的输出获取特定错误或警告的 `EventId`
- 使用 `LinkedObjectType` 和 `LinkedObjectId` 参数：删除与特定预配方案关联的所有错误和警告
- 使用 `All` 参数：删除所有错误和警告

有关详细信息，请参阅 [Citrix PowerShell SDK](#)。

## 删除没有虚拟机管理程序访问权限的计算机

删除虚拟机或配置方案时，MCS 需要从 VM 中移除标签，有时还需要从基础磁盘中移除标记，这样 MCS 就不会再跟踪或识别删除选项中包含的资源。但是，其中一些资源只能通过虚拟机管理程序访问。即使没有虚拟机管理程序访问权限，也可以使用 `Remove-ProvVM` PowerShell 中的 `PurgeDBOnly` 选项从数据库中删除 VM 资源对象，例如 VM、基础磁盘、ACG 中的映像等。

此选项在以下情况下启用：

- 所有支持的虚拟机管理程序
- 永久和非永久 VM

## 限制

不能同时使用 `-PurgeDBOnly` 和 `-ForgetVM` 命令。

## 使用 `PurgeDBOnly` 命令

在以下情况下，运行 PowerShell 命令 `Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -ForgetVM` 时，删除操作可能会失败：

- 主机连接处于维护模式
- 凭据无效
- 身份验证失败
- 未经授权的操作
- 无法访问虚拟机管理程序

注意：

Remove-provVM -ForgetVM 仅针对永久 VM。如果列表中的其中一个虚拟机是非永久 VM，则操作将失败。

如果由于无法访问虚拟机管理程序而导致操作失败，则会出现以下提示：

Try to use -PurgeDBOnly option to clean DDC database.

使用 Remove-ProvVM PowerShell 命令中的 -PurgeDBOnly 选项从 MCS 数据库中删除虚拟机的引用。例如，

```
Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -PurgeDBOnly
```

## 故障排除

- 对于状态为 [Power State Unknown](#) 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](#)。
- 如果 Cloud Connector 无法正常运行，MCS 配置操作（例如目录更新）需要比平时更长的时间，并且管理控制台性能会显著下降。

## 下一步的去向

有关管理特定虚拟机管理程序目录的信息，请参阅：

- [管理 AWS 目录](#)
- [管理 Google 云端平台目录](#)
- [管理 Microsoft Azure 目录](#)
- [管理 Microsoft System Center Virtual Machine Manager 目录](#)
- [管理 VMware 目录](#)
- [管理 XenServer 目录](#)

## 管理 **AWS** 目录

January 23, 2024

[管理计算机目录](#)介绍了用于管理计算机目录的向导。以下信息涵盖了特定于 AWS 云环境的详细信息。

注意：

在管理 AWS 目录之前，您需要完成创建 AWS 目录的过程。请参阅[创建 AWS 目录](#)。

## 移除标签

创建目录或 VM 时，会在以下资源上创建标记：

- 虚拟机
- 根磁盘容量
- 身份磁盘容量
- 弹性网络接口 (ENI)
- 根磁盘映像 (AMI)
- 启动模板
- AMI 或根磁盘的快照

您可以从 Citrix 数据库中移除虚拟机和计算机目录并删除 Citrix 创建的标签。可以使用以下图标：

- 带 `ForgetVM` 参数的 `Remove-ProvVM` 用于从单个虚拟机中删除 VM 和 Citrix 创建的标签，或从计算机目录中移除虚拟机列表。

注意：

使用 `ForgetVM` 参数，虚拟机将从 Citrix 的配置方案数据库中移除，但是，虚拟机将继续保留在虚拟机管理程序中。

- 使用 `ForgetVM` 参数的 `Remove-ProvScheme` 从 Citrix 数据库中删除计算机目录，从计算机目录中删除资源。

为此，您需要：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 在删除 VM 之前解锁 VM。例如：

```
1 Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id>"
2 <!--NeedCopy-->
```

4. 运行以下命令之一，从资源中移除虚拟机、计算机目录和 Citrix 创建的标签。

- 运行带 `ForgetVM` 的 `Remove-ProvVM` 可从 Citrix 数据库中移除 VM，从 VM 中移除 Citrix 创建的标签。例如：



```
1 Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>" -ForgetVM
2 <!--NeedCopy-->
```

- 运行 `Remove-ProvScheme` 以从 Citrix 数据库中删除计算机目录，并从计算机目录中删除资源。例如：

```
1 Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -ForgetVM
2 <!--NeedCopy-->
```

5. 确认虚拟机已从 Delivery Controller 中移除，但未从虚拟机管理程序中移除。

- a) 运行 `Get-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"`。这绝不能返回任何内容。
- b) 转至 AWS EC2 控制台。您必须看到虚拟机，但是，Citrix 创建的标签现已删除。Citrix 从以下资源中创建的标签已删除：
  - 虚拟机
  - 根磁盘容量
  - 身份磁盘容量
  - ENI

6. 如果您删除计算机目录，请确认该目录已从 Delivery Controller 中删除。

- a) 运行 `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`。这必须返回一个错误。
- b) 在 AWS EC2 控制台中确认以下资源已删除。
  - 根磁盘映像 (AMI)
  - 启动模板
  - AMI 或根磁盘的快照

识别 **MCS** 创建的资源

以下是 MCS 向 AWS 平台上的资源添加的标签。表中的标签表示方式为 “key” :” value”。

资源名称	标记
ID 磁盘	“Name” : “VMName_IdentityDisk” “XdConfig” : “XdProvisioned=true” “CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx”

资源名称	标记
映像	“XdConfig” : “XdProvisioned=true” “CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx”
ENI	“Description” : “XD Nic” “XdConfig” : “XdProvisioned=true” “CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx”
操作系统磁盘	“Name” : “VMName_rootDisk” “XdConfig” : “XdProvisioned=True” “CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx” [当 AwsCaptureInstanceProperties = true 时] “Citrix Resource” : “” [当 AwsCaptureInstanceProperties = true 并且 AwsOperationalResourcesTagging = true 时] “CitrixOperationalResource” : “”
PrepVM	“Name” : “Preparation - CatalogName - xxxxxxxxxxxxx” “XdConfig” : “XdProvisioned=true” “CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx” [当 AwsCaptureInstanceProperties = true 时] “Citrix Resource” : “” [当 AwsCaptureInstanceProperties = true 并且 AwsOperationalResourcesTagging = true 时] “CitrixOperationalResource” : “”
已发布的快照	“XdConfig” : “XdProvisioned=true” 如果不是 Volume Worker AMI 的快照，则为 “CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx”
模板	[当 AwsCaptureInstanceProperties = true 时] “XdConfig” : “XdProvisioned=true” [当 AwsCaptureInstanceProperties = true 时] “CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx”

资源名称	标记
目录中的 VM	<div>[当 AwsCaptureInstanceProperties = true 时] “CitrixResource” : “” [当 AwsCaptureInstanceProperties = true 并且 AwsOperationalResourcesTagging = true 时] “CitrixOperationalResource” : “” “XdConfig” : “XdProvisioned=true” “CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx” [当 AwsCaptureInstanceProperties = true 时] “CitrixResource” : “” [当 AwsCaptureInstanceProperties = true 时] “aws:ec2launchtemplate:id” :” lt-xxxx” [当 AwsCaptureInstanceProperties = true 时] “aws:ec2launchtemplate:version” : “n” [当 AwsCaptureInstanceProperties = true 并且 AwsOperationalResourcesTagging = true 时] “CitrixOperationalResource” : “” “XdConfig” : “XdProvisioned=true”</div>
卷工作线程 AMI	<div>“Name” : “XenDesktop Temp” “XdConfig” : “XdProvisioned=true” “CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx” [当 AwsCaptureInstanceProperties = true 并且 AwsOperationalResourcesTagging = true 时] “CitrixVolumeWorkerBootstrapper” : “”</div>
卷工作线程 bootstraper	<div>“Name” : “Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx” “XdConfig” : “XdProvisioned=true”</div>
卷工作线程实例	

更多信息

- [创建和管理连接和资源](#)
- [与 AWS 的连接](#)
- [创建计算机目录](#)
- [创建 AWS 目录](#)
- [管理计算机目录](#)

## 管理 Google 云端平台目录

February 9, 2024

[管理计算机目录](#)介绍了用于管理计算机目录的向导。以下信息涵盖了特定于 Google Cloud 环境的详细信息。

注意：

在管理 Google 云端平台目录之前，您需要完成创建 Google 云端平台目录。请参阅[创建 Google 云端平台目录](#)。

### 向目录中添加计算机

要将计算机添加到目录中，请执行以下步骤：

1. 在管理 > 完整配置中，选择左窗格中的计算机目录。
2. 选择要向其中添加计算机的计算机目录。
3. 在操作栏中选择添加计算机。
4. 在虚拟机页面上，指定要添加的计算机数量，然后选择下一步。
5. 在计算机标识页面上，选择一个 Active Directory 帐户，然后选择下一步。
6. 在域凭据页面上，选择输入凭据，键入用户名和密码，选择保存，然后选择下一步。
7. 在摘要页面上，确认信息，然后选择完成。

### 更新计算机

此功能在您想要更新主映像或最低功能级别的情况下非常有用。

要更新计算机，请按照以下步骤进行操作：

1. 在管理 > 完整配置中，选择左窗格中的计算机目录。
2. 选择包含要更新的计算机的计算机目录。
3. 在操作栏中选择“更改主映像”。
4. 在映像页面上，选择虚拟机和目录的最低功能级别，然后选择下一步。
5. 在前滚策略页面上，指定要更新计算机的时间，然后选择下一步。
6. 在摘要页面上，确认信息，然后选择完成。

### 回滚计算机更新

要回滚计算机更新，请按照以下步骤进行操作：

重要提示：

请勿重命名、删除或移动主映像。否则，您将无法回滚更新。

1. 在管理 > 完整配置中，选择左窗格中的计算机目录。
2. 选择包含要回滚计算机更新的计算机目录。
3. 在操作栏中选择“回滚主映像”。
4. 在概览页面上，确认信息，然后选择下一步。
5. 在前滚策略页面上，配置前滚策略，然后选择下一步。
6. 在摘要页面上，确认信息，然后选择完成。

## 电源管理

Citrix DaaS 允许您对 Google Cloud 计算机进行电源管理。使用导航窗格中的搜索节点查找要进行电源管理的计算机。以下电源操作可用：

- Delete
- 启动
- 重新启动
- 强制重新启动
- 关闭
- 强制关闭
- 添加到交付组
- 管理标记
- 打开维护模式

还可以使用 AutoScale 来管理 Google Cloud 计算机的电源。为此，请将 Google Cloud 计算机添加到交付组，然后为该交付组启用 AutoScale。有关 AutoScale 的详细信息，请参阅 [Autoscale](#)。

## 使用 PowerShell 更新已预配的计算机

`Set-ProvScheme` 命令更改了预配方案。但是，它不会影响现有计算机。您现在可以使用 PowerShell 命令 `Set-ProvVMUpdateTimeWindow` 将当前的预配方案应用到现有的永久性计算机或非永久性计算机或者一组计算机。目前，在 GCP 中，此功能支持的属性更新是计算机配置文件、服务产品和自定义目录设置。

可以更新以下对象：

- 单个 VM
- 与预配方案 ID 关联的特定 VM 或所有现有 VM 的列表
- 与预配方案名称关联的特定 VM 或所有现有 VM 的列表

要更新现有 VM，请执行以下操作：

1. 检查现有计算机的配置。例如，

```
1 Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
2 <!--NeedCopy-->
```

## 2. 更新预配方案。例如，

- 更新计算机配置文件

```
1 `Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
   MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
   machineprofileinstance.vm"
2 <!--NeedCopy-->
```

- 更新服务产品

```
1 Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
   ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
   serviceoffering.folder<service-offering>.serviceoffering"
2 <!--NeedCopy-->
```

## 3. 检查 VM 的当前属性是否与当前的预配方案相匹配，以及 VM 上是否有任何待处理的更新操作。例如，

```
1 Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
2 <!--NeedCopy-->
```

还可以查找具有特定版本的计算机。例如，

```
1 Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
   VMName, ProvisioningSchemeVersion
2 <!--NeedCopy-->
```

## 4. 更新现有计算机。

- 要更新所有现有计算机，请执行以下操作：

```
1 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
   -StartsNow -DurationInMinutes -1
2 <!--NeedCopy-->
```

- 要更新特定计算机的列表，请执行以下操作：

```
1 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
   -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
   -1
2 <!--NeedCopy-->
```

- 要根据 Get-ProvVM 的输出更新计算机，请执行以下操作：

```
1 Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
   ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
   -StartsNow -DurationInMinutes -1
```

```
2 <!--NeedCopy-->
```

注意：

- **StartsNow** 表示计划的开始时间为当前时间。
- **DurationInMinutes** 负数（例如-1）表示计划的时间范围没有上限。

5. 查找已安排更新的计算机。例如，

```
1 Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
   , ProvisioningSchemeUpdateAfter
2 <!--NeedCopy-->
```

6. 请重新启动计算机。下次启动时，属性更改将应用到现有计算机。可以使用以下命令检查更新后的状态：

```
1 Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
2 <!--NeedCopy-->
```

## 更改现有目录的磁盘相关自定义属性

可以更改现有目录和目录的现有 VM 的以下磁盘相关自定义属性：

- **PersistOSDisk**
- **PersistWBC**
- **StorageType**
- **IdentityDiskStorageType**
- **WbcDiskStorageType**

注意：

- **StorageType** 属性面向操作系统磁盘
- 只能为启用了回写式缓存的非永久性目录设置 **PersistOsDisk** 属性

即使在创建目录之后，此实施也能帮助您为不同的磁盘选择不同的存储类型，从而平衡与不同存储类型相关的定价。

要执行此操作，请使用 PowerShell 命令 **Set-ProvScheme** 和 **Set-ProvVMUpdateTimeWindow**：

1. 打开 **PowerShell** 窗口。
2. 运行 **asnp citrix\***。
3. 运行 **Get-ProvVM -VMName <VM name>** 以获取自定义属性。
4. 更改自定义属性字符串：
  - a) 将自定义属性复制到记事本并更改自定义属性。

- b) 在 **PowerShell** 窗口中, 粘贴记事本中修改过的自定义属性, 并为修改后的自定义属性分配一个变量。例如:

```
1 $cp = '<CustomProperties xmlns=http://schemas.citrix.com
2 /2014/xd/machinecreation xmlns:xsi="http://www.w3.org/2001/
3 XMLSchema-instance">
4 <Property xsi:type="StringProperty" Name="CatalogZones" Value
5 ="" />
6 <Property xsi:type="StringProperty" Name="PersistWBC" Value="
7 true" />
8 <Property xsi:type="StringProperty" Name="PersistOSDisk" Value
9 ="true" />
10 <Property xsi:type="StringProperty" Name="WBCDiskStorageType"
11 Value="pd-standard" />
12 <Property xsi:type="StringProperty" Name="StorageType" Value="
13 pd-standard" />
14 </CustomProperties>'
15 <!--NeedCopy-->
```

5. 更新现有目录。例如:

```
1 Set-ProvScheme -ProvisioningSchemeName <yourCatalogName> -
2 CustomProperties $cp
3 <!--NeedCopy-->
```

6. 更新现有 VM: 例如:

```
1 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
2 VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
3 <!--NeedCopy-->
```

7. 重新启动 VM。下次启动时, 自定义属性更改将应用到现有 VM。

## 防止意外删除计算机

借助 Citrix DaaS, 您可以保护 Google Cloud 上的 MCS 资源, 以防止意外删除。请通过将 `deletionProtection` 标志设置为 `TRUE` 来配置已预配的 VM。

默认情况下, 通过 MCS 或 Google Cloud 插件预配的 VM 是在启用了 `InstanceProtection` 的情况下创建的。该实现既适用于持久性目录, 也适用于非持久性目录。从模板重新创建实例时, 将更新非持久性目录。对于现有的持久性计算机, 您可以在 Google Cloud 控制台中设置标志。有关设置标志的详细信息, 请参阅 [Google 文档站点](#)。添加到持久性目录的新计算机在创建时已启用 `deletionProtection`。

如果您尝试删除已设置 `deletionProtection` 标志的 VM 实例, 请求将失败。但是, 如果您被授予了权限 `compute.instances.setDeletionProtection` 或分配了 IAM 计算管理员角色, 则可以重置该标志以允许删除资源。



识别 **MCS** 创建的资源

下面是 MCS 向 GCP 平台上的资源添加的标签。表中的标签表示方式为 “key” :” value”。

资源名称	标记
ID 磁盘	“CitrixResource” : “internal”  “CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx”
映像	“CitrixResource” : “internal”  “CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx”
操作系统磁盘	“CitrixResource” : “internal”  “CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx”
准备 VM	“CitrixResource” : “internal”  “CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx”
已发布的快照	“CitrixResource” : “internal”
存储桶	“CitrixResource” : “internal”
模板	“CitrixResource” : “internal”  “CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx”
目录中的 VM	“CitrixResource” : “internal”  “CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx” 。该插件还为 MCS 预配的 VM 添加了以下标签:” citrix-provisioning-scheme-id” : “provSchemeld”。您可以在 GCP 控制台中使用此标签按目录进行筛选。
WBC 磁盘	“CitrixResource” : “internal”  CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx”

注意：

如果添加了 **CitrixResource** 标记以将某个 VM 标识为 MCS 创建的资源，该 VM 在 Citrix 清单中将不可见。您可以删除或重命名该标记以使其可见。

## 更多信息

- [创建和管理连接和资源](#)
- [与 Google Cloud 环境的连接](#)
- [创建计算机目录](#)
- [创建 Google 云端平台目录](#)
- [管理计算机目录](#)

## 管理 **HPE Moonshot** 目录（预览版）

January 23, 2024

[管理计算机目录](#)介绍了用于管理计算机目录的向导。以下信息涵盖了特定于 HPE Moonshot 目录的详细信息。

### 注意：

在管理 HPE Moonshot 目录之前，您需要完成 HPE Moonshot 目录的创建。请参阅[创建 HPE Moonshot 计算机目录（预览版）](#)。

## 电源管理

Citrix DaaS 允许您对 HPE Moonshot 计算机进行电源管理。使用导航窗格中的搜索节点查找要进行电源管理的计算机。以下电源操作可用：

- 启动
- 关闭
- 强制关闭
- 重新启动
- 重置

### 注意：

不支持暂停和恢复电源操作。

## 更多信息

- [创建和管理连接和资源](#)
- [连接到 HPE Moonshot](#)
- [创建计算机目录](#)
- [创建 HPE Moonshot 计算机目录](#)
- [管理计算机目录](#)

## 管理 Microsoft Azure 目录

January 23, 2024

[管理计算机目录](#)介绍了用于管理计算机目录的向导。以下信息涵盖了特定于 Microsoft Azure Resource Manager 云环境的详细信息。

### 注意：

在管理 Microsoft Azure 目录之前，您需要完成创建 Microsoft Azure 目录。请参阅[创建 Microsoft Azure 目录](#)。

### 关闭 VM 时将存储类型更改为较低的层

关闭 VM 时，您可以通过将托管磁盘的存储类型切换到较低的层来节省存储成本。为此，请使用 `StorageTypeAtShutdown` 自定义属性。

关闭 VM 时，磁盘的存储类型更改为较低层（如 `StorageTypeAtShutdown` 自定义属性中所指定）。打开 VM 的电源后，存储类型将更改回原始类型（如 `StorageType` 自定义属性或 `WBCDiskStorageType` 自定义属性中所指定）。

### 重要：

- 在 VM 至少开机一次之前，磁盘不存在。因此，您无法在首次打开 VM 电源时更改存储类型。
- 将存储类型更改为较低层后，虚拟机可能需要更长的时间才能启动。

### 要求

- 适用于托管磁盘。这意味着您将自定义属性 `UseManagedDisks` 设置为 `true`。
- 适用于具有永久操作系统磁盘的永久和非永久目录。这意味着您将自定义属性 `persistOsDisk` 设置为 `true`。
- 适用于具有永久 WBC 磁盘的非永久目录。这意味着您将自定义属性 `persistWBC` 设置为 `true`。

### 限制

- 根据 Microsoft 的说法，您每天只能更改两次磁盘类型。请参阅 [Microsoft 文档](#)。根据 Citrix 的说法，每当 VM 执行“启动”或“取消分配”操作时，就会进行 `StorageType` 更新。因此，请将每个 VM 的电源操作次数限制为每天两次。例如，早上执行一次电源操作以启动 VM，晚上执行一次电源操作以取消分配 VM。

### 将存储类型更改为较低的存储层

在继续执行这些步骤之前，请参阅要求和限制。

1. 添加自定义属性 `StorageTypeAtShutdown`，将值设置为 `Standard_LRS (HDD)`，然后使用 `New-ProvScheme` 创建目录。有关使用 PowerShell 创建目录的信息，请参阅 <https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>。

注意：

如果 `StorageTypeAtShutdown` 除空值或 `Standard_LRS (HDD)` 之外还有其他任何值，操作将失败。

创建永久目录时设置自定义属性的示例：

```
1 $customProperties='<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
2 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
3 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
4   true" />
5 <Property xsi:type="StringProperty" Name="StorageType" Value="
6   Premium_LRS " />
7 <Property xsi:type="StringProperty" Name="ResourceGroups" Value=""
8   />
9 <Property xsi:type="StringProperty" Name="LicenseType" Value="
10  Windows_Client" />
11 <Property xsi:type="StringProperty" Name="SchemaVersion" Value="2"
12   />
13 <Property xsi:type="StringProperty" Name="OsType" Value="Windows"
14   />
15 <Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
16   Value="Standard_LRS" />
17 </CustomProperties>'
18 <!--NeedCopy-->
```

创建非永久目录时设置自定义属性的示例：

```
1 $customProperties='<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
2 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
3 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
4   true" />
5 <Property xsi:type="StringProperty" Name="StorageType" Value="
6   Premium_LRS" />
7 <Property xsi:type="StringProperty" Name="WbcDiskStorageType"
8   Value="Standard_SSD_LRS" />
9 <Property xsi:type="StringProperty" Name="ResourceGroups" Value=""
10  />
11 <Property xsi:type="StringProperty" Name="LicenseType" Value="
12  Windows_Client" />
13 <Property xsi:type="StringProperty" Name="SchemaVersion" Value="2"
14   />
15 <Property xsi:type="StringProperty" Name="OsType" Value="Windows"
16   />
17 <Property xsi:type="BooleanProperty" Name="persistWBC" Value=true
18   />
```

```

11 <Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=
    true />
12 <Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
    Value="Standard_LRS" />
13 </CustomProperties>'
14 <!--NeedCopy-->

```

注意：

使用计算机配置文件时，自定义属性优先于在 **MachineProfile** 中定义的属性。

2. 关闭 VM 并在 Azure 门户中检查 VM 的存储类型。磁盘的存储类型更改为较低的层，如 **StorageTypeAtShutdown** 自定义属性中所指定。
3. 打开 VM。磁盘的存储类型切换回下面提及的存储类型：
  - 操作系统磁盘的 **StorageType** 自定义属性
  - 仅当您在 **CustomProperties** 中指定了 WBC 磁盘的 **WBCDiskStorageType** 自定义属性时。否则，它会切换回 **StorageType** 中提到的存储类型。

将 **StorageTypeAtShutdown** 应用到现有目录

在继续执行这些步骤之前，请参阅要求和限制。

使用 **Set-ProvScheme** 将 **StorageTypeAtShutdown** 应用到添加到现有目录中的新 VM。

将 VM 添加到现有目录时设置自定义属性的示例：

```

1 $customProperties='<CustomProperties xmlns="http://schemas.citrix.com
    /2014/xd/machinecreation"
2 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
3 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
4 <Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS" />
5 <Property xsi:type="StringProperty" Name="WbcDiskStorageType" Value="
    Standard_SSD_LRS" />
6 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
7 <Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
8 <Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
9 <Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
10 <Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />
11 <Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />
12 <Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value
    ="Standard_LRS" />
13 </CustomProperties>'
14
15 $ProvScheme = Get-ProvScheme -ProvisioningSchemeName $CatalogName
16

```

```
17 Set-ProvScheme -ProvisioningSchemeName $ProvScheme.  
    ProvisioningSchemeName -CustomProperties $customProperties  
18 <!--NeedCopy-->
```

关闭时将现有 **VM** 的存储类型更改为较低的层级

在继续执行这些步骤之前，请参阅要求和限制。

当 VM 关闭时，您可以通过将现有 VM 的存储类型更改为较低的层级来节省存储成本。

要在 VM 关闭时将目录中的现有计算机的存储类型更改为较低的层级，请执行以下操作：

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 运行 `Get-Provscheme -ProvisioningSchemeName $CatalogName`。
4. 更改自定义属性字符串。

```
1 $customProperties = '<CustomProperties xmlns="http://schemas.  
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.  
    org/2001/XMLSchema-instance">  
2 <Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"  
    Value="Standard_LRS" />  
3 </CustomProperties>'  
4 <!--NeedCopy-->
```

5. 更新现有目录的预配方案。该更新适用于运行 `Set-ProvScheme` 后添加的新 VM。

```
1 Set-ProvScheme -ProvisioningSchemeName $CatalogName -  
    CustomProperties $customProperties  
2 <!--NeedCopy-->
```

6. 更新现有 VM 以启用 `StorageTypeAtShutdown`。

```
1 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -  
    StartsNow -DurationInMinutes -1  
2 <!--NeedCopy-->
```

7. 下次打开计算机电源时，计算机的 `StorageTypeAtShutdown` 属性会更新。存储类型在下次关闭时发生变化。
8. 运行以下命令查看目录中每个 VM 的 `StorageTypeAtShutdown` 值。

```
1 Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach {  
2     $vmName = $_.VMName; $storageTypeAtShutdown = ($_.CustomVmData  
    | ConvertFrom-Json).StorageTypeAtShutdown.  
    DiskStorageAccountType; return New-Object psobject -Property  
    @{  
3     "VMName" = $vmName; "StorageTypeAtShutdown" =  
        $storageTypeAtShutdown }  
}
```

```
4     }  
5  
6 <!--NeedCopy-->
```

将预配的计算机更新为当前预配方案状态

`Set-ProvScheme` 命令更改了预配方案。但是，它不会影响现有计算机。可以使用 PowerShell 命令 `Set-ProvVMUpdateTimeWindow` 将当前的预配方案应用到现有的永久性计算机或非永久性计算机或者一组计算机。您还可以为现有 MCS 已配置计算机的配置更新安排一个时段。在安排的时段内打开电源或重新启动都会对计算机应用安排的预配方案更新。目前，在 Azure 中，您可以更新 `ServiceOffering`、`MachineProfile` 和以下自定义属性：

- `StorageType`
- `WBCEDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

注意：

- 在 Azure 环境中，只能使用托管磁盘更新目录的 `StorageType`、`WBCEDiskStorageType` 和 `IdentityDiskStorageType` 自定义属性。
- 如果您运行 `Set-ProvVMUpdateTimeWindow` 两次，最新的命令将生效。

可以更新以下对象：

- 单个 VM
- 与预配方案 ID 关联的特定 VM 或所有现有 VM 的列表
- 与预配方案名称（计算机目录名称）关联的特定 VM 或所有现有 VM 的列表

对预配方案做以下更改后，将在 Azure 中为永久目录重新创建 VM 实例：

- 更改 `MachineProfile`
- 删除 `LicenseType`
- 删除 `DedicatedHostGroupId`

注意：

现有计算机的操作系统磁盘及其所有数据保持原样，新的 VM 已连接到该磁盘。

在更新现有 VM 之前：

1. 检查现有计算机的配置。例如，

```
1 Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
2 <!--NeedCopy-->
```

2. 更新预配方案。例如，

- 使用 VM 作为计算机配置文件输入：

```
1 Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
   MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
   machineprofile.folder<resource-group>.resourcegroup<
   virtual-machine>.vm"
2 <!--NeedCopy-->
```

- 使用模板规范作为计算机配置文件输入：

```
1 Set-ProvScheme -ProvisioningSchemeName "my-catalog"
2 -MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
   machineprofile.folder<resource-group>.resourcegroup<
   template-spec>.templatespec<template-spec-version>.
   templatespecversion"
3 -ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
   serviceoffering.folder<service-offering>.serviceoffering"
4 <!--NeedCopy-->
```

- 仅提供服务：

```
1 Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
   ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
   serviceoffering.folder<service-offering>.serviceoffering"
2 <!--NeedCopy-->
```

3. 检查 VM 的当前属性是否与当前的预配方案相匹配，以及 VM 上是否有任何待处理的更新操作。例如，

```
1 Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
2 <!--NeedCopy-->
```

还可以查找具有特定版本的计算机。例如，

```
1 Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
   VMName, ProvisioningSchemeVersion
2 <!--NeedCopy-->
```

要请求在下次重新启动时应用现有计算机的更新，请执行以下操作：

1. 运行以下命令以更新现有计算机并在下次重新启动时应用更新。

- 更新所有现有计算机。例如，



```

1 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
  -StartsNow -DurationInMinutes -1
2 <!--NeedCopy-->

```

- 更新特定计算机的列表。例如，

```

1 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
  -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
  -1
2 <!--NeedCopy-->

```

- 根据 Get-ProvVM 的输出更新计算机。例如，

```

1 Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
  ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
  -StartsNow -DurationInMinutes -1
2 <!--NeedCopy-->

```

注意：

- StartsNow** 表示计划的开始时间为当前时间。
- 使用负数（例如-1）的 **DurationInMinutes** 表示计划的时间范围没有上限。

- 查找已安排更新的计算机。例如，

```

1 Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
  , ProvisioningSchemeUpdateAfter
2 <!--NeedCopy-->

```

- 请重新启动计算机。下次启动时，属性更改将应用到现有计算机。可以使用以下命令检查更新后的状态。例如，

```

1 Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
  ProvisioningSchemeVersion
2 <!--NeedCopy-->

```

要安排 VM 下次在计划的时间范围内启动时更新到最新的预配设置，请执行以下操作：

- 运行以下命令：

- 要安排以开始时间作为当前时间的更新，请执行以下操作：

```

1 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
  -VMName vm1 -StartsNow -DurationInMinutes 120
2 <!--NeedCopy-->

```

- 要安排在周末更新，请执行以下操作：

```

1 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName " my-
  catalog " -VMName "vm1" -StartTimeInUTC "10/15/2022
  9:00am" -DurationInMinutes (New - TimeSpan - Days 2).
  TotalMinutes

```

```
2 <!--NeedCopy-->
```

注意：

- **VMName** 是可选的。如果未指定，则安排对整个目录进行更新。
- 使用 **StartsNow** 代替 **StartTimeInUTC** 来表示计划开始时间为当前时间。
- **DurationInMinutes** 是可选的。默认值为 120 分钟。负数（例如 -1）表示计划的时间范围没有上限。

## 2. 检查更新状态。

```
1 Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
2 <!--NeedCopy-->
```

## 3. 打开 VM 的电源。如果您在安排的时段之后打开计算机电源，则不会应用配置更新。如果您在安排的时段内打开计算机电源，

- 如果计算机已关闭电源，并且
  - 您未打开计算机电源，未应用配置更新
  - 您打开了计算机电源，应用了配置更新
- 如果计算机已开机，并且
  - 您未重新启动计算机，未应用配置更新
  - 您重新启动了计算机，应用了配置更新

要取消配置更新，请执行以下操作：

也可以取消单个 VM、多个 VM 或整个目录的配置更新。要取消配置更新，请执行以下操作：

## 1. 运行 **Clear-ProvVMUpdateTimeWindow**。例如：

- 要取消为单个 VM 安排的配置更新，请执行以下操作：

```
1 Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-
   catalog" -VMName "vm1"
2 <!--NeedCopy-->
```

- 要取消为多个 VM 安排的配置更新，请执行以下操作：

```
1 Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-
   catalog" -VMName "vm1","vm2"
2 <!--NeedCopy-->
```

注意：

VM 必须来自同一个目录。

## 更新各个 VM 的属性

您可以使用 PowerShell 命令 `Set-ProvVM` 更新永久性 MCS 计算机目录中各个 VM 的属性。但是，更新不会立即应用。要应用更新，必须使用 PowerShell 命令 `Set-ProvVMUpdateTimeWindow` 设置时间范围。

此实现可以帮助您高效地管理各个 VM，而无需更新整个计算机目录。目前，此功能仅适用于 Azure 环境。

当前，您可以更新的属性包括：

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

通过此功能，您可以：

- 更新 VM 的属性
- 在更新计算机目录后，保留在 VM 上更新的属性
- 还原应用于 VM 的配置更新

在更新 VM 的属性之前，请执行以下操作：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 检查现有计算机目录的配置。例如：

```
1 Get-ProvScheme -ProvisioningSchemeName AzureCatalog
2 <!--NeedCopy-->
```

4. 检查要对其应用更新的 VM 的配置。例如：

```
1 Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
2 <!--NeedCopy-->
```

## 更新 VM 的属性

请执行以下操作以更新 VM 的属性：

1. 关闭要对其应用更新的 VM。
2. 更新 VM 的属性。例如，如果要更新 VM 的存储类型 (`StorageType`) 自定义属性，请运行以下命令：

```
1 Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
  CustomProperties "...<Property Name='StorageType' Value='
  Premium_LRS' />..."
2 <!--NeedCopy-->
```

您可以同时更新计算机目录中两个 VM 的属性。例如：

```
1 Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
  CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
2 <!--NeedCopy-->
```

```
1 Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2 -
  CustomProperties "...<Property Name='StorageType' Value='
    StandardSSD_LRS' />..."
2 <!--NeedCopy-->
```

注意：

更新不会立即应用。

3. 获取指定要更新的属性的列表以及配置版本。例如：

```
1 Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -
  VMName machine1
2 <!--NeedCopy-->
```

检查 `Version` 的属性值以及要更新的属性（在此例中为 `StorageType`）。

4. 检查配置版本。例如：

```
1 Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
2 <!--NeedCopy-->
```

检查 `ProvVMConfigurationVersion` 的属性值。此更新尚未应用。VM 仍采用旧配置。

5. 请求计划的更新。例如：

```
1 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
  StartsNow -DurationInMinutes -1
2 <!--NeedCopy-->
```

有关计划的更新的详细信息，请参阅[将预配的计算机更新为当前预配方案状态](#)。

注意：

还将应用任何挂起的预配方案更新。

6. 重新启动 VM。例如：

```
1 New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
2 <!--NeedCopy-->
```

7. 检查配置版本。例如：

```
1 Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
2 <!--NeedCopy-->
```

检查 `ProvVMConfigurationVersion` 的属性值。更新现已应用。VM 现在采用新配置。

8. 要对 VM 进一步应用配置更新，请关闭 VM 并重复执行这些步骤。

在更新计算机目录后，保留在 **VM** 上更新的属性

请执行以下操作以保留在 VM 上更新的属性：

1. 关闭要对其应用更新的 VM。
2. 更新计算机目录。例如，如果要更改 VM 大小 (*ServiceOffering*) 和存储类型 (*StorageType*)，请运行以下命令：

```
1 Set-ProvScheme -ProvisioningSchemeName AzureCatalog -
  ServiceOffering Standard_E4_v3 -CustomProperties "...<Property
  Name='StorageType' Value='StandardSSD_LRS' />..."
2 <!--NeedCopy-->
```

3. 获取计算机目录的配置详细信息。例如：

```
1 Get-ProvScheme -ProvisioningSchemeName AzureCatalog
2 <!--NeedCopy-->
```

*ProvisioningSchemeVersion* 现在以 1 为增量。VM 大小和存储类型也已更新。

4. 更新 VM 的属性。例如，向 VM 提供计算机配置文件。

```
1 Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
  MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
  machineprofile.folder<resource-group>.resourcegroup<template-
  spec>.templatespec<template-spec-version>.templatespecversion"
2 <!--NeedCopy-->
```

注意：

计算机配置文件输入包含标记并指定了不同的 VM 大小 (*ServiceOffering*)。

5. 获取将 VM 上的配置更新与计算机目录更新合并后 VM 将拥有的属性的列表。例如：

```
1 Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName
  AzureCatalog -VMName machine1
2 <!--NeedCopy-->
```

注意：

VM 上的任何更新都将覆盖在计算机目录上完成的更新。

6. 请求对 VM 进行计划的更新。例如：

```
1 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
  VMName machine1 -StartsNow -DurationInMinutes -1
2 <!--NeedCopy-->
```

7. 重新启动 VM。例如：

```
1 New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
2 <!--NeedCopy-->
```

VM 会保留更新后的 VM 大小，该大小派生自计算机配置文件。计算机配置文件中指定的标记值也会应用于 VM。但是，存储类型派生自最新的预配方案。

8. 获取 VM 的配置版本。例如：

```
1 Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
2 <!--NeedCopy-->
```

`ProvisioningSchemeVersion` 和 `ProvVMConfigurationVersion` 现在显示的是最新版本。

#### 还原应用于 **VM** 的配置更新

1. 对 VM 应用更新后，关闭 VM。
2. 请运行以下命令以删除应用于 VM 的更新。例如：

```
1 Set-ProvVM -RevertToProvSchemeConfiguration -
    ProvisioningSchemeName AzureCatalog -VMName machine1
2 <!--NeedCopy-->
```

3. 请求对 VM 进行计划的更新。例如：

```
1 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
2 <!--NeedCopy-->
```

4. 重新启动 VM。例如：

```
1 New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
2 <!--NeedCopy-->
```

5. 检查 VM 的配置版本。例如：

```
1 Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
2 <!--NeedCopy-->
```

`ProvVMConfigurationVersion` 值现在是计算机目录的配置版本。

#### 检索 **Azure VM**、快照、操作系统磁盘和库映像定义的信息

可以显示 Azure VM 的信息，包括操作系统磁盘和类型、快照和库映像定义。分配计算机目录时，将为主映像上的资源显示此信息。使用此功能可以查看和选择 Linux 或 Windows 映像。PowerShell 属性

`TemplateIsWindowsTemplate` 已添加到 `AdditionDatafield` 参数中。此字段包含 Azure 特定的信息：VM 类型、操作系统磁盘、库映像信息和操作系统类型信息。将 `TemplateIsWindowsTemplate` 设置为 **True** 表示操作系统类型为 Windows；将 `TemplateIsWindowsTemplate` 设置为 **False** 表示操作系统类型为 Linux。

提示：

`TemplateIsWindowsTemplate` PowerShell 属性显示的信息来自 Azure API。有时，此字段可能为空。例如，数据磁盘中的快照不包含 `TemplateIsWindowsTemplate` 字段，因为无法从快照中检索操作系统类型。

例如，使用 PowerShell 将 Windows 操作系统类型的 Azure VM `AdditionData` 参数设置为 **True**：

```
1 PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork\image.  
    folder\username-dev-testing-rg.resourcegroup\username-dev-tsvda.vm).  
    AdditionalData  
2 Key Value  
3 ServiceOfferingDescription Standard_B2ms  
4 HardDiskSizeGB 127  
5 ResourceGroupName FENGHUAJ-DEV-TESTING-RG  
6 ServiceOfferingMemory 8192  
7 ServiceOfferingCores 2  
8 TemplateIsWindowsTemplate True  
9 ServiceOfferingWithTemporaryDiskSizeInMb 16384  
10 SupportedMachineGenerations Gen1,Gen2  
11 <!--NeedCopy-->
```

检索 **Azure VM**、托管磁盘、快照、**Azure VHD** 和 **ARM** 模板的区域名称信息

您可以显示 Azure VM、托管磁盘、快照、Azure VHD 和 ARM 模板的区域名称信息。分配计算机目录后，将为主映像上的资源显示此信息。当您使用 `AdditionalData` 参数运行 PowerShell 命令时，名为的 PowerShell 属性 `RegionName` 会显示区域名称信息。

例如，使用以下 PowerShell 命令在 Azure 中获取 VM 信息。

```
1 PS C:\Windows\system32> (get-item XDHyp:\HostingUnits\myAzureNetwork\  
    image.folder\hu-dev-testing-rg.resourcegroup\hu-dev-tsvda.vm).  
    AdditionalData  
2 Key Value  
3 HardDiskSizeGB 127  
4 ResourceGroupName HU-DEV-TESTING-RG  
5 RegionName East US  
6 TemplateIsWindowsTemplate True  
7 LicenseType  
8 ServiceOfferingDescription Standard_B2ms  
9 ServiceOfferingMemory 8192  
10 ServiceOfferingCores 2  
11 SupportedMachineGenerations Gen1,Gen2  
12 ServiceOfferingWithTemporaryDiskSizeInMb 16384
```

```
13 SecurityType
14 SecureBootEnabled
15 VTpmEnabled
16 <!--NeedCopy-->
```

识别 **MCS** 创建的资源

以下是 MCS 向 Azure 平台上的资源添加的标签。表中的标签表示方式为 “key” :” value”。

资源名称	标记
ID 磁盘	“CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx” “CitrixResource” : “Internal”
映像	“CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx” “CitrixResource” : “Internal”
NIC	“CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx” “CitrixResource” : “Internal”
操作系统磁盘	“CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx” “CitrixResource” : “Internal”
准备工作虚拟机	“CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx” “CitrixResource” : “Internal”
已发布的快照	“CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx” “CitrixResource” : “Internal”
资源组	“CitrixResource” : “Internal”  CitrixSchemaVersion: 2.0  “CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx”
存储帐户	“CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx” “CitrixResource” : “Internal”
目录中的 VM	“CitrixProvisioningSchemeld” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx”



资源名称	标记
WBC 磁盘	“CitrixResource” : “Internal” “CitrixProvisioningSchemeId” : “XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX” “CitrixResource” : “Internal”

注意：

如果添加了 **CitrixResource** 标记以将某个 VM 标识为 MCS 创建的资源，该 VM 在 Citrix 清单中将不可见。您可以删除或重命名该标记以使其可见。

移除标签

创建目录或 VM 时，会在以下资源上创建标记：

- 资源组
- 虚拟机
- 操作系统磁盘
- 身份磁盘
- 网络接口
- 存储帐户

您可以从 Citrix 数据库中删除虚拟机和计算机目录并移除标签。可以使用以下图标：

- 带 **ForgetVM** 参数的 **Remove-ProvVM** 从单个虚拟机或计算机目录中的虚拟机列表中删除虚拟机和标签。
- 带 **ForgetVM** 参数的 **Remove-ProvScheme** 从 Citrix 数据库中删除计算机目录和从整个计算机目录中删除标签。

此功能仅适用于永久性 VM。

为此，您需要：

1. 打开 **PowerShell** 窗口。
2. 运行 **asnp citrix\*** 以加载 Citrix 特定的 PowerShell 模块。
3. 运行 **Remove-ProvVM** 从 Citrix 数据库中删除虚拟机和从虚拟机中删除标签。

例如：

```
1 Remove-ProvVM -ProvisioningSchemeName "ProvisioningSchemeName" -
   VMName "vmname" -ForgetVM
2 <!--NeedCopy-->
```

4. 运行 **Remove-ProvScheme** 从 Citrix 数据库中删除计算机目录并从计算机目录中删除标签。例如：

```
1 Remove-ProvScheme -ProvisioningSchemeName "ProvisioningSchemeName" -ForgetVM
2 <!--NeedCopy-->
```

注意：  
在 `Remove-ProvScheme` 中使用 `ForgetVM` 参数后，如果自带资源组 (BYORG) 或 Citrix 托管资源组中存在配置方案，则 MCS 会删除包括基础磁盘快照在内的所有快照。

更多信息

- [创建和管理连接和资源](#)
- [与 Microsoft Azure 的连接](#)
- [创建计算机目录](#)
- [创建 Microsoft Azure 目录](#)
- [管理计算机目录](#)

管理 **Microsoft System Center Virtual Machine Manager** 目录

January 23, 2024

[管理计算机目录](#)介绍了用于管理计算机目录的向导。以下信息涵盖了特定于 Microsoft System Center Virtual Machine Manager (VMM) 虚拟化环境的详细信息。

注意：  
在管理 VMM 目录之前，您需要完成创建 VMM 目录。请参阅[创建 Microsoft System Center Virtual Machine Manager 目录](#)。

识别 **MCS** 创建的资源

下面是 MCS 向 SCVMM 平台上的资源添加的标签。表中的标签表示方式为 “key” :” value”。

资源名称	标记
准备 VM	标记字符串:” CitrixProvisioningSchemeld” : “XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX” 自定义属性条目:” XdConfig:” XdProvisioned=True”
目录中的 VM	标记字符串:” CitrixProvisioningSchemeld” : “XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX”

资源名称

标记

自定义属性条目:” XdConfig:” XdProvisioned=True”

更多信息

- [创建和管理连接和资源](#)
- [与 Microsoft System Center Virtual Machine Manager 的连接](#)
- [创建计算机目录](#)
- [创建 Microsoft System Center Virtual Machine Manager 目录](#)
- [管理计算机目录](#)

管理 VMware 目录

January 23, 2024

[管理计算机目录](#)介绍了用于管理计算机目录的向导。以下信息涵盖了特定于 VMware 虚拟化环境的详细信息。

注意：

在管理 VMware 目录之前，您需要完成创建 VMware 目录。请参阅[创建 VMware 目录](#)。

更新计算机目录的文件夹 ID

您可以通过在 `Set-ProvScheme` 命令的自定义属性中指定 `FolderId` 来更新 MCS 计算机目录的文件夹 ID。更新文件夹 ID 后创建的 VM 将在此新文件夹 ID 下创建。如果未在 `CustomProperties` 中指定此属性，则会在主映像所在的文件夹下创建 VM。

要更新计算机目录的文件夹 ID，请执行以下步骤。

1. 打开 Web 浏览器，然后输入 **vSphere Web Client** 的 URL。
2. 输入凭据，然后单击登录。
3. 在 **vSphere Web Client** 中创建用于放置 VM 的文件夹。
4. 打开 PowerShell 窗口。
5. 运行 **asnp citrix\*** 以加载 Citrix 特定的 PowerShell 模块。
6. 在 `Set-ProvScheme` 的 `CustomProperties` 中指定 `FolderID`。在此示例中，文件夹 ID 值为 `group-v2406`。

```

1 Set-ProvScheme -ProvisioningSchemeUid "50bb319c-2e83-4a37-9ea1-94
  f630687372" -CustomProperties "<CustomProperties xmlns=""http
  ://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi=""
  http://www.w3.org/2001/XMLSchema-instance"><Property xsi:type=
  ""StringProperty"" Name=""FolderId"" Value=""group-v2406"" /></
  CustomProperties>"
2 <!--NeedCopy-->

```

7. 使用 Studio 将 VM 添加到计算机目录。

8. 检查 vSphere Web Client 上是否有新 VM。新 VM 将在新文件夹下创建。

使用 **PowerShell** 命令查找文件夹 ID

使用 Powershell 命令 `Get-HypConfigurationDataForItem` 在 VMware 虚拟机管理程序中查找现有文件夹的文件夹 ID。

为 VMware 虚拟机管理程序创建主机连接和资源组。然后，执行以下步骤，在该虚拟机管理程序上查找某个文件夹的文件夹 ID。

1. 确定 vm 文件夹树根目录的 XDHyp 路径。例如：

```

1 XDHyp:\Connections\VMwareConn\Datacenter.datacenter
2 <!--NeedCopy-->

```

2. 使用 `Get-HypConfigurationDataForItem` 检索树结构。例如：

```

1 Get-HypConfigurationDataForItem -LiteralPath XDHyp:\Connections\
  VMwareConn\Datacenter.datacenter
2 <!--NeedCopy-->

```

3. 运行以下命令从输出 XML 中识别文件夹 ID。在此示例中，在 XML 输出中查找 `ExampleFolder` 的文件夹 ID。

```

1 $result = Get-HypConfigurationDataForItem -LiteralPath XDHyp:\
  Connections\VMwareConn\Datacenter.datacenter
2 $result.VmPlacementFolder
3 <!--NeedCopy-->

```

**XML 输出：**

```

1 <?xml version="1.0" encoding="utf-16"?>
2 <CtxVmPlacementFolder xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
3 <Name>vm</Name>
4 <Id>group-v4</Id>
5 <SubFolder>
6 <CtxVmPlacementFolder>
7 <Name>vCLS</Name>
8 <Id>group-v75</Id>

```

```
9      <SubFolder />
10    </CtxVmPlacementFolder>
11    <CtxVmPlacementFolder>
12      <Name>MyOtherFolder</Name>
13      <Id>group-v1110</Id>
14      <SubFolder />
15    </CtxVmPlacementFolder>
16    <CtxVmPlacementFolder>
17      <Name>ExampleFolder</Name>
18      <Id>group-v4658</Id>
19      <SubFolder />
20    </CtxVmPlacementFolder>
21  </SubFolder>
22 </CtxVmPlacementFolder>
23 <!--NeedCopy-->
```

在 **vSphere** 中查找文件夹 **ID**

访问任何 ESXi 或 vCenter 服务器系统中的 MOB 以查找 VM 的文件夹 ID。

托管对象浏览器 (MOB) 是一款基于 Web 的服务器应用程序，内置于所有 ESX/ESXi 和 vCenter 服务器系统中。此 vSphere 实用程序允许您查看有关 VM、数据存储和资源池等对象的详细信息。

- 1. 打开 Web 浏览器并输入 <http://x.x.x.x/mob>，其中 x.x.x.x 为 vCenter Server 或 ESX/ESXi 主机的 IP 地址。例如，<https://10.60.4.70/mob>。
- 2. 在 MOB 的主页上，单击属性 **content** 的值。
- 3. 单击 **rootFolder** 的值。
- 4. 单击 **childEntity** 的值。
- 5. 单击 **vmFolder** 的值。
- 6. 您可以在 **childEntity** 的值中找到文件夹 ID。

识别 **MCS** 创建的资源

下面是 MCS 向 VMware 平台上的资源添加的标签。表中的标签表示方式为 “key” :” value”。

资源名称	标记
准备 VM	“CitrixProvisioningSchemeld” : “XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX” “XdConfig:” XdProvisioned=True”
目录中的 VM	“CitrixProvisioningSchemeld” : “XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX” “XdConfig:” XdProvisioned=True”

更多信息

- [创建和管理连接和资源](#)
- [与 VMware 的连接](#)
- [创建计算机目录](#)
- [创建 VMware 目录](#)
- [管理计算机目录](#)

管理 **XenServer** 目录

January 23, 2024

[管理计算机目录](#)介绍了用于管理计算机目录的向导。以下信息涵盖特定于 XenServer 虚拟环境的详细信息。

注意：

在管理 XenServer 目录之前，需要完成 XenServer 目录的创建。请参阅[创建 XenServer 目录](#)。

识别 **MCS** 创建的资源

当 Machine Creation Services (MCS) 生成磁盘等资源时，它会分配一个 ProvisioningScheme ID 标签，以更好地利用这些资源。

标签对管理员很有帮助，因为他们可以更好地管理和组织资源。例如，如果对未使用的磁盘等资源进行了标记，则管理员可以轻松识别资源的创建位置，从而提高清理过程的效率。

以下是 MCS 在 XenServer 平台上向资源添加的标签。表中的标签表示方式为 “key” :” value”。

资源名称	标记
每个网络或本地存储上的磁盘副本（仅限本地）	“CitrixProvisioningSchemeld” : “XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX”
ID 磁盘	“CitrixProvisioningSchemeld” : “XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX”
操作系统磁盘	“CitrixProvisioningSchemeld” : “XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX”
准备 VM	“CitrixProvisioningSchemeld” : “XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX”
目录中的 VM	“CitrixProvisioningSchemeld” : “XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX”

资源名称

标记

WBC 磁盘

“CitrixProvisioningSchemeId” :  
“XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX”

检索有关配置方案的信息

要检索有关配置方案的详细信息，可以执行以下 PowerShell 命令。将 `XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX` 替换为实际的预配方案 ID：

1. 将占位符 ID 替换为您的实际预配方案 ID

```
1 $provisioningSchemeId = "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX"
2 <!--NeedCopy-->
```

2. 检索有关配置方案的详细信息：

```
1 Get-ProvisioningScheme -Id $provisioningSchemeId
2 <!--NeedCopy-->
```

检索 MCS 创建的资源列表

运行以下命令以获取 MCS 创建的完整资源列表。

1. 将占位符 ID 替换为您的实际配置方案 ID。

```
1 $provisioningSchemeId = "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX"
2 <!--NeedCopy-->
```

2. 检索 MCS 创建的完整资源列表。

```
1 Get-ProvResource -ProvisioningSchemeUid $provisioningSchemeId |
  ConvertTo-JSON -Depth 6
2 <!--NeedCopy-->
```

执行后，您会得到以下输出：

- 配置方案的名称和 ID。
- 配置方案中的配置映像版本列表。每个条目包括：
  - 映像名称和 ID。
  - 磁盘的磁盘 ID 和存储 ID。
- 配置虚拟机列表。每个条目包括：
  - 操作系统磁盘的操作系统磁盘 ID 和父磁盘 ID。
  - 操作系统磁盘的存储 ID。
  - 身份磁盘及其存储 ID。

## 更多信息

- [创建和管理连接和资源](#)
- [连接到 XenServer](#)
- [创建计算机目录](#)
- [创建 XenServer 目录](#)
- [管理计算机目录](#)

## 电源管理

December 6, 2023

借助 Citrix DaaS，您可以在各种支持的虚拟机管理程序和云服务上对由 MCS 配置的虚拟机进行强力管理。电源管理操作为您提供：

- 最佳用户体验
- 成本管理和节能

可用的电源操作有：

- 启动
- 关闭
- 重新启动
- 挂起
- 继续
- 强制重启
- 强制关闭

注意：

- 对于非永久性虚拟机，重启电源（关机/启动和重启）会导致操作系统磁盘被重置。
- 电源操作功能和行为因虚拟机管理程序或云服务而异。

本文介绍了与某些支持的虚拟机管理程序相关的关键电源管理功能。

- [对 AWS 虚拟机进行电源管理](#)
- [对 Azure 虚拟机进行电源管理](#)



## 对 **AWS VM** 进行电源管理

March 5, 2024

有关所需权限的信息，请参阅 [关于 AWS 权限](#)。

### 实例休眠

休眠过程存储实例的内存中状态及其专用 IP 地址和弹性 IP 地址，使其能够准确地从其离开的位置继续操作。

当一个实例被指示进入休眠状态时，它会将内存中状态写入到根 EBS 卷中的文件，然后自行关闭。Amazon EBS 卷是一种耐用的块级存储设备，您可以将其连接到自己的实例。将卷连接到实例后，您可以像使用物理硬盘驱动器一样使用。加密实例的根 EBS 卷。加密可确保将敏感数据从内存复制到 EBS 卷时得到适当的保护。有关 EBS 加密的信息，请参阅 [Amazon EBS encryption](#) (Amazon EBS 加密)。

下面是支持的实例休眠的限制：

- 仅支持最大 150 GB 的实例内存 (RAM)
- 不支持 UEFI 引导模式
- 通用 SSD 和预配的 IOPS SSD 仅作为 EBS 卷类型受支持。

下面是虚拟机管理程序级别的主机连接功能。

- 支持暂停的虚拟机管理程序：VMware、XenServer（前身为 Citrix Hypervisor）、Hyper-V 和 GCP
- 具有挂起功能的虚拟机管理程序：Nutanix、Azure 和 AWS

#### 注意：

- 所有挂起和休眠功能都称为挂起。
- 对于 AWS，计算机级别支持挂起功能，但在虚拟机管理程序级别不支持挂起功能。

### 创建支持休眠的 **VM**

要创建支持休眠的 VM，请执行以下操作：

1. 创建主机连接。请参阅 [与 AWS 的连接](#)。
2. 启动一个加密 EBS 根目录并启用 **Stop-Hibernate** 属性的实例。有关详细信息，请参阅：
  - [实例生命周期](#)
  - [Amazon EBS 加密](#)
  - [休眠先决条件](#)
  - [为实例启用休眠](#)
  - [休眠您的按需实例或竞价型实例](#)

3. 使用此实例作为主映像来创建 AMI。

4. 准备主映像：

- a) 在主映像上安装 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。有关如何安装 VDA 的详细信息，请参阅[安装 VDA](#)。
  - b) 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。
5. 从该实例创建 AMI。有关从实例创建 AMI 的信息，请参阅 [Create an AMI from an Amazon EC2 Instance](#) (从 Amazon EC2 实例创建 AMI)。
6. 使用 `New-ProvScheme` 命令创建计算机目录。将 `AwsCaptureInstanceProperties` 自定义属性设置为 **True**。有关在“完整配置”接口中启用 AWS 实例属性的信息，请参阅在“完整配置”界面中应用 AWS 实例属性和标记运行资源。

```
1 New-ProvScheme -AdminAddress "xxx" -CleanOnBoot
2 -CustomProperties "AwsCaptureInstanceProperties,true;"
3 -HostingUnitName "xxx" -IdentityPoolName $catalog_name -
  InitialBatchSizeHint 1
4 -MasterImageVM "xyz.template" -NetworkMapping @{
5   "0"="XDHyp:\HostingUnits\MyConn\us-east-2a.availabilityzone
     \10.0.0.0\`/24 (vpc-0f1771e45671aedcd).network" }
6
7 -ProvisioningSchemeName $catalog_name
8 -RunAsynchronously -Scope @() -SecurityGroup @("xxx") -
  ServiceOffering "xxx"
9 <!--NeedCopy-->
```

有关使用 PowerShell 命令创建计算机目录的信息，请参阅 <https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/>。

如果满足以下条件，则会创建可以休眠的 VM：

- 您可以选择从启用了 **Stop-Hibernate** 属性的主映像创建的 AMI。
- 主 VM 已加入域并且安装了 VDA。
- 请选择可以处理休眠的正确 VM 大小（服务产品）。

在以下情况下，**New-ProvScheme** 命令将失败并显示相应的错误消息：

- 主 VM 已启用休眠，但该服务产品无法处理休眠。
- 如果主 VM 未加入域且未安装 VDA。

服务产品和 **AMI** 的休眠状态

要获取服务产品和 AMI（模板）的休眠状态，请运行以下命令：

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b(ami-0e6c5b33a52d2a6b6).template'`

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

更新支持休眠的现有预配方案的服务产品

1. 运行 `Set-ProvScheme` 命令。例如，

```
1 Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering <String>
2 <!--NeedCopy-->
```

如果服务产品不兼容，系统会显示异常消息。

创建支持休眠的计算机目录

创建计算机目录时，您可以使用支持休眠的计算机配置文件。

1. 在目录创建向导中，按照说明进行操作，直到选择计算机配置文件。
2. 在 计算机模板 页面上，单击 选择计算机配置文件 并选择计算机配置文件。
3. 在“虚拟机”页面上，单击“编辑”图标并选择 VM。

注意：

如果计算机配置文件启用了休眠，则系统仅显示那些可以休眠的虚拟机。

4. 按照屏幕上的说明完成所有设置。摘要 页面显示目录的休眠状态。

注意：

在编辑计算机目录中，当您将计算机配置文件更改为启用休眠的配置文件时，系统会要求您相应地重新配置虚拟机。

更新支持休眠的计算机目录

如果您尝试使用不支持休眠的计算机目录更新现有计算机目录，更新将失败并显示相应的错误消息。

休眠的 **VM** 的电源管理

您可以在休眠的虚拟机上执行以下电源管理操作：

1. 将 VM 从运行状态中暂停。
2. 将 VM 从暂停状态恢复。
3. 从暂停状态重新启动 VM。

要查看电源管理选项，请在“管理” > “完整配置”界面中，右键单击休眠的虚拟机。

根据您在虚拟机上执行的电源操作，您还可以将每个 VM 的电源状态显示为“暂停”和“已暂停”。

## 对 Azure VM 进行电源管理

March 30, 2024

有关所需权限的信息，请参阅[所需的 Azure 权限](#)。

### Azure 按需预配

使用 Azure 按需置备时，只有在置备完成后，Citrix DaaS 启动开机操作时才会创建 VM。

使用 MCS 在 Azure Resource Manager 中创建计算机目录时，Azure 按需预配功能：

- 降低存储成本
- 加快目录创建过程

创建 MCS 目录时，Azure 门户会显示资源组中的网络安全组、网络接口、基础映像和身份磁盘。

直到 Citrix DaaS 为虚拟机启动开机操作后，Azure 门户才会显示虚拟机。然后，VM 在“完整配置”界面中的状态更改为“开”。有两种类型的计算机，它们有以下区别：

- 对于池计算机，仅当存在 VM 时才会有操作系统磁盘和写回缓存。在控制台中关闭池计算机时，该 VM 在 Azure 门户中不可见。如果您经常关闭计算机（例如，在工作时间以外），则可以节省大量的存储成本。
- 对于专用计算机，在首次打开 VM 时创建操作系统磁盘。Azure 门户中的 VM 将保留在存储中，直到计算机标识被删除。在控制台中关闭专用计算机时，该 VM 仍在 Azure 门户中可见。

#### 注意：

不推荐支持在按需配置功能（“旧版”目录）之前创建的 Azure 目录。因此，重新创建 Azure 旧版目录虚拟机。然后按需配置目录，从而节省存储成本。

### 重启电源时保留已置备的虚拟机

选择在重启电源时是否保留预配的虚拟机。使用 PowerShell 参数 `New-ProvScheme CustomProperties`。此参数支持额外的属性 `PersistVm`，用于确定重启电源后预配的虚拟机是否仍然存在。将 `PersistVm` 属性设置为 **true** 以在关闭电源时保留虚拟机，或者将属性设置为 **false** 以确保在关闭电源时不保留虚拟机。

#### 注意：

**PersistVm** 属性仅适用于启用了属性 **CleanOnBoot** 和 **UseWriteBackCache** 的预配方案。如果未为非持久虚拟机指定 **PersistVm** 属性，则它们将在关闭电源时从 Azure 环境中删除。

在以下示例中，**New-ProvScheme CustomProperties** 参数将 **PersistVm** 属性设置为 **true**：

```

1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
  instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
  />
3 <Property xsi:type="StringProperty" Name="StorageType" Value="
  Standard_LRS" />
4 <Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />
5 <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
  />
6 <Property xsi:type="StringProperty" Name="PersistVm" Value="true" />
7 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
  resourcegroup" />
8 <Property xsi:type="StringProperty" Name="LicenseType" Value="
  Windows_Client" />
9 </CustomProperties>
10 <!--NeedCopy-->

```

在以下示例中，**New-ProvScheme CustomProperties** 参数通过将 **PersistVM** 设置为 **true** 来保留回写式缓存：

```

1 New-ProvScheme
2 -AzureAdJoinType "None"
3 -CleanOnBoot
4 -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=`"
  StringProperty`" Name=`"StorageType`" Value=`"Standard_LRS`" /><
  Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"
  false`" /><Property xsi:type=`"StringProperty`" Name=`"
  PersistOsDisk`" Value=`"true`" /><Property xsi:type=`"
  StringProperty`" Name=`"PersistVm`" Value=`"true`" /><Property xsi:
  type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"demo-
  resourcegroup`" /><Property xsi:type=`"StringProperty`" Name=`"
  LicenseType`" Value=`"Windows_Client`" /></CustomProperties>"
5 -HostingUnitName "demo"
6 -IdentityPoolName "NonPersistent-MCSI0-PersistVM"
7 -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-test.
  resourcegroup\demo-snapshot.snapshot"
8 -NetworkMapping @ {
9 "0"="XDHyp:\HostingUnits\demo\virtualprivatecloud.folder\East US.
  region\virtualprivatecloud.folder\ji-test.resourcegroup\jitest-vnet
  .virtualprivatecloud\default.network" }
10
11 -ProvisioningSchemeName "NonPersistent-MCSI0-PersistVM"
12 -ServiceOffering "XDHyp:\HostingUnits\demo\serviceoffering.folder\
  Standard_B2ms.serviceoffering" -UseWriteBackCache

```

```

13 -WriteBackCacheDiskSize 127
14 -WriteBackCacheMemorySize 256
15 <!--NeedCopy-->

```

提示：

**PersistVm** 属性决定是否保留预配的虚拟机。**PersistOsdisk** 属性决定是否保留操作系统磁盘。要保留预配的虚拟机，请先保留操作系统磁盘。如果不先删除虚拟机，则无法删除操作系统磁盘。可以在不使用指定 **PersistVm** 参数的情况下使用 **PersistOsdisk** 属性。

### 自定义存储类型更改失败时的开机行为

开机时，由于 Azure 出现故障，托管磁盘的存储类型可能无法更改为所需类型。在这些情况下，VM 将保持关闭状态并向您发送故障消息。但是，您可以选择在存储无法还原到其配置的类型时打开 VM 的电源，也可以选择保持 VM 处于关闭状态。

- 如果您将自定义属性 **FailSafeStorageType** 配置为 **true** (默认设置) 或者未在 **New-ProvScheme** 或 **Set-ProvScheme** 命令中指定该属性：
  - 开机后，虚拟机使用错误的存储类型开机。
  - 关闭时，VM 保持关闭状态，但存储类型不正确。
- 如果您在 **New-ProvScheme** 或 **Set-ProvScheme** 命令中将自定义属性 **FailSafeStorageType** 配置为 **false**：
  - 开机后，虚拟机仍处于关闭状态，存储类型不正确。
  - 关闭时，VM 保持关闭状态，但存储类型不正确。

要创建包含 **FailSafeStorageType** 自定义属性的计算机目录，请执行以下操作：

1. 打开 PowerShell 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 创建标识池（如果尚未创建）。
4. 在 **New-ProvScheme** 中添加自定义属性。例如：

```

1 New-ProvScheme -HostingUnitName "Azure-Resources-1" -
  IdentityPoolName "name" -InitialBatchSizeHint 1
2 -MasterImageVM "XDHyp:\HostingUnits\Azure-Resources-1\image.folder
  \abc.resourcegroup\def.snapshot"
3 -NetworkMapping @{
4   "0"="XDHyp:\HostingUnits\Azure-Resources-1\ght.folder\abc.
  resourcegroup\abc-vnet.virtualprivatecloud\default.network" }
5
6 -ProvisioningSchemeName "name"
7 -ServiceOffering "XDHyp:\HostingUnits\Azure-Resources-1\
  serviceoffering.folder\Standard_DS2_v2.serviceoffering"

```

```

8 -CustomProperties "<CustomProperties xmlns="http://schemas.citrix
    .com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org
    /2001/XMLSchema-instance">
9 <Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS" />
10 <Property xsi:type="StringProperty" Name="StorageTypeAtShutdown
    " Value="Standard_LRS" />
11 <Property xsi:type="StringProperty" Name="FailSafeStorageType"
    Value="true" />
12 </CustomProperties>"
13 <!--NeedCopy-->

```

5. 然后, 创建计算机目录。有关如何使用 Remote PowerShell SDK 创建目录的信息, 请参阅 <https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>。

更新现有计算机目录以包含自定义属性 `FailSafeStorageType`。此更新不影响现有 VM。

1. 更新 `Set-ProvScheme` 命令中的自定义属性。例如:

```

1 Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "
2 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
3 <Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="IdentityDiskStorageType
    " Value="Premium_LRS" />
5 <Property xsi:type="StringProperty" Name="FailSafeStorageType"
    Value="false" />
6 </CustomProperties>"
7 <!--NeedCopy-->

```

要将在 `Set-ProvScheme` 中所做的更改应用到现有 VM, 请运行 `Request-ProvVMUpdate` 命令。

1. 运行 `Request-ProvVMUpdate` 命令。例如:

```

1 Request-ProvVMUpdate -ProvisioningSchemeName <String> -VMName <
    List-Of-Vm-Names>
2 <!--NeedCopy-->

```

2. 重新启动 VM。

## 创建具有休眠功能的 VM (预览版)

在 Azure 环境中, 您可以创建支持休眠的 MCS 计算机目录。使用此功能, 您可以挂起 VM, 然后在用户再次登录时重新连接到 VM 的先前状态。

休眠功能适用于以下对象:

- 单会话操作系统

- 永久和非永久 VM
- 静态和随机（池）VDI 桌面

无论 VDI 桌面是静态还是随机，都可以在 VM 休眠后恢复到同一个会话。

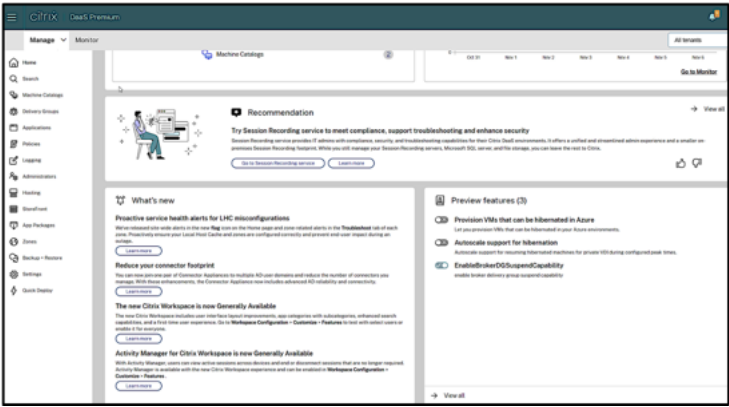
在本部分内容中，请参阅以下内容：

- [必备条件](#)
- [限制](#)
- [创建和管理具有休眠功能的计算机目录](#)
- [为现有的具有休眠功能的 VM 创建计算机目录](#)
- [在现有的 MCS 预配的 VM 上启用休眠](#)
- [检查休眠属性](#)
- [VM 的电源管理（手动和自动）](#)

使用休眠的必备条件

要使用休眠，请务必完成以下任务：

- 为您的 Azure 订阅启用该功能。请参阅[为您的订阅启用休眠功能](#)。
- 在 **DaaS > 主页 > 预览功能**中启用以下开关：
  - 配置可以在 **Azure** 中休眠的 **VM**
  - **AutoScale** 对休眠的支持



- 在适用于 Windows 和 Linux 的主映像上安装 Azure 虚拟机代理。Windows 映像的页面文件可以位于临时磁盘上。在计算机目录上启用了休眠时，MCS 会将页面文件位置设置为基础磁盘中的 C: 驱动器。
- MCS 自动为生成的资源设置休眠属性。您无需配置主资源的属性即可支持休眠。
- 在订阅中使用支持休眠的 VM 大小。
- 创建具有休眠功能的计算机配置文件（VM 或模板规范），以便 VM 继承休眠功能。要创建 VM，请参阅 [Getting started with hibernation](#)（开始休眠）。



注意：

根据 Microsoft 的说法，您可以从操作系统磁盘部署启用了休眠的 VM。目前，某些区域支持此功能，并将很快在所有区域推出。有关详细信息，请参见 [从操作系统磁盘部署启用休眠的虚拟机](#)。

要创建模板规范，请执行以下操作：

1. 打开 Azure 门户。选择要在模板中使用其配置的 VM。在左侧窗格中选择导出模板。
2. 清除 **Include parameters**（包括参数）复选框。复制上下文并将其另存为 JSON 文件，例如 `VMExportTemplate.json`。
3. 确保参数 `hibernationEnabled` 在模板上设置为 **true**。如果该参数未设置未 **true**，请检查您使用的 VM 配置。可以在模板文件中指定支持的 VM 大小。但是，也可以在创建目录时指定计算机大小。
4. 将网络接口资源的模板添加到 JSON 文件 `VMExportTemplate.json` 中。因此，您有一个包含两个资源的 ARM 模板文件。
5. 选择 **Azure Portal**（Azure 门户）> **Template specs**（模板规范）> **Import template**（导入模板）> **Choose local template file**（选择本地模板文件），将此模板文件作为 ARM 模板规范导入。
6. 创建 ARM 模板规范后，可以将其用作计算机配置文件。

注意：

同步到 Citrix Studio 可能需要几分钟时间。

有关详细信息，请参阅 Microsoft 文档 [Prerequisites to use hibernation](#)（使用休眠的必备条件）。

## 限制

- 仅支持单会话操作系统计算机目录（永久和非永久）。
- 临时操作系统磁盘和 MCS I/O 功能不支持 Azure 休眠。
- 在 Windows 自动更新过程中，休眠可能会失败。

有关详细信息，请参阅 [Microsoft 文档](#)。

## 创建和管理具有休眠功能的计算机目录

要创建支持休眠的虚拟机，您可以使用以下方法创建和管理支持休眠的计算机目录：

- 完整配置界面，或
- PowerShell 命令

### 使用完整配置界面创建目录

1. 登录 Citrix Cloud。在左上角的菜单中，选择我的服务 > **DaaS**。

2. 在管理 > 完整配置中，选择左窗格中的计算机目录。
3. 选择创建计算机目录。目录创建向导将打开。
4. 在计算机类型页面上，为此目录选择单会话操作系统计算机类型。
5. 在计算机管理页面上，请按如下所示选择设置：
  - a) 选择进行电源管理的计算机（例如，虚拟机或刀片式 **PC**）。
  - b) 选择 **Citrix Machine Creation Services (MCS)**。
6. 在桌面体验页面上，根据需要选择随机或静态桌面体验。
7. 在映像页面上，选择一个主映像。选中使用计算机配置文件复选框，然后选择支持休眠功能的计算机配置文件。单击工具提示以了解计算机配置文件是否支持休眠。
8. 在存储和许可证类型页面上，选择用于此目录的存储和许可证。
9. 在虚拟机页面上，选择 VM 数量、VM 大小和可用性区域。

注意：

显示支持休眠功能的计算机大小仅供您进行选择。

10. 在 **NIC** 页面上，添加您希望 VM 使用的 NIC。
11. 在磁盘设置页面上，选择回写式缓存磁盘的存储类型和大小。
12. 在资源组页面上，选择要预配 VM 的资源组。
13. 在计算机标识页面上，选择创建新的 **Active Directory** 帐户。然后，请指定帐户命名方案。
14. 在域凭据页面上，单击输入凭据。输入您的域凭据，以便在目标 Active Directory 域中执行帐户创建操作。
15. 在摘要页面上，输入计算机目录的名称，然后单击完成。

MCS 计算机目录创建完成后，在目录列表中找到该目录，然后单击模板属性选项卡。**Hibernation**（休眠）参数的值必须设置为 **Supported**（受支持）。

如果要编辑计算机目录，请注意以下限制：

- 如果当前计算机目录支持休眠，您将无法：
  - 将 VM 大小更改为不支持休眠功能的 VM 大小。
  - 将计算机配置文件更改为不支持休眠功能的配置文件。
- 如果当前的计算机目录不支持休眠，您将无法：
  - 目前，使用完整配置界面将计算机配置文件更改为支持休眠的配置文件。但是，您可以使用 PowerShell 命令来执行此操作。请参阅在现有的 MCS 预配的 VM 上启用休眠。

创建计算机目录来管理现有的具有休眠功能的 **VM** 如果您已经拥有具有休眠功能的 VM 并希望将其挂起并恢复，请创建计算机目录以导入这些 VM 进行电源管理。

注意：

可以创建包含具有休眠功能和不支持休眠功能的 VM 的计算机目录。但是，如果您想要与休眠相关的功能，则必须创建仅包含支持休眠的虚拟机的计算机目录。

要使用完整配置界面为支持休眠的现有虚拟机创建目录，请按照屏幕上的说明完成这些步骤并注意以下关键设置：

1. 在 计算机管理 页面上，选择 受电源管理的计算机，然后选择 其他服务或技术 作为部署计算机的方式。
2. 在虚拟机页面上，仅添加或导入具有休眠功能的 VM。

使用 **PowerShell** 命令创建计算机目录 满足使用休眠的所有要求后，您可以使用 `New-ProvScheme` 命令创建具有休眠功能的计算机目录。有关如何使用 Remote PowerShell SDK 创建目录的信息，请参阅 <https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>。

创建目录时，可以使用以下 PowerShell 命令检查 VM 大小和计算机配置文件是否支持休眠：

- 对于 VM 大小，请运行以下命令并检查属性 `supportsHibernation` 是否设置为 **True**。例如，

```
1 Get-ChildItem -AdminAddress "localhost:19097" -LiteralPath @"(
    XDHyp:\HostingUnits\ <VirtualNetwork> \serviceoffering.folder"
) | select Name, AdditionalData | ConvertTo-Json
2 <!--NeedCopy-->
```

- 对于计算机配置文件，请运行以下命令并检查属性 `supportsHibernation` 是否设置为 **True**。例如，

```
1 Get-ChildItem -AdminAddress "localhost:19097" -LiteralPath @"(
    XDHyp:\HostingUnits\ <VirtualNetwork> \machineprofile.folder\
    abc.resourcegroup") | select Name, AdditionalData | ConvertTo-Json
2 <!--NeedCopy-->
```

如果要编辑计算机目录，请注意以下限制：

- 如果当前计算机目录支持休眠，您将无法：
  - 将 VM 大小更改为不支持休眠功能的 VM 大小
  - 将计算机配置文件更改为不支持休眠功能的配置文件
- 如果当前的计算机目录不支持休眠，您将无法：
  - 目前，使用完整配置界面将计算机配置文件更改为支持休眠的配置文件。但是，您可以使用 PowerShell 命令来执行此操作。请参阅在现有的 MCS 预配的 VM 上启用休眠。

有关如何使用 Remote PowerShell SDK 修改目录的 VM 大小和计算机配置文件的信息，请参阅 <https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/>。

在现有的 **MCS** 预配的 **VM** 上启用休眠

可以在现有的以下设备上启用 Azure 休眠：

- 不使用临时磁盘创建的计算机目录的 Windows MCS 预配的 VM。
- 使用和不使用临时磁盘创建的计算机目录的 Linux MCS 预配的 VM。

注意：

- 现有的 MCS 预配的 VM 必须安装 Azure VM Agent。
- 当前，您只能使用 PowerShell 命令来启用此功能。

为此，您需要：

1. 打开 **PowerShell** 窗口。
2. 运行 `asnp citrix*` 以加载 Citrix 特定的 PowerShell 模块。
3. 检查现有计算机的配置。例如：

```
1 Get-ProvScheme | select ProvisioningSchemeName,  
   ProvisioningSchemeVersion  
2 <!--NeedCopy-->
```

4. 使用 `Set-ProvScheme` 命令在此计算机目录上启用休眠。例如：

```
1 Set-ProvScheme -provisioningSchemeName xxxx  
2 -machineprofile <path-to-machineprofile-with-hibernation-enabled>  
3 -serviceoffering "XDHyp:\HostingUnits\msc-dev\serviceoffering.  
   folder\Standard_D4as_v5.serviceoffering"  
4 <!--NeedCopy-->
```

5. 请求更新计算机目录中的现有 VM。

```
1 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeUid xxxx -VMName <  
   String[]  
2 <!--NeedCopy-->
```

6. 重新启动 VM 以触发现有 VM 上的更新。例如：

```
1 New-BrokerHostingPowerAction -machinename "<name>" -Action Restart  
2 <!--NeedCopy-->
```

## 检查休眠属性

可以使用 PowerShell 命令检查计算机目录、VM 和 Broker 计算机的休眠属性：

- 要检查预配方案的休眠属性，请运行以下 PowerShell 命令。`HibernationEnabled` 参数必须为 `True`。

```
1 (Get-ProvScheme -provisioningSchemeName <YourSchemeName>).  
   VMMetadata -join "" | ConvertFrom-Json | Select  
   HibernationEnabled  
2 <!--NeedCopy-->
```

- 要检查预配 VM 的休眠属性，请运行以下 PowerShell 命令。`SupportsHibernation` 参数必须为 `True`。

```
1 (Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json  
   | Select SupportsHibernation  
2 <!--NeedCopy-->
```

- 要检查 Broker 计算机的休眠容量，请运行以下 PowerShell 命令。挂起和恢复电源操作表示具有休眠功能。

```
1 (Get-BrokerMachine -MachineName <YourMachineName>).  
   SupportedPowerActions  
2 <!--NeedCopy-->
```

#### 具有休眠功能的 **VM** 的电源管理

可以在具有休眠功能的 VM 上执行以下电源管理操作：

- 将 VM 从运行状态挂起
- 将 VM 从挂起状态恢复
- 从已挂起状态强制关闭 VM
- 从已挂起状态强制重新启动 VM

有关详细信息，请参阅以下内容：

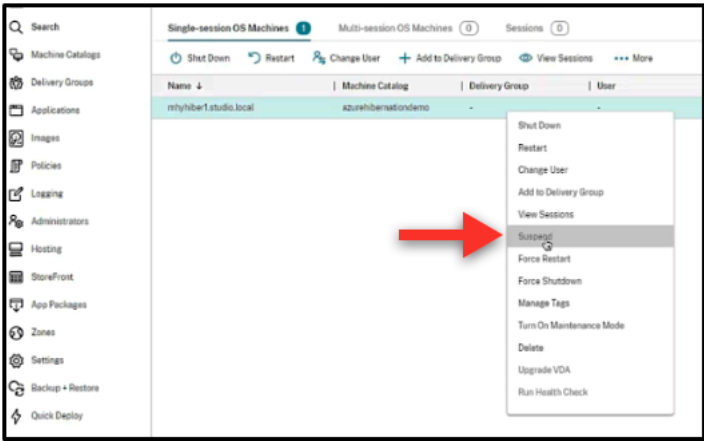
- 挂起
- 继续

**挂起** 您可以使用以下方法之一暂停虚拟机：

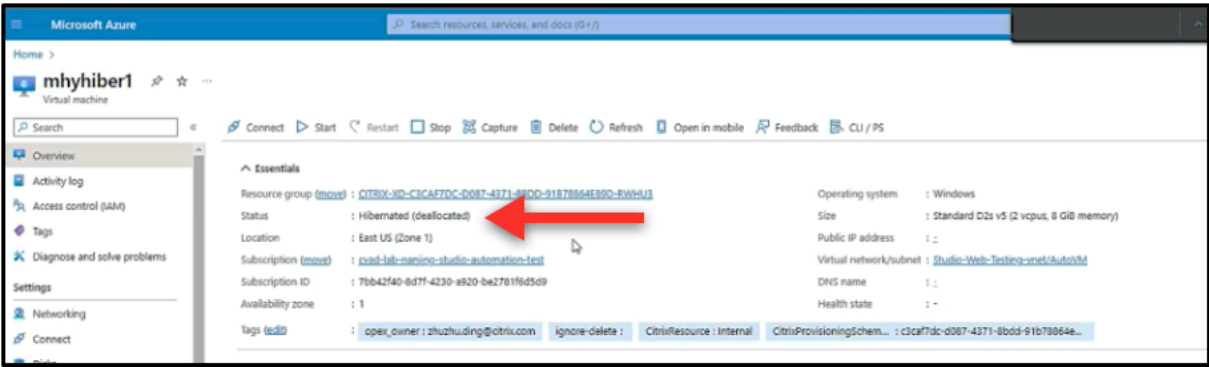
- 手动 使用完整配置界面
- 自动 使用超时策略：有关详细信息，请参阅 [其他设置](#)。

要手动挂起 VM，请执行以下操作：

1. 右键单击 VM，然后选择挂起。单击是确认操作。电源状态从正在挂起更改为已挂起。

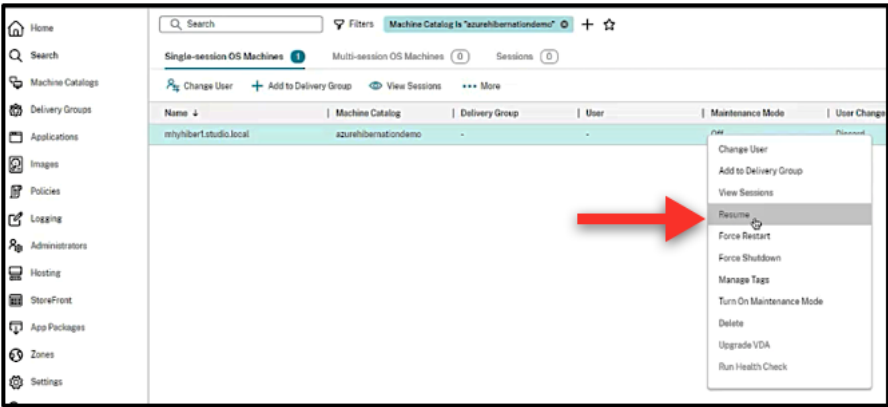


可以在 Azure 门户中检查 VM 的状态。

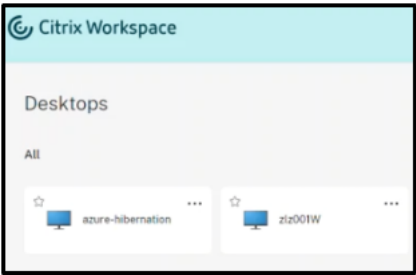


继续 要恢复休眠的 VM，请使用以下方法之一：

- 手动：
  - 管理员可以使用完整配置界面恢复虚拟机。

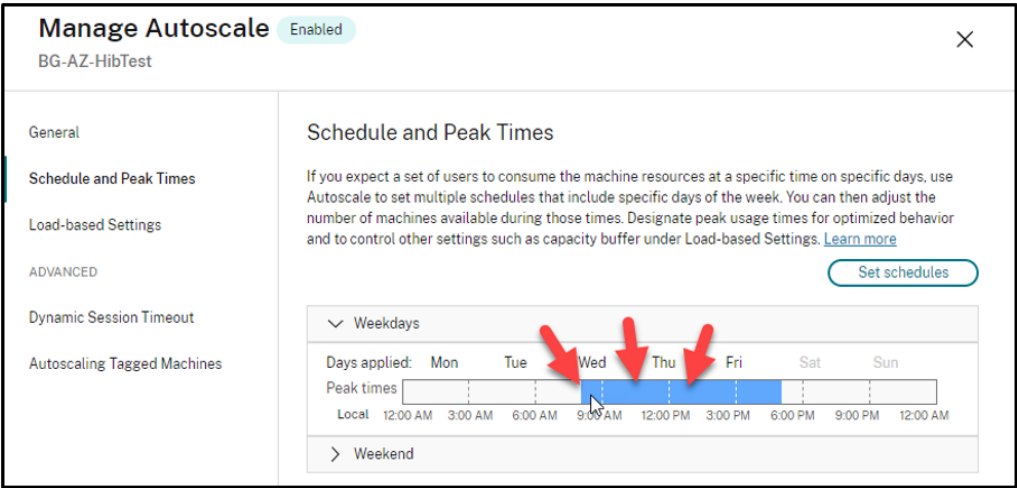


- 最终用户单击桌面图标后，可以使用 Citrix Workspace 菜单启动虚拟机。

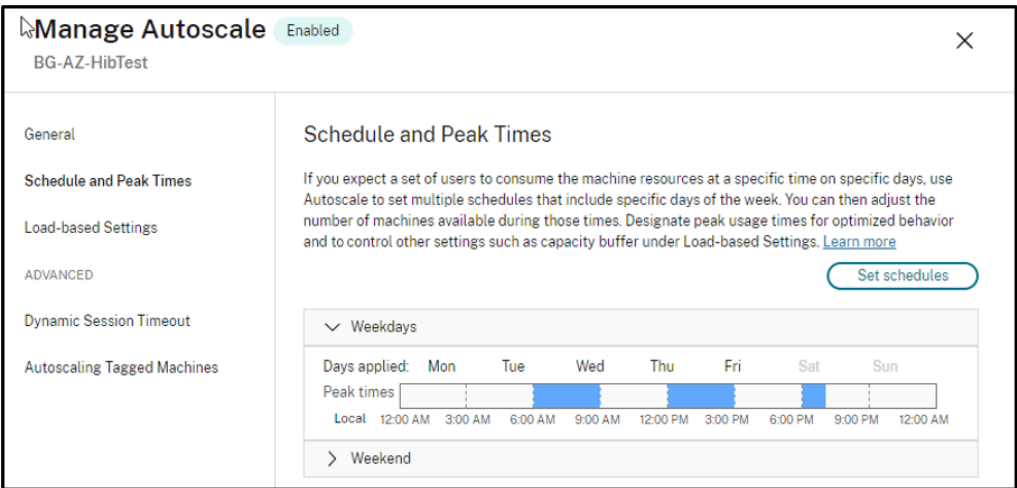


- 自动：
  - 如果您正确配置了高峰时间，AutoScale 可以自动打开休眠计算机的电源。可以通过单击时间表每隔 30 分钟设置一次高峰时间。每个蓝框代表一个标记为高峰时间的时段。高峰时段可以有连续和非连续的时段。

★ 连续时段



★ 非连续时段



注意：

在管理 **AutoScale** > 基于负载的设置中，如果将操作配置为挂起，则请确保该交付组中的所有 VM 都具有休眠功能。否则，无法休眠的 VM 将继续运行。

Manage Autoscale

Enabled

×

BG-AZ-HibTest

General

Schedule and Peak Times

Load-based Settings

ADVANCED

Dynamic Session Timeout

Autoscaling Tagged Machines

Load-based Settings

Capacity buffer

Capacity buffer is used to accommodate sudden spikes in demand by keeping a buffer of machines powered on based on the maximum load index of the delivery group. By default, the capacity buffer is 10% of the maximum supported load index of the delivery group. A lesser value decreases the cost. A greater value ensures an optimized user experience so that users do not have to wait for additional machines to power on when launching sessions. [Learn more](#)

During peak times

During off-peak times

Capacity buffer (%):

0

0

Power policies

Configure policies for power managing machines in different scenarios. For each scenario, specify the waiting period (in minutes) and the action to take after the specified period elapses.

After disconnection

	Waiting period (min)	Action
During peak times	1	Suspend
During off-peak times	1	Suspend

After logoff

	Waiting period (min)	Action
During peak times	1	Suspend
During off-peak times	1	Suspend

If no user logs on after machine is powered on by Autoscale

	Waiting period (min)	Action
During peak times	0	No action

更多信息

有关 Citrix Azure 休眠的详细信息，请参阅 [Citrix Tech Zone](#) 一文。



## 安全策略

April 11, 2023

本文介绍了各种支持的虚拟机管理程序的安全功能。安全功能包括：

- [安全组](#)
- [安全启动](#)
- [加密功能](#)

## 安全组

April 11, 2023

安全组是一组安全规则，用于过滤虚拟网络中资源之间的网络流量。安全规则允许或拒绝进入多种类型资源的入站网络流量或来自多种资源的出站网络流量。每条规则都指定了以下属性：

- 名称：网络安全组中的唯一名称
- 优先级：规则按优先级顺序处理，较小的数字在较高的数字之前处理，因为数字越小，优先级越高
- 源或目标：任何或单个 IP 地址、无类域间路由 (CIDR) 块（例如 10.0.0.0/24）、服务标签或应用程序安全组
- 协议：您为每个安全组添加规则所依据的协议
- 方向：该规则适用于入站流量还是出站流量
- 端口范围：您可以指定单个端口或端口范围
- 操作：允许或拒绝

有关支持的虚拟机管理程序的更多信息，请参阅以下内容：

- [AWS 中的安全组](#)
- [Microsoft Azure 中的安全组](#)
- [Google Cloud Platform 中的安全组](#)

## AWS 中的安全组

安全组用作控制 VPC 中的实例的流量的虚拟防火墙。您负责向安全组中添加允许公共子网中的实例与专用子网中的实例进行通信的规则。您还可以将这些安全组与 VPC 中的每个实例相关联。入站规则控制您的实例的传入流量，出站规则控制来自您的实例的传出流量。

有关映像准备期间网络设置的更多信息，请参阅[映像准备期间的网络设置](#)。

启动实例时，您可以指定一个或多个安全组。要配置安全组，请参阅[配置安全组](#)。

## Microsoft Azure 中的安全组

Citrix DaaS 支持 Azure 中的网络安全组。网络安全组应与子网关联。有关更多信息，请参阅 [网络安全组](#)。

有关在映像准备期间创建的网络安全组的更多信息，请参阅 [使用 Azure Resource Manager 映像创建计算机目录](#)。

## Google Cloud Platform 中的安全组

在准备计算机目录期间，将准备计算机映像作为目录的主映像系统磁盘。发生此过程时，磁盘将临时连接到虚拟机。此 VM 必须在隔离的环境中运行，以阻止所有入站和出站网络流量。这是通过一对拒绝所有防火墙规则实现的。有关更多信息，请参阅 [防火墙规则](#)。

## 安全启动

June 1, 2023

安全启动旨在确保仅使用可信软件来启动系统。固件具有可信证书数据库，并验证其加载的映像是否由其中一个可信证书签名。如果该图像加载了更多图像，则还必须以相同的方式验证该图像。

vTPM 是传统物理 TPM 模块的虚拟化软件实例。vTPM 通过测量虚拟机的整个启动链（UEFI、操作系统、系统和驱动程序）来实现认证。

有关支持的虚拟机管理程序的更多信息，请参阅以下内容：

- [在 Google Cloud Platform 中安全启动](#)
- [在 Microsoft Azure 中安全启动](#)
- [在 VMware 中安全启动](#)

### 在 Google Cloud Platform 中安全启动

可以在 GCP 上配置屏蔽的虚拟机。通过使用安全启动、虚拟可信平台模块、UEFI 固件和完整性监视等高级平台安全功能，使用一组安全控制来增强受保护的虚拟机，这些控制可为 Compute Engine 实例提供可验证的完整性。

有关使用 PowerShell 使用安全增强型虚拟机创建目录的更多信息，请参阅[使用 PowerShell 使用安全增强型虚拟机创建目录](#)。

### 在 Microsoft Azure 中安全启动

在 Azure 环境中，您可以创建启用受信任启动的计算机目录。Azure 提供受信任启动，以无缝方式提高第 2 代虚拟机的安全性。受信任启动可防范高级和持续攻击技术。受信任启动的根源是虚拟机的安全启动。受信任启动还使用 vTPM 执行云端远程认证。这用于平台运行状况检查和做出基于信任的决策。您可以单独启用安全启动和 vTPM。

有关使用受信任启动创建计算机目录的更多信息，请参阅[使用受信任启动创建计算机目录](#)。

## 在 **VMware** 中安全启动

MCS 支持创建计算机目录，其中附有 vTPM 的 VMware 模板作为计算机配置文件输入的来源。如果在主映像上安装了 Windows 11，则需要为主映像启用 vTPM。因此，作为计算机配置文件来源的 VMware 模板必须附加 vTPM。有关更多信息，请参阅[使用计算机配置文件创建计算机目录](#)。

## 加密功能

June 1, 2023

加密功能保护虚拟机的内容免受共享虚拟机主机上的恶意访客的攻击，以及管理主机上所有虚拟机的虚拟机管理程序控制软件发起的攻击。

有关支持的虚拟机管理程序的更多信息，请参阅以下内容：

- [AWS 中的加密功能](#)
- [Google Cloud Platform 中的加密功能](#)
- [Microsoft Azure 中的加密功能](#)

## **AWS** 中的加密功能

本节介绍了 AWS 虚拟化环境中的加密功能。

### 自动加密

您可以对在您的帐户中创建的新 Amazon EBS 卷和快照副本开启自动加密。有关更多信息，请参阅 [自动加密](#)。

## **Google Cloud Platform** 中的加密功能

本节介绍了 Google Cloud Platform (GCP) 虚拟化环境中的加密功能。

如果您需要对密钥操作的控制超过 Google 管理的加密密钥所允许的范围，则可以使用客户管理的加密密钥。使用客户管理的加密密钥时，当对象存储在存储桶中时，Cloud Storage 会使用该密钥对其进行加密，当向请求者提供对象时，Cloud Storage 会自动解密该对象。有关更多信息，请参阅 [客户管理的加密密钥](#)。

可以将客户管理的加密密钥 (CMEK) 用于 MCS 目录。有关详细信息，请参阅[使用客户管理的加密密钥 \(CMEK\)](#)。

## **Microsoft Azure** 中的加密功能

本节介绍了 Azure 虚拟化环境中的加密功能。

### Azure 服务器端加密

大多数 Azure 托管磁盘都使用 Azure 存储加密进行加密，Azure 存储加密使用服务器端加密 (SSE) 来保护您的数据并帮助您兑现安全性和合规性承诺。Citrix DaaS 通过 Azure 密钥保管库支持 Azure 托管磁盘的客户托管加密密钥。有关详细信息，请参阅 [Azure 服务器端加密](#)。

### Azure 双加密

双重加密是平台端加密（默认）和客户管理加密（CMEK）。因此，如果您是高度安全敏感的客户，并且担心与任何加密算法、实施或密钥泄露相关的风险，则可以选择这种双重加密。永久操作系统和数据磁盘、快照和映像均使用双重加密进行静态加密。有关更多信息，请参阅[托管磁盘上的双重加密](#)。

## 快速部署

November 16, 2023

### 简介

在 Citrix DaaS 中，使用 Microsoft Azure 托管您的桌面和应用程序时，**Manage**（管理）> **Quick Deploy**（快速部署）界面可以快速部署应用程序和桌面。此界面提供了基本配置，不提供高级功能。

使用快速部署可以执行以下操作：

- 预配交付 Microsoft Azure 中托管的桌面和应用程序的虚拟机和目录。
- 为现有计算机创建 Remote PC Access 目录。

通过快速部署，您可以使用 [Citrix 托管 Azure](#) 订阅，也可以使用自己的 Azure 订阅。

（尽管名称相似，但快速部署与在快速部署界面中创建目录的快速创建方法不同。）

作为快速部署的替代方案，**Full Configuration**（完整配置）界面提供了高级配置功能。有关 **Manage**（管理）选项卡选项的信息，请参阅[管理接口](#)。

### 管理界面之间的差异

下表比较了“完整配置”与“快速部署”界面。

功能	快速部署	完整配置
使用 Azure 进行部署	是	是 *
使用其他云服务进行部署	否	是
使用本地虚拟机管理程序进行部署	否	是
Citrix 准备的映像可用	是	否
简化的用户体验	是	否

\* 使用 Citrix 托管 Azure 订阅时，必须在创建映像或目录时使用快速部署。

如果您熟悉使用完整配置创建和管理目录，则快速部署具有以下区别。

- 不同的术语。
  - 在快速部署中，您可以创建一个目录。
  - 在完整配置中，您可以创建计算机目录。实际上，它通常称为简单目录。
- 资源位置和 Cloud Connector。
  - 当您创建第一个目录时，快速部署会自动创建包含两个 Cloud Connector 的资源位置。
  - 在“完整配置”中，创建资源位置和添加 Cloud Connector 是在创建目录之前必须在 Citrix Cloud 中完成的单独步骤。
- 用于创建目录的映像。
  - 快速部署提供了多个 Citrix 准备的 Windows 和 Linux 计算机映像。可以使用这些映像创建目录。  
还可以使用这些映像创建映像，然后对新映像进行自定义以满足您独特的部署需求。此功能称为映像生成器。也可以从 Azure 订阅导入映像。
  - 在完整配置中，您可以自定义所使用的受支持主机中的映像。Citrix 准备的映像不可用。
- 目录显示：
  - 在快速部署中创建的目录在“快速部署”和“完整配置”显示屏中可见。
  - 在“完整配置”中创建的目录在“快速部署”显示屏中不可见。
- 交付组：
  - 您不能在快速部署中创建交付组。在快速部署中，您可以指定目录中的计算机、应用程序、桌面和用户（订阅者）。  
Citrix 使用与目录相同的名称为每个快速部署目录自动创建交付组。该操作在后台进行。您无需执行任何操作即可创建交付组。交付组仅显示在“完整配置”界面中，而不显示在“快速部署”中。
  - 在“完整配置”中，您可以创建交付组并指明其中包含的计算机。（可选）还可以指定应用程序、桌面和用户。此外，还可以创建应用程序组。

- 布局和用户界面。
  - “快速部署”界面的布局和样式与“完整配置”不同。快速部署包含更多屏幕指导。

这些接口不相互排斥。可以使用“快速部署”创建一些目录，然后使用“完整配置”创建其他目录。

### 管理在“快速部署”界面中创建的目录

在“快速部署”界面中创建目录后，可以继续在该界面中管理该目录。有关详细信息，请参阅[在快速部署中管理目录](#)。还可以使用“完整配置”界面。

在“快速部署”中创建目录时，系统会为该目录（以及在后台自动创建的交付组和托管连接）分配作用域 **Citrix managed object**。作用域在[委派管理](#)中用于对对象进行分组。

在“完整配置”界面中，禁止通过某些操作对目录、交付组以及与作用域 **Citrix managed object** 的连接进行操作。（允许在“完整配置”中执行这些操作可能会对系统同时支持“快速部署”和“完整配置”的能力产生不利影响，因此这些操作处于禁用状态。）在“完整配置”界面中：

- 目录：大多数目录管理操作不可用。您无法删除目录。
- 交付组：大多数交付组管理操作都可用。您无法删除交付组。
- 连接：大多数连接管理操作不可用。您无法删除连接。不能创建基于具有 **Citrix managed object** 作用域的连接。

如果您使用自己的 Azure 订阅（已添加到“快速部署”中）在“快速部署”中创建目录，并且想要完全在“完整配置”中管理目录（及其交付组和连接），则可以转换目录。

- 转换目录会将其管理限制为仅限于“完整配置”界面。转换目录后，您将无法再使用“快速部署”界面来管理该目录。
- 转换目录后，可以选择以前在“完整配置”中不可用的操作。（**Citrix managed object** 作用域将从转换后的目录、交付组和托管连接中删除。）
- 要转换目录，请执行以下操作：
  - 在 **Manage（管理） > Quick Deploy（快速部署）** 控制板中，单击目录的条目中的任意位置。在详细信息选项卡的高级设置下，选择转换目录。出现提示时，确认转换。
- 不能转换使用 Citrix 托管 Azure 订阅在“快速部署”中创建的目录。

### 更换早期的 **Azure** 快速部署界面

快速部署将替换早期的名为 Azure 快速部署的界面。“快速部署”显示包括使用 Azure 快速部署创建的所有目录。

如果您开始在 Azure 快速部署中创建目录，但没有完成，该目录显示在快速部署目录列表中。但是，快速部署中唯一可用的操作是删除。

### 要求

- 快速部署仅支持 Azure 工作负载。它不适用于任何其他云主机类型、服务或虚拟机管理程序。
- 快速部署仅在 Citrix DaaS for Azure Premium 和 Advanced Edition 以及 Workspace Premium Plus 中可用。
- 您必须拥有 Citrix Cloud 帐户并订阅 Citrix DaaS。
- 如果您订购了 [Citrix 托管 Azure Consumption Fund](#)，则可以在创建目录和映像时使用 Citrix 托管 Azure 订阅。

如果您没有订购 Consumption Fund（或者更喜欢使用自己的 Azure 订阅），则必须拥有 Azure 订阅。

- 您必须在 Citrix DaaS 中具有相应的权限才能查看管理选项卡。有关详细信息，请参阅[委派管理](#)。

#### 重要说明：

为确保您获得有关 Citrix Cloud 和您订阅的 Citrix 服务的重要信息，请确保您能够接收所有电子邮件通知。例如，Citrix 每月发送信息性通知电子邮件，详细说明 Azure 的消耗情况（使用情况）。

在 Citrix Cloud 控制台的右上角，展开客户名称和 OrgID 字段右侧的菜单。选择帐户设置。在我的个人资料选项卡上，选择电子邮件通知部分中的所有条目。

### Citrix Gateway 注意事项

如果您使用自己的 Citrix Gateway，该网关必须具有对在目录创建向导中指定的 VNet 的访问权限。VPN 可以提供该访问权限。

Citrix Gateway 服务自动与快速部署目录一起工作。

### 接下来做什么

请按照[入门](#)中的快速部署设置指南进行操作。

使用快速部署设置部署后，可以继续使用界面执行以下管理任务。

- [管理目录](#)。目录管理包括添加或删除计算机、管理应用程序、管理电源管理计划。
- [管理映像](#)。映像管理包括准备或导入映像、使用新映像更新目录、重命名或删除映像以及在映像上安装或升级 VDA。
- [在目录中添加或删除用户](#)。
- [管理资源位置](#)。

## 快速部署入门

May 19, 2023

本文总结了使用 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）的“快速部署”界面交付桌面和应用程序的设置任务。我们建议您在实际执行之前查看每个过程，以便您知道操作的结果。

要使用“快速部署”设置 Remote PC Access 部署，请参阅 [Remote PC Access](#)。

### 安装任务摘要

本文的以下部分将指导您完成设置任务：

1. 查看并完成系统要求和准备中的必要任务。
2. 设置快速概念证明部署或生产部署。
3. 将 Workspace URL 发送给用户。

### 系统要求和准备

- [注册 Citrix Cloud 和 Citrix DaaS](#)。

此外，如果您计划使用 [Citrix 托管 Azure](#)，请务必通过 Citrix 或 Azure 应用商店订购 Citrix Azure Consumption Fund（Citrix DaaS 除外）。

- **Windows** 许可：确保您已获得正确的远程桌面服务许可，以运行 Windows Server 工作负载或 Windows 10 的 Azure 虚拟桌面许可。有关详细信息，请参阅[配置 Microsoft RDS 许可证服务器](#)。
- 如果计划使用 Citrix 托管 Azure 订阅，并希望使用 Active Directory 组策略将 VDA 加入域，您必须是具有在 Active Directory 中执行该操作的权限的管理员。有关详细信息，请参阅[客户的职责](#)。
- 配置到企业内部网络的连接有额外的要求。
  - 任何连接（Azure vNet 对等互连或 SD-WAN）：[所有连接的要求](#)。
  - Azure vNet 对等连接：[vNet 对等互连要求和准备工作](#)。
  - SD-WAN 连接：[SD-WAN 连接的要求和准备工作](#)。
- 如果您计划在创建目录时使用自己的 Azure 映像，则这些映像必须满足特定要求。
- Internet 连接要求：[系统和连接要求](#)。
- Citrix DaaS 部署中的资源限制：[限制](#)。



## 支持的操作系统

在 Citrix 托管 Azure 订阅中使用快速部署时：

- Windows 10 单会话
- Windows 10 多会话
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Red Hat Enterprise Linux 和 Ubuntu

在客户管理的 Azure 订阅中使用快速部署时：

- Windows 10 Enterprise 单会话
- Windows 10 Enterprise 虚拟桌面多会话
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Red Hat Enterprise Linux 和 Ubuntu

## 设置快速概念证明部署

此过程需要 Citrix 托管 Azure 订阅。

1. [使用快速创建创建目录](#)。
2. 将[用户添加到托管 Azure AD](#)。
3. 将[用户添加到目录](#)。
4. 向用户通知 Workspace URL。

## 设置生产部署

1. 如果您使用自己的 Active Directory 或 Azure Active Directory 来对用户进行身份验证，请在[Citrix Cloud 中连接并设置该方法](#)。
2. 如果您使用已加入域的计算机，请[确认您拥有有效的 DNS 服务器条目](#)。
3. 如果使用自己的 Azure 订阅（而非 Citrix 托管 Azure 订阅），请[添加您的 Azure 订阅](#)。
4. [创建或导入映像](#)。尽管您可以在目录中按原样使用 Citrix 准备的其中一个映像，但它们主要用于概念验证部署。
5. 如果您使用的是 Citrix 托管 Azure 订阅，并希望用户能够访问网络中的项目（例如文件服务器），请设置[Azure vNet 对等连接](#)或[Citrix SD-WAN 连接](#)。
6. [使用自定义创建创建目录](#)。
7. 如果要创建多会话计算机的目录，请根据需要[将应用程序添加到目录](#)中。

8. 如果您使用 Citrix 托管 Azure AD 对用户进行身份验证，请将[用户添加到目录](#)中。
9. [将用户添加到目录](#)。
10. 向用户通知 Workspace URL。

设置部署后，请使用快速部署 > 监视控制板查看[桌面使用情况](#)、[会话](#)和[计算机](#)。

## Workspace URL

创建目录并分配用户后，通知用户在哪里可以找到他们的桌面和应用程序：Workspace URL。Workspace URL 对于所有目录和用户都是相同的。

Workspace URL 在两个位置提供：

- 在 Citrix DaaS 中的 **Manage**（管理）> **Quick Deploy**（快速部署）中，通过展开右侧的 **User Access & Authentication**（用户访问和身份验证）来查看 URL。
- 在 Citrix Cloud 控制台中，从左上角的菜单中选择 **Workspace Configuration**（工作区配置）。“访问”选项卡包含工作区 URL。

有关自定义 Workspace URL 的信息，请参阅[自定义 Workspace URL](#)。

用户导航到 Workspace URL 并进行身份验证后，他们可以启动自己的桌面和应用程序。

### 获取帮助

- 请查看[故障排除](#)一文。
- 如果 Citrix DaaS 仍然存在问题，请按照[如何获取帮助和支持](#)中的说明开立一个票证。

## 使用快速部署创建目录

May 11, 2022

使用本文中的过程可通过“快速部署”管理界面创建 Microsoft Azure 计算机的目录。

请在创建目录之前查看整个过程，这样您就会知道操作结果。

要使用“完整配置”界面创建目录，请参阅[创建计算机目录](#)。

### 计算机类型

快速部署目录可以包含以下类型的计算机之一：

- 静态：目录包含单会话静态计算机（又称为个人桌面、专用桌面或持久桌面）。静态意味着当用户启动某个桌面时，该桌面“属于”该用户。用户对桌面所做的任何更改都将在注销时保留。稍后，当该用户返回 Citrix Workspace 并启动桌面时，它就是同一个桌面。
- 随机：目录包含单会话随机计算机（又称为非持久桌面）。随机意味着当用户启动桌面时，注销后该用户对该桌面所做的任何更改都将被丢弃。稍后，当该用户返回 Citrix Workspace 并启动桌面时，它可能是同一个桌面，也可能不是。
- 多会话：目录包含具有应用程序和桌面的计算机。多个用户可以同时访问其中的每台计算机。用户可以从其工作区启动桌面或应用程序。可以共享应用程序会话。不允许在应用程序与桌面之间共享会话。
  - 创建多会话目录时，可以选择工作负载：轻（例如数据输入）、中（例如办公应用程序）、重（例如工程）或自定义。每个选项都表示特定计算机数量以及每台计算机的特定会话数，这将产生目录支持的会话总数。
  - 如果选择自定义工作负载，则可以从 CPU、RAM 和存储的可用组合中进行选择。键入计算机数量以及每台计算机的会话数，这将产生目录支持的会话总数。

部署桌面时，静态和随机计算机类型有时称为“桌面类型”。

使用“快速部署”创建目录的方法

可以通过几种方法创建和配置目录：

- 快速创建是最快的入门方法。您提供最少的信息，Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）负责其余的信息。快速创建目录非常适合测试环境或概念证明。
- 自定义创建允许使用的配置选项比快速创建多。它更适合生产环境而非快速创建目录。
- **Remote PC Access** 目录包含用户远程访问的现有计算机（通常是物理机）。有关这些目录的详细信息和说明，请参阅 [Remote PC Access](#)。

下面是快速创建和自定义创建的比较：

快速创建	自定义创建
要提供的信息较少。	要提供的信息较多。
某些功能的选择较少。	某些功能的选择较多。
Citrix 托管 Azure Active Directory 用户身份验证。	选择：Citrix 托管 Azure Active Directory，或者您的 Active Directory/Azure Active Directory。
没有与本地网络的连接。	选择：不连接到本地网络、Azure vNet 对等互连和 SD-WAN。
使用 Citrix 准备的 Windows 10 映像。该映像包含当前的桌面 VDA。	选择：Citrix 准备的映像、从 Azure 导入的映像，或者在 Citrix DaaS 中基于 Citrix 准备或导入的映像构建的映像。
每个桌面都有 Azure 标准磁盘 (HDD) 存储。	有几种存储选项可供选择。
仅限静态桌面。	静态、随机或多会话桌面。

快速创建	自定义创建
在创建过程中无法配置电源管理计划。会话结束时，托管桌面的计算机会关闭电源。（您可以稍后更改此设置。）	可以在创建过程中配置电源管理计划。（快速部署电源管理计划不同于您可以使用“完整配置”管理界面创建的电源管理计划。）
必须使用 Citrix 托管 Azure 订阅。	可以使用 Citrix 托管 Azure 订阅或自己的 Azure 订阅。

有关过程详细信息，请参阅：

- 使用快速创建创建快速部署目录
- 使用自定义创建创建快速部署目录

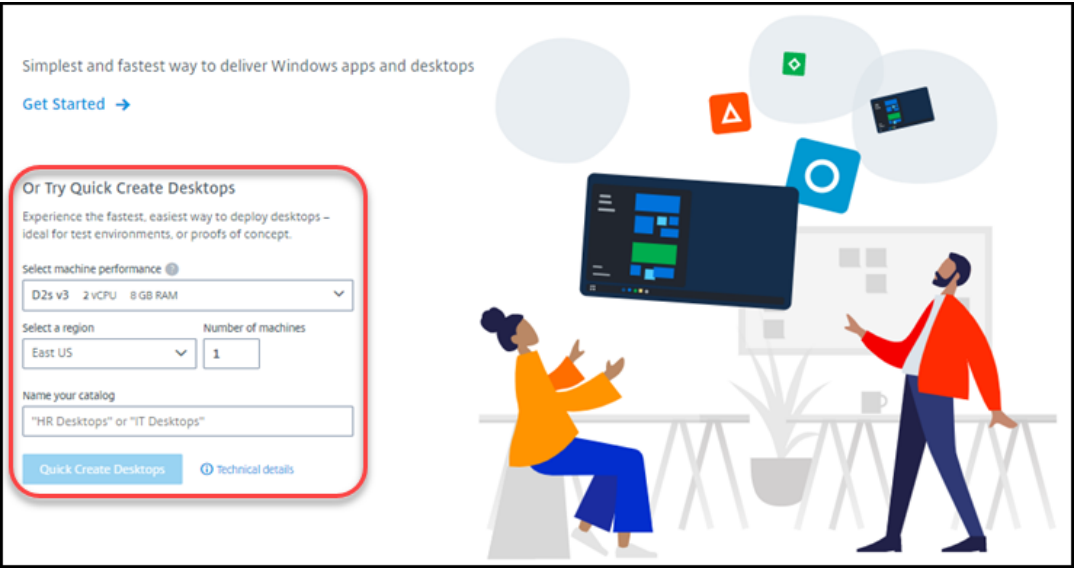
重要：

首次使用 Citrix 托管 Azure 订阅创建目录（或映像）时，系统会要求您确认并同意自己对产生的费用的责任。使用 Citrix 托管 Azure 订阅创建更多目录或映像时，也可能会出现关于同意的提醒。

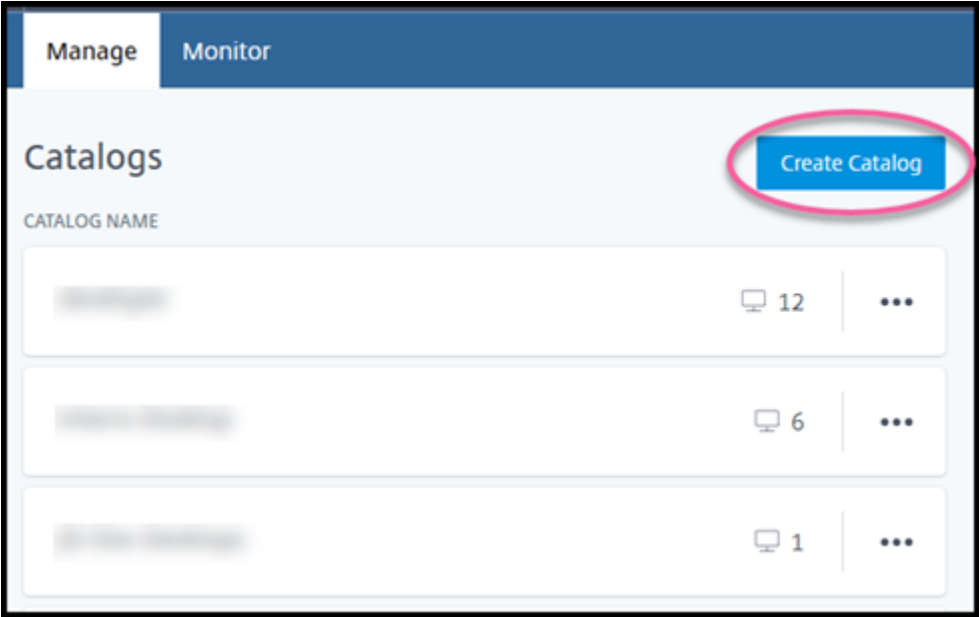
使用快速创建创建快速部署目录

快速创建方法使用 Citrix 托管 Azure 订阅和 Citrix 准备的 Windows 10 映像来创建包含静态计算机的目录。电源管理设置使用“Cost Saver”（成本节省程序）预设值。没有与您的公司网络的连接。必须使用 Citrix 托管 Azure AD 添加用户。

1. 登录 Citrix Cloud。
2. 在左上角的菜单中，选择我的服务 > DaaS。
3. 选择 **Manage**（管理）> **Quick Deploy**（快速部署）。
4. 如果目录尚未创建，系统会将您引导至 **Welcome**（欢迎）页面。选择以下方法之一：
  - 在此页面上配置目录。继续执行步骤 6 到 10。



- 选择 **Get Started**（入门）。您将转到 **Manage**（管理）> **Quick Deploy**（快速部署）控制板。选择 **Create Catalog**（创建目录）。
5. 如果已创建目录（并且您正在创建另一个目录），您将转到 **Manage**（管理）> **Quick Deploy**（快速部署）控制板。选择 **Create Catalog**（创建目录）。



6. 如果尚未选择，请选择页面顶部的 **Quick Create**（快速创建）。

**Create Catalog**

Custom Create Quick Create

Select machine performance ⓘ

D2s v3 2 vCPU 8 GB RAM

Select a region

East US

Name your catalog

Enter a friendly name to identify this group of desktops like "Marketing" or "HR"

"HR Desktops" or "IT Desktops"

Number of machines

1

Quick Create Catalogs Use

- Static machines
- Managed Azure AD
- No connectivity to your corporate network
- Citrix-managed Windows 10 master image
- Cost Saver preset power settings

Create Catalog Cancel Users will be assigned after the machines

- **Machine performance**（计算机性能）：选择计算机类型。每种选择都有 CPU、RAM 和存储的独特组合。计算机的性能越高，每个月的成本也越高。
- **区域**：选择要在其中创建计算机的区域。可以选择一个靠近您的用户的区域。
- **Name**（名称）：键入目录的名称。此字段为必填字段，没有默认值。
- **计算机数量**：键入所需的计算机数量。

7. 完成后，选择 **Create Catalog**（创建目录）。（如果要从 **Welcome**（欢迎）页面创建第一个目录，请选择 **Quick Create Desktops**（快速创建桌面）。）

8. 如果这是您使用 Citrix 托管 Azure 订阅创建的第一个目录，请在系统提示时，确认您对相关费用的责任。

创建目录时，目录的名称将添加到目录列表中，表明其在创建过程中的进度。

Citrix DaaS 还会自动创建资源位置并添加两个 Citrix Cloud Connector。

后续操作：

- 您可以在创建目录时将用户添加到托管 [Azure AD 目录](#) 中。
- 创建目录后，请将用户添加到目录中。

## 使用自定义创建快速部署目录

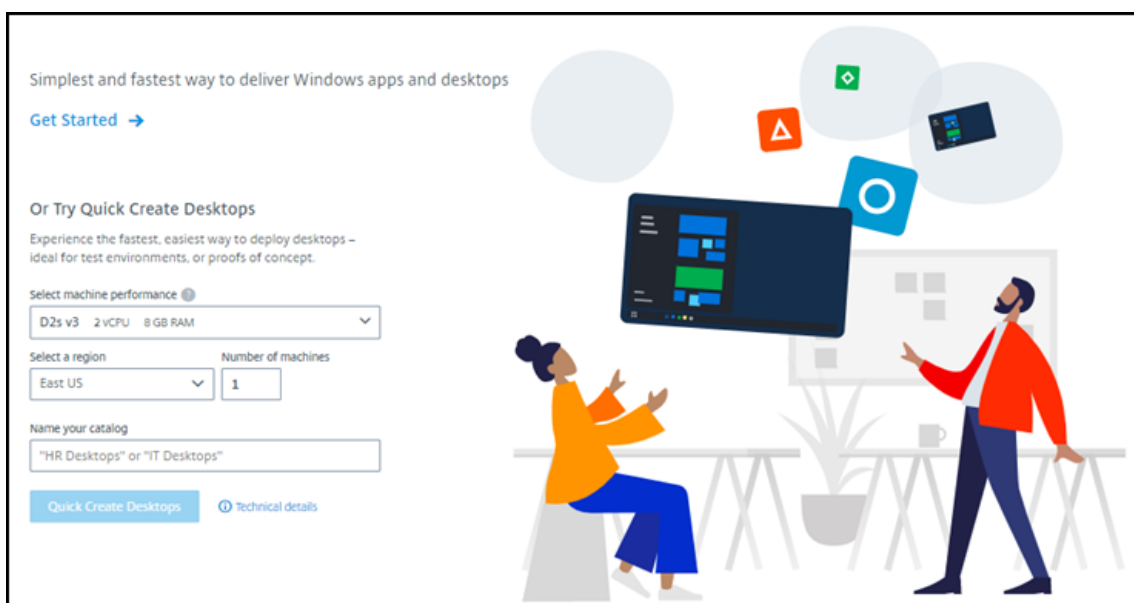
如果您使用的是 Citrix 托管 Azure 订阅，并计划使用与本地网络资源的连接，请[创建该网络连接](#)，然后再创建目录。要允许用户访问本地资源或其他网络资源，还需要该位置的 Active Directory 信息。

如果您没有 Citrix 托管 Azure 订阅，则可以：

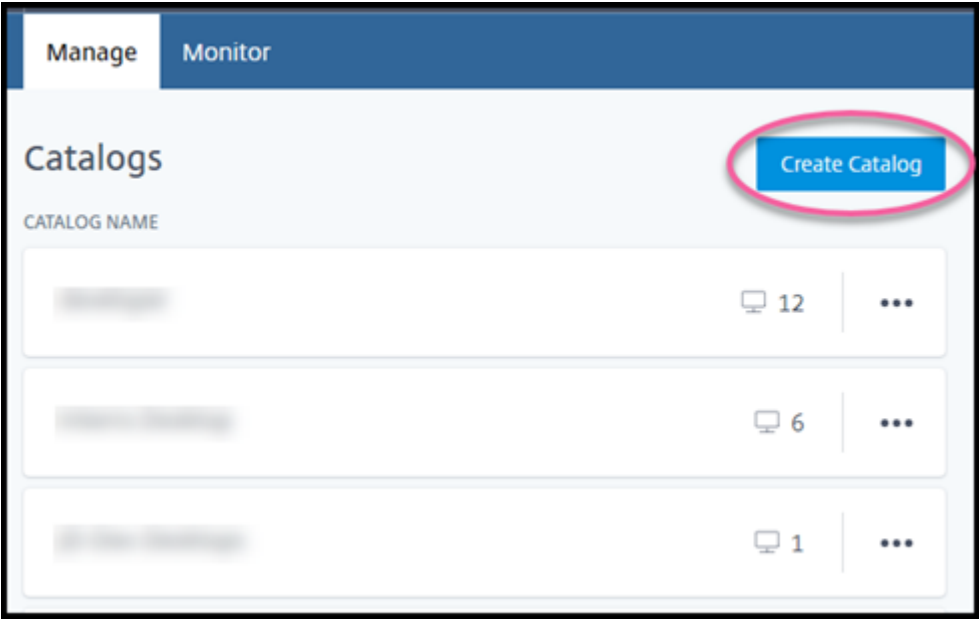
- 通过 Azure 应用商店[订购 Azure Consumption Fund](#)，该应用商店可为您提供 Citrix 托管 Azure 订阅。
- 在创建目录之前，[将您自己的一个或多个 Azure 订阅导入（添加）](#)到 Citrix DaaS。

要创建目录，请执行以下操作：

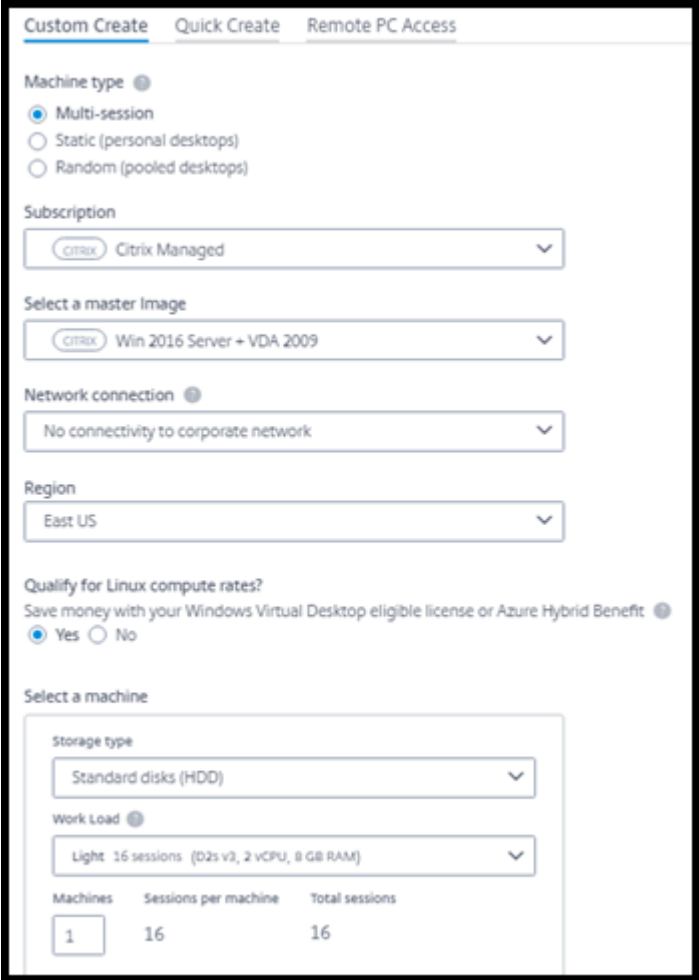
1. 登录 [Citrix Cloud](#)。
2. 在左上角的菜单中，选择我的服务 > **DaaS**。
3. 选择 **Manage**（管理）> **Quick Deploy**（快速部署）。
4. 如果目录尚未创建，系统会将您引导至 **Welcome**（欢迎）页面。选择 **Get Started**（入门）。在简介页面的末尾，您将转到 **Manage**（管理）> **Quick Deploy**（快速部署）控制板。选择 **Create Catalog**（创建目录）。



如果已创建目录，则将转到 **Manage**（管理）> **Quick Deploy**（快速部署）控制板。选择 **Create Catalog**（创建目录）。



5. 如果尚未选择，请在页面顶部选择 **Custom Create**（自定义创建）。





6. 填写以下字段。（某些字段仅对某些计算机类型有效。字段顺序可能会有所差别。）

- **Machine type**（计算机类型）。选择计算机类型。有关详细信息，请参阅计算机类型。
- **Subscription**（订阅）。选择 [Azure 订阅](#)。
- 主映像：选择要用于目录的计算机的操作系统映像。
- 网络连接：选择要用于访问网络中的资源的 [网络连接](#)。

如果选择了 Citrix 托管 Azure 订阅，则可以选择以下选项：

- **No Connectivity**（无连接）：用户无法访问本地企业网络中的位置和资源。
- 连接：选择之前创建的连接，例如 VNet 对等互连或 SD-WAN 连接。

如果选择了客户管理的 Azure 订阅，请选择适当的资源组、虚拟网络和子网。

- **Region**（区域）：（仅当您选择了 **Network connection**（网络连接）中的 **No Connectivity**（无连接）时才可用。）选择要在其中创建桌面的区域。可以选择一个靠近您的用户的区域。

如果在 **Network connection**（网络连接）中选择一个连接，目录将使用该网络的区域。

- **Qualify for Linux compute rates?**（有资格获得 Linux 计算费率？）（仅当选择了 Windows 映像时才可用。）使用符合条件的许可证或 Azure 混合权益时，可以节省费用。

**Windows Virtual Desktop benefit**（Windows 虚拟桌面权益）：面向以下对象的 Windows 10 或 Windows 7 每用户许可证：

- Microsoft 365 E3/ES
- Microsoft 365 A3/AS/学生使用权益
- Microsoft 365 F3
- Microsoft 365 Business Premium
- Windows 10 Enterprise E3/E5
- Windows 10 Education A3/A5
- Windows 10 VDA 每用户

RDS CAL 的每用户或每设备许可证，附带针对 Windows Server 工作负载的软件保障。

**Azure Hybrid benefit**（Azure 混合权益）：附带活动软件保障或同等合格订阅许可证的 Windows Server 许可证。请参阅 <https://azure.microsoft.com/en-us/pricing/hybrid-benefit/>。

- **Machine**（计算机）：
  - **Storage type**（存储类型）。HDD 或 SSD。
  - **Machine performance**（计算机性能）（面向 **Static**（静态）或 **Random**（随机）计算机类型）或 **Workload**（工作负载）（面向多会话计算机类型）。选项仅包括与所选映像的世代类型（gen1 或 gen2）匹配的选项。

如果选择自定义工作负载，请在 **Machine Performance**（计算机性能）字段中键入计算机数和每台计算机的会话数。

- 计算机。您希望此目录中包含的计算机数量。
- 计算机命名方案：请参阅计算机命名方案。
- **Name**（名称）：键入目录的名称。此名称显示在 **Manage**（管理）控制板上。
- **Power schedule**（电源计划）：默认选中 **I'll configure this later**（我稍后将对此进行配置）复选框。有关详细信息，请参阅[电源管理计划](#)。（此电源管理计划不同于 Citrix DaaS 的“完整配置”管理界面中提供的电源管理功能。）
- **Join the local Active Directory domain**（加入本地 Active Directory 域）：（仅当您在网络连接中选择了 Azure vNet 对等连接时才可用。）请选择是或否。如果选择是，请输入：
  - 域的 FQDN（例如 Contoso.com）。
  - 组织单位：要使用默认 OU（计算机），请将此字段留空。
  - Citrix DaaS 帐户名称：必须是 name@domain 或 domain\name 格式的域或企业管理员。
  - Citrix DaaS 帐户名称的密码。
- 高级设置：请参阅创建目录时的资源位置设置。

7. 完成后，选择 **Create Catalog**（创建目录）。

8. 如果这是您使用 Citrix 托管 Azure 订阅创建的第一个目录，请在系统提示时，确认您对相关费用的责任。

**Manage**（管理）> **Quick Deploy**（快速部署）控制板会指示目录的创建时间。Citrix DaaS 还会自动创建资源位置并添加两个 Citrix Cloud Connector。

后续操作：

- 如果尚未执行此操作，请为您的用户[配置身份验证方法](#)以向 Citrix Workspace 进行身份验证。
- 创建目录后，请[将用户添加到目录中](#)。
- 如果您创建的多会话目录，请[添加应用程序](#)（在添加用户之前或之后）。

### 创建目录时的资源位置设置

创建目录时，可以选择配置多个资源位置设置。

在目录创建对话框中选择 **Advanced settings**（高级设置）时，Citrix DaaS 将检索资源位置信息。

- 如果您已为目录选择了域和网络连接的资源位置，则可以将其保存以供正在创建的目录使用。

如果该资源位置只有一个 Cloud Connector，则会自动安装另一个。可以选择为要添加的 Cloud Connector 指定高级设置。
- 如果没有为目录选择的域和网络连接设置资源位置，系统会提示您配置一个位置。

配置高级设置：

- （仅当资源位置已设置时才需要。）资源位置的名称。

- 外部连接类型：通过 Citrix Gateway 服务或从企业网络内部。
- Cloud Connector 设置：
  - （仅在使用客户管理的 Azure 订阅时才可用）计算机性能。此选择用于资源位置中的 Cloud Connector。
  - （仅在使用客户管理的 Azure 订阅时才可用）Azure 资源组。此选择用于资源位置中的 Cloud Connector。默认值为资源位置上次使用的资源组（如果适用）。
  - 组织单位 (OU)。默认值为资源位置上次使用的 OU（如果适用）。

完成高级设置后，选择保存以返回到目录创建对话框。

创建目录后，可以执行几项资源位置操作。有关详细信息，请参阅[资源位置操作](#)。

## 计算机命名方案

要在创建目录时指定计算机命名方案，请选择 **Specify machine naming scheme**（指定计算机命名方案）。使用 1-4 个通配符（哈希标记）来指示名称中的顺序数字或字母出现的位置。规则：

- 命名方案必须至少包含一个通配符，但不能超过四个通配符。所有通配符必须在一起。
- 包括通配符在内的整个名称必须介于 2 到 15 个字符之间。
- 名称不能包括空格、斜杠、反斜杠、冒号、星号、尖括号、管道符号、逗号、波浪符、感叹号、at 符号、美元符号、百分号、插入符号、小括号、大括号或下划线。
- 名称不能以句点开头。
- 名称不能仅包含数字。
- 请勿在名称末尾使用以下字母：-GATEWAY、-GW 和 -TAC。

指明顺序值是数字 (0-9) 还是字母 (A-Z)。

例如，命名方案 **PC-Sales-##**（选择 **0-9**）会生成名为 **PC-Sales-01**、**PC-Sales-02**、**PC-Sales-03** 等的计算机帐户。

请留出足够的增长空间。

- 例如，包含 2 个通配符和 13 个其他字符（例如 **MachineSales-##**）的命名方案使用的是最大字符数 (15)。
- 一旦目录包含 99 台计算机，下一次计算机创建将失败。Citrix DaaS 尝试创建一台带三位数字 (100) 的计算机，但这将创建一个包含 16 个字符的名称。最大值为 15。
- 因此，在本例中，较短的名称（例如 **PC-Sales-##**）允许扩展超过 99 台计算机。

如果不指定计算机命名方案，Citrix DaaS 将使用默认命名方案 **DAS%%%%-\*\*-###**。

- %%%% = 五个与资源位置前缀匹配的随机字母数字字符
- \*\* = 目录的两个随机字母数字字符
- ### = 三位数字。

## 相关信息

- [Remote PC Access 目录](#)
- [在使用代理服务器的网络中创建目录](#)
- [显示目录信息](#)
- [在快速部署中管理目录](#)

## 在快速部署中管理目录

April 18, 2022

本文介绍了可用于管理在快速部署中创建的目录的目录管理任务。

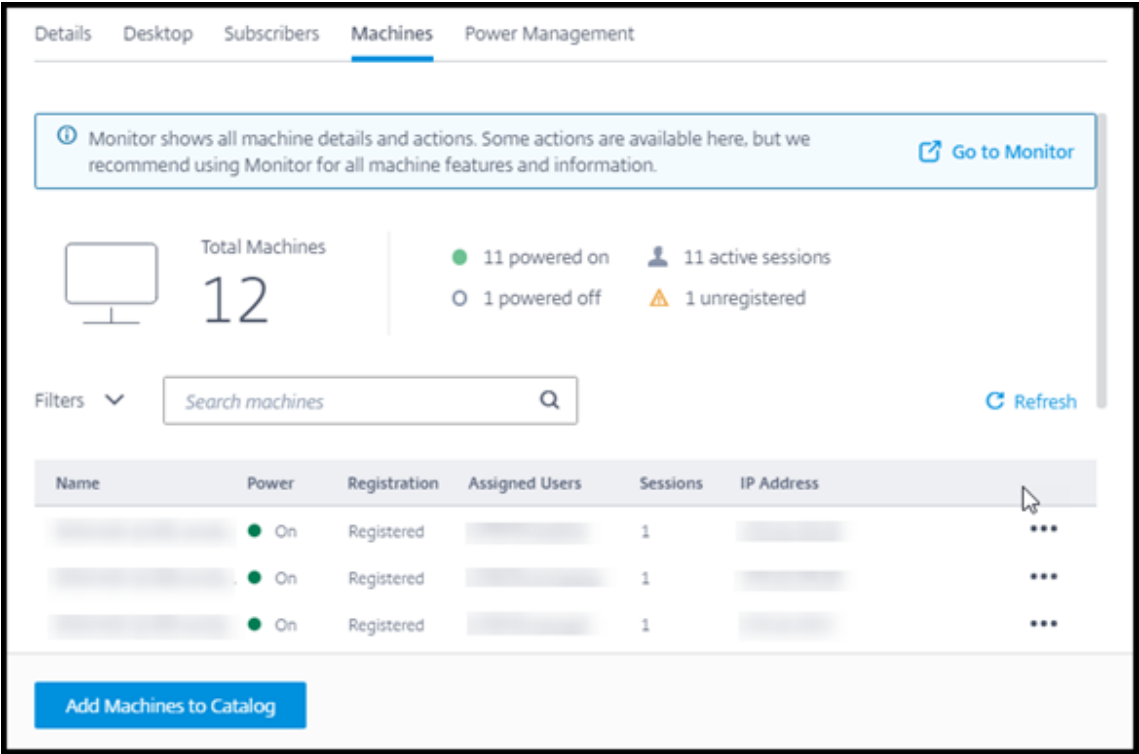
请记住：如果您使用快速部署创建目录，然后使用“完整配置”界面对该目录执行任何管理任务，则无法再使用该目录的“快速部署”界面。

(有关在“完整配置”管理界面中管理目录的信息，请参阅[管理计算机目录](#)。)

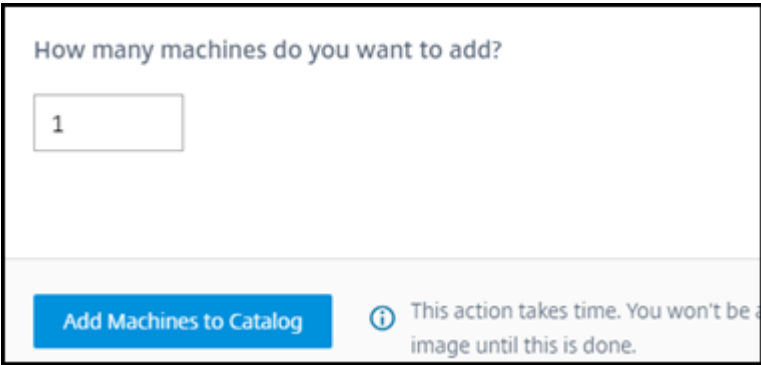
## 向目录中添加计算机

向快速部署目录中添加计算机时，您无法对该目录进行任何其他更改。

1. 在 **Manage** (管理) > **Quick Deploy** (快速部署) 中，单击目录的条目中的任意位置。
2. 在 **Machines** (计算机) 选项卡上，选择 **Add Machines to Catalog** (向目录中添加计算机)。



3. 输入要向目录中添加的计算机数量。



4. (仅当目录已加入域时才有效。) 键入 Citrix DaaS (以前称为 Citrix Virtual Apps and Desktops 服务) 帐户的用户名和密码。

5. 选择 **Add Machines to Catalog** (向目录中添加计算机)。

不能减少目录的计算机数量。但是，您可以使用电源管理计划设置来控制打开电源的计算机数量，或者从计算机选项卡中删除单个计算机。有关从计算机选项卡中删除计算机的信息，请参阅管理目录中的计算机。

### 更改每台计算机的会话数

更改每台多会话计算机的会话数会影响用户的体验。增加此值会减少分配给并发会话的计算资源。

建议：观察使用数据，以确定用户体验与成本之间的适当平衡。

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，选择包含多会话计算机的目录。
2. 在 **Details**（详细信息）选项卡上，选择 **Sessions per Machine**（每台计算机的会话）旁边的 **Edit**（编辑）。
3. 输入每台计算机的新会话数。
4. 选择 **Update Number of Sessions**（更新会话数量）。
5. 确认您的请求。

此更改不会影响当前会话。将最大会话数更改为低于计算机的当前活动会话的值时，新值将通过正常减少活动会话来实现。

如果在更新过程开始之前出现故障，目录的 **Details**（详细信息）显示屏将保留正确的会话数。如果在更新过程中出现故障，显示屏将指示您想要的会话数。

### 管理目录中的计算机

注意：

**Manage**（管理）> **Quick Deploy**（快速部署）中的许多操作还可以从快速部署的 **Monitor**（监视）选项卡中获取。

要从 **Manage**（管理）> **Quick Deploy**（快速部署）中选择操作，请执行以下操作：

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，单击目录的条目中的任意位置。
2. 在 **Machines**（计算机）选项卡上，找到要管理的计算机。在该计算机的省略号菜单中，选择所需的操作：
  - **Restart**（重新启动）：重新启动选定的计算机。
  - **Start**（启动）：启动选定的计算机。仅当计算机关闭电源时，此操作才可用。
  - **Shutdown**（关闭）：关闭选定的计算机。仅当计算机已打开电源时，此操作才可用。
  - **Turn maintenance mode on/off**（打开/关闭维护模式）：为所选计算机打开维护模式（如果已关闭）或关闭维护模式（如果已打开）。默认情况下，计算机的维护模式处于关闭状态。

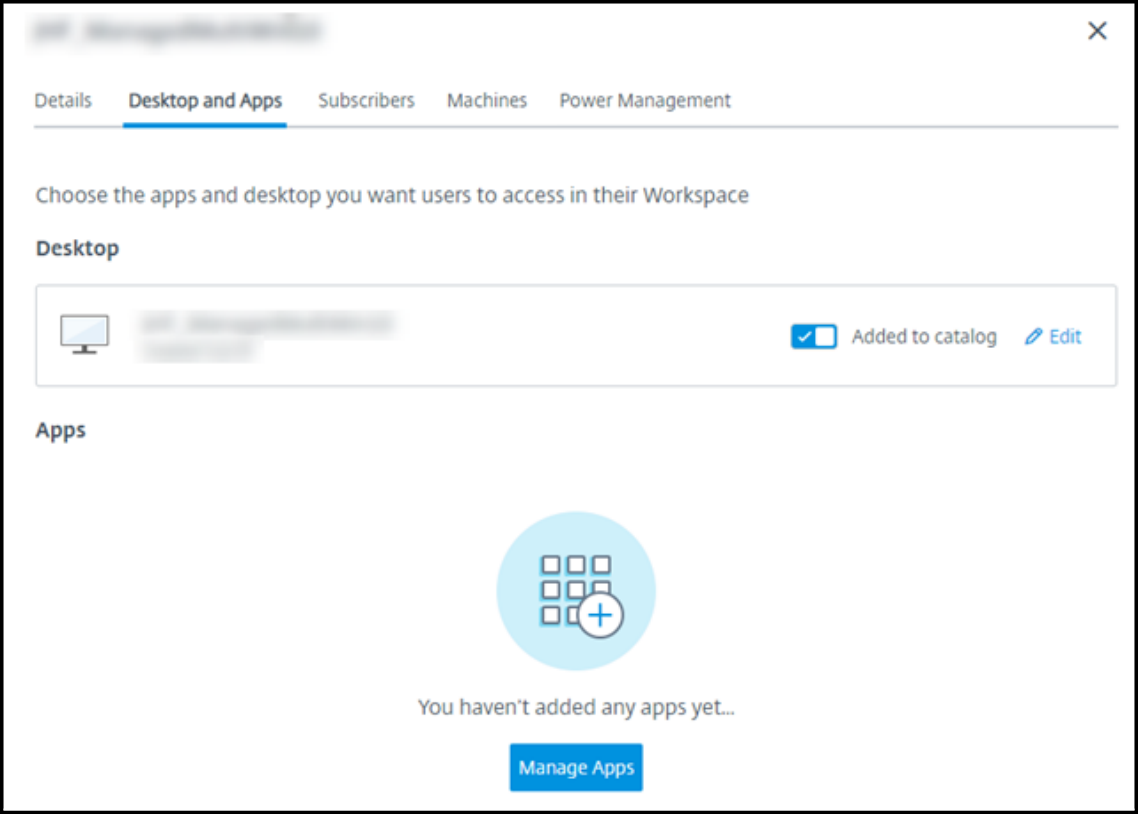
打开维护模式将阻止连接到该计算机的新连接。用户可以连接到该计算机上的现有会话，但他们无法在该计算机上启动新会话。

在应用修补程序之前或进行故障排除时，可以将计算机置于维护模式。
  - **Delete**（删除）：删除选定的计算机。仅当计算机的会话计数为零时，此操作才可用。确认删除。

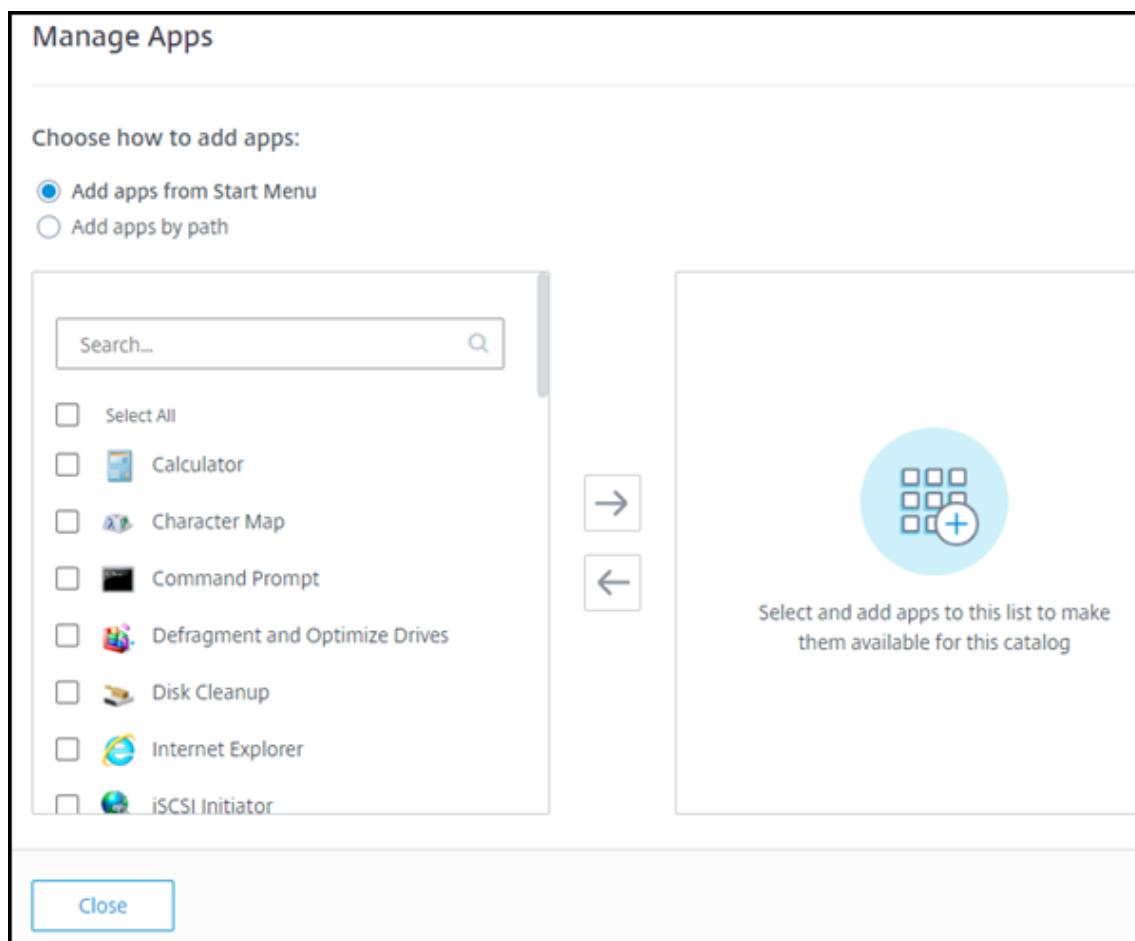
删除计算机后，计算机上的所有数据都将被删除。
  - **Force restart**（强制重新启动）：强制重新启动选定的计算机。仅当计算机的 **Restart**（重新启动）操作失败时才能选择此操作。

向目录中添加应用程序

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，单击目录的条目中的任意位置。
2. 在 **Desktop and Apps**（桌面和应用程序）选项卡上，选择 **Manage Apps**（管理应用程序）。



3. 选择添加应用程序的方式：从目录中的计算机的开始菜单中，或者从计算机上的其他路径中。
4. 要从开始菜单中添加应用程序，请执行以下操作：



- 在左侧栏中选择可用的应用程序。（使用搜索可定制应用程序列表。）在列之间选择向右箭头。选定的应用程序将移动到右侧列。
- 同样，要删除应用程序，请在右侧列中进行选择。选择两个列之间的向左箭头。
- 如果开始菜单具有同一应用程序的多个版本，并且名称相同，则只能添加一个。要添加该应用程序的另一个版本，请编辑该版本以更改其名称。然后您可以添加该版本的应用程序。

5. 要按路径添加应用程序，请执行以下操作：



**Manage Apps**


Choose how to add apps:

☐ Add apps from Start Menu

☒ Add apps by path

Enter the App Details Displayed to Users

App Name \*

 [Change Icon](#) ⓘ

Description

Enter the App Parameters


Path \*

Command Line Parameters:

Working Directory:

→

←



Select and add apps to this list to make them available for this catalog

Close

- 输入应用程序的名称。这是用户在 Citrix Workspace 中看到的名称。
- 显示的图标是用户在 Citrix Workspace 中看到的图标。要选择另一个图标，请选择 **Change icon**（更改图标）并导航到要显示的图标。
- （可选）输入应用程序的说明。
- 输入应用程序的路径。此字段为必填字段。或者，添加命令行参数和工作目录。有关命令行参数的详细信息，请参阅将参数传递到已发布的应用程序。

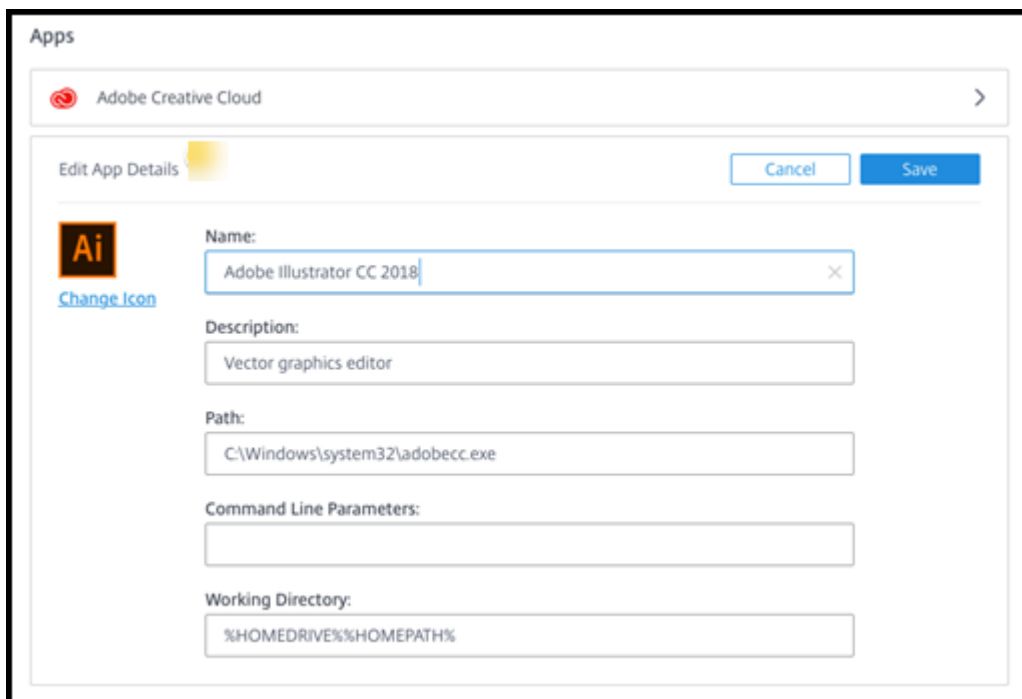
6. 完成后，选择 **Close**（关闭）。

在 Windows Server 2019 VDA 上，在配置期间和用户的工作区中，某些应用程序图标可能无法正确显示。解决方法如下：在发布应用程序后，编辑应用程序，然后使用 **Change icon**（更改图标）功能分配正确显示的其他图标。

在目录中编辑应用程序

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，单击目录的条目中的任意位置。
2. 在 **Desktop and Apps**（桌面和应用程序）选项卡上，单击包含要编辑的应用程序的行中的任意位置。

## 3. 选择铅笔图标。



## 4. 在以下任意字段中键入更改：

- **Name**（名称）：用户在 Citrix Workspace 中看到的名称。
- 说明
- **Path**（路径）：可执行文件的路径。
- 命令行参数：有关详细信息，请参阅将参数传递到已发布的应用程序。
- 工作目录

5. 要更改用户在 Citrix Workspace 中看到的图标，请选择 **Change icon**（更改图标）并导航到要显示的图标。6. 完成后，选择 **Save**（保存）。

## 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，百分号和星号（用双引号引起）会附加在命令行的末尾。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。请在该路径两侧添加双引号，并在百分号和星号两侧添加另一组双引

号。在路径的右引号与百分比和星号的左引号之间添加一个空格。

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" "%*`

## 从目录中删除应用程序

从目录中删除应用程序不会将其从计算机中删除。它只是阻止其出现在 Citrix Workspace 中。

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，单击目录的条目中的任意位置。
2. 在 **Desktop and Apps**（桌面和应用程序）选项卡上，选择要删除的应用程序旁边的垃圾桶图标。

## 删除目录

删除目录时，目录中的所有计算机都将永久销毁。无法撤消删除目录。

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，单击目录的条目中的任意位置。
2. 在 **Details**（详细信息）选项卡上，选择 **Delete Catalog**（删除目录）。
3. 确认删除。

为了帮助识别必须删除的剩余 Active Directory 计算机帐户，可以下载计算机和 Cloud Connector 名称的列表。

## 管理电源管理计划

电源管理计划会影响目录中的所有计算机。计划提供：

- 最佳用户体验：计算机可在需要时供用户使用。
- 安全性：在指定时间间隔内保持空闲状态的桌面会话将断开连接，这要求用户在其工作区中启动新会话。
- 成本管理和节能：仍处于空闲状态的带桌面的计算机已关闭电源。计算机已打开电源以满足计划和实际需求。

可以在创建自定义目录时或稍后配置电源计划。如果未选择或配置任何计划，会话结束时计算机将关闭电源。

使用快速创建创建目录时，无法选择或配置电源计划。默认情况下，快速创建目录使用“Cost Saver”（成本节省程序）预设计划。可以稍后为该目录选择或配置不同的计划。

计划管理包括：

- 了解计划包含的信息
- 创建计划

计划中的信息

下图显示了包含多会话计算机的目录的计划设置。包含单会话（随机或静态）计算机的目录的设置略有不同。

DetailsDesktop and AppsSubscribersMachinesPower Management

Presets

Cost Saver

General

Disconnect desktop sessions when idle

After 15 Minutes

Log Off Disconnected Sessions

After 15 Minutes

Power Off Delay

After 30 Minutes

Work hours

Time Zone

(UTC-05:00) Eastern Time (US & Canada)

Power on machines

SUNMONTUEWEDTHUFRI

SAT

Start

End

Capacity buffer

10%

Minimum running machines

1

After-hours

Capacity buffer

10%

Minimum running machines

1

Save Changes

电源管理计划包含以下信息。

预设计划 Citrix DaaS 提供几个预设计划。您还可以配置和保存自定义计划。尽管您可以删除自定义预设，但不能删除 Citrix 提供的预设。

**时区** 与打开电源的计算机设置一起使用，根据所选时区确定工作时间和下班时间。

此设置适用于所有计算机类型。

**打开计算机的电源：工作时间和下班时间** 构成工作时间的每周的天数和一天中的开始-停止时间。这通常表示您希望打开计算机电源的时间间隔。超出这些时间间隔的任何时间都被视为下班时间。多个计划设置允许您为工作时间和下班时间输入单独的值。其他设置始终适用。

此设置适用于所有计算机类型。

**空闲时断开桌面会话的连接** 在断开会话连接之前，桌面可以保持空闲状态（未使用）的时间。断开会话连接后，用户必须转到 **Workspace** 并重新启动桌面。这是一项安全设置。

此设置适用于所有计算机类型。一个设置始终适用。

**关闭空闲桌面的电源** 在关闭电源之前，计算机可以保持断开连接的时间。关闭计算机电源后，用户必须转到 **Workspace** 并重新启动桌面。这是一种省电设置。

例如，假设您希望桌面在空闲 10 分钟后断开连接。然后，如果计算机保持断开连接 15 分钟，则将关闭计算机的电源。

如果 Tom 停止使用其桌面并离开去参加一个小时的会议，10 分钟后桌面将断开连接。再过 15 分钟，计算机将关闭电源（总共 25 分钟）。

从用户的角度来看，这两种空闲设置（断开连接和关闭电源）具有相同的效果。如果 Tom 离开桌面 12 分钟或 1 个小时，他必须从 **Workspace** 重新启动桌面。两个计时器的差异影响提供桌面的虚拟机的状态。

此设置适用于单会话（静态或随机）计算机。可以输入工作时间和下班时间的值。

**注销断开连接的会话** 在关闭会话之前，计算机可以保持断开连接的时间。

此设置适用于多会话计算机。一个设置始终适用。

**关机延迟** 计算机在符合关闭电源条件之前必须打开电源的最短时间（以及其他标准）。此设置可以防止计算机在不稳定的会话需求期间反复打开和关闭。

此设置适用于多会话计算机，并始终应用。

**运行的最少计算机数** 必须保持打开电源的计算机数量，而无论其处于空闲状态或断开连接多长时间。

此设置适用于随机和多会话计算机。可以输入工作时间和下班时间的值。

**容量缓冲区** 容量缓冲区通过保持计算机的缓冲区打开电源，有助于应对突然激增的需求。缓冲区是按当前会话需求的百分比指定的。例如，如果有 100 个活动会话，容量缓冲区为 10%，Citrix DaaS 将为 110 个会话提供容量。在工作时间或向目录中添加新计算机时可能会出现需求激增的情况。

较低的值会降低成本。更高的值有助于确保优化的用户体验。启动会话时，用户不必等待额外的计算机打开电源。

如果有足够的计算机来支持目录中所需的已打开电源的计算机数量（包括容量缓冲区），则会关闭额外的计算机的电源。关闭电源可能是因为非高峰时间、会话注销或目录中的计算机较少。关闭计算机电源的决定必须符合以下标准：

- 计算机已打开电源但未处于维护模式。
- 计算机已注册为可用或在打开电源后等待注册。
- 计算机没有活动的会话。剩余的任何会话都已结束。（计算机在空闲超时期限内处于空闲状态。）
- 计算机已打开电源至少“X”分钟，其中“X”是为目录指定的断电延迟。

在静态目录中，在分配了目录中的所有计算机后，容量缓冲区不会在打开或关闭计算机电源方面发挥作用。

此设置适用于所有计算机类型。可以输入工作时间和下班时间的值。

#### 创建电源管理计划

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，单击目录的条目中的任意位置。
2. 在 **Power Management**（电源管理）选项卡上，确定任何预设计划（在顶部菜单中）是否满足您的需求。选择一个预设以查看其使用的值。如果要使用预设，请将其保持选中状态。
3. 如果更改任何字段（例如天、时间或时间间隔）中的值，预设选择将自动更改为 **Custom**（自定义）。星号表示自定义设置尚未保存。
4. 为自定义计划设置所需的值。
5. 选择顶部的 **Custom**（自定义），然后将当前设置另存为新预设。输入新预设的名称，然后选择复选标记。
6. 完成后，选择 **Save Changes**（保存更改）。

稍后，您可以使用 **Presets**（预设）菜单中的铅笔或垃圾桶图标来编辑或删除自定义预设。不能编辑或删除常见预设。

#### 相关信息

- [使用新映像更新目录](#)
- [在目录中添加和删除用户](#)

#### 快速部署中的 **Azure** 订阅

August 14, 2023

简介

在快速部署中创建目录或构建映像时，可以从可用的 Azure 订阅中进行选择。快速部署支持 Citrix 托管 Azure 订阅以及您自己的客户托管 Azure 订阅。

- 要使用自己的 Azure 订阅，首先要将一个或多个订阅导入（添加）到 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）中。该操作使 Citrix DaaS 能够访问您的 Azure 订阅。
- 使用 Citrix 托管 Azure 订阅不需要执行任何订阅配置。但是，除了 Citrix DaaS 外，Citrix 托管 Azure 订阅仅在您[订购 Citrix Azure Consumption Fund](#) 时可用。

某些 Citrix DaaS 功能会有所差别，具体取决于目录是使用 Citrix 托管 Azure 订阅还是使用自己的 Azure 订阅。

Citrix 托管 Azure 订阅	你自己的 Azure 订阅
支持加入域或未加入域的计算机。	仅支持加入域的计算机。
支持快速创建和自定义创建目录。	仅支持自定义创建目录。
创建目录和映像时始终可用。	在创建目录之前，必须将 Azure 订阅添加到 Citrix DaaS 中。
对于用户身份验证，支持 Citrix 托管 Azure Active Directory 或自己的 Active Directory。	可以连接自己的 Active Directory 和 Azure Active Directory。
网络连接选项包括 无连接。	网络连接选项仅包括您自己的虚拟网络。
使用 Azure VNet 对等互连连接到您的资源时，必须在 Citrix DaaS 中创建一个 VNet 对等连接。	选择现有的虚拟网络。
从 Azure 导入映像时，您可以指定映像的 URI。	导入映像时，可以在 Azure 订阅中选择 VHD 或浏览存储。
可以在客户的 Azure 订阅中创建堡垒计算机以对计算机进行故障排除。	无需创建堡垒计算机，因为您已经可以访问订阅中的计算机。

查看 **Azure** 订阅

要查看 Azure 订阅详细信息，请从 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Cloud Subscriptions**（云订阅）。然后选择一个订阅条目。

- **Details**（详细信息）页面包括计算机的数量，以及使用订阅的目录和映像的编号和名称。
- “资源位置” 页面列出了使用订阅的资源位置。

添加客户管理的 **Azure** 订阅

必须在创建目录或构建使用该订阅的映像之前将其添加到 Citrix DaaS，才能使用客户管理的 Azure 订阅。添加 Azure 订阅时有两种选择：

- 如果您是目录的全局管理员并且拥有订阅的所有者权限：只需向您的 Azure 帐户进行身份验证即可。
- 如果您不是全局管理员并且拥有订阅的所有者权限：在将订阅添加到 Citrix DaaS 之前，在 Azure AD 中创建 Azure 应用程序，然后将该应用程序添加为订阅的贡献者。向 Citrix DaaS 中添加该订阅时，需要提供相关的应用程序信息。

如果您是全局管理员，请添加客户管理的 **Azure** 订阅

此任务需要目录的全局管理员权限，以及订阅的所有者权限。

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Cloud Subscriptions**（云订阅）。
2. 选择 **Add Azure subscription**（添加 Azure 订阅）。
3. 在 **Add Subscriptions**（添加订阅）页面上，选择 **Add your Azure subscription**（添加您的 Azure 订阅）。
4. 选择允许 Citrix DaaS 代表您访问 Azure 订阅的按钮。
5. 选择 **Authenticate Azure Account**（身份验证 Azure 帐户）。您被带到 Azure 登录页面。
6. 输入您的 Azure 凭据。
7. 您将自动返回到 Citrix DaaS。 **Add Subscription**（添加订阅）页面列出了发现的 Azure 订阅。如果需要，使用搜索框筛选列表。选择一个或多个订阅。完成后，选择 **Add Subscriptions**（添加订阅）。
8. 确认您要添加所选订阅。

展开订阅时，将列出您选择的 Azure 订阅。创建目录或映像时，可以选择添加的订阅。

如果您不是全局管理员，则添加客户管理的 **Azure** 订阅

当您不是全局管理员时，添加 Azure 订阅是由两部分组成的过程：

- 在向 Citrix DaaS 中添加订阅之前，请在 Azure AD 中创建一个应用程序，然后将该应用程序添加为订阅的贡献者。
- 使用有关您在 Azure 中创建的应用程序的信息向 Citrix DaaS 中添加订阅。

在 **Azure AD** 中创建应用程序并将其添加为贡献者

1. 在 Azure AD 中注册新应用程序：
  - a) 在浏览器中，导航到 <https://portal.azure.com>。
  - b) 在左上角的菜单中，选择 **Azure Active Directory**。
  - c) 在 **Manage**（管理）列表中，选择 **App registrations**（应用程序注册）。
  - d) 选择 **+ New registration**（+ 新注册）。
  - e) 在 **注册申请** 页面上，提供以下信息：



- 名称：输入连接名称
- 应用程序类型：选择 **Web app /API**
- 重定向 **URI**：留空

f) 选择创建。

2. 创建应用程序的私有访问密钥并添加角色分配：

- a) 从上一步中，选择 应用程序注册 以查看详细信息。
- b) 记下 **Application ID**（应用程序 ID）和 **Directory ID**（目录 ID）。稍后您将在向 Citrix DaaS 中添加订阅时使用此选项。
- c) 在 **Manage**（管理）下，选择 **Certificates & secrets**（证书和密码）。
- d) 在 客户端密码 页面上，选择 **+** 新客户端密钥。
- e) 在 添加客户端密码 页面上，提供描述并选择过期间隔。然后选择 **Add**（添加）。
- f) 记下客户端密码值。稍后您将在向 Citrix DaaS 中添加订阅时使用此选项。
- g) 选择要链接（添加）到 Citrix DaaS 的 Azure 订阅，然后选择 **Access control (IAM)**（访问控制 (IAM)）。
- h) 在 **Add a role assignment**（添加角色分配）框中，选择 **Add**（添加）。
- i) 在 添加角色分配 选项卡上，选择以下选项：
  - **Role**（角色）：贡献者
  - 分配访问权限：Azure AD 用户、组或服务主体
  - 选择：之前创建的 Azure 应用程序的名称。
- j) 选择保存。

将您的订阅添加到 **Citrix DaaS** 您需要在 Azure AD 中创建的应用程序中的应用程序 ID、目录 ID 和客户端密码值。

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Cloud Subscriptions**（云订阅）。
2. 选择 **Add Azure subscription**（添加 Azure 订阅）。
3. 在 **Add Subscriptions**（添加订阅）页面上，选择 **Add your Azure subscriptions**（添加您的 Azure 订阅）。
4. 选择 我拥有具有订阅贡献者角色的 **Azure** 应用程序。
5. 输入在 Azure 中创建的应用程序的租户 ID（目录 ID）、客户端 ID（应用程序 ID）和客户端密码。
6. 选择 **Select your subscription**（选择您的订阅），然后选择所需的订阅。

稍后，从 Citrix DaaS 控制板中的订阅的 **Details**（详细信息）页面中，可以更新客户端密钥或从省略号菜单中替换 Azure 应用程序。

如果 Citrix DaaS 在添加 Azure 订阅后无法访问该订阅，则不允许使用多个目录电源管理和单个计算机操作。一条消息再次提供了用于添加订阅的选项。如果订阅最初是使用 Azure 应用程序添加的，则可以替换 Azure 应用程序。

## 添加 Citrix 托管 Azure 订阅

Citrix 托管 Azure 订阅支持一定数量的计算机。（在这种情况下，计算机是指安装了 Citrix VDA 的 VM。这些计算机将应用程序和桌面交付给用户。它不包括资源位置中的其他计算机，例如 Cloud Connector。）

如果你的 Citrix 托管 Azure 订阅很可能很快达到限制，并且你有足够的 Citrix 许可证，则可以申请另一个 Citrix 托管 Azure 订阅。接近限制时，控制板将显示通知。

如果使用该 Citrix 托管 Azure 订阅的所有目录的计算机总数超过限制，则无法创建目录（或将计算机添加到目录中）。

例如，假设每个 Citrix 托管 Azure 订阅的假设限制为 1000 台计算机。

- 假设您有两个目录（**Cat1** 和 **Cat2**）具有相同的 Citrix 托管 Azure 订阅。**Cat1** 当前包含 500 台计算机，**Cat2** 包含 250 台计算机。
- 在规划未来容量需求时，您可以向**Cat2**中添加 200 台计算机。Citrix 托管 Azure 订阅现在支持 950 台计算机（**Cat 1** 中包含 500 台计算机，**Cat 2** 中包含 450 台计算机）。仪表板指示订阅已接近其限制。
- 当您还需要 75 台计算机时，不能使用该订阅创建包含 75 台计算机的目录（或向现有目录中添加 75 台计算机）。这将超过订阅限制。相反，你请求另一个 Citrix 托管 Azure 订阅。然后，您可以使用该订阅创建目录。

当你有多个 Citrix 托管 Azure 订阅时：

- 这些订阅之间没有任何共享。
- 每个订阅都有唯一的名称。
- 在以下情况下，你可以在 Citrix 托管 Azure 订阅（以及已添加的任何客户管理的 Azure 订阅）中进行选择：
  - 创建目录。
  - 构建或导入映像。
  - 创建 VNet 对等连接或 SD-WAN 连接。

要求：

- 你必须拥有足够的 Citrix 许可证才能保证添加另一个 Citrix 托管 Azure 订阅。使用上一个假设示例，如果你有 2,000 个 Citrix 许可证，预计通过 Citrix 托管订阅部署至少 1,500 台计算机，则可以添加另一个 Citrix 托管 Azure 订阅。

要添加 Citrix 托管 Azure 订阅：

1. 请与 Citrix 代表联系以请求另一个 Citrix 托管 Azure 订阅。当您可以继续时会收到通知。
2. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Cloud Subscriptions**（云订阅）。
3. 选择 **Add Azure subscription**（添加 Azure 订阅）。
4. 在 **Add Subscriptions**（添加订阅）页面上，选择 **Add a Citrix Managed Azure subscription**（添加 Citrix 托管 Azure 订阅）。
5. 在 **Add a Citrix Managed Subscription**（添加 Citrix 托管订阅）页面上，选择页面底部的 **Add Subscription**（添加订阅）。

如果在创建 Citrix 托管 Azure 订阅期间收到错误的通知，请联系 Citrix 支持。

## 删除 **Azure** 订阅

在删除 Azure 订阅之前，必须删除使用该订阅的所有目录和映像。

如果您有一个或多个 Citrix 托管 Azure 订阅，则无法删除所有这些订阅。必须至少保留一个订阅。

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Cloud Subscriptions**（云订阅）。
2. 选择订阅条目。
3. 在 **Details**（详细信息）选项卡上，选择 **Remove Subscription**（删除订阅）。
4. 选择 **Authenticate Azure Account**（身份验证 Azure 帐户）。您被带到 Azure 登录页面。
5. 输入您的 Azure 凭据。
6. 您将自动返回到 Citrix DaaS。确认删除，然后选择 **Yes, Delete Subscription**（是，删除订阅）。

## 更新过期的客户端机密

当订阅的客户端机密到期时，您无法为其创建计算机目录，并且订阅的条目中会显示警报。要解决此问题，您有两种选择：

- 更新正在使用的 Azure 应用程序的客户端密钥
- 切换到具有有效到期日期的 Azure 应用程序

### 更新正在使用的 **Azure** 应用程序的客户端密钥

要继续使用现有 Azure 应用程序访问 Azure 资源，请按照以下步骤操作：

1. 在 Azure 中，为正在使用的 Azure 应用程序创建客户端机密。记下新机密和过期日期以备将来使用。有关更多信息，请参阅[在 Azure 中创建应用程序机密](#)。
2. 在 DaaS 中，向订阅提供新创建的机密信息。详细步骤如下所示：
  - a) 在 Citrix DaaS for Azure 中的“管理”>“**Azure** 快速部署”控制板中，展开右侧的云订阅。
  - b) 单击需要机密更新的订阅。
  - c) 在出现的订阅页面上，单击 **Azure** 应用程序详细信息窗格中的省略号菜单，然后选择“更新客户端机密”。
  - d) 在“更新客户端机密”页面上，键入新的客户端机密和机密过期日期。
  - e) 单击“更新机密”。

### 切换到具有有效到期日期的 **Azure** 应用程序

要切换到有效的 Azure 应用程序以访问 Azure 资源，请使用以下步骤获取必要的应用程序信息并将其提供给订阅：

1. 在 Azure 中，获取有效的 Azure 应用程序并记下其详细信息。确保为新 Azure 应用程序分配了“贡献者”角色。有关更多信息，请参阅[在 Azure AD 中创建应用程序并将其添加为贡献者](#)。
2. 在 DaaS 中，向订阅提供 Azure 应用程序的详细信息。详细步骤如下所示：

- a) 在 Citrix DaaS for Azure 中的“管理” > “**Azure** 快速部署”控制板中，展开右侧的云订阅。
- b) 单击需要机密更新的订阅。
- c) 在出现的订阅页面上，单击 **Azure** 应用程序详细信息 窗格中的省略号菜单，然后选择“替换 **Azure** 应用程序”。
- d) 在替换 **Azure** 应用程序页面上，在服务主体的目录 (租户) ID、应用程序 (客户端) ID、客户端机密和机密过期日期的相应字段中键入新的 Azure 应用程序详细信息。
- e) 单击“替换应用程序”。

## 快速部署中的映像

March 30, 2024

创建目录以交付桌面或应用程序时，将使用映像（与其他设置一起）作为创建计算机的模板。

快速部署提供了一组准备好的映像，您可以选择在快速部署中构建和自定义映像。也可以从 Azure 订阅导入（添加）映像。

## Citrix 准备的映像

快速部署提供了 Citrix 准备的几个映像：

- Windows 10 Enterprise（单会话）
- Windows 10 Enterprise 虚拟桌面（多会话）
- 带 Office 365 ProPlus 的 Windows 10 Enterprise 虚拟桌面（多会话）
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Linux Ubuntu（单会话和多会话）

Citrix 准备的映像安装了最新的 Citrix Virtual Delivery Agent (VDA) 和故障排除工具。VDA 是用户的计算机与管理 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）的 Citrix Cloud 基础结构之间的通信机制。Citrix 提供的映像带有 **CITRIX** 符号。

Citrix 准备的映像可在 Citrix DaaS 的“完整配置”界面中不可用。

也可以从 Azure 导入和使用自己的映像。

## 在快速部署中使用映像的方法

您可以：

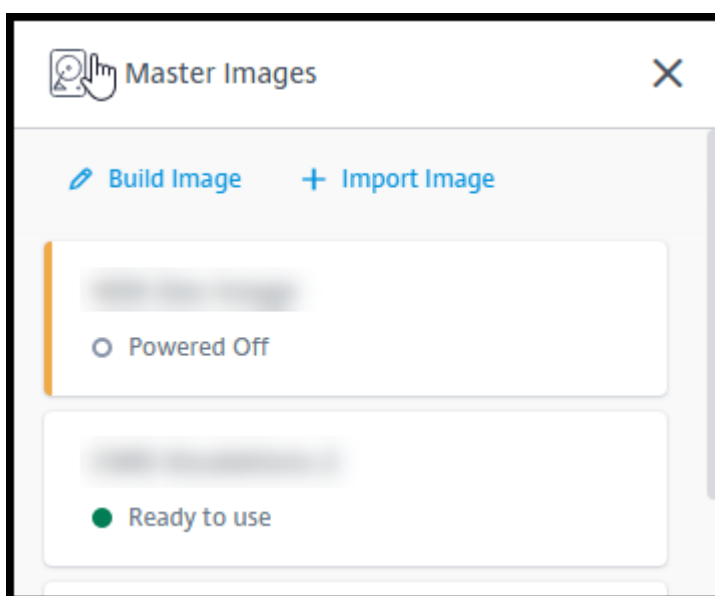
- 创建目录时使用 **Citrix** 准备的映像。建议仅对概念证明部署使用此选项。
- 使用 **Citrix** 准备的映像创建另一个映像。创建新映像后，您可以通过添加用户需要的应用程序和其他软件对其进行自定义。然后，您可以在创建目录时使用该自定义映像。
- 从 **Azure** 导入映像。从 Azure 导入映像后，可以在创建目录时使用该映像。

或者，您可以使用该映像创建新映像，然后通过添加应用程序对其进行自定义。然后，您可以在创建目录时使用该自定义映像。

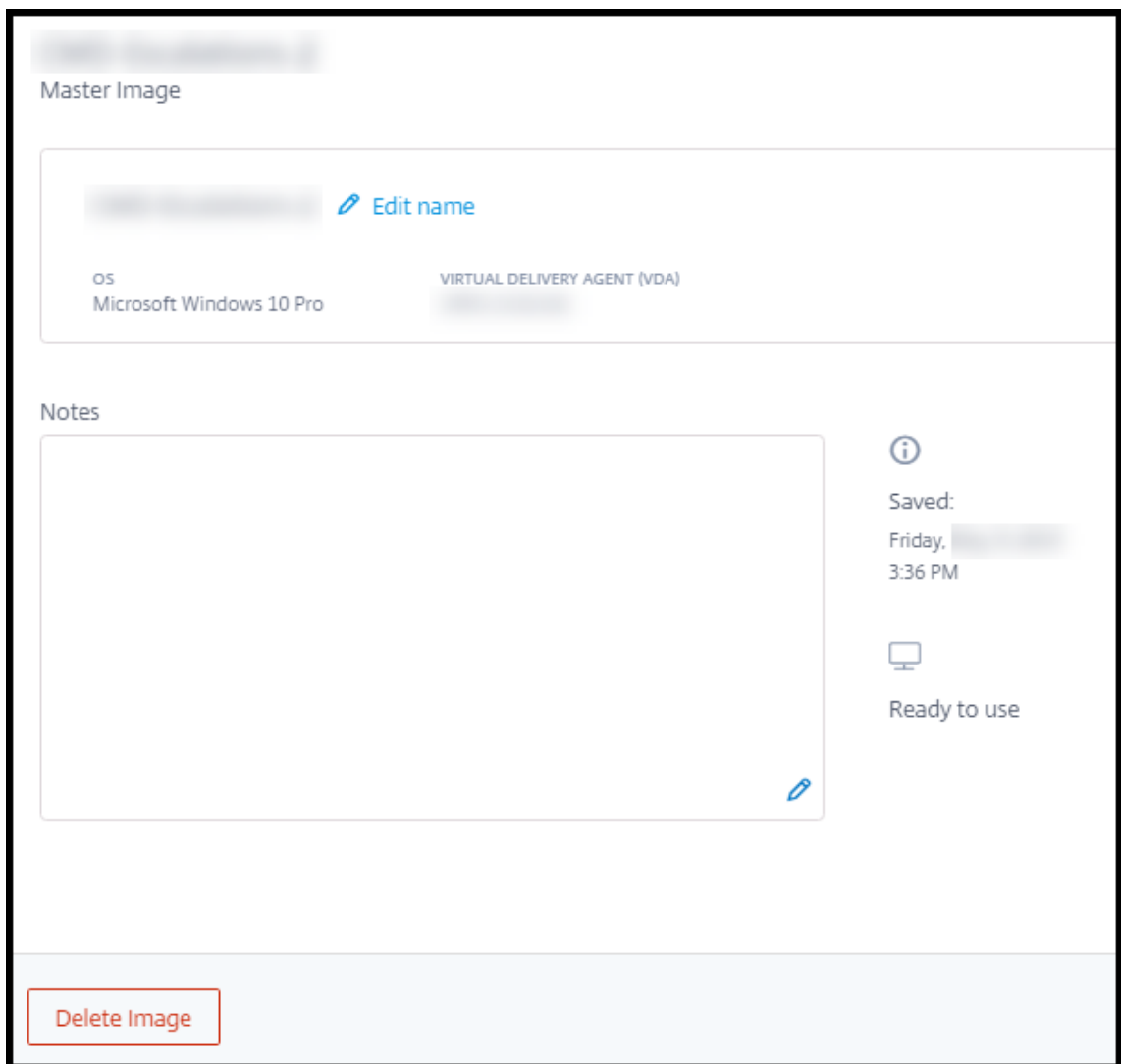
创建目录时，Citrix DaaS 将验证映像是否使用有效的操作系统，并安装 Citrix VDA 和故障排除工具（以及其他检查）。

### 显示映像信息

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Master Images**（主映像）。显示屏列出了 Citrix 准备的映像以及您导入的任何映像。



2. 选择映像以显示其详细信息。



在详细信息卡中，您可以：

- 更改（编辑）映像的名称。
- 添加和编辑备注（仅适用于您准备或导入的映像，不适用于 Citrix 准备的映像）。
- 删除映像。

## 准备新映像

准备新映像包括创建映像然后对其进行自定义。创建映像时，将创建一个新 VM 以加载新映像。

要求：

- 了解计算机所需的性能特征。例如，运行 CAD 应用程序可能需要与其他办公应用程序不同的 CPU、RAM 和存储。
- 如果您计划使用与本地资源的连接，请在创建映像和目录之前设置该连接。有关详细信息，请参阅[网络连接](#)。

使用 Citrix 准备的 Ubuntu 映像构建新映像时，将为新映像创建 root 用户密码。您可以更改该 root 用户密码，但只能在映像创建和自定义过程中进行更改。（在目录中使用映像后，您无法更改 root 用户密码。）

- 创建映像后，您指定的管理员帐户（映像构建计算机的登录详细信息）将添加到 `sudoers` 组中。
- 在 RDP 到包含新映像的计算机之后，启动终端应用程序并键入 `sudo passwd root`。出现提示时，请提供您在创建映像时指定的密码。验证后，系统会提示您输入 root 用户的新密码。

要创建映像，请执行以下操作：

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Master Images**（主映像）。
2. 选择 **Build Image**（构建映像）。

Name the new master image

Select a master image as base

Subscription

Network connection

Region

Set log-on credentials for the image machine

Login details for image building machine

Performance (the machine that runs the image)

Restricted IP access

+ Add IP addresses

Add Notes

3. 在以下字段中输入值：
- **Name**（名称）：输入新映像的名称。
  - **Master image**（主映像）：选择现有映像。这是用于创建新映像的基础映像。
  - **Subscription**（订阅）：选择 Azure 订阅。

- 网络连接：
  - 如果使用 Citrix 托管 Azure 订阅，请选择 **No connectivity**（无连接）或之前创建的连接。
  - 如果使用自己的客户管理的 Azure 订阅，请选择资源组、虚拟网络和子网。然后添加域详细信息：FQDN、OU、Citrix DaaS 帐户名称和凭据。
- 区域：（仅适用于 **No connectivity**（无连接）。）选择要在其中创建包含映像的计算机的区域。
- **Logon credentials for image machine**（映像计算机的登录凭据）：稍后将在连接 (RDP) 到包含新映像的计算机时使用这些凭据，以便您能够安装应用程序和其他软件。
- **Machine performance**（计算机性能）：这是运行映像的计算机的 CPU、RAM 和存储信息。选择符合您的应用程序要求的计算机性能。
- **Restricted IP access**（受限 IP 访问）：如果要限制对特定地址的访问，请选择 **Add IP addresses**（添加 IP 地址），然后输入一个或多个地址。添加地址后，选择 **Done**（完成）以返回到 **Build image**（构建映像）卡。
- **Notes**（备注）：最多可以选择添加 1024 个字符的备注。创建映像后，您可以从映像的详细信息显示中更新备注。
- **Local domain join**（本地域加入）：指明是否要加入本地 Active Directory 域。
  - 如果选择 **Yes**（是），请输入 FQDN、OU、Citrix DaaS 帐户名称和凭据。
  - 如果选择 **No**（否），请输入主机的凭据。

4. 完成后，选择 **Build Image**（构建映像）。

构建映像最多可能需要 30 分钟。在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Master Images**（主映像）以查看当前状态（例如 **Building image** 或 **Ready to customize**）。

后续操作：连接到新映像并对其进行自定义。

#### 连接到新映像并对其进行自定义

创建新映像后，其名称将添加到映像列表中，状态为 **Ready to customize**（或类似词句）。要自定义该映像，首先需要下载 RDP 文件。使用该文件连接到映像时，可以将应用程序和其他软件添加到映像中。

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Master Images**（主映像）。选择要连接到的映像。
2. 选择 **Download RDP file**（下载 RDP 文件）。RDP 客户端下载。

如果创建映像计算机后不久没有对其进行 RDP，则可能会关闭该映像计算机的电源。这样可以节省成本。出现这种情况时，请选择 **Power On**（打开电源）。
3. 启动下载的 RDP 客户端。它会尝试自动连接到包含新映像的计算机的地址。出现提示时，输入您在创建映像时指定的凭据。



4. 连接到计算机后，添加或删除应用程序、安装更新并完成任何其他自定义工作。

请勿通过 Sysprep 准备映像。

5. 完成自定义新映像后，返回到 **Master Images**（主映像）框并选择 **Finish build**（完成构建）。新映像会自动经过验证测试。

稍后，创建目录时，新映像将包含在您可以选择的映像列表中。

在 **Manage**（管理）> **Quick Deploy**（快速部署）中，右侧的映像显示屏显示了使用每个映像的目录和计算机数量。

注意：

准备好映像后，您无法对其进行编辑。必须创建一个新映像（可以选择使用以前的映像作为起点），然后更新新映像。

## 从 Azure 导入映像

从 Azure 中导入具有 Citrix VDA 和用户所需应用程序的映像时，可以使用该映像创建目录或替换现有目录中的映像。

### 导入的映像的要求

注意：

Citrix DaaS 不支持导入与 Azure 第 2 代 VM 关联的磁盘。

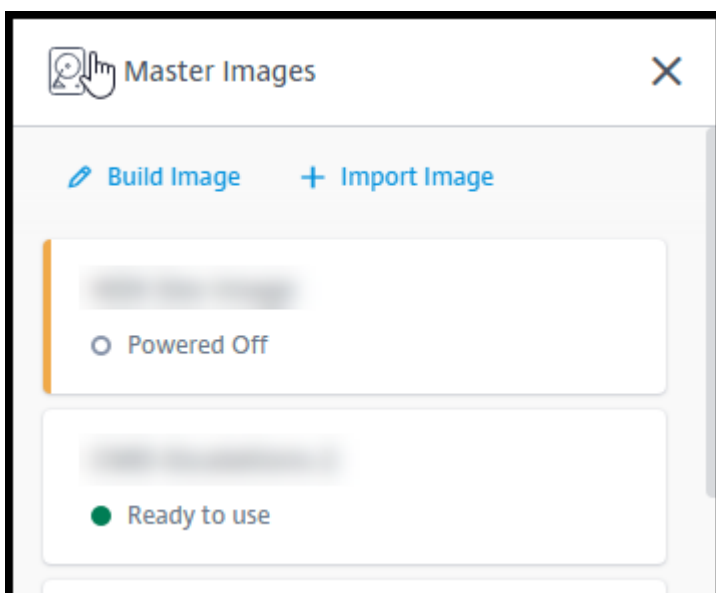
Citrix 会对导入的映像运行验证测试。在准备要导入到 Citrix DaaS 中的映像时，请确保满足以下要求。

- 支持的操作系统：映像必须是[受支持的操作系统](#)。要检查 Windows 操作系统版本，请运行 `Get-WmiObject Win32_OperatingSystem`。
- **Supported generation**（支持的世代）：仅支持第 1 代 VM。
- **Not generalized**（不具有通用性）：映像不得具有通用性。
- **No configured Delivery Controllers**（没有已配置的 Delivery Controller）：确保映像中未配置 Citrix Delivery Controller。请务必清除以下注册表项。
  - HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\ListOfDDCs
  - HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\ListOfDDCs
  - HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\FarmGUID
  - HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\FarmGUID
- **Personality.ini file**（Personality.ini 文件）：`personality.ini` 文件必须存在于系统驱动器上。
- **Valid VDA**（有效的 VDA）：映像必须安装比 7.11 更新的 Citrix VDA。

- Windows: 要进行检查, 请使用 `Get HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Citrix Virtual Desktop Agent`。有关安装指南, 请参阅在映像上安装 Windows VDA。
- Red Hat Enterprise Linux 和 Ubuntu: 有关安装指南, 请参阅 [产品文档](#)。
- **Azure Virtual Machine Agent** (Azure 虚拟机代理): 导入映像之前, 请确保映像上安装了 Azure 虚拟机代理。有关详细信息, 请参阅 Microsoft 文章 [Azure Virtual Machine Agent overview](#) (Azure 虚拟机代理概述)。

使用快速部署导入映像

1. 在 **Manage** (管理) > **Quick Deploy** (快速部署) 中, 展开右侧的 **Master Images** (主映像)。



2. 选择 **Import Image** (导入映像)。

Choose how to import your image

☒ Browse storage account  
☐ Use Azure public URL

Subscription  
[Dropdown menu]

Choose resource group  
[Dropdown menu]

Storage account  
[Dropdown menu]

Choose master image  
[Dropdown menu]

Master image type  
☒ Windows  
☐ Linux

Name the new master image  
[Text field: Eg. "Windows 10 + My Apps"]

Add Notes  
[Text area: Enter notes here (up to 1024 characters). You can see and change them in the image's details.]

3. 选择如何导入映像。

- 对于托管磁盘，请使用导出功能生成 SAS URL。将过期时间设置为 7200 秒或更长时间。
- 对于存储帐户中的 VHD，请选择以下选项之一：
  - 为 VHD 文件生成 SAS URL
  - 将块存储容器的访问级别更新为 blob 或容器。然后，获取文件的 URL。

4. 如果选择了 **Browse storage account**（浏览存储帐户）：

- a) 按顺序选择订阅 > 资源组 > 存储帐户 > 映像。
- b) 为映像命名。

5. 如果选择了 **Azure public URL**（Azure 公用 URL）：

- a) 输入 Azure 生成的 VHD 的 URL。有关指导，请选择指向 Microsoft 文档[从 Azure 下载 Windows VHD](#) 的链接。
- b) 选择订阅。（只有选择客户管理的订阅时才能导入 Linux 映像。）
- c) 为映像命名。

6. 完成后，选择 **Import Image**（导入映像）。

使用新映像更新快速部署目录

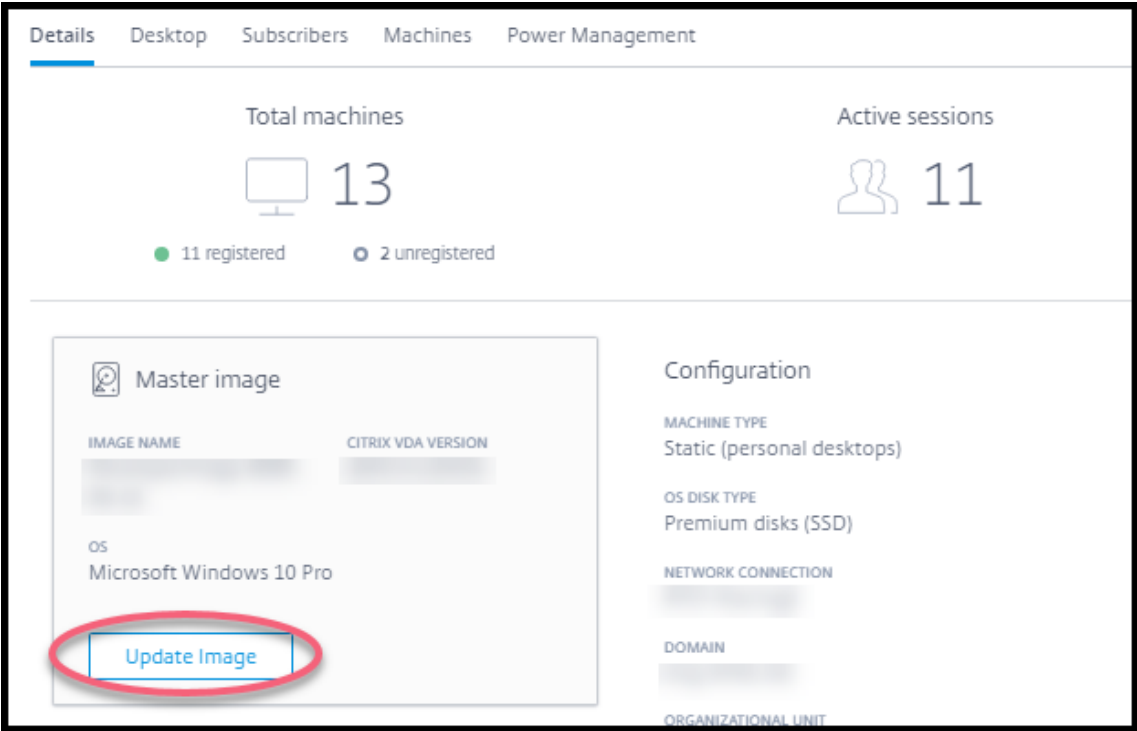
目录类型决定了更新目录时更新哪些计算机。

- 对于随机目录，目录中当前的所有计算机都将使用最新的映像进行更新。如果向该目录中添加更多桌面，这些桌面将基于最新的映像。
- 对于静态目录，目录中当前的计算机不会使用最新的映像进行更新。目录中当前的计算机继续使用创建这些计算机时所基于的映像。但是，如果向该目录中添加更多计算机，这些计算机将基于最新的映像。

如果目录的计算机支持 gen2，则可以使用 gen2 映像更新包含具有 gen1 映像的计算机的目录。同样，如果目录的计算机支持 gen1，则可以使用 gen1 映像更新包含 gen2 计算机的目录。

要使用新映像更新目录，请执行以下操作：

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，单击目录的条目中的任意位置。
2. 在 **Details**（详细信息）选项卡上，选择 **Update Image**（更新映像）。



3. 选择一个映像。
4. 对于随机目录或多会话目录：请选择注销时间间隔。Citrix DaaS 完成初始映像处理后，订阅者会收到一条警告，要求保存其工作并从桌面中注销。注销时间间隔表示订阅者在收到消息后会话自动结束之前可以执行操作的时间长度。
5. 选择 **Update Image**（更新映像）。

## 从快速部署中删除映像

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Master Images**（主映像）。
2. 选择要删除的映像。
3. 选择卡底部的 **Delete Image**（删除映像）。确认删除。

## 在映像上安装 **Windows VDA**

在准备要导入到 Citrix DaaS 中的 Windows 映像时，请使用以下步骤。

有关 Linux VDA 安装指南，请参阅 [Linux VDA 产品文档](#)。

1. 在 Azure 环境中，连接到映像 VM（如果您尚未连接）。
2. 可以使用 Citrix Cloud 导航栏上的 **Downloads**（下载）链接下载 VDA。或者，使用浏览器导航到 Citrix DaaS [下载](#) 页面。  
  
将 VDA 下载到 VM 上。桌面（单会话）操作系统和服务端（多会话）操作系统有单独的 VDA 下载包。
3. 通过双击下载的文件启动 VDA 安装程序。此时将启动安装向导。
4. 在 **Environment**（环境）页面上，选择用于使用 MCS 创建映像的选项，然后选择 **Next**（下一步）。
5. 在核心组页面上，选择下一步。
6. 在 **Delivery Controller** 页面上，选择让 **Machine Creation Services** 自动创建，然后选择下一步。如果系统提示，请确认您的选择。
7. 除非 Citrix 另有指示，否则请将默认设置保留在 其他组件（Additional Components）、**Features**（功能）和 **Firewall**（防火墙）页面上。在每个页面上选择 **Next**（下一步）。
8. 在 **Summary**（摘要）页面上，选择 **Install**（安装）。必备项将开始安装。当系统提示重新启动时，同意。
9. VDA 安装将自动继续。必备项安装完成，然后安装组件和功能。在 **Call Home** 页面上，保留默认设置（除非 Citrix 另有指示）。连接后，选择 **Next**（下一步）。
10. 选择完成。计算机会自动重新启动。
11. 为确保配置正确无误，请启动您在 VM 上安装的一个或多个应用程序。
12. 关闭 VM。请勿通过 Sysprep 准备映像。

有关安装 VDA 的详细信息，请参阅[安装 VDA](#)。

## 快速部署中的网络连接

April 19, 2022

### 简介

本文提供了有关在使用 Citrix 托管 Azure 订阅时如何创建与公司资源的网络连接的详细信息。

使用自己的客户托管 Azure 订阅时，无需创建网络连接。

创建快速部署目录时，可以指示用户是否以及如何从 Citrix 桌面和应用程序访问其公司本地网络中的位置和资源。使用连接时，必须先创建连接，然后再创建目录。

使用 Citrix 托管 Azure 订阅时，可以选择：

- 无连接
- Azure VNet 对等互连
- SD-WAN

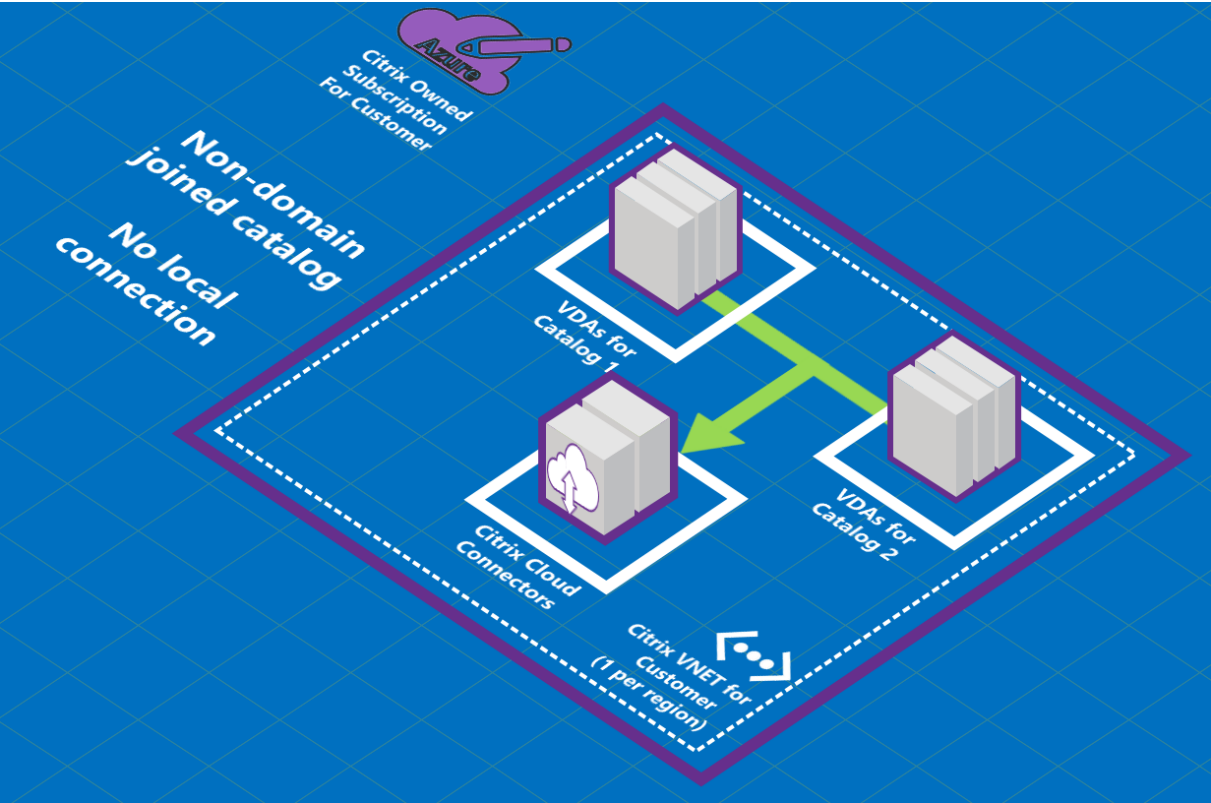
创建目录后，无法更改目录的连接类型。

### 所有网络连接的要求

- 创建连接时，必须具有有效的 [DNS 服务器条目](#)。
- 使用安全 DNS 或第三方 DNS 提供程序时，必须将分配给 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）使用的地址范围添加到允许列表中的 DNS 提供程序的 IP 地址中。该地址范围是在您创建连接时指定的。
- 所有使用连接的服务资源（已加入域的计算机）必须能够到达网络时间协议 (NTP) 服务器，以确保时间同步。

### 无连接

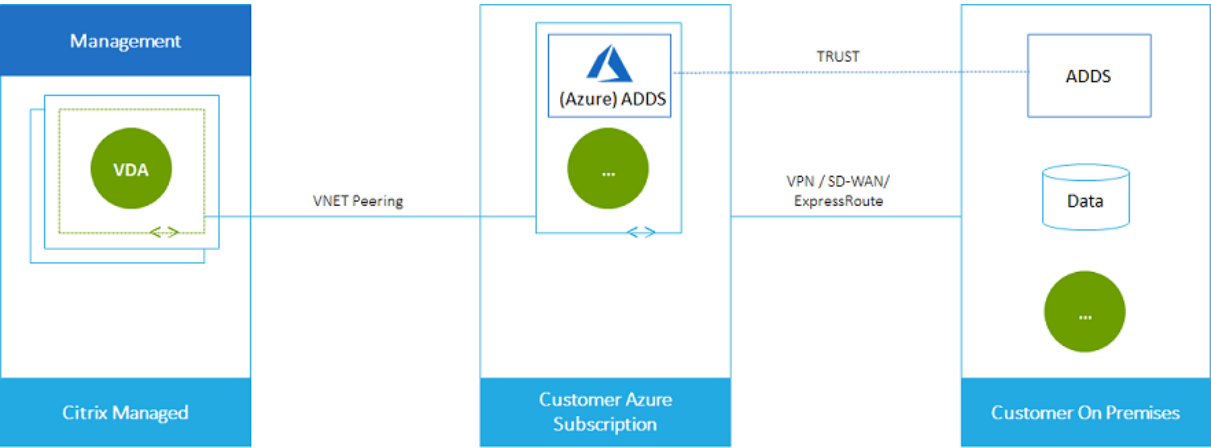
为目录配置了 **No connectivity**（无连接）时，用户将无法访问其本地或其他网络中的资源。这是使用快速创建创建目录时唯一的选择。



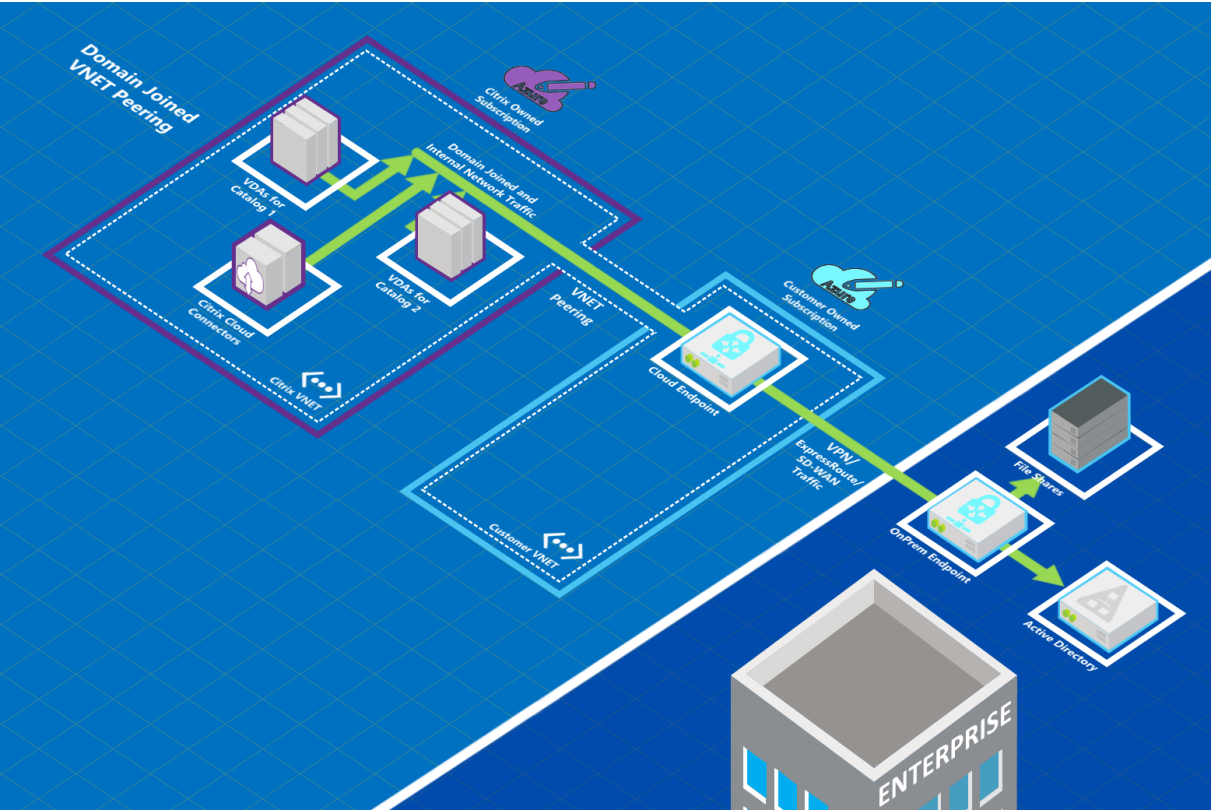
关于 **Azure VNet** 对等互连连接

虚拟网络对等互连无缝连接下面两个 Azure 虚拟网络 (VNet)：您的 VNet 和 Citrix DaaS VNet。对等互连还有助于用户访问您的本地网络中的文件和其他项目。

如下图所示，您可以使用 Azure VNet 对等互连创建从 Citrix 托管 Azure 订阅到贵公司的 Azure 订阅中的 VNet 的连接。



下面是 VNet 对等互连的另一个例证。



创建目录时，用户可以通过加入本地域来访问其网络资源（例如文件服务器）。（也就是说，您加入了文件共享和其他所需资源所在的 AD 域。）您的 Azure 订阅连接到这些资源（在图形中，使用 VPN 或 Azure ExpressRoute）。创建目录时，您需要提供域、OU 和帐户凭据。

重要：

- 请在此服务中使用 Azure VNet 对等互连之前了解其信息。
- 在创建使用 VNet 对等互连连接的目录之前创建 VNet 对等连接。

**Azure VNet 对等互连自定义路由**

自定义或用户定义的路由会覆盖 Azure 的默认系统路由，用于定向 VNet 对等互连中的虚拟机、本地网络和 Internet 之间的流量。如果 Citrix DaaS 资源期望访问某些网络，但某些网络不是通过 VNet 对等互连直接连接的，则可以使用自定义路由。例如，您可以创建自定义路由，将流量强制通过网络设备传入 Internet 或本地网络子网。

要使用自定义路由，请执行以下操作：

- 您必须在 Citrix DaaS 环境中拥有现有的 Azure 虚拟网络网关或网络设备，例如 Citrix SD-WAN。
- 添加自定义路由时，必须使用 Citrix DaaS 的目标 VNet 信息更新公司的路由表，以确保端到端连接。
- 自定义路由将按输入路由的顺序在 Citrix DaaS 中显示。此显示顺序不影响 Azure 选择路由的顺序。

在使用自定义路由之前，请查看 Microsoft 文章 [Virtual network traffic routing](#)（虚拟网络流量路由），了解如何使用自定义路由、下一个跃点类型以及 Azure 如何为出站流量选择路由。



可以在创建 Azure VNet 对等互连连接时添加自定义路由，也可以添加到 Citrix DaaS 环境中的现有路由。准备好在 VNet 对等互连中使用自定义路由时，请参阅本文中的以下部分：

- 对于具有新 Azure VNet 对等互连的自定义路由：创建 Azure VNet 对等连接
- 对于使用现有 Azure VNet 对等互连的自定义路由：管理现有 Azure VNet 对等连接的自定义路由

### Azure VNet 对等互连的要求和准备工作

- Azure 订阅所有者的凭据。这必须是 Azure Active Directory 帐户。此服务不支持其他帐户类型，例如 live.com 或外部 Azure AD 帐户（在不同的租户中）。
- Azure 订阅、资源组和虚拟网络 (VNet)。
- 设置 Azure 网络路由，以便 Citrix 托管 Azure 订阅中的 VDA 可以与您的网络位置通信。
- 将 Azure 网络安全组从您的 VNet 打开到指定的 IP 范围。
- **Active Directory**：对于已加入域的场景，我们建议您在对等互连的 VNet 中运行某种形式的 Active Directory 服务。这利用了 Azure VNet 对等互连技术的低延迟特性。

例如，配置可能包括 Azure Active Directory 域服务 (AADDS)、VNet 中的域控制器 VM 或 Azure AD 连接到您的本地 Active Directory。

启用 AADDS 后，如果不删除托管域，则无法将您的托管域移动到其他 VNet。因此，选择正确的 VNet 来启用托管域非常重要。在继续之前，请查看 Microsoft 文章 [Networking considerations for Azure AD Domain Services](#) (Azure AD 域服务的网络连接注意事项)。

- **VNet IP range** (VNet IP 范围)：创建连接时，必须提供可用的 CIDR 地址空间 (IP 地址和网络前缀)，该空间在网络资源与正在连接的 Azure VNet 中是唯一的。这是分配给 Citrix DaaS 的对等互连 VNet 中的 VM 的 IP 范围。

确保指定的 IP 范围不与您在 Azure 和本地网络中使用的任何地址重叠。

- 例如，如果您的 Azure VNet 的地址空间为 10.0.0.0 /16，请在 Citrix DaaS 中创建 VNet 对等互连连接，例如 192.168.0.0 /24。
- 在此示例中，创建 IP 范围 10.0.0.0 /24 的对等互连连接将被视为重叠的地址范围。

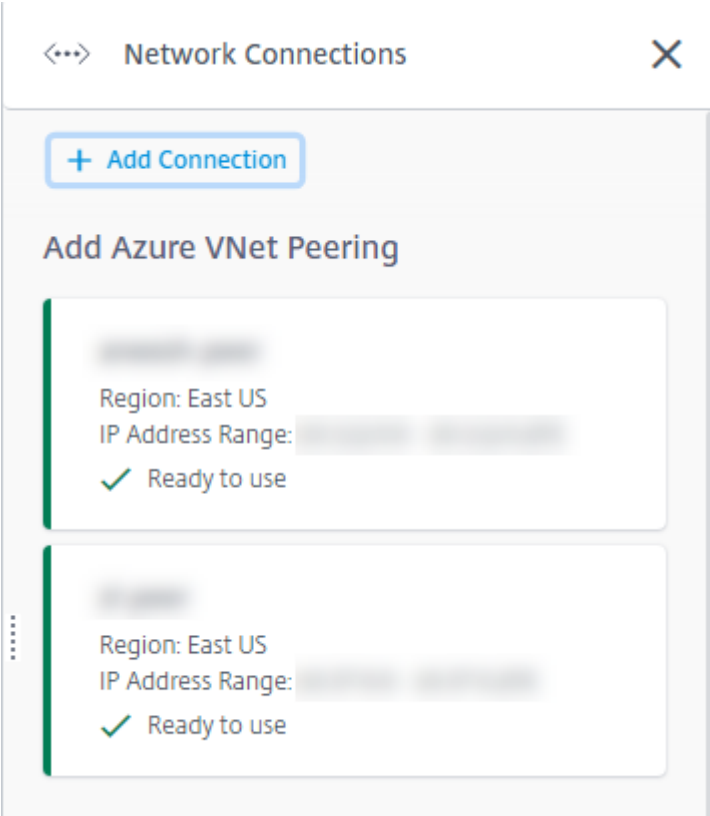
如果地址重叠，VNet 对等互连连接可能无法成功创建。对于站点管理任务，它也不能正常运行。

要了解有关 VNet 对等互连的信息，请参阅以下 Microsoft 文章。

- [虚拟网络对等互连](#)
- [Azure VPN 网关](#)
- [在 Azure 门户中创建站点到站点连接](#)
- [VPN 网关常见问题解答](#) (搜索“重叠”)

创建 **Azure VNet** 对等互连连接

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Network Connections**（网络连接）。  
如果您已设置连接，系统会将其列出。



2. 选择 **Add Connection**（添加连接）。
3. 单击 **Add Azure VNet Peering**（添加 Azure VNet 对等互连）框中的任意位置。

## Add a network connection

Choose how you want to connect to your local network:

**Add Azure VNet Peering**  
Easy setup for Azure customers – Seamlessly connect your Azure virtual network.

4. 选择 **Authenticate Azure Account**（身份验证 Azure 帐户）。


Add Azure VNet Peering

<...>

Citrix managed  
Azure subscription

<...>

Customer owned  
Azure subscription



On-premises  
network resources

What's ahead

Virtual network peering seamlessly connects two Azure virtual networks (VNETs): yours and the Citrix Managed Desktops VNet. Peering also helps enable users to access files and other items from your on-premises networks.

You will need the following:

1. An Azure subscription, resource group, and virtual network (VNet).

2. Credentials for an Azure Resource Manager subscription owner.

3. An available IP address and network prefix (in CIDR format) that is unique among the network resources and the Azure VNETs being connected.

4. For domain-joined scenarios, we recommend that you have some form of Active Directory services running in the peered VNet.

Cancel

Authenticate Azure Account

5. Citrix DaaS 会自动将您引导至 Azure 登录页面对您的 Azure 订阅进行身份验证。登录 Azure（使用全局管理员帐户凭据）并接受条款后，您将返回到连接创建详细信息对话框。

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

636

## Add Azure VNet Peering

Azure VNet peering name

VNet details to peer

Select Azure Subscription

Select Resource Group

Select VNet to Peer

✓ This VNet is in the West US region, which is supported

Is this VNet using an Azure Virtual Network Gateway?

☒ No ☐ Yes

IP address and network prefix to be used by VNet peering ?

⚠ The IP addresses cannot conflict with any existing IP addresses in your network.

/

?

✓ 10.2.0.0 - 10.2.0.255 (251 addresses available for machines)

Do you want to add routes? ?

☒ No ☐ Yes

Cancel

Add VNet Peering

6. 键入 Azure VNet 对等方的名称。
7. 选择 Azure 订阅、资源组以及要建立对等连接的 VNet。
8. 指示选定的 VNet 是否使用 Azure 虚拟网络网关。有关信息，请参阅 Microsoft 文章 [Azure VPN Gateway](#) (Azure VPN 网关)。
9. 如果在上一步中回答 **Yes** (是) (VNet 使用 Azure 虚拟网络网关)，请指示是否要启用虚拟网络网关路由传播。启用后，Azure 会自动学习 (添加) 通过网关建立的所有路由。

您可以稍后在连接的 **Details** (详细信息) 页面上更改此设置。但是，对其进行更改可能会导致路由模式更改和 VDA 流量中断。此外，如果以后将其禁用，则必须手动向 VDA 要使用的网络添加路由。
10. 键入 IP 地址并选择网络掩码。系统将显示要使用的地址范围以及该范围支持的地址数量。确保 IP 范围不会重叠您在 Azure 和本地网络中使用的任何地址。
  - 例如，如果您的 Azure VNet 的地址空间为 10.0.0.0 /16，请在 Citrix DaaS 中创建 VNet 对等互连连接，例如 192.168.0.0 /24。
  - 在此示例中，创建 IP 地址范围为 10.0.0.0 /24 的 VNet 对等互连连接被视为重叠的地址范围。

如果地址重叠，VNet 对等互连连接可能无法成功创建。对于站点管理任务，它也无法正常运行。
11. 指示是否要向 VNet 对等互连连接添加自定义路由。如果选择 **Yes** (是)，请输入以下信息：
  - a) 为自定义路由键入友好名称。
  - b) 输入目标 IP 地址和网络前缀。网络前缀必须介于 16 到 24 之间。
  - c) 为要将流量路由到的位置选择下一个跃点类型。如果选择 **Virtual appliance** (虚拟设备)，请输入设备的内部 IP 地址。

Do you want to add routes? ?

☐ No ☒ Yes

**i** Make sure your company's route tables are updated with the Citrix Managed Desktops VNet information to ensure end-to-end connectivity: 10.2.0.0/24 (provided above).  
Added routes override Azure default routing. Routes apply to all connections from machines using this VNet peering.

Route name

USA-traffic

Destination IP address and network prefix ?

10.2.0.0

/ 24 ?

✓ 10.2.0.0 - 10.2.0.255

Next hop type ?

Virtual appliance

Next hop address ?

10.2.0.124

[+ Add route](#)

有关下一个跃点类型的详细信息，请参阅 Microsoft 文章 [Virtual network traffic routing](#)（虚拟网络流量路由）中的 *Custom routes*（自定义路由）部分。

d) 要为连接创建另一个自定义路由，请选择 **Add route**（添加路由）。

12. 选择 **Add VNet Peering**（添加 VNet 对等互连）。

创建连接后，此连接将在 **Manage**（管理）> **Quick Deploy**（快速部署）控制板右侧的 **Network Connections**（网络连接）> **Azure VNet Peers**（Azure VNet 对等方）下列出。创建目录时，此连接将包含在可用网络连接列表中。



查看 **Azure VNet** 对等互连连接详细信息

Details

Routes

Not in use

Catalogs

0

Machines

0

Images

0

Bastions

0

Region

VNet 1

East US

VNet 2 - CITRIX MANAGED

East US

Allocated Network Space

IP ADDRESS RANGE

IP ADDRESS AVAILABLE FOR MACHINES

DNS SERVERS

Peered Virtual Network Details

VIRTUAL NETWORK

SUBSCRIPTION ID

RESOURCE GROUP

AZURE VIRTUAL NETWORK GATEWAY

Disabled

Delete Connection



1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Network Connections**（网络连接）。
2. 选择要显示的 Azure VNet 对等互连连接。

详细信息包括：

- 使用此连接的目录、计算机、映像和堡垒的数量。
- 区域、分配的网络空间和对等互连的 VNet。
- 当前为 VNet 对等互连连接配置的路由。

管理现有 **Azure VNet** 对等互连连接的自定义路由

可以向现有连接添加新的自定义路由或修改现有的自定义路由，包括禁用或删除自定义路由。

重要

:

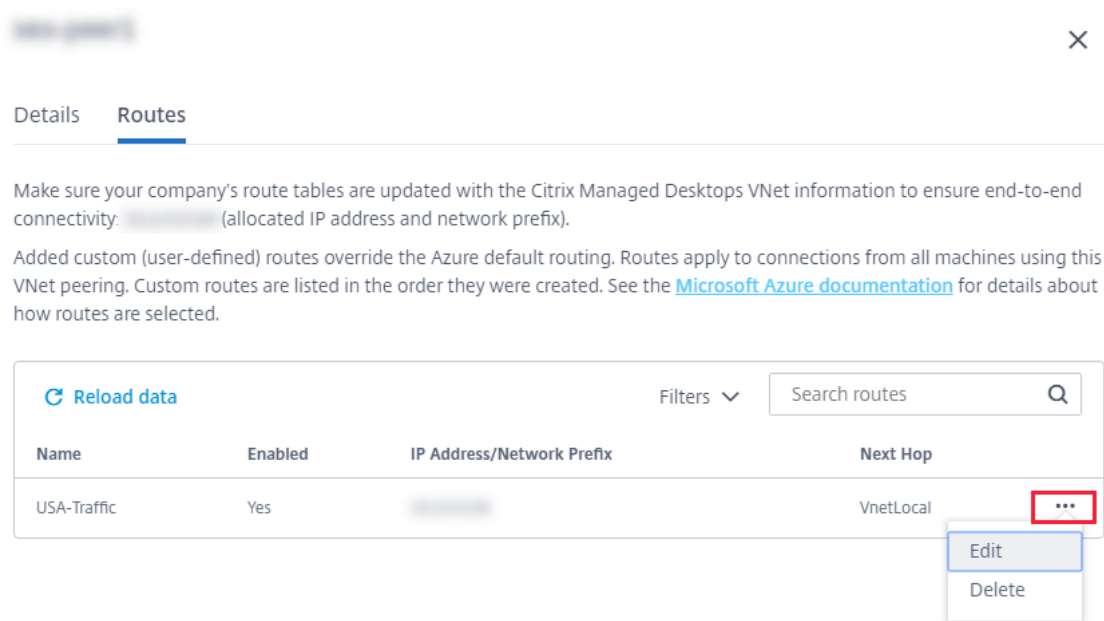
修改、禁用或删除自定义路由会更改连接的流量，并且可能会中断可能处于活动状态的任何用户会话。

要添加自定义路由，请执行以下操作：

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Network Connections**（网络连接）。
2. 选择要删除的连接。
3. 在连接详细信息中，选择 **Routes**（路由），然后选择 **Add Route**（添加路由）。
4. 输入友好名称、目标 IP 地址和前缀以及要使用的下一个跃点类型。如果选择 **Virtual Appliance**（虚拟设备）作为下一个跃点类型，请输入设备的内部 IP 地址。
5. 指示是否要启用自定义路由。默认情况下，自定义路由处于启用状态。
6. 选择 **Add Route**（添加路由）。

要修改或禁用自定义路由，请执行以下操作：

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Network Connections**（网络连接）。
2. 选择要删除的连接。
3. 在连接详细信息中，选择 **Routes**（路由），然后找到要管理的自定义路由。
4. 从省略号菜单中，选择 **Edit**（编辑）。



5. 根据需要对目标 IP 地址和前缀或下一个跃点类型进行任何必要的更改。
6. 要启用或禁用自定义路由，请在 **Enable this route?**（启用此路由？）中，选择 **Yes**（是）或 **No**（否）。
7. 选择保存。

要删除自定义路由，请执行以下操作：

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Network Connections**（网络连接）。
2. 选择要删除的连接。
3. 在连接详细信息中，选择 **Routes**（路由），然后找到要管理的自定义路由。
4. 从省略号菜单中，选择 **Delete**（删除）。
5. 选择 **Deleting a route may disrupt active sessions**（删除路由可能会中断活动的会话），以确认删除自定义路由的影响。
6. 选择 **Delete Route**（删除路由）。

### 删除 Azure VNet 对等互连连接

在删除 Azure VNet 对等互连连接之前，请删除与之关联的所有目录。请参阅[删除目录](#)。

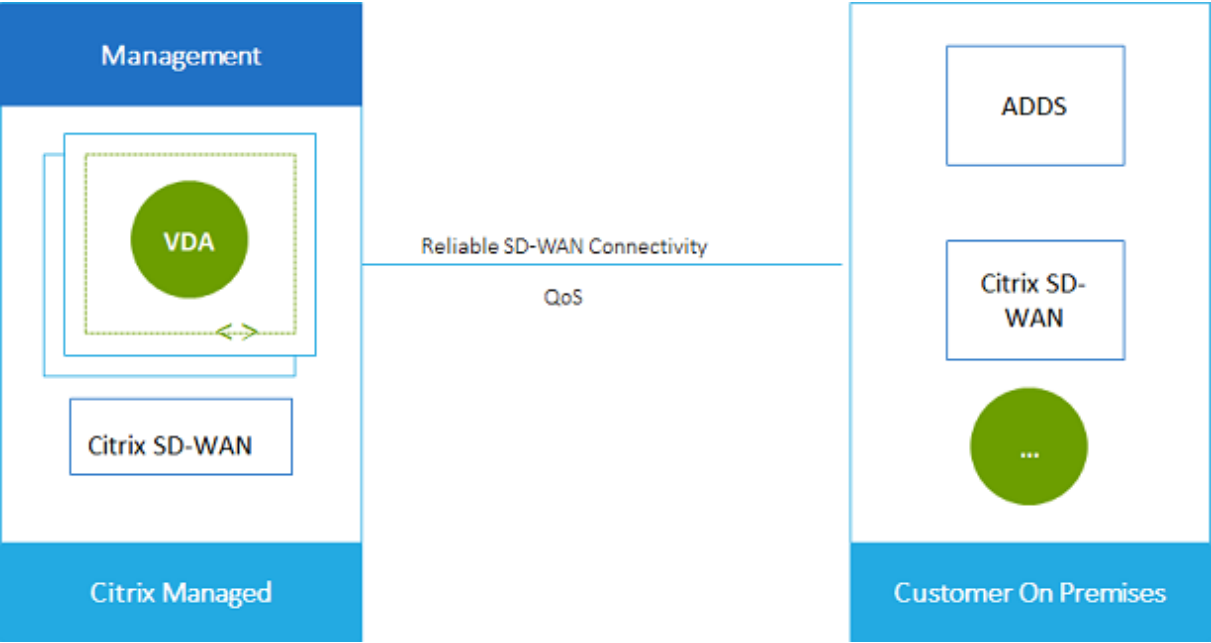
1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Network Connections**（网络连接）。
2. 选择要删除的连接。
3. 从连接详细信息中，选择 **Delete Connection**（删除连接）。

关于 **SD-WAN** 连接

Citrix SD-WAN 优化 Citrix DaaS 所需的所有网络连接。Citrix SD-WAN 与 HDX 技术协同工作，为 ICA 和带外 Citrix DaaS 流量提供了服务质量和连接可靠性。Citrix SD-WAN 支持以下网络连接：

- 用户与其虚拟桌面之间的多流 ICA 连接
- 从虚拟桌面到 Web 站点、SaaS 应用程序和其他云属性的 Internet 访问
- 从虚拟桌面返回访问本地资源，例如 Active Directory、文件服务器和数据库服务器
- 实时/交互流量通过 RTP 从 Workspace 应用程序中的媒体引擎传输到云托管的统一通信服务（例如 Microsoft Teams）
- 客户端从 YouTube 和 Vimeo 等站点提取视频

如下图所示，可以创建从 Citrix 托管 Azure 订阅到您的站点的 SD-WAN 连接。在创建连接过程中，SD-WAN VPX 设备是在 Citrix 托管 Azure 订阅中创建的。从 SD-WAN 的角度来看，该位置被视为分支机构。



**SD-WAN** 连接要求和准备工作

- 如果不满足以下要求，SD-WAN 网络连接选项将不可用。
  - Citrix Cloud 服务授权：Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）和 SD-WAN Orchestrator。
  - 已安装并配置的 SD-WAN 部署。部署必须包括主控制节点 (MCN)（无论是在云端还是本地），并使用 SD-WAN Orchestrator 进行管理。
- VNet IP range (VNet IP 范围)：提供可用的 CIDR 地址空间（IP 地址和网络前缀），该空间在所连接的网络资源中是唯一的。这是分配给 Citrix DaaS 的互连 VNet 中的 VM 的 IP 范围。

确保指定的 IP 范围不与您在云端和本地网络中使用的任何地址重叠。

- 例如，如果您的网络的地址空间为 10.0.0.0 /16，请在 Citrix DaaS 中创建该连接，例如 192.168.0.0 /24。
- 在此示例中，创建 IP 范围 10.0.0.0 /24 的连接将被视为重叠的地址范围。

如果地址重叠，则可能无法成功创建连接。对于站点管理任务，它也不能正常运行。

- 连接配置过程包括您（Citrix DaaS 管理员）和 SD-WAN Orchestrator 管理员必须完成的任务。此外，要完成任务，您需要 SD-WAN Orchestrator 管理员提供的信息。

我们建议您在实际创建连接之前查看本文档中的指南以及 SD-WAN 文档。

## 创建 SD-WAN 连接

### 重要

:

有关 SD-WAN 配置的详细信息，请参阅[适用于 Citrix DaaS 集成的 SD-WAN 配置](#)。

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Network Connections**（网络连接）。
2. 选择 **Add Connection**（添加连接）。
3. 在 **Add a network connection**（添加网络连接）页面上，单击“SD-WAN”框中的任意位置。
4. 下一页总结了接下来的操作。阅读完毕后，选择 **Start Configuring SD-WAN**（开始配置 SD-WAN）。
5. 在 **Configure SD-WAN**（配置 SD-WAN）页面上，输入 SD-WAN Orchestrator 管理员提供的信息。
  - **Deployment mode**（部署模式）：如果选择 **High availability**（高可用性），则会创建两个 VPX 设备（建议用于生产环境）。如果选择 **Standalone**（独立），则会创建一个设备。以后不能更改此设置。要更改到部署模式，必须删除并重新创建分支和所有关联的目录。
  - **Name**（名称）：键入 SD-WAN 站点的名称。
  - **Throughput and number of offices**（吞吐量和办公室数量）：此信息由您的 SD-WAN Orchestrator 管理员提供。
  - **Region**（区域）：将创建 VPX 设备所在的区域。
  - **VDA subnet and SD-WAN subnet**（VDA 子网和 SD-WAN 子网）：此信息由您的 SD-WAN Orchestrator 管理员提供。有关避免冲突的信息，请参阅 SD-WAN 连接要求和准备工作。
6. 完成后，选择 **Create Branch**（创建分支）。
7. 下一页总结了在 **Manage**（管理）> **Quick Deploy**（快速部署）控制板上查找的内容。阅读完毕后，选择 **Got it**（明白了）。
8. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，**Network Connections**（网络连接）下的新 SD-WAN 条目显示了配置过程的进度。当该条目随消息“**Awaiting activation by SD-WAN administrator**”变为橙色时，请通知您的 SD-WAN Orchestrator 管理员。

9. 有关 SD-WAN Orchestrator 管理员任务，请参阅 SD-WAN Orchestrator [产品文档](#)。
10. SD-WAN Orchestrator 管理员完成时，**Network Connections**（网络连接）下的 SD-WAN 条目将变为绿色，并显示消息 “[You can create catalogs using this connection](#)”。

#### 查看 **SD-WAN** 连接详细信息

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Network Connections**（网络连接）。
2. 如果该选项不是唯一的选择，请选择 **SD-WAN**。
3. 选择要显示的连接。

展示内容包括：

- **Details**（详细信息）选项卡：配置连接时指定的信息。
- **Branch Connectivity**（分支机构连接）选项卡：每个分支机构和 MCN 的名称、云连接性、可用性、带宽层、角色和位置。

#### 删除 **SD-WAN** 连接

在删除 SD-WAN 连接之前，请删除与之关联的所有目录。请参阅[删除目录](#)。

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Network Connections**（网络连接）。
2. 如果该选项不是唯一的选择，请选择 SD-WAN。
3. 选择要删除的连接，以展开其详细信息。
4. 在 **Details**（详细信息）选项卡上，选择 **Delete Connection**（删除连接）。
5. 确认删除。

### 快速部署中的用户和身份验证

October 26, 2023

#### 用户身份验证方法

用户必须在登录 Citrix Workspace 时进行身份验证才能启动其桌面或应用程序。

快速部署支持以下用户身份验证方法：

- **Managed Azure AD**（托管 Azure AD）：托管 Azure AD 是 Citrix 提供和管理的 Azure Active Directory (AAD)。您不需要提供自己的 Active Directory 结构。只需将您的用户添加到目录中即可。
- 您的身份提供商：您可以在 Citrix Cloud 中使用任何可用的身份验证方法。

**注意：**

- 远程 PC 访问部署仅使用 Active Directory。有关详细信息，请参阅 [Remote PC Access](#)。
- 如果使用 Azure AD 域服务：Workspace 登录 UPN 必须包含启用 Azure AD 域服务时指定的域名。登录不能为您创建的自定义域使用 UPN，即使该自定义域被指定为主域亦如此。

设置用户身份验证包括以下步骤：

1. 在 Citrix Cloud 和 Workspace 配置中配置用户身份验证方法。
2. 如果您使用托管 Azure AD 进行用户身份验证，请 将用户添加到目录。
3. 将用户添加到目录。

### 在 **Citrix Cloud** 中配置用户身份验证

要在 Citrix Cloud 中配置用户身份验证：

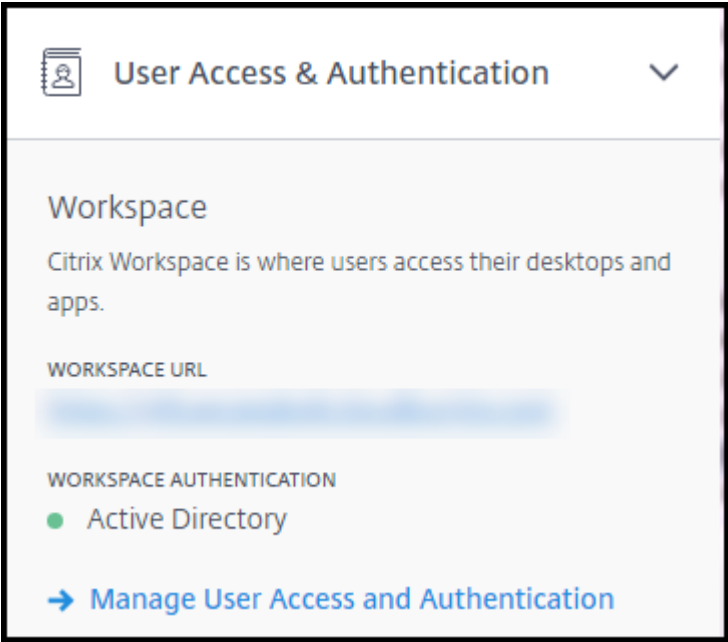
- 连接到要使用的用户身份验证方法。（在 Citrix Cloud 中，您可以“连接”或“断开”与身份验证方法的连接。）
- 在 Citrix Cloud 中，将 Workspace 身份验证设置为使用已连接的方法。

**注意：**

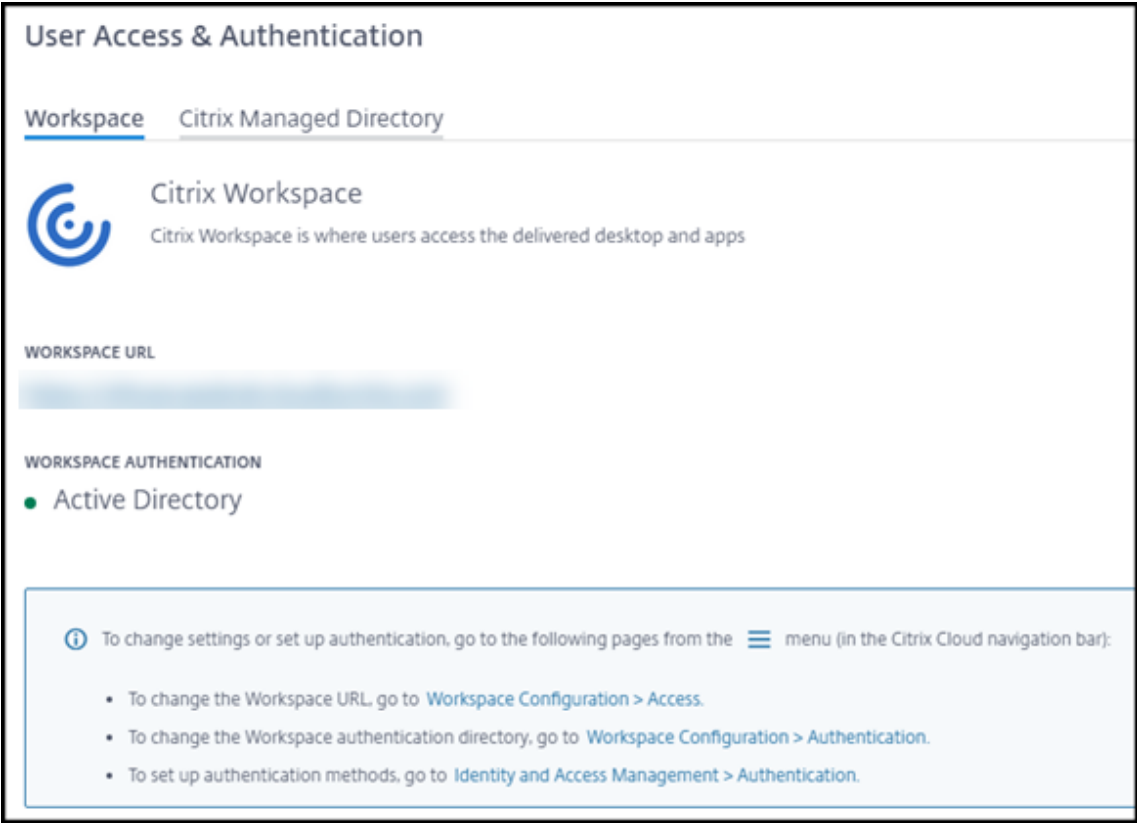
默认情况下，托管 Azure AD 身份验证方法已配置。也就是说，该方法在 Citrix Cloud 中自动连接，并且 Workspace 身份验证将自动设置为使用托管 Azure AD 提供 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）。如果要使用此方法（以前未配置过其他方法），请继续在托管 Azure AD 中添加和删除用户。如果托管 Azure AD 已断开连接，则工作空间身份验证将切换到 Active Directory。如果您想使用其他身份验证方法，请按照以下步骤操作。

要更改身份验证方法，请执行以下操作：

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，选择右侧的 **User Access & Authentication**（用户访问和身份验证）。



2. 选择 **Manage User Access and Authentication**（管理用户访问和身份验证）。选择 **Workspace**（工作区）选项卡（如果尚未选中）。（另一个选项卡指示当前配置了哪种用户身份验证方法。）



3. 点击链接 要设置身份验证方法。该链接将您带到 Citrix Cloud。在省略号菜单中选择所需方法的 连接。
4. 仍在 Citrix Cloud 中时，选择左上角菜单中的“工作区配置”。在 身份验证 选项卡上，选择所需的方法。

后续操作：

- 如果您使用的是托管 Azure AD，请将用户添加到目录。
- 对于所有身份验证方法，请将用户添加到目录。

在托管 **Azure AD** 中添加和删除用户

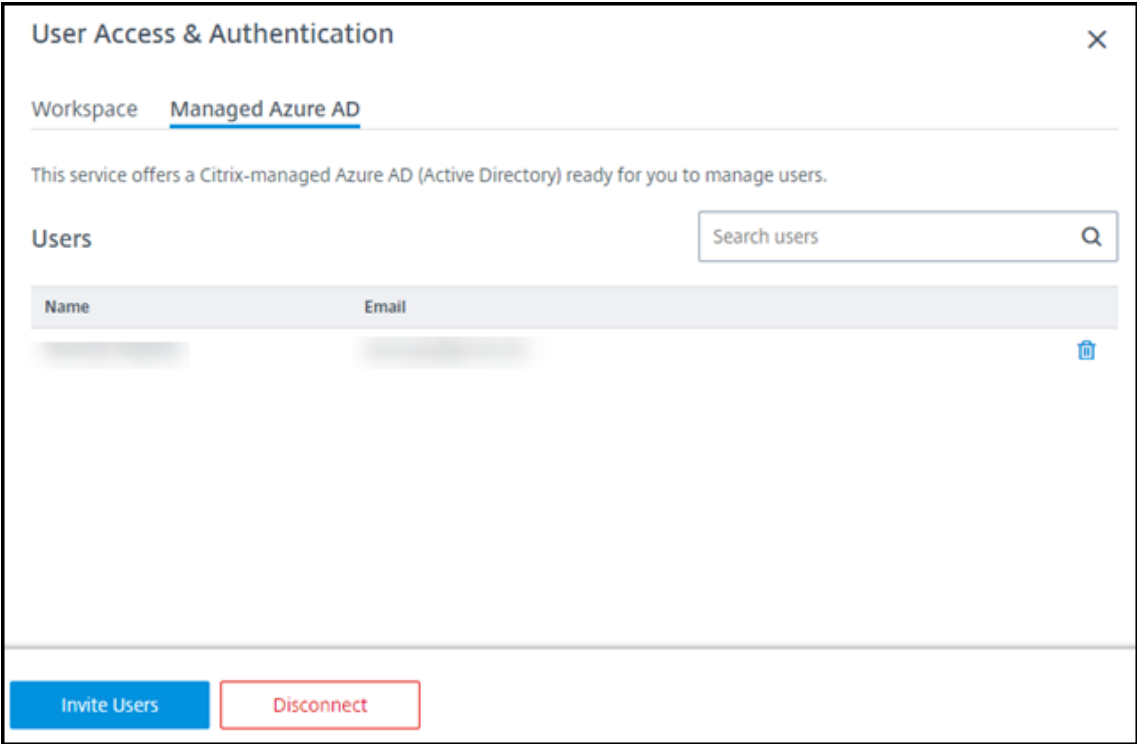
仅当您使用托管 Azure AD 进行 Citrix Workspace 的用户身份验证时，才能完成此过程。

您可以提供用户的姓名和电子邮件地址。然后，Citrix 将通过电子邮件向每个地址发送邀请。该电子邮件指示用户选择将其加入 Citrix 托管 Azure AD 的链接。

- 如果用户已拥有包含您提供的电子邮件地址的 Microsoft 帐户，则使用该帐户。
- 如果用户没有包含电子邮件地址的 Microsoft 帐户，Microsoft 将创建一个帐户。

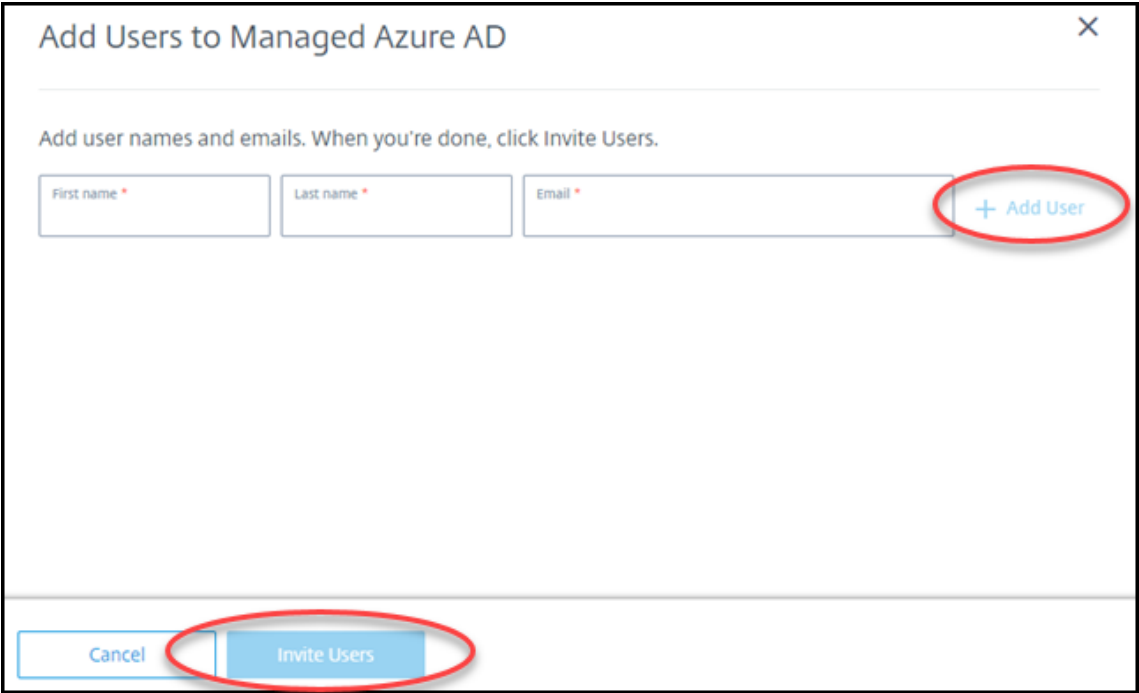
要将用户添加到托管 Azure AD 以及邀请其加入，请执行以下操作：

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **User Access & Authentication**（用户访问和身份验证）。选择 **Manage User Access and Authentication**（管理用户访问和身份验证）。
2. 选择 **Managed Azure AD**（托管 Azure AD）选项卡。
3. 选择 **Invite Users**（邀请用户）。



4. 键入用户的姓名和电子邮件地址，然后选择 **Add User**（添加用户）。



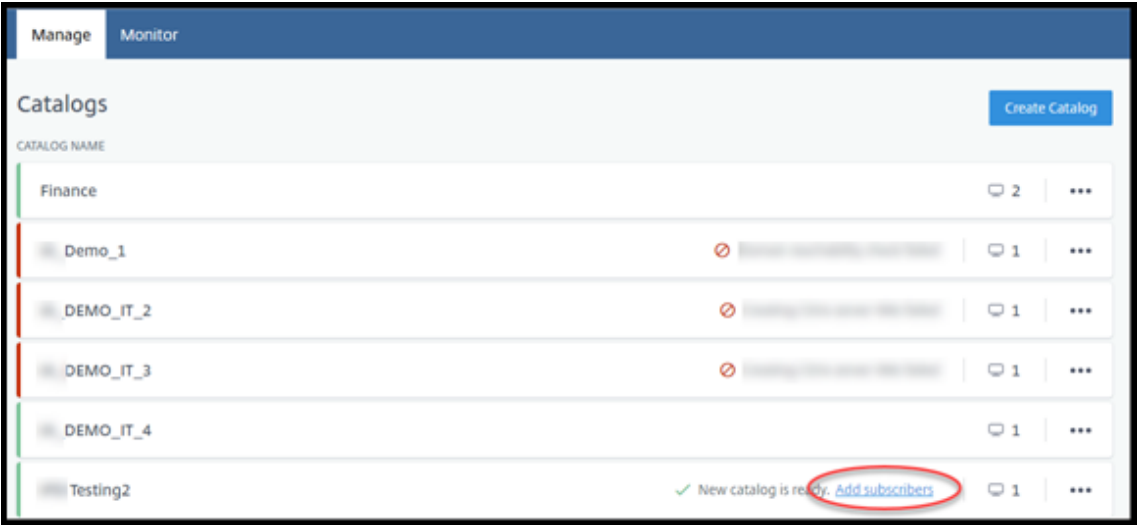


- 5. 重复上述步骤以添加其他用户。
  - 6. 添加完用户信息后，选择卡底部的 **Invite Users**（邀请用户）。
- 要从托管 Azure AD 中删除用户，请选择要从目录中删除的用户名称旁边的垃圾桶图标。确认删除。
- 接下来要做什么：将用户添加到目录

在目录中添加或删除用户

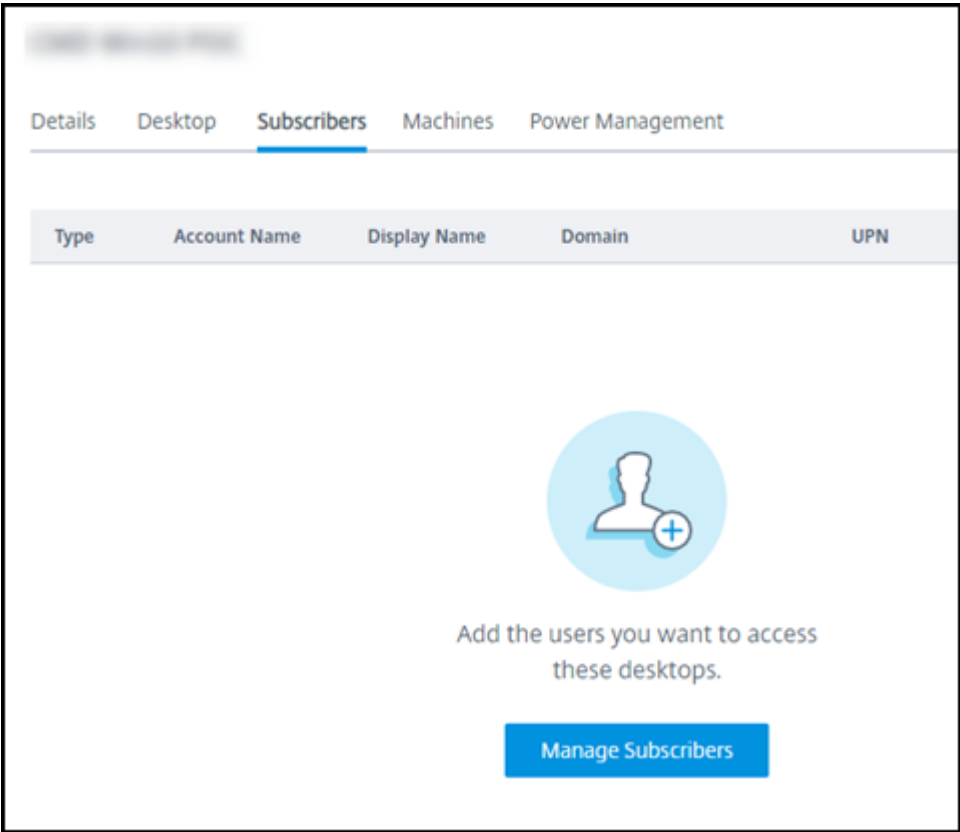
无论使用何种身份验证方法，都请完成此过程。

- 1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，如果尚未向目录中添加任何用户，请选择 **Add subscribers**（添加订阅者）。

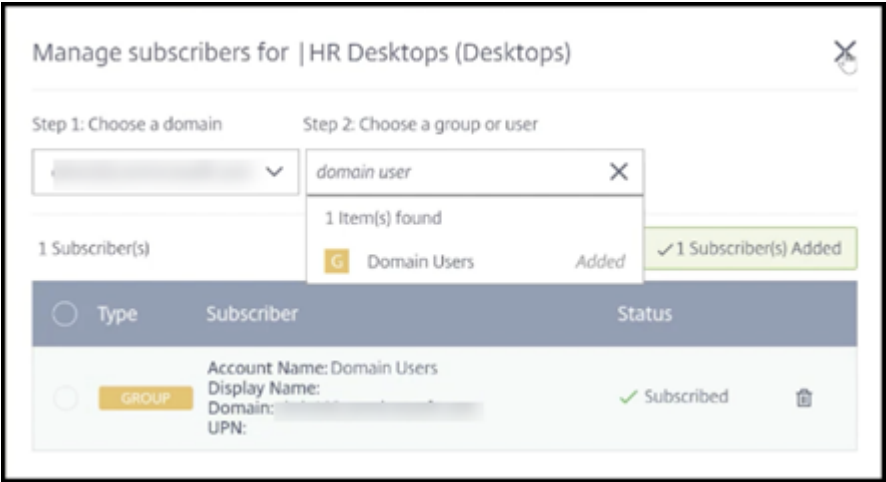


要将用户添加到已包含用户的目录，请单击目录的条目中的任意位置。

2. 在 **Subscribers**（订阅者）选项卡上，选择 **Manage Subscribers**（管理订阅者）。



3. 选择一个域。（如果您使用托管 Azure AD 进行用户身份验证，则域字段中只有一个条目。）然后选择一个用户。



4. 根据需要选择其他用户。完成后，选择右上角的 **X**。

要从目录中删除用户，请执行步骤 1 和 2。在步骤 3 中，选择要删除的名称旁边的垃圾桶图标（而非选择域和组/用户）。此操作将从目录中删除用户，而非从源（例如托管 Azure AD 或您自己的 AD 或 AAD）中删除。

后续操作：

- 对于包含多会话计算机的目录，[请添加应用程序](#)（如果尚未添加）。
- 对于所有目录，[请将 Citrix Workspace URL 发送给用户](#)。

### 更多信息

有关 Citrix Cloud 中身份验证的更多信息，请参阅 [身份和访问管理](#)。

## 快速部署中的 Remote PC Access

September 1, 2023

### 简介

通过 Citrix Remote PC Access，用户能够远程使用办公室中的物理 Windows 或 Linux 计算机。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。

Remote PC Access 支持已加入域的计算机。

本文介绍了如何使用快速部署界面创建 Remote PC Access 部署。要使用“完整配置”界面创建 Remote PC Access 部署，请参阅 [Remote PC Access](#)。

## 交付虚拟桌面和应用程序之间的差别

如果您熟悉交付虚拟桌面和应用程序，则知晓 Remote PC Access 功能有以下几点差别：

- Remote PC Access 目录通常包含现有的物理机。因此，您无需准备映像或预配计算机即可使用 Remote PC Access。交付桌面和应用程序通常使用虚拟机 (VM)，映像用作预配 VM 的模板。
- 当 Remote PC Access 随机池目录中的计算机关闭电源时，它不会重置为映像的原始状态。
- 对于 Remote PC Access 静态用户分配目录，分配发生在用户登录之后（无论是在计算机上还是通过 RDP）。交付桌面和应用程序时，如果计算机可用，则会为用户分配。

## 安装和配置摘要

在开始执行任务之前，请查看本部分内容。

1. 开始之前：
  - a) 请查看要求和注意事项。
  - b) 完成准备任务。
2. 在 Citrix Cloud 中：
  - a) 设置一个 [Citrix Cloud 帐户并订阅 Citrix DaaS](#)。
  - b) 设置可以访问 Active Directory 资源的资源位置。在资源位置中至少安装两个 Cloud Connector。Cloud Connector 与 Citrix Cloud 进行通信。

请按照[创建资源位置并在其中安装 Cloud Connector](#)的指导进行操作。此信息包括系统要求、准备和过程。
  - c) 将 [Active Directory](#) 连接到 [Citrix Cloud](#)。
3. 在用户将远程访问的每台计算机上安装 Citrix Virtual Delivery Agent (VDA)。VDA 通过资源位置中的 Cloud Connector 与 Citrix Cloud 进行通信。
4. 在 **Manage**（管理）> **Quick Deploy**（快速部署）：
  - a) 创建 Remote PC Access 目录。在此过程中，您可以指定资源位置的位置并选择用户分配方法。
  - b) 如果需要，请向[目录中添加订阅者（用户）](#)。如果目录使用静态自动分配或随机池用户分配方法，请向目录中添加用户。您无需将用户添加到静态预分配的目录中。
5. 将 [Workspace URL](#) 发送给用户。用户可以从其工作区登录办公室中的计算机。

## 要求和注意事项

本部分中对计算机的引用是指用户远程访问的计算机。

### 常规

- 计算机必须运行单会话 Windows 10 或 Linux（Red Hat Enterprise Linux 和 Ubuntu）操作系统。
- 必须将计算机加入到 Active Directory 域服务域。
- 如果您熟悉如何将 Remote PC Access 与 Citrix Virtual Apps and Desktops 结合使用，则知晓局域网唤醒功能在 Citrix DaaS 中不可用。

### 网络

- 计算机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：
  - 设置电源设置以保持无线适配器处于打开状态。
  - 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，计算机无法进行远程访问。
  - 确保可以从 Wi-Fi 网络访问 Cloud Connector。

### 设备和外围设备

- 以下设备不受支持：
  - 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。
- 将键盘和鼠标直接连接到计算机。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。
- 对于便携式计算机和 Surface Pro 设备：确保便携式计算机连接到电源，而不是依靠电池运行。配置便携式计算机电源选项以匹配台式机的选项。例如：
  - 禁用休眠功能。
  - 禁用睡眠功能。
  - 将合盖操作设置为不执行任何操作。
  - 将按下电源按钮的操作设置为关闭。
  - 禁用显卡和 NIC 节能功能。

使用扩展坞时，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 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。

要为 Remote PC Access 设备启用停靠和取消停靠，请执行以下操作：

- 在开始 > 设置 > 系统 > 电源和睡眠中，将睡眠设置为从不。

- 在设备管理器 > 网络适配器 > 以太网适配器中，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。

## Linux VDA

- 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。
- 包含 Linux 计算机的目录必须使用静态预分配的用户分配方法。包含 Linux 计算机的目录不能使用静态自动分配或随机池分配方法。

## Workspace 注意事项

- 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计算机，该计算机将显示为不可用。

## 准备

- 决定如何在计算机上安装 VDA。有几种方法可用：
  - 在每台计算机上手动安装 VDA。
  - [使用脚本](#)通过组策略推送 VDA 安装。
  - 使用 Microsoft System Center Configuration Manager (SCCM) 等电子软件分发 (ESD) 工具推送 VDA 安装。有关详细信息，请参阅[使用 SCCM 安装 VDA](#)。
- 了解用户分配方法并决定要使用哪种方法。可以在创建 Remote PC Access 目录时指定方法。
- 决定计算机（实际上是您在计算机上安装的 VDA）将如何向 Citrix Cloud 注册。必须注册 VDA 才能与 Citrix Cloud 中的会话代理建立通信。

VDA 通过 Cloud Connector 在其资源位置进行注册。可以在安装 VDA 时指定 Cloud Connector 地址，也可以稍后指定。

对于 VDA 的首次（初始）注册，Citrix 建议使用基于策略的 GPO 或 LGPO。初始注册后，Citrix 建议使用默认启用的自动更新功能。[了解有关 VDA 注册的更多信息](#)。

## 安装 VDA

在用户将远程访问的每台物理机上下载并安装 VDA。

## 下载 VDA

- 要下载 Windows VDA，请执行以下操作：
  1. 使用 Citrix Cloud 帐户凭据，浏览至 [Citrix DaaS 下载页面](#)。
  2. 下载最新的 VDA。有两种类型的安装包可供选择。VDA 标题中的年份和月份值有所差别。
- 要下载适用于 Remote PC Access 的 Linux VDA，请按照 [Linux VDA 文档](#) 中的指导进行操作。

**Windows VDA 安装软件包类型** Citrix 下载站点提供了两种可用于 Remote PC Access 计算机的 Windows VDA 安装软件包类型：

- 单会话核心 VDA 安装程序 (*release* 为 *yymm*)： [VDAWorkstationCoreSetup\\_release.exe](#)

单会话核心 VDA 安装程序专为 Remote PC Access 量身定制。它轻巧且易于通过网络（与其他 VDA 安装程序相比）部署到所有计算机。它不包括这些部署中通常不需要的组件，例如 Citrix Profile Management、Machine Identity Service 和用户个性化层。

但是，如果未安装 Citrix Profile Management，Citrix Analytics for Performance 的显示和某些监视详细信息将不可用。有关这些限制的详细信息，请参阅博客文章 [Monitor and troubleshoot Remote PC Access machines](#) (Remote PC Access 计算机监视和故障排除)。

如果您想要完整的分析和监视显示屏幕，请使用单会话完整 VDA 安装程序。

- 单会话完整 VDA 安装程序 (*release* 为 *yymm*)： [VDAWorkstationSetup\\_release.exe](#)

尽管单会话完整 VDA 安装程序是比单会话核心 VDA 安装程序更大的软件包，但是您可以进行定制以仅安装所需的组件。例如，您可以安装支持 Profile Management 的组件。

## 以交互方式安装用于 Remote PC Access 的 Windows VDA

1. 双击您下载的 VDA 安装文件。
2. 在 **Environment**（环境）页面上，选择 **Enable Remote PC Access**（启用 Remote PC Access），然后单击 **Next**（下一步）。
3. 在 **Delivery Controller** 页面上，选择以下选项之一：
  - 如果您知道 Cloud Connector 的地址，请选择 **Do it manually**（手动执行）。输入 Cloud Connector 的 FQDN，然后单击 **Add**（添加）。对资源位置中的其他 Cloud Connector 重复此操作。
  - 如果您知道在 AD 结构中安装 Cloud Connector 的位置，请选择 **Choose locations from Active Directory**（从 Active Directory 中选择位置），然后导航到该位置。对其他 Cloud Connector 重复此操作。
  - 如果要在 Citrix 组策略中指定 Cloud Connector 地址，请选择 **Do it later (Advanced)**（稍后执行此操作 (高级)），然后在出现提示时确认该选择。

完成后，单击 **Next**（下一步）。

4. 如果您使用的是单会话完整 VDA 安装程序，请在 **Additional Components**（其他组件）页面上，选择要安装的组件，例如 Profile Management。（如果您使用的是单会话核心 VDA 安装程序，则不会显示此页面。）
5. 在 **Features**（功能）页面上，单击 **Next**（下一步）。
6. 在 **Firewall**（防火墙）页面上，选择 **Automatically**（自动）（如果尚未选择）。然后，单击下一步。
7. 在 **Summary**（摘要）页面上，单击 **Install**（安装）。
8. 在 **Diagnose**（诊断）页面上，单击 **Connect**（连接）。确保选中该复选框。出现提示时，输入您的 Citrix 帐户凭据。验证凭据后，单击 **Next**（下一步）。
9. 在 **Finish**（完成）页面上，单击 **Finish**（完成）。

有关完整的安装信息，请参阅[安装 VDA](#)。

#### 使用命令行安装适用于 **Remote PC Access** 的 **Windows VDA**

- 如果您使用的是单会话核心 VDA 安装程序：运行 `VDAWorkstationCoreSetup.exe`，然后包括 `/quiet`、`/enable_hdx_ports` 和 `/enable_hdx_udp_ports` 选项。要指定 Cloud Connector 地址，请使用 `/controllers` 选项。

例如，以下命令将安装单会话核心 VDA。不安装 Citrix Workspace 应用程序和其他非核心服务。此时将指定两个 Cloud Connector 的 FQDN，并且 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 "Connector-East
.domain.com" "Connector-East2.domain.com" /enable_hdx_ports /
noreboot
```

- 如果您使用的是单会话完整 VDA 安装程序，并且想要包括 Profile Management（或其他可选组件）：运行 `VDAWorkstationSetup.exe` 并包括 `/remotepc` 和 `/includeadditional` 选项。`/remotepc` 选项阻止安装大多数附加组件。`/includeadditional` 选项准确指定要安装的其他组件。

例如，以下命令阻止安装除 Profile Management 以外的所有可选附加组件。

```
VDAWorkstationSetup.exe /quiet /remotepc /includeadditional "
Citrix User Profile Manager", "Citrix User Profile Manager WMI
Plugin" /controllers "connector.domain.com" "connector2.domain.
com" /enable_hdx_ports /noresume /noreboot
```

有关详细信息，请参阅[用于安装 VDA 的命令行选项](#)。

#### 安装 **Linux VDA**

请按照 [Linux 文档](#) 中的指导以交互方式或使用命令行安装 Linux VDA。



## 创建 **Remote PC Access** 目录

必须存在一个至少包含两个 Cloud Connector 的资源位置，才能成功创建目录。

### 重要：

一台计算机一次只能属于一个目录。当您指定要添加到目录的计算机时，不会强制执行此限制。但是，忽略此限制可能会导致以后出现问题。

1. 登录 [Citrix Cloud](#)。
2. 在左上角的菜单中，选择我的服务 > **DaaS**。
3. 如果尚未创建任何目录，请单击 **Welcome**（欢迎）页面上的 **Get Started**（开始使用）。
4. 选择 **Manage**（管理）> **Quick Deploy**（快速部署）。
5. 选择 **Create Catalog**（创建目录）。
6. 在 **Remote PC Access** 选项卡上，选择将用户分配给计算机的方法。
7. 输入目录的名称，然后选择您创建的资源位置。
8. 添加计算机。
9. 单击创建目录。
10. 在 **Your Remote PC Access catalog is being created**（正在创建您的 Remote PC Access 目录）页面上，单击 **Done**（完成）。
11. 新目录的条目显示在 **Manage**（管理）> **Quick Deploy**（快速部署）控制板上。

成功创建目录后，单击其中一个指向[向目录中添加订阅者（用户）](#)的链接。如果目录使用静态自动分配或随机池未分配的用户分配方法，则此步骤适用。

在创建目录并将用户（如果需要）添加用户后，向您的用户[发送 Workspace URL](#)。

## 用户分配方法

创建目录时选择的用户分配方法指示如何将用户分配给计算机。

- **Static autoassigned**（静态自动分配）：在计算机上安装 VDA 后，用户登录计算机（不使用 Citrix，例如，面对面或通过 RDP）时，将发生用户分配。之后，如果其他用户登录到该计算机（不使用 Citrix），这些用户也会被分配。一次只有一个用户能够使用此计算机。对于共享计算机的办公室工作人员或轮班工作人员来说，这是典型设置。

Windows 计算机支持此方法。它不能与 Linux 计算机结合使用。

- **Static preassigned**（静态预分配）：用户预先分配给计算机。（这通常是通过上载包含计算机-用户映射的 CSV 文件来配置的。）安装 VDA 后，无需用户登录即可建立分配。创建目录后也无需将用户分配给目录。这非常适合办公室工作人员。

Windows 和 Linux 计算机支持此方法。

- **Random pool unassigned** (未分配的随机池)：用户被随机分配到可用的计算机。一次只有一个用户能够使用此计算机。这非常适合学校的计算实验室。

Windows 计算机支持此方法。它不能与 Linux 计算机结合使用。

## 向目录中添加计算机的方法

请记住：每台计算机上都必须安装 VDA。

创建或编辑目录时，可以通过三种方法将计算机添加到目录中：

- 逐个选择计算机帐户。
- 选择 OU。
- 使用 CSV 文件批量添加。模板可供您用于 CSV 文件。

### 添加计算机名称

此方法逐个添加计算机帐户。

1. 选择您的域。
2. 搜索计算机帐户。
3. 单击添加。
4. 重复操作以添加更多计算机。
5. 添加完计算机后，单击 **Done** (完成)。

### 添加 OU

此方法根据计算机帐户所在的组织单位添加计算机帐户。

选择 OU 时，请选择较低级别的 OU 以获得更大的粒度。如果不需要该粒度，则可以选择更高级别的 OU。

例如，如果是 **Bank/Officers/Tellers**，请选择 **Tellers** 以获得更大的粒度。否则，您可以根据要求选择 **Officers** 或 **Bank**。

将 OU 分配到 Remote PC Access 目录后移动或删除这些 OU 会影响 VDA 关联并导致未来的分配出现问题。确保您的 AD 更改计划说明了目录的 OU 分配更新。

要添加 OU，请执行以下操作：

1. 选择您的域。
2. 选择包含要添加的计算机帐户的 OU。
3. 在复选框中指示是否包括在选择中包含的子文件夹。
4. 完成选择 OU 后，单击 **Done** (完成)。

## 批量添加

1. 单击 **Download CSV Template**（下载 CSV 模板）。
2. 在模板中，添加计算机帐户信息（最多添加 100 个条目）。CSV 文件还可以包含分配给每台计算机的用户的名称。
3. 保存该文件。
4. 可以将该文件拖动到 **Add machines in bulk**（批量添加计算机）页面或浏览至该文件。
5. 此时将显示文件内容的预览。如果这不是您想要的文件，则可以创建另一个文件，然后拖动或浏览到相应的文件。
6. 完成后，请单击 **Done**（完成）。

## 管理 Remote PC Access 目录

要显示或更改 Remote PC Access 目录的配置信息，请从 **Manage**（管理）> **Quick Deploy**（快速部署）控制板中选择该目录（单击目录的条目中的任意位置）。

- 在 **Details**（详细信息）选项卡中，可以添加或删除计算机。
- 在 **Subscribers**（订阅者）选项卡中，可以添加或删除用户。
- 在 **Machines**（计算机）选项卡中，可以：
  - 添加或删除计算机：**Add or remove machines**（添加或删除计算机）按钮。
  - 更改用户分配：**Remove assignment**（删除分配）垃圾桶图标、省略号菜单中的 **Edit machine assignment**（编辑计算机分配）。
  - 查看哪些计算机已注册，并将计算机置于或退出维护模式。

## 在快速部署中进行监视

May 11, 2022

在 **Monitor**（监视）控制板中，您可以查看 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）部署中的桌面使用情况、会话和计算机。还可以控制会话、电源管理计算机、终止正在运行的应用程序和结束正在运行的进程。

要访问 **Monitor**（监视）控制板，请执行以下操作：

1. 如果尚未登录 [Citrix Cloud](#)，请登录。在左上角的菜单中，选择我的服务 > **DaaS**。
2. 在 **Manage**（管理）> **Quick Deploy**（快速部署）控制板，选择 **Monitor**（监视）选项卡。

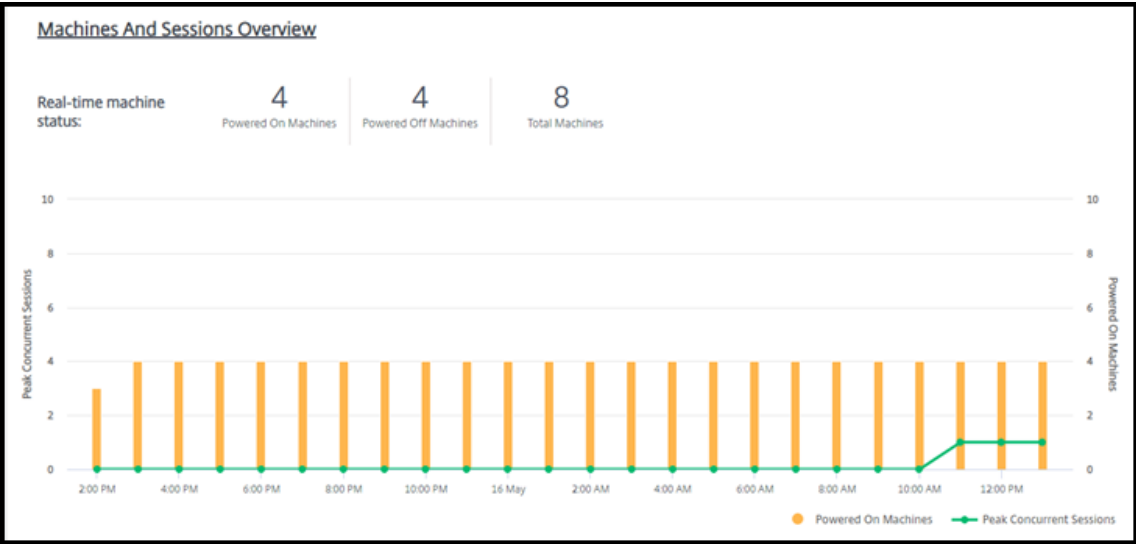
## 监视桌面使用情况

此页面上的显示内容每五分钟刷新一次。

- **Machine and Sessions Overview**（计算机和会话概述）：可以自定义显示屏幕以显示有关所有目录（默认值）或选定目录的信息。还可以自定义时间段：最后一天、上周、上个月或过去三个月。

显示屏幕顶部的计数指示计算机总数以及已打开和关闭电源的计算机数量。将鼠标悬停在某个值上可显示单会话和多会话的数量。

计数下方的图表显示了在所选时间段内已打开电源的计算机数量和常规时段的峰值并发会话数。将鼠标悬停在图表中的某个点上可显示该点的计数。



- **Top 10s**（排名前 10）：要自定义排名前 10 位的显示屏幕，请选择一个时间段：上周（默认值）、上个月或过去三个月。还可以自定义显示屏幕以仅显示涉及单会话计算机、多会话计算机或应用程序的活动的信息。
  - **Top 10 Active Users**（排名前 10 的活动用户）：列出在此时间段内启动桌面最频繁的用户。悬停在行上将显示总启动次数。
  - **Top 10 Active Catalogs**（排名前 10 的活动目录）：列出在所选时间段内持续时间最长的目录。持续时间是该目录中所有用户会话的总和。

## 桌面使用情况报告

要下载包含上个月计算机启动信息的报告，请选择 **Launch Activity**（启动活动）。一条消息指示正在处理请求。报告会自动下载到本地计算机上的默认下载位置。

## 筛选和搜索以监视计算机和会话

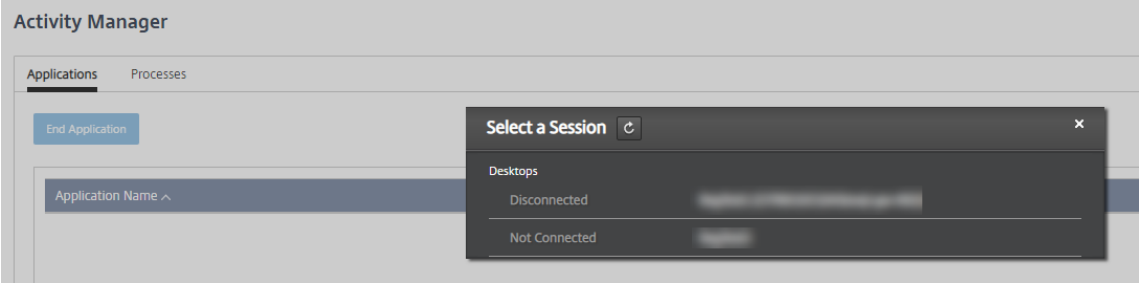
监视会话和计算机信息时，默认情况下将显示所有计算机或会话。您可以：

- 按计算机、会话、连接或应用程序筛选显示屏幕。
- 通过选择所需的条件，使用表达式构建过滤器来优化会话或计算机的显示。
- 保存您构建的过滤器以供重复使用。

## 控制用户的应用程序

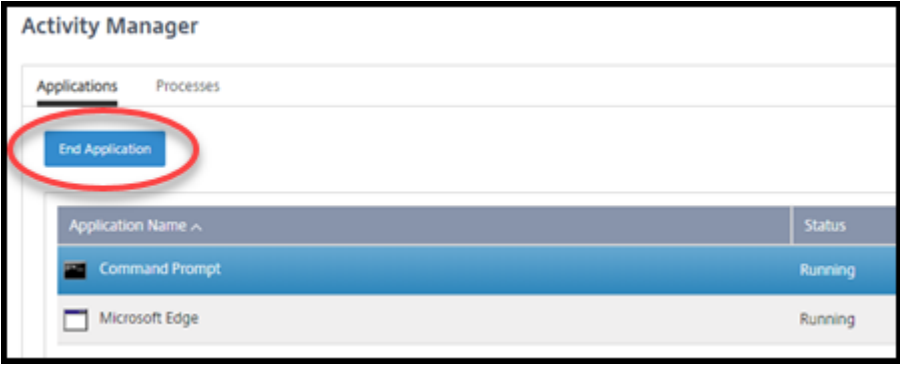
可以为具有正在运行的会话或已分配的桌面的用户显示和管理应用程序和进程。

1. 在 Citrix DaaS 的 **Monitor**（监视）控制板中，选择 **Search**（搜索）并输入用户名（或用户名的开头字符）、计算机或端点。从搜索结果中，选择要查找的项目。（要在不搜索的情况下折叠搜索框，请再次选择 **Search**（搜索）。）
2. 选择一个会话。



活动管理器列出了用户会话的应用程序和进程。

3. 要结束应用程序，请在活动管理器的 **Applications**（应用程序）选项卡上，在应用程序的行中选择该应用程序，然后选择 **End Application**（结束应用程序）。



4. 要结束进程，请在活动管理器的 **Processes**（进程）选项卡上，在进程的行中进行选择以选择该进程，然后选择 **End Process**（结束进程）。
5. 要显示会话详细信息，请选择右上角的 **Details**（详细信息）。要返回到应用程序和进程显示屏幕，请选择右上角的活动管理器。
6. 要控制会话，请选择 **Session Control**（会话控制） > **Log Off**（注销）或 **Session Control**（会话控制） > **Disconnect**（断开连接）。

## 重影用户

使用重影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。要验证该连接，请检查 **User** 标题栏中列出的计算机名称。

重影功能将在新的浏览器选项卡中启动。确保您的浏览器允许显示来自 Citrix Cloud URL 的弹出窗口。

只有已加入域的计算机上的用户才支持重影。必须设置堡垒计算机，才能对未加入域的计算机执行重影操作。有关详细信息，请参阅[堡垒访问](#)。

重影必须从与已加入域的计算机位于同一虚拟网络中的计算机启动，并且还必须满足任何端口要求。

#### 启用重影

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）> **Monitor**（监视）中，转到 **User Details**（用户详细信息）视图。
2. 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选择重影。

#### 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。

监视器使用 FQDN 连接到目标 Linux VDA。确保监视器客户端可以解析 Linux VDA 的 FQDN。

- VDA 必须安装 `python-websocketify` 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。在每个监视器客户端和 Linux VDA 上安装 SSL 证书。

按照“会话重影”中的说明为 Linux VDA 配置重影。

1. 启用重影后，重影连接将初始化，并且用户设备上将显示确认提示。
2. 指示用户选择 **Yes**（是）以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。安装 VDA 时启用 `Use Windows Remote Assistance` 功能。

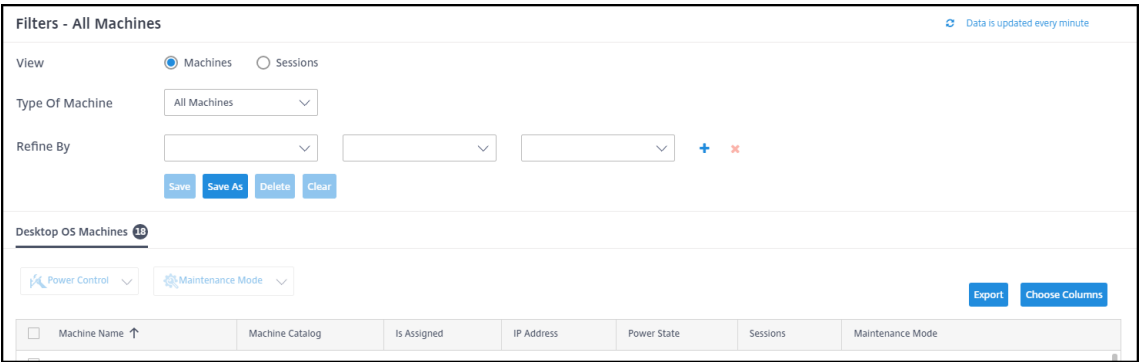
1. 启用重影后，重影连接将初始化，并显示一个对话框，提示您打开或保存 `.msrc incident` 文件。
2. 请使用远程协助查看器（如果默认情况下尚未选择）打开事件文件。此时将在用户设备上显示一个确认提示窗口。
3. 指示用户选择 **Yes**（是）以启动计算机或会话共享。
4. 要执行更多控制操作，请要求用户共享键盘和鼠标控制。

#### 监视和控制会话

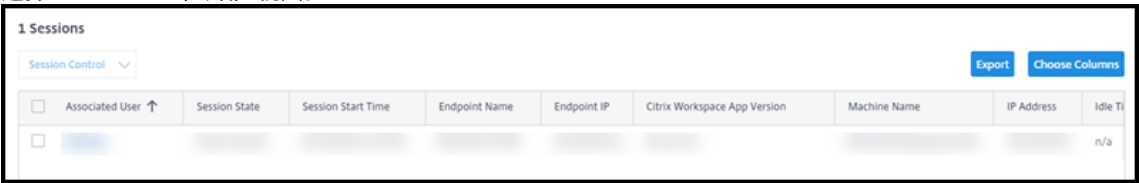
会话显示屏幕每分钟更新一次。

除了查看会话之外，还可以断开一个或多个会话的连接，或者从会话中注销用户。

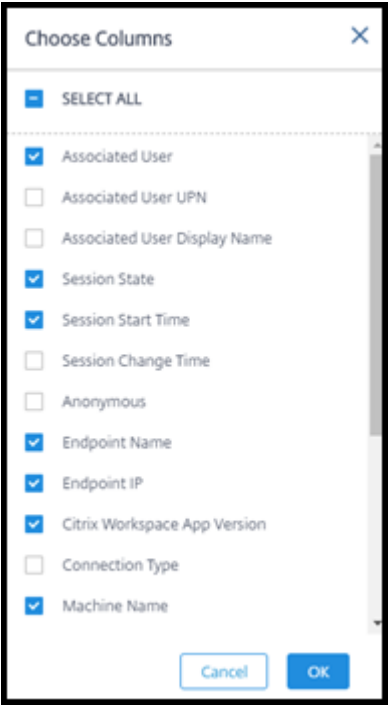
1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）> **Monitor**（监视）中，选择 **Filters**（过滤器）。



2. 选择 **Sessions**（会话）视图。



3. 要定制显示屏幕，请选择 **Choose Columns**（选择列），然后选中要显示的项目的复选框。完成后，选择 **OK**（确定）。会话显示会自动刷新。



4. 选中要控制的每个会话左侧的复选框。
5. 要注销或断开会话连接，请选择 **Session Control**（会话控制）> **Log Off**（注销）或 **Session Control**（会话控制）> **Disconnect**（断开连接）。

请记住，目录的电源管理计划还可以控制断开会话连接和从断开连接的会话中注销用户。

作为上述过程的替代方法，您还可以 **Search**（搜索）用户、选择要控制的会话，然后显示会话详细信息。注销和断开连接选项也可用。

会话信息报告

要下载会话信息，请在会话显示屏幕上选择 **Export**（导出）。一条消息指示正在处理请求。报告会下载到本地计算机上的默认下载位置。

监视计算机以及对其进行电源控制

计算机显示屏幕每分钟更新一次。

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）> **Monitor**（监视）中，选择 **Filters**（过滤器）。
2. 选择 **Machines**（计算机）视图。

<input type="checkbox"/>	Machine Name ↑	Is Assigned	IP Address	Delivery Group	Failure Type	Failure Reason	Failure Time	Power State	Sessions	Maintenance Mode
<input type="checkbox"/>					n/a	None		On	0	Off
<input type="checkbox"/>					n/a	None		On	0	Off
<input type="checkbox"/>					n/a	None		Off	0	Off

默认情况下，显示屏幕会列出单会话操作系统计算机。或者，您可以显示多会话计算机。

3. 要定制显示屏幕，请选择 **Choose Columns**（选择列），然后选中要显示的项目的复选框。完成后，选择 **OK**（确定）。计算机显示屏幕会自动刷新。

**Choose Columns**

☒ SELECT ALL

☒ DNS Name

☐ Machine Catalog

☒ Is Physical

☐ Persist User Changes

☐ Provisioning Type

☐ Allocation Type

☐ Is Assigned

☒ IP Address

☒ VDA Version

☐ Remote PC Access

☐ Delivery Group

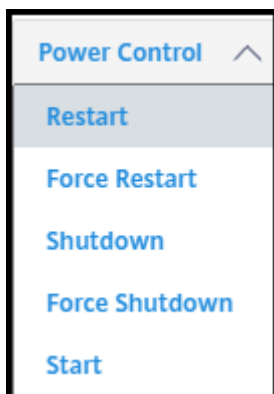
☐ Failure Type

Cancel OK

4. 要控制计算机的电源或将其置于或退出维护模式，请选中要控制的每台计算机左侧的复选框。



5. 要控制所选计算机的电源，请选择 **Power Control**（电源控制）并选择一项操作。



6. 要将选定的计算机置于或退出维护模式，请选择 **Maintenance Mode**（维护模式）> **ON**（开）或 **Maintenance Mode**（维护模式）> **OFF**（关）。

使用搜索功能查找和选择计算机时，您将看到计算机详细信息、利用率、历史利用率（过去七天内）和平均 IOPS。

#### 计算机信息报告

要下载会话信息，请在计算机显示屏幕上选择 **Export**（导出）。一条消息指示正在处理请求。报告会自动下载到本地计算机上的默认下载位置。

#### 检查应用程序和桌面运行状况

探测操作会自动执行检查已发布的应用程序和桌面的运行状况的过程。运行状况检查结果可以通过 **Monitor**（监视）控制板获取。有关详细信息，请参阅：

- [应用程序探测](#)
- [桌面探测](#)

#### 快速部署中的故障排除

October 11, 2022

#### 简介

资源位置包含用于交付桌面和应用程序的计算机。这些计算机是在目录中创建的，因此目录被视为资源位置的一部分。每个资源位置还包含 Cloud Connector。Cloud Connector 使 Citrix Cloud 能够与资源位置进行通信。通常情况下，Citrix 会安装并更新 Cloud Connector。

或者，您可以启动多项 Cloud Connector 和资源位置操作。请参阅：

- [资源位置操作](#)
- [创建目录时的资源位置设置](#)

Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）具有故障排除和可支持性工具，可帮助解决交付桌面和应用程序的计算机 (VDA) 的配置和通信问题。例如，创建目录可能会失败，或者用户可能无法启动其桌面或应用程序。

此故障排除包括通过堡垒计算机或直接 RDP 访问 Citrix 托管 Azure 订阅的权限。获得订阅的访问权限后，可以使用 Citrix 可支持性工具来查找和解决问题。有关详细信息，请参阅：

- 使用堡垒或直接 RDP 进行 VDA 故障排除
- 堡垒访问
- 直接 RDP 访问

### 使用堡垒或直接 **RDP** 进行 **VDA** 故障排除

可支持性功能适用于在解决 Citrix 问题方面有经验的用户。其中包括：

- Citrix Citrix Service Provider (CSP) 和具备 Citrix DaaS 产品技术知识和故障排除经验的其他用户。
- Citrix 支持人员。

如果您不熟悉或无法自如地应对 Citrix 组件的故障排除，则可以向 Citrix 技术支持请求帮助。Citrix 技术支持代表可能会要求您设置本部分中介绍的访问方法之一。但是，Citrix 代表使用 Citrix 工具和技术进行实际的故障排除。

#### 重要

:

这些可支持性功能仅适用于已加入域的计算机。如果您的目录中的计算机未加入域，系统将引导您向 Citrix 技术支持请求故障排除帮助。

### 访问方法

这些访问方法仅适用于 Citrix 托管 Azure 订阅。有关详细信息，请参阅 [Azure 订阅](#)。

提供了两种可支持性访问方法。

- 通过客户的专用 Citrix 托管 Azure 订阅中的堡垒计算机访问您的资源。堡垒是允许访问订阅中的计算机的单个接入点。它允许来自指定范围内的 IP 地址的远程流量，从而提供与这些资源的安全连接。

此方法的步骤包括：

- 创建堡垒计算机
- 下载 RDP 代理
- RDP 到堡垒计算机

- 从堡垒计算机连接到订阅中的其他 Citrix 计算机

堡垒计算机目的是在短期内使用。此方法适用于涉及目录或映像计算机的创建的问题。

- 直接 RDP 访问客户的专用 Citrix 托管 Azure 订阅中的计算机。要允许传输 RDP 流量，必须在网络安全组中定义端口 3389。

此方法适用于除创建以外的目录问题，例如用户无法启动桌面。

请记住：作为这两种访问方法的替代方法，请联系 Citrix 技术支持以获取帮助。

## 堡垒访问

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Troubleshoot & Support**（故障排除和支持）。
2. 单击 **View troubleshooting options**（查看故障排除选项）。
3. 在 **Troubleshoot**（故障排除）页面上，选择前两种问题类型之一，然后单击 **Use our troubleshooting machine**（使用我们的故障排除计算机）。
4. 在 **Troubleshoot with Bastion Machine**（使用堡垒计算机进行故障排除）页面上，选择目录。
  - 如果选定目录中的计算机未加入域，系统会指示您联系 Citrix 技术支持。
  - 如果已创建堡垒计算机，且能够通过 RDP 访问选定目录的网络连接，请跳至步骤 8。
5. 此时将显示 RDP 访问范围。如果要将 RDP 访问限制到比网络连接允许的范围更小的范围，请选中 **Restrict RDP access to only computers in IP address range**（限制仅对 IP 地址范围内的计算机进行 RDP 访问）复选框，然后输入所需的范围。
6. 键入在通过 RDP 访问堡垒计算机时用于登录的用户名和密码。[密码要求](#)。

请勿在用户名中使用 Unicode 字符。
7. 单击 **Create Bastion Machine**（创建堡垒计算机）。

成功创建堡垒计算机后，页面标题将更改为 **Bastion -connection**（堡垒-\* 连接\*）。

如果堡垒计算机创建失败（或者如果在运行过程中失败），请单击失败通知页面底部的 **Delete**（删除）。请再次尝试创建堡垒计算机。

可以在创建堡垒计算机后更改 RDP 范围限制。单击编辑。输入新值，然后单击复选标记以保存更改。（单击 **X** 可取消更改。）
8. 单击 **Download RDP File**（下载 RDP 文件）。
9. 使用您在创建堡垒时指定的凭据通过 RDP 访问堡垒。（堡垒计算机的地址嵌入在您下载的 RDP 文件中。）
10. 从堡垒计算机连接到订阅中的其他 Citrix 计算机。然后，您可以收集日志并运行诊断。

创建堡垒计算机时会打开其电源。为了节省成本，如果计算机在启动后保持空闲状态，则将自动关闭电源。几个小时后，计算机将自动删除。

可以使用页面底部的按钮进行电源管理或删除堡垒计算机。如果选择删除堡垒计算机，则必须确认计算机上的所有活动会话都将自动结束。此外，保存在计算机上的所有数据和文件都将被删除。

## 直接 RDP 访问

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Troubleshoot & Support**（故障排除和支持）。
2. 单击 **View troubleshooting options**（查看故障排除选项）。
3. 在 **Troubleshoot**（故障排除）页面上，选择 **Other catalog issue**（其他目录问题）。
4. 在 **Troubleshoot with RDP Access**（使用 RDP 访问进行故障排除）页面上，选择目录。

如果已对选定目录的网络连接启用了 RDP，请跳至步骤 7。

5. 此时将显示 RDP 访问范围。如果要将 RDP 访问限制到比网络连接允许的范围更小的范围，请选中 **Restrict RDP access to only computers in IP address range**（限制仅对 IP 地址范围内的计算机进行 RDP 访问）复选框，然后输入所需的范围。
6. 单击 **Enable RDP Access**（启用 RDP 访问）。

成功启用 RDP 访问后，页面标题将更改为 **RDP Access -connection**（RDP 访问-\* 连接 \*）。

如果未成功启用 RDP 访问，请单击失败通知页面底部的 **Retry Enabling RDP**（重新尝试启用 RDP）。

7. 使用 Active Directory 管理员凭据连接到计算机。然后，您可以收集日志并运行诊断。

## 获取帮助

如果仍然遇到问题，请按照[如何获取帮助和支持](#)中的说明开立一个票证。

## 快速部署参考

April 11, 2023

## “Quick Deploy”（快速部署）控制板上的目录选项卡

在 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）中的 **Manage**（管理）> **Quick Deploy**（快速部署）控制板中，单击目录的条目中的任意位置。以下选项卡包含有关目录的信息：

- **Details** (详细信息): 列出创建目录 (或其最近编辑) 时指定的信息。它还包含有关用于创建目录的映像的信息。

在此选项卡中, 您可以:

- [更改目录中使用的映像](#)。
- [删除目录](#)。
- 访问包含目录所使用的资源位置的详细信息的页面。

- **Desktop** (桌面): 仅适用于包含单会话 (静态或随机) 计算机的目录。在此选项卡中, 您可以更改目录的名称和说明。

- **Desktop and Apps** (桌面和应用程序): **Desktops and Apps** (桌面和应用程序) 选项卡仅适用于包含多会话计算机的目录。在此选项卡中, 您可以:

- [添加](#)、[编辑](#)或[删除](#)目录的用户可以在 Citrix Workspace 中访问的应用程序。
- 更改目录的名称和说明。

- **Subscribers** (订阅者): 列出所有用户, 包括其类型 (用户或组)、帐户名称、显示名称及其 Active Directory 域和用户主体名称。

在此选项卡中, 您可以为目录[添加或删除用户](#)。

- **Machines** (计算机): 显示目录中的计算机总数, 以及已注册的计算机、未注册的计算机和已打开维护模式的计算机的数量。

对于目录中的每台计算机, 显示内容包括每台计算机的名称、电源状态 (开/关)、注册状态 (已注册/未注册)、已分配的用户、会话计数 (0/1) 和维护模式状态 (指示打开或关闭的图标)。

在此选项卡中, 您可以:

- 添加或删除计算机
- 启动、重新启动、强制重新启动或关闭计算机
- 打开或关闭计算机的维护模式

有关详细信息, 请参阅[管理目录](#)。许多计算机操作也可以从“快速部署”控制板上的 **Monitor** (监视) 选项卡中找到。请参阅[监视计算机以及对其进行电源控制](#)。

- **Power Management** (电源管理): 使您能够管理目录中的计算机打开和关闭电源的时间。计划还指示空闲计算机断开连接的时间。

可以在创建自定义目录时或以后配置电源计划。如果没有明确设置计划, 会话结束时计算机将关闭电源。

使用快速创建目录时, 无法选择或配置电源计划。默认情况下, 快速创建目录使用“Cost Saver” (成本节省程序) 预设计划。但是, 您可以稍后编辑该目录并更改计划。

有关详细信息, 请参阅[管理电源管理计划](#)。

## DNS 服务器

本部分内容适用于包含已加入域的计算机的所有部署。如果您只使用未加入域的计算机，则可以忽略本部分内容。

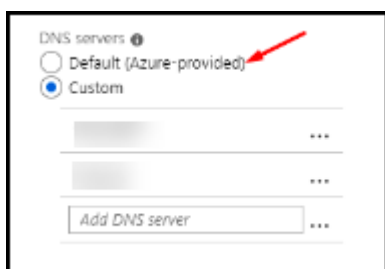
1. 在创建已加入域的目录（或连接，前提是您使用的是 Citrix 托管 Azure 订阅）之前，请检查是否有可以解析公用和专用域名的 DNS 服务器条目。

当 Citrix DaaS 创建目录或连接时，它至少会查找一个有效的 DNS 服务器条目。如果找不到有效的条目，创建操作将失败。

查看位置：

- 如果您使用自己的 Azure 订阅，请检查 Azure 中的 **DNS servers**（DNS 服务器）条目。
- 如果您使用的是 Citrix 托管 Azure 订阅并创建 Azure VNet 对等互连连接，请检查您正在建立对等互连的 Azure VNet 中的 **DNS servers**（DNS 服务器）条目。
- 如果您使用 Citrix 托管 Azure 订阅并创建 SD-WAN 连接，请检查 [SD-WAN Orchestrator](#) 中的 DNS 条目。

2. 在 Azure 中，**Custom**（自定义）设置必须至少有一个有效条目。此服务不能与 **Default (Azure-provided)**（默认 (Azure 提供)）设置一起使用。



- 如果启用了 **Default (Azure-provided)**（默认 (Azure 提供)），请将该设置更改为 **Custom**（自定义），然后至少添加一个 DNS 服务器条目。
  - 如果 **Custom**（自定义）下已有 DNS 服务器条目，请验证要与此服务一起使用的条目是否可以解析公用和专用域 IP 名称。
  - 如果您没有任何可以解析域名的 DNS 服务器，Citrix 建议添加 Azure 提供的具有这些功能的 DNS 服务器。
3. 如果更改任何 DNS 服务器条目，请重新启动连接到虚拟网络的所有计算机。重新启动操作会分配新的 DNS 服务器设置。（VM 将继续使用其当前的 DNS 设置，直到重新启动。）

如果您想以后更改 DNS 地址，请在创建连接后：

- 使用自己的 Azure 订阅时，可以在 Azure 中对其进行更改（如前面的步骤中所述）。或者，也可以在此服务中对其进行更改。
- 使用 Citrix 托管 Azure 订阅时，此服务不会同步您在 Azure 中对 DNS 地址所做的更改。但是，您可以在此服务中更改连接的 DNS 设置。

请记住，更改 DNS 服务器地址可能会导致目录中使用该连接的计算机出现连接问题。

## 通过此服务添加 DNS 服务器

在向连接中添加 DNS 服务器地址之前，请确保 DNS 服务器可以解析公用域名和内部域名。Citrix 建议您在添加 DNS 服务器之前测试与 DNS 服务器的连接。

1. 要在创建连接时添加、更改或删除 DNS 服务器地址，请在 **Add connection type**（添加链接类型）页面上选择 **Edit DNS servers**（编辑 DNS 服务器）。或者，如果消息指示未找到任何 DNS 服务器地址，请选择 **Add DNS Servers**（添加 DNS 服务器）。继续执行步骤 3。
2. 要为现有连接添加、更改或删除 DNS 服务器地址，请执行以下操作：
  - a) 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Network Connections**（网络连接）。
  - b) 选择要编辑的连接。
  - c) 选择 **Edit DNS servers**（编辑 DNS 服务器）。
3. 添加、更改或删除地址。
  - a) 要添加地址，请选择 **Add DNS server**（添加 DNS 服务器），然后输入 IP 地址。
  - b) 要更改地址，请在地址字段内单击并更改数字。
  - c) 要删除地址，请选择地址条目旁边的垃圾桶图标。不能删除所有 DNS 服务器地址。连接必须至少有一个 DNS 服务器地址。
4. 完成后，选择页面底部的 **Confirm Changes**（确认更改）。
5. 重新启动所有使用该连接的计算机。重新启动操作会分配新的 DNS 服务器设置。（VM 将继续使用其当前的 DNS 设置，直到重新启动。）

## 策略

### 为未加入域的计算机设置组策略

1. RDP 到正用于映像的计算机。
2. 安装 Citrix 组策略管理：
  - a) 浏览至 [CTX220345](#)。下载附件。
  - b) 双击下载的文件。在 **Group Policy Templates 1912 > Group Policy Management** 文件夹中，双击 **CitrixGroupPolicyManagement\_x64.msi**。
3. 使用运行命令，启动 **gpedit.msc** 以打开组策略编辑器。
4. 在 **User Configuration Citrix Policies > Unfiltered** 中，选择 **Edit Policy**（编辑策略）。

如果组策略管理控制台出现故障（如 [CTX225742](#) 中所述），请安装 Microsoft Visual C++ 2015 运行时（或该运行时的更高版本）。

5. 根据需要启用策略设置。例如：

- 在设置选项卡上的计算机配置或用户配置（取决于您要配置的内容）中，在 **Category > ICA / Printing** 中，选择自动创建 **PDF** 通用打印机并设置为 **Enabled**。
- 如果您希望已登录的用户成为其桌面的管理员，请将 **Interactive User**（交互用户）组添加到内置管理员组中。

6. 完成后，保存映像。

7. [更新现有目录](#) 或使用新映像 [创建新目录](#)。

#### 为已加入域的计算机设置组策略

1. 确保已安装组策略管理功能。

- 在 Windows 多会话计算机上，使用用于添加角色和功能（例如添加角色和功能）的 Windows 工具添加组策略管理功能。
- 在 Windows 单会话计算机上，为适当的操作系统安装远程服务器管理工具。（此安装需要域管理员帐户。）安装完成后，开始菜单中将提供组策略管理控制台。

2. 从 Citrix [下载页面](#) 下载并安装 Citrix 组策略管理软件包，然后根据需要配置策略设置。请按照为未加入域的计算机设置组策略中的过程进行操作，执行步骤 2 直到最后一个步骤。

请参阅 [策略设置参考](#) 文章，了解可用的设置。所有策略功能都可以从 Citrix DaaS 的“完整配置”界面获取。

#### 资源位置操作

创建用于发布桌面和应用程序的第一个目录时，Citrix 会自动创建一个资源位置和两个 Cloud Connector。可以在创建目录时指定与该资源位置相关的一些信息。请参阅 [创建目录时的资源位置设置](#)。

对于 Remote PC Access，您可以创建资源位置和 Cloud Connector。

本部分内容介绍创建资源位置后的可用操作。

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **Cloud Subscriptions**（云订阅）。

2. 选择订阅。

- **Details**（详细信息）选项卡显示订阅中的目录和映像的数量和名称。它还指示可以交付桌面或应用程序的计算机数量。该计数不包括用于其他用途的计算机，例如映像、Cloud Connector 或 RDS 许可证服务器。
- **Resource Locations**（资源位置）选项卡列出了每个资源位置。每个资源位置条目都包括该资源位置中的每个 Cloud Connector 的状态和地址。

资源位置的条目中的省略号菜单包含以下操作。



### **Run Health Check** (运行运行状况检查)

选择 **Run Health Check** (运行运行状况检查) 将立即启动连接检查。如果检查失败，Cloud Connector 的状态将是未知的，因为它不与 Citrix Cloud 进行通信。您可能想重新启动 Cloud Connector。

### **Restart Connectors** (重新启动 Connector)

Citrix 建议一次只重新启动一个 Cloud Connector。重新启动会使 Cloud Connector 脱机，并中断用户访问权限和计算机连接。

选中要重新启动的 Cloud Connector 的复选框。选择 **Restart** (重新启动)。

### **Add Connectors** (添加 Connector)

添加 Cloud Connector 通常需要 20 分钟才能完成。

请提供以下信息：

- 要添加的 Cloud Connector 数量。
- 域服务帐户凭据，用于将 Cloud Connector 计算机加入域。
- 计算机性能。
- Azure 资源组。默认值为资源位置上次使用的资源组。
- 组织单位 (OU)。默认值为资源位置上次使用的 OU。
- 您的网络是否需要代理服务器才能建立 Internet 连接。如果指示 **Yes** (是)，请提供代理服务器 FQDN 或 IP 地址以及端口号。

完成后，选择 **Add Connectors** (添加 Connector)。

### **Delete Connectors** (删除 Connector)

如果 Cloud Connector 无法与 Citrix Cloud 通信，并且重新启动无法解决问题，Citrix 技术支持可能会建议您删除该 Cloud Connector。

选中要删除的 Cloud Connector 的复选框。然后选择 **Delete** (删除)。出现提示时，确认删除。

还可以删除可用的 Cloud Connector。但是，如果删除该 Cloud Connector 会导致资源位置中的可用 Cloud Connector 少于两个，则不允许删除选定的 Cloud Connector。

### 选择 **“Update Time”** (更新时间)

Citrix 自动为 Cloud Connector 提供软件更新。在更新过程中，一个 Cloud Connector 将处于脱机状态并进行更新，而其他 Cloud Connector 仍提供服务。第一次更新完成后，另一个 Cloud Connector 将脱机并进行更新。此过

程一直持续到资源位置中的所有 Cloud Connector 都完成更新为止。开始更新的最佳时机通常在您的常规营业时间以外的时间。

选择开始更新的时间，或者指示您希望在更新可用时开始更新。完成后，选择 **Save**（保存）。

#### 重命名

输入资源位置的新名称。选择保存。

#### 配置连接

指示用户可以通过 Citrix Gateway 服务访问桌面和应用程序，还是只能从企业网络内部访问桌面和应用程序。

## Profile Management

**Profile Management** 确保个人设置适用于用户的虚拟应用程序，而无论用户设备的位置如何。

配置 Profile Management 是可选操作。

可以使用配置文件优化服务启用 Profile Management。此服务为在 Windows 中管理这些设置提供了一种可靠的方法。管理配置文件可通过维护跟随用户的单个配置文件来确保一致的体验。它会自动整合并优化用户配置文件，以最大限度地减少管理和存储需求。配置文件优化服务需要的管理、支持和基础结构最少。此外，配置文件优化为用户提供了更好的登录和注销体验。

配置文件优化服务需要一个文件共享，其中所有个人设置都将保留。您管理文件服务器。我们建议设置网络连接以允许访问这些文件服务器。必须将文件共享指定为 UNC 路径。路径可以包含系统环境变量、Active Directory 用户属性或 Profile Management 变量。要了解有关 UNC 文本字符串格式的详细信息，请参阅[指定用户存储的路径](#)。

启用 Profile Management 时，请考虑通过配置文件夹重定向来进一步优化用户的配置文件，以尽量减少用户配置文件大小的影响。应用文件夹重定向补充了 Profile Management 解决方案。有关详细信息，请参阅[Microsoft 文件夹重定向](#)。

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

此服务在交付 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）。安装了 Citrix VDA 的 Windows 计算机必须能够联系 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 Citrix DaaS 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](#)。

## 使用组策略设置配置 RDS 许可证服务器

1. 在其中一个可用的 VM 上安装远程桌面服务许可证服务器。VM 必须始终可用。Citrix DaaS 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。

## 消耗量承诺使用情况

注意：

此功能在预览版中提供。

在 **Manage**（管理）> **Quick Deploy**（快速部署）中，选择 **General**（常规）卡。**Consumption**（消耗量）值表示当前日历月内使用了多少消耗量。该值包括月度和定期承诺。

选择 **General**（常规）时，**Notifications**（通知）选项卡包括：

- 本月使用的总消耗量（每月和定期）。
- 每月消耗量承诺的单位数量。
- 定期消耗量承诺的百分比。

值和进度条可以提醒您注意潜在的或实际的使用超量。

实际数据可能需要 24 小时才能显示。使用情况和账单数据被视为一个日历月结束后的最后 72 小时。

有关更多使用信息，请参阅[监视许可证和活动使用情况](#)。

当消耗使用量（每月、定期或两种承诺）达到指定级别时，可以有选择地要求在 **Manage**（管理）> **Quick Deploy**（快速部署）控制板中显示通知。默认情况下，通知处于禁用状态。

1. 在 **Notifications**（通知）选项卡上，选择 **Edit Notification Preferences**（编辑通知首选项）。
2. 要启用通知，请单击滑块以便显示复选标记。
3. 输入一个值。如果需要，请对其他消耗量类型重复此操作。
4. 选择保存。

要禁用通知，请单击滑块以使复选标记不再显示，然后选择 **Save**（保存）。

## 监视 Citrix 许可证使用情况

要查看 Citrix 许可证使用情况信息，请按照[监视许可证和活动使用情况](#)中的指导进行操作。您可以查看：

- 许可摘要

- 使用情况报告
- 使用趋势和许可证活动
- 许可用户

您还可以发布许可证。

## 负载均衡

负载均衡适用于多会话计算机，而非单会话计算机。

重要：

更改负载均衡方法会影响您的部署中的所有目录。这包括使用任何受支持的主机类型（基于云和本地）创建的所有目录，与用于创建这些目录的界面（例如完整配置或快速部署）无关。

在继续操作之前，请确保为所有目录配置了最大会话限制。

- 在快速部署中，该设置位于每个目录的 **Details**（详细信息）选项卡上。
- 在完整配置中，请参阅[平衡计算机负载](#)。

负载均衡测量计算机负载，并确定在当前条件下为传入用户会话选择哪台多会话计算机。此选择基于配置的负载均衡方法。

可以配置两种负载均衡方法之一：水平或垂直。该方法适用于 Citrix DaaS 部署中的所有多会话目录（因此，适用于所有多会话计算机）。

- **Horizontal load balancing**（水平负载均衡）：将传入用户会话分配给可用的、负载最少且已打开电源的计算机。

示例：您有两台计算机，每台计算机配置了 10 个会话。第一台计算机处理五个并发会话。第二台计算机处理五个并发会话。

水平负载均衡提供了较高的用户性能，但随着更多的计算机处于打开电源和忙碌状态，它可能会增加成本。

默认启用此方法。

- **Vertical load balancing**（垂直负载均衡）：将传入用户会话分配给负载指数最高的已打开电源的计算机。Citrix DaaS 计算每台多会话计算机，然后为其分配负载指数。计算会考虑 CPU、内存和并发等因素。

此方法将使现有计算机饱和，然后再转移到新计算机。当用户断开连接并释放现有计算机上的容量时，将为这些计算机分配新负载。

示例：您有两台计算机，每台计算机配置了 10 个会话。第一台计算机处理前 10 个并发会话。第二台计算机处理第十一个会话。

通过垂直负载均衡，会话可以最大限度地提高已打开电源的计算机的容量，从而节省计算机成本。

要配置负载均衡方法，请执行以下操作：

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，展开右侧的 **General**（常规）。
2. 在 **Global Settings**（全局设置）下，选择 **View All**（查看全部）。
3. 在 **Global Settings**（全局设置）页面上的 **Multi-Session Catalog Load Balancing**（多会话目录负载均衡）下，选择负载平衡方法。
4. 选择确认。

## 在使用代理服务器的网络中创建目录

如果您的网络需要使用代理服务器建立 Internet 连接，并且您正在使用自己的 Azure 订阅，请遵循此过程。（不支持将 Citrix 托管 Azure 订阅与需要代理服务器的网络结合使用。）

1. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，首先通过提供所需的信息开始[目录创建过程](#)，然后选择页面底部的 **Create Catalog**（创建目录）。
2. 由于代理要求，目录创建失败。但是，创建了一个资源位置。该资源位置的名称以“DAS”开头，除非您在创建目录时提供了资源位置名称。在 **Manage**（管理）> **Quick Deploy**（快速部署）控制板上，展开右侧的 **Cloud Subscriptions**（云订阅）。在 **Resource Locations**（资源位置）选项卡上，检查新创建的资源位置中是否有任何 Cloud Connector。如果是，请将其删除。
3. 在 Azure 中，创建两个 VM（请参阅[Cloud Connector 系统要求](#)）。将这些计算机加入到域中。
4. 在 Citrix Cloud 控制台中，在每个 VM 上[安装 Cloud Connector](#)。确保 Cloud Connector 与之前创建的资源位置相同。请按照以下内容中的指导进行操作：
  - [Cloud Connector 代理和防火墙配置](#)
  - [系统和连接要求](#)
5. 在 **Manage**（管理）> **Quick Deploy**（快速部署）中，重复目录创建过程。创建目录时，它将使用您在上述步骤中创建的资源位置和 Cloud Connector。

## 获取帮助

- 请查看[故障排除](#)。
- 如果需要有关 Citrix DaaS 的进一步帮助，请按照[如何获取帮助和支持](#)中的指导开立一个票证。

## 创建交付组

March 5, 2024

## 简介

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。交付组还可以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，应先创建计算机目录，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。

在创建交付组之前，请注意以下事项：

- 查看本节以了解您所做的选择和提供的信息。
- 确保您已创建与虚拟机管理程序、云服务或其他托管计算机的资源连接。
- 确保已创建包含虚拟机或物理机的计算机目录。

要启动交付组创建向导，请执行以下操作：

1. 登录 [Citrix Cloud](#)。在左上角的菜单中，选择我的服务 > **DaaS**。
2. 选择管理。
3. 如果这是正在创建的第一个交付组，控制台将引导您完成正确的选择（例如“设置要显示为服务的交付组”）。交付组创建向导将打开并引导您完成该过程。
4. 如果您已经创建了交付组并想要创建另一个交付组，请按照以下步骤操作：
  - a) 在管理 > 完整配置中，选择左窗格中的交付组。
  - b) 要使用文件夹组织交付组，请在默认 交付组 文件夹下创建文件夹。有关更多信息，请参阅 [创建组文件夹](#)。
  - c) 选择要在其中创建组的文件夹，然后单击“创建交付组”。组创建向导打开。

该向导将引导您浏览以下部分中描述的页面。根据您所做的选择，您看到的向导页面可能会有所不同。

## 步骤 1. 计算机

选择一个计算机目录并选择要从该目录中使用的计算机数。

须知：

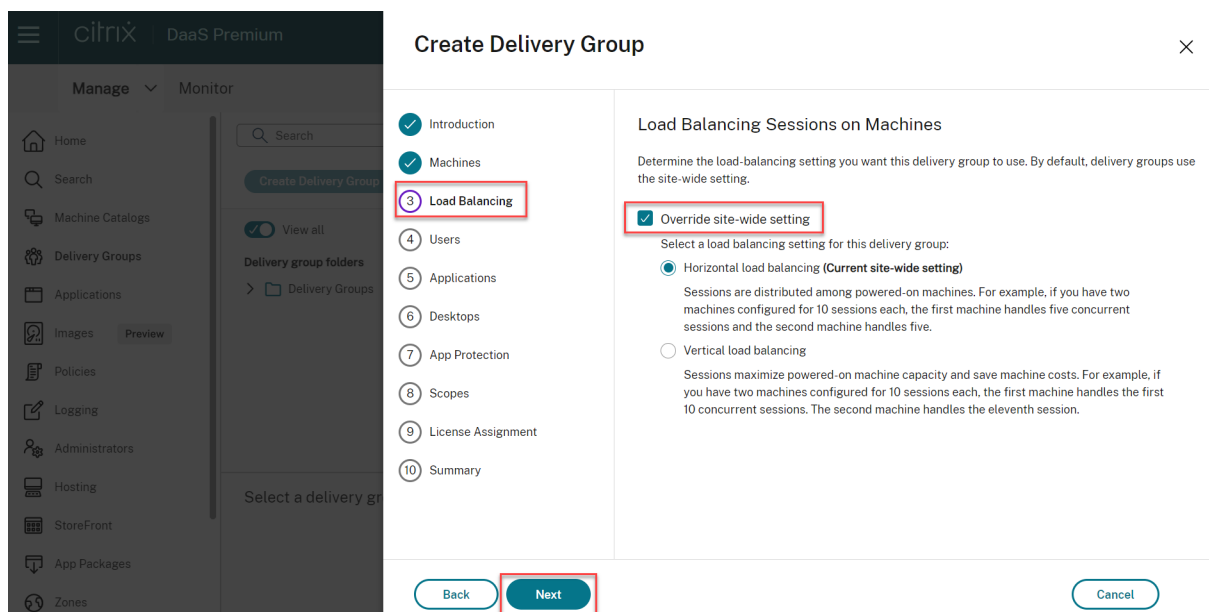
- 在选定的目录中，必须至少有一台计算机处于未使用状态。
- 可以在多个交付组中指定目录。但是，只能在一个交付组中使用计算机。
- 交付组可以使用多个目录中的计算机。但是，这些目录必须包含相同的计算机类型（多会话操作系统、单会话操作系统或 Remote PC Access）。换言之，您无法在交付组中混合使用多个计算机类型。同样，如果您的部署中包含 Windows 计算机的目录和 Linux 计算机的目录，则交付组可以包含其中一种操作系统类型中的计算机，但不能同时包含这两种操作系统类型中的计算机。
- MCS 交付组只能添加 MCS 类型的目录。

- Citrix 建议您使用最新版本安装或升级所有 VDA，然后根据需要对计算机目录和交付组执行更改功能级别。创建交付组时，如果选择安装了不同 VDA 版本的多台计算机，交付组将与最新版本的 VDA 兼容。例如，如果您选择的其中一台计算机安装了 VDA 7.1，其他计算机安装了更高版本，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，在该组中可能无法使用需要更高版本的 VDA 的某些功能。
- 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. 负载均衡（预览版）

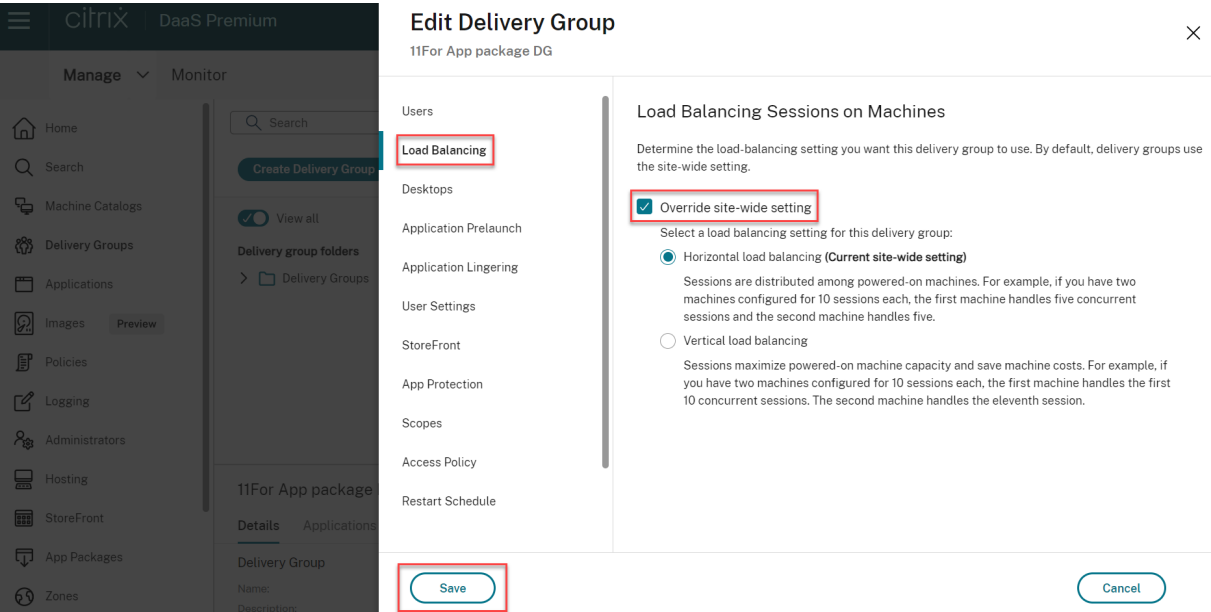
要在创建交付组时配置负载均衡设置，请执行以下操作：

1. 登录 DaaS Premium。
2. 在左侧导航中，单击交付组。
3. 在 交付组 页面中，单击 创建交付组。
4. 在创建交付组向导中，单击下一步。此时将打开计算机向导。
5. 在计算机向导中，选择所需的计算机目录，然后单击下一步。此时将打开负载均衡向导。
6. 在负载均衡向导中，选中“覆盖全站设置”复选框。
7. 根据需要选择“水平负载均衡”或“垂直负载均衡”选项，然后单击“下一步”。



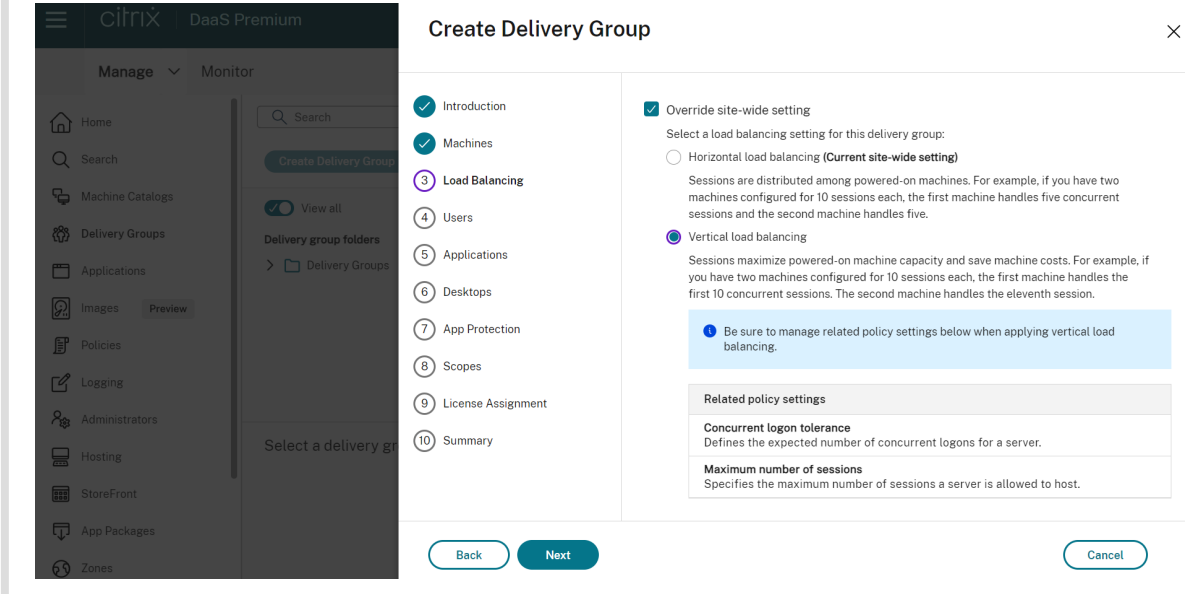
要在编辑现有交付组时配置负载均衡设置，请执行以下操作：

1. 登录 DaaS Premium。
2. 在左侧导航中，单击交付组。
3. 从列表选择一个 交付组，然后单击“编辑”。此时将打开编辑交付组向导。
4. 在编辑交付组页面中，单击负载均衡。
5. 选中 **Override site-wide setting**（覆盖站点范围的设置）复选框。
6. 根据需要选择 水平负载均衡 或 垂直负载均衡 选项，然后单击“保存”。



注意：

应用“垂直负载均衡”设置时，请确保正确配置并发登录容差和最大会话数策略。



有关站点级别和交付组级别的负载均衡的更多信息，请参阅 [负载均衡计算机](#)。



### 步骤 3. 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计算机目录后，才会显示此页面。选择应用程序或桌面。不能同时启用这两者。

如果您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，则假定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 4. AppDisk

请忽略此页面。选择“下一步”。

### 步骤 5. 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

用户列表是在您创建或编辑以下内容时指定的：

- 部署的用户访问列表，不是通过此控制台配置的。默认情况下，应用程序授权策略规则包括所有人。有关详细信息，请参阅 PowerShell SDK `BrokerAppEntitlementPolicyRule` cmdlet。
- 交付组。
- 应用程序。

注意：

指定用户列表时，您可以从 Citrix Cloud 帐户所连接的以下任何身份提供商中选择用户帐户：Active Directory、Azure Active Directory 或 Okta。

能够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。

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。（对于包含桌面操作系统计算机的交付组，您可以在以后通过编辑交付组导入用户数据（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都必须安装多会话 OS VDA。启用未经身份验证的用户时，您必须具有未经身份验证的 StoreFront 存储。

启动会话时，将按需创建未经身份验证的用户帐户，并命名为 AnonXYZ，其中，XYZ 是一个唯一的三位数值。

未经身份验证的用户会话的默认空闲超时为 10 分钟，当客户端断开连接时，这些会话将自动注销。不支持重新连接、客户端之间漫游以及工作区控制。

下表介绍了用户页面上的选项：

		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？
启用访问权限的用户	是否添加/分配用户和用户组？	
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

限制用户或组访问权限

您还可以通过将用户或用户组添加到允许列表来限制交付组的使用。只有允许列表中的用户才能访问交付组中的应用程序和桌面。您还可以通过单击添加阻止列表将用户和用户组添加到阻止列表中，这会阻止用户使用所选交付组中的应用程序和桌面。只有在用于屏蔽允许列表中的用户时，屏蔽列表才有意义。

步骤 6. 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将放置在名为 Applications 的文件夹中。可以指定其他文件夹。有关详细信息，请参阅[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[应用程序](#)一文。
- 如果您尝试添加某个应用程序，但同一文件夹中已存在同名应用程序，则系统将提示您重命名要添加的应用程序。如果拒绝，添加的应用程序将附带一个后缀，使其在该应用程序文件夹中成为唯一的存在。

- 在将某个应用程序添加到多个交付组中时，如果您无权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。
- 如果要向相同的用户发布两个同名应用程序，请更改“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。

选择添加菜单以显示应用程序源。

- 从“开始”菜单：此类应用程序是在通过映像创建的计算机上发现的，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，然后选择确定。
- 手动定义：位于部署中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，选择确定。
- 现有：此类应用程序以前已添加到部署中，可能位于另一个交付组。如果选择此源，则会启动一个新页面，其中会列出已发现的应用程序；请选择您要添加的应用程序，然后选择确定。
- **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，然后选择确定。

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，如果部署中没有添加任何应用程序，则无法使用现有源。或者，应用程序也可能与所选计算机目录中的计算机上支持的会话类型不兼容。

## 步骤 7. App Protection

以下信息是 Citrix Virtual Apps and Desktops 文档中的 [App Protection](#) 文章的补充。要在 Citrix DaaS 部署中使用 App Protection，请遵循该文章中的一般指导，注意以下细节。

- 您必须拥有有效的 Citrix Cloud 订阅和有效的 App Protection 权限。要购买 App Protection 功能，您可以联系您的 Citrix 销售代表。
- App Protection 需要 XML 信任。要启用 XML 信任，请转到设置 > 启用 **XML** 信任。
- 关于反屏幕捕获：
  - 在 Windows 和 macOS 上，只有受保护的内容的窗口是空白的。当受保护的窗口未最小化时，App Protection 处于活动状态。
  - 在 Linux 中，整个捕获内容是空白的。无论受保护的窗口是否最小化，App Protection 都处于活动状态。

## 步骤 8. 桌面（或桌面分配规则）

此页面的标题取决于您先前在向导中选择的计算机目录：

- 如果所选目录包含池计算机，则此页面的标题为桌面。
- 如果您选择了包含已分配计算机的目录并在 交付类型 页面上指定了“桌面”，则此页面的标题为 桌面分配规则。
- 如果您在 交付类型 页面上选择包含已分配计算机和指定的“应用程序”的目录，则此页面的标题为 应用程序。

选择添加。在此对话框中：

- 在显示名称和说明字段中，键入要在 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，然后从菜单中选择标记。
- 使用单选按钮，您可以：
  - 允许有权访问此交付组的所有人使用桌面。交付组中的所有用户都可以启动桌面（适用于包含池化计算机的组），也可以在启动桌面时为其分配计算机（适用于具有已分配计算机的组）。
  - 通过将用户和用户组添加到允许列表来限制桌面的使用。只有允许列表中的用户才能访问桌面。您还可以通过单击添加阻止列表将用户和用户组添加到阻止列表中，这会阻止用户使用所选交付组中的桌面。只有在用于屏蔽允许列表中的用户时，屏蔽列表才有意义。
- 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，请选择确定。

## 步骤 9. 许可证分配

确定您希望交付组使用哪个许可证。默认情况下，交付组使用站点许可证。有关详细信息，请参阅[多类型许可](#)。

## 步骤 10：本地主机缓存设置

此设置仅对包含使用 MCS 或 Citrix Provisioning 置备的单会话池计算机的交付组可见。

默认情况下，这些计算机在本地主机缓存 (LHC) 模式下不可用。要在 LHC 模式下更改默认行为并使其可用于新用户连接，请选择“保持资源可用”。

或者，您可以使用 PowerShell 命令更改默认行为。有关更多信息，请参阅[应用程序和桌面支持](#)。

### 重要提示：

启用对电源管理的单会话池计算机的访问权限可能会导致先前用户会话中的数据和更改出现在后续会话中。

## 步骤 11. 总结

输入交付组的名称。您也可以（选择性）输入说明，该说明显示在 Workspace 应用程序和“完整配置”管理界面中。

查看摘要信息，然后单击完成。如果您没有选择或指定任何要交付的应用程序或桌面，系统会询问您是否要继续。

## 更多信息

- [管理交付组](#)
- [Applications](#)

管理交付组

March 30, 2024

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。

这些过程按类别进行组织：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。因此，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

- 查看组详细信息
- 更改交付类型
- 更改 StoreFront 地址
- 更改功能级别
- 管理 Remote PC Access 交付组
- 更改交付组的许可证
- 使用文件夹整理交付组
- 管理 App Protection

查看组详细信息

1. 使用搜索功能查找特定的交付组。有关说明，请参阅[搜索实例](#)。
2. 根据需要从搜索结果中选择一个组。
3. 有关组列的描述，请参阅下表。
4. 单击底部详细信息窗格中的选项卡，了解有关该组的更多信息。

列	说明
交付组	组名称和会话类型。会话类型包括单会话操作系统和多会话操作系统。

列	说明
交付	从该组交付的资源类型。可能的值包括应用程序、桌面以及应用程序和桌面。如果交付组由专用计算机组成，则会显示“静态计算机分配”。
正在使用的会话	已设置的计算机数量和处于“已断开连接”状态的计算机数量。
分配的数量	目录中分配给交付组的计算机数量。
文件夹	该组在交付组树中的位置。它显示该组所在的文件夹的名称（包括尾部的反斜杠），或者 -（如果该组位于根级别）。

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。

在将应用程序类型更改为桌面类型之前，请从组中删除所有应用程序。

1. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择一个组，然后在操作栏中选择编辑。
3. 在交付类型页面上，选择所需的交付类型。
4. 选择应用以应用所做的任何更改并使窗口保持打开状态。或者，选择确定应用所做的更改并关闭窗口。

更改 **StoreFront** 地址

1. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择一个组，然后在操作栏中选择编辑。
3. 在 **StoreFront** 页面上，指出是稍后指定 StoreFront 服务器地址（手动）还是选择新增以指定要使用的 StoreFront 服务器（自动）。
4. 选择应用以应用所做的任何更改并使窗口保持打开状态。或者，选择确定应用所做的更改并关闭窗口。

也可以通过在控制台的左侧窗格中选择 **StoreFront** 来指定 StoreFront 服务器地址。

更改功能级别

升级交付组计算机上的 VDA 以及包含交付组中使用的计算机的计算机目录后，更改交付组的功能级别。

开始之前：

- 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。

- 启动包含升级后的 VDA 的计算机，以便它们可以在 Citrix DaaS 中注册。此过程告知控制台交付组中必须进行哪些更改。
- 如果必须使用早期的 VDA 版本，更新的产品功能可能不可用。有关详细信息，请参阅升级文档。

要更改交付组的功能级别，请执行以下操作：

1. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择一个组，然后在操作栏中选择“更改功能级别”。只有检测到升级的 VDA 时，才会出现“更改功能级别”操作。

显示屏会显示哪些计算机（如果有）无法更改为功能级别以及原因。然后，您可以取消更改操作，解决计算机问题，然后再次执行更改操作。

更改完成后，可以将计算机还原到以前的状态。选择交付组，然后在操作栏中选择撤消功能级别更改。

### 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给用户，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或用户需要计算机分配时，将计算机分配给哪个交付组：值越低，优先级越高。如果 Remote PC Access 计算机目录具有多个交付组分配，该软件将选择优先级最高的匹配项。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。此关联意味着添加到目录的计算机帐户或组织单位稍后可以添加到交付组。此关联可以关闭或开启。

添加或删除 Remote PC Access 计算机目录与交付组的关联：

1. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择 Remote PC Access 组。
3. 在详细信息部分，选择计算机目录选项卡，然后选择 Remote PC Access 目录。
4. 要添加或还原关联，请选择添加桌面。要删除关联，请选择删除关联。

### 更改交付组的许可证

要更改交付组的许可证权利，请执行以下步骤：

1. 在导航窗格中选择交付组。
2. 选择一个组，然后在操作栏中单击编辑。
3. 在许可证分配页面上，选择您希望组使用的许可证。
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，单击保存应用所做的更改并关闭窗口。

有关交付组级权利的更多信息，请参阅[多类型许可](#)。

## 使用文件夹整理交付组

可以创建文件夹来整理交付组以便于轻松访问。

**必需的角色** 默认情况下，您需要具有以下内置角色才能创建和管理交付组文件夹：云管理员、完全权限管理员或交付组管理员。如有必要，您可以自定义用于创建和管理交付组文件夹的角色。有关详细信息，请参阅 [必需权限](#)。

**创建交付组文件夹** 在开始之前，请先计划如何整理您的交付组。请注意以下事项：

- 最多可以嵌套五级文件夹（不包括默认的根本文件夹）。
- 一个文件夹可以包含交付组和子文件夹。
- 完整配置 中的所有节点（例如计算机目录、应用程序和交付组节点）在后端共享一个文件夹树。为避免在重命名或移动文件夹时与其他节点发生名称冲突，我们建议您为不同节点中的第一级文件夹指定不同的名称。

要创建交付组文件夹，请执行以下步骤：

1. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 在文件夹层次结构中，选择一个文件夹，然后在操作栏中选择创建文件夹。
3. 输入新文件夹的名称，然后单击完成。

提示：

如果您在非预期位置创建文件夹，则可以将其拖动到正确的位置。

## 移动交付组

您可以在文件夹之间移动交付组。详细步骤如下所示：

1. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 按文件夹查看组。也可以打开文件夹层次结构上方的查看全部以同时查看所有组。
3. 在某个组上单击鼠标右键，然后选择移动交付组。
4. 选择要将该组移动到的文件夹，然后单击完成。

提示：

您可以将组拖到文件夹中。

## 管理交付组文件夹

您可以删除、重命名和移动交付组文件夹。

请注意，仅当文件夹及其子文件夹不包含交付组时，才能删除该文件夹。

要管理文件夹，请执行以下步骤：



1. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 在文件夹层次结构中，选择一个文件夹，然后根据需要在 操作 栏中选择一个操作：
  - 要重命名文件夹，请选择重命名文件夹。
  - 要删除文件夹，请选择删除文件夹。
  - 要移动文件夹，请选择移动文件夹。
3. 请按照屏幕上的说明完成其余步骤。

所需的权限 下表列出了对交付组文件夹执行操作所需的权限。

操作	所需的权限
创建交付组文件夹	创建交付组文件夹
删除交付组文件夹	删除交付组文件夹
移动交付组文件夹	移动交付组文件夹
重命名交付组文件夹	编辑交付组文件夹
将交付组移动到文件夹中	编辑交付组文件夹和编辑交付组属性

管理 **App Protection**

以下信息是 Citrix Virtual Apps and Desktops 文档中的 [App Protection](#) 文章的补充。要在 Citrix DaaS 部署中使用 App Protection，请遵循该文章中的一般指导，注意以下细节。

1. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择一个组，然后在操作栏中选择编辑。
3. 在 **App Protection** 页面上，您可以启用防键盘记录和防屏幕截图。
  - 您必须拥有有效的 Citrix Cloud 订阅和有效的 App Protection 权限。要购买 App Protection 功能，您可以联系您的 Citrix 销售代表。
  - App Protection 需要 XML 信任。要启用 XML 信任，请转到设置 > 启用 **XML** 信任。
  - 关于反屏幕捕获：
    - 在 Windows 和 macOS 上，只有受保护的内容的窗口是空白的。当受保护的窗口未最小化时，App Protection 处于活动状态。
    - 在 Linux 中，整个捕获内容是空白的。无论受保护的窗口是否最小化，App Protection 都处于活动状态。

用户

注意：

“将用户管理留给 **Citrix Cloud**” 选项已被删除。要管理设置为将用户管理留给 **Citrix Cloud** 的现有交付组的用户分配，有两种选择：Citrix Cloud 库或“完整配置”。有关完整配置方法的更多信息，请参阅管理 Citrix Cloud 库管理的交付组的用户分配。

本主题涵盖以下部分：

- 更改用户设置
- 添加或删除用户
- 管理 Citrix Cloud 库管理的交付组的用户分配

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. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择一个组，然后在操作栏中选择编辑。
3. 在用户设置页面上，更改下表中的任何设置。
4. 选择应用以应用所做的任何更改并使窗口保持打开状态。或者，选择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。注意：更改交付组上的时区可能会重新启动该交付组中的计算机。为了避免这种情况，请务必在非生产时间更改时区设置。
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。
每个用户的最大桌面数	用户可以拥有的桌面数量。

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. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择一个组，然后在操作栏中选择编辑交付组。
3. 在用户页面上：
  - 要添加用户，请选择添加，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，然后选择删除。
  - 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. 选择应用以应用所做的任何更改并使窗口保持打开状态。或者，选择确定应用所做的更改并关闭窗口。

管理用户分配 要管理用户分配，请执行以下操作：

1. 在管理 > 完整配置中，选择交付组。
2. 选择一个组，然后在操作栏中选择编辑。
3. 在计算机分配页面上，添加或删除用户。要添加用户，请浏览至这些用户，或输入以分号分隔的用户名列表。

输入用户名时，请考虑以下事项：

- 如果用户在 Active Directory 中，请直接输入名称。如果没有，请按以下格式输入名称：<identity provider>:<user name>。示例：AzureAD:username。

#### 管理 Citrix Cloud 库管理的交付组的用户分配

要管理由 Citrix Cloud 库管理的交付组的用户分配，请使用 Citrix Cloud 库或“完整配置”。

要使用“完整配置”完成此任务，请执行以下步骤：

1. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择 Citrix Cloud 管理的交付组，然后在操作栏中选择编辑。
3. 要限制某些用户使用桌面，请按照以下步骤操作：
  - a) 在“桌面”或“桌面分配规则”页面上，选择桌面并单击“编辑”。将出现“编辑桌面”页面，并选择“限制桌面使用”选项。
  - b) 单击“添加”，根据需要选择一个或多个用户，然后单击“完成”。
  - c) 单击确定。
4. 要限制特定用户使用该组中的应用程序，请在左侧窗格中单击“应用程序分配规则”，然后按照步骤 3 中描述的类似步骤添加用户。

#### 计算机

- 更改用户的计算机分配情况

- 为单会话池 VDA 启用本地主机缓存
- 更新计算机
- 为桌面添加、更改或删除标记限制
- 删除计算机
- 限制对资源的访问
- 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
- 管理计算机负载
- 管理 AutoScale

除了本文中介绍的功能外，请参阅 [AutoScale](#) 了解有关主动对计算机进行电源管理的信息。

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. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择一个组，然后在操作栏中选择编辑。
3. 在计算机分配页面上，指定新用户。
4. 选择应用以应用所做的任何更改并使窗口保持打开状态。或者，选择确定应用所做的更改并关闭窗口。

为单会话池 **VDA** 启用本地主机缓存

默认情况下，使用 MCS 或 Citrix Provisioning 置备的单会话池计算机在本地主机缓存模式下不可用。您可以针对每个交付组覆盖默认行为。详细步骤如下所示：

1. 在管理 > 完整配置中，选择左窗格中的交付组。  
在组列表中，包含由 MCS 或 Citrix Provisioning 置备的单会话池计算机的组显示警告图标。
2. 根据需要选择一个组，然后在操作栏中选择编辑。
3. 在“本地主机缓存”页面上，选择“保持资源可用”。
4. 选择应用以应用所做的任何更改并使窗口保持打开状态。或者，选择确定应用所做的更改并关闭窗口。

或者，您可以使用 PowerShell 命令覆盖默认行为。有关更多信息，请参阅[应用程序和桌面支持](#)。

重要：

启用对电源管理的单会话池计算机的访问权限可能会导致先前用户会话中的数据和更改出现在后续会话中。

### 更新交付组中的计算机

1. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择一个组，然后在操作栏中选择查看计算机。
3. 选择一台计算机，然后在操作栏中选择更新计算机。

要选择其他映像，请选择“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
- 用户将收到的消息

### 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考虑启动的桌面有意外影响。请查看[标记](#)中的注意事项和警告。

1. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择一个组，然后在操作栏中选择编辑。
3. 在桌面页面上，选择桌面并选择编辑。
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. 选择应用以应用所做的任何更改并使窗口保持打开状态。或者，选择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. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择一个组，然后在操作栏中选择查看计算机。
3. 请确保所有计算机都已关闭。

4. 选择计算机，然后在操作栏中选择从交付组中删除。

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。

限制对交付组中资源的访问权限

无论使用何种方法，您为限制对交付组中资源的访问所做的任何更改都将取代先前的设置。您可以：

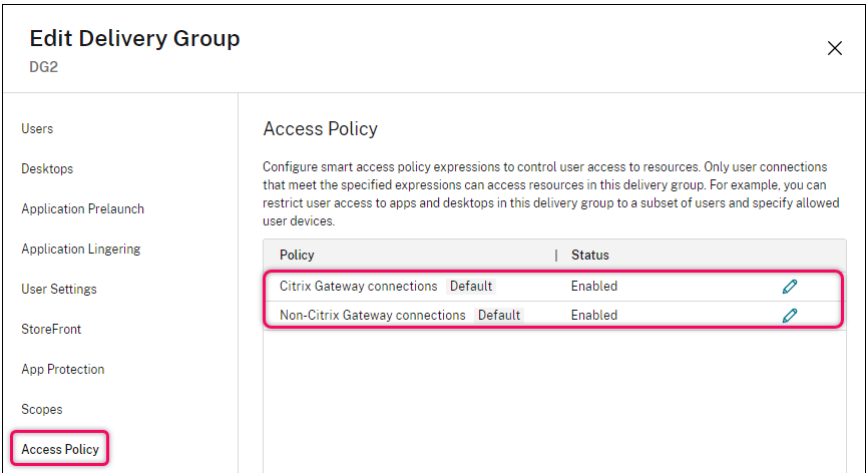
- 使用委托管理作用域限制管理员的访问权限：您可以创建和分配一个允许管理员访问所有应用程序的作用域和另一个仅提供对特定应用程序访问权限的作用域。有关详细信息，请参阅[委派管理](#)。
- 通过智能访问策略表达式限制用户的访问权限：您可以配置访问策略规则来控制用户对特定交付组的访问权限。示例包括：
  - 限制部分用户的访问权限并指定允许的用户设备。
  - 限制通过 Workspace（而非 StoreFront）连接的用户的访问权限。
  - 限制通过特定 Workspace URL 连接的用户的访问权限。

本节指导您如何通过访问策略规则限制用户对交付组的访问权限：

- 关于访问策略规则
- 添加访问策略规则
- 使用完整配置管理访问策略规则
- 使用 PowerShell 添加和完善策略规则

**关于访问策略规则** 您可以为交付组配置多访问策略规则。当用户的连接符合您为交付组定义的任何访问策略规则时，无论顺序如何，交付组中的应用程序和桌面都会显示在用户的 StoreFront 或 Workspace 中。

可以单独启用或禁用每条规则。评估访问策略时，禁用的规则将被忽略。



在完整配置中，访问策略列表包括以下默认 SmartAccess 策略规则。您可以根据需要添加更多。

- **Citrix Gateway** 连接。此策略仅允许通过 Citrix Gateway 建立的用户连接访问交付组中的资源。启用“设备状态”或“网络位置”功能时通过 Workspace 建立的用户连接也被视为通过 Citrix Gateway 建立的连接。
- 非 **Citrix Gateway** 连接。此策略仅允许非通过 Citrix Gateway 建立的用户连接才能访问交付组中的资源。

注意：

- 为防止默认规则覆盖新配置的规则，必须禁用默认规则或对其进行细化以排除新策略中使用的过滤器。
- 无法删除默认策略，但可以将其禁用。要禁用策略，请单击“编辑”图标，然后将策略状态更改为“已禁用”。
- 策略列表还显示了使用 PowerShell 命令添加的规则。这些策略可以删除，但不能在“完整配置”中编辑。

使用完整配置添加访问策略规则 访问策略规则由一组过滤器组成。有关过滤器的更多信息，请参阅[本文](#)。添加访问策略规则时，您可以根据需要向该规则添加多个条件过滤器。

要使用完整配置为交付组添加策略，请执行以下步骤：

1. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择一个组，然后在操作栏中单击编辑。
3. 在“访问策略”页面上，单击“添加”。将出现“添加策略”页面。

4. 在“策略名称”字段中，键入策略的描述性名称。该名称在您的部署中必须是唯一的。
5. 要定义允许的用户连接的标准，请执行以下步骤：
  - a) 选择符合以下条件的连接。
  - b) 单击“添加标准”。
  - c) 在“过滤器”字段中，键入要使用的过滤器的名称。在“值”字段中，为过滤器键入所需的值。例如，要仅允许通过 Workspace（而非 StoreFront）连接的用户访问此交付组中的资源，请键入 `Citrix-Via-Workspace` 表示过滤器，键入 `True` 表示值。

d) 要添加更多标准，请重复步骤 b-c。

e) 选择标准之间的关系：

- 匹配任意。仅当传入用户连接满足任何已配置的筛选条件时才允许访问。
- 全部匹配。仅当传入用户连接满足所有已配置的筛选条件时才允许访问。

6. 要定义禁止用户连接的标准，请执行以下步骤：

a) 选择“不符合以下任何条件的连接”。

b) 单击“添加标准”。

c) 在“过滤器”字段中，键入要使用的过滤器的名称。在“值”字段中，为过滤器键入所需的值。例如，禁止通过 `example.cloud.com` Workspace URL 连接的用户访问此交付组中的资源。键入 `Citrix.Workspace.UsingDomain` 表示过滤器，键入 `example.cloud.com` 表示值。

d) 要添加更多标准，请重复步骤 b-c。

注意：

禁止符合任何配置条件的用户连接访问此交付组中的资源。

7. 单击完成。

新策略出现在策略列表中。

8. 审查和完善默认策略规则，以避免无意中与本新政策所涵盖的连接重叠。要完善现有政策，请使用以下方法：

- 禁用默认策略规则。
- 配置默认策略规则，将您添加到新策略的包含条件中的 SmartAccess 过滤器排除在外。有关更多信息，请参阅使用完整配置管理策略规则和使用 PowerShell 添加和管理访问策略规则。

重要：

如关于访问策略规则中所述，当用户的连接与交付组中的一个或多个策略规则相匹配时，用户将获得对其资源的访问权限。因此，创建规则后，必须仔细检查和完善现有规则，以避免与新规则涵盖的连接发生任何无意的重叠。

**使用完整配置管理访问策略规则** 您可以使用包含和排除标准来完善默认策略。例如，要限制对这些连接子集的访问权限，请执行以下步骤：

1. 编辑默认策略。
2. 选择符合以下任一条件的连接。
3. 添加、编辑或删除允许用户访问方案的 SmartAccess 策略表达式。

有关详细信息，请参阅 Citrix Gateway 文档。



使用 **PowerShell** 添加和管理访问策略规则 您可以使用以下 PowerShell cmdlet 来添加和管理交付组的访问策略规则：

- New-BrokerAccessPolicyRule
- Get-BrokerAccessPolicyRule
- Set-BrokerAccessPolicyRule
- Rename-BrokerAccessPolicyRule
- Remove-BrokerAccessPolicyRule

有关详细信息，请参阅 [Citrix Developer 文档](#) 中的相关文章。

#### 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：

1. 在管理 > 完整配置中，选择左窗格中的交付组。
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，请在操作栏中选择打开维护模式。

要为一台计算机打开维护模式，请在操作栏中选择查看计算机。选择计算机，然后在操作栏中选择打开维护模式。

4. 要针对交付组中的一台或所有计算机关闭维护模式，请按照之前的说明操作，但要在操作栏中选择关闭维护模式。

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“不允许连接到此计算机”，“远程主机配置用户登录模式”设置为“允许重新连接，但阻止新登录”或“允许重新连接”，但在服务器重新启动之前禁止新登录。

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. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择一个组，然后在操作栏中选择查看计算机。
3. 选择计算机，然后在操作栏中选择以下操作之一：

注意：

- 以下操作仅适用于受电源管理的计算机。
- 某些选项可能不可用，具体取决于计算机状态。
- 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。

在交付组中创建和管理计算机的重新启动计划

注意：

- 将重新启动计划应用于启用了 AutoScale 的交付组时，其计算机只是关闭电源，并让 AutoScale 打开其电源。
- 将重新启动计划应用于随机单会话计算机时，这些计算机将关闭电源而不是重新启动，以节省成本。我们建议您使用 AutoScale 来打开计算机电源。
- 更改交付组上的时区可能会重新启动该交付组中的计算机。为了避免这种情况，请务必在非生产时间更改时区设置。

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（在此例中为计算机）。

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。持续时间是指“同时启动所有受影响的计算机”或重新启动所有受影响的计算机很可能采用的时间间隔。

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. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择一个组，然后在操作栏中选择编辑。
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。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。

**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（应用）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。

1. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择包含受计划控制的计算机的组。
3. 选择查看计算机，然后选择要为其添加标记的计算机。
4. 选择操作栏中的管理标记。
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，请选择创建，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选择保存。

## 创建重新启动计划

1. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择一个组，然后在操作栏中选择编辑。
3. 在重新启动计划页面上，选择添加。
4. 在添加重新启动计划页面上：
  - 要启用该计划，请选择是。要禁用该计划，请选择否。
  - 键入计划名称和描述。
  - 对于限制标记，请应用标记限制。
  - 对于包括处于维护模式的计算机，请选择是否包括此计划中处于维护模式的计算机。要改用 PowerShell，请参阅对处于维护模式的计算机执行计划的重新启动。
  - 对于重新启动频率，请选择进行重新启动的频率：每日、每周或每月或一次。如果选择每周或每月，则可以指定一个或多个特定日期。
  - 对于重复间隔，请指定您希望计划运行的频率。
  - 对于开始日期，请指定计划首次发生的开始日期。
  - 对于重新启动开始时间，请使用 24 小时制格式指定开始重新启动的时间。
  - 对于重新启动持续时间：
    - 如果不想使用自然重新启动，请选择同时重新启动所有计算机或在一段时间内重新启动所有计算机。
    - 如果想使用自然重新启动，请选择耗尽所有会话后重新启动所有计算机。

在启动配置为使用自然重新启动的重新启动计划时：

- ★ 属于交付组的所有空闲计算机将立即重新启动
- ★ 注销所有会话后，属于交付的每台具有一个或多个活动会话的计算机都将重新启动。

注意：

可以将此选项用于进行电源管理的计算机以及未进行电源管理的计算机。

- 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适用计算机的通知消息。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五分钟重复显示此消息一次。默认情况下，不会重复显示该消息。
- 输入通知标题和文本。不存在默认文本。

如果您希望消息包含重新启动倒计时，请包含变量 **%m%**。除非选择同时启动所有计算机，否则在重新启动之前的相应时间，每台计算机上均会显示该消息。

5. 单击完成以应用所做的更改并关闭添加重新启动计划窗口。
6. 单击应用以应用所做的更改并使编辑交付组窗口保持打开状态。或者，单击保存应用所做的更改并关闭窗口。

**立即运行重新启动计划** 重新启动计划指定交付组中的计算机何时定期重新启动。还可以立即运行重新启动计划以重新启动该计划中的计算机。

要立即运行重新启动计划，请执行以下步骤：

1. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择适用的交付组，然后选择操作栏中的编辑
3. 在重新启动计划页面上，选择要运行的计划，然后选择立即运行计划。

注意：

- 如果配置了耗尽会话后重新启动所有计算机设置，则无法立即运行计划。
- 一次只能对一个计划应用立即运行计划。
- 编辑计划之后，立即运行计划将变得不可用。选择应用以使其可用。

**编辑、删除、启用或禁用重新启动计划**

1. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择一个组，然后在操作栏中选择编辑。
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，请选择编辑。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，请选择编辑。选中或取消选中启用重新启动计划复选框。
  - 要删除计划，请选择删除。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。此操作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（从凌晨 3 点开始）重新启动。站点数据库会在计划的重新启动开始前一小时（凌晨 2 点）发生中断。中断将持续六个小时（直到上午 8 点）。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 现在在原始计划后的五小时开始重新启动。此操作可能会导致 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。

对处于维护模式的计算机执行计划的重新启动 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和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。

## 对交付组中的计算机进行负载管理

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当前不可用。

可以在 Director（监视）、“完整配置”管理界面搜索和 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 [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。

## 管理 **AutoScale**

默认情况下，对交付组禁用 **AutoScale**。要管理交付组的 **AutoScale**（如果适用），请执行以下步骤：

1. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择一个组，然后选择操作栏中的管理 **AutoScale**。此时将显示管理 **AutoScale** 窗口。
3. 根据需要配置设置。有关 **AutoScale** 设置的信息，请参阅 [AutoScale](#)。
4. 选择应用以应用所做的任何更改并使窗口保持打开状态。或者，选择保存应用所做的更改并关闭窗口。

## 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
- 配置会话漫游
- 在维护模式下从计算机断开连接时控制会话重新连接

注销或断开会话或者向“交付组”用户发送消息

1. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择一个组，然后在操作栏中选择查看计算机。
3. 要使用户注销会话，请选择会话或桌面，然后在操作栏中选择注销。会话随即关闭，此时计算机可供其他用户使用，除非已将其分配给特定用户。
4. 要断开会话，请选择会话或桌面，然后在操作栏中选择断开连接。应用程序继续运行，计算机仍分配给此用户。用户可以重新连接同一计算机。
5. 要向用户发送消息，请选择会话、计算机或用户，然后在操作栏中选择发送消息。输入消息。

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可通过以下方式帮助指定用户快速访问应用程序：

- 在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后保持应用程序会话处于活动状态（会话延迟）

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，而且还需更多 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。
- 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。
- 对于定制这些功能以实现互补而言，仔细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. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择一个组，然后在操作栏中选择编辑。
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。
- 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。

Edit Delivery Group

×

Application Prelaunch

Application Lingering

User Settings

StoreFront

Scopes

Restart Schedule

License Assignment

Prelaunch Sessions for Applications

With prelaunch, sessions launch when users log on to Citrix Workspace app, so applications are available sooner.

When do you want sessions to launch?

☒ Launch when users start an application (no prelaunch)

☐ Prelaunch when any user in the delivery group logs on to Citrix Workspace app for Windows

☐ Prelaunch when any of the following users log on to Citrix Workspace app for Windows:

If no application is started, when do you want prelaunched sessions to end?

After a specified time:

Hours

8

☐ When average load on all machines exceeds (%):

0

☐ The load on any machine exceeds (%):

0

Save

Apply

Cancel

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. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择一个组，然后在操作栏中选择编辑。
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。

Edit Delivery Group

Application Prelaunch

Application Linging

User Settings

StoreFront

Scopes

Restart Schedule

License Assignment

Lingering Sessions for Applications

With lingering, sessions remain active after all applications are closed.

When do you want sessions to launch?

☐ Immediately after all applications in the session are closed (no lingering)

☒ Keep sessions active until:

After a specified time:

Hours

8

☐ The average load on all machines exceeds (%):

0

☐ The load on any machine exceeds (%):

0

Save

Apply

Cancel

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。

配置会话漫游

默认情况下，交付组的会话漫游处于启用状态。会话随用户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同时可用。您可以在多个设备上查看应用程序。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。或者，也可以使用 PowerShell。有关详细信息，请参阅[会话漫游](#)。

为应用程序配置会话漫游 要为应用程序配置会话漫游，请执行以下步骤：

1. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择一个组，然后在操作栏中选择编辑交付组。
3. 在 **Users**（用户）页面上，选中 **Sessions roam with users as they move between devices**（当用户在设备之间移动时会话随用户漫游）复选框来启用会话漫游。
  - 启用后，如果用户启动了一个应用程序会话，然后再移动到另一台设备时，则将使用相同的会话，并且应用程序在两台设备上均可用。禁用后，会话将不再在设备之间漫游。

4. 选择确定应用所做的更改并关闭窗口。

为桌面配置会话漫游 要为桌面配置会话漫游，请执行以下步骤：

1. 在管理 > 完整配置中，选择左窗格中的交付组。
2. 选择一个组，然后在操作栏中选择编辑交付组。
3. 在桌面页面上，选择桌面并选择编辑。
4. 通过选中会话漫游复选框启用会话漫游。
  - 启用后，如果用户启动了一个桌面，然后再移动到另一台设备时，则将使用相同的会话，并且应用程序在两台设备上均可用。禁用后，会话将不再在设备之间漫游。
5. 选择确定应用所做的更改并关闭窗口。

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。

2021 年 5 月底之前，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。现在，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（无论会话类型为何）。

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。

- 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指示预期注册但未注册的计算机数。例如，一台或多台计算机已开机，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

August 14, 2023

### 简介

可以借助应用程序组管理应用程序的集合。可为在不同交付组之间共享的应用程序或由交付组中的部分用户使用的应用程序创建应用程序组。应用程序组是可选的。它们提供了向多个交付组添加相同应用程序的备选方法。交付组可与多个应用程序组相关联，应用程序组可与多个交付组关联。

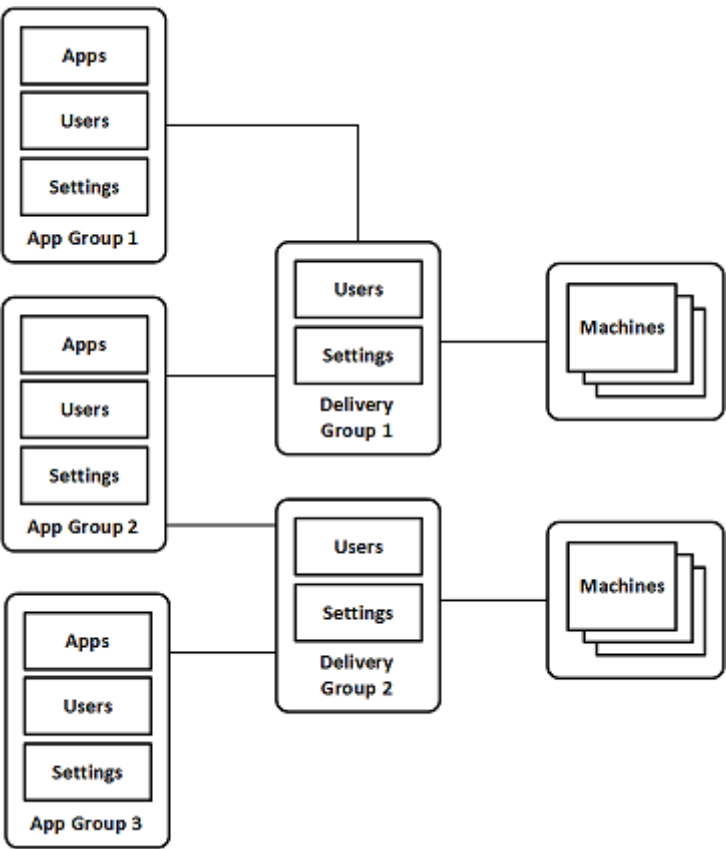
与使用多个交付组相比，使用应用程序组可以提供应用程序管理和资源控制优势：

- 通过对应用程序及其设置进行逻辑分组，可以作为一个单元来管理这些应用程序。例如，不需要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可能非常有益。
- 可以使用标记限制功能从应用程序组发布应用程序，仅考虑所选交付组中的一部分计算机。通过使用标记限制，可以使用现有计算机来完成多个发布任务，从而节省与部署和管理其他计算机有关的成本。标记限制可以视为对交付组中的计算机进行划分（或分区）。对交付组中的一部分计算机进行隔离和故障排除时，将应用程序组或桌面与标记限制结合使用很有帮助。

### 示例配置

#### 示例 1

下图显示了一个包含多个应用程序组的部署：



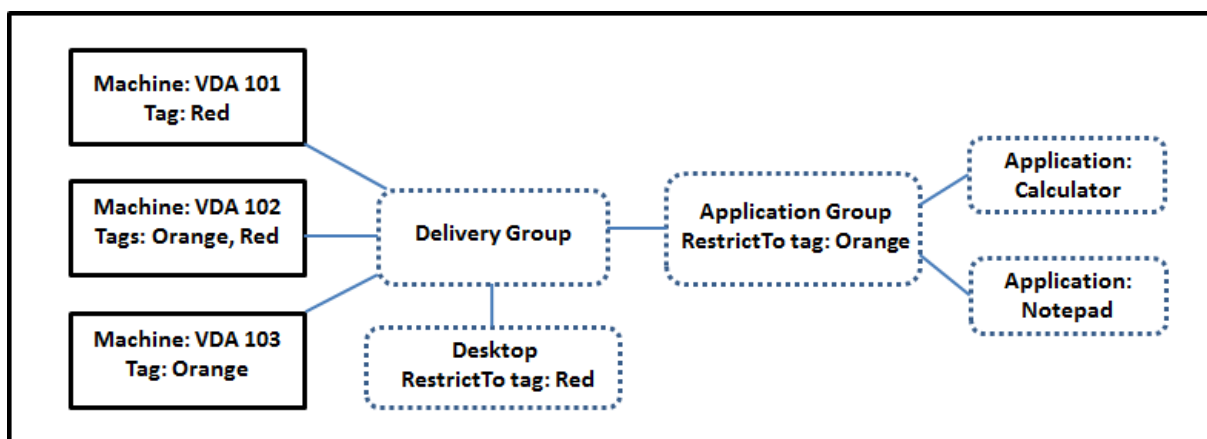
在此配置中，应用程序被添加到应用程序组中，而非添加到交付组中。交付组指定将使用的计算机。（虽然未显示，但计算机位于计算机目录中。）

应用程序组 1 与交付组 1 相关联。应用程序组 1 中的应用程序可以由在应用程序组 1 中指定的用户访问，只要这些应用程序同时位于交付组 1 的用户列表中。遵从的指导原则为：应用程序组的用户列表应属于相关联的交付组的用户列表的一部分（限制）。应用程序组 1 中的设置（例如，在应用程序组之间共享应用程序会话、相关联的交付组）适用于该组中的应用程序和用户。交付组 1 中的设置（例如，匿名用户支持）适用于应用程序组 1 和 2 中的用户，因为这些应用程序组已与该交付组相关联。

应用程序组 2 与两个交付组 1 和 2 相关联。可以在应用程序组 2 中为其中的每个交付组分配一个优先级，用于指示启动应用程序时交付组的检查顺序。优先级相同的交付组已实现负载均衡。应用程序组 2 中的应用程序可以由在应用程序组 2 中指定的用户访问，只要这些应用程序同时位于交付组 1 和交付组 2 的用户列表中。

## 示例 2

此简单布局使用标记限制来限制哪些计算机将被考虑用于启动特定的桌面和应用程序。该站点有一个共享交付组、一个发布的桌面以及一个配置了两个应用程序的应用程序组。



已为所有三台计算机 (VDA 101-103) 添加了标记。

应用程序组创建时使用了“Orange”标记限制，因此它的所有应用程序（Calculator 和 Notepad）只能在该交付组中具有标记“Orange”的计算机（VDA 102 和 103）上启动。

有关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。这需要：

1. 升级交付组中使用的计算机上的 VDA。
2. 将包含这些计算机的计算机目录更改为更高的功能级别
3. 将交付组更改为更高的职能级别。

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](#)。

本文引用将一个应用程序与多个应用程序组相“关联”来区分该操作与从可用源中添加该应用程序的一个新实例。同样，多个交付组与多个应用程序组相关联（反之亦然），而非相互添加或作为对方的组件。

## 与应用程序组共享会话

启用了应用程序会话共享时，所有应用程序在同一应用程序会话中启动。这可节省与启动其他应用程序会话关联的成本，并允许使用涉及剪贴板的应用程序功能（例如复制粘贴操作）。但是，在某些情况下，您可能希望关闭会话共享。

使用应用程序组时，可以按以下三种方式配置应用程序会话共享，这些方式扩展了仅使用交付组时可用的标准会话共享行为：

- 在应用程序组之间已启用会话共享。
- 仅在同一应用程序组中的应用程序之间启用会话共享。
- 已禁用会话共享。

#### 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。如果用户运行 Word 的现有会话适合运行记事本，则记事本将在现有会话中启动。如果无法从现有会话运行记事本（例如，如果标记限制将运行会话的计算机排除在外），则在合适的计算机上创建一个新会话，而不是使用会话共享。

- 在应用程序组之间禁用会话共享非常有用时的示例如下：

您有一组与同一计算机上安装的其他应用程序之间的互操作不顺畅的应用程序，例如，同一软件套件的两个不同的版本，或者同一 Web 浏览器的两个不同的版本。您不希望某个用户在同一会话中同时启动两个版本。

您为软件套件的每个版本分别创建一个应用程序组，并将软件套件的每个版本对应的应用程序添加到相应的应用程序组中。如果为其中每个应用程序组禁用了在组之间共享会话的功能，在这些组中指定的用户将能够在同一会话中运行同一版本的应用程序，并且同时仍然能够运行其他应用程序，只是不在同一会话中。如果该用户启动了版本不同的应用程序的其中一个版本（位于不同的应用程序组中），或者启动了未包含在应用程序组中的任何应用程序，该应用程序将在新会话中启动。

在应用程序组之间共享会话的功能不属于安全沙盒功能。此功能非常复杂，并且无法阻止用户通过其他方式在其会话中启动应用程序（例如，通过 Windows 资源管理器）。

如果计算机已满载，则不会在其中启动新会话。将会根据需要使会话共享在计算机上的现有会话中启动新应用程序（前提是这符合此处所述的会话共享限制）。

只能使预启动的会话可用于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](#)。

#### 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。如果在该应用程序组中的应用程序之间禁止会话共享，则当在其中指定的某个用户在另一个用户启动了一个应用程序之后启动它，则它们在单独的会话中启动，用户可以将各应用程序移到单独的显示器。

默认情况下，创建应用程序组时，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

使用创建应用程序组的过程在 Citrix Workspace 应用程序中创建应用程序类别。应用程序类别允许在 Citrix Workspace 中管理应用程序集合。

要创建应用程序组，请执行以下操作：

1. 在管理 > 完整配置中，选择左窗格中的应用程序，然后选择应用程序组选项卡。
2. 要使用文件夹组织应用程序组，请在应用程序组根文件夹下创建文件夹。
3. 选择要在其中创建组的文件夹，然后单击“创建应用程序组”。组创建向导启动，并显示简介页面。您可以从将来启动此向导时删除该页面。
4. 按照向导在下述页面上配置设置。完成每个页面之后，请选择下一步，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）服务器或桌面操作系统计算机。
- 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。

所选交付组指定将用于交付应用程序的计算机。请选中要与应用程序组关联的交付组旁边的复选框。



要添加标记限制，请选择限制启动带标记的计算机，然后从下拉框中选择标记。

## 步骤 2. 用户

指定哪些人能够使用应用程序组中的应用程序。可以允许您在上一页面中选择的交付组中的所有用户和用户组使用，也可以从这些交付组中选择特定用户和用户组。如果限制为由指定的用户使用，则只有在交付组和应用程序组中指定的用户能够访问此应用程序组中的应用程序。实际上，应用程序组中的用户列表提供了一个与交付组中的用户列表有关的过滤器。

允许或禁止未经身份验证的用户使用应用程序功能仅在交付组中可用，在应用程序组中不可用。

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将放置在名为 **Applications** 的文件夹中。可以指定其他文件夹。如果您尝试添加某个应用程序，但同一文件夹中已存在同名应用程序，则系统将提示您重命名要添加的应用程序。如果您同意使用建议的唯一名称，则会使用该新名称添加应用程序。否则，您必须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“完整配置”管理界面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。

选择添加下拉菜单以显示应用程序源。

- 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，然后选择确定。

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，选择确定。
- 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，然后选择确定。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，然后选择确定。有关更多信息，请参阅[部署和交付 App-V 应用程序](#)。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）。

注意：

在 VDA 2003 及更高版本中，不支持从 HTTP URL 发布 App-V 包。您不能从列表中选择这些应用程序。

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. 总结

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 30, 2023

### 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。同样，如果

已将该应用程序显式添加到与应用程序组关联的交付组（添加到应用程序组除外），禁用应用程序组不会影响这些交付组中的应用程序。

应用程序组在创建时即会启用。创建组时不能更改此设置。

1. 在管理 > 完整配置中，选择左窗格中的应用程序，然后选择应用程序组选项卡。
2. 选择应用程序组，然后在操作栏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. 选择应用以应用您所做的任何更改并使窗口保持打开，或者选择确定应用更改并关闭窗口。

### 在应用程序组之间启用或禁用应用程序会话共享

创建应用程序组时，在应用程序组之间启用会话共享。创建组时不能更改此设置。有关详细信息，请参阅[在应用程序组之间共享会话](#)。

1. 在管理 > 完整配置中，选择左窗格中的应用程序，然后选择应用程序组选项卡。
2. 选择应用程序组，然后在操作栏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. 选择应用以应用您所做的任何更改并使窗口保持打开，或者选择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。在某些情况下需要执行此操作。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，如果您启动记事本，此时有一个运行记事本的已断开连接的会话，则将重新连接该会话，而不是创建新会话。如果有多个已断开连接的合适会话，则以随机但确定性的方式选择其中一个会话进行重新连接。如果在相同情况下再次出现这种情形，则选择同一会话，但在其他情况下，会话不一定可预测。

可以使用 PowerShell SDK 对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，或者创建禁用了应用程序会话共享的应用程序组。

### PowerShell cmdlet 示例

要禁用会话共享，请使用 Broker PowerShell cmdlet `New-BrokerApplicationGroup` 或 `Set-BrokerApplicationGroup`，并将参数 `-SessionSharingEnabled` 设置为 `False`，以及将参数 `-SingleAppPerSession` 设置为 `True`。

- 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
```

#### 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，一个组的选项设置为 `True`，另一个组的选项设置为 `False`，这将导致发生不可预测的行为。

#### 重命名应用程序组

1. 在管理 > 完整配置中，选择左窗格中的应用程序，然后选择应用程序组选项卡。
2. 选择应用程序组，然后在操作栏中选择重命名应用程序组。
3. 指定新的唯一名称，然后选择确定。

#### 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. 在管理 > 完整配置中，选择左窗格中的应用程序，然后选择应用程序组选项卡。
2. 选择应用程序组，然后在操作栏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，请选择添加。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，选择确定。
5. 要删除交付组，请选中要删除的组的复选框，然后选择删除。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，然后选择编辑优先级。输入优先级（0 = 最高），然后选择确定。
7. 选择应用以应用您所做的任何更改并使窗口保持打开，或者选择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考虑用于启动应用程序的计算机有意外影响。请查看[标记](#)中的注意事项和警告。

1. 在管理 > 完整配置中，选择左窗格中的应用程序，然后选择应用程序组选项卡。
2. 选择应用程序组，然后在操作栏中选择编辑应用程序组。
3. 选择交付组页面。
4. 要添加标记限制，请选择限制启动带标记的计算机，然后从菜单中选择标记。
5. 要更改或删除标记限制，请从菜单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删除标记限制。
6. 选择应用以应用您所做的任何更改并使窗口保持打开，或者选择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. 在管理 > 完整配置中，选择左窗格中的应用程序，然后选择应用程序组选项卡。
2. 选择应用程序组，然后在操作栏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，请选择添加，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，然后选择删除。
4. 选择应用以应用您所做的任何更改并使窗口保持打开，或者选择确定应用更改并关闭窗口。

## 添加、更改或删除应用程序组中的应用程序图标

执行以下步骤以添加、更改或删除应用程序图标。

1. 在导航窗格中选择应用程序。
2. 在所有应用程序选项卡上，选择一个应用程序，然后选择属性。

要在应用程序组级别进行更改，请导航到应用程序组选项卡，选择组中的应用程序，然后选择属性。
3. 选择交付页面，然后选择更改。此时将显示选择图标窗口。
4. 在选择图标窗口中，执行以下任一操作：
  - 要添加图标，请选择添加，然后浏览至该图标。
  - 要删除图标，请选择该图标，然后选择删除。
  - 要更改图标，请为应用程序选择该图标。

### 重要：

- 不能添加大小大于 200 KB 的图标。
- 只能添加 .icon 文件。
- 不能删除内置图标。

- 不能删除正在使用的应用程序的图标。

5. 选择确定应用所做的更改并关闭窗口。

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. 在管理 > 完整配置中，选择左窗格中的应用程序，然后选择应用程序组选项卡。
2. 在中间窗格中选择一个应用程序组，然后在操作栏中选择编辑应用程序组。
3. 选择作用域页面。选中或取消选中要更改的作用域旁边的复选框。
4. 选择应用以应用您所做的任何更改并使窗口保持打开，或者选择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，则会导致一个或多个应用程序不再属于某个组，并且系统会向您发出警告，指出删除该组还将删除这些应用程序。然后您可以确认或取消删除。

删除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. 在管理 > 完整配置中，选择左窗格中的应用程序，然后选择应用程序组选项卡。
2. 选择应用程序组，然后在操作栏中选择删除组。
3. 出现提示后，确认删除。

使用文件夹组织应用程序组

您可以创建文件夹来组织应用程序组以便于访问。

必需的角色

默认情况下，必须具有以下内置角色之一才能为应用程序组创建和管理文件夹：

- 云管理员
- 完全权限管理员
- 应用程序组管理员

您可以通过创建自定义角色将管理操作委托给其他用户。下表列出了每个操作所需的权限。

操作	必需的权限
创建应用程序组文件夹	创建应用程序组文件夹

操作	必需的权限
删除应用程序组文件夹	删除应用程序组文件夹
移动应用程序组文件夹	移动应用程序组文件夹
重命名应用程序组文件夹	编辑应用程序组文件夹
将应用程序组移至文件夹	编辑应用程序组文件夹，编辑应用程序组属性

有关详细信息，请参阅[创建和管理角色](#)。

创建和管理文件夹

您可以使用操作栏或右键单击菜单来创建和管理应用程序组文件夹。此外，您可以将应用程序组或文件夹拖到文件夹树中的所需位置。

须知：

- 最多可以嵌套五层文件夹（不包括默认根文件夹）。
- 一个文件夹可以包含应用程序组和子文件夹。只有当文件夹及其子文件夹不包含应用程序组时，才能删除该文件夹。
- 完整配置中的所有资源（例如计算机目录、交付组、应用程序和应用程序组）在后端共享一个文件夹树。为避免在重命名或移动文件夹时与其他资源文件夹发生名称冲突，我们建议您为不同文件夹树中的第一级文件夹指定不同的名称。

Remote PC Access

September 1, 2023

注意：

本文介绍了如何使用“完整配置”界面配置 Remote PC Access。如果您使用的是“快速部署”界面，请按照“快速部署”中的 Remote PC Access 中的指导进行操作。

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。
- 能够使用 CSV 文件添加计算机。此功能有助于在有 OU 结构限制的情况下批量添加 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。默认情况下，Citrix DaaS 会自动将多个用户分配给下一台未分配的计算机。要限制对单个用户的自动分配，请导航到完整配置 > 设置，然后关闭“启用自动分配多个用户以实现 **Remote PC Access** 功能”设置。

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 DaaS 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 DaaS 和 Workspace Premium Plus 有效。

## 注意事项

虽然适用于 Citrix Virtual Apps and Desktops 和 Citrix DaaS 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
  - 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 和 Citrix DaaS 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。下面两个选项可用：
  - 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 计算机目录
  - Windows/Linux 专用 PC
  - Windows/Linux 专用的多用户 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。
  - 共用的 Windows/Linux PC。此用例适用于多个随机用户能够访问的物理 PC，例如计算机实验室。

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。
- 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。
- 可以选择 OU 以将计算机批量添加到计算机目录中。在某些情况下，由于 OU 结构限制，这样做并不容易。相反，您可以使用 CSV 文件批量添加计算机。通过该功能，您可以更加灵活地批量添加计算机。只能添加计算机（用于用户自动分配）或将计算机与用户分配一起添加。
- 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：

- [Remote PC Access VDA](#) 的物理显示器空白功能可用，但并非适用于所有 Linux 发行版。对于不受支持的 Linux 发行版，只能在非 3D 模式下在物理机上使用 Linux VDA。否则，由于 NVIDIA 驱动程序的限制，启用 HDX 3D 模式时，电脑的本地屏幕无法变黑并显示会话的活动。显示此屏幕存在安全风险。
- 对于物理 Linux 计算机，我们建议您使用单会话操作系统类型的计算机目录。

## 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。
  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。

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 /physicalmachine` 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 Citrix 下载站点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。

## 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时，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+ALT+DEL），远程用户的会话自动断开连接。要阻止此自动操作，请在办公 PC 上添加以下注册表项，然后重新启动计算机。

### 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：

#### HKKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC

- 名称：RpccaMode
- 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：RpccaTimeout
- 类型：DWORD
- 数据：十进制值格式的超时秒数

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报 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附加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。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。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 DaaS
- Citrix Virtual Apps and Desktops 2009 或更高版本
- 物理 PC：
  - 2009 或更高版本
  - Windows 10 或 Windows 11。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

要配置局域网唤醒，可以使用“完整配置”管理界面或 PowerShell。

在“完整配置”界面中配置局域网唤醒 要创建局域网唤醒连接，请执行以下操作：

1. 导航到左侧的托管节点。
2. 选择添加连接和资源。
3. 在向导的连接页面中，提供以下内容：
  - a) 连接类型：Remote PC 局域网唤醒
  - b) 区域名称：选择 Remote PC Access 目录所在的区域
  - c) 连接名称：输入局域网唤醒连接的名称。
4. 完成“添加连接和资源”向导中的剩余步骤。

要将局域网唤醒连接添加到 Remote PC Access 计算机目录中，请执行以下操作：

1. 如果要创建新的 Remote PC Access 计算机目录，则可以使用下拉列表在“计算机目录设置”向导的“计算机类型”页面上添加连接。
2. 如果要将局域网唤醒连接添加到现有计算机目录，请执行以下操作：
  - a) 导航到左侧的计算机目录节点。
  - b) 选择相应的 Remote PC Access 计算机目录。
  - c) 右键单击计算机目录或选择上方的更多菜单。
  - d) 选择编辑计算机目录。
  - e) 在电源管理页面中，选择是。
  - f) 从下拉列表中选择相应的连接。
  - g) 选择保存。

### 注意：

当前，只有 Citrix DaaS 才能通过“完整配置”界面配置局域网唤醒。

通过 **PowerShell** 配置局域网唤醒 要通过 PowerShell 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。
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：

```
1 # Load Citrix SnapIns
2 Add-PSSnapIn -Name "\\*citrix\*"
3
4 # Provide the name of the Wake on LAN host connection
5 [string]$connectionName = "Remote PC Access Wake on LAN"
6
7 # Create the hypervisor connection
8 $hypHc = New-Item -Path xdhyp:\Connections `
9             -Name $connectionName `
10            -HypervisorAddress "N/A" `
11            -UserName "woluser" `
12            -Password "wolpwd" `
13            -ConnectionType Custom `
14            -PluginId VdaWOLMachineManagerFactory `
15            -CustomProperties "<CustomProperties></CustomProperties>" `
16            -Persist
17
18 $bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
19 $hypHc.HypervisorConnectionUid
20
21 # Wait for the connection to be ready before trying to use it
22 while (-not $bhc.IsReady)
23 {
24     Start-Sleep -s 5
25     $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
26         $hypHc.HypervisorConnectionUid
27 }
28 <!--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：

```
1 $bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
2 $hypUid = $bhc.Uid
3 <!--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：

```
1 Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
2   RemotePCHypervisorConnectionUid $hypUid
3 <!--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。
- 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“完整配置”界面或 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，“完整配置”界面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。

## 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

#### 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](#)。

## 删除组件

September 1, 2023

要删除您安装的组件（例如 VDA），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脚本来删除组件。

删除组件时，不会删除必备项，也不会更改防火墙设置。

删除 VDA 时，默认情况下，计算机将在删除后自动重新启动。

### 使用专门用于删除或更改程序的 **Windows** 功能删除组件

使用专门用于删除或更改程序的 Windows 功能：

- 要删除 VDA，请选择 **Citrix Virtual Delivery Agent** < 版本 >，然后单击鼠标右键并选择卸载。此时将启动安装程序，从中可选择要删除的组件。
- 要删除通用打印服务器，请选择 **Citrix** 通用打印服务器，然后单击鼠标右键并选择卸载。

### 使用命令行删除 **VDA**

运行用于安装 VDA 的命令：[VDAServerSetup.exe](#)、[VDAWorkstationSetup.exe](#) 或 [VDAWorkstationCoreSetup.exe](#)。有关语法说明，请参阅[使用命令行安装](#)。

- 要仅删除 VDA 或仅删除 Citrix Workspace 应用程序，请使用 [/remove](#) 和 [/components](#) 选项。
- 要删除 VDA 和 Citrix Workspace 应用程序，请使用 [/removeall](#) 选项。

例如，以下命令将从多会话操作系统计算机中删除 VDA 和 Citrix Workspace 应用程序。

```
VDAServerSetup.exe /removeall
```

例如，以下命令将从单会话操作系统计算机中删除 VDA，但不删除适用于 Windows 的 Citrix Workspace 应用程序（如果已安装）。

```
VDAWorkstationSetup.exe /remove /components vda
```

还可以使用 Citrix 提供的脚本删除 VDA。请参阅[使用脚本删除 VDA](#)。

## 用户个性化层

February 9, 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。

### 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。

重要提示：

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
- Virtual Delivery Agent (VDA)，版本 1912 或更高版本
- 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 11 Enterprise x64
- 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：

如果您使用的是服务器操作系统，则仅支持服务器 VDI。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。

## 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。

注意：

在映像上升级 Windows 10 后首次登录所花费的时间比平时长。用户的层需要针对新版本的 Windows 10 进行更新，从而延长登录时间。

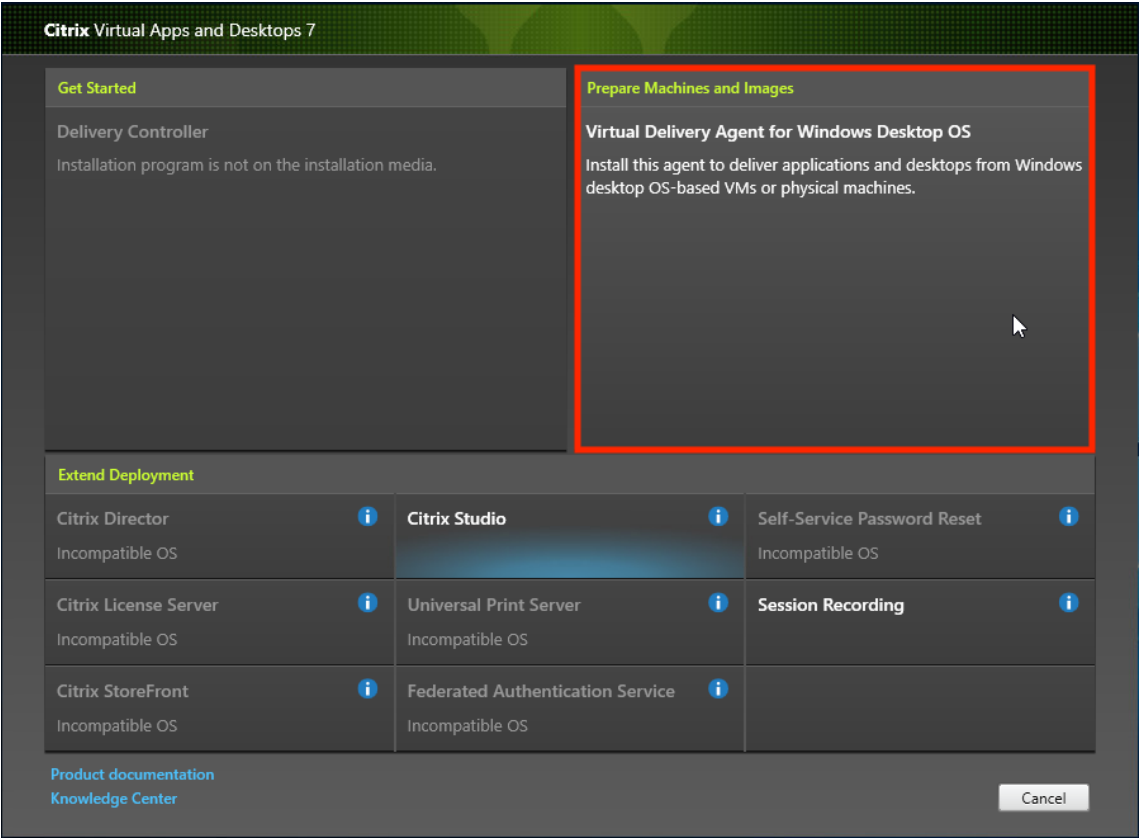
**步骤 1: 验证 Citrix Virtual Apps and Desktops 环境是否可用**

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](#)。

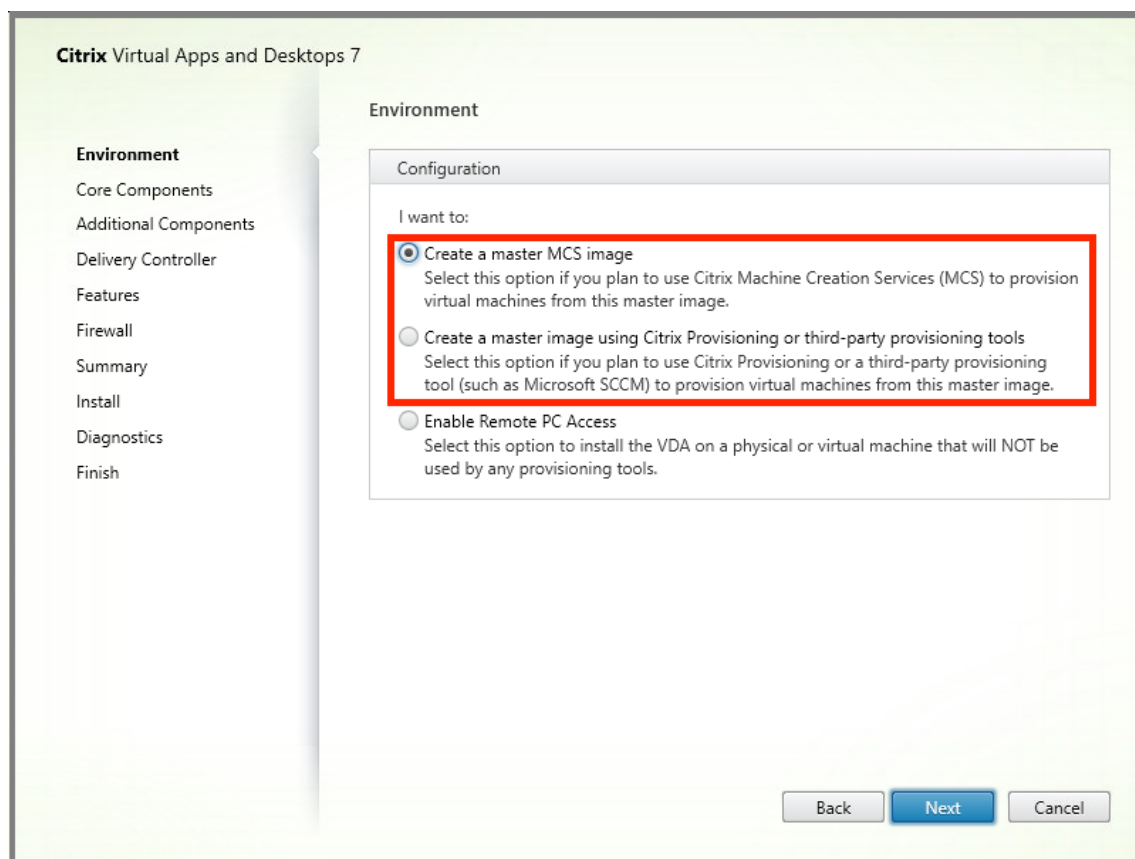
**步骤 2: 准备您的主映像**

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 或更高版本。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**：



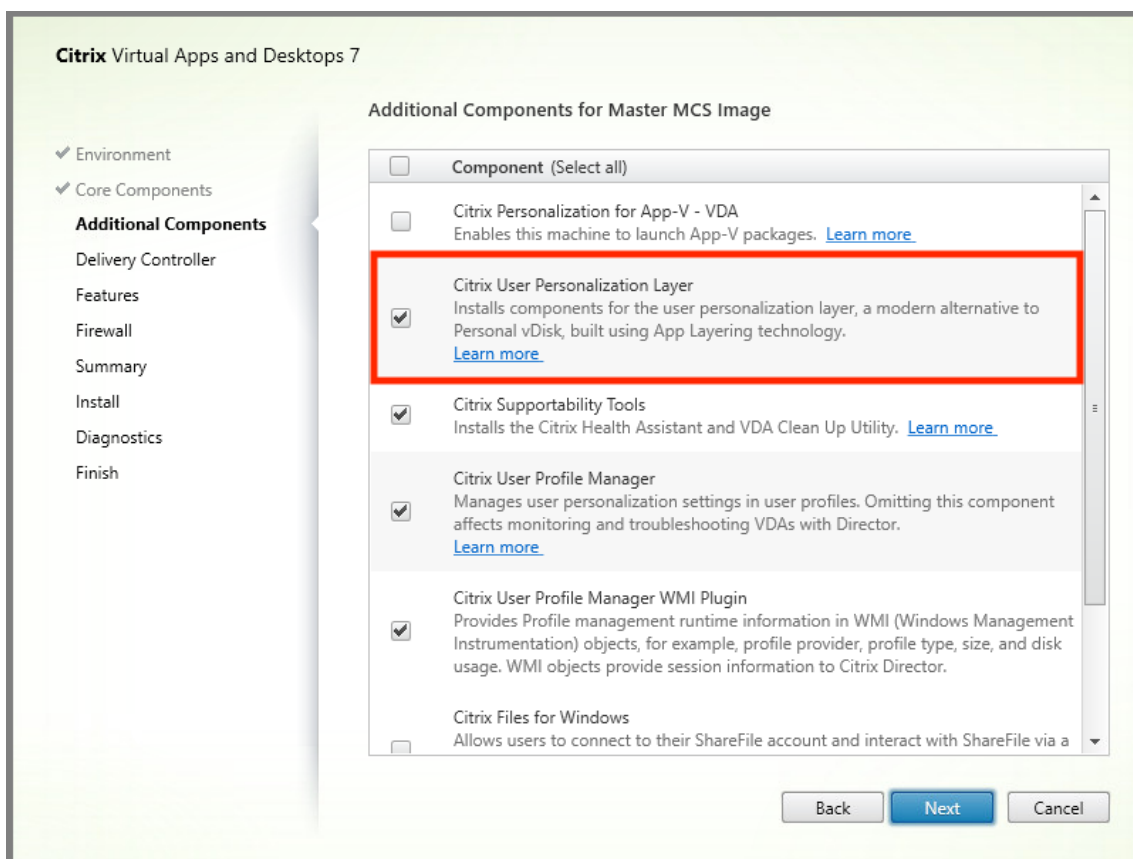
a) 环境：选择创建主 **MCS** 映像或使用 **Citrix Provisioning** 或第三方预配工具创建主映像。



a) 核心组件：单击下一步。

b) 其他组件：选中 **Citrix User Personalization Layer**。





- 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。

注意：

如果您只想升级用户个性化层 (UPL)，则可以使用更新版本的 UPL 和独立软件包进行升级。您无需升级 VDA。

### 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，如下示例中所示：
  - 池随机：

Machine Catalog Setup

✓ Introduction

✓ Machine Type

✓ Machine Management

4 Desktop Experience

5 Master Image

6 Storage

7 Virtual Machines

8 Disk Settings

9 Machine Identities

10 Domain Credentials

11 Scopes

12 WEM (Optional)

13 Summary

Desktop Experience

Which desktop experience do you want users to have?

☒ I want users to connect to a new (random) desktop each time they log on.

☐ I want users to connect to the same (static) desktop each time they log on.

Do you want to save any changes that the user makes to the desktop?

☒ Yes, create a dedicated virtual machine and save changes on the local disk.

☐ No, discard all changes and clear virtual desktops when the user logs off.

Back

Next

Cancel

- 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：

Machine Catalog Setup

✓ Introduction

✓ Machine Type

✓ Machine Management

4 Desktop Experience

5 Master Image

6 Storage

7 Virtual Machines

8 Disk Settings

9 Machine Identities

10 Domain Credentials

11 Scopes

12 WEM (Optional)

13 Summary

Desktop Experience

Which desktop experience do you want users to have?

☐ I want users to connect to a new (random) desktop each time they log on.

☒ I want users to connect to the same (static) desktop each time they log on.

Do you want to save any changes that the user makes to the desktop?

☐ Yes, create a dedicated virtual machine and save changes on the local disk.

☒ No, discard all changes and clear virtual desktops when the user logs off.

Back

Next

Cancel

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. 如果您使用的是 MCS，请选择映像和上一节中创建的映像的快照。
- 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：

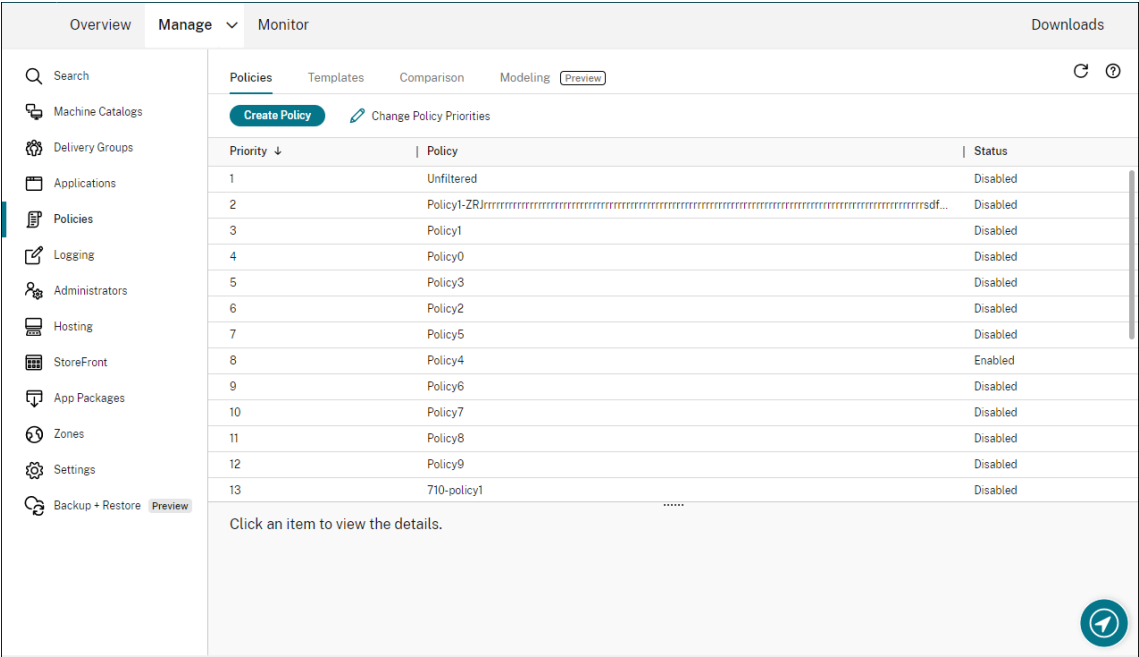
- 在网络上访问用户层的位置。
- 允许用户层磁盘增长的大小。

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

740

在 Web Studio 中将参数定义为自定义 Citrix 策略并将其分配给交付组。

1. 登录 Web Studio 并在左侧窗格中选择策略：



2. 在操作栏中选择创建策略。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三个策略：

- 用户层排除
- 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. 选中用户层存储库路径旁边的复选框，然后单击编辑。此时将显示编辑设置窗口。

5. 在值字段中输入路径，然后单击保存：

- 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`

Edit Setting

**User Layer Repository Path**

Value:

☐ Use default value:

▼ Applies to the following VDA versions  
Virtual Delivery Agent: 2008 Desktop OS, 2008 Desktop OS

▼ Description  
The SMB directory path where user layer VHDs are located. Format: '\\server\share\path'

OK Cancel

可以使用 %USERNAME% 和 %USERDOMAIN% 变量、计算机环境变量和 Active Directory (AD) 属性自定义路径。展开时，这些变量会生成显式路径。

环境变量示例：

- 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`

Edit Setting

**User Layer Repository Path**

Value:

☐ Use default value:

▼ Applies to the following VDA versions  
Virtual Delivery Agent: 2008 Desktop OS, 2008 Desktop OS

▼ Description  
The SMB directory path where user layer VHDs are located. Format: '\\server\share\path'

OK Cancel

自定义 AD 属性的示例：

- 路径格式：\\Server-name-or-address\share-name\AD-attribute
- 路径示例：\\Server\share\#sAMAccountName#
- 生成的路径示例：\\Server\share\JohnSmith（如果 #sAMAccountName# 解析为当前用户 JohnSmith）

6. 可选：选中用户层大小 **(GB)** 旁边的复选框，然后单击编辑：

Create Policy

1 Select Settings

2 Assign Policy To

3 Summary

Select Settings

(All Versions)All Settingsuser layer

Settings 0 selectedView selected only

> User Layer Repository Path  
Computer setting - User Personalization Layer  
Not Configured (Default: \\server\share\path)Select

> User Layer Size in GB  
Computer setting - User Personalization Layer  
Not Configured (Default: 10)Select

Next

Cancel

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。单击保存。

8. 可选：选中用户层排除旁边的复选框，然后单击编辑。

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

744

Edit Setting

User Layer Exclusions

Value:

☒ Use default value:

Description

Excludes a list of files and directories so that they don't persist in the user layer.

Directories are excluded if there is a \ at the end of the path.  
Example: C:\Program Files\AntiVirusHome\.

Files are excluded if there is no \ at the end of the path.  
Example: C:\ProgramData\AntiVirus\virusdefs.db.

There is no limit to the number of exclusion rules that you can add. You can also use a \* as a wildcard in a path. For example, C:\Users\\*\AppData\Local\Temp excludes the Temp directory for all users. There is only one \* allowed in the rule, and that \* only matches one level of directories.

Applies to the following VDA versions

Desktop OS: 2303, 2305

9. 可选：指定要排除的文件和文件夹，然后单击保存。有关详细信息，请参阅 [Citrix App Layering 文档](#)。
10. 单击下一步配置要分配的用户和计算机。单击此图像中突出显示的交付组分配链接：



Create Policy

✓ Select Settings

2 Assign Policy To

3 Summary

Assign Policy To

Selected user and machine objects

All objects in the site

User and machine objects: 0 selected

View selected only

> Delivery Group

Applies to all settings

Assign

> Delivery Group type

Applies to all settings

Assign

> Organizational Unit (OU)

Applies to all settings

Assign

> Tag

Applies to all settings

Assign

Back

Next

Cancel

11. 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。

Assign Policy

Delivery Group

Apply policy based on the delivery group membership of the desktop running the session.

Delivery Group elements:

Mode

Delivery group

Allow

+

Enable

12. 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.

746

Create Policy

Select Settings

Assign Policy To

3

Summary

Summary

Enable policy

View a summary of the settings you configured and provide a name for your new policy.

Policy name:

Example: East Coast Policy 1

Description:

Settings configured: 1

Assigned to: 1 user and machine objects

User Layer Size in GB

Computer setting - User Personalization Layer

10 (Default: 10)

> Delivery Group

Applies to all settings

Back

Finish

Cancel

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

## 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。

```
1 C:\ProgramData\Unidesk\Logs\ulayersvc.log  
2 <!--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。

- 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：

```
gpupdate /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”。

- 域用户帐户不得是最后一个登录到主映像的用户。否则，基于该映像预配的计算机将出现问题。
- 在纯 Azure AD 环境中启用了 UPL 时，由于在 Azure 上运行的 Windows 中存在潜在问题，自定义证书不会持续存在。如果 Microsoft 在将来的增强版本中修复了此问题，我们将更新本文。

## 升级 VDAs

September 1, 2023

### 简介

Citrix 负责维护您的部署中除 VDA 以外的所有 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）组件。

开始升级 VDA 之前：

- 查看整篇文章，以便了解所需的对象。
- 查看 Citrix DaaS 的[生命周期策略](#)。

要升级 VDA，请下载 VDA 安装程序并在计算机或映像上运行该安装程序。可以使用安装程序的图形界面或命令行界面。有关指导，请参阅：

- [VDA 安装程序](#)
- [使用图形界面安装 VDA](#)
- [使用命令行安装 VDA](#)

如果 VDA 最初是使用 `VDAWorkstationCoreSetup.exe` 安装的：

- 如果使用同一安装程序的最新版本升级 VDA，则保留该配置。
- 如果您在该计算机上运行 `VDAWorkstationSetup.exe`，则可以启用 `VDAWorkstationCoreSetup.exe` 中不支持的功能。请记住，其中某些功能可能会在 `VDAWorkstationSetup.exe` 安装程序中默认启用。还可以安装 Citrix Workspace 应用程序。

**注意：**

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计算机。本次重新启动是不可避免的。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`）。

升级 VDA 后，请[更新使用该 VDA 的映像和目录](#)。

## 使用完整配置界面升级 VDA

**重要：**

- 作为最佳实践，我们建议您在投入生产之前全面测试 VDA 升级。
- 只要从早期版本切换到更高版本，就可以在 CR VDA 和 LTSR VDA 之间切换。您无法从更高版本切换到较早的版本，因为这被视为降级。例如，您无法从 2212 CR 降级到 2203 LTSR（任何 CU），但可以从 2112 CR 升级到 2203 LTSR（任何 CU）。
- 不支持按需更新（例如主要版本之间的修补程序和补丁）。

使用完整配置界面，您可以按目录或每台计算机升级 VDA。您可以立即或在预定时间升级它们。

要了解有关 VDA 升级服务的更多信息，请参阅 [技术简介：Citrix VDA Upgrade 服务](#)。在这里，您将找到该服务的概述、有关其工作原理的详细信息以及其他有用的资源。

### 必备条件

- 控制平面：Citrix DaaS
- VDA 类型：单会话或多会话操作系统 VDA
- VDA 版本：2109 或更高版本，或 2203 LTSR 或更高版本

注意：

我们建议使用最新的 CR VDA 或最新的 LTSR CU VDA。

- 预配类型：永久性计算机（例如 MCS 预配的计算机、Remote PC Access 计算机、适用于 Windows 365 的 [Citrix HDX Plus](#)）。请参阅[支持的计算机类型](#)。
- VDA 必须安装了 [VDA 升级代理](#)并且服务必须正在运行。
- 您有权升级 VDA。
- VDA 升级使用完整配置中正确的 CR 或 LTSR 轨道进行配置。
- VDA 未在使用中。（用户必须从他们那里注销。）

注意：

任何正在使用或处于断开状态的 VDA 都将跳过升级。我们建议安排一个升级窗口并要求用户注销 vDA。

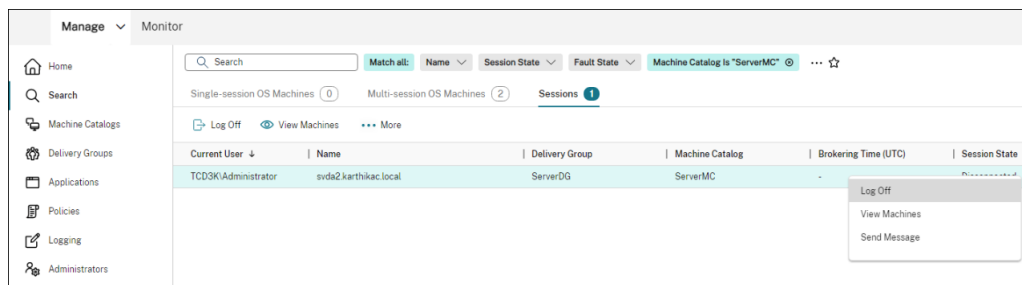
- VDA 未处于维护模式。（管理员可以将 VDA 置于维护模式。如果 VDA 已超过允许的最大注册尝试次数，也可以自动将其置于维护模式。）
- 如果 URL 过滤已到位，相关的 URL 已添加到允许列表中。请参阅 [VDA 升级要求](#)。
- VDA 必须属于交付组并在 DaaS 中注册。
- 功能级别设置正确，因此 VDA 升级功能可供使用。查看 [VDA 版本和功能级别](#)。
- 目标 VDA 支持当前 VDA 的操作系统。

## 已知问题

**问题 1：**无法将 **LTSR vDA** 升级到 **LTSR 累积更新 (CU)** 版本 尝试将 LTSR VDA 升级到 LTSR 累积更新 (CU) 版本可能会失败。尽管在“完整配置”中升级过程似乎已成功完成，但安装的 VDA 版本并未更改，状态在一两分钟后变回升级可用。安装了 VDA Upgrade Agent 版本 7.35.0.7 或更早版本的 VDA 会出现问题。

要解决此问题，请登录 VDA 并将 VDA 升级代理升级到 7.37.0.7 或更高版本（使用 VDA 安装程序版本 2303 或更高版本）。自版本 7.37.0.7 起，VDA 升级代理支持自动升级，因此在 VDA 上运行的早期版本的代理可以自动升级到最新版本。借助此自动更新功能，VDA 升级服务会检查代理报告的 VDA 版本，然后在一小时内安排升级，以自动将代理升级到最新版本。此自动升级功能减少了您的维护工作量。

要使 VDA 上的代理自动升级，请务必注销会话，以便 VDA 升级服务可以启动自动升级。您可以在“完整配置”中注销会话。



如果代理无法自动升级，请登录 VDA 并按如下所示手动升级代理：

1. 运行以下 cmdlet 以在“控制面板” > “卸载或更改程序”中显示 VDA 升级代理。

```
1 (Get-ChildItem -Path 'HKLM:\SOFTWARE\Microsoft\Windows\
   CurrentVersion\Uninstall' | ? {
2   $_.GetValue('DisplayName') -eq 'Citrix VDA Upgrade Agent
   Service - x64' }
3 ).GetValue('SystemComponent')
4 (Get-ChildItem -Path 'HKLM:\SOFTWARE\Microsoft\Windows\
   CurrentVersion\Uninstall' | ? {
5   $_.GetValue('DisplayName') -eq 'Citrix VDA Upgrade Agent
   Service - x64' }
6 ) | Set-ItemProperty -Name SystemComponent -Value 0
7 <!--NeedCopy-->
```

2. 安装最新的 VDA 升级代理。要执行无提示安装，请使用以下 cmdlet：

- `msiexec /i CitrixUpgradeAgent_x64.msi /q`

可以使用 cmdlet 或脚本识别 VDA 升级代理的版本。请参阅[故障排除](#)。

**问题 2：不支持代理** 目前，VDA 升级代理不支持代理配置。当代理尝试通过代理服务器建立连接时，此限制可能会导致连接问题。

您可以应用变通办法来解决这个问题。请按照以下步骤操作：

1. 在以下位置找到 VDA 升级代理配置文件：`C:\Program Files\Citrix\CitrixUpgradeAgent\Citrix.UpdateServices.UpdateAgent.exe.config`。
2. 使用文本编辑器打开配置文件。
3. 在文件末尾添加以下行，`ProxyServerName` 替换为实际的代理服务器名称：

```
1 <system.net>
2 <defaultProxy enabled="true" useDefaultCredentials="true">
3   <proxy proxyaddress="http://PROXYSERVER:PORT" usesystemdefault
   ="false" />
4 </defaultProxy>
5 </system.net>
6 </configuration>
7 <!--NeedCopy-->
```

4. 重新启动 Citrix VDA Upgrade Agent Service 以应用更新的配置。

## 常规工作流程

使用完整配置界面升级 VDA 的常规工作流程如下所示：

1. 为目录启用 VDA 升级。

- 您可以在[创建目录](#)时启用 VDA 升级。
- [编辑目录](#)时可以启用 VDA 升级。

2. 在每个目录或每台计算机的基础上升级 VDA。有关更多信息，请参阅[为 VDA 配置自动升级](#)。

### 注意：

在为目录安排 VDA 升级时，请注意，该目录中的所有计算机都将包含在升级范围内。因此，我们建议在启动升级之前备份这些计算机。

## 故障排除

如果出现升级失败，您可以使用以下日志自行解决问题，也可以在联系 Citrix 技术支持寻求帮助时提供日志。

- `%temp%/Citrix/XenDesktop Installer` 下的 VDA 初始安装的安装日志
- `C:\Windows\Temp\Citrix\XenDesktop Installer` 下的升级日志

要检查 VDA 升级代理版本，请使用以下 cmdlet: `Get-VusComponentVersion -ComponentType VUS`。它列出了所有 VDA 及其 VDA 升级代理版本。

要获取 VDA 名称，请使用以下 cmdlet: `Get-BrokerMachine -UUID "<version number>"`，其中 `<version number>` 是您从 `Get-VusComponentVersion` cmdlet 获得的 VDA 升级代理版本。

要在目录级别检查 VDA 升级代理版本，可以使用以下脚本：

### 注意：

该脚本仅作为示例，可能需要进行调整以适应您的特定环境。我们建议您在生产环境中使用脚本之前对其进行全面测试。

```
1 Param(
2     [Parameter (Mandatory=$true)]
3     [string] $CatalogName
4 )
5
6 try
7 {
8
9     $Uuids = Get-BrokerMachine -CatalogName $CatalogName | Select-Object -Property UUID
```



```

10
11     if($Uuids -eq $null)
12     {
13
14         throw "Cannot find CatalogName "+$CatalogName
15     }
16
17     Write-Output("Catalog Name passed is "+$CatalogName)
18
19     foreach($Uuid in $Uuids)
20     {
21
22         $compVersion = Get-VusComponentVersion -MachineId $machine.UUID
23                     -ComponentType VUS
24         $Machine = Get-BrokerMachine -UUID $compVersion.MachineId
25         Write-Output("MachineName: "+$Machine.MachineName+", Machine
26                     UUID:"+$machine.MachineId+", VUA Version:"+$compVersion.
27                     Version)
28     }
29 }
30
31 catch
32 {
33     Write-Output("Exception Occured")
34     Write-Host $_
35 }
36 <!--NeedCopy-->

```

与 **VDA** 升级代理相关的日志 您还可以收集与 VDA 升级代理相关的日志。您可以收集的日志包括：

- **Citrix** 诊断工具 (**CDF**) 追踪。
- **Windows** 事件日志。写入 Windows 事件日志的信息。在 事件查看器 > 应用程序和服务日志 > **Citrix VDA Upgrade Agent Service** 中查看日志。

如果需要，您可以修改 VDA Upgrade Agent 配置文件，以便将日志持续写入文件中。要启用文件登录功能，请执行以下步骤：

1. 转到文件夹 `C:\Program Files\Citrix\CitrixUpgradeAgent`。
2. 打开文件 `Citrix.UpdateServices.UpdateAgent.exe.config`。
3. 将 `LogToFile` 的值更改为 1。
4. 重新启动 Citrix VDA Upgrade Agent Service。这将在以下位置创建日志文件：`C:\ProgramData\Citrix\Update Services\Logs`。

## 注意：

- 启用文件日志记录功能会持续写入日志，可能会消耗存储空间。问题解决后，记得禁用日志记录。要禁用日志记录，请先将 `LogToFile` 设置为 `0` 然后重新启动 Citrix VDA Upgrade Agent Service。
- 设置 `LogToFile=1` 后，日志仅写入文件。它们不会出现在 CDF 轨迹中。

排除 **VDA** 升级下载失败故障 按照以下步骤对与 VDA 升级功能相关的下载失败进行故障排除和解决：

1. 如果 URL 过滤已到位，请确保相关的 URL 已添加到允许列表中。请参阅 [VDA 升级要求](#)。
2. 将必要的 URL 添加到允许列表后，尝试重新安排 VDA 升级。

您可以启用 CDF 跟踪或将 `LogToFile` 设置为 `1` 以捕获详细日志进行分析。如果下载失败问题仍然存在，请检查错误。如果您看到以下错误消息“下载失败：此访问控制列表不是规范格式，因此无法修改”，则表示 `C:\ProgramData\Citrix\UpgradeServices\Downloads\VDA` 文件夹的权限不正确。要解决此问题，请执行以下任一操作：

- 选项 **1**：使用以下命令重置文件夹上的访问控制列表 (ACL)。（该命令使用所有匹配文件的默认继承 ACL 重置 ACL。）

```
- icacls.exe "C:\ProgramData\Citrix\UpgradeServices\Downloads\
VDA"/reset /T /C /L /Q
```

- 选项 **2**：删除“下载”下的 VDA 文件夹，然后安排 VDA 升级。

排除 **VDA** 升级验证失败故障 按照以下步骤对与 VDA 升级功能相关的下载失败进行故障排除和解决：

1. 如果 URL 过滤已到位，请确保已将相关 URL 添加到允许列表中，尤其是吊销检查所需的证书吊销列表 (CRL) 或在线证书状态协议 (OCSP) URL。请参阅 [VDA 升级要求](#)。
2. 将必要的 URL 添加到允许列表后，尝试重新安排 VDA 升级。

我们建议启用 CDF 跟踪或将 `LogToFile` 设置为 `1` 以捕获详细日志进行分析。日志可能包含以下错误：

- 吊销状态未知
- 吊销功能无法检查证书的吊销状态。
- 吊销功能无法检查撤销，因为吊销服务器处于脱机状态。

VDA 升级代理依赖 Windows 系统调用来验证证书和执行吊销检查。上述错误表明代理无法与 CRL 或 OCSP URL 建立连接。

请注意，VDA 升级代理目前不支持代理设置。CryptoAPI 发出的出站 CRL 和 OCSP 调用不了解代理配置，这可能会导致故障。

如果您的环境设置了代理，则可以在 VDA 上配置系统代理以方便出站 CRL 呼叫。按照以下步骤配置系统代理：

```
1 netsh winhttp import proxy source=ie
2
3 Or
4
5 netsh winhttp set proxy proxy-server=http://Proxy_Server:Port
6 <!--NeedCopy-->
```

## 使用 PowerShell 升级 VDA

可以使用远程 PowerShell SDK 配置 VDA 升级。有关远程 PowerShell SDK 的详细信息，请参阅 [Citrix DaaS Remote PowerShell SDK](#)。

下面是 PowerShell cmdlet:

- **Get-VusCatalog**

使用此 cmdlet 获取目录的详细信息，例如 `Name`、`Uid`、`Uuid`、`UpgradeState` (`Available`、`UpToDate`、`Scheduled`、`Unknown`)、`UpgradeType` (`CR/LTSR`)、`Upgrade scheduled` 和 `StateId` (`Upgrade scheduled` 的状态)。

- **Get-VusMachine**

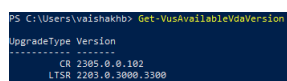
使用此 cmdlet 获取计算机的详细信息，例如 `MachineName`、`Uid`、`Uuid`、`UpgradeState` (`Available`、`UpToDate`、`Scheduled`、`Unknown`)、`UpgradeType` (`CR/LTSR`) 和 `StateId` (`Upgrade scheduled` 的状态)。

- **Get-VusComponentVersion**

使用此 cmdlet 来检查 VDA 是否已报告组件版本。使用 `MachineId` 筛选 VDA。`MachineId` 是来自 `Get-BrokerMachine` 的 UUID。

- **Get-VusAvailableVdaVersion**

使用此 cmdlet 查看通过 VDA 更新服务发布的最新 CR/LTSR 版本。



```
PS C:\Users\vaishakh> Get-VusAvailableVdaVersion
UpgradeType Version
-----
CR 2305.0.0.102
LTSR 2203.0.3000.3300
```

- **Set-VusCatalogUpgradeType**

使用此 cmdlet 将目录的升级类型设置为 CR 或 LTSR。升级类型只能在计算机目录级别设置。

- **New-VusMachineUpgrade**

使用此 cmdlet 在计算机级别配置 VDA 升级。

- **New-VusCatalogSchedule**

使用此 cmdlet 在计算机目录级别安排 VDA 升级。

计算机级别的 **cmdlet** 示例

- 设置升级类型。

示例：

```
- Set-VusCatalogUpgradeType -CatalogName test-catalog -UpgradeType  
  LTSR
```

- 使用 `Get-VusMachine` 检查目录中的计算机的 `UpgradeState`。

示例：

```
- Get-VusMachine -CatalogName test-catalog
```

```
PS C:\Users> Get-VusMachine -CatalogName test-catalog_

CatalogName      : test-catalog
DNSName           : test-machine-1
DurationInHours   :
LastStateChange   :
MachineName       : test-machine-1
MachineUid        : 35
MachineUuid       : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType  : MCS
ScheduledTime     :
SessionSupport    : SingleSession
StateId           :
StatusMessage     :
UpgradeState      : UpgradeAvailable
UpgradeType       : LTSR
UpgradeVersion    :

CatalogName      : test-catalog
DNSName           : test-machine-2
DurationInHours   :
LastStateChange   :
MachineName       : test-machine-2
MachineUid        : 36
MachineUuid       : cfa55303-6000-4973-bee8-e38c9916719e
ProvisioningType  : MCS
ScheduledTime     :
SessionSupport    : SingleSession
StateId           :
StatusMessage     :
UpgradeState      : UpgradeAvailable
UpgradeType       : LTSR
UpgradeVersion    :
```

如果您看到 `UpgradeState` 为 `Unknown`，可能的原因之一是 VDA 上安装的 Citrix VDA Upgrade Agent 尚未向 VDA 更新服务报告该版本。可以使用 `Get-VusComponentVersion` cmdlet 来检查 VDA 是否已报告组件版本。

```
- Get-VusComponentVersion -MachineId ""
```

```
PS C:\Users> Get-VusComponentVersion -MachineId d664614a-cd37-44d6-b1f0-6f6b70f8299c
```

ComponentType	MachineId	Uid	Version
VDA	d664614a-cd37-44d6-b1f0-6f6b70f8299c	7505fa4c-1811-ee11-907e-0022484becbd	2203.0.0.33220
VUS	d664614a-cd37-44d6-b1f0-6f6b70f8299c	7705fa4c-1811-ee11-907e-0022484becbd	7.37.0.7
Mps	d664614a-cd37-44d6-b1f0-6f6b70f8299c	7805fa4c-1811-ee11-907e-0022484becbd	7.33.0.26
SupportabilityTools	d664614a-cd37-44d6-b1f0-6f6b70f8299c	7a05fa4c-1811-ee11-907e-0022484becbd	1.5.0.17
Upm	d664614a-cd37-44d6-b1f0-6f6b70f8299c	7c05fa4c-1811-ee11-907e-0022484becbd	22.3.0.7
UpmVdaPlugin	d664614a-cd37-44d6-b1f0-6f6b70f8299c	7d05fa4c-1811-ee11-907e-0022484becbd	22.3.0.7

如果未显示任何结果，请验证以下内容：

- VDA 是目录和交付组的一部分。
- VDA 升级代理已安装在 VDA 上并且正在运行。如有必要，请尝试重新启动代理。

注意：如果仍然没有结果，请在重新启动 VDA Upgrade Agent 的同时收集 Citrix 诊断设施跟踪信息并解决问题。

- 安排 VDA 升级。在开始之前，请注意以下事项：
  - **DurationInHours**：允许您提供升级过程的持续时间（以小时为单位）。VDA 将进入维护模式。将下载 VDA 安装程序并执行升级。如果有许多 VDA 需要升级，则提供更长的持续时间。
  - **UpgradeNow**：使用此开关可立即安排升级或设置 **ScheduledTimeInUtc**。
  - **ScheduledTimeInUtc**：允许您在特定的日期和时间安排升级。

示例：

- `New-VusMachineUpgrade -MachineUuid d664614a-cd37-44d6-b1f0-6f6b70f8299c -ScheduledTimeInUtc ([System.DateTime]::ParseExact("06/23/2023 03:35 PM", 'MM/dd/yyyy hh:mm tt', $null))-DurationInHours 2`

您可以使用 **MachineUuid**、**MachineId** 和 **MachineName** 来安排 VDA 升级。

```
PS C:\Windows\system32> New-VusMachineUpgrade -MachineUuid d664614a-cd37-44d6-b1f0-6f6b70f8299c -ScheduledTimeInUtc ([System.DateTime]::ParseExact("06/23/2023 03:35 PM", 'MM/dd/yyyy hh:mm tt', $null)) -DurationInHours 2
DurationInHours : 2
MachineName     : test-machine-1
MachineUuid     : d664614a-cd37-44d6-b1f0-6f6b70f8299c
MachineId       : 35
ScheduledTimeInUtc : 6/23/2023 11:35:00 AM
UpgradeVersion   : 2203.0.3000.3300
```

- 检查升级状态。

示例：

- `Get-VusMachine -MachineName test-machine-1`

```
PS C:\Windows\system32> Get-VusMachine -MachineName test-machine-1
```

```
CatalogName      : test-catalog
DNSName          : test-machine-1
DurationInHours  : 2
LastStateChange  : 6/23/2023 11:47:35 AM
MachineName      : test-machine-1
MachineUid       : 35
MachineUuid      : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 11:35:00 AM
SessionSupport   : SingleSession
StateId          : UpgradeInProgress
StatusMessage    :
UpgradeState     : UpgradeScheduled
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300
```

```
PS C:\Users\vaishakhb> Get-VusMachine -MachineName test-machine-1
```

```
CatalogName      : test-catalog
DNSName          : test-machine-1
DurationInHours  : 4
LastStateChange  : 6/23/2023 12:18:21 PM
MachineName      : test-machine-1
MachineUid       : 35
MachineUuid      : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 12:00:00 PM
SessionSupport   : SingleSession
StateId          : UpgradeSuccess
StatusMessage    : Upgrade completed successfully or is already up to date
UpgradeState     : UpToDate
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300
```

#### 目录级别 cmdlet 示例

- 在计算机目录级别设置升级类型。

示例：

```
- Set-VusCatalogUpgradeType -CatalogName test-catalog -UpgradeType  
LTSR
```

- 使用 Get-VusCatalog 检查目录中的计算机的 UpgradeState:

示例：

```
- Get-VusCatalog -Name test-catalog
```

```
PS C:\Windows\system32> Get-VusCatalog -Name test-catalog_

CancelledUpgrades      :
DurationInHours        :
FailedUpgrades         :
InProgressUpgrades     :
LastStateChangeInUtc   :
MaxConcurrentUpgrades  :
Name                   : test-catalog
ProvisioningType        : MCS
ScheduledTimeInUtc     :
SecurityCheckFailedUpgrades :
SessionSupport         : SingleSession
StateId                :
SuccessfulUpgrades     :
TotalMachines          :
Uid                    : 30
UpgradeState           : UpgradeAvailable
UpgradeType            : LTSR
UpgradeVersion         :
Uuid                   : 3ad4253c-3dfa-4982-8e6e-7686bf904da1
```

如果您看到 `UpgradeState` 为 `Unknown`，可能的原因之一是 VDA 上安装的 Citrix VDA Upgrade Agent 尚未向 VDA 更新服务报告该版本。可以使用 `Get-VusComponentVersion` cmdlet 来检查 VDA 是否已报告组件版本。

- `Get-VusComponentVersion -MachineId ""`

```
PS C:\Users> Get-VusComponentVersion -MachineId d664614a-cd37-44d6-b1f0-6f6b70f8299c

ComponentType MachineId                               Uid                               Version
-----
VDA d664614a-cd37-44d6-b1f0-6f6b70f8299c 7505fa4c-1811-ee11-907e-0022484becbd 2203.0.0.33220
VUS d664614a-cd37-44d6-b1f0-6f6b70f8299c 7705fa4c-1811-ee11-907e-0022484becbd 7.37.0.7
Mps d664614a-cd37-44d6-b1f0-6f6b70f8299c 7805fa4c-1811-ee11-907e-0022484becbd 7.33.0.26
SupportabilityTools d664614a-cd37-44d6-b1f0-6f6b70f8299c 7a05fa4c-1811-ee11-907e-0022484becbd 1.5.0.17
Upm d664614a-cd37-44d6-b1f0-6f6b70f8299c 7c05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
UpmVdaPlugin d664614a-cd37-44d6-b1f0-6f6b70f8299c 7d05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
```

如果未显示任何结果，请验证以下内容：

- VDA 是目录和交付组的一部分。
- VDA 升级代理已安装在 VDA 上并且正在运行。如有必要，请尝试重新启动代理。

注意：如果仍然没有结果，请在重新启动 VDA Upgrade Agent 的同时收集 Citrix 诊断设施跟踪信息并解决问题。

- 安排 VDA 升级。在开始之前，请注意以下事项：
  - `DurationInHours`：允许您提供升级过程的持续时间（以小时为单位）。目录中的 VDA 将进入维护模式。将下载 VDA 安装程序并对每个 VDA 执行升级。如果目录包含许多 VDA，请提供更长的持续时间。
  - `UpgradeNow`：使用此开关可立即安排升级或设置 `ScheduledTimeInUtc`。
  - `ScheduledTimeInUtc`：允许您在特定的日期和时间安排升级。

示例：

```
- New-VusCatalogSchedule -CatalogName test-catalog -ScheduledTimeInUtc
([System.DateTime]::ParseExact("06/23/2023 04:00 PM", 'MM/dd
/yyyy hh:mm tt', $null)) -DurationInHours 4
```

可以使用 `CatalogName`、`Uid` 和 `Uuid` 来安排升级。

```
PS C:\Windows\system32> New-VusCatalogSchedule -CatalogName test-catalog -ScheduledTimeInUtc ([System.DateTime]::ParseExact("06/23/2023 04:00 PM", 'MM/dd/yyyy hh:mm tt', $null)) -DurationInHours 4
CatalogName      : test-catalog
CatalogUID       : 3ad4253c-3dfa-4982-8e6e-7686bf904da1
CatalogUid       : 30
DurationInHours   : 4
LastStateChangeInUtc : 6/23/2023 12:08:14 PM
ScheduledTimeInUtc : 6/23/2023 12:00:00 PM
State             : UpgradeScheduled
UpgradeVersion    : 2203.0.3000.3300
```

- 检查升级状态。使用 `Get-VusCatalog` 或 `Get-VusMachine` cmdlet 定期检查 VDA 升级状态。使用 `MachineUuid`、`MachineUid` 和 `MachineName` 筛选 VDA。

示例：

```
-Get-VusCatalog -Name test-catalog
```

```
PS C:\Windows\system32> Get-VusCatalog -Name test-catalog

CancelledUpgrades      : 0
DurationInHours        : 4
FailedUpgrades         : 0
InProgressUpgrades     : 0
LastStateChangeInUtc   : 6/23/2023 12:08:43 PM
MaxConcurrentUpgrades  : 100
Name                   : test-catalog
ProvisioningType        : MCS
ScheduledTimeInUtc     : 6/23/2023 12:00:00 PM
SecurityCheckFailedUpgrades : 0
SessionSupport         : SingleSession
StateId                : UpgradeInProgress
SuccessfulUpgrades     : 0
TotalMachines          : 2
Uid                    : 30
UpgradeState           : UpgradeScheduled
UpgradeType            : LTSR
UpgradeVersion          : 2203.0.3000.3300
Uuid                   : 3ad4253c-3dfa-4982-8e6e-7686bf904da1
```

使用 `Get-VusMachine` 查看目录中每台计算机的 VDA 升级状态。



```
PS C:\Users\vaishakb> Get-VusMachine -CatalogName test-catalog

CatalogName      : test-catalog
DNSName           : test-machine-1
DurationInHours   : 4
LastStateChange   : 6/23/2023 12:18:21 PM
MachineName       : test-machine-1
MachineUid        : 35
MachineUuid       : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType   : MCS
ScheduledTime     : 6/23/2023 12:00:00 PM
SessionSupport    : SingleSession
StateId           : UpgradeSuccess
StatusMessage     : Upgrade completed successfully or is already up to date
UpgradeState      : UpToDate
UpgradeType       : LTSR
UpgradeVersion    : 2203.0.3000.3300

CatalogName      : test-catalog
DNSName           : test-machine-2
DurationInHours   : 4
LastStateChange   : 6/23/2023 12:17:33 PM
MachineName       : test-machine-2
MachineUid        : 36
MachineUuid       : cfa55303-6000-4973-bee8-e38c9916719e
ProvisioningType   : MCS
ScheduledTime     : 6/23/2023 12:00:00 PM
SessionSupport    : SingleSession
StateId           : UpgradeInProgress
StatusMessage     :
UpgradeState      : UpgradeScheduled
UpgradeType       : LTSR
UpgradeVersion    : 2203.0.3000.3300
```

## 如果 VDA 安装了 Personal vDisk

如果 VDA 上曾安装过 Personal vDisk (PvD) 组件，则无法将该 VDA 升级到 1912 LTSR 或更高版本，直指您删除该组件。

即使您从未使用 PvD，此指导亦适用。下面是 PvD 组件在早期版本中的安装方式：

- 在 VDA 安装程序的图形界面中，PvD 是其他组件页面上的一个选项。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（或在任何版本中明确启用了该选项），则安装了 PvD。
- 在命令行上，`/baseimage` 选项安装了 PvD。如果指定了此选项，或使用了包含此选项的脚本，则安装了 PvD。

### 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 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 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，则会自动删除该组件并继续进行升级。
- **CLI**：如果安装程序检测到 PvD 组件，该命令将失败。为避免命令失败，请在命令中包括以下选项：`/remove_pvd_ack`。

如果要在 Windows 10（1607 及更早版本，无更新）计算机上继续使用 PvD，VDA 7.15 LTSR 为受支持的最新版本。请注意，XenApp 和 XenDesktop 7.15 LTSR 的扩展支持计划不适用于与 Citrix DaaS 一起使用的 VDA。有关详细信息，请参阅 Citrix 支持知识中心中的[扩展支持客户指南](#)。

## 早期版本的操作系统

[系统要求](#)一文列出了当前版本 VDA 支持的 Windows 操作系统。

- 对于 LTSR VDA，请参阅 LTSR 版本的系统要求一文。
- 有关 Linux VDA 的信息，请参阅 [Linux Virtual Delivery Agent](#) 文档。

对于操作系统不再支持安装最新 VDA 的 Windows 计算机，您可以选择以下选项。

对于非 WVD 环境：

- 将计算机重置映像到受支持的 Windows 版本，然后安装新 VDA。
- 如果无法对计算机重置映像，但您要升级操作系统，请在升级操作系统之前卸载 VDA。否则，VDA 将处于不受支持的状态。升级操作系统后，安装新 VDA。
- 如果计算机上安装了版本 7.15 LTSR（并且您尝试安装更高版本），则会显示一条消息，告知您使用的是支持的最新版本。
- 如果计算机上安装的版本早于 7.15 LTSR，则会显示一条消息，指导您参阅 [CTX139030](#) 了解相关信息。可以从 Citrix Web 站点下载 7.15 LTSR VDA。

## 将配置迁移到 Citrix Cloud

March 30, 2024

### 为什么使用自动配置

负责大型或复杂环境的 IT 管理员通常会发现迁移是一个繁琐的过程。他们最终经常编写自己的工具来成功完成此任务，因为它往往是特定于他们的使用案例。

Citrix 希望通过使用自动配置工具自动执行迁移过程来帮助简化此过程。管理员可以轻松地在 Citrix Cloud 中测试当前配置，并利用 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）提供的优势，同时保持当前环境不变。由于自动配置可在后台无缝运行，因此也不会对最终用户造成影响。这些好处包括在 Citrix 管理部分后端和控制平面时降低管理过载、自动和可自定义的 Citrix Cloud 组件更新等。

Citrix 使用行业标准配置即代码来提供一种帮助自动化迁移过程的机制。自动配置发现一个或多个本地站点并将其导出为配置文件的集合。然后，可以将这些文件的配置导入到 Citrix DaaS 中。

自动配置还允许管理员将多个本地站点合并到一个站点中，同时避免名称冲突。管理员可以控制本地配置还是云配置控制资源。

自动配置不仅是一次性迁移工具，还可以在 Citrix Cloud 中自动执行日常配置。移动 Citrix DaaS 配置有很多好处，原因如下：

- 将您的站点从测试或阶段同步到生产
- 备份和还原配置
- 达到资源限制
- 从一个区域迁移到另一个区域

下面这个 2 分钟的视频提供了自动配置的快速浏览。

这是一个嵌入式视频。单击链接观看视频

有关自动配置的更多信息，请参阅 Tech Zone 上的概念证明：自动配置工具。

要深入了解如何移动您的部署和准备好迁移本地配置，请参阅 Tech Zone 上的部署指南：将 Citrix Virtual Apps and Desktops 从本地迁移到 Citrix Cloud。

### 下载自动配置

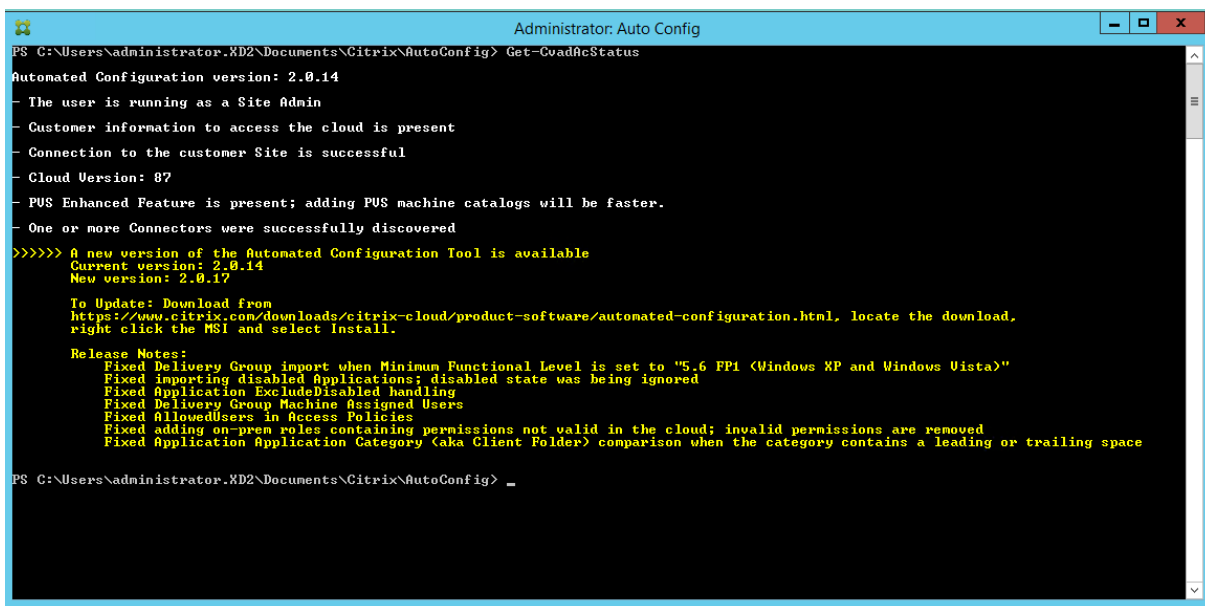
从 Citrix 下载并安装自动配置工具。

重要：

为防止功能出现错误，请始终使用可用的最新版本的自动配置。

### 升级自动配置

在自动配置中运行访问云的 cmdlet 时，当有更新版本可供下载时，该工具会提醒您。



```

Administrator: Auto Config
PS C:\Users\administrator.XD2\Documents\Citrix\AutoConfig> Get-CvadAcStatus

Automated Configuration version: 2.0.14
- The user is running as a Site Admin
- Customer information to access the cloud is present
- Connection to the customer Site is successful
- Cloud Version: 87
- PUS Enhanced Feature is present; adding PUS machine catalogs will be faster.
- One or more Connectors were successfully discovered
>>>>> A new version of the Automated Configuration Tool is available
Current version: 2.0.14
New version: 2.0.17

To Update: Download from
https://www.citrix.com/downloads/citrix-cloud/product-software/automated-configuration.html, locate the download,
right click the MSI and select Install.

Release Notes:
Fixed Delivery Group import when Minimum Functional Level is set to "5.6 FP1 (Windows XP and Windows Vista)"
Fixed importing disabled Applications; disabled state was being ignored
Fixed Application ExcludeDisabled handling
Fixed Delivery Group Machine Assigned Users
Fixed AllowedUsers in Access Policies
Fixed adding on-prem roles containing permissions not valid in the cloud; invalid permissions are removed
Fixed Application Application Category (aka Client Folder) comparison when the category contains a leading or trailing space

PS C:\Users\administrator.XD2\Documents\Citrix\AutoConfig> _

```

可以按照以下步骤确保拥有最新版本：

1. 双击自动配置图标。此时将显示 PowerShell 窗口。
2. 运行以下命令以检查您的版本号。  
  
`Get-CvadAcStatus`
3. 根据警告或 [Citrix 下则](#) 中列出的版本检查您的工具版本。该工具的最新版本位于此处。
4. 下载并安装最新版本的工具。无需卸载旧版本即可升级自动配置。

#### 注意：

每次运行访问云的 cmdlet 时都会出现警报。有关 cmdlet 的详细信息，请参阅[自动配置工具 cmdlet](#)。

## 已知限制

- 通过 Machine Creation Services 预配的计算机目录具有特殊注意事项。有关 MCS 的详细信息，请参阅[了解迁移 Machine Creation Services 预配的目录](#)。

## 支持的迁移对象

自动配置支持移动以下组件的配置：

- 标记
- 委派管理员
  - 作用域
  - 角色

- 主机连接
  - 单个资源池
  - 管理员作用域
- 计算机目录
  - 管理员作用域
  - 计算机
  - Remote PC Access、物理、池化、已预配、MCS、已分配
- StoreFront
- 交付组
  - 访问策略
  - 管理员范围关联
  - 应用程序访问策略
  - 分配策略
  - 注册/桌面策略
  - 电源计划
  - 会话延迟
  - 会话预启动
  - 重新启动计划
  - 标记
- 应用程序组
  - 管理员范围关联
  - 交付组
  - 用户和组
- 应用程序
  - 应用程序文件夹
  - 图标
  - 应用程序
  - 代理配置的 FTA
  - 标记
- 组策略
- 用户区域首选项

## 组件迁移顺序

此处列出了组件及其依赖关系。组件的依赖关系必须到位，才能将其导入或合并。如果缺少依赖关系，则可能会导致导入或合并命令失败。如果导入或合并失败，日志文件的 **Fixups** 部分会显示缺少依赖关系。

1. 标记

- 无预依赖关系

2. 委派管理员

- 无预依赖关系

3. 主机连接

- CvadAcSecurity.yml 中的安全信息

4. 计算机目录

- Active Directory 中存在的计算机
- 主机连接
- 标记

5. StoreFront

6. 交付组

- Active Directory 中存在的计算机
- Active Directory 中存在的用户
- 计算机目录
- 标记

7. 应用程序组

- 交付组
- 标记

8. 应用程序

- 交付组
- 应用程序组
- 标记

9. 组策略

- 交付组
- 标记

10. 用户区域首选项

## 常见的必备条件

以下是自动配置正常运行所需的一些常见先决条件。这些必备条件同时在[本地到云](#)和[云到云](#)的迁移中使用。

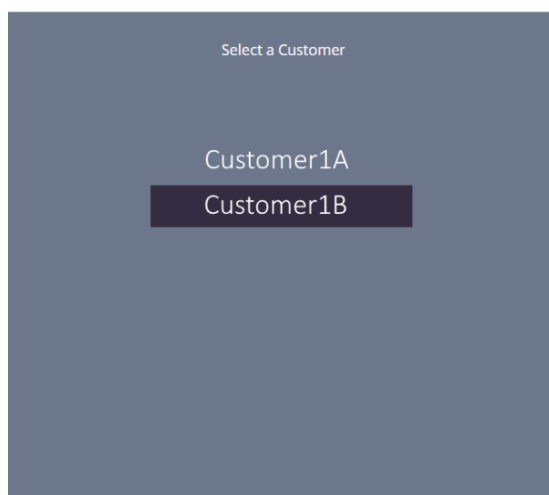
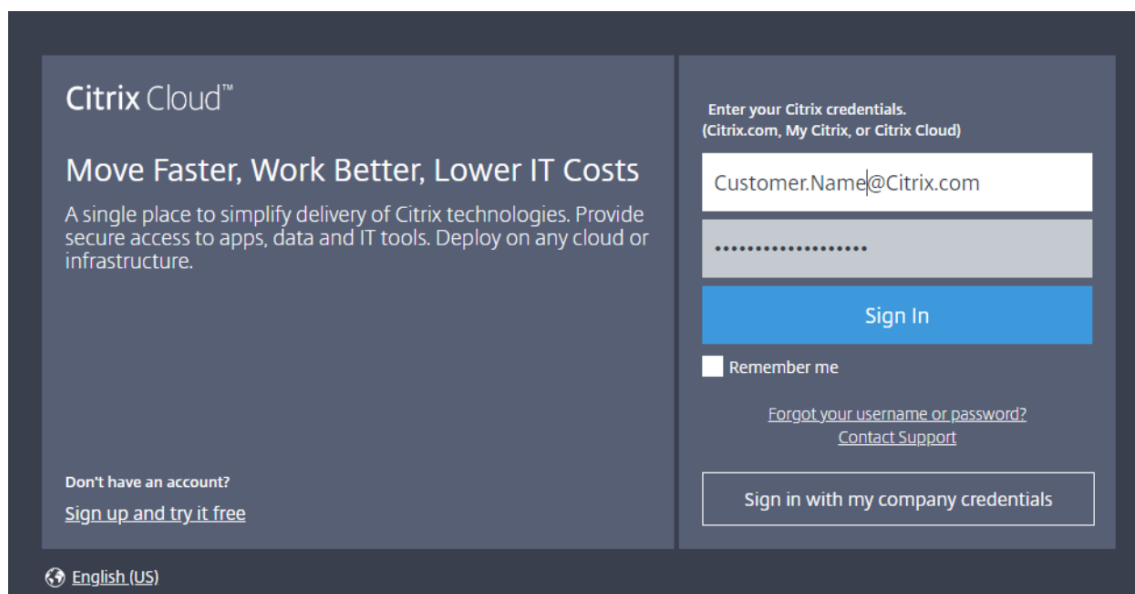
生成客户 ID、客户端 ID 和密钥

在使用自动配置开始迁移之前，您需要 Citrix Cloud 客户 ID，并且必须创建客户端 ID 和密钥才能将配置导入 Citrix Cloud。所有访问云的 cmdlet 都需要这些值。

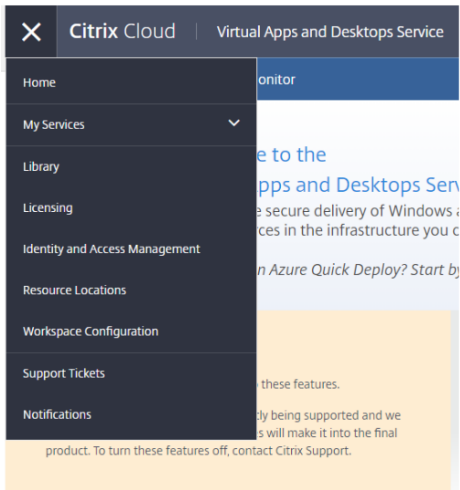
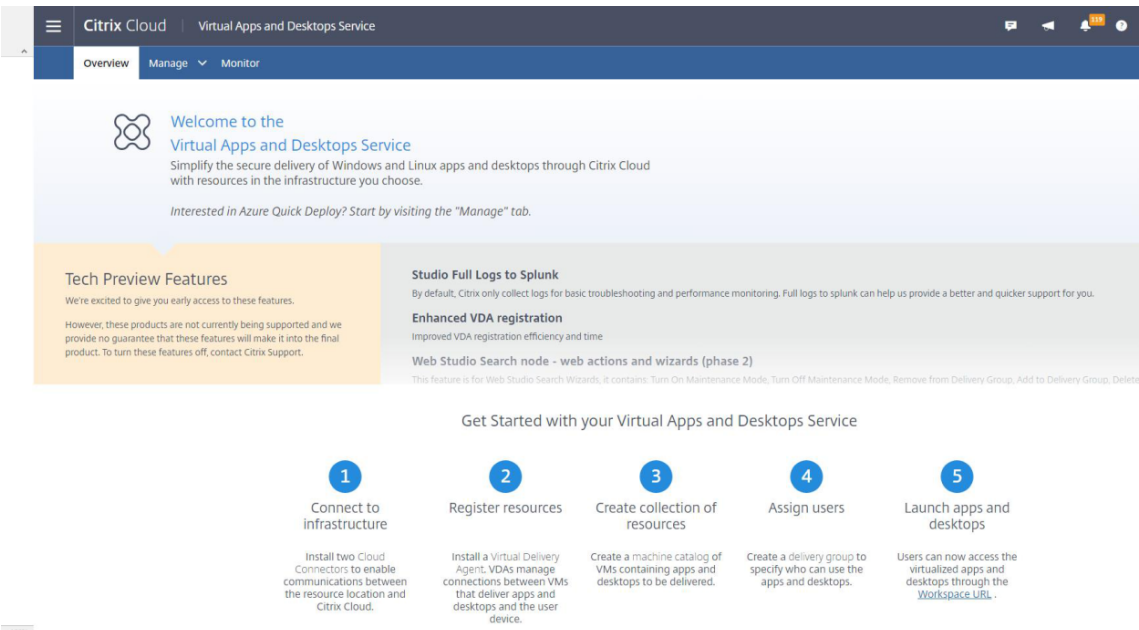
以下步骤允许您检索客户 ID 并创建客户端 ID 和密钥。

要检索客户 ID，请执行以下操作：

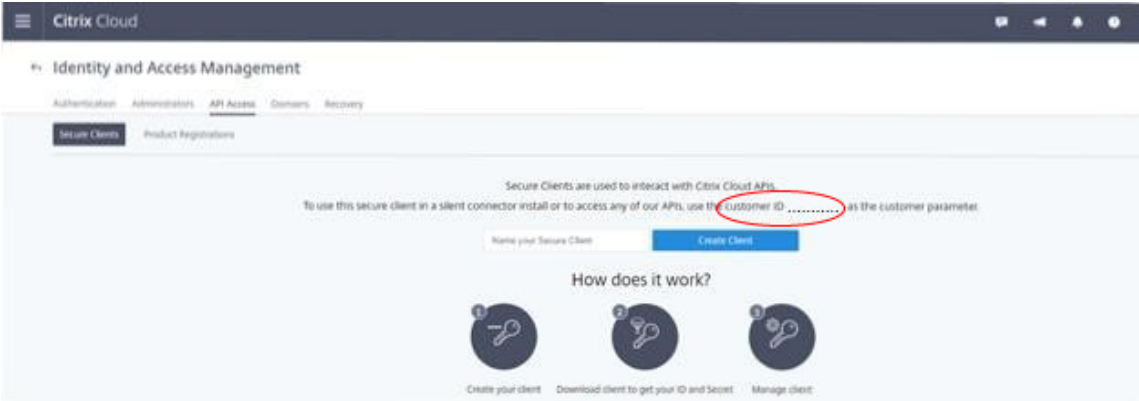
1. 登录到您的 Citrix Cloud 帐户并选择相应客户。



2. 单击汉堡菜单，然后选择下拉菜单中的身份识别和访问管理。



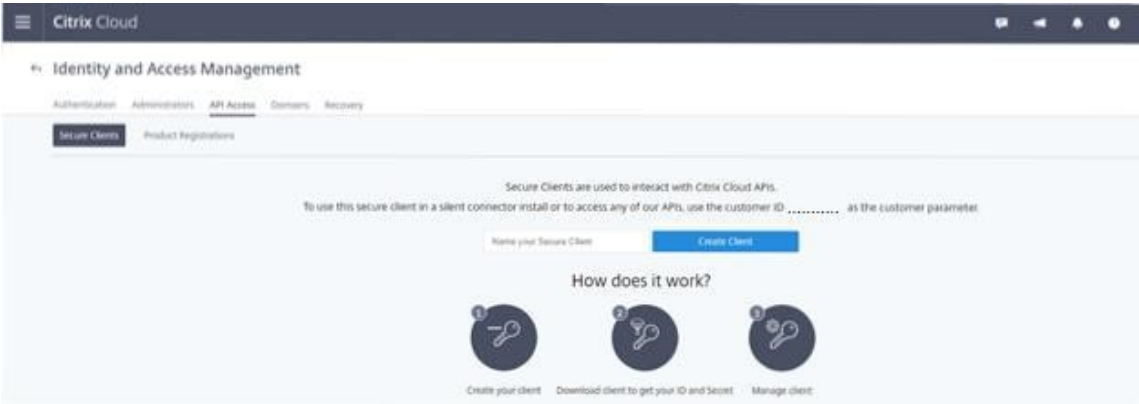
3. 客户 ID 位于身份和访问管理页面上。



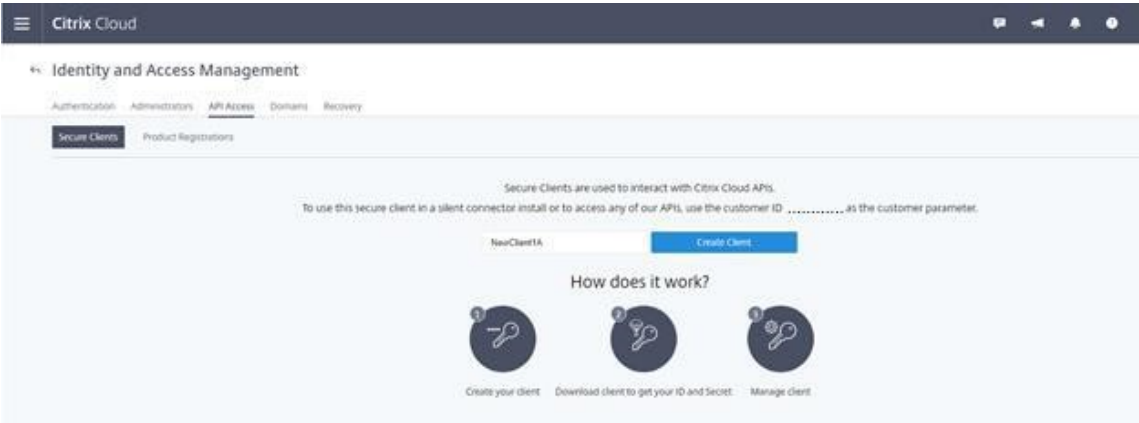


要检索客户端 ID 和密钥，请执行以下操作：

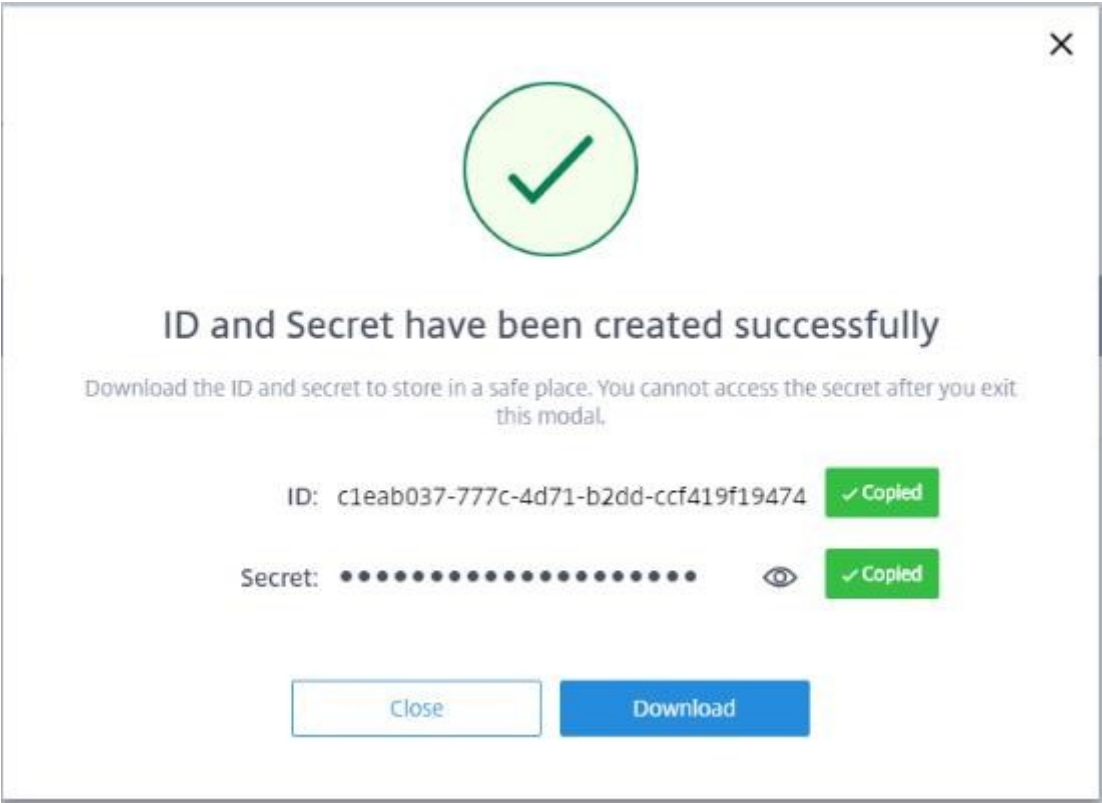
1. 在身份识别和访问管理页面上，单击 **API** 访问选项卡。



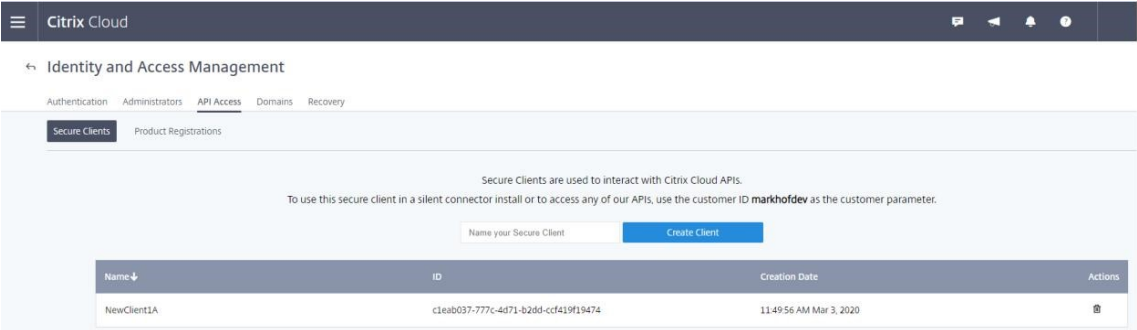
2. 在该框中输入名称。此名称用于区分多个客户端 ID 和密钥。单击创建客户端以创建客户端 ID 和密钥。



3. 成功创建客户端 ID 和密钥后，将显示以下对话框。请务必将这两个值复制到安全位置并下载包含这些信息的.csv 文件。.csv 文件可用于创建 CustomerInfo.yml 文件。



4. 已成功创建客户端 ID 和密钥。



将这些值置于安全位置，并仅与需要访问该工具或访问云 REST API 的受信任公司成员共享。客户端 ID 和密钥不会过期。如果它们被盗用，请立即使用垃圾桶图标将其删除，然后创建新的客户端 ID 和密钥。

注意：

密钥在丢失或忘记的情况下无法找回；必须创建新的客户端 ID 和密钥。

填充客户信息文件

使用 CustomerInfo.yml 文件无需在执行每个 cmdlet 时提供客户信息参数。使用 cmdlet 参数可以覆盖任何客户信息。

通过使用 `New-CvadAcCustomerInfoFile` cmdlet 来创建 CustomerInfo.yml 文件。

**重要：**

请勿手动编辑 CustomerInfo.yml 文件。这样做可能会导致出现意外的格式错误。

`New-CvadAcCustomerInfoFile` 具有以下必需参数。

- `CustomerId` – 客户的 ID。
- `ClientId` – 客户的客户端 ID（在 Citrix Cloud 上创建）。
- `Secret` – 客户的密钥（在 Citrix Cloud 上创建）。

```
New-CvadAcCustomerInfoFile -CustomerId markhof123 -ClientId 6813EEA6
-46CC-4F8A-BC71-539F2DAC5984 -Secret TwBLaaaaaaaaaaaaaaw==
```

还可以使用指向下载的 security.csv 文件的 `SecurityCsvFileSpec` 参数创建 CustomerInfo.yml。还必须指定 CustomerId。

```
New-CvadAcCustomerInfoFile -SecurityCsvFileSpec C:\Users\my_user_name
\downloads\security.csv -CustomerId markhof123
```

通过使用 `Set-CvadAcCustomerInfoFile` cmdlet 来更新 CustomerInfo.yml 文件。此 cmdlet 只会更改客户端 ID。

```
Set-CvadAcCustomerInfoFile -ClientId C80487EE-7113-49F8-85DD-2CFE30CC398E
```

下面是一个示例 CustomerInfo.yml 文件。

```
1      # Created/Updated on 2020/01/29 16:46:47
2      CustomerId: 'markhof123'
3      ClientId: '6713FEA6-46CC-4F8A-BC71-539F2DDK5384'
4      Secret: 'TwBLaaabbbbaaaaaaaaaaaw=='
5      Environment: Production
6      AltRootUrl: ''
7      StopOnError: False
8      AlternateFolder: ''
9      Locale: 'en-us'
10     Editor: 'C:\Program Files\Notepad++\notepad++.exe'
11     Confirm: True
12     DisplayLog: True
```

**填充区域映射文件**

本地区域相当于云资源位置。与其他站点组件不同，您无法自动将本地区域导入到云中。相反，必须使用 `ZoneMapping.yml` 文件手动对其进行映射。如果区域名称与现有资源位置名称未关联，则可能会发生导入失败。

对于只有一个区域的本地站点和只有一个资源位置的云站点，自动配置工具可以进行正确的关联，这样将无需手动管理 `ZoneMapping.yml` 文件。

对于具有多个区域的本地站点或具有多个资源位置的云站点，ZoneMapping.yml 文件必须手动更新，以反映本地区域到云资源位置的正确映射。在尝试向云中执行任何导入操作之前，必须执行此操作。

ZoneMapping.yml 文件位于%%HOMEPATH%\Documents\Citrix\AutoConfig 下。yml 文件的内容是区域名称为键且资源位置名称为值的字典。

例如，将包含名为“Zone-1”的主区域和名为“Zone-2”的辅助区域的本地 Citrix Virtual Apps and Desktops 站点迁移到包含两个新创建的名称为“Cloud-RL-1”和“Cloud-RL-2”的云资源位置的 Citrix DaaS 部署。在这种情况下，ZoneMapping.yml 将按如下所示进行配置：

```
1      Zone-1: Cloud-RL-1
2
3      Zone-2: Cloud-RL-2
```

注意：

冒号与资源位置名称之间必须有一个空格。如果区域或资源位置名称中使用空格，请将名称用引号引起。

主机连接

可以使用自动配置导出和导入主机连接及其关联的虚拟机管理程序。

向主机连接添加虚拟机管理程序需要特定于虚拟机管理程序类型的安全信息。出于安全考虑，无法从本地站点导出此信息。您必须手动提供该信息，以便自动配置能够成功地将主机连接和虚拟机管理程序导入云站点。

导出过程会在 %HOMEPATH%\Documents\Citrix\AutoConfig 中创建 CvadAcSecurity.yml 文件，该文件包含特定的虚拟机管理程序类型所需的每个安全项目的占位符。在导入到云站点之前，必须更新 CvadAcSecurity.yml 文件。在根据需要添加新的安全占位符的多次导出过程中，将保留管理员进行的更新。禁止删除安全项目。有关更多信息，请参阅 [手动更新 CvadAcSecurity.yml 文件](#)

```
1      HostConn1:
2      ConnectionType: XenServer
3      UserName: root
4      PasswordKey: rootPassword
5      HostCon2:
6      ConnectionType: AWS
7      ApiKey: 78AB6083-EF60-4D26-B2L5-BZ35X00DA5CH
8      SecretKey: TwBLaaaaaaaaaaaaaaaaaw==
9      Region: East
```

每个虚拟机管理程序的安全信息 下面列出了每种虚拟机管理程序类型所需的安全信息。

- XenServer、Hyper-V、VMware
  - 用户名
  - 明文密码
- Microsoft Azure

- 订阅 ID
- 应用程序 ID
- 应用程序机密
- Amazon Web Services
  - 服务帐户 ID
  - 应用程序机密
  - 地理区域

**特殊安全注意事项** 所有安全信息都以明文形式输入。如果不建议使用明文，则可以使用管理 > 完整配置界面手动创建主机连接和关联的虚拟机管理程序。主机连接和虚拟机管理程序名称必须与其本地主机连接和虚拟机管理程序名称完全相同，以便成功导入使用主机连接的计算机目录。

## 激活站点

本地站点和云站点中的 Delivery Controller 可以控制诸如代理桌面、应用程序和重新启动计算机等资源。当一组常见的资源由两个或更多站点控制时会出现问题。从本地站点迁移到云站点时，可能会发生这种情况。本地 Delivery Controller 和云端 Delivery Controller 都可以管理相同的一组资源。这种双重管理可能会导致资源变得不可用和无法管理，并且可能难以诊断。

站点激活允许您控制活动站点的控制位置。

使用交付组维护模式管理站点激活。当站点处于非活动状态时，交付组将处于维护模式。对于处于活动状态的站点，将从交付组中删除维护模式。

站点激活不会影响或管理 VDA 注册或计算机目录。

- `Set-CvadAcSiteActiveStateCloud`
- `Set-CvadAcSiteActiveStateOnPrem`

所有 cmdlet 都支持 `IncludeByName` 和 `ExcludeByName` 过滤。此参数允许您选择哪些交付组可以更改其维护模式。可以根据需要有针对性地更改交付组。

## 将控制权导入和转移到云

下面是关于如何将控制权从本地站点导入和转移到云站点的高级说明。

1. 将本地站点导出并导入到云中。确保任何导入 cmdlet 上都不存在 `-SiteActive` 参数。本地站点处于活动状态，云站点处于非活动状态。默认情况下，云站点交付组处于维护模式。
2. 验证云内容和配置。
3. 在空闲时间，将本地站点设置为非活动状态。`-SiteActive` 参数必须不存在。所有本地站点交付组都处于维护模式。

- `Set-CvadAcSiteActiveStateOnPrem`

4. 将云站点设置为活动状态。- `SiteActive` 参数必须存在。没有云站点交付组处于维护模式。

- `Set-CvadAcSiteActiveStateCloud -SiteActive`

5. 验证云站点是否处于活动状态且本地站点处于非活动状态。

将控制权转移回本地站点

要将控制权从云站点转移到本地站点，请执行以下操作：

1. 在空闲时间，将云站点设置为非活动状态。所有云站点交付组都处于维护模式。

- `Set-CvadAcSiteActiveStateCloud`

2. 将本地站点设置为活动状态。没有本地站点交付组处于维护模式。

- `Set-CvadAcSiteActiveStateOnPrem -SiteActive`

其他站点激活信息

- 如果没有计算机进行电源管理且没有重新启动计划（这通常表示没有主机连接），则可以将所有云交付组导入为活动状态。向 `Merge-CvadAcToSite/Import-CvadAcToSite` 中添加 `-SiteActive` 或导入后运行 `Set-CvadAcSiteActiveStateCloud -SiteActive`。
- 如果计算机受到电源管理或者有重新启动计划，则需要不同的过程。例如，在这种情况下从本地切换到云时，使用 `Set-CvadAcSiteActiveStateOnPrem` 将本地站点设置为非活动状态。然后，使用 `Set-CvadAcSiteActiveStateCloud -SiteActive` 将云站点设置为活动状态。
- `Set-CvadAcSiteActiveStateCloud` 和 `Set-CvadAcSiteActiveStateOnPrem` cmdlet 也用于反转该过程。例如，先运行不带 `-SiteActive` 参数的 `Set-CvadAcSiteActiveStateCloud`，然后再运行带 `-SiteActive` 参数的 `Set-CvadAcSiteActiveStateOnPrem`。

了解迁移 **Machine Creation Services** 预配的目录

注意：

此功能仅在 3.0 及更高版本中提供。在自动配置中使用 `Get-CvadAcStatus` 检查您的版本。

Machine Creation Services (MCS) 目录创建两种不同类型的目录：

- 当对计算机所做的更改丢失/撤销时（通常是在其中发布应用程序的服务器操作系统）- 这是一个池 VDI/多会话用例
- 在重新启动过程中保留对计算机所做的更改时（通常为具有专有用户的客户端操作系统）- 这是一个静态 VDI 用例

可以在 Citrix Studio 的目录节点中确认目录类型，然后查看目录的“用户数据:”值。

注意：

无法使用自动配置从云中备份 MCS。

## 池 VDI/多会话目录

包含“用户数据：丢弃”的目录是池 VDI 目录，只能迁移主映像和配置。不会迁移这些目录中的任何虚拟机。这是因为虚拟机的生命周期由您从中导入的站点进行维护，这意味着每次打开计算机时，其状态都可能会发生变化。这将导致无法导入，因为虚拟机的导入数据很快就会失去同步。

使用该工具迁移这些目录时，它会创建目录元数据并启动主映像创建，但不会导入任何计算机。

由于根据主映像的大小创建此过程可能需要一些时间，因此该工具中的导入命令只会启动 MCS 目录的创建过程，而不会等待创建完成。导入完成后，在云部署中使用“完整配置”管理界面监视目录创建进度。

创建主映像后，可以预配计算机。需要考虑容量注意事项，因为本地使用时会消耗容量。

使用该目录的所有其他对象（交付组/应用程序/策略等）都可以导入，而不必等待主映像创建。目录创建完成后，可以将计算机添加到导入的目录中，用户之后可以启动其资源。

注意：

使用该工具中可用的相同命令迁移目录以及所有其他对象。

## 静态 VDI 目录

注意：

由于此操作会导入存储在数据库中的低级别详细信息，因此必须从具有数据库访问权限的计算机运行此过程。

静态 VDI 目录迁移主映像、配置和所有虚拟机。与池 VDI 用例不同，不需要创建任何映像。

VDA 必须指向连接器才能在云中注册。

请参阅[激活站点](#)部分以使云站点处于活动状态，以便重新启动计划、电源管理和其他项目由云控制。

迁移完成后，如果要从本地站点删除此目录，则必须选择退出 VM 和 AD 帐户。否则，它们将被删除，云站点将指向已删除的 VM。

## 更新 MCS 标签以在迁移后检测孤立资源

从本地配置迁移到云站点，或从云配置迁移到另一个云站点后，如果是永久虚拟机，则必须更新 MCS 站点 ID 标记，这样才能正确检测孤立资源。要执行此操作，请使用 PowerShell 命令 `Set-ProvResourceTags`。目前，此功能适用于 Azure。

详细步骤如下所示：

1. 使用 PowerShell 命令 `Set-ProvResourceTags` 从新 Citrix 站点更新 MCS 站点 ID 标签。例如：

```
1 Set-ProvResourceTags -ProvisioningSchemeUid xxxxx [-VMName <
  String>] [-VMBatchSize XX] [-ResourceType XX]
2 <!--NeedCopy-->
```

或者，

```
1 Set-ProvResourceTags -ProvisioningSchemeName xxxxx [-VMName <
  String>] [-VMBatchSize XX] [-ResourceType XX]
2 <!--NeedCopy-->
```

参数详细信息如下：

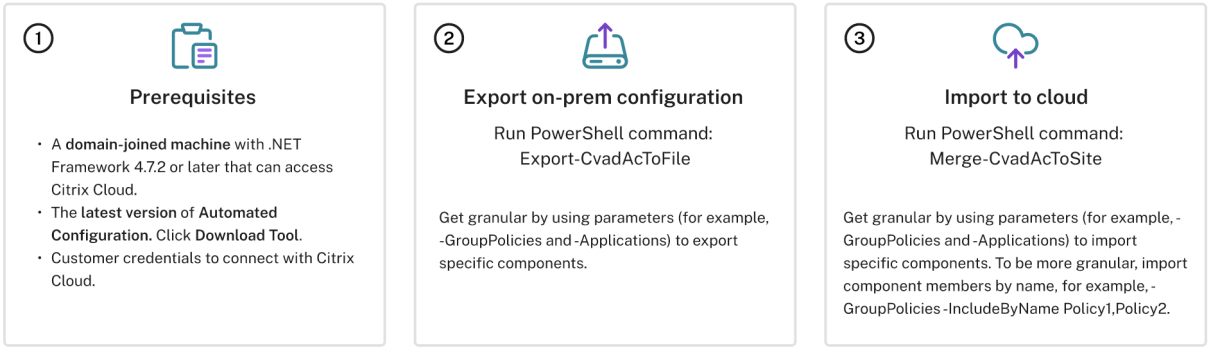
- `ProvisioningSchemeUid` 或者 `ProvisioningSchemeName` 是必选参数。
- `VMName` 是可选参数。如果未指定 `VMName`，则更新该计算机目录中所有虚拟机的标签。
- `VMBatchSize` 是将所有虚拟机分成批的可选参数。如果未指定 `VMBatchSize`，则应用默认值 (10)。范围在 1 到 60 之间。
- `ResourceType` 可以是以下之一：
  - `MachineCatalog`：用于更新计算机目录资源的标签。
  - `VirtualMachine`：用于更新虚拟机相关资源的标签。
  - `All`：(默认资源类型)：用于更新计算机目录和虚拟机相关资源的标签。

从本地迁移到云

March 30, 2024

自动配置允许您自动将本地配置移动到云站点。

下图是自动配置如何将配置迁移到云的高级视图。





## 迁移配置的必备条件

要从 Citrix Virtual Apps and Desktops 导出 配置，您需要：

- Citrix Virtual Apps and Desktops：当前版本及其直接前代产品或 Citrix Virtual Apps and Desktops、XenApp 和 XenDesktop LTSR：所有版本
- 安装了 .NET Framework 4.7.2 或更高版本以及 Citrix PowerShell SDK 的已加入域的计算机。这将自动安装在 Delivery Controller 上。（要在本地 Delivery Controller 以外的计算机上运行，必须安装 Citrix Studio，这样 Studio 才能安装正确的 PowerShell 管理单元。Studio 安装程序位于 Citrix Virtual Apps and Desktops [安装介质](#)中。）

要将您的配置导入到 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）中，您需要：

- 有权访问 Citrix Cloud 的计算机。这不一定是 Delivery Controller 或加入了域的计算机。
- Citrix DaaS 已预配。
- 安装了 Connector 并加入到与本地设置相同的域的活动资源位置。
- 必须允许并且可以连接到访问 Citrix Cloud 的站点。有关详细信息，请参阅[系统和连接要求](#)。

注意：

无法在 Cloud Connector 系统中安装自动配置。

## 导出 **Citrix Virtual Apps and Desktops** 本地配置

重要：

- 您必须附上您的 CustomerInfo.yml 文件以及您的客户 ID、客户端 ID 和密钥信息。有关如何检索客户 ID、客户端 ID 和密钥的详细信息，请参阅[生成客户 ID、客户端 ID 和密钥](#)。有关如何将这些信息添加到 CustomerInfo.yml 文件中的信息，请参阅[填充客户信息文件](#)。
- ZoneMapping.yml 文件必须包含将本地区域映射到云中的资源位置的信息。有关如何映射您的区域的详细信息，请参阅[填充区域映射文件](#)。
- 如果您有主机连接，则必须在 CvadAcSecurity.yml 文件中输入相应的信息。

1. [安装自动配置](#)。
2. 双击自动配置图标。此时将显示 PowerShell 窗口。
3. 运行以下命令以导出所有组件。导出您的本地配置不会以任何方式更改这些配置。

### `Export-CvadAcToFile`

首次运行任何 cmdlet 之后，系统将创建包含.yml 配置文件和日志的 export 文件夹。该文件夹位于 %HOMEPATH%\Documents\Citrix\AutoConfig 中。每次连续导出都将创建一个子文件夹。父文件夹 %HOMEPATH%\Documents\Citrix\AutoConfig 始终包含最近导出的对象中的导出文件。

### 注意：

如果 Delivery Controller 上未安装自动配置，请在通过 PowerShell 使用该工具之前运行 `import-module Citrix.AutoConfig.Commands`。如果使用自动配置图标打开自动配置，则不需要执行此步骤。

如果您遇到任何错误或异常，请参阅日志文件中的 **Fixups** 部分。

## 将配置导入到 Citrix DaaS

### 重要：

- 您必须附上您的 CustomerInfo.yml 文件以及您的客户 ID、客户端 ID 和密钥信息。有关如何检索客户 ID、客户端 ID 和密钥的详细信息，请参阅[生成客户 ID、客户端 ID 和密钥](#)。有关如何将这些信息添加到 CustomerInfo.yml 文件中的信息，请参阅[填充客户信息文件](#)。
- ZoneMapping.yml 文件必须包含将本地区域映射到云中的资源位置的信息。有关如何映射您的区域的详细信息，请参阅[填充区域映射文件](#)。
- 如果您有主机连接，则必须在 CvadAcSecurity.yml 文件中输入相应的信息。

### 运行导入

1. 双击自动配置图标。此时将显示 PowerShell 窗口。
2. 运行以下命令以导入所有组件。

```
Merge-CvadAcToSite
```

请使用新的当前状态来验证预期状态。各种导入选项控制导入结果相同还是属于本地站点的子集。

运行该 cmdlet 之后，系统将创建包含.yml 配置文件和日志的 export 文件夹。该文件夹位于 `%HOMEPATH%\Documents\Citrix\AutoConfig` 中。

如果您遇到任何错误或异常，请参阅日志文件中的 **Fixups** 部分。

### 注意：

如果 Delivery Controller 上未安装自动配置，请在通过 PowerShell 使用该工具之前运行 `import-module Citrix.AutoConfig.Commands`。如果使用自动配置图标打开自动配置，则不需要执行此步骤。

要还原到原来的 Citrix DaaS 配置，请参阅[备份 Citrix DaaS 配置](#)。

### 详细的导入操作

导入过程旨在准确执行更新，仅执行所需的更新，并验证所有更新是否正确进行。下面是所有导入操作遵循的步骤。

1. 读取导出的.yml 文件（预期状态）。
2. 读取云（当前状态）。
3. 将预导入云状态备份到.yml 文件（如有必要，可以还原预备份）。
4. 评估预期状态与当前状态之间的差异。这决定了要进行哪些更新。
5. 进行更新。
6. 重读云（新的当前状态）。
7. 将导入后的云状态备份到.yml 文件（如有必要，可以还原备份后状态）。
8. 将新的当前状态与预期状态进行比较。
9. 报告比较的结果。

## 粒度迁移

重要：

有关组件迁移顺序的详细信息，请参阅[组件迁移顺序](#)。

您可以有选择地仅迁移组件，甚至仅迁移组件名称。

- 支持的组件参数包括 `MachineCatalogs`、`Tags` 等等。
- 支持的组件名称参数包括 `IncludeByName` 和 `ExcludeByName` 参数以及其他参数。

有关参数及其使用方法的详细信息，请参阅[粒度迁移参数](#)。

## 激活站点

站点激活允许您控制处于活动状态的站点并控制您的资源。有关详细信息，请参阅[激活站点](#)。

## 将多个站点合并到一个站点中

March 30, 2024

面向自动配置的多站点支持提供了一种将多个本地站点合并到单个云站点的方法。

多站点支持在每个本地站点的基础上为组件名称添加唯一的前缀和后缀，从而确保在多个本地站点合并到单个云站点后名称的唯一性。

可以在每个本地站点的基础上为以下每个组件分配前缀和后缀。

- `AdminScope`
- `AdminRole`
- `ApplicationAdmin`
- `ApplicationFolder`

- `ApplicationGroup`
- `ApplicationUser`
- `DeliveryGroup`
- `GroupPolicy`
- `HostConnection`
- `MachineCatalog`
- `StoreFront`
- `Tag`

应用程序文件夹支持前缀、后缀和重新生根。重新生根将额外的顶层文件夹添加到应用程序的现有文件夹结构中。

### 前缀和后缀规则

1. 前缀和后缀不能包含以下任何特殊字符：\ , / ; : # . \* ? = < > | ( ) " ' { } [ ]
2. 前缀和后缀可以包含尾随空格，但不能包含前导空格。
3. 前缀和后缀必须用双引号引起才能包含尾随空格。
4. 在导入、合并和添加时，会应用前缀和后缀。源.yml 文件永远不会被修改。
5. 如果适用，前缀和后缀过程会自动为相关组件名称添加前缀或后缀。例如，如果计算机目录名称以“East”作为前缀，则引用这些名称的交付组也会以“East”作为前缀。
6. 如果组件名称以前缀或后缀开头，则不会添加前缀或后缀。组件名称不能包含两个相同的前缀或后缀。
7. 前缀和后缀可以单独使用，也可以组合使用。
8. 在组件上使用前缀或后缀是可选的。

注意：

完整配置界面按字母顺序显示组件。

### 按站点分组

使用前缀可以直观地对单个站点中的组件进行分组。每个站点都在自己的组中列出，前缀按字母顺序控制不同站点组的顺序。

### 按名称分组

使用后缀可以直观地对来自多个站点的类似命名组件进行分组。来自不同站点的类似命名组件看上去会交替使用。

### SitePrefixes.yml 文件

站点前缀从包含一个或多个本地站点的站点前缀和后缀映射的 `SiteMerging.yml` 文件开始。可以手动管理 `SiteMerging.yml` 文件，也可以使用[合并多个本地站点 cmdlet](#) 部分中列出的可用 cmdlet 来管理 `SiteMerging.yml` 文件。

## 导出、导入、合并和添加

合并在导出本地站点之后才能开始进行。要导出本地站点，请参阅[从本地迁移到云](#)。

## 中央导出目标文件夹

本部分中介绍的方法可将多个站点导出放置到一个中央文件共享位置。SiteMerging.yml 文件、CustomerInfo.yml 文件和所有导出文件都位于该文件共享位置，允许您从独立于本地站点的一个位置进行导入。

云访问操作永远不会引用本地站点或 Active Directory，因此允许您从任何位置执行云访问操作。

## 直接文件共享

导出、导入、合并和新建/添加操作提供了一个参数，用于定位或获取默认文件夹 %HOMEPATH%\Documents\Citrix\AutoConfig 以外的文件夹。以下示例使用 \\share.central.net 下管理员已有权访问的中央文件共享，并根据需要提供了凭据。

要将导出定位到特定于站点的文件夹，请使用 -TargetFolder 参数：

来自 East DDC：

```
mkdir \\share.central.net\AutoConfig\SiteEast  
Export-CvadaToFile -TargetFolder \\share.central.net\AutoConfig\SiteEast
```

来自 West DDC：

```
mkdir \\share.central.net\AutoConfig\SiteWest  
Export-CvadaToFile -TargetFolder \\share.central.net\AutoConfig\SiteWest
```

导出完成后，创建 CustomerInfo.yml 和 SiteMerging.yml 文件并将其放置在 \\share.central.net\AutoConfig 中。

### 注意：

使用此直接文件共享引用方法时，创建 SitePrefixes.yml 时请勿使用 SiteRootFolder 参数。

要从直接文件共享导入、合并或添加，您必须决定要从哪台计算机执行云访问操作。选项包括：

- 已安装该工具的其中一个本地 DDC。
- 托管文件共享的计算机。
- 另一台计算机。

自动配置必须安装在访问云的计算机上。本地 PowerShell SDK、DDC 和 Active Directory 均未使用，因此云访问执行要求比导出要求简单。

要将 East DDC 合并到云，请执行以下操作：

```
Merge-CvadAcToSite -SiteName East -SourceFolder \\share.central.net\AutoConfig\SiteEast -CustomerInfoFileSpec \\share.central.net\AutoConfig\CustomerInfo.yml
```

要将 West DDC 合并到云，请执行以下操作：

```
Merge-CvadAcToSite -SiteName West -SourceFolder \\share.central.net\AutoConfig\SiteWest -CustomerInfoFileSpec \\share.central.net\AutoConfig\CustomerInfo.yml
```

下面是上一个示例中使用的 SitePrefixes.yml 文件示例。

```
1      East:
2          SiteRootFolder: "" # Important: leave this empty
3          AdminScopePrefix: "East_"
4          AdminRolePrefix: "East_"
5          ApplicationAdminPrefix: "East_"
6          ApplicationFolderPrefix: "" # Note that a new parent root folder
           is used instead
7          ApplicationFolderRoot: "East"
8          ApplicationGroupPrefix: "East_"
9          ApplicationUserPrefix: "East_"
10         DeliveryGroupPrefix: "East_"
11         GroupPolicyPrefix: "East_"
12         HostConnectionPrefix: "East_"
13         MachineCatalogPrefix: "East_"
14         StoreFrontPrefix: "East_"
15         TagPrefix: "East_"
16         AdminScopeSuffix: "_east"
17         AdminRoleSuffix: "_east"
18         ApplicationAdminSuffix: "_east"
19         ApplicationFolderSuffix: "_east"
20         ApplicationGroupSuffix: "_east"
21         ApplicationUserSuffix: "_east"
22         DeliveryGroupSuffix: "_east"
23         GroupPolicySuffix: "_east"
24         HostConnectionSuffix: "_east"
25         MachineCatalogSuffix: "_east"
26         StoreFrontSuffix: "_east"
27         TagSuffix: "_east"
28     West:
29         SiteRootFolder: "" # Important: leave this empty
30         AdminScopePrefix: "Western "
31         AdminRolePrefix: "Western "
32         ApplicationAdminPrefix: "Western "
33         ApplicationFolderPrefix: "" # Note that a new parent root folder
           is used instead
34         ApplicationFolderRoot: "Western"
```

```
35     ApplicationGroupPrefix: "Western "  
36     ApplicationUserPrefix: "Western "  
37     DeliveryGroupPrefix: "Western "  
38     GroupPolicyPrefix: "Western "  
39     HostConnectionPrefix: "Western "  
40     MachineCatalogPrefix: "Western "  
41     StoreFrontPrefix: "Western "  
42     TagPrefix: "Western "  
43     AdminScopeSuffix: ""  
44     AdminRoleSuffix: ""  
45     ApplicationAdminSuffix: ""  
46     ApplicationFolderSuffix: ""  
47     ApplicationGroupSuffix: ""  
48     ApplicationUserSuffix: ""  
49     DeliveryGroupSuffix: ""  
50     GroupPolicySuffix: ""  
51     HostConnectionSuffix: ""  
52     MachineCatalogSuffix: ""  
53     StoreFrontSuffix: ""  
54     TagSuffix: ""
```

### 使用 **SiteMerging.yml** 的文件共享参考

此方法使用站点的前缀集的 **SiteRootFolder** 成员。虽然这种方法比直接文件共享方法参与度更高，但它可以降低导出、导入、合并或添加时以错误文件夹为目标的可能性。

首先，为 **SiteMerging.yml** 文件中的每个站点设置 **SiteRootFolder**。必须在共享位置执行此操作。

```
New-CvadaSiteMergingInfo -SiteName East -SiteRootFolder \\share.  
central.net\AutoConfig\SiteEast -SitePrefixesFolder \\share.central.  
net\AutoConfig
```

```
New-CvadaSiteMergingInfo -SiteName West -SiteRootFolder SiteWest -  
SitePrefixesFolder \\share.central.net\AutoConfig
```

在此示例中，East 为完全限定的文件夹规范，West 为相对文件夹规范。

要使用 **SiteMerging.yml** 文件将导出定位到特定于站点的文件夹，请执行以下操作：

来自 East DDC：

```
mkdir \\share.central.net\AutoConfig\SiteEast  
Export-CvadaToFile -SiteName East -CustomerInfoFileSpec \\share.  
central.net\AutoConfig\CustomerInfo.yml
```

来自 West DDC：

```
mkdir \\share.central.net\AutoConfig\SiteWest  
Export-CvadaToFile -SiteName West -CustomerInfoFileSpec \\share.  
central.net\AutoConfig\CustomerInfo.yml
```

导出 cmdlet 使用 CustomerInfo.yml 文件夹位置来查找 SiteMerging.yml 文件。就 East 而言，SiteRootFolder 是完全限定的规范。它按原样使用。就 West 而言，SiteRootFolder 不是完全限定的规范。它与 CustomerInfo.yml 文件夹位置相结合，以检索 West 的完全限定文件夹位置。

要将 East DDC 合并到云，请执行以下操作：

```
Merge-CvadAcToSite -SiteName East -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

要将 West DDC 合并到云，请执行以下操作：

```
Merge-CvadAcToSite -SiteName West -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

下面是上一个示例中使用的 SitePrefixes.yml 文件示例。

```
1      East:
2      SiteRootFolder: "\\share.central.net\AutoConfig\SiteEast"
3      AdminScopePrefix: "East_"
4      AdminRolePrefix: "East_"
5      ApplicationAdminPrefix: "East_"
6      ApplicationFolderPrefix: "" # Note that a new parent root folder
   is used instead
7      ApplicationFolderRoot: "East"
8      ApplicationGroupPrefix: "East_"
9      ApplicationUserPrefix: "East_"
10     DeliveryGroupPrefix: "East_"
11     GroupPolicyPrefix: "East_"
12     HostConnectionPrefix: "East_"
13     MachineCatalogPrefix: "East_"
14     StoreFrontPrefix: "East_"
15     TagPrefix: "East_"
16     AdminScopeSuffix: "_east"
17     AdminRoleSuffix: "_east"
18     ApplicationAdminSuffix: "_east"
19     ApplicationFolderSuffix: "_east"
20     ApplicationGroupSuffix: "_east"
21     ApplicationUserSuffix: "_east"
22     DeliveryGroupSuffix: "_east"
23     GroupPolicySuffix: "_east"
24     HostConnectionSuffix: "_east"
25     MachineCatalogSuffix: "_east"
26     StoreFrontSuffix: "_east"
27     TagSuffix: "_east"
28     West:
29     SiteRootFolder: "\\share.central.net\AutoConfig\SiteWest"
30     AdminScopePrefix: "Western "
31     AdminRolePrefix: "Western "
32     ApplicationAdminPrefix: "Western "
33     ApplicationFolderPrefix: "" # Note that a new parent root folder
   is used instead
34     ApplicationFolderRoot: "Western"
35     ApplicationGroupPrefix: "Western "
```



```
36     ApplicationUserPrefix: "Western "
37     DeliveryGroupPrefix: "Western "
38     GroupPolicyPrefix: "Western "
39     HostConnectionPrefix: "Western "
40     MachineCatalogPrefix: "Western "
41     StoreFrontPrefix: "Western "
42     TagPrefix: "Western "
43     AdminScopeSuffix: ""
44     AdminRoleSuffix: ""
45     ApplicationAdminSuffix: ""
46     ApplicationFolderSuffix: ""
47     ApplicationGroupSuffix: ""
48     ApplicationUserSuffix: ""
49     DeliveryGroupSuffix: ""
50     GroupPolicySuffix: ""
51     HostConnectionSuffix: ""
52     MachineCatalogSuffix: ""
53     StoreFrontSuffix: ""
54     TagSuffix: ""
```

如果未使用中央文件共享方法，而导入、合并或添加是从单个 DDC 完成的，则在每个要迁移到云的 DDC 上创建和复制 `SiteMerging.yml` 文件。默认位置为 `%HOMEPATH%\Documents\Citrix\AutoConfig`。必须指定 `- SiteName` 参数才能选择正确的站点前缀。

## 合并站点

Citrix 建议分步执行云操作，并在执行下一个云操作之前对每个结果进行全面审查。例如，如果将三个站点合并到单个云站点：

1. 使用适当的 `SiteName` 值将初始站点合并到云。
2. 在“完整配置”管理界面中查看结果。
3. 如果结果不正确，请确定问题及其原因，更正，然后重新运行合并。如有必要，请删除云组件，然后使用 `Remove-CvadAcFromSite` 为选定的组件和成员从头开始执行操作。如果结果正确，则请继续。
4. 如果初始合并正确，则将第二个站点合并到单个云站点。
5. 重复步骤 2 和 3。
6. 如果第二次合并正确，则将第三个站点合并到单个云站点。
7. 重复步骤 2 和 3。
8. 从用户的角度查看资源并验证视图是否处于所需状态。

## 使用站点前缀删除组件

可以通过使用 `Remove-CvadAcFromSite` cmdlet 的 `- IncludeByName` 参数上的前缀有选择地删除单个站点组件。在以下示例中，West DDC 交付组不正确。要仅删除 West 站点的交付组，请执行以下操作：

```
Remove-CvadAcFromSite -DeliveryGroups -IncludeByName "Western *
```

要删除所有 West 组件，请按顺序运行以下 cmdlet。

```
Remove-CvadAcFromSite -GroupPolicies -IncludeByName "Western ★"
```

```
Remove-CvadAcFromSite -Applications -IncludeByName "Western ★"
```

```
Remove-CvadAcFromSite - ApplicationGroups -IncludeByName "Western ★"
```

```
Remove-CvadAcFromSite -DeliveryGroups -IncludeByName "Western ★"
```

```
Remove-CvadAcFromSite -MachineCatalogs -IncludeByName "Western ★"
```

```
Remove-CvadAcFromSite -HostConnections -IncludeByName "Western ★"
```

```
Remove-CvadAcFromSite -Tags -IncludeByName "Western ★"
```

要删除 East 组件的组策略，请使用后缀：

```
Remove-CvadAcFromSite -GroupPolicies -IncludeByName "★_east"
```

## 从云迁移到云

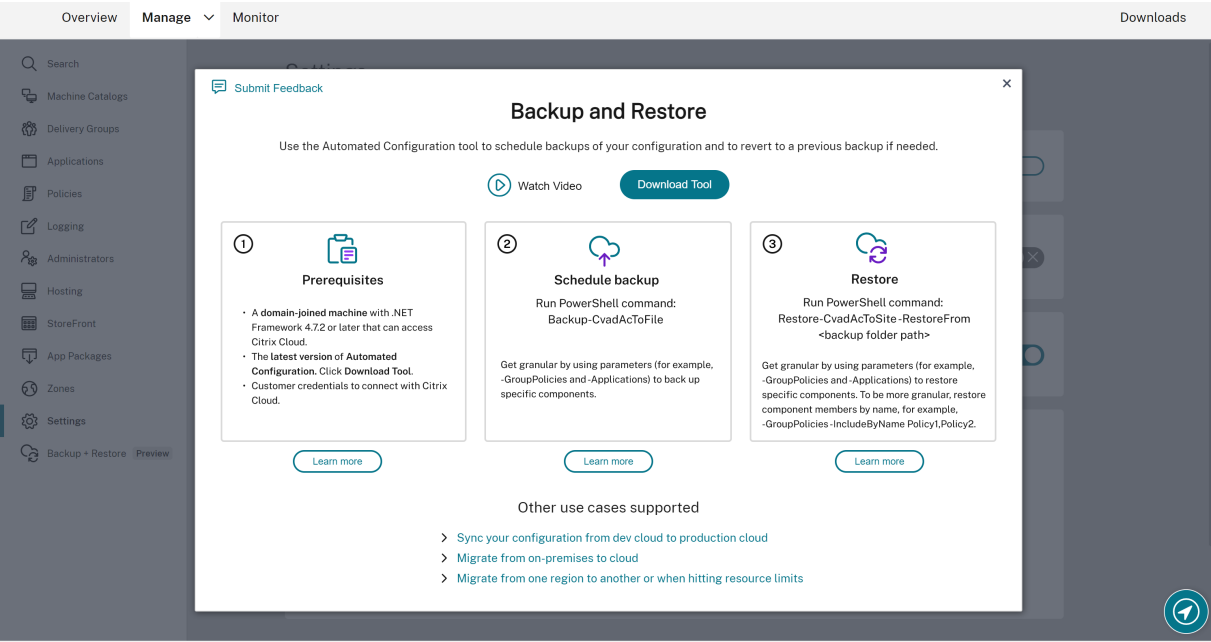
March 30, 2024

自动配置允许您自动将云配置移动到另一个云站点，或允许您还原自己的云站点。

使用自动配置可以解决许多用例：

- 将您的站点从测试或阶段同步到生产
- 备份和还原配置
- 达到资源限制
- 从一个区域迁移到另一个区域

在 Citrix Cloud 上的完整配置中，有关自动配置以及如何使用自动配置将配置从云迁移到云的信息，请参阅备份和还原节点。



迁移配置的必备条件

要备份和还原您的配置，您需要：

- 预配的 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）。
- 安装了 Connector 的活动资源位置。
- 必须允许并且可以连接到访问 Citrix Cloud 的站点。有关详细信息，请参阅[系统和连接要求](#)。

注意：

无法使用自动配置从云中备份 MCS。

备份 **Citrix DaaS** 配置

- 重要：
- 您必须附上您的 CustomerInfo.yml 文件以及您的客户 ID、客户端 ID 和密钥信息。有关如何检索客户 ID、客户端 ID 和密钥的详细信息，请参阅[生成客户 ID、客户端 ID 和密钥](#)。有关如何将这些信息添加到 CustomerInfo.yml 文件中的信息，请参阅[填充客户信息文件](#)。
  - ZoneMapping.yml 文件必须包含将资源区域映射到云中的信息。有关如何映射您的区域的详细信息，请参阅[填充区域映射文件](#)。
  - 如果您有主机连接，则必须在 CvadAcSecurity.yml 文件中输入相应的信息。

1. [安装自动配置](#)。

**注意：**

对于云到云的迁移，可以在管理员有权直接访问 Internet 的计算机上安装自动配置。

2. 双击自动配置图标。此时将显示 PowerShell 窗口。
3. 请运行以下命令以执行备份。

```
Backup-CvadAcToFile
```

首次运行任何 cmdlet 之后，系统将创建包含.yml 配置文件和日志的 export 文件夹。该文件夹位于 %HOMEPATH%\Documents\Citrix\AutoConfig 中。

如果您遇到任何错误或异常，请参阅日志文件中的 **Fixups** 部分。

### 将配置还原到 Citrix DaaS

1. 双击自动配置图标。此时将显示 PowerShell 窗口。
2. 请运行以下命令以执行还原。

```
Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
```

请使用新的当前状态来验证预期状态。

运行该 cmdlet 之后，系统将创建包含.yml 配置文件和日志的 export 文件夹。该文件夹位于 %HOMEPATH%\Documents\Citrix\AutoConfig 中。

如果您遇到任何错误或异常，请参阅日志文件中的 **Fixups** 部分。

备份和还原过程可保护您免受无意中的云站点配置更改或损坏的影响。虽然自动配置在每次进行更改时都会进行备份，但此备份反映了更改之前云站点配置的状态。保护自己需要定期备份云站点配置，并将其保存在一个安全的位置。如果发生了不希望的更改或损坏，备份可以用于在粒度或完整站点配置级别修复更改或损坏。

### 粒度迁移

**重要：**

有关组件迁移顺序的更多信息，请参阅[组件迁移顺序](#)。

### 还原整个组件

还原一个组件涉及选择一个或多个组件参数。

要还原整个交付组和计算机目录组件，请按照以下示例进行操作：

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig\Backup_yyyy_mm_dd_hh_mm_ss
```

## 还原组件成员

还原一个或多个组件成员将使用 `IncludeByName` 功能。`Restore cmdlet` 随 `RestoreFolder` 参数以及选定的单个组件和包含列表一起调用。

要从备份中还原两个组策略，请按照以下示例进行操作：

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
-GroupPolicies -IncludeByName Policy1,Policy2
-DeliveryGroups -MachineCatalogs
```

## 还原整个云站点配置

还原完整的云站点配置意味着选择要还原的所有组件。

要还原整个云站点配置，请按照以下示例进行操作：

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

## 激活站点

站点激活允许您控制处于活动状态的站点并控制您的资源。有关详细信息，请参阅[激活站点](#)。

## 自动配置工具 **cmdlet**

March 30, 2024

此页面列出了该工具支持的所有 `cmdlet` 和参数。

所有 `cmdlet` 都采用具有以下类型之一的参数。

- 字符串
- 字符串列表
- 布尔值：`$true` 或 `$false`
- SwitchParameter：存在参数表示 `$true`；缺少参数表示 `$false`

注意：

SwitchParameter 是选择 `true` 或 `false` 的首选方法，但是由于遗留问题，该工具中仍使用布尔值。

下表汇总了所有 cmdlet。请参阅每个单独的部分以了解每个 cmdlet 支持的参数。

类别	cmdlet	说明
本地到云迁移	<a href="#">Export-CvadAcToFile</a>	将本地文件导出为 YAML 文件。
	<a href="#">Import-CvadAcToSite</a>	
	<a href="#">Merge-CvadAcToSite</a>	
	<a href="#">New-CvadAcToSite</a>	
	<a href="#">Sync-CvadAcToSite</a>	
云到云 cmdlet		粒度迁移 对于组件，请在上面的命令中使用参数。示例： <a href="#">MachineCatalogs</a> 、 <a href="#">Tags</a> 。 对于组件名称，请在上面的命令中使用参数。示例： <a href="#">IncludeByName</a> 、 <a href="#">ExcludeByName</a> 。
	<a href="#">Backup-CvadAcToFile</a>	备份云站点中的所有配置。
	<a href="#">Restore-CvadAcToSite</a>	
	<a href="#">Remove-CvadAcFromSite</a>	
		粒度迁移 对于组件，请在上面的命令中使用参数。示例： <a href="#">MachineCatalogs</a> 、 <a href="#">Tags</a> 。 对于组件名称，请在上面的命令中使用参数。示例： <a href="#">IncludeByName</a> 、 <a href="#">ExcludeByName</a> 。
其他基本 cmdlet	<a href="#">Compare-CvadAcToSite</a>	将本地.yml 文件与云配置进行比较。
与必备条件有关的 cmdlet	<a href="#">New-CvadAcCustomerInfoFile</a>	创建客户信息文件。
		<a href="#">Set-CvadAcCustomerInfoFile</a>
支持和故障排除 cmdlet	<a href="#">New-CvadAcZipInfoForSupport</a>	将所有日志和.yml 文件压缩到单个 zip 文件中，以发送给 Citrix 以获得支持。

类别	cmdlet	说明
		<a href="#">Get-CvadAcStatus</a>
		<a href="#">Test-CvadAcConnectionWithSite</a>
		<a href="#">Find-CvadAcConnector</a>
		<a href="#">Get-CvadAcCustomerSites</a>
		<a href="#">New-CvadAcTemplateToFile</a>
		<a href="#">Show-CvadAcDocument</a>
		<a href="#">Find-CvadAcInFile</a>
站点激活 cmdlet	<a href="#">Set-CvadAcSiteActiveStateOnPrem</a>	将本地站点状态设置为活动或非活动状态。
		<a href="#">Set-CvadAcSiteActiveStateCloud</a>
合并多个本地站点 cmdlet	<a href="#">New-CvadAcSiteMergingInfo</a>	创建一个合并前缀/后缀信息集的站点。
		<a href="#">Set-CvadAcSiteMergingInfo</a>
		<a href="#">Remove-CvadAcSiteMergingInfo</a>

有关参数及其使用方法的详细信息，请参阅粒度迁移参数。

基本 cmdlet

本地到云 cmdlet

- [Export-CvadAcToFile](#) - 将本地文件导出为 YAML 文件。  
导出本地设置中的配置。这是自动配置的默认导出操作。不对本地站点配置进行任何修改。导出的文件将放置在位于命名的导出子文件夹的目录 `%HOMEPATH%\Documents\Citrix\AutoConfig` 中。文件夹

`%HOMEPATH%\Documents\Citrix\AutoConfig` 始终包含最新导出的本地站点配置。

参数：

名称	说明	必需？	类型
按组件迁移	请参阅按组件迁移		SwitchParameters
按对象名称过滤	请参阅按对象名称过滤		字符串列表
<code>TargetFolder</code>	指定导出目标文件夹。		字符串
<code>Locale</code>	指定可以导出的人类可读文本的语言。		字符串
<code>Quiet</code>	禁止登录控制台。		SwitchParameter
<code>AdminAddress</code>	在 Delivery Controller 上未运行导出时，指定 Delivery Controller 的 DNS 或 IP 地址。		字符串
<code>CheckUserAndMachine</code>	验证用户和计算机是否在 Active Directory 中。不在 Active Directory 中的用户和计算机可能会导致导入失败。		<code>\$true</code> 或 <code>\$false</code>
<code>ZipResults</code>	将备份 YAML 文件压缩到单个 zip 文件中。该文件与备份的 YAML 文件位于同一文件夹中，并且与文件夹具有相同的名称。		SwitchParameter

返回结果：

- 请参阅 Cmdlet 返回值

有三种方法可以将数据导入到云中。运行特定的 cmdlet 可能会导致云站点上出现三种操作组合之一：

- 添加、更新和删除
- 仅添加和更新
- 仅添加

cmdlet	添加	更新	删除
导入	X	X	X
合并	X	X	
新建	X		

- `Import-CvadaToSite` - 将 YAML 文件导入云中。支持创建、更新和删除操作。

将所有本地文件导入到云端。此命令可确保云端状态与本地状态相同。此选项将删除云中存在的所有更改。导入的站点配置文件来自 `%HOMEPATH%\Documents\Citrix\AutoConfig`。请小心使用。



参数：

名称	说明	必需?	类型
按组件迁移	请参阅按组件迁移。		SwitchParameters
按对象名称过滤	请参阅按对象名称筛选。		字符串列表
云访问参数	请参阅云访问参数。		SwitchParameters
SourceFolder	标识 %HOMEPATH%\Documents\Citrix\AutoConfig 的替代根文件夹。		字符串
Locale	指定可以导出的人类可读文本的语言。		字符串
Quiet	禁止登录控制台。		SwitchParameter
DisplayLog	在 cmdlet 完成时显示日志文件。设置为 \$false 将禁止日志显示。		\$true 或 \$false
Merge	设置为 \$true 时，仅向云站点添加组件。组件不会被删除。设置为 \$false 将删除组件。		\$true 或 \$false
AddOnly	设置为 \$true 时，仅添加新组件，不会更新或删除现有组件。设置为 \$false 将允许更新和删除。当此参数为 \$true 时，将忽略 Merge。		\$true 或 \$false
MergePolicies	合并策略设置和过滤器。仅当正在导入的策略已存在于云 DDC 中时，才会进行合并。合并策略的结果是，除了导入的任何新设置和过滤器外，云端 DDC 策略还包含其已有的设置和过滤器。请注意，当发生设置和过滤器冲突时，导入的值优先。		SwitchParameter
OnErrorAction	请参阅 OnErrorAction 参数。		字符串

返回结果：

- 请参阅 Cmdlet 返回值

- Merge-CvadaCToSite - 将 YAML 文件导入云中。支持创建和更新操作。

将本地文件合并到云端，但不删除云中或本地站点中的任何组件。这将保留已在云中进行的更改。如果 Citrix Cloud 中存在同名组件，此命令可以修改该组件。这是自动配置的默认导入操作。合并的站点配置文件来自 %HOMEPATH%\Documents\Citrix\AutoConfig。

参数：

名称	说明	必需?	类型
按组件迁移	请参阅按组件迁移。		SwitchParameters

名称	说明	必需?	类型
按对象名称过滤	请参阅按对象名称筛选。		字符串列表
云访问参数	请参阅云访问参数。		SwitchParameters
SourceFolder	标识 %HOMEPATH%\Documents\Citrix\AutoConfig 的替代根文件夹。		字符串
Locale	指定可以导出的人类可读文本的语言。		字符串
Quiet	禁止登录控制台。		SwitchParameter
DisplayLog	在 cmdlet 完成时显示日志文件。设置为 <code>\$false</code> 将禁止日志显示。		<code>\$true</code> 或 <code>\$false</code>
Merge	设置为 <code>\$true</code> 时，仅向云站点添加组件。组件不会被删除。设置为 <code>\$false</code> 将删除组件。		<code>\$true</code> 或 <code>\$false</code>
AddOnly	设置为 <code>\$true</code> 时，仅添加新组件，不会更新或删除现有组件。设置为 <code>\$false</code> 将允许更新和删除。当此参数为 <code>\$true</code> 时，将忽略 <code>Merge</code> 。		<code>\$true</code> 或 <code>\$false</code>
MergePolicies	合并策略设置和过滤器。仅当正在导入的策略已存在于云 DDC 中时，才会进行合并。合并策略的结果是，除了导入的任何新设置和过滤器外，云端 DDC 策略还包含其已有的设置和过滤器。请注意，当发生设置和过滤器冲突时，导入的值优先。		SwitchParameter
OnErrorAction	请参阅 <a href="#">OnErrorAction</a> 参数。		字符串

返回结果：

- 请参阅 Cmdlet 返回值
- [New-CvadAcToSite](#) - 将 YAML 文件导入云中。支持创建和更新操作。

将本地站点配置导入到云端，但仅添加新组件。现有云站点组件既不会更新，也不会删除。如果现有云站点组件必须保持不变，请使用此命令。

参数：

名称	说明	必需?	类型
按组件迁移	请参阅按组件迁移。		SwitchParameters
按对象名称过滤	请参阅按对象名称筛选。		字符串列表
云访问参数	请参阅云访问参数。		SwitchParameters

名称	说明	必需?	类型
SourceFolder	标识 %HOMEPATH%\Documents\Citrix\AutoConfig 的替代根文件夹。		字符串
Locale	指定可以导出的人类可读文本的语言。		字符串
Quiet	禁止登录控制台。		SwitchParameter
DisplayLog	在 cmdlet 完成时显示日志文件。设置为 <code>\$false</code> 将禁止日志显示。		<code>\$true</code> 或 <code>\$false</code>
OnErrorAction	请参阅 <a href="#">OnErrorAction</a> 参数。		字符串

返回结果：

- 请参阅 Cmdlet 返回值
  - [Sync-CvadAcToSite](#) - 在一个步骤中完成导出和导入操作。
- Sync 在一个步骤中同时执行导出和导入。使用 [SourceTargetFolder](#) 参数指定导出/导入目标文件夹。

参数：

名称	说明	必需?	类型
按组件迁移	请参阅按组件迁移		SwitchParameters
按对象名称过滤	请参阅按对象名称过滤		字符串列表
云访问参数	请参阅云访问参数		SwitchParameters
<a href="#">SourceTargetFolder</a>	指定导出/导入目标文件夹。		字符串
Locale	指定可以导出的人类可读文本的语言。		字符串
AdminAddress	在 Delivery Controller 上未运行导出时，指定 Delivery Controller 的 DNS 或 IP 地址。		字符串
Quiet	禁止登录控制台。		SwitchParameter
DisplayLog	在 cmdlet 完成时显示日志文件。设置为 <code>\$false</code> 将禁止日志显示。		<code>\$true</code> 或 <code>\$false</code>
Merge	设置为 <code>\$true</code> 时，仅向云站点添加组件。组件不会被删除。设置为 <code>\$false</code> 将删除组件。		<code>\$true</code> 或 <code>\$false</code>
AddOnly	设置为 <code>\$true</code> 时，仅添加新组件，不会更新或删除现有组件。设置为 <code>\$false</code> 将允许更新和删除。当此参数为 <code>\$true</code> 时，将忽略 <a href="#">Merge</a> 。		<code>\$true</code> 或 <code>\$false</code>

名称	说明	必需?	类型
MergePolicies	合并策略设置和过滤器。仅当正在导入的策略已存在于云 DDC 中时，才会进行合并。合并策略的结果是，除了导入的任何新设置和过滤器外，云端 DDC 策略还包含其已有的设置和过滤器。请注意，当发生设置和过滤器冲突时，导入的值优先。		SwitchParameter

返回结果：

- 请参阅 Cmdlet 返回值

云到云 cmdlet

- Backup-CvadAcToFile - 备份云站点中的所有配置。

将云配置导出到.yml 文件。此备份可以在备份和还原过程中用来还原丢失的组件。

参数：

名称	说明	必需?	类型
按组件迁移	请参阅按组件迁移		SwitchParameters
云访问参数	请参阅云访问参数		SwitchParameters
TargetFolder	指定导出目标文件夹。		字符串
Locale	指定可以导出的人类可读文本的语言。		字符串
Quiet	禁止登录控制台。		SwitchParameter
DisplayLog	在 cmdlet 完成时显示日志文件。设置为 \$false 将禁止日志显示。		\$true 或 \$false
ZipResults	将备份 YAML 文件压缩到单个 zip 文件中。该文件与备份的 YAML 文件位于同一文件夹中，并且与文件夹具有相同的名称。		SwitchParameter

返回结果：

- 请参阅 Cmdlet 返回值

- Restore-CvadAcToSite - 将备份 YAML 文件还原到云站点。此云站点可以与源云站点相同，也可以不同。

将云站点还原到之前的配置。导入的文件来自使用 `-RestoreFolder` 参数指定的文件夹，该参数标识包含要还原到云站点的.yml 文件的文件夹。这必须是完全限定的文件夹规范。此 cmdlet 可用于还原到之前的配置或用于对云站点进行备份和还原。此命令可以添加、删除和更新您的云站点。

参数：

名称	说明	必需?	类型
按组件迁移	请参阅按组件迁移。		SwitchParameters
按对象名称过滤	请参阅按对象名称筛选。		字符串列表
云访问参数	请参阅云访问参数。		SwitchParameters
<code>RestoreFolder</code>	标识包含要还原到云站点的.yml 文件的文件夹。这必须是完全限定的文件夹规范。		字符串
<code>Locale</code>	指定可以导出的人类可读文本的语言。		字符串
<code>Quiet</code>	禁止登录控制台。		SwitchParameter
<code>DisplayLog</code>	在 cmdlet 完成时显示日志文件。设置为 <code>\$false</code> 将禁止日志显示。		<code>\$true</code> 或 <code>\$false</code>
<code>Merge</code>	设置为 <code>\$true</code> 时，仅向云站点添加组件。组件不会被删除。设置为 <code>\$false</code> 将删除组件。		<code>\$true</code> 或 <code>\$false</code>
<code>AddOnly</code>	设置为 <code>\$true</code> 时，仅添加新组件，不会更新或删除现有组件。设置为 <code>\$false</code> 将允许更新和删除。当此参数为 <code>\$true</code> 时，将忽略 <code>Merge</code> 。		<code>\$true</code> 或 <code>\$false</code>
<code>MergePolicies</code>	合并策略设置和过滤器。仅当正在导入的策略已存在于云 DDC 中时，才会进行合并。合并策略的结果是，除了导入的任何新设置和过滤器外，云端 DDC 策略还包含其已有的设置和过滤器。请注意，当发生设置和过滤器冲突时，导入的值优先。		SwitchParameter
<code>OnErrorAction</code>	请参阅 <code>OnErrorAction</code> 参数。		字符串

返回结果：

- 请参阅 Cmdlet 返回值
  - `Remove-CvadAcFromSite` - 从云中删除组件成员。
- 可以重置整个站点或删除组件中的成员项 (例如，从目录列表中删除一个计算机目录)。当与 `IncludeByName` 参数结合使用以选择性地删除特定成员时，可以使用此命令。

参数：

名称	说明	必需?	类型
按组件迁移	请参阅按组件迁移		SwitchParameters
按对象名称过滤	请参阅按对象名称过滤		字符串列表
云访问参数	请参阅云访问参数		SwitchParameters
Quiet	禁止登录控制台。		SwitchParameter
DisplayLog	在 cmdlet 完成时显示日志文件。设置为 <code>\$false</code> 将禁止日志显示。		<code>\$true</code> 或 <code>\$false</code>

返回结果：

- 请参阅 Cmdlet 返回值

其他基本 **cmdlet**

- **Compare-CvadaCtoSite** - 将本地.yml 文件与云配置进行比较,生成 **Import**、**Merge** 或 **Restore** cmdlet 所做的更改的报告。

参数：

名称	说明	必需?	类型
按组件迁移	请参阅按组件迁移。		SwitchParameters
按对象名称过滤	请参阅按对象名称筛选。		字符串列表
云访问参数	请参阅云访问参数。		SwitchParameters
SourceFolder	标识 <code>%HOMEPATH%\Documents\Citrix\AutoConfig</code> 的替代根文件夹。		字符串
Locale	指定可以导出的人类可读文本的语言。		字符串
Quiet	禁止登录控制台。		SwitchParameter
DisplayLog	在 cmdlet 完成时显示日志文件。设置为 <code>\$false</code> 将禁止日志显示。		<code>\$true</code> 或 <code>\$false</code>
Merge	设置为 <code>\$true</code> 时，仅向云站点添加组件。组件不会被删除。设置为 <code>\$false</code> 将删除组件。		<code>\$true</code> 或 <code>\$false</code>
AddOnly	设置为 <code>\$true</code> 时，仅添加新组件，不会更新或删除现有组件。设置为 <code>\$false</code> 将允许更新和删除。当此参数为 <code>\$true</code> 时，将忽略 <b>Merge</b> 。		<code>\$true</code> 或 <code>\$false</code>
OnErrorAction	请参阅 <b>OnErrorAction</b> 参数。		字符串

返回结果：

- 请参阅 Cmdlet 返回值

## 粒度迁移参数

### 按组件迁移

以下组件可以使用支持这些组件的 cmdlet 来指定。未指定组件参数时，`All` 选项将自动选择。为避免错误，我们建议您按以下顺序迁移组件：

- `All`
- `Tags`
- `AdminRoles`
- `AdminScopes`
- `HostConnections`
- `MachineCatalogs`
- `StoreFronts`
- `DeliveryGroups`
- `ApplicationGroups`
- `ApplicationFolders`
- `Applications`
- `GroupPolicies`
- `UserZonePreference`

### 按对象名称过滤

**按组件名称迁移** `IncludeByName` 和 `ExcludeByName` 参数允许按名称在 cmdlet 中包含和排除组件成员。在任何受支持的 cmdlet 中，一次只能选择一个组件（例如，交付组）。如果组件成员在这两个区域中，排除操作将覆盖任何其他参数，并且日志修复列表中新增一个条目，以标识排除的组件和成员名称。

`IncludeByName` 和 `ExcludeByName` 将获取组件成员名称的列表。任何名称都可以包含一个或多个通配符。支持两种类型的通配符。当任何成员名称包含特殊字符时，组件成员名称列表必须用单引号引起。

- \* 匹配任意数量的字符
- ? 匹配单个字符

`IncludeByName` 和 `ExcludeByName` 也可以获取包含成员列表的文件，其中每个成员都可以是直接显示的或包含通配符。该文件中的每一行都可以包含一个成员。前导空格和尾随空格将自动从成员名称中去掉。文件名前面必须带有 @ 符号，并且用单引号括起来（这是 PowerShell 的要求，因此不会重新解释 @）。除了与成员名称混用之外，还可以列出多个文件。

将写入合并名称以 `DgSite1` 开头且包含 `Home2` 的所有交付组的一个示例：

```
Merge-CvadAcToSite -DeliveryGroups -IncludeByName DgSite1*,*Home2*
```

按交付组名称 `ByDeliveryGroupName` 按应用程序和应用程序组的交付组名称进行筛选。此参数始终是一个包含列表，根据其交付组关联标识要包括的成员。

`ByDeliveryGroupName` 获取交付组名称的列表。任何名称都可以包含一个或多个通配符。支持两种类型的通配符。

- `*` 匹配任意数量的字符
- `?` 匹配单个字符

以下示例合并引用以 `EastDg` 开头的所有交付组名称的所有应用程序。

```
Merge-CvadAcToSite -Applications -ByDeliveryGroupName EastDg*
```

排除已禁用 `ExcludeDisabled` 从导入操作中筛选出禁用的所有应用程序和应用程序组。`ExcludeDisabled` 默认设置为 **false**，这意味着无论其启用状态如何，所有应用程序和应用程序组都会导入。

按计算机名称 `ByMachineName` 按计算机目录和交付组的计算机名称进行筛选。此参数始终是一个包含列表，根据其计算机名称关联标识要包括的成员。

`ByMachineName` 获取计算机名称列表，其中任何名称都可以包含一个或多个通配符。支持两种类型的通配符。

- `*` 匹配任意数量的字符
- `?` 匹配单个字符

使用 `ByMachineName` 导出或导入，并且计算机名称过滤器导致计算机目录或交付组中没有计算机时，计算机目录或交付组将从导出或导入中排除。

注意：

在任何导入类型 cmdlet 中使用 `ByMachineName` 都会导致 `MergeMachines` 设置为 `$true`。

合并计算机 `MergeMachines`，设置为 `$true` 时，指示导入操作仅将计算机添加到计算机目录或交付组。计算机不会被删除，允许进行增量添加操作。

`MergeMachines` 默认设置为 `false`，表示如果计算机目录或交付组.yml 文件中不存在计算机，则将删除计算机。使用 `ByMachineName` 时，`MergeMachines` 设置为 `$true`，但可以通过将 `MergeMachines` 设置为 `false` 进行覆盖。



与必备条件有关的 **cmdlet**

- **New-CvadAcCustomerInfoFile** - 创建客户信息文件。默认情况下，客户信息文件位于 `%HOMEPATH%\Documents\Citrix\AutoConfig` 下。

参数：

名称	说明	必需？	类型
<b>CustomerId</b>	客户的 ID。	x	字符串
<b>ClientId</b>	在 Citrix Cloud 上创建的客户的客户端 ID。使用此参数时，必须指定 CustomerId 和密钥。	有条件地	字符串
<b>Secret</b>	在 Citrix Cloud 上创建的客户的密钥。使用此参数时，必须指定 CustomerId 和 ClientId。	有条件地	字符串
<b>Environment</b>	Production、ProductionGov 或 ProductionJP 环境。		枚举
<b>LogFileName</b>	将日志文件前缀从 CitrixLog 更改为其他内容。		字符串
<b>AltRootUrl</b>	只能在 Citrix 的指导下使用。		字符串
<b>StopOnError</b>	第一次出现错误时停止操作。		<code>\$true</code> 或 <code>\$false</code>
<b>TargetFolder</b>	使用指定的文件夹作为根文件夹，代替 <code>%HOMEPATH%\Documents\Citrix\AutoConfig</code> 。		字符串
<b>Locale</b>	使用指定的本地设置，而非从运行该工具的系统派生的区域设置。		字符串
<b>Editor</b>	使用指定的编辑器在每个 cmdlet 完成时显示日志。Notepad.exe 为默认编辑器。此参数必须在编辑器中包含完全限定的文件规范，编辑器必须将日志文件规范作为其唯一的参数。		字符串
<b>SecurityCsvFilePath</b>	指向从 Citrix Identity and Access Management 下载的 SecurityClient.csv 文件的完全限定文件规范。使用此参数时必须指定 CustomerId。		字符串

返回结果：

- 请参阅 Cmdlet 返回值
- **Set-CvadAcCustomerInfoFile** - 更新现有的客户信息文件。只有 cmdlet 指定的参数会被更改。CustomerInfo.yml 文件中所有未指定的参数值都保持不变。

参数：

名称	说明	必需？	类型
CustomerId	客户的 ID。		字符串
ClientId	在 Citrix Cloud 上创建的客户的客户端 ID。		字符串
Secret	在 Citrix Cloud 上创建的客户的密钥。		字符串
Environment	Production、ProductionGov 或 ProductionJP 环境。		枚举
LogFileName	将日志文件前缀从 CitrixLog 更改为其他内容。		字符串
StopOnError	第一次出现错误时停止操作。		\$true 或 \$false
TargetFolder	使用指定的文件夹作为根文件夹，代替 %HOMEPATH%\Documents\Citrix\AutoConfig。		字符串
Locale	使用指定的本地设置，而非从运行该工具的系统派生的区域设置。		字符串
Editor	使用指定的编辑器在每个 cmdlet 完成时显示日志。Notepad.exe 为默认编辑器。此参数必须在编辑器中包含完全限定的文件规范，编辑器必须将日志文件规范作为其唯一的参数。		字符串
SecurityCsvFilePath	指向从 Citrix Identity and Access Management 下载的 SecurityClient.csv 文件的完全限定文件规范。使用此参数时必须指定 CustomerId。		字符串

返回结果：

- 请参阅 Cmdlet 返回值

与必备条件有关的参数

除了云访问参数外，以下参数还可以与必备条件相关的 cmdlet 一起使用：

- **Environment** - 生产或生产管控环境。
- **LogFileName** - 将 CitrixLog 日志文件前缀更改为其他内容。
- **StopOnError** - 第一次出现错误时停止操作。
- **AlternateRootFolder** - 使用指定的文件夹作为根文件夹，代替 %HOMEPATH%\Documents\Citrix\AutoConfig。
- **Locale** - 使用指定的本地设置，而非从运行该工具的系统派生的区域设置。
- **Editor** - 使用指定的编辑器在每个 cmdlet 完成时显示日志。Notepad.exe 为默认编辑器。此参数必须在编辑器中包含完全限定的文件规范，编辑器必须将日志文件规范作为其唯一的参数。

支持和故障排除 **cmdlet**

- **New-CvadAcZipInfoForSupport** - 将所有日志和.yml 文件压缩到单个 zip 文件中，以发送给 Citrix 以获得支持。客户敏感信息 (CustomerInfo.yml 和 CvadAcSecurity.yml) 不包含在 zip 文件中。Icon.yml 文件也因其大小而被排除在外。zip 文件根据日期和时间戳放置在 %HOMEPATH%\Documents\Citrix\AutoConfig 中，名称为 CvadAcSupport\_yyyy\_mm\_dd\_hh\_mm\_ss.zip。此 zip 文件也可以作为备份。

参数：

名称	说明	必需？	类型
<b>TargetFolder</b>	指定要创建和保存 zip 文件的目标文件夹。		字符串
<b>Quiet</b>	禁止登录控制台。		SwitchParameter

返回结果：

- 命令提示符下会显示带有 zip 文件名和位置的 zip 文件。
- **Get-CvadAcStatus** - 用于测试连接并确保满足所有必备条件。返回有关该工具的信息，例如版本号、与云的连接以及连接器状态。

参数：

名称	说明	必需？	类型
云访问参数	请参阅云访问参数		SwitchParameters
<b>SiteId</b>	标识要连接到的站点。		字符串
<b>AdminAddress</b>	这是用于验证管理员访问级别的本地 Delivery Controller 的 DNS 或 IP 地址。如果该工具不在 Delivery Controller 上运行，则此操作是必需的。		字符串

返回结果：

- 显示每个项目的结果。
- **Test-CvadAcConnectionWithSite** - 测试与云站点的连接以验证通信连接是否正常工作。此 cmdlet 使用云访问参数或 CustomerInfo.yml 文件来指定客户连接信息。

参数：

名称	说明	必需?	类型
云访问参数	请参阅云访问参数		SwitchParameters
<a href="#">Quiet</a>	禁止登录控制台。		SwitchParameter

返回结果：

- 测试结果将显示在命令行上。
- [Find-CvadAcConnector](#) - 查找现有连接器并确定其运行状态。此 cmdlet 使用 CustomerInfo.yml 文件中的信息或客户 ID 参数来查找客户的连接器。

参数：

名称	说明	必需?	类型
<a href="#">CustomerInfoFilePath</a>	指向客户信息文件以覆盖默认位置和名称的文件规范。提供了 <a href="#">CustomerId</a> 参数时，此参数将被忽略。		字符串
<a href="#">CustomerId</a>	客户的 ID。此参数将覆盖 CustomerInfo.yml 文件中的相同值。		字符串

返回结果：

- 结果显示在命令行中。
- [Get-CvadAcCustomerSites](#) - 返回所有客户站点的列表。此 cmdlet 使用云访问参数或 Customer-Info.yml 文件来指定客户连接信息。

参数：

- 请参阅云访问参数

返回结果：

- 显示找到的客户地点 ID 的列表。
- [New-CvadAcTemplateToFile](#) - 为选定组件创建模板文件，以便手动创建导入文件。

参数：

名称	说明	必需?	类型
按组件迁移	请参阅按组件迁移		SwitchParameters
<a href="#">TargetFolder</a>	指定导出目标文件夹。		字符串

名称	说明	必需?	类型
----	----	-----	----

返回结果：

- 请参阅 Cmdlet 返回值
- [Show-CvadAcDocument](#) - 在默认浏览器中显示此文档。

参数：

- 无。

返回结果：

- 在默认的 Web 浏览器中显示此 Web 页面。
- [Find-CvadAcInFile](#) - 在文件中查找将搜索组件 YAML 文件中与可能包含通配符的一个或多个名称匹配的成员。结果是找到的成员的报告。在文件中查找一次只能搜索一个组件。在文件中查找将搜索当前文件夹及所有子文件夹中的所有 YAML 文件。请使用 [FindSourceFolder](#) 限制要搜索的文件数量。

参数：

名称	说明	必需?	类型
按组件迁移	请参阅按组件迁移。注意：-All 值无效。		SwitchParameters
<a href="#">IncludeByName</a>	一个列表，用于指定在将站点活动状态设置为活动时包含的交付组名称。支持在名称中使用 “*” 和 “?” 通配符。		字符串列表
<a href="#">Unique</a>	仅报告找到的唯一成员。		SwitchParameter
<a href="#">IncludeYaml</a>	包括成员特定的 YAML。		SwitchParameter
<a href="#">FindSourceFolder</a>	文件夹查找将开始搜索。		字符串
<a href="#">DisplayLog</a>	在 cmdlet 完成时显示日志文件。设置为 \$false 将禁止日志显示。		SwitchParameter
<a href="#">Quiet</a>	禁止登录控制台。		SwitchParameter

返回：

- 为指定的组件创建包含找到的成员的报告。

站点激活 **cmdlet**

有关激活站点和使用这些 cmdlet 的详细信息，请参阅[激活站点](#)。

- **Set-CvadAcSiteActiveStateOnPrem** - 将本地站点状态设置为活动或非活动状态。

参数：

名称	说明	必需?	类型
云访问参数	请参阅云访问参数		SwitchParameters
<b>SiteActive</b>	如果存在，则将本地站点设置为主动从所有交付组中删除维护模式。此参数不存在时，将在所有交付组上设置维护模式。		SwitchParameter
<b>IncludeByName</b>	一个列表，用于指定在将站点活动状态设置为活动时要包括的交付组名称。支持在名称中使用 “*” 和 “?” 通配符。		字符串列表
<b>ExcludeByName</b>	一个列表，用于指定在将站点活动状态设置为活动时要排除的交付组名称。支持在名称中使用 “*” 和 “?” 通配符。		字符串列表
<b>Quiet</b>	禁止登录控制台。		SwitchParameter
<b>DisplayLog</b>	在 cmdlet 完成时显示日志文件。设置为 <code>\$false</code> 将禁止日志显示。		<code>\$true or \$false</code>

返回结果：

- 请参阅 Cmdlet 返回值

- **Set-CvadAcSiteActiveStateCloud** - 将云站点状态设置为活动或非活动状态。

参数：

名称	说明	必需?	类型
云访问参数	请参阅云访问参数		SwitchParameters
<b>SiteActive</b>	如果存在，则将云站点设置为活动状态，从所有交付组中删除维护模式。此参数不存在时，将在所有交付组上设置维护模式。		SwitchParameter
<b>IncludeByName</b>	一个列表，用于指定在将站点活动状态设置为活动时要包括的交付组名称。支持在名称中使用 “*” 和 “?” 通配符。		字符串列表
<b>ExcludeByName</b>	一个列表，用于指定在将站点活动状态设置为活动时要排除的交付组名称。支持在名称中使用 “*” 和 “?” 通配符。		字符串列表
<b>Quiet</b>	禁止登录控制台。		SwitchParameter

名称	说明	必需?	类型
<code>DisplayLog</code>	在 cmdlet 完成时显示日志文件。设置为 <code>\$false</code> 将禁止日志显示。		<code>\$true or \$false</code>

返回结果：

- 请参阅 Cmdlet 返回值

合并多个本地站点 **cmdlet**

有关这些 cmdlet 的站点合并和使用的详细信息，请参阅[将多个站点合并到一个站点中](#)。

- `New-CvadAcSiteMergingInfo` - 创建一个合并前缀/后缀信息集的站点。开始时没有必要知晓所有前缀或后缀。可以通过 `Set-CvadAcSiteMergingInfo` 或手动编辑 `SiteMerging.yml` 文件来对其进行更新。

参数：

名称	说明	必需?	类型
<code>SiteName</code>	用于标识特定站点的前缀/后缀集的名称。它可以与实际站点的名称匹配，但不需要匹配。	x	字符串
站点合并参数	请参阅站点合并参数		SwitchParameters
<code>Quiet</code>	禁止登录控制台。		SwitchParameter

返回结果：

- 无

- `Set-CvadAcSiteMergingInfo` - 更新现有站点合并前缀/后缀信息集。

参数：

名称	说明	必需?	类型
<code>SiteName</code>	用于标识特定站点的前缀/后缀集的名称。它可以与实际站点的名称匹配，但不需要匹配。	x	字符串

名称	说明	必需?	类型
站点合并参数	请参阅站点合并参数		SwitchParameters
<a href="#">Quiet</a>	禁止登录控制台。		SwitchParameter

返回结果：

- 无
- [Remove-CvadAcSiteMergingInfo](#) - 删除现有站点合并前缀/后缀信息集。

参数：

- [SiteName](#) - 标识一组站点前缀和后缀。这是一个字符串，是必需的。

返回结果：

- 无

站点合并参数

运行站点合并 cmdlet 时可以使用以下参数。列出的所有参数都是字符串。

- [SiteName](#) - 用于标识特定站点的前缀/后缀集的名称。它可以与实际站点的名称匹配，但不需要匹配。  
[SiteName](#) 是必需的参数。
- [AdminScopedPrefix](#) - 要应用到管理员作用域的前缀。
- [ApplicationPrefix](#) - 应用到应用程序的前缀。
- [ApplicationFolderPrefix](#) - 应用到应用程序文件夹的前缀；[ApplicationFolderPrefix](#) 可以与 [ApplicationFolderRoot](#) 结合使用。
- [ApplicationFolderRoot](#) - 应用程序文件夹的新根文件夹。这将创建额外的文件夹层次结构。  
[ApplicationFolderRoot](#) 可以与 [ApplicationFolderPrefix](#) 结合使用。
- [ApplicationGroupPrefix](#) - 应用程序组的前缀。
- [ApplicationUserPrefix](#) - 应用到用户看到的应用程序名称的前缀。
- [ApplicationAdminPrefix](#) - 应用到管理员看到的应用程序名称的前缀。
- [DeliveryGroupPrefix](#) - 要应用到交付组的前缀。
- [GroupPolicyPrefix](#) - 要应用到策略名称的前缀。
- [HostConnectionPrefix](#) - 要应用到主机连接的前缀。
- [MachineCatalogPrefix](#) - 要应用到计算机目录的前缀。
- [StoreFrontPrefix](#) - 要应用到 [StoreFront](#) 名称的前缀。
- [TagPrefix](#) - 要应用到标记的前缀。
- [AdminScopedSuffix](#) - 要应用到管理员作用域的后缀。
- [ApplicationSuffix](#) - 适用于应用程序的后缀。



- **ApplicationFolderSuffix** - 要应用到应用程序文件夹的后缀;**ApplicationFolderSuffix** 可以与 **ApplicationFolderRoot** 结合使用。
- **ApplicationGroupSuffix** - 应用程序组的后缀。
- **ApplicationUserSuffix** - 要应用到用户看到的应用程序名称的后缀。
- **ApplicationAdminSuffix** - 要应用到管理员看到的应用程序名称的后缀。
- **DeliveryGroupSuffix** - 要应用到交付组的后缀。
- **GroupPolicySuffix** - 要应用到策略名称的后缀。
- **HostConnectionSuffix** - 要应用到主机连接的后缀。
- **MachineCatalogSuffix** - 要应用到计算机目录的后缀。
- **StoreFrontSuffix** - 要应用到 **StoreFront** 名称的后缀。
- **TagSuffix** - 要应用到标记的后缀。
- **SiteRootFolder** - 用于导出和导入的完全限定文件夹名称; 可以是本地文件夹或文件共享。

## 泛型参数

### 云访问参数

所有访问云的 cmdlet 都支持以下额外的参数。

#### 注意：

可以将 **CustomerId**、**ClientId** 和 **Secret** 放置在 **CustomerInfo.yml** 文件中，也可以使用以下参数通过 cmdlet 指定。在两个位置都指定时，cmdlet 参数优先。

- **CustomerId** - 已在 REST API 中使用且访问所有 REST API 所需的客户 ID。您的客户 ID 位于 Citrix Cloud 中。
- **ClientId** - 在 Citrix Cloud 身份识别和访问管理网站上创建的客户端 ID。获取对所有 Rest API 进行身份验证所需的持有者令牌时，需要此信息。
- **Secret** - 在 Citrix Cloud 身份识别和访问管理网站上创建的密钥。获取对所有 Rest API 进行身份验证所需的持有者令牌时，需要此信息。
- **CustomerInfoFileSpec** - 指向客户信息文件以覆盖默认位置和名称的文件规范。

### 迁移模式参数

修改云站点配置 (**Import**、**Restore**、**Merge**、**New** 和 **Sync**) 的 Cmdlet 还额外支持以下参数，以提高灵活性。

- **CheckMode** - 执行导入操作，但不进行任何更改。在导入完成之前，将报告所有预期更改。您可以使用此命令在执行导入之前测试导入操作。
- **BackupFirst** - 在修改云配置之前，将云内容备份到 .yml 文件中。默认情况下此选项处于启用状态。

- **Confirm** - 如果为 `true`，则提示用户确认是否要对云站点配置进行更改。由于具有破坏性，**Remove** cmdlet 会显示一条提示。如果不需要提示（例如，在自动化脚本中运行），则设置为 `false`。**Confirm** 默认设置为 `true`。
- **SecurityFileFolder** - 这是包含 `CustomerInfo.yml` 文件的完全限定文件夹，该文件可能会指向可能会受身份验证控制的本地文件夹或网络共享文件夹。该工具将不提示输入凭据；必须在运行该工具之前获取对受控资源的访问权限。
- **SiteName** - 指定导入时要使用的站点合并前缀和后缀设置。
- **SiteActive** - 指定导入的站点处于活动状态还是非活动状态。默认情况下，此参数设置为 `$false`，表示导入的站点处于非活动状态。

#### 日志显示参数

**Export**、**Import**、**Sync**、**Restore**、**Backup**、**Compare** 和 **Remove** cmdlet 会在该操作完成时显示日志文件。您可以通过将 `-DisplayLog` 参数设置为 `$false` 以禁止显示日志。默认情况下，将使用 `Notepad.exe` 来显示日志文件。您可以在 `CustomerInfo.yml` 文件中指定不同的编辑器。

**Editor:** `C:\Program Files\Notepad++\notepad++.exe`

#### Cmdlet 返回值

##### ActionResult

所有 cmdlet 都将返回以下值。

```

1      public class ActionResult
2      {
3
4          public bool                Overall_Success;
5          public Dictionary<string, string> Individual_Success;
6          public object              CustomResult;
7      }
```

**Overall\_Success** 将返回一个布尔值，以显示所有选定组件中的 cmdlet 是否均成功：`true` 表示成功，`false` 表示不成功。

**Individual\_Success** 将返回每个主组件的一个或三个值。组件的结果可以是“成功”、“失败”或“已跳过”。“已跳过”表示未选择以供 cmdlet 执行的组件。

**CustomResult** 特定于 cmdlet。

##### CustomResult

**Import**、**Merge**、**Restore**、**Sync**、**Compare**、**Compare File** 和 **Remove** 将返回 `EvaluationResultData` 单个实例的以下自定义结果信息。

注意：

**Export** 和 **Template** cmdlet 不返回自定义结果。

```

1      public class EvaluationResultData
2      {
3
4          public Dictionary<string, Dictionary<string,
              ActionResultValues >> EvaluationResults;
5          public int Added;
6          public int Updated;
7          public int Deleted;
8          public int NoChange;
9          public int TotalChanged;
10         public EvaluationResults OverallResult;
11         public string CloudBackupFolder;
12         public string SourceBackupFolder;
13     }
14
15     Where:
16     public enum ActionResultValues
17     {
18
19         Add,
20         Update,
21         Delete,
22         Identical,
23         DoNothing
24     }
25
26     public enum EvaluationResults
27     {
28
29         Success,
30         Failure,
31         Skipped
32     }

```

**EvaluationResults** 将显示一个列表，其中包含每个选定组件对应的一个条目。键是组件名称，值是每个组件成员以及对该组件成员执行的操作的列表。操作可以是 **ActionResultValues** 的任何一个值。

**Added**、**Updated**、**Deleted** 和 **NoChange** 指示按该顺序添加、更新、删除或未执行任何操作的组件成员总数。

**TotalChanged** 是 **Added**、**Updated** 和 **Deleted** 的总和。

**OverallResult** 是一个表示 cmdlet 结果的布尔值。True 表示所有组件均成功，false 表示处理一个或多个组件时失败。

**CloudBackupFolder** 是在 cmdlet 执行任何云修改操作之前，云站点配置备份的完全限定文件规范。

**SourceBackupFolder** 是在 cmdlet 完成执行后进行的源文件备份的完全限定文件规范。默认情况下，这些文

件位于 %HOMEPATH%\Documents\Citrix\AutoConfig 中。

PowerShell 帮助

我们为每个 cmdlet 均提供了 PowerShell 帮助。所有参数均与每个 cmdlet 以及相应 cmdlet 的简要说明一起记录。要访问任何 cmdlet 的帮助，请在 cmdlet 前面键入 `Get-Help`。

`Get-Help Import-CvadAcToSite`

自动配置故障排除及其他信息

March 30, 2024

**重要：**  
有关自动配置和相应解决方案的常见错误消息，请参阅知识中心文章 [CTX277730](#) 中的 故障排除常见问题解答。

自动配置工具错误

自动配置工具操作有时会产生错误。发生这种情况时，例如，在处理计算机目录、交付组或组策略等组件时可能会出现故障。使用 `OnErrorAction` 和延续参数允许您在处理过程中发现错误，解决错误，然后从上次中断的地方继续操作。

默认 `OnErrorAction` 值为 `StopCompEnd`。出现错误时，该工具将完成对当前组件的处理。不处理任何其他组件，错误不会延续到下游的依赖组件。解决任何错误后，可以在应用任何延续参数的情况下重新运行 cmdlet。

OnErrorAction 参数

您可以定义迁移命令的 `OnErrorAction` 参数值，以控制该工具如何响应其在处理组件时发现的错误。

下表显示了参数值及其说明：

值	说明
<code>Continue</code>	尝试处理尽可能多的所有组件。
<code>Pause</code>	处理结束时暂停，提示您继续或停止。
<code>StopCompEnd</code>	尝试处理尽可能多的组件。组件完成后停止。（默认）
<code>StopImmediately</code>	发现错误后，处理就会停止。

迁移 cmdlet

您可以将 `OnErrorAction` 参数应用于以下迁移命令：

- `Compare-CvadAcToSite`
- `Import-CvadAcToSite`
- `Merge-CvadAcToSite`
- `New-CvadAcToSite`
- `Restore-CvadAcToSite`

示例：`Merge-CvadAcToSite -OnErrorAction StopImmediately`

恢复参数

这些参数定义了在工作因错误而暂停或停止后工具如何恢复。

您可以将恢复参数应用于包含以下 `OnErrorAction` 参数值之一的迁移 cmdlet：

- `Pause`
- `StopCompEnd`
- `StopImmediately`

下表显示了参数值及其说明：

值	说明
<code>-AllRemaining</code>	需要起始组件。处理从起始组件开始，并处理所有剩余组件。处理多个组件。
<code>-Resume</code>	使用 <code>CurrentComponent.txt</code> 中的组件作为起点。所有剩余的都设置为 <code>true</code> 。处理多个组件。
<code>-Repeat</code>	使用 <code>CurrentComponent.txt</code> 中的组件作为起点。所有剩余的都设置为 <code>false</code> 。只处理一个组件。

最后处理的组件存储在 `AutoConfig` 文件夹的 `CurrentComponent.txt` 文件中。不建议编辑此文件。  
如果指定 `-Resume` 或 `-Repeat`，且 `CurrentComponent.txt` 缺失或无效，则处理将停止，并提示您选择组件。

在 `CustomerInfo.yml` 文件中设置 `OnErrorAction`

您也可以在 `CustomerInfo.yml` 文件中设置 `OnErrorAction` 值。使用以下 cmdlet 设置值：

- 对于新文件：`New-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`

- 对于现有文件: `Set-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`

## 日志

运行任何 cmdlet 都会创建日志文件并在主历史记录日志文件中输入一个条目。所有操作日志文件都位于备份文件夹中。所有日志文件名都以 **CitrixLog** 开头, 然后显示自动配置操作以及 cmdlet 执行的日期和时间戳。日志不会自动删除。

主历史日志位于 `*%HOMEPATH%\Documents\Citrix\AutoConfig*` 下名为 **History.Log** 的文件中。每个 cmdlet 执行都会生成一个主日志条目, 其中包含执行的日期、操作、结果、备份和日志文件位置。

还可以使用 `New-CvadAcZipInfoForSupport` cmdlet 收集日志以发送给 Citrix 寻求支持。此 cmdlet 将所有日志和.yml 文件压缩到一个 zip 文件中。客户敏感信息 (CustomerInfo.yml 和 CvadAcSecurity.yml) 不包含在 zip 文件中。Icon.yml 文件也因其大小而被排除在外。zip 文件根据日期和时间戳放置在 `%HOMEPATH%\Documents\Citrix\AutoConfig` 中, 名称为 `CvadAcSupport_YYYY_MM_DD_HH_MM_SS.zip`。此 zip 文件也可以作为备份。

每个日志文件均包含以下内容:

- 操作名称以及检查模式是否已启用
- 开始和结束日期与时间
- 与每个组件的操作对应的多个条目, 以及成功/失败通知
- 执行的操作的摘要, 包括已创建的各种对象的数量
- 建议的修复 (如果适用)
- 备份文件夹位置 (如果适用)
- 主日志位置
- 持续时间

## 诊断文件

诊断文件可帮助您确定和解决问题。以下文件是在运行其操作时创建的。它们位于 `%HOMEPATH%\Documents\Citrix\AutoConfig` 下特定于操作的子文件夹中。在提供信息以获取问题解决支持时, 请附上这些文件。

## 导出

### `PoshSdk_YYYY_MM_DD_HH_MM_SS.ps1`

此文件将计算进行的所有代理 PowerShell SDK 调用数量, 以将站点配置导出到文件。

导入、合并、还原、同步、备份、比较

`Transaction_yyyy_mm_dd_hh_mm_ss.txt`

此文件记录了每个 REST API 调用及相关信息。

`RestApiContent_yyyy_mm_dd_hh_mm_ss.txt`

此文件包含所有 **Add**、**Update** 和 **Delete** REST API 内容。

## 依赖关系引起的问题

导入和合并可能会因缺少依赖关系而失败。一些常见问题包括：

1. 组策略缺少交付组过滤器。通常的原因是尚未导入的交付组。
2. 应用程序无法导入或合并。通常的原因是缺少尚未导入的交付组或应用程序组。
3. 应用程序组缺少 **RestrictToTag** 标签。通常的原因是尚未导入的标签。
4. 主机连接失败。通常的原因是 `CvadAcSecurity.yml` 文件中缺少安全信息。
5. 计算机目录失败。通常的原因是未导入的主机连接。
6. 计算机目录和交付组中缺少计算机。通常的原因是在 **Active Directory** 中找不到的计算机。
7. 交付组中缺少用户。通常的原因是在 **Active Directory** 中找不到的用户。

## 建议

- 一次不要运行多个自动配置实例。运行多个并发实例会导致在云站点中产生不可预知的结果。如果出现这种情况，请重新运行一个自动配置实例，使站点恢复到预期状态。
- 运行自动配置时，请勿在“完整配置”的“管理”选项卡中使用或更改数据。
- 务必在“完整配置”中直观地验证合并、导入或还原结果，以确保云站点符合预期。

## 文件夹

### 默认文件夹根位置

所有自动配置工具操作都发生在根文件夹或其中的子文件夹中。根文件夹位于 `%HOMEPATH%\Documents\Citrix\AutoConfig` 中。

### 导出

所有导出的文件均位于这两个文件夹位置，以方便使用并提供导出历史记录。导出的内容始终位于根文件夹中。副本位于名为 **Export** 的子文件夹中，并显示了导出日期和时间。

根文件夹包含的永远都是导出的最新本地站点配置。每个 **Export** 子文件夹都包含在指定日期和时间完成的导出，并保留导出的历史记录。您可以使用任何 **Export** 子文件夹来配置云站点。自动配置不会删除或修改现有的导出子文件夹。

## 导入/合并/同步/比较

**Import**、**Merge** 和 **Compare** 操作始终源自位于根文件夹中的文件。每个操作都会创建一个用于将根文件夹中的文件复制到的子文件夹，从而提供云站点更改源文件的历史记录。

## Restore（还原）

**Restore** 操作将使用现有子文件夹来配置云站点。源文件夹是通过所需的 **-RestoreFolder** 参数指定的。与其他命令不同，该命令不会创建新的子文件夹，因为 **Restore** 操作会使用现有子文件夹。还原文件夹可以是根文件夹，但仍必须通过 **-RestoreFolder** 参数来指定。

## 备份

自动配置可初始化、更新和备份云站点配置。在使用过程中，随着时间的推移，许多不同的配置可能会在云站点上发生变化。为便于长期使用和保留历史更改，自动配置采用了保留方案，以保存更改的历史记录，并作为一种还原早期状态的方法。

始终对名为 **Backup** 且包含备份的数据和时间的子文件夹进行云站点配置备份。自动配置不会删除或修改现有的导出子文件夹。

您可以使用备份来还原特定组件或整个配置。要还原整个交付组和计算机目录组件，请使用 cmdlet：

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups -MachineCatalogs
```

注意：

上述 cmdlet 中的备份文件信息基于您自己的备份。

要还原整个云站点配置，请使用 cmdlet：

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

注意：

上述 cmdlet 中的备份文件信息基于您自己的备份。

## 更改默认根文件夹

**Export**、**Import**、**Merge**、**Sync** 和 **Compare** 操作可以通过使用 **-AlternateFolder** 参数来更改默认根文件夹。每个操作子文件夹的创建和管理与之前所述的方式相同。



复制到子文件夹中的文件

所有带有“.yaml”扩展名的文件都将复制到操作子文件夹，以下文件除外：

- CustomerInfo.yaml
- ZoneMapping.yaml
- CvadAcSecurity.yaml

自动防故障云站点备份

在运行更改配置的操作之前，先备份当前云站点配置。此配置包括 **Import**、**Merge**、**Sync** 和 **Restore** 参数。备份始终位于操作子文件夹下方的子文件夹中。

如果使用 **Restore**，则备份文件夹是通过 **-RestoreFolder** 参数指定的文件夹的子文件夹。

自动化

自动配置工具 cmdlet 可以在没有管理员干预的情况下在自动化脚本中运行，方法是在 cmdlet 完成时抑制提示和显示日志结果。此外，您也可以通过使用 CustomerInfo.yaml 文件来设置参数以执行相同的操作。

将以下参数添加到云修改 cmdlet 以禁止显示提示。

**-Confirm \$false**

将以下参数添加到 cmdlet 中，以禁止在 cmdlet 完成运行时显示日志。

**-DisplayLog \$false**

请将以下参数添加到 cmdlet 中以禁止记录到 PowerShell 命令窗口。

**-Quiet**

另一种方法是将以下参数置于 CustomerInfo.yaml 文件中。

**Confirm: False**

**DisplayLog: False**

从 **Delivery Controller** 以外的 **PC** 导出

自动配置工具使用多个 Citrix PowerShell SDK 将本地站点配置导出到文件中。这些 SDK 将自动安装在 Delivery Controller 上，从而无需执行额外操作即可在 Delivery Controller 上运行该工具。在非 Delivery Controller 计算机上运行时，需要安装该工具所需的 Citrix PowerShell SDK 集。此 SDK 集是 Citrix Studio 的一部分，后者可通过 Citrix Virtual Apps and Desktops 安装介质进行安装。

注意：

无法在 Cloud Connector 上运行自动配置。

## 转向 **Citrix Cloud Government** 和 **Japan Control Plane**

Citrix Cloud Government 和 Japan Control Plane 环境使用不同的接入点来验证和分配访问令牌。这一独特要求适用于访问云的任何自动配置工具。执行以下步骤以在这些环境中使用自动配置。

1. 在 %HOMEPATH%\Documents\Citrix\AutoConfig 文件夹中，编辑 CustomerInfo.yml。
2. 根据要连接到的环境，将以下行之一添加到 CustomerInfo.yml 中（或进行更改，如果已存在）。

```
Environment: 'ProductionGov'
```

或

```
Environment: 'ProductionJP'
```

现在可以在这些环境中使用自动配置。

## **Citrix Cloud** 数据收集

有关 Citrix Cloud 收集的的信息的信息，请参阅 [Citrix Cloud 服务客户内容和日志处理](#)。

## 其他资源

### 论坛

访问[针对自动配置的 Citrix Discussions 论坛](#)。

### 视频

观看 YouTube 上的 [Under the Hood of the Automated Configuration Tool for Citrix Virtual Apps and Desktops](#)（适用于 Citrix Virtual Apps and Desktops 的自动配置工具的高级选项）。

### 培训

Cloud Learning Center 包含构建服务部署的分步视频指南，其中包括本文中介绍的任务。请参阅[将 Citrix Virtual Apps and Desktops 迁移到 Citrix Cloud 学习路径](#)。

## 使用 **Image Portability Service** 在资源位置之间迁移工作负载

March 5, 2024

Image Portability Service 简化了跨平台管理映像的过程。Citrix Virtual Apps and Desktops REST API 可用于自动管理 Citrix Virtual Apps and Desktops 站点中的资源。

当您使用 Citrix Cloud 开始在两个资源位置之间迁移映像时，映像可移植性工作流程即开始。导出映像后，Image Portability Service 可帮助您传输和准备映像，以便在目标虚拟机管理程序或公有云上运行。最后，Citrix Provisioning 或 Machine Creation Services 将在目标环境中预置映像。

### 组件

Image Portability Service 组件包括：

- Citrix Cloud 服务
- Citrix Credential Wallet
- Citrix Connector Appliance
- Compositing Engine VM
- PowerShell 示例脚本

### **Citrix Cloud** 服务

Citrix Cloud 服务 API 是一项 REST API 服务，可与 Image Portability Service 进行交互。使用 REST API 服务，您可以创建和监视 Image Portability 作业。例如，您调用 API 来启动 Image Portability 作业（例如导出磁盘），然后调用以获取任务的状态。

### **Citrix Credential Wallet**

Citrix Credentials Wallet 服务可以安全地管理系统凭据，从而允许 Image Portability Service 与您的资产进行交互。例如，将磁盘从 vSphere 导出到 SMB 共享时，Image Portability Service 需要凭据才能打开与 SMB 共享的连接才能写入磁盘。如果凭据存储在 Credential Wallet 中，则 Image Portability Service 可以检索和使用这些凭据。

此服务使您能够完全管理您的凭据。云服务 API 充当接入点，使您能够创建、更新和删除凭据。

### **Compositing Engine**

Compositing Engine 是 Image Portability Service 的主力。Compositing Engine (CE) 是在 Image Portability 导出或准备作业开始时创建的单个 VM。这些 VM 是在执行作业的同一环境中创建的。例如，从 vSphere 导出磁

盘时，将在 vSphere 服务器上创建 CE。同样，在 Azure、AWS 或 Google Cloud 中运行准备任务时，CE 分别在 Azure、AWS 或 Google 中创建。CE 会将您的磁盘装载到自身，然后对磁盘进行必要的操作。完成准备或导出作业后，CE VM 及其所有组件都将被删除。

## Connector Appliance

Connector Appliance 运行用于管理 IPS 资源的提供商软件，可在您的环境（本地和 Azure、AWS 或 Google Cloud 订阅中）运行，充当单个任务的控制器。它接收来自云服务的作业指令，并创建和管理 Compositing Engine VM。Connector Appliance VM 充当云服务与您的环境之间的单个安全通信点。在每个资源位置（本地、Azure、AWS 或 Google Cloud）部署一个或多个 Connector Appliance。为了安全起见，每个资源位置都部署了 Connector Appliance。通过将 Connector Appliance 和 Compositing Engine 放在同一位置，部署的安全状况将大大提高，因为所有组件和通信都保存在您的资源位置内。

## PowerShell 模块

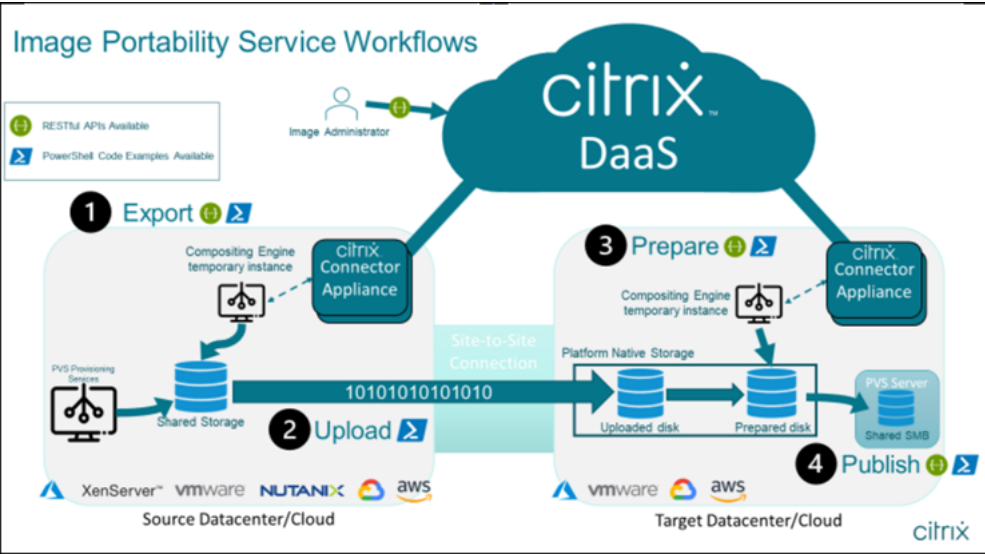
我们提供了一组在脚本中使用的 PowerShell 模块，作为开发您自己的自定义自动化的起点。提供的模块按原样受支持，但如果部署有需要，您可以对其进行修改。

PowerShell 自动化使用提供的配置参数编写对 Citrix Cloud API 服务的 REST 调用以启操作业，然后随着作业的进展为您提供定期更新。

如果您想开发自己的自动化解决方案，则可以使用首选的编程语言直接调用云服务。有关配置和使用 Image Portability Service [REST 端点](#)和 [PowerShell 模块](#)的详细信息，请参阅 [API 门户](#)。

## 工作流

Image Portability Service 使用多阶段工作流从本地资源位置为您的公有云订阅准备主目录映像。该服务将从本地虚拟机管理程序平台导出映像，然后将其上载到公有云订阅（我们提供的 PowerShell 上载实用程序可以帮助实现此操作的自动化）。然后，Image Portability 会准备映像，使其与您的公有云平台兼容。最后，映像将发布并准备作为您的云资源位置中的新计算机目录进行部署。



这些高级工作流基于映像的源和目标预配置（计算机创建或 Citrix Provisioning）。所选工作流决定了需要执行哪些 Image Portability 作业步骤。

请参见下表，了解每个受支持的 IPS 工作流都需要哪些作业。

工作流（从源到目标）	导出	上载	准备	发布
MCS 到 MCS	Y	Y	Y	N
PVS 到 MCS*	N	Y	Y	N
Azure/Google Cloud 上的 PVS 到 PVS*	N	Y	Y	Y
Azure/Google Cloud 上的 MCS 到 PVS	Y	Y	Y	Y

\* 假设您拥有作为 Citrix Provisioning 虚拟磁盘的原始映像，并且不需要将其直接导出源平台虚拟机管理程序。

要求

要开始使用 Image Portability，您必须满足以下要求。

Citrix 计算机目录映像

IPS 要求使用具有下列经过测试的配置之一的映像：

- Windows Server 2016、2019 和 2022H2

- Windows 10 或 11
- 使用 Machine Creation Services 或 Citrix Provisioning
- Citrix Virtual Apps and Desktops VDA 版本 1912CU6、1912CU7、2203CU1、2203CU2、2212、2303 或 2305
- 在 Azure 中为控制台访问启用了远程桌面服务

Image Portability Service 支持以下虚拟机管理程序和云平台：

源平台：

- VMware vSphere 7.0 和 8.0
- XenServer/XenServer 8.2
- Nutanix Prism Element 3.x
- Microsoft Azure
- Google 云端平台

目的地平台：

- VMware vSphere 8.0
- Microsoft Azure
- AWS
- Google 云端平台

## A Citrix Connector Appliance

您需要在计划使用 Image Portability 的每个资源位置安装和配置 Citrix Connector Appliance。例如，如果您使用 Image Portability 将映像从 vSphere 移动到 Azure、AWS 和 Google Cloud，则至少需要四个 Citrix Connector 设备：

有关详细说明，请参阅部署 Connector Appliance。

## SMB (Windows) 文件共享

在使用 Image Portability Service 的本地资源位置托管的导出作业期间，您需要一个 Windows **SMB** 文件共享来临时存储数据。请确保共享上的可用空间至少是映像的文件系统所配置的大小的两倍。

一台用于运行 **PowerShell** 脚本的计算机

请确保运行 PowerShell 脚本的计算机具有以下对象：

- PowerShell 版本 5.1。
- 与 SMB 文件共享的快速网络连接。它可以是托管文件共享的同一台计算机。
- 与您计划使用 Image Portability 功能的公有云平台的快速网络连接。例如，Azure、AWS 或 Google Cloud。

有关如何从 PowerShell 库下载和配置 Image Portability 模块的详细信息，请参阅为 PowerShell 准备计算机部分。

您的 **Citrix Cloud** 客户 ID

确保您拥有有效的 [Citrix DaaS 订阅](#)。

要继续，您需要访问 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）。如果您没有访问权限，请联系您的 Citrix 代表。

请参阅 [API Getting Started](#)（API 入门）文档，了解如何创建和配置用于 Image Portability 的 API 客户端。

#### **Azure** 所需的权限和配置

要使 Image Portability Service 对您的 Azure 资源执行操作，您需要向 Image Portability Service 所使用的 Azure 服务委托人授予某些 Azure 功能的权限。有关详细列表，请参阅 Microsoft Azure 所需的权限。

您可以将参与者角色分配给关联资源中的服务委托人。或者，要分配所需的最低权限，您可以创建具有所需权限的自定义角色，然后将其分配给作用域为相应资源的服务主体。

有关为 [Azure 服务主体配置安全角色](#)和[创建自定义角色](#)的信息，请参阅 Azure 文档。

#### **Google Cloud** 需要权限和配置

要使 Image Portability Service 在您的 Google Cloud 项目中执行操作，您需要向 Image Portability Service 使用的 Google Cloud 服务主体授予某些功能的权限。

有关详细列表，请参阅 Google Cloud 所需的权限。

可以使用以下角色分配这些权限：

- Cloud Build 编辑者
- 计算管理员
- 存储管理员
- 服务帐户用户

有关配置服务帐号权限的详细信息，请参阅 [Google Cloud documentation](#)（Google Cloud 文档）。

## Amazon Web Services 需要权限和配置

要使用 Amazon Web Services (AWS) 帐户执行 Image Portability Service 工作流程，相应的身份和访问管理 (IAM) 身份必须具有正确的权限。

有关详细列表，请参阅 AWS 必需的权限。

## 设置 Image Portability Service

要设置 Image Portability Service，您可以：

- 部署 Connector Appliance
- 为 PowerShell 准备计算机
- 向 Credential Wallet 中添加凭据

### 部署 Connector Appliance

Image Portability 要求 Citrix Connector Appliance 创建 Image Portability 作业。Connector Appliance 可帮助保护与您的本地和公有云环境的交互。Connector Appliance 的通信回传到 Image Portability Service 以报告作业状态和整体服务运行状况。

要在您的环境中部署和配置 Connector Appliance，请按照 [Connector Appliance for Cloud Services](#)（适用于云服务的 Connector Appliance）中的步骤进行操作。

规划部署时，请注意设备所需的 [hardware configuration](#)（硬件配置）和 [network port access](#)（网络端口访问权限）。

部署和注册设备后，将自动安装启用 Image Portability 所需的组件。

### 为 PowerShell 准备计算机

为了帮助您启动和运行 Image Portability，我们创建了 PowerShell 模块，您可以自定义这些模块并与该服务一起使用。

以下各部分内容介绍了如何准备计算机以运行 PowerShell 脚本。这些脚本只是几个示例。请修改或增强这些脚本以满足您的需求。

注意：

初始安装后，请使用 **Update-Module** 更新 PowerShell 模块。



**PowerShell 要求** 要使用 PowerShell 脚本，您需要满足以下条件：

- 一台 Windows 计算机，用于运行驱动 Image Portability 作业的 PowerShell 脚本。计算机：
  - 有最新版本的 PowerShell。
  - 与本地 SMB 文件共享的网络连接为 10 Gbs 或更高，并且可以快速连接到您的公有云（例如 Azure、AWS 或 Google Cloud）。
  - 可以是托管文件共享的同一台计算机。
  - 是运行 Windows 10、Windows Server 2019 或 Windows Server 2022 的计算机，并带有最新的 Microsoft 修补程序。
  - 可以连接到 Microsoft PowerShell 库以下载所需的 PowerShell 库。

根据您的 Windows 版本，您可能需要禁用 TLS 1.0/1.1 支持。有关详细信息，请参阅 [Microsoft PowerShell Gallery TLS 支持文档](#)。

默认情况下，PowerShell 不会通过代理服务器自动进行身份验证。请确保您已按照 Microsoft 和代理供应商最佳实践将 PowerShell 会话配置为使用代理服务器。

如果在运行涉及 PowerShellGet 缺失或旧版本的 PowerShellGet 的 PowerShell 脚本时看到错误，则需要按如下所示安装最新版本：

```
1 Install-Module -Name PowerShellGet -Force -Scope CurrentUser -  
   AllowClobber  
2 <!--NeedCopy-->
```

**安装库和模块** Image Portability Service 利用 Microsoft PowerShell 库中的库来推动可移植性操作。

重要提示：

初始安装后，请使用 **Update-Module** 安装新版本。

1. 运行以下 PowerShell 命令以下载最新模块：

```
1 Install-Module -Name "Citrix.Workloads.Portability","Citrix.Image.  
   Uploader" -Scope CurrentUser  
2 <!--NeedCopy-->
```

- 要更改 PATH 环境变量，请执行以下操作：

按 **Y** 和 **Enter** 键接受。

- 要安装 NuGet 提供程序，请执行以下操作：

按 **Y** 和 **Enter** 键接受。

- 如果被告知库不受信任：

按 **A**（全部）并按 **Enter** 键继续。

2. 通过运行以下命令确认所有必需的模块都已下载：

```
1 Get-InstalledModule -Name Citrix.*
2 <!--NeedCopy-->
```

此命令返回类似于以下内容的输出：

名称	存储库	说明
Citrix.Image.Uploader	PSGallery	将 VHD (x) 上载到 Azure 存储帐户、AWS 或 GCP 以及获取有关 VHD 信息的命令 (x)
Citrix.Workloads.Portability	PSGallery	用于 Citrix Image Portability Service 的映像作业的独立 Cmdlet

将模块更新到最新版本 运行以下命令将脚本更新到最新版本。

```
1 Update-Module -Name "Citrix.Workloads.Portability","Citrix.Image.Uploader" -Force
2 <!--NeedCopy-->
```

安装 **Citrix Virtual Apps and Desktops Remote PowerShell SDK** Image Portability Service 需要 Citrix Virtual Apps and Desktops Remote PowerShell SDK 在 Citrix Cloud 中创建和管理可移植性作业。

在您的计算机上下载并安装 [Remote PowerShell SDK](#)。

安装平台特定的第三方组件 Image Portability Service PowerShell 模块不安装第三方依赖项。因此，您可以将安装限制在您的目标平台上。如果您使用以下平台之一，请按照安装平台依赖项的相关说明进行操作：

**VMware** 如果您正在创建与 VMware 环境通信的映像可移植性作业，请运行以下命令来安装所需的 VMware PowerShell 模块。

```
1 Install-Module -Name VMWare.PowerCLI -Scope CurrentUser -AllowClobber -Force -SkipPublisherCheck
2 <!--NeedCopy-->
```

**Amazon Web Services** 如果您要在 AWS 中创建 Image Portability 作业，请下载并安装 [AWS 命令行界面](#)，然后运行以下命令来安装所需的 AWS PowerShell 模块：

```
1 Install-Module -Name AWS.Tools.Installer
2 Install-AWSToolsModule AWS.Tools.EC2,AWS.Tools.S3
3 <!--NeedCopy-->
```

**Azure** 如果要在 Azure 中创建 Image Portability 作业，请下载并安装 [Azure 命令行实用程序](#)，然后运行以下命令以安装所需的 Azure PowerShell 模块：

```
1 Install-Module -Name Az.Accounts -Scope CurrentUser -AllowClobber - Force
2 Install-Module -Name Az.Compute -Scope CurrentUser -AllowClobber -Force
3 <!--NeedCopy-->
```

**Google Cloud** 如果您要在 Google Cloud 中创建 Image Portability 作业，请在计算机上下载并安装 [Google Cloud SDK](#)。

**卸载脚本和模块** 运行以下命令卸载 Image Portability 软件使用的模块。

注意：

卸载 IPS 模块时，不会自动删除第三方脚本和组件。

要卸载模块，请执行以下操作：

```
1 Get-InstalledModule -Name "Citrix.Workloads.Portability","Citrix.Images
  .Uploader" | Uninstall-Module
2 <!--NeedCopy-->
```

向 **Credential Wallet** 中添加凭据

对于端到端自动化场景，您可以将 Image Portability Service 配置为与 Citrix Cloud、您的公有云和本地资源进行非交互式身份验证。此外，每当我们的 API 直接使用您的本地和公有云资源进行身份验证时，Image Portability Service 都会使用存储在 Citrix Credential Wallet 中的凭据。按照本部分内容所述设置凭据是运行导出、准备和发布作业的必需步骤。

运行作业时，Image Portability Service 需要访问您可以控制的资源。例如，要使 Image Portability Service 将磁盘从 vSphere 服务器导出到 SMB 共享，该服务需要对这两个系统的登录访问权限。为了保护此帐户信息的安全，Image Portability Service 使用 Citrix Credential Wallet 服务。此服务使用用户定义的名称将您的凭据存储在钱包中。要运行作业时，请提供要使用的凭据的名称。此外，这些凭据可以随时更新或从钱包中删除。

通常会为以下平台存储凭据：

- Microsoft Azure
- AWS
- Google Cloud
- SMB 共享
- VMware vSphere
- Nutanix AHV
- XenServer

要管理凭据，请参阅 [Developer API Portal](#)（开发人员 API 门户）的 [Image Portability Service APIs](#)（Image Portability Service API）和“凭据管理”部分。

## 使用 **Image Portability Service**

将本地资源位置中的映像准备到您的公有云订阅需要在 Citrix Cloud 中创建 Image Portability 作业。您可以创建任务以在脚本或程序中对服务进行直接 API 调用，也可以使用我们开发的示例 PowerShell 模块来自动调用 API。有关使用 REST API 和 PowerShell 模块创建 IPS 作业的信息，请参阅 [Image Portability Service Developer API Portal](#)（Image Portability Service 开发人员 API 门户）。

## 使用 **Citrix Provisioning** 发布计算机目录

Image Portability Service (IPS) 与 Azure、AWS 和 Google Cloud 中的 Machine Creation Services (MCS) 一起使用，在 Azure 或 Google Cloud 中与 Citrix Provisioning (PVS) 一起使用。您可以将本指南中描述的 PowerShell 和 REST 解决方案与您的平台的工具、平台的 API 或 Citrix DaaS SDK 相结合，创建无缝自动化的端到端工作流程，用于根据准备好的映像创建计算机目录。根据您的云平台，从完成 IPS 准备工作到创建目录或分配给 PVS 目标，可能需要一些中间步骤。

**AWS** IPS 在 AWS 上准备任务会产生一定的容量。Machine Creation Services 需要在目录创建期间使用 Amazon Machine Image (AMI)。要从迁移的映像生成 AMI，您首先需要从生成的卷创建映像快照，然后基于该快照创建 AMI。这可以通过 AWS 命令行接口 (CLI) 来完成：

```
1 > aws ec2 create-snapshot --volume-id <VolumeId>
2 > aws ec2 register-image --name <AmiName> --architecture 'x86_64' --
    root-device-name '/dev/sda1' --boot-mode uefi --ena-support --
    virtualization-type 'hvm' --block-device-mappings 'DeviceName=/dev/
    sda1,Ebs={
3   SnapshotId=<SnapshotID> }
4   '
5 <!--NeedCopy-->
```

<VolumeId> 是 IPS 准备作业的输出。生成的 AMI 可用作 MCS 主映像。

Citrix.Workloads.Portability 模块中提供了用于自动执行这部分工作流程的 PowerShell 示例脚本，其脚本名为 [New-IpsAwsImage.ps1](#)。

**Azure** 在 Azure 上，IPS 生成可直接用作 MCS 主映像的托管磁盘。为了将生成的映像分配给 PVS 目标，IPS 提供了“发布”操作，用于将托管磁盘复制到 PVS 存储中的 VHD (x) 文件中。

**Google Cloud** IPS 在 Google Cloud 上准备工作生成磁盘。MCS 需要 Google Cloud 实例模板。[准备主虚拟机实例和永久磁盘](#)中详细介绍了从磁盘创建 MCS 实例模板的过程。

对于 Google Cloud 上的 PVS 目标，IPS 提供“发布”操作，用于将磁盘复制到 PVS 商店中的 VHD (x) 文件中。

## 自动执行 VDA 配置

准备源自本地的 Citrix 管理的映像时，您可以在映像中重新配置 VDA，以支持正在准备的映像的目标环境。Image Portability Service 可以在工作流的准备阶段动态应用 VDA 配置更改。以下配置参数定义了 VDA 在迁移的映像中的运行方式：**InstallMisa**、**XdReconfigure** 和 **InstallMcsio**。在创建 IPS 任务时，请参阅 [Image Portability Service PowerShell 示例](#)，以定义这些参数。

## 配置

- 将 **InstallMisa** 配置为 **true** 使 Image Portability Service 能够安装使用 MCS 配置映像所需的任何缺失的 VDA 组件。
- 将 **InstallMisa** 配置为 **true** 或者将 **InstallMcsio** 配置为 **true** 也需要将 **CloudProvisioningType** 配置为 **Mcs**。
- 将 **InstallPvs** 设置为部署映像的 PVS 服务器的版本。设置 **InstallPvs** 后，Image Portability Service (IPS) 会在准备作业期间自动在映像中安装指定版本的 PVS 目标设备软件。IPS 支持最新的两个长期服务版本 (LTSR) 和当前版本 (CR) 的最新两个版本（基本版本或累积更新）。

配置 **InstallPvs** 还需要将 **CloudProvisioningType** 配置为 **Pvs**。

对于 **InstallMisa** 和 **InstallMcsio**，请注意以下几点：

- 这些功能仅在 VDA 的最新 LTSR 和 CR 版本中受支持。
- 如果已安装的 VDA 的必要组件已存在，则即使配置了这些参数，也不会进行任何更改。
- 对于受支持的 VDA 版本，即使必要的 VDA 组件不存在，Image Portability 也会安装所需组件的适当版本。
- 对于不受支持的 VDA 版本，重新配置将失败，如果必要的 VDA 组件不存在，则会记录一条消息。即使 VDA 重新配置未完成，准备工作也已完成。

**XdReconfigure** 需要以下值之一：**controllers** 或 **site\_guid**。下面是使用每个值的配置参数示例：

使用 **controllers**：

```
1 XdReconfigure = @(
2     [pscustomobject]@{
3
4         ParameterName = 'controllers'
5         ParameterValue = 'comma-separated-list-of-your-cloud-connectors
6             -fqdns'
7     }
8 )
9 <!--NeedCopy-->
```

其中 **ParameterValue** 是要指向 VDA 的新 DDC 的 FQDN 列表。可以用逗号分隔的格式指定多个 DDC。

使用 **site\_guid**：

```

1 XdReconfigure = @(
2     [pscustomobject]@{
3
4         ParameterName = 'site_guid'
5         ParameterValue = 'active-directory-site-guid'
6     }
7 )
8 )
9 <!--NeedCopy-->

```

**XdReconfigure** 还接受使用 **/reconfigure** 安装开关运行 VDA 命令行安装程序时支持的值，例如 **XenDesktopV-daSetup.exe /reconfigure**。这些值的一些示例包括 **wem\_agent\_port**、**wem\_cached\_data\_sync\_port**、**wem\_cloud\_connectors** 或 **wem\_server**。有关 VDA 重新配置命令行选项的完整列表，请参阅 [Citrix DaaS VDA 文档](#)。

将 **InstallMcsio** 配置为 **true** 自动在映像上安装 MCSIO。要禁用映像上的自动 MCSIO 安装，请将 **InstallMcsio** 配置为 **false**。

注意：

您可以在运行命令 **-DryRun** 时使用来验证您的配置和 Connector Appliance 的网络设置。

## 参考

本部分内容根据您的需要详细介绍了技术参考信息。

## Image Portability Service 所需的权限

本部分内容详细介绍了 Image Portability Service 在每个受支持的本地和云平台上所需的权限。

**Connector Appliance** 所需的权限 Connector Appliance 需要访问以下 URL 才能在 Image Portability Service 中准备映像：

```

1 *.layering.cloud.com
2 credentialwallet.citrixworkspaceapi.net
3 graph.microsoft.com
4 login.microsoftonline.com
5 management.azure.com
6 *.blob.storage.azure.net
7 <!--NeedCopy-->

```

**VMware vCenter** 所需的权限 要在 VMware 环境中运行 IPS 导出磁盘作业，必须具有以下 vCenter 权限。这些权限可在 vCenter 管理面板的 **Access Control**（访问控制）部分的 **Roles**（角色）下找到。

```

1 - Cryptographic operations
2   - Direct Access
3
4 - Datastore
5   - Allocate space
6   - Browse datastore
7   - Low level file operations
8   - Remove file
9
10 - Folder
11   - Create folder
12   - Delete folder
13
14 - Network
15   - Assign network
16
17 - Resource
18   - Assign virtual machine to resource pool
19
20 - Virtual machine
21   - Change Configuration
22     - Add existing disk
23     - Add new disk
24     - Remove disk
25
26   - Edit Inventory
27     - Create from existing
28     - Create new
29     - Remove
30
31   - Interaction
32     - Power off
33     - Power on
34 <!--NeedCopy-->

```

**Microsoft Azure** 所需的权限 Image Portability 要求您的 Azure 服务帐户具有以下权限。

当指定用于合成引擎的资源组时（即在 REST 请求的 *resourceGroup* 属性中或使用 Citrix.Workloads.Portability PowerShell 命令时在 *-AzureVmResourceGroup* 参数中），则需要在资源组范围内具有以下权限。

```

1 Microsoft.Compute/disks/beginGetAccess/action
2 Microsoft.Compute/disks/endGetAccess/action
3 Microsoft.Compute/disks/delete
4 Microsoft.Compute/disks/read
5 Microsoft.Compute/disks/write
6 Microsoft.Compute/virtualMachines/delete
7 Microsoft.Compute/virtualMachines/powerOff/action
8 Microsoft.Compute/virtualMachines/read
9 Microsoft.Compute/virtualMachines/write
10 Microsoft.Network/networkInterfaces/delete
11 Microsoft.Network/networkInterfaces/join/action

```

```
12 Microsoft.Network/networkInterfaces/read
13 Microsoft.Network/networkInterfaces/write
14 Microsoft.Network/networkSecurityGroups/delete
15 Microsoft.Network/networkSecurityGroups/join/action
16 Microsoft.Network/networkSecurityGroups/read
17 Microsoft.Network/networkSecurityGroups/write
18 Microsoft.Resources/deployments/operationStatuses/read
19 Microsoft.Resources/deployments/read
20 Microsoft.Resources/deployments/write
21 Microsoft.Resources/subscriptions/resourcegroups/read
22 <!--NeedCopy-->
```

未指定用于 Compositing Engine 的资源组时，在订阅范围内需要以下权限。

```
1 Microsoft.Compute/disks/beginGetAccess/action
2 Microsoft.Compute/disks/endGetAccess/action
3 Microsoft.Compute/disks/read
4 Microsoft.Compute/disks/write
5 Microsoft.Compute/virtualMachines/powerOff/action
6 Microsoft.Compute/virtualMachines/read
7 Microsoft.Compute/virtualMachines/write
8 Microsoft.Network/networkInterfaces/join/action
9 Microsoft.Network/networkInterfaces/read
10 Microsoft.Network/networkInterfaces/write
11 Microsoft.Network/networkSecurityGroups/join/action
12 Microsoft.Network/networkSecurityGroups/read
13 Microsoft.Network/networkSecurityGroups/write
14 Microsoft.Resources/deployments/operationStatuses/read
15 Microsoft.Resources/deployments/read
16 Microsoft.Resources/deployments/write
17 Microsoft.Resources/subscriptions/resourceGroups/delete
18 Microsoft.Resources/subscriptions/resourceGroups/write
19 Microsoft.Authorization/roleAssignments/read
20 Microsoft.Authorization/roleDefinitions/read
21 <!--NeedCopy-->
```

在指定目标资源组（即在 REST 请求的 *targetDiskResourceGroupName* 属性中指定的资源组或使用 PowerShell 时使用 *-TargetResourceGroup* 参数指定的资源组）范围内需要以下权限。

```
1 Microsoft.Compute/disks/beginGetAccess/action
2 Microsoft.Compute/disks/delete
3 Microsoft.Compute/disks/read
4 Microsoft.Compute/disks/write
5 Microsoft.Compute/snapshots/delete
6 Microsoft.Compute/snapshots/read
7 Microsoft.Compute/snapshots/write
8 <!--NeedCopy-->
```

在指定的虚拟网络资源组（即 REST 请求的 *virtualNetworkResourceGroupName* 属性中指定的资源组或使用 PowerShell 时使用 *-AzureVirtualNetworkResourceGroupName* 参数指定的资源组）范围内需要以下权限。

```
1 Microsoft.Network/virtualNetworks/read
2 Microsoft.Network/virtualNetworks/subnets/join/action
```



3 <!--NeedCopy-->

**重要提示：**

“prepare” 和 “prepareAndPublish” 任务的 **ceVmSku** 选项控制生成的托管磁盘适用的 Azure 虚拟机类型。您必须选择与要从输出映像中预置的虚拟机具有相同系列和版本的 **ceVmSku**。 **Standard\_D2S\_v3** 的默认值适合在所有 v3 D 系列计算机上运行。在 v4 及更新的 VM SKU 中，Microsoft 已将连接到 VM 的临时资源磁盘设为可选。这会影响页面文件的正确放置。如果您打算为使用输出映像配置的计算机使用 不带 临时资源磁盘的 VM SKU，则必须确保您的 **ceVmSku** 也没有临时资源磁盘。如果 **ceVmSku** 是带有临时资源磁盘的类型，则 IPS 会将 Windows 页面文件移至该磁盘。如果您在没有临时资源磁盘的 SKU 上使用以这种方式准备的磁盘，则每次登录时都会收到警告对话框。如果 **ceVmSku** 没有临时磁盘，则页面文件是在系统根卷上配置的。如果您在包含临时资源磁盘的 SKU 上使用以这种方式准备的图片，这可能会导致意外的 I/O 费用。

**Google Cloud** 所需的权限 Image Portability 要求您的 Google Cloud 服务帐号具有以下权限：

```
1 cloudbuild.builds.create
2 cloudbuild.builds.get
3 cloudbuild.builds.list
4 compute.disks.create
5 compute.disks.delete
6 compute.disks.get
7 compute.disks.list
8 compute.disks.setLabels
9 compute.disks.use
10 compute.globalOperations.get
11 compute.images.create
12 compute.images.delete
13 compute.images.get
14 compute.images.list
15 compute.images.setLabels
16 compute.images.useReadOnly
17 compute.instances.create
18 compute.instances.delete
19 compute.instances.get
20 compute.instances.setLabels
21 compute.instances.setMetadata
22 compute.instances.setServiceAccount
23 compute.instances.setTags
24 compute.instances.stop
25 compute.instances.updateDisplayDevice
26 compute.networks.get
27 compute.subnetworks.use
28 compute.subnetworks.useExternalIp
29 compute.zoneOperations.get
30 compute.zones.list
31 iam.serviceAccounts.actAs
32 iam.serviceAccounts.get
33 iam.serviceAccounts.list
34 resourceManager.projects.get
35 storage.buckets.create
```

```
36 storage.buckets.delete
37 storage.buckets.get
38 storage.objects.create
39 storage.objects.delete
40 storage.objects.get
41 storage.objects.list
42 <!--NeedCopy-->
```

**AWS** 所需的权限 Image Portability 要求您将具有以下配置的 JSON 策略文档附加到 Identity and Access Management (IAM) 用户：

```
1 {
2
3   "Version": "2012-10-17",
4   "Statement": [
5     {
6
7       "Action": [
8         "ebs:StartSnapshot",
9         "ebs:PutSnapshotBlock",
10        "ebs:CompleteSnapshot",
11        "ec2:CreateTags",
12        "ec2:CreateImage",
13        "ec2>DeleteSnapshot",
14        "ec2>DeleteVolume",
15        "ec2:DeregisterImage",
16        "ec2:DescribeImages",
17        "ec2:DescribeInstances",
18        "ec2:DescribeRegions",
19        "ec2:DescribeSecurityGroups",
20        "ec2:DescribeSnapshots",
21        "ec2:DescribeSubnets",
22        "ec2:RebootInstances",
23        "ec2:RegisterImage",
24        "ec2:RunInstances",
25        "ec2:TerminateInstances",
26      ],
27      "Effect": "Allow",
28      "Resource": "*"
29    }
30  ]
31 }
32
33
34 <!--NeedCopy-->
```

注意：

您可能需要根据需要进一步缩小资源的范围。

**Nutanix AHV** 所需的权限 Image Portability 要求您成为 Nutanix AHV 配置的群集管理员。

**XenServer** 所需的权限 Image Portability 要求您至少拥有 XenServer 主机所在池的“虚拟机管理员”角色。

**网络连接** Image Portability Service (IPS) 创建一个名为合成引擎 (CE) 的工作虚拟机来执行映像操作。关联资源位置中的所有 Connector Appliance 都必须能够通过 HTTPS 与 CE 通信。

Connector Appliance (CA) 与 CE 之间的所有通信均由 CA 发起，但 vSphere 除外，其中 CE 和 CA 之间存在双向 HTTPS 通信。

在云环境 (Azure、AWS、Google Cloud) 中，CE 是使用私有 IP 地址创建的。因此，CE 必须与 CA 位于同一个虚拟网络上，或者位于可从 CA 访问的虚拟网络上。

此外，对于涉及 SMB 共享上文件的作业（例如，导出任务），CE 必须位于连接到 SMB 共享的网络上。

有关如何在每个支持的平台上指定用于 CE 的网络的详细信息，请参阅 [Image Portability Service API 文档](#)。

对于“准备”作业，将启动映像中包含的操作系统（在 CE 上）以执行专业化和其他任务。如果映像包含呼叫控制服务器的管理或安全代理，则这些进程可能会干扰准备过程。

如果指定了域取消加入选项，则网络连接可能会影响结果。如果合成引擎虚拟机可以通过网络到达 Active Directory 域控制器，则取消加入会将计算机帐户从域中移除。这打破了提取映像的源 VM 的域成员资格。

因此，我们建议将为操作提供的网络与其他网络资源隔离。这可以通过子网隔离或防火墙规则来完成。有关详细信息，请参阅网络隔离。

在某些本地虚拟机管理程序环境中，虚拟机管理程序可能会使用 TLS 服务器证书进行配置，该证书要么不受 CA 的可信根证书颁发机构的信任，要么与服务器的主机名不匹配。对于此类情况，**IPS** 提供了任务请求 属性，可用于解决问题。有关详细信息，请参阅 TLS 证书。

**网络代理** 如果 CA 和互联网之间的网络流量通过执行 TLS 自检的代理，则可能需要将代理的根证书颁发机构（即代理用于签署其生成的 TLS 证书的证书）添加到 CA 的根证书颁发机构集中。有关详细信息，请参阅 [在 Citrix Cloud 上注册您的 Connector Appliance](#)。

#### 网络隔离

- Azure

在 Azure 中，如果操作中使用的 Azure 服务主体具有必要的 Azure 权限<sup>1</sup>，则默认情况下，CE 是在其 NIC 上附加网络安全组 (NSG) 的情况下创建的。

- Microsoft.Network/networkSecurityGroups/join/action
- Microsoft.Network/networkSecurityGroups/read
- Microsoft.Network/networkSecurityGroups/write

否则，如果未使用显式资源组，则在订阅范围内使用以下权限：

- \* Microsoft.Network/networkSecurityGroups/delete
- \* Microsoft.Network/networkSecurityGroups/join/action
- \* Microsoft.Network/networkSecurityGroups/read
- \* Microsoft.Network/networkSecurityGroups/write

此 NSG 配置为阻止所有进出 CE 的流量，但以下情况除外：

- SMB（端口 445）出站
- HTTPS（端口 443）入站
- 内部 Azure 服务所必需的

通过将任务请求中的 *networkIsolation* 属性设置为 *true*，可以强制使用 NSG。在这种情况下，如果操作中使用的服务主体没有必要的权限，则任务将失败。通过将 *networkIsolation* 属性设置为 *false*，可以禁用 NSG 的使用。

#### • AWS

在 AWS 中，为了实现 CE 的网络隔离，您可以创建一个或多个网络安全组来阻止所有不需要的流量，然后在任务请求中，使用 *securityGroupIds* 请求参数将安全组分配给 CE 实例，该参数将安全组 ID 列表作为值。

#### • Google Cloud

在 Google Cloud 中，为了实现 CE 的网络隔离，您可以创建防火墙规则来阻止所有不想要的流量，然后通过网络标签将这些规则应用于 CE。IPS 使用网络标记 *compositing-engine* 创建 CE，您可以使用 *networkTags* 作业请求参数为其分配其他网络标记，该参数将标记列表作为值。

**TLS 证书** 如果虚拟机管理程序的服务器证书由 CA 不信任的机构签署，则可以使用两种替代方法来解决这个问题。

1. 在任务请求中指定额外的根证书颁发机构证书，用于证书验证。此证书必须是用于签署虚拟机管理程序服务器证书的根证书颁发机构。
2. 在任务请求中指定虚拟机管理程序服务器证书的 SHA-1 指纹。在这种情况下，证书验证是通过验证虚拟机管理程序返回的证书的 SHA-1 指纹是否与任务请求中提供的指纹相匹配来完成的。如果 CE 和虚拟机管理程序之间有 TLS 拦截代理，则此方法可能不起作用。

下面分别给出了每个平台的上述任务请求参数为：

#### • vSphere

1. vCenterSslCaCertificate
2. vCenterSslFingerprint

#### • Nutanix

1. prismSslCaCertificate
2. prismSslFingerprint

#### • XenServer

1. xenSslCaCertificate
2. xenSslFingerprint


有关更多详细信息，请参阅 [Image Portability Service API](#) 文档。

当虚拟机管理程序服务器的主机名与其证书中的主机名不匹配时，也会出现证书验证错误。在这种情况下，可以通过在任务请求中将以下参数设置为 *true* 来禁用主机名匹配：

- vSphere
  - vCenterSslNoCheckHostname
- Nutanix
  - prismSslNoCheckHostname
- XenServer
  - xenSslNoCheckHostname

#### 相关文档

- [Image Portability Service API](#) 文档
- 适用于云服务的 [Connector Appliance](#)
- [Google Cloud](#) 文档
- [Google Cloud](#) 服务帐户
- [Microsoft Azure app registration and authentication](#) (Microsoft Azure 应用程序注册和身份验证)

1. If 正在使用显式资源组进行操作，然后在该资源组的范围内使用以下权限： 

## 打印

April 18, 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。

要了解有关在 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）环境中打印的完整信息，请先阅读[打印](#)。阅读完该文章后，您可以继续阅读以下文章：

- [打印配置示例](#)
- [最佳做法](#)
- [打印策略和首选项](#)
- [置备打印机](#)
- [维护打印环境](#)

### 在打印服务器上安装通用打印服务器

1. 确保每个打印服务器都安装了 Microsoft Virtual C++ Runtime 2017 32 位和 64 位。
2. 导航到 Citrix 通用打印服务器 [下载页面](#)并单击 下载文件。
3. 在各个打印服务器上运行下列其中一个命令：

- 对于 32 位操作系统：**UpsServer\_x86.msi**。
- 对于 64 位操作系统：**UpsServer\_x64.msi**。

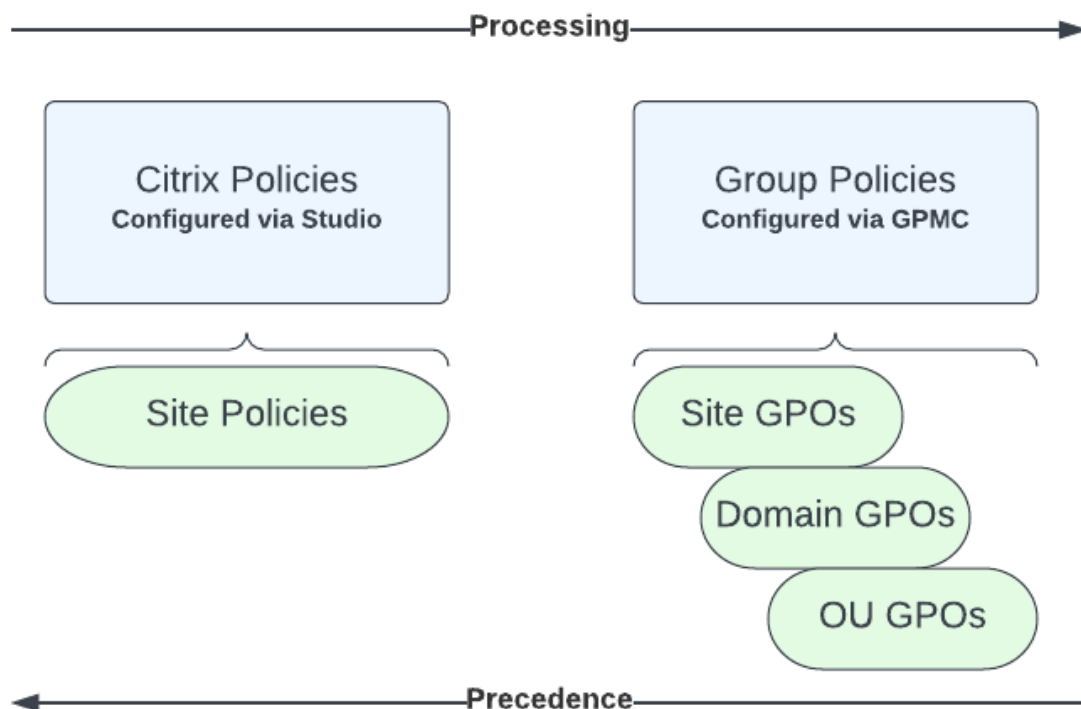
安装通用打印服务器后，请按照[预配打印机](#)中的指南进行配置。

## 策略

April 11, 2023

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。

您可以将策略设置应用于 VDA 或用户。您可以在 Web Studio 或 Active Directory 组策略对象 (GPO) 中编辑设置。您可以为策略指定过滤器（对象分配）。如果您没有专门为筛选器分配策略，则设置将应用于所有用户会话。



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 级别的策略会覆盖站点组策略对象级别的策略。站点组策略对象级别会覆盖 Microsoft 和 Citrix 本地策略级别上存在冲突的所有策略。

所有 Citrix 站点策略均在 Web 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。

Web Studio 使用建模向导来帮助管理员比较模板和策略中的配置设置，以帮助消除冲突和冗余的设置。

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。

Web Studio 策略还可能与 Active Directory 中的组策略发生冲突，后者可能会根据情况相互覆盖。

所有策略按照以下顺序处理：

1. 在 Citrix Workspace 应用程序中，最终用户使用域凭据登录 VDA。
2. Citrix 策略是为最终用户和 VDA 处理的
3. 策略按以下顺序应用：
  - a) 本地策略
  - b) 站点策略

- c) 域策略
- d) OU（组织单位）策略

注意：

- 并非所有策略都存在于四个级别。对于大多数客户，仅使用站点策略。本地策略要求用户登录 VDA 才能编辑策略。因此，这些策略几乎从未被使用过。
- 我们不支持在同一个 GPO 中混合使用 Windows 策略和 Citrix 策略。

有关 Citrix 策略的完整信息，请参阅以下内容：

- [使用策略](#)
- [策略模板](#)
- [创建策略](#)
- [对策略进行优先排序、建模、比较和故障排除](#)
- [默认策略设置](#)
- [策略设置参考](#)

注意：

Citrix DaaS 的策略设置引用与 Citrix Virtual Apps and Desktops 策略设置相同。因此，您也可以参阅 Citrix DaaS 的 Citrix Virtual Apps and Desktops 文档中的[策略设置参考](#)部分。

## 使用策略

May 19, 2023

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

- Studio-使用 Studio 创建的策略存储在站点数据库中，更新将推送到 VDA，以下任一情况发生：
  - 当该 VDA 向控制器注册时
  - 当用户启动会话时
- 组策略管理控制台-如果您的网络环境使用 Active Directory 并且您有权管理组策略，则可以使用组策略管理控制台 (GPMC) 为站点创建和编辑策略。在控制台中，您可以使用所需的设置和筛选器配置组策略对象 (GPO)。这些策略的优先级将高于 Studio 中配置的策略。有关详细信息，请参阅 [CTX238166](#)。



### 策略处理顺序和优先级

组策略设置的处理顺序如下：

1. Citrix DaaS 站点 GPO（存储在站点数据库中）
2. 域级 GPO
3. 组织单位

但是，如果在两个 GPO 中对同一个策略应用不同的设置，则上次处理的策略设置将覆盖之前处理的设置。此配置意味着策略设置的优先级顺序如下：

1. 组织单位
2. 域级 GPO
3. Citrix DaaS 站点 GPO（存储在站点数据库中）

使用多个策略时，可以向包含冲突设置的策略分配优先级。有关详细信息，请参阅[对策略进行优先排序、建模、比较和故障排除](#)。

### Citrix 策略 workflow

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。根据客户请求，在 Citrix Cloud 托管的 Web Studio 中可用“建模”选项卡

### 导航 Citrix 策略和设置

策略设置根据其所影响的功能或特性分为几类。例如，Profile Management 部分包含用于 Profile Management 的策略设置。

- 计算机设置（应用于计算机的策略设置）定义虚拟桌面的行为并在虚拟桌面启动时应用。即使虚拟桌面上没有活动的用户会话，也会应用这些设置。
- 用户设置定义用户体验。用户设置在用户连接或重新连接时应用

要访问策略、设置或模板，请在 Web Studio 导航窗格中选择 策略。

- 策略选项卡列出所有策略。选择策略时，底部会显示以下选项卡：
  - 概述-列出名称、优先级、启用/禁用状态和描述
  - 设置-列出所有已配置的设置
  - 分配给-列出交付组。您可以编辑或删除分配给设置。根据运行会话的桌面的交付组成员身份应用策略。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。当您选择模板时，底部的选项卡会显示：
  - 说明（您可能想使用模板的原因）
  - 设置（已配置的设置列表）。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这些设置进行比较。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[对策略进行优先排序、建模、比较和故障排除](#)。
  - 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[对策略进行优先排序、建模、比较和故障排除](#)。

要搜索策略或模板中的设置，请执行以下操作：

1. 选择策略或模板。
2. 选择 编辑策略 或 编辑模板 选项卡。
3. 在“选择设置”页面上，开始键入设置的名称。

可以通过选择以下选项来优化搜索：

- 类别（例如，带宽）
  - “仅查看选定项”复选框
  - 仅搜索已添加到选定策略的设置。
- 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，并键入设置的名称。

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。

## 策略模板

November 11, 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..”。
- 与 Citrix 支持人员或可信第三方沟通策略的方法。您可以通过导入或导出模板来实现。

## 内置 Citrix 模板

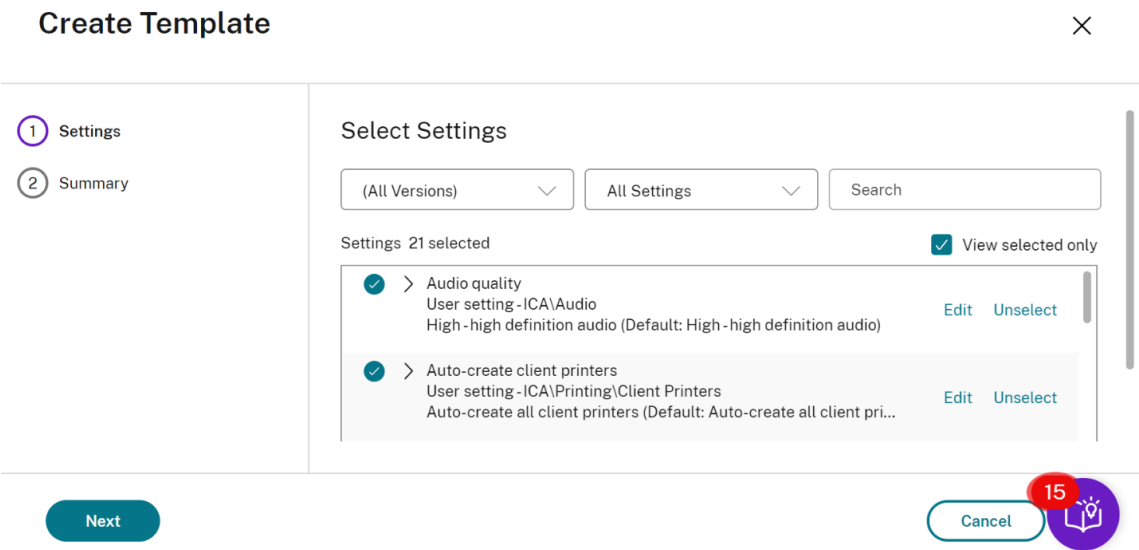
以下策略模板可用：

- 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。
- 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。它提供了良好的用户体验，同时增加了您可以在单个服务器上托管的用户数量。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。此模板适用于分支机构中使用共享广域网或具有低带宽连接的远程位置的任务工作人员。工作人员使用图形上简单的用户界面和很少的多媒体内容访问应用程序。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。在风险容忍度较低的环境中使用此模板，以最大限度地减少 Citrix DaaS 中默认启用的功能。此模板包含禁止访问以下内容的设置：
  - 打印
  - 剪贴板
  - 外围设备
  - 驱动器映射
  - Port redirection（端口重定向）
  - 用户设备上的 Flash 加速

应用此模板可能会占用更多带宽并降低每个服务器的用户密度。

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。

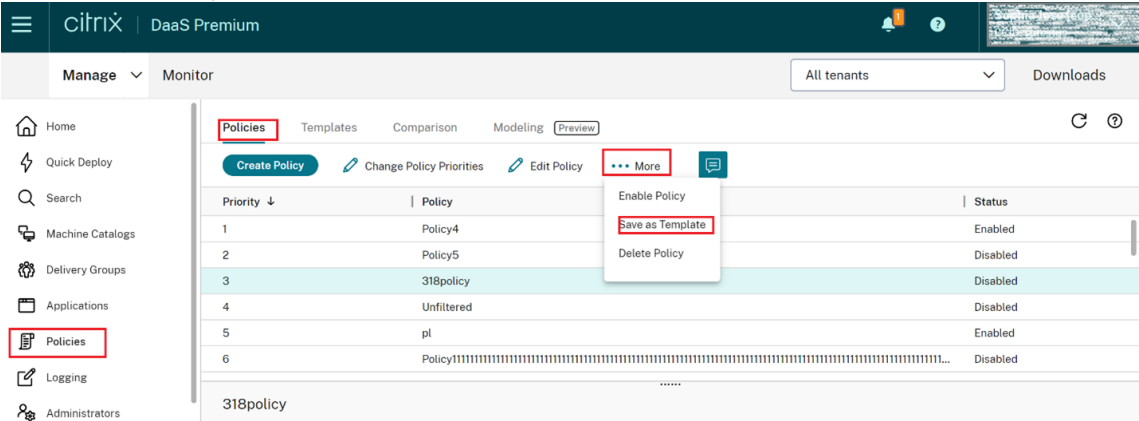




4. 选择并配置要包含在新模板中的策略设置。
5. 单击下一步。此时将显示摘要屏幕。
6. 为新模板输入一个名称。
7. 单击完成。新模板显示在“模板”选项卡上

要基于策略创建模板，请执行以下操作：

1. 在 Web Studio 导航窗格中选择策略。
2. 选择“策略”选项卡，然后选择用于创建模板的策略。



3. 单击“更多”选项卡。
4. 选择“另存为模板”。此时将显示选择设置屏幕。

Save as Template

318policy

1 Settings

2 Summary

Select Settings

(All Versions)All SettingsSearch

Settings 2 selectedView selected only

Accelerate folder mirroring  
Computer setting - Profile Management\File system\Synchronization  
Disabled (Default: Disabled)

EditUnselect

Active Directory actions  
Computer setting - Profile Management\Log settings  
Disabled (Default: Disabled)

EditUnselect

Next

Cancel

15

5. 选择并配置要包含在模板中的任何新策略设置。
6. 单击下一步。此时将显示摘要屏幕。

Save as Template

318policy

Settings

2 Summary

Summary

View a summary of the settings you configured and provide a name for your new custom template.

Template name:Example: High Performance Template

Description:

318policy

Accelerate folder mirroring

Back

Finish

Cancel

15

7. 输入模板的名称和说明，然后单击完成。

创建策略

October 26, 2023

创建策略前，确定可能会受此策略影响的用户或设备组。您可能希望创建基于用户工作职责、连接类型、用户设备或地理位置的策略。

如果您已经创建了应用到某个组的策略，请考虑编辑该策略，而非创建其他策略。编辑策略后，请配置相应的设置。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，可以在策略模板中的设置基础上进行创建，并根据需要对设置进行自定义。也可以在不使用模板的情况下进行创建，并添加所需的所有设置。

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”。

在创建策略和配置设置时，系统会提供查看设置类型的选项。您可以查看以下设置类型：

- 所有设置 - 查看所有 VDA 版本的所有设置
- 仅限当前设置 - 仅查看当前 VDA 版本的设置
- 仅限旧版设置 - 仅查看已弃用的 VDA 版本的设置

要在配置设置时查看设置，请执行以下操作：

1. 登录 DaaS Premium。
2. 在左侧导航栏中，单击“策略”。
3. 在“策略”选项卡中，单击“创建策略”。
4. 在“选择设置”表中，单击“设置”旁边的下拉列表。
5. 从下拉列表中选择以下选项之一：
  - 所有设置 - 查看所有 VDA 版本的所有设置
  - 仅限当前设置 - 仅查看当前 VDA 版本的设置
  - 仅限旧版设置 - 仅查看已弃用的 VDA 版本的设置
6. “设置”表列出了基于上一步的可用设置。

## 策略设置

策略设置的状态可以是已启用、已禁用或未配置。默认情况下，未配置策略设置，这意味着它们未添加到策略中。仅在将设置添加到策略时才会应用这些设置。

在配置用于创建或编辑策略的设置时，如果禁用了所有交付组，则系统会显示“此筛选器中的所有元素均未启用”警告通知标志。如果启用了至少一个交付组，则系统不会显示警告标志。

要在创建策略时查看警告，请执行以下操作：

1. 登录 DaaS Premium。
2. 在左侧导航栏中，单击“策略”。
3. 在“策略”选项卡中，单击“创建策略”。
4. 在“选择设置”表中，选择任意设置，然后单击“下一步”。
5. 在“将策略分配给”表中，从下拉列表选择一个筛选器。
6. 取消选中“启用”复选框并单击“保存”。

注意：

并非所有筛选器都支持取消选中“启用”复选框。

在“过滤器”表中，过滤器会显示警告。

要在编辑策略时查看警告，请执行以下操作：

1. 登录 DaaS Premium。
2. 在左侧导航栏中，单击“策略”。
3. 在“策略”选项卡中，选择列出的任意策略，然后单击“编辑策略”。
4. 在“编辑策略”页面中，单击左侧导航栏中的“将策略分配给”。
5. 在“筛选器”表中，为所需的筛选器选择或单击“编辑”：
  - 如果筛选器没有“编辑”按钮，请选择该过滤器。
  - 如果筛选器有编辑按钮，请单击“编辑”。
6. 取消选择“启用”选项，然后单击“保存”。

注意：

并非所有筛选器都支持取消选中“启用”复选框。

在“过滤器”表中，过滤器会显示警告。

某些策略设置可处于以下状态之一：

- 1 - Allowed or Prohibited allows or prevents the action controlled by the setting. Sometimes users are allowed or prevented from managing the setting's action in a session. For example, **if** the menu animation setting is set to Allowed, users can control menu animations in their client environment
- 2 - Enabled or Disabled turns the setting on or off. If you disable a setting, it is not enabled in lower-ranked policies.

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。必须将此设置和 客户端网络驱动器 设置都添加到策略中，以允许用户访问其网络驱动器。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。

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。此选择禁用设置的配置，只允许在应用策略时使用设置的默认值。无论在选择使用默认值之前输入的值为何，均会出现这种选择。

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。
- 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。

如果您未指定任何分配，或者指定了分配但将其禁用，策略将应用到所有连接。

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：

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。
Citrix SD-WAN	用户会话是否通过 Citrix SD-WAN 启动。注意：您只能向策略添加一个 Citrix 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。
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。

分配名称	应用策略的根据
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。

- 如果您使用 Web Studio 管理 Citrix 策略，则添加到“未过滤”策略的设置将应用于站点中的所有服务器、桌面和连接。
- 站点和连接必须在包含策略的组策略对象 (GPO) 的范围内。例如，Sales OU 包含名为 Sales-US 的 GPO，该 GPO 包含美国销售团队的所有成员。该 Sales-US GPO 是使用包含多项用户策略设置的“未过滤”策略进行配置的。当美国的销售经理登录到站点时，“未过滤”策略中的设置将自动应用到该会话。此配置是因为用户是 Sales-US GPO 的成员。

分配模式决定策略是否仅应用于匹配所有分配标准的连接。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 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”。

当销售经理从办公室登录网站时，由于连接不符合 Assignment F 的要求，因此该策略不适用。

## 策略集（预览版）

November 16, 2023

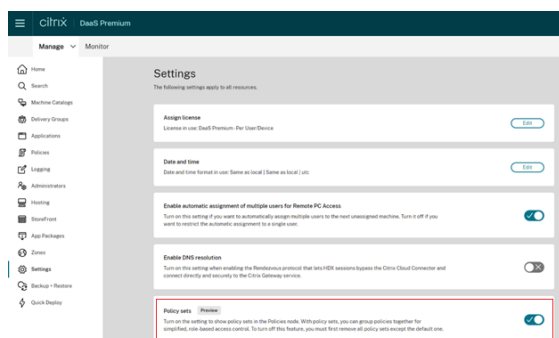
策略集是 Citrix DaaS 中的对象，它聚合策略以实现简化、基于角色的访问和轻松管理。您可以创建策略集来反映管理员团队和公司中的逻辑分区。例如，您可以为每个地理区域、业务部门或特定用例创建策略集。创建后，范围和交付组将分配给策略集，因此只有经过授权的管理员才能管理适用于其相关用户和计算机的策略。

### 优势

- 分布式管理员团队基于角色的访问控制
- 简化的合并、收购和整合
- 有限的故障域
- 对策略的多租户支持

### 启用策略集

在 Citrix DaaS 的“管理”选项卡中，导航到“设置”，然后打开“策略集”设置。



注意：

在创建策略集之前，必须启用策略集。

### 功能比较

在应用策略集之前

整个站点的策略、设置、筛选器和策略优先级在 Citrix Studio 中的一个位置进行配置。

如果您管理一个策略，则必须管理每个策略。

大型分布式环境中的策略变得复杂且难以管理。

应用策略集之后

策略、设置、过滤器和策略优先级是为每个策略集单独配置的。

完全管理员可以将个人管理特定策略的权限委托给较低级别的管理员。

大型和分布式环境中的策略可以轻松划分和管理。

策略集是如何运作的

一般概述

- 策略集已分配给交付组
- 策略集具有一个或多个范围
- 未分配策略集的交付组将接收默认策略集
- 一个交付组只能分配一个策略集
- 多个交付组可以使用相同的策略集
- 尽管策略集已分配给交付组，但策略仍会保留其过滤器

默认策略集

- 启用策略集设置后，所有现有策略都将分组到默认策略集中
- 除非管理员团队创建策略集并将其分配给交付组，否则每个交付组都会收到默认策略集。
- 为交付组分配了不同的策略集后，它将不再从默认策略集获取策略

策略集创建

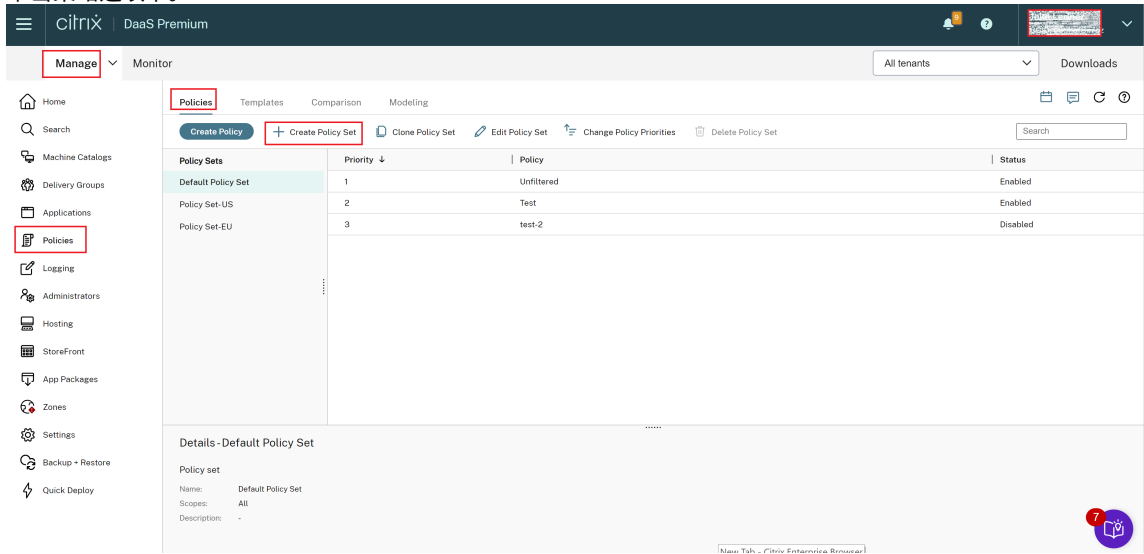
可以通过以下两种方式创建策略集：

- 创建策略集-此操作会创建空策略集
- 克隆策略集-此操作基于现有策略集创建策略集

创建策略集

1. 在 Citrix DaaS 配置页面上，单击“管理”选项卡。

2. 单击策略选项卡。



3. 选择“创建策略集”。将出现“简介”选项卡。
4. 单击“下一步”或单击“名称和描述”选项卡。
5. 输入策略集的名称和描述。
6. 单击“下一步”或单击“任务”选项卡。
7. 选择要向其分配策略集的一个或多个交付组。
8. 单击“下一步”或单击“范围”选项卡。
9. 选择策略集的范围。
10. 单击 **Create**（创建）。策略集是使用定义的分配和范围创建的。

克隆策略集

1. 在 Citrix DaaS 配置页面上，单击“管理”选项卡。
2. 单击策略选项卡。
3. 选择“克隆策略集”。
4. 修改策略集的名称。
5. 修改或创建策略集的分配，然后单击“下一步”。
6. 选择或取消选择要包含在克隆策略集中的策略。
7. 修改策略的范围。
8. 单击 **Create**（创建）。策略集已创建。

编辑策略集

1. 在 Citrix DaaS 配置页面上，单击“管理”选项卡。
2. 单击策略选项卡。
3. 选择“编辑策略集”。
4. 修改策略集的名称，然后单击“下一步”。

5. 修改或创建策略集的分配，然后单击“下一步”。
6. 修改策略的范围。
7. 单击 **Create**（创建）。

### 策略集分配

策略集已分配给交付组。您可以在创建或编辑策略集时配置分配。您还可以在创建或编辑交付组时配置任务。

### 策略集范围

管理员可以定义策略集的范围，以便只有经过授权的管理员才能查看或编辑策略集。在创建或编辑策略集时，您可以配置范围。

## 对策略进行优先排序、建模、比较和故障排除

June 1, 2023

您可以根据以下内容使用策略自定义环境以满足用户的需求：

- 工作职能
- 地理位置
- 连接类型

例如，为了提高安全性，对经常与敏感数据交互的用户组设置限制。

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。您可以为用户组中需要访问其本地驱动器的用户创建其他策略。然后，您可以对这两个策略进行排名，以控制哪个策略优先。使用许多策略时，必须确定：

- 如何确定策略的优先级
- 如何创建异常
- 在政策冲突时如何查看有效的策略

### 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。当用户登录系统时，就会识别与连接分配相匹配的所有策略。已识别的策略及其关联设置按优先级顺序排序。根据策略的优先级应用每个设置。

您可以通过在 **Web Studio** 中为策略指定不同的优先级编号来确定策略的优先级。默认情况下，新策略的优先级最低。如果策略设置之间存在冲突，则优先级较高的策略会覆盖优先级较低的策略。优先级编号为 1 的策略是最高优先级的策略。策略设置根据以下内容进行合并：

- 策略的优先级
- 策略的过滤器中指定的条件

要确定策略的优先级，请执行以下步骤：

1. 在左侧窗格中选择策略。
2. 在“策略”选项卡上，选择操作栏中的“更改策略优先级”。此时将出现“更改策略优先级”页面。
3. 在优先级列表中，使用以下方法更改策略的优先级：
  - 将策略拖动到所需位置。
  - 要将其向上或向下移动一个位置，请分别单击向上或向下箭头图标。
  - 要将其移至列表的顶部或底部，请分别单击“顶部”或“底部”箭头图标。
  - 要更改优先级编号，请单击“编辑”图标，根据需要输入数字，然后单击“保存”。
4. 单击保存。

## 例外

当您创建策略并使用筛选器将其分配给用户组、用户设备或计算机时，您可能会发现组中的某些成员需要对某些策略设置进行例外。可以通过以下方式创建例外情况：

- 仅为需要例外的特定群组成员创建策略，然后将该策略的排名高于整个群组的策略
- 对添加到策略的分配使用“拒绝”模式

模式设置为“拒绝”的分配仅将策略应用于与分配标准不匹配的连接。例如，策略包括以下分配：

- 分配 A 是指定范围 208.77.88.\* 的客户端 IP 地址分配。该模式设置为“允许”。
- 分配 B 是指定特定用户帐户的用户分配。模式设置为“拒绝”。

该策略适用于使用 IP 地址在分配 A 中指定的范围内登录站点的所有用户。但是，该政策不适用于使用任务 B 中指定的用户帐户登录网站的用户。

### 注意：

在“分配策略”步骤中，如果取消选中“启用”复选框，则会禁用策略的分配。如果禁用了策略的唯一分配，则等同于没有任何分配，因此，该策略适用于站点中的所有对象。

## 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。您可以计算策略的结果集并确定如何合并连接的最终策略设置。

您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 模拟连接场景并辨别如何应用 Citrix 策略。可以为连接方案指定条件，例如：

- 用户
- Citrix 策略分配证据值

- 使用 组策略结果 创建报告，描述对给定用户和 Virtual Delivery Agent (VDA) 生效的 Citrix 策略。

当您从组策略 管理控制台运行 Citrix 组策略建模向导时，使用 **Web Studio** 创建的站点策略设置不包含在策略结果集中。为了验证您是否获得了最全面的策略结果集，Citrix 建议从 **Web 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。

## 使用策略建模向导

策略建模可帮助您使用用于规划和测试目的的过滤器来模拟已启用的策略。只有启用了过滤器的策略才会被建模。永远不会应用禁用的策略，并且始终应用不带过滤器的已启用的策略。

执行以下步骤打开策略建模向导：

1. 在“完整配置”中，选择“策略”。
2. 选择“建模”选项卡。
3. 在操作栏中选择 策略建模。
4. 阅读简介页面，然后单击“下一步”。
5. 选择用户或计算机。您可以浏览容器或特定用户或计算机。单击下一步。
6. 选择您的过滤证据。您可以选择通过输入其他详细信息（例如交付组、标记、客户端 **IP** 地址等）来更精细地进行模拟。单击下一步。
7. 查看您的选择摘要，然后单击“运行”。

单击“运行”后，向导会生成建模结果报告。在查看此报告时，您可以：

- 选择是否要在下拉菜单中查看“所有设置”、“计算机设置”或“用户设置”。
- 使用搜索栏查找特定设置。
- 单击特定设置可查看该设置的详细信息。例如，如果所有用户设置均未应用于特定策略，则详细信息窗格会向您显示未应用这些设置的原因。
- 单击“导出”，以 JSON 格式或 HTML 格式导出建模结果。

运行策略建模后，您可以使用更多选项。您可以：

- 查看建模报告：这将从上面打开相同的建模报告，因此您可以再次查看或导出它。
- 重新运行策略建模：这允许您使用先前选择的相同标准集重新运行策略建模并生成新的建模结果。如果某些政策已更改，并且您想看看这些更改如何影响您当前的模型，这将很有用。
- 删除建模报告：这将删除当前的建模报告。

## 比较策略和模板

您可以将策略或模板中的设置与其他策略或模板的设置进行比较。例如，您可能需要验证设置值以保持符合最佳实践。您可能还需要将策略或模板中的设置与默认设置进行比较。



1. 在 **Web 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。要在比较中包括默认值，请选中“与默认设置比较”复选框。
4. 单击“比较”后，配置的设置将显示在列中。
5. 要查看所有设置，请选择“显示所有设置”。要返回默认视图，请选择“显示常用设置”。

## 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，这种情况会导致出现冲突。运行 **Citrix** 组策略建模向导时，您可能会发现没有任何策略适用于用户连接。在这种情况下，策略设置不适用于在符合策略评估标准的条件下连接到其应用程序和桌面的用户。这种情况发生在以下情况下：

- 没有任何策略的分配与策略的评估标准相匹配。
- 与分配相匹配的策略未配置任何设置。
- 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。

### 注意：

在双跳场景的第二跳中，请考虑单会话操作系统 VDA 连接到多会话操作系统 VDA。在这种情况下，Citrix 策略在单会话操作系统 VDA 上起作用，就好像它是用户设备一样。例如，请考虑将策略设置为在用户设备上缓存图像。在此示例中，在双跳场景中为第二跳缓存的图像缓存在单会话操作系统 VDA 计算机上。

## Director

非管理员可以使用 Director 查看适用于用户会话的策略。

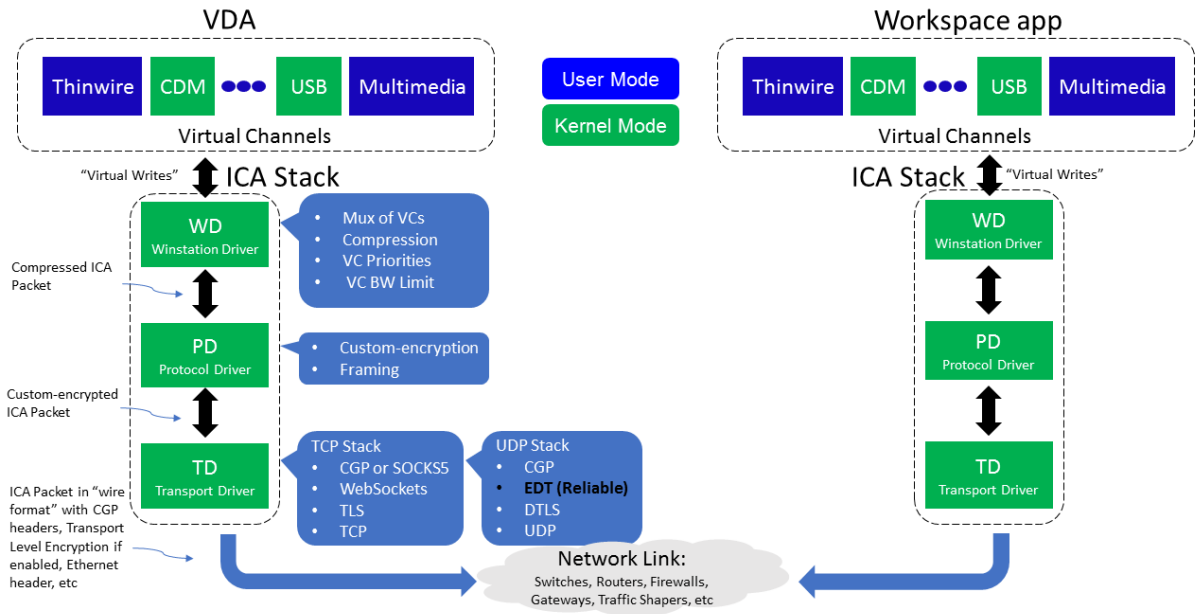
## HDX 概述

November 16, 2023

### 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。

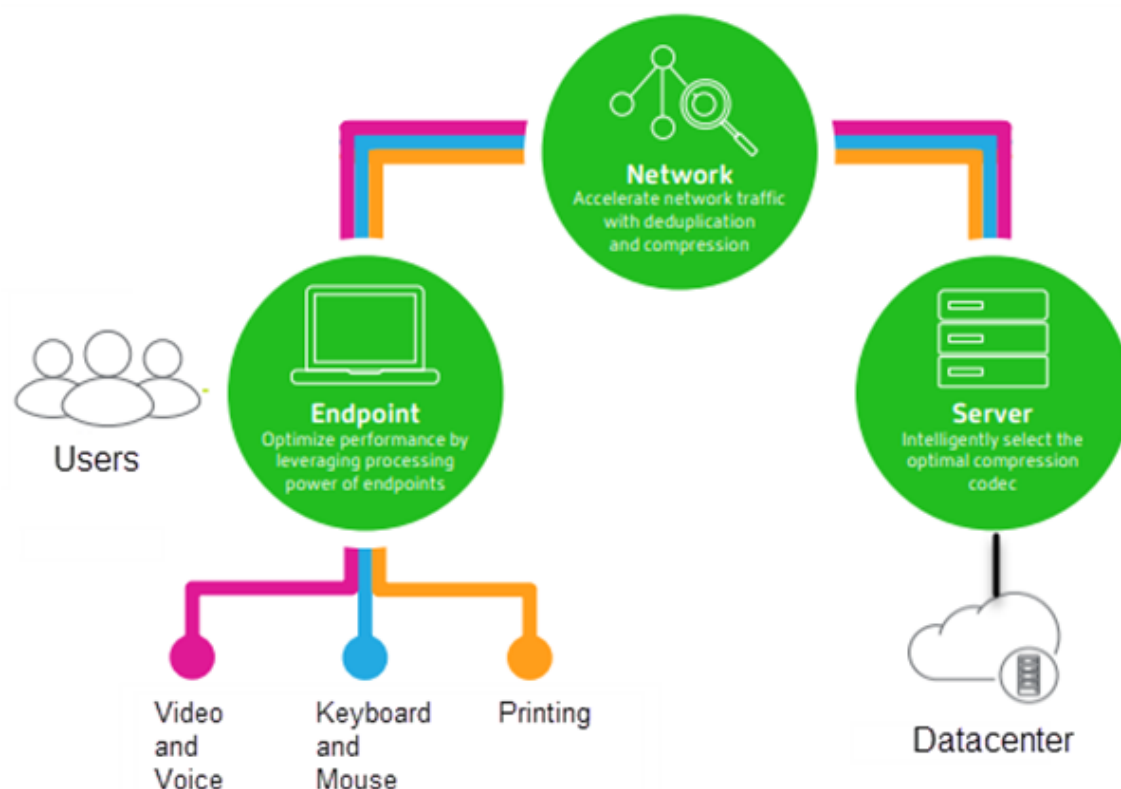


HDX 围绕三个技术原则设计：

- 智能重定向
- 自适应压缩
- 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 通道监视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。

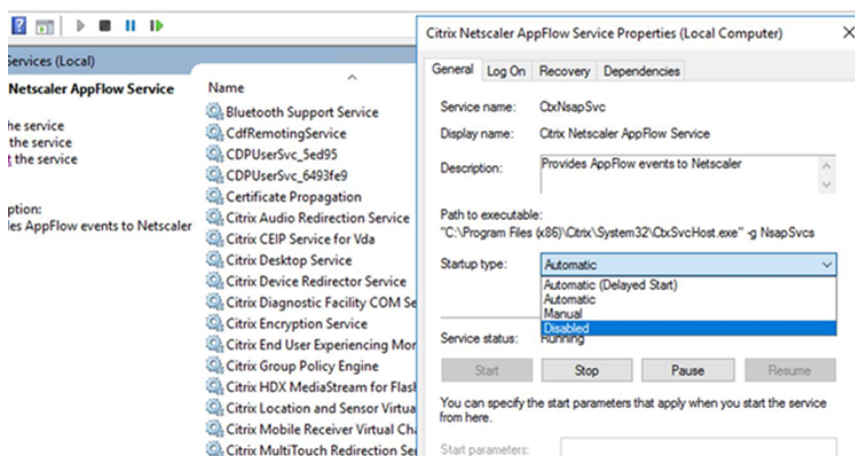
可以允许 NetScaler 使用 HDX Insight 虚拟通道移动所有未压缩格式的必需数据点。如果禁用此功能，NetScaler 设备将跨多个虚拟通道解密并解压缩 ICA 通信。使用单个虚拟通道降低了复杂性，增强了可扩展性，并且更具成本效益。

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）。



## 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。
- 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。

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缓冲区智能地调整 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。
- 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 DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）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，请向注册表项添加以下 DWORD 注册表项值：HKCU\Software\Citrix\HdxRealTime: 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。

安装在 Windows 10 和 Windows 8 计算机上的 Virtual Delivery Agent (VDA) 支持多通道流媒体连接。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。

### 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，请在策略中添加以下 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 Branch Repeater 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。

### 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。

## Citrix ICA 虚拟通道

March 5, 2024

### 警告：

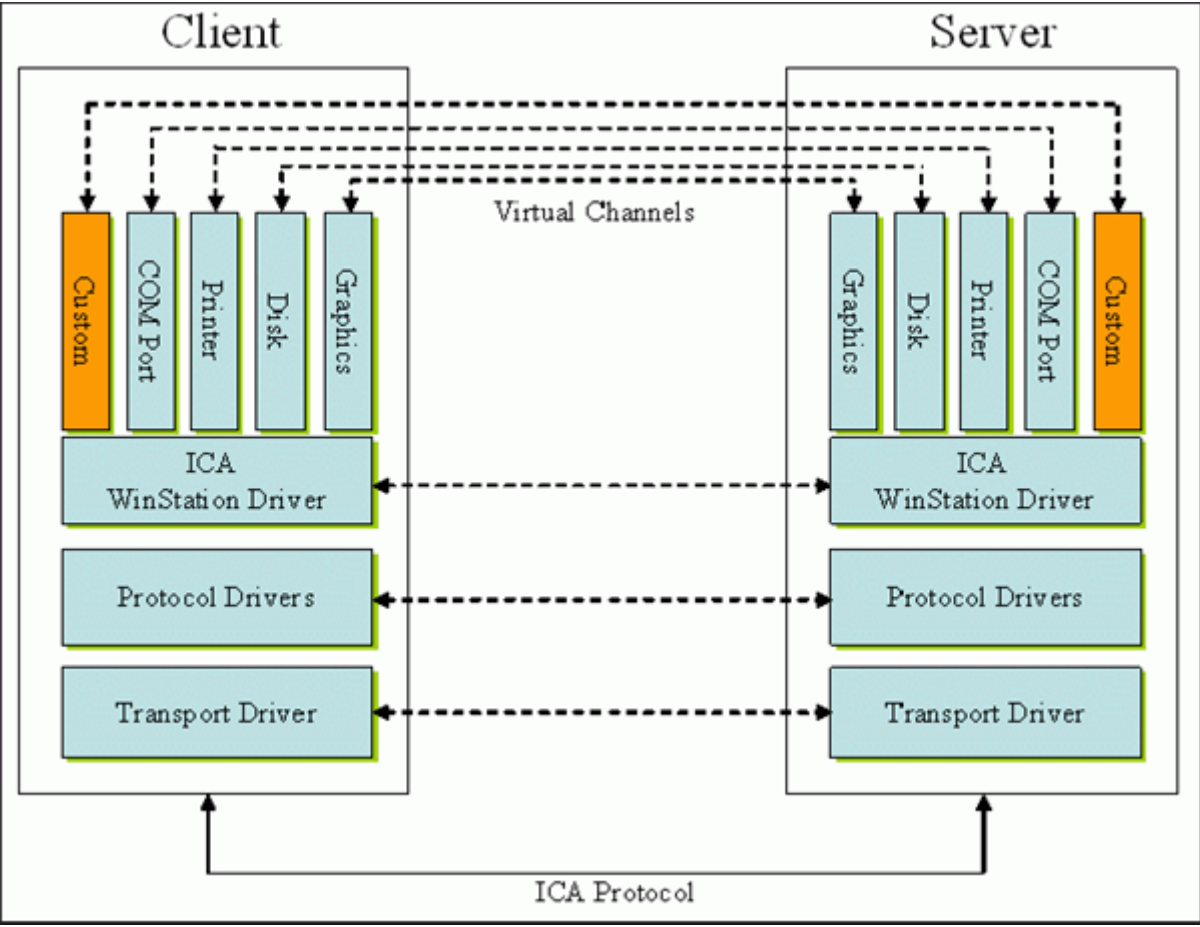
注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当而导致的问题能够得到解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

## ICA 虚拟频道是什么

Citrix Workspace 应用程序与 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）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 DaaS 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 Citrix DaaS 和 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 DaaS 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
- 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
- vdmtn.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

## 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
- Icausb.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 XenDesktop 7.0 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。

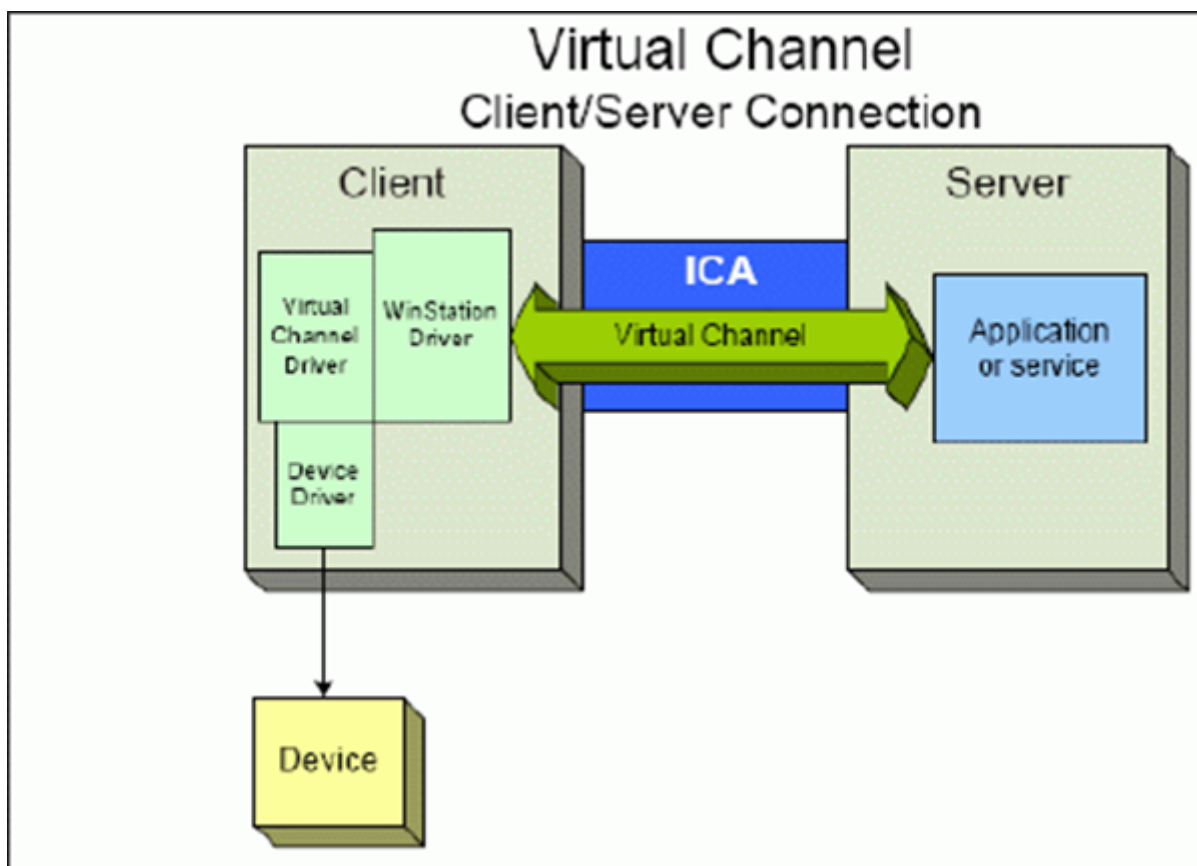
在 **Windows** 服务中托管专业通道

在 Citrix DaaS 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：

- 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 ICA Status Channel Service

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 DaaS 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。
  - 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

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 DaaS 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。

重要提示：

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。

有关详细信息，请参阅 [Client Object API Specification Programmer's Guide](#)（《客户端对象 API 规范程序员指南》）。

### 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
- 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

重要提示：

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。

### 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
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

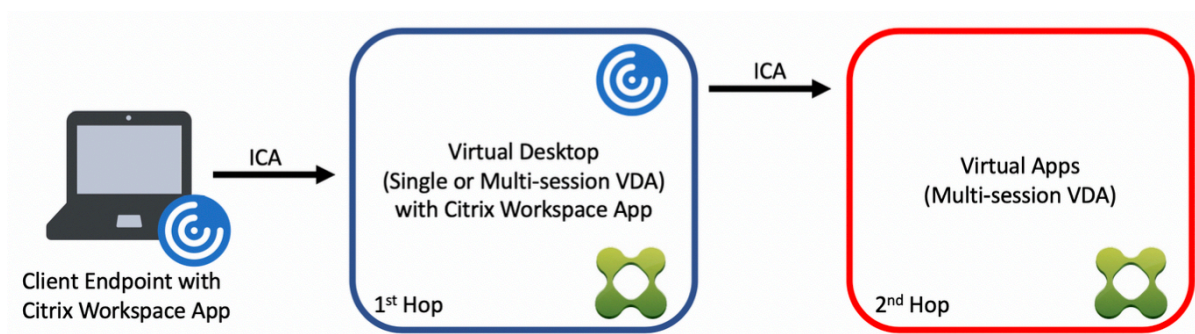
- [ICA 虚拟通道 SDK](#)

- [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 DaaS 中的双跃点

April 18, 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 DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）版本都支持双跃点。

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](#)。

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](#)

## HDX 传输

April 21, 2023

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
- 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。

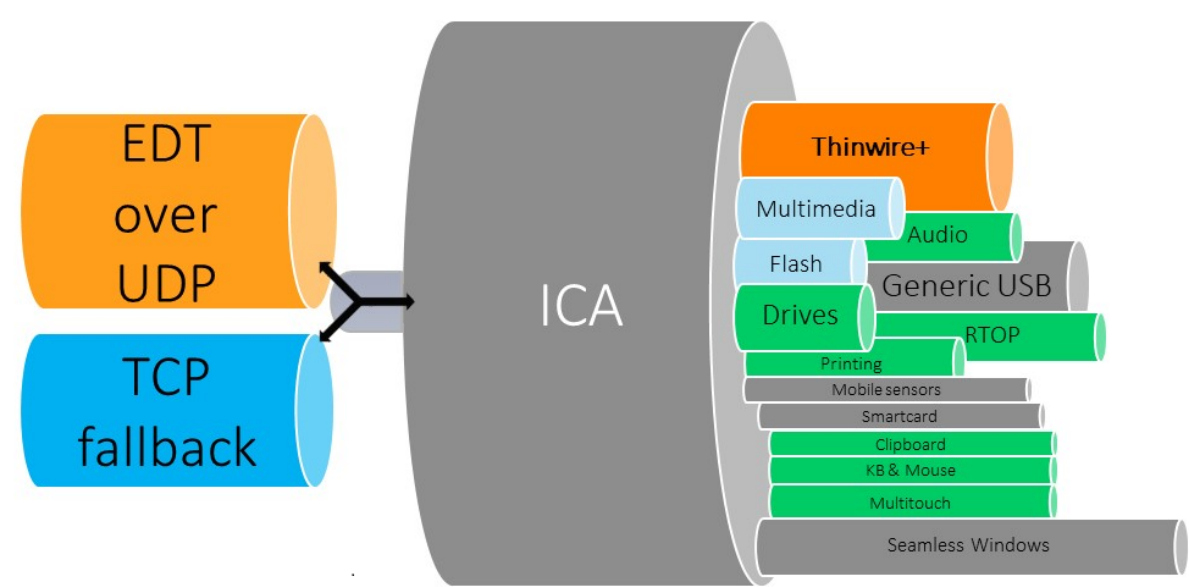
在 HDX 产品中，您可以通过独特的专有传输协议进行连接，并在使用 Citrix Gateway Service 时使用 Rendezvous 协议进行连接。

## 自适应传输

January 23, 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) 或 EDT Lossy 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。

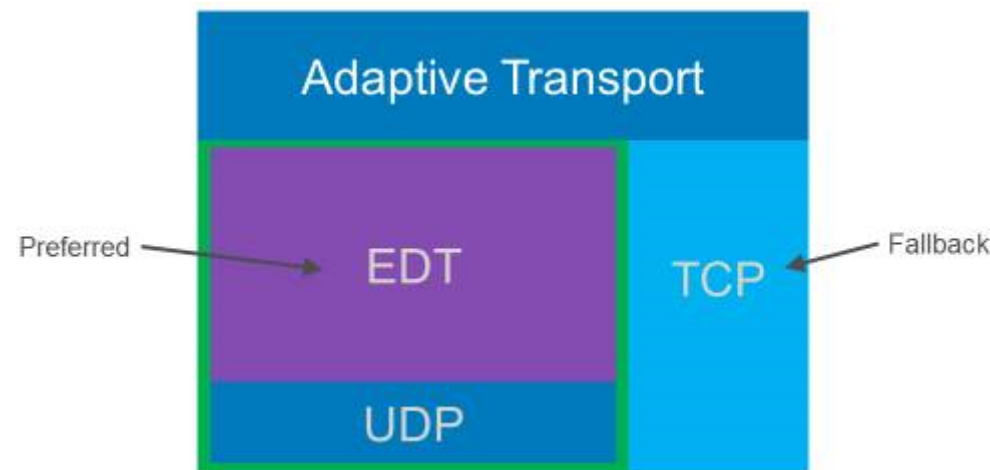
EDT 是基于用户数据报协议 (UDP) 构建的 Citrix 专有传输协议。它在保持服务器可扩展性的同时，在具有挑战性的长途连接方面提供了出色的用户体验。EDT 提高了不可靠网络中所有 ICA 虚拟通道的数据吞吐量，从而提供更出色、更一致的用户体验。



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
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 1912 或更高版本
- Virtual Delivery Agent
  - 版本 1912 或更高版本（建议使用 2203 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（仅在部署中使用时适用）
  - 版本 3.12.x
  - 版本 1912.0.x
- Citrix Workspace 应用程序
  - Windows：版本 2105 或更高版本
  - Linux：版本 2109 或更高版本
  - Mac：版本 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)
  - 13.1.17.42 或更高版本（推荐）
  - 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。

## 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](#)。



Session Details

Session Control ▾

Shadow

Send Message

ID	2
Session State	Active
Application State	Desktop
Anonymous	No
Time in state	0 minutes
Endpoint name	
Endpoint IP	
Connection type	HDX
Protocol	UDP
Citrix Workspace App Version	21.5.0.48
ICA RTT	67 ms
ICA Latency	65 ms
Launched via	n/a
Connected via	

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）

```

Administrator: Windows PowerShell
PS C:\windows\system32> ctxsession -v

Session Id 2:
Transport Protocols: UDP -> DTLS -> CGP -> ICA
  Local Address:
  Remote Address:
  Client Address:
Security Protocol: UNKNOWN VALUE - 131072
Security Cipher: 128 bit AES
Cipher Strength: 128 bits
ICA Encryption: Basic

EDT Reliable Statistics:
Bandwidth 121.777 Mbps, Send Rate 0 bps, Recv Rate 0 bps, RTT 65.531 ms
Sent 0, Sent Lost 0 (0.00%), Rcvd 0, Rcvd Lost 0 (0.00%)
Sent ACKs 0, Sent NAKs 0, Rcvd ACKs 0, Rcvd NAKs 0
Flow Window 16383, Congest Window 4050, Delivery Rate 7591
EDT MTU: 1400

ICA Statistics:
SentBandwidth (bps) = 6376 RecvBandwidth (bps) = 568
SentPreCompression = 1800688 RecvPreExpansion = 32864
SentPostCompression = 1429125 RecvPostExpansion = 137041
Compression Ratio % = 79 Expansion Ratio % = 23
LastLatency = 67 AverageLatency = 53
IcaBufferLength = 980
  
```

## 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。

### 重要：

- 必须启用会话可靠性才能使 MTU 发现正常工作。
- 带多流 ICA 的 MTU Discovery 在 VDA 版本 2209 及更高版本中可用。

## 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。

## 丢失容忍模式

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。您可以使用[容丢模式](#)和[容错阈值](#)设置禁用该功能或调整丢包和延迟阈值。

重要：

- 必须启用会话可靠性才能使容损模式正常工作。
- 容损模式仅适用于适用于 Windows 的 Citrix Workspace 应用程序。
- 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。

## 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。
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。

## Rendezvous 协议

September 1, 2023

使用 Citrix Gateway 服务时，Rendezvous 协议允许 VDA 绕过 Citrix Cloud Connector，以直接安全地连接到 Citrix Cloud 控制平面。

有两种类型的流量需要注意：

1. VDA 注册和会话代理的控制流量。
2. HDX 会话流量。

有两种版本的 Rendezvous 可用：

- 版本 1 (V1)：仅支持绕过用于 HDX 会话流量的 Citrix Cloud Connector。
- 版本 2 (V2)：支持绕过用于控制流量和 HDX 会话流量的 Citrix Cloud Connector。

有关每个 Rendezvous 版本的系统要求、注意事项和配置的详细信息，请查看各自的文档。

[Rendezvous V1 文档](#)

[Rendezvous V2 文档](#)

## Rendezvous V1

April 21, 2023

使用 Citrix Gateway 服务时，Rendezvous 协议允许 VDA 绕过 Citrix Cloud Connector，以直接安全地连接到 Citrix Cloud 控制平面。

### 要求

- 使用 Citrix Workspace 和 Citrix Gateway 服务访问环境。
- 控制平面：Citrix DaaS (Citrix Cloud)。
- VDA：1912 或更高版本。
  - 版本 2012 是 EDT Rendezvous 所需的最低版本。
  - 版本 2012 是非透明代理支持所需的最低版本（不支持 PAC 文件）。
  - 版本 2103 是使用 PAC 文件进行代理配置所需的最低版本。
- 在 Citrix 策略中启用 Rendezvous 协议。有关详细信息，请参阅 [Rendezvous 协议策略设置](#)。
- VDA 必须对 [https://\\*.nssvc.net](https://*.nssvc.net) 具有访问权限，包括所有子域。如果无法通过该方式将所有子域添加到允许列表中，请该为使用 [https://\\*.c.nssvc.net](https://*.c.nssvc.net) 和 [https://\\*.g.nssvc.net](https://*.g.nssvc.net)。有关详细信息，请参阅 Citrix Cloud 文档（在 Citrix DaaS 下）的 [Internet 连接要求](#) 部分和知识中心文章 [CTX270584](#)。

- VDA 必须能够分别连接到上文 TCP Rendezvous 和 EDT Rendezvous 的 TCP 443 和 UDP 443 中提到的地址。
- 在代理会话时，Cloud Connector 必须获取 VDA 的 FQDN。通过以下两种方式之一完成此任务：
  - 为站点启用 **DNS** 解析。导航到完整配置 > 设置并打开启用 **DNS** 解析设置。或者，使用 Citrix Virtual Apps and Desktops 远程 PowerShell SDK 并运行命令 `Set-BrokerSite -DnsResolutionEnabled $true`。有关 Citrix Virtual Apps and Desktops 远程 PowerShell SDK 的详细信息，请参阅 [SDK](#) 和 [API](#)。
  - 具有 **VDA** 的 **PTR** 记录的 **DNS** 反向查找区域。如果选择此选项，我们建议您将 VDA 配置为始终尝试注册 PTR 记录。为此，请使用组策略编辑器或组策略对象，导航到计算机配置 > 管理模板 > 网络 > **DNS** 客户端，然后将注册 **PTR** 记录设置为已启用并注册。如果连接的 DNS 后缀与域的 DNS 后缀不匹配，您还必须配置 **Connection-specific DNS suffix**（连接特有的 DNS 后缀）设置，以便计算机能够成功注册 PTR 记录。

注意：

如果使用 DNS 解析选项，则 Cloud Connector 必须能够解析 VDA 计算机的完全限定域名 (FQDN)。在内部用户直接连接到 VDA 计算机的情况下，客户端设备还必须能够解析 VDA 计算机的 FQDN。

如果使用 DNS 反向查找区域，则 PTR 记录中的 FQDN 必须与 VDA 计算机的 FQDN 相匹配。如果 PTR 记录包含不同的 FQDN，则汇聚连接将失败。例如，如果计算机的 FQDN 是 `vda01.domain.net`，则 PTR 记录必须包含 `vda01.domain.net`。使用其他 FQDN（例如 `vda01.sub.domain.net`）将不起作用。

## 代理配置

VDA 支持通过代理建立汇聚连接。

### 代理注意事项

在 Rendezvous 中使用代理时，请注意以下事项：

- 支持透明代理、非透明 HTTP 代理和 SOCKS5 代理。
- 不支持数据包解密和检查。配置异常，以便 VDA 与网关服务之间的 ICA 流量不会被拦截、解密或检查。否则，连接会中断。
- HTTP 代理通过使用协商和 Kerberos 或 NT 局域网管理器 (NTLM) 身份验证协议支持基于计算机的身份验证。连接到代理服务器时，协商身份验证方案会自动选择 Kerberos 协议。如果 Kerberos 不受支持，协商将回退到 NTLM 进行身份验证。

注意：

要使用 Kerberos，必须为代理服务器创建服务主体名称 (SPN)，并将其与代理的 Active Directory 帐户关联。VDA 在建立会话时生成格式为 `HTTP/<proxyURL>` 的 SPN，其中代理 URL 是从 **Rendezvous** 代理策略设置中检索的。如果不创建 SPN，身份验证将回退到 NTLM。在这两种情况下，VDA 计算机的身份都用于身份验证。

- 当前不支持使用 SOCKS5 代理进行身份验证。如果使用 SOCKS5 代理，必须配置例外，以便发往网关服务地址的流量（在要求中指定）可以绕过身份验证。
- 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。

### 透明代理

如果在网络中使用透明代理，则不需要在 VDA 上进行其他配置。

### 非透明代理

如果在网络中使用非透明代理，请配置**汇聚代理配置**设置。启用该设置后，请指定 HTTP 或 SOCKS5 代理地址，或者输入 PAC 文件的路径，以便 VDA 知晓要使用的代理。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`

如果使用 PAC 文件配置代理，请使用 Windows HTTP 服务所需的语法定义代理：`PROXY [<scheme>=]<URL or IP>:<port>`。例如，`PROXY socks5=<URL or IP>:<port>`。

### Rendezvous 验证

如果您满足所有要求，请按照下列步骤验证是否正在使用 Rendezvous：

1. 在 HDX 会话中启动 PowerShell 或命令提示符。
2. 运行 `ctxsession.exe -v`。
3. 正在使用的传输协议指明连接类型：
  - TCP 汇聚：**TCP > SSL > CGP > ICA**
  - EDT 汇聚：**UDP > DTLS > CGP > ICA**
  - 通过 Cloud Connector 代理：**TCP > CGP > ICA**

## 其他注意事项

### Windows 密码套件顺序

对于自定义密码套件顺序，请确保在以下列表中包含 VDA 支持的密码套件：

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

如果自定义密码套件顺序不包含这些密码套件，汇聚连接将失败。

### Zscaler Private Access

如果使用 Zscaler Private Access (ZPA)，建议您为网关服务配置绕过设置，以避免延迟增加和相关的性能影响。为此，您必须为网关服务地址定义应用程序段（在要求中指定），并将其设置为始终绕过。有关配置应用程序段以绕过 ZPA 的信息，请参阅 [Zscaler 文档](#)。

## Rendezvous V2

February 9, 2024

使用 Citrix Gateway 服务时，Rendezvous 协议允许 VDA 绕过 Citrix Cloud Connector，以直接安全地连接到 Citrix Cloud 控制平面。

加入标准域的计算机、加入混合 Azure AD 的计算机、加入 Azure AD 的计算机和未加入域的计算机支持 Rendezvous V2。

#### 注意：

目前，无连接器部署仅适用于 \_ 已加入 Azure AD\_ 和 \_ 未加入域 \_ 的计算机。加入标准 AD 域的计算机和加入混合 Azure AD 的计算机仍需要 Cloud Connector 进行 VDA 注册和会话代理。但是，使用 Rendezvous V2 没有 DNS 要求。

Cloud Connector 对与 VDA 通信无关的其他功能（例如连接到本地 AD 域、将 MCS 配置到本地虚拟机管理程序等）的要求保持不变。

## 要求

使用 Rendezvous V2 的要求是：

- 使用 Citrix Workspace 和 Citrix Gateway 服务访问环境。



- 控制平面：Citrix DaaS
- VDA 版本 2203
- 在 Citrix 策略中启用 Rendezvous 协议。有关详细信息，请参阅 [Rendezvous 协议策略设置](#)。
- 必须在 VDA 上启用会话可靠性
- VDA 计算机必须有权访问：
  - [https://\\*.xendesktop.net](https://*.xendesktop.net) (通过 TCP 443)。如果您无法以这种方式允许所有子域，则可以使用 [https://<customer\\_ID>.xendesktop.net](https://<customer_ID>.xendesktop.net)，其中 <customer\_ID> 是您的 Citrix Cloud 客户 ID，如 Citrix Cloud 管理员门户所示。
  - TCP 443 上的 [https://\\*.nssvc.net](https://*.nssvc.net) 用于与网关服务的控制连接。
  - [https://\\*.nssvc.net](https://*.nssvc.net) (对于使用 TCP 和 EDT 进行连接的 HDX 会话，分别通过 TCP 443 和 UDP 443)。

注意：

如果您不允许所有子域名使用 [https://\\*.nssvc.net](https://*.nssvc.net)，则可以改用 [https://\\*.c.nssvc.net](https://*.c.nssvc.net) 和 [https://\\*.g.nssvc.net](https://*.g.nssvc.net)。有关详细信息，请参阅知识中心文章 [CTX270584](#)。

## 代理配置

使用 Rendezvous 时，VDA 支持通过代理连接控制流量和 HDX 会话流量。两种类型的流量的要求和注意事项不同，因此请仔细查看。

### 控制流量代理注意事项

- 仅支持 HTTP 代理。
- 不支持数据包解密和检查。配置例外，以便 VDA 和 Citrix Cloud 控制平面之间的控制流量不会被拦截、解密或检查。否则，连接将失败。
- 不支持代理身份验证。

### HDX 流量代理注意事项

- 支持 HTTP 和 SOCKS5 代理。
- EDT 只能与 SOCKS5 代理一起使用。
- 默认情况下，HDX 流量使用为控制流量定义的代理。如果必须为 HDX 流量使用不同的代理（无论是不同的 HTTP 代理还是 SOCKS5 代理），请使用 [Rendezvous 代理配置策略设置](#)。
- 不支持数据包解密和检查。配置例外，以便 VDA 和 Citrix Cloud 控制平面之间的 HDX 流量不会被拦截、解密或检查。否则，连接将失败。

- 只有 HTTP 代理支持基于计算机的身份验证，并且前提是 VDA 计算机已加入 AD 域。它可以使用协商/Kerberos 或 NTLM 身份验证。

注意：

要使用 Kerberos，请为代理服务器创建服务主体名称 (SPN)，并将其与代理的 Active Directory 帐户关联。VDA 在建立会话时生成格式为 `HTTP/<proxyURL>` 的 SPN，其中代理 URL 是从 [Rendezvous 代理配置策略](#) 设置中检索的。如果不创建 SPN，身份验证将回退到 NTLM。在这两种情况下，VDA 计算机的身份都用于身份验证。

- 当前不支持使用 SOCKS5 代理进行身份验证。如果使用 SOCKS5 代理，请配置例外，以便发往网关服务地址的流量（在要求中指定）可以绕过身份验证。
- 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。

## 透明代理

如果在网络中使用透明代理，则不需要在 VDA 上进行其他配置。

## 非透明代理

如果在网络中使用非透明代理，请在 VDA 安装期间指定代理，以便控制流量可以到达 Citrix Cloud 控制平面。在继续安装和配置之前，请务必查看控制流量代理注意事项。

在 VDA 安装向导中，在其他组件页面中选择 **Rendezvous** 代理配置。此选项使 **Rendezvous** 代理配置页面稍后在安装向导中可见。请在此处输入代理地址或 PAC 文件的路径，以便 VDA 知晓要使用的代理。例如：

- 代理地址：`http://<URL or IP>:<port>`
- PAC 文件：`http://<URL or IP>/<path/<filename>.pac`

如 HDX 流量代理注意事项中所述，默认情况下，HDX 流量使用在 VDA 安装期间定义的代理。如果必须为 HDX 流量使用不同的代理（无论是不同的 HTTP 代理还是 SOCKS5 代理），请使用 [Rendezvous 代理配置策略](#) 设置。启用此设置后，请指定 HTTP 或 SOCKS5 代理地址。还可以输入 PAC 文件的路径，以便 VDA 知晓要使用的代理。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`

如果使用 PAC 文件配置代理，请使用 Windows HTTP 服务所需的语法定义代理：`PROXY [<scheme>=] <URL or IP>:<port>`。例如，`PROXY socks5=<URL or IP>:<port>`。

## 如何配置 Rendezvous

下面是在您的环境中配置 Rendezvous 的步骤：

1. 请确保满足所有要求。
2. 如果必须在环境中使用非透明 HTTP 代理，请在 VDA 安装期间对其进行配置。有关详细信息，请参阅代理配置部分。
3. 安装完成后重新启动 VDA 计算机。
4. 创建 Citrix 策略或者编辑现有策略：
  - 将 **Rendezvous** 协议设置设为允许。
  - 如果必须为 HDX 流量配置 HTTP 或 SOCKS5 代理，请配置 **Rendezvous** 代理配置设置。
  - 请务必正确设置 Citrix 策略过滤器。该策略适用于需要启用 Rendezvous 的计算机。
5. 请确保 Citrix 策略具有正确的优先级，以免覆盖其他策略。

注意：

如果您使用的是 VDA 版本 2308 或更早版本，则默认使用 V1。有关如何配置要使用的版本的更多信息，请参阅[通过注册表管理的 HDX 功能](#)。

## Rendezvous 验证

如果您满足所有要求并且已完成配置，请按照以下步骤验证 Rendezvous 是否正在使用中：

1. 在虚拟桌面中，打开命令提示符或 PowerShell。
2. 运行 `ctxsession.exe -v`。
3. 显示的传输协议指明连接类型：
  - TCP 汇聚：TCP > SSL > CGP > ICA
  - EDT 汇聚：UDP > DTLS > CGP > ICA
  - 不是 Rendezvous：TCP > CGP > ICA
4. 报告的 Rendezvous 版本表示正在使用的版本。

## 其他注意事项

### Windows 密码套件顺序

如果已在 VDA 计算机中修改密码套件顺序，请务必包含 VDA 支持的密码套件：

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

如果自定义密码套件顺序不包含这些密码套件，汇聚连接将失败。

## Zscaler Private Access

如果使用 Zscaler Private Access (ZPA)，建议您为网关服务配置绕过设置，以避免延迟增加和相关的性能影响。为此，您必须为网关服务地址定义应用程序段（在要求中指定），并将其设置为始终绕过。有关配置应用程序段以绕过 ZPA 的信息，请参阅 [Zscaler 文档](#)。

### 已知问题

如果之前使用过 **Rendezvous V1**，则 **Rendezvous V2** 不起作用

如果您在 DaaS 站点中启用 DNS 解析设置以使用 Rendezvous V1，则 Rendezvous V2 连接将失败。要使用 Rendezvous V2，您必须使用以下选项之一在 DaaS 站点中禁用 DNS 解析：

- 导航到完整配置 > 设置，然后关闭启用 **DNS** 解析设置
- 使用 Citrix DaaS Remote PowerShell SDK 并运行命令 `Set-BrokerSite -DnsResolutionEnabled $false`

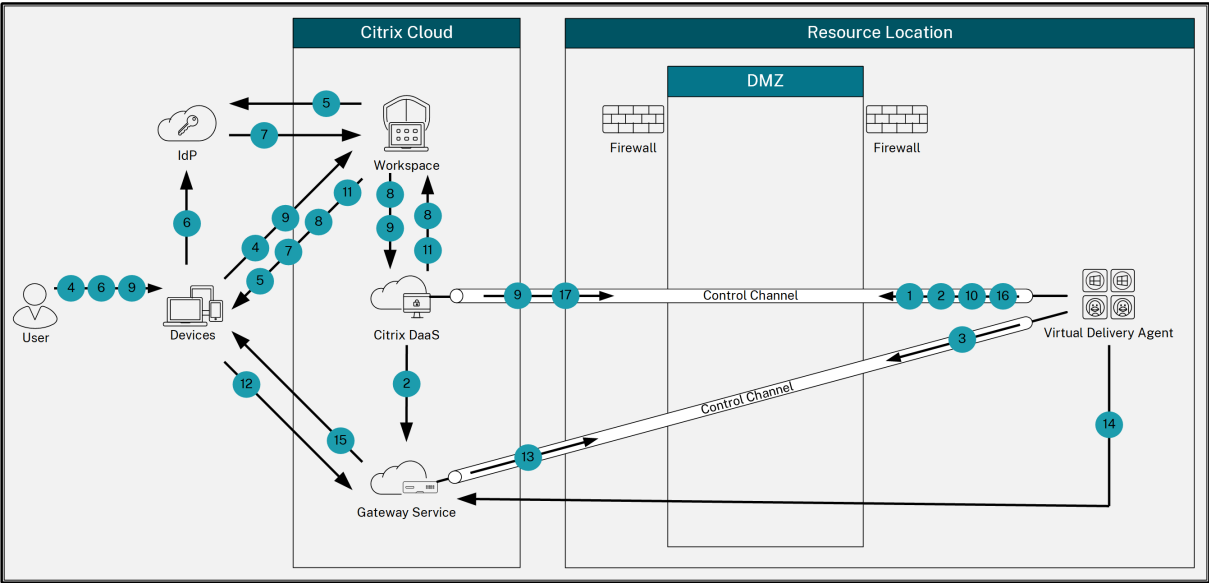
### **VDA 2203** 安装程序不允许为代理地址输入斜杠 (/)

解决方法：可以在安装 VDA 后在注册表中配置代理：

```
1      Key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
2      Value type: String
3      Value name: ProxySettings
4      Value data: Proxy address or path to pac file. For example:
5          Proxy address: http://squidk.test.local:3128
6          Pac file: http://file.test.com/config/proxy.pac
```

## Rendezvous 通信流

下图说明了有关 Rendezvous 通信流的步骤顺序。



1. VDA 与 Citrix Cloud 建立 WebSocket 连接并注册。
2. VDA 在 Citrix Gateway 服务中注册并获得专用令牌。
3. VDA 与 Gateway 服务建立永久控制连接。
4. 用户导航到 Citrix Workspace。
5. Workspace 评估身份验证配置并将用户重定向到相应的 IdP 进行身份验证。
6. 用户输入自己的证书。
7. 成功验证用户凭据后，用户将被重定向到 Workspace。
8. Workspace 为用户计算资源的数量并显示这些资源。
9. 用户从 Workspace 中选择桌面或应用程序。Workspace 向 Citrix DaaS 发送请求，后者代理连接并指示 VDA 为会话做好准备。
10. VDA 使用 Rendezvous 功能及其标识进行响应。
11. Citrix DaaS 会生成启动票据，并通过 Workspace 将其发送到用户设备。
12. 用户的端点连接到网关服务，并提供启动票据以验证和标识要连接的资源。
13. 网关服务将连接信息发送到 VDA。
14. VDA 为与 Gateway 服务的会话建立直接连接。
15. Gateway 服务完成端点与 VDA 之间的连接。
16. VDA 验证会话的许可。
17. Citrix DaaS 向 VDA 发送适用的策略。

## HDX Direct（预览版）

January 23, 2024

访问 Citrix 提供的资源时，如果可以进行直接通信，HDX Direct 允许内部和外部客户端设备与会话主机建立安全的直

接连接。

重要：

HDX Direct 目前处于预览阶段。此功能在不支持的情况下提供，尚不建议在生产环境中使用。要提交反馈或报告问题，请使用[此表单](#)。

系统要求

以下是使用 HDX Direct 的系统要求：

- 控制平面
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2311 或更高版本
- Virtual Delivery Agent (VDA)
  - Windows：版本 2311 或更高版本
- Workspace 应用程序
  - Windows：版本 2311 或更高版本
- 访问层
  - 带有 Citrix Gateway 服务的 Citrix Workspace
  - 带有 NetScaler Gateway 的 Citrix Workspace
- 其他
  - 必须为外部直接连接启用自适应传输

网络要求

以下是使用 HDX Direct 的网络要求。

会话主机

如果您的会话主机具有防火墙（例如 Windows Defender Firewall），则必须允许以下入站流量进行内部连接。

说明	源	协议	端口
直接内部连接	客户端	TCP	443

说明	源	协议	端口
直接内部连接	客户端	UDP	443

注意：

VDA 安装程序将相应的入站规则添加到 Windows Defender Firewall。如果您使用其他防火墙，则必须添加上述规则。

客户端网络

下表描述了内部和外部用户的客户端网络。

内部用户

说明	协议	源	源端口	目标	目的端口
直接内部连接	TCP	客户端网络	1024-65535	VDA 网络	443
直接内部连接	UDP	客户端网络	1024-65535	VDA 网络	443

外部用户

说明	协议	源	源端口	目标	目的端口
STUN（仅限外部用户）	UDP	客户端网络	1024-65535	Internet（请参见下面的备注）	3478, 19302
外部用户连接	UDP	客户端网络	1024-65535	数据中心的公有 IP 地址	1024-65535

数据中心网络

下表描述了内部和外部用户的数据中心网络。

内部用户

说明	协议	源	源端口	目标	目的端口
直接内部连接	TCP	客户端网络	1024-65535	VDA 网络	443
直接内部连接	UDP	客户端网络	1024-65535	VDA 网络	443

外部用户

说明	协议	源	源端口	目标	目的端口
STUN（仅限外部用户）	UDP	VDA 网络	1024-65535	Internet（请参见下面的备注）	3478, 19302
外部用户连接	UDP	DMZ /内部网络	1024-65535	VDA 网络	55000-55250
外部用户连接	UDP	VDA 网络	55000-55250	客户的公有 IP	1024-65535

注意：

VDA 和 Workspace 应用程序都尝试以相同的顺序向以下服务器发送 STUN 请求：

- [stunserver.stunprotocol.org](https://stunserver.stunprotocol.org): 3478
- [employees.org](https://employees.org): 3478
- [stun.l.google.com](https://stun.l.google.com): 19302

如果您使用 **HDX Direct** 端口范围策略设置更改外部用户连接的默认端口范围，则相应的防火墙规则必须与您的自定义端口范围相匹配。

配置

默认情况下，HDX Direct 处于禁用状态。您可以使用 Citrix 策略中的 **HDX Direct** 设置来配置此功能。

- **HDX Direct**：启用或禁用某项功能。
- **HDX Direct** 模式：确定 **HDX Direct** 是仅适用于内部客户端还是同时适用于内部和外部客户端。
- **HDX Direct** 端口范围：定义 VDA 用于外部客户端连接的端口范围。

注意事项

下面是使用 HDX Direct 的注意事项：

- 外部用户的 HDX Direct 仅在 EDT (UDP) 作为传输协议时才可用。因此，必须启用自适应传输。
- 如果您使用的是 **HDX Insight**，请注意，使用 **HDX Direct** 会阻止 HDX Insight 数据收集，因为会话将不再通过 NetScaler Gateway 进行代理。



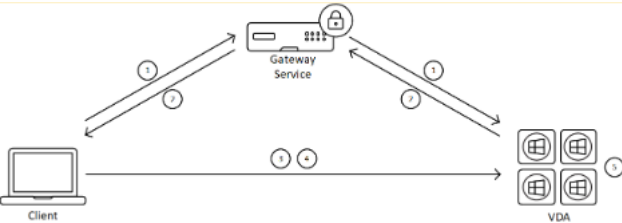
- 为虚拟应用程序和桌面使用非持久性计算机时，Citrix 建议在会话主机上启用 **HDX Direct**，而不是在主/模板映像中启用 HDX Direct，以便每台计算机生成自己的证书。
- 目前不支持在 HDX Direct 中使用自己的证书。

工作原理

可以进行直接通信时，HDX Direct 允许客户端与会话主机建立直接连接。使用 HDX Direct 进行直接连接时，使用自签名证书通过网络级别加密 (TLS/DTLS) 保护直接连接。

内部用户

下图描述了内部用户的 HDX Direct 连接过程的概述。



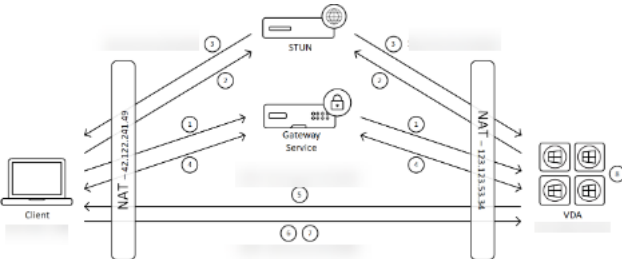
1. 客户端通过网关服务建立 HDX 会话。
2. 成功连接后，VDA 通过 HDX 连接向客户端发送 VDA 计算机的 FQDN、其 IP 地址列表以及 VDA 计算机的证书。
3. 客户端探测 IP 地址以查看其是否可以直接到达 VDA。
4. 如果客户端可以使用共享的任何 IP 地址直接访问 VDA，则客户端使用与步骤 (2) 中交换的证书与 VDA 建立直接连接，使用 (D)TLS 进行保护。
5. 成功建立直接连接后，会话将传输到新连接，并且与网关服务的连接将终止。

注意：

在上述步骤 2 中建立连接后，会话处于活动状态。后续步骤不会延迟或干扰用户使用虚拟应用程序或桌面的能力。如果任何后续步骤失败，则在不中断用户会话的情况下保持通过网关的连接。

外部用户

下图概述了外部用户的 HDX Direct 连接过程：



1. 客户端通过网关服务建立 HDX 会话。
2. 成功连接后，客户端和 VDA 都会发送 STUN 请求以发现其公有 IP 地址和端口。
3. STUN 服务器使用其相应的公有 IP 地址和端口响应客户端和 VDA。
4. 通过 HDX 连接，客户端和 VDA 交换其公有 IP 地址和 UDP 端口，然后 VDA 将其证书发送给客户端。
5. VDA 将 UDP 数据包发送到客户端的公有 IP 地址和 UDP 端口。客户端向 VDA 的公有 IP 地址和 UDP 端口发送 UDP 数据包。
6. 收到来自 VDA 的消息后，客户端会以安全连接请求进行响应。
7. 在 DTLS 握手期间，客户端验证证书是否与步骤 (4) 中交换的证书相匹配。验证后，客户端发送其授权令牌。现已建立安全的直接连接。
8. 成功建立直接连接后，会话将传输到新连接，并且与网关服务的连接将终止。

注意：

在上述步骤 2 中建立连接后，会话处于活动状态。后续步骤不会延迟或干扰用户使用虚拟应用程序或桌面的能力。如果任何后续步骤失败，则在不中断用户会话的情况下保持通过网关的连接。

## 证书管理

### 会话主机

VDA 计算机上的以下两项服务处理证书创建和管理，这两个服务都设置为在计算机启动时自动运行：

- Citrix ClxMtp Service：负责 CA 证书密钥的生成和轮换。
- Citrix Certificate Manager Service：负责生成和管理自签名的根 CA 证书和计算机证书。

以下步骤描述了证书管理流程：

1. 服务在计算机启动时启动。
2. 如果尚未创建任何密钥，**Citrix ClxMtp Service** 将创建密钥。
3. Citrix Certificate Manager Service 检查是否启用 **HDX Direct**。否则，该服务会自行停止。
4. 如果启用了 **HDX Direct**，Citrix Certificate Manager Service 将检查是否存在自签名的根 CA 证书。如果不存在，则创建自签名的根证书。
5. 一旦根 CA 证书可用，Citrix Certificate Manager Service 就会检查自签名的计算机证书是否存在。否则，该服务会生成密钥并使用计算机的 FQDN 创建新证书。
6. 如果存在由 Citrix Certificate Manager Service 创建的现有计算机证书，并且使用者名称与计算机的 FQDN 不匹配，则会生成新证书。

注意：

Citrix Certificate Manager Service 生成利用 2048 位密钥的 RSA 证书。

## 客户端设备

要成功建立安全的 **HDX Direct** 连接，客户端必须信任用于保护会话的证书。为方便起见，客户端通过 ICA 文件（由 Workspace 提供）接收会话的 CA 证书，因此没有必要将 CA 证书分发到客户端设备的证书存储区。

## NAT 兼容性

January 23, 2024

为了在外部用户设备和会话主机之间建立直接连接，HDX Direct 利用打孔进行 NAT 遍历和 STUN 来促进客户端设备和会话主机的公有 IP 地址和端口映射的交换。这类似于 VoIP、统一通信和 P2P 解决方案的工作方式。

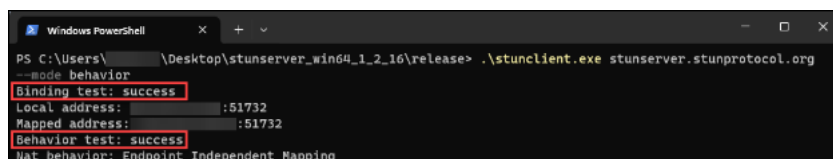
只要将防火墙和其他网络组件配置为允许 STUN 请求和 HDX 会话的 UDP 流量，外部用户的 HDX Direct 就有望发挥作用。但是，在某些情况下，用户和会话主机网络的 NAT 类型会导致不兼容的组合，从而导致 HDX Direct 出现故障。

## 验证

您可以使用 STUNTMAN 的 STUN 客户端实用程序验证客户端和会话主机上的 NAT 类型：

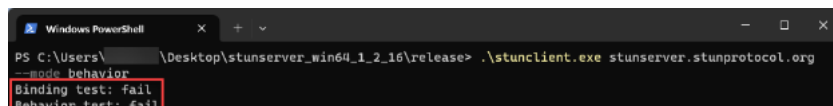
1. 从 [stunprotocol.org](https://stunprotocol.org) 下载适用于目标平台的相应软件包，然后提取内容。
2. 打开终端提示符并导航到提取内容的目录。
3. 请运行以下命令：  
`.\stunclient.exe stunserver.stunprotocol.org --mode behavior`
4. 记下输出。

如果绑定和行为测试成功，则绑定测试和行为测试都会报告成功并指定 NAT 行为：



```
Windows PowerShell
PS C:\Users\...\Desktop\stunserver_win64_1.2.16\release> .\stunclient.exe stunserver.stunprotocol.org
--mode behavior
Binding test: success
Local address: ...:51732
Mapped address: ...:51732
Behavior test: success
NAT behavior: Endpoint Independent Mapping
```

如果测试失败，绑定测试和行为测试都会报告失败。



```
Windows PowerShell
PS C:\Users\...\Desktop\stunserver_win64_1.2.16\release> .\stunclient.exe stunserver.stunprotocol.org
--mode behavior
Binding test: fail
Behavior test: fail
```

参见下表，根据客户端和会话主机的测试结果，确定面向外部用户的 HDX Direct 是否有效：

客户端设备	会话主机	预计会起作用吗？
端点独立映射	端点独立映射	是
端点独立映射	端点相关映射	是
端点相关映射	端点独立映射	是
端点相关映射	端点相关映射	否
失败	任何 NAT 类型	否
任何 NAT 类型	失败	否
失败	失败	否

故障排除

January 23, 2024

要确认 **HDX Direct** 已成功建立直接连接，您可以在 VDA 计算机上使用 `CtxSession.exe` 实用程序。

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 -v`。如果成功建立 **HDX Direct** 连接，则 **HDX Direct** 状态为 `Connected`。

```
PS C:\Users\[redacted]> ctxsession -v
Session Id 1:
Transport Protocols: UDP -> DTLS -> CGP -> ICA
  Local Address: [redacted]:55000
  Remote Address: [redacted]:60410
  Client Address: [redacted]:63274
Security Protocol: DTLS 1.2
Security Cipher: 256 bit AES
Cipher Strength: 256 bits
ICA Encryption: Transport Only
Rendezvous Version: None
HDX Direct State: Connected - External
Reducer Version: 4.0

EDT Reliable Statistics:
  Bandwidth 301.904 Mbps, RTT 57.690 ms, EDT MTU: 1480

EDT Unreliable Statistics:
  Bandwidth 7.544 Kbps, RTT 1 us, EDT MTU: 1480

EDT Reliable Basic FEC Statistics:
  Bandwidth 92.090 Mbps, RTT 35.164 ms, EDT MTU: 1480

ICA Statistics:
  SentBandwidth (bps) = 0
  HDX Latency = 63
  IcaBufferLength = 1436
```

您还可以查看会话主机的事件日志，了解 HDX Direct 连接是成功建立还是失败的信息。有关详细信息，请参阅事件日志部分。

**注意：**

根据环境和会话主机可用的 IP 地址数量，建立 HDX Direct 连接最多可能需要 5 分钟。

**当 HDX Direct 无法建立直接连接时**

如果 HDX Direct 无法建立直接连接，请查看以下步骤：

1. 根据系统要求，确保正在使用的 VDA 版本和 Workspace 应用程序版本支持该功能。
2. 确认您已将启用 HDX Direct 的 VDA 应用了策略，并且没有其他优先级更高的策略禁用该功能。
3. 确认您已在 VDA 上应用了设置所需的 HDX Direct 模式的策略，并且没有其他优先级更高的策略覆盖该配置。
4. 确保 Citrix ClxMtp Service 正在会话主机上运行。
5. 确保 Citrix Certificate Manager Service 正在会话主机上运行。如果它没有运行，请尝试手动启动。如果禁用 HDX Direct，该服务将自动停止。
6. 检查会话主机是否有自签名的根 CA 证书：
  - a) 颁发对象：CA-`<hostname>`（例如，CA-FTLW11-001）
  - b) 颁发者：CA-`<hostname>`（例如，CA-FTLW11-001）
  - c) 颁发者详细信息：该组织为 Citrix Systems, Inc.
7. 检查会话主机是否有其自签名的服务器证书：
  - a) 颁发对象：`<host FQDN>`（例如，FTLW11-001.ctxlab.net）
  - b) 颁发者：CA-`<hostname>`（例如，CA-FTLW11-001）
  - c) 颁发者详细信息：该组织为 Citrix Systems, Inc.
8. 如果缺少证书，请联系 Citrix 技术支持。
9. 如果证书存在：
  - a) 停止会话主机上的 Citrix Certificate Manager Service。
  - b) 删除自签名的根 CA 证书和自签名的服务器证书。
  - c) 在会话主机上启动 Citrix Certificate Manager Service。该服务启动后会创建新证书。
10. 对于内部用户：
  - a) 确保会话主机的防火墙没有阻止 UDP 443 或 TCP 443 上的入站流量，分别适用于 EDT 上的 HDX 和基于 TCP 的 HDX。
  - b) 确保您的网络防火墙没有阻止客户端网络和会话主机网络之间的 UDP 443 和 TCP 443 上的流量。
11. 对于外部用户：
  - a) 检查客户端和会话主机的 NAT 类型，并确保组合有效。有关详细信息，请参阅 NAT 兼容性部分。
  - b) 如果 NAT 测试在客户端或会话主机上失败：
    - i. 如果系统上运行防火墙，请确保它没有阻止 UDP 3478 上的出站流量。
    - ii. 确保您的网络防火墙没有阻止 UDP 3478 上的出站流量。

iii. 确保防火墙没有阻止 STUN 服务器的响应。

- c) 确保您的网络防火墙配置了适当的规则，以允许所有必要的流量。有关详细信息，请参阅“[网络要求](#)”部分。
- d) 如果您使用 HDX Direct 端口范围策略设置更改默认端口范围，请确保为自定义端口范围设置防火墙规则。

事件日志

以下事件记录在 VDA 计算机的事件日志中：

日志	ID	源	级别	说明
应用程序和服务日志 > Citrix-HostCore- HDX Direct/操作	1	HDX Direct	信息	已建立内部用户 <username> 的 HDX Direct 连接。
应用程序和服务日志 > Citrix-HostCore- HDX Direct/操作	2	HDX Direct	信息	已建立外部用户 <username> 的 HDX Direct 连接。
应用程序和服务日志 > Citrix-HostCore- HDX Direct/操作	3	HDX Direct	信息	用户 <username> 的 HDX Direct 连接失 败。

已知问题

在已经启用 HDX Direct 的计算机上执行 VDA 的就地升级后，**HDX Direct** 可能会停止运行。

要解决此问题，请完成以下步骤：

1. 停止会话主机上的 Citrix Certificate Manager Service。
2. 删除自签名的根 CA 证书和自签名的服务器证书。
3. 打开注册表。
4. 删除 `HKLM\Software\Citrix\HDX-Direct` 密钥。
5. 转到 `HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\icawd`。
6. 将 **SSLEnabled** 值设置为 0。
7. 删除 **SSLThumbprint** 值的内容。
8. 启动 **Citrix Certificate Manager Service**。

设备

September 1, 2023

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：

- [客户端驱动器映射](#)
- [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](#)
- [Webcams](#)
- [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

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

客户端驱动器映射 (CDM)

October 26, 2023

客户端驱动器映射可以使客户端端点上的存储驱动器在 Citrix HDX 会话中可用，从而允许将文件和文件夹从客户端传输到会话主机，反之亦然。默认情况下，此功能处于启用状态，同时具有读取和写入权限。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为允许，并且也已添加到该策略中。

作为一种安全预防措施，端点驱动器默认在没有运行权限的情况下进行映射。要允许用户直接从映射的客户端驱动器运行可执行文件，请在会话主机中编辑 **ExecuteFromMappedDrive** 注册表值。有关详细信息，请参阅通过注册表管理的 **HDX** 功能中的[映射的客户端驱动器](#)部分

要求

以下是 CDM 的使用要求：

Citrix 控制平面

- Citrix Virtual Apps and Desktops 1912 或更高版本
- Citrix DaaS

会话主机

- 操作系统
  - Windows 10 1809 或更高版本
  - Windows Server 2016 或更高版本
  - Linux：请参阅 Linux VDA [系统要求](#)
- VDA
  - Windows: Citrix Virtual Apps and Desktops 1912 或更高版本
  - Linux：请参阅 Linux VDA [文档](#)



## 客户端设备

- 操作系统
  - Windows 10 1809 或更高版本
  - Linux: 请参阅适用于 Linux 的 Workspace 应用程序的[系统要求](#)

## 相关策略

有关 CDM 设置, 请参阅[策略设置参考](#)部分。

## 双跃点场景

双跃点场景支持 CDM。默认情况下, 客户端端点的驱动器会映射到第二个跃点会话, 而第一个跃点的驱动器则不可用。但是, 可以对此进行设置, 以便在第二个跃点的会话中而非在客户端端点的驱动器中映射第一个跃点的驱动器。

要配置功能, 请编辑以下注册表值:

- 注册表项: HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced
- 值名称: NativeDriveMapping
- 值类型: REG\_SZ
- 值数据:
  - True - 在第二个跃点会话中映射第一个跃点会话的驱动器
  - False - 在第二个跃点会话中映射客户端端点的驱动器

### 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 无法保证由于注册表编辑器使用不当而导致的问题能够得到解决。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。

## 通用 **USB** 设备

November 16, 2023

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
- 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](#)。

## 支持移动和触摸屏客户端设备

February 20, 2024

Citrix Virtual Apps and Desktops 使用户能够通过移动和触摸屏客户端设备访问其已发布的应用程序和桌面。

### 要求

#### **Citrix** 控制平面

- Citrix Virtual Apps and Desktops 7.15 或更高版本
- Citrix DaaS

#### 会话主机

- 操作系统
  - Windows 10 1903 或更高版本
  - Windows Server 2016 或更高版本
- VDA
  - Windows: 版本 7.15 或更高版本

## 客户端设备

- 操作系统
  - Windows 10 1809 或更高版本
- 适用于 Windows 的 Citrix Workspace 应用程序 1808 或更高版本

## 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。当 VDA 检测到支持触控的客户端上存在键盘或鼠标时，它会将客户端置于桌面模式。如果没有键盘或鼠标，VDA 会将客户端置于平板电脑/手机模式。此检测发生在会话连接和重新连接时，也会在连接或断开键盘或鼠标时发生在会话中。

默认情况下启用该功能。要禁用此功能，请配置策略设置[平板电脑模式切换策略设置](#)。

除了上述触摸屏设备的要求外，Windows Continuum 还需要满足以下要求：

## XenServer

- Citrix Hypervisor 8.2 或更高版本
- 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**

### 重要提示：

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。

## 会话主机

- 操作系统
  - Windows 10 1903 或更高版本
  - Windows 11
- VDA
  - Windows：版本 7.16 或更高版本
  - 由于操作系统配置中的当前限制，用户在启动第一个 **ICA** 会话并重新启动 **VDA** 后，必须从下拉菜单中设置以下选项：
    - ★ 设置 > 系统 > 平板电脑模式
      - 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）

## Tablet mode

When I sign in

Use the appropriate mode for my hardware ▾

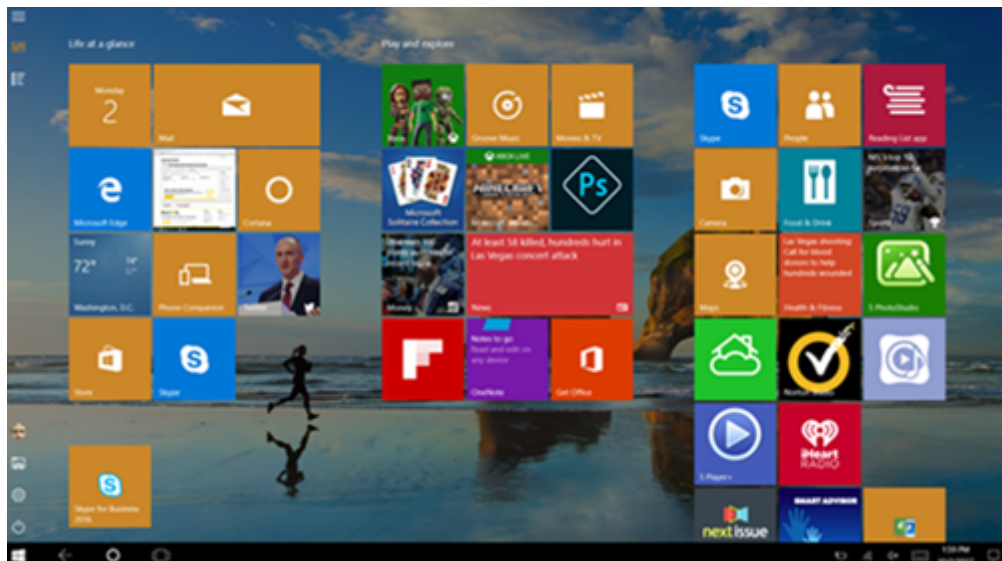
When this device automatically switches tablet mode on or off

Don't ask me and always switch ▾

平板电脑模式提供了更适于触摸屏的用户界面：

- 按钮稍大一点
- “开始”屏幕和您启动的所有应用程序都会以全屏模式打开
- 任务栏包含返回按钮
- 图标已从任务栏中删除

您可以访问文件资源管理器。



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。

适用于 HTML5 的 Citrix Workspace 应用程序不支持 Windows Continuum 功能。

桌面模式提供传统的用户界面，您可以像使用电脑和键盘鼠标一样进行交互。

## 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。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。

下面是支持笔功能的要求：

### Citrix 控制平面

- Citrix Virtual Apps and Desktops 1903 或更高版本
- Citrix DaaS

### 会话主机

- 操作系统
  - Windows 10 1809 或更高版本
  - Windows Server 2016 或更高版本
  - Windows 11
- VDA
  - Windows: 版本 1903 或更高版本

### 客户端设备

- 操作系统
  - Windows 10 1809 或更高版本
- 适用于 Windows 的 Citrix Workspace 应用程序最低版本 1902

要获取 Windows Ink 和笔功能的演示，请单击此图形：



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。

## 已知问题

下面是笔支持功能的已知问题：

- 由于 Windows Server 2k22 中的操作系统限制，用户在连接到 2k22 服务器应用程序或桌面时，将无法在“控制面板”中设置笔快捷键或调整笔/墨水设置。
- 由于操作系统限制，支持笔的 Windows 11 客户端不支持笔快捷方式。

## 串行端口

April 18, 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。

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。

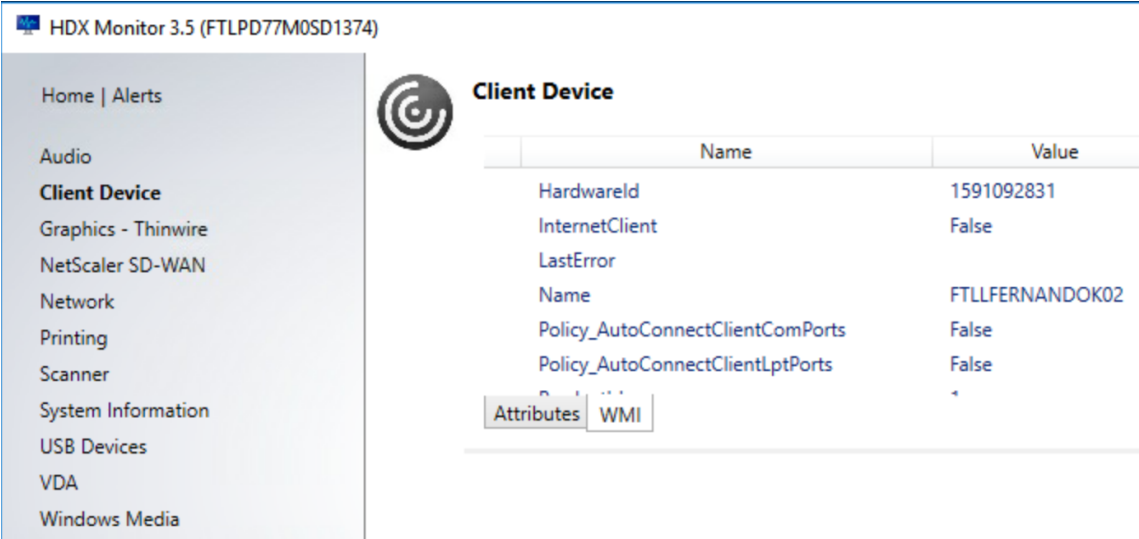
重要:

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:

- “管理”控制台策略。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：

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

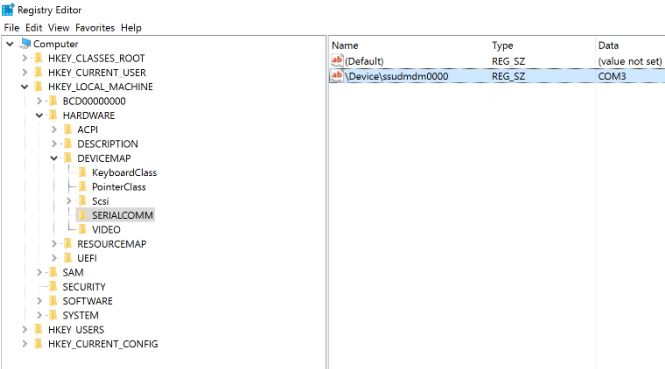
:

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 **chgpport /query** 查找此信息。



 C:\Windows\system32\cmd.exe

```
C:\Users\fernandok>chgpport /query  
COM3 = \Device\ssudmdm0000
```

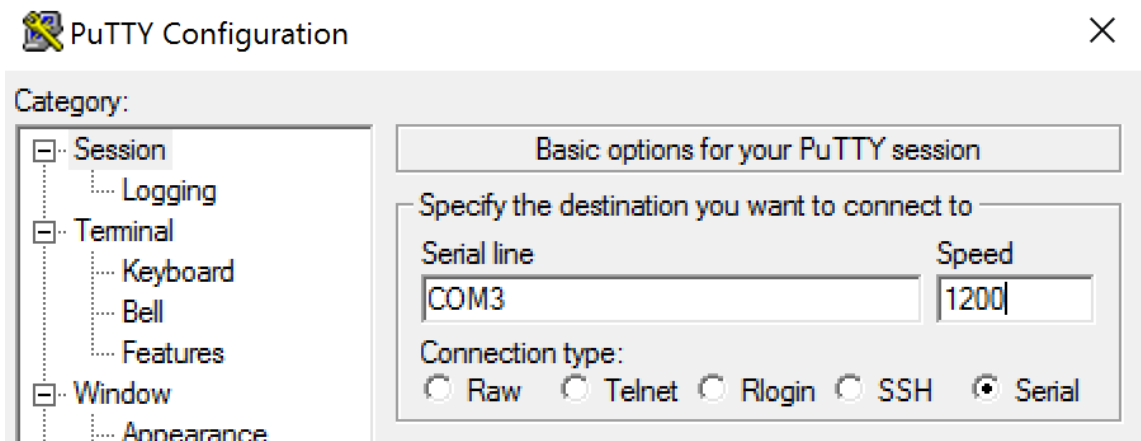
```
C:\Users\fernandok>mode
```

```
Status for device COM3:
```

```
-----
```

Baud:	1200
Parity:	Even
Data Bits:	7
Stop Bits:	1
Timeout:	OFF
XON/XOFF:	OFF
CTS handshaking:	OFF
DSR handshaking:	OFF
DSR sensitivity:	OFF
DTR circuit:	ON
RTS circuit:	ON

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。



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 而非服务的“管理” > “完整配置”界面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“管理”控制台策略，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

November 16, 2023

### 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。

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。如果启用了支持 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。如果启用了支持 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

April 18, 2022

### 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

August 16, 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

April 18, 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）。
- 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

April 18, 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 DaaS（以前称为 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 DaaS 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 DaaS 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。

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](#)
- [Thinwire](#)
- [基于文本的会话水印](#)

## HDX 3D Pro

January 23, 2024

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。

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：

- XenServer
  - 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 23, 2024

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。

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 XenServer 硬件兼容性列表, 请参阅[虚拟机管理程序硬件兼容性列表](#)。
- 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。

- 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

January 23, 2024

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、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。

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\Citrix 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。

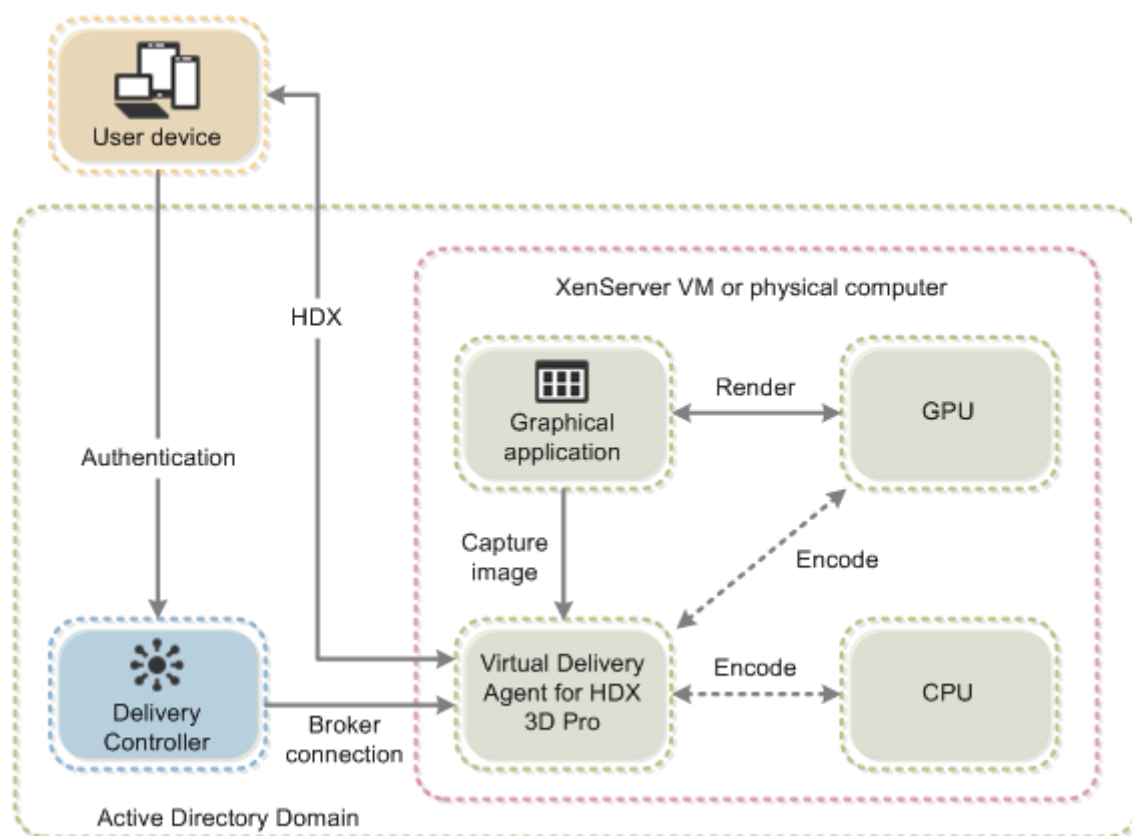
- 支持使用虚拟直接图形加速 (vDGA) 的 VMware vSphere 和 VMware ESX —可针对 RDS 和 VDI 工作负载将 HDX 3D Pro 与 vDGA 结合使用。
- 支持使用 NVIDIA GRID vGPU 和 AMD MxGPU 的 VMware vSphere/ESX。
- 对使用 Windows Server 2016 中离散设备分配的 Microsoft HyperV 的支持。
- 对具有 Intel Xeon Processor E3 系列的数据中心图形的支持。HDX 3D Pro 支持多显示器（最多 3 个）、控制台消隐、自定义分辨率和受支持的 Intel 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>。
- 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。XenServer 和 Hyper-V 支持 GPU 直通。有关详细信息，请参阅 [AMD 虚拟化解决方案](#)。
- 访问适用于 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。



### 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。

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

May 19, 2023

### 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 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 针对现代操作系统进行了优化，包括 Windows Server 2012 R2、Windows Server 2016、Windows Server 2019 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。之所以包含在内，是为了在使用 XenApp 7.15 LTSR、XenDesktop 7.15 LTSR 和之前的 VDA 版本时向后兼容。

- 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。

- [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。在这种情况下，可以考虑改用 [H.264 设为无损](#)。



1 Select Settings

2 Summary

Select Settings

(All Versions)

Graphics

Search

Settings 1 selected

View selected only

> Notify user when display mode is degraded  
Computer setting - ICA\Graphics  
Not Configured (Default: Disabled)

Select

> Optimize for 3D graphics workload  
User setting - ICA\Graphics  
Not Configured (Default: Disabled)

Select

> Persistent cache threshold  
Computer setting - ICA\Graphics\Caching  
Not Configured (Default: 3000000 Kbps)

Select

> Queuing and tossing  
Computer setting - ICA\Graphics  
Not Configured (Default: Enabled)

Select

> Use hardware encoding for video codec  
User setting - ICA\Graphics  
Not Configured (Default: Enabled)

Select

> Use video codec for compression  
User setting - ICA\Graphics  
Not Configured (Default: Use when preferred)

Select

Next

Cancel

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](#)

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。或者，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。



HDX

Download System Report

	Adobe® Flash®	Virtual channel: Idle Flash redirection: Inactive
	Graphics - Framehawk	Virtual channel: Idle Current FPS: 0
	Scanner	Virtual channel: Idle Compression level: Medium
	Smart Cards	Virtual channel: Idle Number of devices: 0
	Legacy Graphics	Virtual channel: Active Still image compression: Medium
	Audio	Virtual channel: Idle Number of devices: 1
	Graphics - Thinwire	Virtual channel: Active Current FPS: 1
	Mapped Client Drives	Virtual channel: Idle Client drives available: 0
	Network	Bandwidth used: 0% Average latency: 47 ms
	Printing	Mapped printers: 4 Virtual channel: Idle
	VDA	Version: Session ID: 3
	Windows Media	Virtual channel: Idle Active streams: 2

3. 选择图形 - **Thinwire**。

Graphics - Thinwire

There are no alerts at this time.

Status

Virtual channel state	Idle
Virtual channel priority	High
Monitors	1
Frames Per Second	1
Provider	Standard (RDS)
Video codec use	None

Monitor 0

Monitor ID	0
Primary	True
Left	0
Top	0
Right	1280
Bottom	800

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

## 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

April 18, 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窃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。

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。

## 多媒体

April 18, 2022

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 DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）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。

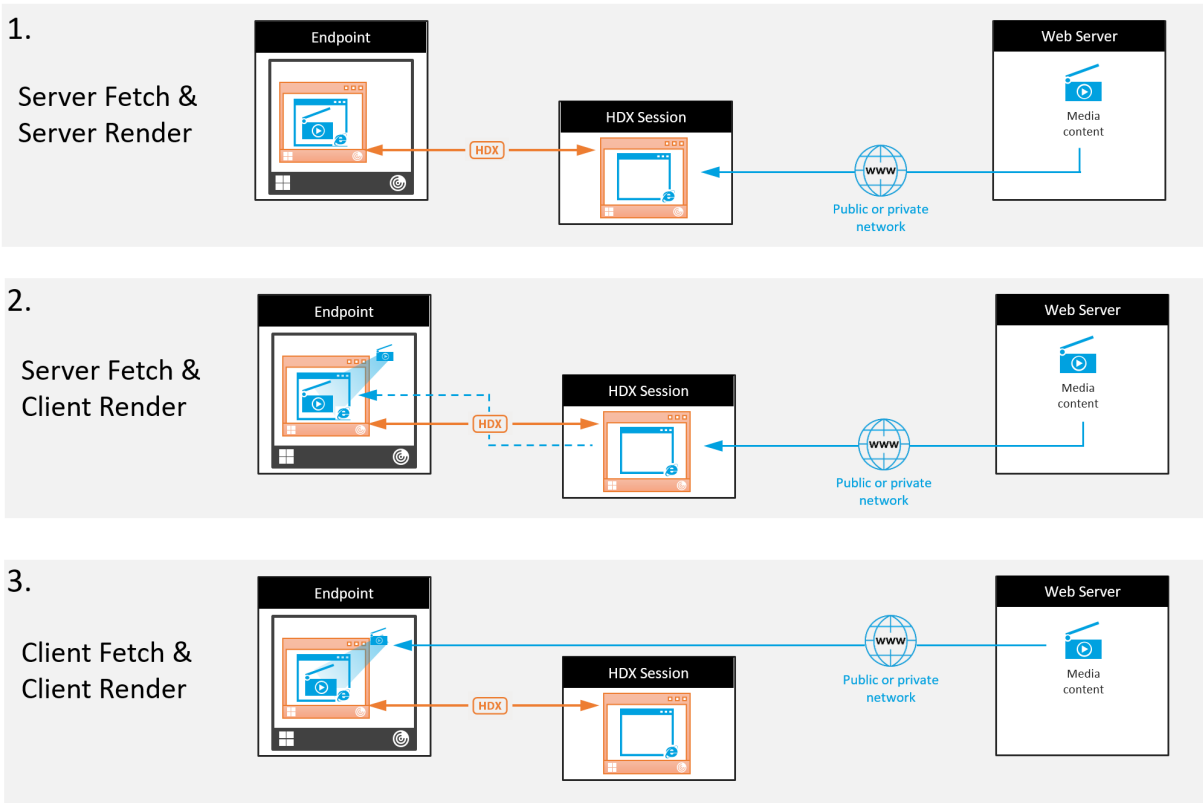
- Windows Media 重定向针对许多种通常与 Windows Media Player 关联的媒体格式来卸载服务器的负载。
- HTML5 视频变得非常盛行，Citrix 为这种类型的内容引入了重定向技术。我们建议使用 HTML5、HLS、DASH 或 WebRTC 对 Web 站点进行浏览器内容重定向。

- 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。

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，解码在服务器上完成，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。

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 20, 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。

## 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），将音频质量降低至最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”。

## 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。

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  
EnableUDPTThroughGateway=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。

### 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 和 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）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：

- 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。

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)。

### 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）。必须在服务的“管理”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

June 24, 2022

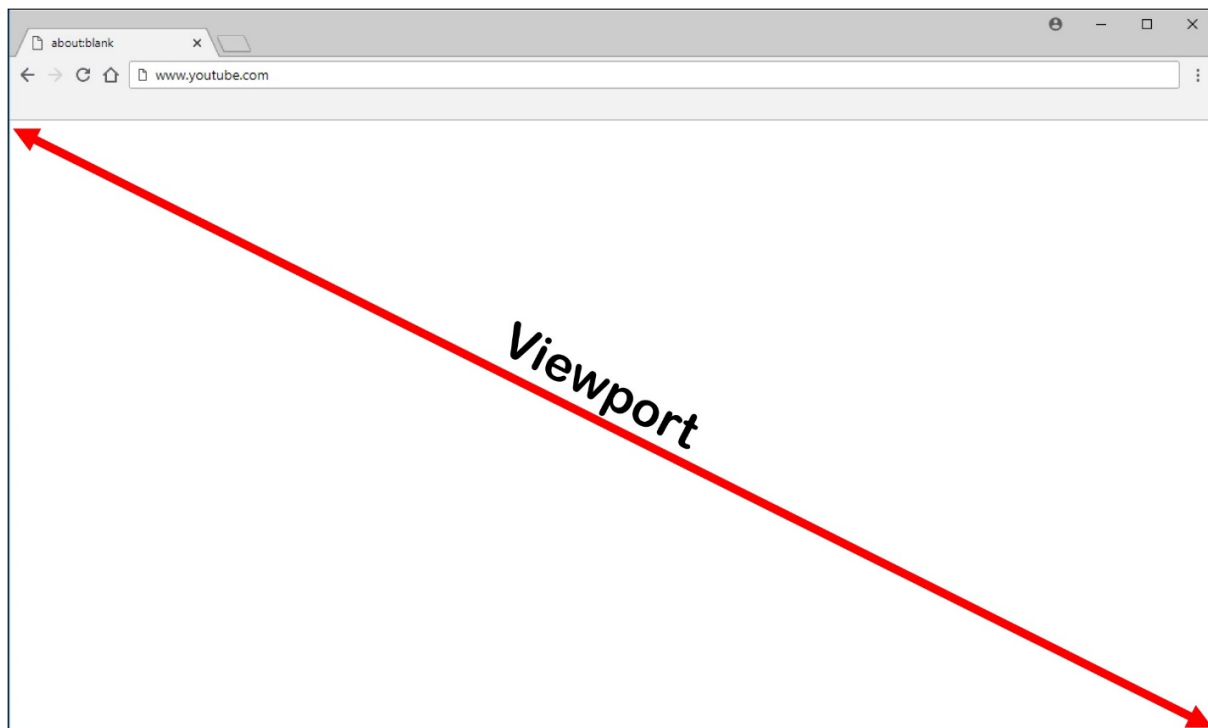
浏览器内容重定向会阻止在 VDA 端呈现允许列表中的 Web 页面。此功能会使用 Citrix Workspace 应用程序在客户端实例化相应的呈现引擎，该引擎会从 URL 提取 HTTP 和 HTTPS 内容。

#### 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。



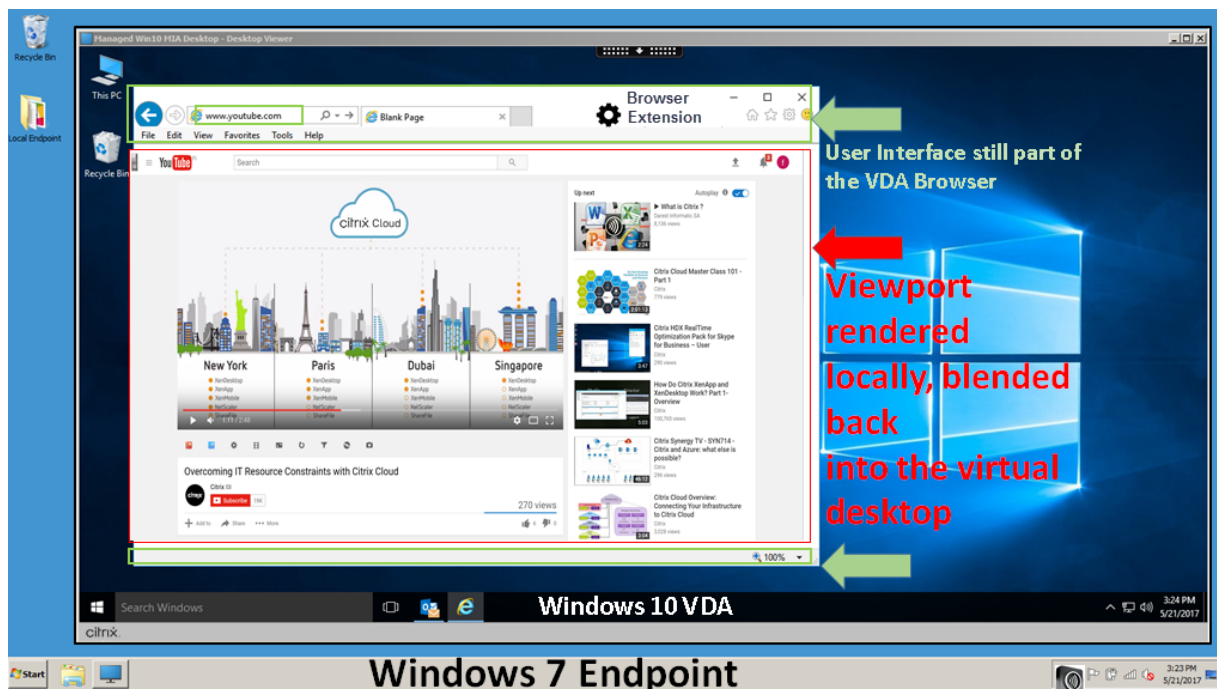
1. 在“管理” > “完整配置”界面中配置策略，该策略指定访问控制列表，其中包含从允许或阻止列表中进行重定向的 URL。为了使 VDA 上的浏览器检测用户正在导航到的 URL 与允许列表匹配还是与阻止列表不匹配，某个浏览器扩展将执行比较。适用于 Internet Explorer 11 的浏览器扩展程序 (BHO) 包含在安装介质中并自动安装。对于 Chrome，浏览器扩展程序在 Chrome 网上应用店中提供，可以使用组策略和 ADMX 文件进行部署。Chrome 扩展程序基于每个用户安装。不需要更新黄金映像即可添加或删除扩展程序。
2. 如果在允许列表中找到一个匹配项（例如 <https://www.mycompany.com/>），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。





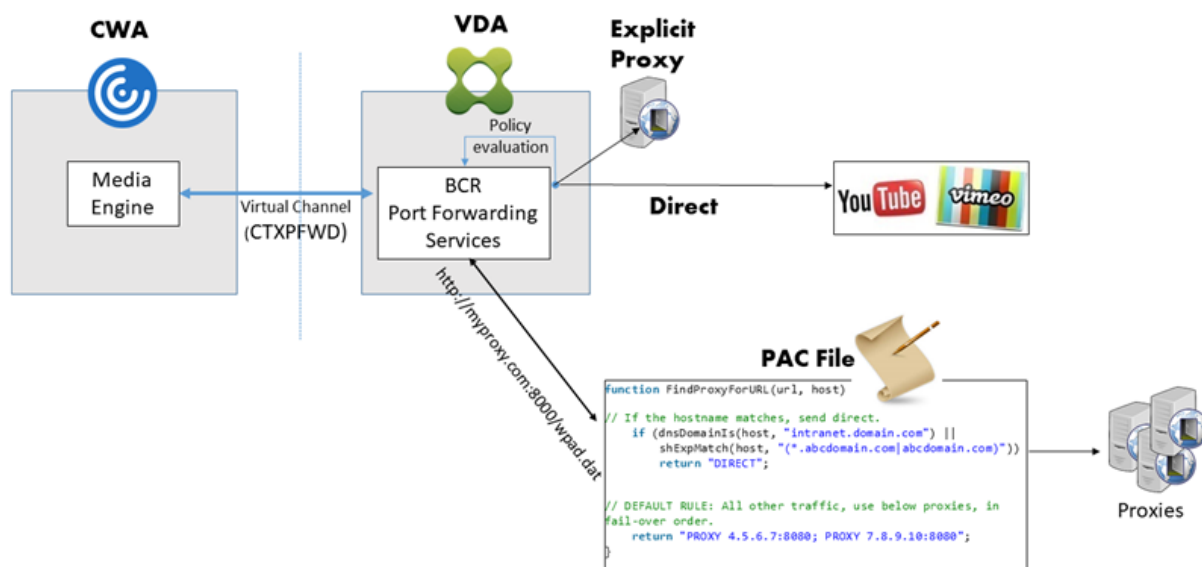
下面是 Citrix Workspace 应用程序提取内容的方式的几种情况：

- 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。

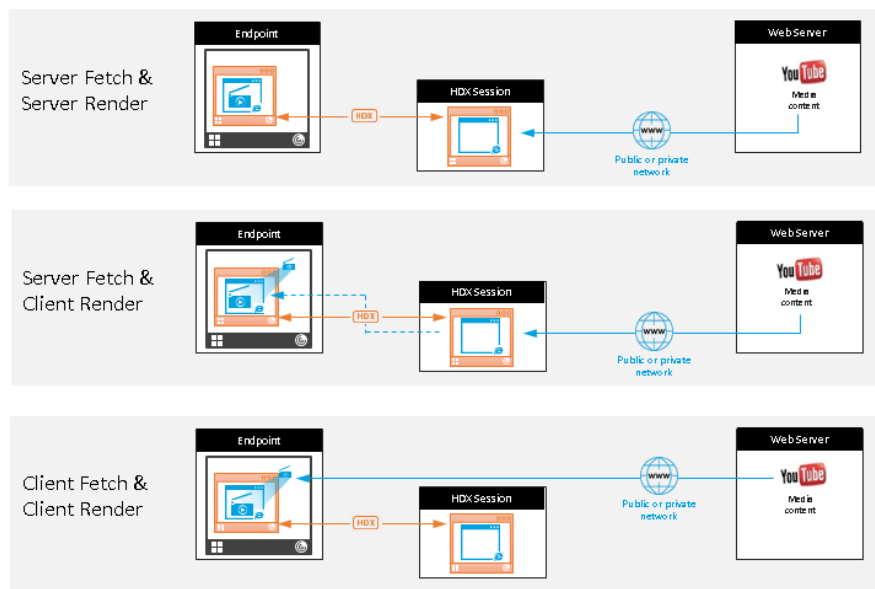
可选择的策略选项：

- 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。



- 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。

## Redirection scenarios



### Benefits:

- Better end user experience (Adaptive Bit Rate (ABR))
- Reduced VDA resource usage (CPU/RAM/IO)
- Reduced bandwidth consumption

### 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 或 11
- 适用于 Windows 的 Citrix Workspace 应用程序 1809 或更高版本

注意：

仅当前版本的适用于 Windows 的 Citrix Workspace 应用程序支持浏览器内容重定向，而在 Citrix Workspace 应用程序 LTSR 版本（1912 和 2203.1）上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
- Citrix Receiver for Linux 13.9 或更高版本
- 瘦客户端端点必须包括 WebKitGTK+

Citrix Virtual Apps and Desktops 7 1808 以及 XenApp and XenDesktop 7.15 CU5、7.18、7.17、7.16：

- VDA 操作系统：Windows 10（最低版本 1607）、Windows Server 2012 R2、Windows Server 2016
- 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、Citrix Virtual Apps and Desktops 7 1808 VDA 和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>。

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**。

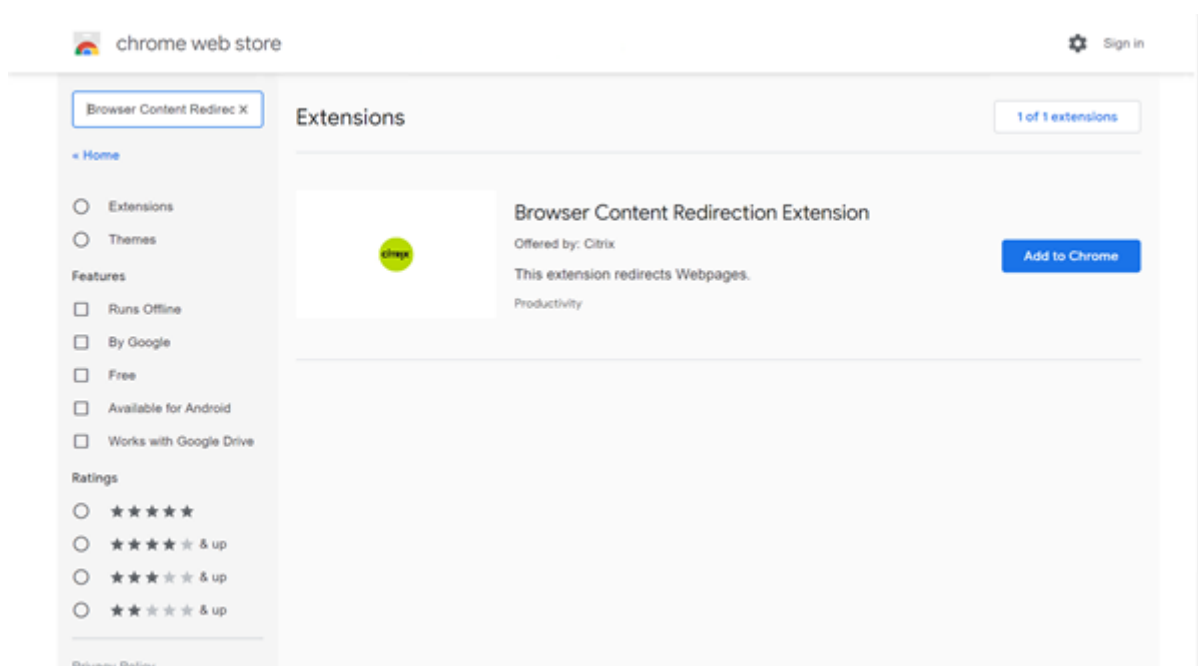
用户的客户端计算机中不需要此扩展程序，仅在 VDA 中需要。

## 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：

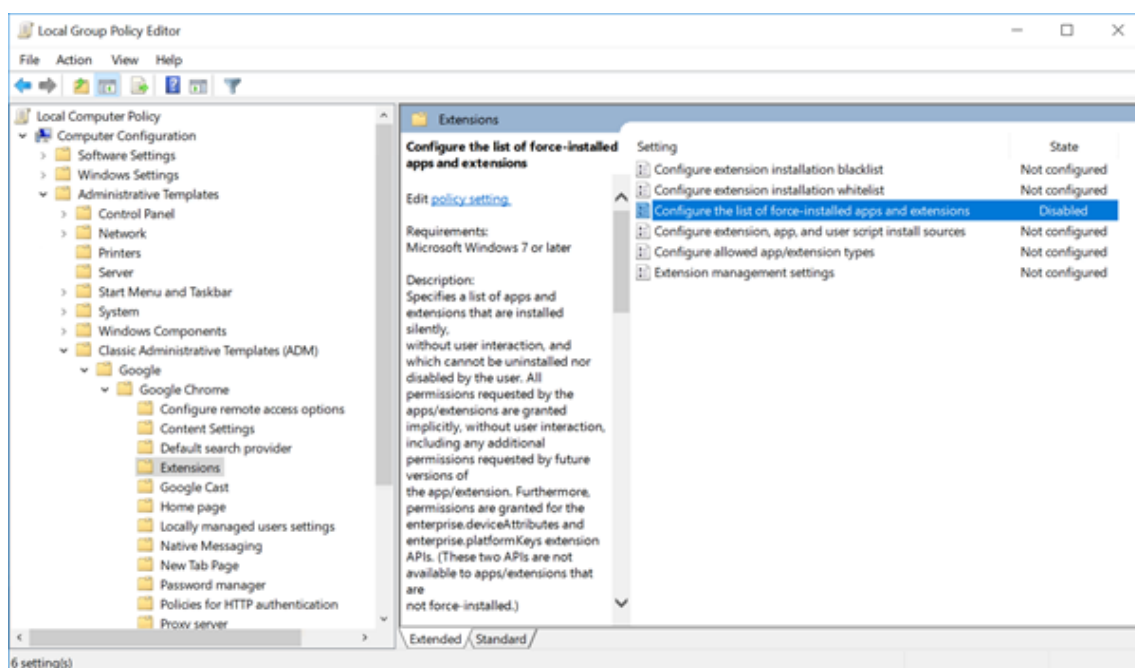
仅当前版本的适用于 Windows 的 Citrix Workspace 应用程序支持浏览器内容重定向，而在 Citrix Workspace 应用程序 LTSR 版本（1912 和 2203.1）上不支持浏览器内容重定向。



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。

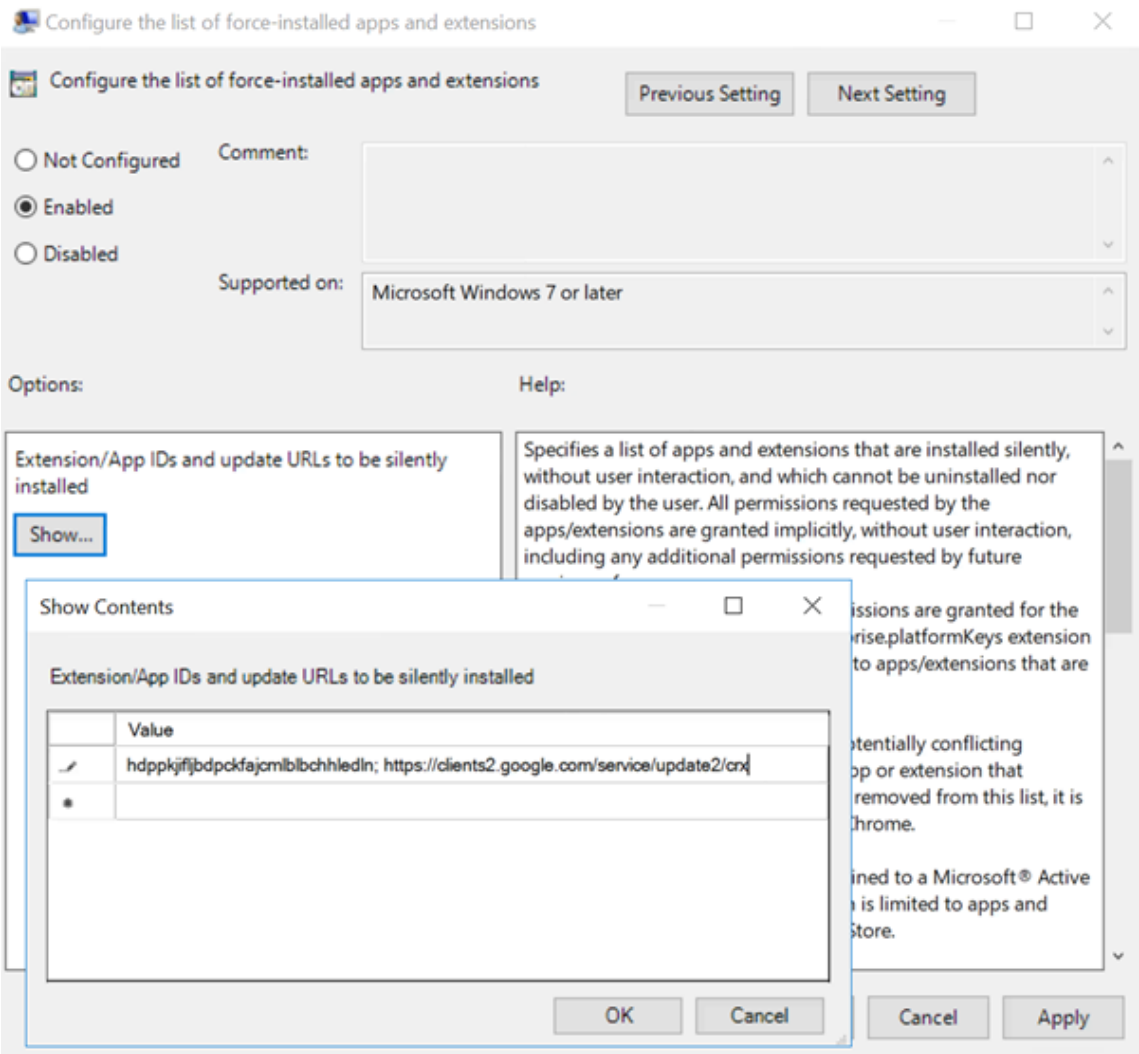
## 使用组策略部署扩展程序

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](#)。
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`



4. 应用设置并执行 **gpupdate** 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。

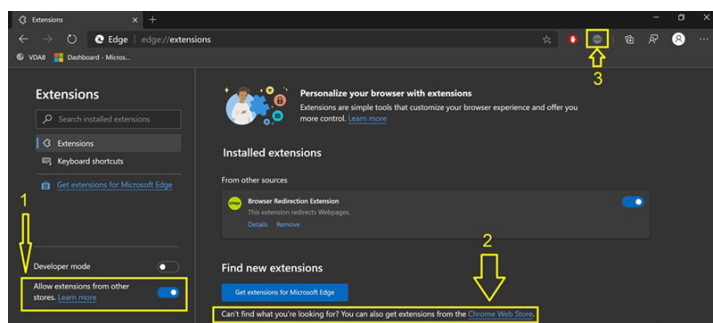
扩展程序的所有更新都将通过在设置中指定的更新 URL 自动安装在用户的计算机上。

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](#)。



## 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](#)。

## 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。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

March 30, 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。

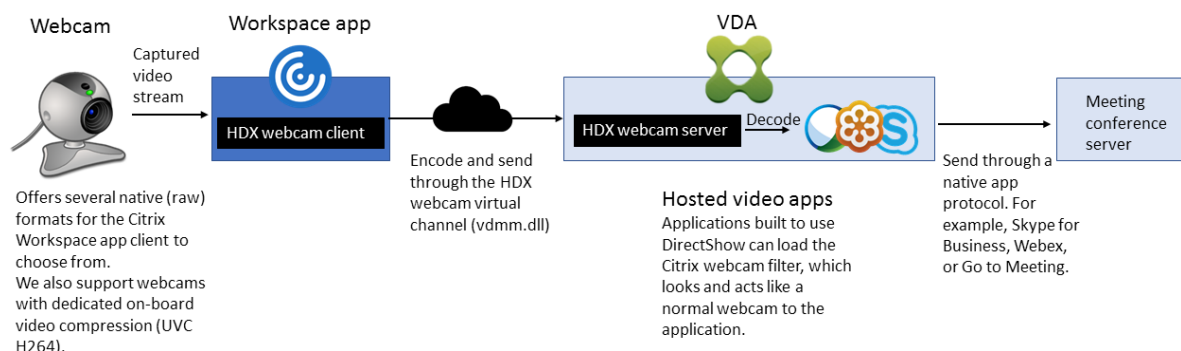
## HDX 网络摄像机视频压缩

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捕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。



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。

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。

## 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

May 19, 2023

HTML5 多媒体重定向扩展了 HDX MediaStream 的多媒体重定向功能，将 HTML5 音频和视频包括进来。由于多媒体内容联机分发（尤其是向移动设备）的增长，浏览器行业开发了更有效的音频和视频呈现方式。

Flash 曾是标准，但它需要插件、不能在所有设备上运行，并且在移动设备上运行时电池使用量较高。YouTube 和 Netflix.com 等公司以及 Mozilla、Google 和 Microsoft 的更高浏览器版本正在转向 HTML5，使其成为新的标准。

与专有插件相比，基于 HTML5 的多媒体具有多个优势，包括：

- 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
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 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 <a href="https://wiki.mozilla.org/CA:AddRootToFirefox">https://wiki.mozilla.org/CA:AddRootToFirefox</a> 。	Windows 10 x86 (1607 RS1) 和 x64 (1607 RS1); Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2
Chrome 51	Windows 10 x86 (1607 RS1) 和 x64 (1607 RS1); Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2

## HTML5 视频重定向解决方案的组成部分

- **HdxVideo.js** - 在 Web 站点上截获视频命令的 JavaScript 挂钩。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/XenDesktop Engineering; CN = Citrix XenApp/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/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX Service)  
位置: 证书 (本地计算机) > 个人 > 证书。
- **WebSocketService.exe** - 在本地系统上运行, 并执行 SSL 终止和用户会话映射。TLS 安全 WebSocket 侦听 127.0.0.1 端口 9001。
- **WebSocketAgent.exe** - 在用户会话中运行, 并根据 WebSocketService 命令的指示呈现视频。

## 如何启用 HTML5 视频重定向?

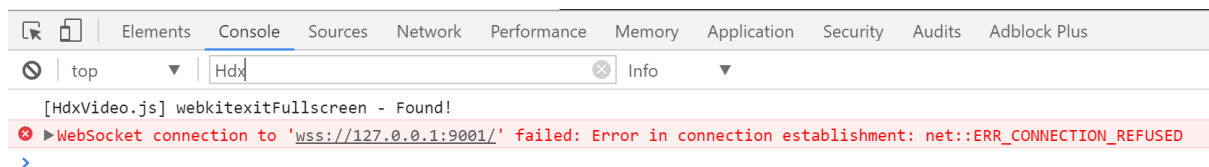
在此版本中, 此功能仅用于受控 Web 页面。它要求将 HdxVideo.js JavaScript (包含在 Citrix Virtual Apps and Desktops 安装介质中) 添加到提供 HTML5 多媒体内容的 Web 页面。例如, 内部培训站点上的视频。

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：



## Microsoft Teams 的优化

February 9, 2024

注意：

新的 Microsoft Teams 2.1 现已正式可用于 VDA。此 Microsoft Teams 版本与使用 WebRTC (VDI 1.0) 的 Citrix Microsoft Teams 优化兼容。这需要在 VDA 中设置新的注册表配置以使新的 Microsoft Teams 能够访问 Citrix 虚拟频道。

要启用 Microsoft Teams 2.1 优化，请在 VDA 中配置以下注册表项：

位置：HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService

注册表项 (REG\_Multi\_SZ)：ProcessWhitelist

值：msedgewebview2.exe

有关详细信息，请参阅 [Microsoft](#) 文档。

Citrix 使用 Citrix Virtual Apps and Desktops 和 Citrix Workspace 应用程序为基于桌面的 Microsoft Teams 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。

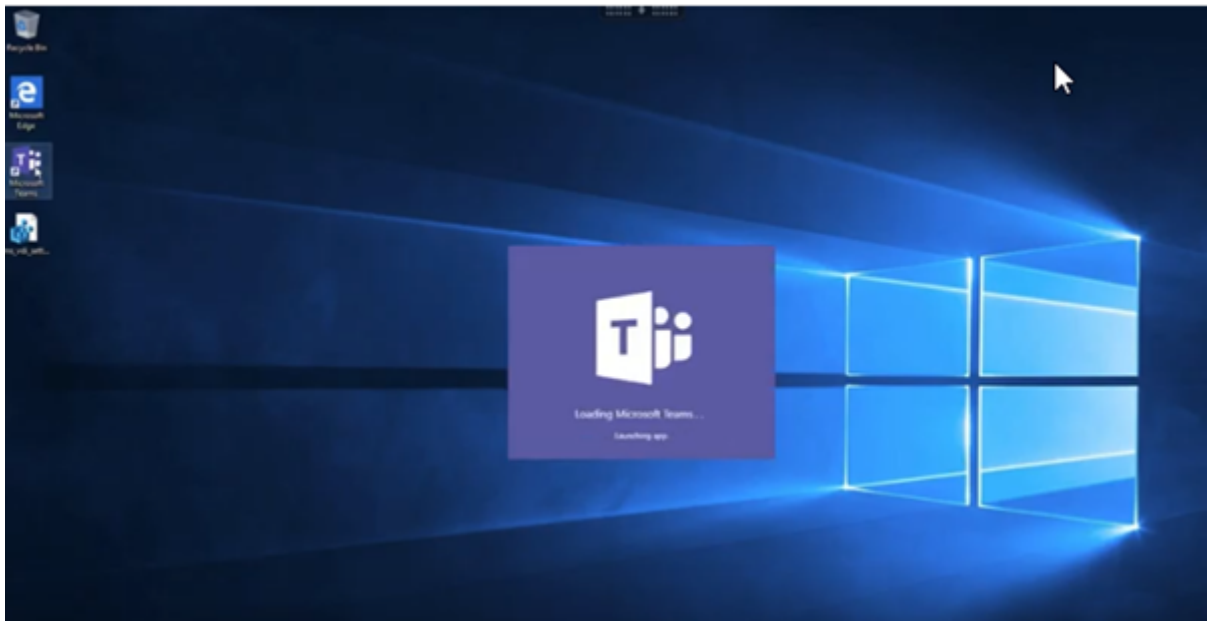
我们针对 Microsoft Teams 的优化包括一个 VDA 端 HDX 服务和 API，用于与 Microsoft Teams 托管的应用程序进行交互以接收命令。这些组件将向 Citrix Workspace 应用程序端媒体引擎打开控制虚拟通道 (CTXMTOP)。端点在本地图解并提提供多媒体，从而将 Citrix Workspace 应用程序窗口移回托管的 Microsoft Teams 应用程序中。

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** 属于命令，用于控制虚拟通道。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

Citrix 和 Microsoft 建议使用最新版本的 Microsoft Teams 并使其保持最新状态。

不支持发布日期早于当前版本的发布日期 90 天的 Microsoft Teams 桌面应用程序版本。

不受支持的 Microsoft Teams 桌面应用程序版本会向用户显示屏蔽页面，并请求更新应用程序。

有关最新的可用版本的信息，请参阅 [Update history for Teams App \(Desktop and Mac\)](#)（更新 Teams 应用程序（桌面版和 Mac 版）的历史记录）。

我们建议您遵循 [Microsoft Teams 计算机范围的安装准则](#)。请避免使用在 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` 标志在 `C:\Program Files (x86)\Microsoft\Teams` 中安装。

```
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，Microsoft 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。还显示在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 `ALLUSER=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。

**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。

## 用于 Remote PC Access

我们建议您先安装 VDA，然后安装 Microsoft Teams 版本 1.4.00.22472 或更高版本。否则，您需要注销并重新登录，Microsoft Teams 才能按预期检测 VDA。版本 1.4.00.22472 及更高版本包括在 Microsoft Teams 启动时运行的增强逻辑以及用于 VDA 检测的登录时间。这些版本还包括活动会话类型标识（HDX、RDP 或本地连接到客户端计算机）。如果您在本地连接，Microsoft Teams 的早期版本可能无法检测并禁用某些功能或 UI 元素。例如，分组讨论会议室、用于会议和聊天的弹出窗口或会议反应。

**重要：**

当您从本地会话漫游到 HDX 会话时，如果 Microsoft Teams 保持打开状态并在后台运行，则必须退出并重新启动 Microsoft Teams 才能正确使用 HDX 进行优化。

相反，如果您通过优化的 HDX 会话远程使用 Microsoft Teams，请断开 HDX 会话的连接，然后在设备上本地重新连接到同一 Windows 会话。在办公室工作时，必须重新启动 Microsoft Teams，这样它才能正确检测 Remote PC 状态（HDX 或本地）。因为 Microsoft Teams 只能在应用程序启动时评估 VDI 模式，而不能在已在后台运行时评估 VDI 模式。如果不重新启动，Microsoft Teams 可能无法加载弹出窗口、分组讨论室或会议回应等功能。

## 面向 App Layering

如果使用 Citrix App Layering 来管理不同层中的 VDA 和 Microsoft Teams 安装，则必须先在 Windows VDA 上创建新的注册表项，然后才能在命令行中使用 `ALLUSER=1` 标志安装 Microsoft Teams。有关详细信息，请参阅[多媒体](#)下的[借助 Citrix App Layering 优化 Microsoft Teams](#)部分。

## 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。

**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**
- 名称：**Teams**
- 类型：**REG\_SZ**
- 值：**C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe**

**注意：**

注册表位置因底层操作系统和位数而异。

**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。

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, 用户特定信息包括用户数据、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 请按照 [Microsoft](#) 文档中的说明从 Microsoft Teams 缓存文件夹中排除这些文件和目录。此操作可帮助您减小用户缓存大小以进一步优化您的非持久性设置。

**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。在常见的虚拟桌面部署中, 每个用户分配有一个桌面, 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。

## Edit Setting

### Profile container - List of folders to be contained in profile disk

☒ **Enabled**  
This setting will be enabled.

☐ **Disabled**  
This setting will be disabled.

☐ Use default value: Disabled

✓ **Applies to the following VDA versions**

Server OS: 7.0, 7.1, 7.5, 7.6, 7.7, 7.8, 7.9, 7.11, 7.12, 7.13, 7.14, 7.15, 7.16, 7.17, 7.18, 1808, 1811, 1903, 1906, 1909, 1912, 2003, 2006, 2009, 2012, 2103, 2106, 2109

Desktop OS: 5.6, 7.0, 7.1, 7.5, 7.6, 7.7, 7.8, 7.9, 7.11, 7.12, 7.13, 7.14, 7.15, 7.16, 7.17, 7.18, 1808, 1811, 1903, 1906, 1909, 1912, 2003, 2006, 2009, 2012, 2103, 2106, 2109

✓ **Description**

A profile container is a VHDX based profile solution that lets you specify the folders to contain on the profile disk. The profile container attaches the profile disk containing those folders, thus eliminating the need to save a copy of the folders to the local profile. Doing so decreases logon times.

To use a profile container, enable this policy and add the relative paths of the folders to the list. Citrix recommends that you include the folders containing large cache files in the list. For example,

Save

Cancel

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。



## 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 2022、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 11。
- Windows 10 64 位，版本为 1607 及更高版本。适用于 Windows 的 Citrix Workspace 应用程序 2109.1 及更高版本支持 VM 托管应用程序。
- Windows Server 2022、2019、2016 和 2012 R2 (Standard Edition 和 Datacenter Edition)。

要求：

- BCR\_x64.msi - 包括 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 11。
- Windows 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) (对 Windows 8.1 的支持已在版本 2204.1 时停止)。
- Windows 10 IoT Enterprise 2016 LTSC (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 和 AIO。
- 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 4.8。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禁用 Microsoft Teams。

#### 最低版本 - 适用于 **Linux** 的 **Citrix Workspace** 应用程序 **2006**

软件：

- [GStreamer](#) 1.0 或更高版本或者 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 Microsoft 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。更新完成后，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 及更高版本。
- macOS Monterey。

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。

默认情况下，Microsoft Teams 优化在 Citrix Workspace 应用程序 2012 及更高版本和 macOS 10.15 中运行。

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 Citrix Workspace 应用程序：

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

最低版本 - 最新版本的 **Chrome OS** 上运行的适用于 **Chrome OS** 的 **Citrix Workspace** 应用程序的最新版本

硬件：

- 性能相当于或优于 Intel i3、四核 2.4 GHz 的处理器。

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](#)。

### 单服务器可扩展性

本部分内容提供建议和指导，以估计单个物理主机上可以支持多少用户或虚拟机 (VM)。这通常称为 Citrix Virtual Apps and Desktops 单服务器可扩展性 (SSS)。在 Citrix Virtual Apps (CVA) 或会话虚拟化环境中，它通常也称为用户密度。这种想法是找出在运行主虚拟机管理程序的单个硬件上可以运行多少用户或 VM。

注意：

本部分内容包含估算 SSS 的指导。请注意，该指南是高级别指南，可能不一定特定于您的特殊情况或环境。真正了解 Citrix Virtual Apps and Desktops SSS 的唯一方法是使用可扩展性或负载测试工具，例如登录 VSI。Citrix 建议使用本指南和这些简单的规则来仅快速估算 SSS。但是，Citrix 建议使用登录 VSI 或您选择的负载测试工具来验证结果，尤其是在购买硬件或做出任何财务决策之前。

硬件（系统正在测试）

- Dell PowerEdge R740
- Intel Xeon (Gold) 6126 @ 2.60 GHz（最大 Turbo 3.70 GHz），每个插槽 12 个内核，支持启用了超线程的双插槽
- 382 GB RAM
- 本地 SSD RAID 0 存储（11 个磁盘）6 TB

## 软件

操作系统为运行 Citrix Virtual Apps and Desktops 2106 的 Windows 2019 (TSVDA) 的单个虚拟机（40 个逻辑处理器）

VMware ESXi 6.7

## 术语

- 知识型员工的工作负载：包括 Acrobat Reader、Freemind/Java、照片查看器、Edge 和 MS Office 应用程序，例如 Excel、Outlook、PowerPoint 和 Word。
- 基础：服务器可扩展性测试在知识型员工工作负载下运行（不使用 Microsoft Teams）。
- Microsoft Teams 工作负载：知识型员工典型工作负载 + Microsoft Teams。

## Microsoft Teams 是如何经过压力测试的

- Microsoft Teams 使用 HDX 进行了优化。因此，所有多媒体处理都被卸载到端点或客户端，并且不是测量的一部分。
- 在工作负载开始之前，所有 Microsoft Teams 进程都停止或终止。
- 打开 Microsoft Teams（冷启动）。
- 衡量 Microsoft Teams 加载和抓取 Microsoft Teams 主窗口焦点所花费的时间。
- 使用键盘快捷方式切换到聊天窗口。
- 使用键盘快捷方式切换到日历窗口。
- 使用键盘快捷方式将聊天消息发送给特定用户。
- 使用键盘快捷方式切换到 Microsoft Teams 窗口。

## 结果

- 与基准工作负载（137 个用户）相比，Microsoft Teams 工作负载（81 个用户）的可扩展性影响为 40%。
- 与基准工作负载一样，将服务器容量增加约 40%（以 CPU 为单位）可恢复用户数量。
- 与基准工作负载相比，Microsoft Teams 工作负载需要 20% 的额外内存。
- 将每个用户的存储大小增加 512-1024 MB。
- IOPS 写入量增加约 50%，IOPS 读取量增加约 100%。在存储速度较慢的环境中，Microsoft Teams 可能会产生重大影响。

## 功能列表和版本支持

功能	Microsoft Teams (最低版本)	VDA (最低版本)	适用于			
			Windows 的 Citrix Workspace 应用程序 CR (最低版本)	适用于 Mac 的 Citrix Workspace 应用程序 (最低版本)	适用于 Linux 的 Citrix Workspace 应用程序 (最低版本)	适用于 Chrome OS 的 Citrix Workspace 应用程序
音频/视频 (P2P 和会议)	当前版本减去 90 天	1906	1907	2009	2004	2105.5
屏幕共享	当前版本减去 90 天	1906	1907	2012	2006	2105.5
i. 屏幕指示器红色边框	当前版本减去 90 天	1906	2002	2012	2006	否
ii. 将捕获限制为 Desktop Viewer	当前版本减去 90 天	1906	2009.5	2012	2006	否
iii. 多显示器	当前版本减去 90 天	1912 CU6+	2106 (1)	2106	2106	否
DTMF	当前版本减去 90 天	不适用	2102	2101	2101	2111.1
代理服务器支持	当前版本减去 90 天	不适用	2012 (2)	2104 (3)	2101 (3)	2305
应用程序共享	当前版本减去 90 天	2109	2109.1	2203.1	2209	否
直播字幕	当前版本减去 90 天	不适用 (4)	2109.1	2109	2109	2303
Dynamic e911	当前版本减去 90 天	不适用	2112.1	2112	2112	2112
授予控制权	当前版本减去 90 天	不适用	2112.1	2203.1	否	否
请求控制权	当前版本减去 90 天	不适用	2112.1	2203.1	2203	2303
多窗口	1.5.00.11865	2112、1912 CU6 (5)	2112.1	2203.1	2203	2303
会议转录	当前版本减去 90 天	2112.1、1912 CU6+	2112	2203.1	2203	2303
背景模糊	当前版本减去 90 天	2112、1912 CU6+	2207	2301	2212	2303

- 1. 仅限全屏模式下的 CD 查看器。Shift+F2 不受支持。
- 2. 协商/Kerberos、NTLM、基本和摘要式。此外，还支持 [Pac](#) 文件。

3. 仅限匿名。
4. 如果 VDA 为 2112 或更高版本，则仅当 Citrix Workspace 应用程序版本为 2203.1（适用于 MAC）、2203（适用于 Linux）或 2112（适用于 Windows）时，实时字幕才起作用。这是因为如果 Microsoft Teams 处于单窗口 UI 模式或多窗口模式，实时字幕的行为会有所差别。
5. 多窗口已在 2112 VDA 中推出，但后来被向后移植到 VDA 1912 LTSR CU6 版本中。

注意：

适用于 **Windows** 的 **Citrix Workspace** 应用程序 **1912 CU6**（或更高版本）中列出的所有功能均适用于 Windows 的 Citrix Workspace 应用程序 2203.1 LTSR CU1。

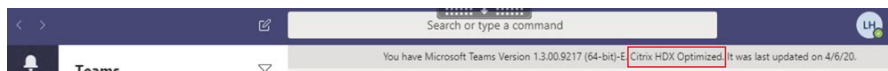
## 启用 Microsoft Teams 优化

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，此策略设置为开。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，**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。

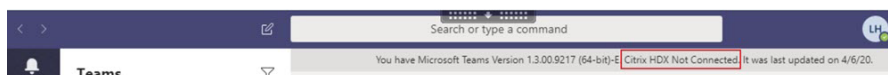
注意：

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 仍然可以进行优化。默认情况下，在 VDA 中启用“Microsoft Teams 的 HDX 优化”。

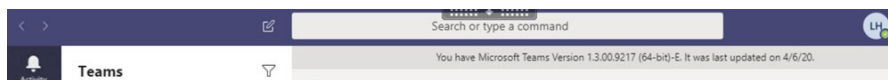
如果单击关于 > 版本，则会显示 **Citrix HDX Optimized**（Citrix HDX 已优化）图例：



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。



重要：会话重新连接

- 连接发生变化时，您可能需要重新启动 Microsoft Teams 才能获得 HDX 优化的会话。例如，如果您正在从不受支持的端点（适用于 iOS、Android 或旧版本的 Windows/Linux/Mac 的 Workspace 应用程序）漫游到受支持的端点（适用于 Windows/Linux/Mac/ChromeOS/HTML5 的 Workspace 应用程序），反之亦然。

- 如果您在 VDA 中使用 Microsoft Teams .exe 安装程序安装了该应用程序，还需要重新启动 Microsoft Teams。建议将 .exe 安装程序用于永久 VDI 部署。在此类情况下，当 HDX 会话处于断开连接状态时，Microsoft Teams 可以自动更新。因此，重新连接到 HDX 会话的用户会发现 Microsoft Teams 未优化运行。
- 从本地会话漫游到 HDX 会话时，必须重新启动 Microsoft Teams 才能使用 HDX 进行优化。此操作是 Remote PC Access 场景中的必需操作。

## 网络要求

Microsoft Teams 依赖 Microsoft 365 中的媒体处理器服务器进行会议或多方呼叫。此外，Microsoft Teams 还依赖于 Microsoft 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 Microsoft 365 云之间的网络运行状况决定通话的性能。有关网络规划的详细指南，请参阅 [Microsoft 365 network connectivity principles](#)（Microsoft 365 网络连接原则）。

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 Microsoft 365 网络。
- 为分支机构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。
- 如果必须在分支机构使用以下任何内容，请确保 RTP/UDP 流量（由 Citrix Workspace 应用程序中的 HdxRtcEngine.exe 处理）不受阻碍。
  - 绕过代理服务器
  - 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）

### 重要：VPN 拆分通道配置

HdxRtcEngine.exe 流量必须从 VPN 通道转移，并允许使用用户的本地 Internet 连接直接连接到服务。完成此操作的方式将因所使用的 VPN 产品和计算机平台而异，但大多数 VPN 解决方案都允许对策略进行一些简单的配置以应用此逻辑。有关特定于 VPN 平台的拆分通道指南的详细信息，请参阅 [此 Microsoft 文章](#)。

Workspace 应用程序 (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 为 RTP 提供机密性和身份验证。对于此功能，对称密钥（与 DTLS 协商）用于加密媒体以及使用 AES 加密密码控制消息。

建议使用以下指标来保证正面的用户体验：

指标	Microsoft 365 的端点
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%
数据包到达抖动	在任何 15 秒时间间隔内 <30 毫秒

有关详细信息，请参阅[Microsoft Teams 准备贵组织的网络](#)。

针对带宽要求，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 和 H264 是点对点和电话会议的首选编解码器。

重要：

就性能而言，在客户端计算机上使用 CPU 时，编码比解码更昂贵。您可以在适用于 Linux 和 Windows 的 Citrix Workspace 应用程序中对最大编码分辨率进行硬编码。请参阅[编解码器性能估算器](#)和 [Microsoft Teams 的优化](#)。

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，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，然后绕过 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。此外，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。此外，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 Microsoft 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以下 Microsoft Teams 中继服务器的 FQDN：
  - `worldaz.relay.teams.microsoft.com`
  - `inaz.relay.teams.microsoft.com`
  - `uaeaz.relay.teams.microsoft.com`
  - `euaz.relay.teams.microsoft.com`
  - `usaz.relay.teams.microsoft.com`
  - `turn.dod.teams.microsoft.us`
  - `turn.gov.teams.microsoft.us`

如果 DNS 请求不成功，与外部用户的 P2P 通话和建立电话会议媒体将失败。

- 会议服务器的位置是根据第一个参与者的虚拟桌面位置（而非客户端）选择的。

## 通话建立和媒体流路径

如有可能，Citrix Workspace 应用程序 (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 高端口被阻止，媒体引擎将回退到 TCP/TLS 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。此支持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，并且您要加入多方通话或会议。HdxRtcEngine.exe 使用 Microsoft 365 中的 Microsoft Teams 传输中继服务器访问其他对等方或媒体处理器（用于举办会议）。您

的客户端计算机必须能够访问三个 Microsoft 365 子网 IP 地址范围和四个 UDP 端口（如果阻止 UDP，则可以访问 TCP/TLS 443 作为回退）。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	<b>UDP</b> : 3478、3479、 3480、3481 <b>TCP</b> : 443 (回退)

这些范围包括传输中继和媒体处理器，前端由 Azure 负载均衡器提供。

Microsoft Teams 传输中继提供 STUN 和 TURN 功能，但它们不是 ICE 端点。此外，Microsoft Teams 传输中继不会终止媒体、TLS，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 HdxRtcEngine.exe 使用 TCP）桥接到 UDP。

Workspace 应用程序 WebRTC 媒体引擎在 Microsoft 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/TLS 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 HdxRtcEngine.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”。

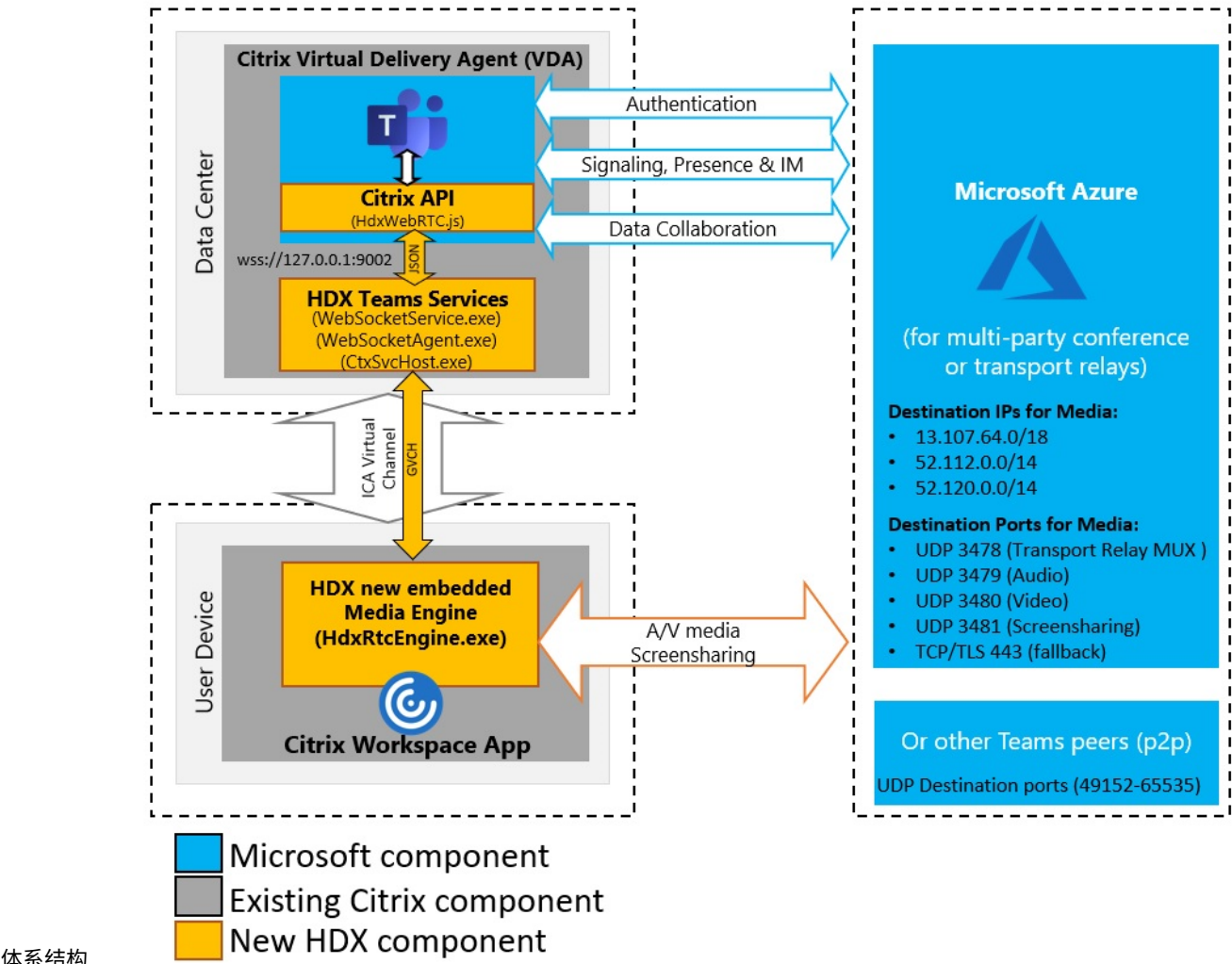
注意：

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。

# Architecture



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. Microsoft 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 Microsoft Teams Redirection Service (CtxSvcHost.exe) 来实例化通用虚拟通道。
6. Citrix Workspace 应用程序的 wfica32.exe (HDX Engine) 产生一个名为 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 Microsoft 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 HdxRtcEngine 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 Microsoft 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 HdxRtcEngine 与其他对端（或 Microsoft 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 Microsoft 365 云中对 Microsoft Teams 启用呼叫控制和 PBX。Microsoft Teams 的优化使用 Microsoft 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 (DTMF) 功能：

- 适用于 Windows 的 Citrix Workspace 应用程序版本 2102
- 适用于 Windows LTSR 1912 CU5 的 Citrix Workspace 应用程序（仅限 Windows 10 操作系统）
- 适用于 Linux 的 Citrix Workspace 应用程序 2101
- 适用于 Mac 的 Citrix Workspace 应用程序 2101
- 适用于 Chrome OS 的 Citrix Workspace 应用程序版本 2111.1

## 支持 Dynamic e911

自版本 2112 起，Citrix Workspace 应用程序支持动态紧急呼叫。在 Microsoft 通话套餐、接线员连接和直接路由中使用，它允许您执行以下操作：

- 配置和路由紧急呼叫。
- 通知安全人员。

提供通知的依据是端点上运行的 Citrix Workspace 应用程序的当前位置，而非 VDA 上运行的 Microsoft Teams 客户端。

雷·鲍姆的法律要求将 911 呼叫者的可调度位置传送到相应的公共安全应答点 (PSAP)。当与以下版本的 Citrix Workspace 应用程序结合使用时，使用 HDX 进行的 Microsoft Teams 优化符合 Ray Baum 的定律：

- 适用于 Windows 的 Citrix Workspace 应用程序版本 2112.1 及更高版本

- 适用于 Linux 的 Citrix Workspace 应用程序 2112 及更高版本
- 适用于 Mac 的 Citrix Workspace 应用程序 2112 及更高版本
- 适用于 Chrome OS 的 Citrix Workspace 应用程序版本 2112 及更高版本

要启用动态紧急呼叫，管理员必须使用 Microsoft Teams 管理中心并配置以下内容以创建网络或紧急位置图：

- 网络设置
- 位置信息服务 (LIS)

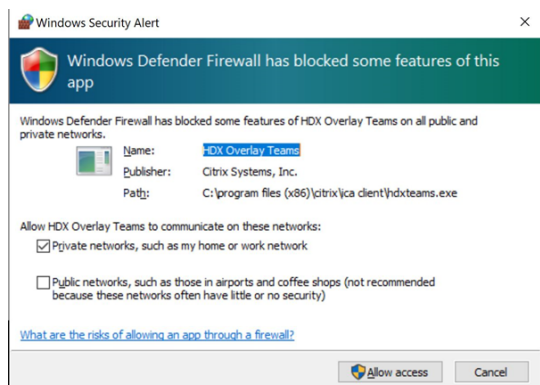
有关动态紧急呼叫的详细信息，请参阅 [Microsoft 的文档](#)。

Citrix Workspace 应用程序中继给 Microsoft Teams 的可调度位置信息如下：

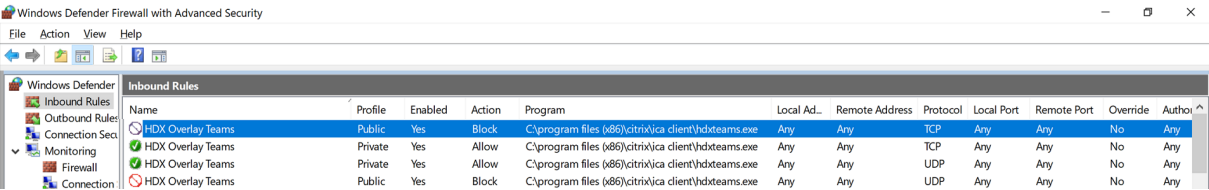
- 使用链路层发现协议 (LLDP) 进行以太网/交换机连接的机壳 ID/端口 ID。以太网/交换机 (LLDP) 在以下操作系统中受支持：
  - Windows 8.1 和 10
  - macOS，此操作系统需要 LLDP 支持软件。要下载 LLDP 支持软件，请转至 [www.microsoft.com](http://www.microsoft.com) 并搜索 LLDP 支持软件。
  - Linux，此操作系统要求将 LLDP 库包含在瘦客户端的操作系统 (OS) 发行版中。
- 安装了 Citrix Workspace 应用程序的端点的 WLAN BSSID 和 {IPv4-IPv6; 子网; MAC 地址}。
  - 适用于 Windows、Linux 和 Mac 的 Citrix Workspace 应用程序支持基于子网和 WiFi 的位置。
- 纬度和经度（如果在安装了 Citrix Workspace 应用程序的操作系统级别授予用户权限）。
  - 在所有 Workspace 应用程序平台上都受支持。但是，对于适用于 Linux 的 Citrix Workspace，您必须将 [libgps](#) 库包含在瘦客户端 (`sudo apt-get install libgps23 gpsd lldpd`) 的操作系统发行版中。

## 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 Microsoft Teams) 的通信。



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。

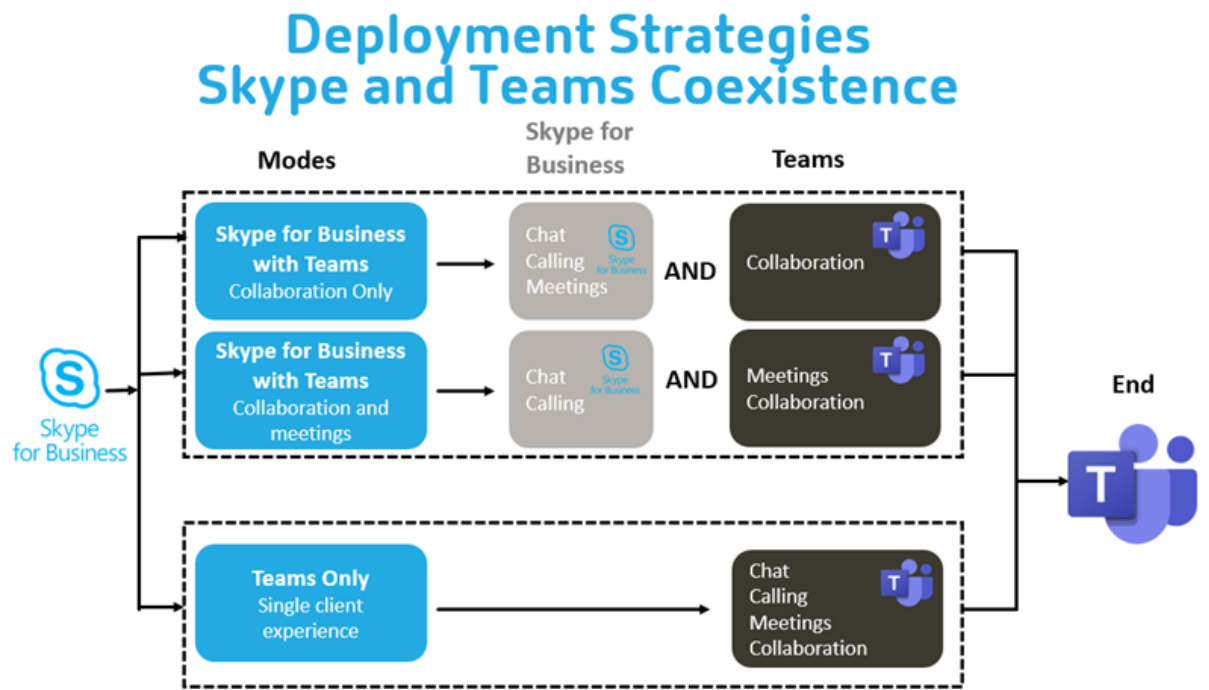


**Microsoft Teams 和 Skype for Business 同时存在**

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。示例包括孤岛模式以及 Skype for Business 与 Microsoft Teams 协作。还包括 Skype for Business 与 Microsoft Teams 协作以及会议。

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。



**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 Microsoft 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



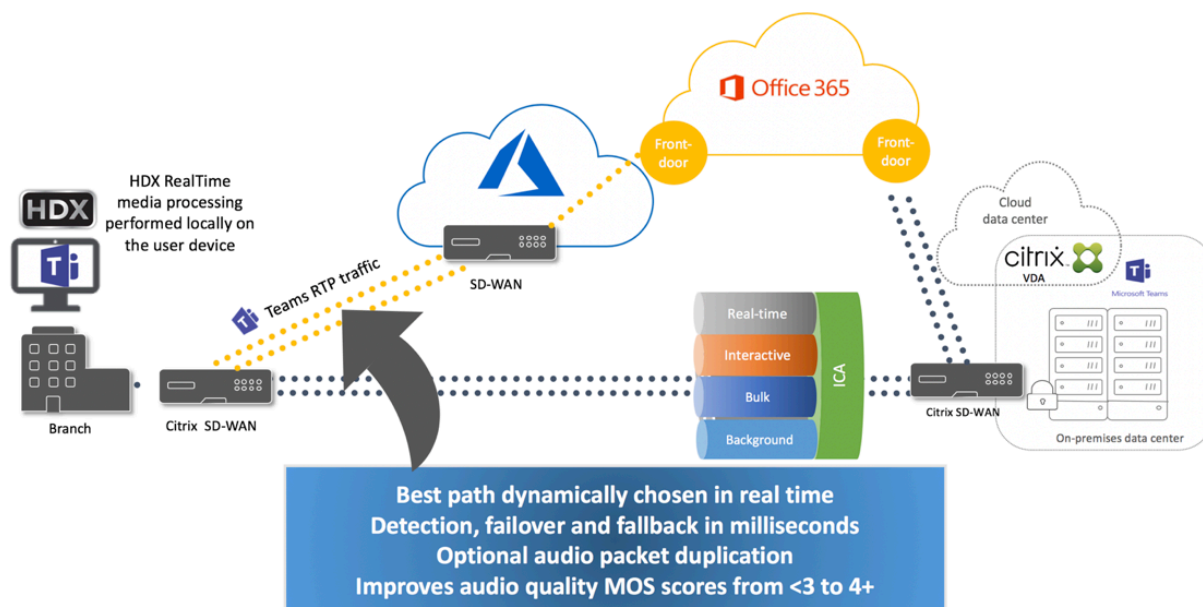
增加过多的延迟。这也可能会导致 WAN 链接上出现拥堵 Citrix SD-WAN 按照 Microsoft 365 网络连接性原则优化 Microsoft Teams 的连接性。Citrix SD-WAN 使用基于 Microsoft REST 的 Microsoft 365 IP 地址和 Web 服务以及近似 DNS。这种用法是为了识别、分类和引导 Microsoft Teams 流量。

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 Microsoft 365。此服务为所有受 Internet 限制的流量提供可靠和安全交付。

如果不考虑分支机构 Internet 连接的质量，则可能足以将延迟降至最低。请将 Microsoft Teams 流量直接从 Citrix SD-WAN 分支机构设备引导至最近的 Microsoft 365 前门，以最大程度地减少延迟。有关详细信息，请参阅 [Citrix SD-WAN Office 365 优化](#)。



## 多窗口会议和聊天

您可以在 Windows 中为 Microsoft Teams 使用多个会议或聊天窗口。有关弹出功能的详细信息，请参阅 Microsoft 365 站点上的 [Microsoft Teams Pop-Out Windows for Chats and Meetings](#) (Microsoft Teams 用于聊天和会议的弹出窗口)。

### 注意：

适用于 Windows 21H2.1、Mac 2203、Linux 2203、ChromeOS 2303 的 Citrix Workspace 应用程序支持此功能。它需要 VDA 2112 或更高版本，并已向后移植到 1912 CU6+ LTSR 和 VDA 2112。

## 背景模糊和背景效果

适用于 Windows、Mac、Linux 和 ChromeOS/HTML5 的 Citrix Workspace 应用程序支持使用 HDX 进行的 Microsoft Teams 优化中的背景模糊和背景效果。

您可以模糊背景或使用默认图像替换背景，并通过帮助对话专注于轮廓（身体和面部）来避免意外干扰。可以将此功能用于 P2P 或电话会议。

### 注意：

此功能已与 Microsoft Teams UI/按钮集成。多窗口支持是要求 VDA 更新到 2112 或更高版本的必备条件。有关详细信息，请参阅[多窗口会议和聊天](#)。

Microsoft Teams 用于背景模糊和效果的用户界面控件需要以下最低版本：

- 适用于 Windows 的 Citrix Workspace 应用程序 2207
- 适用于 Mac 的 Citrix Workspace 应用程序 2301
- 适用于 Linux 的 Citrix Workspace 应用程序 2212
- 适用于 ChromeOS 的 Citrix Workspace 应用程序 2303

### 限制：

- 将背景图像替换为 Microsoft Teams 默认图像时，客户端必须连接到 Internet。
- Microsoft Teams UI 不支持管理员和用户定义的背景图像替换。如果自定义背景图像也存储在客户端上，则可以使用客户端上的配置设置配置自定义背景图像。

## 设置自定义背景图像

仅当您不打算使用 Microsoft Teams UI 来控制该功能，或者管理员想要覆盖默认行为时，才需要以下注册表项。例如，禁用背景模糊，因为端点不够强大。

在 **Windows** 中 管理员或最终用户必须在客户端或端点上配置以下注册表项，才能设置自定义背景图像：

位置：[HKEY\\_CURRENT\\_USER\SOFTWARE\Citrix\HDXMediaStream](#)

- 名称：VideoBackgroundEffect
- 类型：DWORD
- 值：0（已禁用）、1（已启用）、2（背景图像替换）

设置为 1 的值将使背景模糊。此值可以由最终用户或管理员设置。

设置为 2 的值还需要存在 **VideoBackgroundImage** 注册表项。只有管理员才能设置此值。仅当您想要替换背景图像而非模糊背景时，才需要以下注册表项：

- 名称：VideoBackgroundImage



- 类型: REG\_SZ
- 值: my\_image\_name.jpeg

视频背景图像必须存在于 `C:\Program Files (x86)\Citrix\ICA Client` 目录中。

此注册表配置还可用于在没有 Microsoft Teams UI 选择器的情况下在 Citrix Workspace 应用程序 2206 中启用背景模糊或图像替换。换句话说,如果您的环境或 VDA 不支持多窗口,您仍然可以对 Citrix Workspace 应用程序 2206 或更高版本应用 HKCU 注册表解决方法来获得类似的结果,尽管用户无法在 HDX 会话或 Microsoft Teams 调用期间控制功能亦如此。

注册表项更改仅在 HDX 会话连接时生效。

在 **Mac** 上 用户下载的照片位置: `/Users/username/Downloads/any_image.png`

运行以下命令将自定义图像设置为默认图像:

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2
defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "/Users/username/Downloads/any_image.png"
```

在 **Linux** 中 用户下载的照片位置: `/home/username/Downloads/any_image.jpg`

创建文件 `/var/.config/citrix/hdx_rtc_engine/config.json` 并以 JSON 格式添加以下配置密钥。例如,

```
1 {
2
3
4 "VideoBackgroundEffect":2,
5
6 "VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"
7
8 }
9
10 <!--NeedCopy-->
```

在 **HTML5** 上 对于 HTML5,仅支持背景模糊。不支持自定义图像替换。

要进行背景模糊,请执行以下操作:

1. 导航到 **HTML5Client** 文件夹中的 **configuration.js** 文件。
2. 添加 **backgroundEffects** 属性并将该属性设置为 **true**。例如,

```
1 'features' : {
2
3   'msTeamsOptimization' :
4   {
5
```

```
6      'backgroundEffects' : true
7    }
8
9  }
10
11 <!--NeedCopy-->
```

### 3. 保存更改。

#### 客户端 CPU 占用注意事项

虽然模糊功能在 CPU 上很节约，但您可以预期占用量会增加。例如，在配备四核、1.5 GHz Intel® Pentium® Silver 芯片，并且 TurboBoost 最高可达 2.8 GHz 的瘦客户端上，背景模糊会使 CPU 使用率增加约 2%。平均 CPU 使用率低于 20%。

#### Microsoft Teams 中的库视图和活动扬声器

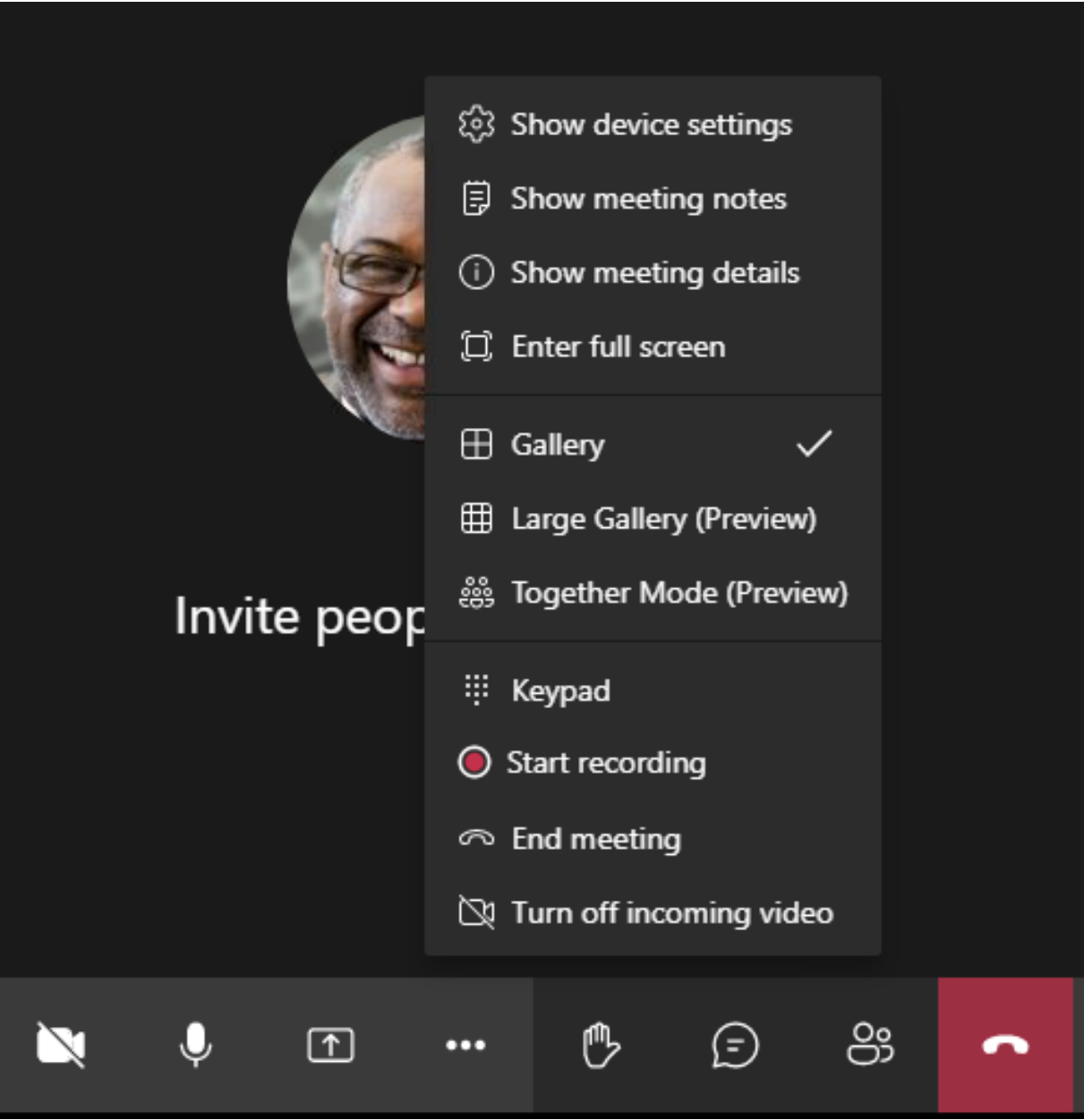
Microsoft Teams 支持 **Gallery**（库）、**Large gallery**（大型库）和 **Together mode**（共聚模式）布局。

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，Microsoft Teams 将四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。Microsoft 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。



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 及更高版本）：

- **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。

下表提供了库和大型库布局的比较：

	库视图 2x2（默认）	大型库视图
布局/网格	显示一个 2x2 网格，其中包含四名参与者的视频流。屏幕上只显示最后四个最活跃的发言者，其他参与者不会出现在网格中。	显示一个 7x7 网格，其中包含 49 个参与者的视频流。
混合技术	媒体路由器将来自每个参与者的单独流转发给每个用户。	中央会议服务器对所有音频或视频进行混合和转码，为每位参与者创建量身定制的复合布局。此操作会带来一些额外的延迟。
活跃的发言者	新的活跃发言者将替换网格中最不活跃的发言者。	显示所有参与者，无论他们是活跃的还是不活跃的参与者。
在端点进行编码	如果启用了联播，则可以在端点对一个或多个视频流进行编码。有关联播支持的详细信息，请参阅联播。	如果启用了联播，则可以在端点对一个或多个视频流进行编码。有关联播支持的详细信息，请参阅联播。
在端点进行解码	每位参与者最多可获得四个单独的媒体流。这会增加端点上 HdxRtcEngine.exe 的 CPU 占用量（用于解码/呈现）。	每个参与者只能获得一个音频和视频流。此设置降低了端点的 CPU 占用量。
最大分辨率	720p. 当四个参与者共享视频时，每个视频源的最大分辨率为 360p。如果共享视频的参与者少于四个，每个视频源的分辨率可能会更高。	720p 适用于复合布局或混合布局在复合布局中，每个参与者都不需要高质量的视频流。由于这种情况，每个发送者都会降低分辨率或上载比特率。
“用户速度缓慢”问题	发送方将每种模式的（音频/视频/屏幕共享）质量修改为参与者中最低的通用网络质量。然后将此多媒体流转发给所有其他参与者。因此，网络状况不佳的参与者会影响通话中其他所有人的质量。	不太容易受到最低的常见网络质量情况的影响。会议服务器根据单个参与者的网络状况提供不同的质量。
自助预览	在小缩略图中实时显示自己。	在缩略图中显示自己，并与其余的视频源混合。因此，您可能会看到自己包含在主视频布局中，但会有一些额外的延迟。

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。

从适用于 Windows、Linux、Mac 的 Citrix Workspace 应用程序 2109 或更高版本开始，适用于 ChromeOS 的

Citrix Workspace 应用程序 2303 用户可以同时共享屏幕和摄像机。

在早期版本中，如果您正在进行视频通话，而另一个对等方开始共享桌面，则原始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。

#### PowerPoint Live 的备注

如果您要共享来自 PowerPoint Live 的内容，则不存在此限制。在这种情况下，其他对等方仍然可以看到您的网络摄像机和内容，并来回导航以查看其他幻灯片。在这种情况下，幻灯片将在 VDA 上呈现。要访问 PowerPoint Live 幻灯片，请单击“共享托盘”按钮，然后选择其中一张建议的 PowerPoint 幻灯片，或者单击“浏览”并在您的计算机或 OneDrive 中查找 PowerPoint 文件。

传出屏幕共享也进行了优化，并卸载到 Citrix Workspace 应用程序。在这种情况下，媒体引擎仅捕获和传输 Citrix Desktop Viewer (CDViewer.exe) 窗口，并在窗口周围绘制红色边框。不会捕获与 Desktop Viewer 重叠的任何本地应用程序。

#### 注意

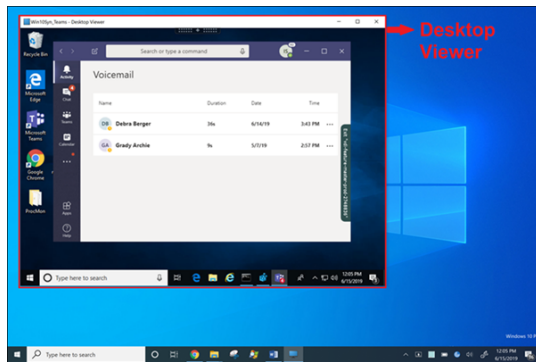
在适用于 Mac 的 Citrix Workspace 应用程序中设置特定权限以启用屏幕共享。有关详细信息，请参阅[系统要求](#)。

## 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。

已知限制：

- 如果禁用了 Desktop Viewer 或者如果正在使用 Desktop Lock，多显示器选择功能在 Microsoft Teams 屏幕选择器中将不可用。可以通过编辑 `.ICA` 文件模板或 `StoreFront web.config` 来禁用 Desktop Viewer。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。请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。
- 如果使用虚拟显示器布局功能（单个物理显示器的逻辑分区）配置 Citrix Workspace 应用程序，多显示器屏幕共享可能不起作用。在这种情况下，所有虚拟显示器都作为复合映像共享。
- 适用于 Windows 的 Citrix Workspace 应用程序的较旧版本（1907 至 2008）还共享在客户端计算机上运行的本地应用程序。仅当本地应用程序叠加在 Desktop Viewer 之上时，才能进行此共享。此行为在 2009.6 或更高版本以及 1912 CU5 或更高版本中已删除。
- 屏幕共享时，如果从窗口模式更改为全屏，屏幕共享将停止。必须停止并重新共享，才能使屏幕共享正常运行。



来自无缝应用程序的屏幕共享：

如果要将 Microsoft Teams 发布为独立的无缝应用程序，屏幕共享会捕获您的物理端点的本地桌面。需要 Citrix Workspace 应用程序 1909（最低版本）。

### 应用程序共享

自适用于 Windows 的 Citrix Workspace 应用程序 2112.1 和 VDA 2112 起，Microsoft Teams 支持应用程序共享。

从适用于 Windows 的 Citrix Workspace 应用程序 2109、适用于 Mac 的 Citrix Workspace 应用程序 2203、适用于 Linux 的 Citrix Workspace 应用程序 2209 和适用于 VDA 的 Citrix Workspace 应用程序 2109 开始，Microsoft Teams 支持在虚拟会话中运行的特定应用程序的屏幕共享。要共享特定的应用程序，请执行以下操作：

1. 在远程会话中导航到 Microsoft Teams 应用程序。
2. 在 Microsoft Teams UI 中单击共享内容。
3. 选择要在会议中共享的应用程序。红色边框出现在您选择的应用程序周围，通话中的对等方可以看到共享的应用程序。

要共享其他应用程序，请再次单击共享内容，然后选择新应用程序。

如果要禁用应用程序共享，请在 VDA 上在 `HKLM\SOFTWARE\Citrix\Graphics` 下创建以下注册表项：

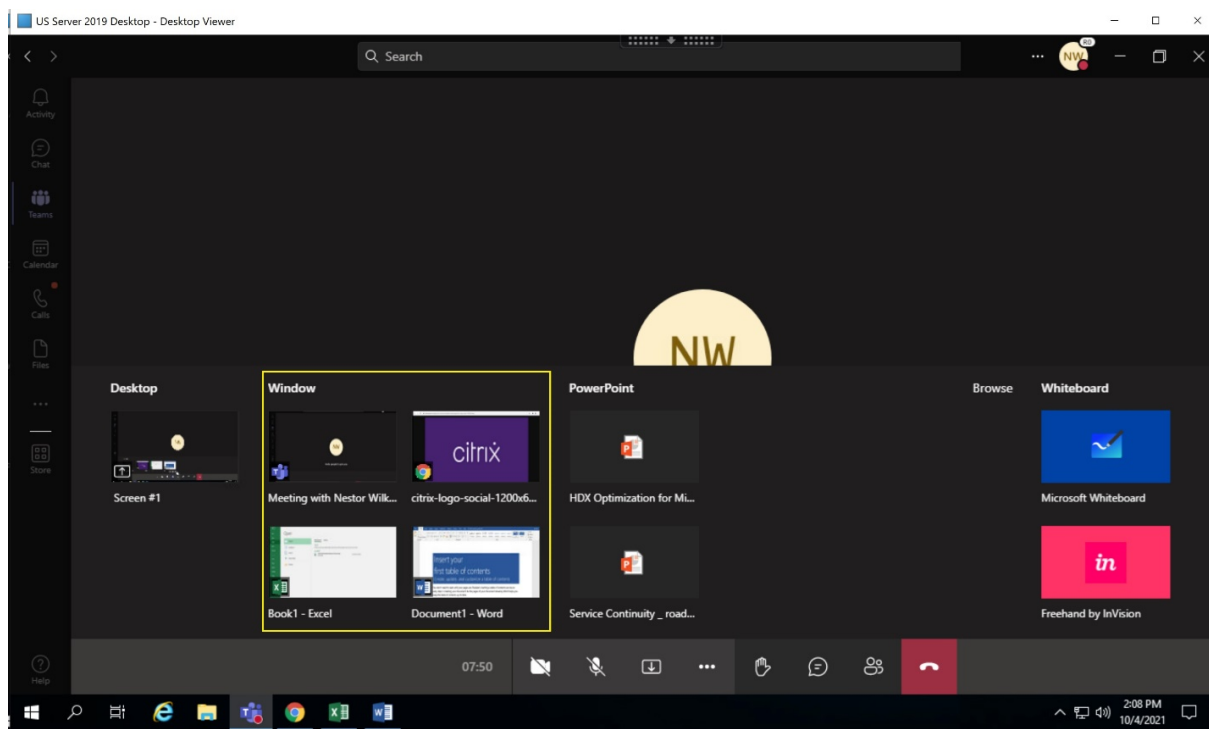
名称： `UseWsProvider`

类型： `DWORD`

值： `0`

#### 注意：

- Microsoft 推出此更新时，您可以查看 [CTX253754](#) 以获取文档更新和公告。
- 如果最小化某个应用程序，Microsoft Teams 将显示共享应用程序中的最后一张图像。您可以最大化该窗口以恢复屏幕共享。
- 屏幕共享取决于 VDA 端对窗口的捕获。内容随后将以最大速率中继到 Citrix Workspace 应用程序。最大速率为每秒 30 帧。Citrix Workspace 应用程序将内容转发给对等方或会议服务器。



特定应用程序的屏幕共享的已知限制：

- 在您通过屏幕共享共享应用程序时，鼠标指针不可见。
- 如果您在共享某个应用程序时将其最小化，屏幕选取器中只会显示该应用程序图标。应用程序的缩略图不会在屏幕选取器中预览。在最大化应用程序之前，您无法共享内容，并且红色边框不会出现。
- LAA 应用程序显示可与 VDA 中经过优化的 Microsoft Teams 中的桌面应用程序共享的应用程序列表。但是，当您从列表中选择应用程序时，结果可能与预期不符。

#### 与 **App Protection** 的兼容性

特定应用程序的屏幕共享与 HDX 优化的 Microsoft Teams 中的 App Protection 功能兼容。如果您是从启用了 App Protection 的交付组启动的应用程序或桌面，则可以对特定应用程序进行屏幕共享。

在 Microsoft Teams UI 中单击共享内容时，屏幕选取器会删除桌面选项。只能选择窗口选项来共享任何打开的应用程序。

注意：

在启用了 App Protection 功能的交付组中启动应用程序或桌面时，您将无法观看传入的视频或者查看屏幕共享。

**Microsoft Teams** 中的给予和请求控制权 以下版本的 Citrix Workspace 应用程序支持此功能（不依赖于 VDA 版本或操作系统、单会话或多会话）：

- 适用于 Windows 的 Citrix Workspace 应用程序版本 2112.1 及更高版本
- 适用于 Mac 的 Citrix Workspace 应用程序 2203.1 及更高版本
- 适用于 Linux 的 Citrix Workspace 应用程序 2203 及更高版本

- 适用于 ChromeOS 的 Citrix Workspace 应用程序版本 2303 及更高版本

参与者正在共享屏幕时，您可以在 Microsoft Teams 通话期间请求控制权。具有控制权后，您可以对共享屏幕进行选择、编辑或者执行其他键盘和鼠标活动。

要在共享屏幕时获取控制权，请单击 Microsoft Teams 用户界面中的请求控制权按钮。共享屏幕的会议参与者可以允许或拒绝您的请求。

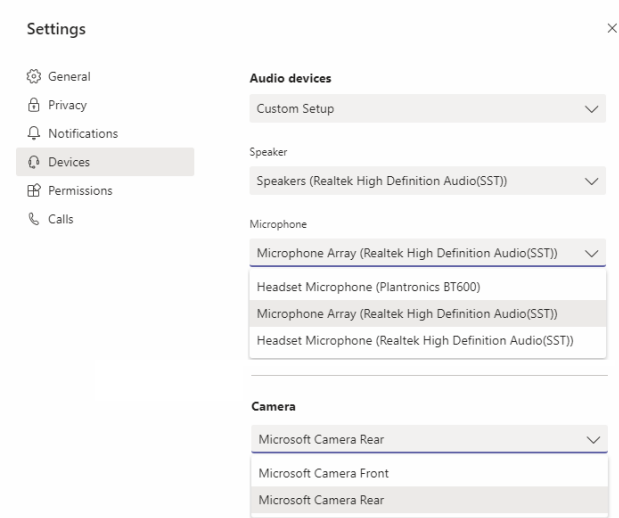
获得控制权后，您可以对共享屏幕进行选择、编辑和其他修改。对于这些操作，您可以同时使用键盘和鼠标。完成后，单击请求控制权。

限制：

- 如果用户共享单个应用程序（也称为应用程序共享），则“给予控制权”和“请求控制权”不可用。必须共享完整的桌面或显示器。
- 将控制栏固定到特定位置的功能不可用。

## 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。



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。

默认情况下，不会选择在 Microsoft Teams 处于活动状态时插入的外围设备。必须从 Microsoft Teams UI 的设置 > 设备屏幕中手动选择外围设备。选择外围设备后，Microsoft Teams 将缓存外围设备的信息。因此，当您从同一端点重新连接到会话时，系统会自动选择外围设备。

建议：



- [经 Microsoft Teams 认证的耳机](#)，内置回声消除功能。在包含额外的外围设备的设置中，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。使用外置扬声器时，请将其放置在尽可能远离麦克风的位置。此外，请将其放置在远离任何可能使声音折射到麦克风中的表面位置。
- [Microsoft Teams 认证的相机](#)，尽管 [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 Citrix 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，Microsoft 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!
```

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。

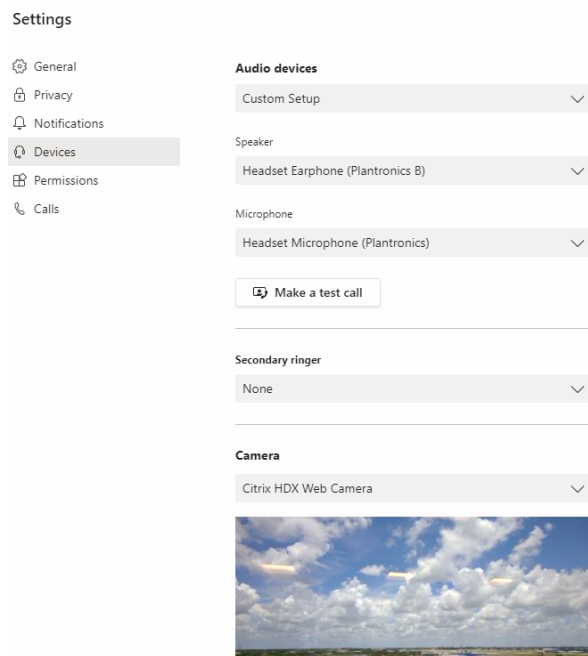
## 回退模式

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。旧版 HDX 技术可能是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。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 Microsoft Teams 版本 1.3.0.13565 或更高版本。

在查看 Microsoft Teams 应用程序中的设置 > 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。

## 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。
- 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 App Protection 加载项功能可防止出站屏幕共享，并阻止传入屏幕共享和视频。
- 用户在 VDA 上使用截图工具时无法截取 Microsoft Teams 内容的屏幕截图。但是，如果在客户端使用截图工具，则可以捕获内容。

VDA 的限制：

- 将 Citrix Workspace 应用程序的“高 DPI”设置配置为是时，重定向的视频窗口不会显示在恰当的位置。当显示器的 DPI 缩放系数设置为大于 100% 的任何值时，就会出现此限制。

Citrix Workspace 应用程序和 VDA 的限制：

- 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。

#### 联播

在 Windows 和 Mac 上为经过优化的 Microsoft Teams 视频会议通话启用了联播支持。对于 Linux，请咨询您的瘦客户端供应商。

启用联播功能后，通过调整到适当的分辨率以便为所有呼叫者提供最佳通话体验，可以改善跨不同端点的视频会议通话的质量和体验。

通过这种改进的体验，每个用户都可以提供分辨率不同（例如 720p、360p 等）的多个视频流，具体取决于多种因素，包括端点能力、网络条件等。然后，接收端点会请求其能够处理的最大质量分辨率，从而为所有用户提供最佳视频体验。

#### 注意：

此功能仅在 Microsoft Teams 推出更新后可用。有关 ETA 的信息，请访问 <https://www.microsoft.com/> 并搜索 Microsoft 365 路线图。Microsoft 推出此更新时，您可以查看 [CTX253754](#) 以获取文档更新和公告。

#### Microsoft 限制

- 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。
- 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。
- 不支持基于位置的路由和媒体旁路。
- 不支持呼叫合并（选项未显示在用户界面中）。

#### Citrix 和 Microsoft 限制

- 执行屏幕共享时，包括系统音频选项不可用。
- ChromeOS 不支持联播。

#### 即将推出的 Microsoft Teams 单窗口 EOL

2024 年 1 月 31 日，Microsoft 将在使用 VDI Microsoft Teams 优化时停用 Microsoft Teams 对单窗口用户界面的支持，仅支持多窗口体验。Microsoft 于 2023 年 8 月 9 日在 M365s 管理中心（帖子 ID: MC674419）中发布了此

次弃用通知。

有关多窗口功能的公开细节可以在 Tech Community 文章 [New Meeting and Calling Experience in Microsoft Teams](#) (Microsoft Teams 中的新建会议和通话体验) 中找到。

必须将您的 VDA 和 Citrix Workspace 应用程序升级到受支持的版本，才能继续在优化模式下使用 Microsoft Teams 进行视频和屏幕共享。如果不升级基础架构和端点以支持多窗口，则只能建立音频通话。您将无法使用经过优化的视频和屏幕共享功能。

下表说明了在 Citrix VDI 上的 Microsoft Teams 中继续使用优化通话所需的 VDA 和 Citrix Workspace 应用程序的最低版本、LTSR 版本和推荐版本：

组件	最低版本	支持 LTSR 的版本	推荐版本
Microsoft Teams	1.5.00.11865	不适用	最高版本
VDA	1912 CU6 LTSR、2203 LTSR、2112 CR	1912 CU7+、2203 CU2+	2308 CR+
适用于 Windows 的 Citrix Workspace 应用程序	2205 CR	2203 CU2+	2309 CR+
适用于 Mac 的 Citrix Workspace 应用程序	2209 CR	不适用	2308 CR+
适用于 Linux 的 Citrix Workspace 应用程序	2209 CR	不适用	2308 CR+
适用于 ChromeOS 或 HTML5 的 Citrix Workspace 应用程序	2303 CR	不适用	2309 CR+

宣布弃用 **WebRTC** 中的 **SDP** 格式（**B** 计划）

Citrix 计划在未来版本中弃用 WebRTC 对当前 SDP 格式（B 计划）的支持。必须在 WebRTC 中使用 Unified Plan 来支持经过优化的 Microsoft Teams 功能。

受影响的产品

在 Citrix Workspace 应用程序的未来版本中，将不支持在安装即将发布的 Citrix Workspace 应用程序的端点与安装了 Citrix Workspace 应用程序 2108 或更早版本的端点之间进行通话。这种通话不兼容性包括 1912 LTSR Citrix Workspace 应用程序客户端 (CWA)。以下 CWA 客户端受到影响：

- 适用于 Windows 的 Citrix Workspace 应用程序
- 适用于 Linux 的 Citrix Workspace 应用程序
- 适用于 Mac 的 Citrix Workspace 应用程序

- 适用于 Chrome 的 Citrix Workspace 应用程序

## B 计划的替代方案

如果您运行的 Citrix Workspace 应用程序版本早于 2109，则必须升级到受支持的版本（最好是最新的 CR 版本）。否则，任何使用未来版本或更高版本的端点的通话都将无法连接。如果联合合作伙伴尚未升级其 Citrix Workspace，则未来版本与您的联合通信合作伙伴之间的通话也可能无法完成。

Citrix Workspace 应用程序版本 2108 已于 2023 年 3 月结束其支持日期，必须升级到更新的版本。有关详细信息，请参阅 [Workspace 应用程序](#)，详细了解 Citrix Workspace 应用程序版本支持。

有关弃用 B 计划的详细信息，请参阅 [WebRTC](#) 文档。

## 其他信息

- [监视、故障排除和支持 Microsoft Teams](#)
- [将 Microsoft 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](#)

## Windows Media 重定向

March 30, 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

March 30, 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

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

March 30, 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。

## 双向内容重定向配置

February 9, 2024

双向内容重定向允许根据配置将 URL 从客户端重定向到服务器或从服务器重定向到客户端。此策略设置取代了以下三个已过时的设置：

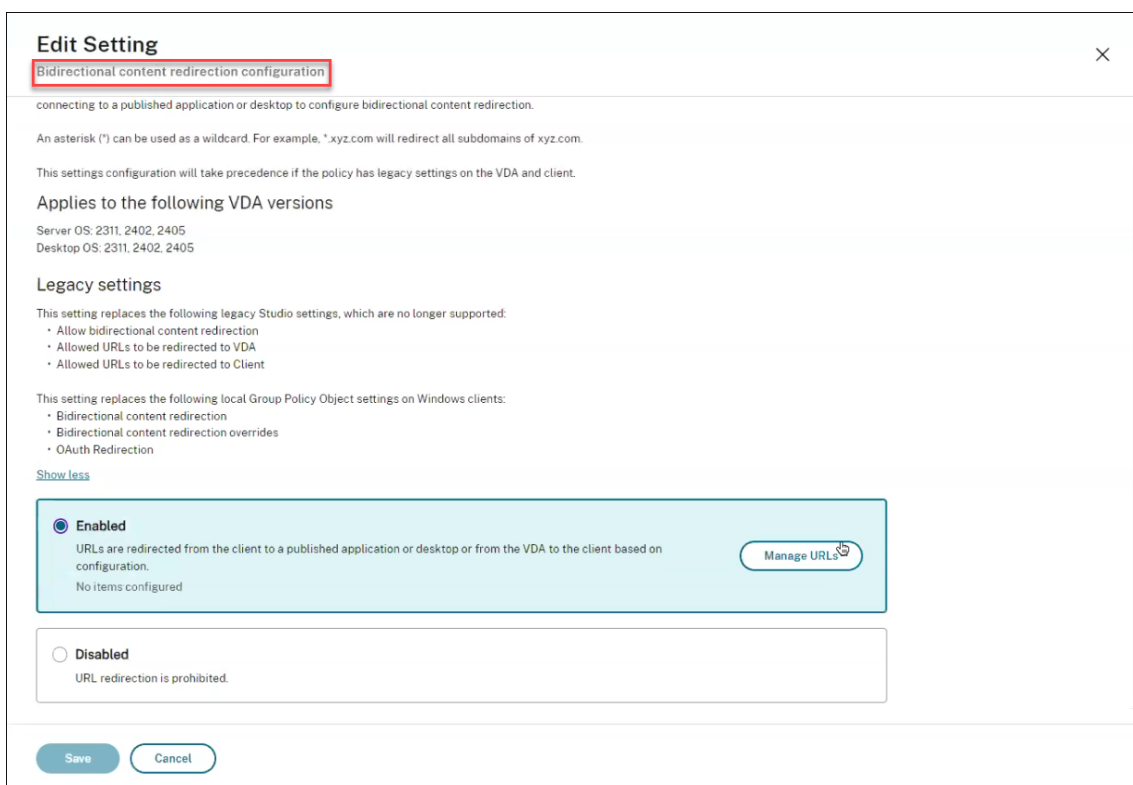
- 允许双向内容重定向
- 允许重定向到 VDA 的 URL
- 允许重定向到客户端的 URL

它还取代了 Windows 客户端上的以下三个本地 GPO 设置：

- 双向内容重定向
- 双向内容重定向覆盖
- OAuth 重定向

如果配置了此设置，此设置将优先于 Studio 和客户端中的旧设置。要配置双向内容重定向策略，请执行以下操作：

1. 在 Citrix DaaS 配置页面上，单击“管理”选项卡。
2. 单击策略选项卡。
3. 单击创建策略。“创建策略”刀片打开。
4. 在搜索字段中搜索 **Bidirectional content redirection configuration**，选中复选框并单击“编辑”。
5. 在“编辑设置”刀片中，将此策略设置为“已启用”，然后单击“管理 URL”。



**Edit Setting**

**Bidirectional content redirection configuration**

connecting to a published application or desktop to configure bidirectional content redirection.

An asterisk (\*) can be used as a wildcard. For example, \*.xyz.com will redirect all subdomains of xyz.com.

This settings configuration will take precedence if the policy has legacy settings on the VDA and client.

**Applies to the following VDA versions**

Server OS: 2311, 2402, 2405  
Desktop OS: 2311, 2402, 2405

**Legacy settings**

This setting replaces the following legacy Studio settings, which are no longer supported:

- Allow bidirectional content redirection
- Allowed URLs to be redirected to VDA
- Allowed URLs to be redirected to Client

This setting replaces the following local Group Policy Object settings on Windows clients:

- Bidirectional content redirection
- Bidirectional content redirection overrides
- OAuth Redirection

[Show less](#)

☒ **Enabled**

URLs are redirected from the client to a published application or desktop or from the VDA to the client based on configuration.  
No items configured

[Manage URLs](#)

☐ **Disabled**

URL redirection is prohibited.

[Save](#) [Cancel](#)

6. 在“管理 URL”刀片中，对于 VDA 到客户端重定向，请指定以下内容：

- **URL（必填）**：添加应从 VDA 重定向以在客户端上打开的 URL。对于 OAuth 重定向，请在客户端上设置身份验证方案和模式，以将会话重定向回主机。
- **模式（可选）**：URL 正则表达式，当通过 VDA 到客户端 URL 重定向到客户端时，会像启动 OAuth 身份验证流程一样对其进行跟踪；当流程完成时（由打开的结果架构或重定向 URL 模式检测到），生成的 URL 将被重定向回启动该流程的主机 VDA。
- **方案（可选）**：如果指定了架构，则终止 URL 的格式应为：**scheme://<something>**。如果未指定“方案”（空），则通过正则表达式捕获组（必须在模式中指定）从模式中提取原始生成的 URL。



模式，并将原始 URL 重写为使用 `citrix-oauth-redir://` 重定向 URL。流程完成后，原始重定向 URL 将被重定向回主机 (VDA)。在这种情况下，必须将任何 OAuth 授权服务器配置为允许 `citrix-oauth-redir://byIndex/1 (2, 3, ... N)` 重定向 URL。

注意：

尽管模式和方案都是可选的，但如果指定了模式，则还必须指定模式。

7. 在“管理 **URL**”刀片中，对于客户端到 **VDA** 重定向，请指定以下内容：

- 类型：选择桌面或应用程序。
- 名称：为该类型提供一个名称。
- **URL**：提供您要重定向到源的 URL。您可以添加多个 URL 并删除不需要的 URL

8. 单击保存。“编辑设置”刀片显示已配置的项目数量。

9. 单击保存。“创建策略”刀片显示配置的当前值。单击下一步。

10. 在“将策略分配给”步骤中，单击“下一步”。

11. 在“摘要”步骤中，选中“启用策略”复选框并在“策略名称”字段中提供名称。

12. 单击完成。策略已列出。

13. 选择创建的新策略以查看配置的设置。

有关传统设置，请参阅[主机到客户端重定向](#)和[双向内容重定向](#)。

## 主机到客户端重定向

February 9, 2024

注意：

本文介绍了传统的主机到客户端的重定向设置。有关最新设置，请参阅[双向内容重定向配置](#)。新策略设置将优先于旧版设置。Citrix 建议仅使用新策略设置并删除所有旧版设置，以避免出现意外行为。

主机到客户端重定向允许在用户终端设备上使用相应的应用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网页上访问或在 Citrix 会话中运行的网络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

使用“**主机到客户端**”重定向 Citrix 策略来启用此功能。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 应用程序向 Windows 服务器注册，以确保它可以拦截 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。

```
1 <?xml version="1.0" encoding="UTF-8"?>
2
3 <DefaultAssociations>
4
5 <Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="
   ServerFTA" />
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
- 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://;customtype2://`

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

要为一组特定的网站启用主机到客户端的重定向，请在服务器 VDA 上创建注册表项和值。

- 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

启用本节中提及的主机到客户端重定向将取代服务器 VDA 上先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

February 9, 2024

注意：

本文介绍了旧版双向内容重定向设置。有关最新的策略设置，请参阅[双向内容重定向配置](#)。新策略设置将优先于旧版设置。Citrix 建议仅使用新策略设置并删除所有旧版设置，以避免出现意外行为。

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：

- 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：

```
%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。

## 从 Citrix VDA 到客户端的通配符重定向

双向内容重定向支持在定义要重定向的 URL 时使用通配符。要配置双向内容重定向，请参阅[配置说明](#)。

在 Citrix Studio 中，在允许重定向到客户端的 **URL** 中设置通配符 URL。星号 (\*) 属于通配符。

注意：

- 请勿在客户端策略中设置允许重定向到 VDA 的 **URL**。确保站点设置了允许重定向到 VDA 的 **URL**，以避免无限次循环执行重定向操作。
- 不支持顶级域。例如，[https://www.citrix.\\*](https://www.citrix.*) 或 [http://www.citrix.co\\*](http://www.citrix.co*) 未重定向。

## 从 VDA 到客户端的自定义协议重定向

双向内容重定向支持将自定义协议从 Citrix VDA 重定向到客户端。支持 HTTP 或 HTTPS 以外的协议。要配置双向内容重定向，请参阅[配置说明](#)。

在 Citrix Studio 中，在允许重定向到客户端的 **URL** 中设置自定义协议。

注意：

- 客户端必须注册了一个应用程序才能处理该协议。否则，URL 会重定向到客户端并且无法启动。
- 您在 Chrome 和 Edge 浏览器中输入或启动的自定义协议 URL 不受支持，也不会重定向。
- 不支持以下协议：[rtsp://](#)，[rtspu://](#)，[pnm://](#)，[mms://](#)。

## 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

June 13, 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：

- 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。

## 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：

- Edge，最新版本
- Firefox，最新版本和扩展的支持版本
- Chrome，最新版本

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）。
  - 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为启用，则不支持浏览器内容重定向。

## 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：

- 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. 在管理 > 完整配置中，选择左侧窗格中的策略。
2. 在操作栏中选择创建策略。
3. 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。
4. 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。
5. 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。
6. 在“编辑设置”窗口中，单击添加以添加 URL，然后单击确定。
7. 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。
8. 在“编辑设置”窗口中，单击添加以添加 URL，然后单击确定。
9. 在“设置”页面上，单击下一步。
10. 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。
11. 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，请执行以下步骤：

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

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[入门](#)和搜索组策略对象管理模板。
- 仅当您将 `CitrixBase.admx/CitrixBse.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 Citrix DaaS 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. 在管理 > 完整配置中，选择左窗格中的应用程序。
2. 在中上部的窗格中，右键单击空白区域，然后从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。
3. 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
```

## 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

February 9, 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。

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。
- 使用 Citrix 软件将会话代理到 Azure 虚拟机时，Citrix 将为 USB 重定向到 Azure 虚拟机提供最大努力支持。我们支持修复 Citrix 软件问题，但我们不支持基础 Azure 虚拟机。
- 可以重定向具有光盘刻录功能的 CD/DVD 设备，但不能使用这些设备的刻录功能。这是由于会话的缓冲区限制。

## 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。

## 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、Windows Server 2016、Windows Server 2019 或 Windows Server 2022。
- 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](#)。

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。



## Edit Setting

### Client USB device redirection

☒ Allowed  
This setting will be allowed.

☐ Prohibited  
This setting will be prohibited.

▼ Applies to the following VDA versions

Server OS: 7.0, 7.1, 7.5, 7.6, 7.7, 7.8, 7.9, 7.11, 7.12, 7.13, 7.14, 7.15, 7.16, 7.17, 7.18, 1808, 1811, 1903, 1906, 1909, 1912, 2003, 2006, 2009, 2012, 2103, 2106, 2109

Desktop OS: 5.6, 7.0, 7.1, 7.5, 7.6, 7.7, 7.8, 7.9, 7.11, 7.12, 7.13, 7.14, 7.15, 7.16, 7.17, 7.18, 1808, 1811, 1903, 1906, 1909, 1912, 2003, 2006, 2009, 2012, 2103, 2106, 2109

▼ Description

Enables or disables redirection of USB devices to and from the client (workstation hosts only).

▼ Related settings

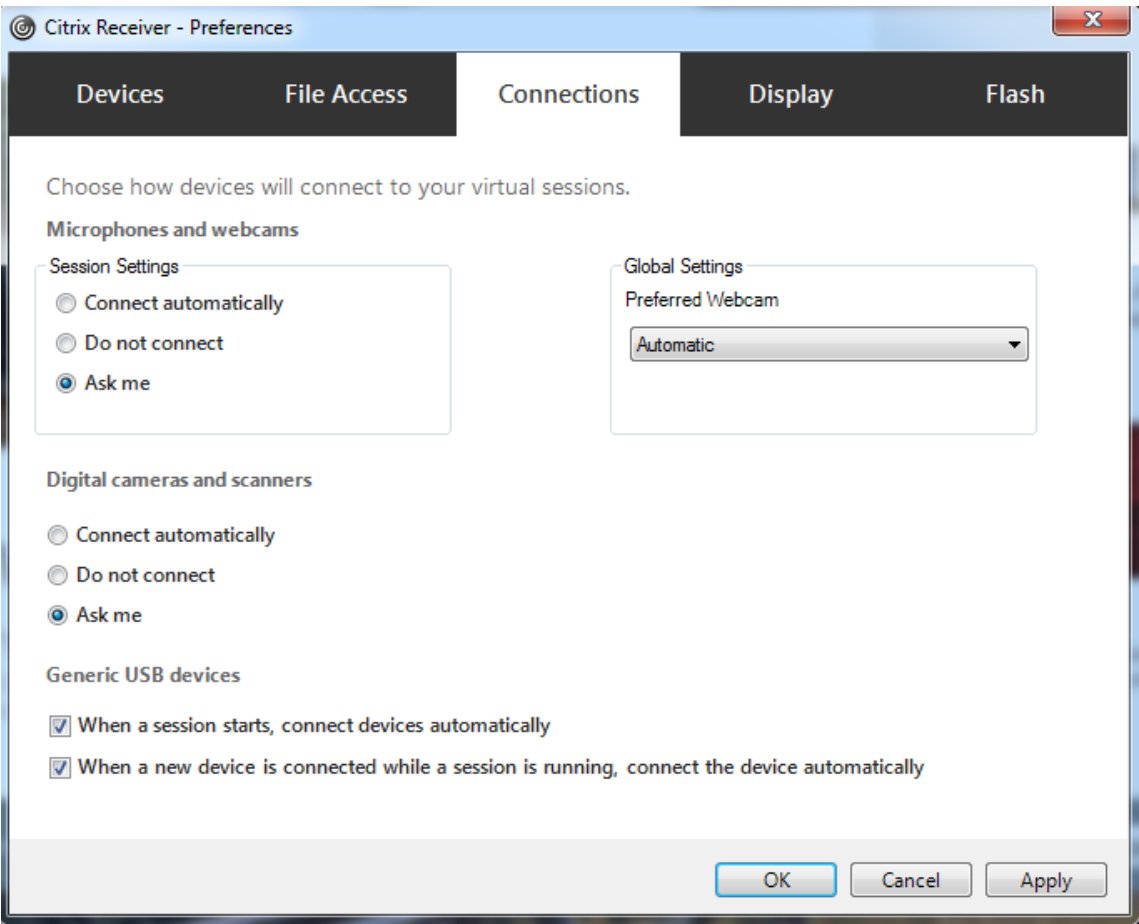
Client USB device redirection rules

SaveCancel

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。



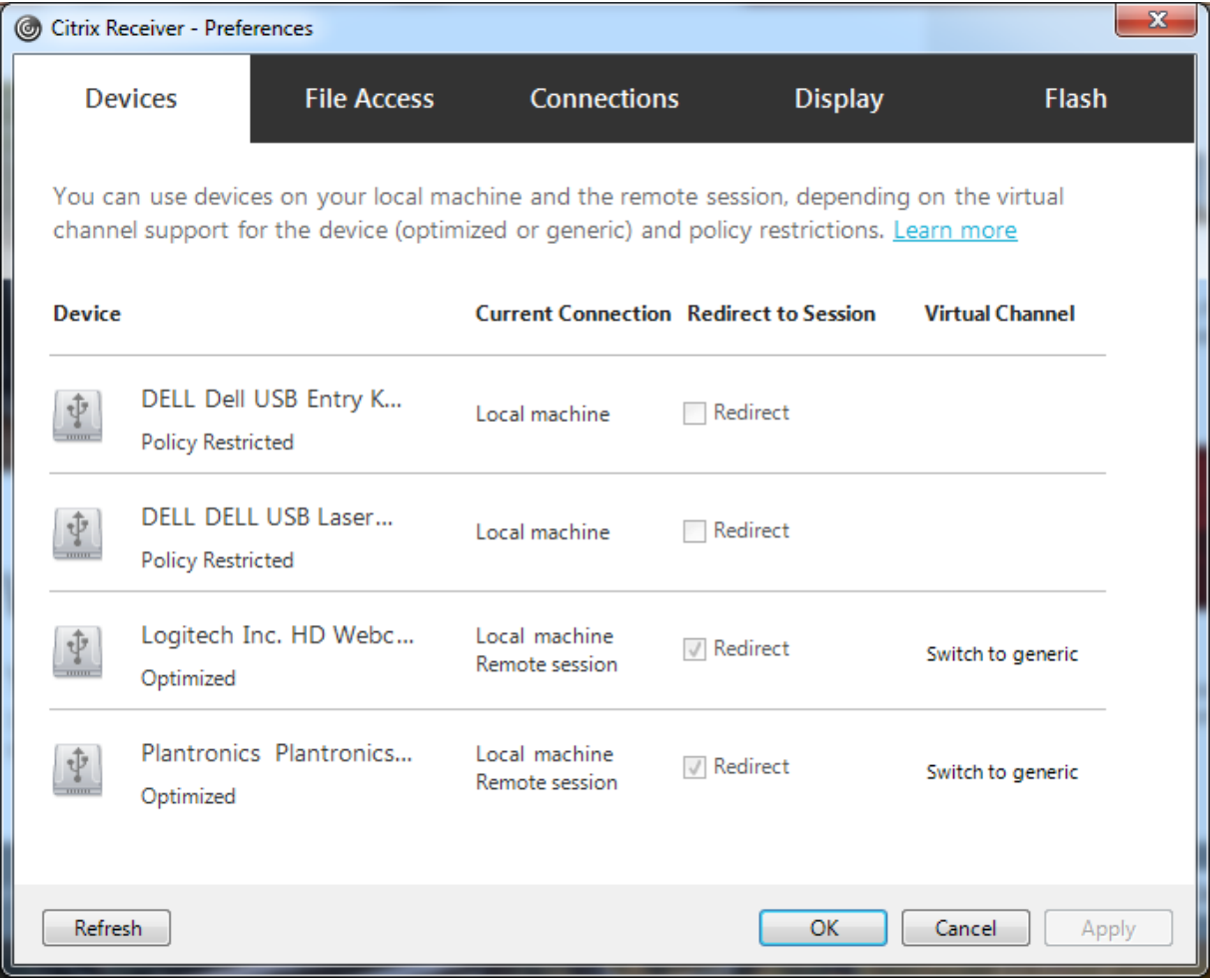
如果已在上一步中为 VDA 指定了 USB 策略规则，请为 Citrix Workspace 应用程序指定相同的策略规则。

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](#)。



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。

- 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。

可以通过同时为 VDA 和 Citrix Workspace 应用程序指定 USB 设备重定向规则以覆盖默认 USB 策略规则，来控制可进行通用 USB 重定向的 USB 设备。

对于 VDA：

- 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：
  - 对于 x64: dvd root \os\lang\x64\Citrix Policy\ CitrixGroupPolicyManagement\_x64.msi
  - 对于 x86: dvd root \os\lang\x86\Citrix Policy\ CitrixGroupPolicyManagement\_x86.msi

在适用于 Windows 的 Citrix Workspace 应用程序上：

- 编辑用户设注册表。安装介质中包含一个管理模板（ADM 文件），以便您可以通过 Active Directory 组策略更改用户设备：

dvd root \os\lang\Support\Configuration\icaclient\_usb.adm

警告：

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

产品的默认规则存储在 HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules 中。请勿编辑这些产品默认规则，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 HKLM\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRules 中。GPO 策略规则的格式为 **{Allow: | Deny:}**，后接一组以空格分隔的 *tag=value* 表达式。

支持以下标记：

标记	说明
VID	设备描述符中的供应商 ID
PID	设备描述符中的产品 ID
REL	设备描述符中的版本 ID
类	设备描述符或接口描述符中的类；请参阅 USB Web 站点 <a href="http://www.usb.org/">http://www.usb.org/</a> 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

标记	说明
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：

- 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。

管理

September 1, 2023

Citrix 通过在 Citrix Cloud 中安装和维护核心组件和功能来管理 Citrix Virtual Apps and Desktops 服务部署。您负责管理资源位置中用于交付应用程序和桌面的计算机 (VDA)。您还负责管理与这些资源位置的连接以及应用程序、桌面和用户。

- **Autoscale**：一致的高性能解决方案，以主动管理您的计算机的电源。
- **应用程序**：管理交付组中的应用程序。

- **虚拟 IP 和虚拟环回**：Microsoft 虚拟 IP 地址功能为每个会话的已发布应用程序提供动态分配的唯一 IP 地址。通过 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。
- **VDA 注册**：VDA 必须在 Cloud Connector 中注册（建立通信），才能有助于应用程序和桌面的交付。可以使用多种方法指定 Cloud Connector 地址，如本文中所述。添加 Cloud Connector 时，VDA 必须具有最新信息。
- **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。
- **使用搜索**：要在“完整配置”管理界面中查看有关计算机、会话、计算机目录、应用程序或交付组的信息，请使用灵活的搜索功能。
- **IPv4/IPv6 支持**：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。
- **Profile management**：安装 VDA 时可以安装 Citrix Profile Management。如果要使用此用户配置文件解决方案，请查看其文档。
- **Citrix Insight Services**：Citrix Insight Services (CIS) 是用于性能监测、遥测以及生成业务见解的 Citrix 平台。安装 VDA 时将收集分析和诊断信息。
- **本地主机缓存**：本地主机缓存功能允许在资源位置中的 Cloud Connector 无法与 Citrix Cloud 通信时继续执行连接代理操作。还提供了**规模、大小和其他配置注意事项**。
- **委派管理**：借助委派管理，您可以根据管理员在组织中的角色配置所有管理员所需的访问权限。
- **配置日志记录**：配置日志记录可跟踪配置更改和管理活动。
- **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。
- **许可证**：您可以从 Citrix Cloud 控制台查看此服务的 Citrix 许可证使用信息。
- **平衡计算机负载**：您可以控制如何平衡计算机的负载。

## 自适应访问

June 24, 2022

在当今不断变化的形势下，应用程序安全性对任何企业都至关重要。做出具有上下文意识的安全决策，然后启用对应用程序的访问权限可在允许用户访问的同时降低相关风险。

自适应访问功能提供了全面的零信任访问方法，可提供对应用程序的安全访问。自适应访问使管理员能够根据上下文提供用户可以访问的应用程序的精细级别访问权限。术语“上下文”是指：

- 用户和组（用户和用户组）
- 设备（台式机或移动设备）
- 位置（地理位置或网络位置）
- 设备状态（设备状态检查）
- 风险（用户风险评分）

## Device Posture

March 5, 2024

Citrix Device Posture Service 是一种基于云的解决方案，可帮助管理员强制执行终端设备必须满足的某些要求，才能访问 Citrix DaaS（Citrix Virtual Apps and Desktops）或 Citrix Secure Private Access 资源（SaaS 和 Web 应用程序或 TCP 和 UDP 应用程序）。通过检查设备的状态来建立设备信任对于实现基于零信任的访问至关重要。Device Posture 服务在允许最终用户登录之前检查终端设备的合规性（托管/BYOD 和安全状态），从而在您的网络中强制执行零信任原则。

有关详细信息，请参阅 [Device Posture](#)。

## 自适应身份验证服务

March 30, 2024

Citrix Cloud 客户可以使用 Citrix Workspace 向 Citrix DaaS 提供自适应身份验证。自适应身份验证是一项 Citrix Cloud 服务，可为登录 Citrix Workspace 的客户和用户启用高级身份验证。自适应身份验证服务是 Citrix 托管并由 Citrix Cloud 托管的 ADC，可提供所有高级身份验证功能，例如：

- 使用不同的身份验证方法（例如 AD、RADIUS、证书、使用 SAML 2.0、OAuth、OIDC、谷歌验证码的多个第三方 IdP）进行多重身份验证。
- 根据位置、设备状态和用户组等因素验证用户身份和授权级别。
- 启用对 DaaS（虚拟化）和 SPA（Web 和 SaaS 应用程序等非虚拟化资源）的上下文或智能访问。
- 登录页面自定义

有关自适应身份验证的完整详细信息，请参阅 [自适应身份验证服务](#)。

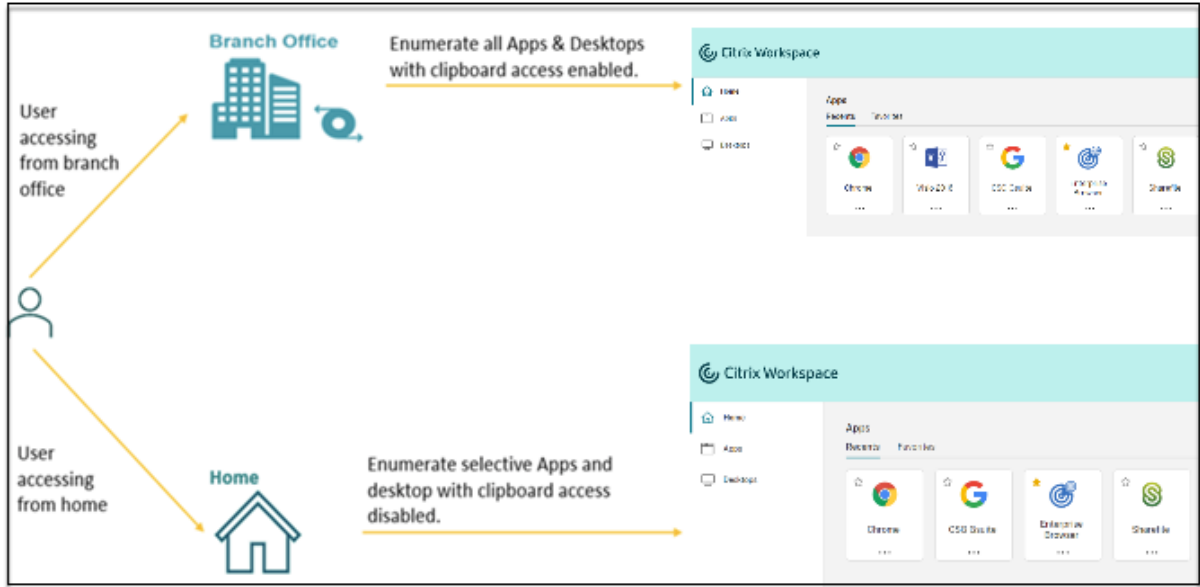
## 基于用户网络位置的自适应访问

February 9, 2024



Citrix Workspace 自适应访问功能使用高级策略基础结构，允许根据用户的网络位置访问 Citrix DaaS。该位置是使用 IP 地址范围或子网地址定义的。

管理员可以定义策略，根据用户的网络位置枚举或不枚举虚拟应用程序和桌面。管理员还可以根据用户的网络位置通过启用或禁用剪贴板访问权限、打印机、客户端驱动器映射等来控制用户操作。例如，管理员可以设置策略，使在家中访问资源的用户对应用程序具有有限的访问权限，而从分支机构访问资源的用户具有完全访问权限。



管理员可以实施以下策略来访问应用程序：

- 仅从公司所在地或其分支机构列举一些敏感应用程序。
- 如果员工从外部网络访问工作区，请勿枚举敏感应用程序。
- 请禁用从分支机构访问打印机的功能。
- 当用户不在公司网络中时，请禁用剪贴板访问和打印机访问权限。

应享权利

自适应访问功能适用于拥有以下任何许可证的客户。

- DaaS Premium / Premium Plus
- Secure Private Access Advanced

必备条件

- 确保启用 自适应访问 功能（**Citrix Workspace** > 访问 > 自适应访问）。有关详细信息，请参阅 [启用自适应访问功能](#)。

启用自适应访问后，DaaS 访问策略将更新为使用“通过 **Citrix Gateway** 进行连接”选项。

注意：

NetScaler Gateway 需要在 DaaS 访问策略中添加智能访问标签。但是，由于 DaaS 使用来自设备状态、自适应访问和自适应身份验证服务的标签，因此不必在设置中配置 NetScaler Gateway。

- 了解位置标签。有关详细信息，请参阅 [网络位置标记](#)。

需要注意的事项

仅当您想根据位置限制应用程序枚举时，以下几点才适用。如果您计划使用自适应访问根据网络位置限制用户控制，例如禁用剪贴板访问、打印机重定向、客户端驱动器映射，则可以忽略这些准则。

- 在创建交付组时，如果选择将用户管理留给 **Citrix Cloud** 选项，则无法应用智能访问策略（例如，根据网络位置对 Citrix DaaS 进行自适应访问）。这是因为交付组成为库产品，因此不由 Web Studio 处理。
- 如果您计划根据网络位置有选择地枚举 Citrix DaaS，则必须使用 Citrix Studio 策略而不是工作区对这些交付组执行用户管理。创建交付组时，在用户设置中，选择限制使用此交付组用户或允许任何经过身份验证的用户使用此交付组。这使您能够在交付组下的访问策略选项卡中配置自适应访问。

Create Delivery Group

Introduction

Machines

Users

Desktops

App Protection

Scopes

License Assignment

Policy Set

Local Host Cache

Summary

Users

Specify who can use the applications and desktops in this delivery group. You can assign users and user groups who log on with valid credentials.

Allow any authenticated users to use this delivery group.

Restrict use of this delivery group:

Sessions must launch in a user's home zone, if configured.

To let non-Active Directory users (for example, Azure AD and Okta users) launch Active Directory joined machines, select the following option:

Allow users not in Active Directory to use this delivery group

- 启用自适应访问后，对直接工作负载连接进行了更改。
  - 位置标签 字段在 **Citrix Cloud > 网络位置 > 添加网络位置 > 位置标签** 中可见。
  - 现有的直接工作负载连接策略按预期运行。
  - 必须在网络位置服务（不定义标签）和交付组上创建新策略。此外，网络连接类型必须为“内部”。

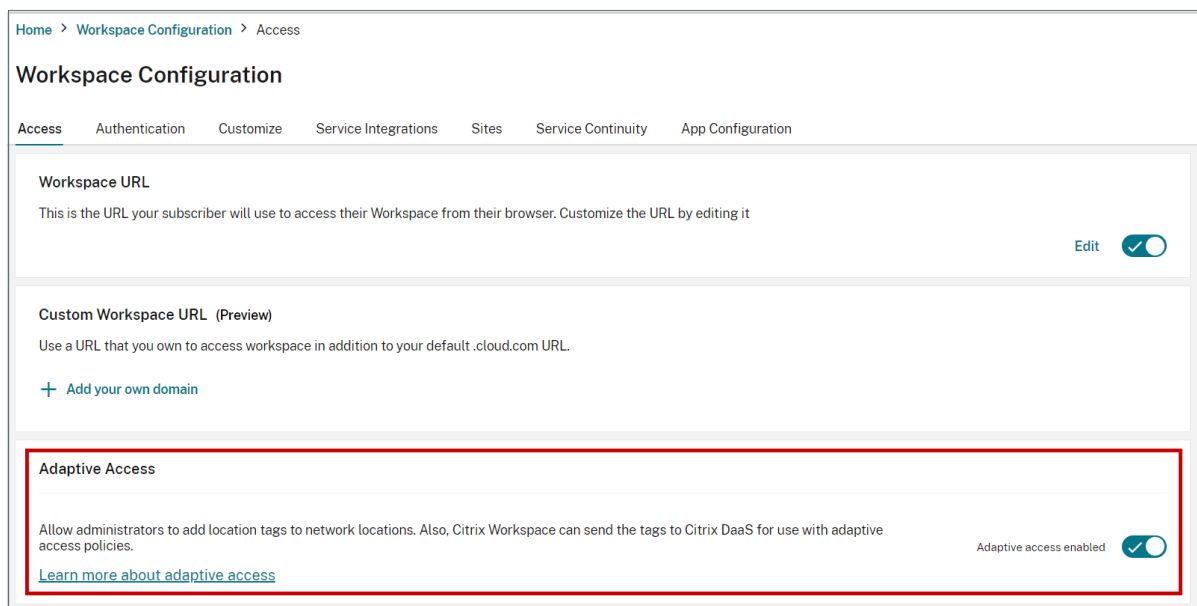
© 1999–2024 Cloud Software Group, Inc. All rights reserved.


1019

- 对于带有标签的直接工作负载连接的新策略，必须在网络位置服务中定义标签，还必须在 DaaS Studio 中的交付组或访问策略上定义相同的标签。此外，网络连接类型必须为“内部”。位置标签与直接工作负载连接无关。
- 建议您使用以下方法测试您的 Citrix DaaS 部署。
  - 请标识一个测试交付组或创建一个交付组来实施此功能。
  - 创建策略或标识可用于测试交付组的策略。

### 启用自适应访问功能

1. 登录 Citrix Cloud。
2. 从汉堡菜单中选择“**Workspace** 配置”。
3. 默认情况下，自适应访问 开关处于关闭状态。打开“自适应访问”开关。
4. 在确认消息上单击“是，启用自适应访问”。





**Are you sure you want to enable adaptive access?**


If you enable adaptive access, Web Studio access policies will be enforced as if all connections were routed through Citrix Gateway.

Yes, enable adaptive access

No, keep adaptive access disabled


启用自适应访问后，您可以定义自适应访问的位置标记（**Citrix Cloud** > 网络位置 > 添加网络位置 > 位置标记）。

**Add a Network Location**


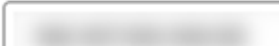



Adaptive access based on network locations allow you to specify networks in your organization. Administrators can now define tags for the users accessing from defined locations and use these tags in access policy rules in DaaS for resource enumeration and access type for the resources.


Location name


Argentina-loc

Public IP address range





Location tags 

Argloc1, Argloc2

 Define location tags for adaptive access.  
If you are configuring direct workload connection, location tags can be skipped.

Choose a network connectivity type:

☒ Internal 

☐ External 

Save

禁用自适应访问后，您无法添加网络位置。在这种情况下，位置标签不适用。

## Add a Network Location

Adaptive access based on network locations allow you to specify networks in your organization. Administrators can now define tags for the users accessing from defined locations and use these tags in access policy rules in DaaS for resource enumeration and access type for the resources.

Location name


Argentina

Public IP address range

Save

重要提示:

当您尝试禁用自适应访问功能时，会出现以下消息。请注意，禁用该功能后，Workspace 不会将标签发送到 DaaS 以进行自适应访问。

**Are you sure you want to disable adaptive access?**

If you disable adaptive access, Citrix Workspace will not send the tags to Citrix DaaS for use with adaptive access policies. This will also impact your device posture service if enabled.

Yes, disable adaptive access

No, keep adaptive access enabled

## 配置自适应访问

根据网络位置配置自适应访问涉及以下高级步骤。

1. 定义网络位置策略
2. 在 DaaS Studio 中定义标签

在配置示例中，选择了两种用户类型（**BranchOffice** 用户和 **WorkFromHome** 用户）来实现以下用例。

- BranchOffice 用户必须能够访问具有所有访问权限的应用程序。
- WorkFromHome 用户不得具有剪贴板访问权限。

在此配置示例中，使用“家庭”和“办公室”作为示例中的标签。

#### 配置网络位置策略

1. 登录 Citrix Cloud。
2. 从汉堡菜单中选择“网络位置”。  
确保已启用“自适应访问”开关。否则，将显示直接工作负载连接的用户界面。
3. 单击“添加网络位置”。
  - 位置名称：为策略输入相应的名称。  
示例：BranchOffice 或 WorkFromHome
  - 公有 IP 地址范围：定义网络的公有 IP 地址范围。  
示例：172.9.2.1-172.9.2.30
  - 位置标签：为您的位置定义标签。这可以是指您所在位置的名称。这些标记用于在 Citrix Studio 中配置自适应访问策略。有关详细信息，请参阅在 **Citrix Studio** 中定义标记。  
示例：办公室 或 家庭
  - 连接类型：定义应用程序启动类型。  
内部 - 绕过网关启动应用程序。  
外部 - 使用 Citrix Gateway 服务或传统网关启动应用程序。
4. 单击保存。

现在，您可以在 DaaS Studio 上使用这些标签来启用自适应访问。

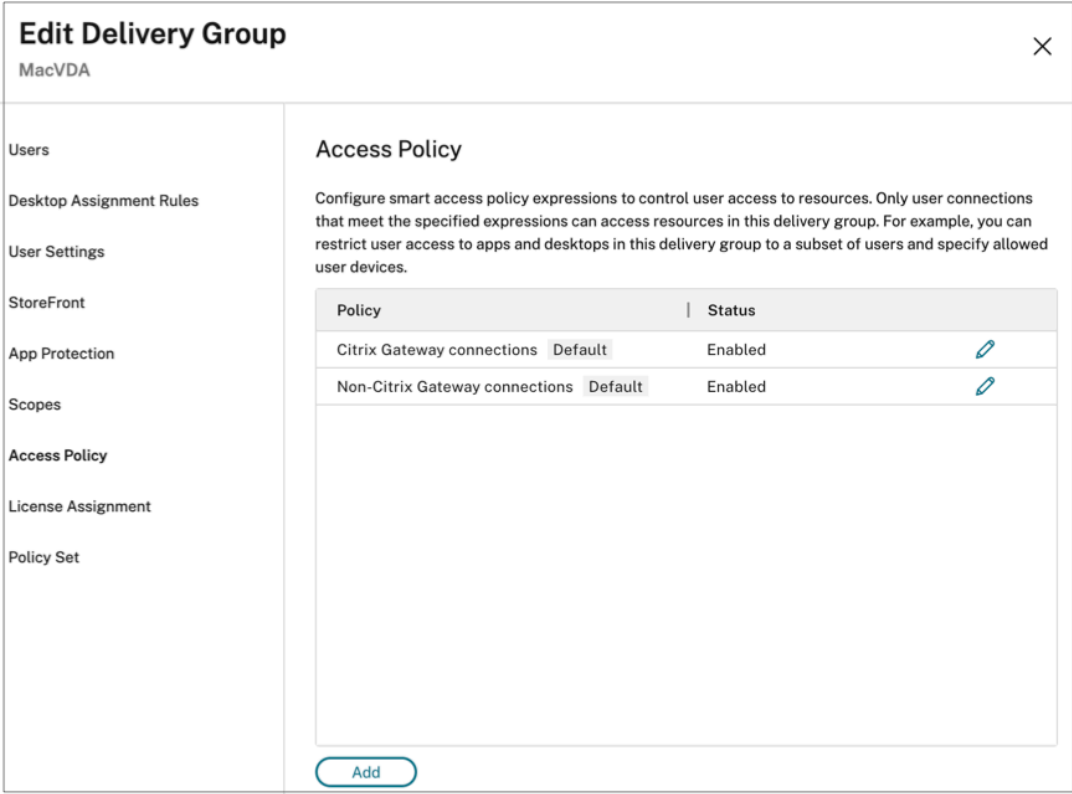
#### 使用 GUI 在 Citrix Studio 中定义标签

在此示例中，在交付组中定义了标签，以限制用户的应用程序枚举。创建了两个交付组。

- 自适应访问交付组—适用于来自位置 **BranchOffice** 的用户。这些用户必须看到该交付组中的所有应用程序。
- WFH 交付组—适用于来自位置 **WorkFromHome** 的用户。这些用户必须看到来自该交付组的应用程序。

1. 登录 Citrix Cloud。

- 2. 在 **Citrix DaaS** 磁贴上，单击 “管理”。
- 3. 创建交付组。有关详细信息，请参阅[创建交付组](#)。
- 4. 选择您创建的交付组，然后单击 编辑交付组。
- 5. 单击访问策略。
- 6. 对于在 Citrix Workspace 平台内使用自适应访问的客户，请执行以下步骤，将交付组的访问权限限制为仅限内部网络：
  - a) 右键单击交付组并选择编辑。
  - b) 在左侧窗格中选择访问策略。
  - c) 单击 “编辑” 图标修改默认 Citrix Gateway 连接策略。



- d) 在 “编辑策略” 页面上，选择 “符合以下条件的连接”，选择 “匹配任意”，然后添加标准。

☒ Connections meeting the following criteria

☐ Match all

☒ Match any

Filter:

Value:

Workspace

LOCATION\_TAG\_WORKFROMHOME

+ Add criterion

☐ Connections not meeting any of the following criteria

No criteria added

对于 WorkFromHome 用户，请在相应的交付控制器中输入以下值。

场: Workspace

过滤器: LOCATION\_TAG\_HOME

对于分支机构用户，在相应的交付控制器中输入以下值。

过滤器: Workspace

值: LOCATION\_TAG\_OFFICE

现在，您可以使用这些标签来限制对应用程序的访问。

限制应用程序的访问权限

在此示例中，对来自 WorkFromHome 位置的用户禁用了客户端剪贴板重定向。

1. 登录 Citrix DaaS。

2. 导航到“策略”，然后单击“创建策略”。

3. 选择“客户端剪贴板重定向”，然后单击“禁止”。

4. 单击下一步。

1 Select Settings

2 Assign Policy To

3 Summary

Select Settings

View by category

All Settings

Connector for Configuration Manager 2012

ICA

Load Management

Profile Management

User Personalization Layer

VDA Data Collection

Virtual Delivery Agent Settings

Virtual RDP

Workspace Environment Management

Settings: 1 selected

☐ Include legacy settings

☐ View selected only

Search

☐ A. Browser Content Redirection Authentication...

☐ A. Browser Content Redirection Block List Con...

☐ A. Browser Content Redirection Integrated WL...

☐ A. Browser Content Redirection Proxy Configu...

☐ A. Browser Content Redirection Server Fetch...

☒ A. Citrix Cloud Connectors

☐ A. Client audio redirection

☒ A. Client clipboard redirection

☐ A. Client clipboard write allowed formats

☐ A. Client COM port redirection

☐ A. Client drive redirection

☐ A. Client feed drives

Prohibited

Prohibited

Prohibited

Prohibited

Prohibited

Allowed

Prohibited

Prohibited

Allowed

Allowed

Prohibit

Edit

1. 在将策略分配给页面中，选择 访问控制。

2. 为策略定义以下值：



- 模式：允许
- 连接类型：使用 **Citrix Gateway**
- 网关场名称：**Workspace**
- 访问条件：**LOCATION\_TAG\_HOME**（全部为大写）

Assign Policy

Access control

Apply policy based on the access control conditions through which a client connects.

Access control elements:

Mode	Connection type	Gateway farm name	Access condition	
Allow	With Citrix Gateway	Workspace	ORKFROMHOME	<input checked="" type="checkbox"/> Enable

1. 单击下一步。
2. 输入策略的名称并添加策略描述。
3. 单击完成。

来自 **WorkFromHome** 位置的用户无法对其启动的资源执行剪贴板访问权限。

网络位置标记

网络位置服务提供以下标签。

- 默认标签：这些标签是在网络位置服务上定义的。以下默认标签可用。
  - **Location\_internal**：当网络连接类型设置为“**INTERNAL**”时，默认情况下会发送标记。
  - **Location\_externa**：当网络连接类型设置为“**EXTERNAL**”时，默认情况下会发送标记。
  - **Location\_undefined**：为未在策略中定义但通过网络位置服务发送的 IP 地址发送的标签。这些用户的启动与资源组中定义的相同。
- 自定义标签：管理员可以在策略中定义自定义标签名称。示例：办公室、家庭、分支机构

示例：

默认标签：LOCATION\_INTERNAL、LOCATION\_EXTERNAL、LOCATION\_UNDEFINED

自定义标签：LOCATION\_TAG\_OFFICE、LOCATION\_TAG\_HOME

注意：

为网络定位服务定义标签时，请确保满足以下条件：

- 默认标签始终以前缀 “LOCATION\_<tag name>” 开头。例如，LOCATION\_INTERNAL。
- 自定义标签始终以前缀 “LOCATION\_TAG” 开头<tag name>。例如，LOCATION\_TAG\_OFFICE。

### 已知问题

如果在启用 Adaptive Access 功能并设置规则（标签和连接类型）后将其禁用，则尽管位置标签和连接类型列处于隐藏状态，但这并不会从“网络位置”页面中移除这些位置。但是这些位置在后端被禁用了。这是一个表面问题。

## 应用程序包

March 5, 2024

Microsoft 提供三种封装技术来向用户交付应用程序：App-V、MSIX 和 MSIX 应用程序附加。本文向您介绍如何在 Citrix DaaS 环境中部署和交付这些打包的应用程序：

- 部署和交付 App-V 应用程序
- 部署和交付 MSIX 和 MSIX 应用附加应用程序

### 部署和交付 **App-V** 应用程序

本部分包含以下信息：

- 概述。描述 Citrix DaaS 用于交付和管理 App-V 软件包的管理方法。
- 程序。提供部署和交付这些包的过程。

#### 概述

本节介绍了 Citrix DaaS 用于交付和管理 App-V 包的管理方法。有关在交付 App-V 打包应用程序时与之交互的组件和概念的更多信息，请参阅 Microsoft 文档：<https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-for-windows>。

Citrix DaaS 使用以下方法交付和管理 App-V 软件包：

- 双重管理员。应用程序包在 App-V 服务器上进行配置和管理。Citrix DaaS 和 App-V 服务器协同工作以交付和管理软件包。

此方法要求 Citrix DaaS 定期刷新 App-V 服务器状态的快照视图。它会产生硬件、基础架构和管理开销。Citrix DaaS 和 App-V 服务器必须保持同步，尤其是在用户权限方面。

双管理在 App-V 和 Citrix Cloud 紧密结合的部署中效果最佳：

- **App-V** 管理服务器。发布和管理 App-V 包和[动态配置文件](#)的生命周期。
- 安装在 VDA 计算机上的 **Citrix** 个性化组件。管理应用程序启动所需的相应 App-V 发布服务器的注册。

此方法可确保 App-V 发布服务器在适当的时间为用户同步。发布服务器维护包生命周期的其他方面，例如，登录时刷新和连接组。

- 单管理。应用程序包存储在网络共享上。Citrix DaaS 独立交付和管理软件包。

此方法可减少开销，因为部署中不需要 App-V 服务器和数据库基础架构。

在此方法中，您可以将 App-V 软件包存储在网络共享上，然后将其元数据从该位置上载到 Citrix Cloud。然后，安装在 VDA 计算机上的 Citrix 个性化组件按如下方式管理和交付应用程序：

- 启动应用程序时处理部署配置文件和用户配置文件。
- 管理主机上的包生命周期的各个方面。

您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存在的 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（双管理）中的文件。

## 过程

要支持 App-V 应用程序的交付，必须在 VDA 计算机上安装 Citrix 个性化组件。有关详细信息，请参阅在 VDA 计算机上安装 Citrix 个性化组件。

要向您的用户交付 App-V 封装的应用程序，请执行以下步骤：

1. 将应用程序包存储在网络共享上。
2. 将应用程序包上载到 Citrix Cloud。
3. 将应用程序添加到交付组。
4. 要启用相互依赖的 App-V 包的自动交付，请创建隔离组。

要让 Citrix DaaS 在单一管理员方法中识别和应用 App-V 动态配置文件，请参阅此 [Citrix 博客](#)。

## 部署和交付 **MSIX** 和 **MSIX** 应用附加应用程序

本部分包含以下信息：

- 概述。描述 Citrix DaaS 如何交付和管理 MSIX 和 MSIX 应用程序附加包。
- 程序。提供部署和交付这些包的过程。

### 概述

Citrix DaaS 通过安装在 VDA 计算机上的 Citrix 个性化组件向用户提供 MSIX 和 MSIX 应用程序附加应用程序。该组件管理主机上软件包生命周期的各个方面。

有关 MSIX 和 MSIX 应用附加的详细信息，请分别参阅 Microsoft 文档 <https://docs.microsoft.com/en-us/windows/msix/> 和 <https://docs.microsoft.com/en-us/azure/virtual-desktop/what-is-app-attach>。

### 过程

要支持 MSIX 和 MSIX 应用附加包的交付，必须在 VDA 计算机上安装 Citrix 个性化组件。有关详细信息，请参阅在 VDA 计算机上安装 Citrix 个性化组件。

要向您的用户交付 MSIX 和 MSIX 应用附加封装的应用程序，请执行以下步骤：

1. 将应用程序包存储在网络共享上。
2. 将应用程序包上载到 Citrix Cloud。
3. 将应用程序添加到交付组。

### 在 VDA 计算机上安装 Citrix 个性化组件

Citrix Personalization 组件管理 App-V、MSIX 和 MSIX 应用附加格式的应用程序包的发布过程。安装 VDA 时，默认情况下不安装此组件。可以在 VDA 安装期间或之后安装此组件。

要在 VDA 安装期间安装此组件，请使用以下任一方法：

- 在安装向导中，转到其他组件页面，然后选中 **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。

要在安装 VDA 后安装此组件，请执行以下步骤：

1. 在 VDA 计算机上，转到控制面板 > 程序 > 程序和功能，右键单击 **Citrix Virtual Delivery Agent**，然后选择更改。
2. 在出现的向导中，前往其他组件页面，然后启用 **Citrix Personalization for App-V - VDA** 复选框。

#### 注意：

Microsoft App-V Desktop Client 是在用户设备上运行来自 App-V 包的虚拟应用程序的组件。Windows 10 (1607 或更高版本)、Windows Server 2016 和 Windows Server 2019 已经包含了这款 App-V 客户端软件。您只需要在 VDA 计算机上将其启用即可。有关详细信息，请参阅这篇 Microsoft 文档文章：<https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-enable-the-app-v-desktop-client>。

## 将应用程序包存储在网络共享中

设置基础结构后，生成应用程序包并将其存储在网络位置（例如 UNC 或 SMB 网络共享）或 Azure 文件共享中。

详细步骤如下所示：

1. 生成应用程序包。有关详细信息，请参阅 Microsoft 文档。
2. 将应用程序包存储在网络位置：
  - 对于 **App-V** 单管理：将包和相应的动态配置文件 (App-V) 存储在 UNC 或 SMB 网络共享或 Azure 文件共享中。
  - 对于 **App-V** 双管理：将包从 UNC 路径发布到 App-V 管理服务器。（不支持从 HTTP URL 发布。）
  - 对于 **MSIX** 或 **MSIX** 应用附加：将包存储在 UNC 或 SMB 网络共享或 Azure 文件共享中。
3. 确保 VDA 对包存储路径具有读取权限：
  - 如果您将包存储在 AD 域中的 UNC 或 SMB 网络共享中，请授予 VDA 计算机对存储路径的读取权限。为此，您可以明确授予计算机的 AD 帐户对共享的读取权限，也可以将该帐户包含在具有该权限的 AD 组中。
  - 如果将包存储在 Azure 文件共享中，请先向用户帐户授予对 Azure 中的存储路径的读取权限。接下来，将在 VDA 计算机上运行的 **ctxAppVService** 配置为使用该用户帐户访问包存储路径。有关详细步骤，请参阅以下部分。

## 更改用户登录帐户

VDA 调用 **ctxAppVService** 以访问包存储路径。默认情况下，**ctxAppVService** 使用计算机的本地系统帐户访问包存储路径。这种类型的计算机身份验证适用于 AD 域。但是，它在需要基于用户帐户的身份验证的 AD 和 Azure AD 集成场景中不起作用。

如果您将包存储在 Azure 文件共享中，请将 **ctxAppVService** 的登录帐户更改为对包存储路径具有读取权限的用户帐户。详细步骤如下所示：

1. 启动 **Services**（服务），右键单击 **ctxAppVService**，然后选择 **Properties**（属性）。
2. 在 **Log on**（登录）选项卡上，选择 **This account**（此帐户），输入对包存储路径具有读取权限的用户帐户，然后输入两次该用户的密码。
3. 单击确定。

## 将应用程序包上载到 Citrix Cloud

根据需要将应用程序包存储到网络位置后，将其上载到 Citrix Cloud 进行交付。根据需要使用以下方法之一：

- 批量上载
- 逐个上载

准备工作

Citrix DaaS 使用 VDA 计算机设置与网络位置的连接以进行包发现。因此，请事先 [创建交付组](#)，并确保该组中至少有一个 VDA 满足以下要求：

- VDA 版本：
  - 要发现 App-V 包，请执行以下操作：2203 或更高版本
  - 要发现 MSIX 和 MSIX 应用附加包，请执行以下操作：2209 或更高版本
- Citrix Personalization for App-V 组件：已安装
- 对包位置的权限：读取（有关详细信息，请参阅步骤 2：将应用程序包存储在网络共享中。）
- 电源：开
- 状态：已注册

必需的角色

默认情况下，如果您具有云管理员或完全权限管理员角色，则可以将应用程序包上载到 Citrix Cloud。您还可以创建自定义角色来执行上载操作。下表列出了应用程序包操作所需的权限。

操作	必需的权限
添加包（逐个上载）	创建应用程序发现会话
添加源（批量上载）	创建应用程序发现配置文件
检查软件包更新	创建应用程序发现会话
移除来源	移除应用程序发现配置文件

批量上载应用程序包

将网络位置中的软件包上载到 Citrix Cloud。在上载之前，请确保您已准备好以下商品：

- 满足准备要求的交付组
- 网络位置路径

要批量上载包裹，请按照以下步骤操作：

1. 从管理 > 完整配置中，选择左侧窗格中的应用程序软件包。
2. 在“源”选项卡上，单击“添加源”按钮。此时将出现添加源页面。
3. 在名称字段中，输入包来源的描述性名称。

4. 在交付组字段中，单击选择交付组。接下来，请选择满足 Preparation（准备）中所述要求的交付组，然后单击 **OK**（确定）。
5. 在 **Location type**（位置类型）字段中，根据包的存储位置选择 **Microsoft App-V server**（Microsoft App-V 服务器）或 **Network share**（网络共享），然后完成相应的设置：
  - 如果选择 **Microsoft App-V server**（Microsoft App-V 服务器），请输入以下信息：
    - 管理服务器的 URL。示例：<http://appv-server.example.com>
    - 管理服务器管理员的登录凭据。
    - 发布服务器的 URL 和端口号。示例：<http://appv-server.example.com:3330>
  - 如果选择了 **Network share**（网络共享），请指定以下信息：
    - 输入网络共享的 UNC 路径。示例：[\\Package-Server\apps\](#)
    - 选择要上载的包类型。选项包括“App-V”、“MSIX”和“MSIX 应用附加”。
    - 指定是否在子文件夹中搜索包。
6. 单击 **Add Source**（添加源）。

“添加源”页面将关闭，新添加的源将显示在源列表中。Citrix DaaS 使用交付组中的 VDA 将包上载到 Citrix Cloud。上载完成后，状态字段将显示 导入成功。相应的包将显示在 **Packages**（包）选项卡上。

**注意：**

要检查源位置中的包更新并将其导入 Citrix Cloud，请在源列表中选择该位置，然后单击 检查包更新。

## 逐个上载应用程序包

将应用程序包从网络共享上载到 Citrix Cloud。在上载之前，请确保您已准备好以下项目：

- 满足准备中所述要求的交付组
- 网络位置路径。

要将软件包上载到 Citrix Cloud，请执行以下步骤：

1. 从管理 > 完整配置中，选择左侧窗格中的应用程序软件包。
2. 在“包”选项卡上，单击“添加包”按钮。此时将出现添加包页面。
3. 在交付组字段中，单击选择交付组。下一步，选择满足准备中所述要求的交付组，然后单击确定。
4. 在包完整路径字段中，根据需要输入路径：
  - 要一次上载多个包，请输入其完整路径，用分号 (;) 分隔。示例：[\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd](#)
  - 要上载网络共享中存在的所有包，请输入存储路径。示例：[\package-Server\apps\](#)
5. 单击添加包。

应用程序包显示在 **Packages**（包）选项卡上。

## 将应用程序添加到交付组中

应用程序包完全上载后，根据需要将其应用程序添加到一个或多个交付组中。因此，与这些交付组关联的用户可以访问这些应用程序。

注意：

打包的应用程序只能分配给应用程序或桌面和应用程序类型的交付组。

要将包中的一个或多个应用程序添加到多个交付组中，请执行以下步骤：

1. 从管理 > 完整配置中，选择左侧窗格中的应用程序软件包。
2. 在包选项卡上，根据需要选择一个包。
3. 在操作栏中，单击“将应用程序分配给交付组”。将出现“将应用程序分配给交付组”页面。
4. 根据需要在包中选择一个或多个应用程序，然后单击下一步。此时将出现应用程序或桌面和应用程序交付类型的交付组。
5. 在交付组列表中，选择要向其分配应用程序的组，然后单击下一步。  
注意：如果您选择了 MSIX 或 MSIX 应用附加包，则列表中仅显示功能级别为 2106 或更高版本的交付组。
6. 单击完成。

在以下情况下，您还可以在交付组中添加打包的应用程序：

- 创建交付组。有关详细信息，请参阅[创建交付组](#)。
- 编辑现有的交付组或应用程序组。有关详细信息，请参阅[添加应用程序](#)。

## （可选）为 **App-V** 包创建隔离组

可以创建隔离组以启用相互依赖的 App-V 包的自动交付。

注意：

App-V 单管理方法支持隔离组。如果您使用的是 App-V 双管理方法，可以通过在 Microsoft App-V 基础结构中创建连接组来实现相同的目标。有关详细信息，请参阅这篇 Microsoft 文档文章：<https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-connection-group-file>。

## 关于隔离组

隔离组是相互依赖的应用程序包的集合，它们必须在同一 Windows 沙盒中运行才能创建虚拟环境。Citrix App-V 隔离组与 App-V 连接组相似但不完全相同。隔离组包括两种类型的包：

- 显式应用程序包。具有特定许可要求的应用程序。可以通过将这些应用程序添加到交付组来将其限制到特定范围的用户。
- 自动应用程序包。无论是否将应用程序添加到交付组，所有用户都可以随时访问这些应用程序。



例如，应用程序 **app-a** 需要 JRE 1.7 才能运行。可以创建一个包含 **app-a**（标记为显式）和 JRE 1.7（标记为自动）的隔离组。接下来，将 **app-a** 的 App-V 包添加到一个或多个交付组。用户启动 **app-a** 时，JRE 1.7 会通过它自动部署。

当用户在隔离组中启动标记为 显式 的 App-V 应用程序时，Citrix DaaS 会检查用户对交付组中应用程序的访问权限。如果用户具有访问应用程序的权限，则同一隔离组中的任何 *Automatic* 应用程序包均可供该用户使用。

无需将自动包添加到任何交付组。如果隔离组中还有另一个显式应用程序包，则只有当该包位于同一个交付组中时，才可供用户使用。

有关隔离组的详细信息，请参阅此 [Citrix 博客](#)。

**创建 App-V 隔离组** 创建隔离组并将相互依赖的应用程序包添加到其中。详细步骤如下所示：

1. 在隔离组选项卡上，单击添加隔离组。
2. 输入隔离组的名称和描述。Citrix Cloud 中的所有应用程序包都将显示在“可用软件包”列表中。
3. 从“可用软件包”列表中，根据需要选择应用程序，然后单击向右箭头。选定的应用程序显示在隔离组中的包列表中。
4. 在部署字段中，为应用程序选择显式或自动。
5. 重复执行步骤 2-3 以添加更多包。
6. 要调整列表中包的顺序，请单击向上或向下箭头。
7. 单击保存。

**注意：**

隔离组配置会在 VDA 上创建 App-V 连接组。部署场景可能会变得复杂，App-V 客户端一次仅支持一个活动连接组中的包。我们建议您避免向添加到同一个交付组中的两个不同的隔离组添加同一个包。

## 在单会话或共享桌面 **VDA** 上发布打包的应用程序

现在，您可以直接通过交付组将 App-V、MSIX 和 MSIX 应用附加包交付到您的单会话或共享桌面 VDA 会话中。根据在应用程序上设置的无障碍访问权限，您可以在登录时在桌面 VDA 上访问打包的应用程序。

### 优势

- 应用程序在登录时可在 VDA 上使用，不能通过 Workspace 或 StoreFront 按需暂存。
- 缩短了访问打包的应用程序时的启动时间。
- 便于独立维护打包的应用程序，与 VDA 的基础映像分开。

### 注意事项

- 此选项仅通过相应的 PowerShell SDK 面向单会话 VDA 提供。它目前在完整配置工作流程中不可用。可以使用 PowerShell SDK 发布到共享桌面，也可以通过完整配置工作流程以现有方式发布。有关现有过程的详细信息，

请参阅向交付组中添加应用程序。

- 应用程序必须是交付组的一部分。

#### 开始之前的准备工作

- 请确保打包的应用程序已签名并在文件共享或 UNC 位置提供。有关详细信息，请参阅将应用程序包存储在网络共享中。
- 在 VDA 计算机上安装 Citrix 个性化组件。

#### 过程

要将打包的应用程序交付到桌面 VDA，请执行以下步骤：

1. 将应用程序包导入到完整配置。
2. 发布打包的 Broker 应用程序。
3. 限制应用程序在完整配置下的可见性。

#### 将应用程序包导入到完整配置

1. 登录 Citrix Cloud。
2. 在 **DaaS** 磁贴中，单击 管理。
3. 转到交付组页面，然后创建交付组。有关详细信息，请参阅[创建交付组](#)。
4. 将应用程序包导入到完整配置。有关更多信息，请参见[将应用程序包上传到 Citrix Cloud](#)。

#### 在 **Broker** 应用程序中发布打包的应用程序

如果您要发布到多会话（共享）VDA 或单会话应用程序 VDA，发布过程将保持不变。有关详细信息，请参阅[向交付组中添加应用程序](#)。

发布到单会话桌面 VDA 时，请执行以下操作：

在 Delivery Controller 上，运行以下 PowerShell 命令：

1. 要检索软件包中存在的命令，请执行以下操作：

```
Import-Module "D:\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.  
Admin.v1.psm1"
```

注意：

支持此功能的 **App-V package discovery module** 的版本存在于此路径上的 Citrix Virtual Apps and Desktops ISO (2311 或更高版本) 中。

2. 要检索相关的交付组 ID 和打包的应用程序 ID，请执行以下操作：

```
Get-BrokerDesktopGroup | Format-Table Uid, Name
Get-AppLibAppVApplication | Format-Table Uid, Name
```

3. 要发布包并创建相应的 BrokerMachineConfigurations，请执行以下操作：

```
Publish-PackagedApplication -AppLibraryApplicationUid <AppLibraryApplication.Uid> -DesktopGroupUid <DesktopGroup.Uid>
```

4. 要同步 Broker 配置（稍后将在 VDA 上发送给 Broker 代理），请执行以下操作：

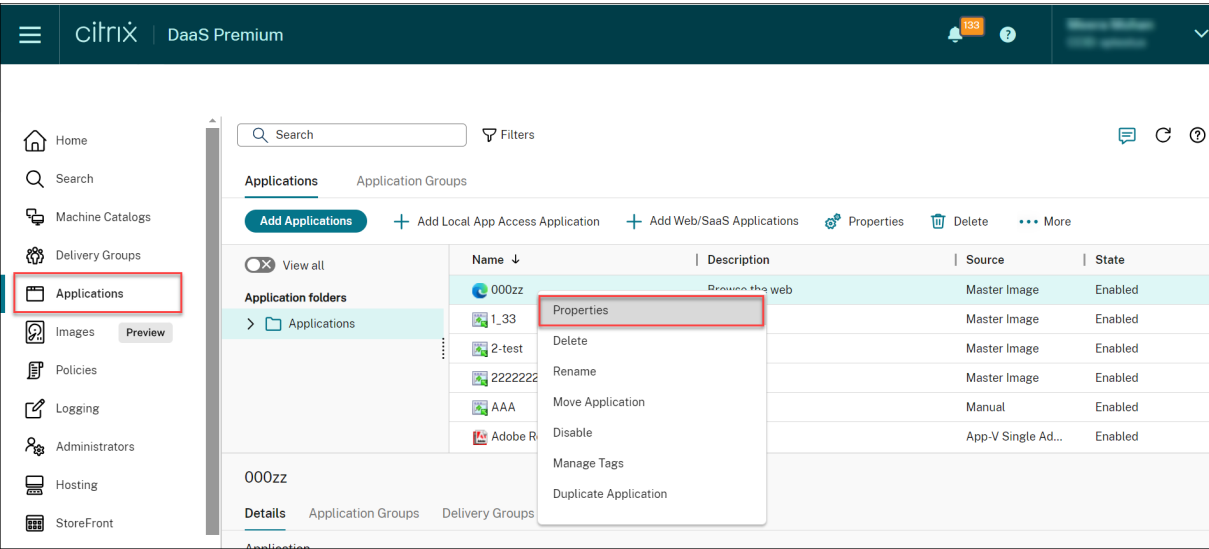
```
Update-DesktopGroupMachineConfigurations -DesktopGroupUid <DesktopGroup.Uid>
```

注意：

确保在 VDA 中发布或删除打包的应用程序后运行 PowerShell 命令 `Update-DesktopGroupMachineConfigurations`。

限制应用程序在完整配置下的可见性

默认情况下，用户将所有打包的应用程序分配给为在其桌面会话中可用的 VDA 提供服务的交付组。通过在完整配置中设置应用程序对特定用户或组的可见性，您可以控制打包应用程序在桌面 VDA 上的可见性。要管理打包应用程序的可见性，请参见[更改应用程序属性](#)或参阅以下图片。



Application Settings

hostedOnDesktop

Identification

Delivery

Location

Groups

Limit Visibility

File Type Association

Zone

By default, applications are visible to all users in a delivery group, but you can hide them in Citrix Workspace app from some users. All users can still start this application, so if you want it to be unavailable to some users, rather than hidden, put it in a separate delivery group.

Show this application to the entire delivery group

Limit visibility for this application to the users listed below

Name

Add

Remove

Save

Apply

Cancel

AutoScale

March 5, 2024

AutoScale 提供了一种一致、高性能的解决方案，可以主动管理您的计算机。它旨在平衡成本和用户体验。Autoscale 将弃用的 Smart Scale 技术集成到管理控制台的电源管理解决方案中。

Autoscale 可对交付组中的所有已注册的单会话和多会话操作系统计算机进行主动电源管理。

Autoscale 功能包括：

- 基于计划和基于负载的设置
- 动态会话超时
- 自动缩放带标记的计算机（云突发）
- 动态计算机预配
- 用户注销通知

## 支持的 **VDA** 托管平台

AutoScale 支持 Citrix DaaS 支持的所有平台。这包括各种基础架构平台，包括 XenServer（前身为 Citrix Hypervisor）、Amazon Web Services、Google 云端平台、Microsoft Azure Resource Manager、VMware vSphere 等。有关支持的平台的完整列表，请参阅 Citrix DaaS 的[系统要求](#)。

## 支持的工作负载

Autoscale 支持多会话操作系统和单会话操作系统交付组。有三个用户界面需要注意：

- 多会话操作系统交付组（以前称为 RDS 交付组）的 Autoscale 用户界面
- 单会话操作系统随机（池）交付组（以前称为池 VDI 交付组）的 Autoscale 用户界面
- 单会话操作系统静态交付组（以前称为静态 VDI 交付组）的 Autoscale 用户界面

有关不同交付组的用户界面的详细信息，请参阅 [Autoscale 用户界面](#)。

## 优势

AutoScale 功能具有以下优势：

- 为您提供单一、一致的机制来管理交付组中的计算机电源。
- 通过基于负载或基于计划的电源管理或两者的组合为计算机管理电源，确保可用性并控制成本。
- 要监视成本节约和容量利用率等指标，以及启用通知，请使用监视选项卡上提供的 [Director](#)。

观看时长为 **2** 分钟的视频

下面的视频提供了 AutoScale 的快速教程。

[这是一个嵌入式视频。单击链接观看视频](#)

## 开始使用 **Autoscale**

October 26, 2023

AutoScale 在交付组级别运行。它会根据您设置的计划主动对交付组中的计算机进行电源管理。

AutoScale 适用于所有类型的交付组：

- 单会话静态操作系统

- 单会话随机操作系统
- 多会话随机操作系统

本文介绍了与 AutoScale 相关的基本概念，并就如何为交付组启用和配置 AutoScale 提供了指导。

## 基本概念

在开始之前，请先了解 AutoScale 中的以下基本概念：

- 计划
- 容量缓冲区
- 负载指数

### 计划

AutoScale 会根据您设置的计划打开和关闭交付组中的计算机的电源。

计划包括每个时段的活动计算机数量，并定义了高峰和非高峰时段。

计划设置因交付组的类型而异。有关详细信息，请参阅：

- [多会话操作系统交付组](#)
- [单会话操作系统随机交付组](#)
- [单会话操作系统静态交付组](#)

### 容量缓冲区

容量缓冲区用于为当前需求添加备用容量，以对动态负载增加负责。您需要注意以下两种情况：

- 对于多会话操作系统交付组，容量缓冲区根据负载指数定义为占交付组总容量的百分比。
- 对于单会话操作系统交付组，容量缓冲区定义为交付组中的计算机总数的百分比。

### 负载指数

重要：

负载索引仅适用于多会话交付组。

负载指数衡量指标决定了计算机接收用户登录请求的可能性。该值是使用针对并发登录、会话、CPU、磁盘和内存使用配置的 **Citrix Load Management** 策略设置计算的。

负载指数的范围介于 0 到 10000 之间。默认情况下，计算机在托管 250 个会话时被视为处于满载状态。

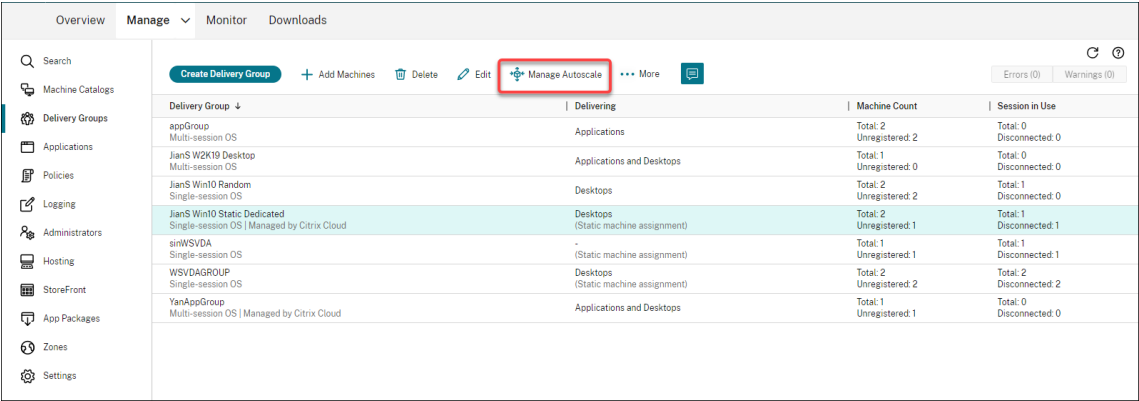
- 数字“0”表示卸载了负载的计算机。负载指数值为 0 的计算机处于基准负载状态。
- 数字“10000”表示已满载的计算机无法再运行任何会话。

为交付组启用 **AutoScale**

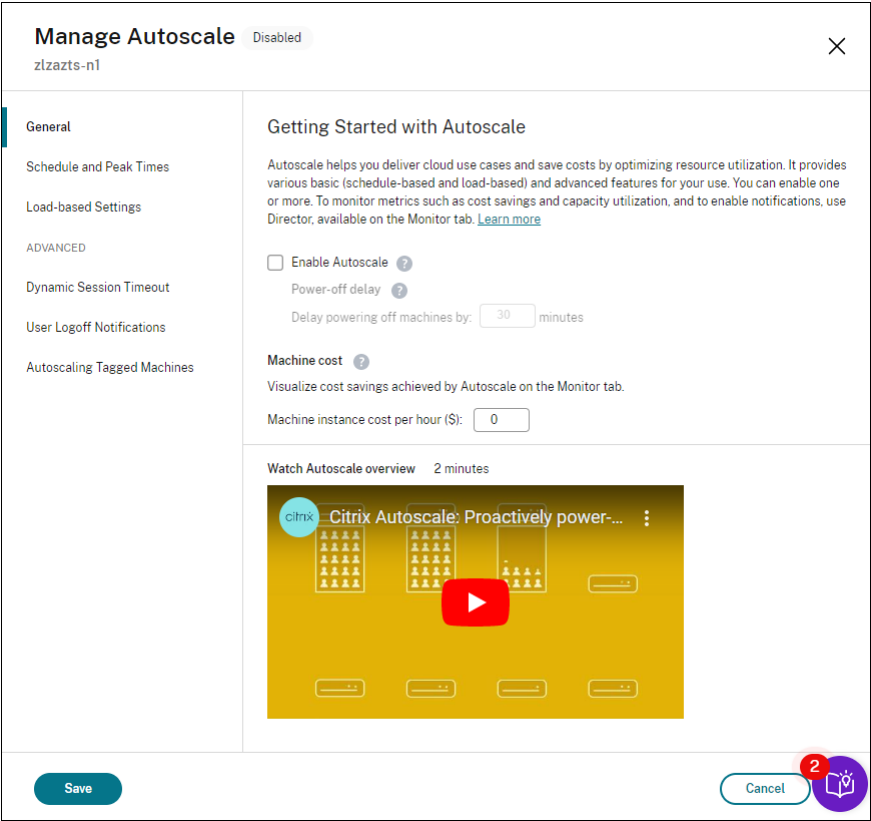
创建交付组时，默认情况下，Autoscale 处于禁用状态。要使用完整配置界面为交付组启用和配置 AutoScale，请执行以下步骤：

您也可以使用 PowerShell 命令为交付组启用和配置 AutoScale。有关详细信息，请参阅 [Broker PowerShell SDK 命令](#)。

- 1. 在管理 > 完整配置中，选择左窗格中的交付组。
- 2. 选择要管理的交付组，然后单击管理 **AutoScale**。



- 3. 在管理 **Autoscale** 页面上，选中启用 **Autoscale** 复选框以启用 Autoscale。启用 AutoScale 后，页面上的选项将启用。



4. 要根据组织的需求更改默认设置，请完成以下设置：

- [设置计划](#)
- 要更有效地关闭非活动计算机的电源，请使用[动态会话超时](#)和[用户注销通知](#)
- 要对交付组中的一部分计算机进行电源管理，请使用[自动缩放已标记的计算机](#)

要禁用 AutoScale，请取消选中 **AutoScale** 复选框。页面上的选项变为灰色，以指示已为选定的交付组禁用 AutoScale。

重要：

- 如果禁用 AutoScale，则 AutoScale 管理的所有计算机将保留在禁用时的状态。
- 禁用 AutoScale 后，处于耗尽状态的计算机将从耗尽状态中恢复。有关耗尽状态的详细信息，请参阅耗尽状态。

您可以使用 PowerShell 脚本为群组动态配置计算机。有关更多信息，请参阅[动态计算机配置](#)。

**Monitor** 指标

为交付组启用 AutoScale 后，可以从监视选项卡监视 AutoScale 管理的计算机的以下指标。

- 计算机使用情况



- 预计节省量
- 计算机和会话的警报通知
- 计算机状态
- 负载评估趋势

注意：

最初为交付组启用 AutoScale 时，可能需要几分钟才能显示该交付组的监视数据。

如果为交付组启用 Autoscale 后将其禁用，监视数据将保持可用状态。AutoScale 每隔 5 分钟收集一次监视数据。

有关指标的详细信息，请参阅[监视 Autoscale 托管的计算机](#)。

## 须知

AutoScale 在交付组级别运行。它是根据每个交付组进行配置的。它仅管理选定交付组中的计算机。

## 容量和计算机注册

AutoScale 仅包括在确定容量时在站点中注册的计算机。未注册的已打开电源的计算机无法接受会话请求。因此，这些计算机不包括在交付组的总容量中。

## 跨多个计算机目录扩展

在某些站点中，多个计算机目录可能与单个交付组相关联。AutoScale 从每个目录随机打开计算机的电源，以满足计划或会话需求的要求。

例如，某个交付组有两个计算机目录：目录 A 有三台打开电源的计算机，目录 B 有一台打开电源的计算机。如果 AutoScale 需要打开额外的计算机的电源，则可能会从目录 A 或目录 B 中打开计算机的电源。

## 计算机预配和会话需求

与交付组关联的计算机目录必须有足够的计算机，以便随需求的增加和减少而打开和关闭电源。如果会话需求超过交付组中已注册的计算机总数，Autoscale 将确保所有已注册的计算机都已打开电源。但是，**AutoScale** 不会预置额外的计算机。

要克服此瓶颈，可以使用 PowerShell 脚本动态创建计算机并将其删除。有关更多信息，请参阅[动态配置计算机](#)

## 实例大小注意事项

如果您在公有云中正确调整了实例的大小，则可以优化您的成本。我们建议您预配较小的实例，前提是其符合您的工作负载性能和容量要求。

较小的实例托管的用户会话数少于较大的实例。因此，AutoScale 将计算机置于耗尽状态的速度要快得多，因为注销最后一个用户会话所需的时间更短。因此，AutoScale 更快地关闭较小实例的电源，从而降低成本。

## 耗尽状态

AutoScale 尝试将交付组中已打开电源的计算机数量缩小到配置的池大小和容量缓冲区。

为了实现这一目标，AutoScale 会将会话最少的多余计算机置于“耗尽状态”，并在注销所有会话后关闭其电源。当会话需求减少并且计划所需的计算机少于打开电源的计算机时会出现此行为。

AutoScale 将多余的计算机逐个置于“耗尽状态”：

- 如果两台或多台计算机具有相同数量的活动会话，AutoScale 会耗尽为指定的关机延迟打开电源的计算机。  
这样做可以避免将最近打开电源的计算机置于耗尽状态，因为这些计算机的会话更可能最少。
- 如果两台或多台计算机已为实现指定的关机延迟打开电源，AutoScale 将随机逐一耗尽这些计算机。

处于耗尽状态的计算机不再托管新的会话启动，并且正在等待现有会话注销。仅当所有会话都注销时，计算机才会成为关闭候选项。但是，如果没有立即可用于会话启动的计算机，AutoScale 将更倾向于将会话启动定向到处于耗尽状态的计算机，而非打开计算机电源。

满足以下条件之一时，计算机将脱离耗尽状态：

- 计算机已关闭电源。
- 已为计算机所属的交付组禁用 AutoScale。
- AutoScale 使用计算机来满足计划或负载需求的要求。当计划（基于计划的扩展）或当前需求（基于负载的扩展）所需的计算机超过当前打开电源的计算机数量时会出现这种情况。

### 重要：

如果没有立即可用于会话启动的计算机，AutoScale 将更倾向于将会话启动定向到处于耗尽状态的计算机，而非打开计算机电源。托管会话启动的处于耗尽状态的计算机仍处于耗尽状态。

要找出哪些计算机处于耗尽状态，请使用 `Get-BrokerMachine` PowerShell 命令。例如：`Get-BrokerMachine -DrainingUntilShutdown $true`。或者，您可以使用“管理”控制台。请参阅显示处于耗尽状态的计算机。

显示处于耗尽状态的计算机

注意：

此功能仅适用于多会话计算机。

在管理 > 完整配置中，您可以显示处于耗尽状态的计算机，让您知晓哪些计算机即将关闭。完成以下步骤：

1. 导航到搜索节点，然后单击要显示的列。
2. 在要显示的列窗口中，选中耗尽状态。
3. 单击保存退出要显示的列窗口。

耗尽状态列可以显示以下信息：

- 在关机前耗尽。在计算机关闭之前处于耗尽状态时出现。
- 不耗尽。计算机尚未处于耗尽状态时出现。

Overview

Manage

Monitor

Downloads

Search

Machine Catalogs

Delivery Groups

Applications

Policies

Logging

Administrators

Hosting

StoreFront

App-V Publishing

Zones

Single-session OS Machines (6)

Multi-session OS Machines (3)

Sessions (2)

Columns to Display

Name ↓	Machine Catalog	Delivery Group	Maintenance Mode	User Change Per...	Power State	Registration State	Sessio...	Drain State
318zjh001.xd.local	zjh-mul	zjh-mul	Off	Discard	On	Registered	-	Draining until shutdown
318zjh002.xd.local	zjh-mul	zjh-mul	Off	Discard	On	Registered	1	Not draining
318zjh003.xd.local	zjh-mul	zjh-mul	Off	Discard	On	Registered	1	Not draining

Click an item to view the details.

更多信息

有关 Autoscale 的详细信息，请参阅 Tech Zone 中的 [Citrix Autoscale](#)。

基于计划和基于负载的设置

October 26, 2023

AutoScale 如何管理计算机电源

AutoScale 根据所选计划打开和关闭计算机的电源。通过 AutoScale，您可以设置多个计划，其中包括一周中的特定天数，并调整在这些时间内可用的计算机数量。如果您期望一组用户在特定日期的特定时间使用计算机资源，AutoScale

可以帮助提供优化的体验。请注意，这些计算机将在计划期间打开电源，而无论其上是否存在正在运行的会话。

注意：

Autoscale 支持任何电源管理的计算机。

计划基于交付组的时区。要更改时区，您可以更改交付组中的用户设置。有关详细信息，请参阅[管理交付组](#)。

AutoScale 有两个默认计划：工作日（星期一至星期五）和周末（星期六和星期日）。默认情况下，工作日计划在高峰时段上午 7:00 至下午 6:30 保持一台计算机处于开机状态，在非高峰时段保持无开机状态。在高峰时段和非高峰时段，默认容量缓冲区设置为 10%。默认情况下，周末计划不会保持打开任何计算机的电源。

注意：

AutoScale 仅将在站点中注册的计算机视为其进行计算时可用容量的一部分。“已注册”是指计算机可供使用或已在使用中。这样做可确保只有可以接受用户会话的计算机包含在交付组的容量中。

用户界面

有三种类型的用户界面需要注意。

单会话操作系统静态交付组的用户界面：

Manage Autoscale

Enabled

General

Schedule and Peak Ti...

Load-based Settings

ADVANCED

Restrict Autoscale

Schedule and Peak Times

If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. [Learn more](#)

Set schedules

Weekdays

Days applied: Mon Tue Wed Thu Fri Sat Sun

Peak times

12:00 AM 3:00 AM 6:00 AM 9:00 AM 12:00 PM 3:00 PM 6:00 PM 9:00 PM 12:00 AM

Weekend

Save Cancel Apply

Manage Autoscale

Enabled

General

Schedule and Peak Ti...

Load-based Settings

ADVANCED

Restrict Autoscale

Load-based Settings

Capacity buffer is used to accommodate sudden spikes in demand by keeping a buffer of machines powered on based on the maximum load index of the delivery group. By default, the capacity buffer is 10% of the maximum supported load index of the delivery group. A lesser value decreases the cost. A greater value ensures an optimized user experience so that users do not have to wait for additional machines to power on when launching sessions. [Learn more](#)

	During peak times		During off-peak times	
Capacity buffer (%):	<input type="text" value="10"/>		<input type="text" value="10"/>	
When disconnected (minutes):	<input type="text" value="0"/>	<div>No action</div>	<input type="text" value="0"/>	<div>No action</div>
When logged off (minutes):	<input type="text" value="0"/>	<div>No action</div>	<input type="text" value="0"/>	<div>No action</div>

Save

Cancel

Apply

单会话操作系统随机交付组的 Autoscale 用户界面：

Manage Autoscale

Enabled

General

Schedule and Peak Ti...

Load-based Settings

ADVANCED

Restrict Autoscale

Schedule and Peak Times

If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. [Learn more](#)

Set schedules

New schedule

Days applied: Mon Tue Wed Thu Fri Sat Sun

Machines [Edit](#)

5

4

3

2

1

0

12:00 AM

03:00 AM

06:00 AM

09:00 AM

12:00 PM

03:00 PM

06:00 PM

09:00 PM

12:00 AM

Peak times

> Weekdays

> Weekend

Save

Cancel

Apply

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

1047

Manage Autoscale

Enabled

General

Schedule and Peak Ti...

Load-based Settings

ADVANCED

Restrict Autoscale

Load-based Settings

Capacity buffer is used to accommodate sudden spikes in demand by keeping a buffer of machines powered on based on the maximum load index of the delivery group. By default, the capacity buffer is 10% of the maximum supported load index of the delivery group. A lesser value decreases the cost. A greater value ensures an optimized user experience so that users do not have to wait for additional machines to power on when launching sessions. [Learn more](#)

During peak times

During off-peak times

Capacity buffer (%):

4

10

When disconnected (minutes):

2

Suspend

3

Shut down

Save

Cancel

Apply

多会话操作系统交付组的 Autoscale 用户界面：

Manage Autoscale

Enabled

General

Schedule and Peak Ti...

Load-based Settings

ADVANCED

Dynamic Session Tim...

Force User Logoff

Restrict Autoscale

Schedule and Peak Times

If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. [Learn more](#)

Set schedules

New schedule

Days applied: Mon Tue Wed Thu Fri Sat Sun

Machines [Edit](#)

5

4

3

2

1

0

12:00 AM

03:00 AM

06:00 AM

09:00 AM

12:00 PM

03:00 PM

06:00 PM

09:00 PM

12:00 AM

Peak times

> Weekdays

> Weekend

Save

Cancel

Apply



## Manage Autoscale

Enabled

General

Schedule and Peak Times

Load-based Settings

ADVANCED

Dynamic Session Timeout

Force User Logoff

Restrict Autoscale

### Load-based Settings

Capacity buffer is used to accommodate sudden spikes in demand by keeping a buffer of machines powered on based on the maximum load index of the delivery group. By default, the capacity buffer is 10% of the maximum supported load index of the delivery group. A lesser value decreases the cost. A greater value ensures an optimized user experience so that users do not have to wait for additional machines to power on when launching sessions. [Learn more](#)

	During peak times	During off-peak times
Capacity buffer (%):	<input type="text" value="11"/>	<input type="text" value="12"/>

Save

Cancel

Apply

## 基于计划的设置

### Autoscale 计划。允许您添加、编辑、选择和删除计划。

应用的日期。突出显示您应用于所选计划的日期。剩余的日期将显示为灰色。

编辑。允许您每小时或每半小时分配一次计算机。可以按数量和百分比分配计算机。

注意：

- 此选项仅在多会话操作系统和单会话操作系统随机交付组的 Autoscale 用户界面中可用。
- 编辑旁边的直方图绘制在不同时间段运行的计算机的数量或百分比。
- 可以通过单击高峰时段上方的编辑为每个时间段分配计算机。您可以按数量或百分比分配计算机，具体取决于从要启动的计算机窗口中的菜单中选择的选项。
- 对于多会话操作系统交付组，您可以按每天 30 分钟的粒度增量单独设置运行的计算机的最小数量。对于单会话操作系统随机交付组，您可以按每天 60 分钟的粒度增量单独设置运行的计算机的最小数量。

要定义您自己的计划，请按照以下步骤进行操作：

1. 在管理 **Autoscale** 窗口的计划和高峰时间页面上，单击设置计划。
2. 在编辑 **Autoscale** 计划窗口中，选择要应用到每个计划的日期。也可以删除计划（如果适用）。
3. 单击完成以保存计划并返回到计划和高峰时间页面。
4. 选择适用的计划并根据需要进行配置。
5. 单击应用退出管理 **Autoscale** 窗口或在其他页面上配置设置。

**重要：**

- AutoScale 不允许同一天在不同的时间表中重叠。例如，如果您在 schedule1 中选择星期一后在 schedule2 中选择星期一，则将在 schedule1 中自动清除星期一。
- 计划名称不区分大小写。
- 计划名称不得为空或仅包含空格。
- AutoScale 允许字符之间存在空格。
- 计划名称不得包含以下字符：\ / ; : # . \* ? = < > | [ ] ( ) { } “ ”。
- AutoScale 不支持重复的计划名称。请为每个计划输入不同的名称。
- AutoScale 不支持空计划。这意味着不保存没有选择日期的计划。

**注意：**

所选计划中包含的日期将突出显示，而未包含的日期则显示为灰色。

## 基于负载的设置

**高峰时段。**允许您定义在所选计划中应用的日期的高峰时段。可以通过右键单击水平条形图来执行此操作。定义高峰时段后，剩余的未定义时间默认为非高峰时段。默认情况下，上午 7:00 至下午 7:00 时间段被定义为选定计划中包含的日期的高峰时段。

**重要：**

- 对于多会话操作系统交付组，高峰时段条形图用于容量缓冲区。
- 对于单会话操作系统交付组，高峰时段条形图用于容量缓冲区，并控制在注销和/或断开连接后触发的操作。
- 可以按 30 分钟的粒度级别同时为多会话操作系统和单会话操作系统交付组定义计划中包含的天数的高峰时间。或者，也可以改为使用 `New-BrokerPowerTimeScheme PowerShell` 命令。有关详细信息，请参阅 [Broker PowerShell SDK 命令](#)。

**容量缓冲区。**允许您保留已打开电源的计算机的缓冲区。较小的值会降低成本。更大的值可确保优化用户体验，以便在启动会话时，用户无需等待其他计算机打开电源。默认情况下，高峰和非高峰时段的容量缓冲区为 10%。如果将容量缓冲区设置为 0（零），则在启动会话时，用户可能必须等待其他计算机打开电源。通过 AutoScale，您可以分别确定高峰和非高峰时段的容量缓冲区。

## 其他设置

## 提示：

- 可以选择使用 Broker PowerShell SDK 配置其他设置。有关详细信息，请参阅 [Broker PowerShell SDK 命令](#)。
- 要了解与断开连接和注销设置时关联的 SDK 命令，请参阅[https://citrix.github.io/delivery-controller-sdk/Broker/about\\_Broker\\_PowerManagement/#power-policy](https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy)。

断开连接时。允许您指定断开连接的锁定计算机在会话断开连接后、挂起或关闭之前保持打开电源的时间。如果指定了时间值，则在指定的断开连接时间过去时，计算机将挂起或关闭，具体取决于您配置的操作。默认情况下，不会向断开连接的计算机分配任何操作。您可以为高峰和非高峰时段分别定义操作。为此，请单击向下箭头，然后从菜单中选择以下选项之一：

- 无操作。如果选择此选项，会话断开连接后计算机将保持打开电源。Autoscale 不会对其执行任何操作。
- 挂起。如果选择此选项，AutoScale 会在指定的断开连接时间过去时暂停计算机而非将其关闭。选择暂停后，以下选项将变得可用。
  - 如果在 **(分钟)** 内没有重新连接。已挂起的计算机在断开连接的用户重新连接时仍可用，但不适用于新用户。要使计算机再次可用于处理所有工作负载，请将其关闭。指定超时（以分钟为单位），超时后 Autoscale 会将其关闭。
- 关闭。如果选择此选项，则在指定的断开连接时间过后，AutoScale 将关闭计算机。

## 注意：

此选项仅在单会话操作系统随机交付组和静态交付组的 Autoscale 用户界面中可用。

注销时。允许您指定计算机在会话注销后、挂起或关闭之前保持打开电源的时间。如果指定了时间值，则在指定的注销时间过去时，计算机将挂起或关闭，具体取决于您配置的操作。默认情况下，不会向注销的计算机分配任何操作。您可以为高峰和非高峰时段分别定义操作。为此，请单击向下箭头，然后从菜单中选择以下选项之一：

- 无操作。如果选择此选项，会话注销后计算机将保持打开电源。Autoscale 不会对其执行任何操作。
- 挂起。如果选择此选项，AutoScale 会在指定的注销时间过去时暂停计算机而非将其关闭。
- 关闭。如果选择此选项，则在指定的注销时间过后，AutoScale 将关闭计算机。

## 注意：

此选项仅在单会话操作系统静态交付组的 Autoscale 用户界面中可用。

## 对断开连接的会话转换到不同时间段的单会话操作系统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单会话操作系统计算机。它不适用于具有已注销的会话的单会话操作系统计算机。
- 要使此增强功能生效，您需要为适用的交付组启用 AutoScale 功能。否则，断开连接电源策略操作不会在

周期转换时触发。

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）的时间段的单会话操作系统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。

自本版本起，在指定的断开连接时间过后，AutoScale 将暂停或关闭计算机电源，具体取决于为目标时间段配置的断开连接操作。

例如，可以为单会话操作系统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”

注意：

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](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单会话操作系统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。自本版本起，`OffPeakDisconnectAction` 和 `OffPeakDisconnectTimeout` 策略操作将在周期转换时应用到单会话操作系统计算机。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（true；启用之前的行为）。默认情况下，值为 0（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
  - 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单会话操作系统交付组。
- 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。

## 容量缓冲区的工作原理

容量缓冲区用于为当前需求添加备用容量，以对动态负载增加负责。您需要注意以下两种情况：

- 对于多会话操作系统交付组，容量缓冲区根据负载指数定义为占交付组总容量的百分比。有关负载指数的详细信息，请参阅[负载指数](#)。
- 对于单会话操作系统交付组，容量缓冲区根据计算机数量定义为占交付组总容量的百分比。

### 注意：

在将 Autoscale 限制到带标记的计算机场景中，容量缓冲区按负载指数定义为交付组中带标记的计算机总容量的百分比。

通过 AutoScale，您可以分别设置高峰和非高峰时段的容量缓冲区。容量缓冲区字段中的值越小，成本则越低，因为 AutoScale 打开的备用容量越少。更大的值可确保优化用户体验，以便在启动会话时，用户无需等待其他计算机打开电源。默认情况下，容量缓冲区为 10%。

### 重要：

当总备用容量降低至低于交付组总容量的“X”百分比的水平时，容量缓冲区会导致计算机打开电源。这样做可以预留所需的备用容量百分比。

## 多会话操作系统交付组

### 计算机何时打开电源？

#### 重要：

如果选择了计划，AutoScale 将打开在计划中配置为打开电源的所有计算机的电源。无论负载如何，Autoscale 都会在计划期间保持此指定数量的计算机打开电源。

如果交付组中打开电源的计算机数量不能再满足根据负载指数计算的缓冲区容量所需的缓冲区，AutoScale 将打开其他计算机的电源。例如，假设您的交付组有 20 台计算机，作为基于计划的扩展的一部分，其中 3 台计算机计划打开电源，并且容量缓冲区为 20%。最终，当没有负载时，4 台计算机将打开电源。这是因为需要 4 x 10k 负载指数作为缓冲区；因此至少需要打开 4 台计算机的电源。这种情况可能发生在高峰时段、计算机上的负载增加、新会话启动以及向交付组中添加新计算机时。请注意，AutoScale 仅打开满足以下条件的计算机的电源：

- 计算机不处于维护模式。
- 运行计算机的虚拟机管理程序不处于维护模式。
- 计算机当前已关闭电源。
- 计算机没有待处理的电源操作。

## 计算机何时关闭电源？

### 重要：

- 如果选择了计划，AutoScale 将根据计划关闭计算机的电源。
- AutoScale 不会关闭计划中配置为在计划期间打开电源的计算机的电源。

如果有足够多的计算机支持交付组的已打开电源的计算机（包括缓冲区）的目标数量，AutoScale 将关闭额外的计算机的电源。这种情况可能发生在非高峰时段、计算机上的负载降低、会话注销以及从交付组中删除计算机时。AutoScale 仅关闭满足以下条件的计算机的电源：

- 计算机和运行计算机的虚拟机管理程序不处于维护模式。
- 计算机当前已打开电源。
- 计算机注册为可用或在启动后等待注册。
- 计算机没有活动会话。
- 计算机没有待处理的电源操作。
- 计算机满足指定的关机延迟条件。这意味着计算机已打开电源至少“X”分钟，其中“X”是为交付组指定的关机延迟。

## 示例方案

假设您遇到以下情况：

- 交付组配置。您希望 AutoScale 管理电源的交付组包含 10 台计算机（M1 到 M10）。
- **AutoScale 配置**
  - 容量缓冲区设置为 10%。
  - 所选计划中不包括任何计算机。

该方案按以下顺序执行：

1. 没有用户登录。
2. 用户会话增加。
3. 更多用户会话启动。
4. 由于会话终止，用户会话负载会降低。
5. 用户会话负载进一步降低，直到会话负载仅由本地资源进行处理。

有关 AutoScale 在上述场景中如何工作的详细信息，请参阅下文。

- 无用户负载（初始状态）

- 一台计算机（例如，M1）已打开电源。由于配置的容量缓冲区，计算机已打开电源。在这种情况下， $10 \text{ (计算机数量)} \times 10000 \text{ (负载指数)} \times 10\% \text{ (配置的容量缓冲区)}$  等于 10000。因此，一台计算机已打开电源。
- 已打开电源的计算机 (M1) 的负载指数值为基准负载（负载指数等于 0）。
- 第一个用户登录
  - 会话将定向到托管在计算机 M1 上。
  - 已打开电源的计算机 M1 的负载指数增加，计算机 M1 不再处于基准负载。
  - 由于配置了容量缓冲区，AutoScale 开始打开额外的计算机 (M2) 的电源以满足需求。
  - 计算机 M2 的负载指数值为基准负载。
- 用户增加负载
  - 这些会话在计算机 M1 和 M2 之间进行负载平衡。因此，已打开电源的计算机 (M1 和 M2) 的负载指数增加。
  - 总备用容量的负载指数仍处于 10000 以上的水平。
  - 计算机 M2 的负载指数值不再为基准负载。
- 更多用户会话启动
  - 这些会话在计算机 (M1 和 M2) 之间进行负载平衡。因此，已打开电源的计算机 (M1 和 M2) 的负载指数进一步增加。
  - 当总备用容量降至负载指数低于 10000 的水平时，由于配置了容量缓冲区，AutoScale 将开始打开额外的计算机 (M3) 以满足需求。
  - 计算机 M3 的负载指数值为基准负载。
- 更多用户会话启动
  - 这些会话在计算机 (M1 到 M3) 之间进行负载平衡。因此，已打开电源的计算机 (M1 到 M3) 的负载指数增加。
  - 总备用容量的负载指数处于 10000 以上的水平。
  - 计算机 M3 的负载指数值不再为基准负载。
- 由于会话终止，用户会话负载会降低
  - 用户从其会话中注销或空闲会话超时后，计算机 M1 到 M3 上释放的容量将重新用于托管其他用户启动的会话。
  - 当总备用容量的负载指数增加到 10000 以上的水平时，AutoScale 将其中一台计算机（例如 M3）置于耗尽状态。因此，除非出现新更改，否则其他用户启动的会话将不再定向到该计算机。例如，最终用户负载再次增加或者其他计算机的负载变得最少。
- 用户会话负载继续降低
  - 在计算机 M3 上的所有会话终止并且指定的关机延迟超时后，AutoScale 将关闭计算机 M3 的电源。
  - 更多用户终止其会话后，已打开电源的计算机 (M1 和 M2) 上释放的容量将重新用于托管其他用户启动的会话。

- 当总备用容量的负载指数增加到 10000 以上的水平时，AutoScale 将其中一台计算机（例如 M2）置于耗尽状态。因此，其他用户启动的会话将不再定向到该计算机。
- 用户会话负载将继续降低，直至没有会话
  - 在计算机 M2 上的所有会话终止并且指定的关机延迟超时后，AutoScale 将关闭计算机 M2 的电源。
  - 已打开电源的计算机 (M1) 的负载指数值为基准负载。由于配置了容量缓冲区，AutoScale 不会将计算机 M1 置于耗尽状态。

**注意：**

对于多会话操作系统交付组，当用户注销会话时，对桌面所做的所有更改都将丢失。但是，如果已配置，用户特定的设置将随用户配置文件一起漫游。

### 单会话操作系统随机交付组

容量缓冲区用于根据交付组中的计算机总数保持计算机的缓冲区打开电源来适应突然出现的需求峰值。默认情况下，容量缓冲区占交付组中计算机总数的 10%。

如果计算机数（包括容量缓冲区）超过当前已打开电源的计算机总数，则会打开其他计算机的电源以满足需求。如果计算机数（包括容量缓冲区）少于当前已打开电源的计算机总数，则多余的计算机将关闭或暂停，具体取决于您配置的操作。

### 电源策略

配置策略以管理不同场景下的计算机电源。对于每种情况，您可以指定等待时间（以分钟为单位）和在指定时间结束后要采取的操作。电源策略适用于单会话操作系统随机交付组和单会话操作系统静态交付组。



Manage Autoscale

Enabled

×

Single-random

General

Schedule and Peak Times

Load-based Settings

ADVANCED

Dynamic Session Timeout

Autoscaling Tagged Machines

Load-based Settings

Capacity buffer

Capacity buffer is used to accommodate sudden spikes in demand by keeping a buffer of machines powered on based on the maximum load index of the delivery group. By default, the capacity buffer is 10% of the maximum supported load index of the delivery group. A lesser value decreases the cost. A greater value ensures an optimized user experience so that users do not have to wait for additional machines to power on when launching sessions. [Learn more](#)

During peak times

During off-peak times

Capacity buffer (%):

10

10

Power policies

Configure policies for power managing machines in different scenarios. For each scenario, specify the waiting period (in minutes) and the action to take after the specified period elapses.

After disconnection

	Waiting period (min)	Action
During peak times	<div>0</div>	<div>No action</div>
During off-peak times	<div>0</div>	<div>No action</div> <div>Suspend</div> <div>Shut down</div>

Save

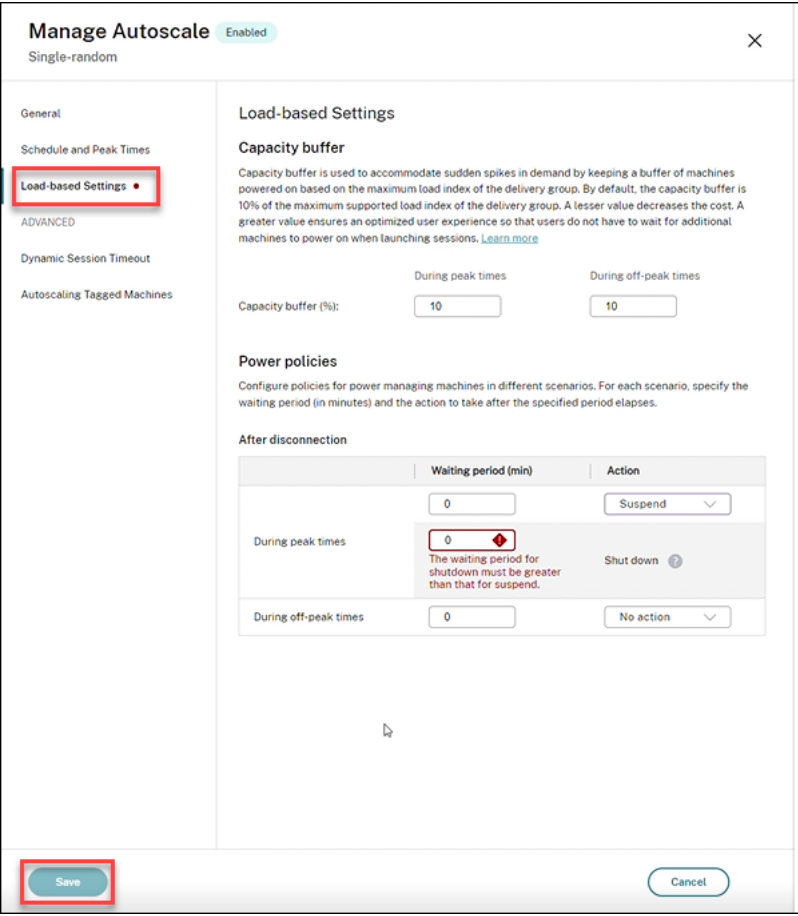
Cancel

断开连接后，以下设置适用于高峰时段和非高峰时段：

- 您可以从下拉列表中设置以分钟为单位的等待时间以及诸如无操作、暂停或关闭之类的操作。
- 如果选择暂停操作，请配置额外的等待时间以关闭计算机。

注意：

- 在高峰和非高峰时段，关机操作的等待时间必须大于暂停的等待时间。
- 只有已断开连接的用户在重新连接时才能访问已暂停的计算机。要使暂停的计算机可供新用户使用，请将其关闭。
- 如果暂停和关闭字段的时间设置配置不正确，则“保存”选项将被禁用，并且导航项目旁边还会出现一个红点，表示设置错误。



举个例子

- 如果您将等待时间设置为 12 分钟，并将第一个操作选择为无操作，则在 12 分钟结束后，计算机将继续处于开机状态。
- 如果您将等待时间设置为 15 分钟，并选择第一个操作暂停，将第二个等待时间设置为 20 分钟，则在 15 分钟结束后，计算机将暂停。在第二个等待时间结束后，计算机将关闭。
- 如果您将等待时间设置为 18 分钟并选择要关闭的第一个操作，则在 18 分钟结束后，计算机将关闭。

示例方案

假设您遇到以下情况：

- 交付组配置。您希望 AutoScale 管理电源的交付组包含 10 台计算机（M1 到 M10）。
- **AutoScale** 配置
  - 容量缓冲区设置为 10%。
  - 所选计划中不包括任何计算机。

该方案按以下顺序执行：

1. 没有用户登录。
2. 用户会话增加。
3. 更多用户会话启动。
4. 由于会话终止，用户会话负载会降低。
5. 用户会话负载进一步降低，直到会话负载仅由本地资源进行处理。

有关 AutoScale 在上述场景中如何工作的详细信息，请参阅下文。

- 无用户负载（初始状态）
  - 一台计算机 (M1) 已打开电源。由于配置的容量缓冲区，计算机已打开电源。在这种情况下， $10 \text{ (计算机数量)} \times 10\%$ （配置的容量缓冲区）等于 1。因此，一台计算机已打开电源。
- 第一个用户登录
  - 用户首次登录以使用桌面时，将从已打开电源的计算机上托管的桌面池中为用户分配一个桌面。在这种情况下，将从计算机 M1 为用户分配桌面。
  - 由于配置了容量缓冲区，AutoScale 开始打开额外的计算机 (M2) 的电源以满足需求。
- 第二个用户登录
  - 用户将从计算机 M2 分配一个桌面。
  - 由于配置了容量缓冲区，AutoScale 开始打开额外的计算机 (M3) 的电源以满足需求。
- 第三个用户登录
  - 从计算机 M3 为用户分配桌面。
  - 由于配置了容量缓冲区，AutoScale 开始打开额外的计算机 (M4) 的电源以满足需求。
- 用户注销
  - 用户注销或用户的桌面超时后，释放的容量（例如 M3）可用作缓冲区。因此，AutoScale 开始关闭计算机 M4 的电源，因为容量缓冲区配置为 10%。
- 更多用户注销，直至没有用户
  - 在更多用户注销后，AutoScale 将关闭计算机的电源（例如，M2 或 M3）。
  - 即使没有用户剩余，AutoScale 也不会关闭剩余的最后一台计算机（例如 M1）的电源，因为该计算机预留为备用容量。

**注意：**

对于单会话操作系统随机交付组，当用户注销会话时，对桌面所做的所有更改都将丢失。但是，如果已配置，用户特定的设置将随用户配置文件一起漫游。

## 单会话操作系统静态交付组

容量缓冲区用于根据交付组中未分配的计算机总数保持未分配的计算机的缓冲区打开电源来适应突然出现的需求峰值。默认情况下，容量缓冲区占交付组中未分配的计算机总数的 10%。

### 重要：

分配交付组中的所有计算机后，容量缓冲区不会在打开或关闭计算机电源方面发挥作用。

如果计算机数（包括容量缓冲区）超过当前已打开电源的计算机总数，则会打开其他未分配的计算机的电源以满足需求。如果计算机数（包括容量缓冲区）少于当前已打开电源的计算机总数，则多余的计算机将关闭电源或暂停，具体取决于您配置的操作。

对于单会话操作系统静态交付组，Autoscale：

- 仅当适用的单会话操作系统交付组的 `AutomaticPowerOnForAssigned` 属性设置为 `true` 时，才能在高峰时段打开已分配的计算机的电源以及在非高峰时段关闭其电源。
- 将在高峰时段自动打开计算机的电源，前提是计算机已关闭电源并且计算机所属的交付组的 `AutomaticPowerOnForAssignedDuringPeak` 属性已设置为 `true`。

要了解容量缓冲区如何与已分配的计算机结合使用，请注意以下事项：

- 仅当交付组有一个或多个未分配的计算机时，容量缓冲区才起作用。
- 如果交付组没有未分配的计算机（交付组中的所有计算机都已分配），则容量缓冲区不会在打开或关闭计算机电源方面发挥作用。
- `AutomaticPowerOnForAssignedDuringPeak` 属性确定已分配的计算机是否在高峰时段打开电源。如果设置为 `true`，Autoscale 会在高峰时段保持计算机处于打开电源状态。即使关闭了电源，Autoscale 也会打开其电源。

## 电源策略

配置策略以管理不同场景下的计算机电源。对于每种情况，您可以指定等待时间（以分钟为单位）和在指定时间结束后要采取的操作。电源策略适用于单会话操作系统随机交付组和单会话操作系统静态交付组。

Manage Autoscale

Enabled

×

single-static

General

Schedule and Peak Times

Load-based Settings

ADVANCED

Dynamic Session Timeout

Autoscaling Tagged Machines

Load-based Settings

Capacity buffer

Capacity buffer is used to accommodate sudden spikes in demand by keeping a buffer of machines powered on based on the maximum load index of the delivery group. By default, the capacity buffer is 10% of the maximum supported load index of the delivery group. A lesser value decreases the cost. A greater value ensures an optimized user experience so that users do not have to wait for additional machines to power on when launching sessions. [Learn more](#)

During peak times

During off-peak times

Capacity buffer (%):

10

10

Power policies

Configure policies for power managing machines in different scenarios. For each scenario, specify the waiting period (in minutes) and the action to take after the specified period elapses.

After disconnection

	Waiting period (min)	Action
During peak times	0	Suspend
During off-peak times	0	Suspend

After logoff

	Waiting period (min)	Action
During peak times	0	Suspend
During off-peak times	0	Suspend

If no user logs on after machine is powered on by Autoscale

	Waiting period (min)	Action
During peak times	10	Suspend

Save

Cancel

对于“断开连接后”和“注销之后”，以下设置适用于高峰时段和非高峰时段：

您可以从下拉列表中设置等待时间（以分钟为单位）和诸如无操作、暂停或关闭之类的操作。

如果在 **Autoscale** 开机后没有用户登录，则以下设置仅在高峰时段适用：

您可以设置以分钟为单位的等待时间，也可以在高峰时段从下拉菜单中设置诸如不执行任何操作、暂停或关闭之类的操作。

示例方案

假设您遇到以下情况：

- 交付组配置。您希望 **AutoScale** 管理电源的交付组包含 10 台计算机（M1 到 M10）。
- **AutoScale** 配置
  - 分配计算机 M1 到 M3，并取消分配计算机 M4 到 M10。
  - 高峰和非高峰时段的容量缓冲区设置为 10%。
  - 根据选定的时间表，**AutoScale** 在上午 9:00 至下午 6:00 之间对计算机进行电源管理。

有关 **AutoScale** 在上述场景中如何工作的详细信息，请参阅下文。

- 时间表开始时间 - 上午 9:00
  - AutoScale 打开计算机 M1 到 M3 的电源。
  - 由于已配置的容量缓冲区，AutoScale 将打开另一台计算机（例如 M4）的电源。计算机 M4 未分配。
- 第一个用户登录
  - 用户首次登录以使用桌面时，将从已打开电源的未分配计算机上托管的桌面池中为用户分配一个桌面。在这种情况下，将从计算机 M4 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。
  - 由于配置了容量缓冲区，AutoScale 开始打开额外的计算机（例如 M5）的电源以满足需求。
- 第二个用户登录
  - 从已打开电源的未分配计算机为用户分配桌面。在这种情况下，将从计算机 M5 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。
  - 由于配置了容量缓冲区，AutoScale 开始打开额外的计算机（例如 M6）的电源以满足需求。
- 用户注销
  - 当用户从其桌面注销或桌面超时，Autoscale 会在上午 9:00 至下午 6:00 期间保持打开计算机 M1 到 M5 的电源。当这些用户下次登录时，将连接到首次使用时分配的同一桌面。
  - 未分配的计算机 M6 正在等待向未分配的传入用户提供桌面服务。
- 时间表结束时间 - 下午 6:00
  - 在下午 6:00，AutoScale 关闭计算机 M1 到 M5 的电源。
  - 由于配置了容量缓冲区，AutoScale 将保持未分配的计算机 M6 打开电源。该计算机正在等待向未分配的传入用户提供桌面服务。
  - 在交付组中，计算机 M6 到 M10 为未分配的计算机。

## 动态会话超时

June 20, 2023

此功能允许您为高峰和非高峰使用时间配置断开连接和空闲的会话超时，以实现更快的计算机终止和节省成本。此功能适用于单会话和多会话操作系统计算机。VDA 报告空闲超过 10 分钟的会话的空闲时间，因此动态会话超时将无法在空闲 10 分钟内断开空闲会话的连接。值越小，则可以更快地消除延迟的会话，从而降低成本。

Manage Autoscale

Enabled

×

CYAZinfo1027

General

Schedule and Peak Times

Load-based Settings

ADVANCED

Dynamic Session Timeout

Force User Logoff

Autoscaling Tagged Machines

Dynamic Session Timeout

Configure dynamic timeouts for your peak and off-peak usage times to achieve faster VM draining and cost savings. Larger values can improve user experience and smaller values can achieve faster draining.  
[Learn more](#)

During peak times

During off-peak times

Idle session timeout: ?

Disable

min

3

min

Disconnected session timeout: ?

4

min

5

min

⚠

Autoscale dynamic timeouts are for cost savings. If used for security purposes, the configured timeouts might conflict with your GPO or Studio policies. When a conflict occurs, the shorter timeout prevails. ↗

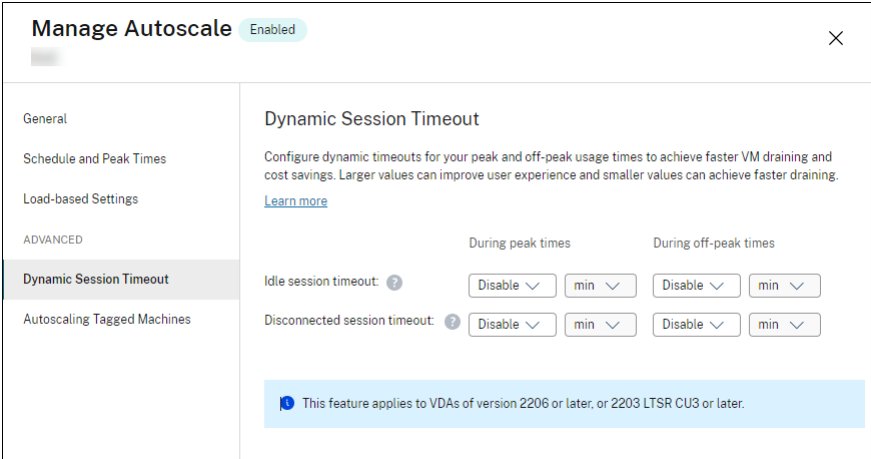
Save

Apply

Cancel

↶

- 注意：
- 此功能始终适用于多会话操作系统交付组。
  - 对于单会话操作系统交付组，此功能适用于 2206 CR 或更高版本或 2203 LTSR CU3 或更高版本的 VDA。请确保这些 VDA 已在 Citrix Cloud 中至少注册过一次。不可用时，将显示以下用户界面：



- Autoscale 动态超时是为了节省成本。如果出于安全目的，配置的超时可能会与您的 GPO 或“管理”控制台策略相冲突。发生冲突时，请以较短的超时为准。

空闲会话超时。启用或禁用用于指定在没有用户输入的情况下保持不间断的用户连接的时间的计时器。此计时器过期后，会话将处于断开连接状态，并且断开连接的会话超时适用。如果断开连接的会话超时处于禁用状态，会话将不注销。

重要：

- 如果指定的值小于或等于 10 分钟（600 秒），Autoscale 会在相关会话空闲 10 分钟后断开连接。这是因为 AutoScale 依赖于 VDA 报告的会话空闲时间。VDA 仅报告空闲超过 10 分钟的会话的空闲时间。
- 如果用户在达到空闲会话超时的最后 5 分钟内与空闲会话进行交互，该会话仍将处于断开连接状态。

断开连接的会话超时。启用或禁用用于指定断开连接的桌面在会话注销之前保持锁定状态的时长。如果已启用，断开连接的会话将在计时器超时时注销。

## 自动缩放带标记的计算机（云突发）

March 2, 2023

注意：

此功能以前成为“限制 AutoScale”。

### 简介

AutoScale 只能灵活地管理交付组中计算机子集的电。为此，请将标记应用到一台或多台计算机，然后将 AutoScale 配置为仅对带标记的计算机进行电源管理。

此功能在云爆发用例中非常有用，在此类用例中，您希望在基于云的资源满足额外需求（即工作负载爆发）之前使用本地资源（或预留的公有云实例）处理工作负载。要让本地计算机（或预留的实例）首先处理工作负载，必须使用标记限制以及区域首选项。



标记限制指定由 AutoScale 进行电源管理的计算机。区域首选项指定首选区域中的计算机以处理用户启动请求。有关区域首选项的详细信息，请参阅[标记](#)和[区域首选项](#)。

要自动扩展某些带标记的计算机，可以使用“管理”控制台或 PowerShell。

使用“管理”控制台自动缩放某些带标记的计算机

要自动缩放某些带标记的计算机，请完成以下步骤：

1. 创建标记并将该标记应用到交付组中适用的计算机。有关详细信息，请参阅[管理标记和标记限制](#)。
2. 选择交付组，然后打开管理 **Autoscale** 向导。
3. 在自动缩放已标记的计算机页面上，选择为带标记的计算机启用 **Autoscale**，从列表选择一个标记，然后单击应用以保存更改。

单会话操作系统静态和随机交付组的用户界面：

Manage Autoscale

Enabled

151515

General

Schedule and Peak Times

Load-based Settings

ADVANCED

Autoscaling Tagged Machines

Autoscaling Tagged Machines

Use this feature to power manage only tagged machines within the delivery group. This feature is useful for cloud burst or disaster recovery use cases where you want to give preference to on-premises or reserved instances over pay-as-you-go cloud instances. To use it, tag the cloud instances, specify the tag below, and then configure zone preference. [Learn more](#)

☐

Enable Autoscale for machines with tag

Select a tag

Save

Apply

Cancel

多会话操作系统交付组的用户界面：

Manage Autoscale

Enabled

×

CYAZinfo1027

General

Schedule and Peak Times

Load-based Settings

ADVANCED

Dynamic Session Timeout

Force User Logoff

Autoscaling Tagged Machines

Autoscaling Tagged Machines

Use this feature to power manage only tagged machines within the delivery group. This feature is useful for cloud burst or disaster recovery use cases where you want to give preference to on-premises or reserved instances over pay-as-you-go cloud instances. To use it, tag the cloud instances, specify the tag below, and then configure zone preference. [Learn more](#)

☐

Enable Autoscale for machines with tag

Select a tag

▼

Save

Apply

Cancel

警告：

- 自动缩放带特定标记的计算机可能会导致直方图自动更新以反映每个标记的计算机数量。如果需要，在计划和高峰时间页面上，您可以根据每个时段手动分配计算机。
- 您无法删除正在带标记的计算机上使用的标记。要删除标记，必须首先删除标记限制。

应用标记限制后，您可能希望稍后将其从交付组中删除。为此，请转到管理 **Autoscale** > 自动缩放已标记的计算机页面，然后取消选中为带标记的计算机启用 **Autoscale**。

警告：

- 如果在未清除为带标记的计算机启用 **Autoscale** 的情况下从适用的计算机中删除标记，则在打开管理 **Autoscale** 向导时可能会收到警告。从计算机中删除标记不会让 Autoscale 管理任何计算机，因为您在 Autoscale 中指定的标记已失效。要解决该警告，请转到自动缩放已标记的计算机 页面，删除无效标记，然后单击应用以保存更改。

控制 **Autoscale** 打开资源电源的时间

还可以根据未标记计算机的使用情况控制 **Autoscale** 何时开始打开带标记的计算机的电源。这有助于您进一步优化带标记的工作负载或公有云工作负载的使用。

为此，请完成以下步骤：

- 1. 在自动缩放已标记的计算机页面上，选择控制 **AutoScale** 何时开始打开已标记的计算机的电源。
- 2. 输入要在高峰时段和非高峰时段达到的未标记计算机使用率的百分比，然后单击应用。支持的值：0—100。

Manage Autoscale

Enabled

✕

General

Schedule and Peak Times

Load-based Settings

ADVANCED

Dynamic Session Timeout

User Logoff Notifications

Autoscaling Tagged Machines

Autoscaling Tagged Machines

Use this feature to power manage only tagged machines within the delivery group. This feature is useful for cloud burst or disaster recovery use cases where you want to give preference to on-premises or reserved instances over pay-as-you-go cloud instances. To use it, tag the cloud instances, specify the tag below, and then configure zone preference. [Learn more](#)

☒ Enable Autoscale for machines with tag

▼

☐ Control when Autoscale starts powering on tagged machines ?

During peak times

During off-peak times

When percentage of remaining untagged capacity falls below (%) ?

10

10

Save

Cancel

提示：

百分比控制 AutoScale 何时开始打开带标记的计算机的电源。当百分比降至阈值以下（默认值为 10%）时，AutoScale 开始打开带标记的计算机的电源。当百分比超过阈值时，AutoScale 进入关机模式。输入百分比时，请考虑两种情况：

- 对于单会话操作系统交付组：该值定义为处于空闲状态的未标记计算机总数的百分比。示例：您有 10 台未标记的单会话操作系统计算机。当只剩下一台没有会话时，AutoScale 开始打开带标记的计算机的电源。
- 对于多会话操作系统交付组：该值定义为可用未标记计算机的总容量（按负载指数计算）的百分比。示例：您有 10 台未标记的多会话操作系统计算机。当它们的负载达到 90% 时，AutoScale 开始打开带标记的计算机的电源。

## 使用 **PowerShell** 自动缩放某些带标记的计算机

要直接使用 PowerShell SDK，请完成以下步骤：

1. 创建标记。使用 `New-BrokerTag` PowerShell 命令创建标记。
  - 例如：`$managed = New-BrokerTag Managed`。在这种情况下，标记名为“Managed”。有关 `New-BrokerTag` PowerShell 命令的详细信息，请参阅 <https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/>。
2. 将标记应用到计算机。使用 `Get-BrokerMachine` PowerShell 命令将标记应用到您希望 AutoScale 进行电源管理的目录中的计算机。
  - 例如：`Get-BrokerMachine -CatalogName "cloud" | Add-BrokerTag $managed.Name`。在这种情况下，目录名为“cloud”。
  - 有关 `Get-BrokerMachine` PowerShell 命令的详细信息，请参阅 <https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/>。

注意：

应用标记后，可以将新计算机添加到目录中。标记 *NOT* 将自动应用到这些新计算机。

3. 将带标记的计算机添加到您希望 **AutoScale** 进行电源管理的交付组。使用 `Get-BrokerDesktopGroup` PowerShell 命令向包含计算机的交付组添加标记限制（换句话说，“限制在带有标记 X 的计算机上启动”）。
  - 例如：`Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`。在这种情况下，交付组的 UID 为 1。
  - 有关 `Get-BrokerDesktopGroup` PowerShell 命令的详细信息，请参阅 <https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>。

应用标记限制后，您可能希望稍后将其从交付组中删除。要执行此操作，请使用 `Get-BrokerDesktopGroup` PowerShell 命令。

示例：`Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTag $null`。在这种情况下，交付组的 UID 为 1。

**注意：**

未标记的计算机在用户关闭电源后自动重新启动。这种行为可以确保其可用于更快地处理工作负载。可以使用 `Set-BrokerDesktopGroup` 的 `AutomaticRestartForUntaggedMachines` 属性在每个桌面组上启用或禁用此功能。有关详细信息，请参阅 <https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>。

**示例方案**

假设您遇到以下情况：

- 计算机目录配置。有两个计算机目录（C1 和 C2）。
  - 目录 C1 包含本地部署中的 5 台本地计算机（M1 到 M5）。
  - 目录 C2 包含云部署中的 5 台远程计算机（M6 到 M10）。
- 标记限制。创建名为“Cloud”的标记并将其应用于目录 C2 中的 M6 到 M10 计算机。
- 区域配置。创建两个区域（Z1 和 Z2）。
  - 包含目录 C1 的区域 Z1 对应本地部署。
  - 包含目录 C2 的区域 Z2 对应云部署。
- 交付组配置
  - 交付组包含 10 台计算机（M1 到 M10），5 台来自目录 C1 的计算机（M1 到 M5）以及 5 台来自目录 C2 的计算机（M6 到 M10）。
  - 计算机 M1 到 M5 手动打开电源，并在整个计划中保持打开电源。
- **AutoScale** 配置
  - 容量缓冲区设置为 10%。
  - AutoScale 电源仅管理带有“云”标记的计算机。在这种情况下，AutoScale 对云计算机 M6 到 M10 进行电源管理。
- 已发布的应用程序或桌面配置。为已发布的桌面配置区域首选项（例如），其中区域 Z1 的优先级高于用户启动请求的区域 Z2。
  - 区域 Z1 配置为已发布的桌面的首选区域（主区域）。

该方案按以下顺序执行：

1. 没有用户登录。
2. 用户会话增加。
3. 用户会话将进一步增加，直到占用所有可用的本地计算机。
4. 更多用户会话启动。

5. 由于会话终止，用户会话将减少。
6. 用户会话进一步减少，直到会话负载仅由本地计算机进行处理。

有关 AutoScale 在上述场景中如何工作的详细信息，请参阅下文。

- 无用户负载（初始状态）
  - 本地计算机 M1 到 M5 已打开电源。
  - 云中的一台计算机（例如，M6）已打开电源。由于配置的容量缓冲区，计算机已打开电源。在这种情况下， $10 \text{ (计算机数量)} \times 10000 \text{ (负载指数)} \times 10\% \text{ (配置的容量缓冲区)} = 10000$ 。因此，一台计算机已打开电源。
  - 所有已打开电源的计算机（M1 到 M6）的负载指数值为基准负载（负载指数等于 0）。
- 用户登录
  - 通过配置的区域首选项将会话定向到托管在计算机 M1 到 M5 上，并在这些本地计算机之间进行负载平衡。
  - 已打开电源的计算机（M1 到 M5）的负载指数值增加。
  - 已打开电源的计算机 M6 的负载指数值为基准负载。
- 用户增加负载，消耗所有本地资源
  - 通过配置的区域首选项将会话定向到托管在计算机 M1 到 M5 上，并在这些本地计算机之间进行负载平衡。
  - 所有已打开电源的计算机（M1 到 M5）的负载指数值已达到 10000。
  - 已打开电源的计算机 M6 的负载指数值保持为基准负载。
- 还有一个用户登录
  - 会话溢出区域首选项，并定向到托管在云计算机 M6 上。
  - 所有已打开电源的计算机（M1 到 M5）的负载指数值已达到 10000。
  - 已打开电源的计算机 M6 的负载指数值增加，不再处于基准负载。当总备用容量降至负载指数低于 10000 的水平时，由于配置了容量缓冲区，AutoScale 将开始打开额外的计算机 (M7) 以满足需求。请注意，打开计算机 M7 的电源可能需要一段时间。因此可能会有延迟，直到计算机 M7 准备就绪。
- 更多用户登录
  - 会话将定向到托管在计算机 M6 上。
  - 所有已打开电源的计算机（M1 到 M5）的负载指数值已达到 10000。
  - 已打开电源的计算机 M6 的负载指数值进一步增加，但总备用容量的负载指数处于 10000 以上的水平。
  - 已打开电源的计算机 M7 的负载指数值保持为基准负载。
- 更多用户登录
  - 在计算机 M7 准备就绪后，会话将定向到托管在计算机 M6 和 M7 上，并在这些计算机之间进行负载平衡。
  - 所有已打开电源的计算机（M1 到 M5）的负载指数值已达到 10000。
  - 计算机 M7 的负载指数值不再为基准负载。
  - 已打开电源的计算机（M6 和 M7）的负载指数值增加。
  - 总备用容量的负载指数仍处于 10000 以上的水平。

- 由于会话终止，用户会话负载会降低
  - 用户从其会话中注销或空闲会话超时后，计算机 M1 到 M7 上释放的容量将重新用于托管其他用户启动的会话。
  - 当总备用容量的负载指数增加到 10000 以上的水平时，AutoScale 将其中一台云计算机（M6 到 M7）置于终止状态。因此，除非发生新的更改，否则其他用户启动的会话不再定向到该计算机（例如 M7）；例如，用户负载再次增加或其他云计算机的负载变得最少。
- 用户会话负载进一步降低，直到不再需要一台或多台云计算机
  - 在计算机 M7 上的所有会话终止并且指定的关机延迟超时后，AutoScale 将关闭计算机 M7 的电源。
  - 所有已打开电源的计算机（M1 到 M5）的负载指数值可能会降低至 10000。
  - 已打开电源的计算机（M6）的负载指数值降低。
- 用户会话进一步减少，直到不需要云计算机为止。
  - 即使计算机 M6 上没有任何用户会话，AutoScale 也不会关闭电源，因为该计算机预留给备用容量。
  - 由于配置了容量缓冲区，AutoScale 将保持剩余的云计算机 M6 打开电源。该计算机正在等待向传入用户提供桌面服务。
  - 只要本地计算机有可用容量，就不会将会话定向为托管在计算机 M6 上。

## 动态预配计算机

November 21, 2022

AutoScale 提供动态创建计算机以及将其删除的功能。可以使用 PowerShell 脚本来利用该功能。该脚本可帮助您根据当前负载条件动态增加或减少交付组中的计算机数量。

该脚本提供以下优势（以及更多）：

- 降低存储成本。与有助于降低计算成本的 AutoScale 不同，该脚本提供了一个更具成本效益的解决方案来预配计算机。
- 有效处理负载变化。该脚本通过根据当前的交付组负载自动增加或减少计算机数量来帮助您处理负载变化。

## 下载脚本

PowerShell 脚本在 <https://github.com/citrix/PowerShell-Scripts/tree/master/XAXD/AutoscaleMcs> 提供。

## 脚本的工作原理

重要：

- 不能在多个交付组中指定通过脚本管理的计算机目录。换句话说，如果多个交付组共享同一计算机目录，该脚本将不适用于其中任何交付组。
- 不能同时从多个位置运行同一交付组的脚本。

该脚本在交付组级别运行。它测量负载（根据[负载指数](#)），然后确定是创建计算机还是删除计算机。

通过此脚本创建的计算机具有唯一标记（通过 `ScriptTag` 参数），以便以后可以识别这些计算机。创建或删除计算机是根据：

- 交付组的最大负载百分比。指定为 `AutoScale` 创建计算机以解决额外负载的最大级别。超过此阈值时，将分批创建计算机，以确保当前负载降低到或低于阈值。
- 交付组的最小负载百分比。指定删除通过此脚本创建的并且没有活动会话的计算机的最低级别。超过此阈值时，通过此脚本创建的没有活动会话的计算机将被删除。

此脚本用于跨交付组进行监视，并在满足触发条件时创建或删除计算机。它在每次运行的基础上执行。这意味着您需要定期运行脚本，以便其能够按预期运行。我们建议您以最少 5 分钟的时间间隔运行脚本。这样做可以提高整体响应能力。

该脚本依赖以下参数来运行：

参数	类型	默认值	说明
<code>DeliveryGroupName</code>	字符串	X	要监视以确定当前负载的交付组的名称。可以提供以分号分隔的名称列表。例如： <code>Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName 'dg1;dg2;dg3' -XdProfileName profile</code> 。
<code>XdProfileName</code>	字符串	X	用于对远程服务器进行身份验证的配置文件的名称。有关使用此参数对远程服务器进行身份验证的详细信息，请参阅 <a href="#">身份验证 API</a> 。
<code>HighWatermark</code>	整数	80	为 <code>AutoScale</code> 创建计算机以解决额外负载的最大百分比负载（按负载指数计算）。



参数	类型	默认值	说明
LowWatermark	整数	15	删除通过此脚本创建的没有活动会话的计算机的最小负载百分比（按负载指数计算）。
MachineCatalogName	字符串	X	要创建计算机的计算机目录的名称。
MaximumCreatedMachine	整数	-1	可以在指定交付组中创建的计算机的最大数量。如果值等于或小于 0，脚本将不处理此参数。
ScriptTag	字符串	AutoscaledScripted	适用于通过此脚本创建的计算机的标签。
EventLogSource	字符串	X	在 Windows 事件查看器中显示的源名称。

注意：  
“X” 表示没有为该参数指定默认值。

默认情况下，脚本首次运行时需要所有参数（ScriptTag 参数除外）。在后续运行中，只需要 DeliveryGroupName 和 XdProfileName 参数。或者，您可以选择更新最小和最大负载百分比。

请注意，首次运行脚本时必须指定单个交付组。例如，如果您在首次运行脚本时使用以下 PowerShell 命令指定两个交付组，脚本将不起作用：

```
• Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1;dg2'-XdProfileName profile -LowWatermark 20 -HighWatermark 70 -MachineCatalogName 'cat1\'
```

相反，请首先使用以下命令指定单个交付组（在本示例中为 dg1）：

```
• Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1'-XdProfileName profile -LowWatermark 20 -HighWatermark 70 -MachineCatalogName 'cat1\'
```

然后，请使用以下命令运行第二个交付组的脚本（在此示例中为 dg 2）：

```
• Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1;dg2'-XdProfileName profile
```

## 必备条件

要运行脚本，请确保满足以下必备条件：

- 计算机位于正在创建计算机的同一域中。
- 该计算机上已安装远程 PowerShell SDK。有关远程 PowerShell SDK 的详细信息，请参阅 [SDK 和 API](#)。
- 其他必备条件：
  - 要监视的交付组
  - 通过 Machine Creation Services (MCS) 创建的具有关联预配方案（模板）的计算机目录
  - 与预配方案关联的标识池
  - 要创建的事件日志源，以便脚本能够将信息写入 Windows 事件日志
  - 允许您对远程服务器进行身份验证的安全客户端

## 权限、建议和通知

运行脚本时，请记住以下几点：

- 要使用 `XdProfileName` 参数对远程服务器进行身份验证，您需要使用在 Citrix Cloud 控制台中创建的 API 访问安全客户端来定义身份验证配置文件。有关详细信息，请参阅 [身份验证 API](#)。
- 您必须具有在 Active Directory 中创建和删除计算机帐户的权限。
- 我们建议您使用 Windows 任务计划程序自动执行 PowerShell 脚本。有关详细信息，请参阅 [使用 Windows 任务计划程序创建自动化任务](#)。
- 如果您希望脚本将信息（例如，故障和操作）写入 Windows 事件日志，需要首先使用 `New-EventLog` cmdlet 指定源名称。例如，`New-EventLog -LogName Application -Source <sourceName>`。然后可以在 Windows 事件查看器的应用程序窗格中查看事件。
- 如果在执行脚本过程中出现错误，请手动执行脚本，然后通过执行脚本检查来解决问题。

## 身份验证 API

在运行脚本之前，需要使用 API 访问安全客户端定义身份验证配置文件。必须使用运行脚本的相同帐户创建安全客户端。

安全客户端必须具有以下权限：

- 使用 MCS 创建和删除计算机。
- 编辑计算机目录（以添加和删除计算机）。
- 编辑交付组（以添加和删除计算机）。

创建安全客户端时，请确保您的帐户具有上述权限，因为安全客户端会自动从您的当前帐户继承权限。

要创建安全客户端，请完成以下步骤：

1. 登录 Citrix Cloud 控制台，然后导航到身份识别和访问管理 > **API** 访问。
2. 键入您的安全客户端的名称，然后单击创建客户端。

要对远程服务器进行身份验证，请使用 `Set-XDCredentials` PowerShell 命令。例如：

- `Set-XDCredentials -APIKey <key_id> -CustomerId <customer_id> -SecretKey <secret_key> -StoreAs <name specified by the XdProfileName parameter>`

## 使用 **Windows** 任务计划程序创建自动化任务

可以使用 Windows 任务计划程序自动执行 PowerShell 脚本。这样做可以按某些时间间隔或在满足某些条件时自动运行脚本。要使用 Windows 任务计划程序执行此脚本，请务必在创建任务 > 设置选项卡上选择请勿启动新实例。这样做会阻止 Windows 任务计划程序运行脚本的新实例（如果脚本已在运行）。

## 脚本执行示例

有关执行脚本的示例，请参阅下文。请注意，脚本文件被多次调用。在此示例中，为了模拟负载，将启动一个会话，然后终止。

```
PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName devtest -XdProfileName profile -MachineCatalogName autoscaled -ScriptTag "devtest"
[devtest]: Assuming default values for watermarks [15 : 80].
PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName engtest -XdProfileName profile -MachineCatalogName autoscaled2 -ScriptTag "engtest"
[engtest]: Assuming default values for watermarks [15 : 80].
PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
[engtest]: Provisioning more machines. Current Usage [99.99] >= High Watermark [80].
PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
[engtest]: Began provisioning of [1] machines to [engtest]. Monitoring task [ca2b0cad-9c50-4e20-8f1d-9ff81307b201].
PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
[engtest]: Provisioning task [ca2b0cad-9c50-4e20-8f1d-9ff81307b201] is complete. [1] created. [0] failed to create.
PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
[engtest]: Added [1] machines to [engtest].
PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
[engtest]: Removing extraneous machines: Current Usage [0] <= Low Watermark [15].
PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
[engtest]: Removing [1] machines from [engtest]. Monitoring task [28c6c242-af81-4693-a2a8-0587f09689b4]
PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
[engtest]: Machine deletion task [28c6c242-af81-4693-a2a8-0587f09689b4] is [Finished].
PS C:\Users\crisj\Desktop> .\Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName "devtest;engtest" -XdProfileName profile
```

## 脚本的故障排除清单

该脚本将信息（例如，错误和操作）写入 Windows 事件日志。该信息可帮助您解决执行脚本时遇到的问题。记住以下故障排除清单可能会有所帮助：

- 与远程服务器通信失败。可行的操作：
  - 验证与服务器的连接。

- 验证您使用的 API 密钥是否有效。
- 创建计算机失败。可行的操作：
  - 验证运行脚本的用户帐户是否具有足够的权限，能够在域中创建用户帐户。
  - 验证创建 API 密钥的用户是否具有足够的权限，能够使用 MCS 预配计算机。
  - 验证计算机目录的有效性（即，其映像仍然存在且处于良好状态）。
- 未能将计算机添加到计算机目录或交付组。可行的操作：
  - 验证创建 API 密钥的用户是否具有足够的权限，能够在计算机目录和交付组中添加和删除计算机。

## 用户注销通知（以前是强制用户注销）

June 1, 2023

### 重要：

此功能仅在基于多会话应用程序的交付组的 AutoScale 用户界面中可用。

为了更好地节省成本，AutoScale 允许您强制注销延迟的会话。它允许您向用户发送自定义通知并指定一个宽限期，在此宽限期之后，会话将被强制注销。此操作仅适用于处于 **耗尽状态** 的计算机，不适用于所有已打开电源的计算机。为避免强制用户注销可能导致的数据丢失，您可以改为将此功能配置为仅发送注销提醒而不强制用户注销。

您可以使用以下选项：

- 通知并强制用户注销
- 发送注销提醒而不强制用户注销
- 既不通知也不强制用户注销

### 通知并强制用户注销

如果选中，AutoScale 将在下面指定的时间之后从其会话中注销用户。

Manage Autoscale

Enabled

×

z1zqrr

General

Schedule and Peak Times

Load-based Settings

ADVANCED

Dynamic Session Timeout

User Logoff Notifications

Autoscaling Tagged Machines

User Logoff Notifications

Use this feature to shut down machines faster by removing lingering sessions from the machines in drain state. You can send a notification to users before logging them off after the specified time. To avoid potential data loss caused by forcing user logoffs, you can also configure this feature to only send logoff reminders without forcing user logoff. [Learn more](#)

☐ Neither notify nor force user logoff

☒ Notify and force user logoff

☐ Send logoff reminders without forcing user logoff

☒ Enable force logoff during peak times

Time after which users are logged off from their sessions

90

min

☐ Enable force logoff during off-peak times

Time after which users are logged off from their sessions

min

Display notification after machine enters drain state

Notification title:

Example: A forced logoff has been initiated

Notification message: ?

Example: Warning: To save costs, the machine shuts down in %s% seconds and you will be logged off from the session. Save your work and log back on to get a different machine.

!

If the machine is already in drain state, there are some considerations to keep in mind when changing settings. [Learn more](#)

Save

Cancel

在高峰时段启用强制注销。如果选择此选项，Autoscale 将在指定时间过去时的高峰时间从其会话中注销这些用户。

在非高峰时段启用强制注销。如果选择此选项，Autoscale 将在指定时间过去时的非高峰时间从其会话中注销这些用户。

计算机进入耗尽状态后显示通知。允许您在用户的计算机进入耗尽状态后向用户发送通知。

- 通知标题。允许您指定要发送给用户的通知的标题。示例: `A forced logoff has been initiated.`
- 通知消息。允许您指定要发送给用户的通知的内容。您可以使用 `%s%` 或 `%m%` 作为变量来指示消息中的指定时间。要以秒为单位表示时间，请使用 `%s%`。要以分钟为单位表示时间，请使用 `%m%`。示例: `Warning: To save costs, the machine shuts down in %s% seconds and you will be logged off from the session. Save your work and log back on to get a different machine.`

发送注销提醒而不强制用户注销

如果选中，用户将在计算机进入耗尽状态后收到从计算机注销的提醒。此提醒可以配置为按下面指定的时间间隔发送。

Manage Autoscale

Enabled

×

Multi-CMD-NDJ-0407-1

General

Schedule and Peak Times

Load-based Settings

ADVANCED

Dynamic Session Timeout

User Logoff Notifications

Autoscaling Tagged Machines

User Logoff Notifications

Use this feature to shut down machines faster by removing lingering sessions from the machines in drain state. You can send a notification to users before logging them off after the specified time. To avoid potential data loss caused by forcing user logoffs, you can also configure this feature to only send logoff reminders without forcing user logoff. [Learn more](#)

☐ Neither notify nor force user logoff

☐ Notify and force user logoff

☒ Send logoff reminders without forcing user logoff

☐ Remind users during peak times

Send reminder every

min

☐ Remind users during off-peak times

Send reminder every

min

Logoff reminder

Reminder title

Example: Please log off from your session

Reminder message

Example: To save costs, please log off from your session. Log back on to get a different machine. You are reminded every %m% minutes.

ⓘ

If the machine is already in drain state, there are some considerations to keep in mind when changing settings. [Learn more](#)

Save

Cancel

2

在高峰时段提醒用户。如果选中此选项，则用户会在高峰时段每 X 分钟（X 表示指定时间）收到注销会话的提醒。

在非高峰时段提醒用户。如果选中此选项，则每隔 X 分钟（X 表示指定时间），用户会在非高峰时段收到注销会话的提醒。

注销提醒。允许您配置在计算机进入耗尽状态后发送给用户的提醒。

- 提醒标题。允许您指定要发送给用户的提醒的标题。示例：Please log off from your session。
- 提醒消息。允许您指定要发送给用户的消息。示例：Please log off from your session and log back on to save costs。

既不通知也不强制用户注销

如果选中，Autoscale 既不会强制用户注销处于耗尽状态的计算机，也不会通知用户手动切换到另一台计算机。

注意事项

如果计算机已处于耗尽状态，请在更改设置时考虑以下事项：

- 如果将设置从“发送注销提醒而不强制用户注销”更改为“通知并强制用户注销”，则新设置将立即生效。
- 如果将设置从“通知并强制用户注销”更改为“发送注销提醒而不强制用户注销”，则新设置要等到计算机下次进入耗尽状态时才会生效。用户仍被强制注销。

分析 **AutoScale** 设置的有效性

February 20, 224

要使用此功能，请启用 **DaaS > 主页 > 预览功能** 中的 **Autoscale Insights** 开关。启用 **Autoscale Insights** 后，可能需要大约 15 分钟才能显示出来。

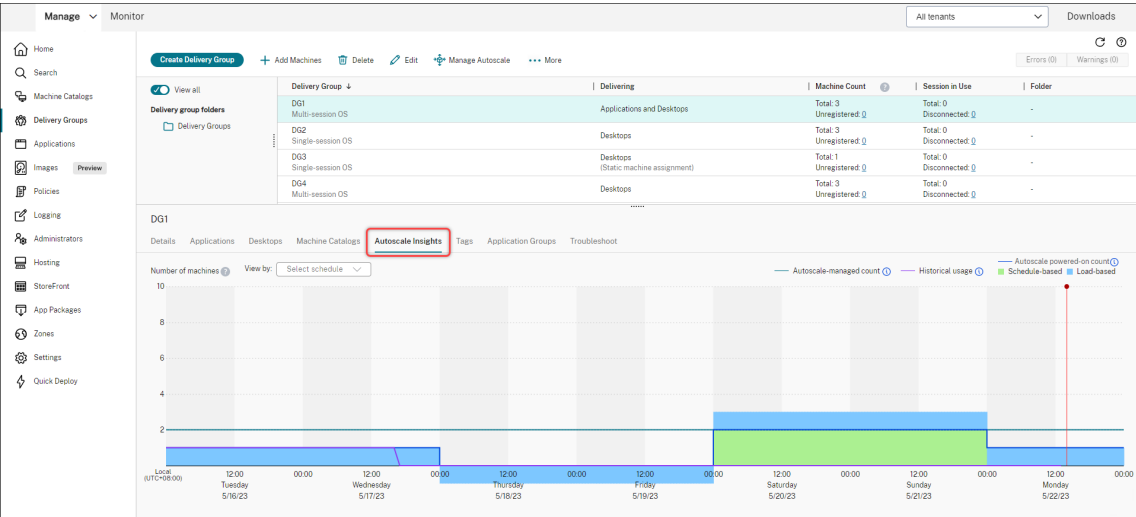
您可以根据前一周的计算机使用情况分析 AutoScale 设置的有效性。通过分析，您可以深入了解 AutoScale 设置的有效性：

- 确定因过度配置而造成的财务浪费。
- 确定用户体验是否因配置不足而受到负面影响。
- 确保配置的容量与计算机的使用情况正确一致。

要实现此目标，请执行以下步骤：

1. 选择启用 AutoScale 功能的交付组。
2. 在底部窗格中，单击 **AutoScale** 见解选项卡。

将出现下图，显示前一周的计算机使用情况数据与基于 AutoScale 设置的要开机的计算机数量之间的比较。



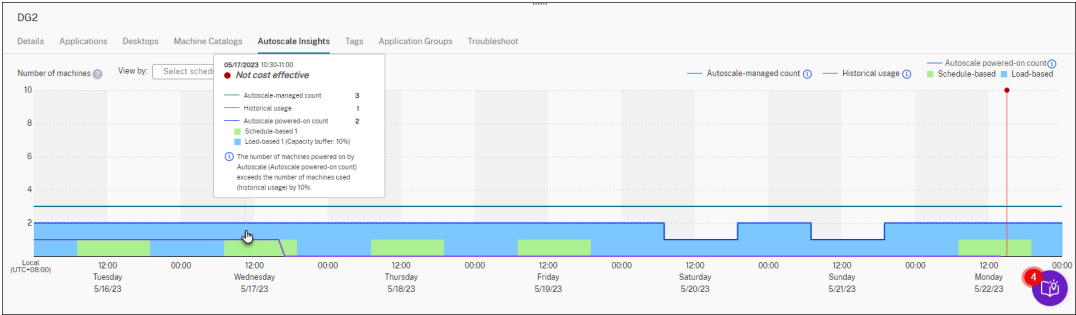
\* 红色垂直线表示当前时间。

下表描述了此图中显示的指标。

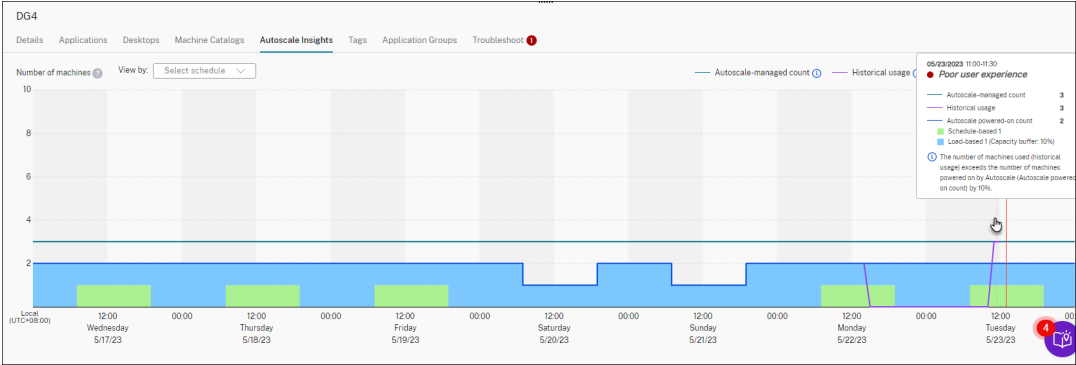
指标	说明
AutoScale 管理的计数	由 AutoScale 管理的计算机总数。AutoScale 管理的计数 = 交付组中的计算机总数—处于维护模式的计算机数量—未标记为 AutoScale 的计算机数量（如果启用了标记的 AutoScale 功能）。
AutoScale 开机次数	由 AutoScale 开启的计算机总数。AutoScale 开机计数 = 基于调度的计算机数量 + 基于负载的计算机数量。
历史使用情况	交付给用户的计算机数量。
基于时间表	根据 AutoScale 基于日程安排的设置开机的计算机数量（注意：基于计划的设置不适用于静态单会话操作系统类型的交付组）。
基于负载	根据基于负载的 AutoScale 设置开机的计算机数量。

3. 要检查特定时段 AutoScale 设置的有效性，请将鼠标悬停在图表上的该时段上。将出现一个信息框，显示比较结果和详细的计算机计数：

- 不具成本效益。历史使用量低于 AutoScale 设置的 90%（开启 AutoScale 的次数）。因此，可能会出现容量浪费。



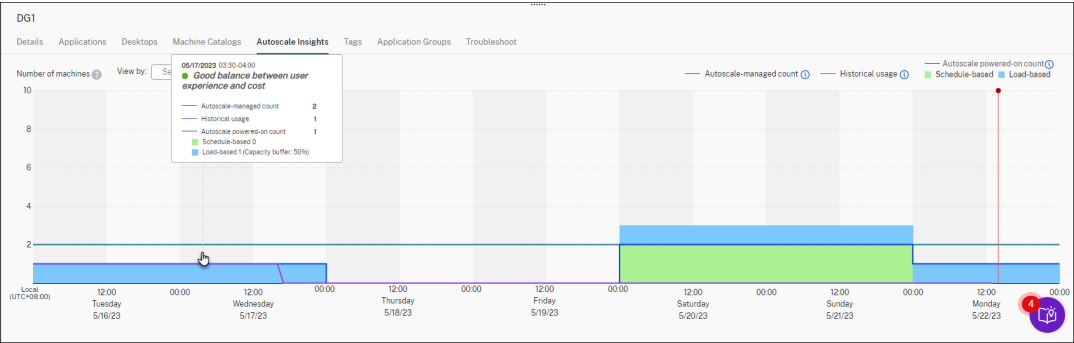
- 用户体验不佳。历史使用量超过 AutoScale 设置的 110%（开启 AutoScale 的次数）。因此，用户等待计算机开机的时间可能会更长。



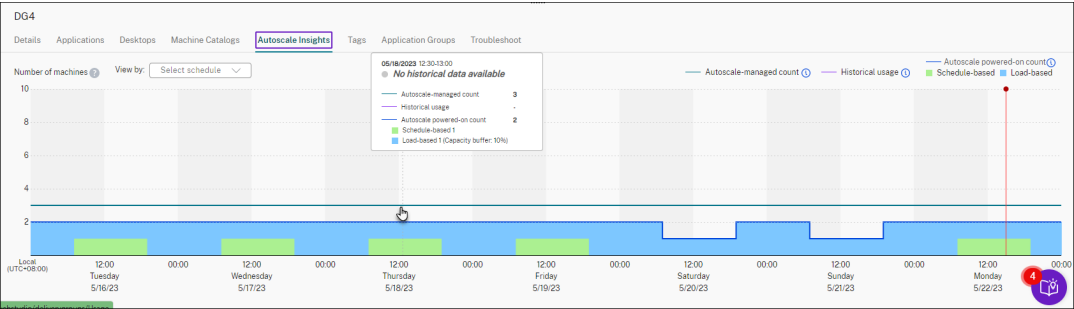
- 在用户体验和成本之间取得良好的平衡。历史使用量和 AutoScale 设置（开启 AutoScale 的次数）之间



的差异小于 10%。AutoScale 设置与历史使用情况保持一致。



- 没有可用的历史数据。没有可用的历史数据。可能的原因包括不到一周前为交付组启用了 AutoScale。



4. 要根据 AutoScale 计划突出显示日期范围，请从“查看依据”字段中选择时间表。
5. 根据您的分析，调整 AutoScale 设置。有关更多信息，请参阅[基于计划和基于负载的设置](#)。

## Broker PowerShell SDK 命令

November 16, 2023

可以使用 Broker PowerShell SDK 为交付组配置 AutoScale。要使用 PowerShell 命令配置 AutoScale，必须使用远程 PowerShell SDK 版本 7.21.0.12 或更高版本。有关远程 PowerShell SDK 的详细信息，请参阅 [SDK](#) 和 [API](#)。

### Set-BrokerDesktopGroup

禁用或启用现有 BrokerDesktopGroup 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/>。

示例

有关如何使用 PowerShell cmdlet 的详细信息，请参阅以下示例：

## 启用 AutoScale

- 假设您希望为名为“MyDesktop”的交付组启用 AutoScale。使用 `Set-BrokerDesktopGroup PowerShell` 命令。例如：

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-AutoscalingEnabled $true
```

## 分别设置高峰和非高峰时段的容量缓冲区

- 假设您希望将容量缓冲区设置为 20%（面向高峰时段），对于名为“MyDesktop”的交付组，将容量缓冲区设置为 10%（面向非高峰时段）。使用 `Set-BrokerDesktopGroup PowerShell` 命令。例如：

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakBufferSizePercent 20 -OffPeakBufferSizePercent 10
```

## 配置断开连接的超时时间设置

- 假设您希望将断开连接的超时时间值设置为 60 分钟（面向高峰时段），对于名为“MyDesktop”的交付组，将断开连接的超时时间设置为 30 分钟（面向非高峰时段）。使用 `Set-BrokerDesktopGroup PowerShell` 命令。例如：

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakDisconnectTimeout 60 -OffPeakDisconnectTimeout 30
```

## 配置注销的超时时间设置

- 假设您希望将注销的超时时间值设置为 60 分钟（面向高峰时段），对于名为“MyDesktop”的交付组，将注销的超时时间设置为 30 分钟（面向非高峰时段）。使用 `Set-BrokerDesktopGroup PowerShell` 命令。例如：

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakLogOffTimeout 60 -OffPeakLogOffTimeout 30
```

## 配置关机延迟设置

- 假设您希望将名为“MyDesktop”的交付组的关机延迟设置为 15 分钟。使用 `Set-BrokerDesktopGroup PowerShell` 命令。例如：

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PowerOffDelay 15
```

## 配置关机延迟不生效的时间段

- 假设您希望将名为“MyDesktop”的交付组的关机延迟设置为在 30 分钟后生效。使用 `Set-BrokerDesktopGroup PowerShell` 命令。例如：

```
- C:\PS> Set-BrokerDesktopGroup "MyDesktop"-SettlementPeriodBeforeAutoShutDown 30。
```

## 配置计算机实例成本设置

- 假设您希望将名为“MyDesktop”的交付组的计算机实例每小时成本设置为 0.2 美元。使用 `Set-BrokerDesktopGroup PowerShell` 命令。例如：

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-MachineCost 0.2
```

## New-BrokerPowerTimeScheme

为交付组创建 BrokerPowerTimeScheme。有关详细信息，请参阅<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/>。

### 示例

假设您要为 UID 值为 3 的交付组创建电源时间方案。新方案涵盖周末、星期一和星期二。上午 8:00 至下午 6:30 这一时间段被定义为方案中包含的日期的高峰时段。对于高峰时段，池大小（保持打开电源的计算机数量）为 20。对于非高峰时段，其大小为 5。可以使用 `Set-BrokerDesktopGroup PowerShell` 命令。例如：

- ```
PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ 5 } else { 20 } } )
```
- ```
PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ $false } else { $true } } )
```
- ```
PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week'-DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48
```

### 动态会话超时参数

通过支持多个新参数，以下 Broker PowerShell SDK cmdlet 已针对动态会话超时进行了扩展：

- Get-BrokerDesktopGroup
- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

这些参数包括：

- **DisconnectPeakIdleSessionAfterSeconds** - 表示空闲会话在高峰时段断开连接的时间（以秒为单位）。此属性的默认值为 0，表示在高峰时段禁用其关联行为。大于 0 的值仅启用交付组在高峰时段的行为。
- **DisconnectOffPeakIdleSessionAfterSeconds** - 表示以秒为单位的时间，在此时间之后，空闲会话在非高峰时段断开连接。此属性的默认值为 0，表示在非高峰期间禁用其关联行为。如果值大于 0，则仅在非高峰时段启用交付组的关联行为。

- **LogoffPeakDisconnectedSessionAfterSeconds** - 表示在高峰时段内断开连接的会话终止的时间（以秒为单位）。此属性的默认值为 0，表示在高峰时段禁用其关联行为。大于 0 的值仅在高峰时段启用交付组的关联行为。
- **LogoffOffPeakDisconnectedSessionAfterSeconds** - 表示在非高峰时段终止断开连接的会话的时间（以秒为单位）。此属性的默认值为 0，表示在非高峰期间禁用其关联行为。如果值大于 0，则仅在非高峰时段启用交付组的关联行为。

#### 示例

假设您想将名为“MyDesktop”的交付组的空闲会话超时设置为高峰时段的 3600 秒。使用 `Set-BrokerDesktopGroup` PowerShell 命令。例如：

```
C:\PS> Set-BrokerDesktopGroup "MyDesktop"-DisconnectOffPeakIdleSessionAfter 3600
```

这样做会断开名为“MyDesktop”的桌面组在非高峰时间空闲超过 1 小时的会话的连接。

## Cloud Health Check

December 9, 2022

#### 注意：

Cloud Health Check 已集成到 Citrix DaaS 中。该集成可作为“完整配置”管理界面中的“运行状况检查”操作提供。有关更多信息，请参阅 [解决 VDA 注册和会话启动问题](#)。

Cloud Health Check 允许您运行检查，以评估站点及其组件的运行状况和可用性。可以针对 Virtual Delivery Agent (VDA)、StoreFront 服务器和 Profile Management 运行运行状况检查。VDA 运行状况检查确定常见 VDA 注册和会话启动问题的可能的原因。

如果检查过程中存在问题，Cloud Health Check 会提供详细报告以及修复问题的操作。每次启动 Cloud Health Check 时，都会检查内容交付网络 (CDN) 中的最新脚本版本，并自动下载这些脚本（如果本地计算机上不存在这些脚本）。Cloud Health Check 始终选择最新的本地脚本版本来运行运行状况检查。

#### 注意：

Cloud Health Check 不会在每次运行时更新。

在 Citrix Cloud 环境中，从加入域的计算机运行 Cloud Health Check，以便在一个或多个 VDA 或 StoreFront 服务器上运行检查。

注意：

您无法在 Cloud Connector 上安装或运行 Cloud Health Check。

Cloud Health Check 应用程序的日志存储在 `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log` 中。可以使用此文件进行故障排除。

查看 Cloud Health Check 的简介。



查看何时使用 Cloud Health Check。



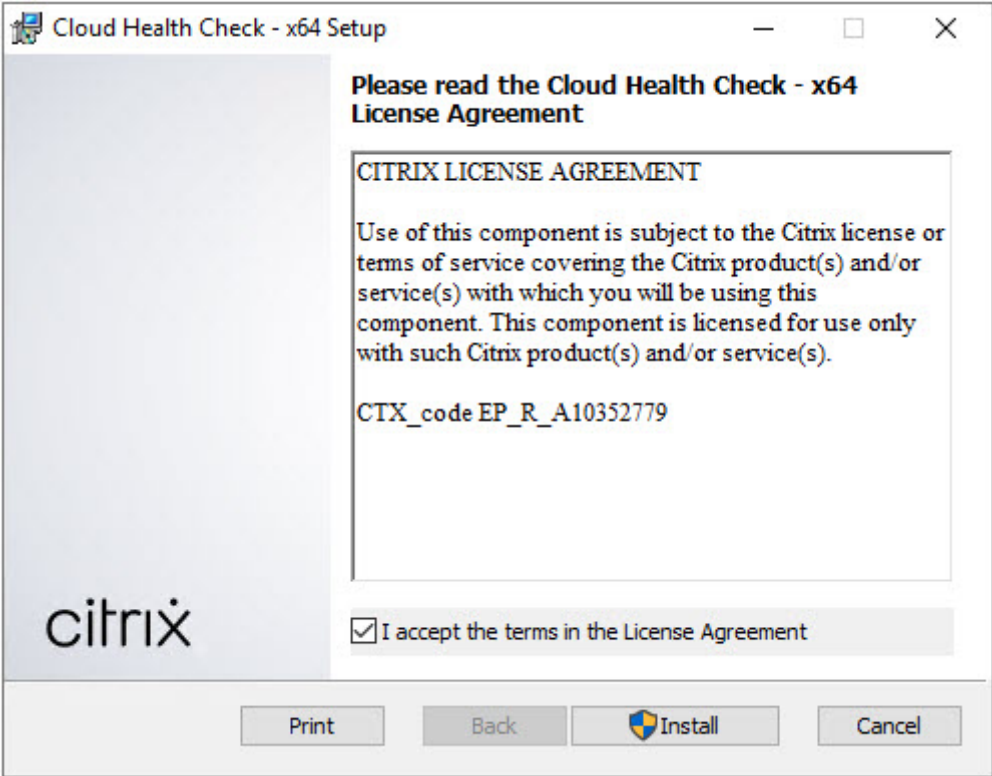
## 安装

您必须拥有加入域的 Windows 计算机，才能准备环境以安装 Cloud Health Check。

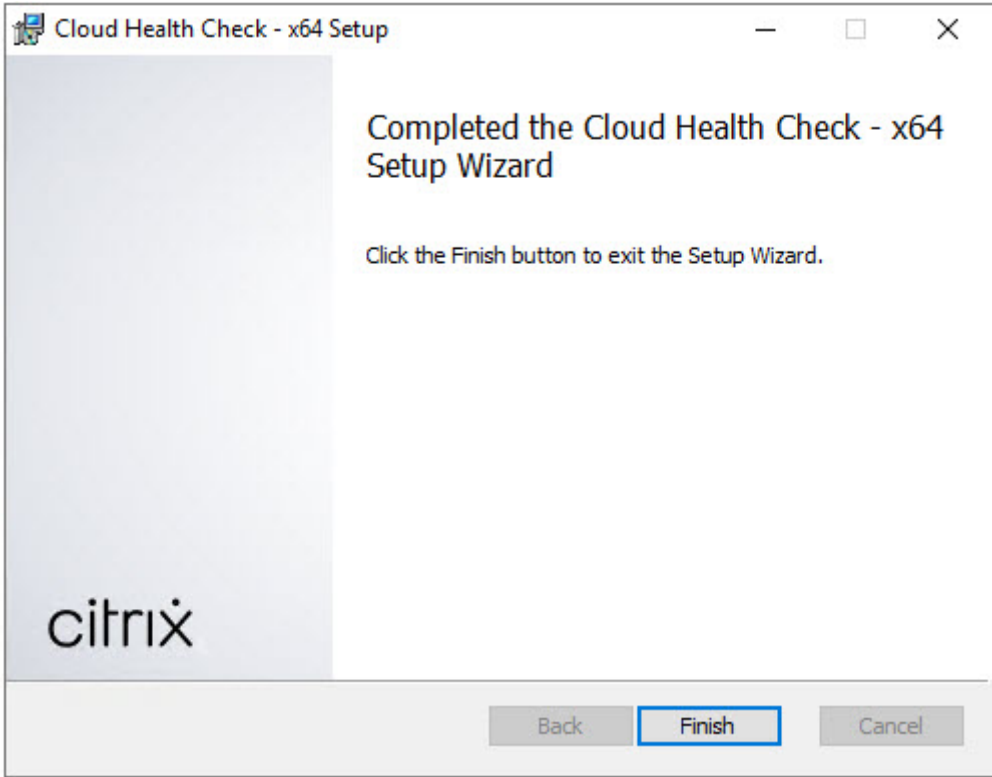
### 注意：

您无法在 Cloud Connector 上安装或运行 Cloud Health Check。

1. 在加入域的计算机上，下载 [Cloud Health Check 安装程序](#)。
2. 双击 CloudHealthCheckInstaller\_x64.msi 文件。
3. 单击框以接受条款。
4. 单击安装。



5. 安装完成后，单击完成。



## 权限和要求

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使用。
- 启动 Cloud Health Check 时，使用以管理员身份运行。

对于每台运行运行状况检查的 VDA 或 StoreFront 计算机：

- 操作系统必须是 64 位。
- Cloud Health Check 必须能够与计算机进行通信。
- 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。
- 必须在计算机上启用 Windows Management Infrastructure (WMI) 访问权限。

## 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。

## VDA 运行状况检查

为在 VDA 上注册，Cloud Health Check 将检查：

- 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
- 与 Controller 进行时间同步
- VDA 注册状态

对于 VDA 上的会话启动，Cloud Health Check 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
- 会话启动注册表设置
- Citrix Universal Injection Driver (CTXUVI) 状态

对于 VDA 上的 Profile Management, Cloud Health Check 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

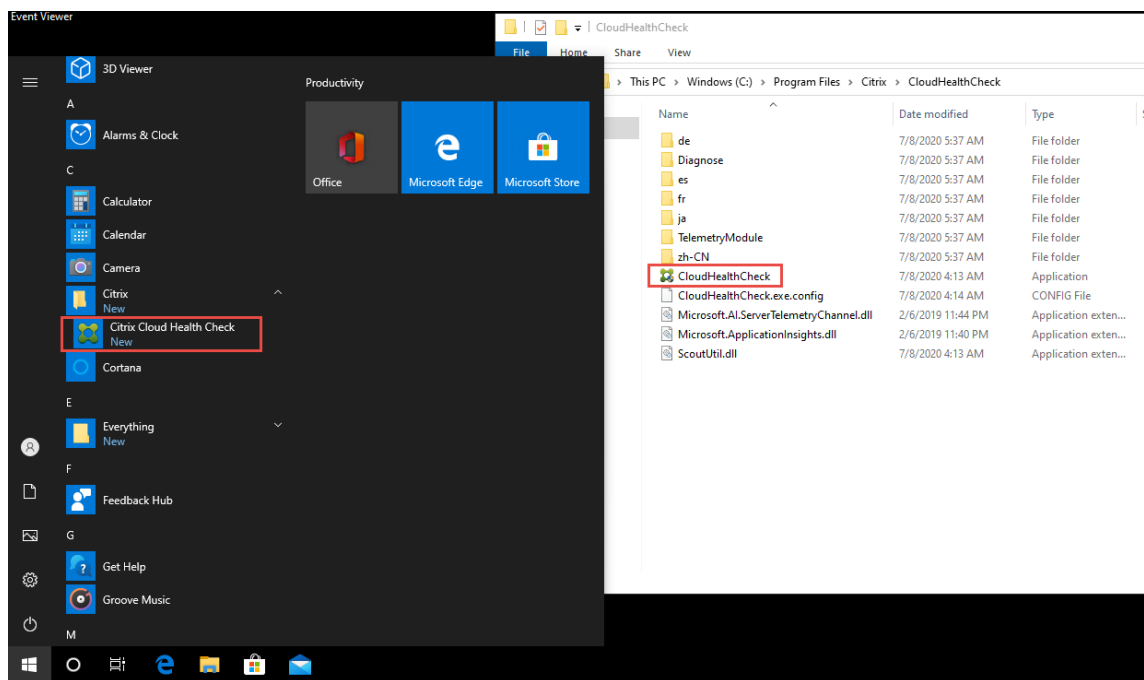
StoreFront 检查将验证是否:

- 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 的连接为端口 88
- 从 StoreFront 服务器到 Active Directory 的连接为端口 389
- 从 StoreFront 服务器到 Active Directory 的连接为端口 464
- 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
- 证书绑定到主机 URL 的 SSL 端口
- 证书链完整
- 证书已过期
- 证书在 30 天内到期

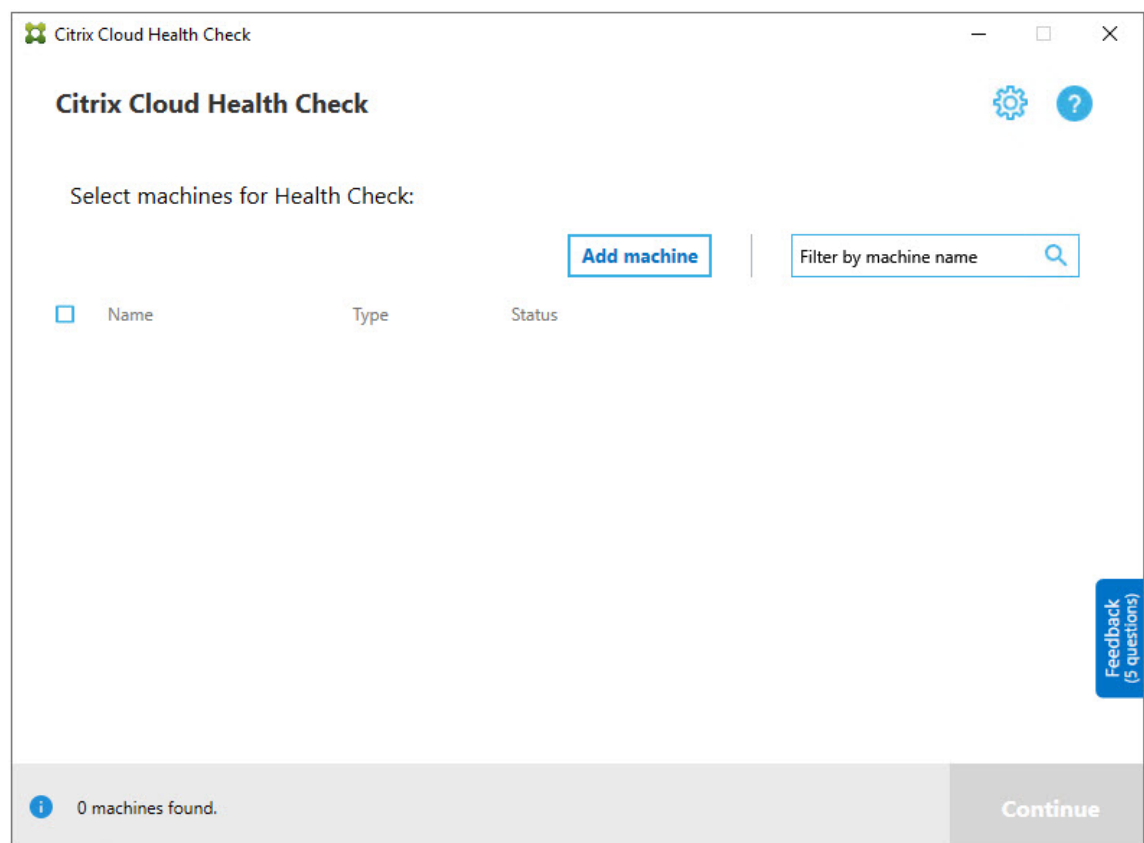
### 运行 Cloud Health Check

要运行 Citrix Cloud Health Check, 请执行以下操作:

1. 从计算机的“开始”菜单中选择 **Citrix > Citrix Cloud Health Check**, 或运行 `C:\Program Files\Citrix\CloudHealthCheck` 中的 `CloudHealthCheck.exe`。

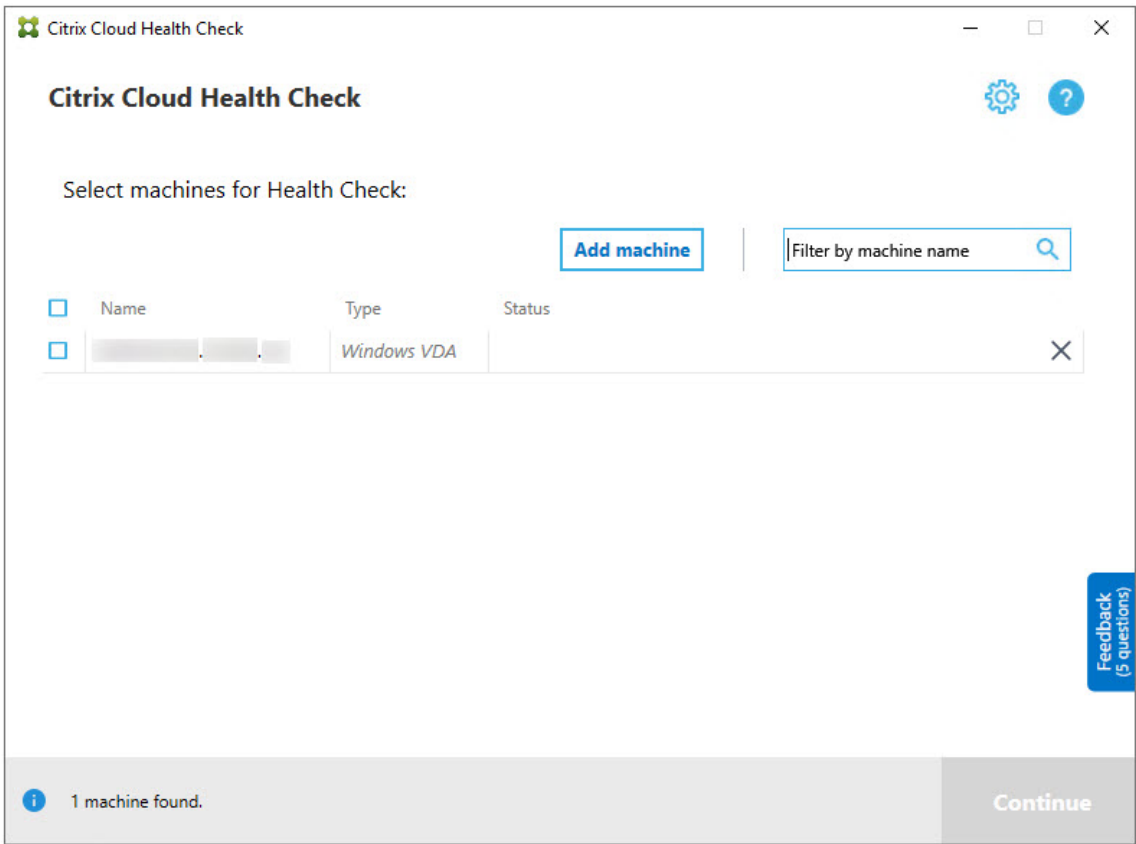


2. 在主 Cloud Health Check 屏幕上，单击添加计算机。



3. 键入要添加的计算机的 FQDN。注意：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。

- 单击 **Continue**（继续）。
- 根据需要重复以上操作以添加其他计算机。



- 要删除手动添加的计算机，请单击行右端的 **X** 并确认删除。重复以上操作以删除其他手动添加的计算机。

Cloud Health Check 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 Cloud Health Check 时，列表顶部仍会列出手动添加的计算机。

### 导入 VDA 计算机

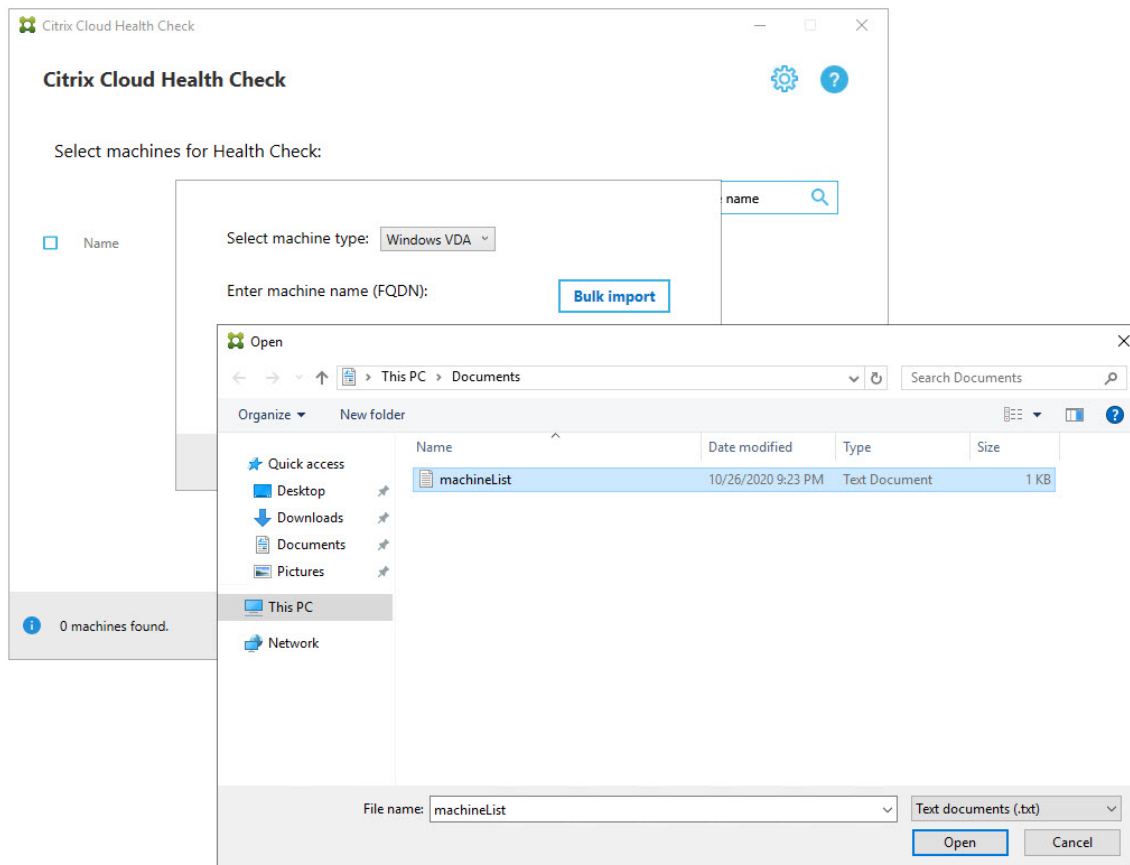
运行运行状况检查时，可以在部署中导入 VDA 计算机。

- 在 Connector 上，使用以下 PowerShell 命令生成计算机列表文件。在 Connector 上，必须输入 Citrix 凭证并在弹出对话框中选择客户。

```
Get-BrokerMachine | foreach { $_.DnsName } | out-file C:\machineList.txt
```

- 将 machineList.txt 文件复制到要在其上运行 Cloud Health Check 的已加入域的计算机。
- 在“Cloud Health Check”页面上，单击添加计算机。
- 选择 Windows VDA 计算机类型。

4. 单击导入 **VDA** 计算机。
5. 选择 machineList.txt 文件。
6. 单击打开。



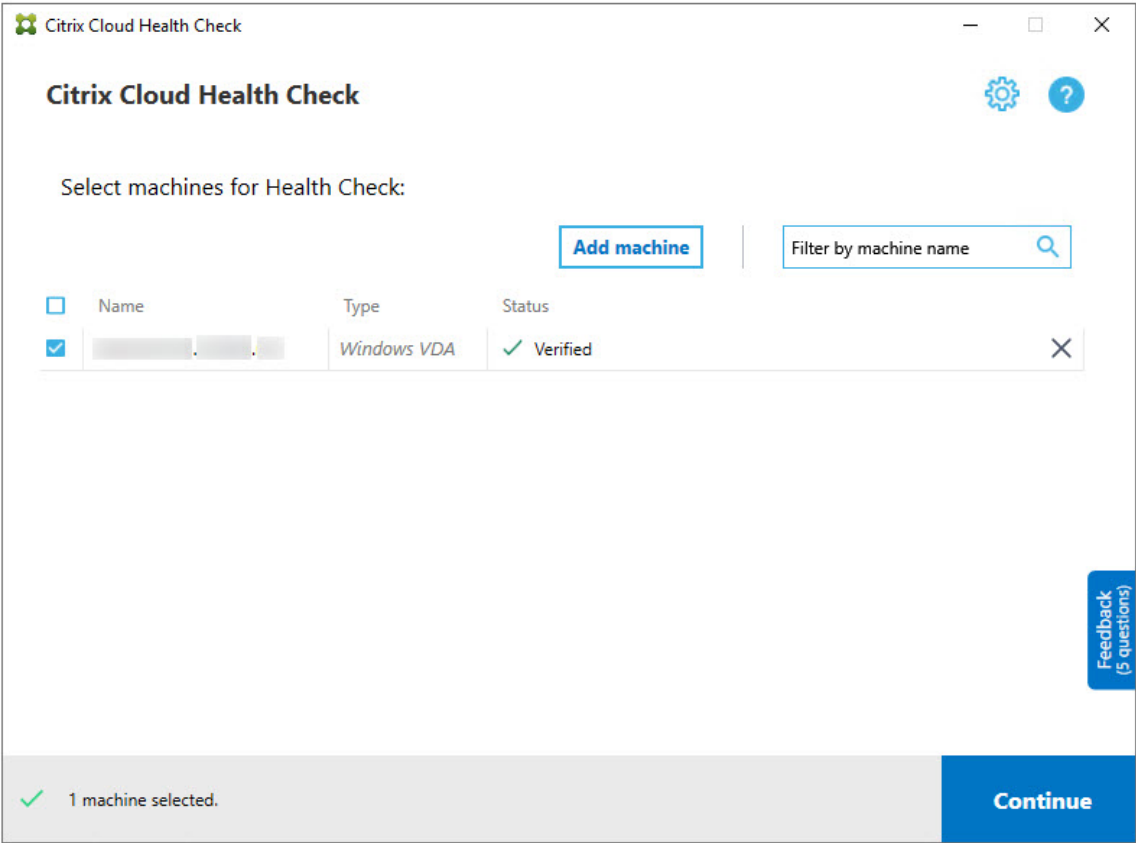
导入的 VDA 计算机将在“Cloud Health Check”页面上列出。

7. 选中要在其上运行运行状况检查的每台计算机旁边的复选框。

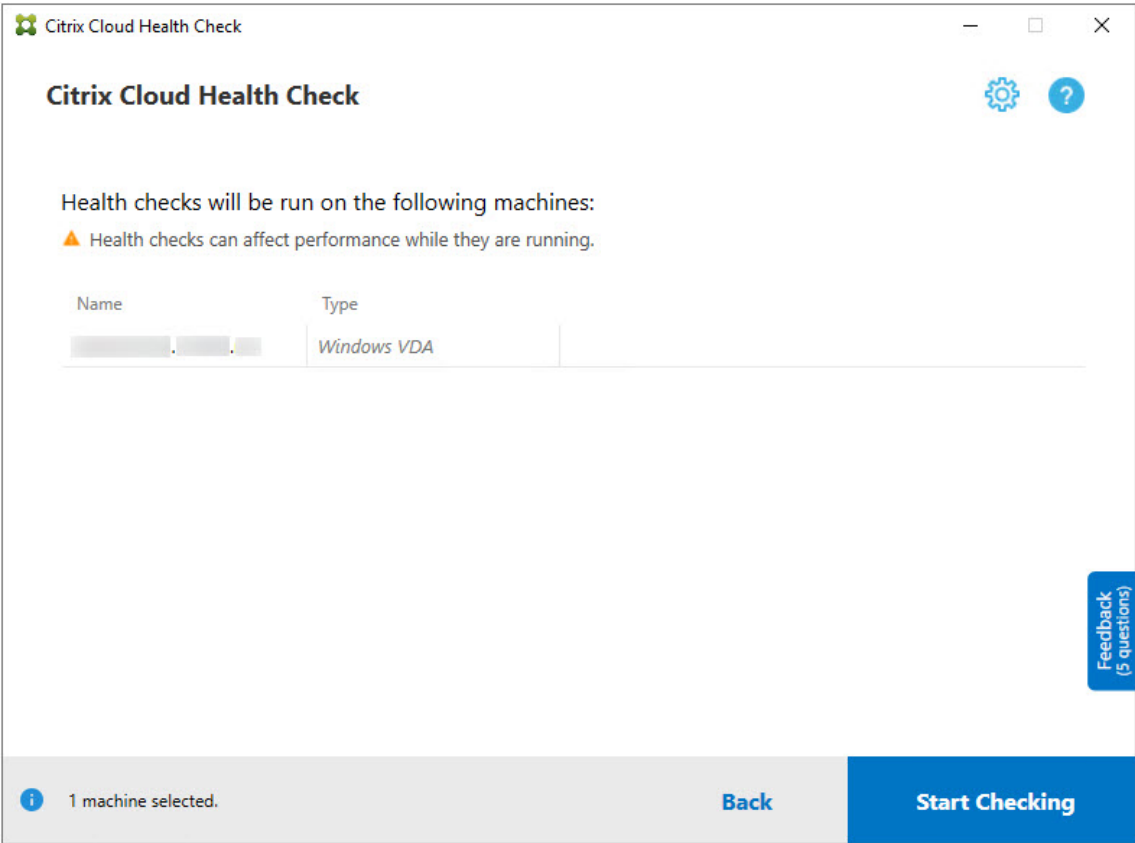
Cloud Health Check 将自动在选择的每台计算机上启动验证测试，以确保计算机满足验证测试中列出的条件。如果验证失败，则 状态 列中会显示一条消息，并且该计算机的复选框将被清除。然后，您可以：

- 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。

8. 验证测试完成后，单击继续。

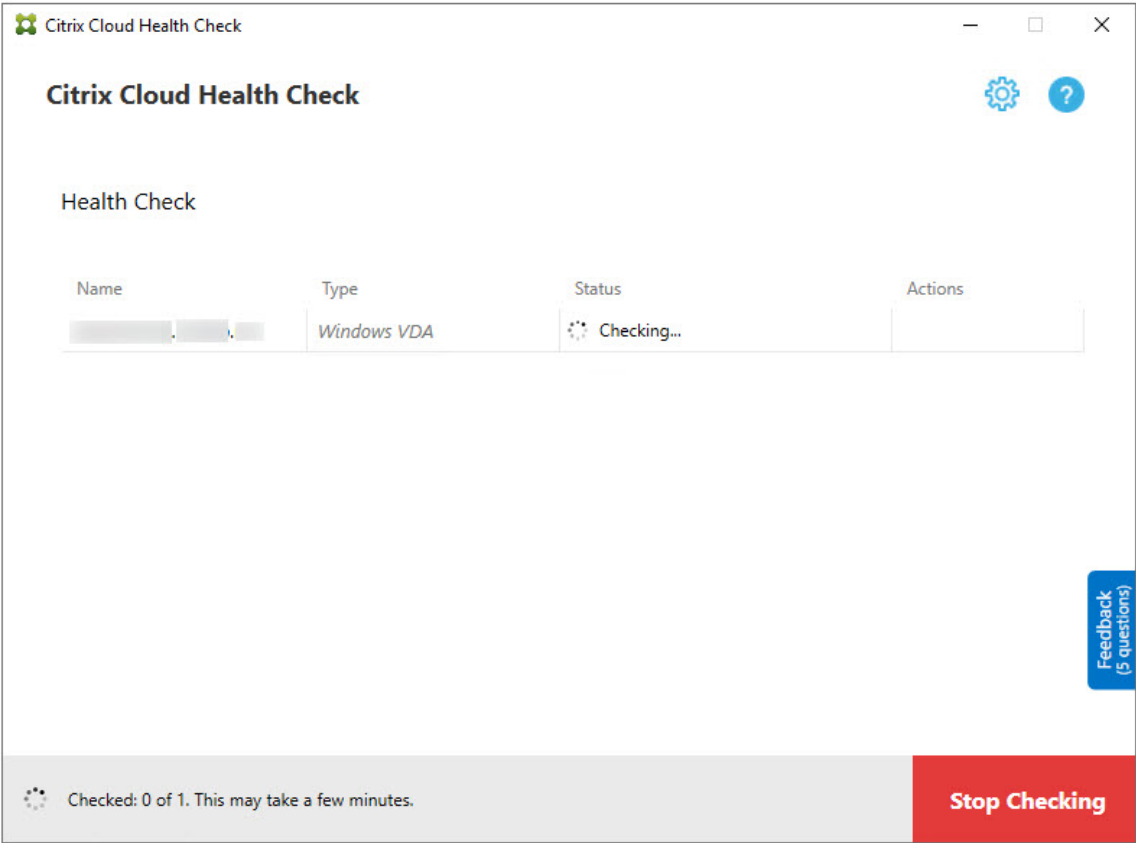


- 9. 在所选计算机上运行运行状况检查。摘要列出了运行测试的所有计算机（您选择的通过验证测试的计算机）。
- 10. 单击开始检查。

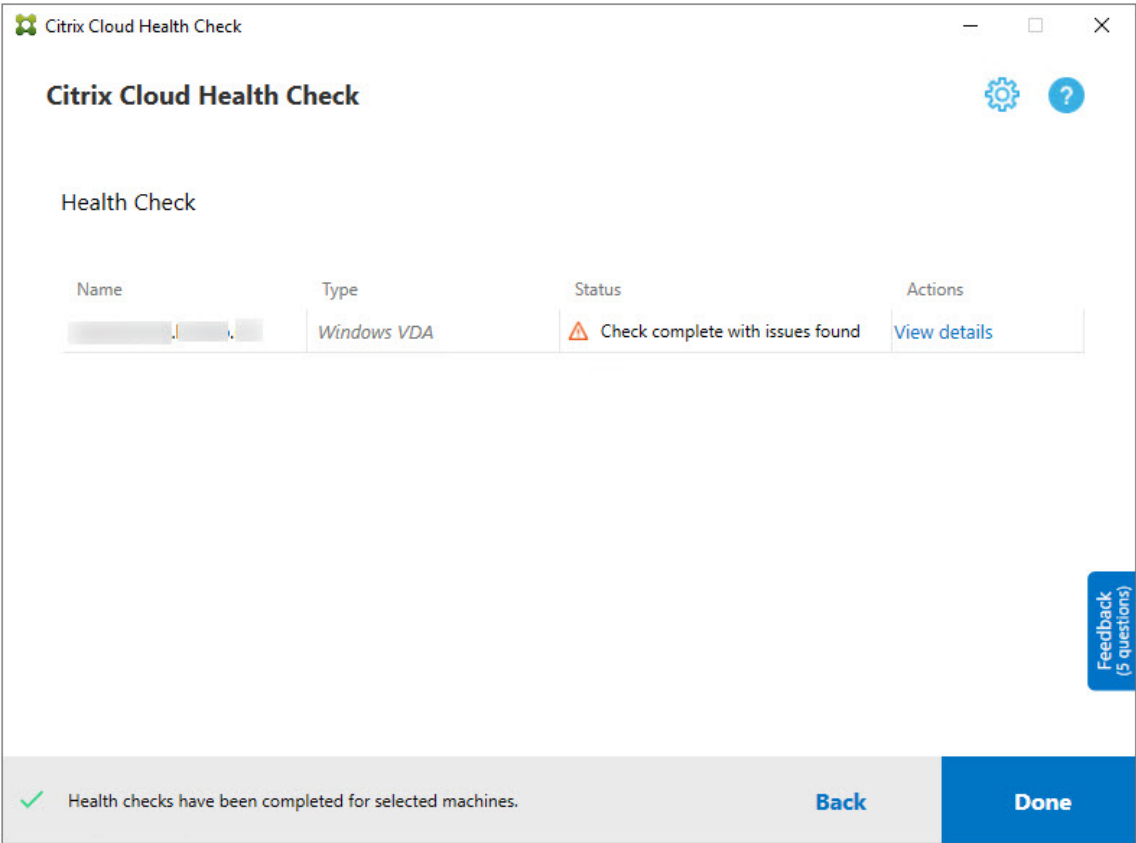


在检查期间和检查之后，状态列将指示计算机的当前检查状态。

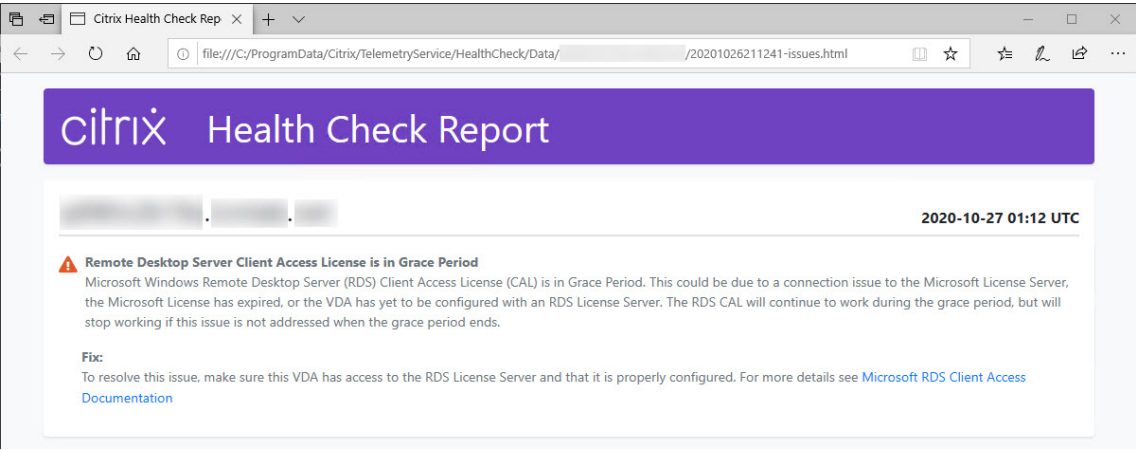
11. 要停止所有正在进行的检查，请单击页面右下角的停止检查。您无法取消单台计算机的运行状况检查，只能取消对所有选定计算机的检查。



12. 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。

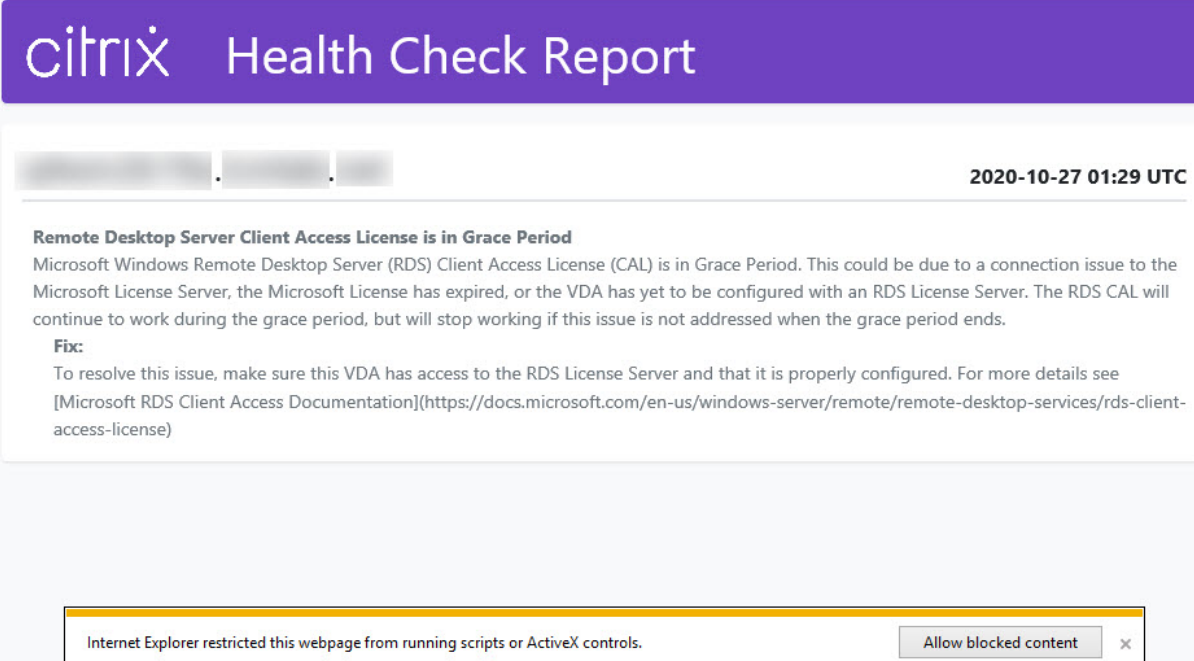


- 如果检查失败，可以在操作列中单击重试。
- 如果检查完成时未发现任何问题，操作列将为空。
- 如果检查发现问题，请单击查看详细信息以查看结果。



如果您使用 Internet Explorer 查看报告，则必须单击允许阻止的内容以显示超链接。





The screenshot shows the Citrix Health Check Report interface. At the top, there's a purple header with the Citrix logo and the title 'Health Check Report'. Below the header, there's a status bar showing '2020-10-27 01:29 UTC'. The main content area displays a warning message: 'Remote Desktop Server Client Access License is in Grace Period'. The message explains that the Microsoft Windows Remote Desktop Server (RDS) Client Access License (CAL) is in Grace Period, which could be due to a connection issue to the Microsoft License Server, the Microsoft License has expired, or the VDA has yet to be configured with an RDS License Server. The RDS CAL will continue to work during the grace period, but will stop working if this issue is not addressed when the grace period ends. A 'Fix:' section provides instructions to resolve the issue by ensuring the VDA has access to the RDS License Server and is properly configured, with a link to Microsoft RDS Client Access Documentation. At the bottom of the screenshot, there's a yellow warning bar from Internet Explorer stating 'Internet Explorer restricted this webpage from running scripts or ActiveX controls.' with an 'Allow blocked content' button.

**citrix Health Check Report**

2020-10-27 01:29 UTC

**Remote Desktop Server Client Access License is in Grace Period**

Microsoft Windows Remote Desktop Server (RDS) Client Access License (CAL) is in Grace Period. This could be due to a connection issue to the Microsoft License Server, the Microsoft License has expired, or the VDA has yet to be configured with an RDS License Server. The RDS CAL will continue to work during the grace period, but will stop working if this issue is not addressed when the grace period ends.

**Fix:**

To resolve this issue, make sure this VDA has access to the RDS License Server and that it is properly configured. For more details see [Microsoft RDS Client Access Documentation](https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-client-access-license)

Internet Explorer restricted this webpage from running scripts or ActiveX controls. [Allow blocked content](#)

完成所有选定计算机的检查后，单击上一步将导致您丢失检查结果。

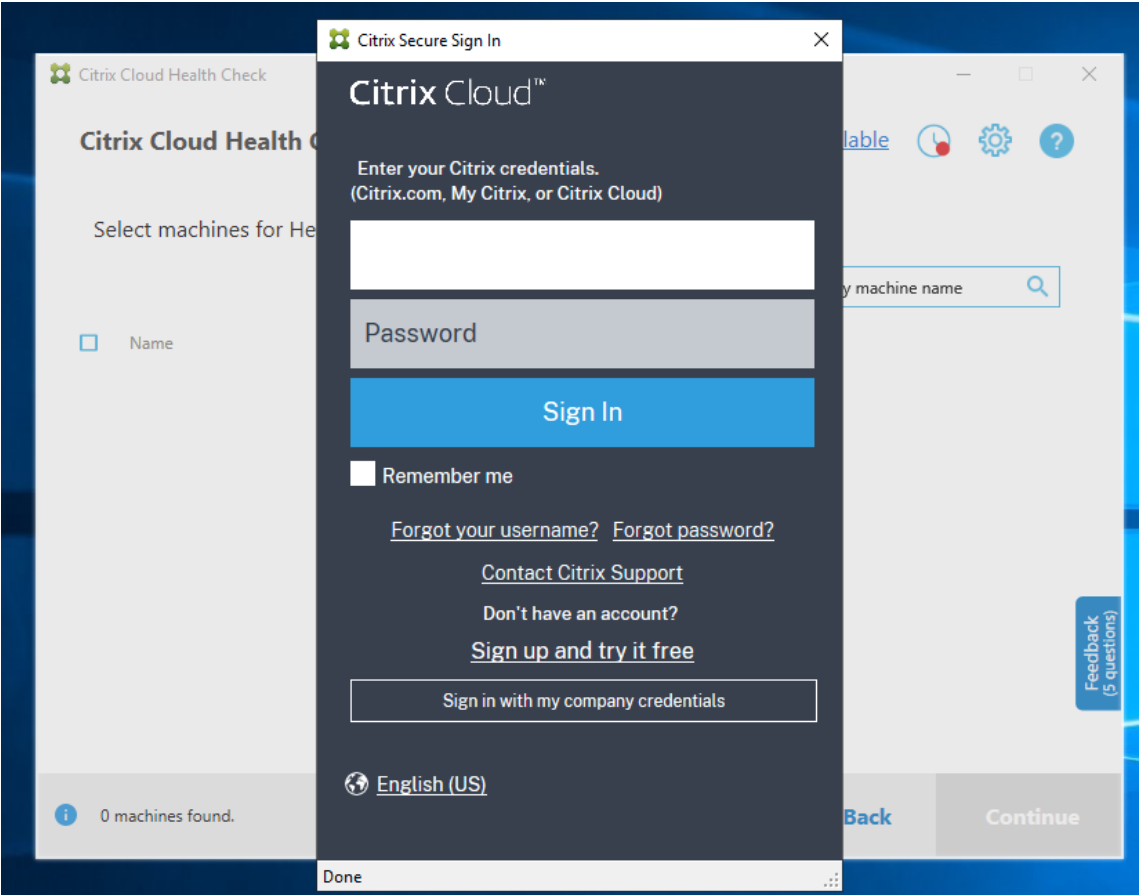
检查完成后，单击完成返回到 Cloud Health Check 主屏幕。

## 检索 VDA 计算机

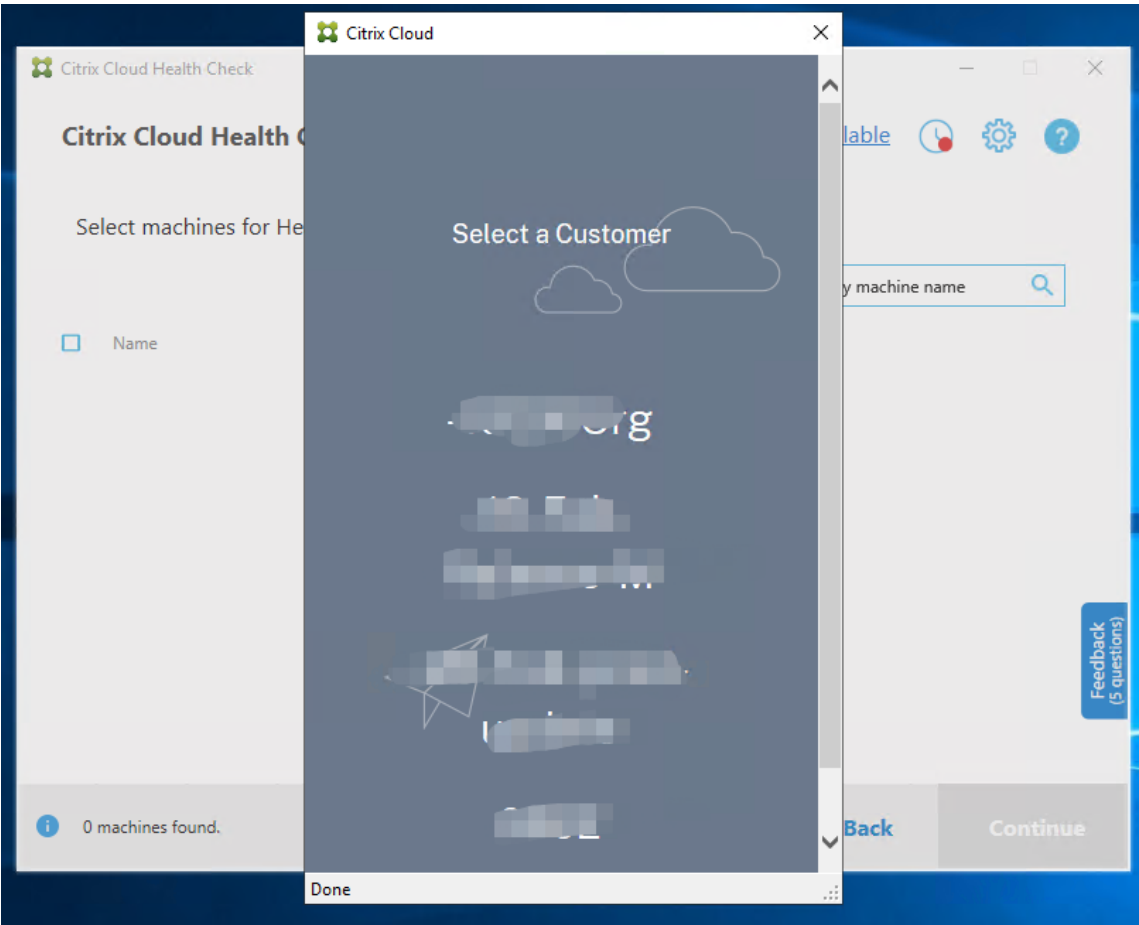
Cloud Health Check 可以自动检测和检索 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）部署中的 VDA。

要检索您的 VDA，请执行以下操作：

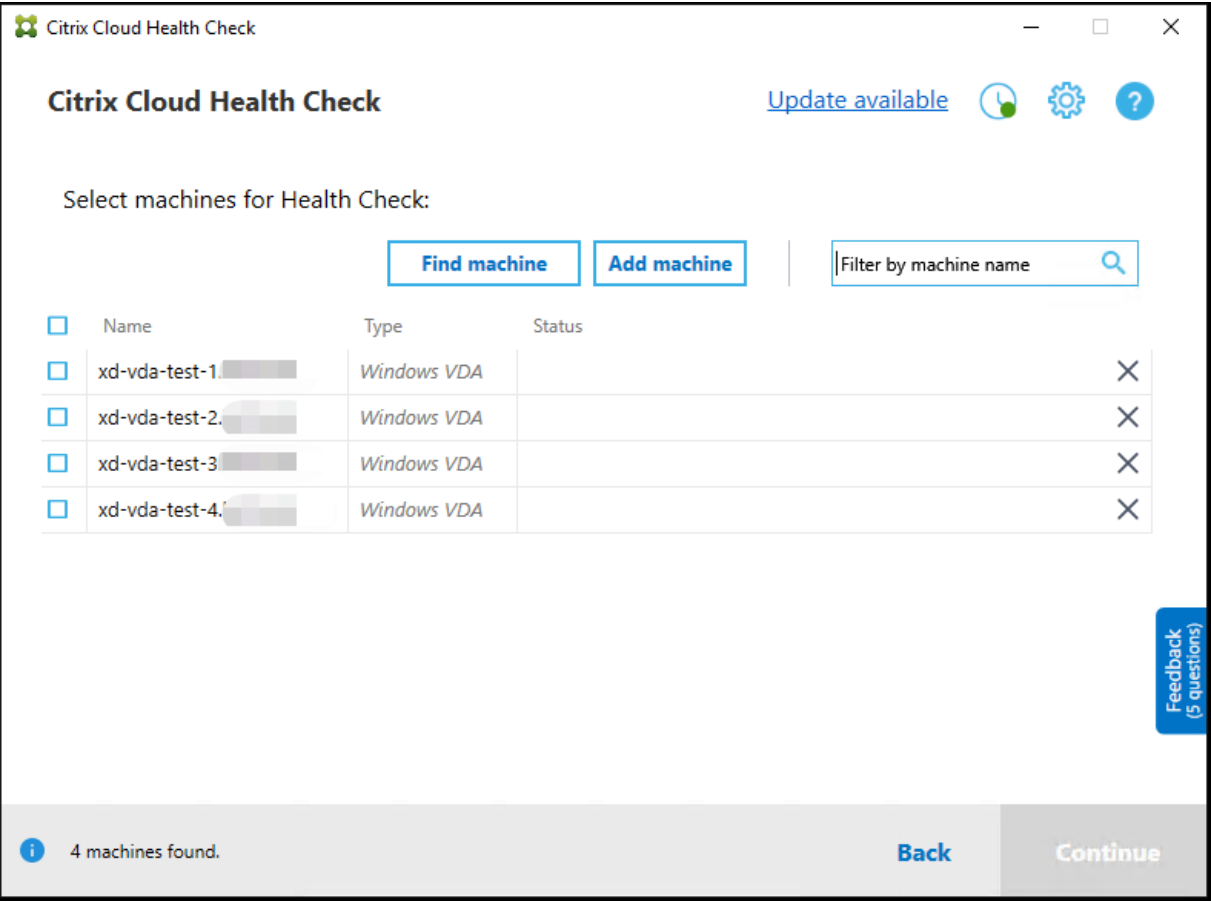
1. 准备一台与运行 Cloud Health Check 的计算机加入同一域林的新计算机。
2. 打开 Cloud Health Check，然后单击 **Find machine**（查找计算机）以登录 Citrix Cloud。



3. 选择具有要检索的云站点的客户。



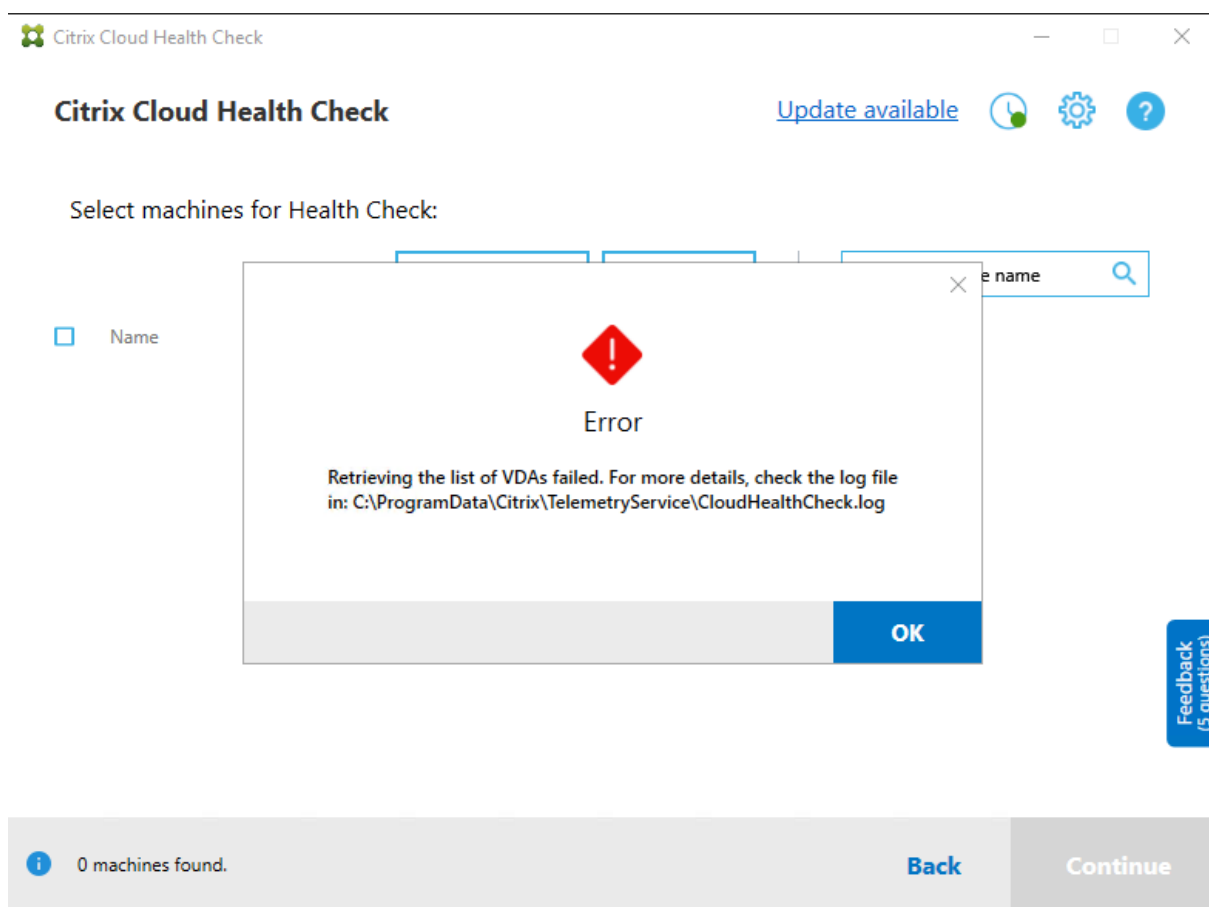
VDA 列表将显示在 Cloud Health Check 中。该列表还保存在 `\ProgramData\Citrix\TelemetryService\ChcDiscovery\ChcDiscoveredMachineList.json` 下的本地文件中。



重新打开 Cloud Health Check 时，计算机列表将加载本地缓存。如果在部署中进行了任何更新，则必须单击查找计算机以刷新计算机列表。

注意：

- Cloud Health Check 仅在运行 Cloud Health Check 的计算机位于同一域林中查找计算机。
- Citrix Cloud 会话将在一小时后过期。一小时后，您必须再次单击查找计算机以获取最新的 VDA 列表。
- 如果检索 VDA 列表失败，则会弹出错误消息。可以查看 `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log` 中的详细信息。



## 运行状况检查结果

生成报告的运行状况检查包含以下元素：

- 生成结果报告的时间和日期
- 已检查的计算机的 FQDN
- 在目标计算机上检查的条件

## 在命令行中运行 **Cloud Health Check**

Cloud Health Check 可以在命令行中运行，以帮助客户执行运行状况检查。您必须是运行 Cloud Health Check 的计算机上的管理员，才能在命令行中使用 Cloud Health Check。

注意：

在命令行中使用 Cloud Health Check 时，一次只能检查一台计算机。只能在目标计算机上同时运行的 **CloudHealthCheck.exe** 一个实例。如果要检查多台计算机，则必须逐个检查这些计算机，方法是将 cmdlet 封装在 cmdlet/PowerShell 脚本中的循环中。还必须关闭任何打开的 Cloud Health Check UI 实例。

## cmdlet

支持的命令行 cmdlet 包括：

- **MachineFQDN** - 此 cmdlet 具有强制性。这是目标计算机的完全限定域名。
- **MachineType** - 此 cmdlet 是可选的。cmdlet 值可以是 Windows VDA（默认值）或 StoreFront。
- **ReportName** - 此 cmdlet 是可选的。cmdlet 值必须是 Windows 上的有效文件名。默认值为 **HealthCheckReport**。
- **SkipAdminCheck** - 此 cmdlet 是可选的。可以添加此选项以跳过需要管理员权限的检查。
- **UpdateScripts** - 此 cmdlet 是可选的。可以添加此选项以更新来自 CDN 服务器的检查脚本。
- **DisableCeip** - 如果在用户界面上启用了 CEIP，则此 cmdlet 是可选的，请添加以禁用 CEIP。
- **Help** - 显示有关参数的帮助信息。

示例：

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local
```

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local -ReportName  
checkreport
```

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local -SkipAdminCheck
```

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local -UpdateScripts
```

```
HealthCheckCLI.exe -MachineFQDN machine1.domain.local,machine2.domain  
.local,machine3.domain.local
```

```
HealthCheckCLI.exe -Help
```

注意：

参数名称不区分大小写。

默认情况下，控制台输出不会显示在命令行控制台窗口中。可以通过将 `|more` 附加到 cmdlet 手动显示输出。

示例：`HealthCheckCLI.exe -MachineFQDN machine.domain.local|more`

命令行默认需要管理员权限才能运行。添加参数 `-SkipAdminCheck` 以替代对管理员权限的需求。

## 退出代码

退出代码解释了命令行中的 Cloud Health Check 检查结果。必须在 cmdlet 之前添加 `start /wait`，才能获取退出代码。

示例：`start /wait HealthCheckCLI.exe -MachineFQDN machine.domain.local`

退出代码为：

- 0 - 正常，检查已完成并通过。
- 1 - 失败，检查已完成，但出现问题。
- 2 - 错误，检查未完成并出现错误。

还可以使用 `cmdlet echo %errorlevel%` 获取上次运行命令的退出代码。

## 报告

Cloud Health Check 为目标计算机创建包含 `HealthCheckDataFolder` 中的计算机名称的文件夹。在安装 Cloud Health Check 的计算机上创建.html 文件和.json 文件。运行状况检查报告位于 `%ProgramData%\Citrix\TelemetryService\HealthCheck\Data` 中的 `HealthCheckDataFolder` 中。

仅当目标计算机上存在问题时才会创建报告。

### 注意：

如果指定的报告名称存在，则会覆盖报告文件。

警报和基本信息存储在.json 报告中。

```

JSON
{
  "version": 1,
  "id": "9547e4ae-022c-4d36-b3a6-77ee61aa72cd",
  "siteId": "00000000-0000-0000-0000-000000000000",
  "generatedTime": "2020-09-08T06:53:25Z",
  "machineReports": [
    {
      "start": 0,
      "startTime": "2020-09-08T02:53:13.000Z",
      "endTime": "2020-09-08T02:53:23.000Z",
      "fqdn": "machine.domain.local",
      "machineType": "VDA",
      "alerts": [
        {
          "start": 0,
          "issueKey": "citrix.vda.network.registration-port-unreachable",
          "issueUuid": "a3547960-fdad-4594-96bd-ebf9c0af7f4a",
          "fixRecommendation": "To resolve this issue, see [CTX227516](https://support.citrix.com/article/CTX227516)",
          "severity": "error",
          "issueName": "Invalid Windows Firewall configuration",
          "issueDescription": "The following Windows Firewall rules are not enabled on the VDA: * Inbound agent connections on TCP port 80 * Outbound Broker connections on TCP port 80 (default) <br>",
          "tags": null,
          "checkNames": [
            {
              "start": 0,
              "name": "VDA Health Check",
              "htmlFix": "Fix:"
            }
          ]
        }
      ]
    }
  ],
  "htmlReportName": "Health Check Report"
}

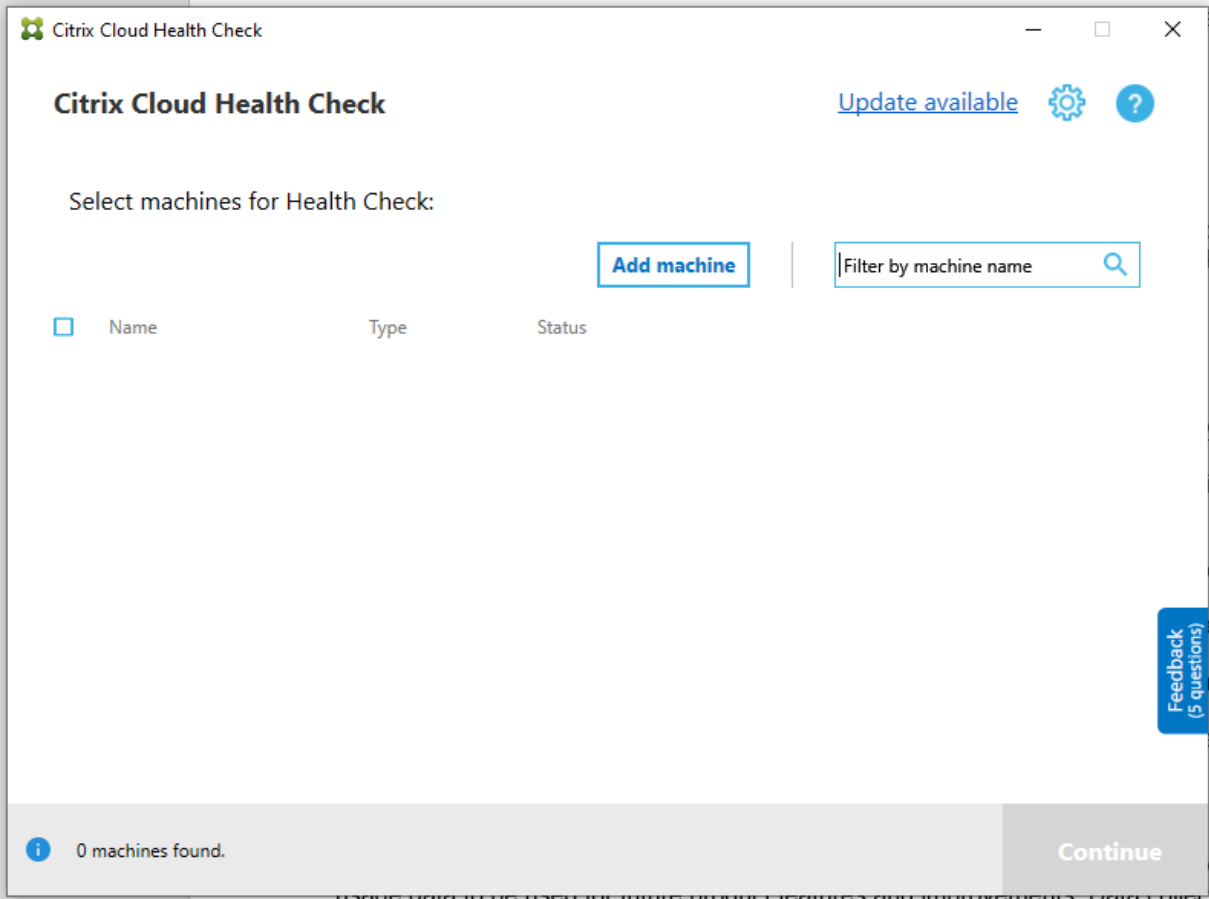
```

报告代码为：

- **issueKey**：问题的纯文本描述。
- **issueUuid**：问题的唯一标识字符串。
- **fixRecommendation**：问题的修复建议。
- **severity**：指示是否必须修复此问题。错误可能指示组件（VDA 或 StoreFront）出现故障，警告指示该组件可以运行，但可能存在一些潜在问题。
- **issueName**：问题的标题。
- **issueDescription**：问题的详细描述。

更新 **Cloud Health Check**

如果有新版本的 Cloud Health Check 可用，“Cloud Health Check”窗口的右上角将显示“有可用更新”链接。单击该链接可转至 Citrix 下载页面以获取新版本。



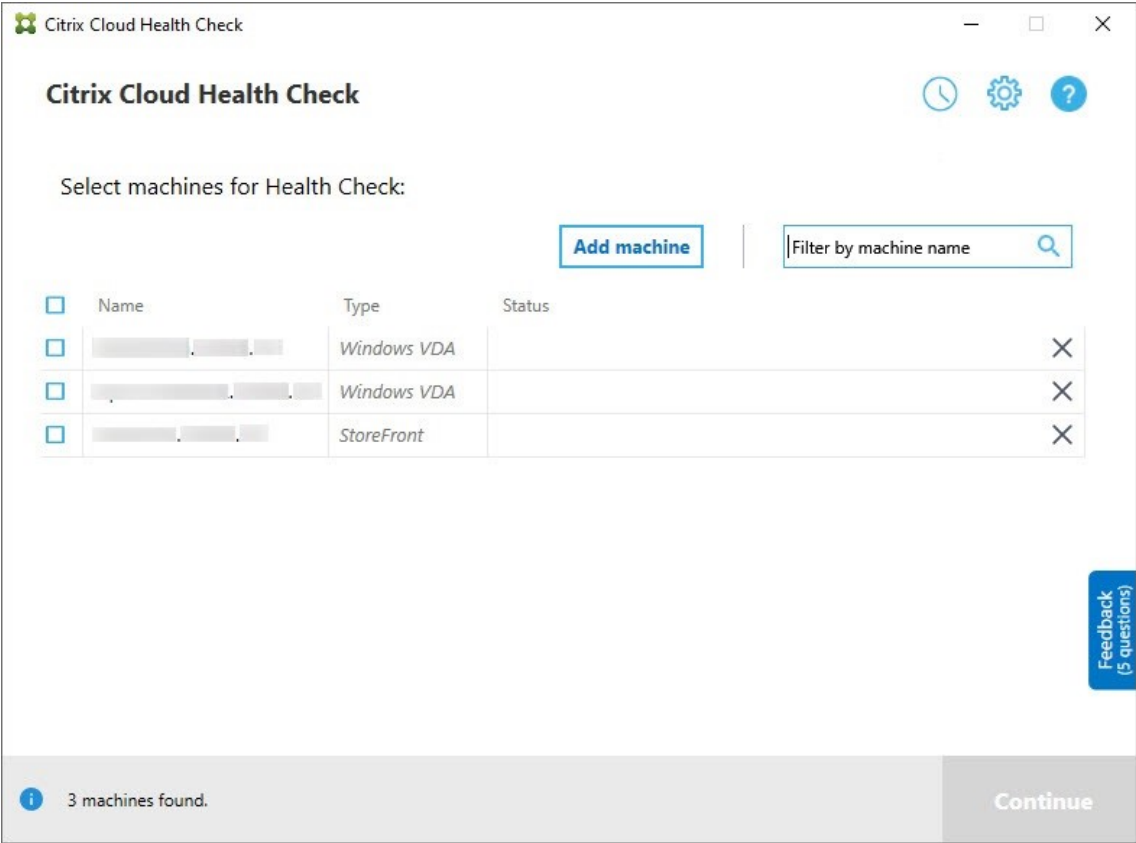
**Cloud Health Check** 计划程序

使用 Cloud Health Check 计划程序定期执行运行状况检查。

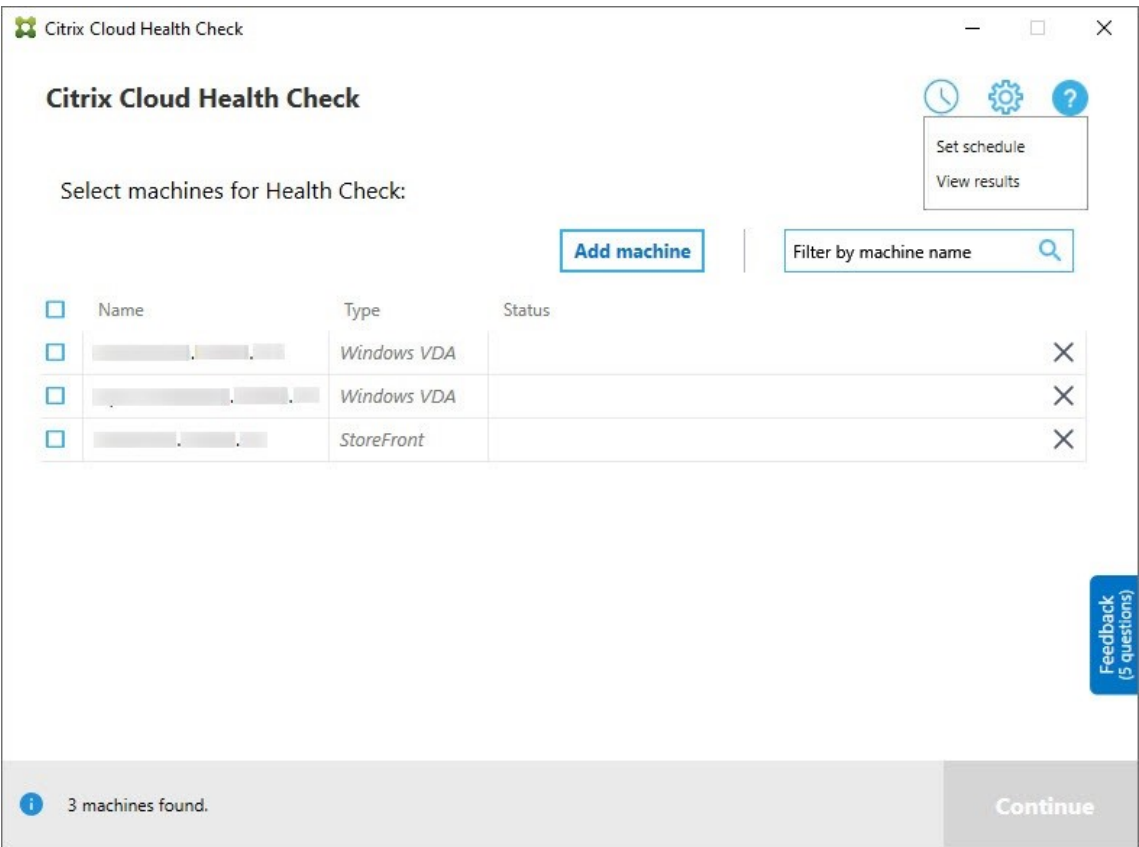
设置时间表

1. 单击 Cloud Health Check 主窗口中的 **Add machine**（添加计算机）以添加要对其运行定期检查的计算机。





2. 单击时钟图标，然后单击设置计划。



3. 选择计划的时间，然后单击下一步。通过选中每隔以下时间重复执行一次任务复选框，可以将任务设置为重复执行。
4. 选择将结果输出到 Windows 事件日志。可以将任务设置为将结果写入 Windows 事件日志。
5. 选择在计划的检查完成后触发自定义 PowerShell 脚本，然后单击下一步。
  - 如果需要，请单击编辑在 Windows PowerShell ISE 中编辑脚本内容。
  - 单击定位以打开文件位置，然后使用其他编辑器打开文件以编辑脚本。
  - 单击重置将脚本重置为其原始设置。

注意：

- 不能更改脚本的脚本名称和路径。
- 可以使用 ChcShceduledTrigger.ps1 脚本实现自定义操作，例如在计划的检查报告准备就绪后发送电子邮件。将以下代码添加到脚本末尾。自定义代码以添加正确的电子邮件帐户和 SMTP 服务器地址。使用运行计划任务的帐户的凭据发送电子邮件通知。

```
1 #Sending email example code:
2 $body = "CreatedTime: $($report.CreatedTime)"
3 $body = $body + "`nStatusCode: $($report.StatusCode)"
4 $body = $body + "`nMachineCount: $($report.MachineReports.Count)"
5 $from = "mock_email_accout"
```

```
6 $to = "mock_email_accout"  
7 $smtpServer = "mock_smtp_server"  
8  
9 Send-MailMessage -Subject "Citrix Cloud Health Check Scheduler  
    Report" -Body $body -From $from -To $to -SmtpServer $smtpServer  
10 <!--NeedCopy-->
```

**Set schedule**

**Schedule**

Select time for your schedule

Frequency

☒ Daily ☐ Off

Time ☐ Repeat task every

03:00  hours

Select post result settings for your schedule

☒ Output results to Windows Event Log ⓘ

☐ Trigger PowerShell script after the completed check ⓘ

C:\ProgramData\Citrix\TelemetryService\ChcSchedule\ChcScheduledTrigger.ps1

6. 为您的计划选择计算机，然后单击下一步。

Set schedule

Schedule

Select Machines

Credentials

Select machines for your schedule

Select machines you added on home page.

Filter by machine name

| <input checked="" type="checkbox"/> | Name | Type        |
|-------------------------------------|------|-------------|
| <input checked="" type="checkbox"/> |      | Windows VDA |
| <input checked="" type="checkbox"/> |      | Windows VDA |
| <input checked="" type="checkbox"/> |      | StoreFront  |

Back

Next

Cancel

7. 输入运行任务的帐户的凭据，然后单击完成。

Set schedule

Schedule

Select Machines

Credentials

Enter user account information for this task

Input the credentials of the account that the health check schedule task runs. Credentials are required to run the task when the account is not logged in. Credentials are stored by Windows Task Scheduler.

Username:

Password:

\*\*\*\*\*

Back

Finish

Cancel

8. 在 Windows 任务计划程序中创建了 CloudHealthCheckScheduler 任务。

GeneralTriggersActionsConditionsSettingsHistory

Name:CloudHealthCheckScheduler

Location:\

Author:

Description:This task is created by Citrix Cloud Health Check, any change to this task will be lost after the next edit by the tool.

Security options

When running the task, use the following user account:

chaom

☐ Run only when user is logged on

☒ Run whether user is logged on or not

☐ Do not store password. The task will only have access to local resources

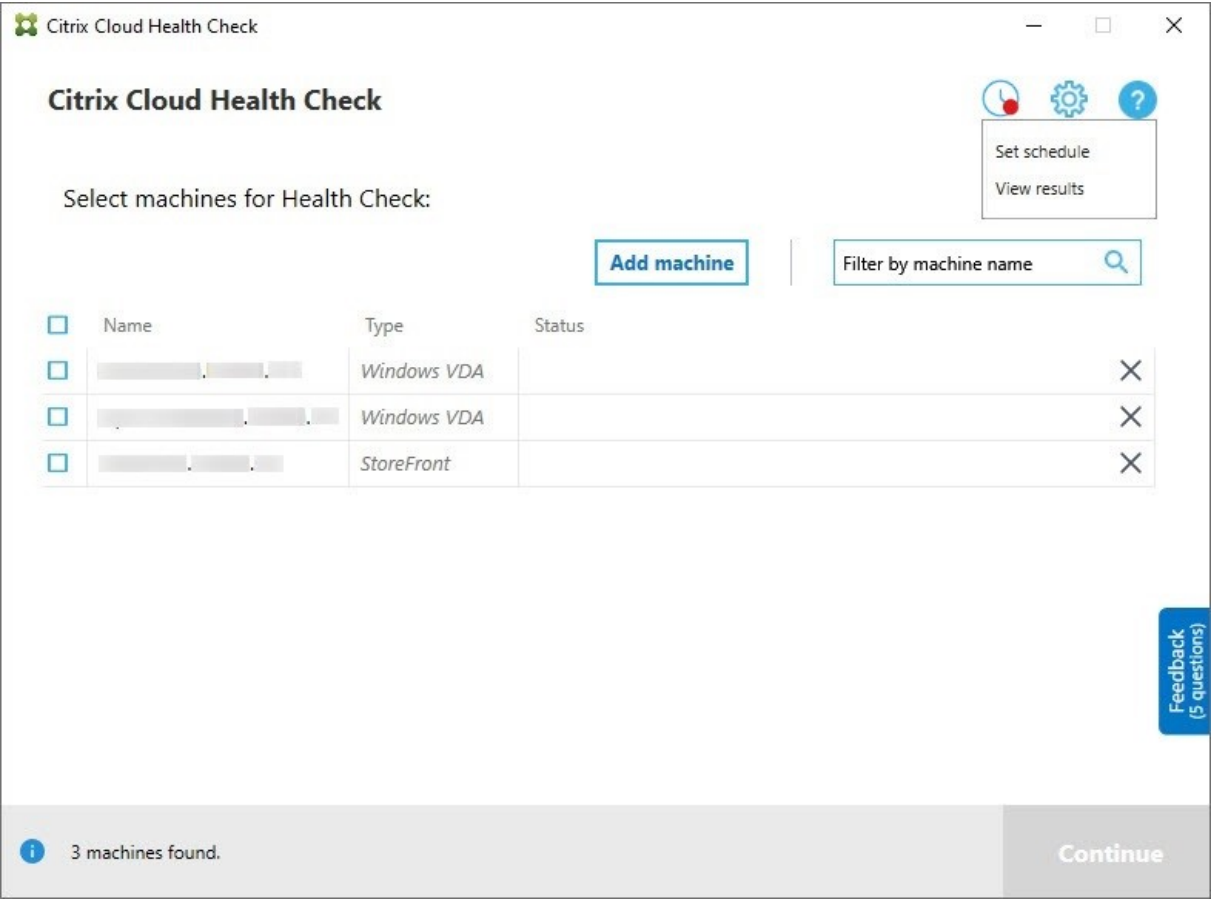
☒ Run with highest privileges

☐ Hidden

Configure for:Windows Vista™, Windows Server™ 2008



查看计划结果


带红点的时钟图标指示在上次检查中发现了问题。要查看结果，请单击时钟图标，然后单击查看结果。



“计划报告” 页面显示所有计划运行状况检查任务的结果。单击查看报告可查看每个计划的报告。

Schedule Reports

| Report Time          | Report Status                                                                                                  | Actions                     |
|----------------------|----------------------------------------------------------------------------------------------------------------|-----------------------------|
| 2021-07-29 09:49 UTC |  Check complete, issues found | <a href="#">View Report</a> |
| 2021-07-29 09:41 UTC |  Check complete, issues found | <a href="#">View Report</a> |


 2 reports generated.

Close

html 报告列出了每个计划的整体报告。下面是该报告的一个示例：


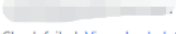
Citrix Health Check Rep


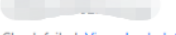
file:///C:/ProgramData/Citrix/TelemetryService/ChcSchedule/report/ChcScheduledChecks\_2021-04-27-143511-108.html


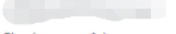
 Health Check Report

Health Check Schedule Report

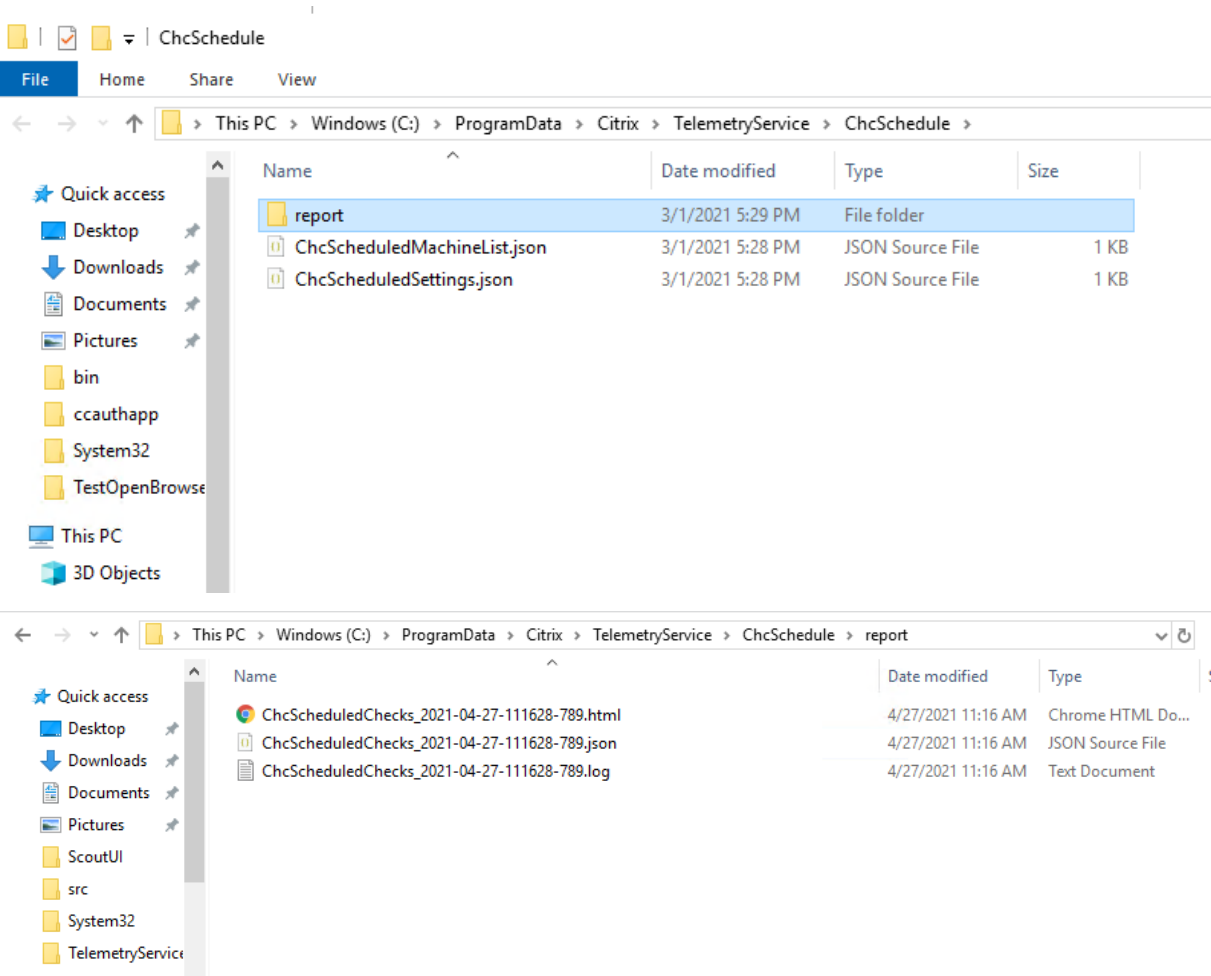
2021-04-27 06:35 UTC

   
Check failed. [View check details.](#)

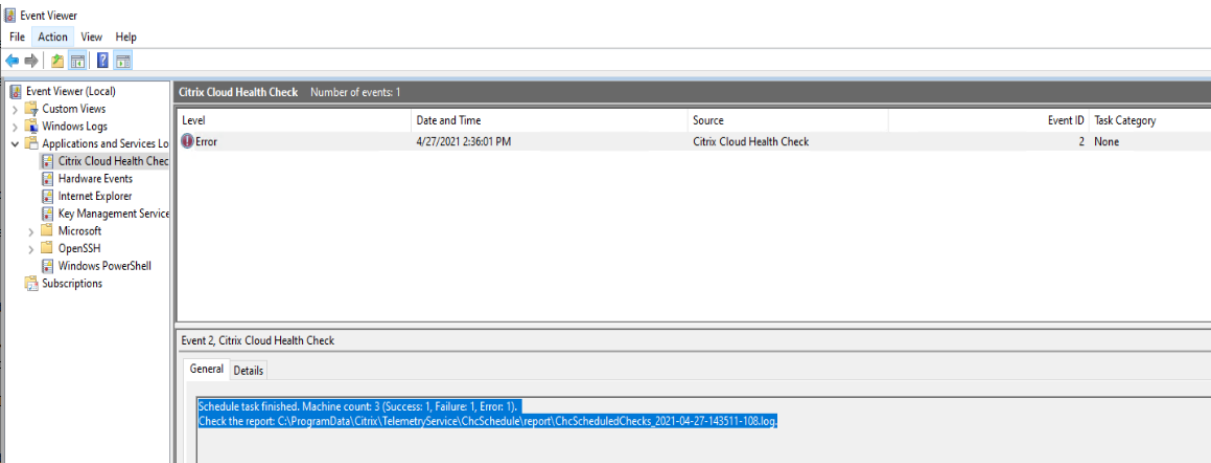
   
Check failed. [View check details.](#)

   
Check successful.

所有运行状况检查结果都存储在名为 ChcSchedule 的文件夹中。Cloud Health Check 在每次检查运行期间创建三个文件。最多可保留 500 个迭代日志。



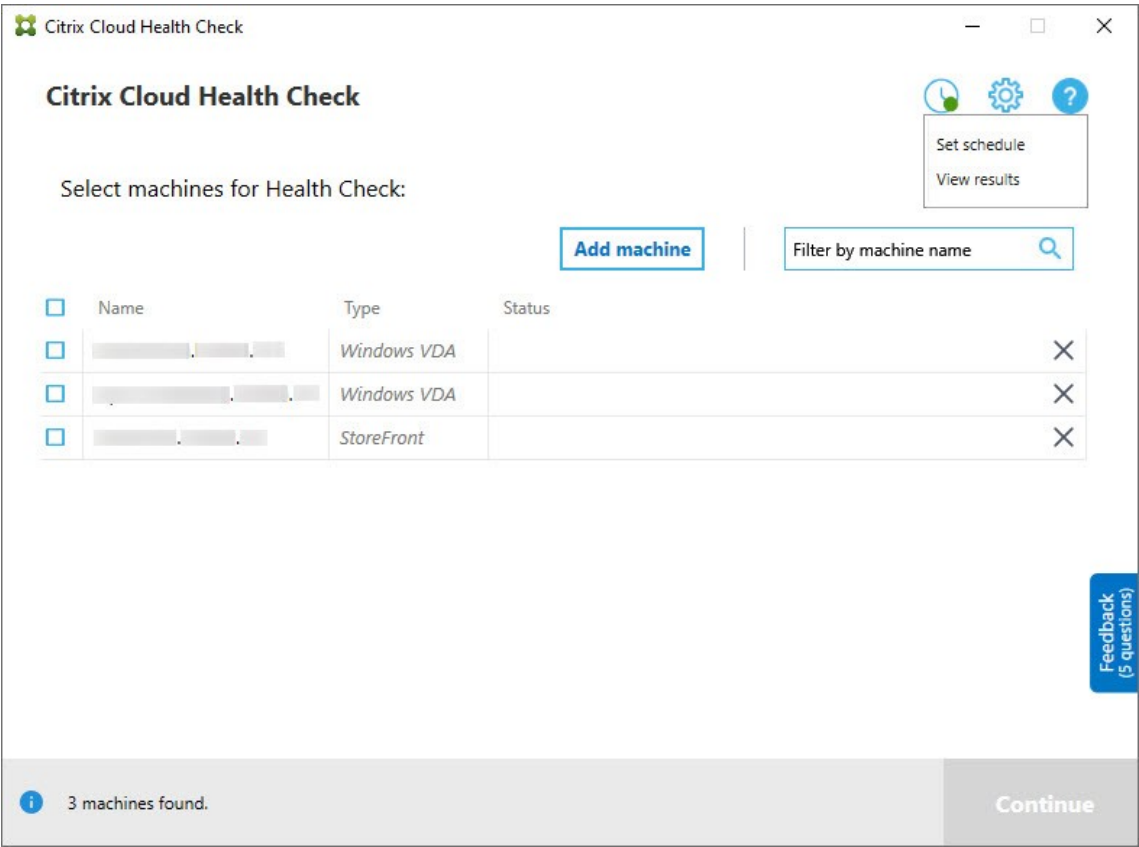
如果选中将结果输出到 **Windows** 事件日志复选框，检查结果也会发送到窗口事件日志。



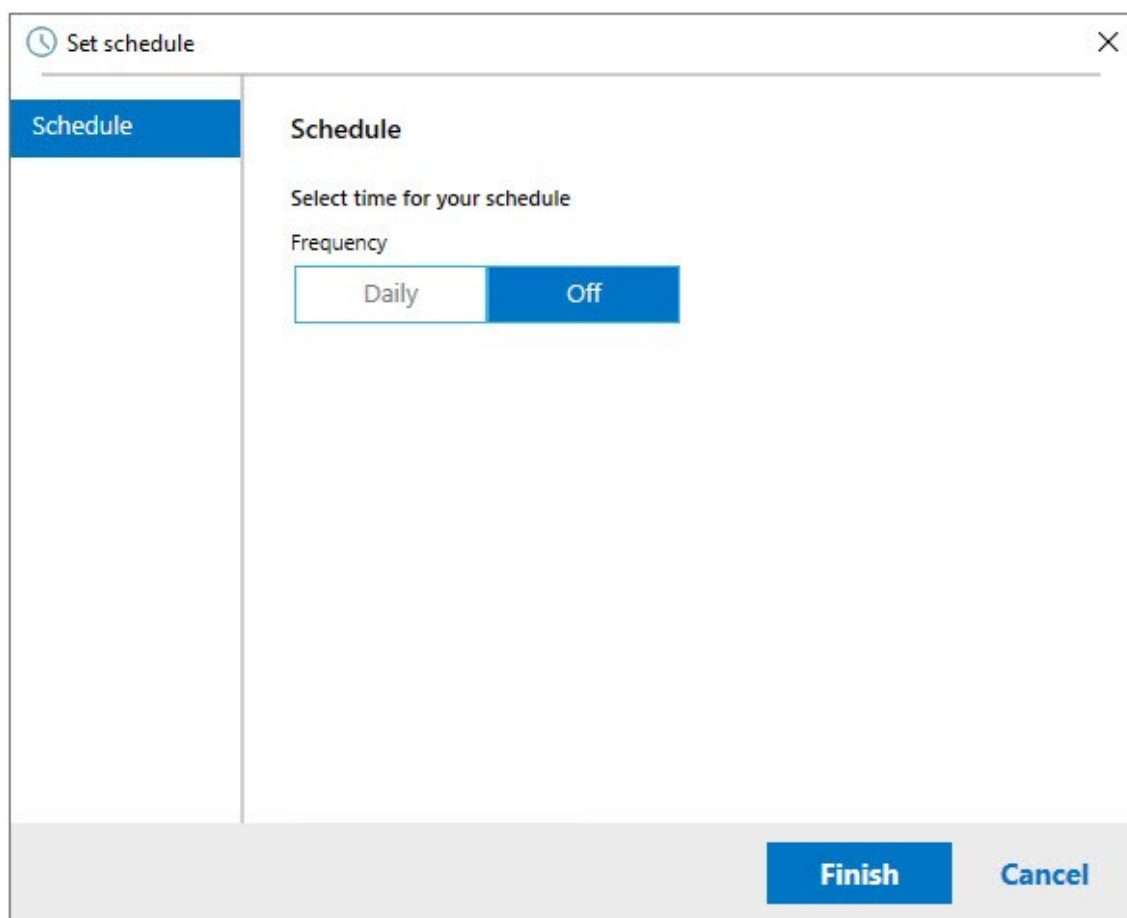
### 禁用计划

1. 单击时钟图标，然后单击设置计划。





2. 单击关，然后单击完成可禁用计划程序。

A screenshot of a 'Set schedule' dialog box. The dialog has a title bar with a clock icon and the text 'Set schedule'. On the left is a sidebar with a 'Schedule' tab. The main area is titled 'Schedule' and contains the text 'Select time for your schedule'. Below this is a 'Frequency' section with two buttons: 'Daily' and 'Off'. The 'Off' button is currently selected. At the bottom right are 'Finish' and 'Cancel' buttons.

Set schedule

Schedule

Select time for your schedule

Frequency

Daily Off

Finish Cancel

#### 更多信息

- 必须首先向 Cloud Health Check 中添加或导入 VDA。有关详细信息，请参阅[导入 VDA 计算机](#)。
- Cloud Health Check 计划程序一次只能在加入了域的计算机上安排一个任务。如果您多次设置计划，则只有最新的计划才会生效。

#### 验证测试

在运行状况检查启动之前，验证测试将针对选定的每台计算机自动运行。这些测试可确保满足运行运行状况检查的要求。如果某台计算机的测试失败，Cloud Health Check 将显示一条消息，提供建议的更正措施。

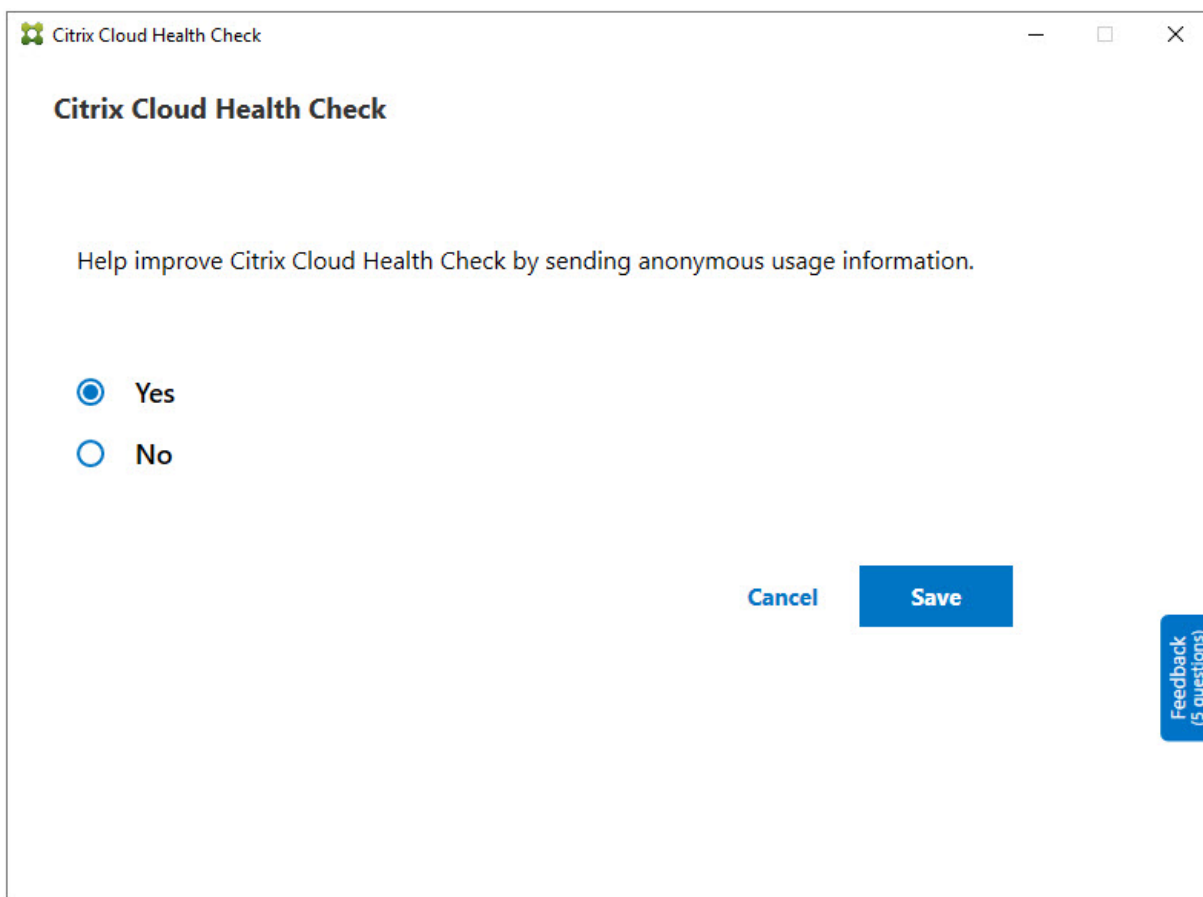
- **Cloud Health Check** 无法访问此计算机 - 请确保：
  - 计算机已打开电源。
  - 网络连接正确运行。（这可以包括验证您的防火墙是否已正确配置。）
  - 已打开文件和打印机共享。请参阅 Microsoft 文档以了解相关说明。
- 启用 **PSRemoting** 和 **WinRM** - 可以通过以管理员身份运行 PowerShell，然后运行 Enable-PSRemoting cmdlet 来启用 PowerShell 远程处理和 WinRM。有关详细信息，请参阅 Microsoft 帮助中的 cmdlet。

- **Cloud Health Check** 要求 **PowerShell 3.0** 或更高版本 - 在计算机上安装 PowerShell 3.0 或更高版本，然后启用 PowerShell 远程处理。
- **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。

## 使用数据收集

使用 Cloud Health Check 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 Cloud Health Check 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。

A screenshot of the Citrix Cloud Health Check dialog box. The title bar says "Citrix Cloud Health Check". The main heading is "Citrix Cloud Health Check". Below it, the text reads "Help improve Citrix Cloud Health Check by sending anonymous usage information." There are two radio buttons: "Yes" (selected) and "No". At the bottom right, there are "Cancel" and "Save" buttons. On the far right, there is a vertical button labeled "Feedback (5 questions)".

Citrix Cloud Health Check

Citrix Cloud Health Check

Help improve Citrix Cloud Health Check by sending anonymous usage information.

☒ Yes

☐ No

Cancel Save

Feedback (5 questions)

## 自动修复

自动修复允许 Cloud Health Check 通过更改设置或重新启动服务来自动检测和修复某些问题。

自动修复将检查以下 VDA 注册项目，并提供建议的修复：


- VDA 计算机域成员身份

- 修复：使用“修复”模型测试连接安全通道进行修复
- VDA 服务状态
  - 修复：重新启动 BrokerAgent 服务
- 与 Controller 通信
  - 修复：重新启动 BrokerAgent 服务
- 与 Controller 进行时间同步
  - 修复：运行 W32tm 命令

对于会话启动，自动修复将检查以下项目，并提供建议安装的修复：

- 会话启动服务状态
  - 修复：重新启动 BrokerAgent 服务

默认情况下启用此功能。要将其禁用，请单击 Cloud Health Check 主窗口右上角的齿轮图标，然后取消选中 **Attempt to automatically fix VDA issues during health check**（尝试在运行状况检查期间自动修复 VDA 问题）。

 Citrix Cloud Health Check

Citrix Cloud Health Check

[Update available](#)

Current version1.0

Installer version1.99.0.0

☒ Attempt to automatically fix VDA issues during health check. Some issues might not resolve. Runs on local machine only.

Help improve Citrix Cloud Health Check by sending anonymous usage information.

☒ Yes

☐ No


Cancel

Save


Feedback  
(5 questions)

结果报告

运行自动修复后，检查结果报告中会有一个部分显示所有详细信息：

 AutoFix Actions Taken

| Issue Name                                                            | Fix                                                                             | Result    |
|-----------------------------------------------------------------------|---------------------------------------------------------------------------------|-----------|
| Citrix Desktop Service displays invalid status                        | get-service -Name brokeragent   Where {\$_.Status -ine Running}   start-service | Succeeded |
| System clocks on the VDA and Delivery controller are not synchronized | net start w32time W32tm /resync /force                                          | Succeeded |

 Citrix Cloud Health Check

Citrix Cloud Health Check

[Update available](#)

Current version1.0

Installer version1.99.0.0

☒ Attempt to automatically fix VDA issues during health check. Some issues might not resolve. Runs on local machine only.

Help improve Citrix Cloud Health Check by sending anonymous usage information.

☒ Yes

☐ No

Cancel

Save

Feedback  
(5 questions)

故障排除

当 Cloud Health Check 无法运行或出现任何异常时，请检查 `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log` 中的 Cloud Health Check 日志。

每台目标计算机的 Cloud Health Check 日志均位于 `C:\ProgramData\Citrix\TelemetryService\HealthCheck\Data\${TargetMachineFQDN}\log.txt` 中。

启用调试日志：

编辑 `C:\Program Files\Citrix\CloudHealthCheck\CloudHealthCheck.exe.config`，更新 `<add name="TraceLevelSwitch" value="3"/>` to `<add name="TraceLevelSwitch" value="4"/>`，保存文件并重新打开 Cloud Health Check。

## 反馈

要留下有关 Cloud Health Check 的反馈，请填写 [Citrix 调查](#)。

## 配置日志记录

March 5, 2024

### 注意：

无论您为 Citrix Cloud 帐户选择哪种语言，配置日志记录都仅以英文显示。与这些记录关联的日期和时间采用 MM/DD/YY 格式，用协调世界时 (UTC) 表示。

配置日志记录是一项用于将 Citrix Virtual Apps and Desktops 和 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）部署配置更改和管理活动捕获到 Citrix Cloud 中的日志记录数据库的功能。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。
- 报告行政活动。

在此 Citrix DaaS 中，始终启用配置日志记录。您无法将其禁用。

在“完整配置”管理界面中，您可以查看按日期范围或全文搜索筛选的配置日志内容。还可以使用 PowerShell 生成 CSV 报告。在此控制台中，您无法编辑或删除日志内容。可以使用远程 PowerShell SDK 安排从日志中定期删除数据。

## 缩短了 Citrix DaaS 中配置登录的保留期

从 2024 年 9 月 9 日起，我们将配置日志记录的保留期缩短到 180 天。

超过 180 天的日志将在 2024 年 9 月 9 日之后删除。随着我们对单个 DaaS 设置的限制不断增加，需要缩短 Config 日志的保留期，以便为客户提供最佳性能和弹性。有关详细信息，请参阅 [限制](#)。

作为最佳实践，我们建议您设置季度导出机制，使用 PowerShell 生成 HTML 或 CSV 格式的报告。有关更多信息，请参阅[生成报告](#)。

Citrix 还建议您定期安排数据删除活动，以保持系统的良好卫生。有关更多信息，请参阅[计划定期删除数据](#)。

所需权限（请参阅[委派管理](#)）：

- Citrix Cloud 中的完全权限管理员以及 Citrix DaaS 云管理员和只读权限管理员可以在管理控制台中查看配置日志。
- 完全权限管理员和云管理员还可以使用 PowerShell 下载日志记录活动的 CSV 报告。

## 记录的内容

将记录以下操作：

- 从管理和监视选项卡启动的配置更改和管理活动
- PowerShell 脚本
- REST API 请求

注意：

您无法看到 Citrix Cloud 平台内部操作（例如数据库设置和管理）的日志条目。

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
- 通过管理控制台执行的 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
- 管理或监视向用户发送消息的功能

以下操作不在记录范围之内。（许多功能对客户管理员不可用。）

- 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 工具可查看这些操作的日志。
- 通过注册表或从“完整配置”管理界面、Monitor 或 PowerShell 以外的其他源所做的更改。

## 查看配置日志内容

要查看配置日志内容，请执行以下步骤：

1. 登录 [Citrix Cloud](#)。在左上角的菜单中选择我的服务 > **DaaS**。
2. 在管理 > 完整配置中，选择左侧窗格中的日志记录 > 事件。

默认情况下，在中心窗格显示的内容会按时间顺序列出日志内容（最新的条目在最前面），并按日期进行分隔。您可以：

- 按列标题对显示的内容进行排序。
- 通过指定一天间隔或自定义时间段，或者通过在搜索框中输入文本来筛选显示内容。要在使用搜索后返回到标准显示，请清除搜索框中的文本。

显示特性：

- 在中上部窗格中列出了管理和监视期间创建的高级别操作。高级别操作会导致出现一个或多个服务和 PowerShell SDK 调用，这些是低级别操作。在中上部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。
- 如果您在 PowerShell 中创建了一项低级别操作，但未指定高级别父操作，配置日志记录将创建替代的高级别操作。
- 如果操作在完成之前失败，可能无法在数据库中完成日志操作。例如，开始记录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，如果您请求过去五天的日志，并且开始时间在过去五天内的某个日期没有结束时间，则会包括该日志。
- 谨记：您无法看到 Citrix Cloud 平台内部操作（例如数据库设置和管理）的日志条目。

### 查看与计算机目录操作有关的任务

要查看与计算机目录操作相关的任务，请导航到管理 > 完整配置 > 日志记录 > 任务。任务选项卡仅显示与通过 Machine Creation Services (MCS) 或 Provisioning Services (PVS) 创建的目录相关的任务。具体而言，将显示与以下计算机目录操作关联的任务：

- 创建目录
- 克隆目录
- 添加计算机
- 删除计算机
- 更新目录（更新映像或计算机）
- 回滚计算机更新

#### 提示：

任务选项卡仅显示与预配方案更改（创建或修改预配方案）相关的任务。

任务可以处于以下状态：

- 已完成
- 未启动
- 正在运行
- 已取消
- 失败
- 未知

要取消正在运行的任务，请选择该任务，然后单击取消。取消需要一些时间才能完成。

记录的任务的示例包括：

- 特定目录的映像更新已完成
- 更新特定目录的映像时出错



- 已取消特定目录的映像更新
- 将 VM 预配到特定目录
- 从特定目录中删除 VM
- 创建了特定目录

默认情况下，在中心窗格中显示的内容会按时间顺序列出记录的任务（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内容进行排序。要清除已完成的任务，请单击任务选项卡下的清除已完成的任务。

## 查看 API 日志

要查看 REST API 日志，请导航到管理 > 完整配置 > 日志记录 > **API**。**API** 选项卡显示在特定时间段内发出的 REST API 请求。

请注意以下事项：

- 注销控制台后，将清除 REST API 日志。（如果刷新浏览器窗口，它们也会被清除。）
- 控制台中导致 API 调用的任何操作都会在 API 选项卡上显示相应的 **API** 请求。
- 该显示屏幕按时间顺序列出 API 请求（首先显示最新条目），并按日期分隔。显示屏幕中的最大 API 请求数为 1000 个。

## 查看 PowerShell 日志

要查看与您在白天执行的用户界面操作相对应的 PowerShell 命令，请导航到管理 > 完整配置 > 日志 > **PowerShell** 标签。

## 将元数据与配置日志关联

通过将名为 **MetadataMap** 的 **name-value** 对与日志记录相关联，您可以将元数据附加到配置日志。

注意：

- 只能将元数据附加到高级操作对象。
- 元数据在执行时与现有记录相关联。

## 设置元数据

运行 PowerShell 命令 **Set-LogHighLevelOperationMetadata** 将日志记录与 **MetadataMap** 相关联。

**Set-LogHighLevelOperationMetadata** 采用以下参数：

- **Id**：高级操作的 ID。

- **InputObject**: 向其中添加元数据的高级操作。这是将高级操作对象或对象列表传递给 PowerShell 命令的 `Id` 参数的替代方案。
- 名称: 要添加的元数据的属性名称。对于指定的高级操作, 该属性必须是唯一的。该属性不能包含以下任何字符:  
( ) \ / ; : # . \* ? = < > | [ ] " ' "
- 值: 属性的值。
- 映射: 属性 (名称、值) 对的字典。这是使用 `-Name` 和 `-Value` 参数设置元数据的替代方法。

例如, 要将元数据附加到 ID 为 40 的所有高级日志记录, 请运行以下 PowerShell 命令:

```
Get-LogHighLevelOperation - Id 40 | Set-LogHighLevelOperationMetadata  
-Name A -Value B
```

要将元数据附加到用户 `abc@example.com` 的高级记录, 请运行以下 PowerShell 命令:

```
Get-LogHighLevelOperation - User `abc@example.com` | Set-LogHighLevelOperation  
-Name C -Value D
```

#### 使用元数据进行检索

请运行以下 PowerShell 命令以使用关联的元数据检索日志记录:

- 按键和值搜索:  

```
Get-LogHighLevelOperation -Metadata "Key:Value"
```
- 按值和任意键搜索:  

```
Get-LogHighLevelOperation -Metadata "*:Value"
```
- 按键和任意值搜索:  

```
Get-LogHighLevelOperation -Metadata "Key:*
```

#### 删除元数据

运行 PowerShell 命令 `Remove-LogHighLevelOperationMetadata` 可删除关联的元数据。

`Remove-LogHighLevelOperationMetadata` 采用以下参数:

- **Id**: 高级操作的 ID。
- **InputObject**: 向其中添加元数据的高级操作。这是将高级操作对象或对象列表传递给 PowerShell 命令的 `Id` 参数的替代方案。
- 名称: 要删除的元数据的属性名称。设置为 `$null` 以删除指定对象的所有元数据。
- 映射: 属性的 (名称、值) 对字典。它可以是哈希表 (使用 `@{ "name1" = "val1" ; "name2" = "val2" }` 创建), 也可以是字符串字典 (使用新对象 `"System.Collections.Generic.Dictionary[String, String]"` 创建)。名称与映射中键匹配的属性将被删除。

## 生成报告

要生成包含配置日志数据的 CSV 或 HTML 报告，请在 Citrix Virtual Apps and Desktops 远程 PowerShell SDK 中对 ConfigLogging Service 的 PowerShell cmdlet。有关详细信息，请参阅：

- [Export-LogReportCsv](#)
- [Export-LogReportHtml](#)

## 计划定期删除数据

使用远程 PowerShell SDK 可指定在配置日志记录数据库中保留数据的时间。（此功能在“完整配置”管理界面中不可用。）在 Citrix DaaS 中，您必须具有完全访问权限。

在 [Set-LogSite](#) cmdlet 中，[-LoggingDBPurgeDurationDays](#) 参数指定配置日志记录数据库中的数据在自动删除之前保留的天数数据。

- 默认情况下，此参数的值为 0。值 0 表示永远不会自动删除配置日志记录数据库中的数据。
- 设置了非零值时，将每隔 120 分钟检查一次数据库。早于保留期限的数据将被删除。

使用 [Get-LogSite](#) 可查看参数的当前值。

## 与本地 **Citrix Virtual Apps and Desktops** 的区别

如果您熟悉本地 Virtual Apps and Desktops 产品中的配置日志记录，则会发现 Citrix Cloud 版本有几个不同之处。在 Citrix Cloud 中：

- 配置日志记录始终处于启用状态。您无法将其禁用。强制日志记录不可用。
- 您无法更改配置日志记录数据库的位置，因为该数据库在 Citrix Cloud 平台中进行管理。
- 配置日志显示不包括在 Citrix Cloud 平台中执行的操作和活动。
- PowerShell 是创建记录的操作的 CSV 或 HTML 报告的唯一选择。在本地产品中，可以从 Citrix Studio 或 PowerShell 生成报告。
- 无法删除配置日志内容。

## 委派管理

March 30, 2024

### 概述

如果在 Citrix Cloud 中具有委派管理权限，则可以根据您的所有管理员在贵组织中的角色来配置其所需的访问权限。

默认情况下，管理员具有完全访问权限。此设置允许访问 Citrix Cloud 中的所有可用的客户管理功能以及所有订阅的服务。要定制管理员的访问权限，请执行以下操作：

- 在 Citrix Cloud 中为管理员的常规管理权限配置自定义访问权限。
- 为订阅的服务配置自定义访问权限。在 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）中，您可以在邀请新管理员时配置自定义访问权限。稍后可以更改管理员的访问权限。

有关显示管理员列表和定义访问权限的信息，请参阅[管理管理员对 Citrix Cloud 的访问权限](#)。

本文介绍如何在 Citrix DaaS 中配置自定义访问权限。

### 管理员、角色和作用域

委派管理对自定义访问权限使用三个概念：管理员、角色和作用域。

- 管理员：管理员表示其 Citrix Cloud 登录标识的人员，通常为电子邮件地址。每个管理员均与一个或多个角色和作用域对相关。
- 角色：角色代表一项工作职能，并且具有与其关联的权限。这些权限允许某些任务是 Citrix DaaS 的唯一任务。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的权限以及其他关联的权限。管理员可以有多个角色。管理员可以是交付组管理员和计算机目录管理员。

Citrix DaaS 提供几个内置的自定义访问角色。您不能更改这些内置角色中的权限，也不能删除这些角色。

您可以创建自己的自定义访问角色以满足贵组织的要求，并委派具有更多详细信息的权限。使用自定义角色可按照操作或任务的粒度来分配权限。只有在未将自定义角色分配给管理员时才能删除该角色。

可以更改管理员具有的角色。

角色始终与作用域配对。

- 作用域：一个作用域代表一个对象集合。作用域用于以与贵组织相关的方式对对象进行分组。对象可以位于多个作用域中。

系统提供一个内置的作用域“全部”，其包含所有对象。Citrix Cloud 和技术支持管理员始终与“全部”作用域配对。无法为这些管理员更改该作用域。

当您邀请（添加）此服务的管理员时，角色始终与作用域（默认为“全部”作用域）配对。

可以在管理 > 完整配置界面中创建和删除作用域。可以在 Citrix Cloud 控制台分配角色/作用域对。

不显示完全访问权限管理员的作用域。根据定义，这些管理员可以访问所有客户管理的 Citrix Cloud 和订阅的服务对象。

## 内置角色和作用域

Citrix DaaS 具有以下内置角色。

- 云管理员：可以执行可从 Citrix DaaS 启动的所有任务。

可以在控制台中查看管理和监视选项卡。此角色始终与“全部”作用域结合使用。不能更改作用域。

请勿被此角色的名称混淆。具有自定义访问权限的云管理员无法执行 Citrix Cloud 级别的任务（Citrix Cloud 任务需要完全访问权限）。

- 只读权限管理员：可以查看指定作用域内的所有对象（以及全局信息），但无法更改任何内容。例如，作用域为“伦敦”的只读权限管理员可以查看所有全局对象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。

可以在控制台中查看管理和监视选项卡。

- 技术支持管理员：可以查看交付组，并可以管理与这些组关联的会话和计算机。可以查看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。

可以在控制台中看到监视选项卡。看不到管理选项卡。此角色始终与“全部”作用域结合使用。不能更改作用域。

- 计算机目录管理员：可以创建和管理计算机目录以及在其中预配计算机。可以管理基础映像并安装软件，但不可向用户分配应用程序或桌面。

可以在控制台中看到 **Monitor** 和管理选项卡。看不到显示器选项卡。可以更改作用域。

- 交付组管理员：可以交付应用程序、桌面和计算机。还可以管理关联的会话。可以管理应用程序和桌面配置，例如策略和电源管理设置。

可以在控制台中看到 **Monitor** 和管理选项卡。可以更改作用域。

### 注意：

要以交付组管理员的身份更改桌面的显示名称，您需要有“执行计算机更新”权限。此权限是必需的，因为更改显示名称涉及更新计算机属性。

- 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。

可以在控制台中看到管理选项卡。看不到显示器选项卡。可以更改作用域。

- 会话管理员：可以查看正在监视的交付组并管理其关联的会话和计算机。

可以在控制台中看到监视选项卡。看不到管理选项卡。不能更改作用域。

- 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。

可以在控制台中查看管理和监视选项卡。此角色始终与全部作用域结合使用。不能更改作用域。

- 完全权限监视管理员：对监视选项卡上的所有视图和命令具有完全访问权限。

可以在控制台中看到监视选项卡。看不到管理选项卡。不能更改作用域。

- 探测代理管理员：具有探测代理 API 的访问权限。

可以在控制台中看到 **Monitor** 和管理选项卡。对应用程序页面具有只读访问权限，但不能访问任何其他视图。

下表汇总了 Citrix DaaS 中的每个自定义访问权限角色可见的控制台选项卡，以及该角色是否可用于自定义作用域。

| 自定义访问权限管理员角色    | 是否可以在控制台中看到管理选项卡？ | 是否可以在控制台中看到监视选项卡？ | 角色是否可以与自定义作用域结合使用？ |
|-----------------|-------------------|-------------------|--------------------|
| 云管理员            | 是                 | 是                 | 否                  |
| 只读权限管理员         | 是                 | 是                 | 是                  |
| 技术支持管理员         | 否                 | 是                 | 否                  |
| 计算机目录管理员        | 是                 | 是                 | 是                  |
| 交付组管理员          | 是                 | 是                 | 是                  |
| 主机管理员           | 是                 | 否                 | 是                  |
| 会话管理员           | 否                 | 是                 | 否                  |
| 完全权限管理员         | 是                 | 是                 | 否                  |
| 完全权限监视管理员       | 否                 | 是                 | 否                  |
| Probe Agent 管理员 | 是                 | 是                 | 否                  |

注意：

自定义访问管理员角色（云管理员和帮助台管理员除外）不适用于适用于 Azure 的 Citrix Virtual Apps and Desktops Standard、Virtual Apps Essentials 和 Virtual Desktops Essentials。

要查看与角色关联的权限，请执行以下操作：

1. 登录 [Citrix Cloud](#)。在左上角的菜单中选择我的服务 > **DaaS**。
2. 在管理 > 完整配置中，选择左侧窗格中的管理员。
3. 选择角色选项卡。
4. 在中上部窗格中选择一个角色。下部窗格中的角色定义选项卡列出了类别和权限。选择一个类别以查看特定的权限。管理员选项卡列出了已分配所选角色的管理员。

已知问题：“完全权限管理员”条目不显示完全访问权限 Citrix DaaS 管理员的正确权限集。

您需要多少管理员

管理员的数量及其权限的粒度通常取决于部署的规模和复杂性。

- 在小规模部署或概念证明部署中，一个或几个管理员便足以完成一切工作。没有自定义访问权限委派。在这种情况下，每个管理员都具有完全访问权限，它始终具有“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，两个管理员具有完全访问权限，其他管理员则为技术支持管理员。此外，管理员可能仅管理特定的对象组（作用域），例如特定部门中的计算机目录。在这种情况下，请创建新作用域以及具有相应自定义访问角色和作用域的管理员。

### 管理员管理摘要

为 Citrix DaaS 设置管理员遵循以下顺序：

1. 如果希望管理员具有完全权限管理员（涵盖 Citrix Cloud 中的所有订阅的服务）以外的角色或内置角色，请参阅创建自定义角色。
2. 如果希望管理员具有“全部”以外的作用域（并且预期角色允许使用不同的作用域，但尚未创建），请创建作用域。
3. 在 Citrix Cloud 中，邀请一个管理员。如果希望新管理员具有默认的完全访问权限以外的任何权限，请指定自定义访问权限角色和作用域对。

以后，如果要更改管理员的访问权限（角色和作用域），请参阅配置自定义访问权限。

### 添加管理员

要添加（邀请）管理员，请按照[向 Citrix Cloud 帐户中添加管理员](#)中的指导进行操作。本文中重复使用该信息的一部分。

#### 重要：

不要混淆“自定义”和“自定义访问权限”的用法。

- 在 Citrix Cloud 控制台中创建管理员和为 Citrix DaaS 分配角色时，“自定义访问权限”一词包括内置角色和在服务的 **管理 > 完整配置** 界面中创建的任何其他自定义角色。
- 在该服务的 **管理 > 完整配置** 界面中，“自定义”只是将该角色与内置角色区分开来。

添加管理员的常规工作流程如下：

1. 登录 [Citrix Cloud](#)，然后选择左上角菜单中的 **Identity and Access Management**（身份识别和访问管理）。
2. 在 **Identity and Access Management**（身份识别和访问管理）页面上，选择 **Administrators**（管理员）。管理员选项卡列出了该帐户的所有当前管理员。
3. 在“管理员”选项卡上，选择您的身份类型，输入管理员的电子邮件地址，然后单击“邀请”。
  - 如果您希望管理员拥有完全访问权限，请选择完全访问权限。这样，管理员就可以访问 Citrix Cloud 和所有已订阅的服务中的所有客户管理员功能。

- 如果您希望管理员具有有限的访问权限，请选择自定义访问权限。然后，您可以选择自定义访问角色和作用域。这样，管理员在登录 Citrix Cloud 时就具有预期的权限。

1. 单击发送邀请。Citrix Cloud 向该电子邮件地址发送邀请，并在管理员完成入门后将管理员添加到列表中。

收到电子邮件后，管理员单击 **Sign In**（登录）链接以接受邀请。

有关添加管理员的详细信息，请参阅[管理 Citrix Cloud 管理员](#)。

或者，转到管理 > **Full Configuration**（完整配置）> **Administrators**（管理员）> **Administrators**（管理员），然后单击 **Add Administrator**（添加管理员）。您将直接转到 **Identity and Access Management**（身份识别和访问管理）> **Administrators**（管理员），它将在新的浏览器选项卡中打开。在该位置添加管理员后，关闭选项卡并返回到控制台，继续执行您的其他配置任务。

## 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。此控制功能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）。

自定义角色名称最多可以包含 64 个 Unicode 字符。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。

角色说明最多可以包含 256 个 Unicode 字符。

1. 如果您尚未登录 [Citrix Cloud](#)，请登录。在左上角的菜单中选择我的服务 > **DaaS**。
2. 在管理 > 完整配置中，选择左侧窗格中的管理员。
3. 选择角色选项卡。
4. 按照要完成的任务的说明进行操作：
  - 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：在操作栏中选择创建角色。请按如下所示配置设置：
    - 输入名称和说明。
    - 配置控制台访问权限。确定管理员可以看到哪些控制台。您无需选择任何控制台即可继续。在这种情况下，具有该角色的管理员无法访问管理和监视，但可以通过 SDK 和 API 访问、查看或管理对象。
    - 选择对象类型和权限。要授予对象类型的完全访问权限，请选中其复选框。要在粒度级别授予权限，请展开对象类型，然后在类型内的 **Manage**（管理）下选择 **Read Only**（只读）或单个对象。



Create Role

Define a role for this administrator based on the administrator's permissions to manage various features.

Name:

Example: My New Role

Description:

Example: My New Role Description

Console access

☒ Manage

☒ Monitor

Permissions:

Select one or more permissions for this role.

> ☐ Administrators

> ☐ Application Groups

> ☐ Application Packages

> ☐ Cloud

> ☐ Delivery Groups

> ☐ Director

> ☐ DirectorProbeAgent

> ☐ Hosts

> ☐ Logging

> ☐ Machine Catalogs

> ☐ Other permissions

> ☐ Policies

> ☐ StoreFronts

> ☐ UPM

> ☐ Zones

- 复制角色：在中间窗格中选择角色，然后在操作栏中选择复制角色。根据需要更改名称、说明、对象类型和权限。完成后，选择 **Save**（保存）。
- 编辑自定义角色：在中间窗格中选择角色，然后在操作栏中选择编辑角色。根据需要更改名称、说明、对

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

1130

象类型和权限。无法编辑内置角色。完成后，选择 **Save**（保存）。

- 删除自定义角色：在中间窗格中选择角色，然后在操作栏中选择删除角色。出现提示时，确认删除。无法删除内置角色。如果某个自定义角色分配给管理员，则无法删除该角色。

## 创建和管理作用域

默认情况下，所有角色都具有其相关对象的全部作用域。例如，交付组管理员可以管理所有交付组。对于某些管理员角色，您可以创建一个作用域，该作用域允许该管理员角色访问相关对象的子集。例如，您可能希望授予计算机目录管理员访问仅包含特定类型的计算机目录而非所有目录的权限。

- 完全访问权限管理员或自定义访问权限云管理员可以为“只读权限管理员”、“计算机目录管理员”、“交付组管理员”和“主机管理员”角色创建作用域。
- 无法为完全访问权限管理员创建作用域，也无法为云管理员或技术支持管理员创建作用域。这些管理员始终具有“全部”作用域。

创建和管理作用域的规则：

- 作用域名称最多可以包含 64 个 Unicode 字符。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、左箭头或右箭头、竖线、左右方括号、左右圆括号、引号和单引号。
- 作用域说明最多可以包含 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。

要创建和管理作用域，请执行以下操作：

1. 登录 [Citrix Cloud](#)。在左上角的菜单中选择我的服务 > **DaaS**。
2. 在管理 > 完整配置中，选择左侧窗格中的管理员。
3. 选择作用域选项卡。
4. 按照要完成的任务的说明进行操作：
  - 查看作用域详细信息：选择作用域。窗格的下部列出了具有该作用域的对象和管理员。
  - 创建作用域：在操作栏中选择创建作用域。输入名称和说明。这些对象按类型列出，例如交付组和计算机目录。
    - 要包括特定类型的所有对象（例如，所有交付组），请选择对象类型对应的复选框。
    - 要包括某种类型内的单个对象，请展开该类型，然后选择对象（例如，特定交付组）对应的交付组。

注意：

应用程序组、交付组或计算机目录将与 DaaS 中的管理保持一致的文件夹结构显示。您可以选择一个文件夹来选择其中的所有对象，也可以展开一个文件夹来选择特定的对象。

- 要创建租户客户，请选中租户作用域复选框。如果选中，为作用域输入的名称则为租户名称。有关租户作用域的详细信息，请参阅租户管理。

完成后，选择 **OK**（确定）。

Create Scope

Define a scope based on objects in your deployment.

Name:

Example: Sales

Description (Optional):

Example: Sales team members

☐ Tenant scope

Objects:

> ☐ Application Groups

> ☐ Delivery Groups

> ☐ Hosting

> ☐ Machine Catalogs

Select all objects of a particular type or specific objects within a type.

OK

Cancel

- 复制作用域：在中间窗格中选择作用域，然后在操作栏中选择复制作用域。更改名称、说明。根据需要更改对象类型和对象。完成后，选择 **Save**（保存）。
- 编辑作用域：在中间窗格中选择作用域，然后在操作栏中选择编辑作用域。根据需要更改名称、说明、对象类型和对象。完成后，选择 **Save**（保存）。
- 删除作用域：在中间窗格中选择作用域，然后在操作栏中选择删除作用域。出现提示时，确认删除。

如果某个作用域分配给某个角色，则无法删除该作用域。如果您尝试执行此操作，则将显示一条错误消息，指示您没有权限。事实上，出现错误的原因是使用此作用域的角色/作用域对分配给管理员。首先，删除所

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

1132

有使用该角色/作用域的角色/作用域分配。然后删除管理控制台中的作用域。

创建作用域后，它会显示在 Citrix Cloud 控制台的 自定义访问 列表中。然后，您可以在向管理员分配角色时选择该角色。

例如，假设您创建了一个名为 CAD 的作用域，然后选择包含适合 CAD 应用程序的计算机的目录。当您返回 Citrix Cloud 控制台并选择 编辑角色作用域 时，可用作用域列表会显示您之前创建的 CAD 作用域。

云管理员和技术支持管理员始终具有“全部”作用域，因此，CAD 作用域不适用于这些管理员。

### 租户管理

使用完整配置管理界面，您可以在单个 Citrix DaaS 下创建互斥的租户。可以通过在管理员 > 作用域中创建租户作用域并将相关配置对象（例如计算机目录和交付组）与这些租户关联来实现这一目标。因此，具有租户访问权限的管理员只能管理与租户关联的对象。

例如，如果您的组织执行以下操作，则此功能非常有用：

- 有不同的业务孤岛（独立的部门或独立的 IT 管理团队）或
- 具有多个本地站点，并希望在单个 Citrix DaaS 实例中保持相同的设置。

该界面允许您按名称筛选租户客户。默认情况下，此界面显示有关所有租户客户的信息。要显示有关特定租户的信息，请从右上角的列表中选择该租户。

**创建租户客户** 要创建租户客户，请在创建作用域时选择租户作用域。通过选择该选项，您可以创建一个唯一的作用域类型，该类型适用于在不同业务部门之间共享 Citrix DaaS 实例的场景中的对象，这些业务部门中的每个业务部门都独立于其他业务部门。创建租户作用域后，无法更改作用域类型。

## Create Scope

Define a scope based on objects in your deployment.

Name:

Example: Sales

Description (Optional):

Example: Sales team members

☐ Tenant scope ?

作用域选项卡显示所有作用域项目。常规作用域与租户作用域之间的唯一区别在于类型列。空白列字段表示常规作用域。如果需要，可以单击类型列对作用域项目进行排序。

要查看附加到作用域的资源（对象），请在左侧窗格中选择管理员。在作用域选项卡上，选择作用域，然后在操作栏中选择编辑作用域。

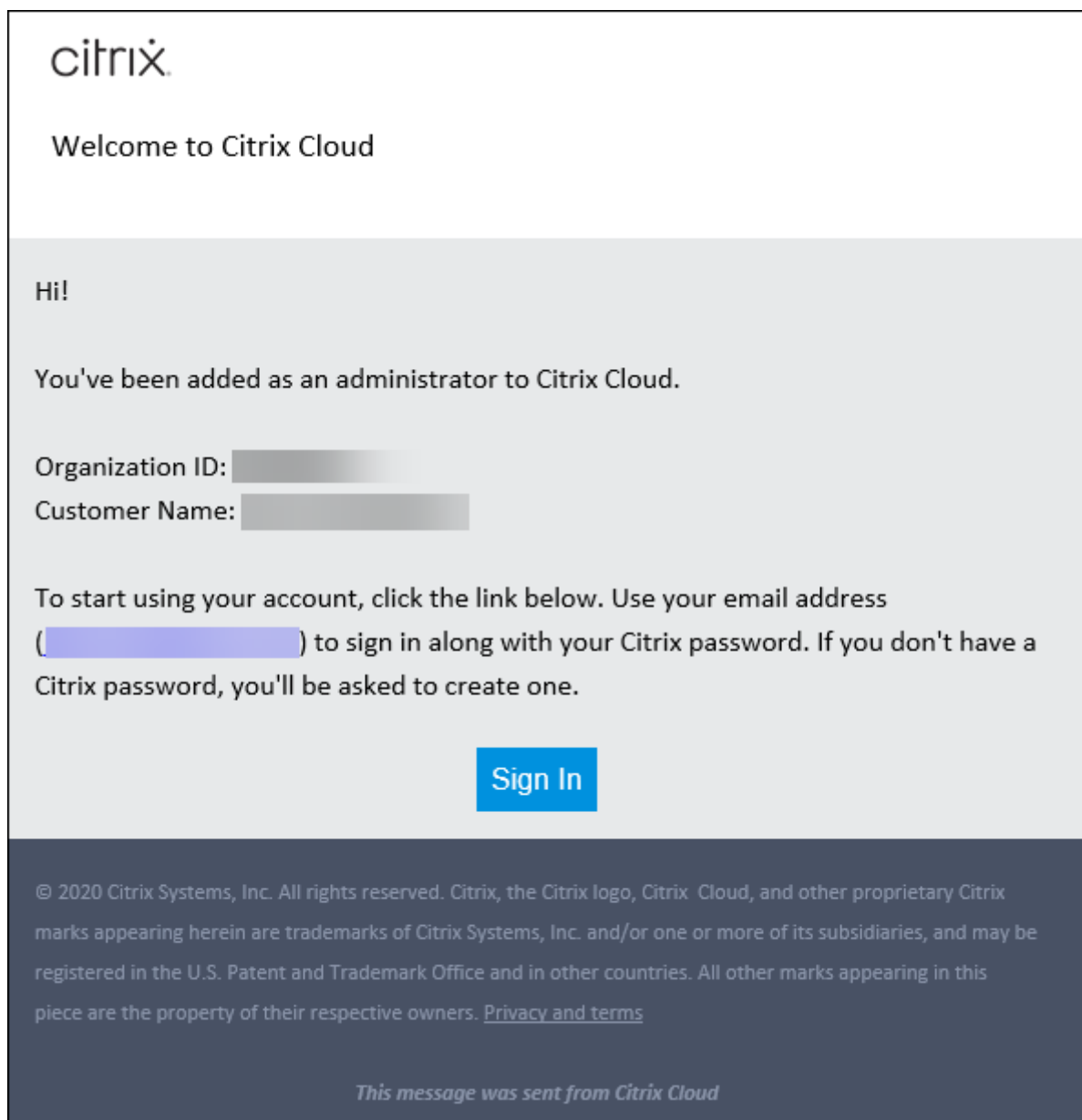
提示：

租户属性是在作用域级别分配的。计算机目录、交付组、应用程序和连接继承适用作用域中的租户属性。

使用租户作用域时，请注意以下注意事项：

- 租户属性按以下顺序分配：托管 > 计算机目录 > 交付组 > 应用程序。级别较低的对象依赖级别更高的对象以从中继承租户属性。例如，选择交付组时，必须选择关联的托管和计算机目录。否则，交付组将无法继承租户属性。
- 创建租户作用域后，可以通过修改对象来编辑租户分配。当租户分配发生变化时，它仍然受到以下约束的约束：必须将其分配给相同的租户或者这些租户的子集。但是，当租户分配发生变化时，不会重新评估级别较低的对象。在更改租户分配时，请确保对象受到适当的限制。例如，如果计算机目录适用于 **TenantA** 和 **TenantB**，则可以为 **TenantA** 创建一个交付组，为 **TenantB** 创建一个交付组。（**TenantA** 和 **TenantB** 都与该计算机目录关联。）然后，您可以更改仅与 **TenantA** 关联的计算机目录。因此，与 **TenantB** 关联的交付组将变得无效。

为管理员配置自定义访问权限 创建租户作用域后，为各自的管理员配置自定义访问权限。有关详细信息，请参阅[为管理员配置自定义访问权限](#)。Citrix Cloud 向您指定的客户管理员发送邀请，并将其添加到列表中。收到电子邮件时，他们将单击 **Sign In**（登录）接受邀请。登录到完整配置管理界面时，他们会看到分配的角色和作用域对包含的资源。



具有租户访问权限的管理员只能管理与租户关联的对象（例如，计算机目录、交付组）。

#### 为管理员配置自定义访问权限

通过此功能，您可以通过与其在组织中的角色相一致的方式定义现有管理员或您邀请的管理员的访问权限。

您对访问权限所做的更改需要 5 分钟才能生效。注销“完整配置”管理界面并重新登录会使更改立即生效。如果管理员在更改生效后仍使用管理界面而不重新连接到该控制台，则当其尝试访问不再具有权限的项目时，会显示一条警告。

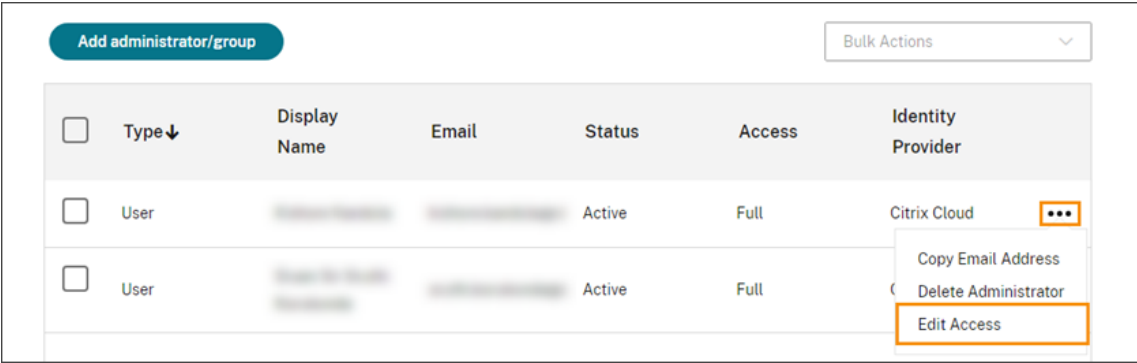
默认情况下，当您邀请管理员时，这些管理员具有完全访问权限。完全访问权限允许管理员管理所有订阅的服务和所有 Citrix Cloud 操作（例如邀请更多管理员）。Citrix Cloud 部署至少需要一位具有完全访问权限的管理员。

您也可以在邀请管理员时授予自定义访问权限。自定义访问权限允许管理员仅管理您指定的服务和操作。

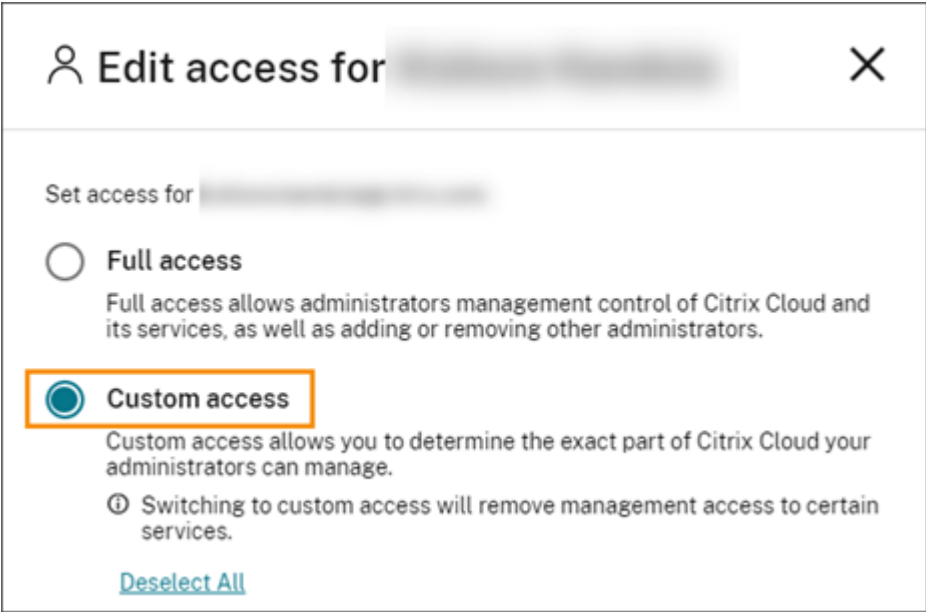
在 Citrix DaaS 中创建角色或作用域时，它会显示在自定义访问列表中并可以选择。为管理员选择角色时，可以根据需要修改作用域以反映管理员在组织中的角色。

要为管理员配置自定义访问权限，请执行以下操作：

1. 登录 [Citrix Cloud](#)。选择左上角菜单中的 **Identity and Access Management**（身份识别和访问管理）> **Administrators**（管理员）。
2. 找到要管理的管理员，选择省略号菜单，然后选择 **Edit access**（编辑访问权限）。



3. 选择 **Custom access**（自定义访问权限）。



4. 在 **DaaS** 下，选择或清除一个或多个角色旁边的复选标记。要修改与分配的角色关联的作用域，请选择 **编辑作用域**。

**Edit access for**

☒ General | All roles selected

☒ DaaS | 2 of 12 roles selected

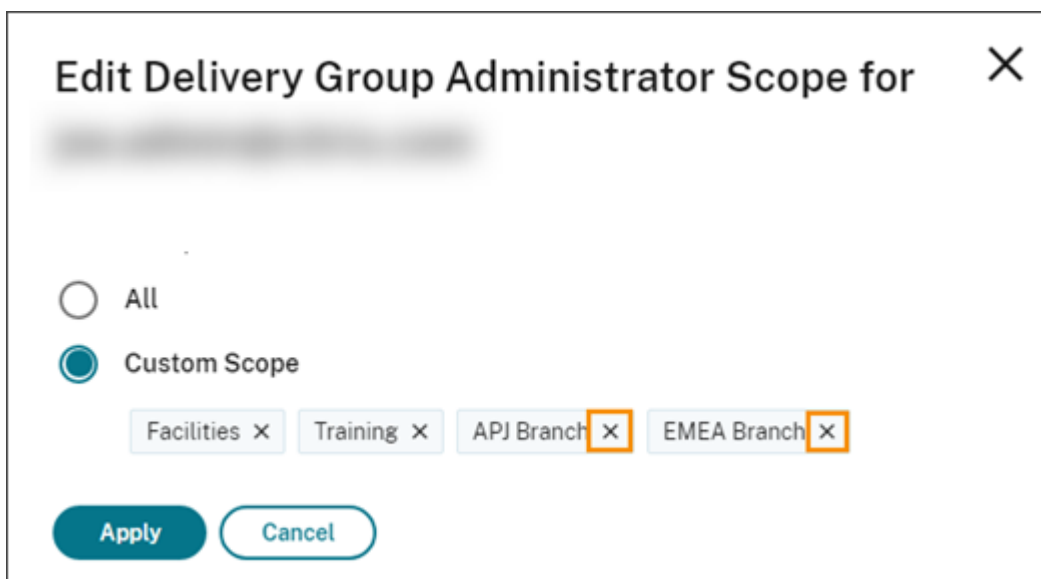
- ☐ Cloud Administrator
- ☒ Delivery Group Administrator [Edit scopes](#)  
All scopes
- ☐ Full Monitor Administrator - Access to 'Monitor' tab only
- ☐ Help Desk Administrator - Access to 'Monitor' tab only
- ☐ Host Administrator
- ☒ Machine Catalog Administrator [Edit scopes](#)  
All scopes
- ☐ Probe Agent Administrator
- ☐ Read Only Administrator
- ☐ Session Administrator - Access to 'Monitor' tab only

**Save** **Cancel**

默认情况下，每个选定角色都选择了所有作用域，如所有作用域标签所示。

5. 要为所选角色指定作用域，请选择 自定义作用域，然后添加或删除相应的作用域。默认情况下，所有自定义作用域都将添加到角色中。要移除作用域，请单击作用域上的 X 图标。





**Edit Delivery Group Administrator Scope for** [Redacted] ✕

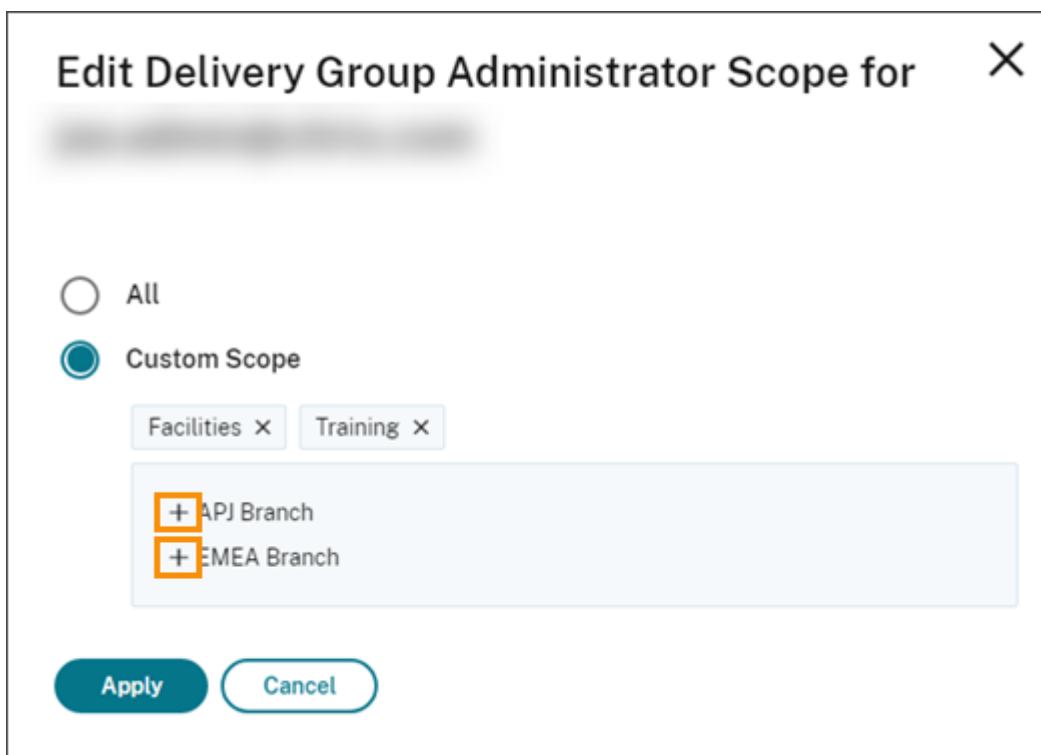
☐ All

☒ Custom Scope

Facilities ✕ Training ✕ APJ Branch ✕ EMEA Branch ✕

**Apply** **Cancel**

已移除但可以添加到角色的作用域显示在已添加的作用域下方的列表中。要向角色添加作用域，请选择作用域的加号图标。



**Edit Delivery Group Administrator Scope for** [Redacted] ✕

☐ All

☒ Custom Scope

Facilities ✕ Training ✕

+ APJ Branch  
+ EMEA Branch

**Apply** **Cancel**

6. 选择完范围后，选择应用。
7. 选择“保存”为管理员保存选定的角色。

## 与本地 **Citrix Virtual Apps and Desktops** 的区别

如果您熟悉本地 Citrix Virtual Apps and Desktops 产品中的委派管理，则会发现 Citrix DaaS 版本有几个不同之处。

在 Citrix Cloud 中：

- 管理员通过其 Citrix Cloud 登录名（而非 Active Directory 帐户）来识别。可以为 Active Directory 个人创建角色/作用域对，但不能创建组。
- 管理员是在 Citrix Cloud 控制台（而非 Citrix DaaS）中创建、配置和删除的。
- 角色/作用域对在 Citrix Cloud 控制台（而非 Citrix DaaS）中分配给管理员。
- 报告不可用。可以在服务的管理 > 完整配置界面中查看管理员、角色和作用域信息。
- 自定义访问云管理员类似于本地版本中的完全权限管理员。两者都具有对正在使用的 Citrix Virtual Apps and Desktops 版本的完全管理和监视权限。

但是，在 Citrix DaaS 中，没有指定的完全权限管理员角色。请勿将 Citrix Cloud 中的“Full access”（完全访问权限）与本地 Citrix Virtual Apps and Desktops 中的“完全权限管理员”等同。Citrix Cloud 中的完全访问权限涵盖平台级别的域、库、通知和资源位置，以及所有订阅的服务。

## 与早期 **Citrix DaaS** 版本的差异

在发布扩展的自定义访问功能（2018 年 9 月）之前，有两个自定义访问管理员角色：完全权限管理员和技术支持管理员。当您的部署启用了委派管理（这是一项平台设置）时，这些角色将自动映射。

- 以前配置为自定义访问权限 **Virtual Apps and Desktops**（或 **XenApp** 和 **XenDesktop**）服务：完全权限管理员的管理员现在为自定义访问权限云管理员。
- 以前配置为自定义访问权限 **Virtual Apps and Desktops**（或 **XenApp** 和 **XenDesktop**）服务：技术支持管理员的管理员现在为自定义访问权限技术支持管理员。

## 更多信息

有关服务的监视控制台中使用的管理员、角色和作用域的信息，请参阅[委派管理和监视](#)。

## 完整配置界面的主页

October 26, 2023

提供 Citrix DaaS 部署和工作负载的概述，以及可帮助您从订阅中获得最大收益的信息。该页面由以下部分组成：

- 服务概述
- 服务运行状况警报
- 建议
- 新增功能
- 预览版功能
- 入门

要访问主页，请执行以下步骤：

1. 登录 [Citrix Cloud](#)。
2. 在 **DaaS** 磁贴中，单击 管理。
3. 选择 “管理” > “完整配置”。此时将显示主页。

服务概述

概述您的 Citrix DaaS 部署和工作负载：

- 资源。按类别显示已部署资源的数量及其计数。

| 资源    | 按类别查看计数                                                                                                                          |
|-------|----------------------------------------------------------------------------------------------------------------------------------|
| 计算机   | 单击 计算机，选择一个状态，然后将鼠标悬停在圆环图上以了解详细信息。可用选项：可用性状态（可用、使用中、关闭和不可用）、注册状态（已注册和未注册）和 维护状态（正在维护和未维护）。按可用性状态查看计算机计数时，您可以单击某个状态以查看相应的计算机详细信息。 |
| 应用程序  | 单击应用程序，然后将鼠标悬停在圆环图上以了解详细信息。                                                                                                      |
| 交付组   | 单击交付组并将鼠标悬停在圆环图上以了解详细信息。                                                                                                         |
| 计算机目录 | 单击计算机目录并将鼠标悬停在圆环图上以了解详细信息。                                                                                                       |

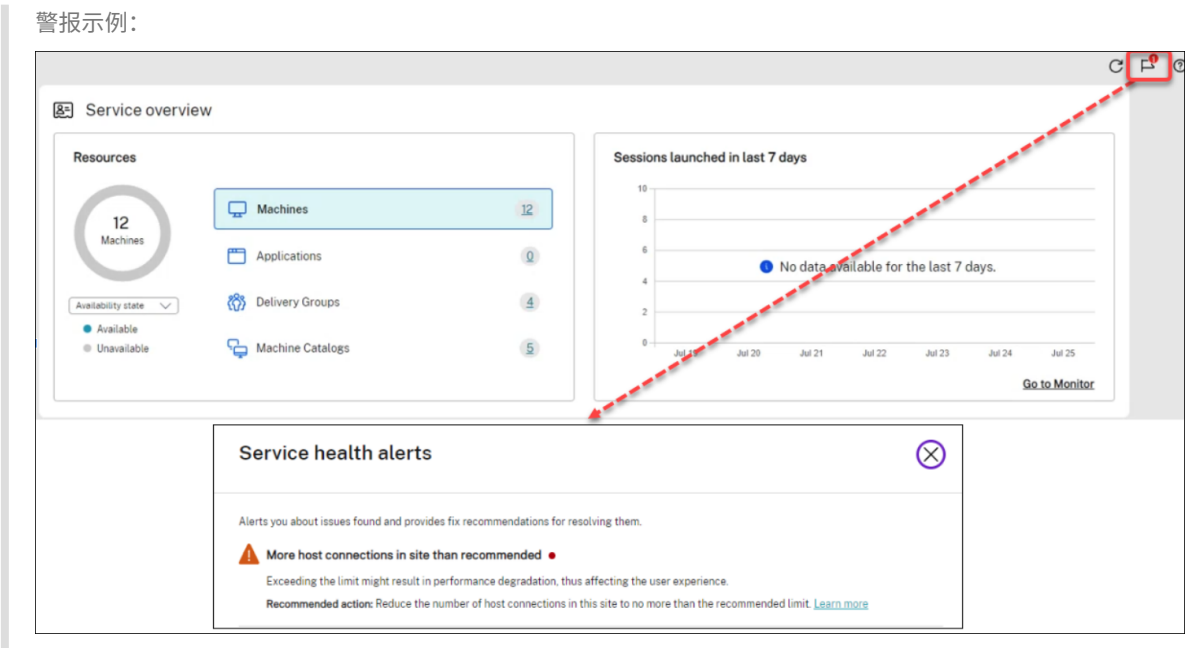
- 会话在过去 **7** 天内启动。显示过去七天每天启动的桌面和应用程序会话数。要深入了解更多信息，请单击 [“转到监视器”](#)。

服务运行状况警报

提醒您发现的问题，并提供解决问题的建议。警报显示有警告和错误符号。

注意：

诊断每小时更新一次。



建议

建议使用您的订阅中可用的功能，例如 [Workspace Environment Management](#) 和 [Autoscale](#)。与我们互动，喜欢或不喜欢推荐并留下您的反馈。

注意：

如果您不喜欢某个推荐，该推荐会消失。如果您不喜欢所有推荐或推荐小部件，则推荐小部件将消失。

新增功能

显示对您的业务最有价值的最新 Citrix DaaS 功能的精选列表。使用这些功能可以帮助您从订阅中获得最大收益。有关新功能的完整列表，请参阅 [新增功能](#)。

预览版功能

显示当前处于预览状态的功能。作为具有完全访问权限的 Citrix Cloud 管理员，您无需联系 Citrix 即可开启或关闭预览功能。更改最多需要 15 分钟才能生效。

建议在非生产环境中使用预览功能。Citrix 技术支持不支持在预览功能中发现的问题。

入门

显示指导您完成应用程序和桌面的初始设置的步骤。

设置步骤如下：

### 1. 创建资源位置

资源位置是指包含要交付给您的用户的应用程序和桌面的位置。通过此步骤，您可以将资源位置添加到 DaaS，并在其中安装 Cloud Connector。Cloud Connector 充当对 Citrix Cloud 与您的资源之间的所有通信进行身份验证和加密的渠道。

### 2. 创建主机连接

主机是在您的资源位置中使用的虚拟机管理程序或云服务。此步骤允许您指定 DaaS 用于与主机上的 VM 通信的信息。详细信息包括资源位置、主机类型、访问凭据、要使用的存储方法以及主机上虚拟机可以使用的网络。

### 3. 准备主映像

主映像包括操作系统、所有必需的应用程序和 Virtual Delivery Agent (VDA)。VDA 在 VM 与用户设备之间建立并维护连接。

### 4. 创建计算机目录

计算机目录是分配给用户的相同单会话或多会话操作系统 VM 的集合。此步骤允许您通过指定预配技术、主映像和 VM 大小来创建计算机目录。

### 5. 分配用户

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。通过此步骤，您可以创建交付组，以指定哪些团队、部门或用户类型可以使用哪些计算机。

### 6. 配置 Workspace

与您的用户共享 **Workspace** 配置 > 访问权限中的 Workspace URL。

## 许可证

October 11, 2022

本文介绍了针对 Microsoft 许可证和 Citrix 许可证的任务和资源。

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

此信息在交付 Windows Server 工作负载时适用。

此服务在交付 Windows Server 工作负载（例如 Windows 2019）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 Microsoft 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 VM 上安装远程桌面服务许可证服务器。VM 必须始终可用。Citrix 服务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。

### Citrix 许可证使用情况

有关 Citrix 许可证使用情况的信息，请参阅：

- [监视云服务的许可证和活动使用情况](#)
- [监视 Citrix DaaS 的许可证和活动使用情况](#)

### 多类型许可

August 14, 2023

多类型许可支持在单个 Citrix DaaS（以前称为 [Citrix Virtual Apps and Desktops 服务](#)）部署中使用不同的许可证授权。如果您有多个 Citrix 许可证权利，则本文适用于您。Citrix 授权是以下各项的组合：

- 在当前 DaaS 的背景下，产品始终为 Citrix DaaS
- 服务版本（例如：Advanced、Advanced Plus、Premium 或 Premium Plus）
- 许可模式（例如：用户/设备或并发）

### 混合权利规则

混合服务版本的规则如下：

- 只允许混用 DaaS Advanced 和 Advanced Plus
- 只允许混用 DaaS Premium 和 Premium Plus
- DaaS Standard 不能与任何其他版本混用

在遵循之前的服务版本规则时，您可以混合使用许可证模式。

### 站点和交付组级别的授权

您可以在以下两个级别配置和使用许可证授权：

- 站点（您对 Citrix DaaS 产品的部署）
- 交付组

如果您尚未配置站点或交付组权利，请注意以下默认行为：

- 如果您有多个授权，则选择可用权利中最有效的授权作为站点范围的授权，前提是它们是同时订购的。否则，除非稍后明确更改，否则第一个出现的将成为全站默认值。
- 除非配置了交付组权利，否则将使用站点权利。

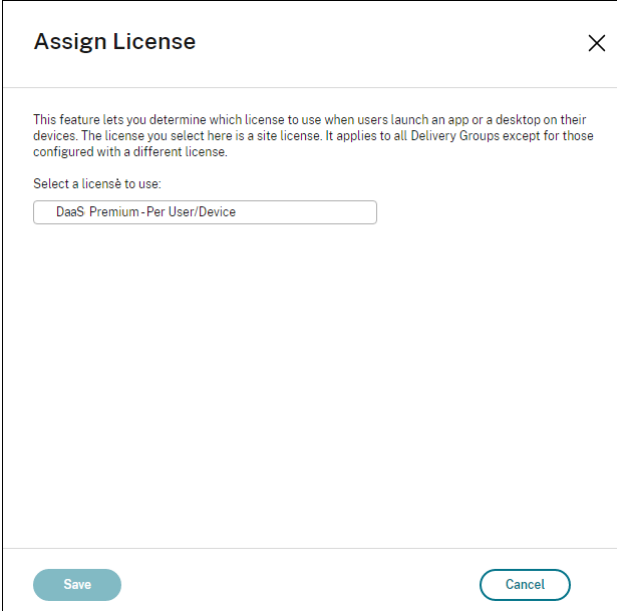
注意：

为站点或交付组配置权利会影响许可证使用情况在[许可证使用情况在 Citrix Cloud 中显示](#)的计数方式。

### 查看和更新站点级权利

要指定要在站点范围内使用的许可证权利，请导航到完整配置 > 设置 > 分配许可证，然后单击编辑。此时将显示 **Assign License**（分配许可证）刀片。有关如何进入 完整配置 页面的信息，请参阅 [Citrix DaaS](#) 文档。

在分配许可证刀片中，选择您希望站点使用的许可证。所选许可证适用于站点上的所有交付组，但使用不同许可证配置的交付组除外。



The image shows a dialog box titled "Assign License" with a close button (X) in the top right corner. The main text explains that this feature allows determining which license to use when users launch an app or desktop on their devices, and that the selected license is a site license applying to all Delivery Groups except those configured with a different license. Below this, there is a section labeled "Select a license to use:" followed by a dropdown menu currently displaying "DaaS Premium - Per User/Device". At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

可供您选择的可能许可证如下：

- Citrix DaaS Premium –每用户/设备
- Citrix DaaS Premium –并发

- 适用于 Google Cloud 的 Citrix DaaS Premium - 每用户/设备
- 适用于 Google Cloud 的 Citrix DaaS Premium —并发
- Citrix DaaS Advanced –每用户/设备
- Citrix DaaS Advanced –并发
- Citrix DaaS Advanced Plus –每用户/设备
- Citrix DaaS Advanced Plus –并发
- 适用于 Azure 的 Citrix DaaS Standard —每用户/设备
- 适用于 Azure 的 Citrix DaaS Standard - 并发
- 适用于谷歌云的 Citrix DaaS 标准——每位用户/设备
- 适用于 Google Cloud 的 Citrix DaaS Standard —并发

如果您只有一个过期的许可证，请联系您的 Citrix 销售代表续订许可证或者购买新许可证。

查看和更新交付组级别的权利

创建或编辑交付组时，可以指定希望交付组使用的许可证。在许可证分配页面上，选择一个选项。

**Create Delivery Group**

**License Assignment**

Determine which license you want this delivery group to use. By default, this delivery group uses the site license.

Select a license you want this delivery group to use:

☒ Use the site license ?  
Citrix DaaS Premium - Per User/Device

☐ Use a different license ?  
Select a license

Back Next Cancel

选项:

- 使用站点许可证。站点许可证适用于所有交付组，但配置了不同许可证的交付组除外。此选项下显示的许可证是正在使用的站点许可证。要配置站点许可证，请转至“管理”>“完整配置”，选择“设置”节点，然后编辑“分配



许可证”。

- 使用其他许可证。此选项允许您将此交付组配置为使用与站点许可证不同的许可证。请记住，许可证权利是产品代码、版本和许可模式的组合。交付组必须使用与站点相同的许可证版本（Standard、Premium 或 Advanced）。如果已配置，交付组将仅使用选定的许可证。即使选定的许可证已完全使用或已失效，交付组也不会回退到站点许可证。

默认情况下，交付组使用站点许可证。

当交付组许可证过期且不再有效时，请使用其他许可证。

注意：

如果以后将交付组配置为使用其他许可证，使用当前许可证的已连接用户可能会暂时失去对其桌面和应用程序的访问权限。

### 混合应享权利的示例

例如，假设客户 A 最初购买了 Advanced 版，后来又购买了 Advanced Plus 版。在这种情况下，客户 A 仍然仅拥有高级版的全站许可证。Citrix 不会修改最初由客户 A 在站点级别设置的设置。客户 A 负责在站点级别将许可证版本修改为 Advanced Plus。

同样，客户 A 也可以在交付组中将许可证版本更新为 Advanced Plus。如果未配置此设置，则交付组将继承在站点级别设置的许可证版本。

客户 A 的管理员可以使用以下方式更新许可证版本：

- 更新站点级许可证版本-转至“管理”>“完整配置”，选择“设置”节点，然后编辑“分配许可证”。
- 更新交付组级别的许可证版本-转到“管理”>“完整配置”，选择“交付组”节点。编辑目标交付组以进行更改。

### 使用 PowerShell 命令更新交付组

用于更新交付组的 PowerShell 命令如下：

```
1 Set-BrokerDesktopGroup -Name <DGName> -ProductCode <Name of the product
   code> -LicenseModel <The type of license model>
2 <!--NeedCopy-->
```

根据您的详细信息更新上述命令。

例如，请参阅以下内容：

- `Set-BrokerDesktopGroup -Name DG1 -ProductCode VADS -LicenseModel CONCURRENT`
- `Set-BrokerDesktopGroup -Name DG1 -ProductCode $null -LicenseModel $null`（将交付组级别配置设置为在站点级别设置的配置）
- `Set-BrokerSite -CloudSiteLicense VADS:ADVANCED:USERDEVICE`

请考虑许可证模式和产品代码不是在交付组级别设置的。在这种情况下，在站点级别设置的这两个属性用于交付组。

有关 Citrix DaaS Remote PowerShell SDK 的更多信息，请参阅 [SDK](#) 和 [API](#) 文档。

#### 更多信息

- [Licenses](#)
- [创建交付组](#)
- [管理交付组](#)

## 平衡计算机负载

December 6, 2023

#### 注意：

此功能适用于所有目录 - 单会话操作系统或多会话操作系统目录。垂直负载平衡仅适用于多会话操作系统计算机。

可以在站点级别和交付组级别配置负载平衡。您有两种选择：垂直和水平。默认情况下，启用水平负载平衡。

#### 站点级别的负载平衡设置

- 垂直负载平衡。将传入用户会话分配给尚未达到最大负载的负载最多的计算机。这将使现有计算机饱和，然后再转移到新计算机。用户断开与现有计算机的连接会释放这些计算机上的容量。然后将传入的负载分配给这些计算机。垂直负载平衡会使用户体验降级，但降低了成本（会话最大限度地提高了已打开电源的计算机容量）。

示例：您有两台计算机，每台计算机配置了 10 个会话。第一台计算机处理前 10 个并发会话。第二台计算机处理第十一个会话。

#### 提示：

要指定计算机可以托管的最大会话数，请使用 [最大会话数](#) 策略设置。

或者，也可以使用 PowerShell 在整个站点中启用或禁用垂直负载平衡。使用 `Set-BrokerSite cmdlet` 中的 `UseVerticalScalingForRdsLaunches` 设置。使用 `Get-BrokerSite` 显示 `UseVerticalScalingForRdsLaunches` 设置的值。有关详细信息，请参阅 `cmdlet` 帮助。

- 水平负载平衡。将传入用户会话分配给已打开电源且负载最少的可用计算机。水平负载平衡可改善用户体验，但会增加成本（因为更多的计算机保持开机状态）。默认情况下，启用水平负载平衡。

示例：您有两台计算机，每台计算机配置了 10 个会话。第一台计算机处理五个并发会话。第二台计算机也处理五个并发会话。

要配置此功能，请从管理 > 完整配置中选择左侧窗格中的设置。在负载平衡多会话目录下选择一个选项。

## 交付组级别的负载均衡设置

在交付组级别配置负载均衡允许您改写从站点级别继承的负载均衡设置。在交付组级别选择垂直负载均衡时，可以实现每台计算机的最大利用率。这将有助于降低公有云的成本。此配置可以在创建新的交付组或编辑现有交付组期间完成。

水平负载均衡。会话分布在开启的计算机之间。例如，如果您将两台计算机分别配置为 10 个会话，则第一台计算机处理五个并发会话，第二台计算机也处理五个并发会话。

垂直负载均衡。会话可以最大限度地提高开机计算机容量并节省计算机成本。例如，如果您将两台计算机分别配置为 10 个会话，则第一台计算机处理前 10 个并发会话。第二台计算机处理第十一个会话。

## 本地主机缓存

February 20, 2024

### 提示：

在 [完整配置](#) > 主页中，服务运行状况警报功能为您提供主动警报，以确保您的本地主机缓存和区域配置正确。因此，当发生中断时，本地主机缓存可以正常工作，您的用户不会受到影响。警报分为两个级别：显示在“主页”（旗帜图标）中的站点范围警报，以及每个区域的“故障排除”选项卡上显示的区域相关警报。有关详细信息，请参阅 [区域](#)。

本地主机缓存允许在 Cloud Connector 无法与 Citrix Cloud 通信时继续在 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）部署中执行连接代理操作。当网络连接断开 60 秒时，本地主机缓存将参与进来。

启用了本地主机缓存时，中断时已连接的用户可以继续工作而不中断。重新连接和新连接会遇到最短连接延迟。

### 重要提示：

如果使用本地 StoreFront 部署，则必须将所有已向其注册（或可能有）VDA 的 Cloud Connector 作为 Delivery Controller 添加到 StoreFront 中。未添加到 StoreFront 的 Cloud Connector 无法转换为中断模式，这可能会导致用户启动失败。

对于没有本地 StoreFront 的部署，请使用服务连续性 Citrix Workspace 平台功能，允许用户在中断期间连接到资源。有关详细信息，请参阅 [服务连续性](#)。

## 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）的标识。

- 主动使用 Citrix Workspace 应用程序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：

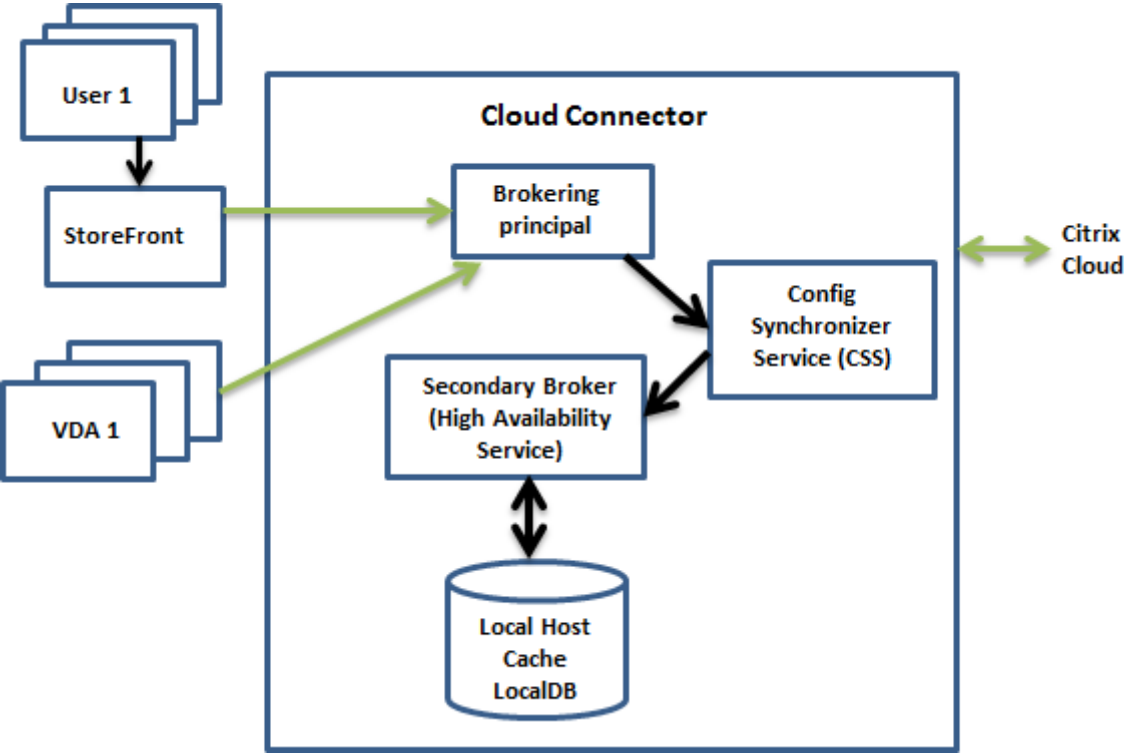
- Citrix Workspace 应用程序执行的任何客户端计算机端点分析的结果。
- 站点涉及的基础结构计算机（例如 Citrix Gateway 和 StoreFront 服务器）的标识。
- 用户进行的最近活动的日期、时间和类型。

工作原理

查看本地主机缓存如何与 Citrix Cloud 交互。

这是一个嵌入式视频。单击链接观看视频

正常操作过程中



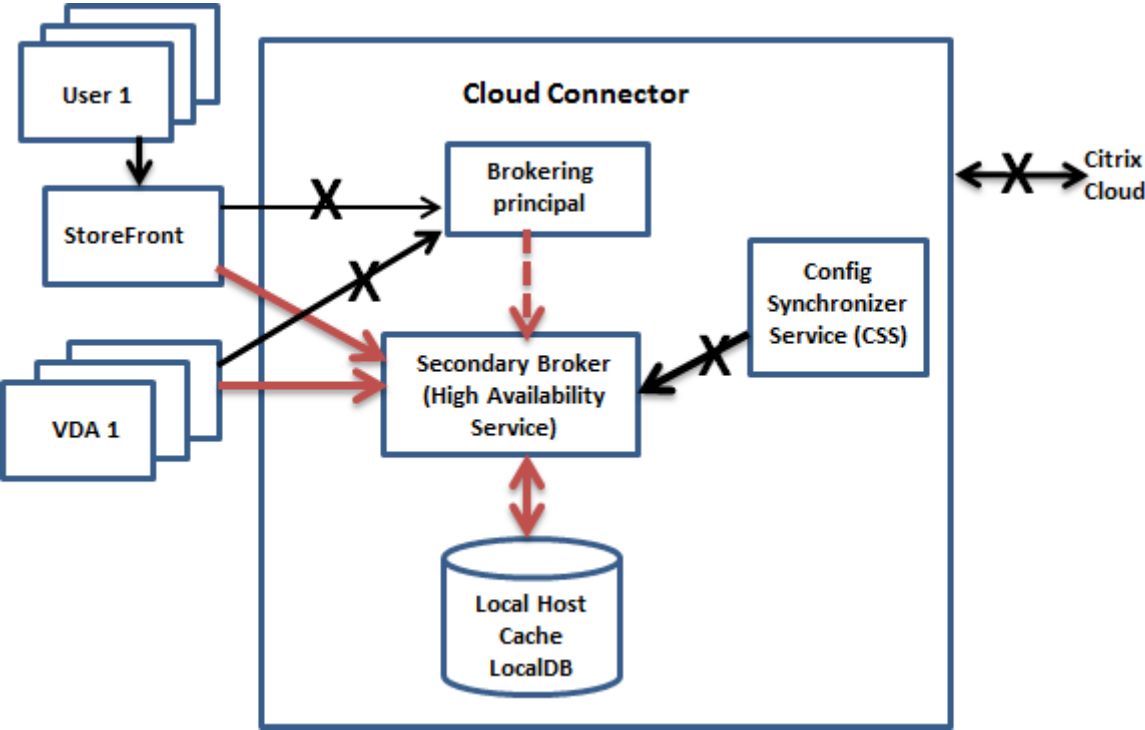
- Cloud Connector 上的代理主体（又称为 Citrix Remote Broker Provider Service）接受来自 StoreFront 的连接请求。代理主体与 Citrix Cloud 进行通信，以将用户与已注册到 Cloud Connector 的 VDA 连接起来。
- Citrix 配置同步器服务 (CSS) 大约每 5 分钟向 Citrix Cloud 中的代理检查一次，以查看是否进行了任何配置更改。这些更改可能是管理员发起的更改（例如，更改交付组属性）或系统操作（例如，计算机分配）。
- 如果自上次检查后更改了配置，CSS 会将信息同步（复制）到 Cloud Connector 上的辅助 Broker。（如上图所示，辅助 Broker 也称为高可用性服务或高可用性 Broker。）

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 Cloud Connector 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 Citrix Cloud 中的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 Cloud Connector 时，Microsoft SQL Server Express LocalDB（由本地主机缓存数据库使用）会自动安装。本地主机缓存数据库不能跨 Cloud Connector 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。

- 如果自上次核对后没有进行任何更改，则不复制配置数据。

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。
- 在辅助代理处理连接的同时，代理主体将继续监视与 Citrix Cloud 的连接。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 Citrix Cloud 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。

事件日志指示何时发生同步和中断。

对中断模式下的操作没有时间限制。

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 **Cloud Connector** 的资源位置

除其他任务外，CSS 还定期向辅助代理提供与资源位置中所有 Cloud Connector 有关的信息。获取该信息后，每个辅助代理都将知晓资源位置中的其他 Cloud Connector 上运行的所有对等辅助代理。

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 重新注册。区域中的非选定辅助 Broker 将主动拒绝传入连接和 VDA 注册请求。

重要提示：

资源位置内的连接器必须能够在以下位置相互连接：[http://<FQDN\\_OF\\_PEER\\_CONNECTOR>:80/Citrix/CdsController/ISecondaryBrokerElection](http://<FQDN_OF_PEER_CONNECTOR>:80/Citrix/CdsController/ISecondaryBrokerElection)。如果连接器无法在此地址通信，则可能会选择多个代理，并且在本地主机缓存事件期间可能会出现间歇性启动失败。

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 Cloud Connector：

- 如果该 Cloud Connector 不是选定的代理，则重新启动没有任何影响。
- 如果该 Cloud Connector 是选定的代理，则将选择另一个 Cloud Connector，这会导致 VDA 进行注册。重新启动的 Cloud Connector 开启后，将自动接管代理，这会导致 VDA 重新注册。在这种情况下，在注册期间，性能会受影响。

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，如果中断是由于其资源位置中的 Citrix Cloud 连接断开导致的，Citrix 建议尽快从资源位置恢复连接。

中断过程中：

- 不能使用管理界面。
- 您对 Remote 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`
  - ★ 将 SDK 身份验证设置为 `OnPrem`, 以便 SDK 代理不会尝试重定向 cmdlet 调用: `$XDSDKAuth = "OnPrem"`
  - ★ 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。

- 中断期间, 监视数据将发生送到 Citrix Cloud。因此, **Monitor** 功能将不显示中断时间间隔内的活动。
- 无法从 Host Service 获取虚拟机管理程序凭据。所有计算机都处于未知电源状态, 因此无法发出任何电源操作。但是, 已打开电源的主机上的 VM 可以用于连接请求。
- 仅当在正常操作过程中发生了分配时, 才可以使用分配的计算机。在中断期间不能执行新分配。
- 不能自动注册和配置 Remote PC Access 计算机。但是, 正常操作过程中注册和配置的计算机可以使用。
- 如果资源在不同的区域中, 服务器托管的应用程序和桌面用户使用的会话可能超过其配置的会话限制。
- 用户只能从包含当前处于活动状态的/选定的代理的区域中已注册的 VDA 启动应用程序和桌面。断电期间不支持跨区域启动 (从一个区域中的 Broker 到另一个区域中的 VDA)。
- 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。此方案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记来指定资源位置的[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。

## StoreFront 要求

如果使用本地 StoreFront 部署, 则必须将所有已向其注册 (或可能有) VDA 的 Cloud Connector 作为 Delivery Controller 添加到 StoreFront 中。未添加到 StoreFront 的 Cloud Connector 无法转换为中断模式, 这可能会导致用户启动失败。

### 资源可用性

可以通过以下两种方式确保资源 (应用程序和桌面) 在中断期间的可用性:

- 在您的部署中的每个资源位置发布资源。

- 如果您使用的是 StoreFront 1912 CU4 或更高版本，请将资源发布到至少一个资源位置，并在所有 StoreFront 服务器上启用高级运行状况检查。对于 StoreFront 2308 之前的版本，高级运行状况检查默认处于关闭状态，并且必须由管理员启用。对于 StoreFront 版本 2308 及更高版本，此功能默认处于启用状态。有关开启高级运行状况检查的更多信息和说明，请参阅 [高级运行状况检查](#)。

## 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（单会话）VDA，如下所示。

- 默认情况下，在本地主机缓存事件期间，池交付组（由 MCS 或 Citrix Provisioning 创建）中启用了 `ShutdownDesktopsAfterUse` 属性的电源管理桌面 VDA 不可用于新连接。您可以更改此默认值，以允许在本地主机缓存期间使用这些桌面。

但是，中断期间您将不可避免地无法依赖电源管理。（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，必须使用 PowerShell 命令在站点范围内启用并针对受影响的每个交付组启用。

对于整个站点，请运行以下命令：

```
Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
```

默认情况下，没有为此功能启用所有交付组。可以通过两个选项在交付组级别将其启用：

- **Enable for selected delivery groups**（为选定交付组启用）：对于受影响的每个交付组，请运行以下命令。

```
Set-BrokerDesktopGroup -Name "name"-ReuseMachinesWithoutShutdownInOutageAllowed $true
```

- **Enable for all delivery groups**（对所有交付组启用）：要在默认情况下启用交付组级别设置，请运行以下命令。此设置适用于新创建的所有交付组（即，启用此设置后创建的所有交付组）。

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutageAllowed $true
```

要为现有交付组启用此功能，请运行上文提到的命令 (`Set-BrokerDesktopGroup -Name "name"-ReuseMachinesWithoutShutdownInOutageAllowed $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。

### 重要提示：

如果不在站点级别启用 `ReuseMachinesWithoutShutdownInOutageAllowed` 以及不在交付组级别启用 `ReuseMachinesWithoutShutdownInOutage`，则在本地主机缓存事件期间，尝试对池化交付组中受电源管



理的桌面 VDA 启动所有会话都将失败。

## 验证本地主机缓存是否正在运行

查看如何验证本地主机缓存是否正确配置。

这是一个嵌入式视频。单击链接观看视频

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：

- 如果使用 StoreFront，请验证本地 StoreFront 部署是否指向该资源位置中的所有 Cloud Connector。
- 确保同步导入成功完成。检查事件日志。
- 确保在每个 Cloud Connector 上创建本地主机缓存数据库。这确认了如果需要，高可用性服务可以接管。
  - 在 Cloud Connector 服务器上，浏览至 `c:\Windows\ServiceProfiles\NetworkService`。
  - 验证 `HaDatabaseName.mdf` 和 `HaDatabaseName_log.ldf` 是否已创建。
- 在资源位置中的所有 Cloud Connector 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 Cloud Connector 放回普通模式。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。每次从 Citrix Cloud 接收更新的配置时都会发生此事件。它指示同步过程的开始。
- 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。
- 3507: 每隔 2 分钟更新一次本地主机缓存的状态, 指示本地主机缓存模式在选定代理上处于活动状态。包含中断摘要, 包括中断持续时间、VDA 注册和会话信息。
- 3508: 宣布本地主机缓存在选定代理上不再处于活动状态, 并且已恢复正常操作。包含中断摘要, 包括中断持续时间、在本地主机缓存事件期间注册的计算机数以及在 LHC 事件期间成功启动的次数。
- 3509: 通知本地主机缓存在非选定代理上处于活动状态。包含每隔 2 分钟中断一次的持续时间, 并指明选定代理。
- 3510: 宣布本地主机缓存在非选定代理上不再处于活动状态。包含中断持续时间并指明选定代理。

### 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。

尽管在强制停机期间可以更新 Cloud Connector, 但可能会出现意外问题。建议您为 [Cloud Connector 更新设置一个计划](#), 以避免出现强制中断模式时间间隔。

要强制中断, 请编辑每个 Cloud Connector 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, 而无论与 Citrix Cloud 的连接状态为何。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。这些选项与其他代理模块一起可以确定问题。

报告: 如果同步导入失败, 您可以生成报告。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
```

本地主机缓存 **PowerShell** 命令

您可以使用 PowerShell 命令管理 Cloud Connector 上的本地主机缓存。

PowerShell 模块位于 Cloud Connector 上的以下位置：

```
C:\Program Files\Citrix\Broker\Service\ControlScripts
```

重要提示：

请仅在 Cloud Connector 上运行此模块。

导入 **PowerShell** 模块 要导入模块，请在 Cloud Connector 上运行以下命令：

```
cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-Module .\HighAvailabilityServiceControl.psm1
```

用于管理 **LHC** 的 **PowerShell** 命令 以下 cmdlet 可帮助您在 Cloud Connector 上激活和管理 LHC 模式。

| cmdlet                                   | 功能                                                                                                                                                                                                |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>Enable-LhcForcedOutageMode</code>  | 将代理置于 LHC 模式。适用于 <code>Enable-LhcForcedOutageMode</code> 的 ConfigSync 服务必须成功创建本地主机缓存数据库文件才能正常运行。这个 cmdlet 仅在运行它的 Cloud Connector 上强制使用 LHC。要使 LHC 处于活动状态，必须在资源位置内的所有 Cloud Connector 上运行此 cmdlet。 |
| <code>Disable-LhcForcedOutageMode</code> | 使代理退出 LHC 模式。此 cmdlet 仅在运行它的 Cloud Connector 上禁用 LHC 模式。 <code>Disable-LhcForcedOutageMode</code> 必须在资源位置内的所有 Cloud Connector 上运行。                                                                |

| cmdlet                                              | 功能                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Set-LhcConfigSyncIntervalOverride</a>   | 设置 Citrix Config Synchronizer Service (CSS) 检查 Citrix DaaS 站点内的配置更改的时间间隔。时间间隔可以从 60 秒（一分钟）到 3600 秒（一小时）不等。此设置仅适用于运行该设置的 Cloud Connector。为了确保 Cloud Connector 之间的一致性，请考虑在每个 Cloud Connector 上运行此 cmdlet。例如：<br><a href="#">Set-LhcConfigSyncIntervalOverride -Seconds 1200</a> |
| <a href="#">Clear-LhcConfigSyncIntervalOverride</a> | 将 Citrix 配置同步器服务 (CSS) 检查 Citrix DaaS 站点内的配置更改的时间间隔设置为默认值 300 秒（五分钟）。此设置仅适用于运行该设置的 Cloud Connector。为了确保 Cloud Connector 之间的一致性，请考虑在每个 Cloud Connector 上运行此 cmdlet。                                                                                                            |
| <a href="#">Enable-LhcHighAvailabilitySDK</a>       | 允许访问其运行时所在的 Cloud Connector 中的所有 <a href="#">Get-Broker*</a> cmdlet。                                                                                                                                                                                                          |
| <a href="#">Disable-LhcHighAvailabilitySDK</a>      | 禁止访问运行的 Cloud Connector 中的 Broker PowerShell 命令。                                                                                                                                                                                                                              |

注意：

- 在 Cloud Connector 上运行 [Get-Broker\\*](#) cmdlet 时使用端口 89。例如：
  - [Get-BrokerMachine -AdminAddress localhost:89](#)
- 不处于 LHC 模式时，Cloud Connector 上的 LHC Broker 仅保存配置信息。
- 在 LHC 模式下，选定的 Cloud Connector 上的 LHC Broker 会保存以下信息：
  - 资源状态
  - 会话详细信息
  - VDA 注册情况
  - 配置信息

更多信息

请参阅[本地主机缓存的规模和大小注意事项](#)，以了解以下相关信息：

- 测试方法和结果
- RAM 大小注意事项
- CPU 核心和套接字配置注意事项
- 存储注意事项

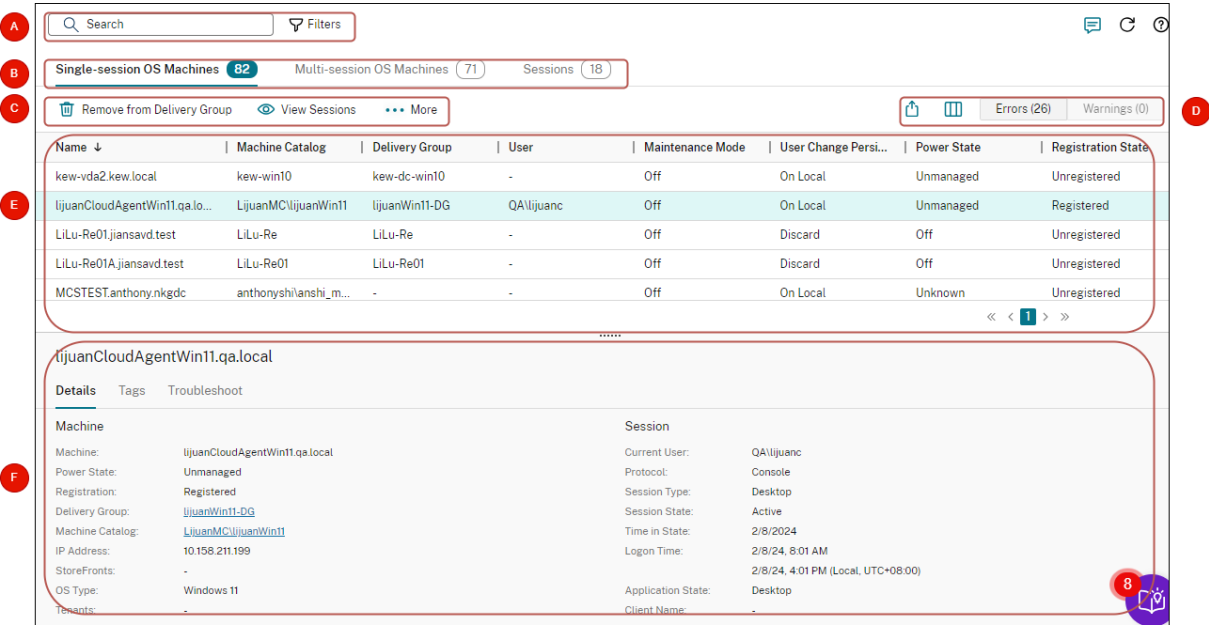
使用搜索监视和管理计算机和会话

March 30, 2024

本文指导您了解如何使用“完整配置” > “搜索”节点监视和管理计算机和会话。

了解该节点

搜索节点为监视和管理计算机和用户会话提供了一个中心位置。



| 标注 | 区域    | 说明                                                                                   |
|----|-------|--------------------------------------------------------------------------------------|
| A  | 搜索栏   | 提供快速搜索和基于筛选器的搜索，允许您定义复杂的搜索条件。有关详细信息，请参阅：<br>搜索实例                                     |
| B  | 键入选项卡 | 显示选项卡，按类型列出计算机或列出所有会话。实例计数显示在选项卡名称中。                                                 |
| C  | 实例级操作 | 显示可以在选定实例（计算机或会话）上执行的操作。有关详细信息，请参阅：<br><a href="#">计算机操作</a><br><a href="#">会话操作</a> |

| 标注 | 区域     | 说明                                                                                                                                                                                                                                                                              |
|----|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| D  | 列表级操作  | <p>显示可以在当前列表上执行的操作：</p> <ul style="list-style-type: none"><li>• 导出图标：将主视图中显示的实例列表导出到 CSV 文件中。</li><li>• 显示栏图标：自定义列表的主视图。</li><li>• 错误标签：启用此标签可在主视图中仅显示有错误的未注册计算机。要查看问题详细信息，请转到详细信息窗格中的故障排除选项卡。</li><li>• 警告标签：启用此标签可在主视图中仅显示带有警告的未注册计算机。要查看问题详细信息，请转到详细信息窗格中的故障排除选项卡。</li></ul> |
| E  | 主视图    | <p>显示实例及其属性。您可以通过选择“要显示的列”图标来自定义主视图。有关可用列的更多信息，请参阅：<br/><a href="#">计算机列</a><br/><a href="#">会话列</a></p>                                                                                                                                                                        |
| F  | 详细信息窗格 | <p>显示以下详细信息：</p> <ul style="list-style-type: none"><li>• 所选实例（计算机或会话）的详细信息</li><li>• 应用于所选计算机的标签</li><li>• 所选计算机的错误或警告的详细信息，包括问题、可能的原因和建议的解决方案</li></ul>                                                                                                                        |

搜索实例

使用搜索功能查找特定的计算机和会话：

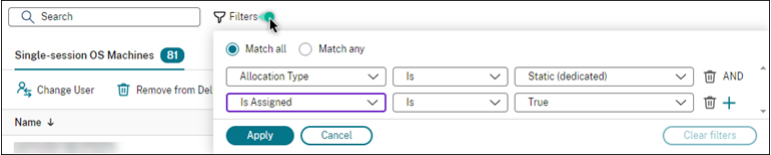
- 使用过滤器进行搜索
- 保存当前过滤器集以便快速搜索
- 在搜索栏中固定筛选器字段
- 使用快速搜索框进行搜索

- 可加快搜索速度的提示

使用过滤器进行搜索

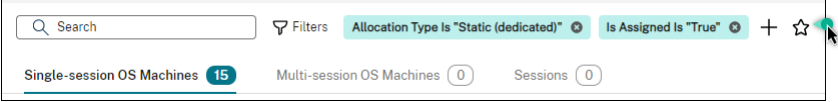
例如，要找到所有静态且分配给用户的单会话操作系统计算机，请执行以下步骤：

1. 在单会话操作系统计算机选项卡上，单击过滤器图标。将出现“过滤器”面板。
2. 添加必要的筛选条件。



3. 如果您希望搜索返回全部匹配筛选条件的结果，请选择“全部匹配”（AND 运算符）。如果您希望搜索返回与任何筛选条件匹配的结果，请选择匹配任意（OR 运算符）。
4. 单击应用。

筛选列表显示所有静态且分配给用户的单会话操作系统计算机。

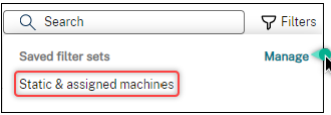


保存当前过滤器集以便快速搜索

例如，要保存为静态并分配给用户以备将来使用的单会话操作系统计算机的过滤器设置，请执行以下步骤：

1. 执行基于筛选器的搜索后，单击搜索栏中的星形图标，如上图所示。
2. 在出现的页面上，输入该筛选器集的名称（例如，静态和分配的计算机）。
3. 单击保存。

当您单击搜索框时，保存的过滤器集将出现在搜索历史列表中。



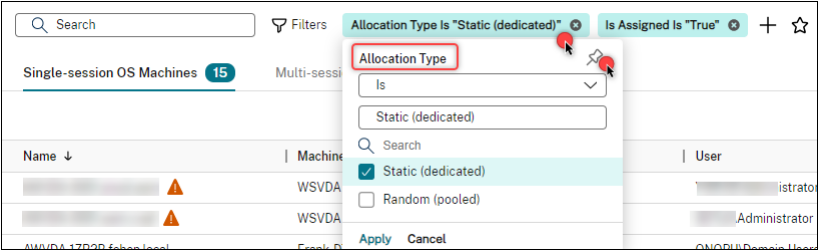
注意：

过滤器集以每个用户帐户为基础保存。要管理已保存的过滤器集，请选择管理。

在搜索栏中固定筛选器字段

将常用的筛选字段固定在搜索栏中以便于访问。例如，在进行基于筛选器的搜索后，您想将“分配类型”固定在搜索栏中。请按照以下步骤进行操作：

1. 单击搜索栏中的筛选器设置。
2. 在出现的面板中，单击“固定”图标将筛选器字段（本示例中的分配类型）固定在搜索栏中。



### 使用快速搜索框进行搜索

快速搜索框为根据与名称相关的属性或保存的过滤器集合搜索实例提供了一种便捷的方式。详细步骤如下所示：

1. 点击搜索框。您最近的搜索和保存的过滤器集显示在下拉列表中。您可以单击之前的搜索或筛选器集进行快速搜索。
2. 要开始新的搜索，请从以下选项中输入完整或部分名称：
  - 计算机名或 DNS 名称
  - 计算机目录名称
  - 交付组名称
  - 会话用户名
  - 会话客户端名称
  - 托管会话的虚拟机的友好名称，由其虚拟机管理程序使用
  - 托管服务器名称

### 可加快搜索速度的提示

使用搜索功能时，请注意以下提示：

- 在搜索节点上，选择任意列以对项目进行排序。
- 要在可以执行搜索和排序的显示画面中显示更多特性，请选择要显示的列或者单击任意列，然后选择要显示的列。在“要显示的列”窗口中，选中要显示的项目旁边的复选框，然后选择“保存”退出。

注意：

性能下降的列标有降级性能标签。

- 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，请在左侧窗格中选择交付组。选择该组，然后从操作栏或上下文菜单中选择“查看计算机”。



执行排序操作时，请记住以下注意事项：

- 只要项目数量不超过 5000，就可以单击任意列对其中的项目进行排序。当数量超过 5000 时，您只能按名称或当前用户（取决于您所在的选项卡）进行排序。要启用排序功能，请使用筛选条件将项目数量减少到 5000 个或更少。
- 当项目数量大于 500 但不超过 5000 时：
  - 我们在本地缓存所有数据以提高排序性能。在单会话操作系统计算机和多会话操作系统计算机选项卡上，当您首次单击某个列（名称列以外的任何列）进行排序时，我们将缓存数据。在会话选项卡上，首次单击要排序的列（当前用户列之外的任何列）时，我们将缓存数据。因此，这种排序需要更长的时间才能完成。为了提高性能，请按名称或当前用户进行排序，或使用过滤器减少项目数量。
  - 表下的以下消息指示已缓存数据：上次刷新时间：<the time when you refreshed the table>。在这种情况下，排序操作将基于之前加载的项目。这些项目可能不是最新的。要使其更新到最新状态，请单击刷新图标。

## 自定义要显示的列

创建个性化主视图以显示对您的日常运营至关重要的属性和状态。详细步骤如下所示：

1. 在搜索节点中，根据需要选择多会话操作系统计算机、单会话操作系统计算机或会话选项卡。
2. 在操作栏中单击“显示列”图标，然后选择列。

有关可用列及其描述的更多信息，请参阅[计算机列](#)和[会话列](#)。

选择列时，您可以看到标有降级性能标签的列。选择这些列可能会降低控制台的性能。请记住以下注意事项：

- 完成自定义后，表会刷新以显示您选择的列。当您刷新表时，显示这些列可能会导致延迟。
- 刷新浏览器或注销控制台然后登录后，会出现一条消息，询问是否保留这些列。如果您选择保留它们，则只能每分钟刷新表格一次以获得最佳的主机性能。要更频繁地刷新，请移除所有会降低性能的列。

## 管理计算机和会话

使用搜索节点中的操作对计算机和会话问题进行故障排除或处理用户请求。

### 须知

您可以管理不同级别的计算机：

- 在单台计算机层面。使用搜索节点查找目标计算机并执行操作。
- 在计算机目录级别，例如更改目录的主映像、从目录中删除计算机以及将计算机添加到目录中。有关详细信息，请参阅[管理计算机目录](#)。

- 在交付组级别，例如打开或关闭组中计算机的维护模式。有关详细信息，请参阅[管理交付组](#)。

除了单个会话级别外，您还可以在交付组级别管理会话，例如为交付组配置会话预启动和延迟。有关详细信息，请参阅[管理交付组](#)。

### 在计算机或会话上执行操作

要在单个实例级别管理计算机或会话，请执行以下步骤：

1. 在搜索节点中，选择多会话操作系统计算机、单会话操作系统计算机或会话选项卡。
2. 根据需要选择一个或多个实例。
3. 从操作栏或右键单击菜单中，根据您在这些实例或用户请求中遇到的问题选择操作。

有关可用操作及其描述的更多信息，请参阅[计算机操作](#)和[会话操作](#)。

#### 注意：

如果您选择两个或更多实例，则只有适用于所有实例的操作才可用。

### 将计算机或会话数据导出到 **CSV** 文件

将选项卡上显示的实例（计算机或会话）列表（最多 30,000 个项目）导出到 CSV 文件中。详细步骤如下所示：

1. 在搜索节点中，根据需要选择多会话操作系统计算机、单会话操作系统计算机或会话选项卡。
2. 单击右上角的导出图标。
3. 在出现的对话框中，单击“继续”。

导出可能需要几分钟才能完成。您可以在浏览器的默认下载文件夹中找到该文件。

#### 注意：

在搜索节点的每个选项卡上，在导出过程中，您无法再执行一次导出。

## 计算机操作和列

March 30, 2024

本文列出了计算机操作和带有说明的列供您参考。

操作

查看可以在计算机上执行的操作及其描述。

| 操作      | 说明                                                                                            | 适用对象                   |
|---------|-----------------------------------------------------------------------------------------------|------------------------|
| 运行健康检查  | 仅适用于已注册的 Windows VDA，版本 2019 或更高版本。在计算机上运行运行状况检查。有关检查内容的更多信息，请参阅：<br><a href="#">关于运行状况检查</a> | 单会话和多会话                |
| 从交付组中移除 | 从交付组中移除一台计算机。                                                                                 | 单会话和多会话                |
| 添加到交付组  | 将计算机添加到交付组。                                                                                   | 单会话和多会话                |
| 查看会话    | 查看在计算机上运行的会话                                                                                  | 单会话和多会话                |
| 管理标记    | 为计算机添加和管理标签。有关标签典型用例的更多信息，请参阅：<br><a href="#">标记</a>                                          | 单会话和多会话                |
| 打开维护模式  | 在应用补丁或进行故障排除之前，将计算机置于维护模式。<br>此模式可防止与该计算机建立新连接。<br>用户可以连接到该计算机上的现有会话，但他们无法在该计算机上启动新会话。        | 单会话和多会话                |
| 关闭维护模式  | 关闭计算机的维护模式。                                                                                   | 单会话和多会话                |
| 升级 VDA  | 升级计算机的 VDA。<br><br><a href="#">了解更多</a>                                                       | 满足特定要求的单会话或多会话操作系统计算机： |
| 注销      | 强制注销计算机                                                                                       | 单会话和多会话                |
| 删除      | 将虚拟机从计算机目录中删除，同时在虚拟机管理程序或云服务上保持不变。                                                            | 单会话和多会话                |
| 更改用户    | 将计算机分配给特定用户。                                                                                  | 单会话静态计算机。              |
| 启动      | 启动一台计算机。                                                                                      | 单会话和多会话                |
| 关闭      | 关闭一台计算机。                                                                                      | 单会话和多会话                |
| 重新启动    | 重启计算机                                                                                         | 单会话和多会话                |

| 操作     | 说明                                                    | 适用对象       |
|--------|-------------------------------------------------------|------------|
| 挂起     | 将计算机置于休眠或暂停状态。当您暂停计算机时，DaaS 会将计算机的内存内容存储在文件中，然后关闭计算机。 | 单会话操作系统计算机 |
| 继续     | 恢复已暂停的计算机。当您恢复已挂起的计算机时，DaaS 会启动该计算机并将其恢复到以前的状态。       | 单会话操作系统计算机 |
| 强制重新启动 | 强制重启计算机。                                              | 单会话操作系统计算机 |
| 强制关闭   | 强制关闭计算机。                                              | 单会话操作系统计算机 |

列

按类型查看所有计算机列及其描述：

- 计算机
- 计算机详细信息
- 应用程序
- 托管
- 连接
- 注册
- 会话详细信息
- 会话

计算机

“计算机”类别中的列。

| 列     | 说明            | 适用对象    |
|-------|---------------|---------|
| 名称    | 计算机的 DNS 主机名。 | 单会话和多会话 |
| 计算机目录 | 计算机所属目录的名称。   | 单会话和多会话 |
| 交付组   | 计算机所属交付组的名称。  | 单会话和多会话 |

| 列            | 说明                                                                                                                | 适用对象    |
|--------------|-------------------------------------------------------------------------------------------------------------------|---------|
| 用户显示名称       | 与计算机关联的用户的全名（通常采用格式 <code>Firstname Lastname</code> ）。关联用户是共享计算机的当前用户和专用计算机的分配用户。                                 | 单会话和多会话 |
| 用户           | 与计算机关联的用户的用户名（采用“域\用户”形式）。关联用户是共享计算机的当前用户和专用计算机的分配用户。                                                             | 单会话和多会话 |
| 用户主体名称       | 与计算机关联的用户的用户主名（采用“user@domain”形式）。关联用户是共享计算机的当前用户和专用计算机的分配用户。                                                     | 单会话和多会话 |
| 桌面显示名称       | 最初用于启动会话的计算机的已发布名称。它是 Citrix Workspace 应用程序或 StoreFront 上显示的名称。<br>注意：要更改桌面的显示屏，您需要“执行计算机更新”权限，因为更改显示名称涉及更新计算机属性。 | 仅限单会话   |
| 桌面状况         | 计算机的出色桌面条件列表。可能的值：Unknown、CPU、ICALatency 和 UPMLogonTime。                                                          | 单会话和多会话 |
| 分配类型         | 计算机的分配类型：永久分配，永久分配给用户时。随机分配时随机。                                                                                   | 单会话和多会话 |
| 维护模式         | 表示计算机是否处于维护模式。                                                                                                    | 单会话和多会话 |
| Windows 连接设置 | Windows 报告的登录模式。<br><br>可能的值：“LogonEnabled”、“Draining”、“DrainingUntilRestart”和“LogonDisabled.”。                   | 仅限多会话   |
| 已分配          | 表示是否已将专用桌面分配给用户或客户端（名称/地址）。可以明确分配用户，也可以通过在首次使用计算机时分配来分配用户。                                                        | 单会话和多会话 |

| 列      | 说明                                                                                                                                                                                                               | 适用对象    |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| 物理     | 表示计算机是否为物理计算机。<br><b>True</b> 表示该计算机是物理计算机，这意味着它不由 DaaS 进行电源管理。<br><b>False</b> 表示其他情况。                                                                                                                          | 单会话和多会话 |
| 预配类型   | 计算机的配置方式。可能的值： <ul style="list-style-type: none"> <li>• 手动：未使用 PVS 或 MCS 进行预配。</li> <li>• PVS：使用 PVS（物理机、刀片机和虚拟机）进行配置</li> <li>• MCS：使用 MCS 进行配置（仅限 VM）</li> </ul>                                               | 单会话和多会话 |
| 预定重启   | 计算机的任何预定重启操作的状态。<br>可能的值： <ul style="list-style-type: none"> <li>• 无：未计划重启。</li> <li>• 待定：正在等待重启但可供使用。</li> <li>• 耗尽：正在等待重启，新会话不可用。但是，仍然允许重新连接到现有连接。</li> <li>• 进行中：正在按计划重启。</li> </ul> -自然：自然重启正在进行中。计算机正在等待重启。 | 单会话和多会话 |
| 区域     | 计算机所在区域的名称。                                                                                                                                                                                                      | 单会话和多会话 |
| 状态     | 与计算机相关的桌面的整体状态，源自各种特定状态，例如会话状态、注册状态和电源状态。<br>可能的状态：关闭、未注册、可用、已断开连接、InUse 和准备中。                                                                                                                                   | 单会话和多会话 |
| 标记     | 与计算机相关的标签列表。                                                                                                                                                                                                     | 单会话和多会话 |
| VDA 升级 | VDA 包升级操作的计算机状态。<br>可能的值：MissingUpgradeType、UpgradeScheduled、UpgradeAvailable、UpToDate 和未知。                                                                                                                      | 单会话和多会话 |
| 可以暂停   | 指明计算机是否支持电源操作（挂起和恢复）。                                                                                                                                                                                            | 单会话和多会话 |

| 列    | 说明                                                                                                 | 适用对象  |
|------|----------------------------------------------------------------------------------------------------|-------|
| 负荷指数 | 当前负荷指数。有关详细信息，请参阅：<br><a href="#">了解更多</a>                                                         | 仅限多会话 |
| 排水状态 | 表示计算机是否正在耗尽电量，是否将在计算机结束所有会话后关闭。<br>True 仅适用于由电源管理的多会话计算机。<br>注意：如果计算机处于维护模式，则不会关闭。它只有在关闭维护模式后才会关闭。 | 仅限多会话 |

计算机详细信息

计算机详细信息类别中的列。

| 列      | 说明                                                         | 适用对象    |
|--------|------------------------------------------------------------|---------|
| 代理版本   | 计算机上安装的 Citrix Virtual Delivery Agent (VDA) 版本。            | 单会话和多会话 |
| IP 地址  | 计算机的 IP 地址。                                                | 单会话和多会话 |
| 已分配    | 表示是否已将专用桌面分配给用户或客户端（名称/地址）。可以明确分配用户，也可以通过在首次使用计算机时分配来分配用户。 | 单会话和多会话 |
| 操作系统类型 | 计算机上运行的操作系统的类型。                                            | 仅限单会话   |

应用程序

“应用程序”类别中的列。

| 列         | 说明                         | 适用对象    |
|-----------|----------------------------|---------|
| 正在使用的应用程序 | 计算机上正在使用的应用程序列表（显示为浏览器名称）。 | 单会话和多会话 |
| 已发布的应用程序  | 计算机发布的应用程序列表（显示为浏览器名称）。    | 单会话和多会话 |

连接

“连接”类别中的列。

| 列             | 说明                                                             | 适用对象    |
|---------------|----------------------------------------------------------------|---------|
| 客户端 (IP)      | 连接到计算机的客户端的 IP 地址。                                             | 仅限单会话   |
| 客户端           | 连接到计算机的客户端的主机名。                                                | 仅限单会话   |
| 插件版本          | 连接的客户端上的 Citrix Workspace 应用程序版本。                              | 仅限单会话   |
| 连接方式          | 传入连接的主机名，通常是网关、路由器或客户端。                                        | 仅限单会话   |
| 通过 (IP) 连接    | 传入连接的 IP 地址，通常是网关、路由器或客户端。                                     | 仅限单会话   |
| 连接类型          | 用于会话的协议。可能的值：HDX、RDP 和控制台。注意：对于 XenDesktop 5 VDA 上的主机会话，该字段留空。 | 仅限单会话   |
| 上次连接时间 (UTC)  | 上次检测到的连接尝试失败或成功的时间。                                            | 单会话和多会话 |
| 上次连接用户        | 上次尝试连接计算机的用户的 SAM 名称（采用“域\用户”形式）。如果 SAM 名称不可用，则使用 SID。         | 单会话和多会话 |
| 安全 ICA 处于活动状态 | 指示 SecureICA 在当前会话中是否处于活动状态。对于多会话计算机，始终为空。                     | 单会话和多会话 |

托管

“主机”类别中的列。

| 列       | 说明                                                    | 适用对象    |
|---------|-------------------------------------------------------|---------|
| VM      | 运行会话的托管计算机的友好名称，由其虚拟机管理程序使用。它不一定与计算机的 DNS 或 AD 名称相匹配。 | 单会话和多会话 |
| 托管服务器名称 | 托管计算机的虚拟机管理程序的 DNS 名称（如果托管）。                          | 单会话和多会话 |
| 连接      | 分配给托管会话的计算机的主机连接的名称。                                  | 单会话和多会话 |



| 列        | 说明                                                                                                                    | 适用对象    |
|----------|-----------------------------------------------------------------------------------------------------------------------|---------|
| 待更新      | 表示托管计算机的虚拟机映像是否已过期，是否将在计算机下次重启时更新为新映像。                                                                                | 单会话和多会话 |
| 用户变更持久性  | 如何处理用户更改，表明更改是否持久： <ul style="list-style-type: none"><li>• OnLocal：持久。用户更改保存在本地。</li><li>• 丢弃：非永久。用户更改将被丢弃。</li></ul> | 单会话和多会话 |
| 待处理的电源操作 | 表示计算机是否有任何待处理的电源操作。                                                                                                   | 单会话和多会话 |
| 电源状态     | 计算机的电源状态。可能的值：Unmanaged、Unknown、Unavailable、Off、On、Suspended、TurningOn、TurningOff、Suspending 和 Resuming。              | 单会话和多会话 |
| 使用后将关闭   | 仅适用于电源管理的单会话计算机。表示计算机是否受污染，是否将在所有会话结束后关闭。<br>注意：如果计算机处于维护模式，则不会关闭。只有在退出维护模式后，它才会关闭。                                   | 仅限单会话   |

注册

注册类别中的列。

| 列      | 说明                | 适用对象    |
|--------|-------------------|---------|
| 上次注册失败 | 最后一次向代理人注销计算机的原因。 | 单会话和多会话 |

| 列              | 说明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 适用对象    |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                | 可能的值为：AgentShutdown、AgentSuspended、AgentRequested、IncompatibleVersion、AgentAddressResolutionFailed、AgentNotContactable、AgentWrongActiveDirectoryOU、EmptyRegistrationRequest、MissingRegistrationCapabilities、MissingAgentVersion、InconsistentRegistrationCapabilities、NotLicensedForFeature、UnsupportedCredentialSecurityVersion、InvalidRegistrationRequest、SingleMultiSessionMismatch、FunctionalLevelTooLowForCatalog、FunctionalLevelTooLowForDesktopGroup、PowerOff、DesktopRestart、DesktopRemoved、AgentRejectedSettingsUpdate、SendSettingsFailure、SessionAuditFailure、SessionPrepareFailure、ContactLost、SettingsCreationFailure、UnknownError 和 BrokerRegistrationLimitReached。 |         |
| 上次注册失败时间 (UTC) | 上次注销计算机的时间。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 单会话和多会话 |
| 注册状态           | 计算机的注册状态。可能的值：Unregistered、Initializing、Registered 和 AgentError。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 单会话和多会话 |
| 故障状态           | 计算机任何当前故障状态的摘要状态。<br>可能的值：                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 单会话和多会话 |

| 列 | 说明                                                                                                                                                                                                                      | 适用对象 |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
|   | <ul style="list-style-type: none"><li>• 无：没有错。计算机正常运行。</li><li>• FailedToStart：计算机的最后一次开机操作失败。</li><li>• StuckOnBoot：计算机在开机后无法启动。</li><li>• 未注册。计算机未能在预期期限内注册或其注册被拒绝。</li><li>• MaxCapacity。计算机正在以最大容量进行自我报告。</li></ul> |      |

会话详细信息

会话详细信息类别中的列。

| 列               | 说明                                               | 适用对象    |
|-----------------|--------------------------------------------------|---------|
| 启动完毕            | 用于启动当前代理会话的 StoreFront 服务器的主机名。对于多会话计算机，始终为空。    | 单会话和多会话 |
| 启动完毕 (IP)       | 用于启动当前代理会话的 StoreFront 服务器的 IP 地址。对于多会话计算机，始终为空。 | 单会话和多会话 |
| 会话更改时间 (UTC)    | 当前会话最后一次状态更改的时间。                                 | 仅限单会话   |
| SmartAccess 过滤器 | 当前会话的智能访问标签。对于多会话计算机，始终为空。                       | 单会话和多会话 |

会话

会话类别中的列。

| 列          | 说明                                                                                                           | 适用对象  |
|------------|--------------------------------------------------------------------------------------------------------------|-------|
| 会话状态       | 当前会话的状态。可能的值：Other、PreparingSession、Connected、Active、Disconnected、Reconnecting、NonBrokeredSession 和 Unknown。 | 仅限单会话 |
| 当前用户       | 当前会话的用户名（以“域\用户”的形式出现）。                                                                                      | 仅限单会话 |
| 开始时间 (UTC) | 当前会话的开始时间。                                                                                                   | 仅限单会话 |
| 会话计数       | 计算机上的会话数。                                                                                                    | 仅限多会话 |

会话操作和列

March 30, 2024

本文列出了计算机操作和带有说明的列供您参考。

操作

查看您可以对会话执行的操作及其描述。

| 操作    | 说明                                                   | 适用于以下对象上的会话           |
|-------|------------------------------------------------------|-----------------------|
| 注销    | 将用户注销会话。                                             | 单会话操作系统计算机或多会话操作系统计算机 |
| 发送消息  | 向会话的用户发送消息。                                          | 单会话操作系统计算机或多会话操作系统计算机 |
| 查看计算机 | 查看会话的主机。                                             | 单会话操作系统计算机或多会话操作系统计算机 |
| 断开连接  | 断开会话。如果会话断开连接，则会话仍处于活动状态，其应用将继续运行，但用户设备将不再与 DaaS 通信。 | 单会话操作系统计算机或多会话操作系统计算机 |
| 关闭计算机 | 关闭与会话关联的计算机。                                         | 单会话操作系统计算机            |
| 重启计算机 | 重新启动与会话关联的计算机。                                       | 单会话操作系统计算机            |

列

查看会话列及其描述。

| 列          | 说明                                                                                   |
|------------|--------------------------------------------------------------------------------------|
| 当前用户       | 用户的名称；用户的用户主体名称 (UPN)。                                                               |
| 名称         | 托管会话的计算机的 DNS 主机名。                                                                   |
| 交付组        | 包含会话托管计算机的交付组的名称。                                                                    |
| 计算机目录      | 包含会话托管计算机的计算机目录的名称。                                                                  |
| 代理版本       | 安装在托管会话的计算机上的 Citrix Virtual Delivery Agent (VDA) 版本。                                |
| 正在使用的应用程序  | 会话中使用的应用程序列表，由其管理名称标识。                                                               |
| 自主代理       | 这是否是通过直接连接建立的 HDX 会话，无需中介。                                                           |
| 代理时间 (UTC) | 会话的中介时间。                                                                             |
| 代理人用户名     | 代理用户的姓名。                                                                             |
| 客户端 (IP)   | 连接到会话的客户端的 IP 地址。                                                                    |
| 客户端        | 连接到会话的客户端的主机名。                                                                       |
| 插件版本       | 在连接到会话的客户端上运行的 Citrix Workspace 应用程序版本。                                              |
| 连接方式       | 传入连接的主机名，通常是网关、路由器或客户端。                                                              |
| 通过 (IP) 连接 | 传入连接的 IP 地址，通常是网关、路由器或客户端。                                                           |
| 分配类型       | 会话是共享的还是专用的。                                                                         |
| 隐藏         | 会话是否对用户隐藏，无法重新连接。                                                                    |
| VM         | 托管会话的虚拟机的友好名称，由其虚拟机管理程序使用。它不一定与计算机的 DNS 或 AD 名称相匹配。                                  |
| 托管服务器名称    | 托管会话托管计算机的虚拟机管理程序的 DNS 名称。                                                           |
| 连接         | 分配给托管会话的计算机的主机连接的名称。                                                                 |
| 待更新        | 托管计算机的虚拟机映像是否已过期，是否将在计算机下次重启时更新为新映像。                                                 |
| 维护模式       | 托管会话的计算机是否处于维护模式。                                                                    |
| IP 地址      | 托管会话的计算机的 IP 地址。                                                                     |
| 物理         | 托管会话的计算机是否为物理计算机。 <b>True</b> 表示该计算机是物理计算机，这意味着它不由 DaaS 进行电源管理。 <b>False</b> 表示其他情况。 |

| 列               | 说明                                                                                                                                                                     |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 启动完毕            | 用于启动会话的 StoreFront 服务器的主机名。如果会话是通过工作区启动的，则为空白。                                                                                                                         |
| 启动完毕 (IP)       | 用于启动会话的 StoreFront 服务器的 IP 地址。如果会话是通过工作区启动的，则为空白。                                                                                                                      |
| 操作系统类型          | 托管会话的操作系统的标识字符串。                                                                                                                                                       |
| 用户变更持久性         | <p>如何处理用户更改，表明更改是否持久：</p> <ul style="list-style-type: none"> <li>• OnLocal：持久。用户更改保存在本地。</li> <li>• 丢弃：非永久。用户更改将被丢弃。</li> </ul>                                        |
| 连接类型            | <p>用于会话的协议，例如 HDX、RDP 或控制台。注意：对于 XenDesktop 5 VDA 上的控制台会话，该字段为空。</p> <p>注意：对于 XenDesktop 5 VDA 上的控制台会话，该字段为空。</p>                                                      |
| 预配类型            | <p>托管会话的计算机是如何配置的：</p> <ul style="list-style-type: none"> <li>• 手动：未使用 PVS 或 MCS 进行预配。</li> <li>• PVS：由 PVS（物理机、刀片机和虚拟机）配置。</li> <li>• MCS：由 MCS 配置（仅限虚拟机）。</li> </ul> |
| 安全 ICA 处于活动状态   | SecureICA 在会话中是否处于活动状态。                                                                                                                                                |
| 会话状态            | <p>会话的状态。可能的值：已连接、活动或已断开连接。功能级别早于 L7 的计算机上的会话可能会出现其他状态，例如 PreparingSession、正在重新连接、NonBrokeredSession、其他和未知。</p>                                                        |
| 会话更改时间          | 会话最近一次状态更改的时间。                                                                                                                                                         |
| 应用程序状态          | <p>会话中应用程序的状态。可能的值：PreLogon、PreLaunched、Active、Desktop、Lingering 和 NoApps。</p>                                                                                         |
| 会话支持            | 托管会话的计算机支持多个会话还是单个会话。                                                                                                                                                  |
| 区域              | 托管会话的计算机所在区域的名称。                                                                                                                                                       |
| SmartAccess 过滤器 | 会话的智能访问标签。                                                                                                                                                             |
| 开始时间 (UTC)      | 会话启动的时间。                                                                                                                                                               |
| 状态              | 计算机的摘要状态。可能的值：Unregistered、Disconnected 或 InUse。                                                                                                                       |
| 状态时间 (UTC)      | 会话处于当前状态多长时间。                                                                                                                                                          |

| 列                   | 说明                                                                                                                               |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Delivery Controller | 注册会话托管计算机的控制器的 DNS 主机名。                                                                                                          |
| 用户显示名称              | 用户的全名。                                                                                                                           |
| 桌面显示名称              | 最初用于启动会话的计算机的已发布名称。它是 Citrix Workspace 应用程序或 StoreFront 上显示的名称。对于应用程序会话，它是启动到会话中的第一个应用程序的名称，即使该应用程序此后已结束。即使资源后来被重命名或删除，名称也会保持不变。 |

## 管理安全密钥

April 11, 2023

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. 在“完整配置”界面中显示安全密钥设置。(使用远程 PowerShell SDK)
2. 为您的部署配置设置。(使用完整配置界面或远程 PowerShell SDK)。
3. 在 StoreFront 中配置各项设置。(使用 PowerShell)。
4. 在 Citrix ADC 中配置设置。

### 在“完整配置”界面中显示安全密钥设置

默认情况下，安全密钥的设置 在“完整配置”界面中处于隐藏状态。要在该界面中显示它们，请使用远程 PowerShell SDK。有关远程 PowerShell SDK 的详细信息，请参阅 [SDK 和 API](#)。

详细步骤如下所示：

1. 运行 Remote 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"`

为您的部署配置设置

您可以使用完整配置或 PowerShell 为部署配置设置。

使用“完整配置”界面

启用此功能后，导航到完整配置 > 设置 > 管理安全密钥，然后单击编辑。此时将显示 **Manage Security Key**（管理安全密钥）刀片。单击保存以应用所做的更改并退出刀片。

Manage Security Key

This feature lets you manage the security key used to authenticate Citrix Gateway and StoreFront when they communicate with the Delivery Controller. [Learn more](#)

Key1: 

s0AfrCW05dn9AT4A6NU1A8iR7W0RGB9wx4KXtjIWpA=

Key2: 

bgDCxeUJvr6UfnrS3DXhd+q/BkV/CnPQsXCZTva3Qrwl=

☐ Require key for communications over XML port (StoreFront only) ?

☐ Require key for communications over STA port ?

Save

Cancel

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刀片。

### 使用远程 **PowerShell SDK**

下面是相当于在“完整配置”界面中执行的操作的 PowerShell 步骤。

1. 运行 Remote 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。

### 在 **StoreFront** 中配置各项设置

完成部署设置后，您需要使用 PowerShell 在 StoreFront 中配置相关设置。

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-STFStoreService` 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](#)。

Dashboard

Configuration

Reporting

Documentation

Downloads

**Citrix ADC IP Address**

If you change the Citrix ADC IP address and subnet mask, click **Reboot** for the changes to become effective. Citrix recommends that you change the default administrator (nsroot) password.

Citrix ADC IP Address\*

10.102.126.31

Netmask\*

255 . 255 . 255 . 0

☐ Change Administrator Password

Done

Back

- 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 地址和负载均衡器虚拟 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](#)。



### Subnet IP Address

A subnet IP address is used by the Citrix ADC to communicate with the backend servers. Citrix ADC uses this subnet IP address as a source IP address to proxy the client connections as well as to send monitor probes to check the health of the backend servers.

The infographic shows the usage of SNIP in client server communication.

Depending on your network topology, you might have to configure additional subnet IP addresses.

For more information about subnet IP addresses, [click here](#).

Subnet IP Address\*

Please enter value

Netmask\*

255 . 255 . 255 . 0

Done

Back

- 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](#)。

Dashboard

Configuration

Reporting

Documentation

Dov

←

Create RSA Key

Key Filename\*

Choose File

SSLTest

Key Size(bits)\*

2048

Public Exponent Value\*

F4

Key Format\*

PEM

PEM Encoding Algorithm

PEM Passphrase

Confirm PEM Passphrase

☐ PKCS8

Create

Close

- 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](#)。

Dashboard

Configuration

Reporting

Documentation

Downloads

←

Install Server Certificate

Certificate-Key Pair Name\*

CertDDC

i

Certificate File Name\*

Choose File

CSR\_DER

i

Key File Name

Choose File

ns-server.key

i

☒ Notify When Expires

2 SNMP Trap destination found.

Notification Period

30

Install

Close

Dashboard

Configuration

Reporting

Documentation

Downloads

←

Install CA Certificate

Certificate-Key Pair Name\*

SSLCert

i

Certificate File Name\*

Choose File

ns-server.cert

i

☒ Notify When Expires

2 SNMP Trap destination found.

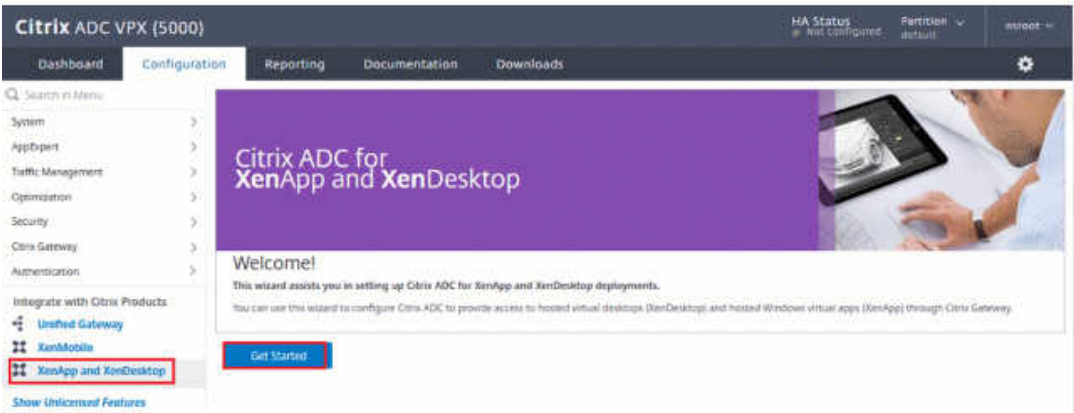
Notification Period

30

Install

Close

- 已为 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）创建了 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](#)。



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)。

DashboardConfigurationReportingDocumentationDownloads

Create Rewrite Action

Name\*

set Type to INSERT\_HTTP\_HEADER ⓘ

Type\*

INSERT\_HTTP\_HEADER ▾

Use this action type to insert a header.

Header Name\*

X-Citrix-XmlServiceKey

Expression

Select ▾Select ▾Select ▾

ⓘ

ⓘ

Evaluate

In string expressions, string constants and expressions can be concatenated with "+" operator. Please make sure that string constants are enclosed in double quotes.

Comments

Create

Close

- a) 在 **Type (类型)** 中，选择 **INSERT\_HTTP\_HEADERS**。
- 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.

1183

```
PS C:\Users\tyadmin> Get-BrokerSite

BaseOU :
BrokerServiceGroupUid :
ColorDepth :
ConfigLastChangeTime :
ConfigurationServiceGroupUid :
ConnectionLeasingEnabled :
DefaultMinimumFunctionalLevel :
DesktopGroupIconUid :
DnsResolutionEnabled :
IsSecondaryBroker :
LicenseEdition :
LicenseGraceSessionsRemaining :
LicenseModel :
LicenseServerName :
LicenseServerPort :
LicensedSessionsActive :
LicensingBurnIn :
LicensingBurnInDate :
LicensingGraceHoursLeft :
LicensingGracePeriodActive :
LicensingOutOfBoxGracePeriodActive :
LocalHostCacheEnabled :
MetadataMap :
Name :
PeakConcurrentLicenseUsers :
RequireXmlServiceKeyForNFuse :
RequireXmlServiceKeyForSta :
ReuseMachinesWithoutShutdownInOutageAllowed :
SecureIcaRequired :
TotalUniqueLicenseUsers :
TrustManagedAnonymousXmlServiceRequests :
TrustRequestsSentToTheXmlServicePort :
UseVerticalScalingForRdsLaunches :
XmlServiceKey1 :
XmlServiceKey2 :
```

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。

DashboardConfigurationReportingDocumentationDownloads

Create Rewrite Policy

Name\*

DDCPolicy

Action\*

set Type to INSERT\_HTTP\_HEADER

Configure Assignments

Configure Rewrite Actions

Log Action

AddEdit

Undefined-Result Action\*

-Global-undefined-result-action-

Expression \*

SelectSelectSelect

HTTP.REQ.IS\_VALID

Expression EditorEvaluate

Comments

Create

Close

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

1184

- 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. 设置负载均衡。必须为每台 STA 服务器配置一个负载均衡虚拟服务器。否则，会话将无法启动。

有关详细信息，请参阅[设置基本负载均衡](#)。

- a) 创建负载均衡虚拟服务器。
  - 导航到 **Traffic Management**（流量管理）> **Load Balancing**（负载均衡）> **Servers**（服务器）。
  - 在 **Virtual Servers**（虚拟服务器）页面中，单击 **Add**（添加）。

Dashboard

Configuration

Reporting

Documentation

Downloads

←

Load Balancing Virtual Server

Basic Settings

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (RFC1918 non-routable) IP address. You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.

Name\*

LBserver1

ⓘ

Protocol\*

HTTP

▼

IP Address Type\*

IP Address

▼

ⓘ

IP Address\*

10.10.10.10

ⓘ

Port\*

80

▶ More

OK

Cancel

- 在协议中，选择 **HTTP**。
  - 添加负载均衡虚拟 IP 地址，然后在 **Port**（端口）中选择 **80**。
  - 单击确定。
- b) 创建负载均衡服务。
- 导航到 **Traffic Management**（流量管理）> **Load Balancing**（负载均衡）> **Services**（服务）。



Dashboard

Configuration

Reporting

Documentation

Downloads

←

Load Balancing Service

Basic Settings

Service Name\*

DDCService1

New Server

Existing Server

Server\*

Protocol\*

HTTP

Port\*

80

▶ More

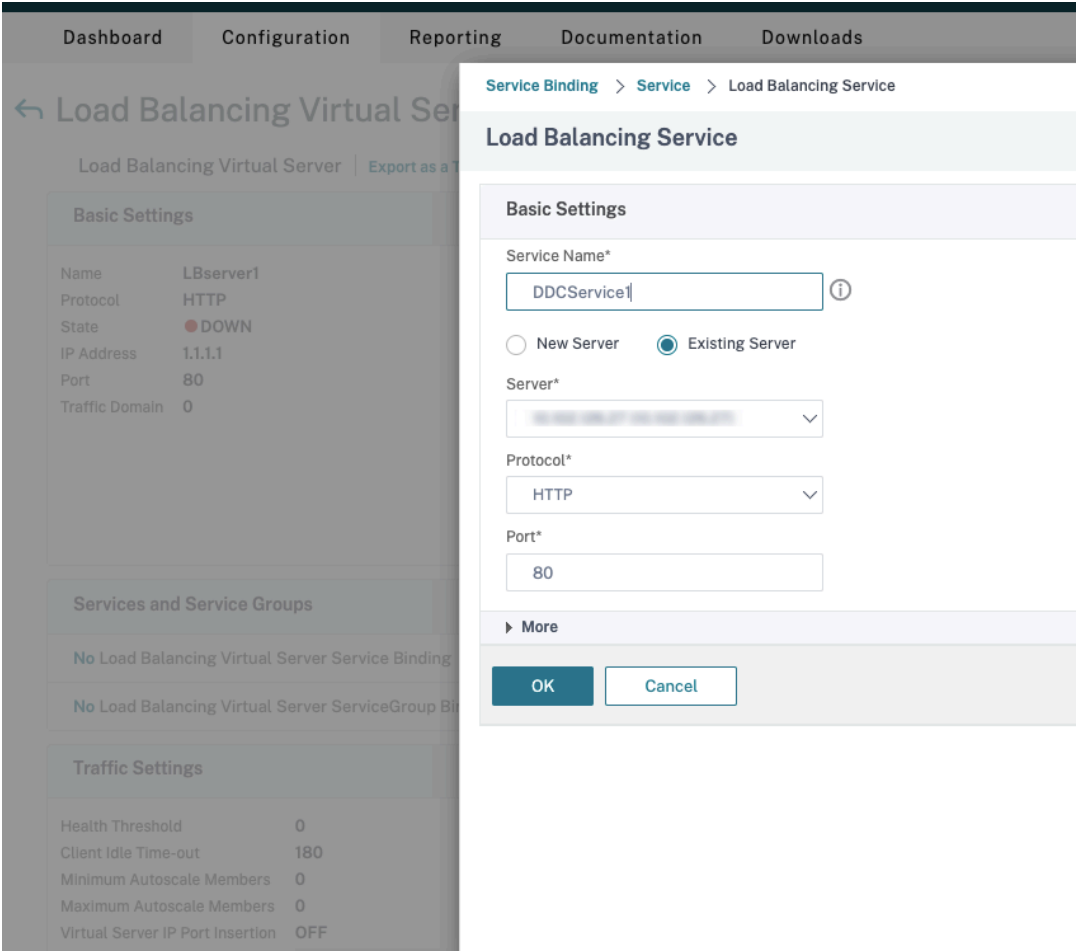
OK

Cancel

- 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。

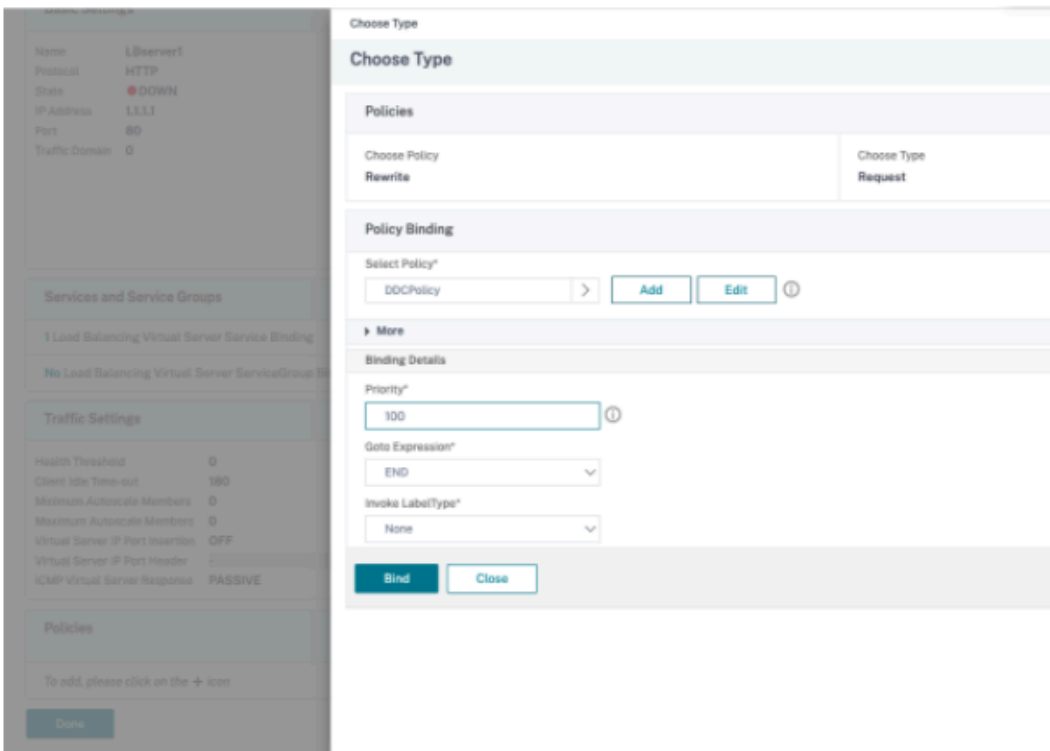
- 选择之前创建的虚拟服务器，然后单击 **Edit**（编辑）。
- 在 **Services and Service Groups**（服务和服务组）中，单击 **No Load Balancing Virtual Server Service Binding**（无负载平衡虚拟服务器服务绑定）。



- 在 **Service Binding**（服务绑定）中，选择之前创建的 Citrix DaaS。
- 单击绑定。

d) 将之前创建的重写策略绑定到虚拟服务器。

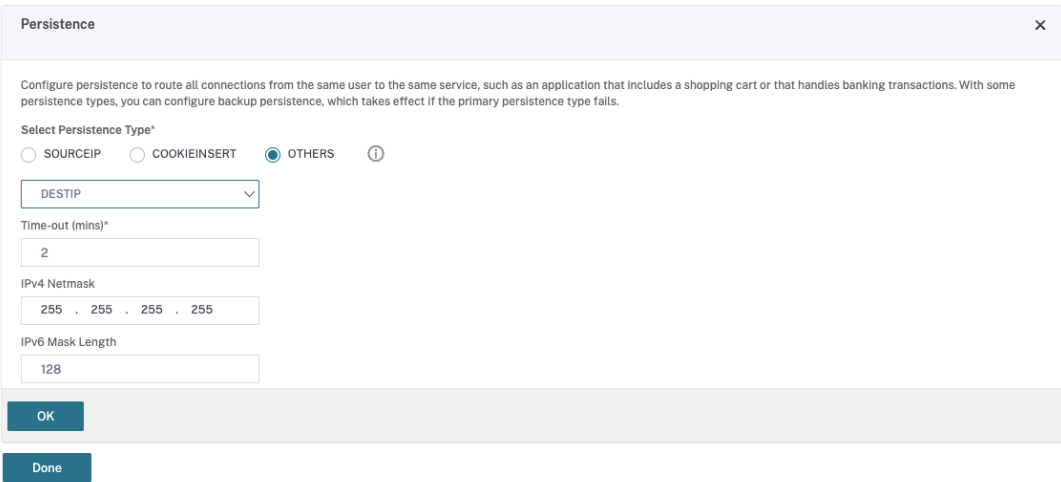
- 选择之前创建的虚拟服务器，然后单击 **Edit**（编辑）。
- 在 **Advanced Settings**（高级设置）中，单击 **Policies**（策略），然后在 **Policies**（策略）部分中单击 **+**。



- 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。
- 单击绑定。
- 单击 **Done**（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）。



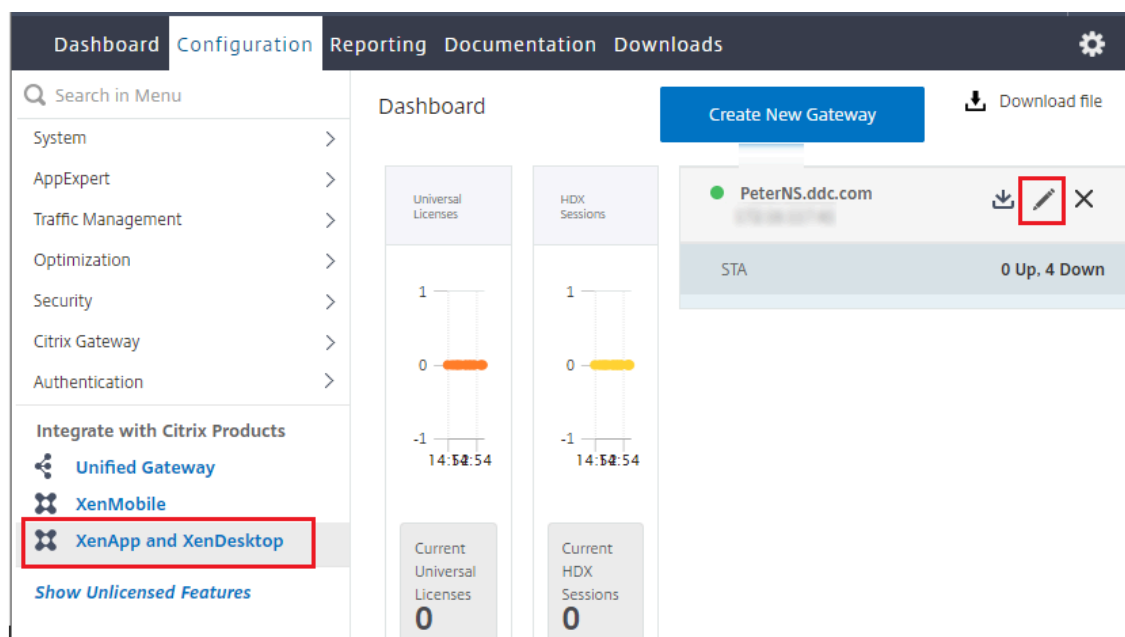
- 选择 **Others**（其他）作为持久性类型。
- 选择 **DESTIP** 以根据虚拟服务器选择的服务的 IP 地址（目标 IP 地址）创建持久性会话
- 在 **IPv4 Netmask**（IPv4 网络掩码）中，添加与 DDC 相同的网络掩码。
- 单击确定。

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 DaaS**，配置会发生变化

如果您已经为 Citrix ADC 设备配置了 Citrix DaaS，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**，以使用负载均衡虚拟服务器的 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 DaaS 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。

| StoreFront                                         |                             |  |
|----------------------------------------------------|-----------------------------|-------------------------------------------------------------------------------------|
| StoreFront URL                                     | https://yj-en2016-1.ddc.com |                                                                                     |
| Storefront Status                                  |                             |                                                                                     |
| Receiver for Web Path                              | /Citrix/StoreWeb            |                                                                                     |
| Default Active Directory Domain                    | ddc.com                     |                                                                                     |
| List of Secure Ticket Authority URL(s) with status |                             |                                                                                     |
| http://[redacted].com                              |                             | ● DOWN                                                                              |
| http://[redacted].com                              |                             | ● DOWN                                                                              |
| http://[redacted].com                              |                             | ● DOWN                                                                              |
| http://[redacted].com                              |                             | ● DOWN                                                                              |

4. 添加 **Secure Ticket Authority URL**。

- 如果启用了安全 XML 功能，STA URL 必须是负载均衡服务的 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。

StoreFront

StoreFront URL\*

https://yj-en2016-1.ddc.com

Retrieve Stores

Receiver for Web Path\*

/Citrix/StoreWeb

Default Active Directory Domain\*

ddc.com

Secure Ticket Authority URL\*

http://[REDACTED].com

×

http://[REDACTED].com

×

http://[REDACTED].com

×

http://[REDACTED].com

×

+

Test STA Connectivity

☐

Use this StoreFront for Authentication

会话恢复设置

March 30, 2024

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。能够在工作站之间快速移动并在每次登录时访问同一组应用程序是许多移动工作人员（例如医院的医护人员）的首要任务。

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。

## 会话可靠性

会话可靠性会使会话在网络连接中断时保持活动状态并显示在用户的屏幕上。用户仍然可以看到他们正在使用的应用程序，直至网络连接恢复。

此功能对于使用无线连接的移动用户尤为有用。例如，使用无线连接的用户进入铁路隧道后将暂时失去连接。通常，会话会断开连接并从用户屏幕上消失，然后该用户必须重新连接到已断开连接的会话。会话可靠性可使会话在计算机上保持活动状态。如果连接已断开，用户的显示内容将冻结，且光标变成一个旋转的沙漏，直至用户到达通道的另一端后恢复连接。用户在连接中断期间可继续访问显示内容，在网络连接恢复后可继续与应用程序交互。会话可靠性可重新连接用户而不提示进行重新身份验证。

Citrix 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（此功能的主要目标是为用户提供方便，因此，它不会提示用户重新进行身份验证）。随着会话保持打开状态的时间延长，用户可能会分散注意力并离开用户设备，从而可能使未经授权的用户可以访问该会话。
- 传入会话可靠性连接使用端口 2598，除非更改会话可靠性端口号策略设置中的端口号。
- 如果您不希望用户无需重新进行身份验证即可重新连接到已中断的会话，请使用客户端自动重新连接功能。您可以配置客户端自动重新连接身份验证策略设置，以便在用户重新连接到中断的会话时提示用户重新进行身份验证。

如果您同时使用了会话可靠性和客户端自动重新连接，这两项功能将按顺序发挥作用。经过在会话可靠性超时策略设置中指定的时间长度之后，会话可靠性将关闭或断开用户会话。之后，客户端自动重新连接策略设置将生效，尝试将用户重新连接到断开连接的会话。

## 客户端自动重新连接

通过客户端自动重新连接功能，Citrix 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 应用程序将尝试在指定时间内重新连接到会话，除非重新连接成功或用户取消了重新连接尝试。默认情况下，此时间为五分钟。要更改此时间段，请在用户设备上编辑以下注册表：

```
HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds  
; DWORD;<seconds>
```

其中 `seconds` 是秒数，超过此时间后不再尝试重新连接会话。

使用以下策略设置启用和配置客户端自动重新连接：

- 客户端自动重新连接：允许或禁止在连接中断后由 Citrix 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时要求用户进行身份验证。
- 客户端自动重新连接日志记录：允许或禁止在事件日志中记录重新连接事件。默认情况下，禁用日志记录。启用后，服务器的系统日志将捕获有关成功和失败的自动重新连接事件的信息。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，然后创建包含加密密钥的 Cookie 并发送到 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。服务器将解密凭据并将其提交到 Windows 登录以进行身份验证。Cookie 过期后，用户必须重新进行身份验证才能重新连接到会话。

如果启用“客户端自动重新连接身份验证”设置，则不使用 Cookie。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 连接配置为在通信链路中断的情况下重置会话，则不会自动重新连接。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）。
- 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。
- 如果服务器配置为重置会话，客户端自动重新连接将创建一个会话。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。启用此功能后，此功能可防止在服务器未检测到任何活动（例如，无时钟变化、无鼠标移动、无屏幕更新）时，远程桌面服务与该会话断开连接。服务器每隔几秒钟会发送一次保持活动



状态数据包，以检测会话是否处于活动状态。如果会话不再处于活动状态，服务器会将该会话标记为已断开连接。

**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 保持活动状态设置会覆盖在 Microsoft Windows 组策略中配置的保持活动状态设置。

使用以下策略设置启用和配置 ICA 保持活动状态：

- **ICA 保持活动状态超时：**指定用于发送 ICA 保持活动状态消息的时间间隔（1—3600 秒）。如果您希望网络监视软件关闭环境（其中连接很少断开，是否允许用户重新连接到会话并不重要）中处于非活动状态的连接，请勿配置此选项。  
  
默认间隔是 60 秒：每 60 秒向用户设备发送一次 ICA 保持活动状态数据包。如果用户设备在 60 秒内没有响应，则 ICA 会话的状态将变为断开连接。
- **ICA 保持活动状态：**发送或阻止发送 ICA 保持活动状态消息。

## 工作区控制

工作区控制允许桌面和应用程序随用户从一个设备移动到另一个设备。此漫游功能使用户在登录后可从任何位置访问所有桌面或打开应用程序，而无需在每个设备中重新启动桌面或应用程序。例如，工作区控制可以帮助医院的医务人员，使他们可以在不同的工作站之间快速移动，并可在每次登录后访问同一组应用程序。如果您将工作区控制选项配置为允许上述功能，则这些工作人员可以与一个客户端设备中的多个应用程序断开连接，然后在其他客户端设备上重新连接以打开相同的应用程序。

工作区控制将影响下列活动：

- **登录：**默认情况下，工作区控制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处于活动状态的任何桌面或应用程序。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”命令配置为使用户从 StoreFront 和所有活动会话一起注销，也可以将其配置为仅从 StoreFront 注销。
- **断开连接：**用户可以一次与所有正在运行的桌面和应用程序断开连接，而无需与每个桌面和应用程序逐个断开连接。

通过 Citrix StoreFront 连接或 Citrix Workspace 应用程序访问桌面和应用程序的用户可以使用工作区控制。默认情况下，虚拟桌面会话的工作区控制处于禁用状态，但对托管应用程序启用工作区控制。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，如果医疗保健工作人员从医院急诊室的客户端设备注销，然后登录到医院 X 射线实验室的工作站，则适用于在 X 射线实验室会话的策略、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

注意：

以下信息指导您使用 PowerShell 配置会话漫游。您可以改用“完整配置”管理界面。有关详细信息，请参阅[管理交付组](#)。

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同时可用。您可以在多个设备上查看应用程序。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）。这可能不符合安全要求。
- 如果禁用会话漫游，则患者记录不会显示在桌面 PC 上，保险单也不会显示在平板电脑上。

示例 2：生产经理在其办公室的 PC 上启动一个应用程序。设备名称和位置确定该会话可以使用的打印机及其他资源。当天晚些时候，该经理进入隔壁大楼的一件办公室参加会议，此会议需要他使用打印机。

- 如果启用会话漫游，该生产经理可能无法访问该会议室附近的打印机，因为他之前在自己的办公室启动的应用程序已导致为其分配了该办公室附近的打印机和其他资源。
- 如果禁用了会话漫游，当他登录到另一台计算机（使用相同的凭据）时，将启动一个新会话，并且附近的打印机和资源都可用。

## 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。（会话可以通过先断开客户端设备的连接来在客户端设备之间漫游，或者使用 Workspace 控制显式漫游它们。）从不使用来自其他客户端设备的活跃连接会话。相反，将启动一个新会话。
- **SameEndpointOnly**：用户为他们使用的每台客户端设备获得一个唯一的会话。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：

键：`HKLM\SOFTWARE\Citrix\PortICA`

- 值：`AutoLogonTimeout`
- 类型：`DWORD`
- 以秒为单位指定十进制时间，范围在 0 到 3600 之间。

如果您更改主映像，请将新图像发布到目录中。有关详细信息，请参阅[更改主映像](#)。

此设置仅适用于包含单会话桌面（工作站）VDA 的 VM。Microsoft 控制包含多会话服务器 VDA 的计算机上的登录超时。

## 标记

November 16, 2023

### 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，您可以定制某些操作，使其仅应用于具有指定标记的项目。

- 定制搜索在“完整配置”管理界面中的现实方式。

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帮助。

本文后面的部分将介绍使用标记限制的详细信息和示例。

- 为交付组中的一部分计算机安排定期重新启动。

通过对计算机使用标记限制，您可以使用新的 PowerShell cmdlet 为交付组中的一部分计算机配置多个重新启动计划。有关示例和详细信息，请参阅[管理交付组](#)。

- 对交付组中的计算机、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
- 交付组
- 应用程序组

可以在“完整配置”管理界面中创建或编辑以下内容时配置标记限制：

- 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

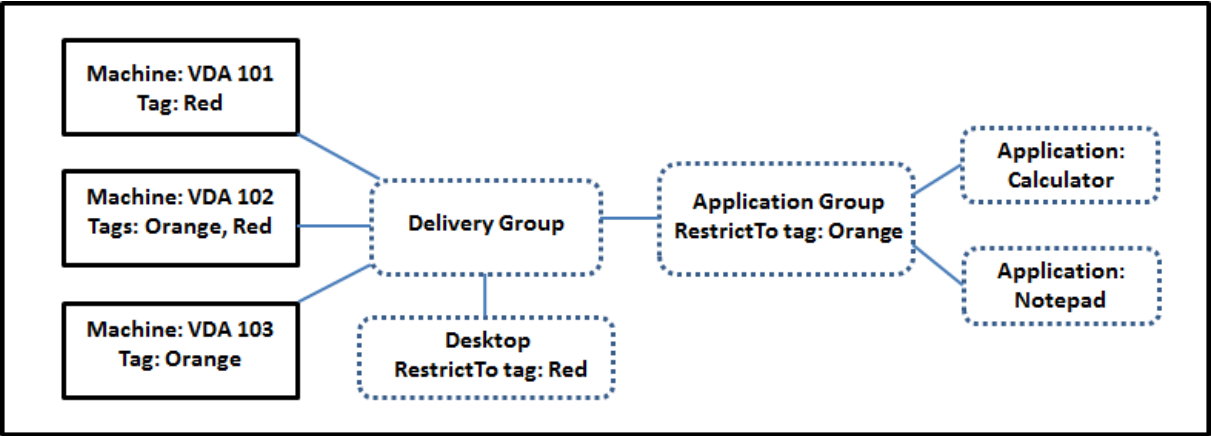
标记限制涉及多个步骤：

- 创建标记，然后将其添加（应用）到计算机。
- 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”）。

标记限制延长了控制器的计算机选择过程。Controller 根据访问策略、配置的用户列表、区域首选项和启动准备情况以及标记限制（如果存在），从关联的交付组中选择一台计算机。对于应用程序，Controller 将按优先级顺序回退到其他交付组，对每个考虑的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。存在一个共享交付组、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。



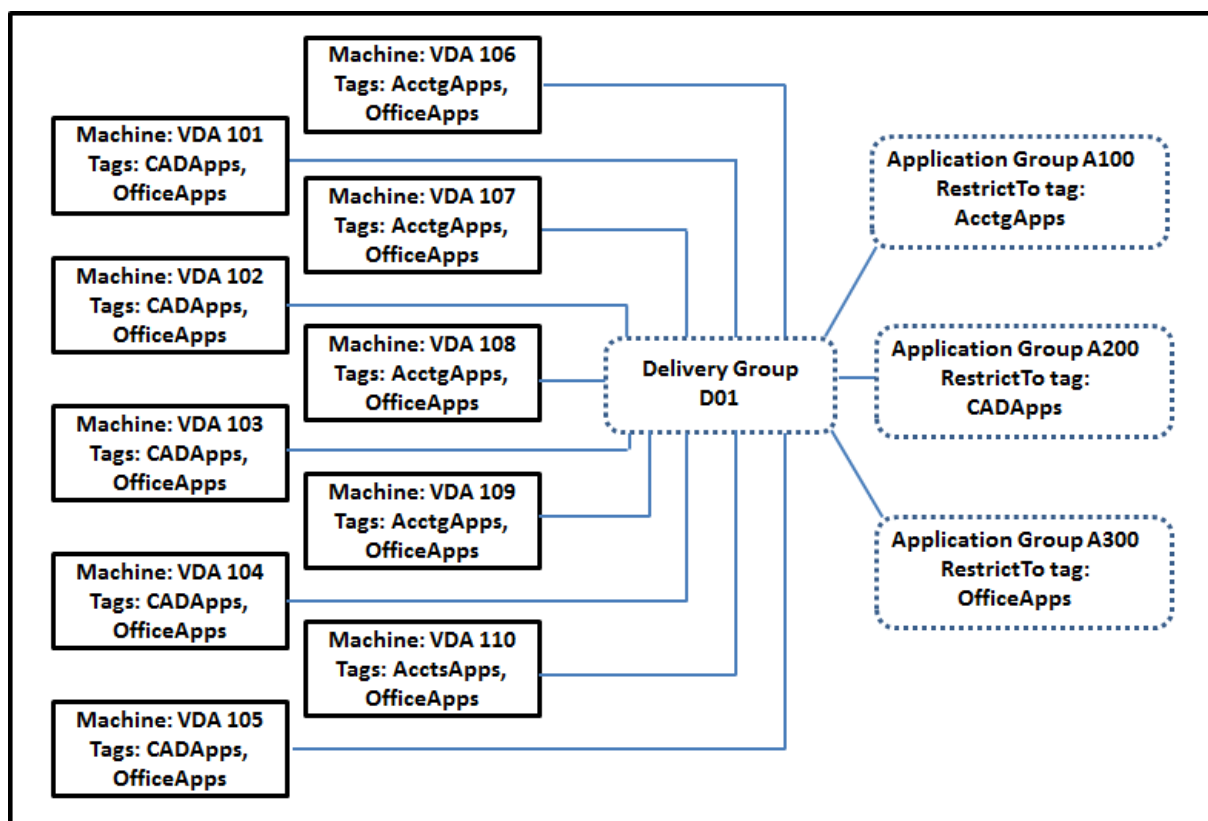
- 已为所有三台计算机 (VDA 101-103) 添加了标记。
- 交付组中的桌面是使用名为 **Red** 的标记限制创建的。因此，该桌面只能在该交付组中具有标记 **Red** 的计算机 (VDA 101 和 102) 上启动。
- 创建应用程序组时使用 **Orange** 标记限制。因此，其每个应用程序 (**Calculator** 和 **Notepad**) 只能在该交付组中具有标记 **Orange** 的计算机 (VDA 102 和 103) 上启动。

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。



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、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

可以通过“完整配置”管理界面中的管理标记操作创建、添加（应用）、编辑标记以及从选定项目中删除标记。

（例外情况：用于策略分配的标记是通过管理标记操作来创建、编辑以及删除的。但是，您在创建策略时应用（分配）标签。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。

## 使用“管理标记”功能

在管理 > 完整配置中，选择要对其应用标记的项目。这些项目包括：

- 一台或多台机器
- 一个或多个应用程序
- 桌面、交付组或应用程序组
- 计算机目录

然后选择操作栏中的管理标记。管理标记对话框列出了所有现有标记，而不仅仅是选定项目的标记。

- 如果启用了复选框，则表示该标记已添加到所选项目中。（在下面的屏幕截图中，选定的计算机应用了名为“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。

Manage Tags

×

Manage tags for the machine

Select tags that you want to apply to the selected item. To add a tag, click Create. To edit a tag, select the tag and click Edit. To delete a tag, select a tag and click Delete.

| <input type="checkbox"/> Tag ↓ | Description |
|--------------------------------|-------------|
| <input type="checkbox"/>       |             |
| <input type="checkbox"/>       |             |
| <input type="checkbox"/>       |             |
| <input type="checkbox"/>       |             |
| <input type="checkbox"/>       |             |
| <input type="checkbox"/>       |             |
| <input type="checkbox"/>       |             |
| <input type="checkbox"/>       |             |
| <input type="checkbox"/>       |             |
| <input type="checkbox"/>       |             |
| <input type="checkbox"/>       |             |
| <input type="checkbox"/>       |             |
| <input type="checkbox"/>       |             |
| <input type="checkbox"/>       |             |
| <input type="checkbox"/>       |             |

Create

Edit

Delete

Save

Cancel

可以从管理标记对话框中执行以下操作。查看使用标记时的注意事项。

- 要创建标记，请执行以下操作：  
选择 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。然后选择 “保存”。



创建标记不会自动将其应用于您选择的任何项目。请使用复选框应用标记。

- 要添加（应用）一个或多个标记，请执行以下操作：

启用标记名称旁边的复选框。包含连字符的复选框表示部分（而非所有）选定项目已应用该标记。当您选择多个项目且标记的复选框具有连字符时，将其更改为复选标记会影响所有选定的计算机。

如果您尝试向计算机添加标记，并且该标记用作应用程序组中的限制，系统会警告您该操作可以使这些计算机可以启动。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。包含连字符的复选框表示部分（而非所有）选定项目已应用该标记。选择多个项目并且标记的复选框具有连字符时，清除该复选框将从所有选定的计算机中删除该标记。

如果您尝试从计算机中删除标记限制，系统会警告您该操作可能会影响考虑启动的计算机。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：

选择标记，然后选择编辑。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，然后选择删除。“删除标记”对话框显示当前有多少项目使用所选标签（例如“2 台计算机”）。选择某个项目可显示更多信息（例如，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，请在左侧窗格中选择交付组。选择一个交付组，然后在操作栏中选择查看计算机。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：

创建标记，然后使用管理标记操作将其添加（应用）到标记限制将会影响的计算机。

- 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。在桌面页面上选择添加或编辑。在 添加桌面 对话框中，选择 限制启动带有标记的计算机，然后从菜单中选择标记。
- 要更改或删除交付组上的标记限制，请执行以下操作：  
  
编辑组。在桌面页面上，选择编辑。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

应用到项目的标记可用于不同的目的。请谨记，添加、移除和删除标记可能会产生意想不到的影响。在“完整配置”管理界面中使用搜索时，可以使用标记对计算机显示进行排序。配置应用程序组或桌面时，可以使用相同的标记作为限制。该操作将考虑启动的对象仅限于指定交付组中具有该标记的计算机。

如果在将标记配置为桌面或应用程序组标记限制之后将标记添加到计算机，系统会警告您这可能会使这些计算机可用于启动更多应用程序或桌面。如果这是您希望得到的结果，请继续。如果不是，请取消操作。

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 标记添加到这些计算机，则会看到类似以下内容的消息：“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，在某个应用程序组中使用标记来限制启动时，直到编辑该组并删除作为限制的该标记后才能将标记删除。（如果您已被允许删除该标记，它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上文第二个示例中说明的应用程序组配置标记限制的步骤。

VDA 和应用程序已经安装在计算机上，且已创建交付组。

创建标记并将其应用于计算机：

1. 在管理 > 完整配置中，选择左窗格中的交付组。选择交付组 **D01**，然后在操作栏中选择查看计算机。
2. 选择计算机 VDA 101-105，然后在操作栏中选择管理标记。
3. 在管理标记对话框中，选择创建。创建一个名为 **CADApps** 的标记。选择确定。
4. 再次选择创建并创建名为 **OfficeApps** 的标记。选择确定。
5. 通过启用每个标记名称（**CADApps** 和 **OfficeApps**）旁边的复选框将新创建的标记添加（应用）到选定的计算机。然后关闭对话框。
6. 选择交付组 **D01**。在操作栏中选择查看计算机。
7. 选择计算机 VDA 106-110，然后在操作栏中选择管理标记。
8. 在管理标记对话框中，选择创建。创建一个名为 **AcctgApps** 的标记。选择确定。
9. 通过选择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。然后关闭对话框。

创建具有标记限制的应用程序组。

1. 在管理 > 完整配置中，选择左窗格中的应用程序。
2. 在操作栏中选择创建应用程序组。向导将启动。
3. 在交付组页面上，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。
4. 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**。
5. 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。
6. 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。

将标记应用到计算机目录

可以使用管理 > 完整配置或 PowerShell 将标记应用到计算机目录。

- [管理标记](#) 介绍了如何使用管理界面。目录显示不指示是否应用了标记。
- 要使用 PowerShell，请参阅使用 PowerShell 将标记应用到目录。

以下是在目录中使用标签的示例：

- 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。将标记应用到该目录即可实现该目标。

使用 **PowerShell** 将标记应用到目录

以下 PowerShell cmdlet 可用：

- 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 会将以前创建的名称为 `fy2018` 的标记添加到名称为 `acctg` 的目录中：`Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`。

有关指导和语法，请参阅 PowerShell cmdlet 帮助。

### 自动标记（预览）

自动标记允许管理员根据自定义规则在各种 DaaS 对象上自动设置和删除标签。此增强功能无需维护为环境优化而定期运行的不同脚本。

### 用例

通过自动标记，您可以实施与业务驱动因素相关的规则，例如降低成本、优化基础架构和推动消费。以下是一些用例：

- 回收未使用的 **VDI** - 将未使用的时间超过预先配置的天数的专用工作负载释放到可用池中。
- 移除应用程序混乱 - 通过识别未使用时间超过预先配置的天数的应用程序来减少应用程序混乱。
- 功能级别低于 **X** 的 **DG** - 查找功能级别低于特定功能级别的交付组。
- 非活跃用户 - 回收未登录时间超过预先配置的天数的用户的资源。

### PowerShell 命令

您可以使用 PowerShell 命令创建自动标签。创建自动标记规则后，将以 600 秒的频率对其进行评估。有关更多信息，请参阅 [New-BrokerAutoTagRule](#)。

示例 `New-BrokerAutoTagRule` 使用与 `Get-BrokerMachine` commandlet 相同的对象类型和过滤器参数。有关更多信息，请参阅 [GetBrokerMachine](#)。

1. 将已超过 30 天未使用的专用 VDI 标记为 ID 为 123：

a) 定义一个标签来标记未使用的 VDI，比如 **unused-VDI**。

- 标签名称：未使用的 VDI
- 标记 ID：123

b) 创建自动标记规则以标记未使用的计算机。定义规则参数：

- 名称：规则的通用名称。
- 对象类型：计算机。
- 规则文本：静态、已分配的上次连接时间大于 30 天或无值的计算机。
- 标签 Uid：您要关联的标签 ID，123。

```
New-BrokerAutoTagRule -Name 'UnusedVdi' -ObjectType 'Machine' -RuleText "-AllocationType Static -IsAssigned $true -Filter { SummaryState -ne 'InUse' -and ( LastConnectionTime -lt '-30' -or LastConnectionTime -eq '$null' )} " -TagUid 123
```

c) 检查标有 **unused-VDI** 标签的 计算机并将其释放。

2. 要标记功能级别低于 X 的交付组（使用 **L7\_20** 作为阈值功能级别），请执行以下操作：

```
New-BrokerAutoTagRule -Name 'LowFL'-ObjectType 'DesktopGroup'-RuleText "-Filter { MinimumFunctionalLevel -lt 'L7_20' } "-TagUid 123
```

3. 要标记在没有文件夹的情况下发布的用户可见应用程序，请执行以下操作：

```
New-BrokerAutoTagRule -Name 'NoFolder'-ObjectType 'Application'-RuleText "-Enabled $true -Filter { ClientFolder -eq $null } "-TagUid 123
```

## 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）。

## 时区设置

March 5, 2024

根据您的喜好在管理控制台中自定义日期和时间格式。

注意：

此设置特定于每个用户帐户。

1. 转到完整配置 > 设置 > 日期和时间。
2. 单击“编辑”配置以下设置：

- 时间格式：
  - 选择使用 12 小时制（例如晚上 9:00）或 24 小时制（例如 21:00）显示时间。

注意：

如果您希望格式与浏览器的时区保持一致，请选择“与本地相同”选项。

- 日期格式：

- 配置日期格式以匹配您的首选项，例如 yyyy/MM/dd。

注意：

如果您希望格式与浏览器的时区保持一致，请选择“与本地相同”选项。

- 时区：

- **UTC**：在整个用户界面中以 UTC 格式显示日期和时间。鼠标悬停器显示您所在时区的本地日期和时间。
- **本地时区**：在整个用户界面中显示您的本地时区中的日期和时间。鼠标悬停器以 UTC 显示日期和时间。

## 对 VDA 注册和会话启动问题进行故障排除

March 30, 2022

我们提供了运行状况检查功能，可让您判定 VDA 的运行状况。该功能允许您通过“完整配置”管理界面确定常见 VDA 注册和会话启动问题的可能原因。

与用于判定站点及其其他组件的运行状况和可用性的独立工具 [Cloud Health Check](#) 不同，该功能在“完整配置”管理界面中作为运行运行状况检查操作提供。

运行运行状况检查操作可以运行与 [Cloud Health Check](#) 相同的检查，但以下检查除外：

- 对于 VDA 注册：
  - VDA 通信端口可用性
- 对于在 VDA 上启动的会话：
  - 会话启动通信端口可用性
  - VDA 应用程序启动路径

### 必备条件

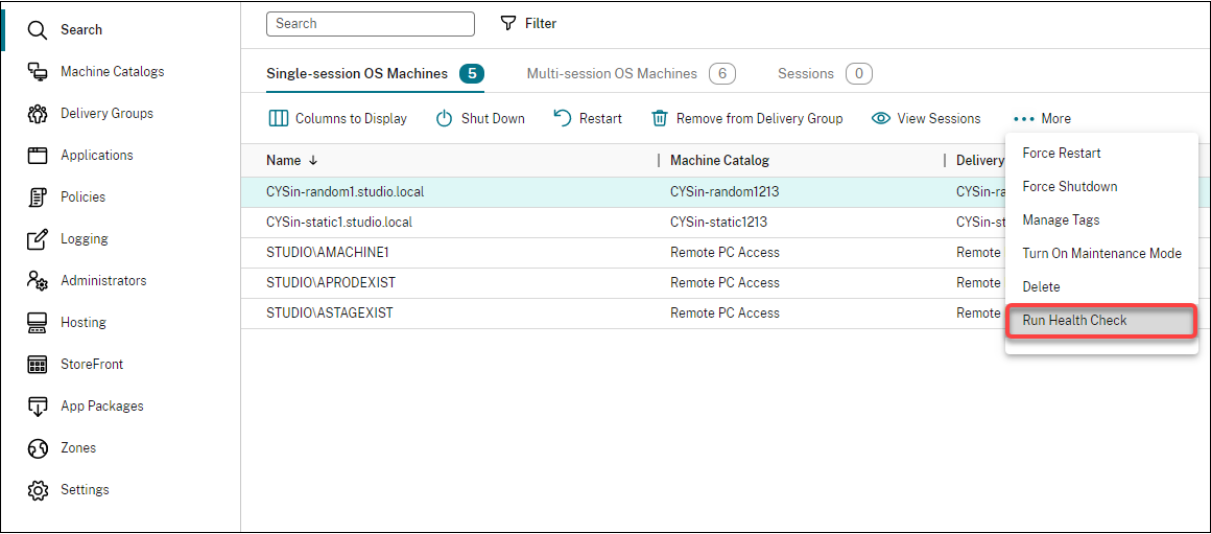
在使用该功能之前，请确认您满足以下必备条件：

- Windows VDA

- VDA 版本 2109 或更高版本
- VDA 已注册

对 **VDA** 运行运行状况检查

1. 在“完整配置”管理界面中，转到 **Search**（搜索）节点。
2. 选择一台或多台计算机，然后从操作栏中选择 **Run Health Check**（运行状况检查）。



注意：

目前，您只能对已注册的 VDA 运行运行状况检查。运行运行状况检查操作对未注册的 VDA 不可用。

选择运行运行状况检查后，将出现一个窗口，显示运行状况检查的进度。请等到运行状况检查完成，或者单击取消取消检查。如有必要，您可以移动窗口。



注意：

如果已存在“运行状况检查正在进行”窗口，则在现有运行状况检查完成之前，您无法运行其他运行状况检查。

运行状况检查完成后，将显示下面两个按钮：查看报告和关闭。要查看运行状况检查的结果，请单击查看报告。



运行状况检查报告将在新浏览器选项卡中打开。该报告包含以下要素：

- 生成结果报告的时间和日期
- 运行运行状况检查的人员
- 检查在目标计算机上运行
- 发现的问题以及修复建议

| citrix   VDA Health Check Report                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-----|
| Created by Jack Zhou 12/14/2021 1:46:05 PM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |     |
| Report - cysin-static1.studio.local                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |     |
| Issue                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | State | Fix |
| <b>Remote Desktop Server Client Access License is in Grace Period</b><br>Microsoft Windows Remote Desktop Server (RDS) Client Access License (CAL) is in Grace Period. This could be due to a connection issue to the Microsoft License Server, the Microsoft License has expired, or the VDA has yet to be configured with an RDS License Server. The RDS CAL will continue to work during the grace period, but will stop working if this issue is not addressed when the grace period ends.                                                                                                                                                                                                                                                                                                                                                                                                                    | ✓     |     |
| <b>VDA software installation missing or corrupted</b><br>The Virtual Delivery Agent software installation on the following machine(s) is not functioning correctly. This issue can occur if the software was not installed correctly or does not support the current OS version on the machine.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | ✓     |     |
| <b>VDA domain membership verification failed</b><br>The domain membership of the following VDA(s) cannot be confirmed. This issue can occur if: * The VDA did not join the domain correctly. * DNS name resolution might not be working. * The domain controller can't be reached. * There is no trust relationship between the VDA and the domain controller. * A restart is required for the VDA due to Windows Update.<br>The VDA must be joined successfully to the domain so the VDA can register with the Site. If the VDA can't register with the Site, users cannot access the applications and desktops that the VDA hosts.                                                                                                                                                                                                                                                                              | ✓     |     |
| <b>Citrix Desktop Service displays invalid status</b><br>The Citrix Desktop service is not running, properly installed, registered on the machine, or the service permissions might not be set correctly. This issue can occur if the service is not started or the system Event Log has traces of service related issues. If the Citrix Desktop Service is not present or running, the VDA can't register with the Site, preventing users from accessing their applications and desktops.                                                                                                                                                                                                                                                                                                                                                                                                                        | ✓     |     |
| <b>Invalid Windows Firewall configuration</b><br>Port BlockPorts blocked by firewall. The following Windows Firewall rules are not enabled on the VDA: * Inbound agent connections on TCP port 80 * Outbound Broker connections on TCP port 80 (default)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | ✓     |     |
| <b>VDA cannot communicate with Delivery Controllers</b><br>The following VDA(s) can't communicate with the Delivery Controllers in the Site. This issue can occur if: * There are network issues preventing communication between the VDA and Delivery Controllers. * The VDA or Delivery Controllers have incorrect DNS settings. * Active Directory OU-based discovery of Delivery Controllers is not configured correctly. * Delivery Controller host names in the ListOfDDCs do not resolve correctly. * Delivery Controller host names in the ListOfDDCs and the Windows Hosts file are incorrect or misspelled. * The Delivery Controllers are not reachable on configured ports.<br>The VDA must be able to communicate with the Delivery Controllers so the VDA can register with the Site. If the VDA can't register with the Site, users can't access the applications and desktops that the VDA hosts. | ✓     |     |
| <b>System clocks on the VDA and Delivery controller are not synchronized</b><br>The time difference between the VDA's system clock and the Delivery Controller's system clock is greater than the maximum difference that Kerberos allows ("5 minutes")                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | ✓     |     |
| <b>VDA is not registered with the Site</b><br>The following VDA(s) are not registered with the Site. This issue might occur if: * VDA Desktop Service has an invalid status. * VDA can't reach the domain controller. * VDA can't communicate with the Site. * There are other undiagnosed conditions affecting the VDA.<br>If the VDA can't register with the Site, users might not be able to log on and access their applications and desktops.                                                                                                                                                                                                                                                                                                                                                                                                                                                                | ✓     |     |
| <b>Session launch services display invalid status</b><br>One or more of the following services are not started, cannot be found, or have invalid permissions: * Citrix ICA Service * Citrix Encryption Service * Citrix Print Manager Service * Citrix Group Policy Engine * Citrix HDX MediaStream for Flash Service * Citrix Pvs for VMs agent (for MCS-provisioned VDAs only)<br>Additionally, the Event Log might contain errors or warnings for the following items: * Citrix Portica * Citrix-HostCore-ICA Service * Citrix-Multimedia-Rave * Citrix-Multimedia-AudioSvc * Citrix-Graphics-Vid3d<br>These services must be running so the VDA can provide access to applications and desktops to users. If these services are not available, users cannot launch sessions and might receive notifications that the applications and desktops they are trying to access are not available.                   | ✓     |     |
| <b>Incorrect Windows firewall configuration for Session Launch services</b><br>Port BlockPorts blocked by firewall. The Windows Firewall configuration on the VDA is preventing inbound connections from Delivery Controllers in the Site. The VDA must allow inbound connections on the following ports: * ICA/HDX TCP port 1494 * ICA/HDX with Session Reliability port 2598 * ICA/HDX over WebSocket TCP port 8008 * ICA/HDX over TLS/DTLS TCP port 443 * ICA/HDX audio over UDP Real-time Transport UDP ports 16500-16509 * ICA/HDX UDP port 1494 * ICA/HDX with Session Reliability UDP port 2598<br>These ports enable the VDA to communicate with the Delivery Controllers, register with the Site, and provide access to users' applications and desktops. If these ports are blocked or used by other applications, users cannot launch sessions and access these resources.                             | ✓     |     |
| <b>Remote Desktop Server Client Access License is invalid</b><br>Microsoft Windows Remote Desktop Server (RDS) Client Access License (CAL) is invalid. This could be due to a connection issue to the Microsoft License Server, the Microsoft License has expired, or the VDA has yet to be configured with an RDS License Server. This VDA cannot host sessions until this issue is addressed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | ✓     |     |

您可以单独运行运行状况检查，也可以分批运行。

注意：

批量运行运行状况检查时，请选择不超过 10 台计算机。否则，运行运行状况检查操作将不可用。

用户访问

April 21, 2023

在 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）部署中，有两个主要组件可以访问应用程序和桌面：



- **Citrix Workspace** 平台：Citrix Workspace 平台是一个完整的数字解决方案，允许您安全访问与个人在组织中的角色相关的信息、应用程序和其他内容。用户会订阅您提供的服务，并可以从任何地方、在任何设备上访问这些服务。Citrix Workspace 平台可帮助您整理和自动化用户协作所需的最重要细节，做出更好的决策并全神贯注于他们的工作。

部署 Citrix Workspace 的努力为零，而且 Citrix 一直保持其常青状态。建议新老客户使用 Citrix Workspace 平台、预览版和概念验证。

- **本地 StoreFront**：客户还可以使用现有 StoreFront 聚合 Citrix Cloud 中的应用程序和桌面。此用例将提供更高的安全性，包括支持双重身份验证以及阻止用户将其密码输入到云服务中。此外，还允许客户自定义其域名和 URL。建议已部署 StoreFront 的所有 Citrix Virtual Apps and Desktops 客户使用此部署类型。

另请参阅本地主机缓存和 StoreFront。

用户从公司防火墙外部连接时，Citrix Cloud 可以使用 Citrix Gateway（以前称为 NetScaler Gateway）技术保护这些与 SSL 的连接的安全性。Citrix Gateway 或 Citrix 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。

## 使用 Citrix Workspace

通过 <https://<customername>.cloud.com> 访问 Workspace。如果需要，您可以自定义 Workspace URL 的 [<customername>](#) 部分。然后，可以为要使用的每个资源位置配置连接，以便最终用户可以访问其工作区中的资源。最终用户使用最新版本的 Citrix Workspace 应用程序访问其工作区。

有关使用 Citrix Workspace 的更多信息，请参阅：

- [配置工作区](#)：用于配置访问和自定义设置。
- [安全工作区](#)：用于配置身份验证。
- [管理您的工作区体验](#)：了解最终用户如何访问其工作区以及工作区的显示方式。

要通过 Citrix Workspace 为最终用户提供远程访问，您可以使用 Citrix Gateway 服务或您自己的 Citrix Gateway。

- 要使用 Citrix Gateway 服务，请执行以下操作：
  1. 在 **Citrix Cloud > Resource Locations**（资源位置）中，选择要使用的资源位置的 **Gateway**（网关）。
  2. 选择 **Gateway Service**（网关服务），然后单击 **Save**（保存）。
  3. 在 **Citrix Cloud > Workspace Configuration (Workspace 配置) > Service Integrations**（服务集成）中，找到“Gateway service”（网关服务），然后从省略号菜单中选择 **Enable**（启用）。
- 要使用您自己的 Citrix Gateway，请执行以下操作：
  1. 将 Citrix Gateway 设置为 ICA 代理（不需要身份验证或会话策略）。
  2. 将资源位置配置为使用 Citrix Gateway：

- a) 在 **Citrix Cloud > Resource Locations** (资源位置) 中, 选择要使用的资源位置的 **Gateway** (网关)。
  - b) 选择 **Traditional Gateway** (传统网关) 并输入外部 FQDN。请勿添加协议。端口为可选项。Citrix Workspace 不支持远程访问和内部访问的组合。
3. 将 Citrix Cloud Connector 作为 Secure Ticket Authority (STA) 服务器绑定到 Citrix Gateway。有关详细信息, 请参阅 [CTX232640](#)。

注意:

只支持 Citrix Cloud Connector 计算机用作 Citrix Gateway 的 STA 服务器。不支持使用其他连接器作为 STA 服务器, 例如连接器设备。

有关 Citrix Gateway 服务和 Citrix Gateway 的详细信息, 请参阅 [Citrix Gateway](#)。

## 使用本地 StoreFront

有关配置本地 StoreFront 的信息, 请参阅 [StoreFront 文档](#)。

使用现有 StoreFront 的一项优势为 Citrix Cloud Connector 提供用户密码的加密。Cloud Connector 使用 AES-256 通过随机生成的一次性密钥加密凭据。此密钥直接返回到 Citrix Workspace 应用程序, 绝不会发送到云。Citrix Workspace 应用程序随后在会话启动期间将其提供给 VDA, 以便解密凭据并提供单点登录到 Windows 的体验。

- 对于传输, 请选择 HTTP 和端口 80。StoreFront 计算机必须能够直接通过提供的 FQDN (完全限定域名) 访问 Cloud Connector。Cloud Connector 必须能够访问 Cloud NFuse/STA URL, 其网址为 <https://<customername>.xendesktop.net/Scripts/wpnbr.dll> 和 [ctxsta.dll](#)。
- 添加 Cloud Connector 作为 Delivery Controller 以实现高可用性。

使用最新版本的 StoreFront。

## 外部访问

要提供通过 Citrix Gateway 和本地 StoreFront 进行的外部访问, 请执行以下操作:

- 使用身份验证和会话策略照常设置 Citrix Gateway。有关详细信息, 请参阅 [Citrix Gateway 文档](#)。
- 将您的本地 StoreFront 应用商店的 Delivery Controller 指向 Citrix Cloud Connector。将 Cloud Connector 作为 STA 服务器绑定到 Citrix Gateway。
- Citrix Gateway 必须与 StoreFront 使用相同的 STA URL。如果尚未将网关配置为使用现有 Citrix Virtual Apps and Desktops 环境的 STA, 则可以将 Cloud Connector 用作 STA。

## 内部访问

要通过本地 StoreFront 提供内部访问, 请将本地 StoreFront 应用商店的 Delivery Controller 指向 Citrix Cloud Connector。

### 外部访问和内部访问

要提供通过 Citrix Gateway 和本地 StoreFront 进行的外部 and 内部访问，请执行以下操作：

- 使用身份验证和会话策略照常设置 Citrix Gateway。有关详细信息，请参阅 [Citrix Gateway 文档](#)。
- 将 Cloud Connector 作为 STA 服务器绑定到 Citrix Gateway。
- 将您的本地 StoreFront 应用商店的 Delivery Controller 指向 Cloud Connector。

### 本地主机缓存和 **StoreFront**

本地主机缓存允许在 Cloud Connector 无法与 Citrix Cloud 通信时继续在 Citrix DaaS 部署中执行连接代理操作。

本地主机缓存功能仅在包含客户部署的本地 StoreFront 的资源位置中起作用。不支持将本地主机缓存用于 Citrix Workspace。

每个资源位置都必须具有客户部署的本地 StoreFront。验证资源位置是否包含指向该资源位置中的所有 Cloud Connector 的本地 StoreFront。

有关详细信息，请参阅[本地主机缓存](#)。

### 虚拟 IP 和虚拟环回

April 18, 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、身份验证或其他目的，因此，这些应用程序在会话中需要使用唯一的 IP 地址或环回地址。其他应用程序可能绑定到某个静态端口，因此，在多用户环境中尝试启动应用程序的其他实例将失败，因为该端口已在使用中。要使这些应用程序能够在 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。

## 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了哪些 IP 地址和端口以及哪些进程名称正在打开这些端口。
4. 配置任何打开服务器的 IP 地址（0.0.0.0 或 127.0.0.1）的进程。
5. 为确保应用程序不会在其他端口上打开相同的 IP 地址，请启动该应用程序的另一实例。

## Microsoft 远程桌面 (RD) IP 虚拟化的工作方式

- 必须在 Microsoft 服务器上启用虚拟 IP 地址。

例如，在 Windows Server 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，应用程序只能看到自己应该使用的 IP 地址。该应用程序对侦听 TCP 或 UDP 通信的任何尝试都会自动绑定到其分配的虚拟 IP 地址（或环回地址），并且该应用程序打开的任何原始连接都源自绑定到该应用程序的 IP 地址。

在返回地址的函数（如 `GetAddrInfo()`，由 Windows 策略控制）中，如果请求本地主机 IP 地址，则虚拟 IP 将查看返回的 IP 地址并将其更改为会话的虚拟 IP 地址。尝试通过此类名称函数获得本地服务器 IP 地址的应用程序，仅会看到分配给该会话的唯一虚拟 IP 地址。此 IP 地址通常用于后续套接字调用，如 `bind` 或 `connect`。有关 Windows 策略的详细信息，请参阅 [Windows Server 中的 RDS IP 虚拟化](#)。

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；这称为环回优先。但是，操作时请注意以下事项：

- 仅在同时启用了虚拟 IP 和虚拟环回的情况下使用环回优先；否则可能会导致意外结果。
- 注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

在应用程序所在的服务器运行注册表。

- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP`

- 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 >

## 区域

February 9, 2024

### 简介

如果 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）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。使用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。在 Citrix DaaS 环境中，每个资源位置都被视为一个区域。

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用户触手可用，从而提高性能。可以为灾难恢复、地理位置相隔很远的数据中心、分支机构、云或云中的可用性区域使用区域。

在本文中，术语“本地”是指正在讨论的区域。例如，“VDA 在本地 Cloud Connector 中注册”是指 VDA 在 VDA 所在区域的 Cloud Connector 中注册。

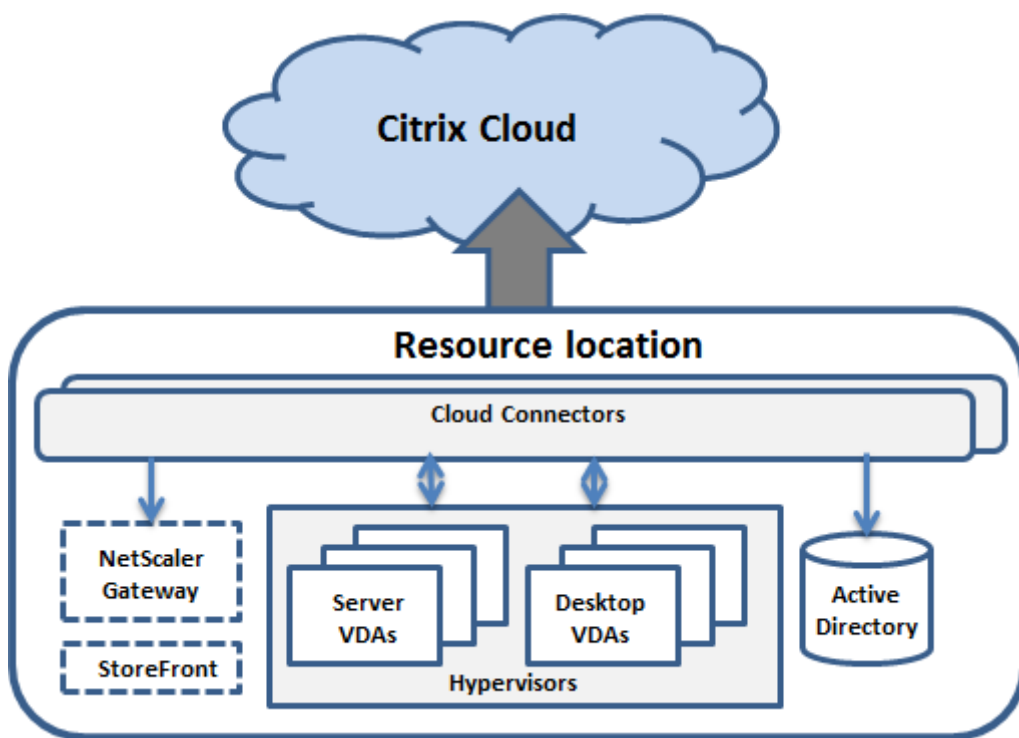
### 与本地 **Citrix Virtual Apps and Desktops** 环境中的区域的区别

Citrix DaaS 环境中的区域相似，但与本地 Citrix Virtual Apps and Desktops 部署中的区域不同。

- 在 Citrix DaaS 中，区域在您创建资源位置并向其中添加 Cloud Connector 时自动创建。与本地部署不同，Citrix DaaS 环境不会将区域分类为主要区域或卫星区域。
- 在 XenApp 6.5 及早期版本中，区域包含在数据收集器中。Citrix DaaS 不对区域使用数据收集器。此外，故障转移和首选区域的工作方式不同。

### 区域中包含的对象

区域与资源位置等效。创建资源位置并安装 Cloud Connector 时，将自动为您创建一个区域。每个区域可以包含不同的资源组，具体取决于您的独特需求和环境。



每个区域必须始终至少安装一个 Cloud Connector，最好安装两个或更多个，以实现冗余。

可以将计算机目录、虚拟机管理程序、主机连接、用户和应用程序放置在区域中。区域还可以包含 Citrix Gateway 和 StoreFront 服务器。区域中必须安装 StoreFront 服务器，才能使用本地主机缓存功能。

Citrix Workspace 和 Citrix Gateway 服务支持区域。

如果将多个项目放置在一个区域中，则将影响 Citrix DaaS 与这些项目以及与其相关的其他对象的交互方式。

- 某个虚拟机管理程序连接放置在一个区域中时，假定通过该连接管理的所有虚拟机管理程序也都位于该区域中。
- 某个计算机目录放置在一个区域中时，假定该目录中的所有 VDA 都位于该区域中。
- 可以将 Citrix Gateway 实例添加到区域中。创建资源位置时，系统会向您提供用于添加 Citrix Gateway 的选项。某个 Citrix Gateway 与某个区域关联后，使用与该区域中的 VDA 的连接时，优先使用该 Citrix Gateway。
- 理想情况下，区域中的 Citrix Gateway 用于从其他区域或外部位置传入到该区域的用户连接。您也可以将其用于区域内的连接。
- 创建更多资源位置并在其中安装 Cloud Connector 后（这将自动创建更多区域），可以在区域之间移动资源。这一灵活性存在隔离彼此紧邻时提供最佳工作效果的项目的风险。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。因此，在区域之间移动项目之前，请考虑预料之外的潜在影响。请将其使用的目录和主机连接保留在相同的区域中。

如果某个区域与 Citrix Cloud 之间的连接中断，本地主机缓存功能将启用区域中的 Cloud Connector 以继续代理与该区域中的 VDA 的连接。（该区域中必须安装 StoreFront。）例如，如果办公室里的工作人员使用本地 StoreFront 站点访问其本地资源，则此类部署会非常有效，即使将其办公室连接到企业网络的 WAN 链接出现故障也是如此。有关详细信息，请参阅[本地主机缓存](#)。

## VDA 的注册位置

VDA 的最低版本必须为 7.7，才能使用以下区域注册功能：

- 区域中的 VDA 在本地 Cloud Connector 中注册。
  - 只要该 Cloud Connector 能够与 Citrix Cloud 通信，常规操作即可继续进行。
  - 如果该 Cloud Connector 可运行，但无法与 Citrix Cloud 通信（并且该区域具有本地 StoreFront），则将进入本地主机缓存中断模式。
  - 如果某个 Cloud Connector 出现故障，该区域中的 VDA 将尝试在其他本地 Cloud Connector 中注册。一个区域中的 VDA 绝不会尝试在另一个区域的 Cloud Connector 中注册。
- 如果在某个区域中（使用 Citrix Cloud 管理控制台）添加或删除 Cloud Connector，并且启用了自动更新，该区域中的 VDA 将收到更新后的可用本地 Cloud Connector 列表，以便其知晓可以注册的位置并接受从其发出的连接。
- 如果将某个计算机目录移动到另一个区域（使用“完整配置”管理界面），该目录中的 VDA 将重新在移动了该目录的区域的 Cloud Connector 中注册。移动目录时，请务必同时将任何关联的主机连接移动到相同的区域。
- 中断过程中（某个区域中的 Cloud Connector 无法与 Citrix Cloud 通信时），只有与在该区域中注册的计算机关联的资源可用。

## 区域首选项

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。

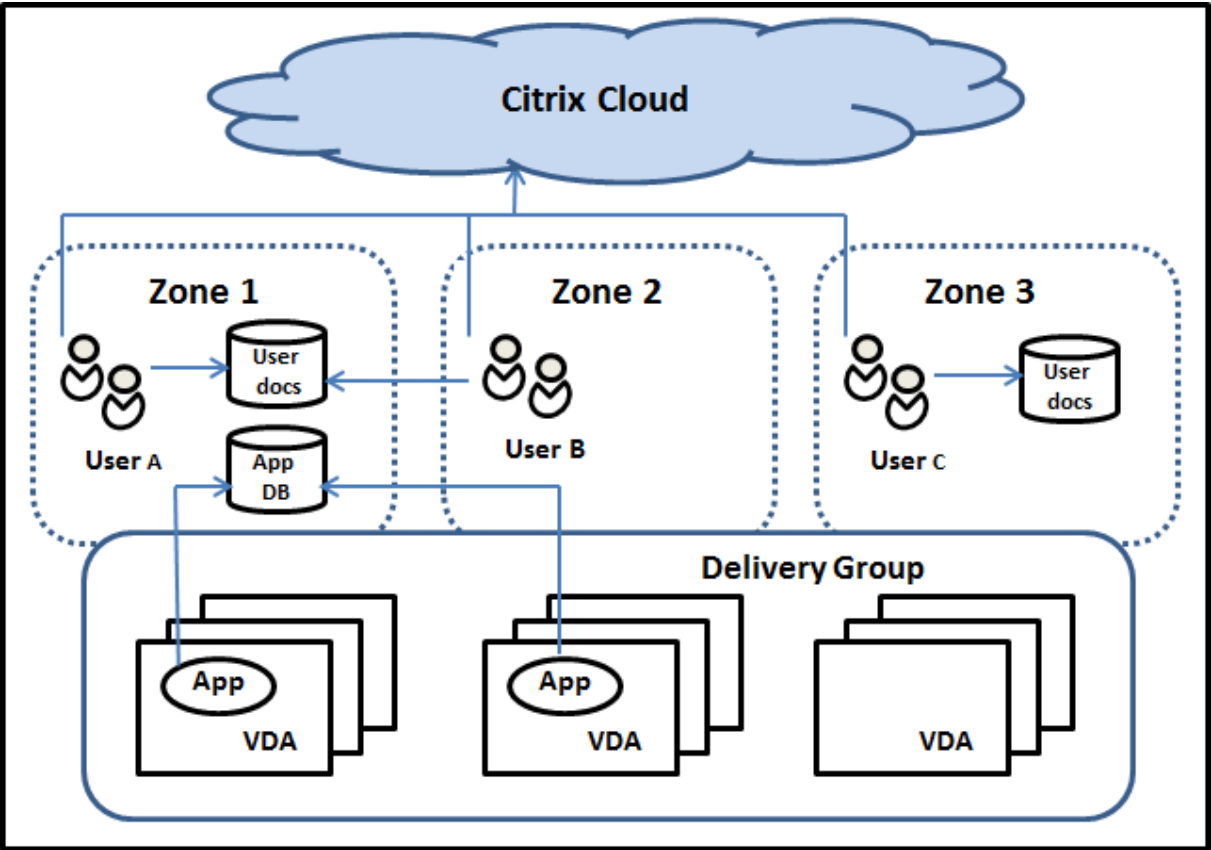
### 区域首选项的工作方式

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。（用户位置需要的最低版本为 StoreFront 3.7 和 Citrix Gateway（以前称为 NetScaler Gateway）11.0-65.x。

下图显示了多区域配置示例。





在此示例中，VDA 分布在三个区域中，但都处在同一个交付组中。因此，Citrix DaaS Broker 可以选择针对用户启动请求使用哪个 VDA。此示例说明了用户可以在不同的位置运行其 Citrix Workspace 应用程序端点。用户 A 使用区域 1 中安装了 Citrix Workspace 应用程序的设备。用户 B 使用区域 2 中的设备。同样，用户的文档可以存储在不同的位置。用户 A 和 B 使用区域 1 中的共享。用户 C 使用区域 3 中的共享。此外，其中一个已发布的应用程序使用区域 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，代理会使用这些关联来帮助选择将会在其中启动会话的区域（如果资源可用）。您：

- 通过向某个区域添加用户的方法来为用户配置主区域。
- 请通过编辑应用程序的属性来为某个应用程序配置主区域。

一名用户或一个应用程序一次只能有一个主区域。（在由于用户组成员关系而出现多个区域成员关系时，可能会出现用户的例外。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。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（或不使用）区域偏好。

- 强制用户主区域使用：在一个交付组中，可以指定“应在用户的主区域（如果该用户具有一个主区域）中启动一个会话，并且资源在主区域中不可用时不会故障转移至另一个区域”。如果您需要避免在区域之间复制大型配置文件或数据文件而带来的风险，这一限制非常有用。换言之，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，可以指定“仅在该区域中启动应用程序，并且资源在应用程序的主区域中不可用时不会故障转移到另一个区域”。
- 无应用程序主区域，并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，还可以指定“在启动该应用程序时不考虑任何已配置的用户区域”。例如，如果希望用户在靠近其计算机的 VDA 上运行一个特定应用程序，请使用用户位置区域偏好，即使某些用户可能拥有不同的主区域也是如此。

### 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，或一个已经在运行正在启动的资源的会话），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，则系统可能会创建新的会话。此操作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. 重新连接到非首选区域中的现有断开连接的会话。
3. 在首选区域中启动新的会话。
4. 重新连接到非首选区域中的现有已连接会话。
5. 在非首选区域中启动新会话。

### 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。代理完成选择之后，该区域将用于后续的会话启动，直到用户的组成员关系变更为止。

- 用户位置区域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。必须将 Citrix 配置为将 IP 地址的范围与特定区域相关联。必须通过 StoreFront 将发现的区域标识传递到 Citrix DaaS。

虽然编写 [Zone Preference Internals](#)（区域偏好时间间隔）博客文章的目的是供区域本地使用，但是其中包含相关的技术详细信息。

### 管理区域的权限

完全权限管理员可以执行所有受支持的区域管理任务。在区域之间移动项目不需要区域相关权限（区域读取权限除外）。但是，必须对要移动的区域具有编辑权限。例如，要将计算机目录从一个区域移动到另一个区域，必须对该目录具有编辑权限。

如果使用 **Citrix Provisioning**：当前的 Citrix Provisioning 控制台无法识别区域，因此，Citrix 建议您使用管理 > 完整配置界面创建要放置在特定区域中的计算机目录。创建目录后，可以使用 Citrix Provisioning 控制台在该目录中预配计算机。

### 创建区域

在 Citrix Cloud 中创建一个资源位置，然后向该资源位置中添加一个 Cloud Connector 时，Citrix DaaS 将自动创建一个区域并命名。以后您可以选择性添加说明。

创建多个资源位置（区域将自动创建）后，可以将资源从一个区域移动到另一个区域。

资源位置和区域将定期同步，通常情况下，大约每隔 5 分钟同步一次。因此，如果您在 Citrix Cloud 中更改了某个资源位置的名称，该变更将在 5 分钟内传播到关联的区域。

### 添加或更改区域说明

虽然您无法更改区域的名称，但是可以添加或更改其说明。

1. 在管理 > 完整配置中，选择左侧窗格中的区域。
2. 在中间窗格中选择一个区域，然后在操作栏中选择编辑区域。
3. 添加或更改区域说明。
4. 选择确定或应用。

## 将资源从一个区域移动到另一个区域

1. 在管理 > 完整配置中，选择左侧窗格中的区域。
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，或者在操作栏中选择移动项目，然后指定要将项目移动到的区域。（虽然您可以选择 Cloud Connector，但是无法实际将其移动到其他区域。）

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所有项目。

谨记：如果计算机目录使用连接到虚拟机管理程序或云服务的主机连接，请确保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

不能删除区域。但是，可以删除资源位置（在删除其 Cloud Connector 之后）。删除资源位置将自动删除区域。

- 如果某个区域不包含任何项目（例如，目录、连接、应用程序或用户），下次在区域与资源位置之间同步时将删除该区域。同步每五分钟进行一次。
- 如果区域包含项目，则会在删除所有项目后自动删除该区域。

## 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. 在管理 > 完整配置中，选择左侧窗格中的区域。
2. 在中间窗格中选择一个区域，然后在操作栏中选择向区域中添加用户。
3. 在将用户添加到区域对话框中，选择添加，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. 选择确定。

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。

1. 在管理 > 完整配置中，选择左侧窗格中的区域。
2. 在中间窗格中选择一个区域，然后在操作栏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，选择删除，然后选择要从该区域中删除的用户和用户组。此操作将仅从区域中删除用户。这些用户保留在其所属的交付组中。
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。

- [创建交付组](#)或[向现有组中添加应用程序](#)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，请在左侧窗格中选择区域。选择一个应用程序，然后选择操作栏中的属性。

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

如果您有多个区域，则可以在添加主机连接或创建目录时指定一个区域。区域将按字母顺序在选择列表中列出。默认情况下，选择按字母顺序列出的第一个名称。

## 故障排除

完整配置为您提供主动警报，以确保您的 [本地主机缓存](#) 和区域配置正确，这样您就可以在中断影响用户之前及时解决问题。此功能有助于保持用户对任务关键型工作负载的持续访问权限。

出现问题的每个区域都会出现“故障排除”选项卡。

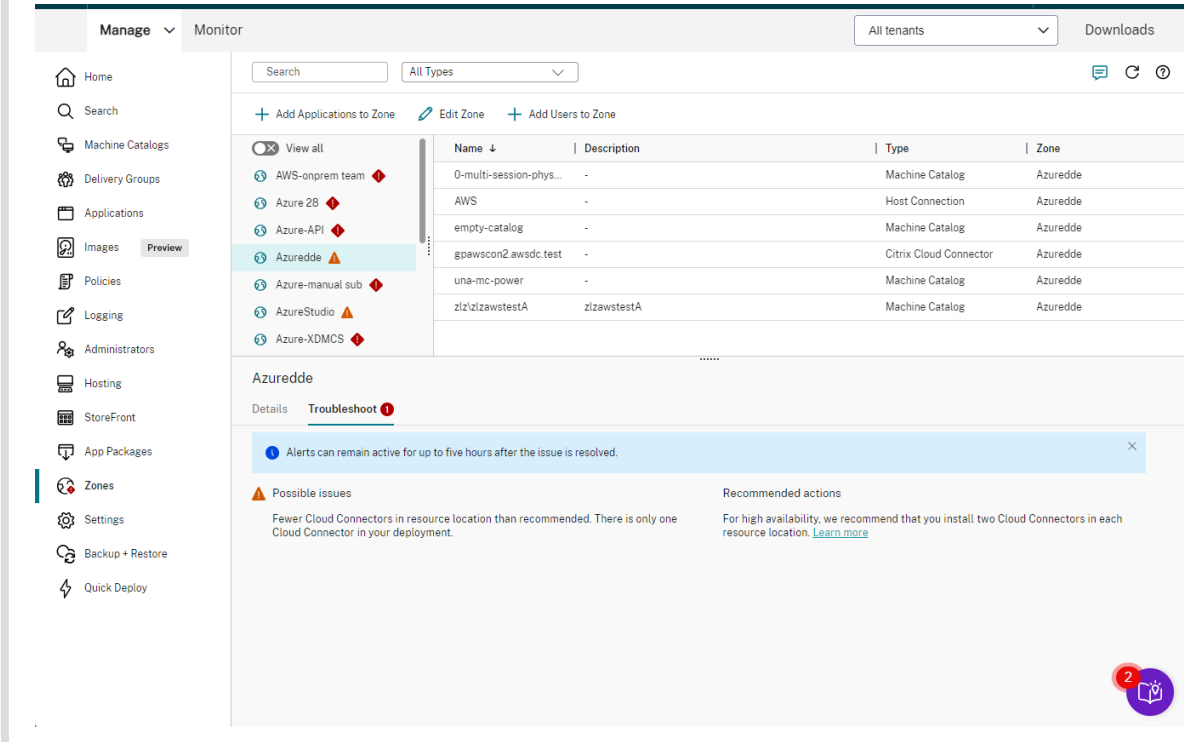
要检查与区域相关的问题，请按照以下步骤操作：

1. 转至 完整配置 > 区域，然后单击带有警告图标的区域。
2. 转到下部窗格中的“故障排除”选项卡，阅读那里的信息。

注意：

诊断每小时更新一次。

故障排除信息示例：



下表提供了与区域相关的警告和错误的完整列表：

| 严重性 | 可能的问题                                                                   | 建议的操作                                                                  |
|-----|-------------------------------------------------------------------------|------------------------------------------------------------------------|
| 警告  | 资源位置包含多个域。如果资源位置有多个域，则如果未正确配置信任关系，VDA 注册可能需要更长时间。此外，VDA 可能无法在高可用性模式下注册。 | 确保正确配置此资源位置中域之间的信任关系。请参阅 <a href="#">Citrix Cloud Connector 技术细节</a> 。 |
| 警告  | 资源位置的主机连接数超出推荐值。超过该限制可能会导致性能下降，从而影响用户体验。                                | 将此资源位置的主机连接数减少到不超过建议的限制。请参阅 <a href="#">限制</a> 。                       |
| 警告  | 逻辑 CPU 处理器数量少于推荐值。在高可用性模式下，性能可能会降低。                                     | 确保每个 Cloud Connector 都满足最低逻辑 CPU 处理器要求。请参阅 <a href="#">本地主机缓存</a> 。    |

| 严重性 | 可能的问题                                                                                               | 建议的操作                                                                                                                     |
|-----|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| 警告  | 资源位置中的云连接器少于建议的数量。您的部署中只有一个 Cloud Connector。                                                        | 为了实现高可用性，我们建议您在每个资源位置安装两个 Cloud Connector。请参阅 <a href="#">Citrix Cloud Connector 技术细节</a> 。                               |
| 错误  | 资源位置上的 VDA 比建议的多。在高可用性模式下，本地主机缓存仅允许注册 10,000 个 VDA。其他 VDA 的注册尝试将失败。                                 | 将此资源位置中的 VDA 数量减少到不超过建议的限制。请参阅 <a href="#">限制</a> 。                                                                       |
| 错误  | 无法访问该资源域中的 Cloud Connector。无法访问该资源域中的任何 Cloud Connector。除非为您的部署配置了本地主机缓存或服务连续性，否则此资源位置中的 VDA 可能不可用。 | 查看资源域中 Cloud Connector 的连接，并检查注册表以验证是否强制使用注册表执行 LHC 模式。如果注册表不强制使用 LHC，可以考虑运行 Cloud Connector 连接检查实用程序。如果问题仍然存在，请开立一个支持票证。 |

## Monitor

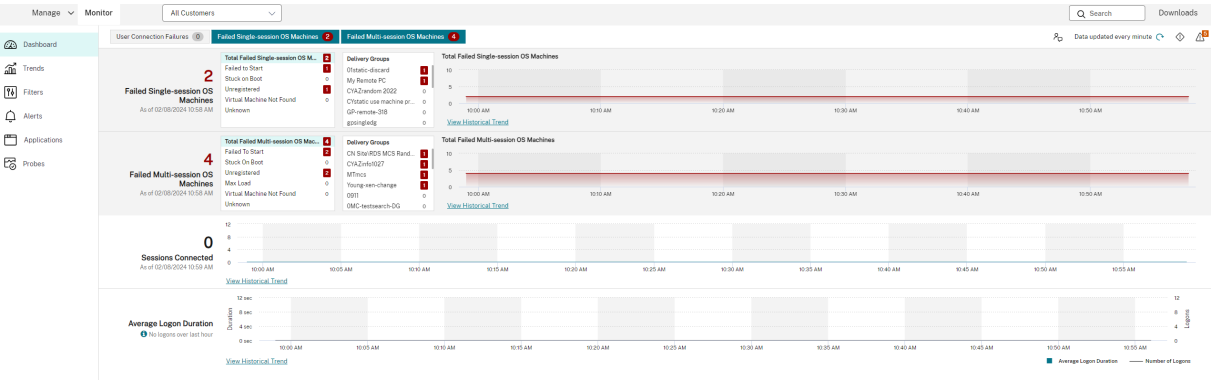
February 20, 2024

管理员和技术支持人员可以在 **Monitor** 中通过监视和故障排除控制台监视 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）。**Monitor** 选项卡显示一个控制板，用于对订阅者进行监视、故障排除和执行支持任务。

注意：

Monitor 可用作 Director 控制台，用于监视 Citrix Virtual Apps and Desktops [当前版本](#)和 [LTSR](#) 部署并对其故障排除。

要访问 **Monitor**，请登录 [Citrix Cloud](#)。在左上角的菜单中，选择我的服务 > **DaaS**。单击 **Monitor**。



注意：

查看 Citrix Monitor 时推荐的最佳屏幕分辨率为 1440 x 1024。

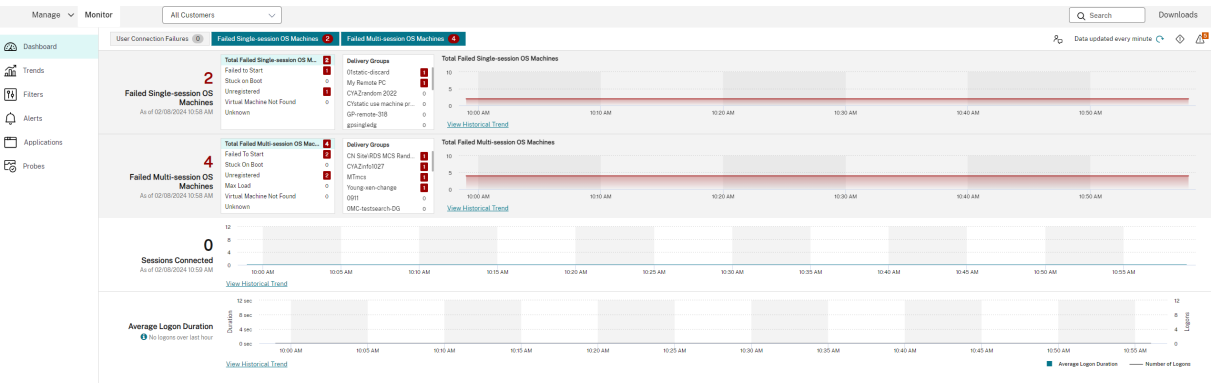
Monitor 提供：

- 使用集成了 Analytics 和 Performance Manager 的统一控制台访问来自 Broker Agent 的实时数据。
- Analytics 包括面向运行状况和容量保障以及历史趋势的性能管理功能，可识别由您的 Citrix DaaS 环境中的瓶颈。
- 存储在 Monitor 数据库中的历史数据，用于访问配置日志记录数据库。
- 可以了解 Citrix DaaS 的虚拟应用程序、桌面和用户的最终用户体验。
- Monitor 使用故障排除控制板。此控制板提供对 Citrix DaaS 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。

站点分析

March 30, 2024

“监视” 控制板提供一个中央位置来监视站点的运行状况和使用情况。



如果当前没有故障且在过去 60 分钟内没有发生任何故障，则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。



| 面板                              | 说明                                                                                                                             |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| 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，根据每个交付组对该数字进行了进一步分类。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 <a href="#">应用程序</a> 。 |
| 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 | 过去 60 分钟内的失败总数根据每个交付组进行分类。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。                                      |
| 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。此平均值不包括早于 XenDesktop 7.0 的 VDA 的登录数据。有关详细信息，请参阅 <a href="#">诊断用户登录问题</a> 。                 |

注意：

当您使用的房东类型不支持任何特定指标时，不会显示该特定指标的图标。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（如前几节所述）解决问题：

- [控制用户计算机电源](#)
- [阻止与计算机连接](#)

监视会话

如果会话断开连接，则会话仍处于活动状态，其应用程序将继续运行。但是，用户设备不再与服务器通信。

| 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。此外，查看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 <a href="#">还原会话</a> 。 |

| 操作               | 说明                                                                                                                      |
|------------------|-------------------------------------------------------------------------------------------------------------------------|
| 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，这将打开“筛选器”视图。在这里，您可以显示基于所选交付组和交付组范围和使用情况的图形会话数据。                      |
| 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。您可以根据关联用户、交付组、会话状态和超过阈值时段的空间时间筛选会话。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 <a href="#">应用程序故障排除</a> 。 |
| 查看较长时间段内的数据      | 在趋势视图上，选择会话选项卡以深入查看更具体的使用情况数据。您可以在更长的时间内深入研究已连接和已断开连接的会话的数据。您可以查看过去 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：

假设用户设备正在旧版 Virtual Delivery Agent (VDA) 上运行，例如版本 7 之前的 VDA 或 Linux VDA。在这种情况下，监视器无法显示有关会话的完整信息。相反，它会显示一条消息，提示该信息不可用。

桌面分配规则限制：

通过“管理”控制台，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 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，监视器不支持 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，您无法在 Monitor 中将特定的桌面映射到计算机。

您可以将 StoreFront 中显示的分配桌面映射到监视中显示的交付组名称。要进行映射，请使用以下 PowerShell 命令：

```
1 Get-BrokerDesktopGroup | Where-Object {
2     $_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
3         $_.PublishedName -eq "<Name on StoreFront>" }
4     ).DesktopGroupUid }
5 | Select-Object -Property Name, Uid
6 <!--NeedCopy-->
```

如[博客](#)中所述，使用 Remote PowerShell SDK 运行前面的 PowerShell 命令。

在活动管理器中禁止显示运行中的应用程序

默认情况下，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。所有有权访问活动管理器功能的管理人员都可以查看此信息。对于委派管理员角色，此视图包括完全管理员、交付组管理员和帮助台管理员。

为了保护用户及其正在运行的应用程序的隐私，您可以禁用“应用程序”选项卡来列出正在运行的应用程序。要进行此活动，请在 VDA 上修改 HKEY\_LOCAL\_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed 上

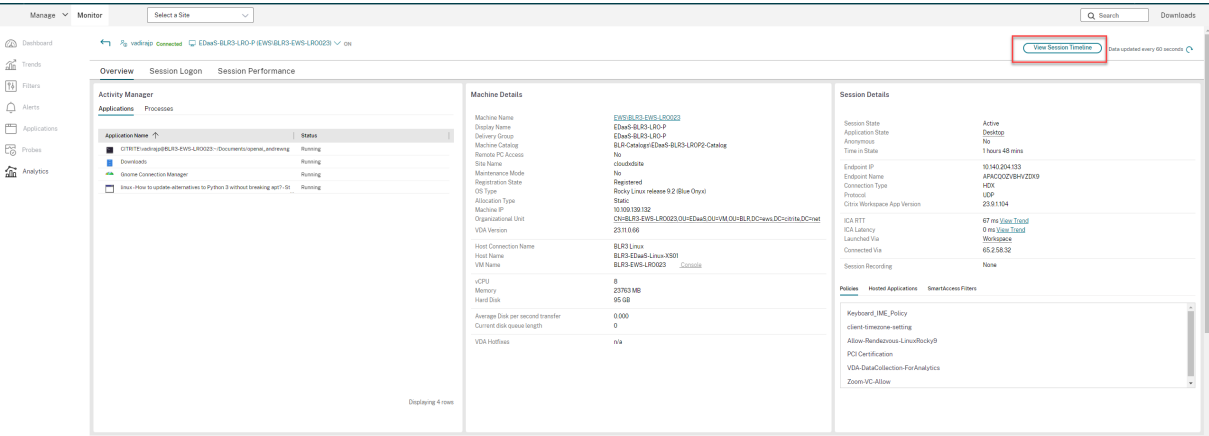
的注册表项。默认情况下，该注册表项设置为 1。将该值更改为 0，这意味着信息不是从 VDA 收集的，因此不会显示在活动管理器中。

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。

访问“Citrix Analytics for Performance - 会话详细信息”

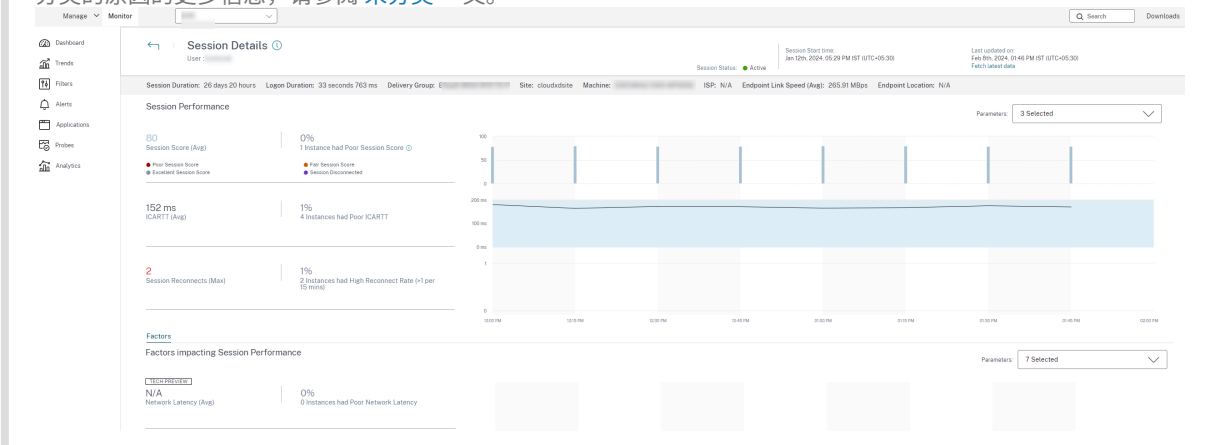
可以访问 Citrix Analytics for Performance 中的“会话详细信息”页面。在 Activity Manager 的“会话详细信息”部分中单击“查看会话时间表”，可在 Monitor 中打开 Citrix Analytics for Performance 的“会话详细信息”页面。



注意：

此功能要求您拥有有效的 Citrix Analytics for Performance 授权。

会话详细信息适用于归类为“优秀”、“一般”或“差”的 Citrix Analytics for Performance 会话。有关会话未分类的原因的更多信息，请参阅 [未分类](#) 一文。



您最多可以查看最近三天会话体验的趋势。该趋势视图还包括影响会话体验的因素。此信息补充了 Monitor 中提供的实时数据，帮助台管理员在解决与会话体验相关的问题时会使用这些数据。

有关“会话详情”页面的更多信息，请参阅 [会话详细信息](#)。

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。

Session Details

Session Control

Shadow user

Send Message

|                   |                         |
|-------------------|-------------------------|
| Session State     | Active                  |
| Application State | <a href="#">Desktop</a> |
| Anonymous         | No                      |
| Time in State     | 8 hours 24 mins         |

Endpoint IP

Endpoint Name

Connection Type

Protocol

Citrix Workspace App Version

ICA RTT

ICA Latency

Launched Via

Connected Via

Session Recording

None

Policies

Hosted Applications

SmartAccess Filters

Unfiltered

Policy1

使用“会话详细信息”窗格中的“会话控制”下拉菜单注销或断开会话。

- 对于 **HDX** 连接类型：
  - 如果 EDT 用于 HDX 连接，协议显示为 **UDP**。
  - 如果 TCP 用于 HDX 连接，协议显示为 **TCP**。
- 对于 **RDP** 连接类型，协议显示为不适用。

配置了自适应传输时，会话传输协议根据网络状况在 EDT（基于 UDP）与 TCP 之间动态切换。如果无法使用 EDT 建立 HDX 会话，它将回退到 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 格式的报告包括以图表和表格表示的趋势。CSV 格式的报告包含可用于生成视图或存档的表格数据。

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”，然后输入报告的名称和格式。

Monitor 根据您选择的筛选条件生成报告。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，会导致监视器服务器、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。

| 报告格式  | 默认的受支持记录数                 |
|-------|---------------------------|
| PDF   | 500                       |
| Excel | 100,000                   |
| CSV   | 100000（在会话选项卡中为 10000000） |

错误处理

导出操作期间可能会遇到的错误：

- **Director** 已超时：此错误可能是由于 Director 服务器或监视服务上的网络问题或资源使用率过高所致。
- 监视器已超时：此错误可能是由于网络问题或监视服务或 SQL 服务器上的资源使用率过高所致。
- 正在进行的最大并发导出或预览操作：在特定时间只能运行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操作。

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

要对您在监视器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：

此功能不适用于使用 Remote PC Access 的物理计算机或计算机。

| 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，选择监视器中显示为“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 | 无需先执行任何关闭程序即可重新启动虚拟机。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   | 无需先执行任何关闭程序即可关闭 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。 |
| 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。如果用户当前已登录，则维护模式将在注销所有用户后生效。对于未注销的用户，发送一条消息，通知他们计算机已在特定时间关闭。您可以使用电源控制来强制关闭计算机。

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。

如果用户尝试在分配的桌面处于维护模式时连接到该桌面，则会显示一条消息，表明该桌面不可用。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工作应用程序性能。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。它显示了如下指标：

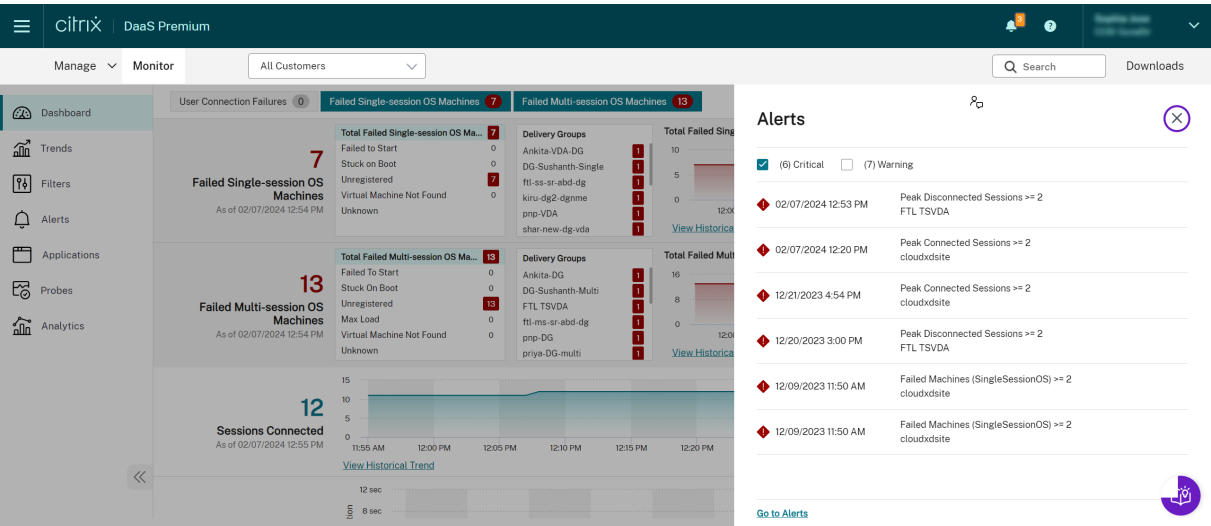
- 探测结果
- 每个应用程序的实例数
- 与已发布应用程序相关的错误和错误

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

February 20, 2024

警报在 Monitor 中的控制板上以及其他高级别视图中显示，带有警告和严重警报符号。警报每分钟自动更新一次；也可以根据需求更新警报。

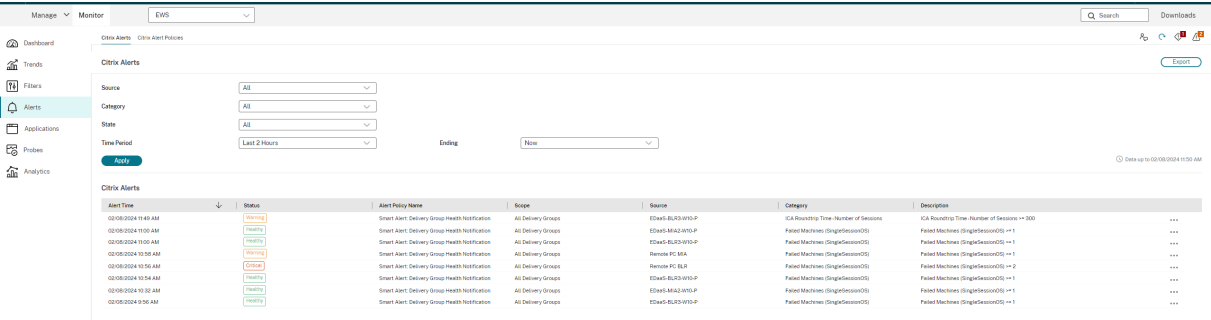


警告警报（琥珀色三角形）指示已达到或超过条件的警告阈值。

严重警报（红色圆形）显示已达到或超过条件的严重阈值。

可以查看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 Monitor 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 警报是指源自 Citrix 组件的警报。可以在 Monitor 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](#)。

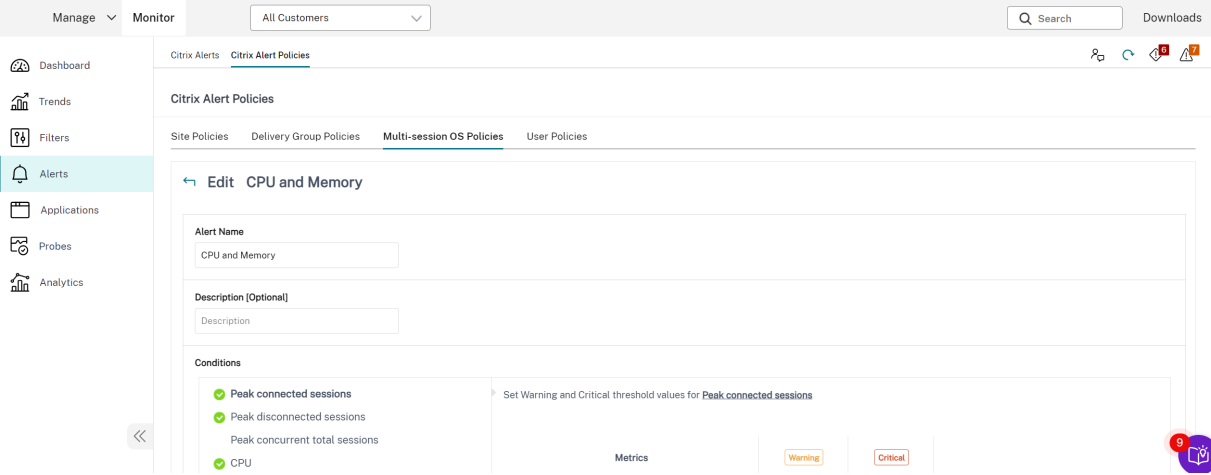
智能警报策略

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。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。

仅当 Monitor 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。





创建警报策略

Citrix AlertsCitrix Alert Policies

Citrix Alert Policies

Site PoliciesDelivery Group PoliciesMulti-session OS PoliciesUser Policies

← Create Alert Policy

Alert Name

Description [Optional]

Description

Conditions

Peak connected sessions

Peak disconnected sessions

Peak concurrent total sessions

CPU

Memory

Connection failure rate

Connection failure count

Failed machines (Single-session OS)

Failed machines (Multi-session OS)

Average logon duration

Set Warning and Critical threshold values for Peak connected sessions

| Metrics                     | Warning | Critical |
|-----------------------------|---------|----------|
| Peak connected sessions:    |         |          |
| Re-Alert interval (in min): | 60      | 60       |

Reset values

Scope

cloudxdsite

Send mails in preferred language to [optional]

User/Email address

EN - Eng... ▾

Add

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。电子邮件通知通过 SendGrid 发

送。确保电子邮件地址 [donotreplynotifications@citrix.com](mailto:donotreplynotifications@citrix.com) 在您的电子邮件设置中列入白名单。

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。

注意：

删除警报策略后，该策略生成的警报通知最多可能需要 30 分钟才能停止。

## 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。

### 最大已连接会话数

- 查看 Monitor 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 Monitor 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 Monitor 中的 Monitor “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%

## 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 Monitor 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 Monitor 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。有关更多信息，请参阅 [Citrix ADM 文档](#)。
- 如果 Citrix ADM 不可用，请检查“Monitor 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。

## 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。有关更多信息，请参阅 [Citrix ADM 文档](#)。
- 如果 Citrix ADM 不可用，请与网络团队联系共同确定根本原因。

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。有关更多信息，请参阅 [Citrix ADM 文档](#)。
- 如果 Citrix ADM 不可用，请与网络团队联系共同确定根本原因。

## 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。

### 出现故障的计算机数 (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 Monitor 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 Monitor 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：

- 作用域：交付组、多会话操作系统作用域
- 阈值：警告 - 1、严重 - 2

## 故障计算机 (以% 为单位)

交付组中出现故障的单会话和多会话操作系统计算机的百分比是根据故障计算机的数量计算的。此警报条件允许您将警报阈值配置为交付组中的故障计算机的百分比，每 30 秒计算一次。

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](#)。

## 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“Monitor”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 Monitor 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

Monitor 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“管理”选项卡中创建宿主连接。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。

| 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。 |

| 警报           | 支持的虚拟机管理程序                       |                     | 触发者                                                 | 条件                                         | 配置 |
|--------------|----------------------------------|---------------------|-----------------------------------------------------|--------------------------------------------|----|
|              |                                  |                     |                                                     |                                            |    |
| 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](#) 或者查看 “VMware vCenter 警报” 文档。

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 Monitor 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 Monitor 中完成。

- 重要提示：
- 所有时间在一天以上的虚拟机管理程序警报都将自动消除。
  - 由虚拟机管理程序触发的警报将在 Monitor 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 Monitor 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将继续显示在 Monitor 中且必须显式消除。
  - 在 Monitor 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。

Citrix AlertsCitrix Alert Policies

Citrix Alerts

SourceAll

CategoryAll

StateAll

Time Period

EndingNow

Apply

Citrix Alerts

Alert Time

Alert Policy Name

Scope

Source

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

Citrix AlertsCitrix Alert Policies

Citrix Alerts

Export

SourceAll

CategoryAll

StateAll

Time PeriodLast 2 Hours

EndingNow

Apply

Data up to 02/07/2024 1:10 PM

Citrix Alerts

| Alert Time          | Status   | Alert Policy Name | Scope                       | Source           | Category                    | Description                 |
|---------------------|----------|-------------------|-----------------------------|------------------|-----------------------------|-----------------------------|
| 02/07/2024 1:08 PM  | Warning  | DG-alert          | Ankita-VDA-DG, DG1, FTL ... | fit-ms-sr-abd-dg | Peak Disconnected Sessio... | Peak Disconnected Sessio... |
| 02/07/2024 12:53 PM | Critical | DG-alert          | Ankita-VDA-DG, DG1, FTL ... | FTL TSVDA        | Peak Disconnected Sessio... | Peak Disconnected Sessio... |
| 02/07/2024 12:20 PM | Critical | kiru test         | cloudxdsite                 | cloudxdsite      | Peak Connected Sessions     | Peak Connected Sessions ... |
| 02/07/2024 12:20 PM | Warning  | foo2              | cloudxdsite                 | cloudxdsite      | Peak Connected Sessions     | Peak Connected Sessions ... |
| 02/07/2024 12:20 PM | Warning  | foo1              | cloudxdsite                 | cloudxdsite      | Peak Connected Sessions     | Peak Connected Sessions ... |
| 01/08/2024 1:57 PM  | Warning  | DG-alert          | Ankita-VDA-DG, DG1, FTL ... | Ankita-DG        | Peak Disconnected Sessio... | Peak Disconnected Sessio... |

过滤数据以排除故障

August 14, 2023

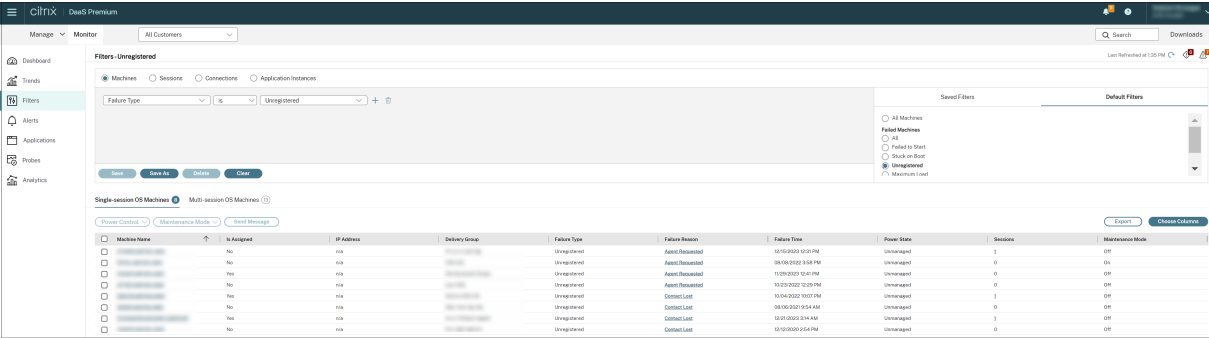
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1241



当您在仪表板上单击数字或从“筛选器”选项卡中选择预定义的默认筛选器时，“筛选器”视图将打开，显示基于所选计算机或故障类型的数据。

您可以创建所有交付组中的计算机、连接、会话和应用程序实例的自定义筛选视图，并保存搜索结果以供日后访问。您可以编辑预定义筛选器并将其另存为“已保存”筛选器。



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。
- 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。单击“关联用户”为该用户打开“活动管理器”。单击 端点 名称可打开该端点的活动管理器。单击“查看详细信息”将分别打开“用户详细信息”或“端点详细信息”页面。有关更多信息，请参阅 [用户详细信息](#)。
- 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。此视图显示多会话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。

2. 从“已保存”或“默认”筛选器列表选择一个筛选器。

3. 使用下拉列表选择更多筛选条件。

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. 要稍后打开筛选器，请从“筛选器”视图中选择视图（计算机、会话、连接或应用程序实例），然后选择保存的筛选器。

7. 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。

8. 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。

9. 在计算机视图和连接视图中，单击故障计算机或失败连接的故障原因以获取有关故障的详细说明以及排除故障的建议操作。[Citrix Director Failure Reasons Troubleshooting Guide](#)（《Citrix Director 故障原因排除指南》）中提供了计算机故障和连接失败的故障/失败原因和建议的操作。

10. 在计算机视图中，单击计算机名称链接转到相应的计算机详细信息页面。此页面显示计算机的详细信息、提供电源控制、显示 CPU、内存、磁盘监视以及 GPU 监视图。此外，单击查看历史利用率可查看计算机的资源利用率趋势。有关详细信息，请参阅[计算机故障排除](#)。
11. 在应用程序实例视图中，可根据大于某个阈值时间段的空闲时间进行排序或过滤。选择要结束的空闲应用程序实例。注销或断开连接应用程序实例会结束在同一会话中的所有活动应用程序实例。有关详细信息，请参阅[应用程序故障排除](#)。如果 VDA 为 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。

注意：

通过“管理”控制台，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 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，监视器不支持 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，不能在监视器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监视器中显示的交付组名称，请使用以下 PowerShell 命令：使用远程 PowerShell SDK 运行 PowerShell 命令，如[博客](#)中所述。

```
1 Get-BrokerDesktopGroup | Where-Object {  
2     $_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {  
3         $_.PublishedName -eq "<Name on StoreFront>" }  
4     }).DesktopGroupUid }  
5 | Select-Object -Property Name, Uid  
6 <!--NeedCopy-->
```

## 监视站点的历史趋势

January 23, 2024

“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

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了哪些人员或哪些方面。

要更改每个图形的默认作用域，请对数据应用其他过滤器。

注意：

- 将时间段设置为“上个月”（立即结束）或更短的时间时，会话、故障和登录性能趋势信息将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。
- Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）支持仅保留 90 天的历史数据。因此，监视器中一年内的趋势和报告将显示最近 90 天的数据。

## 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，以及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 Receiver for Windows 和 Citrix Receiver for Mac。此功能需要 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监视器中：

- 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。

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（仅在选择交付组中的多会话操作系统计算机时可用）和范围。负载评估器指数显示为 CPU、内存、磁盘或会话总数的百分比，并与上一个时间间隔内连接的用户数进行比较。

查看托管应用程序使用情况：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。此页面显示在所选交付组和时间段内启用了 AutoScale 并且已打开电源的多会话和单会话操作系统计算机的数量。此外，还提供了在所选交付组中启用 AutoScale 所实现的预计节省量，此百分比是使用每台计算机的成本计算的。

启用了 AutoScale 功能的计算机的使用趋势表明计算机的实际使用情况，使您能够快速评估站点的容量需求。

- 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：**

图表下方的网格实时显示基于交付组的计算机使用情况数据。数据包括与是否启用 AutoScale 无关的所有计算机的计算机可用性。网格中的“可用计数器”列中显示的计算机数包括处于维护模式的计算机。

监视数据合并取决于您选择的时间段。

- 一天和一周时间段的监视数据每小时合并一次。
- 一个月时间段的监视数据每天合并一次。

计算机状态在合并时读取，不考虑这一时间段内两者之间的任何变化。有关整合期限的信息，请参阅[Monitor API 文档](#)。

有关监视启用了 AutoScale 的计算机的详细信息，请参阅 [Autoscale](#) 一文。

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。

此功能需要 VDA 版本 **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。
- 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 上一个小时内收集的每小时 IOPS 平均值。)
- 计算机深入分析列出了平均 CPU 或平均内存使用率超过 1% 的进程，这可能意味着有时列出的进程少于 10 个。

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 VDA 版本 **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](#)。

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。

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额外列。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 查询创建自定义报告查询。为此，请选择 OData 查询选项，并粘贴复制的 OData 查询。可以保存结果查询供以后执行。

注意：

使用 OData 查询生成的“Preview and Export”（预览和导出）报告中的列名未本地化，而是以英语显示。

图表上的旗帜图标表示此特定时间范围内的重要事件或操作。将鼠标悬停在旗帜上并单击时，可列出事件或操作。

注意：

- 对于版本 7 之前的 VDA 版本，不会收集 HDX 连接登录数据。对于更早版本的 VDA，图表数据将显示为 0。
- 可以在“趋势”过滤器中选择在“管理”控制台中删除的交付组，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。

## 监视 **Autoscale** 托管的计算机

March 30, 2022

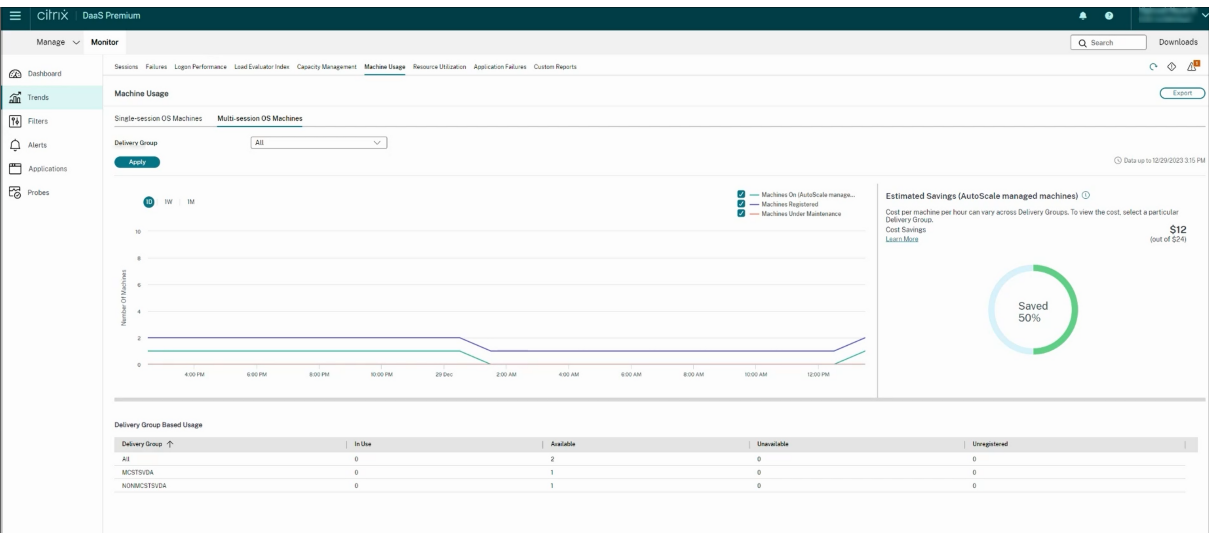
Autoscale 是一项电源管理功能，可对交付组中的所有已注册的多会话和单会话操作系统计算机进行主动电源管理。可以从管理选项卡为所选交付组配置 AutoScale。有关详细信息，请参阅 [Autoscale](#)。

可以从监视选项卡监视启用了 AutoScale 的计算机的主要指标。

### 计算机使用情况

监视 > 趋势 > 计算机使用情况页面显示在所选交付组和时间段内启用了 AutoScale 并且已打开电源的多会话和单会话操作系统计算机的总数。此指标表示交付组中计算机的实际使用情况。

在单会话操作系统计算机或多会话操作系统计算机选项卡中，选择交付组和时间段。

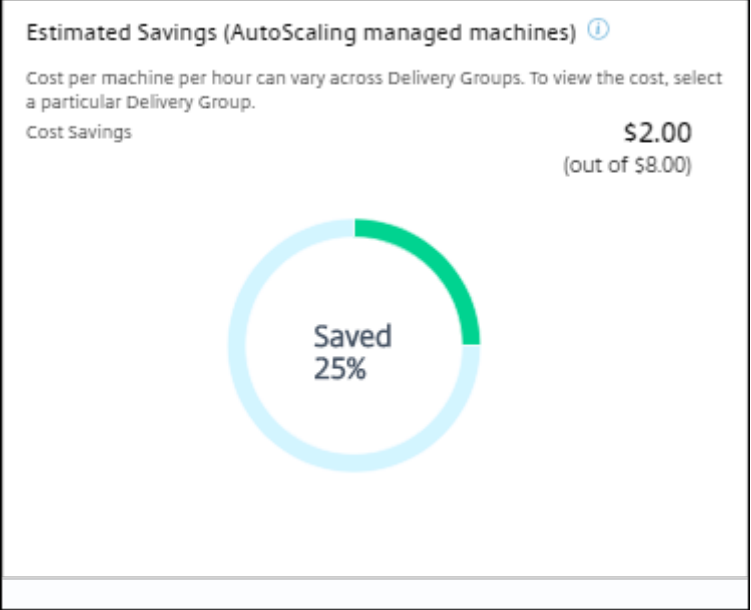


图表绘制了以下指标：

- 已打开的计算机 - 已打开电源并且启用了 AutoScale 的计算机数量
- 已注册的计算机 - 已注册的多会话或单会话操作系统计算机的数量
- 正在维护的计算机 - 已打开维护模式的多会话或单会话操作系统计算机的数量

预计节省量

监视 > 趋势 > 计算机使用情况页面还显示在所选交付组中启用了 AutoScale 而节省的预计成本。



预计节省量的计算方法是在管理 > 编辑交付组 > **Autoscale** 中配置的每台计算机每小时节省的百分比（美元）。有关配置每台计算机节省量的详细信息，请参阅 [Autoscale](#)。

选择所有交付组时，将显示所有交付组的预计节省量的平均值。

预计节省量有助于管理员整合现有的基础结构和规划容量，以实现最大限度的节省量和利用率。

计算机和会话的警报通知

“监视”控制板显示可进一步深入查看的警报通知。警报详细信息显示在监视 > 警报页面上。

- 要在交付组中创建警报策略，请转到监视 > 警报 > **Citrix** 警报策略 > 交付组策略。
- 在此位置，您可以设置以下警告和关键阈值：
  - 出现故障的计算机（单会话操作系统）和出现故障的计算机（多会话操作系统）
  - 交付组中的最大已连接会话数、最大已断开会话数和最大并发会话总数。
- 当交付组中的相应指标达到阈值时，将生成警报。

有关警示策略条件和创建新警报策略的更多详细信息，请参阅[警报和通知](#)。

计算机状态

- 监视 > 过滤器 > 计算机以表格格式显示所有计算机的电源状态。您可以按特定交付组进行过滤。
- 监视 > 过滤器 > 会话按计算机名称显示过滤器，以查看关联的会话及其实时状态。



- 在监视 > 趋势 > 会话中，选择交付组和时间段以查看会话趋势及其关联的指标。

有关详细信息，请参阅[过滤数据以排除故障](#)。

## 负载评估趋势

监视 > 趋势 > 负载评估器指数页面显示一个图表，其中包含与分布在多会话操作系统计算机之间的负载的详细信息。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。负载评估器指数显示为 CPU、内存、磁盘或会话总数的百分比，并与上一个时间间隔内连接的用户数进行比较。

## 部署故障排除

March 30, 2024

作为帮助台管理员，您可以搜索报告问题的用户。然后，显示与该用户相关的会话或应用程序的详细信息。

同样，您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。

以下操作可用：

- 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

July 24, 2023

### 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工作应用程序性能。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应用程序。

此功能需要 VDA 版本 7.15 或更高版本。



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。

对于自定义作用域管理员，监视器不显示在“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](#)。

应用程序失败策略设置控制故障和错误的可用性和显示。有关策略以及如何修改这些策略的详细信息，请参阅“监视策略设置”中的[应用程序故障监视策略](#)。

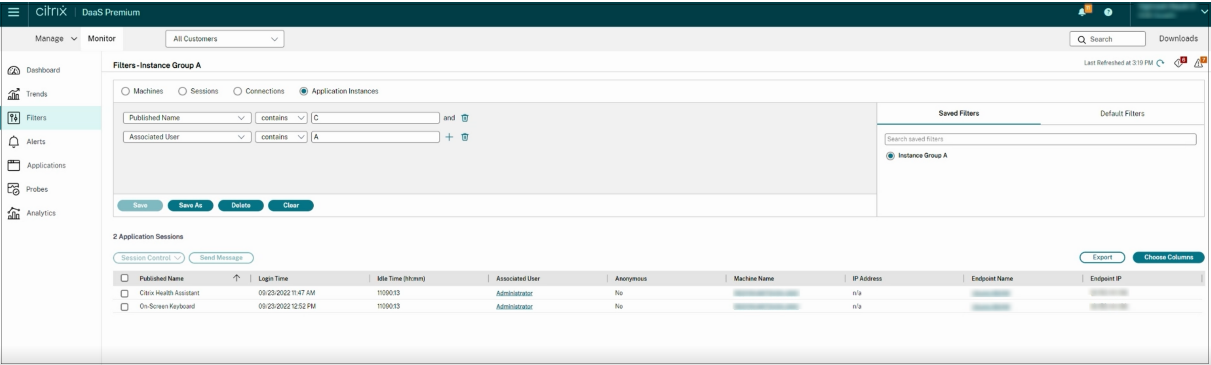
可以使用空闲时间指标对应用程序和会话进行故障排除以确定空闲时间超过特定时间限制的实例。

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多会话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。

在所有许可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。

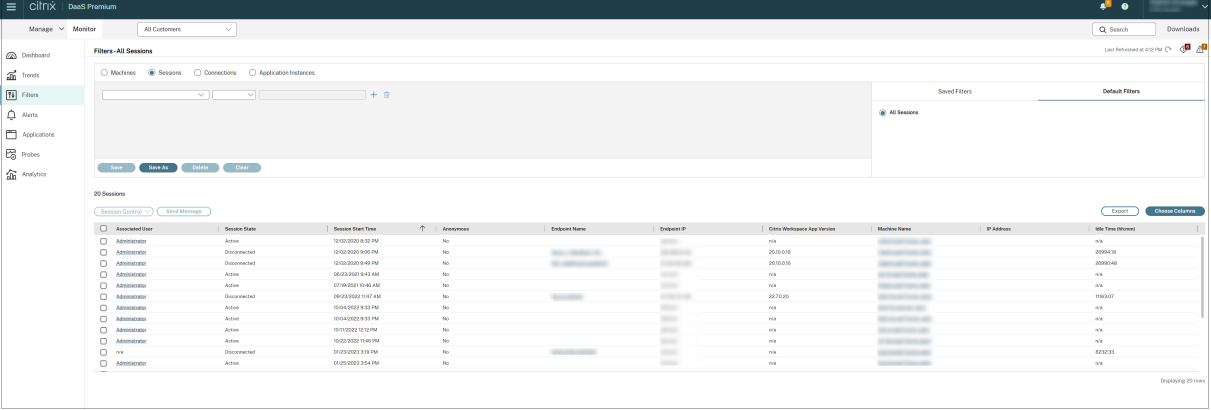


下面是一个过滤器的示例。对于过滤依据条件，请选择（应用程序的）发布的名称和空闲时间。然后，将空闲时间设置为大于或等于特定时间限制并保存该过滤器以供重复使用。从过滤的列表中，选择应用程序实例。选择用于发送消息的选项，或者从会话控制下拉菜单中，选择注销或断开连接，以结束实例。

注意：

注销或断开连接应用程序实例将注销或断开当前会话连接，因此会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。



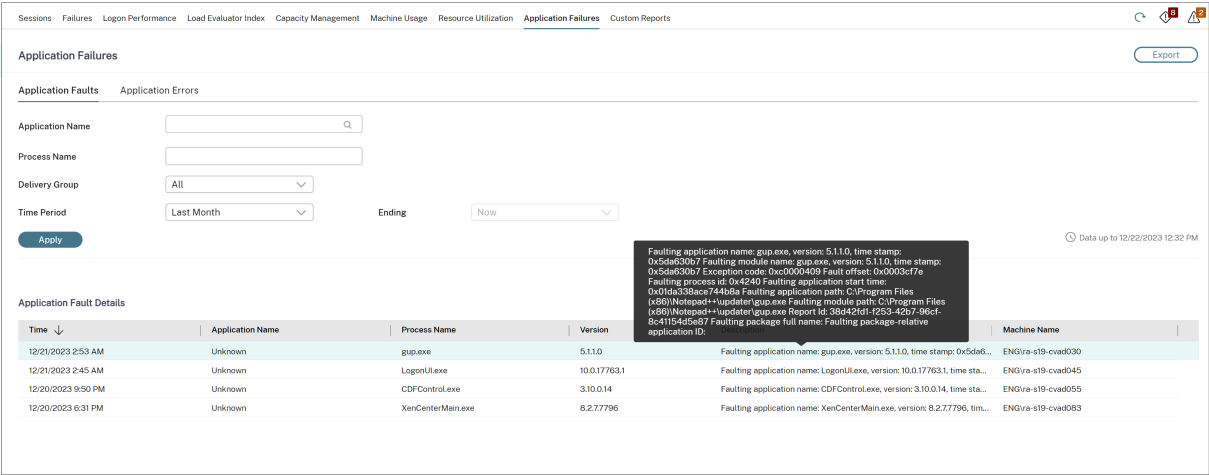
会话或应用程序实例处于以下状态时空闲时间将显示为不适用

- 空闲时间未超过 10 分钟，
- 在单会话操作系统的 VDA 上启动，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。

有关应用程序故障趋势可用性的详细信息，请参阅[数据粒度和保留](#)一文。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



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”将显示为“未知”。已启动的应用程序在桌面会话中出现故障时，或者该应用程序由于依赖的可执行文件导致的未处理的异常而出现故障时，通常会出现此问题。

默认情况下，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 天内在站点中执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

January 18, 2023

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。应用程序探测的结果可在 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）的监视选项卡中查看。Citrix Probe Agent 支持 Citrix Cloud Japan 和 Citrix Cloud Government 控制平面上托管的站点

确保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。

要求：

- 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。
- Citrix Probe Agent 支持 Citrix WorkSpace 支持的基于表单的默认身份 Citrix Probe Agent 不支持其他身份验证方法, 例如单点登录 (SSO) 或多重身份验证 (MFA)。同样, Citrix Probe Agent 仅在未部署 Citrix Gateway 或 Citrix ADC 等代理服务器或负载均衡器时才能运行。
- 确保在要安装探测代理的端点计算机上安装 Microsoft .NET Framework 4.7.2 或更高版本。
- 要在 Citrix Cloud Japan 控制平面中使用探测代理, 请将路径“\HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\”中的注册表值设置为 2。要在 Citrix Cloud Government 控制平面中使用探测代理, 请将路径 \HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region 中的注册表值设置为 3。

运行应用程序探测所需的用户帐户/权限如下所示:

- 要在每个端点计算机上进行探测的唯一 Workspace 用户。Workspace 用户不需要是管理员; 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
- 具有以下权限的完全权限管理员用户帐户。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\删除探测配置
    - \* 查看“配置”页面
    - \* 查看“趋势”页面

## 配置应用程序探测

将应用程序探测配置为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。

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 Citrix Workspace 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（如在监视器中所配置），并将报告结果返回到监视器。

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/component-s/app-probe-agent.html>
3. 启动代理并配置 Citrix Workspace 凭据。在每个端点计算机上配置唯一的 Workspace 用户。凭据将加密并安全地存储。

备注：

- 要访问从外部网络探测的站点，请在 **Workspace 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 Workspace URL。
- 在用户名字段中使用 NetBIOS 作为域名。例如，NetBIOS/username。
- 应用程序探测功能支持使用 Workspace 身份验证（仅限 AD）的 Citrix Content Collaboration 服务。

Citrix Probe Agent

1. Configure Workspace Credentials

2. Configure to Display Probe Result

3. View Summary

Workspace (StoreFront) Site Aggregation Enabled: ☒

Workspace URL (StoreFront URL in case of on-premises Site)

User name ⓘ

Password

Provide unique Workspace user credentials on each probe machine

Next

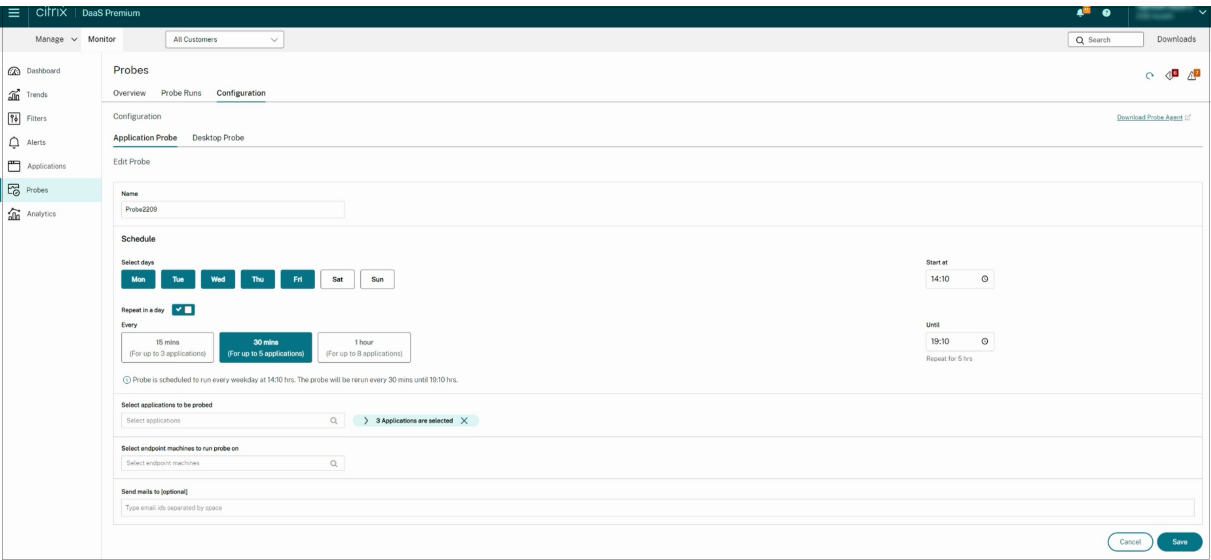
4. 在配置为显示探测结果选项卡上，输入凭据以访问 Citrix DaaS。您可以在 Citrix Cloud 控制台的“API 访问”页面中找到客户名称或客户 ID、客户端 ID 和密钥。

The screenshot shows the 'Citrix Probe Agent' configuration window. On the left is a sidebar with three steps: '1. Configure Workspace Credentials', '2. Configure to Display Probe Result' (which is highlighted with a blue bar), and '3. View Summary'. The main area of the window is titled 'VIEW THE PROBE RESULT ON CITRIX CLOUD:' with a toggle switch set to 'Yes'. Below this, there are three input fields: 'Client ID', 'Secret Key', and 'Customer ID'. The 'Secret Key' field is masked with dots. To the right of the 'Customer ID' field is a 'Validate' button. At the bottom right of the window is a 'Next' button.

**步骤 2：**在“监视”选项卡中配置应用程序探测

1. 在 Citrix DaaS 中，转到配置 > 探测配置 > 应用程序探测，然后单击创建探测：
2. 在创建探测页面中，输入探测的名称。
3. 选择时间表：
  - a) 选择您希望探测在一周中的哪几天运行。
  - b) 输入您希望探测运行的开始时间。
  - c) 此外，您可以选择一天内重复选项。输入结束时间以及您希望探测在一天内重复的时间间隔。例如，以下配置有助于在 12:08 到 16:34 之间运行应用程序探测，每个星期一、星期三、星期四和星期日每隔 30 分钟重复一次。
4. 请根据时间间隔选择建议的要探测的应用程序数量。
5. 选择必须在其上运行探测的端点计算机。
6. 输入将失败探测结果发送到的电子邮件地址，然后单击保存。

在此配置中，应用程序会话在 12:08、12:38、13:08 启动，依此类推，直到每个星期一、星期三、星期四和星期日的 16:08。



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。
- 在“监控”选项卡中进行配置后，代理将从下一个小时开始运行已配置的探测器。
- 在引入一天内重复选项之前设置的探测将继续按预定时间运行。默认情况下，他们禁用一天内重复选项。

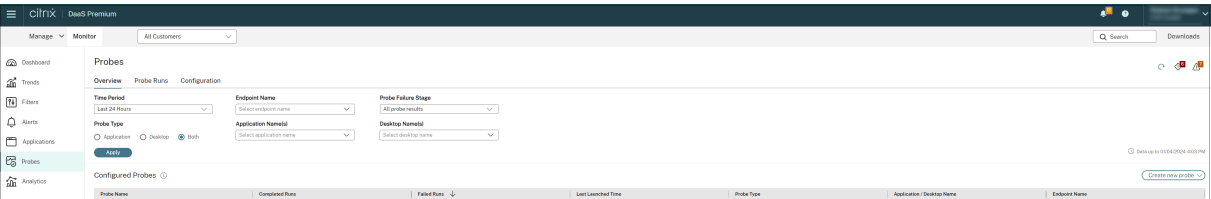
步骤 3：执行探测

代理根据其每小时从监视器中提取的探测配置运行应用程序探测。代理使用 **Workspace** 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监视器。失败情况在以下五个特定阶段报告：

- **Workspace** 可访问性 - 配置的 **Workspace** URL 无法访问。
- **Workspace** 身份验证 - 配置的 **Workspace** 凭据无效。
- **Workspace** 枚举 - **Workspace** 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 Citrix DaaS > 应用程序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 > 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

February 9, 2023

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监视器中获取。Citrix Probe Agent 现在支持 Citrix Cloud Japan 和 Citrix Cloud Government 控制平面上托管的站点。

在监视器的“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 Workspace 的选定桌面的启动，并向就爱您时期报告返回的结果。探测结果将在监视器 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 - Workspace 可访问性、Workspace 身份验证、Workspace 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。

此功能需要 Probe Agent 1903 或更高版本。

要求：

- 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。
- Citrix Probe Agent 支持 StoreFront 和 Citrix WorkSpace 支持的默认基于表单的身份验证。Citrix Probe Agent 不支持其他身份验证方法，例如单点登录 (SSO) 或多重身份验证 (MFA)。同样，Citrix Probe Agent 仅在未部署 Citrix Gateway 或 Citrix ADC 等代理服务器或负载均衡器时才能运行。
- 确保在要安装探测代理的端点计算机上安装 Microsoft .NET Framework 4.7.2 或更高版本。
- 要在 Citrix Cloud Japan 控制平面中使用探测代理，请将路径“\HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\”中的注册表值设置为 2。要在 Citrix Cloud Government 控制平面中使用探测代理，请将路径 \HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region 中的注册表值设置为 3。

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 Workspace 用户。Workspace 用户不需要是管理员；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使用户从活动会话中注销。



- 交付组权限：
  - \* 只读
- 监视权限：
  - \* 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。

## 步骤 1：安装和配置 Citrix Probe Agent

Citrix Probe Agent 是用于模拟用户通过 Workspace 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（如在监视器中所配置），并将报告结果返回到监视器。

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/component-s/app-probe-agent.html>
3. 启动代理并配置您的 Workspace Receiver for Web 凭据。在每个端点计算机上配置唯一的 Workspace 用户。凭据将加密并安全地存储。

### 备注：

- 要访问从网络外部探测的站点，请在“Workspace 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 Workspace URL。此功能适用于 Citrix Gateway 版本 12.1 或更高版本。

- 在用户名字段中使用 NetBIOS 作为域名。例如，NetBIOS/username。
- 桌面探测功能支持使用 Workspace 身份验证（仅限 AD）的 Citrix Content Collaboration 服务。
- 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，输入您的监视器凭据。您可以在 Citrix Cloud 控制台的“API 访问”页面中找到客户名称或客户 ID、客户端 ID 和密钥。

**步骤 2：在监视器中配置桌面探测**

1. 在 Citrix DaaS 中，转到配置 > 探测配置 > 应用程序探测，然后单击创建探测。
2. 在创建探测页面中，输入探测的名称。
3. 选择时间表：
  - a) 选择您希望探测在一周中的哪几天运行。
  - b) 输入您希望探测运行的开始时间。
  - c) 此外，您可以选择一天内重复选项。输入结束时间以及您希望探测在一天内重复的时间间隔。例如，以下配置有助于在 12:10 到 23:35 之间运行桌面探测，每个星期二、星期四和星期五每小时重复一次。
4. 请根据时间间隔选择建议的要探测的桌面数量。
5. 选择必须在其上运行探测的端点计算机。
6. 输入将失败探测结果发送到的电子邮件地址，然后单击保存。

在此配置中，桌面会话在 12:10、13:10、14:10 启动，依此类推，直到每个星期二、星期四和星期五的 23:10。

The screenshot shows the 'Create Probe' form in the Citrix DaaS Configuration console. The form is for a 'Desktop Probe'. It includes the following sections:

- Name:** A text input field.
- Schedule:**
  - Select days:** Radio buttons for Mon, Tue, Wed, Thu, Fri, Sat, Sun. 'Tue', 'Thu', and 'Fri' are selected.
  - Repeat in a day:** A checkbox labeled 'Every' is checked. Below it are three options: '15 mins (For up to 3 desktops)', '30 mins (For up to 5 desktops)', and '1 hour (For up to 8 desktops)'. '1 hour' is selected.
  - Start at:** A time picker set to 12:10.
  - Until:** A time picker set to 23:35.
- Select Desktops to be Probed:** A search input field.
- Select Endpoint Machines to Run Probe On:** A search input field.
- Send Alerts To (optional):** A text input field for email addresses.

Below the form, a summary line states: 'Probe is scheduled to run every Tue, Thu, Fri at 12:10 hrs. The probe will be rerun every 1 hour until 23:35 hrs.'

At the bottom right of the form, there are 'Cancel' and 'Save' buttons.

**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。
- 桌面探测配置完成后，代理将从下一个小时开始运行配置的探测。
- 在引入一天内重复选项之前设置的探测将继续按预定时间运行。默认情况下，他们禁用一天内重复选项。

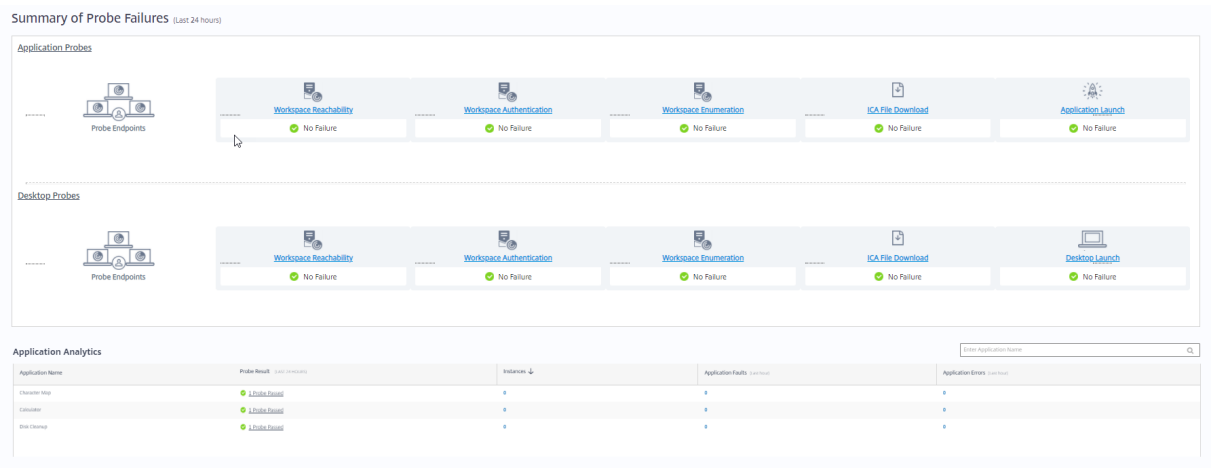
步骤 3：执行探测

代理根据其定期从监视器中提取的探测配置运行桌面探测。代理使用 Workspace 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监视器。失败情况在以下五个特定阶段报告：

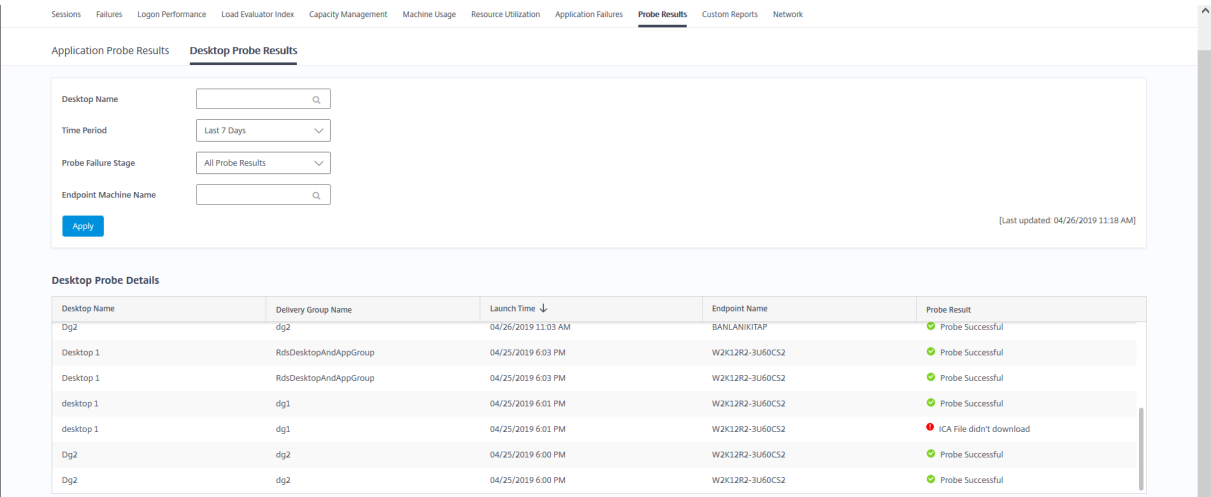
- **Workspace** 可访问性 - 配置的 Workspace URL 无法访问。
- **Workspace** 身份验证 - 配置的 Workspace 凭据无效。
- **Workspace** 枚举 - Workspace 枚举桌面列表不包含要探测的桌面。
- **ICA** 下载 - ICA 文件不可用。
- 桌面启动 - 桌面无法启动。

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。



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

February 20, 2024

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。此工具自动执行若干项运行状况检查，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。

“Monitor” 选项卡中的过滤器 > 计算机视图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 Failure Reasons Troubleshooting Guide](#)（《Citrix Director 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。

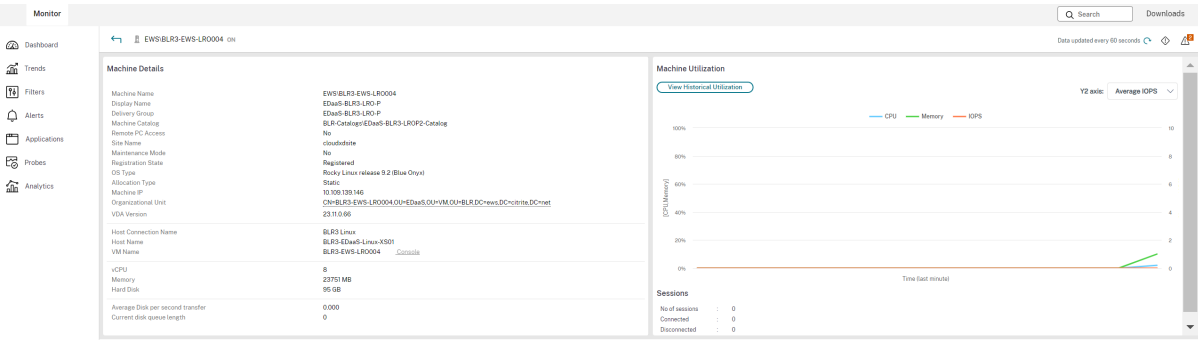
单击计算机名称链接可转到计算机详细信息页面。

“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，磁盘和 GPU 监视图表可用于 VDA 版本 7.14 及更高版本的站点。

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）。



## GPU 利用率

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，从而对多会话和单会话操作系统 VDA 上的 GPU 相关问题进行故障排除。

支持的 **GPU** 版本：

- 运行显示驱动程序版本 369.17 或更高版本的 NVIDIA Tesla M60 GPU。有关详细信息，请参阅 [NVIDIA vGPU 软件](#)。
- AMD Radeon Instinct MI25 GPU 和 AMD EPYC 7V12(Rome) CPU。有关详细信息，请参阅 [AMD 驱动程序和支持](#)。

驱动程序：

必须在 VDA 上安装相应的驱动程序或扩展程序。

- 对于 NVIDIA GPU，请手动或通过扩展程序安装 GRID 驱动程序。有关详细信息，请参阅 [NVIDIA vGPU 软件](#)。
  - 请注意，对于 NVIDIA，仅支持 GRID 驱动程序。CUDA 驱动程序不适用于 NVadsA10 v5 系列，也不受支持。
  - 有关在基于 Azure 的计算机上通过扩展程序安装 Nvidia Grid GPU 驱动程序的示例过程，请参阅 [NVIDIA GRID 驱动程序。NVIDIA GPU 驱动程序扩展 - Azure Windows VM - Azure 虚拟机](#)。
  - 有关手动安装 Nvidia Grid GPU 驱动程序的示例流程，请参阅 [Azure N-series NVIDIA GPU driver setup for Windows - Azure Virtual Machines](#) (适用于 Windows 的 Azure N 系列的 NVIDIA GPU 驱动程序安装 - Azure 虚拟机)。
- 对于 AMD GPU，请手动或通过扩展程序安装 AMD 显卡驱动程序。有关详细信息，请参阅 [AMD 驱动程序和支持](#)。
  - 有关在基于 Azure 的计算机上通过扩展程序安装 AMD GPU 驱动程序的示例流程，请参阅 [AMD GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines](#) (AMD GPU 驱动程序扩展 - Azure Windows VM - Azure 虚拟机)。
  - 有关在 Azure 计算机上手动安装 AMD GPU 驱动程序的示例过程，请参阅 [Install AMD GPU drivers on N-series VMs running Windows](#) (在运行 Windows 的 N 系列 VM 上安装 AMD GPU 驱动程序)。

用法说明：

- “GPU 利用率” 图表仅适用于运行 64 位 Windows 的 VDA。
- AMD GPU 利用率图表仅适用于运行 Citrix Virtual Apps and Desktops 7 2212 或更高版本的 VDA。
- 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。
- 对于 AMD，不单独支持使用编码器和解码器。使用 GPU 的任何编码/解码工作负载都将报告为 GPU 使用情况中的一般 3D 负载。

- 确保在安装期间安装 NVIDIA WMI。此窗口仅在手动安装期间可用。
- 如果已安装驱动程序但 Director 未检测到 GPU
  - 检查任务管理器。如果驱动程序安装正确，GPU 应显示在任务管理器中。
  - 检查计算机是否已注册。有时，计算机可能需要一些时间才能被检测为联机。
- 如果 GPU 使用率在 Director 中未显示任何活动，请确保您正在运行的工作负载正在使用 GPU。对于图形工作负载，可以从“设置”>“系统”>“显示”>“Graphics Settings”（显卡设置）>“Choose the app to set preference”（选择要设置首选项的应用程序）启用此功能。请务必打开“High Performance”（高性能）。有时，当根据其他设置将其设置为系统默认值或省电时，Windows 会默认使用 CPU 处理图形工作负载。
- 数据每分钟更新一次，数据可视化将在选择 **GPU** 利用率后的一分钟内开始工作。

基于计算机的历史资源利用率

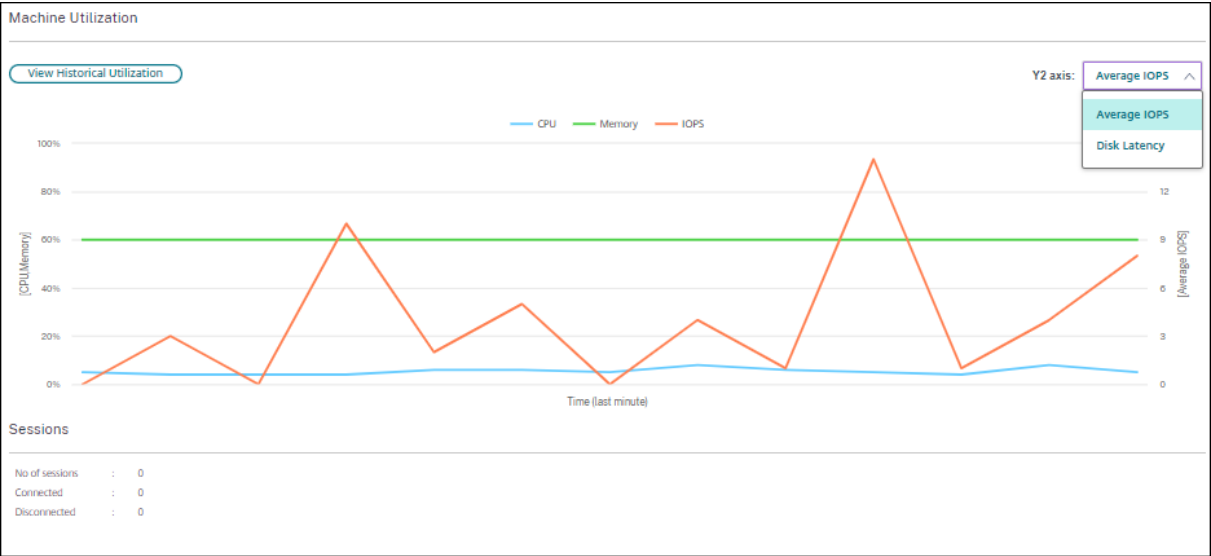
在计算机利用率面板中，单击查看历史利用率可查看选定计算机上资源的历史使用情况。

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。

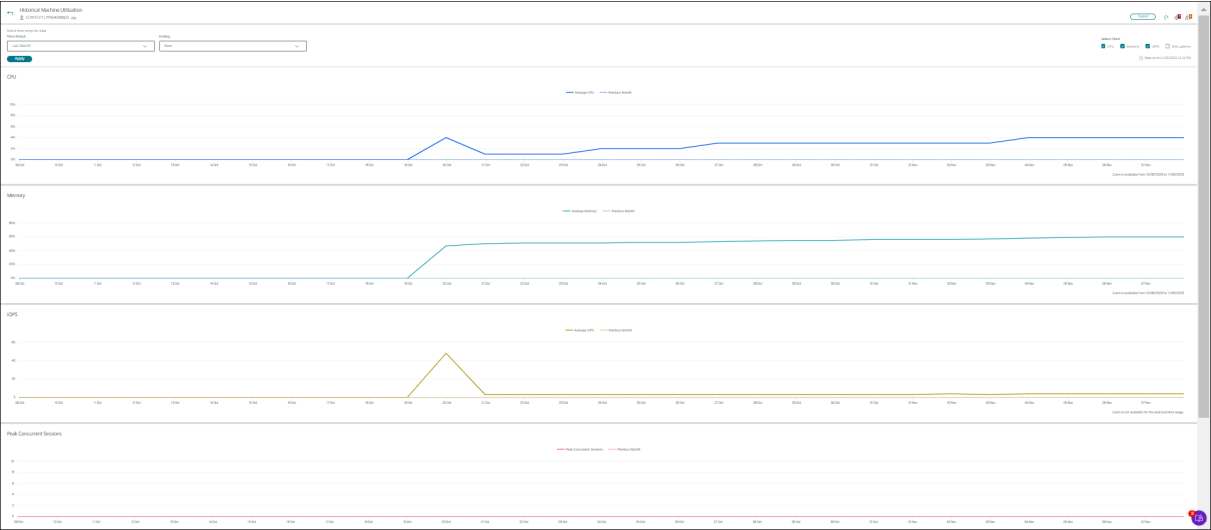


1. 在计算机详细信息视图的计算机利用率面板中，选择查看历史利用率。
2. 在历史计算机利用率页面中，设置时间段以查看过去 2 小时、24 小时、7 天、上个月或上一年的使用情况。

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。



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。
- 如果属于 Citrix Cloud Japan 或 Citrix Cloud Government 平面的站点包含超过 5000 台计算机，则流程数据仅适用于最多 2000 台计算机。必须在这些计算机上启用“过程监视”策略。

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 Monitor 访问在 XenServer 7.3 版及更高版本上托管的桌面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，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 Monitor 访问。

Machine Details

Power Control

Manage Users

|                            |                                 |
|----------------------------|---------------------------------|
| Machine Name               | VWAP2\AWTSVDA-0001              |
| Maintenance Mode           | Off                             |
| Display Name               | FTL TSVDA                       |
| Delivery Group             | FTL TSVDA                       |
| Machine Catalog            | TSVDA1                          |
| Remote PC Access           | No                              |
| Site Name                  | cloudxdsite                     |
| Windows Connection Setting | LogonEnabled                    |
| Registration State         | Unregistered (Health Assistant) |
| OS Type                    | Windows 2016                    |
| Allocation Type            | Random                          |
| Machine IP                 | n/a                             |
| Organizational Unit        | n/a                             |
| VDA Version                | 2009.0.0.27084                  |

|                      |             |
|----------------------|-------------|
| Host Connection Name | n/a         |
| Host Name            | n/a         |
| VM Name              | n/a Console |

|           |     |
|-----------|-----|
| vCPU      | n/a |
| Memory    | n/a |
| Hard Disk | n/a |

|                                  |                           |
|----------------------------------|---------------------------|
| Average Disk per second transfer | n/a                       |
| Current disk queue length        | n/a                       |
| Microsoft RDS License            | n/a                       |
| Load Evaluator Index             | <div><div></div></div> 1% |

|              |     |
|--------------|-----|
| VDA Hotfixes | n/a |
|--------------|-----|

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。
- 控制台访问在新选项卡中启动，请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。



Machine Details

Power Control

Manage Users

|                            |                                             |  |  |
|----------------------------|---------------------------------------------|--|--|
| Machine Name               | WANMQ\AWTSVDA-0001                          |  |  |
| Maintenance Mode           | <div>Off</div>                              |  |  |
| Display Name               | psc server dg                               |  |  |
| Delivery Group             | psc server dg                               |  |  |
| Machine Catalog            | psc server vda                              |  |  |
| Remote PC Access           | No                                          |  |  |
| Site Name                  | cloudxdsite                                 |  |  |
| Windows Connection Setting | LogonEnabled                                |  |  |
| Registration State         | Registered                                  |  |  |
| OS Type                    | Windows 2016                                |  |  |
| Allocation Type            | Random                                      |  |  |
| Machine IP                 | 10.108.92.187                               |  |  |
| Organizational Unit        | CN=AWTSVDA-0001,CN=Computers,DC=xd,DC=local |  |  |
| VDA Version                | 2206.0.0.34067                              |  |  |

|                      |                             |  |  |
|----------------------|-----------------------------|--|--|
| Host Connection Name | n/a                         |  |  |
| Host Name            | n/a                         |  |  |
| VM Name              | n/a <a href="#">Console</a> |  |  |

|           |         |  |  |
|-----------|---------|--|--|
| vCPU      | 2       |  |  |
| Memory    | 4088 MB |  |  |
| Hard Disk | 200 GB  |  |  |

Average Disk per second transfer

Current disk queue length

Microsoft RDS License

Load Evaluator Index

An RDS licensing type is not configured.

Not configured properly

0.80%

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。

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 | Monitor 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）。

PVS 目标设备指标

可以在 Monitor 中的计算机详细信息页面上查看单会话和多会话操作系统计算机的 PVS 目标设备的状态。此面板上提供了网络、启动和缓存的几个衡量指标。这些指标可帮助您监视 PVS 目标设备并对其进行故障排除，以确保其已启动并且正在运行。

| PVS Target Device Metrics     |    |                         |               |                                 |                                          |
|-------------------------------|----|-------------------------|---------------|---------------------------------|------------------------------------------|
| Network                       |    | Boot                    |               | Cache                           |                                          |
| NIC Bandwidth Utilization (%) | 12 | Boot Bytes Read MB      | 231           | Write Cache Type                | Device RAM with overflow on local har... |
| Server Reconnect Count        | 5  | Boot Bytes Written MB   | 0             | Write Cache Volume Drive Letter | D:                                       |
| Total UDP Retry Count         | 7  | Boot From               | vDisk         | Write Cache Volume Size MB      | 6142                                     |
|                               |    | Boot Retry Count        | 0             | Cache File Size MB              | 1058                                     |
|                               |    | Boot Time (sec)         | 31            | Ram Cache Usage MB              | 62.3125                                  |
|                               |    | Target Software Version | 7.23.0        |                                 |                                          |
|                               |    | VDisk Name              | v10VDisk.vhdx |                                 |                                          |

在网络中：

- 网络带宽利用率：所有 NIC 的平均带宽利用率。

- 服务器重新连接计数：服务器由于网络问题或服务器重新平衡或关闭和重新启动 Citrix Provisioning Stream Service 而重新连接的次数。
- UDP 总重试计数：Provisioning 目标设备尝试使用 UDP 重新连接到 Provisioning 服务器的次数。此衡量指标可帮助您了解 Citrix Provisioning Stream Service 中是否存在任何网络问题（例如，错误的交换机配置）。

引导：

- 读取的引导字节 (MB)：引导时读取的字节。
- 写入的引导字节 (MB)：引导时写入的字节。
- 引导位置：引导介质（虚拟磁盘、本地磁盘等）。
- 引导重试计数：引导计算机的重试次数。
- 引导时间：引导计算机所花费的时间（以秒为单位）。默认情况下，两次重试之间有 5 秒的延迟。如果此延迟增长为双位数，则引导时间显著增加。请检查您的预配配置以解决此问题。
- 目标软件版本：Provisioning 目标设备软件的版本。
- 虚拟磁盘名称：从中引导 Provisioning 目标设备的虚拟磁盘。

缓存：

- 写入缓存类型：可以将虚拟磁盘设置为不同类型的缓存。有关详细信息，请参阅知识中心文章 [CTX119469](#)。
- 写入缓存卷驱动器盘符：用于涉及驱动器的写入缓存类型的驱动器盘符。
- 写入缓存卷大小 (MB)：为写入缓存配置的总卷大小。
- 缓存文件大小 (MB)：当前缓存文件大小（在设备 RAM 中缓存并溢出到硬盘）。
- RAM 缓存使用量 (MB)：当前 RAM 缓存大小（在设备 RAM 中缓存并溢出到硬盘）。请仅在必要时使用“溢出到磁盘”。此衡量指标在设置或优化 RAM 缓存的适当大小时非常有用。

有关详细信息，请参阅[在目标设备上使用状态托盘](#)。

Provisioning 目标设备衡量指标仅在以下情况下可用：

- 预配计算机。
- Provisioning 目标设备版本 7.19 及更高版本。
- VDA 版本 2003 及更高版本。

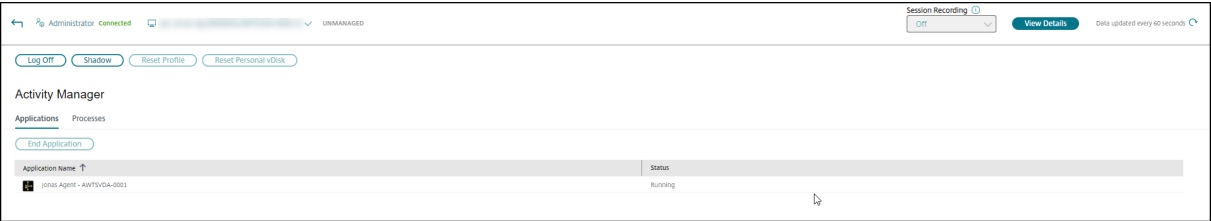
注意：

“服务器重新连接计数”和“UDP 重试计数”的衡量指标仅适用于 Provisioning 目标版本 1912 CU2 及更高版本。

对用户问题进行故障排除

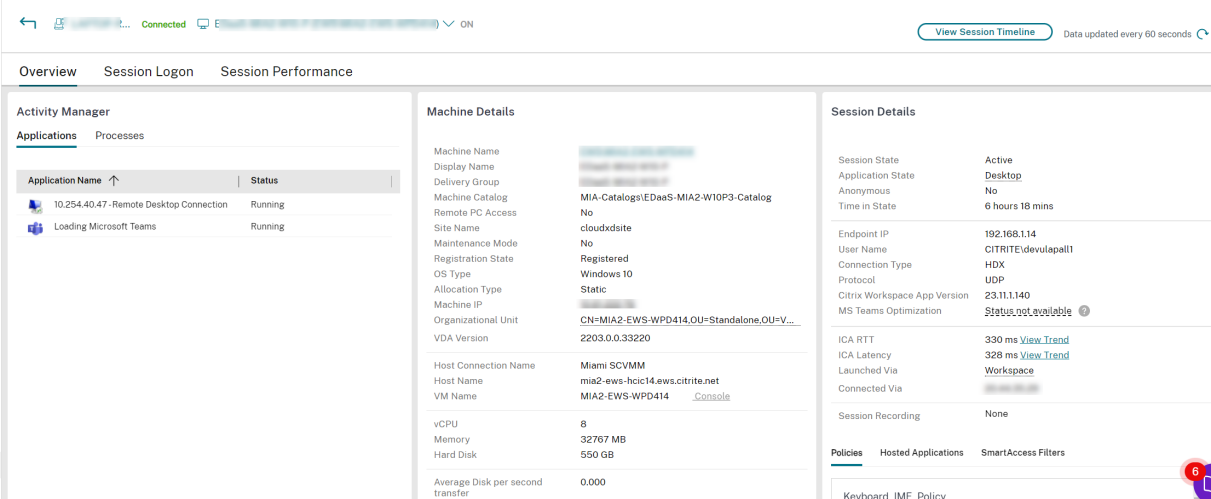
March 5, 2024

使用 Monitor 的技术支持视图（活动管理器 页面）查看有关用户或终端的信息。

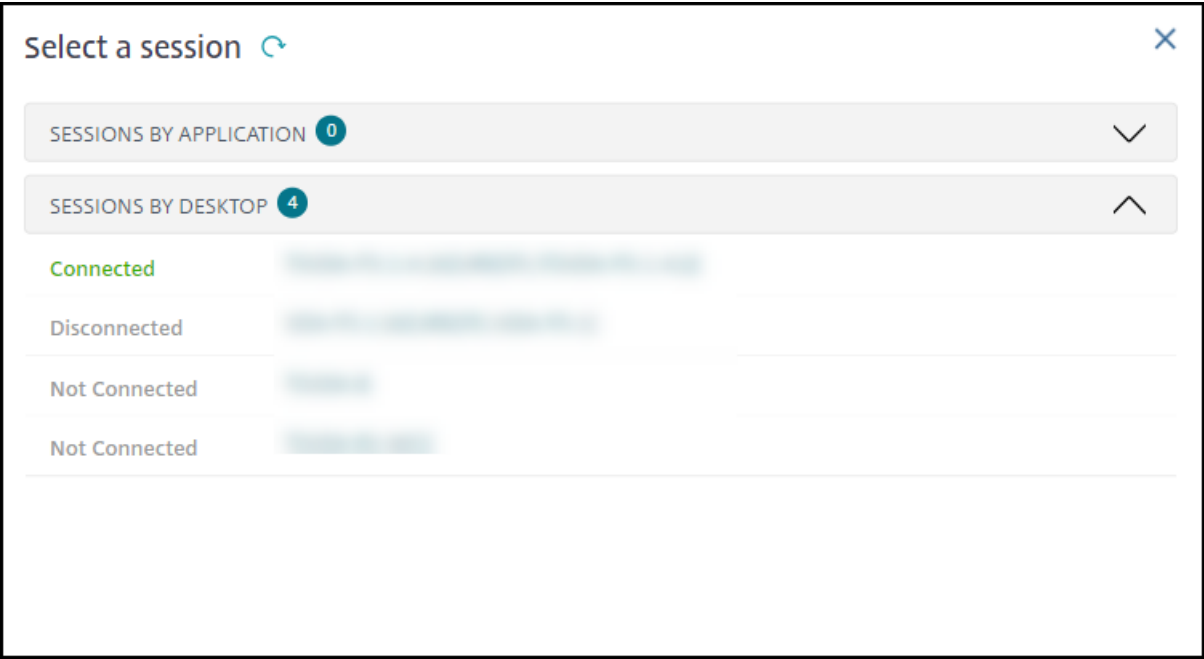


在“用户活动管理器”中单击“查看详细信息”将打开“用户详细信息”页面。

在端点的活动管理器中单击“查看详细信息”可打开“端点详细信息”页面。



如果用户启动了多个会话，则会显示会话选择器。



选择一个会话以查看详细信息。

- 查看有关会话、用户登录体验、会话启动、连接和应用程序的详细信息。
- 您可以对用户的计算机执行重影操作。
- 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。

**Microsoft Teams 优化状态**

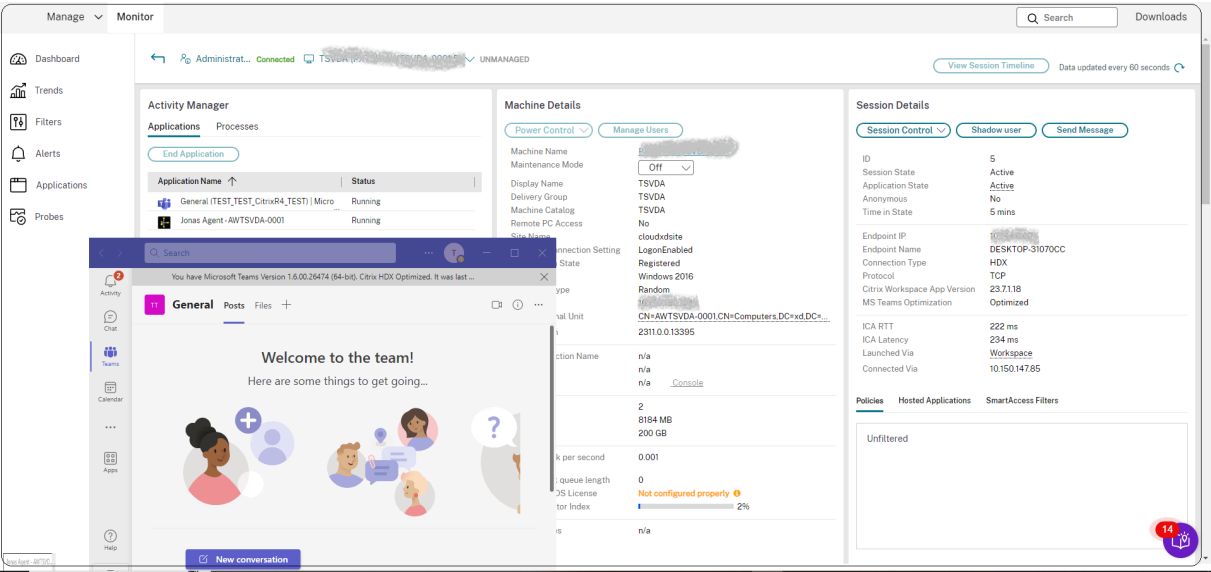
Citrix Monitor 在“用户详细信息”页面 > “会话详细信息”面板 > “**MS Teams 优化**”字段中显示 HDX 会话的 Microsoft Teams 优化状态。Microsoft Teams 的优化对于更好的用户体验（例如清晰的音频和视频）至关重要。Microsoft Teams 优化状态的可见性有助于缩短解决问题所需的时间，并帮助管理员在故障排除期间确定重要指标。

注意：

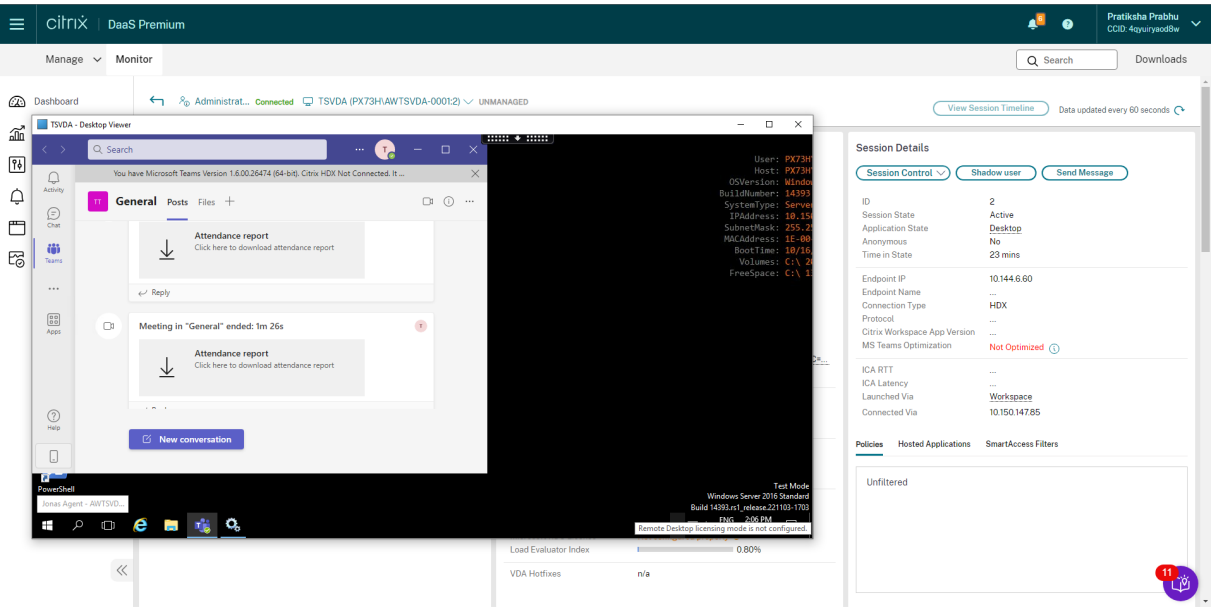
只有当您使用的是 2.0 版之前的 Microsoft Teams 时，Citrix Monitor 才支持。

必备条件：

- [Microsoft Teams 优化](#)中列出了支持的 Citrix Workspace 应用程序版本。
- Microsoft Teams 作为已发布的应用程序运行，也可以在已发布的桌面内运行。
- Citrix HDX HTML5 视频重定向服务等关键服务正在运行。



如果 Microsoft Teams 未进行优化，则工具提示会提供指向 HDX 的外部故障排除实时文章的链接，该文章包含优化 Microsoft Teams 的技巧。[HDX 优化故障排除](#)。



## 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](#)

| 用户问题          | 建议                            |
|---------------|-------------------------------|
| 确定建立会话所涉及的组件  | <a href="#">分析会话拓扑视图</a>      |
| 会话响应缓慢或没有响应   | <a href="#">诊断会话性能问题</a>      |
| 应用程序运行缓慢或没有响应 | <a href="#">解决应用程序故障</a>      |
| 连接失败          | <a href="#">还原桌面连接</a>        |
| 会话执行缓慢或不响应    | <a href="#">还原会话</a>          |
| 视频加载缓慢或画质差    | <a href="#">运行 HDX 通道系统报告</a> |

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。

会话性能

会话性能选项卡增强了故障排除工作流程，首先增强关联实时指标以识别用户会话中的问题的能力。会话拓扑面板可直观地显示已连接的 HDX 会话的会话中路径。性能指标面板提供 ICARTT、ICA 延迟、每秒帧数、可用的输出带宽和占用的输出带宽等会话指标的趋势有助于指明这些指标在一段时间内的表现。有关详细信息，请参阅[诊断会话性能问题](#)。

搜索提示

在配置的所有 Active Directory 中搜索用户名。

当您在搜索字段中键入多用户计算机名称时，将显示指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，将列出连接到特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。此列表允许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。

搜索结果还包括当前未使用或未分配到计算机的用户。

- 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。
- 键入由两部分组成的名称的几个字母并用空格分隔后，结果将包括两个字符串的匹配项。由两部分组成的名称的示例包括用户名、姓氏和名字或显示名称。例如，如果您键入“jo rob”，则结果可能包含诸如“约翰·罗伯逊”或“罗伯特·琼斯”之类的字符串。

要返回登录页面，请单击“监视”选项卡。

## 诊断会话启动问题

February 20, 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，Monitor 还显示会话启动持续时间。此持续时间在用户详细信息和端点详细信息页面上分为 Workspace 应用程序会话启动持续时间和 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。

### 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：

- VDA 1903 或更高版本。
- Citrix End User Experience Monitoring (EUEM) 服务必须在 VDA 上运行。

### 限制

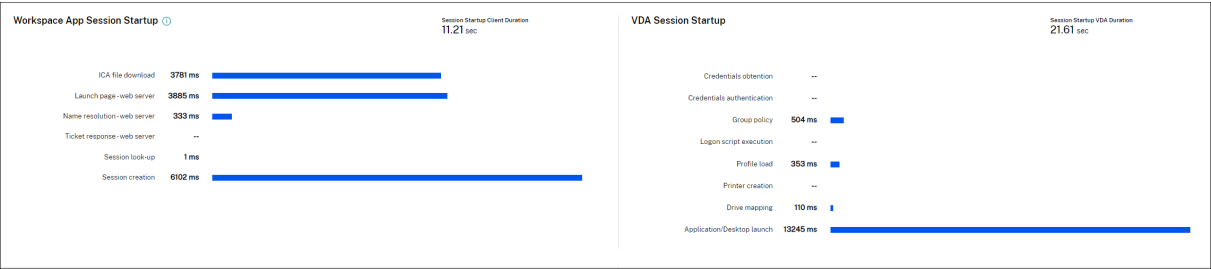
当 Monitor 显示会话启动持续时间数据时，将适用以下限制。

- 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，IFDCD 才可用。
- 对于从 macOS 启动会话，IFDCD 仅适用于 Workspace 应用程序 1902 及更高版本。
- 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，仅针对检测到 Workspace 应用程序的浏览器启动的应用程序显示 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 Monitor 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（单击鼠标），并在客户端设备与 VDA 之间建立 ICA 连接时结束。对于共享会话，此持续时间要小得多，因为不会产生与创建到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。

ICA 文件下载持续时间 (IFDCD)

IFDCD 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）或它们之间的网络连接问题。

### 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。

### 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，指示 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，因而不包含在 VDA 启动持续时间内，则可能会人为地夸大此持续时间。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（可以是 Kerberos、Active Directory 或安全支持提供程序接口 (SSPI)）对用户的凭据进行身份验证所花费的时间。

### 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。

可以使用户或组的登录脚本异步。优化任何应用程序兼容性脚本或改用环境变量。

### 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，请检查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。将终端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。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。

确保基本策略包含用于禁用未使用的虚拟通道（例如音频或 COM 端口映射）的设置，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**。**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。**userinit** 表示 **userinit.exe** 的启动到虚拟桌面或应用程序的用户界面的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 上的会话创建中的杂项延迟。

诊断用户登录问题

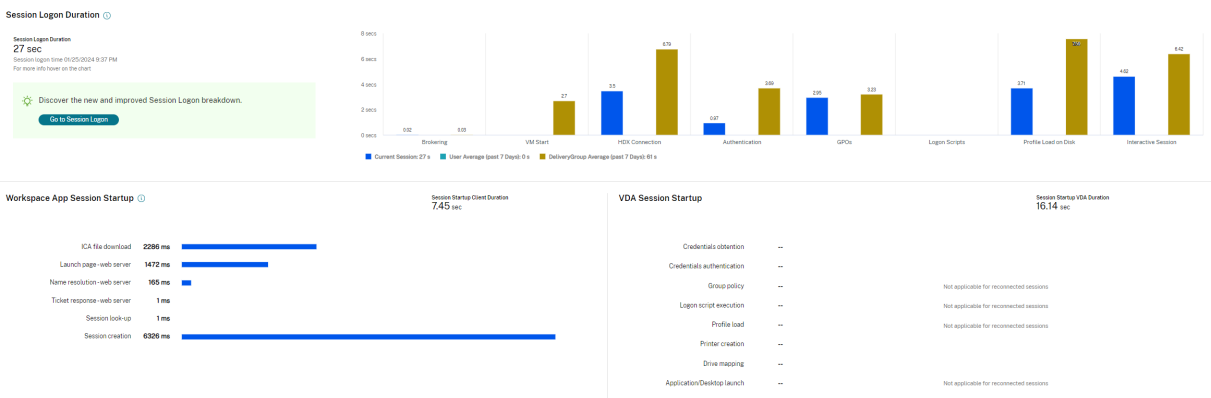
November 16, 2023

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，持续时间显示为一个数值，在其下方显示登录时间以及登录过程各阶段的图形。

在用户登录 Citrix Virtual Apps and Desktops 时，Monitor Service 将跟踪登录过程（从用户在 Citrix Workspace 应用程序中进行连接到桌面准备就绪）的各阶段。



左侧的大数字是总登录时间，其计算方式为：将建立连接和从 **Delivery Controller** 获得桌面所用的时间与执行身份验证和登录虚拟桌面所用的时间相结合。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。

注意：

仅在默认 Windows Shell (explorer.exe) 上而非自定义 Shell 上支持登录持续时间。

## 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。

## 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，则为启动虚拟机所用的时间。

### HDX 连接

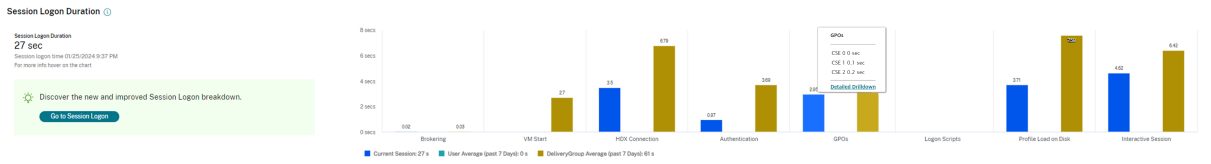
在设置从客户端到虚拟机的 HDX 连接期间需执行的步骤所用的时间。

### 身份验证

完成远程会话的身份验证所用的时间。

GPO

如果在虚拟机上启用了组策略设置，则为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[https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd277416\(v=technet.10\)](https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd277416(v=technet.10))。

登录脚本

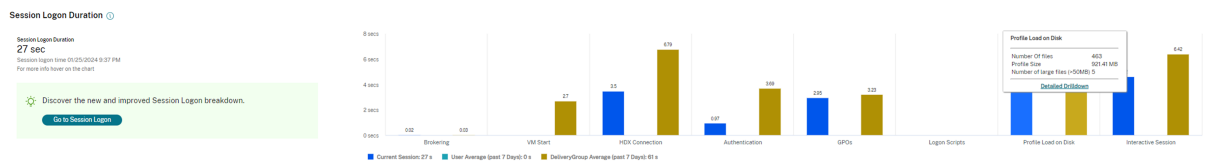
如果为会话配置了登录脚本，则指运行登录脚本所用的时间。

配置文件加载

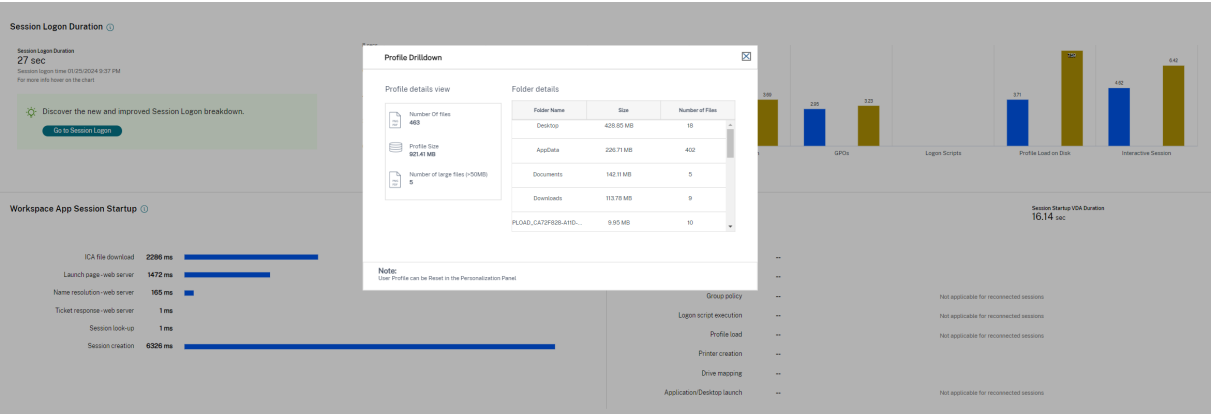
如果为用户或虚拟机配置了配置文件设置，则为加载配置文件所用的时间。

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 及更高版本中可用。

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。此额外的信息可帮助对配置文件加载时间较长的问题进行故障排除。



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）。



配置文件深入分析在 VDA 1811 及更高版本上可用。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，所有文件夹名称都可见。要隐藏文件夹名称，请使用以下步骤编辑 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 **ProfileFolder-sNameHidden**
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：

您可以使用 GPO 或 PowerShell 在多个计算机上应用对注册表值进行的更改。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。
- 配置文件深入分析中不包括的 AppData 文件夹中存在一些隐藏文件。
- 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

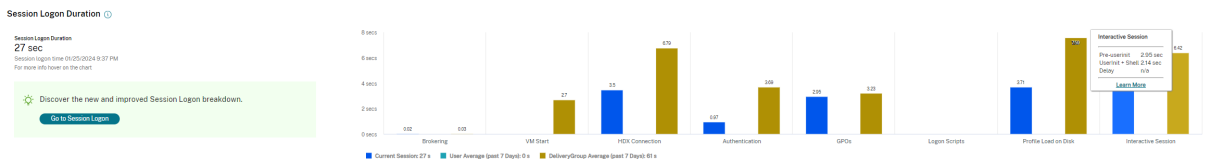
注意：

此功能在 VDA 1811 及更高版本中提供。如果您在 7.18 之前的站点上启动了会话，然后升级到 7.18，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[https://docs.microsoft.com/en-us/previous-versions/ms813609\(v=msdn.10\)](https://docs.microsoft.com/en-us/previous-versions/ms813609(v=msdn.10))。



“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**: 这是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。
- 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额外的处理，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：

“登录时长”图形将显示各登录阶段（以秒为单位）。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。

## 重影用户

November 11, 2022

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。

重影功能在新选项卡中启动，请更新您的浏览器设置以允许来自 Citrix Cloud 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：

- 监视器使用 FQDN 连接到目标 Linux VDA。确保监视器客户端可以解析 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。在每个监视器客户端和 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。

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。

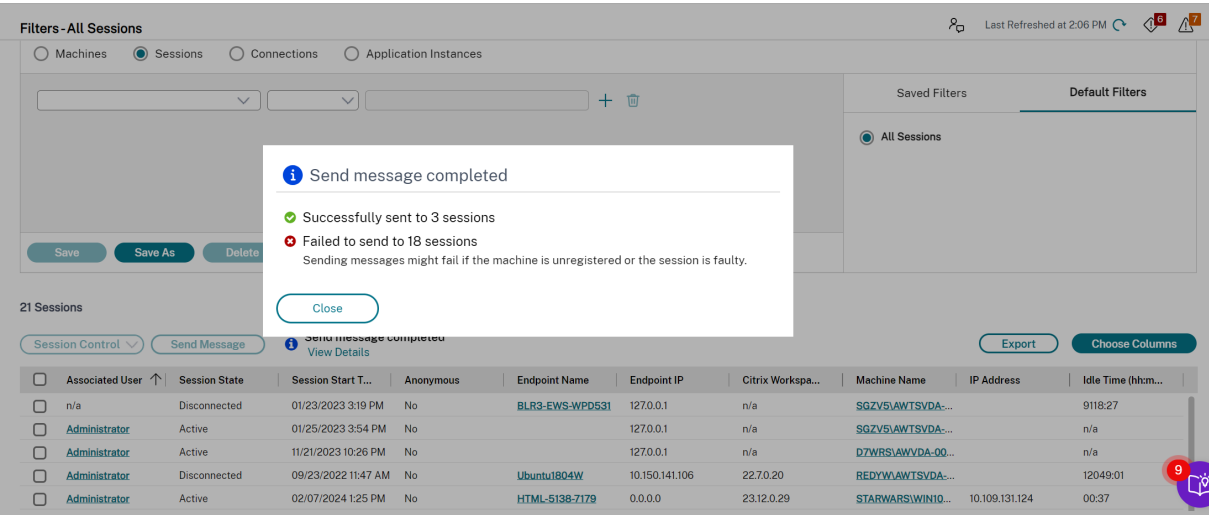
向用户发送消息

January 23, 2024

在监视器中，向连接到一台或多台计算机的用户发送消息。例如，使用此功能发送有关管理操作（如即将发生的桌面维护、计算机注销和重新启动以及配置文件重置）的即时通知。

要向用户发送消息，请按照以下步骤进行操作：

1. 转到 监视 > 过滤器 > 计算机 > 所有计算机。
2. 选择要向其发送消息的计算机，然后单击发送消息。
3. 键入您的消息，然后单击发送。



如果计算机未注册或会话出现故障，则发送消息可能会失败。

如果消息发送成功，将在监视器中显示确认消息。如果用户计算机已连接，则将在其中显示消息。

如果消息未发送成功，则将显示错误消息。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”。

如果您选择向所有连接的会话发送批量消息，则操作进度将以百分比显示。操作完成后，将显示成功发送的消息数量和失败的消息数量。管理大型网站时，发送消息状态特别有用。它有助于了解是否需要将消息重新发送给某些用户。

## 解决应用程序故障

February 9, 2023

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。

列表仅包含已经在会话中启动的应用程序。

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 | 选中不响应的应用程序并单击结束应用程序。终止应用程序后，请求用户重新启动应用程序。                                                                                         |
| 终止不响应的进程   | 如果您拥有所需的权限，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，单击详细信息并打开维护模式选项。上报给相应的管理员。                                                   |

禁用正在运行的应用程序的可见性

默认情况下，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。对活动管理器功能具有访问权限的所有管理员均可以查看此信息。对于委派管理员角色，完全权限管理员、交付组管理员和技术支持管理员均可以查看此信息。

为了保护用户及其正在运行的应用程序的隐私，您可以禁用“应用程序”选项卡以列出正在运行的应用程序。为此，请在 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。

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。

还原桌面连接

March 30, 2022

从监视器的用户标题栏检查当前计算机的用户连接状态。

如果桌面连接失败，将会显示导致连接失败的错误，以帮助您确定如何进行故障排除。

| 操作           | 说明                                                                       |
|--------------|--------------------------------------------------------------------------|
| 确保计算机未处于维护模式 | 请确保在用户详细信息页面上已关闭维护模式。                                                    |
| 重新启动用户的计算机   | 选择计算机，然后单击重新启动。如果用户计算机没有响应或无法连接，比如计算机占用异常高的 CPU 资源（这会导致 CPU 不可用），请使用此选项。 |

还原会话

March 30, 2022

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）。

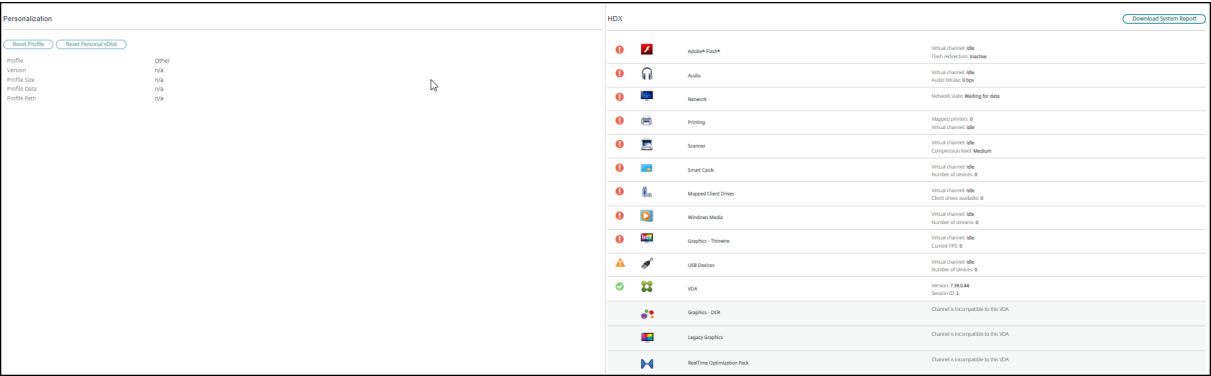
| 操作               | 说明                                                                                               |
|------------------|--------------------------------------------------------------------------------------------------|
| 终止不响应的应用程序或进程    | 单击应用程序选项卡。选中不响应的应用程序并单击结束应用程序。同样，选中对应的不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。                                                |
| 从会话中注销用户         | 单击会话控制并选择注销。                                                                                     |

要测试会话，用户可尝试再次登录会话。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 16, 2023

在 用户详细信息 视图中，在 HDX 面板中检查用户计算机上 HDX 频道的状态。只有在用户计算机使用 HDX 连接时，才可使用此面板。



如果出现了一条指示当前无法获取信息的信息，请等待一分钟以便页面进行刷新，或选择刷新按钮。HDX 数据更新时间比其他数据更新时间稍长。

单击错误或警告图标，以了解更多信息。

提示：

可以在同一对话框中，通过单击标题栏左角的向左和向右箭头，查看其他通道的相关信息。

HDX 通道系统报告主要供 Citrix 技术支持用来进行进一步的故障排除。为此，请在 HDX 面板中，单击下载系统报告。

## 重置用户配置文件

April 18, 2022

小心：

重置配置文件时，虽然用户的文件夹和文件都已保存并复制到新的配置文件，但大部分用户配置文件数据仍将被删除（例如，注册表被重置，应用程序设置可能被删除）。

1. 从监视器中，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。对于 Citrix 用户配置文件，该配置文件在用户桌面显示时已重置。对于 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

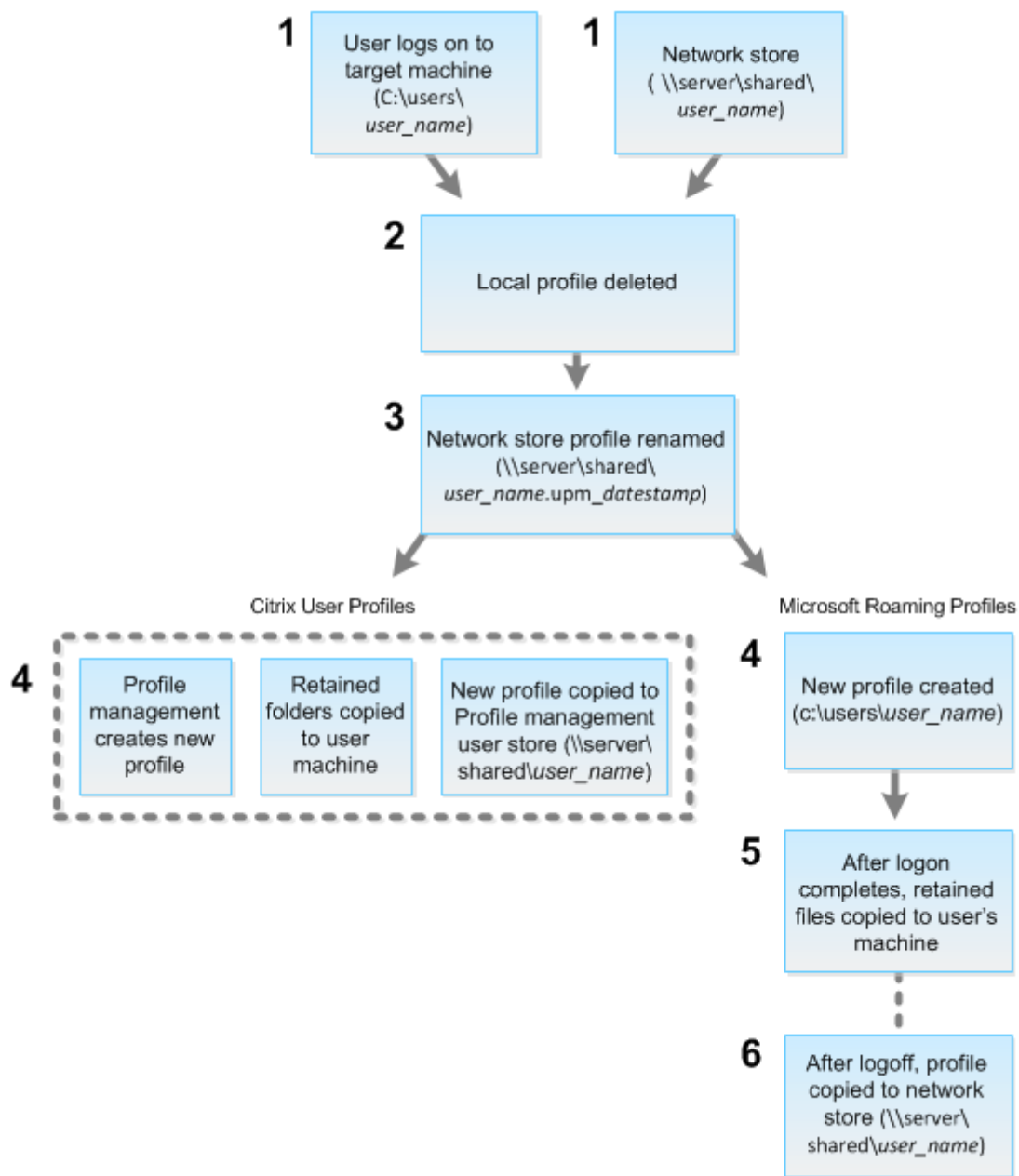
注意：

在 Windows 8 或更高版本中，重置配置文件时不会复制 Cookie。

### 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（在监视器中或使用 PowerShell SDK）后，监视器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。监视器通过 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。



监视器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 Profile Management 负责处理用户，但却接收到漫游配置文件命令，用户将被拒绝（反之亦然）。

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，将使用 Profile Management 导入规则创建新配置文件，然后将文件夹复制回网络配置文件，之后用户可以继续正常登录。如果将漫游配置文件用于重置，则漫游配置文件中的任何注册表设置将



保留在重置配置文件中。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。

### 录制会话

February 20, 2024

您可以使用 Monitor 中的用户详细信息和计算机详细信息屏幕中的 Session Recording 控件来录制 ICA 会话。**Premium** 站点上的客户可以使用此功能。

### 动态会话录制

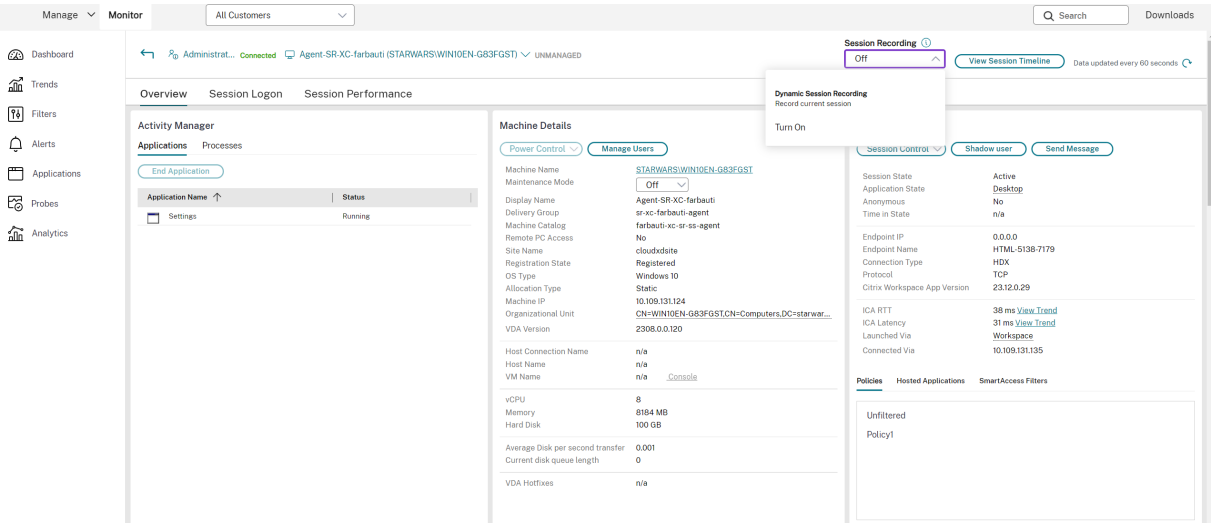
可以使用用户详细信息屏幕上的 Session Recording 控件来录制当前的活动会话。有关动态会话录制的详细信息，请参阅 [Session Recording 服务](#) 一文。

### Monitor 中的 Session Recording 控件

可以使用用户详细信息 > 会话录制操作来录制当前或后续的会话。

- 打开动态会话录制 - 录制当前会话。
- 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。



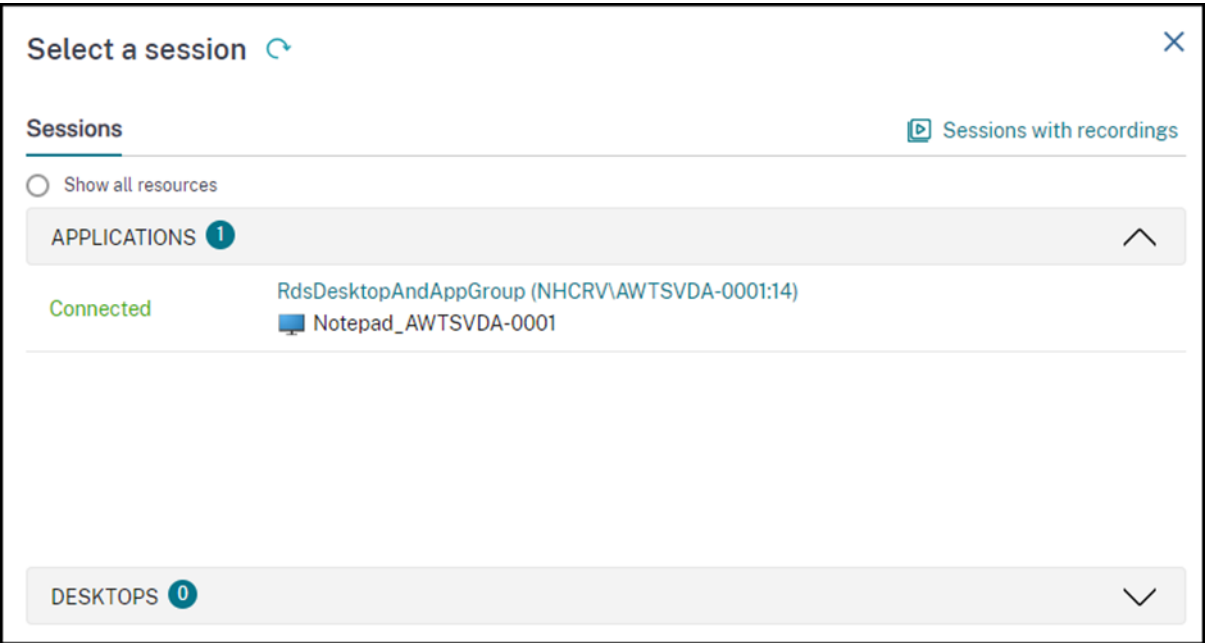
计算机详细信息面板显示该计算机的 Session Recording 策略状态。

播放实时会话和录制的会话

可以播放录制的用户会话和实时用户会话以了解用户遇到的问题。在 Monitor 控制台中随时访问录制文件和会话相关指标，无需在多个 Session Recording Server 上搜索录制文件或寻找第三方应用程序来查看录制内容。它有助于将在录制件中发现的问题与性能指标关联起来。

此功能需要 VDA 和 Session Recording Server 版本 2308 或更高版本。

Monitor 将会话录制文件存储在中央存储库中。单击 **Session Selector**（会话选择器）模式 > **Sessions with recordings**（包含录制文件的会话）链接时，将显示属于用户的录制文件列表。



可以选择查看过去 24 小时或者过去 2 天内处于活动状态的会话录制文件。当前活动会话的实时录制文件的会话结束时间标记为正在运行。

List of sessions with recordings

Sessions active during

☒ Last 24 hours

☐ Last 2 days

2 item(s)

Clicking on a row opens the associated session recording in a new tab.

Refresh

| Session Start Time ↓ | Session End Time    |                        |
|----------------------|---------------------|------------------------|
| 10/18/2023 2:25 PM   | Running             | <a href="#">View ↗</a> |
| 10/12/2023 3:48 PM   | 10/18/2023 12:18 PM |                        |

单击查看链接，使用 Citrix Session Recording 播放服务器在新选项卡中播放录制文件。

功能兼容性列表

September 11, 2023

Citrix Monitor 支持三个 Citrix DaaS (以前称为 Citrix Virtual Apps and Desktops 服务) 版本。它们是 **Premium**、**Citrix DaaS Advanced** 和 **Citrix DaaS Advanced Plus**。下表列出了特定的 Citrix Monitor 功能、VDA 版本、相关组件及其各自的许可证版本。

| 功能                                          | 依赖组件 - 所需的最<br>低版本                 | Premium | Citrix DaaS<br>Advanced | Citrix DaaS<br>Advanced Plus |
|---------------------------------------------|------------------------------------|---------|-------------------------|------------------------------|
| <a href="#">适用于 AMD GPU<br/>的实时 GPU 利用率</a> | 运行 64 位<br>Windows 的 VDA 7<br>2212 | 是       | 是                       | 是                            |

| 功能                                                           | 依赖组件 - 所需的最低版本                      | Premium | Citrix DaaS Advanced | Citrix DaaS Advanced Plus |
|--------------------------------------------------------------|-------------------------------------|---------|----------------------|---------------------------|
| <a href="#">访问 Citrix Analytics for Performance - 会话详细信息</a> | Citrix Analytics for Performance 权限 | 是       | 是                    | 是                         |
| <a href="#">会话自动重新连接</a>                                     | VDA 1906                            | 是       | 是                    | 是                         |
| <a href="#">会话启动持续时间</a>                                     | VDA 1903                            | 是       | 是                    | 是                         |
| <a href="#">桌面探测</a>                                         | Citrix Probe Agent 1903             | 是       | 否                    | 否                         |
| <a href="#">配置文件加载过程中 Citrix Profile Management 的持续时间</a>    | VDA 1903                            | 是       | 是                    | 是                         |
| <a href="#">配置文件深入分析</a>                                     | VDA 1811                            | 是       | 是                    | 是                         |
| <a href="#">虚拟机管理程序警报监视</a>                                  | 无                                   | 是       | 否                    | 否                         |
| <a href="#">应用程序探测</a>                                       | Citrix Application Probe Agent 1811 | 是       | 否                    | 否                         |
| <a href="#">Microsoft RDS 许可证运行状况</a>                        | VDA 7.16                            | 是       | 是                    | 是                         |
| <a href="#">从 Monitor 访问计算机控制台</a>                           | XenServer Hypervisor 7.3            | 是       | 是                    | 是                         |
| <a href="#">导出过滤器数据</a>                                      | 无                                   | 是       | 是                    | 是                         |
| <a href="#">交互式会话深入分析</a>                                    | VDA 1808                            | 是       | 是                    | 是                         |
| <a href="#">GPO 深入分析</a>                                     | VDA 1808                            | 是       | 是                    | 是                         |
| <a href="#">使用 OData API 时可用的计算机历史数据</a>                     | 无                                   | 是       | 是                    | 是                         |
| <a href="#">智能警报策略</a>                                       | 无                                   | 是       | 否                    | 否                         |
| <a href="#">Health Assistant 链接</a>                          | 无                                   | 是       | 是                    | 是                         |
| <a href="#">交互式会话深入分析</a>                                    | 无                                   | 是       | 是                    | 是                         |
| <a href="#">应用程序分析</a>                                       | VDA 7.15                            | 是       | 是                    | 是                         |

| 功能                                         | 依赖组件 - 所需的最低版本 | Premium | Citrix DaaS<br>Advanced | Citrix DaaS<br>Advanced Plus |
|--------------------------------------------|----------------|---------|-------------------------|------------------------------|
| <a href="#">OData API V.4</a>              | 无              | 是       | 是                       | 是                            |
| <a href="#">重影 Linux VDA 用户</a>            | VDA 7.16       | 是       | 是                       | 是                            |
| <a href="#">计算机控制台访问</a>                   | 无              | 是       | 是                       | 是                            |
| <a href="#">应用程序故障监视</a>                   | VDA 7.15       | 是       | 是                       | 是                            |
| <a href="#">以应用程序为中心的故障排除</a>              | VDA 7.13       | 是       | 是                       | 是                            |
| <a href="#">磁盘监视</a>                       | VDA 7.14       | 是       | 是                       | 是                            |
| <a href="#">GPU 监视</a>                     | VDA 7.14       | 是       | 是                       | 是                            |
| <a href="#">“会话详细信息”面板上的传输协议</a>           | VDA 7.13       | 是       | 是                       | 是                            |
| <a href="#">用户友好的连接和计算机故障说明</a>            | VDA 7.x        | 是       | 是                       | 是                            |
| <a href="#">历史数据保留</a>                     | VDA 7.x        | 是       | 否                       | 否                            |
| <a href="#">自定义报告</a>                      | VDA 7.x        | 是       | 否                       | 否                            |
| <a href="#">资源利用率报告</a>                    | VDA 7.11       | 是       | 是                       | 是                            |
| <a href="#">针对 CPU、内存和 ICA RTT 条件扩展了警报</a> | VDA 7.11       | 是       | 否                       | 否                            |
| <a href="#">导出报告改进功能</a>                   | VDA 7.x        | 是       | 是                       | 是                            |
| <a href="#">登录持续时间细分</a>                   | VDA 7.x        | 是       | 是                       | 是                            |
| <a href="#">主动监视和警告</a>                    | VDA 7.x        | 是       | 否                       | 否                            |
| <a href="#">托管应用程序使用情况</a>                 | VDA 7.x        | 是       | 否                       | 否                            |
| <a href="#">单会话和多会话操作系统使用情况</a>            | VDA 7.x        | 是       | 否                       | 否                            |
| <a href="#">支持 Framehawk 虚拟通道</a>          | VDA 7.6        | 是       | 是                       | 是                            |

委派管理和监视

March 30, 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。

管理权限决定向管理员呈现的监视界面以其可以执行的任务。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。

监视功能现在支持委派管理员角色，该角色允许您向管理员分配自定义的已定义角色或内置角色。角色决定可用权限以及管理员如何使用监视功能。您还可以定义适用于这些角色的作用域。作用域定义角色适用的对象。

有关创建委派管理员的信息，请参阅重要的[委派管理](#)文章。

内置角色和权限决定管理员对监视器的使用方式：

| 管理员角色           | 监视器中的权限                                                                                                                                         |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 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以及全局信息。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。可以对单个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。监视器不支持此管理员，因此其无法查看数据。                                                                                                                     |
| Probe Agent 管理员 | 只读访问“应用程序”页面，无法访问任何其他视图。用于在终端计算机上运行 Citrix Probe Agent。                                                                                         |
| 监视完全权限管理员       | 对监视选项卡中的所有视图和命令具有完全访问权限                                                                                                                         |

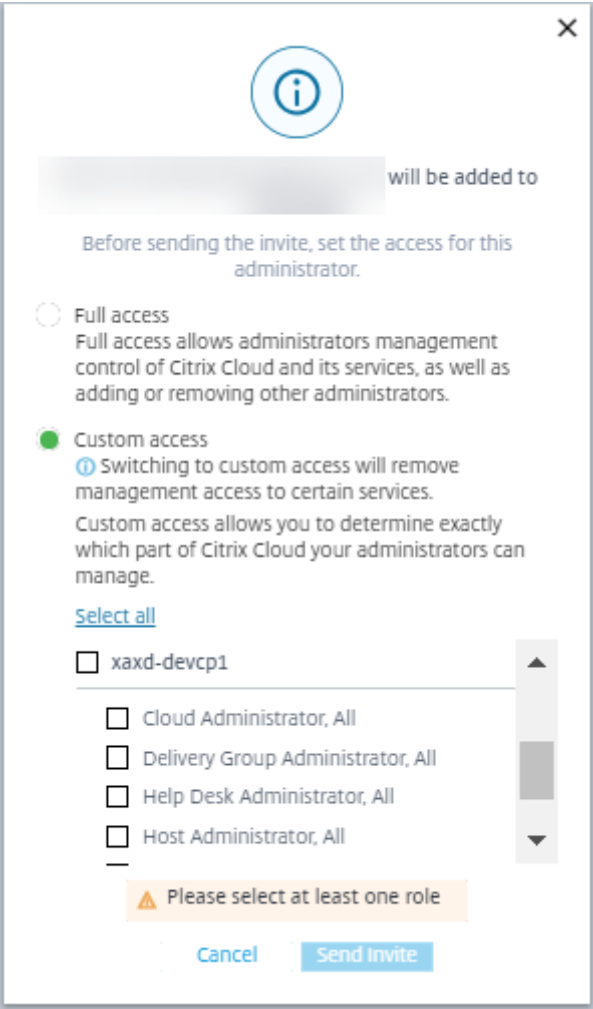
管理员角色

监视器中的权限

会话管理员

可以在监视选项卡的过滤器页面上查看交付组并管理其关联的会话和计算机。

要向用户分配角色（内置角色或自定义角色），请从 Citrix Cloud 菜单中转到身份识别和访问管理 > 管理员。在此处，当您添加或编辑管理员的访问权限时，可以选择自定义访问和列出的角色之一。



可以在完整配置 > 管理员 > 管理员中定义自定义角色和作用域。

将列出具有自定义作用域的内置角色和自定义角色以供选择。



- ☐ Cloud Administrator, All
- ☐ Delivery Group Administrator, All
- ☐ Delivery Group Administrator, rds1DGAndCatalog
- ☐ Delivery Group Administrator, vdaDGOnly
- ☐ Full Monitor Administrator, All - Access to 'Monitor' tab only
- ☐ Full Monitor Administrator, rds1DGAndCatalog - Access to 'Monitor' tab only
- ☐ Full Monitor Administrator, vdaDGOnly - Access to 'Monitor' tab only
- ☐ Help Desk Administrator, All - Access to 'Monitor' tab only
- ☐ Help Desk Administrator, rds1DGAndCatalog - Access to 'Monitor' tab only
- ☐ Help Desk Administrator, vdaDGOnly - Access to 'Monitor' tab only
- ☐ Host Administrator, All
- ☐ Host Administrator, rds1DGAndCatalog
- ☐ Host Administrator, vdaDGOnly
- ☐ Machine Catalog Administrator, All
- ☐ Machine Catalog Administrator, rds1DGAndCatalog
- ☐ Machine Catalog Administrator, vdaDGOnly
- ☐ Probe Agent Administrator, All
- ☐ Probe Agent Administrator, rds1DGAndCatalog
- ☐ Probe Agent Administrator, vdaDGOnly
- ☐ Read Only Administrator, All
- ☐ Read Only Administrator, rds1DGAndCatalog
- ☐ Read Only Administrator, vdaDGOnly
- ☒ TrendsFiltersAndUD, All
- ☐ TrendsFiltersAndUD, rds1DGAndCatalog
- ☐ TrendsFiltersAndUD, vdaDGOnly



## 数据粒度和保留

January 18, 2023

### 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。

### 并发数据评估

您的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不包含数据。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。对于特定的数据粒度，请从特定汇总表中提取最小和最大的 SummaryDate，以确定最早和最新的聚合时间间隔。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，必须注意不存在可能发生的任何部分时间间隔或时间段的开头和结尾部分的汇总数据。

- 缺失的事件和延迟事件。如果在聚合时间段有事件缺失或延迟，聚合到汇总表中的指标可能会略有误差。尽管 Monitor Service 尝试维护准确的最新状态，但是它不会针对缺失或延迟的事件后退到过去重新计算汇总表中的聚合值。
- 连接高可用性。在连接高可用性期间，当前连接的汇总数据计数存在误差，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

监视器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 <= 30 天采用每小时粒度。
- T > 31 天采用每天粒度。

非来源于聚合数据的请求数据来源于原始会话和连接信息。此数据往往增长很快，因此具有自己的整理设置。通过整理可确保仅长期保留相关数据。这样可以确保实现更好的性能，同时维护报告所需的粒度。

|   | 设置名称                        | 受影响的整理                                       | Premium 的保留天数 | Advanced 的保留天数 |
|---|-----------------------------|----------------------------------------------|---------------|----------------|
| 1 | GroomSessionsRetentionDays  | 会话和连接记录保留期限                                  | 90            | 31             |
| 2 | GroomFailuresRetentionDays  | MachineFailureLog 和 Connection-FailureLog 记录 | 90            | 31             |
| 3 | GroomLoadIndexRetentionDays | 负载索引记录                                       | 90            | 31             |

|    | 设置名称                                     | 受影响的整理                                                                                                                            | Premium 的保留天数 | Advanced 的保留天数 |
|----|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|---------------|----------------|
| 4  | GroomDeletedRetentionDays                | 生命周期状态为 “Deleted” 的 Machine、Catalog、DesktopGroup 和 Hypervisor 实体。这还将删除任何相关的 Session、SessionDetail、Summary、Failure 或 LoadIndex 记录。 | 90            | 31             |
| 5  | GroomSummaryRetentionDays                | DesktopGroupSummary、FailureLog-Summary 和 LoadIndex-Summary 记录。聚合数据 - 日粒度。                                                         | 65            | 31             |
| 6  | GroomMachineHourlyRetentionDays          | 应用程序和 Controller 计算机的修补程序                                                                                                         | 90            | 31             |
| 7  | GroomHourlyRetentionDays                 | 聚合数据 - 小时粒度                                                                                                                       | 32            | 31             |
| 8  | GroomApplicationLogRetentionDays         | 应用程序历史记录                                                                                                                          | 90            | 不适用            |
| 9  | GroomNotificationLogRetentionDays        | 通知历史记录                                                                                                                            | 90            | 不适用            |
| 10 | GroomResourceUsageRawDataRetentionDays   | 资源利用率 - 原始数据                                                                                                                      | 3             | 3              |
| 11 | GroomResourceUsageRateDataRetentionDays  | 资源利用率 - 数据 - 小时粒度                                                                                                                 | 30            | 30             |
| 12 | GroomResourceUsageTotalDataRetentionDays | 资源利用率 - 数据 - 天粒度                                                                                                                  | 65            | 31             |
| 13 | GroomProcessUsageRawDataRetentionDays    | 进程利用率 - 原始数据                                                                                                                      | 1             | 1              |

|    | 设置名称                   | 受影响的整理   | Premium 的保留天数 | Advanced 的保留天数 |
|----|------------------------|----------|---------------|----------------|
| 14 | GroomProcessUsage      | 进程利用率数据  | 7             |                |
|    |                        | 小时粒度     |               |                |
| 15 | GroomProcessUsage      | 进程利用率数据  | 30            | 30             |
|    |                        | 天粒度      |               |                |
| 16 | GroomSessionMetrics    | 会话指标数据   | 1             | 1              |
| 17 | GroomMachineMetrics    | 计算节点指标数据 | 3             | 3              |
| 18 | GroomMachineMetrics    | 计算节点指标数据 | 365           | 365            |
|    |                        | 数据       |               |                |
| 19 | GroomApplicationErrors | 应用程序错误数据 | 1             | 1              |
|    |                        | 数据       |               |                |
| 20 | GroomApplicationErrors | 应用程序故障数据 | 1             | 1              |
|    |                        | 数据       |               |                |

小心：

您无法修改 Monitor Service 数据库中的值。

长期保留数据会对表格大小产生以下影响：

- 小时数据。如果允许小时粒度的数据在数据库中最多保留两年，具有 1000 个交付组的站点将导致数据库按以下方式增长：  
  
1000 个交付组 x 24 小时/天 x 365 天/年 x 2 年 = 17,520,000 行数据。聚合表中存在如此巨大的数据量对性能的影响是非常显著的。如果从此表格提取控制板数据，将需要使用大型数据库服务器。数据量过大会对性能造成巨大影响。
- 会话和事件数据。这是指每次启动会话和建立连接/重新连接时收集的数据。对于大型站点（10 万个用户），此数据的增长速度很快。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。

会话启动诊断

March 30, 2024

注意：

会话启动诊断功能当前处于预览阶段。

会话启动涉及多个 Citrix 组件。要诊断会话启动失败情况，请使用 Citrix Monitor（即 Citrix Director 服务）缩小到出现问题的确切组件和阶段。应用建议的操作以解决问题。Citrix Workspace 应用程序生成一个 32 位数 (8-4-4-12) 的事务 ID，可用于诊断会话启动失败情况。

注意：

此功能仅适用于美国、亚太东南部和欧洲地区的云客户。此功能不在日本和政府区域提供。

## 必备条件

如果您使用的是 Citrix DaaS，则系统会自动启动。使用本地 StoreFront 的云客户必须确保已加入受支持的 StoreFront 版本。

- 如果您正在使用 Citrix Analytics 提高性能，请参阅 [数据源](#) 以了解加入本地 StoreFront 的步骤。
- 如果您未使用 Citrix Analytics for Performance:
  1. 转到 <https://analytics.cloud.com/unified-datasources/perf/Citrix%20Virtual%20Apps%20and%20Desktops/site-details>。
  2. 单击 连接到 **StoreFront** 部署，输入详细信息，然后下载配置文件。有关更多信息，请参阅 [使用 StoreFront 接入本地站点](#)。

注意：

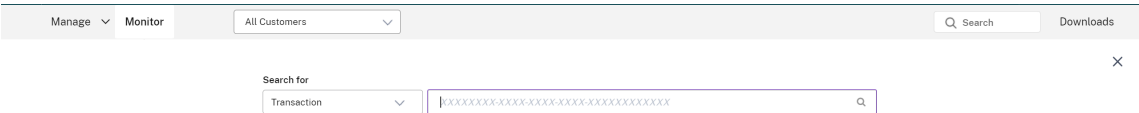
拥有云管理员角色的管理员可以加载 StoreFront 部署，而拥有“完全监视管理员”角色的管理员只能查看 StoreFront 部署。

其他组件支持的最低版本如下：

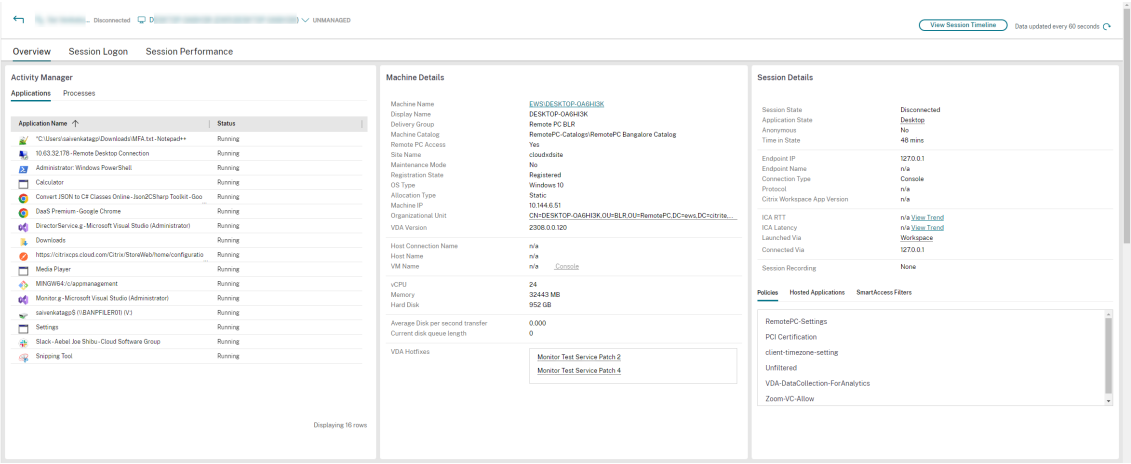
- 适用于 Windows 的 Citrix Workspace 应用程序 2109
- 适用于 Mac 的 Citrix Workspace 应用程序 2112
- 适用于 Linux 的 Citrix Workspace 应用程序 2112
- 适用于 HTML5 2110 的 Citrix Workspace 应用程序
- 适用于 Chrome 2110 的 Citrix Workspace
- 适用于 Android 2110 的 Citrix Workspace 应用程序
- VDA 版本 Citrix Virtual Apps and Desktops 2112
- Citrix StoreFront 1912 LTSR CU4

## 诊断会话启动失败的步骤

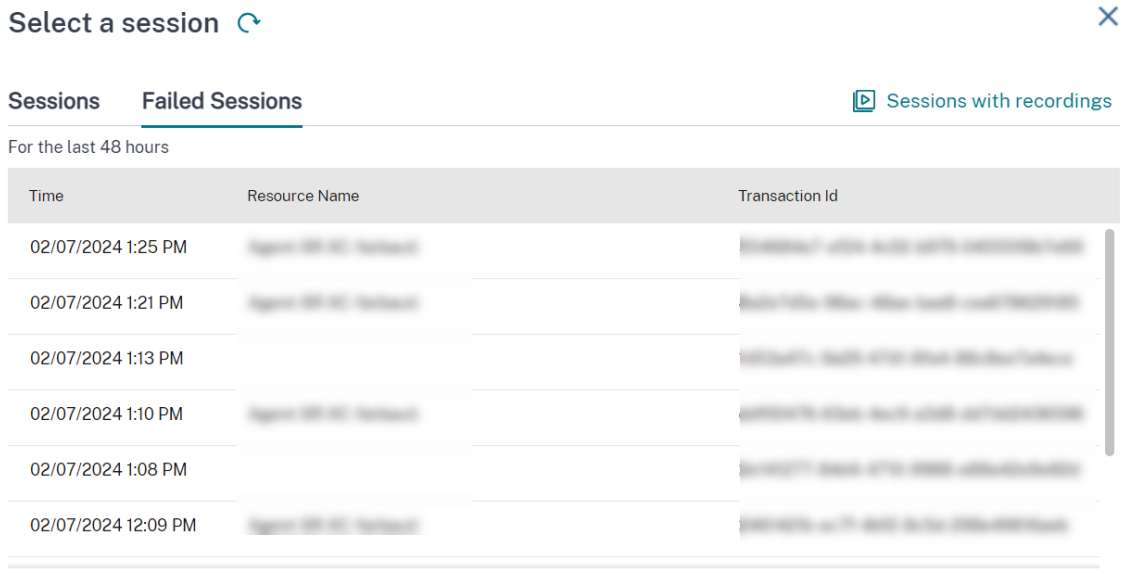
1. 从 Citrix Workspace 应用程序复制失败的事务 ID。
2. 在 Monitor UI 中，搜索 32 位事务 ID，然后单击“详细信息”。



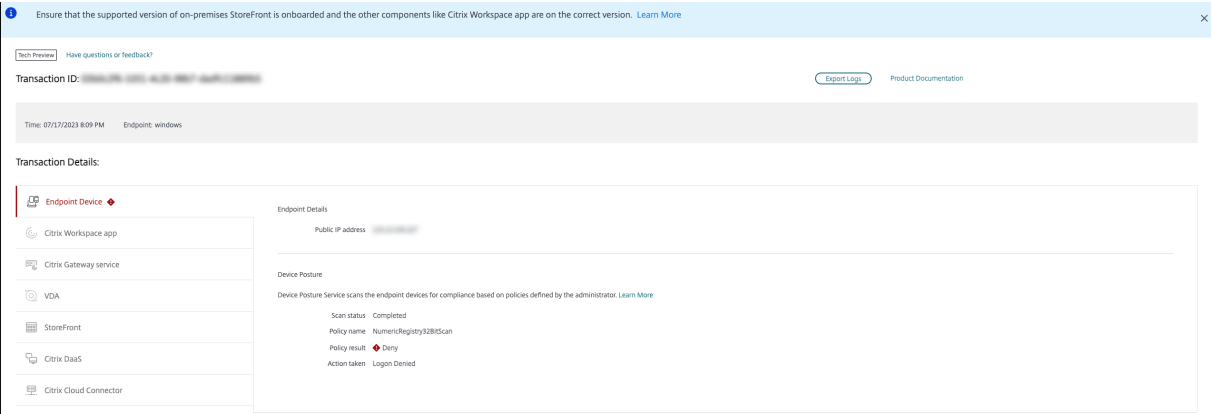
3. 如果事务 ID 不可用，请使用用户名进行搜索。将显示用户的活动管理器。



4. 单击会话选择器。转到“失败的会话”选项卡。将显示过去 48 小时内失败的会话列表。单击所选会话。



5. Citrix Monitor 显示有关事务的关键信息，例如用户名、时间戳以及发生故障的应用程序或桌面。
6. “事务详细信息” 面板包含一个指示故障发生情况的组件列表。
7. 在组件列表中单击端点设备以查看设备状态扫描状态。Device Posture Service 根据管理员定义的策略扫描端点设备的合规性。



将显示扫描状态、策略名称、策略结果和采取的操作。确保设备状态服务已按照 [Device Posture](#) 一文中所述配置了 DaaS。Device Posture 记录的错误在 [Device Posture 错误日志](#) 中介绍。

1. 单击其他组件名称可查看“组件详细信息”和“上次已知故障”详细信息。
2. 此时将显示“失败原因”和“错误代码”。单击了解有关错误的更多信息链接，在“错误代码”部分中查看具体的 [错误代码](#)，其中包含详细说明和建议的操作。
3. 可以导出日志进行查看。日志文件按时间顺序列出会话启动步骤，并显示确切的组件及其发生故障的阶段。
4. 如果组件发生多次故障，则事务页面上仅显示最近已知的故障详细信息。导出的日志包含与事务相关的所有故障的详细信息。

注意：

客户端错误代码和诊断信息仅在 Citrix StoreFront 已加入并正在发送数据时可用。有关加入 StoreFront 的更多信息，请参阅 [先决条件](#)。

## Broker Agent

### bka.prepare.session.failure.validation

- 说明：无法验证准备会话请求。
- 建议的操作：“重试”操作。如果再次出现故障，请检查连接器是否处于正常运行状态。

### bka.prepare.session.failure.rejected

- 说明：VDA 无法接受启动请求。
- 建议的操作：在 VDA 上重新启动 Citrix Delivery Agent 服务或者重新启动 VDA。

### bka.hdx.prepare.failure.general

- 说明：HDX 准备失败。
- 建议的操作：重新启动 VDA。

#### **bka.hdx.validate.failure.ticket\_not\_found**

- 说明：引用的票证或启动项不在启动缓存中。
- 建议的操作：确保 VDA 可以与连接器通信。

#### **bka.ticketing.validate.failure.unlicensed**

- 说明：无法验证启动许可证。
- 建议的操作：联系 Citrix 技术支持。

#### **bka.ticketing.validate.failure.general**

- 描述：验证票证时出现一般故障。
- 建议的操作：收集 VDA 上的日志并联系 Citrix 技术支持。

#### **bka.set.configuration.failure.policy**

- 说明：设置策略时出错。
- 建议的操作：在 VDA 上重新启动 Citrix Delivery Agent 服务或者重新启动 VDA。

#### **bka.set.configuration.failure**

- 说明：设置配置时出错。
- 建议的操作：在 VDA 上重新启动 Citrix Delivery Agent 服务或者重新启动 VDA。

### **Broker**

#### **brk.validate.credentials.failure.invalid**

- 说明：由于某些问题，无法验证凭据。可以在消息参数中扩展原因。
- 建议的操作：“重试”操作。如果再次出现故障，请检查连接器是否处于正常运行状态。

#### **brk.resolve.machine.failure.general**

- 说明：枚举或解析工作线程失败。可以在消息参数中扩展原因。
- 建议的操作：确保能够启动此应用程序的计算机已在 Broker 中注册。确保所有可用的计算机都没有达到其容量。



#### **brk.license.check.failure.constraints**

- 说明：许可限制启动失败的会话。
- 建议的操作：确保有可用于此类应用程序或桌面的许可证。

#### **brk.resolve.machine.failure.t**

- 说明：Broker 在联系数据库时超时。
- 建议的操作：与站点数据库通信时出现问题。联系 Citrix 技术支持。

#### **brk.poweron.forlaunch.queued.failure.general**

- 说明：排队执行的电源操作失败。
- 建议的操作：与站点数据库通信时出现问题。联系 Citrix 技术支持。

#### **brk.set.configuration.failure.general**

- 说明：在目标 VDA 上设置配置时出现未指定的错误。
- 建议的操作：在 VDA 上重新启动 Citrix Delivery Agent 服务或者重新启动 VDA。

#### **brk.prepare.session.failure.host\_unreachable**

- 说明：无法与 VDA 通信。
- 建议的操作：在 VDA 上重新启动 Citrix Delivery Agent 服务或者重新启动 VDA。

#### **brk.prepare.session.failure.general**

- 说明：无法在 VDA 上准备会话、UnsupportedClientType 或 ConnectionRefused 错误。
- 建议的操作：在 VDA 上重新启动 Citrix Delivery Agent 服务或者重新启动 VDA。

#### **brk.validate.ticket.failure.license**

- 说明：无法检索此会话的有效许可证。
- 建议的操作：检查站点的运行状况并确保所有连接器和 Citrix DDC 均可运行。

#### **brk.validate.ticket.failure.general**

- 说明：无效的票证调用。
- 建议的操作：联系 Citrix 技术支持。

### **brk.reverse.prepare.failure.general**

- 说明：会话启动期间出现一般故障。
- 建议的操作：检查站点的运行状况并确保所有连接器和 Citrix DDC 均可运行。

### **brk.reverse.prepare.failure.lease\_revoked**

- 说明：此会话的租约已撤销。
- 推荐的操作：执行“重试”操作，如果再次出现故障，请检查连接器是否处于正常运行状态。

### **brk.reverse.prepare.failure.resource\_unavailable**

- 说明：资源已在使用中或暂时不可用。
- 推荐的操作：执行“重试”操作，如果再次出现故障，请检查连接器是否处于正常运行状态。

### **brk.reverse.prepare.failure.app\_protection**

- 说明：App Protection 功能缺失，但此会话需要此保护。
- 建议的操作：确保在此 VDA 上启用了 App Protection，或者从应用程序中删除 App Protection 要求。

## **HDX VDA Linux**

### **VDA\_LINUX\_ERR\_RECONNECT\_PRE\_LOGOFF**

- 说明：不允许重新连接到处于注销前状态的会话。
- 推荐的操作：重试稍后再启动，这样就可以让会话注销了。

### **VDA\_LINUX\_ERR\_RECONNECT\_NO\_SESSION**

- 说明：重新连接到非退出会话。
- 建议的操作：稍后重试启动。如果仍然失败，请联系 Citrix 技术支持。

### **VDA\_LINUX\_ERR\_SAME\_KEY**

- 说明：准备连接，但现有会话具有相同的会话密钥。
- 建议的操作：联系 Citrix 技术支持。

### **VDA\_LINUX\_ERR\_GET\_FQDN**

- 说明：无法获取此 VDA 的 FQDN。
- 建议的操作：验证 VDA 上的 DNS 配置是否正确

### **VDA\_LINUX\_ERR\_NO\_CGP\_LISTENER**

- 说明：没有正在运行的 CGP 侦听器。
- 建议的操作：验证会话可靠性连接策略是否已启用。验证 CGP 侦听器是否正在监听 VDA 中的预期端口（默认端口为 2598，可通过会话可靠性端口号策略进行更改）。

### **VDA\_LINUX\_ERR\_DTLS\_CONNECT**

- 说明：无法建立与网关服务的 DTLS 连接。
- 建议的操作：确认可从 VDA 访问网关服务 FQDN。验证 VDA 中是否存在路径 `/var/xdm/keystore/cacerts`。删除 `/var/xdm/keystore` 并运行 `/var/xdm/split_ca_bundle.sh` 以重新生成 CA 证书。验证网关服务 FQDN 是否受 VDA 信任。

### **VDA\_LINUX\_ERR\_ACCEPT\_EDT\_CONNECT**

- 说明：无法接受来自客户端的 EDT 握手。
- 建议的操作：联系 Citrix 技术支持。

### **VDA\_LINUX\_ERR\_TCP\_CONNECT**

- 说明：无法建立与网关服务的 TCP 连接。
- 建议的操作：确认可从 VDA 访问网关服务 FQDN。

### **VDA\_LINUX\_ERR\_TLS\_CONNECT**

- 说明：无法建立与网关服务的 TLS 握手。
- 建议的操作：验证 VDA 中是否存在路径 `/var/xdm/keystore/cacerts`。删除 `/var/xdm/keystore` 并运行 `/var/xdm/split_ca_bundle.sh` 以重新生成 CA 证书。验证网关服务 FQDN 是否受信任。

### **VDA\_LINUX\_ERR\_RDVZ\_HANDSHAKE**

- 说明：无法建立与网关服务的 Rendezvous 握手。
- 建议的操作：联系 Citrix 技术支持。

#### **VDA\_LINUX\_ERR\_ACCEPT\_ICA\_CONNECT**

- 说明：无法接受 ICA 连接。
- 建议的操作：联系 Citrix 技术支持。

#### **VDA\_LINUX\_ERR\_RECONNECT\_TO\_ANON\_SESSION\_NOT\_ALLOWED**

- 说明：不允许重新连接到匿名会话。
- 建议的操作：联系 Citrix 技术支持。

#### **VDA\_LINUX\_ERR\_CONN\_NOT\_ALLOWED**

- 说明：不允许连接。
- 建议的操作：如果结果代码为 3，请验证许可证是否未过期，否则，请稍后重试启动。如果无法解决此问题，请联系 Citrix 技术支持。

#### **VDA\_LINUX\_ERR\_CONN\_GENERAL**

- 说明：无法验证连接。
- 建议的操作：联系 Citrix 技术支持。

#### **VDA\_LINUX\_ERR\_USER\_CANCELLED\_LOGIN**

- 说明：最终用户已取消登录。
- 推荐操作：如果禁用 SSO，最终用户单击登录框中的“取消”按钮，则会出现此错误，否则请联系 Citrix 支持人员。

#### **VDA\_LINUX\_ERR\_GET\_TARGET**

- 说明：无法获取目标会话。
- 建议的操作：联系 Citrix 技术支持。

#### **VDA\_LINUX\_ERR\_START\_LOGON\_TIMERS**

- 说明：启动登录计时器失败。
- 建议的操作：联系 Citrix 技术支持。

#### **VDA\_LINUX\_ERR\_SEND\_CMD\_TO\_TARGET**

- 说明：无法向目标会话发送命令。
- 建议的操作：联系 Citrix 技术支持。

#### **VDA\_LINUX\_ERR\_POST\_RECONNECT\_EVENT**

- 说明：无法发布重新连接事件。
- 建议的操作：联系 Citrix 技术支持。

#### **VDA\_LINUX\_ERR\_RECONNECT\_TIMEOUT**

- 说明：重新连接到用户会话超时。
- 建议的操作：联系 Citrix 技术支持。

### **HDX VDA Windows**

#### **RENDEZVOUS\_CONNECT\_FAILED\_TCP**

- 说明：通过 TCP 尝试建立出站 Rendezvous 传输连接失败。
- 建议的操作：由于网络状况不佳，可能会出现零星故障。这是预期行为。如果经常发生这种情况，请检查 VDA 配置，然后联系 Citrix 技术支持。

#### **RENDEZVOUS\_CONNECT\_FAILED\_EDT**

- 说明：通过 TCP 尝试建立出站 Rendezvous 传输连接失败。
- 建议的操作：由于网络状况不佳，可能会出现零星故障。这是预期行为。如果经常发生这种情况，请检查 VDA 配置，然后联系 Citrix 技术支持。

#### **RENDEZVOUS\_CONNECT\_FAILED\_PROXY**

- 说明：由于代理配置无效，出站 Rendezvous 传输连接尝试失败。
- 建议的操作：检查 Rendezvous 代理配置，联系 Citrix 技术支持。

#### **RENDEZVOUS\_CONNECT\_FAILED\_DTLS**

- 描述：由于安全传输握手失败，出站 Rendezvous 传输连接尝试失败。
- 建议的操作：检查 Rendezvous 配置，检查加密配置。联系 Citrix 技术支持。

### **RENDEZVOUS\_CONNECT\_FAILED\_TLS**

- 说明：由于安全传输握手失败，尝试建立出站 Rendezvous 传输连接失败。
- 建议的操作：检查 Rendezvous 配置、检查加密配置以及联系 Citrix 技术支持。

### **RENDEZVOUS\_CONNECT\_FAILED\_CGP**

- 说明：由于 CGP 配置问题，出站 Rendezvous 传输连接尝试失败。
- 建议的操作：检查是否已启用 CGP（会话可靠性）以及是否正在监听 CGP 端口，联系 Citrix 技术支持。

### **CGP\_SR\_SUSPEND\_RESUME\_FAILED\_TIMEOUT**

- 说明：由于超时，网络中断未解决，会话可靠性无法恢复连接。
- 建议的操作：由于网络状况不佳，可能会出现零星故障。这是预期行为。

### **CGP\_SR\_SUSPEND\_RESUME\_FAILED**

- 说明：由于不可预见的错误，无法解决网络中断问题，会话可靠性无法恢复连接。
- 建议的操作：由于网络状况不佳，可能会出现零星故障。这是预期行为。

### **PREPARE\_RECONNECT\_REJECTED**

- 说明：由于会话密钥无效，VDA 拒绝了来自传入 ICA 连接的重新连接请求。
- 建议的操作：检查 VDA 配置，联系 Citrix 技术支持。

### **错误：PREPARE\_REJECTED**

- 说明：由于会话密钥无效，VDA 拒绝了来自传入 ICA 连接的连接请求。
- 建议的操作：检查 VDA 配置，联系 Citrix 技术支持。

### **PREPARE\_LISTENING\_FAILED**

- 说明：VDA 无法启动传入 ICA 连接的侦听器。
- 建议的操作：检查网络配置、验证侦听器端口是否未被其他应用程序使用、联系 Citrix 技术支持。

### **RENDEZVOUSCONNECTIONREQ\_FAILED**

- 描述：VDA 未能通知 ICA 堆栈启动出站 Rendezvous 连接。
- 建议的操作：检查 Rendezvous 配置、检查 Rendezvous 代理配置、检查 CGP（会话可靠性）配置、联系 Citrix 技术支持。

### **RENDEZVOUSCONNECTIONREQ\_FAILED\_PROXYCONFIG**

- 说明：由于代理配置错误，VDA 无法请求 ICA 堆栈启动出站 Rendezvous 连接。
- 建议的操作：检查 Rendezvous 代理配置，联系 Citrix 技术支持。

### **ESTABLISH\_SESSION\_FAILED**

- 说明：VDA 无法为传入的 ICA 连接创建会话，或者无法连接到现有会话。
- 建议的操作：联系 Citrix 技术支持。

### **ICA\_ESTABLISH\_FAILED**

- 说明：ICA 连接接受或握手失败。
- 建议的操作：联系 Citrix 技术支持。

### **VALIDATE\_FAILED**

- 说明：Broker 无法验证来自 VDA 的传入 ICA 连接请求。
- 建议的操作：联系 Citrix 技术支持。

### **VALIDATE\_TICKETING\_FAILED**

- 说明：由于票证问题，Broker 无法验证来自 VDA 的传入 ICA 连接请求。
- 建议的操作：联系 Citrix 技术支持。

### **MCS**

#### **brk.poweron.forlaunch.execution.generalfailure**

- 说明：一般错误。
- 建议的操作：联系 Citrix 技术支持。

#### **brk.poweron.forlaunch.execution.insufficientresourcefailure**

- 说明：由于虚拟机管理程序资源不足，无法完成虚拟机管理程序操作。
- 建议的操作：检查虚拟机管理程序中的资源配额。如果找不到解决方案，请联系 Citrix 技术支持。

#### **brk.poweron.forlaunch.execution.nosuchmanagedmachine**

- 说明：计算机 ID 不存在。
- 建议的操作：检查虚拟机管理程序中的计算机 ID。如果找不到解决方案，请联系 Citrix 技术支持。

#### **brk.poweron.forlaunch.execution.hypervisorconnectionfailure**

- 说明：无法建立与虚拟机管理程序的连接。例如，找不到托管基础结构地址。
- 建议的操作：验证托管基础结构地址是否正确。如果找不到解决方案，请联系 Citrix 技术支持。

#### **brk.poweron.forlaunch.execution.invalidcredentialsfailure**

- 说明：凭据无效。
- 建议的操作：检查虚拟机管理程序连接的凭据。如果找不到解决方案，请联系 Citrix 技术支持。

#### **brk.poweron.forlaunch.execution.authorizationfailure**

- 说明：权限或凭据不足。
- 建议的操作：检查分配给虚拟机管理程序连接凭据的权限。如果找不到解决方案，请联系 Citrix 技术支持。

#### **brk.poweron.forlaunch.execution.sslcertauthfailure**

- 说明：由于 SSL 身份验证问题，无法建立连接。
- 建议的操作：检查虚拟机管理程序的连接证书。如果找不到解决方案，请联系 Citrix 技术支持。

#### **brk.poweron.forlaunch.execution.ratelimitedfailure**

- 说明：云连接报告其受到速率限制。
- 建议的操作：如果请求被虚拟机管理程序的速率限制阻止，请稍后重试连接。如果找不到解决方案，请联系 Citrix 技术支持。



#### **brk.poweron.forlaunch.execution.connectorconnectionfailure**

- 说明：Cloud Connector 上存在错误。例如，等待连接时发生超时。一旦达到超时时间，Cloud Connector 就会断开连接。
- 建议的操作：重新启动 Cloud Connector。如果该操作失败，请联系 Citrix 技术支持。

#### **brk.poweron.forlaunch.execution.remotehclserverconnectionfailure**

- 说明：在设置与插件的连接时，未发现 HCL/远程代理插件或端点上的错误。
- 建议的操作：重新启动连接器。如果该操作失败，请联系 Citrix 技术支持。

#### **brk.poweron.forlaunch.execution.expiredcredentialsfailure**

- 说明：提供的凭证已过期。
- 建议的操作：刷新虚拟机管理程序连接使用的过期凭据。

#### **brk.poweron.forlaunch.execution.mcsmachinemanagementcustomfailure**

- 说明：计算机创建过程中出现错误。
- 建议的操作：联系 Citrix 技术支持。

#### **brk.poweron.forlaunch.execution.detachdiskfailed**

- 说明：虚拟机使用的分离磁盘出现故障。
- 建议的操作：联系 Citrix 技术支持。

#### **brk.poweron.forlaunch.execution.createclonefailed**

- 说明：在虚拟机管理程序中创建克隆磁盘失败。
- 建议的操作：联系 Citrix 技术支持。

#### **brk.poweron.forlaunch.execution.provisionedvmnotfound**

- 说明：找不到预配的 VM。
- 建议的操作：从目录中删除预配的 VM。如果该操作失败，请联系 Citrix 技术支持。

#### **brk.poweron.forlaunch.execution.invalidvmstate**

- 说明：由于 VM 状态无效，操作无法继续。
- 建议的操作：首先重新启动 VM，然后重试该操作。

#### **brk.poweron.forlaunch.execution.insufficientresources**

- 说明：运行期间资源不足。
- 建议的操作：检查虚拟机管理程序使用的资源配额。

#### **brk.poweron.forlaunch.execution.hypervisorinmaintenancemode**

- 说明：该操作无法继续，因为虚拟机管理程序处于维护模式。
- 建议的操作：验证虚拟机管理程序是否处于维护模式。

#### **brk.poweron.forlaunch.execution.delayed**

- 说明：操作已排队。
- 建议的操作：等待进程完成。如果该操作失败，请联系 Citrix 技术支持。

#### **brk.poweron.forlaunch.execution.recreatevmfailed**

- 说明：重新创建 VM 失败。
- 建议的操作：联系 Citrix 技术支持。

#### **brk.poweron.forlaunch.execution.unknownvirtualmachine**

- 说明：未知虚拟机。
- 建议的操作：联系 Citrix 技术支持。

#### **brk.poweron.forlaunch.execution.ratelimitexceed**

- 说明：云连接的速率受到限制。
- 建议的操作：如果请求被虚拟机管理程序的速率限制阻止，请稍后重试连接。

#### **brk.poweron.forlaunch.execution.virtualdisknotyetonstorage**

- 说明：虚拟磁盘未存储。
- 建议的操作：稍后重试。如果该操作失败，请联系 Citrix 技术支持。

## Profile Management

### **xendesktop.upm.userprofile.error.failure**

- 说明：Citrix Profile Management 无法处理用户配置文件。请改为使用临时配置文件。
- 建议的操作：此错误不会导致登录失败。Citrix Profile Management 改为使用临时配置文件。要对错误进行故障排除，请查看 Windows 事件日志。

### **xendesktop.upm.userprofile.error.timeout**

- 说明：Citrix Profile Management 无法在指定时间内处理用户配置文件。
- 建议的操作：此错误不会导致登录失败。Citrix Profile Management 继续处理用户配置文件。要对错误进行故障排除，请查看 Citrix Profile Management 日志。

## WEM 代理

### **wem.agent.userpolicy.error.failure**

- 说明：Workspace Environment Management (WEM) 代理无法处理用户的组策略。用户继续将登录。
- 建议的操作：该错误不会导致登录失败。有关更多详细信息，请参阅 WEM 产品文档并查看 WEM 代理服务日志。

### **wem.agent.userpolicy.error.timeout**

- 说明：Workspace Environment Management (WEM) 代理未能在指定时间内为用户处理组策略。用户继续将登录。
- 建议的操作：该错误不会导致登录失败。有关更多详细信息，请参阅 WEM 产品文档并查看 WEM 代理服务日志。

## Android 启动后

### **SessionManager.Launch.EngineLoadFailed**

- 说明：无法加载或初始化 ICA 引擎。
- 建议的操作：联系 Citrix 技术支持。

### **SessionManager.Launch.ConnectionFailed**

- 说明：引擎在连接之前已终止。
- 建议的操作：联系 Citrix 技术支持。

### **SessionManager.Launch.LogonFailed**

- 说明：会话已断开连接，但未完成登录。
- 建议的操作：联系 Citrix 技术支持。

### **SessionManager.LeaseResolution.Failed**

- 说明：无法尝试启动租约。
- 建议的操作：联系 Citrix 技术支持。

### **SessionManager.clxmtp.SoftDeny**

- 说明：引擎 CLXMTP 协商失败（软拒绝）。
- 建议的操作：联系 Citrix 技术支持。

### **SessionManager.clxmtp.SoftDeny\_Implicit**

- 说明：引擎 CLXMTP 连接失败（隐式软拒绝）。
- 建议的操作：联系 Citrix 技术支持。

### **Transport.Connect.NoCGP\_Fail**

- 说明：连接失败（已禁用 CGP）。
- 建议的操作：联系 Citrix 技术支持。

### **Transport.Connect.FallbackFail**

- 说明：连接失败。已尝试 ICA 回退。
- 建议的操作：联系 Citrix 技术支持。

### **Transport.Connect.Fail**

- 说明：连接不可用。
- 建议的操作：联系 Citrix 技术支持。

## **Android** 预启动

### **CWA-ICADOWNLOAD\_ERR\_00001**

- 说明：发送 ICA 请求类型不正确。
- 建议的操作：联系 Citrix 技术支持。

### **CWA-ICADOWNLOAD\_ERR\_00002**

- 说明：ICA 请求无效。
- 建议的操作：联系 Citrix 技术支持。

### **CWA-ICADOWNLOAD\_ERR\_00003**

- 说明：ICA 请求的存储为空。
- 建议的操作：联系 Citrix 技术支持。

### **CWA-ICADOWNLOAD\_ERR\_00004**

- 说明：ICA 请求的应用商店 URL 为空。
- 建议的操作：联系 Citrix 技术支持。

### **CWA-ICADOWNLOAD\_ERR\_00005**

- 说明：ICA 请求的资源参数为空。
- 建议的操作：联系 Citrix 技术支持。

### **CWA-ICADOWNLOAD\_ERR\_00006**

- 说明：为 ICA 请求提供的资源参数不是有效的资源类型。
- 建议的操作：联系 Citrix 技术支持。

### **CWA-ICADOWNLOAD\_ERR\_00007**

- 说明：为 ICA 请求提供的资源参数对 ICA 启动 URL 为空。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_00008**

- 说明：带有身份验证管理器参数的 ICA 请求为空。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_00009**

- 说明：ICA 请求正文为空。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000010**

- 说明：无法通过 ICA 请求正文创建 HTTP 实体。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000011**

- 说明：由于创建身份验证管理器请求时出现异常，无法下载 ICA 文件。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000012**

- 说明：由于运行身份验证管理器请求时出现异常，无法下载 ICA 文件。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000013**

- 说明：由于来自身份验证管理器请求的意外响应，无法下载 ICA 文件。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000014**

- 说明：从身份验证管理器响应中复制 inputStream 时，无法下载 ICA 文件。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000015**

- 说明：无法使用身份验证管理器响应中的 inputStream 解析 ICA 文档。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000016**

- 说明：下载的 ICA 文档无一例外为空。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000017**

- 说明：由于响应不成功，无法下载 ICA 文件。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000018**

- 说明：资源不可用。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000019**

- 说明：要启动的资源不存在、未启用或对用户不可见。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000020**

- 说明：没有更多活动的会话。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000021**

- 说明：服务器没有执行请求的活动所需的许可证。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000022**

- 说明：没有可用的工作站。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000023**

- 说明：无法连接到工作站。服务器已拒绝连接。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000024**

- 说明：工作站正在维护中，无法使用。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000025**

- 说明：由于 ICA 文件中存在 `resourceerror` 错误，无法启动资源。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000026**

- 说明：由于 ICA 文件中存在 `generalapplaunchererror` 错误，无法启动资源。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000027**

- 说明：由于 ICA 文件中存在未知错误，无法启动资源。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000028**

- 说明：由于 ICA 文件中出现重新启动错误，无法启动资源。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000029**

- 说明：由于 ICA 文件中出现还原错误，无法启动资源。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000030**

- 说明：由于 ICA 文件中存在未定义的错误，无法启动资源。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_000031**

- 说明：无法下载 ICA 文件。但是，在定义的地图中找不到错误代码。
- 建议的操作：联系 Citrix 技术支持。



## Linux 启动后

### **SessionManager.Launch.EngineLoadFailed**

- 说明：无法加载 ICA 引擎。
- 建议的操作：联系 Citrix 技术支持。

### **SessionManager.Launch.Failed**

- 说明：启动会话失败。
- 建议的操作：联系 Citrix 技术支持。

### **SessionManager.Launch.ConnectionFailed**

- 说明：引擎在连接之前已终止。
- 建议的操作：查找与启动尝试关联的其他错误。

### **SessionManager.Launch.LogonFailed**

- 说明：会话已断开连接，但未完成登录。
- 建议的操作：此错误表示登录失败，可能包括用户无法手动输入凭据。调查用户尝试登录远程 VDA 的方式。

### **SessionManager.LeaseResolution.Failed**

- 说明：无法尝试启动租约。
- 建议的操作：验证租约是否已同步到客户端计算机，并且仍然有效。用户可以在联机模式下登录 Citrix Workspace 以触发租约（重新）同步。查找网关或 Cloud Connector 组件发送的错误。这些错误可能会表明失败的原因。

### **Transport.Connect.NoCGP\_Fail**

- 说明：连接失败（已禁用 CGP）。
- 建议的操作：调查客户端无法通过 TCP 或 EDT 联系 VDA 的原因。

### **Transport.Connect.FallbackFail**

- 说明：连接失败。已尝试 ICA 回退。
- 建议的操作：调查客户端为何无法通过 TCP 或 EDT 联系网关、连接器或 VDA。

### **Transport.Connect.Fail**

- 说明：Citrix Workspace 应用程序无法通过 TCP、EDT 或 UDP 连接到网关、连接器或 VDA。
- 建议的操作：调查客户端为何无法通过 TCP、EDT 或 UDP 联系网关、连接器或 VDA。客户端与主机之间的防火墙可能不允许使用协议 (UDP/TCP) 或所需的端口。

### **SessionManager.clxmtp.SoftDeny**

- 说明：引擎 CLXMTP 协商失败（软拒绝）。
- 建议的操作：此错误并不表示启动必须失败。它表示引擎无法通过特定的网络路径成功运行。查找网关或 Cloud Connector 组件发送的错误。这些错误可能会表明失败的原因。

### **SessionManager.clxmtp.SoftDeny\_Implicit**

- 说明：引擎 CLXMTP 连接失败（隐式软拒绝）。
- 建议的操作：此错误并不表示启动必须失败。它表示引擎无法通过特定的网络路径成功运行。调查客户端无法联系连接器或网关的原因。由于网络拓扑或防火墙限制，该主机可能无法访问。

## **Linux 预启动**

### **CWA-ICADOWNLOAD\_ERR\_00001**

- 说明：由于 Citrix Workspace 应用程序没有响应，因此无法连接到应用商店。
- 建议的操作：验证 Citrix Workspace 还是 StoreFront 已关闭。此外，请验证 Internet 连接。

### **CWA-ICADOWNLOAD\_ERR\_00002**

- 说明：用户已取消会话启动。
- 建议的操作：过一段时间后重新启动会话。

### **CWA-ICADOWNLOAD\_ERR\_00003**

- 说明：无法连接到应用商店。验证服务器证书是否有效。
- 建议的操作：验证服务器证书是否已安装且处于活动状态。

### **CWA-ICADOWNLOAD\_ERR\_00004**

- 说明：要启动的资源不存在、未启用或者对用户不可见。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_00005**

- 说明：工作站不适用于此请求。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_00006**

- 说明：服务器没有执行请求的活动所需的许可证。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_00007**

- 说明：服务器已拒绝连接到工作站。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_00008**

- 说明：请求的工作站正在维护中，无法使用。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_00009**

- 说明：已达到最大会话数限制。
- 建议的操作：已达到管理员配置的最大会话数限制。重新启动会话。

#### **CWA-ICADOWNLOAD\_ERR\_000010**

- 说明：无法进一步指定的常规错误。
- 建议的操作：联系 Citrix 技术支持。

### **Mac 启动后**

#### 桌面无法启动

- 说明：“桌面名称”桌面无法启动。事务 ID - “事务 ID”。
- 建议的操作：请与管理员联系并提供错误详细信息。

#### 查看器无法启动

- 说明：查看器无法启动。事务 ID - “事务 ID”。
- 建议的操作：请与管理员联系并提供错误详细信息。

#### 桌面无法启动

- 说明：“桌面名称”桌面正在计划维护中。事务 ID - “事务 ID”。
- 建议的操作：请与管理员联系并提供错误详细信息。

#### 应用程序无法启动

- 描述：“应用程序名称”无法启动。
- 建议的操作：请与管理员联系并提供错误详细信息。

#### 应用程序无法启动

- 描述：“应用程序名称”无法启动。事务 ID - “事务 ID”。
- 建议的操作：请与管理员联系并提供错误详细信息。

#### 桌面无法启动

- 说明：“桌面名称”桌面无法启动。
- 建议的操作：请与管理员联系并提供错误详细信息。

#### 桌面无法启动

- 说明：“桌面名称”桌面无法启动。事务 ID - “事务 ID”。
- 建议的操作：请与管理员联系并提供错误详细信息。

#### 查看器无法启动

- 说明：查看器无法打开“应用程序名称”。事务 ID - “事务 ID”。
- 建议的操作：请与管理员联系并提供错误详细信息。

#### 查看器无法启动

- 说明：查看器无法打开桌面“桌面名称”。事务 ID - “事务 ID”。
- 建议的操作：请与管理员联系并提供错误详细信息。

#### 桌面无法启动

- 说明：“桌面名称”桌面正在计划维护中。
- 建议的操作：请与管理员联系并提供错误详细信息。

#### 桌面无法启动

- 说明：“桌面名称”桌面正在计划维护中。事务 ID - “事务 ID”。
- 建议的操作：请与管理员联系并提供错误详细信息。

#### 无法连接到桌面

- 说明：无法访问“桌面名称”桌面。事务 ID - “事务 ID”。请稍后再试。
- 建议的操作：如果问题仍然存在，请与管理员联系并提供错误详细信息。

#### **Mac** 预启动

##### **CWA-ICADOWNLOAD\_ERR\_00001**

- 说明：ICA 文件无效。
- 建议的操作：联系 Citrix 技术支持。

##### **CWA-ICADOWNLOAD\_ERR\_00002**

- 说明：启动请求已超时。
- 建议的操作：验证 Internet 连接或联系 Citrix 技术支持。

##### **CWA-ICADOWNLOAD\_ERR\_00003**

- 说明：服务器没有响应。
- 建议的操作：联系 Citrix 技术支持。

##### **CWA-ICADOWNLOAD\_ERR\_00004**

- 说明：要启动的资源不存在、未启用或对用户不可见。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_00005**

- 说明：服务器无法访问。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_00006**

- 说明：启动查看器时出错。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_00007**

- 说明：无法启动 Apple 打开事件。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_00008**

- 说明：无法访问查看器路径。
- 建议的操作：联系 Citrix 技术支持。

#### **CWA-ICADOWNLOAD\_ERR\_00009**

- 说明：用户取消了身份验证。
- 建议的操作：要求用户重新启动资源。

#### **CWA-ICADOWNLOAD\_ERR\_000010**

- 说明：用户取消了 LSI 窗口。
- 建议的操作：要求用户重新启动资源。

#### **CWA-ICADOWNLOAD\_ERR\_000011**

- 说明：请求的工作站正在维护中，无法使用。
- 建议的操作：请用户在维护完成且工作站可供使用后再试用。

#### **CWA-ICADOWNLOAD\_ERR\_000012**

- 说明：必须更改用户登录凭据。
- 建议的操作：要求用户更改登录凭据。

### **CWA-ICADOWNLOAD\_ERR\_000013**

- 说明：连接资源的会话不再处于活动状态。
- 建议的操作：请用户重试，或者联系您的 Citrix 技术支持以获得进一步帮助。

### **CWA-ICADOWNLOAD\_ERR\_000014**

- 说明：无法下载 ICA 文件。
- 建议的操作：联系 Citrix 技术支持。

## **Windows 启动后**

### **SessionManager.Launch.EngineLoadFailed**

- 说明：用于建立与远程桌面或应用程序的连接的核心组件无法正确加载或初始化。错误消息中可能会提供额外的详细信息。
- 建议的操作：Citrix Workspace 应用程序无法按预期运行。第三方（非 Citrix）虚拟通道 DLL 或其他系统组件可能会导致出现此问题。可能需要收集并提交 CDF 跟踪以确定故障的性质。

### **SessionManager.Launch.ConnectionFailed**

- 说明：此错误为一般故障，表示启动尝试失败。发出的其他错误可能会表明原因。
- 建议的操作：查找与启动尝试关联的其他错误。

### **SessionManager.Launch.LogonFailed**

- 说明：此错误表示已建立与远程桌面或应用程序的连接。但是，会话在未完成 Windows（或其他操作系统）登录的情况下断开连接。
- 建议的操作：此错误表示登录失败，可能包括用户无法手动输入凭据。调查用户尝试登录远程 VDA 的方式。

### **SessionManager.Launch.Cancelled**

- 说明：Citrix 引擎的连接尝试已取消，很可能是由于用户操作而被取消。
- 建议的操作：此错误指示连接未成功建立的原因，但可能指示正确的行为。

### **SessionManager.LeaseResolution.Failed**

- 描述：表示脱机（也称为“基于租赁”）启动失败。出现此故障的原因是，在客户端计算机上找不到资源的有效且必需的租约。此外，网关或 Cloud Connector 拒绝了启动请求，或者启动请求因某种原因无效。
- 建议的操作：验证租约是否已同步到客户端计算机，并且仍然有效。用户可以在联机模式下登录 Citrix Workspace 以触发租约（重新）同步。查找 Gateway 或 Cloud Connector 组件发送的错误。这些错误可能会表明失败的原因。

### **SessionManager.clxmtp.SoftDeny**

- 说明：尝试了租用启动，连接器或网关通知客户端自己无法完成请求的启动。但是，其他连接器或网关也许能够帮助启动。
- 建议的操作：此错误并不表示启动必须失败。它表示引擎无法通过特定的网络路径成功运行。查找网关或 Cloud Connector 组件发送的错误。这些错误可能会表明失败的原因。

### **SessionManager.clxmtp.SoftDeny\_Implicit**

- 说明：尝试启动租约，但无法访问连接器或网关。但是，其他连接器或网关也许能够帮助启动。
- 建议的操作：此错误并不表示启动必须失败。它表示引擎无法通过特定的网络路径成功运行。调查客户端无法联系连接器或网关的原因。由于网络拓扑或防火墙限制，该主机可能无法访问。

### **Transport.Connect.NoCGP\_Fail**

- 说明：Citrix Workspace 应用程序核心（引擎）组件无法通过 ICA 协议（端口 1494）连接到 VDA 主机。如果发送了此事件，则不会尝试通过 CGP 协议连接到网关或 VDA。
- 建议的操作：调查客户端无法通过 TCP 或 EDT 联系 VDA 的原因。

### **Transport.Connect.FallbackFail**

- 说明：Citrix Workspace 应用程序核心（引擎）组件无法通过 ICA 协议（端口 1494）连接到 VDA 主机。出现此故障后，Citrix Workspace 应用程序无法通过 CGP 协议（端口 2598）连接到网关或 VDA。
- 建议的操作：调查客户端为何无法通过 TCP 或 EDT 联系网关、连接器或 VDA。

### **Transport.Connect.Fail**

- 说明：Citrix Workspace 应用程序核心（引擎）组件无法通过 CGP 协议（端口 2598）连接到网关或 VDA。如果触发了此事件，则不会尝试通过 ICA 协议连接到 VDA。
- 建议的操作：调查客户端为何无法通过 TCP 或 EDT 联系网关、连接器或 VDA。



## **Windows 预启动**

### **CWA-ICADOWNLOAD\_ERR\_00001**

- 说明：由于 Citrix Workspace 应用程序没有响应，因此无法连接到应用商店。
- 建议的操作：验证 Citrix Workspace 还是 StoreFront 已关闭。此外，请验证 Internet 连接。

### **CWA-ICADOWNLOAD\_ERR\_00002**

- 说明：用户已取消会话启动。
- 建议的操作：过一段时间后重新启动会话。

### **CWA-ICADOWNLOAD\_ERR\_00003**

- 说明：无法连接到应用商店。验证服务器证书是否有效。
- 建议的操作：联系您的 IT 管理员并提供错误详细信息。

### **CWA-ICADOWNLOAD\_ERR\_00004**

- 说明：要启动的资源不存在、未启用或者对用户不可见。
- 建议的操作：联系您的 IT 管理员并提供错误详细信息。

### **CWA-ICADOWNLOAD\_ERR\_00005**

- 说明：工作站不适用于此请求。
- 建议的操作：联系您的 IT 管理员并提供错误详细信息。

### **CWA-ICADOWNLOAD\_ERR\_00006**

- 说明：服务器没有执行请求的活动所需的许可证。
- 建议的操作：联系您的 IT 管理员并提供错误详细信息。

### **CWA-ICADOWNLOAD\_ERR\_00007**

- 说明：服务器已拒绝连接到工作站。
- 建议的操作：联系您的 IT 管理员并提供错误详细信息。

#### **CWA-ICADOWNLOAD\_ERR\_00008**

- 说明：请求的工作站正在维护中，无法使用。
- 建议的操作：联系您的 IT 管理员并提供错误详细信息。

#### **CWA-ICADOWNLOAD\_ERR\_00009**

- 说明：已达到最大会话数限制。
- 建议的操作：已达到管理员配置的最大会话数限制。重新启动会话。

#### **CWA-ICADOWNLOAD\_ERR\_000010**

- 说明：无法进一步指定的常规错误。
- 建议的操作：联系您的 IT 管理员并提供错误详细信息。

### 工作区

#### **StoreLaunchIcaEndpoint.LaunchFailed**

- 说明：启动时出错。
- 建议的操作：验证您的 Citrix Virtual Apps and Desktops 日志。联系 Citrix 技术支持。

#### **StoreLaunchSessionEndpoint.BadRequest**

- 说明：启动请求的参数无效或为空。
- 建议的操作：联系 Citrix 技术支持。

#### **StoreLaunchSessionEndpoint.FarmUnavailable**

- 说明：没有可供启动的场。
- 建议的操作：验证您的 Citrix Virtual Apps and Desktops 日志。

#### **StoreLaunchSessionEndpoint.Error**

- 说明：启动时出现内部错误。
- 建议的操作：联系 Citrix 技术支持。

### **StoreGetIcaFileEndpoint.BadRequest**

- 说明：请求中没有提供启动票证。
- 建议的操作：联系 Citrix 技术支持。

### **StoreGetIcaFileEndpoint.RetrieveIcaFileForTicketFailed**

- 说明：Workspace 无法检索 ICA 文件。
- 建议的操作：联系 Citrix 技术支持。

### **StoreGetIcaFileEndpoint.Error**

- 说明：Workspace 无法检索 ICA 文件。
- 建议的操作：联系 Citrix 技术支持。

### **WebProxyGetLaunchStatusEndPoint.DSAuthFailure**

- 说明：存在身份验证问题。
- 建议的操作：尝试重新进行身份验证。联系 Citrix 技术支持。

### **WebProxyGetLaunchStatusEndPoint.LaunchFailed**

- 说明：启动应用程序时出现内部错误。
- 建议的操作：联系 Citrix 技术支持。

### **WebProxyGetLaunchStatusEndPoint.ResourceNotFound**

- 说明：启动失败，因为找不到应用程序。
- 建议的操作：验证您的 Citrix Virtual Apps and Desktops 日志以及应用程序配置。

### **WebProxyLaunchIcaEndpoint.DSAuthFailure**

- 说明：存在身份验证问题。
- 建议的操作：尝试重新进行身份验证。联系 Citrix 技术支持。

### **WebProxyLaunchIcaEndpoint.LaunchFailed**

- 说明：启动应用程序时出现内部错误。
- 建议的操作：联系 Citrix 技术支持。

### **WebProxyLaunchIcaEndpoint.ResourceNotFound**

- 说明：启动失败，因为找不到应用程序。
- 建议的操作：验证您的 Citrix Virtual Apps and Desktops 日志以及应用程序配置。

### **WebProxySessionsLaunchIcaEndpoint.SessionNotFound**

- 说明：Workspace 无法重新连接到现有 HDX 会话。您的会话可能会终止。
- 建议的操作：重新启动应用程序。

### **WebProxySessionsLaunchIcaEndpoint.DSAuthFailure**

- 说明：存在身份验证问题。
- 建议的操作：尝试重新进行身份验证。联系 Citrix 技术支持。

### **WebProxySessionsLaunchIcaEndpoint.ReconnectSessionFailed**

- 说明：Workspace 无法重新连接到现有 HDX 会话。您的会话可能会终止。
- 建议的操作：联系 Citrix 技术支持。

### **WebProxySessionsLaunchIcaEndpoint.Error**

- 说明：重新连接到会话时出现内部错误。
- 建议的操作：联系 Citrix 技术支持。

### **WebProxySessionsGetLaunchStatusEndpoint.DSAuthFailure**

- 说明：存在身份验证问题。
- 建议的操作：尝试重新进行身份验证。联系 Citrix 技术支持。

### **WebProxySessionsGetLaunchStatusEndpoint.ReconnectSessionFailed**

- 说明：Workspace 无法重新连接到 HDX 会话。
- 建议的操作：联系 Citrix 技术支持。

### **WebProxySessionsGetLaunchStatusEndpoint.Error**

- 说明：重新连接到会话时出现内部错误。
- 建议的操作：联系 Citrix 技术支持。

### **DetermineGateway.Error**

- 说明：Workspace 无法确定要连接到哪个网关。
- 建议的操作：验证您的网关配置。联系 Citrix 技术支持。

### **ConnectionRoutingProviderLaunch.Error**

- 说明：Workspace 无法确定要连接到哪个网关。
- 建议的操作：验证您的网关配置。联系 Citrix 技术支持。

### **BrokerGetAddressCall.AnonymousPrelaunchNotSupported**

- 说明：Workspace 无法启动应用程序，因为场不支持匿名启动。
- 建议的操作：联系 Citrix 技术支持。

### **BrokerGetAddressCall.LeasingError**

- 说明：Workspace 收到来自 Citrix Virtual Apps and Desktops 代理的错误。
- 建议的操作：验证您的 Citrix Virtual Apps and Desktops 日志。联系 Citrix 技术支持。

### **BrokerGetAddressCall.ServiceConnectionError**

- 说明：Workspace 无法联系场中的任何 Citrix Virtual Apps and Desktops 代理。
- 建议的操作：验证您的 Citrix Virtual Apps and Desktops 日志。联系 Citrix 技术支持。

### **BrokerGetAddressCall.BrokerError**

- 说明：Workspace 收到来自 Citrix Virtual Apps and Desktops 代理的错误。
- 建议的操作：验证您的 Citrix Virtual Apps and Desktops 日志。联系 Citrix 技术支持。

### **BrokerGetAddressCall.LicensingError**

- 说明：由于许可错误，Workspace 无法启动应用程序。
- 建议的操作：验证您的 Citrix Virtual Apps and Desktops 日志。联系 Citrix 技术支持。

### **BrokerGetAddressCall.Error**

- 说明：Workspace 无法从 Citrix Virtual Apps and Desktops 代理中检索 VDA 详细信息。
- 建议的操作：验证您的 Citrix Virtual Apps and Desktops 日志。联系 Citrix 技术支持。

### **GetLaunchReference.NoAccessToken**

- 说明：Workspace 无法成功连接到 VDA。
- 建议的操作：验证您的 Citrix Virtual Apps and Desktops 日志。联系 Citrix 技术支持。

### **GetLaunchReference.BrokerError**

- 说明：Workspace 无法成功连接到 VDA。
- 建议的操作：验证您的 Citrix Virtual Apps and Desktops 日志。联系 Citrix 技术支持。

### **GetLaunchReference.Error**

- 说明：Workspace 无法成功连接到 VDA。
- 建议的操作：验证您的 Citrix Virtual Apps and Desktops 日志。联系 Citrix 技术支持。

### **GenerateIcaFile.InvalidIcaSetting**

- 说明：建立 HDX 连接时出现内部错误。
- 建议的操作：联系 Citrix 技术支持。

### **StoreIcaFileAndGetTicket.StoreIcaFileAndCreateTicketFailed**

- 说明：建立 HDX 连接时出现内部错误。
- 建议的操作：联系 Citrix 技术支持。

### **StoreIcaFileAndGetTicket.Error**

- 说明：建立 HDX 连接时出现内部错误。
- 建议的操作：联系 Citrix 技术支持。

### **GetFasVdaLogonTicket.Error**

- 说明：建立 HDX 连接时出现内部错误。
- 建议的操作：联系 Citrix 技术支持。

### **GenerateSTATicket.Error**

- 说明：建立 HDX 连接时出现内部错误。
- 建议的操作：联系 Citrix 技术支持。

### **GetVdaAddress.Error**

- 说明：建立 HDX 连接时出现内部错误。
- 建议的操作：联系 Citrix 技术支持。

### **GetTicket.NoAccessToken**

- 说明：建立 HDX 连接时出现内部错误。
- 建议的操作：联系 Citrix 技术支持。

### **GetTicket.BrokerError**

- 说明：Citrix Virtual Apps and Desktops 代理无法启动 HDX 会话。
- 建议的操作：验证错误消息中的 ID 并验证 Citrix Virtual Apps and Desktops 日志。

### **GetTicket.ServiceConnectionError**

- 说明：Workspace 无法联系 Citrix Virtual Apps and Desktops 代理。
- 建议的操作：联系 Citrix 技术支持。

### **GetTicket.Error**

- 说明：建立 HDX 连接时出现内部错误。
- 建议的操作：联系 Citrix 技术支持。

### **GetNetscalerConfigurationByCustomer.Error**

- 说明：建立 HDX 连接时出现内部错误。
- 建议的操作：联系 Citrix 技术支持。

### **DiscoverMPSServerCapabilities.Error**

- 说明：向 Citrix Virtual Apps and Desktops 代理发出请求时出现问题。
- 建议的操作：验证您的 Citrix Virtual Apps and Desktops 日志。联系 Citrix 技术支持。

### **GetResourceLocationNetScalerConfig.Error**

- 说明：建立 HDX 连接时出现内部错误。
- 建议的操作：联系 Citrix 技术支持。

### **GetCustomerResourceLocations.Error**

- 说明：建立 HDX 连接时出现内部错误。
- 建议的操作：联系 Citrix 技术支持。

### **GetResourceLocationFromResourceProvider.Error**

- 说明：建立 HDX 连接时出现内部错误。
- 建议的操作：联系 Citrix 技术支持。

### **GetNetScalerGatewayInfo.Error**

- 说明：建立 HDX 连接时出现内部错误。
- 建议的操作：联系 Citrix 技术支持。

### **GetCustomerEntitlements.Error**

- 说明：建立 HDX 连接时出现内部错误。
- 建议的操作：联系 Citrix 技术支持。

### **GetResourceLocationForServerFeed.Error**

- 说明：建立 HDX 连接时出现内部错误。
- 建议的操作：联系 Citrix 技术支持。

### **GetResourceInformation.Error**

- 说明：建立 HDX 连接时出现内部错误。
- 建议的操作：联系 Citrix 技术支持。

## **Citrix Gateway 即服务**

### **CGS-ICASN\_ERR\_00001**

- 说明：由于请求解析错误，应用程序启动失败。
- 建议的操作：联系 Citrix 技术支持。



#### **CGS-ICASN\_ERR\_00002**

- 说明：无法验证身份验证票据。
- 建议的操作：联系 Citrix 技术支持。

#### **CGS-ICASN\_ERR\_00003**

- 说明：无法验证身份验证票据。
- 建议的操作：联系 Citrix 技术支持。

#### **CGS-ICASN\_ERR\_00004**

- 说明：无法验证身份验证票据。
- 建议的操作：联系 Citrix 技术支持。

#### **CGS-ICASN\_ERR\_00005**

- 说明：无法建立与连接器的连接。
- 建议的操作：验证连接器运行状况。如果问题仍然存在，请联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00006**

- 说明：对连接器的连接请求超时。
- 建议的操作：验证连接器运行状况。验证是否有任何代理设置阻止连接器/VDA 与 NGS 之间的流量。验证 VDA 与连接器之间的连接性。如果问题仍然存在，请联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00007**

- 说明：Citrix Workspace 应用程序已关闭连接。
- 建议的操作：验证客户端网络连接是否稳定。如果问题仍然存在，请联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00008**

- 说明：后端关闭了连接。
- 建议的操作：验证连接器运行状况。验证从连接器/VDA 到公共网络 (NGS) 的网络稳定性。如果问题仍然存在，请联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00009**

- 说明：VDA 与 NGS 的连接建立 (Rendezvous) 失败。
- 建议的操作：验证连接器运行状况。VDA 必须能够联系 NGS 服务。验证 VDA 与连接器之间的连接性。如果问题仍然存在，请联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00010**

- 说明：EDT 到 TCP 回退。验证 EDT 的必备条件。
- 建议的操作：必须启用 Rendezvous，并且 VDA 必须能够通过 UDP 访问 NGS 服务。如果问题仍然存在，请联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00011**

- 说明：NGS 内部服务出现故障。
- 建议的操作：联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00012**

- 说明：NGS 内部服务出现故障。
- 建议的操作：联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00013**

- 说明：GCT 验证失败。
- 建议的操作：联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00014**

- 说明：GCT 验证失败。
- 建议的操作：联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00015**

- 说明：NGS 内部服务出现故障。
- 建议的操作：联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00016**

- 说明：NGS 内部服务出现故障。
- 建议的操作：联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00017**

- 说明：NGS 内部服务出现故障。
- 建议的操作：联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00018**

- 说明：无法验证身份验证票据。
- 建议的操作：联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00019**

- 说明：无法验证身份验证票据。
- 建议的操作：联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00020**

- 说明：CGS 内部许可中出现错误。
- 建议的操作：联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00021**

- 说明：由于禁用了功能标志，Rendezvous v2 回退。
- 建议的操作：联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00022**

- 说明：NGS 内部服务出现故障。
- 建议的操作：联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00023**

- 说明：CLXMTP 交换超时。
- 建议的操作：验证连接器运行状况良好，并且可以访问 NGS 服务。如果问题仍然存在，请联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00024**

- 说明：CLXMTP VSR 验证失败。
- 建议的操作：联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00025**

- 说明：CLXMTP VSR 验证失败。
- 建议的操作：联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00026**

- 说明：连接器在 CLXMTP 中不可用。
- 建议的操作：验证资源位置的连接器是否处于正常运行状态。如果问题仍然存在，请联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00027**

- 说明：CLXMTP 在最长试用期后重定向到连接器失败。
- 建议的操作：验证资源位置的连接器是否处于正常运行状态。验证 [Citrix ClxMtp Service](#) 服务是否在所有连接器中运行。联系 Citrix 技术支持。

#### **CGS\_ICASN\_ERR\_00028**

- 说明：无法与控制器通信。
- 建议的操作：联系 Citrix 技术支持。

#### 成功：**CGS\_ICASN\_SUCCESS\_00001**

- 说明：已收到会话启动请求。
- 建议的操作：不适用

#### 成功：**CGS\_ICASN\_SUCCESS\_00002**

- 说明：会话启动请求已完成。
- 建议的操作：不适用

## **XAXD 代理**

### **XDPXY\_INF\_00001**

- 说明：Broker 向 VDA 发送请求以准备接收传入连接。
- 建议的操作：不适用

### **XDPXY\_INF\_00002**

- 说明：VDA 确认 Broker 的连接请求。
- 建议的操作：不适用

### **XDPXY\_ERR\_00001**

- 说明：无法与 VDA 通信。
- 建议的操作：检查连接器的运行状况。有关详细信息，请参阅 [Citrix Cloud Connector](#) 和 [CTX224133](#)。
  - 在 VDA 上重新启动 Citrix Delivery Agent 服务或重新启动 VDA。
  - 如果您在 Connector 与 Broker 之间有 Web 代理，请确保其配置正确。
  - 如果问题仍然存在，请联系 Citrix 技术支持。

### **XDPXY\_ERR\_00002**

- 说明：XaxdProxy 在等待来自 VDA 的响应时超时。
- 建议的操作：检查连接器的运行状况。有关详细信息，请参阅 [Citrix Cloud Connector](#) 和 [CTX224133](#)。
  - 在 VDA 上重新启动 Citrix Delivery Agent 服务或重新启动 VDA。
  - 如果您在 Connector 与 Broker 之间有 Web 代理，请确保其配置正确。
  - 如果问题仍然存在，请联系 Citrix 技术支持。

### **XDPXY\_ERR\_00003**

- 说明：尝试发出请求时遇到 WCF 错误或异常。
- 建议的操作：检查连接器的运行状况。有关详细信息，请参阅 [Citrix Cloud Connector](#) 和 [CTX224133](#)。
  - 在 VDA 上重新启动 Citrix Delivery Agent 服务或重新启动 VDA。
  - 如果您在 Connector 与 Broker 之间有 Web 代理，请确保其配置正确。
  - 如果问题仍然存在，请联系 Citrix 技术支持。

### **XDPXY\_INF\_00003**

- 说明：请求验证堆栈是否调用传入 ICA 或 RDP 连接。
- 建议的操作：不适用

### **XDPXY\_INF\_00004**

- 说明：验证是否已建立传入 ICA 或 RDP 连接。
- 建议的操作：不适用

### **XDPXY\_ERR\_00001**

- 说明：无法与 VDA 代理通信。
- 建议的操作：检查连接器的运行状况。有关详细信息，请参阅 [Citrix Cloud Connector](#) 和 [CTX224133](#)。
  - 在 VDA 上重新启动 Citrix Delivery Agent 服务或重新启动 VDA。
  - 如果您在 Connector 与 Broker 之间有 Web 代理，请确保其配置正确。
  - 如果问题仍然存在，请联系 Citrix 技术支持。

### **XDPXY\_ERR\_00002**

- 说明：XaxdProxy 在等待来自 VDA 代理的响应时超时。
- 建议的操作：检查连接器的运行状况。有关详细信息，请参阅 [Citrix Cloud Connector](#) 和 [CTX224133](#)。
  - 在 VDA 上重新启动 Citrix Delivery Agent 服务或重新启动 VDA。
  - 如果您在 Connector 与 Broker 之间有 Web 代理，请确保其配置正确。
  - 如果问题仍然存在，请联系 Citrix 技术支持。

### **XDPXY\_ERR\_00003**

- 说明：尝试发出请求时遇到异常。
- 建议的操作：检查连接器的运行状况。有关详细信息，请参阅 [Citrix Cloud Connector](#) 和 [CTX224133](#)。
  - 在 VDA 上重新启动 Citrix Delivery Agent 服务或重新启动 VDA。
  - 如果您在 Connector 与 Broker 之间有 Web 代理，请确保其配置正确。
  - 如果问题仍然存在，请联系 Citrix 技术支持。

### **XDPXY\_INF\_00005**

- 说明：已请求直接发送到 VDA 的 HDX 会话流量。
- 建议的操作：不适用

#### **XDPXY\_INF\_00006**

- 说明：VDA 为 HDX 会话流量建立与 Citrix Cloud 控制平面的直接连接。
- 建议的操作：不适用

#### **XDPXY\_INF\_00007**

- 说明：客户端向本地 StoreFront 发送资源的连接请求。
- 建议的操作：不适用

#### **XDPXY\_INF\_00008**

- 说明：本地 StoreFront 接受来自客户端的资源连接请求。
- 建议的操作：不适用

#### **XDPXY\_ERR\_00004**

- 说明：XaxdProxy 在尝试连接时收到 HTTP 错误响应。
- 建议的操作：检查连接器的运行状况。有关详细信息，请参阅 [Citrix Cloud Connector](#) 和 [CTX224133](#)。
  - 验证从连接器到公共网络的网络稳定性。
  - 如果您在 Connector 与 Broker 之间有 Web 代理，请确保其配置正确。
  - 如果问题仍然存在，请联系 Citrix 技术支持。

#### **XDPXY\_ERR\_00006**

- 说明：XML 请求的格式无效。
- 建议的操作：联系 Citrix 技术支持

#### **XDPXY\_ERR\_00007**

- 说明：XML 请求包含无效的凭证标头和/或格式。
- 建议的操作：注销，重新登录，然后重试操作。如果问题仍然存在，请联系 Citrix 技术支持

#### **XDPXY\_INF\_00011**

- 说明：用户通过 WSA 请求服务连续性启动。
- 建议的操作：不适用

### **XDPXY\_INF\_00012**

- 说明：用户通过 WSA 请求服务连续性启动。
- 建议的操作：不适用

### **XDPXY\_ERR\_00004**

- 说明：XaxdProxy 在尝试连接时遇到 HTTP 错误。
- 建议的操作：检查连接器的运行状况。有关详细信息，请参阅 [Citrix Cloud Connector](#) 和 [CTX224133](#)。
  - 如果您在 Connector 与 Broker 之间有 Web 代理，请确保其配置正确。
  - 如果问题仍然存在，请联系 Citrix 技术支持。

### **XDPXY\_ERR\_00008**

- 说明：服务连续性启动失败，因为 XaxdProxy 超时正在等待响应。
- 建议的操作：检查连接器的运行状况。有关详细信息，请参阅 [Citrix Cloud Connector](#) 和 [CTX224133](#)。
  - 如果您在 Connector 与 Broker 之间有 Web 代理，请确保其配置正确。
  - 如果问题仍然存在，请联系 Citrix 技术支持。

### **XDPXY\_ERR\_00009**

- 说明：由于租约被阻止和/或撤销，服务连续性启动失败。
- 建议的操作：联系您的 Citrix Cloud 管理员并提供错误详细信息。有关详细信息，请参阅[服务连续性](#)文档。
  - 如果问题仍然存在，请联系 Citrix 技术支持。

## **适用于 Citrix Service Provider 的 Citrix DaaS**

February 9, 2024

本文介绍 **Citrix Service Provider (CSP)** 如何在 Citrix Cloud 中为租户客户设置 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）。有关面向 Citrix 合作伙伴的功能的概述，请参阅[面向合作伙伴的 Citrix Cloud](#)。

### **要求**

- 您是 [Citrix 服务提供商合作伙伴](#)。
- 您有一个 Citrix Cloud 帐户。
- 您已订阅 Citrix DaaS。



## 限制和已知问题

### 限制

- 租户名称更改最多需要 24 小时才能应用到所有界面。
- 创建租户时，电子邮件地址必须是唯一的。
- 在管理 > 完整配置中按作用域进行过滤（类似于监视）不可用。要查看附加到作用域的资源，请在左侧窗格中选择管理员。在作用域选项卡上，选择作用域，然后选择“操作”窗格中的编辑作用域。

### 已知问题

- 将作用域分配给资源后，您将无法使用管理控制台将其删除或取消分配。这些任务仅通过 PowerShell 支持。
- 管理 > 完整配置不强制执行作用域。您负责在创建计算机目录、交付组和应用程序组时选择适当的作用域。
- 创建超过 15 个作用域时（自动创建和自定义），管理员 **【Identity and Access Management（身份识别和访问管理）> Administrators（管理员）】** 的 Citrix Cloud 自定义访问信息将无法正确显示。解决方法：将作用域限制为 15 个或更少。

## 添加客户

1. 使用您的 CSP 凭据登录 Citrix Cloud。在左上角的菜单中选择客户。
2. 在“Customer Dashboard”（客户控制板）中，选择 **Invite**（邀请）或 **Add**（添加）。提供请求的信息。
3. 如果客户没有 Citrix Cloud 帐户，添加客户将创建客户帐户。添加客户还会自动将您添加为该客户帐户的完全访问权限管理员。
4. 如果客户拥有 Citrix Cloud 帐户：
  - a) 将显示 Citrix Cloud URL，您将其复制并发送给客户。有关此过程的详细信息，[请参阅邀请客户进行连接](#)。
  - b) 客户必须将您添加为其帐户的完全访问权限管理员。请参阅[向 Citrix Cloud 帐户中添加管理员](#)。

您可以稍后添加更多管理员，并控制其可以在管理和监视控制台上看到哪些客户。

## 为客户添加 Citrix DaaS

1. 使用您的 CSP 凭据登录 Citrix Cloud。在左上角的菜单中选择客户。
2. 在“Customer Dashboard”（客户控制板）中，在客户的省略号菜单中，选择 **Add Service**（添加服务）。
3. 在 **Select a service to add**（选择要添加的服务）中，选择 **Virtual Apps and Desktops**。
4. 选择继续。

完成此过程后，客户将加入 Citrix DaaS 订阅。

加入完成后，系统会在 Citrix DaaS 中自动创建新的客户作用域。作用域在管理 > 完整配置显示屏中可见。此作用域是该客户唯一的作用域。您可以[重命名作用域](#)，但不能将其删除。

使用此作用域为其他管理员定制访问权限。例如，假设您有 10 个客户和两个管理员。使用唯一的作用域，您可以将一名管理员的访问权限限制到仅限其中三个客户。另一个管理员可以访问这三个客户中的一个，外加两个其他客户。有关详细信息，请参阅[控制管理员对客户的访问](#)。

### 设置资源位置

资源位置中包含为客户交付应用程序和桌面的计算机以及 Citrix Cloud Connector 等基础结构组件。有关详细信息，请参阅[连接到 Citrix Cloud](#)。

### 设置目录和组以交付应用程序和桌面

#### 注意：

要管理租户客户的 DAA，必须切换到 CSP 客户的帐户。为此，请在右上角菜单中单击客户名称，然后单击“更改客户”。

目录是一组相同的虚拟机。创建目录时，将使用映像（与其他设置一起）作为创建计算机的模板。有关详细信息，请参阅[创建计算机目录](#)。

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或桌面。有关详细信息，请参阅[创建交付组](#)。

可以借助应用程序组管理应用程序的集合。可为在不同交付组之间共享的应用程序或由交付组中的部分用户使用的应用程序创建应用程序组。有关详细信息，请参阅[创建应用程序组](#)。

配置组时，请确保：

- 交付组的作用域是计算机目录作用域的一个子集。例如，假设目录的作用域为 A 和 B。交付组的作用域可以是 A 或 B，也可以是 A 和 B。
- 应用程序组的作用域是交付组的作用域的一个子集。例如，假设与应用程序组关联的交付组具有作用域 A 和 B。应用程序组的作用域可以是 A 或 B，也可以是 A 和 B。

### 联盟域

通过联盟域，客户用户可以使用附加到您的资源位置的域中的凭据登录到其工作区。这允许您为客户提供专用工作区，客户用户可以使用自定义 Workspace URL（例如，customer.cloud.com）访问这些工作区，而资源位置仍在您的 Citrix Cloud 帐户中。您可以随客户可以使用您的 CSP Workspace URL（例如 cspspartner.cloud.com）访问的共享工作区一起提供专用工作区。

要使客户能够访问其专用工作区，可以将其添加到您管理的相应域中。通过 [Workspace 配置](#) 配置工作区后，客户的用户可以登录其工作区并访问您已提供的应用程序和桌面。

#### 将客户添加到域

1. 使用您的 CSP 凭据登录 Citrix Cloud。在左上角的菜单中选择客户。
2. 在“Customer Dashboard”（客户控制板）中，选择左上角菜单中的 **Identity and Access Management**（身份识别和访问管理）。
3. 在 **Domains**（域）选项卡上，在域的省略号菜单中选择 **Manage Federated Domain**（管理联盟域）。
4. 在 **Manage Federated Domain**（管理联盟域）卡上的 **Available customers**（可用客户）列中，选择要添加到域的客户。选择客户名称旁边的加号。所选客户现在显示在 **Federated customers**（联盟客户）列中。重复操作以添加其他客户。完成后，选择应用。

#### 从域中删除客户

从您管理的域中删除客户时，客户的用户将无法再使用您的域中的凭据访问其工作区。

1. 在 Citrix Cloud 菜单中，选择 **Identity and Access Management**（身份识别和访问管理），然后选择 **Domains**（域）。
2. 找到要管理的域，然后选择省略号按钮。选择 **Manage Federated Domain**（管理联盟域）。
3. 从联盟客户列表中，找到或搜索要删除的客户，然后选择 X 按钮。选择 **Remove all**（全部删除）以从域中删除列表中的所有客户。所选客户将移动到可用客户列表。
4. 选择应用。
5. 查看您选择的客户，然后选择 **Remove Customers**（删除客户）。

#### 控制管理员对客户的访问

可以使用为客户添加 Citrix DaaS 时创建的唯一作用域来控制管理员对客户的访问。可以在添加管理员时或以后配置访问权限。

要了解有关使用 Citrix DaaS 中的角色和作用域限制访问的信息，请参阅[委派管理](#)。

#### 添加具有受限访问权限的管理员

1. 使用您的 CSP 凭据登录 Citrix Cloud。在左上角的菜单中选择客户。
2. 在“Customer Dashboard”（客户控制板）中，选择左上角菜单中的 **Identity and Access Management**（身份识别和访问管理）。
3. 在 **Administrators**（管理员）选项卡上，选择 **Add Administrators From**（添加管理员的来源），然后选择 **Citrix Identity**（Citrix 身份）。
4. 键入您以管理员身份添加的人员的电子邮件地址，然后选择 **Invite**（邀请）。
5. 为管理员配置适当的访问权限。除非您希望管理员拥有对 Citrix Cloud 和所有订阅的服务的管理控制权，否则 Citrix 建议选择 **Custom access**（自定义访问权限）。

6. 选择 **Custom access**（自定义访问权限）后，根据需要为 Citrix DaaS 选择一个或多个角色和作用域对。请务必仅启用包含为客户创建的唯一作用域的条目。
7. 选择角色和作用域对后，选择 **Send Invite**（发送邀请）。

当管理员接受邀请时，他们将具有您分配的访问权限。

#### 编辑管理员的委派管理权限

1. 使用您的 CSP 凭据登录 Citrix Cloud。在左上角的菜单中选择客户。
2. 在“Customer Dashboard”（客户控制板）中，选择左上角菜单中的 **Identity and Access Management**（身份识别和访问管理）。
3. 在 **Administrators**（管理员）选项卡上，从管理员的省略号菜单中选择 **Edit Access**（编辑访问权限）。
4. 根据需要选择并清除 Citrix DaaS 的角色和作用域对。请务必仅启用包含为客户创建的唯一作用域的条目。
5. 选择保存。

#### 查看客户管理员及其分配的角色和作用域

1. 使用您的 CSP 凭据登录 Citrix Cloud。在左上角的菜单中选择客户。
2. 在客户控制面板中，选择左上角菜单中的“我的服务”>“**DaaS**”。
3. 在 Citrix DaaS 中，选择管理 > 完整配置。
4. 在左窗格中选择管理员。

信息可在三个选项卡上找到：

- **Administrators**（管理员）选项卡列出了已创建的管理员及其角色和作用域。
- **Roles**（角色）选项卡列出了所有角色。要查看角色详细信息，请在中间窗格中选择角色。该窗格的下面的部分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。
- **Scopes**（作用域）选项卡列出了所有作用域，包括为 Citrix Partner 的客户生成的作用域。

#### 配置工作区

客户拥有各自的具有唯一 [customer.cloud.com](https://customer.cloud.com) URL 的工作区。此工作区是客户的用户访问其已发布的应用程序和桌面的位置。

Workspace URL 显示在两个位置：

- 在“Customer dashboard”（客户控制板）中，从左上角菜单的菜单中选择 **Workspace Configuration**（工作区配置）。
- 在 Citrix DaaS 欢迎页面（概述选项卡）中，工作区 URL 将显示在页面底部。

您可以更改对工作区的访问和身份验证。还可以自定义工作区外观和首选项。有关详细信息，请参阅以下文章：

- [配置工作区](#)
- [安全的工作区](#)

## 监视客户的服务

CSP 环境中的 **Monitor**（监视）控制板基本上与非 CSP 环境相同。有关详细信息，请参阅[监视](#)。

默认情况下，**Monitor**（监视）控制板显示与所有客户有关的信息。要显示与一个客户有关的信息，请使用 **Select Customer**（选择客户）。

请记住，查看客户的监视显示内容功能由管理员的已配置的访问权限控制。访问权限必须包含一个包括客户唯一的作用域的角色和作用域对。

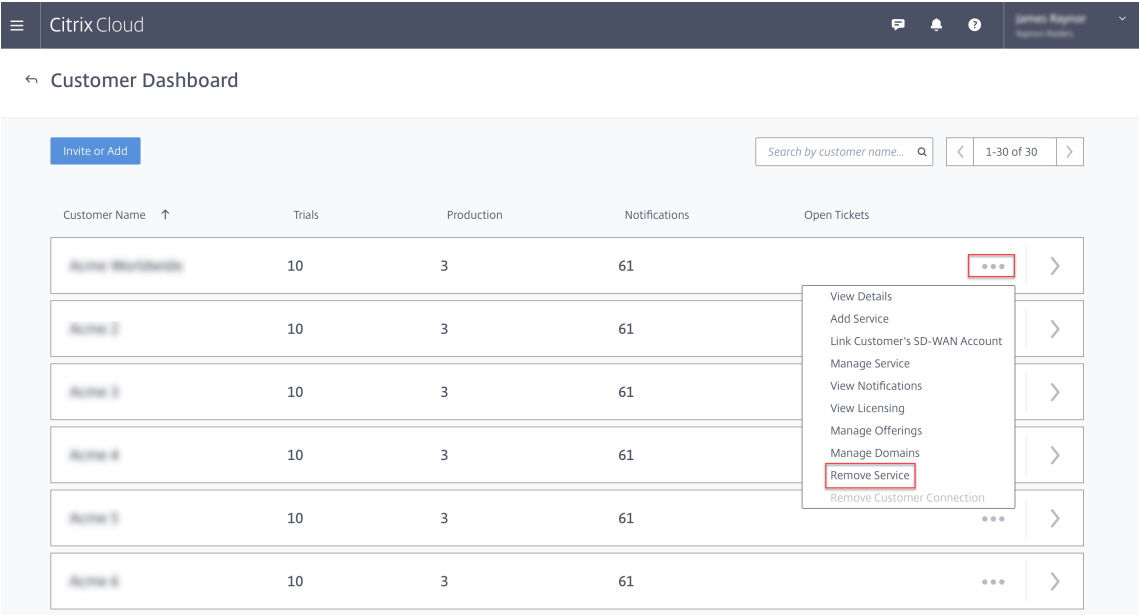
如果使用内置角色配置访问权限：内置角色控制管理员是否可以看到 **Manage**（管理）和 **Monitor**（监视）显示内容。如果仅选择不包括 **Monitor**（监视）选项卡可见性的角色和客户作用域对，该管理员将看不到任何选定客户的 **Monitor**（监视）选项卡。例如，如果您仅授予管理员 **Read Only Administrator,customerABC**（只读管理员，客户 ABC）访问权限，该管理员将看不到客户 ABC 的 **Monitor**（监视）选项卡，因为只读管理员无法访问监视显示内容。

## 删除服务

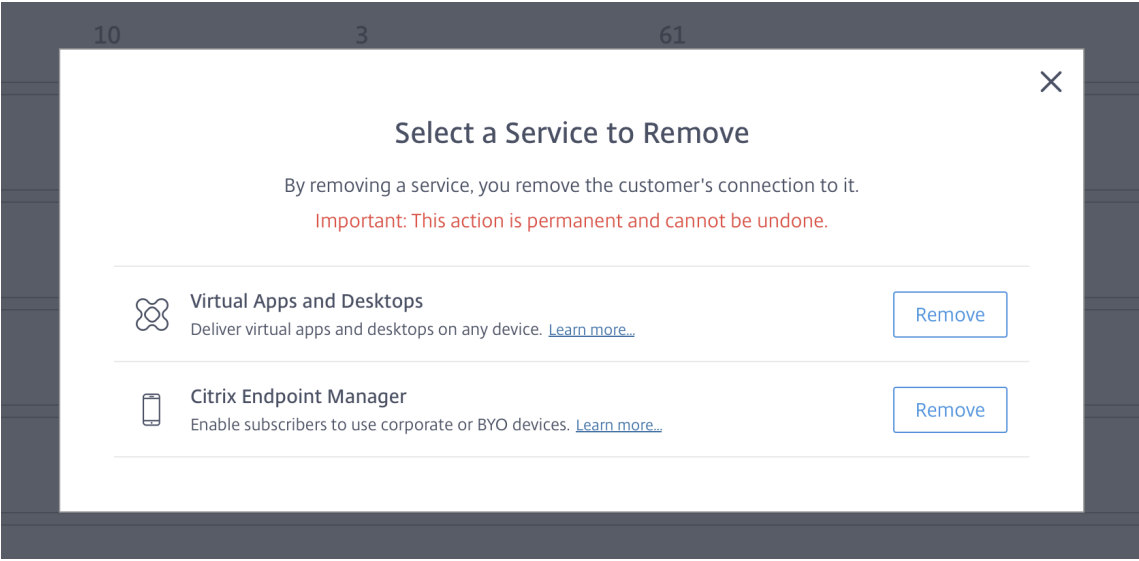
### 必备条件

- 确保您的客户范围未链接到任何 Citrix DaaS 对象。如果这些作用域已链接，则无法删除该服务。要取消作用域的连接，请转到 **Citrix Studio > 管理员 > 作用域**并编辑作用域。
- 要了解客户作用域并对其进行管理，请参阅[创建和管理作用域](#)。

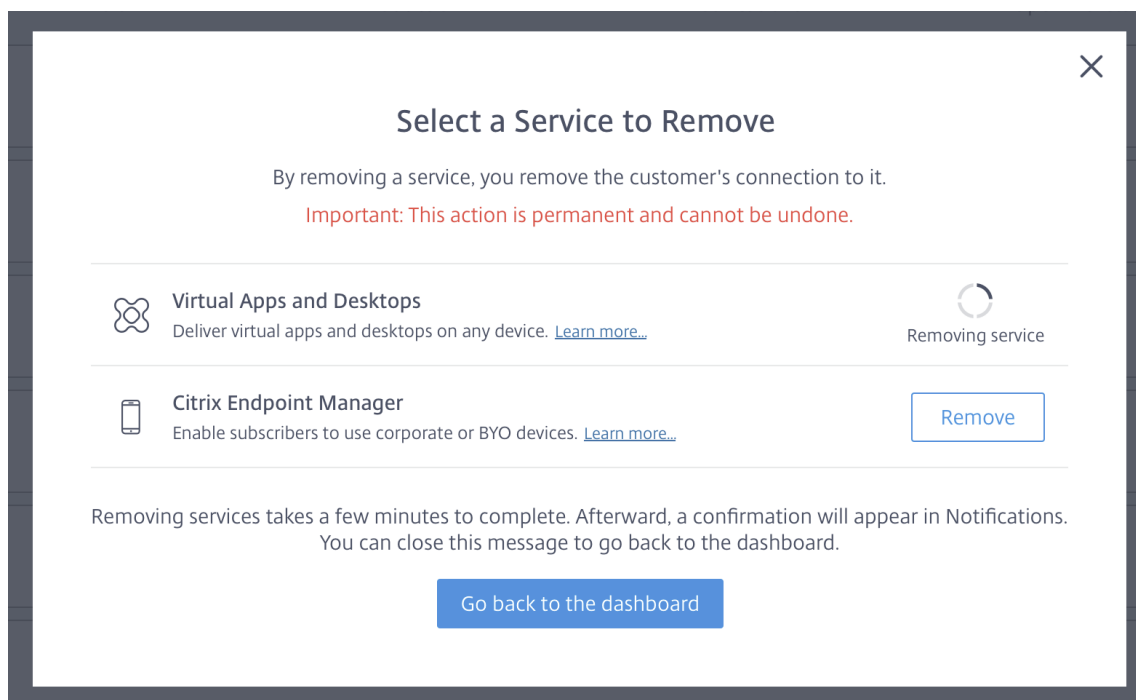
1. 使用您的 Citrix Service Provider 凭据登录 Citrix Cloud。
2. 在“客户”控制板上，单击要从中删除服务的客户的省略号菜单（⋮），然后选择删除服务。



此时将显示要删除的服务页面。



3. 单击删除以删除该服务。



## Citrix Gateway 服务

November 3, 2022

Citrix Gateway 为用户提供了对 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）应用程序的安全访问。

通过 Citrix Gateway 服务，可以安全地远程访问这些应用程序，而不需要在 DMZ 中部署 Citrix Gateway 或者重新配置您的防火墙。使用 Citrix Gateway 的基础结构开销将转移至 Citrix Cloud。

有关 Citrix Gateway 服务的详细信息，请参阅[产品文档](#)。该内容包括如何[启用 Citrix Gateway 服务](#)以及您正在使用的版本的[已知问题](#)。

Citrix ADC 是应用程序交付控制器，用于分析应用程序特定的流量，以智能地分发和优化 Web 应用程序第 4 层 - 第 7 层 (L4-L7) 的网络流量并确保其安全。Citrix ADC VPX 虚拟设备可以托管在各种虚拟化和云平台上。有关详细信息，请参阅[部署 Citrix ADC VPX 实例](#)。

## SDK 和 API

December 18, 2023

## Citrix DaaS 远程 PowerShell SDK

远程 PowerShell SDK 将自动执行复杂的重复性任务。它提供在不使用管理用户界面的情况下用来设置和管理 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）环境的机制。

- [Citrix DaaS SDK](#) 中提供了有关 cmdlet 的详细信息。
- 支持和限制中列出了受支持的模块。该部分内容还列出了此 SDK 中禁用的 cmdlet。
- 远程 PowerShell SDK 可在 [Citrix Web 站点](#) 上下载。

本产品支持 PowerShell 版本 3 至 5。

此 **SDK** 与用于客户管理的部署的 **SDK** 有何不同

在由客户管理员安装和管理的 Citrix Virtual Apps and Desktops 部署中，这些管理员在一个常见域结构中包含 VDA 和 Delivery Controller 的站点中运行 cmdlet 和脚本。相反，Citrix DaaS 分别将 VDA 和 Controller 拆分到某个资源位置和控制平面中。这种拆分意味着最初的 Citrix Virtual Apps and Desktops Virtual Apps and Desktops PowerShell SDK 无法在 Citrix DaaS 环境中运行。它不能跨越资源位置的安全边界连接到控制平面。

解决方案是使用 Citrix DaaS 远程 PowerShell SDK。在资源位置中运行时，远程 PowerShell SDK 会像在本地一样访问控制平面。该 SDK 提供的功能与单个 Citrix Virtual Apps and Desktops 站点相同。仅存在最低的非可见通信层，功能得以增强，可在单个本地站点或云环境中使用。cmdlet 相同，并且大多数现有脚本的工作方式保持不变。

`Get-XdAuthentication` cmdlet 提供从安全的资源位置跨越到控制平面边界的授权。默认情况下，`Get-XdAuthentication` 提示用户输入 CAS 凭据，并且必须在每个 PowerShell 会话中提供一次。或者，用户可以使用在 Citrix Cloud 控制台中创建的 API-Access 安全客户端定义身份验证配置文件。在这两种情况下，我们都会在后续的 PowerShell SDK 调用中持续使用安全信息。如果未明确运行此 cmdlet，它将被第一个 PowerShell SDK cmdlet 调用。

必备条件

要使用 Citrix DaaS Remote PowerShell SDK，请将以下 URL 列入白名单：

商用

- <https://accounts.cloud.com>
- [https://\[service\].citrixworkspacesapi.net/\[customerid\]](https://[service].citrixworkspacesapi.net/[customerid])
- [https://\[customerid\].xendesktop.net:443](https://[customerid].xendesktop.net:443)

日本

- <https://accounts.citrixcloud.jp>
- [https://\[service\].citrixworkspacesapi.jp/\[customerid\]](https://[service].citrixworkspacesapi.jp/[customerid])
- [https://\[customerid\].apps.citrixworkspacesapi.jp:443](https://[customerid].apps.citrixworkspacesapi.jp:443)



## 政府

- <https://accounts.cloud.us>
- [https://\[service\].citrixworkspacesapi.us/\[customerid\]](https://[service].citrixworkspacesapi.us/[customerid])
- [https://\[customerid\].xendesktop.us:443](https://[customerid].xendesktop.us:443)

## 安装和使用远程 PowerShell SDK

### 要求和注意事项：

#### 注意：

请勿在 Citrix Cloud Connector 计算机上安装远程 PowerShell SDK。它可以安装在同一资源位置内的任何加入了域的计算机上。

Citrix 不支持在 Cloud Connector 上运行此 SDK 的 cmdlet。SDK 的操作不涉及 Cloud Connector。

如果您还有 Citrix Virtual Apps and Desktops 部署（Citrix DaaS 部署除外），请不要在本地 Delivery Controller 计算机上安装远程 PowerShell SDK。

- 安装 **Microsoft Edge WebView2**。
- 确保 PowerShell 3.0、4.0 或 5.0 在计算机上可用。
- SDK 安装程序会下载并安装 .NET Framework 4.8（或更高的受支持版本，如果未安装）。
- 如果计算机已经安装了 Citrix Virtual Apps and Desktops SDK，请在安装远程 PowerShell SDK 之前删除该 SDK（从 Windows 的“程序和功能”中）。
- 对于自动化环境，请使用 `-quiet` 参数在没有用户输入的情况下安装 SDK。

要安装远程 PowerShell SDK，请执行以下操作：

1. 从[下载页面](#)下载 Citrix Virtual Apps and Desktops 远程 PowerShell SDK。
2. 安装并运行 SDK。

系统将在 `%TEMP%\CitrixLogs\CitrixPoshSdk` 中创建安装日志。日志可以帮助解决安装问题。

在该资源位置中加入了域的计算机上运行 SDK：

- 打开 PowerShell 命令提示符。不需要以管理员身份运行。
- 如果要使用管理单元（而非模块），请使用 `Add-PSSnapin`（或 `asnp`）cmdlet 添加管理单元。
- 可以使用 `Get-XdAuthentication` cmdlet 显式进行身份验证。或者，运行您的第一个 Remote PowerShell SDK 命令，该命令会提示您进行与相同的身份 `Get-XdAuthentication` 验证。如果您使用的是代理，则必须向代理进行身份验证才能使用 `Get-XdAuthentication` cmdlet。有关更多信息，请参阅 将远程 PowerShell SDK 与代理一起使用。
- 要跳过身份验证提示，可以通过在 Citrix Cloud 控制台中创建的安全客户端使用 `Set-XdCredentials` cmdlet 来创建默认的身份验证配置文件。
- 继续运行 PowerShell SDK cmdlet 或 PowerShell SDK 自动化脚本。请参见示例。

要卸载远程 PowerShell SDK，请从用于删除或更改程序的 Windows 功能中选择 **Citrix Virtual Apps and Desktops Remote PowerShell SDK** (Citrix Virtual Apps and Desktops 远程 PowerShell SDK)。单击鼠标右键并选择卸载。按照对话框进行操作。

将远程 **PowerShell SDK** 与代理一起使用 如果您使用的是代理，则可能无法使用 cmdlet，因为该代理会阻止 `Get-XdAuthentication` cmdlet 发出的 HTTP 请求。

有两种方法可以向代理进行身份验证。您可以使用 `ProxyUseDefault` 参数或 `ProxyUsername` 和 `ProxyPassword` 参数：

- `ProxyUseDefault` 参数允许使用默认代理凭据对代理进行身份验证。例如：

```
1 Get-XdAuthentication -ProxyUseDefault
2 <!--NeedCopy-->
```

- `ProxyUsername` 和 `ProxyPassword` 参数允许在 PowerShell 会话中对代理进行身份验证。例如：

```
1 $secureString = ConvertTo-SecureString -String "password" -
  AsPlainText -Force
2
3 Get-XdAuthentication -ProxyUsername user1 -ProxyPassword
  $secureString
4 <!--NeedCopy-->
```

#### 示例活动

常见活动包括设置计算机目录、应用程序和用户。示例脚本如下所示。

```
1 $users = "xd.local\Domain Users"
2
3 $TSVDACatalogName = "TSVDA"
4
5 $TSVDADGName = "TSVDA"
6
7 $TSVDAMachineName = "xd\ds-tsvda2"
8
9 #Create TSVDA Catalog
10
11 $brokerUsers = New-BrokerUser -Name $users
12
13 $catalog = New-BrokerCatalog -Name $TSVDACatalogName -
  AllocationType "Random" -Description $TSVDACatalogName -
  PersistUserChanges "OnLocal" -ProvisioningType "Manual" -
  SessionSupport "MultiSession" -MachinesArePhysical $true
14
15 #Add TSVDA Machine to Catalog
16
17 $BrokeredMachine = New-BrokerMachine -MachineName $TSVDAMachineName
  -CatalogUid $catalog.uid
```

```
18
19     #Create new desktops & applications delivery group
20
21     $dg = New-BrokerDesktopGroup -Name $TSVDADGName -PublishedName
        $TSVDADGName -DesktopKind "Shared" -SessionSupport "MultiSession"
        -DeliveryType DesktopsAndApps -Description $TSVDADGName
22
23     #Create notepad application
24
25     New-BrokerApplication -ApplicationType HostedOnDesktop -Name "
        Notepad" -CommandLineExecutable "notepad.exe" -DesktopGroup $dg
26
27     #Assign users to desktops and applications
28
29     New-BrokerEntitlementPolicyRule -Name $TSVDADGName -DesktopGroupUid
        $dg.Uid -IncludedUsers $brokerUsers -description $TSVDADGName
30
31     New-BrokerAccessPolicyRule -Name $TSVDADGName -
        IncludedUserFilterEnabled $true -IncludedUsers $brokerUsers -
        DesktopGroupUid $dg.Uid -AllowedProtocols @("HDX","RDP")
32
33     New-BrokerAppEntitlementPolicyRule -Name $TSVDADGName -
        DesktopGroupUid $dg.Uid -IncludedUsers $brokerUsers -description
        $TSVDADGName
34
35     #Add machine to delivery group
36
37     Add-BrokerMachine -MachineName $TSVDAMachineName -DesktopGroup $dg
38     <!--NeedCopy-->
```

## 支持和限制

远程 PowerShell SDK 支持以下操作系统：

- Windows 11
- Windows 10
- Windows 10 IoT Enterprise LTSC x32 2019
- Windows 10 IoT Enterprise LTSC x64 2019
- Windows 10 IoT Enterprise 21h1 x64
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

本版本中支持以下 Citrix Virtual Apps and Desktops PowerShell 模块：

- Broker
- Active Directory (AD) 标识
- 计算机创建

- 配置
- 配置日志记录
- 主机
- 委派管理
- 分析

有关 cmdlet 的详细信息，请参阅 [Citrix Virtual Apps and Desktops SDK](#)。

完成身份验证后，远程访问在 24 小时内在当前的 PowerShell 会话中保持有效。超过该时间后，必须输入您的凭据。

必须在该资源位置中的计算机上运行远程 PowerShell SDK。

以下 cmdlet 在远程操作中处于禁用状态，以保持 Citrix Cloud 控制平面的完整性和安全性。

**Citrix.ADIdentity.Admin.V2:**

- Copy-AcctIdentityPool
- Get-AcctDBConnection
- Get-AcctDBSchema
- Get-AcctDBVersionChangeScript
- Get-AcctInstalledDBVersion
- Remove-AcctServiceMetadata
- Reset-AcctServiceGroupMembership
- Set-AcctDBConnection
- Set-AcctServiceMetadata
- Set-AcctADAccountUserCert
- Test-AcctDBConnection

**Citrix.Analytics.Admin.V1:**

- Get-AnalyticsDBConnection
- Get-AnalyticsDBSchema
- Get-AnalyticsDBVersionChangeScript
- Get-AnalyticsInstalledDBVersion
- Import-AnalyticsDataDefinition
- Remove-AnalyticsServiceMetadata
- Reset-AnalyticsServiceGroupMembership
- Set-AnalyticsDBConnection
- Set-AnalyticsServiceMetadata
- Set-AnalyticsSite
- Set-AnalyticsDBConnection

**Citrix.DelegatedAdmin.Admin.V1:**

- Add-AdminRight

- Get-AdminDBConnection
- Get-AdminDBSchema
- Get-AdminDBVersionChangeScript
- Get-AdminInstalledDBVersion
- Import-AdminRoleConfiguration
- New-AdminAdministrator
- Remove-AdminAdministrator
- Remove-AdminAdministratorMetadata
- Remove-AdminRight
- Remove-AdminServiceMetadata
- Reset-AdminServiceGroupMembership
- Set-AdminAdministrator
- Set-AdminAdministratorMetadata
- Set-AdminDBConnection
- Set-AdminServiceMetadata
- Test-AdminDBConnection

**Citrix.Broker.Admin.V2:**

- Get-BrokerDBConnection
- Get-BrokerDBSchema
- Get-BrokerDBVersionChangeScript
- Get-BrokerInstalledDBVersion
- Get-BrokerLease
- Get-BrokerController
- New-BrokerMachineConfiguration
- Remove-BrokerControllerMetadata
- Remove-BrokerLease
- Remove-BrokerLeaseMetadata
- Remove-BrokerMachineConfigurationMetadata
- Remove-BrokerMachineConfiguration
- Remove-BrokerSiteMetadata
- Remove-BrokerUserFromApplication
- Reset-BrokerLicensingConnection
- Reset-BrokerServiceGroupMembership
- Set-BrokerControllerMetadata
- Set-BrokerDBConnection
- Set-BrokerLeaseMetadata
- Set-BrokerMachineConfiguration
- Set-BrokerMachineConfigurationMetadata
- Set-BrokerSiteMetadata

- Test-BrokerDBConnection
- Test-BrokerLicenseServer
- Update-BrokerBrokerLocalLeaseCache

**Citrix.Configuration.Admin.V2:**

- Export-ConfigFeatureTable
- Get-ConfigDBConnection
- Get-ConfigDBSchema
- Get-ConfigDBVersionChangeScript
- Get-ConfigInstalledDBVersion
- Get-ConfigServiceGroup
- Import-ConfigFeatureTable
- Register-ConfigServiceInstance
- Remove-ConfigRegisteredServiceInstanceMetadata
- Remove-ConfigServiceGroup
- Remove-ConfigServiceGroupMetadata
- Remove-ConfigServiceMetadata
- Remove-ConfigSiteMetadata
- Reset-ConfigServiceGroupMembership
- Set-ConfigDBConnection
- Set-ConfigRegisteredServiceInstance
- Set-ConfigRegisteredServiceInstanceMetadata
- Set-ConfigServiceGroupMetadata
- Set-ConfigServiceMetadata
- Set-ConfigSite
- Set-ConfigSiteMetadata
- Test-ConfigDBConnection
- Unregister-ConfigRegisteredServiceInstance

**Citrix.Host.Admin.V2:**

- Get-HypDBConnection
- Get-HypDBSchema
- Get-HypDBVersionChangeScript
- Get-HypInstalledDBVersion
- Remove-HypServiceMetadata
- Reset-HypServiceGroupMembership
- Set-HypDBConnection
- Set-HypServiceMetadata
- Test-HypDBConnection

**Citrix.ConfigurationLogging.Admin.V1:**

- Get-LogDBConnection
- Get-LogDBSchema
- Get-LogDBVersionChangeScript
- Get-LogInstalledDBVersion
- Remove-LogOperation
- Remove-LogServiceMetadata
- Remove-LogSiteMetadata
- Reset-LogDataStore
- Reset-LogServiceGroupMembership
- Set-LogDBConnection
- Set-LogServiceMetadata
- Set-LogSite
- Set-LogSiteMetadata
- Test-LogDBConnection

**Citrix.MachineCreation.Admin.V2:**

- Get-ProvDBConnection
- Get-ProvDBSchema
- Get-ProvDBVersionChangeScript
- Get-ProvInstalledDBVersion
- Get-ProvServiceConfigurationData
- Remove-ProvServiceConfigurationData
- Remove-ProvServiceMetadata
- Reset-ProvServiceGroupMembership
- Set-ProvDBConnection
- Set-ProvServiceMetadata
- Test-ProvDBConnection

**Citrix.EnvTest.Admin.V1:**

- Get-EnvTestDBConnection
- Get-EnvTestDBSchema
- Get-EnvTestDBVersionChangeScript
- Get-EnvTestInstalledDBVersion
- Remove-EnvTestServiceMetadata
- Reset-EnvTestServiceGroupMembership
- Set-EnvTestDBConnection
- Set-EnvTestServiceMetadata
- Test-EnvTestDBConnection

### **Citrix.Monitor.Admin.V1:**

- Get-MonitorConfiguration
- Get-MonitorDBConnection
- Get-MonitorDBSchema
- Get-MonitorDBVersionChangeScript
- Get-MonitorDataStore
- Get-MonitorDataStore
- Get-MonitorInstalledDBVersion
- Remove-MonitorServiceMetadata
- Reset-MonitorDataStore
- Reset-MonitorServiceGroupMembership
- Set-MonitorConfiguration
- Set-MonitorDBConnection
- Set-MonitorServiceMetadata
- Test-MonitorDBConnection

### **Citrix.Storefront.Admin.V1:**

- Build-SfCluster
- Get-SfClusters
- Get-SfDBConnection
- Get-SfDBSchema
- Get-SfDBVersionChangeScript
- Get-SfInstalledDBVersion

### 用于 **App-V** 包和服务器的 **Citrix DaaS** 发现模块

Citrix DaaS 可以使用以下任一方法将 App-V 包中包含的应用程序交付到端点设备：

- 单管理员管理方法（从网络共享访问软件包）
- 双管理员管理方法（从 Microsoft App-V 管理服务器访问软件包）

使用 Citrix DaaS 向应用程序库注册 App-V 包和 Microsoft App-V 管理和发布服务器的过程与使用本地部署注册包的过程略有差别。但是，向用户分配应用程序并在用户的终端节点上启动应用程序的过程是相同的。

Citrix Cloud 中的 Citrix DaaS 管理控制台无法查看资源位置中的文件。此外，该控制台也无法直接发现您的基础结构中的 App-V 包或 Microsoft App-V 服务器。发现模块提供的功能可用于发现本地基础结构中的 App-V 包信息，并将包信息上载到您的 Citrix DaaS。包信息包括 App-V 包、Microsoft App-V 服务器和包中包含的应用程序。

发现模块使用 Virtual Apps and Desktops 远程 PowerShell SDK。可以从网络共享或 Microsoft App-V 管理服务发现包信息。可以在您的资源位置中的计算机上使用发现模块。

使用发现模块的必备条件：



- 验证 PowerShell 3.0 或更高版本在计算机上是否可用。
- 验证计算机上是否安装了 Citrix Virtual Apps and Desktops 远程 PowerShell SDK。
- 验证您是否有权访问包含 App-V 包的网络共享。
- 验证您是否有权访问安装了 Citrix Cloud Connector 和托管 Microsoft App-V 管理服务器的服务器。

将 **App-V** 包添加到 **Citrix Cloud** 中的应用程序库

下面的过程适用于从网络共享添加 App-V 包（单管理员管理）以及从 Microsoft App-V 管理服务器（双管理员管理）添加所有已发布的 App-V 包。使用双管理员管理方法时，必须像使用单管理员管理方法时一样管理添加的 App-V 包。

1. 从 Citrix DaaS 下载页面 <https://www.citrix.com/downloads/citrix-cloud/product-software/xen-app-and-xendesktop-service.html> 下载发现模块。将 zip 文件 `Citrix.Cloud.AppLibrary.Admin.v1.psm1` 解压到一个便捷的文件夹中。

注意：

`Support\Tools\Scripts` 中的 Citrix Virtual Apps and Desktops ISO 中也提供了此文件。  
可以在本地复制或直接从 CD 驱动器引用。

2. 验证计算机上是否安装了 Virtual Apps and Desktops 远程 PowerShell SDK
3. 导航到包含发现模块的文件夹。在 PowerShell 窗口中，键入包含发现模块的文件夹的完整路径，然后按 **Enter** 键。
4. 使用命令 `Import-Module .\Citrix.Cloud.AppLibrary.Admin.v1.psm1` 导入发现模块。
5. 使用以下任一方法将 App-V 包添加到 Citrix Cloud 中的应用程序库。

- 要从网络共享添加 App-V 包，请运行 PowerShell cmdlet: `Import-AppVPackageToCloud`。

例 如：`Import-AppVPackageToCloud -PackagePath \\AppVSrv\share\Notepad++.appv`

如需 cmdlet 帮助，请键入 `Get-Help Import-AppVPackageToCloud`。

- 要从 Microsoft App-V 管理服务器添加 App-V 包，请运行 PowerShell cmdlet: `Import-AppVPackagesFromManagementServerToCloud`

例如：`Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN AppVMngSrv.domain.local`

如需 cmdlet 帮助，请键入 `Get-Help Import-AppVPackagesFromManagementServerToCloud`

此命令将所有已发布的 App-V 包从 Microsoft App-V 管理服务器导入到 Citrix Cloud。

将 App-V 包添加到 Citrix Cloud 后，必须像使用单管理员管理方法那样对其进行管理。

6. 登录 Citrix Cloud。选择目标客户。脚本成功运行后，App-V 包将添加到 Citrix Cloud 中的应用程序库。

## 高级 PowerShell 功能

该模块包含以下高级函数，您可以从自己的 PowerShell 脚本调用这些函数：

- `Import-AppVPackageToCloud -PackagePath <Full UNC path to App-V package>`

发现所有必需的信息并将其上载到 Citrix DaaS，以从单个 App-V 包发布应用程序。

- `Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN <FQDN of a Microsoft App-V Management Server>`

发现管理服务器发布的软件包的 UNC 路径，然后依次为每个软件包调用 **Import-AppVPackageToCloud**。

以此种方式发现的包将使用单管理员管理方法加载到 Citrix DaaS。Citrix DaaS 无法使用双管理员管理方法交付包。

- `Import-AppVDualAdminToCloud -ManagementSrvUrl <URL of a Microsoft App-V Management Server> -PublishingServerUrl <URL of a Microsoft App-V Publishing Server>`

发现 Microsoft App-V 管理和发布服务器并将内容导入到应用程序库。此 cmdlet 导入使用 Microsoft App-V 管理服务器的所有软件包以及相关信息。可以通过 PowerShell 添加和删除服务器。

此 cmdlet 在双管理员模式下添加 App-V 软件包。仅导入在 Microsoft App-V 管理服务器上发布并添加了 AD 组的 App-V 软件包。如果您更改了 Microsoft App-V 管理服务器，请重新运行此 cmdlet 以将应用程序库与 Microsoft App-V 管理服务器同步。

- `Remove-AppVServerFromCloud -ManagementSrvUrl <URL of a Microsoft App-V Management Server> -PublishingServerUrl <URL of a Microsoft App-V Publishing Server>`

删除添加到应用程序库的 Microsoft App-V 管理和发布服务器。

此 cmdlet 删除指定的 Microsoft App-V 管理和发布服务器，以及所有关联的 App-V 包。

在该资源位置内部加入了域的计算机上运行 App-V 包和服务器的发现模块。请按照安装和使用远程 PowerShell SDK 中的指导进行操作，以开始使用。继续运行 PowerShell cmdlet 或脚本。请参见以下示例。

## 示例活动

导入 Citrix DaaS App-V 包发现模块。

```
1 import-module "D:\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
2 <!--NeedCopy-->
```

循环浏览 App-V 包存储目录并上载每个包。

```
1 Get-ChildItem -Path "\FileServer.domain.net\App-V Packages" -Filter *.  
   appv |  
2 Foreach-Object{  
3  
4     Import-AppVPackageToCloud -PackagePath $_.FullName  
5 }  
6  
7 <!--NeedCopy-->
```

发现并上传使用 Microsoft App-V 管理服务器注册的包。

```
1 Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN  
   AppVManagementServer.domain.net  
2 <!--NeedCopy-->
```

发现 Microsoft App-V 管理和发布服务器并将配置添加到应用程序库。这也会导入 Microsoft App-V 管理服务器在双管理员模式下管理的所有软件包。

```
1 Import-AppVDualAdminCloud -ManagementSrvUrl http://AppVManagementServer  
   .domain.net - PublishingServerUrl http://AppVManagementServer.domain  
   .net:8001  
2 <!--NeedCopy-->
```

阅读模块中包含的 PowerShell 帮助文档。

```
1 Get-Help Import-AppVPackageToCloud  
2 <!--NeedCopy-->
```

## 限制

- 无法直接从 Citrix Cloud 中的 Citrix DaaS 管理控制台发现资源位置基础结构上的 App-V 包。有关 Citrix Cloud 的更多信息，请参阅 [Citrix Cloud](#) 文档。
- Citrix Cloud 中的 Citrix DaaS 管理控制台与 Microsoft App-V 管理服务器未建立实时连接。在重新运行 [Import-AppVDualAdminCloud](#) 之前，对 Microsoft App-V 管理服务器中的软件包和其他配置所做的更改不会反映在 Citrix DaaS 管理控制台中。

## Monitor Service OData API

除使用监视功能显示历史数据外，还可以使用 Monitor Service 的 API 查询数据。使用 API 可以执行以下操作：

- 分析历史趋势以便进行规划
- 对连接失败和计算机故障进行细致的故障排除
- 提取信息以用于其他工具和流程；例如，可以使用 Microsoft Excel 的 PowerPivot 表以不同的方式显示数据
- 基于 API 提供的数据构建自定义用户界面

有关详细信息，请参阅 [Monitor Service OData API](#)。要访问 Monitor Service API，请参阅 [Access Monitor Service data using the OData v4 endpoint in Citrix Cloud](#)（在 Citrix Cloud 中使用 OData v4 端点访问 Monitor Service 数据）。

## Citrix DaaS API

Citrix DaaS API 可在以下位置获得：<https://developer.cloud.com/citrixworkspace/citrix-daas>。

### 免责声明

本软件/示例代码按“原样”提供给您，不提供任何形式的陈述、保证或条件。可以使用、修改和分发本软件/示例代码，风险需自行承担。CITRIX 不承诺任何形式的明示、默示、书面、口头或法定的保证，包括但不限于适销性、特定目的适用性、所有权和非侵权性。在不限制前述内容的一般性的前提下，您承认并同意：(a) 软件/示例代码可能存在错误、设计缺陷或其他问题，可能导致数据丢失或财产损失；(b) 可能无法使软件/示例代码完全正常运行；(c) Citrix 可能在不向您发出通知或承担任何责任的情况下停止提供该软件的当前版本和/或任何未来版本/示例代码。在任何情况下，都不得使用软件/代码来支持超危险活动，包括但不限于生命支持或爆炸活动。根据违约责任或任何其他责任理论，CITRIX 及其分支机构或代理对使用本软件/示例代码导致的任何损害都不承担责任，包括但不限于直接的、特殊的、附带的、后果性的损害或其他损害，即使已被告知造成此类损害的可能性。您同意保护 Citrix 并使 Citrix 免于承担因您使用、修改或分发本代码导致的任何索赔。



© 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).