



# Citrix Hypervisor 8.0

## Contents

<b>Citrix Hypervisor 8.0 当前版本</b>	<b>3</b>
新增功能	4
实验性功能	8
已修复的问题	10
已知问题	11
弃用和删除	13
系统要求	15
配置限制	19
来宾操作系统支持	23
快速入门	29
技术概述	48
常见技术问题解答	55
许可	70
安装	77
安装和部署方案	84
从现有版本升级	89
更新您的主机	97
对安装问题进行故障排除	106
从 <b>SAN</b> 环境引导	107
网络引导安装	110
主机分区布局	114
在小型设备上安装	117
主机和资源池	117

群集池	129
管理用户	133
基于角色的访问控制	139
<b>RBAC 角色和权限</b>	<b>140</b>
结合使用 <b>RBAC</b> 和 <b>CLI</b>	<b>149</b>
网络连接	154
管理网络连接	167
网络连接故障排除	186
存储	190
存储库格式	194
精简预配的共享 <b>GFS2</b> 块存储设备	209
管理存储库	215
存储多路径	225
<b>IntelliCache</b>	<b>227</b>
存储读取缓存	231
<b>PVS 加速器</b>	<b>233</b>
图形概述	240
准备主机以处理图形	243
创建启用了 <b>vGPU</b> 的 <b>VM</b>	252
内存使用率	258
监视和管理您的部署	260
管理虚拟机	279
<b>Windows VM</b>	<b>283</b>
<b>Linux VM</b>	<b>297</b>

<b>VM 内存</b>	<b>312</b>
迁移 <b>VM</b>	<b>317</b>
导入和导出 <b>VM</b>	<b>320</b>
<b>Bromium 安全平台</b>	<b>334</b>
容器管理	<b>336</b>
<b>vApp</b>	<b>342</b>
演示版 <b>Linux</b> 虚拟设备	<b>345</b>
虚拟机高级注释	<b>347</b>
为 <b>Linux VM</b> 启用 <b>VNC</b>	<b>356</b>
对 <b>VM</b> 问题进行故障排除	<b>368</b>
高可用性	<b>370</b>
灾难恢复和备份	<b>376</b>
启用灾难恢复	<b>378</b>
<b>vApp</b>	<b>382</b>
备份和还原主机和 <b>VM</b>	<b>383</b>
<b>VM</b> 快照	<b>387</b>
处理计算机故障	<b>394</b>
故障排除	<b>397</b>
集成概述	<b>400</b>
标准引导补充包	<b>402</b>
<b>Workload Balancing</b>	<b>405</b>
<b>Workload Balancing</b> 入门	<b>407</b>
管理 <b>Workload Balancing</b> 虚拟设备	<b>415</b>
<b>Workload Balancing</b> 的证书	<b>470</b>

<b>Conversion Manager</b>	<b>477</b>
<b>vSwitch 和 Controller</b>	<b>499</b>
<b>管理 vSwitch</b>	<b>502</b>
虚拟网络可见性和控制	<b>507</b>
<b>管理和维护 vSwitch Controller</b>	<b>522</b>
命令	<b>526</b>
对 <b>vSwitch Controller</b> 问题进行故障排除	<b>530</b>
命令行接口	<b>533</b>
<b>SDK 和 API</b>	<b>647</b>

## Citrix Hypervisor 8.0 当前版本

June 4, 2019

您信任的 XenServer 中的技术，该技术是专为虚拟应用程序和桌面工作负载而优化的高性能虚拟机管理程序，基于 Xen 项目虚拟机管理程序，现在称为 Citrix Hypervisor。

Citrix Hypervisor 8.0 是 Citrix Hypervisor 的最新当前版本，本文档介绍了此最新版本中的功能和配置。要了解有关 Citrix Hypervisor 8.0 中的新增功能，请参阅[新增功能](#)。

### 早期版本

有关早期版本的文档，请参阅：

- [XenServer 7.6 CR](#)
- [XenServer 7.1 LTSR](#)
- [XenServer 7.0](#)
- 早期的 Citrix Hypervisor 和 XenServer 版本存档在[旧版文档](#)区域中。

[Citrix Hypervisor 的生命周期里程碑](#)中介绍了 Citrix Hypervisor 当前版本和长期服务版本的产品生命周期策略。

### 关于 Citrix Hypervisor

Citrix Hypervisor 是 Citrix 推出的完整服务器虚拟化平台。Citrix Hypervisor 软件包中包含了创建和管理在 Xen（接近本机性能的开放源代码半虚拟化虚拟机管理程序）上运行的虚拟 x86 计算机部署所需的所有内容。Citrix Hypervisor 已同时针对 Windows 和 Linux 虚拟服务器进行了优化。

Citrix Hypervisor 直接在服务器硬件上运行而不需要底层操作系统，因而是一种高效且可扩展的系统。Citrix Hypervisor 的工作方式是从物理机中提取元素（例如硬盘驱动器、资源和端口），然后将其分配给物理机上运行的虚拟机。

虚拟机 (VM) 是指完全由能够运行自己的操作系统和应用程序的软件组成的计算机，就好像是一台物理计算机。VM 的运行方式与物理计算机十分相似，并且包含自己的虚拟（基于软件）CPU、RAM、硬盘和 NIC。

Citrix Hypervisor 可用于创建 VM、生成 VM 磁盘快照以及管理 VM 工作负载。有关 Citrix Hypervisor 主要功能的综合性列表，请访问 <https://www.citrix.com/products/citrix-hypervisor/>。

### XenCenter

XenCenter 是 Windows GUI 客户端，在管理多个 Citrix Hypervisor 服务器和资源池以及与之关联的虚拟基础结构时，可提供丰富的用户体验。有关详细信息，请参阅[XenCenter 文档](#)。

## 新增功能

September 5, 2019

### 关于此版本

您信任的 XenServer 中的技术，该技术是专为虚拟应用程序和桌面工作负载而优化的高性能虚拟机管理程序，基于 Xen 项目虚拟机管理程序，现在称为 Citrix Hypervisor。

Citrix Hypervisor 8.0 是当前版本 (CR)。当前版本型号允许客户尽早使用新增功能。当前版本与长期服务版本 (XenServer 7.1 LTSR) 截然不同，后者通过功能集来保证稳定性。

Citrix Hypervisor 8.0 在以下版本中提供：

- Premium Edition (以前称为 Enterprise Edition)
- Standard Edition
- Express Edition (以前称为 Free Edition)

有关每个版本中可用的功能的信息，请参阅[Citrix Hypervisor 功能列表](#)。

### **Citrix Hypervisor 8.0** 中的新增功能和改进功能

Citrix Hypervisor 8.0 引入了面向应用程序、桌面和服务器虚拟化用例的增强特性和功能。获得 Citrix Virtual Apps and Desktops (以前称为 XenApp 和 XenDesktop) 许可的所有客户都可以使用 Citrix Hypervisor 8.0 的所有功能。

### 平台刷新

Citrix Hypervisor 平台已更新，可以使用以下软件：

- 内核版本：Linux 4.14
- Xen 虚拟机管理程序版本：4.11
- 控制域操作系统版本：CentOS 7.5

作为内核版本更新的一部分，分配给控制域 (dom0) 的内存量已增加。有关详细信息，请参阅[内存使用率](#)。

内核设备驱动程序也已更新到较新的版本。早期版本中支持的某些硬件可能无法与较新的驱动程序一起使用。升级到 Citrix Hypervisor 8.0 之前请检查[硬件兼容性列表](#)。

此外，随 Citrix Hypervisor 提供的以下设备也已更新，以使用 CentOS 7.5 作为其基本操作系统：

- Citrix Hypervisor Conversion Manager
- Workload Balancing 虚拟设备
- 演示版 Linux 虚拟设备

### 更改了来宾操作系统支持

更新了 Citrix Hypervisor 支持的来宾操作系统的集合。有关详细信息，请参阅[来宾操作系统支持](#)。

### 增加的功能

Citrix Hypervisor 现在支持以下附加 Linux 来宾模板：

- SUSE Linux Enterprise Server 15
- SUSE Linux Enterprise Desktop 15
- CentOS 7.6
- Oracle Linux 7.6
- Red Hat Enterprise Linux 7.6
- Scientific Linux 7.6
- CentOS 6.10
- Oracle Linux 6.10
- Red Hat Enterprise Linux 6.10
- Scientific Linux 6.10
- Windows Server 2019

### 删除的功能

我们移除了对以下来宾模板的支持：

- Debian 6 Squeeze
- Ubuntu 12.04
- Asianux Server 4.2、4.4 和 4.5
- NeoKylin Linux Security OS 5
- Linx Linux 6
- Linx Linux 8
- GreatTurbo Enterprise Server 12
- Yinhe Kylin 4
- 旧版 Windows

#### 注意：

我们在删除旧版 Windows 模板时，还从 Citrix VM Tools ISO 中删除了旧版 Windows 驱动程序。

您可以继续使用安装了这些操作系统的现有 VM。但是，Citrix 不再支持这些 VM。

### 处理器支持的变化

Citrix Hypervisor 8.0 现在支持以下处理器：

- Xeon 82xx/62xx/52xx/42xx/32xx CascadeLake-SP

Citrix Hypervisor 8.0 中不再支持以下旧版处理器：

- Opteron 13xx Budapest
- Opteron 23xx/83xx Barcelona
- Opteron 23xx/83xx Shanghai
- Opteron 24xx/84xx Istanbul
- Opteron 41xx Lisbon
- Opteron 61xx Magny Cours
- Xeon 53xx Clovertown
- Xeon 54xx Harpertown
- Xeon 55xx Nehalem
- Xeon 56xx Westmere-EP
- Xeon 65xx/75xx Nehalem-EX
- Xeon 73xx Tigerton
- Xeon 74xx Dunnington

有关详细信息，请参阅 [硬件兼容性列表](#)。

### 创建大于 **2 TiB** 的 **VDI (Premium Edition)**

现在可以在 GFS2 SR 上创建大于 2 TiB 的虚拟磁盘映像。

### 适用于 **GFS2 SR** 的联机 **LUN** 大小调整 (**Premium Edition**)

现在，您可以对 GFS2 SR 执行联机 LUN 大小调整操作。

### 支持启用了 **vGPU** 的 **VM** 的磁盘和内存快照 (**Premium Edition**)

创建启用了 vGPU 的 VM 的磁盘和内存快照时，该 VM 的状态将包括 vGPU 状态。从快照恢复 VM 时，将还原此 vGPU 的状态。

### **XenCenter** 和 **Citrix Hypervisor Conversion Manager** 的基于 **Web** 的帮助

[XenCenter](#) 和 [Citrix Hypervisor Conversion Manager](#) 的文档现在可以在 [Citrix 产品文档 Web 站点](#) 上联机获取。

此联机文档取代了产品内置的帮助。现在，当您在 UI 中按 **F1** 键或者选择访问上下文帮助时，相关文章将在您的默认浏览器中打开。这些文章还以 PDF 格式提供，以供脱机查看。使用查看 **PDF** 按钮可下载 PDF。

这些基于 Web 的文章为您提供最准确、最新的内容。

### 实验性功能

Citrix Hypervisor 8.0 包括以下实验性功能：

- 来宾 UEFI 引导

有关详细信息，请参阅[实验性功能](#)。

### 安装选项

可以从 [Citrix Hypervisor 产品下载页面](#) 下载 Citrix Hypervisor 8.0 的以下软件包：

- Citrix Hypervisor 8.0 基础安装 ISO。使用此文件可创建全新的 Citrix Hypervisor 8.0 安装或从 XenServer 7.6、7.5、7.1 Cumulative Update 2 或 7.0 进行升级。

此版本的 Citrix Hypervisor 不可作为更新提供。

#### 注意：

- 如果使用 XenCenter 升级您的主机，请在开始操作之前先将 XenCenter 安装更新到 Citrix Hypervisor 8.0 下载页面上提供的最新版本。
- 请始终在升级池中的任何其他主机之前升级池主服务器。
- 请务必先将您的 XenServer 7.1 更新到累积更新 2，然后再升级到 Citrix Hypervisor 8.0。

在开始安装之前，请查看[系统要求](#)和[安装和部署方案](#)。

### 从长期服务版本更改为当前版本

如果您运行的是 XenServer LTSR，但希望利用新增功能，则可以决定更改为 Citrix Hypervisor CR 流。使用 CR 流中的 Citrix Hypervisor 版本需要定期采用新的 CR 以持续获得支持。

请通过从 XenServer 7.1 Cumulative Update 2 LTSR 进行升级来迁移至此当前版本。

### 从当前版本更改为长期服务版本

如果您运行的是 Citrix Hypervisor CR，但希望迁移到具有能够保证的稳定功能集的 Citrix Hypervisor 版本，则可以更改为 XenServer LTSR。可以从 Citrix Hypervisor 产品下载页面下载最新的 XenServer LTSR。

请通过创建全新的 XenServer 7.1 Cumulative Update 2 LTSR 安装迁移到最新的 LTSR。

有关 LTSR 和 CR 的详细信息，请参阅 [Citrix Virtual Apps](#)、[Citrix Virtual Desktops](#) 和 [Citrix Hypervisor 服务方案](#)。

### 许可

客户必须将其 Citrix 许可证服务器升级到版本 11.14 或更高版本，才能使用 Citrix Hypervisor 8.0 的所有许可功能。

有关 Citrix Hypervisor 8.0 许可的详细信息，请参阅[许可](#)。

### 硬件兼容性

有关最新添加的内容以及针对所有硬件兼容性问题的建议，请参阅 Citrix Hypervisor [硬件兼容性列表](#)。

如果您的 VM 连接了虚拟 GPU，请参阅[硬件兼容性列表](#)和 GPU 供应商文档，以确保在升级到最新版本的 Citrix Hypervisor 之前受支持的驱动程序可用。

### 与 Citrix 产品的互操作性

Citrix Hypervisor 8.0 能够与 Citrix XenApp and XenDesktop 7.15 CU3 (LTSR)、Citrix Virtual Apps and Desktops 7 1903 和 Citrix Virtual Apps and Desktops 7 1906 互操作。

Citrix Hypervisor 8.0 能够与 Citrix Provisioning 7.15 CU3 和 1903 互操作。

Citrix Hypervisor 8.0 能够与 Citrix Cloud 互操作。

随着我们统一我们的产品组合，Citrix 产品名称正在发生变迁。有关详细信息，请参阅<https://www.citrix.com/about/citrix-product-guide/>。

### 本地化支持

此版本中也包含 XenCenter 的本地化版本（简体中文和日语）。

### 产品文档

要访问 Citrix Hypervisor 8.0 产品文档，请参阅 [Citrix Hypervisor 8.0 产品文档](#)。有关 Citrix Hypervisor 的常见问题解答，请参阅[技术概述](#)。

在此初始版本发行后，本文档可能会有更新或更改。我们建议您定期访问 [Citrix 产品文档](#) 以了解更新信息。

### 实验性功能

July 10, 2019

实验性功能不适用于在生产环境中使用。Citrix 不保证实验性功能能够在 Citrix Hypervisor 的 GA 版本中可用。

## 来宾 UEFI 引导

Citrix Hypervisor 现在允许最新版本的 Windows 来宾操作系统在 UEFI 模式下引导。UEFI 引导为来宾操作系统提供了更丰富的界面来与硬件交互，这样可以显著缩短 Windows VM 的启动时间。

### 注意：

来宾 UEFI 引导是一项实验性功能。可以在生产环境中的主机上创建启用了 UEFI 的 VM。但是，启用了 UEFI 的 VM 不得用于生产目的。在将主机升级到 Citrix Hypervisor 的较新版本时，可能需要重新创建 VM。

Citrix Hypervisor 在新创建的 Windows 10 (64 位)、Windows Server 2016 (64 位) 和 Windows Server 2019 (64 位) VM 上支持 UEFI 引导。创建 VM 时必须指定引导模式。首次启动 VM 后无法更改 VM 的引导模式。

在 VM 上启用 UEFI 引导时，请注意以下事项：

- 确保启用了 UEFI 的 VM 至少具有两个 vCPU。
- 可以以 OVA、OVF 或 XVA 文件格式导入或导出在 Citrix Hypervisor 中创建的启用了 UEFI 的 VM。不支持从在其他虚拟机管理程序上创建的 OVA 或 OVF 导入启用了 UEFI 的 VM。
- Citrix Machine Creation Services 不支持启用了 UEFI 的 VM。
- 不支持 GPU 直通。
- 不支持 PVS。
- 不支持 UEFI 安全引导。
- 使用 UEFI 设置菜单可更改 XenCenter 控制台的屏幕分辨率。有关详细说明，请参阅更改屏幕分辨率。

## 启用 UEFI 引导

可以使用 XenCenter 或 xe CLI 启用来宾 UEFI 引导。

### 使用 XenCenter

在安装介质上使用新建 VM 向导创建 VM 时，选择 UEFI 引导。

### 注意：

如果您选择的 VM 模板不支持 UEFI 引导，UEFI 引导选项将显示为灰色。

### 使用 xe CLI

创建 VM 时，请在首次引导 VM 之前运行以下命令：

```
1 xe vm-param-set uuid=<UUID> HVM-boot-params:firmware=<MODE>
```

其中，UUID 为 VM 的 UUID，MODE 为“BIOS”或“UEFI”。如果不指定模式，则默认为“BIOS”。

要从模板创建启用了 UEFI 的 VM，请运行以下命令：

```
1   UUID=$(xe vm-clone name-label='Windows 10 (64-bit)'  
2   new-name-label='Windows 10 (64-bit)(UEFI)') xe template-param-set  
   uuid=<UUID> HVM-boot-params:firmware=<MODE>
```

## 更改屏幕分辨率

要更改启用了 UEFI 的 VM 上的 XenCenter 控制台的屏幕分辨率，请执行以下操作：

1. 打开 **Windows** 设置
2. 单击更新和安全按钮
3. 在“恢复”选项卡下，按立即重新启动按钮。
4. 导航到疑难解答 > 高级选项 > **UEFI** 固件设置。
5. 按重新启动。重新启动过程中，UEFI 设置菜单将加载。
6. 导航到设备管理器 > **OVMF** 平台配置。此操作将显示当前的屏幕分辨率。
7. 按 **Enter** 键查看屏幕分辨率选项。
8. 使用箭头键选择所需的屏幕分辨率，然后按 **Enter** 键。
9. 按 **F10** 键保存更改并确认您的选择。
10. 重新启动 VM 以使用更新后的屏幕分辨率查看 XenCenter 控制台。

## 已修复的问题

June 4, 2019

本文列出了此版本中修复的早期版本中存在的问题。

### 常规

- 将新主机添加到群集网络上具有 VLAN 的群集池时，可能会收到错误消息“此服务器需要在网络上具有一个（并且仅限一个）用于群集的 IP 地址”。如果您的 VLAN 位于绑定群集网络顶部，这也将适用。(CA-306864)
- 请勿将超过 32 GB 的内存分配给 Dom0，否则 VM 会间歇性冻结，通常会在启动 VM 过程中冻结。(CA-236674)
- 在 Citrix Virtual Desktop Director 中，VM 控制台不对 XenServer 7.5 和 XenServer 7.6 显示。(CA-309048)
- 分布式虚拟交换机控制器 Web 控制台无法在 Firefox、Google Chrome 和 Microsoft Edge 浏览器中正确加载。(CA-298945)
- 演示版 Linux 虚拟设备首次引导时，将从 DHCP 服务器获取其 IP 地址，即使您已指定其使用静态 IP 地址亦如此。(CA-292640)

## 图形

- 在 XenServer 7.6 中，NVIDIA vGPU 的 RRD 不起作用，并且无法在 XenCenter 中查看这些性能衡量指标的图表。(CA-300751)

## 来宾操作系统

- 在修复 Windows 10 1803 VM 遇到的问题时引入了性能问题。该性能问题现在已修复。(CA-303359)
- 对于从“其他安装介质”模板创建的 VM，在以下情况下 QEMU 无法启动并且 VM 将挂起：
  - 将 VM 从 XenServer 7.5 或更早版本的主机实时迁移到 XenServer 7.6 主机时
  - 在 XenServer 7.5 或更早版本的主机上挂起 VM，然后尝试在 XenServer 7.6 主机上恢复 VM 时

如果出现这种情况，在 XenCenter 中查看时，将不显示任何错误，并且 VM 可能会错误地显示为正在运行。(CA-309144)

- 当池备份元数据 VDI 满载时，VM 元数据备份可能会间歇性失败。池备份元数据 VDI 的默认大小已增加到 500 MiB。(CA-311705)

## XenCenter

- 使用 XenCenter 7.6，当您根据应用后指导 [restarthost](#) 应用来自第三方的更新时，主机在进程结束时不重新启动。(CA-298913)

## 已知问题

June 4, 2019

本文包含 Citrix Hypervisor 8.0 版本中的建议和次要问题以及可以应用的任何解决方法。

## 常规

- VM 运行过程中，池的 CPU 功能集会发生变化。(例如，将新主机添加到现有池时，或者将 VM 迁移到其他池中的主机时。)如果池的 CPU 功能集发生变化，VM 将继续使用启动时应用的功能集。要更新 VM 以使用池的新功能集，必须先关闭再启动该 VM。例如，通过单击 XenCenter 中的“重新启动”重新启动 VM 不会更新 VM 的功能集。(CA-188042)
- Citrix Hypervisor 8.0 中分配给 dom0 的内存量增加意味着可用于运行 VM 的内存略少。在某些硬件上，您可能无法与在早期版本的 XenServer 中的相同硬件上一样在 Citrix Hypervisor 8.0 中运行相同数量的 VM。(CP-29627)

- 尝试使用串行控制台连接到 Citrix Hypervisor 服务器时，串行控制台可能会拒绝接受键盘输入。如果您一直等待，直至控制台刷新两次之后，控制台才能接受键盘输入。(CA-311613)
- 使用群集池时，如果您使用与用于管理或存储相同的网络进行群集操作，中等负载可能会导致整个群集进行自主防护。(CA-312476)

### 图形

- 如果强制关闭附加了 AMD MxGPU 的 VM，或者来宾操作系统异常关闭，您的 Citrix Hypervisor 服务器可能会遇到内存损坏问题。执行协作关机以确保硬件在关机过程中正确清理。(CA-297891)
- 并行启动多个附加了 AMD MxGPU 设备的 VM 时，某些 VM 可能会失败并显示 VIDEO\_TDR\_FAILURE 错误。这可能是由硬件限制造成的。(CA-305555)
- 在极少数情况下，附加了 NVIDIA vGPU 的 VM 在 VM 启动时可能会陷入黄色状态。这可能是由于其中一个 vGPU 设置了“compatibility-metadata”，而实际不应设置导致的。要删除元数据，请暂停并恢复 VM。(CA-312226)

### 来宾操作系统

- 在使用 `bnxt_en` 驱动程序的 Citrix Hypervisor 主机上，Oracle 6.x VM 在连接到网络时会崩溃。请通过安装以下驱动程序磁盘来确保您的 `bnxt_en` 驱动程序是最新的：[Driver Disk for Broadcom bnxt\\_en-1.8.29 - For XenServer 7.x CR](#)。(CA-288010)
- 在极少数情况下，挂起或迁移具有未完成的 xenstore 事务的 Linux VM 可能会由于 VM 的 Linux 内核中的问题而挂起。如果您的 VM 遇到此问题，请强制关闭 VM 并重新启动。(CP-30551)

### 国际化

- 在主机控制台中不能使用非 ASCII 字符（例如带重音符号的字符）。(CA-40845)
- 在安装了 Citrix VM Tools 的 Windows VM 中，如果在 XenCenter 中使用默认桌面控制台，复制并粘贴双字节字符会失败。粘贴的字符显示为问号 (?)。要解决此问题，可以改为使用远程桌面控制台。(CA-281807)

### 存储

- 如果使用的是 GFS2 SR，并且群集池中有两台服务器，则群集可能会在升级到 Citrix Hypervisor 8.0 过程中丢失仲裁和防护。要避免这种情况，请从群集中删除或添加服务器，以确保在升级过程中池中有一个或三个服务器。(CA-313222)
- 如果您以前曾在 XenServer 7.5 上使用作为实验功能的 GFS2 功能，并且未更新到 XenServer 7.6，请在从 XenServer 7.5 更新到 Citrix Hypervisor 8.0 时完成以下步骤：

1. 从这些 SR 中导出要保留的所有数据。
2. 在升级之前从您的池分离并销毁所有 GFS2 SR。
3. 在您的池上禁用群集。
4. 完成到 Citrix Hypervisor 8.0 的更新。
5. 更新完成后，在您的池中所有主机上运行以下命令：

```
1  ‘‘‘
2  rm /var/opt/xapi-clusterd/db
3  ‘‘‘
```

1. 在池主服务器上运行以下命令：

```
1  systemctl restart xapi-clusterd
```

2. 为更新的池创建 GFS2 SR 时，请务必选择格式化，而不是重新连接。不能将使用 XenServer 7.5 创建的 GFS2 SR 重新连接到 Citrix Hypervisor 8.0 池。(CP-29465)
- 由于群集存储的异步插入，GFS2 SR 可能会引发错误的“无法在服务器启动时连接存储”警报。请检查 XenCenter 中的 SR 状态以确定警报是否为误报。(CA-311625)
  - 如果使用的是 GFS2 SR，请务必启用存储多路径以实现最大恢复能力。如果未启用存储多路径，文件系统块写入可能无法完全及时完成。(CA-312678)

## XenCenter

- 在运行 XenCenter 的计算机上修改字体大小或 DPI 会导致用户界面显示不正确。默认字体大小为 96 DPI；Windows 8 和 Windows 10 称此字体大小为 100%。(CA-45514)(CAR-1940)
- 当 XenCenter 安装在 Windows Server 2008 SP2 上时，它可能无法连接到 Citrix Hypervisor 主机并显示消息“无法创建 SSL/TLS 安全通道”。要解决此问题，请确保以下其中一个 Windows Update 已安装在 Windows Server 2008 SP2 系统上：KB4056564 或 KB4019276。有关详细信息，请参阅<http://support.microsoft.com/kb/4019276>。(CA-298456)
- 有时，XenCenter 存储实时迁移或“导入 OVF/OVA”向导不允许您继续操作，并且下一步按钮仍处于禁用状态。发生这种情况时，请重新启动 XenCenter 并再次尝试该过程。(CA-314346)

## 弃用和删除

July 10, 2019

本文声明旨在提前通知您正在逐渐淘汰的平台、Citrix 产品和功能，以便您能够及时制定业务决策。Citrix 将监视客户使用情况和反馈以确定其退出时间。在后续版本中声明可能会有更改，可能不会包括每个弃用的特性或功能。有关产品生命周期支持的详细信息，请参阅[产品生命周期支持策略](#)一文。

### 弃用

以下信息显示了 Citrix Hypervisor 8.0 中已弃用的硬件、平台、Citrix 产品和功能。已弃用的项目不会立即删除。Citrix 在此版本中继续支持这些项目，但将在未来的当前版本中将其删除。

- 以下旧版驱动程序：
  - qla4xxx
  - qla3xxx
  - netxen\_nic
  - qlge
  - qlcnic

早期版本中支持的某些硬件现在可能无法与这些驱动程序一起使用。升级到 Citrix Hypervisor 8.0 之前请检查[硬件兼容性列表](#)。

### 删除

以下信息列出了 Citrix Hypervisor 8.0 中已删除的硬件、平台、Citrix 产品和功能。在 Citrix Hypervisor 中，已删除的项目已被删除或不再受支持。

- XenCenter 安装程序附带 Citrix Hypervisor 安装介质。请改为从[下载页面](#)下载 XenCenter 安装程序。
- 与版本为 6.x 或更早版本的 XenServer 主机建立的 XenCenter 连接
- 支持以下旧版处理器：
  - Opteron 13xx Budapest
  - Opteron 23xx/83xx Barcelona
  - Opteron 23xx/83xx Shanghai
  - Opteron 24xx/84xx Istanbul
  - Opteron 41xx Lisbon
  - Opteron 61xx Magny Cours
  - Xeon 53xx Clovertown
  - Xeon 54xx Harpertown
  - Xeon 55xx Nehalem
  - Xeon 56xx Westmere-EP
  - Xeon 65xx/75xx Nehalem-EX
  - Xeon 73xx Tigerton
  - Xeon 74xx Dunnington

有关详细信息，请参阅 [硬件兼容性列表](#)。

- 支持 qemu-trad。无法再通过设置 `platform-device-model=qemu-trad` 使用 qemu-trad。使用 qemu-trad 设备配置文件创建的所有 VM 都将自动升级到 qemu-upstream-compat 配置文件。

- 支持使用其供应商不再支持的操作系统的下列来宾模板：

- Debian 6 Squeeze
- Ubuntu 12.04
- 旧版 Windows

我们在删除旧版 Windows 模板时，还从 Citrix VM Tools ISO 中删除了旧版 Windows 驱动程序。

- 支持以下来宾模板：

- Asianux Server 4.2、4.4 和 4.5
- NeoKylin Linux Security OS 5
- Linx Linux 6
- Linx Linux 8
- GreatTurbo Enterprise Server 12
- Yinhe Kylin 4

## 系统要求

September 5, 2019

Citrix Hypervisor 至少需要两台单独的 x86 物理计算机：一台作为 Citrix Hypervisor 服务器，另一台运行 XenCenter 应用程序或 Citrix Hypervisor 命令行接口 (CLI)。Citrix Hypervisor 服务器计算机专用于运行 Citrix Hypervisor 和托管 VM 的任务，而不适用于运行其他应用程序。

### 警告：

不支持直接在 Citrix Hypervisor 的控制域中安装第三方软件。作为补充包提供并且由 Citrix 明确认可的软件除外。

要运行 XenCenter，请使用满足硬件要求的任何通用 Windows 系统。此 Windows 系统可用于运行其他应用程序。

在此系统中安装 XenCenter 时，还将安装 Citrix Hypervisor CLI。可以在任何基于 RPM 的 Linux 发行版上安装独立的远程 Citrix Hypervisor CLI。有关详细信息，请参阅[命令行接口](#)。

## Citrix Hypervisor 服务器系统要求

尽管 Citrix Hypervisor 通常部署在服务器级的硬件上，但 Citrix Hypervisor 也与许多工作站和便携计算机模型兼容。有关详细信息，请参阅[硬件兼容性列表 \(HCL\)](#)。

下面的部分介绍建议的 Citrix Hypervisor 硬件规范。

Citrix Hypervisor 服务器必须是 64 位 x86 服务器级计算机，专用于托管 VM。Citrix Hypervisor 创建经过优化及增强的 Linux 分区，并且配备了支持 Xen 的内核。此内核控制面向 VM 的虚拟化设备与物理硬件之间的交互。

Citrix Hypervisor 可以使用：

- 多达 5 TB 的 RAM
- 多达 16 个物理 NIC
- 每个主机多达 288 个逻辑处理器。

注意：

受支持的逻辑处理器的最大数量因 CPU 而异。有关详细信息，请参阅 [硬件兼容性列表 \(HCL\)](#)。

Citrix Hypervisor 服务器的系统要求如下：

## CPU

一个或多个 64 位 x86 CPU，主频最低为 1.5 GHz，建议使用 2 GHz 或更快的多核 CPU。

要支持运行 Windows 或较新版本的 Linux 的 VM，需要使用配备了一个或多个 CPU 的 Intel VT 或 AMD-V 64 位 x86 系统。

注意：

要运行 Windows VM 或较新版本的 Linux VM，请在 Citrix Hypervisor 服务器上启用虚拟化硬件支持功能。虚拟化支持是 BIOS 中的一个选项。您的 BIOS 可能禁用了虚拟化支持。有关详细信息，请参阅 BIOS 文档。

要支持运行受支持的半虚拟化 Linux 的 VM，需要使用配备了一个或多个 CPU 的基于标准 64 位 x86 的系统。

## RAM

最低 2 GB，建议使用 4 GB 或更大

## 磁盘空间

- 最低 46 GB 的本地连接的存储 (PATA、SATA、SCSI)，建议磁盘空间为 70 GB
- 通过从 SAN 的多路径引导功能进行安装时，使用通过 HBA（而非通过软件）的 SAN。

有关兼容的存储解决方案的详细列表，请参阅[硬件兼容性列表 \(HCL\)](#)。

## 网络

100MB/秒或更快的 NIC。为实现更加快速的 P2V 以及导出/导入数据传输和 VM 实时迁移，建议使用 1 GB 或更大的 NIC，或者 10 GB 的 NIC。

我们建议您使用多个 NIC 以实现冗余。NIC 的配置因存储类型而异。有关详细信息，请参阅供应商文档。

Citrix Hypervisor 需要使用 IPv4 网络来管理和传输存储流量。

注意：

- 确保服务器的 BIOS 中的时间设置为 UTC 中的当前时间。
- 在某些支持案例中，出于调试目的，需要串行控制台访问。设置 Citrix Hypervisor 配置时，我们建议您配置串行控制台访问。对于不具备物理串行端口的主机或者无适当物理基础结构可用的情况，请研究能否配置嵌入式管理设备。例如，Dell DRAC 或 HP iLO。有关设置串行控制台访问的详细信息，请参阅 [CTX228930 - 如何在 XenServer 及更高版本上配置串行控制台访问](#)。

## XenCenter 系统要求

XenCenter 具有以下系统要求：

- 操作系统：
  - Windows 10
  - Windows 8.1
  - Windows 7 SP1
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2 SP1
  - Windows Server 2008 SP2（请参阅“备注”）
  - Windows Server 2016
- **.NET Framework**：版本 4.6
- **CPU** 速度：最低 750 MHz，建议使用 1 GHz 或速度更快的 CPU
- **RAM**：最低 1 GB，建议使用 2 GB 或更大
- 磁盘空间：最小 100 MB
- 网络：100 MB/秒或更快的 NIC
- 屏幕分辨率：最低 1024x768 像素

XenCenter 与自 Citrix Hypervisor 以后的所有受支持的版本兼容。

注意：

当 XenCenter 安装在 Windows Server 2008 SP2 上时，请确保以下其中一个 Windows Update 已安装在 Windows Server 2008 SP2 系统上：KB4056564 或 KB4019276。有关详细信息，请参阅 <http://support.microsoft.com/kb/4019276>。

## 支持的来宾操作系统

有关受支持的来宾操作系统的列表，请参阅 [来宾操作系统支持](#)。

### 池要求

资源池是一台或多台服务器的同类或异类聚合，每个池最多包含 64 台服务器。创建池或将服务器加入现有池之前，请确保池中的所有服务器都满足以下要求。

### 硬件要求

Citrix Hypervisor 资源池中的所有服务器必须具有广泛兼容的 CPU，也就是说：

- 所有服务器上的所有 CPU 的 CPU 供应商（Intel 或 AMD）必须都相同。
- 要运行 HVM 虚拟机，所有 CPU 都必须启用虚拟化功能。

### 其他要求

除上述硬件必备条件外，加入池的服务器还需要满足一些其他配置方面的必备条件：

- 它必须具有一致的 IP 地址（服务器上的静态 IP 地址或静态 DHCP 租用）。此要求同样适用于提供共享 NFS 或 iSCSI 存储的服务器。
- 服务器的系统时钟必须与池主服务器同步（例如，通过 NTP）。
- 服务器不能是某个现有资源池的成员。
- 服务器上不能有任何正运行或挂起的 VM，其 VM 中不能有任何正在执行的操作（例如关机或导出）。请先关闭服务器上的所有 VM，再将其添加到池中。
- 不能为服务器配置任何共享存储。
- 服务器不能有绑定的管理接口。请先重新配置管理接口并将其移动到物理 NIC 上，然后再将服务器添加到池中。服务器加入池后，可以再次重新配置管理接口。
- 服务器与池中的服务器必须运行相同版本的 Citrix Hypervisor 软件，修补程序级别也必须相同。
- 为服务器配置的补充包必须与池中已有的服务器相同。补充软件包用于将附加软件安装到 Citrix Hypervisor 控制域 dom0 中。为防止池中出现不一致的用户体验，必须在池中的所有服务器上安装修订版相同的相同补充包。
- 服务器的 Citrix Hypervisor 许可证必须与池中已存在的服务器相同。加入池后，可以更改任意池成员的许可证。许可证级别最低的服务器决定了池中所有成员可以使用的功能。

资源池中的 Citrix Hypervisor 服务器可以包括不同数量的物理网络接口和不同大小的本地存储库。实际上，由于通常很难实现多个服务器使用完全相同的 CPU，因此微小差异是允许的。如果希望您所处的环境允许在同一个资源池中包含配备了不同 CPU 的主机，可以使用 CLI 强制将这些主机加入池。有关强制执行加入操作的信息，请参阅[主机和资源池](#)。

#### 注意：

为池提供 NFS 或 iSCSI 共享存储的服务器必须具有静态 IP 地址或者支持 DNS 寻址。

### 同类池

同类资源池是具有相同 CPU 的服务器的聚合。加入同类资源池的服务器上的 CPU 必须与池中已有的服务器上的 CPU 具有相同的供应商、型号和功能。

### 异构池

使用 Intel (FlexMigration) 和 AMD (Extended Migration) CPU 中提供 CPU 屏蔽或调配功能的技术可以创建异构池。通过这些功能，可以将 CPU 配置为看起来提供与实际不同的样式、型号或功能集。可以通过这些功能创建主机池，尽管这些池具有完全不同的 CPU，但仍能安全地支持实时迁移。

有关创建异构池的信息，请参阅[主机和资源池](#)。

## 配置限制

July 10, 2019

请在为 Citrix Hypervisor 选择和配置虚拟环境和物理环境时使用以下配置限制作为指导原则。Citrix Hypervisor 完全支持以下经过测试的建议配置限制。

- 虚拟机限制
- Citrix Hypervisor 服务器限制
- 资源池限制

硬件和环境等因素会影响下面列出的限制。有关受支持的硬件的详细信息，请参阅[硬件兼容性列表](#)。请查阅您的硬件制造商记录的限制，以确保不超过您的环境支持的配置限制。

### 虚拟机 (VM) 限制

项目	限制
<b>计算</b>	
每个 VM 的虚拟 CPU 数量 (Linux)	32 (请参阅备注 1)
每个 VM 的虚拟 CPU 数量 (Windows)	32
<b>内存</b>	
每个 VM 的 RAM 大小	1.5 TiB (请参阅备注 2)

项目	限制
<b>存储</b>	
每个 VM 的虚拟磁盘映像 (VDI) 数量 (包括 CD-ROM)	255 (请参阅备注 3)
每个 VM 的虚拟 CD-ROM 驱动器数量	1
虚拟磁盘大小 (NFS)	2 TiB 减去 4 GiB
虚拟磁盘大小 LVM)	2 TiB 减去 4 GiB
虚拟磁盘大小 (GFS2)	16 TiB
<b>网络连接</b>	
每个 VM 的虚拟 NIC 数量	7 (请参阅备注 4)

**注意：**

1. 请参阅您的来宾操作系统文档，确保不超过支持的限制。
2. 可由操作系统寻址的最大物理内存量有所不同。将内存设置为超过操作系统支持的限制的级别可能会导致来宾内部出现性能问题。某些 32 位 Windows 操作系统支持 4 GiB 以上的 RAM，但需要使用物理地址扩展 (PAE) 模式。32 位 PV 虚拟机的限制为 64 GiB。有关详细信息，请参阅您的来宾操作系统文档和[来宾操作系统支持](#)。
3. 支持的最大 VDI 数量取决于来宾操作系统。请参阅您的来宾操作系统文档，确保不超过支持的限制。
4. 多种来宾操作系统具有较低的限制，其他来宾要求安装 Citrix VM Tools 以实现这一限制。

**Citrix Hypervisor 服务器限制**

项目	限制
<b>计算</b>	
每个主机的逻辑处理器数量	288 (请参阅备注 1)
每个主机的并发 VM 数量	1000 (请参阅备注 2)
启用了高可用性的每个主机的受保护的并发 VM 数量	500
每个主机的虚拟 GPU VM 数量	128 (请参阅备注 3)
<b>内存</b>	

项目	限制
每个主机的 RAM 大小	5 TB (请参阅备注 4)
<b>存储</b>	
每个主机的并发活动虚拟磁盘数量	4096
<b>网络连接</b>	
每个主机的物理 NIC 数量	16
每个网络绑定的物理 NIC 数量	4
每个主机的虚拟 NIC 数量	512
每个主机的 VLAN 数量	800
每个主机的网络绑定数量	4
<b>图形功能</b>	
每个主机的 GPU 数量	12 (请参阅备注 5)

**注意：**

1. 受支持的逻辑物理处理器的最大数量因 CPU 而异。有关详细信息，请参阅 [硬件兼容性列表](#)。
2. 受支持的最大 VM/主机数量取决于 VM 工作负载、系统负载、网络配置和特定的环境因素。我们有权确定哪些特定的环境因素会影响系统可以正常运行的最大限制。对于运行超过 500 个 VM 的系统，我们建议向控制域 (Dom0) 分配 8 GB RAM。有关配置 Dom0 内存的信息，请参阅 [CTX134951 - 如何在 XenServer 6.2 及更高版本中配置 dom0 内存](#)。
3. 对于 NVIDIA vGPU，每个主机具有 128 个 vGPU 加速的 VM，其中包括 4xM60 个卡 (4x32=128 个 VM)，或者 2xM10 个卡 (2x64=128 个 VM)。对于 Intel GVT-g，每个主机具有 7 个 VM，其显存大小为 1024 MB。较小的显存大小会进一步限制每个主机支持的 GVT-g VM 数量。下图可能会发生变化。有关当前支持的限制，请参阅[硬件兼容性列表](#)。
4. 如果主机具有一个或多个 32 位半虚拟化来宾 (Linux VM)，主机最大支持运行 128 GB 的 RAM。
5. 下图可能会发生变化。有关当前支持的限制，请参阅[硬件兼容性列表](#)。

**资源池限制**

项目	限制
<b>计算</b>	
每个资源池的 VM 数量	4096
每个资源池的主机数量	64 (请参阅备注 1)
<b>网络连接</b>	
每个资源池的 VLAN 数量	800
每个跨服务器专用网络的活动主机数量	64
每个资源池的跨服务器专用网络数量	16
每个跨服务器专用网络的虚拟 NIC 数量	16
每个资源池的跨服务器专用网络虚拟 NIC 数量	256
每个 vSwitch Controller 的主机数量	64
每个 vSwitch Controller 的虚拟 NIC 数量	1024
每个 vSwitch Controller 的 VM 数量	1024
<b>灾难恢复</b>	
每个资源池的集成站点恢复存储库数量	8
<b>存储</b>	
LUN 的路径	8
每个主机的多路径 LUN 数量	256 (请参阅备注 2)
每个主机的多路径 LUN 数量 (由存储库使用)	256 (请参阅备注 2)
每个 SR (NFS、SMB、EXT、GFS2) 的 VDI 数量	20000
每个 SR (LVM) 的 VDI 数量	1000
<b>Storage 实时迁移</b>	
每个 VM 的 (非 CDROM) VDI 数量	6
每个 VM 的快照数量	1
并发传输数量	3

项目	限制
----	----

### XenCenter

每个池的并发操作数量	25
------------	----

#### 注意：

1. 使用 GFS2 存储的群集池在资源池中最多支持 16 个主机。
2. 启用了高可用性功能时，如果主机上存在 30 多个多路径 LUN，我们建议您将默认超时时间增大到至少 120 秒。有关增加高可用性超时时间的信息，请参阅 [CTX139166 - 如何更改高可用性超时设置](#)。

## 来宾操作系统支持

September 5, 2019

安装 VM 并分配资源（例如内存和磁盘空间）时，请遵循操作系统和任何相关应用程序的指导原则。

操作系统	虚拟化模式	最小 RAM	最大 RAM	最小磁盘空间
Windows 7 SP1、 Windows 8.1、 Windows 10 (32 位)	HVM	1 GB	4 GB	24 GB (建议 40 GB 或更大)
Windows 7 SP1 (64 位)	HVM	2 GB	192 GB	24 GB (建议 40 GB 或更大)
Windows 8.1 (64 位)	HVM	2 GB	512 GB	24 GB (建议 40 GB 或更大)
Windows 10 (64 位)	HVM	2 GB	1.5 TB	24 GB (建议 40 GB 或更大)
Windows Server 2008 SP2 (32 位)	HVM	512 MB	64 GB	24 GB (建议 40 GB 或更大)
Windows Server 2008 SP2 (64 位)	HVM	512 MB	1 TB	24 GB (建议 40 GB 或更大)
Windows Server 2008 R2 SP1	HVM	512 MB	1.5 TB	24 GB (建议 40 GB 或更大)

操作系统	虚拟化模式	最小 RAM	最大 RAM	最小磁盘空间
Windows Server 2012、Windows Server 2012 R2 (64 位)	HVM	1 GB	1.5 TB	32 GB (建议 40 GB 或更大)
Windows Server 2016、Windows Server Core 2016 (64 位)	HVM	1 GB	1.5 TB	32 GB (建议 40 GB 或更大)
Windows Server 2019、Windows Server Core 2019 (64 位)	HVM	1 GB	1.5 TB	32 GB (建议 40 GB 或更大)
CentOS 5.x (32 位)	PV	512 MB	16 GB	8 GB
CentOS 5.0–5.7 (64 位)	PV	512 MB	16 GB	8 GB
CentOS 5.8–5.11 (64 位)	PV	512 MB	128 GB	8 GB
CentOS 6.0、6.1 (32 位)	PV	1 GB	8 GB	8 GB
CentOS 6.0、6.1 (64 位)	PV	512 MB	32 GB	8 GB
CentOS 6.2–6.10 (32 位)	PV	512 MB	16 GB	8 GB
CentOS 6.2–6.10 (64 位)	PV	1 GB	128 GB	8 GB
CentOS 7.x (64 位)	HVM	2 GB	1.5 TB	10 GB
Red Hat Enterprise Linux 5.x (32 位)	PV	512 MB	16 GB	8 GB
Red Hat Enterprise Linux 5.0–5.7 (64 位)	PV	512 MB	16 GB	8 GB

操作系统	虚拟化模式	最小 RAM	最大 RAM	最小磁盘空间
Red Hat Enterprise Linux 5.8–5.11 (64 位)	PV	512 MB	128 GB	8 GB
Red Hat Enterprise Linux 6.0、6.1 (32 位)	PV	512 MB	8 GB	8 GB
Red Hat Enterprise Linux 6.0、6.1 (64 位)	PV	1 GB	32 GB	8 GB
Red Hat Enterprise Linux 6.2–6.10 (32 位)	PV	512 MB	16 GB	8 GB
Red Hat Enterprise Linux 6.2–6.10 (64 位)	PV	1 GB	128 GB	8 GB
Red Hat Enterprise Linux 7.x (64 位)	HVM	2 GB	1.5 TB	10 GB
SUSE Linux Enterprise Server 11 SP3、11 SP4 (32 位)	PV	1 GB	16 GB	8 GB
SUSE Linux Enterprise Server 11 SP3、11 SP4 (64 位)	PV	1 GB	128 GB	8 GB
SUSE Linux Enterprise Server 12、12 SP1、12 SP2 (64 位)	PV	1 GB	128 GB	8 GB
SUSE Linux Enterprise Server 12 SP3 (64 位)	HVM	1 GB	1.5 TB	8 GB

操作系统	虚拟化模式	最小 RAM	最大 RAM	最小磁盘空间
SUSE Linux Enterprise Server 15 (64 位)	HVM	1 GB	1.5 TB	8 GB
SUSE Linux Enterprise Desktop 11 SP3 (64 位)	PV	1 GB	128 GB	8 GB
SUSE Linux Enterprise Desktop 12、12 SP1、12 SP2 (64 位)	PV	1 GB	128 GB	8 GB
SUSE Linux Enterprise Desktop 12 SP3 (64 位)	HVM	1 GB	1.5 TB	8 GB
SUSE Linux Enterprise Desktop 15 (64 位)	HVM	1 GB	1.5 TB	8 GB
Oracle Linux 5.0–5.7、5.10、5.11 (32 位)	PV	512 MB	64 GB	8 GB
Oracle Linux 5.8、5.9 (32 位)	PV	512 MB	16 GB	8 GB
Oracle Linux 5.x (64 位)	PV	512 MB	128 GB	8 GB
Oracle Linux 6.x (32 位)	PV	512 MB	8 GB	8 GB
Oracle Linux 6.0、6.1 (64 位)	PV	1 GB	32 GB	8 GB
Oracle Linux 6.2–6.10 (64 位)	PV	1 GB	128 GB	8 GB
Oracle Linux 7.x (64 位)	HVM	2 GB	1.5 TB	10 GB

操作系统	虚拟化模式	最小 RAM	最大 RAM	最小磁盘空间
Scientific Linux 6.6–6.10 (32 位)	PV	512 MB	16 GB	8 GB
Scientific Linux 6.6–6.10 (64 位)	PV	1 GB	128 GB	8 GB
Scientific Linux 7.x (64 位)	HVM	2 GB	1.5 TB	10 GB
Debian Wheezy 7 (32 位)	PV	512 MB	64 GB	8 GB
Debian Wheezy 7 (64 位)	PV	512 MB	128 GB	8 GB
Debian Jessie 8 (32 位)	HVM	128 MB	64 GB	8 GB
Debian Jessie 8 (64 位)	HVM	128 MB	1.5 TB	8 GB
Debian Stretch 9 (32 位)	HVM	256 MB	64 GB	10 GB
Debian Stretch 9 (64 位)	HVM	256 MB	1.5 TB	10 GB
Ubuntu 14.04 (32 位)	HVM	512 MB	64 GB	8 GB
Ubuntu 14.04 (64 位)	HVM	512 MB	1.5 TB	8 GB
Ubuntu 16.04 (32 位)	HVM	512 MB	64 GB	10 GB
Ubuntu 16.04 (64 位)	HVM	512 MB	1.5 TB	10 GB
Ubuntu 18.04 (64 位)	HVM	512 MB	1.5 TB	10 GB
CoreOS Stable (64 位) [测试过的 最新版本为 1911.4.0]	HVM	2 GB	512 GB	8 GB

操作系统	虚拟化模式	最小 RAM	最大 RAM	最小磁盘空间
NeoKylin Linux Advanced Server 6.5 (64 位)	PV	1 GB	128 GB	8 GB
NeoKylin Linux Advanced Server 7.2 (64 位)	HVM	1 GB	1.5 TB	10 GB

**重要:**

- 在 Citrix Hypervisor 8.0 上无法启动配备了原始内核的 RHEL、OL 和 CentOS 5.x 来宾操作系统。在尝试将 Citrix Hypervisor 服务器升级到 8.0 之前，请将内核更新到版本 5.4 (2.6.18-164.el5xen) 或更高版本。
- 不同版本的操作系统对于支持的内存量还会有各自的最大值限制（例如，由于许可原因）。
- 配置来宾内存时，请不要超出操作系统可寻址的最大物理内存量。如果设置的内存最大值超出操作系统支持的限制，可能会导致来宾系统出现稳定性问题。

**注意:**

- 要创建 RHEL 的次要版本高于上表中列出的版本的 VM，请使用以下方法：
  - 从主要版本的最新受支持的介质安装 VM
  - 使用 `yum update` 将 VM 更新到更高的次要版本

此方法还适用于基于 RHEL 的操作系统，例如 CentOS 和 Oracle Linux。

- 某些 32 位 Windows 操作系统可以使用物理地址扩展 (PAE) 模式支持 4 GB 以上的 RAM。要重新配置 RAM 大于 4 GB 的 VM，请使用 `xe CLI`，而不是 XenCenter，因为 CLI 对于 `memory-static-max` 不强加任何上限。

**长期来宾支持**

Citrix Hypervisor 包括适用于 Linux VM 的长期来宾支持 (LTS) 政策。LTS 政策允许您通过以下方法之一使用次要版本更新：

- 从新来宾介质安装
- 从现有的受支持来宾升级

## 快速入门

September 5, 2019

本文分步骤介绍如何安装和配置 Citrix Hypervisor 及其基于 Windows 的图形用户界面 XenCenter。安装完成后，将引导您完成创建 Windows 虚拟机 (VM)，然后创建可用于快速创建多个相似的 VM 的自定义 VM 模板 d 的过程。最后，本文将介绍如何创建主机池；主机池为使用实时迁移功能在主机之间迁移运行中的 VM 提供了基础。

本文重点介绍最基本的方案，旨在帮助您快速做好准备。

本文主要面向 Citrix Hypervisor 和 XenCenter 的新用户，本文面向希望使用 XenCenter 管理 Citrix Hypervisor 的用户。有关如何通过 Citrix Hypervisor 命令行接口 (CLI) 使用基于 Linux 的 xe 命令管理 Citrix Hypervisor 的信息，请参阅[命令行接口](#)。

### 术语和缩略语

- 主机：运行 Citrix Hypervisor 的物理计算机
- 虚拟机 (VM)：完全由能够运行自己的操作系统和应用程序的软件组成的计算机，就好像是一台物理机。VM 的运行方式与物理计算机十分相似，并且包含自己的虚拟（基于软件）CPU、RAM、硬盘和 NIC。
- 池：单个托管实体，用于将多个 Citrix Hypervisor 服务器及其 VM 绑定在一起
- 存储库 (SR)：一种存储容器，用于存储虚拟磁盘

### 主要组件

#### **Citrix Hypervisor**

Citrix Hypervisor 是一个完整的服务器虚拟化平台，具备创建和管理虚拟基础结构所需的全部功能。Citrix Hypervisor 已针对 Windows 和 Linux 虚拟服务器进行了优化。

Citrix Hypervisor 直接在服务器硬件上运行而不需要底层操作系统，因而是一种高效且可扩展的系统。Citrix Hypervisor 从物理机提取元素（例如硬盘驱动器、资源和端口），然后将其分配给物理机上运行的虚拟机。

Citrix Hypervisor 可用于创建 VM、生成 VM 磁盘快照以及管理 VM 工作负载。

#### **XenCenter**

XenCenter 是一种基于 Windows 的图形用户界面。通过 XenCenter，可以管理 Citrix Hypervisor 服务器、池和共享存储。使用 XenCenter 可以从 Windows 桌面计算机部署、管理和监视 VM。

XenCenter 联机帮助也是一种很好的 XenCenter 入门参考资源。随时按 F1 可访问上下文相关信息。

## 安装 Citrix Hypervisor 和 XenCenter

在本部分中，您将设置最低版本的 Citrix Hypervisor 安装。

您将学习的内容

您将学习如何执行以下操作：

- 在单个物理主机上安装 Citrix Hypervisor
- 在 Windows 计算机上安装 XenCenter
- 将 XenCenter 连接到 Citrix Hypervisor 以构建用于创建和运行虚拟机 (VM) 的基础结构。

要求

要开始操作，您需要以下项目：

- 要用作 Citrix Hypervisor 服务器的物理计算机
- 要运行 XenCenter 应用程序的 Windows 计算机
- Citrix Hypervisor 和 XenCenter 的安装文件

Citrix Hypervisor 服务器计算机专用于运行 Citrix Hypervisor 和托管 VM 的任务，而不用于运行其他应用程序。运行 XenCenter 的计算机可以是满足硬件要求的任何通用 Windows 计算机。也可以使用此计算机运行其他应用程序。有关详细信息，请参阅[系统要求](#)。

可以从 [Citrix Hypervisor 下载](#) 下载安装文件。

## 安装 Citrix Hypervisor 服务器

所有主机都至少有一个相关联的 IP 地址。要为主机配置静态 IP 地址（而不使用 DHCP），请在开始此过程之前准备好静态 IP 地址。

提示：

按 **F12** 键可快速前进到下一个安装程序屏幕。要获得常规帮助，请按 **F1** 键。

要安装 Citrix Hypervisor 服务器，请执行以下操作：

1. 将 Citrix Hypervisor 的安装文件刻录成 CD。

注意：

有关使用 HTTP、FTP 或 NFS 作为安装源的信息，请参阅[安装 Citrix Hypervisor](#)。

2. 备份要保留的数据。安装 Citrix Hypervisor 时，会覆盖选择用作安装位置的任何硬盘驱动器上的数据。
3. 将安装 CD 插入主机计算机的 DVD 驱动器中。

4. 重新启动主机计算机。
5. 从 DVD 驱动器引导（如有必要，请参阅硬件供应商提供的文档，了解关于更改引导顺序的信息）。
6. 显示初始引导消息和欢迎使用 **Citrix Hypervisor** 屏幕后，选择要在安装过程中使用的键盘布局。
7. 显示欢迎使用 **Citrix Hypervisor** 安装程序屏幕时，选择确定。
8. 阅读并接受 Citrix Hypervisor EULA。

注意：

如果看到系统硬件警告，并怀疑您的系统是否具有硬件虚拟化协助支持功能，请参阅硬件制造商提供的 BIOS 升级信息。

9. 选择 **OK**（确定）执行全新安装。
10. 如果您拥有多个硬盘，请选择主磁盘进行安装。选择 **OK**（确定）。  
选择要用作虚拟机存储的磁盘。选择 **OK**（确定）。
11. 选择 **Local media**（本地介质）作为安装源。
12. 选择 **Skip Verification**（跳过验证），然后选择 **OK**（确定）。

注意：

如果在安装过程中遇到问题，请验证安装源。

13. 创建并确认 root 用户密码，XenCenter 应用程序将使用此密码连接到 Citrix Hypervisor 服务器。
14. 设置用于连接到 XenCenter 的管理接口。  
如果您的计算机有多个 NIC，请选择希望用来实施流量管理的 NIC（通常是第一个 NIC）。
15. 将管理 NIC 的 IP 地址配置为静态 IP 地址或使用 DHCP。
16. 手动指定或通过 DHCP 自动指定主机名和 DNS 配置。  
如果手动配置 DNS，请在提供的字段中输入主要（必需）、二级（可选）和三级（可选）DNS 服务器的 IP 地址。
17. 选择您所在的时区。
18. 指定希望服务器在确定本地时间时所用的方法：使用 NTP 或手动输入时间。选择 **OK**（确定）。  
如果使用 NTP，则可以指定 DHCP 是否设置时间服务器。或者，也可以在以下字段中输入至少一个 NTP 服务器名称或 IP 地址。
19. 选择安装 **Citrix Hypervisor**。
20. 如果选择手动设置日期和时间，系统会提示您输入这些信息。
21. 如果要从 CD 进行安装，下一个屏幕会询问您是否要从 CD 安装任何补充包。选择否以继续操作。
22. 在 **Installation Complete**（安装完成）屏幕中，从驱动器中弹出安装 CD，然后选择 **\*OK**（确定）以重新启动服务器。  
服务器重新引导后，Citrix Hypervisor 将显示 **xsconsole**（系统配置控制台）。

注意：

记下显示的 IP 地址。请在将 XenCenter 连接到主机时使用此 IP 地址。



### 安装 XenCenter

XenCenter 通常安装在您的本地系统中。可以从 [Citrix 下载站点](#) 下载 XenCenter 安装程序

要安装 XenCenter，请执行以下操作：

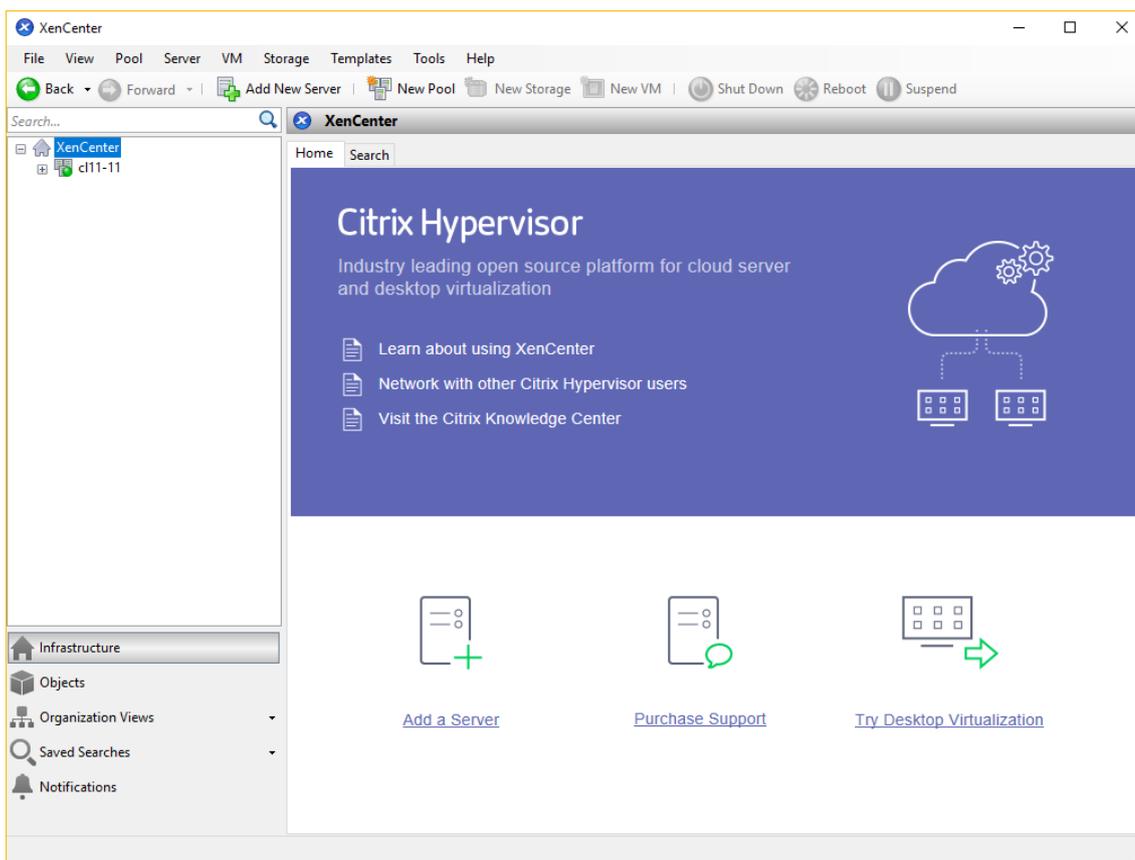
1. 将 XenCenter 安装程序下载或传输到要运行 XenCenter 的计算机。
2. 双击安装程序 .msi 文件开始安装。
3. 按照安装向导操作；该向导允许您修改默认目标文件夹，然后安装 XenCenter。

### 将 XenCenter 连接到 Citrix Hypervisor 服务器

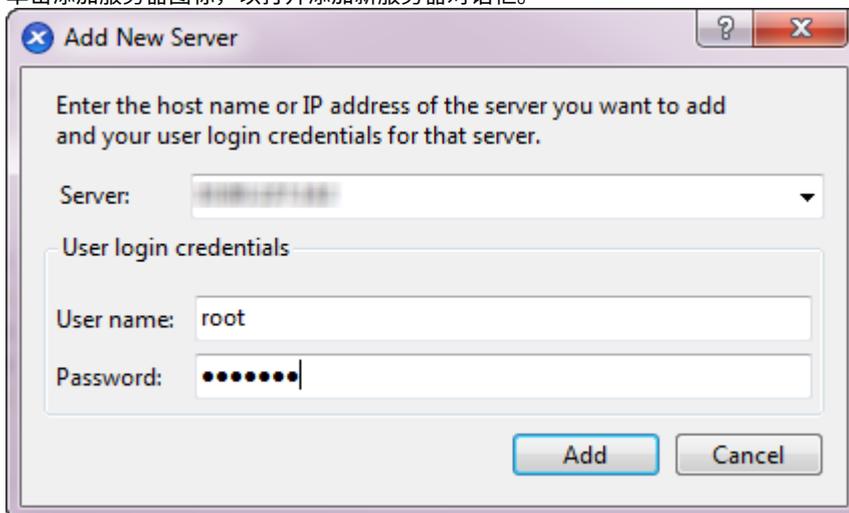
此过程允许您将主机添加到 XenCenter。

要将 XenCenter 连接到 Citrix Hypervisor 服务器，请执行以下操作：

1. 启动 XenCenter。  
程序将在主页选项卡打开。



2. 单击添加服务器图标，以打开添加新服务器对话框。



3. 在服务器字段中，输入主机的 IP 地址。输入在 Citrix Hypervisor 安装期间设置的 root 用户名和密码。选择添加。

注意：

首次添加主机时，将显示保存和还原连接状态对话框。在此对话框中，可以针对主机连接信息的存储及服务器连接的自动还原设置首选项。

## 许可证 Citrix Hypervisor

可以使用没有许可证的 Citrix Hypervisor（免费版）。但是，此版本还提供一组受限制的功能。

如果您有 Citrix Hypervisor 许可证，请立即应用。

有关详细信息，请参阅[许可](#)。

## 创建 Citrix Hypervisor 服务器池

一个资源池由多个 Citrix Hypervisor 服务器安装组成，这些主机绑定在一起形成一个托管实体。

在资源池中，您可以查看多个主机及其连接的作为单个统一资源的共享存储。可以根据资源需求和业务优先级灵活地跨资源池部署 VM。一个池中最多可以包含 64 台主机，这些主机都运行同一版本的 Citrix Hypervisor 软件（具有相同的修补程序级别），而且具有广泛的硬件兼容性。

池中的一个主机被指定为池主服务器。池主服务器为整个池提供单一联系点，以根据需要调整通信路由到池中的其他成员。如有需要，资源池的每个成员都将包含担任主服务器角色所需的所有信息。池主服务器是“XenCenter 资源”窗格中列出的池中的第一个主机。选择池主服务器，单击搜索选项卡，可以查找池主服务器的 IP 地址。

在具有共享存储的池中，可以在内存充足的任何池成员上启动 VM，并在主机之间动态移动 VM。VM 在运行时移动，最大程度地缩短了停机时间。如果单个 Citrix Hypervisor 服务器发生硬件故障，可以在同一个池中的另一台主机上重新启动出现故障的 VM。

如果启用了高可用性功能，则在出现主机故障时，受保护的 VM 将自动移动到其他主机。在启用高可用性的池中，如果主服务器已关闭，则将自动指定新的池主服务器。

### 注意：

有关同类池技术的说明，请参阅[主机和资源池](#)。

## 您将学习的内容

您将学习如何执行以下操作：

- 创建主机池
- 为池设置网络
- 绑定 NIC
- 为池设置共享存储

尽管 Citrix Hypervisor 支持许多共享存储解决方案，但本部分内容将重点介绍 NFS 和 iSCSI 这两种常用类型。

## 要求

要创建使用共享存储的池，您需要以下项目：

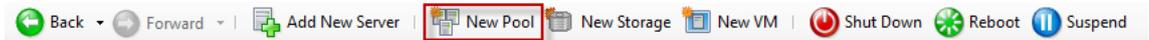
- 第二台 Citrix Hypervisor 服务器，配备相似的处理器类型。  
将此主机连接到您的 XenCenter 应用程序。
- 基于 IP 的存储的存储库

为帮助您快速入门，本节将重点介绍如何创建同类池。在同类池中，所有主机必须有兼容的处理器，并且运行相同版本的 Citrix Hypervisor，使用同一种类型的 Citrix Hypervisor 产品许可证。有关完整的同类池要求列表，请参阅[系统要求](#)。

## 创建池

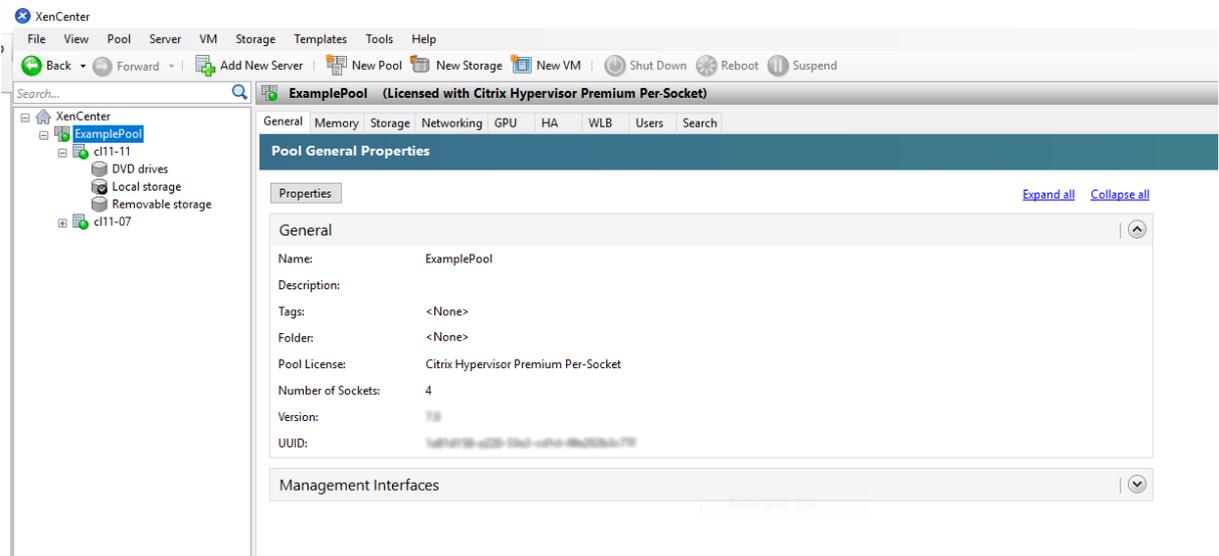
创建池：

1. 在工具栏上，单击新建池按钮。



2. 输入新池的名称和可选说明。
3. 从主服务器列表中选择主机，以指定池主服务器。
4. 从其他成员列表中，选择新池中要放置的第二个主机。
5. 单击创建池。

新池将显示在资源窗格中。



## 为池设置网络

安装 Citrix Hypervisor 时，可以创建网络连接，通常在您（在 Citrix Hypervisor 安装过程中）指定 IP 地址的池中的第一个 NIC 上创建。

但是，您可能需要将池连接到 VLAN 和其他物理网络。为此，您必须将这些网络添加到池中。您可以配置 Citrix Hypervisor，将每个 NIC 连接到一个物理网络和多个 VLAN。

创建网络之前，请确保布线与池中的每个主机相匹配。请将每个主机上的 NIC 插入与其他池成员中对应的 NIC 相同的物理网络中。

注意：

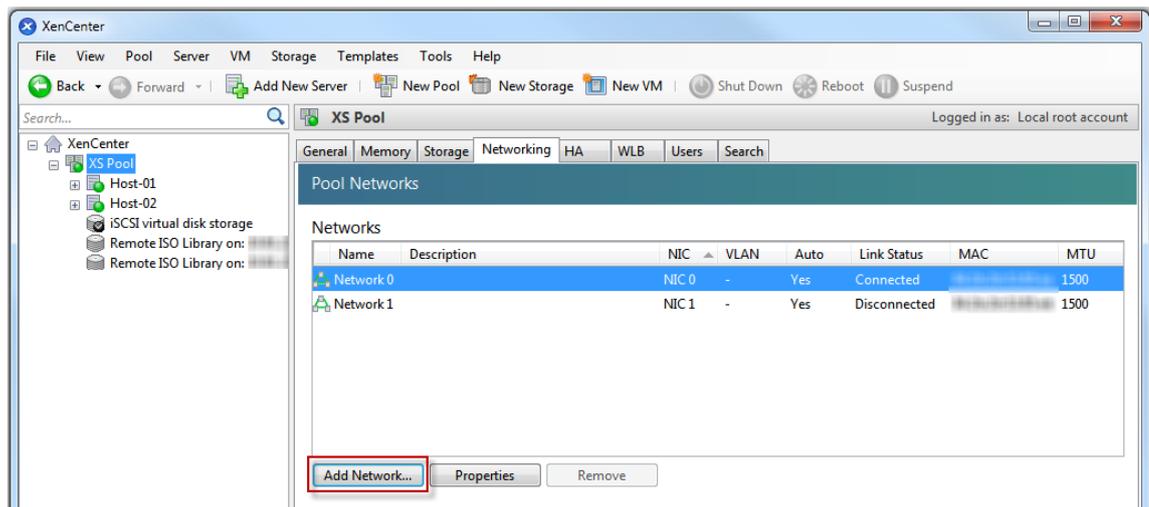
如果安装 Citrix Hypervisor 时未将 NIC 插入到主机上的 NIC 中：

- 将 NIC 插入到
- 在 XenCenter 中，选择 < 您的主机 > > **NIC** 选项卡
- 单击重新扫描使其显示

有关配置 Citrix Hypervisor 网络连接的其他信息，请参阅 *XenCenter* 帮助和[网络连接](#)。

要将网络添加到 Citrix Hypervisor，请执行以下命令：

1. 在 XenCenter 的资源窗格中，选择池。
2. 单击网络连接选项卡。
3. 单击添加网络。



4. 在选择类型页面上，选择外部网络，单击下一步。
5. 在名称页面上，输入有意义的网络名称和说明。
6. 在网络设置页面上，指定以下选项：
  - **NIC**：选择希望 Citrix Hypervisor 用来向网络发送和从网络接收数据的 NIC。
  - **VLAN**：如果网络是 VLAN，请输入 VLAN ID（或“标记”）。
  - **MTU**：如果网络使用巨型帧，请输入一个最大传输单位 (MTU) 值，介于 1500 到 9216 之间。否则，请将 MTU 框保留为其默认值 1500。

如果将许多虚拟机配置为使用此网络，则可以选中自动将此网络添加到新虚拟机复选框。此选项默认添加网络。

7. 单击完成。

## 绑定 NIC

NIC 绑定可以将两个或多个物理 NIC 当作一个高性能通道使用，从而提高服务器的恢复能力。本部分内容提供非常简单的绑定概述，又称为 NIC 绑定。在配置用于生产环境的绑定之前，我们建议阅读有关绑定的更多详细信息。有关详细信息，请参阅[网络连接](#)。

Citrix Hypervisor 支持以下绑定模式：主动/主动、主动/被动（主动/备用）和 LACP。主动/主动可以为基于 VM 的流量提供负载平衡和冗余。对于其他流量类型（存储和管理），主动/主动不能对流量进行负载平衡。因此，对于存储流量，最好选择 LACP 或多路径。有关多路径的信息，请参阅[存储](#)。有关绑定的详细信息，请参阅[网络连接](#)。

LACP 选项不可见或不可用，除非将 vSwitch 配置为网络堆栈。同样，交换机必须支持 IEEE 802.3ad 标准。交换机必须包含为主机上的每个 LACP 绑定配置的单独的 LAG 组。有关创建 LAG 组的更多详细信息，请参阅[网络连接](#)。

要绑定 NIC，请执行以下操作：

1. 确保要绑定在一起的 NIC（绑定从属对象）未在使用中：在创建绑定之前，请关闭任何其虚拟网络接口使用绑定从属对象的 VM。创建绑定后，您需要将虚拟网络接口重新连接至相应的网络。
2. 在资源窗格中选择服务器，然后打开 **NIC** 选项卡并单击创建绑定。
3. 选择想要绑定在一起的 NIC。要选择某 NIC，请在列表选中其复选框。在列表中最多可以选择四个 NIC。清除该复选框可取消选择 NIC。为了保持灵活安全的网络，当 vSwitch 是网络堆栈时，可以绑定两个、三个或四个 NIC。但是，当 Linux 桥接是网络堆栈时，只能绑定两个 NIC。
4. 在绑定模式下，选择绑定类型：
  - 选择主动-主动可配置主动-主动绑定。流量将在两个绑定的 NIC 之间平衡。如果绑定中的一个 NIC 出现故障，主机服务器的网络流量将自动通过第二个 NIC 进行路由。
  - 选择主动-被动可配置主动-被动绑定。流量仅通过其中一个绑定的 NIC 传输。在此模式下，仅当活动 NIC 出现故障时（例如，断开网络连接），第二个 NIC 才会进入活动状态。
  - 选择 **LACP** 与基于源 **MAC** 地址的负载平衡功能绑定可配置 LACP 绑定。传出 NIC 将根据发起流量的 VM 的 MAC 地址进行选择。使用该选项可以在同一主机上有多个 VM 的环境中平衡流量。如果虚拟接口 (VIF) 的数量少于 NIC，此选项则不适用：因为无法在 NIC 之间分割流量，所以无法实现最佳负载平衡。
  - 选择 **LACP** 与基于源和目标的 **IP** 和端口的负载平衡功能绑定可配置 LACP 绑定。源 IP 地址、源端口号、目标 IP 地址和目标端口号用于在 NIC 之间分配流量。使用该选项可以在 NIC 数量超过 VIF 数量的环境中平衡 VM 的流量。

**注意：**

LACP 绑定仅适用于 vSwitch，而主动-主动和主动-被动绑定模式适用于 vSwitch 和 Linux 桥接。  
有关网络堆栈的信息，请参阅[网络连接](#)。

5. 要使用 Jumbo 帧，请将最大传输单位 (MTU) 设置为介于 1500 到 9216 之间的值。
6. 要将新绑定的网络自动添加到使用新建 VM 向导创建的任何新 VM，请选中该复选框。
7. 单击创建以创建 NIC 绑定并关闭对话框。

XenCenter 会在创建新绑定后自动将管理接口和辅助接口从绑定从属对象移至绑定主对象。不允许将管理接口属于某个绑定的服务器加入池。必须先重新配置管理接口并将其移回物理 NIC，服务器才能加入池。

#### 为池设置共享存储

要将池中的主机连接到远程存储阵列，请创建一个 Citrix Hypervisor SR。SR 是存储 VM 的虚拟磁盘的存储容器。SR 是磁盘上持久对象，独立于 Citrix Hypervisor 存在。SR 可以存在于不同类型的物理存储设备上（内部和外部）。这些类型包括本地磁盘设备和共享网络存储。

可以为多种不同的存储类型配置 Citrix Hypervisor SR，其中包括：

- NFS
- 软件 iSCSI
- 硬件 HBA
- SMB
- 光纤通道
- 软件 FCoE

本节将分步骤指导您为主机池设置两种类型的共享 SR：NFS 和 iSCSI。在开始创建 SR 之前，请配置 NFS 或 iSCSI 存储阵列。具体设置因所用存储解决方案的类型而异。有关详细信息，请参阅供应商的文档。通常情况下，在开始操作之前，请完成以下存储解决方案的设置：

- **iSCSI SR**：必须在存储阵列上创建卷和 LUN。
- **NFS SR**：必须在存储设备上创建卷。
- 硬件 **HBA**：必须在运行“新建存储库”向导之前完成公开 LUN 所需的配置
- 软件 **FCoE SR**：必须手动完成将 LUN 显示给主机所需的配置。此设置包括配置 FCoE 架构以及将 LUN 分配给 SAN 的公共全球通用名称 (PWWN)。

如果要为基于 IP 的存储（iSCSI 或 NFS）创建 SR，可以将下列 NIC 之一配置为存储网络：处理管理流量的 NIC 或面向存储流量的新 NIC。要为存储流量配置不同的 NIC，必须通过创建管理接口为 NIC 分配一个 IP 地址。

创建管理接口时，必须为其分配一个满足以下条件的 IP 地址：

- 如果适用，IP 地址应与存储控制器位于同一子网中
- IP 地址所在的子网与您在安装时指定的 IP 地址不同 Citrix Hypervisor
- IP 地址不与任何其他管理接口位于相同的子网中。

要为 NIC 分配 IP 地址，请执行以下操作：

1. 确保 NIC 位于独立子网中或将路由配置为适合您的网络拓扑。此配置强制所需的流量通过所选 INC 进行传输。
2. 在 XenCenter 的资源窗格中，选择池（或独立服务器）。单击网络连接选项卡，然后单击配置按钮。
3. 在配置 IP 地址对话框中，在左侧窗格中，单击添加 IP 地址。

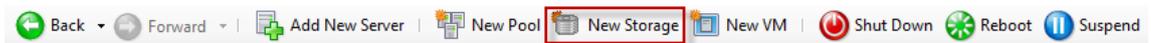
4. 为新接口提供一个有意义的名称（例如，*yourstoragearray\_network*）。选择与用于存储流量的 NIC 相关联的网络。
5. 单击使用以下网络设置。输入要在 NIC、子网掩码和网关上配置的静态 IP 地址。单击确定。此 IP 地址必须与 NIC 连接到的存储控制器位于同一子网上。

注意：

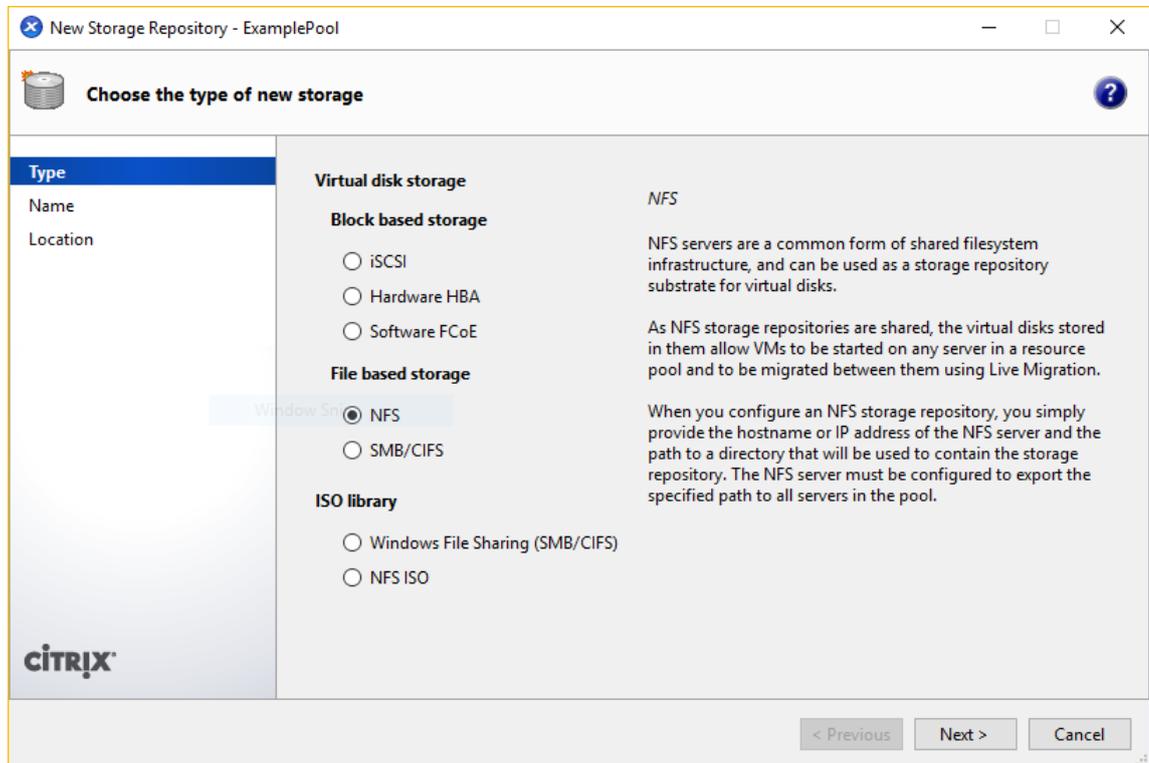
无论何时为 NIC 分配 IP 地址，必须与池中任何其他拥有 IP 地址的 NIC 位于不同子网中。这包括主管理接口。

创建新的 NFS 或 iSCSI 共享存储库：

1. 在资源窗格中，选择池。在工具栏上，单击新建存储按钮。



此时将打开新建存储库向导。



2. 在“虚拟磁盘存储”下，选择“NFS”或“iSCSI”作为存储类型。单击“下一步”继续操作。
3. 如果选择 NFS：

- a) 输入新 SR 的名称及其所在共享的名称。单击扫描，让向导在指定位置扫描现有的 NFS SR。

注意：

必须将配置为 NFS 服务器导出池中所有 Citrix Hypervisor 服务器的指定路径。

- b) 单击完成。

新 SR 将显示在资源窗格的该池中。

#### 4. 如果选择 iSCSI:

- a) 输入新 SR 的名称，以及 iSCSI 目标的 IP 地址或 DNS 名称。

注意:

该 iSCSI 存储目标必须配置为允许池中的每个 Citrix Hypervisor 服务器访问一个或多个 LUN。

- b) 如果已将 iSCSI 目标配置为使用 CHAP 身份验证，请输入用户名和密码。

- c) 单击扫描目标主机按钮，然后从“目标 IQN”列表中选择 iSCSI 目标 IQN。

警告:

iSCSI 目标以及池中的所有服务器必须具有唯一的 IQN。

- d) 单击目标 **LUN** 按钮，然后从“目标 LUN”列表中选择用来创建 SR 的 LUN。

警告:

每个 iSCSI 存储库必须完全包含在单个 LUN 中，不能跨多个 LUN 分布。否则在所选 LUN 上的所有数据都将被毁坏。

- e) 单击完成。

新 SR 将显示在资源窗格的该池中。

现在新的共享 SR 将成为该池的默认 SR。

#### 创建虚拟机

通过 XenCenter，可以使用多种方法创建虚拟机，具体取决于您的需求。无论您是要部署具有不同配置的各个 VM，还是要部署包含多个相似 VM 的组，XenCenter 都只需几个步骤即可启动并运行这些 VM。

Citrix Hypervisor 还提供一种从 VMware 转换批量虚拟机的简单方法。有关详细信息，请参阅[Conversion Manager](#)。

本部分内容重点介绍几种创建 Windows VM 的方法。为帮助您快速入门，这些过程使用最简单的 Citrix Hypervisor 设置：具有本地存储的单个 Citrix Hypervisor 服务器（将 XenCenter 连接到 Citrix Hypervisor 服务器后，即会在该主机的本地磁盘上自动配置存储）。

本部分内容还将介绍如何使用实时迁移功能在池中的各主机之间实时迁移 VM。

解释如何创建和自定义新 VM 后，本部分内容将介绍如何将该现有 VM 转换为 VM 模板。VM 模板会保留您的自定义设置，使您可以始终使用模板创建具有相同（或相似）规格的 VM。它还可以缩短创建多个 VM 所需的时间。

也可以通过现有 VM 的快照创建 VM 模板。快照是运行中的 VM 在某个时间点的记录。快照可保存原始 VM 的存储、配置和网络连接信息，是非常有用的备份方式。快照可提供快速创建 VM 模板的方式。本部分内容将介绍如何生成现有 VM 的快照，然后如何将该快照转换为 VM 模板。最后，本部分内容还将介绍如何基于 VM 模板创建新 VM。

### 您将学习的内容

您将学习如何执行以下操作：

- 创建 Windows 8.1 VM
- 安装 Citrix VM Tools
- 在池中的两台主机之间迁移运行中的 VM
- 创建 VM 模板
- 基于 VM 模板创建 VM

### 要求

要创建使用共享存储的池，您需要以下项目：

- 您设置的 Citrix Hypervisor 池
- XenCenter
- Windows 8.1 的安装文件

### 创建 **Windows 8.1 (32 位) VM**

注意：

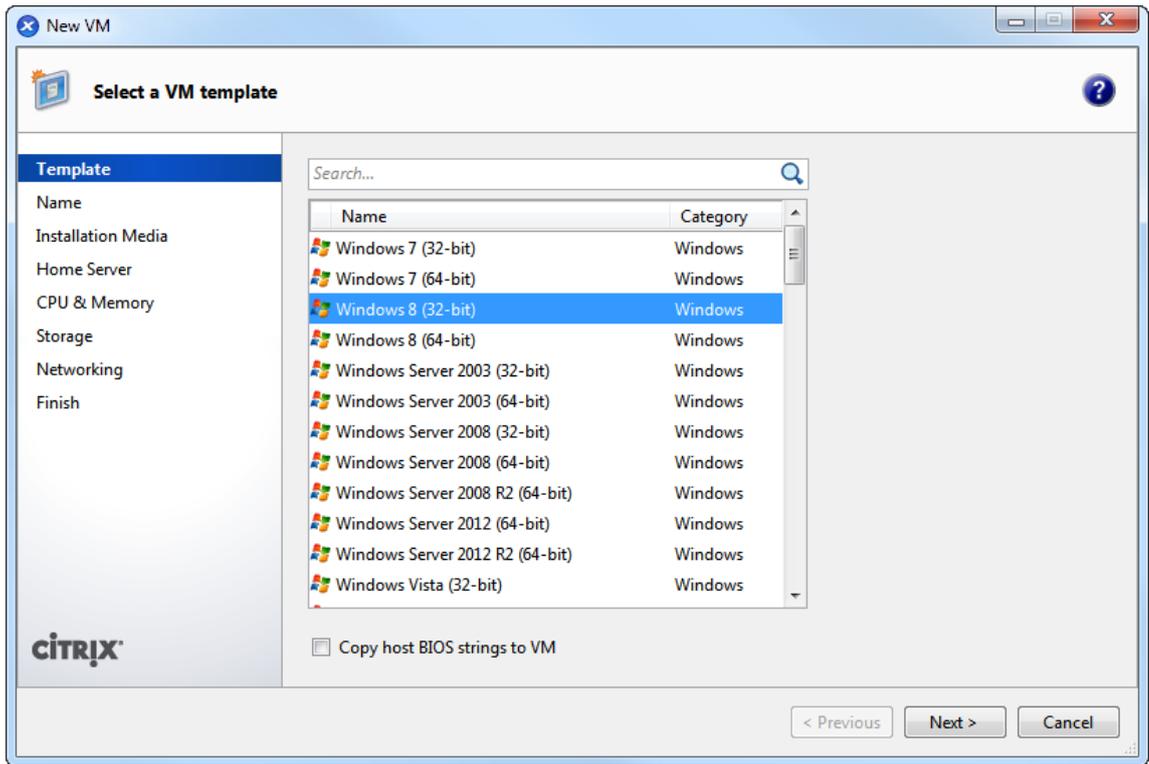
以下过程举例说明创建 Windows 8.1 (32 位) VM 的步骤。默认值可能因您选择的操作系统而异。

创建 Windows VM：

1. 在工具栏上，单击新建 **VM** 按钮以打开“新建 VM”向导。



通过“新建 VM”向导，可以配置新 VM，调整 CPU、存储和网络连接资源的各种参数。



2. 选择一个 VM 模板，然后单击下一步。

每个模板包含创建具有特定来宾操作系统和最佳存储的新 VM 所需的设置信息。此列表列出了 Citrix Hypervisor 当前支持的模板。

注意：

如果要在新 VM 上安装的操作系统仅与原始硬件兼容，请选中将主机 **BIOS** 字符串复制到 **VM** 框。例如，请对与特定计算机打包在一起的操作系统的安装 CD 使用此选项。

3. 为新 VM 输入名称和可选说明。
4. 为将安装在新 VM 上的操作系统选择安装源。

通过 CD/DVD 安装是最简单的入门方法。选择默认安装源选项（DVD 驱动器），将光盘插入 Citrix Hypervisor 服务器的 DVD 驱动器中，然后选择下一步以继续操作。

Citrix Hypervisor 还允许您从多种来源提取操作系统安装介质，包括预先存在的 ISO 库。

要附加已存在的 ISO 库，请单击新建 **ISO** 库并指明 ISO 库的位置和类型。然后可以从列表中选择特定的操作系统 ISO 介质。

5. VM 将在安装的主机上运行。选择下一步继续操作。
6. 分配处理器和内存资源。

对于 Windows 8.1 VM，默认为 1 个虚拟 CPU，1 个插槽（每插槽 1 个核心），2 GB RAM。如有需要，可以选择修改默认设置。单击下一步继续操作。

注意：

每个操作系统都具有不同的配置要求，这些要求将反映在模板中。

#### 7. 分配图形处理器 (GPU)。

新建 **VM** 向导会提示您将专用 GPU 或虚拟 GPU 分配给 VM。此选项使 VM 能够使用 GPU 的处理能力。此选项为 CAD、GIS 和医学成像应用程序等高端三维专业图形应用程序提供更好的支持。

注意：

GPU 虚拟化适用于 Citrix Hypervisor Premium Edition 客户或通过其 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。

#### 8. 为新 VM 配置存储。

单击下一步选择默认分配 (24 GB) 和配置，或者您可能需要：

- a) 通过单击属性更改虚拟磁盘的名称、说明或大小。
- b) 选择添加，添加一个新虚拟磁盘。

注意：

创建 Citrix Hypervisor 服务器池期间，如果正在创建新 VM，可以在此时配置共享存储。

#### 9. 配置新 VM 的网络连接设置。

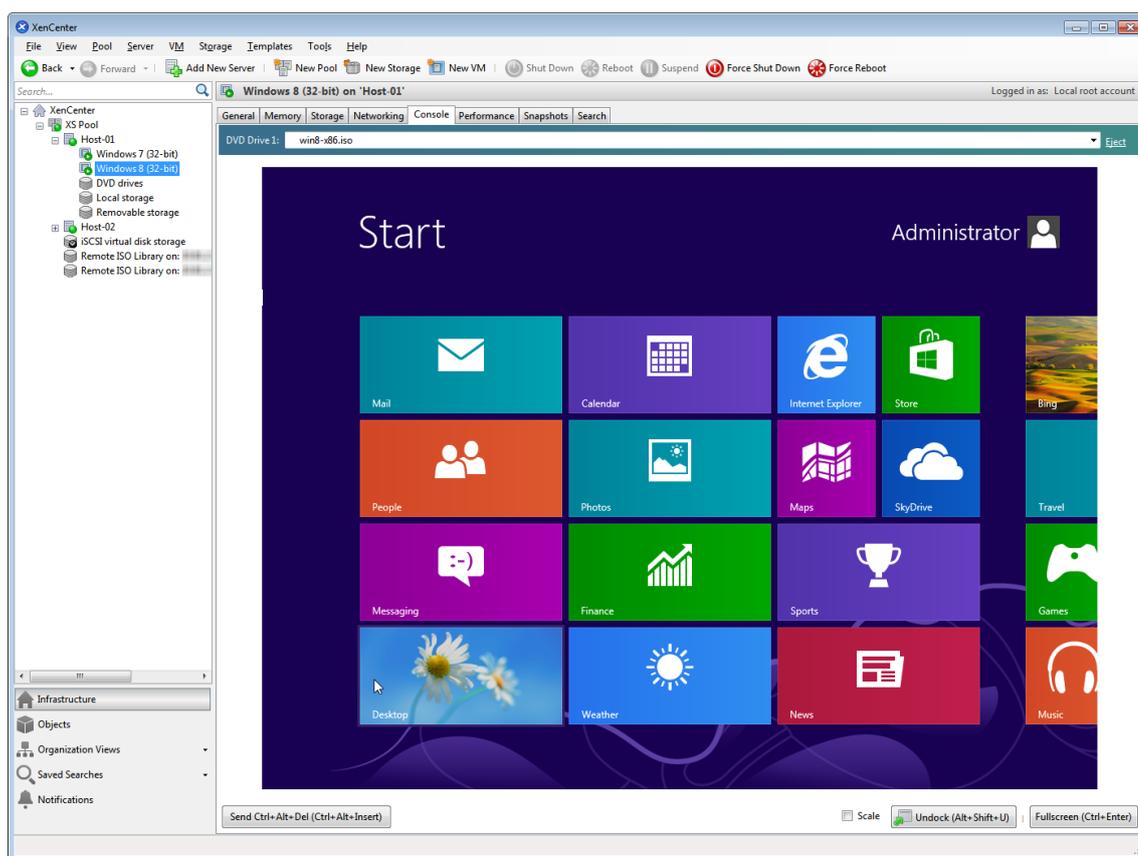
单击下一步选择默认 NIC 和配置，包括为每个 NIC 自动创建的唯一 MAC 地址，或者可以：

- a) 通过单击属性更改虚拟磁盘的物理网络、MAC 地址或服务质量 (QoS) 优先级。
- b) 选择添加，以添加一个新虚拟网络接口。

Citrix Hypervisor 使用虚拟网络接口连接到主机上的物理网络。请务必选择与虚拟机所需的网络对应的网络。要添加物理网络，请参阅为池设置网络

#### 10. 检查设置，然后单击立即创建以创建新 VM 并返回到搜索选项卡。

新 VM 的图标显示在资源窗格中的主机下。



在资源窗格中，选择该 VM，然后单击控制台选项卡以查看 VM 控制台。

11. 按照操作系统安装屏幕上的说明操作并进行选择。
12. 操作系统安装完成并重新启动 VM 后，安装 Citrix VM Tools。

### 安装 Citrix VM Tools

Citrix VM Tools 提供高性能 I/O 服务，而没有传统设备仿真的开销。Citrix VM Tools 由 I/O 驱动程序（也称为半虚拟化的驱动程序或 PV 驱动程序）和管理代理组成。Citrix VM Tools 必须安装在每个 VM 上，才能使 VM 具有完全受支持的配置。VM 可以在未安装这些工具的情况下运行，但性能会降低。Citrix VM Tools 还支持某些功能和特性，包括彻底关闭、重新启动、挂起和实时迁移 VM。

#### 警告：

为每个 Windows VM 安装 Citrix VM Tools。不支持运行未安装 Citrix VM Tools 的 Windows VM。

要安装 Citrix VM Tools，请执行以下操作：

1. 在“资源”窗格中选择 VM，单击鼠标右键，然后单击快捷菜单中的安装 **Citrix VM Tools**。或者，在 VM 菜单中，单击安装 **Citrix VM Tools**。

或

在 VM 的常规选项卡中，单击安装 **I/O** 驱动程序和管理代理。

注意：

在 VM 上安装 Citrix VM Tools 时将同时安装 I/O 驱动程序（PV 驱动程序）和管理代理。

2. 如果针对 VM 的 CD/DVD 驱动器启用了自动播放功能，则片刻之后安装过程将自动启动。此过程会安装 I/O 驱动程序和管理代理，并根据需要重新启动 VM。
3. 如果未启用自动播放功能，Citrix VM Tools 安装程序将显示安装选项。单击安装 **Citrix VM Tools** 继续进行安装。此时将在 VM 的 CD/DVD 驱动器上装载 Citrix VM Tools ISO (`guest-tools.iso`)。
4. 单击运行 **setup.exe** 开始安装 Citrix VM Tools，并在系统提示时重新启动 VM 以完成安装过程。

注意：

I/O 驱动程序将自动安装在可从 Windows Update 接收更新的 Windows VM 上。但是，我们建议您通过安装 Citrix VM Tools 软件包来安装管理代理，并确保配置始终受支持。以下功能仅适用于 Citrix Hypervisor Premium Edition 客户或通过其 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。

- 能够从 Windows Update 接收 I/O 驱动程序
- 自动更新管理代理

安装完 Citrix VM Tools 后，可以安装应用程序并执行任何其他配置，以便对 VM 进行自定义。如果要创建具有相似规格等多个 VM，可以基于现有 VM 生成一个模板，这种方式可以快速创建相似等多个 VM。请使用该模板创建 VM。有关详细信息，请参阅创建 VM 模板。

#### 在池中的两台主机之间迁移正在运行的 VM

使用实时迁移功能，可以在同一个池中的各个主机之间移动正在运行的 VM，而几乎不会造成服务中断。决定在哪里迁移 VM 取决于该 VM 和池的配置。

要迁移正在运行的 VM，请执行以下操作：

1. 在资源窗格中，选择要移动的 VM。

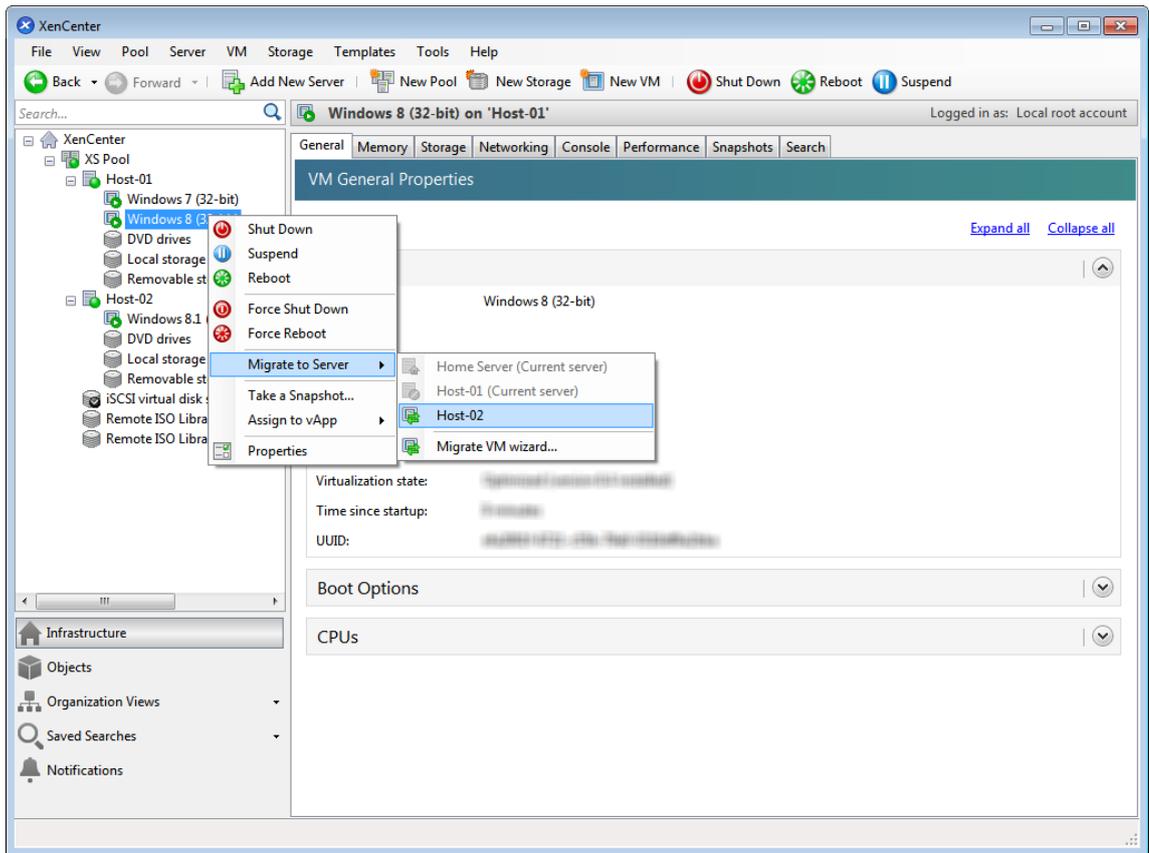
注意：

确保迁移的 VM 不具有本地存储。

2. 在 VM 图标上单击鼠标右键，指向迁移到服务器，然后选择新的 VM 主机。

提示：

也可以将该 VM 拖动到目标主机上。



3. 迁移后的 VM 将显示在资源窗格中的新主机下。

### 创建 VM 模板

基于现有 Windows VM 创建 VM 模板的方法有多种，每一种方法都有各自的优点。本节重点介绍两种方法：将现有 VM 转换为模板，以及基于 VM 的快照创建模板。在这两种情况下，VM 模板均可保留原始 VM 或 VM 快照的自定义配置。然后可以使用该模板快速创建多个新的相似 VM。本节还将介绍如何基于这些模板创建新 VM。

在基于现有 VM 或 VM 快照创建模板之前，我们建议您在原始 VM 上运行 Windows 实用程序 *Sysprep*。通常，运行 *Sysprep* 可以使操作系统做好磁盘克隆和还原的准备。每个 Windows 操作系统安装都包含许多唯一的元素（包括安全标识符和计算机名称）。这些元素必须保持唯一，不能复制到新 VM。如果复制这些元素，很可能导致混淆和问题。运行 *Sysprep* 可以允许为新 VM 生成新的唯一元素，从而避免这些问题。

#### 注意：

对于基本部署或测试环境可能不需要运行 *Sysprep*，因为它适用于生产环境。

有关 *Sysprep* 的详细信息，请参阅 Windows 文档。运行此实用程序的详细过程因安装的 Windows 版本而异。

### 基于现有 VM 创建 VM 模板

基于现有 VM 创建 VM 模：

警告:

基于现有 VM 创建模板时，新模板将替换原始 VM。该 VM 不再存在。

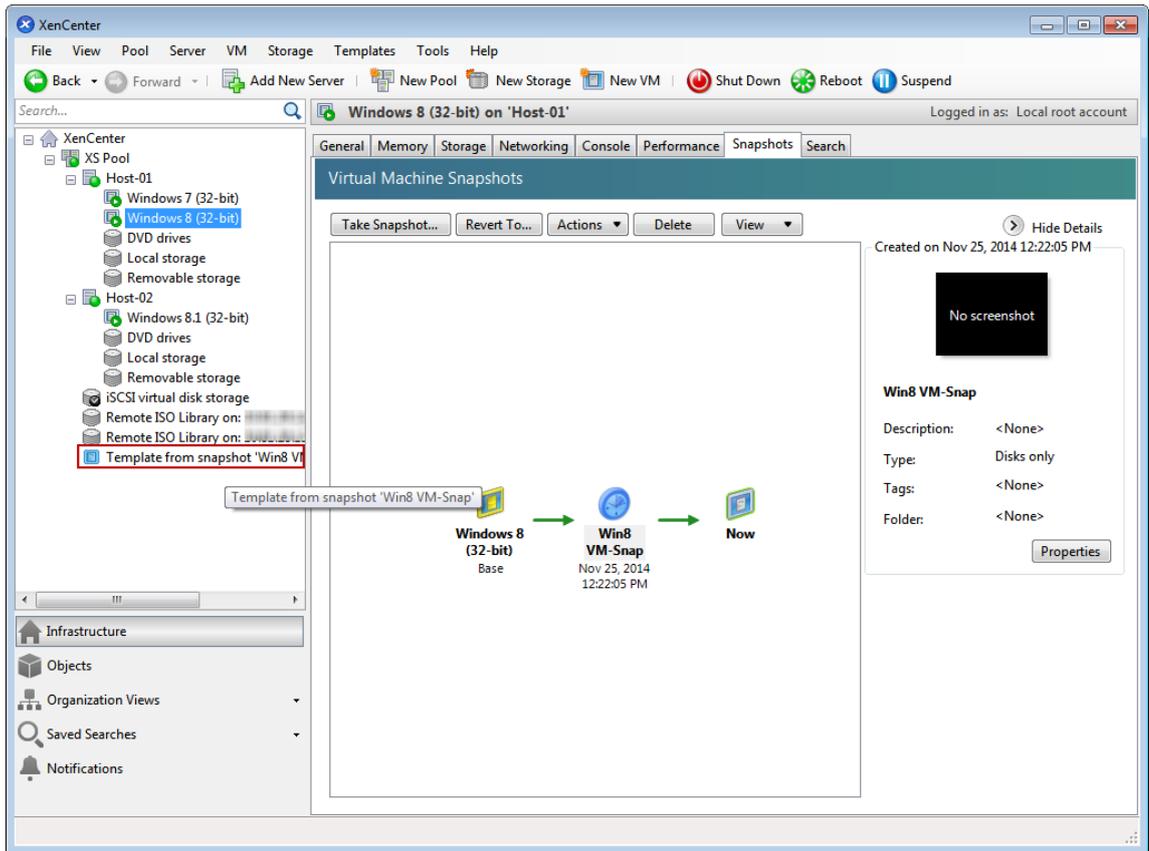
1. 关闭要转换的 VM。
2. 在资源窗格中，在该 VM 上单击鼠标右键，然后选择转换为模板。
3. 单击转换进行确认。

创建模板后，新的 VM 模板将显示在资源窗格中，替换现有的 VM。

基于 VM 快照创建 VM 模板

基于 VM 快照创建模板:

1. 在资源窗格中，选择 VM。单击快照选项卡，然后单击生成快照。
2. 输入新快照的名称和可选说明。单击生成快照。
3. 快照创建完成后会在快照选项卡上显示相关图标，请选择该图标。



4. 在操作列表中，选择另存为模板。
5. 输入模板的名称，然后单击创建。

## 基于 VM 模板创建 VM

要基于自定义 VM 模板创建 VM，请执行以下操作：

1. 在 XenCenter 资源窗格中，在该模板上单击鼠标右键，然后选择新建 **VM** 向导。

此时将打开新建 **VM** 向导。

2. 按照新建 **VM** 向导中的说明进行操作，基于选定模板创建 VM。

注意：

当向导提示您选择操作系统安装介质源时，请选择默认设置并继续。

新 VM 将显示在资源窗格中。

如果使用的模板是基于现有 VM 创建的，还可以选择快速创建选项。此选项不引导您完成新建 **VM** 向导。相反，此选项将立即使用在您的模板中指定的所有配置设置创建并预配一个新 VM。

## 技术概述

July 10, 2019

Citrix Hypervisor 是业界领先的开源平台，实现了经济高效的桌面、服务器和云虚拟化基础结构。通过 Citrix Hypervisor，任意规模或类型的组织都能够整合计算资源并将其转换为虚拟工作负载以满足当今数据中心的要求。同时可以确保将工作负载无缝移动到云中。

Citrix Hypervisor 的主要功能包括：

- 将多个虚拟机 (VM) 整合到一个物理服务器中
- 降低要管理的独立磁盘映像的数量
- 允许与现有网络连接和存储基础结构轻松集成
- 允许您在 Citrix Hypervisor 主机之间实时迁移 VM，在确保零停机时间的情况下安排维护工作
- 使用高可用性功能配置相应的策略（当一台服务器出现故障时在另一台服务器上重新启动 VM），从而确保 VM 的可用性
- 提高 VM 映像的可移植性，因为一个 VM 映像将在一系列部署基础结构中运行

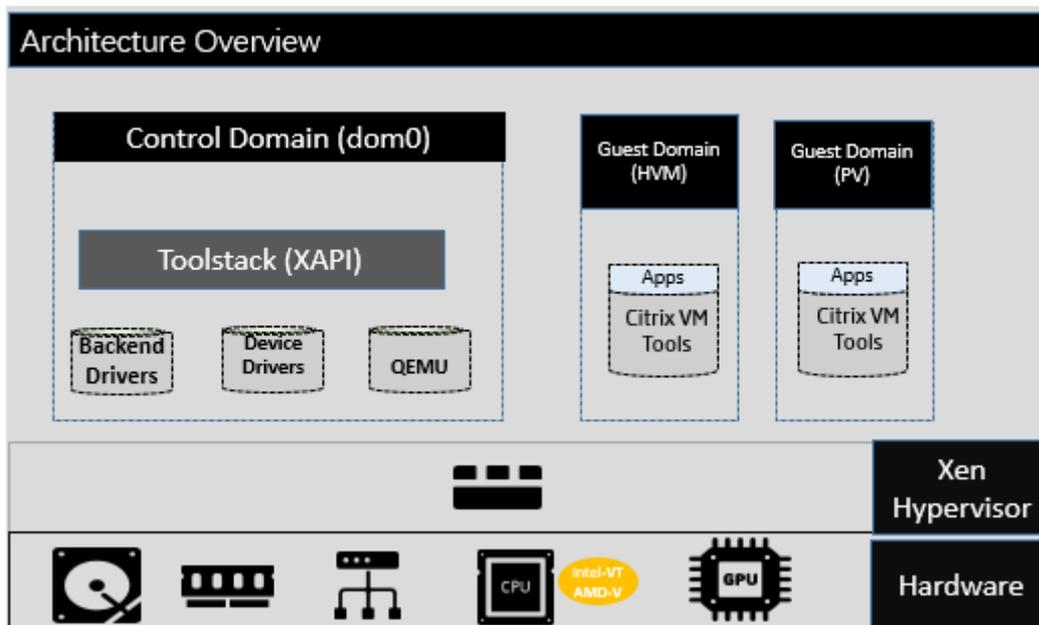
## 虚拟化和虚拟机管理程序

虚拟化（更具体而言，硬件虚拟化）是一种在单个物理机上运行多个独立 VM 的方法。这些虚拟机上运行的软件与基础硬件资源分隔开来。这是一种充分利用最新的功能强大的服务器中可用的物理资源的方式，能够降低服务器部署的总体拥有成本 (TCO)。

虚拟机管理程序是软件的基础抽象层。虚拟机管理程序执行底层任务（例如 CPU 调度），并且负责常驻 VM 的内存隔离。虚拟机管理程序提取 VM 的硬件。虚拟机管理程序无法识别网络连接、外部存储设备及视频等。

## 主要组件

本部分内容将介绍 Citrix Hypervisor 的高级工作原理。请参见下图，了解 Citrix Hypervisor 的主要组件：



## 硬件

硬件层包含物理服务器组件，例如 CPU、内存、网络和磁盘驱动器。

您需要配备了一个或多个 CPU 的基于 Intel VT 或 AMD-V 64 位 x86 的系统，才能运行所有受支持的操作系统。有关 Citrix Hypervisor 主机系统要求的详细信息，请参阅“系统要求”。

有关 Citrix Hypervisor 认证的硬件和系统的完整列表，请参阅[硬件兼容性列表 \(HCL\)](#)。

## Xen 虚拟机管理程序

Xen Project 虚拟机管理程序是开放源类型 1 或裸机虚拟机管理程序。此虚拟机管理程序允许一个操作系统或不同操作系统的实例在单个计算机（或主机）上并行运行。Xen 虚拟机管理程序用作许多不同的商务应用程序和开源应用程序的基础，例如：服务器虚拟化、基础结构即服务 (IaaS)、桌面虚拟化、安全应用程序、嵌入式设备以及硬件设备。

Citrix Hypervisor 基于 Xen Project 虚拟机管理程序，具有 Citrix 提供的额外功能和支持。Citrix Hypervisor 8.0 使用版本为 4.11 的 Xen 虚拟机管理程序。

## 控制域

控制域又称为“Domain 0”或“dom0”，是一个运行 Citrix Hypervisor 管理 Toolstack（称为 XAPI）的安全的特权 Linux VM。此 Linux VM 基于 CentOS 7.5 发行版。除提供 Citrix Hypervisor 管理功能外，dom0 还运行适用于网络连接、存储等的物理设备驱动程序。控制域可以与虚拟机管理程序通信，指示其启动或停止来宾 VM。

## Toolstack

**Toolstack** 或 XAPI 是控制 VM 生命周期操作、主机和 VM 网络连接、VM 存储以及用户身份验证的软件堆栈。此外，还允许管理 Citrix Hypervisor 资源池。

XAPI 提供了一种公开记录的管理 API，可供所有管理 VM 和资源池的工具使用。有关详细信息，请参阅<https://developer-docs.citrix.com>。

## 来宾域 (VM)

来宾域是用户创建的从 dom0 请求资源的虚拟机。Citrix Hypervisor 中的来宾域支持完全虚拟化 (HVM)、半虚拟化 (PV) 和 HVM 上的 PV。有关受支持的发行版的详细列表，请参阅[支持的来宾系统、虚拟内存和磁盘大小限制](#)。

### 完全虚拟化

完全虚拟化或硬件协助虚拟化使用来自主机 CPU 的虚拟化扩展对来宾进行虚拟化。完全虚拟化的来宾不需要任何内核支持。来宾被称为硬件虚拟机 (HVM)。HVM 需要 Intel VT 或 AMD-V 硬件扩展来执行内存和特权操作。Citrix Hypervisor 使用 Quick Emulator (QEMU) 来模拟 PC 硬件，包括 BIOS、IDE 磁盘控制器、VGA 图形适配器、USB 控制器、网络适配器等。为提高硬件敏感操作（例如磁盘或网络访问）的性能，将随 Citrix Hypervisor 工具安装 HVM 来宾。有关详细信息，请参阅 HVM 上的 PV。

HVM 通常在对操作系统进行虚拟化时使用，例如能够在其中修改内核以使其识别虚拟化的 Microsoft Windows。

### 半虚拟化 (PV)

半虚拟化是一种高效的轻型虚拟化技术，最初由 Xen Project 引入，之后由其他虚拟化平台采用。PV 不需要来自主机 CPU 的虚拟化扩展。但是，PV 来宾需要启用了 PV 的内核和 PV 驱动程序，以便来宾能够识别虚拟机管理程序，并且能够有效地运行而不需要虚拟的仿真硬件。Linux、NetBSD、FreeBSD 和 Open Solaris 中存在启用了 PV 的内核。有关受支持的处于 PV 模式的发行版的列表，请参阅 [PV Linux 发行版](#)。

对于 PV 来宾，Xen 虚拟机管理程序会将 I/O 操作请求转发到控制域。来宾可以识别虚拟机管理程序，并将特权指令发送到虚拟机管理程序。

### HVM 上的 PV

HVM 上的 PV 是半虚拟化与完全硬件虚拟化的混合。主要目标是通过使用专门优化的半虚拟化驱动程序来大幅提高 HVM 来宾的性能。此模式允许您利用更新的处理器中的 x86 虚拟容器技术来提高性能。从这些来宾访问网络和存储仍将使用内核中内置的驱动程序在 PV 模式下运行。

Windows 和部分 Linux 发行版在 Citrix Hypervisor 中的“HVM 上的 PV”模式下提供。有关受支持的使用“HVM 上的 PV”的 Linux 发行版的列表，请参阅 [HVM Linux 发行版](#)。

## Citrix VM Tools

Citrix VM Tools 或来宾工具提供高性能 I/O 服务，而没有传统设备仿真的开销。Citrix VM Tools 由 I/O 驱动程序（也称为半虚拟化的驱动程序或 PV 驱动程序）和管理代理组成。

I/O 驱动程序包括前端存储和网络驱动程序以及底层管理接口。这些驱动程序可替代仿真设备，并在 VM 与 Citrix Hypervisor 产品系列软件之间提供高速传输。

管理代理（也称为来宾代理）负责高级虚拟机管理功能。该管理代理向 XenCenter（适用于 Windows VM）提供包括静止快照在内的完整功能。

### 注意：

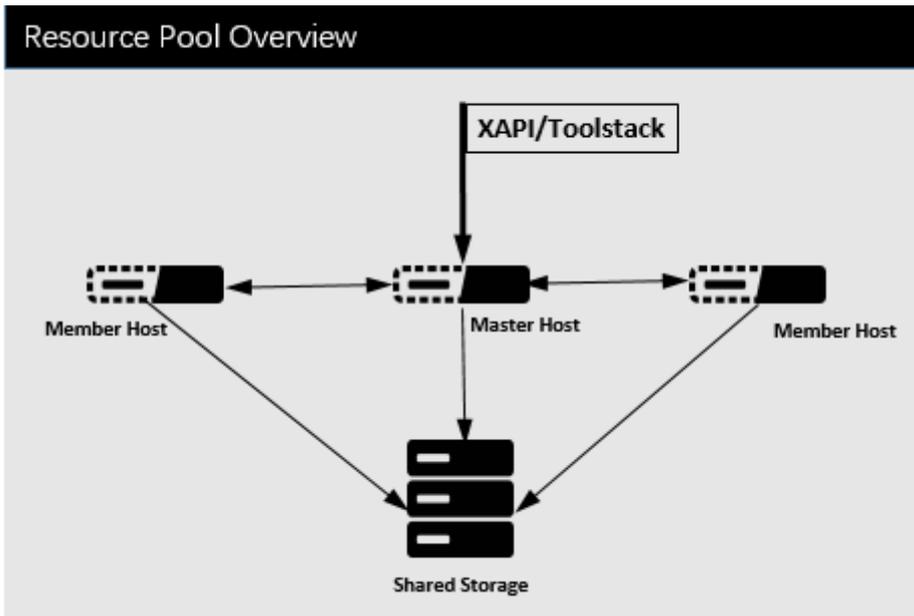
- Citrix VM Tools 必须安装在每个 Windows VM 上，才能使 VM 具有完全受支持的配置。VM 在未安装 Citrix VM Tools 的情况下可以正常工作，但如果不安装 I/O 驱动程序（PV 驱动程序），性能将受到极大影响。
- 对于 Windows VM，Citrix VM Tools 称为 Windows 来宾工具，其中包括 Windows PV 驱动程序和管理代理。
- 对于 Linux VM，PV 驱动程序已包含在 Xen 内核中。

有关详细信息，请参阅[Citrix VM Tools](#)。

## 主要概念

### 资源池

Citrix Hypervisor 允许您使用资源池作为单个实体来管理多个服务器及其连接的共享存储。通过资源池，您可以在不同的 Citrix Hypervisor 主机之间移动和运行虚拟机。此外，还允许所有服务器共享网络和存储的通用框架。一个池中最多可以包含 64 台服务器，这些服务器都运行同一版本的 Citrix Hypervisor 软件（具有相同的修补程序级别），而且具有广泛的硬件兼容性。有关详细信息，请参阅[主机和资源池](#)。



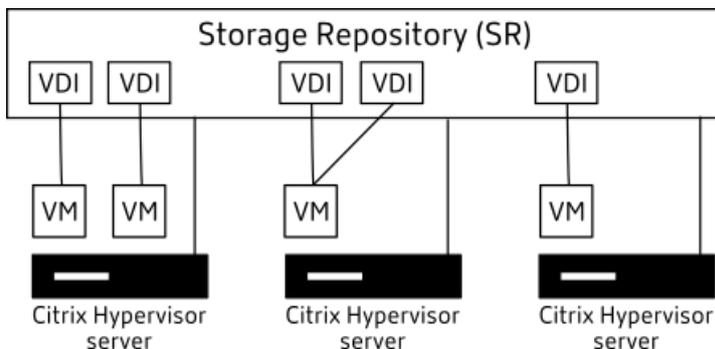
Citrix Hypervisor 资源池采用主服务器/从属服务器体系结构，由 XAPI 实现。XAPI 调用从池主服务器转发到池成员。池成员针对池主服务器进行 DB RPC。主服务器主机负责协调和锁定资源池中的资源，以及处理所有控制操作。成员主机通过 HTTP 和 XMLRPC 与主服务器进行通信，但可以相互通信（通过相同的通道）以便：

- 传输 VM 内存映像（VM 迁移）
- 镜像磁盘（存储迁移）

#### 存储库

Citrix Hypervisor 存储目标称为存储库 (SR)。存储库存储虚拟磁盘映像 (VDI)，后者包含虚拟磁盘的内容。

SR 具有对本地连接的 IDE、SATA、SCSI 和 SAS 驱动器和远程连接的 iSCSI、NFS、SAS 和光纤通道的内置支持，因而非常灵活。SR 和 VDI 抽象允许在支持高级存储功能（例如，精简预配、VDI 快照和快速克隆）的存储目标上提供这些功能。



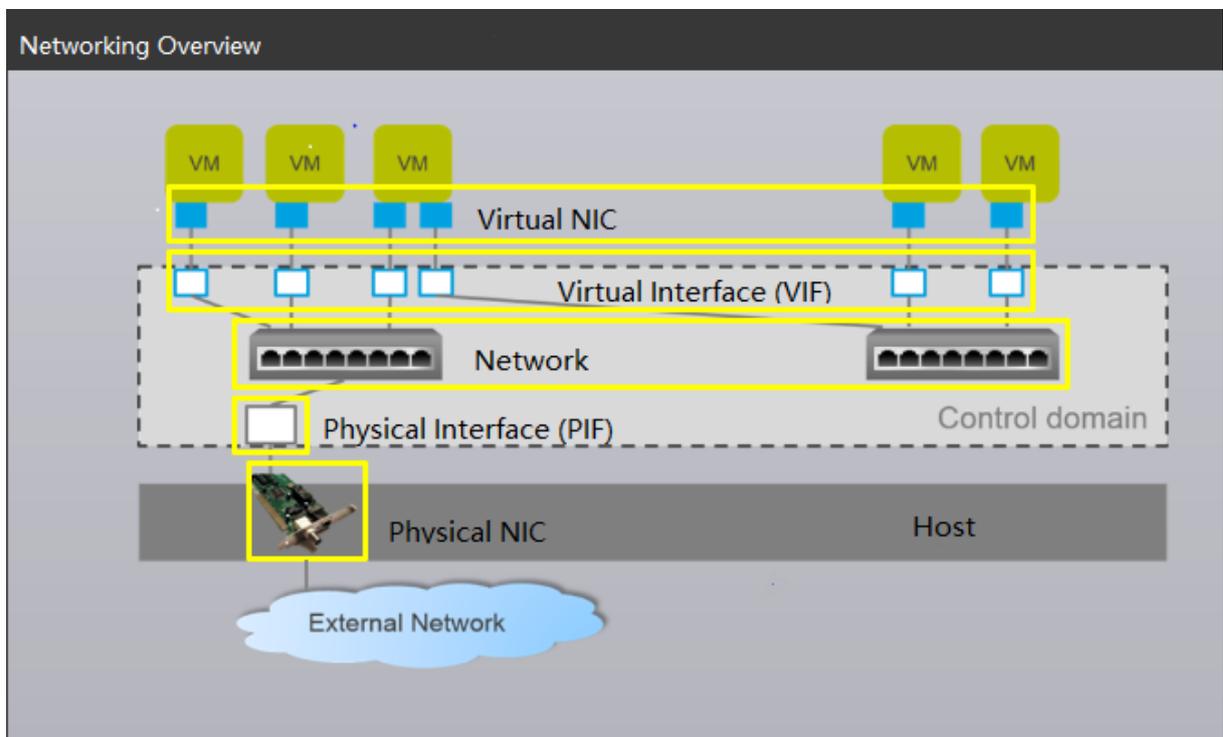
每台 Citrix Hypervisor 主机可以同时使用多个 SR 和不同的 SR 类型。可以在主机之间共享这些 SR，也可以将其专用于特定主机。共享存储会加入一个已定义的资源池，并由该池内的多台主机共用。共享 SR 必须由池中的每台主机通过网络访问。单个资源池中的所有主机必须至少有一个共享 SR。共享存储不能在多个池之间共享。

有关如何使用 SR 的详细信息，请参阅[配置存储](#)。

## 网络连接

在体系结构级别，有三种类型的服务器端软件对象来表示网络连接实体。这些对象包括：

- **PIF**，是指 dom0 中使用的软件对象，表示主机上的一个物理 NIC。PIF 对象具有名称和说明、UUID、所表示的 NIC 的参数，以及连接到的网络和服务器。
- **VIF**，是指 dom0 中使用的软件对象，表示虚拟机上的一个虚拟 NIC。VIF 对象具有名称和说明、UUID 和连接到的网络和 VM。
- **网络**，是指主机上用于路由网络主机上的网络流量的虚拟以太网交换机。网络对象具有名称和说明、UUID 以及连接到的 VIF 和 PIF 的集合。



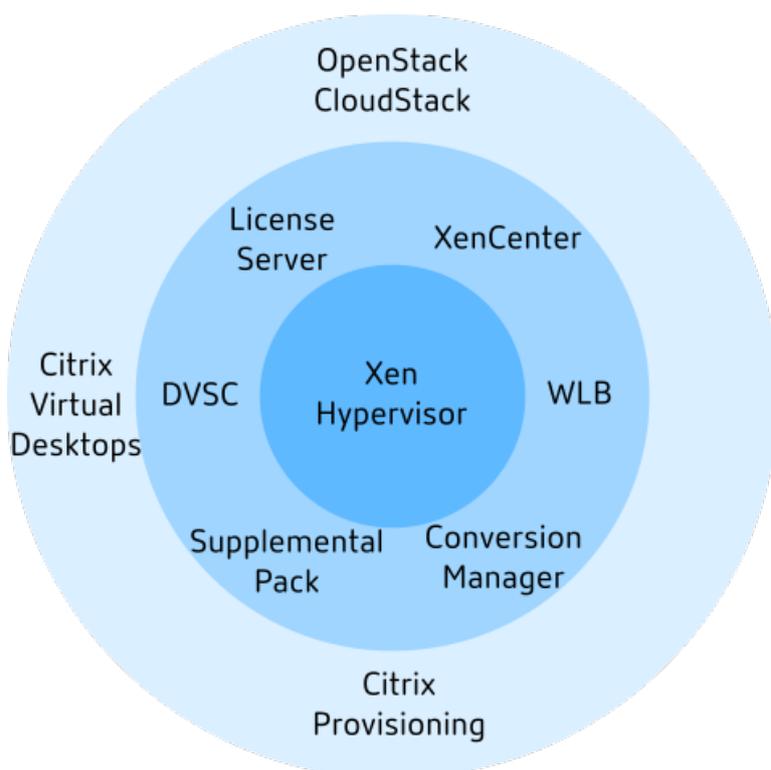
Citrix Hypervisor 管理 API 允许执行以下操作：

- 配置网络连接选项
- 控制要用于管理操作的 NIC
- 创建高级网络连接功能，例如虚拟局域网 (VLAN) 和 NIC 绑定

有关如何管理 XenServer 上的网络的详细信息，请参阅[网络连接](#)。

## 相关加载项和应用程序

虽然 Xen 虚拟机管理程序可以在非常核心的级别运行，但存在与虚拟机管理程序不可知的应用程序以及可用于使虚拟化体验完整的服务有关的 Citrix Hypervisor 特定的加载项。



- **XenCenter**

用于管理 VM 的 Windows GUI 客户端，基于管理 API 实现。XenCenter 提供了管理多个 Citrix Hypervisor 主机、资源池以及与其关联的整个虚拟基础结构的丰富用户体验。

- **Workload Balancing (WLB)**

一种设备，通过将虚拟机重定位到资源池中最适合其工作负载的服务器对池进行负载平衡。有关详细信息，请参阅 [Workload Balancing \(/zh-cn/citrix-hypervisor/vswitch-controller.html\)](#)。

- **分布式虚拟交换机控制器 (DVSC)**

基于 Debian 的设备，用于创建 XAPI 能够识别的开放流规则。此实现由以下各项组成：

- 在每个 Citrix Hypervisor 和 vSwitch Controller 上运行的能够感知虚拟化的交换机 (vSwitch)。
- 集中式服务器，用于管理和协调每个单独的 vSwitch 的行为以提供单个 vSwitch 的外观。

有关详细信息，请参阅 [vSwitch](#) 和 [Controller](#)。

- **Citrix Licensing 服务器**

基于 Linux 的设备，XenCenter 与之联系以请求指定服务器的许可证。

- **Citrix Hypervisor Conversion Manager (XCM)**

带控制台的虚拟设备，允许用户将现有 VMware 虚拟机转换为 Citrix Hypervisor 虚拟机，并具有相媲美的网络连接和存储连接。有关详细信息，请参阅 [Conversion Manager](#)。

- 标准引导补充包

一个补充包，使客户能够在引导时测量其 Citrix Hypervisor 主机的主要组件，并提供使远程证明解决方案能够安全地收集这些衡量指标的 API。有关详细信息，请参阅[标准引导补充包](#)。

- **Citrix Provisioning**

支持从公用映像进行 PXE 引导的 Provisioning Services。在 Citrix Virtual Desktops 和 Citrix Virtual Apps 中广泛使用。有关详细信息，请参阅[预配](#)。

- **Citrix Virtual Desktops**

专用于 Windows 桌面的虚拟桌面基础结构 (VDI) 产品。Citrix Virtual Desktops 使用 XAPI 管理多主机池配置中的 Citrix Hypervisor。有关详细信息，请参阅[Citrix Virtual Apps and Desktops](#)。

- **OpenStack/CloudStack 支持**

用于构建公有云/私有云的开源软件。使用管理 API 控制 XenServer。有关详细信息，请参阅 <https://www.openstack.org/> 和 <https://cloudstack.apache.org/>

## 常见技术问题解答

September 5, 2019

### 硬件

运行 **Citrix Hypervisor** 的最低系统要求是什么？

要了解此版本的最低系统要求，请参阅[系统要求](#)。

我需要配备了 **64 位 x86** 处理器的系统来运行 **Citrix Hypervisor** 吗？

是。需要配备了一个或多个 CPU 的基于 Intel VT 或 AMD-V 64 位 x86 的系统，才能运行所有[支持的来宾操作系统](#)。

有关主机系统要求的详细信息，请参阅[系统要求](#)。

我需要具有硬件虚拟化支持的系统吗？

要运行 Windows 操作系统或 HVM Linux 来宾，您需要在处理器和 BIOS 中支持 Intel VT 或 AMD-V 硬件虚拟化技术且基于 64 位 x86 处理器的系统。

有关 HVM Linux 来宾的详细信息，请参阅 [Linux VM](#)。

### 哪些系统经过认证可运行 **Citrix Hypervisor**?

有关 Citrix Hypervisor 认证的系统的完整列表，请参阅[硬件兼容性列表 \(HCL\)](#)。

### **Citrix Hypervisor** 是否支持 **AMD** 快速虚拟化索引和 **Intel** 扩展页表?

是。Citrix Hypervisor 支持 AMD 快速虚拟化索引和 Intel 扩展页表。快速虚拟化索引提供用于进一步增强 Xen 虚拟机管理程序性能的嵌套表技术的实现。扩展页表提供用于进一步增强 Xen 虚拟机管理程序性能的硬件辅助分页的实现。

### **Citrix Hypervisor** 可以在笔记本电脑或台式机级别的系统上运行吗?

Citrix Hypervisor 在符合最低 CPU 要求的笔记本电脑或台式机级别的系统上运行。但是，Citrix 仅支持已经过认证并在[硬件兼容性列表 \(HCL\)](#) 中列出的系统。客户可以选择在不受支持的系统上运行，以进行演示和测试；但是，某些功能（例如电源管理功能）将不起作用。

#### 产品限制

注意：

有关 Citrix Hypervisor 支持的限制的完整列表，请参阅[配置限制](#)。

### 主机系统上 **Citrix Hypervisor** 可以使用的最大内存大小是多少?

Citrix Hypervisor 主机系统可以使用高达 5 TB 的物理内存。

### **Citrix Hypervisor** 可以使用多少个处理器?

Citrix Hypervisor 支持每个主机最多使用 288 个逻辑处理器。受支持的逻辑处理器的最大数量因 CPU 而异。

有关详细信息，请参阅[硬件兼容性列表 \(HCL\)](#)。

### **Citrix Hypervisor** 上可以同时运行多少个虚拟机?

支持在 Citrix Hypervisor 主机上运行的虚拟机 (VM) 的最大数量为 1000。对于运行超过 500 个 VM 的系统，Citrix 建议向 Dom0 分配 8 GB RAM。有关配置 Dom0 内存的信息，请参阅[CTX134951 - 如何在 XenServer 6.2 及更高版本中配置 dom0 内存](#)。

对于任何特定系统，可以同时运行并且性能可接受的 VM 的数量取决于可用资源和 VM 工作负载。Citrix Hypervisor 根据可用的物理内存自动缩放分配给控制域 (Dom0) 的内存量。

**注意：**

如果每个主机的 VM 超过 50 个，并且主机物理内存小于 48 GB，则建议覆盖此设置。有关详细信息，请参阅[内存使用率](#)。

**Citrix Hypervisor 支持多少个物理网络接口？**

Citrix Hypervisor 最多支持 16 个物理 NIC 端口。可以绑定这些 NIC 以创建多达 8 个逻辑网络绑定。每个绑定最多可以包含 4 个 NIC。

**Citrix Hypervisor 可以向 VM 分配多少个虚拟处理器 (vCPU)？**

Citrix Hypervisor 最多支持每个 VM 32 个 vCPU。可以支持的 vCPU 数量因来宾操作系统而异。

**注意：**

请参阅您的来宾操作系统文档，确保不超过支持的限制

**Citrix Hypervisor 可以向 VM 分配多少内存？**

Citrix Hypervisor 最多支持每个来宾 1.5 TB 内存。可以支持的内存量因来宾操作系统而异。

**注意：**

可由操作系统寻址的最大物理内存量有所不同。将内存设置为超过操作系统支持的限制的级别会导致来宾内部出现性能问题。某些 32 位 Windows 操作系统支持 4 GB 以上的 RAM，但需要使用物理地址扩展 (PAE) 模式。32 位 PV 虚拟机的限制为 64 GB。有关详细信息，请参阅您的来宾操作系统文档和[支持的来宾操作系统](#)。

**Citrix Hypervisor 可以向 VM 分配多少个虚拟磁盘映像 (VDI)？**

Citrix Hypervisor 最多可以向每个 VM 分配 255 个 VDI，包括虚拟 DVD-ROM 设备。

**注意：**

支持的最大 VDI 数量取决于来宾操作系统。请参阅您的来宾操作系统文档，确保不超过支持的限制。

**Citrix Hypervisor 可以向 VM 分配多少个虚拟网络接口？**

Citrix Hypervisor 最多可以向每个 VM 分配 7 个 NIC。可以支持的虚拟 NIC 数量因来宾操作系统而异。

## 资源共享

### 如何在 **VM** 之间分割处理资源？

Citrix Hypervisor 在 vCPU 之间使用公平共享平衡算法分割处理资源。此算法确保所有 VM 都能获得其系统的处理资源的份额。

### **Citrix Hypervisor** 如何选择将哪些物理处理器分配给 **VM**？

Citrix Hypervisor 不会向任何特定的 VM 静态分配物理处理器。相反，Citrix Hypervisor 会根据负载向 VM 动态地分配任何可用的逻辑处理器。这种动态分配可确保高效使用处理器周期，因为 VM 可以在有多余容量的位置运行。

### 如何在 **VM** 之间分割磁盘 **I/O** 资源？

Citrix Hypervisor 使用公平共享资源拆分算法在 VM 之间拆分磁盘 I/O 资源。您还可以向 VM 提供优先级较高或者较低的磁盘 I/O 资源访问权限。

### 如何在 **VM** 之间分割网络 **I/O** 资源？

Citrix Hypervisor 使用公平共享资源算法在 VM 之间分割网络 I/O 资源。您还可以使用 Open vSwitch 控制每个 VM 的带宽限制。

## 来宾操作系统

### **Citrix Hypervisor** 可以作为来宾运行 **32** 位操作系统吗？

是。有关详细信息，请参阅[支持的来宾操作系统](#)。

### **Citrix Hypervisor** 可以作为来宾运行 **64** 位操作系统吗？

是。有关详细信息，请参阅[支持的来宾操作系统](#)。

### 哪些版本的 **Microsoft Windows** 可以在 **Citrix Hypervisor** 上作为来宾运行？

有关支持的 Windows 来宾操作系统的列表，请参阅[支持的来宾操作系统](#)。

### 哪些版本的 **Linux** 可以在 **Citrix Hypervisor** 上作为来宾运行？

有关受支持的 Linux 来宾操作系统的列表，请参阅[支持的来宾操作系统](#)。

我可以运行不同版本的受支持的操作系统或者其他未列出的操作系统吗？

Citrix 仅支持受操作系统供应商支持的操作系统。尽管不受支持的操作系统可能会继续运行，但我们可能会要求您升级到受支持的操作系统 Service Pack，然后我们才能调查任何问题。

适用的驱动程序可能不适用于不受支持的操作系统版本。如果未安装驱动程序，这些操作系统版本将无法以优化的性能运行。

通常可以安装其他 Linux 发行版。但是，Citrix 只能支持支持的来宾操作系统中列出的操作系统。我们可能会要求您先切换到支持的操作系统，然后才能调查任何问题。

**Citrix Hypervisor 是否支持 FreeBSD、NetBSD 或任何其他 BSD 变体作为来宾操作系统？**

Citrix Hypervisor 不支持将任何基于 BSD 的来宾操作系统用于通用虚拟化部署。但是，Citrix Hypervisor 上运行的 FreeBSD VM 已经过认证，可用于特定的 Citrix 产品。

**Citrix VM Tools 是什么？**

Citrix VM Tools 是适用于 Windows 和基于 Linux 的来宾操作系统的软件包。对于 Windows 操作系统，Citrix VM Tools 包括高性能 I/O 驱动程序（半虚拟化驱动程序）和管理代理。对于基于 Linux 的操作系统，Citrix VM Tools 包括向 Citrix Hypervisor 主机提供与 VM 有关的附加信息的来宾代理。有关详细信息，请参阅[Citrix VM Tools](#)。

## XenCenter

我必须在 Windows 计算机上运行 XenCenter 吗？

是。XenCenter 管理控制台在 Windows 操作系统中运行。有关系统要求的信息，请参阅[系统要求](#)。

如果您不想运行 Windows，可以使用 xe CLI 或者使用 xsconsole（系统配置控制台）来管理 Citrix Hypervisor 主机和池。

我可以使用我的 Active Directory 用户帐户登录 XenCenter 吗？

是。可以设置 XenCenter 登录请求以在 Citrix Hypervisor 的所有版本上使用 Active Directory。

我可以将 XenCenter 内的某些功能的访问限制到某些用户吗？

是。与 Active Directory 身份验证相结合的基于角色的访问控制功能可以限制 XenCenter 中的用户的访问。

我可以使用单个 **XenCenter** 控制台连接到多个 **Citrix Hypervisor** 主机吗？

是。可以使用单个 XenCenter 控制台连接到多个 Citrix Hypervisor 主机系统。

我可以 **XenCenter** 连接到运行不同版本的 **Citrix Hypervisor** 的多个主机吗？

是。XenCenter 与运行当前支持的不同版本的 Citrix Hypervisor 多个主机系统向后兼容。

我可以 **XenCenter** 连接到多个资源池吗？

是。可以从单个 XenCenter 控制台连接到多个资源池。

我怎样才能获取对基于 **Linux** 的 **VM** 的控制台的访问权限？

XenCenter 中的“控制台”选项卡提供对运行基于 Linux 的操作系统的 VM 的基于文本的控制台和图形控制台的访问权限。在能够与 Linux VM 的图形控制台连接之前，请确保 VNC 服务器和 X 显示管理器安装在 VM 中并进行了正确的配置。

XenCenter 还允许您使用 VM 的“控制台”选项卡上的“打开 SSH 控制台”选项通过 SSH 连接到 Linux VM。

我怎样才能获取对基于 **Windows** 的 **VM** 的控制台的访问权限？

XenCenter 提供对 Windows VM 的模拟图形的访问权限。如果 XenCenter 检测到 VM 上的远程桌面功能，XenCenter 将提供一个快速连接按钮，以启动连接到 VM 的内置 RDP 客户端。或者，可以使用外部远程桌面软件直接连接到您的来宾。

## 命令行接口 (CLI)

**Citrix Hypervisor** 是否包含 CLI？

是。Citrix Hypervisor 的所有版本都包括一个完整的命令行接口 (CLI) — 称为 **xe**。

我可以直接在主机上访问 **Citrix Hypervisor CLI** 吗？

是。可以使用直接连接到主机的屏幕和键盘或者通过连接到主机的串行端口的终端模拟器访问 CLI。

我可以从远程系统访问 **Citrix Hypervisor CLI** 吗？

是。Citrix 提供 xe CLI，它可以安装在 Windows 和 64 位 Linux 计算机上以远程控制 Citrix Hypervisor。您还可以使用 XenCenter 从“控制台”选项卡访问主机的控制台。

我可以通过我的 **Active Directory** 用户帐户登录 **Citrix Hypervisor CLI** 吗？

是。可以在 Citrix Hypervisor 的所有版本上使用 Active Directory 进行登录。

我可以限制某些用户使用某些 **CLI** 命令吗？

是。可以在 Citrix Hypervisor CLI 上限制用户访问。

## VM

通过 **VMware** 或 **Hyper-V** 创建的 **VM** 是否可以在 **Citrix Hypervisor** 上运行？

是。可以使用行业标准 OVF 格式导出和导入 VM。

还可以使用 Citrix Hypervisor Conversion Manager 批量转换 VM。也可以使用第三方工具。有关详细信息，请参阅 [Conversion Manager](#)。

我可以使用什么类型的安装介质安装来宾操作系统？

可以使用以下安装介质安装来宾操作系统：

- 主机的 CD-ROM 驱动器中的 CD
- 使用 iLO 或 DRAC 等技术的虚拟 CD-ROM 驱动器
- 将 ISO 映像放置在共享网络驱动器中
- 在特定来宾支持的位置进行网络安装。

有关详细信息，请参阅 [管理虚拟机](#)。

我可以克隆现有 **VM** 吗？

是。可以克隆在 Citrix Hypervisor 上创建的任何 VM 或者将其转换为 VM 模板。然后可以使用 VM 模板来创建更多 VM。

可以将 **VM** 从一个版本的 **Citrix Hypervisor** 中导出并移动到另一个版本吗？

是。可以将从较旧版本的 Citrix Hypervisor 中导出的 VM 导入到较新版本中。

我可以将 **VM** 从 **Xen** 的开源版本转换为 **Citrix Hypervisor** 吗？

不能。

**Citrix Hypervisor 是否为 VM 提供磁盘快照功能？**

是。Citrix Hypervisor 在所有版本中都支持创建快照。有关详细信息，请参阅[VM 快照](#)。

**存储**

**可以在 Citrix Hypervisor 中使用哪些类型的本地存储？**

Citrix Hypervisor 支持本地存储，例如 SATA 和 SAS。

**可以在 Citrix Hypervisor 中使用哪些类型的 SAN/NAS 存储？**

Citrix Hypervisor 支持光纤通道、FCoE、基于硬件的 iSCSI (HBA)、iSCSI、NFS 和 SMM 存储存储库。有关详细信息，请参阅[存储](#)和[硬件兼容性列表](#)。

**Citrix Hypervisor 是否支持基于软件的 iSCSI？**

是。Citrix Hypervisor 包括基于内置软件的 iSCSI 启动器 (open-iSCSI)。

**需要什么版本的 NFS 才能远程使用存储？**

Citrix Hypervisor 需要通过 TCP 的 NFSv3 或 NFSv4 才能远程使用存储。Citrix Hypervisor 当前不支持通过用户数据报协议 (UDP) 的 NFS。

**我可以为远程共享存储使用在常规用途的服务器上运行的基于软件 NFS 吗？**

是。虽然 Citrix 建议使用具有高速非易失性缓存并且使用 NFSv3 或 NFSv4 的专用 NAS 设备，以实现可接受的 I/O 性能。

**我可以从 iSCSI、光纤通道或 FCoE SAN 引导 Citrix Hypervisor 主机系统吗？**

可以。Citrix Hypervisor 支持使用光纤通道、FCoE 或 iSCSI HBA 从 SAN 引导。

**我可以从 UEFI 引导 Citrix Hypervisor 主机吗？**

可以。Citrix Hypervisor 支持从 BIOS 和 UEFI 引导。

**Citrix Hypervisor 是否支持对存储连接使用多路径 I/O (MPIO)?**

是。Citrix 建议对弹性存储连接使用多路径。

**Citrix Hypervisor 是否支持基于软件的 RAID 实现?**

否。Citrix Hypervisor 不支持软件 RAID。

**Citrix Hypervisor 是否支持 HostRAID 或 FakeRAID 解决方案?**

否。Citrix Hypervisor 不支持专有的类似 RAID 的解决方案，例如 HostRAID 或 FakeRAID。

**Citrix Hypervisor 是否支持现有 VM 的精简克隆?**

是。除 NFS 和 SMB 存储存储库外，还可以在格式为 EXT3 的本地磁盘上使用精简克隆。

**Citrix Hypervisor 是否支持分布式复制块设备 (DRBD) 存储?**

否。Citrix Hypervisor 不支持 DRBD。

**Citrix Hypervisor 是否支持 ATA-over-Ethernet?**

否。Citrix Hypervisor 不支持基于 ATA-over-Ethernet 的存储。

**网络连接**

**我可以创建隔离 VM 组的专用网络吗?**

是。可以在单个主机上为驻留的 VM 创建专用网络。使用 vSwitch Controller 设备，还可以创建跨多个主机的专用网络，而无论这些主机是否使用加密功能。

**Citrix Hypervisor 是否支持多个物理网络连接?**

是。可以连接到附加到物理主机系统上的不同网络接口的多个物理网络，或者将其关联起来。

**VM 可以连接到多个网络吗?**

是。VM 可以连接到对主机可用的任何网络。

### **Citrix Hypervisor 是否支持 IPv6?**

Citrix Hypervisor 上托管的来宾 VM 可以使用配置了 IPv4 和 IPv6 地址的任意组合。

但是，Citrix Hypervisor 不支持在其控制域 (Dom0) 中使用 IPv6。不能将 IPv6 用于主机管理网络或存储网络。IPv4 必须可供 Citrix Hypervisor 主机使用。

### **Citrix Hypervisor 是否支持在物理网络接口上使用 VLAN?**

是。Citrix Hypervisor 支持将 VM 网络分配给指定的 VLAN。

### **Citrix Hypervisor 虚拟网络是否将所有网络流量传递给所有 VM?**

否。Citrix Hypervisor 使用 Open vSwitch (OVS)，该交换机用作第 2 层交换机。VM 只能看到该 VM 的流量。此外，Citrix Hypervisor 中的多租户支持可提高隔离和安全级别。

### **虚拟网络接口和网络是否支持混杂模式?**

是。可以为混杂模式配置虚拟网络接口，这使您能够看到虚拟交换机上的所有流量。有关混杂模式配置的详细信息，请参阅以下知识中心文章：

- [CTX116493 - How to Enable Promiscuous Mode on a Physical Network Card](#) (CTX116493 - 如何在物理网卡上启用混杂模式)
- [CTX121729 - How to Configure a Promiscuous Virtual Machine in XenServer](#) (CTX121729 - 如何在 XenServer 中配置混杂虚拟机)

此外，Open vSwitch 允许将 RSPAN 配置为捕获网络流量。

### **Citrix Hypervisor 是否支持物理网络接口的绑定或成组?**

是。Citrix Hypervisor 支持通过可选的 LACP 支持进行物理网络接口绑定，以实现故障转移和链路聚合。有关详细信息，请参阅[网络连接](#)。

## 内存

### **运行 Citrix Hypervisor 占用多少内存?**

Citrix Hypervisor 主机的内存占用由三部分构成。

1. Xen 虚拟机管理程序
2. 主机上的控制域 (dom0)

### 3. Citrix Hypervisor 崩溃内核

运行 dom0 所需的内存量将自动调整。分配的内存量基于主机上的物理内存量，如下表所示：

主机内存 (GB)	已分配的控制域内存 (MB)
<24	752
24-47	2048
48-63	3072
64-1024	4096

注意：

分配给控制域的内存量可以增加超过上表中显示的内存量。但是，必须仅在 Citrix 技术支持的指导下增加此分配。

在 XenCenter 中，“内存”选项卡中的“Xen”字段报告由控制域、Xen 虚拟机管理程序本身和 Citrix Hypervisor 崩溃内核占用的内存。对于使用更多内存的主机来说，虚拟机管理程序占用的内存量更大。

有关详细信息，请参阅[内存使用率](#)。

#### Citrix Hypervisor 是否优化 VM 内存使用情况？

是。Citrix Hypervisor 使用动态内存控制 (DMC) 自动调整正在运行的 VM 的内存。这些调整使分配给每个 VM 的内存量保持在指定的最小内存值与最大内存值之间，确保性能并允许更大的 VM 密度。

有关详细信息，请参阅[VM 内存](#)。

#### 资源池

##### 资源池是什么？

资源池是作为一个单元管理的一组 Citrix Hypervisor 主机的集合。资源池通常共享一定数量的网络存储，以允许将 VM 从一台主机快速迁移到池中的另一台主机。有关详细信息，请参阅[主机和资源池](#)。

#### Citrix Hypervisor 是否需要专用主机来管理资源池？

否。必须将池中的一个主机指定为池主服务器。池主服务器控制池所需的所有管理活动。这种设计意味着不存在外部单故障点。如果池主服务器出现故障，池中的其他主机将继续运行，并且驻留 VM 将继续正常运行。如果池主服务器无法恢复联机，Citrix Hypervisor 会将池中的其他主机中的一台主机提升为主服务器以恢复对池的控制。

此过程通过高可用性功能自动进行。有关详细信息，请参阅[高可用性](#)。

### 资源池的配置数据存储在哪里？

配置数据的副本存储在资源池中的每个主机上。如果当前池主服务器出现故障，此数据将使资源池中的任何主机成为新的池主服务器。

### 可以在资源池级别进行哪些类型的配置？

可以在资源池级别进行共享远程存储和网络连接配置。在资源池上共享配置时，主服务器系统会自动将配置更改传播到所有成员系统。

### 新的主机系统是否添加到自动配置了共享设置的资源池？

是。自动添加到资源池中的任何新主机系统都会自动接收相同的共享存储配置和网络设置。

### 我可以在同一个 **Citrix Hypervisor** 资源池中使用不同类型的 **CPU** 吗？

是。Citrix 建议在整个池（同类资源池）中使用相同的 CPU 类型。但是，具有不同 CPU 类型的主机可以加入池（异构），前提是 CPU 来自相同的供应商。

有关详细信息，请参阅[主机和资源池](#)。

有关对特定 CPU 类型掩码的功能的支持的更新信息，请参阅[硬件兼容性列表](#)。

## 实时迁移（以前称为 **XenMotion**）

### 我可以将正在运行的 **VM** 从一个主机移动到另一个主机吗？

通过实时迁移，您可以在主机共享同一个存储（在池中）时移动正在运行的 VM。

此外，存储实时迁移允许在不共享存储的主机之间进行迁移。VM 可以在池内部或跨池迁移。

## 高可用性

### **Citrix Hypervisor** 是否提供高可用性功能？

是。如果启用了高可用性 (HA)，Citrix Hypervisor 将持续监视池中的主机的运行状况。如果高可用性功能检测到主机受损，主机将自动关闭。此操作允许在运行状况良好的备用主机上安全地重新启动 VM。

### **Citrix Hypervisor** 高可用性功能是否支持本地存储？

否。需要共享存储才能使用高可用性功能。此共享存储允许在主机出现故障时重新定位 VM。但是，高可用性功能允许将存储在本地存储上的 VM 标记为在主机重新启动后恢复时自动重新启动。

### 我可以高可用性功能自动对恢复的 VM 的重新启动进行排序吗？

是。高可用性配置允许您定义 VM 的启动顺序。此功能支持彼此相互依赖的 VM 自动排序。

## 性能衡量指标

### **Citrix Hypervisor** 管理工具是否收集性能信息？

是。Citrix Hypervisor 提供详细的性能衡量指标监视数据。这些衡量指标包括 CPU、内存、磁盘、网络、C 状态/P 状态信息和存储。适用情况下，会在每主机和每 VM 的基础上提供这些衡量指标。性能衡量指标可以直接获取（如轮循机制数据库所示），也可以在 XenCenter 或其他第三方应用程序中以图形方式进行访问和查看。有关详细信息，请参阅[监视和管理您的部署](#)。

### 如何收集 **Citrix Hypervisor** 性能衡量指标？

Citrix Hypervisor 性能衡量指标的数据是从各种来源收集的。这些来源包括 Xen 虚拟机管理程序、Dom0、标准 Linux 接口和标准 Windows 接口（例如 WMI）。

### **XenCenter** 是否实时显示性能衡量指标？

是。XenCenter 在“性能”选项卡上显示每个正在运行的 VM 以及 Citrix Hypervisor 主机的实时性能衡量指标。可以自定义显示的衡量指标。

### **XenCenter** 是否存储和显示历史性能衡量指标？

是。Citrix Hypervisor 保留去年的性能衡量指标（粒度降低）。XenCenter 在实时图形显示中提供这些衡量指标的可视化。

## 安装

### **Citrix Hypervisor** 是否安装在已运行现有操作系统的系统上？

否。Citrix Hypervisor 直接安装在裸机硬件上，避免底层操作系统的复杂性、开销和性能瓶颈。

我可以将现有 **Citrix Hypervisor** 或 **XenServer** 安装升级到较新的版本吗？

是。如果您已安装 Citrix Hypervisor 或 XenServer 的受支持的版本，则可以更新或升级到 Citrix Hypervisor 的更新版本来代替重新安装。有关详细信息，请参阅[更新或升级](#)。

我可以从 **Citrix Hypervisor** 或 **XenServer** 安装的不受支持的版本升级到此版本吗？

如果您的 Citrix Hypervisor 或 XenServer 的现有版本不再受支持，则无法直接升级或更新到最新版本 Citrix Hypervisor。

- 对于 XenServer 和 6.5 Service Pack 1，可以先升级到 XenServer 7.1 Cumulative Update 2，然后从 XenServer 7.1 Cumulative Update 2 升级到 Citrix Hypervisor 8.0。
- 对于 XenServer 的其他 6.x 版本，不能升级到最新版本，并且必须创建 Citrix Hypervisor 8.0 的全新安装。
- 对于 XenServer 的不受支持的 7.x 当前版本，不能升级到最新版本，并且必须创建 Citrix Hypervisor 8.0 的全新安装。

这些不受支持的版本的任何其他升级路径都不受支持。

**Citrix Hypervisor** 安装在物理主机系统中需要多少本地存储？

Citrix Hypervisor 在物理主机系统中至少需要 46 GB 的本地存储。

我可以使用 **PXE** 在主机系统对 **Citrix Hypervisor** 进行网络安装吗？

是。可以使用 PXE 在主机系统中安装 Citrix Hypervisor。还可以通过创建预配置的应答文件使用 PXE 自动安装 Citrix Hypervisor。

**Xen** 虚拟机管理程序是否在 **Linux** 上运行？

否。Xen 是直接主机硬件（“裸机”）上运行的类型 1 虚拟机管理程序。虚拟机管理程序加载后，将启动特权管理域（控制域），其中包含极小的 Linux 环境。

**Citrix Hypervisor** 从何处获取其设备驱动程序支持？

Citrix Hypervisor 使用从 Linux 内核获取的设备驱动程序。因此，Citrix Hypervisor 在各种硬件和存储设备上运行。但是，Citrix 建议您使用经过认证的设备驱动程序。

有关详细信息，请参阅 [硬件兼容性列表](#)。

许可

我如何许可使用 **Citrix Hypervisor**?

有关 Citrix Hypervisor 许可的信息，请参阅[许可](#)

技术支持

**Citrix** 是否为 **Citrix Hypervisor** 提供直接技术支持?

是。有关详细信息，请访问 [Citrix 支持和服务](#)。

我可以通过一个支持合约获取对 **Citrix Hypervisor** 和其他 **Citrix** 产品的技术支持吗?

是。Citrix 提供技术支持合约，这些合约允许您开立有关 Citrix Hypervisor 以及其他 Citrix 产品的支持事件。

有关详细信息，请访问 [Citrix 支持和服务](#)。

我是否必须在购买 **Citrix Hypervisor** 的同时购买 **Citrix** 技术支持合约?

否。您可以在产品销售点或其他时间从 Citrix 购买技术支持合约。

是否存在获取 **Citrix Hypervisor** 的技术支持的备选渠道?

是。可以通过几种备选渠道获取 Citrix Hypervisor 的技术支持。还可以使用 [Citrix 支持知识中心](#) 访问我们的论坛或与提供技术支持服务的授权 Citrix Hypervisor 合作伙伴联系。

**Citrix** 是否为开源 **Xen** 项目提供技术支持?

否。Citrix 不为开源 Xen 项目提供技术支持。有关详细信息，请访问 <http://www.xen.org/>。

如果我遇到非技术问题，可以通过 **Citrix** 开立技术支持事件吗?

否。请通过 Citrix 客户服务提出任何有关 Citrix Hypervisor 的非技术问题。例如，与软件维护、许可、管理支持和订单确认有关的问题。

## 许可

June 4, 2019

Citrix Hypervisor 8.0 在以下版本中提供：

- Premium Edition（以前称为 Enterprise Edition）
- Standard Edition
- Express Edition（以前称为 Free Edition）

**Standard Edition** 是我们的入门级商用产品。此版本提供的一系列功能适用于希望使用强大的高性能虚拟化平台，但不需要 Premium Edition 提供的高级功能的客户。同时，这些客户仍希望获得全面的 Citrix 支持和维护保障。

**Premium Edition** 是我们的高级产品，已针对桌面、服务器和云工作负载进行了优化。除 Standard Edition 中提供的功能之外，Premium Edition 还提供以下功能：

- 自动执行 Windows VM 驱动程序更新
- 自动更新管理代理
- 支持 SMB 存储
- 直接检查 API
- 动态工作负载平衡
- 使用 NVIDIA GRID、AMD MxGPU 和 Intel GVT-g 实现的 GPU 虚拟化
- VMware vSphere 到 Citrix Hypervisor 转换实用程序
- Intel Secure Measured Boot (TXT)
- 导出池资源数据
- 内存中读缓存
- PVS 加速器
- 自动更新 - 使用 XenCenter
- Citrix Hypervisor 实时修补
- 能够启用 Citrix Virtual Desktops 平板电脑模式
- 更改块跟踪
- IGMP 监听
- USB 直通
- SR-IOV 网络支持
- 面向共享块存储设备的精简预配

Premium Edition 在 Citrix Hypervisor 的早期版本中称为 Enterprise Edition。此版本的名称已更改，以与其他 Citrix 产品保持一致，但此版本提供的特性和功能未更改。

购买了 Citrix Virtual Apps 或 Citrix Virtual Desktops 的客户具有 Citrix Hypervisor 的授权，其中包括上文列出的 Premium Edition 的所有功能。

**Express Edition** 提供一组缩减的功能，并且没有资格获得 Citrix 支持和维护。Express Edition 不需要许可证。运行 Citrix Hypervisor 的 Express Edition 的主机在 XenCenter 中标记为“未获许可”。

Express Edition 在 Citrix Hypervisor 的早期版本中称为 Free Edition。此版本的名称已更改，以与其他 Citrix 产品保持一致，但此版本提供的特性和功能未更改。

有关详细信息，请参阅 [Citrix Hypervisor 功能列表](#)。

Citrix Hypervisor 使用的许可过程与其他 Citrix 产品相同，因此，需要在许可证服务器上安装有效的许可证。可以从 [Citrix Licensing](#) 下载许可证服务器。以每插槽为基础对 Citrix Hypervisor 进行许可（而不是通过 Citrix Virtual Apps and Desktops 许可证）。环境中的一台独立 Citrix 许可证服务器（无论是物理服务器还是虚拟服务器）会负责集中管理并强制执行许可证分配。应用每插槽许可证后，Citrix Hypervisor 将显示为 *Citrix Hypervisor Per-Socket Edition*。

**注意：**

已获许可的主机和未获许可的主机的混合池将被视为所有主机都未获许可。

未经授权的主机将受到限制。有关详细信息，请参阅其他问题。

### 许可步骤概述

需要以下项目才能许可使用 Citrix Hypervisor Premium Edition 或 Standard Edition：

- Citrix Hypervisor 许可证
- Citrix 许可证服务器
- Citrix Hypervisor 服务器
- XenCenter

以下步骤提供了此过程的概述：

1. 安装 Citrix 许可证服务器或者将 Citrix 许可证服务器虚拟设备导入到 Citrix Hypervisor 服务器中。
2. 下载许可证文件
3. 将许可证文件添加到 Citrix 许可证服务器中
4. 使用 XenCenter 输入许可证服务器详细信息并将其应用到您的资源池中的主机

有关 Citrix Licensing 的详细信息，请参阅 [Citrix Licensing 文档](#)。

### 许可 **Citrix Hypervisor**

问：我可以从何处购买 **Citrix Hypervisor** 许可证？

答：可以从 <http://citrix.com/buy> 购买 Citrix Hypervisor 许可证。

问：我如何应用 **Citrix Hypervisor** 许可证？

答：Citrix Hypervisor 需要许可证服务器。许可使用 Citrix Hypervisor 后，您将获得一个.LIC 许可证访问代码。请在以下设备上安装此许可证访问代码：

- 运行 Citrix 许可证服务器软件的 Windows Server，或者
- Citrix 许可证服务器虚拟设备

如果为 Citrix Hypervisor 服务器分配了许可证，Citrix Hypervisor 会联系指定的 Citrix 许可证服务器，并为指定的服务器申请许可证。如果成功，则将签出一个许可证，并且许可证管理器将显示与许可使用主机时所使用的许可证有关的信息。

有关将 Citrix Hypervisor 许可证应用于 Citrix 许可证服务器虚拟设备的说明，请参阅 [CTX200159 - 如何将 Citrix Hypervisor 许可证文件应用到 Citrix 许可证服务器虚拟设备 \(CLSVA\)](#)。

问：我需要多少个许可证才能许可使用我的资源池？

答：以每 CPU 插槽为基础对 Citrix Hypervisor 进行许可。对于要视为已获许可的池，池中的所有 Citrix Hypervisor 服务器都必须获得许可。Citrix Hypervisor 仅计算填充的 CPU 插槽。

可以使用 Citrix 许可证服务器查看许可证管理控制台控制板中显示的可用许可证数量。

问：我需要为未填充的插槽提供每插槽许可证吗？

答：否。只有填充的 CPU 插槽才计入要许可的插槽数量内。

问：我的许可证过期时是否会丢失我的虚拟机 (VM)？

答：否。不会丢失任何 VM 或其数据。

问：如果我有一个已获得许可的池且许可证服务器变得不可用，会发生什么情况？

答：如果您的许可证未过期，但许可证服务器不可用，您将在以前应用的许可级别收到为期 30 天的宽限期。

问：我正在使用每插槽许可证从早期的 **Citrix Hypervisor** 版本升级到 **Citrix Hypervisor 8.0**，我是否需要执行任何操作？

答：否。可以使用以前购买的每插槽许可证将您的主机升级到 Citrix Hypervisor 8.0 Premium Edition，前提是 Customer Success Services 的有效期至少到 2019 年 3 月 27 日。

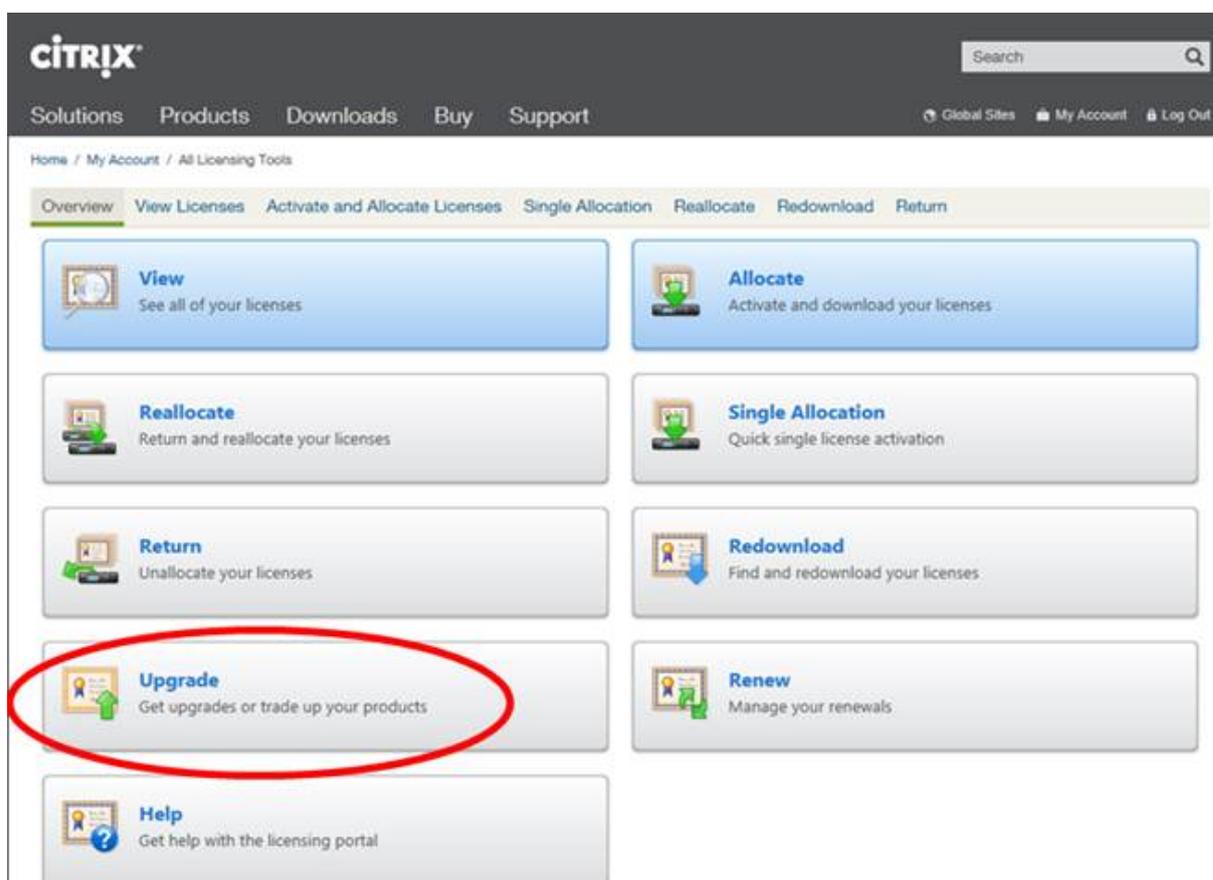
如果您在最初购买后续订了 Customer Success Services，可能需要刷新许可证服务器上的许可证文件，以确保其显示 Customer Success Services 资格。

问：我正在从 **XenServer 7.6** 未获许可的版本移动到 **Citrix Hypervisor 8.0**。我是否需要执行任何操作？

答：否。可以将您的主机升级或更新到 Citrix Hypervisor 8.0。在应用恰当的许可证之前，您仍然没有资格获得支持，并且高级功能无法访问（包括滚动池升级）。

问：我是 **Citrix Virtual Apps and Desktops** 客户，正在从 **XenServer 7.6** 移动到 **Citrix Hypervisor 8.0**。我是否需要执行任何操作？

答：否。Citrix Virtual Apps 或 Citrix Virtual Desktops 客户可以无缝更新到 Citrix Hypervisor 8.0。您现在已安装的 Citrix Virtual Apps 或 Citrix Virtual Desktops 许可证将授予您对 Citrix Hypervisor 的权利，而不需要任何其他更改。



问：我是获得 **Citrix Virtual Apps and Desktops** 授权的 **Citrix Service Provider**。升级到 **Citrix Hypervisor 8.0** 时，我可以对 **Citrix Hypervisor** 使用此许可证吗？

答：可以。Citrix Hypervisor 8.0 支持您的许可证。安装此许可证后，可以使用 Citrix Hypervisor 的 Premium Edition 提供的所有高级功能。要将此许可证应用到您的池，请先升级或更新池中的所有主机以运行 Citrix Hypervisor 8.0。

问：我是订阅了 **Citrix Virtual Apps and Desktops** 服务的客户。我是否有权使用 **Citrix Hypervisor 8.0**？

答：可以。如果您有允许使用本地桌面和应用程序的 Citrix Virtual Apps and Desktops 服务订阅，则将有权使用 Citrix Hypervisor 托管这些桌面和应用程序。

请通过许可管理工具下载许可证。在您的许可证服务器上安装此许可证，以使用具有 Citrix Virtual Apps and Desktops 服务订阅的本地 Citrix Hypervisor。

安装此许可证后，可以使用与使用本地 Citrix Virtual Apps and Desktops 授权时相同的所有高级功能。要将此许可证应用到您的池，请先升级池中的所有主机以运行 Citrix Hypervisor 8.0。

问：使用作为 **Citrix Virtual Apps and Desktops** 的一部分提供的 **Citrix Hypervisor Premium Edition** 高级虚拟化管理功能时有哪些限制？

答：每个版本的 Citrix Virtual Apps and Desktops 都有权访问 Citrix Hypervisor Premium Edition 高级虚拟化管理功能。可以在“Citrix Hypervisor 功能列表”中找到 Citrix Virtual Apps 或 Citrix Virtual Desktops 启用的所有功能的完整列表。

Citrix Hypervisor 授权允许所需的任何基础结构的虚拟化提供 Citrix Virtual Apps 或 Citrix Virtual Desktops 功能组件。这些功能必须由 Citrix Virtual Apps 或 Citrix Virtual Desktops 授权的用户或设备以独占方式进行访问。

此授权还包括额外的基础结构支持服务器，例如 Microsoft 域控制器和 SQL Server，前提是这些服务器与此许可证授权的 Citrix Virtual Apps 或 Citrix Virtual Desktops 在相同的 Citrix Hypervisor 资源池中部署，并且这些支持服务器仅用于支持 Citrix Virtual Apps 或 Citrix Virtual Desktops 基础结构。

Citrix Virtual Apps 或 Citrix Virtual Desktops 许可证授予的 Citrix Hypervisor 权利不能用于不托管 Citrix Virtual Apps 或 Citrix Virtual Desktops 基础结构或 Virtual Delivery Agent (VDA) 授权的 Citrix Hypervisor 池。也不能使用此授权托管上述权限未授权的虚拟机。必须针对这些用途单独购买 Citrix Hypervisor。

## **Citrix** 许可证服务器

问：我可以对 **Citrix Hypervisor** 使用哪些许可证服务器？

答：可以使用 Citrix 许可证服务器软件版本 11.14 或更高版本（安装在运行 Microsoft Windows 的服务器上），或者基于 Linux 的 Citrix 许可证服务器虚拟设备。

问：如何将我的许可证导入到 **Citrix** 许可证服务器中？

答：有关导入许可证文件的信息，请参阅[许可文档](#)。

- [使用 Citrix Licensing Manager 安装许可证](#)
- [使用许可管理控制台导入许可证文件](#)
- [使用命令行安装许可证文件](#)

问：我可以在我的 **Citrix Hypervisor** 池中运行许可证服务器吗？

答：可以。可以在 Windows VM 上安装 Citrix 许可证服务器软件，或者导入基于 Linux 的 Citrix 许可证服务器虚拟设备。为便于部署，Citrix 许可证服务器软件预安装在此虚拟设备上，并且可以在您的 Citrix Hypervisor 池中作为 VM 运行。

Citrix Hypervisor 使用“宽限”许可证运行，直至许可证服务器能够启动。此行为意味着，在您许可使用池中的 Citrix Hypervisor 服务器并重新启动正在运行 Citrix 许可证服务器的主机后，宽限期将应用到该主机，直至设备重新启动。

问：我可以对 **Citrix Hypervisor** 使用 **Windows** 版本的 **Citrix** 许可证服务器吗？

答：可以。

问：我可以在 **Citrix** 许可证服务器虚拟设备上或者在 **Windows** 上安装的 **Citrix** 许可证服务器软件上安装适用于其他 **Citrix** 产品的许可证吗？

答：可以。可以使用 Citrix 许可证服务器虚拟设备或者通过 Windows 上安装的 Citrix 许可证服务器软件许可使用其他 Citrix 产品。有关详细信息，请参阅[Citrix 产品文档](#) Web 站点上的[许可](#)。

许可使用 **Citrix Hypervisor** 池

问：如何使用 **XenCenter** 将许可证应用于所有主机？

答：请按照以下过程应用许可证：

1. 在工具菜单中，单击许可证管理器。
2. 选择希望许可使用的池或主机，然后单击分配许可证。
3. 在应用许可证对话框中，指定要分配给主机的版本类型，然后键入许可证服务器的主机名或 IP 地址。

问：可以在不使用 **XenCenter** 的情况下应用许可证吗？

答：可以。可以使用 xe CLI。请运行 `host-apply-edition` 命令。例如，请输入以下命令以许可使用某个主机：

```
1     xe host-apply-edition edition=enterprise-per-socket|desktop-plus|
      desktop|standard-per-socket \
2
3     license-server-address=<licenseserveraddress> host-uuid=<
      uuidofhost> \
4
5     license-server-port=<licenseserverport>
```

要许可使用某个池，请使用 `pool-apply-edition` 命令。例如：

```
1     xe pool-apply-edition edition=enterprise-per-socket|desktop-plus|
      desktop|standard-per-socket \
2
3     license-server-address=<licenseserveraddress> pool-uuid=<
      uuidofpool> \
4
5     license-server-port=<licenseserverport>
```

问：我如何才能发现我的主机和池的许可证状态？

答：XenCenter 将显示服务器或池的许可证类型。

要查看服务器或池的许可证类型，请在树视图中选择该服务器或池。XenCenter 在该服务器或池的标题栏中的服务器或池名称后显示许可证状态。

已获许可的主机和未获许可的主机的混合池将被视为所有主机都未获许可。在树视图中，XenCenter 将显示未获许可的池，该池带有警告三角形图标。

其他问题

问：我如何获取许可证以评估 **Citrix Hypervisor**？

答：不需要许可证即可评估 Citrix Hypervisor。可以使用处于未获许可状态的 Citrix Hypervisor。但是，您对高级功能没有访问权限。此外，您将没有资格获得 Citrix 支持或维护。

可以获取一个试用版许可证以试用 Premium Edition 功能。有关详细信息，请参阅[快速入门](#)。

问：我可以使用未安装许可证的 **Citrix Hypervisor** 吗？

答：可以。如果使用处于未经许可状态的 Citrix Hypervisor (Express Edition)，您将不能获得 Citrix 支持或维护。此外，以下功能将受到限制，需要许可证：

- 包含三个以上的主机的池

注意：

在您尝试向包含三个或更多主机的现有池中添加另一个主机之前，这些池不受此限制影响。

- 高可用性
- 动态内存控制
- Storage Motion
- 基于角色的访问控制
- GPU 直通
- 站点恢复管理器
- Active Directory 集成
- 滚动池升级

可以获取一个试用版许可证以试用 Citrix Hypervisor Premium Edition。有关详细信息，请参阅[Citrix Hypervisor 入门](#)。

### 更多信息

- 有关 Citrix Hypervisor 8.0 版本的详细信息，请参阅 [Citrix Hypervisor 8.0 发行说明](#)。
- 要访问 Citrix Hypervisor 8.0 产品文档，请参阅 [Citrix Hypervisor 8.0 产品文档](#)。
- 有关 Citrix Hypervisor 产品的概述，请参阅[技术概述](#)。
- [CTX200159 - 如何将 Citrix Hypervisor 许可证文件应用到 Citrix 许可证服务器虚拟设备 \(CLSVA\)](#)。
- 提出 Citrix Hypervisor 的任何非技术性问题，包括 Customer Success Services 计划支持、许可、管理支持以及通过 [Citrix 客户服务](#) 确认订单。

### 安装

June 4, 2019

本部分内容将介绍相应的步骤，来指导您完成 Citrix Hypervisor 的安装、配置和初始操作。本部分内容还将介绍如何解决安装期间可能出现的问题，并提供指向额外的资源的链接。

此信息主要面向需要在物理服务器上设置 Citrix Hypervisor 服务器的系统管理员。

Citrix Hypervisor 直接安装在裸机硬件上，避免底层操作系统的复杂性、开销和性能瓶颈。它使用从 Linux 内核获取的设备驱动程序。因此，Citrix Hypervisor 能够在各种硬件和存储设备上运行。但是，请务必使用经过认证的设备驱动程序。

有关详细信息，请参阅 [硬件兼容性列表 \(HCL\)](#)。

**重要：**

Citrix Hypervisor 服务器必须安装在专用 64 位 x86 服务器上。请勿在 Citrix Hypervisor 服务器的双引导配置中安装任何其他操作系统。此配置不受支持。

### 准备工作

安装 Citrix Hypervisor 8.0 之前，请注意以下因素：

- 您要使用 Citrix Hypervisor 的哪个版本流？
- 恰当的安装方法是什么？
- 系统要求是什么？

### Citrix Hypervisor 版本流

Citrix Hypervisor 的各版本在以下版本流之一中：当前版本 (CR) 或长期服务版本 (LTSR)。Citrix Hypervisor 8.0 是当前版本。选择安装 CR 流还是 LTSR 流中的 Citrix Hypervisor 的版本时，请注意以下事项：

- 要更新 Citrix Hypervisor 的版本的频率是多少？
- 您更倾向于稳定的功能集还是最新的功能集？

#### 当前版本

Citrix Hypervisor 的当前版本允许您抓住尽可能早的机会来使用新功能。CR 流中 Citrix Hypervisor 的新版本每季度发布一次。如果您在 CR 流中，则必须定期采用新 CR 以继续获得支持。在 Citrix Hypervisor CR 中发现的大多数问题在后续在当前版本中修复。安全问题在可以应用到 CR 的修补程序中修复。

如果安装了 XenServer 7.6 或 7.5，则必须移动到 Citrix Hypervisor 8.0 以继续接收支持。

#### 长期服务版本

Citrix Hypervisor 的长期服务版本（以前称为 XenServer）根据 Citrix Hypervisor 内部的功能集来保证稳定性。LTSR 流中 Citrix Hypervisor 的新版本每两年发布一次，最长可获得 10 年支持。Citrix Hypervisor LTSR 中的所有问题都在可以应用到 Citrix Hypervisor LTSR 的修补程序或累积更新中修复。

如果您当前安装了 XenServer 7.1 Cumulative Update 2 LTSR，则可以升级到 Citrix Hypervisor 当前版本流以利用其新增功能。

### 安装方法

Citrix Hypervisor 8.0 可以通过以下方式之一安装：

- 以全新安装方式
- 以升级到 Citrix Hypervisor 的早期受支持版本的方式

Citrix Hypervisor 或 XenServer		
的现有版本	如何获取 Citrix Hypervisor 8.0	要使用的 ISO 文件
无	全新安装	基础安装 ISO
7.6, 7.5, 7.1 Cumulative Update 2, 7.0	升级	基础安装 ISO

**\* 注意：**

仅支持从 LTSR 的最新累积更新进行升级。如果现有 XenServer 版本为 7.1 或 7.1 Cumulative Update 1，请先应用 7.1 Cumulative Update 2，然后再升级到 Citrix Hypervisor 8.0。

不支持从 XenServer 的不再受支持的版本直接升级到 Citrix Hypervisor 8.0。请改为执行全新安装。

### 全新安装

如果要创建 Citrix Hypervisor 8.0 的新安装：

- 使用 **Citrix Hypervisor 8.0** 基础安装 ISO 文件。  
可以从 [Citrix 下载站点](#) 下载此文件
- 在安装 Citrix Hypervisor 之前，请查看[系统要求](#)、[许可 Citrix Hypervisor](#) 和安装 Citrix Hypervisor 和 XenCenter 中的信息。

### 更新

由于平台更新是 Citrix Hypervisor 8.0 提供的，因此，您无法使用更新机制从 XenServer 的早期当前版本进行移动。请改为使用升级机制。

### 升级

如果要从 XenServer 7.1 Cumulative Update 2 或 7.0 升级到 Citrix Hypervisor 8.0，请执行以下操作：

- 使用 **Citrix Hypervisor 8.0** 基础安装 ISO 文件。  
可以从 [Citrix 下载站点](#) 下载此文件
- 在升级 Citrix Hypervisor 之前，请查看[系统要求](#)和[从现有版本升级](#) 中的信息。

## 安装位置

可以使用以下方法之一安装 Citrix Hypervisor 服务器：

- 从 CD 安装

可以下载安装程序（ISO 文件格式）并将其刻录成 CD。

要下载安装程序，请访问 [Citrix 下载](#) 页面。

主安装文件包含在主机上设置 Citrix Hypervisor 所需的基本软件包。

- 设置可通过网络访问的待启动 TFTP 服务器。

有关设置 TFTP 服务器以使用玩过启动安装程序的详细信息，请参阅 [网络引导安装](#)。

- 将 Citrix Hypervisor 安装到 SAN 上的远程磁盘以允许从 SAN 引导

有关详细信息，请参阅 [从 SAN 引导](#)。

## 补充包

在安装 Citrix Hypervisor 之后可以安装所需的任何增补包。将补充包 (filename.iso) 下载到您的计算机上的已知位置，并按照与安装更新相同的方式安装补充包。

有关详细信息，请参阅 [补充包](#) 和 [DDK 指南](#)。

## 升级

安装程序检测到以前安装的 Citrix Hypervisor 版本时，将显示升级选项。升级过程与首次安装过程基本相同，但会跳过几个设置步骤，并保留现有的设置，包括网络连接配置、系统时间设置等。

### 重要：

升级需要小心谨慎，认真规划。有关升级各个 Citrix Hypervisor 和池的详细信息，请参阅 [从现有版本升级](#)。

## 安装 Citrix Hypervisor 服务器

### 提示：

在整个安装过程中，请通过按 F12 键快速前进到下一个屏幕。使用 Tab 键可在元素之间移动，按空格键或 Enter 键可进行选择。要获得常规的帮助信息，请按 F1 键。

### 警告：

安装 Citrix Hypervisor 时，会覆盖选择用作安装位置的任何硬盘驱动器上的数据。请在继续操作前备份希望保留的数据。

要安装或升级 **Citrix Hypervisor** 服务器，请执行以下操作：

1. 从安装 CD 引导计算机，或从 TFTP 服务器进行网络引导（如果适用）。
2. 显示初始引导消息和“欢迎使用 Citrix Hypervisor”屏幕后，选择要在安装过程中使用的键盘映射（键盘布局）。

注意：

如果您的屏幕上显示“系统硬件”警告屏幕以及硬件虚拟化协助支持，请参阅硬件制造商提供的 BIOS 升级信息。

3. 此时将显示“欢迎使用 Citrix Hypervisor 安装程序”屏幕。

Citrix Hypervisor 附带一套全面的驱动程序集，可支持最流行的服务器硬件配置。但是，如果已获得任何其他必要的设备驱动程序，请按 F9 键。安装程序将引导您逐步安装必要的驱动程序。

警告：

在安装过程中，此时只能安装包含驱动程序磁盘的更新包。但是，稍后在安装过程中会提示安装包含补充包的任何更新包。

安装完所有必需的驱动程序后，请选择 **OK**（确定）以继续。

Citrix Hypervisor 允许客户将 Citrix Hypervisor 安装配置为从 FCoE 引导。按 F10 并按照屏幕上显示的说明设置 FCoE。

注意：

在允许您的 Citrix Hypervisor 服务器从 FCoE 引导之前，请手动完成将 LUN 显示给主机所需的配置。这一手动配置包括配置存储架构以及将 LUN 分配给 SAN 的公共全球通用名称 (PWWN)。完成此配置后，可用的 LUN 将作为 SCSI 设备装载到主机的 CNA 中。然后，可以使用该 SCSI 设备访问 LUN，就像它是本地连接的 SCSI 设备一样。有关配置支持 FCoE 的物理交换机和阵列的信息，请参阅供应商提供的文档。

配置 FCoE 架构时，请勿使用 VLAN 0。Citrix Hypervisor 服务器找不到位于 VLAN 0 上的流量。

警告：

有时，使用软件 FCoE 堆栈从 FCoE SAN 引导 Citrix Hypervisor 服务器会导致主机停止响应。此问题是由主机初始化阶段中出现的临时链路中断导致的。如果主机长时间无法响应，则可以重新启动主机以解决此问题。

4. 此时将显示 Citrix Hypervisor EULA。使用 Page Up 和 Page Down 键可滚动浏览并阅读该协议。选择 **Accept EULA**（接受 EULA）以继续。
5. 选择恰当的操作。您可能会看到下面的任意选项：
  - 执行全新安装
  - *Upgrade*（升级）：如果安装程序检测到 Citrix Hypervisor 或 XenServer 以前安装的版本，则会提供升级选项。有关升级 Citrix Hypervisor 服务器的信息，请参阅[从现有版本升级](#)。
  - *Restore*（还原）：如果安装程序检测到以前创建的备份安装，则会提供用于从备份还原 Citrix Hypervisor 的选项。

做出选择，然后选择 **OK**（确定）以继续。

6. 如果您拥有多个本地硬盘，请选择主磁盘进行安装。选择 **OK**（确定）。
7. 选择要用作虚拟机存储的磁盘。可以按 **F5** 键查看有关特定磁盘的信息。

如果要使用精简预配功能来优化可用存储的使用情况，请选择“Enable thin provisioning”（启用精简预配）。此选项将选择主机的本地 SR 作为要用于 VM VDI 的本地缓存的 SR。建议 Citrix Virtual Desktops 用户选择此选项，以便能够正常进行本地缓存。有关详细信息，请参阅[存储](#)。

选择 **OK**（确定）。

8. 选择安装介质源。

要从 CD 进行安装，请选择 **Local media**（本地介质）。要使用网络进行安装，请选择 **HTTP**、**FTP** 或 **NFS**。选择 **OK**（确定）以继续。

如果选择 **HTTP**、**FTP** 或 **NFS**，请设置网络连接，以便安装程序能够连接到 Citrix Hypervisor 安装介质文件：

- a) 如果计算机具有多个 NIC，请选择要用于访问 Citrix Hypervisor 安装介质文件的其中一个 NIC。选择 **OK**（确定）以继续。
- b) 选择 **Automatic configuration (DHCP)**（自动配置 (DHCP)）以使用 DHCP 配置 NIC，或者选择“Static configuration”（静态配置）以手动配置 NIC。如果选择 **Static configuration**（静态配置），请根据需要输入详细信息。
- c) 如果您的安装介质存在于 VLAN 网络中，请提供 VLAN ID。
- d) 如果选择 **HTTP** 或 **FTP**，请提供 HTTP 或 FTP 存储库的 URL，以及用户名和密码（如有需要）。

如果选择 **NFS**，请提供 NFS 共享所在的服务器及其路径。

选择确定继续操作。

9. 指定是否验证安装介质的完整性。如果选择 **Verify installation source**（验证安装源），系统会计算软件包的 SHA256 校验和，并将其与已知值核对。验证过程可能需要一段时间。做出选择，然后选择 **OK**（确定）以继续。
10. 设置并确认 root 用户密码，XenCenter 将使用此密码连接到 Citrix Hypervisor 服务器。您还将使用此密码（对应用户名为“root”）登录 **xconsole**（系统配置控制台）。

注意：

Citrix Hypervisor root 用户的密码不得包含非 ASCII 字符。

11. 设置用来连接到 XenCenter 的主管理接口。

如果您的计算机有多个 NIC，请选择您希望用来实施管理的 NIC。选择 **OK**（确定）以继续。

12. 配置管理 NIC IP 地址，方法是选择 **Automatic configuration (DHCP)**（自动配置 (DHCP)）以使用 DHCP 配置 NIC，或者选择 **Static configuration**（静态配置）以手动配置 NIC。要在 VLAN 网络中配备管理接口，请提供 VLAN ID。

注意：

要成为池的成员，Citrix Hypervisor 服务器必须具有静态 IP 地址或者支持 DNS 寻址。如果使用 DHCP，应确保启用静态 DHCP 保留策略。

13. 手动指定或通过 DHCP 自动指定主机名和 DNS 配置。

在 **Hostname Configuration** (主机名配置) 部分中，选择 **Automatically set via DHCP** (通过 DHCP 自动设置)，使 DHCP 服务器同时提供主机名和 IP 地址。如果选择 **Manually specify** (手动指定)，请在提供的字段中输入服务器的主机名。

注意：

如果手动指定主机名，请输入短主机名而非完全限定域名 (FQDN)。输入 FQDN 会导致外部身份验证失败，或者添加到 AD 中的 Citrix Hypervisor 服务器可能具有其他名称。

在 **DNS Configuration** (DNS 配置) 部分中，选择 **Automatically set via DHCP** (通过 DHCP 自动设置)，以使用 DHCP 获取名称服务配置。如果选择 **Manually specify** (手动指定)，请在提供的字段中输入主 DNS 服务器 (必需)、二级 DNS 服务器 (可选) 和三级 DNS 服务器 (可选) 的 IP 地址。

选择确定继续操作。

14. 按地理区域和城市选择时区。可以键入所需区域设置的第一个字母以跳至第一个以此字母开头的条目。选择 **OK** (确定) 以继续。
15. 指定希望服务器在确定本地时间时所用的方法：使用 NTP 或手动输入时间。做出选择，然后选择 **OK** (确定) 以继续。
16. 如果使用 NTP，请选择 **NTP is configured by my DHCP server** (NTP 由我的 DHCP 服务器配置)，或者在下面的字段中至少提供一个 NTP 服务器名称或 IP 地址。选择 **OK** (确定)。

注意：

Citrix Hypervisor 假定服务器 BIOS 中的时间设置是当前 UTC 时间。

17. 选择安装 **Citrix Hypervisor**。

如果选择了手动设置日期和时间，系统将在安装期间提示您输入这些信息。设置后，选择 **OK** (确定) 以继续。

18. 如果要从 CD 进行安装，下一个屏幕会询问您是否要从 CD 安装任何补充包。如果您打算安装由硬件供应商提供的任何增补包，请选择 **Yes** (是)。

如果您选择安装补充包，系统将提示您将其插入。弹出 Citrix Hypervisor 安装 CD，插入增补包 CD。选择 **OK** (确定)。

选择 **Use media** (使用介质) 继续进行安装。

对要安装的每个包重复执行上述操作。

19. 在 **Installation Complete** (安装完成) 屏幕中，弹出安装 CD (如果是从 CD 进行安装)，然后选择 **OK** (确定) 重新引导服务器。

服务器重新引导后，Citrix Hypervisor 将显示 **xsconsole**（系统配置控制台）。要从 **xsconsole** 访问本地 shell，请按 **Alt+F3**；要返回 **xsconsole**，请按 **Alt+F1**。

注意：

记下显示的 IP 地址。请在将 XenCenter 连接到 Citrix Hypervisor 服务器时使用此 IP 地址。

## 安装 XenCenter

XenCenter 必须安装在可以通过网络连接到 Citrix Hypervisor 服务器的 Windows 计算机上。请务必在此系统中安装 .NET Framework 4.6 或更高版本。

要安装 **XenCenter**，请执行以下操作：

1. 从 [Citrix Hypervisor 下载页面](#) 下载最新版本的 XenCenter 的安装程序。
2. 启动安装程序 `.msi` 文件。
3. 按照安装向导操作；该向导允许您修改默认目标文件夹，然后安装 XenCenter。

## 将 XenCenter 连接到 Citrix Hypervisor 服务器

要将 **XenCenter** 连接到 **Citrix Hypervisor** 服务器，请执行以下操作：

1. 启动 XenCenter。程序将在主页选项卡打开。
2. 单击添加新服务器图标。
3. 在服务器字段中输入 Citrix Hypervisor 服务器的 IP 地址。键入在 Citrix Hypervisor 安装期间所设置的 root 用户名和密码。单击添加。
4. 首次添加主机时，将显示保存和还原连接状态对话框。在此对话框中，可以针对主机连接信息的存储及主机连接的自动还原设置首选项。

如果以后要更改首选项，可以使用 XenCenter 或 Windows 注册表编辑器进行更改。

要在 XenCenter 中执行此操作，请从主菜单中选择工具，然后选择选项。系统将打开选项对话框。选择保存并还原选项卡，设置您的首选项。单击确定以保存更改。

为此，请使用 Windows 注册表编辑器导航到注册表项 `HKEY_LOCAL_MACHINE\Software\Citrix\XenCenter` 并添加一个名为 `AllowCredentialSave` 的注册表项，字符串值为 `true` 或 `false`。

## 安装和部署方案

June 4, 2019

本部分内容将分步骤介绍以下常见的安装和部署方案：

- 一个或多个具有本地存储的 Citrix Hypervisor 服务器
- 具有共享存储的 Citrix Hypervisor 服务器池：
  - 具有共享 NFS 存储的多个 Citrix Hypervisor 服务器
  - 具有共享 iSCSI 存储的多个 Citrix Hypervisor 服务器

### 具有本地存储的 **Citrix Hypervisor** 服务器

Citrix Hypervisor 最简单的部署方案是在一个或多个具有本地存储的 Citrix Hypervisor 服务器上运行 VM。

注意：

仅当共享存储时，才能使用实时迁移在 Citrix Hypervisor 服务器之间迁移 VM。但是，存储实时迁移功能仍然可用。

#### 基础硬件要求

- 一个或多个具有本地存储的 64 位 x86 服务器
- 一个或多个 Windows 系统，与 Citrix Hypervisor 服务器位于同一网络中

#### 高级步骤

1. 在服务器上安装 Citrix Hypervisor 服务器软件。
2. 在系统中安装 XenCenter。
3. 将 XenCenter 连接到 Citrix Hypervisor 服务器。

在将 XenCenter 连接到 Citrix Hypervisor 服务器之后，将自动在主机的本地磁盘上配置存储。

### 具有共享存储的 **Citrix Hypervisor** 服务器池

池由安装的多个 Citrix Hypervisor 服务器组成，这些服务器绑定在一起成为单个管理实体。与共享存储结合使用时，池允许 VM 在该池中内存充足的任何 Citrix Hypervisor 服务器上启动。VM 之后可以在运行时动态地在主机之间移动（实时迁移），从而最大程度地缩短停机时间。如果单个 Citrix Hypervisor 服务器发生硬件故障，可以在同一个池中的另一台主机上重新启动出现故障的 VM。

如果启用了高可用性 (HA) 功能，则在出现主机故障时，受保护 VM 将自动移动到其他主机。

要在池中的主机之间设置共享存储，需要创建存储库。Citrix Hypervisor 存储库 (SR) 是存储虚拟磁盘的存储容器。SR 与虚拟磁盘类似，是磁盘上持久对象，独立于 Citrix Hypervisor 存在。SR 可以存在于不同类型的物理存储设备上（内部和外部），包括本地磁盘设备和网络共享存储。在创建 SR 时，可以使用多种不同类型的存储，包括：

- NFS VHD 存储

- 软件 iSCSI 存储
- 硬件 HBA 存储

下面几部分内容将分步骤指导您为 Citrix Hypervisor 服务器池设置两种常见的共享存储解决方案，即 NFS 和 iSCSI。在开始创建 SR 之前，请配置 NFS 或 iSCSI 存储。具体设置因所用存储解决方案的类型而异。有关详细信息，请参阅供应商文档。在所有情况下，要成为池的成员，提供共享存储的服务器必须具有静态 IP 地址或者支持 DNS 寻址。有关设置共享存储的更多信息，请参阅[存储](#)。

我们建议您在添加共享存储之前先创建一个池。有关池的要求和设置过程，请参阅 XenCenter 帮助或[主机和资源池](#)。

## 具有共享 NFS 存储的 Citrix Hypervisor 服务器

### 基础硬件要求

- 两个或更多具有本地存储的 64 位 x86 服务器
- 一个或多个 Windows 系统，与 Citrix Hypervisor 服务器位于同一网络中
- 一个通过 NFS 导出共享目录的服务器

### 高级步骤

1. 在服务器上安装 Citrix Hypervisor 服务器软件。
2. 在系统中安装 XenCenter。
3. 将 XenCenter 连接到 Citrix Hypervisor 服务器。
4. 创建您的 Citrix Hypervisor 服务器池。
5. 配置 NFS 服务器。
6. 在池级别 NFS 共享上创建 SR。

### 配置 NFS 存储

在创建 SR 之前，请配置 NFS 存储。要成为池的一部分，NFS 共享存储必须具有静态 IP 地址或者支持 DNS 寻址。请将 NFS 服务器配置为具有一个或多个可由 NFS 客户端（例如池中的 Citrix Hypervisor 服务器）装载的目标。具体设置因存储解决方案而异，因此最好参阅供应商提供的文档，以了解详细信息。

在 **XenCenter** 中在池级别的 **NFS** 共享上创建 **SR**：

1. 在资源窗格中，选择池。在工具栏上，单击新建存储按钮。此时将打开新建存储库向导。
2. 在虚拟磁盘存储下，选择“NFS VHD”作为存储类型。选择下一步继续操作。
3. 输入新 SR 的名称及其所在共享的名称。单击扫描，让向导在指定位置扫描现有的 NFS SR。

注意：

必须将配置为 NFS 服务器导出池中所有 Citrix Hypervisor 服务器的指定路径。

4. 单击完成。

新 SR 将显示在资源窗格的池级别。

#### 使用 **xe CLI** 在池级别的 **NFS** 共享上创建 **SR**

1. 在池中的任意 Citrix Hypervisor 服务器上打开控制台。
2. 通过输入以下命令在 `server:/path` 创建存储库：

```
1 xe sr-create content-type=user type=nfs name=label=sr_name= \  
2   shared=true device-config:server=server \  
3   device-config:serverpath=path
```

`device-config-server` 参数表示 NFS 服务器的名称，`device-config-serverpath` 参数表示服务器上的路径。由于 `shared` 设置为 `true`，因此，共享存储将自动连接到池中的每个主机。随后加入的所有主机也将连接到该存储。所创建存储库的 UUID 将显示在控制台中。

3. 使用 `pool-list` 命令查找池的 UUID。
4. 通过输入以下命令将新 SR 设置为池级别的默认 SR：

```
1 xe pool-param-set uuid=pool_uuid \  
2   default-SR=storage_repository_uuid
```

由于已将共享存储设置为池级别的默认共享存储，因此将来的所有 VM 都会在该 SR 上创建自己的磁盘。

#### 具有共享 **iSCSI** 存储的 **Citrix Hypervisor** 服务器

##### 基础硬件要求

- 两个或更多具有本地存储的 64 位 x86 服务器
- 一个或多个 Windows 系统，与 Citrix Hypervisor 服务器位于同一网络中
- 一个提供 iSCSI 共享目录的服务器

##### 高级步骤

1. 在服务器上安装 Citrix Hypervisor 服务器软件。
2. 在 Windows 系统中安装 XenCenter。

3. 将 XenCenter 连接到 Citrix Hypervisor 服务器。
4. 创建您的 Citrix Hypervisor 服务器池。
5. 配置 iSCSI 存储。
6. 如有必要，请在 iSCSI 设备上启用多个启动器。
7. 如有必要，请为每个 Citrix Hypervisor 服务器配置 iSCSI IQN。
8. 在池级别的 iSCSI 共享上创建 SR。

### 配置 iSCSI 存储

在创建 SR 之前，请配置 iSCSI 存储。要成为池的一部分，iSCSI 存储必须具有静态 IP 地址或者支持 DNS 寻址。在 SAN 上为 VM 存储提供 iSCSI 目标 LUN。将 Citrix Hypervisor 服务器配置为能够查看和访问 iSCSI 目标 LUN。iSCSI 目标以及每个 Citrix Hypervisor 服务器上的各 iSCSI 发起程序都必须具有有效并且唯一的 iSCSI 限定名称 (IQN)。要了解配置的详细信息，最好参阅供应商的文档。

### 为每个 Citrix Hypervisor 服务器配置 iSCSI IQN

安装时，Citrix Hypervisor 会自动为每个主机分配一个唯一的 IQN。如果必须遵循本地的管理命名策略，可以通过在主机控制台上输入以下命令来更改 IQN：

```
1 xe-set-iscsi-iqn iscsi_iqn
```

或者，可以通过在 xe CLI 中输入以下命令来进行更改：

```
1 xe host-param-set uuid=host_uuid other-config-iscsi_iqn=iscsi_iqn
```

使用 **XenCenter** 在池级别的 **iSCSI** 共享上创建 **SR**：

#### 警告：

在 iSCSI 或 HBA 存储中创建 Citrix Hypervisor SR 时，该卷中的所有现有内容都将被销毁。

1. 在资源窗格中，选择池。在工具栏上，单击新建存储按钮。此时将打开新建存储库向导。
2. 在虚拟磁盘存储下，选择“软件 iSCSI”作为存储类型。选择下一步继续操作。
3. 输入新 SR 的名称，以及 iSCSI 目标的 IP 地址或 DNS 名称。

#### 注意：

该 iSCSI 存储目标必须配置为允许池中的每个 Citrix Hypervisor 服务器访问一个或多个 LUN。

4. 如果已将 iSCSI 目标配置为使用 CHAP 身份验证，请输入用户和密码。
5. 单击检测 **IQN** 按钮，然后从“目标 IQN”列表中选择 iSCSI 目标 IQN。

**警告：**

iSCSI 目标以及池中的所有服务器必须具有唯一的 IQN。

- 单击检测 **LUN** 按钮，然后从“目标 LUN”列表中选择用来创建 SR 的 LUN。

**警告：**

每个 iSCSI 存储库必须完全包含在单个 LUN 中，不能跨多个 LUN 分布。否则在所选 LUN 上的所有数据都将被毁坏。

- 单击完成。

新 SR 将显示在资源窗格的池级别。

使用 **xe CLI** 在池级别的 **iSCSI** 共享上创建 **SR**：

**警告：**

在 iSCSI 或 HBA 存储中创建 Citrix Hypervisor SR 时，该卷中的所有现有内容都将被销毁。

- 在池中任意服务器的控制台上，运行以下命令：

```
1 xe sr-create name=label=name_for_sr \  
2     host-uuid=host_uuid device-config:target=  
3     iscsi_server_ip_address \  
4     device-config:targetIQN=iscsi_target_iqn device-config:SCSIid=  
5     scsi_id \  
6     content-type=user type=lvmoiscsi shared=true
```

`device-config:target` 参数表示 iSCSI 服务器的主机名或 IP 地址。由于 `shared` 参数设置为 **true**，因此，共享存储将自动连接到池中的每个主机。随后加入的所有主机也将连接到该存储。

该命令返回已创建存储库的 UUID。

- 通过运行 `pool-list` 命令查找池的 UUID。
- 通过输入以下命令将新 SR 设置为池级别的默认 SR：

```
1 xe pool-param-set uuid=pool_uuid default-SR=iscsi_shared_sr_uuid
```

由于已将共享存储设置为池级别的默认共享存储，因此将来的所有 VM 都会在该 SR 上创建自己的磁盘。

## 从现有版本升级

July 10, 2019

我们提供可用于从 Citrix Hypervisor 的某些早期版本移动到 Citrix Hypervisor 8.0 的升级和更新功能。使用升级或更新功能可以应用 Citrix Hypervisor 8.0 而不需要完成完整的安装过程。升级或更新时，Citrix Hypervisor 8.0 将保留您的 VM、SR 和配置。

- 可以使用基础安装 **ISO** 从 XenServer 7.6、7.5、7.1 Cumulative Update 2 (LTSR) 或 7.0 升级到 Citrix Hypervisor 8.0。本部分内容将介绍如何升级到 Citrix Hypervisor 8.0。

注意：

不支持从 XenServer 7.1 升级到 Citrix Hypervisor 8.0。请务必在尝试升级之前对 Citrix Hypervisor 7.1 应用最新的累积更新。

- XenServer 的所有其他版本不能直接升级到 Citrix Hypervisor 8.0。可以先升级到 Citrix Hypervisor 的更高版本，然后将该版本升级到 8.0，也可以使用基础安装 **ISO** 执行全新安装。有关详细信息，请参阅[安装](#)。

注意：

要保留以前安装的 XenServer 中的 VM，请导出这些 VM 并将其导入到您全新安装的 Citrix Hypervisor 8.0 中。可以将从 XenServer 的任何受支持的版本中导出的 VM 导入到 Citrix Hypervisor 8.0 中。有关详细信息，请参阅[导入和导出 VM](#)。

本部分内容介绍了如何使用 XenCenter 或 xe CLI 升级 XenServer。本部分内容将指导您自动（使用 XenCenter 的“滚动池升级”向导）和手动升级您的池 Citrix Hypervisor 服务器和独立的服务器。

重要：

- 升级 Citrix Hypervisor 服务器（尤其是 Citrix Hypervisor 服务器池）时，需要认真规划，而且需要格外谨慎。要避免丢失任何现有数据，可以：
  - 仔细映射您的升级路径。
  - 使用 XenCenter 的“滚动池升级”向导，并确保在分步执行安装程序时选择升级选项。
- 如果要使用 XenCenter 升级您的主机，请下载并安装最新版本的 XenCenter。例如，如果要升级到 Citrix Hypervisor 8.0，请使用随 Citrix Hypervisor 8.0 发布的 XenCenter。不支持使用早期版本的 XenCenter 升级到较新版本的 Citrix Hypervisor。
- 在手动升级过程中，不集成“从 SAN 引导”设置。使用 ISO 或 PXE 过程进行升级时，请按照在以下安装过程中使用的相同说明操作，确保正确配置 `multipathd`。有关详细信息，请参阅[从 SAN 引导](#)。
- 如果要从 XenServer 6.5 Service Pack 1 或更早版本升级到最新版本，NIC 的排序和命名将有所差别。可以在安装过程中更改 NIC 的顺序，以解决此变更。有关详细信息，请参阅[CTX135809 - 如何更改 NIC 的顺序](#)。

### 滚动池升级

Citrix Hypervisor 允许您执行滚动池升级。滚动池升级会保持池提供的所有服务和资源可用，同时升级池中的所有主机。此升级方法每次仅使一个 Citrix Hypervisor 服务器脱机。关键 VM 在升级过程中通过将 VM 实时迁移到池中的其他主机来保持运行状态。

**注意：**

池必须具有共享存储才能保持您的 VM 在执行滚动池升级过程中继续运行。如果您的池没有共享存储，则必须先停止 VM，然后再进行升级，因为 VM 不能实时迁移。

存储实时迁移功能不支持滚动池升级。

可以使用 XenCenter 或 xe CLI 执行滚动池升级。使用 XenCenter 时，我们建议使用“滚动池升级”向导。该向导会自动组织升级路径并引导您完成升级过程。如果使用 xe CLI，请先规划您的升级路径，然后在手动执行滚动池升级过程中在 Citrix Hypervisor 服务器之间实时迁移正在运行的 VM。

“滚动池升级”向导适用于 Citrix Hypervisor Premium Edition 客户或通过其 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。有关 Citrix Hypervisor 许可的详细信息，请参阅[许可](#)。要升级或购买 Citrix Hypervisor 许可证，请访问[Citrix Web 站点](#)。

**重要：**

在“从 SAN 引导”的环境中，请勿使用滚动池升级。有关从 SAN 环境升级引导的详细信息，请参阅[从 SAN 引导](#)。

### 使用 XenCenter 的“滚动池升级”向导升级 Citrix Hypervisor 服务器

可以使用“滚动池升级”向导将 Citrix Hypervisor 服务器、池中的主机或独立主机升级到 Citrix Hypervisor 的当前版本。

“滚动池升级”向导会引导您完成升级过程并自动组织升级路径。对于池来说，池中的每个主机都将从池主服务器开始依次升级。开始升级之前，该向导会执行一系列预检查。这些预检查可确保某些池范围内的功能（例如高可用性）暂时处于禁用状态，并且池中的每个主机都准备好进行升级。一次只有一个主机处于脱机状态。在将升级安装到每个主机之前，任何正在运行的 VM 都自动从该主机中迁出。

“滚动池升级”向导在升级到较新版本的 Citrix Hypervisor 时允许您自动应用可用修补程序。这样，您只需在结束时执行次数很少的重新启动即可使您的独立主机或池保持最新。必须在升级过程中连接到 Internet，此功能才能正常运行。

当您使用随 Citrix Hypervisor 7.6 发布的 XenCenter 从任何受支持的 Citrix Hypervisor 版本升级到 Citrix Hypervisor 7.0 及更高版本时，您可以从自动应用修补程序功能受益。

**注意：**

使用 XenCenter 的“滚动池升级”向导仅适用于 Citrix Hypervisor Premium Edition 客户或通过其 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。

该向导可以在手动或自动模式下运行：

- 在手动模式下，必须依次手动在每个主机上运行 Citrix Hypervisor 安装程序，并按照主机串行控制台上的屏幕说明操作。开始升级时，XenCenter 会立即提示您插入 XenCenter 安装介质，或者为要升级的每个主机指定一个网络引导服务器。
- 在自动模式下，该向导会使用 HTTP、NFS 或 FTP 服务器上的网络安装文件依次升级每个主机。此模式不要求您插入安装介质、手动重新启动或者在每个主机上逐步执行安装程序。如果按这种方式执行滚动池升级，则必须

在开始升级之前将安装介质解压到 HTTP、NFS 或 FTP 服务器上。

## 升级准备

在开始升级之前，请确保进行了如下准备：

- 从 [Citrix Hypervisor 产品下载](#) 页面下载并安装随 Citrix Hypervisor 8.0 发布的 XenCenter。不支持使用早期版本的 XenCenter 升级到较新版本的 Citrix Hypervisor。
- 我们强烈建议您使用 `pool-dump-database` xe CLI 命令对现有池的状态进行备份。有关详细信息，请参阅 [命令行接口](#)。将状态备份后，可确保您在将部分完成的滚动升级还原回其原始状态时，不会丢失任何 VM 数据。
- 确保主机未过度预配：确认主机具有足够的内存来执行升级。一般原则是，如果 N 等于池中的主机总数，则在 N-1 个主机之间必须有足够的内存来运行池中的所有实时 VM。在升级过程中最好将所有非关键的 VM 挂起。
- 如果您的池中运行启用了 vGPU 的 VM，请完成以下步骤以在这些 MV 运行时迁移该池：
  - 确保计划升级到的版本支持您正在使用的 GPU。
  - 确定可用于 Citrix Hypervisor 的当前版本和要升级的 Citrix Hypervisor 的版本的 NVidia GRID 驱动程序版本。如有可能，请选择最新的可用驱动程序。
  - 在 Citrix Hypervisor 服务器上安装新的 GRID 驱动程序，并在任何启用了 vGPU 的 VM 上安装匹配的来宾驱动程序。
  - 请确保您也具有与要升级到的 Citrix Hypervisor 的版本相匹配的 GRID 驱动程序版本。系统会提示您将这些驱动程序作为补充包在滚动池升级过程中安装。

“滚动池升级”向导将检查是否执行了以下操作。请在开始执行升级过程之前执行这些操作：

- 清空池中的 VM 的 CD/DVD 驱动器。
- 禁用高可用性。

要使用 **XenCenter** 的“滚动池升级”向导升级 **Citrix Hypervisor** 主机，请执行以下操作：

1. 打开“滚动池升级”向导：在工具菜单中，选择滚动池升级。
2. 阅读准备工作信息，然后单击下一步继续操作。
3. 选择要升级的池和任何主机，然后单击下一步。
4. 选择以下模式之一：
  - 自动模式，适用于从 HTTP、NFS 或 FTP 服务器上的网络安装文件进行的自动升级
  - 手动模式，适用于从 CD/DVD 或通过网络引导（使用现有基础结构）进行的手动升级

### 注意：

如果选择手动模式，则必须在每个主机上依次运行 Citrix Hypervisor 安装程序。按照主机串行控制台上的屏幕说明进行操作。开始升级时，XenCenter 会立即提示您插入 Citrix Hypervisor 安装介质，或者为要升级的每个主机指定一个网络引导服务器。

5. 选择是否希望 XenCenter 在将服务器升级到较新版本后自动下载并安装最少的一组更新（修补程序）。“应用更新”选项默认处于选中状态。但是，您必须具有 Internet 连接才能下载并安装更新。
6. 选择升级模式后，单击运行预检查。
7. 按照建议解决任何失败的升级预检。如果希望 XenCenter 自动解决所有失败的预检查，请单击全部解决。  
解决所有预检查问题后，单击下一步继续操作。
8. 准备 Citrix Hypervisor 安装介质。

如果选择自动模式，请输入安装介质的详细信息。选择 **HTTP**、**NFS** 或 **FTP**，然后指定适当的 URL、用户名和密码。

注意：

- 1 - 如果选择 FTP，请务必转义 URL 的文件路径部分中的所有前导斜线。
- 2
- 3 - 如果配置了安全凭据，则请输入与您的 HTTP 或 FTP 服务器相关联的用户名和密码。请勿输入与您的 Citrix Hypervisor 池相关联的用户名和密码。
- 4
- 5 - Citrix Hypervisor 仅在被动模式下支持 FTP。

如果选择手动模式，请注意升级计划和说明。

单击启动升级。

9. 升级开始时，“滚动池升级”向导会引导您完成升级每个主机必须执行的任何操作。按照说明进行操作，直到池中的所有主机均已升级并更新。

如果您具有启用了 vGPU 的 VM，则当您开始执行提供补充包选项的步骤时，请上载与启用了 vGPU 的 VM 上的驱动程序匹配的 GRID 驱动程序。请务必为要升级到的版本上载适用于 Citrix Hypervisor 版本的驱动程序版本。

注意：

如果升级或更新过程因任何原因失败，“滚动池升级”向导都将终止该进程。这使您能够修复该问题，然后通过单击重试按钮继续执行升级或更新过程。

10. 升级完成后，“滚动池升级”向导将输出摘要。单击完成关闭向导。

## 使用 **xe CLI** 升级 **Citrix Hypervisor** 服务器

重要：

使用 xe CLI 执行滚动池升级之前需要进行谨慎的规划。请确保在开始之前认真阅读下一节。

### 规划升级路径

在规划升级时，一定要注意以下几点：

- 只能将 VM 从运行早期版本的 Citrix Hypervisor 的 Citrix Hypervisor 服务器迁移到运行相同或更高版本的主机。例如，从版本 7.0 到版本 7.1，或者从版本 7.1 到版本 8.0。不能将 VM 从升级后的主机迁移到运行早期版本的 Citrix Hypervisor 的主机。例如，从版本 8.0 到版本 7.1。请确保在 Citrix Hypervisor 服务器上留出相应的空间。
- 我们强烈建议在非必要情况下不要运行混合模式的池（即一个池中并存多个 Citrix Hypervisor 版本），这是因为在升级过程中，此类池将在降级状态下操作。
- 升级期间，关键的控制操作不可用。请勿尝试执行任何控制操作。尽管 VM 继续正常工作，但除迁移外的其他 VM 操作（例如，关闭、复制和导出）均不可用。具体来说，执行与存储相关的操作（例如添加、删除虚拟磁盘或调整虚拟磁盘大小）是不安全的。
- 请始终优先升级主服务器主机。在执行升级之前，请勿使用 XenCenter 将主机置于维护模式。如果将主机置于维护模式，则将指定一个新主机。
- 升级主机后，请先应用已针对升级后的 Citrix Hypervisor 版本发布的任何修补程序，然后再将 VM 迁移到主机中。
- 我们强烈建议您使用 `pool-dump-database xe` CLI 命令对现有池的状态进行备份。有关详细信息，请参阅[命令行接口](#)。这允许您将部分完成的滚动升级还原到其原始状态而不会丢失任何 VM 数据。如果因任何原因需要还原滚动升级，则可能需要关闭 VM。需要执行此操作，因为不能将 VM 从升级后的 Citrix Hypervisor 服务器迁移到运行较旧版本的 Citrix Hypervisor 的主机。

### 开始执行滚动池升级之前的准备工作

- 如果要使用 XenCenter 进行升级，请将 XenCenter 升级到最新版本。较新版本的 XenCenter 将正确控制较早版本的 Citrix Hypervisor 服务器。
- 清空池中 VM 的 CD/DVD 驱动器。有关详细信息和说明，请参阅升级单个 *Citrix Hypervisor* 服务器之前。
- 禁用高可用性。

### 使用 **xe CLI** 执行滚动池升级

1. 从池主服务器开始升级。使用 `host-disable` 命令禁用主机。这会防止在指定的主机上启动任何新 VM。
2. 请确保池主服务器上未在运行任何 VM。将 VM 关闭、挂起或迁移到池中的其他主机。

要将指定的 VM 迁移到指定的主机，请使用 `vm-migrate` 命令。通过 `vm-migrate` 命令，可以完全控制所迁移的 VM 在池中其他主机上的分布。

要将所有 VM 实时迁移到池中的其他主机，请使用 `host-evacuate` 命令。使用 `host-evacuate` 命令时，所迁移 VM 的分布将由 Citrix Hypervisor 来决定。

3. 关闭池主服务器。

重要：

只有在池主服务器升级完成后，才能与其联系。关闭池主服务器会导致池中的其他主机进入紧急模式。当主机所属池中的主服务器从网络中消失并且经过多次尝试后仍无法联系时，主机会进入紧急模式。VM 在紧急模式的主机上仍然可以运行，但是无法执行控制操作。

4. 使用 Citrix Hypervisor 安装介质和所选方法（如，安装 CD 或网络）引导池主服务器。执行 Citrix Hypervisor 安装过程（请参阅[安装](#)），直到安装程序提供升级选项。选择进行升级。

警告：

- 1 - 请务必选择升级选项，以避免丢失任何现有数据。
- 2
- 3 - 如果任何事情中止了池主服务器的升级，或者如果升级因任何原因失败，请勿尝试继续升级。请重新引导池主服务器，然后还原到该服务器的正常工作版本。

池主服务器重新启动时，池中的其他主机将退出紧急模式，并在几分钟后恢复正常服务。

5. 将已针对新版本的 Citrix Hypervisor 发布的任何修补程序应用到池主服务器。
6. 在池主服务器上，启动或恢复任何已关闭或挂起的 VM。将所需的任何 VM 迁移回池主服务器。
7. 选择升级路径中的下一个 Citrix Hypervisor 服务器。禁用该主机。
8. 确保该主机上未在运行任何 VM。将 VM 关闭、挂起或迁移到池中的其他主机。
9. 关闭主机。
10. 按照第 4 步中针对主服务器的说明执行主机升级过程。

注意：

如果在升级非主服务器的主机时发生故障或者中断，不需要进行恢复。使用 `host-forget` 命令可忽略该主机。在该主机上重新安装 Citrix Hypervisor，然后使用 `pool-join` 命令将该主机作为新主机加入池中。

11. 将已针对新版本的 Citrix Hypervisor 发布的任何修补程序应用到主机。
12. 在该主机上，启动或恢复任何已关闭或挂起的 VM。将所需的任何 VM 迁移回该主机。
13. 对池中的其余主机，重复执行步骤 6 - 10。

## 使用 **xe CLI** 升级单个 **Citrix Hypervisor** 服务器

### 升级单个 **Citrix Hypervisor** 服务器之前的准备工作

在升级独立 Citrix Hypervisor 服务器之前，请将该主机上运行的所有 VM 关闭或挂起。请务必弹出并清空要挂起的任何 VM 的 CD/DVD 驱动器。如果不清空 CD/DVD 驱动器，升级后可能无法恢复挂起的 VM。

空 VM CD/DVD 驱动器是指 VM 既未连接到 ISO 映像，也未连接到通过 Citrix Hypervisor 服务器装载的物理 CD/DVD。此外，必须确保 VM 未连接到 Citrix Hypervisor 服务器上的任何物理 CD/DVD 驱动器。

要使用 **xe CLI** 清空 VM 的 **CD/DVD** 驱动器，请执行以下操作：

1. 通过键入以下命令确定哪些 VM 的 CD/DVD 驱动器未清空：

```
1 xe vbd-list type=CD empty=false
```

该命令将返回所有非空的 VM CD/DVD 驱动器的列表，例如：

```
1      uuid ( RO) : abae3997-39af-2764-04a1-ffc501d132d9
2      vm-uuid ( RO): 340a8b49-866e-b27c-99d1-fb41457344d9
3      vm-name-label ( RO): VM02_DemoLinux
4      vdi-uuid ( RO): a14b0345-b20a-4027-a233-7cbd1e005ede
5      empty ( RO): false
6      device ( RO): xvdd
7
8      uuid ( RO) : ec174a21-452f-7fd8-c02b-86370fa0f654
9      vm-uuid ( RO): db80f319-016d-0e5f-d8db-3a6565256c71
10     vm-name-label ( RO): VM01_DemoLinux
11     vdi-uuid ( RO): a14b0345-b20a-4027-a233-7cbd1e005ede
12     empty ( RO): false
13     device ( RO): xvdd
```

记下 **uuid**，即列表中的第一个条目。

2. 要清空所列出的 VM 的 CD/DVD 驱动器，请键入以下命令：

```
1 xe vbd-eject uuid=uuid
```

使用 **xe CLI** 升级单个 **Citrix Hypervisor** 服务器

使用 **xe CLI** 升级单个 **Citrix Hypervisor** 服务器：

1. 通过键入以下命令禁用要升级的 Citrix Hypervisor 服务器：

```
1 xe host-disable host-selector=host_selector_value
```

禁用 Citrix Hypervisor 服务器后，将无法在该主机上创建或启动 VM。也不能将虚拟机迁移到已禁用的主机上。

2. 使用 `xe vm-shutdown` 或 `xe vm-suspend` 命令关闭或挂起要升级的主机上的任何 VM。
3. 使用 `xe host-shutdown` 命令关闭主机。
4. 执行 Citrix Hypervisor 安装过程，直到安装程序提供升级选项。选择进行升级。有关详细信息，请参阅[安装](#)。

**警告：**

请务必选择升级选项，以避免丢失任何现有数据。

不需要在设置过程中重新配置任何设置。升级过程与首次安装过程基本相同，但会跳过几个设置步骤。保留网络连接配置、系统时间等现有设置。

主机重新启动后，几分钟后可恢复正常服务。

5. 应用已针对新版本的 Citrix Hypervisor 发布的任何修补程序。
6. 重新启动所有已关闭的 VM，并恢复所有挂起的 VM。

## 更新您的主机

July 10, 2019

通常，可以在保证服务中断最小化的情况下应用更新。我们建议客户使用 XenCenter 应用所有更新。如果要更新 Citrix Hypervisor 池，可以使用 XenCenter 中的安装更新向导来避免 VM 停机。安装更新向导将应用更新，一次更新一个主机并在应用修补程序或更新时从每个主机中自动迁出 VM。

可以将 XenCenter 配置为定期检查可用的 Citrix Hypervisor 和 XenCenter 更新及新版本。所有警报都将在通知窗格中显示。

### 更新的类型

以下类型的更新对 Citrix Hypervisor 可用：

- 当前版本 (**CR**)，CR 流中的完整 Citrix Hypervisor 发行版。某些 CR 可以作为更新应用到 CR 流中的受支持的 Citrix Hypervisor 版本。
- 修补程序，通常为一个或多个特定问题提供缺陷修复。修补程序针对长期服务版本 (LTSR) 和当前版本 (CR) 流中的 Citrix Hypervisor 发行版以及不属于其中任一流的一部分的早期受支持版本提供。
- 累积更新，其中包含以前发布的修补程序，并且可能包含对新来宾和硬件的支持。累积更新适用于长期服务版本 (LTSR) 流中的 Citrix Hypervisor 发行版。

还可以将我们的合作伙伴提供的补充包作为更新应用到 Citrix Hypervisor。

### 当前版本

Citrix Hypervisor 8.0 是 Citrix Hypervisor 的当前版本。但是，由于 Citrix Hypervisor 8.0 是平台刷新，因此，无法将其作为更新应用到 XenServer 的早期版本。

对于这些不能作为更新应用 Citrix Hypervisor 8.0 的 XenServer 的各版本，请改为使用基本安装 ISO 并升级现有安装。

### 修补程序

我们可能会发布适用于 Citrix Hypervisor 8.0 的修补程序，用于提供针对特定问题的修复。

Citrix Hypervisor 8.0 的修补程序可以从 [Citrix 知识中心](#) 获取。我们建议客户定期在知识中心中查找是否有新的更新。或者，可以通过在 <http://www.citrix.com.cn/support.html> 注册一个帐户来订阅针对 Citrix Hypervisor 的更新的电子邮件警报。

最新 CR 中的修补程序适用于所有 Citrix Hypervisor 客户。但是，仍然受支持的早期 CR 中的修补程序仅适用于具有活动 Citrix Customer Success Services (CSS) 帐户的客户。

LTSR 流中的修补程序适用于具有活动 CSS 帐户的客户。有关详细信息，请参阅 [许可](#)。

### 累积更新

累积更新针对 Citrix Hypervisor 的 LTSR 提供。这些更新提供问题的修复，并且可能包含面向新来宾和硬件的支持。

累积更新适用于具有活动 CSS 帐户的客户。

Citrix Hypervisor 8.0 是当前版本。未提供任何面向此版本的累积更新。

### 准备池以进行更新

Citrix Hypervisor 的更新可以通过修补程序、累积更新或当前版本的方式提供。必须特别注意随每个更新发布的发行说明。每个更新都可能具有独特的安装说明，特别是对于准备操作和更新后操作。以下几部分内容将介绍对您的 Citrix Hypervisor 系统应用更新的常规指南和说明。

#### 重要：

对 Citrix Hypervisor 池应用更新之前，请特别注意以下事项：

- (仅适用于 Citrix Hypervisor 8.0 修补程序) 池中的所有主机都必须运行 Citrix Hypervisor 8.0，才能应用修补程序。
- 先备份您的数据，然后再应用更新。有关备份过程，请参阅 [灾难恢复和备份](#)。
- 在短时间内更新池中的所有服务器：不支持运行混合模式的池（即同时包含已更新的服务器和未更新的服务器的池）这种配置。安排更新，以将池在混合模式下运行的时间缩至最短。
- 按顺序更新池中的所有服务器，请始终先更新池主服务器。XenCenter 的安装更新向导会自动管理此过程。
- 对池中的所有主机应用更新后，请在重新启动 Citrix Hypervisor 服务器之前更新所需的任何驱动程序磁盘。
- 将累积更新或当前版本应用到主机后，请先应用针对该累积更新或当前版本发布的任何修补程序，然后再将 VM 迁移到主机中。

### 开始更新之前

- 以具有完全访问权限的用户帐户（例如，作为池管理员或使用本地 root 帐户）登录。
- 清空要挂起的任何 VM 的 CD/DVD 驱动器。有关详细信息和说明，请参阅[升级单个 Citrix Hypervisor 服务器之前的准备工作](#)。
- 如果适用，请禁用高可用性。

### 对池应用更新

XenCenter 中的更新安装机制允许您从支持 Web 站点下载和提取选定的更新。可以使用安装更新向导同时对多个主机和池应用更新。在此过程中，安装更新向导将针对每个服务器完成以下步骤：

- 将 VM 迁移出服务器
- 将服务器置于维护模式
- 对服务器应用更新
- 如有必要，请重新启动主机
- 将 VM 迁移回更新后的主机。

在预检阶段为应用更新而执行的任何操作（例如关闭高可用性）都将被还原。

安装更新向导在启动更新过程之前将执行一系列的检查，称为“预检查”。这些检查可以确保池处于有效的配置状态。然后，它会自动管理更新路径和 VM 迁移。如果您愿意手动控制更新路径和 VM 迁移，则可以分别更新每个主机。

### 自动应用更新

XenCenter 允许您应用使服务器保持最新所需的自动更新。可以对一个或多个池应用这些更新。应用自动更新时，XenCenter 将应用使选定池或独立服务器保持更新所需的最少更新集。XenCenter 将使池或独立服务器池保持最新所需执行的重新启动次数降至最低。XenCenter 尽可能只在结束时重新启动一次。有关详细信息，请参阅[应用自动更新](#)。

### 查看可用更新

通知视图的更新部分列出了适用于所有已连接的服务器和池的更新。

注意：

- 默认情况下，XenCenter 将定期检查 Citrix Hypervisor 和 XenCenter 更新。单击刷新可手动检查可用更新。
- 如果更新选项卡因自动检查更新功能已禁用而找不到任何更新，则更新选项卡上将显示相应消息。单击立即检查更新以手动检查更新。

可以从查看列表中选择按更新还是按服务器查看更新列表。

“按更新”查看更新列表时，XenCenter 将显示更新列表。可以按服务器/池或按日期订购这些更新。

- 累积更新和新版本将在此列表的顶部显示。并非所有新版本都可以作为更新进行应用。
- 要将此信息导出为.csv 文件，请单击全部导出。.csv 文件将列出以下信息：
  - 更新名称
  - 更新说明
  - 可以应用此更新的服务器
  - 更新的时间戳
  - 对从中下载更新的 Web 页面的引用
- 要对服务器应用更新，请从该更新的操作列表中选择下载并安装。此选项将提取更新，并在选择了相关服务器的选择服务器页面上打开安装更新向导。有关详细信息，请参阅对池应用更新。
- 要在浏览器中打开更新的发行说明，请单击操作列表，然后选择转至 **Web** 页面。

按服务器查看更新列表时，XenCenter 将显示连接到 XenCenter 的服务器的列表。此列表同时显示可以对服务器应用的更新以及在服务器上安装的更新。

- 要将此信息导出为.csv 文件，请单击全部导出。.csv 文件将列出以下信息：
  - 服务器所属的池
  - 服务器名称
  - 已安装的状态 Citrix Hypervisor
  - 服务器的更新状态
  - 此服务器所需的更新
  - 此服务器的已安装的更新。
- 要应用更新，请单击安装更新。此选择将在“选择更新”页面上打开安装更新向导。有关详细信息，请参阅对池应用更新。

#### 对池应用更新

要使用 XenCenter 对池应用更新，请执行以下操作：

1. 在 XenCenter 菜单中，依次选择工具和安装更新。
2. 阅读准备工作页面上显示的信息，然后单击下一步。
3. “安装更新”向导会在选择更新页面列出可用的更新。从列表中选择所需的更新，然后单击下一步。
4. 在“选择服务器”页面上，选择要更新的池和服务器。

应用累积更新或当前版本时，还可以选择是否应用 CU 或 CR 的最小修补程序集。

单击下一步。

5. 安装更新向导将执行多项更新预检查，以确保池处于有效的配置状态。此外，该向导还会在应用更新后检查是否必须重新启动主机并显示结果。安装更新向导还将检查实时修补程序是否适用于修补程序以及是否能够将实时修补程序应用到主机。有关实时修补的信息，请参阅实时修补。

6. 按照屏幕上的建议进行操作以解决任何失败的更新预检查。如果希望 XenCenter 自动解决所有失败的预检查，请单击全部解决。解决预检查问题后，单击下一步。
7. 如果要安装 CU 或 CR，XenCenter 将下载更新，将其上载到池的默认 SR 并安装更新。上载并安装页面将显示进度。

注意：

- 1 - 如果池中的默认 SR 未共享，或者空间不足，XenCenter 会尝试将更新上载到另一个共享 SR。如果所有共享 SR 的空间都不足，更新将上载到池主服务器上的本地存储。 - 如果更新过程因任何原因无法完成，XenCenter 将终止该进程。这样，您可以解决此问题，然后通过单击\*\*重试\*\*按钮继续执行更新过程。

请参见步骤 10 以完成安装过程。

8. 如果要安装修补程序，请选择更新模式。检查屏幕上显示的信息，然后选择恰当的模式。如果修补程序包含能够成功应用到主机的实时修补程序，则将在要执行的任务屏幕上显示 `No action required`。

注意：

如果在此阶段单击取消，“安装更新”向导将还原更改，并从服务器删除更新文件。

9. 单击安装更新以继续进行安装。“安装更新”向导将显示更新进度，同时显示在更新池中的每个主机时 XenCenter 执行的主要操作。
10. 应用更新后，单击完成关闭“安装更新”向导。如果选择手动执行更新后任务，请立即执行。

## 使用 **xe CLI** 更新 **Citrix Hypervisor** 服务器池

要使用 xe CLI 更新 Citrix Hypervisor 主机池，请执行以下操作：

1. 将更新文件下载到运行 xe CLI 的计算机上的已知位置。记下该文件的路径。
2. 通过运行以下命令，将更新文件上载到要更新的池：

```
1 xe -s server -u username -pw password update-upload file-name=
  filename [sr-uuid=storage_repository_uuid]
```

此处，`-s` 是指池主服务器的名称。Citrix Hypervisor 为更新文件分配一个 UUID，此命令将输出此 UUID。记下该 UUID。

提示：

将更新文件上载到 Citrix Hypervisor 服务器后，可以使用 `update-list` 和 `update-param-list` 命令查看与该文件有关的信息。

3. 如果 Citrix Hypervisor 检测到任何错误或者尚未执行任何准备步骤，则会向您发出警报。请确保在继续更新之前按照所有的指导操作。

如有必要，可以使用 `vm-shutdown` 或 `vm-suspend` 命令关闭或挂起要更新的主机上正在运行的任何 VM。

要将指定的 VM 迁移到指定的主机，请使用 `vm-migrate` 命令。通过 `vm-migrate` 命令，可以完全控制所迁移的 VM 在池中其他主机上的分布。

要自动将所有 VM 实时迁移到池中的其他主机，请使用 `host-evacuate` 命令。使用 `host-evacuate` 命令时，所迁移 VM 的分布将由 Citrix Hypervisor 来决定。

4. 通过运行以下命令更新池，命令中应指定更新文件的 UUID：

```
1 xe update-pool-apply uuid=UUID_of_file
```

此命令将对池中的所有主机应用更新或修补程序，首先对池主服务器应用。

或者，要以滚动方式更新和重新启动主机，可以通过运行以下命令将更新文件应用到各个主机：

```
1 xe update-apply host=host uuid=UUID_of_file
```

请务必先更新池主服务器，然后再更新任何其他池成员。

5. 使用 `update-list` 命令验证是否已应用更新。如果更新成功，`hosts` 字段将包含主机 UUID。
6. 执行所需的所有更新后操作（例如，重新启动 XAPI Toolstack 或者重新启动主机）。请先在池主服务器上执行这些操作。

### 使用 **xe CLI** 更新各个主机

要使用 `xe CLI` 更新各个主机，请执行以下操作：

1. 将更新文件下载到运行 `xe CLI` 的计算机上的已知位置。记下该文件的路径。
2. 使用 `vm-shutdown` 或 `vm-suspend` 命令关闭或挂起要更新的主机上的任何 VM。
3. 通过运行以下命令，将更新文件上传到要更新的主机：

```
1 xe -s server -u username -pw password update-upload file-name=
   filename [sr-uuid=storage_repository_uuid]
```

此处，`-s` 是指主机名。Citrix Hypervisor 为更新文件分配一个 UUID，此命令将输出此 UUID。记下该 UUID。

提示：

将更新文件上传到 Citrix Hypervisor 服务器后，可以使用 `update-list` 和 `update-param-list` 命令查看与更新文件有关的信息。

4. 如果 Citrix Hypervisor 检测到任何错误或者尚未执行任何准备步骤，则会向您发出警报。请确保在继续更新之前按照所有的指导操作。
5. 通过运行以下命令更新主机，命令中应指定主机和更新文件的 UUID：

```
1 xe update-apply host-uuid=UUID_of_host uuid=UUID_of_file
```

如果主机属于池成员，请务必先更新池主服务器，然后再更新任何其他池成员。

6. 使用 `update-list` 命令验证是否已成功应用更新。如果更新成功，`hosts` 字段将包含主机 UUID。

7. 如有必要，请执行所有更新后操作（例如，重新启动 XAPI Toolstack 或者重新启动主机）。

## 应用自动更新

自动更新模式应用适用于主机的任何修补程序和累积更新。此模式将使池或独立服务器池保持最新所需执行的重新启动次数降至最低。自动更新模式最后会尽可能将重新启动次数限制为一次。

如果新的当前版本以更新方式提供，自动更新模式将不应用此更新。相反，必须手动选择才能更新到新的当前版本。

XenCenter 需要 Internet 访问权限才能提取所需的更新。

要查看必需的更新列表，请执行以下步骤：

1. 在 XenCenter 的“资源”窗格中选择主机。
2. 导航到常规选项卡。
3. 展开更新部分。

此时可以看到以下内容：

- 已应用 - 列出已应用的更新。
- 必需的更新 - 列出使服务器保持最新所需的更新集。

注意：

如果不需要安装任何更新，则不显示必需的更新部分。

- 安装的补充包 - 列出服务器上安装的补充包（如果存在）。

注意：

如果选择池而非服务器，“更新”部分会将已应用的更新作为已完全应用列出。

如果要选择并安装特定更新，请参阅对池应用更新部分。

注意：

自动更新功能适用于 Citrix Hypervisor Premium Edition 客户或通过 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。要了解有关 Citrix Hypervisor 各版本以及如何升级的详细信息，请访问 [Citrix Web 站点](#)。有关详细信息，请参阅[许可](#)。

自动更新功能适用于 Citrix Hypervisor Premium Edition 客户。

## 使用“安装更新”向导应用自动更新

以下部分提供了有关如何自动应用所需的更新集以使您的池或独立主机保持最新的操作步骤说明。

1. 在 XenCenter 菜单中，依次选择工具和安装更新。
2. 阅读准备工作页面上显示的信息，然后单击下一步。
3. 在“选择更新”页面上，选择要用于安装更新的机制。系统将显示以下选项：
  - 自动更新 - (默认) 仅当 XenCenter 至少连接到一个已获得许可的池或已获得许可的独立服务器时此选项才可见。选择此选项可自动下载并安装所有当前的更新以使池或独立服务器保持最新。
  - 从 Citrix 下载更新 -“安装更新”向导列出了来自支持站点的可用更新。要应用更新，请参阅对池应用更新。
  - 从磁盘中选择更新或补充包 - 要安装已下载的更新，请参阅对池应用更新。要安装补充包更新，请参阅 XenCenter 帮助中的安装补充包部分。
4. 要继续自动应用修补程序，请选择自动更新，然后单击下一步。
5. 选择要更新的一个或多个池或独立服务器，然后单击下一步。无法更新的所有服务器或池都显示为不可用。
6. 安装更新向导将执行多项更新预检查，以确保池处于有效的配置状态。

按照屏幕上的建议进行操作以解决任何失败的更新预检查。如果希望 XenCenter 自动解决所有失败的预检查，请单击全部解决。解决预检查问题后，单击下一步。

7. 安装更新向导将自动下载并安装建议的更新。该向导还显示更新的整体进度，显示在更新池中的每个服务器时 XenCenter 执行的主要操作。

### 注意：

- 1 - 更新将上载到池的默认 SR。如果默认 SR 未共享，或者空间不足，XenCenter 会尝试将更新上载到具有足够空间的其他共享 SR。如果所有共享 SR 的空间都不足，更新将上载到每个主机上的本地存储。
- 2
- 3 - 更新过程因任何原因无法完成，XenCenter 将终止该进程。这样，您可以解决此问题，然后通过单击\*\*重试\*\*按钮继续执行更新过程。

8. 应用所有更新后，单击完成关闭“安装更新”向导。

## Citrix Hypervisor 中的实时修补

实时修补功能仅适用于修补程序。不能作为实时修补程序应用当前版本和累积更新。

部署了 Citrix Hypervisor 服务器的 Citrix Hypervisor 客户在应用修补程序后通常可以重新启动其主机。此重新启动会导致主机出现不必要的停机时间，在此期间，客户需要等到系统完成重新启动。此不必要的停机会影响业务。通过实

时修补，客户能够安装某些 Linux 内核和 Xen 虚拟机管理程序修补程序，而不需要重新启动主机。此类修补程序包括一个要应用到主机内存的实时修补程序以及一个用于更新磁盘上的文件的修补程序。通过使用实时修补可以降低维护成本并缩短停机时间。

使用 XenCenter 应用更新时，安装更新向导必须在应用更新后检查是否必须重新启动主机，XenCenter 并在预检查页面上显示结果。此检查使客户能够提前充分了解更新后任务并相应地安排应用修补程序。

**注意：**

Citrix Hypervisor 实时修补适用于 Citrix Hypervisor Premium Edition 客户或通过 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。要了解有关 Citrix Hypervisor 各版本以及如何升级的详细信息，请访问 [Citrix Web 站点](#)。有关许可的详细信息，请参阅[许可](#)。

### 实时修补场景

可以跨池和主机或者在独立服务器上实时修补修补程序。有些修补程序需要重新启动，有些修补程序需要重新启动 XAPI Toolstack，有些修补程序不需要执行任何更新后任务。以下场景描述了实时修补程序适用于以及不适用于更新时的行为。

- 通过实时修补程序更新 - 更新 Linux 内核和 Xen 虚拟机管理程序的某些修补程序在应用修补程序后通常不需要重新启动。但是，在极少数情况下，如果无法应用实时修补程序，则可能需要重新启动。
- 不通过实时修补程序更新 - 此时行为没有任何变化。它将照常运行。

**注意：**

如果主机不要求重新启动，或者如果修补程序包含实时修补程序，XenCenter 将在“更新模式”页面上显示 **No action required**。

### 应用自动更新与实时修补

XenCenter 中的自动更新模式允许您自动下载并应用使您的池或独立主机保持最新所需的最小修补程序集。自动更新模式不应用适用于主机的任何累积更新。但是，如果新的当前版本以更新方式提供，自动更新模式将不应用此更新。必须手动选择才能更新到新的当前版本。

使用 XenCenter 中的“自动更新”模式应用修补程序时，您将受益于实时修补功能。如果实时修补程序可用，并且成功应用到使用自动更新模式更新的主机，则可以避免重新启动主机。有关“自动更新”模式的详细信息，请参阅[应用自动更新](#)。

### 使用 XenCenter 和 xe CLI 启用实时修补

默认启用实时修补功能。客户可以使用 XenCenter 或 xe CLI 命令启用或禁用实时修补。

### 使用 XenCenter

1. 在“资源”窗格中选择池或独立主机。
2. 在池菜单（如果在独立主机上，则为服务器）中，选择属性，然后单击实时修补。
3. 在“实时修补”页面上执行以下操作：
  - 选择尽可能使用实时修补可启用实时修补。
  - 选择不使用实时修补可禁用实时修补。

### 使用 xe CLI

- 要启用实时修补，请运行以下命令：

```
1 xe pool-param-set live-patching-disabled=false uuid="pool_uuid"
```

- 要禁用实时修补，请运行以下命令：

```
1 xe pool-param-set live-patching-disabled=true uuid="pool_uuid"
```

## 对安装问题进行故障排除

June 4, 2019

Citrix 提供两种形式的支持服务：[www.citrix.com/support](http://www.citrix.com/support) 上的免费自助支持以及付费的支持服务（可以从支持站点购买）。通过 Citrix 技术支持，您可以打开在线支持案例或者通过电话与支持中心联系。

Citrix 支持站点 [www.citrix.com/support](http://www.citrix.com/support) 托管各种资源。当您在安装过程中遇到异常行为、崩溃或其他问题时，这些资源可能会对您有所帮助。资源包括：论坛、知识库文章、软件更新、安全公告、工具和产品文档。

在安装期间，使用与主机直接连接（不是通过串行端口连接）的键盘，可以访问三个虚拟终端：

- 按 **Alt+F1** 可访问主 Citrix Hypervisor 安装程序
- 按 **Alt+F2** 可访问本地 shell
- 按 **Alt+F3** 可访问事件日志

如果在安装过程中遇到未知错误，请从您的主机中捕获日志文件并将其提供给技术支持人员。要捕获日志文件，请完成以下过程。

捕获并保存日志文件：

1. 按 **Alt+F2** 访问本地 shell。
2. 输入以下命令：

```
1 /opt/xensource/installer/report.py
```

3. 系统将提示您选择要用来保存日志文件的位置：**NFS**、**FTP** 或 **Local media**（本地介质）。

选择 **NFS** 或 **FTP** 可将日志文件复制到网络上的其他计算机。要执行此操作，网络连接必须正常，而且您必须对远程计算机具有写入访问权限。

选择 **Local media**（本地介质）可将日志文件保存到本地计算机上的可移动存储设备（如 USB 闪存驱动器）。

在进行选择之后，程序会将日志文件写入所选位置。文件名为 `support.tar.bz2`。

请将捕获的日志文件发送给支持团队以便其进行检查。

## 从 SAN 环境引导

June 4, 2019

从 SAN 环境引导有许多好处，其中包括较高的性能、冗余度和空间合并。在这些环境中，引导磁盘位于远程 SAN（而非本地主机）上。主机通过主机总线适配器 (HBA) 与 SAN 通信。HBA 的 BIOS 中包含允许主机查找引导磁盘的说明。

从 SAN 引导取决于主机上具有硬件光线通道或 HBA iSCSI 适配器支持的、基于 SAN 的磁盘阵列。如果要从 SAN 环境进行完全冗余的引导，必须为 I/O 访问配置多个路径。为此，请确保根设备已启用多路径支持。有关 SAN 环境是否支持多路径的信息，请咨询您的存储供应商或管理员。如果您有多个路径可用，则可以在安装时在 Citrix Hypervisor 部署中启用多路径。

### 警告：

在升级过程中，不继承“从 SAN 引导”设置。使用 ISO 或网络引导过程进行升级时，请按照在下面的安装过程中使用的相同说明进行操作，确保正确配置 `multipath`。

将 **Citrix Hypervisor** 安装到启用了多路径的 **SAN** 上的远程磁盘：

1. 在“欢迎使用 Citrix Hypervisor”屏幕上，按 **F2** 键。
2. 在引导提示符下，输入 `multipath`

Citrix Hypervisor 安装过程配置 Citrix Hypervisor 服务器从启用了多路径的远程 SAN 引导。

要使用 PXE 或 UEFI 安装来启用文件系统多路径，请将 `device_mapper_multipath=yes` 添加到您的配置文件中。下面是一个示例配置：

```
1 default xenserver
2 label xenserver
3 kernel mboot.c32
4 append /tftpboot/xenserver/xen.gz dom0_max_vcpus=1-2 \
5 dom0_mem=1024M,max:1024M com1=115200,8n1 \
```

```
6 console=com1,vga --- /tftpboot/xenserver/vmlinuz \  
7 xencons=hvc console=hvc0 console=tty0 \  
8 device_mapper_multipath=yes \  
9 install --- /tftpboot/xenserver/install.img
```

有关 Citrix Hypervisor 环境中存储多路径的其他信息，请参阅[存储](#)。

### 适用于 **Cisco UCS** 的 **Software-boot-from-iSCSI**

通过 Software-boot-from-iSCSI 功能，客户能够使用 iSCSI 从 SAN 安装和引导 Citrix Hypervisor。使用此功能，可以将 Citrix Hypervisor 安装到 iSCSI 目标提供的 LUN 中以及从中引导和运行。iSCSI 目标在 iSCSI 引导固件表中指定。此功能允许客户通过 iSCSI 连接根磁盘。

Citrix Hypervisor 支持 Software-boot-from-iSCSI 的以下功能：

- 通过 PXE 引导进行主机安装
- Cisco UCS vNIC  
已使用 Cisco UCS vNIC 以及 Power Vault、NetApp 和 EqualLogic 阵列在旧版 BIOS 和 UEFI 引导模式下测试 Software-boot-from-iSCSI。使用其他配置或许也能运行该功能，但尚未经过验证。
- 通过 Cisco UCS 配置了 Jumbo 帧 (MTU=9000)
- Cisco UCS 线路速率限制
- 无标记的 VLAN
- 使用 vSwitch 后端的网络
- 相同或不同 SAN/NAS 上存在 LVHDoiSCSI SR 和 NFS SR
- iSCSI 根磁盘的多路径
- 与常见的 Citrix Hypervisor（网络、维护）操作兼容

#### 要求

- 主管理接口（可通过 IP 地址访问）和用于传输 VM 流量的网络必须使用不同的接口。
- 存储（iSCSI 目标）所在的第 3 层 (IP) 网络必须与使用主机上的 IP 地址的所有其他网络接口不同。
- 存储必须与 Citrix Hypervisor 服务器的存储接口位于相同的子网中。

### 使用 **CD** 介质安装 **Citrix Hypervisor**

要使用 CD 安装 Citrix Hypervisor，请执行以下步骤：

1. 访问引导菜单；在 `boot:` 提示符下输入 `menu.c32`
2. 使用光标键选择安装选项：
  - 对于单路径 LUN，请选择 **install**
  - 对于多路径 LUN，请选择 **multipath**
3. 按 **Tab** 键。

编辑包含以下命令的行结尾：

```
1 --- /install.img
```

4. 使用光标键编辑此行，使其显示为：

```
1 use_ibft --- /install.img
```

5. 按 **Enter** 键。

Citrix Hypervisor 服务器安装将继续正常进行。

## 使用 PXE 安装 Citrix Hypervisor

要使用 PXE 安装 Citrix Hypervisor，请执行以下步骤：

注意：

请务必在内核参数中添加关键字 **use\_ibft**。如果需要多路径，则必须添加 **device\_mapper\_multipath=enabled**。

下例显示了适用于单 LUN 的 PXE 配置：

```
1 label xenserver
2 kernel mboot.c32
3 append XS/xen.gz dom0_max_vcpus=2 dom0_mem=1024M,max:1024M
4 com1=115200,8n1 console=com1,vga --- XS/vmlinuz xencons=hvc
   console=tty0
5 console=hvc0 use_ibft --- XS/install.img
```

下例显示了适用于多路径 LUN 的 PXE 配置：

```
1 label xenserver
2 kernel mboot.c32
3 append XS/xen.gz dom0_max_vcpus=2 dom0_mem=1024M,max:1024M
4 com1=115200,8n1 console=com1,vga --- XS/vmlinuz xencons=hvc
   console=tty0
5 console=hvc0 use_ibft device_mapper_multipath=enabled --- XS/
   install.img
```

## 网络引导安装

June 4, 2019

Citrix Hypervisor 支持使用 UEFI 模式引导主机。UEFI 模式向 Bootloader 和操作系统提供了一套丰富的标准化工具。此功能使客户能够更加轻松地在默认引导模式为 UEFI 的主机上安装 Citrix Hypervisor。

以下部分介绍如何将 TFTP 和 NFS、FTP 或 HTTP 服务器设置为对 Citrix Hypervisor 服务器安装启用 PXE 和 UEFI 引导。然后说明如何创建 XML 应答文件，通过该文件可以执行无人参与安装。

### 为 Citrix Hypervisor 安装配置 PXE 和 UEFI 环境

在设置 Citrix Hypervisor 安装介质之前，请配置 TFTP 和 DHCP 服务器。以下部分介绍如何将您的 TFTP 服务器配置为进行 PXE 和 UEFI 引导。有关常规设置过程，请查阅供应商文档。

**注意：**

Citrix Hypervisor 6.0 已从 MBR 磁盘分区方案改为使用 GUID 分区表 (GPT)。某些第三方 PXE 部署系统在将映像部署到主机之前，可能会尝试读取该计算机硬盘上的分区表。

如果部署系统与 GPT 分区方案不兼容，并且以前使用该硬盘的 Citrix Hypervisor 版本使用的是 GPT，PXE 部署系统可能会出现故障。此故障的解决方法是删除磁盘上的分区表。

除了 TFTP 和 DHCP 服务器外，还需要一个 NFS、FTP 或 HTTP 服务器来保存 Citrix Hypervisor 安装文件。这些服务器可在同一个服务器上共存，也可分布在网络中的不同服务器上。

此外，每个要进行 PXE 引导的 Citrix Hypervisor 服务器都必须具有一个启用了 PXE 引导的以太网卡。

以下步骤假定所用 Linux 服务器支持 RPM。

### 将 TFTP 服务器配置为进行 PXE 引导

1. 在 `/tftboot` 目录中，创建一个名为 `xenserver` 的目录
2. 将 `mboot.c32` 和 `pxelinux.0` 文件从 `/usr/lib/syslinux` 目录复制到 `/tftboot` 目录。

**注意：**

我们强烈建议您使用来自同一个来源（例如，来自同一个 Citrix Hypervisor ISO）的 `mboot.c32` 和 `pxelinux.0` 文件。

3. 在 Citrix Hypervisor 安装介质中，将文件 `install.img`（来自根目录）、`vmlinuz` 和 `xen.gz`（来自 `/boot` 目录）复制到 TFTP 服务器上的新 `/tftboot/xenserver` 目录。
4. 在 `/tftboot` 目录中，创建一个名为 `pxelinux.cfg` 的目录。

5. 在 `pxelinux.cfg` 目录中，创建名为 `default` 的配置文件。

此文件的内容取决于您对 PXE 引导环境的配置。下面列出了两个示例配置。第一个示例配置在从 TFTP 服务器引导的任何计算机上启动安装过程。此安装过程要求手动响应。第二个示例配置适用于无人参与安装。

注意：

以下示例显示了如何将安装程序配置为在物理控制台 `tty0` 上运行。要使用其他默认设置，应确保您要使用的控制台在最右侧。

```

1  default xenserver
2  label xenserver
3      kernel mboot.c32
4      append /tftpboot/xenserver/xen.gz dom0_max_vcpus=2 \
5          dom0_mem=1024M,max:1024M com1=115200,8n1 \
6          console=com1,vga --- /tftpboot/xenserver/vmlinuz \
7          xencons=hvc console=hvc0 console=tty0 \
8          --- /tftpboot/xenserver/install.img

```

使用位于指定 URL 的应答文件执行无人参与安装的示例配置：

注意：

要指定用于检索应答文件的网络适配器，请将 `answerfile_device=ethX` 或 `answerfile_device=MAC` 参数包括在内，并指定该设备的以太网设备号或 MAC 地址。

```

1  default xenserver-auto
2  label xenserver-auto
3      kernel mboot.c32
4      append /tftpboot/xenserver/xen.gz dom0_max_vcpus=2 \
5          dom0_mem=1024M,max:1024M com1=115200,8n1 \
6          console=com1,vga --- /tftpboot/xenserver/vmlinuz \
7          xencons=hvc console=hvc0 console=tty0 \
8          answerfile=http://pxehost.example.com/answerfile \
9          install --- /tftpboot/xenserver/install.img

```

有关 PXE 配置文件内容的详细信息，请参阅 [SYSLINUX Web 站点](#)。

将 **TFTP** 服务器配置为进行 **UEFI** 引导

将 **TFTP** 服务器配置为进行 **UEFI** 引导：

1. 在 `/tftpboot` 目录中，创建一个名为 `EFI/xenserver` 的目录。
2. 配置 DHCP 服务器以提供 `/EFI/xenserver/grubx64.efi` 作为引导文件。
3. 创建 `grub.cfg` 文件。例如：

- 对于需要手动响应安装提示的安装：

```

1  menuentry "Citrix Hypervisor Install (serial)" {
2
3      multiboot2 /EFI/xenserver/xen.gz dom0_mem=1024M,max:1024M
         watchdog \
4      dom0_max_vcpus=4 com1=115200,8n1 console=com1,vga
5      module2 /EFI/xenserver/vmlinuz console=hvc0
6      module2 /EFI/xenserver/install.img
7  }

```

- 对于使用应答文件的无人参与安装：

```

1  menuentry "Citrix Hypervisor Install (serial)" {
2
3      multiboot2 /EFI/xenserver/xen.gz dom0_mem=1024M,max:1024M
         watchdog \
4      dom0_max_vcpus=4 com1=115200,8n1 console=com1,vga
5      module2 /EFI/xenserver/vmlinuz console=hvc0 console=tty0
         answerfile_device=eth0 answerfile=ftp://ip_address/
         path_to_answerfile install
6      module2 /EFI/xenserver/install.img
7  }

```

有关使用应答文件的详细信息，请参阅为无人参与的 *PXE* 和 *UEFI* 安装创建应答文件。

4. 将 `grub.cfg` 文件复制到 TFTP 服务器上的 `/tftpboot/EFI/xenserver` 目录。
5. 在 Citrix Hypervisor 安装介质中，将文件 `grubx64.efi`、`install.img`（来自根目录）、`vmlinuz` 和 `xen.gz`（来自 `/boot` 目录）复制到 TFTP 服务器上的新 `/tftpboot/EFI/xenserver` 目录。

有关特定操作系统的详细信息，请参阅服务器操作系统手册。此处提供的信息可用作 Red Hat、Fedora 和一些基于 RPM 的其他版本的指南。

在 **HTTP**、**FTP** 或 **NFS** 服务器上设置 **Citrix Hypervisor** 安装介质：

1. 在服务器上，创建一个目录，用于通过 HTTP、FTP 或 NFS 从中导出 Citrix Hypervisor 安装介质。
2. 将 Citrix Hypervisor 安装介质的全部内容复制到 HTTP、FTP 或 NFS 服务器上的新建目录中。此目录将是您的安装库。

注意：

复制 Citrix Hypervisor 安装介质时，请务必将文件 `.treeinfo` 复制到新创建的目录。

准备目标系统：

1. 启动系统并进入引导菜单（在大多数 BIOS 程序中按 **F12** 键）。
2. 选择从以太网卡进行引导。

3. 然后，系统将从您设置的安装源进行 PXE 引导并开始执行安装脚本。如果您设置了一个应答文件，则以无人参与方式执行安装。

### 在 Citrix Hypervisor 安装期间安装补充包

补充包可以通过将软件安装到控制域 (Dom0) 中来修改和扩展 Citrix Hypervisor 的功能。例如，OEM 合作伙伴可能希望在 Citrix Hypervisor 中随附一套需要安装 SNMP 代理才能使用的管理工具。用户可以在初始 Citrix Hypervisor 安装过程中或以后的任意时间添加补充包。

在 Citrix Hypervisor 安装期间安装补充包时，请将每个补充包解压到一个单独的目录中。

此外，还存在一些可供 OEM 合作伙伴在将补充包添加到 Citrix Hypervisor 安装存储库时使用的设施，以允许自动执行出厂安装。

### 创建无人参与 PXE 和 UEFI 安装的应答文件

要以无人参与方式执行安装，请创建一个 XML 应答文件。以下是一个示例应答文件：

```

1  <?xml version="1.0"?>
2    <installation srtype="ext">
3      <primary-disk>sda</primary-disk>
4      <guest-disk>sdb</guest-disk>
5      <guest-disk>sdc</guest-disk>
6      <keymap>us</keymap>
7      <root-password>mypassword</root-password>
8      <source type="url">http://pxehost.example.com/citrix-hypervisor
9        /</source>
10     <post-install-script type="url">
11       http://pxehost.example.com/myscripts/post-install-script
12     </post-install-script>
13     <admin-interface name="eth0" proto="dhcp" />
14     <timezone>Europe/London</timezone>
15   </installation>

```

包含名为 *installation* 的根节点中的所有节点。

#### 注意：

要启用精简预配，请将 `srtype` 属性指定为 `ext`。如果不指定该属性，则默认本地存储类型为 LVM。精简预配将本地存储类型设置为 EXT3 并启用本地缓存，以便 Citrix Virtual Desktops 能够正常运行。有关详细信息，请参阅 [存储](#)。

下表汇总了相应的元素。除非另行说明，否则所有值都是文本。表中指明了哪些是必需的元素。

### <primary-disk>

是否必需是

说明：安装了控制域的存储设备的名称。此元素相当于在手动安装过程的选择主磁盘步骤中所做的选择。

属性：可以指定 `guest-storage` 属性，可能的值为 `yes` 和 `no`。

例如：<code><primary-disk guest-storage="no">sda</primary-disk></code>

默认值为 `yes`。如果指定 `no`，则可以自动执行不创建任何存储库的安装场景。在这种情况下，请不要指定任何 `guest-disk` 键。

### <guest-disk>

是否必需否

说明：用于存储来宾的存储设备的名称。对每个附加磁盘使用其中一个元素。

属性：无

### <keymap>

是否必需是

说明：安装期间使用的键映射名称。<code><keymap>us</keymap></code> 如果不为此元素指定一个值，请考虑默认值 `us`。

属性：无

还可以通过相应地更改应答文件来执行自动升级。将 `installation` 元素的 `mode` 属性设置为 `upgrade`，使用 `existing-installation` 元素指定现有安装所在的磁盘。不指定 `primary-disk` 和 `guest-disk` 元素。例如：

```
1 <?xml version="1.0"?>
2 <installation mode="upgrade">
3     <existing-installation>sda</existing-installation>
4     <source type="url">http://pxehost.example.com/citrix-hypervisor/</
   source>
5     <post-install-script type="url">
6         http://pxehost.example.com/myscripts/post-install-script
7     </post-install-script>
8 </installation>
```

## 主机分区布局

June 4, 2019

Citrix Hypervisor 7.0 引入了全新的主机磁盘分区布局。通过将日志文件移至更大的独立分区，Citrix Hypervisor 可以存储更详细的日志更长时间。此功能改进了诊断问题的能力。同时，新分区布局缓解了对 Dom0 的根磁盘的需求，并且可以避免出现因占用日志文件磁盘空间而导致的潜在空间问题。新布局包含以下分区：

- 大小为 18 GB 的 Citrix Hypervisor 服务器控制域 (dom0) 分区
- 大小为 18 GB 的备份分区
- 大小为 4 GB 的日志分区
- 大小为 1 GB 的交换分区
- 大小为 0.5 GB 的 UEFI 引导分区

在 Citrix Hypervisor 6.5 及早期版本中，大小为 4 GB 的控制域 (dom0) 分区用于所有 dom0 功能，包括交换和日志记录。不使用远程 syslog 的客户或使用第三方监视工具和补充包的客户发现分区大小受到限制。Citrix Hypervisor 解决了此问题，并为 dom0 提供了一个大小为 18 GB 的专用分区。此外，专用于 dom0 的较大分区降低了对 dom0 根磁盘的需求，能够大大提升性能。

引入大小为 4 GB 的专用日志分区后，不会再出现过量日志记录占用 dom0 分区的全部空间并影响主机行为的情形。此分区还使用户能够在更长的时间内保留详细的日志列表，改进了诊断问题的能力。

分区布局还包含一个大小为 500 MB 的分区，专用于 UEFI 引导。

**注意：**

如果要安装包含上述新增分区布局的 Citrix Hypervisor，请确保您具有一个大小至少为 46 GB 的磁盘。

要在更小的设备上安装 Citrix Hypervisor，可以使用旧版 DOS 分区布局执行 Citrix Hypervisor 的全新安装。小型设备是指磁盘空间大于 12 GB 小于 46 GB 的设备。有关详细信息，请参阅[在小型设备上安装](#)。

**重要：**

我们建议您至少分配 46 GB 的磁盘空间，并使用新的 GPT 分区布局安装 Citrix Hypervisor。

### 升级到新分区布局

使用 XenCenter 从 XenServer 6.5 或更早版本升级到 Citrix Hypervisor 8.0 时，主机分区布局将升级到新布局，前提为：

- 本地 SR 上至少包含 46 GB 磁盘空间
- 本地 SR 上不存在 VDI
- 使用随 Citrix Hypervisor 8.0 发布的 XenCenter 执行至 Citrix Hypervisor 8.0 的滚动池升级 (RPU)

**警告：**

客户不能使用 xe CLI 升级到新主机分区布局。

升级过程中，RPU 向导将检查本地 SR 上的 VDI。如果升级过程中不存在任何虚拟磁盘 (VDI)，该向导将提示您移动 VDI。将本地 SR 上的 VDI 移至共享 SR，然后重新启动升级过程以继续使用新布局。如果无法移动 VDI，或者本地 SR 上的空间不足（小于 46 GB），升级将继续使用旧分区布局进行，并从 dom0 分区中分配 0.5 GB 磁盘空间用于 UEFI 引导。

## 还原旧分区布局

如果要将 Citrix Hypervisor 从版本 8.0 还原到版本 6.x，主机分区布局将还原到 6.x 布局。

## 旧版分区布局

- XenServer 5.6 Service Pack 2 及早期版本使用 DOS 分区表将根文件系统和备份与本地存储分离。
- XenServer 6.0 引入了 GUID 分区表，用于将根文件系统和备份与本地存储分离。
- 在必须保留必需初始分区的计算机上通过 Citrix Hypervisor 8.0 安装 XenServer 7.1 将继续使用 DOS 分区方案。

下表列出了安装和升级场景以及在执行这些操作后应用的分区布局：

操作	升级之前的分区数量	安装/升级之后的分区数量	分区表类型
主磁盘空间至少为 46 GB 的全新安装	不适用	6	新 GPT
通过 <code>disable-gpt</code> 执行主磁盘空间至少为 12 GB 的全新安装	不适用	3 (或 4, 如果存在 Utility 分区)	DOS
在具有实用程序分区的计算机上干净安装	不适用	3 (或 4, 如果存在 Utility 分区)	DOS
在本地 SR 上存在 VM 的情况下或主磁盘空间小于 46 GB 的情况下从 Citrix Hypervisor 6.x 进行升级	3	4	旧 GPT
在本地存储中不存在任何 VM 的情况下或主磁盘空间大于 46 GB 的情况下从 Citrix Hypervisor 6.x 进行升级	3	6	新 GPT

操作	升级之前的分区数量	安装/升级之后的分区数量	分区表类型
从 Citrix Hypervisor 6.x DOS 分区 (以及 Utility 分区, 如有) 进行升级	3 (或 4, 如果存在 Utility 分区)	3 (或 4, 如果存在 Utility 分区)	DOS

## 在小型设备上安装

June 4, 2019

Citrix Hypervisor 允许客户使用较小的设备安装使用旧版 DOS 分区布局的 Citrix Hypervisor 8.0。小型设备是指磁盘空间大于 12 GB 小于 46 GB 的设备。旧版 DOS 分区布局包括：

- 大小为 4 GB 的引导分区
- 大小为 4 GB 的备份分区
- SR 分区 (如果存在于本地磁盘上)

要在小型设备上安装 Citrix Hypervisor，必须向 `dom0` 参数中添加 `disable-gpt`。可以使用 `menu.c32` 向 `dom0` 中添加该参数。

### 注意：

安装程序将保留开始执行安装过程之前主机上存在的任何实用程序分区。

### 重要：

我们建议您至少分配 46 GB 的磁盘空间，并使用新的 GPT 分区布局安装 Citrix Hypervisor。有关详细信息，请参阅[主机分区布局](#)。

## 主机和资源池

September 5, 2019

本部分内容通过一系列示例介绍如何使用 `xe` 命令行接口 (CLI) 创建资源池。下面将给出一个简单的基于 NFS 的共享存储配置，并讨论多个简单的 VM 管理示例。还将介绍处理物理节点故障的过程。

## Citrix Hypervisor 服务器和资源池概述

资源池包括多个 Citrix Hypervisor 服务器安装，这些安装绑定在一起形成可以托管虚拟机的单一托管实体。如果与共享存储结合使用，资源池将允许 VM 在该池中内存充足的任何 Citrix Hypervisor 服务器上启动。VM 之后可以在运行时动态地在 Citrix Hypervisor 服务器之间移动，从而最大程度地缩短停机时间（实时迁移）。如果单个 Citrix Hypervisor 服务器发生硬件故障，管理员可以在同一资源池中的另一个 Citrix Hypervisor 服务器上重新启动出现故障的 VM。在资源池上启用了高可用性时，VM 会在其主机发生故障时自动移动。每个资源池最多支持 64 台主机（尽管此限制并不强制执行）。

一个池始终至少包含一个物理节点，称为主节点。只有主节点才会公开（XenCenter 和 Citrix Hypervisor 命令行接口 [称为 xe CLI] 使用的）管理接口。主节点会根据需要向各个成员转发命令。

注意：

如果池的主节点发生故障，只有在启用了高可用性的情况下才会重新选择主节点。

### 创建资源池的要求

资源池是一台或多台同类 Citrix Hypervisor 服务器（或具有限制的异构池）的聚合，每个池最多包含 64 台主机。同类主机的定义是：

- 要加入池的服务器上的 CPU 与池中已有服务器上的 CPU 相同（在供应商、型号和功能方面）。
- 要加入池的服务器运行的 Citrix Hypervisor 软件版本在修补程序级别与池中已有的服务器相同。

向池中加入服务器时，软件将实施附加限制。特别是，Citrix Hypervisor 检查加入池的服务器是否满足以下条件：

- 服务器不是现有资源池的成员。
- 服务器未配置任何共享存储。
- 服务器未托管任何正在运行的或挂起的 VM。
- 服务器上的 VM 上不存在任何正在进行的活动操作，例如 VM 关闭操作。
- 服务器上的时钟同步到与池主服务器相同的时间（例如，通过使用 NTP）。
- 服务器的管理接口未绑定。在服务器成功加入池时可以配置管理接口。
- 管理 IP 地址是静态的（在服务器自身上配置或者使用 DHCP 服务器上的相应配置）。

资源池中的 Citrix Hypervisor 服务器可以包括不同数量的物理网络接口和不同大小的本地存储库。实际上，由于通常很难实现多个服务器使用完全相同的 CPU，因此微小差异是允许的。如果可以接受具有不同 CPU 的主机加入同一个池，可以通过传递 `--force` 参数强制执行池加入操作。

池中的所有主机都必须位于同一个站点中，并且通过低延迟网络连接。

注意：

为池提供共享 NFS 或 iSCSI 存储的服务器必须具有静态 IP 地址。

池必须包含可选择的 Citrix Hypervisor 服务器在其上运行 VM 的共享存储库，以及要在 Citrix Hypervisor 服务器之间动态移动 VM 的共享存储库。如有可能，请在共享存储可用后创建池。我们建议您在添加共享存储后将磁盘位于本地存储中的现有 VM 移动到共享存储。可以使用 `xe vm-copy` 命令或使用 XenCenter 移动 VM。

## 创建资源池

可以使用 XenCenter 或 CLI 创建资源池。新主机加入资源池时，加入的主机会将其本地数据库与池范围内的数据库同步，并从池继承某些设置：

- 将 VM、本地和远程存储配置添加到池范围内的数据库中。除非在主机加入池后明确将资源设置为共享，否则，此配置将应用到池中加入的主机。
- 加入的主机将继承池中现有的共享存储库。创建相应的 PBD 记录，以便新主机能够自动访问现有共享存储。
- 加入的主机会部分继承网络连接信息：全部继承 NIC、VLAN 和绑定接口的结构详细信息，但不继承策略信息。此策略信息必须重新配置，包括：
  - 管理 NIC 的 IP 地址，这类地址通过原始配置保留。
  - 管理接口的位置，保持与原始配置相同。例如，如果其他池主机的管理接口位于绑定接口上，则加入的主机在加入后必须立即迁移到绑定。
  - 专用存储 NIC，必须通过 XenCenter 或 CLI 重新分配给加入的主机，并相应地重新插入 PBD 以路由流量。这是因为加入到池的操作中并不包含分配 IP 地址这一步骤，并且存储 NIC 仅在正确配置了 IP 地址时才能运行。有关如何通过 CLI 指定专用存储 NIC 的详细信息，请参阅[管理网络连接](#)。

### 注意：

仅当新主机的管理接口位于与某个资源池相同的已标记 VLAN 上时，才能将该主机加入该资源池。

## 使用 CLI 将 Citrix Hypervisor 服务器 `host1` 和 `host2` 加入到资源池

1. 在 Citrix Hypervisor 服务器 `host2` 上打开控制台。
2. 运行以下命令，指示 Citrix Hypervisor 服务器 `host2` 加入位于 Citrix Hypervisor 服务器 `host1` 上的池中：

```
1 xe pool-join master-address=host1 master-username=
   administrators_username master-password=password
```

`master-address` 必须设置为 Citrix Hypervisor 服务器 `host1` 的完全限定域名。安装 Citrix Hypervisor 服务器 `host1` 时，`password` 必须为设置的管理员密码。

默认情况下，Citrix Hypervisor 服务器属于未命名池。要创建您的第一个资源池，请重命名现有的无名称的池。使用 `tab-complete` 查找 `pool_uuid`：

```
1 xe pool-param-set name-label="New Pool" uuid=pool_uuid
```

### 创建异构资源池

Citrix Hypervisor 允许将完全不同的主机硬件加入资源池（称为异构资源池），从而简化了不断扩展部署的过程。异构资源池使用提供 CPU“屏蔽”或“调配”的 Intel (FlexMigration) 和 AMD (Extended Migration) CPU 中的技术来实现。通过 CPU 屏蔽和调配功能，可以将 CPU 配置为看起来提供与实际不同的样式、型号或功能。此功能允许您创建主机池，尽管这些池具有完全不同的 CPU，但仍能安全地支持实时迁移。

#### 注意：

加入异构池的 Citrix Hypervisor 服务器的 CPU 必须属于同一个供应商（即 AMD、Intel）作为池中的主机上的 CPU。但是，特定类型（系列、型号和步进编号）不需要。

Citrix Hypervisor 简化了异构池支持功能。现在，不论主机的底层 CPU 属于何种类型，都可以将其加入到现有资源池（只要 CPU 来自同一个供应商系列）。在以下情况下，每次都会对池功能集进行动态计算：

- 新主机加入池
- 池成员离开池
- 池成员在重新启动之后重新连接

池功能集发生任何变化都不会影响当前在池中运行的 VM。正在运行的 VM 继续使用启动时所应用的功能集。此功能集在启动时确定，而且在历经迁移、挂起和恢复操作后一直保持不变。如果功能有所欠缺的主机加入池，导致池的功能水平下降，正在运行的 VM 可以迁移到池中除新添加的主机以外的任何主机。在池中或跨池将 VM 移动或迁移到另一台主机时，Citrix Hypervisor 会将 VM 的功能集与目标主机的功能集相比较。如果发现两者的功能集兼容，则允许迁移 VM。如此便可在池中和跨池自由移动 VM，而不论 VM 正在使用何种 CPU 功能。如果使用 Workload Balancing 为要迁移的 VM 选择最佳目标主机，则不建议将功能集不兼容的主机作为目标主机。

### 添加共享存储

有关支持的共享存储类型的完整列表，请参阅[存储库格式](#)。本部分内容介绍了如何在现有 NFS 服务器中创建共享存储（表示为存储库）。

#### 使用 CLI 将 NFS 共享存储添加到资源池

1. 在池中的任意 Citrix Hypervisor 服务器上打开控制台。
2. 通过发出以下命令在 `server:/path` 上创建存储库：

```
1 xe sr-create content-type=user type=nfs name=label="Example SR"  
   shared=true \  
2   device-config:server=server \  
3   device-config:serverpath=path
```

`device-config:server` 为 NFS 服务器的主机名，`device-config:serverpath` 为 NFS 服务器上的路径。由于 `shared` 设置为 `true`，因此，共享存储将自动连接到池中的每个 Citrix Hypervisor 服务器。

以后加入的任何 Citrix Hypervisor 服务器也将连接到该存储。存储库的全局唯一标识符 (UUID) 将显示在屏幕上。

3. 通过运行以下命令查找池的 UUID:

```
1 xe pool-list
```

4. 使用以下命令将共享存储设置为池范围内的默认值:

```
1 xe pool-param-set uuid=pool_uuid default-SR=sr_uuid
```

由于共享存储已设置为池范围内的默认共享存储, 因此默认情况下, 将来的所有 VM 都会在共享存储上创建自己的磁盘。有关创建其他类型的共享存储的信息, 请参阅[存储库格式](#)。

## 从资源池中移除 Citrix Hypervisor 服务器

### 注意:

在从池中移除任意 Citrix Hypervisor 服务器之前, 请确保关闭该主机上正在运行的所有 VM。否则, 您会看到一条警告消息, 指示无法删除该主机。

从池中删除 (弹出) 主机时, 计算机将重新引导、重新初始化, 最终达到的状态等效于全新安装的状态。如果本地磁盘中存有重要数据, 一定不要从池中弹出 Citrix Hypervisor 服务器。

### 使用 CLI 从资源池移除主机

1. 在池中的任意主机上打开控制台。
2. 运行以下命令, 获取主机的 UUID:

```
1 xe host-list
```

3. 从池中删除所需的主机:

```
1 xe pool-eject host-uuid=host_uuid
```

Citrix Hypervisor 服务器将弹出并最终达到全新安装状态。

### 警告:

如果主机中包含存储在本地磁盘中的重要数据, 请不要从资源池删除该主机。从池中弹出主机时, 将擦除所有数据。如果要保留此数据, 请先使用 XenCenter 或 `xe vm-copy` CLI 命令将 VM 复制到池中的共享存储。

从池中弹出包含本地存储的 VM 的 Citrix Hypervisor 服务器时, 这些 VM 仍将在池数据库中显示。本地存储的 VM 还会被其他 Citrix Hypervisor 服务器看到。这些 VM 将不启动, 除非将与其关联的虚拟磁盘更改为指向能被池中的其他

Citrix Hypervisor 服务器看到的共享存储或直接删除。因此，我们建议您在加入池时将任何本地存储移动到共享存储。移动到共享存储允许弹出单个 Citrix Hypervisor 服务器（或出现物理故障），不会导致数据丢失。

**注意：**

从在带标记的 VLAN 网络中具有管理接口的池中删除主机时，计算机将重新启动，并且其管理接口将在相同的网络中可用。

### 准备 Citrix Hypervisor 服务器的池以执行维护操作

在资源池中的主机上执行维护操作之前，必须将其禁用。禁用该主机可防止在其上启动任何 VM。然后，必须将其 VM 迁移到池中的另一个 Citrix Hypervisor 服务器。可以通过使用 XenCenter 将 Citrix Hypervisor 服务器置于维护模式来实现。有关详细信息，请参阅 XenCenter 帮助。

备份同步每 24 小时进行一次。将主服务器主机置于维护模式会导致脱机 VM 的过去 24 小时的 RRD 更新丢失。

**警告：**

我们强烈建议您先重新引导所有 Citrix Hypervisor 服务器，再安装更新，然后再验证配置。某些配置更改只有在重新启动 Citrix Hypervisor 后才会生效，因此，重新启动可以发现可能导致更新失败的配置问题。

### 使用 CLI 准备池中的主机以执行维护操作

1. 运行以下命令：

```
1 xe host-disable uuid=Citrix Hypervisor_host_uuid
2 xe host-evacuate uuid=Citrix Hypervisor_host_uuid
```

此命令将禁用 Citrix Hypervisor 服务器，然后将任何正在运行的 VM 迁移到池中的其他 Citrix Hypervisor 服务器。

2. 执行所需的维护操作。
3. 维护操作完成后启用 Citrix Hypervisor 服务器：

```
1 xe host-enable
```

4. 重新启动所有已停止的 VM 并恢复所有挂起的 VM。

### 导出资源池数据

使用导出资源数据选项可为您的池生成一份资源数据报告，并可该报告导出为.xls 或.csv 文件。此报告提供有关池内各种资源（例如服务器、网络、存储、虚拟机、VDI 和 GPU）的详细信息。该功能允许管理员根据各种工作负载（例如 CPU、存储和网络）跟踪、计划和分配资源。

**注意：**

导出资源池数据适用于 Citrix Hypervisor Premium Edition 客户或通过其 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。

报告中包含的资源和各种类型的资源数据列表：

**服务器：**

- 名称
- 池主服务器
- UUID
- 地址
- CPU 使用率
- 网络（平均/最大 KB/秒）
- 已用内存
- 存储
- 运行时间
- 说明

**网络：**

- 名称
- 链接状态
- MAC
- MTU
- VLAN
- 类型
- 位置

**VDI：**

- 名称
- 类型
- UUID
- 大小
- 存储
- 说明

**存储：**

- 名称
- 类型
- UUID
- 大小
- 位置

- 说明

VM:

- 名称
- 电源状态
- 运行平台
- 地址
- MAC
- NIC
- 操作系统
- 存储
- 已用内存
- CPU 使用率
- UUID
- 运行时间
- 模板
- 说明

GPU:

- 名称
- 服务器
- PCI 总线路径
- UUID
- 电源使用
- 温度
- 已用内存
- 计算机利用率

注意:

仅当您的 Citrix Hypervisor 服务器连接了 GPU 时关于 GPU 的信息才可用。

导出资源数据

1. 在 XenCenter 的“导航”窗格中，选择基础结构，然后选择相应的池。
2. 选择池菜单，然后选择导出资源数据。
3. 浏览到您希望保存报告的位置，然后单击保存。

## 主机启动

### 远程启动主机

可以使用 Citrix Hypervisor 服务器启动功能，从 XenCenter 或使用 CLI 远程打开和关闭服务器。

要启用主机电源，主机必须具有以下电源控制解决方案之一：

- 启用了“局域网唤醒”的网卡。
- **Dell Remote Access Card (DRAC)**。要将 Citrix Hypervisor 与 DRAC 一起使用，必须安装 Dell 增补包以获取 DRAC 支持。DRAC 支持需要在带有远程访问控制器的服务器上安装 RACADM 命令行实用程序，并启用 DRAC 及其接口。RACADM 通常包含在 DRAC 管理软件中。有关详细信息，请参阅 Dell 的 DRAC 文档。
- **Hewlett-Packard Integrated Lights-Out (iLO)**。要将 Citrix Hypervisor 与 iLO 一起使用，必须在主机上启用 iLO，并将接口连接到网络。有关详细信息，请参阅 HP 的 iLO 文档。
- 基于管理 API 且使您能够通过 Citrix Hypervisor 打开和关闭电源的自定义脚本。有关详细信息，请参阅下面部分中的配置主机启动功能的自定义脚本。

使用主机开机功能时需要执行以下两项任务：

1. 请确保池中的主机支持远程控制电源。例如，主机具有局域网唤醒功能、DRAC 或 iLO 卡，或者您创建了自定义脚本。
2. 使用 CLI 或 XenCenter 启用主机启动功能。

### 使用 CLI 管理主机启动功能

可以使用 CLI 或 XenCenter 管理主机启动功能。本部分内容介绍与使用 CLI 管理主机启动功能有关的信息。

主机启动功能在主机级别（即在每台 Citrix Hypervisor 上）启用。

启用主机启动功能后，可以使用 CLI 或 XenCenter 打开主机。

### 使用 CLI 启用主机启动功能

运行命令：

```
1 xe host-set-power-on-mode host=<host uuid> \  
2     power-on-mode=("","wake-on-lan", "iLO", "DRAC", "custom") \  
3     power-on-config=key:value
```

对于 iLO 和 DRAC，如果您使用的密钥功能，密钥为 `power_on_ip` 以指定密码。有关详细信息，请参阅[机密](#)。

使用 **CLI** 远程打开主机

运行命令：

```
1 xe host-power-on host=<host uuid>
```

配置主机开启功能的自定义脚本

如果服务器的远程电源解决方案使用默认情况下不受支持的协议（例如响铃唤醒或 Intel 主动管理技术），可以创建自定义 Linux Python 脚本，以远程打开 Citrix Hypervisor 计算机。但是，您还可以为 iLO、DRAC 和局域网唤醒远程电源解决方案创建自定义脚本。

本部分内容介绍了与以下内容有关的信息：使用与 Citrix Hypervisor API 调用 `host.power_on` 相关联的键/值对配置主机启动的自定义脚本。

创建自定义脚本时，在每次要在 Citrix Hypervisor 上远程控制电源时从命令行运行该脚本。或者，可以在 XenCenter 中指定该脚本，并使用 XenCenter UI 功能与之交互。

文档“Citrix Hypervisor 管理 API”中介绍了 Citrix Hypervisor API，该文档可从[开发人员文档](#) Web 站点获取。

警告：

请勿更改 `/etc/xapi.d/plugins/` 目录中提供的默认脚本。可以在此目录中包括新脚本，但安装后不得更改该目录中包含的脚本。

键/值对

要使用主机开启功能，请配置 `host.power_on_mode` 和 `host.power_on_config` 键。有关值的信息，请参阅以下部分。

还有一个 API 调用使您能够同时设置以下字段：

```
1 void host.set_host_power_on_mode(string mode, Dictionary<string,string> config)
```

### **host.power\_on\_mode**

- 定义：包含用于指定远程电源解决方案类型（例如 Dell DRAC）的键/值对。
- 可能的值：
  - 空字符串，表示电源控制处于禁用状态
  - iLO：允许您指定 HP iLO。
  - DRAC：允许您指定 Dell DRAC。要使用 DRAC，您必须已安装 Dell 增补包。

- wake-on-lan: 允许您指定“局域网唤醒”。
  - 任何其他名称（用于指定自定义启动脚本）。此选项用于指定电源管理的自定义脚本。
- 类型：字符串

### host.power\_on\_config

- 定义：包含用于模式配置的键/值对。为 iLO 和 DRAC 提供其他信息。
- 可能的值：
  - 如果您配置“iLO”或“DRAC”作为远程电源解决方案的类型，还必须指定下面的某个键：
    - \* power\_on\_ip: 指定用来与电源控制卡通信的 IP 地址。或者，可以键入配置 iLO 或 DRAC 的网络接口的域名。
    - \* power\_on\_user: 与管理处理器相关联的 iLO 或 DRAC 用户名，您可能已更改其出厂时的默认设置。
    - \* power\_on\_password\_secret: 指定使用加密功能来保护密码的安全。
  - 要使用密钥功能来存储密码，请指定键“power\_on\_password\_secret”。有关详细信息，请参阅[机密](#)。
- 类型：Map (string,string)

### 示例脚本

此示例脚本会导入 Citrix Hypervisor API，将脚本本身定义为自定义脚本，然后将特定的参数传递给您要远程控制的主机。必须在所有自定义脚本中定义参数 `session`。

结果在脚本不成功时显示。

```
1 import XenAPI
2 def custom(session,remote_host,
3 power_on_config):
4 result="Power On Not Successful"
5 for key in power_on_config.keys():
6 result=result+' '
7 key=' '+key+' '
8 value=' '+power_on_config[key]
9 return result
```

#### 注意：

创建脚本后，使用.py 扩展名将其保存在 /etc/xapi.d/plugins 中。

## 与 Citrix Hypervisor 服务器和资源池通信

Citrix Hypervisor 使用 TLS 协议加密管理 API 流量。Citrix Hypervisor 与管理 API 客户端（或设备）之间的任何通信现在都将默认使用 TLS 1.2 协议。但是，如果管理 API 客户端或设备不使用 TLS 1.2 进行通信，则可能会使用早期的协议进行通信。

Citrix Hypervisor 使用以下密码套件：

-TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256

-TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA

-TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

-TLS\_RSA\_WITH\_RC4\_128\_SHA

-TLS\_RSA\_WITH\_RC4\_128\_MD5

-TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

Citrix Hypervisor 还允许您将主机或资源池配置为允许通过仅限 **TLS 1.2** 进行通信。此选项允许 Citrix Hypervisor 与管理 API 客户端（或设备）之间的通信使用 TLS 1.2 协议。“仅限 TLS 1.2”选项使用密码套件 `TLS_RSA_WITH_AES_128_CBC_SHA256`。

### 警告：

确保与 Citrix Hypervisor 池通信的所有管理 API 客户端和设备均与 TLS 1.2 兼容后选择仅限 **TLS 1.2** 选项。

## 对 Citrix Hypervisor 池启用 IGMP 监听

Citrix Hypervisor 向所有来宾 VM 发送多播流量，要求其处理未请求的数据包，导致主机设备上出现不必要的负载。启用 IGMP 监听将阻止本地网络中的主机接收未明确加入的多播组的流量，增强了多播的性能。IGMP 监听功能对带宽密集型 IP 多播应用程序（例如 IPTV）特别有用。

可以使用 XenCenter 或命令行接口对池启用 IGMP 监听。要使用 XenCenter 启用 IGMP 监听，请导航到池属性并选择网络选项。有关详细信息，请参阅 XenCenter 帮助。有关 xe 命令，请参阅 [pool-igmp-snooping](#)。

### 注意：

- IGMP 监听仅在网络后端使用 Open vSwitch 时可用。
- 在池中启用了此功能时，可能还有必要在其中一个物理交换机上启用 IGMP 查询器。否则，子网中的多播将回退到广播，并且可能会降低 Citrix Hypervisor 的性能。
- 在运行 IGMP v3 的池中启用了此功能时，VM 迁移或网络绑定故障转移将导致 IGMP 版本切换到 v2。
- 要在 GRE 网络中启用此功能，用户必须在 GRE 网络中的设置一个 IGMP 查询器。或者，可以将 IGMP 查询消息从物理网络转发到 GRE 网络。否则，GRE 网络中的多播流量会被阻止。

## 群集池

June 4, 2019

群集提供使用 GFS2 SR 的资源池所需的额外功能。有关 GFS2 的详细信息，请参阅[配置存储](#)。

群集是指与非群集池相比连接性和协调性更加紧密的 Citrix Hypervisor 主机的池。群集中的主机负责维护选定网络中的主机相互之间的持续通信。群集中的所有主机都能够识别群集中每个主机的状态。这一主机协调功能使群集能够控制对 GFS2 SR 的内容的访问。

### 仲裁

群集中的每个主机都必须始终至少与群集中的一半主机（包括群集本身）进行通信。此状态称为主机具有仲裁功能。

奇数池的仲裁值为群集中的总主机数加 1 的和再除以 2，即  $(n+1)/2$ 。奇数池的仲裁值为群集中的总主机数除以 2，即  $n/2$ 。

对于偶数池，正在运行的群集可以正好对半拆分。正在运行的群集决定哪部分群集进行自主防护以及哪部分群集具有仲裁功能。当偶数群集池从冷启动打开电源时， $(n/2)+1$  个主机必须可用，主机才能具有仲裁功能。主机具有仲裁功能后，该群集将变为活动状态。

如果主机没有仲裁功能，该主机将进行自主防护。

### 自主防护

如果主机检测到自身没有仲裁功能，则会在几秒钟内进行自主防护。当某个主机进行自主防护时，将立即重新启动。由于主机将执行硬关闭，因此，主机上运行的所有 VM 都将终止。在使用高可用性功能的群集池中，Citrix Hypervisor 根据其他池成员上的重新启动配置来重新启动 VM。自主防护的主机将重新启动并尝试重新加入群集。

如果群集中处于活动状态的主机数量低于仲裁值，剩余的所有主机将失去仲裁功能。

在理想情况下，群集池中包含的处于活动状态的主机数将始终高于仲裁功能所需的主机数，并且 Citrix Hypervisor 从不进行防护。要使此情形出现的可能性更高，请在设置群集池时考虑以下建议：

- 确保您具有良好的硬件冗余。
- 使用专用的绑定网络作为群集网络。确保绑定的 NIC 位于同一个 L2 段中。有关详细信息，请参阅[网络连接](#)。
- 在池与 GFS2 SR 之间配置存储多路径。有关详细信息，请参阅[存储多路径](#)。
- 在群集池上配置高可用性。在群集池中，检测信号 SR 必须是 GFS2 SR。有关详细信息，请参阅[高可用性](#)。

### 创建群集池

开始操作之前，请确保满足以下必备条件：

- 群集池中的所有 Citrix Hypervisor 服务器都必须至少具有 2 GiB 的控制域内存。
- 群集中的所有主机都必须使用群集网络的静态 IP 地址。
- 我们建议您仅在至少包含三个主机的池中使用群集，因为包含两个主机的池对自主防护整个池非常敏感。
- 如果在池中的主机之间设置了防火墙，请确保主机能够使用以下端口在群集网络中进行通信：
  - TCP: 8892、21064
  - UDP: 5404、5405

有关详细信息，请参阅[Citrix 技术使用的通信端口](#)。

- 如果要对现有池进行群集操作，请务必禁用高可用性。启用群集功能后，可以重新启用高可用性。

如果喜欢，可以使用 XenCenter 在池中设置群集功能。有关详细信息，请参阅[XenCenter 产品文档](#)。

要使用 xe CLI 创建群集池，请执行以下操作：

1. 创建绑定网络以用作群集网络。在希望作为池主服务器的 Citrix Hypervisor 服务器上，完成以下步骤：

- a) 在 Citrix Hypervisor 服务器上打开控制台。
- b) 使用以下命令命名您的资源池：

```
1 xe pool-param-set name-label="New Pool" uuid=<pool_uuid>
```

- c) 使用以下命令创建用于绑定 NIC 的网络：

```
1 xe network-create name-label=bond0
```

此时将返回新网络的 UUID。

- d) 使用以下命令查找要在绑定中使用的 PIF 的 UUID：

```
1 xe pif-list
```

- e) 在主动-主动模式、主动-被动模式或 LACP 绑定模式下创建绑定网络。根据要使用的绑定模式，完成以下操作之一：

- 要在主动-主动模式（默认模式）下配置绑定，请使用 `bond-create` 命令创建绑定。指定新创建的网络 UUID 和要绑定的各 PIF 的 UUID，以逗号分隔各参数：

```
1 xe bond-create network-uuid=<network_uuid> /  
2     pif-uuids=<pif_uuid_1>,<pif_uuid_2>,<pif_uuid_3>,<  
     pif_uuid_4>
```

绑定两个 NIC 时，请键入两个 UUID；绑定四个 NIC 时，请输入四个 UUID。在运行该命令之后，将返回该绑定的 UUID。

- 要在主动-被动或 LACP 绑定模式下配置绑定，请使用相同的语法，添加可选的 `mode` 参数并指定 `lacp` 或 `active-backup`：

```
1 xe bond-create network-uuid=<network_uuid> pif-uuids=<
   pif_uuid_1>, /
2   <pif_uuid_2>,<pif_uuid_3>,<pif_uuid_4> /
3   mode=balance-slb | active-backup | lacp
```

在池主服务器上创建绑定网络后，当您将其其他 Citrix Hypervisor 服务器加入池时，网络和绑定信息将自动复制到加入的服务器。

有关详细信息，请参阅[网络连接](#)。

2. 创建至少包含三台 Citrix Hypervisor 服务器的资源池。

在每个（非主）池成员的 Citrix Hypervisor 服务器上重复执行以下步骤：

- a) 在 Citrix Hypervisor 服务器上打开控制台。
- b) 使用以下命令将 Citrix Hypervisor 服务器加入池主服务器上的池：

```
1 xe pool-join master-address=master_address master-username=
   administrators_username master-password=password
```

`master-address` 参数的值必须设置为作为池主服务器的 Citrix Hypervisor 服务器的完全限定域名。安装池主服务器时，`password` 必须为设置的管理员密码。

有关详细信息，请参阅[主机和资源池](#)。

3. 对于属于此网络的每个 PIF，请设置 `disallow-unplug=true`。

  - a) 使用以下命令查找属于网络的 PIF 的 UUID：

```
1 xe pif-list
```

- b) 在资源池中的 Citrix Hypervisor 服务器上运行以下命令：

```
1 xe pif-param-set disallow-unplug=true uuid=<pif_uuid>
```

4. 在您的池上启用群集功能。在资源池中的 Citrix Hypervisor 服务器上运行以下命令：

```
1 xe cluster-pool-create network-uuid=<network_uuid>
```

提供您在前面步骤中创建的绑定网络的 UUID。

## 管理群集池

管理群集池时，以下做法可以降低丢失仲裁功能的池的风险。

### 确保主机彻底关闭

主机彻底关闭时，将暂时从群集中移除，直至再次将其启动。主机关闭时，不计入群集的仲裁值。主机缺乏不会导致其他主机丢失仲裁功能。

但是，如果主机被强制关闭或意外关闭，则在进入脱机状态之前不会从群集中移除。此主机将计入群集的仲裁值。关闭此主机将导致其他主机丢失仲裁功能。

### 使用维护模式

在可能会导致主机丢失仲裁功能的主机上执行操作之前，请将该主机置于维护模式。主机处于维护模式时，正在运行的 VM 会将其迁移到池中的另一台主机。此外，如果该主机属于池主服务器，该角色将传递到池中的其他主机。如果您的操作会导致处于维护模式的主机进行自主防护，则不会丢失任何 VM，或者 XenCenter 断开与池的连接。

处于维护模式的主机仍计入群集的仲裁值。

主机处于维护模式时，只能更改作为群集池的一部分的主机的 IP 地址。更改主机的 IP 地址会导致主机离开群集。成功更改 IP 地址后，主机将重新加入群集。主机重新加入群集后，可以使其退出维护模式。

### 恢复进行自主防护或处于脱机状态的主机

请务必恢复进行自主防护的主机。这些群集成员处于脱机状态时，将计入群集的仲裁数，并且会降低可访问的群集成员的数量。这种情况会增加后续主机出现故障导致群集失去仲裁功能并彻底关闭的风险。

群集中包含处于脱机状态的主机还会阻止您执行某些操作。在群集池中，池的每个成员都必须同意每次对池成员身份所做的更改，这些更改才能成功。如果群集成员不可访问，Citrix Hypervisor 将阻止执行更改群集成员身份的操作（例如添加主机或删除主机）。

### 将主机标记为死机

如果无法恢复处于脱机状态的一个或多个主机，则可以将其标记为对群集死机。将主机标记为死机会将其从群集中永久删除。将主机标记为死机后，将不再计入仲裁值。

### 限制

- 群集池最多仅支持每个池包含 16 个主机。
- 如果网络已同时用于管理和群集操作，则不能分离管理网络而不重新创建群集。
- 通过使用 XenCenter 更改群集网络的 IP 地址要求暂时禁用群集功能和 GFS2。
- 群集处于活动状态并且具有正在运行的 VM 时，请勿更改群集网络的绑定。此操作会导致群集进行防护。
- 如果您的至少涉及一个启用了群集功能的主机的群集网络中的一个 IP 地址（多个具有相同 IP 地址的主机）出现冲突，这些主机将不防护。要修复此问题，请解析 IP 地址冲突。

## 管理用户

June 4, 2019

通过定义用户、组、角色和权限，可以控制有权访问 Citrix Hypervisor 服务器和池的用户及其可执行的操作。

首次安装 Citrix Hypervisor 时，会自动将一个用户帐户添加到 Citrix Hypervisor 中。此帐户是本地超级用户 (LSU) 或 root 用户，Citrix Hypervisor 在本地对其进行身份验证。

LSU 或 root 是一个专用于系统管理的特殊用户帐户，该帐户具有所有权限。在 Citrix Hypervisor 中，LSU 是安装时的默认帐户。Citrix Hypervisor 会对 LSU 帐户进行身份验证。LSU 无需任何外部身份验证服务。如果外部身份验证服务失败，LSU 仍可登录并管理系统。LSU 始终可以通过 SSH 访问 Citrix Hypervisor 物理服务器。

您可以通过 XenCenter 的“用户”选项卡或 xe CLI 添加 Active Directory 帐户来创建更多用户。如果您的环境不使用 Active Directory，则您就只能使用 LSU 帐户。

### 注意：

创建用户时，Citrix Hypervisor 不会自动为新创建的用户帐户分配 RBAC 角色。因此，在您为这些帐户分配角色之前，它们对 Citrix Hypervisor 池没有任何访问权限。

这些权限通过角色授予，如使用 *Active Directory (AD)* 对用户进行身份验证部分中所述。

## 使用 **Active Directory (AD)** 对用户进行身份验证

如果您希望在服务器或池上具有多个用户帐户，则必须使用 Active Directory 用户帐户进行身份验证。AD 帐户允许 Citrix Hypervisor 用户使用其 Windows 域凭据登录池。

可以为特定用户配置不同的访问权限级别，方法是：启用 Active Directory 身份验证，添加用户帐户，然后为这些帐户分配角色。

Active Directory 用户可以使用 xe CLI（传递适当的 `-u` 和 `-pw` 参数），也可以使用 XenCenter 连接到该主机。身份验证基于每个资源池执行。

使用者控制用户帐户的访问权限。Citrix Hypervisor 中的一个使用者对应目录服务器上的一个实体（用户或组）。启用外部身份验证后，Citrix Hypervisor 将根据本地 root 用户的凭据来检查用于创建会话的凭据（以防目录服务器不可用），然后根据使用者列表进行检查。要允许访问，请为要向其授予访问权限的用户或组创建一个使用者条目。可以使用 XenCenter 或 xe CLI 创建使用者条目。

如果您熟悉 XenCenter，请注意，在提及 Active Directory 和用户帐户功能时，Citrix Hypervisor CLI 使用的术语略有差别：XenCenter 术语 Citrix Hypervisor CLI 术语用户使用者添加用户添加使用者

虽然 Citrix Hypervisor 是基于 Linux 的，但 Citrix Hypervisor 允许您使用 Active Directory 帐户作为 Citrix Hypervisor 用户帐户。为此，它会将 Active Directory 凭据传递到 Active Directory 域控制器。

当您将在 Active Directory 添加到 Citrix Hypervisor 后，Active Directory 用户和组即成为 Citrix Hypervisor 使用者。使用者在 XenCenter 中被称为用户。当您在 Citrix Hypervisor 中注册使用者时，系统会在您登录时使用 Active Directory 对用户/组进行身份验证。用户和组不需要通过使用域名来限定其用户名。

要限定某个用户名，必须以下层登录名格式键入该用户名，例如 `mydomain\myuser`。

**注意：**

默认情况下，如果未限定用户名，XenCenter 将尝试使用用户加入的域使用户登录 AD 身份验证服务器。LSU 帐户属例外情况，对于 LSU 帐户，XenCenter 始终首先在本地（即在 Citrix Hypervisor 上）对其进行身份验证。

外部身份验证工作流程如下：

1. 将连接到服务器时提供的凭据传递到 Active Directory 域控制器，进行身份验证。
2. 域控制器对凭据进行检查。如果凭据无效，身份验证立即失败。
3. 如果凭据有效，会对 Active Directory 控制器进行查询，以获取与凭据相关联的使用者标识符和组成员身份。
4. 如果使用者标识符与 Citrix Hypervisor 中存储的某个标识符匹配，则身份验证将成功。

您加入域后，可以为池启用 Active Directory 身份验证。但是，池加入域后，只有该域（或与该域具有信任关系的域）中的用户才能连接到该池。

**注意：**

不支持手动更新配置了 DHCP 的网络 PIF 的 DNS 配置，且手动配置可能会导致 AD 集成失败或停止工作，从而导致用户身份验证失败或停止工作。

## 配置 Active Directory 身份验证

Citrix Hypervisor 支持使用运行 Windows 2008 或更新版本的 Active Directory 服务器。

要对 Citrix Hypervisor 服务器使用 Active Directory 身份验证，必须对 Active Directory 服务器（配置为允许互操作）和 Citrix Hypervisor 服务器使用相同的 DNS 服务器。

在某些配置中，Active Directory 服务器本身可以提供 DNS。也可以使用 DHCP 为 Citrix Hypervisor 服务器提供 IP 地址和 DNS 服务器列表，来实现上述目标。或者，可以在使用手动静态配置时设置 PIF 对象的值或使用安装程序。

我们建议启用 DHCP 来分配主机名。请勿为主机分配主机名 `localhost` 或 `linux`。

**警告：**

Citrix Hypervisor 服务器名称在 Citrix Hypervisor 部署中必须唯一。

请注意以下问题：

- Citrix Hypervisor 使用其主机名在 AD 数据库中标记其 AD 条目。如果两个具有相同主机名的 Citrix Hypervisor 服务器加入同一个 AD 域，则第二个 Citrix Hypervisor 会覆盖第一个 Citrix Hypervisor 的 AD 条目。无论这些主机属于相同池还是不同池，都会覆盖。这会导致第一个 Citrix Hypervisor 上的 AD 身份验证停止工作。

如果这两个 Citrix Hypervisor 服务器加入不同的 AD 域，则可以使用相同的主机名。

- Citrix Hypervisor 服务器可以位于不同的时区，因为比较的是 UTC 时间。为确保正确的同步，您可以为 Citrix Hypervisor 池和 Active Directory 服务器使用相同的 NTP 服务器。
- 不支持混合身份验证池。不能将池中的某些服务器配置为使用 Active Directory，而另一些不使用。
- Citrix Hypervisor Active Directory 集成使用 Kerberos 协议与 Active Directory 服务器进行通信。因此，Citrix Hypervisor 不支持与未使用 Kerberos 的 Active Directory 服务器进行通信。
- 要确保使用 Active Directory 的外部身份验证成功，Citrix Hypervisor 服务器上的时钟必须与 Active Directory 服务器上的时钟保持同步。在 Citrix Hypervisor 加入 Active Directory 域时，将会检查同步，如果服务器之间偏差过大，身份验证将失败。

**警告：**

主机名必须由不超过 63 个字母数字字符组成，不得使用纯数字名称。

在启用 Active Directory 身份验证后向池添加服务器时，系统会提示您在要加入池的服务器上配置 Active Directory。系统提示您在要加入的服务器上输入凭据时，键入具有足够权限的 Active Directory 凭据，以将服务器添加到该域。

## Active Directory 集成

请确保以下防火墙端口对出站流量打开，以便 Citrix Hypervisor 能够访问域控制器。

端口	协议	使用
53	UDP/TCP	DNS
88	UDP/TCP	Kerberos 5
123	UDP	NTP
137	UDP	NetBIOS 名称服务
139	TCP	NetBIOS 会话 (SMB)
389	UDP/TCP	LDAP
445	TCP	TCP 上的 SMB
464	UDP/TCP	计算机密码更改
3268	TCP	全局目录搜索

**注意：**

- 要使用 *iptables* 在 Linux 计算机上查看防火墙规则，请运行以下命令：`iptables -nL`。
- Citrix Hypervisor 使用 PowerBroker Identity Services (PBIS) 对 AD 服务器中的 AD 用户进行身份

验证，以及加密与 AD 服务器的通信。

### Citrix Hypervisor 如何管理用于 AD 集成的计算机帐户密码？

与 Windows 客户端计算机类似，PBIS 将自动更新计算机帐户密码。PBIS 每 30 天续订一次密码，或者按 AD 服务器中的计算机帐户密码续订策略的规定进行续订。

在池上启用外部身份验证

可通过 XenCenter 或 CLI 使用以下命令配置使用 Active Directory 的外部身份验证。

```
1 xe pool-enable-external-auth auth-type=AD \  
2   service-name=full-qualified-domain \  
3   config:user=username \  
4   config:pass=password
```

指定的用户必须具有 `Add/remove computer objects or workstations` 权限，这是域管理员的默认权限。

如果您未在 Active Directory 和您的 Citrix Hypervisor 服务器使用的网络上使用 DHCP，可使用以下方法设置 DNS：

1. 设置域 DNS 后缀搜索顺序，用以解析非 FQDN 条目：

```
1 xe pif-param-set uuid=pif_uuid_in_the_dns_subnetwork \  
2   "other-config:domain=suffix1.com suffix2.com suffix3.com"
```

2. 配置 Citrix Hypervisor 服务器上使用的 DNS 服务器：

```
1 xe pif-reconfigure-ip mode=static dns=dnshost ip=ip \  
2   gateway=gateway netmask=netmask uuid=uuid
```

3. 手动设置使用（与您的 DNS 服务器处于同一网络的）PIF 的管理接口：

```
1 xe host-management-reconfigure pif-uuid=pif_in_the_dns_subnetwork
```

#### 注意：

外部身份验证是每个主机都具有的属性。但是，我们建议您基于每个池启用和禁用外部身份验证。利用每个池设置，Citrix Hypervisor 可以处理在特定主机上启用身份验证时出现的任何故障。Citrix Hypervisor 还可以根据需要进行回滚所做的任何更改，从而确保整个池的配置保持一致。使用 `host-param-list` 命令检查主机属性，并通过检查相关字段的值确定外部身份验证的状态。

可使用 XenCenter 或以下 `xe` 命令禁用 Active Directory 身份验证：

```
1 xe pool-disable-external-auth
```

## 用户身份验证

要允许用户访问您的 Citrix Hypervisor 服务器，必须为该用户或其所在的组添加一个使用者。（仍以常规方法检查过渡组成员。例如：为组 A 添加一个使用者，其中组 A 包含组 B 且 user 1 是组 B 的成员，将允许 user 1 具有访问权限）。如果您要管理 Active Directory 中的用户权限，可以创建一个组，然后在该组中添加和删除用户。或者，可以根据您的身份验证要求在 Citrix Hypervisor 中添加和删除单个用户，也可以添加和删除用户和组的组合。您可以从 XenCenter 或使用 CLI 管理使用者列表，如以下部分中所述。

对一个用户进行身份验证时，首先针对本地 root 帐户检查凭据，以支持您恢复 AD 服务器失败的系统。如果凭据（用户名和密码）不匹配，则会向 AD 服务器发出身份验证请求。如果身份验证成功，将检索用户的信息，并根据本地使用者列表验证此信息。如果身份验证失败，访问将被拒绝。如果用户或用户的过渡组成员身份中的组在使用者列表中，根据使用者列表进行的验证将成功。

### 注意：

使用 Active Directory 组为需要主机 SSH 访问权限的池管理员用户授予访问权限时，Active Directory 组中的用户数不得超过 500。

将 AD 使用者添加到 Citrix Hypervisor:

```
1 xe subject-add subject-name=entity_name
```

entity\_name 是要为其授予访问权限的用户或组的名称。虽然在无需消除歧义的情况下行为会相同，但您仍然可以包括实体的域（例如，“xend\user1”而非“user1”）。

查找用户的使用者标识符，标识符是用户或包含用户的组。删除一个组将删除该组中所有用户的访问权限，前提是这些用户未在使用者列表中指定。可使用 `subject list` 命令查找用户的使用者标识符：

```
1 xe subject-list
```

此命令将返回一个含有所有用户的列表。

要对该列表应用过滤器，例如，要查找 testad 域中用户 user1 的使用者标识符，可使用以下命令：

```
1 xe subject-list other-config:subject-name='testad\user1'
```

使用 `subject-remove` 命令删除用户，传递上一步中获得的使用者标识符：

```
1 xe subject-remove subject-uuid=subject_uuid
```

您可以结束此用户已通过身份验证的任何当前会话。有关详细信息，请参阅以下部分中使用 `xe` 终止已通过身份验证的所有会话和使用 `xe` 终止单个用户会话。如果不结束会话，权限已被撤销的用户仍可以在注销前继续访问系统。

运行以下命令可识别具有访问 Citrix Hypervisor 服务器或池权限的用户和组的列表：

```
1 xe subject-list
```

### 删除用户的访问权限

用户通过身份验证后，即可访问服务器，直到用户自己结束其会话或其他用户结束其会话为止。从使用者列表中删除某个用户或从使用者列表中的某个组中删除该用户不会自动撤销该用户具有的已通过身份验证的任何会话。用户可以使用 XenCenter 或自己已创建的其他 API 会话继续访问池。XenCenter 和 CLI 提供了用于强制结束单个会话或所有活动会话的功能。请参阅 XenCenter 帮助了解使用 XenCenter 的过程信息，或参阅以下部分了解使用 CLI 的过程。

使用 **xe** 终止已通过身份验证的所有会话

使用 **xe** 运行以下 CLI 命令可结束已通过身份验证的所有会话：

```
1 xe session-subject-identifier-logout-all
```

使用 **xe** 终止单个用户会话

1. 确定要注销其会话的使用者标识符。使用 `session-subject-identifier-list` 或 `subject-list` `xe` 命令可以找到使用者标识符。第一个命令显示具有会话的用户。第二个命令显示所有用户，但可以对其进行过滤。例如，使用 `xe subject-list other-config:subject-name=xendt\\user1` 之类的命令。可能需要所示的双反斜杠，具体取决于您的 shell。
2. 使用 `session-subject-logout` 命令，将上一步确定的使用者标识符作为参数传递，例如：

```
1 xe session-subject-identifier-logout subject-identifier=subject_id
```

### 退出 AD 域

#### 警告：

退出域（即，禁用 Active Directory 身份验证，并断开池或服务器与其域之间的连接）时，通过 Active Directory 凭据进行身份验证以连接到池或服务器的所有用户均会断开连接。

使用 XenCenter 退出 AD 域。有关详细信息，请参阅 XenCenter 帮助。也可以运行 `pool-disable-external-auth` 命令，在必要时指定池 UUID。

#### 注意：

退出域不会从 AD 数据库中删除主机对象。有关如何删除禁用的主机条目的信息，请参阅 [Microsoft 支持文章](#)。

## 基于角色的访问控制

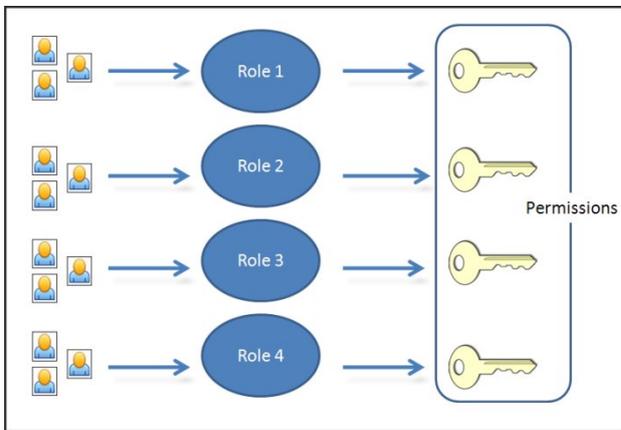
June 4, 2019

通过 Citrix Hypervisor 中的基于角色的访问控制 (RBAC) 功能，您可以分配用户、角色和权限，以控制有权访问您的 Citrix Hypervisor 的用户及其可以执行的操作。Citrix Hypervisor RBAC 系统将一个用户（或一组用户）映射到定义的角色（一组命名权限）。角色具有关联的 Citrix Hypervisor 权限，能够执行某些操作。

权限不直接分配给用户。用户通过为其分配的角色获取权限。因此，要管理单个用户的权限，只需将用户分配到适当的角色即可，这样便简化了常规操作。Citrix Hypervisor 会维护授权用户及其角色的列表。

通过 RBAC，您可以限制不同的用户组可以执行的操作，从而降低缺乏经验的用户造成事故的可能性。

RBAC 还提供“审核日志”功能以开展合规和审核工作。



RBAC 基于 Active Directory 提供身份验证服务。具体而言，Citrix Hypervisor 会保留基于 Active Directory 用户和组帐户的授权用户列表。因此，您必须将池加入域并添加 Active Directory 帐户，然后才能分配角色。

本地超级用户 (LSU) 或 root 是一个用于系统管理的特殊用户帐户，该帐户具有所有权限。在 Citrix Hypervisor 中，本地超级用户是安装时的默认帐户。LSU 通过 Citrix Hypervisor 而非外部身份验证服务进行身份验证。如果外部身份验证服务失败，LSU 仍可登录并管理系统。LSU 始终可以通过 SSH 访问 Citrix Hypervisor 物理主机。

### RBAC 流程

下面的部分介绍了实施 RBAC 并为用户或组分配角色的标准过程：

1. 加入域。有关详细信息，请参阅[启用池的外部身份验证](#)。
2. 向池中添加 Active Directory 用户或组。该用户或组将成为使用者。有关详细信息，请参阅[将使用者添加到 RBAC](#)。
3. 分配（或更改）使用者的 RBAC 角色。有关详细信息，请参阅[向使用者分配 RBAC 角色](#)。

## RBAC 角色和权限

July 10, 2019

### 角色

Citrix Hypervisor 出厂时具有以下六种预先设立的角色：

- 池管理员 - 与本地 root 用户相同。可执行所有操作。

注意：

本地超级用户（root 用户）具有“池管理员”角色。池管理员角色与本地 root 用户具有相同的权限。

- 池操作员 - 可执行除添加/删除用户及更改其角色以外的所有操作。此角色主要管理主机和池（即创建存储、构建池、管理主机等）。
- 虚拟机超级管理员（VM 超级管理员） - 创建和管理虚拟机。此角色主要预配 VM 操作员所使用的 VM。
- 虚拟机管理员（VM 管理员） - 与 VM 超级管理员类似，但不能迁移 VM 或执行快照。
- 虚拟机操作员（VM 操作员） - 与 VM 管理员类似，但不能创建/销毁 VM，可执行启动/停止生命周期操作。
- 只读角色 - 可查看资源池和性能数据。

警告：

使用 Active Directory 组授予需要主机 SSH 访问权限的池管理员用户所需的访问权限时，Active Directory 组中的用户数不得超过 500。

有关每个角色可以具有的权限汇总以及每种权限可执行的操作的详细信息，请参阅下面的部分中的 *RBAC 角色和权限定义*。

在 Citrix Hypervisor 中创建用户时，必须先向新创建的用户分配一个角色，之后才能使用该帐户。Citrix Hypervisor 不自动将角色分配给新创建的用户。因此，在您为这些帐户分配角色之前，它们对 Citrix Hypervisor 池没有任何访问权限。

1. 修改使用者到角色的映射。此操作需要分配/修改角色权限，该权限仅适用于池管理员。
2. 在 Active Directory 中修改包含组成员身份的用户角色。

### RBAC 角色和权限定义

下表汇总了每个角色适用的权限。有关每种权限可执行的操作的详细信息，请参阅权限定义。

角色权限	池管理员	池操作员	VM 超级管理			只读
			员	VM 管理员	VM 操作员	
分配/修改角色	X					
登录到（物理）服务器控制台（通过 SSH 和 XenCenter）	X					
服务器备份/还原	X					
导入/导出 OVF/OVA 包和磁盘映像	X					
设置每个插槽的核心数	X	X	X	X		
使用 Citrix Hypervisor Conversion Manager 转换虚拟机	X					
交换机端口锁定	X	X				
多路径	X	X				
注销活动的用户连接	X	X				
创建和取消警报	X	X				
取消任何用户的任务	X	X				
池管理	X	X				
实时迁移	X	X	X			
Storage 实时迁移	X	X	X			
VM 高级操作	X	X	X			

角色权限	VM 超级管理					
	池管理员	池操作员	员	VM 管理员	VM 操作员	只读
VM 创建/销毁操作	X	X	X	X		
VM 更改 CD 介质	X	X	X	X	X	
VM 更改电源状态	X	X	X	X	X	
查看 VM 控制台	X	X	X	X	X	
XenCenter 视图管理操作	X	X	X	X	X	
取消自己的任务	X	X	X	X	X	X
阅读审核日志	X	X	X	X	X	X
连接到池并阅读所有池元数据	X	X	X	X	X	X
配置虚拟 GPU	X	X				
查看虚拟 GPU 配置	X	X	X	X	X	X
访问配置驱动器 (仅限 CoreOS VM)	X					
容器管理	X					
计划快照 (在现有快照计划中添加/删除 VM)	X	X	X			
计划快照 (添加/修改/删除快照计划)	X	X				
配置运行状况检查	X	X				

角色权限	VM 超级管理					
	池管理员	池操作员	员	VM 管理员	VM 操作员	只读
查看运行状况 检查结果和 置	X	X	X	X	X	X
配置更改块跟 踪	X	X	X	X		
列出更改块	X	X	X	X	X	
配置 PVS 加 速器	X	X				
查看 PVS 加 速器配置	X	X	X	X	X	X

## 权限的定义

### 分配/修改角色：

- 添加/删除用户
- 添加/删除用户的角色
- 启用和禁用 Active Directory 集成（加入域）

此权限允许用户向自身授予任何权限或执行任何任务。

警告：此角色允许用户禁用 Active Directory 集成以及从 Active Directory 添加的所有使用者。

### 登录到服务器控制台：

- 通过 SSH 访问服务器控制台
- 通过 XenCenter 访问服务器控制台

警告：具备对 root shell 的访问权限之后，被分派人可以随意重新配置整个系统（包括 RBAC）。

### 服务器备份/还原 VM 创建/销毁操作：

- 备份和还原服务器
- 备份和还原池元数据

还原备份的能力使被分派人能够还原 RBAC 配置更改。

### 导入/导出 OVF/OVA 包和磁盘映像：

- 导入 OVF 和 OVA 包
- 导入磁盘映像
- 将 VM 导出为 OVF/OVA 包

设置每个插槽的核心数：

- 为 VM 的虚拟 CPU 设置每个插槽的核心数

此权限允许用户为 VM 的虚拟 CPU 指定拓扑。

使用 **Citrix Hypervisor Conversion Manager** 转换 VM：

- 将 VMware VM 转换为 Citrix Hypervisor VM

此权限允许用户将工作负载从 VMware 转换为 Citrix Hypervisor，方法是将 VMware VM 的批处理作业复制到 Citrix Hypervisor 环境。

交换机端口锁定：

- 控制网络中的流量

此权限允许用户默认阻止网络中的所有流量，或定义允许 VM 从中发送流量的特定 IP 地址。

多路径：

- 启用多路径
- 禁用多路径

注销活动的用户连接：

- 断开已登录用户的连接的能力

创建/消除警报：

- 将 XenCenter 配置为当资源使用情况超过特定阈值时生成警报
- 从“警报”视图中删除警报

警告：具有此权限的用户可以取消整个池的警报。

注意：查看警报的能力属于连接到池并读取所有池元数据权限的一部分。

取消任何用户的任务：

- 取消任何用户的正在运行的任务

此权限允许用户请求 Citrix Hypervisor 取消任何用户启动的正在执行的任务。

池管理：

- 设置池属性（命名、默认 SR）
- 创建群集池
- 启用、禁用和配置高可用性
- 设置每个 VM 的高可用性功能重新启动优先级
- 配置 DR、执行 DR 故障转移、故障恢复以及测试故障转移操作
- 启用、禁用和配置 Workload Balancing (WLB)
- 在池中添加和删除服务器
- 紧急转换到主服务器

- 紧急主服务器地址
- 紧急恢复从属服务器
- 指定新的主服务器
- 管理池和服务器证书
- 修补
- 设置服务器属性
- 配置服务器日志记录
- 启用和禁用服务器
- 关闭、重新启动和打开服务器
- 重新启动 Toolstack
- 系统状态报告
- 应用许可证
- 由于使用维护模式或高可用性功能，请将服务器上的所有其他 VM 实时迁移到另一台服务器
- 配置服务器管理接口和辅助接口
- 禁用服务器管理
- 删除故障转储
- 添加、编辑和删除网络
- 添加、编辑和删除 PBD/PIF/VLAN/绑定/SR
- 添加、删除和检索机密信息

此权限包括维护池需执行的所有操作。

注意：如果管理接口无法使用，则除本地 root 登录外，其他登录均无法通过身份验证。

实时迁移：

- 当 VM 位于两个主机共享的存储中时，将 VM 从一个主机迁移到另一个主机

存储实时迁移：

- 当 VM 不位于两个主机之间共享的存储中时，从一个主机迁移到另一个主机
- 将虚拟磁盘 (VDI) 从一个 SR 迁移到另一个 SR

**VM 高级操作：**

- 调整 VM 内存（通过动态内存控制）
- 创建包含内存数据的 VM 快照、生成 VM 快照及回滚 VM
- 迁移 VM
- 启动 VM，包括指定物理服务器
- 恢复 VM

此权限向被授权人提供了足够的权限，使其能够在对所选的 Citrix Hypervisor 服务器不满意时在其他服务器上启动 VM。

**VM 创建/销毁操作：**

- 安装或删除

- 克隆/复制 VM
- 添加、删除和配置虚拟磁盘/CD 设备
- 添加、删除和配置虚拟网络设备
- 导入/导出 XVA 文件
- VM 配置更改
- 服务器备份/还原

注意：

VM 管理员角色可以仅将 XVA 文件导入到具有共享 SR 的池中。VM 管理员角色的权限不足，无法将 XVA 文件导入到主机中或者导入到没有共享存储的池中。

#### **VM 更改 CD 介质：**

- 弹出当前的 CD
- 插入新 CD

导入/导出 OVF/OVA 包；导入磁盘映像

#### **VM 更改电源状态：**

- 启动 VM（自动放置）
- 关闭 VM
- 重新启动 VM
- 挂起 VM
- 恢复 VM（自动放置）

此权限不包括启动、恢复和迁移，这三种权限属于 VM 高级操作权限。

#### **查看 VM 控制台：**

- 查看 VM 控制台以及与其交互

此权限不允许用户查看服务器控制台。

#### **XenCenter 视图管理操作：**

- 创建和修改全局 XenCenter 文件夹
- 创建和修改全局 XenCenter 自定义字段
- 创建和修改全局 XenCenter 搜索

文件夹、自定义字段和搜索在访问池的所有用户间共享

#### **取消自己的任务：**

- 允许用户取消自己的任务

#### **读取审核日志：**

- 下载 Citrix Hypervisor 审核日志

#### **连接到池并读取所有池元数据：**

- 登录到池
- 查看池元数据
- 查看历史性能数据
- 查看登录的用户
- 查看用户和角色
- 查看消息
- 注册参加和接收事件

配置虚拟 **GPU**：

- 指定池范围内的放置策略
- 将虚拟 GPU 分配给 VM
- 从 VM 中删除虚拟 GPU
- 修改允许的虚拟 GPU 类型
- 创建、销毁或分配 GPU 组

查看虚拟 **GPU** 配置：

- 查看 GPU、GPU 放置策略和虚拟 GPU 分配

访问配置驱动器（仅限 **CoreOS VM**）：

- 访问 VM 的配置驱动程序
- 修改云配置参数

容器管理：

- 启动
- 停止
- 暂停
- 恢复
- 访问与容器有关的信息

计划快照：

- 向现有快照计划中添加 VM
- 从现有快照计划中删除 VM
- 添加快照计划
- 修改快照计划
- 删除快照计划

配置运行状况检查：

- 启用运行状况检查
- 禁用运行状况检查
- 更新运行状况检查设置
- 手动上载服务器状态报告

查看运行状况检查结果和设置：

- 查看运行状况检查上载结果
- 查看运行状况检查注册设置

配置更改块跟踪：

- 启用更改块跟踪
- 禁用更改块跟踪
- 销毁与快照关联的数据并保留元数据
- 获取 VDI 的 NBD 连接信息

只能对获得许可的 Citrix Hypervisor Premium Edition 实例启用更改块跟踪。

列出更改块：

- 比较两个 VDI 快照并列这两个快照之间已更改的块

配置 **PVS** 加速器：

- 启用 PVS 加速器
- 禁用 PVS 加速器
- 更新（PVS 加速器）缓存配置
- 添加或删除（PVS 加速器）缓存配置

查看 **PVS** 加速器配置：

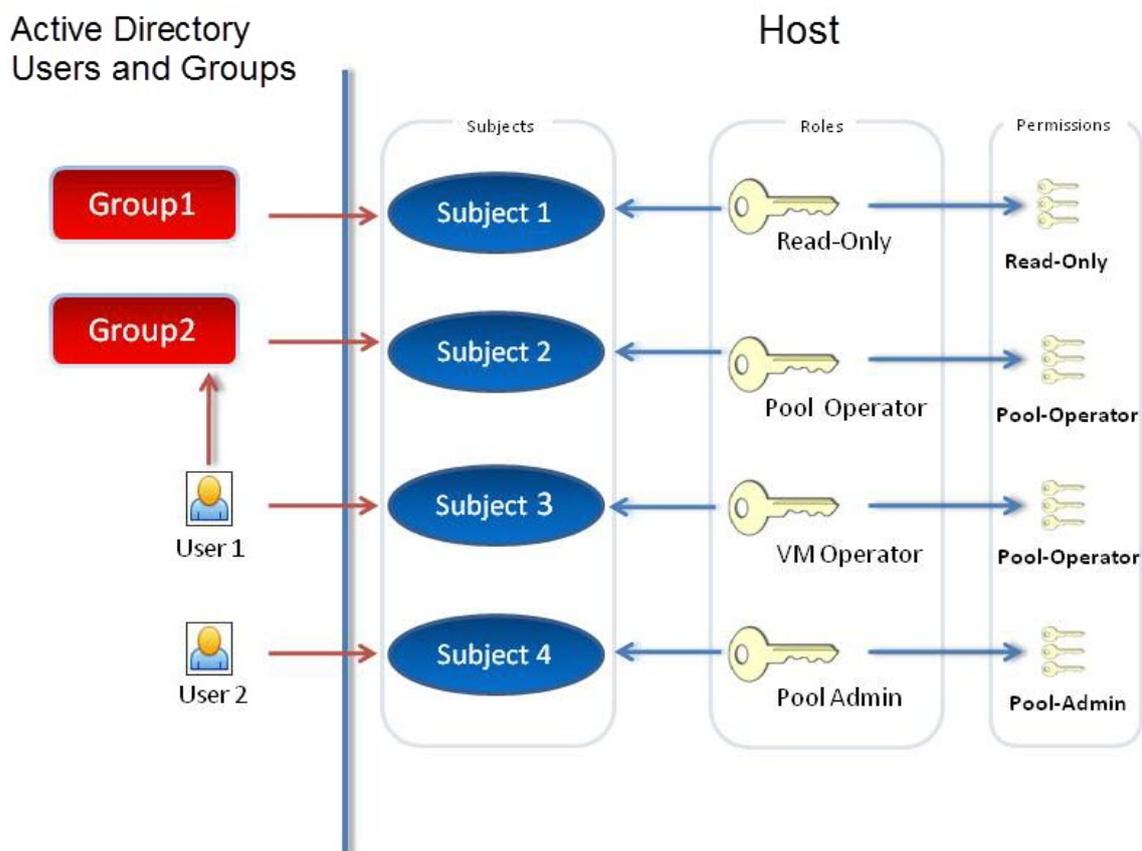
- 查看 PVS 加速器的状态

注意：

有时，具有只读权限的用户无法将资源移动到 XenCenter 中的文件夹，即使在接收到提升提示并提供了更具特权的用户的凭据之后也是如此。在这种情况下，以更具特权的用户身份登录到 XenCenter 并重试该操作。

### **Citrix Hypervisor** 如何计算会话的角色？

1. 使用者通过 Active Directory 服务器进行身份验证，以确定该使用者还可能属于哪些包含组。
2. Citrix Hypervisor 接下来会确定已将哪些角色同时分配给该使用者及其包含组。
3. 由于使用者可以是多个 Active Directory 组的成员，因此，使用者会继承关联角色的所有权限。



## 结合使用 RBAC 和 CLI

June 4, 2019

### RBAC xe CLI 命令

可使用以下命令对角色和使用者进行相应操作。

列出所有可用的已定义角色

运行命令: `xe role-list`

此命令返回当前已定义角色的列表, 例如:

```
1      uuid( RO ): 0165f154-ba3e-034e-6b27-5d271af109ba
```

```
2     name ( R0): pool-admin
3     description ( R0): The Pool Administrator role has full access to
4         all
5         features and settings, including accessing Dom0 and managing
6         subjects,
7         roles and external authentication
8
9     uuid ( R0): b9ce9791-0604-50cd-0649-09b3284c7dfd
10    name ( R0): pool-operator
11    description ( R0): The Pool Operator role manages host- and pool-
12        wide resources,
13        including setting up storage, creating resource pools and managing
14        patches, and
15        high availability (HA).
16
17    uuid( R0): 7955168d-7bec-10ed-105f-c6a7e6e63249
18    name ( R0): vm-power-admin
19    description ( R0): The VM Power Administrator role has full access
20        to VM and
21        template management and can choose where to start VMs and use the
22        dynamic memory
23        control and VM snapshot features
24
25    uuid ( R0): aaa00ab5-7340-bfbc-0d1b-7cf342639a6e
26    name ( R0): vm-admin
27    description ( R0): The VM Administrator role can manage VMs and
28        templates
29
30    uuid ( R0): fb8d4ff9-310c-a959-0613-54101535d3d5
31    name ( R0): vm-operator
32    description ( R0): The VM Operator role can use VMs and interact
33        with VM consoles
34
35    uuid ( R0): 7233b8e3-eacb-d7da-2c95-f2e581cdbf4e
36    name ( R0): read-only
37    description ( R0): The Read-Only role can log in with basic read-
38        only access
```

**注意：**

此角色列表固定不变。您无法添加、删除或修改角色。

显示当前使用者的列表

运行以下命令：

```
1 xe subject-list
```

此命令将返回 Citrix Hypervisor 用户、其 UUID 及其相关联的角色的列表：

```
1  uuid ( RO): bb6dd239-1fa9-a06b-a497-3be28b8dca44
2  subject-identifier ( RO): S
   -1-5-21-1539997073-1618981536-2562117463-2244
3  other-config (MRO): subject-name: example01\user_vm_admin; subject-
   upn: \
4  user_vm_admin@XENDT.NET; subject-uid: 1823475908; subject-gid:
   1823474177; \
5  subject-sid: S-1-5-21-1539997073-1618981536-2562117463-2244;
   subject-gecos: \
6  user_vm_admin; subject-displayname: user_vm_admin; subject-is-
   group: false; \
7  subject-account-disabled: false; subject-account-expired: false;
   \
8  subject-account-locked: false;subject-password-expired: false
9  roles (SRO): vm-admin
10
11  uuid ( RO): 4fe89a50-6a1a-d9dd-afb9-b554cd00c01a
12  subject-identifier ( RO): S
   -1-5-21-1539997073-1618981536-2562117463-2245
13  other-config (MRO): subject-name: example02\user_vm_op; subject-upn
   : \
14  user_vm_op@XENDT.NET; subject-uid: 1823475909; subject-gid:
   1823474177; \
15  subject-sid: S-1-5-21-1539997073-1618981536-2562117463-2245; \
16  subject-gecos: user_vm_op; subject-displayname: user_vm_op; \
17  subject-is-group: false; subject-account-disabled: false; \
18  subject-account-expired: false; subject-account-locked: \
19  false; subject-password-expired: false
20  roles (SRO): vm-operator
21
22  uuid ( RO): 8a63fbf0-9ef4-4fef-b4a5-b42984c27267
23  subject-identifier ( RO): S
   -1-5-21-1539997073-1618981536-2562117463-2242
24  other-config (MRO): subject-name: example03\user_pool_op; \
25  subject-upn: user_pool_op@XENDT.NET; subject-uid: 1823475906; \
26  subject-gid: 1823474177; subject-s id:
27  S-1-5-21-1539997073-1618981536-2562117463-2242; \
```

```
28     subject-gecos: user_pool_op; subject-displayname: user_pool_op; \  
29     subject-is-group: false; subject-account-disabled: false; \  
30     subject-account-expired: false; subject-account-locked: \  
31     false; subject-password-expired: false \  
32     roles (SR0): pool-operator
```

### 将使用者添加到 **RBAC**

为使现有 AD 用户能够使用 RBAC，请在 Citrix Hypervisor 中直接为 AD 用户或为包含组创建一个使用者实例：

运行以下命令以添加新的使用者实例：

```
1 xe subject-add subject-name=AD user/group
```

### 向使用者分配 **RBAC** 角色

添加使用者之后，可以为其分配 RBAC 角色。可以通过角色的 UUID 或名称引用该角色：

运行命令：

```
1 xe subject-role-add uuid=subject uuid role-uuid=role_uuid
```

或

```
1 xe subject-role-add uuid=subject uuid role-name=role_name
```

例如，以下命令会将 UUID 为 b9b3d03b-3d10-79d3-8ed7-a782c5ea13b4 的使用者添加到池管理员角色：

```
1 xe subject-role-add uuid=b9b3d03b-3d10-79d3-8ed7-a782c5ea13b4 role-name  
=pool-admin
```

### 更改使用者的 **RBAC** 角色

要更改用户的角色，需要将用户从现有角色中删除，然后再将其添加到新角色：

运行以下命令：

```
1 xe subject-role-remove uuid=subject_uuid role-name=role_name_to_remove  
2 xe subject-role-add uuid=subject_uuid role-name=role_name_to_add
```

用户必须注销并重新登录以确保新角色生效。此操作需要适用于池管理员或池操作员的“注销活动用户连接”权限。

**警告:**

添加或删除池管理员使用者时，可能需要几秒钟时间来允许池中的所有主机接受与此使用者相关联的 SSH 会话。

## 审核

RBAC 审核日志将记录已登录的用户执行的所有操作。

- 该消息将记录与调用该操作的会话相关联的使用者 ID 和用户名。
- 如果使用者调用某个未获授权的操作，则将记录该操作。
- 还会记录任何成功的操作。如果操作失败，则会记录错误代码。

## 审核日志 **xe CLI** 命令

以下命令将池中 RBAC 审核文件的所有可用记录下载到某个文件中。如果可选参数 “since” 存在，该命令将仅下载自该特定时间点开始的记录。

```
1 xe audit-log-get [since=timestamp] filename=output filename
```

### 获取池中的所有审核记录

运行以下命令：

```
1 xe audit-log-get filename=/tmp/auditlog-pool-actions.out
```

### 获取自精确到毫秒的时间戳开始的池审核记录

运行以下命令：

```
1 xe audit-log-get since=2009-09-24T17:56:20.530Z \  
2 filename=/tmp/auditlog-pool-actions.out
```

### 获取自精确到分钟的时间戳开始的池审核记录

运行以下命令：

```
1 xe audit-log-get since=2009-09-24T17:56Z \  
2 filename=/tmp/auditlog-pool-actions.out
```

## 网络连接

June 4, 2019

本部分内容将概括介绍 Citrix Hypervisor 的网络连接，包括网络、VLAN 和 NIC 绑定。此外，还将讨论如何管理网络连接配置以及进行故障排除。

**重要：**

vSwitch 是 Citrix Hypervisor 的默认网络堆栈。请按照 vSwitch 网络中的说明来配置 Linux 网络堆栈。

如果您已经熟悉了 Citrix Hypervisor 网络连接的概念，可以提前跳至[管理网络连接](#)以获取与以下各部分内容有关的信息：

- 为独立 Citrix Hypervisor 服务器创建网络
- 跨多个 Citrix Hypervisor 服务器创建专用网络
- 为资源池中配置的 Citrix Hypervisor 服务器创建网络
- 为 Citrix Hypervisor 服务器（独立主机或资源池的成员）创建 VLAN
- 为独立 Citrix Hypervisor 服务器创建绑定
- 为资源池中配置的 Citrix Hypervisor 服务器创建绑定

**注意：**

术语“管理接口”用来表示用于传输管理流量并且启用了 IP 的 NIC。术语“辅助接口”用来表示为存储流量配置的启用了 IP 的 NIC。

## 网络连接支持

对于每个主机，Citrix Hypervisor 最多支持 16 个物理网络接口（或最多支持 4 个绑定的网络接口）；对于每个 VM，最多支持 7 个虚拟网络接口。

**注意：**

Citrix Hypervisor 使用 xe 命令行接口 (CLI) 提供 NIC 的自动配置和管理。请勿直接编辑主机的网络连接配置文件。

## vSwitch 网络

与控制器设备结合使用时，vSwitch 网络支持开放流并提供额外的功能，例如访问控制列表 (ACL)。Citrix Hypervisor vSwitch 的控制器设备称为 vSwitch Controller。vSwitch Controller 允许通过 GUI 监视您的网络。vSwitch Controller:

- 支持细化的安全策略，以控制传入和传出 VM 的通信流。

- 详细展示虚拟网络环境中所发送的所有流量的行为和性能。

VSwitch 大大简化了虚拟化网络环境中的 IT 管理过程。即使 VM 从资源池中的一个物理主机迁移到另一个，所有 VM 配置和统计信息仍会绑定到该 VM。有关详细信息，请参阅 [vSwitch](#) 和 [Controller](#)。

要确定配置的网络连接堆栈，请运行以下命令：

```
1 xe host-list params=software-version
```

在命令输出中，查找 `network_backend`。将 vSwitch 配置为网络堆栈时，输出将如下所示：

```
1 network_backend: openvswitch
```

将 Linux 桥接配置为网络堆栈时，输出将如下所示：

```
1 network_backend: bridge
```

要还原到 Linux 网络堆栈，请运行以下命令：

```
1 xe-switch-network-backend bridge
```

在运行此命令之后重新启动您的主机。

**警告：**

Linux 网络堆栈未启用开放流，并且不支持跨服务器专用网络。Citrix Hypervisor vSwitch Controller 不管理 Linux 网络堆栈。

## Citrix Hypervisor 网络连接概述

本节介绍 Citrix Hypervisor 环境中网络连接的一般概念。

在安装期间，Citrix Hypervisor 将为每个物理 NIC 创建一个网络。向池中添加服务器时，默认网络将合并。这是为了确保设备名称相同的所有物理 NIC 都连接到同一个网络。

通常情况下，您将添加一个网络以创建内部网络，使用现有 NIC 设置新 VLAN，或者创建 NIC 绑定。

在 Citrix Hypervisor 中您可以配置四种不同类型的网络：

- 外部网络与物理网络接口相关联。外部网络在虚拟机与连接到网络的物理网络接口之间提供了一个桥梁。外部网络使虚拟机能够连接到可通过服务器的物理 NIC 提供的资源。
- 绑定网络，可在两个或多个 NIC 之间创建一个绑定，以在虚拟机与网络之间创建一个高性能通道。
- 单服务器专用网络与物理网络接口无关联。单服务器专用网络可用于提供指定主机上的虚拟机之间的连接，而与外界无连接。
- 跨服务器专用网络，对单服务器专用网络这一概念进行了扩展，允许不同主机上的 VM 使用 vSwitch 相互通信。

### 注意：

某些网络选项在用于独立 Citrix Hypervisor 服务器与用于资源池时具有不同的行为。本部分内容首先介绍同时适用于独立主机和池的一般信息，之后介绍分别适用于这两种类型的特定信息。

## 网络对象

本部分内容使用三种类型的服务器端软件对象来表示网络连接实体。这些对象包括：

- *PIF*，表示主机上的一个物理 NIC。PIF 对象具有名称和说明、UUID、所表示的 NIC 的参数，以及连接到的网络和服务器。
- *VIF*，表示虚拟机上的一个虚拟 NIC。VIF 对象具有名称和说明、UUID 和连接到的网络和 VM。
- 网络，即主机上的虚拟以太网交换机。网络对象具有名称和说明、UUID 以及连接到的 VIF 和 PIF 的集合。

XenCenter 和 xe CLI 都允许您配置网络连接选项。可以控制用于管理操作的 NIC，以及创建高级网络连接功能，例如 VLAN 和 NIC 绑定。

## 网络

每个 Citrix Hypervisor 服务器都有一个或多个网络，即虚拟以太网交换机。不与 PIF 相关联的网络被视为内部网络。内部网络仅可用于提供给定 Citrix Hypervisor 服务器上的 VM 之间的连接，不与外部连接。与 PIF 相关联的网络被视为外部网络。外部网络在连接到网络的 PIF 与 VIF 之间提供了一个桥梁，从而能够通过 PIF 的 NIC 连接到资源。

## VLAN

按照 IEEE 802.1Q 标准的有关定义，VLAN 允许单个物理网络支持多个逻辑网络。Citrix Hypervisor 服务器通过多种方式支持 VLAN。

### 注意：

所有受支持的 VLAN 配置均可应用于池、独立主机、绑定配置和非绑定配置。

## 在虚拟机中使用 VLAN

配置为 802.1Q VLAN 中继端口的交换机端口可以与 Citrix Hypervisor VLAN 功能结合使用，将来宾虚拟网络接口 (VIF) 连接到特定的 VLAN。在这种情况下，Citrix Hypervisor 服务器将为来宾执行 VLAN 标记/去标记功能，而来宾不会觉察到任何 VLAN 配置。

Citrix Hypervisor VLAN 由另外的代表与指定 VLAN 标记相对应的 VLAN 接口的 PIF 对象表示。可以将 Citrix Hypervisor 网络连接到代表物理 NIC 的 PIF，以查看该 NIC 上的所有流量。或者，也可以将网络连接到代表 VLAN 的 PIF，以仅查看具有指定 VLAN 标记的流量。还可以通过将网络连接到 VLAN 0 来连接网络，以便只能看到本机 VLAN 流量。

有关如何为 Citrix Hypervisor 服务器（独立服务器或资源池中的服务器）创建 VLAN 的步骤，请参阅[创建 VLAN](#)。

### 结合使用 VLAN 和管理接口

可以使用配置为中继端口或访问模式端口的交换机端口在 VLAN 中配置管理端口。使用 XenCenter 或 xe CLI 设置 VLAN 并将其设为管理接口。有关详细信息，请参阅[管理接口](#)。

### 结合使用 VLAN 和管理接口

可以使用配置为中继端口或访问模式端口的交换机端口在 VLAN 中配置管理端口。使用 XenCenter 或 xe CLI 设置 VLAN 并将其设为管理接口。有关详细信息，请参阅[管理接口](#)。

### 使用具有专用存储 NIC 的 VLAN

可以将专用存储 NIC 配置为使用本机 VLAN 或访问模式端口，如上一部分内容中的管理接口部分中所述。专用存储 NIC 又称为启用了 IP 的 NIC 或二级接口。可以将专用存储 NIC 配置为使用中继端口和 Citrix Hypervisor VLAN，如上一部分内容中的虚拟机部分中所述。有关详细信息，请参阅[配置专用存储 NIC](#)。

### 将管理接口和来宾 VLAN 组合到单一主机 NIC 上

一个交换机端口可使用中继端口和本地 VLAN 来配置，这就使得一个主机 NIC 可用作管理接口（在本机 VLAN 上），并可用于将来 VIF 连接到特定的 VLAN ID。

### 巨型帧

可以使用巨型帧来优化存储流量的性能。巨型帧是指包含超过 1500 字节有效负载的以太网帧。巨型帧通常用于实现更高的吞吐量，降低系统总线内存上的负载，并减少 CPU 开销。

#### 注意：

仅在 vSwitch 用作池中所有主机上的网络堆栈时，Citrix Hypervisor 才支持巨型帧。

### 使用巨型帧的要求

使用巨型帧时，客户必须注意以下事项：

- 在池级别配置巨型帧
- vSwitch 必须配置为池中所有主机上的网络后端
- 子网上的每个设备必须配置为使用巨型帧
- 在专用存储网络上启用巨型帧（推荐）
- 在管理网络上启用巨型帧的配置不受支持

- 不支持在 VM 上使用巨型帧

要使用巨型帧，请将最大传输单位 (MTU) 设置为介于 1500 到 9216 之间的值。可以使用 XenCenter 或 xe CLI 来设置 MTU。

## NIC 绑定

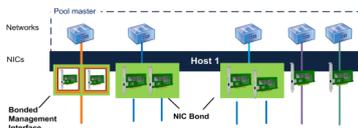
NIC 绑定（有时也称为“NIC 成组”）可以让管理员将两个或更多 NIC 配置在一起，从而提高 Citrix Hypervisor 服务器的恢复能力和带宽。NIC 绑定在逻辑上用作一个网卡，所有绑定的 NIC 共享 MAC 地址。

如果绑定中的一个 NIC 失败，则主机的网络流量会自动通过另一个 NIC 进行重定向。Citrix Hypervisor 最多支持八个绑定网络。

Citrix Hypervisor 支持主动-主动、主动-被动和 LACP 绑定模式。受支持 NIC 数量和受支持绑定模式因网络堆栈而异：

- LACP 绑定仅适用于 vSwitch，而主动-主动和主动-被动适用于 vSwitch 和 Linux 桥接。
- 当 vSwitch 为网络堆栈时，您可以将两个、三个或四个 NIC 绑定在一起。
- 当 Linux 桥接为网络堆栈时，您只能绑定两个 NIC。

在下图中，管理接口位于绑定的 NIC 对上。Citrix Hypervisor 使用此绑定发送管理流量。



所有绑定模式都支持故障转移。但是，并非所有模式都允许所有链路对所有流量类型保持活动状态。Citrix Hypervisor 支持将以下类型的 NIC 绑定在一起：

- **NIC（非管理）**。可以绑定由 Citrix Hypervisor 专用于 VM 流量的 NIC。绑定这些 NIC 不仅提供恢复能力，而且还会在 NIC 之间平衡来自多个 VM 的流量。
- **管理接口**。可以将管理接口绑定到另一个 NIC，以便该 NIC 为管理流量提供故障转移。虽然配置 LACP 链路聚合绑定可以为管理流量提供负载平衡，但主动-主动 NIC 绑定不提供这一功能。可以在绑定 NIC 上创建 VLAN，并且可以将主机管理接口分配给该 VLAN。
- **辅助接口**。您可以绑定已配置为辅助接口的 NIC（例如，用于存储）。但是，对于大多数 iSCSI 软件发起程序存储，我们建议配置多路径而非 NIC 绑定，如“设计 Citrix Hypervisor 网络配置”中所述。

在本部分内容中，术语“基于 IP 的存储流量”是 iSCSI 和 NFS 流量的统称。

如果 VIF 已在使用将绑定在一起的其中一个接口，则可以创建一个绑定，此时 VM 流量将自动迁移到新的绑定接口。

在 Citrix Hypervisor 中，NIC 绑定由额外的 PIF 表示。Citrix Hypervisor NIC 绑定完全包含基础物理设备 (PIF)。

注意：

- 不支持创建仅包含一个 NIC 的绑定。
- 在传输 FCoE 流量的 NIC 上不支持 NIC 绑定。

#### 关于 IP 寻址的要点

绑定的 NIC 可以有一个或没有 IP 地址，如下所示：

- 管理和存储网络。
  - 如果您绑定管理接口或辅助接口，则系统会为绑定分配一个 IP 地址。即，每个 NIC 没有自己的 IP 地址。Citrix Hypervisor 将这两个 NIC 视为一个逻辑连接。
  - 将绑定用于非 VM 流量（例如，用来连接到共享网络存储或 XenCenter 进行管理）时，请为该绑定配置一个 IP 地址。但是，如果您已将 IP 地址分配给绑定中的某个 NIC（即，已创建管理接口或辅助接口），系统会自动将此 IP 地址分配给整个绑定。
  - 如果将管理接口或辅助接口绑定到无 IP 地址的 NIC，此绑定将使用相应接口的 IP 地址。
  - 如果绑定了带标记的 VLAN 管理接口和辅助接口，则将在该绑定 NIC 上创建管理 VLAN。
- **VM 网络。**当绑定的 NIC 用于 VM 流量时，不需要为该绑定配置 IP 地址。这是因为绑定在 OSI 的第 2 层（即数据链路层）上运行，而此层上不使用 IP 地址。虚拟机的 IP 地址与 VIF 相关联。

#### 绑定类型

Citrix Hypervisor 提供三种不同类型的绑定，而且它们都可以使用 CLI 或 XenCenter 配置：

- 主动-主动模式，将在两个绑定的 NIC 之间平衡 VM 流量。请参阅主动-主动绑定。
- 主动-被动模式，只有一个 NIC 主动传输流量。请参阅主动-被动绑定。
- LACP 链路聚合（在交换机和服务器之间协商主动和备用 NIC）。请参阅 LACP 链路聚合控制协议绑定。

#### 注意：

绑定设置为最高延迟 31000 毫秒，最低延迟 200 毫秒。最高延迟的时间看似有点长，但这是有意如此，因为某些交换机要启用端口需要花费一些时间。如果未设置延迟，链路在失败后恢复时，绑定会在交换机准备好传递流量之前重新平衡其上的流量。要将两个连接都移动到另外一台不同的交换机，请移动一个连接，等待 31 秒以便其再次使用，然后再移动另一连接。有关更改延迟的信息，请参阅更改绑定的最高延迟。

#### 绑定状态

Citrix Hypervisor 在每个主机的事件日志中提供绑定状态。如果绑定中的一个或多个链路发生故障或恢复，这一情况会记录在事件日志中。同样，可以使用下例中显示的 `links-up` 参数来查询绑定的链路状态：

```
1 xe bond-param-get uuid=bond_uuid param-name=links-up
```

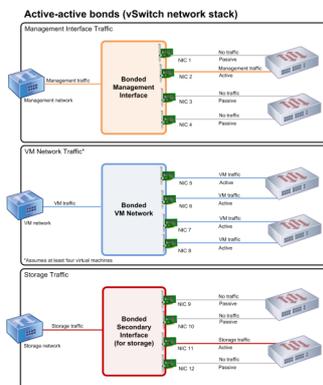
Citrix Hypervisor 每隔 5 秒左右检查一次绑定中链路的状态。因此，如果绑定中的多个链路在五秒期限内出现故障，则将仅在下次检查状态时将此故障记录到日志中。

绑定事件日志在 XenCenter 的“日志”选项卡中显示。对于不运行 XenCenter 的用户，事件日志也会在每个主机的 `/var/log/xen-source.log` 中显示。

### 主动-主动绑定

主动-主动是适用于来宾流量的主动/主动配置，在此配置中，两个 NIC 可以同时路由 VM 流量。当绑定用于管理流量时，绑定中只有一个 NIC 可以路由流量，而另一个 NIC 将保持未使用状态并提供故障转移支持。启用 Linux 桥接或 vSwitch 网络堆栈时，主动-主动模式为默认绑定模式。

将主动-主动绑定与 Linux 桥接一起使用时，只能绑定两个 NIC。将 vSwitch 用作网络堆栈时，可以在主动-主动模式下绑定两个、三个或四个 NIC。但是，在主动-主动模式下，绑定三个或四个 NIC 仅对 VM 流量有利，如下图所示。



当多个 MAC 地址与绑定关联时，Citrix Hypervisor 只能在两个或更多 NIC 上传输流量。Citrix Hypervisor 可以使用 VIF 中的虚拟 MAC 地址跨多个链路发送流量。特别说明：

- **VM 流量。**假设您对仅传输 VM（来宾系统）流量的 NIC 启用绑定，则所有链路都处于活动状态，因而 NIC 绑定可以在各 NIC 之间平衡 VM 流量。单个 VIF 的流量从不在各 NIC 之间拆分。
- **管理或存储流量。**绑定中只有一个链路 (NIC) 处于活动状态，其他 NIC 保持未使用状态，除非将流量故障转移到这些 NIC。在绑定网络上配置管理接口或辅助接口可以提供恢复能力。
- **混合流量。**如果绑定的 NIC 同时传输基于 IP 的存储流量和来宾流量，则仅对来宾流量和控制域流量实施负载均衡。从本质上说，控制域是一个虚拟机，因此，可以像其他来宾一样使用 NIC。Citrix Hypervisor 像平衡 VM 流量一样平衡控制域流量。

### 流量平衡

Citrix Hypervisor 使用数据包的源 MAC 地址在 NIC 之间对流量进行平衡。由于传输管理流量时仅呈现一个源 MAC 地址，因此，主动-主动模式仅使用一个 NIC，并且不平衡流量。流量平衡基于两个因素：

- 虚拟机及其关联的发送或接收流量的 VIF
- 发送的数据量（以 KB 为单位）。

Citrix Hypervisor 会评估每个 NIC 发送和接收的数据量（以 KB 为单位）。如果在一个 NIC 上发送的数据量超出在另一个 NIC 上发送的数据量，Citrix Hypervisor 会重新平衡各 VIF 使用的 NIC。系统将传输 VIF 的全部负载。一个 VIF 的负载从不在两个 NIC 之间拆分。

尽管主动-主动 NIC 绑定可以为来自多个 VM 的流量提供负载平衡，但是不能为单个 VM 提供两个 NIC 的吞吐量。任何给定 VIF 一次只能使用绑定中的一个链路。当 Citrix Hypervisor 定期重新平衡流量时，VIF 不会永久分配给绑定中的某个特定 NIC。

主动-主动模式有时称为源负载平衡 (SLB) 绑定，因为 Citrix Hypervisor 使用 SLB 在绑定的网络接口之间共享负载。SLB 派生自开源自适应负载平衡 (ALB) 模式并重复使用 ALB 功能在各 NIC 之间动态重新平衡负载。

重新平衡时，系统会跟踪给定时间段内通过每个从属（接口）的字节数。如果要发送的数据包包含新的源 MAC 地址，该数据包会分配给具有最低利用率的从属接口。系统会定期重新平衡流量。

每个 MAC 地址都有对应的负载，而且 Citrix Hypervisor 能够在 NIC 之间转移整体负载，具体情况取决于 VM 发送和接收的数据量。对于主动-主动流量，来自一个 VM 的所有流量只能在一个 NIC 上传输。

**注意：**

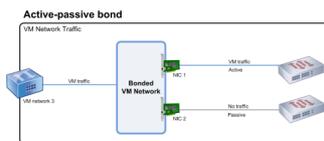
主动-主动绑定不要求交换机支持 EtherChannel 或 802.3ad (LACP)。

### 主动-被动绑定

主动-被动绑定仅通过其中一个 NIC 路由流量。如果主动 NIC 断开了网络连接，流量将故障转移到绑定中的另一个 NIC。主动-被动绑定通过主动 NIC 路由流量。如果主动 NIC 出现故障时，流量将转移到被动 NIC。

主动-被动绑定可在 Linux 桥接和 vSwitch 网络堆栈中可用。与 Linux 桥接一起使用时，您可以绑定两个 NIC。与 vSwitch 一起使用时，只能绑定两个、三个或四个 NIC。但是，无论流量类型为何，在主动-被动模式下绑定 NIC 时，只有一个链路处于活动状态，并且链路之间不会实施负载平衡。

下图显示了在主动-被动模式下配置的两个绑定的 NIC。



主动-主动模式是 Citrix Hypervisor 中的默认绑定配置。如果要使用 CLI 配置绑定，则必须为主动-被动模式指定一个参数。否则，将创建主动-主动绑定。不必因为网络传输管理流量或存储流量而配置主动-被动模式。

主动-被动模式是获得恢复能力的良好选择，因为此模式可以提供多种优势。使用主动-被动绑定时，流量不会在 NIC 之间移动。同样，主动-被动绑定可以让您配置两台交换机以实现冗余，但不需要堆栈。如果管理交换机停机，堆栈交换机会成为单一故障点。

主动-被动模式不要求交换机支持 EtherChannel 或 802.3ad (LACP)。

当您不需要负载平衡或当您只希望在一个 NIC 上传输流量时，请考虑配置主动-被动模式。

**重要:**

在创建了 VIF 或者池投入使用之后，在对绑定进行更改或者创建绑定时一定要小心谨慎。

### **LACP 链路聚合控制协议绑定**

LACP 链路聚合控制协议是一个绑定类型，它可将一组端口捆绑在一起，当作一个逻辑通道使用。LACP 绑定可以提供故障转移，并能增加可用带宽总量。

与其他绑定模式不同，LACP 绑定要求配置链路两端，也就是在主机上创建绑定，并在交换机上为每个绑定创建链路聚合组 (LAG)。请参阅 LACP 绑定的交换机配置。必须将 vSwitch 配置为网络堆栈，才能使用 LACP 绑定。此外，交换机还必须支持 IEEE 802.3ad 标准。

主动-主动 SLB 绑定和 LACP 绑定的比较：

#### **主动-主动 SLB 绑定**

优势：

- 可以与硬件兼容性列表中的任何交换机结合使用。
- 不要求交换机支持堆栈。
- 支持四个 NIC。

注意事项：

- 要实现最佳负载平衡，每个 VIF 至少要使用一个 NIC。
- 存储或管理流量无法在多个 NIC 上拆分。
- 负载平衡仅在有多个 MAC 地址时实施。

### **LACP 绑定**

优势：

- 无论流量类型为何，所有链路都可以处于活动状态。
- 流量平衡不依赖于源 MAC 地址，因此，所有流量类型都可以平衡。

注意事项：

- 交换机必须支持 IEEE 802.3ad 标准。
- 要求在交换机端执行配置。
- 仅支持 vSwitch。
- 要求使用一台交换机或堆栈交换机。

### 流量平衡

Citrix Hypervisor 支持两个 LACP 绑定哈希类型。术语“哈希”指的是 NIC 和交换机分发流量的方式，分别为 (1) 基于源和目标地址的 IP 和端口的负载均衡和 (2) 基于源 MAC 地址的负载均衡。

根据哈希类型和流量模式，LACP 绑定有可能比主动-主动 NIC 绑定更均匀地分发流量。

注意：

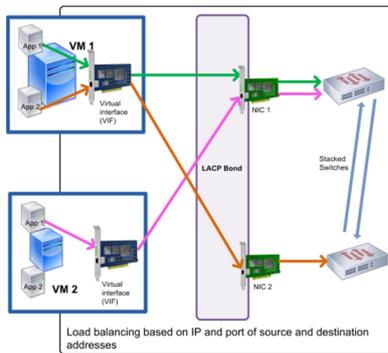
可以在主机和交换机上分别为传出和传入流量配置设置，而且两端的配置不一定匹配。

基于源和目标地址的 **IP** 和端口的负载均衡。

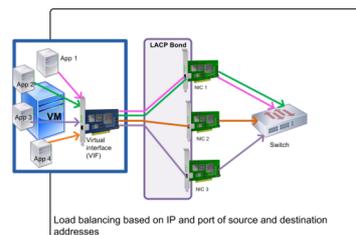
此哈希类型是默认的 LACP 绑定散列算法。如果源或目标 IP 或端口号有变化，来自一个来宾的流量则可以通过两个链路分发。

如果一个虚拟机正在运行多个应用程序，而且每个应用程序都使用不同的 IP 或端口号，此哈希类型就可以通过多个链路分发流量。分发流量将使来宾能够使用聚合吞吐量。此哈希类型可以让一个来宾使用多个 NIC 的整体吞吐量。

如下图所示，此哈希类型能够将虚拟机上两个不同的应用程序的流量分发到两个不同的 NIC 上。



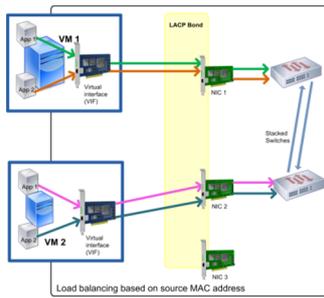
当您希望平衡同一 VM 上两个不同应用程序的流量时，根据源和目标地址的 IP 和端口配置 LACP 绑定很有用。例如，只将一个虚拟机配置为使用三个 NIC 的绑定。



此哈希类型的平衡算法使用五个因素在 NIC 上分发流量，即源 IP 地址、源端口号、目标 IP 地址、目标端口号和源 MAC 地址。

基于源 **MAC** 地址的负载均衡。

当同一主机上有多个虚拟机时，此类型的负载均衡可以发挥很好的作用。流量平衡根据发起流量的 VM 的虚拟 MAC 地址实施。Citrix Hypervisor 使用同一算法发送传出流量，就像在主动-主动绑定模式下一样。来自同一来宾系统的流量不会在多个 NIC 之间拆分。因此，如果 VIF 的数量少于 NIC，此哈希类型不适合使用，原因是由于流量无法在 NIC 之间拆分，负载均衡达不到最佳效果。



### 交换机配置

根据您的冗余需求，可以将绑定中的每个 NIC 连接到同一个或不同的堆栈交换机。如果将其中一个 NIC 连接到另一个冗余的交换机，则在某个 NIC 或交换机出现故障时，流量将故障转移到另一个 NIC。添加第二个交换机可以通过以下方式防止配置中出现单点故障：

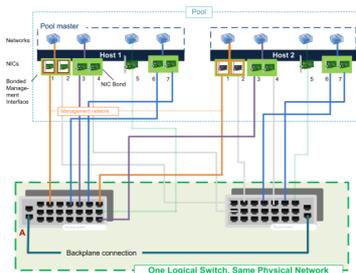
- 将绑定管理接口中的其中一个链路连接到第二个交换机时，如果此交换机出现故障，管理网络依然保持联机，并且主机仍然能够相互通信。
- 将一个链路（适用于任何流量类型）连接到第二个交换机时，如果 NIC 或交换机出现故障，虚拟机将仍保持在网络上，因为其流量会故障转移到另一个 NIC/交换机。

希望将绑定的 NIC 连接到多个交换机并且已配置 LACP 绑定模式时，请使用堆栈交换机。术语“堆栈交换机”指的是将多个物理交换机配置为一个逻辑交换机。必须根据交换机制造商提供的指南，利用交换机管理软件，以物理方式将交换机连接在一起，使多个交换机作为一个逻辑交换装置运行。通常情况下，交换机堆栈仅通过专有扩展实现，而且交换机供应商可能会使用不同的术语宣传此功能。

#### 注意：

如果使用主动-主动绑定时遇到问题，可能需要使用堆栈交换机。主动-被动绑定不需要堆栈交换机。

下图说明绑定中 NIC 的电缆和网络配置的配对情况。



### LACP 绑定的交换机配置

由于交换机配置的具体详情因制造商而异，因此，配置交换机以便与 LACP 绑定结合使用时，需要记住几个关键点：

- 交换机必须支持 LACP 和 IEEE 802.3ad 标准。

- 在交换机上创建 LAG 组时，必须为主机上的每个 LACP 绑定创建一个 LAG 组。例如，如果有一个五主机池，并且已在每个主机上的 NIC 4 和 5 上创建了 LACP 绑定，则必须在交换机上创建五个 LAG 组。每个端口集的一个组对应于主机上的 NIC。

可能还需要将 VLAN ID 添加到 LAG 组中。

- Citrix Hypervisor LACP 绑定要求将 LAG 组中的“静态模式”设置设置为“已禁用”。

如先前在交换机配置中提及的一样，需要通过堆栈交换机将 LACP 绑定连接到多个交换机。

### 设置后的初始网络连接配置

Citrix Hypervisor 服务器的网络配置是在主机初始安装期间指定的。IP 地址配置（DHCP/静态）、用作管理接口的 NIC 和主机名等选项是根据安装期间提供的值设置的。

当主机包含多个 NIC 时，安装后进行的配置取决于安装期间选择用于管理操作的 NIC：

- 为主机中的每个 NIC 创建 PIF
- 使用安装期间指定的 IP 地址选项配置选择用作管理接口的 NIC 的 PIF
- 为每个 PIF 创建一个网络（“network 0”、“network 1”等）
- 将每个网络分别连接到一个 PIF
- 除用作管理接口的 PIF 外，IP 寻址选项对所有 PIF 都保留未配置

当主机包含单一 NIC 时，安装后将进行以下配置：

- 创建对应于该主机的单个 NIC 的一个 PIF
- 使用安装期间指定的 IP 地址选项配置 PIF 并启用主机的管理
- 设置 PIF 以用于主机管理操作
- 创建单个网络，即网络 0
- 将网络 0 连接到 PIF 以启用 VM 的外部连接

在带标记的 VLAN 网络中完成安装 Citrix Hypervisor 时，安装后将存在以下配置：

- 为主机中的每个 NIC 创建 PIF
- 使用安装期间指定的 IP 地址配置来配置选择用作管理接口的 NIC 上的带标记的 VLAN 的 PIF
- 为每个 PIF 创建一个网络（例如：network 1、network 2 等）。创建其他 VLAN 网络（例如，为池范围内的与 VLAN<TAG> 上的 eth0 关联的网络）
- 将每个网络分别连接到一个 PIF。设置 VLAN PIF 以用于主机管理操作

在这两种情况下，生成的网络连接配置允许 Citrix Hypervisor、xe CLI 及任何其他在独立计算机上运行的管理软件通过管理接口的 IP 地址连接到 XenCenter 服务器。配置还为在主机上创建的 VM 提供外部网络连接。

用于管理操作的 PIF 是在 Citrix Hypervisor 安装期间唯一使用 IP 地址配置的 PIF。VM 的外部网络连接通过使用网络对象（用作虚拟以太网交换机）将 PIF 桥接到 VIF 来实现。

网络连接功能（例如 VLAN、NIC 绑定和将 NIC 专用于存储流量）的步骤将在后面各节中介绍。

## 更改网络连接配置

可以通过修改网络对象，更改网络连接配置。为此，请运行影响网络对象或 VIF 的命令。

### 修改网络对象

可以更改网络的各个方面，例如帧大小 (MTU)、名称标签、名称说明、用途以及其他值。请使用 `xe network-param -set` 命令及其相关联的参数来更改值。

运行 `xe network-param-set` 命令时，唯一必需参数是 `uuid`。

可选参数为：

- `default_locking_mode`。请参阅[简化云中的 VIF 锁定模式配置](#)。
- `name-label`
- `name-description`
- `MTU`
- `purpose`。请参阅[向网络中添加用途](#)。
- `other-config`

如果未给定参数值，此参数将被设为空值。要在映射参数中设置 (键, 值) 对，请使用语法 `map-param:key=value`。

### 更改绑定的最高延迟

默认情况下，为绑定设置 31000 毫秒的最高延迟，以免流量在出现故障后重新平衡到 NIC 上。虽然看似较长，但最高延迟对于所有绑定模式都非常重要，而不仅限于主动-主动模式。

但是，如果了解为环境选择的相应的设置，可以使用下面的过程更改绑定的最高延迟。

设置最高延迟（毫秒）：

```
1 xe pif-param-set uuid=<uuid of bond master PIF> other-config:bond-updelay=<delay in ms>
```

要使更改生效，必须拔出物理接口，然后重新插入：

```
1 xe pif-unplug uuid=<uuid of bond master PIF>
```

```
1 xe pif-plug uuid=<uuid of bond master PIF>
```

## 管理网络连接

June 4, 2019

本部分中介绍的网络配置过程会有所差别，具体取决于您要配置的服务器是独立服务器还是资源池中的服务器。

### 跨服务器专用网络

先前版本的 Citrix Hypervisor 允许您创建单服务器专用网络，该网络允许同一台主机上运行的 VM 相互通信。跨服务器专用网络功能，对单服务器专用网络这一概念进行了扩展，允许不同主机上的 VM 相互通信。跨服务器专用网络将单服务器专用网络的相同隔离属性与在资源池中分布主机的额外功能结合在一起。实现这种结合后，VM 可以通过连接跨服务器专用网络来使用各种 VM 灵活性功能（例如，实时迁移）。

跨服务器专用网络是隔离网络。不连接到专用网络的 VM 无法探查流量或者将流量引入到网络中。即使当 VM 位于相同的物理主机上，并且该主机的 VIF 连接到相同的基础物理网络设备 (PIF) 上的网络时，也会出现此问题。VLAN 提供相似的功能。但是，与 VLAN 不同，跨服务器专用网络通过使用通用路由封装 (GRE) IP 通道协议，无需配置物理交换机光纤即可提供隔离。

专用网络无需物理交换机即可提供以下益处：

- 单服务器专用网络的隔离属性
- 跨资源池分布功能，允许连接到同一个专用网络的 VM 依赖于同一资源池中的多个主机
- 与实时迁移等功能的兼容性

跨服务器专用网络在管理接口或辅助接口上创建，因为这些网络需要可进行 IP 寻址的 NIC。可以使用任何启用了 IP 的 NIC 作为底层网络传输。如果选择将跨服务器专用网络流量放置在辅助接口上，该辅助接口必须位于单独的子网中。

如果任何管理接口或辅助接口位于同一子网中，流量将无法正确路由。

#### 注意：

要创建跨服务器专用网络，必须满足以下条件：

- 池中的所有主机必须使用 Citrix Hypervisor 6.0 或更高版本。
- 池中的所有主机都必须将 vSwitch 用于网络连接堆栈。
- vSwitch Controller 必须正在运行，并且必须已添加池。（池必须配置 vSwitch Controller，用来处理 vSwitch 连接所需的初始化和配置任务。）
- 必须在配置为管理接口的 NIC 上创建跨服务器专用网络。该 NIC 可以是管理接口，也可以是专门为该目的

而配置的辅助接口（支持 IP 的 PIF），但前提是它位于一个单独的子网上。

有关配置 vSwitch 的详细信息，请参阅 [vSwitch](#) 和 [Controller](#)。有关基于 UI 的配置专用网络的过程，请参阅 [XenCenter 帮助](#)。

### 在独立服务器中创建网络

安装主机期间会为每个 PIF 创建外部网络，因此仅在执行以下操作时才需要创建额外的网络：

- 使用专用网络
- 支持高级操作，例如 VLAN 或 NIC 绑定

有关如何使用 XenCenter 添加或删除网络的信息，请参阅 [XenCenter 帮助](#)。

打开 Citrix Hypervisor 服务器文本控制台。

使用 `network-create` 命令创建网络，该命令将返回新创建的网络的 UUID：

```
1 xe network-create name=label=mynetwork
```

此时，该网络尚未连接到 PIF，因此属于内部网络。

### 在资源池中创建网络

资源池中的所有 Citrix Hypervisor 服务器必须具有同等数量的物理 NIC。主机加入池时，并不需要严格遵从这一要求。

由于池中的所有主机都共享一组公用网络，因此，池中的 Citrix Hypervisor 服务器具有相同的物理网络配置非常重要。根据设备名称将各个主机上的 PIF 连接到池范围内的网络。例如，池中具有 `eth0` NIC 的所有 Citrix Hypervisor 服务器都将相应的 PIF 插入池范围内的 `Network 0` 网络。这对于具有 `eth1` NIC 和 `Network 1` 的主机以及至少在池中的一个 Citrix Hypervisor 服务器上出现的其他 NIC 同样适用。

如果某个 Citrix Hypervisor 服务器具有的 NIC 数量与池中其他主机具有的 NIC 数量不同，情况就复杂了。复杂性增加是因为并非所有池网络都对所有池主机有效。例如，如果主机 `host1` 和 `host2` 位于同一池中，但 `host1` 有四个 NIC，`host2` 只有两个 NIC，则只有连接到与 `eth0` 和 `eth1` 对应的 PIF 的网络才对 `host2` 有效。VIF 连接到与 `eth2` 和 `eth3` 对应的网络的 `host1` 上的 VM 将无法迁移到主机 `host2`。

### 创建 VLAN

对于资源池中的服务器，可以使用 `pool-vlan-create` 命令。此命令将创建 VLAN，并在池中的主机上自动创建和插入所需的 PIF。有关详细信息，请参阅 [pool-vlan-create](#)。

打开 Citrix Hypervisor 服务器控制台。

创建用于 VLAN 的网络。将返回新网络的 UUID：

```
1 xe network-create name=label=network5
```

使用 `pif-list` 命令找到与物理 NIC（支持所需的 VLAN 标记）对应的 PIF 的 UUID。返回所有 PIF 的 UUID 和设备名称，其中包括任何现有的 VLAN：

```
1 xe pif-list
```

创建 VLAN 对象，该对象指定要连接到新 VLAN 的所有 VM 上所需的物理 PIF 和 VLAN 标记。创建新的 PIF 并将其插入指定的网络。返回新 PIF 对象的 UUID。

```
1 xe vlan-create network-uuid=network_uuid pif-uuid=pif_uuid vlan=5
```

将 VM VIF 连接到新网络。有关详细信息，请参阅在独立服务器中创建网络。

## 在独立主机上创建 NIC 绑定

我们建议您使用 XenCenter 创建 NIC 绑定。有关说明，请参阅 XenCenter 帮助。

本节介绍如何使用 xe CLI 绑定不属于池的 Citrix Hypervisor 服务器上的 NIC 接口。有关使用 xe CLI 在组成资源池的 Citrix Hypervisor 服务器上创建 NIC 绑定的信息，请参阅在资源池中创建 NIC 绑定。

## 创建 NIC 绑定

在绑定 NIC 时，绑定会包含用作管理接口的 PIF/NIC。从 Citrix Hypervisor 6.0 开始，管理接口会自动移动到该绑定的 PIF。

1. 使用 `network-create` 命令创建用于绑定的 NIC 的新网络。将返回新网络的 UUID：

```
1 xe network-create name=label=bond0
```

2. 使用 `pif-list` 命令确定要在绑定中使用的 PIF 的 UUID：

```
1 xe pif-list
```

3. 执行以下操作之一：

- 要在主动-主动模式（默认模式）下配置绑定，请使用 `bond-create` 命令创建绑定。指定新创建的网络 UUID 和要绑定的各 PIF 的 UUID，以逗号分隔各参数：

```
1 xe bond-create network-uuid=network_uuid /  
2     pif-uuids=pif_uuid_1,pif_uuid_2,pif_uuid_3,pif_uuid_4
```

绑定两个 NIC 时，请键入两个 UUID；绑定四个 NIC 时，请输入四个 UUID。在运行该命令之后，将返回该绑定的 UUID。

- 要在主动-被动或 LACP 绑定模式下配置绑定，请使用相同的语法，添加可选的 `mode` 参数并指定 `lACP` 或 `active-backup`：

```
1 xe bond-create network-uuid=network_uuid pif-uuids=pif_uuid_1
   , /
2   pif_uuid_2,pif_uuid_3,pif_uuid_4 /
3   mode=balance-slb | active-backup | lACP
```

### 控制绑定的 **MAC** 地址

绑定管理接口时，将包含正用作管理接口的 PIF/NIC。如果主机使用 DHCP，该绑定的 MAC 地址将与正在使用的 PIF/NIC 相同。管理接口的 IP 地址可以保持不变。

可以更改该绑定的 MAC 地址，使其不同于（当前）管理接口 NIC 的 MAC 地址。但是，当启用了该绑定而正在使用的 MAC/IP 地址发生变化时，与主机的现有网络会话将停止。

可以通过以下两种方式控制该绑定的 MAC 地址：

- 可以在 `bond-create` 命令中指定 `mac` 可选参数。使用此参数可以将该绑定的 MAC 地址设置为任意地址。
- 如果未指定 `mac` 参数，Citrix Hypervisor 将使用管理接口（如果管理接口是绑定中的接口之一）的 MAC 地址。如果管理接口不是绑定的一部分，但另一个管理接口是，则绑定将使用该管理接口的 MAC 地址（以及 IP 地址）。如果绑定中的所有 NIC 都不是管理接口，则绑定将使用第一个指定 NIC 的 MAC 地址。

### 还原 **NIC** 绑定

如果将 Citrix Hypervisor 服务器还原为非绑定配置，`bond-destroy` 命令会自动将主-从属节点配置为要用于管理接口的接口。因此，所有 VIF 都将移动到该管理接口。如果主机的管理接口位于带标记的 VLAN 绑定接口上，执行 `bond-destroy` 时，管理 VLAN 将移至主-从属节点。

术语“主-从属节点”是指在创建绑定时用来复制 MAC 和 IP 配置的 PIF。在绑定两个 NIC 时，主-从属节点是：

1. 管理接口 NIC（如果管理接口是绑定的 NIC 之一）。
2. 任何其他具有 IP 地址的 NIC（如果管理接口不是绑定的一部分）。
3. 第一个指定的 NIC。可以通过运行以下命令来确定它是哪个 NIC：

```
1 xe bond-list params=all
```

### 在资源池中创建 **NIC** 绑定

如果可能，请尽量在创建初始资源池的过程中创建 NIC 绑定，然后再将更多主机加入池或创建 VM。这样，可以在主机加入池时将绑定配置自动复制到其中，并减少所需的步骤。

将 NIC 绑定添加到现有池中需要执行下列操作之一：

- 使用 CLI 在主服务器上配置绑定，然后在池的每个成员上配置绑定。
- 使用 CLI 在主服务器上配置绑定，然后重新启动每个池成员，以便从池主服务器继承设置。
- 使用 XenCenter 在主服务器上配置绑定。XenCenter 会自动将成员服务器上的网络连接设置与主服务器同步，这样，您就不需要重新启动成员服务器。

为简单起见并且为了避免错误配置，我们建议使用 XenCenter 创建 NIC 绑定。有关详细信息，请参阅 XenCenter 帮助。

本部分介绍如何使用 xe CLI 在组成资源池的 Citrix Hypervisor 服务器上创建绑定的 NIC 接口。有关使用 xe CLI 在独立主机上创建 NIC 绑定的信息，请参阅在独立主机上创建 NIC 绑定。

**警告：**

不要在启用了高可用性功能的情况下尝试创建网络绑定。创建绑定的过程会干扰正在进行的高可用性信号检测并导致主机进行自我防护（自行关闭）。主机将无法正确重新启动，并且可能需要运行 `host-emergency-ha-disable` 命令才能恢复。

选择要作为主服务器的主机。默认情况下，主服务器主机属于未命名的池。要使用 CLI 创建资源池，请重命名现有的无名称的池：

```
1 xe pool-param-set name-label="New Pool" uuid=pool_uuid
```

按照创建 NIC 绑定中的说明创建 NIC 绑定。

打开要加入到池的主机中的控制台，然后运行命令：

```
1 xe pool-join master-address=host1 master-username=root master-password=password
```

网络和绑定信息将自动复制到新主机中。管理接口自动从最初创建时所在的主机 NIC 移动到绑定的 PIF。即，管理接口现在包含在绑定中，以便整个绑定用作管理接口。

使用 `host-list` 命令查找正在配置的主机的 UUID：

```
1 xe host-list
```

**警告：**

请勿在启用了高可用性功能的情况下尝试创建网络绑定。创建绑定的过程会干扰正在进行的高可用性信号检测并导致主机进行自我防护（自行关闭）。主机将无法正确重新启动，并且您可能需要运行 `host-emergency-ha-disable` 命令才能恢复。

## 配置专用存储 NIC

可以使用 XenCenter 或 xe CLI 为 NIC 分配 IP 地址，并将其专用于特定功能（例如存储流量）。在为 NIC 配置 IP 地址时，可以通过创建辅助接口来进行配置。（用于管理且支持 IP 的 NIC Citrix Hypervisor 称为管理接口。）

当您希望将辅助接口专用于特定用途时，请确保拥有适当的网络配置。这是为了确保 NIC 仅用于所需的流量。要将 NIC 专用于存储流量，请对 NIC、存储目标、交换机和 VLAN 进行配置，以便只能通过分配的 NIC 访问该目标。如果您的物理配置和 IP 配置不限制可以通过存储 NIC 发送的流量，则可以通过辅助接口来发送流量（例如管理流量）。

创建新辅助接口用于传输存储流量时，必须为其分配一个 IP 地址，即：

- 在与存储控制器相同的子网中（如果适用），并且
- 不在与任何其他辅助接口或管理接口相同的子网中。

配置辅助接口时，每个辅助接口必须位于单独的子网上。例如，如果要为存储额外配置两个辅助接口，则需要 IP 地址位于三个不同的子网中 – 一个用于管理接口的子网，一个用于辅助接口 1 的子网，以及一个用于辅助接口 2 的子网。

如果要使用绑定为存储流量提供恢复能力，您可能希望考虑使用 LACP 而非 Linux 桥接绑定。要使用 LACP 绑定，必须将 vSwitch 配置为网络连接堆栈。有关详细信息，请参阅 [vSwitch 网络](#)。

### 注意：

在选择要配置为辅助接口以与 iSCSI 或 NFS SR 一起使用的 NIC 时，请确保该专用 NIC 使用不能从管理接口路由的单独 IP 子网。如果无法确保上述条件，则由于初始化网络接口的顺序，很可能在主机重新启动后通过主管理接口定向存储流量。

确保 PIF 位于独立子网中或将路由配置为适合您的网络拓扑，以通过所选 PIF 实现所需流量。

为 PIF 设置一个 IP 配置，从而为模式参数添加恰当的值。如果使用静态 IP 寻址，请添加 IP、子网掩码、网关和 DNS 参数：

```
1 xe pif-reconfigure-ip mode=DHCP | Static uuid=pif-uuid
```

将 PIF 的 `disallow-unplug` 参数设置为 `true`：

```
1 xe pif-param-set disallow-unplug=true uuid=pif-uuid
```

```
1 xe pif-param-set other-config:management_purpose="Storage" uuid=pif-  
  uuid
```

如果希望将辅助接口用于也可以从管理接口路由的存储（请记住，此配置并非最佳做法），则有两种选择：

- 主机重新启动后，请确保正确配置了辅助接口。使用 `xe pbd-unplug` 和 `xe pbd-plug` 命令重新初始化主机上的存储连接。此命令将重新启动存储连接并通过正确的接口对其进行路由。
- 或者，可以使用 `xe pif-forget` 从 Citrix Hypervisor 数据库中删除接口，然后在控制域中手动配置该接口。`xe pif-forget` 属于高级选项，要求您熟悉如何手动配置 Linux 网络连接。

## 使用启用了 **SR-IOV** 的 **NIC**

单根 I/O 虚拟化 (SR-IOV) 是一种虚拟化技术，允许单个 PCI 设备在物理系统中显示为多个 PCI 设备。实际的物理设备称为物理功能 (PF)，而其他设备称为虚拟功能 (VF)。虚拟机管理程序可以向虚拟机 (VM) 分配一个或多个 VF：来宾之后可以使用该设备，就像该设备是直接分配的一样。

向 VM 分配一个或多个 NIC VF 将允许其网络流量跳过虚拟交换机。每个 VM 在经过这种配置后，就像直接使用 NIC 一样，这样会降低处理开销并改善性能。

### **SR-IOV** 的优势

SR-IOV VF 的性能优于 VIF。它可以确保流量之间的基于硬件的隔离从不同的 VM 传输到相同的 NIC（跳过 Citrix Hypervisor 网络堆栈）。

通过此功能，您可以：

- 在支持 SR-IOV 的 NIC 上启用 SR-IOV。
- 在支持 SR-IOV 的 NIC 上禁用 SR-IOV。
- 作为 VF 资源池管理 SR-IOV VF。
- 将 SR-IOV VF 分配给 VM。
- 配置 SR-IOV VF（例如，MAC 地址、VLAN、评分）。
- 运行测试，以确认是否作为自动化认证工具包的一部分支持 SR-IOV。

### 系统配置

请正确配置硬件平台以支持 SR-IOV。需要使用以下技术：

- I/O MMU 虚拟化 (AMD-Vi 和 Intel VT-d)
- 备用路由 ID 解释 (ARI)
- 地址转换服务 (ATS)
- 访问控制服务 (ACS)

查看您的系统随附的文档，了解有关如何配置 BIOS 以启用所提及的技术的信息。

### 在 **NIC** 上启用 **SR-IOV** 网络

在 XenCenter 中，使用网络连接选项卡中的新建网络向导在 NIC 上创建并启用 SR-IOV 网络。

将 **SR-IOV** 网络分配给虚拟接口 (**VM** 级别)

在 XenCenter 中，使用网络连接选项卡中的添加虚拟接口向导添加启用了 SR-IOV 的网络作为该 VM 的虚拟接口。有关详细信息，请参阅 XenCenter 帮助。

支持的 **NIC** 和来宾

有关受支持的硬件平台和 NIC 的列表，请参阅[硬件兼容性列表](#)。请参阅特定来宾的供应商提供的文档，以确定其是否支持 SR-IOV。

限制

- 对于某些使用旧版驱动程序的 NIC（例如，Intel I350 系列），必须重新启动主机以启用或禁用这些设备上的 SR-IOV。
- SR-IOV 仅支持 HVM 来宾。
- 不支持具有不同类型的 NIC 的池级别 SR-IOV 网络。
- 由于 NIC 硬件限制，SR-IOV VF 和来自同一 NIC 的常规 VIF 可能无法相互通信。要使这些主机能够进行通信，请确保通信使用模式 VF 到 VF 或 VIF 到 VIF，而非 VF 到 VIF。
- 某些 SR-IOV VF 的服务质量设置不起作用，因为这些设置不支持网络速率限制。
- 不支持在使用 SR-IOV VF 的 VM 上执行实时迁移、挂起和检查点操作。
- SR-IOV VF 不支持热插拔。
- 对于某些使用旧版 NIC 驱动程序的 NIC，即使在主机重新启动之后可能也需要重新启动，这表示 NIC 无法启用 SR-IOV。
- 在早期版本中创建的 VM 无法从 XenCenter 使用此功能。
- 如果您的 VM 具有一个 SR-IOV VF，需要实时迁移的功能将不可用。这是由于 VM 直接绑定到支持 SR-IOV 的物理 NIC VF。通过 SR-IOV VF 发送的任何 VM 网络流量都会绕过 vSwitch。因此，不能创建 ACL 或查看服务质量 (QoS)。
- 硬件限制：使用功能级别重置 (FLR) 的虚拟机管理程序请求时，SR-IOV 功能依赖于要在 100 毫秒内将设备功能重置为原始状态的 Controller。
- 可以在利用高可用性功能的环境中使用 SR-IOV。但是，并不会将 SR-IOV 视为容量规划。当具有相应资源的池中存在主机时，已分配 SR-IOV VF 的 VM 将在最大努力的基础上重新启动。这些资源包括在恰当的网络中启用的 SR-IOV 以及可用的 VF。

将 **SR-IOV VF** 配置为使用旧版驱动程序

通常情况下，可以自动确定 NIC 能够支持的最大 VF 数量。对于使用旧版驱动程序的 NIC（例如，Intel I350 系列），此限制在驱动程序模块配置文件内部定义。此限制可能需要手动调整。要将其设置为最大值，请使用编辑器打开该文件，并更改行起始内容：

```
1 ## VFs-maxvfs-by-user:
```

例如，要将 `igb` 驱动程序的最大 VF 数量设置为 4，请编辑 `/etc/modprobe.d/igb.conf`，使其内容变为：

```
1 ## VFs-param: max_vfs
2 ## VFs-maxvfs-by-default: 7
3 ## VFs-maxvfs-by-user: 4
4 options igb max_vfs=0
```

注意：

- 该值必须小于或等于 `VFs-maxvfs-by-default` 行中的值。
- 请勿更改这些文件中的任何其他行。
- 请在启用 SR-IOV 之前进行更改。

## CLI

请参阅 [SR-IOV 命令](#)，了解有关创建、删除、显示 SR-IOV 网络以及向 VM 分配 SR-IOV VF 的 CLI 说明。

## 控制传出数据的速率 (QoS)

要限制 VM 每秒可以发送的传出数据量，可以针对 VM 虚拟接口 (VIF) 设置可选的服务质量 (QoS) 值。该设置允许您为传出的数据包指定最大传输速率（单位为 KB/秒）。

服务质量值将限制源自 VM 的传输速率。服务质量设置不限制 VM 可以接收的数据量。如果需要限制接收量，我们建议您限制网络中较高层（例如，交换机层）传入数据包的速率。

根据在池中配置的网络连接堆栈，可以在以下两个位置之一中的 VM 虚拟接口 (VIF) 上设置服务质量值。在 vSwitch Controller 上，或者在 Citrix Hypervisor 中（使用 CLI 或 XenCenter）。

## vSwitch

配置方法：

- **vSwitch Controller** 如果 vSwitch 是网络连接堆栈，这将在 VIF 上设置最大传输速率的首选方法。使用 vSwitch 堆栈时，XenCenter 服务质量选项不可用。

- **xe** 命令可以使用以下示例中的命令设置服务质量传输速率。但是，首选方法是通过 vSwitch Controller UI，因为 vSwitch Controller UI 提供更细化的控制。

## Linux 桥

可用的配置方法：

- **XenCenter** 可以在属性对话框中为虚拟接口设置服务质量传输速率限制值。
- **xe** 命令可以在 CLI 中使用下一部分内容中介绍的命令来设置服务质量传输速率。

重要：

当 vSwitch 配置为网络连接堆栈时，可能会无意中在 vSwitch Controller 上和 Citrix Hypervisor 服务器内部配置 QoS 值。在这种情况下，Citrix Hypervisor 会使用您设置的最低速率来限制传出流量。

用于设置 QoS 的 CLI 命令的示例：

要使用 CLI 将 VIF 的最大传输速率限制为 100 kb/秒，请使用 `vif-param-set` 命令：

```
1 xe vif-param-set uuid=vif_uuid qos_algorithm_type=ratelimit
2 xe vif-param-set uuid=vif_uuid qos_algorithm_params:kpbs=100
```

注意：

如果要使用 vSwitch Controller，我们建议在 vSwitch Controller 中而不是使用上面的 CLI 命令来设置传输速率限制。有关在 vSwitch Controller 中设置 QoS 速率限制的说明，请参阅 [vSwitch](#) 和 [Controller](#)。

## 更改网络连接配置选项

本节讨论如何更改 Citrix Hypervisor 服务器的网络连接配置。包括：

- 更改主机名（即，域名系统 (DNS) 名称）
- 添加或删除 DNS 服务器
- 更改 IP 地址
- 更改用作管理接口的 NIC
- 将新的物理 NIC 添加到服务器中
- 向网络中添加用途
- 启用 ARP 过滤（交换机端口锁定）

## Hostname

系统主机名（又称为域名或 DNS 名称）在池级别的数据库中定义，可以按如下所示使用 `xe host-set-hostname -live` CLI 命令进行修改：

```
1 xe host-set-hostname-live host-uuid=host_uuid host-name=host-name
```

基础控制域主机名也将动态更改以反映新主机名。

## DNS 服务器

要在 Citrix Hypervisor 服务器的 IP 寻址配置中添加或删除 DNS 服务器，请使用 `pif-reconfigure-ip` 命令。例如，对于具有静态 IP 的 PIF：

```
1 pif-reconfigure-ip uuid=pif_uuid mode=static DNS=new_dns_ip
```

### 更改独立主机的 IP 地址配置

可以使用 `xe` CLI 更改网络接口配置。请勿直接更改基础网络配置脚本。

要更改 PIF 的 IP 地址配置，请使用 `pif-reconfigure-ip` CLI 命令。有关 `pif-reconfigure-ip` 命令参数的详细信息，请参阅 [pif-reconfigure-ip](#)。有关更改资源池中的主机 IP 地址的信息，请参阅下面的部分。

### 更改资源池中的 IP 地址配置

资源池中的 Citrix Hypervisor 服务器具有用于管理和与池中的其他主机之间的相互通信的单一管理 IP 地址。对于主节点主机和其他主机来说，更改主机的管理接口的 IP 地址所需的步骤是不同的。

#### 注意：

更改服务器的 IP 地址和其他网络连接参数时必须谨慎。根据网络拓扑和正在进行的更改，可能会断开网络存储连接。如果出现此问题，必须使用 XenCenter 中的修复存储功能或使用 `pbid-plug` CLI 命令来重新插入存储。因此，我们建议您先将 VM 从服务器中迁移出来，然后再更改服务器的 IP 配置。

根据需要，使用 `pif-reconfigure-ip` CLI 命令设置 IP 地址。有关 `pif-reconfigure-ip` 命令参数的详细信息，请参阅 [pif-reconfigure-ip](#)。

```
1 xe pif-reconfigure-ip uuid=pif_uuid mode=DHCP
```

使用 `host-list` CLI 命令，通过检查池中的所有其他 Citrix Hypervisor 服务器是否均可见来确认该成员主机是否已成功重新连接到主服务器主机：

```
1 xe host-list
```

更改主 Citrix Hypervisor 服务器的 IP 地址需要执行额外的步骤。这是因为每个池成员都使用公告的池主服务器 IP 地址进行通信。当其 IP 地址发生变化时，池成员不知道如何与主服务器进行联系。

请尽可能使用在池主服务器的池生命周期内不会轻易发生更改的专用 IP 地址。

根据需要，使用 `pif-reconfigure-ip` CLI 命令设置 IP 地址：

```
1 xe pif-reconfigure-ip uuid=pif_uuid mode=DHCP
```

池主服务器的 IP 地址发生变化后，所有成员主机在无法与主服务器主机联系时都将进入紧急模式。

在池主服务器上，使用 `pool-recover-slaves` 命令强制主服务器与每个池成员联系并通知其新的主服务器 IP 地址：

```
1 xe pool-recover-slaves
```

### 管理接口

在具有多个 NIC 的主机上安装 Citrix Hypervisor 后，会选择其中的一个 NIC 作为管理接口。管理接口用于 XenCenter 与主机之间的连接以及主机到主机的通信。

使用 `pif-list` 命令确定哪个 PIF 与要用作管理接口的 NIC 对应。将返回每个 PIF 的 UUID。

```
1 xe pif-list
```

使用 `pif-param-list` 命令验证用作管理接口的 PIF 的 IP 寻址配置。如有必要，请使用 `pif-reconfigure-ip` 命令配置要使用的 PIF 的 IP 寻址。

```
1 xe pif-param-list uuid=pif_uuid
```

使用 `host-management-reconfigure` CLI 命令更改用作管理接口的 PIF。如果此主机属于资源池，则必须在成员主机控制台上发出此命令：

```
1 xe host-management-reconfigure pif-uuid=pif_uuid
```

使用 `network-list` 命令确定哪个 PIF 与用作池中的所有主机的管理接口的 NIC 对应。此时将返回池范围内的网络的 UUID。

```
1 xe network-list
```

使用 `network-param-list` 命令提取池中的所有主机的 PIF UUID。使用 `pif-param-list` 命令验证管理接口的 PIF 的 IP 寻址配置。如有必要，请使用 `pif-reconfigure-ip` 命令配置要使用的 PIF 的 IP 寻址。

```
1 xe pif-param-list uuid=pif_uuid
```

使用 `pool-management-reconfigure` CLI 命令更改用作“网络”列表中列出的管理接口的 PIF。

```
1 xe pool-management-reconfigure network-uuid=network_uuid
```

### 禁用管理访问

要完全禁用对管理控制台的远程访问，请使用 `host-management-disable` CLI 命令。

#### 警告：

禁用了管理接口时，必须登录物理主机控制台才能执行管理任务。XenCenter 等外部接口在禁用了管理接口时不起作用。

### 添加新的物理 NIC

以常规方式在 Citrix Hypervisor 服务器上安装新的物理 NIC。然后，重新启动服务器后，运行 `xe` CLI 命令 `pif-scan` 以为新的 NIC 创建新的 PIF 对象。

### 向网络中添加用途

网络用途可以用来向网络中添加额外的功能。例如，使用网络建立 NBD 连接的功能。

要添加网络用途，请使用 `xe network-param-add` 命令：

```
1 xe network-param-add param-name=purpose param-key=purpose uuid=network-  
  uuid
```

要删除网络用途，请使用 `xe network-param-remove` 命令：

```
1 xe network-param-remove param-name=purpose param-key=purpose uuid=  
  network-uuid
```

网络用途的当前可用值为 `nbd` 和 `insecure_nbd`。有关详细信息，请参阅 [Citrix Hypervisor 更改块跟踪指南](#)。

### 使用交换机端口锁定

通过 Citrix Hypervisor 交换机端口锁定功能，可以限制未知、不受信任或可能存有敌意的 VM 假装拥有未分配给它们的 MAC 或 IP 地址的能力，从而控制从这些 VM 发送的流量。可以使用端口锁定命令，在默认情况下阻止网络上的所有流量，也可以定义特定 IP 地址，以便允许个别 VM 从中发送流量。

交换机端口锁定功能是为环境中关注内部威胁的公有云服务提供商设计的。此功能可以为公有云服务提供商提供帮助，在这些提供商的网络架构中，每个 VM 都有一个与 Internet 连接的公用 IP 地址。由于云租户不受信任，因此，可以采取安全措施（例如，欺骗防御）来确保租户无法攻击云中的其他虚拟机。

通过交换机端口锁定功能，您可以使所有租户或来宾系统使用同一个第 2 层网络，从而简化网络配置。

端口锁定命令的最重要的功能之一是可以限制不受信任的来宾发送的流量。这样将限制来宾假装拥有实际不拥有的 MAC 或 IP 地址的能力。具体而言，可以使用这些命令防止来宾系统：

- 申请 Citrix Hypervisor 管理员指定可以使用的 IP 或 MAC 地址以外的 IP 或 MAC 地址
- 拦截、欺骗或中断其他 VM 的流量

### 要求

- Citrix Hypervisor 交换机端口锁定功能支持 Linux 桥接和 vSwitch 网络连接堆栈。
- 如果在您的环境中启用了基于角色的访问控制 (RBAC)，则配置交换机端口锁定功能的用户必须使用至少拥有池操作员或池管理员角色的帐户进行登录。如果在您的环境中未启用 RBAC，则用户必须使用池主服务器的 root 帐户进行登录。
- 运行交换机端口锁定命令时，网络可以联机或脱机。
- 在 Windows 来宾系统中，断开连接的网络图标仅在 Citrix VM Tools 安装在来宾系统中时显示。

### 注意

如果没有任何交换机端口锁定配置，VIF 将被设为 “network\_default”，网络被设为 “unlocked”。

在环境中使用 vSwitch Controller 和其他第三方控制器时，配置交换机端口锁定不受支持。

交换机端口锁定不阻止云租户：

- 在另一个租户/用户上执行 IP 层攻击。但是，如果它们尝试使用以下手段执行 IP 层攻击并且配置交换机端口锁定：a) 模拟云中的另一个租户或用户，或者 b) 启动对面向另一用户的流量的拦截。
- 耗尽网络资源。
- 通过正常的交换机阻塞行为接收一些面向其他虚拟机的流量（对于广播 MAC 地址或未知目标 MAC 地址）。

同样，交换机端口锁定不限制 VM 向哪里发送流量。

### 实施说明

可以使用命令行或 Citrix Hypervisor API 实施交换机端口锁定功能。但是，在注重自动化的大环境中，最典型的实施方法可能是使用 API。

### 示例

本节提供了交换机端口锁定如何阻止特定类型的攻击的示例。在这些示例中，VM-c 是一个敌对租户（租户 C）租用和用于攻击的虚拟机。VM-a 和 VM-b 是非攻击性租户租用的虚拟机。

示例 1：交换机端口锁定如何阻止 **ARP** 欺骗防御：

ARP 欺骗用于指示攻击者尝试将自己的 MAC 地址与另一节点的 IP 地址相关联。ARP 欺骗可能会导致改为将节点的流量发送给攻击者。为实现此目标，攻击者会将假冒的（具有欺骗性的）ARP 消息发送给以太网 LAN。

情景：

虚拟机 A (VM-a) 想通过将 IP 流量寻址到虚拟机 B (VM-b)，将 IP 流量从 VM-a 发送到 VM-b。虚拟机 C 的所有者希望使用 ARP 欺骗将其 VM 伪装成 VM-c，而其 VM 实际为 VM-b。

1. VM-c 将推测性 ARP 答复流发送到 VM-a。这些 ARP 答复要求将答复中的 MAC 地址 (c\_MAC) 与 IP 地址 b\_IP 项关联。

结果：因为管理员启用了交换机端口锁定，所以这些数据包全部被丢弃，因为启用交换机端口锁定可以防止模拟。

2. VM-b 将 ARP 答复发送到 VM-a，要求将答复 (b\_MAC) 中的 MAC 地址与 IP 地址 b\_IP 关联起来。

结果：VM-a 接收 VM-b 的 ARP 响应。

**示例 2：IP 欺骗防御：**

IP 地址欺骗是指通过使用伪造的源 IP 地址创建 Internet 协议 (IP) 数据包来隐藏数据包身份的过程。

情景：

租户 C 正在尝试使用其主机 Host-C 在远程系统中执行拒绝服务攻击以隐瞒其身份。

**尝试 1：**

租户 C 将 Host-C 的 IP 地址和 MAC 地址设为 VM-a 的 IP 和 MAC 地址 (a\_IP 和 a\_MAC)。租户 C 指示 Host-C 将 IP 流量发送到远程系统。

结果：Host-C 数据包被丢弃。这是因为管理员启用了交换机端口锁定。Host-C 数据包被丢弃，因为启用交换机端口锁定可以防止模拟。

**尝试 2：**

租户 C 将 Host-C 的 IP 地址设置为 VM-a 的 IP 地址 (a\_IP)，并保存其原始 c\_MAC。

租户 C 指示 Host-C 将 IP 流量发送到远程系统。

结果：Host-C 数据包被丢弃。这是因为管理员启用了防止模拟的交换机端口锁定。

**示例 3：Web 托管：**

情景：

Alice 是一名基础结构管理员。

租户 B 是她的租户之一，正在从其 VM VM-b 托管多个 Web 站点。每个 Web 站点都需要一个在同一虚拟网络接口 (VIF) 上托管的不同 IP 地址。

Alice 将 Host-B 的 VIF 重新配置为锁定到单一 MAC 和多个 IP 地址。

## 交换机端口锁定的工作原理

交换机端口锁定功能可以让您在一个或两个层面上控制数据包过滤：

- **VIF 层。**您在 VIF 上配置的设置可以确定数据包的过滤方式。您可以设置 VIF，使其阻止 VM 发送任何流量，限制 VIF，以便它只能使用分配给它的 IP 地址发送流量，或者允许 VM 将流量发送到连接 VIF 的网络上的任何 IP 地址。
- **网络级别。**Citrix Hypervisor 网络可以确定数据包的过滤方式。当 VIF 的锁定模式设置为 `network_default` 时，将引用网络级别锁定设置以确定允许传输的流量。

无论您使用哪个网络连接堆栈，此功能的运行方式都相同。但是，如以下各节的详细描述一样，Linux 桥接不完全支持 IPv6 中的交换机端口锁定。

## VIF 锁定模式状态

Citrix Hypervisor 交换机端口锁定功能提供一种锁定模式，让您将 VIF 配置为四种不同的状态。这些状态仅在 VIF 插入正在运行的虚拟机中时适用。

![ 此图显示将网络锁定模式设置为已解除锁定和配置 VIF 状态时，三种不同的 VIF 锁定模式状态的行为方式。在第一张图中，VIF 状态被设为默认设置，因此，不过滤来自 VM 的流量。VIF 不发送或接收任何数据包，因为锁定模式在第二张图中设置为 `disabled`。在第三张图中，VIF 状态设置为 `locked`。这意味着如果这些数据包包含正确的 MAC 和 IP 地址，VIF 将只能发送数据包。 ](/zh-cn/citrix-hypervisor/media/vif-switch-port-locking-modes.png)

- **Network\_default。**当 VIF 的状态设置为 `network_default` 时，Citrix Hypervisor 将使用网络的 `default-locking-mode` 参数来确定是否以及如何过滤流经 VIF 的数据包。此行为因相关联的网络将网络默认锁定模式参数设为禁用还是已解除锁定而异。

-`default-locking-mode=disabled`，Citrix Hypervisor 应用过滤规则，以便 VIF 丢弃所有流量。

-`default-locking-mode=unlocked`，Citrix Hypervisor 删除所有与 VIF 相关联的过滤规则。默认情况下，默认锁定模式参数设置为 `unlocked`。

有关 `default-locking-mode` 参数的信息，请参阅[网络命令](#)。

网络的默认锁定模式不会影响锁定状态未设置为 `network_default` 的已连接 VIF。

注意：

无法更改连接了活动 VIF 的网络的 `default-locking-mode`。

- **已锁定。**Citrix Hypervisor 应用过滤规则，以便仅允许通过 VIF 向外发送向指定 MAC 和 IP 地址发送的流量或从指定 MAC 和 IP 地址发送的流量。在此模式下，如果不指定 IP 地址，VM 将无法在网络中通过该 VIF 发送任何流量。

要指定 VIF 将接受来自哪些 IP 地址的流量，请通过使用 `ipv4_allowed` 或 `ipv6_allowed` 参数使用 IPv4 或 IPv6 地址。但是，如果您配置了 Linux 桥接，则无需键入 IPv6 地址。

Citrix Hypervisor 允许您在 Linux 桥接处于活动状态时键入 IPv6 地址。但是，Citrix Hypervisor 无法根据键入的 IPv6 地址进行过滤。原因是 Linux 桥接没有用于过滤邻居发现协议 (Neighbor Discovery Protocol,

NDP) 数据包的模块。因此，无法实施完整的保护，并且来宾能够通过伪造 NDP 数据包来模拟另一个来宾。因此，如果指定了一个 IPv6 地址，Citrix Hypervisor 将允许所有 IPv6 流量流经 VIF。如果未指定任何 IPv6 地址，Citrix Hypervisor 将不允许任何 IPv6 流量流经 VIF。

- 未锁定。所有网络流量都可以经过 VIF。也就是说，不对任何传入 VIF 或从 VIF 传出的流量应用过滤器。
- 已禁用。不允许任何流量流经 VIF。（也就是说，Citrix Hypervisor 应用过滤规则，使 VIF 丢弃所有流量。）

### 配置交换机端口锁定

本节提供三种不同的过程：

- 限制 VIF 使用特定 IP 地址
- 向现有的受限列表中添加 IP 地址例如，在 VM 运行过程中并且连接到网络时向 VIF 中添加 IP 地址（例如，如果临时让网络处于脱机状态）。
- 从现有的受限列表删除 IP 地址

如果 VIF 的锁定模式设置为 `locked`，则只能使用在 `ipv4-allowed` 或 `ipv6-allowed` 参数中指定的地址。

因为在某些相对罕见的情况下，VIF 可能有多个 IP 地址，所以可以为 VIF 指定多个 IP 地址。

可以在插入 VIF（或启动 VM）之前或之后执行这些过程。

运行以下命令，将默认锁定模式更改为已锁定（如果尚未使用该模式）：

```
1 xe vif-param-set uuid=vif-uuid locking-mode=locked
```

`vif-uuid` 表示您希望允许发送流量的 VIF 的 UUID。要获取 UUID，请在主机上运行 `xe vif-list` 命令。`vm-uuid` 指示显示哪个虚拟机的信息。设备 ID 指示 VIF 的设备编号。

运行 `vif-param-set` 命令，指定虚拟机可以从哪些 IP 地址发送流量。执行以下一项或多项操作：

- 指定一个或多个 IPv4 IP 地址目标。例如：

```
1 xe vif-param-set uuid=vif-uuid ipv4-allowed=comma separated list
of ipv4-addresses
```

- 指定一个或多个 IPv6 IP 地址目标。例如：

```
1 xe vif-param-set uuid=vif-uuid ipv6-allowed=comma separated list
of ipv6-addresses
```

可以指定多个 IP 地址，使用逗号将其隔开，如上例所示。

执行该过程以限制 VIF 使用特定 IP 地址后，可以添加一个或多个 VIF 能够使用的 IP 地址。

运行 `vif-param-add` 命令，向现有列表中添加 IP 地址。执行以下一项或多项操作：

- 指定 IPv4 IP 地址。例如：

```
1 xe vif-param-add uuid=vif-uuid ipv4-allowed=comma separated list
of ipv4-addresses
```

- 指定 IPv6 IP 地址。例如：

```
1 xe vif-param-add uuid=vif-uuid ipv6-allowed=comma separated list
of ipv6-addresses
```

如果限制 VIF 使用两个或更多 IP 地址，可以从列表中删除其中一个 IP 地址。

运行 `vif-param-remove` 命令，从现有列表中删除 IP 地址。执行以下一项或多项操作：

- 指定要删除的 IPv4 IP 地址。例如：

```
1 xe vif-param-remove uuid=vif-uuid ipv4-allowed=comma separated
list of ipv4-addresses
```

- 指定要删除的 IPv6 IP 地址。例如：

```
1 xe vif-param-remove uuid=vif-uuid ipv6-allowed=comma separated
list of ipv6-addresses
```

#### 阻止虚拟机从特定网络发送或接收流量

以下过程阻止虚拟机通过特定 VIF 进行通信。由于 VIF 连接到特定的 Citrix Hypervisor 网络，因此，可以使用此过程阻止虚拟机从特定网络发送或接收任何流量。这可以比禁用整个网络提供更精细的控制级别。

如果使用 CLI 命令，则不需要拔出 VIF 即可设置 VIF 的锁定模式。此命令在 VIF 运行过程中更改过滤规则。在这种情况下，网络连接仍显示为存在，但是，VIF 会丢弃 VM 尝试发送的任何数据包。

#### 提示：

要查找 VIF 的 UUID，请在主机上运行 `xe vif-list` 命令。设备 ID 指示 VIF 的设备编号。

要阻止 VM 接收流量，请禁用已连接到您希望阻止 VM 从中接收流量的网络的 VIF：

```
1 xe vif-param-set uuid=vif-uuid locking-mode=disabled
```

此外，还可以通过在 VM 的“网络连接”选项卡中选择虚拟网络接口并单击“取消激活”，在 XenCenter 中禁用 VIF。

#### 删除 VIF 对 IP 地址的限制

要还原到默认（原始）锁定模式状态，请使用以下过程。默认情况下，创建 VIF 时，Citrix Hypervisor 可以对其进行配置，不限制它使用特定 IP 地址。

要将 VIF 还原到未锁定状态，请将 VIF 的默认锁定模式更改为 `unlocked`。如果尚未使用该模式，请运行以下命令：

```
1 xe vif-param-set uuid=vif_uuid locking-mode=unlocked
```

### 简化云中的 VIF 锁定模式配置

不对每个 VIF 运行 VIF 锁定模式命令，可以确保所有 VIF 在默认情况下禁用。为此，必须在网络级别更改数据包过滤功能。更改数据包过滤功能会导致 Citrix Hypervisor 网络确定数据包的过滤方式，如上一部分交换机端口锁定的工作原理中所述。

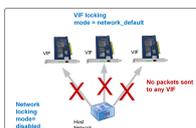
具体而言，网络的 **default-locking-mode** 设置可以确定采用默认设置的新 VIF 的行为方式。只要 VIF 的 **locking-mode** 设置为 **default**，VIF 就会引用网络锁定模式 (**default-locking-mode**) 以确定是否以及如何过滤流经 VIF 的数据包：

- 未锁定。当网络 **default-locking-mode** 参数设置为 **unlocked** 时，Citrix Hypervisor 可以让 VM 将流量发送到 VIF 连接到的网络上的任何 IP 地址。
- 已禁用。当 **default-locking-mode** 参数设置为 **disabled** 时，Citrix Hypervisor 将应用过滤规则，以便 VIF 丢弃所有流量。

默认情况下，在 XenCenter 中创建并且使用 CLI 的所有网络的 **default-locking-mode** 设置为 **unlocked**。

通过将 VIF 的锁定模式设置为其默认设置 (**network\_default**)，可以（在网络级别）为所有连接特定网络的新建 VIF 创建基础默认配置。

此图显示，当 VIF 的 **locking-mode** 设置为其默认设置 (**network\_default**) 时，VIF 如何使用网络 **default-locking-mode** 确定其行为。



例如，默认情况下，创建的 VIF 的 **locking-mode** 设置为 **network\_default**。如果将网络的 **default-locking-mode** 设置为 **disabled**，则尚未为其配置锁定模式的任何新 VIF 都将处于禁用状态。VIF 将保持禁用状态，直至您 (a) 更改各个 VIF 的 **locking-mode** 参数，或者 (b) 将 VIF 的 **locking-mode** 明确设置为 **unlocked**。这在您足够信任某个特定的 VM，完全不希望过滤其流量时非常有用。

更改网络的默认锁定模式设置：

创建网络后，运行以下命令，更改默认锁定模式：

```
1 xe network-param-set uuid=network-uuid default-locking-mode=[unlocked | disabled]
```

#### 注意：

要获取网络的 UUID，请运行 `xe network-list` 命令。此命令在您运行它的主机上显示所有网络的 UUID。

查看网络的默认锁定模式设置：

运行以下命令之一：

```
1 xe network-param-get uuid=network-uuid param-name=default-locking-mode
```

或

```
1 xe network-list uuid=network-uuid params=default-locking-mode
```

使用网络设置过滤 **VIF** 通信

以下过程指示虚拟机上的 VIF 在 Citrix Hypervisor 网络本身上使用该网络的 **default-locking-mode** 设置来确定如何过滤流量。

1. 运行以下命令，将 VIF 锁定状态更改为 `network_default`（如果尚未使用该模式）：

```
1 xe vif-param-set uuid=vif_uuid locking-mode=network_default
```

2. 运行以下命令，将默认锁定模式更改为 `unlocked`（如果尚未使用该模式）：

```
1 xe network-param-set uuid=network-uuid default-locking-mode=  
unlocked
```

## 网络连接故障排除

June 4, 2019

如果在配置网络连接时遇到问题，请先确保您未曾直接更改过任何控制域 `ifcfg-*` 文件。控制域主机代理直接管理 `ifcfg` 文件，所做的任何更改都将被覆盖。

### 诊断网络损坏

某些网卡型号在负载不足或启用了某些优化的情况下需要使用供应商提供的固件升级才能够稳定运行。如果看到传输到 VM 的流量损坏，请先尝试从您的供应商处获取最新的固件，然后应用 BIOS 更新。

如果问题仍然存在，则可以使用 CLI 禁用物理接口上的接收或传输卸载优化。

警告：

禁用接收或传输卸载优化会导致性能降低以及 CPU 使用率增加。

首先，确定物理接口的 UUID。可以根据 `device` 字段进行过滤，如下所示：

```
1 xe pif-list device=eth0
```

然后，在 PIF 上设置以下参数以禁用 TX 卸载：

```
1 xe pif-param-set uuid=pif_uuid other-config:ethtool-tx=off
```

最后，重新连接 PIF 或重新启动主机以使更改生效。

## 紧急网络重置

错误的网络连接设置会导致网络连接断开。没有网络连接时，Citrix Hypervisor 服务器会变得无法通过 XenCenter 或远程 SSH 访问。紧急网络重置可以提供简单的主机网络连接恢复和重置机制。

可以在 CLI 中使用 `xe-reset-networking` 命令以及在 `xsconsole` 的“网络和管理接口”部分中获取紧急网络重置功能。

导致网络连接断开的错误设置包括重命名网络接口、创建绑定或 VLAN，或者更改管理接口时发生的错误。例如，键入错误的 IP 地址。您可能还希望在以下情况下运行此实用程序：

- 执行滚动池升级时，手动升级、修补程序安装或驱动程序安装会导致网络连接断开时，或者
- 如果池主服务器或资源池中的主机无法联系其他主机。

请仅在紧急情况下使用 `xe-reset-networking` 实用程序，因为该实用程序将删除所有与主机相关联的 PIF、绑定、VLAN 和通道的配置。保存来宾系统网络和 VIF。作为该实用程序的一部分，VM 将强制关闭。运行此命令之前，请尽可能彻底关闭 VM。应用重置之前，可以更改管理接口，并指定可以使用的 IP 配置（DHCP 还是静态协议）。

如果池主服务器要求网络重置，请先在池主服务器上重置网络，然后对池成员应用网络重置。对池中的所有剩余主机应用网络重置可确保池的网络连接配置保持同质。网络同质化是实时迁移的重要因素。

### 注意：

如果池主服务器的 IP 地址（管理接口）因网络重置或 `xe host-management-reconfigure` 而发生改变，则必须对池中的其他主机应用网络重置命令。这是为了确保池成员能够重新连接到采用新 IP 地址的池主服务器。在此情况下，必须指定池主服务器的 IP 地址。

启用了高可用性时不支持网络重置。要在这种情况下重置网络配置，必须先手动禁用高可用性，然后再运行网络重置命令。

## 验证网络重置

指定要在网络重置后使用的配置模式之后，`xsconsole` 和 CLI 将显示将在主机重新启动后应用的设置。这是在应用紧急网络重置命令之前进行修改的最后机会。重新启动后，可以在 XenCenter 和 `xsconsole` 中验证新网络配置。在 XenCenter 中，选中主机，单击网络连接选项卡可查看新网络配置。在 `xsconsole` 中，此信息显示在“网络和管理接口”部分。

**注意：**

请对其他池成员应用紧急网络重置，以便从池主服务器的新配置复制绑定、VLAN 或通道。

**使用 CLI 执行网络重置**

下表显示了可以通过运行 `xe-reset-networking` 命令使用的可选参数。

**警告：**

用户负责确保参数对 `xe-reset-networking` 命令的有效性以及仔细检查参数。如果指定了无效参数，网络连接和配置将丢失。在这种情况下，我们建议您重新运行命令 `xe-reset-networking`，而不使用任何参数。

必须首先在池主服务器上重置整个池的网络连接配置，然后对池中的所有剩余主机应用网络重置。

参数	必需/可选	说明
<code>-m</code> 、 <code>-master</code>	可选	池主服务器的管理接口的 IP 地址。默认为已知的最新池主服务器 IP 地址。
<code>-device</code>	可选	管理接口的设备名称。默认为在安装期间指定的设备名称。
<code>-mode=static</code>	可选	启用下列四个网络连接参数，用于管理接口的静态 IP 配置。如果不指定，则将使用 DHCP 配置网络连接。
<code>-ip</code>	如果模式为静态，则为必需	主机管理接口的 IP 地址。仅当模式为静态时有效。
<code>-netmask</code>	如果模式为静态，则为必需	管理接口的网络掩码。仅当模式为静态时有效。
<code>-gateway</code>	可选	管理接口的网关。仅当模式为静态时有效。
<code>-dns</code>	可选	管理接口的 DNS 服务器。仅当模式为静态时有效。
<code>-vlan</code>	可选	管理接口的 VLAN 标记。默认设置为在安装过程中指定的 VLAN 标记。

**池主服务器命令行示例**

可在池主服务器上应用的命令示例：

重置 DHCP 配置的网络连接：

```
1 xe-reset-networking
```

重置静态 IP 配置的网络连接：

```
1 xe-reset-networking --mode= static --ip=ip-address \  
2   --netmask=netmask --gateway=gateway \  
3   --dns=dns
```

如果另一接口在初始设置后变为管理接口，则重置 DHCP 配置的网络连接：

```
1 xe-reset-networking --device=device-name
```

如果另一接口在初始设置后变为管理接口，则重置静态 IP 配置的网络连接：

```
1 xe-reset-networking --device=device-name --mode=static \  
2   --ip=ip-address --netmask=netmask \  
3   --gateway=gateway --dns=dns
```

要在 VLAN 上重置管理接口的网络连接，请执行以下操作：

```
1 xe-reset-networking --vlan=VLAN TAG
```

注意：

`reset-network` 命令还可以与 IP 配置设置结合使用。

池成员命令行示例

所有上述示例也适用于池成员。除此之外，可以指定池主服务器的 IP 地址（如果已更改，则需要指定。）

重置 DHCP 配置的网络连接：

```
1 xe-reset-networking
```

在池主服务器的 IP 地址已更改的情况下重置 DHCP 的网络连接：

```
1 xe-reset-networking --master=master-ip-address
```

假设池主服务器的 IP 地址未更改，重置静态 IP 配置的网络连接：

```
1 xe-reset-networking --mode=static --ip=ip-address --netmask=netmask \  
2   --gateway=gateway --dns=dns
```

在管理接口和池主服务器的 IP 地址已在初始设置后发生变化的情况下重置 DHCP 配置的网络连接：

```
1 xe-reset-networking --device=device-name --master=master-ip-address
```

## 存储

July 10, 2019

本部分内容介绍如何将物理存储硬件映射到虚拟机 (VM)，以及管理 API 用来执行存储相关任务的软件对象。有关受支持的每种存储类型的详细信息部分中包括以下信息：

- 使用 CLI 通过类型特定的设备配置选项为 VM 创建存储的过程
- 生成用于备份的快照
- 管理存储的最佳做法
- 虚拟磁盘 QoS (服务质量) 设置

## 存储库 (SR)

存储库 (SR) 是一个特定存储目标，用于存储虚拟机 (VM) 虚拟磁盘映像 (VDI)。VDI 是一个表示虚拟硬盘驱动器 (HDD) 的存储抽象。

SR 非常灵活，对以下驱动器具有内置支持：

本地连接的驱动器：

- IDE
- SATA
- SCSI
- SAS

远程连接的驱动器：

- iSCSI
- NFS
- SAS
- 光纤通道

SR 和 VDI 抽象允许在支持高级存储功能的存储目标上提供这些功能。例如，诸如精简预配、VDI 快照和快速克隆等高级功能。对于直接不支持高级操作的存储子系统，将提供用于实现这些功能的软件堆栈。此软件堆栈基于 Microsoft 的虚拟硬盘 (VHD) 规范。

SR 命令提供用于创建、销毁、克隆、连接、查找它们包含的各个 VDI 及调整这些 VDI 大小的操作。

存储库是一个永久性的磁盘上数据结构。对于使用基础块设备的 SR 类型，创建 SR 的过程将包括清除指定存储目标上的所有现有数据。其他存储类型（例如 NFS）将在与现有 SR 平行的存储阵列上创建一个容器。

每个 Citrix Hypervisor 服务器可以同时使用多个 SR 和不同的 SR 类型。可以在主机之间共享这些 SR，也可以将其专用于特定主机。共享存储会加入一个已定义的资源池，并由该池内的多台主机共用。共享 SR 必须可由池中的每台主机通过网络访问。单个资源池中的所有服务器必须至少有一个共用的共享 SR。共享存储不能在多个池之间共享。

用于管理存储库的 CLI 操作在[SR 命令](#)中介绍。

### 虚拟磁盘映像 (VDI)

虚拟磁盘映像 (VDI) 是一个表示虚拟硬盘驱动器 (HDD) 的存储抽象。VDI 是 Citrix Hypervisor 中的虚拟化存储的基础单元。VDI 是磁盘上持久对象，独立于 Citrix Hypervisor 服务器而存在。用于管理 VDI 的 CLI 操作在[VDI 命令](#)中说明。数据在磁盘上的表现形式因 SR 类型而异。每个 SR 的独立存储插件接口（称为 SM API）负责管理该数据。

### 物理块设备 (PBD)

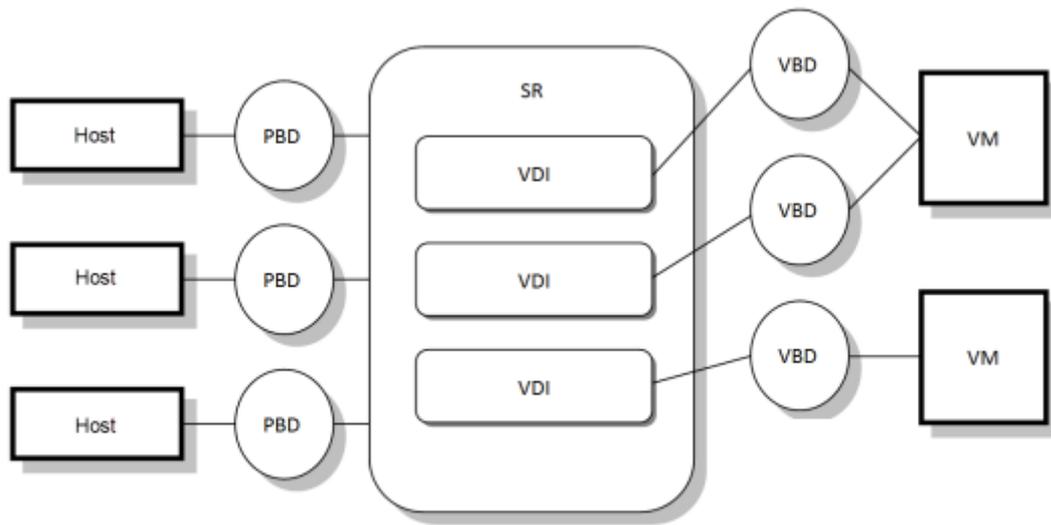
物理块设备表示物理服务器与连接的 SR 之间的接口。PBD 是连接器对象，允许将给定 SR 映射到主机。PBD 存储一些设备配置字段，用于与给定的存储目标进行连接和交互。例如，NFS 设备配置包括 NFS 服务器的 IP 地址和 Citrix Hypervisor 服务器装载的关联路径。PBD 对象管理给定 SR 与给定 Citrix Hypervisor 服务器之间的运行时连接。与 PBD 相关的 CLI 操作在[PBD 命令](#)中介绍。

### 虚拟块设备 (VBD)

虚拟块设备是连接器对象（与上述的 PBD 类似），可用于在 VDI 和 VM 之间进行映射。除了提供用于将 VDI 连接到 VM 的机制外，VBD 还允许微调与给定 VDI 的 QoS（服务质量）和统计信息以及是否可以引导 VDI 有关的参数。与 VBD 相关的 CLI 操作在[VBD 命令](#)中介绍。

### 存储对象摘要

下图概括说明了目前提供的存储对象之间的关系：



## 虚拟磁盘数据格式

一般来说，针对 VDI 的物理存储的映射包括以下几种类型：

1. LUN 上基于逻辑卷的 VHD：默认的基于 Citrix Hypervisor 块的存储将在磁盘上插入逻辑卷管理器。此磁盘是指本地连接的设备 (LVM) 或通过光纤通道、iSCSI 或 SAS 连接了 SAN 的 LUN。VDI 表示为卷管理器中的卷并以 VHD 格式保存，以支持快照和克隆上引用节点的精简预配。
2. LUN 上基于文件的 QCOW2：VM 映像是通过 iSCSI 软件发起程序或硬件 HBA 连接的 LUN 上的 GFS2 共享磁盘文件系统中存储为精简预配的 QCOW2 格式文件。
3. 文件系统中基于文件的 VHD：VM 映像在本机非共享文件系统 (EXT 类型的 SR) 或共享 NFS 目标 (NFS 类型的 SR) 中存储为精简预配的 VHD 格式文件。

## VDI 类型

对于大多数 SR 类型，将创建 VHD 格式的 VDI。在创建 VDI 时可以选择使用原始格式。此选项只能通过使用 xe CLI 来指定。对于 GFS2 SR，将创建 QCOW2 VDI。

要检查 VDI 是否通过 `type=raw` 创建，请检查其 `sm-config` 映射。`sr-param-list` 和 `vdi-param-list` 命令可分别用于实现此目的。

## 使用 xe CLI 创建原始虚拟磁盘

1. 根据您希望放置虚拟磁盘的 SR 的 UUID，运行以下命令创建一个 VDI：

```

1 xe vdi-create sr-uuid=sr-uuid type=user virtual-size=virtual-size
  \
2     name-label=VDI name sm-config:type=raw

```

2. 将新虚拟磁盘连接到 VM。请使用 VM 中的磁盘工具进行分区和格式化，否则，请使用新磁盘。可以使用 `vbd-create` 命令创建 VBD，以将该虚拟磁盘映射到 VM。

### 在 VDI 格式之间转换

原始和 VHD 格式之间不能实现直接转换。相反，可以创建 VDI（如上所述的原始 VDI，或者 VHD），然后将数据从现有卷复制到该 VDI。使用 xe CLI 可确保新 VDI 的虚拟大小至少与从中复制的 VDI 大小相同。可以通过检查其 `virtual-size` 字段来执行此操作，例如使用 `vdi-param-list` 命令。然后将这一新 VDI 连接到 VM，并使用 VM 中的首选工具来直接执行数据的块复制。例如，Windows 中的标准磁盘管理工具或 Linux 中的 `dd` 命令。如果新卷为 VHD 卷，请使用可避免向磁盘中写入空扇区的工具。此操作可确保在基础存储库中以最佳方式使用空间。基于文件的复制方法可能更为合适。

### 基于 VHD 和基于 QCOW2 的 VDI

可以链接 VHD 和 QCOW2 映像，从而允许两个 VDI 共享通用数据。如果克隆基于 VHD 或 QCOW2 支持的 VM，生成的 VM 将共享克隆时的通用磁盘数据。每个 VM 将在 VDI 的单独写入时复制版本中继续进行各自的更改。此功能允许从模板快速克隆此类 VM，便于极快地预配和部署新 VM。

由于不断克隆 VM 及其关联的 VDI，因此这将创建链接的 VDI 的树形结构。删除链中的一个 VDI 时，Citrix Hypervisor 会合理化链中的其他 VDI 以删除不必要的 VDI。此合并过程异步运行。回收的磁盘空间量和执行此过程所花费的时间取决于 VDI 的大小和共享数据量。

VHD 和 QCOW2 格式都支持精简预配。当 VM 将数据写入到磁盘时，映像文件将自动在细粒度块中扩展。对于基于文件的 VHD 和基于 GFS2 的 QCOW2，VM 映像文件仅在物理存储中占用所需的空間，此方法将带来极大的好处。使用基于 LVM 的 VHD 时，基础逻辑卷容器必须与 VDI 的虚拟大小相同。但是，出现快照或克隆时，将回收基础写入时复制实例磁盘上的未使用的空间。两种行为之间的差异描述如下：

- 对于基于 LVM 的 VHD 映像，链中的差异磁盘节点仅占用已写入到磁盘的数据量。但是，叶节点（VDI 克隆）则完全扩大到磁盘的虚拟大小。快照叶节点（VDI 快照）在未使用时保持压缩状态，并且可以附加只读存储以保持压缩分配。附加读写存储的快照节点将在附加后完全扩大，在分离后压缩。
- 对于基于文件的 VHD 和基于 GFS2 的 QCOW2 映像，所有节点都仅占用已写入的数据量。叶节点文件在其主动被写入的过程中将扩大以容纳数据。如果为 VM 分配 100 GB 的 VDI 并且安装了操作系统，VDI 文件的物理大小仅是磁盘上的操作系统数据的大小加上一些次要元数据开销。

基于单个 VHD 或 QCOW2 模板克隆 VM 时，每个子 VM 会形成一个链，其中新更改将写入新 VM。旧块将直接从父模板中读取。如果将新 VM 转化为深层模板并克隆更多 VM，生成的链会导致性能降级。Citrix Hypervisor 支持的最大链长度为 30。如果没有充分的理由，请不要接近此限制。如有疑问，请使用 XenCenter 或使用 `vm-copy` 命令“复制”VM，这会将链长度重置回 0。

## 合并时 VHD 特定的注意事项

只有一个合并过程始终对 SR 保持活动状态。此进程线程在 SR 主服务器主机上运行。

如果有重要的 VM 在池的主服务器上运行，则可以执行以下步骤来缓解 I/O 偶尔缓慢的情况：

- 将 VM 迁移到 SR 主节点以外的主机。
- 将磁盘 I/O 优先级设置为较高的级别，并调整调度程序。有关详细信息，请参阅[虚拟磁盘 QoS 设置](#)。

## 存储库格式

September 5, 2019

可以在 XenCenter 中使用新建存储库向导创建存储库。此向导将引导您完成配置步骤。或者，请使用 CLI 和 `sr-create` 命令。`sr-create` 命令将在存储基底中创建一个 SR（可能会销毁任何现有数据）。还会创建 SR API 对象以及相应的 PBD 记录，从而使 VM 能够使用存储。成功创建 SR 后，自动插入 PBD。如果已设置 SR `shared=true` 标志，则将创建 PBD 记录并为资源池中的每个 Citrix Hypervisor 插入该记录。

如果要为基于 IP 的存储（iSCSI 或 NFS）创建 SR，可以将下列 NIC 之一配置为存储网络：处理管理流量的 NIC 或面向存储流量的新 NIC。要为 NIC 分配 IP 地址，请参阅[配置专用存储 NIC](#)。

所有 Citrix Hypervisor SR 类型都支持调整 VDI 的大小、快速克隆和快照。基于 LVM SR 类型（本地、iSCSI 或 HBA）的 SR 提供用于快照和隐藏父节点的精简预配。其他 SR 类型（EXT3、NFS、GFS2）支持完整的精简预配，包括活动虚拟磁盘的精简预配。

### 警告：

当 VHD VDI 未连接到 VM 时，例如针对 VDI 快照，默认情况下将以精简预配方式进行存储。尝试重新连接 VDI 时，请确保有足够的磁盘空间用于对 VDI 进行密集预配。VDI 克隆是密集预配的。

支持的最大 VDI 大小为：

存储库格式	最大 VDI 大小
EXT3	2 TiB
LVM	2 TiB
NFS	2 TiB
LVMoFCOE	2 TiB
LVMoiSCSI	2 TiB
LVMoHBA	2 TiB
GFS2（使用 iSCSI 或 HBA）	16 TiB

## 本地 LVM

本地 LVM 类型表示本地连接的卷组中的磁盘。

默认情况下，Citrix Hypervisor 使用安装它的物理主机的本地磁盘。Linux 逻辑卷管理器 (LVM) 用于管理 VM 存储。在指定大小的 LVM 逻辑卷中，VDI 采用 VHD 格式实施。

### LVM 性能注意事项

快照和快速克隆功能（用于基于 LVM 的 SR）具有固有的性能开销。需要最佳性能时，Citrix Hypervisor 支持创建原始格式以及默认 VHD 格式的 VDI。原始 VDI 不支持 Citrix Hypervisor 快照功能。

使用默认 Windows VSS 提供程序的不可传送快照适用于所有类型的 VDI。

#### 警告：

请勿尝试为连接了 `type=raw` 磁盘的 VM 生成快照。此操作可能会导致创建部分快照。这种情况下，可以通过检查 `snapshot-of` 字段确定孤立快照 VDI，然后删除这些快照。

## 创建本地 LVM SR

默认情况下，在主机安装期间创建 LVM SR。

LVM SR 的 Device-config 参数为：

参数名称	说明	是否必需
设备	用于 SR 的本地主机上的设备名称	是

要在 `/dev/sdb` 上创建本地 LVM SR，请使用以下命令。

```

1  xe sr-create host-uuid=valid_uuid content-type=user \
2  name-label="Example Local LVM SR" shared=false \
3  device-config:device=/dev/sdb type=lvm

```

## 本地 EXT3

使用 EXT3 在本地存储上启用精简预配。但是，默认存储库类型为 LVM，因为它可以提供一致的写入性能，防止存储过度使用。如果使用 EXT3，您可能在以下情况下看到性能下降：

- 执行 VM 生命周期操作时，例如创建和挂起/恢复 VM
- 在 VM 内部创建大型文件时

必须使用 Citrix Hypervisor CLI 配置本地磁盘 EXT SR。

## 创建本地 EXT3 SR (ext)

ext SR 的 Device-config 参数:

参数名称	说明	是否必需
设备	用于 SR 的本地主机上的设备名称	是

要在 `/dev/sdb` 上创建本地 ext SR，请使用以下命令：

```
1 xe sr-create host-uuid=valid_uuid content-type=user \
2   name-label="Example Local EXT3 SR" shared=false \
3   device-config:device=/dev/sdb type=ext
```

## udev

udev 类型表示插入的设备使用 udev 设备管理器作为 VDI。

Citrix Hypervisor 具有两个代表可移动存储的 udev 类型的 SR。一个用于 Citrix Hypervisor 服务器的物理 CD 或 DVD-ROM 驱动器中的 CD 或 DVD 磁盘。另一个用于插入到 Citrix Hypervisor 服务器的 USB 端口的 USB 设备。插入磁盘或 U 盘，代表介质的 VDI 出现；移除磁盘或 U 盘，VDI 消失。

## ISO

ISO 类型处理以 ISO 格式文件存储的 CD 映像。此 SR 类型在创建共享 ISO 库时十分有用。对于用于存储 ISO 库的存储库，必须将 `content-type` 参数设置为 `iso`。

例如：

```
1 xe sr-create host-uuid=valid_uuid content-type=iso \
2   type=iso name-label="Example ISO SR" \
3   device-config:location=nfs server:path
```

我们建议您使用 SMB 3.0 在 Windows 文件服务器上装载 ISO SR。默认选择版本 3.0，因为与 SMB 1.0 相比，该版本更加安全并且功能更加强大。但是，可以使用以下命令通过 SMB 1.0 装载 ISO SR：

```
1 xe sr-create content-type=iso type=iso shared=true device-config:
2   location=valid location
3   device-config:username=username device-config:cifspassword=
   password
   device-config:type=cifs device-config:vers=Choose either 1.0 or
   3.0 name-label="Example ISO SR"
```

**注意：**

运行 `sr-create` 命令时，可以使用 `device-config:cifspassword_secret` 参数，而不是在命令行中指定密码。有关详细信息，请参阅[机密](#)。

## 软件 iSCSI 支持

Citrix Hypervisor 支持 iSCSI LUN 上的共享 SR。由于使用 Open-iSCSI 软件 iSCSI 发起程序或使用受支持的 iSCSI 主机总线适配器 (HBA)，iSCSI 得到支持。使用 iSCSI HBA 的步骤与使用光纤通道 HBA 的步骤相同。创建基于光纤通道/以太网光纤通道/iSCSI HBA 或 SAS 的共享 LVM SR 中介绍了这两组步骤。

使用软件 iSCSI 发起程序的共享 iSCSI 支持是在 Linux 卷管理器 (LVM) 的基础上实现的。此功能提供的性能优势与本地磁盘中的 LVM VDI 提供的优势相同。使用基于软件的主机启动器的共享 iSCSI SR 能够灵活地支持使用实时迁移功能的 VM：VM 可以在资源池中的任意 Citrix Hypervisor 服务器上启动，并且可以在不会导致明显停机时间的情况下在主机间迁移。

iSCSI SR 利用在创建期间指定的整个 LUN，但不能跨多个 LUN。此外，还为数据路径初始化阶段和 LUN 检测阶段进行的客户端身份验证提供 CHAP 支持。

**注意：**

iSCSI LUN 的块大小必须为 512 字节。

## Citrix Hypervisor 服务器 iSCSI 配置

所有 iSCSI 启动程序和目标都必须具有唯一的名称，以确保可以在网络上对它们进行唯一标识。启动程序具有 iSCSI 启动程序地址，目标具有 iSCSI 目标地址。这些名称统称为 iSCSI 限定名称 (IQN)。

Citrix Hypervisor 服务器支持在主机安装期间使用随机 IQN 自动创建并配置的单个 iSCSI 启动程序。可以使用该单个启动程序并发连接到多个 iSCSI 目标。

iSCSI 目标通常提供使用 iSCSI IQN 列表的访问控制功能。您的 Citrix Hypervisor 服务器访问的所有 iSCSI 目标/LUN 必须配置为允许主机的启动器 IQN 进行访问。同样，必须将用作共享 iSCSI SR 的目标/LUN 配置为允许资源池中的所有主机 IQN 访问。

**注意：**

不提供访问控制的 iSCSI 目标通常默认为仅允许单个发起程序访问 LUN 以确保数据完整性。如果将 iSCSI LUN 用作池中的多个服务器的共享 SR，请务必为指定的 LUN 启用多发起程序访问。

在使用 iSCSI 软件启动程序时，可以通过 XenCenter 或者通过 CLI 使用以下命令来调整 Citrix Hypervisor 服务器 IQN 值：

```
1 xe host-param-set uuid=valid_host_id other-config:iscsi_iqn=new_initiator_iqn
```

**警告:**

- 每个 iSCSI 目标和发起程序都必须具有唯一的 IQN。如果使用非唯一的 IQN 标识符，则可能会导致数据损坏或 LUN 访问被拒绝。
- 不要更改连接了 iSCSI SR 的 Citrix Hypervisor 服务器 IQN。否则可能导致无法连接到新目标或现有 SR。

## 软件 FCoE 存储

软件 FCoE 提供了一个标准框架，硬件提供商可以在此框架中插入具备 FCoE 功能的 NIC，获得与基于硬件的 FCoE 相同的优势。此功能可避免使用昂贵的 HBA。

创建软件 FCoE 存储之前，请手动完成将 LUN 显示给主机所需的配置。此配置包括配置 FCoE 架构以及将 LUN 分配给 SAN 的公共全球通用名称 (PWWN)。完成此配置后，可用的 LUN 将作为 SCSI 设备装载到主机的 CNA。然后，可以使用该 SCSI 设备访问 LUN，就像它是本地连接的 SCSI 设备一样。有关配置支持 FCoE 的物理交换机和阵列的信息，请参阅供应商提供的文档。

**注意:**

可以将软件 FCoE 与 Open vSwitch 和 Linux 桥接一起用作网络后端。

## 创建软件 FCoE SR

创建软件 FCoE SR 之前，客户必须确保将具有 FCoE 功能的 NIC 连接到主机。

FCoE SR 的 Device-config 参数如下:

参数名称	说明	是否必需
SCSIid	目标 LUN 的 SCSI 总线 ID	是

运行以下命令可创建共享 FCoE SR:

```
1 xe sr-create type=lvmofcoe \  
2 name-label="FCoE SR" shared=true device-config:SCSIid=SCSI_id
```

## 硬件主机总线适配器 (HBA)

本部分内容介绍管理 SAS、光纤通道和 iSCSI HBA 所需的各种操作。

## QLogic iSCSI HBA 设置示例

有关配置 QLogic 光纤通道和 iSCSI HBA 的详细信息，请参阅 [Cavium Web 站点](#)。

将 HBA 物理安装到 Citrix Hypervisor 服务器后，请执行下列步骤配置 HBA：

1. 设置 HBA 的 IP 网络连接配置。本示例假设 DHCP 和 HBA 端口为 0。如果使用静态 IP 寻址或多端口 HBA，请指定适当的值。

```
1 /opt/QLogic_Corporation/SANsurferiCLI/iscli -ipdhcp 0
```

2. 将永久性 iSCSI 目标添加到 HBA 的端口 0。

```
1 /opt/QLogic_Corporation/SANsurferiCLI/iscli -pa 0  
iscsi_target_ip_address
```

3. 使用 `xe sr-probe` 命令强制重新扫描 HBA 控制器并显示可用的 LUN。有关详细信息，请参阅 [探测 SR](#) 或创建基于光纤通道/以太网光纤通道/ iSCSI HBA 或 SAS 的共享 LVM SR。

## 删除基于 HBA 的 SAS、FC 或 iSCSI 设备条目

### 注意：

此步骤不是必需步骤。我们建议仅在必要时由高级用户执行此步骤。

每个基于 HBA 的 LUN 都在 `/dev/disk/by-scsibus` 下具有相应的全局设备路径条目（格式为 `<SCSIid>-<adapter>:<bus>:<target>:<lun>`），并在 `/dev` 下具有标准设备路径。要删除不再用作 SR 的 LUN 的设备条目，请执行下列步骤：

1. 根据需要使用 `sr-forget` 或 `sr-destroy` 从 Citrix Hypervisor 服务器数据库中删除 SR。有关详细信息，请参阅 [删除 SR](#)。
2. 删除 SAN 中的将所需 LUN 的区域划分给所需主机的区域划分配置。
3. 使用 `sr-probe` 命令确定与要删除的 LUN 对应的 ADAPTER、BUS、TARGET 和 LUN 值。有关详细信息，请参阅 [探测 SR](#)。
4. 使用以下命令删除设备条目：

```
1 echo "1" > /sys/class/scsi_device/adapter:bus:target:lun/device/  
delete
```

### 警告：

请保证您确定要删除哪个 LUN。意外删除主机操作所需的 LUN（例如引导设备或根设备）将使该主机不可用。

## 共享 LVM 存储

共享 LVM 类型将磁盘表示为在 iSCSI (FC 或 SAS) LUN 上创建的卷组中的逻辑卷。

注意:

iSCSI LUN 的块大小必须为 512 字节。

使用软件 **iSCSI** 发起程序创建基于 **iSCSI** 的共享 **LVM SR**

LVMoiSCSI SR 的 Device-config 参数:

参数名称	说明	是否必需
target	SR 所在的 iSCSI 文件管理器的 IP 地址或主机名	是
targetIQN	SR 所在的 iSCSI 文件管理器的 IQN 目标地址	是
SCSIid	目标 LUN 的 SCSI 总线 ID	是
chapuser	用于 CHAP 身份验证的用户名	否
chappassword	用于 CHAP 身份验证的密码	否
port	在其上查询目标的网络端口号	否
usediscoverynumber	要使用的特定 iSCSI 记录索引	否
incoming_chapuser	iSCSI 过滤器用来针对主机进行身份验证的用户名	否
incoming_chappassword	iSCSI 过滤器用来针对主机进行身份验证的密码	否

要在 iSCSI 目标的特定 LUN 上创建共享 LVMoiSCSI SR, 请使用以下命令。

```

1  xe sr-create host-uuid=valid_uuid content-type=user \
2  name-label="Example shared LVM over iSCSI SR" shared=true \
3  device-config:target=target_ip= device-config:targetIQN=target_iqn=
   \
4  device-config:SCSIid=scsci_id \
5  type=lvmoiscsi

```

## 创建基于光纤通道/以太网光纤通道/ iSCSI HBA 或 SAS 的共享 LVM SR

LVMoHBA 类型的 SR 只能使用 xe CLI 或 XenCenter 创建和管理。

LVMoHBA SR 的 Device-config 参数:

参数名称	说明	是否必需
SCSIid	设备 SCSI ID	是

要创建共享 LVMoHBA SR，请在池中的每个主机上执行下列步骤：

1. 将一个或多个 LUN 中的区域划分给池中的每个 Citrix Hypervisor 服务器。此过程特定于所使用的 SAN 设备。有关详细信息，请参阅 SAN 文档。
2. 如有必要，请使用 Citrix Hypervisor 服务器中包含的 HBA CLI 来配置 HBA：
  - Emulex: `/bin/sbin/ocmanager`
  - QLogic FC: `/opt/QLogic_Corporation/SANsurferCLI`
  - QLogic iSCSI: `/opt/QLogic_Corporation/SANsurferiCLI`

有关 QLogic iSCSI HBA 配置的示例，请参阅上文中的硬件主机总线适配器 (HBA)。有关光纤通道和 iSCSI HBA 的详细信息，请参阅 [Broadcom](#) 和 [Cavium Web](#) 站点。

3. 使用 `sr-probe` 命令确定 HBA LUN 的全局设备路径。`sr-probe` 命令强制重新扫描系统中安装的 HBA，以检测其区域已划分给主机的任何新 LUN。此命令返回找到的每个 LUN 的属性列表。指定 `host-uuid` 参数以确保在所需主机上执行探测。

作为 `<path>` 属性返回的全局设备路径是池中的所有主机的公共路径。因此，创建 SR 时，此路径必须用作 `device-config:device` 参数的值。

如果提供了多个 LUN，请使用供应商、LUN 大小、LUN 序列号或 `<path>` 属性中包含的 SCSI ID 确定所需的 LUN。

```

1  xe sr-probe type=lvmohba \
2  host-uuid=1212c7b3-f333-4a8d-a6fb-80c5b79b5b31
3  Error code: SR_BACKEND_FAILURE_90
4  Error parameters: , The request is missing the device
   parameter, \
5  <?xml version="1.0" ?>
6  <Devlist>
7     <BlockDevice>
8         <path>
9             /dev/disk/by-id/scsi-360
               a9800068666949673446387665336f
10        </path>

```

```
11     <vendor>
12         HITACHI
13     </vendor>
14     <serial>
15         730157980002
16     </serial>
17     <size>
18         80530636800
19     </size>
20     <adapter>
21         4
22     </adapter>
23     <channel>
24         0
25     </channel>
26     <id>
27         4
28     </id>
29     <lun>
30         2
31     </lun>
32     <hba>
33         qla2xxx
34     </hba>
35 </BlockDevice>
36 <Adapter>
37     <host>
38         Host4
39     </host>
40     <name>
41         qla2xxx
42     </name>
43     <manufacturer>
44         QLogic HBA Driver
45     </manufacturer>
46     <id>
47         4
48     </id>
49 </Adapter>
50 </Devlist>
```

4. 在池的主服务器主机上创建 SR。指定从 `sr-probe` 中的 `<path>` 属性中返回的全局设备路径。将创建 PBD 并将其自动插入池中的每个主机。

```
1 xe sr-create host-uuid=valid_uuid \
```

```

2   content-type=user \
3   name-label="Example shared LVM over HBA SR" shared=true \
4   device-config:SCSIid=device_scsi_id type=lvmohba

```

**注意：**

可以使用 XenCenter 修复存储库功能重试 `sr-create` 操作的 PBD 创建和插入部分。创建 SR 后，如果 LUN 区域划分对于池中的一个或多个主机不正确，则此功能非常有用。更正受影响的主机的分区并使用修复存储库功能，而非删除并重新创建 SR。

**精简预配的共享 GFS2 块存储设备**

精简预配通过将磁盘存储空间分配给 VDI（因为数据会写入虚拟磁盘）来更好地利用可用存储，而非提前分配 VDI 的完整虚拟大小。通过精简预配，可以大大降低共享存储阵列上所需的空间量以及您的总体拥有成本 (TCO)。

在以下情况下，面向共享块存储进行精简预配尤其适用：

- 您希望提高空间效率。图像是稀疏的，而不是厚厚地分配。
- 您希望降低存储阵列上的每秒 I/O 操作数。GFS2 SR 是第一种支持在共享块存储上进行存储读取缓存的 SR 类型。
- 您对多个虚拟机使用公共基础映像。这样，各个 VM 的映像通常会占用更少的空间。
- 您使用快照。每个快照都是一个映像，并且每个映像现在都是稀疏的。
- 您的存储不支持 NFS，仅支持块存储。如果您的存储支持 NFS，我们建议您使用 NFS 而非 GFS2。
- 您希望创建大小大于 2 TiB 的 VDI。GFS2 SR 最大支持大小为 16 TiB 的 VDI。

共享 GFS2 类型将磁盘表示为在 iSCSI 或 HBA LUN 上创建的文件系统。GFS2 SR 上存储的 VDI 以 QCOW2 映像格式存储。

要使用共享 GFS2 存储，Citrix Hypervisor 资源池必须是群集池。请先在您的池中启用群集，然后再创建 GFS2 SR。有关详细信息，请参阅[群集池](#)。

请务必在您的群集池与 GFS2 SR 之间设置存储多路径。有关详细信息，请参阅[存储多路径](#)。

GFS2 类型的 SR 只能使用 xe CLI 或 XenCenter 创建和管理。

**限制**

共享 GFS2 存储当前具有以下限制：

- VDI 位于 GFS2 SR 上的 VM 不支持通过存储实时迁移功能迁移 VM。
- GFS2 SR 不支持 FCoE 协议。
- GFS2 SR 上不支持裁剪/取消映射。
- 性能衡量指标不适用于 GFS2 SR 以及这些 SR 上的磁盘。
- GFS2 SR 上存储的 VDI 不支持更改块跟踪功能。
- 不能将大于 2 TiB 的 VDI 导出为 VHD 或 OVA/OVF。但是，可以以 XVA 格式导出 VDI 大于 2 TiB 的 VM。

**注意：**

如果您的至少涉及一个启用了群集功能的主机的群集网络中的 IP 地址出现冲突，在 GFS2 SR 上执行的操作会卡住。在这种情况下，主机将无法进行防护。要修复此问题，请解析 IP 地址冲突。

**使用软件 iSCSI 发起程序创建基于 iSCSI 的共享 GFS2 SR**

可以使用 XenCenter 通过 iSCSI SR 创建 GFS2。有关详细信息，请参阅 XenCenter 文档中的[软件 iSCSI 存储](#)。

或者，也可以使用 xe CLI 通过 iSCSI SR 创建 GFS2。

GFS2 SR 的 Device-config 参数：

参数名称	说明	是否必需
provider	块提供程序实现。在这种情况下为 <code>iscsi</code> 。	是
target	托管此对象的 iSCSI 文件管理器的 IP 地址或主机名	是
targetIQN	托管 SR 的 iSCSI 文件管理器的 IQN 目标地址	是
SCSIid	设备 SCSI ID	是

可以使用 `xe sr-probe-ext` 命令查找要用于这些参数的值。

```
1 xe sr-probe-ext type=<type> host-uuid=<host_uuid> device-config:=<config> sm-config:=<sm_config>
```

1. 首先请运行以下命令：

```
1 xe sr-probe-ext type=gfs2 device-config:provider=iscsi
```

命令的输出会提示您提供其他参数，并在每个步骤中给出可能的值列表。

2. 重复运行该命令，每次添加新参数。
3. 当命令输出以 `The following SRs were found:` 开头时，可以使用指定的 `device-config` 参数在运行 `xe sr-create` 命令时查找 SR。

要在 iSCSI 目标的特定 LUN 上创建共享 GFS2 SR，请在群集池中的服务器上运行以下命令：

```
1 xe sr-create type=gfs2 name-label="Example GFS2 SR" --shared \  
2 device-config:provider=iscsi device-config:targetIQN=target_iqns \  
3 device-config:target=portal_address device-config:SCSIid=scsci_id
```

如果装载 GFS2 文件系统时无法访问 iSCSI 目标，群集池中的某些主机可能会提供保护。

有关使用 iSCSI SR 的详细信息，请参阅[软件 iSCSI 支持](#)。

### 创建基于 HBA 的共享 GFS2 SR

可以使用 XenCenter 通过 HBA SR 创建 GFS2。有关详细信息，请参阅 XenCenter 文档中的[硬件 HBA 存储](#)。

或者，也可以使用 xe CLI 通过 HBA SR 创建 GFS2。

GFS2 SR 的 Device-config 参数：

参数名称	说明	是否必需
<code>provider</code>	块提供程序实现。在这种情况下为 <code>hba</code> 。	是
<code>SCSIid</code>	设备 SCSI ID	是

可以使用 `xe sr-probe-ext` 命令查找要用于 `SCSIid` 参数的值。

```
1 xe sr-probe-ext type=<type> host-uuid=<host_uuid> device-config:=<config> sm-config:=<sm_config>
```

1. 首先请运行以下命令：

```
1 xe sr-probe-ext type=gfs2 device-config:provider=hba
```

命令的输出会提示您提供其他参数，并在每个步骤中给出可能的值列表。

2. 重复运行该命令，每次添加新参数。
3. 当命令输出以 `The following SRs were found:` 开头时，可以使用指定的 `device-config` 参数在运行 `xe sr-create` 命令时查找 SR。

要在 HBA 目标的特定 LUN 上创建共享 GFS2 SR，请在群集池中的服务器上运行以下命令：

```
1 xe sr-create type=gfs2 name-label="Example GFS2 SR" --shared \  
2 device-config:provider=hba device-config:SCSIid=device_scsi_id
```

有关使用 HBA SR 的详细信息，请参阅[硬件主机总线适配器](#)。

## NFS 和 SMB

可以立即将 NFS 服务器上的共享（支持 NFSv4 或 NFSv3）或 SMB 服务器上的共享（支持 SMB 3.0）用作虚拟磁盘的 SR。VDI 仅以 Microsoft VHD 格式存储。此外，由于可以共享这些 SR，因此，共享 SR 上存储的 VDI 允许执行以

下操作：

- 在资源池中的任何 Citrix Hypervisor 服务器上启动 VM
- 使用实时迁移功能在资源池中的 Citrix Hypervisor 服务器之间迁移 VM（无明显停机）

重要：

- 对 SMB 3.0 的支持功能限制为能够使用 3.0 协议连接到共享。透明故障转移等其他功能取决于上游 Linux 内核中的功能的可用性，但在 Citrix Hypervisor 8.0 中不受支持。
- 对于 NFSv4，只有身份验证类型 `AUTH_SYS` 受支持。
- SMB 存储适用于 Citrix Hypervisor Premium Edition 客户或通过其 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。

基于文件的 SR 上存储的 VDI 是精简预配的。当 VM 向磁盘写入数据时分配映像文件。VM 映像文件仅在存储中占用所需的空间，此方式将带来极大的好处。例如，如果为 VM 分配 100 GB 的 VDI 并安装操作系统，VDI 文件将仅反映已写入到磁盘的操作系统数据的大小，而不反映整个 100 GB。

还可以链接 VHD 文件，从而允许两个 VDI 共享通用数据。如果克隆基于文件的 VM，生成的 VM 将共享克隆时的通用磁盘数据。每个 VM 将在 VDI 的单独写入时复制版本中继续进行各自的更改。此功能允许从模板快速克隆基于文件的 VM，便于极快地预配和部署新 VM。

注意：

支持的最长 VHD 链长度为 30。

Citrix Hypervisor 中基于文件的 SR 和 VHD 实现假定其可以完全控制文件服务器上的 SR 目录。管理员不得修改 SR 目录的内容，因为此操作可能会损坏 VDI 的内容。

Citrix Hypervisor 已针对使用稳定 RAM 的企业级存储进行了优化，以快速确认写入请求，同时保留针对故障的高级数据保护。Citrix Hypervisor 已针对使用 Data OnTap 7.3 和 8.1 的 Network Appliance FAS2020 和 FAS3210 存储进行了广泛测试。

警告：

由于基于文件的 SR 上的 VDI 创建为精简预配 VDI，因此，管理员必须确保在基于文件的 SR 上为所有必需的 VDI 保留足够的磁盘空间。Citrix Hypervisor 服务器并不强制基于文件的 SR 上存在 VDI 所需的空间。

### 创建共享 NFS SR (NFS)

要创建 NFS SR，必须提供 NFS 服务器的主机名或 IP 地址。可以在任何有效的目标路径下创建 SR；使用 `sr-probe` 命令可显示服务器导出的有效目标路径列表。

Citrix Hypervisor 与低端存储配合使用时，在将确认传递到 VM 之前，会谨慎地等待所有写入内容得到确认。此方式会导致性能显著下降，但通过设置存储以将 SR 装载点呈现为异步模式导出，可以解决该问题。异步模式将导出实际不在磁盘上的确认写入内容。请考虑仔细在这些情况下失败的风险。

**注意：**

必须将配置为 NFS 服务器导出池中所有服务器的指定路径。如果此配置未完成，创建 SR 和插入 PBD 记录将失败。

默认情况下，Citrix Hypervisor NFS 实现使用 TCP。如果条件允许，可以将该实现配置为在可能对性能有益的情况下使用 UDP。要完成此配置，请在创建 SR 时指定 `device-config` 参数 `useUDP=true`。

NFS SR 的 Device-config 参数：

参数名称	说明	是否必需
<code>server</code>	NFS 服务器的 IP 地址或主机名称	是
<code>serverpath</code>	托管 SR 的 NFS 服务器的路径，包括 NFS 装载点	是

例如，要在 `192.168.1.10:/export1` 上创建共享 NFS SR，请使用以下命令：

```
1 xe sr-create content-type=user \
2   name-label="shared NFS SR" shared=true \
3   device-config:server=192.168.1.10 device-config:serverpath=/export1
   type=nfs \
4   nfsversion="3", "4"
```

要创建非共享 NFS SR，请运行以下命令：

```
1 xe sr-create host-uuid=host_uuid content-type=user \
2   name-label="Non-shared NFS SR" \
3   device-config:server=192.168.1.10 device-config:serverpath=/export1
   type=nfs \
4   nfsversion="3", "4"
```

**创建共享 SMB SR (SMB)**

要创建 SMB SR，请提供 SMB 服务器的主机名或 IP 地址、导出的共享的完整路径以及相应的凭据。

**注意：**

SMB SR 已针对运行 OnTap 8.3 和 Windows Server 2012 R2 的网络设备存储进行测试。

SMB SR 的 Device-config 参数：

参数名称	说明	是否必需
<code>server</code>	服务器上的共享的完整路径	是
<code>username</code>	对共享具有读写访问权限的用户帐户	可选
<code>password</code>	用户帐户的密码	可选

例如，要在 `192.168.1.10:/share1` 上创建共享 SMB SR，请使用以下命令：

```
1  xe sr-create content-type=user \
2  name-label="Example shared SMB SR" shared=true \
3  device-config:server=//192.168.1.10/share1 \
4  device-config:username=valid_username device-config:password=
   valid_password type=smb
```

要创建非共享 SMB SR，请运行以下命令：

```
1  xe sr-create host-uuid=host_uuid content-type=user \
2  name-label="Non-shared SMB SR" \
3  device-config:server=//192.168.1.10/share1 \
4  device-config:username=valid_username device-config:password=
   valid_password type=smb
```

#### 注意：

运行 `sr-create` 命令时，可以使用 `device-config:password_secret` 参数，而不是在命令行中指定密码。有关详细信息，请参阅[机密](#)。

## 硬件 HBA 上的 LVM

硬件 HBA 上 LVM 类型表示磁盘作为卷组中逻辑卷上的 VHD 在提供的 HBA LUN 上创建，例如，基于硬件的 iSCSI 或 FC 支持。

Citrix Hypervisor 服务器通过 Emulex 或 QLogic 主机总线适配器 (HBA) 支持光纤通道 SAN。必须手动完成向主机公开光纤通道 LUN 所需的所有光纤通道配置。此配置包括存储设备、网络设备以及 Citrix Hypervisor 服务器中的 HBA。完成所有 FC 配置后，HBA 将向主机公开一个由 FC LUN 支持的 SCSI 设备。然后，可以使用该 SCSI 设备访问 FC LUN，就像它是本地连接的 SCSI 设备一样。

使用 `sr-probe` 命令可以列出主机上存在的由 LUN 支持的 SCSI 设备。此命令强制扫描由 LUN 支持的新 SCSI 设备。`sr-probe` 返回的 LUN 支持的 SCSI 设备的路径值在将访问该 LUN 的所有主机之间保持一致。因此，创建可由资源池中的所有主机访问的共享 SR 时必须使用此值。

同样的功能也适用于 QLogic iSCSI HBA。

有关创建基于 HBA 的共享 FC 和 iSCSI SR 的详细信息，请参阅[创建存储库](#)。

注意：

Citrix Hypervisor 支持光纤通道，但不支持将 LUN 直接映射到 VM。必须将基于 HBA 的 LUN 映射到主机并指定将其用于 SR。SR 中的 VDI 作为标准块设备向 VM 公开。

## 精简预配的共享 **GFS2** 块存储设备

June 4, 2019

精简预配通过将磁盘存储空间分配给 VDI（因为数据会写入虚拟磁盘）来更好地利用可用存储，而非提前分配 VDI 的完整虚拟大小。通过精简预配，可以大大降低共享存储阵列上所需的空间量以及您的总体拥有成本 (TCO)。

在以下情况下，面向共享块存储进行精简预配尤其适用：

- 您希望提高空间效率。图像是稀疏的，而不是厚厚地分配。
- 您希望降低存储阵列上的每秒 I/O 操作数。GFS2 SR 是第一种支持在共享块存储上进行存储读取缓存的 SR 类型。
- 您对多个虚拟机使用公共基础映像。这样，各个 VM 的映像通常会占用更少的空间。
- 您使用快照。每个快照都是一个映像，并且每个映像现在都是稀疏的。
- 您的存储不支持 NFS，仅支持块存储。如果您的存储支持 NFS，我们建议您使用 NFS 而非 GFS2。
- 您希望创建大小大于 2 TiB 的 VDI。GFS2 SR 最大支持大小为 16 TiB 的 VDI。

共享 GFS2 类型将磁盘表示为在 iSCSI 或 HBA LUN 上创建的文件系统。GFS2 SR 上存储的 VDI 以 QCOW2 映像格式存储。

### 必备条件

开始操作之前，请确保满足以下必备条件：

- 群集池中的所有 Citrix Hypervisor 服务器都必须至少具有 2 GiB 的控制域内存。
- 群集中的所有主机都必须使用群集网络的静态 IP 地址。
- 我们建议您仅在至少包含三个主机的池中使用群集，因为包含两个主机的池对自主防护整个池非常敏感。
- 如果在池中的主机之间设置了防火墙，请确保主机能够使用以下端口在群集网络中进行通信：
  - TCP: 8892、21064
  - UDP: 5404、5405

有关详细信息，请参阅[Citrix 技术使用的通信端口](#)。

- 如果要对现有池进行群集操作，请务必禁用高可用性。启用群集功能后，可以重新启用高可用性。
- 您有一个基于块的存储设备对资源池中的所有 Citrix Hypervisor 服务器可见。

## 设置群集池以使用共享 **GFS2 SR**

要使用共享 GFS2 存储，Citrix Hypervisor 资源池必须是群集池。请先在您的池中启用群集，然后再创建 GFS2 SR。

注意：

群集池的行为与非群集池不同。有关群集行为的详细信息，请参阅[群集池](#)。

如果喜欢，可以使用 XenCenter 在池中设置群集功能。有关详细信息，请参阅[XenCenter 产品文档](#)。

要使用 xe CLI 创建群集池，请执行以下操作：

1. 创建绑定网络以用作群集网络。在希望作为池主服务器的 Citrix Hypervisor 服务器上，完成以下步骤：

- a) 在 Citrix Hypervisor 服务器上打开控制台。
- b) 使用以下命令命名您的资源池：

```
1 xe pool-param-set name-label="New Pool" uuid=<pool_uuid>
```

- c) 使用以下命令创建用于绑定 NIC 的网络：

```
1 xe network-create name-label=bond0
```

此时将返回新网络的 UUID。

- d) 使用以下命令查找要在绑定中使用的 PIF 的 UUID：

```
1 xe pif-list
```

- e) 在主动-主动模式、主动-被动模式或 LACP 绑定模式下创建绑定网络。根据要使用的绑定模式，完成以下操作之一：

- 要在主动-主动模式（默认模式）下配置绑定，请使用 `bond-create` 命令创建绑定。指定新创建的网络 UUID 和要绑定的各 PIF 的 UUID，以逗号分隔各参数：

```
1 xe bond-create network-uuid=<network_uuid> /
2     pif-uuids=<pif_uuid_1>,<pif_uuid_2>,<pif_uuid_3>,<
3     pif_uuid_4>
```

绑定两个 NIC 时，请键入两个 UUID；绑定四个 NIC 时，请输入四个 UUID。在运行该命令之后，将返回该绑定的 UUID。

- 要在主动-被动或 LACP 绑定模式下配置绑定，请使用相同的语法，添加可选的 `mode` 参数并指定 `lacp` 或 `active-backup`：

```
1 xe bond-create network-uuid=<network_uuid> pif-uuids=<
2     pif_uuid_1>, /
3     <pif_uuid_2>,<pif_uuid_3>,<pif_uuid_4> /
4     mode=balance-slb | active-backup | lacp
```

在池主服务器上创建绑定网络后，当您将其其他 Citrix Hypervisor 服务器加入池时，网络和绑定信息将自动复制到加入的服务器。

有关详细信息，请参阅[网络连接](#)。

## 2. 创建至少包含三台 Citrix Hypervisor 服务器的资源池。

在每个（非主）池成员的 Citrix Hypervisor 服务器上重复执行以下步骤：

- a) 在 Citrix Hypervisor 服务器上打开控制台。
- b) 使用以下命令将 Citrix Hypervisor 服务器加入池主服务器上的池：

```
1 xe pool-join master-address=master_address master-username=
  administrators_username master-password=password
```

`master-address` 参数的值必须设置为作为池主服务器的 Citrix Hypervisor 服务器的完全限定域名。安装池主服务器时，`password` 必须为设置的管理员密码。

有关详细信息，请参阅[主机和资源池](#)。

## 3. 对于属于此网络的每个 PIF，请设置 `disallow-unplug=true`。

- a) 使用以下命令查找属于网络的 PIF 的 UUID：

```
1 xe pif-list
```

- b) 在资源池中的 Citrix Hypervisor 服务器上运行以下命令：

```
1 xe pif-param-set disallow-unplug=true uuid=<pif_uuid>
```

## 4. 在您的池上启用群集功能。在资源池中的 Citrix Hypervisor 服务器上运行以下命令：

```
1 xe cluster-pool-create network-uuid=<network_uuid>
```

提供您在前面步骤中创建的绑定网络的 UUID。

## 设置指向您的共享 **GFS2 SR** 的存储多路径

重要：

在尝试启用多路径之前，请验证以下语句是否为真：

- 存储服务器上提供了多个可用目标。

例如，查询给定门户上的 `sendtargets` 的 iSCSI 存储后端应返回多个目标，如下例所示：

```
iscsiadm -m discovery -type sendtargets -portal 192.168.0.161
192.168.0.161:3260,1 iqn.strawberry:litchie
192.168.0.204:3260,2 iqn.strawberry:litchie
```

- 仅限 iSCSI，dom0 在多路径存储使用的每个子网上都有一个 IP 地址。

确保您希望存储的每个路径都有一个 NIC，并且每个 NIC 上都配置了一个 IP 地址。例如，如果您希望存储有四个路径，则必须有四个 NIC，每个 NIC 都配置一个 IP 地址。

- 仅限 HBA，将多个 HBA 连接到交换机结构。

可以使用 XenCenter 设置存储多路径。有关详细信息，请参阅 XenCenter 文档中的[存储多路径](#)。

或者，要使用 xe CLI 设置存储多路径，请在群集池中的所有 Citrix Hypervisor 服务器上完成以下步骤：

1. 在 Citrix Hypervisor 服务器上打开控制台。
2. 使用以下命令拔出服务器上的所有 PBD：

```
1 xe pbd-unplug uuid=<pbid_uuid>
```

3. 使用以下命令将 `other-config:multipathing` 参数的值设置为 `true`：

```
1 xe host-param-set other-config:multipathing=true uuid=<server_uuid>
```

4. 使用以下命令将 `other-config:multipathhandle` 参数的值设置为 `dmp`：

```
1 xe host-param-set other-config:multipathhandle=dmp uuid=<server_uuid>
```

5. 如果服务器上存在以单一路径模式运行但具有多路径的现有 SR：

- 迁移或挂起在受影响的 SR 中存在虚拟磁盘的任何正在运行的来宾系统
- 拔出并重新插入所有受影响的 SR 的 PBD 以使用多路径重新对其进行连接：

```
1 xe pbd-unplug uuid=<pbid_uuid>
2 xe pbd-plug uuid=<pbid_uuid>
```

有关详细信息，请参阅[存储多路径](#)。

## 创建共享 GFS2 SR

可以在 iSCSI 或 HBA LUN 上创建共享 GFS2 SR。

### 通过 iSCSI SR 创建共享 GFS2

可以使用 XenCenter 通过 iSCSI SR 创建 GFS2。有关详细信息，请参阅 XenCenter 文档中的[软件 iSCSI 存储](#)。

或者，也可以使用 xe CLI 通过 iSCSI SR 创建 GFS2。

GFS2 SR 的 Device-config 参数：

参数名称	说明	是否必需
<code>provider</code>	块提供程序实现。在这种情况下为 <code>iscsi</code> 。	是
<code>target</code>	托管此对象的 iSCSI 文件管理器的 IP 地址或主机名	是
<code>targetIQN</code>	托管 SR 的 iSCSI 文件管理器的 IQN 目标地址	是
<code>SCSIid</code>	设备 SCSI ID	是

可以使用 `xe sr-probe-ext` 命令查找要用于这些参数的值。

```
1 xe sr-probe-ext type=<type> host-uuid=<host_uuid> device-config:=<config> sm-config:=<sm_config>
```

1. 首先请运行以下命令：

```
1 xe sr-probe-ext type=gfs2 device-config:provider=iscsi
```

命令的输出会提示您提供其他参数，并在每个步骤中给出可能的值列表。

2. 重复运行该命令，每次添加新参数。
3. 当命令输出以 `The following SRs were found:` 开头时，可以使用指定的 `device-config` 参数在运行 `xe sr-create` 命令时查找 SR。

要在 iSCSI 目标的特定 LUN 上创建共享 GFS2 SR，请在群集池中的服务器上运行以下命令：

```
1 xe sr-create type=gfs2 name-label="Example GFS2 SR" --shared \  
2 device-config:provider=iscsi device-config:targetIQN=target_iqns \  
3 device-config:target=portal_address device-config:SCSIid=scsci_id
```

如果装载 GFS2 文件系统时无法访问 iSCSI 目标，群集池中的某些主机可能会提供保护。

有关使用 iSCSI SR 的详细信息，请参阅[软件 iSCSI 支持](#)。

### 创建基于 HBA 的共享 GFS2 SR

可以使用 XenCenter 通过 HBA SR 创建 GFS2。有关详细信息，请参阅 XenCenter 文档中的[硬件 HBA 存储](#)。

或者，也可以使用 `xe CLI` 通过 HBA SR 创建 GFS2。

GFS2 SR 的 `Device-config` 参数：

参数名称	说明	是否必需
<code>provider</code>	块提供程序实现。在这种情况下为 <code>hba</code> 。	是
<code>SCSIid</code>	设备 SCSI ID	是

可以使用 `xe sr-probe-ext` 命令查找要用于 `SCSIid` 参数的值。

```
1 xe sr-probe-ext type=<type> host-uuid=<host_uuid> device-config:=<config> sm-config:=<sm_config>
```

1. 首先请运行以下命令：

```
1 xe sr-probe-ext type=gfs2 device-config:provider=hba
```

命令的输出会提示您提供其他参数，并在每个步骤中给出可能的值列表。

2. 重复运行该命令，每次添加新参数。
3. 当命令输出以 `The following SRs were found:` 开头时，可以使用指定的 `device-config` 参数在运行 `xe sr-create` 命令时查找 SR。

要在 HBA 目标的特定 LUN 上创建共享 GFS2 SR，请在群集池中的服务器上运行以下命令：

```
1 xe sr-create type=gfs2 name-label="Example GFS2 SR" --shared \  
2 device-config:provider=hba device-config:SCSIid=device_scsi_id
```

有关使用 HBA SR 的详细信息，请参阅[硬件主机总线适配器](#)。

## 限制

共享 GFS2 存储当前具有以下限制：

- VDI 位于 GFS2 SR 上的 VM 不支持通过存储实时迁移功能迁移 VM。
- GFS2 SR 不支持 FCoE 协议。
- GFS2 SR 上不支持裁剪/取消映射。
- 性能衡量指标不适用于 GFS2 SR 以及这些 SR 上的磁盘。
- GFS2 SR 上存储的 VDI 不支持更改块跟踪功能。
- 不能将大于 2 TiB 的 VDI 导出为 VHD 或 OVA/OVF。但是，可以以 XVA 格式导出 VDI 大于 2 TiB 的 VM。
- 群集池最多仅支持每个池包含 16 个主机。
- 如果网络已同时用于管理和群集操作，则不能分离管理网络而不重新创建群集。
- 通过使用 XenCenter 更改群集网络的 IP 地址要求暂时禁用群集功能和 GFS2。
- 群集处于活动状态并且具有正在运行的 VM 时，请勿更改群集网络的绑定。此操作会导致群集进行防护。

- 如果您的至少涉及一个启用了群集功能的主机的群集网络中的一个 IP 地址（多个具有相同 IP 地址的主机）出现冲突，这些主机将不防护。要修复此问题，请解析 IP 地址冲突。

## 管理存储库

July 10, 2019

本节介绍了创建存储库类型并使其可用于 Citrix Hypervisor 服务器。本部分内容介绍了存储库 (SR) 日常管理中所需要的各种操作，包括实时 VDI 迁移。

### 创建存储库

本节介绍了如何创建不同类型的存储库 (SR) 并使其可用于 Citrix Hypervisor 服务器。提供的示例涉及使用 xe CLI 创建 SR。有关使用 XenCenter 通过“新建存储库”向导添加 SR 的详细信息，请参阅 XenCenter 帮助。

注意：

`lvm` 和 `ext3` 类型的本地 SR 只能使用 xe CLI 创建。创建后，可以使用 XenCenter 或 xe CLI 管理所有 SR 类型。

使用 CLI 创建在主机上使用的存储库包括两个基本步骤：

1. 探测 SR 类型以确定任何必需参数的值。
2. 创建 SR 以初始化 SR 对象及关联的 PBD 对象、插入 PBD 以及激活 SR。

根据创建的 SR 类型，这些步骤稍有差异。在所有示例中，如果成功，`sr-create` 命令将返回创建的 SR 的 UUID。

不再使用 SR 时可以将其销毁，以释放物理设备。还可以忽略 SR，以将 SR 与 Citrix Hypervisor 服务器分离，并将其连接到另一个服务器。有关详细信息，请参阅以下部分中的删除 SR。

### 探测 SR

`sr-probe` 命令有以下两种使用方式：

- 确定未知参数以在创建 SR 时使用
- 返回现有 SR 的列表

在这两种情况下，`sr-probe` 通过指定 SR 类型和该 SR 类型的一个或多个 `device-config` 参数起作用。如果提供的参数集不完整，`sr-probe` 命令将返回错误消息，指示参数缺失以及缺失参数的可能选项。如果提供的参数集完整，则将返回现有 SR 的列表。所有 `sr-probe` 输出将以 XML 格式返回。

例如，通过指定已知 iSCSI 目标的名称或 IP 地址，可以探测该目标。将返回该目标上可用的 IQN 集合：

```
1 xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10
2
3 Error code: SR_BACKEND_FAILURE_96
4 Error parameters: , The request is missing or has an incorrect
   target IQN parameter, \
5 <?xml version="1.0" ?>
6 <iscsi-target-iqns>
7   <TGT>
8     <Index>
9       0
10    </Index>
11    <IPAddress>
12      192.168.1.10
13    </IPAddress>
14    <TargetIQN>
15      iqn.192.168.1.10:filer1
16    </TargetIQN>
17  </TGT>
18 </iscsi-target-iqns>
```

再次探测相同的目标并指定名称/IP 地址和所需的 IQN 将返回该目标/IQN 上的可用 SCSIids (LUN) 集合。

```
1 xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10 \
2 device-config:targetIQN=iqn.192.168.1.10:filer1
3
4 Error code: SR_BACKEND_FAILURE_107
5 Error parameters: , The SCSIid parameter is missing or incorrect, \
6 <?xml version="1.0" ?>
7 <iscsi-target>
8   <LUN>
9     <vendor>
10      IET
11    </vendor>
12    <LUNid>
13      0
14    </LUNid>
15    <size>
16      42949672960
17    </size>
18    <SCSIid>
19      149455400000000000000000000000002000000b70200000f000000
20    </SCSIid>
21  </LUN>
22 </iscsi-target>
```

探测相同的目标并提供所有三个参数将返回在 LUN 上存在（如果有）的 SR 的列表。

```

1  xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10 \
2  device-config:targetIQN=192.168.1.10:filer1 \
3  device-config:SCSIid=1494554000000000000000000000002000000
   b70200000f000000
4
5  <?xml version="1.0" ?>
6  <SRlist>
7    <SR>
8      <UUID>
9        3f6e1ebd-8687-0315-f9d3-b02ab3adc4a6
10     </UUID>
11     <Devlist>
12       /dev/disk/by-id/scsi-1494554000000000000000000000002000000
        b70200000f000000
13     </Devlist>
14   </SR>
15 </SRlist>

```

可以针对每个 SR 类型探测以下参数：

SR 类型	device-config 参数 (按依赖关系排序)	是否可以探测?	sr-create 必需?
lvmoiscsi	target	否	是
	chapuser	否	否
	chappassword	否	否
	targetIQN	是	是
	SCSIid	是	是
lvmohba	SCSIid	是	是
NetApp	target	否	是
	username	否	是
	password	否	是
	chapuser	否	否
	chappassword	否	否
	aggregate	否 (请参阅备注 1)	是
	FlexVols	否	否
	allocation	否	否

SR 类型	device-config 参数 (按依赖关系排序)	是否可以探测?	sr-create 必需?
	asis	否	否
nfs	server	否	是
	serverpath	是	是
lvm	device	否	是
ext	device	否	是
EqualLogic	target	否	是
	username	否	是
	password	否	是
	chapuser	否	否
	chappassword	否	否
	storagepool	否 (请参阅备注 2)	是

**注意:**

- 只有在运行 `sr-create` 时才能执行聚合探测。
- 只有在运行 `sr-create` 时才能执行存储池探测。

**删除 SR**

存储库 (SR) 可被临时或永久删除。

**分离:** 断开存储设备与池或主机之间的关联 (PBD Unplug)。SR (及其 VDI) 将变得不可访问。VDI 的内容和 VM 用来访问 VDI 的元信息将被保存。需要临时将 SR 置于脱机状态 (例如, 为了进行维护) 时, 可以使用分离。分离的 SR 随后可以重新连接。

**忘记:** 在物理磁盘上保存 SR 的内容, 但永久删除用于将 VM 连接到其 VDI 的信息。例如, 这允许您将 SR 重新连接到另一个 Citrix Hypervisor 服务器, 而不必删除 SR 的任何内容。

**销毁:** 从物理磁盘删除 SR 的内容。

对于“销毁”或“忘记”操作, 连接到 SR 的 PBD 必须从主机上拔出。

1. 拔出 PBD 以将 SR 与相应的 Citrix Hypervisor 服务器分离:

```
1 xe pbd-unplug uuid=pbid_uuid
```

2. 使用 `sr-destroy` 命令可删除 SR。该命令将销毁 SR, 从 Citrix Hypervisor 服务器数据库中删除 SR 及其相应的 PBD, 并从物理磁盘中删除 SR 内容:

```
1 xe sr-destroy uuid=sr_uuid
```

3. 使用 `sr-forget` 命令可忘记 SR。该命令将从 Citrix Hypervisor 服务器数据库中删除 SR 及其相应的 PBD，但会保持物理介质上的实际 SR 内容不变：

```
1 xe sr-forget uuid=sr_uuid
```

**注意：**

需要一段时间才能完成对与 SR 相对应的软件对象进行垃圾回收。

## 引入 SR

要重新引入以前忘记的 SR，请创建一个 PBD。将该 PBD 手动插入恰当的 Citrix Hypervisor 服务器以激活 SR。

下例引入了一个类型为 `lvmoiscsi` 的 SR。

1. 探测现有 SR 以确定其 UUID：

```
1 xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10 \  
2 device-config:targetIQN=192.168.1.10:filer1 \  
3 device-config:SCSIid=14945540000000000000000000000002000000 \  
   b70200000f000000
```

2. 引入从 `sr-probe` 命令返回的现有 SR UUID。将返回新 SR 的 UUID：

```
1 xe sr-introduce content-type=user name-label="Example Shared LVM \  
   over iSCSI SR" \  
2 shared=true uuid=valid_sr_uuid type=lvmoiscsi
```

3. 创建一个随附 SR 的 PBD。将返回新 PBD 的 UUID：

```
1 xe pbd-create type=lvmoiscsi host-uuid=valid_uuid sr-uuid= \  
   valid_sr_uuid \  
2 device-config:target=192.168.0.1 \  
3 device-config:targetIQN=192.168.1.10:filer1 \  
4 device-config:SCSIid=14945540000000000000000000000002000000 \  
   b70200000f000000
```

4. 插入此 PBD 以连接 SR：

```
1 xe pbd-plug uuid=pbd_uuid
```

5. 验证此 PBD 插件的状态。如果成功，`currently-attached` 属性将为 `true`：

```
1 xe pbd-list sr-uuid=sr_uuid
```

**注意：**

请对资源池中的每个服务器执行步骤 3 到 5。还可以使用 XenCenter 中的“修复存储库”功能执行这些步骤。

## 实时 LUN 扩展

为了满足容量要求，可能需要为存储阵列添加容量，以增加为 Citrix Hypervisor 服务器预配的 LUN 大小。实时 LUN 扩展允许您增加 LUN 的大小而不会出现任何 VM 停机的情况。

将更多容量添加到存储阵列后，请输入

```
1 xe sr-scan sr-uuid=sr_uuid
```

此命令会重新扫描 SR，之后将添加任何额外容量并使其可用。

此操作还在 XenCenter 中可用。选择要调整大小的 SR，然后单击重新扫描。有关详细信息，请按 **F1** 以显示 XenCenter 帮助。

**警告：**

- 无法收缩或截断 LUN。减小存储阵列中的 LUN 大小可能导致数据丢失。

## 实时 VDI 迁移

实时 VDI 迁移允许管理员重新定位 VM 虚拟磁盘映像 (VDI)，而无需关闭 VM。此功能支持执行管理操作，例如：

- 将 VM 从便宜的本地存储移至快速灵活且支持阵列的存储中。
- 将 VM 从开发环境移至生产环境。
- 在存储层中移动 VM（如果 VM 受到存储容量限制）。
- 执行存储阵列升级。

### 限制和注意事项

实时 VDI 迁移受以下限制和注意事项约束

- 在目标库中必须具有充足的磁盘空间。

### 移动虚拟磁盘，工具为 XenCenter

1. 在资源窗格中，选择存储虚拟磁盘的 SR，然后单击存储选项卡。
2. 在虚拟磁盘列表中，选择要移动的虚拟磁盘，然后单击移动。

3. 在移动虚拟磁盘对话框中，选择要将 VDI 移至的目标 SR。

注意：

确保该 SR 具有可容纳另一个虚拟磁盘的充足空间：可用空间在可用 SR 列表中显示。

4. 单击移动以移动虚拟磁盘。

有关 xe CLI 参考，请参阅 [\[vdi-pool-migrate\]\(/zh-cn/citrix-hypervisor/command-line-interface.html#vdi-pool-migrate\)](#)。

### SR 之间的冷 VDI 迁移（脱机迁移）

可以将与 VM 关联的 VDI 从一个 SR 复制到另一个 SR 以符合维护要求或分层存储配置。XenCenter 允许您将 VM 及其所有 VDI 复制到同一个或另一个 SR。可以结合使用 XenCenter 和 xe CLI 在 SR 之间复制各个 VDI。

有关 xe CLI 参考，请参阅 [\[vm-migrate\]\(/zh-cn/citrix-hypervisor/command-line-interface.html#vm-migrate\)](#)。

#### 将 VM 的所有 VDI 复制到另一个 SR

XenCenter 复制 VM 功能可以在同一个或另一个 SR 上创建所选 VM 的所有 VDI 的副本。默认情况下，源 VM 和 VDI 不会受到影响。要将 VM 移动到所选 SR，而非创建副本，请在“复制虚拟机”对话框中选择“删除原始 VM”选项。

1. 关闭 VM。
2. 在 XenCenter 中，选择 VM，然后选择 **VM > 复制 VM** 选项。
3. 选择所需的目标 SR。

#### 将各个 VDI 复制到另一个 SR

可以结合使用 xe CLI 和 XenCenter 来在 SR 之间复制各个 VDI。

1. 关闭 VM。
2. 使用 xe CLI 确定要移动的 VDI 的 UUID。如果 VM 具有 DVD 驱动器，其 `vdi-uuid` 列出为 `not in database`，可以将其忽略。

```
1 xe vbd-list vm-uuid=valid_vm_uuid
```

注意：

`vbd-list` 命令同时显示 VBD 和 VDI 的 UUID。请务必记录 VDI 的 UUID 而不是 VBD 的 UUID。

3. 在 XenCenter 中，选择 **VM** 存储选项卡。对于要移动的每个 VDI，请选择该 VDI，然后单击分离按钮。还可以使用 `vbd-destroy` 命令执行此步骤。

**注意：**

如果使用 `vbd-destroy` 命令分离 VDI 的 UUID，请首先检查 VBD 是否将参数 `other-config:owner` 设置为 `true`。将此参数设置为 `false`。发出带 `other-config:owner=true` 的 `vbd-destroy` 命令还将销毁关联的 VDI。

4. 使用 `vdi-copy` 命令复制要移动到所需 SR 的每个 VM 的 VDI。

```
1 xe vdi-copy uuid=valid_vdi_uuid sr-uuid=valid_sr_uuid
```

5. 在 XenCenter 中，选择 **VM** 存储选项卡。单击连接按钮并从新 SR 中选择 VDI。还可以使用 `vbd-create` 命令执行此步骤。
6. 要删除原始 VDI，请在 XenCenter 中选择原始 SR 的存储选项卡。将列出原始 VDI，其中 VM 字段的值为空。使用删除按钮删除 VDI。

### 将本地光纤通道 **SR** 转换为共享 **SR**

使用 `xe CLI` 和 XenCenter 修复存储库功能，以便将当地 FC SR 转换为共享 FC SR：

1. 将资源池中的所有主机升级为 Citrix Hypervisor 8.0。
2. 确保池中的所有主机都对 SR 的 LUN 进行了适当的分区。有关使用 `sr-probe` 命令验证每台主机上是否都存在 LUN 的详细信息，请参阅探测 SR。
3. 将 SR 转换为共享 SR：

```
1 xe sr-param-set shared=true uuid=local_fc_sr
```

4. 在 XenCenter 中，SR 将从主机级别移动到池级别，指示其现在为共享 SR。使用红色感叹号对该 SR 进行标记，以显示当前并未在池中的所有主机上都插入了该 SR。
5. 选择该 SR，然后选择存储 > 修复存储库选项。
6. 单击修复以创建并为池中的每个主机插上 PBD。

### 使用丢弃功能回收备用阵列上基于块的存储的空间

可以使用空间回收功能释放精简预配的 LUN 上未使用的块。释放空间后，存储阵列随后可以重复使用这一回收的空间。

**注意：**

空间回收功能仅在某些类型的存储阵列上可用。请参阅[硬件兼容性列表](#)和存储供应商特定的文档，确定阵列是否支持此功能，以及是否需要特定的配置。

使用 XenCenter 回收空间：

1. 选择基础结构视图，然后单击连接到 SR 的服务器或池。
2. 单击存储选项卡。
3. 从列表中选择该 SR，然后单击回收释放的空间。
4. 单击是确认该操作。
5. 单击通知，然后单击事件，查看操作状态。

有关详细信息，请在 XenCenter 中按 **F1** 以访问联机帮助。

注意：

- 此操作仅在 XenCenter 中可用。
- 此操作仅适用于基于 LVM 的 SR，这些 SR 基于阵列上经过精简预配的 LUN。本地 SSD 也将从空间回收中受益。
- 基于文件的 SR 不需要空间回收，例如 NFS 和 Ext3。回收释放的空间按钮在 XenCenter 中对这些 SR 类型不可用。
- 空间回收是一种密集型操作，会导致存储阵列性能下降。因此，仅在阵列上需要空间回收时启动此操作。我们建议您将此工作安排在非阵列需求高峰期进行。

### 删除快照时自动回收空间

通过 Citrix Hypervisor 删除快照时，基于 LVM 的 SR 上分配的空间将自动回收，并且无需重新启动 VM。此操作称为“联机合并”。

联机合并仅适用于基于 LVM 的 SR (LVM、LVMoISCSI 和 LVMoHBA)。不适用于 EXT 或 NFS SR，其行为保持不变。在某些情况下，自动执行的空间回收可能无法继续。我们建议您在以下情况下使用脱机合并工具：

- VM I/O 吞吐量相当大时
- 一段时间后未回收空间时

注意：

- 由于需要执行挂起/恢复操作，因此运行“脱机合并”工具会导致 VM 停机。
- 在运行此工具之前，请删除不再需要的任何快照和克隆。该工具将回收尽可能多的空间用于剩余的快照/克隆。如果要回收整个空间，请删除所有快照和克隆。
- VM 磁盘必须位于一个主机的共享或本地存储上。如果 VM 的磁盘采用这两种存储类型，VM 将无法合并。

### 使用脱机合并工具回收空间

注意：

联机合并仅适用于基于 LVM 的 SR (LVM、LVMoISCSI 和 LVMoHBA)，而不适用于 EXT 或 NFS SR (这些 SR 的行为保持不变)。

使用 XenCenter 启用隐藏的对象。单击查看 > 隐藏的对象。在“资源”窗格中，选择要获得 UUID 的 VM。UUID 将显示在常规选项卡中。

在“资源”窗格中，选择资源池主服务器（列表中的第一个主机。常规选项卡将显示 UUID。如果未使用资源池，请选择该 VM 的主机。

1. 在主机上打开控制台并运行以下命令：

```
1 xe host-call-plugin host-uuid=host-UUID \
2   plugin=coalesce-leaf fn=leaf-coalesce args:vm_uuid=VM-UUID
```

例如，如果 VM 的 UUID 为 9bad4022-2c2d-dee6-abf5-1b6195b1dad5，主机的 UUID 为 b8722062-de95-4d95-9baa-a5fe343898ea，请运行以下命令：

```
1 xe host-call-plugin host-uuid=b8722062-de95-4d95-9baa-a5fe343898ea \
2   plugin=coalesce-leaf fn=leaf-coalesce args:vm_uuid=9bad4022-2
   c2d-dee6-abf5-1b6195b1dad5
```

2. 此命令将挂起 VM（除非 VM 已经关机），启动空间回收过程，然后恢复该 VM。

注意：

我们建议您在执行脱机合并工具之前手动关闭或挂起 VM。可以使用 XenCenter 或 Citrix Hypervisor CLI 关闭或挂起 VM。如果在运行中的 VM 上执行合并工具，该工具将自动挂起 VM，执行所需的 VDI 合并操作，然后恢复该 VM。

如果要合并的虚拟磁盘映像 (VDI) 位于共享存储上，则必须在池主服务器上执行脱机合并工具。

如果要合并的 VDI 位于本地存储上，请在本地存储连接到的服务器上执行脱机合并工具。

## 调整磁盘 I/O 调度程序

为了获得一般性能，会对所有新 SR 类型应用默认磁盘调度程序 `noop`。`noop` 调度程序提供可与访问相同设备的 VM 相媲美的最佳性能。为了应用磁盘 QoS，需要覆盖默认设置并将 `cfq` 磁盘调度程序分配给 SR。必须拔出并重新插入相应的 PBD 以使调度程序参数生效。可以使用以下命令调整磁盘调度程序：

```
1 xe sr-param-set other-config:scheduler=noop|cfq|anticipatory|deadline \
2   uuid=valid_sr_uuid
```

注意：

此命令不影响 EqualLogic、NetApp 或 NFS 存储。

## 虚拟磁盘 QoS 设置

虚拟磁盘具有可选 I/O 优先级质量服务 (QoS) 设置。可以按照本节介绍的方法使用 xe CLI 将此设置应用到现有虚拟磁盘。

对于共享 SR (即多个主机访问同一 LUN)，会将 QoS 设置应用到从同一主机访问 LUN 的 VBD。即不会跨池中的主机应用 QoS。

为 VBD 配置任何 QoS 参数之前，请确保已适当设置了 SR 的磁盘调度程序。有关如何调整调度程序的详细信息，请参阅前面部分中的调整磁盘 I/O 调度程序。必须在需要 QoS 的 SR 上将调度程序参数设置为 `cfq`。

注意：

请谨记在 SR 上将该调度程序设置为 `cfq`，并确保已重新插入 PBD 以使调度程序更改生效。

第一个参数为 `qos_algorithm_type`。必须将此参数值设置为 `ionice`，这是此版本中的虚拟磁盘唯一支持的 QoS 算法类型。

QoS 参数本身是使用分配给 `qos_algorithm_param` 参数的键/值对设置的。对于虚拟磁盘，`qos_algorithm_param` 使用 `sched` 键，并且根据参数值，还需要使用 `class` 键。

`qos_algorithm_param:sched` 可能的值包括：

- `sched=rt` 或 `sched=real-time` 将 QoS 调度参数设置为实时优先级，此优先级需要使用类参数来设置
- `sched=idle` 将 QoS 调度参数设置为空闲优先级，此优先级不需要使用类参数来设置
- `sched=anything` 将 QoS 调度参数设置为 best-effort 优先级，此优先级需要使用类参数来设置

`class` 的可能值包括：

- 以下关键词之一：最高、高、普通、低、最低
- 介于 0 到 7 之间的整数，其中 7 表示最高优先级，0 表示最低优先级。例如，优先级为 5 的 I/O 请求的优先级高于优先级为 2 的 I/O 请求。

要启用磁盘 QoS 设置，还必须将 `other-config:scheduler` 设置为 `cfq` 并重新插入所涉及的存储的 PBD。

例如，以下 CLI 命令将虚拟磁盘的 VBD 设置为使用实时优先级 5：

```
1     xe vbd-param-set uuid=vbd_uuid qos_algorithm_type=ionice
2     xe vbd-param-set uuid=vbd_uuid qos_algorithm_params:sched=rt
3     xe vbd-param-set uuid=vbd_uuid qos_algorithm_params:class=5
4     xe sr-param-set uuid=sr_uuid other-config:scheduler=cfq
5     xe pbd-plug uuid=pbd_uuid
```

## 存储多路径

June 4, 2019

系统为光纤通道和 iSCSI 存储后端提供动态多路径支持。可以在 XenCenter 中或 xe CLI 上启用多路径。

**重要：**

在尝试启用多路径之前，请验证以下语句是否为真：

- 存储服务器上提供了多个可用目标。

例如，查询给定门户上的 sendtargets 的 iSCSI 存储后端应返回多个目标，如下例所示：

```
iscsiadm -m discovery -type sendtargets -portal 192.168.0.161
192.168.0.161:3260,1 iqn.strawberry:litchie
192.168.0.204:3260,2 iqn.strawberry:litchie
```

- 仅限 iSCSI，dom0 在多路径存储使用的每个子网上都有一个 IP 地址。

确保您希望存储的每个路径都有一个 NIC，并且每个 NIC 上都配置了一个 IP 地址。例如，如果您希望存储有四个路径，则必须有四个 NIC，每个 NIC 都配置一个 IP 地址。

- 仅限 HBA，将多个 HBA 连接到交换机结构。

1. 在 Citrix Hypervisor 服务器上打开控制台。
2. 使用以下命令拔出服务器上的所有 PBD：

```
1 xe pbd-unplug uuid=<pbid_uuid>
```

3. 使用以下命令将 `other-config:multipathing` 参数的值设置为 **true**：

```
1 xe host-param-set other-config:multipathing=true uuid=<server_uuid>
```

4. 使用以下命令将 `other-config:multipathhandle` 参数的值设置为 `dmp`：

```
1 xe host-param-set other-config:multipathhandle=dmp uuid=<server_uuid>
```

5. 如果服务器上存在以单一路径模式运行但具有多路径的现有 SR：

- 迁移或挂起在受影响的 SR 中存在虚拟磁盘的任何正在运行的来宾系统
- 拔出并重新插入所有受影响的 SR 的 PBD 以使用多路径重新对其进行连接：

```
1 xe pbd-unplug uuid=<pbid_uuid>
2 xe pbd-plug uuid=<pbid_uuid>
```

要禁用多路径，请先拔出 VBD，接着将主机 `other-config:multipathing` 参数设置为 **false**，然后按上述方法重新插入 PBD。请勿修改 `other-config:multipathhandle` 参数，因为此操作是自动完成的。

Citrix Hypervisor 中的多路径支持基于设备映射器 `multipathd components`。存储管理器 API 自动处理激活和停用多路径节点。与 Linux 中的标准 `dm-multipath` 工具不同，设备映射器节点是自动为系统中的所有 LUN 创

建的。仅当 LUN 由存储管理层主动使用时才会预配设备映射器节点。因此，不必使用任何 `dm-multipath` CLI 工具查询或刷新 Citrix Hypervisor 中的 DM 表节点。如果需要手动查询设备映射器的状态，或列出系统中活动设备映射器多路径节点，请使用 `mpathutil` 实用程序：

```
1 mpathutil list
```

```
1 mpathutil status
```

注意：

- 由于与集成多路径管理体系结构不兼容，我们建议您不要将标准 `dm-multipath` CLI 实用程序与 Citrix Hypervisor 结合使用。请使用 `mpathutil` CLI 工具查询主机上的节点状态。
- EqualLogic 阵列中的多路径支持不包括传统意义上的存储 I/O 多路径。必须在网络/NIC 绑定级别处理多路径。有关为 EqualLogic SR/LVMoISCSI SR 配置网络故障转移的信息，请参阅 EqualLogic 文档。

## IntelliCache

June 4, 2019

注意：

此功能仅在将 Citrix Hypervisor 与 Citrix Virtual Desktops 结合使用时受支持。

使用 GFS2 SR 的 VM 不支持 Intellicache。

通过将 Citrix Hypervisor 与 *IntelliCache* 结合使用，可以组合使用共享存储和本地存储，从而提高所托管虚拟桌面基础结构部署的成本效益。当多个虚拟机 (VM) 共享一个公用的操作系统映像时，优势尤其明显。既降低了存储阵列的负载，又提高了性能。此外，当本地存储从共享存储中缓存主映像时，进出共享存储的网络流量会减少。

IntelliCache 的工作原理是从 VM 主机上本地存储中的 VM 父 VDI 中缓存数据。然后，在从父项 VDI 中读取数据时，会填充此本地缓存。当多个 VM 共享一个公用父 VDI 时，某个 VM 可以使用从另一个 VM 读入到缓存的数据。不需要再访问共享存储上的主映像。

精简预配的本地 SR 是 IntelliCache 的必备条件。精简预配是一种优化可用存储空间使用情况的方式。通过这种方式，可以更多地利用本地存储来代替共享存储。它依赖于数据块的按需分配。在其他方法中，将预先分配所有块。

重要：

精简预配将主机的默认本地存储类型由 LVM 改为 EXT3。要正常进行 Citrix Virtual Desktops 本地缓存，必须启用精简预配。

精简预配允许管理员为连接到存储库 (SR) 的 VM 提供比 SR 中可用的存储空间更多的空间。但对空间没有保证，并且在 VM 写入数据前，分配的 LUN 不会要求获得任何数据块。

**警告:**

由于空间中 VM 数量不断增加，从而占用所需磁盘容量，因此精简预配的 SR 可能会出现物理运行空间不足的情况。IntelliCache VM 处理此情况的方法是在本地 SR 缓存满载时自动故障恢复到共享存储。由于 IntelliCache VM 的大小会快速增加，因此请不要在同一个 SR 中混合使用传统虚拟机与 IntelliCache VM。

## IntelliCache 部署

IntelliCache 必须在主机安装期间启用，或在主机运行期间使用 CLI 手动启用。

我们建议您使用高性能本地存储设备来保证实现最快速的数据传输。例如，使用固态硬盘或高性能 RAID 阵列。在确定本地磁盘大小时，对数据吞吐量和存储容量均应加以考虑。用于托管源虚拟磁盘映像 (VDI) 的共享存储类型必须基于 NFS 或 EXT。

### 安装主机时启用

要在安装主机过程中启用 IntelliCache，请在 **Virtual Machine Storage** (虚拟机存储) 屏幕上选择 **Enable thin provisioning (Optimized storage for XenDesktop)** (启用精简预配 (用于 XenDesktop 的优化存储))。此选项将选择主机的本地 SR 作为要用于 VM VDI 的本地缓存的 SR。



### 将现有主机转换为使用精简预配

要删除基于现有 LVM 的本地 SR，并将其替换为基于精简预配的 EXT3 的 SR，请输入以下命令。

**警告:**

这些命令将删除现有的本地 SR，并且该 SR 上的 VM 将被永久删除。

```
1     localsr='xe sr-list type=lvm host=hostname params=uuid --minimal'
2     echo localsr=$localsr
3     pbd='xe pbd-list sr-uuid=$localsr params=uuid --minimal'
4     echo pbd=$pbd
5     xe pbd-unplug uuid=$pbd
6     xe pbd-destroy uuid=$pbd
7     xe sr-forget uuid=$localsr
8     sed -i "s/'lvm'/'ext'/" /etc/firstboot.d/data/default-storage.
        conf
9     rm -f /etc/firstboot.d/state/10-prepare-storage
10    rm -f /etc/firstboot.d/state/15-set-default-storage
11    service firstboot start
12    xe sr-list type=ext
```

要启用本地缓存，请输入以下命令：

```
1     xe host-disable host=hostname
2     localsr='xe sr-list type=ext host=hostname params=uuid --
        minimal'
3     xe host-enable-local-storage-caching host=hostname sr-uuid=
        $localsr
4     xe host-enable host=hostname
```

## VM 引导行为

对于 VM 引导时的 VM VDI 行为，有两个选项：

### 1. 共享桌面模式

在 VM 引导时，VDI 还原为上一次引导时的状态。VM 下次引导时，在 VM 运行时所做的所有更改都将丢失。

如果您打算交付用户无法进行永久性更改的标准化桌面，请选择此选项。

### 2. 专用桌面模式

在 VM 引导时，VDI 处于上一次关机时的状态。

如果您打算允许用户对其桌面进行永久性更改，请选择此选项。

## VM 缓存行为设置

VDI 标志 `allow-caching` 指示缓存行为：

### 共享桌面模式

对于共享桌面，`on-boot` 选项为 `reset`，`allow-caching` 标志为 `true`。新的 VM 数据仅写入本地存储。不写入共享存储。此方法意味着共享存储上的负载将降低。但是，不能在主机之间迁移 VM。

### 专用桌面模式

对于专用桌面，`on-boot` 选项设置为 `persist`，`allow-caching` 标志设置为 `true`。新的 VM 数据同时写入本地存储和共享存储。读取缓存数据不需要传输到共享存储的 I/O 流量，因此，共享存储上的负载将降低。允许将 VM 迁移到其他主机，并且读入数据时会填充新主机上的本地缓存。

### 实现详细信息和故障排除

问：IntelliCache 是否与实时迁移功能和高可用性兼容？

答：当虚拟桌面处于专用模式时（即，`on-boot=persist` 时），可以将实时迁移功能和高可用性功能与 IntelliCache 结合使用。

**警告：**

如果任何 VDI 的缓存行为标志都设置为 `on-boot=reset` 和 `allow-caching=true`，则不能迁移该 VM。尝试迁移具有这些属性的 VM 将失败。

问：本地缓存在本地磁盘中的什么位置？

答：该缓存位于存储库 (SR) 中。每个主机都有一个指示使用哪个（本地）SR 存储缓存文件的配置参数（称为 `local-cache-sr`）。此 SR 通常为 EXT 类型的 SR。在运行采用 IntelliCache 的 VM 时，您将看到 SR 中名为 `uuid.vhdcache` 的文件。此文件是与具有指定 UUID 的 VDI 对应的缓存文件。XenCenter 中不会显示这些文件 - 查看这些文件的唯一方法是登录 `dom0` 并列出行 `/var/run/sr-mount/sr-uuid` 的内容。

问：我如何指定要用作缓存的特定 SR？

答：主机对象字段 `local-cache-sr` 引用本地 SR。可通过运行以下命令来查看其值：

```
1 xe sr-list params=local-cache-sr,uuid,name-label
```

该字段的设置：

- 安装主机后，如果在主机安装程序中选择了“Enable thin provisioning”（启用精简预配）选项，或者
- 通过执行 `xe host-enable-local-storage-caching host=host sr-uuid=sr`。此命令要求禁用指定的主机。使用此命令时，请关闭 VM。

第一个选项使用 EXT 类型的本地 SR 并且在主机安装期间创建。第二个选项使用在命令行中指定的 SR。

**警告：**

只有配置了多个本地 SR 的用户才需要执行这些步骤。

问：何时删除本地缓存？

答：只有在删除 VDI 本身时，才会删除 VDI 缓存文件。在将 VDI 附加到 VM（例如，在 VM 启动时）时，会重置缓存。如果删除 VDI 时主机处于脱机状态，则在启动时运行的 SR 同步将对缓存文件进行回收。

注意：

VM 迁移到不同的主机或关闭时，不会从主机中删除缓存文件。

## 存储读取缓存

June 4, 2019

读取缓存可以改进 VM 的磁盘性能，因为首次从外部磁盘读取后，数据将缓存在主机的可用内存中。在单一基础 VM 上克隆多个 VM 的情况下，读取缓存可以提高性能，因为读取缓存将明显减少从磁盘读取的块数量。例如，在 Citrix Virtual Desktops 环境 Machine Creation Service (MCS) 环境中。

无论何时从磁盘多次读取数据，都可以看到这种性能改进，因为数据缓存在内存中。此变更是在繁重 I/O 情况下发生的最明显的服务降级。例如，在以下情况下：

- 大量最终用户在短时间内启动时（启动高峰）
- 安排大量 VM 同时运行恶意软件扫描时（防病毒高峰）。

当您具有恰当的许可证类型时，默认启用读取缓存。

注意：

存储读取缓存适用于 Citrix Hypervisor Premium Edition 客户。

存储读取缓存适用于通过 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。

## 启用和禁用读取缓存

对于基于文件的 SR，例如 NFS 和 EXT3 SR 类型，读取缓存在默认情况下启用。读取缓存对所有其他 SR 禁用。

要对特定 SR 禁用读取缓存，请运行以下命令：

```
1 xe sr-param-set uuid=sr-uuid other-config:o_direct=true
```

## 限制

- 读取缓存仅适用于 NFS 和 EXT3 SR。它不适用于其他 SR 类型。
- 读取缓存仅适用于只读 VDI 和 VDI 父对象。这些 VDI 存在于从“快速克隆”或磁盘快照创建 VM 的位置。从单一“黄金”映像克隆 VM 时，将看到最显著的性能改进。

- 性能改进取决于主机控制域 (dom0) 中的可用内存量。增加 dom0 的内存量将允许为读取缓存分配更多内存。有关如何配置 dom0 内存的信息，请参阅 [CTX134951](#)。

### 与 IntelliCache 比较

IntelliCache 和基于内存的读取缓存在某种程度上互为补充。IntelliCache 不仅缓存在不同层上，还缓存写入和读取。IntelliCache 将读取的数据从网络缓存到本地磁盘。内存中读取缓存将读取的数据从网络或磁盘缓存到主机内存。内存中读取缓存的优势是，内存仍然比固态硬盘 (SSD) 快一个数量级。启动高峰和其他繁重 I/O 情况下的性能会得以改进。

可以同时启用读取缓存和 IntelliCache。在这种情况下，IntelliCache 将读取的数据从网络缓存到本地磁盘。从该本地磁盘读取的数据通过读取缓存缓存在内存中。

### 设置读取缓存大小

通过为 Citrix Hypervisor 的控制域 (dom0) 分配更多的内存，可以优化读取缓存性能。

#### 重要：

为实现优化，请逐一在池中的所有主机上设置读取缓存大小。此外，还必须在池中的所有主机上设置读取缓存大小的任何后续更改。

在 Citrix Hypervisor 服务器上，打开本地 shell，以 root 用户身份登录。

要设置读取缓存的大小，请运行以下命令：

```
1 /opt/xensource/libexec/xen-cmdline --set-xen dom0_mem=nnM,max:nnM
```

请将初始值和最大值设置为相同的值。例如，将 dom0 内存设置为 2048 MiB：

```
1 /opt/xensource/libexec/xen-cmdline --set-xen dom0_mem=20480M,max:20480M
```

#### 重要：

在更改读取缓存大小后重新启动所有主机。

### 如何查看当前的 dom0 内存分配？

要查看当前的 dom0 内存设置，请输入：

```
1 free -m
```

`free -m` 的输出显示当前的 dom0 内存设置。由于各种开销，该值可能低于预期。以下示例表显示主机输出，dom0 设为 2.6 GiB

	总数	已使用	可用	已共享	缓冲区/缓存	可用
内存:	2450	339	1556	9	554	2019
交换:	1023	0	1023			

可以使用的值范围是什么？

因为 Citrix Hypervisor 控制域 (dom0) 是 64 位的，所以可以使用较大值，例如 32768 MiB。但是，我们建议您不要将 **dom0** 内存减少到 **1 GiB** 以下。

### XenCenter 显示说明

可以将整个主机的内存视为由 Xen 虚拟机管理程序、dom0、VM 和可用内存组成。尽管 dom0 和 VM 的内存大小通常是固定的，但 Xen 虚拟机管理程序使用可变的内存量。使用的内存量取决于多种因素。这些因素包括任意时间主机上正在运行的 VM 的数量以及配置这些 VM 的方式。无法限制 Xen 使用的内存量。限制内存量会导致 Xen 内存不足，并阻止新 VM 启动，即使主机有可用内存亦如此。

要查看分配给主机的内存，在 XenCenter 中选择主机，然后单击内存选项卡。

Citrix Hypervisor 字段显示分配给 dom0 的内存与 Xen 内存的总和。因此，显示的内存量可能高于管理员指定的内存量。启动和停止 VM 时内存大小有所差别，即使管理员为 dom0 设置了固定大小亦如此。

### PVS 加速器

July 10, 2019

Citrix Hypervisor PVS 加速器功能向使用 Citrix Hypervisor 和 Citrix Provisioning 的客户提供了扩展的功能。要对 Citrix Virtual Apps and Desktops 进行映像管理和托管，通常会选择 Citrix Provisioning。PVS 加速器显著提高了已然出色至极的 Citrix Hypervisor 和 Citrix Provisioning 的组合的性能。这一新增功能提供的部分优势包括：

- 数据局部性：利用内存、SSD 和 NVM 设备的性能和局部性来实现读取请求，同时显著降低网络使用率。
- 改进了最终用户体验：数据局部性缩短了缓存的目标设备 (VM) 的读 I/O 延迟，进一步加快了最终用户应用程序的运行速度。
- 加快了 **VM** 启动和启动高峰时期的速度：缩短了读 I/O 延迟并且提高了效率，能够加快 VM 的启动时间，并且可以在大量设备在短时间内启动时提升性能。
- 通过添加更多虚拟机管理程序主机简化了扩展过程：所需的 Citrix Provisioning 服务器数量可能会减少，因为存储负载有效地分散在所有 Citrix Hypervisor 服务器上。峰值负载使用原始主机中的缓存进行处理。

- 降低了 **TCO** 并且简化了基础结构要求：Citrix Provisioning 服务器数量减少意味着硬件和许可证要求降低，并且管理开销也降低。所释放的容量可用于工作负载。

注意：

PVS 加速器适用于 Citrix Hypervisor Premium Edition 客户或通过 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。要使用 PVS 加速器功能，请将许可证服务器升级到版本 11.14。

## PVS 加速器的工作原理

PVS 加速器利用驻留在 Citrix Hypervisor 的控制域 (dom0) 中的代理机制。启用此功能后，Citrix Provisioning 目标设备 (VM) 读取请求将直接在 Citrix Hypervisor 服务器计算机上缓存。这些请求在物理内存或存储库中缓存。该 Citrix Hypervisor 服务器上的后续 VM 发出相同的读取请求时，虚拟磁盘将直接通过流技术从缓存推送，而非从 Citrix Provisioning 服务器推送。不再需要通过流技术从 Citrix Provisioning 服务器推送大大降低了网络利用率以及服务器上的处理量。此方法大大改进了 VM 的性能。

## 启用 PVS 加速器

客户必须在 Citrix Hypervisor 和 Citrix Provisioning 中完成以下配置设置，以启用 PVS 加速器功能：

1. 在池中的每个 Citrix Hypervisor 服务器上安装 PVS 加速器补充包。可以从 [Citrix Hypervisor 产品下载](#) 页面下载该补充包。可以使用 XenCenter 或 xe CLI 安装该补充包。有关如何使用 XenCenter 安装补充包的信息，请参阅 XenCenter 帮助。有关 CLI 的说明，请参阅 [Citrix Hypervisor 补充包和 DDK 指南](#)。
2. 在 Citrix Hypervisor 中使用 XenCenter 或 xe CLI 配置 PVS 加速器。此配置包括添加 Citrix Provisioning 站点以及指定 Citrix Provisioning 缓存存储的位置。
  - 有关 CLI 的说明，请参阅下面部分中的在 *Citrix Hypervisor* 中使用 CLI 配置 PVS 加速器。
  - 有关使用 XenCenter 配置 PVS 加速器的信息，请参阅 XenCenter 帮助。
3. 在 Citrix Hypervisor 中配置 PVS 加速器后，请使用 PVS UI 完成 PVS 站点的缓存配置。有关详细说明，请参阅在 Citrix Provisioning 中完成缓存配置。

## 在 Citrix Hypervisor 中使用 CLI 配置 PVS 加速器

1. 运行以下命令以在 Citrix Hypervisor 上创建 Citrix Provisioning 站点配置：

```
1 PVS_SITE_UUID=$(xe pvs-site-introduce name=label=My PVS Site)
```

2. 对于池中的每个主机，请指定要使用的缓存。可以选择将缓存存储在存储库 (SR) 上或者控制域内存中。

### 在存储库上配置缓存存储

为缓存存储选择存储库 (SR) 时, 请考虑以下特性:

#### 优势:

- 最新读取的数据尽可能缓存在内存中。访问这些数据的速度可以与使用控制域内存一样快。
- 位于 SR 上时, 缓存会变得更大。一般而言, SR 空间的成本远低于内存空间的成本。在 SR 上缓存能够卸载 Citrix Provisioning 服务器上的更多负载。
- 不需要修改控制域内存设置。缓存自动使用控制域中的可用内存, 永远不会导致控制域内存不足。
- 缓存 VDI 可以存储在共享存储中。但是, 此存储选项很少有意义。只有在共享存储比 Citrix Provisioning 服务器快得多, 此方法才有意义。
- 可以使用基于文件或基于块的 SR 进行缓存存储。

#### 劣势:

- 如果 SR 速度缓慢, 并且请求的数据不在内存层中, 缓存过程的速度将低于远程 Citrix Provisioning 服务器的速度。
- 存储在共享存储上的缓存 VDI 无法在主机之间共享。缓存的 VDI 特定于一台主机。

执行以下过程可在存储库上配置缓存存储:

1. 运行以下命令可查找用于缓存的 SR 的 UUID:

```
1 xe sr-list name=label=Local storage host=host-name-label --minimal  
   )
```

2. 创建缓存存储。

```
1 xe pvs-cache-storage-create host=host-name-label pvs-site-uuid=  
   PVS_SITE_UUID \  
2     sr-uuid=SR_UUID size=10GiB
```

#### 注意:

选择存储库 (SR) 时, 该功能最多将占用在 SR 上指定的缓存大小。此外, 该功能还将隐式使用可用控制域内存作为最大努力缓存层。

### 在控制域内存中配置缓存存储

为缓存存储选择控制域内存时, 请考虑以下特性:

#### 优势:

使用内存意味着访问或填充缓存时读/写性能将一直非常快。

#### 劣势:

- 硬件的大小必须适中, 因为用于缓存存储的 RAM 不适用于 VM。

- 必须在配置缓存存储之前扩展控制域内存。

注意：

如果选择在控制域内存中存储缓存，该功能最多将占用控制域内存中指定的缓存大小。此选项仅在已将额外的内存分配给控制域时可用。有关增加控制域内存的信息，请参阅[更改分配给控制域的内存量](#)。

增加分配给主机的控制域的内存量后，可以为 PVS 加速器显式分配额外的内存。

执行以下过程可在控制域内存中配置缓存存储：

1. 运行以下命令可查找要配置为用于缓存的主机的 UUID：

```
1 xe host-list name-label=host-name-label --minimal
```

2. 创建特殊类型 tmpfs 的 SR：

```
1 xe sr-create type=tmpfs name-label=MemorySR host-uuid=
  HOST_UUID device-config:uri=""
```

3. 运行以下命令可创建缓存存储：

```
1 xe pvs-cache-storage-create host-uuid=HOST_UUID
2 pvs-site-uuid=PVS_SITE_UUID sr-uuid=SR_UUID size=1GiB
```

其中 SR\_UUID 是在步骤 b 中创建的 SR 的 UUID

在 **Citrix Provisioning** 中完成缓存配置

在 Citrix Hypervisor 中配置 PVS 加速器后，请执行以下步骤以完成 Citrix Provisioning 站点的缓存配置。

在 Citrix Provisioning 管理员控制台中，使用 Citrix Virtual Desktops 设置向导或流 VM 向导（取决于部署类型）访问代理功能。尽管这两个向导相似，并且共享多个相同的屏幕，但仍存在以下差异：

- **Citrix Virtual Desktops** 设置向导用于配置使用 Citrix Virtual Desktops 控制的 Citrix Hypervisor 虚拟机管理程序上运行的 VM。
- 流 **VM** 向导用于在主机上创建 VM。不涉及 Citrix Virtual Desktops。

启动 Citrix Provisioning 管理员控制台：

1. 导航到 Citrix Provisioning 站点。
2. 选择 Citrix Provisioning 站点，然后单击鼠标右键以显示上下文菜单。
3. 根据部署选择恰当的向导。选择选项对所有虚拟机启用 **PVS** 加速器以启用 PVS 加速器功能。
4. 如果是首次启用虚拟磁盘缓存，流虚拟机设置向导上将显示 **Citrix Hypervisor** 屏幕。此屏幕显示在 Citrix Hypervisor 上配置的尚未与 Citrix Provisioning 站点关联的所有 Citrix Provisioning 站点的列表。使用该

列表可选择要应用 PVS 加速器的 Citrix Provisioning 站点。使用相同的 Citrix Hypervisor 服务器为相同的 Citrix Provisioning 站点运行该向导时将不显示此屏幕。

5. 单击下一步完成缓存配置。
6. 单击完成预配 Citrix Virtual Desktops 或流 VM，并将选定的 Citrix Provisioning 站点与 Citrix Hypervisor 中的 PVS 加速器相关联。完成此步骤后，**PVS** 加速器配置窗口中的查看 **PVS** 服务器按钮将在 XenCenter 中启用。单击查看 **PVS** 服务器按钮将显示与 Citrix Provisioning 站点关联的所有 PVS 服务器的 IP 地址。

## 缓存操作

使用 PVS 加速器功能时，请注意以下事项：

- XenCenter 和 Citrix Provisioning 中的 PVS 加速器用户界面仅在安装了 PVS 加速器补充包时呈现。
- Citrix Provisioning 目标设备能够识别其代理状态。安装该功能后，无需执行其他配置。
- 在部署了多个使用相同 VHD 的 Citrix Provisioning 服务器但具有不同文件系统时间戳的环境中，数据可能会多次缓存。由于存在此限制，因此，我们建议您为虚拟磁盘使用 VHDX 格式，而非 VHD 格式。
- 请勿将大端口范围用于 PVS 服务器通信。很少需要设置超过 20 个端口的范围。使用 PVS 加速器时，较端口范围会减慢数据包处理速度并增加 Citrix Hypervisor 控制域的启动时间。
- 启动启用了 PVS 加速器的 VM 后，VM 的缓存状态将在 XenCenter 中显示：
  - 在池或主机的 **PVS** 选项卡中
  - 在 VM 的常规选项卡中
- 可以在 XenCenter 中使用主机的性能选项卡中的 RRD 衡量指标确认 PVS 加速器的正确操作。有关详细信息，请参阅[监视和管理您的部署](#)。

### 重要：

- PVS 加速器要求 Citrix Provisioning 7.13 或更高版本。
- PVS 加速器适用于 Citrix Hypervisor Premium Edition 客户或通过 Citrix Virtual Desktops 和 Citrix Virtual Apps 授权访问 Citrix Hypervisor 的客户。
- PVS 加速器要求使用许可证服务器 11.14。
- PVS 加速器利用 OVS 的功能，因此在使用 Linux 桥接作为网络后端的主机上不可用。
- PVS 加速器在缓存的 VM 的第一个虚拟网络接口 (VIF) 上运行。因此，请将第一个 VIF 连接到 Citrix Provisioning 存储网络以使缓存功能运行。
- PVS 加速器当前不能在强制将 IP 绑定到某些 MAC 地址的网络端口上使用。此开关功能可能称为“IP 源保护”或类似的名称。在此类环境中，启用 PVS 加速器后，PVS 目标将无法启动，并出现错误“登录请求超时!”。

PVS 加速器功能缓存以下内容：

- 从虚拟磁盘中读取，但不写入到写入缓存或从中读取

- 基于映像版本。多个 VM 使用相同的映像版本时，这些 VM 将共享缓存的块。
- 使用任何非永久写入缓存类型的设备
- 访问模式为“标准映像”的虚拟磁盘。不适用于访问模式为“专用映像”的虚拟磁盘
- 标记为生产或“测试”类型的设备。不缓存标记为维护类型的设备

## PVS 加速器 CLI 操作

下一节介绍了使用 PVS 加速器时客户能够通过 CLI 执行的操作。客户还可以使用 XenCenter 执行这些操作。有关详细信息，请参阅 XenCenter 帮助。

查看 **Citrix Provisioning** 配置的 **Citrix Provisioning** 服务器地址和端口

PVS 加速器通过优化 VM 与 Citrix Provisioning 服务器之间的网络流量运行。在 Citrix Provisioning 服务器上完成配置时，Citrix Provisioning 服务器将使用其 IP 地址和端口填充 Citrix Hypervisor 上的 `pvs-server` 对象。PVS 加速器随后使用此信息专门优化 VM 与其 Citrix Provisioning 服务器之间的流量。可以使用以下命令列出所配置的 Citrix Provisioning 服务器：

```
1 xe pvs-server-list pvs-site-uuid=PVS_SITE_UUID params=all
```

## 配置 VM 以启用缓存

可以使用以下任意工具为 VM 启用 PVS 加速器：

- Citrix Provisioning CLI
- Citrix Virtual Desktops 设置向导
- 流 VM 设置向导
- XenCenter
- xe CLI

xe CLI 使用 VM 的 VIF 配置 PVS 加速器。它将创建一个 Citrix Provisioning 代理，该代理将 VM 的 VIF 与 Citrix Provisioning 站点链接。

要配置 VM，请运行以下命令：

1. 查找 VM 的第一个 VIF 以在其上启用缓存：

```
1 VIF_UUID=$(xe vif-list vm-name=label=pvsdevice_1 device=0 --  
minimal)
```

2. 创建 Citrix Provisioning 代理

```
1 xe pvs-proxy-create pvs-site-uuid=PVS_SITE_UUID vif-uuid=$VIF_UUID
```

## 对 VM 禁用缓存

可以通过销毁将 VM 的 VIF 与 `pvs-site` 链接的 Citrix Provisioning 代理为 VM 禁用 PVS 加速器。

1. 查找 VM 的第一个 VIF:

```
1 VIF_UUID=$(xe vif-list vm-name=label=pvsdevice_1 device=0 --minimal)
```

2. 查找 VM 的 Citrix Provisioning 代理:

```
1 PVS_PROXY_UUID=$(xe pvs-proxy-list vif-uuid=$VIF_UUID --minimal)
```

3. 销毁 Citrix Provisioning 代理:

```
1 xe pvs-proxy-destroy uuid=$PVS_PROXY_UUID
```

## 删除主机或站点的 PVS 加速器存储

要删除主机或站点的 PVS 加速器存储，请运行以下命令：

1. 查找要销毁其存储的主机:

```
1 HOST_UUID=$(xe host-list name=label=HOST_NAME --minimal)
```

2. 查找对象的 UUID:

```
1 PVS_CACHE_STORAGE_UUID=$(xe pvs-cache-storage-list host-uuid=$HOST_UUID --minimal)
```

3. 销毁对象:

```
1 xe pvs-cache-storage-destroy uuid=$PVS_CACHE_STORAGE_UUID
```

## 忘记站点的 PVS 加速器配置

要忘记站点的 PVS 加速器配置，请执行以下操作：

1. 查找 Citrix Provisioning 站点:

```
1 PVS_SITE_UUID=$(xe pvs-site-list name=label=My PVS Site)
```

2. 运行以下命令可忘记 Citrix Provisioning 站点:

```
1 xe pvs-site-forget uuid=$PVS_SITE_UUID
```

## 图形概述

June 4, 2019

本部分内容概述了 Citrix Hypervisor 的 3D 专业图形应用程序和工作站的虚拟交付。这些服务包括 GPU 直通（适用于 NVIDIA、AMD 和 Intel GPU）以及与 NVIDIA GRID™ vGPU™、AMD MxGPU™ 和 Intel GVT-g™ 共享的基于硬件的 GPU。

### GPU 直通

在虚拟化系统中，将共享大多数物理系统组件。这些组件由虚拟机管理程序表示为多个客户端对应的多个虚拟实例。直通 GPU 完全不抽象，但会保留一个物理设备。每个托管虚拟机 (VM) 都会获取自己的专用 GPU，消除了软件的抽象性以及随之产生的性能下降问题。

Citrix Hypervisor 允许您将（Citrix Hypervisor 服务器中的）物理 GPU 分配给同一主机上运行的 Windows 或 HVM Linux VM。此 GPU 直通功能面向图形高级用户（例如 CAD 设计师）。

### 共享 GPU

共享 GPU 允许多个 VM 同时使用一个物理 GPU。由于使用了一部分物理 GPU，因此性能高于仿真图形，并且不需要为每个 VM 配备一个图形卡。此功能实现了资源优化，提高了 VM 的性能。每个虚拟机的图形命令都直接传递到 GPU，不需要通过虚拟机管理程序进行转换。

### 许可注意事项

图形虚拟化适用于 Citrix Hypervisor Premium Edition 客户或通过其 Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。要了解有关 Citrix Hypervisor 版本以及如何升级的详细信息，请单击[此处](#)，访问 Citrix Web 站点。有关详细信息，请参阅[许可](#)。

### 供应商支持

下表列出了来宾支持的 GPU 和共享 GPU：

	适用于 Windows VM 的 GPU	适用于 HVM Linux VM 的 GPU	适用于 Windows VM 的共享 GPU	适用于 Linux VM 的虚拟 GPU
AMD	是		是	
Intel	是		是	
NVIDIA	是	是	是	是

可能需要供应商订阅或许可证，具体取决于使用的图形卡。

## vGPU 实时迁移

vGPU 实时迁移允许使用利用虚拟 GPU 执行实时迁移、存储实时迁移或 VM 挂起功能的 VM。可以迁移具有 vGPU 实时迁移功能的 VM，以避免出现停机。

通过 vGPU 实时迁移，您可以在托管启用了 vGPU 的 VM 的池上执行滚动池升级。有关详细信息，请参阅[滚动池升级](#)。

要使用 vGPU 实时迁移，您的 VM 必须在支持此功能的图形卡上运行，并且安装了 GPU 供应商提供的受支持的驱动程序。

使用 vGPU 实时迁移时受到以下限制：

- 不支持对早期版本的 Citrix Hypervisor 中的 VM 执行实时迁移。
- 实时迁移与 GPU 直通功能不兼容。
- VM 必须安装恰当的 vGPU 驱动程序才能支持任何 vGPU 实时迁移功能。必须为使用 vGPU 的所有来宾安装来宾内驱动程序。
- 迁移过程中不支持在 VM 上执行重新启动和关闭操作。这些操作会导致迁移失败。
- Linux VM 不支持任何 vGPU 实时迁移功能。
- 启用了 vGPU 的 VM 不支持通过 Workload Balancing 设备进行实时迁移。Workload Balancing 设备无法为连接了 vGPU 的 VM 执行容量规划。
- 使用 vGPU 实时迁移功能迁移 VM 后，来宾 VNC 控制台可能会损坏。在执行 vGPU 实时迁移操作后使用 ICA、RDP 或其他基于网络的方法来访问 VM。
- VDI 迁移使用实时迁移功能，因此主机上需要足够的 vGPU 空间才能在主机上备份 vGPU 实例。如果充分利用物理 GPU，则可能无法执行 VDI 迁移。

## 供应商支持

下表列出了对 vGPU 实时迁移功能的支持：

	适用于 Windows VM 的 GPRU	适用于 HVM Linux VM 的 GPU	适用于 Windows VM 的共享 GPU	适用于 Linux VM 的虚拟 GPU
NVIDIA			是	

有关支持此功能的图形卡的详细信息，请参阅本指南中特定于供应商的部分。客户可能需要供应商订阅或许可证，具体取决于使用的图形卡。

## 来宾支持和限制

Citrix Hypervisor 8.0 支持以下来宾操作系统使用虚拟 GPU。

### **NVIDIA vGPU**

Windows 来宾：

- Windows 7 (32 位/64 位)
- Windows 8.1 (32 位/64 位)
- Windows 10 (64 位)
- Windows Server 2008 R2 SP1 (64 位)
- Windows Server 2012 (64 位)
- Windows Server 2012 R2 (64 位)
- Windows Server 2016 (64 位)
- Windows Server 2019 (64 位)

HVM Linux 来宾：

- RHEL 7.x
- CentOS 7.x
- Ubuntu 14.04
- Ubuntu 16.04
- Ubuntu 18.04

### **AMD MxGPU**

Windows 来宾：

- Windows 7 SP1 (64 位)
- Windows 10 (64 位)
- Windows Server 2016 (64 位)
- Windows Server 2019 (64 位)

### **Intel GVT-g**

Windows 来宾：

- Windows 7 (32 位/64 位)
- Windows 8.1 (32 位/64 位)
- Windows 10 (64 位)
- Windows Server 2008 R2 SP1 (64 位)

- Windows Server 2012 R2 (64 位)
- Windows Server 2016 (64 位)

#### 限制

- Citrix Hypervisor 仅支持每个 VM 配备一个 GPU。
- 动态内存控制不支持配备了虚拟 GPU 的 VM。
- Citrix Hypervisor 会自动检测同一池中的各主机上完全相同的物理 GPU，并将其编组在一起。如果将某个 VM 分配给一组 GPU，该 VM 可以在池中具有该组内可用 GPU 的任何主机上启动。
- 可以在利用高可用性功能的环境中使用所有图形解决方案 (Nvidia vGPU、Intel GVT-d、Intel GVT-G、AMD MxGPU 和 vGPU 直通)。但是，不能通过高可用性功能保护使用这些图形解决方案的 VM。存在具有恰当的可用资源的主机时，可以在最大努力的基础上重新启动这些 VM。

## 准备主机以处理图形

July 10, 2019

本部分内容提供有关如何为受支持的图形虚拟化技术准备 Citrix Hypervisor 的分步说明。服务项目包括 NVIDIA GRID vGPU、AMD MxGPU 以及 Intel GVT-d 和 GVT-g。

### **NVIDIA GRID vGPU**

NVIDIA GRID vGPU 允许多个虚拟机 (VM) 同时直接访问单个物理 GPU。此 vGPU 使用在非虚拟化操作系统中部署的 NVIDIA 图形驱动程序。GRID 物理 GPU 可以支持多个虚拟 GPU 设备 (vGPU)。物理 GPU 必须受在 Citrix Hypervisor 控制域 (dom0) 中运行的 NVIDIA 的 GRID Virtual GPU Manager 控制，才能提供此支持。可以直接将 vGPU 分配给 VM。

VM 使用 GRID 虚拟 GPU 的方式与虚拟机管理程序直通的物理 GPU 类似。对于性能关键型快速路径，在 VM 中加载的 NVIDIA 驱动程序能够直接访问 GPU。该驱动程序还向 GRID Virtual GPU Manager 提供半虚拟化的界面。

NVIDIA GRID 与 Citrix Virtual Apps and Desktops 的 HDX 3D Pro 功能兼容。有关详细信息，请参阅[HDX 3D Pro](#)。

#### 许可注意事项

NVIDIA vGPU 适用于 Citrix Hypervisor Premium Edition 客户或通过其 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。要了解有关 Citrix Hypervisor 版本以及如何升级的详细信息，请单击[此处](#)，访问 Citrix Web 站点。有关详细信息，请参阅[许可](#)。

可能需要 NVIDIA 订阅或许可证，具体取决于使用的 NVIDIA 图形卡。

有关许可使用 NVIDIA 卡的信息，请参阅 [NVIDIA Web 站点](#)。

#### 可用的 **NVIDIA GRID vGPU** 类型

NVIDIA GRID 卡包含多个图形处理器 (GPU)。例如，TESLA M10 卡包含四个 GM107GL GPU，TESLA M60 卡包含两个 GM204GL GPU。每个物理 GPU 可以托管多个不同类型的虚拟 GPU (vGPU)。vGPU 类型具有固定数量的帧缓冲区、受支持的显示头数量和最大分辨率，并且适用于不同类型的工作负载。

有关最新支持的 NVIDIA 卡的列表，请参阅[硬件兼容性列表](#)和 [NVIDIA 产品信息](#)。

##### 注意：

同时托管在物理 GPU 上的 vGPU 的类型必须全部相同。但是，对同一个卡上的物理 GPU 没有相应的限制。此限制是自动的，可能会导致出现意外的容量规划问题。

例如，TESLA M60 卡有两个物理 GPU，可以支持 11 种 vGPU 类型：

- GRID M60-1A
- GRID M60-2A
- GRID M60-4A
- GRID M60-8A
- GRID M60-0B
- GRID M60-1B
- GRID M60-0Q
- GRID M60-1Q
- GRID M60-2Q
- GRID M60-4Q
- GRID M60-8Q

在同时启动 vGPU 类型为 M60-1A 的 VM 和 vGPU 类型为 M60-2A 的 VM 的情况下：

- 一个物理 GPU 仅支持 M60-1A 实例
- 另一个物理 GPU 仅支持 M60-2A 实例

无法在该单个卡上启动任何 M60-4A 实例。

#### **NVIDIA GRID** 系统要求

- NVIDIA GRID 卡：
  - 有关最新支持的 NVIDIA 卡的列表，请参阅[硬件兼容性列表](#)和 [NVIDIA 产品信息](#)。
- 可能需要 NVIDIA 订阅或许可证，具体取决于使用的 NVIDIA 图形卡。有关详细信息，请参阅 [NVIDIA 产品信息](#)。

- Citrix Hypervisor Premium Edition (或通过 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor)
- 能够托管 Citrix Hypervisor 和 NVIDIA GRID 卡的服务器。
- 适用于 Citrix Hypervisor 的 NVIDIA GRID vGPU 软件包，由适用于 Citrix Hypervisor 的 GRID Virtual GPU Manager 和 NVIDIA 驱动程序组成。
- 要在运行 NVIDIA vGPU 的 VM 中运行 Citrix Virtual Desktops，还需要：Citrix Virtual Desktops 7.6 或更高版本，完整安装。

注意：

请参阅可以从 [NVIDIA Web 站点](#) 获取的《NVIDIA GRID 虚拟 GPU 用户指南》(参考编号：DU-06920 001)。在 NVIDIA 中注册以访问这些组件。

### vGPU 实时迁移

Citrix Hypervisor 允许使用实时迁移、存储实时迁移，并且能够挂起和恢复启用了 NVIDIA GRID vGPU 的 VM。

要使用 vGPU 实时迁移、存储实时迁移或挂起功能，需满足以下要求：

- NVIDIA GRID 卡 Maxwell 系列或更高版本。
- 适用于启用了实时迁移的 Citrix Hypervisor 的 NVIDIA GRID Virtual GPU Manager。有关详细信息，请参阅 NVIDIA 文档。
- 安装了启用了 NVIDIA 实时迁移的 vGPU 驱动程序的 Windows VM。

vGPU 实时迁移允许在池内使用实时迁移、在池之间使用实时迁移以及使用存储实时迁移和启用了 vGPU 的 VM 的挂起/恢复。

### 准备概述

1. 安装 Citrix Hypervisor
2. 安装 NVIDIA GRID Virtual GPU Manager，适用于 Citrix Hypervisor
3. 重新启动 Citrix Hypervisor 服务器

### Citrix Hypervisor 上的安装

Citrix Hypervisor 可以从 [Citrix Hypervisor 下载](#) 页面下载。

安装以下对象：

- **Citrix Hypervisor 基础安装 ISO**
- **XenCenter Windows 管理控制台**

有关详细信息，请参阅[安装](#)。

### 许可注意事项

vGPU 适用于 Citrix Hypervisor Premium Edition 客户或通过其 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。要了解有关 Citrix Hypervisor 版本以及如何升级的详细信息，请单击[此处](#)，访问 Citrix Web 站点。有关详细信息，请参阅[许可](#)。

可能需要 NVIDIA 订阅或许可证，具体取决于使用的 NVIDIA 图形卡。有关详细信息，请参阅[NVIDIA 产品信息](#)。

有关许可使用 NVIDIA 卡的信息，请参阅 [NVIDIA Web 站点](#)。

### 安装 NVIDIA GRID vGPU Manager，适用于 Citrix Hypervisor

安装可以从 [NVIDIA](#) 获取的 NVIDIA GRID vGPU 软件。NVIDIA GRID 软件由以下组件组成：

- GRID vGPU Manager  
(例如：NVIDIA-vGPU-Citrix Hypervisor-7.2-367.64.x86\_64.rpm)
- Windows 显示驱动程序 (Windows 显示驱动程序取决于 Windows 版本)  
(例如：369.71\_grid\_win10\_server2016\_64bit\_international.exe)

*GRID vGPU Manager* 在 Citrix Hypervisor 控制域 (dom0) 中运行。该管理器以补充包或 RPM 文件的形式提供。有关安装的详细信息，请参阅 NVIDIA GRID vGPU 软件中包含的用户指南。

#### 注意：

示例包括更新、RPM 名称和版本，并且这些示例在您的环境中各不相同。

更新可以通过以下方法之一进行安装：

- 使用 XenCenter (工具 > 安装更新 > 从磁盘中选择更新或补充包)
- 使用 xe CLI 命令 `xe-install-update`。

更新的名称为 `NVIDIA-vGPU-PRODUCT_BRAND-7.2-367.64.x86_64.iso` 或类似的名称。

#### 注意：

如果要使用 RPM 文件安装 GRID vGPU Manager，请务必先将 RPM 文件复制到 dom0，然后再进行安装。

1. 使用 rpm 命令安装软件包：

```
1 rpm -iv NVIDIA-vGPU-PRODUCT_BRAND-7.2-367.64.x86_64.rpm
```

2. 重新启动 Citrix Hypervisor 服务器：

```
1 shutdown -r now
```

3. 重新启动 Citrix Hypervisor 服务器后，请通过检查 NVIDIA 内核驱动程序来验证是否已正确安装并加载 GRID 软件包：

```
1 [root@xenserver ~]#lsmod |grep nvidia
2     nvidia                8152994 0
3     i2c_core                20294 2 nvidia,i2c_i801
```

4. 确认 NVIDIA 内核驱动程序能够成功与您的主机中的 GRID 物理 GPU 通信。运行 `nvidia-smi` 命令以在您的平台中生成类似于以下内容的 GPU 列表：

```
1 [root@xenserver ~]# nvidia-smi
2
3 Thu Jan 26 13:48:50 2017
4 +-----+
5 NVIDIA-SMI 367.64 Driver Version: 367.64 |
6 -----+-----+
7 GPU Name Persistence-M| Bus-Id Disp.A | Volatile Uncorr.
8 Fan Temp Perf Pwr:Usage/Cap| Memory-Usage | GPU-Util
9 Compute M. |
10 =====+=====+=====
11 | 0 Tesla M60 On | 0000:05:00.0 Off | Off |
12 | N/A 33C P8 24W / 150W | 7249MiB / 8191MiB | 0%
13 | Default |
14 +-----+-----+-----+
15 | 1 Tesla M60 On | 0000:09:00.0 Off | Off |
16 | N/A 36C P8 24W / 150W | 7249MiB / 8191MiB | 0%
17 | Default |
18 +-----+-----+-----+
19 | 2 Tesla M60 On | 0000:85:00.0 Off | Off |
20 | N/A 36C P8 23W / 150W | 19MiB / 8191MiB | 0%
21 | Default |
22 +-----+-----+-----+
23 | 3 Tesla M60 On | 0000:89:00.0 Off | Off |
24 | N/A 37C P8 23W / 150W | 14MiB / 8191MiB | 0%
25 | Default |
26 +-----+-----+-----+
27 | Processes: GPU Memory |
```

24	GPU	PID	Type	Process name	Usage
25	=====				
26	No running compute processes found				
27	+-----				

注意：

在 RAM 大于 768 GB 的 Citrix Hypervisor 服务器中使用 NVIDIA vGPU 时，请将参数 `iommu=dom0-passthrough` 添加到 Xen 命令行：

a) 在控制域 (Dom0) 中运行以下命令：

```
/opt/xensource/libexec/xen-cmdline --set-xen iommu=dom0-passthrough
```

b) 重新启动主机。

## AMD MxGPU

AMD MxGPU 允许多个虚拟机 (VM) 使用单根 I/O 虚拟化直接访问单个物理 GPU 的一部分。可以在来宾内部使用在非虚拟化操作系统中部署的相同 AMD 图形驱动程序。

VM 使用 MxGPU GPU 的方式与虚拟机管理程序直通的物理 GPU 相同。对于性能关键型快速路径，在 VM 中加载的 AMD 图形驱动程序能够直接访问 GPU。

有关在 Citrix Hypervisor 中使用 AMD MxGPU 的详细信息，请参阅 [AMD 文档](#)。

### 许可注意事项

MxGPU 适用于 Citrix Hypervisor Premium Edition 客户或通过其 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。要了解有关 Citrix Hypervisor 版本以及如何升级的详细信息，请单击[此处](#)，访问 Citrix Web 站点。有关许可的详细信息，请参阅 [Citrix Hypervisor 许可常见问题解答](#)。

### 可用的 AMD MxGPU vGPU 类型

AMD MxGPU 卡可以包含多个 GPU。例如，S7150 卡包含一个物理 GPU，S7150x2 卡包含两个 GPU。每个物理 GPU 可以托管多个不同类型的虚拟 GPU (vGPU)。vGPU 类型将物理 GPU 拆分为预定义数量的 vGPU。其中的每个 vGPU 都具有相等份额的帧缓冲区以及图形处理能力。不同的 vGPU 类型适用于不同类别的工作负载。将物理 GPU 拆分为几个更小的块的 vGPU 类型更适用于密集型工作负载。

### 注意：

同时托管在物理 GPU 上的 vGPU 的类型必须全部相同。但是，对同一个卡上的物理 GPU 没有相应的限制。此限制是自动的，可能会导致出现意外的容量规划问题。

### AMD MxGPU 系统要求

- AMD FirePro S7100 系列 GPU
- Citrix Hypervisor Premium Edition（或通过 Citrix Virtual Desktops 或 Citrix Virtual Apps 授权访问 Citrix Hypervisor）
- 能够托管 Citrix Hypervisor 和 AMD MxGPU 卡的服务器。由 AMD 验证过的服务器的列表可以在 [AMD Web 站点](#) 上找到。
- 适用于 Citrix Hypervisor 的 AMD MxGPU 主机驱动程序。这些驱动程序可从 [AMD 下载站点](#) 获取。
- AMD FirePro 来宾内部驱动程序，适用于 Citrix Hypervisor 上的 MxGPU。这些驱动程序可从 [AMD 下载站点](#) 获取。
- 要在运行 AMD MxGPU 的 VM 中运行 Citrix Virtual Desktops，还需要：Citrix Virtual Desktops 7.13 或更高版本，完整安装。
- 配置为支持 SR-IOV 的系统 BIOS 和配置为辅助适配器的 MxGPU

### 准备概述

1. 安装 Citrix Hypervisor
2. 安装 AMD MxGPU 主机驱动程序，适用于 Citrix Hypervisor
3. 重新启动 Citrix Hypervisor 服务器

### Citrix Hypervisor 上的安装

Citrix Hypervisor 可以从 [Citrix Hypervisor 下载](#) 页面下载。

安装以下对象：

- **Citrix Hypervisor 8.0 基础安装 ISO**
- **XenCenter 8.0 Windows 管理控制台**

有关安装的详细信息，请参阅《[Citrix Hypervisor 安装指南](#)》。

## 安装 AMD MxGPU 主机驱动程序，适用于 Citrix Hypervisor

完成以下步骤以安装主机驱动程序。

1. 可以使用 XenCenter 或使用 xe CLI 安装包含驱动程序的更新。
  - 要使用 XenCenter 进行安装，请转至工具 > 安装更新 > 从磁盘中选择更新或补充包
  - 要使用 xe CLI 进行安装，请将更新复制到主机并在更新所在的目录中运行以下命令：

```
1 xe-install-supplemental-pack mxgpu-1.0.5.amd.iso
```

2. 重新启动 Citrix Hypervisor 服务器。
3. 重新启动 Citrix Hypervisor 服务器后，请验证是否已正确安装并加载 MxGPU 软件包。通过在 Citrix Hypervisor 服务器控制台中运行以下命令检查是否已加载 gim 内核驱动程序：

```
1 modinfo gim
2 modprobe gim
```

4. 确认 gim 内核驱动程序已成功创建 MxGPU 虚拟功能，这些功能将向来宾提供。运行以下命令：

```
1 lspci | grep "FirePro S7150"
```

此命令的输出将显示虚拟功能具有 S7150V 标识符。

5. 在 XenCenter 中使用“GPU”选项卡确认 MxGPU 虚拟 GPU 类型是否已在系统中作为可用类型列出。

安装 AMD MxGPU 驱动程序后，直通选项对 GPU 不再可用。请改为使用 **MxGPU.1** 选项。

### 创建启用了 MxGPU 的 VM

请先安装 VM，然后再将 VM 配置为使用 MxGPU。确保 AMD MxGPU 支持 VM 操作系统。有关详细信息，请参阅[来宾支持和限制](#)。

安装 VM 后，请按照[创建启用了 vGPU 的 VM](#) 中的说明进行操作，完成配置。

### Intel GVT-d 和 GVT-g

Citrix Hypervisor 支持 Intel 虚拟 GPU (GVT-g)，即一种不需要额外硬件的图形加速解决方案。它使用某些 Intel 处理器中嵌入的 Intel Iris Pro 功能，以及在 VM 内部安装的标准 Intel GPU 驱动程序。

Intel GVT-d 和 GVT-g 与 Citrix Virtual Apps and Desktops 的 HDX 3D Pro 功能兼容。有关详细信息，请参阅[HDX 3D Pro](#)。

**注意：**

由于处理器中嵌入了 Intel Iris Pro 图形功能，因此，CPU 密集型应用程序会导致电源从 GPU 转移。因此，您可能体验不到对纯 GPU 密集型工作负载所执行的完整图形加速功能。

### Intel GVT-g 系统要求和配置

要使用 Intel GVT-g，您的 Citrix Hypervisor 服务器必须具有以下硬件：

- 具有 Iris Pro 图形的 CPU。必须在[硬件兼容性列表](#)中将此 CPU 作为图形支持的 CPU 列出
- 配备了启用了图形的芯片组的主板。例如，适用于 Xeon E3 v4 CPU 的 C226，或适用于 Xeon E3 v5 CPU 的 C236。

**注意：**

在 Intel GPU 直通 (GVT-d) 与 Intel 虚拟 GPU (GVT-g) 之间切换时，请务必重新启动主机。

配置 Intel GVT-g 时，特定 Citrix Hypervisor 服务器上支持的 Intel 虚拟 GPU 的数量取决于其 GPU 条大小。GPU 条大小在 BIOS 中称为“Aperture 大小”。我们建议您将 Aperture 大小设置为 1024 MB，以支持每个主机最多配备七个虚拟 GPU。

如果将 Aperture 大小配置为 256 MB，则只有一个 VM 能够在主机上启动。将其设置为 512 MB 会导致只有三个 VM 在 Citrix Hypervisor 服务器上启动。超过 1024 MB 的 Aperture 大小不受支持，并且不增加在主机上启动的 VM 数量。

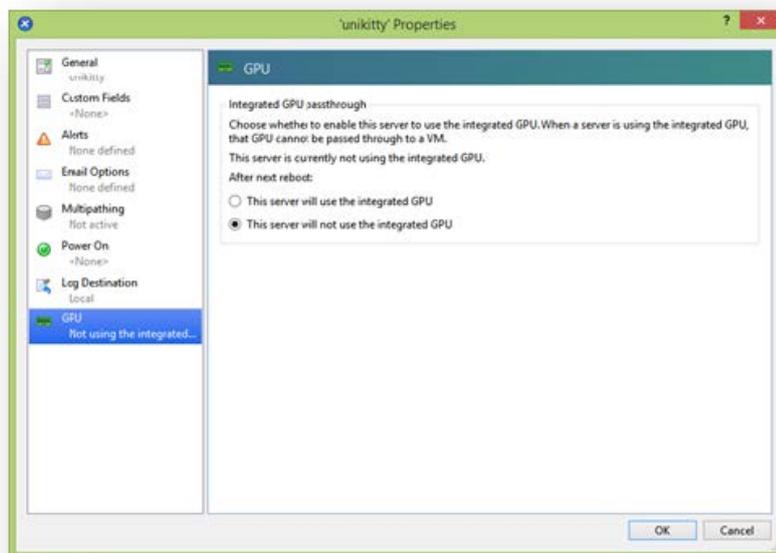
### 启用 Intel GPU 直通

Citrix Hypervisor 支持对使用 Intel 集成 GPU 设备的 Windows 7 和 Windows 8.1 (32/64 位) 使用 GPU 直通功能。有关支持的硬件的详细信息，请参阅[硬件兼容性列表](#)。

在 Intel 服务器上使用 Intel GPU 时，Citrix Hypervisor 服务器的控制域 (dom0) 将有权访问集成 GPU 设备。在此类情况下，GPU 可用于直通。要在 Intel 服务器上使用 Intel GPU 直通功能，请在将 GPU 传递到 VM 之前禁用 dom0 与 GPU 之间的连接。

要禁用此连接，请完成以下步骤：

1. 在资源窗格中，选择 Citrix Hypervisor 服务器。
2. 在常规选项卡上，单击属性，然后单击左侧窗格中的 **GPU**。
3. 在集成 **GPU** 直通部分中，选择此服务器将不使用集成 **GPU**。



此步骤将禁用 dom0 与 Intel 集成 GPU 设备之间的连接。

4. 单击确定。
5. 重新启动 Citrix Hypervisor 服务器以使更改生效。

Intel GPU 现在将在创建新 VM 过程中在“GPU 类型”列表中以及 VM 的属性选项卡中显示。

注意：

禁用 dom0 与 GPU 之间的连接后，Citrix Hypervisor 服务器的外部控制台输出（例如 VGA、HDMI、DP）将不可用。

## 创建启用了 vGPU 的 VM

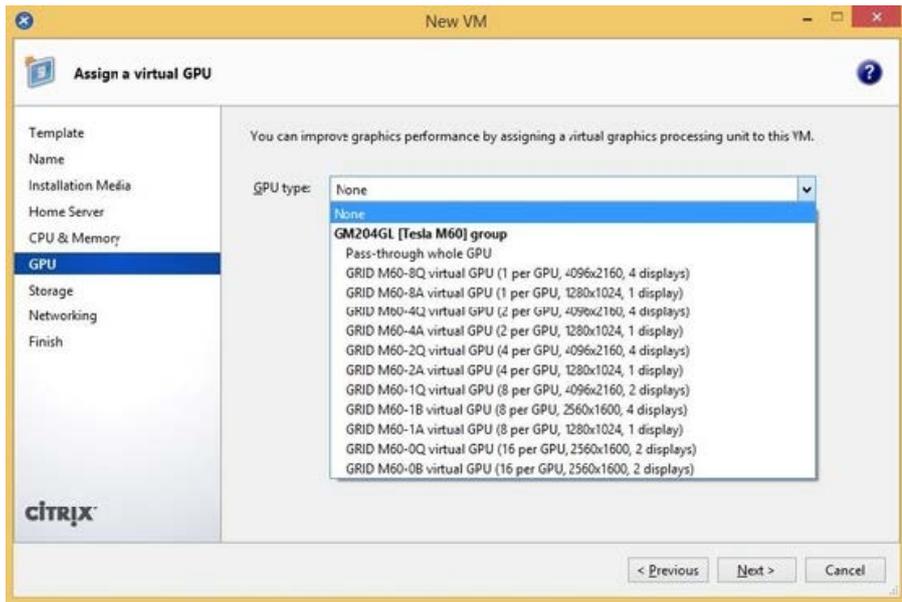
July 10, 2019

本部分内容介绍有关如何创建启用了虚拟 GPU 或 GPU 直通功能的 VM 的分步说明。

注意：

如果要使用 Intel GPU 直通功能，请先查看启用 *Intel GPU* 直通功能部分以了解更多配置，然后完成以下步骤。

1. 使用 XenCenter 创建一个 VM。在“资源”窗格中选择主机，然后在“VM”菜单中选择新建 **VM**。
2. 按照新建 **VM** 配置中的说明进行操作，选择安装介质、主服务器、**CPU** 和内存。
3. 启用了 GPU 的服务器将显示 **GPU** 配置页面：



4. 在 **GPU** 类型列表中，选择在整个 **GPU** 中直通或虚拟 GPU 类型。  
不可用的虚拟 GPU 类型显示为灰色。
5. 单击下一步配置存储，然后单击网络连接。
6. 完成配置后，单击立即创建。

## 安装 Citrix VM Tools

### 1. 安装 Citrix VM Tools

如果没有 Citrix VM Tools 提供的优化网络连接和存储驱动程序，GRID vGPU 上运行的远程图形应用程序将不提供最高性能。

- a) 在资源窗格中选择 VM，单击鼠标右键，然后单击快捷菜单中的安装 **Citrix VM Tools**。或者，在 **VM** 菜单中，单击安装 **Citrix VM Tools**。
- b) 单击消息对话框中的安装 **Citrix VM Tools** 以转至 VM 的控制台并开始进行安装。
- c) 如果针对 VM 的 CD/DVD 驱动器启用了自动播放功能，则片刻之后安装过程将自动启动。此过程将安装 I/O 驱动程序和管理代理。在系统提示时，重新启动 VM，以使 VM 处于优化状态。如果未启用自动播放功能，Citrix VM Tools 安装程序将显示安装选项。单击安装 **Citrix VM Tools** 继续进行安装。此操作将在 VM 的 CD/DVD 驱动器上装载 Citrix VM Tools ISO (guest-tools.iso)。
- d) 单击 **Run setup.exe** (运行 setup.exe) 开始安装 Citrix VM Tools，在系统提示时，重新启动 VM，以使 VM 处于优化状态。

## 安装来宾内部的驱动程序

在 XenCenter 中查看 VM 控制台时，VM 通常引导至处于 VGA 模式、分辨率为 800 x 600 的桌面。可以使用标准 Windows 屏幕分辨率控件将分辨率增加到其他标准分辨率。（控制面板 > 显示 > 屏幕分辨率）

### 注意：

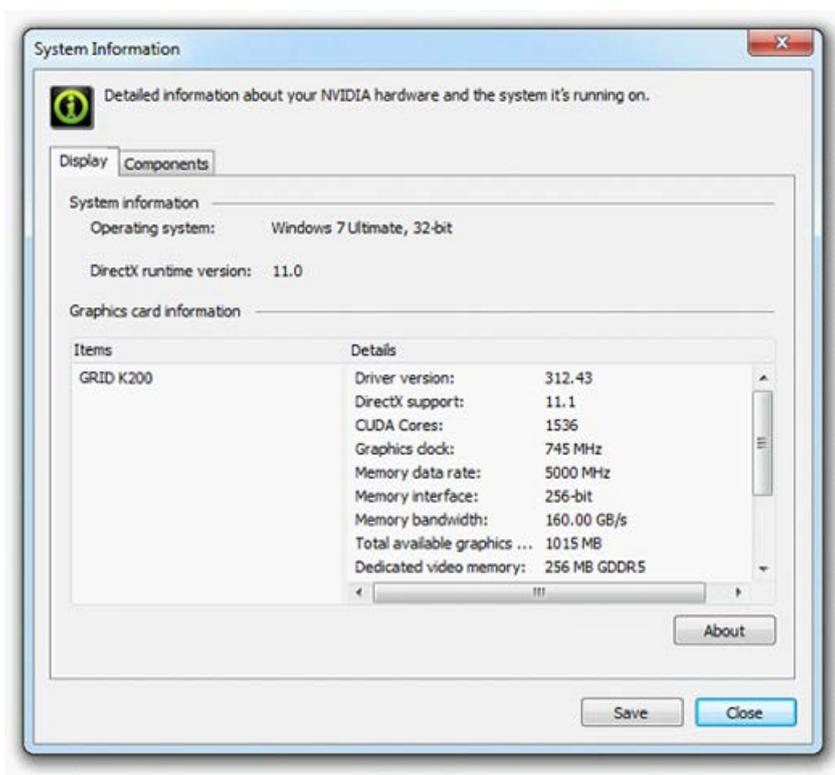
使用 GPU 直通或 MxGPU 时，我们建议您在连接到网络时通过 RDP 或 VNC 安装来宾内部的驱动程序。即，不通过 XenCenter。

## 安装 **NVIDIA** 驱动程序

要启用 vGPU 操作（与物理机 NVIDIA GPU 相同），请在 VM 中安装 NVIDIA 驱动程序。

以下部分提供该过程的概述。有关详细说明，请参阅《NVIDIA 用户指南》。

1. 启动 VM。在资源窗格中，在 VM 上单击鼠标右键，然后单击启动。  
在此启动过程中，Citrix Hypervisor 会动态地将 vGPU 分配给 VM。
2. 按照 Windows 操作系统安装屏幕进行操作。
3. 操作系统安装完成后，重新启动 VM。
4. 安装适用于来宾内部的 GPU 的恰当驱动程序。下例显示了面向 NVIDIA GRID 驱动程序的来宾内安装的特定用例。
5. 将 32 位或 64 位 NVIDIA Windows 驱动程序软件包复制到 VM 中，打开 zip 文件，然后运行 setup.exe。
6. 按照安装程序步骤安装驱动程序。
7. 驱动程序安装完成后，系统可能会提示您重新启动 VM。选择立即重启立即重新启动 VM，或者，退出安装程序软件包，然后在准备就绪时重新启动 VM。VM 启动时，将引导至 Windows 桌面。
8. 要验证该 NVIDIA 驱动程序是否正在运行，请在桌面上单击鼠标右键并选择 **NVIDIA** 控制面板。
9. 在 NVIDIA 控制面板中，选择系统信息。此界面将显示 VM 正在使用的 GPU 类型、其功能以及正在使用的 NVIDIA 驱动程序版本：



注意：

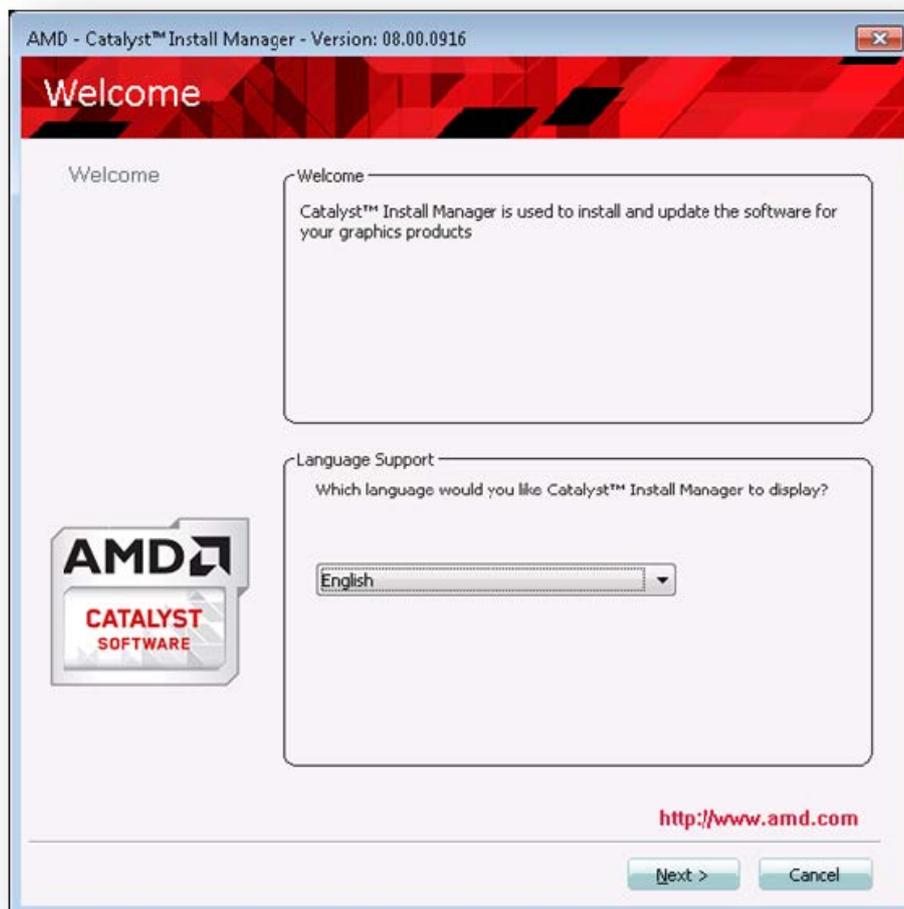
可能需要 NVIDIA 订阅或许可证，具体取决于使用的 NVIDIA 图形卡。有关详细信息，请参阅 [NVIDIA 产品信息](#)。

VM 现在已准备好运行 GPU 支持的完整 DirectX 和 OpenGL 图形应用程序。

## 安装 AMD 驱动程序

要启用 GPU 操作，请在 VM 中安装 AMD 驱动程序。

1. 启动 VM。在资源窗格中，在 VM 上单击鼠标右键，然后单击启动。  
在此启动过程中，Citrix Hypervisor 会动态地将 GPU 分配给 VM。
2. 按照 Windows 操作系统安装屏幕进行操作。
3. 操作系统安装完成后，重新启动 VM。
4. 将 32 位或 64 位 AMD Windows 驱动程序（AMD Catalyst 安装管理器）复制到 VM 中。
5. 运行 AMD Catalyst 安装管理器；选择目标文件夹，然后单击安装。



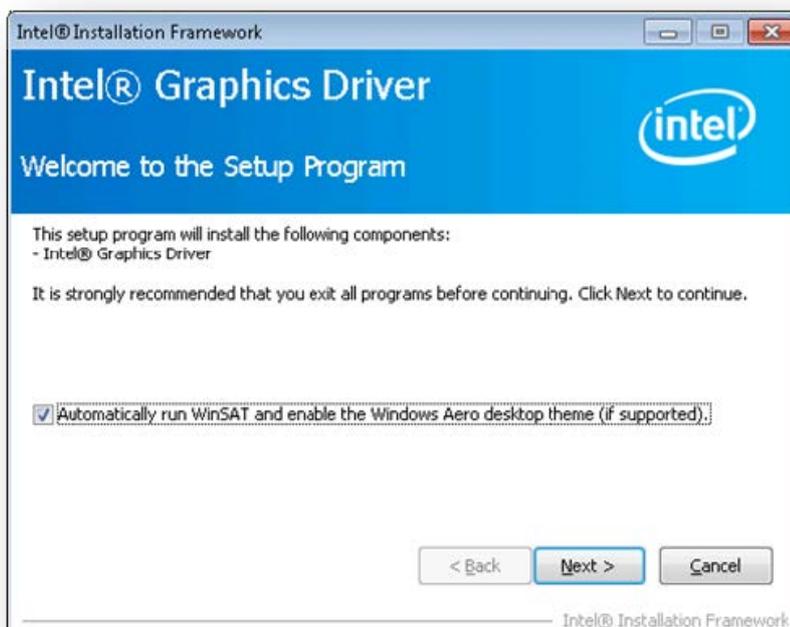
6. 按照安装程序步骤安装驱动程序。
7. 要完成安装，请重新启动 VM。
8. 重新启动 VM 后，检查图形是否正常运行。打开 **Windows** 设备管理器，展开显示适配器，并确保 AMD 图形适配器没有任何警告符号。

### 安装 Intel 驱动程序

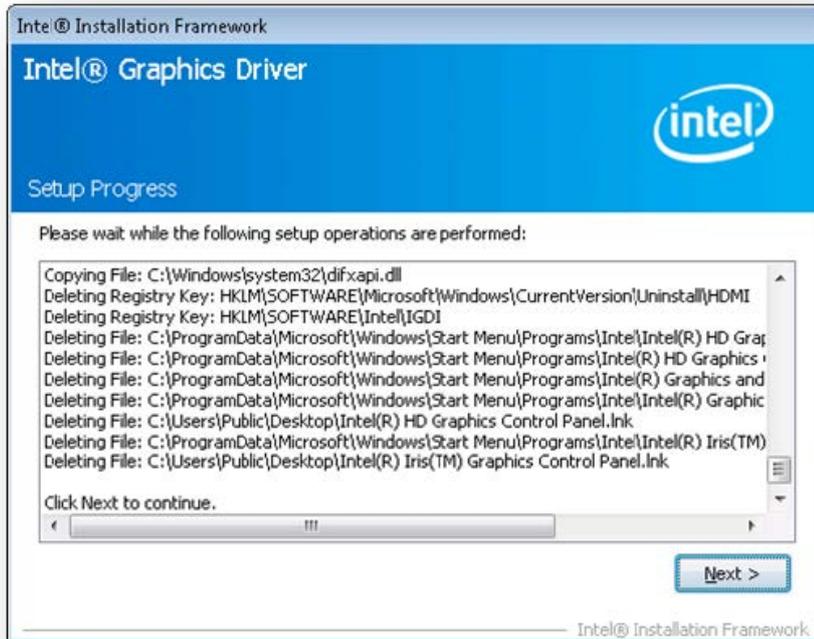
要启用 GPU 操作，请在 VM 中安装 Intel 驱动程序。

1. 启动 **VM**。在资源窗格中，在 VM 上单击鼠标右键，然后单击启动。  
在此启动过程中，Citrix Hypervisor 会动态地将 GPU 分配给 VM。
2. 按照 Windows 操作系统安装屏幕进行操作。
3. 操作系统安装完成后，重新启动 VM。

4. 将 32 位或 64 位 Intel Windows 驱动程序（Intel 图形驱动程序）复制到 VM 中。
5. 运行 **Intel** 图形驱动程序安装程序
6. 选择自动运行 **WinSAT**，然后单击下一步。



7. 要接受许可协议，请单击是，并在“自述文件信息”屏幕中，单击下一步。
8. 等到安装操作完成。系统提示时，单击下一步。



9. 要完成安装，系统将提示您重新启动 VM。选择是，我希望立即重新启动此计算机，然后单击完成。
10. 重新启动 VM 后，检查图形是否正常运行。打开“Windows 设备管理器”，展开显示适配器，并确保 Intel 图形适配器没有任何警告符号。

注意：

可以从 [Intel Web 站点](#) 获取最新的驱动程序。

## 内存使用率

June 4, 2019

Citrix Hypervisor 服务器的内存占用由两部分构成。首先，是 Xen 虚拟机管理程序本身占用的内存。其次，是主机的控制域占用的内存。控制域也称为“Domain0”或“dom0”，是一个运行 Citrix Hypervisor 管理 Toolstack (XAPI) 的享有特权的安全 Linux VM。除了提供 Citrix Hypervisor 管理功能之外，控制域还运行驱动程序堆栈，提供对物理设备的用户创建 VM 访问。

## 控制域内存

分配给控制域的内存量可以自动调整，并且基于物理主机上的物理内存量。默认情况下，Citrix Hypervisor 将 **1 GiB** 加上总物理内存的 **5%** 分配给控制域，最大达 8 GiB。

### 注意：

在 XenCenter 的 Citrix Hypervisor 部分中报告的内存量包括由控制域 (dom0)、Xen 虚拟机管理程序本身和崩溃内核占用的内存量。因此，在 XenCenter 中报告的内存量可能会超过这些值。对于使用更多内存的主机来说，虚拟机管理程序占用的内存量更大。

## 更改分配给控制域的内存量

可以使用 XenCenter 或命令行更改分配给 dom0 的内存量。如果将分配给控制域的内存量增加到超过默认分配的量，这将导致 VM 的可用内存减少。

### 使用 XenCenter 更改 dom0 内存

有关使用 XenCenter 更改 dom0 内存的信息，请参阅 XenCenter 文档中的[更改控制域内存](#)。

### 注意：

不能使用 XenCenter 将 dom0 内存降低到低于最初在 Citrix Hypervisor 安装过程中设置的值。必须使用命令行进行此更改。

### 使用命令行更改 dom0 内存

### 注意：

在内存较小（小于 16 GiB）的主机上，您可能希望将分配给控制域的内存降低到小于在安装过程中设置的默认值。可以使用命令行进行此更改。但是，我们建议您不要将 **dom0** 内存减小到 **1 GiB** 以下，并建议您在支持团队的指导下执行此操作。

1. 在 Citrix Hypervisor 服务器上，打开本地 shell，以 root 用户身份登录。
2. 键入以下命令：

```
1 /opt/xensource/libexec/xen-cmdline --set-xen dom0_mem=<nn>M,max:<nn>M
```

其中 <nn> 代表要分配给 dom0 的内存量（以 MiB 为单位）。

3. 在 xsconsole 上使用 XenCenter 或 `reboot` 命令重新启动 Citrix Hypervisor 服务器。

当该主机重新启动时，在 xsconsole 上，运行 `free` 命令以验证新的内存设置。

## VM 的可用内存量有多少？

要了解可分配给 VM 的主机内存量，请运行 `memory-free` 以获取主机的可用内存值。然后键入命令 `vm-compute-maximum-memory` 以获取可分配给 VM 的实际可用内存量。例如：

```
1 xe host-list uuid=host_uuid params=memory-free
2 xe vm-compute-maximum-memory vm=vm_name total=host_memory_free_value
```

## 监视和管理您的部署

June 4, 2019

Citrix Hypervisor 会提供详细的性能指标监视数据，包括 CPU、内存、磁盘、网络、C-state/P-state 信息以及存储。适用情况下，会针对每个主机和每个 VM 提供这些指标。这些指标可以直接获取，也可以在 XenCenter 或其他第三方应用程序中以图形方式进行访问和查看。

Citrix Hypervisor 也提供系统和性能警报。警报是指为响应选定系统事件而发出的通知。当以下值之一超出在托管主机、VM 或存储库上的指定阈值时，也会发出这些通知：CPU 使用率、网络使用率、内存使用率、控制域内存使用率、存储吞吐量或 VM 磁盘使用量。您可以使用 xe CLI 或 XenCenter 来配置警报。要根据任何可用的主机或 VM 性能指标创建通知，请参阅性能警报。

## 监视 Citrix Hypervisor 性能

客户可以使用通过轮询数据库 (RRD) 公布的指标，监视其 Citrix Hypervisor 服务器和虚拟机 (VM) 的性能。这些指标可以通过 HTTP 或通过 RRD2CSV 工具进行查询。此外，XenCenter 还将使用这些数据生成系统性能图表。有关详细信息，请参阅分析和显示指标。

下表列出了所有可用的主机和 VM 指标。

### 注意：

- 某个时间段内的延迟被定义为此时间段中的平均操作延迟。
- 某些指标的可用性和实用性取决于 SR 和 CPU。
- 性能指标不适用于 GFS2 SR 以及这些 SR 上的磁盘。

### 可用主机指标

指标名称	说明	条件	XenCenter 名称
avgqu_sz_<sr-uuid-short>	平均 I/O 队列大小 (请求)。	主机上的 SR <sr-uuid-short> 中至少有一个插入的 VBD	sr-uuid-short 队列大小
cpu<cpu>-C<cstate>	CPU cpu 处于 C-state cstate 的时间 (以毫秒为单位)。	C-state 存在于 CPU 上	CPU cpu 处于 C-state cstate
cpu<cpu>-P<pstate>	CPU cpu 处于 P-state pstate 的时间 (以毫秒为单位)。	P-state 存在于 CPU 上	CPU cpu 处于 p-state pstate
cpu<cpu>	物理 CPU cpu 的利用率 (片段)。默认情况下启用。	CPU cpu 存在	CPU cpu
cpu_avg	物理 CPU 的平均利用率 (片段)。默认情况下启用。	无	平均 CPU 使用率
inflight_<sr-uuid-short>	当前正在进行的 I/O 请求。默认情况下启用。	主机上的 SR sr 中至少有一个插入的 VBD	sr 传输请求
io_throughput_read_<sr-uuidshort>	从 SR 读取的数据 (MiB/秒)。	主机上的 SR sr 中至少有一个插入的 VBD	sr 读取吞吐量
io_throughput_write_<sr-uuidshort>	写入 SR 的数据 (MiB/秒)。	主机上的 SR sr 中至少有一个插入的 VBD	sr 写入吞吐量
io_throughput_total_<sr-uuidshort>	所有 SR I/O (MiB/秒)。	主机上的 SR sr 中至少有一个插入的 VBD	sr 总吞吐量
iops_read_<sr-uuid-short>	每秒读取请求数。	主机上的 SR sr 中至少有一个插入的 VBD	sr 读取 IOPS
iops_write_<sr-uuid-short>	每秒写入请求数。	主机上的 SR sr 中至少有一个插入的 VBD	sr 写入 IOPS
iops_total_<sr-uuid-short>	每秒 I/O 请求数。	主机上的 SR sr 中至少有一个插入的 VBD	sr 总 IOPS
iowait_<sr-uuid-short>	I/O 等待时间百分比。	主机上的 SR sr 中至少有一个插入的 VBD	sr IO 等待
latency_<sr-uuid-short>	平均 I/O 延迟 (毫秒)。	主机上的 SR sr 中至少有一个插入的 VBD	sr 延迟
loadavg	Domain0 的平均负载。默认情况下启用	无	控制域负载

指标名称	说明	条件	XenCenter 名称
<code>memory_free_kib</code>	可用内存总量 (KiB)。默认情况下启用。	无	可用内存
<code>memory_reclaimed</code>	通过腾出回收的主机内存 (B)。	无	回收的内存
<code>memory_reclaimed_max</code>	通过腾出回收的可用主机内存 (B)。	无	潜在回收的内存
<code>memory_total_kib</code>	主机中的内存总量 (KiB)。默认情况下启用。	无	总内存
<code>network/latency</code>	从本地主机传输到所有在线主机的最后两个检测信号之间的时间间隔 (以秒为单位)。默认情况下禁用。	已启用高可用性	网络延迟
<code>statefile/&lt;t&gt;/latency</code>	从本地主机访问的最新状态文件的周转时间 (以秒为单位)。默认情况下禁用。	已启用高可用性	高可用性状态文件延迟
<code>pif_&lt;pif&gt;_rx</code>	物理接口上每秒接收的字节数 <code>pif</code> 。默认情况下启用。	PIF 存在	XenCenter- <code>pifname</code> 接收 (见注释)
<code>pif_&lt;pif&gt;_tx</code>	物理接口上每秒发送的字节数 <code>pif</code> 。默认情况下启用。	PIF 存在	XenCenter- <code>pifname</code> 发送 (见注释)
<code>pif_&lt;pif&gt;_rx_errors</code>	物理接口 <code>pif</code> 上每秒发生的接收错误数。默认情况下禁用。	PIF 存在	XenCenter- <code>pifname</code> 接收错误数 (见注释)
<code>pif_&lt;pif&gt;_tx_errors</code>	物理接口 <code>pif</code> 上每秒发生的传输错误数。默认情况下禁用	PIF 存在	XenCenter- <code>pifname</code> 发送错误 (见注释)
<code>pif_aggr_rx</code>	所有物理接口上每秒接收的字节数。默认情况下启用。	无	NIC 接收的总数据量
<code>pif_aggr_tx</code>	所有物理接口上每秒发送的字节数。默认情况下启用。	无	NIC 发送的总数据量

指标名称	说明	条件	XenCenter 名称
<code>pvsaccelerator_evicted_bytes</code>	每秒钟从缓存中逐出的字节数	已启用 PVS 加速器	PVS 加速器逐出率
<code>pvsaccelerator_read_hits</code>	每秒钟从缓存送达的读取次数	已启用 PVS 加速器	PVS 加速器命中率
<code>pvsaccelerator_read_misses</code>	每秒钟无法从缓存送达的读取次数	已启用 PVS 加速器	PVS 加速器未命中率
<code>pvsaccelerator_traffic_client</code>	缓存的 PVS 客户端每秒钟发送的字节数	已启用 PVS 加速器	PVS 加速器观察到的来自客户端的网络流量
<code>pvsaccelerator_traffic_server</code>	缓存的 PVS 服务器每秒钟发送的字节数	已启用 PVS 加速器	PVS 加速器观察到的来自服务器的网络流量
<code>pvsaccelerator_read_rate</code>	缓存每秒钟观察到的读取次数	已启用 PVS 加速器	PVS 加速器观察到的读取速率
<code>pvsaccelerator_traffic</code>	PVS 加速器 (而非 PVS 服务器) 每秒钟发送的字节数	已启用 PVS 加速器	PVS 加速器保存的网络流量
<code>pvsaccelerator_space_utilization</code>	此主机上的 PVS 加速器使用的空间所占的百分比 (与缓存存储的总大小相比)	已启用 PVS 加速器	PVS 加速器空间利用率
<code>sr_&lt;sr&gt;_cache_size</code>	IntelliCache SR 的大小 (以字节为单位)。默认情况下启用。	已启用 IntelliCache	IntelliCache 缓存大小
<code>sr_&lt;sr&gt;_cache_hits</code>	每秒缓存命中率。默认情况下启用。	已启用 IntelliCache	IntelliCache 缓存命中数
<code>sr_&lt;sr&gt;_cache_misses</code>	每秒缓存错失率。默认情况下启用。	已启用 IntelliCache	IntelliCache 缓存未命中数
<code>xapi_allocation_kib</code>	XAPI 守护程序完成的内存 (KiB) 分配。默认情况下启用。	无	代理内存分配
<code>xapi_free_memory_kib</code>	XAPI 守护程序的可用内存 (KiB)。默认情况下启用。	无	可用代理内存

指标名称	说明	条件	XenCenter 名称
<code>xapi_healthcheck/latency_health</code>	本地主机上最新 XAPI 状态监视调用的周转时间 (以秒为单位)。默认情况下禁用	已启用高可用性	Citrix Hypervisor 运行状况检查延迟
<code>xapi_live_memory_ki</code>	XAPI 守护程序占用的实时内存 (KiB)。默认情况下启用。	无	活动代理内存
<code>xapi_memory_usage_</code>	XAPI 守护程序占用的已分配总内存 (KiB)。默认情况下启用。	无	代理内存使用率

#### 可用 VM 指标

指标名称	说明	条件	XenCenter 名称
<code>cpu&lt;cpu&gt;</code>	vCPU <code>cpu</code> 的利用率 (片段)。默认情况下启用	vCPU <code>cpu</code> 存在	CPU
<code>memory</code>	当前分配给 VM 的内存 (以字节为单位)。默认情况下启用	无	总内存
<code>memory_target</code>	VM 气球驱动程序的目标 (以字节为单位)。默认情况下启用	无	内存目标
<code>memory_internal_fre</code>	按来宾系统代理报告使用的内存 (KiB)。默认情况下启用	无	可用内存
<code>runstate_fullrun</code>	所有 vCPU 运行的时间片段。	无	vCPU 完全运行
<code>runstate_full_conte</code>	所有 vCPU 的可运行时间片段 (即, 等待 CPU)	无	vCPU 完全争用
<code>runstate_concurrer</code>	有些 vCPU 正在运行和有些 vCPU 可运行的时间片段	无	vCPU 并发危险
<code>runstate_blocked</code>	所有 vCPU 受阻或处于脱机状态的时间片段	无	vCPU 空闲

指标名称	说明	条件	XenCenter 名称
<code>runstate_partial_r</code>	有些 vCPU 正在运行和有些 vCPU 受阻的时间片段	无	vCPU 部分运行
<code>runstate_partial_co</code>	有些 vCPU 可运行和有些 vCPU 受阻的时间片段	无	vCPU 部分争用
<code>vbd_&lt;vbd&gt;_write</code>	写入设备 <code>vbd</code> 的次数 (以字节数/秒为单位)。默认情况下启用	VBD <code>vbd</code> 存在	磁盘 <code>vbd</code> 写入
<code>vbd_&lt;vbd&gt;_read</code>	从设备 <code>vbd</code> 读取的次数 (以字节数/秒为单位)。默认情况下启用。	VBD <code>vbd</code> 存在	磁盘 <code>vbd</code> 读取
<code>vbd_&lt;vbd&gt;_write_latency</code>	写入设备 <code>vbd</code> 的次数 (以毫秒为单位)。	VBD <code>vbd</code> 存在	磁盘 <code>vbd</code> 写入延迟
<code>vbd_&lt;vbd&gt;_read_latency</code>	从设备 <code>vbd</code> 读取的次数 (以毫秒为单位)。	VBD <code>vbd</code> 存在	磁盘 <code>vbd</code> 读取延迟
<code>vbd &lt;vbd&gt;_iops_read</code>	每秒读取请求数。	主机上的非 ISO VDI 至少有一个插入的 VBD	磁盘 <code>vbd</code> 读取 IOPS
<code>vbd &lt;vbd&gt;_iops_write</code>	每秒写入请求数。	主机上的非 ISO VDI 至少有一个插入的 VBD	磁盘 <code>vbd</code> 写入 IOPS
<code>vbd &lt;vbd&gt;_iops_total</code>	每秒 I/O 请求数。	主机上的非 ISO VDI 至少有一个插入的 VBD	磁盘 <code>vbd</code> 总 IOPS
<code>vbd &lt;vbd&gt;_iowait</code>	I/O 等待时间百分比。	主机上的非 ISO VDI 至少有一个插入的 VBD	磁盘 <code>vbd</code> IO 等待
<code>vbd &lt;vbd&gt;_inflight</code>	当前正在进行的 I/O 请求。	主机上的非 ISO VDI 至少有一个插入的 VBD	磁盘 <code>vbd</code> 传输请求
<code>vbd &lt;vbd&gt;_avgqu_sz</code>	平均 I/O 队列大小。	主机上的非 ISO VDI 至少有一个插入的 VBD	磁盘 <code>vbd</code> 队列大小
<code>vif_&lt;vif&gt;_rx</code>	虚拟接口号 <code>vif</code> 上每秒接收的字节数。默认情况下启用。	VIF <code>vif</code> 存在	<code>vif</code> 接收
<code>vif_&lt;vif&gt;_tx</code>	在虚拟接口 <code>vif</code> 上每秒传输的字节数。默认情况下启用。	VIF <code>vif</code> 存在	<code>vif</code> 发送

指标名称	说明	条件	XenCenter 名称
<code>vif_&lt;vif&gt;_rx_errors</code>	虚拟接口 <code>vif</code> 上每秒发生的接收错误数。默认情况下启用。	VIF <code>vif</code> 存在	<code>vif</code> 接收错误数
<code>vif_&lt;vif&gt;_tx_errors</code>	虚拟接口 <code>vif</code> 上每秒发生的传输错误数。默认情况下处于启用状态。	VIF <code>vif</code> 存在	<code>vif</code> 发送错误数

注意：

`<XenCenter-pif-name>` 的值可能为以下任意一项：

```
|||
|-----|-----|
| NIC <pif> | If <pif> contains pif_eth#, where ## is 0-9 |
| <pif> | If <pif> contains pif_eth### or pif_xenbr## or pif_bond## |
| <Internal> Network <pif> | If <pif> contains pif_xapi##, (note that <Internal> appears as is) |
| TAP <tap> | If <pif> contains pif_tap## |
| xapi Loopback | If <pif> contains pif_lo |
```

## 分析和显示指标

XenCenter 中的“性能”选项卡提供整个资源池性能的实时监视统计数据，并以图表方式显示虚拟机和物理机性能的趋势。默认情况下，显示 CPU、内存、网络和磁盘 I/O 的图表包含在“性能”选项卡上。您可以添加更多指标，更改现有图表的外观或创建额外的图表。有关详细信息，请参阅以下部分中的配置指标。

- 可以查看最长 12 个月的性能数据，并可将数据放大，以便更清楚地查看活动高峰。
- 当服务器、VM 或 SR 上的 CPU、内存、网络 I/O、存储 I/O 或磁盘 I/O 使用率超过指定阈值时，XenCenter 会生成性能警报。有关详细信息，请参阅以下部分中的警报。

注意：

安装 Citrix VM Tools（半虚拟化的驱动程序）即可查看完整的 VM 性能数据。

## 配置性能图表

要添加图表，请执行以下操作：

1. 在性能选项卡上，单击操作，然后单击新建图表。此时将显示“新建图表”对话框。
2. 在名称字段中，输入图表的名称。
3. 从数据源列表中，选择图表中要包含的数据源所对应的复选框。

4. 单击保存。

要编辑现有图表，请执行以下操作：

1. 导航到性能选项卡，然后选择要修改的图表。
2. 在图表上单击鼠标右键，选择操作，或者单击操作按钮。然后选择编辑图表。
3. 在“图表详细信息”窗口中，执行必要更改，然后单击确定。

#### 配置图表类型

可以采用折线图或面积图的形式来显示性能图表中的数据。要更改图表类型，请执行以下操作：

1. 在工具菜单上，单击选项，选择图表。
2. 要以折线图形式查看性能数据，请单击折线图选项。
3. 要以面积图形式查看性能数据，请单击面积图选项。
4. 单击确定以保存更改。

有关配置和查看 XenCenter 性能图表的详细信息，请参阅监视系统性能中的“XenCenter 帮助”部分。

#### 配置指标

注意：

C-state 和 P-state 是某些处理器的电源管理功能。可用状态范围取决于主机的物理功能以及电源管理配置。

主机和 VM 命令可以返回以下信息：

- 数据源的完整说明
- 应用于指标的单位
- 可以使用的可能值范围

例如：

```
1 name_label: cpu0-C1
2 name_description: Proportion of time CPU 0 spent in C-state 1
3 enabled: true
4 standard: true
5 min: 0.000
6 max: 1.000
7 units: Percent
```

### 启用特定指标

默认情况下，将启用并收集大部分指标，要启用未启用和收集的指标，请输入以下信息：

```
1 xe host-data-source-record data-source=metric name host=hostname
```

### 禁用特定指标

您可能不想定期收集某些指标。要禁用先前启用的指标，请输入以下信息：

```
1 xe host-data-source-forget data-source=metric name host=hostname
```

### 显示当前已启用的主机指标的列表

要列出当前正在收集的主机指标的列表，请输入以下信息：

```
1 xe host-data-source-list host=hostname
```

### 显示当前已启用的 **VM** 指标的列表

要托管当前收集的 VM 指标，请输入以下信息：

```
1 xe vm-data-source-list vm=vm_name
```

## 使用 **RRD**

Citrix Hypervisor 使用 RRD 存储性能指标。这些 RRD 包含大小固定的数据库中的多个轮询档案 (RRA)。

数据库中的每个档案以指定精度抽取其特定指标样本：

- 在 10 分钟内每隔 5 秒钟
- 在过去 2 个小时内每隔 1 分钟
- 在过去 1 周内每隔 1 小时
- 在过去 1 年内每隔 1 天

每隔 5 秒钟的抽样记录实际数据点，但是，下列 RRA 则使用整合函数。Citrix Hypervisor 支持的整合函数为：

- AVERAGE
- MIN
- MAX

RRD 为单个 VM（包括 dom0）和 Citrix Hypervisor 服务器而存在。VM RRD 存储在它们运行所在的主机上，不运行时，存储在池主服务器上。因此，必须知道 VM 的位置，才能检索相关联的性能数据。

有关如何使用 Citrix Hypervisor RRD 的详细信息，请参阅 [Citrix Hypervisor 软件开发工具包指南](#)。

### 使用 HTTP 分析 RRD

您可以通过 HTTP 从使用 HTTP 处理程序（在 `/host_rrd` 或 `/vm_rrd` 上注册）指定的 Citrix Hypervisor 服务器下载 RRD。两个地址都要求进行 HTTP 身份验证，或者通过提供有效的管理 API 会话参考作为队列参数进行身份验证。例如：

下载主机 RRD。

```
1 wget http://server/host_rrd?session_id=OpaqueRef:SESSION_HANDLE>
```

下载 VM RRD。

```
1 wget http://server/vm_rrd?session_id=OpaqueRef:SESSION_HANDLE>&uuid=VM
  UUID>
```

这两个调用都将以能够导入 `rrdtool` 进行分析或直接解析的格式下载 XML。

### 使用 rrd2csv 分析 RRD

除了查看 XenCenter 中的性能指标，`rrd2csv` 工具还会将 RRD 记录为以逗号分隔的值 (CSV) 格式。提供手册和帮助页面。要显示 `rrd2csv` 工具手册或帮助页面，请运行以下命令：

```
1 man rrd2csv
```

或

```
1 rrd2csv --help
```

注意：

使用多个选项时，应当单独提供。例如：要返回与 VM 或主机相关联的 UUID 和名称标签，应当调用 `rrd2csv`，如下所示：

```
rrd2csv -u -n
```

虽然返回的 UUID 是唯一的，而且可用作主密钥，但是，实体的名称标签可能不必是唯一的。

手册页 (`rrd2csv --help`) 是工具的明确性帮助文本。

### 警报

可以配置 Citrix Hypervisor，根据任何可用的主机或 VM 指标生成警报。此外，当主机经历某些条件和状态时，Citrix Hypervisor 提供可以触发的预配置警报。可以使用 XenCenter 或 `xe CLI` 查看这些警报。

## 使用 XenCenter 查看警报

您可以在 XenCenter 中查看不同类型的警报，方法是单击通知，然后单击警报。“警报”视图将显示各种类型的警报，包括性能警报、系统警报和软件更新警报。

### 性能警报

当以下值之一超出在托管主机、VM 或存储库 (SR) 上的指定阈值时，可以生成性能警报：CPU 使用率、网络使用率、内存使用率、控制域内存使用率、存储吞吐量或 VM 磁盘使用量。

默认情况下，警报重复间隔为 60 分钟，但如果需要，也可以修改此间隔。警报将在 XenCenter 的“通知”区域中的“警报”页面上显示。此外，可以配置 XenCenter 以电子邮件形式发送任何指定的性能警报以及其他严重系统警报。

任何使用 xe CLI 配置的自定义警报也将在 XenCenter 中的“警报”页面上显示。

每个警报都有对应的优先级/严重级别。您也可以修改这些级别，根据需要选择在触发警报时接收电子邮件。默认警报优先级/严重性级别设为 3。

优先级	名称	说明	默认电子邮件警报
1	严重	立即采取行动，否则数据可能永久丢失/损坏。	是
2	重大	立即采取行动，否则某些服务可能无法运行。	是
3	警告	立即采取行动，否则服务可能会中断。	是
4	次要	注意，有些事项仅得到改进。	否
5	信息	日常信息 (VM 启动、停止、恢复等)	否
?	未知	未知错误	否

### 配置性能警报

- 在资源窗格中，选择相应的主机、VM 或 SR，单击常规选项卡，然后单击属性。
- 单击警报选项卡。可以配置以下警报：
  - 主机或 VM 的 **CPU** 使用率警报：选中生成 **CPU** 使用率警报复选框，然后设置将触发该警报的 CPU 使用率和时间阈值
  - 主机或 VM 的网络使用率警报：选中生成网络使用率警报复选框，然后设置将触发该警报的网络使用率

时间阈值。

- 主机的内存使用率警报：选中生成内存使用率警报复选框，然后设置将触发该警报的可用内存和时间阈值。
- 主机的控制域内存使用率警报：选中生成控制域内存使用率警报复选框，然后设置将触发该警报的控制域内存使用率和时间阈值。
- VM 的磁盘使用情况警报：选中生成磁盘使用情况警报复选框，然后设置将触发该警报的磁盘使用情况和时间阈值。
- SR 的存储吞吐量警报：选中生成存储吞吐量警报复选框，然后设置将触发该警报的存储吞吐量和时间阈值。

注意：

物理块设备 (PBD) 代表特定 Citrix Hypervisor 服务器与连接的 SR 之间的接口。当 PBD 上的总读取/写入 SR 吞吐量活动超过您指定的阈值时，与 PBD 连接的主机上将生成警报。与其他 Citrix Hypervisor 服务器警报不同，此警报必须在 SR 上进行配置。

3. 要更改警报重复间隔，请在警报重复间隔框中输入分钟数。达到警报阈值并生成一个警报时，只有在已耗完警报重复间隔时间后，才会生成另一个警报。
4. 单击确定以保存更改。

有关如何查看、过滤和配置性能警报严重性的详细信息，请参阅 XenCenter 帮助。

## 系统警报

下表显示了将触发在 XenCenter 中的“警报”页面上显示的警报的系统事件/条件。

名称	优先级/严重性	说明
license_expires_soon	2	Citrix Hypervisor 许可协议即将过期。
ha-statefile_lost	2	已断开与高可用性存储库的连接，立即采取行动。
ha-heartbeat_approaching_timeout	5	高可用性即将超时，如果不采取行动，主机可能会重新启动。
ha_statefile_approaching_timeout	5	高可用性即将超时，如果不采取行动，主机可能会重新启动。
haxapi_healthcheck_approaching_timeout	5	高可用性即将超时，如果不采取行动，主机可能会重新启动。
ha_network_bonding_error	3	潜在服务丢失。发送高可用性检测信号的网络已中断。

名称	优先级/严重性	说明
ha_pool_overcommitted	3	潜在服务丢失。高可用性无法保障对已配置 VM 的保护。
ha_poor_drop_in_plan_exists_for	3	高可用性保障范围已缩小，很有可能失败，但尚未丢失。
ha_protected_vm_restart_failed	2	服务丢失。高可用性无法重新启动受保护的 VM。
ha_host_failed	3	高可用性检测到某个主机出现故障。
ha_host_was_fenced	4	高可用性已重新启动某个主机，以保护 VM 免遭损坏。
redo_log_healthy	4	XAPI redo 日志已从上一错误中恢复。
redo_log_broken	3	XAPI redo 日志遇到了错误。
ip_configured_pif_can_unplug	3	使用高可用性时，已配置 IP 的 NIC 会被 XAPI 拔出，这有可能导致出现高可用性故障。
host_sync_data_failed	3	无法同步 Citrix Hypervisor 性能统计信息。
host_clock_skew_detected	3	主机时钟与池中其他主机时钟不同步。
host_clock_went_backwards	1	主机时钟已损坏。
pool_master_transition	4	已将新主机指定为池主服务器。
pbd_plug_failed_on_server_start	3	引导时，主机未连接到存储。
auth_external_init_failed	2	主机无法启用外部 AD 身份验证。
auth_external_pool_non-homogeneous	2	池中的主机有不同的 AD 身份验证配置。
multipath_period_alert	3	到 SR 的路径发生故障或已恢复。
bond-status-changed	3	绑定中的链路已断开连接或已重新连接。

#### 软件更新警报

- **XenCenter** 较旧：Citrix Hypervisor 需要使用较新的版本，但仍可连接到当前版本

- **XenCenter** 已过时：XenCenter 太旧，无法连接到 Citrix Hypervisor
- **Citrix Hypervisor** 已过时：Citrix Hypervisor 是当前 XenCenter 无法连接到的旧版本
- 许可证已过期警报：Citrix Hypervisor 许可证已过期
- 缺少 **IQN** 警报：Citrix Hypervisor 使用 iSCSI 存储，但主机 IQN 为空白
- 重复 **IQN** 警报：Citrix Hypervisor 使用 iSCSI 存储，但存在重复的主机 IQN

#### 使用 **xe CLI** 配置性能警报

**注意：**

检查警报触发的最小间隔为 5 分钟。此时间间隔可以避免因检查这些条件导致系统承受过多负载以及误报。将警报重复间隔设置为小于 5 分钟会导致在 5 分钟的最小间隔时仍生成警报。

性能监视 `perfmon` 工具每 5 分钟运行一次，并且平均 1 分钟从 Citrix Hypervisor 请求一次更新。这些默认值可以在 `/etc/sysconfig/perfmon` 中更改。

`perfmon` 工具每 5 分钟读取一次同一主机上运行的性能变量的更新。这些变量分成两组，一组与主机本身相关，另一组与在此主机上运行的每个 VM 相关。对于每个 VM 和主机，`perfmon` 读取参数 `other-config:perfmon`，并且使用此字符串来确定监视哪些变量以及在何种情况下生成消息。

例如，下面显示了通过将 XML 字符串写入参数 `other-config:perfmon` 来配置 VM“CPU 使用率”警报的示例：

```
1   xe vm-param-set uuid=vm_uuid other-config:perfmon=\
2
3   '<config>
4     <variable>
5       <name value="cpu_usage"/>
6       <alarm_trigger_level value="0.5"/>
7     </variable>
8   </config>'
```

**注意：**

您可以使用多个变量节点。

设置新配置后，请使用以下命令为每个主机刷新 `perfmon`：

```
1   xe host-call-plugin host=host_uuid plugin=perfmon fn=refresh
```

如果不执行此刷新，则在新配置生效之前将出现延迟，因为默认情况下，`perfmon` 每隔 30 分钟检查一次新配置。此默认值可以在 `/etc/sysconfig/perfmon` 中更改。

#### 有效的 **VM** 元素

- **name**：变量的名称（无默认值）。如果名称值为 `cpu_usage`、`network_usage` 或 `disk_usage`，则不需要使用 `rrd_regex` 和 `alarm_trigger_sense` 参数，因为将使用这些值的默认值。

- `alarm_priority`: 生成警报的优先级 (默认值为 3)。
- `alarm_trigger_level`: 触发警报的值的级别 (无默认值)。
- `alarm_trigger_sense`: 如果 `alarm_trigger_level` 为最大值, 则值为 `high`, 否则如果 `alarm_trigger_level` 为最小值, 则值为 `low` (默认值为 `high`)。
- `alarm_trigger_period`: 在发送警报之前, 能够接收的 (高于或低于警报阈值) 值的秒数 (默认值为 60)。
- `alarm_auto_inhibit_period`: 在发送某个警报后多久 (秒) 禁用此警报 (默认值为 3600)。
- `consolidation_fn`: 将来自 `rrd_updates` 的变量合并为一个值。对于 `cpu_usage`, 默认值为 `average`, 对于 `fs_usage`, 默认值为 `get_percent_fs_usage`, 对于所有其他变量, 则为 `sum`。
- `rrd_regex`: 匹配来自 `xe vm-data-sources-list uuid=vm_uuid` 的变量的名称, 以计算性能值。此参数具有下列已命名变量的默认值:
  - `cpu_usage`
  - `network_usage`
  - `disk_usage`

如果指定了正则表达式, 将使用根据 `consolidation_fn` 指定的方法, 对 `xe vm-data-source-list` 返回的项中名称与指定的正则表达式匹配的所有项的值进行合并。

#### 有效的主机元素

- `name`: 变量的名称 (无默认值)。
- `alarm_priority`: 生成警报的优先级 (默认值为 3)。
- `alarm_trigger_level`: 触发警报的值的级别 (无默认值)。
- `alarm_trigger_sense`: 当 `alarm_trigger_level` 为最大值时, 该值为 `high`, 否则如果 `alarm_trigger_level` 为最小值, 则为 `low`。(默认值为 `high`)
- `alarm_trigger_period`: 在发送警报之前, 能够接收 (高于或低于警报阈值) 的值的秒数 (默认值为 60)。
- `alarm_auto_inhibit_period`: 在发送某个警报后多久 (秒) 禁用该警报。(默认值为 3600)。
- `consolidation_fn`: 将来自 `rrd_updates` 的变量合并为一个值 (默认值为 `sum` 或 `average`)
- `rrd_regex`: 与 `xe vm-data-source-list uuid=vm_uuid` 命令返回的变量的名称相匹配的正则表达式, 用于计算统计值。此参数具有下列已命名变量的默认值:
  - `cpu_usage`
  - `network_usage`
  - `memory_free_kib`
  - `sr_io_throughput_total_xxxxxxxx` (其中 `xxxxxxxx` 是 SR-UUID 的前八个字符)。

**SR 吞吐量**: 必须在 SR 而非主机上配置存储吞吐量警报。例如:

```
1     xe sr-param-set uuid=sr_uuid other-config:perfmon=\
2     '<config>
3     <variable>
```

```
4         <name value="sr_io_throughput_total_per_host"/>
5         <alarm_trigger_level value="0.01"/>
6     </variable>
7 </config>
```

### 通用示例配置

以下示例显示了一个通用配置：

```
1     <config>
2     <variable>
3         <name value="NAME_CHOSEN_BY_USER"/>
4         <alarm_trigger_level value="THRESHOLD_LEVEL_FOR_ALARM"/>
5         <alarm_trigger_period value="
6             RAISE_ALARM_AFTER_THIS_MANY_SECONDS_OF_BAD_VALUES"/>
7         <alarm_priority value="PRIORITY_LEVEL"/>
8         <alarm_trigger_sense value="HIGH_OR_LOW"/>
9         <alarm_auto_inhibit_period value="
10            MINIMUM_TIME_BETWEEN_ALARMS_FROM_THIS_MONITOR"/>
11        <consolidation_fn value="FUNCTION_FOR_COMBINING_VALUES"/>
12        <rrd_regex value="
13            REGULAR_EXPRESSION_TO_CHOOSE_DATASOURCE_METRIC"/>
14    </variable>
15
16    <variable>
17        ...
18    </variable>
19
20    ...
21 </config>
```

### 配置电子邮件警报

您可以将 Citrix Hypervisor 配置为在 Citrix Hypervisor 服务器生成警报时发送电子邮件通知。此配置可以通过使用 XenCenter 或使用 xe 命令行接口 (CLI) 完成。

#### 使用 XenCenter 启用电子邮件警报

1. 在“资源”窗格中，在池上单击鼠标右键，选择属性。
2. 在“属性”窗口中，选择电子邮件选项。
3. 选中“发送电子邮件警报通知”复选框，然后输入电子邮件地址和 SMTP 服务器详细信息。

注意：

输入不需要身份验证的 SMTP 服务器的详细信息

4. 从邮件语言列表中选择首选语言以接收性能警报电子邮件。可选的三种语言为“英语”、“简体中文”和“日语”。  
用于为 XenCenter 配置性能警报电子邮件语言的默认语言为“英语”。

#### 使用 **xe CLI** 启用电子邮件警报

重要：

使用 XenCenter 或 xe CLI 启用电子邮件通知时，请输入不需要身份验证的 SMTP 服务器的详细信息。通过需要身份验证的 SMTP 服务器发送的电子邮件将不会送达。

要配置电子邮件警报，请指定电子邮件地址和 SMTP 服务器：

```
1    xe pool-param-set uuid=pool_uuid other-config:mail-destination=joe.
    bloggs@domain.tld
2    xe pool-param-set uuid=pool_uuid other-config:ssmtp-mailhub=smtp.
    domain.tld[:port]
```

在发送电子邮件之前，您还可以在消息中指定优先级（在 XenCenter 中也称为“严重性”）字段的最小值：

```
1    xe pool-param-set uuid=pool_uuid other-config:mail-max-priority=
    level
```

默认优先级为 4。

注意：

某些 SMTP 服务器只转发地址使用 FQDN 的邮件。如果您发现无法转发电子邮件，则可能是由于此原因导致。在这种情况下，可以将服务器主机名设置为 FQDN，以便通过此地址连接到您的邮件服务器。

要配置性能警报邮件语言，请执行以下操作：

```
1    xe pool-param-set uuid=pool_uuid other-config:mail-language=en-US |
    zh-CN | ja-JP
```

#### 通过经过身份验证的 **SMTP** 服务器发送电子邮件警报

Citrix Hypervisor 中的 mail-alarm 实用程序使用 sSMTP 发送电子邮件通知。发送电子邮件通知之前，mail-alarm 实用程序会查找配置文件 `mail-alarm.conf`。如果该配置文件存在，则文件的内容将用于配置 sSMTP。否则，将使用 XAPI 数据库（使用 XenCenter 或 xe CLI 配置进行配置）中的详细信息发送电子邮件警报。要通过经过身份验证的 SMTP 服务器发送电子邮件通知，请在 `/etc/` 中使用下列内容创建一个 `mail-alarm.conf` 文件：

```
1 root=postmaster
2 authUser=<username>
3 authPass=<password>
4 mailhub=<server address>:<port>
```

**注意：**

此配置文件将用于 Citrix Hypervisor 服务器生成的所有警报。

**额外的配置选项**

每个 SMTP 服务器在设置上都略有不同，并且可能需要额外配置。从 `ssmtp.conf` 手册页解压的以下内容将显示正确的语法和可用选项：

```
1 NAME
2     ssmtp.conf - ssmtp configuration file
3
4 DESCRIPTION
5     ssmtp reads configuration data from /etc/ssmtp/ssmtp.conf The
6     file contains keyword-argument pairs, one per line. Lines starting with
7     '#'
8     and empty lines are interpreted as comments.
9
10    The possible keywords and their meanings are as follows (both are
11    case-
12    insensitive):
13
14    Root
15    The user that gets all mail for userids less than 1000. If
16    blank,
17    address rewriting is disabled.
18
19    Mailhub
20    The host to send mail to, in the form host | IP_addr port
21    [:
22    port]. The default port is 25.
23
24    RewriteDomain
25    The domain from which mail seems to come. For user
26    authentication.
27
28    Hostname
```

```
24         The full qualified name of the host. If not specified, the
25         host
26         is queried for its hostname.
27
28     FromLineOverride
29         Specifies whether the From header of an email, if any, may
30         over-
31         ride the default domain. The default is "no".
32
33     UseTLS
34         Specifies whether smtp uses TLS to talk to the SMTP server.
35         The default is "no".
36
37     UseSTARTTLS
38         Specifies whether smtp does a EHLO/STARTTLS before
39         starting SSL
40         negotiation. See RFC 2487.
41
42     TLSCert
43         The file name of an RSA certificate to use for TLS, if
44         required.
45
46     AuthUser
47         The user name to use for SMTP AUTH. The default is blank,
48         in
49         which case SMTP AUTH is not used.
50
51     AuthPass
52         The password to use for SMTP AUTH.
53
54     AuthMethod
55         The authorization method to use. If unset, plain text is
56         used.
57         May also be set to "cram-md5".
```

## 自定义字段和标记

XenCenter 支持创建标记和自定义字段，这样，您可以组织和快速搜索 VM、存储等对象。有关详细信息，请参阅 XenCenter 帮助。

## 自定义搜索

XenCenter 支持创建自定义搜索。可以导出和导入搜索，还可以在导航面板中显示搜索结果。有关详细信息，请参阅 XenCenter 帮助。

## 确定物理总线适配器的吞吐量

对于 FC、SAS 和 iSCSI HBA，可以通过以下步骤确定 PBD 的网络吞吐量。

1. 列出主机上的 PBD。
2. 确定哪个 LUN 在哪个 PBD 上路由。
3. 对于每个 PBD 和 SR，列出 SR 上引用 VDI 的 VBD。
4. 针对主机上连接到 VM 的所有活动 VBD，计算组合吞吐量。

针对 iSCSI 和 NFS 存储，检查网络统计，以确定阵列上是否存在吞吐量瓶颈，或者 PBD 是否已饱和。

## 管理虚拟机

September 5, 2019

本节概括介绍使用模板创建虚拟机 (VM) 的方法，以及其他准备方法，包括将物理到虚拟转换 (P2V)、克隆模板及导入先前导出的 VM。

### 什么是虚拟机？

虚拟机 (VM) 是一种软件计算机，与物理计算机类似，都运行操作系统和应用程序。VM 包括由主机的物理资源提供支持的一组规范和配置文件。每个 VM 都有与物理硬件提供相同功能的虚拟设备。VM 具有更易于移植和管理以及更安全的优势。此外，还可以根据您的特定要求定制每个 VM 的引导行为。有关详细信息，请参阅[VM 引导行为](#)。

Citrix Hypervisor 支持具有任何已配置的 IPv4 或 IPv6 地址组合的来宾系统。

### 虚拟机类型

在 Citrix Hypervisor 中，VM 可以在以下两种模式中的一种模式下运行：

- 半虚拟化 (PV)：虚拟机内核使用特定代码，此代码在虚拟机管理程序上运行，以管理设备和内存。
- 全虚拟化 (HVM)：使用特定处理器功能“捕获”虚拟机执行的特权指令。您可以通过此功能使用未经修改的操作系统。为了访问网络和存储，会为虚拟机提供仿真设备。或者，也可以出于性能和可靠性原因，使用 PV 驱动程序。

## 创建 VM

### 使用 VM 模板

从模板准备 VM。模板是包含所有各种设置以创建特定 VM 的实例的黄金映像。Citrix Hypervisor 随附了一组基础模板（即原始 VM），可以在这些模板上安装操作系统。为达到最佳运行状态，不同的操作系统需要使用不同的设置。Citrix Hypervisor 模板已经过优化，可最大程度地提高操作系统的性能。

有两种从模板创建 VM 的基本方法：

- 使用完整的预配置模板（例如，演示版 Linux 虚拟设备）。
- 将操作系统从 CD、ISO 映像或网络存储库安装到所提供的适当模板上。

[Windows VM](#) 介绍如何将 Windows 操作系统安装到 VM 上。

[Linux VM](#) 介绍如何将 Linux 操作系统安装到 VM 上。

#### 注意：

较旧版本的 Citrix Hypervisor 创建的模板可以在较新版本的 Citrix Hypervisor 中使用。但是，在较新版本 Citrix Hypervisor 中创建的模板与较旧版本的 Citrix Hypervisor 不兼容。如果您使用 Citrix Hypervisor 8.0 创建了一个 VM 模板，要在早期版本中使用此模板，请单独导出 VDI 并重新创建 VM。

### 其他 VM 创建方法

除了从提供的模板创建 VM 外，还可以使用以下方法来创建 VM。

#### 物理到虚拟转换

物理到虚拟转换 (P2V) 过程是将物理服务器上的现有 Windows 操作系统转换为自身的虚拟化实例。转换包含文件系统和配置等。然后此虚拟化实例作为 VM 在 Citrix Hypervisor 服务器上传输、实例化并启动。

### 克隆现有 VM

您可以采用克隆模板的方式生成现有 VM 的副本。模板是要在创建 VM 实例时用作主副本的普通 VM。可以自定义 VM 并将其转换为模板。请务必遵循相应的 VM 准备过程。有关详细信息，请参阅[使用 Sysprep 准备克隆 Windows VM](#)或[准备克隆 Linux VM](#)。

#### 注意：

模板不可以用作普通 VM。

Citrix Hypervisor 包含两种克隆 VM 的机制：

- 完整复制

- 写入时复制

写入时复制模式速度更快，它只将修改后的块写入磁盘。“写入时复制”旨在节省磁盘空间并实现快速克隆，但会略微降低正常的磁盘性能。可以对一个模板进行多次快速克隆而不会影响性能。

注意：

如果将模板克隆到 VM 中，然后将克隆转换为模板，磁盘性能可能会降低。降低程度与此过程的发生次数呈线性关系。在此情况下，可使用 `vm-copy` CLI 命令对磁盘执行完整复制，并将磁盘性能恢复到预期水平。

#### 资源池注意事项

如果从共享 SR 上的 VM 虚拟磁盘创建模板，则模板克隆操作将被转发到池中可访问共享 SR 的任何服务器。但是，如果从仅有本地 SR 的某个 VM 虚拟磁盘创建模板，则只能在可访问该 SR 的服务器上运行模板克隆操作。

#### 导入一个导出的 VM

可以通过导入现有已导出的 VM 来创建 VM。与克隆类似，通过导出和导入 VM 可以快速创建更多具有特定配置的 VM。使用此方法可以提高部署速度。例如，您可能拥有一个多次使用的特殊用途服务器配置。根据需要设置 VM 后，可将其导出，并随后将其导入以创建具有特定配置的 VM 的新副本。还可以通过导出和导入 VM 将 VM 移动到位于其他资源池中的 Citrix Hypervisor 服务器上。

有关导入和导出 VM 的详细信息和步骤，请参阅[导入和导出 VM](#)。

## Citrix VM Tools

Citrix VM Tools 提供高性能 I/O 服务，而没有传统设备仿真的开销。Citrix VM Tools 由 I/O 驱动程序（也称为半虚拟化的驱动程序或 PV 驱动程序）和管理代理组成。应在每个 Windows VM 上安装 Citrix VM Tools，相应的 VM 才能具有完全受支持的配置，并且能够使用 xe CLI 或 XenCenter。VM 上安装的 Citrix VM Tools 版本必须与 Citrix Hypervisor 服务器上安装的最新可用版本相同。例如，有些修补程序包含更新后的 Citrix VM Tools ISO，可以更新主机上安装的版本。

I/O 驱动程序包括存储和网络驱动程序以及底层管理接口。这些驱动程序可替代仿真设备，在 Windows 和 Citrix Hypervisor 产品系列软件之间提供高速传输。在安装 Windows 操作系统时，Citrix Hypervisor 使用传统的设备仿真为 VM 提供标准 IDE 控制器和标准网卡。通过此仿真，Windows 可使用内置驱动程序进行安装，但由于控制器驱动程序仿真存在固有的开销，因而导致性能降低。

管理代理（也称为来宾代理）负责高级虚拟机管理功能，并向 XenCenter 提供一组完整功能。这些功能包括静止快照。

必须在每个 Windows VM 上安装 Citrix VM Tools，VM 才能具有完全受支持的配置。VM 上安装的 Citrix VM Tools 版本必须与 Citrix Hypervisor 服务器上安装的版本相同。VM 在未安装 Citrix VM Tools 的情况下可以正常工作，但如果未安装 I/O 驱动程序（PV 驱动程序），性能将受到影响。必须在 Windows VM 上安装 Citrix VM Tools，才能执行以下操作：

- 彻底关闭、重新启动或挂起 VM

- 在中查看 VM 性能数据 XenCenter
- 迁移正在运行的 VM（使用实时迁移或 Storage 实时迁移）
- 创建静止快照或带有内存（检查点）的快照，或者还原到快照
- 调整正在运行的 Linux VM 上的 vCPU 数量（对于 Windows VM，需要重新启动才能使此更改生效）

#### 了解 VM 的虚拟化状态

XenCenter 会在 VM 的常规选项卡上报告 VM 的虚拟化状态。可以确认是否已安装 Citrix VM Tools（I/O 驱动程序和管理代理）。此选项卡还显示 VM 是否可以安装和接收来自 Windows Update 的更新。以下部分列出了在 XenCenter 中显示的消息：

已优化 I/O（未优化 I/O）：此字段显示是否在 VM 上安装了 I/O 驱动程序。单击安装 I/O 驱动程序和管理代理链接将从 Citrix VM Tools ISO 安装 I/O 驱动程序。

注意：

I/O 驱动程序将自动安装在可从 Windows Update 接收更新的 Windows VM 上。有关详细信息，请参阅[更新 Citrix VM Tools](#)。

已安装管理代理（未安装管理代理）：此字段显示是否在 VM 上安装了管理代理。单击安装 I/O 驱动程序和管理代理链接将从 Citrix VM Tools ISO 安装管理代理。

能够接收来自 **Windows Update** 的更新（无法接收来自 **Windows Update** 的更新）：指定 VM 是否可以从 Windows Update 接收 I/O 驱动程序。

注意：

Windows Server Core 2016 不支持使用 Windows Update 安装或更新 I/O 驱动程序。应改为使用 Citrix VM Tools ISO 中的安装程序。

安装 I/O 驱动程序和管理代理：如果 VM 没有安装 I/O 驱动程序或管理代理，则会显示此消息。单击链接以安装 Citrix VM Tools。对于 Linux VM，单击此状态链接可切换至 VM 控制台并加载 Citrix VM Tools ISO。然后，您可以装载该 ISO，手动运行安装，如[安装 Citrix VM Tools](#) 中所述。

#### 支持的来宾系统与资源分配

有关受支持的来宾操作系统的列表，请参阅[支持的来宾系统、虚拟内存和磁盘大小限制](#)。

本节介绍 Citrix Hypervisor 产品系列中各产品在虚拟设备支持方面的差异。

#### Citrix Hypervisor 产品系列虚拟设备支持

Citrix Hypervisor 产品系列的当前版本对 VM 的虚拟设备具有某些常规限制。特定来宾操作系统对某些功能的限制可能更低一些。在各来宾系统的安装部分对这些限制进行了说明。有关配置限制的详细信息，请参阅[配置限制](#)。

硬件和环境等因素会影响这些限制。有关受支持的硬件的信息，请参阅 Citrix Hypervisor [硬件兼容性列表](#)。

### VM 块设备

在半虚拟化 (PV) Linux 的情况下，块设备作为 PV 设备传递。Citrix Hypervisor 不会尝试模拟 SCSI 或 IDE，而是提供更适用于虚拟环境的接口。此接口采用 `xvd*` 设备的形式。此外，有时也可以使用相同机制获取 `sd*` 设备，在这种设备中，VM 中的 PV 驱动程序将占据 SCSI 设备的命名空间。此行为不可取，因此最好在可能的情况下对 PV 来宾系统使用 `xvd*`。`xvd*` 设备是 Debian 和 RHEL 使用的默认设备。

对于 Windows 或其他完全虚拟化的来宾系统，Citrix Hypervisor 以 `hd*` 设备的形式模拟 IDE 总线。使用 Windows 时，安装 Citrix VM Tools 时也就安装了与在 Linux 环境中的工作方式相似的特殊 I/O 驱动程序（在完全虚拟化的环境中除外）。

## Windows VM

September 5, 2019

在 Citrix Hypervisor 服务器上安装 Windows VM 需要硬件虚拟化支持（Intel VT 或 AMD-V）。

### Windows VM 基本创建过程

在 VM 上安装 Windows 的过程包括以下步骤：

1. 选择适当的 Windows 模板
2. 安装 Windows 操作系统
3. 安装 Citrix VM Tools (I/O 驱动程序和管理代理)

警告：

Windows VM 仅在 VM 安装了 Citrix VM Tools 时才受支持。有关详细信息，请参阅 Citrix VM Tools。

### Windows VM 模板

要将 Windows 操作系统安装到 VM 上，可以使用 XenCenter 或 xe CLI 克隆相应的模板，然后安装操作系统。对于适用于各来宾系统的模板，已经设置了用来定义虚拟硬件配置的预定义平台标志。例如，所有 Windows VM 安装都支持 ACPI 硬件抽象层 (HAL) 模式。如果您以后将其中一个 VM 更改为包含多个虚拟 CPU，Windows 会自动将 HAL 切换为多处理器模式。

下面列出了可用的 Windows 模板：

模板名称	说明
Citrix XenApp on Windows Server 2008 (32-bit)	用于安装 Windows Server 2008 SP2 (32 位)。支持所有版本。此模板经过专门调整，可优化 Citrix XenApp 的性能。
Citrix XenApp on Windows Server 2008 (64-bit)	用于安装 Windows Server 2008 SP2 (64 位)。支持所有版本。此模板经过专门调整，可优化 Citrix XenApp 的性能。
Citrix XenApp on Windows Server 2008 R2 (64-bit)	用于安装 Windows Server 2008 R2 和 Windows Server 2008 R2 SP1 (64 位)。支持所有版本。此模板经过专门调整，可优化 Citrix XenApp 的性能。
Windows 7 (32-bit)	用于安装 Windows 7 和 Windows 7 SP1 (32 位)。
Windows 7 (64-bit)	用于安装 Windows 7 和 Windows 7 SP1 (64 位)。
Windows 8.1 (32-bit)	用于安装 Windows 8.1 (32 位)。(请参阅备注)
Windows 8.1 (64 位)	用于安装 Windows 8.1 (64 位)。(请参阅备注)
Windows 10 (32-bit)	用于安装 Windows 10。
Windows 10 (64 位)	用于安装 Windows 10 (64 位)。
Windows Server 2008 (32-bit)	用于安装 Windows Server 2008 SP2 (32 位)。支持所有版本。
Windows Server 2008 (64-bit)	用于安装 Windows Server 2008 SP2 (64 位)。支持所有版本。
Windows Server 2008 R2 (64-bit)	用于安装 Windows Server 2008 R2 和 Windows Server 2008 R2 SP1 (64 位)。支持所有版本。
Windows Server 2012 (64-bit)	用于安装 Windows Server 2012 (64 位)。
Windows Server 2012 R2 (64-bit)	用于安装 Windows Server 2012 R2 (64 位)。
Windows Server 2016 (64-bit)	用于安装 Windows Server 2016 或 Windows Server Core 2016 (64 位)
Windows Server 2019 (64-bit)	用于安装 Windows Server 2019 或 Windows Server Core 2019 (64 位)

**注意：**

不再支持 Windows 8。安装 Windows 8 的用户将升级到 Windows 8.1。

**警告：**

实验来宾操作系统只经过了有限的测试，在未来产品版本中可能无法提供，因此不能在生产系统上启用。我们可能不会对有关实验性功能请求提供帮助。

## 连接 ISO 映像库

可以从 Citrix Hypervisor 服务器上的物理 CD-ROM 驱动器中的安装 CD 或从 ISO 映像安装 Windows 操作系统。有关如何从 Windows 安装 CD 生成 ISO 映像以及如何使该映像可供使用的信息，请参阅[创建 ISO 映像](#)。

## 使用 XenCenter 创建 VM

### 注意：

以下过程举例说明创建 Windows 7（32 位）VM 的步骤。默认值可能因您选择的操作系统而异。

要创建 **Windows 7（32 位）VM**，请执行以下操作：

1. 在 XenCenter 工具栏上，单击新建 **VM** 按钮打开“新建 VM”向导。

通过“新建 VM”向导，可以配置新 VM，调整 CPU、存储和网络连接资源的各种参数。

2. 选择一个 VM 模板，然后单击下一步。

每个模板包含创建具有特定来宾操作系统 (OS) 和最佳存储的 VM 所需的设置信息。此列表列出了 Citrix Hypervisor 当前支持的模板。

### 注意：

如果要在 VM 上安装的操作系统仅与原始硬件兼容，请选中将主机 **BIOS** 字符串复制到 **VM** 框。例如，对于与特定计算机打包在一起的操作系统的安装 CD，可能要使用此选项。

要使用 CLI 复制 BIOS 字符串，请参阅[从经销商可选套件（锁定了 BIOS）介质安装 HVM VM](#)。用于设置用户定义的 BIOS 字符串的选项不适用于 HVM VM。

3. 为新 VM 输入名称及可选说明。
4. 为将安装在新 VM 上的操作系统选择安装源。

通过 CD/DVD 安装是最简单的入门方法。

- a) 选择默认安装来源选项（DVD 驱动器）
- b) 将磁盘插入 Citrix Hypervisor 服务器的 DVD 驱动器中
- c) 选择下一步继续操作。

Citrix Hypervisor 还允许您从多种来源提取操作系统安装介质，包括预先存在的 ISO 库。ISO 映像是一个文件，其中包含光盘（CD、DVD 等）中的所有信息。在这种情况下，ISO 映像包含与 Windows 安装 CD 相同的操作系统数据。

要附加已存在的 ISO 库，请单击新建 **ISO** 库并指明 ISO 库的位置和类型。然后可以从列表中选择特定的操作系统 ISO 介质。

## 5. 为 VM 选择主服务器。

主服务器是为池中的 VM 提供资源的服务器。为 VM 指定主服务器后，Citrix Hypervisor 将尝试在该服务器上启动 VM。如果此操作不可行，将自动选择同一池中的备用服务器。要选择主服务器，请单击将 **VM** 置于此服务器上并从列表中选择一个服务器。

注意：

- 1 - 在启用了 WLB 的池中，指定的主服务器不用于启动、重新启动、恢复或迁移 VM，而是由 WLB 分析 Citrix Hypervisor 资源池指标并提供优化建议，从而为 VM 指定最佳服务器。 - 如果为 VM 分配了虚拟 GPU，主服务器指定将无效。相反，服务器指定将取决于用户设置的虚拟 GPU 放置策略。

如果不希望指定主服务器，请单击不为此 **VM** 分配主服务器。VM 将在具有必备资源的任意服务器上启动。

单击下一步继续操作。

## 6. 为 VM 分配处理器和内存资源。对于 Windows 10 VM，默认设置为 1 个虚拟 CPU 和 2048 MB RAM。也可以选择修改默认设置。单击下一步继续操作。

## 7. 分配虚拟 GPU。新建 VM 向导会提示您将专用 GPU 或虚拟 GPU 分配给 VM。此选项使 VM 能够使用 GPU 的处理能力。借助此功能，可为 CAD/CAM、GIS 和医学成像应用程序等高端三维专业图形应用程序提供更好的支持。

## 8. 为新 VM 分配和配置存储。

单击下一步选择默认分配 (24 GB) 和配置，或者您可能需要进行以下额外配置：

- 通过单击属性更改虚拟磁盘的名称、说明或大小。
- 选择添加，添加一个新虚拟磁盘。

## 9. 配置新 VM 的网络连接设置。

单击下一步选择默认 NIC 和配置，包括为每个 NIC 自动创建的唯一 MAC 地址。或者，您可能想要进行以下额外配置：

- 通过单击属性更改虚拟磁盘的物理网络、MAC 地址或服务质量 (QoS) 优先级。
- 选择添加，以添加一个新虚拟 NIC。

## 10. 检查设置，然后单击立即创建以创建新 VM 并返回到搜索选项卡。

新 VM 的图标显示在资源窗格中的主机下。

在资源窗格中，选择该 VM，然后单击控制台选项卡以查看 VM 控制台。

## 11. 按照操作系统安装屏幕上的说明操作并进行选择。

## 12. 操作系统安装完成并重新启动 VM 后，安装 Citrix VM Tools。

## 安装 Citrix VM Tools

Citrix Hypervisor 具有更加简单的机制，用于在 Windows VM 上安装和更新 Citrix VM Tools (I/O 驱动程序和管理代理)。

Citrix VM Tools 提供高性能 I/O 服务，而没有传统设备仿真的开销。Citrix VM Tools 由 I/O 驱动程序（也称为半虚拟化的驱动程序或 PV 驱动程序）和管理代理组成。必须在每个 Windows VM 上安装 Citrix VM Tools，VM 才能具有完全受支持的配置。尽管没有这些工具 VM 也可以工作，但是性能会受到显著影响。

注意：

要在 Windows VM 上安装 Citrix VM Tools，该 VM 必须运行 Microsoft .NET Framework 4.0 或更高版本。

要安装 **Citrix VM Tools**，请执行以下操作：

1. 在资源窗格中选择 VM，单击鼠标右键，然后单击快捷菜单中的安装 **Citrix VM Tools**。或者，在 **VM** 菜单上，单击安装 **Citrix VM Tools**，或者在 VM 的常规选项卡上，单击安装 **I/O 驱动程序和管理代理**。

注意：

在 VM 上安装 Citrix VM Tools 时将同时安装 I/O 驱动程序 (PV 驱动程序) 和管理代理。

2. 如果针对 VM 的 CD/DVD 驱动器启用了自动播放功能，则片刻之后安装过程将自动启动。该过程可安装 I/O 驱动程序和管理代理。在系统提示时，重新启动 VM，以使 VM 处于优化状态。
3. 如果未启用自动播放功能，请单击安装 **Citrix VM Tools** 以继续执行安装。此操作将在 VM 的 CD/DVD 驱动器上装载 Citrix VM Tools ISO (`guest-tools.iso`)。

在系统提示时，请选择以下选项之一以选择要对 Citrix VM Tools ISO 执行的操作：

- 单击 **Run Setup.exe** (运行 Setup.exe) 开始安装 Citrix VM Tools。此操作将打开 **Citrix Hypervisor Windows** 管理代理安装向导。按照向导中的说明使您的 VM 进入优化状态并执行完成安装过程所需的任何操作。使用此方法安装 Citrix VM Tools 时，管理代理将被配置为自动获取更新。但是，管理代理更新机制不会自动更新 I/O 驱动程序。此行为是默认行为。如果要更改默认行为，请使用以下方法安装 Citrix VM Tools：
  - 单击 **Open folders to view files** (打开文件夹以查看文件)，然后从 CD 驱动器运行 `Setup.exe`。此选项将打开 **Citrix Hypervisor Windows** 管理代理安装向导，您可以在该向导中自定义 Citrix VM Tools 安装和管理代理更新设置。
  - 按照向导中的说明接受许可协议并选择目标文件夹。
  - 自定义 **Installation and Updates Settings** (安装和更新设置) 页面上的设置。**Citrix Hypervisor Windows** 管理代理安装向导显示默认设置。默认情况下，向导将显示以下设置：
    - 立即安装 I/O 驱动程序
    - 允许管理代理自动更新
    - 不允许管理代理自动更新 I/O 驱动程序

- 向 Citrix 发送匿名使用信息

如果不允许管理代理自动更新，请从列表中选择不允许管理代理自动更新。

如果要允许管理代理自动更新 I/O 驱动程序，请选择允许管理代理自动更新 **I/O** 驱动程序。

注意：

如果已选择通过 Windows Update 机制接收 I/O 驱动程序更新，请勿允许管理代理自动更新 I/O 驱动程序。

如果不希望与 Citrix 共享匿名使用信息，请取消选中向 **Citrix** 发送匿名使用信息复选框。传输到 Citrix 的信息包含请求更新的 VM 的 UUID。不收集与该 VM 有关的任何其他信息，也不会将这些信息传输到 Citrix。

- 依次单击下一步和安装开始执行 Citrix VM Tools 安装过程。
- 在系统提示时，请执行完成安装过程所需的任何操作。

注意：

Citrix VM Tools 可以在安装过程中已重新启动 VM 后指定了 `/quiet /norestart` 或 `/quiet /forcerestart` 的情况下请求重新启动。

- 单击完成退出向导。

注意：

I/O 驱动程序将自动安装在可从 Windows Update 接收更新的 Windows VM 上。但是，我们建议您通过安装 Citrix VM Tools 软件包来安装管理代理，并确保配置始终受支持。

要在多个 Windows VM 上安装 I/O 驱动程序和管理代理，请使用首选 MSI 安装工具安装 `managementagentx86.msi` 或 `managementagentx64.msi`。这些文件可在 Citrix VM Tools ISO 上找到。

通过 RDP 安装 Citrix VM Tools 或管理代理的客户可能看不到重新启动提示，因为该提示仅在 Windows 控制台会话中出现。为确保重新启动 VM（如有必要）以及使 VM 进入优化状态，请在 RDP 中指定强制重新启动选项。仅当需要使 VM 进入优化状态时，强制重新启动选项才会重新启动 VM。

无提示安装

要无提示安装 Citrix VM Tools 并阻止系统重新启动，请运行以下命令之一：

```
1 Msiexec.exe /package managementagentx86.msi /quiet /norestart
2 Msiexec.exe /package managementagentx64.msi /quiet /norestart
```

或

```
1 Setup.exe /quiet /norestart
```

可以通过运行以下命令获取非交互式带提示安装：

```
1 Msiexec.exe managementagentx86.msi /passive
2 Msiexec.exe managementagentx64.msi /passive
```

或

```
1 Setup.exe /passive
```

对于交互安装、静默安装和被动安装，在系统下一次重新启动后，可能要自动重新启动几次，才会完整安装 Citrix VM Tools。对于指定了 `/norestart` 标志的安装，也会发生此行为。但是，对于提供了 `/norestart` 标志的安装，首次重新启动可能要手动完成。

默认情况下，Citrix VM Tools 安装在 VM 上的 `C:\Program Files\Citrix\XenTools` 目录中。

注意：

- 要在 Windows VM 上安装 Citrix VM Tools，该 VM 必须运行 Microsoft .NET Framework 4.0 或更高版本。
- `/quiet` 参数仅适用于安装对话框，但不适用于设备驱动程序安装。指定了 `/quiet` 参数时，设备驱动程序安装会要求允许重新启动（如果需要）。
  - 指定了 `/quiet /norestart` 时，在安装了完整的工具后，系统不会重新启动。此行为与用户在重新启动对话框中指定的内容无关。
  - 指定了 `/quiet /forcerestart` 时，在安装了完整的工具后，系统会重新启动。此行为与用户在重新启动对话框中指定的内容无关。
  - 设备驱动程序安装要求允许重新启动时，指定了 `quiet` 参数的工具安装可能仍在进行。请使用任务管理器确认安装程序是否仍在运行。

警告：

安装或升级 Citrix VM Tools 可能会导致某些网络适配器的友好名称和标识符发生变化。安装或升级 Citrix VM Tools 后，可能必须重新配置已配置为使用特定适配器的任何软件。

## 使用 CLI 创建 Windows VM

要用 **xe CLI** 从 **ISO** 存储库创建 **Windows VM**，请执行以下操作：

1. 从模板创建 VM：

```
1 xe vm-install new-name-label=vm_name template=template_name
```

该命令将返回新 VM 的 UUID。

2. 创建 ISO 存储库：

```
1 xe-mount-iso-sr path_to_iso_sr
```

3. 列出所有可用的 ISO:

```
1 xe cd-list
```

4. 将指定的 ISO 插入指定 VM 的虚拟 CD 驱动器中:

```
1 xe vm-cd-add vm=vm_name cd-name=iso_name device=3
```

5. 启动该 VM 并安装操作系统:

```
1 xe vm-start vm=vm_name
```

此时, VM 控制台将在 XenCenter 中可见。

有关使用 CLI 的详细信息, 请参阅[命令行接口](#)。

## 更新 **Windows** 操作系统

本节介绍如何为 Windows VM 更新操作系统以及如何重新安装 Citrix VM Tools。

移动到更高版本的 Citrix Hypervisor 时, 通常需要升级 VM。将您的 VM 升级到更高版本的 Citrix Hypervisor 时需要注意以下限制:

- 使用实时迁移功能迁移 Windows VM 之前, 必须升级每个 VM 上的 Citrix VM Tools。
- 升级 Citrix VM Tools 之前, 不支持在 Windows VM 上执行挂起/恢复操作。
- 除非升级 Citrix VM Tools, 否则使用某些防病毒软件和防火墙应用程序可能会使 Windows VM 崩溃。

### 警告:

在更新 Windows 操作系统之前, 应卸载 Citrix VM Tools。如果在尝试更新期间存在这些工具, 则更新将失败。

在已经安装了 Windows 早期版本的服务器上引导 Windows 安装磁盘时, 它们通常会提供升级选项。

您能够以类似的方式更新 Windows VM 的操作系统。

要卸载 **Citrix VM Tools**, 请执行以下操作:

1. 在开始按钮中, 选择控制面板。
2. 选择程序, 然后选择程序和功能。
3. 选择以下所有项目 (列表取决于您的操作系统以及 VM 上安装的 Citrix VM Tools 的版本):
  - Citrix Hypervisor Windows 管理代理
  - Citrix Tools for Virtual Machines
  - Citrix VM Tools 安装程序
  - Citrix Hypervisor Windows 来宾代理
  - Citrix Hypervisor Xen Windows x64 PV 驱动程序

- Citrix Hypervisor Xen Windows x86 PV 驱动程序
- Citrix Hypervisor VSS 提供程序

#### 4. 选择卸载。

此选项将删除 Citrix VM Tools。操作完成后系统会显示一条消息。单击确定关闭消息框。

完成操作系统更新后，重新安装 Citrix VM Tools，方法与安装全新的 Windows VM 后安装这些工具的方法相同。

### 重新安装 **Citrix VM Tools**

XenCenter 中内置的 `guest-tools.iso` 中提供了 Citrix VM Tools。在 **VM** 菜单上，选择安装 **Citrix VM Tools**。此选项将包含 Citrix VM Tools 的 CD 映像连接到 VM。

如果针对 VM 的 CD/DVD 驱动器启用了自动播放功能，则片刻之后安装过程将自动启动。该过程可安装 I/O 驱动程序和管理代理。在系统提示时，重新启动 VM，以使 VM 处于优化状态。

如果未启用自动播放功能，Citrix VM Tools 安装程序将显示安装选项。单击安装 **Citrix VM Tools** 继续进行安装。此选项将在 VM 的 CD/DVD 驱动器上装载 Citrix VM Tools ISO (`guest-tools.iso`)。单击 **Run setup.exe** (运行 `setup.exe`) 开始安装 Citrix VM Tools，在系统提示时，重新启动 VM，以使 VM 处于优化状态。

### 更新 **Citrix VM Tools**

Citrix Hypervisor 具有一种更加简单的机制，可以自动为 Windows VM 更新 I/O 驱动程序 (PV 驱动程序) 和管理代理。通过此机制，一旦推出更新，客户即可安装，而不必等待修补程序。

在 XenCenter 中，VM 的常规选项卡中的虚拟化状态部分指定 VM 是否可以从 Windows Update 接收更新。默认情况下，从 Windows Update 接收 I/O 驱动程序更新的机制处于开启状态。如果不想从 Windows Update 接收 I/O 驱动程序更新，应在 VM 上禁用 Windows Update，或指定一个组策略。

以下各部分内容介绍了与自动更新 I/O 驱动程序和管理代理有关的信息。

#### 更新 I/O 驱动程序

您可以从 Microsoft Windows Update 自动获取 I/O 驱动程序更新，但前提是：

- 您运行的是 Citrix Hypervisor 8.0 Premium Edition，或者可通过 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor。
- 您已使用随 XenCenter Citrix Hypervisor 发布的 8.0 创建 Windows VM

**重要：**

从早期版本的 Citrix Hypervisor 导入的 VM 无法从 Windows Update 接收 I/O 驱动程序。

- VM 中已启用 Windows Update
- VM 可以访问 Internet，或者可以连接到 WSUS 代理服务器

**注意：**

Windows Server Core 不支持使用 Windows Update 安装或更新 I/O 驱动程序。应改为使用 Citrix VM Tools ISO 中的安装程序。

**注意：**

客户还可以通过管理代理自动更新机制自动接收 I/O 驱动程序更新。可以在 Citrix VM Tools 安装过程中配置此设置。有关详细信息，请参阅安装 *Citrix VM Tools*。

### 查明 I/O 驱动程序的版本

要查明 VM 上安装的 I/O 驱动程序的版本，请执行以下操作：

1. 导航到 `C:\Windows\System32\drivers`。
2. 从列表中找到该驱动程序。
3. 右键单击该驱动程序，然后依次选择属性和详细信息。

文件版本字段将显示 VM 上安装的驱动程序的版本。

### 更新管理代理

您可以使用 Citrix Hypervisor 自动在新的和现有的 Windows VM 上更新管理代理。默认情况下，Citrix Hypervisor 允许管理代理自动更新。但是，不允许管理代理自动更新 I/O 驱动程序。您可以在 Citrix VM Tools 安装过程中自定义管理代理更新设置。管理代理自动更新会无缝地进行，而不会重新启动 VM。如果需要重新启动 VM，VM 的“控制台”选项卡上将显示一条消息，向用户通知需要执行的操作。

您可以自动获取管理代理更新，但前提是：

- 您运行的是 Citrix Hypervisor 8.0 Premium Edition，或者可通过 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor。
- 已安装随 Citrix Hypervisor 7.0 或更高版本发布的 Citrix VM Tools
- Windows VM 能够访问 Internet

**重要：**

Citrix VM Tools 的更新也可以通过标准 Citrix Hypervisor 更新（修补程序）机制发布。这些修补程序同时包含对 I/O 驱动程序和管理代理的更新。更新以修补程序形式发布的 Citrix VM Tools 没有许可限制。

### 查明管理代理的版本

要查明 VM 上安装的管理代理的版本，请执行以下操作：

1. 导航到 `C:\Program Files\Citrix\XenTools`。

2. 右键单击列表中的 `XenGuestAgent`，然后依次单击属性和详细信息。

文件版本字段将显示 VM 上安装的 Management Agent 的版本。

#### 使用 CLI 管理自动更新

Citrix Hypervisor 允许您使用命令行管理 I/O 驱动程序和管理代理的自动更新。您可以在运行 `setup.exe` 或 `msiexec.exe` 时使用下表中列出的参数来指定是否自动更新 I/O 驱动程序和管理代理。有关使用 `setup.exe` 或 `msiexec.exe` 安装 Citrix VM Tools 的信息，请参阅无提示安装。

##### 注意：

对于使用 PVS 或 MCS 管理的 VM，当 Citrix Virtual Desktops VDA 存在并报告计算机是非静态计算机时，会自动关闭自动更新。

参数	值	说明
<code>ALLOWAUTOUPDATE</code>	YES/NO	允许/不允许管理代理自动更新
<code>ALLOWDRIVERINSTALL</code>	YES/NO	允许/不允许 Citrix VM Tools 安装程序安装 I/O 驱动程序
<code>ALLOWDRIVERUPDATE</code>	YES/NO	允许/不允许管理代理自动更新 I/O 驱动程序
<code>IDENTIFYAUTOUPDATE</code>	YES/NO	允许/不允许自动更新机制向 Citrix 发送匿名使用信息

例如：

```
1 setup.exe /passive /forcerestart ALLOWAUTOUPDATE=YES
   ALLOWDRIVERINSTALL=NO \
2   ALLOWDRIVERUPDATE=NO IDENTIFYAUTOUPDATE=YES
```

或

```
1 msiexec.exe /i managementagentx64.msi ALLOWAUTOUPDATE=YES
   ALLOWDRIVERINSTALL=NO \
2   ALLOWDRIVERUPDATE=NO IDENTIFYAUTOUPDATE=YES
```

#### 重定向管理代理更新

客户可以通过 Citrix Hypervisor 在安装管理代理更新之前将其重定向到内部 Web 服务器。此重定向功能让客户可以在 VM 上自动安装更新之前对其进行检查。

要重定向管理代理更新，请执行以下操作：

1. 从 <https://pvupdates.vmd.citrix.com/updates.json> 下载 JSON 文件。
2. 下载在 TSV 文件中引用的管理代理 JSON 文件。
3. 将 MSI 文件上载到您的 VM 可以访问的内部 Web 服务器。
4. 更新 JSON 文件，使其指向内部 Web 服务器上的 MSI 文件。
5. 将 JSON 文件上载到 Web 服务器。

注意：

此文件也以 TSV 格式针对旧版本的管理代理提供。 <https://pvupdates.vmd.citrix.com/updates.tsv>

也可以按每个 VM 或按每个池重定向自动更新。要按每个 VM 重定向更新，请执行以下操作：

1. 在 VM 上，以管理员身份打开一个命令提示窗口。
2. 运行以下命令

```
1 reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools /t REG_SZ /v update_url /  
d \  
2 url of the JSON file on the web server
```

要按每个池重定向管理代理自动更新，请运行以下命令：

```
1 xe pool-param-set uuid=pooluuid guest-agent-config:auto_update_url=url  
of the JSON file on the web server
```

### 禁用管理代理更新

要在每 VM 基础上禁用管理代理的自动更新，请运行以下命令：

1. 在 VM 上，以管理员身份打开一个命令提示窗口。
2. 运行以下命令：

```
1 reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools /t REG_DWORD /v  
DisableAutoUpdate /d 1
```

要按每个池禁用管理代理自动更新，请运行以下命令：

```
1 xe pool-param-set uuid=pooluuid guest-agent-config:auto_update_enabled=  
false
```

### 修改 I/O 驱动程序自动更新设置

在 Citrix VM Tools 安装过程中，可以指定是否允许管理代理自动更新 I/O 驱动程序。如果要在完成 Citrix VM Tools 安装过程后更新此设置，请执行以下步骤：

1. 在 VM 上，以管理员身份打开一个命令提示窗口。
2. 运行以下命令：

```
1 reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools\AutoUpdate /t REG_SZ /v \
2   InstallDrivers /d YES/NO
```

向 **Citrix** 发送匿名使用信息：

Citrix VM Tools 安装过程中，可以指定是否要向 Citrix 发送匿名使用信息。如果要在完成 Citrix VM Tools 安装过程后更新此设置，请执行以下步骤：

1. 在 VM 上，以管理员身份打开一个命令提示窗口。
2. 运行以下命令：

```
1 reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools\AutoUpdate REG_SZ /v \
2   IDENTIFYAUTOUPDATE /d YES/NO
```

### 准备使用 Sysprep 克隆 Windows VM

使用 Windows 实用程序 `sysprep` 准备 VM，这是唯一支持的 Windows VM 克隆方法。

`sysprep` 实用程序将更改本地计算机 SID 以确保各个计算机 SID 的唯一性。`sysprep` 二进制文件位于 `C:\Windows\System32\Sysprep` 文件夹中。

#### 注意：

对于较旧版本的 Windows，`sysprep` 二进制文件位于 Windows 产品 CD 上的 `\support\tools\deploy.cab` 文件中。在使用之前，必须将这些二进制文件复制到您的 Windows VM 中。

要克隆 **Windows VM**，请执行以下操作：

1. 根据需要创建、安装和配置 Windows VM。
2. 应用所有相关的 Service Pack 和更新。
3. 安装 Citrix VM Tools。
4. 安装任何应用程序和执行任何其他配置。
5. 运行 `sysprep`。完成后，此实用程序将关闭 VM。
6. 在 XenCenter 中，将 VM 转换为模板。

7. 根据需要将新创建的模板克隆到新 VM 中。
8. 克隆的 VM 启动时，将完成以下操作，然后才可供使用：
  - 获取新的 SID 和名称
  - 运行最小化安装以在必要时提示输入配置值
  - 最后，重新启动

注意：

在完成 `sysprep` 阶段后，请勿重新启动使用 `sysprep` 处理的原始 VM（“源”VM）。而是在此之后立即将其转换为模板以防重新启动。如果重新启动了源 VM，则必须再次对其运行 `sysprep`，才可以将其安全地用于创建更多克隆。

有关使用 `sysprep` 的详细信息，请访问下面的 Microsoft Web 站点：

- [Windows 自动安装工具包 \(AIK\)](#)

## Windows VM 发行说明

Windows 的许多版本和产品对 Citrix Hypervisor 所提供的功能具有不同支持级别。本节列出了已知差异的说明和勘误表。

### 一般 Windows 问题

- 安装 Windows VM 时，最初的虚拟磁盘数不要超过三个。安装 VM 和 Citrix VM Tools 后，您可以添加额外的虚拟磁盘。确保引导设备始终为某一初始磁盘，以便 VM 无需 Citrix VM Tools 即可成功引导。
- Windows VM 的引导模式为 BIOS 引导时，Windows 将使用主启动记录 (MBR) 对主磁盘进行格式化。MBR 将磁盘的最大可寻址磁盘空间限制到 2 TiB。要在 Windows VM 中使用大于 2 TiB 的磁盘虚拟机，请执行以下操作之一：
  - 如果 Windows 版本支持 UEFI 引导，请确保使用 UEFI 作为 Windows VM 的引导模式。
  - 请创建一个大型磁盘作为 VM 的辅助磁盘，并选择 GUID 分区表 (GPT) 格式。
- 多个 vCPU 将作为 CPU 插槽向 Windows 来宾系统公开，并受 VM 中的许可限制约束。来宾系统中存在的 CPU 数量可以通过查看“设备管理器”确认。可在“任务管理器”中查看 Windows 实际使用的 CPU 数量。
- Windows 来宾系统中的磁盘枚举顺序可能不同于最初添加这些磁盘的顺序。出现此行为的原因是，Windows 中 I/O 驱动程序与即插即用子系统之间的交互。例如，第一个磁盘可能显示为 `Disk 1`，下一个热插拔的磁盘显示为 `Disk 0`，再下一个磁盘显示为 `Disk 2`，后面的磁盘按预期方式向上排。
- VLC Player DirectX 后端存在一个缺陷：在 Windows 显示属性设置为 24 位色时，视频播放中本应显示为黄色的部分显示为蓝色。使用 OpenGL 作为后端的 VLC 正常运行，并且基于 DirectX 或基于 OpenGL 的所有其他视频播放器也正常运行。如果将来宾系统设置为使用 16 位而不是 24 位色，则不会出现上述问题。

- 在 Windows VM 中，报告的半虚拟化的以太网适配器速度为 1 Gbps。此速度是硬编码的值且与虚拟环境无关，因为虚拟 NIC 与虚拟交换机连接。数据速率不受所公布的网络速度限制。

## Windows 7

Microsoft 仅在安装了 Service Pack 1 时才支持使用 Windows 7。对于要在 Citrix Hypervisor 上支持的 Windows 7 VM，请务必安装 SP1 或更高版本。

## Windows 8

我们不再支持 Windows 8 来宾系统。如果安装 Windows 8 VM，则会将其升级到 Windows 8.1。

## Windows Server 2008 R2

Microsoft 仅在安装了 Service Pack 1 时才支持使用 Windows Server 2008 R2。对于要在 Citrix Hypervisor 上支持的 Windows Server 2008 R2 VM，请务必安装 SP1 或更高版本。

## Linux VM

September 5, 2019

创建 Linux VM 时，应使用与要在 VM 上运行的操作系统对应的模板创建 VM。可以使用 Citrix Hypervisor 为您的操作系统提供的模板，也可以使用之前您自己创建的模板。可以从 XenCenter 或 CLI 中创建 VM。本节重点介绍如何使用 CLI。

注意：

如果要创建的 VM 要运行的 RHEL 版本是高于 Citrix Hypervisor 支持安装的版本的次要更新版本，请完成以下步骤：

- 从支持的最新介质安装
- 使用 `yum update` 使 VM 保持最新

此过程也适用于 RHEL 衍生产品，例如 CentOS 和 Oracle Linux。

我们建议您在安装操作系统之后立即安装 Citrix VM Tools。有关详细信息，请参阅安装 Linux 来宾代理。对于某些操作系统，Citrix VM Tools 提供了一个 Citrix Hypervisor 专用的内核，以取代供应商提供的内核。而其他操作系统（例如 RHEL 5.x）则要求您安装供应商提供的特定版本的内核。

下面将概括介绍 Linux VM 的创建过程：

1. 使用 XenCenter 或 CLI 为目标操作系统创建 VM。

2. 使用供应商的安装介质安装操作系统。
3. 安装 Citrix VM Tools (推荐)。
4. 按照在常规非虚拟环境中的配置方式, 在 VM 和 VNC 上配置正确的时间和时区。

Citrix Hypervisor 支持将多个 Linux 版本安装到 VM 中。有以下三种安装方法:

- 从 Internet 存储库安装
- 从物理 CD 安装
- 从 ISO 库安装

**警告:**

其他安装介质模板适用于希望尝试安装运行不受支持操作系统的 VM 的高级用户。Citrix Hypervisor 已经过测试, 只能运行提供的标准模板中包含的受支持发行版本和特定版本。使用其他安装介质模板安装的任何 VM 均不受支持。

使用其他安装介质模板创建的 VM 将作为 HVM 来宾系统创建。此行为可能意味着, 某些 Linux VM 将使用性能较低的仿真设备, 而不是性能较高的 I/O 驱动程序。

有关特定 Linux 版本的信息, 请参阅Linux 发行版安装说明。

## **PV Linux 发行版**

支持的 PV Linux 发行版包括:

- Debian Wheezy 7 (32/64 位)
- Red Hat Enterprise Linux 5.x (32/64 位)  
如果使用 5.4 或更高版本的内核, 则受支持。
- Red Hat Enterprise Linux 6.x (32/64 位)
- CentOS 5.x (32/64 位)
- CentOS 6.x (32/64 位)
- Oracle Linux 5.x (32/64 位)
- Oracle Linux 6.x (32/64 位)
- Scientific Linux 6.6-6.9 (32/64 位)
- SUSE Linux Enterprise Server 11 SP3、SP4 (32/64 位)
- SUSE Linux Enterprise Server 12、12 SP1、12 SP2 (64 位)
- SUSE Linux Enterprise Desktop 11 SP3 (64 位)
- SUSE Linux Enterprise Desktop 12、12 SP1、12 SP2 (64 位)

- NeoKylin Linux Advanced Server 6.5 (64 位)
- NeoKylin Linux Advanced Server 7.2 (64 位)

其他 PV Linux 发行版不受支持。但是，与 Red Hat Enterprise Linux 使用相同安装机制的版本（例如 Fedora Core）可以使用同一模板成功安装。

注意：

- 不支持在内存大于 128 GB 的主机上运行 32 位 PV Linux VM。
- Citrix Hypervisor 硬件安全性功能会降低 32 位 PV VM 的整体性能。如果此问题会对您产生影响，可以执行以下操作之一：
  - 运行 64 位版本的 PV Linux VM
  - 使用 `no-smep no-smap` 选项启动 Xen。

我们不建议使用此选项，因为此选项会降低主机安全性的深度

## HVM Linux 发行版

这些 VM 可以利用新处理器中的 x86 虚拟容器技术来提高性能。从这些来宾系统访问网络和存储仍使用内核中内置的驱动程序在 PV 模式下运行。

支持的 HVM Linux 发行版包括：

- Debian Jessie 8 (32/64 位)
- Debian Stretch 9 (32/64 位)
- Red Hat Enterprise Linux 7.x (64 位)
- CentOS 7.x (64 位)
- Oracle Enterprise Linux 7.x (64 位)
- Scientific Linux 7.x (64 位)
- SUSE Linux Enterprise Server 12 SP3 (64 位)
- SUSE Linux Enterprise Desktop 12 SP3 (64 位)
- SUSE Linux Enterprise Server 15 (64 位)
- SUSE Linux Enterprise Desktop 15 (64 位)
- Ubuntu 14.04 (32/64 位)
- Ubuntu 16.04 (32/64 位)
- Ubuntu 18.04 (64 位)
- CoreOS Stable (64 位)

其他 HVM 发行版不受支持。但是，与 Red Hat Enterprise Linux 使用相同安装机制的版本（例如 Fedora Core）可以使用同一模板成功安装。

## 通过从 **Internet** 存储库进行安装来创建 **Linux VM**

本节以 Debian Squeeze 为例，说明通过从 Internet 存储库安装操作系统来创建 Linux VM 的 xe CLI 过程。

1. 从 Debian Squeeze 模板创建 VM。系统会返回该 VM 的 UUID：

```
1 xe vm-install template=template-name new-name-label=squeeze-vm
```

2. 指定安装存储库。此安装存储库是一个 Debian 镜像，包含安装基本系统所需的软件包，以及在执行 Debian 安装程序期间选择的额外内容：

```
1 xe vm-param-set uuid=UUID other-config:install-repository=
  path_to_repository
```

例如，有效的存储库路径为 <http://ftp.xx.debian.org/debian>，其中 **xx** 是您所在国家/地区的代码（请参阅 Debian 镜像列表，以查看这些代码的一览表）。对于多次安装，我们建议使用本地镜像或 apt 代理，以避免在中央库产生过大的网络流量或负载。

注意：

Debian 安装程序仅支持 HTTP 和 FTP Apt 存储库。NFS 不受支持。

3. 找到要连接到的网络的 UUID。例如，如果网络连接到 *xenbr0*：

```
1 xe network-list bridge=xenbr0 --minimal
```

4. 创建一个 VIF 以将新 VM 连接到此网络：

```
1 xe vif-create vm-uuid=vm_uuid network-uuid=network_uuid mac=random
  device=0
```

5. 启动 VM。它将直接引导至 Debian 安装程序：

```
1 xe vm-start uuid=UUID
```

6. 按照 Debian 安装程序的步骤，以您需要的配置安装 VM。
7. 安装来宾代理，并配置图形显示。有关详细信息，请参阅安装 Linux 来宾代理。

## 通过从物理 **CD** 或 **DVD** 进行安装来创建 **Linux VM**

本节以 Debian Squeeze 为例，说明通过从物理 CD/DVD 安装操作系统来创建 Linux VM 的 xe CLI 过程。

1. 从 Debian Squeeze 模板创建 VM。系统会返回该 VM 的 UUID：

```
1 xe vm-install template=template-name new-name-label=vm-name
```

2. 获取新 VM 根磁盘的 UUID:

```
1 xe vbd-list vm-uuid=vm_uuid userdevice=0 params=uuid --minimal
```

3. 使用返回的 UUID，将根磁盘设置为不可引导:

```
1 xe vbd-param-set uuid=root_disk_uuid bootable=false
```

4. 获取 Citrix Hypervisor 服务器上的物理 CD 驱动器的名称:

```
1 xe cd-list
```

在此命令为您提供的结果中，`name-label` 字段为类似 SCSI 0:0:0:0 的值。

5. 将 Citrix Hypervisor 服务器的 CD 驱动器 `name-label` 参数用作 `cd-name` 参数，向新 VM 添加虚拟 CD-ROM:

```
1 xe vm-cd-add vm=vm_name cd-name="host_cd_drive_name_label" device=3
```

6. 获取与新虚拟 CD 驱动器对应的 VBD 的 UUID:

```
1 xe vbd-list vm-uuid=vm_uuid type=CD params=uuid --minimal
```

7. 将虚拟 CD 的 VBD 设置为可引导:

```
1 xe vbd-param-set uuid=cd_drive_uuid bootable=true
```

8. 将 VM 的安装存储库设置为 CD 驱动器:

```
1 xe vm-param-set uuid=vm_uuid other-config:install-repository=cdrom
```

9. 将 Debian Squeeze 安装 CD 插入到 Citrix Hypervisor 服务器上的 CD 驱动器中。
10. 使用 XenCenter 或 SSH 终端打开 VM 控制台，然后按照相关步骤执行操作系统安装。
11. 启动 VM。它将直接引导至 Debian 安装程序:

```
1 xe vm-start uuid=UUID
```

12. 安装来宾实用程序，并配置图形显示。有关详细信息，请参阅安装 Linux 来宾代理。

## 通过从 ISO 映像进行安装来创建 Linux VM

本节说明通过从支持网络访问的 ISO 安装操作系统来创建 Linux VM 的 xe CLI 过程。

1. 运行以下命令

```
1 xe vm-install template=template new-name-label=name_for_vm sr-uuid=  
=storage_repository_uuid
```

该命令将返回新 VM 的 UUID。

2. 找到要连接到的网络的 UUID。例如，如果网络连接到 *xenbr0*：

```
1 xe network-list bridge=xenbr0 --minimal
```

3. 创建一个 VIF 以将新 VM 连接到此网络：

```
1 xe vif-create vm-uuid=vm_uuid network-uuid=network_uuid mac=random  
device=0
```

4. 将 *other-config* 参数的 *install-repository* 键设置为您的网络存储库的路径。例如，将 [http://mirror.centos.org/centos/6/os/x86\\_64](http://mirror.centos.org/centos/6/os/x86_64) 用作供应商介质的 URL：

```
1 xe vm-param-set uuid=vm_uuid other-config:install-repository=http:  
//mirror.centos.org/centos/6/os/x86_64
```

5. 启动 VM：

```
1 xe vm-start uuid=vm_uuid
```

6. 使用 XenCenter 或 VNC 连接到 VM 控制台，然后执行操作系统安装。

#### 网络安装说明

使用 Citrix Hypervisor 来宾系统安装程序，可以通过支持网络访问的 ISO 映像将操作系统安装到 VM。要准备从 ISO 进行安装，应创建供应商介质（而非 ISO 映像）的分解网络存储库。通过 NFS、HTTP 或 FTP 将其导出，以便可以从 Citrix Hypervisor 服务器管理接口进行访问。

该网络存储库必须可通过 Citrix Hypervisor 服务器的控制域来进行访问，通常使用管理界面进行访问。URL 必须指向网络服务器上的 CD/DVD 映像库，并采用以下格式：

- **HTTP:** <http://<server>/<path>>
- **FTP:** <ftp://<server>/<path>>
- **NFS:** <nfs://<server>/<path>>
- **NFS:** <nfs:<server>/<path>>

有关如何准备进行网络安装的信息（例如，ISO 的解压缩位置），请参阅供应商提供的安装说明。

**注意：**

从 XenCenter 使用 NFS 安装方法时，应始终使用 `nfs://` 样式的路径。

从模板创建 VM 时，XenCenter 新建 **VM** 向导会提示您输入存储库的 URL。使用 CLI 时，正常使用 `vm-install` 安装模板，然后将 `other-config:install-repository` 参数设置为 URL 的值。然后启动 VM 时，将开始执行网络安装过程。

**警告：**

安装基于 Linux 的新 VM 时，务必要完成安装并重新启动该 VM，然后再对其执行任何其他操作。此过程类似于不中断 Windows 安装，否则可能导致 VM 无法正常运行。

### 高级操作系统引导参数

创建 VM 时，可以使用 XenCenter 或 xe CLI 指定高级操作系统引导参数。例如，在配置自动安装半虚拟化来宾系统时，指定高级参数可能很有用。例如，可以按如下过程使用 Debian preseed 或 RHEL kickstart 文件。

要使用 **preseed** 文件安装 **Debian**，请执行以下操作：

1. 创建一个 preseed 文件。有关创建 preseed 文件的信息，请参阅 Debian 文档了解详细信息。
2. 启动 VM 前，应确保正确设置了内核命令行。使用 XenCenter 中的“新建 VM”向导或执行类似如下的 xe CLI 命令：

```
1 xe vm-param-set uuid=uuid PV-args=preseed_arguments
```

要使用 **kickstart** 文件安装 **RHEL**，请执行以下操作：

**注意：**

Red Hat Kickstart 文件是一种自动化的安装方法，与应答文件类似，可以用来对 RHEL 的安装提示提供响应。要创建此文件，请手动安装 RHEL。kickstart 文件位于 `/root/anaconda-ks.cfg` 中。

1. 在 XenCenter 中，选择适当的 RHEL 模板。
2. 在 XenCenter 的“新建 VM”向导中指定要用作内核命令行参数的 kickstart 文件。按照与在 PXE 配置文件中指定此值完全相同的方式指定此值。例如：

```
1 ks=http://server/path ksdevice=eth0
```

3. 在命令行中，使用 `vm-param-set` 设置 `PV-args` 参数以利用 kickstart 文件

```
1 xe vm-param-set uuid=vm_uuid PV-args="ks=http://server/path
ksdevice=eth0"
```

4. 设置存储库的位置，以便 Citrix Hypervisor 知道从何处获取内核和 `initrd` 以用于安装程序引导：

```
1 xe vm-param-set uuid=vm_uuid other-config:install-repository=http://server/path
```

注意：

要使用 kickstart 文件进行安装（不通过新建 VM 向导），可以将相应的命令添加到高级操作系统引导参数文本框中。

## 安装 Linux 来宾代理

虽然受支持的所有 Linux 发行版都是本机半虚拟化的（并且不需要特殊驱动程序即可实现最佳性能），但是 Citrix Hypervisor 仍安装了来宾代理。此来宾代理向主机提供有关 VM 的额外信息。应在每个 Linux VM 上安装来宾代理，才能启用动态内存控制 (DMC)。

升级 Citrix Hypervisor 服务器时务必使 Linux 来宾代理保持最新。有关详细信息，请参阅更新 Linux 内核和来宾实用程序。

注意：

在 SUSE Linux Enterprise Desktop 或 Server 15 来宾上安装来宾代理之前，请务必在来宾上安装 `insserv-compat-0.1-2.15.noarch.rpm`。

要安装来宾代理，请执行以下操作：

1. 所需的文件位于内置 `guest-tools.iso` CD 映像中，也可以通过依次选择 XenCenter 中的 **VM** 和安装 **Citrix VM Tools** 选项进行安装。
2. 通过运行以下命令将映像装载到来宾系统中：

```
1 mount -o ro,exec /dev/disk/by-label/Citrix VM Tools /mnt
```

注意：

如果装载映像失败，可以通过运行以下命令来定位该映像：

```
1 blkid -t LABEL="Citrix VM Tools"
```

3. 以 root 用户身份执行安装脚本：

```
1 /mnt/Linux/install.sh
```

4. 通过运行以下命令从来宾系统卸载映像：

```
1 umount /mnt
```

5. 如果内核已经升级，或 VM 已从上一版本升级，请立即重新启动 VM。

注意：

连接到 Linux 虚拟机的 CD-ROM 驱动器和 ISO 显示为设备，例如 `/dev/xvdd` 或 `/dev/sdd`，而不是您可能认为的 `/dev/cdrom`。出现此行为的原因是，它们不是真正的 CD-ROM 设备，而是普通设备。使用 XenCenter 或 CLI 弹出 CD 时，将从 VM 中热拔出该设备，并且该设备将不再显示。在 Windows VM 中，此行为有所不同，CD 会以空状态保留在 VM 中。

## Linux 发行版安装说明

本节列出了在创建指定的 Linux VM 之前要考虑的供应商特定的配置信息。

有关所有发行版的更多详细发行说明，请参阅 Linux VM 发行说明。

### CentOS 5.x (32/64 位)

对于 CentOS 5.x VM，应确保操作系统使用 CentOS 5.4 内核或更高版本（可从发行版供应商处获取）。5.4 版之前的 Enterprise Linux 内核版本中存在阻止 Citrix Hypervisor VM 正常运行的问题。按照供应商的常规内核升级过程升级内核。

### Red Hat Enterprise Linux 5.x (32/64 位)

对于 RHEL 5.x VM，应确保操作系统使用 RHEL 5.4 内核 (2.6.18-164.el5) 或更高版本（可从发行版供应商处获取）。5.4 版之前的 Enterprise Linux 内核版本中存在阻止 Citrix Hypervisor VM 正常运行的问题。按照供应商的常规内核升级过程升级内核。

### Red Hat Enterprise Linux\* 7.x (32/64 位)

适用于这些来宾系统的新模板指定 2 GB RAM。此 RAM 大小是成功安装 v7.4 及更高版本的一个要求。对于 v7.0 - v7.3，该模板指定 2 GB RAM，但与早期版本的 Citrix Hypervisor 一样，1 GB RAM 已足够。

注意：

此信息适用于 Red Hat 和 Red Hat 衍生产品。

### Oracle Linux 5.x (32/64 位)

对于 OEL 5.x VM，应确保操作系统使用 OEL 5.4 内核或更高版本（可从发行版供应商处获取）。5.4 版之前的 Enterprise Linux 内核版本中存在阻止 Citrix Hypervisor VM 正常运行的问题。

按照供应商的常规内核升级过程升级内核。

对于 OEL 5.6 (64 位)，Unbreakable Enterprise Kernel (UEK) 不支持 Xen 平台。如果您尝试将 UEK 与此操作系统结合使用，内核将无法正确引导。

### Oracle Linux 6.9 (64 位)

对于内存超过 2 GB 的 OEL 6.9 VM，请设置启动参数 `crashkernel=no` 以禁用崩溃内核。仅在设置了此参数时，VM 才会成功重新启动。如果使用早期版本的 OEL 6.x，请在更新到 OEL 6.9 之前设置此启动参数。

要使用 XenCenter 设置此参数，请将其添加到新建 **VM** 向导的安装介质页面中的高级操作系统启动参数字段。

要使用 XenCenter 修改现有 VM，请右键单击 VM，选择属性 > 引导选项 > 操作系统启动参数。

### Debian 6.0 (Squeeze) (32/64 位)

如果在 XenCenter 中指定了专用镜像，此镜像将仅用于检索安装程序内核。运行安装程序时，您必须再次输入要用于检索软件包的镜像的地址。

### Debian 7 (Wheezy) (32/64 位)

如果在 XenCenter 中指定了专用镜像，此镜像将仅用于检索安装程序内核。运行安装程序时，您必须再次输入要用于检索软件包的镜像的地址。

### Apt 存储库 (Debian)

对于不经常进行或一次性的安装来说，建议直接使用 Debian 镜像。但是，如果您计划进行多次 VM 安装，我们建议您使用缓存代理服务器或本地镜像。以下任一工具都可以安装到 VM 中。

- [Apt-cacher](#)：保留本地软件包缓存的代理服务器的实现。
- [debmirror](#)：用于创建 Debian 存储库的部分或完整镜像的工具。

### 准备克隆 Linux VM

通常情况下，克隆 VM 或计算机时，除非要使克隆的映像通用化，否则，将会在您的环境中复制该计算机特有的属性。克隆时复制的其中一些特有属性为 IP 地址、SID 或 MAC 地址。

因此，克隆 Linux VM 时，Citrix Hypervisor 会自动更改某些虚拟硬件参数。使用 XenCenter 复制 VM 时，XenCenter 会自动为您更改 MAC 地址和 IP 地址。如果这些接口是在您的环境中动态配置的，可能不需要修改克隆的 VM。但是，如果这些接口是静态配置的，可能需要修改其网络配置。

可能需要自定义 VM 以识别这些更改。有关特定受支持的 Linux 版本的说明，请参阅 Linux VM 发行说明。

#### 计算机名称

克隆的 VM 是另一台计算机，与网络中的任何新计算机一样，它在网络域中必须具有唯一名称。

## IP 地址

克隆的 VM 必须在所属网络域中具有唯一的 IP 地址。通常情况下，使用 DHCP 分配地址时，此要求不是问题。当 VM 引导时，DHCP 服务器将为其分配一个 IP 地址。如果克隆的 VM 具有静态 IP 地址，必须在克隆的 VM 引导前为其指定一个未使用的 IP 地址。

## MAC 地址

在两种情况下，我们会建议在克隆之前禁用 MAC 地址规则：

1. 在某些 Linux 版本中，克隆 VM 的虚拟网络接口的 MAC 地址记录在网络配置文件中。但是，克隆 VM 时，XenCenter 会为新克隆的 VM 分配一个不同的 MAC 地址。因此，首次启动新 VM 时，网络会识别新 VM，但不会自动显示出来。
2. 某些 Linux 发行版使用 `udev` 规则记住每个网络接口的 MAC 地址，并为该接口保留名称。此行为的目的是使同一物理 NIC 始终映射到同一 `ethn` 接口，这对可移动 NIC（如便捷式计算机）很有用。但是，此行为在 VM 环境中会出现问题。

例如，假设在以下情况下存在此行为：

- ```
1 1. 在 安 装 VM 时 配 置 两 个 虚 拟 NIC
2 1. 关 闭 VM
3 1. 删 除 第 一 个 NIC
```

VM 重新启动时，XenCenter 仅显示一个 NIC，但其称为 `eth0`。同时，VM 会特意强制此 NIC 为 `eth1`。结果导致网络连接无法工作。

对于使用静态名称的 VM，应在克隆之前禁用这些规则。如果您不希望禁用静态名称，则必须在 VM 中重新配置网络连接（按常规方法进行操作）。但是，XenCenter 中显示的信息将与网络中的实际地址不符。

## 更新 Linux 内核和来宾实用程序

可以通过重新运行内置 `guest-tools.iso` CD 映像中的 `Linux/install.sh` 脚本来更新 Linux 来宾实用程序（请参阅安装 Linux 来宾代理）。

对于启用了 `yum` 的发行版（CentOS 5.x、RHEL 5.x 及更高版本），`xe-guest-utilities` 会安装 `yum` 配置文件，以便能够以标准方式使用 `yum` 进行后续更新。

对于 Debian，会填充 `/etc/apt/sources.list` 以便能够在默认情况下使用 `apt` 更新。

升级时，我们建议始终重新运行 `Linux/install.sh`。此脚本可自动确定 VM 是否需要更新，并在需要时安装更新。

升级到 **Ubuntu 14.04**、**RHEL 7** 和 **CentOS 7** 来宾系统

要将现有 Linux 来宾系统升级到当前在 **HVM** 模式下运行的版本（例如，RHEL 7.x、CentOS 7.x 和 Ubuntu 14.04），请执行来宾内部升级。此时，升级的来宾系统仅在 PV 模式下运行，这不受支持且存在已知问题。应运行以下脚本，将新升级的来宾系统转换为受支持的 HVM 模式。

在 Citrix Hypervisor 服务器上，打开本地 shell，以 root 用户身份登录，然后输入以下命令：

```
1 /opt/xensource/bin/pv2hvm vm_name
```

或

```
1 /opt/xensource/bin/pv2hvm vm_uuid
```

重新启动 VM，完成此过程。

## Linux VM 发行说明

大多数主流 Linux 版本直接支持 Xen 半虚拟化，但是具有不同的安装机制和一些内核限制。

### RHEL 图形安装支持

要使用图形安装程序，请在 XenCenter 中逐步完成新建 **VM** 向导。在安装介质页面的高级操作系统启动参数部分中，向列出的参数中添加 `vnc`：

```
1 graphical utf8 vnc
```

![“新建 VM”向导的屏幕截图。在“安装介质”页面上的“高级操作系统启动参数”中输入值 `graphical utf8 vnc`。](/zh-cn/citrix-hypervisor/media/rhel-graphical-network-install.png)

系统将提示您为新 VM 提供网络连接配置，以便能够进行 VNC 通信。依次完成“新建 VM”向导的剩余部分。完成向导后，在基础结构视图中选择 VM，然后单击控制台以查看 VM 的控制台会话。此时，将使用标准安装程序。VM 安装最初在文本模式下启动，并且可能要求提供网络配置。提供后，XenCenter 窗口右上角将显示切换到图形控制台按钮。

## Red Hat Enterprise Linux 5

Citrix Hypervisor 要求运行 RHEL 5.4 内核或更高版本。旧内核具有以下已知问题：

- 在 Citrix Hypervisor 8.0 上，使用原始内核的 RHEL 5.0 64 位来宾操作系统无法启动。在尝试将 Citrix Hypervisor 服务器升级到版本 8.0 之前，应将内核更新到版本 5.4 (2.6.18-164.el5xen) 或更高版本。如果您运行这些来宾系统并已将您的主机升级到 Citrix Hypervisor 8.0，请参阅 [CTX134845](#) 了解有关升级内核的信息。

- 在恢复挂起的 VM 时，可以进行导致交换活动的分配，但是由于仍然需要重新连接交换磁盘，因此交换活动无法执行。这种情况极少发生。(Red Hat 问题 [429102](#))。
- 如果您运行的是 RHEL 5.3 或 5.4 (32/64 位)，请勿使用动态内存控制 (DMC)，因为此功能会导致来宾系统崩溃。如果要使用 DMC，我们建议您升级到更高版本的 RHEL 或 CentOS。[EXT-54]
- 在 RHEL 5.3 中，当有许多设备连接到 VM 时，有时没有足够的时间来连接所有这些设备。在这种情况下，启动将失败。[EXT-17]
- 在 RHEL 5.0-5.3 中，使用 XFS 文件系统在特殊情况下会导致内核混乱。应用 Red Hat RHEL 5.4 或更高版本的内核可解决此问题。[EXT-16]
- 在 RHEL 5.2 和 5.3 中，主机具有 64 GiB RAM 或更高配置时，VM 可能会崩溃。应用 Red Hat RHEL 5.4 或更高版本的内核可解决此问题。[EXT-30]
- 在 RHEL 5.0-5.3 中，网络驱动器存在一个在极少数情况下会导致内核死锁的问题。应用 Red Hat RHEL 5.4 或更高版本的内核可解决此问题。[EXT-45]

### 注意：

在先前的版本中，Citrix Hypervisor 具有一个备用 RHEL 5 内核，修复了某些会阻止 RHEL 5 作为虚拟机有效运行的关键问题。Red Hat 已在 RHEL 5.4 及更高版本中解决了这些问题。因此，Citrix Hypervisor 不再包括 RHEL 5 的特定内核。

### 准备 RHEL 5 来宾系统以进行克隆

要准备 RHEL 5.x 来宾系统以进行克隆，请在将 VM 转换成模板之前编辑 `/etc/sysconfig/network-scripts/ifcfg-eth0`，并删除 `HWADDR` 行。有关详细信息，请参阅准备克隆 Linux VM。

### 注意：

Red Hat 建议使用 kickstart 执行自动安装，而不是直接克隆磁盘映像（请参阅 [Red Hat 知识库文章 1308](#)）。

### Red Hat Enterprise Linux 6

#### 注意：

Red Hat Enterprise Linux 6.x 还包括 Red Hat Enterprise Linux Workstation 6.6 (64 位) 和 Red Hat Enterprise Linux Client 6.6 (64 位)。

- RHEL 6.0 内核存在一个缺陷，将影响多个虚拟化平台上的磁盘 I/O。此问题导致运行 RHEL 6.0 的 VM 丢失中断信号。有关详细信息，请参阅 Red Hat 问题 [681439](#)、[603938](#) 和 [652262](#)。
- 尝试从正在运行的 RHEL 6.1 和 6.2 (32/64 位) VM 分离虚拟磁盘映像 (VDI) 可能会失败。这些失败的尝试会导致来宾系统内核崩溃，并显示错误消息 `NULL pointer dereference at <xyz>`。可将内核更新到 6.3 (2.6.32-238.el6) 或更高版本来解决此问题。有关详细信息，请参阅 [Red Hat 问题 773219](#)。

## **Red Hat Enterprise Linux 7**

迁移或挂起 VM 后，在恢复期间，RHEL 7.x 来宾系统可能会冻结。有关详细信息，请参阅 Red Hat 问题 [1141249](#)。

## **CentOS 5**

有关 CentOS 5.x 发行说明列表，请参阅 Red Hat Enterprise Linux 5。

## **CentOS 6**

有关 CentOS 6.x 发行说明列表，请参阅 Red Hat Enterprise Linux 6。

## **CentOS 7**

有关 CentOS 7.x 发行说明列表，请参阅 Red Hat Enterprise Linux 7。

## **Oracle Linux 5**

有关 Oracle Linux 5.x 发行说明列表，请参阅 Red Hat Enterprise Linux 5。

## **Oracle Linux 6**

如果安装 Oracle Linux 6.x 来宾系统的主机运行的是 v6.5 之前的版本，在升级到 v6.5 后，这些来宾系统仍继续运行 Red Hat 内核。要切换到 UEK 内核（全新安装中使用的默认设置），请删除 dom0 中的 `/etc/pygrub/rules.d/oracle-5.6` 文件。您可以通过编辑 VM 中的引导加载程序配置来选择此 VM 要使用哪个内核。

对于内存超过 2 GB 的 OEL 6.9 VM，请设置启动参数 `crashkernel=no` 以禁用崩溃内核。仅在设置了此参数时，VM 才会成功重新启动。如果使用早期版本的 OEL 6.x，请在更新到 OEL 6.9 之前设置此启动参数。有关详细信息，请参阅 Linux 发行版安装说明。

有关 Oracle Linux 6.x 发行说明列表，请参阅 Red Hat Enterprise Linux 6。

## **Oracle Linux 7**

有关 Oracle Linux 7.x 发行说明列表，请参阅 Red Hat Enterprise Linux 7。

## **Scientific Linux 6**

有关 Scientific Linux 6.x 发行说明列表，请参阅 Red Hat Enterprise Linux 6。

## Scientific Linux 7

有关 Scientific Linux 7.x 发行说明列表，请参阅 Red Hat Enterprise Linux 7。

## SUSE Linux Enterprise 12

默认情况下，SUSE Linux Enterprise 12 VM 在以下模式下受支持：

PV 模式：

- SUSE Linux Enterprise Desktop 12、12 SP1 和 12 SP2
- SUSE Linux Enterprise Server 12、12 SP1 和 12 SP2

HVM 模式：

- SUSE Linux Enterprise Desktop 12 SP3
- SUSE Linux Enterprise Server 12 SP3

准备 **SLES** 来宾系统以进行克隆

注意：

在准备 SLES 来宾系统以进行克隆之前，请确保清除网络设备的 `udev` 配置，如下所示：

```
1 cat < /dev/null > /etc/udev/rules.d/30-net_persistent_names.rules
```

准备 SLES 来宾系统以进行克隆

1. 打开文件 `/etc/sysconfig/network/config`
2. 编辑内容如下的行：

```
1 FORCE_PERSISTENT_NAMES=yes
```

更改为

```
1 FORCE_PERSISTENT_NAMES=no
```

3. 保存更改并重新启动 VM。

有关详细信息，请参阅准备克隆 Linux VM。

## Ubuntu 14.04

尝试引导 PV 来宾系统可能会导致来宾系统崩溃，并显示以下错误：`kernel BUG at /build/buildd/linux-3.13.0/arch/x86/kernel/paravirt.c:239!` 出现此错误的原因是，未从中断上下文正确调用非原子函数。将 Linux 映像包更新到版本 3.13.0-35.62 可解决此问题。有关详细信息，请参阅 Ubuntu Launchpad [1350373](#)。

## VM 内存

June 4, 2019

在创建 VM 时，会为 VM 分配固定的内存量。您可以使用动态内存控制 (DMC) 提高您的 Citrix Hypervisor 环境中的物理内存利用率。DMC 是用于在 VM 之间动态重新分配内存的内存管理功能。

XenCenter 在其内存选项卡中提供了内存使用率的图形显示。有关详细信息，请参阅 XenCenter 帮助。

动态内存控制 (DMC) 具有以下优势：

- 您可以在不重新启动 VM 的情况下添加或删除内存，从而为用户提供无缝体验。
- 服务器满载后，DMC 允许您在这些服务器上启动更多 VM，从而按比例减少分配给正在运行的 VM 的内存量。

### 什么是动态内存控制 (DMC)?

Citrix Hypervisor DMC 的工作原理是：自动调整正在运行的 VM 的内存，使分配给每个 VM 的内存量保持在指定的最小内存值与最大内存值之间，确保性能并允许每台服务器具有更大的 VM 密度。

如果没有 DMC，则当服务器满载时，启动其他 VM 会失败并显示“内存不足”错误。要减少现有 VM 内存分配，为更多 VM 预留空间，请编辑每个 VM 的内存分配，然后重新启动 VM。使用 DMC 时，Citrix Hypervisor 会尝试在正在运行的 VM 的定义内存范围内自动减少其当前内存分配来回收内存。即使在服务器满载时，Citrix Hypervisor 仍会尝试回收内存。

注意：

配备了虚拟 GPU 的 VM 不支持动态内存控制功能。

### 动态范围的概念

对于每个 VM，管理员可以设置一个动态内存范围。动态内存范围是指可以在 VM 中添加/删除内存而无需重新启动 VM 的范围。在 VM 运行时，管理员可以调整动态范围。Citrix Hypervisor 始终保证为 VM 分配的内存量保持在动态范围内。因此，在 VM 运行时调整动态范围可能会导致 Citrix Hypervisor 调整分配给 VM 的内存量。管理员将动态最小/最大内存设置为相同值，从而强制 Citrix Hypervisor 确保为 VM 分配此内存量，这是最极端的情况。如果需要在“满载”的服务器上启动新 VM，则正在运行的 VM 会“腾出”自己的内存以便启动新 VM。获取所需的额外内存的方法是：在正在运行的现有 VM 的预定义动态范围内按比例腾出内存。

DMC 允许您配置动态最小和最大内存级别，从而创建 VM 运行时使用的动态内存范围 (DMR)。

- 动态最小内存：分配给 VM 的内存下限。
- 动态上限：分配给 VM 的内存上限。

例如，如果动态最小内存设置为 512 MB，动态最大内存设置为 1024 MB，则 VM 的动态内存范围 (DMR) 为 512 - 1024 MB，VM 将在此范围内运行。在使用 DMC 时，Citrix Hypervisor 可确保始终在每个 VM 的指定 DMR 内为其分配内存。

#### 静态范围的概念

Citrix Hypervisor 支持的许多操作系统不完全“理解”动态添加或删除内存的概念。因此，Citrix Hypervisor 必须声明 VM 在重新启动时需要占用的最大内存量。声明最大内存量允许来宾操作系统相应调整其页表及其他内存管理结构的大小。这在 Citrix Hypervisor 中引入了静态内存范围的概念。静态内存范围无法在 VM 运行时进行调整。对于特定引导，动态范围受到限制，例如始终限制在此静态范围内。静态最小内存（静态范围的下限）用于保护管理员，设置为操作系统可以在 Citrix Hypervisor 上运行时占用的最小内存量。

#### 注意：

我们建议您不要更改静态最小级别，因为静态最小级别设置为每个操作系统支持的级别。有关更多详细信息，请参阅内存限制表。

将静态最大级别设置为高于动态最大级别后，您以后为 VM 分配更多内存时，无需重新启动 VM。

## DMC 行为

### VM 自动腾出内存

- 如果未启用 DMC，则当主机满载时，新 VM 会因“内存不足”错误而导致启动失败。
- 启用了 DMC 时，即使在主机满载时，Citrix Hypervisor 仍会尝试在正在运行的 VM 的定义动态范围内减少其内存分配来回收内存。这样，正在运行的 VM 在动态最小内存与动态最大内存之间以相同的间距按比例为主机上的所有 VM 腾出内存。

### 启用了 DMC 时

- 主机内存足够时 - 正在运行的所有 VM 都将达到其动态最大内存级别。
- 主机内存不足时 - 正在运行的所有 VM 都将达到其动态最小内存级别。

配置 DMC 时，请记住，只将少量内存分配给 VM 会对其造成负面影响。例如，分配过少内存：

- 使用动态内存控制减少 VM 可用的物理内存量可能会导致 VM 重新启动缓慢。同样，如果为 VM 分配的内存过少，VM 启动可能缓慢。
- 如果为 VM 设置的动态最小内存过低，可能会导致在 VM 启动时出现性能或稳定性不佳的问题。

## DMC 的工作原理

使用 DMC，可以在以下两种模式中的一种模式下运行来宾虚拟机：

1. 目标模式：管理员指定来宾系统的内存目标。Citrix Hypervisor 将调整来宾系统的内存分配以达到该目标。在虚拟服务器环境中，以及在您知道希望来宾系统使用的准确内存量的情况下，指定目标很有用。Citrix Hypervisor 将调整来宾系统的内存分配以达到您指定的目标。
2. 动态范围模式：管理员指定来宾系统的动态内存范围。Citrix Hypervisor 将从该范围内选择一个目标，并调整来宾系统的内存分配以达到该目标。在虚拟桌面环境中，以及您希望 Citrix Hypervisor 动态重新分配主机内存以响应不断变化的来宾系统数目或不断变化的主机内存压力的任何情况下，指定动态内存范围很有用。Citrix Hypervisor 将从该范围内选择一个目标，并调整来宾系统的内存分配以达到该目标。

### 注意：

对于任何正在运行的来宾系统，可以随时在目标模式与动态范围模式之间进行更改。指定新目标或新动态范围，然后由 Citrix Hypervisor 完成剩余的工作。

## 内存限制

Citrix Hypervisor 允许管理员对任意来宾操作系统使用所有内存控制操作。但是，对于所有来宾系统，Citrix Hypervisor 会强制实行以下内存属性顺序限制：

0 `memory-static-min` `memory-dynamic-min` `memory-dynamic-max` `memory-static-max`

Citrix Hypervisor 允许管理员将来宾系统内存属性更改为可满足此限制（受验证检查限制）的任何值。但是，除上述限制外，对于支持的每个操作系统，我们仅支持特定的来宾系统内存配置。受支持的配置的范围取决于正在使用的来宾操作系统。Citrix Hypervisor 不会阻止管理员将来宾系统配置为超出支持的限制。但是，建议客户将内存属性保持在支持的限制内，以避免出现性能或稳定性问题。有关支持的每个操作系统的内存限制和最大内存限制的详细准则，请参阅[来宾操作系统支持](#)。

### 警告：

配置来宾系统内存时，我们建议不要超出操作系统可寻址的最大物理内存数量。如果设置的最大内存超出操作系统支持的限制，可能会导致来宾系统出现稳定性问题。

支持的所有操作系统的动态最小内存必须大约或等于静态最大内存的四分之一。将下限降低到动态最小内存以下也可能导致出现稳定性问题。建议管理员仔细校准其 VM 的大小，并确保其所用应用程序集在动态最小内存下可靠运行。

## xe CLI 命令

显示 VM 的静态内存属性

1. 查找所需 VM 的 uuid：

```
1 xe vm-list
```

- 记下该 **uuid**，然后运行命令 `param-name=memory-static`

```
1 xe vm-param-get uuid=uuid param-name=memory-static-{  
2   min,max }
```

例如，以下命令将显示 **uuid** 以 `ec77` 开头的 VM 的静态最大内存属性：

```
1 xe vm-param-get uuid= \  
2   ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 \  
3   param-name=memory-static-max;  
4   268435456
```

上述示例显示此 VM 的静态最大内存为 268435456 字节 (256 MB)。

#### 显示 **VM** 的动态内存属性

要显示动态内存属性，请按照上述过程进行操作，但使用命令 `param-name=memory-dynamic`：

- 查找所需 VM 的 **uuid**：

```
1 xe vm-list
```

- 记下该 **uuid**，然后运行命令 `param-name=memory-dynamic`：

```
1 xe vm-param-get uuid=uuid param-name=memory-dynamic-\  
2   min,max }
```

例如，以下命令将显示 **uuid** 以 `ec77` 开头的 VM 的动态最大内存属性：

```
1 xe vm-param-get uuid= \  
2   ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 \  
3   param-name=memory-dynamic-max;  
4   134217728
```

上述示例显示此 VM 的动态最大内存为 134217728 字节 (128 MB)。

#### 更新内存属性

##### 警告：

设置静态/动态最小/最大内存参数时顺序应正确。此外，必须保持以下限制有效：

```
0 memory-static-min memory-dynamic-min memory-dynamic-max memory-static-
```

max

更新虚拟机的静态内存范围：

```
1 xe vm-memory-static-range-set uuid=uuid min=value max=value
```

更新虚拟机的动态内存范围：

```
1 xe vm-memory-dynamic-range-set \  
2     uuid=uuid min=value \  
3     max=value
```

在虚拟服务器环境中，以及在您知道希望来宾系统使用的准确内存量的任何情况下，指定目标很有用。Citrix Hypervisor 将调整来宾系统的内存分配以达到您指定的目标。例如：

```
1 xe vm-target-set target=value vm=vm-name
```

更新虚拟机的所有内存限制（静态限制和动态限制）：

```
1 xe vm-memory-limits-set \  
2     uuid=uuid \  
3     static-min=value \  
4     dynamic-min=value \  
5     dynamic-max=value static-max=value
```

注意：

- 要为 VM 分配不会变化的特定内存量，请将动态最大内存和动态最小内存设置为相同值。
- 不能将 VM 的动态内存增加到超过静态最大内存。
- 要更改某个 VM 的静态最大内存，必须关闭该 VM。

更新各个内存属性

警告：

请勿更改静态最小级别，因为此级别设置为每个操作系统支持的级别。有关详细信息，请参阅内存限制。

更新 VM 的动态内存属性。

1. 查找所需 VM 的 uuid：

```
1 xe vm-list
```

2. 记下该 uuid，然后使用命令 `memory-dynamic-{ min,max } =value`

```
1 xe vm-param-set uuid=uuid memory-dynamic-{  
2   min,max }
```

```
3 =value
```

以下示例将动态最大内存更改为 128 MB:

```
1 xe vm-param-set uuid=ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 memory-  
dynamic-max=128MiB
```

## 迁移 VM

September 5, 2019

可以使用实时迁移和存储实时迁移功能迁移正在运行的 VM，以及移动 VM 虚拟磁盘映像 (VDI)，而不需要使 VM 停机。

### 实时迁移和存储实时迁移

以下各部分内容将介绍实时迁移和存储实时迁移功能的兼容性要求和限制。

#### 实时迁移

实时迁移在 Citrix Hypervisor 的所有版本中都可用。当 VM 磁盘位于两个主机共享的存储上时，您可以通过此功能将正在运行的 VM 从一个主机移至另一个主机。高可用性和滚动池升级 (RPU) 等池维护功能可以通过使用实时迁移功能自动移动 VM。可以通过这些功能实现工作负载调整、基础结构恢复以及服务器软件升级，而不需要使 VM 停机。

##### 注意:

只能在同一个池的主机之间共享存储。因此，只能将 VM 迁移至同一个池的主机。

虚拟 GPU 和 Intel GVT-g 功能与实时迁移、存储实时迁移或 VM 挂起功能不兼容。但是，使用 GPU 直通或 vGPU 的 VM 依然可以从任何拥有相应资源的主机启动。有关 NVIDIA vGPU 与这些功能的兼容性信息，请参阅[图形](#)。

#### Storage 实时迁移

##### 注意:

- 请勿在 Citrix Virtual Desktops 部署中使用存储实时迁移。
- 不能在启用了更改块跟踪功能的 VM 上使用存储实时迁移。请在尝试执行 Storage 实时迁移操作之前禁用更改块跟踪功能。
- 存储实时迁移不能用于其 VDI 位于 GFS2 SR 上的 VM。

当 VM 不位于两个主机之间共享的存储上时，存储实时迁移功能则允许将 VM 从一个主机移至另一个主机。因此，可以迁移保存于本地存储上的 VM，而不会带来停机时间，并且可以将 VM 从一个池移至另一个池。系统管理员可以通过此功能：

- 在 Citrix Hypervisor 池之间重新平衡 VM（例如，从开发环境到生产环境）
- 升级和更新独立的 Citrix Hypervisor 服务器，而不会带来任何 VM 停机时间。
- 升级 Citrix Hypervisor 服务器硬件。

### 注意：

将 VM 从一个主机移至另一个主机，从而保留 VM 状态。状态信息包括定义和标识 VM 的信息和历史性能指标（例如 CPU 和网络使用情况）。

### 兼容性要求

通过实时迁移或存储实时迁移功能迁移 VM 时，VM 和目标主机必须满足以下兼容性要求，才能继续进行迁移：

- 目标主机必须安装有相同或更新的 Citrix Hypervisor 作为源主机。
- 必须在要迁移的每个 Windows VM 上安装 Citrix VM Tools。VM 上安装的 Citrix VM Tools 版本必须与目标 Citrix Hypervisor 服务器上安装的版本相同。
- 仅限存储实时迁移：如果源主机和目标主机上的 CPU 不同，那么目标 CPU 必须至少提供与源 CPU 相同的完整功能集。因此，无法在不同的处理器（例如 AMD 和 Intel 处理器）之间移动 VM。
- 不能迁移带有检查点的 VM。
- 仅限存储实时迁移：无法迁移连接了六个以上 VDI 的 VM。
- 目标主机必须具有充足的空闲内存容量或者能够使用动态内存控制释放出充足的容量。如果内存不足，则无法完成迁移。
- 仅限存储实时迁移：目标存储必须具有足够的可用磁盘空间以存储传入的 VM。所需空间是 VDI 大小的三倍（不包含快照）。如果空间不足，迁移将无法完成。

### 限制和注意事项

实时迁移和存储实时迁移存在以下限制：

- 无法迁移使用 PCI 直通功能的 VM。
- 在迁移期间，VM 性能会降低。
- 对于存储实时迁移，受高可用性保护的池应先禁用高可用性，然后再尝试执行 VM 迁移。
- 完成 VM 迁移所需时间取决于 VM 的内存占用量及其活动。此外，通过存储实时迁移功能迁移的 VM 还会受到 VDI 的大小及其存储活动的影响。
- IPv6 Linux VM 要求 Linux 内核版本高于 3.0。

## 使用 XenCenter 迁移 VM

1. 在“资源”窗格中，选择 VM，然后执行以下操作之一：
  - 要使用实时迁移或 Storage 实时迁移迁移正在运行或已挂起的 VM，请在 **VM** 菜单中，单击迁移到服务器，然后单击迁移 **VM** 向导。此操作将打开迁移 **VM** 向导。
  - 要移动已停止的 VM，请在 **VM** 菜单上，选择移动 **VM**。此操作将打开移动 **VM** 向导。
2. 从目标列表中，选择独立服务器或池。
3. 从主服务器列表中，选择要指定为 VM 的主服务器的服务器，然后单击下一步。
4. 在存储选项卡中，指定要放置迁移的 VM 的虚拟磁盘的存储库，然后单击下一步。
  - 将所有虚拟磁盘放置在相同的 **SR** 上单选按钮默认处于选中状态，并且显示目标池中的默认共享 SR。
  - 单击将虚拟磁盘放置在指定 **SR** 上以从存储库列表中指定 SR。此选项支持您为迁移的 VM 上的每个虚拟磁盘选择不同的 SR。
5. 从存储网络列表中，在目标池中选择一个将用于实时迁移 VM 的虚拟磁盘的网络。单击下一步。

注意：

由于性能原因，建议您不要将管理网络用于实时迁移。
6. 检查配置设置，然后单击完成以开始迁移 VM。

## 实时 VDI 迁移

实时 VDI 迁移允许管理员重新定位 VM 虚拟磁盘映像 (VDI)，而无需关闭 VM。此功能支持执行管理操作，例如：

- 将 VM 从便宜的本地存储移至快速灵活且支持阵列的存储中。
- 将 VM 从开发环境移至生产环境。
- 在存储层中移动 VM（如果 VM 受到存储容量限制）。
- 执行存储阵列升级。

## 限制和注意事项

实时 VDI 迁移受以下限制和注意事项约束

- 请勿在 Citrix Virtual Desktops 部署中使用存储实时迁移。
- IPv6 Linux VM 要求 Linux 内核版本高于 3.0。
- 如果您在具有 vGPU 的 VM 上执行实时 VDI 迁移，则将使用 vGPU 实时迁移。主机必须具有足够的 vGPU 空间，才能在主机上创建 vGPU 实例的副本。如果充分利用 pGPU，则可能无法执行 VDI 迁移。

## 移动虚拟磁盘

1. 在资源窗格中，选择存储虚拟磁盘的 SR，然后单击存储选项卡。
2. 在虚拟磁盘列表中，选择要移动的虚拟磁盘，然后单击移动。
3. 在移动虚拟磁盘对话框中，选择要将 VDI 移至的目标 SR。

**注意：**

确保该 SR 具有可容纳另一个虚拟磁盘的充足空间：可用空间在可用 SR 列表中显示。

4. 单击移动以移动虚拟磁盘。

## 导入和导出 VM

September 5, 2019

您可以通过 Citrix Hypervisor 以多种不同的格式导入和导出 VM。使用 XenCenter 的导入向导，可以从磁盘映像 (VHD 和 VMDK)、以开放虚拟化格式 (OVF 和 OVA) 和 Citrix Hypervisor XVA 格式导入 VM。甚至可以导入在其他虚拟化平台（例如由 VMware 和 Microsoft 提供的虚拟化平台）上创建的 VM。

**注意：**

在导入使用其他虚拟化平台创建的 VM 时，应配置或修复来宾操作系统，确保其能够在 Citrix Hypervisor 上引导。XenCenter 中的操作系统修复功能可以提供这种基础级别的互操作性。有关详细信息，请参阅操作系统修复。

使用 XenCenter 的导出向导，可以将 VM 导出为开放虚拟化格式 (OVF 和 OVA) 和 Citrix Hypervisor XVA 格式。

在导入和导出 VM 时，会使用一个临时的 VM（传输 VM）来导入/导出 OVF/OVA 包和磁盘映像。应在 XenCenter 的导入和导出向导中为传输 VM 配置网络连接设置。有关详细信息，请参阅传输 VM。

还可以使用 xe CLI 以 Citrix Hypervisor XVA 格式导入和导出 VM。

## 支持的格式

| 格式                  | 说明                                                                                         |
|---------------------|--------------------------------------------------------------------------------------------|
| 开放虚拟化格式 (OVF 和 OVA) | OVF 是用于打包和分发由一个或多个 VM 组成的虚拟设备的开放标准。                                                        |
| 磁盘映像格式 (VHD 和 VMDK) | 可以使用导入向导导入虚拟硬盘 (VHD) 和虚拟机磁盘 (VMDK) 格式的磁盘映像文件。当存在可用虚拟磁盘映像，但没有与其相关联的 OVF 元数据时，适合使用导入磁盘映像的方式。 |

| 格式                            | 说明                                                                                                  |
|-------------------------------|-----------------------------------------------------------------------------------------------------|
| Citrix Hypervisor XVA 格式      | XVA 是特定于基于 Xen 的虚拟机管理程序的格式，用于将单个 VM 打包为单个文件存档，包括描述符和磁盘映像。其文件扩展名为 <code>.xva</code> 。                |
| Citrix Hypervisor XVA 版本 1 格式 | XVA 版本 1 是特定于基于 Xen 的虚拟机管理程序的原始格式。此格式用于将单个 VM 打包为单个文件存档，其中包括描述符和磁盘映像。其文件扩展名为 <code>ova.xml</code> 。 |

### 使用哪种格式？

对于以下情况，可考虑使用 OVF/OVA 格式：

- 与其他支持 OVF 的虚拟化平台共享 Citrix Hypervisor vApp 和 VM
- 保存多个 VM
- 保护 vApp 或 VM 不被破坏和篡改
- 包括许可协议
- 通过将 OVF 包存储到 OVA 文件中来简化 vApp 的分发

对于以下情况，可考虑使用 XVA 格式：

- 与版本低于 Citrix Hypervisor 的 6.0 共享 VM
- 使用 CLI 从脚本导入和导出 VM

### 开放虚拟化格式（OVF 和 OVA）

OVF 是由分布式管理任务组指定的开放标准，用于打包和分发由一个或多个 VM 组成的虚拟设备。有关 OVF 和 OVA 格式的更多详细信息，请参阅以下信息：

- 知识库文章 CTX121652: [Overview of the Open Virtualization Format](#)（开放虚拟化格式概述）
- [Open Virtualization Format Specification](#)（开放虚拟化格式规范）

#### 注意：

要导入或导出 OVF 或 OVA 包，您必须以 root 用户身份登录，或具有与您的用户帐户关联的池管理员基于角色的访问控制 (RBAC) 角色。

**OVF** 包是组成虚拟设备的一组文件。其中始终包含一个描述符文件以及表示以下软件包属性的所有其他文件：

## 属性

**描述符 (.ovf)**: 描述符始终用于指定软件包对虚拟硬件的要求。此外，它还可以指定其他信息，其中包括:

- 虚拟磁盘、软件包本身和来宾操作系统的说明
- 许可协议
- 在虚拟设备中启动和停止 VM 的说明
- 软件包的安装说明

**签名 (.cert)**: 签名是指公钥证书使用的数字签名 (X.509 格式)，用于对软件包的制作者进行身份验证。

**清单 (.mf)**: 清单用于验证软件包内容的完整性。其中包含软件包中每个文件的 SHA-1 摘要。

**虚拟磁盘**: OVF 不指定磁盘映像格式。OVF 包中包含组成虚拟磁盘的文件 (格式由导出虚拟磁盘所用的虚拟化产品定义)。Citrix Hypervisor 生成的 OVF 包具有动态 VHD 格式的磁盘映像; VMware 产品和 Virtual Box 生成的 OVF 包具有流技术优化 VMDK 格式的虚拟磁盘。

OVF 包也支持其他与非元数据相关的功能，例如压缩、存档、EULA 附件以及注释等功能。

### 注意:

如果导入的 OVF 包经过压缩或包含压缩文件，您可能需要在 Citrix Hypervisor 服务器上释放额外的磁盘空间以正确导入该 OVF 包。

**开放式虚拟设备 (OVA)** 包是采用磁带存档 (tar) 格式的单个存档文件，其中包含组成 OVF 包的各个文件。

## 选择 OVF 或 OVA 格式

OVF 包中包含一系列未压缩的文件，这样，您可以更方便地访问文件中的各个磁盘映像。而 OVA 包只包含一个大文件，尽管您可以压缩该文件，但是它不像一系列文件那样具有灵活性。

OVA 格式更适用于适合只使用一个文件的特定应用程序场合 (例如创建用于 Web 下载的软件包)。选择使用 OVA 只是为了使软件包更易于处理。使用此格式会延长导出和导入过程时间。

## 磁盘映像格式 (VHD 和 VMDK)

使用 XenCenter，可以导入虚拟硬盘 (VHD) 和虚拟机磁盘 (VMDK) 格式的磁盘映像。不支持导出独立磁盘映像。

### 注意:

要导入磁盘映像，请确保您以 root 用户身份登录，或具有与您的用户帐户关联的池管理员 RBAC 角色。

如果存在可用虚拟磁盘映像，但没有任何关联的 OVF 元数据，您可能需要选择导入磁盘映像。在以下情况下，可能需要执行此操作:

- 可以导入磁盘映像，但是无法读取其关联 OVF 元数据
- 虚拟磁盘未在 OVF 包中定义
- 要移出的平台不允许创建 OVF 包 (例如，较早的平台或映像)

- 要导入没有任何 OVF 信息的较早 VMware 设备
- 要导入没有任何 OVF 信息的独立 VM 设备

如有可能，我们建议您导入包含 OVF 元数据的设备软件包，而不是导入单个磁盘映像。OVF 数据提供了导入向导从磁盘映像重新创建 VM 时所需的信息。这些信息包括与 VM 关联的磁盘映像的数量、处理器、存储、网络以及内存要求等。如果缺少这些信息，重新创建 VM 的过程可能会更加复杂，并且更容易出错。

### XVA 格式

XVA 是 Citrix Hypervisor 所特有的虚拟设备格式，用于将单个 VM 打包为一组文件，包括描述符和磁盘映像。文件扩展名为 `.xva`。

描述符（文件扩展名为 `ova.xml`）用于指定单个 VM 的虚拟硬件。

磁盘映像采用文件目录格式。目录名称对应于描述符中的引用名称，对于磁盘映像的每个 1 MB 块，该目录包含 2 个相应文件。每个文件的基本名称是十进制形式的块编号。第一个文件包含磁盘映像的一个块（采用原始二进制格式），而且没有扩展名。第二个文件是第一个文件的校验和，其扩展名为 `.checksum`。

#### 重要：

如果将 VM 从 Citrix Hypervisor 服务器导出后导入到另一个具有不同 CPU 类型的 Citrix Hypervisor 服务器，该 VM 可能无法正常运行。例如，如果从使用已启用虚拟化技术的 Intel® CPU 的主机中导出了一个 Windows VM，在将其导入到使用 AMD-VTM CPU 的主机中后，该 VM 可能无法运行。

### XVA 版本 1 格式

XVA 版本 1 是特定于基于 Xen 的虚拟机管理程序的原始格式。此格式用于将单个 VM 打包为单个文件存档，其中包括描述符和磁盘映像。其文件扩展名为 `ova.xml`。

描述符（文件扩展名为 `ova.xml`）用于指定单个 VM 的虚拟硬件。

磁盘映像采用文件目录格式。目录名称对应于描述符中的引用名称，对于磁盘映像的每个 1 GB 区块，该目录包含 1 个相应文件。每个文件的基本名称包含十进制的区块编号。该文件包含磁盘映像的一个块（采用原始二进制格式），并以 `gzip` 格式压缩。

#### 重要：

如果从 Citrix Hypervisor 服务器导出 VM 并将其导入到另一个使用不同 CPU 类型的 Citrix Hypervisor 服务器，该 VM 可能无法正常运行。例如，如果从使用已启用虚拟化技术的 Intel® CPU 的主机中导出了一个 Windows VM，在将其导入到使用 AMD-VTM CPU 的主机中后，该 VM 可能无法运行。

### 操作系统修复

导入从 Citrix Hypervisor 以外的虚拟化平台创建和导出的虚拟设备或磁盘映像时，可能必须配置 VM，才能在 Citrix Hypervisor 服务器上正常引导该 VM。

XenCenter 包括一项高级虚拟机管理程序互操作性功能（操作系统修复），该功能旨在确保导入到 Citrix Hypervisor 中的 VM 具有基础级别的互操作性。从在其他虚拟化平台上创建的 OVF/OVA 包和磁盘映像导入 VM 时，应使用操作系统修复功能。

操作系统修复过程将尝试解决在不同虚拟机管理程序之间移动时所固有的操作系统设备和驱动程序问题。此过程尝试修复导入的 VM 中与引导设备相关的问题，这些问题可能会阻止操作系统在 Citrix Hypervisor 环境中引导。此功能的设计用途不是为了执行平台之间的转换。

**注意：**

此功能需要一个具有 40 MB 可用空间和 256 MB 虚拟内存的 ISO 存储库。

操作系统修复功能以自动引导的 ISO 映像形式提供，该映像连接到所导入 VM 的 DVD 驱动器。该功能在 VM 首次启动时执行必要的修复操作，然后关闭 VM。下次启动该新 VM 时，将会重置引导设备，VM 会正常启动。

要对导入的磁盘映像或 OVF/OVA 包使用操作系统修复功能，应在 XenCenter 的导入向导的“高级选项”页面上启用该功能。应指定复制修复 ISO 的位置，以供 Citrix Hypervisor 使用。

#### 操作系统修复功能对 VM 执行哪些操作？

“操作系统修复”选项旨在通过尽可能少的更改来允许虚拟系统引导。根据原始主机的来宾操作系统和虚拟机管理程序，使用操作系统修复功能后可能需要执行后续操作。这些操作可能包括更改配置和安装驱动程序。

在修复过程中，会将 ISO 复制到 ISO SR。该 ISO 将连接到一个 VM。引导顺序设置为从虚拟 DVD 驱动器引导，VM 将引导到该 ISO。ISO 中的环境随后会检查该 VM 的每个磁盘，以确定该 VM 采用的是 Linux 系统还是 Windows 系统。如果检测到 Linux 系统，则会确定 GRUB 配置文件的位置。指向 SCSI 磁盘引导设备的所有指针都将被修改为指向 IDE 磁盘。例如，如果 GRUB 包含 `/dev/sda1` 条目（表示第一个 SCSI 控制器上的第一个磁盘），则此条目会更改为 `/dev/hda1`（表示第一个 IDE 控制器上的第一个磁盘）。

如果检测到 Windows 系统，则会从所安装操作系统的驱动程序数据库中提取通用的关键引导设备驱动程序，并在该操作系统中注册此驱动程序。对于早期的 Windows 操作系统，在 SCSI 与 IDE 接口之间更改引导设备时，此过程尤其重要。

如果在 VM 中检测到某些虚拟化工具集，系统会将这些工具集禁用，以防出现性能问题和不必要的事件消息。

#### 传输 VM

传输 VM 是内置 VM，仅在导入或导出虚拟磁盘映像期间运行。它用于在磁盘映像文件位置与 Citrix Hypervisor 存储库之间传输映像内容。

每导入或导出一个磁盘映像，会运行一个传输 VM。如果导入或导出具有多个磁盘映像的虚拟设备，则一次仅传输一个磁盘映像。

运行一个传输 VM 时有如下要求：

---

|        |                                                   |
|--------|---------------------------------------------------|
| 虚拟 CPU | 1                                                 |
| 虚拟内存   | 256 MB                                            |
| 存储     | 8 MB                                              |
| 网络     | 可由 Citrix Hypervisor 服务器访问；静态或动态 IP 地址（建议使用动态地址）。 |

---

默认传输协议是 iSCSI。在这种情况下，Transfer VM 要求 Citrix Hypervisor 服务器上有一个 iSCSI 发起程序。备用传输协议是 RawVDI。

要使用 **RawVDI** 传输协议，请执行以下操作：

1. 备份 `XenCenterMain.exe.config` 文件，该文件位于安装文件夹中。
2. 使用文本编辑器打开 `XenCenterMain.exe.config` 文件。
3. 将以下 `sectionGroup` 添加到 `configSection` 中：

```
1 <sectionGroup name="applicationSettings"
2   type="System.Configuration.ApplicationSettingsGroup, System,
3     Version=2.0.0.0,
4     Culture=neutral, PublicKeyToken=b77a5c561934e089" >
5   <section name="XenOvfTransport.Properties.Settings"
6     type="System.Configuration.ClientSettingsSection, System,
7       Version=2.0.0.0,
8       Culture=neutral, PublicKeyToken=b77a5c561934e089"
9       requirePermission="false"/>
10 </sectionGroup>
```

4. 将以下部分添加到该文件的末尾：

```
1 <applicationSettings>
2   <XenOvfTransport.Properties.Settings>
3     <setting name="TransferType" serializeAs="String"> <value>
4       UploadRawVDI</value>
5     </setting>
6   </XenOvfTransport.Properties.Settings>
7 </applicationSettings>
```

5. 保存 `XenCenterMain.exe.config` 文件。

注意：

如果 XenCenter 无法正常启动，请检查是否已正确添加新的 sectionGroup 和上述部分。

## 导入 VM

导入 VM 时，将有效地创建一个 VM，此过程涉及的许多步骤与预配新 VM 的步骤相同。这些步骤包括指定主机以及配置存储和网络连接。

可以使用 XenCenter 的导入向导导入 OVF/OVA、磁盘映像、XVA 和 XVA 版本 1 文件。还可以通过 xe CLI 导入 XVA 文件。

### 从 OVF/OVA 导入 VM

注意：

要导入 OVF 包或 OVA 包，您必须以 root 用户身份登录，或具有与您的用户帐户关联的池管理员基于角色的访问控制 (RBAC) 角色。

使用 XenCenter 的导入向导，可以导入已经另存为 OVF/OVA 文件的 VM。导入向导引导您完成在 XenCenter 中创建 VM 的常规步骤：指定主机，然后为新 VM 配置存储和网络连接。在导入 OVF 和 OVA 文件时，可能需要执行额外的步骤，例如：

- 在导入使用其他虚拟化平台创建的 VM 时，应运行操作系统修复功能，以确保该 VM 具有基础级别的互操作性。有关详细信息，请参阅操作系统修复。
- 必须为用来执行导入过程的传输 VM 配置网络连接。有关详细信息，请参阅传输 VM。

提示：

请确保目标主机具有足够的 RAM 来支持要导入的虚拟机。缺少可用的 RAM 会导致导入失败。有关解决此问题的更多信息，请参阅 [CTX125120 - 设备导入向导因内存不足而失败](#)。

使用 XenCenter 进行导入时，导入的 OVF 包将显示为 vApp。导入完成后，新 VM 将显示在 XenCenter 资源窗格中，而新 vApp 将显示在管理 **vApp** 对话框中。

要使用从 **OVF/OVA** 导入 **VM**，请执行以下操作：

1. 通过执行以下操作之一打开导入向导：
  - 在资源窗格中，单击鼠标右键，然后选择快捷菜单上的导入。
  - 在文件菜单中，选择导入。
2. 在该向导的第一页上，找到要导入的文件，然后单击下一步继续操作。
3. 查看并接受 EULA（如果适用）。

如果要导入的软件包中包括任何 EULA，请接受这些 EULA，然后单击下一步继续操作。该软件包中不包括 EULA 时，向导将跳过此步骤并直接转至下一页。

4. 指定 VM 要导入到的池或主机，然后（可选）将 VM 分配给主 Citrix Hypervisor 服务器。

要选择主机或池，请从将 **VM** 导入列表中进行选择。

要为每个 VM 分配一个主 Citrix Hypervisor 服务器，请从主服务器中的列表选择一个服务器。如果不希望分配主服务器，请选择不分配主服务器。

单击下一步继续操作。

5. 为导入的 VM 配置存储：选择一个或多个用来放置导入的虚拟磁盘的存储库，然后单击下一步继续操作。

要将导入的所有虚拟磁盘放在同一个 SR 上，请选择将导入的所有虚拟磁盘放在此目标 **SR** 上。从列表选择一个 SR。

要将所导入 VM 的虚拟磁盘存储到不同的 SR 上，请选择将导入的 **VM** 放在指定的目标 **SR** 上。从 SR 列的列表中为每个 VM 选择目标 SR。

6. 为导入的 VM 配置网络连接：将所导入 VM 中的虚拟网络接口映射到目标池中的目标网络。导入 VM 列表中显示的网络和 MAC 地址作为原始（导出）VM 定义的一部分存储在导出文件中。要将传入的虚拟网络接口映射到目标网络，请从“目标网络”列的列表中选择网络。单击下一步继续操作。

7. 指定安全设置：如果为选定的 OVF/OVA 包配置了安全功能（例如证书或清单），请指定必要的信息，然后单击下一步继续操作。

根据 OVF 设备所配置的安全功能，“安全”页面上会显示不同的选项：

- 如果该设备带有签名，将显示验证数字签名复选框，系统自动选中该复选框。单击查看证书可显示用于对软件包进行签名的证书。如果证书显示为不可信，可能是根证书或证书颁发机构在本地计算机上不受信任。如果您不想验证签名，请清除验证数字签名复选框。
- 如果该设备包括清单，则会显示验证清单文件内容复选框。如果选中该复选框，向导将验证软件包中的文件列表。

软件包具有数字签名时，系统会自动验证关联的清单文件，因此，验证清单文件内容复选框不会显示在“安全”页面上。

注意：

如果您选择对清单进行验证，VMware Workstation 7.1.x OVF 文件将无法导入。发生此失败的原因是，VMware Workstation 7.1.x 生成的 OVF 文件包含具有无效 SHA-1 哈希的清单。如果您选择不对清单进行验证，则导入将成功。

8. 启用操作系统修复功能：如果要导入的软件包中的 VM 是在 Citrix Hypervisor 以外的虚拟化平台上构建的，请选择使用操作系统修复复选框。选择可以复制修复 ISO 的 ISO SR，以供 Citrix Hypervisor 访问。有关此功能的详细信息，请参阅操作系统修复。

单击下一步继续操作。

9. 配置传输 VM 网络连接。

从目标池或主机中的可用网络接口列表中选择网络。选择自动或手动配置网络设置。

- 要使用自动化的动态主机配置协议来分配网络设置（包括 IP 地址、子网掩码和网关），请选中使用 **DHCP** 自动获取网络设置。
- 要手动配置网络连接设置，请选择使用以下网络设置，然后输入所需值。输入 IP 地址。（可选）设置子网掩码和网关设置。

单击下一步继续操作。

10. 检查导入设置，然后单击完成，以开始执行导入过程并关闭该向导。

注意：

导入 VM 的过程需要一些时间，具体取决于该 VM 的大小以及网络连接的速度和带宽。

导入进度将显示在 XenCenter 窗口底部的状态栏中以及日志选项卡上。当新导入的 VM 可用时，它将显示在资源窗格中，而新 vApp 将显示在管理 **vApp** 对话框中。

注意：

在使用 XenCenter 导入包含 Windows 操作系统的 OVF 包后，必须设置 `platform` 参数。

1. 将 `platform` 参数设置为 `device_id=0002`。例如：

```
xe vm-param-set uuid=VM uuid platform:device_id=0002
```

2. 将 `platform` 参数设置为 `viridian=true`。例如：

```
xe vm-param-set uuid=VM uuid platform:viridian=true
```

## 导入磁盘映像

使用 XenCenter 的导入向导，可以将磁盘映像作为 VM 导入到池或特定主机中。导入向导引导您完成在 XenCenter 中创建 VM 的常规步骤：指定主机，然后为新 VM 配置存储和网络连接。

### 要求

- 必须以 `root` 用户身份登录，或者所用用户帐户与池管理员基于角色的访问控制 (RBAC) 角色相关联。
- 确保 DHCP 在 Citrix Hypervisor 使用的管理网络中运行。
- 导入向导要求使用其所在服务器上的本地存储。

要使用 **XenCenter** 从磁盘映像导入 **VM**，请执行以下操作：

1. 通过执行以下操作之一打开导入向导：
  - 在资源窗格中，单击鼠标右键，然后选择快捷菜单上的导入。
  - 在文件菜单中，选择导入。
2. 在该向导的第一页上，找到要导入的文件，然后单击下一步继续操作。

3. 指定 VM 名称并分配 CPU 和内存资源。

为基于所导入磁盘映像而创建的新 VM 输入名称，并为其分配 CPU 数量和内存量。单击下一步继续操作。

4. 指定 VM 要导入到的池或主机，然后（可选）将 VM 分配给主 Citrix Hypervisor 服务器。

要选择主机或池，请从将 **VM** 导入列表中进行选择。

要为每个 VM 分配一个主 Citrix Hypervisor 服务器，请从主服务器中的列表选择一个服务器。如果不希望分配主服务器，请选择不分配主服务器。

单击下一步继续操作。

5. 为导入的 VM 配置存储：选择一个或多个用来放置导入的虚拟磁盘的存储库，然后单击下一步继续操作。

要将导入的所有虚拟磁盘放在同一个 SR 上，请选择将导入的所有虚拟磁盘放在此目标 **SR** 上。从列表选择一个 SR。

要将所导入 VM 的虚拟磁盘存储到不同的 SR 上，请选择将导入的 **VM** 放在指定的目标 **SR** 上。从 SR 列的列表中为每个 VM 选择目标 SR。

6. 为导入的 VM 配置网络连接：将所导入 VM 中的虚拟网络接口映射到目标池中的目标网络。导入 VM 列表中显示的网络和 MAC 地址作为原始（导出）VM 定义的一部分存储在导出文件中。要将传入的虚拟网络接口映射到目标网络，请从“目标网络”列的列表中选择网络。单击下一步继续操作。

7. 启用操作系统修复功能：如果要导入的磁盘映像是在 Citrix Hypervisor 以外的虚拟化平台上构建的，请选中“使用操作系统修复”复选框。选择可以复制修复 ISO 的 ISO SR，以供 Citrix Hypervisor 访问。有关此功能的详细信息，请参阅操作系统修复。

单击下一步继续操作。

8. 配置传输 VM 网络连接。

从目标池或主机中的可用网络接口列表中选择网络。选择自动或手动配置网络设置。

- 要使用自动化的动态主机配置协议来分配网络设置（包括 IP 地址、子网掩码和网关），请选中使用 **DHCP** 自动获取网络设置。
- 要手动配置网络连接设置，请选择使用以下网络设置，然后输入所需值。输入 IP 地址。（可选）设置子网掩码和网关设置。

单击下一步继续操作。

9. 检查导入设置，然后单击完成，以开始执行导入过程并关闭该向导。

注意：

导入 VM 的过程需要一些时间，具体取决于该 VM 的大小以及网络连接的速度和带宽。

导入进度将显示在 XenCenter 窗口底部的状态栏中以及日志选项卡上。当新导入的 VM 可用时，将显示在资源窗格中。

**注意：**

在使用 XenCenter 导入包含 Windows 操作系统的磁盘映像后，必须设置 `platform` 参数。此参数值因磁盘映像中包含的 Windows 版本而异：

- 对于 Windows Server 2008 及更高版本，请将 `platform` 参数设置为 `device_id=0002`。例如：

```
1 xe vm-param-set uuid=VM uuid platform:device_id=0002
```

- 对于所有其他 Windows 版本，请将 `platform` 参数设置为 `viridian=true`。例如：

```
1 xe vm-param-set uuid=VM uuid platform:viridian=true
```

**从 XVA 导入 VM**

可以导入先前以 XVA 格式 (`.xva`) 或 XVA 版本 1 格式 (`ova.xml`) 导出并存储在本地的 VM、模板和快照。为此，请按照创建 VM 的常规步骤操作：指定主机，然后为新 VM 配置存储和网络连接。

**警告：**

如果 VM 是从具有不同 CPU 类型的其他服务器导出的，则该 VM 在导入后并不一定能够运行。例如，如果从使用已启用虚拟化技术的 Intel CPU 的服务器中导出了一个 Windows VM，在将其导入到使用 AMD-VTM CPU 的服务器中后，该 VM 可能无法运行。

要使用 **XenCenter** 从 XVA 导入 VM，请执行以下操作：

1. 通过执行以下操作之一打开导入向导：
  - 在资源窗格中，单击鼠标右键，然后选择快捷菜单上的导入。
  - 在文件菜单中，选择导入。
2. 在该向导的第一页上，找到要导入的文件 (`.xva` 或 `ova.xml`)，然后单击下一步继续操作。
 

如果您在文件名框中输入 URL 位置 (`http`、`https`、`file` 或 `ftp`)，单击下一步后，将打开“下载软件包”对话框，您必须指定 XenCenter 主机上存储复制的文件的文件夹。
3. 为导入的 VM 选择要在其上启动的池或主机，然后选择下一步继续。
4. 选择用于存储所导入虚拟磁盘的存储库，然后单击下一步继续操作。
5. 为导入的 VM 配置网络连接：将所导入 VM 中的虚拟网络接口映射到目标池中的目标网络。导入 VM 列表中显示的网络和 MAC 地址作为原始（导出）VM 定义的一部分存储在导出文件中。要将传入的虚拟网络接口映射到目标网络，请从“目标网络”列的列表中选择网络。单击下一步继续操作。
6. 检查导入设置，然后单击完成，以开始执行导入过程并关闭该向导。

**注意：**

导入 VM 的过程需要一些时间，具体取决于该 VM 的大小以及网络连接的速度和带宽。

导入进度将显示在 XenCenter 窗口底部的状态栏中以及日志选项卡上。当新导入的 VM 可用时，将显示在资源窗格中。

要使用 **xe CLI** 从 **XVA** 导入 **VM**，请执行以下操作：

要将 VM 导入目标 Citrix Hypervisor 服务器上的默认 SR 中，请输入以下命令：

```
1 xe vm-import -h hostname -u root -pw password \  
2   filename=pathname_of_export_file
```

要将 VM 导入到目标 Citrix Hypervisor 服务器上的其他 SR 中，请添加可选的 **sr-uuid** 参数：

```
1 xe vm-import -h hostname -u root -pw password \  
2   filename=pathname_of_export_file sr-uuid=uuid_of_target_sr
```

如果要保留原始 VM 的 MAC 地址，请添加可选的 **preserve** 参数并将其设置为 **true**：

```
1 xe vm-import -h hostname -u root -pw password \  
2   filename=pathname_of_export_file preserve=true
```

注意：

导入 VM 的过程需要一些时间，具体取决于该 VM 的大小以及网络连接的速度和带宽。

导入 VM 后，命令提示窗口中将返回新导入的 VM 的 UUID。

## 导出 VM

可以使用 XenCenter 的导出向导导出 OVF/OVA 和 XVA 文件；还可以通过 xe CLI 导出 XVA 文件。

### 将 VM 导出为 OVF/OVA

使用 XenCenter 的导出向导，可以将一个或多个 VM 导出为一个 OVF/OVA 包。将 VM 导出为一个 OVF/OVA 包时，系统会将配置数据与每个 VM 的虚拟硬盘一起导出。

注意：

要导出 OVF 包或 OVA 包，您必须以 root 用户身份登录，或具有与您的用户帐户关联的池管理员基于角色的访问控制 (RBAC) 角色。

要使用 **XenCenter** 将 **VM** 导出为 **OVF/OVA**，请执行以下操作：

1. 关闭或挂起要导出的 VM。
2. 打开导出向导：在资源窗格中，右键单击包含要导出的 VM 的池或主机，然后选择导出。
3. 在该向导的第一个页面上：

- 输入导出文件的名称
- 指定要保存文件的文件夹
- 从格式列表中选择 **OVF/OVA 包 (\*.ovf, \*.ova)**
- 单击下一步继续操作

4. 从可用 VM 列表中，选择要包括在 OVF/OVA 包中的 VM，然后单击下一步继续操作。

5. 如有必要，可以向软件包中添加先前准备的最终用户许可协议 (EULA) 文档 (.rtf 或.txt)。

要添加 EULA，请单击添加并浏览到要添加的文件。添加该文件后，可以从 **EULA** 文件列表中选择该文件，然后单击查看来查看该文档。

EULA 提供了有关使用设备和设备中交付的应用程序的法律条款和条件。

可以添加一个或多个 EULA，为设备上的软件提供法律保护。例如，如果设备中的 VM 使用某个专利操作系统，您可能要包括该操作系统的 EULA 文本。该文本将显示出来，导入设备的用户必须接受该协议。

注意：

如果尝试添加格式不受支持的 EULA 文件（包括 XML 或二进制文件），可能会导致 EULA 导入功能失败。

选择下一步继续操作。

6. 在高级选项页面上，指定清单、签名和输出文件选项，或者直接单击下一步继续操作。

a) 要为包创建清单，请选中创建清单复选框。

清单文件提供软件包中其他文件的清单或列表。清单用于确保最初在创建软件包时包含的文件与软件包创建完成时包含的文件相同。导入文件时，将使用校验和来验证在创建软件包后文件是否发生过更改。

b) 要向软件包添加数字签名，请选中签署 **OVF** 包复选框，通过浏览找到证书。在私钥密码字段中输入与该证书关联的私钥。

导入具有签名的软件包时，用户可以使用公钥来验证数字签名，从而验证软件包创建者的身份。使用您从可信颁发机构创建并导出为 **.pem** 或 **.pfx** 文件的 X.509 证书。该证书必须包含清单文件的签名以及用于创建该签名的证书。

c) 要将选定的 VM 输出为 OVA 格式的单个 (tar) 文件，请选中创建 **OVA 包 (单个 OVA 导出文件)** 复选框。有关不同文件格式的详细信息，请参阅开放虚拟化格式。

d) 要压缩软件包中包括的虚拟硬盘映像 (.VHD 文件)，请选中“压缩 OVF 文件”复选框。

默认情况下，当您创建 OVF 包时，分配给虚拟硬盘映像的空间量与导出的 VM 所占用的空间量相同。例如，如果为一个 VM 分配了 26 GB 空间，该 VM 的硬盘映像占用 26 GB 空间。该硬盘映像将使用此空间，而无论该 VM 实际是否需要这么多空间。

注意：

压缩 VHD 文件会增加导出过程所用时间。导入包含压缩 VHD 文件的软件包所用时间也会增加，因为在导入时，导入向导必须解压缩所有 VHD 映像。

如果创建 **OVA** 包 (单个 **OVA** 导出文件) 和压缩 **OVF** 文件均处于选中状态, 则将生成一个压缩的 OVA 文件 (扩展名为 `.ova.gz`)。

#### 7. 配置传输 VM 网络连接。

从目标池或主机中的可用网络接口列表中选择网络。选择自动或手动配置网络设置。

- 要使用自动化的动态主机配置协议来分配网络设置 (包括 IP 地址、子网掩码和网关), 请选中使用 **DHCP** 自动获取网络设置。
- 要手动配置网络连接设置, 请选择使用以下网络设置, 然后输入所需值。输入 IP 地址。(可选) 设置子网掩码和网关设置。

单击下一步继续操作。

#### 8. 检查导出设置。

要让向导验证导出的软件包, 请选中导出完成时进行验证复选框。单击完成以开始执行导出过程并关闭该向导。

注意:

导出 VM 的过程可能需要一些时间, 具体取决于该 VM 的大小以及网络连接的速度和带宽。

导出进度将显示在 XenCenter 窗口底部的状态栏中以及日志选项卡上。要取消正在进行的导出操作, 请单击日志选项卡, 在事件列表中找到该导出事件, 然后单击取消按钮。

### 将 VM 导出为 XVA

可以使用 XenCenter 的导出向导或 xe CLI 将现有的 VM 导出为 XVA 文件。我们建议将 VM 导出到 Citrix Hypervisor 服务器以外的计算机, 在该计算机上可以维护导出文件库。例如, 可以将 VM 导出到运行 XenCenter 的计算机。

警告:

如果 VM 是从具有不同 CPU 类型的其他服务器导出的, 则该 VM 在导入后并不一定能够运行。例如, 如果从使用已启用虚拟化技术的 Intel CPU 的服务器中导出了一个 Windows VM, 在将其导入到使用 AMD-VTM CPU 的服务器中后, 该 VM 可能无法运行。

要使用 **XenCenter** 将 **VM** 导出为 **XVA** 文件, 请执行以下操作:

1. 关闭或挂起要导出的 VM。
2. 打开导出向导: 在资源窗格中, 右键单击要导出的 VM, 然后选择导出。
3. 在该向导的第一个页面上:
  - 输入导出文件的名称
  - 指定要保存文件的文件夹
  - 从格式列表中选择 **XVA** 文件 (**\*.xva**)
  - 单击下一步继续操作
4. 从可用 VM 列表中选择要导出的 VM, 然后单击下一步继续操作。

## 5. 检查导出设置。

要让向导验证导出的软件包，请选中导出完成时进行验证复选框。单击“完成”以开始执行导出过程并关闭该向导。

注意：

导出 VM 的过程可能需要一些时间，具体取决于该 VM 的大小以及网络连接的速度和带宽。

导出进度将显示在 XenCenter 窗口底部的状态栏中以及日志选项卡上。要取消正在进行的导出操作，请单击日志选项卡，在事件列表中找到该导出事件，然后单击取消按钮。

要使用 **xe CLI** 将 **VM** 导出为 **XVA** 文件，请执行以下操作：

1. 关闭要导出的 VM。
2. 通过运行以下命令导出该 VM：

```
1 xe vm-export -h hostname -u root -pw password vm=vm_name \  
2   filename=pathname_of_file
```

注意：

指定导出文件名时，请务必包含 **.xva** 扩展名。如果导出的 VM 没有此扩展名，则在您尝试导入该 VM 时，XenCenter 可能无法将该文件识别为有效的 XVA 文件。

## Bromium 安全平台

June 4, 2019

Citrix Hypervisor 在 Windows VM 上支持 Bromium 安全平台。此功能保护您的企业免受破坏，并让用户能够执行任何操作而不会危及安全性。

注意：

支持的最低 Bromium 版本为 4.0.4。

通过此功能，您可以：

- 保护您的企业免受已知和未知的威胁。
- 实时检测和监视发生的威胁活动。
- 对呈现的攻击做出反应并查看采取的补救措施。

### 兼容性要求和注意事项

Citrix Hypervisor 在满足以下条件的 VM 上支持 Bromium：

- **CPU:** Intel Core i3、i5、i7 v3 (Haswell) 或更高版本，采用 Intel 虚拟化技术 (Intel VT) 并在系统 BIOS 中启用了扩展页表 (EPT)。

AMD CPU 不受支持。

- **VM:** Windows 7 SP1 (32 位和 64 位)、Windows 8.1 (64 位) 和 Windows 10 (64 位)。
- **VM 资源:** 至少 2 个 vCPU、4 GB RAM 和 32 GB 磁盘空间。

对于运行 Bromium 的 VM，Citrix Hypervisor 不支持并阻止使用以下功能：

- 任何形式的 VM 运动（例如：实时迁移、存储实时迁移）。
- 使用动态内存控制 (DMC)。

注意：

可以对启用了嵌套虚拟化的 VM 使用 PCI 直通和 vGPU。但是，Citrix 不支持此类配置。

重要：

Bromium 安全平台采用嵌套虚拟化支持。Citrix 仅支持在 Bromium 安全平台中使用此功能。其他用例不支持嵌套的虚拟化。要使用此功能，必须运行 Citrix Hypervisor Premium Edition 或者可以通过 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor。

## 配置

要准备您的 Citrix Hypervisor 系统以便与 Bromium 安全平台结合使用，请执行以下步骤：

1. 在每个主机上，通过在命令提示窗口中运行以下命令来强制使用软件 VMCS 重影：

```
1 /opt/xensource/libexec/xen-cmdline --set-xen
   force_software_vmcs_shadow
```

2. 重新启动主机。

3. 在每个 VM 上，使用以下命令启用嵌套虚拟化：

```
1 xe vm-list name-label='vm_name' --minimal
2
3 xe vm-param-set uuid=$VM platform:nested-virt=1
```

注意：

对于 Citrix Virtual Desktops，应使用黄金映像来支持嵌套的虚拟化。

4. 按照其安装说明在 VM 中安装 Bromium 安全平台。

## 容器管理

September 5, 2019

Citrix Hypervisor 包含两个新增功能，用于增强 Citrix Hypervisor 上的 Docker 容器的部署。

- 支持 CoreOS Linux VM 和配置云配置驱动器
- 面向 CoreOS、Debian 8、Ubuntu 14.04 和 RHEL/CentOS/OEL 7 的容器管理功能
- 面向 Windows Server 2016 技术预览版中 Windows Server 容器的容器管理预览功能

CoreOS 是精简版 Linux 发行版，已普遍用于托管 Docker 应用程序。CoreOS 云配置驱动器允许用户自定义各种操作系统配置选项。如果在 VM 上启用了容器管理，Citrix Hypervisor 将能够识别 VM 中运行的任何 Docker 容器。

### 注意：

有关如何安装 CoreOS 来宾系统、配置云配置参数以及管理 Docker 容器的信息，请参阅 XenCenter 帮助。按 **F1** 或单击帮助。

通过容器管理增补包，Citrix Hypervisor 可以执行以下操作：

- 查询 VM
- 与云配置驱动器交互
- 发现应用程序容器
- 在 XenCenter 的基础结构视图中显示应用程序容器。

XenCenter 还能够与容器交互，以允许执行启动、停止和暂停操作以及使用其他监视功能。有关详细信息，请参阅容器管理补充包。

## Docker 是什么

Docker 是一个开放式平台，开发人员和系统管理员能够在此平台上构建、交付和运行已分发的应用程序。Docker 容器仅由应用程序及其依赖项组成。该容器在主机操作系统上的用户空间中作为独立的进程运行，与其他容器共享内核和基本文件系统。有关详细信息，请参阅<https://www.docker.com/whatisdocker>。

### 注意：

Citrix Hypervisor 容器管理功能补充但不会替代 Docker 环境。您可以使用可用的多个 Docker 管理工具之一管理 VM 中的各个 Docker Engine 实例。

## 容器管理补充包

容器管理补充包提供以下功能：

监视和可见性：允许您查看哪些 VM 正在用于 Docker 托管，以及 VM 上的哪些容器正在运行。

**诊断：**可访问基础容器信息，例如，转接的网络端口和原始 Docker 映像名称。此功能有助于加快对可能会影响基础结构和应用程序层的问题的调查速度。

**性能：**深入了解哪些容器正在该 VM 上运行。提供与容器上运行的进程和应用程序以及占用的 CPU 资源有关的信息，具体取决于操作系统提供的信息。

**控制应用程序：**让您可以使用 XenCenter 启动、停止和暂停能够快速终止有问题的应用程序的应用程序容器（如果操作系统支持）。

**注意：**

Citrix Hypervisor 支持使用 XenCenter 安装补充包。有关如何使用 XenCenter 安装补充包的信息，请参阅 XenCenter 帮助。如果您更希望使用 xe CLI 进行安装，请参阅 [Citrix Hypervisor 补充包和 DDK 指南](#)。

## 使用 XenCenter 管理 Docker 容器

本节介绍与使用 XenCenter 管理您的 CoreOS VM 有关的信息。要管理 CoreOS VM，请完成以下步骤：

1. 安装或将您的主机升级到 Citrix Hypervisor 8.0。
2. 安装随 Citrix Hypervisor 8.0 提供的 XenCenter。
3. 安装可从 [Citrix Web 站点](#) 下载页面获取的容器管理增补包。
4. 创建 CoreOS VM 并将该 VM 的配置驱动器包括在内。

在 XenCenter 中创建 CoreOS VM 时，新建 **VM** 向导将提示您为 VM 指定云配置参数。配置驱动器为 VM 实例提供用户数据。如果您计划使用 Citrix Hypervisor 来管理 VM 内部运行的容器，请创建一个配置驱动器。

默认情况下，XenCenter 的“云配置参数”页面上包括一组预定义的参数。可以根据您的要求修改这些参数。有关支持的配置参数的详细信息，请参阅 CoreOS 文档。

**警告：**

如果没有为 VM 创建配置驱动器，容器管理可能无法运行。

5. 为 VM 启用容器管理。可以在 XenCenter 中的 VM 属性选项卡中更新此设置。

**注意：**

如果在池之间迁移容器管理的 VM，容器管理功能将停止对 VM 起作用。出现此行为的原因是，容器管理功能是使用池特定的键实现的。要重新对 VM 启用容器管理功能，请在 VM 首选项中更新云配置驱动器配置。

## 在其他 Linux 来宾系统上管理容器

系统会自动为容器管理准备通过默认云配置驱动器配置创建的 CoreOS VM。只需要启用该功能。可以手动准备其他 Linux 来宾系统。只有 Debian 8、Ubuntu 14.04 和 RHEL/CentOS/OEL 7.x VM 支持此功能。

要手动准备 Linux 来宾，请执行以下操作：

1. 确保 VM 已安装 Citrix VM Tools，并且已按网络要求和安全中所述配置 VM 网络。
2. 在 VM 中安装 Docker、Ncat 和 SSHD。

对于 Ubuntu 14.04:

```
1 apt-get install docker.io nmap openssh-server
```

对于 RHEL/CentOS/OEL 7.x:

```
1 yum install docker nmap openssh-server
```

3. 对 `docker.service` 启用自动启动:

```
1 systemctl enable docker.service
```

4. 启动 `docker.service`

```
1 systemctl start docker.service
```

使用非 `root` 用户进行容器管理。将用户添加到 `docker` 组以提供对 Docker 的访问权限。

5. 为容器管理功能准备 VM；请对池中的其中一个主机上的控制域 (`dom0`) 运行以下命令:

```
1 xscontainer-prepare-vm -v vm_uuid -u username
```

其中，`vm_uuid` 为要准备的 VM，`username` 为容器管理功能用于管理访问的 VM 上的用户名。

准备脚本将引导您完成该过程，并自动为此 VM 启用容器管理功能。

#### 注意:

如果在池之间迁移容器管理的 VM，容器管理功能将停止对 VM 起作用。出现此行为的原因是，容器管理功能是使用池特定的键实现的。要重新为 VM 启用容器管理功能，请在 VM 上再次运行 `xscontainer-prepare-vm` 命令。即使在运行此命令后，仍可能可以在原始 Citrix Hypervisor 池中访问该 VM。

## 访问 **Docker** 容器控制台和日志

对于 Linux VM，XenCenter 允许客户访问容器控制台和查看日志，从而管理和监控在 Docker 容器上运行的应用程序。要使用 XenCenter 访问容器控制台和日志，请执行以下操作:

1. 在资源窗格中选择容器。
2. 在容器的常规属性部分，单击查看控制台查看容器控制台。要查看控制台日志，请单击查看日志。此操作将在运行 XenCenter 的计算机上打开 SSH 客户端。
3. 在系统提示时，使用 VM 用户名和密码登录 SSH 客户端。

注意：

客户可以通过配置 SSH 公钥/私钥来自动完成身份验证过程。有关详细信息，请参阅以下部分。

#### 自动完成身份验证过程（可选）

访问容器控制台和日志时，客户需要输入 VM 的登录凭据才能验证 SSH 连接。但是，客户可以自动完成身份验证过程，以免手动输入凭据。按照以下说明配置自动身份验证过程：

1. 生成公钥/私钥对。
2. 将 SSH 公钥添加到运行容器的 VM 的用户目录。
  - 对于在 CoreOS VM 上运行的容器，将公钥添加到 XenCenter 中的 VM 常规选项卡上的云配置参数部分。
  - 对于 Ubuntu 14.04、RHEL/CentOS/Oracle Linux 7 和 Debian 8 上运行的容器，手动将公钥应手动添加到 `~/.ssh/authorized_keys`。
3. 将 SSH 私钥添加到运行 XenCenter 的计算机上的 `%userprofile%` 目录，并将该密钥重命名为 `ContainerManagement.ppk`。

#### 管理 Windows Server 容器

Windows Server 容器属于 Windows Server 2016 来宾操作系统的一部分。这些容器允许通过将进程隔离到各自的命名空间中封装 Windows 应用程序。Citrix Hypervisor 容器管理功能支持在 Windows Server 2016 来宾操作系统上监视和管理 Windows Server 容器。

注意：

必须为 Windows Server 2016 VM 配置一个或多个静态 IP 地址以用于 TLS 通信，因为 TLS 服务器证书将绑定到某些 IP 地址。

要为容器管理功能准备 Windows Server 容器，请执行以下操作：

1. 确保 VM 已安装 Citrix VM Tools，并且已按网络要求和安全中所述配置 VM 网络。
2. 按 [Microsoft 文档](#) 中所述在 VM 中安装 Windows Server 容器支持功能。Windows Server 容器不是 Hyper-V 容器。
3. 在文件夹 `C:\ProgramData\docker\config` 中创建一个名为 `daemon.json` 且包含以下内容的文件：

```
1 {
2
3     "hosts": ["tcp://0.0.0.0:2376", "npipe://"],
4     "tlsverify": true,
5     "tlscacert": "C:\ProgramData\docker\certs.d\ca.pem",
6     "tlscert": "C:\ProgramData\docker\certs.d\server-cert.pem",
7     "tlskey": "C:\ProgramData\docker\certs.d\server-key.pem"
```

```
8 }
```

4. 为容器管理功能准备 VM；请对池中的其中一个主机上的控制域 (dom0) 运行以下命令之一：

方案 1 (对于单用户 VM)：使用 Citrix Hypervisor 为此 VM 生成 TLS 证书。

重要：

此方案仅在单个用户访问 VM 的环境中是安全的。TLS 服务器和客户端密钥通过使用虚拟 CD 注入到 VM 中。在准备过程中，此信息可能会被恶意用户复制。

```
1 xscontainer-prepare-vm -v vm_uuid -u root --mode tls --generate-
  certs
```

其中 *vm\_uuid* 为要准备的 VM。按照屏幕上的说明进行操作，完成准备 Windows Server 容器的过程。该过程涉及与 dom0 和 VM 交互。

方案 2：使用外部生成的 TLS 证书配置 Citrix Hypervisor

```
1 xscontainer-prepare-vm -v vm_uuid -u root --mode tls \
2   --client-cert client_cert --client-key client_key --ca-cert
  ca_cert
```

其中，*vm\_uuid* 为要准备的 VM，*client\_cert* 为 TLS 客户端证书，*client\_key* 为 TLS 客户端密钥，*ca\_cert* 为 CA 证书。此方案假定已在 VM 中为 TLS 配置 Docker。

## 网络要求和安全

重要：

要使用容器管理功能，可能需要放宽与网络隔离有关的安全要求。

为使虚拟化环境具有最高安全性，我们建议管理员通过将 Citrix Hypervisor 的管理网络（包括 Citrix Hypervisor 控制域）与 VM 隔离对网络进行分区。

启用容器管理功能需要在这两个网络之间进行路由，这增加了恶意 VM 攻击管理网络（即 dom0）的风险。为了缓解允许在 VM 与管理网络进行通信的风险，我们建议配置防火墙规则，以仅允许可信源在这两个网络之间启动连接。

在以下情况下，请勿在生产中使用此功能：

- 如果建议的此网络配置与您的风险状况不一致
- 如果您缺乏必要的网络或防火墙专业知识来针对您的特定用例充分保护此路由的安全

## 网络分区和防火墙

与其他 VM 一样，请勿应将容器管理的 VM 直接连接到 Citrix Hypervisor 的管理网络来提供必要的隔离。

要使用容器管理功能，必须能够从 Citrix Hypervisor 的控制域 (dom0) 访问管理的 VM。要监视基于 Linux 的操作系统中的容器，网络连接拓扑和防火墙必须允许从 dom0 到容器管理的 VM 的出站 SSH 连接。要监视 Windows Server 容器，网络连接拓扑和防火墙必须允许从 dom0 到容器管理的 VM 的出站 Docker TLS (目标 TCP 端口 2376) 连接。为了缓解允许在 VM 与管理网络之间进行通信的风险，应通过外部有状态防火墙传输所有通信。必须由专业人员根据您的具体业务和安全要求手动设置和配置此防火墙。

下面是一个示例配置：

为确保网络之间的连接安全，请执行以下操作：

- 阻止 Citrix Hypervisor 管理网络 (包括 dom0) 与 VM 网络 (包括容器管理的 VM) 之间的所有连接。

添加启用容器管理功能的例外：

- 要监视基于 Linux 的操作系统，请允许 dom0 与容器管理的 VM 之间的出站 SSH (TCP 端口 22) 连接 (新连接以及已建立的连接)。
- 要监视 Windows Server 容器，请允许 dom0 与容器管理的 VM 之间的出站 Docker TLS (TCP 端口 2376) 连接 (新连接以及已建立的连接)。
- 允许容器管理的 VM 响应 dom0 启动的 (已建立) SSH 和 Docker TLS 连接。

#### 基于 **Linux** 的操作系统中的身份验证

Citrix Hypervisor 的容器管理功能使用池特有的 4096 位专用/公用 RSA 密钥对在容器管理的 VM 进行身份验证。私钥存储在 Citrix Hypervisor 控制域 (dom0) 中。相应的公钥在准备过程中使用云配置驱动器或 `~user/.ssh/authorized_keys` 文件在容器管理的 VM 中注册。与所有私钥/公钥对一样，必须安全地保存私钥，因为私钥允许无密码访问所有容器管理的 VM。此访问包括当前管理的 VM 以及过去管理的 VM。

Citrix Hypervisor 的容器管理功能将尝试通过 VM 中运行的 Citrix VM Tools 公告的 IP 地址访问容器管理的 VM。首次连接后，Citrix Hypervisor 会存储容器管理的 VM 的公钥，并验证该公钥在任何后续连接中是否匹配。请确保仅容器管理的 VM 可通过其公告的 IP (使用 IP Source Guard 或类似方法) 进行访问。如果网络拓扑无法确保此行为，我们建议管理员确认 SSH 主机密钥，该密钥是容器管理功能在首次与 VM 建立连接时获取的。

可以使用以下命令访问该密钥：

```
1 xe vm-param-get-uuid=vm_uuid param-name=other-config /
2 param-key=xcontainer-sshhostkey
```

*vm\_uuid* 为 VM 的 UUID

#### 适用于 **Windows Server** 容器的身份验证

Citrix Hypervisor 使用 SSL 或 TLS 监视和控制 Windows Server 容器。在此实例中，Citrix Hypervisor 用作 SSL/TLS 客户端，Windows Server VM 用作 SSL/TLS 服务器。密钥同时存储在 Dom0 和 VM 中。

**重要:**

- 客户端密钥必须安全保存，因为它允许无密码访问 VM 上的 Docker
- 必须安全地保存服务器密钥，因为该密钥用于对 VM 上的监视连接进行身份验证

Citrix Hypervisor 容器管理功能使用 `-generate-certs` 选项生成 TLS 证书和密钥时，会为某个特定池和 VM 生成临时 CA、服务器和客户端证书。证书使用 sha256 哈希，最长有效期为 2\*365 天。过了此时间后，应重复执行准备过程。TLS 连接总是使用 AES128-SHA 密码建立。

**注意**

使用 Citrix Hypervisor 容器管理功能和 Docker 时，请注意以下行为：

- 重命名容器不会触发更新容器管理视图的操作。此外，在 Ubuntu 14.04 上，从 XenCenter 外部暂停或取消暂停容器不会触发更新该视图的操作。此行为可能意味着 Citrix Hypervisor 可能不显示当前（已重命名/已暂停/已取消暂停）的容器状态。根本原因是视图仅刷新以下 Docker 事件通知。解决方法：可以通过对同一 VM 上的无关容器执行某项操作（即启动或停止）来触发刷新操作。

## vApp

September 5, 2019

vApp 是由一个或多个相关虚拟机 (VM) 组成的逻辑组，可以作为单个实体来启动。启动 vApp 时，vApp 中包含的 VM 将按照用户预定义的顺序启动。此功能支持彼此互相依赖的 VM 自动排序。在整个服务需要重新启动时（例如在软件更新后），管理员不再需要手动为依赖其他 VM 的 VM 指定启动顺序。vApp 中的 VM 不必位于同一个主机上，而是可以按照常规规则在池中分布。

在灾难恢复的情况下，vApp 功能很有用。您可以将位于同一个存储库中或与同一个服务级别协议 (SLA) 相关的所有 VM 分组到一起。

**注意:**

可以使用 XenCenter 和 xe CLI 创建和更改 vApp。有关使用 CLI 处理 vApp 的信息，请参阅[命令行接口](#)。

### 在 XenCenter 中管理 vApp

使用管理 **vApp** 对话框，可以在选定池中创建、删除、更改、启动、关闭、导入和导出 vApp。如果在列表中选择某个 vApp，其中包含的 VM 会列在右侧的详细信息窗格中。

可以使用管理 **vApp** 执行以下操作：

- 更改 vApp 的名称或说明
- 在 vApp 中添加或删除 VM

- 更改 vApp 中的 VM 的启动顺序

要更改 **vApp**，请执行以下操作：

1. 选择池，然后在池菜单上，选择管理 **vApp**。  
或者，在资源窗格中单击鼠标右键，然后选择快捷菜单上的管理 **vApp**。
2. 选择 vApp，然后选择属性以打开其“属性”对话框。
3. 选择常规选项卡以更改 vApp 的名称或说明。
4. 选择虚拟机选项卡以在 vApp 中添加或删除 VM。
5. 选择 **VM** 启动顺序选项卡以更改 vApp 中各个 VM 的启动顺序和延迟间隔值。
6. 单击确定保存所做的更改并关闭属性。

有关详细信息，请参阅 XenCenter 帮助。按 **F1** 或单击帮助可显示 XenCenter 帮助。

## 创建 vApp

要将多个 **VM** 一起分组到一个 **vApp** 中，请按照以下过程进行操作：

1. 选择池，然后在池菜单上，选择管理 **vApp**。
2. 输入 vApp 的名称和可选说明。单击下一步。  
可以选择自己喜欢的任何名称，但最好是描述 vApp 的名称。虽然建议不要创建多个同名的 vApp，但不是必须这样。XenCenter 不会强制要求 vApp 名称必须唯一。对于包含空格的名稱，不必使用引号。
3. 选择要包含在新 vApp 中的 VM。单击下一步。  
可以使用搜索字段仅列出名称中包含指定文本字符串的 VM。
4. 为 vApp 中的 VM 指定启动顺序。单击下一步。

| 值                | 说明                                                                                                        |
|------------------|-----------------------------------------------------------------------------------------------------------|
| 启动顺序             | 指定各个 VM 在 vApp 中的启动顺序，使某些 VM 先于其他 VM 重新启动。启动顺序值为 0（零）的 VM 将首先启动。启动顺序值为 1 的 VM 接着启动。然后顺序值为 2 的 VM 启动，以此类推。 |
| 尝试在以下时间后启动下一个 VM | 指定从启动 VM 到尝试启动启动顺序中下一组 VM 之间的等待时间。下一组是启动顺序靠后的一组 VM。                                                       |

1. 在管理 **vApp** 的最后一页上，可以检查 vApp 配置。单击上一步返回并更改任何设置，或者单击完成创建 vApp 并关闭管理 **vApp**。

注意：

一个 vApp 可以跨单个池中的多个服务器，但是不能跨多个池。

## 删除 vApp

要删除 vApp，请按照以下过程进行操作：

1. 选择池，然后在池菜单上，选择管理 vApp。
2. 在列表中选择要删除的 vApp。单击删除。

注意：

vApp 中的 VM 不会被删除。

## 使用 XenCenter 启动和关闭 vApp

要启动或关闭 vApp，请使用可从“池”菜单访问的管理 vApp。在启动 vApp 时，其中所有的 VM 都将自动按顺序启动。为每个 VM 指定的启动顺序和延迟间隔值控制启动序列。这些值可以在首次创建 vApp 时设置。可随时从 vApp 的“属性”对话框或各个 VM 的“属性”对话框更改这些值。

要启动 vApp，请执行以下操作：

1. 打开管理 vApp：选择 vApp 中的 VM 所在的池，在池菜单上，选择管理 vApp。或者，在资源窗格中单击鼠标右键，然后选择快捷菜单上的管理 vApp。
2. 选择 vApp，然后单击启动以启动其中包含的所有 VM。

要关闭 vApp，请执行以下操作：

1. 打开管理 vApp：选择 vApp 中的 VM 所在的池，在池菜单上，选择管理 vApp。或者，在资源窗格中单击鼠标右键，然后选择快捷菜单上的管理 vApp。
2. 选择 vApp，然后单击关闭以关闭该 vApp 中的所有 VM。

尝试对所有 VM 执行软关闭。如果无法执行软关闭，则执行强制关闭。

注意：

软关闭以正常方式关闭 VM，所有正在运行的进程都逐个停止。

强制关闭执行硬关闭，相当于拔出物理服务器。此方式不一定能关闭所有正在运行的进程。如果以此方式关闭 VM，可能会有丢失数据的风险。只有在无法执行软关闭时使用强制关闭。

## 导入和导出 vApp

vApp 可以作为 OVF/OVA 包导入和导出。有关详细信息，请参阅[导入和导出 VM](#)。

要导出 **vApp**，请执行以下操作：

1. 打开管理 **vApp**：在池菜单上，选择管理 **vApp**。
2. 在列表中选择要导出的 vApp。单击导出。
3. 按照将 **VM 导出为 OVF/OVA** 中所述的过程操作。

导出 vApp 可能需要一段时间。

要导入 **vApp**，请执行以下操作：

1. 打开管理 **vApp**：在池菜单上，选择管理 **vApp**。
2. 单击导入打开导入对话框。
3. 按照将 **VM 导入为 OVF/OVA** 中所述的过程操作。

在导入完成后，新的 vApp 将显示在管理 **vApp** 中的 vApp 列表中。

## 演示版 Linux 虚拟设备

September 5, 2019

我们提供基于 CentOS 5.5 发行版且具有完整功能的演示版 Linux 虚拟设备安装文件。

可以从 [Citrix Hypervisor 下载](#) 页面以单独的 *xva* 文件下载该设备。

可以将 *xva* 文件快速导入 XenCenter 中，以创建完全正常的 Linux 虚拟机。不需要执行其他配置步骤。

您可以通过演示版 Linux 虚拟设备快速而简便地部署 VM。可以使用此设备测试 Citrix Hypervisor 产品功能，例如实时迁移、动态内存控制和高可用性。演示版 Linux 虚拟设备中预先安装了 Citrix VM Tools。此外，该设备还包括预先配置的网络连接和一个用于测试目的的 Web 服务器。

### 警告：

请勿将演示版 Linux 虚拟设备用于运行生产工作负载。

## 导入演示版 Linux 虚拟设备

1. 从 [Citrix Hypervisor 下载](#) 页面下载演示版 Linux 虚拟设备。  
客户需要通过访问我的帐户来访问此页面。如果您没有 MyCitrix 帐户，可以在 Citrix 主页上注册。
2. 在资源窗格中，选择所需的主机或池，单击鼠标右键，然后选择导入。此时将显示导入向导。
3. 单击浏览，导航到计算机上所下载的演示版 Linux 虚拟设备 *xva* 文件的存储位置。
4. 单击下一步。

5. 选择目标 Citrix Hypervisor 服务器或池，然后单击下一步。
6. 选择要在其上创建虚拟设备磁盘的存储库，然后单击下一步。
7. 单击完成以导入虚拟设备。

注意：

首次启动该 VM 时，系统会提示您输入 root 用户密码。随后将显示该 VM 的 IP 地址。请务必记录该 IP 地址，因为测试时会用到该地址。

## 有用的测试

本节列出了一些有用的测试，执行这些测试可确保演示版 Linux 虚拟设备的配置正确无误。

1. 测试您是否连接到外部网络。

从 XenCenter 控制台登录 VM。运行以下命令向 Google 发送 ping 数据包并发回结果：

```
1 ping -c 10 google.com
```

安装的其他网络连接工具包括 ifconfig、netstat 和 tracepath。

2. 使用在 VM 引导时显示的 IP 地址，测试能否从外部计算机 ping 该 VM。
3. 测试是否配置了 Web 服务器。

在 Web 浏览器中，输入该 VM 的 IP 地址。此时将打开“Demonstration Linux Virtual Machine”（演示版 Linux 虚拟机）页面。此页面显示有关 VM 装载的磁盘、磁盘大小、位置和使用率的简要信息。

也可以使用此 Web 页面装载磁盘。

## 使用“Demonstration Linux Virtual Machine”（演示版 Linux 虚拟机）Web 页面装载磁盘

1. 在 XenCenter 中，向 VM 中添加一个虚拟磁盘。在资源窗格中选择该 VM，打开存储选项卡，然后单击添加。
2. 输入新虚拟磁盘的名称以及（可选）说明。
3. 输入新虚拟磁盘的大小。

确保用来存储虚拟磁盘的存储库有足够的空间存储新虚拟磁盘。

4. 选择用来存储新虚拟磁盘的 SR。
5. 单击创建添加新虚拟磁盘并关闭该对话框。
6. 单击控制台选项卡，使用常用工具根据需要对磁盘进行分区和格式化。
7. 刷新“Demonstration Linux Virtual Machine”（演示版 Linux 虚拟机）Web 页面，此时新磁盘将显示出来。
8. 单击安装。此操作将装载该磁盘，并显示文件系统信息。

有关添加虚拟磁盘的详细信息，请参阅 XenCenter 帮助。

## 虚拟机高级注释

September 5, 2019

本节介绍有关虚拟机的一些高级注释。

### VM 引导行为

对于 VM 引导时虚拟机 VDI 的行为，有两个选项：

注意：

必须先关闭 VM，才能更改其引导行为设置。

#### 永久 (Citrix Virtual Desktops - 专用桌面模式)

此行为是 VM 引导时的默认行为。VDI 处于上一次关机时的状态。

如果您打算允许用户对其桌面进行永久性更改，请选择此选项。要选择永久，请关闭 VM，然后输入以下命令：

```
1 xe vdi-param-set uuid=vdi_uuid on-boot=persist
```

#### 重置 (Citrix Virtual Desktops - 共享桌面模式)

在 VM 引导时，VDI 还原为上一次引导时的状态。VM 下次引导时，在 VM 运行时所做的任何更改都将丢失。

如果您打算交付用户无法进行永久性更改的标准化桌面，请选择此选项。要选择重置，请关闭 VM，然后输入以下命令：

```
1 xe vdi-param-set uuid=vdi_uuid on-boot=reset
```

警告：

更改 `on-boot=reset` 后，下次关闭/启动或重新启动时将放弃保存到 VDI 的所有数据。

### 使 ISO 库可供 Citrix Hypervisor 服务器使用

要使 ISO 库可供 Citrix Hypervisor 服务器使用，请创建一个外部 NFS 或 SMB/CIFS 共享目录。NFS 或 SMB/CIFS 服务器必须允许对该共享目录进行根访问。对于 NFS 共享，可通过在 NFS 服务器上的 `/etc/exports` 中创建共享条目时设置 `no_root_squash` 标志来允许访问。

然后，使用 XenCenter 连接 ISO 库，或连接到主机控制台并运行以下命令：

```
1 xe-mount-iso-sr host:/volume
```

要实现高级用途，可以向 `mount` 命令传递额外的参数。

要使 Windows SMB/CIFS 共享可供主机使用，请使用 XenCenter，或连接到主机控制台并运行以下命令：

```
1 xe-mount-iso-sr unc_path -t cifs -o username=myname/myworkgroup
```

将 `unc_path` 参数中的反斜杠替换为正斜杠。例如：

```
1 xe-mount-iso-sr //server1/myisos -t cifs -o username=johndoe/mydomain
```

装载共享后，任何可用的 ISO 都将列在 XenCenter 的从 **ISO** 库或 **DVD** 驱动器安装列表中。这些 ISO 还作为 CD 映像 CLI 命令中使用。

将 ISO 连接到合适的 Windows 模板。

## Windows 卷影复制服务 (VSS) 提供程序

Windows 工具还包含一个适用于 Citrix Hypervisor 的 VSS 提供程序，用于在为 VM 快照做准备的过程中使来宾文件系统静止。该 VSS 提供程序会作为 PV 驱动程序安装的一部分进行安装，但默认情况下不启用。

要启用 **Windows Citrix Hypervisor VSS** 提供程序，请执行以下操作：

1. 安装 Windows PV 驱动程序。
2. 导航至安装驱动程序的目录（默认情况下为 `c:\Program Files\Citrix\XenTools` 或 Windows 注册表中的 `HKEY_LOCAL_MACHINE\Software\Citrix\XenTools\Install_dir` 的值）。
3. 双击 `install-XenProvider.cmd` 命令以激活 VSS 提供程序。

注意：

- 卸载 PV 驱动程序时将自动卸载 VSS 提供程序。重新安装 VSS 驱动程序后，应再次将其启用。可以在同一目录中使用 `uninstall-XenProvider.cmd` 命令与 PV 驱动程序分开单独卸载 VSS 提供程序。
- 不支持在 GFS2 SR 上使用 VSS 快照。

## 使用远程桌面连接到 Windows VM

您可以使用以下方法之一查看 Windows VM 控制台，这两种方法均支持充分利用键盘和鼠标。

- 使用 XenCenter。此方法提供标准的图形控制台，并使用 Citrix Hypervisor 的内置 VNC 技术提供对虚拟机控制台的远程访问。
- 使用 Windows 远程桌面进行连接。此方法使用远程桌面协议技术。

在 XenCenter 中的控制台选项卡上，有一个切换到远程桌面按钮。此按钮可禁用 XenCenter 中的标准图形控制台，并切换为使用远程桌面。

如果在 VM 中未启用远程桌面，此按钮将处于禁用状态。要启用此按钮，请安装 Citrix VM Tools。按照下列过程在要使用远程桌面连接的每个 VM 中启用此按钮：

要在 **Windows VM** 上启用远程桌面，请执行以下操作：

1. 打开系统，方法是单击开始按钮，在计算机上单击鼠标右键，然后选择属性。
2. 单击远程设置。如果系统提示您输入管理员密码，请键入您在安装 VM 时创建的密码。
3. 在远程桌面区域中，单击标记为允许运行任意版本远程桌面的计算机连接的复选框 (Windows 7)。
4. 要选择可连接到此 Windows VM 的任何非管理员用户，请单击选择远程用户按钮，然后提供用户名。默认情况下，对 Windows 域拥有管理员权限的用户可以进行连接。

现在，您可以使用远程桌面连接到此 VM。有关详细信息，请参阅 Microsoft 知识库文章[使用“远程桌面连接”连接到另一台计算机](#)。

注意：

不能连接到处于睡眠或休眠状态的 VM。在远程计算机上将睡眠和休眠设置设置为从不。

### Windows VM 中的时间处理

对于 Windows 来宾系统，最初是由控制域时钟驱动时间。在 VM 生命周期操作（例如挂起和重新启动）期间，时间会更新。我们建议在控制域和所有 Windows VM 中运行可靠的 NTP 服务。

如果手动将 VM 设置为比控制域早 2 小时，则其将永久保留。在 VM 中使用时区偏差可能会将 VM 的时间提前。如果以后更改了控制域时间（手动或由 NTP 更改），VM 将相应做出调整，但会保持 2 小时的偏差。更改控制域时区不会影响 VM 时区或时差。Citrix Hypervisor 使用 VM 的硬件时钟设置来同步 VM。Citrix Hypervisor 不使用 VM 的系统时钟设置。

执行挂起和恢复操作或使用实时迁移功能时，请务必安装最新的 Citrix VM Tools。Citrix VM Tools 会在恢复（可能 在其他物理主机上）后向 Windows 内核通知需要进行时间同步。

注意：

如果您在 Citrix Virtual Desktops 环境中运行 Windows VM，必须确保主机时钟与 Active Directory (AD) 域具有相同来源。同步时钟失败会导致 VM 显示错误的时间，并导致 Windows PV 驱动程序崩溃。

### Linux VM 中的时间处理

Citrix Hypervisor 中的 Linux VM 的时间处理取决于 VM 是 PV 来宾系统还是 HVM 来宾系统。

除 Citrix Hypervisor 定义的行为外，操作系统设置和行为可以影响您的 Linux VM 的时间处理行为。某些 Linux 操作系统可能会定期同步其系统时钟和硬件时钟，或者操作系统可能会默认使用自己的 NTP 服务。有关详细信息，请参阅您的 Linux VM 的操作系统文档。

**注意：**

安装新 Linux VM 后，请确保将时区从默认 UTC 更改为本地值。有关特定发行版说明，请参阅 [Linux 发行说明](#)。

**PV Linux VM 中的时间处理**

对于半虚拟化的 Linux 发行版，有两种时钟行为 - 非独立和独立。

**非独立时钟：** PV Linux VM 中的系统时钟会与控制域中运行的时钟同步，并且无法独立更改。此模式很方便，因为只有控制域需要运行网络时间协议 (NTP) 服务来确保所有 VM 的时间准确。

**独立时钟：** PV Linux VM 中的系统时钟不与控制域中运行的时钟同步，并且可以更改。VM 启动时，控制域时间用于设置系统时钟的初始时间。

某些 PV Linux VM 可以使用 `independent_wallclock` 设置来更改 VM 的时钟行为。

下表列出了 PV Linux VM 的时钟行为：

| 来宾操作系统                                    | 默认时钟行为 | <code>independent_wallclock</code> 设置是否可用？ |
|-------------------------------------------|--------|--------------------------------------------|
| CentOS 5.x (32/64 位)                      | 非独立    | 是                                          |
| CentOS 6.x (32/64 位)                      | 独立     |                                            |
| Red Hat Enterprise Linux 5.x (32/64 位)    | 非独立    | 是                                          |
| Red Hat Enterprise Linux 6.x (32/64 位)    | 独立     |                                            |
| Oracle Linux 5.x (32/64 位)                | 非独立    | 是                                          |
| Oracle Linux 6.x (32/64 位)                | 独立     |                                            |
| Scientific Linux 6.x (32/64 位)            | 独立     |                                            |
| SLES 11 SP3、SP4 (32/64 位)                 | 独立     | 是 (无)                                      |
| SLES 12 SP1、SP2 (64 位)                    | 独立     | 是 (无)                                      |
| SLED 11 SP3、SP4 (64 位)                    | 独立     | 是 (无)                                      |
| SLED 12 SP1、SP2 (64 位)                    | 独立     | 是 (无)                                      |
| Debian 7 (32/64 位)                        | 独立     |                                            |
| NeoKylin Linux Advanced Server 6.5 (64 位) | 独立     |                                            |
| NeoKylin Linux Advanced Server 7.2 (64 位) | 独立     |                                            |

对于 `independent_wallclock` 设置可用的 PV Linux VM，可以使用此设置来定义 VM 具有非独立的时钟行为还是独立的时钟行为。

**重要：**

我们建议使用 `independent_wallclock` 设置来启用独立时钟行为，并在 Linux VM 和 Citrix Hypervisor 服务器上运行可靠的 NTP 服务。

要将单独的 **Linux VM** 设置为具有独立时钟行为，请执行以下操作：

1. 在 VM 上的根提示符下，运行以下命令：`echo 1 > /proc/sys/xen/independent_wallclock`
2. 通过更改 `/etc/sysctl.conf` 配置文件并添加以下内容，可以使此设置在每次重新启动后保持不变：

```
1 ## Set independent wall clock time
2 xen.independent_wallclock=1
```

3. 第三种备用方法是，也可以将 `independent_wallclock=1` 作为启动参数传递到 VM。

要将单独的 **Linux VM** 设置为具有非独立时钟行为，请执行以下操作：

1. 在 VM 上的根提示符下，运行以下命令：`echo 0 > /proc/sys/xen/independent_wallclock`
2. 通过更改 `/etc/sysctl.conf` 配置文件并添加以下内容，可以使此设置在每次重新启动后保持不变：

```
1 ## Set independent wall clock time
2 xen.independent_wallclock=0
```

3. 第三种备用方法是，也可以将 `independent_wallclock=0` 作为启动参数传递到 VM。

## HVM Linux VM

HVM Linux VM 中的硬件时钟不与控制域中运行的时钟同步，并且可以独立更改。VM 启动时，控制域时间用于设置硬件时钟和系统时钟的初始时间。

如果您更改了硬件时钟上的时间，此更改在 VM 重新启动时将持续存在。

系统时钟行为取决于 VM 的操作系统。有关详细信息，请参阅您的 VM 操作系统对应的文档。

不能更改 HVM Linux VM 的 Citrix Hypervisor 时间处理行为。

## 从经销商可选套件（锁定了 BIOS）介质安装 HVM VM

有两种类型的 HVM VM：BIOS 通用和 BIOS 自定义。要能够将 Windows 的经销商可选套件（锁定了 BIOS）OEM 版安装到 VM，应从随附了介质的主机中复制该 VM 的 BIOS 字符串。此外，高级用户可以将用户定义的值设置为 BIOS 字符串。

## BIOS 通用

VM 具有通用 Citrix Hypervisor BIOS 字符串。

### 注意：

如果 VM 在启动时未设置 BIOS 字符串，则会向该 VM 中插入标准的 Citrix Hypervisor BIOS 字符串，该 VM 将具有通用 BIOS。

## BIOS 自定义

对于 HVM VM，可以采用两种方式自定义 BIOS：复制主机 BIOS 字符串和用户定义的 BIOS 字符串。

### 复制主机 BIOS 字符串

VM 具有池中特定服务器的 BIOS 字符串的副本。要安装主机随附的锁定了 BIOS 的介质，请按照下面的过程进行操作。

### 使用 XenCenter：

1. 单击“新建 VM 向导”中的将主机 **BIOS** 字符串复制到 **VM** 复选框。

### 使用 CLI：

1. 运行 `vm-install copy-bios-strings-from` 命令。指定 `host-uuid` 作为从其复制字符串的主机（即，随附了介质的主机）：

```
1 xe vm-install copy-bios-strings-from=host uuid \  
2     template=template name sr-name-label=name of sr \  
3     new-name-label=name for new VM
```

此命令将返回新创建的 VM 的 UUID。

例如：

```
1 xe vm-install copy-bios-strings-from=46dd2d13-5aee-40b8-ae2c-95786 \  
2     ef4 \  
3     template="win7sp1" sr-name-label=Local\ storage \  
4     new-name-label=newcentos \  
5     7cd98710-bf56-2045-48b7-e4ae219799db
```

2. 如果将主机中的相关 BIOS 字符串成功复制到 VM 中，则 `vm-is-bios-customized` 命令会确认此操作已成功：

```
1 xe vm-is-bios-customized uuid=VM uuid
```

例如：

```

1 xe vm-is-bios-customized uuid=7cd98710-bf56-2045-48b7-e4ae219799db
2   This VM is BIOS-customized.

```

注意：

启动 VM 时，是在从其复制了 BIOS 字符串的物理主机上启动此 VM。

警告：

任何 EULA 都规定了如何使用安装的锁定了 BIOS 的所有操作系统，您必须遵守其中的规定。

### 用户定义的 BIOS 字符串

用户可以选择使用 CLI/API 在选定的 BIOS 字符串中设置自定义值。要在具有自定义的 BIOS 的 HVM VM 中安装介质，请按照下面的过程进行操作。

使用 CLI：

1. 运行 `vm-install` 命令（不带 `copy-bios-strings-from`）：

```

1 xe vm-install template=template name sr-name-label=name of sr \
2   new-name-label=name for new VM

```

此命令将返回新创建的 VM 的 UUID。

例如：

```

1 xe vm-install template="win7sp1" sr-name-label=Local\ storage \
2   new-name-label=newcentos
3   7cd98710-bf56-2045-48b7-e4ae219799db

```

2. 要设置用户定义的 BIOS 字符串，请在首次启动 VM 之前运行以下命令：

```

1 xe vm-param-set uuid=VM_UUID bios-strings:bios-vendor=VALUE \
2   bios-strings:bios-version=VALUE bios-strings:system-
3   manufacturer=VALUE \
4   bios-strings:system-product-name=VALUE bios-strings:system-
5   version=VALUE \
6   bios-strings:system-serial-number=VALUE bios-strings:enclosure
7   -asset-tag=VALUE

```

例如：

```

1 xe vm-param-set uuid=7cd98710-bf56-2045-48b7-e4ae219799db \
2   bios-strings:bios-vendor="vendor name" \
3   bios-strings:bios-version=2.4 \

```

```
4 bios-strings:system-manufacturer="manufacturer name" \  
5 bios-strings:system-product-name=guest1 \  
6 bios-strings:system-version=1.0 \  
7 bios-strings:system-serial-number="serial number" \  
8 bios-strings:enclosure-asset-tag=abk58hr
```

**注意：**

- 1 - 在单个 CLI/API 调用中设置用户定义的 BIOS 字符串后，将不能进行修改。 - 您可以决定要为设置用户定义的 BIOS 字符串提供的参数数量。

**警告：****您需要：**

- 遵从适用于要在 VM 的 BIOS 中设置的值的所有 EULA 和标准。
- 确保为参数提供的值属于有效参数。提供不正确的参数会导致引导/介质安装失败。

## 为 Windows VM 分配 GPU（与 Citrix Virtual Desktops 结合使用）

您可以通过 Citrix Hypervisor 将 Citrix Hypervisor 服务器中的物理 GPU 分配给同一主机上运行的 Windows VM。需要高性能图形能力的图形高级用户（例如 CAD 设计师）可从此 GPU 直通功能受益。仅支持与 Citrix Virtual Desktops 结合使用。

尽管 Citrix Hypervisor 支持每个 VM 仅使用一个 GPU，但是它会自动检测同一池中各主机上完全相同的物理 GPU 并对其进行分组。将某个 VM 分配给一组 GPU 之后，该 VM 可以在池中具有该组内可用 GPU 的任何主机上启动。VM 连接到 GPU 后，其具有的某些功能（包括实时迁移、含内存数据的 VM 快照和挂起/恢复）将不再可用。

为池中的 VM 分配 GPU 不会干扰池中其他 VM 的运行。但是，连接 GPU 的 VM 将被视为不具有灵活性。如果连接了 GPU 的 VM 属于启用了高可用性的池，则这两项功能将忽略这些 VM。这些 VM 无法自动迁移。

GPU 直通功能仅适用于 Windows VM。可以使用 XenCenter 或 xe CLI 启用该功能。

**要求**

特定的计算机和 GPU 支持 GPU 直通功能。在所有情况下，Citrix Hypervisor 服务器上都必须提供并启用 IOMMU 芯片组功能（对于 Intel 型号称为 VT-d）。在启用 GPU 直通功能之前，请访问[硬件兼容性列表](#)。

### 为 VM 分配 GPU 之前的准备工作

在为 VM 分配 GPU 之前，应将相应的物理 GPU 装到您的 Citrix Hypervisor 服务器中，然后重新启动该计算机。在重新启动时，Citrix Hypervisor 会自动检测任何物理 GPU。要查看池中各个主机上的所有物理 GPU，请使用

`xe pgpu-list` 命令。

确保在主机上启用 IOMMU 芯片组功能。为此，请输入以下命令：

```
1 xe host-param-get uuid=uuid_of_host param-name=chipset-info param-key=iommu
```

如果输出的值为 **false**，表示未启用 IOMMU，因此无法通过指定的 Citrix Hypervisor 服务器使用 GPU 直通功能。

要使用 **XenCenter** 为 **Windows VM** 分配 **GPU**，请执行以下操作：

1. 关闭要为其分配 GPU 的 VM。
2. 打开 VM 属性：右键单击 VM，然后选择属性。
3. 为该 VM 分配 GPU：从 VM 属性列表中选择 GPU，然后选择一种 GPU 类型。单击确定。
4. 启动 VM。

要使用 **xe CLI** 为 **Windows VM** 分配 **GPU**，请执行以下操作：

1. 使用 `xe vm-shutdown` 命令关闭要为其分配 GPU 组的 VM。
2. 通过输入以下命令显示该 GPU 组的 UUID：

```
1 xe gpu-group-list
```

此命令将输出池中的所有 GPU 组。请记录相应 GPU 组的 UUID。

3. 通过输入以下命令将该 VM 连接到相应的 GPU 组：

```
1 xe vpgu-create gpu-group-uuid=uuid_of_gpu_group vm-uuid=uuid_of_vm
```

要确保已连接该 GPU 组，请运行 `xe vgpu-list` 命令。

4. 使用 `xe vm-start` 命令启动该 VM。
5. 启动后，在该 VM 上安装图形卡驱动程序。

必须安装驱动程序，使 VM 能够直接访问主机上的硬件。驱动程序由硬件供应商提供。

注意：

如果您尝试在相应 GPU 组中没有可用 GPU 的主机上启动具有 GPU 直通功能的 VM，Citrix Hypervisor 会输出错误。

要使用 **XenCenter** 将 **Windows VM** 与 **GPU** 分离，请执行以下操作：

1. 关闭 VM。
2. 打开 VM 属性：右键单击 VM，然后选择属性。
3. 将 GPU 与 VM 分离：从 VM 属性列表中选择 **GPU**，然后选择无作为 GPU 类型。单击确定。

4. 启动 VM。

要使用 **xe CLI** 将 **Windows VM** 与 **GPU** 分离，请执行以下操作：

1. 使用 `xe vm-shutdown` 命令关闭 VM。
2. 通过输入以下命令显示与 VM 相连的 vGPU 的 UUID：

```
1 xe vgpu-list vm-uuid=uuid_of_vm
```

3. 通过输入以下命令将 GPU 与 VM 分离：

```
1 xe vgpu-destroy uuid=uuid_of_vgpu
```

4. 使用 `xe vm-start` 命令启动该 VM。

## 创建 ISO 映像

Citrix Hypervisor 可使用 ISO 映像作为 Windows 或 Linux VM 的安装介质和数据来源。本节说明如何通过 CD/DVD 介质创建 ISO 映像。

要在 **Linux** 系统上创建 **ISO**，请执行以下操作：

1. 将 CD- 或 DVD-ROM 磁盘放入驱动器。请确保未装载磁盘。要进行检查，请运行以下命令：

```
1 mount
```

如果光盘已装载，请将其卸载。如有必要，请参阅您的操作系统文档以寻求帮助。

2. 以 root 用户身份运行以下命令：

```
1 dd if=/dev/cdrom of=/path/cding_filename.iso
```

此命令需要一些时间。成功完成该操作后，您将看到类似如下所示的内容：

```
1 1187972+0 records in
2 1187972+0 records out
```

您的 ISO 文件已就绪。

要在 **Windows** 系统上创建 **ISO**，请执行以下操作：

Windows 计算机没有创建 ISO 的等效操作系统命令。大多数 CD 刻录工具可将 CD 另存为 ISO 文件。

## 为 Linux VM 启用 VNC

September 5, 2019

默认情况下，不会将 VM 设置为支持虚拟网络计算 (Virtual Network Computing, VNC)，Citrix Hypervisor 使用该计算方法远程控制 VM。为了可以与 XenCenter 连接，需要确保 VNC 服务器和 X 显示管理器安装在 VM 中并进行了正确的配置。本节介绍如何在支持的每个 Linux 操作系统发行版中配置 VNC 以便能够与 XenCenter 正确交互。

对于基于 CentOS 的 VM，请参照下文中有基于 Red Hat 的 VM 的说明，因为它们使用相同的基础代码提供图形 VNC 访问。CentOS X 建立在 Red Hat Enterprise Linux X 的基础之上。

## 在 Debian VM 上启动图形控制台

### 注意：

在 Debian VM 上启用图形控制台之前，请确保已安装 Linux 来宾代理。有关详细信息，请参阅[安装 Linux 来宾代理](#)。

Debian 虚拟机的图形控制台由在该 VM 内部运行的 VNC 服务器提供。在建议的配置中，由一个标准显示管理器控制台，以便提供登录对话框。

1. 使用桌面系统软件包安装 Debian 来宾系统，或使用 apt（按照标准过程）安装 GDM（显示管理器）。
2. 使用 `apt-get`（或类似命令）安装 Xvnc 服务器：

```
1 apt-get install vnc4server
```

### 注意：

Debian 图形桌面环境使用 Gnome Display Manager 版本 3 守护程序，会耗费大量 CPU 时间。请按如下所示卸载 Gnome Display Manager `gdm3` 软件包并安装 `gdm` 软件包：

```
1 apt-get install gdm
2 apt-get purge gdm3
```

3. 使用 `vncpasswd` 命令设置 VNC 密码（不设置密码将存在严重的安全风险）。传入一个文件名以向其写入密码信息。例如：

```
1 vncpasswd /etc/vncpass
```

4. 修改您的 `gdm.conf` 文件 (`/etc/gdm/gdm.conf`) 以配置 VNC 服务器来管理显示 0，即按如下所示扩展 `[servers]` 和 `[daemon]` 部分：

```
1 [servers]
2 0=VNC
3 [daemon]
4 VTAllocation=false
5 [server-VNC]
6 name=VNC
7 command=/usr/bin/Xvnc -geometry 800x600 -PasswordFile /etc/
    vncpass BlacklistTimeout=0
```

```
8 flexible=true
```

5. 重新启动 GDM，然后等待 XenCenter 检测图形控制台：

```
1 /etc/init.d/gdm restart
```

注意：

可以使用类似于 `ps ax | grep vnc` 的命令检查 VNC 服务器是否正在运行。

## 在 Red Hat、CentOS 或 Oracle Linux VM 中启用图形控制台

注意：

为 VNC 设置 Red Hat VM 之前，请确保已安装了 Linux 来宾代理。有关详细信息，请参阅[安装 Linux 来宾代理](#)。

要在 Red Hat VM 中配置 VNC，请修改 GDM 配置。GDM 配置保存在一个文件中，该文件位置会根据使用的 Red Hat Linux 版本的不同而有所差异。修改之前，先确定此配置文件的位置。在本节后续几个过程中将修改此文件。

注意：

有关为 RHEL、CentOS 或 OEL 6.x VM 启用 VNC 的信息，请参阅为 RHEL、CentOS 或 OEL 6 VM 启用 VNC。

### 确定 VNC 配置文件的位置

如果您使用的是 Red Hat Linux 版本 5.x，则 GDM 配置文件为 `/etc/gdm/custom.conf`。此文件是一个拆分的配置文件，仅包含用于覆盖默认配置的用户指定值。在较新版本的 GDM 中，将默认使用此文件类型。此类型的文件包含在这些版本的 Red Hat Linux 中。

### 配置 GDM 以使用 VNC

1. 以 root 用户身份在 VM 中的文本 CLI 上，运行 `rpm -q vnc-server gdm` 命令。将显示软件包名称 `vnc-server` 和 `gdm`，并指定了它们的版本号。

显示的软件包名称表明已安装相应软件包。如果出现提示未安装某个软件包的消息，则您可能在安装过程中未选择图形桌面选项。安装相应软件包后才能继续。有关在 VM 上安装更多软件的详细信息，请参阅相应的《Red Hat Linux x86 安装指南》。

2. 使用您喜欢的文本编辑器打开 GDM 配置文件，然后将下列行添加到文件中：

```
1 [server-VNC]
2 name=VNC Server
3 command=/usr/bin/Xvnc -SecurityTypes None -geometry 1024x768 -
   depth 16 \
4 -BlacklistTimeout 0
5 flexible=true
```

对于 Red Hat Linux 5.x 中的配置文件，应将这些命令行添加到空的 `[servers]` 部分中。

3. 修改配置，以便使用 `Xvnc` 服务器而不是标准 X 服务器：

- `0=Standard`

请将其修改为：

`0=VNC`

- 如果您使用的是 Red Hat Linux 5.x 或更高版本，则应在 `[servers]` 部分下面、`[server-VNC]` 部分之前添加以上行。

4. 保存并关闭该文件。

运行 `/usr/sbin/gdm-restart` 命令来重新启动 GDM 以使对配置所做的更改生效。

注意：

Red Hat Linux 将运行级别 5 用于图形启动。如果安装的软件以运行级别 3 启动，请更改此配置以便显示管理器能够启动并访问图形控制台。有关详细信息，请参阅查看运行级别。

## 防火墙设置

默认情况下，防火墙配置不允许进行 VNC 通信。如果您在 VM 和 XenCenter 间设置了防火墙，则应允许通过 VNC 连接使用的端口传输通信。默认情况下，VNC 服务器在 TCP 端口 `5900 + n` 上侦听来自 VNC 查看器的连接，其中 `n` 为显示号（通常为 0）。因此，为 `Display-0` 设置的 VNC 服务器将侦听 TCP 端口 5900，为 `Display-1` 设置的 VNC 服务器将侦听 `TCP-5901`，依此类推。请参考防火墙文档，确保这些端口已打开。

如果希望使用 IP 连接跟踪或将连接限制为仅从一端启动，则应进一步配置防火墙。

要配置基于 **Red Hat** 的 **VM** 防火墙以打开 **VNC** 端口，请执行以下操作：

1. 对于 Red Hat Linux 5.x，使用 `system-config-securitylevel-tui`。
2. 选择自定义，然后将 5900 添加到其他端口列表中。

或者，也可以通过运行 `service iptables stop` 命令在下次重新启动之前一直禁用防火墙，或通过运行 `chkconfig iptables off` 将其永久禁用。此配置可能会向外部环境公开额外的服务并降低 VM 的整体安全性。

## VNC 屏幕分辨率

连接到具有图形控制台的 VM 后，屏幕分辨率有时不匹配。例如，该 VM 的显示屏幕太大，无法与图形控制台窗格很好地相配。可以按如下所示通过设置 VNC 服务器的 `geometry` 参数来控制此行为：

1. 使用您喜欢的文本编辑器打开 GDM 配置文件。有关详细信息，请参阅确定 VNC 配置文件的位置。
2. 找到上面添加的 `[server-VNC]` 部分。
3. 例如，将命令行编辑为：

```
1 command=/usr/bin/Xvnc -SecurityTypes None -geometry 800x600
```

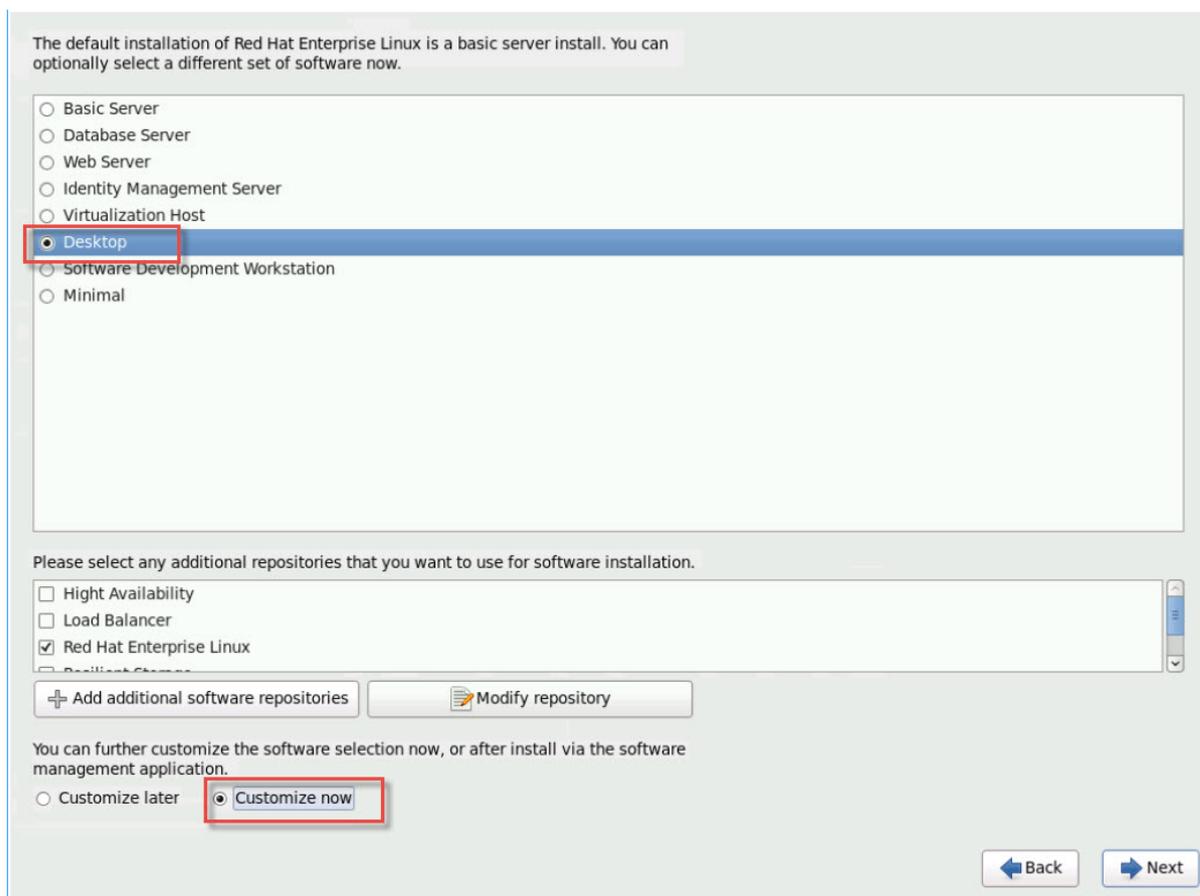
`geometry` 参数的值可以是任何有效的屏幕宽度和高度。

4. 保存并关闭该文件。

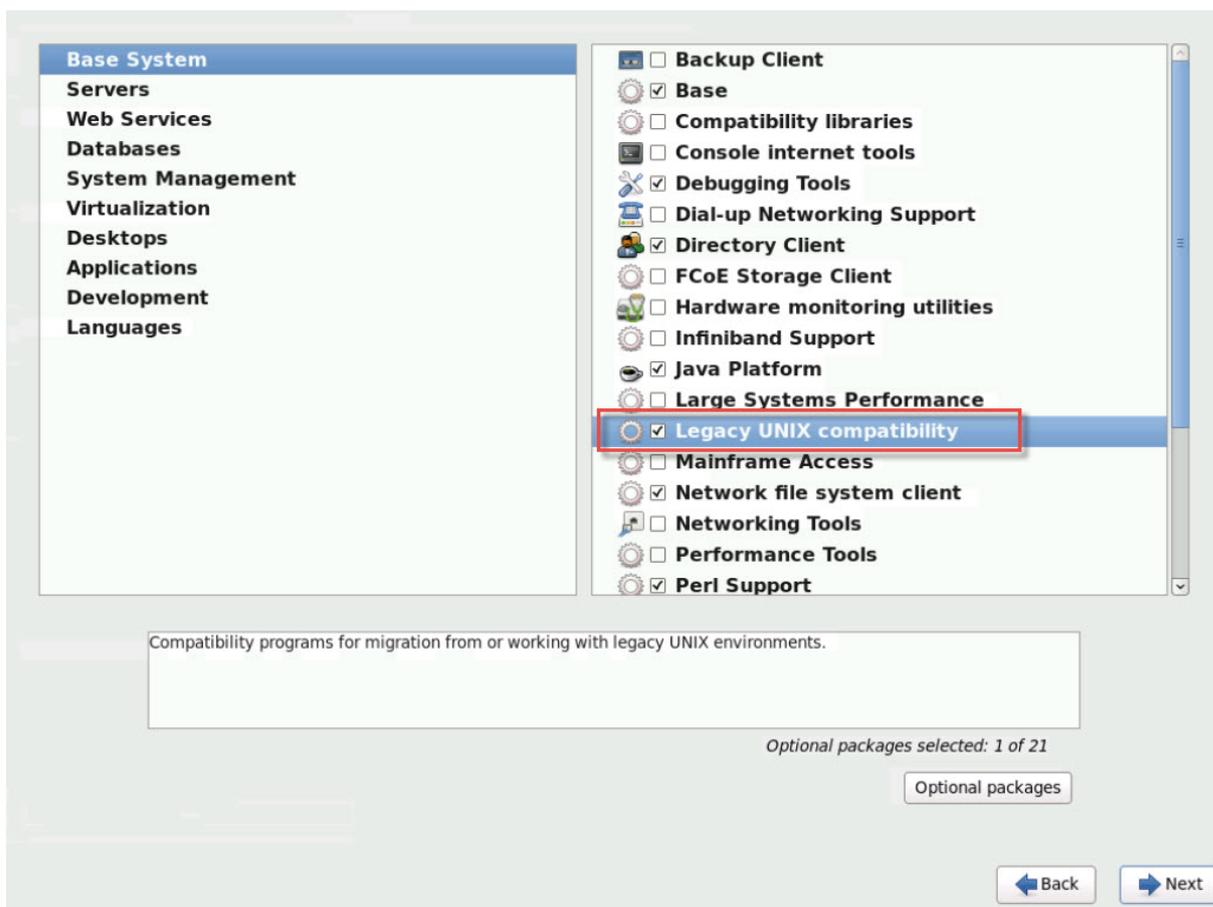
#### 为 RHEL、CentOS 或 OEL 6 VM 启用 VNC

如果您使用的是 Red Hat Linux 版本 6.x，则 GDM 配置文件为 `/etc/gdm/custom.conf`。此文件是一个拆分的配置文件，仅包含用于覆盖默认配置的用户指定值。默认情况下，在较新的 GDM 版本中使用此类型的文件，并且此类型的文件包含在这些版本的 Red Hat Linux 中。

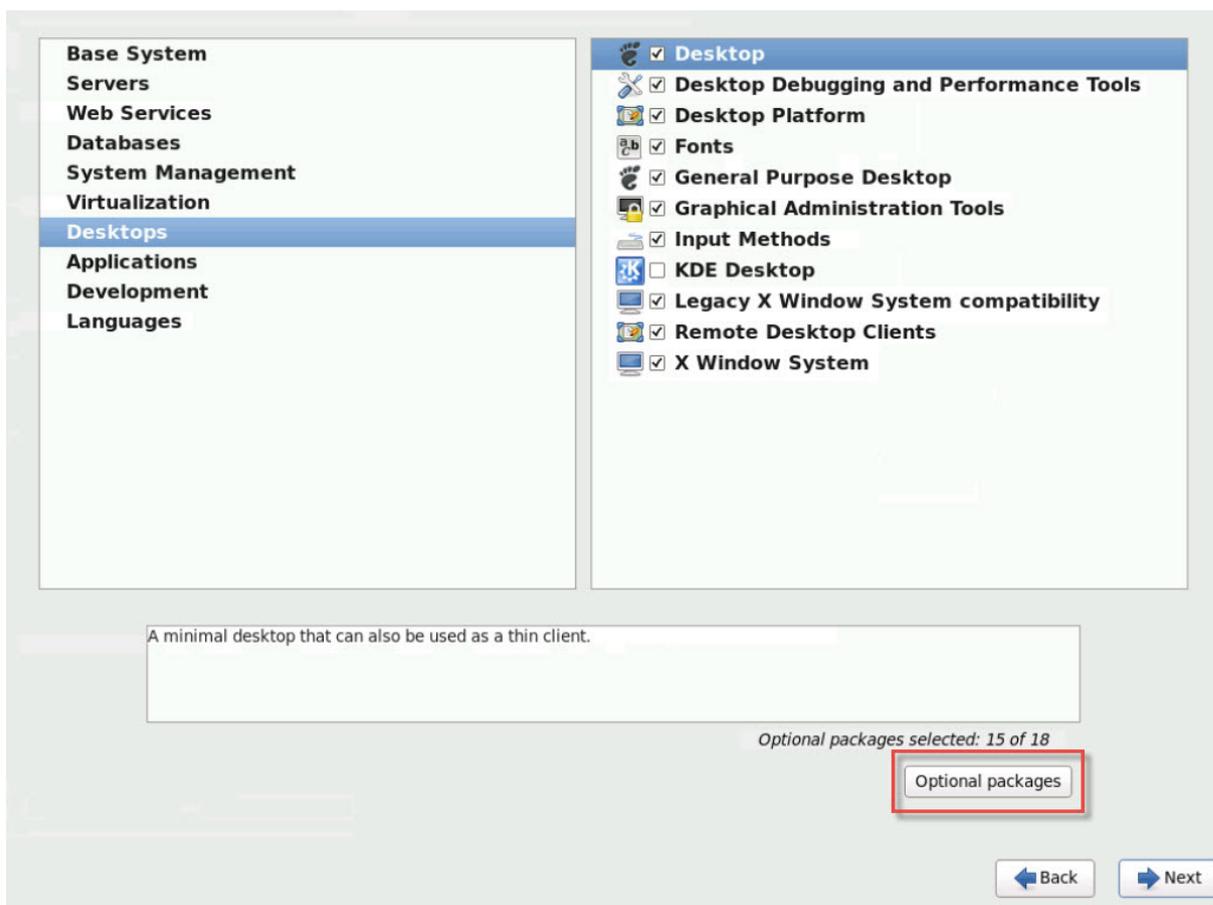
操作系统安装过程中，选择 **Desktop**（桌面）模式。在 RHEL 安装屏幕上，依次选择 **Desktop**（桌面）> **Customize now**（立即自定义），然后单击 **Next**（下一步）：



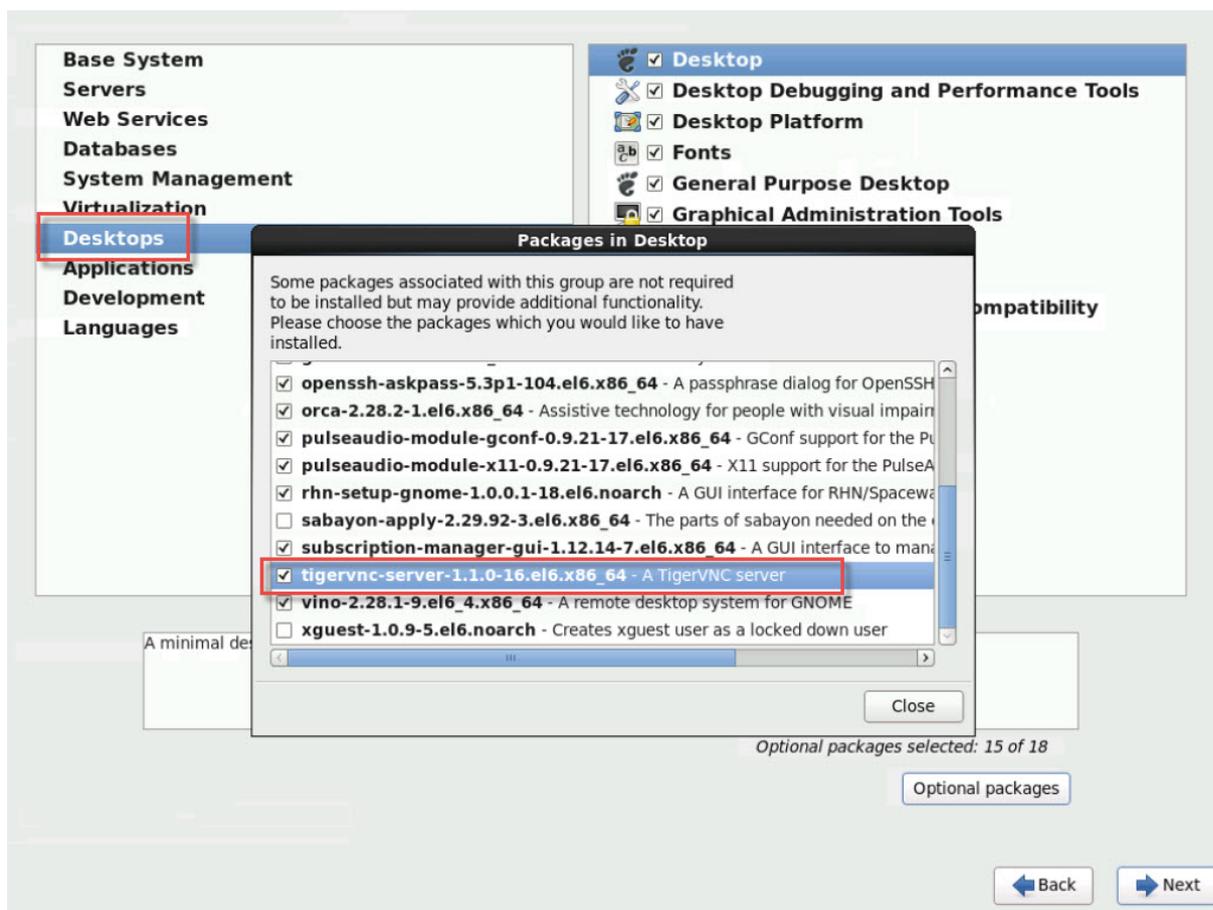
此操作将显示“Base System”（基本系统）屏幕，请务必选择 **Legacy UNIX compatibility**（旧 UNIX 兼容性）：



依次选择 **Desktops** (桌面) > **Optional packages** (可选软件包), 然后单击 **Next** (下一步):



此操作将显示 **Packages in Desktop**（桌面中的软件包）窗口，请选择 **tigervnc-server-<version\_number>**，然后单击 **Next**（下一步）：



完成以下步骤，以继续设置您的 RHEL 6.x VM：

1. 使用您喜欢的文本编辑器打开 GDM 配置文件，然后将下列行添加到相应的部分：

```

1     [security]
2     DisallowTCP=false
3
4     [xdmcp]
5     Enable=true

```

2. 创建文件 `/etc/xinetd.d/vnc-server-stream`：

```

1     service vnc-server
2     {
3
4         id = vnc-server
5         disable = no
6         type = UNLISTED
7         port = 5900
8         socket_type = stream
9         wait = no

```

```
10         user = nobody
11         group = tty
12         server = /usr/bin/Xvnc
13         server_args = -inetd -once -query localhost -
14             SecurityTypes None \
15             -geometry 800x600 -depth 16
16     }
```

3. 输入以下命令以启动 `xinetd` 服务：

```
1 # service xinetd start
```

4. 打开文件 `/etc/sysconfig/iptables`。将以下行添加到内容为 `-A INPUT -j REJECT --reject-with icmp-host-prohibited` 的行上方：

```
1 -A INPUT -m state --state NEW -m tcp -p tcp --dport 5900 -j ACCEPT
```

5. 输入以下命令以重新启动 `iptables`：

```
1 # service iptables restart
```

6. 输入以下命令以重新启动 `gdm`：

```
1 # telinit 3
2 # telinit 5
```

**注意：**

Red Hat Linux 将运行级别 5 用于图形启动。如果安装的软件以运行级别 3 启动，请更改此配置以便显示管理器能够启动并访问图形控制台。有关详细信息，请参阅查看运行级别。

## 为 VNC 设置基于 SLES 的 VM

**注意：**

在为 VNC 设置 SUSE Linux Enterprise Server VM 之前，请确保已安装了 Linux 来宾代理。有关详细信息，请参阅[安装 Linux 来宾代理](#)。

SLES 支持在 YaST 中以一个配置选项方式启用“Remote Administration”（远程管理）。可以选择在安装时启用远程管理（在 SLES 安装程序的网络服务屏幕上提供）。您可以通过此功能将外部 VNC 查看器连接到您的来宾系统以允许您查看图形控制台。使用 SLES 远程管理功能的方法与 XenCenter 提供的方法稍有不同。但是，可以修改 SUSE Linux VM 中的配置文件，以便该 VM 与图形控制台功能集成。

## 检查 VNC 服务器

进行配置更改前，请验证是否安装了 VNC 服务器。默认情况下，SUSE 附带 `tightvnc` 服务器。此服务器适合作为 VNC 服务器使用，但您也可以使用标准 RealVNC 发行版。

可以通过运行以下命令检查是否安装了 `tightvnc` 软件：

```
1 rpm -q tightvnc
```

## 启用远程管理

如果在 SLES 软件安装过程中未启用远程管理，可以执行以下步骤启用该功能：

1. 在 VM 中打开文本控制台，然后运行 YaST 实用程序：

```
1 yast
```

2. 使用箭头键选择左侧菜单中的 **Network Services**（网络服务）。按 **Tab** 键切换到右侧菜单，然后使用箭头键选择 **Remote Administration**（远程管理）。按 **Enter** 键。
3. 在 **Remote Administration**（远程管理）屏幕中，按 **Tab** 键切换到 **Remote Administration Settings**（远程管理设置）部分。使用箭头键选择 **Allow Remote Administration**（允许远程管理），然后按 **Enter** 键在复选框中标记 X。
4. 按 **Tab** 键切换到 **Firewall Settings**（防火墙设置）部分。使用箭头键选择 **Open Port in Firewall**（在防火墙中打开端口），然后按 **Enter** 键在复选框中标记 X。
5. 按 **Tab** 键切换到 **Finish**（完成）按钮，然后按 **Enter** 键。
6. 此时将显示一个消息框，提示您重新启动显示管理器以使设置生效。按 **Enter** 键确认消息。
7. 此时将显示 YaST 的原始顶层菜单。按 **Tab** 键切换到 **Quit**（退出）按钮，然后按 **Enter** 键。

## 修改 xinetd 配置

启用“Remote Administration”（远程管理）后，如果希望允许 XenCenter 进行连接，则修改一个配置文件。或者，也可以使用一个第三方 VNC 客户端。

1. 在首选文本编辑器中，打开文件 `/etc/xinetd.d/vnc`。
2. 该文件包含类似下面的部分：

```
1 service vnc1
2 {
3
4     socket_type = stream
```

```
5 protocol = tcp
6 wait = no
7 user = nobody
8 server = /usr/X11R6/bin/Xvnc
9 server_args = :42 -inetd -once -query localhost -geometry 1024
   x768 -depth 16
10 type = UNLISTED
11 port = 5901
12 }
```

### 3. 将 port 行编辑为

```
1 port = 5900
```

### 4. 保存并关闭该文件。

### 5. 使用下列命令重新启动显示管理器和 xinetd 服务：

```
1 /etc/init.d/xinetd restart
2 rcxdm restart
```

SUSE Linux 将运行级别 5 用于图形启动。如果未显示远程桌面，请验证是否已将 VM 配置为以运行级别 5 启动。有关详细信息，请参阅查看运行级别。

## 防火墙设置

默认情况下，防火墙配置不允许进行 VNC 通信。如果您在 VM 和 XenCenter 间设置了防火墙，则应允许通过 VNC 连接使用的端口传输通信。默认情况下，VNC 服务器在 TCP 端口 5900 + n 上侦听来自 VNC 查看器的连接，其中 n 为显示号（通常为 0）。因此，为 Display-0 设置的 VNC 服务器将侦听 TCP 端口 5900，为 Display-1 设置的 VNC 服务器将侦听 TCP-5901，依此类推。请参考防火墙文档，确保这些端口已打开。

如果希望使用 IP 连接跟踪或将连接限制为仅从一端启动，则应进一步配置防火墙。

要在 **SLES 11.x VM** 防火墙中打开 **VNC** 端口，请执行以下操作：

#### 1. 在 VM 中打开文本控制台，然后运行 YaST 实用程序：

```
1 yast
```

#### 2. 使用箭头键选择左侧菜单中的 **Security and Users**（安全性与用户）。按 **Tab** 键切换到右侧菜单，然后使用箭头键选择 **Firewall**（防火墙）。按 **Enter** 键。

#### 3. 在 **Firewall**（防火墙）屏幕中，使用箭头键选择左侧菜单中的 **Custom Rules**（自定义规则），然后按 **Enter** 键。

- 按 **Tab** 键切换到 **Custom Allowed Rules**（自定义允许的规则）部分中的 **Add**（添加）按钮，然后按 **Enter** 键。
- 在 **Source Network**（源网络）字段中，输入 `0/0`。按 **Tab** 键切换到 **Destination Port**（目标端口）字段并输入 `5900`。
- 按 **Tab** 键切换到 **Add**（添加）按钮，然后按 **Enter** 键。
- 按 **Tab** 键切换到 **Next**（下一步）按钮，然后按 **Enter** 键。
- 在 **Summary**（摘要）屏幕中，按 **Tab** 键切换到 **Finish**（完成）按钮并按 **Enter** 键。
- 在顶层 YaST 屏幕中，按 **Tab** 键切换到 **Quit**（退出）按钮并按 **Enter** 键。
- 使用下列命令重新启动显示管理器和 `xinetd` 服务：

```
1 /etc/init.d/xinetd restart
2 rcxdm restart
```

或者，也可以通过运行 `rcSuSEfirewall2 stop` 命令，在下次重新启动之前一直禁用防火墙，或使用 YaST 永久禁用防火墙。此配置可能会向外部环境公开额外的服务并降低 VM 的整体安全性。

## VNC 屏幕分辨率

连接到具有图形控制台的虚拟机后，屏幕分辨率有时不匹配。例如，该 VM 的显示屏幕太大，无法与图形控制台窗格很好地相配。可以按如下所示通过设置 VNC 服务器的 `geometry` 参数来控制此行为：

- 使用首选文本编辑器打开 `/etc/xinetd.d/vnc` 文件并查找与 `displayID 1` 对应的 `service_vnc1` 部分。
- 将 `server-args` 行中的 `geometry` 参数编辑为所需的显示分辨率。例如，

```
1 server_args = :42 -inetd -once -query localhost -geometry 800x600
   -depth 16
```

`geometry` 参数的值可以是任何有效的屏幕宽度和高度。

- 保存并关闭该文件。
- 重新启动 VNC 服务器：

```
1 /etc/init.d/xinetd restart
2 rcxdm restart
```

## 查看运行级别

Red Hat 和 SUSE Linux VM 将运行级别 5 用于图形启动。本节介绍如何确认 VM 以运行级别 5 启动，以及如何更改此设置。

1. 检查 `/etc/inittab` 以查看设置的默认运行级别。查找以下行:

```
1 id:n:initdefault:
```

如果  $n$  不是 5, 请编辑文件将其更改为 5。

2. 可以在更改后运行 `telinit q ; telinit 5` 命令, 以避免必须重新启动才能改变运行级别。

## 对 VM 问题进行故障排除

September 5, 2019

Citrix 提供两种形式的支持:

- [Citrix Web 站点] ([www.citrix.com/support](http://www.citrix.com/support)) 上的免费自助支持
- 可以从支持站点购买的付费支持服务。

通过 Citrix 技术支持, 您可以在遇到技术问题时, 打开在线支持案例或者通过电话与支持中心联系。

[Citrix 支持](#) 站点包含许多资源, 当您遇到异常行为、崩溃或其他问题时, 这些资源可能会对您有所帮助。资源包括: 技术支持论坛、知识库文章和产品文档。

本节旨在帮助您解决遇到的异常 VM 行为。本部分还提供了应用程序日志所在位置以及其他有助于您的 Citrix Hypervisor 解决方案提供商跟踪并解决问题的信息。

重要:

请仅在您的 Citrix Hypervisor 解决方案提供商或技术支持团队的指导下利用本节的故障排除信息解决问题。

供应商更新: 请使用操作系统供应商提供的更新, 对 VM 进行更新。供应商可能会提供针对 VM 崩溃和其他故障的修复。

## VM 崩溃

如果遇到 VM 崩溃, 内核故障转储可能会帮助您发现问题。请重现崩溃 (如有可能) 并按照此过程进行操作。请咨询来宾操作系统供应商, 以对此问题进行进一步调查。

### 控制 Linux VM 故障转储行为

对于 Linux VM, 可以通过 `actions-after-crash` 参数控制故障转储行为。以下是可能的值:

| 值                     | 说明                  |
|-----------------------|---------------------|
| <code>preserve</code> | 使 VM 处于暂停状态。(供分析使用) |

| 值                    | 说明                       |
|----------------------|--------------------------|
| <code>restart</code> | 不进行核心转储，仅重新启动 VM。（这是默认值） |
| <code>destroy</code> | 不进行核心转储，使 VM 处于停止状态。     |

对 **Linux VM** 故障转储启用保存功能：

1. 在 Citrix Hypervisor 服务器上，通过运行以下命令确定所需 VM 的 UUID：

```
1 xe vm-list name=label=name params=uuid --minimal
```

2. 使用 `xe vm-param-set` 更改 `actions-after-crash` 值；例如，在 `dom0` 上运行以下命令：

```
1 xe vm-param-set uuid=vm_uuid actions-after-crash=preserve
```

3. 使 VM 崩溃。

- 对于 PV 来宾系统，请在 VM 上运行以下命令：

```
1 echo c | sudo tee /proc/sysrq-trigger
```

4. 在 `dom0` 上执行核心转储命令。例如，运行：

```
1 xl dump-core domid filename
```

控制 **Windows VM** 故障转储行为

对于 Windows VM，`actions-after-crash` 参数无法控制核心转储行为。默认情况下，Windows 故障转储放在 Windows VM 自身的 `%SystemRoot%\Minidump` 中。

可以按照以下菜单路径配置 VM 转储级别：我的电脑 > 属性 > 高级 > 启动和故障恢复。

**Linux VM** 上的引导问题故障排除

Citrix Hypervisor 服务器控制域中存在名为 `xe-edit-bootloader` 的实用程序脚本。可以使用此脚本编辑已关闭 Linux VM 的引导加载程序配置，以及解决阻止 VM 启动的问题。

要使用此脚本，请执行以下操作：

1. 运行以下命令：

```
1 xe vm-list
```

此命令可确保涉及的 VM 已关闭 (*power-state* 的值为 *halted*)。

2. 可以按以下方式使用 UUID:

```
1 xe-edit-bootloader -u linux_vm_uuid -p partition_number
```

或者，可以按如下所示使用 *name-label*:

```
1 xe-edit-bootloader -n linux_vm_name_label -p partition_number
```

分区号表示包含文件系统的磁盘分区。对于默认 Debian 模板，分区号为 1，因为它是第一个分区。

3. 此时将打开一个编辑器，其中加载了指定 VM 的 *grub.conf* 文件。更改该文件以对其进行修复，保存该文件并退出编辑器，然后启动 VM。

## 高可用性

September 5, 2019

高可用性功能是一组设计用于为导致 Citrix Hypervisor 服务器出现故障或使其无法访问的问题做出规划以及从这些问题中安全恢复的自动功能。例如，在网络连接发​​生物理损坏或出现主机硬件故障时。

### 概述

高可用性功能可确保当主机变得无法访问或不稳定时，关闭该主机上运行的 VM 并在另一台主机上重新启动。关闭并在另一台主机上重新启动 VM 可避免在新主机上（手动或自动）启动 VM。在稍后的某个时间，将恢复原始主机。这种情况可能会导致同一 VM 的两个实例在不同的主机上运行，并且 VM 磁盘损坏和数据丢失的可能性相对较高。

在池主服务器变得无法访问或不稳定时，高可用性功能还可以恢复池的管理控制能力。高可用功能呢可确保自动恢复管理控制能力，不需要任何手动干预。

(可选) 高可用性功能还可以实现在已知处于良好状态的主机上自动重新启动 VM，而无需手动干预的过程。可以安排这些 VM 成组重新启动，以留出启动服务的时间。它允许在其从属 VM 之前启动基础结构 VM（例如，在其从属 SQL Server 之前启动的 DHCP 服务器）。

#### 警告:

请将高可用性功能与多路径存储和绑定的网络连接结合使用。请先配置多路径存储和绑定的网络连接，然后再尝试设置高可用性功能。当基础结构不稳定时，未设置多路径存储和绑定的网络连接的客户端可能会看到意外的主机重新启动行为（自主防护）。

可以在利用高可用性功能的环境中使用所有图形解决方案（Nvidia vGPU、Intel GVT-d、Intel GVT-G、AMD

MxGPU 和 vGPU 直通)。但是，不能通过高可用性功能保护使用这些图形解决方案的 VM。存在具有恰当的可用资源的主机时，可以在最大努力的基础上重新启动这些 VM。

### 使用过量

在其他位置发生用户定义次数的主机故障后，如果无法重新启动当前正在运行的 VM，则池会被过度使用。

如果在发生故障后池中没有任何足够的可用内存来运行这些 VM，则可能会发生过度使用的情况。但是，还存在一些可能会导致高可用性功能保证无法持续使用的更细微变化：对虚拟块设备 (VBD) 和网络所做的更改会影响哪些 VM 可以在哪些主机上重新启动。Citrix Hypervisor 无法检查所有潜在的操作并确定它们是否会导致违背高可用性功能需求。但是，如果高可用性功能变得无法持续使用，系统将发送异步通知。

Citrix Hypervisor 会动态维护故障转移方案，该方案详细说明了如果池中的一组主机在任意给定时间发生故障时应执行的操作。您需要了解的一个重要概念是允许的主机故障数值，该值被定义为高可用性功能配置的一部分。允许的主机故障数值确定在不中断任何服务的情况下所允许的故障数。例如，对于包含 64 个主机的资源池，允许的故障数将设置为 3。在这种情况下，池将计算允许任何三个主机发生故障的故障转移方案并在另一个主机上重新启动 VM。如果找不到方案，该池将被视为过度使用。方案根据 VM 生命周期操作和移动动态地进行重新计算。如果所做的更改（例如，将新 VM 添加到池中）导致池被过度使用，则会发送警报（通过 XenCenter 或电子邮件）。

### 过度使用警告

如果对启动或恢复 VM 的任何尝试会导致池被过度使用，则会显示警告警报。此警告将显示在 XenCenter 中，还可以作为消息实例通过管理 API 提供。如果您已配置某个电子邮件地址，则还可能向该电子邮件地址发送一条消息。然后，可以取消此操作，或继续操作。继续操作会导致池被过度使用。不同优先级的 VM 所使用的内存量将在池和主机级别显示。

### 主机防护

有时，服务器会由于网络连接中断或遇到控制堆栈问题而发生故障。在这些情况下，Citrix Hypervisor 服务器会进行自主防护以确保 VM 不会同时在两个服务器上运行。采取防护措施后，服务器会突然立即重新启动，导致其上运行的所有 VM 都停止。其他服务器会检测到 VM 不再运行，而这些 VM 将根据分配给它们的重新启动优先级进行重新启动。受防护的服务器将进入重新引导序列，并在重新启动后尝试重新加入资源池。

#### 注意：

当群集池中的主机无法与资源池中超过一半以上的其他主机进行通信时，这些主机也会进行自主防护。有关详细信息，请参阅[群集池](#)。

### 配置要求

要使用高可用性功能，您需要：

- Citrix Hypervisor 池。此功能提供单一资源池内服务器级别的高可用性。

注意：

我们建议您仅对至少包含三个 Citrix Hypervisor 服务器的池启用高可用性功能。有关详细信息，请参阅[CTX129721 - XenServer 池中的检测信号丢失时的高可用性行为](#)。

- 共享存储，其中包含至少一个大小为 356 MB 或更大的 iSCSI、NFS 或光纤通道 LUN - 检测信号 SR。高可用性功能机制将在检测信号 SR 中创建两个卷：

4 MB 检测信号卷：用于检测信号。

256 MB 元数据卷：用于存储进行主服务器故障转移时要使用的池主服务器元数据。

注意：

- 为了最大程度地提高可靠性，我们建议您使用专用的 NFS 或 iSCSI 存储库作为高可用性功能检测信号磁盘。请勿将此存储库用于任何其他用途。
- 如果池是群集池，则检测信号 SR 必须是 GFS2 SR。
- 通过 CHAP 进行身份验证时使用 SMB 或 iSCSI 附加的存储不能用作检测信号 SR。
- 使用 NetApp 或 EqualLogic SR 时，请在阵列上手动预配 NFS 或 iSCSI LUN 以用作检测信号 SR。

- 所有主机的静态 IP 地址。

警告：

如果服务器的 IP 地址在启用了高可用性功能时发生更改，则高可用性功能假定主机的网络发生故障。IP 地址发生更改会导致主机受防护并使其处于无法启动的状态。要对此情况进行补救，请使用 `host-emergency-ha-disable` 命令禁用高可用性功能，使用 `pool-emergency-reset-master` 重置池主服务器，然后重新启用高可用性功能。

- 为了获得最大可靠性，我们建议您使用专用的绑定接口作为高可用性管理网络。

对于受高可用性功能保护的 VM，该 VM 必须灵活。这意味着，VM：

- 必须在共享存储上具有虚拟磁盘。您可以使用任何类型的共享存储。iSCSI、NFS 或光纤通道 LUN 仅是存储检测信号所需的，并且可以用于虚拟磁盘存储。
- 可以使用实时迁移
- 不能连接到配置的本地 DVD 驱动器
- 在池级别的网络上具有自己的虚拟网络接口

注意：

如果启用了高可用性功能，我们强烈建议您在池中的服务器上使用绑定的管理接口，并为检测信号 SR 使用多路径存储。

如果您从 CLI 创建 VLAN 和绑定的接口，则即使已创建，也可能不插入和激活它们。在这种情况下，VM 可能显得不够灵活，无法受高可用性功能保护。您可以使用 CLI `pif-plug` 命令调用 VLAN 和绑定 PIF，以使 VM 变得灵活。您还可以使用 `xe diagnostic-vm-status` CLI 命令精确定义 VM 不灵活的原因。此命令可分析及其放置约束，并且您可以在需要时采取补救措施。

## 重新启动配置设置

可以将虚拟机视为受高可用性功能保护、最大努力或不受高可用性功能保护。`ha-restart-priority` 的值定义将 VM 视为受保护、最大努力还是不受保护。其中每个类别中的 VM 的重新启动行为各不相同。

### 受保护

高可用性功能可保证重新启动进入脱机状态或者其主机进入脱机状态的受保护 VM，前提是池未被过度使用并且 VM 非常灵活。

如果在服务器出现故障时无法重新启动受保护的 VM，高可用性功能将在池中有额外的容量时尝试启动该 VM。在有额外的容量时尝试启动该 VM 现在可能会成功。

`ha-restart-priority` 值: `restart`

### 最大努力

如果某个最大努力 VM 的主机进入脱机状态，高可用性功能会尝试在另一个主机上重新启动该最大努力 VM。仅当成功重新启动所有受保护的 VM 后才能进行此尝试。高可用性功能只会尝试重新启动最大努力 VM 一次。如果本次尝试失败，高可用性功能将不会进一步尝试重新启动该 VM。

`ha-restart-priority` 值: `best-effort`

### 不受保护

如果不受保护的 VM 或运行它的主机停止运行，高可用性功能将不尝试重新启动该 VM。

`ha-restart-priority` 值: 值为空字符串

#### 注意:

高可用性功能从不停止或迁移正在运行的 VM 以便为要重新启动的受保护 VM 或最大努力 VM 释放资源。

如果池遇到服务器故障并且允许的故障数降为零，将不再保证重新启动受保护的 VM。在这种情况下，将生成系统警报。如果发生其他故障，所有设置了重新启动优先级的 VM 将根据最大努力行为运行。

### 启动顺序

启动顺序是指出现故障时 Citrix Hypervisor 高可用性功能尝试重新启动受保护的 VM 的顺序。启动顺序由每个受保护的 VM 的 `order` 属性的值决定。

VM 的 `order` 属性由高可用性功能使用，还由用于启动和关闭 VM 的其他功能使用。任何 VM 都可以设置 `order` 属性，而不仅仅是标记为受高可用性功能保护的 VM。但是，高可用性功能仅使用受保护的 VM 的 `order` 属性。

`order` 属性的值为整数。默认值为 0，表示最高优先级。高可用性功能首先重新启动 `order` 值为 0 的受保护 VM。`order` 属性的值越大，重新启动 VM 的顺序越靠后。

可以使用命令行接口设置 VM 的 `order` 属性的值：

```
1 xe vm-param-set uuid=VM_UUID order=int
```

或者，在 XenCenter 中，在 VM 的“启动选项”面板中，将“启动顺序”设置为所需的值。

## 对 Citrix Hypervisor 池启用高可用性功能

可以使用 XenCenter 或命令行接口对池启用高可用性功能。无论使用哪种方法，都需要指定一组优先级，用来确定当池被过度使用时赋予哪些 VM 最高重新启动优先级。

### 警告：

- 启用高可用性功能后，某些影响 VM 重新启动方案的操作（例如从池中删除服务器）可能会被禁用。您可以暂时禁用高可用性功能以执行此类操作，或者将受高可用性功能保护的 VM 设为不受保护。
- 如果启用了高可用性功能，则无法对池启用群集。暂时禁用高可用性功能以启用群集。您可以对群集池启用高可用性功能。对于群集池，某些高可用性功能的行为（例如自主防护）有所不同。有关详细信息，请参阅[群集池](#)。

## 使用 CLI 启用高可用性功能

1. 确认已将兼容的存储库 (SR) 连接到池。iSCSI、NFS 或光纤通道 SR 都是兼容的 SR。有关如何使用 CLI 配置此类存储库的信息，请参阅[管理存储库](#)。
2. 对每台要保护的 VM 设置重新启动优先级和启动顺序。可以按如下所示设置重新启动优先级：

```
1 xe vm-param-set uuid=vm_uuid ha-restart-priority=restart order=1
```

3. 对池启用高可用性功能，并（可选）指定超时：

```
1 xe pool-ha-enable heartbeat-sr-uuids=sr_uuid ha-config:timeout=
  timeout in seconds
```

超时是指网络连接或存储不能被池中的主机访问的期限。如果在启用高可用性功能时未指定超时，Citrix Hypervisor 将使用默认 30 秒超时。如果任何 Citrix Hypervisor 服务器在超时期限内都无法访问网络连接或存储，则将进行自主防护并重新启动。

4. 运行命令 `pool-ha-compute-max-host-failures-to-tolerate`。此命令返回允许的故障主机最大数目，超过此数目，资源将不足以运行池中所有受保护的 VM。

```
1 xe pool-ha-compute-max-host-failures-to-tolerate
```

允许的故障数决定何时发送警报。系统将在池的状态发生更改时重新计算故障转移方案。使用此计算可以确定池容量，以及在不失去对受保护 VM 的有效保证情况下还可以发生的故障数。当计算的值低于为 `ha-host-failures-to-tolerate` 指定的值时，将生成系统警报。

5. 为允许故障数参数指定一个数目。该值必须小于或等于计算的值：

```
1 xe pool-param-set ha-host-failures-to-tolerate=2 uuid=pool-uuid
```

使用 **CLI** 从 **VM** 中删除高可用性功能保护

要对 VM 禁用高可用性功能，请使用 `xe vm-param-set` 命令将 `ha-restart-priority` 参数设置为空字符串。设置 `ha-restart-priority` 参数不会清除启动顺序设置。可以根据情况将 `ha-restart-priority` 参数设置为 `restart` 或 `best-effort`，以再次对 VM 启用高可用性功能。

恢复无法访问的主机

如果由于某些原因，主机无法访问高可用性功能的状态文件，则主机可能变为无法访问。要恢复 Citrix Hypervisor 安装，可能需要使用 `host-emergency-ha-disable` 命令禁用高可用性功能：

```
1 xe host-emergency-ha-disable --force
```

如果主机是池主服务器，它会在禁用高可用性功能的情况下照常启动。池成员将重新连接并自动禁用高可用性功能。如果主机是池成员，并且无法连接主服务器，则可能需要执行以下操作之一：

- 强制主机以池主服务器身份重新启动 (`xe pool-emergency-transition-to-master`)

```
1 xe pool-emergency-transition-to-master uuid=host_uuid
```

- 告知主机新的主服务器的位置 (`xe pool-emergency-reset-master`):

```
1 xe pool-emergency-reset-master master-address=new_master_hostname
```

成功重新启动所有主机后，重新启用高可用性功能：

```
1 xe pool-ha-enable heartbeat-sr-uuid=sr_uuid
```

在启用高可用性功能的情况下关闭主机

关闭或重新启动主机时应特别注意，以防止高可用性功能机制假定主机已发生故障。要在启用高可用性功能的情况下彻底关闭主机，请通过使用 XenCenter 或 CLI `disable` 主机、`evacuate` 主机，最后 `shutdown` 主机。要在启用了高可用性功能的环境中关闭主机，请运行以下命令：

```
1    xe host-disable host=host_name
2    xe host-evacuate uuid=host_uuid
3    xe host-shutdown host=host_name
```

### 关闭受高可用性功能保护的 VM

如果 VM 受高可用性功能方案保护并设置为自动重新启动，则无法在此保护处于活动状态时关闭该 VM。要关闭 VM，请首先禁用其高可用性功能保护，然后执行 CLI 命令。选择受保护 VM 的关闭按钮时，XenCenter 将显示一个用于自动禁用该保护的对话框。

#### 注意：

如果关闭来宾系统内的某个 VM，并且该 VM 受到保护，则它将在高可用性功能发生故障的情况下自动重新启动。自动重新启动有助于确保操作员错误不会导致受保护的 VM 意外关闭。如果要关闭此 VM，应首先禁用其高可用性功能保护。

## 灾难恢复和备份

June 4, 2019

Citrix Hypervisor 灾难恢复 (DR) 功能允许您从破坏整个池或站点的硬件故障中恢复虚拟机 (VM) 和 vApp。有关如何防止出现单服务器故障的信息，请参阅[高可用性](#)。

#### 注意：

要使用 DR 功能，您必须以 *root* 帐户身份登录，或具有池操作员或更高级别的角色。

### 了解 Citrix Hypervisor DR

Citrix Hypervisor DR 的工作原理是：将恢复业务关键型 VM 和 vApp 所需的全部信息存储在存储库 (SR) 中。然后将 SR 从主（生产）环境复制到备份环境。当主站点上受到保护的池出现故障时，可以从在辅助 (DR) 站点上重新创建的已复制存储恢复该池中的 VM 和 vApp，从而最大限度地减少对应用程序或用户造成的停机时间。

XenCenter 中的灾难恢复设置可以用于查询该存储并在灾难期间将选定的 VM 和 vApp 导入恢复池。当这些 VM 在恢复池中运行时，恢复池的元数据也会被复制。复制池元数据可以在主池恢复时将 VM 设置进行的任何更改填充回主池。有时，同一个 VM 的信息可能位于多个位置。例如，位于主站点中的存储、位于灾难恢复站点中的存储，以及要将数据导入至的池中。如果 XenCenter 发现 VM 的信息位于两个或两个以上的位置，它可以确保其仅使用最新的信息。

可通过 XenCenter 和 xe CLI 使用灾难恢复功能。有关 CLI 命令的信息，请参阅[灾难恢复命令](#)。

### 提示：

还可以使用灾难恢复设置运行测试故障转移，以便对灾难恢复系统进行非中断性测试。在测试故障转移中，所有步骤都与故障转移过程相同。但是，VM 和 vApp 在恢复到灾难恢复站点后不会启动。测试完成后，将执行清理以删除在 DR 站点上重新创建的所有 VM、vApp 和存储。

Citrix Hypervisor VM 包含两个组件：

- 由 VM 使用的虚拟磁盘，存储在 VM 所在池中配置的存储库 (SR) 中。
- 描述 VM 环境的元数据。如果原始 VM 不可用或损坏，则需要此信息以重新创建 VM。大多数元数据配置数据会在创建 VM 时写入，而且仅在对 VM 配置进行了更改时才会更新。对于池中的 VM，此元数据的副本存储在池中的每个服务器上。

在 DR 环境中，将使用池元数据和有关池中所有 VM 和 vApp 的配置信息在辅助站点上重新创建 VM。每个 VM 的元数据都包含其名称、说明、通用唯一标识符 (UUID)、内存、虚拟 CPU、网络连接配置和存储配置。还包括 VM 启动选项 - 启动顺序、延迟间隔、高可用性和重新启动优先级。在高可用性或 DR 环境中重新启动 VM 时，将使用 VM 启动选项。例如，在灾难恢复期间恢复 VM 时，vApp 中的 VM 将按照 VM 元数据中指定的顺序，以指定的延迟间隔在 DR 池中重新启动。

### DR 基础结构要求

要使用 Citrix Hypervisor DR，需要在主站点和辅助站点均设置适当的 DR 基础结构。

- 用于池元数据和 VM 所用虚拟磁盘的存储都必须从主（生产）环境复制到备份环境。例如，使用镜像的存储复制因设备而异。因此，请咨询存储解决方案供应商以了解如何处理存储复制。
- 在恢复到 DR 站点上的池中的 VM 和 vApp 启动并运行后，必须复制包含 DR 池元数据和虚拟磁盘的 SR。该复制允许在主站点重新联机时将恢复后的 VM 和 vApp 复制回主站点（故障恢复）。
- DR 站点的硬件基础结构无需与主站点的硬件基础结构保持一致。但是，Citrix Hypervisor 环境的版本和修补级别必须相同。此外，还必须在目标池中配置足够的资源，才能重新创建和启动所有故障转移的 VM。

### 警告：

灾难恢复设置不会控制任何存储阵列功能。

使用灾难恢复功能的用户必须确保以某种方式在两个站点之间复制元数据存储。某些存储阵列包含可自动执行复制的“镜像”功能。如果您使用这些功能，则必须先禁用镜像功能（“镜像已损坏”），然后再重新启动恢复站点上的 VM。

### 部署注意事项

请在启用灾难恢复之前查看以下步骤。

## 灾难发生之前执行的步骤

下一节将介绍在灾难发生之前执行的步骤。

- 配置 VM 和 vApp。
- 记下将 VM 和 vApp 映射到 SR 的方式，以及将 SR 映射到 LUN 的方式。命名 `name_label` 和 `name_description` 参数时要特别小心谨慎。如果 SR 的名称体现了将 VM 和 vApp 映射到 SR 的方式，以及将 SR 映射到 LUN 的方式，则从复制的存储恢复 VM 和 vApp 将更简单。
- 安排 LUN 的复制。
- 允许将池元数据复制到这些 LUN 上的一个或多个 SR。
- 确保要将主池的元数据复制到的 SR 仅连接到一个池。

## 灾难发生之后执行的步骤

下一节将介绍在灾难发生之后执行的步骤。

- 中断任何现有的存储镜像，使恢复站点可以对共享存储进行读/写访问。
- 确保要用来恢复 VM 数据的 LUN 未连接到任何其他池，否则数据可能会被破坏。
- 如果要防止恢复站点发生灾难，则必须允许将池元数据复制到恢复站点的上一个或多个 SR。

## 恢复之后执行的步骤

下一节将介绍在成功恢复数据之后执行的步骤。

- 重新同步任何存储镜像。
- 在恢复站点上，彻底关闭要移回到主站点的 VM 或 vApp。
- 在主站点上，按照与上一节中所述故障转移过程相同的过程，将选定的 VM 或 vApp 故障恢复到主站点。
- 要防止主站点在将来发生灾难，必须重新允许将池元数据复制到所复制的 LUN 上的一个或多个 SR。

## 启用灾难恢复

June 4, 2019

本节介绍如何在 XenCenter 中启用灾难恢复。使用配置 **DR** 对话框可以标识用来存储池元数据（有关池中所有 VM 和 vApp 的配置信息）的存储库。每当对池中的 VM 或 vApp 配置进行更改时，池元数据都将进行更新。

**注意：**

只有当使用基于 HBA 的 LVM 或基于 iSCSI 的 LVM 时，才能启用灾难恢复。在此存储上需要少量空间来创建新 LUN，用以包含池恢复信息。

在开始之前，请确保已用于 DR 的 SR 仅连接到主站点上的池。已用于 DR 的 SR 不得连接到辅助站点上的池。

要配置灾难恢复，请完成以下步骤：

1. 在主站点上，选择要保护的池。从池菜单中，指向灾难恢复，然后选择配置。
2. 最多选择 8 个用来存储池元数据的 SR。在此存储上需要少量空间来创建新 LUN，用以包含池恢复信息。

**注意：**

将存储池中所有 VM 的信息，而不需要单独选择各个 VM 进行保护。

3. 选择 **OK** (确定)。池现在将受保护。

## 发生灾难时恢复 VM 和 vApp (故障转移)

本节将介绍如何在辅助 (恢复) 站点上恢复 VM 和 vApp。

1. 在 XenCenter 中选择辅助池，在池菜单中，选择灾难恢复，然后选择灾难恢复向导。

“灾难恢复”向导显示以下三个恢复选项：故障转移、故障恢复和测试故障转移。要在辅助站点上恢复，请选择故障转移，然后选择下一步。

**警告：**

如果结合使用光纤通道共享存储和 LUN 镜像将数据复制到辅助站点，请在尝试恢复 VM 之前断开镜像。必须断开镜像以确保辅助站点具有读取/写入访问权限。

2. 选择要恢复的 VM 和 vApp 的池元数据所在的存储库 (SR)。

默认情况下，此向导页面上的列表显示池中当前连接的所有 SR。要扫描查找更多的 SR，请选择查找存储库，然后选择要扫描的存储类型：

- 要扫描所有可用的硬件 HBA SR，请选择查找硬件 **HBA SR**。
- 要扫描软件 iSCSI SR，请选择查找软件 **iSCSI SR**，然后键入目标主机、IQN 和 LUN 详细信息。

在该向导中选择了所需的 SR 之后，选择下一步继续操作。

3. 选择要恢复的 VM 和 vApp。选择相应的恢复后的电源状态选项，以指定是否希望该向导在 VM 和 vApp 已恢复后自动启动它们。或者，您可以在故障转移完成后手动启动它们。

选择下一步前进到下一个向导页面，开始进行故障转移预检查。

4. 在开始故障转移之前，向导将执行多项预检查。例如，确保选定 VM 和 vApp 所需的所有存储均可用。如果此时缺少任何存储，可以选择此页面上的连接 **SR** 以查找并连接相关 SR。

解决预检查页面上的任何问题，然后选择故障转移开始执行恢复过程。

5. 进度页面将显示每个 VM 和 vApp 的恢复过程结果。故障转移过程将从已复制的存储中导出 VM 和 vApp 的元数据。因此，故障转移所用的时间取决于要恢复的 VM 和 vApp。将在主池中重新创建 VM 和 vApp，并且包含虚拟磁盘的 SR 将连接到重新创建的 VM。如果指定，VM 将启动。

6. 当故障转移完成时，选择下一步查看摘要报告。选择摘要报告页面上的完成以关闭向导。

在主站点可用之后，执行“灾难恢复”向导并选择故障恢复以恢复运行该站点上的 VM。

### 在灾难之后将 VM 和 vApp 还原到主站点（故障恢复）

本节介绍如何将从已复制的存储还原 VM 和 vApp。当主站点在灾难之后重新联机时，可以将 VM 和 vApp 还原回主（生产）站点上的池中。要将 VM 和 vApp 故障恢复到主站点，请使用“灾难恢复”向导。

1. 在 XenCenter 中选择主池，在“池”菜单中，选择灾难恢复，然后选择灾难恢复向导。

“灾难恢复”向导显示以下三个恢复选项：故障转移、故障恢复和测试故障转移。要将 VM 和 vApp 还原到主站点，请选择“故障恢复”，然后选择下一步。

#### 警告：

如果结合使用光纤通道共享存储和 LUN 镜像将数据复制到主站点，请在尝试还原 VM 之前断开镜像。必须断开镜像以确保主站点具有读取/写入访问权限。

2. 选择要恢复的 VM 和 vApp 的池元数据所在的存储库 (SR)。

默认情况下，此向导页面上的列表显示池中当前连接的所有 SR。要扫描查找更多的 SR，请选择查找存储库，然后选择要扫描的存储类型：

- 要扫描所有可用的硬件 HBA SR，请选择查找硬件 **HBA SR**。
- 要扫描软件 iSCSI SR，请选择查找软件 **iSCSI SR**，然后键入目标主机、IQN 和 LUN 详细信息。

在该向导中选择了所需的 SR 之后，选择下一步继续操作。

3. 选择要还原的 VM 和 vApp。选择相应的恢复后的电源状态选项，以指定是否希望该向导在 VM 和 vApp 已恢复后自动启动它们。或者，您可以在故障恢复完成后手动启动它们。

选择下一步前进到下一个向导页面，开始进行故障恢复预检查。

4. 在开始故障恢复之前，向导将执行多项预检查。例如，确保选定 VM 和 vApp 所需的所有存储均可用。如果此时缺少任何存储，可以选择此页面上的连接 **SR** 以查找并连接相关 SR。

解决预检查页面上的任何问题，然后选择故障恢复开始执行恢复过程。

5. 进度页面将显示每个 VM 和 vApp 的恢复过程结果。故障恢复过程将从已复制的存储中导出 VM 和 vApp 的元数据。因此，故障恢复过程可能会需要一些时间，具体取决于要还原的 VM 和 vApp 的数量。将在主池中重新创建 VM 和 vApp，并且包含虚拟磁盘的 SR 将连接到重新创建的 VM。如果指定，VM 将启动。

6. 当故障恢复完成时，选择下一步查看摘要报告。选择摘要报告页面上的完成以关闭向导。

## 测试故障转移

故障转移测试是灾难恢复规划中不可或缺的部分。可以使用灾难恢复向导对灾难恢复系统执行非中断性测试。在测试故障转移操作期间，测试步骤与故障转移过程基本相同，只是 VM 和 vApp 在恢复到 DR 站点之后不会启动，而是被置于暂停状态。在测试故障转移操作结束时，在 DR 站点上重新创建的所有 VM、vApp 和存储都将自动删除。在完成初始 DR 配置后，以及在启用 DR 的池中进行重要的配置更改后，请通过执行测试故障转移来验证故障转移是否能正常进行。

1. 在 XenCenter 中选择辅助池，在池菜单上，选择灾难恢复以打开灾难恢复向导。
2. 选择测试故障转移，然后选择下一步。

**注意：**

如果结合使用光纤通道共享存储和 LUN 镜像将数据复制到辅助站点，请在尝试恢复数据之前断开镜像。必须断开镜像以确保辅助站点具有读取/写入访问权限。

3. 选择要恢复的 VM 和 vApp 的池元数据所在的存储库 (SR)。

默认情况下，此向导页面上的列表显示池中当前连接的所有 SR。要扫描查找更多的 SR，请选择查找存储库，然后选择要扫描的存储类型：

- 要扫描所有可用的硬件 HBA SR，请选择查找硬件 **HBA SR**。
- 要扫描软件 iSCSI SR，请选择查找软件 **iSCSI SR**，然后在框中键入目标主机、IQN 和 LUN 详细信息。

在该向导中选择了所需的 SR 之后，选择下一步继续操作。

4. 选择要恢复的 VM 和 vApp，然后选择下一步前进到下一个页面，开始进行故障转移预检查。
5. 在开始测试故障转移之前，向导将执行多项预检查。例如，确保选定 VM 和 vApp 所需的所有存储均可用。

- 检查存储是否可用。如果缺少任何存储，可以选择此页面上的“连接 SR”以查找并连接相关 SR。
- 检查是否未对目标 **DR** 池启用高可用性功能。必须对辅助池禁用高可用性功能，以免在主池和 DR 池上运行相同的 VM。必须禁用高可用性功能以确保在恢复后不会自动启动已恢复的 VM 和 vApp。要对辅助池禁用高可用性功能，只需选择此页面上的禁用高可用性即可。如果此时高可用性功能处于禁用状态，则它会在测试故障转移过程结束时自动重新启用。

解决预检查页面上的任何问题，然后选择故障转移开始执行测试故障转移。

6. 进度页面将显示每个 VM 和 vApp 的恢复过程结果。故障转移过程将从已复制的存储中恢复 VM 和 vApp 的元数据。因此，故障转移过程可能会需要一些时间，具体取决于要恢复的 VM 和 vApp 的数量。将在 DR 池中重新创建所选 VM 和 vApp，包含虚拟磁盘的 SR 将连接到重新创建的 VM。

恢复后的 VM 将被置于暂停状态：在测试故障转移期间，它们将不会在辅助站点上启动。

7. 如果您对成功执行的测试故障转移满意，请在向导中选择“下一步”，使向导在 DR 站点上进行清理：
  - 在测试故障转移期间恢复的 VM 和 vApp 将被删除。
  - 在测试故障转移期间恢复的存储将被分离。

- 如果在预检查阶段为了允许进行测试故障转移而对 DR 池禁用了高可用性功能，则高可用性功能会自动重新启用。

向导将显示清理过程的进度。

8. 选择完成以关闭向导。

## vApp

September 5, 2019

vApp 是一个或多个相关虚拟机 (VM) 的逻辑组。在发生灾难时，vApp 可以作为单个实体来启动。启动 vApp 后，vApp 中包含的 VM 将按照用户预定义的顺序启动。启动顺序允许相互依赖的 VM 自动排序。在整个服务需要重新启动时，管理员不再需要手动为依赖其他 VM 的 VM 指定启动顺序。例如，在软件更新期间，vApp 中的 VM 不必位于同一个主机上，而是按照常规规则在池中分布。在灾难恢复 (DR) 的情况下，vApp 功能很有用。在 DR 情况下，管理员可能会在同一存储库上或与同一服务级别协议 (SLA) 相关的存储库上对所有 VM 进行分组。

要将多个 VM 一起分组到一个 vApp 中，请按照以下过程进行操作：

1. 选择池，然后在池菜单中，单击管理 **vApp**。

2. 键入该 vApp 的名称和说明（可选），然后单击下一步。

可以根据自己的喜好选择任何名称，但通常最好使用信息性名称。尽管我们建议您避免为多个 vApp 使用相同的名称，但并不是必须要这样做，XenCenter 不会针对 vApp 名称的唯一性实施任何约束。对于包含空格的名称，不必使用引号。

3. 选择要包含在新 vApp 中的 VM，然后单击下一步。

可以使用搜索选项仅列出名称中包含指定文本字符串的 VM。

4. 为该 vApp 中的 VM 指定启动顺序，然后单击下一步。

**启动顺序：**指定各个 VM 在 vApp 中的启动顺序，使某些 VM 先于其他 VM 重新启动。启动顺序值为 0（零）的 VM 将首先启动。下一个启动的是启动顺序值为 1 的 VM，然后是值为 2 的 VM，依此类推。

**尝试在以下时间后启动下一个 VM：**延迟时间间隔，用于指定从启动 VM 到尝试启动启动序列中下一组 VM 之间的等待时间。

5. 您可以在最后一页上检查 vApp 配置。单击上一步返回并更改任何设置，或者单击完成以创建 vApp。

注意：

一个 vApp 可以跨单个池中的多个服务器，但是不能跨多个池。

## 在 XenCenter 中管理 vApp

XenCenter 中的管理 **vApp** 可用于创建、删除和更改 vApp。此外，还可用于启动和关闭 vApp，以及导入和导出选定池中的 vApp。在列表中选择某个 vApp 时，其中包含的 VM 会列在详细信息窗格中。有关详细信息，请参阅 XenCenter 帮助。

## 备份和还原主机和 VM

July 10, 2019

请尽可能不更改 Citrix Hypervisor 服务器的安装状态。也就是说，不要在 Citrix Hypervisor 服务器上安装任何其他软件包或启动其他服务，将其视为设备。最好的还原方式是从安装介质重新安装 Citrix Hypervisor 服务器软件。如果您有多个 Citrix Hypervisor 服务器，则最好的方法是配置 TFTP 服务器和相应的应答文件来实现此目的。有关详细信息，请参阅[网络引导安装](#)。

我们建议使用由我们经过认证的合作伙伴之一提供的备份解决方案。有关详细信息，请参阅[Citrix Ready Marketplace](#)。

运行 Citrix Hypervisor 7.3 或更新版本的 Citrix Hypervisor Premium Edition 客户可以利用速度更快、仅限更改块的备份。有关详细信息，请参阅与[更改块跟踪备份 API](#) 有关的 Citrix 博客。

我们建议您尽量经常执行下列备份过程以从可能的服务器和软件故障中恢复。

要备份池元数据，请执行以下操作：

1. 运行命令：

```
1 xe pool-dump-database file-name=backup
```

2. 要还原数据库，请运行以下命令：

```
1 xe pool-restore-database file-name=backup dry-run=true
```

此命令检查目标计算机具有一定数量的适当命名的 NIC，这是成功进行备份的必备条件。

要备份主机配置和软件，请执行以下操作：

1. 运行命令：

```
1 xe host-backup host=host file-name=hostbackup
```

注意：

- 不要在控制域中创建备份。
- 备份过程可以创建大型备份文件。
- 要完成还原，必须重新引导至原始安装 CD。

- 只能将此数据还原到原始计算机。

要备份 **VM**，请执行以下操作：

1. 确保要备份的 VM 处于脱机状态。
2. 运行命令：

```
1 xe vm-export vm=vm_uuid filename=backup
```

注意：

此备份也将备份 VM 的所有数据。导入 VM 时，可以指定要用于已备份数据的存储机制。

警告：

备份过程可能需要更长的时间才能完成，因为它要备份所有 VM 数据。

要仅备份 **VM** 元数据，请执行以下操作：

运行命令：

```
1 xe vm-export vm=vm_uuid filename=backup metadata=true
```

### 备份虚拟机元数据

Citrix Hypervisor 服务器使用各个主机上的数据库存储有关 VM 和相关资源（例如存储和网络）的元数据。当与 SR 结合使用时，此数据库将形成池中所有可用 VM 的完整视图。因此，了解如何备份此数据库以从物理硬件故障和其他灾难情况中恢复，这一点至关重要。

本节首先介绍单主机环境元数据的备份方法，然后介绍更为复杂的池设置。

#### 备份单台主机环境

使用 CLI 备份池数据库。要获得一致的池元数据备份文件，请在 Citrix Hypervisor 服务器上运行 `pool-dump -database` 并将生成的文件存档。此备份文件将包含有关池的敏感身份验证信息，因此请确保安全存储该文件。

要还原池数据库，请对前面的转储文件使用 `xe pool-restore-database` 命令。如果您的 Citrix Hypervisor 服务器完全死机，则必须首先进行全新安装，然后对重新安装的 Citrix Hypervisor 服务器运行 `pool-restore-database` 命令。

还原池数据库后，某些 VM 的注册状态可能仍为 `Suspended`。但是，如果包含挂起的内存状态（在 `suspend-VDI-uuid` 字段中定义）的存储库是本地 SR，则该 SR 可能不可用，因为该主机已重新安装。要将这些 VM 重置回 `Halted` 状态，以便其可以再次启动，请使用 `xe vm-shutdown vm=vm_name -force` 命令或 `xe vm-reset-powerstate vm=vm_name -force` 命令。

### 警告:

Citrix Hypervisor 将保留使用此方法还原的主机的 UUID。如果在原始 Citrix Hypervisor 服务器仍运行时还原到其他物理计算机，则可能存在重复的 UUID。因此，XenCenter 拒绝连接到第二个 Citrix Hypervisor 服务器。池数据库备份不是克隆物理主机的建议机制。请改为使用自动化安装支持。有关详细信息，请参阅[安装](#)。

### 备份池化安装

在池方案中，主服务器主机提供了一个同步镜像到所有池成员主机的授权数据库。此过程可以为池提供内置冗余级别。任何池成员都可以替换主服务器，因为每个池成员都具有正确版本的池数据库。有关如何将成员主机转换为池主服务器的详细信息，请参阅[主机和资源池](#)。

这种保护级别可能远远不够。例如，当包含 VM 数据的共享存储在多个站点中进行了备份，但包含池元数据的本地服务器存储没有备份时。要在给定一组共享存储的情况下重新创建池，必须首先对主服务器主机上的 `pool-dump-database` 文件进行备份，然后将此文件存档。要稍后在一组全新的主机上还原此备份，请执行以下操作：

1. 从安装介质中安装一组全新的 Citrix Hypervisor 服务器，或者从 TFTP 服务器进行网络引导（如果适用）。
2. 在指定为新主服务器的主机上使用 `xe pool-restore-database`。
3. 在新主服务器上运行 `xe host-forget` 命令以删除旧成员计算机。
4. 在成员主机上使用 `xe pool-join` 命令以将这些主机连接到新池。

### 备份 Citrix Hypervisor 服务器

本部分内容介绍 Citrix Hypervisor 服务器控制域的备份和还原步骤。这些步骤不会备份用来容纳 VM 的存储库，而仅备份运行 Xen 和 Citrix Hypervisor 代理的特权控制域。

### 注意:

特权控制域最好保留为已安装状态，而无需使用其他软件包对其进行自定义。我们建议您将网络引导环境设置为从 Citrix Hypervisor 介质干净地安装 Citrix Hypervisor 作为恢复策略。通常情况下，您不需要备份控制域，但我们建议您保存池元数据（请参阅备份虚拟机元数据）。将此备份方法视为备份池元数据的补充方法。

可以采取的另一种方法是使用 `xe` 命令 `host-backup` 和 `host-restore`。`xe host-backup` 命令可将活动分区存档至您指定的文件。`xe host-restore` 命令可在主机的当前非活动磁盘分区中提取由 `xe host-backup` 创建的存档。然后通过引导安装 CD 并选择还原相应备份来激活此分区。

完成上一节中的步骤并重新启动主机后，确保将 VM 元数据还原为一致的状态。在 `/var/backup/pool-database- $\{$ DATE $\}$`  上运行 `xe pool-restore-database` 以还原 VM 元数据。此文件由 `xe host-backup` 使用 `xe pool-dump-database` 命令在存档正在运行的文件系统之前创建，以便对 VM 元数据的一致状态生成快照。

要备份 **Citrix Hypervisor** 服务器，请执行以下操作：

在具有足够磁盘空间的远程主机上，运行以下命令

```
1 xe host-backup file-name=filename -h hostname -u root -pw password
```

此命令创建控制域文件系统的压缩映像。此映像将存储在由 `file-name` 参数指定的位置。

要还原正在运行的 **Citrix Hypervisor** 服务器，请执行以下操作：

1. 如果要从特定备份还原 Citrix Hypervisor 服务器，请在该 Citrix Hypervisor 已启动并可以连接时运行以下命令：

```
1 xe host-restore file-name=filename -h hostname -u root -pw
password
```

此命令会将压缩映像还原到运行此命令的 Citrix Hypervisor 服务器（而不是 `filename` 驻留的主机）的硬盘中。在该上下文中，“还原”有些用词不当，因为该词通常表示已完全恢复备份的状态。还原命令仅对压缩的备份文件进行解压缩并将其还原到正常形式。但是，它会写入其他分区 (`/dev/sda2`)，并且不会覆盖当前版本的文件系统。

2. 要使用已还原版本的根文件系统，请使用 Citrix Hypervisor 安装 CD 重新引导 Citrix Hypervisor 服务器，然后选择 **Restore from backup**（从备份还原）选项。

从备份还原完成后，重新引导 Citrix Hypervisor 服务器，该主机将从还原映像启动。

3. 最后，使用以下命令还原 VM 元数据：

```
1 xe pool-restore-database file-name=/var/backup/pool-database-* -h
hostname -u root -pw password
```

#### 注意：

如此节所述，从备份进行还原不会破坏备份分区。

要重新启动已崩溃的 **Citrix Hypervisor** 服务器，请执行以下操作：

如果您的 Citrix Hypervisor 服务器已崩溃并且无法访问，请使用 Citrix Hypervisor 安装 CD 进行升级安装。升级安装完成后，重新启动此计算机并确保可以使用 XenCenter 或远程 CLI 连接到您的主机。

然后继续按本节中所述备份 Citrix Hypervisor 服务器。

## 备份 VM

我们建议使用由我们经过认证的合作伙伴之一提供的备份解决方案。有关详细信息，请参阅[Citrix Ready Marketplace](#)。

运行 Citrix Hypervisor 7.3 或更新版本的 Citrix Hypervisor Premium Edition 客户可以利用速度更快、仅限更改块的备份。有关详细信息，请参阅与[更改块跟踪备份 API](#) 有关的 Citrix 博客。

## VM 快照

July 10, 2019

Citrix Hypervisor 提供了一种简便的机制。借助该机制，可以在给定的时间生成 VM 存储和元数据的快照。如有必要，在生成快照时会暂时停止 I/O，以确保捕获具有自我一致性的磁盘映像。

快照操作会生成类似于模板的快照 VM。VM 快照包含所有存储信息和 VM 配置（包括已连接的 VIF），可以导出并还原这些信息和配置以进行备份。快照在所有存储类型中都受支持。但是，对于基于 LVM 的存储类型，必须满足以下要求：

- 如果存储库是在早期版本的 Citrix Hypervisor 上创建的，则必须对其进行升级
- 卷必须采用默认格式（无法生成 `type=raw` 卷的快照）

快照操作过程分为 2 个步骤：

- 将元数据捕获为模板。
- 创建磁盘的 VDI 快照。

支持三种类型的 VM 快照：常规快照、静止快照以及包含内存数据的快照

### 常规快照

常规快照处于持续崩溃状态，可以在所有 VM 类型（包括 Linux VM）上执行。

### 静止快照

静止快照利用 Windows 卷快照服务 (VSS)，生成和应用程序一致的实时快照。VSS 框架帮助可识别 VSS 的应用程序（例如 Microsoft SQL Server）在生成快照前将数据刷新到磁盘并为快照做好准备。

因此，还原静止快照比较安全，但当生成静止快照时，这些快照可能会对系统性能产生更大的影响。如果负载不足，它们还可能会失败，因此生成该快照可能需要进行多次尝试。

Citrix Hypervisor 在下列平台上支持静止快照：

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008 (32/64 位)

静止快照不支持 Windows 10、Windows 8.1 和 Windows 7。有关静止快照的详细信息，请参阅静止快照高级说明。

## 包含内存数据的快照

除保存 VM 内存（存储）和元数据外，包含内存数据的快照还保存 VM 状态 (RAM)。此功能在升级或修补软件时可能非常有用，但是您还可以选择还原到更改前的 VM 状态 (RAM)。还原到包含内存数据的快照无需重新启动 VM。

可以通过管理 API、xe CLI 或使用 XenCenter 来生成包含正在运行或已挂起 VM 的内存数据的屏幕快照。

## 创建 VM 快照

生成快照之前，请参阅以下有关特定于任何特殊操作系统的配置和注意事项的信息：

- [准备使用 Sysprep 克隆 Windows VM](#)
- [准备克隆 Linux VM](#)

首先确保 VM 正在运行或已挂起，以便可以捕获内存状态。选择要对其执行操作的 VM 的最简单方法是提供参数 `vm=name` 或 `vm=vm uuid`。

运行 `vm-snapshot` 和 `vm-snapshot-with-quietse` 命令以生成 VM 的快照。

```
1 xe vm-snapshot vm=vm uuid new-name-label=vm_snapshot_name
2 xe vm-snapshot-with-quietse vm=vm uuid new-name-label=vm_snapshot_name
```

## 创建包含内存数据的快照

运行 `vm-checkpoint` 命令，为包含内存数据的快照指定一个描述性名称，以便以后能识别该快照：

```
1 xe vm-checkpoint vm=vm uuid new-name-label=name of the checkpoint
```

Citrix Hypervisor 创建完包含内存数据的快照之后，系统会显示其 UUID。

例如：

```
1 xe vm-checkpoint vm=2d1d9a08-e479-2f0a-69e7-24a0e062dd35 \  
2 new-name-label=example_checkpoint_1  
3 b3c0f369-59a1-dd16-ecd4-a1211df29886
```

包含内存数据的快照需要每个磁盘至少有 4 MB 的磁盘空间，以及加上 RAM 的大小，再加上约 20% 的开销。因此，具有 256 MB RAM 的检查点需要约 300 MB 的存储空间。

注意：

在创建检查点的过程中，VM 会短时暂停，在暂停期间不能使用。

列出 **Citrix Hypervisor** 池的所有快照

运行 `snapshot-list` 命令：

```
1 xe snapshot-list
```

此命令会列出 Citrix Hypervisor 池中的所有快照。

列出特殊 **VM** 的快照

通过运行 `vm-list` 命令获取特定 VM 的 UUID。

```
1 xe vm-list
```

此命令会显示所有 VM 及其 UUID 的列表。例如：

```
1 xe vm-list
2 uuid ( RO): 116dd310-a0ef-a830-37c8-df41521ff72d
3 name-label ( RW): Windows Server 2012 (1)
4 power-state ( RO): halted
5
6 uuid ( RO): 96fde888-2a18-c042-491a-014e22b07839
7 name-label ( RW): Windows 2008 R2 (1)
8 power-state ( RO): running
9
10 uuid ( RO): dff45c56-426a-4450-a094-d3bba0a2ba3f
11 name-label ( RW): Control domain on host
12 power-state ( RO): running
```

也可以通过过滤字段值上的完整 VM 列表，来指定 VM。

例如，指定 `power-state=halted` 将会选择电源状态字段为“halted”的所有 VM。如果有多个匹配的 VM，则必须指定选项 `--multiple` 才能执行该操作。可匹配字段的完整列表可以通过命令 `xe vm-list params=all` 获得。

查找所需的 VM，然后输入以下内容：

```
1 xe snapshot-list snapshot-of=vm uuid
```

例如：

```
1 xe snapshot-list snapshot-of=2d1d9a08-e479-2f0a-69e7-24a0e062dd35
```

此命令会列出当前位于该 VM 上的快照：

```
1    uuid ( RO): d7eefb03-39bc-80f8-8d73-2ca1bab7dcff
2    name-label ( RW): Regular
3    name-description ( RW):
4    snapshot_of ( RO): 2d1d9a08-e479-2f0a-69e7-24a0e062dd35
5    snapshot_time ( RO): 20090914T15:37:00Z
6
7    uuid ( RO): 1760561d-a5d1-5d5e-2be5-d0dd99a3b1ef
8    name-label ( RW): Snapshot with memory
9    name-description ( RW):
10   snapshot_of ( RO): 2d1d9a08-e479-2f0a-69e7-24a0e062dd35
11   snapshot_time ( RO): 20090914T15:39:45Z
```

将 **VM** 还原为其先前的状态

确保知道要还原的快照的 UUID，然后运行 `snapshot-revert` 命令：

1. 运行 `snapshot-list` 命令以查找要还原的快照或检查点的 UUID：

```
1 xe snapshot-list
```

2. 记下快照的 `uuid`，然后运行以下命令进行还原：

```
1 xe snapshot-revert snapshot-uuid=snapshot uuid
```

例如：

```
1 xe snapshot-revert snapshot-uuid=b3c0f369-59a1-dd16-ecd4-
  a1211df29886
```

将 VM 还原为检查点后，VM 将被挂起。

注意：

- 如果没有足够的磁盘空间可用于对快照进行密集预配，则在当前磁盘的状态被释放之前，无法还原到快照。如果发生此问题，请重试此操作。
- 不可能还原到任何快照。还原操作期间不会删除现有快照和检查点。

## 删除快照

确保知道要删除的检查点或快照的 UUID，然后运行以下命令：

1. 运行 `snapshot-list` 命令以查找要还原的快照或检查点的 UUID：

```
1 xe snapshot-list
```

- 记下快照的 UUID，然后运行 `snapshot-uninstall` 命令将其删除：

```
1 xe snapshot-uninstall snapshot-uuid=snapshot-uuid
```

- 此命令会警告您要删除的 VM 和 VDI。键入 `yes` 以进行确认。

例如：

```
1 xe snapshot-uninstall snapshot-uuid=1760561d-a5d1-5d5e-2be5-
  d0dd99a3b1ef
2 The following items are about to be destroyed
3 VM : 1760561d-a5d1-5d5e-2be5-d0dd99a3b1ef (Snapshot with memory)
4 VDI: 11a4aa81-3c6b-4f7d-805a-b6ea02947582 (0)
5 VDI: 43c33fe7-a768-4612-bf8c-c385e2c657ed (1)
6 VDI: 4c33c84a-a874-42db-85b5-5e29174fa9b2 (Suspend image)
7 Type 'yes' to continue
8 yes
9 All objects destroyed
```

如果您只希望删除检查点或快照的元数据，请运行以下命令：

```
1 xe snapshot-destroy snapshot-uuid=snapshot-uuid
```

例如：

```
1 xe snapshot-destroy snapshot-uuid=d7eefb03-39bc-80f8-8d73-2ca1bab7dcff
```

## 快照模板

从快照创建模板

可以从快照创建 VM 模板。但是，其内存状态将被删除。

- 使用命令 `snapshot-copy` 指定该模板的 **new-name-label**：

```
1 xe snapshot-copy new-name-label=vm-template-name \  
2 snapshot-uuid=uuid of the snapshot
```

例如：

```
1 xe snapshot-copy new-name-label=example_template_1  
2 snapshot-uuid=b3c0f369-59a1-dd16-ecd4-a1211df29886
```

**注意：**

此命令会在 SAME 池中创建一个模板对象。此模板仅存在于当前池的 Citrix Hypervisor 数据库中。

2. 要验证该模板是否已创建，请运行命令 `template-list`：

```
1 xe template-list
```

此命令会列出 Citrix Hypervisor 服务器上的所有模板。

### 将快照导出到模板

导出 VM 快照时，VM 的完整副本（包括磁盘映像）会作为单独的文件存储到本地计算机上。此文件包含 `.xva` 文件扩展名。

1. 使用命令 `snapshot-export-to-template` 创建模板文件：

```
1 xe snapshot-export-to template snapshot-uuid=snapshot-uuid \  
2     filename=template- filename
```

例如：

```
1 xe snapshot-export-to-template snapshot-uuid=b3c0f369-59a1-dd16-  
    ecd4-a1211df29886 \  
2     filename=example_template_export
```

可以通过多种不同的方式使用 VM 导出/导入功能：

- 作为一种便捷的 VM 备份工具。在发生灾难情况时，可以使用导出的 VM 文件恢复整个 VM。
- 作为一种快速复制 VM 的方式，例如，多次使用的特殊用途服务器配置。您只需以希望的方式配置 VM，将其导出，然后再将其导入，即可创建原始 VM 的副本。
- 作为一种将 VM 移到其他服务器的简单方法。

有关使用模板的详细信息，请参阅[创建 VM](#) 以及 XenCenter 帮助中的“管理 VM”部分。

### 静止快照高级说明

**注意：**

不要忘记在 Windows 来宾系统中安装 Xen VSS 提供程序，以便支持 VSS。此安装可以使用 Citrix VM Tools 随附的 `install-XenProvider.cmd` 脚本来完成。有关详细信息，请参阅[Windows VM](#)。

一般来说，使用 VSS 接口，VM 只能访问自身的 VDI 快照（而非 VDI 克隆）。Citrix Hypervisor 管理员可以将 `snapmanager=true` 的属性添加到 VM `other-config`，以允许该 VM 从其他 VM 导入 VDI 的快照。

**警告:**

此配置存在一个安全漏洞。请谨慎使用。通过此配置，管理员可以使用 VSS 层生成的来宾系统可传送快照 ID，将 VSS 快照连接到其他 VM 以进行备份。

**VSS 静止超时:** 将 Microsoft VSS 静止时段设置为 10 秒钟的非可配置值。快照很有可能无法按时完成。例如，如果 XAPI 守护程序在队列中又添加了其他块任务（例如 SR 扫描），则 VSS 快照可能会超时并失败。如果发生此超时情况，请重试该操作。

**注意:**

连接到 VM 的 VBD 越多，达到此超时的可能性越大。我们建议最多将 2 个 VBD 连接到 VM，以避免超时。但是，有一个解决方法可以解决此问题。如果 VM 的所有 VDI 位于不同的 SR 上，使用 2 个以上的 VBD 成功生成基于 VSS 的 VM 快照的可能性就会增加。

**所有磁盘均连接到 VM 的 VSS 快照:** 用于存储在生成 VSS 快照时可用的所有数据。XAPI 管理器可生成与使用 Citrix Hypervisor 存储管理器 API 生成快照的 VM 相关联的所有磁盘和 VM 元数据的快照。如果 VSS 层请求仅生成一小部分磁盘的快照，则不会生成所有 VM 的快照。

**vm-snapshot-with-quiet:** 生成可引导的快照 VM 映像：Citrix Hypervisor VSS 硬件提供程序将制作可写入的快照卷，其中包括引导卷的快照。

卷的 VSS 快照托管在 Windows 来宾系统的动态磁盘中：**vm-snapshot-with-quiet** CLI 和 Citrix Hypervisor VSS 硬件提供程序不支持 Windows VM 上的动态磁盘中托管的卷的快照。

**注意:**

不要忘记在 Windows 来宾系统中安装 Xen VSS 提供程序，以便支持 VSS。此安装可以使用 Citrix VM Tools 随附的 `install-XenProvider.cmd` 脚本来完成。有关详细信息，请参阅[Windows VM](#)。

## 计划快照

计划快照功能为关键服务 VM 提供了一个简单的备份和还原实用程序。系统将自动生成定期计划快照，并用来还原相应的 VM。快照计划功能的工作原理是为池中选定的 VM 创建池范围内的快照计划。启用快照计划后，将在每小时、每天或每周的预定时间生成指定 VM 的快照。在一个池中可以启用多个计划快照，这些快照可以涵盖不同的 VM 并且包含不同的计划。一次只能将一个 VM 分配至一个快照计划。

XenCenter 提供了一系列工具来帮助您使用此功能：

- 要定义计划快照，请使用新建快照计划向导。
- 要启用、禁用、编辑和删除池的计划快照，请使用 **VM** 快照计划对话框。
- 要编辑快照计划，请从 **VM** 快照计划对话框中打开其属性对话框。
- 要将 VM 还原到计划快照，请在快照选项卡上选择快照，然后将 VM 还原到该快照。

有关计划快照的详细信息，请参阅 *XenCenter* 帮助。

## 处理计算机故障

September 5, 2019

本节详细介绍如何从各种故障方案中恢复。所有故障恢复方案都需要使用[备份](#)中列出的一个或多个备份类型。

### 成员故障

如果缺少高可用性功能，主节点将通过接收常规检测信号消息检测成员的故障。如果在 600 秒内还没有接收到检测信号，主服务器就会认为该成员已停止活动。可通过下列两种方式从此问题中恢复：

- 修复停止活动的主机（例如，以物理方式重新启动主机）。还原与该成员的连接后，主服务器会再次将该成员标记为活动成员。
- 关闭主机并使用 `xe host-forget` CLI 命令指示主服务器忽略该成员节点。忘记该成员后，会将该成员上运行的所有 VM 标记为脱机，然后在其他 Citrix Hypervisor 服务器上将其重新启动。请注意，确保 Citrix Hypervisor 服务器确实脱机非常重要，否则可能会损坏 VM 数据。请注意，不要使用 `xe host-forget` 将您的池拆分为单一主机的多个池，因为这可能会导致这些池全都映射相同的共享存储并损坏 VM 数据。

#### 警告：

- 如果您准备将已忽略的主机再次用作活动主机，请全新安装 Citrix Hypervisor 软件。
- 如果此池中启用了高可用性功能，请不要使用 `xe host-forget` 命令。首先请禁用高可用性功能，然后忽略主机，接着重新启用高可用性功能。

成员 Citrix Hypervisor 服务器出现故障后，某些 VM 可能仍然以正在运行状态进行注册。如果您确定成员 Citrix Hypervisor 服务器确实已关闭，请使用 `xe vm-reset-powerstate` CLI 命令将 VM 的电源状态设置为 `halted`。有关详细信息，请参阅 [vm-reset-powerstate](#)。

#### 警告：

如果此命令使用不当，则会导致数据损坏。请仅在必要时使用此命令。

在另一个 Citrix Hypervisor 服务器上启动 VM 之前，还需要释放 VM 存储的锁定。SR 中的每个磁盘一次只能由一个主机使用，因此，在一个主机出现故障后，必须使磁盘可供其他 Citrix Hypervisor 服务器访问。为此，请在池主服务器上针对任何受影响 VM 的磁盘所在的每个 SR 运行以下脚本：`/opt/xensource/sm/resetvdis.py host_UUID SR_UUID master`

崩溃时，如果出现故障的主机是 SR 主服务器 - 池主服务器或使用本地存储的 Citrix Hypervisor 服务器，您只需提供第三个字符串（“master”）。

#### 警告：

在执行此命令之前，请务必确保主机已关闭。如果此命令使用不当，则会导致数据损坏。

如果在运行上述脚本之前，尝试在另一个 Citrix Hypervisor 服务器上启动 VM，则将收到下面的错误消息：`VDI < UUID> already attached RW`。

## 主服务器故障

如果需要，资源池的每个成员都将包含担任主服务器角色所需的所有信息。如果主节点发生故障，将依次发生下列事件：

1. 如果禁用高可用性功能，则会自动选出另一个主服务器。
2. 如果未启用高可用性功能，则每个成员都将等待主服务器恢复。

此时如果主服务器恢复，它会与其成员重新建立通信，操作恢复正常。

如果主服务器已停用，请选择一个成员并在其上运行 `xe pool-emergency-transition-to-master` 命令。当该成员成为主服务器后，运行命令 `xe pool-recover-slaves`，这些成员此时将指向新的主服务器。

如果修复或替换用作原始主服务器的服务器，您只需启动服务器，安装 Citrix Hypervisor 服务器软件，然后将其添加到池中。由于池中的 Citrix Hypervisor 服务器强制为同类主机，因此实际上不需要将替换的服务器设为主服务器。

将成员 Citrix Hypervisor 服务器转换为主服务器后，您还应检查默认池存储库是否设置了适当的值。通过使用 `xe pool-param-list` 命令并验证 `default-SR` 参数是否指向有效的存储库，可实现此操作。

## 池故障

如果您的整个资源池不幸发生故障，就需要从头开始重新创建池数据库。请务必使用 `xe pool-dump-database CLI` 命令定期备份池元数据（请参阅 [pool-dump-database](#)）。

要还原彻底出故障的池，请执行以下操作：

1. 安装一组全新的主机。请不要在此阶段将这些主机组成池。
2. 对于任命为主服务器的主机，请使用 `xe pool-restore-database` 命令从备份中还原池数据库（请参阅 [pool-restore-database](#)）。
3. 使用 XenCenter 连接到主服务器主机并确保所有共享存储和 VM 都再次可用。
4. 在已全新安装的其余成员主机上执行池加入操作，并在相应主机上启动 VM。

## 处理因配置错误导致的故障

如果物理主机可以运行但软件或主机配置被损坏，可按以下方式处理：

1. 运行以下命令可还原主机软件和配置：

```
1 xe host-restore host=host file-name=hostbackup
```

2. 重新启动到主机安装 CD 并选择 **Restore from backup**（从备份还原）。

## 物理计算机故障

如果物理主机发生故障，请使用下面列出的相应过程进行恢复。

### 警告：

所有曾在发生了故障的先前成员（或先前主机）上运行的 VM，在数据库中仍将被标记为 **Running**。这是出于安全考虑，因为在两个不同的主机上同时启动 VM 会导致磁盘严重损坏。如果确定计算机（和 VM）处于脱机状态，可以将 VM 电源状态重置为 **Halted**：

```
xe vm-reset-powerstate vm=vm_uuid --force
```

以后可以使用 XenCenter 或 CLI 重新启动 VM。

要用仍处于运行状态的成员替换发生故障的主服务器，请执行以下操作：

1. 运行以下命令：

```
1 xe pool-emergency-transition-to-master
2 xe pool-recover-slaves
```

2. 如果命令成功，请重新启动 VM。

要还原所有主机都发生故障的池，请执行以下操作：

1. 运行命令：

```
1 xe pool-restore-database file-name=backup
```

### 警告：

只有当目标计算机具有合适数量的正确命名的 NIC 时，此命令才能成功。

2. 如果目标计算机具有与原始计算机不同的存储视图（例如，具有不同 IP 地址的块镜像），请依次使用 **pbddestroy** 命令和 **pbd-create** 命令修改存储配置以重新创建存储配置。有关这些命令的文档，请参阅 **pbd** 命令。
3. 如果您已创建新的存储配置，请使用 **pbd-plug** 或“存储”>“修复存储库”菜单项（在 XenCenter 中）以应用新配置。
4. 重新启动所有 VM。

要在 **VM** 存储不可用时还原 **VM**，请执行以下操作：

1. 运行以下命令：

```
1 xe vm-import filename=backup metadata=true
```

2. 如果元数据导入失败，请运行以下命令：

```
1 xe vm-import filename=backup metadata=true --force
```

此命令将“尽最大努力”尝试还原 VM 元数据。

3. 重新启动所有 VM。

## 故障排除

September 5, 2019

### 支持

Citrix 提供两种形式的支持服务：[Citrix 支持 Web](#) 站点上的免费自助支持以及付费的支持服务（可以从支持站点购买）。通过 Citrix 技术支持，您可以在遇到技术问题时，打开在线支持案例或者通过电话与支持中心联系。

[Citrix 知识中心](#) 包含多种资源，可在出现异常行为、崩溃或其他问题时为您提供帮助。资源包括：论坛、知识库文章、白皮书、产品文档、修补程序和其他更新。

如果您遇到有关 Citrix Hypervisor 服务器的技术难题，本部分可帮助您解决问题（如有可能）。如果无法解决问题，请使用本部分中的信息收集可帮助您的解决方案提供商跟踪和解决问题所需的应用程序日志和其他数据。

有关对 Citrix Hypervisor 安装问题进行故障排除的信息，请参阅[对安装问题进行故障排除](#)。有关对虚拟机问题进行故障排除的信息，请参阅[对 VM 问题进行故障排除](#)。

#### 重要：

我们建议您仅在解决方案提供商或技术支持团队的指导下按照本部分中的故障排除信息进行操作。

在某些支持案例中，出于调试目的，需要串行控制台访问。因此，设置 Citrix Hypervisor 配置时，建议您配置串行控制台访问。对于不具备物理串行端口的主机（例如刀片式服务器）或者无适当物理基础结构可用的情况，客户应当研究能否配置嵌入式管理设备，例如 Dell DRAC 或 HP iLO。

有关设置串行控制台访问的信息，请参阅 [CTX121442](#)。

### 运行状况检查

使用运行状况检查功能可生成服务器状态报告并将其上载至 Citrix Insight Services (CIS) 以及在 XenCenter 中接收 CIS 分析报告。

将任何符合条件的池连接到 XenCenter 时，系统都会提示您为池启用运行状况检查功能。在注册过程中，可以执行以下操作：

- 指定要用于自动将服务器状态报告上载至 CIS 的计划
- 输入用于建立与池的连接 Citrix Hypervisor 凭据
- 对与 CIS 的上载进行身份验证

成功注册池以进行运行状况检查后，您将在 XenCenter 中收到与池的运行状况有关的通知。您可以使用此功能根据 CIS 生成的报告，主动监视 Citrix Hypervisor 系统的运行状况。

### 要求

要使用运行状况检查功能，请执行以下操作：

- 池中的所有主机都必须运行 Citrix Hypervisor 8.0
- 使用随 Citrix Hypervisor 8.0 提供的 XenCenter 连接到 Citrix Hypervisor 池
- XenCenter 必须能够访问 Internet
- 运行状况检查服务必须在 XenCenter 计算机上安装并运行。
- 如果使用 Active Directory (AD)，您必须具有池操作员或更高级别的角色

有关运行状况检查的详细信息以及注册池以进行运行状况检查的分步说明，请参阅 XenCenter 帮助。

## Citrix Hypervisor 服务器日志

XenCenter 可用于收集 Citrix Hypervisor 服务器信息。

单击工具菜单中的服务器状态报告，以打开服务器状态报告任务。可以从不同类型的信息（各种日志、故障转储等）列表中进行选择。这些信息将编译并下载到正在运行 XenCenter 的计算机上。有关详细信息，请参阅 XenCenter 帮助。

此外，Citrix Hypervisor 服务器包括多个 CLI 命令，通过这些命令，可以使用 `xen-bugtool` 实用程序整理日志输出以及各种其他系统信息。使用 `xe` 命令 `host-bugreport-upload` 可以收集适当的日志文件和系统信息并将其上传到技术支持 FTP 站点。有关此命令及其可选参数的完整说明，请参阅 [\[host-bugreport-upload\]\(/zh-cn/citrix-hypervisor/command-line-interface.html#host-bugreport-upload\)](#)。如果系统要求您将故障转储发送给技术支持团队，请使用 `xe` 命令 `host-crashdump-upload`。有关此命令及其可选参数的完整说明，请参阅 [\[host-crashdump-upload\]\(/zh-cn/citrix-hypervisor/command-line-interface.html#host-crashdump-upload\)](#)。

#### 重要：

Citrix Hypervisor 服务器日志可能包含敏感信息。

### 将主机日志消息发送到中央服务器

可以将 Citrix Hypervisor 服务器配置为将日志写入远程服务器，而不是写入控制域文件系统。远程服务器必须运行 `syslogd` 守护程序，才能接收日志并将它们正确地聚合。`syslogd` 守护程序是 Linux 和 Unix 的所有版本的标准部件，Windows 和其他操作系统可以使用第三方版本。

将 `syslog_destination` 参数设置为要在其中写入日志的远程服务器的主机名或 IP 地址：

```
1 xe host-param-set uuid=BRAND_SERVER_host_uuid logging:
   syslog_destination=hostname
```

运行命令：

```
1 xe host-syslog-reconfigure uuid= BRAND_SERVER_host_uuid
```

强制执行该更改。（也可以通过指定 `host` 参数远程执行此命令。）

## XenCenter 日志

XenCenter 还提供客户端日志。此文件包括使用 XenCenter 时执行的所有操作以及出现的所有错误的完整描述，还包含事件的信息记录，以便为您提供发生的各种操作的审核追踪。XenCenter 日志文件存储在您的配置文件文件夹中。如果 XenCenter 安装在 Windows 2008 中，则路径为

```
%userprofile%\AppData\Citrix\XenCenter\logs\XenCenter.log
```

如果 XenCenter 安装在 Windows 8.1 中，则路径为

```
%userprofile%\AppData\Citrix\Roaming\XenCenter\logs\XenCenter.log
```

要找到 XenCenter 日志文件，例如，要打开该日志文件或通过电子邮件发送它的时候，可单击 XenCenter“帮助”菜单中的“查看应用程序日志文件”。

## 对 XenCenter 和 Citrix Hypervisor 服务器之间的连接进行故障排除

如果您在将 Citrix Hypervisor 服务器连接到 XenCenter 时遇到问题，请检查以下内容：

- XenCenter 的版本是否低于您正在尝试连接到的 Citrix Hypervisor 服务器的版本？

XenCenter 应用程序是向后兼容的，可以与旧版本的 Citrix Hypervisor 服务器正常通信，但是旧版本的 XenCenter 无法与较新版本的 Citrix Hypervisor 服务器正常通信。

要更正此问题，请安装与 Citrix Hypervisor 服务器版本相同的 XenCenter 版本或更新的版本。

- 您的许可证是否有效？

您可以在 XenCenter 中的许可证详细信息部分下 Citrix Hypervisor 服务器的常规选项卡中查看许可证访问代码的过期日期。

有关许可主机的详细信息，请参阅[许可](#)。

- Citrix Hypervisor 服务器通过以下端口使用 HTTPS 与 XenCenter 通信：

- 端口 443（使用管理 API 进行命令和响应的双向连接）
- 端口 5900（用于与半虚拟化 Linux VM 的图形 VNC 连接）。

如果在 Citrix Hypervisor 服务器和运行客户端软件的计算机之间启用了防火墙，请确保防火墙允许通过这些端口的流量。

## 集成概述

June 4, 2019

通过 Citrix Hypervisor-Nutanix 集成功能，Citrix Hypervisor 客户可以享受 Nutanix 的超融合基础结构 (HCI) 优势，例如线性可扩展性和较低的复杂性。此功能还允许 Nutanix 客户在 Nutanix HCI 平台上部署 Citrix Hypervisor。可以将 Citrix Hypervisor 集成到更广泛的 Citrix 堆栈中，并利用这一成熟、功能齐全且高度优化的集成。该堆栈包括具有 MCS 和 PVS 的 Citrix Virtual Apps and Desktops，以及应用程序磁盘。此外，Nutanix 客户还将受益于 Citrix Hypervisor 的独特卖点，例如：

- 领先的图形虚拟化解决方案
- 通过 Windows Update 自动交付 I/O 驱动程序
- 容器支持
- PVS 读取缓存
- 使用直接检查 API 的高级威胁检测

客户可以使用 Nutanix Prism Web 控制台配置存储和群集（池），以及监视 HCI 平台，包括 VM 存储。可以通过使用 XenCenter 来管理 Citrix Hypervisor 和执行 VM 生命周期操作。

### 注意：

- Citrix Hypervisor-Nutanix 集成仅适用于 Nutanix 服务器以及运行 Nutanix 堆栈的认证服务器。有关受支持服务器的列表，请参阅[硬件兼容性列表](#)。
- 本指南作为对 [Nutanix 上的 Citrix Hypervisor 管理指南](#) 进行补充的辅助文档。
- 每个 Citrix Hypervisor 版本均要求使用兼容的 Nutanix 版本，以启用 Citrix Hypervisor-Nutanix 集成功能。有关兼容版本的信息，请参阅 [Nutanix 上的 Citrix Hypervisor 管理指南](#)。

## 兼容性要求和注意事项

由于 Nutanix 与 Citrix Hypervisor 紧密集成，以下 Citrix Hypervisor 功能不适用于 Nutanix HCI 部署：

- 存储实时迁移 - 存储实时迁移支持将 VM 的存储从一个存储库 (SR) 移动到另一个存储库。但是，Nutanix 支持对整个群集的存储进行聚合。
- 灾难恢复 (**DR**) - Citrix Hypervisor 中的 DR 功能基于在 Nutanix 部署中不适用的阵列级别镜像。
- **WLB** 电源管理 - 在 HCI 环境中，必须对任何硬件的删除进行严格管理。此删除通过 Nutanix Prism UI 进行调配，因此 Nutanix 部署不允许使用 Citrix Hypervisor Workload Balancing (WLB) 中的电源管理功能。
- **SR** - HCI 托管其自己的 SR，从而简化可选择的 SR 类型。本地、NFS、iSCSI、硬件 HBA、SMB/CIFS 和软件 FCoE 不可用。但是，ISO 库受支持。

- **IntelliCache** - Citrix Hypervisor 中的 IntelliCache 功能不适用，因为 Nutanix 存储已经确保了数据局部性。
- **XenCenter** 自动更新 - 主机聚合群集存储要求以特定的顺序重新启动主机。  
使用 XenCenter 安装工具向导时，自动更新选项不可用。但是，可以选择从 **Citrix** 下载更新或新版本或从磁盘选择更新或补充包。  
安装更新后，如果需要重新启动，请使用 Nutanix Prism 控制台来触发滚动池重新启动。此过程可确保以正确的顺序重新启动。

此外，在 Nutanix 上使用 Citrix Hypervisor 时，以下限制同样适用：

- Nutanix 中的“群集”概念对应于 Citrix Hypervisor 中“池”的概念。此对应意味着群集大小被限制为每个群集最多 64 个主机。
- 高可用性功能仅允许一个主机出现故障（假定群集中至少有三个主机）。此限制仅在 XenCenter 中强制执行。
- 客户必须使用 OVS 作为网络后端。不支持 Linux 桥接。
- 支持静止快照的 Citrix Hypervisor VSS 提供程序不适用，因为集成基于 Nutanix 本机快照格式。

## 配置

使用 Nutanix Prism Web 控制台可以配置存储和群集基础结构，以及监视 HCI 平台，包括 VM 存储。可以通过使用 XenCenter 来管理 Citrix Hypervisor 和执行 VM 生命周期操作。

### 注意：

使用 Nutanix Prism 控制台可以管理群集和池中的主机成员身份。pool-join 和 pool-eject 选项在 Citrix Hypervisor 用户界面上处于禁用状态。提出此建议是因为 Citrix Hypervisor 池中的主机必须与 Nutanix 群集中的主机匹配。

Nutanix 软件堆栈在每个主机上称为 Controller VM (CVM) 的特权 VM 中运行。与 Citrix Hypervisor 控制域 (dom0) 类似，CVM 域在主机的 **Nutanix CVM** 控制台选项卡上的 CLI 和 XenCenter 中可见。Controller VM 在 XenCenter 中未显示为 VM。

要修改分配给 **Controller VM** 的内存，请执行以下操作：

根据您使用的 Nutanix 功能，您可以选择修改分配给 Controller VM 的内存。在 Controller VM 上运行以下命令以修改内存分配：

```
1 xe vm-memory-limits-set uuid=<CVM UUID>
2 static-min=10GiB dynamic-min=10GiB dynamic-max=10GiB
3 static-max=10GiB
```

### 注意：

重新启动主机以使更改生效。

## 标准引导补充包

June 4, 2019

使用 Citrix Hypervisor 标准引导补充包，客户可以在启动时评测其 Citrix Hypervisor 主机的关键组件。它还提供了 API，允许远程验证解决方案安全地收集这些评测结果。此补充包与支持可信执行技术 (TXT) 的 Intel 计算机系统兼容。

可以从 [Citrix Hypervisor 8.0 Premium Edition](#) 页面下载该补充包。

### 注意：

标准引导补充包可供以下客户使用：Citrix Hypervisor Premium Edition 客户，或可通过其 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。

## 背景

安装该补充包后，当 Citrix Hypervisor 服务器下次启动时，Intel 的 TXT 会评测低级别系统组件（例如，固件、BIOS、Xen 虚拟机管理程序、dom0 内核和 dom0 initrd），并将评测结果存储在主机上被称为可信平台模块 (TPM) 的安全位置。为客户端提供远程认证解决方案等新界面，以安全地收集这些度量。

## 远程验证

远程验证解决方案的工作方式是通过连接到处于“已知良好”干净状态的 Citrix Hypervisor 服务器。它可以安全地远程查询 Citrix Hypervisor 服务器的 TPM，以获取低级别关键系统评测的列表。它会将这些度量存储在“白名单”或“已知良好”的度量列表中。

此时，远程认证软件将定期收集关键系统度量，并将其与“已知良好”列表进行比较。

在以下情况下，主机将被视为“不受信任”：

- 如果远程认证软件无法收集度量
- 如果度量发生了更改
- 如果加密密钥无效

在这种情况下，客户将收到通知。CloudStack、OpenStack 或 Workload Balancing 软件等较高级别的调配软件可以对受影响的主机执行智能安全操作。

## 准备 Citrix Hypervisor 服务器

为使此补充包正常运行，请在尝试收集数据之前，在其主机的 BIOS 中编辑以下设置：

1. 将 Citrix Hypervisor 服务器设置为在旧模式下启动。

注意：

Measured Boot 不支持 UEFI 引导模式。

2. 启用 **Intel AES-NI**。
3. 开启 **TPM 安全性**或 **On with Pre-boot Measurements**。
4. 清除 TPM。

此操作会擦除以前的所有设置以及与 TPM 相关联的密码，以允许 Citrix Hypervisor 标准引导补充包控制 TPM。

注意：

执行此步骤后需要重新启动。

5. 启用 **TPM**。
6. 启用 **Intel TXT**。

注意：

- 执行步骤 5 和步骤 6 后需要重新启动。
- BIOS 设置因硬件制造商而异。请参阅硬件文档以了解如何为特定环境启用 TPM 和 TXT。

## 安装补充包

使用 Citrix Hypervisor CLI 安装该补充包。与任何软件更新一样，我们建议您在应用此补充包之前先备份数据。

可以在 *zip* 文件中传输补充包。如果补充包 ISO 包含在 zip 文件中，请先解压此 zip 文件（以生成磁盘 ISO 映像），然后再执行以下步骤。

### 安装到正在运行的 **Citrix Hypervisor** 系统

1. 将补充包直接下载到要更新的 Citrix Hypervisor 主机。

我们建议将其存储在 `/tmp/` 目录中。

或者，可以将该文件下载到连接 Internet 的计算机，并将 ISO 映像刻录为 CD。

2. 使用 XenCenter 访问 Citrix Hypervisor 主机的控制台，或者使用 Secure Shell (SSH) 直接登录。
3. 最简单的方法是直接使用 ISO 文件进行安装。输入以下命令：

```
1 xe-install-supplemental-pack /tmp/Citrix Hypervisor-8.0-measured-  
boot.iso
```

或者，如果选择将 ISO 刻录为 CD，则必须装载磁盘。例如，对于 CD-ROM，请输入以下信息：

```
1   mkdir -p /mnt/tmp
2   mount /dev/<path to cd-rom> /mnt/tmp
3   cd /mnt/tmp/
4   ./install.sh
5   cd /
6   umount /mnt/tmp
```

4. 为使所做的更改生效，请重新启动主机。

### 重新安装

如果要在存在早期版本的基础上安装此补充包，请确认覆盖之前的安装。在安装 `xe-install-supplemental-pack` 期间出现提示时，输入 Y。

### 更新默认密码

在早期版本的补充包中，默认密码已设置为 `xenroot` 且带有一个尾随换行。在此版本的补充包中，已删除默认密码的该尾随换行，新的默认密码为 `xenroot`。

自定义密码可以在 `/opt/xensource/tpm/config` 中进行设置，并且必须是纯文本密码的 sha1 哈希，该密码可通过 `echo -n <password | sha1sum` 生成。如果忽略此命令行中的 `-n`，密码中将包含尾随换行。

### 设置资产标签

可以使用包含 `--tpm_set_asset_tag` 和 `--tpm_clear_asset_tag` 方法的 `/opt/xensource/tpm/xentpm` 二进制文件设置资产标签，也可以使用具有 `tpm_set_asset_tag`（具有 `tag` 参数）和 `tpm_clear_asset_tag` 功能的管理 API `tpm` 插件进行设置：

```
1   /opt/xensource/tpm/xentpm --tpm_set_asset_tag <tag_sha1>
2   /opt/xensource/tpm/xentpm --tpm_clear_asset_tag
3   xe host-call-plugin uuid=<host_uuid> plugin=tpm fn=
    tpm_set_asset_tag args:tag=<tag_sha1>
4   xe host-call-plugin uuid=<host_uuid> plugin=tpm fn=
    tpm_clear_asset_tag
```

#### 注意：

执行此步骤后需要重新启动。

## 更多信息

要下载标准引导补充包，请参阅 [Citrix Hypervisor 8.0 Premium Edition](#) 页面。

如果遇到与安装该补充包有关的任何问题，请联系 [Citrix 技术支持](#)。

有关 Citrix Hypervisor 8.0 文档，请访问 [Citrix 产品文档](#) Web 站点。

## Workload Balancing

June 4, 2019

Workload Balancing 是以虚拟设备形式打包的 Citrix Hypervisor 组件，可用于：

- 创建关于 Citrix Hypervisor 环境中 VM 性能的报告
- 评估资源利用情况，并根据工作负载将虚拟机放置在池中最合适的主机上

### 注意：

- Workload Balancing 适用于 Citrix Hypervisor Premium Edition 客户或者通过 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。
- Workload Balancing 8.0 与所有受支持版本的 Citrix Hypervisor 和 XenServer 均兼容。

即使您不想使用 Workload Balancing 来平衡 VM 负载，也仍可能需要运行该组件以使用工作负载报告功能。部署 Workload Balancing 来管理虚拟机工作负载后，该组件可以：

- 在 Citrix Hypervisor 资源池中的各主机之间平衡 VM 工作负载
- 确定用来启动虚拟机的最佳主机
- 确定用来恢复已关闭虚拟机的最佳主机
- 确定主机出现故障时虚拟机将移动到的最佳主机
- 将主机置于维护模式或使主机退出维护模式时，确定该主机每个虚拟机的最佳服务器

Workload Balancing 可以根据您所选的优先顺序自动完成这些任务，或者提示您接受其重新平衡和放置建议。您还可以将 Workload Balancing 配置为在一天中的特定时间自动关闭主机（例如在晚上关闭主机以节约能源）。

Workload Balancing 的工作是评估池中各个 VM 的使用情况。当主机超出性能阈值时，Workload Balancing 会将 VM 重新定位到池中负载较低的主机。为重新平衡工作负载，Workload Balancing 会移动 VM 以平衡各主机上的资源使用情况。

为确保重新平衡和放置建议能够满足环境的需求，您可以将 Workload Balancing 配置为根据资源性能优化工作负载，或者配置为最大化可主机上安装的虚拟机数。可以将这些优化模式配置为在预定义的时间自动切换，或者始终保持不变。为提高精细程度，可以调整各个资源指标（CPU、网络、磁盘和内存）的权重。

Workload Balancing 提供有关主机和池运行状况、优化和 VM 性能的历史报告，以及 VM 移动历史记录，以帮助您完成容量规划。

## 工作负载报告

由于 Workload Balancing 会捕获性能数据，因此您可以使用该组件来生成有关虚拟化环境的报告，也称为工作负载报告。

工作负载报告提供关于池或主机的运行状况、审核、优化及放置（或移动）历史记录的数据。此外，您还可以运行计费报告，该报告会显示虚拟机的使用情况并帮助您度和分配成本。

要运行报告，无需将 Workload Balancing 配置为提供放置建议或移动虚拟机。但是，您必须配置 Workload Balancing 组件。理想情况下，必须将临界阈值设置为反映池中主机性能降级点的值。

有关详细信息，请参阅[生成工作负载报告](#)。

## Workload Balancing 基本概念

虚拟机运行期间，将在物理主机上占用计算资源，例如 CPU、内存、网络读取、网络写入、磁盘读取和磁盘写入。例如，与同一主机上的其他虚拟机相比，有些虚拟机占用的 CPU 资源可能更多，具体取决于其工作负载。工作负载由在虚拟机上运行的应用程序及其用户事务决定。当然，主机上所有虚拟机的合并资源占用量会使主机的可用资源减少。

Workload Balancing 会捕获虚拟机和物理主机上资源性能的数据，并将这些数据存储在数据库中。Workload Balancing 将这些数据与您设置的首选项相结合，用以提供优化和放置建议。

优化是“改进”主机以与您的目标保持一致的一种方式：Workload Balancing 提供在池中的主机之间重新分发虚拟机以提高性能或密度的建议。Workload Balancing 提出建议时，将以其目标（在池中各主机之间实现平衡或协调）为出发点。如果 Workload Balancing 实施这些建议，该操作就被称为优化。

在 Workload Balancing 环境中：

- 性能指主机上物理资源的使用情况（例如，主机上 CPU、内存、网络和磁盘的利用率）。将 Workload Balancing 设置为实现最高性能时，它提供的虚拟机放置建议将确保每个虚拟机获得最多的可用资源。
- 密度指主机上的 VM 数。将 Workload Balancing 设置为实现最大密度时，它提供的 VM 放置建议可以减少池中启动的主机数量。它可以确保 VM 具有足够的计算能力。

Workload Balancing 不会与您已指定的高可用性设置冲突：这些功能兼容。

## 池要求

要通过 Workload Balancing 实现池的负载平衡，池中的各主机必须满足实时迁移功能的要求，其中包括：

- 共享的远程存储
- 相似的处理配置
- 千兆位以太网

如果主机不满足这些要求，Workload Balancing 将无法迁移池中的虚拟机。

注意

包含启用了 vGPU 的 VM 的池不支持 Workload Balancing。Workload Balancing 无法为连接了 vGPU 的 VM 执行容量规划。

## Workload Balancing 入门

June 4, 2019

只需几个简单的步骤即可配置 Workload Balancing 虚拟设备：

1. 从 <http://www.citrix.com/downloads> 下载 Workload Balancing 虚拟设备，然后将其导入 XenCenter。
2. 从虚拟设备控制台配置 Workload Balancing 设备。
3. 将池连接到 Workload Balancing 虚拟设备。

要使用 Workload Balancing 对池进行平衡，池中的主机必须满足[管理](#)中所述的实时迁移功能的要求。

### 导入 Workload Balancing 虚拟设备

Workload Balancing 虚拟设备是设计为在 Citrix Hypervisor 服务器上运行的单个预安装虚拟机。导入该虚拟设备前，请查看必备条件信息和注意事项。

#### 必备条件

此设备设计为在 Citrix Hypervisor 7.1 和更高版本上运行。它能够对运行 Citrix Hypervisor 5.5 和更高版本的主机的池进行监视。我们建议使用 XenCenter 管理控制台导入虚拟设备。运行 Workload Balancing 虚拟设备至少需要 2 GB RAM 和 20 GB 磁盘空间。

#### 导入虚拟设备前需要考虑的事项

在导入 Workload Balancing 虚拟设备之前，请注意以下事项并根据需要对环境进行相应的更改。此外，还请查看 Workload Balancing 发行说明，了解特定版本的最新要求。

- 通信端口。在启动 Workload Balancing 配置向导之前，需要确定 Workload Balancing 虚拟设备要用来进行通信的端口。在 Workload Balancing 配置期间，系统会提示您设置此端口。默认情况下，Workload Balancing 服务器使用 8012。

注意：

请勿将 Workload Balancing 端口设置为端口 443。Workload Balancing 虚拟设备不能接受通过端

□ 443 (标准的 SSL/HTTPS 端口) 建立的连接。

- **Workload Balancing** 帐户。Workload Balancing 配置向导要求您为 Workload Balancing 帐户和数据库帐户选择并输入用户名和密码。在运行配置向导之前，不需要创建这些帐户。配置向导将为您创建这些帐户。
- 跨池监视。可以将 Workload Balancing 虚拟设备放在一个池中，而使用该设备监视另一个池。（例如，Workload Balancing 虚拟设备位于池 A 中，但使用该设备监视池 B）。

注意：

Workload Balancing 虚拟设备要求托管虚拟设备的物理计算机上的时间与受监视的池正在使用的时间相匹配。无法更改 Workload Balancing 虚拟设备上的时间。我们建议您将托管 Workload Balancing 的物理计算机和所监视池中的各主机指向同一个网络时间 (NTP) 服务器。

- **Citrix Hypervisor 与 Workload Balancing 通过 HTTPS 进行通信。**因此，在 Workload Balancing 配置期间，Workload Balancing 会代表您自动创建一个自签名证书。可以将此证书更改为来自某个证书颁发机构颁发的证书，并且/或者将 Citrix Hypervisor 配置为对证书进行验证。有关信息，请参阅《Workload Balancing 管理员指南》。
- 历史数据存储量和磁盘空间大小。可以存储的历史数据量取决于以下因素：
  - 分配给 Workload Balancing 的虚拟磁盘的大小（默认为 20 GB）
  - 所需的最小磁盘空间，默认为 2048 MB，由 wlb.conf 文件中的 `GroomingRequiredMinimumDiskSizeInMB` 参数控制。

如果要存储大量历史数据，可以执行以下操作之一：

- 按[管理](#)中所述存档数据
- 增大分配给 Workload Balancing 虚拟设备的虚拟磁盘大小。

例如，当您希望使用 WLB 池审核追踪功能并将报告精度配置为中等或更高级别时。

要增大磁盘大小，请导入该虚拟设备，然后通过执行《Workload Balancing 管理员指南》中的过程来增大虚拟磁盘大小。

- 实现 **Workload Balancing** 的负载平衡。如果您想要使用 Workload Balancing 虚拟设备来管理自身，请在导入该虚拟设备时指定远程共享的存储。

注意：

使用 Workload Balancing 来管理自身时，Workload Balancing 无法针对 Workload Balancing 虚拟设备执行“启动于”放置建议。进行自身管理的 Workload Balancing 之所以无法提供放置建议，是因为要执行该功能就必须运行该虚拟设备。但是，它可以平衡 Workload Balancing 虚拟设备的负载，就像平衡所管理的任何其他 VM 一样。

## 规划资源池大小

Workload Balancing 需要进行特定的配置才能在大型池中成功运行。

## 下载虚拟设备

Workload Balancing 虚拟设备以 `.xva` 格式打包。您可以从 Citrix 下载页面 <http://www.citrix.com/downloads> 下载该虚拟设备。在下载该文件时，将其保存到本地硬盘驱动器（通常位于安装 XenCenter 的计算机上）上的一个文件夹中。`.xva` 下载完成后，您可以将其导入 XenCenter。

## 将虚拟设备导入 XenCenter

使用 XenCenter 将 Workload Balancing 虚拟设备导入池。

要将虚拟设备导入 Citrix Hypervisor，请执行以下操作：

1. 打开 XenCenter。
2. 在要导入虚拟设备软件包的池（或主机）上单击鼠标右键，然后选择导入。
3. 浏览到 `vpx-wlb.xva` 软件包。
4. 选择要运行 Workload Balancing 虚拟设备的池或主服务器。

如果选择池，VM 将自动在该池中最适合的主机上启动。

或者，如果您不使用 Workload Balancing 管理 Workload Balancing 虚拟设备，则可以为 Workload Balancing 虚拟设备设置主服务器。此设置可确保虚拟设备始终在同一主机上启动。

5. 选择用于存储 Workload Balancing 虚拟设备的虚拟磁盘的存储库。此存储库必须至少有 20 GB 可用空间。  
可以选择本地存储，也可以选择远程存储。但是，如果选择本地存储，则无法使用 Workload Balancing 来管理虚拟设备。
6. 为 Workload Balancing 虚拟设备定义虚拟接口。在此版本中，Workload Balancing 设计为通过单个虚拟接口通信。
7. 选择能够访问 Workload Balancing 所管理的池的网络。
8. 使导入后启动 **VM** 复选框处于启用状态，然后单击完成以导入虚拟设备。
9. 在完成 Workload Balancing `.xva` 文件的导入之后，Workload Balancing 虚拟机将出现在 XenCenter 中的资源窗格中。

## 配置 Workload Balancing 虚拟设备

在完成 Workload Balancing 虚拟设备的导入后，必须先对其进行配置才能使用它来管理池。为了引导您完成配置，Workload Balancing 虚拟设备在 XenCenter 中提供了一个配置向导。要显示该向导，请在资源窗格中选择该虚拟设备，然后单击控制台选项卡。对于所有选项，按 Enter 键以接受默认选项。

1. 在导入 Workload Balancing 虚拟设备之后，单击控制台选项卡。
2. 输入 `yes` 以接受许可协议的条款。要拒绝 EULA，请输入 `no`。

注意：

Workload Balancing 虚拟设备也受 Workload Balancing 虚拟设备中 `/opt/vpx/wlb` 目录中所包含的许可证的约束。

3. 为 Workload Balancing 虚拟机输入新的 root 用户密码并进行确认。Citrix 建议选择强密码。

注意：

当您输入密码时，控制台上不显示字符占位符（如星号）。

4. 输入要分配给 Workload Balancing 虚拟设备的计算机名称。

5. 输入该虚拟设备的域后缀。

例如，如果虚拟设备的完全限定的域名 (FQDN) 为 `wlb-vpx-pos-pool.domain4.bedford4.ctx`，则输入 `domain4.bedford4.ctx`。

注意：

Workload Balancing 虚拟设备不会自动将其 FQDN 添加到域名系统 (DNS) 服务器。因此，如果您希望池使用 FQDN 连接到 Workload Balancing，则必须手动将该 FQDN 添加到 DNS 服务器。

6. 输入 `y` 以使用 DHCP 自动获取 Workload Balancing 虚拟机的 IP 地址。否则，输入 `n`，然后输入该虚拟机的静态 IP 地址、子网掩码和网关。

注意：

只要 IP 地址的租用期未过期，就可以使用 DHCP。重要的是，IP 地址不要发生更改：如果发生更改，XenServer 与 Workload Balancing 之间的连接将中断。

7. 输入 Workload Balancing 数据库的用户名，或者按 **Enter** 键以使用数据库帐户的默认用户名 (`postgres`)。

此时将针对 Workload Balancing 数据库创建一个帐户。Workload Balancing 服务使用该帐户对 Workload Balancing 数据库进行读/写操作。记下用户名和密码。如果您要直接管理 Workload Balancing PostgreSQL 数据库（例如，要导出数据），可能需要这些信息。

8. 输入 Workload Balancing 数据库的密码。在按 **Enter** 键之后，会显示一些消息，指出配置向导正在加载数据库对象。

9. 输入 Workload Balancing 服务器的用户名和密码。

此操作将会创建 Citrix Hypervisor 用来连接到 Workload Balancing 的帐户。默认用户名为 **wlbuser**。

10. 输入 Workload Balancing 服务器的端口。Workload Balancing 服务器使用此端口进行通信。

默认情况下，Workload Balancing 服务器使用 8012 端口。该端口号不能设置为 443（默认的 SSL 端口号）。

注意：

如果更改此处的端口，请在将池连接到 Workload Balancing 时指定新的端口号。例如，通过在连接 **WLB** 服务器对话框中指定该端口。

请确保您为 Workload Balancing 指定的端口在所有的防火墙中都处于打开状态。

按 **Enter** 键之后，Workload Balancing 将继续进行虚拟设备配置，包括创建自签名证书。

11. 此时，还可以通过输入 VM 用户名（通常为 `root`）和之前创建的 `root` 用户密码来登录虚拟设备。但是，只有当您需要进行登录。

配置 Workload Balancing 后，按照连接 Workload Balancing 虚拟设备中的说明，将池连接到 Workload Balancing 虚拟设备。

如有必要，可以在以下位置找到 Workload Balancing 配置文件：`/opt/vpx/wlb/wlb.conf`。Workload Balancing 日志文件位于以下位置：`/var/log/wlb/LogFile.log`。有关这些文件及其用途的详细信息，请参阅《Workload Balancing 管理员指南》。

### 连接 Workload Balancing 虚拟设备

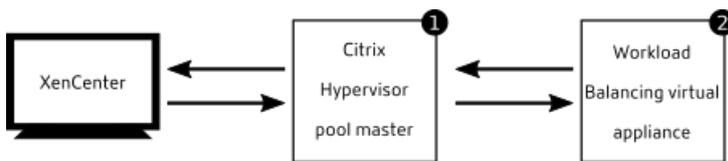
注意：

Workload Balancing 适用于 Citrix Hypervisor Premium Edition 客户或者通过 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。有关 Citrix Hypervisor 许可的详细信息，请参阅[许可](#)。要升级或购买 Citrix Hypervisor 许可证，请访问[Citrix Web 站点](#)。

配置 Workload Balancing 之后，使用 CLI 或 XenCenter 将要管理的池连接到 WLB 虚拟设备。

要完成后续的 XenCenter 过程，需要以下信息：

- Workload Balancing 虚拟设备的 IP 地址或 FQDN 及其端口号。
- 您希望 Workload Balancing 监视的资源池（即池主服务器）的凭据。
- 在 Workload Balancing 配置期间创建的 Workload Balancing 帐户的凭据。Citrix Hypervisor 使用此帐户与 Workload Balancing 进行通信。



要在连接 Workload Balancing 服务器时指定 Workload Balancing FQDN，请先将 Workload Balancing 服务器的主机名和 IP 地址添加到 DNS 服务器。

首次连接 Workload Balancing 时，它将使用默认的阈值和设置来平衡工作负载。默认情况下自动功能（例如自动优化模式、电源管理和自动化）处于禁用状态。

### 连接 Workload Balancing 和证书

如果要上载其他（受信任的）证书或者配置证书验证，在将池连接到 Workload Balancing 之前，请注意以下几点：

- 如果您希望 Citrix Hypervisor 验证自签名的 Workload Balancing 证书，必须使用 Workload Balancing IP 地址连接到 Workload Balancing。系统将基于该 IP 地址将自签名证书颁发给 Workload Balancing。
- 如果要使用证书颁发机构颁发的证书，在连接 Workload Balancing 时可以更方便地指定 FQDN。但是，您可以在连接 **WLB** 服务器对话框中指定静态 IP 地址。使用此 IP 地址作为证书中的使用者备用名称 (SAN)。

《Workload Balancing 管理员指南》中提供了有关配置证书的详细信息。

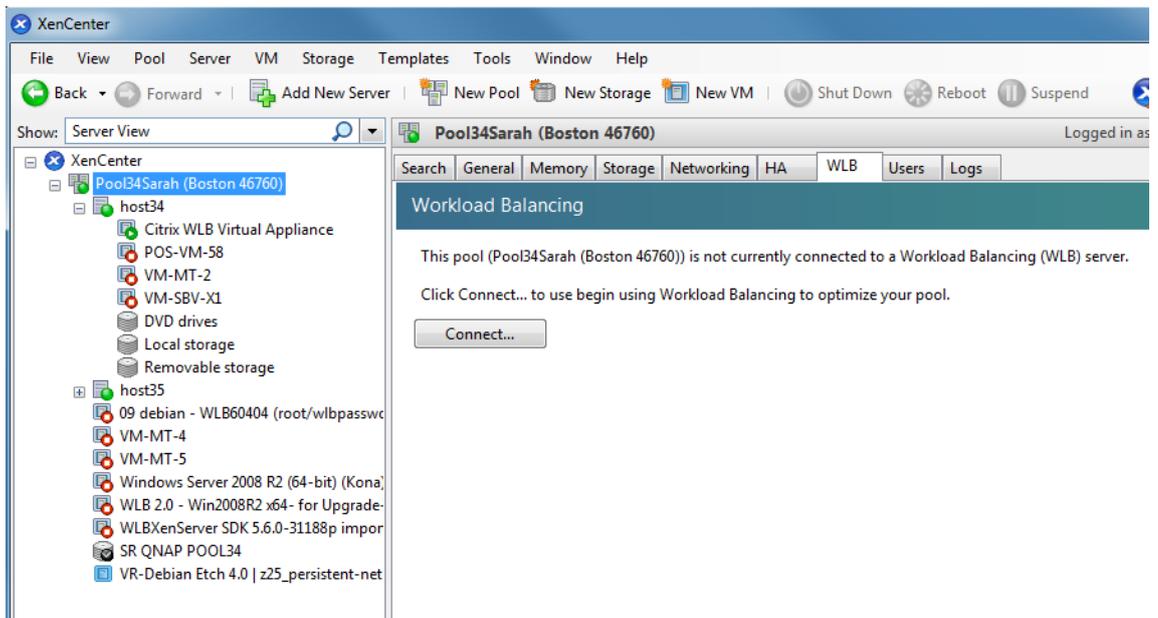
### 将池连接到 **Workload Balancing** 虚拟设备

注意：

Workload Balancing 适用于 Citrix Hypervisor Premium Edition 客户或者通过 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。要升级或购买 Citrix Hypervisor 许可证，请访问 [Citrix Web 站点](#)。

1. 在 XenCenter 的“基础结构”窗格中，选择 XenCenter > *your-resource-pool*。
2. 在“属性”窗格中，单击“WLB”选项卡。

“WLB”选项卡将显示“连接”按钮。



3. 在“WLB”选项卡中，单击“连接”。此时将显示“连接 WLB 服务器”对话框。

**Connect to WLB Server**

**Server Address**  
Enter the address of the Workload Balancing server this Citrix Hypervisor resource pool will use.

Address:

Port:  (Default is 8012)

**WLB Server Credentials**  
Enter the credentials Citrix Hypervisor will use to connect to the Workload Balancing server.

Username:

Password:

**Citrix Hypervisor Credentials**  
Enter the credentials the Workload Balancing Server will use to connect to Citrix Hypervisor.

Username:

Password:

Use the current XenCenter credentials

OK Cancel

4. 在“服务器地址”部分中，输入以下信息：

- a) 在“地址”框中，键入 Workload Balancing 设备的 IP 地址或 FQDN。例如，您的 WLB-appliance-computername.yourdomain.net。

提示：

有关详细信息，请参阅获取 WLB 虚拟设备的 IP 地址。

- b) (可选) 如果您在 Workload Balancing 配置期间更改了 Workload Balancing 端口，请在“端口”框中输入端口号。Citrix Hypervisor 使用此端口与 Workload Balancing 进行通信。

默认情况下，Citrix Hypervisor 通过端口 8012 连接 Workload Balancing。

注意：

仅在 Workload Balancing 配置期间更改了此端口号时才对其进行编辑。在 Workload Balancing 配置期间指定的端口号、在任何防火墙中指定的端口号以及在“连接 WLB 服务器”对话框中指定的端口号都必须一致。

5. 在“WLB 服务器凭据”部分中，输入 Citrix Hypervisor 池（主服务器）将用来连接 Workload Balancing 虚拟设备的用户名和密码。

Update Credentials

**WLB Server Credentials**

Enter the credentials Citrix Hypervisor will use to connect to the Workload Balancing server.

Username:

Password:

这些凭据必须是在 Workload Balancing 配置期间创建的帐户。默认情况下，此帐户的用户名为 **wlbuser**。

- 在“Citrix Hypervisor 凭据”部分中，输入您正在配置的池的用户名和密码（通常是池主服务器的密码）。Workload Balancing 将使用这些凭据连接池中的主机。

**Citrix Hypervisor Credentials**

Enter the credentials the Workload Balancing Server will use to connect to Citrix Hypervisor.

Username:

Password:

Use the current XenCenter credentials

要使用当前登录 Citrix Hypervisor 所使用的凭据，请选中“使用当前 XenCenter 凭据”复选框。如果您已使用 RBAC 功能为此帐户分配了角色，应确保该角色有足够的权限来配置 Workload Balancing。有关详细信息，请参阅《Workload Balancing 管理员指南》的 RBAC 部分。

- 在将池连接到 Workload Balancing 虚拟设备之后，Workload Balancing 会自动开始以默认的优化设置监视池。要修改这些设置或者更改为特定资源指定的优先级，请在继续操作之前至少等待 60 秒。或者等到 XenCenter 日志显示发现已完成。

**重要：**

在 Workload Balancing 运行一段时间之后，如果您没有收到最佳建议，请按照[管理](#)中所述对性能阈值进行评估。根据环境为 Workload Balancing 设置正确的阈值至关重要，否则它可能无法提供适当的建议。

**获取 WLB 虚拟设备的 IP 地址**

- 在 XenCenter 的“资源”窗格中选择 Workload Balancing 虚拟设备，然后选择“控制台”选项卡。
- 登录该设备。输入在导入该设备时创建的 VM 用户名（通常为“root”）及 root 用户密码。
- 在提示符处输入以下命令：

```
1 ifconfig
```

## 管理 **Workload Balancing** 虚拟设备

September 5, 2019

本文提供有关以下主题的信息：

- 使用 Workload Balancing 在可能的最佳主机上启动 VM
- 接受 Workload Balancing 提出的建议，以将 VM 移动到其他主机

注意：

Workload Balancing 适用于 Citrix Hypervisor Premium Edition 客户或者通过 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。有关 Citrix Hypervisor 许可的详细信息，请参阅[许可](#)。要升级或购买 Citrix Hypervisor 许可证，请访问 [Citrix Web 站点](#)。

### 基本任务简介

Workload Balancing 是包含许多功能的强大 Citrix Hypervisor 组件，旨在优化您的环境中的工作负载。这些功能包括：

- 主机电源管理
- 计划优化模式切换
- 运行报告。

此外，您还可以调整 Workload Balancing 在提供优化建议时使用的条件。

但是，当您刚开始使用 Workload Balancing 时，需要每天（或定期）使用 Workload Balancing 执行两项主要任务：

- 确定用来运行 VM 的最佳主机
- 接受 Workload Balancing 优化建议

在环境中运行有关工作负载的报告（在生成工作负载报告中介绍）是另一项常用的任务。

### 确定用来运行 **VM** 的最佳主机

使用 VM 放置可以确定用来启动并运行 VM 的主机。当您需要重新启动电源已关闭的 VM 并要将 VM 迁移到另一台主机时，此功能非常有用。放置建议在 Citrix Virtual Desktops 环境中可能也很有用。

### 接受 **Workload Balancing** 建议

Workload Balancing 运行一段时间后，将开始提供有关环境改进方法的建议。例如，如果您的目标是提高主机上 VM 的密度，Workload Balancing 可能会不定期就如何将 VM 合并到一台主机上提出建议。如果未在自动化模式下运行，

您可以选择接受并应用此建议或将其忽略。

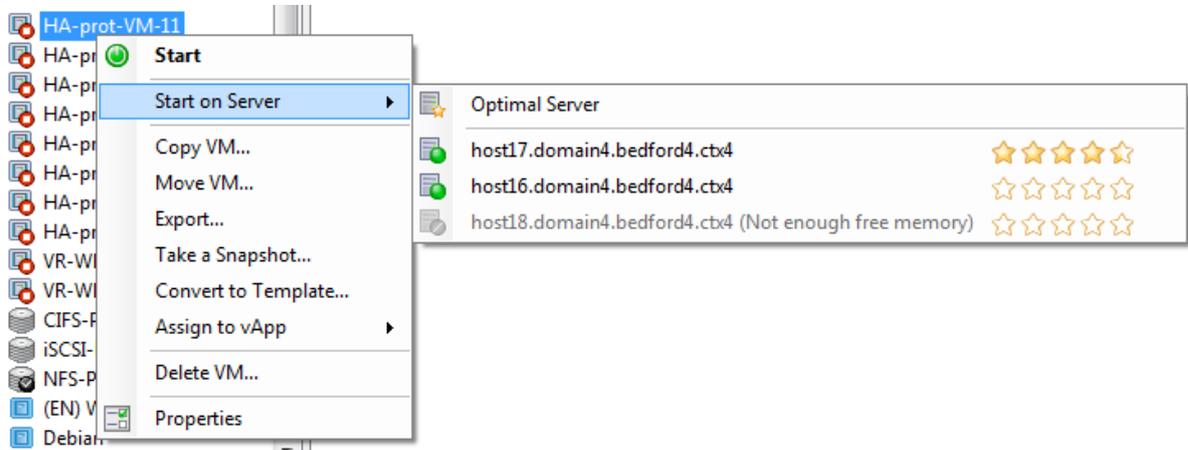
这些任务以及在 XenCenter 中执行这些任务的方法将在后面的各节中更深入地介绍。

重要：

在 Workload Balancing 运行一段时间之后，如果您没有收到最佳放置建议，请对性能阈值进行评估。了解 Workload Balancing 在何时提出建议中对此评估进行了介绍。根据环境为 Workload Balancing 设置正确的阈值至关重要，否则它可能无法提供适当的建议。

## 为 VM 选择最佳主机

启用了 Workload Balancing 并重新启动脱机 VM 后，XenCenter 建议在最佳池成员上启动 VM。因为最佳主机使用星形符号来指示，因此这些建议又称为星级评价。



术语最佳是指最适合托管工作负载的物理服务器。Workload Balancing 在确定哪一个主机是工作负载的最优选择时会考虑以下几个因素：

- 池中每个主机上的可用资源量。当池在“最高性能”模式下运行时，Workload Balancing 会尽量在各主机之间均衡分配 VM，以使所有 VM 都能达到良好的性能。当池在“最大密度”模式下运行时，Workload Balancing 会在确保 VM 有足够资源的同时，尽可能密集地将 VM 放置到主机上。
- 池运行时所采用的优化模式（“最高性能”或“最大密度”）。当池在“最高性能”模式下运行时，Workload Balancing 会尽可能将 VM 放置在可用资源最多且资源类型符合 VM 需求的主机上。当池在“最大密度”模式下运行时，Workload Balancing 会将 VM 放置在已有 VM 在运行的主机上。此方法可以确保 VM 在尽可能少的主机上运行。
- **VM** 所需资源的数量和类型。在 WLB 监视 VM 一段时间后，它将使用 VM 指标根据 VM 所需的资源类型提出放置建议。例如，如果 VM 需要，Workload Balancing 可能会选择一个可用 CPU 较少但可用内存较多的主机。

启用 Workload Balancing 后，XenCenter 会提供评级以指示用于启动 VM 的最佳主机。此外，还提供了以下评级：

- 您要在 VM 关机时将其启动
- 您要在 VM 挂起时将其启动

- 您要将 VM 迁移到其他主机（迁移和维护模式）

如果在启用 Workload Balancing 的情况下使用这些功能，主机建议将在物理主机名称旁边显示为星级评级。五颗空星表示服务器的等级最低（最差）。如果无法启动 VM 或无法将其迁移到某个主机，该主机的名称将在放置功能的菜单命令中处于灰显状态。旁将显示其无法接受 VM 的原因。

通常，如果您在 Workload Balancing 推荐的主机上启动 VM，则 Workload Balancing 的工作效率更高，提出的优化建议更加有效，并且提出建议的频率也更低。要遵循主机建议，请使用其中一项放置功能选择旁边具有最多星形符号的主机。

#### 在最佳服务器上启动虚拟机

1. 在 XenCenter 的“资源”窗格中，选择要启动的 VM。
2. 在 VM 菜单中，选择在服务器上启动，然后选择以下选项之一：
  - 最佳服务器。最佳服务器是指最能满足所启动 VM 的资源要求的物理主机。Workload Balancing 根据服务器性能指标的历史记录和您的放置策略来确定最佳服务器。最佳服务器是星级最高的服务器。
  - “最优服务器”命令下列出的带有星级的一台服务器。五颗星代表最值得推荐的（最佳）服务器，五颗空星代表最不值得推荐的服务器。

提示：

也可以通过在“资源”窗格中右键单击要启动的 VM，来选择“在服务器上启动”功能。

#### 在最佳服务器上恢复虚拟机

1. 在 XenCenter 的“资源”窗格中，选择要恢复的已挂起 VM。
2. 在 VM 菜单中，选择在服务器上恢复，然后选择以下选项之一：
  - 最佳服务器。最佳服务器是指最能满足所启动 VM 的资源要求的物理主机。Workload Balancing 根据服务器性能指标的历史记录和您的放置策略来确定最佳服务器。最佳服务器是星级最高的服务器。
  - “最优服务器”命令下列出的带有星级的一台服务器。五颗星代表最值得推荐的（最佳）服务器，五颗空星代表最不值得推荐的服务器。

提示：

也可以通过在“资源”窗格中右键单击已挂起的 VM，来选择“在服务器上恢复”功能。

#### 接受优化建议

Workload Balancing 将就 VM 的迁移方法提供建议，用以优化环境。优化建议显示在 XenCenter 的“WLB”选项卡中。

Optimization Recommendations [View History...](#)

| VM/Host                      | Operation                                                             | Reason           |
|------------------------------|-----------------------------------------------------------------------|------------------|
| HA-prot-VM-7                 | Relocate from 'host17.domain4.bedford4.ctx4' to 'host16.domain4.be... | Consolidation    |
| host17.domain4.bedford4.ctx4 | Power off                                                             | Release Resource |

[Apply Recommendations](#)

这些优化建议基于：

- 您选择的放置策略（即优化模式）。
- 资源的性能指标，例如物理主机的 CPU、内存、网络 and 磁盘利用率。
- 资源池中主机的角色。提出放置建议时，只有在没有其他主机能接受工作负载时，Workload Balancing 才会考虑将 VM 放置在池主服务器上。同样，如果池在“最大密度”模式下运行，则 Workload Balancing 在决定 VM 填入各主机的顺序时，会最后考虑池主服务器。

优化建议将显示以下信息：

- Workload Balancing 建议重新定位的 VM 的名称
- VM 当前所在的主机
- Workload Balancing 建议作为新位置的主机。

优化建议中还将显示 Workload Balancing 建议移动 VM 的原因。例如，建议将显示“CPU”，表示需要提高 CPU 使用率。如果启用 Workload Balancing 电源管理功能，Workload Balancing 还会为其提供开机或关机建议的主机显示优化建议。具体而言，是对这些建议进行合并。

单击“应用建议”后，Citrix Hypervisor 将执行“优化建议”列表中所列的所有操作。

提示：

通过使用 XenCenter 选择某个池来查找该池的优化模式。请查看“WLB”选项卡中的“配置”部分以了解该信息。

接受优化建议

1. 在 XenCenter 的“资源”窗格中，选择要显示建议的资源池。
2. 单击“WLB”选项卡。如果针对所选资源池中的任何 VM 提出了任何优化建议，这些建议都将显示在“WLB”选项卡的“优化建议”部分中。
3. 要接受这些建议，请单击“应用建议”。Citrix Hypervisor 将开始执行“优化建议”部分的“操作”列中列出的所有操作。

单击“应用建议”之后，XenCenter 会自动显示“日志”选项卡，这样您就能看到 VM 迁移的进度。

了解 **WLB** 建议的优先级低于高可用性

如果在同一个池中同时启用了 Workload Balancing 和 Citrix Hypervisor 高可用性功能，了解这两项功能的交互方式非常有用。根据设计，Workload Balancing 不会影响高可用性功能。如果 Workload Balancing 建议与高可用性设置之间存在冲突，高可用性设置始终优先。实际上，此优先级意味着：

- 如果尝试在主机上启动 VM 违反高可用性计划，Workload Balancing 不会授予您星级评价。
- 超出配置高可用性对话框中的“允许的故障数”框中指定的故障数时，Workload Balancing 将不会自动关闭任何主机。
  - 但是，Workload Balancing 建议关闭的主机数仍有可能多于允许的主机故障数。（例如，高可用性仅配置为容许一个主机故障时，Workload Balancing 仍可能建议关闭两台主机。）但是，尝试应用该建议时，XenCenter 可能会显示不再保证高可用性这一错误消息。
  - 当 Workload Balancing 在自动化模式下运行并启用了电源管理功能时，任何超出允许的主机故障数的建议都将被忽略。在此情况下，Workload Balancing 日志将显示一条消息，说明由于启用了高可用性而未应用电源管理建议。

### 生成工作负载报告

本节介绍有关使用 Workload Balancing 组件生成环境相关报告的信息，其中包括关于主机和 VM 的报告。具体来说，本节提供关于以下主题的信息：

- 如何生成报告
- 哪些工作负载报告可供使用

注意：

Workload Balancing 适用于 Citrix Hypervisor Premium Edition 客户或者通过 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。有关 Citrix Hypervisor 许可的详细信息，请参阅[许可](#)。要升级或购买 Citrix Hypervisor 许可证，请访问 [Citrix Web 站点](#)。

### 工作负载报告概述

Workload Balancing 报告可以帮助您执行容量规划、确定虚拟服务器运行状况以及评估所配置的阈值级别的效力。

Workload Balancing 允许生成三类对象的报告：物理主机、资源池和 VM。在较高级别上，Workload Balancing 提供两种类型的报告：

- 按日期显示信息的历史报告
- “汇总”式报告，提供某方面的汇总概况

Workload Balancing 提供一些用于审核目的的报告，以便您做出相关决策，例如确定 VM 的移动次数。

可以使用“池运行状况”报告来评估优化阈值的效力。虽然 Workload Balancing 提供默认阈值设置，但您可能需要调整这些默认设置，以提供适合所用环境的值。如果没有根据所用环境将优化阈值调整为正确的级别，Workload Balancing 的建议可能不适用于该环境。

要生成 Workload Balancing 报告，池必须正在运行 Workload Balancing。理想情况下，池应持续运行 Workload Balancing 达数小时或足以生成要在报告中显示的数据的时间。

### 生成 Workload Balancing 报告

1. 在 XenCenter 中，从“池”菜单中选择“View Workload Reports”（查看工作负载报告）。

提示：

也可以通过在“WLB”选项卡上单击“报告”按钮来显示“工作负载报告”屏幕。

2. 从工作负载报告屏幕的报告窗格中选择一份报告。
3. 选择报告期的开始日期和结束日期。根据所选报告，可能需要在主机列表框中指定一个主机。
4. 单击运行报告。该报告显示在报告窗口中。有关报告含义的信息，请参阅 Workload Balancing 报告词汇表。

### 在 Workload Balancing 报告中导航

生成报告之后，您可以使用报告中的工具栏按钮来导航和执行某些任务。要显示工具栏按钮的名称，请将鼠标指针停在工具栏图标上。

| 工具栏按钮                                                                               | 说明                                                         |
|-------------------------------------------------------------------------------------|------------------------------------------------------------|
|  | 文档结构图用于显示可帮助您在大型报告中进行导航的文档结构图。                             |
|  | 上一页和下一页用于在报告中向前或向后移动一页。                                    |
|  | 当与向下钻取报告结合使用时，返回到父报告用于返回到父报告。注意：此按钮仅适用于向下钻取报告，例如“池运行状况”报告。 |
|  | 停止呈现可取消生成报告。                                               |
|  | 打印用于打印报告并指定常规打印选项。这些选项包括：打印机、页数和份数。                        |
|  | 打印布局用于在打印前显示报告预览。要退出打印布局，请再次单击打印布局按钮。                      |
|  | 页面设置用于指定打印选项，例如纸张大小、页面方向和页边距。                              |

| 工具栏按钮                                                                             | 说明                                                    |
|-----------------------------------------------------------------------------------|-------------------------------------------------------|
|  | 导出用于以 Acrobat (.PDF) 文件格式或以带.XLS 扩展名的 Excel 文件格式导出报告。 |
|  | 查找用于在报告中搜索词语，例如 VM 的名称。                               |

### 打印 **Workload Balancing** 报告

打印报告之前，必须首先生成报告。

1. (可选) 通过单击下面的“打印布局”按钮预览打印的文档：
2. (可选) 通过单击下面的“页面设置”按钮更改纸张大小和来源、页面方向或页边距：
3. 单击以下打印按钮：

### 导出 **Workload Balancing** 报告

可以采用 Microsoft Excel 或 Adobe Acrobat (PDF) 格式导出报告。

1. 生成报告后，单击下面的导出按钮：
2. 从导出按钮菜单中选择以下项目之一：
  - Excel
  - Acrobat (PDF) 文件

#### 注意：

不同的报告导出格式显示的数据可能不一致，具体取决于所选导出格式。导出为 Excel 格式的报告包含可供报告使用的所有数据，包括“向下钻取”数据。导出为 PDF 格式并显示在 XenCenter 中的报告仅包含在生成报告时所选择的数据。

### **Workload Balancing** 报告词汇表

本节提供关于以下 Workload Balancing 报告的信息：

#### 计费使用分析

可以使用“计费使用分析”报告（计费报告）确定组织内的特定部门对某资源的使用量。具体而言，该报告显示池中所有 VM 的信息，包括其可用性和资源使用率。由于该报告提供 VM 运行时间信息，因而可以帮助您证明与服务级别协议的符合性及可用性。

计费报告可帮助您实施简单的计费解决方案，并简化收费方式。要对使用特定资源的客户收费，可以生成此报告，将其保存为 Excel 格式，然后编辑该电子表格来加入单价。或者，也可以将 Excel 数据导入到账单系统中。

如果您想要对使用 VM 的内部或外部客户收费，可以在 VM 命名约定中加入部门或客户名称。这种做法会使计费报告更易于阅读。

计费报告中的资源报告有时以各 VM 的物理资源分配量为基础。

该报告中的平均内存数据以当前分配给 VM 的内存量为基础。Citrix Hypervisor 支持采用固定内存分配量或自动调整内存分配量（动态内存控制）。

计费报告包含以下数据列：

- **VM 名称**。该行各列数据所对应的 VM 的名称。
- **VM Uptime** (VM 运行时间)。VM 开启（更确切地说，是 XenCenter 中该 VM 旁显示绿色图标）的分钟数。
- **vCPU Allocation** (vCPU 分配)。在 VM 上配置的虚拟 CPU 的数目。每个虚拟 CPU 将在主机上获得相等份额的物理 CPU。例如，考虑在包含两个物理 CPU 的主机上配置了八个虚拟 CPU 的情况。如果 **vCPU Allocation** (vCPU 分配) 列为 1，则此值等于该主机上总处理能力的 2/16。
- **Minimum CPU Usage (%)** (最低 CPU 使用率 (%))。在报告期间内所记录的最低虚拟 CPU 使用率值。该值以 VM 的 vCPU 容量的百分比来表示。容量基于分配给 VM 的 vCPU 数量。例如，如果为某个 VM 分配了一个 vCPU，则 **Minimum CPU Usage** (最低 CPU 使用率) 表示记录的最低 vCPU 使用率百分比。如果为该 VM 分配了两个 vCPU，则值是基于这两个 vCPU 总容量的最低使用率 (%)。

从根本上说，CPU 使用率百分比表示虚拟 CPU 所处理的最低记录工作负载。例如，如果为某个 VM 分配了一个 vCPU，而主机上的 pCPU 为 2.4 GHz，则向该 VM 分配 0.3 GHz。如果该 VM 的 **Minimum CPU Usage** (最低 CPU 使用率) 为 20%，则在报告期间该 VM 的物理主机的最低 CPU 使用率为 60 MHz。

- **Maximum CPU Usage (%)** (最高 CPU 使用率 (%))。在报告期间内 VM 所占用的虚拟 CPU 容量的最高百分比。占用的 CPU 容量是基于分配给 VM 的虚拟 CPU 容量的百分比。例如，如果为该 VM 分配了一个 vCPU，则“Maximum CPU Usage” (最高 CPU 使用率) 表示在报告期间所记录的最高 vCPU 使用率百分比。如果为该 VM 分配了两个虚拟 CPU，则此列中的值表示基于这两个虚拟 CPU 总容量的最高利用率。
- **Average CPU Usage (%)** (平均 CPU 使用率 (%))。在报告期间内所用 VM 虚拟 CPU 容量的平均量，以百分比表示。CPU 容量是分配给 VM 的虚拟 CPU 容量。如果为该 VM 分配了两个虚拟 CPU，则此列中的值表示基于这两个虚拟 CPU 总容量的平均利用率。
- **Total Storage Allocation (GB)** (总存储分配 (GB))。运行报告时当前分配给 VM 的磁盘空间量。通常，此磁盘空间量是您在创建 VM 时为其分配的磁盘空间量，除非对其进行了修改。
- **Virtual NIC Allocation** (虚拟网卡分配)。分配给 VM 的虚拟接口 (VIF) 的数目。
- **Current Minimum Dynamic Memory (MB)** (当前最低动态内存 (MB))。

- **Fixed memory allocation** (固定内存分配)。如果为 VM 分配了固定大小的内存（例如 1024 MB），以下各列中都将显示此内存量：“Current Minimum Dynamic Memory (MB)” (当前最低动态内存 (MB))、“Current Maximum Dynamic Memory (MB)” (当前最高动态内存 (MB))、“Current

Assigned Memory (MB)” (当前分配内存 (MB)) 以及 “Average Assigned Memory (MB)” (平均分配内存 (MB))。

- **Dynamic memory allocation** (动态内存分配)。如果将 Citrix Hypervisor 配置为使用动态内存控制，则此列中将显示为该范围指定的最低内存量。如果该范围的最低内存量为 1024 MB，最大内存量为 2048 MB，则 **Current Minimum Dynamic Memory (MB)** (当前最低动态内存 (MB)) 列将显示 1024 MB。

- **Current Maximum Dynamic Memory (MB)** (当前最高动态内存 (MB))。

- **Dynamic memory allocation** (动态内存分配)。如果 Citrix Hypervisor 根据范围自动调整 VM 的内存，则此列中将显示为该范围指定的最高内存量。例如，如果内存范围值为最低 1024 MB、最高 2048 MB，则 **Current Maximum Dynamic Memory (MB)** (当前最高动态内存 (MB)) 列中将显示 2048 MB。
- **Fixed memory allocation** (固定内存分配)。如果为 VM 分配了固定大小的内存 (例如 1024 MB)，以下各列中都将显示此内存量：“Current Minimum Dynamic Memory (MB)” (当前最低动态内存 (MB))、“Current Maximum Dynamic Memory (MB)” (当前最高动态内存 (MB))、“Current Assigned Memory (MB)” (当前分配内存 (MB)) 以及 “Average Assigned Memory (MB)” (平均分配内存 (MB))。

- **Current Assigned Memory (MB)** (当前分配内存 (MB))。

- **Dynamic memory allocation** (动态内存分配)。如果配置动态内存控制，则该值表示在报告运行时 Citrix Hypervisor 分配给 VM 的内存量。
- **Fixed memory allocation** (固定内存分配)。如果为 VM 分配了固定大小的内存 (例如 1024 MB)，以下各列中都将显示此内存量：“Current Minimum Dynamic Memory (MB)” (当前最低动态内存 (MB))、“Current Maximum Dynamic Memory (MB)” (当前最高动态内存 (MB))、“Current Assigned Memory (MB)” (当前分配内存 (MB)) 以及 “Average Assigned Memory (MB)” (平均分配内存 (MB))。

注意：

如果在运行此报告之前刚刚更改了 VM 的内存分配，则该列中的值将反映您配置的新内存分配。

- **Average Assigned Memory (MB)** (平均分配内存 (MB))。

- **Dynamic memory allocation** (动态内存分配)。如果配置动态内存控制，则该值表示在报告期间 Citrix Hypervisor 分配给 VM 的平均内存量。
- **Fixed memory allocation** (固定内存分配)。如果为 VM 分配了固定大小的内存 (例如 1024 MB)，以下各列中都将显示此内存量：“Current Minimum Dynamic Memory (MB)” (当前最低动态内存 (MB))、“Current Maximum Dynamic Memory (MB)” (当前最高动态内存 (MB))、“Current Assigned Memory (MB)” (当前分配内存 (MB)) 以及 “Average Assigned Memory (MB)” (平均分配内存 (MB))。

注意：

如果在运行此报告之前刚刚更改了 VM 的内存分配，该列中的值可能与先前显示的值相同。此列中的值反映的是一段时期的平均值。

- **Average Network Reads (BPS)** (平均网络读取量 (BPS))。VM 在报告期间接收的平均数据量 (比特/秒)。
- **Average Network Writes (BPS)** (平均网络写入量 (BPS))。VM 在报告期间发送的平均数据量 (比特/秒)。
- **Average Network Usage (BPS)** (平均网络使用量 (BPS))。平均网络读取量和平均网络写入量的总和 (比特/秒)。如果 VM 在报告期间平均发送 1027 bps 且平均接收 23831 bps，则 “Average Network Usage” (平均网络使用量) 是这些值的总和，即 24858 bps。
- **Total Network Usage (BPS)** (网络使用总量 (BPS))。在报告期间发生的所有网络读写事务的总量 (比特/秒)。

### 主机运行状况历史记录

此报告显示特定主机上与阈值相关的资源 (CPU、内存、网络读取和网络写入) 性能。

彩色线 (红色、绿色和黄色) 代表不同的阈值。可以将此报告与主机的池运行状况报告结合使用，来确定主机的性能可能会对整体池运行状况产生的影响。编辑性能阈值时，可以通过此报告深入了解主机性能。

可以通过日均或时均方式显示资源使用情况。时均方式可以让您了解一天中最忙的几个小时，它显示某一时段内的平均资源使用情况。

要查看按小时分组的报告数据，请在主机运行状况历史记录下展开 **Click to view report data grouped by house for the time period** (单击以查看该时段内按小时分组的报告数据)。

Workload Balancing 将显示所设置时段内每小时的平均值。数据点基于该时段内所有日期该小时的平均利用率。例如，在 2009 年 5 月 1 日到 2009 年 5 月 15 日的报告中，“平均 CPU 使用率”数据点表示全部 15 天中每天 12:00 的资源使用率。此信息是加总后的平均值。如果在 5 月 1 日正午 12:00 的 CPU 使用率是 82%，在 5 月 2 日正午 12:00 的使用率是 88%，在所有其他日期中正午 12:00 的使用率都是 75%，那么正午 12:00 的平均使用率显示为 76.3%。

注意：

Workload Balancing 将对尖峰进行平滑处理，因此数据不会出现虚假的高峰。

### 池优化性能历史记录

优化性能报告显示针对池的平均资源使用情况进行优化事件。优化资源池时，这些事件是实例。具体来说，它将显示 CPU、内存、网络读取和网络写入的资源使用情况。

虚线表示在所选日期期间内池的平均利用率。蓝色条指示进行池优化的日期。

此报告可以帮助您确定 Workload Balancing 在您的环境中是否正常工作。可以使用此报告查看导致优化事件的原因 (即，Workload Balancing 提供优化建议前的资源使用情况)。

此报告将显示每天的平均资源使用情况。而不显示峰值利用率，例如当系统处于高负荷状态时。如果 Workload Balancing 没有提供优化建议，您还可以使用此报告查看资源池的性能情况。

一般来说，在优化事件后，资源使用情况将降低或保持不变。如果在优化后资源使用情况未出现改进，请考虑重新调整阈值。此外，请考虑资源池是否有过多 VM，以及在您指定的时段内是否添加或删除了新的 VM。

### 池审核追踪

此报告显示 Citrix Hypervisor 审核日志的内容。审核日志是旨在记录对未经授权操作的执行尝试和选择授权操作的 Citrix Hypervisor 功能。这些操作包括：

- 导入和导出
- 主机和池备份
- 来宾和主机控制台访问。

如果为 Citrix Hypervisor 管理员提供了自己的用户帐户，并通过 RBAC 功能为其分配了不同的角色，则该报告可以提供比较有用的信息。

#### 重要：

要运行审核日志报告，必须启用审核日志记录功能。默认情况下，在 Workload Balancing 虚拟设备中始终启用审核日志。

增强的池审核追踪功能使您能够指定审核日志报告的精度。您也可以搜索审核追踪日志并按特定用户、对象和时间过滤这些日志。默认情况下，池审核追踪精度设置为最低。此选项可捕获有限数量的特定用户和对象类型的数据。您可以根据报告所需的信息详细程度随时修改设置。例如，将用户友好的审核日志报告的精度设置为中。如果您需要详细的报告，可以将此选项设置为最高。

### 报告内容

池审核追踪报告包含以下信息：

- 时间。Citrix Hypervisor 记录用户操作的时间。
- 用户名。创建会话（在该会话中执行操作）的人员的名称。有时，此值可能是用户 ID
- 事件对象。作为操作主体的对象（例如，VM）。
- 事件操作。发生的操作。有关这些操作的定义，请参阅审核日志事件名称。
- Access（访问权限）。用户是否有权执行操作。
- 对象名称。对象的名称（例如，VM 的名称）。
- 对象 UUID。对象的 UUID（例如，VM 的 UUID）。
- 成功。此信息提供操作的状态（即，操作是否成功）。

## 审核日志事件名称

审核日志报告会记录 Citrix Hypervisor 事件、事件对象和操作，包括导入/导出、主机和池备份以及来宾和主机控制台访问。下表定义了 Citrix Hypervisor“审核日志”和“池审核追踪”报告中经常出现的一些典型事件。该表还指定了这些事件的精度。

在“池审核追踪”报告中，**Event Action** 列中列出的事件适用于池、VM 或主机。要确定事件应用的对象，请参阅报告中的**Event Object**和**Object Name**列。有关更多事件定义，请参阅《Citrix Hypervisor 管理 API》中关于事件的部分。

| 池审核追踪精度 | 事件操作                                     | 用户操作                               |
|---------|------------------------------------------|------------------------------------|
| 最低      | <code>pool.join</code>                   | 指示主机加入新池                           |
| 最低      | <code>pool.join_force</code>             | 指示（强制）主机加入池                        |
| 中       | <code>SR.destroy</code>                  | 已销毁存储库                             |
| 中       | <code>SR.create</code>                   | 已创建存储库                             |
| 中       | <code>VDI.snapshot</code>                | 生成 VDI 的一个只读快照，返回引用给快照             |
| 中       | <code>VDI.clone</code>                   | 生成一个与 VDI 完全相同的副本，返回对新磁盘的引用        |
| 中       | <code>VIF.plug</code>                    | 热插拔指定的 VIF，将它动态连接到运行中的 VM          |
| 中       | <code>VIF.unplug</code>                  | 热插拔指定的 VIF，动态断开它与运行中的 VM 的连接       |
| 最高      | <code>auth.get_subject_identifier</code> | 查询外部目录服务，从便于用户理解的主题名称获取字符串形式的主题标识符 |
| 最高      | <code>task.cancel</code>                 | 已请求取消任务                            |
| 最高      | <code>VBD.insert</code>                  | 将新的介质插入设备                          |
| 最高      | <code>VIF.get_by_uuid</code>             | 获得对含有指定 UUID 的 VIF 实例的引用           |
| 最高      | <code>VDI.get_sharable</code>            | 获得给定 VDI 的可共享字段                    |
| 最高      | <code>SR.get_all</code>                  | 返回系统已知的所有 SR 的列表。                  |
| 最高      | <code>pool.create_new_blob</code>        | 为与此池相关的已命名二进制数据段创建一个占位符            |
| 最高      | <code>host.send_debug_keys</code>        | 将给定字符串作为调试密钥注入到 Xen 中              |

| 池审核追踪精度 | 事件操作                            | 用户操作                                                      |
|---------|---------------------------------|-----------------------------------------------------------|
| 最高      | <code>VM.get_boot_record</code> | 返回一个描述 VM 动态状态的记录，该状态在 VM 启动和更新时初始化，以反映运行时配置变化，例如，CPU 热插拔 |

### 池运行状况

池运行状况报告显示资源池及其主机在四个不同阈值范围（临界阈值、高阈值、中阈值和低阈值）所花费时间的百分比。您可以使用池运行状况报告来评估性能阈值的效力。

关于本报告的几点解释：

- 不论您选择哪种放置策略，平均中阈值（蓝色）的资源利用率都是最佳资源利用率。同样，饼图中的蓝色部分指示主机使用资源的最佳时间量。
- 平均低阈值百分比（绿色）的资源利用率不一定是正值。低资源利用率是否为正取决于放置策略。如果放置策略为“最大密度”，而且资源使用情况为绿色，则 WLB 可能不会在该主机或池上安装最大数量的 VM。如果是这种情况，请调整性能阈值，直到大部分资源利用率下降到“平均中”（蓝色）阈值范围内。
- 平均临界阈值百分比（红色）的资源利用率指示平均资源利用率达到或超过临界阈值的时间量。

如果双击有关主机资源使用情况的饼图，XenCenter 将显示该主机上该资源的主机运行状况历史记录报告。单击工具栏上的返回到父报告可返回到池运行状况历史记录报告。

如果您发现大多数报告结果都不在“平均中阈值”范围内，您可能需要调整此池的“临界”阈值。Workload Balancing 提供默认的阈值设置，但这些默认设置并非在所有环境中都有效。如果没有根据所用环境将阈值调整为正确的级别，Workload Balancing 优化和放置建议可能不适用。有关详细信息，请参阅更改临界阈值。

### 池运行状况历史记录

此报告提供池中所有物理主机的资源利用率随时间变化的线图。通过此报告，您可以了解资源利用率的趋势 - 是否相对于所设定的阈值（临界、高、中和低）趋向于增加。通过监视该报告中数据点的趋势，您可以评估性能阈值的效力。

当您池连接到 Workload Balancing 时，Workload Balancing 会根据您设置的临界阈值来推断阈值范围。虽然与池运行状况报告相似，但池运行状况历史记录报告显示的是资源在某一特定日期的平均利用率。而不是资源处于某个阈值范围的总时长。

除“平均可用内存”图外，数据点的平均值在任何时候都不应越过临界阈值线（红色）。对于“平均可用内存”图，数据点的平均值在任何时候都不应在临界阈值线（位于该图底部）之下。由于此图显示可用内存，因此临界阈值为低值，这与其他资源不同。

关于本报告的几点解释：

- 当表中的“平均使用率”线接近“平均中阈值”（蓝色）线时，它表示池的资源利用率处于最佳状态。无论配置哪种放置策略，都会出现此情况。
- 接近“平均低阈值”（绿色）的资源利用率不一定为正值。低资源利用率是否为正取决于放置策略。在以下情况下：
  - 放置策略为“最大密度”
  - 大部分日期的平均利用率线与绿线重合或低于绿线，那么 Workload Balancing 可能不会尽可能密集地在该池上放置 VM。如果是这种情况，请调整池的临界阈值，直到大部分资源利用率下降到“平均中”（蓝色）阈值范围内。
- 当“平均使用率”线与“平均临界阈值百分比”（红色）相交时，这表示平均资源利用率达到或超过该资源临界阈值的天数。

如果图中的数据点都不在平均中阈值范围内，但您又对此池的性能很满意，您可能需要调整该池的临界阈值。有关详细信息，请参阅更改临界阈值。

#### 池优化历史记录

利用池优化历史记录报告可以按时间顺序查看 Workload Balancing 优化活动。

优化活动以图形和表格形式进行汇总。深入表格内部的日期字段时，将显示当日执行的每个池优化的详细信息。

利用此报告可以查看以下信息：

- VM 名称。Workload Balancing 优化的 VM 的名称。
- Reason（原因）。进行优化的原因。
- Method（方法）。优化是否成功。
- From Host（源主机）。最初托管 VM 的物理服务器。
- To Host（目标主机）。VM 迁移到的物理服务器。
- 时间。发生优化的时间。

提示：

还可以通过在“WLB”选项卡上单击“查看历史记录”链接来生成“池优化历史记录”报告。

#### 虚拟机移动历史记录

此线图显示一段时间内资源池中 VM 的迁移次数。它指示迁移是否源于优化建议，以及 VM 移动到哪个主机。此报告还将指示进行优化的原因。您可以使用该报告审核池中发生迁移的次数。

关于本报告的几点解释：

- 图表左侧的数值代表可能的迁移次数。此值基于资源池中的 VM 数量。
- 展开报告“日期”部分中的 + 号，可以查看特定日期的迁移详细信息。

### 虚拟机性能历史记录

此报告显示在您指定的时段内特定主机上每个 VM 的性能数据。Workload Balancing 的性能数据基于为 VM 分配的虚拟资源数量。例如，如果 VM 的“Average CPU Usage”（平均 CPU 使用率）为 67%，则 VM 在指定时段内平均使用其 vCPU 的 67%。

该报告的初始视图显示在指定的时段内资源利用率的平均值。

展开 + 号后，将显示各资源的线图。可以使用这些图来查看资源利用率随时间变化的趋势。

该报告显示 CPU 使用率、可用内存、网络读取/写入和磁盘读取/写入的数据。

### 管理 **Workload Balancing** 功能和设置

本节介绍如何对 Workload Balancing 设置进行可选的更改，其中包括如何：

- 调整优化模式
- 自动优化及管理电源
- 更改临界阈值
- 调整指标加权
- 从建议中排除主机
- 配置高级自动设置和数据存储
- 调整池审核追踪精度设置

本节假定您已经将池连接到 Workload Balancing 虚拟设备。有关下载、导入和配置 Workload Balancing 虚拟设备的信息，请参阅[快速入门](#)。要连接虚拟设备，请参阅[连接 Workload Balancing 虚拟设备](#)。

### 更改 **Workload Balancing** 设置

连接到 Workload Balancing 虚拟设备后，可以根据需要编辑 Workload Balancing 在计算放置和优化建议时所使用的设置。

您可以修改的放置和优化设置包括如下：

- 更改放置策略
- 配置自动优化和电源管理
- 编辑性能阈值和指标加权
- 排除主机。

Workload Balancing 设置会集中应用于池中的所有 VM 和主机。

如果网络和磁盘阈值与环境中的硬件相符，初始时可以考虑使用 Workload Balancing 中的大多数默认设置。

在 Workload Balancing 启用一段时间后，我们建议评估性能阈值，并确定是否要编辑这些阈值。例如，以下情况下应考虑调整阈值：

- 在尚不需要建议时获得建议。如果出现这种情况，请尝试调整阈值，直到 Workload Balancing 开始提供适当的建议。
- 在您预期收到建议时却并未得到建议。例如，如果网络带宽不足，而您却未收到建议，则可能需要调整设置。如果出现这种情况，请尝试降低网络临界阈值，直到 Workload Balancing 开始提供建议。

在编辑阈值前，您可以为池中的每台物理主机生成池运行状况报告以及池运行状况历史记录报告。

可以使用 XenCenter 中的 Workload Balancing 配置属性修改配置设置。

要更新 Citrix Hypervisor 与 Workload Balancing 服务器通信时所使用的凭据，请参阅编辑 Workload Balancing 配置文件。

在 XenCenter 的“基础结构”窗格中，选择 XenCenter > `your-pool`。

在“属性”窗格中，单击“WLB”选项卡。

在“WLB”选项卡中，单击“设置”。

#### 调整优化模式

Workload Balancing 根据您选择的放置策略提出建议，以重新平衡或优化环境中的 VM 工作负载。放置策略被称为优化模式。

Workload Balancing 允许您选择两种优化模式：

- 最高性能。（默认）Workload Balancing 尝试在资源池中的所有物理主机上平均分布工作负载。目标是最大限度地降低所有主机上 CPU、内存和网络的压力。如果选择“最高性能”放置策略，Workload Balancing 将在某个主机达到高阈值时提出优化建议。
- 最大化密度。Workload Balancing 将尝试通过合并活动的 VM 来最大限度地减少需要联机的物理主机数量。

如果选择“最大密度”放置策略，可以指定与“最高性能”策略相似的参数。但是，Workload Balancing 会使用这些参数来确定如何将 VM 并入一个主机。如果放置策略为“最大密度”，Workload Balancing 将在某台虚拟机达到低阈值时提出合并优化建议。

Workload Balancing 还允许您始终应用这些优化模式（“固定”模式），或者按指定的时段在各模式之间进行切换（“排定”模式）：

- 固定优化模式会将 Workload Balancing 设置为始终具有特定的优化行为。此行为可以是实现最佳性能，也可以是实现最高密度。
- 您可以通过计划优化模式安排 Workload Balancing 在一天中的不同时间应用不同的优化模式。例如，在白天，当有用户处于连接状态时，您可能希望将 Workload Balancing 配置为优化性能。而在夜晚，为了节约能源，可以将 Workload Balancing 指定为以最大密度为目的进行优化。

配置计划优化模式时，Workload Balancing 会在指定时段开始时自动切换为相应优化模式。可以配置“每天”、“工作日”、“周末”或具体某些天。对于小时，可以选择一天中的具体时刻。

在 XenCenter 的“资源”窗口中，选择 XenCenter > [your-pool](#)。

在“属性”窗格中，单击“WLB”选项卡。

在“WLB”选项卡中，单击“设置”。

在左侧窗格中，单击“优化模式”。

在“优化模式”页面的固定部分中，选择以下优化模式之一：

- 最高性能。（默认）尝试在资源池中的所有物理主机上平均分布工作负载。目标是最大限度地降低所有主机上 CPU、内存和网络的压力。
- 最大化密度。尝试在一台物理主机上安装尽可能多的 VM。目标是最大限度地减少需要联机的物理主机数量。（Workload Balancing 将考虑合并后 VM 的性能，并在主机上的某项资源达到临界阈值时，提出提高性能的建议。）

在 XenCenter 的“基础结构”窗格中，选择 XenCenter > [your-pool](#)。

在“属性”窗格中，单击“WLB”选项卡。

在“WLB”选项卡中，单击“设置”。

在左侧窗格中，单击“优化模式”。

在“优化模式”窗格中，选择计划。计划部分将变为可用状态。

单击“添加新项”。

在“更改为”框中，选择以下模式之一：

- 最高性能。尝试在资源池中的所有物理主机上平均分布工作负载。目标是最大限度地降低所有主机上 CPU、内存和网络的压力。
- 最大化密度。尝试在一台物理主机上安装尽可能多的 VM。目标是最大限度地减少需要联机的物理主机数量。

选择希望 Workload Balancing 开始以此模式运行的星期和时间。

创建更多的计划模式更改（即“任务”），直至达到所需的数量。如果只计划一项任务，Workload Balancing 将按计划切换到该模式，但不会再切换回原来的模式。

单击确定。

按照上述过程中的第 1 到 4 步操作，以显示“优化模式”对话框。

从“计划模式更改”列表中选择要删除或禁用的任务。

执行以下操作之一：

- 永久删除任务。单击“删除”按钮。
- 暂时停止任务运行。右键单击任务，然后单击“禁用”。

提示：

- 1 - 此外，通过选择任务，单击“编辑”并选中“优化模式”对话框中的“启用任务”复选框，可以禁用或启用任务。
- 2 - 要重新启用某项任务，请右键单击“计划模式更改”列表中的该任务，然后单击“启用”。

执行以下操作之一：

- 双击要编辑的任务。
- 选择要编辑的任务，并单击“编辑”。

在“更改为”框中，选择其他模式或者根据需要进行其他更改。

注意：

在单击“确定”前，如果单击“取消”，将撤消在“优化”选项卡中进行的所有更改，包括删除任务操作。

## 自动优化及管理电源

可以将 Workload Balancing 配置为自动应用建议（自动化），并自动打开或关闭主机。要自动关闭主机（例如，在使用率较低的时段），必须将 Workload Balancing 配置为自动应用建议并启用电源管理功能。电源管理和自动化功能都将在后面的部分加以介绍。

### 自动应用建议

可以将 Workload Balancing 配置为代表您自动应用建议，并自动实施其建议的优化措施。您可以使用此功能（称为自动接受优化）自动应用任何建议，包括提高性能或关闭主机的建议。但是，要在 VM 使用率下降时关闭主机，必须配置自动化功能、电源管理功能和“最大密度”模式。

默认情况下，Workload Balancing 不自动应用建议。如果希望 Workload Balancing 自动应用建议，必须启用“自动化”功能。如果未启用，则必须通过单击“应用建议”手动应用建议。

如果建议与高可用性设置冲突，则 Workload Balancing 不会自动将这些建议应用于主机或 VM。如果应用 Workload Balancing 优化建议导致池被过度使用，XenCenter 将询问您是否要继续应用建议。如果启用“自动化”功能，Workload Balancing 应用的电源管理建议的数量不会超出“高可用性”计划中允许的主机故障数量。

在启用“自动化”功能的情况下运行 Workload Balancing 时，这种行为有时称为在自动化模式下运行。

可以调整 Workload Balancing 在自动化模式下应用建议的方式。有关信息，请参阅设置保守或主动的自动化建议。

### 启用 Workload Balancing 电源管理

术语“电源管理”是指开启或关闭物理主机电源的能力。在 Workload Balancing 环境中，此术语是指根据池的总工作负载开启或关闭该池中的主机。

在主机上配置 Workload Balancing 电源管理需要满足以下条件：

- 主机的硬件具有远程开/关机功能
- 为该主机配置主机开启功能
- 已将该主机明确选择为参与 (Workload Balancing) 电源管理

此外, 如果希望 Workload Balancing 自动关闭主机, 还需要将 Workload Balancing 配置为执行以下操作:

- 自动应用建议
- 自动应用电源管理建议

如果 WLB 在“最大密度”模式下检测到池中有未使用的资源, 则会提出关闭主机的建议, 直到耗尽池中的所有过剩容量。如果池中足够的主机容量来关闭主机, WLB 建议不要关闭主机, 直到池工作负载降至池中有足够的主机容量为止。如果您将 Workload Balancing 配置为自动关闭额外主机, 它会应用这些建议, 其结果与手动模式相同。

将主机设置为参与电源管理时, Workload Balancing 会根据需要提出开/关机建议。

如果您在“最高性能”模式下运行:

- 如果将 WLB 配置为自动打开主机, WLB 将在主机上的资源利用率超过高阈值时打开主机。
- Workload Balancing 一旦将主机开启就不会再将其关闭。

如果启用用于自动应用电源管理建议的选项, 应在池级别启用。但可以指定希望池中的哪些主机参与电源管理。

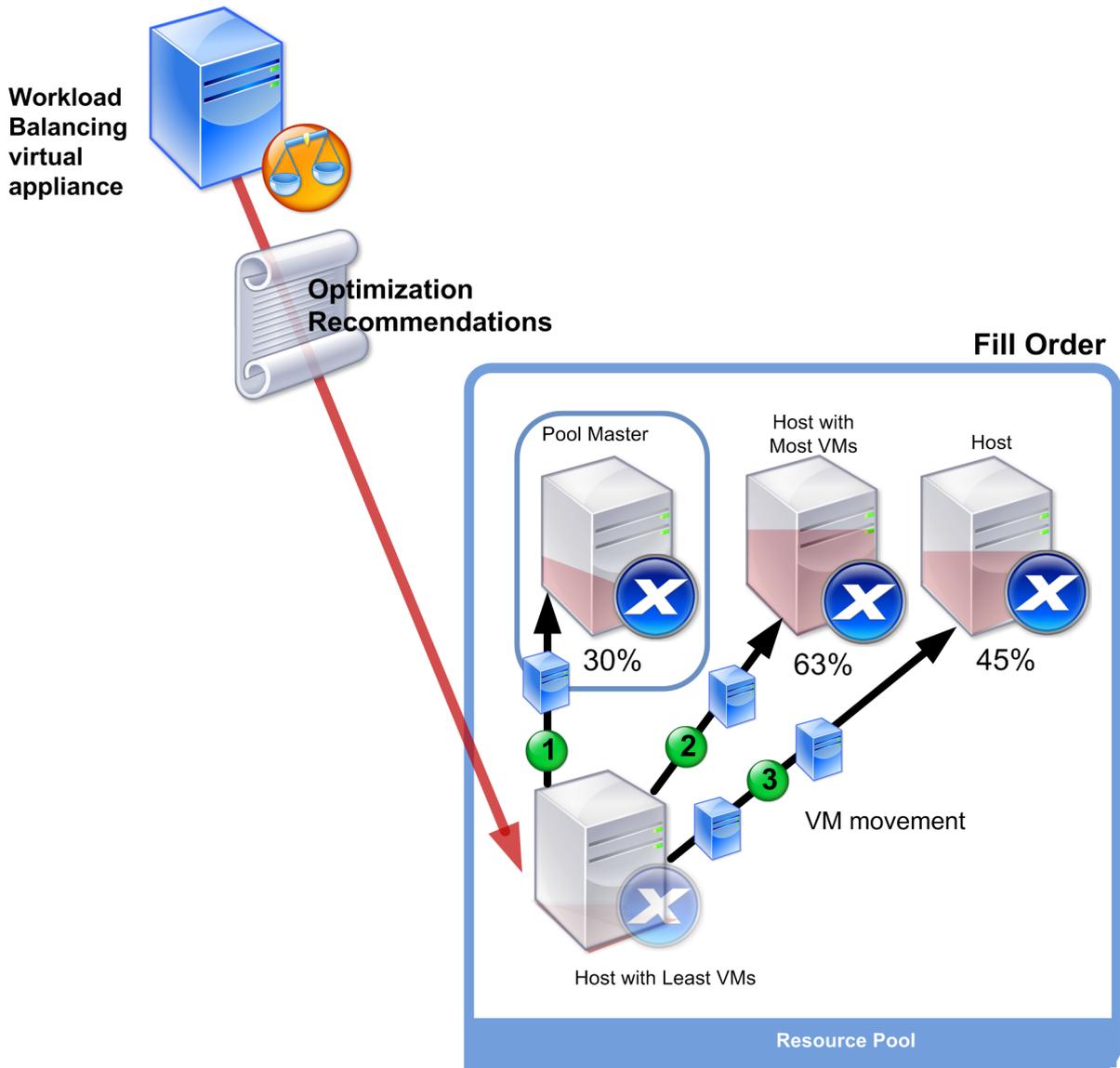
了解电源管理行为

Workload Balancing 在提出开启或关闭主机的建议之前, 会选择 VM 要转移 (即“填充”) 到的主机。按以下顺序进行转移:

1. 填充池主服务器, 因为该主机无法关闭。
2. 填充包含最多 VM 的主机。
3. 在后续主机中选择运行最多 VM 的主机来填充。

当 Workload Balancing 填充池主服务器时, 会为该服务器假定一个低 (内部) 阈值。Workload Balancing 使用这些低阈值作为缓冲, 来防止池主服务器过载。

Workload Balancing 按照此顺序填充主机以提高密度。



当池处于“最大密度”模式时，如果 WLB 检测到性能问题，它会建议在已开启的主机之间迁移工作负载。如果 Workload Balancing 通过这种方法不能解决该问题，它会尝试打开主机。（Workload Balancing 在决定要打开的主机时，所应用的标准与将优化模式设置为“最高性能”时所采用的标准相同。）

当 WLB 在“最高性能”模式下运行时，只要所有池成员上的资源利用率未降至高阈值以下，Workload Balancing 就会提出开启主机的建议。

在迁移 VM 时，如果 Workload Balancing 确定提高容量对池的整体性能有益，它会自动开启主机，或者建议开启主机。

**重要：**

仅当主机是由 Workload Balancing 关闭时，Workload Balancing 才会建议您将其打开。

针对电源管理和 VM 整合设计环境

规划 Citrix Hypervisor 实施时，如果您想要配置自动 VM 整合和电源管理，应考虑工作负载设计。例如，您可能需要：

- 将不同类型的工作负载放置在不同的池中。如果您的环境中包含不同类型的工作负载，请考虑是否在不同的池中定位托管这些工作负载的 VM。此外，请考虑将 VM 拆分为不同的池，这些 VM 托管在使用某些类型的硬件时具有更高性能的各种类型的应用程序。

由于电源管理和 VM 合并在池级别进行管理，因此设计的池中应包含要以相同比率合并的工作负载。请确保考虑多项因素，例如控制自动化建议中讨论的因素。

- 从 **Workload Balancing** 中排除主机。某些主机可能需要始终处于开启状态。有关详细信息，请参阅从建议中排除主机。

#### 自动应用优化建议

1. 在 XenCenter 的“基础结构”窗格中，选择 XenCenter > *your-pool*。
2. 在“属性”窗格中，单击“WLB”选项卡。
3. 在“WLB”选项卡中，单击“设置”。
4. 在左侧窗格中，单击“自动化”。
5. 选中以下一个或多个复选框：
  - 自动应用优化建议。如果选中此选项，则无需手动接受优化建议。Workload Balancing 会自动接受提供的优化和放置建议。
  - 自动应用电源管理建议。此选项的行为因池的优化模式而异：
    - “最高性能”模式。当启用了自动应用电源管理建议时，如果可以通过开启主机来提高主机性能，Workload Balancing 将自动开启主机。
    - “最大密度”模式。当启用了自动应用电源管理建议时，Workload Balancing 将在资源利用率降低到阈值以下时，自动关闭主机。也就是说，Workload Balancing 将在低使用率期间自动关闭主机。
6. (可选。) 单击“设置”对话框左侧窗格中的“高级”并执行以下一项或多项操作，以调整优化建议：
  - 指定在 Workload Balancing 自动应用优化建议前必须达到的建议次数。默认值为三次，也就是说，将在第三次提出某建议时应用该建议。
  - 选择希望 Workload Balancing 自动应用的优化建议所应达到的最低级别。默认值为“高”。
  - 更改 Workload Balancing 应用优化建议的主动性。

您可能也需要指定 Workload Balancing 在将优化建议应用到最新移动的 VM 前必须等待的时间（分钟）。

所有这些设置将在设置保守或主动的自动化建议中更深入地介绍。
7. 执行以下操作之一：

- 如果要配置电源管理功能，请单击“自动化/电源管理”并继续选择要进行电源管理的主机。
- 如果不希望配置电源管理并且已完成自动化功能的配置，请单击确定。

#### 选择要进行电源管理的主机

1. 在“电源管理”部分，选择希望 Workload Balancing 提供开启和关闭建议的主机。

##### 注意：

如果在未选中自动应用电源管理建议的情况下选择要获得电源管理建议的主机，则会导致 WLB 提出电源管理建议，但不会自动应用这些建议。

2. 单击确定。如果资源池中的所有主机均不支持远程电源管理，Workload Balancing 会显示“所有主机均不支持电源管理”消息。

#### 了解 Workload Balancing 在何时提出建议

Workload Balancing 将对照阈值不断评估所管理的池中各物理主机和 VM 的资源指标。阈值是相当于边界值的预设值，主机必须超过这些值 Workload Balancing 才会提出优化建议。指标达到非常高的水平。Workload Balancing 的处理过程如下所示：

1. Workload Balancing 检测到某资源已超出阈值。
2. Workload Balancing 评估是否应提出优化建议。
3. Workload Balancing 确定其建议的哪个主机与目标主机的功能相同。目标主机是 Workload Balancing 建议用来重新定位一个或多个 VM 的主机。
4. Workload Balancing 提出建议。

在 WLB 确定主机可以受益于优化之后并提出建议之前，它会评估池中的其他主机以确定以下事项：

1. 实施优化的顺序（哪些主机、哪些 VM）
2. 提出建议时建议在何处放置 VM

为完成这两项任务，Workload Balancing 将使用阈值和加权，如下所示：

- 阈值是 Workload Balancing 用来比较池的资源指标的边界值。阈值用于确定是否提出建议以及哪些主机适合托管重新定位的 VM。
- 加权是根据所需关注度排列资源优先级的方式，用于确定处理顺序。Workload Balancing 决定提出建议后，将使用指定的重要资源来确定以下内容：
  - 首先解决哪些主机的性能问题
  - 建议首先迁移哪些 VM

对于 Workload Balancing 所监视的每个资源，系统都提供了四个阈值级别（临界、高、中、低），这些级别将在后面的部分进行讨论。Workload Balancing 将在主机上的资源指标达到以下程度时评估是否提出建议：

- 当池在“最高性能”模式下运行时，超过高阈值（改善性能）
- 当池在“最大密度”模式下运行时，低于低阈值（合并主机上的 VM）
- 当池在“最大密度”模式下运行时，超过临界阈值（改善性能）

例如，如果在“最高性能”模式下运行的池的高阈值为 80%，则当主机上的 CPU 使用率达到 80.1% 时，WLB 将评估是否提出建议。

当资源超出阈值范围时，WLB 将根据历史性能评估资源的指标，以避免根据短时尖峰而提出优化建议。为此，Workload Balancing 将评估在以下时间点收集的资源利用率数据，从而计算历史平均利用率指标：

| 收集数据的时间      | 权重  |
|--------------|-----|
| 超出阈值时（即实时数据） | 70% |
| 超出阈值前 30 分钟  | 25% |
| 超出阈值前 24 小时  | 5%  |

如果主机上的 CPU 使用率在中午 12:02 超出阈值，WLB 将检查当天上午 11:32 和前一天中午 12:02 的利用率。例如，如果 CPU 使用率为以下值，WLB 将不提出建议：

- 在当天中午 12:02 为 80.1%
- 在当天上午 11:32 为 50%
- 前一天中午 12:32 为 78%

出现此行为是因为历史平均利用率为 72.47%，因此 Workload Balancing 认为该利用率为短时尖峰。但如果上午 11:32 的 CPU 使用率为 78%，Workload Balancing 将提出建议，因为历史平均利用率为 80.1%。

#### 优化和合并过程

Workload Balancing 确认可能的优化措施的过程因优化模式（“最高性能”或“最大密度”）而异。但无论采用何种优化模式，提出优化和放置建议的过程都分为两个阶段：

1. 确定可能的优化措施。（即将哪些 VM 迁出主机。）
2. 确定放置建议。（即哪些主机适合成为新主机。）

#### 注意：

Workload Balancing 仅建议迁移符合 Citrix Hypervisor 实时迁移条件（包括目标主机必须拥有 VM 所需要的存储）的 VM。目标主机还必须具有充足的资源来支持添加 VM，而不会超出对池配置的优化模式的阈值。例如，“最高性能”模式下的高阈值和“最大密度”模式下的临界阈值。

当 Workload Balancing 在自动化模式下运行时，您可以调整其应用建议的方式。有关详细信息，请参阅设置保守或主动的自动化建议。

## “最高性能”模式下的优化建议过程

在“最高性能”模式下运行时，Workload Balancing 采用以下过程来确定可能的优化措施：

1. Workload Balancing 每两分钟对池中的各主机进行一次资源利用率评估。为此，它将监视每个主机并确定每项资源的利用率是否超出其高阈值。有关高阈值的详细信息，请参阅更改临界阈值。

在“最高性能”模式下，如果资源利用率超出其高阈值，WLB 将启动该过程以确定是否应提出优化建议。Workload Balancing 在确定是否应提出优化建议时，将以这些建议能否缓解性能降低（例如高阈值导致的性能降低）为依据。

例如，如果 Workload Balancing 发现主机 A 上 VM 的性能因 CPU 资源不足而受到负面影响，则当 Workload Balancing 找到 CPU 使用率较低的另一台主机时，它将建议将一个或多个 VM 迁移到该主机。

2. 如果主机上的资源利用率超出相关的阈值，Workload Balancing 会将以下数据结合起来，算出历史平均利用率：
  - 资源的当前利用率
  - 30 分钟前的历史数据
  - 24 小时前的历史数据

如果历史平均利用率超出资源阈值，Workload Balancing 将确定应提出优化建议。

3. Workload Balancing 使用指标加权来确定应该首先优化的主机。Workload Balancing 将首先尝试解决分配了最高权重的资源。有关指标加权的详细信息，请参阅调整指标加权。
4. Workload Balancing 确定哪些主机可以支持要从主机中迁出的 VM。

Workload Balancing 在进行此项决定时，会计算在主机上放置不同 VM 组合时将对资源利用率产生的预期影响。（Workload Balancing 将采用数学上称为排列的方法执行这些计算。）

为此，Workload Balancing 将创建一个指标或分数来预测将 VM 迁移到主机所产生的影响。该分数代表主机作为更多 VM 宿主的适合程度。

要对主机性能进行评分，Workload Balancing 将结合使用以下指标：

- 主机的当前指标
  - 过去 30 分钟的主机指标
  - 24 小时前的主机指标
  - VM 的指标。
5. 对主机和 VM 评分后，WLB 将尝试使用 VM 的不同组合来构建主机情况的虚拟模型。WLB 使用这些模型来确定用于放置 VM 的最佳主机。

在“最高性能”模式下，Workload Balancing 将使用指标加权来确定首先优化哪些主机以及首先迁移这些主机上的哪些 VM。Workload Balancing 基于指标加权来构建其模型。例如，如果为 CPU 使用率分配了最高的重要性，Workload Balancing 将对主机和 VM 进行排序以根据以下标准进行优化：

- 首先，CPU 使用率对哪些主机的影响最大（即，以最接近 CPU 使用率的高阈值运行）
- 哪些 VM 拥有的 CPU 使用率最高（或以最接近其高阈值运行）。

6. Workload Balancing 继续进行优化计算。它将这些主机视为潜在的优化候选主机，并将这些 VM 视为迁移候选 VM，直至 VM 主机上的预计资源利用率降至高阈值以下。“预计资源利用率”是指 Workload Balancing 预测的、主机在由 Workload Balancing 从其添加或删除 VM 后将达到的资源利用率。

#### “最大密度”模式下的合并过程

WLB 确定是否根据以下标准提出建议：是否可以将 VM 迁移到某个主机上且仍在低于临界阈值以下时运行该主机。

1. 当资源利用率降至其低阈值以下时，Workload Balancing 开始计算可能的合并方案。
2. 当 WLB 检测到可以合并主机上的 VM 的方法时，将评估目标主机是否适合成为 VM 的宿主。
3. 与“最高性能”模式类似，Workload Balancing 将对主机进行评分，以确定主机作为新 VM 宿主的适合程度。

在 WLB 提出整合更少主机上的 VM 的建议之前，它会检查将 VM 重新定位到这些主机后，这些主机上的资源利用率是否低于临界阈值。

注意：

Workload Balancing 在提出合并建议时，不考虑指标加权。只有在确保主机性能时才考虑指标加权。

4. 对主机和 VM 评分后，WLB 将尝试使用 VM 的不同组合来构建主机情况的虚拟模型。它使用这些模型来确定用于放置 VM 的最佳主机。
5. WLB 会计算将 VM 添加到主机所产生的影响，直至其预测到添加其他 VM 会导致主机资源超出临界阈值。
6. Workload Balancing 在提出建议时，始终建议首先填充池主服务器，因为该主机不能关闭。但 Workload Balancing 会对池主服务器应用一个缓冲值，以防该服务器被过度分配。
7. WLB 继续建议将 VM 迁移到主机上，直至所有主机在迁移 VM 后都不超出临界阈值。

#### 更改临界阈值

可能需要通过更改临界阈值来控制触发优化建议的时机。本节提供关于以下内容的指导：

- 如何在池中的主机上修改默认临界阈值
- 为临界阈值设置的值如何更改高、中和低阈值。

Workload Balancing 将根据主机上资源的历史平均利用率是否超出阈值范围来决定是否提出建议。如果在“最高性能”模式下超出高阈值，或者在“最大密度”模式下超出低阈值和临界阈值，将触发 Workload Balancing 建议。有关详细信息，请参阅优化和合并过程。为某个资源指定某个新“临界”阈值后，Workload Balancing 将相对于该新临界阈值重置资源的其他阈值。（为了简化用户界面，通过 XenCenter 只能更改临界阈值。）

下表显示了 Workload Balancing 阈值的默认值：

| 指标      | 严重  | 高     | 中   | 低     |
|---------|-----|-------|-----|-------|
| CPU 使用率 | 90% | 76.5% | 45% | 22.5% |

| 指标   | 严重      | 高          | 中         | 低         |
|------|---------|------------|-----------|-----------|
| 可用内存 | 51 MB   | 63.75 MB   | 510 MB    | 1020 MB   |
| 网络读取 | 25 MB/秒 | 21.25 MB/秒 | 12.5 MB/秒 | 6.25 MB/秒 |
| 网络写入 | 25 MB/秒 | 21.25 MB/秒 | 12.5 MB/秒 | 6.25 MB/秒 |
| 磁盘读取 | 25 MB/秒 | 21.25 MB/秒 | 12.5 MB/秒 | 6.25 MB/秒 |
| 磁盘写入 | 25 MB/秒 | 21.25 MB/秒 | 12.5 MB/秒 | 6.25 MB/秒 |

在计算除内存以外的所有指标的数值时，Workload Balancing 会将临界阈值的新值与以下因数相乘：

- 高阈值因数：0.85
- 中阈值因数：0.50
- 低阈值因数：0.25

例如如果您将 CPU 使用率的临界阈值提高至 95%，WLB 会将高、中和低阈值分别重置为 80.75%、47.5% 和 23.75%。

在计算可用内存的阈值时，Workload Balancing 将临界阈值与以下因数相乘：

- 高阈值因数：1.25
- 中阈值因数：10.0
- 低阈值因数：20.0

要对特定阈值执行此计算，请将阈值因数与您为该资源输入的临界阈值相乘：

高、中或低阈值 = 临界阈值 \* 阈值因数

例如，如果您将“网络读取”的临界阈值更改为 40 MB/秒，以计算其低阈值，可以用 40 乘以 0.25，得出 10 MB/秒。要得到中阈值，可以用 40 乘以 0.50，依此类推。

尽管临界阈值可以触发许多优化建议，但其他阈值也可以触发优化建议，如下所述：

- 高阈值。
  - 最高性能。超出高阈值会触发将 VM 重定位到资源利用率较低的主机的优化建议。
  - 最大密度。如果将 VM 移动到主机会导致主机资源利用率超出高阈值，Workload Balancing 将不会提出将该 VM 放置到该主机的建议。
- 低阈值。
  - 最高性能。Workload Balancing 不会因低阈值而触发建议。
  - 最大密度。当某个指标值降低到低阈值以下时，WLB 就会确定主机利用率偏低，并提出将 VM 合并到更少主机上的优化建议。Workload Balancing 将持续提出将 VM 移动到某个主机的建议，直至该主机某个资源的指标值达到其高阈值为止。

但是，重新定位 VM 后，该 VM 的新主机上的资源利用率将超出临界阈值。在这种情况下，WLB 将临时使用与“最大性能”负载平衡算法类似的算法来为 VM 查找新主机。Workload Balancing 将持续使用此算法来提出移动 VM 的建议，直到池中各主机上的资源利用率都降至高阈值以下。

#### 更改临界阈值

1. 在 XenCenter 的“基础结构”窗格中，选择 XenCenter > `your-resource-pool`。
2. 在“属性”窗格中，单击“WLB”选项卡。
3. 在“WLB”选项卡中，单击“设置”。
4. 在左侧窗格中，选择“临界阈值”。这些临界阈值用于评估主机资源利用率。
5. 在临界阈值页面的临界阈值框中，键入一个或多个新值。这些值代表主机的资源利用率。

在提供 VM 放置和池优化建议时，Workload Balancing 会使用这些阈值。Workload Balancing 会努力将主机的资源利用率保持在设定的临界阈值以下。

#### 调整指标加权

确定首先处理的主机和 VM 时，Workload Balancing 对指标加权的使用方式因优化模式而异：“最大密度”或“最高性能”。

Workload Balancing 处理优化建议时，将创建优化顺序。确定此顺序时，Workload Balancing 将最重要资源拥有最高指标值的主机排在最优先处理的位置，资源的重要性通过指标加权页面排定。

通常，指标加权在池处于“最高性能”模式时使用。但是，当 Workload Balancing 处于“最大密度”模式时，如果某个资源超出其临界阈值，也会使用指标加权。

#### “最高性能”模式

在性能最大化模式下，Workload Balancing 使用指标加权确定：(a) 首先处理哪些主机的性能；(b) 建议首先迁移哪些 VM。

例如，如果网络写入量是 WLB 的最重要资源，WLB 将首先针对具有最高每秒网络写入量的主机提出优化建议。要使网络写入量称为最重要的资源，请将指标加权滑块移到右侧并将所有其他滑块移到中间。

如果将所有资源配置为同等重要，则 Workload Balancing 将首先解决 CPU 使用率问题，然后解决内存问题，因为这些资源通常是最受限制的资源。要使所有资源同等重要，请将所有资源的指标加权滑块设置为处于相同的位置。

#### “最大密度”模式

在“最大密度”模式下，Workload Balancing 仅在主机达到临界阈值时使用指标加权。此时，Workload Balancing 应用的算法与“最高性能”所采用的算法类似，直至没有主机超出临界阈值为止。使用此算法时，Workload Balancing 按照与“最高性能”模式相同的方式，使用指标加权来确定优化顺序。

如果两个或多个主机的资源超出其临界阈值，Workload Balancing 将验证您为每个资源设置的重要性。它使用此重要性来确定首先优化哪些主机以及在该主机上首先重新定位哪些 VM。

例如，池中包含主机 A 和主机 B，二者分别处于以下状态：

- 主机 A 上的 CPU 使用率超出了其临界阈值，而 CPU 使用率的指标加权设置在最右端：更重要。
- 主机 B 上的内存利用率超出了其临界阈值，而内存利用率的指标加权设置在最左端：不太重要。

Workload Balancing 将提出首先优化主机 A 的建议，因为该主机上达到临界阈值的资源是权重值最高的资源。在 Workload Balancing 确定必须处理主机 A 的性能问题后，Workload Balancing 将开始提出在该主机上放置 VM 的建议。先以具有最高 CPU 使用率的 VM 开始，因为 CPU 使用率是具有最高权重的资源。

Workload Balancing 在提出优化主机 A 的建议后，将提出主机 B 的优化建议。当它为主机 B 上的 VM 提出放置建议时，将首先处理 CPU 使用率，因为 CPU 使用率具有最高权重。

如果有其他需要优化的主机，Workload Balancing 将处理 CPU 使用率排在第三位的主机的性能问题。

默认情况下，所有指标加权设置在滑块的最远点（更重要）。

**注意：**

指标加权是相对值。如果将所有指标设置为相同级别，那么即使该级别为“不太重要”，它们的权重也是相同的。比起为每个指标设置的实际权重，各指标之间的关系更重要。

### 编辑指标加权系数

1. 停止
2. 在 XenCenter 的“基础结构”窗格中，选择 XenCenter > `your-resource-pool`。
3. 单击“WLB”选项卡，然后单击“设置”。
4. 在左侧窗格中，选择“指标加权”。
5. 在“指标加权”页面中，可以根据需要调整各资源旁的滑块。

如果将滑块移向“不太重要”，表明在该池中，确保 VM 始终具有最高数量的可用该资源不太重要。

### 从建议中排除主机

配置 Workload Balancing 时，可以指定从 Workload Balancing 优化和放置建议（包括“启动”放置建议）中排除特定的物理主机。

可能需从建议中排除主机的情况如下：

- 要在“最大密度”模式下运行池、合并及关闭主机，但希望某些特定主机不实施该行为。
- 拥有两个必须始终在同一主机上运行的 VM 工作负载。例如，如果 VM 具有互补应用程序或工作负载。
- 不希望移动某些工作负载（例如，域控制器或数据库服务器）。

- 需要对主机执行维护，而不希望将 VM 放置在该主机上。
- 工作负载性能的重要性非常高，因此专用硬件的成本无关紧要。
- 特定主机上正在运行高优先级的工作负载 (VM)，而您并不希望使用高可用性功能来为这些 VM 确定优先级。
- 主机中的硬件对于池中的其他工作负载并不是最优选择。

无论指定固定优化模式还是计划优化模式，即使切换优化模式，已排除的主机仍会被排除。因此，如果您只希望阻止 Workload Balancing 自动关闭某个主机，则应考虑不为该主机启用（或取消选择）电源管理功能。有关详细信息，请参阅自动优化及管理电源。

从建议中排除某个主机时，意味着告诉 Workload Balancing 完全不管理该主机。此配置意味着，Workload Balancing 将不就排除的主机提出任何优化建议。相反，当您选择不让某个主机参与电源管理时，WLB 仍会管理该主机，但不会就该主机提出电源管理建议。

### 从 **Workload Balancing** 排除主机

使用以下步骤从池（Workload Balancing 通过电源管理、主机评估、放置和优化建议对该池进行管理）中排除主机。

1. 在 XenCenter 的“资源”窗口中，选择 XenCenter > [your-resource-pool](#)。
2. 在“属性”窗格中，单击“WLB”选项卡。
3. 在“WLB”选项卡中，单击“设置”。
4. 在左侧窗格中，选择“排除的主机”。
5. 在“排除的主机”页面中，选择您不希望 WLB 提出备用放置和优化建议的主机。

### 控制自动化建议

Workload Balancing 提供了某些高级设置，可用来控制 Workload Balancing 应用自动化建议的方式。这些设置显示在“Workload Balancing 配置”对话框的“高级”页面上。

在 XenCenter 的“资源”窗口中，选择 XenCenter > [your-resource-pool](#)。

在“属性”窗格中，单击“WLB”选项卡。

在“WLB”选项卡中，单击“设置”。

在左侧窗格中，选择“高级”。

### 设置保守或主动的自动化建议

在自动化模式下运行时，提供优化和合并建议的频率以及自动应用这些建议的时间由多种因素决定，包括：

- 指定 Workload Balancing 从 VM 迁移完毕到提出下一个建议之间的等待时间
- Workload Balancing 在自动应用某个建议之前必须达到的建议数

- 在自动应用优化前建议必须达到的严重级别
- Workload Balancing 在自动应用建议之前需要达到的建议一致性级别（建议移动的 VM，目标主机）

重要：

通常，只能在以下情况下调整设置：

- Citrix 技术支持人员可提供指导
- 在启用 Workload balancing 的情况下，已对池的行为进行了有效地观察和测试

未正确配置这些设置可能会导致 Workload Balancing 不提出任何建议。

### VM 迁移时间间隔

在 WLB 能够对最后一次移动的 VM 提出其他建议之前，可以指定在最后一次移动该 VM 后 WLB 等待的分钟数。

建议间隔用于防止 Workload Balancing 由于不实的原因（例如，利用率短暂达到峰值）生成建议。

如果配置了“自动化”功能，则修改建议间隔时务必要非常小心。如果出现导致持续、反复出现尖峰的问题，则提高频率（即设置更低的间隔值）会产生大量建议，从而发生多次重新定位。

注意：

Workload Balancing 需要等待一段时间才会考虑将最新重新平衡的主机纳入针对启动放置、恢复及维护模式的建议，而设置建议时间间隔不会对这段等待时间产生影响。

### 建议计数

Workload Balancing 每两分钟进行一次检查，判断能否为正在监视的池生成建议。启用“自动化”功能时，可以指定 Workload Balancing 必须提供多少次一致的建议才能自动应用该建议。为此，需要配置一项称为“建议计数”的设置。“建议计数”和“优化入侵”设置用于调整在环境中自动应用程序建议的方式。

如主动性部分中所述，Workload Balancing 使用建议的相似性进行以下检查：

1. 是否确实需要提出建议
2. 目标主机是否能够长时间保持足够稳定的性能以接受重新定位的 VM（无需不久后再次将其从主机中迁出）

Workload Balancing 使用“建议计数”值来确定在 Workload Balancing 自动应用建议之前必须重复提出该建议的次数。

Workload Balancing 按如下所述使用此设置：

1. 每次 Workload Balancing 生成满足一致性要求（由“优化入侵”设置指定）的建议时，Workload Balancing 都会将“建议计数”值递增。如果该建议不满足一致性要求，Workload Balancing 可能会将“建议计数”重置为零，具体取决于优化入侵中所述的因素。
2. 当 WLB 生成的一致建议的数目足以满足“建议计数”值（在“建议”文本框中指定）时，它将自动应用建议。

如果您选择修改此设置，要设置的值将因环境而异。请考虑以下情形：

- 如果所在环境中的主机负载和活动急速增加，可能需要增大“建议计数”的值。Workload Balancing 每两分钟生成一次建议。举例来说，如果将此间隔设置为 **3**，则在六分钟后，Workload Balancing 将自动应用建议。
- 如果所在环境中的主机负载和活动逐渐增加，则可能需要减小“建议计数”的值。

在 Workload Balancing 重新定位 VM 时，接受建议会占用系统资源，并对性能产生影响。增大“建议计数”会增加 Workload Balancing 应用建议之前必须提出的匹配建议的数量。此设置鼓励 Workload Balancing 应用更保守、更稳妥的建议，并且可以降低虚假 VM 移动的可能性。默认情况下，“建议计数”将设置为保守值。

由于调整此设置可能会对您的环境产生潜在影响，因此更改时务必极其小心。最好在经过测试并反复更改值后或在 Citrix 技术支持人员的指导下进行这些调整。

### 建议严重性

所有优化建议都包含一个严重性级别（严重、高、中、低），用于指示建议的重要程度。Workload Balancing 根据以下因素的组合进行该评级：

- 设置的配置选项，例如阈值和指标调整
- 可用于工作负载的资源
- 资源使用情况历史记录。

建议的严重性级别显示在“WLB”选项卡的“优化建议”窗格中。

如果将 WLB 配置为自动应用建议，则可以在 Workload Balancing 自动应用建议之前，设置与该建议相关联的最低严重性级别。

### 优化入侵

在自动化模式下运行时，为了提供更多的保证，Workload Balancing 针对自动接受优化建议设定了一致性条件。这有助于避免因尖峰和异常而移动 VM。在自动化模式下，Workload Balancing 不会接受所生成的第一个建议，而是一直等到主机或 VM 持续表现一致行为时，Workload Balancing 才自动应用建议。“持续表现一致行为”包括某个主机是否持续触发建议，以及该主机上的相同 VM 是否持续触发建议等因素。

Workload Balancing 通过使用一致性条件以及规定同一个建议提出次数的条件来判断行为是否一致。您可以使用“优化入侵”设置来配置希望 Workload Balancing 应用一致性条件的严格程度。

我们设计“优化入侵”设置主要是为了进行演示。但是，您可以使用此设置来控制在 Workload Balancing 应用优化建议之前环境中需要达到的稳定程度。默认情况下配置为最稳定的设置（低入侵）。在此上下文中，术语“稳定”是指建议的更改具有持续的相似性，如本节中所述。在大多数环境中，不需要具有主动性。因此，“低”是默认设置。

Workload Balancing 最多使用四个条件来确定一致性。必须满足的条件数因您在优化入侵设置中设定的级别而异。级别越低（例如“低”或“中”），Workload Balancing 接受建议的入侵就越低。换言之，当入侵设置为“低”时，Workload Balancing 对于满足一致性条件的要求更加严格（或者说更具限制性或更不主动）。

例如，如果主动性级别设置为“低”，则在自动应用建议之前，每个“低”值条件都必须符合由“建议计数”值指定的次数。

如果将“建议计数”设置为 **3**，则 Workload Balancing 将一直等到满足下面针对“低”主动性所列的所有条件并且连续三次重复提出建议时，才会应用该建议。此设置有助于确保 VM 确实需要移动，而且推荐的目标主机在较长时间内具

有稳定的资源利用率。这样可以降低最新移动的 VM 因移动后主机性能变化而又从主机移出的可能性。默认情况下，此项设置为保守设置（“低”）以促进稳定性。

我们建议您不要通过增加“优化入侵”设置值来提高主机优化频率。如果您觉得您的主机优化速度不够快或频率不够高，请尝试调整临界阈值。根据池运行状况报告比较各个阈值。

与不同主动性级别相关联的一致性条件如下：

低：

- 后续建议中的所有 VM 都必须相同（通过匹配每个建议中的 UUID 来判断）
- 后续建议中的所有目标主机都必须相同
- 初始建议后面紧跟的建议必须匹配，否则“建议计数”将还原为 1

中：

- 后续建议中的所有 VM 都必须来自同一个主机；但可以不同于首个建议中的 VM。
- 后续建议中的所有目标主机都必须相同
- 初始建议后面紧跟的两个建议之一必须匹配，否则“建议计数”将还原为 1

高：

- 建议中的所有 VM 都必须来自同一个主机。但是，建议不必立即彼此遵循。
- 在每个建议中，Workload Balancing 建议移动 VM 的主机必须相同
- 当首个建议紧跟的两个建议不匹配时，“建议计数”不会还原为 1

示例

下面的示例说明 Workload Balancing 如何使用“优化入侵”设置和“建议计数”来确定是否自动接受建议。

第一列代表建议编号。第二列“放置建议”代表 Workload Balancing 在提出优化建议时所提出的放置建议：每个建议包含三个 VM 放置（移动）建议。第三、四、五列代表“优化入侵”设置对各组放置建议的影响。行表示组，例如建议 1。主动性列中的数字代表使用该“优化主动性”设置时连续建议的次数。例如，建议 2 中级主动性列中的值为 1，表示使用该“优化入侵”设置时的建议未达到一致性要求。计数器已重置为 1。

在下表中，当“优化入侵”设置设为“高”时，“建议计数”在建议 1、2 和 3 之后继续递增。即使每个建议中针对新放置所建议的 VM 并不相同，也会进行此递增。Workload Balancing 将应用建议 3 的放置建议，因为它认为就这三个连续的建议而言，该主机具有相同的行为。

相反，当设置为“低”主动性时，对于前四个建议，连续建议计数并不增加。每个建议都会将“建议计数”重置为 1，因为放置建议中的 VM 不同。直到建议 5 中提出相同建议时，“建议计数”才开始增加。最后，Workload Balancing 将在提出三次相同的放置建议后自动应用建议 6 中所提出的建议。

建议 1：

- 将 VM1 从主机 A 移动到主机 B

- 将 VM3 从主机 A 移动到主机 B
- 将 VM5 从主机 A 移动到主机 C

高主动性时的建议计数：1

中主动性时的建议计数：1

低主动性时的建议计数：1

**建议 2:**

- 将 VM1 从主机 A 移动到主机 B
- 将 VM3 从主机 A 移动到主机 C
- 将 VM7 从主机 A 移动到主机 C

高主动性时的建议计数：2

中主动性时的建议计数：1

低主动性时的建议计数：1

**建议 3:**

- 将 VM1 从主机 A 移动到主机 B
- 将 VM3 从主机 A 移动到主机 C
- 将 VM5 从主机 A 移动到主机 C

高主动性时的建议计数：3（应用）

中主动性时的建议计数：1

低主动性时的建议计数：1

**建议 4:**

- 将 VM1 从主机 A 移动到主机 B
- 将 VM3 从主机 A 移动到主机 B
- 将 VM5 从主机 A 移动到主机 C

中主动性时的建议计数：2

低主动性时的建议计数：1

**建议 5:**

- 将 VM1 从主机 A 移动到主机 B
- 将 VM3 从主机 A 移动到主机 B
- 将 VM5 从主机 A 移动到主机 C

中主动性时的建议计数：3（应用）

低主动性时的建议计数：2

**建议 6:**

- 将 VM1 从主机 A 移动到主机 B
- 将 VM3 从主机 A 移动到主机 B
- 将 VM5 从主机 A 移动到主机 C

低主动性时的建议计数：3（应用）

#### 配置 VM 建议间隔

1. 在 XenCenter 的“资源”窗口中，选择 XenCenter > your-pool。
2. 在“属性”窗格中，单击“WLB”选项卡。
3. 在“WLB”选项卡中，单击“设置”。
4. 在左侧窗格中，单击“高级”。
5. 在“VM Recommendation Interval”（VM 建议间隔）部分中，执行以下一项或多项操作：
  - 在“分钟”框中，键入 Workload Balancing 就刚刚重新平衡的主机提出其他优化建议之前需要等待的分钟数。
  - 在“建议”框中，键入希望 Workload Balancing 在自动应用优化建议之前提出的建议的数量。
  - 选择自动应用优化之前的最低严重性级别。
  - 修改 Workload Balancing 在自动化模式下运行时应用优化建议的主动性。如果增加主动性级别，则会在自动应用建议之前，减少对这些建议一致程度的约束。“优化入侵”设置是对“建议计数”设置（即“建议”框）的直接补充。

注意：

如果在“建议”设置中键入值 1，则“优化入侵”设置无效。

#### 修改池审核追踪精度设置

按照此过程修改精度设置：

1. 在基础结构视图中选择池，单击 WLB 选项卡，然后单击设置。
2. 在左侧窗格中，单击高级。
3. 在“高级”页面上，单击池审核追踪报告精度列表，然后从列表中选择一个选项。

重要：

根据您的审核日志要求选择精度。例如，如果您将审核日志报告精度设置为“最低”，则报告只能捕获有限数量的特定用户和对象类型的数据。如果将精度设置为中，该报告将提供用户友好的审核日志报告。如果您选择将精度设置为“最大”，则报告将包含有关审核日志报告的详细信息。将审核日志报告设置为最高会使 Workload Balancing 服务器使用更多磁盘空间和内存。

4. 要确认更改，请单击“确定”。

在 **XenCenter** 中查看基于对象的审核跟踪报告

请按照以下过程进行操作，运行并查看基于选定对象的池审核跟踪报告：

1. 设置“池审核跟踪精度”设置后，单击报告。此时将显示工作负载报告页面。
2. 在左侧窗格中选择“池审核追踪”。
3. 可以通过从对象列表中进行选择来运行并查看基于特定对象的报告。例如，从列表中选择主机将获取仅基于主机的报告。

## 管理 **Workload Balancing**

本节提供关于以下主题的信息：

- 如何将池重新配置为使用不同的 Workload Balancing 虚拟设备
- 如何将池与 Workload Balancing 断开连接或暂时停止 Workload Balancing
- 数据库整理
- 如何更改配置选项

注意：

Workload Balancing 适用于 Citrix Hypervisor Premium Edition 客户或者通过 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。有关 Citrix Hypervisor 许可的详细信息，请参阅[许可](#)。要升级或购买 Citrix Hypervisor 许可证，请访问 [Citrix Web 站点](#)。

## 管理和维护 **Workload Balancing**

Workload Balancing 运行一段时间后，您可能需要执行一些例行任务，使 Workload Balancing 保持以最佳状态运行。更改环境（例如不同的 IP 地址或凭据）、升级硬件或执行例行维护工作后，可能需要执行这些任务。

您可能会对 Workload Balancing 执行一些管理任务，这些任务包括：

- 将池连接或重新连接到 Workload Balancing 虚拟设备
- 将池重新配置为使用其他 Workload Balancing 虚拟设备
- 重命名 Workload Balancing 用户帐户
- 将 Workload Balancing 虚拟设备与池断开连接
- 删除 Workload Balancing 虚拟设备
- 了解 Workload Balancing 需要的基于角色的访问控制权限

对于 Workload Balancing，您可以通过名为 wlb.conf 的配置文件调整其在某些方面的行为。

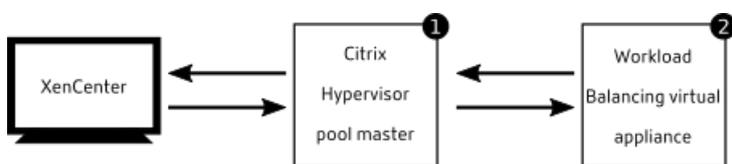
本节还将为希望通过其他方式管理 Workload Balancing 数据库的用户介绍一些数据库管理任务。

### 连接 **Workload Balancing** 虚拟设备

配置 Workload Balancing 之后，使用 CLI 或 XenCenter 将要管理的池连接到 Workload Balancing 虚拟设备。同样，您有时可能还需要重新连接同一个虚拟设备。

要完成后续的 XenCenter 过程，需要以下信息：

- Workload Balancing 虚拟设备的主机名称（或 IP 地址）和端口。
- 希望 Workload Balancing 监视的资源池所使用的凭据。
- 在 Workload Balancing 虚拟设备上创建的帐户的凭据。此帐户通常称为“Workload Balancing 用户帐户”。Citrix Hypervisor 使用此帐户与 Workload Balancing 进行通信。此帐户是您在 Workload Balancing 配置期间在 Workload Balancing 虚拟设备上创建的帐户。



要指定在连接到 Workload Balancing 虚拟设备时要使用的 Workload Balancing 虚拟设备的主机名，请先将其主机名和 IP 地址添加到 DNS 服务器。

如果要配置某个证书颁发机构颁发的证书，我们建议指定未过期的 FQDN 或 IP 地址。

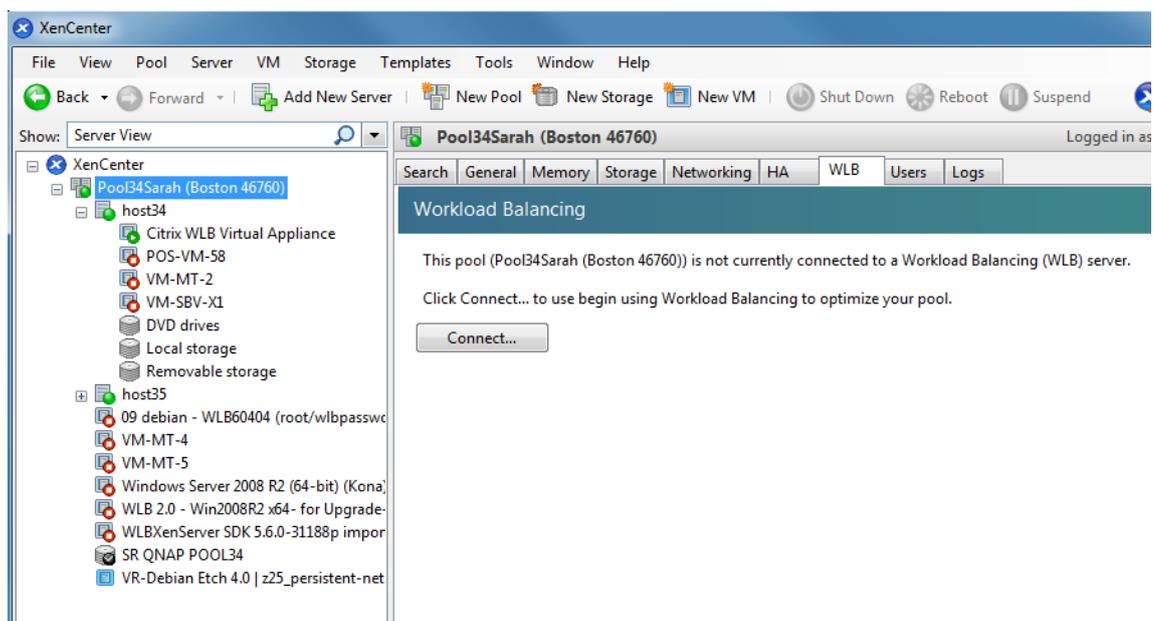
首次连接 Workload Balancing 时，它将使用默认的阈值和设置来平衡工作负载。默认情况下自动功能（例如自动优化模式、电源管理和自动化）处于禁用状态。

#### 注意：

Workload Balancing 适用于 Citrix Hypervisor Premium Edition 客户或者通过 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。有关 Citrix Hypervisor 许可的详细信息，请参阅[许可](#)。要升级或购买 Citrix Hypervisor 许可证，请访问 [Citrix Web 站点](#)。

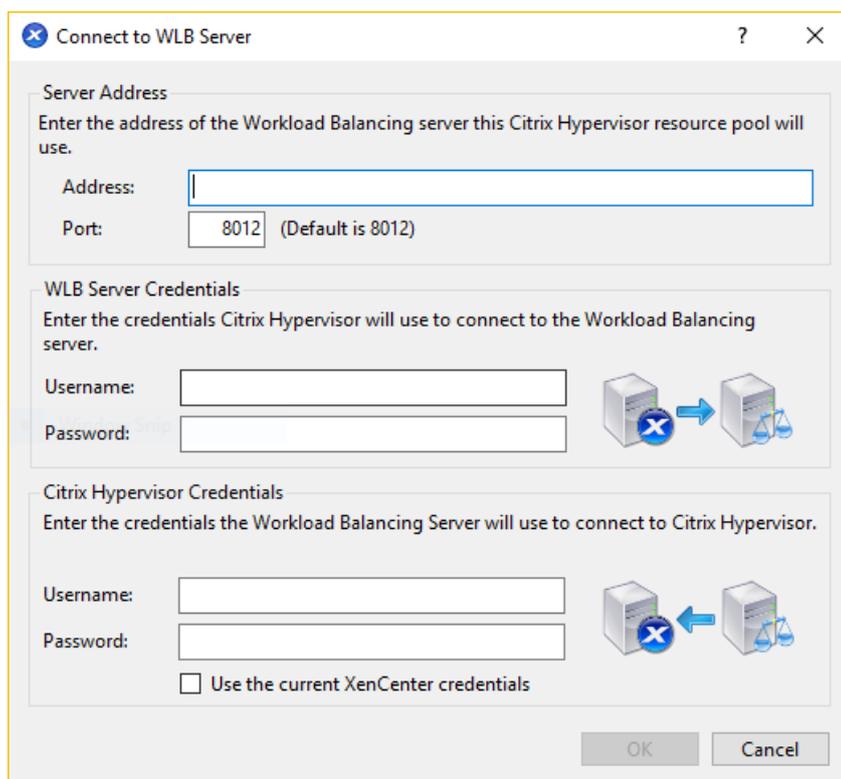
### 将池连接到 **Workload Balancing** 虚拟设备

1. 在 XenCenter 的“资源”窗口中，选择 XenCenter > `your-resource-pool`。
2. 在“属性”窗格中，单击“WLB”选项卡。  
“WLB”选项卡将显示“连接”按钮。



3. 在“WLB”选项卡中，单击“连接”。

此时将显示“连接 WLB 服务器”对话框。



4. 在“服务器地址”部分中，输入以下信息：

- a) 在“地址”框中，键入 Workload Balancing 设备的 IP 地址或 FQDN (例如, `your-WLB-appliance-computername.yourdomain.net`)。

提示：

有关详细信息，请参阅获取 WLB 虚拟设备的 IP 地址。

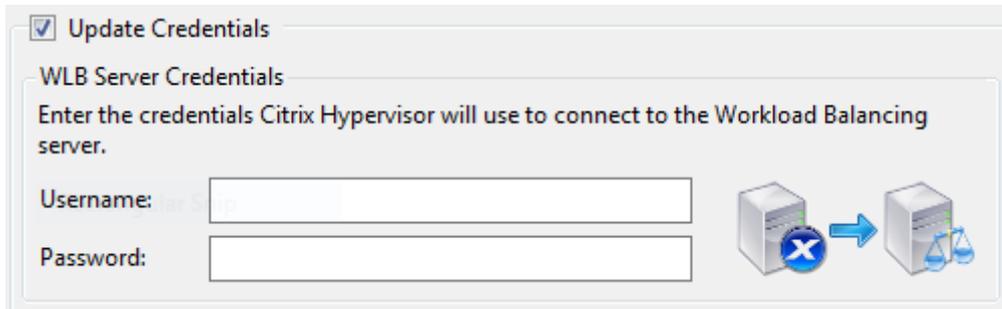
- b) 在“端口”框中输入端口号。Citrix Hypervisor 使用此端口与 Workload Balancing 进行通信。

默认情况下，Citrix Hypervisor 通过端口 8012 连接 Workload Balancing（具体而言，是指 Web 服务主机服务）。如果在 Workload Balancing 配置期间更改了端口号，则必须在此处输入该端口号。

注意：

除非您在 Workload Balancing 配置期间更改了默认端口号，否则将使用该端口号。在 Workload Balancing 配置期间指定的端口号、在任何防火墙中指定的端口号以及在“连接 WLB 服务器”对话框中指定的端口号都必须一致。

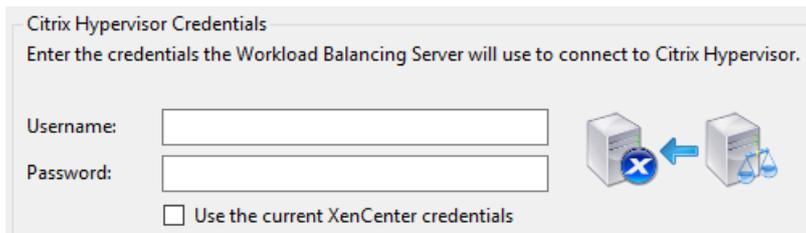
5. 在“WLB 服务器凭据”部分，输入池在连接到 Workload Balancing 虚拟设备时要使用的用户名（例如 `wlbuser`）和密码。



The screenshot shows a dialog box titled "Update Credentials". It has a checked checkbox at the top left. Below it is a section titled "WLB Server Credentials" with the instruction "Enter the credentials Citrix Hypervisor will use to connect to the Workload Balancing server." There are two input fields: "Username:" and "Password:". To the right of these fields is an icon showing two server racks connected by a blue arrow, with a blue 'X' over the left server.

这些凭据必须是在 Workload Balancing 配置期间创建的帐户。默认情况下，此帐户的用户名为 `wlbuser`。

6. 在“Citrix Hypervisor 凭据”部分，输入所配置池的用户名和密码。Workload Balancing 将使用这些凭据连接到池中的 Citrix Hypervisor 服务器。



The screenshot shows a dialog box titled "Citrix Hypervisor Credentials" with the instruction "Enter the credentials the Workload Balancing Server will use to connect to Citrix Hypervisor." There are two input fields: "Username:" and "Password:". Below these fields is a checkbox labeled "Use the current XenCenter credentials". To the right of the fields is an icon showing two server racks connected by a blue arrow, with a blue 'X' over the left server.

要使用当前登录 Citrix Hypervisor 所使用的凭据，请选中“使用当前 XenCenter 凭据”复选框。如果您已使用访问控制功能 (RBAC) 为此帐户分配了角色，应确保该角色有足够的权限来配置 Workload Balancing。有关详细信息，请参阅 Workload Balancing 访问控制权限。

7. 在将池连接到 Workload Balancing 虚拟设备之后，Workload Balancing 会自动开始以默认的优化设置监视池。如果您希望修改这些设置或者更改为特定资源指定的优先级，请在执行这些操作之前等到 XenCenter 日志显示已完成发现过程。有关详细信息，请参阅更改 Workload Balancing 设置。

获取 **WLB** 虚拟设备的 IP 地址

1. 在 XenCenter 的“资源”窗格中选择 WLB 虚拟设备，然后选择“控制台”选项卡。
2. 登录该设备。输入在导入该设备时创建的 VM 用户名（通常为“root”）及 root 用户密码。
3. 在提示符处输入以下命令：

```
1 ifconfig
```

### Workload Balancing 访问控制权限

在环境中实施基于角色的访问控制 (RBAC) 时，所有用户角色均可显示“WLB”选项卡。但是，并非所有角色都可以执行所有操作。下表列出了管理员要使用 Workload Balancing 功能至少要具有的角色：

| 任务                      | 至少要具有的角色 |
|-------------------------|----------|
| 配置、初始化、启用、禁用 WLB        | 池操作员     |
| 应用 WLB 优化建议（在“WLB”选项卡中） | 池操作员     |
| 修改 WLB 报告订阅             | 池操作员     |
| 接受 WLB 放置建议（“星级”建议）     | VM 超级管理员 |
| 生成 WLB 报告，包括池审核追踪报告     | 只读       |
| 显示 WLB 配置               | 只读       |

### 权限的定义

下表提供了关于权限的更多详细信息。

| 权限                      | 允许被授权人执行的操作                               |
|-------------------------|-------------------------------------------|
| 配置、初始化、启用、禁用 WLB        | 配置 WLB                                    |
|                         | 初始化 WLB 和更改 WLB 服务器                       |
|                         | 启用 WLB                                    |
|                         | 禁用 WLB                                    |
| 应用 WLB 优化建议（在“WLB”选项卡中） | 应用“WLB”选项卡中显示的所有优化建议                      |
| 修改 WLB 报告订阅             | 更改生成的 WLB 报告或其接收者                         |
| 接受 WLB 放置建议（“星级”建议）     | 选择其中一种服务器 Workload Balancing 放置建议（“星级”建议） |
| 生成 WLB 报告，包括池审核追踪报告     | 查看和运行 WLB 报告，包括“池审核追踪”报告                  |

|           |                         |
|-----------|-------------------------|
| 权限        | 允许被授权人执行的操作             |
| 显示 WLB 配置 | 查看如“WLB”选项卡上显示的池 WLB 设置 |

如果用户尝试使用 Workload Balancing，但该用户没有足够的权限，系统会显示一个角色提升对话框。有关 RBAC 的详细信息，请参阅[基于角色的访问控制](#)。

### 确定 Workload Balancing 虚拟设备的状态

运行 `service workloadbalancing status` 命令，如 Workload Balancing 命令中所述。

### 将池重新配置为使用其他 WLB 设备

可以将资源池重新配置为使用其他 Workload Balancing 虚拟设备。

但是，为了防止旧 Workload Balancing 虚拟设备在某个池中运行，请确保先断开该池与旧 Workload Balancing 虚拟设备的连接。

将池与原 Workload Balancing 虚拟设备断开连接后，可以通过指定新 Workload Balancing 虚拟设备的名称来连接该池。针对要连接其他 Workload Balancing 虚拟设备的池执行此过程中的后续步骤。

要使用其他 Workload Balancing 虚拟设备，请执行以下操作：

1. 从“池”菜单中，选择“断开 Workload Balancing 服务器连接”，然后在出现提示时单击“断开连接”。
2. 在“WLB”选项卡中，单击“连接”。此时将显示连接 WLB 服务器对话框。
3. 在“地址”框中，键入新 Workload Balancing 服务器的 IP 地址或 FQDN。
4. 在“WLB 服务器凭据”部分中，输入 Citrix Hypervisor 池在连接到 Workload Balancing 虚拟设备时要使用的用户名和密码。

这些凭据必须是在 Workload Balancing 配置期间为新虚拟设备创建的帐户。默认情况下，此帐户的用户名为 `wlbuser`。

5. 在“Citrix Hypervisor 凭据”部分中，输入您正在配置的池的用户名和密码（通常是池主服务器的密码）。Workload Balancing 将使用这些凭据连接池中的主机。

要使用当前登录 Citrix Hypervisor 所使用的凭据，请选中“使用当前 XenCenter 凭据”复选框。如果您已使用访问控制功能 (RBAC) 为此帐户分配了角色，应确保该角色有足够的权限来配置 Workload Balancing。有关详细信息，请参阅 Workload Balancing 访问控制权限。

### 更新 **Workload Balancing** 凭据

完成初始配置后，如果需要更新 Citrix Hypervisor 与 Workload Balancing 设备用来通信的凭据，请按照以下过程操作：

1. 通过在“WLB”选项卡中单击“暂停”，来暂停 Workload Balancing。
2. 通过运行 `wlbconfig` 命令更改 WLB 凭据。有关详细信息，请参阅 Workload Balancing 命令。
3. 重新启用 Workload Balancing 并指定新凭据。
4. 完成全部进度之后，单击连接。

此时将显示“连接 WLB 服务器”对话框。

5. 单击更新凭据。
6. 在“服务器地址”部分，根据需要修改以下内容：
  - 在地址框中，键入 Workload Balancing 设备的 IP 地址或 FQDN。
  - (可选) 如果在 Workload Balancing 配置期间更改了端口号，请输入该端口号。Citrix Hypervisor 使用您在此框中以及 Workload Balancing 配置期间指定的端口来连接 Workload Balancing。

默认情况下，Citrix Hypervisor 通过端口 8012 连接 Workload Balancing。

**注意：**

仅在运行“Workload Balancing 配置”向导时更改了此端口号才对其进行编辑。在运行“Workload Balancing 配置”向导时指定的端口号与“连接 WLB 服务器”对话框中的端口号必须一致。

7. 在“WLB 服务器凭据”部分中，输入运行 Citrix Hypervisor 的计算机在连接 Workload Balancing 服务器时使用的用户名（例如 `wlbuser`）和密码。
8. 在“Citrix Hypervisor 凭据”部分中，输入您正在配置的池的用户名和密码（通常是池主服务器的密码）。Workload Balancing 将使用这些凭据连接到该池中运行 Citrix Hypervisor 的计算机。
9. 在“Citrix Hypervisor 凭据”部分，输入所配置池的用户名和密码。Workload Balancing 将使用这些凭据连接到该池中运行 Citrix Hypervisor 的计算机。

要使用当前登录 Citrix Hypervisor 所使用的凭据，请选中“使用当前 XenCenter 凭据”复选框。

### 更改 **Workload Balancing** 的 IP 地址

可能需要更新 Workload Balancing 虚拟设备的 IP 地址的情形

要更改 Workload Balancing IP 地址，请执行以下操作：

1. 通过在虚拟设备上运行 `service workloadbalancing stop` 命令来停止 Workload Balancing 服务。
2. 通过在虚拟设备上运行 `ifconfig` 命令来更改 Workload Balancing 的 IP 地址。

3. 重新启用 Workload Balancing 并指定新 IP 地址。
4. 通过在虚拟设备上运行 `service workloadbalancing start` 命令来启动 Workload Balancing 服务。

### 停止 Workload Balancing

由于 Workload Balancing 在池级别进行配置，因此如果希望其停止管理某个池，就必须执行以下操作之一：

- **暂停 Workload Balancing。** 如果暂停 Workload Balancing，XenCenter 将停止显示针对指定资源池提出的建议并停止管理该池。暂停旨在短时间停止设备运行，您无需重新配置即可恢复监视。暂停 Workload Balancing 时，针对该资源池的数据收集会停止，直至您重新启用 Workload Balancing。
- **断开池与 Workload Balancing 的连接。** 断开与 Workload Balancing 虚拟设备的连接时，将中断 Workload Balancing 与池之间的连接，如果可以，从 Workload Balancing 数据库中删除池数据。断开与 Workload Balancing 的连接后，Workload Balancing 将停止收集该池的数据。

1. 在 XenCenter 的“资源”窗格中，选择要禁用 Workload Balancing 的资源池。
2. 在“WLB”选项卡中，单击“暂停”。此时“WLB”选项卡上将显示一条消息，说明 Workload Balancing 处于暂停状态。

提示：

要恢复监视，请单击“WLB”选项卡中的“恢复”按钮。

3. 在 XenCenter 的“基础结构”窗格中，选择要停止 Workload Balancing 的资源池。
4. 从“基础结构”菜单中，选择断开 *Workload Balancing* 服务器连接。此时将显示断开 *Workload Balancing* 服务器连接对话框。
5. 单击“断开连接”以永久停止 Workload Balancing 对池的监视。

提示：

如果断开了池与 Workload Balancing 虚拟设备的连接，要对该池重新启用 Workload Balancing，必须重新连接到 Workload Balancing 设备。有关信息，请参阅连接 Workload Balancing 虚拟设备。

### 在启用 Workload Balancing 的状态下进入维护模式

启用 Workload Balancing 后，如果将主机置于维护模式，Citrix Hypervisor 会将该主机上运行的 VM 迁移到最佳主机上（如果可用）。Citrix Hypervisor 根据 Workload Balancing 建议（性能数据、您的放置策略以及性能阈值）来迁移这些 VM。

如果没有可用的最佳主机，“进入维护模式”对话框中会显示“单击此处挂起 VM”字样。在这种情况下，Workload Balancing 不会提供放置建议，因为所有主机都没有足够的资源来运行此 VM。您可以将此 VM 挂起，或者退出“维护模式”，并将同一池中另一台主机上的一个 VM 挂起。这样，当您再次进入进入维护模式对话框时，Workload Balancing 可能会列出一台适合迁移的候选主机。

**注意：**

如果您将一台主机脱机以进行维护，并且 Workload Balancing 处于启用状态，则“进入维护模式”向导中会显示“Workload Balancing”字样。

要在启用 **Workload Balancing** 的状态下进入维护模式，请自行以下操作：

1. 在 XenCenter 的“资源”窗格中，选择要脱机的物理主机。在服务器菜单中，选择进入维护模式。
2. 在“进入维护模式”对话框中，单击“进入维护模式”。主机上运行的 VM 会根据 Workload Balancing 的性能数据、放置策略和性能阈值，自动迁移到最佳主机上。

要使主机退出维护模式，请右键单击主机，然后选择“退出维护模式”。主机退出维护模式之后，Citrix Hypervisor 会自动将该主机的原始 VM 还原到该主机。

### 增加 **Workload Balancing** 磁盘大小

此过程将介绍如何调整 Workload Balancing 虚拟设备虚拟磁盘的大小。执行这些步骤前，请关闭虚拟设备。Workload Balancing 将在约五分钟内保持不可用状态。

**警告：**

我们建议在执行此过程前生成数据快照。如果不正确执行这些步骤，可能导致 Workload Balancing 虚拟设备损坏。

1. 关闭 Workload Balancing 虚拟设备。  
在 XenCenter 资源窗格中，选择 Workload Balancing 虚拟设备。
2. 单击“存储”选项卡。
3. 选择“vdi\_xvda”磁盘，然后单击属性按钮。
4. 在“vdi\_xvda”属性对话框中，选择大小和位置。
5. 根据需要增加磁盘大小，然后单击确定。
6. 启动 Workload Balancing 虚拟设备并进行登录。
7. 在 Workload Balancing 虚拟设备上运行以下命令：

```
1  resize2fs /dev/xvda
```

**注意：**

如果未安装 `resize2fs` 工具，请务必连接到 Internet 并使用以下命令进行安装：

```
yum install -y --enablerepo=base,updates --disablerepo=citrix-*  
e2fsprogs
```

如果没有 Internet 访问权限，请执行以下操作：

1. 从 [http://mirror.centos.org/centos-7/7.2.1511/os/x86\\_64/Packages/](http://mirror.centos.org/centos-7/7.2.1511/os/x86_64/Packages/) 下载以下内容。

- libss-1.42.9-7.el7.i686.rpm
- e2fsprogs-libs-1.42.9-7.el7.x86\_64.rpm
- e2fsprogs-1.42.9-7.el7.x86\_64.rpm

2. 使用 SCP 或任何其他适用的工具将这些文件上载到 WLB VM。

3. 在 WLB VM 中运行以下命令：

```
1 rpm -ivh libss-*.rpm e2fsprogs-*.rpm
```

工具 `resize2fs` 现已安装。

4. 运行 `df -h` 命令以确认新的磁盘大小。

### 删除 **Workload Balancing** 虚拟设备

我们建议按从 XenCenter 中删除 VM 的标准过程来删除 Workload Balancing 虚拟设备。

删除 Workload Balancing 虚拟设备时，包含 Workload Balancing 的 PostgreSQL 数据库将随之删除。要保存此数据，必须在删除 Workload Balancing 虚拟设备前将其从数据库中迁出。

### 管理 **Workload Balancing** 数据库

Workload Balancing 数据库是 PostgreSQL 数据库。PostgreSQL 是开放源代码关系数据库。您可以搜索 Web 来查找 PostgreSQL 的文档。

以下信息专门面向数据库管理员以及熟悉数据库管理任务的高级 PostgreSQL 用户。如果没有使用 PostgreSQL 的经验，我们建议您在尝试执行以下部分所介绍的数据库任务前先熟悉该数据库。

默认情况下，PostgreSQL 用户名为 `postgres`。可以在 Workload Balancing 配置期间为此帐户设置密码。

可以存储的历史数据量取决于为 WLB 分配的虚拟磁盘大小和所需的最小磁盘空间。默认情况下，分配给 WLB 的虚拟磁盘的大小为 20 GB。有关详细信息，请参阅数据库整理参数。

要存储大量的历史数据（例如，如果要启用池审核追踪报告），您可以执行以下操作之一：

- 增大分配给 Workload Balancing 虚拟设备的虚拟磁盘大小。为此，请导入虚拟设备，然后通过执行增加 Workload Balancing 磁盘大小中所述的步骤增加虚拟磁盘的大小。
- 通过启用对数据库的远程客户端访问并使用第三方数据库管理工具，定期创建重复的数据备份副本。

就管理数据库而言，可以通过配置数据库整理来控制数据库数据占用的空间。

### 访问数据库

Workload Balancing 虚拟设备配置有防火墙。您必须先将 `postgres` 服务器端口添加至 `iptables`，然后才能访问数据库。

在 Workload Balancing 虚拟设备控制台中，运行以下命令：

```
1 iptables -A INPUT -i eth0 -p tcp -m tcp --dport 5432 -m \
2 state --state NEW,ESTABLISHED -j ACCEPT
```

(可选。) 要在此配置在重新启动虚拟设备后持久存在，请运行以下命令：

```
1 iptables-save > /etc/sysconfig/potables
```

### 控制数据库整理

当 VPX 达到 Workload Balancing 运行所需的最小磁盘空间量时，Workload Balancing 数据库将自动删除最早的数据。默认情况下，所需最小磁盘空间量设置为 1024 MB。

Workload Balancing 数据库整理选项通过 `wlb.conf` 文件进行控制。

当 Workload Balancing 虚拟设备的剩余磁盘空间不足时，Workload Balancing 将自动开始整理历史数据。此流程如下：

1. Workload Balancing 数据收集器按预定义的整理时间间隔检查是否需要进行整理。当数据库数据已经增长到未使用的空间只能满足最小磁盘空间要求时，需要进行整理。使用 `GroomingRequiredMinimumDiskSizeInMB` 设置所需的最小磁盘空间。  
如果需要，您可以使用 `GroomingIntervalInHour` 更改整理时间间隔。但是默认情况下，Workload Balancing 每小时执行一次检查，以确认是否需要进行整理。
2. 如果需要进行整理，Workload Balancing 首先整理日期最早的数据。然后，Workload Balancing 检查是否有足够的磁盘空间，以使其满足最小磁盘空间要求。
3. 如果第一次整理未释放出足够的磁盘空间，那么 Workload Balancing 将重复进行整理，直至达到 `GroomingRetryCounter` 次数，而不会等至 `GroomingIntervalInHour` 时刻。
4. 如果第一次或重复进行的整理释放出足够的磁盘空间，那么 Workload Balancing 将等至 `GroomingIntervalInHour` 时刻并返回步骤 1。
5. 如果由 `GroomingRetryCounter` 启动的整理未释放出足够的磁盘空间，那么 Workload Balancing 将等至 `GroomingIntervalInHour` 时刻并返回步骤 1。

### 数据库整理参数

`wlb.conf` 文件中有五个参数用于控制数据库整理的各个方面。这些参数如下：

- `GroomingIntervalInHour`。控制在完成下一次整理检查之前经过的小时数。例如，如果输入 **1**，Workload Balancing 将每小时检查一次磁盘空间。如果输入 **2**，Workload Balancing 将每两小时检查一次磁盘空间，以确定是否需要进行整理。
- `GroomingRetryCounter`。控制 Workload Balancing 尝试重新运行整理数据库查询的次数。

- **GroomingDBDataTrimDays**。控制 Workload Balancing 每次尝试整理数据时将从数据库中删除几天的数据。默认值为一天。
- **GroomingDBTimeoutInMinute**。控制数据库整理在超时或被取消前将持续的时间（分钟）。如果整理查询的时间超出预期值并且未在超时期间内完成运行，整理任务将被取消。默认值是 0 分钟，这意味着数据库整理永远不超时。
- **GroomingRequiredMinimumDiskSizeInMB**。控制分配给 Workload Balancing 虚拟设备的虚拟磁盘中的最小剩余可用空间量。当虚拟磁盘中的数据增长到虚拟磁盘上仅剩余最小磁盘大小的程度时，Workload Balancing 将触发数据库整理。默认值为 2048 MB。

要编辑这些值，请参阅编辑 Workload Balancing 配置文件。

#### 更改数据库密码

尽管可以通过 `wlb.conf` 文件更改数据库密码，但我们建议您改为运行 `wlbconfig` 命令。有关详细信息，请参阅修改 Modify the Workload Balancing 配置选项。

#### 将数据库数据存档

为避免旧的历史数据被删除，您可以选择复制数据库中的数据以进行存档。为此，您必须执行以下任务：

1. 针对数据库启用客户端身份验证。
2. 使用选择的 PostgreSQL 数据库管理工具设置存档。

#### 针对数据库启用客户端身份验证

尽管您可以通过 Workload Balancing 控制台直接连接数据库，但也可以使用 PostgreSQL 数据库管理工具。下载数据库管理工具后，将其安装到要连接数据库的系统上。例如，可以在运行 XenCenter 的同一便携式计算机上安装该工具。

针对数据库启用远程客户端身份验证前，必须执行以下操作：

1. 修改数据库配置文件（包括 `pg_hba.conf` 文件和 `postgresql.conf`）以允许进行连接。
2. 停止 Workload Balancing 服务，重新启动数据库，然后重新启动 Workload Balancing 服务。
3. 在数据库管理工具中，配置数据库的 IP 地址（即 Workload Balancing VPX 的 IP 地址）及数据库密码。

#### 修改数据库配置文件

要对数据库启用客户端身份验证，必须在 Workload Balancing 虚拟设备上修改两个文件：`pg_hba.conf` 文件和 `postgresql.conf` 文件。

要编辑 **pg\_hba.conf** 文件，请执行以下操作：

1. 修改 `pg_hba.conf` 文件。从 Workload Balancing 虚拟设备控制台，通过编辑器（例如 VI）打开 `pg_hba.conf` 文件。例如：

```
1 vi /var/lib/pgsql/9.0/data/pg_hba.conf
```

2. 如果网络使用 IPv4，请将所连接计算机的 IP 地址添加到此文件中。例如：

在配置部分中，在 `##IPv4 local connections` 下输入以下信息：

- **TYPE:** host
- **DATABASE:** all
- **USER:** all
- **CIDR-ADDRESS:** 0.0.0.0/0
- **METHOD:** trust

3. 在 `CIDR-ADDRESS` 字段中输入您的 IP 地址。

注意：

如果不输入 `0.0.0.0/0`，可以输入自己的 IP 地址并将后三位替换为 `0/24`。/ 尾部的“24”表示子网掩码，只允许从该子网掩码内的 IP 地址建立连接。

如果在 `Method` 字段中输入 `trust`，则连接无需密码即可完成身份验证。如果在 `Method` 字段中输入 `password`，则在连接数据库时必须提供密码。

4. 如果网络使用 IPv6，请将所连接计算机的 IP 地址添加到此文件中。例如：

在 `##IPv6 local connections` 下输入以下信息：

- **TYPE:** host
- **DATABASE:** all
- **USER:** all
- **CIDR-ADDRESS:** ::0/0
- **METHOD:** trust

在 `CIDR-ADDRESS` 字段中输入 IPv6 地址。在本例中，`::0/0` 将针对来自任何 IPv6 地址的连接打开数据库。

5. 保存文件并退出编辑器。
6. 更改任何数据库配置后，都必须重新启动数据库，以应用这些更改。运行以下命令：

```
1 service postgresql-9.0 restart
```

要编辑 `postgresql.conf` 文件，请执行以下操作：

1. 修改 `postgresql.conf` 文件。从 Workload Balancing 虚拟设备控制台，通过编辑器（例如 VI）打开 `postgresql.conf` 文件。例如：

```
1 vi /var/lib/pgsql/9.0/data/postgresql.conf
```

2. 编辑该文件，使设备侦听任何端口而不仅仅是本地主机。例如：

a) 找到以下行：

```
1 # listen_addresses='localhost'
```

b) 删除注释符(##)并编辑该行，使其如下所示：

```
1 listen_addresses='*'
```

3. 保存文件并退出编辑器。

4. 更改任何数据库配置后，都必须重新启动数据库，以应用这些更改。运行以下命令：

```
1 service postgresql-9.0 restart
```

### 更改数据库维护时段

默认情况下，Workload Balancing 自动在每天 12:05 AM GMT (00:05) 执行例行的数据库维护。在此维护时段期间，仍然继续收集数据，但数据的记录可能会延迟。但是，在此时段内，Workload Balancing 用户界面控制台仍可使用，Workload Balancing 仍然会提出优化建议。

注意：

要避免 Workload Balancing 丢失，请：

- 在维护时段内，Workload Balancing 服务器重新启动。请务必不要同时重新启动 VM。
- 在其他时候，重新启动池中的所有 VM 时，请勿重新启动 Workload Balancing 服务器。

数据库维护工作包括释放已分配但未使用的磁盘空间以及重新构建数据库的索引。维护工作将持续约 6 到 8 分钟。在较大的池中，维护可能会持续较长的时间，具体取决于 Workload Balancing 执行发现所花费的时长。

您可能需要更改进行维护的时间，这取决于您所处的时区。例如，在日本标准时间 (JST) 时区，Workload Balancing 维护工作从上午 9:05 (09:05) 开始，在某些组织中，这可能与高峰使用时段相冲突。如果要指定季节性时差（例如夏令时），必须将该时差纳入所输入的值中。

要更改维护时间，请执行以下操作：

1. 在 Workload Balancing 控制台中，从任何目录运行以下命令：

```
1 crontab -e
```

Workload Balancing 将显示如下内容：

```
1 05 0 * * * /opt/vpx/wlb/wlbmaintenance.sh
```

值 05 0 代表 Workload Balancing 执行维护工作的默认时间，05 为分钟，0 为小时。（星号表示作业运行的年月日：请勿编辑这些字段。）条目 05 0 指示数据库维护发生的时间为格林威治标准时间 (GMT) 每天晚上

12:05 或 00:05。此设置表示，如果您居住在纽约市，冬季月份的维护时间为晚上 7:05 (19:05)，夏季月份为晚上 8:05。

**重要：**

请不要编辑作业运行的年月日（用星号表示）。数据库维护作业必须每天运行。

2. 输入的维护时间为 GMT 时间。例如，假定您希望维护作业在午夜运行：

| 如果您所处的时区                   | UTC 偏差  | 本地维护时间为凌晨      |      |
|----------------------------|---------|----------------|------|
|                            |         | 12:05 时对应的标准时间 | 夏令时值 |
| 美国太平洋时区 (PST)<br>(例如加利福尼亚) | UTC-08  | 05 8           | 05 7 |
| 日本标准时间 (JST)               | UTC+09  | 05 15          | 不适用  |
| 北京时间                       | UTC +08 | 04 15          | 不适用  |

1. 保存文件并退出编辑器。

### 自定义 **Workload Balancing**

Workload Balancing 提供多种自定义方法：

- 用于编写脚本的命令行。有关这些命令，请参阅 Workload Balancing 命令。
- 主机启动脚本支持。也可以（间接）通过主机启动脚本自定义 Workload Balancing。

### 升级 **Workload Balancing**

出于安全原因，弃用了联机升级 Workload Balancing 的功能。客户无法再使用 yum repo 进行升级。通过从 <https://www.citrix.com/downloads/citrix-hypervisor/product-software/> 下载最新的 WLB VPX，客户可以将 WLB 升级到最新版本。

### **Workload Balancing** 故障排除

尽管通常情况下 Workload Balancing 都会顺畅地运行，但本系列部分仍提供了一些有用信息，可以在您遇到问题时为您提供指导。

#### 常规故障排除提示

- 执行故障排除时，首先应查看 Workload Balancing 日志文件 (LogFile.log 和 wlb\_install\_log.log)。这些日志位于 Workload Balancing 虚拟设备上的以下位置（默认位置）：
  - /var/log/wlb

- 查看 XenCenter“日志”选项卡上的日志可了解更多（不同）信息。
- 要查看 Workload Balancing 虚拟设备的内部版本号，请在由 VPX 监视的池中的主机上运行以下命令：

```
1 xe pool-retrieve-wlb-diagnostics | more
```

Workload Balancing 版本号显示在输出内容的最上方。

#### 错误消息

Workload Balancing 将错误以对话框形式显示在屏幕上，并以错误消息形式显示在 XenCenter 中的“日志”选项卡上。

如果出现错误消息，请查看 XenCenter 事件日志以获得更多信息。有关此日志位置的信息，请参阅 XenCenter 帮助。

#### 输入 **Workload Balancing** 凭据时遇到问题

如果在配置“连接 WLB 服务器”对话框时无法成功输入虚拟设备的用户帐户和密码，请尝试以下操作：

- 确保 Workload Balancing 虚拟设备已导入且配置正确，并且其所有服务都在运行。有关详细信息，请参阅 [\[wlb-start\]](#) (#wlb-start)。
- 检查以确保输入的凭据正确无误。默认凭据显示在《Workload Balancing 快速入门》中。
- 可以在“地址”框中输入主机名，但该名称必须是 Workload Balancing 虚拟设备的完全限定的域名 (FQDN)。请勿输入托管设备的物理服务器的主机名。例如 `yourcomputername`。如果在输入计算机名称时遇到问题，请尝试改用 Workload Balancing 设备的 IP 地址。
- 确认主机正在使用正确的 DNS 服务器，并且 Citrix Hypervisor 服务器可以使用 FQDN 与 Workload Balancing 服务器联系。要执行此检查，请从 Citrix Hypervisor 服务器使用其 FQDN 对 Workload Balancing 设备执行 ping 命令。例如，在 Citrix Hypervisor 服务器控制台中输入以下命令：

```
1 ping wlb-vpx-1.mydomain.net
```

#### 防火墙问题

如果 Workload Balancing 虚拟设备处于（硬件）防火墙保护下，但您没有配置相应的防火墙设置，则会出现以下错误：“There was an error connecting to the Workload Balancing server: <pool name> Click Initialize WLB to reinitialize the connection settings.”（连接 Workload Balancing 服务器时出错：<池名称> 请单击“初始化 WLB”以重新初始化连接设置。）如果因其他原因无法访问 Workload Balancing 设备，也可能会显示此错误。

解决方案：

如果 Workload Balancing 虚拟设备处于防火墙保护下，请打开端口 8012。

同样，Citrix Hypervisor 用来联系 Workload Balancing 的端口（默认为 8012）必须与运行 Workload Balancing 配置向导时所指定的端口号匹配。

### 与 **Workload Balancing** 失去连接

配置并连接 Workload Balancing 后，如果收到连接错误，可能因为凭据不再有效。要解决此问题，请尝试：

- 确认在连接 WLB 服务器对话框中输入的凭据与以下凭据匹配：
  - 在 Workload Balancing 配置期间创建的凭据
  - Citrix Hypervisor 上的凭据（即池主服务器凭据）
- 确认您在连接 WLB 服务器对话框中输入的 Workload Balancing 虚拟设备的 IP 地址或 FQDN 正确无误。
- 确认您在 Workload Balancing 配置期间创建的用户名与在“连接 WLB 服务器”对话框中输入的凭据一致。

### **Workload Balancing** 连接错误

如果在“WLB”选项卡上的“Workload Balancing 状态”行中收到连接错误消息，可能需要为该池重新配置 Workload Balancing。

单击“WLB”选项卡上的“连接”按钮，然后重新输入服务器凭据。

### **Workload Balancing** 停止工作

如果 Workload Balancing 不工作（例如不允许您保存对设置进行的更改），请检查 Workload Balancing 日志文件中是否存在以下错误消息：

```
1 dwmdatacolsvc.exe: Don't have a valid pool. Trying again in 10 minutes.
```

原因：

出现此错误通常是因为池中有一个或多个存在问题的 VM。当 VM 存在问题时，您可能会看到以下行为：

- **Windows**。Windows VM 因停止错误而崩溃（“蓝屏”）。
- **Linux**。Linux VM 可能在控制台中无响应，并且通常无法关闭。

解决方法：

1. 强制关闭 VM。为此，可以对问题 VM 所在的主机执行以下操作之一：

- 在 XenCenter 中，选择 VM，然后从 VM 菜单中，单击“强制关闭”。
- 运行 `vm-shutdown xe` 命令，并将 `force` 参数设置为 `true`，如《Citrix Hypervisor 管理员指南》中所述。例如：

```
1 xe vm-shutdown force=true uuid=vm_uuid
```

可以在该主机的“常规”选项卡中（XenCenter 中）或者通过运行 `host-list xe` 命令，找到主机 UUID。可以在 VM 的“常规”选项卡中或者通过运行 `vm-list xe` 命令，找到 VM UUID。有关详细信息，请参阅[命令行接口](#)。

2. 在向崩溃 VM 提供服务器的 Citrix Hypervisor 的 `xsconsole` 中或者在 XenCenter 中，将所有 VM 迁移到另一个主机上，然后运行 `xe-toolstack-restart` 命令。

### Workload Balancing 服务器的更改问题

如果在将池连接到其他 Workload Balancing 服务器时，没有先断开该池与 Workload Balancing 的连接，则原来的和新的 Workload Balancing 服务器都会监视该池。

要解决此问题，可以执行以下操作之一：

- 关闭并删除原来的 Workload Balancing 虚拟设备。
- 手动停止 Workload Balancing 服务。这些服务为分析、数据收集器和 Web 服务。

注意：

请勿使用 `pool-deconfigure-wlb xe` 命令断开池与 Workload Balancing 虚拟设备的连接，或者使用 `pool-initialize-wlb xe` 命令指定其他设备。

### Workload Balancing 命令

本节提供有关 Workload Balancing 命令的参考。可以从 Citrix Hypervisor 服务器或控制台执行以下命令以控制 Citrix Hypervisor 服务器上的 Workload Balancing 或配置 Workload Balancing 设置。本附录将介绍 `xe` 命令和服务命令。

在 Workload Balancing 设备上运行以下服务命令。为此，必须登录 Workload Balancing 虚拟设备。

#### 登录 Workload Balancing 虚拟设备

在运行任何服务命令或编辑 `wlb.conf` 文件之前，必须先登录 Workload Balancing 虚拟设备。要登录，必须输入用户名和密码。除非在虚拟设备上创建其他用户帐户，否则请以 `root` 用户身份登录。该帐户是您在运行 Workload Balancing 配置向导时（在将池连接到 Workload Balancing 之前）指定的。可以选择在 XenCenter 中使用“控制台”选项卡登录该设备。

要登录 Workload Balancing 虚拟设备，请执行以下操作：

1. 在 `name-of-your-WLB-VPX` 登录提示符处，输入帐户用户名。例如，其中 `wlb-vpx-pos-pool` 是 Workload Balancing 设备的名称：

```
1 wlb-vpx-pos-pool login: root
```

2. 在密码提示符处，输入帐户的密码：

```
1 wlb-vpx-pos-pool login: root
```

注意：

要注销 Workload Balancing 虚拟设备，只需在命令提示窗口下键入 `logout` 即可。

## **wlb restart**

从 Workload Balancing 设备中的任意位置运行 `wlb restart` 命令，可停止 Workload Balancing 数据收集、Web 服务和数据分析服务，然后再重新启动它们。

## **wlb start**

从 Workload Balancing 设备中的任意位置运行 `wlb start` 命令，可启动 Workload Balancing 数据收集、Web 服务和数据分析服务。

## **wlb stop**

从 Workload Balancing 设备中的任意位置运行 `wlb stop` 命令，可停止 Workload Balancing 数据收集、Web 服务和数据分析服务。

## **wlb status**

从 Workload Balancing 设备中的任意位置运行 `wlb status` 命令，可确定 Workload Balancing 服务器的状态。执行此命令后，将显示三个 Workload Balancing 服务（Web 服务、数据收集服务和数据分析服务）的状态。

## 修改 **Modify the Workload Balancing** 配置选项

许多 Workload Balancing 配置（如数据库和 Web 服务配置选项）都存储在 `wlb.conf` 文件中。`wlb.conf` 文件是 Workload Balancing 虚拟设备上的配置文件。

为了方便修改最常用的选项，Citrix 提供了 `wlb config` 命令。如果在 Workload Balancing 虚拟设备上运行 `wlb config` 命令，可以重命名 Workload Balancing 用户帐户、更改其密码或更改 PostgreSQL 密码。执行此命令后，Workload Balancing 服务将重新启动。

要运行 `wlb config` 命令，请执行以下操作：

1. 从命令提示窗口中运行以下命令：

```
1 wlb config
```

屏幕将显示一系列问题，以引导您更改 Workload Balancing 用户名和密码以及 PostgreSQL 密码。请按照屏幕上的问题来更改这些项目。

**重要：**

请仔细检查您在 `wlb.conf` 文件中输入的所有值：Workload Balancing 不会对 `wlb.conf` 文件中的值进行验证。因此，如果您指定的配置参数不在所需范围内，Workload Balancing 不会生成错误日志。

### 编辑 Workload Balancing 配置文件

可以通过编辑 `wlb.conf` 文件（存储在 Workload Balancing 虚拟设备上的 `/opt/vpx/wlb` 目录中）来修改 Workload Balancing 配置选项。一般情况下，只能在 Citrix 的指导下更改此文件中的设置。但是，您可以根据需要更改以下三类别的设置：

- **Workload Balancing** 帐户名称和密码。通过运行 `wlb config` 命令可以更方便地修改这些凭据。
- 数据库密码。可以使用 `wlb.conf` 文件修改此密码。但是，Citrix 建议使用 `wlb config` 命令进行修改，因为该命令不仅修改 `wlb.conf` 文件，还自动更新数据库中的密码。如果您选择修改 `wlb.conf` 文件，则必须运行查询以使用新密码更新数据库。
- 数据库整理参数。您可以使用该文件修改数据库整理参数（如数据库整理时间间隔），具体说明请参阅数据库管理部分。但 Citrix 建议您修改时要仔细谨慎。

对于 `wlb.conf` 文件中的所有其他设置，Citrix 目前建议将其均保留为默认值，除非 Citrix 指示您进行修改。

要编辑 **wlb.conf** 文件，请执行以下操作：

1. 在 Workload Balancing 虚拟设备（使用 VI 作为实例）上的命令提示窗口中运行以下命令：

```
1 vi /opt/vpx/wlb/wlb.conf
```

屏幕将显示配置选项的多个不同部分。

2. 修改配置选项，并退出编辑器。

编辑 `wlb.conf` 文件后，无需重新启动 Workload Balancing 服务。所做的更改在退出编辑器后立即生效。

**重要：**

请仔细检查您在 `wlb.conf` 文件中输入的所有值：Workload Balancing 不会对 `wlb.conf` 文件中的值进行验证。因此，如果您指定的配置参数不在所需范围内，Workload Balancing 不会生成错误日志。

### 提高 Workload Balancing 日志的详细级别

Workload Balancing 日志提供 Workload Balancing 虚拟设备上的事件列表，包括针对分析引擎、数据库和审核日志的操作。该日志文件位于 `/var/log/wlb/LogFile.log` 中。

您可以根据需要提高 Workload Balancing 日志的详细级别。为此，可以修改 Workload Balancing 配置文件 (wlb.conf) 的跟踪标志部分，该文件位于 /opt/vpx/wlb/wlb.conf 中。输入 1 或 true 可启用对特定跟踪的日志记录，输入 0 或 false 可禁用日志记录。例如，要对分析引擎跟踪启用日志记录，请输入：

```
1 AnalEngTrace=1
```

在向 Citrix 技术支持人员报告问题或进行故障排除之前，您可能希望提高日志记录的详细级别。

| 日志记录选项 | 跟踪标志                              | 益处或用途                                                                                             |
|--------|-----------------------------------|---------------------------------------------------------------------------------------------------|
| 分析引擎跟踪 | <code>AnalEngTrace</code>         | 记录分析引擎计算的详细信息。显示引擎做出的决策和分析的详细信息，并了解 Workload Balancing 不提出建议的原因。                                  |
| 数据库跟踪  | <code>DatabaseTrace</code>        | 记录有关数据库读取/写入的详细信息。但是，一直启用此项跟踪会使日志文件的大小迅速增加。                                                       |
| 数据收集跟踪 | <code>DataCollectionTrace</code>  | 记录检索指标的操作。此值允许您查看 Workload Balancing 检索并插入到 Workload Balancing 数据存储中的指标。但是，一直启用此项跟踪会使日志文件的大小迅速增加。 |
| 数据压缩跟踪 | <code>DataCompactionTrace</code>  | 记录有关压缩指标数据所花费的毫秒数的详细信息。                                                                           |
| 数据事件跟踪 | <code>DataEventTrace</code>       | 此项跟踪提供有关 Workload Balancing 从 XenServer 缓存的事件的详细信息。                                               |
| 数据整理跟踪 | <code>DataGroomingTrace</code>    | 此项跟踪提供有关数据库整理的详细信息。                                                                               |
| 数据指标跟踪 | <code>DataMetricsTrace</code>     | 记录有关分析指标数据的详细信息。一直启用此项跟踪会使日志文件的大小迅速增加。                                                            |
| 队列管理跟踪 | <code>QueueManagementTrace</code> | 记录有关数据收集队列管理处理的详细信息。(此选项供内部使用。)                                                                   |
| 数据保存跟踪 | <code>DataSaveTrace</code>        | 记录有关要保存到数据库中的池的详细信息。                                                                              |

| 日志记录选项   | 跟踪标志                            | 益处或用途                                                                                             |
|----------|---------------------------------|---------------------------------------------------------------------------------------------------|
| 主机得分跟踪   | <code>ScoreHostTrace</code>     | 记录有关 Workload Balancing 如何得出主机得分的详细信息。此项跟踪将显示当 Workload Balancing 计算星级以选择用于放置 VM 的最佳服务器时所得出的详细分数。 |
| 审核日志跟踪   | <code>AuditLogTrace</code>      | 显示所捕获并写入的审核日志数据的操作。（此选项仅供内部使用，不提供在审核日志中捕获的信息。）但是，一直启用此项跟踪会使日志文件的大小迅速增加。                           |
| 计划的任务跟踪  | <code>ScheduledTaskTrace</code> | 记录关于计划的任务的详细信息。例如，如果您计划的模式更改不起作用，您可能要启用此跟踪来调查原因。                                                  |
| Web 服务跟踪 | <code>WlbWebServiceTrace</code> | 记录与 Web 服务接口进行通信有关的详细信息。                                                                          |

## Workload Balancing 的证书

June 4, 2019

本节将介绍为确保证书安全可以执行的两项可选任务：

- 将 Citrix Hypervisor 配置为验证可信证书机构颁发的证书
- 将 Citrix Hypervisor 配置为验证默认的 Citrix WLB 自签名证书

### 概述

Citrix Hypervisor 与 Workload Balancing 通过 HTTPS 进行通信。因此，在 Workload Balancing 配置期间，该向导会自动创建一个自签名测试证书。此自签名测试证书允许 Workload Balancing 与 Citrix Hypervisor 建立 SSL 连接。

#### 注意：

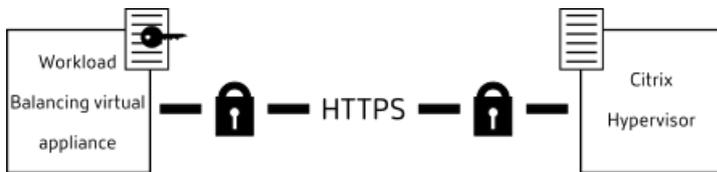
自签名证书是一个占位符，可用来方便实现 HTTPS 通信，该证书并非来自可信证书机构。为提高安全性，我们建

议使用可信证书机构颁发的证书。

默认情况下，Workload Balancing 将自动与 Citrix Hypervisor 创建此 SSL 连接。在为创建此 SSL 连接而配置 Workload Balancing 期间，或者在此之后，您无需执行任何证书配置。

但是，要使用其他证书颁发机构的证书（例如商业机构颁发的证书），您必须将 Workload Balancing 和 Citrix Hypervisor 配置为使用该证书。

无论 Workload Balancing 使用哪个证书，默认情况下，Citrix Hypervisor 在与 Workload Balancing 建立连接前都不会验证证书的身份。要将 Citrix Hypervisor 配置为对特定证书进行检查，必须导出用来签署该证书的根证书，将其复制到 Citrix Hypervisor，然后将 Citrix Hypervisor 配置为在与 Workload Balancing 建立连接时检查该证书。在这种情况下，Citrix Hypervisor 相当于客户端，Workload Balancing 相当于服务器。



根据您的安全目标，可以：

- 将 Citrix Hypervisor 配置为验证自签名证书。请参阅将 Citrix Hypervisor 配置为验证自签名证书。
- 将 Citrix Hypervisor 配置为验证可信证书机构颁发的证书。请参阅将 Citrix Hypervisor 配置为验证证书颁发机构颁发的证书。

### 将 Citrix Hypervisor 配置为验证自签名证书

可以将 Citrix Hypervisor 配置为在 Citrix Hypervisor 允许 Workload Balancing 建立连接之前验证 Citrix WLB 自签名证书的可信性。

**重要：**

要验证 Citrix WLB 自签名证书，必须使用其主机名连接到 Workload Balancing。要查找 Workload Balancing 主机名，请在虚拟设备上运行 `hostname` 命令。

如果想要将 Workload Balancing 配置为验证 Citrix WLB 自签名证书，请执行后面过程中的步骤。

**\*\* 要将 Citrix Hypervisor 配置为验证自签名证书，请执行以下操作： \*\***

1. 将自签名证书从 Workload Balancing 虚拟设备复制到池主服务器。Citrix WLB 自签名证书存储在 `/etc/ssl/certs/server.pem` 中。在池主服务器上运行以下命令以复制证书：

```
1 scp root@wlb-ip:/etc/ssl/certs/server.pem .
```

2. 如果收到指示无法确定 `wlb-ip` 真实性的消息，请键入 `yes` 以继续。
3. 提示时，输入 Workload Balancing 虚拟设备 `root` 用户密码，证书将复制到当前目录。
4. 安装证书。从要复制的证书所在的目录运行 `pool-certificate-install` 命令。例如：

```
1 xe pool-certificate-install filename=server.pem
```

5. 通过在池主服务器上运行 `pool-certificate-list` 命令来验证证书是否已正确安装：

```
1 xe pool-certificate-list
```

如果正确安装了证书，此命令的输出中将包括所导出的根证书（例如 `server.pem`）。运行此命令会列出所有已安装的 SSL 证书，其中包括刚刚安装的证书。

6. 在池主服务器上运行 `pool-certificate-sync` 命令，以将主服务器上的证书同步到池中的所有主机：

```
1 xe pool-certificate-sync
```

在主服务器上运行 `pool-certificate-sync` 命令可将所有池服务器上的此证书以及证书吊销列表与主服务器进行同步。这样可以确保池中的所有主机使用相同的证书。

此命令无输出。但如果此命令未成功运行，下一个步骤将无法进行。

7. 指示 Citrix Hypervisor 在连接 Workload Balancing 虚拟设备前验证证书。在池主服务器上运行以下命令：

```
1 xe pool-param-set wlb-verify-cert=true uuid=uuid_of_pool
```

提示：

按 Tab 键可自动填充池的 UUID。

8. (可选) 要验证此过程是否已成功完成，请执行以下步骤：

- a) 要测试证书是否已同步到池中的其他主机，请在这些主机上运行 `pool-certificate-list` 命令。
- b) 要测试 Citrix Hypervisor 是否设置为进行证书验证，请运行 `pool-param-get` 命令（带 `param-name=param-name=wlb-verify-cert` 参数）。例如：

```
1 xe pool-param-get param-name=wlb-verify-cert uuid=uuid_of_pool
```

## 将 Citrix Hypervisor 配置为验证证书颁发机构颁发的证书

可以将 Citrix Hypervisor 配置为验证由可信证书机构颁发的证书。

对于可信证书机构颁发的证书，Citrix Hypervisor 需要使用 .pem 格式带公钥的导出证书或证书链（即中间证书和根证书）。

如果希望 Workload Balancing 使用可信证书机构颁发的证书，请执行以下操作：

1. 从证书颁发机构获得签名证书。请参阅任务 1：获得证书颁发机构颁发的证书。
2. 根据任务 2：指定新证书中的说明指定并应用新证书。

3. 在池主服务器上安装获取的证书并启用证书验证功能。请参阅任务 3：将证书链导入池中。

开始执行这些任务前，请确保：

- 知道 Citrix Hypervisor 池主服务器的 IP 地址。
- Citrix Hypervisor 可以解析 Workload Balancing 主机名。（例如，可以从池主服务器的 Citrix Hypervisor 控制台尝试 ping 通 Workload Balancing FQDN。）

重要：

如果要使用 IP 地址连接 Workload Balancing，则在创建证书时必须将该 IP 地址指定为使用者备用名称 (SAN)。

### 任务 1：获得证书颁发机构颁发的证书

要从证书颁发机构获得证书，必须生成证书签名请求 (CSR)。为 Workload Balancing 虚拟设备生成 CSR 的过程由两个任务组成。必须 (1) 创建私钥，并 (2) 使用该私钥生成 CSR。必须在 Workload Balancing 虚拟设备上执行这两个过程。

#### 指定公用名的指导原则

创建 CSR 时指定的公用名 (CN) 必须与 Workload Balancing 虚拟设备的 FQDN，以及在“连接 WLB 服务器”对话框中的“地址”框中指定的 FQDN 或 IP 地址完全一致。

要确保名称相符，请遵照以下指导原则之一来指定公用名：

- 为证书的公用名指定与在“连接 WLB 服务器”对话框中指定的信息相同的信息。例如，如果 Workload Balancing 虚拟设备的名称为 `wlb-vpx.yourdomain`，请在“连接 WLB 服务器”中指定 `wlb-vpx.yourdomain`，并在创建 CSR 时提供 `wlb-vpx.yourdomain` 作为公用名。
- 如果使用 IP 地址将池连接到 Workload Balancing，则使用 FQDN 作为公用名，并指定 IP 地址作为使用者备用名称 (SAN)。但是，这可能并不适用于所有情况。

注意：

证书验证是旨在防止意外连接的安全措施。因此，Workload Balancing 证书必须满足严格的要求，否则证书验证将不会成功，Citrix Hypervisor 将不允许进行连接。同样，要使证书验证成功，必须将这些证书存储在 Citrix Hypervisor 用来查找证书的特定位置。

要创建私钥文件，请执行以下操作：

1. 创建私钥文件：

```
1 openssl genrsa -des3 -out privatekey.pem 2048
```

2. 删除密码：

```
1 openssl rsa -in privatekey.pem -out privatekey.nop.pem
```

**注意：**

如果输入的密码不正确或者不一致，系统可能会显示一些消息，指出用户界面存在错误。您可以忽略此消息，并重新运行用于创建私钥文件的命令。

要生成 **CSR**，请执行以下操作：

**1. 生成 CSR：****a) 使用私钥创建 CSR：**

```
1 openssl req -new -key privatekey.nop.pem -out csr
```

**b) 按提示提供生成 CSR 所需的信息：**

**Country Name** (国家/地区名称)。输入所在国家/地区的 SSL 证书国家/地区代码。例如，CA 代表加拿大，JM 代表牙买加。可以在 Web 上查找 SSL 证书国家/地区代码的列表。

**State or Province Name (full name)** (州名或省名 (全称))。输入资源池所在的州或省。例如，马萨诸塞或艾伯塔。

**Locality Name** (地点名称)。资源池所在城市的名称。

组织名称。公司或组织的名称。

**Organizational Unit Name** (组织单位名称)。输入部门名称。此字段为可选字段。

常用名称。输入 Workload Balancing 服务器的 FQDN。此名称必须与池用来连接 Workload Balancing 的名称匹配。

电子邮件地址。生成证书时，此电子邮件地址将包括在证书中。

**c) 提供可选属性，或单击 Enter 键以跳过提供这些信息。**

CSR 请求保存在当前目录中并命名为 `csr`。

**2. 在 Workload Balancing 设备控制台中运行以下命令，以在控制台窗口中显示 CSR：**

```
1 cat csr
```

**3. 复制整个证书请求并使用 CSR 向证书颁发机构请求证书。****任务 2：指定新证书**

使用此过程可以指定 Workload Balancing 使用证书颁发机构颁发的证书。此过程将安装根证书（如果可用）和中间证书。

要指定新证书，请执行以下操作：

1. 下载签名证书、根证书和（如果证书颁发机构有中间证书）证书颁发机构颁发的中间证书。
2. 如果未将证书下载到 Workload Balancing 虚拟设备，执行以下操作之一：
  - a) 如果将证书从 Windows 计算机复制到 Workload Balancing 设备，请使用 WinSCP 或其他复制实用程序复制文件。

对于主机名，可以输入 IP 地址并保留默认端口。通常情况下，用户名为 root，密码为您在配置期间设置的密码。

- a) 如果将证书从 Linux 计算机复制到 Workload Balancing 设备，请使用 SCP 或其他复制实用程序将文件复制到 Workload Balancing 设备上的所选目录。例如：

```
1 scp root_ca.pem root@wlb-ip:/path_on_your_WLB
```

3. 在 Workload Balancing 虚拟设备上，将所有证书（根证书、中间证书（如果存在）和签名证书）合并成一个文件。例如：

```
1 cat signed_cert.pem intermediate_ca.pem root_ca.pem > server.pem
```

4. 使用 move 命令重命名现有证书和密钥：

```
1 mv /etc/ssl/certs/server.pem /etc/ssl/certs/server.pem_orig
2 mv /etc/ssl/certs/server.key /etc/ssl/certs/server.key_orig
```

5. 复制合并的证书：

```
1 mv server.pem /etc/ssl/certs/server.pem
```

6. 复制以前创建的私钥：

```
1 mv privatekey.nop.pem /etc/ssl/certs/server.key
```

7. 使该私钥仅可由 root 用户读取。使用 chmod 命令修复权限。

```
1 chmod 600 /etc/ssl/certs/server.key
```

8. 重新启动 stunnel：

```
1 killall stunnel
2 stunnel
```

### 任务 3：将证书链导入池中

获取证书后，必须将证书导入（安装至）Citrix Hypervisor 池主服务器，并同步池中的主机以使用这些证书。然后可以配置 Citrix Hypervisor，使其在 Workload Balancing 每次连接主机时验证证书的身份和有效性。

1. 将签名证书、根证书和证书颁发机构颁发的中间证书（如果证书颁发机构有中间证书）复制到 Citrix Hypervisor 池主服务器中。

2. 在池主服务器上安装根证书：

```
1 xe pool-certificate-install filename=root_ca.pem
```

3. 如果适用，在池主服务器上安装中间证书：

```
1 xe pool-certificate-install filename=intermediate_ca.pem
```

4. 通过在池主服务器上运行此命令来验证两种证书都已正确安装：

```
1 xe pool-certificate-list
```

运行此命令后，将列出所有已安装的 SSL 证书。如果证书已成功安装，将显示在此列表中。

5. 将池主服务器上的证书同步到池中所有主机上：

```
1 xe pool-certificate-sync
```

在主服务器上运行 `pool-certificate-sync` 命令可将所有池服务器上的此证书以及证书吊销列表与池主服务器进行同步。这样可以确保池中的所有主机使用相同的证书。

6. 指示 Citrix Hypervisor 在连接 Workload Balancing 虚拟设备前验证证书。在池主服务器上运行以下命令：

```
1 xe pool-param-set wlb-verify-cert=true uuid=uuid_of_pool
```

提示：

按 Tab 键可自动填充池的 UUID。

7. 如果在启用证书验证前，在“连接 WLB”对话框中指定了 IP 地址，系统可能会提示您将池重新连接到 Workload Balancing。

在这种情况下，请在“连接 WLB”对话框的“地址”框中为 Workload Balancing 设备指定与在证书公用名 (CN) 中显示的完全相同的 **FQDN**。（公用名必须与 Citrix Hypervisor 用来进行连接的名称一致，因此必须输入 FQDN。）

#### 故障排除提示

- 如果在配置证书验证后，池无法连接到 Workload Balancing，请检查在关闭证书验证的情况下池能否连接（通过运行 `xe pool-param-set wlb-verify-cert=false uuid=uuid_of_pool`）。如果在关闭验证功能的情况下可以进行连接，问题可能出在证书配置。如果不能连接，则问题可能出在 Workload Balancing 凭据或网络连接。

- 一些商业证书颁发机构提供多种工具来验证证书安装的正确性。如果上述过程无法帮助解决问题，可以考虑运行这些工具。如果这些工具要求指定 SSL 端口，请指定端口 8012 或者在 Workload Balancing 配置期间设置的端口。
- 在执行这些过程之后，如果在 WLB 选项卡上显示一条错误消息，内容是“**There was an error connecting to the WLB server**”（连接 WLB 服务器时出错），则说明证书中的公用名与 Workload Balancing 虚拟设备名称之间可能存在冲突。Workload Balancing 虚拟设备的名称与证书的公用名必须完全匹配。

## Conversion Manager

July 10, 2019

Citrix Hypervisor Conversion Manager 可以将成批的 VMware 虚拟机移至 Citrix Hypervisor 环境，从而帮助您将工作负载从 VMware 迁移到 Citrix Hypervisor。

Citrix Hypervisor Conversion Manager 可以简化迁移操作，而不仅仅是转换虚拟机。Citrix Hypervisor Conversion Manager 可以帮助您准备虚拟机，以便进行网络连接和存储连接。转换后，虚拟机就几乎准备就绪，可随时运行。

### 从 **VMware** 转换为 **Citrix Hypervisor**

Citrix Hypervisor Conversion Manager 可用于：

- 使用一个简单的向导转换多个 VM
- 映射 VMware 和 Citrix Hypervisor 之间的网络设置，以便转换后的 VM 可以在正确的网络设置下启动并运行
- 选择希望新的 Citrix Hypervisor VM 运行的存储位置

注意：

- Citrix Hypervisor Conversion Manager 不会删除或更改现有的 VMware 环境。VM 将复制到 Citrix Hypervisor 环境中，而不会从 VMware 中删除。
- Citrix Hypervisor Conversion Manager 适用于 Citrix Hypervisor Premium Edition 客户或通过其 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。有关 Citrix Hypervisor 许可的详细信息，请参阅[许可](#)。要升级或购买 Citrix Hypervisor 8.0 许可证，请访问 [Citrix Web 站点](#)。

### 了解 **Citrix Hypervisor**

在转换您的环境之前，建议您先熟悉 Citrix Hypervisor 概念。有关详细信息，请参阅[技术概述](#)。

要成功使用 Citrix Hypervisor Conversion Manager，请执行以下任务：

- 设置基本 Citrix Hypervisor 环境，包括安装 Citrix Hypervisor。有关详细信息，请参阅[快速入门](#)[(/zh-cn/citrix-hypervisor/quick-start.html)] 和[安装](#)。
- 在 Citrix Hypervisor 中创建网络，以将 IP 地址分配给 NIC。有关详细信息，请参阅[快速入门](#)。
- 连接到存储。有关详细信息，请参阅[快速入门](#)。

注意：

Citrix Hypervisor 文档可从 docs.citrix.com 获取，知识中心文章和白皮书可以从 [Citrix 知识中心](#) 获取。

### 比较 VMware 和 Citrix Hypervisor 术语

下表列出了与常见的 VMware 功能、概念和组件对应的类似 Citrix Hypervisor 功能、概念和组件：

| VMware 术语          | Citrix Hypervisor 等效术语                   |
|--------------------|------------------------------------------|
| VMware vSphere 客户端 | XenCenter (适用于 Citrix Hypervisor 的管理控制台) |
| 群集/资源池             | 资源池                                      |
| 数据存储               | 存储库                                      |
| vMotion            | 实时迁移                                     |
| 分布式资源调度 (DRS)      | Workload Balancing                       |
| 高可用性 (HA)          | 高可用性 (HA)                                |
| vCenter 转换器        | Citrix Hypervisor Conversion Manager     |
| 基于角色的访问控制 (RBAC)   | 基于角色的访问控制 (RBAC)                         |

### 转换概述

Citrix Hypervisor Conversion Manager 将创建每个目标 VM 的副本。将目标 VM 转换为具有相当的网络连接和存储连接的 Citrix Hypervisor VM 后，它会将该 VM 导入 Citrix Hypervisor 池或主机。您可以使用 Citrix Hypervisor Conversion Manager 转换至少一或两个 VM，或对整个环境执行批量转换。

注意：

从 vSphere 转换 VM 之前，必须先关闭 vSphere 上的 VM（用于转换）。当前版本的 Citrix Hypervisor Conversion Manager 不支持转换正在运行的使用从 vSphere 复制到 Citrix Hypervisor 的内存的 VM。

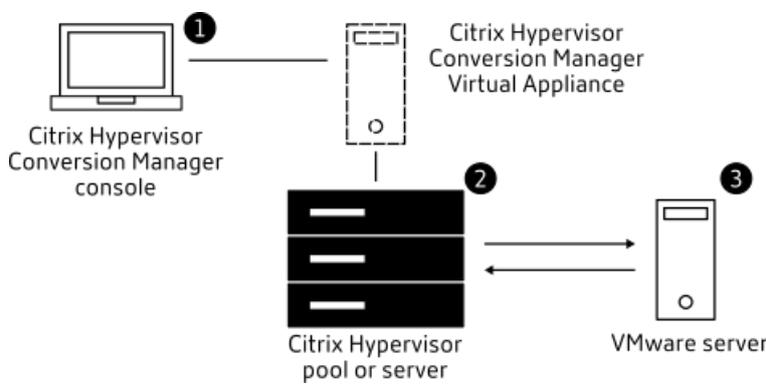
Citrix Hypervisor Conversion Manager 转换过程需要四种工具：

- **Citrix Hypervisor Conversion Manager** 控制台 - 设置转换选项和控制转换的用户界面。可以在 Windows 或 Linux 本地桌面上安装该控制台。Citrix Hypervisor Conversion Manager 控制台需要连接到 Citrix

Hypervisor 以及 Citrix Hypervisor Conversion Manager 虚拟设备。

- **Citrix Hypervisor Conversion Manager** 虚拟设备 - 导入到要运行转换后的 VM 的 Citrix Hypervisor 主机或池的预打包 VM。该虚拟设备会将 VMware VM 的副本转换为 Citrix Hypervisor 虚拟机格式。转换完成后，它会将这些副本导入到 Citrix Hypervisor 池或主机中。
- **Citrix Hypervisor** 独立主机或池 - 要运行转换后的 VM 的 Citrix Hypervisor 环境。
- **VMware** 服务器。Citrix Hypervisor Conversion Manager 需要连接到用于管理要转换的 VM 的 VMware 服务器。该连接可以是与 vCenter Server、ESXi Server 或 ESX Server 的连接。这些 VM 不会从 VMware 服务器中删除。相反，Citrix Hypervisor Conversion Manager 虚拟设备会创建这些 VM 的副本，并将其转换为 Citrix Hypervisor 虚拟机格式。

下图说明了这些组件之间的关系：



此图显示：

1. Citrix Hypervisor Conversion Manager 如何与 Citrix Hypervisor Conversion Manager 虚拟设备进行通信。
2. Citrix Hypervisor Conversion Manager 虚拟设备如何使用 VMware 服务器进行身份验证。
3. VMware 服务器在转换期间如何响应 Citrix Hypervisor Conversion Manager 虚拟设备。

只有当 Citrix Hypervisor Conversion Manager 虚拟设备在整个转换期间从 VMware 服务器中查询环境信息和磁盘数据时，VMware 服务器才会与该设备进行通信。

#### 如何转换 VM 的摘要

只需几个简单的步骤即可配置 Citrix Hypervisor Conversion Manager 并开始转换 VM：

1. 从 [Citrix Hypervisor 8.0 Premium Edition 页面] 下载 Citrix Hypervisor Conversion Manager 虚拟设备和 Citrix Hypervisor Conversion Manager 控制台。
2. 使用 XenCenter 将 Citrix Hypervisor Conversion Manager 虚拟设备导入 Citrix Hypervisor。
3. 使用 XenCenter 配置 Citrix Hypervisor Conversion Manager 虚拟设备。
4. 安装 Citrix Hypervisor Conversion Manager 控制台。
5. 从 Citrix Hypervisor Conversion Manager 控制台启动转换向导并开始转换 VM。

以下几节将详细介绍这些步骤。还可以在 Citrix Hypervisor Conversion Manager 帮助（显示在 Citrix Hypervisor Conversion Manager 中）中获取这些信息。

## 准备环境

转换 VMware 环境之前，必须创建和准备目标 Citrix Hypervisor 独立主机或环境以运行转换后的 VMware VM。准备环境的工作包含以下活动：

1. 定义如何转换 VMware 环境的策略。是否要仅转换 1 个或 2 个 VM？是否要转换整个环境？是否要先创建试点以确保配置正确无误？是否并行运行这两种环境？是否要在转换为 Citrix Hypervisor 时继续使用现有的群集设计？
2. 规划网络连接配置。是否要连接到相同的物理网络？是否要简化或更改网络连接配置？
3. 在池所需的主机上安装 Citrix Hypervisor。理想情况下，您应在开始安装之前，将主机上的 NIC 插接到其物理网络。
4. 创建池并执行任何基本的网络连接配置。例如，执行以下操作：
  - 配置网络以连接到 Citrix Hypervisor 主机上的 VMware 群集（如果该群集与 Citrix Hypervisor 主机不在同一网络中）。
  - 配置网络以连接到存储阵列。即，如果使用基于 IP 的存储，请创建连接到存储阵列的物理网络的 Citrix Hypervisor 网络。
  - 创建池，并将主机添加到该池中。
5. (对于共享存储和 Citrix Hypervisor 池。) 准备用于存储虚拟磁盘的共享存储，并创建与池中称为存储库 (SR) 的存储的连接。
6. (可选)。虽然不要求进行转换，但是您可以在 Citrix Hypervisor 池中配置管理员帐户，以匹配 VMware 服务器上的相应帐户。有关为 Active Directory 帐户配置基于角色的访问控制的信息，请参阅 [XenCenter 帮助](#) 或 [快速入门](#)。

## 安装 Citrix Hypervisor 并创建池

在可以转换 VMware VM 之前，请确保创建要运行转换后的 VM 的 Citrix Hypervisor 池或主机。此池必须配置了网络连接，以便可以连接到 VMware 服务器。您可能还想在位于 VMware 群集中的 Citrix Hypervisor 池中配置相同的物理网络，或简化网络连接配置。如果要在某个池中运行转换后的 VM，请在转换之前创建存储库并将共享存储添加到该池中。

如果您是 Citrix Hypervisor 的新用户，可以阅读 [快速入门](#) 以了解有关 Citrix Hypervisor 的基础知识，包括基本信息和配置。

## Citrix Hypervisor 环境注意事项

在安装 Citrix Hypervisor 并导入虚拟设备之前，请考虑以下可能会更改转换策略的因素：

选择要运行 **Citrix Hypervisor Conversion Manager** 虚拟设备的主机。将虚拟设备导入独立主机或导入运行转换后的 VM 的池中的主机。

对于池，可以在池中的任何主机上运行虚拟设备，只要其存储满足存储要求即可。

为要运行转换后的 **VM** 的池或主机配置的存储必须满足特定要求。如果在池中运行新转换的 VM，必须在共享存储中存储其虚拟磁盘。但是，如果转换后的 VM 在一个独立主机（而非池中）上运行，则其虚拟磁盘可以使用本地存储。

如果要在池中运行转换后的 VM，请确保通过创建存储库将共享存储添加到池中。

支持转换的来宾操作系统。Citrix Hypervisor Conversion Manager 支持转换运行 Citrix Hypervisor 支持的任何 Windows 来宾操作系统的 VMware VM。有关 Citrix Hypervisor 支持的 Windows 来宾操作系统的列表，请参阅[来宾操作系统支持](#)。还支持以下 Linux 操作系统。

- RHEL 5.4/5.6/6.4/7.0
- CentOS 5.5/6.3/6.4/6.5/7.0
- SLES 11 SP1/SP2/SP3/SP4
- Ubuntu 14.04/16.04

### 满足网络连接要求

要转换 VMware VM，Citrix Hypervisor Conversion Manager 虚拟设备需要连接到可访问 VMware 服务器的物理网络或 VLAN。（在以下部分中，此网络称为“VMware 网络”。）

如果 VMware 服务器与 Citrix Hypervisor 池中的主机位于不同的物理网络中，请在转换之前将网络添加到 Citrix Hypervisor 中。

### 映射现有的网络配置

Citrix Hypervisor Conversion Manager 中包含的功能可以减少从现有 VMware VM 转换到 Citrix Hypervisor 后所需的手动网络连接配置工作量。例如，Citrix Hypervisor Conversion Manager 可以：

- 在 VMware VM 上保留虚拟 MAC 地址，并在转换后的 Citrix Hypervisor VM 中重新使用它们。保留与虚拟网络适配器（虚拟 MAC 地址）相关联的 MAC 地址可以：
  - 帮助在使用 DHCP 的环境中保留 IP 地址
  - 如果对软件程序的许可引用的是虚拟 MAC 地址，则会非常有用
- 映射（虚拟）网络适配器。Citrix Hypervisor Conversion Manager 可以将 VMware 网络映射到 Citrix Hypervisor 网络，以便在转换 VM 后，相应地连接其虚拟网络接口。您选择的 Citrix Hypervisor 网络包括标准物理网络（称为外部网络）、VLAN、单服务器专用网络，以及跨服务器专用网络。

例如，如果将 VMware“虚拟网络 4”映射到 Citrix Hypervisor“网络 0”，则虚拟适配器连接到“虚拟网络 4”的任何 VMware VM 将在转换后连接到“网络 0”。Citrix Hypervisor Conversion Manager 不转换或迁移任何虚拟机管理程序网络设置。向导将仅根据提供的映射更改转换后的 VM 的虚拟网络接口连接。

注意：

不需要将所有 VMware 网络都映射到相应的 Citrix Hypervisor 网络。但是，如果您愿意，可以更改 VM 使用的网络，减少或整合新 Citrix Hypervisor 配置中的网络数。

要从这些功能中获得最大益处，Citrix 建议您执行以下操作：

- 安装 Citrix Hypervisor 之前，请将主机连接到要对主机配置的交换机（即端口）上的网络。
- 确保 Citrix Hypervisor 池可以显示您要检测的网络。具体来说，将 Citrix Hypervisor 主机连接到可与 VMware 群集访问相同网络的交换机端口。

虽然将 Citrix Hypervisor NIC 连接到与 VMware 主机上的 NIC 相同的网络更简单，但是不需要这样做。如果要更改 NIC/网络关联，可以将 Citrix Hypervisor NIC 连接到不同的物理网络。

#### 准备 Citrix Hypervisor Conversion Manager 网络连接要求

执行转换时，必须创建与 VMware 服务器所在的网络的网络连接。Citrix Hypervisor Conversion Manager 将使用此连接实现 Citrix Hypervisor 主机和 VMware 服务器之间的转换通信。

要创建此网络连接，必须执行以下两个任务：

- 导入 Citrix Hypervisor Conversion Manager 虚拟设备时，将为转换通信添加的网络指定为虚拟网络接口。可以通过配置接口 1 来实现这一点，以便连接到该网络。
- 运行转换向导之前，请将连接 VMware 和 Citrix Hypervisor 的网络添加到要运行转换后的 VM 的 Citrix Hypervisor 主机。

默认情况下，当您导入 Citrix Hypervisor Conversion Manager 虚拟设备时，XenCenter 将创建一个与网络 0 和 NIC0 (eth0) 关联的虚拟网络接口。但是，默认情况下，Citrix Hypervisor 安装程序会 NIC0 配置为管理接口，即用于 Citrix Hypervisor 管理通信的 NIC。因此，添加网络以进行转换时，您可能想选择 NIC 而非 NIC0。选择其他网络可能会提高处于繁忙状态的池的性能。有关管理接口的详细信息，请参阅 XenCenter 帮助。

将网络添加到 **Citrix Hypervisor**：

1. 在 XenCenter 中的资源窗格中，选择要在其中运行 Citrix Hypervisor Conversion Manager 的池。
2. 单击网络连接选项卡。
3. 单击添加网络。
4. 在选择类型页面上，选择外部网络，单击下一步。
5. 在名称页面上，为网络输入有意义的名称（例如，“VMware 网络”）和说明。
6. 在接口页面上，指定以下设置：

- **NIC**。希望 Citrix Hypervisor 用于创建网络的 NIC。选择连接到 VMware 服务器的物理或逻辑网络的 NIC。
- **VLAN**。如果 VMware 网络是 VLAN，请输入 VLAN ID（或“标记”）。
- **MTU**。如果 VMware 网络使用 Jumbo 帧，请为“最大传输单位”(MTU) 输入介于 1500 到 9216 之间的值。否则，请将 MTU 框保留为其默认值 1500。

注意：

请勿选中自动将此网络添加到新虚拟机复选框。

7. 单击完成。

### 满足存储要求

转换成批的 VMware VM 之前，请考虑存储要求。转换后的 VM 磁盘存储在 Citrix Hypervisor 存储库中。

此存储库的容量应该足够大，以便能够容纳要在该池中运行的所有转换后的 VM 的虚拟磁盘。对于仅在独立主机上运行的转换后的计算机，可以指定本地或共享存储作为转换后的虚拟磁盘的位置。对于在池中运行的转换后的计算机，只能指定共享存储。

要创建存储库，请执行以下操作：

1. 在 XenCenter 中的资源窗格中，选择要在其中运行 Citrix Hypervisor Conversion Manager 虚拟设备的池。
2. 单击存储选项卡。
3. 单击新建 **SR**，然后按照向导中的说明进行操作。有关更多说明，请按 **F1** 以显示联机帮助。

### Citrix Hypervisor 要求

可以在以下版本的 Citrix Hypervisor 上运行使用此版本的 Citrix Hypervisor Conversion Manager 进行转换的 VM：

- XenServer 7.0
- XenServer 7.1 Cumulative Update 2
- XenServer 7.5
- XenServer 7.6
- Citrix Hypervisor 8.0

### VMware 要求

Citrix Hypervisor Conversion Manager 可以从以下版本的 VMware 转换 VMware VM：

- vCenter Server 5.5.0、6.0.0 和 6.5.0
- vSphere 5.5.0、6.0.0 和 6.5.0

- ESXi 5.5.0、6.0.0 和 6.5.0

注意：

Citrix Hypervisor Conversion Manager 无法将具有四个或更多磁盘的 VMWare VM 转换为 Citrix Hypervisor VM。您的 VMWare VM 必须具有三个或更少的磁盘。

### 准备导入虚拟设备

在导入 Workload Balancing 虚拟设备之前，请注意以下事项并根据需要对环境进行相应的更改。

### 下载虚拟设备

以 xva 格式打包 Citrix Hypervisor Conversion Manager 虚拟设备。您可以从 [Citrix Hypervisor 8.0 Premium Edition 页面] 下载该虚拟设备。下载该文件时，请将其保存到本地硬盘驱动器（通常但不一定位于安装了 XenCenter 的计算机上）上的文件夹中。在.xva 文件位于硬盘驱动器后，可以将其导入 XenCenter。

注意：

Citrix Hypervisor Conversion Manager 适用于 Citrix Hypervisor Premium Edition 客户或通过其 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。有关 Citrix Hypervisor 许可的详细信息，请参阅[许可](#)。要升级或购买 Citrix Hypervisor 8.0 许可证，请访问 [Citrix Web 站点]。

### 虚拟设备的必备条件

Citrix Hypervisor Conversion Manager 虚拟设备至少需要：

- XenServer 7.0、XenServer 7.1 Cumulative Update 2、XenServer 7.5、XenServer 7.6、Citrix Hypervisor 8.0
- 磁盘空间：30 GB 的磁盘空间
- 内存：6.5 GB
- 虚拟 CPU 分配：1 个 vCPU

### 导入和配置 **Citrix Hypervisor Conversion Manager** 虚拟设备

Citrix Hypervisor Conversion Manager 虚拟设备是设计用于在 Citrix Hypervisor 主机上运行的单个预安装 VM。在导入之前，请查看准备导入虚拟设备部分中的必备条件信息和注意事项。

### 将虚拟设备导入 **Citrix Hypervisor**

将 Citrix Hypervisor Conversion Manager 虚拟设备导入要在其中运行转换后的 VM 的池或主机。要导入 Citrix Hypervisor Conversion Manager 虚拟设备，请使用 XenCenter 的导入向导。

要将虚拟设备导入 XenCenter，请执行以下操作：

1. 打开 XenCenter。在要导入虚拟设备软件包的池（或主机）上单击鼠标右键，然后选择导入。
2. 浏览找到该虚拟设备的软件包。
3. 选择要在其中运行 Citrix Hypervisor Conversion Manager 虚拟设备的池或主服务器。

注意：

主服务器是为池中的 VM 提供资源的主机。虽然 Citrix Hypervisor 可以在其他主机上启动 VM，但是在尝试其他主机之前，它会先尝试在该主机上启动 VM。如果选择某个主机，Citrix Hypervisor Conversion Manager 虚拟设备会使用此主机作为主服务器。如果选择池，虚拟设备将自动启动该池中最适合的主机。

4. 选择要在其上为 Citrix Hypervisor Conversion Manager 虚拟设备存储虚拟磁盘的存储库，然后单击导入。要将存储库添加到池中，请参阅“满足存储要求”部分。可以选择本地或共享存储。
5. 确保将要用于转换的网络（将 VMware 服务器连接到 Citrix Hypervisor 主机的网络）选择作为与接口 1（“虚拟 NIC 1”）相关联的网络。
  - 如果接口 1 旁边未显示正确的网络，请使用网络列中的列表选择其他网络。
  - 如果尚未添加与池位于不同的物理网络中的 VMware 网络，请执行以下操作：
    - a) 退出向导。
    - b) 将该网络添加到池中。
    - c) 重新运行向导。

有关详细信息，请参阅将网络添加到 **Citrix Hypervisor** 中。

警告：

请勿将客户网络配置为 NIC0。仅将 NIC0 分配为“主机内部管理网络”。

6. 使导入后启动 **VM** 复选框处于启用状态，然后单击完成以导入虚拟设备。
7. 导入.xva 文件后，Citrix Hypervisor Conversion Manager 虚拟设备将显示在 XenCenter 中的资源窗格中。

### 配置 Citrix Hypervisor Conversion Manager 虚拟设备

完成导入 Citrix Hypervisor Conversion Manager 虚拟设备后，您必须先对其进行配置，然后才能使用它来转换 VMware VM。按照 XenCenter 控制台选项卡中提示进行操作。

1. 导入 Citrix Hypervisor Conversion Manager 虚拟设备后，请单击控制台选项卡。
2. 输入是以接受许可协议的条款。若要拒绝 EULA，请输入否。
3. 输入并确认 Citrix Hypervisor Conversion Manager 虚拟设备的新 root 用户密码。Citrix 建议选择强密码。
4. 输入 Citrix Hypervisor Conversion Manager 虚拟设备的主机名。

5. 输入该虚拟设备的域后缀。例如，如果虚拟设备的完全限定的域名 (FQDN) 为 `citrix-migrate-vm.domain4.bedford4.ctx4`，则输入 `domain4.bedford4.ctx4`。
6. 输入 **y** 以使用 DHCP 以自动获取 Citrix Hypervisor Conversion Manager 虚拟设备的 IP 地址。否则，请输入 **n**，然后输入 VM 的静态 IP 地址、子网掩码和网关。
7. 检查主机名和网络设置，然后在出现提示时输入 **y**。此步骤将完成 Citrix Hypervisor Conversion Manager 虚拟设备的配置过程。
8. 成功配置该设备后，将显示登录提示。输入登录凭据并按 Enter 键，以登录到 Citrix Hypervisor Conversion Manager 虚拟设备。

完成配置 Citrix Hypervisor Conversion Manager 虚拟设备后，安装 Citrix Hypervisor Conversion Manager 控制台。有关详细信息，请参阅安装 Conversion Manager 控制台。

## 安装 **Conversion Manager** 控制台

配置 Citrix Hypervisor Conversion Manager 虚拟设备后，继续在本地工作站上安装 Citrix Hypervisor Conversion Manager 控制台。Citrix Hypervisor Conversion Manager 控制台是用于执行大多数转换任务的用户界面。从 Citrix Hypervisor Conversion Manager 控制台中，您可以启动转换向导，启动该向导后，您可以选择要转换的 VMware VM。

### 注意：

Citrix Hypervisor Conversion Manager 适用于 Citrix Hypervisor Premium Edition 客户或可通过其 Citrix Virtual Apps and Desktops 授权访问 Citrix Hypervisor 的客户。有关 Citrix Hypervisor 许可的详细信息，请参阅[许可](#)。要升级或购买 Citrix Hypervisor 许可证，请访问 [Citrix Web 站点]。

## 系统要求

支持的来宾操作系统：

Citrix Hypervisor Conversion Manager 支持转换运行 Citrix Hypervisor 支持的任何 Windows 来宾操作系统的 VMware VM。有关 Citrix Hypervisor 支持的 Windows 来宾操作系统的列表，请参阅[来宾操作系统支持](#)。还支持以下 Linux 操作系统。

- RHEL 5.4/5.6/6.4/7.0
- CentOS 5.5/6.3/6.4/6.5/7.0
- SLES 11 SP1/SP2/SP3/SP4
- Ubuntu 14.04/16.04

软件要求：

Microsoft .NET Framework 4.6

安装所需的硬盘驱动器空间：

10 MB

安装

Citrix Hypervisor Conversion Manager 控制台安装在运行 XenCenter 的同一台计算机上。

重要：

- 在安装 Citrix Hypervisor Conversion Manager 控制台之前，请从计算机中删除任何其他版本的控制台。
- Citrix Hypervisor Conversion Manager 控制台取决于浏览器的代理设置。如果 Citrix Hypervisor、ESXi 和 vCenter 只能通过代理服务器访问，则应在浏览器的代理设置中输入代理服务器的详细信息。如果 Citrix Hypervisor、ESXi 和 vCenter 无需通过代理服务器访问，并且用户已将浏览器的代理设置为访问 Internet，则应在浏览器的代理设置的代理例外中添加 Citrix Hypervisor、ESXi 和 vCenter 的地址。

要安装 **Citrix Hypervisor Conversion Manager** 控制台，请执行以下操作：

1. 双击 **convui\_setup.msi**。
2. 在欢迎使用 **Citrix Hypervisor Conversion Manager** 安装向导页面上，单击下一步。
3. 查看许可协议，然后选择我接受许可协议中的条款以接受协议的条款。单击下一步。
4. 在目标文件夹页面上，选择要安装 Conversion Manager 控制台的位置，然后单击下一步。

注意：

默认情况下，Conversion Manager 控制台安装在 `C:\Program Files (x86)\Citrix\XCM` 中。

5. 单击安装以安装 Conversion Manager 控制台。
6. 单击完成。

要删除 **Citrix Hypervisor Conversion Manager** 控制台，请执行以下操作：

1. 打开 Windows 控制面板。
2. 打开程序和功能。
3. 选择 **Citrix Hypervisor Conversion Manager**。
4. 单击卸载。

## 转换 VMware VM

转换 VMware VM 时，它们将被导入运行 Citrix Hypervisor Conversion Manager 虚拟设备的 Citrix Hypervisor 池或独立主机中。转换后的 VM 将保留虚拟处理器和虚拟内存的原始 VMware 设置。

使用 Citrix Hypervisor Conversion Manager 转换 VM 需要执行以下任务：

1. 启动 Citrix Hypervisor Conversion Manager 控制台。
2. 连接到 Citrix Hypervisor 主机。
3. 启动该向导可启动新的转换作业，但是需要指定 VMware 服务器凭据并选择 VM 和存储库。

注意：

- Citrix Hypervisor Conversion Manager 支持使用不同的存储（例如精简预配、密集预配、IDE 和 SCSI）来转换 VMware VM。
- Citrix Hypervisor Conversion Manager 不需要源 VM 即可安装 VMware Tools。您可以对 VMware VM 执行转换，而无论是否安装了 VMware Tools。
- Citrix Hypervisor Conversion Manager 无法将具有四个或更多磁盘的 VMWare VM 转换为 Citrix Hypervisor VM。您的 VMWare VM 必须具有三个或更少的磁盘。

#### 任务 1：启动 **Citrix Hypervisor Conversion Manager** 控制台

要启动 **Citrix Hypervisor Conversion Manager** 控制台，请执行以下操作：

1. 从“开始”菜单中，选择所有程序 > **Citrix** > **Citrix Hypervisor Conversion Manager**。

注意：

每台计算机只能运行 Citrix Hypervisor Conversion Manager 的一个实例。

2. 继续选择连接到 **Citrix Hypervisor**。

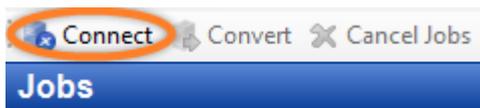
#### 任务 2：连接到 **Citrix Hypervisor** 主机

启动 Citrix Hypervisor Conversion Manager 控制台时，必须将其连接到 Citrix Hypervisor 主机。

在开始之前，请确保具有 Citrix Hypervisor 池（或独立主机）的凭据。接受 root 帐户凭据或配置了“池管理员”角色的基于角色的访问控制 (RBAC) 帐户。

要连接到 **Citrix Hypervisor** 主机，请执行以下操作：

1. 如果在启动 Citrix Hypervisor Conversion Manager 控制台时连接到 **Citrix Hypervisor** 对话框不显示，请单击工具栏中的连接按钮。



2. 在连接到 **Citrix Hypervisor** 对话框中，输入以下详细信息：

- 服务器。输入在其中导入了 Citrix Hypervisor Conversion Manager 虚拟设备的 Citrix Hypervisor 主机的 IP 地址或完全限定的域名 (FQDN)。要查找该 IP 地址，请在 XenCenter“资源”窗口中选择该主机，然后单击搜索选项卡。
- 用户名。为池（或独立主机）输入 Citrix Hypervisor 帐户的用户名。此帐户必须是主机或池的 root 帐户，或具有“池管理员”角色的 RBAC。

有关 RBAC 的详细信息，请参阅 [RBAC 概述](#)。

- 密码。为该帐户输入密码并单击连接。

成功连接到 Citrix Hypervisor 主机后，Citrix Hypervisor Conversion Manager 将显示作业页面。

### 任务 3：启动新的转换作业

在开始转换过程之前，请确保满足以下条件：

- 具有包含要转换的 VM 的 VMware 服务器的凭据。转换过程要求您将 Citrix Hypervisor Conversion Manager 控制台连接到 VMware 服务器。
- 要转换的 VMware 虚拟机已关闭。
- 运行转换后的 VM 的 Citrix Hypervisor 池（或主机）已连接到存储库。存储库必须包含足够的空间以容纳转换后的虚拟磁盘。
- 要转换的 VM 的虚拟磁盘大小小于 2 TiB。
- Citrix Hypervisor 池（或主机）具有转换后的 VM 所使用的网络。

要转换 **VMware VM**，请执行以下操作：

1. 单击作业屏幕中的转换按钮。

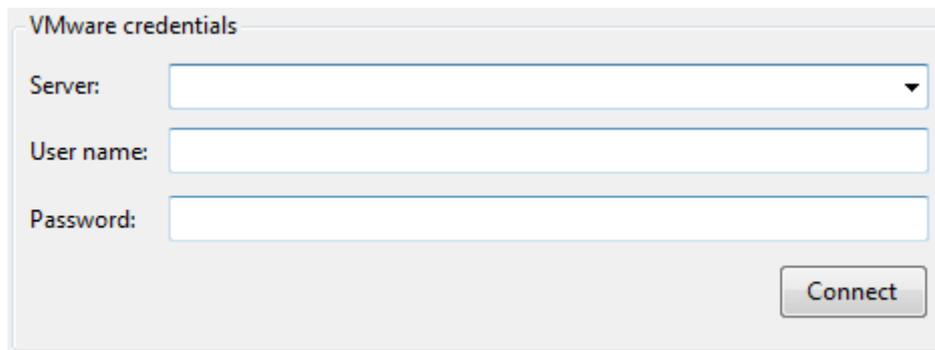


2. 在凭据页面上，输入以下信息，然后单击连接：

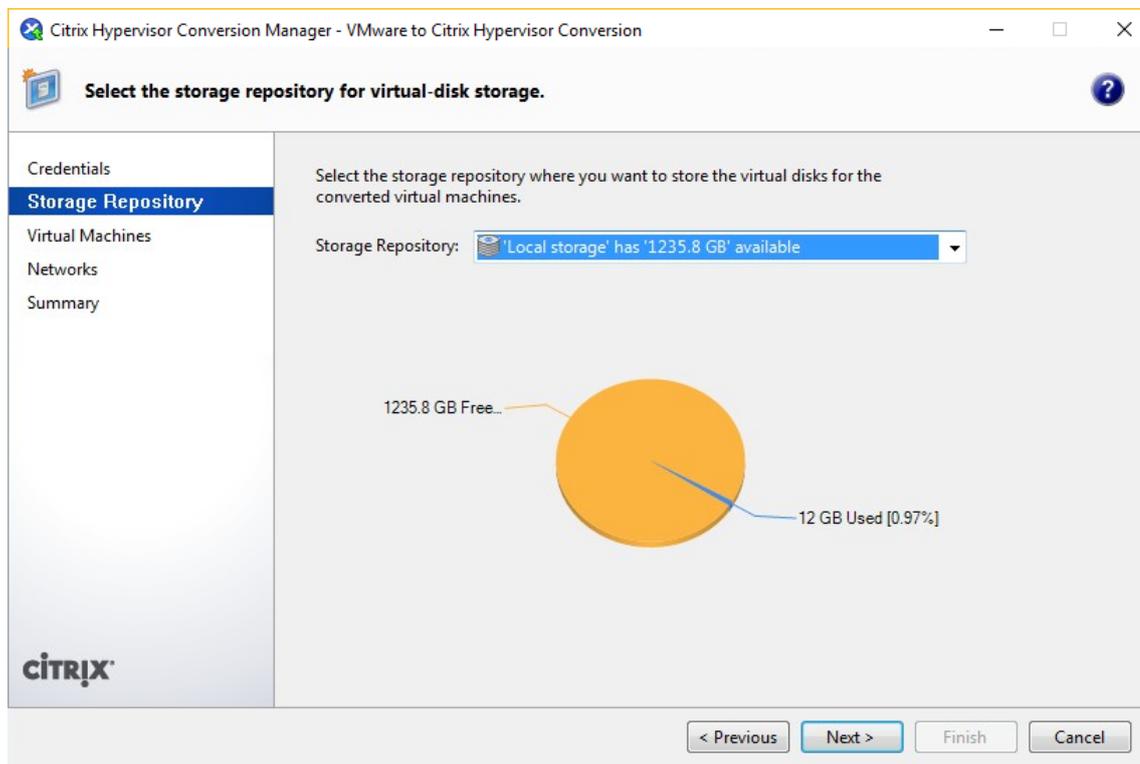
服务器。输入包含要转换为 Citrix Hypervisor 的 VM 的 VMware 服务器的 IP 地址或 FQDN。

用户名。为此 VMware 服务器输入有效的用户名。此帐户必须是 VMware 管理员帐户或具有 Root 用户角色。

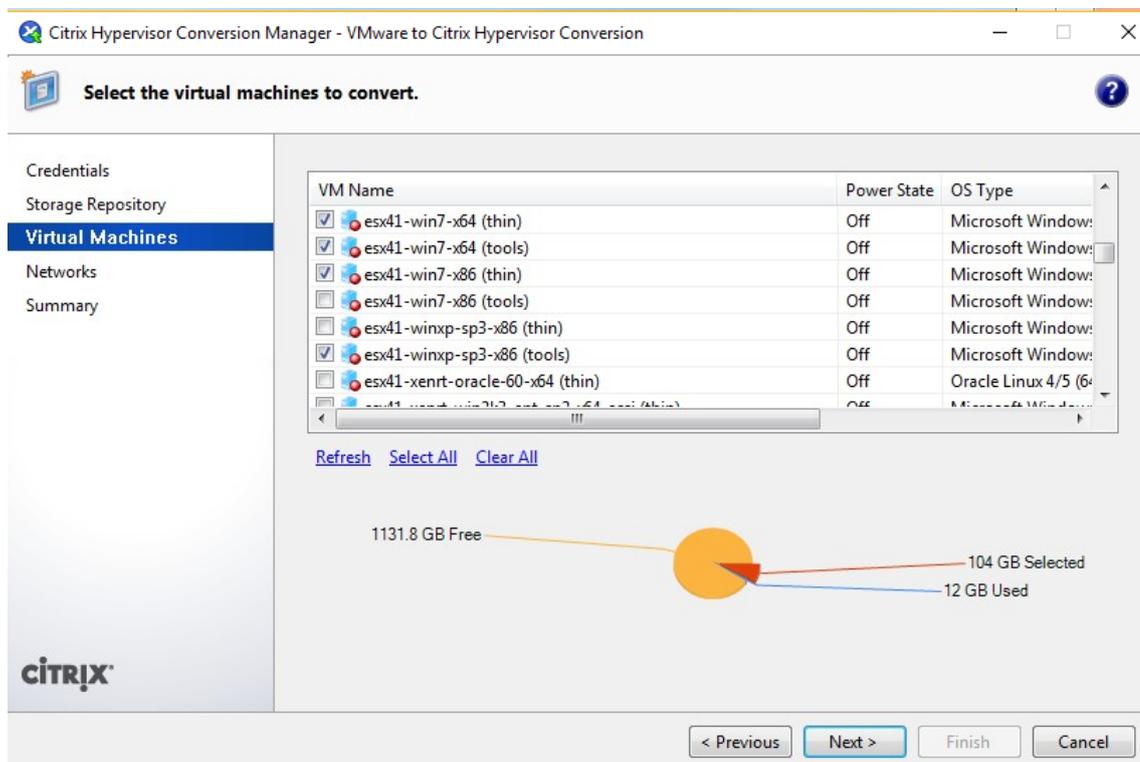
密码。输入用户名框中指定的用户帐户的密码。

A screenshot of the 'VMware credentials' form. It has three input fields: 'Server' (a dropdown menu), 'User name' (a text box), and 'Password' (a text box). A 'Connect' button is located at the bottom right of the form.

3. 在存储库页面上，选择要在转换期间使用的存储库。此存储库是永久存储您创建的 VM 和虚拟磁盘的位置。



4. 在虚拟机页面上，选择要转换的 VMware VM，然后单击下一步。



在选择要转换的 VM 时，红色扇形将变大，以指示转换后的 VM 的虚拟磁盘要占用的可用存储比例。

转换过程中，Citrix Hypervisor Conversion Manager 将为未更新的 Linux VM 下载并安装更新后的内核。如果无权访问 Internet，Citrix Hypervisor Conversion Manager 将从 Citrix Hypervisor Conversion Manager 设备的以下位置安装内核。

```
1 /opt/vpaxcm/conversion/linuxv2v/${
2   distro }
3 /
```

下表列出了转换过程中支持的各种 Linux 操作系统的内核版本。

| 操作系统         | 32 位/64 位 | 建议的内核版本号                 |
|--------------|-----------|--------------------------|
| CentOS 5.5   | 32 位      | 2.6.18-412 (kernel-Xen)  |
| CentOS 6.3   | 32 位      | 2.6.32-642               |
| CentOS 6.4   | 32 位      | 2.6.32-642               |
| CentOS 6.5   | 32 位      | 2.6.32-642               |
| RHEL 5.4     | 32 位      | 2.6.18-164               |
| RHEL 5.6     | 32 位      | 2.6.18-412               |
| RHEL 6.4     | 32 位      | 2.6.32-642               |
| SLES 11 SP3  | 32 位      | 3.0.76-0                 |
| SLES 11 SP4  | 32 位      | 3.0.101-63               |
| Ubuntu 14.04 | 32 位      | 更新 Xen 内核不需要 Internet 连接 |
| Ubuntu 16.04 | 32 位      | 更新 Xen 内核不需要 Internet 连接 |
| RHEL 5.4     | 64 位      | 2.6.18-411               |
| RHEL 5.6     | 64 位      | 2.6.18-411               |
| RHEL 6.4     | 64 位      | 2.6.32-642               |
| RHEL 7.0     | 64 位      | 更新 Xen 内核不需要 Internet 连接 |
| CentOS 5.5   | 64 位      | 2.6.18-412 (kernel-Xen)  |
| CentOS 6.3   | 64 位      | 2.6.32-642               |
| CentOS 6.4   | 64 位      | 2.6.32-642               |
| CentOS 6.5   | 64 位      | 2.6.32-642               |
| CentOS 7.0   | 64 位      | 更新 Xen 内核不需要 Internet 连接 |

---

| 操作系统         | 32 位/64 位 | 建议的内核版本号                 |
|--------------|-----------|--------------------------|
| SLES 11 SP3  | 64 位      | 3.0.76-0                 |
| SLES 11 SP4  | 64 位      | 3.0.101-59               |
| Ubuntu 14.04 | 64 位      | 更新 Xen 内核不需要 Internet 连接 |
| Ubuntu 16.04 | 64 位      | 更新 Xen 内核不需要 Internet 连接 |

---

5. (可选。) 在网络页面上，执行以下一个或多个任务以指定 Citrix Hypervisor Conversion Manager 如何在待转换的 VM 中转换虚拟网络适配器：

更改 **VMware** 网络适配器映射到的任何 **Citrix Hypervisor** 网络。Citrix Hypervisor Conversion Manager 在要转换的 VM 上检测到虚拟网络适配器，并允许您将这些适配器与 Citrix Hypervisor 中的网络关联。转换完成后，新的 VM 将具有连接到您在此步骤中指定的 Citrix Hypervisor 网络的虚拟网络接口。

接受默认网络映射。如果导入 Citrix Hypervisor Conversion Manager 虚拟设备时指定了 VMware 物理网络或 VLAN，则可能要保留此页面上网络的默认设置。

选中“保留虚拟 **MAC** 地址”复选框。Citrix Hypervisor 可以在创建或导入 VM 时自动生成虚拟 MAC 地址。但是，您可能想在 VMware VM 上保留虚拟 MAC 地址，以在使用 DHCP 的环境中保留 IP 地址。有关详细信息，请参阅为满足 **Citrix Hypervisor Conversion Manager** 网络连接要求做好准备。

6. 在摘要页面上，查看转换详细信息并单击“完成”。在转换过程中，状态将显示在作业页面中。

The screenshot shows the Citrix Hypervisor Conversion Manager interface. The main window displays a list of conversion jobs with columns for Name, Source, Destination, Status, Start Time, and Completed Time. The first job, 'Converting Redhat 6.4 32 RHN ...', is currently in progress at 15%. Below the list, the 'Job Summary' section provides details for the selected job, including its ID, destination storage, network and disk usage, and conversion time.

| Name                             | Source                               | Destination                      | Status     | Start Time            | Completed Time        |
|----------------------------------|--------------------------------------|----------------------------------|------------|-----------------------|-----------------------|
| Converting Redhat 6.4 32 RHN ... | dt65.xenrt.citrite.net/Redhat 6.4... | perfuk-01-11/Redhat 6.4 32 RH... | 15%        | 10/26/2016 7:38:42 AM | -                     |
| Converting RedHat_6.4_32         | dt26.xenrt.citrite.net/RedHat_6...   | perfuk-01-11/RedHat_6.4_32       | Completed  | 10/26/2016 7:22:44 AM | 10/26/2016 7:38:42 AM |
| Converting RedHat_6.4_32         | dt26.xenrt.citrite.net/RedHat_6...   | perfuk-01-11/RedHat_6.4_32       | Completed  | 10/26/2016 7:11:07 AM | 10/26/2016 7:14:21 AM |
| Converting Redhat 6.4 32 RHN ... | dt65.xenrt.citrite.net/Redhat 6.4... | perfuk-01-11/Redhat 6.4 32 RH... | Completed  | 10/26/2016 6:36:34 AM | 10/26/2016 6:47:20 AM |
| Converting RedHat_6.4_32         | dt26.xenrt.citrite.net/RedHat_6...   | perfuk-01-11/RedHat_6.4_32       | Completed  | 10/26/2016 6:18:15 AM | 10/26/2016 6:31:45 AM |
| Converting RedHat_6.4_32         | dt26.xenrt.citrite.net/RedHat_6...   | perfuk-01-11/RedHat_6.4_32       | Completed  | 10/26/2016 3:32:11 AM | 10/26/2016 3:46:24 AM |
| Converting RedHat_6.4_32         | dt26.xenrt.citrite.net/RedHat_6...   | perfuk-01-11/RedHat_6.4_32       | Completed  | 10/26/2016 3:11:05 AM | 10/26/2016 3:26:04 AM |
| Converting RedHat_6.4_32         | dt26.xenrt.citrite.net/RedHat_6...   | perfuk-01-11/RedHat_6.4_32       | Completed  | 10/26/2016 1:47:44 AM | 10/26/2016 1:54:42 AM |
| Converting RedHat_6.4_32         | dt26.xenrt.citrite.net/RedHat_6...   | perfuk-01-11/RedHat_6.4_32       | Completed  | 10/25/2016 9:40:48 AM | 10/25/2016 9:54:37 AM |
| Converting RedHat_6.4_32         | dt26.xenrt.citrite.net/RedHat_6...   | perfuk-01-11/RedHat_6.4_32       | Completed  | 10/25/2016 8:51:13 AM | 10/25/2016 9:11:12 AM |
| Converting Redhat 6.4 32 RHN ... | dt65.xenrt.citrite.net/Redhat 6.4... | perfuk-01-11/Redhat 6.4 32 RH... | Completed  | 10/25/2016 8:17:15 AM | 10/25/2016 8:37:14 AM |
| Converting Redhat5.4_x86_32      | dt78.xenrt.citrite.net/Redhat5.4_... | perfuk-01-11/Redhat5.4_x86_32    | Completed  | 10/25/2016 7:52:31 AM | 10/25/2016 7:58:14 AM |
| Converting Redhat5.4_x86_32      | dt78.xenrt.citrite.net/Redhat5.4_... | perfuk-01-11/Redhat5.4_x86_32    | Completed  | 10/25/2016 7:35:22 AM | 10/25/2016 7:40:29 AM |
| Converting RedHat_6.4_32         | dt26.xenrt.citrite.net/RedHat_6...   | perfuk-01-11/RedHat_6.4_32       | Completed  | 10/25/2016 6:54:54 AM | 10/25/2016 7:08:38 AM |
| Converting RedHat_5.6_32         | dt26.xenrt.citrite.net/RedHat_5...   | perfuk-01-11/RedHat_5.6_32       | Completed  | 10/25/2016 6:49:32 AM | 10/25/2016 6:54:54 AM |
| Converting Redhat5.4_x86_32      | dt78.xenrt.citrite.net/Redhat5.4_... | perfuk-01-11/Redhat5.4_x86_32    | Incomplete | 10/25/2016 6:31:29 AM | 10/25/2016 6:36:39 AM |
| Converting CentOS6_5_32          | dt78.xenrt.citrite.net/CentOS6.5...  | perfuk-01-11/CentOS6.5_32        | Completed  | 10/25/2016 3:44:41 AM | 10/25/2016 3:55:54 AM |
| Converting CentOS6_4_32          | dt78.xenrt.citrite.net/CentOS6.4...  | perfuk-01-11/CentOS6.4_32        | Completed  | 10/25/2016 3:34:48 AM | 10/25/2016 3:44:41 AM |

**Job Summary**

ID: 636130640980581810 [Get additional log information...](#)

Destination SR: Local storage

Network read: 0.59 compressed GB

Disk write: 1.41 GB

Total conversion time: -

Status: [Running] Importing VM disks from ESXi/vSphere. This could take several minutes, depending on the size of the disks.

注意：

从 ESXi 或 vSphere 进行的转换可能需要几分钟时间，具体取决于虚拟磁盘的大小。

#### 任务 4：转换后执行的步骤

转换完成后，打开 XenCenter 并对新转换的 VM 执行以下步骤：

在 **Windows** 计算机上：

1. 在 Windows VM 上，根据 Microsoft 许可模型，您可能需要重新激活 VM 的 Windows 许可证。发生此情况的原因是，Windows 操作系统会在硬件发生变化后察觉到进行了转换。
2. 在 Windows VM 上，安装 Citrix VM Tools 以获取高速 I/O，从而增强磁盘并提升网络性能。Citrix VM Tools 还支持某些功能和特性，包括彻底关闭、重新启动、挂起和实时迁移 VM。

如果要使用未安装 Citrix VM Tools 的 VM，则“属性”窗格中的常规选项卡上将显示“未安装 Citrix VM Tools”的消息。对于 Windows VM，可以双击此文本以切换至 VM 控制台，加载 Citrix VM Tools ISO 并启动 Citrix VM Tools 安装向导。

注意：

必须在每个 VM 上安装 Citrix VM Tools，才能使 VM 具有完全受支持的配置。虽然 VM 可以在未安装 Citrix VM

Tools 的情况下正常运行，但是其性能会受到影响。

## 在 Linux 计算机上启用 VNC

在 Linux VM 上，执行以下步骤以配置 VNC 服务器。

注意：

VNC 密码必须至少包含 6 个字符。

### 对于 CentOS 5.5 和 RHEL 5.4/5.6

1. 自定义基于 RHEL 的 VM 防火墙以使用以下命令打开 VNC 端口：

```
1 system-config-securitylevel-tui
```

2. 选择自定义，然后将 **5900** 添加到 \*\* 其他端口列表中。或者，也可以通过运行以下命令在下次重新启动前一直禁用防火墙：

```
1 service iptables stop
```

3. 对于 CentOS 5.5 和 RHEL 5.4/5.6，如果 VNC 图形控制台未正确显示，请运行：

```
1 init 5
```

然后检查图形控制台是否正确显示。

### 对于 CentOS 6.3/6.4/6.5 和 RHEL 6.4

1. 设置 VNC 密码

```
1 vncpasswd
```

2. 重新启动 VNC 服务器

```
1 service vncserver start
```

3. 对于防火墙设置，请打开文件 `/etc/sysconfig/iptables` 并添加以下行：

```
1 -A INPUT -m state --state NEW -m tcp -p tcp --dport 5900 -j ACCEPT
```

注意：

在以下命令后面添加上述行：`-A INPUT -j REJECT \--reject-with icmp-host-`

```
prohibited:
```

4. 输入以下命令以重新启动 iptables:

```
1 \>service iptables restart
```

#### 对于 SLES Linux Enterprise Server 11 SP3 到 SP4

1. 在启动控制台中设置 VNC 密码。

```
1 vncpasswd
```

问题 `Would you like to enter a view-only password(y/n)?` n 的答案 n

2. 按如下所示配置防火墙设置:

- a) 在 VM 中打开文本控制台，然后运行 YaST 实用程序:

```
1 yast
```

- b) 使用箭头键选择左侧菜单中的 **Security and Users** (安全性与用户)，然后按 Tab 键切换到右侧菜单并使用箭头键选择 **Firewall** (防火墙)。按 **Enter** 键。
- c) 在 **Firewall** (防火墙) 屏幕中，使用箭头键选择左侧菜单中的 **Custom Rules** (自定义规则)，然后按 **Enter** 键。
- d) 按 Tab 键切换到 **Custom Allowed Rules** (自定义允许的规则) 部分中的 **Add** (添加) 按钮，然后按 **Enter** 键。
- e) 在 **Source Network** (源网络) 字段中，输入 **0/0**。按 Tab 键切换到 **Destination Port** (目标端口) 字段并输入 **5900**。
- f) 按 Tab 键切换到 **Add** (添加) 按钮，然后按 **Enter** 键。
- g) 按 Tab 键切换到 **Next** (下一步) 按钮，然后按 **Enter** 键。在 **Summary** (摘要) 屏幕中，按 Tab 键切换到 **Finish** (完成) 按钮并按 **Enter** 键。最后，在顶层 YaST 屏幕中，按 Tab 键切换到 **Quit** (退出) 按钮并按 **Enter** 键。

3. 单击 **Switch to Graphical Console** (切换到图形控制台)。
4. 如果图形控制台未正确显示，请切换到 **Text Console** (文本控制台)，然后运行以下命令:

```
1 /etc/init.d/vncserver restart
```

5. 单击 **Switch to Graphical Console** (切换到图形控制台)。

**注意：**

- 对于其他图形控制台显示问题，请运行：`/etc/init.d/vncserver restart`。
- SLES 11 SP3 到 SP4 不支持转换配备了 IDE 磁盘的 VM。

### 其他转换任务

此部分列出了在转换 VM 时可能要执行的其他任务。这些任务包括清除作业、保存作业摘要、重试作业、取消作业，以及显示日志文件。

#### 清除所有作业

在作业菜单中，选择清除作业。

#### 保存作业摘要

在文件菜单中，单击保存作业摘要。

#### 重试作业

单击重试作业。

**注意：**

只能针对失败的作业或取消的作业启用重试作业选项。

#### 取消作业

单击取消作业。

**注意：**

只能针对已排队的作业或正在运行的作业启用“取消作业”。

### 保存 **Citrix Hypervisor Conversion Manager** 应用程序日志文件

1. 在帮助菜单中，选择保存支持日志文件。
2. 在系统提示时，指定要将 Citrix Hypervisor Conversion Manager 控制台 (`XCMUI.log`) 和 Citrix Hypervisor Conversion Manager 虚拟设备 (`XCM.log`) 日志的日志文件存储到的位置。

#### 显示转换详细信息

1. 选择 Citrix Hypervisor Conversion Manager 作业窗口中的作业。
2. 在作业摘要窗格中，单击获取其他日志信息链接。

Citrix Hypervisor Conversion Manager 将从 Citrix Hypervisor Conversion Manager 虚拟设备中检索日志，并在文本编辑器中显示结果。

#### 获取日志详细信息

Windows 和 Linux 客户机的日志都存在于 `/var/log/conversion/convsvc.log` 文件中。如果转换失败，请单击获取其他日志信息按钮以查看详细信息。对于 Linux VM，其他日志都存在于 `/var/log/conversion/linuxxenfix.log` 中。

#### 对转换进行故障排除

此部分提供了有关对转换过程和转换后的 VM 进行故障排除的信息。

#### 启动转换后的 VM 时出现问题

一般情况下，转换会平稳运行且 Citrix Hypervisor Conversion Manager 转换 VM 时不会出现任何问题。但是，在极少数情况下，可能会在尝试打开转换后的 VM 时收到错误。以下部分提供有关如何解决错误和其他问题的一些指导。

#### 蓝屏并显示 **Windows** 停止代码 **0x0000007B**

此停止代码指示 Citrix Hypervisor Conversion Manager 无法配置对首次启动 Citrix Hypervisor 至关重要的 Windows 设备。保存日志并将其发送给 Citrix 技术支持以获取更多指导。

#### **Windows** 产品激活

根据您的许可模式，尝试启动 Windows VM 时，可能会显示一条有关系统激活的错误消息。

注意：

从 ESXi 或 vSphere 进行的转换可能需要几分钟时间，具体取决于虚拟磁盘的大小。

#### **Windows VM** 中的网络设置丢失

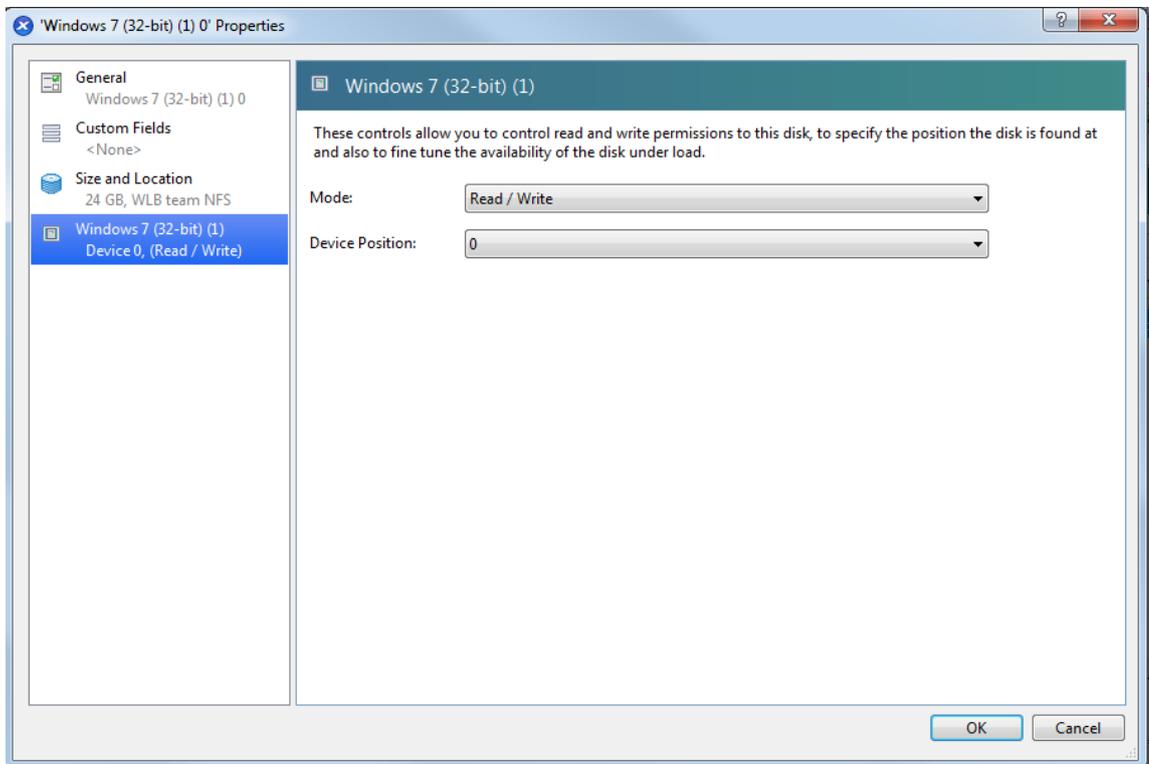
如果将 Windows VM 从 ESXi 服务器导入到 Citrix Hypervisor，IPv4/IPv6 网络设置可能会丢失。要保留网络设置，请在完成转换后重新配置 IPv4/IPv6 设置。

### 无法启动 VMware SCSI 磁盘

如果 VMware VM 从 SCSI 磁盘启动，但还配置了一个或多个 IDE 硬盘驱动器，则 VM 在您将其转换为 Citrix Hypervisor 时可能不启动。这是因为迁移过程分配的 IDE 硬盘设备编号比 SCSI 磁盘的硬盘设备编号小。但是，Citrix Hypervisor 从分配了设备 0 的硬盘启动。要解决此问题，请重新安排虚拟磁盘在 XenCenter 中的位置，以便 VM 从包含操作系统的虚拟磁盘重新启动。

要更改包含操作系统的虚拟磁盘的位置，请执行以下操作：

1. 在 XenCenter“资源”窗格中，选择已关闭的来宾 VM。
2. 选择存储选项卡。
3. 在虚拟磁盘页面上，选择包含操作系统的虚拟磁盘，然后单击属性。
4. 在 **\*operating\_system\*** 属性对话框中，单击 **operating\_system** 选项卡以显示设备选项。



5. 在设备位置列表中，选择 **0**，然后单击确定。

### 转换过程中出现问题

如果您在转换 Linux VM 时看到任何错误，请删除转换后的 VM，重新启动 Citrix Hypervisor Conversion Manager 虚拟设备并重试。失败转换的日志存储在 `/var/log/xensource.log` 中。在联系 Citrix 技术支持以提出任何问题时，我们建议您提供日志文件以进行故障排除。

## vSwitch 和 Controller

June 4, 2019

vSwitch 可以查看和控制 Citrix Hypervisor 虚拟化网络环境并增强其安全性。它由以下组件组成：

- *vSwitch*，即在每个 Citrix Hypervisor 上运行的能够感知虚拟化的交换机
- *vSwitch Controller*，即集中式服务器，用于管理和协调每个单独的 vSwitch 的行为以提供单个 vSwitch 的外观

vSwitch Controller 支持细化的安全策略，以控制传入和传出 VM 的通信流。它提供虚拟网络环境中所有流量的行为和性能的详细视图。vSwitch 大大简化了您的环境中的 IT 管理工作。使用 vSwitch 时，即使它从一个物理主机迁移到另一个物理主机，VM 配置和统计信息会保持绑定到 VM。

### 快速入门

#### 要求

- 至少在 XenCenter 中配置一个 Citrix Hypervisor 资源池
- 该池中有足够的容量来部署 vSwitch Controller 虚拟设备

下一节介绍了运行控制器的主机的要求。

### 进程

设置 vSwitch Controller 涉及以下任务：

1. 部署 vSwitch Controller 虚拟设备
2. 访问 vSwitch Controller
3. 配置 vSwitch Controller IP 地址
4. 添加资源池
5. 配置高可用性（可选）

#### 注意：

本版本的 vSwitch Controller 可以与所有受支持版本的 Citrix Hypervisor 互操作。

### 部署 vSwitch Controller 虚拟设备

运行 vSwitch Controller 的 Citrix Hypervisor 服务器必须满足以下最低要求：

- 2 个 CPU
- 2 GB DRAM

- 16 GB 磁盘

vSwitch Controller 设备的最低允许 VM 配置和导入的默认配置为：

- 2 个 vCPU
- 2 GB DRAM
- 16 GB 磁盘

此配置支持连接到 vSwitch Controller 的由多达 16 个 Citrix Hypervisor 服务器和 256 个虚拟接口 (VIF) 组成的池。对于较大的池（所有池达到最大受支持的限制：总计 64 个 Citrix Hypervisor 服务器和 1024 个 VIF），请将 VM 配置修改为：

- 4 个 vCPU
- 4 GB DRAM
- 16 GB 磁盘

注意：

- 如果该设备的磁盘存储在网络存储中，并将控制基础 XenServer 主机的网络流量，则在已加载的情况下可能会出现死锁，并且整个池的网络流量可能会停止传递。要防止出现此情况，Citrix 强烈建议客户将 DVSC 磁盘存储在本地存储上或将设备移入不由该 DVSC 控制的另一个池。
- 对于每个池，您必须将池大小限制为 16 个以下的主机。

vSwitch Controller VM 可以在其管理的资源池中运行。通常情况下，此配置的运行方式犹如 vSwitch Controller VM 是单独运行的。但是，在发生 Controller 迁移或重新启动时，连接所有 vSwitch 可能需要花费稍微长一点的时间（最多 2 分钟）。此时间的产生原因是，各个 vSwitch 路由器控制连接的方式不同。

要安装 vSwitch Controller，请将提供的虚拟设备 VM 映像导入 Citrix Hypervisor 资源池。在导入过程中，将导入的 VM 连接到网络，您可以通过网络访问您要控制的主机或池。

导入 VM 后，启动 VM 以开始执行配置 DVS 的过程。

### 访问 **vSwitch Controller** 命令行接口

您可以从 XenCenter 中访问 vSwitch Controller 命令行接口 (CLI) 或远程使用 SSH 客户端。vSwitch Controller VM 首次启动时，XenCenter 中的控制台将显示要用于远程访问 Controller 的 IP 地址。如果 VM 未收到 IP 地址，文本控制台将指示必须通过 CLI 分配地址。在任一情况下，文本控制台将在 XenCenter 控制台中显示在本地登录 CLI 的登录提示。[命令行接口](#)中包含可用 CLI 命令的完整文档。

### 访问 **vSwitch Controller GUI**

使用 Web 浏览器远程访问 vSwitch Controller GUI 或在 XenCenter 控制台中进行本地访问。

vSwitch Controller VM 启动时，XenCenter 中的控制台将显示用于远程访问 GUI 的 IP 地址。如果 VM 未收到 IP 地址，则无法在本地或远程使用 GUI，直到分配了一个 IP 地址为止。控制台将提供在命令行接口中本地设置 IP 地址的说明。Controller VM 具有 IP 地址后，您可以在 XenCenter 控制台中本地访问 GUI。

注意：

如果 VNC 处于禁用状态，则只能从 Web 浏览器访问 vSwitch Controller GUI。

## 远程访问 vSwitch Controller GUI

要远程访问 vSwitch Controller 接口，请执行以下操作：

1. 打开浏览器并键入以下 URL，其中 *server* 是 Controller VM 的 IP 地址或主机名：`https://server-name:443/`
2. 键入您的用户名和密码，然后单击登录。默认管理员用户名和密码是 **admin** 和 **admin**。

注意：

默认情况下，vSwitch Controller Web 服务器使用自签名证书。证书可能会导致浏览器在连接到 GUI 时显示安全错误。您可以安全地忽略该错误并将证书安装到您的浏览器中。

支持以下浏览器：Firefox 3.x、Safari 4.x、Internet Explorer 7 和 8。其他具有相似功能的现代浏览器（例如，Opera 或 Google Chrome）不受支持，但可能会起作用。Internet Explorer 9 解决了已知的内存和资源泄漏问题。但是尚未经过全面测试。

首次登录时，系统会提示您更改默认管理员密码。请务必创建强管理员密码以保护环境的安全。

## 配置 vSwitch Controller IP 地址

首次启动 vSwitch Controller 时，它会尝试使用 DHCP 获取 IP 地址。但是，我们建议您分配静态 IP 地址。如果配置了 DHCP，则无法将资源池设置为防故障模式

要分配静态 IP 地址，请执行以下操作：

1. 在本地访问 vSwitch Controller 接口。
2. 在侧面板中选择设置选项卡，然后选择 **IP** 配置。此时将显示当前设置。
3. 选择修改配置，指定新 IP 地址信息，然后选择 **Make Changes**（更改）。
4. 重新启动 vSwitch Controller 虚拟设备。

## 添加资源池

添加资源池即表示允许 vSwitch Controller 开始自动管理该池中的所有 Citrix Hypervisor 服务器。

要添加资源池，请执行以下操作：

1. 在 **Visibility & Control**（可见性和控制）下，打开状态选项卡并在资源树中选择 **All Resource Pools**（所有资源池）以打开所有资源池的状态页面。
2. 单击添加资源池。如果没有添加其他资源池所需的正确许可证，将显示一条错误消息。

3. 在池主服务器 **(DNS/IP)** 框中键入主服务器 Citrix Hypervisor 服务器的 IP 地址或 DNS 名称。
4. 键入用户名和密码以获取对服务器的管理访问权限。

在资源池中，用户必须具有完全管理功能能力。该帐户具有受限功能时，vSwitch Controller 无法正确管理该池。

通常情况下，此帐户是名为 `root` 的用户，但是当 Citrix Hypervisor 平台的 RBAC 功能处于使用状态时，此帐户可以是不同的名称。

5. 仅当要覆盖此资源池的任何现有 vSwitch Controller 配置时，才能选中盗用框。
6. 单击连接。

vSwitch Controller 使用提供的用户名和密码与使用 XAPI 协议的池主服务器使用进行通信。建立通信后，新资源池以及所有相关联的资源将被添加到资源树中。如果 vSwitch Controller VM 无法与池主服务器进行通信，它将显示一条错误消息，以描述通信失败情况。

**注意：**

要使 vSwitch Controller 与 Citrix Hypervisor 资源池通信，Citrix Hypervisor 资源池必须使用向后兼容模式。此模式是默认设置。您可以在 XenCenter 中的池属性页面上指定此设置。有关详细信息，请参阅 *XenCenter* 帮助。

### 配置高可用性功能

为确保 Citrix Hypervisor 服务器始终能够访问活动的 vSwitch Controller，请使用 vSwitch Controller VM 的 Citrix Hypervisor 高可用性。有关在 Citrix Hypervisor 上启用高可用性的详细信息，请参阅[高可用性](#)。vSwitch Controller 的持续正常运行对于所有 VM 的联网操作至关重要。为确保 vSwitch Controller VM 的高可用性，请将其 `restart-priority` 设置为 1，将 `ha-always-run` 设置为 true。

## 管理 vSwitch

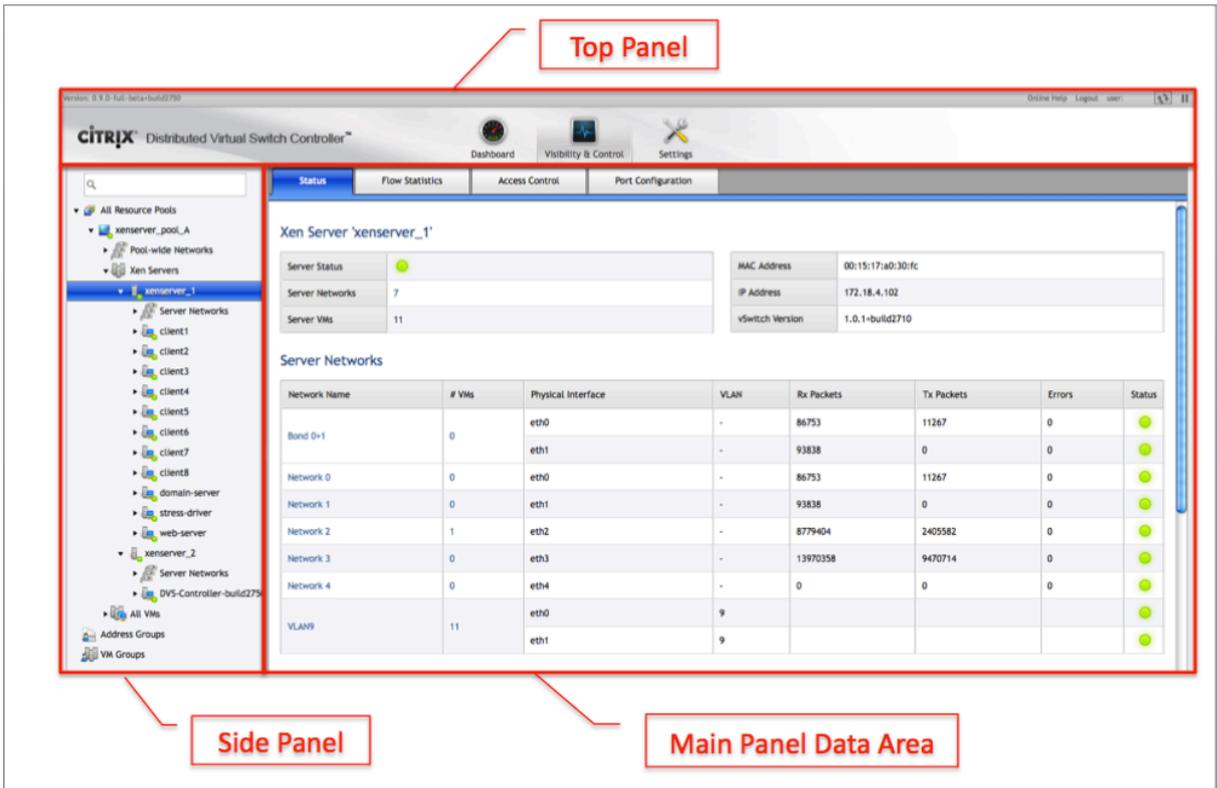
June 4, 2019

使用 vSwitch Controller GUI 可以执行各种管理任务，包括：

- 查看虚拟网络中各元素的状态和流统计信息
- 设置 VM 访问控制、服务质量和流量镜像策略
- 修改 vSwitch Controller 虚拟设备的配置

### 界面概述

vSwitch Controller GUI 有三种不同的面板。这些面板如下图中所示。



## 顶部面板

在使用 GUI 时，顶部面板始终可见且包含一个状态栏和一组主要导航图标。

## 状态栏

vSwitch Controller 窗口顶部的灰色状态栏包含以下信息和功能（从左到右）：

- 版本：当前 vSwitch Controller 版本。
- 联机帮助：单击以显示或关闭靠近 Controller 窗口顶部的联机帮助区域。
- 注销：单击以注销 vSwitch Controller GUI。
- 用户：显示当前登录的用户的用户名。
- 刷新图标：单击以更新页面上的信息。
- 播放/暂停：单击以对 GUI 是否使用后台更新自动刷新屏幕上的数据进行切换。在播放模式下，显示的数据将每隔 15 秒自动刷新一次。在暂停模式中，大多数数据不会更新。但是，少数几个元素会更新，尤其是资源树。按钮后面的状态栏背景将变为橙色，并且在处于暂停模式时，“数据更新已暂停”指示器将显示在状态栏中。

## 顶部图标

单击顶部图标可访问 GUI 中的主要功能区域。

- 控制板：查看汇总统计信息以及有关网络和管理事件的信息。请参阅使用控制板监视网络状态。
- 可见性和控制：查看网络状态和统计信息或配置访问控制、QoS，以及虚拟网络的流量镜像策略。请参阅[虚拟网络可见性和控制](#)。
- 设置：执行 vSwitch Controller 维护和管理功能。请参阅[管理和维护 vSwitch Controller](#)。

## 侧面板

侧面板仅在“可见性和控制”和“设置”部分中可用。

对于“可见性和控制”部分，侧面板包含可用于浏览虚拟网络环境中的网络元素的资源树。与 XenCenter 中的资源树类似，元素按照层次结构进行组织，并提供了一种浏览系统中元素的简单方法。要展开资源树的某个部分，请单击节点文本旁边的侧向箭头。已展开的节点标有向下箭头，您可以单击该箭头进行折叠。

从资源树中选择某个元素后，主面板将在树中显示该节点的状态和配置数据。例如，如果您从资源树中选择某个 VM，并在可见性和控制部分中选择状态，主面板将显示所选 VM 的状态信息。

资源树包含搜索功能。要基于搜索字符串过滤内容，请在搜索字段中输入文本，然后按 **Enter** 键。单击 **X** 符号以清除搜索。搜索支持通配符（对于一个或多个字符，使用 \*，对于单个字符，使用 ?）。如果未使用通配符，系统将执行子字符串搜索，犹如 \* 通配符位于搜索字符串的开头和结尾。例如，搜索“Lab”可找到名称中带有“Lab”的所有项目，例如“Laboratory-1”和“New-Lab-5”。

对于“设置”部分，侧面板包含用于选择用户要查看或修改哪部分 vSwitch Controller 配置的图标

## 使用资源树

在最高级别，资源树将显示以下项目：

- 所有资源池：所有可用资源池的列表。此列表是顶级资源，用于查看所有 Citrix Hypervisor 服务器、网络、VM 和属于每个资源池的 VIF。
- 地址组：指定的 IP 地址和子网范围集。这些组用于以下目的：
  - 限制在访问控制部分中应用规则
  - 限制流统计信息部分中的查询范围
- VM 组：指定的 VM 集，用于简化查看特定 VM 集合的状态和流统计信息的过程。

当您展开资源树中的资源池时，将显示以下项目：

- 池范围的网络：此列表包括资源池中的所有网络，且与 XenCenter 的“网络”选项卡中的列表类似。您可以展开该列表以显示各个网络、展开某个网络以显示该网络中的 VM，以及展开某个 VM 以显示该网络中该 VM 的 VIF。
- Citrix Hypervisor 服务器。此列表与 XenCenter 中的服务器层次结构类似。您可以展开该列表以显示池中的所有服务器，也可以展开一个服务器条目以显示网络、VM 以及与服务器关联的 VIF。服务器网络列表与您在单击 XenCenter 中的服务器并选择“网络”选项卡时显示的内容类似。
- 所有 VM：不管是否为单个服务器配置了 VM，此列表都会显示资源池中的所有 VM。您可以展开该列表以显示各个 VM，然后展开某个 VM 以显示其 VIF。

节点上的右键单击上下文菜单在大多数节点上均可用，可提供一种在资源树中添加、修改和删除项目的简单方式。

### 采用颜色编码的图标

资源树中彩色编码的图标显示顶级“所有资源池”节点下的树节点的状态。与 XenCenter 类似，这些颜色代码基于通过 XAPI 从每个池主服务器检索到的数据。节点状态发生改变时，图标将更新为如下所示：

- 绿色：绿色图标表示资源在网络上处于活动状态且由 vSwitch Controller 正确托管。
- 红色：对于“资源池”节点，红色表示无法建立与池主服务器的 XAPI 连接。如果“资源池”节点为绿色，则其下面的所有节点的红色图标表示元素当前在网络上不处于活动状态。例如，该元素已关闭或断开连接。
- 橙色：橙色图标表示节点或其子节点之一未正确连接或受到正确托管。关联资源的状态页面将显示一条描述该问题的错误消息。

树菜单项上的颜色代码也将显示在该节点的“状态”页面上。有关颜色代码和状态信息的详细信息，请参阅[对 vSwitch Controller 问题进行故障排除](#)。

### 主面板数据区域

主面板数据区域包含状态信息、统计信息和配置设置。

- 控制板：无侧边菜单，并且主面板数据区域占用了顶部面板下的整个区域。控制板主面板概述了由 vSwitch Controller 托管的所有虚拟网络。
- 可见性和控制：主面板占用顶部面板下的右侧窗口。该面板包括顶部对应于以下重要可见性和控制功能的选项：
  - 状态：查看选定资源树节点的详细状态信息。
  - 流统计信息：查看选定节点的网络活动图和数据。
  - 访问控制：设置选定节点的访问控制策略。
  - 端口配置：设置选定节点的服务质量和流量镜像策略。
- 设置：主面板占用顶部面板下的右侧窗口。设置主面板显示的详细信息将用于基于在侧面板中选择的子区段查看或配置 vSwitch Controller 设置。

在“可见性和控制”部分中，主面板中显示的数据将发生更改，以反映您在侧面板中选择的层次结构级别和特定项目。

例如，如果您在侧面板中选择资源池并单击“访问控制”选项卡，则主面板将显示以下内容：

- 全局访问控制安全策略
- 选定资源池的策略

如果您从侧面板中选择虚拟接口 (VIF) 并单击“访问控制”选项卡，则主面板将显示：

- 全局访问控制安全策略
- 包含 VIF 的资源池的策略
- 包含 VIF 的 VM 的策略
- 选定 VIF 的策略

## 使用控制板监视网络状态

控制板显示汇总统计信息以及有关虚拟网络环境中事件的信息。要显示控制板，请单击 vSwitch Controller 接口顶部的控制板图标。

控制板将划分为此部分中所述的各个区域。信息每隔几秒钟就会自动更新一次。

### 服务器统计信息

此部分提供有关 vSwitch Controller 的以下常规信息。

- 运行时间：自 vSwitch Controller 上次启动以来的时间长度。
- CPU 负载：vSwitch Controller 虚拟设备的当前 CPU 使用率百分比。

### 网络统计信息

此部分显示网络元素的清单（资源池、Citrix Hypervisor 服务器、网络 and VM）对于每个以下类别：

- 托管：根据 XAPI 处于运行状态且当前由 vSwitch Controller 托管的此类型的元素数。
- 活动：根据 XAPI 处于运行状态的此类型的元素数。包括托管和非托管元素。
- 总计：通过 XAPI 已知存在的此类型的元素数。

当系统正确配置和运行时，托管和活动计数是相同的。总计数始终等于或大于托管和活动计数。已关闭的组件不会显示为由 Controller 托管。

### 最新的网络事件

此部分列出了自 vSwitch Controller 上次重新启动以来托管虚拟网络中发生的最新事件。使用右侧的滚动条来滚动浏览列表。最新的事件将首先列出。随着时间的推移，较旧的事件将从列表中删除。

将为每个网络事件报告以下信息：

- 优先级：事件的相对重要性。
- 日期/时间：事件发生的日期和时间。
- 事件：事件的说明。您可以单击事件说明中的超链接以访问事件中提及的网络元素的相应“可见性和控制”状态页面。

可以将网络事件导出到 syslog 服务器以进行更永久地记录。有关详细信息，请参阅[导出 syslog 文件](#)。

### 最新的管理事件

此部分列出 vSwitch Controller 中发生的事件，通常是由于管理员在 GUI 中更改配置所致。使用右侧的滚动条来滚动浏览列表。最新的事件将首先列出。随着时间的推移，较旧的事件将从列表中删除。

将为每个管理事件报告的以下信息：

- 优先级：事件的相对重要性。
- 日期/时间：事件发生的日期和时间。
- 事件：事件的说明。您可以单击事件说明中的超链接以访问事件中提及的网络元素的“可见性和控制”状态页面。

可以将网络事件导出到 `syslog` 服务器以进行更永久地记录。有关详细信息，请参阅[导出 syslog 文件](#)。

### 吞吐量、流和比特率图表

这些图表显示最活跃的 VM 和协议的相关行为信息。

图表将显示以下信息：

- 过去一小时的总吞吐量（比特/秒）
- 过去一小时的总数据包速率（数据包/秒）
- 过去一小时的总连接速率（流/秒）

## 虚拟网络可见性和控制

June 4, 2019

“Visibility and Control”（可见性和控制）部分允许您监视网络行为和配置网络策略。要访问各个页面，请选择 vSwitch Controller 界面顶部的 **Visibility and Control**（可见性和控制）图标。

### 查看状态

状态选项卡以表格形式提供有关在资源树中选择的节点的详细信息。显示的信息类型因选定节点而异。最独特的表格条目是链接。您可以单击这些链接以显示适用于该表格条目的状态页面。

即使 Citrix Hypervisor 服务器重新启动或 VM 重新启动或迁移，所有字节计数和错误计数还是会继续累积。颜色代码遵循与侧面板中的颜色代码相同的规则。请参阅[采用颜色编码的图标](#)。

### 全局级别

在全局级别，“状态”页面会显示一个表格，该表格列出了所有资源池和以下信息：

- 资源池：资源池的名称。
- 服务器数：池中的服务器数。
- 网络数：池中的网络数。
- VM 数：池中的 VM 数。
- 状态：显示当前池状态的采用颜色编码的图标。

单击某行右侧的齿轮图标可提供用于修改资源池的各种选项。

在此页面上，您还可以为端口配置策略指定可用的目标 VLAN。请参阅设置端口配置策略。

#### 资源池级别

对于选定资源池，“状态”页面将显示以下信息：

- 状态：显示当前池状态的采用颜色编码的图标。
- 池主服务器：池中主服务器的 IP 地址或 DNS 名称。
- 池范围的网络数：池中的网络数。
- Citrix Hypervisor：池中的服务器数。
- 所有 VM：池中的 VM 数。
- 服务器列表：池中的服务器的列表，包括服务器名称、网络数、VM 数和状态。

除了显示状态信息以外，您还可以配置池中的 Citrix Hypervisor 服务器转发 Netflow 数据的方式。根据需要选中以下复选框，然后单击 **Save Netflow Configuration**（保存 Netflow 配置）：

- vSwitch Controller（默认情况下处于选中状态）：将 Netflow 信息转发到 vSwitch Controller 以供 GUI 的“Flow Statistics”（流统计信息）部分使用。如果取消选中此复选框，Netflow 数据将不会发送到 vSwitch Controller，并且“流统计信息”页面将不显示数据。
- 外部 Netflow 控制器：允许您将 Netflow 数据转发到外部第三方 Netflow 收集器。输入外部收集器的 IP 地址。

#### 防故障模式

使用故障模式部分配置 vSwitch 在无法连接到其 vSwitch Controller 时强制执行访问控制规则的方式。请务必保持较高级别的 vSwitch Controller 可用性，以避免数据丢失。在 vSwitch Controller 不可用的时间段内，以下故障模式适用：

- 故障时打开：在 vSwitch 能够通过 vSwitch Controller 重新连接之前，允许所有流量，之前定义的 ACL 将不再适用。
- 防故障：现有 ACL 继续适用。

在正常运行时，vSwitch 将保持与其已配置的 vSwitch Controller 的连接，以交换网络管理和状态信息。如果 vSwitch Controller 变得不可用，vSwitch 将在网络流量降低时最长等待到不活动超时。在不活动超时后，vSwitch 将进入已配置的故障模式。

在防故障模式下，现有 ACL 将在 vSwitch 失去与其已配置的 vSwitch Controller 的连接后继续适用。与现有 ACL 不匹配的流量将被拒绝。所有 ACL（在 Controller 提供的策略层次结构的任何级别）都将被强制作为 vSwitch 中 VIF 上的规则集。因此，在 Controller 不可用时于防故障模式下显示的新 VIF 将无法通信，直到 Controller 再次变得可用。拔出然后重新插入的现有 VIF 与新的 VIF 具有相同的行为。即使现有 VIF 上存在允许通信的更高级别的 ACL 策略规则（全局、按资源池、按网络或按 VM），也会出现这种情况。此外，vSwitch Controller 还可以基于其识别到的 IP 地址定义 ACL。在防故障模式下，VM 使用 Controller 在变得可用之前未将其与 VM 关联的 IP 地址发送的数据包将被拒绝。例如，在可以再次访问 Controller 之前，使用新 IP 地址的现有 VM 无法通信。在防故障模式下流量被拒绝的其他示例包括：

- 新插入的 VIF
- 新的 VM
- 迁移的 VM (例如实时迁移或 Workload Balancing)
- 主机上添加到池中的 VM
- 充当路由器的应用程序

如果 vSwitch 在防故障模式下重新启动且 Controller 在 vSwitch 启动后仍然不可用，则所有 ACL 都将丢失且所有流量都将被拒绝。在重新建立与 Controller 的连接并且 Controller 将 ACL 向下推入 vSwitch 之前，vSwitch 将一直处于防故障模式。

**警告：**

在处于防故障模式时从 vSwitch Controller 管理删除资源池可能会导致 vSwitch 断开网络连接并出现强制进行紧急重置的情况。为防止出现这种情况，请仅在其状态为绿色时删除资源池。

您还可以在此页面上为端口配置策略指定可用的目标 VLAN。有关详细信息，请参阅设置端口配置策略。

## 服务器级别

对于选定服务器，“状态”页面将显示以下信息：

- 服务器状态：显示当前服务器状态的采用颜色编码的图标。
- 服务器网络数：资源池中的网络数。
- MAC 地址：服务器管理接口的 MAC 地址。
- IP 地址：服务器管理接口的 IP 地址。
- vSwitch 版本：在此 Citrix Hypervisor 上运行的 vSwitch 的 Build 和版本号。
- 服务器网络：与服务器相关联的所有网络的列表。此信息包括：
  - 使用该网络的服务器上的 VM 数
  - 关联的物理接口、
  - VLAN
  - 传输和接收的字节数
  - 错误数
  - 状态
- 服务器 VM：与服务器相关联的所有 VM 的列表。对于 VM 上的每个 VIF，此信息还包括：
  - MAC 地址
  - 网络
  - IP 地址
  - 自 VM 启动以来传输和接收的总字节数
  - 状态

在此页面上，您还可以为端口配置策略指定可用的目标 VLAN。请参阅设置端口配置策略。

## 网络级别

池范围的网络的“状态”选项卡将列出有关资源池中每个网络的摘要信息。单个网络的“状态”选项卡将列出网络本身的相关信息。该选项卡包含有关当前连接到网络的物理接口和 VM 接口的信息的超链接表格。

可以使用以下颜色显示状态图标：

- 如果网络处于活动状态且由 vSwitch Controller 正确托管，则为绿色
- 如果网络没有连接的接口，则为红色
- 如果出现错误状况，则为橙色。相关联的文本将描述相应错误。

对于池范围的网络，将显示以下信息：

- 网络名称：特定网络。
- VM 数：与网络相关联的 VM 数。
- Citrix Hypervisor：与网络对应的服务器。
- 物理接口：网络的服务器接口。
- 传输 (Tx) 和接收 (Rx) 数据包数：指定网络上所有 VIF 的计数器之和。
- 错误数：指定网络上所有 VIF 的计数器之和。
- 状态：显示当前网络的采用颜色编码的图标。

对于选定网络，将显示以下信息：

- 网络状态：显示当前网络的采用颜色编码的图标。
- VM 数：与网络相关联的 VM 数。
- 物理接口：物理接口的列表，包括 VLAN、传输和接收的字节数、错误数和状态。
- 切换 Citrix Hypervisor（仅在跨服务器专用网络上存在）：为网络指定当前处于活动状态的交换主机。

跨服务器专用网络允许同一资源池中的 VM 进行通信，而无需对物理网络进行任何额外配置。VM 可以在不同的主机上运行。通过让“切换主机”建立与池中的其他每个主机的 GRE 通道，可以实现此功能。GRE 通道将以星形拓扑的形式设置。其他主机具有在专用网络中运行的活动 VM。

如果交换主机变得不可用或被删除，系统将自动选中新的交换主机并配置新的 GRE 通道。有关跨服务器专用网络的详细信息，请参阅[网络连接](#)。

- VM 接口：VM 的列表，包括 MAC 地址、IP 地址、传输和接收的字节数，以及状态。

在此页面上，您还可以为端口配置策略指定可用的目标 VLAN。有关详细信息，请参阅[设置端口配置策略](#)。

## 虚拟机 (VM) 级别

将为所有 VM 显示以下信息：

- VM 名称：特定 VM 的名称。
- MAC 地址：分配给 VM 的 MAC 地址。
- 网络名称：向其分配 VM 的网络。
- 检测到的 IP 地址：分配给 VM 的 IP 地址。
- 传输 (Tx) 和接收 (Rx) 数据包数：指定 VM 上所有 VIF 的计数器之和。

- 错误数：指定 VM 上所有 VIF 的计数器之和。

对于选定 VM，“状态”页面将显示以下信息：

- 状态：显示当前 VM 状态的采用颜色编码的图标。
- 资源池：VM 所属的资源池。
- 服务器名称：向其分配 VM 的服务器的名称。如果 VM 未在运行且未绑定到特定服务器，则此信息为空。
- VM 组成员身份：向其分配 VM 的管理组的列表。
- VM 接口：VM 上 VIF 的列表。此信息包括：
  - MAC 地址
  - 网络名称
  - 检测到的 IP 地址
  - 传输和接收的字节数、数据包数和错误计数
  - 状态
- 网络事件：涉及 VM 的网络事件的列表，包括优先级、日期/时间和说明。

#### 虚拟接口 (VIF) 级别

对于选定 VIF，“状态”页面将显示以下信息：

- 状态：显示当前 VIF 状态的采用颜色编码的图标。
- 资源池：VIF 所属的资源池。
- 网络：VIF 所属的网络。
- VM 名称：VIF 所属的 VM。
- MAC 地址：VIF 的 MAC 地址。
- IP 地址：VIF 的 IP 地址。
- 传输和接收的字节数、数据包数和错误数：VIF 的流量计数。
- 交换机端口 ACL 统计信息：与传输和接收计数不同，ACL 命中计数是从当前 vSwitch 的 ACL 规则统计信息读取的即时统计信息。因此，策略变更和暂停、关闭或迁移等 VM 操作会导致这些统计信息被重置。  
vSwitch ACL 统计信息需要能够在网络中被识别的 IP 地址，并且能够收集基于 IP 的协议的统计信息。如果您发现没有针对基于 IP 的规则的计算，请验证 IP 地址是否将显示在“IP 地址”字段中。

#### 查看流统计信息

默认情况下，每个托管 Citrix Hypervisor 上的 vSwitch 会将 Netflow 流发送给使用此数据生成流统计信息表格和图表的 vSwitch Controller。在处于不活动状态 5 秒或总活动时间为 60 秒后，vSwitch 会为所有 IPv4 流生成 Netflow 记录。

流的数据速率将表示为流的总流量在流持续时间内的平均值。例如，如果某个流持续 10 秒，并且第 1 秒发送了 900 KB，剩余 9 秒中每秒均发送 10 KB，则产生的数据将被绘制为仿佛整个流期间的速率为 100 KB/秒。

Netflow 将使用 UDP 数据报在交换机和收集器之间传输 NetFlow 记录（例如，vSwitch Controller）。由于 NetFlow 使用 UDP 数据报，因此收集器通常无法知道未收到 NetFlow 记录的原因。丢弃的记录可能会导致“Flow Statistics”

(流统计信息) 表格或图表具有不确定性。例如，假定每秒生成 10 个流的网络中有一个持续 10 秒的 1 GB 文件传输。该网络将总计生成 202 个流 (100 个 hping stimuli、100 个 hping 响应、1 个文件传输 stimulus 和 1 个文件传输响应)。如果 50% 的 UDP 数据报被丢弃，则收集器报告 1 GB 数据或 2 KB 的可能性均为 50%。

由于池中的每个 vSwitch 均会生成 Netflow 记录，因此不同 Citrix Hypervisor 服务器上运行的源和目标会导致出现两个记录，从而使统计信息计数翻倍。

在部署的 100 多个 VM 中禁用流可见性，以避免过度加载 vSwitch Controller 虚拟设备和用于发送 NetFlow 记录的网络。

**Flow Statistics** (流统计信息) 选项卡将显示图表和关联的表格以显示所选节点的流。



使用页面顶部的列表指定以下内容：

- 方向：双向、传入、传出
- 单位：字节、位、数据包、流
- 以下分组之一的顶部或底部项目（最高或最低值）：
  - VM：位于资源池中作为流量的源/目标的 VM
  - IP 地址：作为流量的源或目标的 IP 地址
  - 协议：ICMP、TCP 和 UDP 等 IP 协议流量
- 注意：
  - 由于用于生成结果的 Netflow 协议存在限制，因此将不显示以太网层协议（如 ARP）。
- Application（应用程序）：应用程序级别的协议流量，由 TCP/UDP 端口或 ICMP 类型/代码识别
- Traffic (by type) (流量 (按类型))：VM、IP 地址、协议、应用程序（由协议类型和端口号显示，此信息允许您推断使用的服务）
- 时间间隔。

图下方的表格显示以下部分或全部信息，具体取决于在列表中选择的项目的类型：

- VM
- IP
- 传入的字节数
- 传入的数据速率 (KB/秒)
- 传出的字节数
- 传出的数据速率 (KB/秒)
- 总字节数
- 总数据速率 (bps)

如果 NetFlow 未被转发到 vSwitch Controller，则“Flow Statistics” (流统计信息) 选项卡下将显示警告蓝色状态文

本: [One or more selected pools are not configured to forward NetFlow records to vSwitch Controller](#)

要重新配置转发，请单击蓝色状态文本以查看资源池列表。从列表中选择所需的资源池以导航到池状态页面。在状态页面中，您可以配置 NetFlow 数据转发。

## 管理地址组

您可以设置地址组以指定要用作 ACL 的源或目标的 IP 地址，以用于报告流统计信息。

要添加地址组，请执行以下操作：

1. 在 **Visibility & Control**（可见性和控制）下，在资源树（侧面板）中选择 **Address Groups**（地址组）以打开所有地址组的“状态”页面。
2. 单击创建组。
3. 输入用于识别组的名称，以及可选说明。
4. 单击创建组。新组将被添加到地址组列表中。
5. 在资源树中选择新的组以打开其状态页面。
6. 单击 **Add Members**（添加成员）按钮。
7. 在弹出窗口中，指定一个或多个 IP 地址或子网（以逗号分隔）。示例：192.168.12.5、192.168.1.0/24
8. 单击添加。可以根据需要继续添加更多网络。每组地址将作为节点添加到“地址组”列表中的网络下。

新的地址组现在对 ACL 策略和流程统计信息可用。

可以通过单击现有地址组的“所有地址组”行中的“删除”链接来删除该地址组。

您也可以更新地址组的名称或说明：

1. 在资源树中选择新的组以打开其状态页面。
2. 单击 **Modify Group**（修改组）按钮。
3. 在打开的对话框中，更改名称和说明。
4. 单击 **Modify Group**（修改组）按钮以保存所做的更改。

## 管理虚拟机组

VM 组是一组 VM，您可以将其识别为用于查看状态和流统计信息的组。VM 组中的每个 VM 必须已位于资源池中。否则，组将与资源池和服务器无关。

要添加 VM 组，请执行以下操作：

1. 在 **Visibility & Control**（可见性和控制）下，在资源树（侧面板）中选择 **VM Groups**（VM 组）以打开所有地址组的“状态”页面。
2. 单击“创建组”按钮。
3. 输入用于识别组的名称，以及可选说明。
4. 单击创建组。新组将被添加到 VM 组列表中。

5. 在资源树中选择新的组以打开其状态页面。
6. 单击 **Add Member** (添加成员)。
7. 在弹出窗口中，从列表中选择该 VM。
8. 单击添加。可以根据需要继续添加更多 VM。每个 VM 将作为子节点添加到“VM Groups” (VM 组) 列表中的组下。

以下右键单击选项对每个 VM 组可用：

- Add VM to group (将 VM 添加到组中)：添加新的组成员。
- Modify Name/Description (修改名称/说明)：更改名称或说明。
- 删除组：删除组。

## DVS 策略配置层次结构

使用 **Visibility & Control** (可见性和控制) 中的“访问控制”和“端口配置”选项卡可配置访问控制、QoS，以及虚拟网络环境中的流量镜像策略。虽然所有策略均在 VIF 级别应用，但是 vSwitch Controller 会显示支持在 VIF 集中声明默认策略的分层策略模型。vSwitch Controller 还提供了一种覆盖此默认策略的方法，即在需要时创建详细的例外。例如，您可以从默认资源池策略中排除特定 VM。

与资源树中使用的层次结构类似，策略层次结构具有以下级别：

- 全局 (最常规级别)：包括所有资源池中的所有 VIF。
- 资源池：特定资源池中的所有 VIF。
- 网络：连接到特定网络的所有 VIF。
- VM：连接到特定 VM 的所有 VIF
- VIF (最具体级别)：单个 VIF。

注意：

Citrix Hypervisor 服务器不包含在策略层次结构中，因为无论资源池中的 Citrix Hypervisor 是否在运行 VM，都必须应用策略。

## 设置访问控制策略

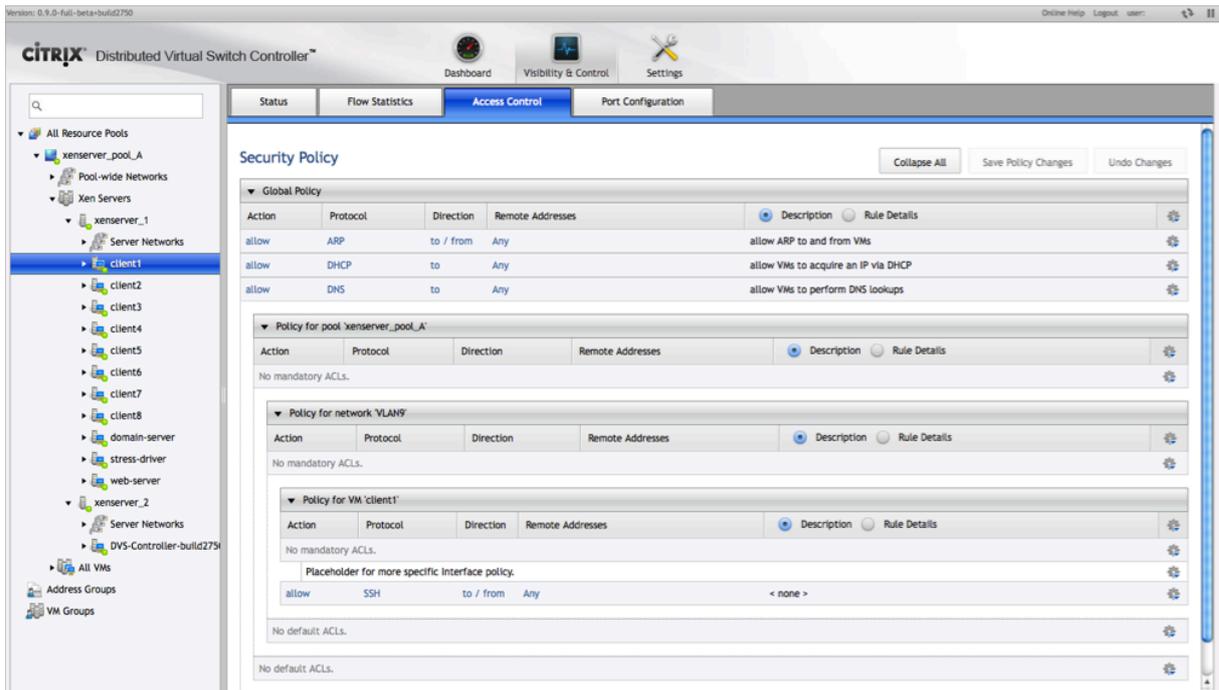
选择访问控制选项卡以设置允许或拒绝基于数据包属性的 VM 流量的策略。

ACL 策略包含一组规则，每个规则均包括以下部分：

- 操作：指示是否允许 (允许) 或丢弃 (拒绝) 与规则匹配的流量。
- 协议：要将规则应用到的网络协议。您可以将规则应用到所有协议 (任何)，从现有协议列表中进行选择或指定新的协议。
- 方向：要将规则应用到的流量的方向。从左到右读取规则文本：“到”表示从 VM 传出的流量，“从”表示传入到 VM 的流量。
- 远程地址：表示是否将规则限制为在一组特定的远程 IP 地址中传入/传出流量。

ACL 策略的管理严格遵循资源树层次结构。您可以在任何受支持的层次结构级别指定策略。在每个级别，规则将按如下进行组织：

- 强制性规则：这些规则将在任何子策略规则之前进行评估。优先于它们的唯一规则是父（较笼统）策略的强制性规则。强制性规则用于指定子（更具体）策略无法覆盖的规则。
- 子规则：子策略占位符将按规则顺序指示位置，子策略中的规则按该顺序进行评估。它可以强制将强制性规则与默认规则分开。
- 默认规则：这些规则是最后进行评估的，即在评估完所有强制性规则和所有子策略默认规则之后进行。它们仅优先于父策略的默认规则。它们用于指定仅在更具体的子策略未指定冲突行为时才应用的行为。



### 全局访问控制列表 (ACL) 规则

要设置全局 ACL 规则，请单击资源树中的所有资源池。该页面将列出在全局级别定义的所有 ACL 规则。

### 资源池访问控制列表 (ACL) 规则

要设置资源池的 ACL 规则，请选择资源树中的资源池。

该页面将显示全局策略的可展开栏和资源池规则的可展开区域。如果单击全部展开按钮，您可以查看在全局策略框架中嵌入资源池规则的方式。

### 网络访问控制列表 (ACL) 规则

要在网络级别设置 ACL 规则，请单击资源树中的网络。

页面将显示以下信息：

- 全局规则的可展开栏
- 网络所属的资源池的可展开栏
- 网络规则的可展开区域

如果单击全部展开，您可以查看在资源策略框架和全局策略框架中嵌入网络策略的方式。

### **VM 访问控制列表 (ACL) 规则**

要在 VM 级别设置策略，请单击资源树中的 VM。

页面将显示以下信息：

- 全局规则的可展开栏
- 资源池和 VM 所属的网络的可展开栏
- VM 规则的可展开区域

如果单击全部展开按钮，您可以查看在网络、资源池和全局框架中嵌入 VM 规则的方式。

如果 VM 包含多个网络中的 VIF，“Change Network”（更改网络）链接将显示在网络的示例栏右侧。此链接允许您查看可能应用于该 VM 上的 VIF 的每个网络级别策略的规则。

### **VIF 访问控制列表 (ACL) 规则**

要在 VIF 级别设置策略，请单击资源树中的 VIF。由于策略仅在 VIF 级别进行打包和应用，因此您必须显示 VIF 页面才能看到完整的策略上下文。

页面将显示以下信息：

- 全局规则的可展开栏
- 资源池、网络和 VIF 所属的 VM 的可展开栏
- VIF 规则的可展开区域

如果单击全部展开按钮，您可以查看在 VM、网络、资源池和全局框架中嵌入 VIF 规则的方式。

### **访问控制列表 (ACL) 规则实施顺序**

虽然可以在策略配置层次结构的不同级别定义 ACL，但是 ACL 是根据 VIF 实施的。对于实际实施，层次结构将按照此部分中所述的顺序进行组合并应用于每个 VIF。要查看当前对 VIF 和关联统计信息应用的规则，请选择资源树中的 VIF。在“状态”选项卡中查看 ACL 列表。

实施顺序如下所示：

1. 全局级别的强制性规则
2. 包含 VIF 的资源池的强制性规则

3. 包含 VIF 的网络的强制性规则
4. 包含 VIF 的 VM 的强制性规则
5. 包含 VIF 的 VIF 的规则
6. 包含 VIF 的 VM 的默认规则
7. 包含 VIF 的网络的默认规则
8. 包含 VIF 的资源池的默认规则
9. 包含 VIF 的全局默认规则

将执行匹配的的第一个规则，并且不评估其他规则。

注意：

当 vSwitch Controller 不可用时，资源池会根据配置的故障模式实施访问控制规则。请参阅“查看状态”下称为“资源池级别”的部分，以了解有关资源池的故障模式的更多详细信息。

### 定义访问控制列表 (ACL) 规则

要定义新的 ACL 规则，请使用资源树在策略配置层次结构中选择位于相应级别的节点。您可以在每个级别为该级别和更高级别添加规则。例如，如果您选择资源池，您可以为该资源池添加规则和全局规则。

如果您选择的资源树节点与策略配置层次结构中的某个级别不对应，将显示一条消息。该消息提供了用于选择另一个级别的链接。

可以通过以下方式添加新规则：

- 要添加强制性规则，请单击相应级别的标题栏中的齿轮图标，然后选择 **Add New Mandatory ACL**（添加新的强制性 ACL）。
- 要添加默认规则，请单击相应级别的标题栏中的齿轮图标，然后选择 **\*\* Add New Default ACL\*\***（添加新的默认 ACL）。
- 要添加现有规则条目上面的某个规则，请单击该条目的齿轮图标，并选择 **Add New ACL Above**（添加上方的新 ACL）。
- 要添加现有规则条目下面的某个规则，请单击该条目的齿轮图标，并选择 **Add New ACL Below**（添加下方的新 ACL）。

新规则将被添加到具有以下默认设置的页面：

- 操作：允许
- 协议：任何
- 方向：到/从
- 远程地址：任何
- Description（说明）：无

要更改规则中的特定字段，请单击表示当前字段值的链接，并应用如以下列表中所述的更改。应用更改时，规则将更新以显示值。

- 操作：单击链接并选择 **Change Action to Deny**（将操作更改为拒绝）或 **Change Action to Allow**（将操作更改为允许）。
- 协议：单击并选择以下选项之一：
  - 选择 **Match Any Protocol**（匹配任何协议）以将规则应用到所有协议。
  - 选择 **Use an Existing Protocol**（使用现有协议）以指定某个协议。从列表中选择该协议，然后单击 **Use Protocol**（使用协议）。
  - 选择 **Use a New Protocol**（使用新协议）以指定自定义协议特性。在弹出窗口中指定以下信息，然后单击 **Save & Use**（保存并使用）：
    - \* Ether type（以太网类型）：选择 IP 或输入其他以太网类型。
    - \* IP Protocol（IP 协议）：选择其中一个列出的协议，或输入另一个协议。
    - \* Destination Port（TCP/UDP only）（目标端口（仅限 TCP/UDP））：输入端口号或指定任何。
    - \* Source Port（TCP/UDP only）（源端口（仅限 TCP/UDP））：输入端口号或指定任何。在定义使用已知的服务器端口的应用程序时，将该已知端口定义为目标端口并将源端口保留为任何。例如，可以对 HTTP 使用此方法，即使用端口 80。
    - \* ICMP Type（ICMP only）（ICMP 类型（仅限 ICMP））：选择 **Any**（任何）或输入特定 ICMP 类型的协议（ICMP）。
    - \* ICMP Code（ICMP only）（ICMP 代码（仅限 ICMP））：选择 **Any**（任何）或输入特定的 ICMP 代码。
    - \* Match reply traffic（匹配回复流量）：指示是否自动允许将返回流量作为规则的一部分。例如，如果该规则允许 UDP 目标端口 7777 流量从 VM 传输到指定的远程地址，并且选中“Match reply traffic”（匹配回复流量），则还允许 UDP 流量从远程地址的源端口 7777 传输至 VM。为需要双向通信的任何 UDP 协议启用此选项（始终为 TCP 启用此选项）。
    - \* One-time Use vs. Multiple Uses（一次性使用和多次使用）：选择是否仅针对当前规则使用此协议，还是将其添加到协议菜单中的协议列表中。
  - 选择 **View/Modify Current Protocol**（查看/修改当前协议）以修改已定义协议的特性。
- 方向：选择规则是应用自还是应用至指定的远程地址，或者通过这两种方式应用。
- 远程地址：要指定远程地址，请执行以下操作：
  1. 单击任何链接以打开弹出窗口，其中列出了可用的地址组。
  2. 选择一个或多个地址组并使用箭头将其移动到已选中列中。
  3. 使用所有按钮选中或取消选中所有组。
  4. 要指定不属于现有地址组的 IP 地址或子网，请输入地址或子网（x.x.x.x or x.x.x.x/n）。单击添加。请重复此操作以添加更多地址。
  5. 单击完成。
- 说明：要添加规则的文本说明，请执行以下操作：
  1. 单击说明按钮。
  2. 单击相应的条目（< 无 > 如果当前没有说明）。此时将显示文本输入区域。输入文本并按 **Enter** 键。
- 规则详细信息：单击规则详细信息按钮以显示该规则的简短摘要。

单击 **Save Policy Changes**（保存策略更改）以应用新规则。执行此操作后，所做的更改将立即在虚拟网络环境中生效。如果尚未保存这些规则，您可以单击撤消更改以撤消您进行的更改。

当您更改某个 ACL 时，vSwitch Controller GUI 的所有后台更新都将暂停。如果另一个管理员同时修改该策略并先

于您提交更改，请刷新页面以从服务器检索新策略。重新输入您所做的更改。

通过单击规则的齿轮图标并选择上移或下移，您可以更改级别中各个规则的顺序。不能在层次结构中的各级别之间移动规则。要删除某个规则，请单击齿轮图标并选择删除。单击说明按钮以显示 ACL 说明。或单击规则按钮以显示您构建的 ACL 规则。

ACL 规则将始终从 VM 的虚拟接口角度进行解释，即使在策略层次结构中配置了更高级别时也是如此。考虑规则中“Remote Addresses”（远程地址）字段的意义时，此行为很重要。

例如，如果池中的某个 VM 具有 IP 地址 10.1.1.1，您可能希望池中具有用于指定“拒绝连接到 IP 10.1.1.1 的所有协议”的规则，以防止任何流量访问该 VM。对于资源池中的所有其他 VM，都会出现此行为，因为每个 VM 都会在 VM 传输时实施该规则。但是，资源池外部的资源池也可以与 IP 地址为 10.1.1.1 的 VM 进行通信。出现此行为的原因是，没有用于控制外部计算机的传输行为的规则。另一个原因是，IP 地址为 10.1.1.1 的 VM 的 VIF 具有一个可丢弃拥有该地址的传输流量的规则。但是，该规则不会丢弃具有该地址的接收流量。

如果意外出现此策略行为，请查看虚拟界面的“状态”选项卡，通过该界面可以查看所有策略级别的整个规则集。

## 设置端口配置策略

使用端口配置选项卡配置应用于 VIF 端口的策略。支持以下策略类型：

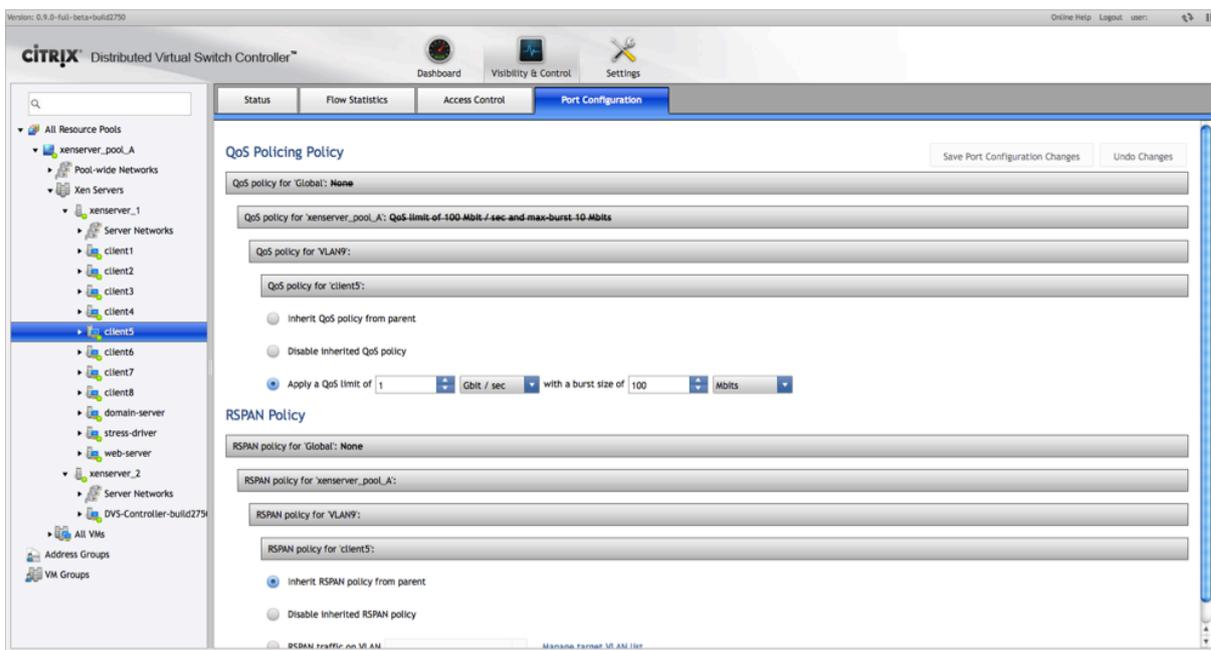
- QoS：质量服务 (QoS) 策略控制连接到 DVS 端口的 VM 的最大传输速率。
- Traffic Mirroring（流量镜像）：远程交换端口分析器 (RSPAN) 策略支持在 VIF 上接收或发送到 VLAN 的监视流量以支持流量监视应用程序。
- Disable MAC address spoof check（禁用 MAC 地址欺骗检查）：MAC 地址欺骗检查策略控制是否对从 VIF 传出的流量执行 MAC 地址实施。如果 vSwitch Controller 从某个 VIF 检测到一个具有未知 MAC 地址的数据包，则会丢弃来自该 VIF 的数据包和所有后续流量。MAC 地址欺骗检查策略默认情况处于开启状态。在于 Microsoft Windows 服务器上运行 Network Load Balancing 等软件的 VIF 上禁用这些策略。

### 警告：

在未正确配置物理和虚拟网络的情况下启用 RSPAN 可能会导致出现严重的网络中断问题。请在启用此功能之前仔细阅读配置 RSPAN 中的说明。

您可以在全局、资源池、网络、VM 和 VIF 级别配置 QoS 和“Traffic Mirroring”（流量镜像）端口策略。当您选择资源树中的某个节点并选择端口配置选项卡时，它会显示层次结构中每个父级别的配置。但是，只能更改选定策略级别的唯一。例如，如果您选择 VM，端口配置选项卡将显示在全局、资源池和网络级别配置的值。该选项卡允许您更改 VM 级别的值。

给定级别的 QoS 和“Traffic Mirroring”（流量镜像）配置会覆盖在更高级别的配置。如果配置被覆盖，则端口配置选项卡将显示更高级别的配置已被删除。例如，下图显示了网络级别的 QoS 配置，该配置将覆盖资源池级别的配置。



要配置端口策略，请选择资源树中的节点并选择端口配置选项卡。如果您选择不支持端口配置策略的节点，则将显示一条消息，其中包含指向支持端口配置的节点的链接。

## 配置 QoS

有关 QoS 策略，请从以下选项中进行选择：

- **Inherit QoS policy from parent (default)** (从父节点继承 QoS 策略 (默认))：从更高（即更笼统）的层次结构级别应用策略。此选项在全局级别不存在。
- **Disable inherited QoS policy** (禁用继承的 QoS 策略)：忽略在更高（即更笼统）的级别设置的任何策略，在该级别，此策略级别中包含的所有 VIF 都将未配置 QoS。
- **Apply a QoS limit** (应用 QoS 限制)：选择速率限制（带单位）和脉冲大小（带单位）。发送到此策略级别中包含的所有 VIF 的流量被限制为指定速率，并将各个脉冲限制为指定的数据包数。

### 警告：

相对于速率限制设置过小的脉冲大小可能会阻止 VIF 发送足够多的流量才能到达速率限制。对于执行 TCP 等拥塞控制的协议，很可能发生此行为。

至少，脉冲速率必须大于本地网络的最大传输单位 (MTU)。

针对 vSwitch Controller 所在的任何接口将 QoS 设置为不合适的低脉冲速率可能会导致断开与 vSwitch Controller 的所有通信。此通信会错失“强制紧急重置”的情况。

要阻止发生任何继承的实施，请在 VM 级别禁用 QoS 策略。

单击 **Save Port Configuration Changes** (保存端口配置更改) 以实施更改，或单击撤消更改以删除任何未保存的更改。此策略将在保存后立即生效。

## 配置 RSPAN

### 警告：

当服务器连接到无法识别 VLAN 的交换机或未正确配置为支持 RSPAN VLAN 时，配置 RSPAN 可能会导致流量复制和网络中断。请在启用 RSPAN 功能之前，先检查物理交换机的文档和配置。在必须涉及多个物理交换机的更高层次结构级别进行此检查特别重要。

启用 RSPAN 需要执行一系列步骤，如下所述：

## 标识 RSPAN VLAN

在 VIF 上启用 RSPAN 时，该 VIF 的 vSwitch 会生成发送到该 VIF 或从该 VIF 发送的每个数据包的副本。vSwitch 将传输使用 VLAN 值（称为目标 VLAN）标记的该数据包的副本。然后管理员会将执行监视的主机放在配置为使用该目标 VLAN 的交换机端口上。如果监视主机接口使用混杂模式，它可以查看发送到配置为使用 RSPAN 的 VIF 或从该 VIF 发送的所有流量。

## 使用目标 VLAN 配置物理网络

正确配置物理网络以识别 RSPAN 流量至关重要，可避免出现网络中断。如果连接所有启用了 RSPAN 的 VIF 的物理交换基础结构可以配置为禁用识别目标 VLAN，则仅启用 RSPAN。有关详细信息，请参阅交换机制造商提供的文档。

此外，还必须将在目标 VLAN 上发送的流量从每个 vSwitch 转发至监视主机。如果物理基础结构在某个层次结构中包含多个交换机，则此转发要求在不同的交换机之间中继目标 VLAN。有关详细信息，请参阅交换机制造商提供的文档。

## 使用目标 VLAN 配置 vSwitch Controller

在使用该 VLAN ID 配置 RSPAN 端口之前，请告知 vSwitch Controller 有关每个目标 VLAN 的信息。您可以在资源池、网络或服务器级别指定可用的目标 VLAN ID。在层次结构级别和更低的层次结构级别配置 RSPAN 端口配置时，在该级别添加的目标 VLAN 将可用。用于指定目标 VLAN 的正确级别取决于配置物理基础结构以识别该目标 VLAN 的广泛性。

要指定可用的目标 VLAN，请执行以下操作：

1. 在 **Visibility & Control**（可见性和控制）中，打开所有资源池、特定资源池、特定服务器或特定网络的状态选项卡。
2. 在 **RSPAN Target VLAN ID**（RSPAN 目标 VLAN ID）区域中，单击 **+** 并输入 VLAN ID。
3. 重复此操作以添加更多 VLAN ID。
4. 单击 **Save Target VLAN Change**（保存目标 VLAN 更改）。

现在可以在“端口配置”选项卡上选择 VLAN，如此部分中所述。

## 修改端口配置以为一组 VIF 启用 RSPAN

要在端口配置选项卡中配置 RSPAN 策略，请在资源树中选择相应的节点并从以下选项中进行选择：

- **Inherit RSPAN policy from parent (default)** (从父节点继承 RSPAN 策略 (默认))：从下一个更高 (即更笼统) 的层次结构级别应用策略。
- **Disable inherited RSPAN policy** (禁用继承的 RSPAN 策略)：忽略在更高 (即更笼统) 的级别设置的任何策略，在该级别，此策略级别中包含的所有 VIF 都将未配置 RSPAN。
- **RSPAN traffic on VLAN** (VLAN 上的 RSPAN 流量)：从目标 VLAN 的列表选择一个 VLAN。显示在该列表中的唯一目标 VLAN 是为包含当前选择的节点的策略级别配置的 VLAN。

#### 配置 MAC 地址欺骗检查

要禁用 MAC 地址实施，请选择 **MAC address spoof checking** (MAC 地址欺骗检查)。实施只能根据每个 VIF 进行配置，并且不会继承或覆盖父配置。

#### 保存更改

单击“Save Port Configuration Changes” (保存端口配置更改) 以实施更改，或单击撤消更改以删除任何未保存的更改。此策略将在保存后立即生效。

## 管理和维护 vSwitch Controller

June 4, 2019

使用 **Settings** (设置) 页面可在 vSwitch Controller 上执行维护和管理功能。要访问“Settings” (设置) 页面，请选择“vSwitch Controller”窗口的顶部面板中的 **Settings** (设置) 图标。

#### 配置 IP 地址设置

使用 **IP Configuration** (IP 配置) 页面可验证和配置 vSwitch Controller 的 IP 地址。首次启动 vSwitch Controller 时，将通过 DHCP 获取 IP 地址。但是，我们建议您分配静态 IP 地址。如果配置了 DHCP，则无法将资源池设置为防故障模式。

要查看和配置 Controller IP 地址，请执行以下操作：

1. 在 **Settings** (设置) 下，选择 **IP Configuration** (IP 配置) 以显示当前配置。
2. 要修改配置，请单击 **Modify Configuration** (修改配置)。
3. 选择 **Manual Configuration** (手动配置) 以分配静态 IP 地址。
4. 输入以下信息：
  - 新 IP 地址
  - 网络掩码
  - 网关 IP 地址
  - (可选) 一个或两个 DNS 服务器 IP 地址

注意：

必须至少指定一个 DNS 服务器 IP 地址，以在 Controller 上启用名称解析。

5. 单击 **Make Changes**（进行更改）以实施更改。

警告：

更改 vSwitch Controller 的 IP 地址后，可能会看到一条错误消息：池由 *old\_ip\_address* 托管。此错误消息将显示在 vSwitch Controller 管理的池的 **Status**（状态）列中。如果看到此消息，则必须指示 Controller 再次开始管理池。

在 **All Resource Pools**（所有资源池）选项卡中，单击资源池的 **Status**（状态）列旁边的齿轮图标。选择 **Steal Pool**（盗用池）。

默认情况下，vSwitch Controller 虚拟设备对与每个 Citrix Hypervisor 上运行的 vSwitch 的连接使用自签名 SSL 证书。可以获取一个证书颁发机构，以便为您的 vSwitch 连接提供签名证书。生成要签名的公钥/私钥对时，请按照您计划使用的证书颁发机构的说明进行操作。向颁发机构提交密钥。从颁发机构获取签名的证书后，请按照本部分中的步骤进行操作。

在 **Settings**（设置）中，单击 **Server and Certificate Maintenance**（服务器和证书维护）。

单击 **Update OVS Certificate**（更新 OVS 证书）。

浏览以选择 SSL/TLS 证书文件。

上传该文件后，单击 **Update Certificate**（更新证书）。

要查看与 vSwitch SSL 安全证书有关的信息，请执行以下操作：

1. 在 **Settings**（设置）中，单击 **Server and Certificate Maintenance**（服务器和证书维护）。
2. 单击 **View OVS Certificate**（查看 OVS 证书）。

此信息还包括证书的过期时间。

更新 vSwitch SSL 证书后，添加新池进行管理时，池中每个服务器的 vSwitch 将自动下载新证书。但是，对于在受管理的现有池中运行的 vSwitch，则必须手动更新其 SSL 证书。

在 Citrix Hypervisor 服务器上，将 SSL 证书复制到 `/etc/openvswitch/vswitchd.cacert`

重新启动 Citrix Hypervisor 服务器。

## 配置 Controller 主机名

要验证和配置 Controller 主机名和 DNS 域，请使用“IP Configuration”（IP 配置）页面。默认情况下，Controller 主机名为 `dvsc`，并且 DNS 域名未分配。

在 **Settings**（设置）下，选择 **IP Configuration**（IP 配置）以显示当前配置。

单击 **Modify Host Settings**（修改主机设置）。

在相应字段中输入所需的主机名和域名。

域名的值同时用于主机的域名以及用于搜索非限定主机名的域。

单击 **Make Changes** (进行更改) 以保存更改, 或者选择 **Cancel** (取消)。

### 收集故障报告的信息

要收集信息以提供故障报告, 请执行以下操作:

1. 在 **Settings** (设置) 中, 单击 **Server and Certificate Maintenance** (服务器和证书维护)。
2. 单击 **Collect & Zip All Logs** (收集并压缩所有日志), 将所有相关的 vSwitch Controller 日志添加到 zip 文件以供下载。
3. zip 操作完成后, 单击弹出窗口中的此处链接以下载 dump.tar.gz 文件。
4. 下载后, 单击 **Close** (关闭) 关闭弹出窗口。

### 重新启动 vSwitch Controller 软件

要重新启动 vSwitch Controller 软件, 请单击“Settings”(设置) 下的 **Server and Certificate Maintenance** (服务器和证书维护), 然后单击 **Restart Network Controller** (重新启动网络控制器)。重新启动完成后, 将打开登录页面。

### 管理管理帐户

在访问 GUI 时, 可以使用多个用户帐户为某些用户提供有限权限。“Administrative Events log”(管理事件日志) 中的条目包含执行操作的用户的名称。有多个用户可以帮助确定哪个用户最近做出了配置更改。

要添加用户帐户以访问 vSwitch Controller 和更改用户密码, 请执行以下操作:

1. 在 **Settings** (设置) 下, 选择 **Administrative Accounts** (管理帐户)。
2. 单击 **Create Account** (创建帐户)。
3. 输入用户名和密码, 然后重新输入密码以进行确认。指定以下任一用户权限级别:
  - 超级用户: 所有权限。
  - 读写: 除修改其他用户帐户和还原快照之外的所有权限。
  - 只读: 可以在 GUI 中查看大多数信息, 但不能修改 vSwitch Controller 中的任何内容, 但用户自己的密码除外。
4. 单击 **Add User** (添加用户)。

要更改用户密码, 请单击该用户的 **Password** (密码) 链接。输入并确认新密码, 然后单击 **Change Password** (更改密码)。

要删除用户, 请单击该用户的 **Remove** (删除) 链接。您无法删除管理员用户。

## 管理配置快照

快照提供了一种保存当前 vSwitch Controller 配置的机制，以便您可以在稍后恢复到该确切配置。在做出主要配置更改之前创建系统快照可能非常有用。默认情况下，系统每隔 12 小时自动创建一次自动快照。

单击 **Settings**（设置）下的 **Configuration Snapshots**（配置快照），查看配置备份的列表以及从备份还原。该页面列出了所有最近的备份，其中最先列出的是最新的备份。自动备份每天创建两次，每次 vSwitch Controller 都会重新启动。从备份还原时，不会更新 vSwitch Controller 的当前 IP 配置。要更改 vSwitch Controller IP 地址，请参阅配置 IP 地址设置。

要从备份还原配置，请单击快照的齿轮图标，然后选择 **Restore to Snapshot**（还原到快照）。当系统询问您是否要继续时，请单击 **Yes, Restore**（是，还原）。

要按需创建备份，请单击 **Create New Snapshot**（创建新快照）。可以输入可选说明来标识快照。单击 **Create Snapshot**（创建快照）。新备份将添加到列表顶部。

要下载快照以存储在其他系统上，请单击快照的齿轮图标，然后选择 **Download**（下载）。按照弹出窗口中的说明保存快照文件。

要将以前保存的快照上载到 Controller，请单击 **Upload Snapshot**（上载快照）。浏览以选择快照文件，然后单击 **Upload Snapshot**（上载快照）。上载的快照将添加到“Configuration Snapshots”（配置快照）页面上的列表中。

要删除快照，请单击快照的齿轮图标，然后选择 **Delete Snapshot**（删除快照）。当系统询问您是否要继续时，请单击 **Delete Snapshot**（删除快照）。

快照表还包含有关软件版本和兼容性的信息。兼容性指示快照中的数据是否与当前软件版本兼容。如果兼容，则显示绿色指示符，如果不兼容，则显示红色指示符。要恢复为不兼容的快照，必须先将软件更改为兼容版本，如“Software Version”（软件版本）列中所列。

默认情况下，系统每隔 12 小时创建一次配置快照。这些快照与 **Automatic periodic snapshot**（自动定期快照）的说明标签一起列出。此外，每次重新启动 vSwitch Controller 时都会创建配置快照。这些快照与 **Startup snapshot**（启动快照）的说明标签一起列出。系统启动的快照在超过 30 天时会自动删除。手动创建快照时，请输入唯一的说明标签，以便其不会被误认为是系统启动的快照并在 30 天后删除。如果系统启动的快照必须保留超过 30 天，请下载，然后使用唯一的说明标签重新上载。

## 添加网络时间协议 (NTP) 服务器

vSwitch Controller 虚拟设备使用与外部网络时间协议 (NTP) 服务器的连接来管理其时间设置。Controller 随附已配置的默认服务器。由于这些 NTP 服务器可能不适合您的环境，因此，可以按照以下说明将其替换为本地 NTP 服务器。

要添加 NTP 服务器，请执行以下操作：

1. 在 **Settings**（设置）下，选择 **Time & NTP**（时间和 NTP）。
2. 单击 **Add Server**（添加服务器）。
3. 输入服务器的 IP 地址，然后单击添加。

4. 根据需要添加更多服务器。

要删除 NTP 服务器，请单击 **Remove**（删除）链接。

## 导出 Syslog 文件

使用 Syslog 页面添加服务器可接收远程 syslog 消息，其中包括系统生成的管理和网络事件消息。最新的 syslog 条目也显示在控制板上。

要添加 syslog 服务器，请执行以下操作：

1. 在 **Settings**（设置）下，选择 **Syslog**。
2. 单击 **Add Server Address**（添加服务器地址）。
3. 输入服务器的 IP 地址，然后单击添加。
4. 根据需要添加更多服务器。

要删除服务器，请单击 **Remove**（删除）链接。

## 命令

June 4, 2019

本部分内容介绍了 vSwitch Controller CLI 命令。可以从 XenCenter 中的 Controller VM 的文本控制台本地访问 CLI。要远程访问 CLI，请使用 SSH 客户端应用程序并连接到端口 22 上的 Controller VM 主机名或 IP 地址。

在 CLI 会话期间，可以通过以下任一方式获取 CLI 命令的帮助：

- 键入 **help**，然后按 **Enter** 键。
- 输入命令的一部分，后跟空格和问号 (?)，然后按 **Enter** 键。

按 **Tab** 键时，界面支持完成命令参数。通常情况下，可以将命令缩写为每个级别的最短唯一字符串，以减少输入。可以通过按箭头键访问当前会话中的命令历史记录。

## 生命周期命令

### 停止 vSwitch Controller

```
1 halt controller
```

此命令通过正常关闭 Controller 来停止 vSwitch Controller 设备。

## 重新启动 **Controller**

```
1 restart controller appliance
```

此命令将关闭并重新启动整个 **Controller** 设备。

此命令主要适用于故障排除。通常情况下，`halt` 命令用于关闭 **Controller** 设备的电源。

## 重新启动 **Controller** 守护程序

```
1 restart controller daemon
```

此命令将关闭并重新启动用于实现 **Controller** 功能的进程。

此命令主要适用于故障排除。

## 设置命令

使用这些命令可配置 vSwitch **Controller**。

## 设置 **Controller** 设备的主机名

```
1 set controller hostname hostname
```

此命令将设置 **Controller** 设备的主机名。

如果提供的主机名包含一个或多个句点字符 (.)，设备的主机名将设置为第一个句点之前的字符串。设备的域名将设置为第一个句点之后的字符串。

## 通过 **DHCP** 设置 **Controller** 管理接口的 **IP** 地址

```
1 set controller management-interface config dhcp
```

此命令使用 **DHCP** 设置 **Controller** 管理接口的 **IP** 地址。如果配置了 **DHCP**，则无法将资源池设置为防故障模式。

此命令在执行时生效，因此，如果地址发生变化，对 **CLI** 的远程访问可能会断开。

为 **Controller** 管理接口设置静态 IP 地址

```
1 set controller management-interface config static
2         IP-address
3         netmask
4         gateway-IP
5         [dns-server-IP]
6         [dns-server-IP2
7         dns-search]] ‘
```

此命令设置 Controller 管理接口的静态 IP 地址。DNS 配置信息是可选的。指定 DNS 搜索路径的功能需要指定两个 DNS 服务器。

此命令在执行时生效，因此，如果地址发生变化，对 CLI 的远程访问可能会断开。

显示命令

使用这些命令可显示与当前的 vSwitch Controller 配置有关的信息。

显示当前 **Controller** 的主机名

```
1 show controller hostname
```

显示管理接口的当前配置和状态的摘要

```
1 show controller management-interface
```

显示管理接口的配置值

```
1 show controller management-interface config
```

显示 **Controller** 的当前默认网关

```
1 show controller management-interface default-gateway
```

显示 **Controller** 的当前 **DNS** 配置

```
1 show controller management-interface dns-server
```

显示 **Controller** 管理接口的当前 **IP** 地址

```
1 show controller management-interface ip-address
```

显示 **Controller** 管理接口的当前网络掩码

```
1 show controller management-interface netmask
```

显示 **Controller** 的软件版本

```
1 show controller version
```

其他命令

终止当前的 **CLI** 会话

```
1 exit
```

获取有关命令的信息

```
1 help
```

升级或降级 **Controller** 的现有版本

```
1 install controller software-update scp-format-remote-filename
```

此命令从指定的远程位置安全地复制 **Controller** 更新文件，并安装该版本来代替现有版本。

此命令可用于安装升级和降级的软件版本。升级会自动将配置迁移到新版本。降级还原为最新的兼容配置快照或者在不兼容快照时为空配置。

**ping** 指定的远程系统

```
1 ping name-or-IP-address [count]
```

此命令将 ICMP 回显请求发送到由名称或 IP 地址标识的远程系统，并等待答复。如果未指定计数，则每秒发送一次请求，直到使用 Ctrl-C 中断。如果指定了计数，则会发送 ping 的次数。

## 对 vSwitch Controller 问题进行故障排除

June 4, 2019

本节包含的信息可帮助您对 vSwitch Controller 问题进行故障排除。

## 资源树节点状态

下表介绍了每种资源类型对应的状态图标。这些图标显示在资源树以及相应项目的“状态”页面上。

| 项目/状态图标      | 说明                                                                               |
|--------------|----------------------------------------------------------------------------------|
| <b>VIF</b>   |                                                                                  |
| 红色           | 关联的虚拟机 (VM) 已关闭或无法访问。                                                            |
| 绿色           | 虚拟接口 (VIF) 已打开且受管理。                                                              |
| 橙色           | VM 正在运行，但 VIF 所在的 Citrix Hypervisor 未连接到 vSwitch Controller。                     |
| <b>VM</b>    |                                                                                  |
| 红色           | VM 已关闭或无法访问。                                                                     |
| 绿色           | VM 处于运行状态且 VIF 受管理。                                                              |
| 橙色           | VM 正在运行，但 VM 所在的 Citrix Hypervisor 未正确连接到 vSwitch Controller。此状态取决于各个 VIF 的收集状态。 |
| <b>服务器网络</b> |                                                                                  |
| 红色           | Citrix Hypervisor 已关闭或无法访问，或者没有 VM 具有与网络关联的 VIF。                                 |
| 绿色           | Citrix Hypervisor 已正确连接到 vSwitch Controller。                                     |

| 项目/状态图标                  | 说明                                                                       |
|--------------------------|--------------------------------------------------------------------------|
| 橙色                       | Citrix Hypervisor 未正确配置为连接到 vSwitch Controller（取决于关联的物理接口和 VIF 的收集状态）。   |
| <b>Citrix Hypervisor</b> |                                                                          |
| 红色                       | Citrix Hypervisor 已关闭或无法访问。                                              |
| 绿色                       | Citrix Hypervisor 已正确连接到 vSwitch Controller。                             |
| 橙色                       | Citrix Hypervisor 未配置为连接到 vSwitch Controller（取决于关联的物理接口和 VIF 的收集状态）。     |
| <b>池范围内的网络</b>           |                                                                          |
| 红色                       | 主服务器 Citrix Hypervisor 已关机或无法访问。                                         |
| 绿色                       | 主服务器 Citrix Hypervisor 已配置为连接到 vSwitch Controller 且连接已启动并处于正常运行状态。       |
| 橙色                       | 主服务器 Citrix Hypervisor 未配置为连接到 vSwitch Controller（取决于关联物理接口和 VIF 的集体状态）。 |
| <b>资源池</b>               |                                                                          |
| 红色                       | 主服务器 Citrix Hypervisor 已关机或无法访问。                                         |
| 绿色                       | 主服务器 Citrix Hypervisor 已配置为连接到 vSwitch Controller 且连接已启动并处于正常运行状态。       |
| 橙色                       | 主服务器 Citrix Hypervisor 未配置为连接到 vSwitch Controller（取决于关联物理接口和 VIF 的集体状态）。 |

## 对访问策略问题进行故障排除

当访问控制策略未正常运行时，以下建议在进行故障排除时可能有帮助：

1. 为该策略会影响的 VM 的 VIF 选择状态页面。生成该策略未正确处理的流量时，查看每个规则的命中次数。识别流量实际命中的规则，而非您要命中的规则。出于调试目的，您可以添加与所有流量相匹配的默认规则，作为全局级别优先级最低的默认规则。

注意：

可以对此规则执行允许或拒绝操作，具体取决于调试时所需的网络行为。在调试后删除此规则。

2. 如果流量命中的规则的优先级低于预期命中的规则，请仔细检查与准则匹配的规则。是否正确指定了流量的方向？

是否可以正常识别远程主机？是否正确定义了协议？例如，协议指定的是 UDP 端口而非 TCP 端口，还是指定的是 TCP 端口而非 UDP 端口？

3. 如果流量命中的规则的优先级高于预期命中的规则，请解决此规则与您希望流量命中的规则之间的冲突。您可以通过以下方法解决冲突：将规则重新定义为更详细或更简单，或者更改这两个规则的相对优先级。例如，您可以将规则范围限制为仅应用于一组特定的远程 IP 地址。
4. 如果 VM 具有多个 VIF，请检查它是否在策略应用到的 VIF 上传输和接收流量。在适当的情况下，使用 RSPAN 将流量从 VIF 镜像到网络分析器。可以使用此镜像的流量来确保流量已存在且与规则匹配。

注意：

当 vSwitch Controller 不可用时，资源池会根据配置的故障模式实施访问控制规则。请参阅“查看状态”下称为“资源池级别”的部分，以了解有关资源池的故障模式的更多详细信息。

## 创建故障报告

为了有效地解决问题，请从问题中涉及的 Citrix Hypervisor 和 vSwitch Controller 收集信息。出现问题后，请尽快收集此信息。将该信息与故障报告一起提交。

- 包含问题中涉及的每个 Citrix Hypervisor 的服务器状态报告。有关生成服务器状态报告的信息，请参阅[运行状况检查](#)
- 通过单击服务器和证书维护设置页面中的收集并压缩所有日志，可包括 vSwitch Controller 中的日志包。有关详细信息，请参阅[收集故障报告的信息](#)。

## 控制器错误消息

可以看到以下错误消息：

- 连接到池 - 在添加新池且 vSwitch Controller 尚未成功连接到池主服务器时显示。或者，在 vSwitch Controller 重新启动且尚未成功连接到池主服务器时显示。如果在 30 秒内未成功建立连接，此消息将被替换为“Pool Connection Failed”（池连接失败）。
- **Network control channels disconnected**（网络控制通道已断开连接）- Citrix Hypervisor 未正确连接到 vSwitch Controller。
- **Missing Pool Address**（缺少池地址）- 没有对池可用的 DNS 名称或 IP 地址。
- **Pool Connection Failed**（池连接失败）- 在以下情况下，将显示此消息：
  - Controller 与池主服务器之间出现网络问题
  - DNS 名称解析失败
  - 存在无效的 DNS 名称或池主服务器 IP 地址
  - 池主服务器已关闭或配置错误
- **Unsupported Pool Version**（不受支持的池版本）- 为池配置的 DNS 名称或 IP 地址未解析为 Citrix Hypervisor 的兼容版本。

- **Duplicate Pool: Pool Disabled** (重复的池: 池已禁用) - 池报告 XAPI UUID 与 vSwitch Controller 数据库中已存在的另一个池相同。
- **Pool Authentication Failure** (池身份验证失败) - vSwitch Controller 无法使用提供的用户名和密码对池主服务器进行身份验证。
- **Pool Identity Changed** (池身份已更改) - 池已重新安装且与匹配池的状态不匹配。
- **Pool Synchronization Error** (池同步错误) - 使用 XAPI 与池主服务器通信时, 会显示不受支持的操作。
- **Unknown Error** (未知错误) - 错误的原因是未知的。

## 命令行接口

September 5, 2019

xe CLI 可用于编写脚本和自动完成系统管理任务。使用 CLI 可将 Citrix Hypervisor 集成到现有 IT 基础结构中。

### 安装 **xe CLI**

默认情况下, xe 命令行接口安装在所有 Citrix Hypervisor 服务器上并包含在 XenCenter 中。对于 Linux, 还可以使用独立远程 CLI。

#### 在 **Windows** 中

在 Windows 上, `xe.exe` 命令随 XenCenter 安装。

要使用 `xe.exe` 命令, 请打开 Windows 命令提示窗口, 并将目录更改为 `xe.exe` 文件所在的目录 (通常为 `C:\Program Files\Citrix\XenCenter`)。如果将 `xe.exe` 安装位置添加到系统路径中, 则无需切换到该目录即可使用该命令。

#### 在 **Linux** 中

在基于 RPM 的发行版 (如 Red Hat) 上, 您可以从主 Citrix Hypervisor 安装 ISO 上名为 `client_install/xapi-xe-BUILD.x86_64.rpm` 的 RPM 安装独立的 xe 命令。

要从 RPM 进行安装, 请使用以下命令:

```
1 rpm -ivh xapi-xe-BUILD.x86_64.rpm
```

运行 xe 命令时, 可以在命令中使用参数来定义要使用的 Citrix Hypervisor 服务器、用户名和密码。但是, 您也可以选择将此信息设置为环境变量。例如:

```
1 export XE_EXTRA_ARGS="server=<host name>,username=<user name>,password=<password>"
```

注意：

尝试通过安全连接运行命令时，Linux 上的远程 xe CLI 可能会挂起，这些命令涉及文件传输。如果是这种情况，可以使用 `--no-ssl` 参数通过与 Citrix Hypervisor 服务器的不安全连接运行命令。

## 获取 **xe** 命令的帮助

要获得有关主机上的 CLI 命令的基础帮助，请键入：

```
1 xe help command
```

要显示最常使用的 xe 命令的列表，请键入：

```
1 xe help
```

或者，要显示所有 xe 命令的列表，请键入：

```
1 xe help --all
```

## 基本 **xe** 语法

所有 Citrix Hypervisor xe CLI 命令的基础语法是：

```
1 xe command-name argument=value argument=value
```

每个特定命令都有自己的一组参数，参数形式为 `argument=value`。一些命令具有必需参数，大多数命令都多少有些可选参数。通常情况下，如果调用一个命令时未使用某些可选参数，该命令将假定这些可选参数使用默认值。

如果远程执行 xe 命令，则会使用额外参数进行连接和身份验证。这些参数也采用 `argument=argument_value` 形式。

`server` 参数用于指定主机名或 IP 地址。`username` 和 `password` 参数用于指定凭据。

可以指定 `password-file` 参数，而不直接指定密码。在这种情况下，xe 命令将尝试从指定文件中读取密码，并使用该密码进行连接。（去掉文件结尾的任何尾随 CR 和 LF。）此方法比在命令行中只直接指定密码更安全。

可选 `port` 参数可用于指定远程 Citrix Hypervisor 服务器上的代理端口（默认为 443）。

示例：在本地 Citrix Hypervisor 服务器上：

```
1 xe vm-list
```

示例：在远程 Citrix Hypervisor 服务器上：

```
1 xe vm-list -user username -password password -server hostname
```

速记语法也适用于远程连接参数：

- -u 用户名
- -pw 密码
- -pwf 密码文件
- -p 端口
- -s 服务器

示例：在远程 Citrix Hypervisor 服务器上：

```
1 xe vm-list -u myuser -pw mypassword -s hostname
```

参数还取自环境变量 XE\_EXTRA\_ARGS，形式为逗号分隔键/值对。例如，要在远程 Citrix Hypervisor 服务器上运行命令，请先运行以下命令：

```
1 export XE_EXTRA_ARGS="server=jeffbeck,port=443,username=root,password=pass"
```

运行此命令后，不再需要在运行的每个 xe 命令中指定远程 Citrix Hypervisor 服务器参数。

使用 XE\_EXTRA\_ARGS 环境变量也可以在对远程 Citrix Hypervisor 服务器执行 xe 命令时对命令启用 Tab 键自动补齐功能，该功能在默认情况下处于禁用状态。

## 特殊字符和语法

要在 xe 命令行中指定参数/值对，请写入：`argument=value`

除非值中包含空格，否则请勿使用引号。参数名称、等号 (=) 和值之间不应存在任何空格。不符合此格式的参数都将被忽略。

对于包含空格的值，请写入：`argument="value with spaces"`

使用 Citrix Hypervisor 服务器上的 CLI 时，命令将具有 Tab 键自动补齐功能，该功能类似于标准 Linux Bash Shell 中的 Tab 键自动补齐功能。例如，如果您键入 `xe vm-l` 并按 **TAB** 键，则该命令的其余部分也将显示出来。如果多个命令都以 `vm-l` 开头，则再次按 **TAB** 键将列出所有可能的命令。此功能对在命令中指定对象 UUID 非常有用。

### 注意：

如果在远程 Citrix Hypervisor 服务器上执行命令，Tab 键自动补齐功能将无法正常运行。但是，如果您在输入命令的计算机上设置 XE\_EXTRA\_ARGS 变量，Tab 键自动补齐功能将处于启用状态。有关详细信息，请参阅基本 xe 语法。

## 命令类型

CLI 命令可以分为两种。低级命令将侧重于 API 对象的列表和参数篡改。较高级别的命令用于在更抽象的层面与 VM 或主机进行交互。

低级命令包括：

- `class-list`
- `class-param-get`
- `class-param-set`
- `class-param-list`
- `class-param-add`
- `class-param-remove`
- `class-param-clear`

其中 `class` 可以是以下任一项：

- `bond`
- `console`
- `host`
- `host-crashdump`
- `host-cpu`
- `network`
- `patch`
- `pbid`
- `pif`
- `pool`
- `sm`
- `sr`
- `task`
- `template`
- `vbd`
- `vdi`
- `vif`

- `vlan`
- `vm`

并不是 `class` 的每个值都有完整的 `class-param-action` 命令集。`class` 的某些值具有更小的命令集。

### 参数类型

使用 `xe` 命令处理的对象具有标识这些对象并定义其状态的参数集。

大多数参数只使用单一值。例如，VM 的 `name-label` 参数包含单一字符串值。在参数列表命令的输出中（例如 `xe vm-param-list`），括号中的值表示参数是读写 (RW) 还是只读 (RO)。

指定 VM 上 `xe vm-param-list` 的输出可能具有以下行：

```
1 user-version ( RW): 1
2 is-control-domain ( RO): false
```

第一个参数 `user-version` 为写入参数，值为 1。第二个参数 `is-control-domain` 为只读参数，值为 `false`。

其他两个类型的参数都是多值参数。`set` 参数包含一系列值。`map` 参数是一组键/值对。例如，请参阅下面指定 VM 上 `xe vm-param-list` 的输出示例：

```
1 platform (MRW): acpi: true; apic: true; pae: true; nx: false
2 allowed-operations (SRO): pause; clean_shutdown; clean_reboot; \
3 hard_shutdown; hard_reboot; suspend
```

`platform` 参数包含表示键/值对的一系列项。键名后跟冒号字符 (:)。各键/值对之间用分号字符 (;) 分隔。RW 前面的 M 表示这是一个 `map` 参数，既可读又可写。`allowed-operations` 参数包含构成一组项的列表。RO 前面的 S 表示这是一个 `set` 参数，可读但不可写。

要按 `map` 参数过滤或者设置 `map` 参数，请使用冒号 (:) 分隔 `map` 参数名称与键/值对。例如，要将 VM 的 `other-config` 参数的 `foo` 键值设置为 `baa`，使用的命令应为：

```
1 xe vm-param-set uuid=VM uuid other-config:foo=baa
```

#### 注意：

在早期版本中，连字符 (-) 用于指定 `map` 参数。此语法现在仍然有效，但不建议使用。

### 低级参数命令

有多个命令可在对象参数上运行：`class-param-get`、`class-param-set`、`class-param-add`、`class-param-remove`、`class-param-clear` 和 `class-param-list`。其中的每个命令都利用 `uuid` 参数指定特殊对象。由于这些命令都是低级命令，因此必须使用 UUID 而不是 VM 名称标签。

- **class-param-list** `uuid=uuid`  
列出所有参数及其相关的值。与 `class-list` 命令不同，此命令将列出相当多的字段的值。
- **class-param-get** `uuid=uuid param-name=parameter param-key=key`  
返回特殊参数的值。对于 `map` 参数，指定 `param-key` 将使该值与 `map` 中的键关联。如果不指定 `param-key`，或者该参数为 `set`，则该命令将返回 `set` 或 `map` 的字符串表示形式。
- **class-param-set** `uuid=uuid param=value`  
设置一个或多个参数的值。
- **class-param-add** `uuid=uuid param-name=parameter key=value param-key=key`  
添加到 `map` 或 `set` 参数。对于 `map` 参数，请使用 `key=value` 语法添加键/值对。如果该参数为 `set`，则使用 `param-key=key` 语法添加键。
- **class-param-remove** `uuid=uuid param-name=parameter param-key=key`  
从 `map` 删除键/值对，或者从 `set` 删除键。
- **class-param-clear** `uuid=uuid param-name=parameter`  
完全清除 `set` 或 `map`。

#### 低级列表命令

`class-list` 命令用于列出 `class` 类型的对象。默认情况下，此类型的命令将列出所有对象，并列出一部分参数。可以按以下方式修改此行为：

- 它可以过滤对象，以便仅输出子集
- 可以修改要列出的参数。

要更改列出的参数，请将参数 `params` 指定为所需参数的以逗号分隔的列表。例如：

```
1 xe vm-list params=name-label,other-config
```

或者，要列出所有参数，请使用以下语法：

```
1 xe vm-list params=all
```

`list` 命令不会显示某些需要进行大量计算的参数。例如，这些参数将显示为：

```
1 allowed-VBD-devices (SR0): <expensive field>
```

要获取这些字段，请使用 `class-param-list` 或 `class-param-get`

要过滤列表，CLI 需要将参数值与在命令行上指定的参数值相匹配，以便只列出满足所有指定的限制的对象。例如：

```
1 xe vm-list HVM-boot-policy="BIOS order" power-state=halted
```

此命令将只列出满足以下条件的 VM：值均为已停止的两个字段 `power-state` 以及值为 *BIOS* 顺序的字段 `HVM-boot-policy`。

还可以根据 `map` 中的键值或 `set` 中存在的值来过滤列表。基于 `map` 中的键进行过滤的语法是 `map-name:key=value`。基于 `set` 中存在的值进行过滤的语法是 `set-name:contains=value`。

编写脚本时，一种有用的技术是在命令上传递 `--minimal`，以使 `xe` 只列出以逗号分隔的列表中的第一个字段。举例来说，在安装有三个 VM 的主机上，`xe vm-list --minimal` 命令为这些 VM 提供了三个 UUID：

```
1 a85d6717-7264-d00e-069b-3b1d19d56ad9,aaa3eec5-9499-bcf3-4c03-
  af10baea96b7, \
2 42c044de-df69-4b30-89d9-2c199564581d
```

## 机密

Citrix Hypervisor 提供了一种机密机制，以避免密码以明文形式存储在命令行历史记录或 API 对象中。XenCenter 自动使用此功能，也可以从 `xe CLI` 中为需要密码的任何命令使用此功能。

### 注意

密码机密不能用于从 `xe CLI` 的远程实例对 Citrix Hypervisor 主机进行身份验证。

要创建机密对象，请在 Citrix Hypervisor 主机上运行以下命令。

```
1 xe secret-create value=my-password
```

机密创建并存储在 Citrix Hypervisor 主机上。该命令将输出机密对象的 UUID。例如 `99945d96-5890-de2a-3899-8c04ef2521db`。将 `_secret` 附加到密码参数的名称后面，以将此 UUID 传递给需要密码的任何命令。

示例：在创建机密的 Citrix Hypervisor 主机上，可以运行以下命令：

```
1 xe sr-create device-config:location=sr_address device-config:type=
  cifs device-config:username=cifs_username \
2 device-config:cifspassword_secret=secret_uuid name-label="CIFS ISO
  SR" type="iso" content-type="iso" shared="true"
```

## xe 命令参考

本节按照命令要寻址的对象对命令进行分组。这些对象按字母顺序列出。

## 设备命令

用来创建和修改 VM 设备（又称 vApp）的命令。有关详细信息，请参阅[vApp](#)。

## 设备参数

设备命令具有下列参数：

| 参数名称                          | 说明      | 类型 |
|-------------------------------|---------|----|
| <code>uuid</code>             | 设备 UUID | 必需 |
| <code>name-description</code> | 设备说明    | 可选 |
| <code>paused</code>           |         | 可选 |
| <code>force</code>            | 强制关闭    | 可选 |

## **appliance-assert-can-be-recovered**

```
1 appliance-assert-can-be-recovered uuid=appliance-uuid database:vdi-uuid  
=vdi-uuid
```

测试存储是否可用于恢复此 VM 设备/vApp。

## **appliance-create**

```
1 appliance-create name-label=name-label [name-description=name-  
description]
```

创建设备/vApp。例如：

```
1 xe appliance-create name-label=my_appliance
```

向设备中添加 VM：

```
1 xe vm-param-set uuid=VM-UUID appliance=appliance-uuid
```

## **appliance-destroy**

```
1 appliance-destroy uuid=appliance-uuid
```

销毁设备/vApp。例如：

```
1 xe appliance-destroy uuid=appliance-uuid
```

### **appliance-recover**

```
1 appliance-recover uuid=appliance-uuid database:vdi-uuid=vdi-uuid [
  paused=true | false]
```

从提供的 VDI 中包含的数据库恢复 VM 设备/vApp。

### **appliance-shutdown**

```
1 appliance-shutdown uuid=appliance-uuid [force=true | false]
```

关闭设备/vApp 中的所有 VM。例如：

```
1 xe appliance-shutdown uuid=appliance-uuid
```

### **appliance-start**

```
1 appliance-start uuid=appliance-uuid [paused=true | false]
```

启动设备/vApp。例如：

```
1 xe appliance-start uuid=appliance-uuid
```

### **审核命令**

审核命令下载池中 RBAC 审核文件的所有可用记录。如果可选参数 `since` 存在，该命令将仅下载自该特定时间点开始的记录。

### **audit-log-get 参数**

`audit-log-get` 具有以下参数

| 参数名称                  | 说明                        | 类型 |
|-----------------------|---------------------------|----|
| <code>filename</code> | 将池的审核日志写入 <i>filename</i> | 必需 |
| <code>since</code>    | 特定的日期/时间点                 | 可选 |

## audit-log-get

```
1 audit-log-get [since=timestamp] filename=filename
```

例如，要获取自某个精确的毫秒时间戳以来的池审核记录，请运行以下命令：

运行以下命令：

```
1 xe audit-log-get since=2009-09-24T17:56:20.530Z filename=/tmp/auditlog-
pool-actions.out
```

## 绑定命令

用于使用网络绑定的命令，以通过物理接口故障转移提供恢复能力。有关详细信息，请参阅[网络连接](#)。

绑定对象是将主节点和成员 PIF 粘附在一起的引用对象。主节点 PIF 是必须用作整体 PIF 以引用绑定的绑定接口。成员 PIF 是组合成高级绑定接口的两个或更多个物理接口的集合。

## 绑定参数

绑定具有下列参数：

| 参数名称                 | 说明                | 类型 |
|----------------------|-------------------|----|
| <code>uuid</code>    | 绑定的唯一标识符/对象引用     | 只读 |
| <code>master</code>  | 主节点绑定 PIF 的 UUID  | 只读 |
| <code>members</code> | 基础绑定 PIF 的 UUID 集 | 只读 |

## bond-create

```
1 bond-create network-uuid=network_uuid pif-uuids=pif_uuid_1,pif_uuid_2
,...
```

在通过现有 PIF 对象列表指定的网络上创建绑定网络接口。在以下任何情况下，该命令都会失败：

- 如果 PIF 已位于其他绑定中
- 如果任何成员已设置了 VLAN 标记
- 如果所引用的 PIF 不在同一 Citrix Hypervisor 服务器上
- 如果提供的 PIF 少于 2 个

## **bond-destroy**

```
1 bond-destroy uuid=bond_uuid
```

从主机删除由绑定接口的 UUID 指定的相应绑定接口。

## **bond-set-mode**

```
1 bond-set-mode uuid=bond_uuid mode=bond_mode
```

更改绑定模式。

## **CD 命令**

与 Citrix Hypervisor 服务器上的物理 CD/DVD 驱动器一起使用的命令。

## **CD 参数**

CD 具有下列参数：

| 参数名称                            | 说明                      | 类型        |
|---------------------------------|-------------------------|-----------|
| <code>uuid</code>               | CD 的唯一标识符/对象引用          | 只读        |
| <code>name-label</code>         | CD 的名称                  | 读取/写入     |
| <code>name-description</code>   | CD 的说明文本                | 读取/写入     |
| <code>allowed-operations</code> | 可对此 CD 执行的操作的列表         | 只读 set 参数 |
| <code>current-operations</code> | 当前正在对此 CD 执行的操作的列表      | 只读 set 参数 |
| <code>sr-uuid</code>            | 此 CD 所属的 SR 的唯一标识符/对象引用 | 只读        |
| <code>sr-name-label</code>      | 此 CD 所属的 SR 的名称         | 只读        |

| 参数名称                 | 说明                                                       | 类型           |
|----------------------|----------------------------------------------------------|--------------|
| vbd-uuids            | 连接到此 CD 的 VM 上的 VBD 的唯一标识符列表                             | 只读 set 参数    |
| crashdump-uuids      | 未在 CD 上使用。由于故障转储无法写入 CD                                  | 只读 set 参数    |
| virtual-size         | CD 在 VM 中显示时的大小（以字节为单位）                                  | 只读           |
| physical-utilisation | CD 映像 in SR 上占用的物理空间大小（以字节为单位）                           | 只读           |
| type                 | 对于 CD，设置为用户                                              | 只读           |
| sharable             | CD 驱动器是否可共享。默认值为 <b>false</b> 。                          | 只读           |
| read-only            | CD 是否为只读，如果为 <b>false</b> ，则设备可写入。对 CD 始终为 <b>true</b> 。 | 只读           |
| storage-lock         | 如果在存储级别锁定此磁盘，则值为 <b>true</b> 。                           | 只读           |
| parent               | 如果此 CD 是链的一部分，则引用父磁盘。                                    | 只读           |
| missing              | 如果 SR 扫描操作报告此 CD 未在磁盘上显示，则值为 <b>true</b>                 | 只读           |
| other-config         | 为 CD 指定额外配置参数的键/值对列表                                     | 读取/写入 map 参数 |
| location             | 装载设备的路径                                                  | 只读           |
| managed              | 如果设备被托管，则值为 <b>true</b>                                  | 只读           |
| xenstore-data        | 插入到 xenstore 树中的数据                                       | 只读 map 参数    |
| sm-config            | 存储管理器设备配置键的名称和描述                                         | 只读 map 参数    |
| is-a-snapshot        | 如果此模板为 CD 快照，则值为 <b>true</b>                             | 只读           |
| snapshot_of          | 以此模板为快照的 CD 的 UUID                                       | 只读           |
| snapshots            | 根据此 CD 生成的任何快照的 UUID                                     | 只读           |

| 参数名称                       | 说明       | 类型 |
|----------------------------|----------|----|
| <code>snapshot_time</code> | 快照操作的时间戳 | 只读 |

## cd-list

```
1 cd-list [params=param1,param2,...] [parameter=parameter_value]
```

列出 Citrix Hypervisor 服务器或池上的 CD 和 ISO（CD 映像文件），按可选参数 `params` 过滤。

如果使用可选参数 `params`，则 `params` 的值是一个字符串，其中包含您希望显示的此对象的参数列表。或者，可以使用关键字 `all` 显示所有参数。如果不使用 `params`，则返回的列表将显示所有可用参数的默认子集。

可选参数可以为本节开头列出的 CD 参数中的任意数量。

## 群集命令

用于使用群集池的命令。

群集池是启用了群集功能的资源池。将这些池与 GFS2 SR 结合使用。有关详细信息，请参阅[群集池](#)。

可以使用标准对象列出命令（`xe cluster-list` 和 `xe cluster-host-list`）列出群集对象和群集主机对象，并使用标准参数命令操纵参数。有关详细信息，请参阅低级参数命令。

用于使用群集池的命令。

## 群集参数

群集具有以下参数：

| 参数名称                       | 说明                                            | 类型        |
|----------------------------|-----------------------------------------------|-----------|
| <code>uuid</code>          | 群集的唯一标识符/对象参考                                 | 只读        |
| <code>cluster-hosts</code> | 群集中主机的唯一标识符/对象引用的列表                           | 只读 set 参数 |
| <code>cluster-token</code> | <code>xapi-clusterd</code> 在其他主机上与自身通信时所使用的密钥 | 只读        |
| <code>cluster-stack</code> | 提供群集功能的技术堆栈。可能的值为 <code>corosync</code> 。     | 只读        |

| 参数名称                                   | 说明                                              | 类型           |
|----------------------------------------|-------------------------------------------------|--------------|
| <code>allowed-operations</code>        | 列出在此种状态下允许执行的操作。此列表只是建议性的，并且客户端读取此字段时群集状态可能已更改。 | 只读 set 参数    |
| <code>current-operations</code>        | 列出当前正在执行的操作。此列表只是建议性的，并且客户端读取此字段时群集状态可能已更改。     | 只读 set 参数    |
| <code>token-timeout</code>             | corosync 令牌超时，以秒为单位                             | 只读           |
| <code>token-timeout-coefficient</code> | corosync 令牌超时系数，以秒为单位                           | 只读           |
| <code>pool-auto-join</code>            | 如果自动向群集中加入新池成员，则为 true。此参数将设置为 <b>true</b> 。    | 只读           |
| <code>cluster-config</code>            | 为群集指定额外配置参数的键/值对的列表。                            | 只读 map 参数    |
| <code>other-config</code>              | 为群集指定额外配置参数的键/值对的列表。                            | 读取/写入 map 参数 |

### **cluster-host-create**

```
1 cluster-host-create cluster-uuid=cluster_uuid host-uuid=host_uuid pif-uuid=pif_uuid
```

将主机添加到现有群集。

### **cluster-host-destroy**

```
1 cluster-host-destroy uuid=host_uuid
```

销毁群集主机，实际上就是离开群集。

### **cluster-host-disable**

```
1 cluster-host-disable uuid=cluster_uuid
```

为已启用的群集主机禁用群集成员身份。

### **cluster-host-enable**

```
1 cluster-host-enable uuid=cluster_uuid
```

为已禁用的群集主机启用群集成员关系。

### **cluster-host-force-destroy**

```
1 cluster-host-force-destroy uuid=cluster_host
```

强制销毁群集主机对象，实际上就是离开群集。

### **cluster-pool-create**

```
1 cluster-pool-create network-uuid=network_uuid [cluster-stack=
  cluster_stack] [token-timeout=token_timeout] [token-timeout-
  coefficient=token_timeout_coefficient]
```

创建池级别的群集。

### **cluster-pool-destroy**

```
1 cluster-pool-destroy cluster-uuid=cluster_uuid
```

销毁池级别的群集。池将继续存在，但不再是群集化的，且无法再使用 GFS2 SR。

### **cluster-pool-force-destroy**

```
1 cluster-pool-force-destroy cluster-uuid=cluster_uuid
```

强制销毁池级别的群集。

### **cluster-pool-resync**

```
1 cluster-pool-resync cluster-uuid=cluster_uuid
```

在池之间重新同步群集。

## 控制台命令

用于控制台的命令。

可以使用标准对象列出命令 (`xe console-list`) 列出控制台对象，并使用标准参数命令操纵参数。有关详细信息，请参阅低级参数命令。

## 控制台参数

控制台具有下列参数：

| 参数名称                       | 说明                                                                                                           | 类型           |
|----------------------------|--------------------------------------------------------------------------------------------------------------|--------------|
| <code>uuid</code>          | 控制台的唯一标识符/对象引用                                                                                               | 只读           |
| <code>vm-uuid</code>       | 打开控制台的 VM 的唯一标识符/对象引用                                                                                        | 只读           |
| <code>vm-name-label</code> | 打开控制台的 VM 的名称                                                                                                | 只读           |
| <code>protocol</code>      | 此控制台使用的协议。可能的值为 <code>vt100</code> (VT100 终端)、 <code>rfb</code> (远程帧缓冲协议，用于 VNC) 或 <code>rdp</code> (远程桌面协议) | 只读           |
| <code>location</code>      | 控制台服务的 URI                                                                                                   | 只读           |
| <code>other-config</code>  | 为控制台指定额外配置参数的键/值对列表。                                                                                         | 读取/写入 map 参数 |

## console

```
1 console
```

连接到特定的控制台。

## 诊断命令

用于从 Citrix Hypervisor 收集诊断信息的命令。

## diagnostic-compact

```
1 diagnostic-compact
```

执行主要 GC 收集和堆压缩。

### **diagnostic-db-log**

```
1 diagnostic-db-log
```

开始记录数据库操作。警告：启动后，无法停止此操作。

### **diagnostic-db-stats**

```
1 diagnostic-db-stats
```

显示数据库统计信息。

### **diagnostic-gc-stats**

```
1 diagnostic-gc-stats
```

显示 GC 统计信息。

### **diagnostic-license-status**

```
1 diagnostic-license-status
```

帮助诊断池级别的许可问题。

### **diagnostic-net-stats**

```
1 diagnostic-net-stats [uri=uri] [method=method] [params=param1,param2  
...]
```

显示网络统计信息。

### **diagnostic-timing-stats**

```
1 diagnostic-timing-stats
```

显示计时统计信息。

### **diagnostic-vdi-status**

```
1 diagnostic-vdi-status uuid=vdi_uuid
```

查询 VDI 的锁定和共享状态。

### **diagnostic-vm-status**

```
1 diagnostic-vm-status uuid=vm_uuid
```

查询可在其上启动 VM 的主机，检查所有 VBD 的共享/锁定状态。

### 灾难恢复命令

用来在发生灾难后恢复 VM 的命令

### **drtask-create**

```
1 drtask-create type=type sr-whitelist=sr-white-list device-config=device  
-config
```

创建灾难恢复任务。例如，要连接到 iSCSI SR 以准备进行灾难恢复，请运行以下命令：

```
1 xe drtask-create type=lvmoiscsi device-config:target=target-ip-address  
  \  
2   device-config:targetIQN=targetIQN device-config:SCSIid=SCSIid \  
3   sr-whitelist=sr-uuid-list
```

#### 注意：

命令 `sr-whitelist` 将列出 SR UUID。 `drtask-create` 命令仅引入并连接到其中一个 UUID 处于白名单中的 SR。

### **drtask-destroy**

```
1 drtask-destroy uuid=dr-task-uuid
```

销毁灾难恢复任务并忘记所引入的 SR。

### **vm-assert-can-be-recovered**

```
1 vm-assert-can-be-recovered uuid=vm-uuid database:vdi-uuid=vdi-uuid
```

测试存储是否可用于恢复此 VM。

### **appliance-assert-can-be-recovered**

```
1 appliance-assert-can-be-recovered uuid=appliance-uuid database:vdi-uuid
  =vdi-uuid
```

检查包含设备/vAPP 磁盘的存储是否可见。

### **appliance-recover**

```
1 appliance-recover uuid=appliance-uuid database:vdi-uuid=vdi-uuid [force
  =true | false]
```

从提供的 VDI 中包含的数据库恢复设备/vAPP。

### **vm-recover**

```
1 vm-recover uuid=vm-uuid database:vdi-uuid=vdi-uuid [force=true | false]
```

从提供的 VDI 中包含的数据库恢复 VM。

### **sr-enable-database-replication**

```
1 sr-enable-database-replication uuid=sr_uuid
```

允许将 XAPI 数据库复制到指定（共享）SR。

## sr-disable-database-replication

```
1 sr-disable-database-replication uuid=sr_uuid
```

禁止将 XAPI 数据库复制到指定 SR。

### 示例用法

以下示例显示上下文中的 DR CLI 命令：

在主站点上，启用数据库复制：

```
1 xe sr-database-replication uuid=sr-uuid
```

发生灾难后，在辅助站点上连接到该 SR。device-config 命令与 sr-probe 具有相同的字段。

```
1 xe drtask-create type=lvmoiscsi \  
2     device-config:target=target ip address \  
3     device-config:targetIQN=target-iqn \  
4     device-config:SCSIid=scsi-id \  
5     sr-whitelist=sr-uuid
```

在 SR 上查找数据库 VDI：

```
1 xe vdi-list sr-uuid=sr-uuid type=Metadata
```

在数据库 VDI 中查询存在的 VM：

```
1 xe vm-list database:vdi-uuid=vdi-uuid
```

恢复 VM：

```
1 xe vm-recover uuid=vm-uuid database:vdi-uuid=vdi-uuid
```

销毁 DR 任务。由 DR 任务引入但并非 VM 所需的任何 SR 都将被销毁：

```
1 xe drtask-destroy uuid=drtask-uuid
```

### 事件命令

用于事件的命令。

## 事件类

下表列出了事件类：

| 类名称     | 说明                          |
|---------|-----------------------------|
| pool    | 物理主机的池                      |
| vm      | 虚拟机                         |
| host    | 物理主机                        |
| network | 虚拟网络                        |
| vif     | 虚拟网络接口                      |
| pif     | 物理网络接口（将独立的 VLAN 表示为多个 PIF） |
| sr      | 存储库                         |
| vdi     | 虚拟磁盘映像                      |
| vbd     | 虚拟块设备                       |
| pbd     | 物理块设备，主机可通过这些设备访问 SR        |

**event-wait**

```
1 event-wait class=class_name [param-name=param_value] [param-name=/=
  param_value]
```

阻止其他命令执行，直到存在满足命令中给定条件的对象。参数 `x=y` 表示“等待字段 x 取值 y”，`x/=y` 表示“等待字段 x 取除 y 以外的任何值”。

示例：等待特定 VM 运行。

```
1 xe event-wait class=vm name-label=myvm power-state=running
```

在名为 `myvm` 的 VM 的 `power-state` 为“正在运行”之前，将一直阻止执行其他命令。

示例：等待特定 VM 重新启动：

```
1 xe event-wait class=vm uuid=$VM start-time=/=$(xe vm-list uuid=$VM
  params=start-time --minimal)
```

在 UUID 为 `$VM` 的 VM 重新启动之前，将一直阻止执行其他命令。此命令使用值 `start-time` 来确定 VM 重新启动的时间。

类名称可以是本节开头列出的任意事件类。参数可以是 CLI 命令 `class-param-list` 列出的任意参数。

**GPU 命令**

用于使用物理 GPU、GPU 组和虚拟 GPU 的命令。

可以使用标准对象列出命令列出 GPU 对象: `xe pgpu-list`、`xe gpu-group-list` 和 `xe vgpu-list`。可以使用标准参数命令操纵参数。有关详细信息, 请参阅低级参数命令。

**物理 GPU 参数**

物理 GPU (pGPU) 具有下列参数:

| 参数名称                              | 说明                                                                       | 类型           |
|-----------------------------------|--------------------------------------------------------------------------|--------------|
| <code>uuid</code>                 | pGPU 的唯一标识符/对象引用                                                         | 只读           |
| <code>vendor-name</code>          | pGPU 的供应商名称                                                              | 只读           |
| <code>device-name</code>          | 供应商分配给此 pGPU 型号的名称                                                       | 只读           |
| <code>gpu-group-uuid</code>       | Citrix Hypervisor 已自动将此 pGPU 分配到的 GPU 组的唯一标识符/对象引用。池中各主机上相同的 pGPU 将组合到一起 | 只读           |
| <code>gpu-group-name-label</code> | 将 pGPU 分配到的 GPU 组的名称                                                     | 只读           |
| <code>host-uuid</code>            | 此 pGPU 连接到的 Citrix Hypervisor 服务器的唯一标识符/对象引用                             | 只读           |
| <code>host-name-label</code>      | 此 pGPU 连接到的 Citrix Hypervisor 服务器的名称                                     | 只读           |
| <code>pci-id</code>               | PCI 标识符                                                                  | 只读           |
| <code>dependencies</code>         | 列出直通到同一个 VM 的相关 PCI 设备                                                   | 读取/写入 map 参数 |
| <code>other-config</code>         | 为 pGPU 指定额外配置参数的键/值对列表                                                   | 读取/写入 map 参数 |
| <code>supported-VGPU-types</code> | 底层硬件支持的虚拟 GPU 类型的列表                                                      | 只读           |
| <code>enabled-VGPU-types</code>   | 已为此 pGPU 启用的虚拟 GPU 类型的列表                                                 | 读取/写入        |
| <code>resident-VGPUs</code>       | 在此 pGPU 上运行的 vGPU 的列表                                                    | 只读           |

**pgpu-disable-dom0-access**

```
1 pgpu-disable-dom0-access uuid=uuid
```

禁用对 dom0 的 pGPU 访问。

**pgpu-enable-dom0-access**

```
1 pgpu-enable-dom0-access uuid=uuid
```

启用对 dom0 的 pGPU 访问。

**GPU 组参数**

GPU 组具有下列参数：

| 参数名称                              | 说明                                               | 类型            |
|-----------------------------------|--------------------------------------------------|---------------|
| <code>uuid</code>                 | GPU 组的唯一标识符/对象引用                                 | 只读            |
| <code>name-label</code>           | GPU 组的名称                                         | 读取/写入         |
| <code>name-description</code>     | GPU 组的描述性文本                                      | 读取/写入         |
| <code>VGPU-uuids</code>           | 列出 GPU 组中虚拟 GPU 的唯一标识符/对象引用                      | 只读 set 参数     |
| <code>PGPU-uuids</code>           | 列出 GPU 组中 pGPU 的唯一标识符/对象引用                       | 只读 set 参数     |
| <code>other-config</code>         | 为 GPU 组指定额外配置参数的键/值对列表                           | 读取/写入 map 参数  |
| <code>supported-VGPU-types</code> | 底层硬件支持的所有虚拟 GPU 类型的联合体                           | 只读            |
| <code>enabled-VGPU-types</code>   | 已在底层 pGPU 上启用的所有虚拟 GPU 类型的联合体                    | 只读            |
| <code>allocation-algorithm</code> | 组中 pGPU 上分配虚拟 GPU 的 Depth-first/Breadth-first 设置 | 读取/写入 enum 参数 |

**GPU 组操作**

用于 GPU 组的命令

**gpu-group-create**

```
1 gpu-group-create name=label=name_for_group [name-description=
  description]
```

创建一个可将 pGPU 迁入的新（空）GPU 组。

**gpu-group-destroy**

```
1 gpu-group-destroy uuid=uuid_of_group
```

销毁 GPU 组；仅允许空组。

**gpu-group-get-remaining-capacity**

```
1 gpu-group-get-remaining-capacity uuid=uuid_of_group vgpu-type-uuid=
  uuid_of_vgpu_type
```

返回可在此 GPU 组中实例化的指定类型的虚拟 GPU 新增数量。

**gpu-group-param-set**

```
1 gpu-group-param-set uuid=uuid_of_group allocation-algorithm=breadth-
  first|depth-first
```

更改 GPU 组用于将虚拟 GPU 分配给 pGPU 的算法。

**gpu-group-param-get-uuid**

```
1 gpu-group-param-get-uuid uuid=uuid_of_group param-name=supported-vGPU-
  types|enabled-vGPU-types
```

返回此 GPU 组的受支持或已启用类型。

## 虚拟 GPU 参数

虚拟 GPU 具有以下参数：

| 参数名称              | 说明                 | 类型 |
|-------------------|--------------------|----|
| <code>uuid</code> | 虚拟 GPU 的唯一标识符/对象引用 | 只读 |

| 参数名称                              | 说明                                         | 类型           |
|-----------------------------------|--------------------------------------------|--------------|
| <code>vm-uuid</code>              | 将虚拟 GPU 分配到的 VM 的唯一标识符/对象引用                | 只读           |
| <code>vm-name-label</code>        | 将虚拟 GPU 分配到的 VM 的名称                        | 只读           |
| <code>gpu-group-uuid</code>       | 虚拟 GPU 所属的 GPU 组的唯一标识符/对象引用                | 只读           |
| <code>gpu-group-name-label</code> | 虚拟 GPU 所属的 GPU 组的名称                        | 只读           |
| <code>currently-attached</code>   | 如果具有 GPU 直通功能的 VM 正在运行，则返回 true，否则返回 false | 只读           |
| <code>other-config</code>         | 为虚拟 GPU 指定额外配置参数的键/值对列表                    | 读取/写入 map 参数 |
| <code>type-uuid</code>            | 此虚拟 GPU 的虚拟 GPU 类型的唯一标识符/对象引用              | 读取/写入 map 参数 |
| <code>type-model-name</code>      | 与虚拟 GPU 类型相关联的模型名称                         | 只读           |

#### 虚拟 GPU 类型参数

##### 注意：

除非存在 GPU 供应商提供的受支持的软件和图形卡，否则 GPU 直通功能和虚拟 GPU 与实时迁移、存储实时迁移或 VM 挂起功能不兼容。不能迁移没有此支持的 VM 以避免出现停机时间。有关 NVIDIA vGPU 与实时迁移、存储实时迁移和 VM 挂起功能的兼容性信息，请参阅[图形](#)。

虚拟 GPU 类型具有以下参数：

| 参数名称                      | 说明                                | 类型 |
|---------------------------|-----------------------------------|----|
| <code>uuid</code>         | 虚拟 GPU 类型的唯一标识符/对象引用              | 只读 |
| <code>vendor-name</code>  | 虚拟 GPU 供应商的名称                     | 只读 |
| <code>model-name</code>   | 与虚拟 GPU 类型相关联的模型名称                | 只读 |
| <code>freeze-frame</code> | 虚拟 GPU 类型的 Framebuffer 大小（以字节为单位） | 只读 |

| 参数名称                            | 说明                      | 类型 |
|---------------------------------|-------------------------|----|
| <code>max-heads</code>          | 虚拟 GPU 类型支持的最大显示数量      | 只读 |
| <code>supported-on-PGPUs</code> | 支持此虚拟 GPU 类型的 pGPU 的列表  | 只读 |
| <code>enabled-on-PGPUs</code>   | 启用了此虚拟 GPU 类型的 pGPU 的列表 | 只读 |
| <code>VGPU-uuids</code>         | 此类型的虚拟 GPU 的列表          | 只读 |

## 虚拟 GPU 操作

### `vgpu-create`

```
1 vgpu-create vm-uuid=uuid_of_vm gpu_group_uuid=uuid_of_gpu_group [vgpu-type-uuid=uuid_of_vgpu-type]
```

创建虚拟 GPU。此命令将 VM 连接到指定的 GPU 组并根据需要指定虚拟 GPU 类型。如果未指定虚拟 GPU 类型，则假设使用“直通”类型。

### `vgpu-destroy`

```
1 vgpu-destroy uuid=uuid_of_vgpu
```

销毁指定的虚拟 GPU。

### 为使用虚拟 GPU 的 VM 禁用 VNC

```
1 xe vm-param-add uuid=uuid_of_vmparam-name=platform vgpu_vnc_enabled=true|false
```

使用 `false` 禁用 VM 的 VNC 控制台，因为它可以将 `disablevnc=1` 传递到显示模拟器。默认情况下，启用 VNC。

## 主机命令

与 Citrix Hypervisor 服务器交互的命令。

Citrix Hypervisor 服务器是运行 Citrix Hypervisor 软件的物理服务器。在这些主机上运行的 VM 受具有特权的虚拟机（称为控制域或域 0）的控制。

可以使用标准对象列出命令列出 Citrix Hypervisor 服务器对象：`xe host-list`、`xe host-cpu-list` 和 `xe host-crashdump-list`。可以使用标准参数命令操纵参数。有关详细信息，请参阅低级参数命令。

### 主机选择器

此处列出的多个命令具有用于选择在其上执行操作的一个或多个 Citrix Hypervisor 服务器的通用机制。最简单的方法是提供参数 `host=uuid_or_name_label`。也可以通过按字段值过滤主机的完整列表来指定 Citrix Hypervisor。例如，指定 `enabled=true` 将会选择 `enabled` 字段为 `true` 的所有 Citrix Hypervisor 服务器。如果有多个匹配的 Citrix Hypervisor 服务器并且操作可以在多个 Citrix Hypervisor 服务器上执行，则必须指定 `--multiple` 才能执行该操作。本节开头介绍了可匹配的完整参数列表。您可以通过运行命令 `xe host-list params=all` 来获取此命令的列表。如果未提供用于选择 Citrix Hypervisor 服务器的参数，则将在所有 Citrix Hypervisor 服务器上执行该操作。

### 主机参数

Citrix Hypervisor 服务器具有以下参数：

| 参数名称                                           | 说明                                                                                               | 类型           |
|------------------------------------------------|--------------------------------------------------------------------------------------------------|--------------|
| <code>uuid</code>                              | Citrix Hypervisor 服务器的唯一标识符/对象引用                                                                 | 只读           |
| <code>name-label</code>                        | Citrix Hypervisor 服务器的名称                                                                         | 读取/写入        |
| <code>name-description</code>                  | Citrix Hypervisor 服务器的描述字符串                                                                      | 只读           |
| <code>enabled</code>                           | 如果禁用，则值为 <code>false</code> 。这样可以防止任何新 VM 在主机上启动并让主机做好关闭或重新启动准备。如果主机处于启用状态，则值为 <code>true</code> | 只读           |
| <code>API-version-major</code>                 | 主版本号                                                                                             | 只读           |
| <code>API-version-minor</code>                 | 次版本号                                                                                             | 只读           |
| <code>API-version-vendor</code>                | API 供应商的标识                                                                                       | 只读           |
| <code>API-version-vendor-implementation</code> | 供应商实现的详细信息                                                                                       | 只读 map 参数    |
| <code>logging</code>                           | 日志记录配置                                                                                           | 读取/写入 map 参数 |
| <code>suspend-image-sr-uuid</code>             | 挂起的映像所在 SR 的唯一标识符/对象引用                                                                           | 读取/写入        |

| 参数名称                               | 说明                                                                                           | 类型           |
|------------------------------------|----------------------------------------------------------------------------------------------|--------------|
| <code>crash-dump-sr-uuid</code>    | 故障转储所在的 SR 的唯一标识符/对象引用                                                                       | 读取/写入        |
| <code>software-version</code>      | 版本控制参数及其值的列表                                                                                 | 只读 map 参数    |
| <code>capabilities</code>          | Citrix Hypervisor 服务器可以运行的 Xen 版本列表                                                          | 只读 set 参数    |
| <code>other-config</code>          | 为 Citrix Hypervisor 服务器指定额外配置参数的键/值对列表                                                       | 读取/写入 map 参数 |
| <code>chipset-info</code>          | 用来指定芯片组相关信息的键/值对列表                                                                           | 只读 map 参数    |
| <code>hostname</code>              | Citrix Hypervisor 服务器主机名                                                                     | 只读           |
| <code>address</code>               | Citrix Hypervisor 服务器 IP 地址                                                                  | 只读           |
| <code>license-server</code>        | 用来指定许可证服务器相关信息的键/值对列表。与 Citrix 产品通信使用的默认端口为 27000。有关因发生冲突而更改端口号的信息，请参阅 <a href="#">更改端口号</a> | 只读 map 参数    |
| <code>supported-bootloaders</code> | Citrix Hypervisor 服务器支持的引导加载器列表，例如 pygrub、eliloader                                          | 只读 set 参数    |
| <code>memory-total</code>          | Citrix Hypervisor 服务器上的物理 RAM 总量（以字节为单位）                                                     | 只读           |
| <code>memory-free</code>           | 可分配给 VM 的剩余物理 RAM 总量（以字节为单位）                                                                 | 只读           |
| <code>host-metrics-live</code>     | 如果主机可以正常运行，则为 true                                                                           | 只读           |
| <code>logging</code>               | <code>syslog_destination</code> 键可设置为远程侦听 syslog 服务的主机名。                                     | 读取/写入 map 参数 |
| <code>allowed-operations</code>    | 列出在此种状态下允许执行的操作。此列表只是建议性的，并且客户端读取此字段时服务器状态可能已更改。                                             | 只读 set 参数    |
| <code>current-operations</code>    | 列出当前正在执行的操作。此列表只是建议性的，并且客户端读取此字段时服务器状态可能已更改。                                                 | 只读 set 参数    |

| 参数名称                        | 说明                            | 类型        |
|-----------------------------|-------------------------------|-----------|
| patches                     | 主机修补程序集                       | 只读 set 参数 |
| blobs                       | 二进制数据存储                       | 只读        |
| memory-free-computed        | 对主机上最大可用内存量的保守估算              | 只读        |
| ha-statefiles               | 所有高可用性功能状态文件的 UUID            | 只读        |
| ha-network-peers            | 出现故障时可托管此主机上 VM 的所有主机的 UUID   | 只读        |
| external-auth-type          | 外部身份验证类型，例如 Active Directory。 | 只读        |
| external-auth-service-name  | 外部身份验证服务的名称                   | 只读        |
| external-auth-configuration | 外部身份验证服务的配置信息。                | 只读 map 参数 |

Citrix Hypervisor 服务器包含的一些其他对象也具有参数列表。

Citrix Hypervisor 服务器上的 CPU 具有下列参数：

| 参数名称        | 说明                                                   | 类型 |
|-------------|------------------------------------------------------|----|
| uuid        | CPU 的唯一标识符/对象引用                                      | 只读 |
| number      | Citrix Hypervisor 服务器中的物理 CPU 内核数量                   | 只读 |
| vendor      | 表示 CPU 名称的供应商字符串                                     | 只读 |
| speed       | CPU 时钟速度（以赫兹为单位）                                     | 只读 |
| modelname   | 表示 CPU 型号的供应商字符串，例如，“Intel(R) Xeon(TM) CPU 3.00 GHz” | 只读 |
| stepping    | CPU 修订号                                              | 只读 |
| flags       | 物理 CPU 的标志（功能字段的解码版本）                                | 只读 |
| Utilisation | 当前 CPU 使用率                                           | 只读 |
| host-uuid   | CPU 所在主机的 UUID                                       | 只读 |

| 参数名称                | 说明         | 类型 |
|---------------------|------------|----|
| <code>model</code>  | 物理 CPU 的型号 | 只读 |
| <code>family</code> | 物理 CPU 系列号 | 只读 |

Citrix Hypervisor 服务器上的故障转储具有下列参数：

| 参数名称                   | 说明                                                                                                 | 类型 |
|------------------------|----------------------------------------------------------------------------------------------------|----|
| <code>uuid</code>      | 故障转储的唯一标识符/对象引用                                                                                    | 只读 |
| <code>host</code>      | 故障转储对应的 Citrix Hypervisor 服务器                                                                      | 只读 |
| <code>timestamp</code> | 故障转储发生日期和时间的戳，格式为 <code>yyyymmdd-hhmmss-ABC</code> ，其中 <code>ABC</code> 是时区指示器，例如 <code>GMT</code> | 只读 |
| <code>size</code>      | 故障转储的大小（以字节为单位）                                                                                    | 只读 |

## host-all-editions

```
1 host-all-editions
```

获取所有可用版本的列表

## host-apply-edition

```
1 host-apply-edition [host-uuid=host_uuid] [edition=xenserver_edition="free" "per-socket" "xendesktop"]
```

将 Citrix Hypervisor 许可证分配给主机服务器。分配许可证时，Citrix Hypervisor 会联系许可证服务器，并申请指定类型的许可证。如果有可用许可证，则会将该许可证从许可证服务器中签出。

对于适用于 Citrix Virtual Desktops 版本的 Citrix Hypervisor，请使用 `"xendesktop"`。

对于初始许可配置，另请参阅 `license-server-address` 和 `license-server-port`。

## host-backup

```
1 host-backup file-name=backup_filename host=host_name
```

将指定的 Citrix Hypervisor 服务器的控制域备份下载到调用此命令的计算机。将其作为名为 `file-name` 的文件保存在该计算机上。

重要：

`xe host-backup` 命令在本地主机上执行（即不指定特定主机名）时可以起作用，但是不要以这种方式使用此命令。这样做将使用备份文件填充控制域分区。仅从保留了存储备份文件空间的远程主机外计算机上使用此命令。

### **host-bugreport-upload**

```
1 host-bugreport-upload [host-selector=host_selector_value...] [url=
  destination_url http-proxy=http_proxy_name]
```

生成全新错误报告（使用 `xen-bugtool`，包括所有可选文件）并上载到支持 `ftp` 站点或某个其他位置。

将使用标准选择机制来选择应在其上执行此操作的主机（请参阅上文中的主机选择器）。可选参数可以为本节开头列出的主机参数中的任意数量。

可选参数是 `http-proxy`：使用指定的 `http` 代理以及 `url`：上载到此目标 URL。如果未使用可选参数，则不会识别任何代理服务器，并且目标位置为默认的支持 `ftp` 站点。

### **host-call-plugin**

```
1 host-call-plugin host-uuid=host_uuid plugin=plugin fn=function [args=
  args]
```

使用可选参数调用指定主机上的插件中的功能。

### **host-compute-free-memory**

```
1 host-compute-free-memory
```

计算主机上的可用内存量。

### **host-compute-memory-overhead**

```
1 host-compute-memory-overhead
```

计算主机的虚拟化内存开销。

## host-cpu-info

```
1 host-cpu-info [uuid=uuid]
```

列出了有关主机的物理 CPU 的信息。

## host-crashdump-destroy

```
1 host-crashdump-destroy uuid=crashdump_uuid
```

从 Citrix Hypervisor 服务器中删除通过 UUID 指定的主机故障转储。

## host-crashdump-upload

```
1 host-crashdump-upload uuid=crashdump_uuid [url=destination_url] [http-proxy=http_proxy_name]
```

将故障转储上载到支持 ftp 站点或其他位置。如果未使用可选参数，则不会识别任何代理服务器，并且目标位置为默认的支持 ftp 站点。可选参数是 `http-proxy`：使用指定的 http 代理以及 `url`：上载到此目标 URL。

## host-declare-dead

```
1 host-declare-dead uuid=host_uuid
```

声明主机已停止，而不与其进行显式连接。

**警告：**

如果主机实际上并非停止，则此调用比较危险，可能会导致数据丢失。

## host-disable

```
1 host-disable [host-selector=host_selector_value...]
```

禁用指定的 Citrix Hypervisor 服务器，防止在这些主机上启动任何新 VM。此操作可以为关闭或重新启动 Citrix Hypervisor 服务器做好准备。

将使用标准选择机制来选择应在其上执行此操作的主机（请参阅主机选择器）。可选参数可以为本节开头列出的主机参数中的任意数量。

### **host-disable-display**

```
1 host-disable-display uuid=host_uuid
```

禁止显示该主机。

### **host-disable-local-storage-caching**

```
1 host-disable-local-storage-caching
```

禁用指定主机上的本地缓存存储。

### **host-dmesg**

```
1 host-dmesg [host-selector=host_selector_value...]
```

从指定的 Citrix Hypervisor 服务器中获取 Xen dmesg（内核环缓冲的输出）。

将使用标准选择机制来选择应在其上执行此操作的主机（请参阅上文中的主机选择器）。可选参数可以为本节开头列出的主机参数中的任意数量。

### **host-emergency-ha-disable**

```
1 host-emergency-ha-disable [--force]
```

禁用本地主机上的高可用性功能。仅用于恢复安装的高可用性功能已损坏的池。

### **host-emergency-management-reconfigure**

```
1 host-emergency-management-reconfigure interface=  
  uuid_of_management_interface_pif
```

重新配置此 Citrix Hypervisor 服务器的管理接口。仅当 Citrix Hypervisor 服务器处于紧急模式时才使用此命令。紧急模式是指此主机所属资源池的主服务器从网络中消失，经过多次重新尝试后仍无法连接。

### **host-enable**

```
1 host-enable [host-selector=host_selector_value...]
```

启用指定的 Citrix Hypervisor 服务器，以允许在这些主机上启动新 VM。

将使用标准选择机制来选择应在其上执行此操作的主机（请参阅上文中的主机选择器）。可选参数可以为本节开头列出的主机参数中的任意数量。

### **host-enable-display**

```
1 host-enable-display uuid=host_uuid
```

允许显示该主机。

### **host-enable-local-storage-caching**

```
1 host-enable-local-storage-caching sr-uuid=sr_uuid
```

启用指定主机上的本地缓存存储。

### **host-evacuate**

```
1 host-evacuate [host-selector=host_selector_value...]
```

将所有正在运行的 VM 实时迁移到池上的其他适合主机。首先，通过使用 `host-disable` 命令禁用该主机。

如果退出的主机是池主服务器，那么必须选择其他主机作为池主服务器。要在高可用性功能禁用时更改池主服务器，请使用 `pool-designate-new-master` 命令。有关详细信息，请参阅 `pool-designate-new-master`。

启用高可用性功能时，只能选择关闭该服务器，这将导致高可用性功能随机选择一个新主服务器。有关详细信息，请参阅 `host-shutdown`。

将使用标准选择机制来选择应在其上执行此操作的主机（请参阅上文中的主机选择器）。可选参数可以为本节开头列出的主机参数中的任意数量。

### **host-forget**

```
1 host-forget uuid=host_uuid
```

XAPI 代理将忽略指定的 Citrix Hypervisor 服务器，不与其进行显式连接。

使用 `--force` 参数可避免系统提示您确认是否确实想要执行该操作。

**警告:**

如果此池中启用了高可用性功能，请不要使用此命令。首先禁用高可用性功能，然后在您忽略了该主机后再重新启用它。

如果要“忘记”的 Citrix Hypervisor 服务器已停止，此命令将非常有用。但是，如果 Citrix Hypervisor 服务器处于活动状态并且属于池的一部分，请改为使用 `xe pool-eject`。

### **host-get-cpu-features**

```
1 host-get-cpu-features {
2   features=pool_master_cpu_features }
3   [uuid=host_uuid]
```

打印代表主机物理 CPU 功能的十六进制值。

### **host-get-server-certificate**

```
1 host-get-server-certificate
```

获取已安装的服务器 SSL 证书。

### **host-get-sm-diagnostics**

```
1 host-get-sm-diagnostics uuid=uuid
```

显示每个主机的 SM 诊断信息。

### **host-get-system-status**

```
1 host-get-system-status filename=name_for_status_file [entries=
  comma_separated_list] [output=tar.bz2|zip] [host-selector=
  host_selector_value...]
```

将系统状态信息下载到指定文件。可选参数 `entries` 是系统状态条目的逗号分隔列表，这些条目从 `host-get-system-status-capabilities` 命令返回的功能 XML 片段获取。有关详细信息，请参阅 `host-get-system-status-capabilities`。如果未指定，则所有系统状态信息都保存在此文件中。参数 `output` 可能为 `tar.bz2`（默认值）或 `zip`。如果未指定此参数，文件将保存在 `tar.bz2` 表中。

将使用标准选择机制来选择应在其上执行此操作的主机（请参阅上文中的主机选择器）。

## host-get-system-status-capabilities

```
1 host-get-system-status-capabilities [host-selector=host_selector_value
  ...]
```

获取指定主机的系统状态功能。这些功能将作为 XML 片段返回且与以下示例类似：

```
1 <?xml version="1.0" ?>
2 <system-status-capabilities>
3   <capability content-type="text/plain" default-checked="yes" key="
4     xenserver-logs" \
5     max-size="150425200" max-time="-1" min-size="150425200" min-
6     time="-1" \
7     pii="maybe"/>
8   <capability content-type="text/plain" default-checked="yes" \
9     key="xenserver-install" max-size="51200" max-time="-1" min-size
10    ="10240" \
11    min-time="-1" pii="maybe"/>
12   ...
13 </system-status-capabilities>
```

每个功能条目可能具有以下属性。

- **key** 功能的唯一标识符。
- **content-type** 可以是 `text/plain` 或 `application/data`。指示 UI 是否可以呈现条目以供用户使用。
- **default-checked** 可以为 `yes` 或 `no`。指示默认情况下 UI 是否应选择此条目。
- **min-size**, **max-size** 指示此条目的大致大小范围（以字节为单位）。-1 指示大小并不重要。
- **min-time**, **max-time** 指示收集此条目所需的大致时间范围（以秒为单位）。-1 指示时间并不重要。
- **pii** 个人可识别信息。指示条目是否将包含用于标识系统所有者的信息，或网络拓扑的详细信息。属性可能具有以下值之一：
  - **no**：这些条目中不包含 PII
  - **yes**：这些条目中可能或一定包含 PII
  - **maybe**：您可能希望审核这些条目是否包含 PII
  - **if\_customized** 如果未修改文件，则其不包含 PII。但是，由于我们鼓励编辑这些文件，因此此类自定义操作可能会引入 PII。此值尤其适用于控制域中的网络连接脚本。

不管存在任何 PII 声明，任何错误报告都不会包括密码。

将使用标准选择机制来选择应在其上执行此操作的主机（请参阅上文中的主机选择器）。

## host-get-thread-diagnostics

```
1 host-get-thread-diagnostics uuid=uuid
```

显示每个主机的线程诊断信息。

### **host-get-vms-which-prevent-evacuation**

```
1 host-get-vms-which-prevent-evacuation uuid=uuid
```

返回阻止撤走特定主机的 VM 的列表，并显示阻止撤走每个主机的原因。

### **host-is-in-emergency-mode**

```
1 host-is-in-emergency-mode
```

如果 CLI 正在与之通信的主机处于紧急模式，则返回 **true**，否则返回 **false**。此 CLI 命令直接作用于从属主机，即使没有主服务器主机。

### **host-license-add**

```
1 host-license-add [license-file=path/license_filename] [host-uuid=host_uuid]
```

对于 Citrix Hypervisor（免费版），用于解析本地许可证文件，并将其添加到指定的 Citrix Hypervisor 服务器。

### **host-license-remove**

```
1 host-license-remove [host-uuid=host_uuid]
```

删除应用于主机的任何许可。

### **host-license-view**

```
1 host-license-view [host-uuid=host_uuid]
```

显示 Citrix Hypervisor 服务器许可证的内容。

## host-logs-download

```
1 host-logs-download [file-name=logfile_name] [host-selector=  
host_selector_value...]
```

下载指定 Citrix Hypervisor 服务器的日志副本。默认情况下副本保存在一个带时间戳的文件中，文件名为 `hostname-yyyymm-dd T hh:mm:ssZ.tar.gz`。可以使用可选参数 `file-name` 指定其他文件名。

将使用标准选择机制来选择应在其上执行此操作的主机（请参阅上文中的主机选择器）。可选参数可以为本节开头列出的主机参数中的任意数量。

### 重要：

`xe host-logs-download` 命令在本地主机上执行（即不指定特定主机名）时可以起作用，但是不要以这种方式使用此命令。这样做将因日志副本而使控制域分区变得混乱。应该仅从保留了存储日志副本空间的远程主机外计算机上使用此命令。

## host-management-disable

```
1 host-management-disable
```

禁用侦听外部管理网络接口的主机代理，并断开所有连接的 API 客户端（如 XenCenter）。此命令直接在 CLI 连接到的 Citrix Hypervisor 服务器上运行。应用于成员 Citrix Hypervisor 服务器时，该命令不会被转发到池主服务器。

### 警告：

在除主机外的计算机上使用此 CLI 命令时需谨慎。运行此命令后，您无法通过网络远程连接到控制域以重新启用主机代理。

## host-management-reconfigure

```
1 host-management-reconfigure [interface=device] [pif-uuid=uuid]
```

重新配置 Citrix Hypervisor 服务器以将指定网络接口用作其管理接口，即用于连接到 XenCenter 的接口。此命令将重写 `/etc/xen-source-inventory` 中的 `MANAGEMENT_INTERFACE` 键。

如果指定了接口（必须具有 IP 地址）的设备名称，Citrix Hypervisor 服务器将立即重新绑定。此命令适用于正常模式和紧急模式。

如果指定了 PIF 对象的 UUID，Citrix Hypervisor 服务器将确定重新绑定到自身的 IP 地址。执行此命令时一定不能处于紧急模式。

**警告:**

在除主机外的计算机上使用此 CLI 命令时需谨慎，并确保在新接口上有网络连接。请先使用 `xe pif-reconfigure` 建立一个连接。否则，后续 CLI 命令将无法到达 Citrix Hypervisor 服务器。

## host-power-on

```
1 host-power-on [host=host_uuid]
```

打开 Citrix Hypervisor 服务器电源，并启用主机开启功能。使用此命令之前，请在主机上启用 `host-set-power-on`。

## host-reboot

```
1 host-reboot [host-selector=host_selector_value...]
```

重新启动指定的 Citrix Hypervisor 服务器。首先必须使用 `xe host-disable` 命令禁用指定的主机，否则将显示 `HOST_IN_USE` 错误消息。

将使用标准选择机制来选择应在其上执行此操作的主机（请参阅上文中的主机选择器）。可选参数可以为本节开头列出的主机参数中的任意数量。

如果指定的 Citrix Hypervisor 服务器是池的成员，则将处理在关闭时断开的连接，并且池将在 Citrix Hypervisor 服务器重新启动时恢复。其他成员和主服务器将继续正常运行。

如果关闭主服务器，池将不起作用，直到执行以下操作之一为止：

- 使某个成员成为主服务器
- 重新启动原始主服务器并恢复联机状态。

当主服务器恢复联机状态时，成员将重新连接并与主服务器同步。

## host-restore

```
1 host-restore [file-name=backup_filename] [host-selector=host_selector_value...]
```

还原 Citrix Hypervisor 服务器控制软件的名为 `file-name` 的备份。此处使用的“还原”不是通常意义上的完整还原，它仅仅指压缩的备份文件已经解压缩并且解压缩到辅助分区。执行 `xe host-restore` 后，必须引导安装 CD，并使用其“从备份还原”选项。

将使用标准选择机制来选择应在其上执行此操作的主机（请参阅上文中的主机选择器）。可选参数可以为本节开头列出的主机参数中的任意数量。

## host-send-debug-keys

```
1 host-send-debug-keys host-uuid=host_uuid keys=keys
```

将指定的虚拟机管理程序调试密钥发送到指定的主机。

## host-set-hostname-live

```
1 host-set-hostname host-uuid=uuid_of_host hostname=new_hostname
```

更改由 `host-uuid` 指定的 Citrix Hypervisor 服务器的主机名。此命令将控制域数据库中的主机名和 Citrix Hypervisor 服务器的实际 Linux 主机名进行相同设置。`hostname` 的值与 `name_label` 字段的值不同。

## host-set-power-on-mode

```
1 host-set-power-on-mode host=host_uuid power-on-mode={
2   "" | "wake-on-lan" | "iLO" | "DRAC" | "custom" }
3   \
4   [ power-on-config:power_on_ip=ip-address power-on-config:
      power_on_user=user power-on-config:power_on_password_secret=
      secret-uuid ]
```

用于在与远程电源解决方案兼容的 Citrix Hypervisor 主机上启用主机开启功能。使用 `host-set-power-on` 命令时，必须在主机上指定电源管理解决方案的类型（即 `power-on-mode`）。然后使用 `power-on-config` 参数及其关联的键值对指定配置选项。

要使用加密功能存储密码，请指定键 `"power_on_password_secret"`。有关详细信息，请参阅机密。

## host-shutdown

```
1 host-shutdown [host-selector=host_selector_value...]
```

关闭指定的 Citrix Hypervisor 服务器。首先必须使用 `xe host-disable` 命令禁用指定的 Citrix Hypervisor 服务器，否则将显示 `HOST_IN_USE` 错误消息。

将使用标准选择机制来选择应在其上执行此操作的主机（请参阅上文中的主机选择器）。可选参数可以为本节开头列出的主机参数中的任意数量。

如果指定的 Citrix Hypervisor 服务器是池的成员，则将处理在关闭时断开的连接，并且池将在 Citrix Hypervisor 服务器重新启动时恢复。其他成员和主服务器将继续正常运行。

如果关闭主服务器，池将不起作用，直到执行以下操作之一为止：

- 使某个成员成为主服务器
- 重新启动原始主服务器并恢复联机状态。

当主服务器恢复联机状态时，成员将重新连接并与主服务器同步。

如果启用了池的高可用性功能，则将自动使一个成员成为主服务器。如果禁用了高可用性功能，您必须使用 `pool-designate-new-master` 命令将所需服务器手动指定为主服务器。有关详细信息，请参阅 `pool-designate-new-master`。

### **host-sm-dp-destroy**

```
1 host-sm-dp-destroy uuid=uuid dp=dp [allow-leak=true|false]
```

尝试销毁并清理主机上的存储数据路径。如果提供了 `allow-leak=true`，则即使无法完全关闭，它也会删除数据路径的所有记录。

### **host-sync-data**

```
1 host-sync-data
```

将池主服务器上存储的非数据库数据与指定主机同步。

### **host-syslog-reconfigure**

```
1 host-syslog-reconfigure [host-selector=host_selector_value...]
```

在指定的 Citrix Hypervisor 服务器上重新分配 `syslog` 守护程序。此命令应用在主机 `logging` 参数中定义的配置信息。

将使用标准选择机制来选择应在其上执行此操作的主机（请参阅上文中的主机选择器）。可选参数可以为本节开头列出的主机参数中的任意数量。

### **host-data-source-list**

```
1 host-data-source-list [host-selectors=host selector value...]
```

列出可为主机记录的数据源。

使用标准选择机制来选择要在其上执行此操作的主机（请参阅主机选择器）。可选参数可以为本节开头列出的主机参数中的任意数量。如果未提供用于选择主机的参数，将在所有主机上执行该操作。

数据源具有两个参数：`standard` 和 `enabled`。此命令将输出这些参数的值：

- 如果数据源的 `enabled` 设置为 `true`，则指标当前被记录到性能数据库中。
- 如果数据源的 `standard` 设置为 `true`，则默认情况下指标会被记录到性能数据库中。此数据源的 `enabled` 的值也会被设置为 `true`。
- 如果数据源的 `standard` 设置为 `false`，则默认情况下指标不会被记录到性能数据库中。此数据源的 `enabled` 的值也会被设置为 `false`。

要开始将数据源指标记录到性能数据库，请运行 `host-data-source-record` 命令。此命令将 `enabled` 设置为 `true`。要停止记录，请运行 `host-data-source-forget`。此命令将 `enabled` 设置为 `false`。

### host-data-source-record

```
1 host-data-source-record data-source=name_description_of_data_source [
  host-selectors=host_selector_value...]
```

记录主机的指定数据源。

此操作会将数据源中的信息写入指定主机的静态性能指标数据库中。由于性能的原因，此数据库不同于普通的代理数据库。

使用标准选择机制来选择要在其上执行此操作的主机（请参阅主机选择器）。可选参数可以为本节开头列出的主机参数中的任意数量。如果未提供用于选择主机的参数，将在所有主机上执行该操作。

### host-data-source-forget

```
1 host-data-source-forget data-source=name_description_of_data_source [
  host-selectors=host_selector_value...]
```

停止为主机记录指定数据源并忽略所有已记录的数据。

使用标准选择机制来选择要在其上执行此操作的主机（请参阅主机选择器）。可选参数可以为本节开头列出的主机参数中的任意数量。如果未提供用于选择主机的参数，将在所有主机上执行该操作。

### host-data-source-query

```
1 host-data-source-query data-source=name_description_of_data_source [
  host-selectors=host_selector_value...]
```

显示主机的指定数据源。

使用标准选择机制来选择要在其上执行此操作的主机（请参阅主机选择器）。可选参数可以为本节开头列出的主机参数中的任意数量。如果未提供用于选择主机的参数，将在所有主机上执行该操作。

## 日志命令

用于处理日志的命令。

### **log-get**

```
1 log-get
```

返回当前存储在字符串记录器中的日志。

### **log-get-keys**

```
1 log-get-keys
```

列出记录器已知的键。

### **log-reopen**

```
1 log-reopen
```

重新打开所有记录器（使用此功能旋转文件）。

### **log-set-output**

```
1 log-set-output output=output [key=key] [level=level]
```

将所有记录器设置为指定的输出（nil、stderr、string、file:*filename*、syslog:*something*）。

## 消息命令

用于消息的命令。创建消息以通知用户重要事件，并作为警报在 XenCenter 中显示。

可以使用标准对象列出命令（`xe message-list`）列出消息对象，并使用标准参数命令操纵参数。有关详细信息，请参阅低级参数命令。

## 消息参数

| 参数名称                   | 说明                         | 类型 |
|------------------------|----------------------------|----|
| <code>uuid</code>      | 消息的唯一标识符/对象引用              | 只读 |
| <code>name</code>      | 消息的唯一名称。                   | 只读 |
| <code>priority</code>  | 消息优先级。数值越大表明优先级越高。         | 只读 |
| <code>class</code>     | 消息类型，例如 VM。                | 只读 |
| <code>obj-uuid</code>  | 受影响对象的 <code>uuid</code> 。 | 只读 |
| <code>timestamp</code> | 生成该消息的时间。                  | 只读 |
| <code>body</code>      | 消息内容。                      | 只读 |

### message-create

```
1 message-create name=message_name body=message_text [[host-uuid=
  uuid_of_host] | [sr-uuid=uuid_of_sr] | [vm-uuid=uuid_of_vm] | [pool-
  uuid=uuid_of_pool]]
```

创建消息。

### message-destroy

```
1 message-destroy [uuid=message_uuid]
```

销毁现有消息。您可以构建一个脚本来销毁所有消息。例如：

```
1 # Dismiss all alerts \
2   IFS=","; for m in $(xe message-list params=uuid --minimal); do \
3     xe message-destroy uuid=$m \
4     done
```

### 网络命令

用于网络的命令。

可以使用标准对象列出命令 (`xe network-list`) 列出网络对象，并且使用标准参数命令操纵参数。有关详细信息，请参阅低级参数命令。

## 网络参数

网络具有下列参数：

| 参数名称                                     | 说明                                                                                                                                                                                                                                              | 类型        |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <code>uuid</code>                        | 网络的唯一标识符/对象引用                                                                                                                                                                                                                                   | 只读        |
| <code>name-label</code>                  | 网络名称                                                                                                                                                                                                                                            | 读取/写入     |
| <code>name-description</code>            | 网络的说明文本                                                                                                                                                                                                                                         | 读取/写入     |
| <code>VIF-uuids</code>                   | 从 VM 连接到此网络的 VIF（虚拟网络接口）的唯一标识符列表                                                                                                                                                                                                                | 只读 set 参数 |
| <code>PIF-uuids</code>                   | 从 Citrix Hypervisor 服务器连接到此网络的 PIF（物理网络接口）的唯一标识符列表                                                                                                                                                                                              | 只读 set 参数 |
| <code>bridge</code>                      | 与此网络对应的桥在本地 Citrix Hypervisor 服务器上的名称                                                                                                                                                                                                           | 只读        |
| <code>default-locking-mode</code>        | 与 VIF 对象一起用于 ARP 过滤的网络对象。设置为 <code>unlocked</code> 将删除所有与 VIF 相关联的过滤规则。设置为 <code>disabled</code> ，以便 VIF 丢弃所有通信。                                                                                                                                | 读取/写入     |
| <code>purpose</code>                     | 设置 Citrix Hypervisor 服务器使用此网络的用途。设置为 <code>nbd</code> 将使用网络建立 NBD 连接。                                                                                                                                                                           | 读取/写入     |
| <code>other-config:staticroutes</code>   | <code>subnet/netmask/gateway</code> 格式条目的逗号分隔列表，指定用来路由子网的网关地址。例如，将 <code>other-config:static-routes</code> 设置为 <code>172.16.0.0/15/192.168.0.3,172.18.0.0/16</code> 会使 172.16.0.0/15 上的通信通过 192.168.0.3 路由，172.18.0.0/16 上的通信通过 192.168.0.4 路由。 | 读取/写入     |
| <code>other-config:ethtoolautoneg</code> | 设置为 <code>no</code> 会禁用物理接口或网桥的自动协商。默认值为 <code>yes</code> 。                                                                                                                                                                                     | 读取/写入     |
| <code>other-config:ethtool-rx</code>     | 设置为 <code>on</code> 会启用接收校验和，设置为 <code>off</code> 会禁用接收校验和                                                                                                                                                                                      | 读取/写入     |

| 参数名称                                  | 说明                                       | 类型    |
|---------------------------------------|------------------------------------------|-------|
| <code>other-config:ethtool-tx</code>  | 设置为 on 会启用发送校验和，设置为 off 会禁用发送校验和         | 读取/写入 |
| <code>other-config:ethtool-sg</code>  | 设置为 on 会启用分散收集，设置为 off 会禁用分散收集           | 读取/写入 |
| <code>other-config:ethtool-tso</code> | 设置为 on 会启用 TCP 分段卸载，设置为 off 会禁用 TCP 分段卸载 | 读取/写入 |
| <code>other-config:ethtool-ufo</code> | 设置为 on 会启用 UDP 段卸载，设置为 off 会禁用 UDP 段卸载   | 读取/写入 |
| <code>other-config:ethtool-gso</code> | 设置为 on 会启用通用分段卸载，设置为 off 会禁用通用分段卸载       | 读取/写入 |
| <code>blobs</code>                    | 二进制数据存储                                  | 只读    |

## network-create

```
1 network-create name=label=name_for_network [name-description=
  descriptive_text]
```

创建网络。

## network-destroy

```
1 network-destroy uuid=network_uuid
```

销毁现有网络。

## SR-IOV 命令

用于处理 SR-IOV 的命令。

可以使用标准对象列出命令 (`xe network-sriov-list`) 列出 network-sriov 对象，并使用标准参数命令操纵参数。有关详细信息，请参阅低级参数命令。

## SR-IOV 参数

SR-IOV 具有以下参数：

| 参数名称                            | 说明                                        | 类型 |
|---------------------------------|-------------------------------------------|----|
| <code>physical-PIF</code>       | 用于启用 SR-IOV 的 PIF。                        | 只读 |
| <code>logical-PIF</code>        | SR-IOV 逻辑 PIF。用户可以使用此参数创建 SR-IOV VLAN 网络。 | 只读 |
| <code>requires-reboot</code>    | 如果设置为 True，则用于重新启动主机以使 SR-IOV 生效。         | 只读 |
| <code>remaining-capacity</code> | 剩余的可用 VF 的数量。                             | 只读 |

### **network-sriov-create**

```
1 network-sriov-create network-uuid=network_uuid pif-uuid=
  physical_pif_uuid
```

为指定的物理 PIF 创建 SR-IOV 网络对象，并在物理 PIF 上启用 SR-IOV。

### **network-sriov-destroy**

```
1 network-sriov-destroy uuid=network_sriov_uuid
```

删除网络 SR-IOV 对象，并禁用其物理 PIF 上的 SR-IOV。

### **分配 SR-IOV VF**

```
1 xe vif-create device=device_index mac=vf_mac_address network-uuid=
  sriov_network vm-uuid=vm_uuid
```

从 SR-IOV 网络向 VM 分配 VF。

### **SDN 控制器命令**

用于使用 SDN 控制器的命令。

### **sdn-controller-forget**

```
1 sdn-controller-introduce [address=address] [protocol=protocol] [tcp-
  port=tcp_port]
```

引入 SDN 控制器。

### **sdn-controller-introduce**

```
1 sdn-controller-forget uuid=uuid
```

删除 SDN 控制器。

通道命令

用于使用通道的命令。

### **tunnel-create**

```
1 tunnel-create pif-uuid=pif_uuid network-uuid=network_uuid
```

在主机上创建新的通道。

### **tunnel-destroy**

```
1 tunnel-destroy uuid=uuid
```

销毁通道。

修补程序命令

用于使用修补程序的命令。

### **patch-apply**

```
1 patch-apply uuid=patch_uuid host-uuid=host_uuid
```

将之前上载的修补程序应用于指定主机。

### **patch-clean**

```
1 patch-clean uuid=uuid
```

删除之前上载的修补程序文件。

### **patch-destroy**

```
1 patch-destroy uuid=uuid
```

从服务器中删除未应用的修补程序记录 and 文件。

### **patch-pool-apply**

```
1 patch-pool-apply uuid=uuid
```

将之前上载的修补程序应用于池中的所有主机。

### **patch-pool-clean**

```
1 patch-pool-clean uuid=uuid
```

在池中的所有主机上删除之前上载的修补程序文件。

### **patch-precheck**

```
1 patch-precheck uuid=uuid host-uuid=host_uuid
```

运行之前上载到指定主机的修补程序中包含的预检查。

### **patch-upload**

```
1 patch-upload file-name=file_name
```

将修补程序文件上载到服务器。

### **PBD 命令**

用于 PBD（物理块设备）的命令。PBD 是软件对象，Citrix Hypervisor 服务器通过这些对象访问存储库 (SR)。

可以使用标准对象列出命令 (`xe pbd-list`) 列出 PBD 对象，并使用标准参数命令操纵参数。有关详细信息，请参阅低级参数命令。

**PBD 参数**

PBD 具有下列参数：

| 参数名称                            | 说明                                                      | 类型           |
|---------------------------------|---------------------------------------------------------|--------------|
| <code>uuid</code>               | PBD 的唯一标识符/对象引用。                                        | 只读           |
| <code>sr-uuid</code>            | PBD 指向的存储库                                              | 只读           |
| <code>device-config</code>      | 提供给主机的 SR 后端驱动程序的<br>额外配置信息                             | 只读 map 参数    |
| <code>currently-attached</code> | 如果 SR 已连接到此主机，则为<br>True，否则为 False                      | 只读           |
| <code>host-uuid</code>          | 提供 PBD 的物理机的 UUID                                       | 只读           |
| <code>host</code>               | <code>host</code> 字段已弃用。请使用<br><code>host_uuid</code> 。 | 只读           |
| <code>other-config</code>       | 额外的配置信息。                                                | 读取/写入 map 参数 |

### **pbid-create**

```
1 pbid-create host-uuid=uuid_of_host sr-uuid=uuid_of_sr [device-config:key
   =corresponding_value]
```

在您的 Citrix Hypervisor 服务器上创建 PBD。只能在创建时设置只读 `device-config` 参数。

要将映射从 “path” 添加到 “/tmp”，命令行应包含参数 `device-config:path=/tmp`

有关每个 SR 类型上受支持的 `device-config` 键/值对的完整列表，请参阅[存储](#)。

### **pbid-destroy**

```
1 pbid-destroy uuid=uuid_of_pbid
```

销毁指定的 PBD。

### **pbid-plug**

```
1 pbid-plug uuid=uuid_of_pbid
```

尝试将 PBD 插入 Citrix Hypervisor 服务器。如果此命令成功，则引用的 SR（和包含在其中的 VDI）应对 Citrix Hypervisor 服务器可见。

## pbd-unplug

```
1 pbd-unplug uuid=uuid_of_pbd
```

尝试从 Citrix Hypervisor 服务器中拔出 PBD。

## PIF 命令

用于 PIF（代表物理网络接口的对象）的命令。

可以使用标准对象列出命令 ([xe pif-list](#)) 列出 PIF 对象，并使用标准参数命令操纵参数。有关详细信息，请参阅低级参数命令。

## PIF 参数

PIF 具有下列参数：

| 参数名称                                 | 说明                                                     | 类型           |
|--------------------------------------|--------------------------------------------------------|--------------|
| <code>uuid</code>                    | PIF 的唯一标识符/对象引用                                        | 只读           |
| <code>device machine-readable</code> | 接口的名称（例如 eth0）                                         | 只读           |
| <code>MAC</code>                     | PIF 的 MAC 地址                                           | 只读           |
| <code>other-config</code>            | 额外的 PIF 配置 <code>name:value</code> 对。                  | 读取/写入 map 参数 |
| <code>physical</code>                | 如果为 <code>true</code> ，则 PIF 指向实际的物理网络接口               | 只读           |
| <code>currently-attached</code>      | PIF 当前是否连接到此主机？ <code>true</code> 或 <code>false</code> | 只读           |
| <code>MTU</code>                     | PIF 的最大传输单位（以字节为单位）。                                   | 只读           |
| <code>VLAN</code>                    | 通过此接口的所有通信的 VLAN 标记。-1 表示未分配 VLAN 标记                   | 只读           |
| <code>bond-master-of</code>          | 此 PIF 作为主服务器的绑定的 UUID（如果有）                             | 只读           |
| <code>bond-slave-of</code>           | 此 PIF 作为从属服务器的绑定的 UUID（如果有）                            | 只读           |

| 参数名称                  | 说明                                                             | 类型 |
|-----------------------|----------------------------------------------------------------|----|
| management            | 是否将此 PIF 指定为控制域的管理接口                                           | 只读 |
| network-uuid          | 此 PIF 连接到的虚拟网络的唯一标识符/对象引用                                      | 只读 |
| network-name-label    | 此 PIF 连接到的虚拟网络的名称                                              | 只读 |
| host-uuid             | 此 PIF 连接到的 Citrix Hypervisor 服务器的唯一标识符/对象引用                    | 只读 |
| host-name-label       | 此 PIF 连接到的 Citrix Hypervisor 服务器的名称                            | 只读 |
| IP-configuration-mode | 使用的网络地址配置类型；DHCP 或 static                                      | 只读 |
| IP                    | PIF 的 IP 地址。如果 IP 配置模式为 static，则在此处定义；如果 IP 配置模式为 DHCP，则不在此处定义 | 只读 |
| netmask               | PIF 的网络掩码。如果 IP 配置模式为 static，则在此处定义；如果由 DHCP 提供，则不在此处定义        | 只读 |
| gateway               | PIF 的网关地址。如果 IP 配置模式为 static，则在此处定义；如果由 DHCP 提供，则不在此处定义        | 只读 |
| DNS                   | PIF 的 DNS 地址。如果 IP 配置模式为 static，则在此处定义；如果由 DHCP 提供，则不在此处定义     | 只读 |
| io_read_kbs           | 设备的平均读取速率（以 kb/秒为单位）                                           | 只读 |
| io_write_kbs          | 设备的平均写入速率（以 kb/秒为单位）                                           | 只读 |
| carrier               | 此设备的链路状态                                                       | 只读 |
| vendor-id             | 分配给 NIC 供应商的 ID                                                | 只读 |
| vendor-name           | NIC 供应商的名称                                                     | 只读 |
| device-id             | 供应商分配给此 NIC 型号的 ID                                             | 只读 |
| device-name           | 供应商分配给此 NIC 型号的名称                                              | 只读 |

| 参数名称                                      | 说明                                                                               | 类型    |
|-------------------------------------------|----------------------------------------------------------------------------------|-------|
| <code>speed</code>                        | NIC 的数据传输速率                                                                      | 只读    |
| <code>duplex</code>                       | NIC 的双工模式：“全”或“半”                                                                | 只读    |
| <code>pci-bus-path</code>                 | PCI 总线路径地址                                                                       | 只读    |
| <code>other-config: ethtoolspeed</code>   | 设置连接速度（以 Mbps 为单位）                                                               | 读取/写入 |
| <code>other-config: ethtoolautoneg</code> | 设置为 <code>no</code> 会禁用物理接口或网桥的自动协商。默认值为 <code>yes</code> 。                      | 读取/写入 |
| <code>other-config: ethtoolduplex</code>  | 设置 PIF 的双工功能：“全”或“半”。                                                            | 读取/写入 |
| <code>other-config: ethtool-rx</code>     | 设置为 <code>on</code> 会启用接收校验和，设置为 <code>off</code> 会禁用接收校验和                       | 读取/写入 |
| <code>other-config: ethtool-tx</code>     | 设置为 <code>on</code> 会启用发送校验和，设置为 <code>off</code> 会禁用发送校验和                       | 读取/写入 |
| <code>other-config: ethtool-sg</code>     | 设置为 <code>on</code> 会启用分散收集，设置为 <code>off</code> 会禁用分散收集                         | 读取/写入 |
| <code>other-config: ethtool-tso</code>    | 设置为 <code>on</code> 会启用 TCP 分段卸载，设置为 <code>off</code> 会禁用 TCP 分段卸载               | 读取/写入 |
| <code>other-config: ethtool-ufo</code>    | 设置为 <code>on</code> 会启用 UDP 段卸载，设置为 <code>off</code> 会禁用 UDP 段卸载                 | 读取/写入 |
| <code>other-config: ethtool-gso</code>    | 设置为 <code>on</code> 会启用通用分段卸载，设置为 <code>off</code> 会禁用通用分段卸载                     | 读取/写入 |
| <code>other-config: domain</code>         | 用于设置 DNS 搜索路径的逗号分隔列表                                                             | 读取/写入 |
| <code>other-config: bondmiimon</code>     | 链接活跃性检查之间的间隔（以毫秒为单位）                                                             | 读取/写入 |
| <code>other-config: bonddowndelay</code>  | 断开链接后等待的毫秒数，超过此时间即认为链接确实已断开。此参数允许出现短暂的链接中断现象                                     | 读取/写入 |
| <code>other-config: bondupdelay</code>    | 建立链接后等待的毫秒数，超过此时间即认为链接确实已建立。允许链接出现不稳定的状态。默认值为 <code>31s</code> ，以留出交换机开始转发通信的时间。 | 读取/写入 |

| 参数名称                         | 说明                                  | 类型    |
|------------------------------|-------------------------------------|-------|
| <code>disallow-unplug</code> | 如果此 PIF 为专用存储 NIC，则为 true，否则为 false | 读取/写入 |

**注意：**

对 PIF 的 `other-config` 字段所做的更改仅在重新启动后生效。另外，使用 `xe pif-unplug` 和 `xe pif -plug` 命令会导致重写 PIF 配置。

### **pif-forget**

```
1 pif-forget uuid=uuid_of_pif
```

销毁特定主机上的指定 PIF 对象。

### **pif-introduce**

```
1 pif-introduce host-uuid=host_uuid mac=mac_address_for_pif device=
  interface_name
```

在指定的 Citrix Hypervisor 服务器上创建代表物理接口的 PIF 对象。

### **pif-plug**

```
1 pif-plug uuid=uuid_of_pif
```

尝试显示指定的物理接口。

### **pif-reconfigure-ip**

```
1 pif-reconfigure-ip uuid=uuid_of_pif [mode=dhcp|mode=static] gateway=
  network_gateway_address IP=static_ip_for_this_pif netmask=
  netmask_for_this_pif [DNS=dns_address]
```

修改 PIF 的 IP 地址。对于静态 IP 配置，请将 `mode` 参数设置为 **static**，同时将 `gateway`、`IP` 和 `netmask` 参数设置为相应的值。要使用 DHCP，请将 `mode` 参数设置为 `DHCP` 并将静态参数保持为未定义状态。

注意：

对于使用跨树协议并且关闭了（或不支持）STP 快速链接的交换机，当物理网络接口与该交换机上的端口相连时，如果在这些物理网络接口上使用静态 IP 地址，则会产生没有网络流量的时段。

### **pif-reconfigure-ipv6**

```
1 pif-reconfigure-ipv6 uuid=uuid_of_pif mode=mode [gateway=
  network_gateway_address] [IPv6=static_ip_for_this_pif] [DNS=
  dns_address]
```

重新配置 PIF 的 IPv6 地址设置。

### **pif-scan**

```
1 pif-scan host-uuid=host_uuid
```

在 Citrix Hypervisor 服务器上扫描新物理接口。

### **pif-set-primary-address-type**

```
1 pif-set-primary-address-type uuid=uuid primary_address_type=
  address_type
```

更改此 PIF 使用的主地址类型。

### **pif-unplug**

```
1 pif-unplug uuid=uuid_of_pif
```

尝试拔出指定的物理接口。

### 池命令

用于池的命令。池是一个或多个 Citrix Hypervisor 服务器的聚合。一个池使用一个或多个共享存储库，以便在池中的一个主机上运行的 VM 可以准实时地迁移到该池中的另一台主机。此迁移在 VM 仍在运行时发生，无需关闭后再重新打开它。默认情况下，每个 Citrix Hypervisor 服务器实际上是由单个成员组成的一个池。Citrix Hypervisor 服务器加入某个池时，将被指定为一个成员，而其所加入的池将成为池的主服务器。

可使用标准对象列出命令 (`xe pool-list`) 列出单个池对象。可以使用标准参数命令操纵其参数。有关详细信息，请参阅低级参数命令。

## 池参数

池具有下列参数：

| 参数名称                                      | 说明                                         | 类型           |
|-------------------------------------------|--------------------------------------------|--------------|
| <code>uuid</code>                         | 池的唯一标识符/对象引用                               | 只读           |
| <code>name-label</code>                   | 池的名称                                       | 读取/写入        |
| <code>name-description</code>             | 池的描述字符串                                    | 读取/写入        |
| <code>master</code>                       | 分配为池主服务器的 Citrix Hypervisor 服务器的唯一标识符/对象引用 | 只读           |
| <code>default-SR</code>                   | 池的默认 SR 的唯一标识符/对象引用                        | 读取/写入        |
| <code>crash-dump-SR</code>                | 保存池成员的任何故障转储的 SR 的唯一标识符/对象引用               | 读取/写入        |
| <code>metadata-vdis</code>                | 池的所有已知元数据 VDI                              | 只读           |
| <code>suspend-image-SR</code>             | 保存池成员上挂起 VM 的 SR 的唯一标识符/对象引用               | 读取/写入        |
| <code>other-config</code>                 | 为池指定额外配置参数的键/值对列表                          | 读取/写入 map 参数 |
| <code>supported-sr-types</code>           | 此池可以使用的 SR 类型                              | 只读           |
| <code>ha-enabled</code>                   | 如果池启用了高可用性功能，则为 true，否则为 false             | 只读           |
| <code>ha-configuration</code>             | 保留以供将来使用。                                  | 只读           |
| <code>ha-statefiles</code>                | 列出高可用性功能使用的 VDI 的 UUID 以确定存储运行状况           | 只读           |
| <code>ha-host-failures-to-tolerate</code> | 允许的主机故障数，超过此数量即发送系统警报                      | 读取/写入        |
| <code>ha-plan-exists-for</code>           | 根据高可用性功能算法的计算，可实际处理的主机故障数                  | 只读           |
| <code>ha-allow-overcommit</code>          | 如果允许过度使用池，则为 True，否则为 False                | 读取/写入        |

| 参数名称                                | 说明                                          | 类型    |
|-------------------------------------|---------------------------------------------|-------|
| <code>ha-overcommitted</code>       | 如果池被过度使用, 则为 True                           | 只读    |
| <code>blobs</code>                  | 二进制数据存储                                     | 只读    |
| <code>live-patching-disabled</code> | 设置为 False 可启用实时修补。设置为 True 可禁用实时修补。         | 读取/写入 |
| <code>igmp-snooping-enabled</code>  | 设置为 True 可启用 IGMP 监听。设置为 False 可禁用 IGMP 监听。 | 读取/写入 |

### **pool-apply-edition**

```
1 pool-apply-edition edition=edition [uuid=uuid] [license-server-address=address] [license-server-port=port]
```

在池中应用某个版本。

### **pool-certificate-install**

```
1 pool-certificate-install filename=file_name
```

在池级别安装 SSL 证书。

### **pool-certificate-list**

```
1 pool-certificate-list
```

列出所有已安装的 SSL 证书。

### **pool-certificate-sync**

```
1 pool-certificate-sync
```

将 SSL 证书和证书吊销列表从主服务器同步到从属服务器。

### **pool-certificate-uninstall**

```
1 pool-certificate-uninstall name=name
```

卸载 SSL 证书。

### **pool-crl-install**

```
1 pool-crl-install filename=file_name
```

在池级别安装 SSL 证书吊销列表。

### **pool-crl-list**

```
1 pool-crl-list
```

列出所有已安装的 SSL 证书吊销列表。

### **pool-crl-uninstall**

```
1 pool-crl-uninstall name=name
```

卸载 SSL 证书吊销列表。

### **pool-deconfigure-wlb**

```
1 pool-deconfigure-wlb
```

永久删除 Workload Balancing 的配置。

### **pool-designate-new-master**

```
1 pool-designate-new-master host-uuid=uuid_of_new_master
```

指示指定的成员 Citrix Hypervisor 服务器成为现有池的主服务器。此命令会将主服务器主机的角色有序移交给资源池中的其他主机。在当前主服务器处于联机状态时，此命令才有效。它不会替代下列紧急模式命令。

### **pool-disable-external-auth**

```
1 pool-disable-external-auth [uuid=uuid] [config=config]
```

禁止在池中的所有主机中进行外部身份验证。

### **pool-disable-local-storage-caching**

```
1 pool-disable-local-storage-caching uuid=uuid
```

禁用池中的本地存储缓存。

### **pool-disable-redo-log**

```
1 pool-disable-redo-log
```

如果正在使用恢复日志，则禁用该日志，除非启用了高可用性功能。

### **pool-disable-ssl-legacy**

```
1 pool-disable-ssl-legacy [uuid=uuid]
```

在每个主机上将 ssl-legacy 设置为 False。

### **pool-dump-database**

```
1 pool-dump-database file-name=filename_to_dump_database_into_(on_client)
```

下载整个池数据库的副本并将其转储到客户端上的文件。

### **pool-enable-external-auth**

```
1 pool-enable-external-auth auth-type=auth_type service-name=  
  service_name [uuid=uuid] [config:=config]
```

允许在池中的所有主机中进行外部身份验证。请注意，auth-type 的某些值需要特定的 config: 值。

### **pool-enable-local-storage-caching**

```
1 pool-enable-local-storage-caching uuid=uuid
```

启用池中的本地存储缓存。

### **pool-enable-redo-log**

```
1 pool-ensable-redo-log sr-uuid=sr_uuid
```

如果正在使用恢复日志，则在给定 SR 上启用该日志，除非启用了高可用性功能。

### **pool-enable-ssl-legacy**

```
1 pool-enable-ssl-legacy [uuid=uuid]
```

在每个主机上将 ssl-legacy 设置为 True。

### **pool-eject**

```
1 pool-eject host-uuid=uuid_of_host_to_eject
```

指示指定的 Citrix Hypervisor 服务器退出现有池。

### **pool-emergency-reset-master**

```
1 pool-emergency-reset-master master-address=address_of_pool_master
```

指示从属成员 Citrix Hypervisor 服务器将其主服务器地址重置为新值，并尝试与其建立连接。请勿在主服务器主机上运行此命令。

### **pool-emergency-transition-to-master**

```
1 pool-emergency-transition-to-master
```

指示成员 Citrix Hypervisor 服务器成为池主服务器。Citrix Hypervisor 服务器仅在已切换到紧急模式后才接受此命令。紧急模式是指该主机所属池的主服务器从网络中消失，经过多次重新尝试后仍无法连接。

如果由于主机加入了池而修改主机密码，此命令可能会导致重置主机密码。有关详细信息，请参阅用户命令。

### **pool-ha-enable**

```
1 pool-ha-enable heartbeat-sr-uuids=uuid_of_heartbeat_sr
```

对资源池启用高可用性功能，同时使用指定的 SR UUID 作为中央检测信号存储库。

### **pool-ha-disable**

```
1 pool-ha-disable
```

禁用对资源池的高可用性功能。

### **pool-ha-compute-hypothetical-max-host-failures-to-tolerate**

计算在当前池配置下允许的最大主机故障数。

### **pool-ha-compute-max-host-failures-to-tolerate**

```
1 pool-ha-compute-hypothetical-max-host-failures-to-tolerate [vm-uuid=  
vm_uuid] [restart-priority=restart_priority]
```

计算在提供的建议受保护 VM 数量下允许的最大主机故障数。

### **pool-initialize-wlb**

```
1 pool-initialize-wlb wlb_url=url wlb_username=wlb_username wlb_password=  
wlb_password xenserver_username=username xenserver_password=password
```

为具有目标 WLB 服务器的当前池初始化 Workload Balancing。

### **pool-join**

```
1 pool-join master-address=address master-username=username master-  
password=password
```

指示 Citrix Hypervisor 服务器加入现有池。

## pool-management-reconfigure

```
1 pool-management-reconfigure [network-uuid=network-uuid]
```

将池中的所有主机的管理接口重新配置为使用指定的网络接口，即用于连接到 XenCenter 的接口。此命令将为池中的所有主机重写 `/etc/xensource-inventory` 中的 `MANAGEMENT_INTERFACE` 键。

如果指定了接口（必须具有 IP 地址）的设备名称，则 Citrix Hypervisor 主机将立即重新绑定。此命令适用于正常模式和紧急模式。

根据指定的网络 UUID，可以标识 PIF 对象的 UUID 并将其映射到用于确定重新绑定到自身的 IP 地址的 Citrix Hypervisor 服务器。执行此命令时一定不能处于紧急模式。

### 警告：

在除主机外的计算机上使用此 CLI 命令时需谨慎，并确保在新接口上有网络连接。请先使用 `xe pif-reconfigure` 建立一个连接。否则，后续 CLI 命令将无法到达 Citrix Hypervisor 服务器。

## pool-recover-slaves

```
1 pool-recover-slaves
```

指示池主服务器尝试重置当前以紧急模式运行的所有成员的主服务器地址。通常在使用 `pool-emergency-transition-to-master` 将其中的一个成员设置为新主服务器后使用此命令。

## pool-restore-database

```
1 pool-restore-database file-name=filename_to_restore_from_on_client [dry-run=true | false]
```

将数据库备份（使用 `pool-dump-database` 创建）上载到池中。接收上载的内容后，主服务器将自行重新启动并使用新数据库。

该命令中还包含一个 `dry run` 选项，借助此选项，您可以确定是否可在无需实际执行操作的情况下还原池数据库。默认情况下，`dry-run` 设置为 `false`。

## pool-retrieve-wlb-configuration

```
1 pool-retrieve-wlb-configuration
```

从 Workload Balancing 服务器中检索池优化条件。

### **pool-retrieve-wlb-diagnostics**

```
1 pool-retrieve-wlb-diagnostics [filename=file_name]
```

从 Workload Balancing 服务器中检索诊断信息。

### **pool-retrieve-wlb-recommendations**

```
1 pool-retrieve-wlb-recommendations
```

从 Workload Balancing 服务器为池检索 VM 迁移建议。

### **pool-retrieve-wlb-report**

```
1 pool-retrieve-wlb-report report=report [filename=file_name]
```

从 Workload Balancing 服务器检索报告。

### **pool-send-test-post**

```
1 pool-send-test-post dest-host=destination_host dest-port=
  destination_port body=post_body
```

使用 HTTPS 将给定正文发送到指定主机和端口，并显示响应。此命令用于调试 SSL 层。

### **pool-send-wlb-configuration**

```
1 pool-send-wlb-configuration [config:=config]
```

为 Workload Balancing 服务器设置池优化条件。

### **pool-sync-database**

```
1 pool-sync-database
```

强制池数据库在资源池中的所有主机上进行同步。在正常操作时不需要使用此命令，因为系统会自动定期复制数据库。但是，在执行一系列重要的 CLI 操作后，该命令对于确保快速复制变更可能有用。

### 设置池 **igmp-snooping**

```
1 pool-param-set [uuid=pool-uuid] [igmp-snooping-enabled=true | false]
```

在 Citrix Hypervisor 池中启用或禁用 IGMP 监听。

### **PVS** 加速器命令

用于使用 PVS 加速器的命令。

### **pvs-cache-storage-create**

```
1 pvs-cache-storage-create sr-uuid=sr_uuid pvs-site-uuid=pvs_site_uuid  
size=size
```

在指定主机的指定 SR 上配置 PVS 缓存。

### **pvs-cache-storage-destroy**

```
1 pvs-cache-storage-destroy uuid=uuid
```

删除 PVS 缓存。

### **pvs-proxy-create**

```
1 pvs-proxy-create pvs-site-uuid=pvs_site_uuid vif-uuid=vif_uuid
```

将 VM/VIF 配置为使用 PVS 代理。

### **pvs-proxy-destroy**

```
1 pvs-proxy-destroy uuid=uuid
```

删除（或关闭）此 VIF/VM 的 PVS 代理。

### **pvs-server-forget**

```
1 pvs-server-forget uuid=uuid
```

忽略 PVS 服务器。

### **pvs-server-introduce**

```
1 pvs-server-introduce addresses=addresses first-port=first_port last-port
  =last_port pvs-site-uuid=pvs_site_uuid
```

引入新的 PVS 服务器。

### **pvs-site-forget**

```
1 pvs-site-forget uuid=uuid
```

忽略 PVS 站点。

### **pvs-site-introduce**

```
1 pvs-site-introduce name-label=name_label [name-description=
  name_description] [pvs-uuid=pvs_uuid]
```

引入新的 PVS 站点。

### 存储管理器命令

用于控制存储管理器插件的命令。

可以使用标准对象列出命令 (`xe sm-list`) 列出存储管理器对象。可以使用标准参数命令操纵参数。有关详细信息，请参阅低级参数命令。

### **SM 参数**

SM 包含下列参数：

| 参数名称                              | 说明                                    | 类型 |
|-----------------------------------|---------------------------------------|----|
| <code>uuid</code>                 | SM 插件的唯一标识符/对象引用                      | 只读 |
| <code>name-label</code>           | SM 插件的名称                              | 只读 |
| <code>name-description</code>     | SM 插件的描述字符串                           | 只读 |
| <code>type</code>                 | 此插件连接到的 SR 类型                         | 只读 |
| <code>vendor</code>               | 创建此插件的供应商的名称                          | 只读 |
| <code>copyright</code>            | 此 SM 插件的版权声明                          | 只读 |
| <code>required-api-version</code> | Citrix Hypervisor 服务器上要求的最低 SM API 版本 | 只读 |
| <code>configuration</code>        | 设备配置键的名称和说明                           | 只读 |
| <code>capabilities</code>         | SM 插件的功能                              | 只读 |
| <code>driver-filename</code>      | SR 驱动程序的文件名。                          | 只读 |

## 快照命令

用于使用快照的命令。

### snapshot-clone

```
1 snapshot-clone new-name-label=name_label [uuid=uuid] [new-name-
  description=description]
```

如果可用，请通过使用存储级别的快速磁盘克隆操作克隆现有快照，来创建新模板。

### snapshot-copy

```
1 snapshot-copy new-name-label=name_label [uuid=uuid] [new-name-
  description=name_description] [sr-uuid=sr_uuid]
```

通过复制现有 VM，但不使用存储级别的快速磁盘克隆操作（即使该操作可用），来创建新模板。保证 VM 副本的磁盘映像为“完整映像”，即该磁盘映像不是 CoW 链的一部分。

### snapshot-destroy

```
1 snapshot-destroy [uuid=uuid] [snapshot-uuid=snapshot_uuid]
```

销毁快照。这会使与快照关联的存储保留不变。要同时删除存储，请使用 `snapshot-uninstall`。

### **snapshot-disk-list**

```
1 snapshot-disk-list [uuid=uuid] [snapshot-uuid=snapshot_uuid] [vbd-params=vbd_params] [vdi-params=vdi_params]
```

列出所选 VM 上的磁盘。

### **snapshot-export-to-template**

```
1 snapshot-export-to-template filename=file_name snapshot-uuid=snapshot_uuid [preserve-power-state=true|false]
```

将快照导出到 文件名。

### **snapshot-reset-powerstate**

```
1 snapshot-reset-powerstate [uuid=uuid] [snapshot-uuid=snapshot_uuid] [--force]
```

强制 VM 电源状态仅在管理 Toolstack 数据库中变为已停止。此命令用于恢复标记为“已挂起”的快照。此操作存在潜在危险：您必须确保不再需要内存映像（即，您将无法再恢复快照）。

### **snapshot-revert**

```
1 snapshot-revert [uuid=uuid] [snapshot-uuid=snapshot_uuid]
```

将现有 VM 还原到之前的检查点或快照状态。

### **snapshot-uninstall**

```
1 snapshot-uninstall [uuid=uuid] [snapshot-uuid=snapshot_uuid] [--force]
```

卸载快照。此操作将销毁编辑为 RW 且仅连接到此快照的 VDI。要仅销毁 VM 记录，请使用 `snapshot-destroy`。

## SR 命令

用于控制 SR（存储库）的命令。

可以使用标准对象列出命令 (`xe sr-list`) 列出 SR 对象，并使用标准参数命令操纵参数。有关详细信息，请参阅低级参数命令。

## SR 参数

SR 包含下列参数：

| 参数名称                              | 说明                                                                                                                                             | 类型        |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <code>uuid</code>                 | SR 的唯一标识符/对象引用                                                                                                                                 | 只读        |
| <code>name-label</code>           | SR 的名称                                                                                                                                         | 读取/写入     |
| <code>name-description</code>     | SR 的描述字符串                                                                                                                                      | 读取/写入     |
| <code>allowed-operations</code>   | 在此状态下的 SR 上允许执行的操作的列表                                                                                                                          | 只读 set 参数 |
| <code>current-operations</code>   | 当前此 SR 上正在进行的操作的列表                                                                                                                             | 只读 set 参数 |
| <code>VDIs</code>                 | 此 SR 中虚拟磁盘的唯一标识符/对象引用                                                                                                                          | 只读 set 参数 |
| <code>PBDs</code>                 | 连接到此 SR 的 PBD 的唯一标识符/对象引用                                                                                                                      | 只读 set 参数 |
| <code>physical-utilisation</code> | 此 SR 上当前使用的物理空间（以字节为单位）。对于精简预配的磁盘格式，物理利用率可能低于虚拟分配                                                                                              | 只读        |
| <code>physical-size</code>        | SR 的总物理空间大小（以字节为单位）                                                                                                                            | 只读        |
| <code>type</code>                 | SR 的类型，用于指定要使用的 SR 后端驱动程序                                                                                                                      | 只读        |
| <code>introduced-by</code>        | 引入 SR 的 drtask（如果有）                                                                                                                            | 只读        |
| <code>content-type</code>         | SR 内容的类型。用于将 ISO 库与其他 SR 区分开来。对于用于存储 ISO 库的存储库，必须将 <code>content-type</code> 设置为 <code>iso</code> 。对于其他情况，我们建议将此参数设置为空或字符串 <code>user</code> 。 | 只读        |

| 参数名称                            | 说明                                                        | 类型           |
|---------------------------------|-----------------------------------------------------------|--------------|
| <code>shared</code>             | 如果可以在多个 Citrix Hypervisor 服务器之间共享此 SR, 则为 True; 否则为 False | 读取/写入        |
| <code>other-config</code>       | 为 SR 指定额外配置参数的键/值对列表                                      | 读取/写入 map 参数 |
| <code>host</code>               | 存储库主机名称                                                   | 只读           |
| <code>virtual-allocation</code> | 此存储库中的所有 VDI 的总虚拟大小值 (以字节为单位)                             | 只读           |
| <code>sm-config</code>          | SM 依赖数据                                                   | 只读 map 参数    |
| <code>blobs</code>              | 二进制数据存储                                                   | 只读           |

## sr-create

```
1 sr-create name=label=name physical-size=size type=type content-type=
  content_type device-config:config_name=value [host-uuid=host_uuid] [
  shared=true | false]
```

在磁盘上创建一个 SR, 将其引入到数据库中, 然后创建一个将该 SR 连接到 Citrix Hypervisor 服务器的 PBD。如果 `shared` 设置为 `true`, 则为池中的每个 Citrix Hypervisor 服务器创建一个 PBD。如果未指定 `shared` 或将其设置为 `false`, 则仅为使用 `host-uuid` 指定的 Citrix Hypervisor 服务器创建一个 PBD。

具体的 `device-config` 参数因设备 `type` 的不同而异。有关不同存储后端上这些参数的详细信息, 请参阅[存储](#)。

## sr-data-source-forget

```
1 sr-data-source-forget data-source=data_source
```

停止为 SR 记录指定数据源并忽略所有已记录的数据。

## sr-data-source-list

```
1 sr-data-source-list"
```

列出可为 SR 记录的数据源。

### **sr-data-source-query**

```
1 sr-data-source-query data-source=data_source
```

查询从 SR 数据源读取的最后一个值。

### **sr-data-source-record**

```
1 sr-data-source-record data-source=data_source
```

记录 SR 的指定数据源。

### **sr-destroy**

```
1 sr-destroy uuid=sr_uuid
```

销毁 Citrix Hypervisor 服务器上指定的 SR。

### **sr-enable-database-replication**

```
1 sr-enable-database-replication uuid=sr_uuid
```

允许将 XAPI 数据库复制到指定（共享）SR。

### **sr-disable-database-replication**

```
1 sr-disable-database-replication uuid=sr_uuid
```

禁止将 XAPI 数据库复制到指定 SR。

### **sr-forget**

```
1 sr-forget uuid=sr_uuid
```

XAPI 代理将忽略 Citrix Hypervisor 服务器上的指定 SR。XAPI 代理忽略了某个 SR，该 SR 被分离，您无法访问其上的 VDI，但该 SR 在源介质中保持原样（数据未丢失）。

## sr-introduce

```
1 sr-introduce name=label=name physical-size=physical_size type=type  
content-type=content_type uuid=sr_uuid
```

即将 SR 记录添加到数据库中。使用 `device-config` 以 `device-config:parameter_key=parameter_value` 形式指定其他参数，例如：

```
1 xe sr-introduce device-config:device=/dev/sdb1
```

### 注意：

此命令不用于正常操作中。此高级操作对于在创建 SR 后必须将 SR 重新配置为共享这种情况可能很有用，或者有助于在出现各种故障情形后恢复 SR。

## sr-probe

```
1 sr-probe type=type [host-uuid=host_uuid] [device-config:config_name=  
value]
```

使用提供的 `device-config` 键执行特定于后端的扫描。如果已为 SR 后端完成 `device-config`，则此命令将返回设备上的 SR 的列表（如果有）。如果仅完成部分 `device-config` 参数，则将执行特定于后端的扫描，返回结果将有助于您改进其余 `device-config` 参数。扫描结果以特定于后端的 XML 形式返回，显示在 CLI 上。

具体的 `device-config` 参数因设备 `type` 的不同而异。有关不同存储后端上这些参数的详细信息，请参阅[存储](#)。

## sr-probe-ext

```
1 sr-probe-ext type=type [host-uuid=host_uuid] [device-config:=config] [  
sm-config:-sm_config]
```

执行存储探测。可以通过 `device-config:devs=/dev/sdb1` 等指定 `device-config` 参数。与 `sr-probe` 不同，此命令将返回格式与每个 SR 类型一样可读的结果。

## sr-scan

```
1 sr-scan uuid=sr_uuid
```

强制执行 SR 扫描，同时将 XAPI 数据库与基础存储基底中的 VDI 同步。

## **sr-update**

```
1 sr-update uuid=uuid
```

刷新数据库中 SR 对象的字段。

## **lvhd-enable-thin-provisioning**

```
1 lvhd-enable-thin-provisioning sr-uuid=sr_uuid initial-allocation=  
initial_allocation allocation-quantum=allocation_quantum
```

对 LVHD SR 启用精简预配。

## **使用者命令**

用于使用使用者的命令。

## **session-subject-identifier-list**

```
1 session-subject-identifier-list
```

返回所有已通过外部身份验证的现有会话的所有用户使用者 ID 列表。

## **session-subject-identifier-logout**

```
1 session-subject-identifier-logout subject-identifier=subject_identifier
```

注销与用户使用者 ID 关联的所有已通过外部身份验证的会话。

## **session-subject-identifier-logout-all**

```
1 session-subject-identifier-logout-all
```

注销所有已通过外部身份验证的会话。

### **subject-add**

```
1 subject-add subject-name=subject_name
```

将使用者添加到可以访问池的使用者列表中。

### **subject-remove**

```
1 subject-remove subject-uuid=subject_uuid
```

从可以访问池的使用者列表中删除某个使用者。

### **subject-role-add**

```
1 subject-role-add uuid=uuid [role-name=role_name] [role-uuid=role_uuid]
```

向使用者添加角色。

### **subject-role-remove**

```
1 subject-role-remove uuid=uuid [role-name=role_name] [role-uuid=
  role_uuid]
```

删除使用者的角色。

### **secret-create**

```
1 secret-create value=value
```

创建密钥。

### **secret-destroy**

```
1 secret-destroy uuid=uuid
```

销毁密钥。

## 任务命令

用于长时间运行的异步任务的命令。这些命令是启动、停止和挂起虚拟机等任务。这些任务通常由一组共同完成请求的操作的其他原子任务组成。

可以使用标准对象列出命令 (`xe task-list`) 列出任务对象，并使用标准参数命令操纵参数。有关详细信息，请参阅低级参数命令。

## 任务参数

任务包含下列参数：

| 参数名称                            | 说明                                                          | 类型 |
|---------------------------------|-------------------------------------------------------------|----|
| <code>uuid</code>               | 任务的唯一标识符/对象引用                                               | 只读 |
| <code>name-label</code>         | 任务的名称                                                       | 只读 |
| <code>name-description</code>   | 任务的描述字符串                                                    | 只读 |
| <code>resident-on</code>        | 运行任务的主机的唯一标识符/对象引用                                          | 只读 |
| <code>status</code>             | 任务的状态                                                       | 只读 |
| <code>progress</code>           | 如果任务尚未完成，则此字段包含估算的已完成百分比（介于 0 到 1 之间）。如果任务已完成，无论成功与否，值均为 1。 | 只读 |
| <code>type</code>               | 如果任务已成功完成，此参数将包含编码结果的类型。类型是其参考位于结果字段中的类别的名称。否则，此参数的值处于未定义状态 | 只读 |
| <code>result</code>             | 如果任务已成功完成，此字段将包含结果值（为空或对象引用）；否则，此参数的值处于未定义状态                | 只读 |
| <code>error_info</code>         | 如果任务已失败，则此参数包含一组相关的错误字符串。否则，此参数的值处于未定义状态                    | 只读 |
| <code>allowed_operations</code> | 此状态下允许执行的操作的列表                                              | 只读 |
| <code>created</code>            | 创建任务的时间                                                     | 只读 |

| 参数名称                    | 说明                                          | 类型 |
|-------------------------|---------------------------------------------|----|
| <code>finished</code>   | 任务完成时间（即，成功或失败）。<br>如果任务状态是未完成，则此字段的值没有任何意义 | 只读 |
| <code>subtask_of</code> | 包含以此任务为子任务的任务的 UUID                         | 只读 |
| <code>subtasks</code>   | 包含此任务的所有子任务的 UUID                           | 只读 |

## task-cancel

```
1 task-cancel [uuid=task_uuid]
```

指示取消指定的任务并返回。

### 模板命令

用于 VM 模板的命令。

模板实质上是 `is-a-template` 参数设置为 `true` 的 VM。模板是包含所有各种设置以实例化特定 VM 的“黄金映像”。Citrix Hypervisor 随附了一组基础模板，它们是通用的“原始”VM，能够引导操作系统厂商提供的安装 CD（例如，RHEL、CentOS、SLES、Windows）。您可以创建 VM，按照您的特定需要以标准形式配置它们，将它们的副本保存为模板供将来在 VM 部署中使用。

可以使用标准对象列出命令 (`xe template-list`) 列出模板对象，并使用标准参数命令操纵参数。有关详细信息，请参阅低级参数命令。

#### 注意：

不能通过将 `is-a-template` 参数设置为 `false` 来将模板直接转换为 VM。不支持将 `is-a-template` 参数设置为 `false`，这样会导致 VM 无法启动。

### VM 模板参数

模板包含下列参数：

- `uuid`（只读）模板的唯一标识符/对象引用
- `name-label`（读取/写入）模板的名称
- `name-description`（读取/写入）模板的描述字符串
- `user-version`（读取/写入）用于输入版本信息的 VM 和模板创建者的字符串

- `is-a-template` (读取/写入) 如果此 VM 为模板, 则为 `true`。  
模板 VM 无法启动, 它们仅用于克隆其他 VM。将此值设置为 `true` 后, 将无法再重置为 `false`。不能使用此参数将模板 VM 转换为 VM。
- `is-control-domain` (只读) 如果是控制域 (域 0 或驱动程序域), 则为 `true`
- `power-state` (只读) 当前电源状态。对于模板, 此值始终为已停止
- `memory-dynamic-max` (只读) 最大动态内存 (以字节为单位)。  
当前未使用, 但如果更改则必须遵守以下限制: `memory_static_max >= memory_dynamic_max >= memory_dynamic_min >= memory_static_min`。
- `memory-dynamic-min` (读取/写入) 最小动态内存 (以字节为单位)。  
当前未使用, 但如果更改, 则必须遵守与针对 `memory-dynamic-max` 的限制相同的限制。
- `memory-static-max` (读取/写入) 静态设置 (绝对) 最大内存 (以字节为单位)。此字段是用于确定分配给 VM 的内存量的主要值。
- `memory-static-min` (读取/写入) 静态设置 (绝对) 最小内存 (以字节为单位)。  
此字段代表绝对最小内存, 并且 `memory-static-min` 必须小于 `memory-static-max`。  
此值当前未用于正常操作, 但是必须遵守前面提到的限制。
- `suspend-VDI-uuid` (只读) 存储挂起映像的 VDI (对于模板没有意义)
- `VCPUs-params` (读取/写入 map 参数) 所选 vCPU 策略的配置参数。

可以使用以下命令调整 vCPU 固定:

```
1 xe template-param-set uuid=<template_uuid> vCPUs-params:mask=1,2,3
```

从此模板创建的 VM 稍后将仅在物理 CPU 1、CPU 2 和 CPU 3 上运行。

还可以使用 `cap` 和 `weight` 参数调整 vCPU 优先级 (xen 调度)。例如:

```
1 xe template-param-set uuid=<template_uuid> VCPUs-params:weight=512
xe template-param-set uuid=<template_uuid> VCPUs-params:cap=100
```

基于此模板且权重为 512 的 VM 所获得的 CPU 将是竞争主机上权重为 256 的域的两倍。合法的权重范围为 1 到 65535, 默认值为 256。

上限可选地规定基于此模板的 VM 可以占用的最大 CPU 量, 即使 Citrix Hypervisor 服务器具有空闲 CPU 周期也应用此上限。此上限以一个物理 CPU 的百分比表示: 100 是 1 个物理 CPU, 50 是半个物理 CPU, 400 是 4 个物理 CPU, 依此类推。默认值为 0, 表示无上限。

- `VCPUs-max` (读取/写入) 最大 vCPU 数量
- `VCPUs-at-startup` (读取/写入) vCPU 的引导编号

- `actions-after-crash` (读取/写入) 当基于此模板的 VM 崩溃时要采取的操作
- `console-uuids` (只读 `set` 参数) 虚拟控制台设备
- `platform` (读取/写入 `map` 参数) 特定于平台的配置

禁用 HVM 来宾系统 (例如, Windows 来宾系统) 的并行端口模拟:

```
1 xe vm-param-set uuid=<vm_uuid> platform:parallel=none
```

禁用 HVM 来宾系统的串行端口模拟:

```
1 xe vm-param-set uuid=<vm_uuid> platform:hvm_serial=none
```

禁用 HVM 来宾系统的 USB 控制器和 USB 平板电脑设备模拟:

```
1 xe vm-param-set uuid=<vm_uuid> platform:usb=false
2 xe vm-param-set uuid=<vm_uuid> platform:usb_tablet=false
```

- `allowed-operations` (只读 `set` 参数) 在此状态下允许执行的操作的列表
- `current-operations` (只读 `set` 参数) 当前正在对此模板执行的操作的列表
- `allowed-VBD-devices` (只读 `set` 参数) 可供使用的 VBD 标识符的列表, 用 0 到 15 之间的整数表示。此列表仅供参考, 可以使用未在此列表中列出的其他设备 (但可能无法正常运行)。
- `allowed-VIF-devices` (只读 `set` 参数) 可供使用的 VIF 标识符的列表, 用 0 到 15 之间的整数表示。此列表仅供参考, 可以使用未在此列表中列出的其他设备 (但可能无法正常运行)。
- `HVM-boot-policy` (读取/写入) HVM 来宾系统的引导策略。BIOS 顺序或空字符串。
- `HVM-boot-params` (读取/写入 `map` 参数) `order` 键控制 HVM 来宾系统引导顺序, 以字符串表示, 其中每个字符代表一种引导方法: `d` 代表 CD/DVD, `c` 代表根磁盘, `n` 代表网络 PXE 引导。默认值为 `dc`。
- `PV-kernel` (读取/写入) 内核路径
- `PV-ramdisk` (读取/写入) `initrd` 路径
- `PV-args` (读取/写入) 内核命令行参数字符串
- `PV-legacy-args` (读取/写入) 使旧 VM 基于此模板引导的参数字符串
- `PV-bootloader` (读取/写入) 引导加载程序的名称或路径
- `PV-bootloader-args` (读取/写入) 引导加载程序的其他参数的字符串
- `last-boot-CPU-flags` (只读) 描述上次引导基于此模板的 VM 时所在的 CPU 的标志; 不为模板填充此参数
- `resident-on` (只读) 基于此模板的 VM 所在的 Citrix Hypervisor 服务器。对于模板, 将显示为 `not in database`

- `affinity` (读取/写入) 基于此模板的 VM 在其上具有优先运行权的 Citrix Hypervisor 服务器。由 `xe vm-start` 命令用于确定在何处运行 VM
- `other-config` (读取/写入 `map` 参数) 为模板指定额外配置参数的键/值对列表
- `start-time` (只读) 读取基于此模板的 VM 指标的日期和时间的时戳, 以 `yyyymmddThh:mm:ss z` 的形式表示, 其中 `z` 是单字母军用时区指示器, 例如, `Z` 表示 UTC (GMT)。对于模板, 设置为 `1 Jan 1970 Z` (Unix/POSIX 新纪元的起始日期)
- `install-time` (只读) 读取基于此模板的 VM 指标的日期和时间的时戳, 以 `yyyymmddThh:mm:ss z` 的形式表示, 其中 `z` 是单字母军用时区指示器, 例如, `Z` 表示 UTC (GMT)。对于模板, 设置为 `1 Jan 1970 Z` (Unix/POSIX 新纪元的起始日期)
- `memory-actual` (只读) 基于此模板的 VM 正在使用的实际内存; 对于模板, 该值为 0
- `VCPUs-number` (只读) 分配给基于此模板的 VM 的虚拟 CPU 数目; 对于模板, 该值为 0
- `VCPUs-Utilization` (只读 `map` 参数) 虚拟 CPU 及其权重只读 `map` 参数 `os-version` (基于此模板的 VM 的操作系统版本) 的列表。对于模板, 将显示为 `not in database`
- `PV-drivers-version` (只读 `map` 参数) 基于此模板的 VM 的半虚拟化驱动程序版本。对于模板, 将显示为 `not in database`
- `PV-drivers-detected` (只读) 基于此模板的 VM 的半虚拟化驱动程序的最新版本的标志。对于模板, 将显示为 `not in database`
- `memory` (只读 `map` 参数) 由基于此模板的 VM 上的代理报告的内存指标。对于模板, 将显示为 `not in database`
- `disks` (只读 `map` 参数) 由基于此模板的 VM 上的代理报告的磁盘指标。对于模板, 将显示为 `not in database`
- `networks` (只读 `map` 参数) 由基于此模板的 VM 上的代理报告的网络指标。对于模板, 将显示为 `not in database`
- `other` (只读 `map` 参数) 由基于此模板的 VM 上的代理报告的其他指标。对于模板, 将显示为 `not in database`
- `guest-metrics-last-updated` (只读) 来宾代理对这些字段执行最后一次写入操作时的时戳。以 `yyyymmddThh:mm:ss z` 的形式表示, 其中 `z` 是单字母军用时区指示器, 例如, `Z` 代表 UTC (GMT)
- `actions-after-shutdown` (读取/写入) 将在 VM 关闭后执行的操作
- `actions-after-reboot` (读取/写入) 将在 VM 重新启动后执行的操作
- `possible-hosts` (只读) 可以托管 VM 的潜在主机列表
- `HVM-shadow-multiplier` (读取/写入) 应用于被设置为可供来宾系统使用的重影量的系数
- `dom-id` (只读) 域 ID (如果可用, 否则为 -1)
- `recommendations` (只读) 此 VM 的建议值和属性范围的 XML 规范

- `xenstore-data` (读取/写入 `map` 参数) 在创建 VM 后将插入到 `xenstore` 树 (`/local/domain/domid/vmdata`) 的数据。
- `is-a-snapshot` (只读) 如果此模板为 VM 快照, 则为 `true`
- `snapshot_of` (只读) 以此模板为快照的 VM 的 UUID
- `snapshots` (只读) 根据此模板生成的任何快照的 UUID
- `snapshot_time` (只读) 最近生成的 VM 快照的时间戳
- `memory-target` (只读) 为此模板设置的目标内存量
- `blocked-operations` (读取/写入 `map` 参数) 列出无法对此模板执行的操作
- `last-boot-record` (只读) 此模板的上次引导参数的记录, 使用 XML 格式
- `ha-always-run` (读取/写入) 如果此模板的实例在其所在的主机发生故障后始终在其他主机上重新启动, 则为 `True`。此参数现已弃用。请改为使用 `ha-restartpriority` 参数。
- `ha-restart-priority` (只读) 重新启动或最大努力读取/写入 `blob` 二进制数据存储
- `live` (只读) 仅与正在运行的 VM 相关。

## template-export

```
1 template-export template-uuid=uuid_of_existing_template filename=  
   filename_for_new_template
```

将指定模板的副本导出到文件, 使用指定的新文件名。

## template-uninstall

```
1 template-uninstall template-uuid=template_uuid [--force]
```

卸载自定义模板。此操作将销毁这些标记为由此模板“所有”的 VDI。

### 更新命令

下一节包含 Citrix Hypervisor 服务器更新命令。

可以使用标准对象列出命令 (`xe update-list`) 列出更新对象, 并使用标准参数命令操纵参数。有关详细信息, 请参阅低级参数命令。

## 更新参数

Citrix Hypervisor 服务器更新具有以下参数：

| 参数名称                              | 说明                               | 类型 |
|-----------------------------------|----------------------------------|----|
| <code>uuid</code>                 | 更新的唯一标识符/对象引用                    | 只读 |
| <code>host</code>                 | 此更新应用到的主机列表                      | 只读 |
| <code>host-uuid</code>            | 要查询的 Citrix Hypervisor 服务器的唯一标识符 | 只读 |
| <code>name-label</code>           | 更新的名称                            | 只读 |
| <code>name-description</code>     | 更新的描述字符串                         | 只读 |
| <code>applied</code>              | 是否已应用更新; true 或 false            | 只读 |
| <code>installation-size</code>    | 更新的大小 (以字节为单位)                   | 只读 |
| <code>after-apply-guidance</code> | XAPI Toolstack 或主机是否需要重新启动       | 只读 |
| <code>version</code>              | 更新的版本                            | 只读 |

### update-upload

```
1 update-upload file-name=update_filename
```

将指定的更新文件上传到 Citrix Hypervisor 服务器。此命令可以为应用更新做好准备。成功时，会显示已上传更新的 UUID。如果先前已上传过此更新，则将返回 `UPDATE_ALREADY_EXISTS` 错误，而不会再次上传该修补程序。

### update-precheck

```
1 update-precheck uuid=update_uuid host-uuid=host_uuid
```

对指定 Citrix Hypervisor 服务器运行包含在指定更新中的预检查。

### update-destroy

```
1 update-destroy uuid=update_file_uuid
```

从池中删除未应用的更新文件。可用于删除不能应用到主机的更新文件。

### update-apply

```
1 update-apply host-uuid=host_uuid uuid=update_file_uuid
```

应用指定的更新文件。

### **update-pool-apply**

```
1 update-pool-apply uuid=update_uuid
```

将指定更新应用到池中的所有 Citrix Hypervisor 服务器。

### **update-introduce**

```
1 update-introduce vdi-uuid=vdi_uuid
```

引入更新 VDI。

### **update-pool-clean**

```
1 update-pool-clean uuid=uuid
```

从池中的所有主机删除更新文件。

用户命令

### **user-password-change**

```
1 user-password-change old=old_password new=new_password
```

更改用户登录密码。未选中旧密码字段，因为使用此命令需要主管特权。

### **VBD 命令**

用于 VBD（虚拟块设备）的命令。

VBD 是一个软件对象，用于将 VM 连接到 VDI（代表虚拟磁盘的内容）。VBD 具有将 VDI 绑定到 VM 的属性（是否可引导、其读取/写入指标等）。VDI 包含与虚拟磁盘的物理属性有关的信息（SR 类型、磁盘是否可共享、介质是可读写介质还是只读介质等）。

可以使用标准对象列出命令 (`xe vbd-list`) 列出 VBD 对象，并使用标准参数命令操纵参数。有关详细信息，请参阅低级参数命令。

**VBD 参数**

VBD 包含下列参数：

| 参数名称                                  | 说明                                                                                                        | 类型                        |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------|---------------------------|
| <code>uuid</code>                     | VBD 的唯一标识符/对象引用                                                                                           | 只读                        |
| <code>vm-uuid</code>                  | 此 VBD 连接到的 VM 的唯一标识符/对象引用                                                                                 | 只读                        |
| <code>vm-name-label</code>            | 此 VBD 连接到的 VM 的名称                                                                                         | 只读                        |
| <code>vdi-uuid</code>                 | 此 VBD 映射到的 VDI 的唯一标识符/对象引用                                                                                | 只读                        |
| <code>vdi-name-label</code>           | 此 VBD 映射到的 VDI 的名称                                                                                        | 只读                        |
| <code>empty</code>                    | 如果为 <code>true</code> ，则此 VBD 代表空驱动器                                                                      | 只读                        |
| <code>device</code>                   | 可对来宾系统显示的设备，例如 <code>hda</code>                                                                           | 只读                        |
| <code>userdevice</code>               | <code>vbd-create</code> 期间通过 <code>device</code> 参数指定的设备号，例如，0 表示 <code>hda</code> ，1 表示 <code>hdb</code> | 读取/写入                     |
| <code>bootable</code>                 | 如果此 VBD 可引导，则为 <code>true</code>                                                                          | 读取/写入                     |
| <code>mode</code>                     | 装载 VBD 应使用的模式                                                                                             | 读取/写入                     |
| <code>type</code>                     | VBD 对 VM 的显示方式，例如磁盘或 CD                                                                                   | 读取/写入                     |
| <code>currently-attached</code>       | 如果 VBD 已连接到此主机，则为 <code>True</code> ，否则为 <code>false</code>                                               | 只读                        |
| <code>storage-lock</code>             | 如果获得了存储级别锁定，则为 <code>true</code>                                                                          | 只读                        |
| <code>status-code</code>              | 与上次连接操作相关联的错误/成功代码                                                                                        | 只读                        |
| <code>status-detail</code>            | 与上次连接操作状态相关联的错误/成功信息                                                                                      | 只读                        |
| <code>qos_algorithm_type</code>       | 要使用的 QoS 算法                                                                                               | 读取/写入                     |
| <code>qos_algorithm_params</code>     | 所选 QoS 算法的参数                                                                                              | 读取/写入 <code>map</code> 参数 |
| <code>qos_supported_algorithms</code> | 此 VBD 支持的 QoS 算法                                                                                          | 只读 <code>set</code> 参数    |

| 参数名称                            | 说明                                                                   | 类型           |
|---------------------------------|----------------------------------------------------------------------|--------------|
| <code>io_read_kbs</code>        | 此 VBD 的平均读取速率（以 kbps 为单位）                                            | 只读           |
| <code>io_write_kbs</code>       | 此 VBD 的平均写入速率（以 kbps 为单位）                                            | 只读           |
| <code>allowed-operations</code> | 此状态下允许执行的操作的列表。此列表只是建议性的，并且客户端读取此字段时服务器状态可能已更改。                      | 只读 set 参数    |
| <code>current-operations</code> | 将每个使用此对象（通过引用）的正在运行的任务链接到描述此任务本质的 <code>current_operation</code> 枚举。 | 只读 set 参数    |
| <code>unpluggable</code>        | 如果此 VBD 支持热拔出，则为 True                                                | 读取/写入        |
| <code>attachable</code>         | 如果设备可以连接，则为 True                                                     | 只读           |
| <code>other-config</code>       | 额外的配置                                                                | 读取/写入 map 参数 |

## vbd-create

```
1 vbd-create vm-uuid=uuid_of_the_vm device=device_value vdi-uuid=
   uuid_of_vdi_to_connect_to [bootable=true] [type=Disk|CD] [mode=RW|RO]
]
```

在 VM 上创建 VBD。

`device` 字段允许使用的值为介于 0 到 15 之间的整数，并且每个 VM 的数值必须唯一。可以在指定 VM 上的 `allowed-VBD-devices` 参数中查看当前允许使用的值。在 `vbd` 参数中，此值被视为 `userdevice`。

如果 `type` 为 `Disk`，则 `vdi-uuid` 为必填字段。对于磁盘，模式可以为 `RO` 或 `RW`。

如果 `type` 为 `CD`，则 `vdi-uuid` 是可选字段。如果不指定 VDI，则为 CD 创建空 VBD。对于 CD，模式必须为 `RO`。

## vbd-destroy

```
1 vbd-destroy uuid=uuid_of_vbd
```

销毁指定的 VBD。

如果 VBD 将其 `other-config:owner` 参数设置为 `true`，则其关联的 VDI 也将被销毁。

## vbd-eject

```
1 vbd-eject uuid=uuid_of_vbd
```

从 VBD 代表的驱动器中删除介质。仅当介质是可移动类型（物理 CD 或 ISO）时，此命令才有效。否则，将返回错误消息 `VBD_NOT_REMOVABLE_MEDIA`。

## vbd-insert

```
1 vbd-insert uuid=uuid_of_vbd vdi-uuid=uuid_of_vdi_containing_media
```

将新介质插入到 VBD 代表的驱动器中。仅当介质是可移动类型（物理 CD 或 ISO）时，此命令才有效。否则，将返回错误消息 `VBD_NOT_REMOVABLE_MEDIA`。

## vbd-plug

```
1 vbd-plug uuid=uuid_of_vbd
```

尝试在 VM 处于运行状态时连接 VBD。

## vbd-unplug

```
1 vbd-unplug uuid=uuid_of_vbd
```

尝试在 VM 处于运行状态时将 VBD 从 VM 分离。

## VDI 命令

用于 VDI（虚拟磁盘映像）的命令。

VDI 是一个软件对象，代表对 VM 可见的虚拟磁盘的内容。与 VBD 不同，此对象是将 VM 绑定到 VDI 的对象。VDI 包含与虚拟磁盘的物理属性有关的信息（SR 类型、磁盘是否可共享、介质是可读写介质还是只读介质等）。VBD 具有将 VDI 绑定到 VM 的属性（是否可引导、其读取/写入指标等）。

可以使用标准对象列出命令 (`xe vdi-list`) 列出 VDI 对象，并使用标准参数命令操纵参数。有关详细信息，请参阅低级参数命令。

## VDI 参数

VDI 包含下列参数：

| 参数名称                              | 说明                                          | 类型           |
|-----------------------------------|---------------------------------------------|--------------|
| <code>uuid</code>                 | VDI 的唯一标识符/对象引用                             | 只读           |
| <code>name-label</code>           | VDI 的名称                                     | 读取/写入        |
| <code>name-description</code>     | VDI 的描述字符串                                  | 读取/写入        |
| <code>allowed-operations</code>   | 在此状态下允许执行的操作的列表                             | 只读 set 参数    |
| <code>current-operations</code>   | 此 VDI 上当前正在进行的操作的列表                         | 只读 set 参数    |
| <code>sr-uuid</code>              | VDI 所在的 SR                                  | 只读           |
| <code>vbd-uuids</code>            | 引用此 VDI 的 VBD 的列表                           | 只读 set 参数    |
| <code>crashdump-uuids</code>      | 引用此 VDI 的故障转储的列表                            | 只读 set 参数    |
| <code>virtual-size</code>         | 向 VM 提供的磁盘大小（以字节为单位）。此大小可能会不准确，具体取决于存储后端的类型 | 只读           |
| <code>physical-utilisation</code> | VDI 在 SR 上占用的物理空间量（以字节为单位）                  | 只读           |
| <code>type</code>                 | VDI 的类型，例如系统或用户                             | 只读           |
| <code>sharable</code>             | 如果此 VDI 可以共享，则为 True                        | 只读           |
| <code>read-only</code>            | 如果此 VDI 仅可以装载为只读，则为 True                    | 只读           |
| <code>storage-lock</code>         | 如果此 VDI 锁定在存储级别，则为 True                     | 只读           |
| <code>parent</code>               | 如果此 VDI 是链的一部分，则引用父 VDI                     | 只读           |
| <code>missing</code>              | 如果 SR 扫描操作报告此 VDI 不存在，则为 True               | 只读           |
| <code>other-config</code>         | 此 VDI 的额外配置信息                               | 读取/写入 map 参数 |
| <code>sr-name-label</code>        | 所包含的存储库的名称                                  | 只读           |
| <code>location</code>             | 位置信息                                        | 只读           |
| <code>managed</code>              | 如果 VDI 是托管的，则为 True                         | 只读           |

| 参数名称                          | 说明                                                                                                                                                  | 类型        |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <code>xenstore-data</code>    | 在连接 VDI 后将插入到 xenstore 树 (/local/domain/0/backend/vbd/ <i>domid</i> / <i>dev</i> / <i>id</i> /sm-data) 的数据。SM 后端通常在 <code>vdi_attach</code> 上设置此字段。 | 只读 map 参数 |
| <code>sm-config</code>        | SM 依赖数据                                                                                                                                             | 只读 map 参数 |
| <code>is-a-snapshot</code>    | 如果此 VDI 是 VM 存储快照, 则为 True                                                                                                                          | 只读        |
| <code>snapshot_of</code>      | 以此 VDI 为快照的存储的 UUID                                                                                                                                 | 只读        |
| <code>snapshots</code>        | 此 VDI 的所有快照的 UUID                                                                                                                                   | 只读        |
| <code>snapshot_time</code>    | 创建此 VDI 的快照操作的时间戳                                                                                                                                   | 只读        |
| <code>metadata-of-pool</code> | 创建此元数据 VDI 的池的 UUID                                                                                                                                 | 只读        |
| <code>metadata-latest</code>  | 指示 VDI 中是否包含此池的最新已知元数据的标志                                                                                                                           | 只读        |
| <code>cbt-enabled</code>      | 指示是否为 VDI 启用了更改块跟踪的标记                                                                                                                               | 读取/写入     |

## **vdi-clone**

```
1 vdi-clone uuid=uuid_of_the_vdi [driver-params:key=value]
```

创建指定 VDI 的新可写副本, 此副本可直接使用。它是 `vdi-copy` 的变体, 可公开其所在的映像高速克隆工具。

使用可选 `driver-params` 映射参数将额外的供应商特定的配置信息传递到 VDI 所基于的后端存储驱动程序。有关详细信息, 请参阅存储供应商驱动程序文档。

## **vdi-copy**

```
1 vdi-copy uuid=uuid_of_the_vdi sr-uuid=uuid_of_the_destination_sr
```

将 VDI 复制到指定的 SR。

## **vdi-create**

```
1 vdi-create sr-uuid=uuid_of_sr_to_create_vdi_on name=label=  
   name_for_the_vdi type=system|user|suspend|crashdump virtual-size=  
   size_of_virtual_disk sm-config-*=storage_specific_configuration_data
```

创建 VDI。

`virtual-size` 参数可以以字节为单位进行指定，也可以使用 IEC 标准后缀 KiB、MiB、GiB 和 TiB 来指定。

注意：

支持磁盘的精简预配的 SR 类型（例如本地 VHD 和 NFS）不强制执行磁盘的虚拟分配。在 SR 上过量分配虚拟磁盘空间时应十分小心。当过量分配的 SR 变满时，SR 目标基底上必须提供可用磁盘空间，或通过删除 SR 中未使用的 VDI 来获得磁盘空间。

某些 SR 类型可能会对 `virtual-size` 值进行舍入处理，以使此值可被已配置块的大小整除。

### **vdi-data-destroy**

```
1 vdi-data-destroy uuid=uuid_of_vdi
```

销毁与指定 VDI 关联的数据，但保留更改块跟踪元数据。

注意：

如果使用更改块跟踪功能对 VDI 进行增量备份，请务必使用 `vdi-data-destroy` 命令删除快照，但保留元数据。请勿在启用了更改块跟踪功能的 VDI 的快照上使用 `vdi-destroy`。

### **vdi-destroy**

```
1 vdi-destroy uuid=uuid_of_vdi
```

销毁指定的 VDI。

注意：

如果使用更改块跟踪功能对 VDI 进行增量备份，请务必使用 `vdi-data-destroy` 命令删除快照，但保留元数据。请勿在启用了更改块跟踪功能的 VDI 的快照上使用 `vdi-destroy`。

对于本地 VHD 和 NFS SR 类型，使用 `vdi-destroy` 不能立即释放磁盘空间，而是在存储库扫描操作期间定期释放磁盘空间。如果必须强制使删除所得的磁盘空间可用，应手动调用 `[sr-scan](#sr-scan)`。

### **vdi-disable-cbt**

```
1 vdi-disable-cbt uuid=uuid_of_vdi
```

对 VDI 禁用更改块跟踪。

### **vdi-enable-cbt**

```
1 vdi-enable-cbt uuid=uuid_of_vdi
```

对 VDI 启用更改块跟踪。

注意：

只能对获得许可的 Citrix Hypervisor Premium Edition 实例启用更改块跟踪功能。

### **vdi-export**

```
1 vdi-export uuid=uuid_of_vdi filename=filename_to_export_to [format=
  format] [base=uuid_of_base_vdi] [--progress]
```

将 VDI 导出到指定的文件名。您可以采用以下格式之一导出 VDI：

- raw
- vhd

VHD 格式可以为稀疏。如果 VDI 中存在未分配的块，则可能从 VHD 文件中忽略这些块，因此使 VHD 文件更小。您可以从所有受支持的基于 VHD 的存储类型（EXT、NFS）导出到 VHD 格式。

如果指定 `base` 参数，此命令将仅导出那些在已导出的 VDI 和基础 VDI 之间发生更改的块。

### **vdi-forget**

```
1 vdi-forget uuid=uuid_of_vdi
```

从数据库无条件删除 VDI 记录，不涉及存储后端。在正常操作中，您应当使用 `[vdi-destroy](#vdi-destroy)`。

### **vdi-import**

```
1 vdi-import uuid=uuid_of_vdi filename=filename_to_import_from [format=
  format] [--progress]
```

导入 VDI。您可以采用以下格式之一导入 VDI：

- raw
- vhd

## **vdi-introduce**

```
1 vdi-introduce uuid=uuid_of_vdi sr-uuid=uuid_of_sr name=label=
  name_of_new_vdi type=system|user|suspend|crashdump location=
  device_location_(varies_by_storage_type) [name-description=
  description_of_vdi] [sharable=yes|no] [read-only=yes|no] [other-
  config=map_to_store_misc_user_specific_data] [xenstore-data=
  map_to_of_additional_xenstore_keys] [sm-config=
  storage_specific_configuration_data]
```

创建代表现有存储设备的 VDI 对象，无需实际修改或创建任何存储。此命令主要在内部使用，用来自动引入热插入存储设备。

## **vdi-list-changed-blocks**

```
1 vdi-list-changed-blocks vdi-from-uuid=first-vdi-uuid vdi-to-uuid=second
  -vdi-uuid
```

比较两个 VDI 并以 base64 编码的字符串格式返回两个 VDI 之间更改的块的列表。此命令仅适用于启用了更改块跟踪功能的 VDI。

有关详细信息，请参阅[更改块跟踪](#)。

## **vdi-pool-migrate**

```
1 vdi-pool-migrate uuid=VDI_uuid sr-uuid=destination-sr-uuid
```

将 VDI 迁移到指定的 SR，同时将 VDI 连接到正在运行的来宾系统。（存储实时迁移）

有关详细信息，请参阅[迁移 VM](#)。

## **vdi-resize**

```
1 vdi-resize uuid=vdi_uuid disk-size=new_size_for_disk
```

更改由 UUID 指定的 VDI 的大小。

## **vdi-snapshot**

```
1 vdi-snapshot uuid=uuid_of_the_vdi [driver-params=params]
```

生成 VDI 的读写版本，该版本可用作进行备份或创建模板时的参考。使用快照可以执行备份，而非在 VM 内部安装和运行备份软件。当外部备份软件将快照内容发送到备份介质时，VM 可以继续运行。同样，快照可用作“黄金映像”，可以基于此映像创建模板。可以使用任何 VDI 创建模板。

使用可选 `driver-params` 映射参数将额外的供应商特定的配置信息传递到 VDI 所基于的后端存储驱动程序。有关详细信息，请参阅存储供应商驱动程序文档。

克隆快照应始终生成可写 VDI。

## **vdi-unlock**

```
1 vdi-unlock uuid=uuid_of_vdi_to_unlock [force=true]
```

尝试取消对指定 VDI 的锁定。如果将 `force=true` 传递给此命令，它将强制执行取消锁定操作。

## **vdi-update**

```
1 vdi-update uuid=uuid
```

刷新数据库中 VDI 对象的字段。

## **VIF 命令**

用于 VIF（虚拟网络接口）的命令。

可以使用标准对象列出命令 (`xe vif-list`) 列出 VIF 对象，并使用标准参数命令操纵参数。有关详细信息，请参阅低级参数命令。

## **VIF 参数**

VIF 包含下列参数：

- `uuid`（只读）VIF 的唯一标识符/对象引用
- `vm-uuid`（只读）此 VIF 所在 VM 的唯一标识符/对象引用
- `vm-name-label`（只读）此 VIF 所在 VM 的名称
- `allowed-operations`（只读 set 参数）在此状态下允许执行的操作的列表
- `current-operations`（只读 set 参数）当前正在对此 VIF 执行的操作的列表
- `device`（只读）此 VIF 的整数标签，指示 VIF 后端的创建顺序
- `MAC`（只读）对 VM 公开的 VIF 的 MAC 地址

- **MTU** (只读) VIF 的最大传输单位 (以字节为单位)。

此参数为只读参数，但是可以通过使用 `other-config` 映射参数的 `mtu` 键覆盖 MTU 设置。例如，在虚拟 NIC 上重置 MTU 以使用巨型帧：

```
1 xe vif-param-set \
2     uuid=<vif_uuid> \
3     other-config:mtu=9000
```

- `currently-attached` (只读) 如果连接了设备，则为 `true`
- `qos_algorithm_type` (读取/写入) 要使用的 QoS 算法
- `qos_algorithm_params` (读取/写入 map 参数) 所选 QoS 算法的参数
- `qos_supported_algorithms` (只读 set 参数) 此 VIF 支持的 QoS 算法
- `MAC-autogenerated` (只读) 如果自动生成 VIF 的 MAC 地址，则为 `True`
- `other-config` (读取/写入 map 参数) 额外的配置 `key:value` 对
- `other-config:ethtoolrx` (读取/写入) 设置为 `on` 会启用接收校验和，设置为 `off` 会禁用接收校验和
- `other-config:ethtooltx` (读取/写入) 设置为 `on` 会启用发送校验和，设置为 `off` 会禁用发送校验和
- `other-config:ethtoolsg` (读取/写入) 设置为 `on` 会启用分散收集，设置为 `off` 会禁用分散收集
- `other-config:ethtooltso` (读取/写入) 设置为 `on` 会启用 TCP 分段卸载，设置为 `off` 会禁用 TCP 分段卸载
- `other-config:ethtoolufo` (读取/写入) 设置为 `on` 会启用 UDP 段卸载，设置为 `off` 会禁用 UDP 段卸载
- `other-config:ethtoolgso` (读取/写入) 设置为 `on` 会启用通用分段卸载，设置为 `off` 会禁用通用分段卸载
- `other-config:promiscuous` (读取/写入) 为 `true` 时，VIF 在桥上为混杂模式，以便监测通过该桥的所有通信。对于在 VM 中运行入侵检测系统 (IDS) 或类似系统会有所帮助。
- `network-uuid` (只读) 此 VIF 连接到的虚拟网络的唯一标识符/对象引用
- `network-name-label` (只读) 此 VIF 连接到的虚拟网络的描述性名称
- `io_read_kbs` (只读) 此 VIF 的平均读取速率 (以 kb/秒为单位)
- `io_write_kbs` (只读) 此 VIF 的平均写入速率 (以 kb/秒为单位)
- `locking_mode` (读取/写入) 影响 VIF 能不能过滤到/来自 MAC 和 IP 地址列表的通信。需要额外参数。
- `locking_mode:default` (读取/写入) 因 VIF 网络的默认锁定模式而异。

如果将 `default-locking-mode` 设为 `disabled`，则 Citrix Hypervisor 应用过滤规则，使 VIF 无法发送或接收通信。如果将 `default-locking-mode` 设为 `unlocked`，Citrix Hypervisor 将删除所有与 VIF 相关联的过滤规则。有关详细信息，请参阅网络命令。

- `locking_mode:locked` (读取/写入) 仅允许通过 VIF 传输发送到指定 MAC 和 IP 地址的流量或从这些地址发送的流量。如果不指定 IP 地址, 则不允许任何流量。
- `locking_mode:unlocked` (读取/写入) 不对任何传入或传出 VIF 的流量应用任何过滤器。
- `locking_mode:disabled` (读取/写入) Citrix Hypervisor 会应用一个过滤规则, 以使 VIF 丢弃所有通信。

## **vif-create**

```
1 vif-create vm-uuid=uuid_of_the_vm device=see below network-uuid=
   uuid_of_network_to_connect_to [mac=mac_address]
```

在 VM 上创建 VIF。

`device` 字段中相应的值列在指定 VM 上的 `allowed-VIF-devices` 参数中。如果 VM 中尚不存在 VIF, 则值为从 0 到 15 之间的整数。

`mac` 参数为标准 MAC 地址, 格式为 `aa:bb:cc:dd:ee:ff`。如果不指定此地址, 则会创建一个适当的随机 MAC 地址。还可以通过指定 `mac=random` 显式设置一个随机 MAC 地址。

## **vif-destroy**

```
1 vif-destroy uuid=uuid_of_vif
```

销毁 VIF。

## **vif-move**

```
1 vif-move uuid=uuid network-uuid=network_uuid
```

将 VIF 移到另一个网络。

## **vif-plug**

```
1 vif-plug uuid=uuid_of_vif
```

尝试在 VM 处于运行状态时连接 VIF。

## vif-unplug

```
1 vif-unplug uuid=uuid_of_vif
```

当 VM 处于运行状态时尝试将 VIF 从中分离出来。

## vif-configure-ipv4

为此虚拟接口配置 IPv4 设置。按如下所示设置 IPv4 设置：

```
1 vif-configure-ipv4 uuid=uuid_of_vif mode=static address=CIDR_address
  gateway=gateway_address
```

例如：

```
1 VIF.configure_ipv4(vifObject,"static", " 192.168.1.10/24", "
  192.168.1.1")
```

按如下所示清理 IPv4 设置：

```
1 vif-configure-ipv4 uuid=uuid_of_vif mode=none
```

## vif-configure-ipv6

为此虚拟接口配置 IPv6 设置。按如下所示设置 IPv6 设置：

```
1 vif-configure-ipv6 uuid=uuid_of_vif mode=static address=IP_address
  gateway=gateway_address
```

例如：

```
1 VIF.configure_ipv6(vifObject,"static", "fd06:7768:b9e5:8b00::5001/64",
  "fd06:7768:b9e5:8b00::1")
```

按如下所示清理 IPv6 设置：

```
1 vif-configure-ipv6 uuid=uuid_of_vif mode=none
```

## VLAN 命令

用于 VLAN（虚拟网络）的命令。要列出并编辑虚拟接口，请参阅 PIF 命令，这些命令包含 VLAN 参数以指示虚拟接口具有关联虚拟网络。有关详细信息，请参阅 PIF 命令。例如，要列出 VLAN，请使用 `xe pif-list`。

## **vlan-create**

```
1 vlan-create pif-uuid=uuid_of_pif vlan=vlan_number network-uuid=
   uuid_of_network
```

在 Citrix Hypervisor 服务器上创建 VLAN。

## **pool-vlan-create**

```
1 pool-vlan-create pif-uuid=uuid_of_pif vlan=vlan_number network-uuid=
   uuid_of_network
```

通过确定特定网络所在的每个主机的接口（例如 `eth0`），并在每个相应的主机上创建和插入一个新的 PIF 对象，为池中的所有主机创建一个 VLAN。

## **vlan-destroy**

```
1 vlan-destroy uuid=uuid_of_pif_mapped_to_vlan
```

销毁 VLAN。需要使用表示 VLAN 的 PIF 的 UUID。

## **VM 命令**

控制 VM 及其属性的命令。

### **VM 选择器**

此处列出的几个命令具有一个共同的机制，即可选择一个或多个要对其执行操作的 VM。最简单的方法是提供参数 `vm=name_or_uuid`。例如，获取实际 VM 的 UUID 的一种简单的方法是执行 `xe vm-list power-state=running`。（获取可通过使用命令 `xe vm-list params=all` 进行匹配的字段的完整列表）例如，指定 `power-state=halted` 将选择其 `power-state` 参数等于 `halted` 的 VM。如果有多个匹配的 VM，则应指定选项 `--multiple` 来执行此操作。本节开头介绍了可匹配的完整参数列表。

可以使用标准对象列出命令 (`xe vm-list`) 列出 VM 对象，并使用标准参数命令操纵参数。有关详细信息，请参阅低级参数命令。

### **VM 参数**

VM 具有下列参数：

**注意：**

当 VM 运行时，可以更改所有可写入的 VM 参数值，但不会动态应用新参数，并且重新启动 VM 之后才能应用新参数。

- `appliance` (读取/写入) VM 所属的设备/vApp
- `uuid` (只读) VM 的唯一标识符/对象引用
- `name-label` (读取/写入) VM 的名称
- `name-description` (读取/写入) VM 的描述字符串
- `order start order` (读取/写入) 用于 vApp 启动/关闭以及在进行高可用性故障转移之后启动
- `version` (只读) 此 VM 已经恢复的次数。如果要使用较早的版本覆盖新 VM，则调用 `vm-recover`
- `user-version` (读取/写入) 用于输入版本信息的 VM 和模板创建者的字符串
- `is-a-template` (读取/写入) 除非此 VM 为模板，否则为 False。模板 VM 无法启动，它们仅用于克隆其他 VM。将此值重置为 `true` 后，将无法再重置为 `false`。不能使用此参数将模板 VM 转换为 VM。
- `is-control-domain` (只读) 如果是控制域 (域 0 或驱动程序域)，则为 True
- `power-state` (只读) 当前电源状态
- `start-delay` (读取/写入) 在用来启动 VM 的调用返回之前等待的时间
- `shutdown-delay` (读取/写入) 在用来关闭 VM 的调用返回之前等待的时间
- `memory-dynamic-max` (读取/写入) 最大动态内存 (以字节为单位)
- `memory-dynamic-min` (读取/写入) 最小动态内存 (以字节为单位)
- `memory-static-max` (读取/写入) 静态设置 (绝对) 最大内存 (以字节为单位)。如果要更改此值，必须关闭 VM。
- `memory-static-min` (读取/写入) 静态设置 (绝对) 最小内存 (以字节为单位)。如果要更改此值，必须关闭 VM。
- `suspend-VDI-uuid` (只读) 存储挂起映像的 VDI
- `VCPUs-params` (读取/写入 map 参数) 所选 vCPU 策略的配置参数。

可以使用以下命令调整 vCPU 固定

```
1 xe vm-param-set uuid=<vm_uuid> VCPUs-params:mask=1,2,3
```

然后，所选 VM 仅在物理 CPU 1、2 和 3 上运行。

还可以使用 `cap` 和 `weight` 参数调整 vCPU 优先级 (xen 调度)。例如：

```
1 xe vm-param-set uuid=<vm_uuid> VCPUs-params:weight=512 xe vm-
  param-set uuid=<vm_uuid> VCPUs-params:cap=100
```

在竞争的 Citrix Hypervisor 服务器上，权重为 512 的 VM 获得的 CPU 将是权重为 256 的域的两倍。合法的权重范围为 1 到 65535，默认值为 256。即使 Citrix Hypervisor 服务器具有空闲 CPU 周期，该上限也可以选择性地确定 VM 能够占用的最大 CPU 量。此上限以一个物理 CPU 的百分比表示：100 是 1 个物理 CPU，50 是半个物理 CPU，400 是 4 个物理 CPU，依此类推。默认值为 0，表示无上限。

- `VCPUs-max`（读取/写入）虚拟 CPU 的最大数量。
- `VCPUs-at-startup`（读取/写入）虚拟 CPU 的引导编号
- `actions-after-crash`（读取/写入）VM 崩溃后执行的操作。对于 PV 来宾，有效的参数如下：
  - `preserve`（仅供分析使用）
  - `coredump_and_restart`（记录核心转储并重新启动 VM）
  - `coredump_and_destroy`（记录核心转储并使 VM 处于已停止状态）
  - `restart`（不记录核心转储并重新启动 VM）
  - `destroy`（不记录核心转储并使 VM 处于已停止状态）
- `console-uuids`（只读 set 参数）虚拟控制台设备
- `platform`（读取/写入 map 参数）特定于平台的配置

要禁止 Virtual Desktop Agent (VDA) 将 Windows 10 切换到平板电脑模式，请执行以下操作：

```
1 xe vm-param-set uuid=<vm_uuid> platform:acpi_laptop_slate=0
```

要允许 VDA 将 Windows 10 切换到平板电脑模式，请执行以下操作：

```
1 xe vm-param-set uuid=<vm_uuid> platform:acpi_laptop_slate=1
```

要检查当前状态，请执行以下操作：

```
1 xe vm-param-get uuid=<vm_uuid> param-name=platform param-key=
  acpi_laptop_slate
```

- `allowed-operations`（只读 set 参数）在此状态下允许执行的操作的列表
- `current-operations`（只读 set 参数）当前正在对 VM 执行的操作的列表
- `allowed-VBD-devices`（只读 set 参数）可供使用的 VBD 标识符的列表，用 0 到 15 之间的整数表示。此列表仅供参考，可以使用未在此列表中列出的其他设备（但可能无法正常运行）。
- `allowed-VIF-devices`（只读 set 参数）可供使用的 VIF 标识符的列表，用 0 到 15 之间的整数表示。此列表仅供参考，可以使用未在此列表中列出的其他设备（但可能无法正常运行）。
- `HVM-boot-policy`（读取/写入）HVM 来宾系统的引导策略。BIOS 顺序或空字符串。
- `HVM-boot-params`（读取/写入 map 参数）`order` 键控制 HVM 来宾系统引导顺序，以字符串表示，其中每个字符代表一种引导方法：d 代表 CD/DVD，c 代表根磁盘，n 代表网络 PXE 引导。默认值为 dc。

- `HVM-shadow-multiplier` (读取/写入) 浮点值, 用于控制授予 VM 的影子内存开销量。默认值为 1.0 (最小值), 只有高级用户才能更改此值。
- `PV-kernel` (读取/写入) 内核路径
- `PV-ramdisk` (读取/写入) `initrd` 路径
- `PV-args` (读取/写入) 内核命令行参数字符串
- `PV-legacy-args` (读取/写入) 引导旧 VM 的参数字符串
- `PV-bootloader` (读取/写入) 引导加载程序的名称或路径
- `PV-bootloader-args` (读取/写入) 引导加载程序的其他参数的字符串
- `last-boot-CPU-flags` (只读) 描述上次引导 VM 时所在的 CPU 的标志
- `resident-on` (只读) VM 所在的 Citrix Hypervisor 服务器
- `affinity` (读取/写入) VM 在其上具有优先运行权的 Citrix Hypervisor 服务器。由 `xe vm-start` 命令用于确定在何处运行 VM
- `other-config`(读取/写入 `map` 参数)为 VM 指定额外配置参数的键/值对列表。例如,如果 `other-config` 参数包括键/值对 `auto_poweron: true`, 则引导主机后将自动启动 VM
- `start-time` (只读) 读取 VM 的指标的日期和时间的戳。此时间戳以 `yyyymmddThh:mm:ss z` 的形式表示, 其中 `z` 是单字母军用时区指示器, 例如, `Z` 代表 UTC (GMT)
- `install-time` (只读) 读取 VM 的指标的日期和时间的戳。此时间戳以 `yyyymmddThh:mm:ss z` 的形式表示, 其中 `z` 是单字母军用时区指示器, 例如, `Z` 代表 UTC (GMT)
- `memory-actual` (只读) VM 使用的实际内存
- `VCPUs-number` (只读) 为 PV (半虚拟化) 或 HVM (硬件虚拟机) Linux VM 分配给 VM 的虚拟 CPU 数量。此数量可能与 `VCPUS-max` 不同且使用 `vm-vcpu-hotplug` 命令就可以对此数量进行更改, 而不必重新引导 VM。有关详细信息, 请参阅 `[vm-vcpu-hotplug](#vm-vcpu-hotplug)`。Windows VM 始终在 `vCPU` 数量设置为 `VCPUSmax` 的情况下运行并且必须重新启动才可以更改此值。如果为 `VCPUs-number` 设置的值大于 Citrix Hypervisor 服务器上的物理 CPU 数量, 性能将急剧下降。
- `VCPUs-Utilization` (只读 `map` 参数) 虚拟 CPU 及其权重的列表
- `os-version` (只读 `map` 参数) VM 的操作系统版本
- `PV-drivers-version` (只读 `map` 参数) VM 的半虚拟化驱动程序版本
- `PV-drivers-detected` (只读) VM 的半虚拟化驱动程序最新版本的标志
- `memory` (只读 `map` 参数) 由 VM 上的代理报告的内存指标
- `disks` (只读 `map` 参数) 有 VM 上的代理报告的磁盘指标
- `networks` (只读 `map` 参数) 由 VM 上的代理报告的网络指标
- `other` (只读 `map` 参数) 由 VM 上的代理报告的其他指标

- `guest-metrics-lastupdated` (只读) 来宾代理对这些字段执行最后一次写入操作时的时间戳。此时间戳以 `yyyymmddThh:mm:ss z` 的形式表示, 其中 `z` 是单字母军用时区指示器, 例如, `Z` 代表 UTC (GMT)
- `actions-after-shutdown` (读取/写入) 将在 VM 关闭后执行的操作
- `actions-after-reboot` (读取/写入) 将在 VM 重新启动后执行的操作
- `possible-hosts` 可能驻留此只读 VM 的主机
- `dom-id` (只读) 域 ID (如果可用, 否则为 -1)
- `recommendations` (只读) 此 VM 的建议值和属性范围的 XML 规范
- `xenstore-data` (读取/写入 `map` 参数) 在创建 VM 后将插入到 xenstore 树 (`/local/domain/domid/vm-data`) 的数据。
- `is-a-snapshot` (只读) 如果此 VM 为快照, 则为 `True`
- `snapshot_of` (只读) 以此 VM 为快照的 VM 的 UUID
- `snapshots` (只读) 此 VM 的所有快照的 UUID
- `snapshot_time` (只读) 创建此 VM 快照的快照操作的时间戳
- `memory-target` (只读) 为此 VM 设置的目标内存量
- `blocked-operations` (读取/写入 `map` 参数) 列出无法对此 VM 执行的操作
- `last-boot-record` (只读) 此模板的上次引导参数的记录, 使用 XML 格式
- `ha-always-run` (读取/写入) 如果此 VM 在其所在的主机发生故障后始终在其他主机上重新启动, 则为 `True`。此参数现已弃用。请改为使用 `ha-restart-priority` 参数。
- `ha-restart-priority` (读取/写入) 重新启动或最大努力
- `blobs` (只读) 二进制数据存储
- `live` (只读) 如果 VM 正在运行, 则为 `True`。如果高可用性功能猜测 VM 可能没有运行, 则为 `False`。

### **vm-assert-can-be-recovered**

```
1 vm-assert-can-be-recovered uuid [database] vdi-uuid
```

测试存储是否可用于恢复此 VM。

### **vm-call-plugin**

```
1 vm-call-plugin vm-uuid=vm_uuid plugin=plugin fn=function [args:key=
  value]
```

使用可选参数 (args:key=value) 调用指定 VM 上的插件中的功能。要传递其中包含特殊字符 (例如, 换行) 的 “value”, 可以适当使用替代语法 args:key:file=local\_file, 其中 local\_file 的内容将作为整体进行检索并分配给 “key”。

### vm-cd-add

```
1 vm-cd-add cd-name=name_of_new_cd device=  
integer_value_of_an_available_vbd [vm-selector=vm_selector_value...]
```

将新虚拟 CD 添加到所选的 VM。应从 VM 的 `allowed-VBD-devices` 参数值中选择 `device` 参数。

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息, 请参阅 VM 选择器。可选参数可以为本节开头列出的 VM 参数中的任意数量。

### vm-cd-eject

```
1 vm-cd-eject [vm-selector=vm_selector_value...]
```

从虚拟 CD 驱动器弹出 CD。仅当只有一个 CD 连接到 VM 时, 此命令才有效。如果有两个或更多 CD, 请使用命令 `xe vbd-eject`, 并指定 VBD 的 UUID。

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息, 请参阅 VM 选择器。可选参数可以为本节开头列出的 VM 参数中的任意数量。

### vm-cd-insert

```
1 vm-cd-insert cd-name=name_of_cd [vm-selector=vm_selector_value...]
```

将 CD 插入到虚拟 CD 驱动器。仅当只有一个空 CD 设备连接到 VM 时, 此命令才有效。如果有两个或多个空 CD 设备, 请使用命令 `xe vbd-insert`, 并指定要插入的 VBD 和 VDI 的 UUID。

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息, 请参阅 VM 选择器。可选参数可以为本节开头列出的 VM 参数中的任意数量。

### vm-cd-list

```
1 vm-cd-list [vbd-params] [vdi-params] [vm-selector=vm_selector_value...]
```

列出连接到指定 VM 的 CD。

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息, 请参阅 VM 选择器。可选参数可以为本节开头列出的 VM 参数中的任意数量。

还可以选择要列出哪些 VBD 和 VDI 参数。

## vm-cd-remove

```
1 vm-cd-remove cd-name=name_of_cd [vm-selector=vm_selector_value...]
```

从指定 VM 中移除虚拟 CD。

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息，请参阅 VM 选择器。可选参数可以为本节开头列出的 VM 参数中的任意数量。

## vm-checkpoint

```
1 vm-checkpoint new-name-label=name_label [new-name-description=
description]
```

如果可用，请使用存储级别的快速磁盘克隆操作生成现有 VM 的检查点。

## vm-clone

```
1 vm-clone new-name-label=name_for_clone [new-name-description=
description_for_clone] [vm-selector=vm_selector_value...]
```

如果可用，请使用存储级别的快速磁盘克隆操作克隆现有的 VM。使用 **new-name-label** 和 **new-name-description** 参数为生成的克隆 VM 指定名称和可选说明。

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息，请参阅 VM 选择器。可选参数可以为本节开头列出的 VM 参数中的任意数量。

## vm-compute-maximum-memory

```
1 vm-compute-maximum-memory total=
amount_of_available_physical_ram_in_bytes [approximate=add overhead
memory for additional vCPUS? true|false] [vm-selector=
vm_selector_value...]
```

通过将物理 RAM 的总量用作上限来计算可以分配给现有 VM 的最大静态内存量。可选参数 **approximate** 在计算过程中保留足够的额外内存，以便以后将额外的 vCPU 添加到 VM。

例如：

```
1 xe vm-compute-maximum-memory vm=testvm total='xe host-list params=
memory-free --minimal'
```

此命令使用 `xe host-list` 命令返回的 `memory-free` 参数的值设置名为 `testvm` 的 VM 的最大内存。

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息，请参阅 VM 选择器。可选参数可以为本节开头列出的 VM 参数中的任意数量。

### **vm-compute-memory-overhead**

```
1 vm-compute-memory-overhead
```

计算 VM 的虚拟化内存开销。

### **vm-copy**

```
1 vm-copy new-name-label=name_for_copy [new-name-description=
  description_for_copy] [sr-uuid=uuid_of_sr] [vm-selector=
  vm_selector_value...]
```

复制现有 VM，但不使用存储级别的快速磁盘克隆操作（即使该操作可用）。保证 VM 副本的磁盘映像为完整映像，即该磁盘映像不是写入时复制 (CoW) 链的一部分。

使用 `new-name-label` 和 `new-name-description` 参数为生成的 VM 副本指定名称和可选说明。

使用 `sr-uuid` 为生成的 VM 副本指定目标 SR。如果未指定此参数，则目标 SR 与原始 VM 所在的 SR 相同。

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息，请参阅 VM 选择器。可选参数可以为本节开头列出的 VM 参数中的任意数量。

### **vm-copy-bios-strings**

```
1 vm-copy-bios-strings host-uuid=host_uuid
```

将指定主机的 BIOS 字符串复制到 VM。

### **vm-crashdump-list**

```
1 vm-crashdump-list [vm-selector=vm selector value...]
```

列出与指定 VM 关联的故障转储。

使用可选参数 `params` 时，`params` 的值是一个字符串，其中包含您希望显示的此对象的参数列表。或者，可以使用关键字 `all` 显示所有参数。如果不使用 `params`，则返回的列表将显示所有可用参数的默认子集。

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息，请参阅VM 选择器。可选参数可以为本节开头列出的VM 参数中的任意数量。

### **vm-data-source-list**

```
1 vm-data-source-list [vm-selector=vm selector value...]
```

列出可为 VM 记录的数据源。

通过使用标准选择机制来选择要在其上执行此操作的 VM。有关详细信息，请参阅VM 选择器。可选参数可以为本节开头列出的VM 参数中的任意数量。如果未提供用于选择主机的参数，将在所有 VM 上执行该操作。

数据源具有两个参数：`standard` 和 `enabled`，可以在此命令的输出中看到这两个参数。如果数据源的 `enabled` 设置为 `true`，则指标当前被记录到性能数据库中。如果数据源的 `standard` 设置为 `true`，则默认情况下指标会记录到性能数据库中（因此，该数据源的 `enabled` 也将设置为 `true`）。如果数据源的 `standard` 设置为 `false`，则默认情况下指标不会记录到性能数据库中（因此，该数据源的 `enabled` 也将设置为 `false`）。

要开始将数据源指标记录到性能数据库，请运行 `vm-data-source-record` 命令。此命令将 `enabled` 设置为 `true`。要停止记录，请运行 `vm-data-source-forget`。此命令将 `enabled` 设置为 `false`。

### **vm-data-source-record**

```
1 vm-data-source-record data-source=name_description_of_data-source [vm-selector=vm selector value...]
```

记录 VM 的指定数据源。

此操作会将数据源中的信息写入指定 VM 的静态性能指标数据库中。由于性能的原因，此数据库不同于普通的代理数据库。

通过使用标准选择机制来选择要在其上执行此操作的 VM。有关详细信息，请参阅VM 选择器。可选参数可以为本节开头列出的VM 参数中的任意数量。如果未提供用于选择主机的参数，将在所有 VM 上执行该操作。

### **vm-data-source-forget**

```
1 vm-data-source-forget data-source=name_description_of_data-source [vm-selector=vm selector value...]
```

停止为 VM 记录指定数据源并忽略所有已记录的数据。

通过使用标准选择机制来选择要在其上执行此操作的 VM。有关详细信息，请参阅VM 选择器。可选参数可以为本节开头列出的VM 参数中的任意数量。如果未提供用于选择主机的参数，将在所有 VM 上执行该操作。

## vm-data-source-query

```
1 vm-data-source-query data-source=name_description_of_data-source [vm-selector=vm_selector_value...]
```

显示 VM 的指定数据源。

通过使用标准选择机制来选择要在其上执行此操作的 VM。有关详细信息，请参阅VM 选择器。可选参数可以为本节开头列出的VM 参数中的任意数量。如果未提供用于选择主机的参数，将在所有 VM 上执行该操作。

## vm-destroy

```
1 vm-destroy uuid=uuid_of_vm
```

销毁指定的 VM。这会使与 VM 关联的存储保留不变。要同时删除存储，请使用 `xe vm-uninstall`。

## vm-disk-add

```
1 vm-disk-add disk-size=size_of_disk_to_add device=uuid_of_device [vm-selector=vm_selector_value...]
```

将磁盘添加到指定 VM。从 VM 的 `allowed-VBD-devices` 参数值中选择 `device` 参数。

`disk-size` 参数可以以字节为单位进行指定，也可以使用 IEC 标准后缀 KiB、MiB、GiB 和 TiB 来指定。

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息，请参阅VM 选择器。可选参数可以为本节开头列出的VM 参数中的任意数量。

## vm-disk-list

```
1 vm-disk-list [vbd-params] [vdi-params] [vm-selector=vm_selector_value...]
```

列出连接到指定 VM 的磁盘。`vbd-params` 和 `vdi-params` 参数控制要输出的各个对象的字段。以逗号分隔列表的形式指定这些参数，或者为整个列表指定特殊键 `all`。

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息，请参阅VM 选择器。可选参数可以为本节开头列出的VM 参数中的任意数量。

## vm-disk-remove

```
1 vm-disk-remove device=integer_label_of_disk [vm-selector=  
vm_selector_value...]
```

从指定 VM 移除磁盘并将其销毁。

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息，请参阅 VM 选择器。可选参数可以为本节开头列出的 VM 参数中的任意数量。

## vm-export

```
1 vm-export filename=export_filename [metadata=true|false] [vm-selector=  
vm_selector_value...]
```

将指定 VM（包括磁盘映像）导出到本地计算机上的文件中。使用 `filename` 参数指定将 VM 导出到的文件的文件名。按照惯例，此文件名的扩展名应该为 `.xva`。

如果 `metadata` 参数是 `true`，则不会导出磁盘。只有 VM 元数据才会被写入到输出文件中。当基础存储通过其他机制进行传输时使用此参数，并允许重新创建 VM 信息。有关详细信息，请参阅 `vm-import`。

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息，请参阅 VM 选择器。可选参数可以为本节开头列出的 VM 参数中的任意数量。

## vm-import

```
1 vm-import filename=export_filename [metadata=true|false] [preserve=true  
|false] [sr-uuid=destination_sr_uuid]
```

从之前导出的文件导入 VM。如果将 `preserve` 设置为 `true`，则将保留原始 VM 的 MAC 地址。`sr-uuid` 确定要将 VM 导入的目标 SR。如果未指定此参数，则使用默认 SR。

`filename` 参数还可以指向 XVA 格式的 VM，这是 Citrix Hypervisor 3.2 的传统导出格式。某些第三方供应商会使用此格式来提供虚拟设备。XVA 格式使用目录存储 VM 数据，因此将 `filename` 设置为 XVA 导出的根目录而不是实际的文件。导入的传统来宾系统的后续导出内容将自动升级到新的基于文件名的格式，这种格式可以存储更多关于 VM 配置的数据。

### 注意：

早期的基于目录的 XVA 格式不能完整保留所有 VM 属性。尤其是导入的 VM 在默认情况下不会连接任何虚拟网络接口。如果需要网络连接，则使用 `vif-create` 和 `vif-plug` 创建一个网络连接。

如果 `metadata` 为 `true`，则可以导入之前导出的一组元数据，而不会导入与之关联的磁盘块。如果找不到 VDI（按照 SR 和 `VDI.location` 命名），只导入元数据的操作将会失败，除非指定 `--force` 选项，这时无论遇到什么情况

导入都会继续。如果可以对磁盘进行镜像或将其移到带外，则元数据导入/导出是一种在无连接的池之间移动 VM 的快捷方法。例如，作为灾难恢复方案的一部分。

注意：

以串行方式导入多个 VM 比使用并行方式更快。

## vm-install

```
1 vm-install new-name-label=name [template-uuid=uuid_of_desired_template]
   [template=template_uuid_or_name] [sr-uuid=sr_uuid | sr-name-label=
   name_of_sr][copy-bios-strings-from=host_uuid]
```

基于模板安装或克隆 VM。使用 `template-uuid` 或 `template` 参数指定模板名称。使用 `sr-uuid` 或 `sr-name-label` 参数指定 SR。指定使用 `copy-bios-strings-from` 参数安装锁定了 BIOS 的介质。

注意：

在基于包含现有磁盘的模板进行安装时，将默认在现有磁盘所在的同一个 SR 中创建新磁盘。如果该 SR 支持基于模板的安装，这些磁盘将进行快速复制。如果在命令行上指定了其他 SR，则将在该 SR 中创建新磁盘。在这种情况下，无法实现快速复制，磁盘将进行完整复制。

基于不含现有磁盘的模板进行安装时，将在指定的 SR 中创建任何新磁盘；如果没有指定 SR，则将在池的默认 SR 中创建新磁盘。

## vm-is-bios-customized

```
1 vm-is-bios-customized
```

指示是否已自定义 VM 的 BIOS 字符串。

## vm-memory-balloon

```
1 vm-memory-balloon target=target
```

设置正在运行的 VM 的内存目标。指定的值必须位于 VM 的 `memory_dynamic_min` and `memory_dynamic_max` 值所定义的范围内。

## vm-memory-dynamic-range-set

```
1 vm-memory-dynamic-range-set min=min max=max
```

配置 VM 的动态内存范围。动态内存范围定义 VM 的内存下限和上限。可以在 VM 正在运行或已停止时更改这些字段。动态范围必须在静态范围内。

### **vm-memory-limits-set**

```
1 vm-memory-limits-set static-min=static_min static-max=static_max  
   dynamic-min=dynamic_min dynamic-max=dynamic_max
```

配置 VM 的内存限制。

### **vm-memory-set**

```
1 vm-memory-set memory=memory
```

配置 VM 的内存分配。

### **vm-memory-shadow-multiplier-set**

```
1 vm-memory-shadow-multiplier-set [vm-selector=vm_selector_value...] [  
   multiplier=float_memory_multiplier]
```

设置指定 VM 的影子内存系数。

这是用于修改分配给硬件辅助 VM 的影子内存量的高级选项。

在 Citrix Virtual Apps 等某些专用应用程序工作负载中，需要具有额外的影子内存才能获得最佳性能。

此内存视为一种系统开销。在计算 VM 内存时，此种内存与普通内存分开计算。调用此命令后，可用主机内存量将减少(减少量视系数而定)，并且 `HVM_shadow_multiplier` 字段将使用 Xen 分配给 VM 的值进行更新。如果没有足够的可用 Citrix Hypervisor 服务器内存，将返回错误。

将使用标准选择机制来选择应在其上执行此操作的 VM。有关详细信息，请参阅 VM 选择器。

### **vm-memory-static-range-set**

```
1 vm-memory-static-range-set min=min max=max
```

配置 VM 的静态内存范围。静态内存范围定义 VM 内存的下限和上限。只能在 VM 已停止时更改这些字段。静态范围必须大于动态范围。

**vm-memory-target-set**

```
1 vm-memory-target-set target=target
```

设置已停止或正在运行的 VM 的内存目标。指定的值必须位于 VM 的 `memory_static_min` and `memory_static_max` 值所定义的范围内。

**vm-memory-target-wait**

```
1 vm-memory-target-wait
```

等待正在运行的 VM 达到其当前内存目标。

**vm-migrate**

```
1 vm-migrate [copy=true|false] [host-uuid=destination_host_uuid] [host=
  name_or_uuid_of_destination_host] [force=true|false] [live=true|
  false] [vm-selector=vm_selector_value...] [remote-master=
  destination_pool_master_uuid] [remote-username=
  destination_pool_username] [remote-password=
  destination_pool_password] [remote-network=
  destination_pool_network_uuid] [vif:=vif_uuid] [vdi=vdi_uuid]
```

此命令在物理主机之间迁移指定的 VM。 `host` 参数可以是 Citrix Hypervisor 服务器的名称或 UUID。例如，要将 VM 迁移到池中的其他主机，其中，VM 磁盘位于两个主机共享的存储上，请运行以下命令：

```
1 xe vm-migrate uuid=vm_uuid host-uuid=host_uuid
```

要在同一个池中不共享存储的主机之间移动 VM（存储实时迁移），请运行以下命令：

```
1 xe vm-migrate uuid=vm_uuid remote-master=12.34.56.78 \
2   remote-username=username remote-password=password \
3   host-uuid=destination_host_uuid vdi=vdi_uuid
```

可以选择存储每个 VDI 的 SR：

```
1 xe vm-migrate uuid=vm_uuid host-uuid=destination_host_uuid \
2   vdi1:vdi_1_uuid=destination_sr_uuid \
3   vdi2:vdi_2_uuid=destination_sr2_uuid \
4   vdi3:vdi_3_uuid=destination_sr3_uuid
```

此外，还可以选择迁移后要连接 VM 的网络：

```
1 xe vm-migrate uuid=vm_uuid \  
2     vdi1:vdi_1_uuid=destination_sr_uuid \  
3     vdi2:vdi_2_uuid=destination_sr2_uuid \  
4     vdi3:vdi_3_uuid=destination_sr3_uuid \  
5     vif:vif_uuid=network_uuid
```

对于跨池迁移：

```
1 xe vm-migrate uuid=vm_uuid remote-master=12.34.56.78 \  
2     remote-username=username remote-password=password \  
3     host-uuid=destination_host_uuid vdi=vdi_uuid
```

有关存储实时迁移、实时迁移和实时 VDI 迁移的详细信息，请参阅[迁移 VM](#)。

默认情况下，VM 将挂起、迁移并在另一台主机上恢复。`live` 参数选择实时迁移。实时迁移使 VM 在执行迁移时继续运行，从而使 VM 停机时间缩短至小于一秒。在某些情况下（如 VM 中的内存工作负载繁重），实时迁移将自动恢复到默认模式，并在完成内存传输前将 VM 挂起一小段时间。

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息，请参阅 VM 选择器。可选参数可以为本节开头列出的 VM 参数中的任意数量。

## vm-pause

```
1 vm-pause
```

暂停正在运行的 VM。请注意，此操作不会释放关联的内存（请参阅 `vm-suspend`）。

## vm-query-services

```
1 vm-query-services
```

查询由给定 VM 提供的系统服务。

## vm-reboot

```
1 vm-reboot [vm-selector=vm_selector_value...] [force=true]
```

重新启动指定的 VM。

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息，请参阅 VM 选择器。可选参数可以为本节开头列出的 VM 参数中的任意数量。

使用 `force` 参数会导致非正常重新启动。关闭类似于拔出物理服务器上的插头。

### **vm-recover**

```
1 vm-recover vm-uuid [database] [vdi-uuid] [force]
```

从提供的 VDI 中包含的数据库恢复 VM。

### **vm-reset-powerstate**

```
1 vm-reset-powerstate [vm-selector=vm_selector_value...] {  
2   force=true }
```

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息，请参阅 VM 选择器。可选参数可以为本节开头列出的 VM 参数中的任意数量。

这是一个高级命令，仅在池中的成员主机出现故障时使用。您可以使用此命令强制池主服务器将 VM 的电源状态重置为 **halted**。实际上，此命令将强制锁定 VM 及其磁盘，以便可在另一台池主机上启动此 VM。此调用要求指定 **force** 标志，如果命令行中不存在 **force** 标志，则调用将失败。

### **vm-resume**

```
1 vm-resume [vm-selector=vm_selector_value...] [force=true|false] [on=  
   host_uuid]
```

恢复指定的 VM。

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息，请参阅 VM 选择器。可选参数可以为本节开头列出的 VM 参数中的任意数量。

如果 VM 位于主机池中的共享 SR 上，则使用 **on** 参数指定在其上启动 VM 的池成员。默认情况下，系统会确定合适的主机，该主机可能是池的任意成员。

### **vm-retrieve-wlb-recommendations**

```
1 vm-retrieve-wlb-recommendations
```

检索针对所选 VM 的 Workload Balancing 建议。

### **vm-shutdown**

```
1 vm-shutdown [vm-selector=vm_selector_value...] [force=true|false]
```

关闭指定的 VM。

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息，请参阅VM 选择器。可选参数可以为本节开头列出的VM 参数中的任意数量。

使用 `force` 参数将导致非正常关机，与拔掉物理服务器上的插头相似。

### vm-snapshot

```
1 vm-snapshot new-name-label=name_label [new-name-description+
   name_description]
```

如果可用，请使用存储级别的快速磁盘克隆操作生成现有 VM 的快照。

### vm-snapshot-with-quiet

```
1 vm-snapshot-with-quiet new-name-label=name_label [new-name-
   description+name_description]
```

如果可用，请使用存储级别的快速磁盘克隆操作生成现有 VM 的静止快照。

### vm-start

```
1 vm-start [vm-selector=vm_selector_value...] [force=true|false] [on=
   host_uuid] [--multiple]
```

启动指定的 VM。

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息，请参阅VM 选择器。可选参数可以为本节开头列出的VM 参数中的任意数量。

如果 VM 位于主机池中的共享 SR 上，则使用 `on` 参数指定在其上启动 VM 的池成员。默认情况下，系统会确定合适的主机，该主机可能是池的任意成员。

### vm-suspend

```
1 vm-suspend [vm-selector=vm_selector_value...]
```

挂起指定的 VM。

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息，请参阅VM 选择器。可选参数可以为本节开头列出的VM 参数中的任意数量。

## vm-uninstall

```
1 vm-uninstall [vm-selector=vm_selector_value...] [force=true|false]
```

卸载 VM — 销毁其磁盘（标记了 RW 且仅连接到此 VM 的 VDI）及其元数据记录。要仅销毁 VM 元数据，请使用 `xe vm-destroy`。

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息，请参阅 VM 选择器。可选参数可以为本节开头列出的 VM 参数中的任意数量。

## vm-unpause

```
1 vm-unpause
```

取消暂停已暂停的 VM。

## vm-vcpu-hotplug

```
1 vm-vcpu-hotplug new-vcpus=new_vcpu_count [vm-selector=vm_selector_value ...]
```

动态调整正在运行的 PV 或 HVM Linux VM 可用的 vCPU 数量。vCPU 数量由参数 `VCPUs-max` 进行限制。Windows VM 始终在 vCPU 数量设置为 `VCPUs-max` 的情况下运行并且必须重新启动才可以更改此值。

使用标准选择机制来选择将在其上执行此操作的 PV 或一个或多个 HVM Linux VM。有关详细信息，请参阅 VM 选择器。可选参数可以为本节开头列出的 VM 参数中的任意数量。

注意：

```
运行未安装 Citrix VM Tools 的某些 Linux VM 时，请以 root 用户身份在 VM 上运行以下命令以确保使用新热插拔的 vCPU: ## for i in /sys/devices/system/cpu/cpu[1-9]*/online; do if [ "$(cat $i)" = 0 ]; then echo 1 > $i; fi; done
```

## vm-vif-list

```
1 vm-vif-list [vm-selector=vm_selector_value...]
```

列出指定 VM 中的 VIF。

使用标准选择机制选择要在其上执行此操作的一个或多个 VM。有关详细信息，请参阅 VM 选择器。过滤时选择器将对 VM 记录执行操作，而不对 VIF 值执行操作。可选参数可以为本节开头列出的 VM 参数中的任意数量。

## 计划快照

用于控制 VM 计划快照及其属性的命令。

可以使用标准对象列出命令 (`xe vmss-list`) 列出 `vmss` 对象，并使用标准参数命令操纵参数。有关详细信息，请参阅低级参数命令。

### **vmss-create**

```
1 vmss-create enabled=True/False name=label=name type=type frequency=
  frequency retained-snapshots=value name-description=description
  schedule:schedule
```

在池中创建快照计划。

例如：

```
1 xe vmss-create retained-snapshots=9 enabled=true frequency=daily \
2   name-description=sample name=label=samplepolicy type=snapshot \
3   schedule:hour=10 schedule:min=30
```

快照计划具有以下参数：

| 参数名称                            | 说明                                                                                                                     | 类型    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------|-------|
| <code>name-label</code>         | 快照计划的名称。                                                                                                               | 读取/写入 |
| <code>name-description</code>   | 快照计划的说明。                                                                                                               | 读取/写入 |
| <code>type</code>               | 磁盘快照；内存快照；静止快照                                                                                                         | 读取/写入 |
| <code>frequency</code>          | 每小时；每日；每周                                                                                                              | 读取/写入 |
| <code>retained-snapshots</code> | 要保留的快照。范围：1-10。                                                                                                        | 读取/写入 |
| <code>schedule</code>           | <code>schedule:days</code> (星期一到星期日)， <code>schedule:hours</code> (0 到 23)， <code>schedule:minutes</code> (0、15、30、45) | 读取/写入 |

### **vmss-destroy**

```
1 vmss-destroy uuid=uuid
```

销毁池中的快照计划。

## USB 直通

### USB 直通启用/禁用

```
1 pusb-param-set uuid=pusb_uuid passthrough-enabled=true/false
```

启用/禁用 USB 直通。

### pusb-scan

```
1 pusb-scan host-uuid=host_uuid
```

扫描 PUSB 和更新。

### vusb-create

```
1 vusb-create usb-group-uuid=usb_group_uuid vm-uuid=vm_uuid
```

在池中创建虚拟 USB。启动 VM 以将 USB 直接传递到 VM。

### vusb-unplug

```
1 vusb-unplug uuid=vusb_uuid
```

从 VM 中拔出 USB 设备。

### vusb-destroy

```
1 vusb-destroy uuid=vusb_uuid
```

从 VM 中删除虚拟 USB 列表。

## SDK 和 API

June 4, 2019

以下 Citrix Hypervisor 开发人员文档在 <https://developer-docs.citrix.com/> 上提供。

- [管理 API 指南](#)
- [软件开发工具包指南](#)
- [更改块跟踪指南](#)
- [补充包和 DDK 指南](#)

**Locations**

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States

Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2019 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, 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).