



VMware Horizon 7 版本 7.11 发行说明

2019 年 12 月 12 日发行

本发行说明包括以下主题：

- [此版本的新增功能](#)
- [准备工作](#)
- [国际化](#)
- [兼容性说明](#)
- [支持的 Windows 10 操作系统](#)
- [支持 Red Hat Enterprise Linux Workstation](#)
- [Horizon 7 的早期版本](#)
- [已知问题](#)
- [已解决的问题](#)

此版本的新增功能

VMware Horizon 7 版本 7.11 提供了以下新功能和增强功能。这些信息是按可安装的组件分组的。

- [产品增强功能](#)
- [内部部署的 Horizon Connection Server](#)
- [Horizon Agent for Linux](#)
- [Horizon Agent](#)
- [Horizon GPO 包](#)
- [Horizon Client](#)
- [Horizon 7 Cloud Connector](#)
- [在 VMware Cloud on AWS 上部署的 Horizon 7](#)

有关此版本中所解决问题的信息，请参阅[已解决的问题](#)。

产品增强功能

VMware Horizon 7 版本 7.11 包含 Horizon Connection Server 和 Horizon Agent 的许多新功能和增强功能，包括继续构建 Horizon Console 的同等功能。Horizon Console 是基于 HTML5 的 Web 控制台，最终将取代 Horizon Administrator，而 Horizon Administrator 将于 2020 年初停用。

内部部署的 Horizon Connection Server

- [Horizon Console（基于 HTML5 的 Web 界面）](#)
对 Horizon Console 进行了多项功能增强。这些增强功能包括：
 - Horizon Console 现在是 Horizon 7 中推荐的主要 Web 界面。现有的基于闪存的 Horizon Administrator Web 界面仍受支持，但将于 2020 年初停用。请参阅《VMware Horizon Console 管理指南》文档中的[登录到 Horizon Console](#) 主题。
 - Horizon Help Desk Tool 将以更明显的方式集成到 Horizon Console 中。在 Horizon Console 中，单击“监控 > 技术支持”以打开 Horizon Help Desk Tool。请参阅《VMware Horizon Console 管理指南》文档中的[在 Horizon Console 中启动 Horizon Help Desk Tool](#) 主题。

- 您可以自定义在 RADIUS 双因素身份验证登录对话框中显示的用户名和密码标签。请参阅《VMware Horizon Console 管理指南》文档中的[在 Horizon Console 中启用双因素身份验证](#)主题。
- 您可以配置全局客户端限制设置，以将客户端会话连接限制为不受支持的 Horizon Client 版本的桌面和已发布应用程序。请参阅《VMware Horizon Console 管理指南》文档中的[Horizon Console 中客户端会话的全局客户端限制设置](#)主题。
- 您可以在 Horizon Console 中查看每个连接服务器的 CPU 和内存消耗情况。请参阅《VMware Horizon Console 管理指南》文档中的[监控 Horizon Connection Server 的负载状态](#)主题。
- “管理 Composer 桌面池映像”特权已重命名为“管理自动桌面和场的维护操作”特权。您可以使用此特权对即时克隆桌面池或场执行“推送映像”操作。请参阅《VMware Horizon Console 管理指南》文档中的[特定于对象的特权](#)。
- 在查看场的会话信息时，您可以查看与会话关联的已发布应用程序名称。请参阅《VMware Horizon Console 管理指南》文档中的[在 Horizon Console 中管理已发布的桌面和应用程序会话](#)主题。
- Cloud Pod 架构
 - 已验证 Horizon 7 版本 7.11 中每个容器有 12,000 个会话。
 - 要查看包含特定桌面池的全局桌面授权，您可以在 Horizon Console 中选择清单，>桌面。包含桌面池的全局桌面授权的名称将显示在“桌面池”页面上该桌面池的“全局授权”列中。您也可以在此“桌面池”页面上单击桌面池名称，然后在摘要选项卡上查看全局桌面授权的名称。
 - 您可以配置备份全局授权。当主全局授权因池容量不足或容器不可用等问题而无法启动会话时，备份全局授权会提供远程桌面或已发布的应用程序。备份全局授权可以包含来自容器联合中任何容器的池。请参阅《在 Horizon 7 中管理 Cloud Pod 架构》文档中的[实施备份全局授权](#)主题。
- 已发布的桌面和应用程序
 - Horizon 7 支持通用 Windows 平台 (UWP) 应用程序，这些应用程序是在 Windows 10 虚拟桌面 (WVD) 主机或桌面池上运行。请参阅《在 Horizon Console 中设置已发布的桌面和应用程序》文档中的[远程桌面服务主机](#)主题。
- 虚拟桌面
 - 进度条指示针对即时克隆池首次发布的主虚拟机和快照的暂挂映像状态。
- True SSO
 - 您可以使用第三方身份提供程序，该身份提供程序使用具有 True SSO 功能的 Unified Access Gateway 设备。请参阅《Horizon 7 管理指南》文档中的[设置 True SSO](#)主题。
- 负载均衡
 - VMware Avi 网络支持连接服务器、Unified Access Gateway 设备和 App Volumes Manager 的负载均衡。

Horizon Agent for Linux

- 支持的版本

Horizon Agent for Linux 现在支持 Linux 远程桌面的以下操作系统。有关详细信息，请参阅《设置 Horizon 7 for Linux 桌面》文档中的[Horizon 7 for Linux 的系统需求](#)主题。

 - RHEL 7.7
 - CentOS 7.7
 - CentOS 8.0
- RHEL/CentOS 8 桌面上的 True SSO

在运行 RHEL/CentOS 8 版本的手动和自动完整克隆桌面上支持 True SSO 功能。即时克隆 RHEL 8 桌面不支持 True SSO。请参阅《设置 Horizon 7 for Linux 桌面》文档中的[在 RHEL/CentOS 8 桌面上配置 True SSO](#)主题。

Horizon Agent

- 远程协议
 - 动态编码器切换支持在视频优化编码器（H.264 4:2:0 或 H.264 4:4:4）和文本优化编码器（Blast 编解码器或自适应编码器）之间进行切换。这种切换可帮助保持清晰的文本和视频，并减少使用的带宽。请参阅《Horizon 7 架构规划指南》文档中的[VMware Blast Extreme](#)主题。
 - HW 编码器支持 5 个或更多显示器。

- 将采用较大的数据包来批处理和发送暂挂消息，从而减少数据传输所用的带宽。
- 远程体验
 - 管理员可以使用注册表键字符串或为应用程序和进程配置 GPO 设置“VMware AppTap 配置”，以便在用户注销远程会话时，阻止远程会话终止的应用程序和进程将被忽略。在《在 Horizon 7 中配置远程桌面功能》文档中的 [VMware View Agent 配置 ADMX 模板设置](#) 主题中列出了 GPO 设置。
 - 为使用嵌套模式而准备桌面或 RDSH 映像时，您可以按任意顺序安装 Horizon Agent 和 Horizon Client。
 - Horizon Agent 安装程序支持已启用 LSA 的计算机。请参阅《在 Horizon Console 中设置虚拟桌面》文档中的 [在虚拟机上安装 Horizon Agent](#) 主题。

Horizon GPO 包

- VMware View Agent 配置 ADMX 模板文件 vdm_agent.admx 包含以下新设置：
 - 启用电池状态重定向
 - 在 RDSH 平台上启用 UWP 支持
 - VMware AppTap 配置
- VMware Horizon Client 配置 ADMX 模板文件 vdm_client.admx 包含以下新设置：
 - 将分辨率和 DPI 保存到服务器

Horizon Client

有关 Horizon Client 5.3 的新功能（包括 HTML Access 5.3）的信息，请参阅 [Horizon Client 文档](#) 页面上的发行说明。

Horizon 7 Cloud Connector

适用于 VMware Horizon 通用许可证客户。Horizon Cloud Connector 虚拟设备是 Horizon 7 版本 7.6 及更高版本的一个必要组件，支持通过 Horizon Cloud Service 管理 Horizon 7 容器。

在 VMware Cloud on AWS 上部署的 Horizon 7

有关 VMware Cloud on AWS 支持的 Horizon 7 功能列表，请参阅 [VMware 知识库文章 58539](#)。

准备工作

- **有关安装 VMware View Composer 的重要说明**

如果打算安装或升级到 View Composer 7.2 或更高版本，您必须将 Microsoft .NET Framework 升级到版本 4.6.1。否则，安装将会失败。
- **有关安装 VMware Tools 的重要说明**

如果您打算安装从 VMware 产品下载网站下载的 VMware Tools 版本，而不是随 vSphere 提供的默认版本，请确保支持该 VMware Tools 版本。要确定支持哪些 VMware Tools 版本，请访问 [VMware 产品互操作性列表](#)，选择 VMware Horizon View 解决方案和版本，然后选择 VMware Tools (仅可下载)。
- 如果要静默安装 View Composer，请参阅 VMware 知识库 (KB) 文章 2148204 [适用于 Horizon Composer 的 Microsoft Windows Installer 命令行选项](#)。
- 该 Horizon 7 版本包含与以前某些版本不同的新配置要求。请参阅《Horizon 7 升级指南》文档以了解升级说明。
- 如果要升级 Horizon 7 版本 6.2 以前的安装版本，并且连接服务器、安全服务器或 View Composer 服务器使用默认安装的自签名证书，则在执行升级之前，必须先移除现有的自签名证书。如果现有的自签名证书保留在原位，则连接可能无法正常工作。在升级过程中，安装程序不会替换任何现有证书。移除旧的自签名证书可确保新证书得到安装。与 6.2 以前的版本相比，此版本中的自签名证书具有更长的 RSA 密钥（2048 位，而不是 1024 位）和更强的签名（具有 RSA 的 SHA-256，而不是具有 RSA 的 SHA-1）。请注意，自签名证书并不安全，应尽可能替换为 CA 签名的证书，同时 SHA-1 证书也不再被认为是安全的，应替换为 SHA-2 证书。VMware 建议不要移除安装的用于生产的 CA 签名证书。在升级到该版本后，CA 签名的证书将继续正常工作。

作。

- 在执行全新安装或者将所有连接服务器实例升级到 Horizon 7 版本 7.2 或更高版本后，您无法将连接服务器实例降级到低于 Horizon 7 版本 7.2 的版本，因为用于保护 LDAP 数据的密钥已更改。要在计划升级到 Horizon 7 版本 7.2 或更高版本时保留降级连接服务器实例的可能性，您必须在开始升级之前执行 LDAP 备份。如果需要降级连接服务器实例，您必须降级所有连接服务器实例，然后将 LDAP 备份应用到最后降级的连接服务器。
- 如果在安装 Horizon Agent 时选择“扫描仪重定向”安装选项，可能会严重影响主机整合率。为了实现最佳主机整合，请确保仅为需要“扫描仪重定向”安装选项的用户启用此选项。（默认情况下，在安装 Horizon Agent 时，不会选择“扫描仪重定向”选项。）对于需要“扫描仪重定向”功能的用户，请配置单独的桌面池，并只在该池中选择此安装选项。
- Horizon 7 仅使用 TLSv1.1 和 TLSv1.2。在 FIPS 模式下，它仅使用 TLSv1.2。除非应用 vSphere 修补程序，否则，您可能无法连接到 vSphere。有关重新启用 TLSv1.0 的信息，请参阅《Horizon 7 升级指南》文档中的[对从连接服务器进行的 vCenter 连接启用 TLSv1.0](#)和[对从 View Composer 进行的 vCenter 和 ESXi 连接启用 TLSv1.0](#)。
- 6.2 以前的版本不支持 FIPS 模式。如果在 Windows 中启用 FIPS 模式并将 Horizon Composer 或 Horizon Agent 从低于 Horizon View 6.2 的版本升级到 Horizon 7 版本 7.2 或更高版本，则不会显示 FIPS 模式选项。您必须执行全新安装，而不是以 FIPS 模式安装 Horizon 7 版本 7.2 或更高版本。
- 对于 VMware Blast 显示协议，Linux 桌面使用端口 22443。
- 从 Horizon 7 版本 7.2 开始，您可以通过连接服务器强制设置密码套件顺序。有关详细信息，请参阅《Horizon 7 安全指南》文档。
- 从 Horizon 7 版本 7.2 开始，连接服务器必须能够在端口 32111 上与同一容器中的其他连接服务器进行通信。如果在安装或升级期间此通信被阻止，安装将会失败。
- 从 Horizon 7 版本 7.3.2 开始，端口 443 上的 TLS 握手必须在 10 秒内完成；如果启用了智能卡身份验证，则必须在 100 秒内完成。在之前版本的 Horizon 7 中，在任何情况下，均允许端口 443 上的 TLS 握手在 100 秒内完成。您可以通过设置配置属性 `handshakeLifetime` 来调整端口 443 上的 TLS 握手时间。（可选）可自动将导致 TLS 握手超时运行的客户端添加到黑名单中。来自黑名单的客户端的新连接将延迟可配置的一段时间再进行处理，以便优先处理其他客户端的连接。您可以通过设置配置属性 `secureHandshakeDelay` 来启用此功能。有关设置配置属性的详细信息，请参阅《Horizon 7 安全指南》文档。
- 当不存在“远程桌面服务”角色时，Horizon Agent 安装程序会提示您以 RDS 模式或桌面模式安装 Horizon Agent。

国际化

Horizon Administrator 和 Horizon Console 用户界面、Horizon Administrator 和 Horizon Console 联机帮助以及 Horizon 7 产品文档提供日语、法语、德语、西班牙语、简体中文、繁体中文和韩语版本。有关文档，请参阅 [VMware Horizon 7 文档中心](#)。

兼容性说明

- 有关单用户计算机和 RDS 主机上 Horizon Agent 支持的客户端操作系统，请参阅 VMware 知识库 (KB) 文章 2150295 [远程桌面系统中 Horizon Agent 支持的 Windows 版本](#)。
- 如果使用的 Horizon 7 服务器具有 6.2 之前的 View Agent 版本，您需要为 PCoIP 连接启用 TLSv1.0。6.2 之前的 View Agent 版本仅在 PCoIP 中支持安全协议 TLSv1.0。默认情况下，Horizon 7 服务器（包括连接服务器和安全服务器）将禁用 TLSv1.0。您可以按照 VMware 知识库 (KB) 文章 2130798 [在 Horizon 6 版本 6.2 和更高版本以及 Horizon Client 3.5 和更高版本中为 PCoIP 配置安全协议](#)中的说明为这些服务器上的 PCoIP 连接启用 TLSv1.0。
- 有关 Horizon Agent 支持的 Linux 客户端操作系统，请参阅《设置 Horizon 7 for Linux 桌面》文档中的[Horizon 7 for Linux 的系统要求](#)。
- 有关连接服务器、安全服务器和 View Composer 支持的操作系统，请参阅《Horizon 7 安装指南》文档中的[服务器组件的系统要求](#)。
- 该版本提供了一组更新的 Horizon Client，因此 Horizon 7 功能得到了增强。例如，VMware Blast Extreme 连接需要使用 Horizon Client 4.0 或更高版本。请参阅 [VMware Horizon Client 文档](#)页面以了解有关支持的

Horizon Client 的信息。

- 即时克隆功能需要使用 vSphere 6.0 Update 1 或更高版本。
- 即时克隆适用于 Windows 7 和 Windows 10，但不适用于 Windows 8 或 Windows 8.1。
- 请参阅 [VMware 产品互操作性列表](#) 以了解 Horizon 7 与当前和以前的 vSphere 版本的兼容性信息。
- 有关受支持的 Active Directory 域服务 (AD DS) 域功能级别，请参阅《Horizon 7 安装指南》文档中的[准备 Active Directory](#)。
- 有关详细的系统要求（如 Horizon Administrator 支持的浏览器），请参阅《Horizon 7 安装指南》文档。
- 根据 RFC 7465 “禁止使用 RC4 密码套件”、RFC 7568 “不再支持安全套接字层 3.0 版”、PCI-DSS 3.1 “支付卡行业 (PCI) 数据安全标准”和 SP800-52r1 “选择、配置和使用传输层安全 (TLS) 实施的准则”，将在 Horizon 7 组件中默认禁用 RC4、SSLv3 和 TLSv1.0。如果您需要在连接服务器、安全服务器、View Composer 或 Horizon Agent 计算机上重新启用 RC4、SSLv3 或 TLSv1.0，请参阅《Horizon 7 安全指南》文档中的[在 View 中禁用的旧协议和密码](#)。
- 如果已为 PCoIP 连接部署了 PCoIP 安全网关 (PSG)，零客户端的固件必须为 4.0 或更高版本。
- 在使用客户端驱动器重定向 (Client Drive Redirection, CDR) 时，请部署 Horizon Client 3.5 或更高版本和 View Agent 6.2 或更高版本，以确保将 CDR 数据通过加密的虚拟通道从外部客户端设备发送到 PCoIP 安全服务器以及从安全服务器发送到远程桌面。如果部署以前版本的 Horizon Client 或 Horizon Agent，将加密到 PCoIP 安全服务器的外部连接，但在企业网络中以未加密的形式将数据从安全服务器发送到远程桌面。您可以通过在 Active Directory 中配置 Microsoft 远程桌面服务组策略设置来禁用 CDR。有关详细信息，请参阅《在 Horizon 7 中配置远程桌面功能》文档中的[管理对客户端驱动器重定向的访问](#)。
- 默认情况下，将取消选中 Horizon Agent 安装程序中的“USB 重定向”安装选项。您必须选择此选项才会安装 USB 重定向功能。有关安全地使用 USB 重定向的说明信息，请参阅《Horizon 7 安全指南》文档中的[在安全的 View 环境中部署 USB 设备](#)。
- 全局策略多媒体重定向 (MMR) 默认为拒绝。要使用 MMR，您必须打开 Horizon Administrator，编辑“全局策略”并将该值明确设置为允许。要控制对 MMR 的访问，可以全局启用或禁用多媒体重定向 (MMR) 策略，也可以针对单独池或用户启用或禁用该策略。多媒体重定向 (MMR) 数据在不采用应用程序加密的情况下跨网络传输，其中可能包含敏感数据，具体取决于被重定向的内容。为确保无法在网络上监视此数据，请仅在安全网络中使用 MMR。
- 在 Horizon Administrator 中设置透明页面共享 (TPS) 级别之前，VMware 建议您了解安全影响。有关指导说明，请参阅 VMware 知识库 (KB) 文章 2080735 [安全注意事项和禁用虚拟机之间的透明页面共享](#)。
- 要在 vSphere 5.5 或更高版本的环境中使用 View Storage Accelerator，桌面虚拟机的大小不能超过 512 GB。在大于 512 GB 的虚拟机上，View Storage Accelerator 将被禁用。虚拟机大小由 VMDK 总容量定义。例如，一个 VMDK 文件大小可以为 512 GB，或一组 VMDK 文件的总大小为 512 GB。此要求同样适用于在早期版本的 vSphere 中创建并后期升级到 vSphere 5.5 的虚拟机。
- Horizon 7 不支持 vSphere Flash Read Cache（之前称为 vFlash）。
- 在 Horizon（包含 View）6.0 和更高版本中，不再支持 View PowerCLI cmdlet Get-TerminalServer、Add-TerminalServerPool 和 Update-TerminalServerPool。
- 默认情况下，将在通过 vSphere 6.0 和更高版本创建的虚拟机中禁用屏幕 DMA。View 要求启用屏幕 DMA。如果禁用了屏幕 DMA，在连接到远程桌面时，用户将会看到黑屏。在 Horizon 7 置备桌面池时，将自动为池中的所有 vCenter Server 管理的虚拟机启用屏幕 DMA。不过，如果在虚拟机中以未管理模式安装 Horizon Agent (VDM_VC_MANAGED_AGENT=0)，则不会启用屏幕 DMA。有关手动启用屏幕 DMA 的信息，请参阅 VMware 知识库 (KB) 文章 2144475 [在虚拟机中手动启用屏幕 DMA](#)。
- vSphere 2016 及更高版本支持启用 vGPU 的即时克隆桌面池。
- Microsoft Windows Server 要求在 Horizon 7 环境中的所有连接服务器之间打开一系列动态端口。Microsoft Windows 需要使用这些端口来执行常规的远程过程调用 (RPC) 和 Active Directory 复制操作。有关动态端口范围的更多信息，请参阅 Microsoft Windows Server 文档。
- 在 Horizon 7 版本 7.2 或更高版本中，viewDBChk 工具将无法访问 vCenter 或 View Composer 凭据，并且将在必要时提示这一信息。
- 在此版本中，更改了连接服务器实例和安全服务器接收的 HTTP 请求的转发规则。如果已在 locked.properties 中定义 frontMapping 自定义条目，应在升级前将这些条目移除。如果您希望禁止管理员连接到特定连接服务器实例，则可以不定义 frontMapping 自定义条目，而是将以下条目添加到 locked.properties 中：

```
frontServiceWhitelist =  
tunnel|ajp:broker|ajp:portal|ajp:misc|moved:*|file:docroot
```

在安全服务器上，将会自动应用此条目，无需在 `locked.properties` 中对其进行设置。

- Horizon Persona Management 与使用“UIA + 配置文件”模板创建的用户可写卷不兼容。
- 在 Horizon 7 版本 7.0.3 或更高版本中，内部验证检查确定即时克隆和内部模板是否具有有效的 IP 地址和网络连接。如果虚拟机具有无法在置备期间分配 IP 地址的网卡，即时克隆置备将失败。
- 要了解 Horizon 7 支持的 NVIDIA GPU 卡型号，请参阅 <https://docs.nvidia.com/grid/9.0/product-support-matrix/index.html>。
- 支持 AMD v340 显卡。
- IPv6 环境支持实时音频-视频 (RTAV)。
- 有关 Horizon 7 与最新版本的 VMware Unified Access Gateway、VMware Identity Manager、VMware App Volumes、VMware User Environment Manager 和 VMware Tools 的兼容性信息，请参阅 [VMware 产品互操作性列表](#)。
- JMP Server 支持 VMware App Volumes 2.14 或更高版本，但不支持 App Volumes 4.0。要使用 JMP Server，必须安装 2.14 或更高版本的 App Volumes 2.xx。
- 在 VMware Cloud on AWS 上，由于逻辑交换机上存在 NSX-t 限制，因此即时克隆桌面池和包含完整虚拟机的桌面池仅限于 1000 个桌面。
- 在 IPv6 环境中，RDSH 即时克隆池不支持 PCoIP。在 IPv6 环境中，远程桌面支持 PCoIP。
- 从版本 18.2.7 开始，Avi 网络 (VMware NSX Advanced Load Balancer) 支持连接服务器、Unified Access Gateway 设备和 App Volumes Manager 的负载均衡。

支持的 Windows 10 操作系统

有关支持的 Windows 10 操作系统的更新列表，请参阅 VMware 知识库 (KB) 文章 2149393 [在 Horizon 7 上支持的 Windows 10 版本](#)。

有关 Windows 10 操作系统的升级要求的详细信息，请参阅此处的 VMware 知识库 (KB) 文章 2148176 [Windows 10 操作系统的升级要求](#)。

支持 Red Hat Enterprise Linux Workstation

Horizon Agent for Linux 支持安装在运行 Red Hat Enterprise Linux Workstation 的系统上。不支持 Red Hat Enterprise Linux Server。

设置 [Horizon 7 for Linux 桌面](#) 文档中出现的所有“Red Hat Enterprise Linux”和“RHEL”都仅指 Red Hat Enterprise Linux Workstation。

有关支持的 Red Hat Enterprise Linux Workstation 版本的列表，请参阅 [Horizon 7 for Linux 的系统要求](#)。

Horizon 7 的早期版本

以前版本的发行说明介绍了各个版本中引入的功能以及现有的已知问题。

已解决的问题

- 1864296：如果您最初使用用户名和密码登录，并尝试使用智能卡身份验证以递归方式进行解锁，以登录到启用了组策略设置“解锁客户端计算机后解锁远程会话”的本地计算机，然后在 Horizon Client 中使用“以当前用户身份登录”，将显示 GSSAPI_ERROR 消息。
- 2260206：Windows 虚拟机未关闭，因为不存在对用户配置的驱动程序卸载回调调用。
- 2344754：由于拒绝权限，用户配置管理同步将在每个复制间隔时间内失败一次。

- 2373674：当用户登录到启用了 Deep Security 的远程桌面时，该计算机会在用户配置复制大型文件时挂起。
- 2414242：启用了 Deep Security 后，无法删除从文件共享复制到本地磁盘的文件。
- 2403057：将用户配置与 Deep Security 组合使用时，会出现 BSOD REGISTRY_FILTER_DRIVER_EXCEPTION (135)。
- 2373808：安装 Adobe Acrobat 阅读器时，启用了用户配置的 Windows 计算机会崩溃，并出现 BSOD (bugcheck 3B)。
- 2403061：对于日语字处理器 Ichitaro 编写的文档，无法正确同步用户配置文件。
- 2292092：当桌面处于注销过程中时，已注销的用户可以登录到同一桌面。
- 2412281：使用 Blast 或 PCoIP 连接到 Windows 2016 发布的桌面时，用户无法保存“使用桌面语言栏 (如果可用)”设置。

已知问题

已知问题可归为以下几类。

- [Horizon Persona Management](#)
- [View Composer](#)
- [Horizon Connection Server](#)
- [Horizon Agent for Linux](#)
- [Horizon Agent](#)
- [Horizon GPO 包](#)
- [Horizon Client](#)
- [Horizon JMP Server 和 JMP Integrated Workflow](#)
- [Horizon Cloud Connector](#)

Horizon Persona Management

- 在每次登录后，用户配置管理需要很长时间来复制使用“v6”用户配置文件版本的客户机操作系统上的第一个用户配置。
- **当您使用个人配置文件登录 Windows 10 LTSC 计算机并尝试通过“快速访问”来访问重定向的文件夹(例如“下载”或“我的文档”)时，会出现以下错误：**

C:\Users\vduser7\Downloads 不可用。Microsoft 未提供用于将文件夹或文件添加到“快速访问”的 API (C:\Users\vduser7\Downloads is unavailable. Microsoft doesn't provide the API to add folder or file to Quick Access)。

解决办法：无

- 您第二次登录配置了用户配置管理功能的虚拟机时，Microsoft Edge 浏览器会崩溃，并会显示一条错误消息，说明从未使用过 OneDrive 应用程序。此外，也无法正确复制相应的文件和文件夹。Windows 10 内部版本 1703 和更高版本中会出现此问题。
解决办法：禁用用户配置管理设置漫游本地设置文件夹。禁用此设置后，Microsoft Edge 浏览器正常工作，但 OneDrive 应用程序仅在第一次登录时可用。
- 在启用了 Horizon Persona Management 设置的 Windows Server 2012 虚拟机上不显示文件的脱机图标。
解决办法：尚未找到任何解决办法。
- 初次成功登录到虚拟机后，如果 Horizon Agent 安装在 Windows 10 版本 1703 CBB 上并且已启用用户配置管理，则会在后续登录尝试时显示消息“OneDrive - 无效的映像错误 (OneDrive -Bad Image error)”。

解决办法： 在 Windows 10 版本 1703 CBB 系统上，请勿使用 OneDrive。在组策略管理编辑器中，禁用计算机配置 > 策略 > 管理模板 > VMware View Agent 配置 > 用户配置管理 > 漫游和同步文件夹中的“漫游本地设置文件夹”设置。

View Composer

- 在装有最新 Windows 更新的 Windows Server 2016 上从命令行运行 View Composer 安装程序时，出现 Microsoft .NET 4.6 Framework 错误。出现此问题是因为，CLI 安装程序不能识别最新版本的 Microsoft .NET 4.7。
解决办法： 使用 View Composer 安装程序用户界面运行安装程序。
- 在 Windows 10 操作系统的父虚拟机从内部版本 1511 升级至内部版本 1607 后，创建或重构桌面池失败。内部版本 1607 是指 Windows 10 Anniversary Update 操作系统。
解决办法：
 - 方法 1：在父虚拟机上执行 Windows 10 内部版本 1607 的全新安装。
 - 方法 2：不要在桌面池创建向导中选择“重定向一次性文件”。
- 运行以下命令时与 View Composer 连接失败：viewdbchk.cmd -findMachine
解决办法： 将 View Composer 的自签名证书导入到连接服务器的密钥库或使用自定义 CA 证书。
- 由于最近对 vSphere 6.7 中客户机自定义实用程序进行了更改，因此在 Horizon 7 到版本 7.5 的升级过程中，无法在早期版本的 Horizon Agent 上使用 View Composer 7.5 来通过 Sysprep 自定义方法置备及重构链接克隆池。在置备或重构操作期间，链接克隆桌面和场无限期地停滞在自定义状态。
解决办法： 在父虚拟机上升级到最新版本的 VMware Tools，并将 Horizon Agent 升级到版本 7.5，然后对升级的父虚拟机拍摄快照。随后，在 vSphere 6.7 中使用 Sysprep 自定义方法置备或重构链接克隆桌面池。
- 对于 Win2k12 Standard 和 Datacenter 版本，链接克隆停滞在自定义状态。
解决办法： 有关如何修复此问题的更多信息，请参阅 VMware 知识库文章 <https://kb.vmware.com/s/article/57348>。

Horizon Connection Server

- 在置备即时克隆桌面池期间，如果在数据存储上没有足够的可用空间，将在 Horizon Administrator 中显示“克隆虚拟机 <虚拟机名称> 失败 - VC_FAULT_FATAL：无法将交换文件从 0 KB 扩展到 2097152 KB (Cloning of VM <VM name> has failed - VC_FAULT_FATAL: Failed to extend swap file from 0 KB to 2097152 KB)”错误消息。该消息未明确指出问题的根本原因。
解决办法： 不需要。
- 在 Horizon Administrator 中，如果转到目录 > 桌面池，双击一个即时克隆桌面池，转到清单选项卡，然后单击计算机 (即时克隆详细信息)，窗口将显示即时克隆详细信息。不过，操作系统磁盘数据存储列不显示任何信息。
解决办法： 无
- 在大规模环境中，即时克隆桌面池中的某些桌面可能会进入“无效 IP”状态。
解决办法： 在 Horizon Administrator 中，转到池清单，选择处于无效 IP 状态的桌面，然后单击恢复。
- 从 vCenter Server 或 Windows 操作系统菜单中重新启动或重置在桌面池中具有最终用户会话的虚拟机时，将重新启动虚拟机，但虚拟机可能在 Horizon Administrator 中显示“已使用”状态。
以下池类型可能会出现该问题：
 - 即时克隆桌面池。
 - 启用了“注销时删除”的链接克隆浮动桌面池。
 - 启用了“注销时刷新”的链接克隆浮动桌面池。
 - 启用了“注销时删除”的完整克隆浮动桌面池。**解决办法：** 使用 Horizon Administrator 或 Horizon Client 重新启动或重置即时克隆桌面池中的虚拟机。如果虚拟机已处于“已使用”状态，请移除虚拟机。该操作根据池置备设置自动创建新的虚拟机。
- 如果在本地数据存储上置备即时克隆，则无法将相应的主机置于维护模式。出现该问题是因为，内部虚拟机和即时克隆存储在本地数据存储上，因此无法进行迁移。
解决办法： 删除即时克隆桌面池。这将删除相关的虚拟机，并使相应的主机进入维护模式。

- 如果已打开电源的主机上存在即时克隆父虚拟机，则使用 VUM 的 ESXi 主机修复会失败。
解决办法： 有关详细信息，请参阅 VMware 知识库 (KB) 文章 2144808 [使具有 Horizon 即时克隆的 ESXi 主机进入和退出维护模式](#)。
- 在 Windows Server 2016 和 Windows Server 2019 RDS 主机上不支持将通用 Windows 平台 (UWP) 应用程序用作已发布的应用程序。
- 对于 True SSO，仅在用于访问 Horizon Administrator 的连接服务器的系统运行状况仪表板上显示连接服务器实例和注册服务器之间的连接状态。例如，如果在 Horizon Administrator 中使用 `https://server1.example.com/admin`，则仅为 `server1.example.com` 连接服务器收集注册服务器的连接状态。您可能会看到下面的一条或两条消息：
 - **无法连接到主注册服务器以管理该连接服务器上的会话** (The primary enrollment server cannot be contacted to manage sessions on this connection server)。
 - **无法连接到辅助注册服务器以管理该连接服务器上的会话** (The secondary enrollment server cannot be contacted to manage sessions on this connection server)。
 必须将一个注册服务器配置为主注册服务器。配置辅助注册服务器是可选的。如果只有一个注册服务器，则只会看到第一条消息（出错时）。如果具有主要和辅助注册服务器，并且两个服务器都出现了连接问题，则会看到两条消息。
- 如果在具有 CA 和 SubCA 的环境中设置 True SSO 并为 CA 和 SubCA 设置了不同的模板，则允许组合使用一个 CA 或 SubCA 中的模板和另一个 CA 或 SubCA 中的模板来配置 True SSO。因此，仪表板可能会将 True SSO 状态显示为绿色。不过，在尝试使用 True SSO 时，将会失败。
- 在 Horizon Help Desk Tool 中，如果会话为本地会话或在本地容器中运行的会话，则不会显示容器名称。
解决办法： 设置 Cloud Pod 架构环境以在 Horizon Help Desk Tool 中查看容器名称。
- Workspace ONE 中的副本服务器未反映 Workspace ONE 模式设置。
解决办法： 在连接服务器中配置 Workspace ONE 模式。
- 在创建完整克隆桌面池时，由于缓存问题，有时会显示错误的模板并隐藏有效的模板。
解决办法： 重新启动连接服务器。
- 尝试在 Horizon Administrator 中添加 SAML 身份验证器时，在“管理 SAML 身份验证器”页中禁用添加按钮。
解决办法： 以具有管理员或本地管理员角色的用户身份登录到 Horizon Administrator。
- 在 Cloud Pod 架构环境中，在 Horizon Administrator 的 **清单 > 搜索会话** 中不显示从全局应用程序授权中预启动的应用程序会话。
解决办法： 登录到托管容器中的连接服务器实例的 Horizon Administrator 用户界面，然后选择 **监控 > 事件** 以查看预启动的会话信息。
- 对于分配有 20 到 50 个 Cloud Pod 架构全局应用程序授权的用户，无论通过任何 Horizon Client 版本连接，在对 Horizon 7 进行身份验证时，均存在 20 到 30 秒的延迟。
注意： 在 Horizon 7 版本 7.2，此连接时间略有改善。
解决办法： 无。
- 对于 Intel vDGA，仅支持 Haswell 和 Broadwell 系列的 Intel 集成 GPU。仅在 vSphere 6 Update 1b 和更高版本上支持 Broadwell 集成 GPU。在 vSphere 5.5 和更高版本上支持 Haswell 集成 GPU。必须在 BIOS 中启用此 GPU，然后 ESXi 才能识别该 GPU。有关详细信息，请参阅特定 ESXi 主机的文档。Intel 建议将 BIOS 中的图形内存设置设为默认值。如果选择更改这些设置，请将光圈设置保留默认值 (256M)。
- 根据配置为使用 NVIDIA GRID vGPU 的 View Composer 桌面池置备虚拟机失败，并出现以下错误：“父资源池中的可用图形资源数量不足，无法执行该操作 (The amount of graphics resource available in the parent resource pool is insufficient for the operation)。”
解决办法： 对集群中所有配置为 3D 渲染的虚拟桌面使用一个 vGPU 配置文件。
- 对于 vCenter Server 6.0 U3 或更高版本（包括 vCenter Server 6.5），出现故障时内部父虚拟机会迁移到另一台主机。此迁移会导致出现问题，因为目标主机驻留多余的父虚拟机。
解决办法： 手动移除这些父虚拟机。有关详细信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档。

- 为了降低可能会出现内存耗尽的情况，帧缓冲区为 512 MB 或低于 512 MB 的 vGPU 配置文件在 Windows 10 客户机操作系统上仅支持一个虚拟显示器。

以下 vGPU 配置文件的帧缓冲区等于或少于 512 MB：

- Tesla M6-0B、M6-0Q
- Tesla M10-0B、M10-0Q
- Tesla M60-0B、M60-0Q
- GRID K100、K120Q
- GRID K200、K220Q

解决办法：使用支持多个虚拟显示器且至少具有 1 GB 帧缓冲区的配置文件。

- 对于已发布的桌面和应用程序池，如果已启用客户端限制功能，且有权访问配置单向 AD 信任的域，将无法启动。

解决办法：无

- 升级后，如果您拥有具备“管理场以及桌面和应用程序池”特权（特定于对象的特权）的角色，则用于添加场的选项将显示为灰色。

解决办法：编辑角色，或将角色重新创建为具备“管理场以及桌面和应用程序池”特权，这也会添加“管理全局配置和策略”特权。

- 升级后，Workspace ONE 中不显示书签。

解决办法：重新从 Workspace ONE 的目录中添加书签。

- 断开连接网络电缆再重新连接，然后单击客户端计算机上的“断开并注销”，远程桌面不会断开连接并注销。

解决办法：手动关闭远程桌面窗口，并从远程会话断开连接。

- 在 Horizon Administrator 中，在对包含完整虚拟机的自动池进行克隆时，“即将完成”步骤不显示多个字段的值。但是，克隆操作依旧成功。

解决办法：无。

- 在使用 Sysprep 自定义方法创建链接克隆和完整克隆时，自定义和域加入有时候在 Windows 10 客户机操作系统上失败。

解决办法：这是因 Microsoft Windows 问题所致。要解决此问题，请按照以下 Microsoft 知识库 (KB) 文章中的步骤操作：<https://support.microsoft.com/en-us/help/2769827>。

- 如果没有配置 Horizon 7 许可证，无法在 Horizon Console 中创建链接克隆桌面池或场。

解决办法：使用 Horizon Administrator 可在没有 Horizon 7 许可证的情况下创建链接克隆桌面池或场。

- 从 Internet Explorer 浏览器中登录到 Horizon Console 时，仅显示关键字，而不显示图标。在使用 IP 地址而不是 DNS 名称连接到连接服务器或安全服务器时，将会出现该问题。

解决办法：在连接时，请使用 DNS 名称而不是 IP 地址。有关详细信息，请参阅 VMware 知识库 (KB) 文章 <https://kb.vmware.com/s/article/2150307>。

- 在将 Safari 10.1.1 版作为 Web 浏览器并使用完全限定域名登录到 Horizon Console 时，可能会出现一些用户界面问题，例如，底部面板空白。

解决办法：Safari 10.1.1 版是 Horizon Console 不支持的 Web 浏览器版本。请使用早于 10.1.1 的 Safari 版本或 11.0.2 和更高版本登录到 Horizon Console。

- 对于 Cloud Pod 架构部署中的全局 Linux 会话，在 Horizon Help Desk Tool 中出现以下用户界面问题：

- 在“详细信息”选项卡上单击会话详细信息时，显示“发生内部错误” (An internal error occurred) 消息，不显示 Skype for Business 状态并且操作系统版本显示为“-”。
- 在单击“远程协助”时，显示“未能获取远程协助票证” (failed to get Remote Assistance ticket) 消息。

- 在单击“应用程序”选项卡时，显示“发生内部错误” (An internal error occurred) 消息。

解决办法：无。对于 Linux 桌面，Horizon 技术支持工具不支持以下用户界面功能：Skype for Business 状态、远程协助、“应用程序”选项卡以及会话空闲状态。

- 在将 VMFS6 与自动 UNMAP 功能一起使用的 vSphere 6.7 版上，Horizon Administrator 不会更新 vCenter Server 空间回收信息。
解决办法：无。
- 在升级到 Horizon 7 版本 7.5 后，仅安装的第一个连接服务器可以连接到注册服务器。
解决办法：停止 Horizon Connection Server 服务，从 VMware Horizon View 证书存储区中移除具有友好名称“vdm.ec”的证书，然后重新启动 Horizon Connection Server 服务。
- 如果在 Horizon Console 的“已超时”选项卡中访问 Horizon Administrator，然后从 Horizon Administrator 中单击 Horizon Console 链接，单点登录无法正常工作。
解决办法：在浏览器中清除网站数据并重新启动浏览器。
- 如果在 Firefox、Google Chrome、Microsoft Edge、Firefox 或 Safari Web 浏览器中使用 IP 地址登录到 Horizon Console，则登录 Horizon Console 将失败。
解决办法：使用完全限定域名 (FQDN) 登录到 Horizon Console。有关使用 FQDN 登录到 Web 应用程序的详细信息，请参阅《Horizon 7 安全指南》文档。
- 在“用户和组”页的用户名列中，Horizon Administrator 为以下用户显示空/空：Account Operators、Incoming Forest Trust Builders、Terminal Server License Servers、Windows Authorization Access Group、Server Operators 和 Pre-Windows 2000 Compatible Access。
解决办法：无。
- 在升级到 vSphere 6.7 后，您无法使用通过早于 6.7 的 vSphere 版本创建的自定义规范。
解决办法：在升级到 vSphere 6.7 后，创建新的自定义规范并使用该规范进行池置备。
- Horizon Help Desk Tool 显示代理容器和托管容器的登录时间，但不显示代理容器和托管容器以外的容器的登录时间。如果代理容器是远程容器，Horizon Help Desk Tool 在几分钟后显示托管容器的登录时间。
解决办法：如果 Horizon Help Desk Tool 不显示托管容器的登录时间，请关闭显示会话详细信息的页面，等待 7-8 分钟，然后导航到“详细信息”选项卡以再次查看会话详细信息。
- VMware Identity Manager 有时无法启动桌面。如果首次在 VMware Identity Manager 中保存 SAML 配置详细信息并在连接服务器上启用了 SAML，则无法启动桌面。
解决办法：再次保存配置文件，并在新的配置文件上执行同步操作。可以每小时或每天执行一次同步操作，具体时间由管理员设置。
- 在尝试将表的内容导出为 CSV 时，处于隐身模式的 Chrome 上的 Horizon Administrator 显示错误：无法导出文件，因为当前已打开具有相同名称的文件。关闭该文件重试或使用其他文件名。(The file cannot be exported because a file of the same name is currently open. Close the file and try again or use a different file name.)
解决办法：在正常模式下使用 Chrome 上的 Horizon Administrator 导出该表。
- 当您在 vCenter Server 6.7 上使用 Sysprep 自定义 Windows 10 链接克隆时，在置备或重构操作期间，链接克隆桌面无限期停滞在自定义状态。
解决办法：使用 vCenter Server 6.5 U2 或更低版本。如果您必须使用 vCenter Server 6.7，则使用 Quickprep 自定义方法。
- 在 Horizon Administrator 中，您可以将远程访问用户添加为未验证访问用户。但是，未验证访问用户无法从外部网关获取远程访问权限。用户将无法访问虚拟桌面，并且只能以未验证访问用户的身份启动应用程序。如果用户尝试使用正常访问登录，将显示“请求了错误的身份验证类型” (Incorrect authentication type requested) 错误消息。
解决办法：无。

- 当信任身份验证设置的范围设为“选择性身份验证”时，Horizon 单点登录失败。

解决办法：利用以下解决办法之一来解决此问题。

- 使用域范围的身份验证。
- 继续使用“选择性身份验证”安全设置，但在位于信任域或林中的计算机对象（资源计算机）的所有域控制器上，为每个 Horizon Connection Server 主机（本地系统）帐户明确授予“允许身份验证”权限。有关如何授予“允许身份验证”权限的信息，请参阅 Microsoft 文章“在信任域或林中的计算机上授予‘允许身份验证’权限”。
- 对于 Cloud Pod 架构功能，在某些情况下，RDS 许可服务器向混合模式许可环境中的同一客户端颁发多个永久许可证。

解决办法：无。这是一个第三方问题，这个问题符合 Microsoft RDS License Server 颁发许可证的方式，即使没有安装 Horizon 7 也会出现此问题。

- 在 Horizon Administrator 中，对链接克隆池或自动池进行克隆时，如果池中包含在 vSAN 数据存储上创建的完整虚拟机，则“存储优化”步骤中“使用 VMware Virtual vSAN”选项不会显示为“已选中”。但是，克隆操作依旧成功。

解决办法：无。

- 在编辑包含完整虚拟机的自动桌面池时，如果浏览数据存储，则会出现以下问题：

- 在“vCenter 设置”选项卡中，单击“浏览数据存储”，将显示推荐的最小 GB 值。
- 在“置备设置”选项卡中，增加计算机的最大数量，然后选择“vCenter 设置”选项卡并单击“浏览数据存储”。推荐的最小 GB 值有所增加，但会添加到现有值中。
- 对于包含三台计算机的桌面池（其中一台可用，而另一台仍处于自定义或置备阶段），编辑该桌面池，然后选择“vCenter 设置”选项卡并单击“浏览数据存储”。将显示所有三台计算机的推荐的最小 GB 值。

解决办法：在编辑包含完整虚拟机的自动桌面池时，使用 Horizon Administrator 浏览数据存储，以查看正确的推荐的最小 GB 存储值。

- 如果您在编辑即时克隆桌面池时浏览数据存储，则会出现以下问题：

- 在即时克隆桌面池中的所有计算机都处于可用状态后，编辑该桌面池，并在“vCenter 设置”选项卡中单击“浏览数据存储”。“推荐的最小值 (GB)”、“推荐的最大值 (GB)”和“50% 使用率”值均具有正值。
- 在即时克隆桌面池中的所有计算机都处于可用状态后，编辑该桌面池，在“置备设置”选项卡中增加计算机的最大数量，然后在“vCenter 设置”选项卡中单击“浏览数据存储”。“推荐的最小值 (GB)”、“推荐的最大值 (GB)”和“50% 使用率”值均有所增加，但会添加到现有值中。
- 对于包含三台计算机的桌面池（其中一台可用，而另一台仍处于自定义或置备阶段），编辑该桌面池，然后选择“vCenter 设置”选项卡并单击“浏览数据存储”。显示所有三台计算机的“推荐的最小值 (GB)”、“推荐的最大值 (GB)”和“50% 使用率”值。

解决办法：在编辑即时克隆桌面池时，使用 Horizon Administrator 浏览数据存储，以查看正确的“推荐的最小值 (GB)”、“推荐的最大值 (GB)”和“50% 使用率”值。

- 当您创建包含完整虚拟机的自动桌面池然后进行编辑时，如果该池拥有两个或以上名称，并且“保持打开电源状态的未分配计算机的数量”值小于指定的实际名称数，则“保持打开电源状态的未分配计算机的数量”字段不接受与池创建过程中指定的名称总数相等的值，并显示不正确的错误消息。

解决办法：使用 Horizon Administrator 编辑包含完整虚拟机并拥有两个或以上名称的自动桌面池，以正确更新“保持打开电源状态的未分配计算机的数量”字段值。

- 对于大多数浏览器，如果未进行额外的配置，尝试使用 IP 地址或 CNAME 连接到 HTML Access 门户或其中一个管理控制台会失败。其中大多数情况会报告错误，但有时会显示一则空白的错误消息。

解决办法：要解决此问题，请参阅《Horizon 7 安全指南》文档中的“来源检查”。

- 配置 Skype for Business 时，有一项可选功能可以启用媒体绕过，从而绕过中介服务器。对于针对 PSTN 用户的 Skype for Business 呼入/呼出优化通话，无论是否启用媒体绕过，媒体都将始终通过中介服务器进行路由。

解决办法：无。适用于 Skype for Business 的 Virtualization Pack 不支持媒体绕过。请参阅 <https://kb.vmware.com/s/article/56977>

- 如果同一用户同时位于两个需要在 Cloud Pod 架构环境中进行配对的连接服务器容器中，Horizon Administrator 将“源容器”的值显示为 2，指示该用户来源于两个容器。虽然管理员可以从两个容器编辑用户，但这样做可能会导致在混合登录时用户配置不一致。此外，无法为该用户禁用混合登录。
解决办法：您必须从这两个容器中删除此用户，然后重新创建该用户，并为其配置混合登录。
- 在 Horizon Administrator 中，不会为从 vCenter Server 启动的远程会话禁用“注销会话”和“断开会话”按钮。
解决办法：对于从 vCenter Server 启动的远程会话，使用 Horizon Console 可获得禁用“注销会话”和“断开会话”按钮的功能。但是，当您导航到“清单”>“桌面”，选择桌面池并单击“计算机”选项卡、“计算机 (即时克隆详细信息)”选项卡或“计算机 (View Composer 详细信息)”选项卡时，这种方法不起作用。
- 在嵌套 ESXi 或嵌套虚拟 ESXi 上添加虚拟卷数据存储时生成核心转储错误消息。
解决办法：无。
- 浏览 vSAN 数据存储以导入永久磁盘时，Horizon Administrator 和 Horizon Console 都显示内部文件夹名称而不是实际文件夹名称。
解决办法：无。
- 在 Horizon Administrator 和 Horizon Console 中，拥有“管理技术支持门户 (只读)”特权的自定义角色显示为可应用于访问组。
解决办法：无。
- 具有“管理员 (只读)”角色的用户在 Horizon Administrator 中看不到 View 配置 > Cloud Pod 架构。
解决办法：使用 Horizon Console。
- 在 Horizon Administrator 中，当添加或编辑使用 vSAN 数据存储的链接克隆场时，“中断时间”会被禁用。
解决办法：使用 Horizon Console 为使用 vSAN 数据存储的链接克隆场设置中断时间。
- 在 Horizon Administrator 中，如果自动桌面池包含完整的虚拟机，则其计算机摘要中的“重建”按钮不起作用。
解决办法：在 Horizon Administrator 中，使用“计算机”>“vCenter Server”中的重建功能。
- 使用现有的 PowerShell 脚本向连接服务器添加 vCenter Server 时，显示以下错误消息：未能添加 VC 实例：没有枚举常量 com.vmware.vdi.commonutils.Thumbprint.Algorithm.SHA-1 (Failed to add vc instance: No enum constant com.vmware.vdi.commonutils.Thumbprint.Algorithm.SHA-1)。出现此问题的原因是，在 Horizon 7 版本 7.8 中添加了 certificateEncoding 属性，该属性指示自签名证书的证书覆盖。因此，具有错误值 SHA-1 的早期版本的 VMware PowerCLI 脚本会失败。
解决办法：更新 PowerShell 脚本以使用属性值 DER_BASE64_PEM，而不是 SHA-1。例如，设置 `$certificate_override.sslCertThumbprintAlgorithm = 'DER_BASE64_PEM'`。
- 升级通用 Windows 平台 (UWP) 应用程序后，包含版本的路径会发生更改，无法通过原始路径访问该应用程序。该应用程序的状态在 Horizon Administrator 中为不可用，并且用户无法启动该应用程序。
解决办法：升级后，在 Horizon Administrator 中更新应用程序路径，并确认应用程序状态为可用。或者，不要升级应用程序。
- 为客户端驱动器重定向功能配置设备筛选后，当用户使用 RDP 显示协议进行连接时，设备筛选无法正常使用。
解决办法：为客户端驱动器重定向配置设备筛选后，配置连接服务器以便禁止 RDP 连接。

- True SSO 桌面解锁功能在 PCoIP 和 Blast 协议中受支持，但在远程桌面协议 (RDP) 中不受支持。

- 在 Horizon Console 中，用户或组摘要在以下情况下由于域信任问题而无法加载：
 - 用户和组属于单向信任域，且已登录的管理员拥有单向信任域中的必需权限。
 - 用户和组属于双向信任域，且已登录的管理员拥有双向信任域中的必需权限。
 - 用户和组属于单向或双向信任域，且已登录的管理员来自子域并拥有必需的权限。

解决办法：使用 Horizon Administrator 访问用户或组摘要。

- 在 Horizon Console 中，由于连接服务器时间未按照连接服务器时区正确设置，某些事件可能不会列出。

解决办法：使用 Horizon Administrator 查看所有事件。

- 可以恢复具有活动会话的即时克隆虚拟机。此问题在 Horizon Administrator 和 Horizon Console 中均会出现。

解决办法：无。

- 在 Horizon Administrator 和 Horizon Console 中，在移除具有已分离的永久磁盘的 vCenter Server 后，Horizon Administrator 仍会显示该 vCenter Server 中的这些磁盘，但无法对这些磁盘进行操作。Horizon Console 不会显示任何已分离的磁盘，但会显示内部错误横幅。

解决办法：不存在已知的解决办法。在移除之前，先确认 vCenter Server 中没有已分离的磁盘。

- 在 Horizon Console 中，当创建手动桌面池时，如果“会话类型”选项为“应用程序”或“桌面和应用程序”，则不会更新“空会话超时 (仅限应用程序)”字段。

解决办法：编辑手动桌面池以更新“空会话超时 (仅限应用程序)”字段。

- 在 Horizon 7 中，不会列出也不支持通过在 vSphere Client for vSphere 7 中选择 Windows 2019 操作系统而创建的安装有 Windows 2019 的虚拟机。

解决办法：通过在 vSphere Client 中选择 Windows 2016 操作系统版本，在虚拟机上安装 Windows 2019。

- 当您在 VMware Cloud on AWS 控制台中更改分段名称时，如果为即时克隆桌面池或场选择了网络，则 Horizon Console 不会反映端口组或分段的新名称。

解决办法：无。

- 通过 Horizon 7 Administrator 控制台图标或在浏览器地址栏中输入 `https://localhost/admin` 或 `https://localhost/newadmin` 启动 Horizon Administrator 时，您会被重定向到 `https://127.0.0.1/admin`。这种到 IP 地址的重定向可能会导致身份验证失败，如 VMware 知识库 (KB) 文章 2150307 中所述：[无法登录到 Horizon Administrator 或 Horizon Blue Desk Tool 之类的 VMware Web 应用程序](#)。

解决办法：要防止重定向到 IP 地址，可在浏览器的地址栏中输入 `https://localhost/admin/`（请确保将“/”附加到 URL 的末尾）。

Horizon Agent for Linux

本节介绍了 Horizon Agent for Linux 或配置 Linux 桌面时可能出现的问题。

- 有时，在连接到远程桌面并单击“协作”UI 图标后，可能不显示“协作”窗口。

解决办法：调整桌面窗口的大小，或重新连接到远程桌面。

- 在 vSphere 6.0 中，不支持在 RHEL 6.6 或 CentOS 6.6 虚拟机上配置四个分辨率为 2560x1600 的显示器。

解决办法：使用 2048x1536 分辨率，或在 vSphere 5.5 中部署此配置。

- 如果将键盘输入法系统设置为 `fcitx`，Linux 代理的键盘布局和区域设置与客户端不同步。

解决办法：将键盘输入法系统设置为 `iBus`。

- 在使用系统安全服务守护进程 (SSSD) 添加域时，单点登录 (SSO) 在 RHEL/CentOS 7.2 桌面上无法正常工作。
解决办法：在使用 SSSD 添加域后，使用 VMware 知识库文章 2150330 [在 RHEL/CentOS 7.2 桌面上使用 SSSD 加入 AD 时所需的 SSO 配置更改](#) 中的信息修改 `/etc/pam.d/password-auth` 文件。
- 如果使用智能卡重定向进行身份验证的客户端用户连接到 Ubuntu 18.04/16.04 或 SLED/SLES 12 SP3 桌面，并在输入 PIN 之前移除或重新插入智能卡，则桌面似乎无法识别所做的更改。
仅在用户关闭要求输入 PIN 的提示后，桌面才会检测到智能卡状态的更改。
解决办法：出现提示时，输入智能卡 PIN，然后单击“确定”。或者，单击“取消”以关闭提示而不输入 PIN。
- 当客户端用户连接到 Ubuntu 18.04/16.04 或 SLED/SLES 12 SP 3 桌面时，登录屏幕上显示“错误 2306: 无合适令牌可用” (Error 2306: No suitable token available)。
此错误消息指示智能卡已从客户端系统中移除。用户可以通过输入用户密码或重新插入智能卡来登录到桌面。
- 在 Ubuntu 16.04 上，如果管理员尝试通过在 `/etc/vmware/config` 配置文件中将 `WC.ScRedir.Enable` 设为“FALSE”来禁用智能卡重定向，则桌面将在登录屏幕上挂起。
- 在连接到 Ubuntu 16.04 桌面后，如果在进行智能卡身份验证时输入错误的 PIN，则客户端用户会看到登录提示，要求其输入用户密码，而不是智能卡 PIN。
客户端用户可以单击“确定”以关闭该用户密码提示。随即会显示一个新提示，要求用户输入智能卡 PIN。
- 在 Ubuntu 18.04/16.04 和 SLED/SLES 12 SP3 上，当用户从客户端系统中移除智能卡时，桌面屏幕保护程序不会按预期锁定。
默认情况下，即使在客户端用户移除用于进行身份验证以访问桌面的智能卡后，桌面屏幕保护程序也不会锁定。要在这些情况下锁定屏幕保护程序，必须在桌面上配置 `pkcs11_eventmgr`。
解决办法：配置 `pkcs11_eventmgr` 以指定在响应智能卡事件时的正确屏幕保护程序行为。
- 在 RHEL 7.0 桌面上安装启用了智能卡重定向（-m 参数设置为“是”）的 Horizon Agent 后，Horizon Administrator、Horizon Console 或 vSphere 可能显示黑屏。运行 RHEL 7.1 或更高版本的桌面支持智能卡重定向。RHEL 7.0 桌面不支持此功能。
解决办法：在运行 RHEL 7.1 或更高版本的桌面上安装启用了智能卡重定向的 Horizon Agent。
- 如果配置两个具有不同分辨率的显示器，并且主屏幕的分辨率低于辅助屏幕，则可能无法移动鼠标或将应用程序窗口拖到屏幕的某些区域。
解决办法：确保主显示器的分辨率至少与辅助显示器一样大。
- 如果在 RHEL 7 桌面上使用智能卡，并且启用在移除智能卡时锁定屏幕的选项，则在使用智能卡登录后，屏幕可能会立即锁定。这是 RHEL 7 的一个已知问题。
解决办法：要访问桌面，请在使用智能卡登录后解锁屏幕。

Horizon Agent

- 在 FIPS 模式下，如果将 Horizon Agent 安装到 C 驱动器以外的驱动器，Horizon Agent 无法与连接服务器配对使用并且池状态不可用。
解决办法：在 FIPS 模式下运行时，在 C 驱动器上安装 Horizon Agent。
- 在 Windows Server 2016 上卸载 Horizon Agent 时，显示有关正在使用应用程序的警告消息。
解决办法：使用 Windows 的“添加或删除程序”卸载 Horizon Agent 时，在出现的对话框中单击“忽略”。如果从命令行中卸载 Horizon Agent，请使用 `msiexec /x /qn {GUID of Agent}` 命令，而不是 `msiexec /x {GUID of Agent}` 命令。

- 在卸载 Horizon Agent 时，鼠标速度变得很慢并且出现抖动。在卸载 Horizon Agent 时，还会卸载 vmkbd.sys 驱动程序。
解决办法：在 Horizon Agent 虚拟机上修复 VMware Tools。
- 在 Windows 7 客户机操作系统上从 Horizon Agent 7.1 升级到 Horizon Agent 7.2 时，会出现一个“文件正在使用”对话框。该对话框说明 VMware Horizon Agent 应用程序正在使用需要由安装程序更新的文件。
解决办法：单击“忽略”以继续升级。
- 如果激活了“注销时刷新或删除”策略，则在配置文件管理完成用户数据同步之前，会刷新或删除桌面。
解决办法：无
- 安装 Windows 10 32 位 Horizon Agent 时引发“参数无效”异常，在单击“确定”后安装继续。出现此错误是因为打印后台处理程序服务被禁用。
解决办法：启用打印后台处理程序服务后，安装即可按预期进行。
- 如果会话所有者观看的视频在协作会话期间使用 MMR 进行了加速，协作者会看到黑屏，而不是视频。
解决办法：作为会话所有者，如果您需要在协作会话期间播放视频，请勿使用 Windows Media Player 或 Internet Explorer 播放视频，或者请在启用协作功能的池上禁用 MMR。
- 如果协作者加入多显示器会话，并在其客户端上启用了相对鼠标模式，则鼠标可能会移动到协作者看不到的辅助显示器中。
解决办法：将鼠标移回到屏幕上。或者，在多显示器会话中不使用相对鼠标模式。
- 如果您使用 Chrome 进行 URL 内容重定向，同时在筛选规则中将 https 协议设置了“*.google.*”，并在 Chrome 中将 Google 设主页，则每当您打开一个新选项卡时都会重定向到 google.com。
解决办法：更改主页或者筛选规则。
- 在设置协作会话时，从双向受信任的域中按电子邮件地址添加协作者失败。
解决办法：使用 domain\user 格式添加协作者。
- HTML5 多媒体重定向适用于 1803 之前的 Windows 10 虚拟桌面中的 Edge，但在更新为最新的 Windows 10 1803 版本（如 17133）后，重定向无法正常工作，尤其是使用自动播放的网站，如 youtube.com。
解决办法：强制重新启动 Windows 10 虚拟桌面。
- 在客户端会话处于空闲状态时，即使使用 GPO 或非 GPO 方法为空闲会话超时设置了 MaxIdleTime，已发布的应用程序也不会断开连接。虽然会显示断开连接警告消息，但应用程序并未断开连接。
- 使用多媒体重定向对媒体执行查找操作后，音频和视频变得不顺畅。
解决办法：等待几分钟或重新打开当前的流媒体。
- 有时，当用户在 Edge 浏览器中使用“HTML5 多媒体重定向”功能播放 YouTube 视频时，该视频会一直缓冲，且没有任何图像或声音。
解决办法：刷新页面。
- 在连接到启用了“实时音频-视频”功能的远程桌面后，您可能会看到以下消息：“需要重新启动您的 PC 才能完成此设备的设置: *devicename* (VDI)” (Your PC needs to be restarted to finish setting up this device: *devicename* (VDI))。
解决办法：您可以忽略此消息，因为该设备可以在远程桌面中使用。或者，您可以关闭 Windows 设置通知，以阻止显示该消息。

- 如果您连接到使用多个高分辨率显示器 (4K) 的桌面，并使用新的 Blast 编解码器以全屏模式播放视频，则播放性能可能较差（帧速率较低）。

解决办法：使用 H.264 以全屏模式播放视频。

- 如果将代理组策略设置 COM 端口隔离模式设为完全隔离（默认设置），则在 RDS 主机中安装 Horizon Agent 后，用户将无法对串行打印机使用“串行端口重定向”功能。此问题会同时影响 Windows 和 Linux 客户端。虚拟桌面不会出现此问题。

解决办法：编辑 COM 端口隔离模式组策略设置，将模式更改为隔离已禁用，然后重新启动 Horizon Agent。有关详细信息，请参阅《在 Horizon 7 中配置远程桌面功能》文档中的“串行端口重定向组策略设置”。

- 使用 VMware Integrated Printing 功能时，如果您从 Windows 7 客户端计算机连接到 Windows 10 代理计算机，并且通过重定向的打印机来打印包含 delta 字体的文档，则无法正常显示这些字体。

解决办法：无。这是一个第三方问题。

Horizon GPO 包

- 无法在即时克隆上应用需要重新引导才能生效的基于计算机的全局策略对象 (GPO)。

解决办法：请参阅 VMware 知识库 (KB) 文章 [2150495](#)。

- 在以下嵌套模式配置中，如果您在一级虚拟桌面配置二级桌面，“指定在重定向客户端打印机时使用的筛选器”组策略设置不影响二级桌面：一级桌面（安装 Horizon Client 和 Horizon Agent 的计算机）是虚拟桌面，而二级桌面是已发布的桌面。

解决办法：如果您要筛选二级桌面的打印机，请在二级桌面中配置“指定在重定向客户端打印机时使用的筛选器”组策略。

Horizon Client

本节介绍了最终用户使用 Horizon Client 或 HTML Access 连接到远程桌面和应用程序时可能遇到的问题。对于仅在特定的 Horizon Client 平台中出现的问题，请参阅 [Horizon Client 文档页面](#) 中的 Horizon Client 发行说明。

- RDS 主机上的多个用户会话缺少配置文件数据。如果会话处于断开连接状态，但 RDS 主机上的任务管理器仍显示这些会话，则会出现该问题。

解决办法：从 RDS 主机中删除会话，或者从发布的桌面或应用程序中注销用户。

- 在登录到 Workspace ONE 时，不会触发预启动应用程序会话。仅当从 Horizon Client 成功登录到连接服务器时，才会触发预启动会话。

解决办法：从 Workspace ONE 手动启动应用程序或桌面，以触发启用了预启动的应用程序的启动操作。

- 如果使用 VMware Blast 显示协议并禁用了 Blast 安全网关 (BSG)，Horizon Client 有时无法从短暂（约 1 分钟）网络中断中恢复并断开到桌面的连接。在启用了 BSG 的情况下，不会发生此问题。

解决办法：重新连接会话。

- RDS 主机仅存储会话中首次启动应用程序时的一组应用程序数据。任何后续的应用程序启动数据都会丢失。

解决办法：注销会话，然后启动其他应用程序以存储该数据。

- 在 Windows 10 客户端操作系统上使用 HTML Access 从 Internet Explorer 或 Microsoft Edge Web 浏览器连接到连接服务器、安全服务器或副本服务器时，桌面无法启动。此问题影响使用 Windows 10 N、Windows 10 KN、Windows 7 N 和 Windows 7 KN 客户机操作系统的桌面。

解决办法：为 HTML Access 使用 Firefox 或 Google Chrome Web 浏览器。

- 对于 Intel vDGA，多显示器支持仅限于不超过 3 个显示器。Intel 驱动程序最多仅支持 3 个显示器，并且分辨率最多为 3840x2160。如果尝试连接 4 个显示器，连接将显示 3 个黑屏，而只有一个屏幕正常工作。

- 如果 VDI 桌面位于远程位置并出现较长的网络延迟，则使用智能卡身份验证的递归解锁可能无法正常工作。

解决办法：手动解锁桌面。

- 如果 Windows 8 远程桌面用户使用 Kerberos 身份验证登录，然后桌面锁定，Windows 8 默认为用户显示的桌面解锁用户帐户是相关的 Windows Active Directory 帐户，而不是 Kerberos 域中的原始帐户。用户看不到自己登录所用的帐户。这是一个 Windows 8 问题，而不是直接由 Horizon 7 导致的问题。使用 Windows 7 时也可能出现这种问题（但不常见）。

解决办法：用户必须通过选择“其他用户”解锁桌面。然后 Windows 会显示正确的 Kerberos 域，这样用户才能使用 Kerberos 身份登录。

- 在远程桌面或应用程序上使用 Ambir Image Scan Pro 490i 执行扫描时，对话框始终显示“正在扫描... (Scanning...)”，并且扫描没有完成。

解决办法：在客户端执行扫描。客户端扫描会校准扫描仪。在完成校准操作后，保存校准文件并将其部署到 ProgramData\AmbirTechnology\ImageScanPro490i

- 对于 Horizon 7 for Linux 桌面中的 HTML Access，无法正确使用 Unicode 键盘输入。
 - 在连接到 Linux 桌面时，一些键盘输入无法正常工作。例如，如果您在客户端设备和远程桌面上都使用非英语 IME，某些非英语键将无法正确显示。
- 解决办法：**在客户端设备上设置英语 IME，并在远程桌面上设置非英语 IME。
- 有时从 Skype 到 Skype for Business 的音频呼叫不能正确启动。Skype for Business 客户端上的呼叫状态为“正在连接呼叫...”

解决办法：无。

- 如果在非持久桌面中使用 Skype for Business，可能会达到 Skype for Business 16 个设备证书的限制。当达到此限制并且 Skype for Business 尝试新登录时，将颁发新证书，并吊销最早分配的证书。
- 如果您启动的适用于 Linux 的 Horizon Client 4.8 或更低版本已启用 FIPS 模式，并且您尝试连接到已启用 FIPS 模式的 Horizon Agent 7.6 或者 Horizon 连接服务器 7.6 或更高版本，则会显示错误消息“RDS 许可证的许可证信息无效: 缺少客户端 ID” (Invalid license info for rds-license: Missing client id)。

解决办法：要使用已启用 FIPS 模式的适用于 Linux 的 Horizon Client 来连接到已启用 FIPS 模式的 Horizon Agent 7.6 或更高版本或者 Horizon 连接服务器 7.6 或更高版本，请使用适用于 Linux 的 Horizon Client 4.9 或更高版本。

- macOS 10.15、iOS 13 和 Chrome OS 76 上运行的 Chrome 浏览器、Safari 浏览器或 VMware Horizon 客户端可能无法使用在 Unified Access Gateway、Horizon Connection Server 和安全服务器上生成的默认自签名 TLS 服务器证书。出现此问题的原因可能是 Apple 更改了上述操作系统版本中受信任 TLS 服务器证书的要求。默认的自签名证书当前不满足这些新要求。如果通过终止 TLS 的中间负载均衡器或代理从客户端连接到 Horizon，则还必须在上述设备上满足新的证书要求。在 macOS 10.15 上的适用于 Mac 的 Horizon Client 上，如果不验证自签名证书，“在连接到不受信任的服务器之前发出警告”模式可能会失效，并弹出“不受信任的服务器连接”对话框，其中显示错误消息“VMware Horizon Client 无法验证您的连接。请联系您的管理员” (VMware Horizon Client cannot verify your connection. Contact your administrator.)，并且只有“显示证书”和“不连接”按钮可用。

解决办法：VMware 通常建议将默认的自签名 TLS 服务器证书替换为环境中受信任的 CA 签名证书。此建议在任何时候都是一种良好的安全实践。在这种情况下，只要受信任的 CA 签名证书满足 Apple 的新要求，就不会出现此问题。对于 macOS 和 iOS Horizon 客户端，备用解决办法是将 SSL 配置设为不验证服务器证书。有关 Apple 证书要求的更多信息，请参阅 <https://support.apple.com/zh-cn/HT210176>

Horizon JMP Server 和 JMP Integrated Workflow

- 在安装了多个 JMP Server 的环境中，在创建或删除 JMP 分配时，如果多个 JMP Server 引用相同的 User Environment Manager 配置共享，则可能会发生冲突。

解决办法：无。

- 如果将 JMP 设置配置为仅使用一个 VMware App Volumes Manager，并在创建 JMP 分配期间选择了 Horizon Agent 未指向该配置的 App Volumes Manager 的桌面池，您仍可以从桌面池的 Horizon Agent 指向的 App Volumes Manager 实例中选择 AppStack。此外，如果将 JMP 设置配置为使用多个 App Volumes Manager 实例，即使您选择 Horizon Agent 指向其中的一个 App Volumes Manager 实例的桌面池，您仍可以从在 JMP 设置中配置的其他 App Volumes Manager 实例中选择 AppStack。但在启动桌面池时，从其他 App Volumes Manager 中选择的 AppStack 不可用。

解决办法：无。

- 如果使用 App Volumes Manager 或编辑 JMP 分配以重命名现有 JMP 分配当前使用的 AppStack，不会使用新的 AppStack 名称更新现有 JMP 分配的摘要页面。

解决办法：无。

- 如果在相同的 JMP Server 实例中注册两个 Horizon 7 实例，并且它们使用相同的 App Volumes Manager，从一个 Horizon 7 实例中删除 JMP 分配可能会删除在另一个 Horizon 7 实例中的另一个 JMP 分配使用的 AppStack 分配。

解决办法：无。

- 在“JMP 设置”页中添加或编辑 Active Directory 信息时，如果为绑定用户名输入的值包含 30 个三字节中文字符中的一个或多个字符（如“试”字符）而导致 Active Directory 身份验证失败，该操作将失败。

解决办法：使用 Active Directory 中的另一个绑定用户名，该用户具有管理特权，并且不包含 30 个三字节中文字符中的任何字符，如“试”字符。

- 在“JMP 设置”页中添加或编辑 App Volumes Manager 实例信息时，如果为服务帐户用户名输入的值包含 30 个三字节中文字符中的一个或多个字符（如“试”字符）而导致 App Volumes Manager 实例身份验证失败，该操作将失败。

解决办法：使用 App Volumes Manager 实例中的另一个绑定用户名，该用户具有管理特权，并且不包含 30 个三字节中文字符中的任何字符，如“试”字符。

- 在启动 Windows 10 1703 桌面池时，不会显示使用 VMware Dynamic Environment Manager 9.2.1 版本映射的驱动器映射设置。

解决办法：在启动 Windows 10 1703 桌面池后，执行以下命令。

```
C:\Program Files\Immidio\Flex Profiles\FlexEngine.exe -UemRefreshDrives
```

有关其他信息，请参阅 VMware 知识库 (KB) 文章 <https://kb.vmware.com/s/article/2113657>。

- 如果您使用 localhost 访问 Horizon Console，在 Horizon Console 的“JMP 设置”窗格中显示“JMP Server 当前无法访问。”(JMP server is not reachable at the moment.) 错误消息。

解决办法：仅使用完全限定域名 (FQDN) 访问 Horizon Console，而不是使用 localhost。

- 在创建新的 JMP 分配时，可能会在应用程序选项卡中显示以下警告消息：“与选定的桌面池关联的 App Volumes 实例与任何注册的 App Volumes 实例均不匹配。”(The App Volumes instance associated with the selected desktop pool does not match any of the registered App Volumes instances.)在满足以下条件之一时，将会出现该问题：

- 使用 IP 地址安装桌面池中使用的 App Volumes Agent，而不是使用完全限定域名 (FQDN)
- 使用 FQDN 安装桌面池中使用的 App Volumes Agent，但在 JMP 设置中注册了 App Volumes Manager 实例的 IP 地址。

解决办法：使用 FQDN 重新安装 App Volumes Agent，并在设置 (JMP) > App Volumes 选项卡中注册 App Volumes Manager 实例时使用 FQDN。

- 在安装 VMware Horizon JMP Server 时，JMP Server 安装程序无法继续执行，因为 McAfee Antivirus 检测到 NSSM.EXE 并将其视为威胁。

解决办法：在重新安装 JMP Server 之前，将以下文件添加到 McAfee Antivirus 排除列表中。

C:\Program Files (x86)\VMware\JMP\nssm-2.24\nssm-2.24\win32\nssm.exe

C:\Program Files (x86)\VMware\JMP\com\xmp\node_modules\winser\bin\nssm.exe

- 如果在 Horizon 7 连接服务器安装期间选择了授权本地 Administrators 组选项（这会创建 BUILTIN\Administrators 组而不是 <domainName>\Administrator），使用 Horizon Console 添加 JMP Server 信息将失败，并显示“没有足够的 Horizon 特权” (Insufficient Horizon Privileges) 错误消息。

解决办法：通过使用 Horizon Administrator，注册具有完全管理员访问权限的

<domainName>/administrator。重新登录到 Horizon Console 并添加 JMP Server 信息。

- 在创建 JMP 分配时，如果将鼠标悬停在即时克隆桌面池之上，“3D 呈现器”选项所显示的值为已禁用而不是使用 vSphere Client 管理。

解决办法：无。

- 当信任身份验证设置的范围设为“选择性身份验证”时，JMP Server 注册失败。

解决办法：利用以下解决办法之一来解决此问题。

- 使用域范围的身份验证。
- 继续使用“选择性身份验证”安全设置，但在位于信任域或林中的计算机对象（资源计算机）的所有域控制器上，为每个 Horizon Connection Server 主机（本地系统）帐户明确授予“允许身份验证”权限。有关如何授予“允许身份验证”权限的信息，请参阅 Microsoft 文章[在信任域或林中的计算机上授予‘允许身份验证’权限](#)。

- 由于无法确定有关桌面池使用的 App Volumes Manager 以及 JMP Server 使用的 User Environment Manager 版本的信息，JMP 分配无法按预期工作。

解决办法：在配置桌面池时，将“置备设置”窗格中“桌面池尺寸调整”部分的备用 (已打开电源) 计算机数量值设置为大于或等于 1。此外，如果在“置备时间安排”部分选择了按需置备计算机选项，则还应将计算机的最小数量值设置为大于或等于 1。

- 在当前安装有 JMP Server 版本 1.0.0.516 的主机上运行 JMP Server 版本 1.0.2.x 安装程序文件时，安装过程不会执行。

解决办法：使用控制面板卸载 JMP Server 版本 1.0.0.516。运行 JMP Server 版本 1.0.2.x 的安装文件，并按照向导说明完成安装。在安装过程中提供与安装 JMP Server 版本 1.0.0.516 时所用的相同 SQL Server 数据库信息，以便保留您具有的任何数据。

- 在以下情况下，尝试使用 JMP Server 安装程序版本 1.1.0.xxx 升级当前安装时，升级会失败，安装将进行回滚，之后 JMP Server 实例变得不可用。

- JMP Server 安装中缺少 SQL Server 数据库证书，且升级过程中选中了启用 SSL 复选框。
- 通过选择 Windows 身份验证连接模式完成了 JMP Server 升级，但没有为 JMP Server 主机系统创建 SQL Server 登录帐户。
- 单击取消取消了升级操作。

解决办法：通过重新运行 JMP Server 安装程序版本 1.1.0.xxx 再次尝试升级。您必须重新输入用于安装以前 JMP Server 版本的相同 SQL Server 数据库信息。成功升级后，确认为 JMP Server 配置的所有证书仍完好无损。根据安装失败或取消安装的时间，证书可能已被更改。

- 尝试添加 Dynamic Environment Manager (DEM) 配置共享时，可能会出现以下错误：runOne] 运行 file_share.createFileShare 时出错 { 代码: 400, \n 用时: 221, \n 数据: {}, \n 错误: “无法创建文件共享 <fileshare-unc-path>。” (runOne] Error running file_share.createFileShare { code: 400,\n took: 221,\n data: {},\n error: 'Unable to create file share <fileshare-unc-path>.')

DEM 配置共享的密码包含以下字符之一时，添加 DEM 配置共享会失败：“#+,;<=>\~

解决办法：使用包含以下某一允许的字符的其他密码：!\$%&'()*-./:?[\\^_`{|}

Horizon Cloud Connector

- 使用基于 HTML5 的 vSphere Web Client 部署 Horizon Cloud Connector 虚拟设备 OVA 文件时，出现以下错误：“为属性 proxySsl 指定的值 ‘false’ 无效。未能部署 OVF 软件包 (Invalid value 'false' specified for property proxySsl. Failed to deploy OVF package)。”

解决办法：使用基于 Flex 或基于 Flash 的 vSphere Web Client 部署 Horizon Cloud Connector 虚拟设备 OVA 文件。

- 启动 Horizon Cloud Connector 时，您看到以下消息：“[失败] 未能启动，请等待网络完成配置。有关详细信息，请参阅 ‘systemctl status systemd-networkd-wait-online.service’ 。” ([FAILED] Failed to start Wait for Network to be Configured. See 'systemctl status systemd-networkd-wait-online.service' for details.)

该消息显示有误，并不表示网络实际出现问题。您可以忽略该消息，并照常继续使用 Horizon Cloud Connector。