

Horizon Console 管理指南

2019 年 7 月

VMware Horizon 7 7.9



vmware®

您可以从 VMware 网站下载最新的技术文档:

<https://docs.vmware.com/cn/>。

如果您对本文档有任何意见或建议, 请将反馈信息发送至:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

威睿信息技术(中国)有限公司
北京办公室
北京市
朝阳区新源南路 8 号
启皓北京东塔 8 层 801
www.vmware.com/cn

上海办公室
上海市
淮海中路 333 号
瑞安大厦 804-809 室
www.vmware.com/cn

广州办公室
广州市
天河路 385 号
太古汇一座 3502 室
www.vmware.com/cn

版权所有 © 2018-2019 VMware, Inc. 保留所有权利。 [版权和商标信息](#)

目录

1	《VMware Horizon Console 管理指南》	10
2	使用 VMware Horizon Console	11
	支持的 Horizon 7 功能	11
	使用 Horizon Console 的优势	13
	安装和配置 Horizon Console	13
	登录到 Horizon Console	13
3	在 Horizon Console 中配置 Horizon 连接服务器	15
	在 Horizon Console 中配置 vCenter Server 和 Horizon Composer	15
	为 Horizon Composer AD 操作创建用户帐户	15
	在 Horizon Console 中安装产品许可证密钥	16
	在 Horizon Console 中将 vCenter Server 实例添加到 Horizon 7	17
	配置 Horizon Composer 设置	19
	配置 Horizon Composer 域	20
	在 Horizon Console 中添加即时克隆域管理员	21
	允许 vSphere 回收链接克隆虚拟机中的磁盘空间	22
	为 vCenter Server 配置 Horizon Storage Accelerator	23
	vCenter Server 和 Horizon Composer 的并发操作数限制	24
	设置并发电源操作率来支持远程桌面登录风暴	25
	接受默认 TLS 证书的指纹	25
	从 Horizon 7 中移除 vCenter Server 实例	27
	从 Horizon 7 中移除 Horizon Composer	27
	vCenter Server 唯一 ID 冲突	28
	在 Horizon Console 中备份 Horizon 连接服务器	28
	在 Horizon Console 中配置客户端会话设置	29
	Horizon Console 中客户端会话的全局设置	29
	Horizon Console 中客户端会话和连接的全局安全性设置	31
	在 Horizon Console 中禁用或启用 Horizon 连接服务器	32
	编辑 Horizon 连接服务器实例的外部 URL	33
	在 Horizon Console 中注册网关	34
4	设置智能卡身份验证	35
	使用智能卡登录	35
	在 Horizon 连接服务器上配置智能卡身份验证	36
	获取证书颁发机构证书	37
	从 Windows 获取 CA 证书	37

- 将 CA 证书添加到服务器信任存储区文件中 38
- 修改 Horizon 连接服务器配置属性 38
- 在 Horizon Console 中配置智能卡设置 39
- 在第三方解决方案上配置智能卡身份验证 41
- 为智能卡身份验证准备 Active Directory 42
 - 为智能卡用户添加 UPN 42
 - 将根证书添加到 Enterprise NTAAuth 存储 43
 - 将根证书添加到受信任的根证书颁发机构 43
 - 将中间证书添加到中间证书颁发机构 44
- 在 Horizon Console 中验证智能卡身份验证配置 44
- 使用智能卡证书撤销检查 45
 - 登录时进行 CRL 检查 46
 - 登录时进行 OCSP 证书撤销检查 46
 - 配置 CRL 检查 46
 - 配置 OCSP 证书撤销检查 47
 - 智能卡证书撤销检查属性 48
- 5 设置其他类型的用户身份验证 49**
 - 使用双因素身份验证 49
 - 使用双因素身份验证登录 50
 - 在 Horizon Console 中启用双因素身份验证 50
 - RSA SecurID 访问被拒绝故障排除 52
 - 排除 RADIUS 访问被拒故障 52
 - 使用 SAML 身份验证 53
 - 为 VMware Identity Manager 集成使用 SAML 身份验证 53
 - 在 Horizon Console 中配置 SAML 身份验证器 54
 - 为 VMware Identity Manager 配置代理支持 56
 - 在连接服务器上更改服务提供程序元数据的过期时间 56
 - 生成 SAML 元数据以便连接服务器可用作服务提供程序 57
 - 多个动态 SAML 身份验证器的响应时间注意事项 57
 - 在 Horizon Console 中配置 Workspace ONE 访问策略 57
 - 配置生物身份验证 58
- 6 对用户和组进行身份验证 60**
 - 限制网络外部的远程桌面访问 60
 - 配置远程访问 60
 - 配置未验证访问 61
 - 创建未验证访问用户 61
 - 授权未验证访问用户访问已发布的应用程序 62
 - 删除未验证访问用户 62
 - 从 Horizon Client 未验证访问 63

7 在 Horizon Console 中配置基于角色的委派管理 64

了解角色和特权 64

在 Horizon Console 中使用访问组委派池和场的管理权 65

为不同访问组配置不同管理员 65

为同一访问组配置不同管理员 66

了解权限 66

对管理员进行管理 67

在 Horizon Console 中创建管理员 67

在 Horizon Console 中移除管理员 68

管理和查看权限 68

在 Horizon Console 中添加权限 69

在 Horizon Console 中删除权限 69

在 Horizon Console 中查看权限 70

管理和查看访问组 70

在 Horizon Console 中添加访问组 71

在 Horizon Console 中将桌面池或场移至不同的访问组 71

在 Horizon Console 中移除访问组 71

查看访问组中的对象 72

查看访问组中的 vCenter 虚拟机 72

管理自定义角色 72

在 Horizon Console 中添加自定义角色 73

在 Horizon Console 修改自定义角色中的特权 73

在 Horizon Console 中移除自定义角色 73

预定义的角色和特权 74

预定义的管理员角色 74

全局特权 76

特定于对象的特权 77

内部特权 78

执行常见任务所需的特权 78

管理池所需的特权 78

管理计算机所需的特权 79

管理永久磁盘所需的特权 79

管理用户和管理员所需的特权 80

Horizon Help Desk Tool 任务所需的特权 80

执行常规管理任务和命令所需的特权 81

针对管理员用户和组的最佳实践 81

8 在 Horizon Console 中设置策略 82

配置全局策略 82

9 维护 Horizon 7 组件 84

- 备份和还原 Horizon 7 配置数据 84
 - 备份 Horizon 连接服务器和 Horizon Composer 数据 84
 - 计划 Horizon 7 配置备份 85
 - Horizon 7 配置备份设置 86
 - 从 Horizon 连接服务器中导出配置数据 86
- 还原 Horizon 连接服务器和 Horizon Composer 配置数据 87
 - 将配置数据导入 Horizon 连接服务器中 88
 - 还原 Horizon Composer 数据库 89
 - 还原 Horizon Console 数据库时显示的结果代码 90
- 导出 Horizon Composer 数据库中的数据 91
 - 导出 Horizon Composer 数据库时显示的结果代码 92
- 在 Horizon Console 中更改产品许可证密钥或许可证模式 92
- 监控许可证使用情况 93
 - 重置许可证使用情况数据 94
- 客户体验提升计划 94

10 在 Horizon Console 中创建虚拟桌面池 95

- 创建即时克隆桌面池 95
 - 用于在 Horizon Console 中创建即时克隆桌面池的工作表 96
 - 创建即时克隆桌面池 100
 - 在 Horizon Console 中更改即时克隆桌面池的映像 101
 - 在 Horizon Console 中监控推送映像操作 102
 - 在 Horizon Console 中重新计划或取消推送映像操作 102
- 创建包含完整虚拟机的自动桌面池 102
 - 用于在 Horizon Console 中创建包含完整虚拟机的自动池的工作表 103
 - 创建包含完整虚拟机的自动池 105
 - 通过 Horizon Console 在完整克隆桌面池中重建虚拟机 106
- 在 Horizon Console 中创建链接克隆桌面池 107
 - 用于在 Horizon Console 中创建链接克隆桌面池的工作表 107
 - Horizon Console 中适用于链接克隆桌面池的桌面池设置 114
 - 在 Horizon Console 中创建链接克隆桌面池 115
- 在 Horizon Console 中创建手动桌面池 116
 - 用于在 Horizon Console 中创建手动桌面池的工作表 117
 - 在 Horizon Console 中创建手动桌面池 118
 - Horizon Console 中适用于手动池的桌面池设置 119
- 配置桌面池 120
 - Horizon Console 中的桌面池用户分配 120
 - 手动自定义计算机 127
 - Horizon Console 中适用于所有桌面池类型的桌面池设置 128

在 Horizon Console 中管理桌面池和虚拟桌面	131
管理桌面池	131
管理基于虚拟机的桌面	134
在 Horizon Console 中将 Horizon 7 信息导出到外部文件	135
管理 Horizon Composer 链接克隆桌面虚拟机	136
在 Horizon Console 中管理未受管和已注册的计算机	147
排除计算机和桌面池的问题	148
在 Horizon Console 中显示出现问题的计算机	148
确认桌面池的用户分配	149
在 Horizon Console 中重新启动桌面并重置虚拟机	150
在 Horizon Console 中向桌面用户发送消息	150
在 Horizon Console 中管理未授权用户的计算机和策略	151
11 在 Horizon Console 中创建已发布的桌面和应用程序	152
在 Horizon Console 中创建场	152
用于在 Horizon Console 中创建手动场的工作表	153
在 Horizon Console 中创建手动场	154
用于在 Horizon Console 中创建自动即时克隆场的工作表	154
在 Horizon Console 中创建自动即时克隆场	158
用于在 Horizon Console 中创建自动链接克隆场的工作表	159
在 Horizon Console 中创建自动链接克隆场	163
在 Horizon Console 中创建已发布的桌面池	164
用于创建已发布桌面池的工作表	164
在 Horizon Console 中创建已发布的桌面池	165
在 Horizon Console 中创建应用程序池	165
用于在 Horizon Console 中手动创建应用程序池的工作表	166
在 Horizon Console 中创建应用程序池	169
在 Horizon Console 中为应用程序池配置反关联性规则	169
在 Horizon Console 中管理场	171
在 Horizon Console 中编辑场	171
在 Horizon Console 中删除场	171
在 Horizon Console 中禁用或启用场	171
在 Horizon Console 中安排自动即时克隆场维护	172
在 Horizon Console 中管理应用程序池	174
在 Horizon Console 中编辑应用程序池	174
在 Horizon Console 中删除应用程序池	174
更改已发布应用程序的图标	174
移除已发布应用程序的图标	175
在 Horizon Console 中管理 RDS 主机	175
在 Horizon Console 中编辑 RDS 主机	175
在 Horizon Console 中将 RDS 主机添加到手动场	176

- 通过 Horizon Console 从场中移除 RDS 主机 176
 - 从 Horizon 7 中移除 RDS 主机 177
 - 在 Horizon Console 中禁用或启用 RDS 主机 177
 - 在 Horizon Console 中监控 RDS 主机 178
 - Horizon Console 中的 RDS 主机状态 179
 - 在 Horizon Console 中管理已发布的桌面和应用程序会话 180
- 12 在 Horizon Console 中授权用户和组 181**
 - 在 Horizon Console 中为桌面池或应用程序池添加授权 181
 - 在 Horizon Console 中移除对桌面池或应用程序池的授权 182
 - 查看桌面或应用程序池授权 182
 - 为授权池配置快捷方式 183
 - 在 Horizon Console 中为桌面池创建快捷方式 183
 - 在 Horizon Console 中为应用程序池创建快捷方式 184
 - 对桌面和应用程序池实施客户端限制 186
- 13 JMP Integrated Workflow 入门 187**
 - 关于 JMP Integrated Workflow 187
 - 开始使用 JMP 集成工作流 187
- 14 管理 JMP 设置 189**
 - 首次配置 JMP 设置 189
 - 管理 JMP 设置 191
 - 编辑 JMP Server 设置 192
 - 编辑 Horizon 7 凭据 192
 - 编辑 Horizon 连接服务器 URL 192
 - 添加 Active Directory 域 193
 - 编辑 Active Directory 域信息 194
 - 删除 Active Directory 域信息 194
 - 添加 App Volumes 信息 195
 - 编辑 App Volumes 实例信息 195
 - 删除 App Volumes 实例信息 196
 - 添加 User Environment Manager 配置共享信息 196
 - 编辑 User Environment Manager 配置文件共享信息 197
 - 删除 User Environment Manager 配置共享信息 197
- 15 管理 JMP 分配 198**
 - 创建 JMP 分配 198
 - 编辑 JMP 分配 200
 - 复制 JMP 分配 201
 - 删除 JMP 分配 201

16 在 Horizon Console 中配置事件报告 203

在 Horizon Console 中为 Horizon 7 事件添加数据库和数据库用户 203

在 Horizon Console 中为事件报告准备 SQL Server 数据库 204

在 Horizon Console 中配置事件数据库 205

在 Horizon Console 中为 Syslog 服务器配置事件日志记录 206

在 Horizon 7 中监控事件 207

Horizon 7 事件消息 208

17 在 Horizon Console 中使用 Horizon Help Desk Tool 209

在 Horizon Console 中启动 Horizon Help Desk Tool 210

在 Horizon Help Desk Tool 中对用户进行故障排除 210

Horizon Help Desk Tool 的会话详细信息 213

Horizon Help Desk Tool 的会话进程 217

Horizon Help Desk Tool 的应用程序状态 218

在 Horizon Help Desk Tool 中对桌面或应用程序会话进行故障排除 218

《VMware Horizon Console 管理指南》

1

《VMware Horizon Console 管理指南》介绍了如何在 Horizon Console 中配置和管理 VMware Horizon® 7、如何创建管理员、如何设置用户身份验证，以及如何配置策略和执行管理任务。本文档还介绍了如何对 Horizon 7 组件进行维护和故障排除。

有关如何使用 Horizon Console 配置和管理 Cloud Pod 架构环境的信息，请参阅《在 Horizon 7 中管理 Cloud Pod 架构》文档。

目标读者

本文档中的信息面向任何需要配置和管理 VMware Horizon 7 的人员。本文档中的信息专为已熟练掌握虚拟机技术和数据中心操作并且具有丰富经验的 Windows 或 Linux 系统管理员所编写。

使用 VMware Horizon Console

VMware Horizon Console 是最新版本的 Web 界面，您可以通过该控制台创建和管理虚拟桌面及已发布的桌面和应用程序。Horizon Console 还集成了用于管理工作区的 VMware Horizon Just-in-Time Management Platform (JMP) 集成 workflow 功能。

安装并配置 Horizon 连接服务器后，便可以使用 Horizon Console。

有关配置连接服务器的更多信息，请参阅《Horizon 7 管理指南》。

有关 JMP 集成 workflow 功能的更多信息，请参阅[第 13 章 JMP Integrated Workflow 入门](#)。

本章讨论了以下主题：

- 支持的 Horizon 7 功能
- 使用 Horizon Console 的优势
- 安装和配置 Horizon Console
- 登录到 Horizon Console

支持的 Horizon 7 功能

Horizon Console 实施了部分 Horizon 7 功能。您可以使用经典的 Web 界面 Horizon Administrator 来访问 Horizon Console 中尚不可用的那些功能。

有关 Horizon Administrator 中支持的 Horizon 7 功能的信息，请参阅《Horizon 7 管理指南》文档。

支持以下功能：

- 服务器
 - Horizon 连接服务器配置
 - 事件数据库
- 授权
 - 用户和组授权
 - 桌面授权
 - 应用程序授权
 - 全局授权
 - 全局策略

- 身份验证
 - 远程访问身份验证
 - 已发布应用程序的未验证访问
 - 智能卡身份验证
 - 基于角色的委托管理
 - 虚拟桌面
 - 完整虚拟机的自动专用分配池
 - 自动即时克隆专用分配池和浮动分配池
 - 自动链接克隆桌面池
 - 完整虚拟机的自动浮动分配池
 - 手动桌面池
 - 永久磁盘
 - 已发布的桌面
 - 手动场
 - 自动即时克隆场
 - 自动链接克隆场
 - RDS 桌面池
 - 已发布的应用程序
 - 手动应用程序池
 - 基于现有应用程序的应用程序池
 - 虚拟机
 - vCenter Server 中的可用虚拟机
 - vCenter Server 中的不可用已注册计算机
 - Cloud Pod 架构
- 不支持以下功能：
- 克隆自动桌面池
 - ThinApp 应用程序

使用 Horizon Console 的优势

使用 Horizon Console 的优势包括：能够简化桌面和应用程序部署过程，交付 Just-in-Time 桌面，以及提供更安全的 Web 界面以消除安全风险。

Horizon Console Web 界面进行了更新，为部署桌面和应用程序及进行故障排除提供了一些易于使用的工作流。

Horizon Console 中还包含 JMP Integrated Workflow 功能，这些功能将即时克隆、VMware App Volumes 和 VMware User Environment Manager 技术纳入到一个集成的工作流中，以便交付可快速部署和扩展的按需桌面。有关更多信息，请参阅[关于 JMP Integrated Workflow](#)。

Horizon Console 具有基于 HTML5 的 Web 界面，此界面已经更新，消除了许多安全风险和漏洞，因此更加安全。

安装和配置 Horizon Console

在您使用 Horizon 连接服务器安装程序安装并配置连接服务器后，可从 Horizon Administrator Web 界面中访问 Horizon Console URL。使用 JMP Server 安装程序安装并配置 JMP Server 之后，可在 Horizon Console 中使用 JMP Integrated Workflow。

有关安装连接服务器的更多信息，请参阅《Horizon 7 安装指南》文档。

有关配置连接服务器的更多信息，请参阅《Horizon 7 管理指南》文档。

有关安装和配置 JMP Server 的更多信息，请参阅《VMware Horizon JMP Server 安装和设置指南》文档。

登录到 Horizon Console

要执行桌面或应用程序池部署任务、故障排除任务或管理 JMP 工作流，您必须登录到 Horizon Console。您可以通过 Horizon Administrator Web 界面使用安全 (TLS) 连接访问 Horizon Console。

前提条件

- 确认已在专用计算机上安装 Horizon 连接服务器。
- 必须为用户分配任何预定义的角色或预定义角色组合，用户才能在 Horizon Administrator 中查看 Horizon Console 链接，并登录到 Horizon Console。但是，当用户分配了自定义角色，或者预定义角色和自定义角色的组合时，Horizon Console 链接不会显示在 Horizon Administrator 中。有关配置基于角色的访问权限的更多信息，请参阅《Horizon 7 管理指南》文档。
- 确认您使用的是 Horizon Console 支持的 Web 浏览器。有关受支持 Web 浏览器的更多信息，请参阅《Horizon 7 安装指南》文档。

步骤**1** 登录到 Horizon Administrator 界面。

打开 Web 浏览器并输入以下 URL，其中 **server** 是连接服务器实例的主机名。

https://server/admin

注 当主机名不可解析时，如果您需要访问连接服务器实例，则可以使用 IP 地址。但是，所连接的主机将与为连接服务器实例配置的 TLS 证书不匹配，从而导致访问被阻止或访问的安全性降低。

对 Horizon Administrator 的访问取决于连接服务器计算机上配置的证书类型。

如果在连接服务器主机上打开 Web 浏览器，请使用 **https://127.0.0.1**（而非 **https://localhost**）进行连接。该方法可以避免在解析 localhost 时遭受潜在 DNS 攻击，从而提高安全性。

选项	说明
为连接服务器配置一个由 CA 签发的证书。	首次连接时，您的 Web 浏览器会显示 Horizon Console。
配置了连接服务器提供的默认自签名证书。	第一次连接时，Web 浏览器可能会显示一个页面，警告与该地址相关联的安全证书不是由受信任的证书颁发机构颁发的。 单击 忽略 可继续使用当前的 TLS 证书。

2 以具有管理员帐户访问凭据的用户身份登录。

当您在副本组中安装独立的连接服务器实例或第一个连接服务器实例时，可以为管理员角色指定首个分配。默认情况下，会选择安装连接服务器时使用的帐户，但您也可以将此帐户更改为管理员本地组或域的全局组。

如果您选择管理员本地组，那么您可以使用直接添加到此组或通过全局组成员资格添加到此组的任何域用户。您不能使用添加到此组的本地用户。

3 在 Horizon Administrator 中，单击 **Horizon Console**。

将在新选项卡中打开 Horizon Console Web 界面。通过单点登录来登录到 Horizon Console。

在 Horizon Console 中配置 Horizon 连接服务器

3

安装 Horizon 连接服务器并对其执行初始配置后，可以向 Horizon 7 部署中添加 vCenter Server 实例和 Horizon Composer 服务、设置可委派管理员职责的角色以及创建配置数据备份计划。

本章讨论了以下主题：

- 在 Horizon Console 中配置 vCenter Server 和 Horizon Composer
- 在 Horizon Console 中备份 Horizon 连接服务器
- 在 Horizon Console 中配置客户端会话设置
- 在 Horizon Console 中禁用或启用 Horizon 连接服务器
- 编辑 Horizon 连接服务器实例的外部 URL
- 在 Horizon Console 中注册网关

在 Horizon Console 中配置 vCenter Server 和 Horizon Composer

要将虚拟机用作远程桌面，必须配置 Horizon 7，使其与 vCenter Server 通信。要创建和管理链接克隆桌面池，必须在 Horizon Console 中配置 Horizon Composer 设置。

也可对 Horizon 7 配置存储设置。您可允许 ESXi 主机回收链接克隆虚拟机上的磁盘空间。为了允许 ESXi 主机缓存虚拟机数据，您必须为 vCenter Server 启用 Horizon Storage Accelerator。

为 Horizon Composer AD 操作创建用户帐户

如果您使用 Horizon Composer，则必须在 Active Directory 中创建一个用户帐户，以允许 Horizon Composer 在 Active Directory 中执行特定操作。Horizon Composer 需要使用该帐户将链接克隆虚拟机加入到您的 Active Directory 域中。

为了确保安全，请创建一个单独的用户帐户以用于 Horizon Composer。通过创建单独的帐户，可以确保该帐户不具有针对其他目的定义的额外特权。您可以为该帐户授予在指定的 Active Directory 容器中创建和移除计算机对象所需的最低特权。例如，Horizon Composer 帐户不需要域管理员特权。

步骤

- 1 在 Active Directory 中，在您的连接服务器主机所在的域或某个受信任的域中创建一个用户帐户。

- 2 在用于创建和接收链接克隆计算机帐户的 **Active Directory** 容器中，授予该帐户**创建计算机对象**、**删除计算机对象**和**写入全部属性**权限。

以下列表显示了该用户帐户需要的所有权限，包括默认分配的权限：

- 列出内容
- 读取全部属性
- 写入全部属性
- 读取权限
- 重置密码
- 创建计算机对象
- 删除计算机对象

注 如果为桌面池选择**允许重用预先存在的计算机帐户**设置，则所需的权限较少。确保已将以下权限分配给用户帐户：

- 列出内容
- 读取全部属性
- 读取权限
- 重置密码

- 3 确保该用户帐户的权限可应用于 **Active Directory** 容器及其所有子对象。

后续步骤

在 Horizon Console 中执行以下操作时指定该帐户：在**添加 vCenter Server** 向导中配置 Horizon Composer 域，以及配置和部署链接克隆桌面池。

在 Horizon Console 中安装产品许可证密钥

您必须先输入产品许可证密钥，然后才能使用连接服务器。

注 如果您拥有 **Horizon 7** 订阅许可证，则不需要产品许可证密钥。有关订阅许可证的更多信息，请参阅《**Horizon 7 安装指南**》文档中的“为订阅许可证启用 **Horizon 7**”。

首次登录时，**Horizon Console** 会显示“许可和使用情况”页面。

安装连接服务器副本实例或安全服务器时，不需要配置许可证密钥。副本实例和安全服务器使用存储在 **View LDAP** 配置中的通用许可证密钥。

注 连接服务器需要有效的许可证密钥。产品许可证密钥是一个包含 **25** 个字符的密钥。

步骤

- 1 在 Horizon Console 中，选择**设置 > 产品许可和使用情况**。

- 2 在**许可设置**面板中，单击**编辑许可证**。
- 3 输入许可证序列号，然后单击**确定**。
- 4 验证许可证的过期日期。
- 5 根据产品许可证授权您使用的 VMware Horizon 7 版本，验证是启用还是禁用了桌面、应用程序远程处理和 View Composer 许可证。

并非所有版本都提供 VMware Horizon 7 的所有特性和功能。有关各个版本中的功能集的比较，请参阅 <http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf>。

在 Horizon Console 中将 vCenter Server 实例添加到 Horizon 7

您必须将 Horizon 7 配置为连接到 Horizon 7 部署中的 vCenter Server 实例。vCenter Server 可创建并管理 Horizon 7 在桌面池中使用的虚拟机。

如果是在链接模式组中运行 vCenter Server 实例，就必须将每个 Horizon 7 实例分别添加到 View Manager。

Horizon 7 使用安全通道 (TLS) 连接至 vCenter Server 实例。

前提条件

- 安装连接服务器产品许可证密钥。
- 准备一个有权在 vCenter Server 中执行支持 Horizon 7 所需操作的 vCenter Server 用户。要使用 Horizon Composer，您必须为该用户授予额外的特权。

有关为 Horizon 7 配置 vCenter Server 用户的详细信息，请参阅《Horizon 7 安装指南》文档。
- 确认 vCenter Server 主机上安装了 TLS 服务器证书。在生产环境中，安装由受信任证书颁发机构 (Certificate Authority, CA) 签名的有效证书。

在测试环境中，您可以使用随 vCenter Server 一起安装的默认证书，但在 Horizon 7 中添加 vCenter Server 时必须接受证书指纹。
- 确认副本组中的所有连接服务器实例都信任 vCenter Server 主机上安装的服务器证书的根 CA 证书。检查根 CA 证书是否位于连接服务器主机上 Windows 本地计算机证书存储区中的**受信任的根证书颁发机构 > 证书**文件夹中。如果没有，请将根 CA 证书导入 Windows 本机证书存储区。

请参阅《Horizon 7 安装指南》文档中的“将根证书和中间证书导入 Windows 证书存储区”。
- 确认 vCenter Server 实例包含 ESXi 主机。如果 vCenter Server 实例中未配置主机，则无法在 Horizon 7 中添加实例。
- 如果您要升级到 vSphere 5.5 或更高版本，请确认您用作 vCenter Server 用户的域管理员帐户已由 vCenter Server 本地用户明确分配了登录 vCenter Server 的权限。
- 如果您计划以 FIPS 模式使用 Horizon 7，请确认您具有 vCenter Server 6.0 或更高版本以及 ESXi 6.0 或更高版本的主机。

有关更多信息，请参阅《Horizon 7 安装指南》文档中的“以 FIPS 模式安装 Horizon 7”。

- 熟悉用于确定 vCenter Server 和 Horizon Composer 最大操作数限制的设置。

步骤

- 1 在 Horizon Console 中，导航到 **设置 > 服务器**。
- 2 在 **vCenter Server** 选项卡上，单击 **添加**。
- 3 在 vCenter Server 设置 **服务器地址** 文本框中，键入 vCenter Server 实例的完全限定域名 (FQDN)。

FQDN 包含主机名和域名。例如，在 FQDN *myserverhost.companydomain.com* 中，*myserverhost* 是主机名，*companydomain.com* 是域名。

注 如果通过 DNS 名称或 URL 来输入服务器，则 Horizon 7 不会执行 DNS 查找来确认管理员之前是否是使用 IP 地址将该服务器添加到 Horizon 7 中的。如果同时使用 DNS 名称和 IP 地址添加 vCenter Server，则会发生冲突。

- 4 键入 vCenter Server 用户的名称。
例如：domain\user 或 user@domain.com
- 5 键入 vCenter Server 用户密码。
- 6 （可选）键入该 vCenter Server 实例的描述。
- 7 键入 TCP 端口号。
默认端口为 443。
- 8 （可选）如果 vCenter Server 部署在 VMware Cloud on AWS 上，请选择 **VMware Cloud on AWS**。
有关将 Horizon 7 与 VMware Cloud on AWS 集成的更多信息，请参阅《Horizon 7 集成指南》文档。
- 9 在“高级设置”下，设置 vCenter Server 和 Horizon Composer 操作的并发操作数限制。
- 10 单击 **下一步**，然后按照提示完成向导。

后续步骤

配置 Horizon Composer 设置。

- 如果为 vCenter Server 实例配置了 TLS 签名证书，且连接服务器信任根证书，则“添加 vCenter Server”向导会显示“Horizon Composer 设置”页面。
- 如果为 vCenter Server 实例配置了默认证书，则必须先确定是否接受现有证书的指纹。请参阅[接受默认 TLS 证书的指纹](#)。

如果 Horizon 7 使用多个 vCenter Server 实例，请重复执行此步骤添加其他 vCenter Server 实例。

配置 Horizon Composer 设置

要使用 Horizon Composer，您必须配置允许 Horizon 7 连接到 Horizon Composer 服务的设置。Horizon Composer 可安装在独立的主机上，也可与 vCenter Server 安装在同一主机上。

在每个 Horizon Composer 服务和 vCenter Server 实例之间必须存在一对一的映射关系。每个 Horizon Composer 服务仅适用于一个 vCenter Server 实例。每个 vCenter Server 实例仅能与一个 Horizon Composer 服务相关联。

完成初始 Horizon 7 部署后，您可以将 Horizon Composer 服务迁移到新的主机以支持对 Horizon 7 部署进行扩展或更改。您可以在 Horizon Console 中编辑初始 Horizon Composer 设置，但是必须执行其他一些步骤来确保迁移成功。

前提条件

- 确认您在 Active Directory 中创建了一个有权从您的链接克隆所在 Active Directory 域添加和删除虚拟机的用户。请参阅[为 Horizon Composer AD 操作创建用户帐户](#)。
- 确认您已将 Horizon 7 配置为连接到 vCenter Server。为此，您必须完成“添加 vCenter Server”向导中的“vCenter Server 信息”页面。请参阅在[Horizon Console 中将 vCenter Server 实例添加到 Horizon 7](#)。
- 确认该 Horizon Composer 服务尚未配置为连接到不同的 vCenter Server 实例。

步骤

- 1 在 Horizon Console 中，导航到**设置 > 服务器**。
- 2 在 **vCenter Server** 选项卡上，单击**添加**并填写 **vCenter Server 设置**页面上的 vCenter Server 信息，然后单击**下一步**。
- 3 在 **Horizon Composer 设置**页面上，如果您未使用 Horizon Composer，请选择**不使用 Horizon Composer**。

如果选择**不使用 Horizon Composer**，则其他的 Horizon Composer 设置将无效。单击**下一步**后，“添加 vCenter Server”向导会显示**存储设置**页面。

4 如果您使用 Horizon Composer，请选择 Horizon Composer 主机的位置。

选项	说明
Horizon Composer 与 vCenter Server 安装在同一主机上。	a 选择 Horizon Composer 与 vCenter Server 一同安装 。 b 确保端口号与您在 vCenter Server 上安装 Horizon Composer 服务时指定的端口号相同。默认端口号为 18443。
Horizon Composer 安装在独立的主机上。	a 选择 独立的 Horizon Composer Server 。 b 在 Horizon Composer Server 地址文本框中，键入 Horizon Composer 主机的完全限定域名 (FQDN)。 c 键入 Horizon Composer 用户的名称。 例如: domain.com\user 或 user@domain.com d 键入 Horizon Composer 用户的密码。 e 确保端口号与您安装 Horizon Composer 服务时指定的端口号相同。默认端口号为 18443。

5 单击下一步以显示 **Horizon Composer 域** 页面。

后续步骤

配置 Horizon Composer 域。

- 如果为 Horizon Composer 实例配置了 TLS 签名证书，且连接服务器信任根证书，则“添加 vCenter Server”向导会显示“Horizon Composer 域”页面。
- 如果为 Horizon Composer 实例配置了默认证书，则必须先确定是否接受现有证书的指纹。

配置 Horizon Composer 域

您必须配置一个 Active Directory 域，以便 Horizon Composer 在其中部署链接克隆桌面。您可以为 Horizon Composer 配置多个域。首次将 vCenter Server 和 Horizon Composer 设置添加到 Horizon 7 后，您可以通过在 Horizon Console 中编辑 vCenter Server 实例来添加更多 Horizon Composer 域。

前提条件

- 您的 Active Directory 管理员必须为 AD 操作创建 Horizon Composer 用户。此域用户必须具有在包含链接克隆的 Active Directory 域中添加和移除虚拟机的权限。有关此用户所需权限的信息，请参阅[为 Horizon Composer AD 操作创建用户帐户](#)。
- 在 Horizon Console 中，确认您已完成[添加 vCenter Server](#) 向导中的 **vCenter Server 设置**和 **Horizon Composer 设置**页面。

步骤

- 1 在 Horizon Console 中，导航到**设置 > 服务器**。
- 2 在 **vCenter Server** 选项卡上，单击**添加**并填写 **vCenter Server 设置**页面上的 vCenter Server 信息，然后单击**下一步**。

- 3 在 **Horizon Composer 设置** 页面上，如果您使用 Horizon Composer，请选择 Horizon Composer 主机的位置，然后单击 **下一步**。

有关 Horizon Composer 的更多信息，请参阅[配置 Horizon Composer 设置](#)。

- 4 在 **Horizon Composer 域** 页面上，单击 **添加**，为 AD 操作帐户信息添加 Horizon Composer 用户。

- 5 键入 Active Directory 域的域名。

例如: **domain.com**

- 6 键入 Horizon Composer 用户的域用户名，包括域名。

例如: **domain.com\admin**

- 7 键入帐户密码。

- 8 单击 **确定**。

- 9 要添加在部署链接克隆池的其他 Active Directory 域中具有特权的域用户帐户，请重复以上的步骤。

- 10 单击 **下一步** 以显示 **存储设置** 页面。

后续步骤

启用虚拟机磁盘空间回收，并为 Horizon 7 配置 Horizon Storage Accelerator。

在 Horizon Console 中添加即时克隆域管理员

必须先向 Horizon 7 中添加即时克隆域管理员，然后才能创建即时克隆桌面池。

前提条件

- 确认即时克隆域管理员具有所需的 Active Directory 域特权。有关更多信息，请参阅《Horizon 7 安装指南》文档中的“为即时克隆操作创建用户帐户”。

步骤

- 1 在 Horizon Console 中，选择 **设置 > 即时克隆域帐户**。
- 2 单击 **添加**。
- 3 选择即时克隆域管理员的域。
- 4 输入用户名和密码。

后续步骤

在 Horizon Console 中，您可以添加或移除即时克隆域管理员，也可以将即时克隆管理员列表导出到 Microsoft Excel。导航到 **设置 > 即时克隆域帐户**，然后选择一个即时克隆域管理员。单击 **编辑** 可编辑该管理员的域和登录信息。单击 **移除** 可移除管理员。单击“导出”图标可将即时克隆管理员列表导出到 Microsoft Excel 文件。

允许 vSphere 回收链接克隆虚拟机中的磁盘空间

在 vSphere 版本 5.1 或更高版本中，可以启用 Horizon 7 的磁盘空间回收功能。Horizon 7 能够以高效的磁盘格式创建链接克隆虚拟机，这种磁盘格式允许 ESXi 主机回收链接克隆中未使用的磁盘空间，从而减少链接克隆所需的总存储空间。

随着用户与链接克隆桌面的交互，克隆的操作系统磁盘会逐渐增大，最终会使用几乎与完整克隆桌面相同的磁盘空间。磁盘空间回收有助于减少操作系统磁盘的大小，无需刷新或重构链接克隆。在虚拟机处于开启状态时以及用户与远程桌面交互时，都可以回收空间。

对于无法利用存储空间节省策略（例如，注销时刷新）的部署来说，磁盘空间回收功能尤其有用。例如，在专用远程桌面上安装用户应用程序的知识型员工在远程桌面刷新或重构时，可能会丢失自己的个人应用程序。通过磁盘空间回收，Horizon 7 可以将链接克隆的大小保持在接近于这些克隆初次置备后启动时的较小大小。

此功能由两部分组成：节省空间的磁盘格式和空间回收操作。

在 vSphere 版本 5.1 或更高版本中，如果父虚拟机的虚拟硬件版本为 9 或更高版本，无论是否启用空间回收操作，Horizon 7 都会创建具有能节省空间的操作系统磁盘的链接克隆。

要启用空间回收操作，您必须使用 Horizon Console 启用 vCenter Server 的空间回收，并回收各桌面池的虚拟机磁盘空间。vCenter Server 的空间回收设置支持您在所有受 vCenter Server 实例管理的桌面池上禁用此功能。禁用 vCenter Server 的该功能会覆盖桌面池级别的设置。

以下指导原则适用于空间回收功能：

- 仅对链接克隆上能节省空间的操作系统磁盘有效。
- 不会影响 Horizon Composer 永久磁盘。
- 仅适用于虚拟硬件版本为 9 或更高版本的虚拟机上的 vSphere 版本 5.1 或更高版本。
- 不适用于完整克隆桌面。
- 适用于具有 SCSI 控制器的虚拟机。不支持 IDE 控制器。

如果池中包含具有能节省空间的磁盘的虚拟机，则不支持本地 NFS 快照技术 (VAAI)。

前提条件

- 确认 vCenter Server 和 ESXi 主机（包括群集中的所有 ESXi 主机）版本为 5.1，且具有 ESXi 5.1 下载补丁程序 ESXi510-201212001 或更高版本。

步骤

- 1 在 Horizon Console 中，导航到**设置 > 服务器**。
- 2 在 **vCenter Server** 选项卡上，单击**添加**，然后完成**添加 vCenter Server** 向导页面，之后会显示**存储设置**页面。
- 3 在**存储设置**页面上，选择**回收虚拟机磁盘空间**。

如果是执行 Horizon 7 的全新安装，则默认已选中此选项。如果是升级到 Horizon 7 的更高版本，则必须选择**回收虚拟机磁盘空间**。

后续步骤

在**存储设置**页面上，配置 Horizon Storage Accelerator。

要完成 Horizon 7 中的磁盘空间回收配置，需要为桌面池设置空间回收。

为 vCenter Server 配置 Horizon Storage Accelerator

在 vSphere 中，您可以将 ESXi 主机配置为缓存虚拟机磁盘数据。这项称为 Horizon Storage Accelerator 的功能可以使用 ESXi 主机中的 Content Based Read Cache (CBRC) 功能。Horizon Storage Accelerator 可以在发生 I/O 风暴（大量虚拟机同时启动或同时运行防病毒扫描时可能会发生）时提高 Horizon 7 性能。对于需要频繁加载应用程序或数据的管理员或用户来说，这项功能同样有益。主机不再从存储系统中一遍遍地读取整个操作系统或应用程序，而是从缓存中读取常规数据块。

通过在发生引导风暴时减少 IOPS 数量，Horizon Storage Accelerator 可降低对存储阵列的需求，使您能够用更少的存储 I/O 带宽支持 Horizon 7 部署。

您需要按照此过程中所述，在 Horizon Console 的**添加 vCenter Server** 向导中选择 Horizon Storage Accelerator 设置，以启用 ESXi 主机上的缓存功能。

请确保也为各桌面池配置了 Horizon Storage Accelerator。要对某个桌面池进行操作，必须为 vCenter Server 和该桌面池启用 Horizon Storage Accelerator。

默认情况下，会为桌面池启用 Horizon Storage Accelerator。可以在创建或编辑池时禁用或启用此功能。最佳方法是在首次创建桌面池时启用此功能。如果通过编辑现有池来启用此功能，您必须确保先创建新副本及其摘要磁盘，再置备链接克隆。可以通过将池重构为新的快照或者将池重新平衡为新的数据存储来创建新副本。仅当桌面池中的虚拟机处于关闭状态时，才能为它们配置摘要文件。

您可以在包含链接克隆的桌面池和包含完整虚拟机的池中启用 Horizon Storage Accelerator。

启用了 Horizon Storage Accelerator 的池不支持本地 NFS 快照技术 (VAAI)。

Horizon Storage Accelerator 现在可在使用 Horizon 7 副本分层的配置下运行，在此配置下，副本存储于单独的数据存储中，而不是链接克隆中。虽然将 Horizon Storage Accelerator 与 Horizon 7 副本分层搭配使用在性能方面并没有太大的实质性提升，但是通过将副本存储到单独的数据存储，还是能够带来一些容量方面的好处。因此，我们对这种组合方式进行了测试，并提供支持。

重要事项 如果您计划使用此功能，并且正在使用多个共享某些 ESXi 主机的 Horizon 7 容器，则必须为共享的 ESXi 主机上的所有池启用 Horizon Storage Accelerator 功能。如果多个容器中的设置不一致，可能会导致共享 ESXi 主机上的虚拟机出现不稳定。

前提条件

- 确认 vCenter Server 和 ESXi 主机版本为 5.1 或更高。

在 ESXi 群集中，确认所有主机的版本均为 5.1 或更高。

- 确认在 vCenter Server 中为 vCenter Server 用户分配了**主机 > 配置 > 高级设置**特权。

请参阅《Horizon 7 安装指南》文档中有关介绍 vCenter Server 用户所需的 Horizon 7 和 Horizon Composer 特权的主题。

步骤

- 1 在 Horizon Console 中，导航到**设置 > 服务器**。
- 2 在 **vCenter Server** 选项卡上，单击**添加**，然后完成**添加 vCenter Server** 向导页面，完成这些页面后会显示**存储设置**页面。
- 3 在**存储设置**页面上，选择**启用 Horizon Storage Accelerator**。
默认情况下，此选项处于选定状态。
- 4 指定默认的主机缓存大小。
默认的缓存大小适用于此 vCenter Server 实例管理的所有 ESXi 主机。
默认值为 1,024 MB。缓存大小必须在 100 MB 和 2,048 MB 之间。
- 5 要为单个 ESXi 主机指定不同的缓存大小，请选择 ESXi 主机并单击**编辑缓存大小**。
 - a 在“主机缓存”对话框中，选中 **覆盖默认主机缓存大小**。
 - b 键入一个介于 100 MB 和 2,048 MB 之间的**主机缓存大小**值，并单击**确定**。
- 6 在“存储设置”页面上，单击**下一步**。
- 7 检查**即将完成**页面上的设置后，单击**提交**。

后续步骤

配置客户端会话和连接设置。请参阅《Horizon 7 管理指南》文档中的“配置客户端会话设置”。

要完成 Horizon 7 中的 Horizon Storage Accelerator 设置，请为桌面池配置 Horizon Storage Accelerator。请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“为桌面池配置 Horizon Storage Accelerator”。

vCenter Server 和 Horizon Composer 的并发操作数限制

在将 vCenter Server 添加到 Horizon 7 或编辑 vCenter Server 设置时，您可以配置多个选项，这些选项用来设置由 vCenter Server 和 Horizon Composer 所执行的并发操作的最大数量。

可以在**添加 vCenter Server** 向导的 **vCenter Server 设置** 页面上的“高级设置”面板中配置这些选项。

表 3-1. vCenter Server 和 Horizon Composer 的并发操作数限制

设置	说明
最大并发 vCenter 置备操作数量	<p>确定连接服务器在此 vCenter Server 实例中置备和删除完整虚拟机时可以发出的最大并发请求数。</p> <p>默认值为 20。</p> <p>此设置仅适用于完整的虚拟机。</p>
最大并发电源操作数量	<p>确定此 vCenter Server 实例中的连接服务器所管理的虚拟机上可以发生的最大并发电源操作数（启动、关闭、挂起等）。</p> <p>默认值为 50。</p> <p>有关计算该设置的值的指导原则，请参阅设置并发电源操作率来支持远程桌面登录风暴。</p> <p>此设置适用于完整的虚拟机和链接克隆。</p>

设置	说明
最大并发 Horizon Composer 维护操作数	<p>确定在此 Horizon Composer 实例所管理的链接克隆上可以发生的最大并发 Horizon Composer 刷新、重构和重新平衡操作数。</p> <p>默认值为 12。</p> <p>必须先注销包含活动会话的远程桌面，然后才能开始维护操作。如果强制用户在维护操作开始时立即注销，则需要注销的远程桌面上的最大并发操作数将只达到所配置的值的一半。例如，如果将此设置配置为 24，并强制用户注销，则需要注销的远程桌面上的最大并发操作数为 12。</p> <p>此设置仅适用于链接克隆。</p>
最大并发 Horizon Composer 置备操作数	<p>确定在此 Horizon Composer 实例所管理的链接克隆上可以发生的最大并发创建和删除操作数。</p> <p>默认值为 8。</p> <p>此设置仅适用于链接克隆。</p>
最大并发即时克隆引擎操作数	<p>确定在此 vCenter Server 实例所管理的即时克隆上可以发生的最大并发创建和删除操作数。</p> <p>此设置仅适用于即时克隆。</p>

设置并发电源操作率来支持远程桌面登录风暴

最大并发电源操作数量设置用于控制可在 vCenter Server 实例的远程桌面虚拟机上发生的最大并发电源操作数量。这一限制默认设置为 50。当大量用户同时登录其桌面时，可更改此值以支持开机峰值速率。

作为最佳实践，您可通过试运行来确定此设置的正确值。有关规划指导原则，请参阅《Horizon 7 架构规划指南》文档中的“体系结构设计元素与规划指导原则”。

所需并发电源操作数量基于桌面开启的峰值速率，以及桌面开启、引导到可供连接所花费的时间。总之，建议的电源操作限制值就是桌面启动所花费的总时间乘以开机峰值速率。

例如，桌面的平均启动时间在二到三分钟之间。因此，并发电源操作限制值应是开机峰值速率的 3 倍。默认设置 50 应该可支持每分钟 16 个桌面的开机峰值速率。

系统等待桌面启动的最长时间为五分钟。如果启动时间更长的话，有可能会出现其他错误。为了保守起见，您可将并发电源操作限制值设为开机峰值速率的 5 倍。采用这种谨慎方法，默认设置 50 可以支持每分钟 10 个桌面的开机峰值速率。

登录操作以及桌面开启操作，通常会平均分布在特定时段内。您可以估算开机峰值速率，方法是：假设开机峰值发生在时段中间，在此期间大约 40% 的开机操作发生在该时段的 1/6 时间内。例如，如果用户在上午 8:00 到 9:00 之间登录，时段为一小时，40% 的登录操作会发生在上午 8:25 到 8:35 这 10 分钟之内。如果有 2000 名用户，其中 20% 的用户关闭了桌面，那么这 400 个桌面开启操作中会有 40% 发生在这 10 分钟之内。开机峰值速率为每分钟 16 个桌面。

接受默认 TLS 证书的指纹

在向 Horizon 7 添加 vCenter Server 和 Horizon Composer 实例时，必须确保用于 vCenter Server 和 Horizon Composer 实例的 TLS 证书有效且受连接服务器信任。如果随 vCenter Server 和 Horizon Composer 一起安装的默认证书仍然存在，则必须确定是否接受这些证书的指纹。

如果为 vCenter Server 或 Horizon Composer 实例配置了 CA 签发的证书，且根证书受连接服务器信任，则无需接受证书指纹。无需采取任何操作。

如果使用 CA 签发的证书替换默认证书，但连接服务器不信任根证书，则必须确定是否接受证书指纹。指纹是证书的加密哈希值。通过指纹可以快速确定提供的证书是否与另一个证书（例如之前接受的证书）相同。

注 如果您在同一 Windows Server 主机上安装 vCenter Server 和 Horizon Composer，它们可以使用相同的 TLS 证书，但必须单独为每个组件配置证书。

有关配置 TLS 证书的详细信息，请参阅《Horizon 7 安装指南》文档中的“为 Horizon 7 Server 配置 TLS 证书”。

您需要首先在 Horizon Console 中使用**添加 vCenter Server** 向导添加 vCenter Server 和 Horizon Composer。如果证书不受信任而您也未接受指纹，则无法添加 vCenter Server 和 vCenter Server。

添加这些服务器后，您可以在**编辑 vCenter Server** 对话框中重新配置它们。

注 从较早的版本进行升级时，如果 vCenter Server 或 Horizon Composer 证书不受信任，或者您使用不受信任的证书替换了受信任证书，您也必须接受证书指纹。

步骤

- 1 当 Horizon Console 显示“检测到无效的证书”对话框时，单击**查看证书**。
- 2 检查“证书信息”窗口中的证书指纹。
- 3 检查为 vCenter Server 或 Horizon Composer 实例配置的证书指纹。
 - a 在 vCenter Server 或 Horizon Composer 主机上，启动 MMC 管理单元并打开 Windows 证书存储区。
 - b 导航到 vCenter Server 或 Horizon Composer 证书。
 - c 单击“证书详细信息”选项卡显示证书指纹。

同样还需要检查 SAML 身份验证器的证书指纹。如果可以，请针对 SAML 身份验证器主机执行之前的步骤。
- 4 验证“证书信息”窗口中的指纹是否与 vCenter Server 或 Horizon Composer 实例的指纹相匹配。

同样还需要验证这些指纹是否与 SAML 身份验证器相匹配。
- 5 确定是否接受证书指纹。

选项	说明
指纹匹配。	单击 接受 以使用默认证书。
指纹不匹配。	单击 拒绝 。 对不匹配的证书进行故障排除。例如，您可能为 vCenter Server 或 Horizon Composer 提供了错误的 IP 地址。

从 Horizon 7 中移除 vCenter Server 实例

您可以移除 Horizon 7 与 vCenter Server 实例之间的连接。移除后，Horizon 7 将不再管理在该 vCenter Server 实例中创建的虚拟机。

前提条件

删除所有与 vCenter Server 实例关联的虚拟机。有关删除虚拟机的更多信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“删除桌面池”。

步骤

- 1 在 Horizon Console 中，导航到**设置 > 服务器**。
- 2 在 **vCenter Server** 选项卡上，选择 vCenter Server 实例。
- 3 单击**移除**。

此时会显示一条对话框消息，警告您 Horizon 7 将不再能够访问由此 vCenter Server 实例管理的虚拟机。

- 4 单击**确定**。

Horizon 7 无法再访问在 vCenter Server 实例中创建的虚拟机。

从 Horizon 7 中移除 Horizon Composer

您可以移除 Horizon 7 和已关联到 vCenter Server 实例的 Horizon Composer 服务之间的连接。

在禁用与 Horizon Composer 的连接之前，您必须从 Horizon 7 中移除由 Horizon Composer 创建的所有链接克隆虚拟机。如果仍存在任何关联的链接克隆，Horizon 7 会阻止您移除 Horizon Composer。禁用与 Horizon Composer 的连接之后，Horizon 7 将无法置备或管理新的链接克隆。

步骤

- 1 移除由 Horizon Composer 创建的链接克隆桌面池。

- a 在 Horizon Console 中，选择**清单 > 桌面**。
- b 选择链接克隆桌面池并单击**删除**。

这时将出现一个对话框，警告您将从 Horizon 7 中永久删除链接克隆桌面池。如果链接克隆虚拟机是使用永久磁盘配置的，您可以分离或删除永久磁盘。

- c 单击**确定**。

随后将从 vCenter Server 中删除虚拟机。此外，还将移除关联的 Horizon Composer 数据库条目以及由 Horizon Composer 创建的副本。

- d 对由 Horizon Composer 创建的每个链接克隆桌面池重复执行这些步骤。

- 2 导航到**设置 > 服务器**。
- 3 在 **vCenter Server** 选项卡上，选择与 Horizon Composer 关联的 vCenter Server 实例。
- 4 单击**编辑**。

- 5 在 **Horizon Composer** 选项卡上的“Horizon Composer Server 设置”下方，选择**不使用 Horizon Composer**，然后单击**确定**。

您将无法再在此 vCenter Server 实例中创建链接克隆桌面池，但您可以继续在 vCenter Server 实例中创建及管理完整虚拟机桌面池。

后续步骤

如果您想要在其他主机上安装 Horizon Composer 并将 Horizon 7 重新配置为连接到新的 Horizon Composer 服务，则必须执行一些额外的步骤。有关如何在不迁移链接克隆虚拟机的情况下迁移 Horizon Composer 的更多信息，请参阅《Horizon 7 管理指南》文档。

vCenter Server 唯一 ID 冲突

如果在您的环境中配置了多个 vCenter Server 实例，添加新实例时可能会因为唯一 ID 冲突而失败。

问题

您尝试向 Horizon 7 中添加一个 vCenter Server 实例，但是新 vCenter Server 实例的唯一 ID 与现有实例的 ID 冲突。

原因

两个 vCenter Server 实例不能使用相同的唯一 ID，默认情况下，vCenter Server 唯一 ID 是随机生成的，但您可以对它进行编辑。

解决方案

- 1 在 vSphere Client 中，单击**管理 > vCenter Server 设置 > 运行时设置**。
- 2 键入一个新的唯一 ID，然后单击**确定**。

有关编辑 vCenter Server 唯一 ID 值的详细信息，请参阅 vSphere 文档。

在 Horizon Console 中备份 Horizon 连接服务器

完成对 Horizon 连接服务器的初始配置后，您应当计划对 Horizon 7 和 Horizon Composer 配置数据进行定期备份。

有关备份和还原 Horizon 7 配置的信息，请参阅[备份 Horizon 连接服务器](#)和[Horizon Composer 数据](#)。

在 Horizon Console 中配置客户端会话设置

您可以对能够影响由连接服务器实例或复制组管理的客户端会话和连接的全局设置进行配置。您可以设置会话超时长度，显示登录前消息和警告消息，以及设置安全相关客户端连接选项。

Horizon Console 中客户端会话的全局设置

常规全局设置决定会话超时时长、SSO 实现和超时限制、Horizon Console 中的状态更新、是否显示登录前提示和警告消息、Horizon Console 是否将 Windows Server 视为支持的远程桌面操作系统，以及其他设置。

对下表中任何设置所做的更改都将立即生效。您不需要重新启动 Horizon 7 连接服务器或 Horizon Client。

表 3-2. 客户端会话的常规全局设置

设置	说明
View Administrator 会话超时	<p>确定 Horizon Console 会话持续闲置多久后超时。</p> <hr/> <p>重要事项 Horizon Console 会话超时值（以分钟为单位）设置较高会增加未授权使用 Horizon Console 的风险。允许闲置会话持续较长时间时应慎重考虑。</p> <hr/> <p>默认情况下，Horizon Console 会话超时为 30 分钟。可将会话超时时间设置为 1 到 4320 分钟（72 小时）间的任何值。</p>
强制断开用户连接	<p>自用户登录到 Horizon 7 时起达到指定分钟数后，断开所有桌面和应用程序连接。无论桌面和应用程序是被用户何时打开的，都将同时断开连接。</p> <p>对于不支持应用程序远程的客户端，如果此设置的值为从不或大于 1200 分钟，将应用 1200 分钟的最大超时值。</p> <p>默认值为 600 分钟之后。</p>
单点登录 (SSO)	<p>如果启用了 SSO，Horizon 7 可缓存用户的凭据，使用户不必提供凭据登录远程 Windows 会话便可启动远程桌面或应用程序。默认值为已启用。</p> <p>如果您打算使用 Horizon 7 或更高版本中引入的 True SSO 功能，则必须启用 SSO。通过 True SSO，当用户使用 Active Directory 凭据以外的其他某种身份验证形式登录时，在用户登录到 VMware Identity Manager 后，True SSO 功能会生成短期证书以供使用，而不是生成缓存凭据。</p> <hr/> <p>注 如果桌面是从 Horizon Client 中启动，并被用户或 Windows 根据安全策略锁定，并且运行的是 Horizon 7 Agent 6.0 或更高版本或者 Horizon Agent 7.0 或更高版本，Horizon 7 连接服务器将放弃用户的 SSO 凭据。用户必须提供登录凭据才能启动新桌面或新应用程序，或者重新连接到任何已断开连接的桌面或应用程序。要再次启用 SSO，用户必须断开与 Horizon 7 连接服务器的连接或退出 Horizon Client，然后重新连接 Horizon 7 连接服务器。但是，如果桌面是从 Workspace ONE 或 VMware Identity Manager 中启动，当桌面被锁定时，将不会丢弃 SSO 凭据。</p>
启用自动状态更新	<p>确定 Horizon Console 左上角的全局状态窗格是否每隔几分钟显示一次状态更新。Horizon Console 的仪表板页面也会每隔几分钟更新一次。</p> <p>默认情况下不启用此设置。</p>

设置	说明
对于支持应用程序的客户端。 如果用户停止使用键盘和鼠标，断开应用程序连接并放弃 SSO 凭据：	<p>在客户端设备上无键盘或鼠标活动时保护应用程序会话。如果设置为 …分钟之后，Horizon 7 将在无用户活动达到指定的分钟数后断开所有应用程序连接并放弃 SSO 凭据。桌面会话不会断开连接。用户必须重新登录以重新连接被断开的应用程序或者启动新的桌面或应用程序。</p> <p>此设置也适用于 True SSO 功能。丢弃 SSO 凭据后，系统将提示用户提供 Active Directory 凭据。如果用户登录 VMware Identity Manager 时未使用 AD 凭据，并且也不知道要输入的 AD 凭据是什么，则用户可以注销 VMware Identity Manager，然后重新登录，以访问其远程桌面和应用程序。</p> <hr/> <p>重要事项 用户必须注意，当他们同时打开了应用程序和桌面时，应用程序会因为超时而断开连接，桌面则会保持连接。用户不能依赖此超时来保护他们的桌面。</p> <hr/> <p>如果设置为从不，Horizon 7 将绝不会因用户不活动而断开应用程序连接或放弃 SSO 凭据。</p> <p>默认值为从不。</p>
其他客户端。 放弃 SSO 凭据：	<p>在指定的分钟后放弃 SSO 凭据。此设置适用于不支持应用程序远程的客户端。如果设置为 …分钟之后，那么自用户登录到 Horizon 7 时起达到指定分钟数后，用户必须重新登录以连接到桌面，而不管客户端设备上的用户活动情况如何。</p> <p>如果设置为从不，Horizon 7 将存储 SSO 凭据，直到用户关闭 Horizon Client 或达到强制断开用户连接超时值为止（以先发生者为准）。</p> <p>默认值为 15 分钟之后。</p>
显示登录前的消息	<p>当 Horizon Client 用户登录时，向其显示免责声明或其他消息。</p> <p>在“全局设置”对话框的文本框中键入您的信息或说明。</p> <p>如果不希望显示任何消息，请不要选中该复选框。</p>
强制注销前显示警告	<p>当用户因为计划更新或即时更新（如要开始桌面刷新操作）被强制注销时，显示一条警告信息。此设置还可确定从显示警告到注销用户之间的时间间隔。</p> <p>选中该框可显示警告消息。</p> <p>键入从显示警告到注销用户之间的分钟数。默认值是 5 分钟。</p> <p>键入您的警告消息。您可以使用默认的消息：</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>您的桌面将按计划执行一项重要更新，并将在 5 分钟后关闭。请立即保存尚未保存的工作。</p> </div>
启用 Windows Server 桌面	<p>决定是否可以选择可用的 Windows Server 2008 R2 和 Windows Server 2012 R2 计算机用作桌面。启用此设置后，Horizon Console 将显示所有可用的 Windows Server 计算机，包括安装了 Horizon 7 Server 组件的计算机。</p> <hr/> <p>注 Horizon Agent 软件无法与任何其他 Horizon 7 server 软件组件（包括安全服务器、Horizon 7 连接服务器或 Horizon 7 Composer）共存于同一虚拟机或物理机上。</p>
关闭 HTML Access 的选项卡时清除凭据	<p>当用户在 HTML Access Client 中关闭连接到远程桌面或应用程序的选项卡，或者关闭连接到桌面和应用程序选择页面的选项卡时，从缓存中移除用户的凭据。</p> <p>启用此设置时，在以下 HTML Access 客户端场景中，Horizon 7 也会从缓存中移除凭据：</p> <ul style="list-style-type: none"> ■ 用户刷新桌面和应用程序选择页面或远程会话页面。 ■ 服务器提供自签名证书，用户启动远程桌面或应用程序，并且用户在系统显示安全警告时接受证书。 ■ 用户在包含远程会话的选项卡中运行 URI 命令。 <p>如果禁用此设置，则凭据将保留在缓存中。默认情况下将禁用此功能。</p> <hr/> <p>注 此功能在 Horizon 7 版本 7.0.2 及更高版本中可用。</p>

设置	说明
在客户端用户界面中隐藏服务器信息	启用此安全设置，在 Horizon Client 4.4 或更高版本中隐藏服务器 URL 信息。
在客户端用户界面中隐藏域列表	<p>启用此安全设置，在 Horizon Client 4.4 或更高版本中隐藏域下拉菜单。</p> <p>在用户登录到启用了在客户端用户界面中隐藏域列表全局设置的连接服务器实例时，将在 Horizon Client 中隐藏域下拉菜单，用户可以在 Horizon Client 用户名文本框中提供域信息。例如，用户必须按照 domain\username 或 username@domain 格式输入其用户名。</p> <p>重要事项 如果启用在客户端用户界面中隐藏域列表设置，并为连接服务器实例选择双因素身份验证（RSA SecureID 或 RADIUS），则不要强制实施 Windows 用户名匹配。实施 Windows 用户名匹配将禁止用户在用户名文本框中输入域信息，登录将始终失败。如果具有单个用户域，则该功能不适用于 Horizon Client 5.0 和更高版本。</p> <p>重要事项 有关该设置的安全性和可用性影响的更多信息，请参阅《Horizon 7 安全指南》文档。</p>

Horizon Console 中客户端会话和连接的全局安全性设置

全局安全性设置决定了网络中断后是否对客户端重新进行身份验证、是否启用消息安全模式以及是否增强安全状态。

到 Horizon 7 的所有 Horizon Client 连接和 Horizon Console 连接都需要使用 TLS。如果您的 Horizon 7 部署使用负载均衡器或其他面向客户端的中间服务器，可以将 TLS 负载分流到这些负载均衡器或中间服务器，然后在单个连接服务器实例和安全服务器上配置非 TLS 连接。

表 3-3. 客户端会话和连接的全局安全性设置

设置	说明
网络中断后对安全加密链路连接重新进行身份验证	<p>在 Horizon Client 使用安全加密链路连接访问远程桌面的情况下，决定网络中断后是否必须对用户凭据重新进行身份验证。</p> <p>如果选择此设置，当安全加密链路连接中断时，Horizon Client 会要求用户重新进行身份验证，然后才能重新连接。</p> <p>此设置可提高安全性。例如，如果一台笔记本电脑被盗并转移到其他网络，用户在不输入凭据的情况下，将无法自动获得对远程桌面的访问权限。</p> <p>如果不选择此设置，客户端将重新连接到远程桌面，而不要求用户重新进行身份验证。</p> <p>不使用安全加密链路时，此设置无效。</p>
消息安全模式	<p>确定用于在各个组件之间发送 JMS 消息的安全机制</p> <ul style="list-style-type: none"> ■ 当此模式设置为已启用时，将会对 Horizon 7 组件之间传输的 JMS 消息进行签名和验证。 ■ 如果将该模式设置为已增强，将会通过相互身份验证的 TLS，JMS 连接和对 JMS 主题的访问控制来提供安全功能。 <p>对于新安装，默认情况下消息安全模式设置为已增强。如果从先前版本进行升级，则将保留在先前版本中使用的设置。</p>
增强安全状态（只读）	<p>将消息安全模式从已启用更改为已增强时显示的只读字段。由于更改分阶段进行，此字段根据阶段显示进度：</p> <ul style="list-style-type: none"> ■ 等待 Message Bus 重新启动是第一阶段。此状态将一直显示，直到您手动重新启动容器中的所有连接服务器实例或容器中所有连接服务器主机上的 VMware Horizon Message Bus 组件服务。 ■ 等待增强是下一阶段。重新启动所有 Horizon Message Bus 组件服务后，系统开始将所有桌面和安全服务器的消息安全模式更改为已增强。 ■ 已增强是最终状态，表明所有组件现在正使用已增强消息安全模式。

在 Horizon Console 中禁用或启用 Horizon 连接服务器

您可以禁用连接服务器实例，以阻止用户登录到其虚拟或发布的桌面和应用程序。禁用实例后，可以重新启用。

禁用某个连接服务器实例时，当前已登录到桌面和应用程序的用户不会受到影响。

您的 Horizon 7 部署决定了禁用实例会对用户产生怎样的影响。

- 如果是单一独立的连接服务器实例，用户将无法登录到其桌面或应用程序。他们无法连接到连接服务器。
- 如果是连接服务器副本实例，那么您的网络拓扑结构将确定用户是否可以路由到另一个副本实例。如果用户可以访问另一实例，他们将可以登录到自己的桌面和应用程序。

步骤

- 1 在 Horizon Console 中，选择**设置 > 服务器**。
- 2 在**连接服务器**选项卡上，选择连接服务器实例。
- 3 单击**已禁用**。

您可以通过单击**已启用**再次启用该实例。

编辑 Horizon 连接服务器实例的外部 URL

可以使用 Horizon Console 编辑连接服务器实例的外部 URL。

默认情况下，仅位于同一网络的安全加密链路客户端可以连接到连接服务器主机。在网络外运行的安全加密链路客户端必须使用客户端可解析的 URL 来连接到连接服务器主机。

用户通过 PCoIP 显示协议连接到远程桌面时，Horizon Client 可进一步连接到连接服务器主机上的 PCoIP 安全网关。要使用 PCoIP 安全网关，客户端系统必须能够访问允许该客户端连接到连接服务器主机的 IP 地址。在 PCoIP 外部 URL 中指定此 IP 地址。

第三个 URL 允许用户通过 Blast 安全网关建立安全连接。

安全加密链路外部 URL、PCoIP 外部 URL 和 Blast 外部 URL 都必须是客户端系统用于连接此主机的地址。

步骤

- 1 在 Horizon Console 中，选择**设置 > 服务器**。
- 2 在**连接服务器**选项卡上，选择连接服务器实例，并单击**编辑**。
- 3 在**外部 URL** 文本框中键入安全加密链路的外部 URL。

URL 必须包含协议、客户端可解析的主机名和端口号。

例如：https://horizon.example.com:443

注 当主机名不可解析时，如果您需要访问连接服务器实例，则可以使用 IP 地址。但是，您连接的主机将与为连接服务器实例配置的 TLS 证书不匹配，从而导致访问被阻止或访问的安全性降低。

- 4 在 **PCoIP 外部 URL** 文本框中键入 PCoIP 安全网关的外部 URL。

将 PCoIP 外部 URL 指定为包含端口号 4172 的 IP 地址。请勿包含协议名。

例如：10.20.30.40:4172

URL 中必须包含客户端系统可用于连接到此连接服务器实例的 IP 地址和端口号。

- 5 在 **Blast 外部 URL** 文本框中键入 Blast 安全网关的外部 URL。

URL 必须包含 HTTPS 协议、客户端可解析的主机名和端口号。

例如：https://myserver.example.com:8443

默认情况下，URL 包含安全加密链路外部 URL 的 FQDN 和默认端口号 8443。URL 中必须包含客户端系统可用于连接此主机的 FQDN 和端口号。

- 6 确认此对话框中的所有地址都允许客户端系统连接此主机。
- 7 单击**确定**保存更改。

外部 URL 将立即更新。您无需重新启动连接服务器，所做的更改即可生效。

在 Horizon Console 中注册网关

Horizon Client 会通过您在 Horizon Console 中注册的网关或 Unified Access Gateway 设备进行连接。

您可以在 Horizon Console 中注册或取消注册网关。要取消注册网关，请选择相应的网关或 Unified Access Gateway 设备，然后单击**取消注册**。

步骤

- 1 在 Horizon Console 中，选择**设置 > 服务器**。
- 2 在**网关**选项卡上，单击**注册**。
- 3 输入网关或 Unified Access Gateway 设备的 FQDN。
- 4 单击**确定**。

设置智能卡身份验证

为了增强安全性，可以对连接服务器实例或安全服务器进行配置，以使用户和管理员能够使用智能卡进行身份验证。

智能卡是一种内含计算机芯片的小型塑料卡。其中的芯片就像一个微型计算机，具备数据安全存储，可存储私钥和公钥证书。美国国防部使用的智能卡类型称为通用访问卡 (CAC)。

使用智能卡身份验证时，用户或管理员可以将智能卡插入连接到客户端计算机的智能卡读卡器中，然后输入 PIN。智能卡身份验证通过验证用户是否具有智能卡以及用户是否知道 PIN 来提供双因素身份验证。

有关实现智能卡身份验证的硬件和软件要求的信息，请参阅《Horizon 7 安装指南》文档。Microsoft TechNet 网站中包含为 Windows 系统规划和实施智能卡身份验证方面的详细信息。

要使用智能卡，客户端计算机必须具有智能卡中间件和智能卡读卡器。要在智能卡上安装证书，您必须将一台计算机设置为注册站点。如需了解一个特定类型的 Horizon Client 是否支持智能卡，请参阅 <https://docs.vmware.com/cn/VMware-Horizon-Client/index.html> 网站上的 Horizon Client 文档。

本章讨论了以下主题：

- 使用智能卡登录
- 在 Horizon 连接服务器上配置智能卡身份验证
- 在第三方解决方案上配置智能卡身份验证
- 为智能卡身份验证准备 Active Directory
- 在 Horizon Console 中验证智能卡身份验证配置
- 使用智能卡证书撤销检查

使用智能卡登录

当用户或管理员将智能卡插入智能卡读卡器中后，如果客户端操作系统是 Windows，智能卡上的用户证书将被复制到客户端系统上的本地证书存储中。本地证书存储中的证书可供客户端计算机上运行的所有应用程序（包括 Horizon Client）使用。

当用户或管理员与配置为使用智能卡身份验证的连接服务器实例或安全服务器建立连接时，连接服务器实例或安全服务器将向客户端系统发送受信任的证书颁发机构 (CA) 列表。客户端系统将依据可用的用户证书来检查受信任 CA 列表，选择合适的证书，然后提示用户或管理员输入智能卡 PIN 码。如果存在多个有效的用户证书，客户端系统会提示用户或管理员选择其中一个证书。

客户端系统将用户证书发送给连接服务器实例或安全服务器，连接服务器实例或安全服务器将通过检查证书的信任和有效期限对其进行检验。通常情况下，只要签发了用户证书而且该证书有效，用户和管理员即可成功通过身份验证。如果配置了证书撤销检查，已撤销用户证书的用户或管理员将无法通过身份验证。

在一些环境中，用户的智能卡证书可以映射到多个 **Active Directory** 域用户帐户。用户可能有多个具有管理员权限的帐户，因此需要指定在智能卡登录时“用户名提示”字段中使用哪个帐户。要使 **Horizon Client** 登录对话框中显示“用户名提示”字段，管理员必须在 **Horizon Console** 中为连接服务器实例启用智能卡用户名提示功能。然后，在智能卡登录期间，智能卡用户可以在“用户名提示”字段中输入用户名或 UPN。

如果您的环境使用 **Unified Access Gateway** 设备来确保外部访问的安全，则必须配置 **Unified Access Gateway** 设备，以使其支持智能卡用户名提示功能。仅 **Unified Access Gateway 2.7.2** 和更高版本支持智能卡用户名提示功能。有关在 **Unified Access Gateway** 设备中启用智能卡用户名提示功能的信息，请参阅《部署和配置 **Unified Access Gateway**》文档。

在 **Horizon Client** 中使用智能卡身份验证时，不支持显示协议切换。要在 **Horizon Client** 中使用智能卡进行身份验证后更改显示协议，用户必须注销并重新登录。

在 Horizon 连接服务器上配置智能卡身份验证

要配置智能卡身份验证，您必须获得一个根证书并将其添加到服务器信任存储区文件，修改连接服务器配置属性，并配置智能卡身份验证设置。根据您的具体环境，您可能需要执行附加步骤。

步骤

1 获取证书颁发机构证书

您必须为用户和管理员提供的智能卡上的所有受信任的用户证书获取所有相应的 **CA**（证书颁发机构）证书。如果用户的智能卡证书是由中间证书颁发机构颁发的，则这些证书包括根证书，并且可以包括中间证书。

2 从 Windows 获取 CA 证书

如果您拥有 **CA** 签发的用户证书或包含 **CA** 签发的用户证书的智能卡，且 **Windows** 信任此根证书，则可以从 **Windows** 导出此根证书。如果用户证书的颁发者是中间证书颁发机构，则您可以导出该证书。

3 将 CA 证书添加到服务器信任存储区文件中

您必须将信任的所有用户和管理员的根证书和/或中间证书添加到服务器信任存储区文件中。连接服务器实例和安全服务器使用此信息对智能卡用户和管理员进行身份验证。

4 修改 Horizon 连接服务器配置属性

您必须修改连接服务器上的连接服务器配置属性，才能启用智能卡身份验证。

5 在 Horizon Console 中配置智能卡设置

您可以使用 **Horizon Console** 指定相应设置，以适应不同的智能卡身份验证场景。

获取证书颁发机构证书

您必须为用户和管理员提供的智能卡上的所有受信任的用户证书获取所有相应的 **CA**（证书颁发机构）证书。如果用户的智能卡证书是由中间证书颁发机构颁发的，则这些证书包括根证书，并且可以包括中间证书。

如果您没有获取对用户和管理员提供的智能卡上的证书签名的 **CA** 的根证书或中间证书，则可以从 **CA** 签名的用户证书或包含此类证书的智能卡中导出这些证书。请参阅[从 Windows 获取 CA 证书](#)。

步骤

- ◆ 从以下某个源中获取 **CA** 证书。
 - 运行 **Microsoft** 证书服务的 **Microsoft IIS** 服务器。有关安装 **Microsoft IIS**、颁发证书以及在组织中分发证书的信息，请参见 **Microsoft TechNet** 网站。
 - 受信任的 **CA** 签名的公用根证书。如果环境中具有智能卡基础架构，以及标准的智能卡分发和身份验证方式，就属于最常用的根证书源。

从 Windows 获取 CA 证书

如果您拥有 **CA** 签发的用户证书或包含 **CA** 签发的用户证书的智能卡，且 **Windows** 信任此根证书，则可以从 **Windows** 导出此根证书。如果用户证书的颁发者是中间证书颁发机构，则您可以导出该证书。

步骤

- 1 如果用户证书存储在智能卡上，您只需将智能卡插入读卡器，就可以将用户证书添加到您的个人存储区中。
如果用户证书未显示在您的个人存储区中，可使用读取器软件将用户证书导出到文件中。此文件在该流程的步骤 4 中使用。
- 2 在 **Internet Explorer** 中，选择**工具 > Internet 选项**。
- 3 在**内容选项卡**上，单击**证书**。
- 4 在**个人选项卡**上，选择您要使用的证书，然后单击**查看**。
如果用户证书未显示在列表中，请单击**导入**从文件中手动导入该证书。导入证书后，您就可以从列表中选择该证书。
- 5 在**证书路径选项卡**上，选择树状结构顶端的证书，然后单击**查看证书**。
如果用户证书是作为信任层次结构的一部分签发的，则签发证书可能由另一较高级别的证书签发。选择父证书（即实际签发用户证书的证书）作为您的根证书。在某些情况下，颁发者可能是中间 **CA**。
- 6 在**详细信息选项卡**上，单击**复制到文件**。
屏幕上将显示**证书导出向导**。
- 7 单击**下一步 > 下一步**，然后键入要导出的文件的名称和位置。
- 8 单击**下一步**将该文件作为根证书保存到指定的位置。

将 CA 证书添加到服务器信任存储区文件中

您必须将信任的所有用户和管理员的根证书和/或中间证书添加到服务器信任存储区文件中。连接服务器实例和安全服务器使用此信息对智能卡用户和管理员进行身份验证。

前提条件

- 获取用于对用户或管理员提供的智能卡上的证书进行签名的根证书或中间证书。请参阅[获取证书颁发机构证书](#)和[从 Windows 获取 CA 证书](#)。

重要事项 如果用户的智能卡证书是由中间证书颁发机构颁发的，则这些证书可以包括中间证书。

- 确认 `keytool` 实用程序已添加到连接服务器或安全服务器主机上的系统路径。有关更多信息，请参阅《Horizon 7 安装指南》文档。

步骤

- 1 在连接服务器或安全服务器主机上，使用 `keytool` 实用程序将根证书和/或中间证书导入服务器信任存储区文件中。

例如：

```
keytool -import -alias alias -file root_certificate -keystore truststorefile.key
```

在此命令中，*alias* 是信任存储区文件中新条目的唯一名称（区分大小写），*root_certificate* 是已获得或导出的根证书或中间证书，*truststorefile.key* 是要将根证书添加到的信任存储区文件的名称。如果该文件不存在，请在当前目录中创建。

注 `keytool` 实用程序可能会提示您为信任存储区文件创建密码。如果您以后需要向信任存储区文件中添加更多证书，就必须提供此密码。

- 2 将信任存储区文件复制到连接服务器或安全服务器主机上的 SSL 网关配置文件夹下。

例如：`install_directory\VMware\VMware View\Server\sslgateway\conf`
`\truststorefile.key`

后续步骤

修改连接服务器配置属性以启用智能卡身份验证。

修改 Horizon 连接服务器配置属性

您必须修改连接服务器上的连接服务器配置属性，才能启用智能卡身份验证。

前提条件

将所有可信用户证书的证书颁发机构 (Certificate Authority, CA) 证书添加到服务器信任存储区文件中。如果用户的智能卡证书是由中间证书颁发机构颁发的，则这些证书包括根证书，并且可以包括中间证书。

步骤

- 1 在连接服务器主机的 TLS/SSL 网关配置文件夹中创建或编辑 `locked.properties` 文件。
例如, `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`。
- 2 将 `trustKeyfile`、`trustStoretype` 和 `useCertAuth` 属性添加到 `locked.properties` 文件中。
 - a 将 `trustKeyfile` 属性设为您的信任存储区文件名。
 - b 将 `trustStoretype` 设置为 `jks`。
 - c 将 `useCertAuth` 属性设为 `true`, 以启用证书身份验证。
- 3 重新启动连接服务器服务以使所做的更改生效。

示例: locked.properties 文件

此处所示的文件指定所有受信任用户的根证书位于 `longa.key` 文件中, 将信任存储区类型设置为 `jks`, 并启用了证书身份验证。

```
trustKeyfile=longa.key
trustStoretype=jks
useCertAuth=true
```

后续步骤

如果您为连接服务器实例配置了智能卡身份验证, 请在 Horizon Console 中配置智能卡身份验证设置。

在 Horizon Console 中配置智能卡设置

您可以使用 Horizon Console 指定相应设置, 以适应不同的智能卡身份验证场景。

前提条件

- 在连接服务器主机上修改连接服务器配置属性。
- 确认 Horizon Client 直接与连接服务器或安全服务器主机建立 HTTPS 连接。如果将 TLS 负载分流到中间设备, 将不支持智能卡身份验证。

步骤

- 1 在 Horizon Console 中, 选择**设置 > 服务器**。
- 2 在**连接服务器**选项卡上, 选择连接服务器实例, 并单击**编辑**。

3 要为远程桌面和应用程序用户配置智能卡身份验证，请执行以下步骤。

- a 在**身份验证**选项卡上，从“**Horizon 身份验证**”部分的**用户的智能卡身份验证**下拉菜单中选择一个配置选项。

选项	操作
不允许	在该连接服务器实例上禁用了智能卡身份验证。
可选	用户可以使用智能卡身份验证或密码身份验证连接到该连接服务器实例。如果智能卡身份验证失败，用户就必须提供密码。
需要	<p>用户连接到该连接服务器实例时必须使用智能卡身份验证。</p> <p>要求进行智能卡身份验证时，连接到连接服务器实例时选择以当前用户身份登录复选框的用户的身份验证将失败。这些用户登录到连接服务器时必须用智能卡和 PIN 码重新进行身份验证。</p> <p>注 智能卡身份验证仅可替换 Windows 密码身份验证。如果已启用 SecuriID，用户就必须同时使用 SecuriID 和智能卡身份验证机制进行身份验证。</p>

- b 配置智能卡移除策略。

当智能卡身份验证被设置为**不允许**时，您无法配置智能卡移除策略。

选项	操作
用户移除智能卡后断开用户与连接服务器的连接。	选择 移除智能卡时断开用户会话 复选框。
在用户移除智能卡时保持用户与连接服务器的连接，并允许用户无需重新进行身份验证即可启动新的桌面或应用程序会话。	取消选择 移除智能卡时断开用户会话 复选框。

智能卡移除策略不适用于在选择了**以当前用户身份登录**复选框的情况下连接连接服务器实例的用户，即使他们使用智能卡来登录到其客户端系统，也无法使用此策略。

- c 配置智能卡用户名提示功能。

当智能卡身份验证被设置为**不允许**时，您无法配置智能卡用户名提示功能。

选项	操作
允许用户使用单个智能卡证书对多个用户帐户进行身份验证。	选中 允许智能卡用户名提示 复选框。
禁止用户使用单个智能卡证书对多个用户帐户进行身份验证。	取消选中 允许智能卡用户名提示 复选框。

- 要登录到 Horizon Console 的管理员配置智能卡身份验证，请从 **Horizon Administrator 身份验证** 部分的**管理员的智能卡身份验证**下拉菜单中选择一个配置选项。

选项	操作
不允许	在该连接服务器实例上禁用了智能卡身份验证。
可选	管理员可以使用智能卡身份验证或密码身份验证方式登录到 Horizon Console。如果智能卡身份验证失败，管理员必须提供密码。
需要	管理员必须在登录到 Horizon Console 时使用智能卡身份验证。

- 单击**确定**。

- 重新启动连接服务器服务。

必须重新启动连接服务器服务，对智能卡设置所做的更改才能生效，但有一个例外。您可以在**可选**和**必需**之间更改智能卡身份验证设置，而无需重新启动连接服务器服务。

智能卡设置的更改不会影响当前已登录的用户和管理员。

后续步骤

如果需要，准备 Active Directory 以进行智能卡身份验证。请参阅[为智能卡身份验证准备 Active Directory](#)。

验证智能卡身份验证配置。请参阅[在 Horizon Console 中验证智能卡身份验证配置](#)。

在第三方解决方案上配置智能卡身份验证

第三方解决方案（如负载均衡器和网关）可以传送包含智能卡的 X.590 证书和加密的 PIN 的 SAML 声明以执行智能卡身份验证。

本主题简要说明了在设置第三方解决方案以完成以下操作时涉及的任务：在伙伴设备验证相关的 X.590 证书后，为连接服务器提供该证书。由于该功能使用 SAML 身份验证，因此其中的一个任务是在 Horizon Console 中创建 SAML 身份验证器。

有关在 Unified Access Gateway 上配置智能卡身份验证的信息，请参阅 Unified Access Gateway 文档。

步骤

- 为第三方网关或负载均衡器创建一个 SAML 身份验证器。
请参阅[在 Horizon Console 中配置 SAML 身份验证器](#)。
- 延长连接服务器元数据的过期时间，以免远程会话在 24 小时后就终止。
请参阅[在连接服务器上更改服务提供程序元数据的过期时间](#)。
- 如有必要，请配置第三方设备以使用连接服务器中的服务提供程序元数据。
请参阅第三方设备的产品文档。
- 在第三方设备上配置智能卡设置。
请参阅第三方设备的产品文档。

为智能卡身份验证准备 Active Directory

实施智能卡身份验证时，您可能需要在 Active Directory 中执行特定的任务。

- **为智能卡用户添加 UPN**

由于智能卡登录依赖用户主体名称 (UPN)，因此在 Horizon 7 中使用智能卡进行身份验证的用户和管理员的 Active Directory 帐户必须具备有效的 UPN。

- **将根证书添加到 Enterprise NTAAuth 存储**

如果使用 CA 颁发智能卡登录或域控制器证书，则必须将根证书添加到 Active Directory 中的 Enterprise NTAAuth 存储。如果 Windows 域控制器充当根 CA，则不需要执行此步骤。

- **将根证书添加到受信任的根证书颁发机构**

如果使用证书颁发机构 (CA) 颁发智能卡登录或域控制器证书，则必须将根证书添加到 Active Directory 中受信任的根证书颁发机构组策略中。如果 Windows 域控制器充当根 CA，则不需要执行此步骤。

- **将中间证书添加到中间证书颁发机构**

如果使用中间证书颁发机构 (CA) 颁发智能卡登录或域控制器证书，则必须将中间证书添加到 Active Directory 的中间证书颁发机构组策略中。

为智能卡用户添加 UPN

由于智能卡登录依赖用户主体名称 (UPN)，因此在 Horizon 7 中使用智能卡进行身份验证的用户和管理员的 Active Directory 帐户必须具备有效的 UPN。

如果智能卡用户所在的域和颁发根证书的域不同，您必须将用户的 UPN 设置为受信任 CA 的根证书内包含的使用者备用名称 (SAN)。如果您的根证书是从智能卡用户当前所在域中的服务器上颁发的，则不需要修改用户的 UPN。

注 即便是从同一个域颁发证书，您仍然可能需要设置内置 Active Directory 帐户的 UPN。内置帐户（包括 Administrator 帐户）在默认情况下未设置 UPN。

前提条件

- 通过查看证书属性，获取受信任 CA 的根证书中包含的 SAN。
- 如果您的 Active Directory 服务器上没有“ADSI 编辑”实用程序，请从 Microsoft 网站下载并安装相应的 Windows 支持工具。

步骤

- 1 在 Active Directory 服务器上，启动“ADSI 编辑”实用程序。
- 2 在左侧窗格中，展开用户所在的域并双击 CN=Users。
- 3 在右侧窗格中，右键单击用户，然后单击**属性**。
- 4 双击 userPrincipalName 属性并键入受信任 CA 证书的 SAN 值。
- 5 单击**确定**保存属性设置。

将根证书添加到 Enterprise NTAAuth 存储

如果使用 CA 颁发智能卡登录或域控制器证书，则必须将根证书添加到 Active Directory 中的 Enterprise NTAAuth 存储。如果 Windows 域控制器充当根 CA，则不需要执行此步骤。

步骤

- ◆ 在 Active Directory 服务器上使用 `certutil` 命令，将证书发布到 Enterprise NTAAuth 存储区中。

例如: `certutil -dspublish -f CA 根证书路径 NTAAuthCA`

此时该 CA 即为颁发此类证书的受信任机构。

将根证书添加到受信任的根证书颁发机构

如果使用证书颁发机构 (CA) 颁发智能卡登录或域控制器证书，则必须将根证书添加到 Active Directory 中受信任的根证书颁发机构组策略中。如果 Windows 域控制器充当根 CA，则不需要执行此步骤。

步骤

- 1 在 Active Directory 服务器上，导航至组策略管理插件。

AD 版本	导航路径
Windows 2003	<ol style="list-style-type: none"> a 选择开始 > 所有程序 > 管理工具 > Active Directory 用户和计算机。 b 右键单击域，然后单击属性。 c 在组策略选项卡上，单击打开以打开组策略管理插件。 d 右键单击默认域策略并单击编辑。
Windows 2008	<ol style="list-style-type: none"> a 选择开始 > 管理工具 > 组策略管理。 b 展开您的域，右键单击默认域策略并单击编辑。
Windows 2012 R2	<ol style="list-style-type: none"> a 选择开始 > 管理工具 > 组策略管理。 b 展开您的域，右键单击默认域策略并单击编辑。
Windows 2016	<ol style="list-style-type: none"> a 选择开始 > 管理工具 > 组策略管理。 b 展开您的域，右键单击默认域策略并单击编辑。

- 2 展开计算机配置区域，然后打开 Windows 设置\安全性设置\公钥。
- 3 右键单击受信任的根证书颁发机构，然后选择导入。
- 4 按照向导中的提示导入根证书（如 rootCA.cer）并单击确定。
- 5 关闭“组策略”窗口。

此时，域中的所有系统在其信任的根存储中都有一个根证书的副本。

后续步骤

如果中间证书颁发机构 (CA) 为您颁发了智能卡登录或域控制器证书，请将此中间证书添加到 Active Directory 中的中间证书颁发机构组策略中。请参阅[将中间证书添加到中间证书颁发机构](#)。

将中间证书添加到中间证书颁发机构

如果使用中间证书颁发机构 (CA) 颁发智能卡登录或域控制器证书，则必须将中间证书添加到 **Active Directory** 的中间证书颁发机构组策略中。

步骤

- 1 在 **Active Directory** 服务器上，导航至组策略管理插件。

AD 版本	导航路径
Windows 2003	<ol style="list-style-type: none"> a 选择开始 > 所有程序 > 管理工具 > Active Directory 用户和计算机。 b 右键单击域，然后单击属性。 c 在组策略选项卡上，单击打开以打开组策略管理插件。 d 右键单击默认域策略并单击编辑。
Windows 2008	<ol style="list-style-type: none"> a 选择开始 > 管理工具 > 组策略管理。 b 展开您的域，右键单击默认域策略并单击编辑。
Windows 2012 R2	<ol style="list-style-type: none"> a 选择开始 > 管理工具 > 组策略管理。 b 展开您的域，右键单击默认域策略并单击编辑。
Windows 2016	<ol style="list-style-type: none"> a 选择开始 > 管理工具 > 组策略管理。 b 展开您的域，右键单击默认域策略并单击编辑。

- 2 展开**计算机配置**区域，然后打开 **Windows 设置\安全性设置\公钥策略**。
- 3 右键单击**中间证书颁发机构**，然后选择**导入**。
- 4 按照向导中的提示导入中间证书（如 **intermediateCA.cer**）并单击**确定**。
- 5 关闭“组策略”窗口。

此时，域中的所有系统在其中间证书颁发机构存储区中都有一个中间证书的副本。

在 Horizon Console 中验证智能卡身份验证配置

当您首次设置智能卡身份验证后，或智能卡身份验证无法正常工作时，应检查您的智能卡身份验证配置。

步骤

- ◆ 确认每个客户端系统都配有智能卡中间件、带有有效证书的智能卡以及智能卡读卡器。确认最终用户有 **Horizon Client**。

有关配置智能卡软件和硬件的信息，请参见您的智能卡供应商提供的文档。

- ◆ 在每个客户端系统上，选择开始 > 设置 > 控制面板 > **Internet 选项** > 内容 > 证书 > 个人以验证证书是否可用于智能卡身份验证。

当用户或管理员将智能卡插入智能卡读卡器时，**Windows** 将证书从智能卡复制到用户的计算机。客户端系统上的应用程序（包括 **Horizon Client**）可以使用这些证书。

- ◆ 在连接服务器或安全服务器主机的 `locked.properties` 文件中，检查 `useCertAuth` 的属性是否被设置为 **true** 且拼写正确。

`locked.properties` 文件位于 `install_directory\VMware\VMware View\Server\sslgateway\conf` 中。`useCertAuth` 属性通常会被错误地拼写为 `userCertAuth`。

- ◆ 如果您在连接服务器实例上配置了智能卡身份验证，请在 Horizon Console 中检查智能卡的身份验证设置。
 - a 选择**设置 > 服务器**。
 - b 在**连接服务器**选项卡上，选择连接服务器实例，并单击**编辑**。
 - c 如果为用户配置了智能卡身份验证，则在**身份验证**选项卡上，验证用户的智能卡身份验证是否设置为**可选或必需**。
 - d 如果为管理员配置了智能卡身份验证，则在**身份验证**选项卡上，验证**管理员智能卡身份验证**是否设置为**可选或必需**。

必须重新启动连接服务器服务，对智能卡设置所做的更改才能生效。

- ◆ 如果智能卡用户所在的域不是颁发根证书的域，请验证用户的 UPN 是否设置为受信任 CA 的根证书内包含的 SAN。
 - a 通过查看证书属性，找出受信任 CA 的根证书中包含的 SAN。
 - b 在 Active Directory 服务器上，选择**开始 > 管理工具 > Active Directory 用户和计算机**。
 - c 右键单击**用户**文件夹中的用户，然后选择**属性**。

UPN 显示在**帐户**选项卡上的**用户登录名**文本框中。

- ◆ 如果智能卡用户选择使用 PCoIP 显示协议或 VMware Blast 显示协议连接到单会话桌面，请确认单用户计算机上已安装称为“智能卡重定向”的 Horizon Agent 组件。通过智能卡功能，用户可以使用智能卡登录到单会话桌面。已安装“远程桌面服务”角色的 RDS 主机自动支持智能卡功能，因而您无需安装该功能。
- ◆ 检查连接服务器或安全服务器主机上的 `drive:\Documents and Settings\All Users\Application Data\VMware\VDM\logs` 中的日志文件中的消息是否指明已启用智能卡身份验证。

使用智能卡证书撤销检查

通过配置证书撤销检查，可以阻止已撤销用户证书的用户通过智能卡进行身份验证。当用户离开组织、丢失智能卡或从一个部门调往另一个部门时，其证书通常会被撤销。

Horizon 7 支持通过证书撤销列表 (Certificate Revocation List, CRL) 和联机证书状态协议 (Online Certificate Status Protocol, OCSP) 进行证书撤销检查。CRL 是由颁发证书的 CA 发布的吊销证书列表。OCSP 是一种证书验证协议，用于获取 X.509 证书的撤销状态。

您可以在连接服务器实例或安全服务器上配置证书撤销检查。如果连接服务器实例与安全服务器配对，则您要在安全服务器上配置证书撤销检查。CA 必须能够从连接服务器或安全服务器主机上访问。

您可以在同一个连接服务器实例或安全服务器上配置 CRL 和 OCSP。如果您配置了两种类型的证书撤销检查，Horizon 7 会首先尝试使用 OCSP 检查，如果 OCSP 检查失败，则转而进行 CRL 检查。如果 CRL 失败，Horizon 7 不会改用 OCSP。

- [登录时进行 CRL 检查](#)

如果配置了 CRL 检查，Horizon 7 会构造并读取 CRL 以确定用户证书的撤销状态。

- [登录时进行 OCSP 证书撤销检查](#)

如果您配置了 OCSP 证书撤销检查，Horizon 7 会向 OCSP Responder 发送请求，以确定特定用户证书的撤销状态。Horizon 7 将使用 OCSP 签发证书，以检验它从 OCSP Responder 收到的响应的真伪。

- [配置 CRL 检查](#)

如果您配置了 CRL 检查，Horizon 7 将读取 CRL，以确定智能卡用户证书的撤销状态。

- [配置 OCSP 证书撤销检查](#)

如果您配置了 OCSP 证书撤销检查，Horizon 7 会向 OCSP Responder 发送验证请求，以确定智能卡用户证书的撤销状态。

- [智能卡证书撤销检查属性](#)

您可以设置 `locked.properties` 文件中的值，以启用和配置智能卡证书撤销检查。

登录时进行 CRL 检查

如果配置了 CRL 检查，Horizon 7 会构造并读取 CRL 以确定用户证书的撤销状态。

如果证书已撤销，并且智能卡身份验证是可选操作，则**输入您的用户名和密码**对话框将出现，而用户必须提供密码进行身份验证。如果必须进行智能卡身份验证，用户会收到错误消息，并且被禁止进行身份验证。如果 Horizon 7 无法读取 CRL，也会发生同样的事件。

登录时进行 OCSP 证书撤销检查

如果您配置了 OCSP 证书撤销检查，Horizon 7 会向 OCSP Responder 发送请求，以确定特定用户证书的撤销状态。Horizon 7 将使用 OCSP 签发证书，以检验它从 OCSP Responder 收到的响应的真伪。

如果用户证书已撤销，并且智能卡身份验证是可选操作，则**输入您的用户名和密码**对话框将出现，而用户必须提供密码进行身份验证。如果必须进行智能卡身份验证，用户会收到错误消息，并且被禁止进行身份验证。

如果 Horizon 7 没有收到 OCSP Responder 的响应或响应无效，就会重新进行 CRL 检查。

配置 CRL 检查

如果您配置了 CRL 检查，Horizon 7 将读取 CRL，以确定智能卡用户证书的撤销状态。

前提条件

熟悉用于 CRL 检查的 `locked.properties` 文件属性。请参阅[智能卡证书撤销检查属性](#)。

步骤

- 1 在连接服务器或安全服务器主机的 TLS/SSL 网关配置文件夹中创建或编辑 `locked.properties` 文件。

例如, `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`。

- 2 将 `enableRevocationChecking` 和 `crlLocation` 属性添加到 `locked.properties` 文件中。
 - a 将 `enableRevocationChecking` 属性设为 **true**, 以启用智能卡证书撤销检查。
 - b 将 `crlLocation` 属性设为 CRL 的地址。此值可以是 URL 或文件路径。
- 3 重新启动连接服务器服务或安全服务器服务, 使所做的更改生效。

示例: locked.properties 文件

列出的文件可启用智能卡身份验证和智能卡证书撤销检查, 配置 CRL 检查并为 CRL 位置指定一个 URL。

```
trustKeyfile=longa.key
trustStoretype=jks
useCertAuth=true
enableRevocationChecking=true
crlLocation=http://root.ocsp.net/certEnroll/ocsp-ROOT_CA.crl
```

配置 OCSP 证书撤销检查

如果您配置了 OCSP 证书撤销检查, Horizon 7 会向 OCSP Responder 发送验证请求, 以确定智能卡用户证书的撤销状态。

前提条件

熟悉用于 OCSP 证书撤销检查的 `locked.properties` 文件属性。请参阅[智能卡证书撤销检查属性](#)。

步骤

- 1 在连接服务器或安全服务器主机的 TLS/SSL 网关配置文件夹中创建或编辑 `locked.properties` 文件。

例如, `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`。

- 2 将 `enableRevocationChecking`、`enableOCSP`、`ocspURL` 和 `ocspSigningCert` 属性添加到 `locked.properties` 文件中。
 - a 将 `enableRevocationChecking` 属性设为 **true**, 以启用智能卡证书撤销检查。
 - b 将 `enableOCSP` 属性设为 **true**, 以启用 OCSP 证书撤销检查。
 - c 将 `ocspURL` 设为 OCSP Responder 的 URL。
 - d 将 `ocspSigningCert` 属性设为包含 OCSP Responder 签发证书的文件的位罝。
- 3 重新启动连接服务器服务或安全服务器服务, 使所做的更改生效。

示例：locked.properties 文件

列出的文件可启用智能卡身份验证和智能卡证书撤销检查，配置 CRL 与 OCSP 证书撤销检查，指定 OCSP Responder 的位置，并识别包含 OCSP 签发证书的文件。

```
trustKeyFile=longa.key
trustStoretype=jks
useCertAuth=true
enableRevocationChecking=true
enableOCSP=true
allowCertCRLs=true
ocspSigningCert=te-ca.signing.cer
ocspURL=http://te-ca.longa.int/ocsp
```

智能卡证书撤销检查属性

您可以设置 locked.properties 文件中的值，以启用和配置智能卡证书撤销检查。

表 4-1. 智能卡证书撤销检查属性 列出了证书撤销检查的 locked.properties 文件属性。

表 4-1. 智能卡证书撤销检查属性

属性	说明
enableRevocationChecking	将该属性设为 true 可启用证书撤销检查。 如果该属性设为 false ，则禁用证书撤销检查，并忽略其他所有证书撤销检查属性。 默认值为 false 。
crlLocation	指定 CRL 的位置，可以是 URL 或文件路径。 如果您不指定 URL 或者指定的 URL 无效，在 allowCertCRLs 被设为 true 或尚未指定时，Horizon 7 将使用用户证书上的 CRL 列表。 如果 Horizon 7 无法访问 CRL，则 CRL 检查将会失败。
allowCertCRLs	如果该属性设为 true ，Horizon 7 将从用户证书中提取 CRL 列表。 默认值为 true 。
enableOCSP	将该属性设为 true 可启用 OCSP 证书撤销检查。 默认值为 false 。
ocspURL	指定 OCSP Responder 的 URL。
ocspResponderCert	指定包含 OCSP Responder 签发证书的文件。Horizon 7 使用该证书检验 OCSP Responder 响应的真伪。
ocspSendNonce	如果该属性设为 true ，nonce 将会随 OCSP 请求发送，以防止重复响应。 默认值为 false 。
ocspCRLFailover	该属性设为 true 时，如果 OCSP 证书撤销检查失败，Horizon 7 将进行 CRL 检查。 默认值为 true 。

设置其他类型的用户身份验证

Horizon 7 可利用您现有的 Active Directory 基础架构对用户和管理员进行身份验证和管理。除了智能卡身份验证之外，您还可以将 Horizon 7 与其他形式的身份验证（例如，生物识别身份验证或双因素身份验证解决方案，如 RSA SecurID 和 RADIUS）相集成，以对远程桌面和应用程序用户进行身份验证。

本章讨论了以下主题：

- [使用双因素身份验证](#)
- [使用 SAML 身份验证](#)
- [配置生物身份验证](#)

使用双因素身份验证

您可以配置 Horizon 连接服务器实例，以便要求用户使用 RSA SecurID 身份验证或 RADIUS（远程身份验证拨入用户服务）身份验证。

- RADIUS 支持提供了各种基于令牌的备用双因素身份验证选项。
- Horizon 7 还提供了一个开放的标准扩展接口，以允许第三方解决方案供应商将高级身份验证扩展集成到 Horizon 7 中。

由于双因素身份验证解决方案（如 RSA SecurID 和 RADIUS）需要使用安装在不同服务器上的身份验证管理器，因此您必须配置这些服务器并使其可供连接服务器主机访问。例如，如果您使用 RSA SecurID，则身份验证管理器将会是 RSA Authentication Manager。如果您使用 RADIUS，则身份验证管理器将会是 RADIUS 服务器。

要使用双因素身份验证，每个用户必须具有由其身份验证管理器注册的令牌（如 RSA SecurID 令牌）。双因素身份验证令牌是一个可以按固定间隔生成身份验证代码的硬件或软件。通常身份验证需要同时提供 PIN 码和身份验证代码。

如果您有多个连接服务器实例，则可以在一些实例上配置双因素身份验证，在另一些实例上配置其他的用户身份验证方法。例如，您可以仅为那些通过 Internet 从企业网络外部访问远程桌面和应用程序的用户配置双因素身份验证。

Horizon 7 通过了 RSA SecurID Ready 程序的认证，支持各种 SecurID 功能，包括新建 PIN 模式、下一个令牌代码模式、RSA Authentication Manager 以及负载平衡等。

- [使用双因素身份验证登录](#)

如果用户连接到启用了 RSA SecurID 身份验证或 RADIUS 身份验证的连接服务器实例，则 Horizon Client 中将显示一个特殊登录对话框。

- [在 Horizon Console 中启用双因素身份验证](#)

通过在 Horizon Console 中修改连接服务器设置，您可以为连接服务器实例启用 RSA SecurID 身份验证或 RADIUS 身份验证。

- [RSA SecurID 访问被拒绝故障排除](#)

Horizon Client 通过 RSA SecurID 身份验证进行连接时，访问被拒绝。

- [排除 RADIUS 访问被拒故障](#)

Horizon Client 通过 RADIUS 双因素身份验证进行连接时访问被拒绝。

使用双因素身份验证登录

如果用户连接到启用了 RSA SecurID 身份验证或 RADIUS 身份验证的连接服务器实例，则 Horizon Client 中将显示一个特殊登录对话框。

用户在特殊登录对话框中输入其 RSA SecurID 或 RADIUS 身份验证的用户名和通行码。双重身份验证的通行码通常由 PIN 后跟令牌代码组成。

- 用户输入其 RSA SecurID 用户名和通行码后，如果 RSA Authentication Manager 要求输入新的 RSA SecurID PIN 码，将出现 PIN 码对话框。设置新的 PIN 码后，系统将提示用户先等待下一个令牌代码再登录。如果 RSA Authentication Manager 配置为采用系统生成的 PIN 码，将出现确认 PIN 码的对话框。
- 登录 Horizon 7 时，RADIUS 身份验证的工作方式与 RSA SecurID 很像。如果 RADIUS 服务器发出访问质询，Horizon Client 会显示与 RSA SecurID 的下一令牌代码提示相似的对话框。目前支持的 RADIUS 质询仅限于提示输入文本。不显示 RADIUS 服务器发出的任何质询文本。目前不支持更复杂格式的质询，如多项选择和图像选择。

用户在 Horizon Client 中输入凭据后，RADIUS 服务器可以向用户的手机发送一条包含代码的文字短信或电子邮件或者文本（使用其他消息外发机制）。用户可以将此文本和代码输入 Horizon Client 来完成身份验证。

- 由于某些 RADIUS 供应商提供从 Active Directory 导入用户的功能，因此在提示用户输入 RADIUS 身份验证用户名和通行码之前，可能会先提示他们提供 Active Directory 凭据。

在 Horizon Console 中启用双因素身份验证

通过在 Horizon Console 中修改连接服务器设置，您可以为连接服务器实例启用 RSA SecurID 身份验证或 RADIUS 身份验证。

前提条件

在身份验证管理器服务器上安装并配置双因素身份验证软件，如 RSA SecurID 软件或 RADIUS 软件。

- 对于 RSA SecurID 身份验证，从 RSA Authentication Manager 中导出连接服务器实例的 `sdconf.rec` 文件。请参阅 RSA Authentication Manager 文档。

- 对于 RADIUS 身份验证，请遵循供应商的配置文档。记录 RADIUS 服务器的主机名或 IP 地址、其侦听 RADIUS 身份验证的端口号（通常为 1812）、身份验证类型（PAP、CHAP、MS-CHAPv1 或 MS-CHAPv2）以及共享密码。您需在 Horizon Console 中输入这些值。可以为主要和辅助 RADIUS 身份验证器输入这些值。

步骤

- 1 在 Horizon Console 中，导航到**设置 > 服务器**。
- 2 在**连接服务器**选项卡上，选择连接服务器实例，并单击**编辑**。
- 3 在**身份验证**选项卡上，从**高级身份验证**部分的**双因素身份验证**下拉菜单中，选择 **RSA SecurID 或 RADIUS**。
- 4 要强制要求 RSA SecurID 或 RADIUS 用户名与 Active Directory 中的用户名匹配，请选择**强制要求 SecurID 与 Windows 用户名匹配**或**强制要求双因素与 Windows 用户名匹配**。

如果选择此选项，用户必须使用同一 RSA SecurID 或 RADIUS 用户名进行 Active Directory 身份验证。如果不选择此选项，则可以使用不同的用户名。

- 5 对于 RSA SecurID，单击**上传文件**，键入 `sdconf.rec` 文件的位置，或单击**浏览**搜索该文件。
- 6 对于 RADIUS 身份验证，完成其余字段：

- a 如果初始 RADIUS 身份验证使用可触发令牌代码带外传输的 Windows 身份验证，且此令牌代码用作 RADIUS 质询的一部分，则选择**使用相同的用户名和密码进行 RADIUS 和 Windows 身份验证**。

如果您选中此复选框，则在 RADIUS 身份验证使用 Windows 用户名和密码时，将不会在 RADIUS 身份验证后提示用户输入 Windows 凭据。用户不必在 RADIUS 身份验证后重新输入 Windows 用户名和密码。

- b 从**身份验证器**下拉菜单中，选择**创建新的身份验证器**，并完成此页。

- 如果您不希望启用 RADIUS 计帐，请将**记帐端口**设置为 **0**。仅在您的 RADIUS 服务器支持收集计帐数据时，将此端口设置为非零数字。如果 RADIUS 服务器不支持计帐消息，且您将此端口设置为非零数字，则会发送并忽略这些消息，然后重试多次，从而导致身份验证发生延迟。

可使用计帐数据来根据使用时间和数据给用户开具帐单。还可将计帐数据用于统计目的和常规的网络监视。

- 如果指定领域前缀字符串，则会将其放在用户名的开头并发送到 RADIUS 服务器。例如，如果在 Horizon Client 中输入的用户名为 `jdoe`，且指定领域前缀 `DOMAIN-A\`，则会将用户名 `DOMAIN-A\jdoe` 发送到 RADIUS 服务器。同样，如果使用领域后缀或词尾字符串 `@mycorp.com`，则会将用户名 `jdoe@mycorp.com` 发送到 RADIUS 服务器。

- 7 单击**确定**保存更改。

您无需重新启动连接服务器服务。系统将自动分发必要的配置文件，配置设置可立即生效。

当用户打开 Horizon Client 并向连接服务器进行身份验证时，系统将提示他们进行双因素身份验证。对于 RADIUS 身份验证，登录对话框将显示包含您指定的令牌标签的文本提示。

更改 RADIUS 身份验证设置将会影响在更改配置后启动的远程桌面和应用程序会话。当前会话不会受到 RADIUS 身份验证设置更改的影响。

后续步骤

如果您具有连接服务器实例的副本组，且希望也对其设置 RADIUS 身份验证，则可以重新使用现有的 RADIUS 身份验证器配置。

RSA SecurID 访问被拒绝故障排除

Horizon Client 通过 RSA SecurID 身份验证进行连接时，访问被拒绝。

问题

通过 RSA SecurID 进行验证的 Horizon Client 连接显示 Access Denied（访问被拒绝），并且 RSA Authentication Manager 登录监视器显示错误消息 Node Verification Failed（验证节点失败）。

原因

此时需重置 RSA Agent 主机节点秘密。

解决方案

- 1 在 Horizon Console 中，导航到**设置 > 服务器**。
- 2 在**连接服务器**选项卡上，选择连接服务器实例，并单击**编辑**。
- 3 在**身份验证**选项卡上，从**高级身份验证**部分的**双因素身份验证**下拉菜单中，选择 **RSA SecurID**。
- 4 选择**清除节点密钥**，然后单击**确定**。
- 5 在运行 RSA Authentication Manager 的计算机上，选择**开始 > 程序 > RSA Security > RSA Authentication Manager Host Mode**。
- 6 选择**代理主机 > 编辑代理主机**。
- 7 从列表中选择连接服务器，然后取消选中**已创建节点密钥**复选框。
每当您进行编辑时，将默认选中**已创建节点秘密**。
- 8 单击**确定**。

排除 RADIUS 访问被拒故障

Horizon Client 通过 RADIUS 双因素身份验证进行连接时访问被拒绝。

问题

使用 RADIUS 双因素身份验证进行 Horizon Client 连接时显示 Access Denied。

原因

RADIUS 没有收到 RADIUS 服务器的回复，从而导致 Horizon 7 超时。

以下常见的配置错误通常会导致出现这种情况：

- 尚未将 RADIUS 服务器配置为接受连接服务器实例作为 RADIUS 客户端。必须将使用 RADIUS 的每个连接服务器实例设置为 RADIUS 服务器上的客户端。请参阅您的 RADIUS 双因素身份验证产品对应的文档。
- 连接服务器实例和 RADIUS 服务器上的共享密码值不匹配。

使用 SAML 身份验证

安全断言标记语言 (SAML) 是一种基于 XML 的标准，用于在不同安全域之间描述和交换身份验证及授权信息。SAML 使用称为 SAML 断言的 XML 文档在身份提供程序与服务提供程序之间传递有关用户的信息。

您可以使用 SAML 身份验证将 Horizon 7 与 VMware Workspace ONE、VMware Identity Manager 或者合格的第三方负载均衡器或网关相集成。为第三方设备配置 SAML 时，请参阅供应商文档以了解有关配置 Horizon 7 以便与该设备配合使用的信息。如果启用了 SSO，登录到 VMware Identity Manager 或第三方设备的用户无需再次进行登录，即可启动远程桌面和应用程序。您还可以使用 SAML 身份验证在 VMware Access Point 或第三方设备上实施智能卡身份验证。

要将身份验证职责委派给 Workspace ONE、VMware Identity Manager 或第三方设备，您必须在 Horizon 7 中创建一个 SAML 身份验证器。SAML 身份验证器包含在 Horizon 7 与 Workspace ONE、VMware Identity Manager 或第三方设备之间交换的信任和元数据信息。您需要将 SAML 身份验证器与连接服务器实例进行关联。

为 VMware Identity Manager 集成使用 SAML 身份验证

Horizon 7 与 VMware Identity Manager（以前称为 Workspace ONE）的集成使用 SAML 2.0 标准建立相互信任关系，这对于单点登录 (Single Sign-On, SSO) 功能而言很重要。如果启用了 SSO，使用 Active Directory 凭据登录到 VMware Identity Manager 或 Workspace ONE 的用户无需再次进行登录，即可启动远程桌面和应用程序。

将 VMware Identity Manager 与 Horizon 7 集成后，VMware Identity Manager 会在用户登录到 VMware Identity Manager 并单击桌面或应用程序图标时生成唯一的 SAML 项目。VMware Identity Manager 将使用此 SAML 项目创建一个统一资源标识符 (Universal Resource Identifier, URI)。该 URI 中包含有关桌面或应用程序池所在的连接服务器实例、要启动哪个桌面或应用程序以及 SAML 项目的信息。

VMware Identity Manager 将 SAML 项目发送到 Horizon Client，Horizon Client 转而又将该项目发送到连接服务器实例。连接服务器实例使用 SAML 项目从 VMware Identity Manager 中检索 SAML 断言。

连接服务器实例检索到 SAML 断言后，会验证该断言、解密用户的密码，然后使用解密的密码启动桌面或应用程序。

设置 VMware Identity Manager 与 Horizon 7 的集成涉及到使用 Horizon 7 信息配置 VMware Identity Manager 以及配置 Horizon 7 将身份验证职责委托给 VMware Identity Manager。

要将身份验证职责委托给 VMware Identity Manager，您必须在 Horizon 7 中创建一个 SAML 身份验证器。SAML 身份验证器包含 Horizon 7 与 VMware Identity Manager 之间的信任和元数据交换信息。您需要将 SAML 身份验证器与连接服务器实例进行关联。

注 如果您想要通过 VMware Identity Manager 提供对桌面和应用程序的访问权限，请确认您在 Horizon Console 中以对根访问组拥有管理员角色的用户身份创建这些桌面和应用程序池。如果您向用户提供根访问组以外的其他访问组的管理员角色，VMware Identity Manager 将不会识别您在 Horizon 7 中配置的 SAML 身份验证器，并且您也将无法在 VMware Identity Manager 中配置池。

在 Horizon Console 中配置 SAML 身份验证器

要从 VMware Identity Manager 中启动远程桌面和应用程序，或者通过第三方负载均衡器或网关连接到远程桌面和应用程序，您必须在 Horizon Console 中创建一个 SAML 身份验证器。SAML 身份验证器包含 Horizon 7 和客户端连接到的设备之间交换的信任和元数据信息。

您需要将 SAML 身份验证器与连接服务器实例进行关联。如果您的部署包括多个连接服务器实例，则必须将 SAML 身份验证器与每个实例都进行关联。

您可以同时启用一个静态身份验证器和多个动态身份验证器。您可以配置 vIDM（动态）和 Unified Access Gateway（静态）身份验证器并将其保持活动状态。您可以通过这两种身份验证器之一建立连接。

您可以在连接服务器上配置多个 SAML 身份验证器，并且所有身份验证器可以同时处于活动状态。不过，在连接服务器上配置的各个 SAML 身份验证器的实体 ID 不能相同。

仪表板中的 SAML 身份验证器的状态始终是绿色的，因为它实质上是静态的预定义元数据。红色和绿色切换仅适用于动态身份验证器。

有关为 VMware Unified Access Gateway 设备配置 SAML 身份验证器的信息，请参阅 Unified Access Gateway 文档。

前提条件

- 确认安装并配置了 Workspace ONE、VMware Identity Manager 或者第三方网关或负载均衡器。请参阅该产品的安装文档。
- 确认连接服务器主机上安装了 SAML 服务器证书的签名 CA 的根证书。VMware 建议不要配置 SAML 身份验证器使用自签名证书。有关证书身份验证的信息，请参阅《Horizon 7 安装指南》文档。
- 记下 Workspace ONE 服务器、VMware Identity Manager 服务器或面向外部的负载均衡器的 FQDN 或 IP 地址。
- 如果您使用 Workspace ONE 或 VMware Identity Manager，则记下连接器 Web 界面的 URL。
- 如果您为要求生成 SAML 元数据并创建静态身份验证器的 Unified Access Gateway 设备或第三方设备创建身份验证器，则在设备上执行此过程以生成 SAML 元数据，然后复制该元数据。

步骤

- 1 在 Horizon Console 中，导航到**设置 > 服务器**。
- 2 在**连接服务器**选项卡上，选择一个要与 SAML 身份验证器关联的服务器实例，然后单击**编辑**。

- 3 在身份验证选项卡上，从将身份验证委派给 VMware Horizon (SAML 2.0 身份验证器) 下拉菜单中选择一项设置来启用或禁用 SAML 身份验证器。

选项	说明
已禁用	禁用 SAML 身份验证。您只能从 Horizon Client 中启动远程桌面和应用程序。
已允许	启用 SAML 身份验证。您可以从 Horizon Client 和 VMware Identity Manager 或第三方设备中启动远程桌面和应用程序。
需要	启用 SAML 身份验证。您只能从 VMware Identity Manager 或第三方设备中启动远程桌面和应用程序。无法从 Horizon Client 中手动启动桌面或应用程序。

您可以根据自己的需要，将部署中的每个连接服务器实例配置为使用不同的 SAML 身份验证设置。

- 4 单击**管理 SAML 身份验证器**，然后单击**添加**。
- 5 在“添加 SAML 2.0 身份验证器”对话框中配置 SAML 身份验证器。

选项	描述
类型	对于 Unified Access Gateway 设备或第三方设备，选择 静态 。对于 VMware Identity Manager，选择 动态 。对于动态身份验证器，您可以指定一个元数据 URL 和一个管理 URL。对于静态身份验证器，您必须先在 Unified Access Gateway 设备或第三方设备上生成元数据，然后将该元数据复制并粘贴到 SAML 元数据 文本框中。
标签	用于标识 SAML 身份验证器的唯一名称。
描述	SAML 身份验证器的简要描述。此值为可选项。
元数据 URL	（对于动态身份验证器）此 URL 用于检索在 SAML 身份提供程序和连接服务器实例之间交换 SAML 信息所需的全部信息。在 URL <code>https://<YOUR HORIZON SERVER NAME>/SAAS/API/1.0/GET/metadata/idp.xml</code> 中，单击 <YOUR HORIZON SERVER NAME> ，然后将其替换为 VMware Identity Manager 服务器或面向外部的负载均衡器（第三方设备）的 FQDN 或 IP 地址。
管理 URL	（对于动态身份验证器）此 URL 用于访问 SAML 身份提供程序的管理控制台。对于 VMware Identity Manager，此 URL 应指向 VMware Identity Manager Connector Web 界面。此值为可选项。
SAML 元数据	（对于静态身份验证器）您从 Unified Access Gateway 设备或第三方设备中生成并复制的元数据文本。
已为连接服务器启用	选中此复选框可启用身份验证器。您可以启用多个身份验证器。只有已启用的身份验证器才会显示在列表中。

- 6 单击**确定**保存 SAML 身份验证器的配置。

如果您提供了有效信息，则必须接受自签名证书（不建议）或为 Horizon 7 和 VMware Identity Manager 或第三方设备使用可信证书。

“管理 SAML 身份验证器”对话框显示新创建的身份验证器。

后续步骤

延长连接服务器元数据的过期时间，以免远程会话在 24 小时后就终止。请参阅[在连接服务器上更改服务提供程序元数据的过期时间](#)。

为 VMware Identity Manager 配置代理支持

Horizon 7 为 VMware Identity Manager (vIDM) 服务器提供了代理支持。代理详细信息（如主机名和端口号）可以在 ADAM 数据库中进行配置，而 HTTP 请求将通过代理来路由。

此功能支持混合部署，在这种部署中，内部部署的 Horizon 7 可以与云中托管的 vIDM 服务器进行通信。

前提条件

步骤

- 1 在您的连接服务器主机上启动“ADSI 编辑”实用程序。
- 2 展开以下对象路径下的 ADAM ADSI 树：
`cd=vdi,dc=vmware,dc=int,ou=Properties,ou=Global,cn=Common Attributes`。
- 3 选择操作 > 属性，然后添加 `pae-SAMLProxyName` 和 `pae-SAMLProxyPort` 条目的值。

在连接服务器上更改服务提供程序元数据的过期时间

如果未更改过期时间，连接服务器将在 24 小时后停止接受来自 SAML 身份验证器（如 Unified Access Gateway 设备或第三方身份提供程序）的 SAML 断言，并且必须重新执行元数据交换过程。

此过程用于指定在连接服务器停止接受来自身份提供程序的 SAML 断言之前可经过的天数。此数值将在当前过期时间结束时使用。例如，如果当前过期时间为 1 天，而您指定的是 90 天，那么经过 1 天后，连接服务器会生成过期时间为 90 天的元数据。

前提条件

请参阅 Microsoft TechNet 网站，了解如何在您的 Windows 操作系统版本上使用“ADSI 编辑”实用程序。

步骤

- 1 在您的连接服务器主机上启动“ADSI 编辑”实用程序。
- 2 在控制台树中，选择**连接到**。
- 3 在**选择或键入可分辨名称或命名上下文**文本框中，键入可分辨名称 `DC=vdi, DC=vmware, DC=int`。
- 4 在“计算机”窗格中，选择或键入 `localhost:389` 或者连接服务器主机的完全限定域名 (Fully Qualified Domain Name, FQDN) 后跟端口 389。

例如：`localhost:389` 或 `mycomputer.example.com:389`。
- 5 展开“ADSI 编辑”树，展开 **OU=Properties**，选择 **OU=Global**，然后在右侧窗格中双击 **CN=Common**。
- 6 在“属性”对话框中，编辑 `pae-NameValuePair` 属性以添加以下值：

```
cs-samlencryptionkeyvaliditydays=number-of-days
cs-samlsigningkeyvaliditydays=number-of-days
```

在此示例中，*number-of-days* 是在远程连接服务器停止接受 SAML 断言之前经过的天数。在这段时间过后，必须重新执行 SAML 元数据交换过程。

生成 SAML 元数据以便连接服务器可用作服务提供程序

在为要使用的身份提供程序创建并启用 SAML 身份验证器后，可能需要生成连接服务器元数据。您可以使用此元数据在作为身份提供程序的 Unified Access Gateway 设备或第三方负载平衡器上创建服务提供程序。

前提条件

确认您已为以下身份提供程序创建 SAML 身份验证器：Unified Access Gateway 或者第三方负载平衡器或网关。

步骤

- 1 打开新的浏览器选项卡，然后输入用于获取连接服务器 SAML 元数据的 URL。

`https://connection-server.example.com/SAML/metadata/sp.xml`

在此示例中，`connection-server.example.com` 是连接服务器主机的完全限定域名。

该页面显示连接服务器中的 SAML 元数据。

- 2 使用**另存为**命令将网页保存为 XML 文件。

例如，您可以将该页面保存到名为 `connection-server-metadata.xml` 的文件中。该文件的内容以下面的文本开头：

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...
```

后续步骤

在身份提供程序上使用相应的过程复制连接服务器 SAML 元数据。请参阅 Unified Access Gateway 或者第三方负载平衡器或网关的相关文档。

多个动态 SAML 身份验证器的响应时间注意事项

如果在连接服务器实例上将 SAML 2.0 身份验证配置为可选或必需的身份验证，并将多个动态 SAML 身份验证器与连接服务器实例相关联，则当任何动态 SAML 身份验证器变得无法访问时，从其他动态 SAML 身份验证器中启动远程桌面的响应时间将会增加。

您可以使用 Horizon Console 禁用无法访问的动态 SAML 身份验证器，以缩短其他动态 SAML 身份验证器上对启动远程桌面的响应时间。有关禁用 SAML 身份验证器的信息，请参阅在 [Horizon Console 中配置 SAML 身份验证器](#)。

在 Horizon Console 中配置 Workspace ONE 访问策略

Workspace ONE 或 VMware Identity Manager (vIDM) 管理员可以在 Horizon 7 中配置访问策略，以限制对授权桌面和应用程序的访问。要强制实施在 vIDM 中创建的策略，您需将 Horizon Client 置于 Workspace ONE 模式，以便 Horizon Client 可以将用户推送到 Workspace ONE 客户端来启动授权。当您登录到 Horizon Client 时，访问策略会引导您通过 Workspace ONE 登录以访问已发布的桌面和应用程序。

前提条件

- 在 Workspace ONE 中配置应用程序的访问策略。有关设置访问策略的更多信息，请参阅《VMware Identity Manager 管理指南》。
- 在 Horizon Console 中授权用户使用已发布的桌面和应用程序。

步骤

- 1 在 Horizon Console 中，导航到**设置 > 服务器**。
- 2 在**连接服务器**选项卡上，选择一个与 SAML 身份验证器关联的服务器实例，然后单击**编辑**。
- 3 在**身份验证**选项卡上，将**将身份验证委派给 VMware Horizon (SAML 2.0 身份验证器)**选项设置为**需要**。

“需要”选项将启用 SAML 身份验证。最终用户只能使用由 vIDM 或第三方身份提供程序提供的 SAML 令牌连接到 Horizon Server。无法从 Horizon Client 中手动启动桌面或应用程序。

- 4 选择**启用 Workspace ONE 模式**。
- 5 在 **Workspace ONE 服务器主机名**文本框中，输入 Workspace ONE 主机名 FQDN 值。
- 6 （可选）选择**阻止不支持 Workspace ONE 模式的客户端连接**以仅限支持 Workspace ONE 模式的 Horizon Client 访问应用程序。

版本低于 4.5 的 Horizon Client 不支持 Workspace ONE 模式功能。如果选择此选项，版本低于 4.5 的 Horizon Client 将无法访问 Workspace ONE 中的应用程序。如果 Workspace ONE 版本低于 2.9.1，则不会为高于 Horizon 7 版本 7.2 的版本启用 Workspace ONE 模式功能。

配置生物身份验证

您可以编辑 LDAP 数据库中的 `pae-ClientConfig` 属性以配置生物身份验证。

前提条件

有关如何在 Windows 服务器上使用“ADSI 编辑”实用程序的信息，请参阅 Microsoft TechNet 网站。

步骤

- 1 在连接服务器主机上启动“ADSI 编辑”实用程序。
- 2 在“连接设置”对话框中，选择或连接到 **DC=vdi,DC=vmware,DC=int**。
- 3 在“计算机”窗格中，选择或键入 **localhost:389** 或者连接服务器主机的完全限定域名 (Fully Qualified Domain Name, FQDN) 后跟端口 389。

例如：**localhost:389** 或 **mycomputer.mydomain.com:389**

- 在 **CN=Common, OU=Global, OU=Properties** 对象上，编辑 **pae-ClientConfig** 属性并添加 **BioMetricsTimeout=<integer>** 值。

以下 BioMetricsTimeout 值有效：

BioMetricsTimeout 值	说明
0	不支持生物身份验证。这是默认值。
-1	支持生物身份验证，并且没有任何时间限制。
任意正整数	支持生物身份验证，并且可以在指定的分钟数内使用。

新设置将立即生效。您无需重新启动连接服务器服务或客户端设备。

对用户和组进行身份验证

登录到 **Horizon Console** 后，您可以通过为用户和组设置身份验证来控制对应用程序和桌面的访问权限。

您可以通过配置远程访问来限制用户和组从网络以外的位置访问桌面。您可以通过设置相应配置来使未通过身份验证的用户无需 AD 凭据即可从 **Horizon Client** 访问其已发布的应用程序。

本章讨论了以下主题：

- [限制网络外部的远程桌面访问](#)
- [配置未验证访问](#)

限制网络外部的远程桌面访问

您可以允许特定的授权用户和组从外部网络访问远程桌面，而限制其他授权用户和组的访问。所有授权用户都将可以从内部网络访问桌面和应用程序。如果您选择不将访问权限限制给外部网络的特定用户，那么所有授权用户都将可以从外部网络进行访问。

出于安全原因，管理员可能会需要限制网络外部的用户和组访问网络内部的远程桌面和应用程序。当受限的用户从外部网络访问系统时，会显示一条消息，指明此用户无权使用该系统。此用户必须在内部网络中才有权访问桌面和应用程序池。

配置远程访问

您可以允许一些用户和组从网络外部访问连接服务器实例，同时限制其他用户和组的访问。

前提条件

- 必须在网络外部部署 **Unified Access Gateway** 设备、安全服务器或负载均衡器，作为用户有权访问的连接服务器实例的网关。有关部署 **Unified Access Gateway** 设备的更多信息，请参阅《部署和配置 **Unified Access Gateway**》文档。
- 要进行远程访问的用户必须有权访问桌面或应用程序池。

步骤

- 1 在 **Horizon Console** 中，选择用户和组。
- 2 单击 **远程访问** 选项卡。
- 3 单击 **添加**，选择一个或多个搜索条件，然后单击 **查找** 以根据搜索条件查找用户或组。

注 未验证访问用户将不会显示在搜索结果中。

- 4 要向某个用户、组或未验证访问用户提供远程访问权限，请选择相应用户或组，然后单击**确定**。
- 5 要从远程访问中移除用户或组，请选择相应用户或组，单击**删除**，然后单击**确定**。

配置未验证访问

管理员可以为未验证用户设置配置，以便这些用户无需 AD 凭据即可从 **Horizon Client** 访问其已发布的应用程序。如果您的用户需要访问具有安全和用户管理要求的无缝应用程序，可考虑设置未验证访问。

当用户启动配置为未验证访问的已发布的应用程序，RDS 主机会根据需要创建本地用户会话，并向用户分配会话。

该功能需要设置 **Horizon 7** 版本 **7.1** 环境和 **Horizon Client** 版本 **4.4**。

有关为用户配置未验证访问的规则和指南的信息，请参阅《**Horizon 7** 管理指南》文档。

创建未验证访问用户

管理员可以为已发布的应用程序创建未验证访问用户。管理员配置未验证访问用户后，用户仅可以使用未验证访问从 **Horizon Client** 登录连接服务器实例。

前提条件

- 管理员只能为每个 **Active Directory** 帐户创建一个用户。
- 管理员无法创建未验证用户组。如果您创建一个未验证访问用户，而该 **AD** 用户已存在客户端会话，您必须重新启动客户端会话，以使更改生效。
- 如果选择具有桌面授权的用户，并将该用户设置为未验证访问用户，该用户将无权访问授权的桌面。

步骤

- 1 在 **Horizon Console** 中，选择**用户和组**。
- 2 在**未验证访问**选项卡上，单击**添加**。
- 3 在**添加未验证用户**向导中，选择一个或多个搜索条件，然后单击**查找**，根据搜索条件查找用户。
- 4 选择一个用户，然后单击**下一步**。
- 5 输入用户别名。

默认的用户别名是已为 **AD** 帐户配置的用户名。最终用户可以使用用户别名，从 **Horizon Client** 登录连接服务器实例。

- 6 （可选）检查用户详细信息并添加备注。
- 7 单击**提交**。

连接服务器将创建未验证访问用户，并显示用户详细信息，包括用户别名、用户名、名字和姓氏、域、应用程序授权和会话。

后续步骤

创建未验证访问用户后，您必须在连接服务器中启用未验证访问，以便用户可以连接和访问已发布的应用程序。请参阅《Horizon 7 管理指南》文档中的“启用用户未验证访问”。

授权未验证访问用户访问已发布的应用程序

创建未验证访问用户后，您必须授权该用户访问已发布的应用程序。

前提条件

- 根据 RDS 主机组创建场。请参阅[在 Horizon Console 中创建场](#)。
- 为在 RDS 主机场上运行的已发布的应用程序创建应用程序池。请参阅[在 Horizon Console 中创建应用程序池](#)。

步骤

- 1 在 Horizon Console 中，选择**用户和组**。
- 2 在**授权**选项卡上，从**授权**下拉菜单中选择**添加应用程序授权**。
- 3 单击**添加**，选择一个或多个搜索条件，选中**未验证用户**复选框，然后单击**查找**以根据搜索条件查找未验证访问用户。
- 4 选择池中获得应用程序授权的用户，然后单击**确定**。
- 5 选择池中的应用程序，然后单击**提交**。

后续步骤

使用未验证访问用户身份登录 Horizon Client。请参阅[从 Horizon Client 未验证访问](#)。

删除未验证访问用户

在删除未验证访问用户时，您必须同时移除该用户的应用程序池授权。

您不能删除作为默认用户的未验证访问用户。如果删除默认用户，Horizon Console 会显示一个内部错误消息和一个用户成功移除消息。但是，不会从 Horizon Console 中删除默认用户。

注 如果您删除一个未验证访问用户，而该 AD 用户已存在客户端会话，则您必须重新启动客户端会话，以使更改生效。

步骤

- 1 在 Horizon Console 中，选择**用户和组**。
- 2 在**未验证访问**选项卡中，选择用户，然后单击**删除**。
- 3 单击**确定**。

后续步骤

移除用户的应用程序授权。

从 Horizon Client 未验证访问

以未验证访问用户身份登录 Horizon Client，启动已发布的应用程序。

为确保获得更高安全性，未验证访问用户具有您可用于登录 Horizon Client 的用户别名。如果您选择用户别名，则无需提供该用户的 AD 凭据或 UPN。登录 Horizon Client 后，您可以单击已发布的应用程序，启动该应用程序。有关安装和设置 Horizon Client 的更多信息，请参阅 [VMware Horizon Client 文档](#) 网页中的 Horizon Client 文档。

前提条件

- 确认为 Horizon 7 7.1 版连接服务器配置了未验证访问。
- 确认已在 Horizon Administrator 中创建了未验证访问用户。如果默认未验证用户是唯一未验证访问用户，则 Horizon Client 使用默认用户连接到连接服务器实例。

步骤

- 1 启动 Horizon Client。
- 2 在 Horizon Client 中，选择**以未验证访问匿名登录**。
- 3 连接到连接服务器实例。
- 4 从下拉菜单中选择一个用户别名，然后单击**登录**。
默认用户的后缀为“default”。
- 5 双击已发布的应用程序，以启动该应用程序。

在 Horizon Console 中配置基于角色的委派管理

7

Horizon 7 环境中的一项关键管理任务是确定哪些用户能够使用 Horizon Console，以及这些用户有执行哪些任务的权限。通过基于角色的委派管理，您可以将管理员角色分配给特定 Active Directory 用户和组，从而有选择地分配管理权限。

本章讨论了以下主题：

- [了解角色和特权](#)
- [在 Horizon Console 中使用访问组委派池和场的管理权](#)
- [了解权限](#)
- [对管理员进行管理](#)
- [管理和查看权限](#)
- [管理和查看访问组](#)
- [管理自定义角色](#)
- [预定义的角色和特权](#)
- [执行常见任务所需的特权](#)
- [针对管理员用户和组的最佳实践](#)

了解角色和特权

能否在 Horizon Console 中执行任务由一个访问控制系统掌控，该系统由管理员角色和特权组成。该系统类似于 vCenter Server 访问控制系统。

管理员角色就是一组特权的集合。特权可授予执行特定操作的能力，例如授予用户对桌面池的权限。特权还控制管理员可在 Horizon Console 中查看的内容。例如，如果某个管理员不具有查看或修改全局策略的特权，那么该管理员登录到 Horizon Console 时将看不到导航面板中的**全局策略**设置。

管理员特权可以针对全局或特定对象。全局特权控制整个系统的操作，例如查看和更改全局设置。特定于对象的特权则控制对特定对象类型的操作。

管理员角色通常具有执行较高级别管理任务所需的各种特权。Horizon Console 中包含的预定义角色具有执行常见管理任务所需的特权。您可以将这些预定义角色分配给管理员用户和组，也可以通过组合特定特权来自行创建角色。您无法修改预定义角色。

要创建管理员，可以从 **Active Directory** 用户和组中选择用户和组并分配管理员角色。如果角色中包含特定于对象的特权，您可能需要将该角色应用于访问组。管理员通过其角色分配获取特权。您无法将特权直接分配给管理员。具有多个角色的管理员拥有这些角色中包含的所有特权。

在 Horizon Console 中使用访问组委派池和场的管理权

默认情况下，自动桌面池、手动桌面池和场在根访问组中创建，在 **Horizon Console** 中显示为 / 或 **Root(/)**。已发布的桌面池和应用程序池将继承其场的访问组。您可以在根访问组下创建访问组，然后将特定池或场的管理权委托给不同的管理员。

注 您无法直接更改已发布桌面池或应用程序池的访问组。您必须更改已发布桌面池或应用程序池所属的场的访问组。

虚拟机或物理机从其桌面池继承访问组。连接的永久磁盘从其计算机继承访问组。包括根访问组在内，最多可以有 100 个访问组。

通过在访问组上为管理员分配角色，就可以为管理员配置对该访问组中资源的访问权限。管理员只能访问为其分配了相应角色的访问组中的资源。管理员在访问组上的角色决定了其对该访问组中资源所具有的访问权限级别。

由于角色可从根访问组继承而来，因此在根访问组上具有某个角色的管理员在所有访问组上都具有该角色。在根访问组上具有管理员角色的管理员是超级管理员，因为他们对系统中的所有对象具有完全访问权限。

角色必须包含至少一个特定于对象的特权才能应用于访问组。只包含全局特权的角色不能应用于访问组。

您可以使用 **Horizon Console** 创建访问组，并将现有桌面池移到访问组中。创建自动桌面池、手动池或场时，您可以接受默认根访问组，也可以选择其他访问组。

- **为不同访问组配置不同管理员**

您可以创建不同的管理员来管理配置中的每个访问组。

- **为同一访问组配置不同管理员**

您可以创建不同的管理员来管理同一访问组。

为不同访问组配置不同管理员

您可以创建不同的管理员来管理配置中的每个访问组。

例如，如果您的企业桌面池位于一个访问组中，而软件开发人员的桌面池位于另一个访问组中，那么您可以创建不同的管理员来管理每个访问组中的资源。

表 7-1. 为不同访问组配置不同管理员 显示了这种配置的示例。

表 7-1. 为不同访问组配置不同管理员

管理员	角色	访问组
view-domain.com\Admin1	清单管理员	/CorporateDesktops
view-domain.com\Admin2	清单管理员	/DeveloperDesktops

在此示例中，名为 **Admin1** 的管理员在名为 **CorporateDesktops** 的访问组中具有 **Inventory Administrators** 角色，名为 **Admin2** 的管理员在名为 **DeveloperDesktops** 的访问组上具有 **Inventory Administrators** 角色。

为同一访问组配置不同管理员

您可以创建不同的管理员来管理同一访问组。

例如，如果您的企业桌面池位于一个访问组中，您可以创建一名可以查看和修改这些池的管理员，另外再创建一名只能查看这些池的管理员。

[表 7-2. 为同一访问组配置不同管理员](#) 显示了这种配置的示例。

表 7-2. 为同一访问组配置不同管理员

管理员	角色	访问组
view-domain.com\Admin1	清单管理员	/CorporateDesktops
view-domain.com\Admin2	清单管理员 (只读)	/CorporateDesktops

在此示例中，名为 **Admin1** 的管理员在名为 **CorporateDesktops** 的访问组上拥有“清单管理员”角色，名为 **Admin2** 的管理员在同一访问组上拥有“清单管理员 (只读)”角色。

了解权限

Horizon Console 提供角色、管理员用户或组以及访问组的组合作为权限。角色定义了可以执行的操作，用户或组指明了谁可以执行操作，访问组则包含操作的目标对象。

根据您的选择的是管理员用户或组、访问组还是角色，Horizon Console 中将显示不同的权限。

下表显示了当您选择管理员用户或组时，Horizon Console 中是如何显示权限的。管理员用户名为 **Admin 1**，具有两个权限。

表 7-3. “管理员和组”选项卡上显示的 Admin 1 权限

角色	访问组
清单管理员	MarketingDesktops
管理员 (只读)	/

第一个权限表示 **Admin 1** 在名为 **MarketingDesktops** 的访问组上具有 **Inventory Administrators** 角色。第二个权限表示 **Admin 1** 在根访问组上具有 **管理员 (Read only)** 角色。

下表显示了当您选择 **MarketingDesktops** 访问组时，Horizon Console 中如何显示同样的权限。

表 7-4. “文件夹”选项卡上显示的 MarketingDesktops 权限

Admin	角色	已继承
horizon-domain.com\Admin1	清单管理员	
horizon-domain.com\Admin1	管理员 (只读)	是

第一个权限与表 7-3. “管理员和组”选项卡上显示的 Admin 1 权限中显示的第一个权限相同。第二个权限是从表 7-3. “管理员和组”选项卡上显示的 Admin 1 权限中显示的第二个权限继承而来。因为访问组从根访问组继承权限，因此 Admin1 在 MarketingDesktops 访问组上具有管理员 (Read only) 角色。如果权限是继承而来，那么“是否为继承”列中就会显示“是”。

下表显示了当您选择“清单管理员”角色时，表 7-3. “管理员和组”选项卡上显示的 Admin 1 权限中的第一个权限如何在 Horizon Console 中显示。

表 7-5. “角色权限”选项卡上显示的清单管理员权限

Administrator	访问组
horizon-domain.com\Admin1	/MarketingDesktops

对管理员进行管理

具有 Administrators 角色的用户可以使用 Horizon Console 来添加和移除管理员用户和组。

管理员角色是 Horizon Console 中权限最高的角色。最初，Horizon Administrators 帐户的成员会被授予 Administrators 角色。当您安装连接服务器时，可以指定 Administrators 帐户。管理员帐户可以是连接服务器计算机上的本地 Administrators 组 (BUILTIN\Administrators)，也可以是域用户或组帐户。

注 默认情况下，Domain Admins（域管理员）组是本地管理员组的成员。如果指定 Administrators 帐户作为本地管理员组，并且不想使域管理员拥有对清单对象和 Horizon 7 配置设置的完全访问权限，您必须从本地管理员组中删除 Domain Admins（域管理员）组。

■ 在 Horizon Console 中创建管理员

要创建管理员，您需要在 Horizon Console 中从 Active Directory 用户和组内选择一个用户或组，然后分配管理员角色。

■ 在 Horizon Console 中移除管理员

您可以移除管理员用户或组，但无法移除系统中的最后一个超级管理员。超级管理员是在根访问组上具有管理员角色的管理员。

在 Horizon Console 中创建管理员

要创建管理员，您需要在 Horizon Console 中从 Active Directory 用户和组内选择一个用户或组，然后分配管理员角色。

前提条件

- 熟悉预定义的管理员角色。请参阅[预定义的角色和特权](#)。

- 熟悉创建管理员用户和组的最佳实践。请参阅[针对管理员用户和组的最佳实践](#)。
- 如果要为管理员分配自定义角色，请创建自定义角色。请参阅[在 Horizon Console 中添加自定义角色](#)。
- 要创建可以管理特定桌面池的管理员，请创建一个访问组并将桌面池移到该访问组中。请参阅[管理和查看访问组](#)。

步骤

- 1 在 Horizon Console 中，导航到**设置 > 管理员**。
- 2 在**管理员和组**选项卡中，单击**添加用户或用户组**。
- 3 单击**添加**，选择一个或多个搜索条件，然后单击**查找**，根据您的搜索条件来筛选 Active Directory 用户或用户组。
- 4 选择您希望将其设为管理员用户或组的 Active Directory 用户或用户组，然后依次单击**确定**和**下一步**。
您可以按 **Ctrl** 和 **Shift** 键来选择多个用户和组。
- 5 选择一个要分配给管理员用户或用户组的角色。

已应用于访问组列指示角色是否应用于访问组。只有包含特定于对象的特权的角色才可以应用于访问组。只包含全局特权的角色不能应用于访问组。

选项	操作
将您所选的角色应用于访问组	选择一个或多个访问组，然后单击 下一步 。
您希望将该角色应用于所有访问组	选择根访问组，然后单击 下一步 。

- 6 单击**完成**创建管理员用户或组。

新的管理员用户或组将显示在**管理员和组**选项卡上的左侧窗格中，您选择的角色和访问组显示在右侧窗格中。

在 Horizon Console 中移除管理员

您可以移除管理员用户或组，但无法移除系统中的最后一个超级管理员。超级管理员是在根访问组上具有管理员角色的管理员。

步骤

- 1 在 Horizon Console 中，导航到**设置 > 管理员**。
- 2 在**管理员和组**选项卡上，选择所需的管理员或组，然后依次单击**移除用户或用户组**和**确定**。

管理员和组选项卡上将不再显示该管理员用户或组。

管理和查看权限

您可以使用 Horizon Console 添加、删除和查看特定管理员用户和组、角色及访问组的权限。

- [在 Horizon Console 中添加权限](#)

您可以添加包含特定管理员用户或组、特定角色或特定访问组的权限。

■ 在 Horizon Console 中删除权限

可以删除包含特定管理员用户或组、特定角色或特定访问组的权限。

■ 在 Horizon Console 中查看权限

您可以查看包含特定管理员或组、特定角色或特定访问组的权限。

在 Horizon Console 中添加权限

您可以添加包含特定管理员用户或组、特定角色或特定访问组的权限。

步骤

- 1 在 Horizon Console 中，导航到**设置 > 管理员**。
- 2 创建权限。

选项	操作
创建包含特定管理员用户或组的权限。	<ol style="list-style-type: none"> a 在管理员和组选项卡上，选择所需的管理员或组，然后单击添加权限。 b 选择一个角色。 c 如果该角色不适用于访问组，单击完成。 d 如果该角色适用于访问组，单击下一步，选择一个或多个访问组，然后单击完成。角色必须包含至少一个特定于对象的特权才能应用于访问组。
创建包含特定角色的权限。	<ol style="list-style-type: none"> a 在角色权限选项卡上，选择所需的角色，单击权限，然后单击添加权限。 b 单击添加，选择一个或多个搜索条件，然后单击查找来查找符合搜索条件的管理员用户或组。 c 选择要包含在权限中的管理员用户或组，然后单击确定。您可以按 Ctrl 和 Shift 键来选择多个用户和组。 d 如果该角色不适用于访问组，单击完成。 e 如果该角色适用于访问组，单击下一步，选择一个或多个访问组，然后单击完成。角色必须包含至少一个特定于对象的特权才能应用于访问组。
创建包含特定访问组的权限。	<ol style="list-style-type: none"> a 在访问组选项卡上，选择访问组并单击添加权限。 b 单击添加，选择一个或多个搜索条件，然后单击查找来查找符合搜索条件的管理员用户或组。 c 选择要包含在权限中的管理员用户或组，然后单击确定。您可以按 Ctrl 和 Shift 键来选择多个用户和组。 d 单击下一步选择一个角色，然后单击完成。角色必须包含至少一个特定于对象的特权才能应用于访问组。

在 Horizon Console 中删除权限

可以删除包含特定管理员用户或组、特定角色或特定访问组的权限。

移除管理员用户或组的最后一个权限后，该管理员用户或组也随之被移除。由于至少有一个管理员必须在根访问组上具有管理员角色，因此您无法删除会导致管理员被删除的权限。您无法删除继承而来的权限。

步骤

- 1 在 Horizon Console 中，导航到**设置 > 管理员**。

2 选择要删除的权限。

选项	操作
删除应用于特定管理员或组的权限。	在 管理员和组 选项卡上选择管理员或组。
删除应用于特定角色的权限。	在 角色 选项卡上选择角色。
删除应用于特定访问组的权限。	在 访问组 选项卡上选择文件夹。

3 选择所需的权限，然后单击**移除权限**。

在 Horizon Console 中查看权限

您可以查看包含特定管理员或组、特定角色或特定访问组的权限。

步骤

- 1 在 Horizon Console 中，导航到**设置 > 管理员**。
- 2 查看权限。

选项	操作
查看包含特定管理员或组的权限。	在 管理员和组 选项卡上选择管理员或组。
查看包含特定角色的权限。	在 角色权限 选项卡上选择角色，然后单击 权限 。
查看包含特定访问组的权限。	在 访问组 选项卡上选择文件夹。

管理和查看访问组

您可以使用 Horizon Console 添加和删除访问组，以及查看特定访问组中的桌面池和计算机。

■ 在 Horizon Console 中添加访问组

您可以通过创建访问组，将特定计算机、桌面池或场的管理权委托给不同的管理员。默认情况下，桌面池、应用程序池和场驻留在根访问组中。

■ 在 Horizon Console 中将桌面池或场移至不同的访问组

创建访问组后，您可以将自动桌面池、手动池或场移至新的访问组。

■ 在 Horizon Console 中移除访问组

当访问组不包含任何对象时，您可以移除该访问组。但是，您无法移除根访问组。

■ 查看访问组中的对象

您可以在 Horizon Console 中查看特定访问组中的桌面池、应用程序池、场或永久磁盘。

■ 查看访问组中的 vCenter 虚拟机

您可以在 Horizon Console 中查看特定访问组中的 vCenter 虚拟机。vCenter 虚拟机从其池中继承访问组。

在 Horizon Console 中添加访问组

您可以通过创建访问组，将特定计算机、桌面池或场的管理权委托给不同的管理员。默认情况下，桌面池、应用程序池和场驻留在根访问组中。

包括根访问组在内，最多可以有 100 个访问组。

步骤

- 1 在 Horizon Console 中，导航到“访问组”对话框。

选项	操作
从桌面中	<ul style="list-style-type: none"> ■ 选择清单 > 桌面。 ■ 从访问组下拉菜单中，选择新建访问组。
从场中	<ul style="list-style-type: none"> ■ 选择清单 > 场。 ■ 从访问组下拉菜单中，选择新建访问组。

- 2 为访问组键入名称和描述，然后单击**确定**。

描述是可选项。

后续步骤

将一个或多个对象移至该访问组。

在 Horizon Console 中将桌面池或场移至不同的访问组

创建访问组后，您可以将自动桌面池、手动池或场移至新的访问组。

步骤

- 1 在 Horizon Console 中，选择**清单 > 桌面**或**清单 > 场**。
- 2 选择一个池或场。
- 3 从**访问组**下拉菜单中选择**更改访问组**。
- 4 选择访问组并单击**确定**。

Horizon Console 会将该池或场移至所选的访问组。

在 Horizon Console 中移除访问组

当访问组不包含任何对象时，您可以移除该访问组。但是，您无法移除根访问组。

前提条件

如果访问组包含对象，请将这些对象移动到另一访问组或根访问组中。请参阅[在 Horizon Console 中将桌面池或场移至不同的访问组](#)。

步骤

- 1 在 Horizon Console 中，导航到**设置 > 管理员**。

- 2 在访问组选项卡上，选择访问组并单击**移除访问组**。
- 3 单击**确定**移除访问组。

查看访问组中的对象

您可以在 Horizon Console 中查看特定访问组中的桌面池、应用程序池、场或永久磁盘。

步骤

- 1 在 Horizon Console 中，导航到对象的主页。

对象	操作
桌面池	选择 清单 > 桌面 。
应用程序池	选择 清单 > 应用程序 。
场	选择 清单 > 场 。
永久磁盘	选择 清单 > 永久磁盘 。

默认情况下显示所有访问组中的对象。

- 2 从主窗口窗格的**访问组**下拉菜单中选择访问组。

将显示访问组中您所选择的对象。

查看访问组中的 vCenter 虚拟机

您可以在 Horizon Console 中查看特定访问组中的 vCenter 虚拟机。vCenter 虚拟机从其池中继承访问组。

步骤

- 1 在 Horizon Console 中，导航到**清单 > 计算机**。
- 2 选择 **vCenter 虚拟机**选项卡。
默认情况下，将显示所有访问组中的 vCenter 虚拟机。
- 3 从**访问组**下拉菜单中选择一个访问组。
将显示您选择的访问组中的 vCenter 虚拟机。

管理自定义角色

您可以使用 Horizon Console 添加、修改和删除自定义角色。

- 在 [Horizon Console](#) 中添加自定义角色
如果预定义的管理员角色不符合您的要求，您可以在 Horizon Console 中组合特定特权以自行创建角色。
- 在 [Horizon Console](#) 修改自定义角色中的特权
您可以修改自定义角色中的特权，**pactara**。但无法修改预定义的管理员角色。

■ 在 Horizon Console 中移除自定义角色

如果自定义角色不包含在权限中时，您可以移除该角色，但您无法移除预定义的管理员角色。

在 Horizon Console 中添加自定义角色

如果预定义的管理员角色不符合您的要求，您可以在 Horizon Console 中组合特定特权以自行创建角色。

前提条件

熟悉可用于创建自定义角色的管理员特权。请参阅[预定义的角色和特权](#)。

注 创建自定义管理员角色时，自定义管理员用户没有全局权限。只有预定义的管理员角色才具有全局权限，能够管理 Cloud Pod 架构 环境中的全局授权。

步骤

- 1 在 Horizon Console 中，导航到**设置 > 管理员**。
- 2 在**角色特权**选项卡上，单击**添加角色**。
- 3 为新角色输入名称和描述，选择一个或多个特权，然后单击**确定**。
新角色将显示在左侧窗格中。

在 Horizon Console 修改自定义角色中的特权

您可以修改自定义角色中的特权，pactara。但无法修改预定义的管理员角色。

前提条件

熟悉可用于创建自定义角色的管理员特权。请参阅[预定义的角色和特权](#)。

步骤

- 1 在 Horizon Console 中，导航到**设置 > 管理员**。
- 2 在**角色特权**选项卡上，选择所需的角色。
- 3 查看角色中的特权，然后单击**编辑**。
- 4 选择或取消选择特权。
- 5 单击**确定**保存更改。

在 Horizon Console 中移除自定义角色

如果自定义角色不包含在权限中时，您可以移除该角色，但您无法移除预定义的管理员角色。

前提条件

如果角色包含在权限中，请删除该权限。请参阅[在 Horizon Console 中删除权限](#)。

步骤

- 1 在 Horizon Console 中，导航到**设置 > 管理员**。

- 2 在**角色特权**选项卡上，选择所需的角色，然后单击**移除角色**。

对于预定义角色或者包含在权限中的自定义角色，**移除角色**按钮不可用。

- 3 单击**确定**移除角色。

预定义的角色和特权

Horizon Console 中提供了一些预定义角色，您可以将这些角色分配给管理员用户和组。您也可以组合特定的特权，自行创建管理员角色。

- **预定义的管理员角色**

预定义的管理员角色具有执行常见管理任务所需的所有特权。您无法修改预定义角色。

- **全局特权**

全局特权控制整个系统的操作，例如查看和更改全局设置。只包含全局特权的角色不能应用于访问组。

- **特定于对象的特权**

对象专用特权用于控制可对特定类型的清单对象执行的操作。包含特定于对象的特权的角色可以应用于访问组。

- **内部特权**

某些预定义的管理员角色包含内部特权。您在创建自定义角色时无法选择内部特权。

预定义的管理员角色

预定义的管理员角色具有执行常见管理任务所需的所有特权。您无法修改预定义角色。

注 通过为用户分配预定义角色或自定义角色组合，可授权用户执行那些单独具有某个预定义角色或自定义角色时无法完成的操作。

下表说明了预定义角色，并指出了角色是否可以应用于访问组。

表 7-6. Horizon Console 中的预定义角色

角色	用户能力	应用于访问组
管理员	<p>执行所有管理员操作，包括创建其他管理员用户和组。在 Cloud Pod 架构环境中，拥有此角色的管理员可以配置和管理容器联合，以及管理远程容器会话。</p> <p>在根访问组上拥有“管理员”角色的管理员是超级用户，因为他们对系统中的所有清单对象拥有完全访问权限。由于管理员角色包含所有特权，您应该将其分配给一组有限的用户。最初，将在根访问组上为连接服务器主机上的本地 Administrators 组成员授予此角色。</p> <p>重要事项 管理员必须在根访问组上拥有“管理员”角色才能执行以下任务：</p> <ul style="list-style-type: none"> ■ 添加和删除访问组。 ■ 在 Horizon Console 中管理 ThinApp 应用程序和配置设置。 ■ 使用 vdmadmin、vdmimport 和 lmvutil 命令。 	是
管理员 (只读)	<ul style="list-style-type: none"> ■ 查看但不能修改全局设置和清单对象。 ■ 查看但不能修改 ThinApp 应用程序和设置。 ■ 运行所有 PowerShell 命令和命令行实用程序（包括 vdmexport，但不包括 vdmadmin、vdmimport 和 lmvutil）。 <p>在 Cloud Pod 架构环境中，拥有此角色的管理员可以查看全局数据层中的清单对象和设置。</p> <p>当管理员在某个访问组上拥有此角色时，他们只能查看该访问组中的清单对象。</p>	是
代理注册管理员	注册未受管的计算机（如物理系统、独立的虚拟机和 RDS 主机）。	否
全局配置和策略管理员	查看和修改除管理员角色和权限以外的全局策略和配置设置，以及 ThinApp 应用程序和设置。	否
全局配置和策略管理员 (只读)	查看但不能修改除管理员角色和权限以外的全局策略和配置设置，以及 ThinApp 应用程序和设置。	否
技术支持管理员	<p>执行桌面和应用程序操作（如关闭、重置和重新启动），以及远程协助操作（如结束用户桌面或应用程序的进程）。管理员必须具有根访问组权限才能访问 Horizon Help Desk Tool。</p> <ul style="list-style-type: none"> ■ 对 Horizon Help Desk Tool 进行只读访问。 ■ 管理全局会话。 ■ 可以登录到 Horizon Console。 ■ 执行所有计算机命令和会话相关命令。 ■ 管理远程进程和应用程序。 ■ 对虚拟桌面或已发布的桌面进行远程协助。 	否
技术支持管理员 (只读)	<p>查看用户和会话信息，以及深入了解会话详细信息。管理员必须具有根访问组权限才能访问 Horizon Help Desk Tool。</p> <ul style="list-style-type: none"> ■ 对 Horizon Help Desk Tool 进行只读访问。 ■ 可以登录到 Horizon Console。 	否

角色	用户能力	应用于访问组
清单管理员	<ul style="list-style-type: none"> ■ 执行所有与计算机、会话和池相关的操作。 ■ 管理永久磁盘。 ■ 对链接克隆池进行重新同步、刷新和重新平衡，以及更改默认池映像。 ■ 管理自动场。 <p>当管理员在某个访问组上拥有此角色时，他们只能对该访问组中的清单对象执行这些操作。</p> <p>拥有此角色的管理员不能创建手动场或未受管的手动池，也不能在该场或未受管的手动池中添加或移除 RDS 主机。</p>	是
清单管理员 (只读)	<p>查看但不能修改清单对象。</p> <p>当管理员在某个访问组上拥有此角色时，他们只能查看该访问组中的清单对象。</p>	是
本地管理员	<p>执行除创建其他管理员用户和组以外的所有本地管理员操作。在 Cloud Pod 架构环境中，拥有此角色的管理员不能对全局数据层执行操作或管理远程容器上的会话。</p> <p>注 拥有“本地管理员”角色的管理员不能访问 Horizon Help Desk Tool。非 CPA 环境中的管理员不具有“管理全局会话”特权，而这是在 Horizon Help Desk Tool 中执行任务所必需的。</p>	是
本地管理员 (只读)	<p>除了不能查看全局数据层中的清单对象和设置外，其他都与“管理员 (只读)”角色相同。拥有此角色的管理员只对本地容器具有只读权限。</p> <p>注 拥有“本地管理员 (只读)”角色的管理员不能访问 Horizon Help Desk Tool。非 CPA 环境中的管理员不具有“管理全局会话”特权，而这是在 Horizon Help Desk Tool 中执行任务所必需的。</p>	是

全局特权

全局特权控制整个系统的操作，例如查看和更改全局设置。只包含全局特权的角色不能应用于访问组。

下表介绍了全局特权，并列出了包含各个特权的预定义角色。

表 7-7. 全局特权

特权	用户能力	预定义角色
控制台交互	登录并使用 Horizon Console。	管理员 管理员 (只读) 清单管理员 清单管理员 (只读) 全局配置和策略管理员 全局配置和策略管理员 (只读) 技术支持管理员 技术支持管理员 (只读) 本地管理员 本地管理员 (只读)
直接交互	运行所有 PowerShell 命令和命令行实用程序（vdmadmin 和 vdmimport 除外）。 管理员必须在根访问组上具有管理员角色才能使用 vdmadmin、vdmimport 和 lmvutil 命令。	管理员 管理员 (只读)
管理全局配置和策略	查看和修改全局策略与配置设置（针对管理员角色和权限的设置除外）。	管理员 全局配置和策略管理员
管理全局会话	在 Cloud Pod 架构环境中管理全局会话。	管理员
管理角色和权限	创建、修改和删除管理员角色和权限。	管理员
注册代理	在未受管的计算机（如物理系统、独立的虚拟机和 RDS 主机）上安装 Horizon Agent。 在 Horizon Agent 安装过程中，您必须提供管理员登录凭据，才能在连接服务器实例上注册未受管理的计算机。	管理员 代理注册管理员

特定于对象的特权

对象专用特权用于控制可对特定类型的清单对象执行的操作。包含特定于对象的特权的角色可以应用于访问组。

下表介绍了特定于对象的特权。预定义角色 **Administrators** 和 **Inventory Administrators** 中包含所有这些特权。

表 7-8. 特定于对象的特权

特权	用户能力	对象
启用场和桌面池	启用和禁用桌面池。	桌面池、场
授权桌面和应用程序池	添加和移除用户授权。	桌面池、应用程序池
管理 Composer 桌面池映像	对链接克隆池进行重新同步、刷新和重新平衡，以及更改默认池映像。	桌面池
管理计算机	执行与计算机和会话相关的所有操作。	计算机
管理永久磁盘	执行所有 Horizon Composer 永久磁盘操作，包括附加、分离和导入永久磁盘。	永久磁盘

特权	用户能力	对象
管理场以及桌面和应用程序池	添加、修改和删除场。添加、修改、删除和授权桌面及应用程序池。添加和移除计算机。	桌面池、应用程序池、场
管理会话	断开连接并注销会话，然后向用户发送消息。	会话
管理重新引导操作	重置虚拟机或重新启动虚拟桌面。	计算机

内部特权

某些预定义的管理员角色包含内部特权。您在创建自定义角色时无法选择内部特权。

下表介绍了内部特权，并列出了包含各个特权的预定义角色。

表 7-9. 内部特权

特权	说明	预定义角色
完整 (只读)	授予对所有设置的只读访问权限。	管理员 (只读)
管理清单 (只读)	授予对清单对象的只读访问权限。	清单管理员 (只读)
管理全局配置和策略 (只读)	授予只读访问配置设置和全局策略的权限，管理员和角色除外。	全局配置和策略管理员 (只读)

执行常见任务所需的特权

许多常见管理任务需要使用一组相互配合的特权。某些操作除了需要访问所操作对象的权限外，还需要根访问组的权限。

管理池所需的特权

管理员必须拥有某些特权才能在 Horizon Console 中管理池。

下表列出了常见的池管理任务，并显示了执行每项任务所需的特权。

表 7-10. 池管理任务和特权

任务	所需特权
启用或禁用桌面池。	启用场和桌面池
授权或取消授权用户访问池。	授权桌面和应用程序池
添加池。	管理场以及桌面和应用程序池 注 不适用于添加未受管桌面池。管理员还必须具有“全局配置和策略管理员 (只读)”角色，才能执行此任务。
修改或删除池。	管理场以及桌面和应用程序池 注 不适用于删除未受管桌面池。管理员还必须具有“全局配置和策略管理员 (只读)”角色，才能执行此任务。

任务	所需特权
在池中添加或移除桌面。	管理场以及桌面和应用程序池 注 不适用于在桌面池中添加或移除未受管虚拟桌面。管理员还必须具有“全局配置和策略管理员 (只读)”角色，才能执行此任务。
刷新、重构、重新平衡或更改默认的 Horizon Console 映像。	管理 Composer 桌面池映像
更改访问组。	同时对源和目标访问组拥有 管理场以及桌面和应用程序池 特权。

管理计算机所需的特权

管理员必须拥有某些特权才能在 Horizon Console 中管理计算机。

下表列出了常见的计算机管理任务，并显示了执行每项任务所需的特权。

表 7-11. 计算机管理任务和特权

任务	所需特权
移除虚拟机。	管理计算机或管理场以及桌面和应用程序池 注 不适用于从桌面池或场中移除未受管桌面或 RDS 主机。管理员还必须具有“全局配置和策略管理员 (只读)”角色，才能执行此任务。
重置虚拟机。	管理重新引导操作
重新启动虚拟桌面。	管理重新引导操作
分配或移除用户所有权。	管理计算机
进入或退出维护模式。	管理计算机
断开会话连接或注销会话。	管理会话

管理永久磁盘所需的特权

管理员必须拥有某些特权才能在 Horizon Console 中管理永久磁盘。

下表列出了常见的永久磁盘管理任务，并显示了执行每项任务所需的特权。您可在 Horizon Console 中的“永久磁盘”页面上执行这些任务。

表 7-12. 永久磁盘管理任务和特权

任务	所需特权
分离磁盘。	对磁盘拥有 管理永久磁盘 特权，对池拥有 管理场以及桌面和应用程序池 特权。
附加磁盘。	对磁盘拥有 管理永久磁盘 特权，对计算机拥有 管理场以及桌面和应用程序池 特权。
编辑磁盘。	对磁盘拥有 管理永久磁盘 特权，对选定的池拥有 管理场以及桌面和应用程序池 特权。
更改访问组。	对源和目标访问组拥有 管理永久磁盘 特权。
重新创建桌面。	对磁盘拥有 管理永久磁盘 特权，对最后一个池拥有 管理场以及桌面和应用程序池 特权。

任务	所需特权
从 vCenter 导入。	对文件夹拥有 管理永久磁盘 特权，对池拥有 管理池 特权。
删除磁盘。	对磁盘拥有 管理永久磁盘 特权。

管理用户和管理员所需的特权

管理员必须拥有某些特权才能在 Horizon Console 中管理用户和管理员。

下表列出了常见的用户和管理员管理任务，并显示了执行每项任务所需的特权。您可在 Horizon Console 中的**用户和组**页面上对用户进行管理，并在 Horizon Console 中的**全局管理员视图**页面上对管理员进行管理。

表 7-13. 用户和管理员管理任务和特权

任务	所需特权
更新常规用户信息。	管理全局配置和策略
向用户发送消息。	计算机上的 管理远程会话 。
添加管理员用户或组。	管理角色和权限
添加、修改或删除管理员权限。	管理角色和权限
添加、修改或删除管理员角色。	管理角色和权限

Horizon Help Desk Tool 任务所需的特权

Horizon Help Desk Tool 管理员必须拥有某些特权才能在 Horizon Console 中执行故障排除任务。

下表列出了 Horizon Help Desk Tool 管理员可以执行的常见任务，并显示了执行每项任务所需的特权。

表 7-14. Horizon Help Desk Tool 任务和特权

任务	所需特权
对 Horizon Help Desk Tool 进行只读访问。	管理技术支持门户 (只读)
管理全局会话。	管理全局会话
可以登录到 Horizon Console。	控制台交互
执行所有计算机命令和会话相关命令。	管理计算机
重置或重新启动计算机。	管理重新引导操作
断开会话连接和注销会话。	管理会话
管理远程进程和应用程序。	管理远程进程和应用程序
对虚拟桌面或已发布的桌面进行远程协助。	远程协助
全局会话的断开连接、注销、重置和重新启动操作。	管理技术支持门户 (只读) 以及 管理全局会话
本地会话的重置和重新启动操作。	管理技术支持门户 (只读) 以及 管理重新引导操作
远程协助操作。	管理技术支持门户 (只读) 以及 远程协助
结束远程进程和应用程序。	管理技术支持门户 (只读) 以及 管理远程进程和应用程序

任务	所需特权
在 Horizon Help Desk Tool 中执行所有任务。	管理技术支持门户 (只读)、管理全局会话、管理重新引导操作、远程协助以及管理远程进程和应用程序
远程协助操作，以及结束远程进程和应用程序。	管理技术支持门户 (只读)、远程协助以及管理远程进程和应用程序
本地会话的断开连接和注销操作。	管理技术支持门户 (只读) 以及管理会话

执行常规管理任务和命令所需的特权

管理员必须具有某些特权才能执行常规管理任务和运行命令行实用程序。

下表显示了执行常规管理任务和运行命令行实用程序所需的特权。

表 7-15. 执行常规管理任务和命令所需的特权

任务	所需特权
添加或删除访问组	必须在根访问组上具有管理员角色。
在 Horizon Administrator 中管理 ThinApp 应用程序和设置	必须在根访问组上具有管理员角色。
在未受管的计算机（如物理系统、独立虚拟机或 RDS 主机）上安装 Horizon Agent	注册代理
查看或修改 Horizon Administrator 中的配置设置（针对管理员的设置除外）	管理全局配置和策略
运行所有 PowerShell 命令和命令行实用程序（vdmadmin 和 vdmimport 除外）。	直接交互
使用 vdmadmin 和 vdmimport 命令	必须在根访问组上具有管理员角色。
使用 vdmexport 命令	必须在根访问组上具有管理员角色或管理员 (Read only) 角色。

针对管理员用户和组的最佳实践

要增加您的 Horizon 7 环境的安全性和可管理性，在管理管理员用户和组时应该遵循以下最佳实践。

- 在 Active Directory 中创建新用户组并向这些组分配管理角色。避免使用 Windows 内置组或其他可能包含不需要或不应该具有 Horizon 7 特权的用户的现有组。
- 使具有 Horizon 7 管理特权的用户数量最少。
- 由于管理员角色具有所有特权，因此该角色不应当用于日常管理。
- 由于名称 Administrator 太过明显而且很容易猜到，因此在创建管理员用户和组时要避免使用该名称。
- 创建访问组以隔离敏感的桌面和场。将这些访问组的管理权委托给一组有限的用户。
- 创建可以修改全局策略和 Horizon 7 配置设置的单独管理员。

在 Horizon Console 中设置策略

您可以使用 **Horizon Console** 配置客户端会话策略。

您可以将这些策略设置为影响特定用户、特定桌面池或所有客户端会话用户。影响特定用户和桌面池的策略称为用户级别策略和桌面池级别策略。影响所有会话和用户的策略称为全局策略。

用户级别策略将从等效的桌面池级别策略设置继承设置。同样，桌面池级别策略将从等效的全局策略设置继承设置。桌面池级别策略设置优先于等效的全局策略设置。用户级别策略设置优先于等效的全局和池级别策略设置。

低级别策略设置可能比等效的高级别设置或多或少地要严格。例如，您可以将某个全局策略设置为**拒绝**，并将等效的桌面池级别策略设置为**允许**，反之亦然。

注 仅全局策略适用于已发布的桌面和应用程序池。无法为已发布的桌面和应用程序池设置用户级别的策略或池级别的策略。

本章讨论了以下主题：

- [配置全局策略](#)

配置全局策略

您可以配置全局策略以控制所有客户端会话用户的行为。

步骤

- 1 在 **Horizon Console** 中，选择**设置 > 全局策略**。

全局策略窗格显示了将影响所有客户端会话、桌面池或用户的设置。

表 8-1. Horizon 策略

策略	说明
多媒体重定向 (MMR)	<p>确定是否为客户端系统启用 MMR。</p> <p>MMR 是一种 Windows Media Foundation 过滤器，可直接通过 TCP 套接字将多媒体数据从远程桌面中的特定编解码器转发至客户端系统。随后，直接在播放数据的客户端系统中解码数据。</p> <p>默认值为拒绝。</p> <p>如果客户端系统没有足够的资源来处理本地多媒体解码，请将设置保留为拒绝。</p> <p>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。</p>
USB 访问	<p>确定远程桌面是否可以使用 USB 设备连接客户端系统。</p> <p>默认值为允许。如果出于安全因素阻止使用外部设备，请将设置更改为拒绝。</p>
PCoIP 硬件加速	<p>确定是否启用 PCoIP 显示协议的硬件加速，指定分配给 PCoIP 用户会话的加速优先级。</p> <p>仅在托管远程桌面的物理机中装有 PCoIP 硬件加速设备时，此设置才有效。</p> <p>默认值为允许，优先级为中。</p>

2 单击**编辑策略**以更改设置。

3 单击**确定**保存更改。

维护 Horizon 7 组件

为保持 Horizon 7 组件可用并正常运行，您可以执行多种维护任务。

本章讨论了以下主题：

- 备份和还原 Horizon 7 配置数据
- 还原 Horizon 连接服务器和 Horizon Composer 配置数据
- 导出 Horizon Composer 数据库中的数据
- 在 Horizon Console 中更改产品许可证密钥或许可证模式
- 监控许可证使用情况
- 客户体验提升计划

备份和还原 Horizon 7 配置数据

您可以通过在 Horizon Console 中计划或运行自动备份来备份 Horizon 7 和 Horizon Composer 配置数据。通过手动导入备份的 View LDAP 文件和 Horizon Composer 数据库文件，可以还原 Horizon 7 配置。

您可以使用备份和还原功能保留和迁移 Horizon 7 配置数据。

备份 Horizon 连接服务器和 Horizon Composer 数据

完成连接服务器的初始配置后，您应计划对 Horizon 7 和 Horizon Composer 配置数据进行定期备份。您可以通过使用 Horizon Console 来保留 Horizon 7 和 Horizon Composer 数据。

Horizon 7 将连接服务器配置数据存储在 View LDAP 存储库中。Horizon Composer 将链接克隆桌面的配置数据存储在 Horizon Composer 数据库中。

当您使用 Horizon Console 执行备份时，Horizon 7 会备份 View LDAP 配置数据和 Horizon Composer 数据库。两个备份文件集都存储在同一位置。View LDAP 数据将以加密的 LDAP 数据交换格式 (LDIF) 导出。有关 View LDAP 的说明，请参阅《Horizon 7 管理指南》文档中的“View LDAP 目录”。

您可以通过多种方式来执行备份。

- 使用 Horizon 7 配置备份功能可计划自动备份。
- 使用 Horizon Console 中的**立即备份**功能可即刻开始备份。
- 使用 vdmexport 实用程序手动导出 View LDAP 数据。每个连接服务器实例均附带了此实用程序。

vdmexport 实用程序可将 View LDAP 数据导出为加密 LDIF 数据、纯文本或移除了密码和其他敏感数据的纯文本。

注 **vdmexport** 工具仅备份 View LDAP 数据。此工具不会备份 Horizon Console 数据库信息。

有关 **vdmexport** 的更多信息，请参阅[从 Horizon 连接服务器中导出配置数据](#)。

以下指导原则适用于 Horizon 7 配置数据备份：

- Horizon 7 可以从任何连接服务器实例中导出配置数据。
- 如果您的副本实例组中有多个连接服务器实例，则只需从一个实例中导出数据。所有副本实例均包含相同的配置数据。
- 不要将连接服务器副本实例作为备份机制。如果 Horizon 7 将各个连接服务器副本实例中的数据同步，那么一个实例中的任何数据丢失可能会导致所有组成员中均丢失相应数据。
- 如果连接服务器结合使用多个 vCenter Server 实例和多种 Horizon Composer 服务，那么 Horizon 7 会备份与 vCenter Server 实例关联的所有 Horizon Composer 数据库。

计划 Horizon 7 配置备份

您可计划定期备份 Horizon 7 配置数据。Horizon 7 将备份 View LDAP 存储库（连接服务器实例用其存储配置数据）的内容。

选择连接服务器实例并单击**立即备份**，即可立即备份配置。

前提条件

熟悉备份设置。请参阅[Horizon 7 配置备份设置](#)。

步骤

- 1 在 Horizon Console 中，选择**设置 > 服务器**。
- 2 在**连接服务器**选项卡上，选择要备份的连接服务器实例，然后单击**立即备份**。
- 3 在**备份**选项卡上，指定 Horizon 7 配置备份设置以配置备份频率、最大备份数以及备份文件所在的文件夹位置。
- 4 （可选）更改数据恢复密码。
 - a 单击**更改数据恢复密码**。
 - b 键入并再次键入新的密码。
 - c （可选）键入密码提醒。
 - d 单击**确定**。
- 5 单击**确定**。

Horizon 7 配置备份设置

Horizon 7 可以定期备份连接服务器和 Horizon Composer 配置数据。您可以在 Horizon Console 中设置备份操作的频率和其他设置。

表 9-1. Horizon 7 配置备份设置

设置	说明
自动备份频率	<p>每小时：每小时整点进行备份。</p> <p>每 6 小时：在零点、上午 6 点、中午 12 点和下午 6 点进行备份。</p> <p>每 12 小时：在零点和中午 12 点进行备份。</p> <p>每天：每天零点进行备份。</p> <p>每 2 天：在星期六、星期一、星期三和星期五的零点进行备份。</p> <p>每周：在每周星期六的零点进行备份。</p> <p>每 2 周：在每隔一周的星期六零点进行备份。</p> <p>从不：不自动进行备份。</p>
备份时间	计划备份的时间。
备份时间偏移	已计划的备份的时间偏移。
最大备份数量	<p>连接服务器实例上可以存储的最大备份文件数。该数必须是大于 0 的整数。</p> <p>达到最大数量时，Horizon 7 会删除最早的备份文件。</p> <p>此设置还适用于您使用立即备份功能创建的备份文件。</p>
文件夹位置	<p>运行连接服务器的计算机上的默认备份文件位置：C:\Programdata\VMware\VDM\backups</p> <p>当您使用立即备份时，Horizon 7 也会将备份文件存储在此位置。</p>

从 Horizon 连接服务器中导出配置数据

您可以通过导出 Horizon 连接服务器实例的 View LDAP 存储库内容来备份其配置数据。

使用 **vdmexport** 命令将 View LDAP 配置数据导出到加密的 LDIF 文件中。也可使用 **vdmexport -v**（逐字）选项将数据导出到纯文本 LDIF 文件中，或使用 **vdmexport -c**（已清除）选项将数据以纯文本形式导出，并移除密码和其他敏感数据。

您可以在任意连接服务器实例上运行 **vdmexport** 命令。如果您的副本实例组中有多个连接服务器实例，则只需从一个实例中导出数据。所有副本实例均包含相同的配置数据。

注 **vdmexport** 命令仅备份 View LDAP 数据。此命令不会备份 Horizon Composer 数据库信息。

前提条件

- 从以下默认路径中找出随连接服务器安装的 **vdmexport.exe** 命令可执行文件。

C:\Program Files\VMware\VMware View\Server\tools\bin

- 以管理员或管理员 (只读) 用户角色登录到连接服务器实例。

步骤

- 1 选择开始 > 命令提示符。

- 2 在命令提示符下，键入 `vdmexport` 命令，并将输出重定向至文件。例如：

```
vdmexport > Myexport.LDF
```

默认情况下，导出数据是加密的。

您可以将输出文件的名称指定为 `-f` 选项的一个参数。例如：

```
vdmexport -f Myexport.LDF
```

您可以使用 `-v` 选项以纯文本的格式（逐字）导出数据。例如：

```
vdmexport -f Myexport.LDF -v
```

您可以使用 `-c` 选项以纯文本格式导出数据并移除密码和敏感数据（已清除）。例如：

```
vdmexport -f Myexport.LDF -c
```

注 不要使用清除过的备份数据来还原 View LDAP 配置。清除过的配置数据缺少密码和其他重要信息。

有关 `vdmexport` 命令的更多信息，请参阅《Horizon 7 集成指南》文档。

后续步骤

您可使用 `vdmimport` 命令来还原或传输连接服务器的配置信息。

有关导入 LDIF 文件的详细信息，请参阅[还原 Horizon 连接服务器](#)和[Horizon Composer 配置数据](#)。

还原 Horizon 连接服务器和 Horizon Composer 配置数据

您可以手动还原由 Horizon 7 备份的连接服务器 LDAP 配置文件和 Horizon Composer 数据库文件。

您需要手动运行不同的实用程序来还原连接服务器和 Horizon Composer 配置数据。

还原配置数据前，请确认您在 Horizon Console 中备份了配置数据。请参阅[备份 Horizon 连接服务器和 Horizon Composer 数据](#)。

使用 `vdmimport` 实用程序将连接服务器数据从 LDIF 备份文件导入到连接服务器实例中的 View LDAP 存储库。

您可以使用 `SviConfig` 实用程序将 Horizon Composer 数据从 `.svi` 备份文件导入到 Horizon Composer SQL 数据库中。

注 在某些情况下，您可能需要安装当前版本的连接服务器实例，然后通过导入连接服务器 LDAP 配置文件来还原现有的 Horizon 7 配置。您可能需要将此过程纳入业务连续性和灾难恢复 (BC/DR) 计划中，也可能需要将其作为使用现有 Horizon 7 配置设置其他数据中心的一个步骤，或者出于其他原因需要执行此过程。有关更多信息，请参阅《Horizon 7 安装指南》文档。

将配置数据导入 Horizon 连接服务器中

您可以通过导入 LDIF 文件中存储的数据备份副本，来还原连接服务器实例的配置数据。

使用 `vdmimport` 命令将 LDIF 文件的数据导入到连接服务器实例中的 View LDAP 存储库。

如果您已通过使用 Horizon Console 或默认 `vdmexport` 命令备份了 View LDAP 配置，则导出的 LDIF 文件是加密的。在导入前您必须解密此 LDIF 文件。

如果导出的 LDIF 文件是纯文本格式的，则您无需解密该文件。

注 不要以清除过的格式（移除了密码和其他敏感数据的纯文本）导入 LDIF 文件。否则，重要配置信息将从恢复的 View LDAP 存储库中丢失。

有关备份 View LDAP 存储库的信息，请参阅[备份 Horizon 连接服务器和 Horizon Composer 数据](#)。

前提条件

- 从以下默认路径中找出随连接服务器安装的 `vdmimport` 命令可执行文件。
`C:\Program Files\VMware\VMware View\Server\tools\bin`
- 以具有管理员角色的用户身份登录到连接服务器实例。
- 确认您知道数据恢复密码。如果配置了密码提醒，则您可通过运行不含密码选项的 `vdmimport` 命令来显示提醒。

步骤

- 1 通过停止在其中运行 Horizon Composer 的服务器上的 VMware Horizon Composer Windows 服务，停止 Horizon Composer 的所有实例。
- 2 卸载所有 Horizon 连接服务器实例。
 卸载 VMware Horizon 连接服务器和 AD LDS Instance VMwareVDMDS。
- 3 安装连接服务器的一个实例。
- 4 通过停止 Windows 服务 VMware Horizon 连接服务器停止连接服务器实例。
- 5 单击**开始 > 命令提示符**。
- 6 解密已加密的 LDIF 文件。

通过命令提示符键入 `vdmimport` 命令。指定 `-d` 选项、包含数据恢复密码的 `-p` 选项和包含现有加密 LDIF 文件的 `-f` 选项（后附已解密 LDIF 文件的名称）。例如：

如果您不记得数据恢复密码，则可键入不带 `-p` 选项的命令。实用程序显示密码提醒并提示您输入密码。

- 7 导入解密的 LDIF 文件还原 View LDAP 配置。
 指定含有已解密的 LDIF 文件的 `-f` 选项。例如：
- 8 卸载连接服务器。
 仅卸载 VMware Horizon 连接服务器软件包。

- 9 重新安装连接服务器。
- 10 登录到 Horizon Console 并验证配置是否正确。
- 11 启动 Horizon Composer 实例。
- 12 重新安装副本服务器实例。

`vdmimport` 命令将使用该 LDIF 文件中的配置数据更新连接服务器中的 View LDAP 存储库。有关 `vdmimport` 命令的更多信息，请参阅《Horizon 7 安装指南》文档。

注 确保要还原的配置与 vCenter Server 和 Horizon Composer（如果在使用中）的已知虚拟机相匹配。必要时，请从备份还原 Horizon Composer 配置。请参阅[还原 Horizon Composer 数据库](#)。还原 Horizon Composer 配置后，如果 vCenter Server 中的虚拟机自备份 Horizon Composer 配置以来发生过更改，则您可能需要手动解决此不一致问题。

还原 Horizon Composer 数据库

您可以将 Horizon Composer 配置的备份文件导入存储链接克隆信息的 Horizon Composer 数据库中。

使用 `SviConfig restoredata` 命令，您可以在系统出现故障后还原 Horizon Composer 数据库数据，或是将 Horizon Composer 配置恢复到某个早期状态。

重要事项 只能由经验丰富的 Horizon Composer 管理员使用 `SviConfig` 实用程序。该实用程序旨在解决与 Horizon Composer 服务相关的问题。

前提条件

确认 Horizon Composer 数据库备份文件的位置。默认情况下，Horizon 7 将备份文件存储在连接服务器计算机的 C: 驱动器上，路径为 `C:\Programdata\VMWare\VDM\backups`。

Horizon Composer 备份文件采用带日期戳和 `.svi` 后缀的命名约定。

`Backup-YearMonthDayCount-vCenter Server Name_Domain Name.svi`

例如: `Backup-20090304000010-foobar_test_org.svi`

熟悉 `SviConfig restoredata` 参数:

- **DsnName** - 用于连接至数据库的 DSN。DsnName 参数是必填项，并且不能是空字符串。
- **Username** - 用于连接至数据库的用户名。如果未指定该参数，则使用 Windows 身份验证。
- **Password** - 连接至数据库的用户密码。如果未指定该参数且未使用 Windows 身份验证，系统会提示您稍后再输入密码。
- **BackupFilePath** - Horizon Composer 备份文件的路径。

DsnName 和 **BackupFilePath** 参数是必填项，并且不能是空字符串。**Username** 和 **Password** 参数是可选项。

步骤

- 1 将 Horizon Composer 备份文件从连接服务器计算机复制到可从安装了 VMware Horizon Composer 服务的计算机访问的位置。
- 2 在安装了 Horizon Composer 的计算机上，停止 VMware Horizon Composer 服务。
- 3 打开 Windows 命令提示并导航到 SviConfig 可执行文件。

该文件与 Horizon Composer 应用程序位于同一位置。默认路径为 C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe。

- 4 运行 SviConfig restoredata 命令。

```
sviconfig -operation=restoredata
          -DsnName=target_database_source_name_(DSN)
          -Username=database_administrator_username
          -Password=database_administrator_password
          -BackupFilePath=path_to_View_Composer_backup_file
```

例如：

```
sviconfig -operation=restoredata -dsnname=LinkedClone
          -username=Admin -password=Pass
          -backupfilepath="C:\Program Files (x86)\VMware\VMware View
          Composer\Backup-20090304000010-foobar_test_org.SVI"
```

- 5 启动 VMware Horizon Composer 服务。

后续步骤

有关 SviConfig restoredata 命令的输出结果代码，请参阅[还原 Horizon Console 数据库时显示的结果代码](#)。

还原 Horizon Console 数据库时显示的结果代码

还原 Horizon Console 数据库时，SviConfig restoredata 命令会显示一个结果代码。

表 9-2. Restoredata 结果代码

代码	说明
0	操作成功结束。
1	找不到所提供的 DSN。
2	提供的数据库管理员凭据无效。
3	数据库的驱动程序不受支持。
4	出现异常问题，命令无法完成。
14	其他应用程序正在使用 VMware Horizon Console 服务。执行命令前，请关闭该服务。
15	还原过程中出现问题。屏幕日志输出中提供了详细信息。

导出 Horizon Composer 数据库中的数据

您可以将 Horizon Composer 数据库中的数据导出到文件。

重要事项 只有经验丰富的 Horizon Composer 管理员才能使用 SviConfig 实用程序。

前提条件

默认情况下，Horizon 7 将备份文件存储在连接服务器计算机的 C: 驱动器上，路径为 C:\Programdata\VMware\VDM\backups。

熟悉 SviConfig exportdata 参数：

- DsnName - 用于连接至数据库的 DSN。如果未指定，DSN 名称、用户名和密码将从服务器配置文件中检索。
- Username - 用于连接至数据库的用户名。如果未指定该参数，则使用 Windows 身份验证。
- Password - 连接至数据库的用户密码。如果未指定该参数且未使用 Windows 身份验证，系统会提示您稍后再输入密码。
- OutputFilePath - 输出文件路径。

步骤

- 1 在安装了 Horizon Composer 的计算机上，停止 VMware Horizon Composer 服务。
- 2 打开 Windows 命令提示并导航到 SviConfig 可执行文件。

该文件与 Horizon Composer 应用程序位于同一位置。

Horizon-Composer-installation-directory\sviconfig.exe

- 3 运行 SviConfig exportdata 命令。

```
sviconfig -operation=exportdata
          -DsnName=target_database_source_name_(DSN)
          -Username=database_administrator_username
          -Password=database_administrator_password
          -OutputFilePath=path_to_Horizon_Composer_output_file
```

例如：

```
sviconfig -operation=exportdata -dsname=LinkedClone
          -username=Admin -password=Pass
          -outputfilepath="C:\Program Files\VMware\VMware View
Composer\Export-20090304000010-foobar_test_org.SVI"
```

后续步骤

有关 SviConfig exportdata 命令的导出结果代码，请参阅[导出 Horizon Composer 数据库时显示的结果代码](#)。

导出 Horizon Composer 数据库时显示的结果代码

导出 Horizon Composer 数据库时，SviConfig exportdata 命令会显示一个退出代码。

表 9-3. Exportdata ExitStatus 代码

代码	说明
0	数据导出成功结束。
1	无法找到提供的 DSN 名称。
2	所提供的凭据无效。
3	所提供数据库不支持的驱动程序。
4	出现异常问题。
18	无法连接到数据库服务器。
24	无法打开输出文件。

在 Horizon Console 中更改产品许可证密钥或许可证模式

如果系统中当前的许可证到期，或者您要访问当前未经许可的 Horizon 7 功能，则可以使用 Horizon Console 更改产品许可证密钥。根据 VMware Horizon Cloud Service 上的 Horizon 7 部署，您可以获取适用于 Horizon 7 的永久许可证或订阅许可证。您可以使用 Horizon Console 将容器的许可证模式从订阅许可证更改为永久许可证，反之亦然。

Horizon 7 正在运行时，您可以向 Horizon 7 添加许可证。无需重新引导系统，对桌面和应用程序的访问也不会中断。

前提条件

- 要成功操作 Horizon 7 及其加载功能（如 Horizon Composer 和已发布的应用程序），请获取有效的产品许可证密钥。
- 要使用订阅许可证，请确认为订阅许可证启用 Horizon 7。请参阅《Horizon 7 安装指南》文档。许可面板会显示有关 Horizon 7 容器订阅许可证的信息。

步骤

- 1 在 Horizon Console 中，选择**设置 > 产品许可和使用情况**。
将在**许可**面板中显示当前许可证密钥的第一个和最后五个字符。
- 2 要编辑许可证密钥，请单击**编辑许可证**，输入许可证序列号，然后单击**确定**。
许可**设置**面板将显示更新的许可信息。
- 3 （可选）要将 Horizon 7 容器从订阅许可证更改为永久许可证，请单击**使用永久许可证**，然后单击**确定**。
许可**设置**面板将显示更新的许可信息。

- 4 （可选）要将 Horizon 7 容器从永久许可证更改为订阅许可证，请单击**使用订阅许可证**，然后单击**确定**。然后，VMware Horizon Cloud Service 管理员可以为订阅许可证启用 Horizon 7 容器。

许可设置面板将显示更新的许可信息。

- 5 验证许可证的过期日期。
- 6 根据产品许可证授权您使用的 VMware Horizon 7 版本，验证是启用还是禁用了桌面、应用程序远程处理和 Horizon Composer 许可证。

并非所有版本都提供 VMware Horizon 7 的所有特性和功能。有关各个版本中的功能集的比较，请参阅 <http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf>。

- 7 验证许可使用模式是否与产品许可证中使用的模式匹配。

使用情况是按照命名用户或并发用户数计算的，具体取决于产品许可证的版本和使用协议。

监控许可证使用情况

在 Horizon Console 中，您可以监控同时连接到 Horizon 7 的活动用户。**使用情况设置**面板会显示当前和最高历史使用用户数。您可以通过这些数字跟踪产品许可证的使用情况。另外，还可以重置历史使用情况数据并重新开始当前数据。

Horizon 7 提供了两种许可使用模式，一种模式用于命名用户，另一种模式用于并发用户。Horizon 7 计算环境中的命名用户和并发用户，而无论使用哪种产品许可证版本或使用模式协议。

对于命名用户，Horizon 7 计算已访问 Horizon 7 环境的唯一用户数。如果命名用户运行多个单用户桌面、已发布的桌面和已发布的应用程序，则将该用户计入一次。

对于命名用户，**使用情况设置**面板上的**当前**列会显示在首次配置 Horizon 7 部署或上次重置命名用户计数后的用户数。**最高**列不适用于命名用户。

对于并发用户，Horizon 7 计算每个会话的单用户桌面连接数。如果并发用户运行多个单用户桌面，将单独计算每个连接的桌面会话。

对于并发用户，将计算每个用户的已发布桌面和应用程序连接数。如果并发用户运行多个已发布的桌面会话和应用程序，则仅将该用户计入一次，即使在不同的 RDS 主机上托管了不同的已发布桌面或应用程序也是如此。如果并发用户运行一个单用户桌面以及其他已发布的桌面和应用程序，则仅将该用户计入一次。

对于并发用户，**使用情况设置**面板上的**最高**列会显示在首次配置 Horizon 7 部署或上次重置最大计数后的最高并发桌面会话数以及已发布的桌面和应用程序用户数。

您可以监视协作会话的数量以及连接到会话的会话协作者数量。

- “活动 - 协作会话”：会话所有者邀请了一个或多个用户加入会话的会话数量。示例：John 邀请了一个人加入他的会话，Mary 邀请了一个人加入她的会话。此行的值为 2，而不管是否有任何受邀者加入了会话。

- “活动 - 协作者总数”：连接到协作会话的用户总数，包括会话所有者和任何协作者。示例：John 邀请了一个人，但只有一个人加入了会话。Mary 邀请了一个人，但该人没有加入会话。此行的值为 3：John 的协作会话有一个主协作者和一个辅助协作者，而 Mary 的协作会话有一个主协作者和零个辅助协作者。由于计入了会话所有者，因此可以确保协作者的总数始终大于或等于协作会话的总数。

重置许可证使用情况数据

在 Horizon Console 中，您可以重置历史产品使用情况数据并使用当前数据重新开始。

具有**管理全局配置和策略**特权的管理人员可以选择**重置最大计数**和**重置已命名用户计数**设置。要限制访问这些设置，请仅为指定的管理员授予该特权。

前提条件

熟悉产品许可证使用情况。请参阅[监控许可证使用情况](#)。

步骤

- 1 在 Horizon Console 中，选择**设置 > 产品许可和使用情况**。
- 2 （可选）在**使用情况**窗格中，选择**重置最大计数**。
并发连接的最高历史数量将重置为当前数量。
- 3 （可选）在**使用情况**窗格中，选择**重置已命名用户计数**。

客户体验提升计划

此产品参与 VMware 客户体验提升计划 (Customer Experience Improvement Program, CEIP)。您可以选择将此产品加入或退出 CEIP。

“信任与保证中心”（网址为 <http://www.vmware.com/trustvmware/ceip.html>）详细阐述了通过 CEIP 收集的数据以及 VMware 将此数据用于何种用途。

步骤

- 1 在 Horizon Console 中，选择**设置 > 产品许可和使用情况**。
- 2 在**客户体验计划**选项卡中，单击**编辑设置**。
- 3 选择**加入 VMware 客户体验提升计划**以加入 CEIP。
如果不选择此选项，您就不能加入 CEIP。
- 4 （可选）选择您所在的地理位置、您的纵向业务或贵组织中的员工数量。
- 5 单击**确定**。

在 Horizon Console 中创建虚拟桌面池

10

借助 **Horizon 7**，您可以创建包含成千上万个虚拟桌面的桌面池。您可以部署在虚拟机 (VM) 和物理机上运行的桌面。创建一个虚拟机作为主映像后，**Horizon 7** 便可通过该映像生成大量虚拟桌面。主映像也称为基础映像或最佳配置映像。

有关如何创建基础映像或最佳配置映像，以及如何配置用于克隆的虚拟机的更多信息，请参阅《在 **Horizon 7** 中设置虚拟桌面》文档。

在 **Horizon Console** 中，可以创建包含完整虚拟机的即时克隆桌面池或自动桌面池。

本章讨论了以下主题：

- [创建即时克隆桌面池](#)
- [创建包含完整虚拟机的自动桌面池](#)
- [在 **Horizon Console** 中创建链接克隆桌面池](#)
- [在 **Horizon Console** 中创建手动桌面池](#)
- [配置桌面池](#)
- [在 **Horizon Console** 中管理桌面池和虚拟桌面](#)
- [排除计算机和桌面池的问题](#)

创建即时克隆桌面池

要为用户提供对即时克隆桌面的访问权限，必须创建一个即时克隆桌面池。

即时克隆桌面池基于 **vCenter Server** 中的父虚拟机，又称为主映像。对于即时克隆桌面，父虚拟机是 **Horizon 7** 创建并维护的内部虚拟机，该虚拟机基于主映像。您无法修改此内部父虚拟机。但是，您可以对主映像进行更改。

有关创建和维护即时克隆桌面池所需配置的更多信息，请参阅《在 **Horizon 7** 中设置虚拟桌面》文档。

用于在 Horizon Console 中创建即时克隆桌面池的工作表

在创建即时克隆桌面池时，您可以配置某些选项。您可以使用此工作表在创建池之前记录您的配置选项。

在创建即时克隆桌面池之前，需要在 vCenter Server 中为父虚拟机拍摄快照。拍摄快照之前必须在 vCenter Server 中关闭父虚拟机。快照是 vCenter Server 中用于克隆的主映像。

注 您无法通过虚拟机模板创建即时克隆桌面池。

表 10-1. 工作表：用于创建即时克隆桌面池的配置选项

选项	说明	在此填写您要指定的值
用户分配	<p>选择浮动或专用。</p> <p>在浮动用户分配中，会向用户分配池中的随机桌面。</p> <p>在专用用户分配中，会向每个用户分配一个特定的远程桌面，并在每次登录时返回到同一个桌面。在每次登录到注销期间，将会保留同一个桌面的计算机名称和 MAC 地址。用户对该桌面所做的任何其他更改均不会被保留。</p>	
vCenter Server	选择 即时克隆 ，然后选择管理即时克隆虚拟机的 vCenter Server。	
桌面池 ID	<p>标识池的唯一名称。</p> <p>如果您有多个连接服务器配置，请确保不同的连接服务器配置不会使用相同的池 ID。连接服务器配置既可包含单个连接服务器，也可包含多个连接服务器</p>	
显示名称	用户从客户端登录时所看到的池名称。如果您未指定名称，则使用池 ID。	
访问组	<p>为池选择访问组，或者将池留在默认的根访问组中。</p> <p>如果使用访问组，则可以将池的管理委托给某个具有特定角色的管理员。</p> <p>注 访问组不同于存储桌面虚拟机的 vCenter Server 文件夹。您稍后会在向导中选择 vCenter Server 文件夹。</p>	
状态	如果设置为 已启用 ，则表示池已经准备就绪，在置备后便可以使用。如果设置为 已禁用 ，则用户无法使用池。在置备期间，如果禁用池，置备会停止。	
连接服务器限制	<p>您可以限制只有特定连接服务器才能访问池，方法是：单击浏览，然后选择一个或多个连接服务器。</p> <p>如果您想通过 VMware Identity Manager 提供桌面访问，并且配置了连接服务器限制，则当桌面实际受到限制时，VMware Identity Manager 应用程序可能会向用户显示这些桌面。VMware Identity Manager 用户将无法启动这些桌面。</p>	
类别文件夹	为包含 Windows 客户端设备上桌面池授权的“开始”菜单快捷方式的类别文件夹指定名称。	
断开连接后自动注销	<ul style="list-style-type: none"> ■ 立即。用户在断开连接时会被注销。 ■ 从不。永不注销用户。 ■ 之后。用户断开连接的时间超过此设置后即注销。键入持续时间（以分钟为单位）。 <p>注销时间适用于以后断开的连接。如果在设置注销时间时桌面会话已经断开，则该用户的注销持续时间以设置注销时间的时刻为起点，而不是会话最初断开的时刻。例如，如果您将此值设置为 5 分钟，而会话在 10 分钟前断开，Horizon 7 将会在您设置完该值的 5 分钟后注销本次会话。</p>	

选项	说明	在此填写您要指定的值
允许用户重置/重新启动计算机	<p>指定用户是否可以重置虚拟机或重新启动虚拟桌面。</p> <p>重置操作会重置虚拟机而不正常重新启动操作系统。此操作仅适用于包含 vCenter Server 虚拟机的自动池或手动池。</p> <p>重新启动操作会重新启动虚拟机，并正常重新启动操作系统。此操作仅适用于包含 vCenter Server 虚拟机的自动池或手动池。</p>	
注销后刷新操作系统磁盘	<p>选择是否刷新操作系统磁盘，以及何时刷新。</p> <ul style="list-style-type: none"> ■ 始终。用户每次注销时均刷新操作系统磁盘。 ■ 间隔时间。操作系统磁盘在指定的时间间隔（以天为单位）定期刷新。输入天数。 <p>天数将从最后一次刷新开始计算，如未进行过刷新，则从最初置备开始计算。例如，如果指定的值为 3 天，且从上次刷新开始计算，已超过 3 天，那么桌面将在用户注销后刷新。</p> ■ 特定量。当操作系统磁盘当前的容量达到其允许的最大容量的指定百分比时，刷新该操作系统磁盘。即时克隆操作系统磁盘的最大容量为副本操作系统磁盘的容量。输入执行刷新操作的百分比。 ■ 从不。从不刷新操作系统磁盘。 	
回收虚拟机磁盘空间	<p>确定是否允许 ESXi 主机回收以节省空间的磁盘格式创建的即时克隆上的未使用磁盘空间。空间回收功能可减少即时克隆桌面所需的总存储空间。</p>	
在虚拟机上的未使用空间超出以下值时启动回收：	<p>键入要触发空间回收而必须在即时克隆操作系统磁盘上累积的未使用磁盘空间的最小数量（以千兆字节为单位）。当未使用的磁盘空间超过此阈值时，Horizon 7 将启动操作，指示 ESXi 主机回收操作系统磁盘上的空间。</p> <p>此值根据虚拟机而测得。未使用的磁盘空间必须超过单个虚拟机上指定的阈值，然后 Horizon 7 才会开始对该计算机执行空间回收过程。</p> <p>默认值为 1 GB。</p>	
允许用户从不同的客户端设备启动单独的会话	<p>选择该选项时，从不同的客户端设备连接到同一桌面池的用户将获取不同的桌面会话。用户只能从相同的客户端设备重新连接到现有会话。如果未选择该设置，则无论使用哪个客户端设备，用户都将始终重新连接到他们的现有会话。</p>	
默认显示协议	<p>选择默认显示协议。选项包括 Microsoft RDP、PCoIP 和 VMware Blast。</p>	
允许用户选择协议	<p>指定用户能否选择除默认显示协议之外的其他显示协议。</p> <p>不允许用户选择显示协议。</p>	

选项	说明	在此填写您要指定的值
3D 呈现器	<p>为桌面选择 3D 图形呈现。</p> <p>在虚拟硬件版本为 8 或更高版本的虚拟机上运行的 Windows 7 或更高版本的客户机上支持 3D 呈现。在 vSphere 5.1 环境中的虚拟硬件版本 9（最低）上支持基于硬件的呈现器。在 vSphere 5.0 环境中的虚拟硬件版本 8（最低）上支持软件呈现器。</p> <p>在 ESXi 5.0 主机上，呈现器允许使用的最大 VRAM 大小为 128MB。在 ESXi 5.1 和更高版本的主机上，最大 VRAM 大小为 512MB。在 vSphere 6.0 中的硬件版本 11 (HWv11) 虚拟机上，已更改 VRAM 值（显存）。选择“使用 vSphere Client 管理”选项并在 vSphere Web Client 中为这些计算机配置显存。有关详细信息，请参阅《vSphere 虚拟机管理》指南中的“配置 3D 图形”。</p> <p>如果选择 Microsoft RDP 以作为默认显示协议，并且不允许用户选择显示协议，则会禁用 3D 呈现。</p> <ul style="list-style-type: none"> ■ NVIDIA GRID vGPU。 已为 NVIDIA GRID vGPU 启用 3D 呈现。虚拟机开启时，ESXi 主机按照先到先得的原则预留 GPU 硬件资源。在选择该选项时，您无法使用 vSphere Distributed Resource Scheduler (DRS)。 <p>您可以为即时克隆桌面池选择 PCoIP 或 VMware Blast 来作为使用 NVIDIA GRID vGPU 的显示协议。</p> <ul style="list-style-type: none"> ■ 使用 vSphere Client 管理。 在 vSphere Web Client（或 vSphere 5.1 或更高版本中的 vSphere Client）中为虚拟机设置的“3D 呈现器”选项决定了 3D 图形呈现的类型。Horizon 7 不会控制 3D 呈现。在 vSphere Web Client 中，可配置自动、软件或硬件选项。这些选项与在 Horizon Console 中设置它们时的效果相同。在配置 vDGA 和采用 vDGA 的 AMD 多用户 GPU 时使用此设置。此设置也是 vSGA 的一个选项。选择使用 vSphere Client 管理选项时，为 3D 客户机配置虚拟 RAM、显示器最大数量和任意一台显示器的最大分辨率设置在 Horizon Console 中无效。可以在 vSphere Web Client 中配置内存量。 ■ 已禁用。 3D 呈现无效。默认值为“已禁用”。 	
HTML Access	<p>选择已启用以允许用户从 Web 浏览器连接到远程桌面。有关此功能的更多信息，请参阅《VMware Horizon HTML Access 安装和设置指南》。</p> <p>要将 HTML Access 与 VMware Identity Manager 配合使用，必须将连接服务器与 SAML 身份验证服务器进行配对，如《Horizon 7 管理指南》文档中所述。必须安装并配置 VMware Identity Manager，才能与连接服务器一起使用。</p>	
允许会话协作	选择 已启用 ，以允许桌面池用户邀请其他用户加入其远程桌面会话。会话所有者和会话协作者必须使用 VMware Blast 协议。	
出现错误时停止置备	指定在出现错误时 Horizon 7 是否停止置备桌面虚拟机，以及是否阻止错误影响多个虚拟机。	
命名模式	指定 Horizon 7 在所有桌面虚拟机名称中用作前缀的模式，其后跟有一个唯一编号。	
计算机的最大数量	指定池中桌面虚拟机的总数。	
备用 (已打开电源) 计算机数量	指定保持用户可用的桌面虚拟机数量。	

选项	说明	在此填写您要指定的值
按需置备计算机 计算机的最小数量 预先置备所有计算机	<p>指定在创建池时置备所有桌面虚拟机，还是根据需要置备虚拟机。</p> <ul style="list-style-type: none"> ■ 预先置备所有计算机。创建池时，Horizon 7 会根据您在计算机的最大数量中指定的值，创建相应数量的虚拟机。 ■ 按需置备计算机。创建池时，Horizon 7 会根据计算机的最小数量值或备用 (已打开电源) 计算机数量值（以较大者为准），创建相应数量的虚拟机。系统会额外创建一些虚拟机，以便在用户连接到桌面时保持有此最小数量的可用虚拟机。 	
为副本磁盘和操作系统磁盘选择单独的数据存储	<p>指定是否在不同于即时克隆所在的数据存储上存储副本磁盘和操作系统磁盘。</p> <p>如果选择此选项，您可以通过选择相应的选项来选择一个或多个即时克隆数据存储或副本磁盘数据存储。</p>	
vCenter 中的父虚拟机	为池选择 vCenter Server 中的父虚拟机。	
快照 (默认映像)	<p>您可以为即时克隆桌面池指定显示器数量和分辨率，方法是在父虚拟机中设置这些参数并拍摄快照。所需的虚拟 RAM 大小会根据您的规格计算出来。选择要用作池的主映像的父虚拟机快照。创建的即时克隆桌面池将基于该快照，并继承这些内存设置。有关在 vSphere Client 中配置显存设置的更多信息，请参阅 vSphere 文档中的《vSphere 单台主机管理》指南。有关更改即时克隆桌面池分辨率的更多信息，请参阅 VMware 知识库 (Knowledge Base, KB) 文章 http://kb.vmware.com/kb/2151745。</p> <p>快照列出了以下详细信息：</p> <ul style="list-style-type: none"> ■ 显示器数量 ■ 虚拟 RAM 大小 ■ 分辨率 	
虚拟机文件夹位置	为桌面虚拟机选择 vCenter Server 中的文件夹。	
群集	为桌面虚拟机选择 vCenter Server 群集。	
资源池	为桌面虚拟机选择 vCenter Server 资源池。	
数据存储	<p>为桌面虚拟机选择一个或多个数据存储。</p> <p>选择即时克隆数据存储窗口提供了估算池的存储要求的高级指导原则。这些指导原则可帮助您确定哪些数据存储有足够大的空间来存储克隆。“存储过载”值始终设置为“无限制”，且无法进行配置。</p> <p>注 即时克隆与 Storage vMotion 兼容。在 Storage DRS 数据存储上创建即时克隆桌面池时，Storage DRS 群集不会显示在数据存储列表中。但是，您可以选择单个 Storage DRS 数据存储。</p>	
副本磁盘数据存储	<p>选择一个或多个要在其中存储即时克隆的副本磁盘数据存储。如果您为副本磁盘和操作系统磁盘选择不同的数据存储，则会显示此选项。</p> <p>“添加场”向导的选择副本磁盘数据存储页面上的表格简要说明了估算场的存储要求的准则。这些准则可帮助您确定哪些副本磁盘数据存储有足够大的空间来存储即时克隆。</p>	
网络	<p>选择用于即时克隆桌面池的网络。您可以选择多个 vLAN 网络来创建较大的即时克隆桌面池。默认设置将使用当前主映像中的网络。</p> <p>选择网络向导中的表格提供了可使用的网络、端口和端口绑定。要使用多个网络，必须取消选择使用当前父虚拟机中的网络，然后选择要用于即时克隆的网络。</p>	

选项	说明	在此填写您要指定的值
vGPU 配置文件	<p>池的 vGPU 配置文件是您选择的快照的 vGPU 配置文件。池将继承此配置文件。在池创建过程中无法编辑此配置文件。</p> <p>在置备池后，可以发布要更改 vGPU 配置文件的映像。</p> <p>支持在单个 vSphere 群集（包含任意数量的 ESXi 主机）上混用 vGPU 配置文件。</p> <p>对于 vCenter Server 版本 6.0，仅支持含有性能模式的单个 vGPU 配置文件。</p> <p>对于 vCenter Server 版本 6.5 及更高版本，使用多个 vGPU 配置文件时请遵循以下准则：</p> <ul style="list-style-type: none"> ■ 您可以将多个 vGPU 配置文件以及 GPU 整合 分配策略用于群集内的所有 GPU 主机。 ■ 支持包含已启用 GPU 和未启用 GPU 的主机的混合群集。 ■ 不建议使用其中部分主机使用 GPU 整合 分配策略，部分主机使用 GPU 性能 分配策略的混合群集。 <p>为了从用于所有 vGPU 桌面的单个配置文件获得最佳性能，您需要将群集内所有 GPU 主机的 GPU 分配策略设置为最佳性能。</p>	
域	选择一个 Active Directory 域。下拉列表显示了您在配置即时克隆域管理员时指定的域。	
AD 容器	<p>指定 Active Directory 容器的相对标识名。</p> <p>例如：CN=Computers</p> <p>在添加桌面池窗口中，您可以浏览容器的 Active Directory 树。您还可以复制、粘贴或输入容器 AD 树的路径。</p>	
允许重新使用已存在的计算机帐户	<p>选择此选项可在新即时克隆的虚拟机名称与 Active Directory 中的现有计算机帐户名称匹配时，使用现有计算机帐户。</p> <p>创建即时克隆时，如果现有 AD 计算机帐户名称与即时克隆虚拟机名称匹配，Horizon 7 会在重置密码后使用现有计算机帐户。否则，需创建新的计算机帐户。</p> <p>删除即时克隆时，Horizon 7 不会删除对应的计算机帐户。</p> <p>现有计算机帐户必须位于您通过 AD 容器设置指定的 Active Directory 容器中。</p> <p>如果禁用此选项，则在 Horizon 7 创建即时克隆时，将创建一个新的 AD 计算机帐户。如果找到现有计算机帐户，Horizon 7 会在重置密码后使用现有计算机帐户。</p> <p>删除即时克隆时，Horizon 7 也会删除对应的计算机帐户。默认情况下禁用此选项。</p>	
关机脚本	指定在桌面虚拟机关闭前要在这些虚拟机上运行的脚本的路径名称以及脚本参数。	
同步后脚本	指定在创建桌面虚拟机后要在这些虚拟机上运行的脚本的路径名称以及脚本参数。	

创建即时克隆桌面池

即时克隆桌面池是一个自动桌面池。vCenter Server 会根据您在创建池时指定的设置创建桌面虚拟机。

前提条件

- 确认即时克隆虚拟机连接的虚拟交换机具有足够的端口来支持预期的虚拟机数量。虚拟机上的每个网卡需要一个端口。

- 确认您已准备好主映像。有关更多信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“创建和准备虚拟机”。
- 收集池的配置信息。请参阅[用于在 Horizon Console 中创建即时克隆桌面池的工作表](#)。
- 确认已在 Horizon Administrator 中添加即时克隆域管理员。请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“添加即时克隆域管理员”。

步骤

- 1 在 Horizon Console 中，选择**清单 > 桌面**。
- 2 单击**添加**。
- 3 选择**自动桌面池**，并单击**下一步**。
- 4 选择**即时克隆**，选择 vCenter Server 实例，然后单击**下一步**。
- 5 按照提示创建池。

使用您在工作表中收集的配置信息。您可以通过在导航窗格中单击页面名称，直接返回至任意向导页面。

后续步骤

授予用户访问池的权限。请参阅[在 Horizon Console 中为桌面池或应用程序池添加授权](#)。

在 Horizon Console 中更改即时克隆桌面池的映像

您可以更改即时克隆桌面池的映像，以推送更改或恢复到之前的映像。您可以从任何虚拟机中选择任何快照作为新映像。

置备池后，您无法通过编辑池或更改池的映像来编辑 vGPU 配置文件。在将新映像推送到即时克隆池时，您必须确认新映像具有的 vGPU 配置文件与之前的映像相同，否则，推送映像操作可能会失败。要更改即时克隆池的 vGPU 配置文件，您必须删除该池，然后使用所需的 vGPU 配置文件创建新的池。

步骤

- 1 在 Horizon Console 中，选择**清单 > 桌面**
- 2 单击池 ID。
- 3 在**摘要**选项卡上，单击**维护 > 调度**。

此时会打开**调度推送映像**窗口。

- 4 按照提示操作。

您可以安排任务立即开始或在以后的某个时间开始。对于具有用户会话的克隆，您可以指定强制用户注销还是等待。用户注销后，Horizon 7 会重新创建克隆。

- 5 单击**完成**。

在启动此操作后，将会立即开始发布新映像。克隆的重新创建将会于您在**调度推送映像**向导中指定的时间开始。

在 Horizon Console 中监控推送映像操作

您可以监控对即时克隆桌面池执行的推送映像操作的进度。

步骤

1 在 Horizon Console 中，选择**清单 > 桌面**。

2 单击池 ID。

摘要选项卡显示了当前映像和待处理映像的信息。

3 单击**任务**选项卡。

此时会显示与推送映像操作关联的任务列表。

在 Horizon Console 中重新计划或取消推送映像操作

您可以对即时克隆桌面池重新计划或取消推送映像操作。

步骤

1 在 Horizon Console 中，选择**清单 > 桌面**。

2 单击池 ID。

摘要选项卡显示了当前映像和待处理映像的信息。

3 选择**维护 > 重新计划**或**维护 > 取消**。

4 按照提示操作。

如果您在正创建克隆时取消推送映像操作，则具有新映像的克隆会保留在池中，并且该池包含混合的克隆，其中某些克隆具有新映像，其他一些则具有旧映像。要确保所有克隆具有相同的映像，您可以移除所有克隆。Horizon 7 会重新创建具有相同映像的克隆。

创建包含完整虚拟机的自动桌面池

利用包含完整虚拟机的自动桌面池，可以创建虚拟机模板，Horizon 7 使用该模板为每个桌面创建虚拟机。还可以选择性创建自定义规范，以加快自动池的部署。

为创建自动桌面池，Horizon 7 会根据您应用于该池的设置动态置备计算机。Horizon 7 使用虚拟机模板作为池的基础。通过模板，Horizon 7 在 vCenter Server 中为每个桌面创建新虚拟机。

有关创建和维护包含完整虚拟机的自动桌面池所需配置的更多信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档。

用于在 Horizon Console 中创建包含完整虚拟机的自动池的工作表

在创建自动桌面池时，您可以配置某些选项。您可以使用此工作表在创建池之前准备配置选项。

表 10-2. 工作表：用于创建包含完整虚拟机的自动池的配置选项

选项	说明	在此填写您要指定的值
用户分配	<p>选择用户分配类型：</p> <ul style="list-style-type: none"> ■ 在专用分配池中，每个用户会分配给一台计算机。用户每次登录到该池时都会收到相同的计算机。 ■ 在浮动分配池中，用户每次登录时都会接收到不同的计算机。 	
启用自动分配	<p>在专用分配池中，计算机在用户首次登录池时分配给该用户。还可以将计算机明确分配给用户。</p> <p>如果不启用自动分配，必须明确为每个用户分配计算机。</p> <p>即使在启用自动分配时，您也可以手动分配计算机。</p>	
vCenter Server	选择用于管理池中虚拟机的 vCenter Server。	
桌面池 ID	<p>用于在 Horizon Administrator 中标识池的唯一名称。</p> <p>如果您的环境中运行了多个 vCenter Server，应确保其他 vCenter Server 没有使用同一个池 ID。</p> <p>连接服务器配置可以是独立的连接服务器实例，也可以是共享通用 View LDAP 配置的副本实例的容器。</p>	
显示名称	用户从客户端设备登录时所看到的池名称。如果不指定显示名称，系统将向用户显示池 ID。	
访问组	<p>选择用来存放池的访问组，或者将池留在默认的根访问组中。</p> <p>如果使用访问组，则可以将池的管理委托给某个具有特定角色的管理员。</p> <p>注 访问组不同于用来存储桌面虚拟机的 vCenter Server 文件夹。稍后，您需要在向导中选择存储其他 vCenter Server 设置的 vCenter Server 文件夹。</p>	
注销后删除虚拟机	<p>如果您选择浮动用户分配，需要选择是否在用户注销后删除计算机。</p> <p>注 可以在“桌面池设置”页面设置该选项。</p>	
桌面池设置	这些设置用于确定桌面状态、虚拟机处于未使用状态时的电源状态，例如显示协议，等等。	
出现错误时停止置备	您可以指示 Horizon 7 在置备虚拟机期间出现错误后停止置备或继续置备桌面池中的虚拟机。如果选择该设置，可以防止置备错误在多个虚拟机上重现。	
虚拟机命名	选择置备计算机的方式是手动指定计算机名称列表，还是提供命名模式和计算机总数。	
手动指定名称	如果手动指定名称，请准备计算机名称列表，以及关联的用户名（可选）。	

选项	说明	在此填写您要指定的值
命名模式	如果要采用这种命名方式，则需要提供命名模式。 指定的模式用作所有计算机名称的前缀，后接一个唯一的编号，以标识每个计算机。	
计算机的最大数量	如果您使用命名模式，需要指定池中的计算机总数。 您还可以指定在首次创建池时要置备的最小计算机数。	
备用 (已打开电源) 计算机数量	如果手动指定名称或者使用命名模式，需要指定可供新用户使用并且已打开电源的计算机的数量。 手动指定名称时，该选项称为 保持打开电源状态的未分配计算机的数量 。	
计算机的最小数量	如果您使用命名模式并根据需要置备计算机，则需要指定池中的最小计算机总数。 创建池时会创建最小数量的计算机。 如果您按需置备计算机，则在用户首次连接到池或在您将计算机分配给用户时创建其他计算机。	
使用 VMware vSAN	指定是否使用 VMware vSAN（如果可用）。vSAN 是一个软件定义的存储层，可以虚拟化在 ESXi 主机的群集上可用的本地物理存储磁盘。	
模板	选择要用于创建池的虚拟机模板。	
vCenter Server 文件夹	选择要在其中驻留桌面池的 vCenter Server 文件夹。	
主机或群集	选择要在其中运行虚拟机的 ESXi 主机或群集。 在 vSphere 5.1 或更高版本中，您可以选择最多包含 32 台 ESXi 主机的群集。	
资源池	选择要在其中驻留桌面池的 vCenter Server 资源池。	
数据存储	选择数据存储的类型： <ul style="list-style-type: none"> ■ 单个数据存储。选择要在其中存储桌面池的单个数据存储。 ■ Storage DRS。选择包含共享或本地数据存储的 Storage Distributed Resource Scheduler (DRS) 群集。Storage DRS 是一个负载均衡实用程序，可将存储工作负载分配并移动到可用的数据存储。 <p>如果您的桌面池是从 Horizon 7 版本 7.1 升级到 Horizon 7 版本 7.2 的，并且您希望修改该池以使用 Storage DRS 群集，则必须取消选择现有数据存储并改为选择 Storage DRS。</p> <p>注 如果使用 vSAN，只能选择一个数据存储。</p>	

选项	说明	在此填写您要指定的值
使用 View Storage Accelerator	<p>确定 ESXi 主机是否缓存常用虚拟机磁盘数据。View Storage Accelerator 可以提高性能并减少用于管理引导风暴和防病毒扫描 I/O 风暴的额外存储 I/O 带宽需求。</p> <p>vSphere 5.0 及更高版本支持此功能。</p> <p>该功能在默认情况下为启用状态。</p> <p>注 如果添加或删除中断时间，然后禁用 View Storage Accelerator，Horizon Console 将不保存中断时间。</p>	
透明页面共享范围	<p>选择允许透明页面共享 (TPS) 的级别。选项包括：虚拟机（默认）、池、容器或全局。如果在池、容器或全局级别为所有计算机打开 TPS，ESXi 主机将消除因这些计算机使用同一客户机操作系统或应用程序而产生的内存冗余副本。</p> <p>页面共享发生在 ESXi 主机上。例如，如果在池级别启用 TPS，但池分散到多个 ESXi 主机，则只有同一主机和同一池中的虚拟机将共享页面。在全局级别，同一 ESXi 主机上所有受 Horizon 7 管理的计算机都可以共享内存页，而不管这些计算机驻留在哪个池中。</p> <p>注 默认设置是不在计算机之间共享内存页，因为 TPS 可能会带来安全风险。调查表明可能会在非常有限的配置场景下滥用 TPS 来获取对数据的未授权访问。</p>	
客户机自定义	<p>从列表中选择一种自定义规范 (SYSPREP)，以配置许可、域附属、DHCP 设置以及计算机上的其他属性。您只能选择与模板的客户机操作系统匹配的自定义规范。</p> <p>或者，您也可以在创建计算机后手动自定义计算机。</p>	

创建包含完整虚拟机的自动池

您可以根据所选择的虚拟机模板来创建自动桌面池。Horizon 7 会动态地部署桌面，在 vCenter Server 中为每个桌面创建一个新虚拟机。

前提条件

- 为 Horizon 7 准备创建计算机时要使用的虚拟机模板。必须在模板上安装 Horizon 7。请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“创建和准备虚拟机”。
- 如果您希望使用自定义规范，请确保规范的准确性。在 vSphere Client 中，使用自定义规范按照您的模板部署和自定义虚拟机。全面测试生成的虚拟机，包括 DHCP 和身份验证。
- 确认用于虚拟机（用作远程桌面）的 ESXi 虚拟交换机上的端口数量充足。如果要创建大型桌面池，默认值可能不足以满足要求。ESXi 主机上的虚拟交换机端口的数量必须大于或等于虚拟机数量与每个虚拟机的虚拟网卡数量的乘积。
- 收集您在创建池时必须提供的配置信息。请参阅[用于在 Horizon Console 中创建包含完整虚拟机的自动池的工作表](#)。

- 确定如何配置电源设置、显示协议、Adobe Flash 质量及其他设置。请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“适用于所有桌面池类型的桌面和池设置”。
- 如果您想要通过 VMware Identity Manager 提供对桌面和应用程序的访问，请确认您在 Horizon Administrator 中以拥有根访问组的管理员角色的用户身份来创建桌面和应用程序池。如果您向用户提供根访问组以外的其他访问组的管理员角色，VMware Identity Manager 将不会识别您在 Horizon 7 中配置的 SAML 身份验证器，并且您也将无法在 VMware Identity Manager 中配置池。

步骤

- 1 在 Horizon Console 中，选择**清单 > 桌面**。
- 2 单击**添加**。
- 3 选择**自动桌面池**，并单击**下一步**。
- 4 选择**完整虚拟机**，选择 vCenter Server 实例，然后单击**下一步**。
- 5 按照提示创建池。

使用您在工作表中收集的配置信息。您可以通过在导航窗格中单击页面名称，直接返回至任意向导页面。

后续步骤

授予用户访问池的权限。

通过 Horizon Console 在完整克隆桌面池中重建虚拟机

如果要将虚拟机替换为新虚拟机并且要重用虚拟机名称，可以在完整克隆桌面池中重建虚拟机。可以重建处于错误状态的虚拟机，以使用同名但无错误的虚拟机替换该虚拟机。重建虚拟机时，将会删除虚拟机，然后使用相同的虚拟机名称对其进行克隆，并且会重用 AD 计算机帐户。之前虚拟机中的所有用户数据或设置都将丢失，新虚拟机将使用桌面池模板进行创建。

前提条件

- 创建自动完整克隆桌面池。请参阅[创建包含完整虚拟机的自动池](#)。

步骤

- 1 在 Horizon Console 中，选择**清单 > 桌面**。
- 2 选择要重建的虚拟机所在的桌面池，然后单击**清单**选项卡。
- 3 选择要重建的虚拟机，然后单击**重建**。

您可以在 vCenter Client 中查看虚拟机被删除，然后使用相同的名称被再次克隆的过程。在 Horizon Console 中，重建的虚拟机会经过以下状态：**正在删除 > 正在置备 > 正在自定义 > 可用**。

在 Horizon Console 中创建链接克隆桌面池

对于链接克隆桌面池，Horizon 7 会基于您选择的父虚拟机创建桌面池。Horizon Composer 服务可在 vCenter Server 中为每个桌面动态创建链接克隆虚拟机。

Horizon 7 会根据您应用于池的设置动态地置备链接克隆桌面池。由于链接克隆桌面会共享一个基础系统磁盘映像，因此它们使用的存储空间比完整虚拟机要少。

用于在 Horizon Console 中创建链接克隆桌面池的工作表

在创建链接克隆桌面池时，您可以配置某些选项。可以使用此工作表在创建链接克隆桌面池之前准备配置选项。

在创建链接克隆池之前，您必须使用 vCenter Server 为准备用作池的父虚拟机拍摄快照。为父虚拟机拍摄快照之前必须将其关闭。Horizon Composer 将使用该快照作为基础映像来创建克隆。

注 您不能从虚拟机模板来创建链接克隆池。

表 10-3. 工作表：用于创建链接克隆桌面池的配置选项

选项	说明	在此填写您要指定的值
vCenter Server	选择用于管理池中虚拟机的 vCenter Server。	
用户分配	选择用户分配类型： <ul style="list-style-type: none"> ■ 在专用分配池中，每个用户会分配给一台计算机。用户每次登录时接收到的都是同一台计算机。 ■ 在浮动分配池中，用户每次登录时都会接收到不同的计算机。 	
启用自动分配	在专用分配池中，计算机在用户首次登录池时分配给该用户。还可以将计算机明确分配给用户。 如果不启用自动分配，必须明确为每个用户分配计算机。	

选项	说明	在此填写您要指定的值
永久磁盘	<p>如果您选择专用用户分配，需要选择将 Windows 用户配置文件数据存储在单独的 Horizon Composer 永久磁盘上，还是与操作系统数据存储在单一磁盘上。</p> <ul style="list-style-type: none"> ■ 将 Windows 配置文件重定向到永久磁盘。选择此选项可将数据存储在单独的 Horizon Composer 永久磁盘上。您可以使用单独的永久磁盘保留用户数据和设置。Horizon Composer 刷新、重构和重新平衡操作不会影响永久磁盘。您可以将永久磁盘从链接克隆分离，并通过分离的磁盘重新创建链接克隆虚拟机。例如，删除计算机或池时，您可以分离永久磁盘并重新创建桌面，从而保留原始用户数据和设置。 ■ 磁盘大小。如果将用户配置文件数据存储在单独的 Horizon Composer 永久磁盘上，需提供磁盘大小（以兆字节为单位）。 ■ 驱动器盘符。如果将用户配置文件数据存储在单独的 Horizon Composer 永久磁盘上，需提供驱动器盘符。 <p>注 不要选择父虚拟机上已经存在的驱动器盘符，或者与网络上装载的驱动器所用的驱动器盘符冲突的驱动器盘符。</p> <ul style="list-style-type: none"> ■ 不重定向 Windows 配置文件。如果将 Windows 配置文件存储在操作系统磁盘中，请选择此选项。用户数据和设置在刷新、重构和重新平衡操作期间将被移除。 	
一次性文件重定向	<p>选择是否将客户机操作系统的页面文件和临时文件重定向到单独的非永久磁盘。</p> <ul style="list-style-type: none"> ■ 将一次性文件重定向到非永久磁盘。选择此选项可将客户机操作系统的页面文件和临时文件重定向到单独的非永久磁盘。使用该配置时，当链接克隆关闭电源后，一次性文件磁盘被替换为使用链接克隆池创建的原始磁盘的副本。链接克隆的大小在用户与其桌面交互过程中会增长。一次性文件重定向可以减缓链接克隆的增长速度，从而节省存储空间。 ■ 磁盘大小。如果将一次性文件重定向到非永久磁盘，需提供磁盘大小（以兆字节为单位）。 <p>磁盘大小应大于客户机操作系统的页面文件大小。要确定页面文件大小，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“记录父虚拟机的页面文件大小”。配置一次性文件磁盘大小时，需注意格式化磁盘分区的实际大小比您在 Horizon Console 中提供的值略小。</p> <ul style="list-style-type: none"> ■ 驱动器盘符。如果将一次性文件重定向到非永久磁盘，需提供驱动器盘符。您可以为一次性文件磁盘选择一个驱动器盘符。默认值为自动，可引导 Horizon 7 分配驱动器盘符。 ■ 不重定向一次性文件。如果不希望重定向客户机操作系统的页面文件和临时文件，请选择此选项。 <p>注 不要选择父虚拟机上已经存在的驱动器盘符，或者与网络上装载的驱动器所用的驱动器盘符冲突的驱动器盘符。</p>	

选项	说明	在此填写您要指定的值
使用 VMware vSAN	指定是否使用 VMware vSAN（如果可用）。vSAN 是一个软件定义的存储层，可以虚拟化在 ESXi 主机的群集上可用的本地物理存储磁盘。有关更多信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“使用 vSAN 实现高性能存储和基于策略的管理”。	
为永久磁盘和操作系统磁盘选择单独的数据存储	（仅在不使用 vSAN 时有效）如果将用户配置文件重定向到单独的永久磁盘，则可以将永久磁盘和操作系统磁盘存储在不同的数据存储中。	
为副本磁盘和操作系统磁盘选择单独的数据存储	<p>（仅在不使用 vSAN 或虚拟卷时有效）可以将副本（主）虚拟机磁盘存储在高性能数据存储中，而将链接克隆存储在单独的数据存储中。</p> <p>有关详细信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档。</p> <p>如果您将副本磁盘和操作系统磁盘存储在单独的数据存储中，则本地 NFS 快照无法使用。NAS 设备上的本地克隆仅在副本磁盘和操作系统磁盘存储在相同的数据存储中时发生。</p>	
桌面池 ID	<p>标识池的唯一名称。</p> <p>如果您的环境中正在运行多个连接服务器配置，应确保其他连接服务器配置未使用同一个池 ID。</p> <p>连接服务器配置可以是独立的连接服务器实例，也可以是共享通用 View LDAP 配置的副本实例的容器。</p>	
显示名称	用户从客户端设备登录时所看到的池名称。如果不指定显示名称，系统将向用户显示池 ID。	
访问组	<p>选择用来存放池的访问组，或者将池留在默认的根访问组中。</p> <p>如果使用访问组，则可以将池的管理委托给某个具有特定角色的管理员。有关详细信息，请参阅《Horizon 7 管理指南》文档中基于角色的委托管理章节。</p> <p>注 访问组不同于存储用作桌面的虚拟机的 vCenter Server 文件夹。稍后，您需要在向导中选择存储其他 vCenter Server 设置的 vCenter Server 文件夹。</p>	
启用置备	选择此选项可在桌面池中置备虚拟机。	
出现错误时停止置备	您可以指示 Horizon 7 在置备虚拟机期间出现错误后停止置备或继续置备桌面池中的虚拟机。如果选择该设置，可以防止置备错误在多个虚拟机上重现。	
虚拟机命名	<p>选择置备计算机的方式是手动指定计算机名称列表，还是提供命名模式和计算机总数。</p> <p>有关详细信息，请参阅在 Horizon Console 中手动命名计算机或提供命名模式。</p>	
手动指定名称	如果手动指定名称，请准备计算机名称列表，以及关联的用户名（可选）。	

选项	说明	在此填写您要指定的值
命名模式	<p>如果要采用这种命名方式，则需要提供命名模式。</p> <p>指定的模式用作所有计算机名称的前缀，后接一个唯一的编号，以标识每个计算机。</p> <p>有关详细信息，请参阅为自动桌面池使用命名模式。</p>	
计算机的最大数量	<p>如果您使用命名模式，需要指定池中的计算机总数。</p> <p>您还可以指定在首次创建池时要置备的最小计算机数。</p>	
备用 (已打开电源) 计算机数量	<p>如果手动指定名称或者使用命名模式，需要指定可供新用户使用并且已打开电源的计算机的数量。有关详细信息，请参阅在 Horizon Console 中手动命名计算机或提供命名模式。</p> <p>手动指定名称时，该选项称为保持打开电源状态的未分配计算机的数量。</p>	
Horizon Composer 维护操作期间就绪 (已置备) 计算机的最小数量	<p>如果手动指定名称或使用命名模式，请指定在执行 Horizon Composer 维护操作时处于已置备状态以在远程桌面会话中使用的最小计算机数量。</p> <p>通过使用该设置，用户可以在 Horizon Composer 刷新、重构或重新平衡池中的计算机时保持现有的连接或发送新的连接请求。该设置不区别准备接受新连接的备用计算机和已在现有桌面会话中连接的计算机。</p> <p>该值必须小于计算机的最大数量，这是在按需置备计算机时指定的。</p> <p>有关更多信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档。</p>	
按需置备计算机 或 预先置备所有计算机	<p>如果使用命名模式，请选择是在创建池时置备所有计算机还是按需置备计算机。</p> <ul style="list-style-type: none"> ■ 预先置备所有计算机。创建池时，系统置备的计算机数量为您在计算机的最大数量中指定的数量。 ■ 按需置备计算机。创建池时，系统创建的计算机数量为您在计算机的最小数量中指定的数量。其他计算机在用户首次连接池或您为用户分配计算机时创建。 	
计算机的最小数量	<p>如果您使用命名模式，并根据需要置备桌面，则需要指定池中计算机的最小数量。</p> <p>系统会在您创建池时创建最小数量的计算机。即使其他设置（如注销时删除或刷新计算机）导致计算机被删除，也会保持这一数量。</p>	
父虚拟机	为池选择父虚拟机。	
快照 (默认映像)	<p>选择要用作池的基础映像的父虚拟机快照。</p> <p>不要删除 vCenter Server 中的快照和父虚拟机，除非池中的链接克隆均不使用此默认映像，且不会根据此默认映像创建链接克隆。系统需要使用父虚拟机和快照根据池策略在池中置备新的链接克隆。Horizon Composer 维护操作也需要父虚拟机和快照。</p>	
虚拟机文件夹位置	选择要在其中驻留桌面池的 vCenter Server 文件夹。	

选项	说明	在此填写您要指定的值
主机或群集	<p>选择要用来运行桌面虚拟机的 ESXi 主机或群集。</p> <p>使用 vSAN 数据存储 (vSphere 5.5 Update 1 的一项功能)，可以选择最多包含 20 个 ESXi 主机的群集。使用虚拟卷数据存储 (vSphere 6.0 的一项功能)，可以选择最多包含 32 个 ESXi 主机的群集。</p> <p>在 vSphere 5.1 或更高版本中，如果副本存储在 VMFS5 或更高版本的数据存储中或 NFS 数据存储中，您就可选择最多含有 32 个 ESXi 主机的群集。如果您将副本磁盘存储在 VMFS5 之前的版本中，群集最多可包含 8 台主机。</p> <p>在 vSphere 5.0 中，如果副本存储于 NFS 数据存储中，则可选择包含八台以上 ESXi 主机的群集。如果您在 VMFS 数据存储中存储副本，则一个群集最多包含八台主机。请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“在包含超过 8 个主机的群集上配置桌面池”。</p>	
资源池	选择要在其中驻留桌面池的 vCenter Server 资源池。	
链接克隆数据存储	<p>选择一个或多个要在其中存储桌面池的数据存储区。</p> <p>“添加池”向导中 选择链接克隆数据存储 页面上的表格简要说明了估算池的存储要求的准则。这些信息能帮助您确定哪个数据存储有足够空间存储链接克隆磁盘。有关详细信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“确定链接克隆桌面池的存储大小”。</p> <p>您可将共享数据存储或本地数据存储用于单个的 ESXi 主机或 ESXi 群集。如果您在 ESXi 群集中使用本地数据存储，则您必须考虑桌面部署的 vSphere 基础架构限制。请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“在本地数据存储上存储链接克隆”。</p> <p>使用 vSAN 数据存储 (vSphere 5.5 Update 1 的一项功能)，可以选择最多包含 20 个 ESXi 主机的群集。使用虚拟卷数据存储 (vSphere 6.0 的一项功能)，可以选择最多包含 32 个 ESXi 主机的群集。</p> <p>有关为链接克隆创建的磁盘的更多信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“链接克隆数据磁盘”。</p> <p>注 如果使用 vSAN，只能选择一个数据存储。</p>	
副本磁盘数据存储	<p>选择一个要在其中存储副本的副本磁盘数据存储。</p> <p>在 vSphere 5.1 或更高版本中，如果副本存储在 VMFS5 (或更高版本) 或 NFS 数据存储中，则群集可包含 8 台以上的 ESXi 主机。在 vSphere 5.0 中，副本只有存储在 NFS 数据存储中时，群集才能包含 8 台以上的 ESXi 主机。请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“在包含超过 8 个主机的群集上配置桌面池”。</p>	
注销时删除或刷新虚拟机	<p>如果选择浮动用户分配，需要选择在用户注销后刷新计算机、删除计算机还是不执行任何操作。</p> <p>注 可以在“桌面池设置”页面设置该选项。</p>	

选项	说明	在此填写您要指定的值
桌面池设置	<p>这些设置用于确定计算机状态、虚拟机处于未使用状态时的电源状态、显示协议、Adobe Flash 质量等。</p> <p>有关说明，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“适用于所有桌面池类型的桌面池设置”。</p> <p>有关适用于链接克隆池的设置列表，请参阅 Horizon Console 中适用于链接克隆桌面池的桌面池设置。</p> <p>有关电源策略和自动池的更多信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“为桌面池设置电源策略”。</p>	
使用 Horizon Storage Accelerator	<p>确定是否使用 Horizon Storage Accelerator，该功能可允许 ESXi 主机缓存常用虚拟机磁盘数据。Horizon Storage Accelerator 可以提高性能并减少用于管理引导风暴和防病毒扫描 I/O 风暴的额外存储 I/O 带宽需求。</p> <p>vSphere 5.0 及更高版本支持此功能。</p> <p>该功能在默认情况下为启用状态。</p> <p>有关详细信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档。</p>	
存储过载	<p>确定在每个数据存储上创建链接克隆时的存储过载级别。</p> <p>随着级别的增加，数据存储上装载的链接克隆会越来越多，而为单个克隆的增长所保留的空间则越来越少。如果设置较高的存储过载级别，您创建的链接克隆的总逻辑大小就可以大于数据存储的物理存储限制。有关详细信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“设置链接克隆虚拟机的存储过载级别”。</p> <p>注 如果使用 vSAN，则该设置无效。</p>	
使用本地 NFS 快照 (VAAI)	<p>（仅在不使用 vSAN 时有效）如果部署中包含支持 vStorage APIs for Array Integration (VAAI) 的 NAS 设备，则可以使用本地快照技术克隆虚拟机。</p> <p>仅当您选择了位于通过 VAAI 支持本地克隆操作的 NAS 设备上的数据存储时，才可以使用此功能。</p> <p>如果您将副本磁盘和操作系统磁盘存储在单独的数据存储中，则无法使用这些功能。无法在包含能节省空间的磁盘的虚拟机上使用此功能。</p> <p>vSphere 5.0 及更高版本支持此功能。</p> <p>有关详细信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档。</p>	
回收虚拟机磁盘空间	<p>（仅在不使用 vSAN 或虚拟卷时有效）确定是否允许 ESXi 主机回收以节省空间的磁盘格式创建的链接克隆上的未用磁盘空间。空间回收功能减少了链接克隆桌面所需的总存储空间。</p> <p>vSphere 5.1 及更高版本支持此功能。链接克隆虚拟机必须是虚拟硬件版本 9 或更高版本。</p> <p>有关详细信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“在链接克隆虚拟机上回收磁盘空间”。</p>	

选项	说明	在此填写您要指定的值
在虚拟机上的未使用空间超出以下值时启动回收：	<p>（仅在不使用 vSAN 或虚拟卷时有效）键入必须在链接克隆操作系统磁盘上累积从而触发空间回收的未用磁盘空间的最小数量（千兆字节）。当未使用的磁盘空间超过此阈值时，Horizon 7 将启动操作，指示 ESXi 主机回收操作系统磁盘上的空间。</p> <p>此值根据虚拟机而测得。未使用的磁盘空间必须超过单个虚拟机上指定的阈值，然后 Horizon 7 才会开始对该计算机执行空间回收过程。</p> <p>例如：2 GB。</p> <p>默认值为 1 GB。</p>	
中断时间	<p>配置中断天数和时间，在此期间不进行 Horizon Storage Accelerator 重新生成和虚拟机磁盘空间回收操作。</p> <p>为了确保必要时 ESXi 资源专供前台任务使用，您可以在指定日期的指定时段内禁止 ESXi 主机执行这些操作。</p> <p>有关详细信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“设置虚拟机上 ESXi 操作的中断时间”。</p>	
透明页面共享范围	<p>选择允许透明页面共享 (TPS) 的级别。选项包括：虚拟机（默认）、池、容器或全局。如果在池、容器或全局级别为所有计算机打开 TPS，ESXi 主机将消除因这些计算机使用同一客户机操作系统或应用程序而产生的内存页冗余副本。页面共享发生在 ESXi 主机上。例如，如果在池级别启用 TPS，但池分散到多个 ESXi 主机，则只有同一主机和同一池中的虚拟机将共享页面。在全局级别，同一 ESXi 主机上所有受 Horizon 7 管理的计算机都可以共享内存页，而不管这些计算机驻留在哪个池中。</p> <p>注 默认设置是不在计算机之间共享内存页，因为 TPS 可能会带来安全风险。调查表明可能会在非常有限的配置场景下滥用 TPS 来获取对数据的未授权访问。</p>	
域	<p>选择 Active Directory 域和用户名。</p> <p>Horizon Composer 要求使用特定用户特权来创建链接克隆池。QuickPrep 或 Sysprep 使用域和用户帐户来自定义链接克隆计算机。</p> <p>当您为 vCenter Server 配置 Horizon Composer 设置时，应指定此用户。配置 Horizon Composer 设置时，可以指定多个域和用户。使用添加桌面池向导创建池时，必须从列表中选择一个域和用户。</p>	
AD 容器	<p>提供 Active Directory 容器的相对标识名。</p> <p>例如：CN=Computers</p> <p>当您运行添加桌面池向导时，可以浏览 Active Directory 树以找到所需容器。</p>	

选项	说明	在此填写您要指定的值
允许重新使用已存在的计算机帐户	<p>选择此选项可将 Active Directory 中现有的计算机帐户用于 Horizon Composer 置备的链接克隆。此选项允许您控制在 Active Directory 中创建的计算机帐户。</p> <p>置备链接克隆后，如果现有 AD 计算机帐户名与链接克隆计算机名匹配，则 Horizon Composer 会使用现有的计算机帐户。否则，需创建新的计算机帐户。</p> <p>现有的计算机帐户必须位于您通过 Active Directory 容器 设置而指定的 Active Directory 容器中。</p> <p>如果禁用此选项，Horizon Composer 置备链接克隆时将创建新的 AD 计算机帐户。默认情况下禁用此选项。</p> <p>有关详细信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“针对链接克隆使用现有的 Active Directory 计算机帐户”。</p>	
Use QuickPrep or a customization specification (Sysprep) (使用 QuickPrep 或自定义规范 (Sysprep))	<p>选择使用 QuickPrep 还是选择自定义规范 (Sysprep) 来配置许可、域附属、DHCP 设置和其他计算机属性。</p> <p>仅 vSphere 4.1 或更高版本软件支持 Sysprep 用于链接克隆。</p> <p>使用 QuickPrep 或 Sysprep 创建池后，无法在以后创建或重构池中的计算机时转换为其他自定义方法。</p> <p>有关详细信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“选择 QuickPrep 或 Sysprep 来自定义链接克隆计算机”。</p>	
关机脚本	<p>QuickPrep 可以在链接克隆计算机的电源关闭之前在这些计算机上运行自定义脚本。</p> <p>提供父虚拟机上的脚本的路径以及脚本参数。</p>	
同步后脚本	<p>QuickPrep 可以在创建、重构和刷新克隆计算机后在这些计算机上运行自定义脚本。</p> <p>提供父虚拟机上的脚本的路径以及脚本参数。</p>	

Horizon Console 中适用于链接克隆桌面池的桌面池设置

配置包含由 **Horizon Composer** 创建的链接克隆的自动池时，您必须指定计算机和桌面池设置。适用于专用用户分配池和浮动用户分配池的设置有所不同。

下表列出了适用于专用分配链接克隆池和浮动分配链接克隆池的设置。

有关每个设置的说明，请参阅《在 **Horizon 7** 中设置虚拟桌面》文档中的“适用于所有桌面池类型的桌面池设置”。

表 10-4. 链接克隆桌面自动池的设置

设置	专用分配链接克隆池	浮动分配链接克隆池
状态	是	是
连接服务器限制	是	是
类别文件夹（*在 Horizon Administrator 中受支持）	是	是
远程计算机电源策略	是	是

设置	专用分配链接克隆池	浮动分配链接克隆池
断开连接后自动注销	是	是
允许用户重置/重新启动计算机	是	是
允许用户从不同的客户端设备启动单独的会话		是
注销时删除或刷新虚拟机		是
注销后刷新操作系统磁盘	是	
默认显示协议	是	是
允许用户选择协议	是	是
3D 呈现器	是	是
显示器最大数量	是	是
任意一台显示器的最大分辨率	是	是
Adobe Flash 质量	是	是
Adobe Flash 调节	是	是
覆盖全局 Mirage 设置	是	是
Mirage 服务器配置	是	是

在 Horizon Console 中创建链接克隆桌面池

您可以根据所选择的父虚拟机来创建自动链接克隆桌面池。Horizon Composer 服务可在 vCenter Server 中为每个桌面动态创建新的链接克隆虚拟机。

前提条件

- 确认在与 vCenter Server 相同的主机或其他主机上安装了 Horizon Composer 服务，并且配置了 Horizon Composer 数据库。请参阅《Horizon 7 安装指南》文档。
- 确认在 Horizon Administrator 中配置了适用于 vCenter Server 的 Horizon Composer 设置。请参阅《Horizon 7 管理指南》文档。
- 确认用于虚拟机（用作远程桌面）的 ESXi 虚拟交换机上的端口数量充足。如果要创建大型桌面池，默认值可能不足以满足要求。ESXi 主机上的虚拟交换机端口的数量必须大于或等于虚拟机数量与每个虚拟机的虚拟网卡数量的乘积。
- 确认已准备好父虚拟机。必须在该父虚拟机上安装 Horizon Agent。请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“创建并准备虚拟机以进行克隆”。
- 在 vCenter Server 中为父虚拟机拍摄一个快照。为父虚拟机拍摄快照之前必须将其关闭。Horizon Composer 将使用该快照作为基础映像来创建克隆。

注 您不能从虚拟机模板来创建链接克隆池。

- 收集您在创建池时必须提供的配置信息。请参阅[用于在 Horizon Console 中创建链接克隆桌面池的工作表](#)。

- 确定如何配置电源设置、显示协议、Adobe Flash 质量及其他设置。请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“适用于所有桌面池类型的桌面和池设置”。
- 如果您想要通过 VMware Identity Manager 提供对桌面和应用程序的访问权限，请确认您在 Horizon Console 中以对根访问组拥有管理员角色的用户身份创建这些桌面和应用程序池。如果您向用户提供根访问组以外的其他访问组的管理员角色，VMware Identity Manager 将不会识别您在 Horizon 7 中配置的 SAML 身份验证器，并且您也将无法在 VMware Identity Manager 中配置池。

重要事项 创建链接克隆池时，不要在 vCenter Server 中修改父虚拟机。例如，不要将父虚拟机转换为模板。Horizon Composer 服务要求父虚拟机在池创建过程中保持静止不变的状态。

步骤

- 1 在 Horizon Console 中，选择**清单 > 桌面**。
- 2 单击**添加**。
- 3 选择**自动桌面池**，并单击**下一步**。
- 4 选择 **View Composer 链接克隆**，选择 vCenter Server 实例，然后单击**下一步**。
- 5 按照提示创建池。

使用您在工作表中收集的配置信息。您可以通过在导航窗格中单击页面名称，直接返回至任意向导页面。

在 Horizon Console 中，您可以在将计算机添加到池时查看这些计算机，方法是选择**清单 > 桌面**。

链接克隆在置备期间可能会重新启动一次或多次。如果链接克隆处于错误状态，自动恢复机制将尝试打开链接克隆的电源，或者关闭并重新启动链接克隆。如果多次恢复尝试失败，则此链接克隆将被删除。

Horizon Composer 还会创建一个用作主映像的副本虚拟机，以供置备链接克隆。为减少占用的空间，该副本将被创建一个精简磁盘。如果重构或删除了所有虚拟机，且没有任何克隆链接到副本，则系统将把副本虚拟机从 vCenter Server 中删除。

如果您未将副本存储在单独的数据存储中，Horizon Composer 会在创建链接克隆的每个数据存储中创建一个副本。

如果您将副本存储在单独的数据存储中，则 View Composer 将为整个池创建一个副本，即使链接克隆是在多个数据存储上创建的。

后续步骤

授予用户访问池的权限。请参阅[在 Horizon Console 中为桌面池或应用程序池添加授权](#)。

在 Horizon Console 中创建手动桌面池

在手动桌面池中，最终用户访问的每个远程桌面都是一个单独的计算机。创建手动桌面池时，需要选择现有的计算机。您可以通过创建手动桌面池并选择一个计算机来创建包含单一桌面的池。

Horizon 7 可以在手动池中使用多种类型的计算机：

- vCenter Server 管理的虚拟机

- 在不同于 vCenter Server 的虚拟化平台上运行的虚拟机
- 物理机

有关创建使用 Linux 虚拟机的手动桌面池的信息，请参阅《《设置 Horizon 7 for Linux 桌面》》指南。

用于在 Horizon Console 中创建手动桌面池的工作表

在创建手动桌面池时，您可以配置某些选项。您可以使用此工作表在创建池之前准备配置选项。

注 在手动池中，您必须对每台计算机完成准备工作，才能实现远程桌面访问。必须在每台计算机上安装并运行 Horizon Agent。

表 10-5. 工作表：用于创建手动桌面池的配置选项

选项	说明	在此填写您要指定的值
用户分配	<p>选择用户分配类型：</p> <ul style="list-style-type: none"> ■ 在专用分配池中，每个用户会分配给一台计算机。用户每次登录时接收到的都是同一台计算机。 ■ 在浮动分配池中，用户每次登录时都会接收到不同的计算机。 <p>有关详细信息，请参阅 Horizon Console 中的桌面池用户分配。</p>	
vCenter Server	<p>用来管理计算机的 vCenter Server。</p> <p>仅当计算机是受 vCenter Server 管理的虚拟机时，才会显示此选项。</p>	
计算机源	<p>要包含在桌面池中的虚拟机或物理机。</p> <ol style="list-style-type: none"> 1 确定要使用的计算机类型。可以使用受 vCenter Server 管理的虚拟机，也可以使用未受管的虚拟机和物理机。 2 准备好要包含在桌面池中的 vCenter Server 虚拟机或未受管虚拟机和物理机的列表。 3 在要包含在桌面池中的每台计算机上安装 Horizon Agent。 <p>要在未受管的虚拟机或物理机上使用 PCoIP，必须使用 Teradici 硬件。</p> <p>注 在 Horizon Console 中启用 Windows Server 桌面时，Horizon Console 会显示所有可用的 Windows Server 计算机作为潜在计算机源，包括安装了连接服务器和其他 Horizon 7 Server 的计算机。</p> <p>如果计算机上已安装 Horizon 7 Server 软件，则无法为桌面池选择计算机。Horizon Agent 不能与任何其他 Horizon 7 软件组件（包括连接服务器、安全服务器、View Composer 或 Horizon Client）共存于同一台虚拟机或物理机上。</p>	
桌面池 ID	<p>用户登录时看到的池名称，用于在 Horizon Console 中标识池。</p> <p>如果您的环境中运行了多个 vCenter Server，应确保其他 vCenter Server 没有使用同一个池 ID。</p>	

选项	说明	在此填写您要指定的值
桌面池设置	<p>这些设置用于确定计算机状态、虚拟机处于未使用状态时的电源状态、显示协议、Adobe Flash 质量等。</p> <p>有关详细信息，请参阅 Horizon Console 中适用于所有桌面池类型的桌面池设置。</p> <p>有关适用于手动池的设置列表，请参阅 Horizon Console 中适用于手动池的桌面池设置。</p>	
透明页面共享范围	<p>选择允许透明页面共享 (TPS) 的级别。选项包括：虚拟机（默认）、池、容器或全局。如果在池、容器或全局级别为所有计算机打开 TPS，ESXi 主机将消除因这些计算机使用同一客户机操作系统或应用程序而产生的内存冗余副本。</p> <p>页面共享发生在 ESXi 主机上。例如，如果在池级别启用 TPS，但池分散到多个 ESXi 主机，则只有同一主机和同一池中的虚拟机将共享页面。在全局级别，同一 ESXi 主机上所有受 Horizon 7 管理的计算机都可以共享内存页，而不管这些计算机驻留在哪个池中。</p> <p>注 默认设置是不在计算机之间共享内存页，因为 TPS 可能会带来安全风险。调查表明可能会在非常有限的配置场景下滥用 TPS 来获取对数据的未授权访问。</p>	

在 Horizon Console 中创建手动桌面池

可以创建从现有虚拟机或物理计算机置备桌面的手动桌面池。必须选择要包含在桌面池中的计算机。

对于包含由 vCenter Server 管理的虚拟机的手动池，Horizon 7 会确保打开备用计算机的电源，以便用户能够与其建立连接。无论哪个电源策略有效，备用计算机都会打开电源。

前提条件

- 准备用于进行远程桌面访问的计算机。在手动池中，必须单独准备每台计算机。必须在每台计算机上安装并运行 Horizon Agent。

要准备由 vCenter Server 管理的虚拟机，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“创建和准备虚拟机”。

要准备未受管的虚拟机和物理机，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“准备未受管的计算机”。

- 收集您在创建池时必须提供的配置信息。请参阅[用于在 Horizon Console 中创建手动桌面池的工作表](#)。
- 确定如何配置电源设置、显示协议、Adobe Flash 质量及其他设置。请参阅 [Horizon Console 中适用于所有桌面池类型的桌面池设置](#)。

步骤

- 1 在 Horizon Console 中，选择**清单 > 桌面**。
- 2 单击**添加**。
- 3 选择**手动桌面池**。

- 4 选择由 vCenter Server 管理的虚拟机或不受 vCenter Server 管理的未受管虚拟机，然后单击下一步。

选项	说明
vCenter 虚拟机	由 vCenter Server 管理的虚拟机。选择虚拟机所在的 vCenter Server。
其他源	不受 vCenter Server 管理的物理机或虚拟机

- 5 选择用户分配类型。

选项	说明
专用	虚拟机分配给一个用户。只有该用户才可以登录此桌面。
浮动	虚拟机由具有池授权的所有用户共享。只要没有用户正在使用，任何得到授权的用户均可以登录此桌面。

- 6 按照向导中的提示创建池。

使用您在工作表中收集的配置信息。通过在导航面板中单击页面名称，您可以直接返回至已完成的任意向导页面。

在 Horizon Console 中，您可以在将计算机添加到池时查看这些计算机，方法是选择**清单 > 桌面**。

后续步骤

授予用户访问池的权限。请参阅[在 Horizon Console 中为桌面池或应用程序池添加授权](#)。

Horizon Console 中适用于手动池的桌面池设置

配置手动桌面池时，您必须指定计算机和池的设置。并非所有设置都适用于所有类型的手动池。

手动桌面池的设置列出了适用于配置了以下属性的手动桌面池的设置：

- 专用用户分配
- 浮动用户分配
- 受管的计算机（vCenter Server 虚拟机）
- 未受管的计算机

这些设置也适用于包含单个计算机的手动池。

有关每种桌面池设置的描述，请参阅[Horizon Console 中适用于所有桌面池类型的桌面池设置](#)。

表 10-6. 手动桌面池的设置

设置	受管的专用分配手动池	受管的浮动分配手动池	未受管的专用分配手动池	未受管的浮动分配手动池
状态	是	是	是	是
连接服务器限制	是	是	是	是
远程计算机电源策略	是	是		

设置	受管的专用分配手动池	受管的浮动分配手动池	未受管的专用分配手动池	未受管的浮动分配手动池
断开连接后自动注销	是	是	是	是
允许用户重置/重新启动计算机	是	是		
允许用户从不同的客户端设备启动单独的会话		是		是
默认显示协议	是	是	是 要在不受 vCenter Server 管理的虚拟机中使用 PCoIP，您必须在该虚拟机上安装 Teradici 硬件。	是 要在不受 vCenter Server 管理的虚拟机中使用 PCoIP，您必须在该虚拟机上安装 Teradici 硬件。
允许用户选择协议	是	是	是	是
3D 呈现器	是	是		
显示器最大数量	是	是		
任意一台显示器的最大分辨率	是	是		
Adobe Flash 质量	是	是	是	是
Adobe Flash 调节	是	是	是	是
覆盖全局 Mirage 设置	是	是	是	是
Mirage 服务器配置	是	是	是	是

配置桌面池

创建桌面池时，您需要选择配置选项，从而确定池的管理方式，以及用户与桌面的交互方式。

这些任务适用于在单用户计算机上部署的桌面池，不适用于 RDS 桌面池。

Horizon Console 中的桌面池用户分配

您可以在桌面池中为桌面选择浮动用户分配或专用用户分配。

通过专用分配，可以将每个桌面分配给特定用户。首次登录的用户会获得一个未分配给其他用户的桌面。之后在登录后，该用户将始终获得此桌面，并且任何其他用户都不能使用此桌面。在每次登录到注销期间，将会保留同一个桌面的计算机名称和 MAC 地址。用户对该桌面所做的任何其他更改均不会被保留。

通过浮动分配，用户会在每次登录时获得一个随机桌面。用户注销时，该桌面会返回到池。

对于浮动即时克隆，用户注销时桌面始终会被删除，并从当前映像重新进行创建。

使用浮动分配，您也许能够降低软件许可成本。

在 Horizon Console 中手动命名计算机或提供命名模式

对于完整虚拟机或 View Composer 链接克隆的自动桌面池，您可以为桌面计算机指定一系列名称或提供命名模式。对于即时克隆桌面池，您只能在置备池时指定命名模式。

如果通过指定列表来命名计算机，您可以使用公司的命名方案，并且可以将每个计算机名称与一个用户相关联。

如果您提供了命名模式，Horizon 7 可以根据用户的需要动态创建和分配计算机。

下表对两种命名方法进行了比较，显示了每种方法对桌面池创建和管理方式的影响。

表 10-7. 手动命名计算机或提供计算机命名模式

功能	使用计算机命名模式	手动命名计算机
计算机名称	<p>通过将一个数字附加到命名模式后面来生成计算机名称。</p> <p>有关详细信息，请参阅为自动桌面池使用命名模式。</p>	<p>您要指定一个计算机名称列表。</p> <p>在专用分配池中，您可以通过列出用户名和计算机名称将用户与计算机配对。</p> <p>有关详细信息，请参阅在Horizon Console 中指定计算机名称列表。</p>
池大小	您要指定计算机的最大数量。	您指定的计算机名称列表决定计算机的数量。
向池中添加计算机	您可以增加池大小的上限。	<p>您可以向列表中添加计算机名称。</p> <p>有关详细信息，请参阅将计算机添加到通过名称列表置备的自动池中。</p>
按需置备	<p>可用。</p> <p>在用户首次登录时或者当您将计算机分配给用户时，Horizon 7 会动态创建和置备指定的最小数量和备用数量的计算机。</p> <p>Horizon 7 还可以在您创建池时创建和置备所有计算机。</p>	<p>不可用。</p> <p>Horizon 7 会创建和置备您在创建池时在列表中指定的所有计算机。</p>
初始自定义	<p>可用。</p> <p>置备计算机后，Horizon 7 可以运行您选择的自定义规范。</p>	<p>可用。</p> <p>置备计算机后，Horizon 7 可以运行您选择的自定义规范。</p>
手动自定义专用计算机	<p>不可用于即时克隆。</p> <p>要自定义计算机并将桌面访问权限返回给用户，您必须移除并重新分配每个计算机的所有权。根据是否在首次登录时分配计算机，您可能需要将这些步骤执行两次。您不能在维护模式下启动计算机。创建池后，您可以手动将计算机置于维护模式。</p>	<p>您可以在不重新分配所有权的情况下对计算机进行自定义和测试。</p> <p>创建池时，您可以在维护模式下启动所有计算机，以阻止用户访问。您可以自定义这些计算机，然后退出维护模式，将访问权返回给用户。</p> <p>有关详细信息，请参阅手动自定义计算机。</p>

功能	使用计算机命名模式	手动命名计算机
动态或固定的池大小	<p>动态。</p> <p>如果从专用分配池中的某个计算机移除用户分配，该计算机将被返回到可用计算机池。</p> <p>如果您在浮动分配池中选择注销后删除计算机，那么根据活动用户会话的数量，池大小可能会增大或缩小。</p> <p>注 即时克隆池只能为浮动分配池。计算机始终会在注销时被删除。</p>	<p>固定。</p> <p>池中包含的计算机数量取决于您在计算机名称列表中提供的信息。</p> <p>如果您手动命名计算机，则不能选择注销后删除计算机设置。</p>
备用计算机	<p>您可以指定一些备用计算机，Horizon 7 会使这些计算机保持处于电源打开状态，以供新用户使用。</p> <p>Horizon 7 会创建新的计算机以维持指定的数量。池的大小达到上限后，Horizon 7 将停止创建备用计算机。</p> <p>Horizon 7 会使备用计算机保持处于电源打开状态，即便池的电源策略为关闭或挂起，或者您并未设置电源策略，也都是如此。</p> <p>注 即时克隆池没有电源策略。</p>	<p>您可以指定一些备用计算机，Horizon 7 会使这些计算机保持处于电源打开状态，以供新用户使用。</p> <p>Horizon 7 不会创建新的备用计算机来维持指定的数量。</p> <p>Horizon 7 会使备用计算机保持处于电源打开状态，即便池的电源策略为关闭或挂起，或者您并未设置电源策略，也都是如此。</p>
用户分配	<p>您可以为专用分配池和浮动分配池使用命名模式。</p>	<p>您可以为专用分配池和浮动分配池指定计算机名称。</p> <p>注 在浮动分配池中，您不能将用户名与计算机名称相关联。计算机不会专供关联的用户使用。在浮动分配池中，当前未处于使用状态的所有计算机均可供登录的用户访问。</p>

在 Horizon Console 中指定计算机名称列表

您可以通过手动指定计算机名称列表来置备自动桌面池。此命名方法允许您使用自己公司的命名约定来标识池中的计算机。

如果您明确指定计算机名称，那么用户登录其远程桌面时将看到基于其所在公司组织的熟悉名称。

按照以下指南手动指定计算机名称：

- 每个计算机名称都输入到单独的一行中。
- 计算机名称最多可以包含 15 个字母数字字符。
- 可以在每个计算机条目中添加一个用户名。使用逗号将用户名与计算机名称隔开。

在此示例中指定了两个计算机。第二个计算机与某个用户关联：

```
Desktop-001
Desktop-002,abccorp.com\jdoe
```

注 在浮动分配池中，您不能将用户名与计算机名称相关联。计算机不会专供关联的用户使用。在浮动分配池中，当前未处于使用状态的所有计算机均可供登录的用户访问。

前提条件

确保每个计算机名称都是唯一的。不能使用 vCenter Server 中现有虚拟机的名称。

步骤

- 1 创建一个包含计算机名称列表的文本文件。

如果要创建仅包含几个计算机的桌面池，您可以直接在**添加池**向导中键入计算机名称。而不必创建单独的文本文件。

- 2 在 Horizon Console 中启动**添加池**向导，以开始创建包含完整虚拟机的自动桌面池。

- 3 在“置备设置”页面上，选择**手动指定名称**，然后单击**输入名称**。

- 4 复制**输入计算机名称**页面中的计算机名称列表，然后单击**下一步**。

- 5 单击**提交**。

- 6 （可选）选择在**维护模式下启动计算机**。

利用此选项，您可以先自定义计算机，然后再允许用户登录和使用计算机。

- 7 按照向导中的提示完成桌面池的创建。

Horizon 7 会为列表中的每个名称创建一个计算机。对于包含计算机和用户名的条目，Horizon 7 会将该计算机分配给条目中的用户。

创建桌面池之后，您可以导入另一个包含其他计算机名称和用户的列表文件，从而添加更多计算机。请参阅[将计算机添加到通过名称列表置备的自动池中](#)。

为自动桌面池使用命名模式

您可以置备池中的计算机，方法是提供命名模式以及池中所需的计算机总数。默认情况下，Horizon 7 会将提供的模式用作所有计算机名称的前缀，并附加一个唯一编号，以标识每个计算机。

计算机名称中命名模式的长度

计算机名称限制为 15 个字符，其中包括命名模式和自动生成的编号。

表 10-8. 计算机名称中命名模式的最大长度

设置的池中计算机数	最大前缀长度如下
1-99	13 个字符
100-999	12 个字符
1,000 或更多	11 个字符

包含固定长度令牌的名​​称具有不同的长度限制。请参阅[使用固定长度令牌时的命名模式长度](#)。

在计算机名称中使用令牌

通过使用令牌，您可以将自动生成的编号放置在名称中的任何位置。当您键入池名称时，需要在大括号中键入 **n** 来指定令牌。

例如：amber-{n}-desktop

创建计算机时，Horizon 7 会将 **{n}** 替换为一个唯一编号。

您可以通过键入 **{n:fixed=位数}** 来生成一个固定长度的令牌。

Horizon 7 会将令牌替换为包含指定位数的编号。

例如，如果您键入 **amber-{n:fixed=3}**，Horizon 7 会将 **{n:fixed=3}** 替换为一个三位数的编号，并创建以下计算机名称：**amber-001**、**amber-002** 和 **amber-003** 等等。

使用固定长度令牌时的命名模式长度

包括命名模式和令牌位数在内，包含固定长度令牌的名称的长度不能超过 15 个字符。

表 10-9. 使用固定长度令牌时的命名模式最大长度

固定长度的令牌	命名模式的最大长度
{n:fixed=1}	14 个字符
{n:fixed=2}	13 个字符
{n:fixed=3}	12 个字符

计算机命名示例

此示例显示了如何创建两个使用相同计算机名称，但各有一组不同编号的自动桌面池。此示例中使用的策略实现了具体的用户目标并展示了计算机命名方法的灵活性。

我们的目标是创建两个具有相同命名约定的池，如 **VDIABC-XX**，其中 **XX** 代表编号。每个池具有一组不同的顺序编号。例如，第一个池包含的计算机可能是 **VDIABC-01** 到 **VDIABC-10**，第二个池包含的计算机可能是 **VDIABC-11** 到 **VDIABC-20**。

您可以使用任意一种计算机命名方法来实现此目标。

- 要一次创建多组固定的计算机，请手动指定计算机名称。
- 要在用户首次登录时动态创建计算机，请提供一种命名模式，并使用令牌指定顺序编号。

手动指定名称

- 1 为第一个池（包含从 **VDIABC-01** 到 **VDIABC-10** 的计算机名称列表）准备一个文本文件。
- 2 在 Horizon Console 中，创建池并手动指定计算机名称。
- 3 单击**输入名称**并将您的列表复制到**输入计算机名称**列表框中。
- 4 对第二个池（使用桌面名称 **VDIABC-11** 到 **VDIABC-20**）重复这些步骤。

有关详细说明，请参阅[在 Horizon Console 中指定计算机名称列表](#)。

您可以在创建每个池后向其中添加计算机。例如，您可以将计算机 **VDIABC-21** 到 **VDIABC-30** 添加到第一个池中，将 **VDIABC-31** 到 **VDIABC-40** 添加到第二个池中。请参阅[将计算机添加到通过名称列表置备的自动池中](#)。

使用令牌提供命名模式

- 1 在 Horizon Console 中，创建第一个池，并使用命名模式置备计算机名称。
- 2 在命名模式文本框中键入 **VDIABC-0{n}**。

3 将池的最大大小限定为 9。

4 对第二个池重复这些步骤，但在命名模式文本框中键入 **VDIABC-1{n}**。

第一个池将包含计算机 VDIABC-01 到 VDIABC-09，第二个池将包含计算机 VDIABC-11 到 VDIABC-19。

也可以通过使用 2 位数的固定长度令牌，将每个池配置为最多包含 99 个计算机：

- 对于第一个池，键入 **VDIABC-0{n:fixed=2}**。
- 对于第二个池，键入 **VDIABC-1{n:fixed=2}**。

将每个池的最大大小限定为 99。此配置生成的计算机将具有 3 位数的顺序命名模式。

第一个池：

```
VDIABC-001
VDIABC-002
VDIABC-003
```

第二个池：

```
VDIABC-101
VDIABC-102
VDIABC-103
```

有关命名模式和令牌的详细信息，请参阅[为自动桌面池使用命名模式](#)。

将计算机添加到通过名称列表置备的自动池中

要将计算机添加到通过手动指定计算机名称置备的自动桌面池，应另外提供一个新计算机名称的列表。利用此功能，您可以扩展桌面池并继续使用您公司的命名约定。

手动添加计算机名称时请遵循以下准则：

- 每个计算机名称都输入到单独的一行中。
- 计算机名称最多可以包含 15 个字母数字字符。
- 可以在每个计算机条目中添加一个用户名。使用逗号将用户名与计算机名称隔开。

在本例中，添加了两个计算机。第二个计算机与某个用户关联：

```
Desktop-001
Desktop-002,abccorp.com/jdoe
```

注 在浮动分配池中，您不能将用户名与计算机名称相关联。计算机不会专供关联的用户使用。在浮动分配池中，当前未处于使用状态的所有计算机均可供登录的用户访问。

前提条件

确认已通过手动指定计算机名称创建了完整虚拟机的自动桌面池。如果通过提供命名模式创建了池，则无法通过提供新计算机名称添加计算机。

步骤

- 1 创建一个文本文件，其中包含附加计算机名称的列表。
如果打算只添加几个计算机，可以直接在**添加池**向导中键入计算机名称。而不必创建单独的文本文件。
- 2 在 Horizon Console 中，选择**清单 > 桌面**。
- 3 选择要扩展的桌面池。
- 4 单击**编辑**。
- 5 单击**置备设置**选项卡。
- 6 单击**添加计算机**。
- 7 复制**输入计算机名称**页面中的计算机名称列表，然后单击**下一步**。
- 8 单击**提交**。
- 9 单击**确定**。

在 vCenter Server 中，您可以监视新虚拟机的创建操作。

在 Horizon Console 中，您可以在将计算机添加到桌面池时查看这些计算机，方法是选择**清单 > 桌面**。

在 Horizon Console 中更改由命名模式置备的自动池的大小

使用命名模式置备自动桌面池时，可以通过更改计算机的最大数量来增加或减少池大小。

前提条件

- 确认您是使用命名模式来置备桌面池的。
- 确认桌面池为自动池。

步骤

- 1 在 Horizon Console 中，选择**清单 > 桌面**。
- 2 单击桌面池 ID，然后单击**编辑**。
- 3 在**置备设置**选项卡中，在**计算机的最大数量**文本框中键入桌面池中新的计算机的数量。

如果您增加桌面池的大小，则可向池中添加新的计算机，直到达到最大数量。

如果减小浮动分配池的大小，未使用的计算机将被删除。如果登录池的用户数超过了新的最大值，用户注销后，池的容量会减小。

如果减小专用分配池的大小，未分配的计算机将被删除。如果给计算机分配的用户超过了新的最大值，取消用户分配后，池大小会减小。

注 当您减小池大小时，如果当前登录或分配给计算机的用户数大于**计算机的最大数量**中指定的值，计算机的实际数量可能会大于**计算机的最大数量**。

手动自定义计算机

创建自动池后，您可以自定义特定的计算机而无需重新分配所有权。通过在维护模式下启动计算机，您可以在将计算机发布给用户之前对计算机进行修改和测试。

注 此功能不可用于即时克隆桌面池。

维护模式阻止用户访问桌面。如果您在维护模式下启动计算机，**Horizon 7** 会在创建计算机后将每个计算机都置于维护模式下。在完整虚拟机的专用分配池中，您可以使用维护模式登录计算机，而无需为自己的管理员帐户重新分配所有权。完成自定义后，不必将所有权交还给为计算机分配的用户。

要对自动池中的所有计算机进行同样的自定义，可以先对准备作为模板或父虚拟机的虚拟机进行自定义。**Horizon 7** 会将您的自定义内容部署到所有计算机。

注 当您为池手动指定计算机名称，而不是通过提供命名模式来命名计算机时，可以在维护模式下启动计算机。

在 Horizon Console 中在维护模式下自定义现有计算机

创建桌面池后，您可以将各个计算机置于维护模式，从而自定义、修改或测试这些计算机。当计算机处于维护模式时，用户无法访问虚拟机桌面。

您一次只能将一个现有计算机置于维护模式。您可以通过一个操作使多个计算机退出维护模式。

创建桌面池时，如果您手动指定计算机名称，则可以在维护模式下启动该池中的所有计算机。

步骤

- 1 在 Horizon Console 中，选择**清单 > 桌面**，双击某个池 ID，然后选择**清单**选项卡。
- 2 选择一个计算机。
- 3 从**更多命令**下拉菜单中选择**进入维护模式**。
- 4 自定义、修改或测试虚拟机桌面。
- 5 重复**步骤 2**到**步骤 4**
- 6 选择自定义的计算机，然后从**更多命令**下拉菜单中选择**退出维护模式**。

修改后的虚拟机桌面即可供用户使用。

在 Horizon Console 中自定义单个计算机

创建池之后，您可以通过在维护模式下启动计算机来自定义各个计算机。

步骤

- 1 在 Horizon Console 中，启动**添加池**向导，开始创建自动桌面池。
- 2 在“置备设置”页面上，选择**手动指定名称**。
- 3 选择在**维护模式下启动计算机**。
- 4 完成**添加池**向导，以完成桌面池的创建。

5 在 vCenter Server 中，登录、自定义并测试各个虚拟机。

您可以手动自定义计算机，也可以使用标准的 Windows 系统管理软件（如 Altiris、SMS、LanDesk 或 BMC）来进行自定义。

6 在 Horizon Console 中，选择**清单 > 计算机**。

7 选择要发布给用户的特定计算机。

8 单击**更多命令 > 退出维护模式**。

后续步骤

通知用户他们可以登录桌面。

Horizon Console 中适用于所有桌面池类型的桌面池设置

在配置包含完整虚拟机的自动池、链接克隆桌面池、手动桌面池以及即时克隆桌面池时，必须指定计算机和桌面池的设置。并非所有设置都适用于所有类型的桌面池。

表 10-10. 桌面池设置描述

设置	选项
状态	<ul style="list-style-type: none"> ■ 已启用。桌面池创建后将自动启用，并可以立即投入使用。 ■ 已禁用。桌面池在创建完成后将被禁用且无法使用，池的置备也将停止。如果要执行部署后的活动，如测试或其他形式的基准维护，则该设置很适用。 <p>当此状态生效时，远程桌面不可用。</p>
连接服务器限制	<ul style="list-style-type: none"> ■ 无。任何连接服务器实例均可以访问桌面池。 ■ 带有标记。选择一个或多个连接服务器标签，可仅允许带有这些标签的连接服务器实例访问桌面池。您可以使用复选框选择多个标记。 <p>如果您想通过 VMware Identity Manager 提供桌面访问，并且配置了连接服务器限制，则当桌面实际受到限制时，VMware Identity Manager 应用程序可能会向用户显示这些桌面。VMware Identity Manager 用户将无法启动这些桌面。</p>
类别文件夹	<p>为包含 Windows 客户端设备上桌面池授权的“开始”菜单快捷方式的类别文件夹指定名称。有关更多信息，请参阅《在 Horizon 7 中设置已发布的桌面和应用程序》文档中的“为桌面和应用程序池配置‘开始’菜单快捷方式”。此功能适用于 Horizon Administrator。</p>
会话类型	<p>您可以通过选择桌面池支持的会话类型，来基于桌面池创建应用程序池：</p> <ul style="list-style-type: none"> ■ 桌面。仅支持桌面。 ■ 应用程序。仅支持应用程序。 ■ 桌面和应用程序。同时支持桌面和应用程序。
远程计算机电源策略	<p>确定用户从关联的桌面注销后该虚拟机的行为方式。</p> <p>有关电源策略选项的说明，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“桌面池的电源策略”。</p> <p>有关电源策略如何影响自动池的更多信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“为桌面池设置电源策略”。</p> <p>不适用于即时克隆桌面池。即时克隆始终处于电源打开状态。</p>

设置	选项
断开连接后自动注销	<ul style="list-style-type: none"> ■ 立即。用户在断开连接后立即注销。 ■ 从不。永不注销用户。 ■ 之后。用户断开连接的时间超过此设置后即注销。键入持续时间（以分钟为单位）。 <p>注销时间适用于以后断开的连接。如果在设置注销时间时桌面会话已经断开，则该用户的注销持续时间以设置注销时间的时刻为起点，而不是会话断开的时刻。例如，如果您将此值设置为五分钟，而会话在 10 分钟前断开，View 将会在您设置完该值的五分钟后注销本次会话。</p>
允许用户重置/重新启动计算机	允许用户重置或重新启动自己的桌面。
允许用户从不同的客户端设备启动单独的会话	<p>选择该设置时，从不同的客户端设备连接到同一桌面池的用户将获取不同的桌面会话。用户只能从启动该会话的客户端设备重新连接到现有的会话。未选择该设置时，用户可以使用任意客户端设备重新连接到其现有的会话。</p> <p>注 在桌面池上运行的应用程序不支持多会话，因此该设置不适用于从桌面池创建的应用程序。</p>
注销后删除虚拟机	<p>选择是否删除浮动分配的完整虚拟机。</p> <ul style="list-style-type: none"> ■ 否。用户注销后，虚拟机保留在桌面池中。 ■ 是。用户注销后立即关闭并删除虚拟机。 <p>对于即时克隆桌面，注销后始终会删除并重新创建虚拟机。</p>
注销时删除或刷新虚拟机	<p>选择将浮动分配链接克隆虚拟机删除、刷新还是保持不变。</p> <ul style="list-style-type: none"> ■ 从不。用户注销后，虚拟机保留在池中而不进行刷新。 ■ 立即删除。用户注销后立即关闭并删除虚拟机。用户注销时，虚拟机会立即进入正在删除状态。 ■ 立即刷新。用户注销后立即刷新虚拟机。用户注销时，虚拟机会立即进入维护模式，以防止其他用户在刷新操作开始时登录。 <p>对于即时克隆桌面，注销后始终会删除并重新创建虚拟机。</p>
注销后刷新操作系统磁盘	<p>选择是否以及何时刷新专用分配链接克隆虚拟机的操作系统磁盘。</p> <ul style="list-style-type: none"> ■ 从不。从不刷新操作系统磁盘。 ■ 始终。用户每次注销时均刷新操作系统磁盘。 ■ 间隔时间。操作系统磁盘在指定的时间间隔（以天为单位）定期刷新。键入天数。 <p>天数将从最后一次刷新开始计算，如未进行过刷新，则从最初置备开始计算。例如，如果指定的值为 3 天，而且从上次刷新开始算起已超过 3 天，那么计算机将在用户注销后刷新。</p> <ul style="list-style-type: none"> ■ 特定量。当操作系统磁盘当前的容量达到其允许的最大容量的指定百分比时，刷新该操作系统磁盘。链接克隆操作系统磁盘的最大容量就是副本操作系统磁盘的容量。键入启动刷新操作的百分比。 <p>使用 特定量 选项时，数据存储中的链接克隆操作系统的大小将与允许的最大容量进行对比。磁盘利用率百分比不能反映您在计算机客户机操作系统中看到的磁盘使用情况。</p> <p>刷新专用分配链接克隆池中的操作系统磁盘时，View Composer 永久磁盘不受影响。</p> <p>对于即时克隆桌面，注销后始终会删除并重新创建虚拟机。</p>

设置	选项
默认显示协议	<p>选择您希望连接服务器与客户端进行通信时使用的显示协议。</p> <p>VMware Blast VMware Blast Extreme 协议构建于 H.264 协议之上，支持任何网络中最广泛的客户端设备，包括智能手机、平板电脑、超低成本 PC 和 Mac。此协议具有最低的 CPU 资源消耗率，因此能够延长移动设备上的电池寿命。</p> <p>PCoIP PCoIP 可作为具有 Teradici 硬件的虚拟机和物理机的显示协议。PCoIP 为 LAN 或 WAN 中的广大用户提供了交付的图像、音频和视频内容方面的最佳 PC 体验。</p> <p>Microsoft RDP Microsoft 远程桌面连接 (RDC) 使用 RDP 来传输数据。RDP 是一种允许用户远程连接计算机的多通道协议。</p>
允许用户选择协议	<p>允许用户使用 Horizon Client 覆盖其桌面的默认显示协议。</p>
3D 呈现器	<p>如果池包含 Windows 7 或更高版本桌面，则您可以选择是否启用 3D 图形呈现。根据安装在 ESXi 5.1 或更高版本主机上的物理 GPU 显卡，您可配置 3D 呈现器 使用软件呈现或硬件呈现。</p> <p>要启用此功能，您必须选择 PCoIP 或 VMware Blast 作为协议，并禁用 允许用户选择协议 设置（选择否）。</p> <p>使用基于硬件的 3D 呈现器 选项，用户可利用图形应用程序执行设计、建模和多媒体操作。使用软件 3D 呈现器 选项，用户可利用诸如 AERO、Microsoft Office 和 Google Earth 之类的要求相对低一些的应用程序中的图形增强功能。有关系统要求，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“为桌面配置 3D 呈现”。</p> <p>如果您的 View 部署不是运行在 vSphere 5.0 或更高版本中，此设置会不可用，且在 View Administrator 中会处于非活动状态。</p> <p>在选择该功能时，如果选择 自动、软件 或 硬件 选项，则可以配置为池中的计算机分配的 VRAM 量。最大显示器数为 2 个，最大分辨率为 1920 x 1200。</p> <p>如果选择 使用 vSphere Client 管理 或 NVIDIA GRID vGPU，则必须在 vCenter Server 中配置 3D 内存量和显示器数。您可以为用作远程桌面的计算机选择最多四个显示器，具体取决于显示器分辨率。</p> <p>注 在配置或编辑此设置后，必须关闭现有虚拟机的电源，确认在 vCenter Server 中重新配置了这些计算机，然后打开其电源以使新设置生效。重新启动虚拟机不会使新设置生效。</p> <p>对于即时克隆桌面池，NVIDIA GRID vGPU 是唯一可用的 3D 呈现器选项。</p>
显示器最大数量	<p>如果选择 PCoIP 或 VMware Blast 作为显示协议，您可以选择用户用于显示桌面的 显示器最大数量。您最多可以选择四个显示器。</p> <p>如果未选择 3D 呈现器 设置，显示器最大数量 设置将影响分配到池中计算机的 VRAM 大小。当您增加显示器数量时，相关联的 ESXi 主机将会消耗更多的内存。</p> <p>如果未选择 3D 呈现器 设置，禁用了 Aero 的 Windows 7 客户机操作系统在 3840x2160 分辨率下最多支持三个显示器。对于其他操作系统或启用了 Aero 的 Windows 7，在 3840x2160 分辨率下支持一个显示器。</p> <p>如果选择了 3D 呈现器 设置，在 3840x2160 分辨率下支持一个显示器。在较低的分辨率下，可以较好地支持多个显示器。如果选择较高的分辨率，请选择较少的显示器。</p> <p>注 您必须关闭并重新启动现有的虚拟机，才能使该设置生效。重新启动虚拟机不会使设置生效。</p>

设置	选项
任意一台显示器的最大分辨率	<p>如果选择 PCoIP 或 VMware Blast 作为显示协议，您应该指定任意一台显示器的最大分辨率。</p> <p>默认情况下，任意一台显示器的最大分辨率设置为 1920x1200 像素，但您可以配置该值。</p> <p>如果未选择 3D 呈现器设置，任意一台显示器的最大分辨率设置将影响分配给池中的计算机的 VRAM 大小。当您分辨率调大后，相关联的 ESXi 主机将会消耗更多的内存。</p> <p>如果未选择 3D 呈现器设置，禁用了 Aero 的 Windows 7 客户机操作系统在 3840x2160 分辨率下最多支持三个显示器。对于其他操作系统或启用了 Aero 的 Windows 7，在 3840x2160 分辨率下支持一个显示器。</p> <p>如果选择了 3D 呈现器设置，在 3840x2160 分辨率下支持一个显示器。在较低的分辨率下，可以较好地支持多个显示器。如果选择较高的分辨率，请选择较少的显示器。</p> <p>注 您必须关闭并重新启动现有的虚拟机，才能使该设置生效。重新启动虚拟机不会使设置生效。</p>
HTML Access	<p>选择已启用以允许用户从其 Web 浏览器连接到远程桌面。</p> <p>当用户通过 VMware Horizon Web 门户页面或 VMware Identity Manager 应用程序登录并选择远程桌面时，HTML Access 代理允许用户通过 HTTPS 连接到该桌面。桌面显示在用户的浏览器中。其他的显示协议如 PCoIP 或 RDP 不被使用。无需在客户端设备上安装 Horizon Client 软件。</p> <p>要使用 HTML Access，必须在 View 部署中安装 HTML Access。有关详细信息，请参阅《使用 HTML Access》（可从 https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html 获得）。</p> <p>要将 HTML Access 与 VMware Identity Manager 配合使用，必须将连接服务器与 SAML 身份验证服务器进行配对，如《Horizon 7 管理指南》文档中所述。必须安装并配置 VMware Identity Manager，才能与连接服务器一起使用。</p>
允许会话协作	<p>选择已启用，允许池用户邀请其他用户加入其远程桌面会话。会话所有者和会话协作者必须使用 VMware Blast 显示协议。</p>

在 Horizon Console 中管理桌面池和虚拟桌面

在 Horizon Console 中，您可以管理桌面池、基于虚拟机的桌面、基于物理机的桌面和桌面会话。

管理桌面池

您可以对桌面池执行各种管理任务，如编辑其属性以及启用、禁用或删除池。

编辑桌面池

您可以编辑现有桌面池，以配置备用计算机数量、数据存储和自定义规范等设置。

前提条件

熟悉在创建桌面池后可以更改和无法更改的桌面池设置。请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“修改现有桌面池中的设置”和“现有桌面池中的固定设置”。

步骤

- 1 在 Horizon Console 中，选择**清单 > 桌面**。
- 2 选择一个桌面池，然后单击**编辑**。
- 3 在“编辑”对话框中单击某个选项卡，然后重新配置桌面池选项。
- 4 单击**确定**。

如果更改即时克隆桌面池的映像，将立即启动映像发布操作。在 **Horizon Administrator** 中，桌面池的摘要页面将等待处理的映像状态显示为正在发布。

如果更改即时克隆桌面池的群集，则会在新群集中创建新的副本和父虚拟机。您可以使用相同的映像启动推送映像以在新群集中创建新的克隆。不过，在创建克隆过程中使用的模板虚拟机保留在旧群集中。您可以将模板虚拟机所在的 **ESXi** 主机置于维护模式，但无法迁移模板虚拟机。要从旧群集中完全移除所有基础架构虚拟机（包括模板虚拟机），您可以使用新映像启动推送映像。

删除桌面池

当您删除某个桌面池时，用户将无法在该池中启动新的远程桌面。

根据桌面池的类型，有各种有关 **Horizon 7** 如何处理永久磁盘、**vCenter Server** 完整虚拟机和用户活动会话的选项可供您选择。

默认情况下，您可以删除桌面池，即使在池中具有桌面计算机。有关详细信息，请参阅《在 **Horizon 7** 中设置虚拟桌面》文档中的“配置桌面池删除设置”。如果配置该设置，您必须删除桌面池中的所有计算机，然后才能删除该池。

对于即时克隆的自动桌面池，**Horizon 7** 始终会从磁盘中删除虚拟机。

重要事项 在通过 **Horizon Console** 删除桌面池之前，请不要在 **vCenter Server** 中删除虚拟机。该操作会使 **Horizon 7** 组件的状态不一致。

步骤

- 1 在 **Horizon Console** 中，选择**清单 > 桌面**。
- 2 选择一个桌面池，然后单击**删除**。
- 3 选择如何删除桌面池。

池	选项
不带永久磁盘的即时克隆的自动桌面池。	无可用选项。 Horizon 7 将从磁盘中删除所有虚拟机。用户访问远程桌面的会话将终止。
完整虚拟机的自动桌面池。	选择在 vCenter Server 中是保留还是删除虚拟机。
RDS 桌面池。 完整虚拟机的自动桌面池。	如果有用户已连接到其远程桌面，请选择是保持用户会话处于活动状态还是终止会话。请注意，连接服务器不会跟踪保持活动状态的会话。

删除桌面池时，完整虚拟机的计算机帐户将保留在 **Active Directory** 中。要移除这些帐户，您必须从 **Active Directory** 中手动删除它们。

如果删除即时克隆桌面池，**Horizon 7** 可能需要一些时间来从 **vCenter Server** 中删除内部虚拟机。在确认已删除所有内部虚拟机后，才能从 **Horizon Console** 中移除 **vCenter Server**。

禁用或启用桌面池

当您禁用某个桌面池时，该池将不再提供给用户且池置备将停止。用户无法访问该池。禁用池后，您可以重新启用池。

前提条件

在准备桌面时，您可以禁用桌面池以防止用户访问他们的远程桌面。如果不再需要某个桌面池，您可以使用禁用功能撤消池的可用状态，而无需从 Horizon 7 中删除该桌面池的定义。

步骤

- 1 在 Horizon Console 中，选择**清单 > 桌面**。
- 2 选择一个桌面池并更改池的状态。

选项	操作
禁用池	从 状态 下拉菜单中选择 禁用桌面池 。
启用池	从 状态 下拉菜单中选择 启用桌面池 。

- 3 单击**确定**。

在桌面池中禁用或启用置备

在自动桌面池中禁用置备时，Horizon 7 将停止为该池置备新虚拟机。禁用置备后，您可以重新启用置备。

在更改桌面池的配置之前，您可以禁用置备来确保不会使用旧配置创建新计算机。当池的可用空间快要填满时，您也可以禁用置备来防止 Horizon 7 使用更多存储空间。

步骤

- 1 在 Horizon Console 中，选择**清单 > 桌面**。
- 2 选择一个桌面池并更改池的状态。

选项	操作
禁用置备	从 状态 下拉菜单中选择 禁用置备 。
启用置备	从 状态 下拉菜单中选择 启用置备 。

- 3 单击**确定**。

管理基于虚拟机的桌面

基于虚拟机的桌面是来自包含 vCenter Server 虚拟机的自动或手动桌面池的桌面。

在 Horizon Console 中向用户分配计算机

在专用分配池中，您可以分配一个用户作为托管远程桌面的虚拟机的所有者。只有分配的用户才可以登录并连接到该远程桌面。

在以下情况中，Horizon Console 会向用户分配计算机。

- 当您创建一个桌面池并选择**允许自动分配**设置时。

注 如果您选择了**允许自动分配**设置，仍可以手动向用户分配计算机。

- 当您创建自动池时，选择**手动指定名称**设置，并提供用户名和计算机名称。

如果您在专用分配池中未选择任何设置，用户将无法访问虚拟桌面。您必须手动向每个用户分配计算机。

也可以使用 `vdmadmin` 命令向用户分配计算机。有关 `vdmadmin` 命令的更多信息，请参阅《Horizon 7 管理指南》指南。

前提条件

- 确认虚拟机属于专用分配池。在 Horizon Console 中，桌面池分配显示在**桌面池**页面上的**用户分配**列中。

步骤

- 1 在 Horizon Console 中，选择**清单 > 桌面**，双击池 ID，然后单击**清单**选项卡。
- 2 选择计算机。
- 3 从**更多命令**下拉菜单中选择**分配用户**。
- 4 选择是查找用户还是查找组，选择域，然后在**名称或描述**文本框中键入搜索字符串。
- 5 选择用户名或组名，然后单击**确定**。

在 Horizon Console 中取消专用计算机的用户分配

在专用分配池中，您可以移除针对用户的计算机分配。

您也可以使用 `vdmadmin` 命令移除针对用户的计算机分配。有关 `vdmadmin` 命令的更多信息，请参阅《Horizon 7 管理指南》指南。

步骤

- 1 在 Horizon Console 中，选择**清单 > 桌面**，双击池 ID，然后单击**清单**选项卡。
- 2 选择计算机。
- 3 从**更多命令**下拉菜单中选择**取消分配用户**。
- 4 单击**确定**。

计算机将变为可用并可以分配给其他用户。

在 Horizon Console 中删除虚拟机桌面

删除虚拟机桌面后，用户再也无法访问该桌面。

如果您将虚拟机保留在 vCenter Server 中，当前处于活动会话状态的用户可以继续使用完整的虚拟机桌面。用户注销后，他们无法访问已删除的虚拟机桌面。

对于即时克隆，vCenter Server 始终会从磁盘上删除虚拟机。

注 在通过 Horizon Console 删除虚拟机桌面之前，请不要在 vCenter Server 中删除虚拟机。该操作会使 Horizon 7 组件的状态不一致。

步骤

- 1 在 Horizon Console 中，选择**清单 > 计算机**
- 2 选择 **vCenter 虚拟机**选项卡。
- 3 选择一个或多个计算机，然后单击**删除**。
- 4 选择如何删除虚拟机桌面。

选项	说明
包含完整虚拟机桌面的池	<p>选择在 vCenter Server 中是保留还是删除虚拟机。</p> <p>如果您从磁盘上删除了虚拟机，处于活动会话中的用户将从其桌面断开。</p> <p>如果您在 vCenter Server 中保留虚拟机，请选择是允许处于活动会话中的用户与其桌面保持连接还是将他们断开。</p>
不带永久磁盘的即时克隆池	vCenter Server 将从磁盘上删除即时克隆虚拟机。当前处于活动会话中的用户将从其远程桌面断开。

在 Horizon Console 中将 Horizon 7 信息导出到外部文件

在 Horizon Console 中，您可以将 Horizon 7 表信息导出到外部文件。您可以导出那些列出了用户和组、池、计算机、View Composer 永久磁盘、ThinApp 应用程序、事件和 VDI 会话的表。您可以在电子表格或其他工具中查看和管理这些信息。

例如，您可以收集受多个连接服务器实例或连接服务器副本实例组管理的计算机的相关信息。您可以从每个 Horizon Console 界面导出“计算机”表，然后在电子表格中查看此表。

导出 Horizon Console 表时，该表将另存为 Microsoft Excel Open XML 格式的电子表格 (XLSX) 文件。此功能将导出整个表，而不是单个页面。

步骤

- 1 在 Horizon Console 中，显示您要导出的表。
例如，单击**清单 > 计算机**以显示计算机表。
- 2 单击位于表右上角的导出图标。
当您指向该图标时，会显示导出表内容提示信息。
- 3 在“选择下载位置”对话框中键入 XLSX 文件的文件名。

4 浏览到用来存储该文件的位置。

5 单击**保存**。

后续步骤

打开电子表格或其他工具来查看该 XLSX 格式的文件。

管理 Horizon Composer 链接克隆桌面虚拟机

您可以更新 Horizon Composer 链接克隆桌面计算机、减少其操作系统数据的大小，以及重新平衡数据存储中的计算机。您还可以管理与链接克隆关联的永久磁盘。

在 Horizon Console 中通过计算机刷新减少链接克隆的大小

计算机刷新操作可将每个链接克隆的操作系统磁盘还原至其原始状态和大小，从而降低存储成本。

如果可能，请计划在非峰值时间执行刷新操作。

有关指导原则，请参阅[计算机刷新操作](#)。

前提条件

- 决定计划何时执行刷新。默认情况下，Horizon Composer 会立即启动该操作。

您仅可以对给定的一组链接克隆在某个时间计划一次刷新操作。您可以计划多个刷新操作，前提是这些操作针对不同的链接克隆。

- 决定在操作开始时强制所有用户注销，还是等每个用户注销后再刷新该用户的链接克隆桌面。

如果强制用户注销，Horizon 7 将在断开之前通知用户，并允许他们关闭应用程序和注销。

如果强制用户注销，则需要注销的远程桌面上的最大并发刷新操作数将为**最大并发 View Composer 维护操作数量**设置值的一半。例如，如果将此设置配置为 24，并强制用户注销，则需要注销的远程桌面上的最大并发刷新操作数为 12。

- 如果您的部署包括连接服务器副本实例，请确认所有实例均为相同版本。

步骤

1 在 Horizon Console 中，选择**清单 > 计算机**。

2 选择链接克隆虚拟机。

3 在**清单**选项卡中，选择刷新一个虚拟机或多个虚拟机。

- 要刷新一个虚拟机，请选择该虚拟机，然后从 **View Composer** 下拉菜单中选择**刷新**。
- 要刷新多个虚拟机，请选择多个虚拟机，然后从 **View Composer** 下拉菜单中选择**刷新**。

4 按照向导说明进行操作。

操作系统磁盘将减小到其原始大小。

在 vCenter Server 中，您可以监视链接克隆虚拟机执行刷新操作的进度。

在 Horizon Console 中，您可以监控该操作，方法是选择**清单 > 桌面**，单击池 ID，然后单击**任务**选项卡。您可以单击**暂停任务**、**取消任务**或**恢复任务**来挂起任务、取消任务或恢复挂起的任务。

计算机刷新操作

随着用户与链接克隆进行交互，克隆的操作系统磁盘会逐渐增长。计算机刷新操作可将操作系统磁盘还原为其原始状态和大小，从而降低存储成本。

刷新操作不会影响 Horizon Composer 永久磁盘。

链接克隆使用的存储空间少于父虚拟机，后者包含完整的操作系统数据。但是，每次在客户机操作系统中写入数据时，克隆的操作系统磁盘都会增大。

当 Horizon Composer 创建链接克隆时，它会为克隆的操作系统磁盘生成快照。该快照会用唯一标识标注此链接克隆虚拟机。刷新操作会把操作系统磁盘恢复到该快照。

Horizon Composer 刷新链接克隆所需的时间仅为删除并重新创建该克隆所需时间的一半。

在刷新操作中请遵循以下指导原则：

- 可以按需要刷新桌面池，可以将其设置为计划事件，也可以在操作系统数据达到指定的大小时进行刷新。

您仅可以对给定的一组链接克隆在某个时间计划一次刷新操作。如果您立即开始刷新操作，此操作将覆盖以前计划的全部任务。

您可以计划多个刷新操作，前提是这些操作针对不同的链接克隆。

在计划新的刷新操作之前，必须取消以前计划的全部任务。

- 您可以刷新专用分配池和浮动分配池。
- 仅当用户断开与其链接克隆桌面的连接后，才可以执行刷新。
- 刷新操作会保留 QuickPrep 或 Sysprep 设置的唯一计算机信息。您不需要在刷新后重新运行 Sysprep 来还原系统驱动器中安装的第三方软件的 SID 或 GUID。
- 重构链接克隆后，Horizon 7 会为该链接克隆的操作系统磁盘创建新的快照。此后的刷新操作将把操作系统数据还原到该快照，而不是还原到在最初创建该链接克隆时拍摄的快照。

如果您使用本地 NFS 快照 (VAAI) 技术生成链接克隆，某些供应商的 NAS 设备可在刷新链接克隆操作系统磁盘时为副本磁盘拍摄快照。这些 NAS 设备不支持直接为每个克隆操作系统磁盘拍摄快照。

- 您可以设置在刷新操作过程中，用户仍可进行连接的、已置备的就绪桌面的最小数量。

注 可通过将链接克隆的页面文件和系统临时文件重定向到临时磁盘中，以降低链接克隆的增长速度。链接克隆关闭电源后，Horizon 7 会将临时磁盘替换为 Horizon Composer 使用链接克隆池创建的原始临时磁盘的副本。此操作会将临时磁盘压缩为其原始大小。

您可以在创建链接克隆桌面池时配置此选项。

在 Horizon Console 中更新链接克隆桌面

您可以在父虚拟机上创建新的基础映像，然后使用重构功能将更新的映像分发到链接克隆，通过这种方式更新链接克隆虚拟机。

准备父虚拟机以重构链接克隆

在重构链接克隆桌面池之前，您必须更新用作该链接克隆的基础映像的父虚拟机。

Horizon Composer 不支持重构与父虚拟机使用不同操作系统的链接克隆。例如，您不能使用 Windows 8 父虚拟机的快照重构 Windows 7 链接克隆。

步骤

- 1 在 vCenter Server 中，更新父虚拟机以便重构。
 - 在父虚拟机中安装操作系统修补程序或服务包、新应用程序、应用程序更新或执行其他更改。
 - 也可以准备另一个虚拟机，以在重构过程中选作新的父虚拟机。
- 2 在 vCenter Server 中，关闭更新的或新的父虚拟机。
- 3 在 vCenter Server 中，为父虚拟机拍摄快照。

后续步骤

重构链接克隆桌面池。

在 Horizon Console 中重构链接克隆虚拟机

虚拟机重构会同时更新与父虚拟机绑定的所有链接克隆虚拟机。

如果可能，请计划在非峰值时间执行重构。

前提条件

- 确认您拥有父虚拟机的快照。请参阅[准备父虚拟机以重构链接克隆](#)。
- 熟悉重构指南。请参阅[通过重构来更新链接克隆](#)。
- 决定计划何时执行重构操作。默认情况下，Horizon Composer 会立即启动重构操作。

您仅可以对给定的一组链接克隆在某个时间计划一次重构操作。您可以计划多个重构，前提是这些操作针对不同的链接克隆。
- 决定在重构开始时强制所有用户注销，还是等每个用户注销后再重构该用户的链接克隆桌面。

如果强制用户注销，Horizon 7 将在断开之前通知用户，并允许他们关闭应用程序和注销。
- 决定是否在出现第一个错误时停止置备。选择此选项后，如果在 Horizon Composer 置备链接克隆时出现错误，针对桌面池中所有克隆的置备都将停止。您可以选择此选项来防止不必要的资源消耗（如存储）。

选择在出现第一个错误时停止选项对自定义不起作用。如果链接克隆出现自定义错误，将继续置备和自定义其他克隆。
- 确认桌面池置备已启用。当桌面池置备禁用时，Horizon 7 在重构桌面之后会停止自定义桌面。

- 如果您的部署包括 Horizon 连接服务器副本实例，请确认所有实例均为相同版本。

步骤

- 1 选择重构整个桌面池还是单个计算机。

选项	操作
重构桌面池中的所有虚拟机	<ol style="list-style-type: none"> a 在 Horizon Console 中，选择清单 > 桌面。 b 通过单击池 ID，选择要重构的桌面池。 c 在清单选项卡中，单击计算机。 d 选择左侧列中的所有计算机 ID。 e 从 Horizon Composer 下拉菜单中选择重构。
重构选定的虚拟机	<ol style="list-style-type: none"> a 在 Horizon Console 中，选择清单 > 计算机。 b 通过单击左侧列中的计算机 ID，选择要重构的计算机。 c 在摘要选项卡上，从 Horizon Composer 下拉菜单中选择重构。

- 2 按照向导说明进行操作。

您可以选择一个新的虚拟机用作桌面池的父虚拟机。

在“即将完成”页面上，您可以单击**显示详细信息**以显示重构的链接克隆桌面。

链接克隆虚拟机将刷新并更新。操作系统磁盘将减小到其原始大小。

在专用分配池中，未分配的链接克隆将被删除并重新创建。这时会保持指定数量的备用虚拟机。

在浮动分配池中，所有链接克隆将被重构。

在 vCenter Server 中，您可以监视链接克隆虚拟机执行重构的进度。

在 Horizon Console 中，您可以监控该操作，方法是选择**清单 > 桌面**，单击池 ID，然后单击**任务**选项卡。您可以单击**暂停任务**、**取消任务**或**恢复任务**来挂起任务、取消任务或恢复挂起的任务。

注 如果在创建桌面池时使用 Sysprep 自定义规范来自定义链接克隆，则可能会为重构的虚拟机生成新的 SID。

通过重构来更新链接克隆

在重构操作中，您可以提供操作系统修补程序，安装或更新应用程序，或者修改桌面池中所有链接克隆的虚拟机硬件设置。

要重构链接克隆虚拟机，您需要在 vCenter Server 中更新父虚拟机，或者选择一个不同的虚拟机作为新的父虚拟机。接下来，为新的父虚拟机配置拍摄快照。

您可以在不影响链接克隆的情况下更改父虚拟机，因为链接克隆链接到副本虚拟机，而不是直接链接到父虚拟机。

然后，您需要选择要用作桌面池新基础映像的快照，开始重构。Horizon Composer 会创建一个新副本，将重新配置的操作系统磁盘复制到链接克隆，然后将链接克隆绑定到新副本。

重构还会刷新链接克隆，降低其操作系统磁盘的大小。

桌面重构不会影响 Horizon Composer 永久磁盘。

在重构时请遵循以下指导原则：

- 您可以重构专用分配桌面池和浮动分配桌面池。
- 可以按需重构桌面池，也可以将其设置为计划事件。

您仅可以对给定的一组链接克隆在某个时间计划一次重构操作。在计划新的重构操作之前，必须取消以前计划的全部任务或等到前一次操作完成之后。在立即启动新的重构操作之前，必须取消以前计划的全部任务。

您可以计划多个重构，前提是这些操作针对不同的链接克隆。

- 可以重构选定的链接克隆，也可以重构桌面池中的所有链接克隆。
- 当桌面池中的不同链接克隆派生自同一基础映像的不同快照或不同基础映像时，桌面池中包含多个副本。
- 仅当用户注销其链接克隆桌面后，才能执行重构操作。
- 当链接克隆和新的或更新的父虚拟机使用不同的操作系统时，您无法重构链接克隆。
- 您无法将链接克隆重构为比其当前版本低的硬件版本。例如，您无法将使用硬件版本 8 的克隆重构为使用硬件版本 7 的父虚拟机。
- 在重构操作过程中，您可设置仍然可供用户连接的就绪、已置备桌面的最小数量。

注 如果在创建桌面池时使用 **Sysprep** 自定义规范来自定义链接克隆，则可能会为重构的虚拟机生成新的 SID。

更正失败的重构

您可以更正失败的重构。如果您在重构链接克隆时使用的不是您想要的基础映像，那么可以采取更正措施。

问题

重构失败时，虚拟机会处于错误或过期状态。

原因

在重构期间，vCenter Server 主机、vCenter Server 或数据存储中可能发生系统故障或问题。

或者，重构操作所用的虚拟机快照中所捕获的操作系统可能与原始父虚拟机的操作系统不同。例如，您可能会使用一个 Windows 8 快照重构 Windows 7 链接克隆。

解决方案

- 1 选择上一次成功重构时使用的快照。

您也可以选择新的快照，将链接克隆更新到新状态。

快照中所捕获的操作系统必须与原始父虚拟机快照中的操作系统相同。

- 2 再次重构桌面池。

Horizon Composer 将从快照创建基础映像，并重新创建链接克隆操作系统磁盘。

重构期间将保留包含用户数据和设置的 Horizon Composer 永久磁盘。

根据错误重构的情况，您可能需要刷新或重新平衡链接克隆而不是再次重构，也可能需要再次执行重构，并刷新或重新平衡链接克隆。

注 如果您未配置 Horizon Composer 永久磁盘，所有重构操作都会删除用户在链接克隆虚拟机中生成的更改。

在 Horizon Console 中重新平衡链接克隆虚拟机

重新平衡操作会在可用的数据存储之间重新平均分配链接克隆虚拟机。

如果可能，请计划在非峰值时间执行重新平衡操作。

前提条件

- 熟悉重新平衡操作。请参阅[#unique_185](#)。
- 决定计划何时执行重新平衡操作。默认情况下，Horizon Composer 会立即启动该操作。
您仅可以对给定的一组链接克隆在某个时间计划一次重新平衡操作。您可以计划多个重新平衡操作，前提是这些操作针对不同的链接克隆。
- 决定在操作开始时强制所有用户注销，还是等每个用户注销后再重新平衡该用户的链接克隆桌面。
如果强制用户注销，Horizon 7 将在断开之前通知用户，并允许他们关闭应用程序和注销。
如果强制用户注销，需要注销的远程桌面上的最大并发重新平衡操作数量为**最大并发 Horizon Composer 维护操作数**设置的值的一半。例如，如果将此设置配置为 24，并强制用户注销，则需要注销的远程桌面上的最大并发重新平衡操作数量为 12。
- 确认桌面池置备已启用。当池置备禁用时，Horizon 7 在重新平衡虚拟机之后会停止自定义这些虚拟机。
- 如果您的部署包括连接服务器副本实例，请确认所有实例均为相同版本。

步骤

- 1 选择重新平衡整个桌面池还是单个计算机。

选项	操作
重新平衡桌面池中的所有虚拟机	<ol style="list-style-type: none"> a 在 Horizon Console 中，选择清单 > 桌面。 b 通过单击池 ID，选择要重新平衡的桌面池。 c 在清单选项卡中，单击计算机。 d 选择左侧列中的所有计算机 ID。 e 从 View Composer 下拉菜单中选择重新平衡。
重新平衡选定的虚拟机	<ol style="list-style-type: none"> a 在 Horizon Console 中，选择清单 > 计算机。 b 通过单击左侧列中的计算机 ID，选择要重新平衡的计算机。 c 在摘要选项卡中，从 View Composer 下拉菜单中选择重新平衡。

- 2 按照向导说明进行操作。

链接克隆虚拟机将刷新和重新平衡。操作系统磁盘将减小到其原始大小。

在 Horizon Console 中，您可以监控该操作，方法是选择**清单 > 桌面**，双击池 ID，然后单击**任务**选项卡。您可以单击**暂停任务**、**取消任务**或**恢复任务**来挂起任务、取消任务或恢复挂起的任务。

在逻辑驱动器之间重新平衡链接克隆

重新平衡操作会在可用的逻辑驱动器之间重新平均分配链接克隆虚拟机。它可以节省过载驱动器上的存储空间，并确保充分利用所有驱动器。

当您创建大型链接克隆桌面池并使用多个逻辑单元号 (LUN) 时，如果初始大小不准确，可能无法有效利用空间。如果设置激进的存储过载级别，链接克隆可能会快速增长，并用完数据存储中的所有可用空间。

当虚拟机使用的空间达到数据存储空间的 95% 时，Horizon 7 会生成一个警告日志条目。

重新平衡还会刷新链接克隆，从而降低其操作系统磁盘的大小。它不会影响 Horizon Composer 永久磁盘。

在重新平衡时请遵循以下指导原则：

- 您可以重新平衡专用分配桌面池和浮动分配桌面池。
- 可以重新平衡选定的链接克隆或池中的所有克隆。
- 可以按需重新平衡桌面池，也可以将其设置为计划事件。

您仅可以对给定的一组链接克隆在某个时间计划一次重新平衡操作。如果立即开始重新平衡操作，此操作将覆盖以前计划的所有任务。

您可以计划多个重新平衡操作，前提是这些操作针对不同的链接克隆。

在计划新的重新平衡操作之前，必须取消之前计划的全部任务。

- 您只能重新平衡处于“可用”、“错误”或“正在自定义”状态且没有计划取消或等待取消的虚拟机。
- 最佳实践是不要将链接克隆虚拟机和其他类型的虚拟机混合存储在单一数据存储中。这样，Horizon Composer 就可以重新平衡数据存储中的所有虚拟机。
- 如果您编辑某个池并更改主机或群集以及存储链接克隆的数据存储，则您只能在新选择的主机或群集能够完全访问原始和新数据存储的情况下，才可以重新平衡链接克隆。新群集中的所有主机必须能够访问原始和新数据存储。

例如，您可能会在一个独立的主机上创建一个链接克隆桌面池，并选择一个本地数据存储来存储克隆。如果您编辑该桌面池并选择一个群集和共享数据存储，重新平衡操作将会因为群集中的主机无法访问原始的本地数据存储而失败。

- 在重新平衡操作过程中，您可设置可供用户连接的就绪、已置备虚拟机的最小数量。

重要事项 如果您使用 vSAN 数据存储，只能使用重新平衡操作将桌面池中的所有虚拟机从 vSAN 数据存储迁移到某种其他类型的数据存储，或者反向执行此操作。如果桌面池使用 vSAN 数据存储，vSAN 可提供负载平衡功能并优化整个 ESXi 群集内的资源使用情况。

重新平衡操作后链接克隆磁盘的文件名

重新平衡链接克隆虚拟机后，vCenter Server 会更改移到新数据存储的链接克隆中的 Horizon Composer 永久磁盘和一次性数据磁盘的文件名。

原始文件名标识了磁盘类型。重新命名后的磁盘不包括标识标签。

原始永久磁盘的文件名带有 `user-disk` 标签：`desktop_name-vdm-user-disk-D-ID.vmdk`。

原始一次性数据磁盘的文件名带有 `disposable` 标签：`desktop_name-vdm-disposable-ID.vmdk`。

重新平衡操作将链接克隆移到新数据存储后，vCenter Server 会对这两种类型的磁盘使用相同的文件名语法：`desktop_name_n.vmdk`。

管理 Horizon Composer 永久磁盘

您可以将 Horizon Composer 永久磁盘与链接克隆虚拟机分离，然后将其附加到另一个链接克隆。利用此功能，您可以分开管理用户信息和链接克隆虚拟机。

Horizon Composer 永久磁盘

使用 Horizon Composer，您可以在链接克隆虚拟机中的不同磁盘上配置操作系统数据和用户信息。更新、刷新或重新平衡操作系统数据时，Horizon Composer 会将用户信息保留在永久磁盘上。

Horizon Composer 永久磁盘包含用户设置和其他由用户生成的数据。在创建链接克隆桌面池时会创建永久磁盘。

您可以将永久磁盘与其链接克隆虚拟机分离，并将该磁盘存储在其原始数据存储或其他数据存储中。分离此磁盘后，链接克隆虚拟机随之删除。已分离的永久磁盘不再与任何虚拟机关联。

您可以使用几种方法将分离的永久磁盘连接到其他链接克隆虚拟机。这种灵活性优势具有许多用途：

- 您可以在删除链接克隆时保留用户数据。
- 在员工离开公司后，另一位员工可以访问他的用户数据。
- 拥有多个远程桌面的用户可以将用户数据整合到一个远程桌面上。
- 如果虚拟机在 vCenter Server 中变得不可访问，但永久磁盘完整无缺，您可以导入永久磁盘并使用此磁盘创建一个新的链接克隆。

注 永久磁盘必须重新连接到其创建时所使用的操作系统。例如，无法将永久磁盘与 Windows 7 链接克隆分离，并重新创建永久磁盘或将其附加到 Windows 8 链接克隆。

在 Horizon Console 中分离 Horizon Composer 永久磁盘

从链接克隆虚拟机分离 Horizon Composer 永久磁盘时，将存储该磁盘，但会删除链接克隆。通过分离永久磁盘，您可以存储用户相关信息，并在另一个虚拟机上重新使用这些信息。

步骤

- 1 在 Horizon Console 中，选择**清单 > 永久磁盘**。
- 2 选择要分离的永久磁盘，然后单击**分离**。

3 选择用来存储永久磁盘的位置。

选项	说明
使用当前数据存储	将永久磁盘存储到其当前所在的数据存储。
使用以下数据存储	<p>选择用来存储永久磁盘的新数据存储。单击浏览，然后单击向下箭头，从选择数据存储菜单中选择一个新的数据存储。</p> <p>您可以从筛选结果中选择兼容的非 vSAN 数据存储来存储已分离的永久磁盘。或者，选择显示所有数据存储 (包括本地数据存储)，以查看所有数据存储，包括共享数据存储和 vSAN 数据存储。您无法使用 vSAN 数据存储。</p>

Horizon Composer 永久磁盘保存在数据存储中。链接克隆虚拟机将被删除，并且不会出现在 Horizon Console 中。

在 Horizon Console 中将 Horizon Composer 永久磁盘附加到另一链接克隆

您可以将一个已分离的永久磁盘附加到另一链接克隆虚拟机。附加永久磁盘会使该磁盘中的用户设置和信息可供另一虚拟机的用户使用。

您会将已分离的永久磁盘作为辅助磁盘附加到选定的链接克隆虚拟机上。链接克隆的新用户可以访问该辅助磁盘，也可以访问现有的用户信息和设置。

您不能将非 vSAN 数据存储上存储的永久磁盘附加到 vSAN 数据存储上存储的虚拟机。同样，也不能将 vSAN 数据存储上存储的磁盘附加到非 vSAN 数据存储上存储的虚拟机。Horizon Console 会阻止您选择跨 vSAN 和非 vSAN 数据存储的虚拟机。

如果您将某个永久磁盘附加到没有永久磁盘数据存储的链接克隆桌面池，该永久磁盘的信息会显示在**计算机 (View Composer 详细信息)** 选项卡下方以及该桌面池的**永久磁盘**选项卡上。

前提条件

- 确认选择的虚拟机与之前创建永久磁盘的链接克隆使用相同的操作系统。

步骤

- 1 在 Horizon Console 中，选择**清单 > 永久磁盘**。
- 2 在**已分离**选项卡上，选择永久磁盘并单击**附加**。
- 3 选择一个要附加该永久磁盘的链接克隆虚拟机。
- 4 选择要将该永久磁盘附加到的计算机。
- 5 单击**确定**。

后续步骤

确认链接克隆的用户拥有足够的特权来使用附加的磁盘。例如，如果原始用户对永久磁盘有一定的访问权限，而永久磁盘作为驱动器 D 附加在新的链接克隆上，那么链接克隆的新用户必须对驱动器 D 拥有与原始用户一样的访问权限。

以管理员身份登录链接克隆的客户机操作系统并为新用户分配适当的特权。

在 Horizon Console 中编辑 Horizon Composer 永久磁盘池或用户

如果已从 Horizon 7 中删除了原始桌面池或用户，您可以将分离的 Horizon Composer 永久磁盘分配给新的桌面池或用户。

分离的永久磁盘仍然与其原始桌面池和用户相关联。如果从 Horizon 7 中删除了该桌面池或用户，您将无法使用该永久磁盘重新创建链接克隆虚拟机。

通过编辑桌面池和用户，您可以使用分离的永久磁盘在新桌面池中重新创建虚拟机。该虚拟机会分配给新用户。

您可以选择新桌面池、新用户或同时选择二者。

前提条件

- 确认已从 Horizon 7 中删除了永久磁盘的桌面池或用户。
- 确认新桌面池与创建永久磁盘的桌面池使用相同的操作系统。

步骤

- 1 在 Horizon Console 中，选择**清单 > 永久磁盘**。
- 2 选择已删除了用户或桌面池的永久磁盘，然后单击**编辑**。
- 3 （可选）从列表选择一个链接克隆桌面池。
- 4 （可选）为永久磁盘选择一个用户。

您可以浏览 Active Directory 以查找域和用户名。

后续步骤

使用分离的永久磁盘重新创建链接克隆虚拟机。

在 Horizon Console 中使用分离的永久磁盘重新创建链接克隆

分离 Horizon Composer 永久磁盘时会删除链接克隆。您可以通过从分离的磁盘重新创建链接克隆虚拟机，授予原始用户访问分离的用户设置和信息的权限。

注 如果您在已达到最大大小的桌面池中重新创建链接克隆虚拟机，重新创建的虚拟机仍然会被添加到桌面池中。桌面池的大小会增加，然后又会随着未分配的计算机被删除而减小。

如果某个永久磁盘的原始桌面池或用户已从 Horizon 7 中删除，您可以为该永久磁盘分配一个新的桌面池或用户。请参阅[在 Horizon Console 中编辑 Horizon Composer 永久磁盘池或用户](#)。

如果新虚拟机存储在 vSAN 数据存储上，Horizon 7 将不支持使用存储在非 vSAN 数据存储上的永久磁盘重新创建虚拟机。同样，如果永久磁盘存储在 vSAN 上，Horizon 7 不支持在非 vSAN 上重新创建虚拟机。

要将一个已分离的永久磁盘从非 vSAN 数据存储移动到 vSAN 数据存储，您可以在一个非 vSAN 数据存储上存储的某个虚拟机中重新创建该磁盘，然后将该虚拟机的桌面池重新平衡到一个 vSAN 数据存储。

步骤

- 1 在 Horizon Console 中，选择**清单 > 永久磁盘**。

- 2 在**已分离**选项卡上，选择永久磁盘，然后单击**重新创建计算机**。

您可以选择多个永久磁盘，以便为每个磁盘重新创建一个链接克隆虚拟机。

- 3 单击**确定**。

Horizon 7 将为您选择的每个永久磁盘创建一个链接克隆虚拟机，并且将创建的虚拟机添加到原始桌面池中。

永久磁盘仍然保留在其所在的数据存储中。

在 Horizon Console 中通过从 vSphere 导入永久磁盘来还原链接克隆

当某个链接克隆虚拟机在 Horizon 7 中变得不可访问时，如果该虚拟机配置了 Horizon Composer 永久磁盘，您可以还原该虚拟机。您可以从 vSphere 数据存储向 Horizon 7 中导入永久磁盘。

导入的永久磁盘文件在 Horizon 7 中将作为已分离的永久磁盘。您可以在 Horizon 7 中将该已分离的磁盘附加到现有虚拟机，或者重新创建原始的链接克隆。

步骤

- 1 在 Horizon Console 中，选择**清单 > 永久磁盘**。
- 2 在**已分离**选项卡上，单击**从 vCenter 导入**。
- 3 选择一个 vCenter Server 实例。
- 4 选择磁盘文件所在的数据存储。
- 5 选择一个链接克隆桌面池。

注 选择某个桌面池后，您只能浏览并选择基于该桌面池数据存储的永久磁盘。例如，如果您选择具有 vSAN 数据存储的桌面池，则您将只能浏览并选择 vSAN 数据存储中的永久磁盘。

- 6 选择一个访问组。
- 7 在**永久磁盘文件**文本框中，单击**浏览**，然后单击向下箭头，从**选择数据存储**菜单中选择一个数据存储。
- 8 要导入本地数据存储中的永久磁盘，请选择**显示所有数据存储 (包括本地数据存储)**。
- 9 单击数据存储名称，显示其磁盘存储文件和虚拟机文件。
- 10 选择要导入的永久磁盘文件，然后单击**确定**。
- 11 在**用户**文本框中，单击**浏览**，选择要分配给该虚拟机的用户，然后单击**确定**。
- 12 单击**提交**。

磁盘文件将作为已分离的永久磁盘导入 Horizon 7 中。

后续步骤

要还原链接克隆虚拟机，您可以重新创建原始虚拟机或者将已分离的永久磁盘附加到另一虚拟机。

有关详细信息，请参阅在 [Horizon Console 中使用分离的永久磁盘重新创建链接克隆](#)和在 [Horizon Console 中将 Horizon Composer 永久磁盘附加到另一链接克隆](#)。

在 Horizon Console 中删除已分离的 Horizon Composer 永久磁盘

删除分离的永久磁盘时，您可以从 Horizon 7 中移除该磁盘但将其保留在数据存储中；也可以将其从 Horizon 7 和数据存储中删除。

步骤

- 1 在 Horizon Console 中，选择**清单 > 永久磁盘**。
- 2 在**已分离**选项卡上，选择永久磁盘，然后单击**删除**。
- 3 选择从 Horizon Console 中移除磁盘后，是从数据存储中删除该磁盘，还是将其保留在数据存储中。

选项	说明
仅从 View Manager 中删除	删除后，不能再从 Horizon 7 访问永久磁盘，但该磁盘仍然保留在数据存储中。
从磁盘删除	删除后，永久磁盘将不再存在。

- 4 单击**确定**。

在 Horizon Console 中管理未受管和已注册的计算机

在 Horizon Console 中，您可以移除未受管的计算机，还可以从 Horizon 7 中移除已注册的计算机。

未受管的计算机包括不由 vCenter Server 管理的物理机、RDS 主机和虚拟机。因此，必须在连接服务器实例中注册这些未受管计算机，然后才能将它们添加到桌面池中。

Horizon 7 中有两种类型的已注册计算机：“RDS 主机”和“其他”。未受管的计算机属于“其他”类别。使用未受管的计算机可构成不含 vCenter Server 虚拟机的手动桌面池。

重新配置某个影响未受管计算机的设置时，新设置最多需要 10 分钟才能生效。例如，如果更改池的**断开连接后自动注销**设置，Horizon 7 最多可能需要 10 分钟来重新配置受影响的未受管计算机。

通过 Horizon Console 从桌面池中移除未受管计算机

您可以通过从池中移除未受管计算机来减少桌面池的大小。

步骤

- 1 在 Horizon Console 中，选择**清单 > 计算机**。
- 2 选择**其他**选项卡。
- 3 选择要移除的未受管计算机。
- 4 单击**移除**。
- 5 单击**确定**。

未受管计算机将从池中移除。

在 Horizon Console 中移除已注册的计算机

如果您不打算再次使用某个已注册的计算机，可以从 Horizon 7 中移除该计算机。

移除某个已注册的计算机后，该计算机在 Horizon 7 中将不可用。要使计算机再次可用，您必须重新安装 Horizon Agent。

前提条件

确认任何桌面池中均未使用您要移除的已注册的计算机。

步骤

- 1 在 Horizon Console 中，选择**设置 > 已注册的计算机**。
- 2 单击 **RDS 主机**选项卡。
- 3 选择一个或多个计算机，然后单击**移除**。
您只能选择未被桌面池使用的计算机。
- 4 单击**确定**进行确认。

排除计算机和桌面池的问题

您可以采取多种操作来诊断和修复在创建和使用计算机及桌面池时遇到的问题。

用户在使用 Horizon Client 访问桌面和应用程序时可能会遇到困难。您可以采取故障排除操作来调查问题原因并尝试自行解决问题，也可以从 VMware 技术支持部门获取帮助。

在 Horizon Console 中显示出现问题的计算机

您可以采用列表形式显示 Horizon 7 检测到操作可疑的计算机。

Horizon Console 会显示出现以下问题的计算机：

- 已开机但没有响应。
- 长时间保持置备状态。
- 已就绪但报告中指出不接受连接。
- 在 vCenter Server 中丢失。
- 当前有用户登录控制台，有未经授权的用户登录，或者未从连接服务器实例登录。

步骤

- 1 在 Horizon Console 中，选择**清单 > 计算机**。
- 2 在 **vCenter** 选项卡上，从“计算机”下拉菜单中单击**问题计算机**。

后续步骤

您应当采取的措施取决于 Horizon Console 所报告的计算机问题。

- 如果计算机已开启但没有响应，应重新启动该计算机的虚拟机。如果计算机仍没有响应，则需要验证计算机操作系统是否支持该 Horizon Agent 版本。您可以使用带 -A 选项的 vdmadmin 命令显示 Horizon Agent 版本。有关更多信息，请参阅《View 管理指南》文档。
- 如果计算机长时间保持置备状态，应删除其虚拟机并重新克隆。验证是否有足够的磁盘空间用来置备计算机。
- 如果计算机报告其已经就绪，但不接受连接，请检查防火墙配置，确保显示协议未被阻止。
- 如果 vCenter Server 中缺少某个计算机，请验证是否已在预期的 vCenter Server 上配置该计算机的虚拟机，或者该计算机是否已被移到其他 vCenter Server 上。
- 如果计算机当前有用户登录，但不是在控制台上登录，则必定是远程会话。如果无法联系已登录的用户，则可能需要重新启动虚拟机以强行注销这些用户。

确认桌面池的用户分配

对于专用用户分配，您可以验证分配给虚拟机的用户是否为连接到虚拟桌面的用户。

前提条件

- 确认虚拟机属于专用分配池。在 Horizon Console 中，桌面池分配显示在**桌面池**页面上的**用户分配**列中。
- 确认已授权用户使用该桌面池。

步骤

- 1 在 Horizon Console 中，选择**清单 > 计算机**。
- 2 在 **vCenter** 选项卡中，选择查看已分配的用户或已连接的用户。

选项	说明
已分配的用户	已分配的用户列显示已分配给桌面池的用户。 注 已分配的用户列不会显示浮动桌面池的任何用户。
已连接的用户	已连接的用户列显示已连接到虚拟机的用户。在大多数情况下，如果已分配的用户已连接到桌面，则已连接的用户与已分配的用户相同。在其他情况下，如果某个管理员已连接到虚拟机，则已连接的用户列会显示该管理员。

在 Horizon Console 中重新启动桌面并重置虚拟机

您可以在虚拟桌面上执行重新启动操作，这会执行正常的虚拟机操作系统重新启动。您可以在虚拟机上执行重置操作，而不正常重新启动操作系统，这会执行硬虚拟机电源关闭和打开。

表 10-11. 重置和重新启动功能

池类型	重置功能 (池、计算机、会话和 Horizon Client)	重新启动功能 (池、计算机、会话和 Horizon Client)
完整克隆池（未启用“注销时删除”选项的专用池和浮动池）	重置虚拟机（关闭虚拟机电源和打开虚拟机电源）	重新启动虚拟机（正常操作系统重新启动）
即时克隆池（浮动池）	关闭虚拟机电源 > 删除虚拟机 > 创建新的虚拟机 > 打开电源	正常操作系统关闭 > 删除虚拟机 > 创建新的虚拟机 > 打开电源
发布的桌面池	不适用（不支持）	不适用（不支持）

注 重新启动功能适用于 Horizon Client 4.4 和更高版本。

步骤

- 1 在 Horizon Console 中，选择**清单 > 计算机**。
- 2 在 **vCenter** 选项卡上，选择以重新启动虚拟桌面或重置虚拟机。

选项	说明
重新启动桌面	重新启动虚拟机并正常重新启动操作系统。该操作仅适用于包含 vCenter Server 虚拟机的自动池或手动池。
重置虚拟机	重置虚拟机而不正常重新启动操作系统。该操作仅适用于包含 vCenter Server 虚拟机的自动池或手动池。

- 3 单击**确定**。

在 Horizon Console 中向桌面用户发送消息

有些情况下，您可能需要向当前已登录桌面的用户发送消息。例如，如果您需要对计算机进行维护，可以要求用户临时注销或警告他们服务将会中断。您可向多个用户发送消息。

步骤

- 1 在 Horizon Console 中，单击**清单 > 桌面**。
- 2 单击池 ID，然后单击**会话**选项卡。
- 3 选择一个或多个计算机，然后单击**发送消息**。
- 4 键入消息，选择消息类型，然后单击**确定**。

消息类型可以是**信息**、**警告**或**错误**。

消息将发送至活动会话中选定的所有计算机。

在 Horizon Console 中管理未授权用户的计算机和策略

您可以显示分配给授权已被移除的用户的计算机，还可以显示已应用于未授权用户的策略。

未授权用户可能已永久离开组织，或者您在较长时间内暂停了他们的帐户。尽管为这些用户分配了计算机，但是他们不再有权使用计算机池。

您也可以使用带有 `-O` 或 `-P` 选项的 `vdmadmin` 命令来显示未授权的计算机和策略。有关更多信息，请参阅《Horizon 7 管理指南》文档。

步骤

- 1 在 Horizon Console 中，选择**清单 > 计算机**。
- 2 选择**更多命令 > 查看未授权的计算机**。
- 3 移除未授权用户的计算机分配。
- 4 选择**更多命令 > 查看未授权的计算机**或**更多命令 > 查看未授权的策略**（视情况而定）。
- 5 更改或移除应用于未授权用户的策略。

在 Horizon Console 中创建已发布的桌面和应用程序

11

利用 Horizon 7，您可以创建与场关联的已发布桌面，场是一组 Windows 远程桌面服务 (Remote Desktop Service, RDS) 主机。您还可以通过创建应用程序池，将已发布的应用程序传送给多个用户。应用程序池中的已发布应用程序在 RDS 主机的一个场中运行。

本章讨论了以下主题：

- 在 Horizon Console 中创建场
- 在 Horizon Console 中创建已发布的桌面池
- 在 Horizon Console 中创建应用程序池
- 在 Horizon Console 中管理场
- 在 Horizon Console 中管理应用程序池
- 在 Horizon Console 中管理 RDS 主机
- 在 Horizon Console 中管理已发布的桌面和应用程序会话

在 Horizon Console 中创建场

场是一组 Windows 远程桌面服务 (RDS) 主机。可以创建与场关联的已发布桌面。您还可以通过创建应用程序池，将已发布的应用程序传送给多个用户。应用程序池中的已发布应用程序在 RDS 主机的一个场中运行。

场可以简化在企业中管理 RDS 主机、已发布的桌面和应用程序的任务。您可以创建手动或自动场，以便为不同规模或具有不同桌面或应用程序要求的用户群提供服务。

手动场包含已存在的 RDS 主机。RDS 主机可以是物理机，也可以是虚拟机。在创建场时，您可以手动添加 RDS 主机。

自动场包含作为 vCenter Server 中的即时克隆虚拟机的 RDS 主机。

连接服务器根据您在创建场时指定的参数创建即时克隆虚拟机。即时克隆共享父虚拟机的虚拟磁盘，因此所占用的存储空间要比完整虚拟机少。此外，即时克隆还共享父虚拟机的内存，并且可使用 vmFork 技术进行创建。

创建应用程序池或已发布的桌面池时，必须指定一个（且只能指定一个）场。场中的 RDS 主机可以托管已发布的桌面和/或应用程序。一个场最多可以支持一个已发布的桌面池，但可以支持多个应用程序池。一个场可同时支持这两种类型的池。

有关场的更多信息，请参阅《Horizon 7 管理指南》文档。

用于在 Horizon Console 中创建手动场的工作表

在创建手动场时，您可以配置某些场设置。

表 11-1. 工作表：用于创建手动场的配置设置

设置	说明	在此填写您要指定的值
ID	标识场的唯一名称。	
说明	此场的描述。	
访问组	为场选择访问组，或者将场留在默认的根访问组中。	
默认显示协议	选择 VMware Blast 、 PCoIP 或 Microsoft RDP 。Microsoft RDP 仅适用于桌面池。用于应用程序池的显示协议始终为 VMware Blast 或 PCoIP 。如果选择 Microsoft RDP 并计划使用该场来托管应用程序池，则必须将 允许用户选择协议 设置为 是 。默认设置为 PCoIP 。	
允许用户选择协议	选择 是 或 否 。该设置仅适用于已发布的桌面池。如果选择 是 ，则用户可以在从 Horizon Client 中连接到已发布的桌面时选择显示协议。默认值为 是 。	
预启动会话超时 (仅应用程序)	确定配置为预启动的应用程序保持打开的时间。默认值为 10 分钟 。 如果最终用户未在 Horizon Client 中启动任何应用程序，则在空闲会话超时或预启动会话超时后，应用程序会话将断开连接。 如果要在超时后结束预启动会话，必须将 注销断开的会话 选项设置为 立即 。	
空会话超时 (仅限应用程序)	确定空应用程序会话保持打开的时间。如果应用程序会话中运行的所有应用程序都已关闭，此会话便为空。当会话为打开状态时，用户可更快地打开应用程序。如果将空应用程序会话断开连接或注销，可以节省系统资源。选择 从不 、 立即 ，或者设置分钟数作为超时值。默认值为 在 1 分钟后 。如果您选择 立即 ，会话将在 30 秒内注销或断开连接。 您可以通过在安装 Horizon Agent 的 RDS 主机上编辑注册表项，来进一步缩短会话注销或断开连接的时间。导航到 HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wssm\applaunchmgr\Params 并设置 WindowCheckInterval 的值。默认值为 20000。这表示每 20 秒轮询一次空会话检查，也就是从最后一个应用程序关闭到会话注销之间的最长时间设置为 40 秒。您可以将此值更改为 2500。这表示每 2.5 秒轮询一次空会话检查，也就是从最后一个应用程序关闭到会话注销之间的最长时间设置为 5 秒。	
发生超时	确定在达到 空会话超时 限制后将空应用程序会话断开连接还是注销。选择 断开连接 或 注销 。会话注销可以释放资源，但打开应用程序将花费更长的时间。默认值为 断开连接 。	
注销断开的会话	确定何时注销断开连接的会话。此设置同时应用于桌面会话和应用程序会话。选择 从不 、 立即 或 …分钟之后 。选择 立即 或 …分钟之后 ，请慎重考虑。注销断开连接的会话时，该会话将丢失。默认值为 从不 。	
允许 HTML Access 访问此场上的桌面和应用程序	确定是否允许 HTML Access 访问已发布的桌面和应用程序。选中 已启用 复选框将允许 HTML Access 访问已发布的桌面和应用程序。在创建场后编辑该设置时，新值将应用于现有的和新的桌面以及应用程序。	
允许会话协作	选择 已启用 将允许基于此场的桌面池用户邀请其他用户加入其远程桌面会话。会话所有者和协作者必须使用 VMware Blast 协议。	

在 Horizon Console 中创建手动场

可以在授权用户访问已发布的应用程序或桌面的过程中创建手动场。

前提条件

- 设置属于场的 RDS 主机。请参阅《在 Horizon 7 中设置已发布的桌面和应用程序》文档中的“设置远程桌面服务主机”。
- 确认所有 RDS 主机均为“可用”状态。在 Horizon Console 中，选择 **设置 > 已注册的计算机**，并在“RDS 主机”选项卡上检查每个 RDS 主机的状态。
- 收集创建场时必须提供的配置信息。请参阅[用于在 Horizon Console 中创建手动场的工作表](#)。

步骤

- 1 在 Horizon Console 中，选择 **清单 > 场**。
- 2 单击 **添加**。
- 3 选择 **手动场**。
- 4 按照向导中的提示创建场。

使用您在工作表中收集的配置信息。您可以通过在导航窗格中单击页面名称，直接返回至任意向导页面。

- 5 选择要添加到场的 RDS 主机，然后单击 **下一步**。
- 6 单击 **完成**。

后续步骤

创建已发布的应用程序或桌面池。

用于在 Horizon Console 中创建自动即时克隆场的工作表

在创建自动即时克隆场时，您可以配置某些设置。

表 11-2. 工作表：用于创建自动即时克隆场的配置设置

设置	说明	在此填写您要指定的值
ID	标识场的唯一名称。	
说明	此场的描述。	
访问组	为场选择访问组，或者将场留在默认的根本访问组中。	
默认显示协议	选择 VMware Blast 、 PCoIP 或 Microsoft RDP 。Microsoft RDP 仅适用于桌面池。用于应用程序池的显示协议始终为 VMware Blast 或 PCoIP 。如果选择 Microsoft RDP 并计划使用该场来托管应用程序池，则必须将 允许用户选择协议 设置为 是 。默认设置为 PCoIP 。	
允许用户选择协议	选择 是 或 否 。该设置仅适用于已发布的桌面池。如果选择 是 ，则用户可以在从 Horizon Client 中连接到已发布的桌面时选择显示协议。默认值为 是 。	

设置	说明	在此填写您要指定的值
3D 呈现器	<p>为桌面选择 3D 图形呈现。</p> <p>在虚拟硬件版本为 11 或更高版本的虚拟机上运行的 Windows 2008、Windows 2012 和 Windows 2016 客户机上支持 3D 呈现。在 vSphere 6.0 U1 及更高版本环境中的虚拟硬件版本 11 及更高版本（最低）上支持基于硬件的呈现器。在 vSphere 6.0 U1 及更高版本环境中的虚拟硬件版本 11（最低）上支持软件呈现器。</p> <p>在 ESXi 5.0 主机上，呈现器允许使用的最大 VRAM 大小为 128MB。在 ESXi 5.1 和更高版本的主机上，最大 VRAM 大小为 512MB。在 vSphere 6.0 中的硬件版本 11 (HWv11) 虚拟机上，已更改 VRAM 值（显存）。选择“使用 vSphere Client 管理”选项并在 vSphere Web Client 中为这些计算机配置显存。有关详细信息，请参阅《vSphere 虚拟机管理》指南中的“配置 3D 图形”。</p> <p>如果选择 Microsoft RDP 以作为默认显示协议，并且不允许用户选择显示协议，则会禁用 3D 呈现。</p> <ul style="list-style-type: none"> ■ NVIDIA GRID vGPU。已为 NVIDIA GRID vGPU 启用 3D 呈现。虚拟机开启时，ESXi 主机按照先到先得的原则预留 GPU 硬件资源。在选择该选项时，您无法使用 vSphere Distributed Resource Scheduler (DRS)。 <p>要将 NVIDIA GRID vGPU 用于即时克隆桌面池，建议选择 VMware Blast 作为协议，并且不允许用户选择自己的显示协议。</p> <ul style="list-style-type: none"> ■ 使用 vSphere Client 管理。在 vSphere Web Client（或 vSphere 5.1 或更高版本中的 vSphere Client）中为虚拟机设置的“3D 呈现器”选项决定了 3D 图形呈现的类型。Horizon 7 不会控制 3D 呈现。在 vSphere Web Client 中，可配置自动、软件或硬件选项。这些选项与在 Horizon Console 中设置它们时的效果相同。在配置 vDGA 和采用 vDGA 的 AMD 多用户 GPU 时使用此设置。此设置也是 vSGA 的一个选项。选择使用 vSphere Client 管理选项时，为3D 客户机配置虚拟 RAM、显示器最大数量和任意一台显示器的最大分辨率设置在 Horizon Console 中无效。可以在 vSphere Web Client 中配置内存量。 ■ 已禁用。3D 呈现无效。默认值为“已禁用”。 	
预启动会话超时 (仅应用程序)	<p>确定配置为预启动的应用程序保持打开的时间。默认值为 10 分钟。</p> <p>如果最终用户未在 Horizon Client 中启动任何应用程序，则在空闲会话超时或预启动会话超时后，应用程序会话将断开连接。</p> <p>如果要在超时后结束预启动会话，必须将注销断开的会话选项设置为立即。</p>	
空会话超时 (仅限应用程序)	<p>确定空应用程序会话保持打开的时间。如果应用程序会话中运行的所有应用程序都已关闭，此会话便为空。当会话为打开状态时，用户可更快地打开应用程序。如果将空应用程序会话断开连接或注销，可以节省系统资源。选择从不、立即，或者设置分钟数作为超时值。默认值为在 1 分钟后。如果您选择立即，会话将在 30 秒内注销或断开连接。</p> <p>您可以通过在安装 Horizon Agent 的 RDS 主机上编辑注册表项，来进一步缩短会话注销或断开连接的时间。导航到 HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wssm\applaunchmgr\Params 并设置 WindowCheckInterval 的值。默认值为 20000。这表示每 20 秒轮询一次空会话检查，也就是将从最后一个应用程序关闭到会话注销之间的最长时间设置为 40 秒。您可以将此值更改为 2500。这表示每 2.5 秒轮询一次空会话检查，也就是将从最后一个应用程序关闭到会话注销之间的最长时间设置为 5 秒。</p>	
发生超时	<p>确定在达到空会话超时限制后将空应用程序会话断开连接还是注销。选择断开连接或注销。会话注销可以释放资源，但打开应用程序将花费更长的时间。默认值为断开连接。</p>	

设置	说明	在此填写您要指定的值
注销断开的会话	确定何时注销断开连接的会话。此设置同时应用于桌面会话和应用程序会话。选择 从不 、 立即 或 …分钟之后 。选择 立即 或 …分钟之后 ，请慎重考虑。注销断开连接的会话时，该会话将丢失。默认值为 从不 。	
允许 HTML Access 访问此场上的桌面和应用程序	确定是否允许 HTML Access 访问已发布的桌面和应用程序。选中 已启用 复选框将允许 HTML Access 访问已发布的桌面和应用程序。在创建场后编辑该设置时，新值将应用于现有的和新的桌面以及应用程序。	
允许会话协作	选择 已启用 将允许基于此场的桌面池用户邀请其他用户加入其远程桌面会话。会话所有者和会话协作者必须使用 VMware Blast 显示协议。	
每个 RDS 服务器的最大会话数	确定 RDS 主机可以支持的最大会话数。选择 不受限制 或 不超过… 。默认值是 不受限制 。	
启用置备	选中该复选框以在完成此向导后启用置备。默认情况下选中该框。	
出现错误时停止置备	选中该复选框以在出现置备错误时停止置备。默认情况下选中该框。	
命名模式	指定前缀或名称格式。Horizon 7 将附加或插入自动生成的编号以组成计算机名称，从 1 开始。如果要编号放在末尾，则只需指定前缀。否则，在字符串中的任意位置指定 {n}，{n} 将替换为编号。您还可以指定 {n:fixed=<number of digits>}，其中 fixed=<number of digits> 指示编号使用的位数。例如，指定 vm-{n:fixed=3}-sales，则计算机名称是 vm-001-sales、vm-002-sales，依此类推。 注 每个计算机名称（包括自动生成的编号）具有 15 个字符限制。	
计算机的最大数量	要置备的计算机数。	
即时克隆维护操作期间就绪 (已置备) 计算机的最小数量	通过使用该设置，在连接服务器对场中的计算机执行维护操作时，您可以保留指定数量的计算机以接受连接请求。如果您计划即时维护，则不会使用该设置。	
使用 VMware vSAN	指定是否使用 VMware vSAN（如果可用）。vSAN 是一个软件定义的存储层，可以虚拟化在 ESXi 主机的群集上可用的本地物理存储磁盘。	
为副本磁盘和操作系统磁盘选择单独的数据存储	（仅在不使用 vSAN 时有效）出于性能或其他原因，您可以将副本和操作系统磁盘放在不同的数据存储中。 如果选择此选项，您可以通过选择相应的选项来选择一个或多个即时克隆数据存储或副本磁盘数据存储。	
父虚拟机	从列表中选择一个父虚拟机。请注意，该列表包括未安装 View Composer Agent 的虚拟机。您不能选择其中的任何虚拟机，因为需要使用 View Composer Agent。最佳做法是使用指示虚拟机是否安装了 View Composer Agent 的命名约定。	
快照	选择要用作场的基础映像的父虚拟机快照。 不要删除 vCenter Server 中的快照和父虚拟机，除非场中的即时克隆不使用该默认映像，并且不会根据该默认映像创建更多即时克隆。系统需要使用父虚拟机和快照根据场策略在场中置备新的即时克隆。连接服务器维护操作也需要父虚拟机和快照。	
虚拟机文件夹位置	选择场所在的 vCenter Server 文件夹。	

设置	说明	在此填写您要指定的值
群集	<p>选择要用来运行桌面虚拟机的 ESXi 主机或群集。</p> <p>使用 vSAN 数据存储 (vSphere 5.5 Update 1 的一项功能)，可以选择最多包含 20 个 ESXi 主机的群集。使用虚拟卷数据存储 (vSphere 6.0 的一项功能)，可以选择最多包含 32 个 ESXi 主机的群集。</p> <p>在 vSphere 5.1 或更高版本中，如果副本存储在 VMFS5 或更高版本的数据存储中或 NFS 数据存储中，您就可选择最多含有 32 个 ESXi 主机的群集。如果您将副本磁盘存储在 VMFS5 之前的版本中，群集最多可包含 8 台主机。</p> <p>在 vSphere 5.0 中，如果副本存储于 NFS 数据存储中，则可选择包含八台以上 ESXi 主机的群集。如果您在 VMFS 数据存储中存储副本，则一个群集最多包含八台主机。</p>	
资源池	选择场所在的 vCenter Server 资源池。	
数据存储	<p>选择一个或多个要在其中存储场的数据存储。</p> <p>“添加场”向导的选择即时克隆数据存储页面上的表格简要说明了估算场的存储要求的准则。这些准则可帮助您确定哪些数据存储有足够大的空间来存储即时克隆。“存储过载”值始终设置为“无限制”，且无法进行配置。</p> <p>注 如果使用 vSAN，只能选择一个数据存储。</p>	
副本磁盘数据存储	<p>选择一个或多个要在其中存储即时克隆的副本磁盘数据存储。如果您为副本磁盘和操作系统磁盘选择不同的数据存储，则会显示此选项。</p> <p>“添加场”向导的选择副本磁盘数据存储页面上的表格简要说明了估算场的存储要求的准则。这些准则可帮助您确定哪些副本磁盘数据存储有足够大的空间来存储即时克隆。</p>	
网络	<p>选择要用于自动即时克隆场的网络。您可以选择多个 vLAN 网络来创建较大的即时克隆桌面池。默认设置将使用当前父虚拟机映像中的网络。</p> <p>选择网络向导中的表格提供了可使用的网络、端口和端口绑定。要使用多个网络，必须取消选择使用当前父虚拟机中的网络，然后选择要用于即时克隆场的网络。</p>	
域	<p>选择 Active Directory 域和用户名。</p> <p>连接服务器需要具有场的特定用户特权。ClonePrep 使用域和用户帐户来自定义即时克隆计算机。</p> <p>当您为 vCenter Server 配置连接服务器设置时，应指定此用户。配置连接服务器设置时，可以指定多个域和用户。在使用添加场向导创建场时，必须从列表表中选择一个域和用户。</p>	
AD 容器	<p>提供 Active Directory 容器的相对标识名。</p> <p>例如：CN=Computers</p> <p>在运行添加场向导时，可以浏览 Active Directory 树以找到所需的容器。可以剪切、复制或粘贴容器名称。</p>	
允许重新使用已存在的计算机帐户	<p>选择此选项可在新即时克隆的虚拟机名称与 Active Directory 中的现有计算机帐户名称匹配时，使用现有计算机帐户。</p> <p>创建即时克隆时，如果现有 AD 计算机帐户名称与即时克隆虚拟机名称匹配，Horizon 7 会使用现有计算机帐户。否则，需创建新的计算机帐户。</p> <p>现有计算机帐户必须位于您通过 AD 容器设置指定的 Active Directory 容器中。</p> <p>如果禁用此选项，则在 Horizon 7 创建即时克隆时，将创建一个新的 AD 计算机帐户。默认情况下禁用此选项。</p>	

设置	说明	在此填写您要指定的值
使用 ClonePrep	<p>提供 ClonePrep 自定义规范以自定义虚拟机。</p> <ul style="list-style-type: none"> ■ 关机脚本名称。在即时克隆计算机关机前，ClonePrep 在这些计算机上运行的自定义脚本的名称。需提供该脚本在父虚拟机中的路径。 ■ 关机脚本参数。提供在即时克隆计算机关机前，ClonePrep 可用来在这些计算机上运行自定义脚本的参数。例如，使用 p1。 ■ 同步后脚本名称。在创建即时克隆计算机或将映像推送到即时克隆计算机后，ClonePrep 在这些计算机上运行的自定义脚本的名称。需提供该脚本在父虚拟机中的路径。 ■ 同步后脚本参数。提供在创建即时克隆计算机或将映像推送到即时克隆计算机后，ClonePrep 在这些计算机上运行的脚本的参数。例如，使用 p2。 	
即将完成	查看自动即时克隆场的设置。	

在 Horizon Console 中创建自动即时克隆场

可以在授权用户访问已发布的应用程序或桌面的过程中创建自动即时克隆场。

前提条件

- 确认安装了连接服务器。请参阅《Horizon 7 安装指南》文档。
- 确认在 Horizon Administrator 中配置了适用于 vCenter Server 的连接服务器设置。请参阅《Horizon 7 管理指南》文档。
- 确认用于虚拟机（用作远程桌面）的 ESXi 虚拟交换机上的端口数量充足。如果要创建大型桌面池，默认值可能不足以满足要求。
- 确认已准备好父虚拟机。必须在该父虚拟机上安装 Horizon Agent。请参阅《在 Horizon 7 中设置已发布的桌面和应用程序》文档中的“为自动场准备父虚拟机”。
- 在 vCenter Server 中为父虚拟机拍摄一个快照。为父虚拟机拍摄快照之前必须将其关闭。连接服务器将使用该快照作为创建克隆所用的基础映像。
- 收集创建场时必须提供的配置信息。请参阅[用于在 Horizon Console 中创建自动即时克隆场的工作表](#)。

步骤

- 1 在 Horizon Console 中，选择**清单 > 场**。
- 2 单击**添加**。
- 3 选择**自动场**。
- 4 选择**即时克隆**。
- 5 按照向导中的提示创建场。

使用您在工作表中收集的配置信息。通过在导航面板中单击页面名称，您可以直接返回至已完成的任意向导页面。

后续步骤

创建已发布的应用程序池或已发布的桌面池。请参阅在 [Horizon Console 中创建已发布的桌面池](#)或在 [Horizon Console 中创建应用程序池](#)。

用于在 Horizon Console 中创建自动链接克隆场的工作表

在创建自动链接克隆场时，您可以配置某些设置。

表 11-3. 工作表：用于创建自动链接克隆场的配置设置

设置	说明	在此填写您要指定的值
ID	用于在 Horizon Console 中标识场的唯一名称。	
描述	此场的描述。	
访问组	要在其中放置此场中所有池的访问组。 有关访问组的更多信息，请参阅《Horizon 7 管理指南》文档中的基于角色的委派管理一章。	
默认显示协议	选择 VMware Blast 、 PCoIP 或 RDP 。RDP 仅适用于桌面池。用于应用程序池的显示协议始终为 VMware Blast 或 PCoIP 。如果选择 RDP 并计划使用该场来托管应用程序池，则必须将 允许用户选择协议 设置为 是 。默认设置为 PCoIP 。	
允许用户选择协议	选择 是 或 否 。该设置仅适用于 RDS 桌面池。如果选择 是 ，则用户可以在从 Horizon Client 中连接到 RDS 桌面时选择显示协议。默认值为 是 。	
预启动会话超时 (仅应用程序)	确定配置为预启动的应用程序保持打开的时间。默认值为 10 分钟 。 如果最终用户未在 Horizon Client 中启动任何应用程序，则在空闲会话超时或预启动会话超时后，应用程序会话将断开连接。 如果要在超时后结束预启动会话，必须将 注销断开的会话 选项设置为 立即 。	
空会话超时 (仅限应用程序)	确定空应用程序会话保持打开的时间。如果应用程序会话中运行的所有应用程序都已关闭，此会话便为空。当会话为打开状态时，用户可更快地打开应用程序。如果将空应用程序会话断开连接或注销，可以节省系统资源。选择 从不 、 立即 ，或者设置分钟数作为超时值。默认值为 在 1 分钟后 。如果您选择 立即 ，会话将在 30 秒内注销或断开连接。 您可以通过在安装 Horizon Agent 的 RDS 主机上编辑注册表项，来进一步缩短会话注销或断开连接的时间。导航到 HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wssm\applaunchmgr\Params 并设置 WindowCheckInterval 的值。默认值为 20000。这表示每 20 秒轮询一次空会话检查，也就是将从最后一个应用程序关闭到会话注销之间的最长时间设置为 40 秒。您可以将此值更改为 2500。这表示每 2.5 秒轮询一次空会话检查，也就是将从最后一个应用程序关闭到会话注销之间的最长时间设置为 5 秒。	
发生超时	确定在达到 空会话超时 限制后将空应用程序会话断开连接还是注销。选择 断开连接 或 注销 。会话注销可以释放资源，但打开应用程序将花费更长的时间。默认值为 断开连接 。	
注销断开的会话	确定何时注销断开连接的会话。此设置同时应用于桌面会话和应用程序会话。选择 从不 、 立即 或 …分钟之后 。选择 立即 或 …分钟之后 ，请慎重考虑。注销断开连接的会话时，该会话将丢失。默认值为 从不 。	

设置	说明	在此填写您要指定的值
允许 HTML Access 访问此场上的桌面和应用程序	确定是否允许 HTML Access 访问 RDS 桌面和应用程序。选中 已启用 复选框将允许 HTML Access 访问 RDS 桌面和应用程序。在创建场后编辑该设置时，新值将应用于现有的和新的桌面以及应用程序。	
允许会话协作	选择 已启用 将允许基于此场的桌面池用户邀请其他用户加入其远程桌面会话。会话所有者和会话协作者必须使用 VMware Blast 协议。	
每个 RDS 服务器的最大会话数	确定 RDS 主机可以支持的最大会话数。选择 不受限制 或 不超过... 。默认值是 不受限制 。	
启用置备	选中该复选框以在完成此向导后启用置备。默认情况下选中该框。	
出现错误时停止置备	选中该复选框以在出现置备错误时停止置备。默认情况下选中该框。	
命名模式	<p>指定前缀或名称格式。Horizon 7 将附加或插入自动生成的编号以组成计算机名称，从 1 开始。如果要编号放在末尾，则只需指定前缀。否则，在字符串中的任意位置指定 {n}，{n} 将替换为编号。您还可以指定 {n:fixed=<number of digits>}，其中 fixed=<number of digits> 指示编号使用的位数。例如，指定 vm-{n:fixed=3}-sales，则计算机名称是 vm-001-sales、vm-002-sales，依此类推。</p> <p>注 每个计算机名称（包括自动生成的编号）具有 15 个字符限制。</p>	
计算机的最大数量	要置备的计算机数。	
View Composer 维护操作期间就绪 (已置备) 计算机的最小数量	通过使用该设置，在 View Composer 重构场中的计算机时，您可以保留指定数量的计算机以接受连接请求。	
使用 VMware vSAN	指定是否使用 VMware vSAN（如果可用）。vSAN 是一个软件定义的存储层，可以虚拟化在 ESXi 主机的群集上可用的本地物理存储磁盘。有关更多信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“使用 vSAN 实现高性能存储和基于策略的管理”。	
为副本磁盘和操作系统磁盘选择单独的数据存储	（仅在不使用 vSAN 时有效）出于性能或其他原因，您可以将副本和操作系统磁盘放在不同的数据存储中。	
父虚拟机	从列表中选择父虚拟机。请注意，该列表包括未安装 View Composer Agent 的虚拟机。您不能选择其中的任何虚拟机，因为需要使用 View Composer Agent。最佳做法是使用指示虚拟机是否安装了 View Composer Agent 的命名约定。	
快照	<p>选择要用作场的基础映像的父虚拟机快照。</p> <p>不要删除 vCenter Server 中的快照和父虚拟机，除非场中的链接克隆不使用该默认映像，并且不会根据该默认映像创建链接克隆。系统需要使用父虚拟机和快照根据场策略在场中置备新的链接克隆。View Composer 维护操作也需要父虚拟机和快照。</p>	
虚拟机文件夹位置	选择场所在的 vCenter Server 文件夹。	

设置	说明	在此填写您要指定的值
群集	<p>选择要用来运行桌面虚拟机的 ESXi 主机或群集。</p> <p>使用 vSAN 数据存储 (vSphere 5.5 Update 1 的一项功能)，可以选择最多包含 20 个 ESXi 主机的群集。使用虚拟卷数据存储 (vSphere 6.0 的一项功能)，可以选择最多包含 32 个 ESXi 主机的群集。</p> <p>在 vSphere 5.1 或更高版本中，如果副本存储在 VMFS5 或更高版本的数据存储中或 NFS 数据存储中，您就可选择最多含有 32 个 ESXi 主机的群集。如果您将副本磁盘存储在 VMFS5 之前的版本中，群集最多可包含 8 台主机。</p> <p>在 vSphere 5.0 中，如果副本存储于 NFS 数据存储中，则可选择包含八台以上 ESXi 主机的群集。如果您在 VMFS 数据存储中存储副本，则一个群集最多包含八台主机。</p>	
资源池	选择场所在的 vCenter Server 资源池。	
数据存储	<p>选择一个或多个要在其中存储场的数据存储。</p> <p>“添加场”向导中的 选择链接克隆数据存储 页上的一个表简要说明了估算场的存储要求的准则。这些信息能帮助您确定哪个数据存储有足够空间存储链接克隆磁盘。有关详细信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“确定即时克隆和链接克隆桌面池的存储大小”。</p> <p>您可将共享数据存储或本地数据存储用于单个的 ESXi 主机或 ESXi 群集。如果您在 ESXi 群集中使用本地数据存储，则您必须考虑桌面部署的 vSphere 基础架构限制。有关详细信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“在本地数据存储上存储链接克隆”。</p> <p>注 如果使用 vSAN，只能选择一个数据存储。</p>	
存储过载	<p>确定在每个数据存储上创建链接克隆时的存储过载级别。</p> <p>随着级别的增加，数据存储上装载的链接克隆会越来越多，而为单个克隆的增长所保留的空间则越来越少。如果设置较高的存储过载级别，您创建的链接克隆的总逻辑大小就可以大于数据存储的物理存储限制。有关详细信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“View Composer 链接克隆虚拟机的存储过载”。</p> <p>注 如果使用 vSAN，则该设置无效。</p>	
使用本地 NFS 快照 (VAAI)	<p>(仅在不使用 vSAN 时有效) 如果部署中包含支持 vStorage APIs for Array Integration (VAAI) 的 NAS 设备，则可以使用本地快照技术克隆虚拟机。</p> <p>仅当您选择了位于通过 VAAI 支持本地克隆操作的 NAS 设备上的数据存储时，才可以使用此功能。</p> <p>如果您将副本磁盘和操作系统磁盘存储在单独的数据存储中，则无法使用这些功能。无法在包含能节省空间的磁盘的虚拟机上使用此功能。</p> <p>vSphere 5.0 及更高版本支持此功能。</p> <p>有关详细信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“将 VAAI 存储用于 View Composer 链接克隆”。</p>	
回收虚拟机磁盘空间	<p>(仅在不使用 vSAN 或虚拟卷时有效) 确定是否允许 ESXi 主机回收以节省空间的磁盘格式创建的链接克隆上的未用磁盘空间。空间回收功能减少了链接克隆桌面所需的总存储空间。</p> <p>vSphere 5.1 及更高版本支持此功能。链接克隆虚拟机必须是虚拟硬件版本 9 或更高版本。</p> <p>有关详细信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“回收链接克隆虚拟机上的磁盘空间”。</p>	

设置	说明	在此填写您要指定的值
在虚拟机上的未使用空间超出以下值时启动回收：	<p>（仅在不使用 vSAN 或虚拟卷时有效）键入必须在链接克隆操作系统磁盘上累积从而触发空间回收的未用磁盘空间的最小数量（千兆字节）。当未使用的磁盘空间超过此阈值时，Horizon 7 将启动操作，指示 ESXi 主机回收操作系统磁盘上的空间。</p> <p>此值根据虚拟机而测得。未使用的磁盘空间必须超过单个虚拟机上指定的阈值，然后 Horizon 7 才会开始对该计算机执行空间回收过程。</p> <p>例如：2 GB。</p> <p>默认值为 1 GB。</p>	
中断时间	<p>配置不进行虚拟机磁盘空间回收操作的日期和时间。</p> <p>为了确保必要时 ESXi 资源专供前台任务使用，您可以在指定日期的指定时段内禁止 ESXi 主机执行这些操作。</p> <p>有关详细信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“为 View Composer 链接克隆设置 Storage Accelerator 和空间回收中断时间”。</p>	
透明页面共享范围	<p>选择允许透明页面共享 (TPS) 的级别。选项包括：虚拟机（默认）、场、容器或全局。如果在场、容器或全局级别为所有计算机启用 TPS，ESXi 主机将消除因这些计算机使用同一客户机操作系统或应用程序而产生的内存冗余副本。</p> <p>页面共享发生在 ESXi 主机上。例如，如果在场级别启用 TPS，但场分散到多个 ESXi 主机，则仅相同主机和相同场中的虚拟机共享页面。在全局级别，同一 ESXi 主机上所有受 Horizon 7 管理的计算机都可以共享内存页，而不管这些计算机驻留在哪个场中。</p> <p>注 默认设置是不在计算机之间共享内存页，因为 TPS 可能会带来安全风险。调查表明可能会在非常有限的配置场景下滥用 TPS 来获取对数据的未授权访问。</p>	
域	<p>选择 Active Directory 域和用户名。</p> <p>View Composer 需要具有场的特定用户权限。Sysprep 使用域和用户帐户来自定义链接克隆计算机。</p> <p>当您为 vCenter Server 配置 View Composer 设置时，应指定此用户。配置 View Composer 设置时，可以指定多个域和用户。在使用添加场向导创建场时，必须从列表中选择一个域和用户。</p> <p>有关配置 View Composer 的信息，请参阅《Horizon 7 管理指南》文档。</p>	
AD 容器	<p>提供 Active Directory 容器的相对标识名。</p> <p>例如：CN=Computers</p> <p>在运行添加场向导时，可以浏览 Active Directory 树以找到所需的容器。</p>	

设置	说明	在此填写您要指定的值
允许重新使用已存在的计算机帐户	<p>选择该设置以将 Active Directory 中的现有计算机帐户用于 View Composer 置备的链接克隆。该设置允许您控制在 Active Directory 中创建的计算机帐户。</p> <p>置备链接克隆后，如果现有 AD 计算机帐户名与链接克隆计算机名匹配，则 View Composer 会使用现有的计算机帐户。否则，需创建新的计算机帐户。</p> <p>现有的计算机帐户必须位于您通过 Active Directory 容器 设置而指定的 Active Directory 容器中。</p> <p>如果禁用该设置，在 View Composer 置备链接克隆时，将创建新的 AD 计算机帐户。默认情况下禁用此设置。</p> <p>有关详细信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“针对链接克隆使用现有的 Active Directory 计算机帐户”。</p>	
使用自定义规范 (Sysprep)	提供 Sysprep 自定义规范以自定义虚拟机。	

在 Horizon Console 中创建自动链接克隆场

可以在授权用户访问已发布的应用程序或已发布的桌面的过程中创建自动链接克隆场。

前提条件

- 确认安装了 **View Composer** 服务。请参阅《**Horizon 7** 安装指南》文档。
- 确认配置了适用于 **vCenter Server** 的 **View Composer** 设置。请参阅《**Horizon 7** 管理指南》文档。
- 确认用于虚拟机（用作远程桌面）的 **ESXi** 虚拟交换机上的端口数量充足。如果要创建大型桌面池，默认值可能不足以满足要求。**ESXi** 主机上的虚拟交换机端口的数量必须大于或等于虚拟机数量与每个虚拟机的虚拟网卡数量的乘积。
- 确认已准备好父虚拟机。必须在该父虚拟机上安装 **Horizon Agent** 和 **View Composer Agent**。请参阅《**Horizon 7** 管理指南》文档。
- 在 **vCenter Server** 中为父虚拟机拍摄一个快照。为父虚拟机拍摄快照之前必须将其关闭。**View Composer** 将使用该快照作为基础映像来创建克隆。

注 您不能从虚拟机模板创建链接克隆场。

- 收集创建场时必须提供的配置信息。请参阅[用于在 Horizon Console 中创建自动链接克隆场的工作表](#)。

步骤

- 1 在 **Horizon Console** 中，选择**清单 > 场**。
- 2 单击**添加**。
- 3 选择**自动场**。
- 4 选择 **View Composer** **链接克隆**。
- 5 按照向导中的提示创建场。

使用您在工作表中收集的配置信息。通过在导航面板中单击页面名称，您可以直接返回至已完成的任意向导页面。

此时，您可以在 Horizon Console 中单击**清单 > 场**以查看该场。

后续步骤

创建已发布的应用程序池或已发布的桌面池。请参阅[在 Horizon Console 中创建已发布的桌面池](#)或在[Horizon Console 中创建应用程序池](#)。

在 Horizon Console 中创建已发布的桌面池

为授予用户远程访问基于会话的桌面的权限，需要执行的任务之一是创建一个已发布的桌面池。已发布的桌面池在 RDS 主机场上运行，所具备的属性能够满足远程桌面部署的某些特定要求。

有关已发布的桌面池的属性的更多信息，请参阅《在 Horizon 7 中设置已发布的桌面和应用程序》文档。

用于创建已发布桌面池的工作表

创建将在 RDS 主机的场上运行的已发布桌面池时，可以指定特定的池设置。并非所有池设置都适用于所有类型的桌面池。这些设置特定于已发布的桌面池。

表 11-4. 已发布桌面池的设置

设置	说明	默认值
状态	<ul style="list-style-type: none"> ■ 已启用。桌面池创建后将自动启用，并可以立即投入使用。 ■ 已禁用。桌面池在创建完成后将被禁用且无法使用，池的置备也将停止。如果要执行部署后的活动，如测试或其他形式的基准维护，则该设置很适用。 <p>当此状态生效时，远程桌面不可用。</p>	已启用
连接服务器限制	<p>您可以限制只有特定连接服务器才能访问桌面池，方法是：单击浏览，然后选择一个或多个连接服务器。</p> <p>如果您想通过 VMware Identity Manager 提供桌面访问权限，并且配置了连接服务器限制，则当桌面实际受到限制时，VMware Identity Manager 应用程序可能会向用户显示这些桌面。VMware Identity Manager 用户将无法启动这些桌面。</p>	无
类别文件夹	为包含 Windows 客户端设备上桌面池授权的“开始”菜单快捷方式的类别文件夹指定名称。	已禁用
客户端限制	<p>选择是否限制只能从特定客户端计算机访问授权的桌面池。</p> <p>您必须在 Active Directory 安全组中添加可访问桌面池的计算机名称。将用户或组添加到桌面池授权时，您可以选择此安全组。</p>	已禁用

在 Horizon Console 中创建已发布的桌面池

在授权用户访问在 RDS 主机场上运行的桌面的过程中，可以创建已发布的桌面池。

前提条件

- 设置 RDS 主机。请参阅《在 Horizon 7 中设置已发布的桌面和应用程序》文档中的“设置远程桌面服务主机”。
- 创建包含 RDS 主机的场。请参阅[在 Horizon Console 中创建场](#)。
- 确定如何配置池设置。请参阅《在 Horizon 7 中设置已发布的桌面和应用程序》文档中的“适用于 RDS 桌面池的桌面池设置”。

步骤

- 1 在 Horizon Console 中，选择**清单 > 桌面**。
- 2 单击**添加**。
- 3 选择 **RDS 桌面池**，然后单击**下一步**。
- 4 提供池 ID、显示名称和描述。

池 ID 是用于在 Horizon Administrator 中标识池的唯一名称。显示名称是用户登录到 Horizon Client 时所看到的 RDS 桌面池的名称。如果您未指定显示名称，该名称将与池 ID 相同。

- 5 选择池设置。
- 6 为该池选择或创建一个场。

后续步骤

授予用户访问池的权限。

在 Horizon Console 中创建应用程序池

为用户提供应用程序的远程访问权限所需执行的一个任务是创建应用程序池。有权访问应用程序池的用户可以从各种客户端设备远程访问该应用程序。

通过应用程序池，您可以将一个应用程序提供给很多用户。该应用程序会在 RDS 主机场或桌面池上运行。

创建应用程序池时，您在用户从任意网络位置均可访问的数据中心内部署应用程序。

一个应用程序池只有一个应用程序，并且只与一个场或桌面池相关联。为了避免出现错误，您必须在场或桌面池中的所有 RDS 主机上安装该应用程序。

当您创建应用程序池时，Horizon 7 会自动显示场或桌面池中所有 RDS 主机的**开始**菜单中可供所有用户（而非个别用户）使用的应用程序。您可以从列表选择一个或多个应用程序。如果您从列表中选择多个应用程序，则会为每个应用程序创建一个单独的应用程序池。您也可以手动指定列表中没有的应用程序。如果要手动指定的应用程序尚未安装，Horizon 7 会显示警告消息。

创建应用程序池时，您无法指定用于放置池的访问组。对于已发布的应用程序池和桌面池，需在创建场或桌面池时指定访问组。

应用程序支持 PCoIP 和 VMware Blast 显示协议。要启用 HTML Access，请参阅《VMware Horizon HTML Access 安装和设置指南》文档。

用于在 Horizon Console 中手动创建应用程序池的工作表

当您创建应用程序池并手动指定应用程序时，您可以添加有关应用程序的信息。并不需要应用程序已安装在任何 RDS 主机上。

表 11-5. 工作表：用于手动创建应用程序池的应用程序属性

属性	说明	在此填写您要指定的值
选择 RDS 场或桌面池	从具有支持的会话类型（“应用程序”或“应用程序和桌面”）的桌面列表中选择一个场或桌面池。	
ID	用于在 Horizon Administrator 中标识池的唯一名称。此字段为必填字段。	
显示名称	用户登录到 Horizon Client 时看到的池名称。如果不指定显示名称，该名称将与 ID 相同。	
版本	应用程序的版本。	
发布者	应用程序的发布者。	
路径	应用程序的完整路径名。例如，C:\Program Files\app1.exe。此字段为必填字段。	
开始文件夹	应用程序的开始目录的完整路径名。	
参数	应用程序启动时传递给应用程序的参数。例如，您可以指定 <code>-username user1 -loglevel 3</code> 。	
说明	对此应用程序池的描述。	
预启动	<p>选择此选项可配置应用程序，以便在用户在 Horizon Client 中打开应用程序之前启动应用程序会话。在启动已发布的应用程序后，可以在 Horizon Client 中更快地打开该应用程序。</p> <p>如果启用此选项，则配置的应用程序会话会在用户在 Horizon Client 中打开应用程序之前启动，而无论用户如何从 Horizon Client 连接到服务器。</p> <p>注 基于桌面池的应用程序不支持此设置。</p> <p>注 如果在添加或编辑应用程序场时设置了预启动会话超时 (仅应用程序) 选项，应用程序会话可能会断开连接。</p>	
连接服务器限制	<p>您可以限制只有特定连接服务器才能访问应用程序池，方法是：单击浏览，然后选择一个或多个连接服务器。</p> <p>如果您想通过 VMware Identity Manager 提供桌面访问权限，并且配置了连接服务器限制，则当桌面实际受到限制时，VMware Identity Manager 应用程序可能会向用户显示这些桌面。VMware Identity Manager 用户将无法启动这些桌面。</p>	

属性	说明	在此填写您要指定的值
类别文件夹	为包含 Windows 客户端设备上应用程序池授权的“开始”菜单快捷方式的类别文件夹指定名称。	

属性	说明	在此填写您要指定的值
客户端限制	<p>选择是否限制只能从特定客户端计算机访问授权的应用程序池。</p> <p>您必须在 Active Directory 安全组中添加可访问应用程序池的计算机名称。将用户或组添加到应用程序池授权时，您可以选择此安全组。</p>	
多会话模式	<p>您可在以下模式下启动已发布的应用程序会话：</p> <p>单会话模式：如果用户在客户端 A 上以单会话模式打开一个已发布的应用程序，然后在客户端 B 上打开同一已发布应用程序或同一场中的另一个已发布应用程序，客户端 A 上的会话会断开连接并在客户端 B 上重新连接。</p> <p>多会话模式：如果用户在客户端 A 上以多会话模式打开一个已发布的应用程序，然后在客户端 B 上打开同一已发布应用程序或同一场中的另一个已发布应用程序，该已发布的应用程序会在客户端 A 上保持打开状态，同时在客户端 B 上打开该已发布应用程序的一个新会话。断开连接时，这些会话会被注销。启用多会话模式时，无法启用会话预启动功能。</p> <p>多会话模式具有以下值：</p> <ul style="list-style-type: none"> ■ 已禁用。不支持多会话模式。 ■ 已启用 (默认关闭)。支持多会话模式，但该模式默认处于禁用状态。要使用多会话模式，用户必须在 Horizon Client 4.10 或更高版本中启用多启动设置。如果用户使用早期版本的 Horizon Client，将始终以单会话模式启动应用程序。 ■ 已启用 (默认打开)。支持多会话模式，且该模式默认处于启用状态。用户可以通过在 Horizon Client 4.10 或更高版本中禁用多启动设置来禁用多会话模式。如果用户使用早期版本的 Horizon Client，将始终以单会话模式启动应用程序。 ■ 已启用 (强制)。多会话模式始终处于启用状态。用户在任何版本的 Horizon Client 中都不能禁用此功能，应用程序始终以多会话模式启动。如果用户使用早期版本的 Horizon Client，会看到以下错误消息：“此应用程序不支持请求的启动模式” (This application does not support the requested launch mode)。 <p>启用多会话模式后，您还可以配置最大会话计数设置。此值设置用户可以从不同客户端设备为同一个已发布应用程序启动的多个并发会话的最大数量。</p> <p>根据多会话模式配置，您可以从客户端同时以单会话模式和多会话模式打开已发布的应用程序。在这种情况下，客户端具有一个单会话和一个多会话。</p> <p>有关使用多启动设置的更多信息，请参阅 Horizon Client 4.10 文档。</p> <p>注 基于桌面池的应用程序不支持此设置。</p>	

在 Horizon Console 中创建应用程序池

您可以在向用户授予对 RDS 主机或桌面池上运行的应用程序的访问权限过程中，创建一个应用程序池。

前提条件

- 设置 RDS 主机。请参阅《在 Horizon 7 中设置已发布的桌面和应用程序》文档中的“设置远程桌面服务主机”。
- 创建包含 RDS 主机的场。请参阅[在 Horizon Console 中创建场](#)。
- 创建手动或自动桌面池。请参阅第 10 章 [在 Horizon Console 中创建虚拟桌面池](#)。
- 如果要手动添加应用程序池，应收集有关该应用程序的信息。请参阅[用于在 Horizon Console 中手动创建应用程序池的工作表](#)

步骤

- 1 在 Horizon Console 中，选择**清单 > 应用程序**。
- 2 单击**添加**。
- 3 按照向导中的提示创建池。

如果选择手动添加应用程序池，可使用工作表中收集的配置信息。如果从 Horizon Console 显示的列表中选择应用程序，可以选择多个应用程序。会为每个应用程序创建一个单独的池。

后续步骤

授予用户访问池的权限。

确保最终用户可以访问 Horizon Client 3.0 或更高版本的软件，以支持已发布的应用程序。

如果您需要确保连接服务器仅在具有足够资源以运行应用程序的 RDS 主机上启动应用程序，请为应用程序池配置一个反关联性规则。

注 对于在桌面池上运行的应用程序，只有通过浮动桌面池（而不是专用桌面池）创建的应用程序支持反关联性规则。

请参阅[在 Horizon Console 中为应用程序池配置反关联性规则](#)。

在 Horizon Console 中为应用程序池配置反关联性规则

为应用程序池配置反关联性规则时，Horizon 连接服务器将尝试仅在具有足够的资源以运行应用程序的 RDS 主机上启动该应用程序。要控制使用大量 CPU 或内存资源的应用程序，该功能可能是非常有用的。

反关联性规则包含应用程序匹配模式和最大计数。例如，应用程序匹配模式可能是 `autocad.exe`，而最大计数可能是 2。

连接服务器将反关联性规则发送到 RDS 主机上的 Horizon Agent。如果在 RDS 主机上运行的任何应用程序的进程名称与应用程序匹配模式相匹配，则 Horizon Agent 会计入这些应用程序的当前实例数，并将该数字与最大计数进行比较。如果超过最大计数，在选择 RDS 主机以运行应用程序的新会话时，连接服务器将跳过该 RDS 主机。

前提条件

- 创建应用程序池。请参阅[在 Horizon Console 中创建应用程序池](#)。
- 熟悉反关联性功能的限制。请参阅[反关联性功能限制](#)。

步骤

- 1 在 Horizon Console 中，选择**清单 > 应用程序**。
- 2 选择要修改的池，然后单击**编辑**。
- 3 在**反关联性模式**文本框中，键入以逗号分隔的模式列表以匹配在 RDS 主机上运行的其他应用程序的进程名称。

模式字符串可以包含星号 (*) 和问号 (?)通配符。星号与零个或多个字符匹配，问号与任何单个字符匹配。

例如，***pad.exe,*notepad.???** 与 wordpad.exe、notepad.exe 和 notepad.bat 匹配，但它与 wordpad.bat 或 notepad.script 不匹配。

注 Horizon 7 将与单个会话中的应用程序匹配的多个模式计为一个匹配项。

- 4 在**反关联性计数**文本框中，键入拒绝在 RDS 主机中运行新的应用程序会话之前可在 RDS 主机上运行的其他应用程序的最大数量。

最大计数可以是 1 到 20 之间的整数。

- 5 单击**提交**以保存更改。

反关联性功能限制

反关联性功能具有某些限制。

- 反关联性规则仅影响新应用程序会话。如果 RDS 主机包含用户以前在其中运行应用程序的会话，将始终重新使用该主机运行相同的应用程序。该行为覆盖报告的负载首选项和反关联性规则。
- 反关联性规则不影响从 RDS 桌面会话中启动应用程序。
- RDS 会话限制禁止创建应用程序会话，而无论使用哪种反关联性规则。
- 在某些情况下，可能不会将 RDS 主机上的应用程序实例限制为指定的最大计数。例如，如果正在启动其他待处理会话的其他应用程序，则 Horizon 7 无法确定确切的实例数。
- 不支持应用程序之间的反关联性规则。例如，无法在单个规则中计算大型应用程序类别，例如，Autocad 和 Visual Studio 实例。
- 对于最终用户在移动客户端上使用 Horizon Client 的环境，请不要使用反关联性规则。反关联性规则可导致在最终用户的同一个场中出现多个会话。如果重新连接到移动客户端上的多个会话，可能会导致不确定的行为。
- 反关联性规则只会为负载平衡考虑已连接会话数。但是，RDS 主机的负载平衡则会为负载平衡考虑已连接会话、待处理会话和断开的会话的总和。

在 Horizon Console 中管理场

在 Horizon Console 中，您可以添加、编辑、删除、启用及禁用场。

创建场之后，您可以添加或移除 RDS 主机以为更多或更少的用户提供支持。

在 Horizon Console 中编辑场

对于现有的场，您可以对配置设置进行更改。

前提条件

熟悉场的设置。

步骤

- 1 在 Horizon Console 中，选择**清单 > 场**。
- 2 选择一个场，然后单击**编辑**。
- 3 更改场的设置。
- 4 单击**确定**。

在 Horizon Console 中删除场

如果您不再需要某个场或要创建拥有不同 RDS 主机的新场，可以删除该场。只能删除未与已发布的桌面池或应用程序池关联的场。

前提条件

确认场未与任何已发布的桌面池或应用程序池关联。

步骤

- 1 在 Horizon Console 中，选择**清单 > 场**。
- 2 选择一个或多个场，然后单击**删除**。
- 3 单击**确定**进行确认。

在 Horizon Console 中禁用或启用场

禁用场后，用户将无法再从与场关联的已发布桌面池和应用程序池中启动已发布的桌面或应用程序。用户可以继续使用当前已打开的已发布桌面和应用程序。

如果计划对某个场中的 RDS 主机或与该场关联的已发布桌面池和应用程序池进行维护，可以禁用该场。禁用场后，某些用户可能仍在使用在禁用场之前已打开的已发布桌面或应用程序。

步骤

- 1 在 Horizon Console 中，选择**清单 > 场**。
- 2 选择一个或多个场，然后单击**更多命令**。
- 3 单击**启用或禁用**。

4 单击**确定**进行确认。

您可以选择**清单 > 桌面**或**清单 > 应用程序**来查看这些池的状态。

在 Horizon Console 中安排自动即时克隆场维护

通过维护操作，您可以对自动即时克隆场中的所有 RDS 主机安排定期或即时维护。在每个维护周期，将刷新父虚拟机中的所有 RDS 主机。

您可以对父虚拟机进行修改，而不会影响 RDS 主机即时克隆，因为维护使用的是当前父虚拟机的快照。在自动场中创建的即时克隆使用父虚拟机的信息进行系统配置。

您可以安排自动场维护，但不能安排场中的各个 RDS 主机的维护。

如果可能的话，安排在非高峰时间执行维护操作，以确保所有 RDS 主机都能完成维护，并在高峰时间投入使用。

前提条件

- 确定计划何时执行维护操作。默认情况下，连接服务器会立即开始执行此操作。
您可以对场安排即时维护或定期维护或同时安排这两项维护。您可以同时安排多个场的维护操作。
- 确定是在开始执行维护操作时强制注销所有用户，还是等到刷新各个用户的计算机时再注销该用户。
如果强制用户注销，Horizon 7 将在断开之前通知用户，并允许他们关闭应用程序和注销。
- 确定最小场大小。最小场大小是始终保持可用的 RDS 主机数量，以便允许用户继续使用场。例如，如果场大小为 10，而最小场大小为 2，则将对 8 个 RDS 主机执行维护。当每个 RDS 主机重新可用时，将对剩余的主机进行维护。所有 RDS 主机均单独进行管理，因此，当一个主机可用时，将对剩余的其中一个主机进行维护。

但是，如果您安排即时维护，则将对场中的所有 RDS 主机进行维护。

所有 RDS 主机还应遵循策略，根据配置的策略，等待注销或强制注销用户。

- 决定是否在出现第一个错误时停止置备。如果选择此选项，并且在连接服务器置备即时克隆时出现错误，将停止置备。您可以选择此选项来防止不必要的资源消耗（如存储）。
选择在出现第一个错误时停止选项对自定义不起作用。如果即时克隆出现自定义错误，将继续置备和自定义其他克隆。
- 确认已启用置备。如果禁用了置备，在刷新计算机后，Horizon 7 禁止自定义这些计算机。
- 如果您的部署包括连接服务器副本实例，请确认所有实例均为相同版本。

步骤

- 1 在 Horizon Console 中，选择**清单 > 场**。
- 2 单击您要安排维护的场的池 ID。
- 3 单击**维护 > 调度**。

4 在安排定期维护向导中，选择一种维护模式。

选项	操作
定期	<p>安排定期维护场中的所有 RDS 主机服务器。</p> <ul style="list-style-type: none"> ■ 选择维护生效的日期和时间。 ■ 选择维护周期。您可以选择以下维护周期：每天、每月或每周。 ■ 选择定期维护操作的时间间隔（单位：天）。 <p>如果对场安排即时维护，则即时维护日期成为定期维护的有效日期。如果您取消即时维护，则当前日期成为定期维护的有效日期。</p>
立即	<p>安排即时维护场中的所有 RDS 主机服务器。即时维护为即时维护或即将进行的维护创建一次性维护时间表。当您要应用紧急的安全修补程序时，可使用即时维护刷新新的父虚拟机映像或快照中的场。</p> <p>选择一种即时维护配置。</p> <ul style="list-style-type: none"> ■ 选择立即启动，立即启动维护操作。 ■ 选择启动时间，在即将到来的日期和时间启动维护操作。输入日期和 Web 浏览器本地时间。 <p>注 定期维护将暂停，直到即时维护完成为止。</p>

5 单击**下一步**。

6 （可选）单击**更改**以更改父虚拟机。

7 选择一个快照。

未清除**使用当前父虚拟机映像**复选框，将无法选择其他快照。

8 （可选）单击**快照详细信息**以显示有关该快照的详细信息。

9 单击**下一步**。

10 （可选）指定是强制注销用户，还是等待用户注销。

默认情况下，将选择强制注销用户的选项。

11 （可选）指定是否在出现第一个错误时停止置备。

默认情况下，此选项处于选定状态。

12 单击**下一步**。

将显示**即将完成**页。

13 单击**完成**。

在 Horizon Console 中管理应用程序池

在 Horizon Console 中，您可以添加、编辑、删除或授权应用程序池。

在 Horizon Console 中编辑应用程序池

您可以编辑现有的应用程序池来配置显示名称、版本、发布者、路径、开始文件夹、参数和描述等设置。不能更改应用程序池的 ID 或访问组。

前提条件

- 熟悉应用程序池的设置。
- 您可能需要配置一个反关联性规则，以确保连接服务器仅在具有足够的资源来运行应用程序的 RDS 主机上启动该应用程序。

步骤

- 1 在 Horizon Console 中，选择**清单 > 应用程序**。
- 2 选择一个池，然后单击**编辑**。
- 3 更改池的设置。
- 4 单击**确定**。

在 Horizon Console 中删除应用程序池

您删除应用程序池后，用户无法再启动池中的应用程序。

即使用户当前正在访问某个应用程序，您也可以删除应用程序池。用户关闭该应用程序后，将无法再访问该应用程序。

步骤

- 1 在 Horizon Console 中，选择**清单 > 应用程序**。
- 2 选择一个或多个应用程序池，然后单击**删除**。
- 3 单击**确定**进行确认。

更改已发布应用程序的图标

您可以为最终用户自定义已发布应用程序的图标。更改已发布应用程序的图标后，最终用户可以在已发布的桌面上查看新的应用程序图标。

前提条件

- 确认图标使用的是 PNG 文件格式。

步骤

- 1 在 Horizon Console 中，选择**清单 > 应用程序**。
- 2 选择一个或多个应用程序池，然后单击**应用程序图标 > 关联应用程序图标**。

3 要上载图标，请单击**上载图标文件**，然后浏览以找到一个 .PNG 格式的图标。

图标文件必须介于 16x16 像素和 256x256 像素之间。

4 单击**确定**。

已发布应用程序的图标此时将显示在已发布桌面上。

移除已发布应用程序的图标

您可以移除已发布应用程序的图标，以将其替换为其他图标。当您移除某个已发布应用程序的图标后，该已发布的应用程序将被替换为已发布桌面上的默认图标。仅当所有已发布应用程序具有相同图标时，才能从多个已发布应用程序中移除图标。您无法选择多个具有不同图标的已发布应用程序来移除图标。

步骤

1 在 Horizon Console 中，选择**清单 > 应用程序**。

2 选择一个或多个应用程序池，然后单击**应用程序图标 > 移除应用程序图标**。

已发布应用程序的图标将被替换为已发布桌面上的默认图标。

在 Horizon Console 中管理 RDS 主机

您可以管理手动设置的 RDS 主机以及在添加自动场时自动创建的 RDS 主机。

在手动设置 RDS 主机时，将自动在 Horizon 连接服务器中注册该主机。您无法手动向连接服务器注册 RDS 主机。对于手动设置的 RDS 主机，您可以执行以下管理任务：

- 编辑 RDS 主机。
- 将 RDS 主机添加到手动场中。
- 从场中移除 RDS 主机。
- 启用 RDS 主机。
- 禁用 RDS 主机。

对于在添加自动场时自动创建的 RDS 主机，您可以执行以下管理任务：

- 从场中移除 RDS 主机。
- 启用 RDS 主机。
- 禁用 RDS 主机。

在 Horizon Console 中编辑 RDS 主机

您可以更改 RDS 主机可以支持的连接数量。这是您唯一可以更改的设置。默认值为 150。您可以将此值设置为任意正数或不受限制。

您只能编辑手动设置的 RDS 主机，而不能编辑自动场中的 RDS 主机。

步骤

- 1 在 Horizon Console 中，选择**设置 > 已注册的计算机**。
- 2 选择一个 RDS 主机并单击**编辑**。
- 3 为**连接数量**设置指定一个值。
- 4 单击**确定**。

在 Horizon Console 中将 RDS 主机添加到手动场

您可以将手动设置的 RDS 主机添加到手动场中，以扩大场规模或实现其他目的。您只能将 RDS 主机添加到手动场中。

步骤

- 1 在 Horizon Console 中，选择**清单 > 场**。
- 2 单击场 ID。
- 3 选择 **RDS 主机**选项卡。
- 4 单击**添加**。
- 5 选择一个或多个 RDS 主机。
- 6 单击**确定**。

通过 Horizon Console 从场中移除 RDS 主机

您可以从手动场中移除 RDS 主机，以减小场规模，在 RDS 主机上执行维护或实现其他目的。最佳做法是禁用 RDS 主机并确保用户已从活动会话中注销，然后再从场中移除主机。

如果用户在您移除的主机上有应用程序或桌面会话，会话将保持活动状态，但 Horizon 7 不会跟踪这些会话。用户从会话断开连接后将无法重新连接到该主机，未保存的所有数据都可能会丢失。

也可以从自动场中移除 RDS 主机。一个可能的原因是，RDS 主机处于无法恢复的错误状态。

步骤

- 1 在 Horizon Console 中，选择**清单 > 场**。
- 2 单击场 ID。
- 3 选择 **RDS 主机**选项卡。
- 4 选择一个或多个 RDS 主机。
- 5 单击**从场中移除**。
- 6 单击**确定**。

从 Horizon 7 中移除 RDS 主机

您可以从 Horizon 7 中移除手动设置的 RDS 主机以及不打算再使用的 RDS 主机。RDS 主机不能当前位于手动场中。

前提条件

确认 RDS 主机不属于场。

步骤

- 1 在 Horizon Console 中，选择**设置 > 已注册的计算机**。
- 2 选择一个 RDS 主机并单击**移除**。
- 3 单击**确定**。

移除 RDS 主机后，必须重新安装 Horizon Agent，才能再次使用该主机。

在 Horizon Console 中禁用或启用 RDS 主机

禁用 RDS 主机后，Horizon 7 将不再使用该主机托管新的已发布桌面或应用程序。用户可以继续使用当前已打开的已发布桌面和应用程序。

步骤

- 1 在 Horizon Console 中，选择**清单 > 场**。
- 2 单击场 ID。
- 3 选择 **RDS 主机** 选项卡。
- 4 选择一个 RDS 主机并单击**更多命令**。
- 5 单击**启用或禁用**。
- 6 单击**确定**。

如果您启用 RDS 主机，“已启用”列中将显示复选标记，“状态”列中将显示“可用”。如果您禁用 RDS 主机，“已启用”列将为空，“状态”列中将显示“已禁用”。

在 Horizon Console 中监控 RDS 主机

您可以在 Horizon Console 中监控 RDS 主机的状态并查看其属性。

步骤

- ◆ 在 Horizon Console 中，导航到显示待查看属性的页面。

属性	操作
DNS 名称、类型、映像、等待处理的映像、任务、最大连接数量、会话、代理版本、已启用、状态	<ul style="list-style-type: none"> ■ 在 Horizon Console 中，选择清单 > 场。 ■ 选择一个场，然后单击 RDS 主机 选项卡。
RDS 主机、场、桌面池、代理版本、会话、状态	<ul style="list-style-type: none"> ■ 在 Horizon Console 中，选择清单 > 计算机。 ■ 单击 RDS 主机 选项卡。
DNS 名称、类型、RDS 场、最大连接数量、会话、代理版本、已启用、状态	<ul style="list-style-type: none"> ■ 在 Horizon Console 中，选择设置 > 已注册的计算机。 ■ 单击 RDS 主机 选项卡。

将显示属性，属性含义如下：

属性	说明
RDS 主机	RDS 主机的名称。
场	RDS 主机所属的场。
桌面池	与场相关联的已发布桌面池。
代理版本	在 RDS 主机上运行的 Horizon Agent 的版本。
会话	客户端会话数。
DNS 名称	RDS 主机的 DNS 名称。
类型	在 RDS 主机上运行的 Windows Server 的版本。
RDS 场	RDS 主机所属的场。
映像	场中 RDS 主机的映像。
等待处理的映像	场中 RDS 主机的等待处理的映像。
任务	正在场的 RDS 主机上执行的任务。
最大连接数量	RDS 主机可以支持的最大连接数量。
已启用	RDS 主机是否已启用。
状态	RDS 主机的状态。有关可能状态的说明，请参阅 Horizon Console 中的 RDS 主机状态 。

Horizon Console 中的 RDS 主机状态

RDS 自初始化后可能会处于各种不同的状态。最佳做法是，在 RDS 主机上执行任务或操作前后，检查主机是否处于预期状态。

表 11-6. RDS 主机的状态

状态	说明
启动	RDS 主机上的 Horizon Agent 已经启动，但所需的其他服务（如显示协议等）仍正在启动。在该代理启动时段内，其他进程（例如协议服务）可同时启动。
正在禁用	RDS 主机正在被禁用，但会话仍在该主机上运行。会话终止后，状态将更改为“已禁用”。
已禁用	禁用 RDS 主机的过程已完成。
正在验证	在连接服务器首次识别 RDS 主机后出现，通常是在启动或重新启动连接服务器之后，首次成功在 RDS 主机上与 Horizon Agent 通信之前。通常情况下，该状态是暂时的。该状态与 Agent 无法访问状态不同，后者指示存在通信问题。
已禁用代理	如果连接服务器禁用 Horizon Agent ，会出现此情况。该状态确保一个新的桌面或应用程序会话无法在 RDS 主机上启动。
无法访问代理	连接服务器无法与 RDS 主机上的 Horizon Agent 建立通信。
无效 IP	子网掩码注册表设置在 RDS 主机上进行配置，在配置范围内，没有活动的网络适配器具有 IP 地址。
代理需要重新引导	Horizon 7 组件已升级，必须重新启动 RDS 主机， Horizon Agent 才能运行已升级的组件。
协议失败	RDP 显示协议未正确运行。如果 RDP 未运行，但 PCoIP 正在运行，客户端将无法使用 RDP 或 PCoIP 进行连接。但是，如果 RDP 正在运行，而 PCoIP 未运行，客户端可以使用 RDP 进行连接。
域失败	RDS 主机在访问域时遇到问题。无法访问域服务器或者域身份验证失败。
配置错误	RDS 角色在服务器上未启用。
未知	RDS 主机处于未知状态。
可用	RDS 主机可用。如果主机在场中，并且该场与已发布的桌面或应用程序池相关联，则将使用该主机向用户交付已发布的桌面或应用程序。

在 Horizon Console 中管理已发布的桌面和应用程序会话

用户启动已发布的桌面或应用程序时，会创建一个会话。您可以断开连接并注销会话、向客户端发送消息以及重置和重新启动虚拟机。

步骤

- 1 在 Horizon Console 中，导航到显示会话信息的位置。

会话类型	导航
远程桌面会话	<p>选择清单 > 桌面，单击池的 ID，然后单击会话选项卡。此外，会话列还会显示在所有桌面的桌面池页面上。</p> <p>选择清单 > 场，单击场的 ID，然后单击会话选项卡。此外，会话列还会显示在所有场的场页面上。</p> <p>选择设置 > 已注册的计算机，然后查看会话列。</p>
远程桌面和应用程序会话	选择 监控 > 会话 。
与用户或用户组相关联的会话	<ul style="list-style-type: none"> ■ 选择用户和组。 ■ 单击用户的名称或用户组的名称。 ■ 单击会话选项卡。

- 2 选择会话。

要向用户发送消息，可以选择多个会话。您一次只可在一个会话中执行其他操作。您只能对不是从 vSphere 控制台连接的会话执行注销操作。

- 3 选择是断开连接、注销、发送消息、重新启动桌面，还是重置虚拟机。

选项	说明
断开会话	将用户从会话断开连接。
注销会话	将用户注销会话。未保存的数据会丢失。
发送消息	向 Horizon Client 发送消息。您可将消息标记为 信息 、 警告 或 错误 。
重新启动桌面	在虚拟桌面上执行重新启动操作，这会执行正常的虚拟机操作系统重新启动。
重置虚拟机	在虚拟机上执行重置操作，而不正常重新启动操作系统，这会执行硬虚拟机电源关闭和打开。

- 4 单击**确定**。

在 Horizon Console 中授权用户和组

12

您通过配置授权来控制用户可以访问哪些远程桌面和应用程序。您可以配置受限制的授权功能，在用户选择远程桌面时根据他们连接的 Horizon 连接服务器实例来控制桌面访问。您还可以限制网络外部的一组用户的访问，禁止他们连接网络内部的远程桌面和已发布应用程序。

有关在 Cloud Pod 架构环境中配置全局授权的信息，请参阅《在 Horizon 7 中管理 Cloud Pod 架构》文档。

注 对于手动或链接克隆桌面池，不支持添加、移除或查看授权。

本章讨论了以下主题：

- 在 Horizon Console 中为桌面池或应用程序池添加授权
- 在 Horizon Console 中移除对桌面池或应用程序池的授权
- 查看桌面或应用程序池授权
- 为授权池配置快捷方式
- 对桌面和应用程序池实施客户端限制

在 Horizon Console 中为桌面池或应用程序池添加授权

在用户能够访问远程桌面或应用程序前，必须授权这些用户使用桌面池或应用程序池。

前提条件

创建一个桌面池或应用程序池。

步骤

- 1 选择桌面池或应用程序池。

选项	操作
为桌面池添加授权	在 Horizon Console 中，选择 清单 > 桌面 ，然后单击桌面池的名称。
为应用程序池添加授权	在 Horizon Console 中，选择 清单 > 应用程序 ，然后单击应用程序池的名称。

- 2 从**授权**下拉菜单中选择**添加授权**。

- 单击**添加**，选择一个或多个搜索条件，然后单击**查找**根据搜索条件查找用户或组。

注 未验证访问用户会被从搜索结果中筛选掉。混合模式域搜索结果中将不包含域本地用户组。如果您的域是在混合模式下配置的，您将不能为域本地用户组中的用户授权。

- 选择要授权其使用池中桌面或应用程序的用户或组，然后单击**确定**。
- 单击**确定**保存更改。

在 Horizon Console 中移除对桌面池或应用程序池的授权

您可以移除对桌面池或应用程序池的授权，以阻止特定用户或组访问桌面或应用程序。

步骤

- 选择桌面池或应用程序池。

选项	操作
为桌面池添加授权	在 Horizon Console 中，选择 清单 > 桌面 ，然后单击桌面池的名称。
为应用程序池添加授权	在 Horizon Console 中，选择 清单 > 应用程序 ，然后单击应用程序池的名称。

- 从**授权**下拉菜单中选择**移除授权**。
- 选择您要移除其授权的用户或用户组，然后单击**移除**。
- 单击**确定**保存更改。

查看桌面或应用程序池授权

您可以查看某个用户或用户组有权访问的桌面池或应用程序池。

步骤

- 在 Horizon Console 中，选择**用户和组**，然后单击用户或用户组的名称。
- 单击**授权**选项卡并查看某个用户或用户组有权访问的桌面池或应用程序池。

选项	操作
列出用户或组有权访问的桌面池	单击 桌面授权 。
列出用户或组有权访问的应用程序池	单击 应用程序授权 。

为授权池配置快捷方式

可以为授权池配置快捷方式。当授权用户从 Windows 客户端连接到连接服务器实例时，适用于 Windows 的 Horizon Client 会将这些快捷方式放在用户的客户端设备上的“开始”菜单中和/或桌面上。可以在创建或修改池时配置快捷方式。

在快捷方式配置期间，必须选择类别文件夹或根 (/) 文件夹。您可以添加并命名自己的类别文件夹。您最多可以配置四个文件夹级别。例如，可以添加一个名为“Office”的类别文件夹，并为所有与工作相关的应用程序（例如 Microsoft Office 和 Microsoft PowerPoint）选择该文件夹。

对于“开始”菜单快捷方式，在 Windows 7 客户端设备上，Horizon Client 会将类别文件夹和快捷方式放在“开始”菜单中的“VMware 应用程序”文件夹中。如果您为快捷方式选择根 (/) 文件夹，则 Horizon Client 会将快捷方式直接放在“VMware 应用程序”文件夹中。在 Windows 8 和 Windows 10 客户端设备上，Horizon Client 会将类别文件夹和快捷方式放在“应用程序”列表中。如果您为快捷方式选择根 (/) 文件夹，则 Horizon Client 会将快捷方式直接放在“应用程序”列表中。

创建快捷方式后，会在 Horizon Administrator 和 Horizon Console 中该池的**应用程序快捷方式**列中显示一个勾号。

默认情况下，当授权用户首次连接到服务器时，适用于 Windows 的 Horizon Client 会提示他们安装快捷方式。您可以通过修改在 **Horizon Server 上配置快捷方式后自动安装快捷方式** 组策略设置，配置适用于 Windows 的 Horizon Client 自动安装快捷方式或从不安装快捷方式。有关更多信息，请参阅《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档。

默认情况下，用户每次连接到服务器时，都会将您对快捷方式所做的更改同步到用户的 Windows 客户端设备。Windows 用户可在 Horizon Client 中禁用快捷方式同步功能。有关更多信息，请参阅《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档。

对于 Windows 用户，此功能需要在客户端系统上安装适用于 Windows 的 Horizon Client 4.6 或更高版本。对于 Mac 用户，此功能需要在客户端系统上安装适用于 Mac 的 Horizon Client 4.10 或更高版本。

还可以在创建或修改全局授权时配置快捷方式。有关配置全局授权的信息，请参阅《在 Horizon 7 中管理 Cloud Pod 架构》文档。

在 Horizon Console 中为桌面池创建快捷方式

可以在 Horizon Console 中为授权的桌面池创建快捷方式，以便桌面池显示在用户 Windows 客户端设备上的 Windows “开始”菜单中和/或 Windows 桌面上。您最多可以为快捷方式指定四个类别文件夹级别。可以在创建桌面池时创建快捷方式。此外，也可以在编辑桌面池时创建和修改快捷方式。

前提条件

确定如何基于要创建的桌面池类型配置池设置。

步骤

- 1 在 Horizon Console 中，单击**清单 > 桌面**，然后单击**添加**。
- 2 在**添加池**向导中，选择要创建的桌面池类型，然后单击**下一步**。
- 3 按照向导提示转到**桌面池设置**页面。

4 为桌面池创建快捷方式。

- a 单击“类别文件夹”的**浏览**按钮。
- b 选择**从文件夹列表选择一个类别文件夹**选项。
- c 在**选择一个类别文件夹或创建一个新文件夹**，以将该池的快捷方式放置在客户端设备中文本框中键入一个文件夹名称。

文件夹名称最长可包含 64 个字符。要指定子文件夹，请输入反斜线 (\) 字符，例如，**dir1\dir2\dir3\dir4**。您最多可以输入四个文件夹级别。您不能在文件夹名称的开头或结尾使用反斜线，也不能将两个或更多反斜线组合到一起使用。例如，**\dir1**、**dir1\dir2**、**dir1\dir2** 以及 **dir1\\dir2** 均无效。您不能输入 **Windows** 保留关键字。

- d 选择快捷方式创建方法。

可以选择一种或两种方法。

选项	说明
“开始”菜单/启动程序	在 Windows 客户端设备上创建 Windows “开始”菜单快捷方式。
桌面	在 Windows 客户端设备的桌面上创建快捷方式。

- e 要保存更改，请单击**提交**。

5 按照向导提示转到**即将完成**页面，选择**此向导完成后授权用户**，然后单击**提交**。

6 在**添加授权**向导中，单击**添加**，选择一个或多个搜索条件，单击**查找**以基于您的搜索条件查找用户或组，选择要授权其使用池中的桌面的用户或组，然后单击**确定**。

该桌面池在**桌面池**页面上对应的**应用程序快捷方式**列中会显示一个勾号。

在 Horizon Console 中为应用程序池创建快捷方式

可以在 Horizon Console 中为授权的应用程序创建快捷方式，以便快捷方式显示在用户 Windows 客户端设备上的 Windows “开始”菜单中和/或 Windows 桌面上。您最多可以为快捷方式指定四个类别文件夹级别。您可以在创建应用程序池时创建快捷方式。此外，也可以在编辑应用程序池时创建快捷方式。

在 Mac 客户端上，如果将适用于 Mac 的 Horizon Client 配置为从本地系统上的应用程序文件夹中运行已发布的应用程序，并允许使用服务器中的文件夹设置，则类别文件夹会显示在 Mac 客户端设备上的应用程序文件夹中。有关更多信息，请参阅《适用于 Mac 的 VMware Horizon Client 安装和设置指南》文档。

前提条件

- 设置 RDS 主机。请参阅《在 Horizon 7 中设置桌面和应用程序池》文档中的“设置远程桌面服务主机”。
- 创建包含 RDS 主机的场。请参阅[在 Horizon Console 中创建场](#)。
- 如果要手动添加应用程序池，应收集有关该应用程序的信息。请参阅[用于在 Horizon Console 中手动创建应用程序池的工作表](#)。
- 在客户端设备上安装适用于 Windows 的 Horizon Client 4.6 或更高版本。

步骤

1 在 Horizon Console 中，单击**清单 > 应用程序**，然后单击**添加**。

2 选择要创建的应用程序池类型。

选项	说明
手动添加应用程序池	输入有关应用程序的信息。请参阅 用于在 Horizon Console 中手动创建应用程序池的工作表 。
选择安装的应用程序	按名称、安装路径或应用程序类型筛选以查找应用程序，或者从安装的应用程序列表中选择应用程序。有关配置其他选项的信息，请参阅 用于在 Horizon Console 中手动创建应用程序池的工作表 。

3 在**添加应用程序池**向导中，选择一个 RDS 场，然后输入一个池 ID 以及应用程序的完整路径名。

4 为应用程序池创建快捷方式。

a 单击“类别文件夹”的**浏览**按钮。

b 选择**从文件夹列表选择一个类别文件夹**选项。

c 从列表选择一个类别文件夹，或者在**选择一个类别文件夹或创建一个新文件夹**，以将该池的快捷方式放置在客户端设备中文本框中键入一个文件夹名称。

文件夹名称最长可包含 64 个字符。要指定子文件夹，请输入反斜线 (\) 字符，例如，**dir1\dir2\dir3\dir4**。您最多可以输入四个文件夹级别。您不能在文件夹名称的开头或结尾使用反斜线，也不能将两个或更多反斜线组合到一起使用。例如，**\dir1**、**dir1\dir2**、**dir1\dir2** 以及 **dir1\\dir2** 均无效。您不能输入 Windows 保留关键字。

注 如果需要，非 Windows 客户端可将反斜杠转换为正斜杠。

d 选择快捷方式创建方法。

可以选择一种或两种方法。

选项	说明
“开始”菜单/启动程序	在 Windows 客户端设备上创建 Windows “开始”菜单快捷方式。
桌面	在 Windows 客户端设备的桌面上创建快捷方式。

e 要保存更改，请单击**提交**。

5 选择**此向导完成后授权用户**。

6 在**添加授权**向导中，单击**添加**，选择一个或多个搜索条件，单击**查找**以基于您的搜索条件查找用户或组，选择要授权使用池中的应用程序的用户或组，然后单击**确定**。

该应用程序池在**应用程序池**页面上对应的**应用程序快捷方式**列中会显示一个勾号。

对桌面和应用程序池实施客户端限制

您可以限制只有特定客户端计算机才能访问授权的已发布桌面和应用程序池。要限制访问，您必须在 **Active Directory** 安全组中添加可访问已发布的桌面或应用程序的客户端计算机名称，然后授权该组访问池。**Active Directory** 安全组可以包含属于任何 **AD** 组织单位 (**Organizational Unit, OU**) 或默认计算机容器的客户端计算机。

客户端限制功能具有特定的要求和限制。

- 在创建或修改已发布的桌面或应用程序池时，您必须启用客户端限制策略。默认情况下，客户端限制策略处于禁用状态。有关已发布的桌面池设置的信息，请参阅[用于创建已发布桌面池的工作表](#)。有关应用程序池设置的信息，请参阅[用于在 Horizon Console 中手动创建应用程序池的工作表](#)。
- 在创建或修改已发布的桌面或应用程序池的授权时，您必须添加包含可访问已发布的桌面或应用程序池的客户端计算机名称的 **Active Directory** 安全组。
- 客户端限制功能只允许特定客户端计算机访问已发布的桌面和应用程序池。该功能不会授予用户访问非授权桌面和应用程序池的权限。例如，如果某个用户未包含在应用程序池授权中（作为用户或用户组成员），则即使该用户的客户端计算机所在的 **AD** 安全组被授权访问应用程序池，该用户也无法访问应用程序池。
- 在此版本中，仅 **Windows** 客户端计算机支持客户端限制功能。客户端计算机需要安装适用于 **Windows** 的 **Horizon Client 4.6** 或更高版本。
- 为已发布的桌面或应用程序池启用客户端限制策略后，非 **Windows** 客户端、运行版本低于 **4.6** 的适用于 **Windows** 的 **Horizon Client** 的 **Windows** 客户端以及 **HTML Access** 客户端均无法启动受限制的池中的桌面或应用程序。
- 客户端限制功能仅限制 **Windows** 客户端中的新会话。此功能不会限制先前用户会话中现有的应用程序会话连接。
- 适用于 **Windows** 的 **Horizon Client 5.0** 版要求属于 **Active Directory** 安全组的客户端计算机位于默认 **AD** 位置 “**CN=Computers**” 中。

JMP Integrated Workflow 入门

熟悉高级 JMP Integrated Workflow 概念并完成开始使用 JMP Integrated Workflow 功能所需的任务。

本章讨论了以下主题：

- [关于 JMP Integrated Workflow](#)
- [开始使用 JMP 集成工作流](#)

关于 JMP Integrated Workflow

通过 VMware HorizonJMP (Just-in-Time Management Platform) 集成工作流功能，您可以使用一个控制台来定义和管理用户或用户组的桌面工作区。

桌面工作区可通过定义一个包含 VMware Horizon 桌面池、VMware App Volumes AppStack 和 VMware User Environment Manager 设置相关信息的 JMP 分配来创建。提交 JMP 分配后，JMP 自动化引擎会与 Horizon 7、App Volumes 和 User Environment Manager 系统进行通信，以授权用户访问桌面。

您可以使用 Horizon Console 中的**分配 (JMP)** 选项卡来管理现有的 JMP 分配。还可以使用每个组件分配各自的 JMP 组件控制台修改每个组件分配。例如，还可以通过在 Horizon Console 中选择**清单 > 桌面**，对在 JMP 分配中定义的桌面池进行的更改进行修改。

在 Horizon Console 中打开 JMP 分配时，将验证 JMP 分配中每个组件的当前状态，以确保组件处于所预期的状态。发现差异后，会在控制台中突出显示受影响的区域，您可以接受当前状态，也可以修改分配以达到所需的状态并重新为用户授权。

您安装并配置 VMware HorizonJMP Server 后，即可在 Horizon Console 中使用 JMP Integrated Workflow 功能。请参阅 [开始使用 JMP 集成工作流](#)和《VMware Horizon JMP Server 安装和设置指南》以了解相关信息。

注 由于 App Volumes 不支持 VMware Cloud，因此在 AWS 上 JMP Integrated Workflow 功能不支持 VMware Cloud®

开始使用 JMP 集成工作流

要开始使用 JMP Integrated Workflow 功能，必须安装和设置 JMP Server，并配置 JMP 设置。

前提条件

查看您计划安装的所有技术组件所需要的必备条件和系统要求。

步骤

- 1 如有必要，在 Active Directory 中设置所需的管理人员用户和组。
请参阅《Horizon 7 安装指南》文档中的“准备 Active Directory”。在配置 JMP 设置时，需要提供 Active Directory 信息。
- 2 设置 Microsoft SQL Server，并确保已创建您计划在 JMP Server 安装过程中使用的登录凭据。有关更多信息，请参阅《VMware Horizon JMP Server 安装和设置指南》文档中的“JMP Server 的数据库要求”。
- 3 安装并设置 VMware Horizon 7 版本 7.5 或更高版本。
请参阅《Horizon 7 安装指南》文档。
- 4 （可选）安装并设置 VMware App Volumes 2.14 或更高版本，该版本可提供用于实时应用程序交付的功能。
有关详细信息，请参阅《VMware App Volumes 安装指南》文档。
- 5 （可选）要提供上下文策略管理，请安装并设置 VMware User Environment Manager 9.2.1 或更高版本。
请参阅《安装和配置 VMware User Environment Manager》文档。
- 6 获取 JMP Server 与组织网络内其他服务器进行安全通信所需使用的 CA 签名的 SSL 证书。
- 7 安装 JMP Server 并配置 SSL 证书，以便 JMP Server 能够与 JMP Integrated Workflow 功能所需的其他服务器进行通信。
请参阅《VMware Horizon JMP Server 安装和设置指南》了解更多信息。
- 8 首次配置 JMP 设置。有关详细信息，请参阅[首次配置 JMP 设置](#)。

后续步骤

成功完成前面的任务之后，您现在可以创建一个 JMP 分配。有关信息，请参阅[创建 JMP 分配](#)。

管理 JMP 设置

安装 JMP Server 后，必须先使用必要的凭据配置 JMP 设置，然后才能创建任何 JMP 分配并开始使用 JMP Integrated Workflow 功能。可以先编辑初始 JMP 设置，然后在适用时添加新的设置信息。

本章讨论了以下主题：

- 首次配置 JMP 设置
- 管理 JMP 设置

首次配置 JMP 设置

在创建任何 JMP 分配之前，都必须先使用 Horizon Console 配置 JMP 设置。对于用来为用户或用户组分配桌面工作区的 Active Directory 域，必须为其提供凭据。您可以选择包含凭据信息，以在创建 JMP 分配时使用 App Volumes AppStack 和 User Environment Manager 配置共享。

前提条件

- 确认已成功安装 VMware HorizonJMP Server，并且您有其 URL。请参阅《VMware Horizon JMP Server 安装和设置指南》了解更多信息。
- 获取您计划与 JMP Server 一起使用的 Horizon 7 版本 7.5 或更高版本的管理员帐户凭据。
- 获取必须在 JMP Server 上使用的 Active Directory 凭据。
- 如果要向 JMP 分配中分配应用程序，请确保您具有要使用的 VMware App Volumes Manager 实例的 URL 和管理员帐户凭据。如果由负载均衡器管理计划使用的 App Volumes Manager 实例，请获取负载均衡器的 URL，并在配置 App Volumes Manager 信息时使用此 URL。
- 如果选择使用 VMware User Environment Manager 配置共享，请获取其 UNC 路径和对其进行访问所需的 administrator 帐户凭据。

步骤

- 1 在 Horizon Console 中，单击 **JMP 配置**。
- 2 输入 JMP Server 信息。
 - a 在 **JMP Server** 选项卡中，单击**添加 JMP Server**。
 - b 以 `https://jmp.yourcompany.com` 的格式输入 JMP Server URL。
 - c 单击**保存**。

将对 JMP Server URL 进行验证。如果收到消息 JMP Server 无法访问 (JMP Server is unreachable)，请确认输入的 URL 正确无误、JMP Server 已正确配置，以及 JMP Server 可以访问。

3 输入计划用于 JMP Server 的 Horizon 7 连接服务器版本 7.5 或更高版本的帐户信息。

- a 单击 **Horizon 7** 选项卡。
- b 如果**连接服务器 URL** 值未自动填充，请输入该值。此 URL 与 Horizon Console 连接到的 Horizon 7 连接服务器的 URL 相同。
- c 输入 Horizon 7 服务帐户用户名和密码。
- d 在**服务帐户域**文本框中，输入有效的名称以用于要创建的 JMP 分配，然后按 **Enter**。
- e 单击**保存**。

4 输入要用于 JMP 分配的 Active Directory 的信息。

- a 单击 **Active Directory** 选项卡。
- b 单击**新建**。
- c 在 **NETBIOS 名称**文本框中，从可用 NetBIOS 域名列表中选择域名。
将使用默认值更新“DNS 域名”和“上下文”文本框。
- d 确认 **DNS 域名**文本框中添加的默认值是要使用的正确值。还可以选择输入其他 Active Directory 完全限定域名。例如，mycompany.com。
- e 在**协议**部分中，选择 Active Directory 使用的协议。
- f 在**绑定用户名**和**绑定密码**文本框中，输入绑定标识名 (Distinguished Name, DN) 用户帐户的凭据。例如，administrator。
- g 如果要使用默认值之外的其他值，可以修改**上下文**文本框中的值。
此值用作 Active Directory 数据搜索的根目录。
- h (可选) 单击**高级属性**并修改默认端口号值。
默认端口值取决于先前选择的协议。您可以修改端口值或将文本框留空。
- i 在**域控制器**文本框中，可以选择输入一个或多个主机名或 IP 地址，用于处理 Active Directory 流量。
例如，adserver.mycompany.com, 10.111.XXX.XXX。如果将此文本框留空，将使用 **DNS 域名** 文本框中的值。
- j 单击**保存**。

5 如果计划在创建 JMP 分配时使用 App Volumes AppStack，请配置想要使用的 App Volumes Manager。

- a 单击 **App Volumes** 选项卡。
- b 单击**新建**。

- c 在**名称**文本框中，输入要分配给 App Volumes 实例的名称。如果将此文本框留空，将使用在 **App Volumes Server URL** 文本框中输入的值。
- d 输入希望与 JMP Server 容器关联的 App Volumes Manager 的有效 URL。

重要事项 如果由负载均衡器来管理计划使用的 App Volumes Manager，请输入该负载均衡器的 URL。

- e 输入 JMP Server 可用来访问 App Volumes Manager 的 App Volumes Manager 或负载均衡器管理员帐户凭据。
 - f 输入将用于 JMP 分配的 App Volumes Manager 服务帐户的域名。
 - g （可选）如果要注册多个 App Volumes Manager，可以使用切换按钮来指示要添加的 App Volumes Manager 是否为创建 JMP 分配时要使用的默认服务器。可以更改要在创建 JMP 分配时使用的实例。
 - h 单击**保存**。
- 6 如果要在创建 JMP 分配时使用 User Environment Manager 配置共享，请在 JMP 设置中添加该共享的信息。
- a 单击 **UEM** 选项卡。
 - b 单击**新建**。
 - c 在**文件共享 UNC 路径**文本框中以 \\fileserver-name\UEM-configuration-share-pathname 格式输入一个值。例如，\\FileServer\UEMConfig。

重要事项 请不要在您输入的文件共享 UNC 路径中包含 General。

- d 输入用来连接到 User Environment Manager 配置共享的 User Environment Manager 管理员帐户凭据。
- e 从 **Active Directory** 列表中，选择要用于 User Environment Manager 配置共享的域名。

注 一个 Active Directory 只能与一个 User Environment Manager 配置共享关联。

- f 单击**保存**。

后续步骤

成功配置初始 JMP 设置后，您现在可以创建 JMP 分配。请参阅[创建 JMP 分配](#)了解更多信息。

管理 JMP 设置

您可以使用 Horizon Console 修改、添加或删除 JMP 设置的信息。

- 具有修改特定 JMP 设置所需的必要信息。
- 要修改 JMP 设置，请确保您具有相应的管理特权。

编辑 JMP Server 设置

可以使用 Horizon Console 对现有 JMP Server 设置进行更改。

前提条件

- 具有修改特定 JMP Server 设置所需的必要信息。
- 确保具有登录 Horizon Console 和修改 JMP Server 设置所需的适当管理特权。

步骤

- 1 在 Horizon Console 中，选择 **JMP 配置**。
- 2 在“JMP 设置”窗格中，单击 **JMP Server** 选项卡。
- 3 单击 **编辑**。
- 4 输入一个新的 **JMP Server URL**。
- 5 单击 **保存**。

将验证新的 JMP Server URL，如果无效，将显示一条错误消息。

编辑 Horizon 7 凭据

可以使用 Horizon Console 对现有 Horizon 7 连接服务器凭据进行更改。

步骤

- 1 在 Horizon Console 中，单击 **JMP 配置**。
- 2 单击 **Horizon 7** 选项卡。
- 3 单击 **编辑凭据**。
- 4 根据需要在 **服务帐户用户名** 中输入新用户名。
- 5 根据需要在 **服务帐户密码** 中输入新密码。
- 6 根据需要更改 **服务帐户域** 中的值。
- 7 单击 **保存**。

编辑 Horizon 连接服务器 URL

如果要将现有 JMP 分配关联到其他 Horizon Connection Server，您必须修改通过 JMP Server 设置进行注册并与这些 JMP 分配相关联的 Horizon Connection Server URL。

Horizon Connection Server 中没有可用于修改 Horizon Console 信息的用户界面。要修改 JMP 设置中的现有 Horizon Connection Server 主机 URL，您必须使用 SQL Server Management Studio。

前提条件

- 确保您具备登录到 SQL Server Management Studio 会话的相应系统管理员特权，以及对为 JMP Server 创建的 SQL Server 数据库的访问权限。

- 在对数据库进行修改之前，备份 SQL Server 数据库。

步骤

- 1 如果您当前已登录到 Horizon Console 会话，请注销。
- 2 以 sysadmin (SA) 身份或使用具有 SA 特权的用户帐户登录 SQL Server Management Studio 会话。
- 3 确认您打算使用的替换 Horizon Connection Server 主机 URL 尚未在其他 JMP Server 实例中注册。

例如，如果替换 Horizon Connection Server 主机 URL 是 new-horizon-host.com，请使用以下 SQL 语句来确认该 URL 尚未注册。

```
SELECT * from xms_services
WHERE xms_services.host = "new-horizon-host.com"
```

- 4 如果上面的 SQL 语句未返回任何结果，请继续执行下一步。否则，请使用以下语句删除现有 Horizon Connection Server 主机的信息。

```
DELETE from xms_services
WHERE xms_services.host = "new-horizon-host.com"
```

- 5 使用以下语句更新现有 JMP Server 设置，其中 new-horizon-server-host.com 是替换 Horizon Connection Server 主机的 URL，old-horizon-host.com 是当前已注册 Horizon Connection Server 主机的 URL。

```
UPDATE xms_service_endpoints
SET host = 'new-horizon-host.com', is_available = 1
WHERE service_id = (SELECT id FROM xms_services WHERE service_type = 'horizon'
AND host = 'old-horizon-host.com')
AND host = 'old-horizon-host.com'

UPDATE xms_services
SET [name] = 'horizon-https://new-horizon-host.com', host = 'new-horizon-host.com'
WHERE service_type = 'horizon'
AND host = 'old-horizon-host.com'
```

- 6 使用新的 Horizon Connection Server URL 登录到 Horizon Console，并确认新 Horizon Connection Server 主机现在关联的现有 JMP 分配之前与旧的 Horizon Connection Server 主机相关联。

添加 Active Directory 域

如果您在设置初始 Active Directory 域后需要再添加一个这样的域，可以使用 Horizon Console。

步骤

- 1 在 Horizon Console 中，单击 **JMP 配置**。
- 2 单击 **Active Directory** 选项卡，然后单击 **添加**。
- 3 在 **NETBIOS 名称** 文本框中，从可用 NetBIOS 域名列表中选择域名。

将使用默认值更新“DNS 域名”和“上下文”文本框。

- 4 在 **DNS 域名** 文本字段中，确认 **NETBIOS** 名称更新后添加了默认值。还可以选择输入其他 **Active Directory** 完全限定域名。例如，**mycompany.com**。
- 5 在**协议**部分中，选择 **Active Directory** 使用的协议。
- 6 在**绑定用户名**和**绑定密码**文本字段中，输入绑定标识名 (DN) 用户帐户的凭据，如 **Administrator**。
- 7 如果要使用默认值之外的其他值，可以修改**上下文**文本字段中的值。
- 8 （可选）单击**高级属性**并修改默认端口号值。
默认端口值取决于先前选择的协议。您可以修改端口值或将文本字段留空。
- 9 在**域控制器**文本字段中，可以选择输入一个或多个主机名或 IP 地址，用于处理 **Active Directory** 流量。
- 10 单击**保存**。

有关新添加的 **Active Directory** 域的信息会显示在 **Active Directory** 表中。

编辑 Active Directory 域信息

如果在初始配置 JMP 设置后更改了某些信息，可以使用 **Horizon Console** 来修改 **Active Directory** 域设置信息。

步骤

- 1 在 **Horizon Console** 中，单击 **JMP 配置**。
- 2 单击 **Active Directory** 选项卡。
- 3 在 **Active Directory** 域表中选择一行，然后单击**编辑**。
- 4 修改需要更新的 **Active Directory** 信息。
- 5 单击**保存**。

删除 Active Directory 域信息

如果必须删除现有的 **Active Directory (AD)** 域设置信息，请使用 **Horizon Console**。

仅当所有现有 **JMP** 分配都未在使用已注册的 **Active Directory** 域时，才能从 **JMP** 设置中删除有关该域的信息。

步骤

- 1 在 **Horizon Console** 中，单击 **JMP 配置**。
- 2 单击 **Active Directory** 选项卡。
- 3 选择要从 **JMP** 设置中删除的 **Active Directory** 域所在的表行。
- 4 在出现的删除确认对话框中，阅读消息，然后单击**删除**以确认您要删除此 **Active Directory** 域信息。

如果没有 **JMP** 分配使用该 **Active Directory** 域，该域将被移除。

如果 Active Directory 域被任何 JMP 分配使用，会显示一个警告对话框。警告消息中包含使用该 Active Directory 域的 JMP 分配列表。仅当从 JMP 分配中移除此域，或删除使用此域的那些 JMP 分配后，才能删除域信息。

添加 App Volumes 信息

可以使用 Horizon Console 添加可在创建 JMP 分配时使用的任何其他 App Volumes Manager 的信息。

步骤

- 1 在 Horizon Console 中，单击 **JMP 配置**。
- 2 单击 **App Volumes** 选项卡，然后单击**添加**。
将显示**添加 App Volumes 实例**对话框。
- 3 在**名称**文本框中，输入要分配给 App Volumes 实例的唯一名称。如果将此文本框留空，将使用在 **App Volumes Server URL** 文本框中输入的值。
- 4 在 **App Volumes Server URL** 文本框中，为要与 JMP Server 关联的 App Volumes Manager 输入一个有效的 URL。如果由负载均衡器来管理所添加的 App Volumes Manager，请输入该负载均衡器的 URL。

注 如果所添加的 App Volumes Manager 连接到不同的 SQL 数据库，则 App Volumes 选项卡中将显示有关所添加 App Volumes Manager 的信息。如果 App Volumes Manager 连接到同一个 SQL 数据库，则 App Volumes 选项卡中将仅显示有关之前已注册的 App Volumes Manager 的信息。

- 5 输入 JMP Server 可用于访问 App Volumes Manager 的 App Volumes 管理员用户名和密码。
- 6 为用于 JMP 分配的 App Volumes 服务帐户输入域名。
- 7 要将当前添加的 App Volumes Manager 设为创建 JMP 分配时使用的默认 App Volumes Manager 服务器，请单击切换按钮。可以更改要在创建 JMP 分配时使用的服务器。
切换按钮会变成蓝色，并带有**是**标签。
- 8 单击**保存**。

编辑 App Volumes 实例信息

如果必须修改有关由 JMP 分配使用的 App Volumes 实例的现有信息，可以使用 Horizon Console。

步骤

- 1 在 Horizon Console 中，单击 **JMP 配置**。
- 2 单击 **App Volumes** 选项卡，然后选择要修改的 App Volumes 实例所在的表行。
- 3 单击**编辑**。
将显示**添加 App Volumes 实例**对话框。
- 4 修改要更新的 App Volumes 实例信息。
- 5 单击**保存**。

删除 App Volumes 实例信息

如果必须删除有关 App Volumes 实例的现有设置信息，请使用 Horizon Console。

仅当已注册的 App Volumes 实例未被任何 JMP 分配使用时，才能从 JMP 设置中删除有关该实例的信息。

步骤

- 1 在 Horizon Console 中，单击 **JMP 配置**。
- 2 单击 **App Volumes** 选项卡。
- 3 选择要从 JMP 设置中删除的 App Volumes 实例信息所在的行。
- 4 单击 **删除** 以确认您要删除此 App Volumes 实例信息。

如果没有 JMP 分配使用此 App Volumes 实例，将移除该实例。

如果此 App Volumes 实例被任何 JMP 分配使用，会显示一个警告对话框。警告消息中包含使用 App Volumes 实例的 JMP 分配的列表。仅当从 JMP 分配中移除此 App Volumes 实例，或删除使用此实例的那些 JMP 分配后，才能删除此实例的信息。

添加 User Environment Manager 配置共享信息

如果在设置初始 User Environment Manager 配置共享信息后必须添加另一个配置共享信息，可以使用 Horizon Console。

每个 AD 域只能添加一个 User Environment Manager 配置共享。因此，您要添加的配置共享的 IP 或 DNS 地址不能与 JMP Server 设置中已有的配置共享的 IP 或 DNS 相同。

步骤

- 1 在 Horizon Console 中，单击 **JMP 配置**。
- 2 单击 **UEM** 选项卡，然后单击 **添加**。
将显示 **添加 UEM 文件共享** 对话框。
- 3 在 **文件共享 UNC 路径** 文本框中以 `\\server-name\UEM-configuration-share-pathname` 格式输入一个值。
例如，如果配置共享位置为 `\\<IP-address>\uemshare\config\general\FlexRepository\...`，那么您需要在 **文件共享 UNC 路径** 文本框中输入的路径为 `\\<IP-address>\uemshare\config`。
- 4 输入连接 User Environment Manager 配置文件共享时必须使用的 User Environment Manager 用户名和密码。
- 5 从 **Active Directory** 列表中，选择要用于 User Environment Manager 配置文件共享的域名。

注 一个 Active Directory 只能与一个 User Environment Manager 配置文件共享关联。

- 6 单击 **保存**。

有关 User Environment Manager 配置文件共享的信息将添加到 JMP 设置中，并会在 **UEM** 选项卡上的表中添加一个新行。

编辑 User Environment Manager 配置文件共享信息

如果必须修改有关 JMP 分配所使用的 User Environment Manager 配置文件共享的现有信息，可以使用 Horizon Console。

步骤

- 1 在 Horizon Console 中，单击 **JMP 配置**。
- 2 单击 **UEM** 选项卡，然后从现有信息表中选择要修改的 User Environment Manager 配置文件共享所在的行。
- 3 单击 **编辑**。
将显示 **编辑 UEM 文件共享** 对话框。
- 4 修改需要更新的 User Environment Manager 配置文件共享信息。
- 5 单击 **保存**。

删除 User Environment Manager 配置共享信息

如果必须删除有关 User Environment Manager 配置共享的现有设置信息，请使用 Horizon Console。

仅当已注册的 User Environment Manager 配置共享未被任何 JMP 分配使用时，才能从 JMP 设置中删除有关该配置共享的信息。

步骤

- 1 在 Horizon Console 中，单击 **JMP 配置**。
- 2 单击 **UEM** 选项卡。
- 3 选择要从 JMP 设置中删除的 User Environment Manager 配置共享信息所在的行。
- 4 单击 **删除**以确认您要删除此 User Environment Manager 配置共享信息。

如果没有 JMP 分配使用此 User Environment Manager 配置共享，将移除此配置共享。

如果此 User Environment Manager 配置共享被任何 JMP 分配使用，会显示一个警告对话框。警告消息中包含使用该 User Environment Manager 配置共享的 JMP 分配的列表。仅当将 User Environment Manager 配置共享从 JMP 分配中移除，或删除使用该配置共享的那些 JMP 分配之后，才能删除此配置共享信息。

管理 JMP 分配

安装 JMP Server 并配置 JMP 设置后，可以开始使用 JMP Integrated Workflow 功能来创建、修改、复制或删除 JMP 分配。

必须先安装 JMP Server 并配置 JMP 设置，然后才能开始创建 JMP 分配。有关更多信息，请参阅《VMware Horizon JMP Server 安装和设置指南》和[首次配置 JMP 设置](#)。

在创建、编辑、复制或删除 JMP 分配前，请确保满足以下必备条件。

- 确认使用 JMP 设置注册的 Horizon 7 实例已启动且正在运行。
- 确保至少有一个 Active Directory 域使用 JMP 设置进行了注册。
- 确认使用 JMP 设置注册的 App Volumes 实例已启动且正在运行。
- 确认在 JMP 设置中定义的 User Environment Manager 配置共享已启动且正在运行。

注 不支持全局授权。

尝试创建、编辑、复制或删除 JMP 分配时，可能会收到一条消息，指出所尝试的操作未成功完成。例如，尝试访问其中一个底层 JMP 技术组件时可能会遇到某些问题，从而分配验证无法成功完成。可以在 JMP 分配摘要屏幕上，尝试通过执行以下操作之一来更正此问题。

- 单击**编辑**手动更正这些问题。
- 单击**修复**让 JMP Server 尝试修复当前 JMP 分配上发现的问题。
- 单击**强制删除**移除整个 JMP 分配。

本章讨论了以下主题：

- [创建 JMP 分配](#)
- [编辑 JMP 分配](#)
- [复制 JMP 分配](#)
- [删除 JMP 分配](#)

创建 JMP 分配

使用 Horizon Console，您可以创建 JMP 分配，然后使用它们来为用户或用户组创建桌面工作区。

您可以选择 Horizon 桌面池、App Volumes AppStack 和 User Environment Manager 设置以定义 JMP 分配。

前提条件

确保已满足第 15 章 管理 JMP 分配中列出的必备条件。

步骤

- 1 在 Horizon Console，单击**分配 (JMP)**。
- 2 单击**新建**。
- 3 在“新建分配”向导的**用户**选项卡中，输入 **Active Directory** 下拉列表旁边的几个字符，然后选择要包含在新 JMP 分配中的用户或用户组。
所选的用户或用户组将添加到“已选择的用户/组”部分中。
- 4 单击**下一步**。
- 5 在**桌面**选项卡中，选择要包含在 JMP 分配中的桌面池，然后单击**下一步**。
- 6 在**应用程序**选项卡中，单击想要包含在 JMP 分配中的应用程序名称旁边的复选框。选择完成后，单击**下一步**。
- 7 在**用户环境**选项卡中，确定是否要使用任何可用的用户环境设置来配置 JMP 分配。
 - 将**是否禁用 UEM 设置?** 设置为**否**时，单击**跳过**意味着 User Environment Manager 分配文件将不会保存到 User Environment Manager 配置共享中。所有 User Environment Manager 设置都将应用于使用当前所创建的 JMP 分配为用户创建的虚拟桌面工作区。
 - 将**是否禁用 UEM 设置?** 设置为**否**时，选择要应用于所创建的 JMP 分配的用户环境设置。单击**下一步**将使用选定的用户环境设置创建 User Environment Manager 分配文件。所选的设置将应用于使用当前所创建的 JMP 分配为用户创建的虚拟桌面工作区。
 - 将**是否禁用 UEM 设置?** 设置为**是**时，将从视图中移除可用用户环境设置列表。当您单击**下一步**时，会将空分配文件写入 User Environment Manager 配置共享。通过禁用 User Environment Manager 设置，可确保不会对使用当前所创建的 JMP 分配为用户创建的虚拟桌面工作区，应用任何用户环境设置。
- 8 在**定义**选项卡中，接受 JMP 分配的默认名称，或替换为其他名称，并添加描述（可选）。
- 9 在 **AppStack 连接**下拉列表中，选择何时将 AppStack 附加到 JMP 分配，然后单击**下一步**。
- 10 在**摘要**选项卡，查看新分配的详细信息。如果可以接受，请单击**提交**。如果必须进行更改，请单击**上一步**以进行调整。

新 JMP 分配将会排入队列，等待存储到 JMP 数据库，并添加到“JMP 分配”窗格中的分配列表中。将 JMP 分配成功添加到 JMP 数据库后，其状态会从“等待处理”发生更改。JMP 分配将变为可从 JMP 分配列表中进行选择，以便您能够对其执行编辑、复制或删除操作。

您还可以使用以下信息验证为新 JMP 分配创建的分配或授权。

- 要验证为 JMP 分配创建的有关 Horizon 桌面池的信息，请使用 Horizon Console。选择**清单 > 桌面**，然后找到 JMP Server 创建的桌面池。
- 要查看 JMP Server 为新 JMP 分配创建的 AppStack 信息，请使用 App Volumes Manager 控制台。选择**卷 > AppStack**，然后找到 JMP Server 创建的 AppStack。

- 要验证您为 JMP 分配配置的用户环境设置，请使用 **User Environment Manager** 管理控制台并单击 **用户环境** 选项卡。从左侧窗格中，选择 JMP 分配所使用的用户环境设置，然后在出现的对话框中单击 **分配** 选项卡，以查看该用户环境设置的 JMP 分配信息。

编辑 JMP 分配

您可能会由于定义现有 JMP 分配时所使用的组件发生了更改而需要修改该分配。您可以使用 **Horizon Console** 对 JMP 分配做出必要的更改。

前提条件

- 确保已满足第 15 章 **管理 JMP 分配** 中列出的必备条件。
- 您计划编辑的 JMP 分配不能处于“等待处理”状态。

步骤

- 1 在 **Horizon Console** 中，单击 **分配 (JMP)**。
- 2 通过单击复选框或列表中的 JMP 分配名称，选择要编辑的 JMP 分配。
- 3 单击 **编辑**。
- 4 在“编辑分配”向导中，修改当前设置。

如果要在编辑过程中的任何时候停止操作，请单击 **取消**。

- a 如果您要移除当前选定的任何用户或组，请单击删除图标 (X)。
- b 单击 **下一步**。
- c 在 **桌面** 选项卡中，选择要包括在 JMP 分配中的桌面池。单击 **下一步**。
- d 在 **应用程序** 选项卡中，选择要添加到 JMP 分配的可用应用程序，或取消选择之前选择的可用应用程序。单击 **下一步**。
- e 在 **用户环境** 选项卡中，确定是否要使用任何可用的用户环境设置来配置 JMP 分配。
 - 将 **是否禁用 UEM 设置?** 设置为 **否** 时，单击 **跳过** 意味着 **User Environment Manager** 分配文件将不会保存到 **User Environment Manager** 配置共享中。所有 **User Environment Manager** 设置都将应用于使用当前所编辑的 JMP 分配为用户创建的虚拟桌面工作区。
 - 将 **是否禁用 UEM 设置?** 设置为 **否** 时，选择要应用于所创建的 JMP 分配的用户环境设置。单击 **下一步** 将使用选定的用户环境设置创建 **User Environment Manager** 分配文件。选定的设置将应用于使用当前所编辑的 JMP 分配为用户创建的虚拟桌面工作区。
 - 将 **是否禁用 UEM 设置?** 设置为 **是** 时，将从视图中移除可用用户环境设置列表。当您单击 **下一步** 时，会将空分配文件写入 **User Environment Manager** 配置共享。通过禁用 **User Environment Manager** 设置，可确保不会对使用当前所编辑的 JMP 分配为用户创建的虚拟桌面工作区，应用任何用户环境设置。
- f 在 **定义** 选项卡中，（如果适用）修改 **名称** 和 **描述** 的当前值或将 **AppStack** 附加到 JMP 分配的时间。

- g 单击**下一步**。
- h 查看所做更改的摘要，然后单击**提交**以保存修改。

如果提交成功，会保存所做的更改。如果遇到任何问题，会提供进一步信息，同时显示您可以执行的可行操作。

复制 JMP 分配

可以通过复制与想要创建的 JMP 分配相似的现有 JMP 分配，更快速地创建 JMP 分配。

前提条件

- 确保已满足第 15 章 [管理 JMP 分配](#)中列出的必备条件。
- 计划复制的 JMP 分配不能为“等待处理”或“错误”状态。

步骤

- 1 从 Horizon Console 中，选择**分配 (JMP)**。
- 2 选择要复制的 JMP 分配，然后单击**复制**。
- 3 在“新建分配”向导中，根据需要修改复制的 JMP 分配。
 - a 选择新用户或组，或者移除所有当前选定的用户或组。单击**下一步**。
 - b 在“桌面”窗格中，选择一个新的桌面池，或移除所复制的 JMP 分配中包含的任何桌面池。单击**下一步**。
 - c 选择要包含在新 JMP 分配中的其他应用程序，并取消选择当前选定的应用程序。单击**下一步**。
 - d 在“用户环境”窗格中，选择要应用于新 JMP 分配的 User Environment Manager 设置。单击**下一步**。
 - e 在“定义名称”中，可以根据需要替换所创建的默认名称。添加描述，然后指定希望将 AppStack 附加到新 JMP 分配的时间。
 - f 单击**下一步**，然后查看新 JMP 分配的详细信息摘要。
 - g 如果对这些信息满意，请单击**提交**。否则，请单击**上一步**进行任何更正。

将验证新 JMP 分配，这可能需要一些时间。验证成功后，会将新创建的 JMP 分配添加到“JMP 分配”窗格上的列表中。将指针放到该分配的名称上时，可以看到它处于等待处理状态，直至成功保存到 JMP 数据库为止。JMP 分配不再处于等待处理状态后，可以对该分配执行任何其他操作。

删除 JMP 分配

可以使用 Horizon Console 删除 JMP 分配。

删除 JMP 分配后，将删除与 JMP 分配关联的 Horizon 池授权、AppStack 分配和 UEM 授权。但是，如果 JMP 分配使用的 Horizon 池授权或 AppStack 分配在创建 JMP 分配之前就存在，将不会被删除。删除 JMP 分配后，它将不再应用于用户或桌面。

前提条件

- 确认已满足第 15 章 管理 JMP 分配中列出的必备条件。
- 计划删除的 JMP 分配不能为“等待处理”状态。

步骤

- 1 在 Horizon Console 中，单击**分配 (JMP)**。
- 2 在“JMP 分配”窗格中，选择一个或多个 JMP 分配，然后单击**删除**。
- 3 在确认对话框中，单击**删除**以确认您要永久删除此分配。

如果删除成功，将从 JMP 数据库以及“JMP 分配”窗格的列表中移除 Horizon 池授权。

如果删除操作未完全成功，将不会删除 JMP 分配。单击状态指示器可提供有关删除操作失败原因的更多信息。

在 Horizon Console 中配置事件报告

16

您可以创建事件数据库来记录有关 Horizon 7 事件的信息。此外，如果您使用 Syslog 服务器，则可以对连接服务器进行配置，使其向 Syslog 服务器发送事件或创建以 Syslog 格式编写的事件平面文件。

本章讨论了以下主题：

- 在 Horizon Console 中为 Horizon 7 事件添加数据库和数据库用户
- 在 Horizon Console 中为事件报告准备 SQL Server 数据库
- 在 Horizon Console 中配置事件数据库
- 在 Horizon Console 中为 Syslog 服务器配置事件日志记录
- 在 Horizon 7 中监控事件

在 Horizon Console 中为 Horizon 7 事件添加数据库和数据库用户

您可以通过将事件数据库添加到现有数据库服务器，从而创建一个事件数据库。之后，便可以使用报告软件来分析数据库中的事件。

在专用服务器上部署事件数据库的数据库服务器，以便事件日志记录活动不会影响置备和对 Horizon 7 部署比较重要的其他活动。

注 您无需为此数据库创建 ODBC 数据源。

前提条件

- 确认在连接服务器实例可访问的系统上具有支持的 Microsoft SQL Server 或 Oracle 数据库服务器。
有关受支持的数据库的最新信息，请参阅 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php 上的“VMware 产品互操作性列表”。有关**解决方案/数据库互操作性**，选择产品和版本后，在“添加数据库”步骤中选择**任意**，然后单击**添加**可查看所有受支持的数据库的列表。
- 确认您拥有在数据库服务器上创建数据库和用户所需的数据库特权。
- 如果您不熟悉在 Microsoft SQL Server 数据库服务器上创建数据库的过程，请参阅《Horizon 7 安装指南》文档中的“将 View Composer 数据库添加到 SQL Server”。
- 如果您不熟悉在 Oracle 数据库服务器上创建数据库的过程，请参阅《Horizon 7 安装指南》文档中的“将 View Composer 数据库添加到 Oracle 12c 或 11g”。

步骤

- 1 向服务器中添加一个数据库，并为其提供一个描述性名称，如 **HorizonEvents**。

对于 Oracle 12c 或 Oracle 11g 数据库，还需要提供 Oracle 系统标识符 (System Identifier, SID)，当您在 Horizon Console 中配置事件数据库时将使用该标识符。

- 2 为该数据库添加一个用户，该用户应具有创建表、视图、Oracle 触发器和序列的权限，以及读写这些对象的权限。

对于 Microsoft SQL Server 数据库，不要使用集成 Windows 身份验证 (Integrated Windows Authentication) 安全模式方法进行身份验证。请确认您使用的是 SQL Server 身份验证方法进行身份验证。

随即会创建数据库，但模式将在 Horizon Console 中配置数据库之后才会安装。

后续步骤

按照在 [Horizon Console 中配置事件数据库](#) 中的说明操作。

在 Horizon Console 中为事件报告准备 SQL Server 数据库

您必须先配置正确的 TCP/IP 属性并确认 Microsoft SQL Server 使用了 SQL Server 身份验证，然后才能使用 Horizon Console 在该服务器上配置事件数据库。

前提条件

- 为事件报告创建一个 SQL Server 数据库。请参阅在 [Horizon Console 中为 Horizon 7 事件添加数据库和数据库用户](#)。
- 确认您拥有配置数据库所需的数据库特权。
- 确认数据库服务器使用 SQL Server 身份验证方法。不要使用 Windows 身份验证。

步骤

- 1 打开 SQL Server Configuration Manager 并展开 **SQL Server YYYY 网络配置**。
- 2 选择 **server_name** 使用的协议。
- 3 在协议列表中，右键单击 **TCP/IP** 并选择**属性**。
- 4 将已启用属性设置为**是**。
- 5 确认已分配了一个端口，或者在必要时分配一个端口。

有关静态和动态端口以及如何分配端口的信息，请参阅 SQL Server Configuration Manager 的联机帮助。

- 6 确认该端口未被防火墙阻止。

后续步骤

使用 Horizon Console 将数据库连接到连接服务器。按照在 [Horizon Console 中配置事件数据库](#) 中的说明操作。

在 Horizon Console 中配置事件数据库

事件数据库会将有关 Horizon 7 事件的信息存储为数据库记录，而不是日志文件记录。

安装连接服务器实例后，您便可以配置事件数据库。您只需要在连接服务器组中配置一个主机。组中剩余的主机会自动进行配置。

注 确保连接服务器实例与外部数据库之间的数据库连接安全是管理员的职责，但事件流量仅限于有关 Horizon 7 环境运行状况的信息。如果想采取额外的预防措施，可以通过 IPsec 或其他途径保护此通道的安全，也可以在连接服务器计算机本地部署数据库。

您可使用 Microsoft SQL Server 或 Oracle 数据库报告工具检查数据库表中的事件。有关更多信息，请参阅《Horizon 7 集成指南》文档。

您还可以生成 Syslog 格式的 Horizon 7 事件，以便第三方分析软件能够访问事件数据。您可以使用带 -I 选项的 vdmadmin 命令以 Syslog 格式在事件日志文件中记录 Horizon 7 事件消息。请参阅《Horizon 7 管理指南》文档中的“使用 -I 选项生成 Syslog 格式的 Horizon 7 事件日志消息”。

前提条件

配置事件数据库时需要以下信息：

- 数据库服务器的 DNS 名称或 IP 地址。
- 数据库服务器的类型：Microsoft SQL Server 或 Oracle。
- 用来访问数据库服务器的端口号。适用于 Oracle 的默认端口号是 1521；适用于 SQL Server 的默认端口号是 1433。对于 SQL Server，如果数据库服务器是已经命名的实例，或者您使用的是 SQL Server Express，您可能需要确定端口号。有关连接到已命名的 SQL Server 实例的信息，请参阅 <http://support.microsoft.com/kb/265808> 上的 Microsoft 知识库文章。
- 您在数据库服务器上创建的事件数据库名称。请参阅在 [Horizon Console 中为 Horizon 7 事件添加数据库和数据库用户](#)。

对于 Oracle 12c 或 11g 数据库，在 Horizon Console 中配置事件数据库时，必须使用 Oracle 系统标识符 (SID) 作为数据库名称。

- 为该数据库创建的用户的用户名和密码。请参阅在 [Horizon Console 中为 Horizon 7 事件添加数据库和数据库用户](#)。

为该用户使用 SQL Server 身份验证 (SQL Server Authentication)。不要使用集成 Windows 身份验证 (Integrated Windows Authentication) 安全模式方法进行身份验证。

- 事件数据库中表的前缀，如 VE_。通过添加前缀，可在安装的 Horizon 7 之间共享数据库。

注 您必须输入对当前使用的数据库软件有效的字符。填写完对话框时不会对前缀语法进行检查。如果输入的字符对当前使用的数据库软件无效，则当连接服务器尝试连接数据库服务器时将会出现错误。日志文件会提示所有错误，其中包括该错误和数据库名称无效时从数据库服务器返回的任何其他错误。

步骤

- 1 在 Horizon Console 中，选择 **设置 > 事件配置**。

- 2 在**事件数据库**区域中，单击**编辑**，然后在提供的字段中输入信息，最后单击**确定**。

要清除事件数据库信息，请单击**清除**。

- 3 （可选）在”事件设置“窗口中，单击**编辑**，分别更改事件的显示时间长度以及将事件归为新事件的天数，然后单击**确定**。

这些设置可控制事件在 Horizon Console 界面中显示的时间长度。在此之后，事件仅在历史数据库表中可见。

- 4 选择**监视 > 事件**，确认已成功连接到事件数据库。

如果连接失败，则会显示错误消息。如果您使用 SQL Express 或命名的 SQL Server 实例，您可能需要确定正确的端口号，如前提条件中提到的端口号。

在 Horizon Console 中为 Syslog 服务器配置事件日志记录

您可以生成 Syslog 格式的 Horizon 7 事件，以便分析软件能够访问事件数据。

您只需要在连接服务器组中配置一个主机。组中剩余的主机会自动进行配置。

如果启用基于文件的事件日志记录，则事件会在本地日志文件中累积。如果指定文件共享，这些日志文件将移至该共享中。

- 仅在配置期间进行快速故障排除时（可能在配置事件数据库之前）使用本地文件，这样就有办法查看事件。

在删除最早的文件之前，事件日志记录的本地目录最大（包含已关闭的日志文件）为 300MB。Syslog 输出的默认目标位置为 %PROGRAMDATA%\VMware\VDM\events\。

- 对于时间很长的事件记录，或者如果您没有 Syslog 服务器，或者当前的 Syslog 服务器无法满足您的要求，请使用 UNC 路径保存日志文件。

您也可以使用 vdmadmin 命令以 Syslog 格式配置基于文件的事件日志记录。请参阅《Horizon 7 管理指南》文档中有关使用 vdmadmin 命令的 -I 选项生成 Syslog 格式的 Horizon 7 事件日志消息的主题。

重要事项 Syslog 数据在不采用软件加密的情况下跨网络传输，它可能包含敏感数据，例如用户名。VMware 建议使用链路层安全机制（例如 IPSEC）来避免这类数据在网络上受到监视。

前提条件

配置连接服务器时需要使用以下信息，以便能以 Syslog 格式记录事件和/或将事件发送到 Syslog 服务器：

- 如果您计划使用 Syslog 服务器侦听 UDP 端口上的 Horizon 7 事件，您必须具有 Syslog 服务器的 DNS 名称或 IP 地址以及 UDP 端口号。默认 UDP 端口号为 514。
- 如果您计划以平面文件格式收集日志，则必须拥有指向存有日志文件的文件共享和文件夹的 UNC 路径，同时还必须具备有权对文件共享执行写入操作的帐户的用户名、域名和密码。

步骤

- 1 在 Horizon Console 中，选择**设置 > 事件配置**。

- 2 （可选）在 **Syslog** 区域，要将连接服务器配置为向 Syslog 服务器发送事件，请单击 **发送到 Syslog 服务器** 下方的 **添加**，然后提供服务器名称或 IP 地址以及 UDP 端口号。
- 3 （可选）要以 Syslog 格式生成 Horizon 7 事件日志消息并将其存储在日志文件中，请选中 **记录到文件：启用** 复选框。

如果不指定文件共享的 UNC 路径，日志文件会保留在本地。

- 4 （可选）要将 Horizon 7 事件日志消息存储在文件共享中，请单击 **复制到位置** 下方的 **添加**，然后提供文件共享的 UNC 路径和用于存储日志文件的文件夹，以及具有文件共享写入权限的帐户的用户名、域名和密码。

以下是 UNC 路径示例：

```
\\syslog-server\folder\file
```

在 Horizon 7 中监控事件

事件数据库存储了连接服务器主机或组、Horizon Agent 以及 Horizon Console 中所发生事件的相关信息，并会在仪表板中显示事件数量。您可以在 **事件** 页面上查看事件的详细信息。

注 事件会在 Horizon Console 界面中持续显示一段有限的时间。在此之后，事件仅在历史数据库表中可见。您可使用 Microsoft SQL Server 或 Oracle 数据库报告工具检查数据库表中的事件。有关更多信息，请参阅《Horizon 7 集成指南》文档。

注 如果事件数据库变得不可用，Horizon 7 将保留在此不可用期间发生的事件的审计记录，待事件数据库变得可用后，再将这些记录保存到事件数据库。您必须重新启动事件数据库和连接服务器，才能在 Horizon Console 界面中查看这些事件。

除了监控 Horizon Console 中的事件外，还可以生成 Syslog 格式的 Horizon 7 事件，从而允许分析软件访问事件数据。请参阅《Horizon 7 安装指南》文档中的 [在 Horizon Console 中为 Syslog 服务器配置事件日志记录](#) 和“使用 -l 选项以 Syslog 格式生成 Horizon 7 事件日志消息”。

如果为多个连接服务器配置了事件数据库，则 Horizon Console 将在 **事件** 页面上显示与所有连接服务器相关的事件。Horizon Console 会根据您执行的任务筛选事件，并在相关页面上显示这些事件，例如 **桌面池** 页面或 **应用程序池** 页面。

前提条件

按照《Horizon 7 安装指南》文档中所述，创建并配置事件数据库。

步骤

- 1 在 Horizon Console 中，选择 **监控 > 事件**。
- 2 （可选）在 **事件** 页面上，您可以选择事件的时间范围，对事件应用筛选器，并在一个或多个列中对列出的事件进行排序。

后续步骤

在 Horizon Console 中，导航到桌面或应用程序池、虚拟机、永久磁盘、用户或组，然后单击**事件**选项卡以查看特定事件。

Horizon 7 事件消息

每当系统状态变化或者遇到问题时，Horizon 7 均会报告发生的事件。您可以根据事件消息中的信息来采取适当措施。

下表显示了 Horizon 7 报告的事件类型。

表 16-1. Horizon 7 所报告事件的类型

事件类型	说明
Audit Failure（审核失败）或 Audit Success（审核成功）	报告管理员或用户对 Horizon 7 的操作或配置所做的更改是否成功。
错误	报告 Horizon 7 所执行的错误操作。
信息	报告 Horizon 7 内的正常操作。
警告	报告在操作或配置设置中，今后有可能导致更严重问题的轻微问题。

如果您看到与“审核失败”、“错误”或“警告”事件相关的消息，则可能需要采取相应的措施。对于“审核成功”或“信息”事件，则不需要采取措施。

在 Horizon Console 中使用 Horizon Help Desk Tool

17

Horizon Help Desk Tool 是一个 Web 应用程序，可用于获取 Horizon 7 用户会话的状态以及执行故障排除和维护操作。

在 Horizon Help Desk Tool 中，您可以查找要对问题进行故障排除的用户会话，还可以执行桌面维护操作，如重新启动或重置桌面。

要配置 Horizon Help Desk Tool，必须满足以下要求：

- Horizon 7 的 Horizon Enterprise 版许可证或 Horizon Apps Advanced 版许可证。要确认您具有正确的许可证，请参阅《Horizon 7 管理指南》文档。
- 用来存储 Horizon 7 组件相关信息的事件数据库。有关配置事件数据库的更多信息，请参阅《Horizon 7 安装指南》文档。
- 用来登录到 Horizon Help Desk Tool 的“技术支持管理员”角色或“技术支持管理员 (只读)”角色。有关这些角色的更多信息，请参阅《Horizon 7 管理指南》文档。
- 在每个连接服务器实例上启用时间安排分析器，以查看登录分段。

使用以下 `vdadmin` 命令可在每个连接服务器实例上启用时间安排分析器：

```
vdadmin -I -timingProfiler -enable
```

使用以下 `vdadmin` 命令可在管理端口的连接服务器实例上启用时间安排分析器：

```
vdadmin -I -timingProfiler -enable -server {ip/server}
```

本章讨论了以下主题：

- [在 Horizon Console 中启动 Horizon Help Desk Tool](#)
- [在 Horizon Help Desk Tool 中对用户进行故障排除](#)
- [Horizon Help Desk Tool 的会话详细信息](#)
- [Horizon Help Desk Tool 的会话进程](#)
- [Horizon Help Desk Tool 的应用程序状态](#)
- [在 Horizon Help Desk Tool 中对桌面或应用程序会话进行故障排除](#)

在 Horizon Console 中启动 Horizon Help Desk Tool

Horizon Help Desk Tool 已集成到 Horizon Console 中。您可以搜索要在 Horizon Help Desk Tool 中为其排除故障的用户。

步骤

- 1 在 Horizon Console 的“用户搜索”字段中输入用户名。

Horizon Console 会在搜索结果中显示用户的列表。搜索最多可返回 100 个匹配结果。

- 2 选择一个用户名。

用户卡中将会显示相应的用户信息。

后续步骤

要对问题进行故障排除，请单击用户卡中的相关选项卡。

在 Horizon Help Desk Tool 中对用户进行故障排除

在 Horizon Help Desk Tool 中，您可以在用户卡中查看基本用户信息。您可以单击用户卡中的选项卡以获取有关特定组件的更多详细信息。

用户详细信息有时会显示在表中。您可以按表列对这些用户详细信息进行排序。

- 要按升序对某列进行排序，请单击该列一次。
- 要按降序对某列进行排序，请单击该列两次。
- 要不对该列进行排序，请单击该列三次。

基本用户信息

显示基本用户信息，例如用户的用户名、电话号码和电子邮件地址，以及用户的状态（已连接或已断开连接）。如果用户具有桌面或应用程序会话，则用户的状态为已连接。如果用户没有任何桌面或应用程序会话，则用户的状态为已断开连接。

您可以单击电子邮件地址来向用户发送消息。

您还可以单击电话号码打开 **Skype for Business** 会话，以致电用户来与其协作完成故障排除任务。

注 对于 Linux 桌面用户，不会显示 Skype for Business 信息。

会话

会话选项卡显示有关用户连接到的桌面或应用程序会话的信息。

您可以使用**筛选器**文本框筛选桌面或应用程序会话。

注 对于使用 Microsoft RDP 显示协议的会话，或者从 vSphere Client 或 ESXi 访问虚拟机的会话，会话选项卡不显示相应的会话信息。

会话选项卡包含以下信息：

表 17-1. “会话”选项卡

选项	说明
状态	<p>显示有关桌面或应用程序会话状态的信息。</p> <ul style="list-style-type: none"> ■ 如果会话已连接，则显示绿色。 ■ 如果会话是本地会话或在本地容器中运行的会话，则显示 L。
计算机名称	<p>桌面或应用程序会话的名称。单击该名称可在一个信息卡中打开会话信息。</p> <p>您可以单击会话信息卡中的选项卡以查看其他信息：</p> <ul style="list-style-type: none"> ■ 详细信息选项卡显示虚拟机信息、CPU 或内存使用情况等用户信息。 ■ 进程选项卡显示有关 CPU 和内存相关进程的信息。 ■ 应用程序选项卡显示有关正在运行的应用程序的详细信息。 <p>注 对于 Linux 桌面会话，您无法访问应用程序选项卡。</p>
协议	桌面或应用程序会话的显示协议。
类型	显示桌面是已发布的桌面、虚拟机桌面，还是应用程序。
连接时间	会话连接到连接服务器的时间。
会话持续时间	会话保持连接到连接服务器的时长。

桌面

桌面选项卡显示有关用户有权使用的已发布桌面或虚拟桌面的信息。

表 17-2. 桌面

选项	说明
状态	<p>显示有关桌面会话状态的信息。</p> <ul style="list-style-type: none"> ■ 如果会话已连接，则显示绿色。
桌面池名称	会话的桌面池的名称。对于 Linux 桌面会话，Linux 显示为桌面池。
桌面类型	<p>显示桌面是已发布的桌面，还是虚拟机桌面。</p> <p>注 如果会话在容器联合内的其他容器中运行，则不会显示任何信息。</p>
类型	<p>显示有关桌面授权类型的信息。</p> <ul style="list-style-type: none"> ■ 对于本地授权，显示“本地”。
vCenter	<p>显示 vCenter Server 中虚拟机的名称。</p> <p>注 如果会话在容器联合内的其他容器中运行，则不会显示任何信息。</p>
默认协议	桌面或应用程序会话的默认显示协议。

应用程序

应用程序选项卡显示有关用户有权使用的已发布应用程序的信息。

注 对于 Linux 桌面会话，您无法访问应用程序选项卡。

表 17-3. 应用程序

选项	说明
状态	显示有关应用程序会话状态的信息。 ■ 如果会话已连接，则显示绿色。
应用程序	显示应用程序池中已发布应用程序的名称。
场	会话连接到的 RDS 主机所在的场名称。 注 如果存在全局应用程序授权，此列显示全局应用程序授权中的场数量。
类型	显示有关应用程序授权类型的信息。 ■ 对于本地授权，显示“本地”。
发布者	已发布的应用程序的软件制造商名称。

活动

活动选项卡显示有关用户活动的事件日志信息。您可以按时间范围（如过去 12 小时或过去 30 天）或按管理员名称筛选活动。单击**仅技术支持事件**可仅按 Horizon Help Desk Tool 活动进行筛选。单击刷新图标可刷新事件日志。单击导出图标可将事件日志导出为文件。

注 在 Cloud Pod 架构环境中，不会显示用户的事件日志信息。

表 17-4. 活动

选项	说明
时间	选择时间范围。默认值为过去 12 小时。 ■ 过去 12 小时 ■ 过去 24 小时 ■ 过去 7 天 ■ 过去 30 天 ■ 全部
管理员	管理员用户的名称。
消息	向用户或管理员显示特定于用户或管理员所执行活动的消息。
资源名称	显示有关执行活动时所在的桌面池或虚拟机名称的信息。

Horizon Help Desk Tool 的会话详细信息

单击会话选项卡的计算机名称选项中的用户名时，会话详细信息会显示在详细信息选项卡中。您可以查看 Horizon Client、虚拟或已发布桌面以及 CPU 和内存的详细信息。

Horizon Client

显示的信息取决于 Horizon Client 的类型，这些信息包括用户名、Horizon Client 的版本、客户端计算机的 IP 地址和客户端计算机的操作系统等详细信息。

注 如果升级了 Horizon Agent，您还必须将 Horizon Client 升级到最新版本。否则，不会显示 Horizon Client 的版本。有关升级 Horizon Client 的更多信息，请参阅《Horizon 7 升级指南》文档。

虚拟机

显示有关虚拟桌面或已发布桌面的信息。

表 17-5. 虚拟机详细信息

选项	说明
计算机名称	桌面或应用程序会话的名称。
代理版本	Horizon Agent 版本。
操作系统版本	操作系统版本。
连接服务器	会话连接到的连接服务器。
池	桌面或应用程序池的名称。对于 Linux 桌面池，显示 Linux。
vCenter	vCenter Server 的 IP 地址。
会话状态	桌面或应用程序会话的状态。会话状态可能是空闲、活动或已断开。如果用户处于不活动状态的时间达到一分钟，则会话状态会变为空闲。状态图标显示绿色轮廓时表示空闲，显示纯绿色时表示活动，显示灰色时表示已断开连接。 注 Linux 桌面会话不显示空闲状态。
会话持续时间	会话保持连接到连接服务器的时间。
状态持续时间	会话保持处于同一状态的时间。
登录时间	用户登录到会话的时间。
登录时长	用户保持登录到会话的时间。
网关/代理名称	安全服务器、Unified Access Gateway 设备或负载均衡器的名称。此信息在连接到会话之后可能需要 30 到 60 秒才能显示。
网关/代理 IP	安全服务器、Unified Access Gateway 设备或负载均衡器的 IP 地址。此信息在连接到会话之后可能需要 30 到 60 秒才能显示。
场	已发布的桌面或应用程序会话的 RDS 主机的场。

用户体验衡量指标

显示使用 PCoIP 或 VMware Blast 显示协议的虚拟或已发布桌面会话的性能详细信息。要查看这些性能详细信息，请单击[更多](#)。要刷新这些详细信息，请单击刷新图标。

表 17-6. PCoIP 显示协议详细信息

选项	说明
TX 带宽	PCoIP 会话中的传输带宽（单位为 kbps）。
帧速率	PCoIP 会话中的帧速率（帧/秒）。
数据包丢失	PCoIP 会话中的数据包丢失百分比。
Skype 状态	PCoIP 会话中的 Skype for Business 状态。 <ul style="list-style-type: none"> ■ 已优化 ■ 回退 ■ 已优化 (版本不匹配) ■ 回退 (版本不匹配) ■ 正在连接 ■ 已断开连接 ■ 未定义 对于 Linux 桌面会话，此选项显示为“不适用”。

表 17-7. Blast 显示协议详细信息

选项	说明
帧速率	Blast 会话中的帧速率（帧/秒）。
Skype 状态	Blast 会话中的 Skype for Business 状态。 <ul style="list-style-type: none"> ■ 已优化 ■ 回退 ■ 已优化 (版本不匹配) ■ 回退 (版本不匹配) ■ 正在连接 ■ 已断开连接 ■ 未定义 对于 Linux 桌面会话，此选项显示为“不适用”。
BLAST 会话计数器	<ul style="list-style-type: none"> ■ 估计的带宽 (上行链路)。上行链路信号的估计带宽。 ■ 数据包丢失 (上行链路)。上行链路信号的数据包丢失百分比。
BLAST 图像处理计数器	<ul style="list-style-type: none"> ■ 发送的字节数。为进行 Blast 会话而发送的图像处理数据的总字节数。 ■ 接收的字节数。为进行 Blast 会话而接收的图像处理数据的总字节数。

选项	说明
BLAST 音频计数器	<ul style="list-style-type: none"> ■ 发送的字节数。为进行 Blast 会话而发送的音频数据的总字节数。 ■ 接收的字节数。为进行 Blast 会话而接收的音频数据的总字节数。
BLAST CDR 计数器	<ul style="list-style-type: none"> ■ 发送的字节数。为进行 Blast 会话而发送的客户端驱动器重定向数据的总字节数。 ■ 接收的字节数。为进行 Blast 会话而接收的客户端驱动器重定向数据的总字节数。

CPU 和内存使用情况及网络和磁盘性能

显示虚拟或已发布桌面或应用程序的 CPU 和内存使用情况图表，以及 PCoIP 或 Blast 显示协议的网络或磁盘性能图表。

注 在桌面上启动或重新启动 Horizon Agent 后，性能图表可能不会立即显示时间轴。时间轴会在几分钟后显示。

表 17-8. CPU 使用情况

选项	说明
会话 CPU	当前会话的 CPU 使用情况。
主机 CPU	向其分配会话的虚拟机的 CPU 使用情况。

表 17-9. 内存使用情况

选项	说明
会话内存	当前会话的内存使用情况。
主机内存	向其分配会话的虚拟机的内存使用情况。

表 17-10. 网络性能

选项	说明
延迟	<p>显示 PCoIP 或 Blast 会话的延迟图表。</p> <p>对于 Blast 显示协议，延迟时间为往返时间（以毫秒为单位）。用于跟踪此延迟时间的性能计数器是 VMware Blast 会话计数器 > RTT。</p> <p>对于 PCoIP 显示协议，延迟时间为往返延迟时间（以毫秒为单位）。用于跟踪此延迟时间的性能计数器是 PCoIP 会话网络统计信息 > 往返延迟。</p>

表 17-11. 磁盘性能

选项	说明
读取	每秒读取输入/输出 (Input/Output, I/O) 操作的次数。
写入	每秒写入 I/O 操作的数量。

选项	说明
磁盘延迟	显示磁盘延迟的图表。磁盘延迟是从 Windows 性能计数器中检索每秒输入/输出操作 (Input/Output Operations Per Second, IOPS) 数据的时间 (以毫秒为单位)。
平均读取速率	每秒随机读取 I/O 操作的平均次数。
平均写入速率	每秒随机写入 I/O 操作的平均次数。
平均延迟	从 Windows 性能计数器中检索 IOPS 数据的平均延迟时间 (以毫秒为单位)。

会话登录分段

显示登录时长以及在登录过程中创建的使用情况分段。

表 17-12. 会话登录分段

选项	说明
登录时长	该时长从用户单击桌面或应用程序池时开始计算，直到 Windows 资源管理器启动时为止。
会话登录时间	用户登录到会话的时间长度。
登录分段	<p>显示在登录过程中创建的分段。</p> <ul style="list-style-type: none"> ■ 代理。连接服务器处理会话连接或重新连接的总时间。从用户单击桌面池时开始计算，直到设置了安全加密链路连接时为止。包括完成各项连接服务器任务 (例如用户身份验证、计算机选择和为设置安全加密链路连接准备计算机) 所用的时间。 ■ GPO 加载。处理 Windows 组策略的总时间。如果未配置全局策略，则显示 0。 ■ 配置文件加载。处理 Windows 用户配置文件的总时间。 ■ 交互式。Horizon Agent 处理会话连接或重新连接的总时间。从 PCoIP 或 Blast Extreme 使用安全加密链路连接时开始计算，直到 Windows 资源管理器启动时为止。 ■ 协议连接。在登录过程中完成 PCoIP 或 Blast 协议连接所用的总时间。 ■ 登录脚本。登录脚本从开始执行到完成所用的总时间。 ■ 身份验证。连接服务器对会话进行身份验证的总时间。 ■ 虚拟机启动。启动虚拟机所用的总时间。该时间包括引导操作系统、恢复挂起的计算机的时间，以及 Horizon Agent 发出信号表明它已做好连接准备的时间。

在使用登录分段中的信息进行故障排除时，以下准则适用：

- 如果会话是新的虚拟桌面会话，将显示所有登录分段。如果未配置任何全局策略，则 **GPO 加载** 登录分段的时间为 0。
- 如果虚拟桌面会话是断开连接后重新连接的会话，将显示 **登录时长**、**交互式** 和 **代理** 登录分段。

- 如果会话是已发布的桌面会话，将显示**登录时长**、**GPO 加载**或**配置文件加载**登录分段。新会话将显示**GPO 加载**和**配置文件加载**登录分段。如果新会话没有显示这些登录分段，则必须重新启动 RDS 主机。
- 如果会话是 Linux 桌面会话，则不会显示 **GPO 加载**和**配置文件加载**分段。
- 在连接桌面会话时不会立即显示登录数据。登录数据会在几分钟后显示。

Horizon Help Desk Tool 的会话进程

单击**会话**选项卡的**计算机名称**选项中的用户名时，会话进程会显示在**进程**选项卡中。

进程

对于每个会话，您可以查看有关 CPU 和内存相关进程的其他详细信息。例如，如果您发现会话的 CPU 和内存使用情况异常高，则可以在**进程**选项卡中查看该进程的详细信息。

对于 RDS 主机会话，**进程**选项卡会显示由当前用户或当前系统进程启动的当前 RDS 主机会话进程。

表 17-13. 会话进程详细信息

选项	说明
进程名称	会话进程的名称。例如， chrome.exe 。
CPU	进程的 CPU 使用情况，以百分比为单位。
内存	进程的内存使用情况，以 KB 为单位。
磁盘	内存磁盘 IOPS。使用以下公式进行计算： (当前时间的 I/O 总字节数) - (当前时间前一秒的 I/O 总字节数)。 如果任务管理器显示正值，此计算可以显示值为 0 KB/秒。
用户名	进程所属的用户的用户名。
主机 CPU	向其分配会话的虚拟机的 CPU 使用情况。
主机内存	向其分配会话的虚拟机的内存使用情况。
进程	虚拟机中的进程计数。
刷新	刷新图标可刷新进程列表。
结束进程	结束正在运行的进程。 注 您必须具有技术支持管理员角色才能结束进程。 要结束进程，请选择相应的进程，然后单击 结束进程 按钮。 您无法结束 进程 选项卡中可能会列出的关键进程，例如 Windows 核心进程。如果要结束某个关键进程，则 Horizon Help Desk Tool 会显示一条消息，指示其无法结束此系统进程。

Horizon Help Desk Tool 的应用程序状态

在会话选项卡上的计算机名称选项中单击某个用户名时，可以在应用程序选项卡中查看应用程序的状态和详细信息。对于 Linux 桌面会话，您无法访问应用程序选项卡。

应用程序

对于每个应用程序，可以查看当前状态以及其他详细信息。

您可以为最终用户结束应用程序进程。要结束应用程序进程，请单击**结束应用程序**，然后单击**确定**以确认更改。

注 如果应用程序正在等待用户交互（例如存在未保存的数据），或者由于出现其他异常，结束应用程序进程的操作可能会失败。但是，在您结束应用程序时，Horizon Help Desk Tool 不会显示任何成功或失败消息。

表 17-14. 应用程序详细信息

选项	说明
应用程序	应用程序的名称。
说明	应用程序的描述。
状态	应用程序的状态。显示应用程序是否正在运行。
主机 CPU	向其分配会话的虚拟机的 CPU 使用情况。
主机内存	向其分配会话的虚拟机的内存使用情况。
应用程序	正在运行的应用程序列表。
刷新	刷新图标可刷新应用程序列表。

在 Horizon Help Desk Tool 中对桌面或应用程序会话进行故障排除

在 Horizon Help Desk Tool 中，您可以根据用户的连接状态对桌面或应用程序会话进行故障排除。

前提条件

- 启动 Horizon Help Desk Tool。

步骤

- 1 在用户卡上，单击**会话**选项卡。

此时将出现一个性能卡，其中显示了 CPU 和内存使用情况，并包含有关 Horizon Client 以及虚拟桌面或已发布的桌面的信息。

2 选择一个故障排除选项。

选项	操作
发送消息	<p>向已发布的桌面或虚拟桌面上的用户发送消息。您可以选择消息的严重性以包含“警告”、“信息”或“错误”。</p> <p>单击发送消息，输入严重性类型和消息详细信息，然后单击提交。</p>
远程协助	<p>您可以为已连接的桌面或应用程序会话生成远程协助票证。管理员可以使用该远程协助票证控制用户的桌面并对问题进行故障排除。</p> <p>注 此功能不适用于 Linux 桌面用户。</p> <p>单击远程协助并下载技术支持票证文件。打开票证，并等待远程桌面上的用户接受该票证。您只能在 Windows 桌面上打开票证。用户接受票证之后，您可以与用户聊天并请求控制用户的桌面。</p> <p>注 技术支持远程协助功能基于 Microsoft 远程协助。您必须在已发布的桌面上安装 Microsoft 远程协助并启用远程协助功能。如果 Microsoft 远程协助存在连接或升级问题，技术支持远程协助可能无法启动。有关更多信息，请参阅 Microsoft 网站上的 Microsoft 远程协助文档。</p>
重新启动	<p>在虚拟桌面上启动 Windows 重新启动过程。此功能不适用于已发布的桌面或应用程序会话。</p> <p>单击重新启动 VDI。</p>
断开连接	<p>断开桌面或应用程序会话连接。</p> <p>单击更多 > 断开连接。</p>
注销	<p>对已发布的桌面或虚拟桌面启动注销过程，或对应用程序会话启动注销过程。</p> <p>单击更多 > 注销。</p>
重置	<p>启动虚拟机重置操作。此功能不适用于已发布的桌面或应用程序会话。</p> <p>单击更多 > 重置虚拟机。</p> <p>注 用户可能会丢失未保存的工作。</p>