

OpenManage Integration for VMware vCenter 版本 4.3

Web 客户端安装指南

注、小心和警告

① | **注:** “注” 表示帮助您更好地使用该产品的重要信息。

△ | **小心:** “小心” 表示可能会损坏硬件或导致数据丢失，并说明如何避免此类问题。

⚠ | **警告:** “警告” 表示可能会造成财产损失、人身伤害甚至死亡。

1 简介	5
OpenManage Integration for VMware vCenter 许可	5
主机和 vCenter 服务器的许可证要求	5
购买并上传软件许可证	6
上传许可证之后的选项	6
强制执行措施	7
重要注释中的参考信息	7
硬件要求	7
配置部署模式	8
BIOS、iDRAC 和 Lifecycle Controller 版本	8
PowerEdge 服务器支持的功能	11
PowerEdge 机箱支持的功能	13
已配置存储所需的空间	13
软件要求	13
OpenManage Integration for VMware vCenter 要求	13
端口信息	15
虚拟设备和受管节点	15
前提条件核对表	17
安装、配置和升级 OMIVV	17
下载 OpenManage Integration for VMware vCenter	17
使用 vSphere Web 客户端部署 OMIVV OVF	18
生成证书签名请求	19
上传 HTTPS 证书	19
以非管理员用户的身份注册 vCenter 服务器	20
注册 OpenManage Integration for VMware vCenter 和导入许可证文件	22
升级已注册的 vCenter	26
验证安装	26
更新虚拟设备存储库位置和虚拟设备	26
将 OMIVV 从现有版本升级至当前版本	27
通过备份和还原更新设备	27
注销较早版本的 OMIVV 后恢复 OMIVV	28
2 VMware vCenter 的设备配置	29
通过配置向导配置任务	29
查看配置向导“欢迎”对话框	29
选择 vCenter	30
创建连接配置文件	30
计划资源清册作业	32
运行保修检索作业	33
配置事件和警报	33
配置 SNMP 陷阱团体字符串	34

通过设置选项卡配置任务.....	34
设备设置.....	34
vCenter 设置.....	37
创建机箱配置文件.....	38
3 访问 Dell EMC 支持站点上的文档.....	40
4 相关说明文件.....	41

简介

本指南提供使用 PowerEdge 服务器安装和配置 OpenManage Integration for VMware vCenter (OMIVV) 的逐步说明。OMIVV 安装完成后，可在位于 Dell.com/support/manuals 的 *OpenManage Integration for VMware vCenter 用户指南* 中查看有关所有管理方面（包括资源清册管理、监测和警报、固件更新以及保修管理）的信息。

主题：

- [OpenManage Integration for VMware vCenter 许可](#)
- [重要注释中的参考信息](#)
- [硬件要求](#)
- [软件要求](#)
- [端口信息](#)
- [前提条件核对表](#)
- [安装、配置和升级 OMIVV](#)

OpenManage Integration for VMware vCenter 许可

OpenManage Integration for VMware vCenter 有两种类型的许可证：

- **评估许可证** — 当 OMIVV 设备首次开机时，将自动安装评估许可证。试用版包含一个评估许可证，可由 OpenManage Integration for VMware vCenter 管理五个主机（服务器）。此 90 天的试用版本是发货时随附的默认许可证。
- **标准许可证** — 完整产品版本中包含一个标准许可证，可用于最多 10 个 vCenter 服务器。您可以购买任何数量的由 OMIVV 管理的主机连接。

从评估许可证升级到完整标准许可证后，您将收到一封订单确认电子邮件，然后便可从 Dell Digital Locker 下载许可证文件。将许可证 .XML 文件保存到您的本地系统，并使用**管理控制台**上传新的许可证文件。

许可将显示以下信息：

- **最大 vCenter 连接许可证数** — 启用最多 10 个注册的和使用中的 vCenter 连接。
- **最大主机连接许可证数** — 已购买的主机连接数量。
- **使用中** — 使用中的 vCenter 连接或主机连接许可证的数量。对于主机连接，该数量代表已查找到并进行过资源清册的主机（或服务器）的数量。
- **可用** — 可供未来使用的 vCenter 连接或主机连接许可证的数量。

① | 注：标准许可证有效期仅为 3 或 5 年，而附加的许可证会附加到现有许可证，而不是覆盖。

购买许可证时，可从 Dell Digital Locker ([Dell Digital Locker](#)) 下载 .XML 文件（许可证密钥）。如果您无法下载许可证密钥，请转至 [订单支持](#) 找到您产品的区域 Dell 支持电话号码，联系 Dell 支持部门。

主机和 vCenter 服务器的许可证要求

以下是主机和 vCenter 的许可要求：

- 您可以购买许可证以支持 OMIVV 管理的 Dell EMC 服务器的数量。仅当主机添加到连接配置文件后，才能使用许可证。许可证与特定服务器无关联。

- 一个 OMIVV 实例最多可支持 10 个 vCenter 服务器。对于 vCenter 服务器数量没有单独的许可证。

购买并上传软件许可证

您正在运行的是试用版许可证，直到您升级到完整的产品版本。使用 [购买许可证](#) 链接以从产品导航至 Dell 网站，并购买许可证。购买后，使用 [管理控制台](#) 进行上传。

关于此任务

① 注: 使用试用许可证的情况下才会显示购买许可证选项。

步骤

- 1 在 OpenManage Integration for VMware vCenter 中，请执行以下任务之一：
 - 在许可选项卡中的软件许可证旁边，单击购买许可证。
 - 在使用入门选项卡中的基本任务下，单击购买许可证。
- 2 将从 Dell Digital Locker 下载的许可文件保存到已知位置。
- 3 在 Web 浏览器中，键入管理控制台 URL。
使用格式：`https://<ApplianceIPAddress>`
- 4 在管理控制台登录窗口中，键入密码并单击登录。
- 5 单击上传许可证。
- 6 在上传许可证窗口中，单击浏览导航到许可证文件。
- 7 选择该许可证文件，然后单击上传。

① 注: 许可证文件可能打包在 .zip 文件中。确保解压缩 .zip 文件，然后仅上传许可证 .xml 文件。许可证文件通常基于订单号命名，如 123456789.xml。

上传许可证之后的选项

新购买过程中的许可证文件

当您下订单购买新许可证时，您将收到 Dell 发出的有关订单确认的电子邮件，您可以从 [Dell Digital Locker](#) 上的 Dell Digital Locker 下载新的许可证文件。许可证采用 .xml 格式。如果许可证是 .zip 格式，请从 .zip 文件中提取 license.xml 文件，然后再上传。

堆叠许可证

从 OMIVV 2.1 版本开始，OMIVV 可通过叠加多个标准许可证来增加支持的主机数，但不超过上传的许可证中包含的主机总数。评估版许可证不能叠加。受支持的 vCenter 服务器数量不能通过叠加许可证来增加，它需要使用多个设备。

叠加许可证的功能存在一些限制。如果在现有的标准许可证到期前上传了新的标准许可证，这两个许可证将会叠加。然而，如果在现有许可证过期后上传了新的许可证，则只支持新许可证包含的主机数量。如果已上传了多个许可证，则支持的主机数是最后一个许可证上传时未过期许可证包含的主机总数。

过期许可证

超过支持期限（通常自购买之日起三或五年）的许可证将被阻止上传。如果许可证在上传后过期，现有主机的功能将继续，但无法升级到 OMIVV 的新版本。

更换许可证

如果您的订单出现问题，并且收到了 Dell 的更换许可证，则更换许可证包含的授权 ID 与之前的许可证相同。上传更换许可证时，如果已上传了具有相同授权 ID 的许可证，则更换许可证将被替换。

强制执行措施

设备的更新

当所有许可证已过期时，设备不得再更新到较新版本。请获取并上传新许可证，然后再尝试升级设备。

评估许可证

当评估许可证过期时，多个关键功能将停止工作，并显示一条错误消息。

将主机添加到连接配置文件

在尝试将主机添加到连接配置文件时，如果许可的第 11 代或更高代系主机的数量超出许可证数量，将无法添加更多主机。

重要注释中的参考信息

- 从 OMIVV 4.0 开始，仅支持 VMware vSphere Web 客户端，不支持 vSphere Desktop 客户端。
- 对于 vCenter 6.5 及更高版本，OMIVV 设备仅适用于 Flash 版本。OMIVV 设备不适用于 HTML5 版本。
- 对于使用 DNS 服务器，建议做法是：
 - OMIVV 仅支持 IPv4 IP 地址。虽然支持静态 IP 分配和 DHCP 分配，但建议您分配静态 IP 地址。部署具有有效的 DNS 注册的 OMIVV 设备，分配一个静态 IP 地址和主机名。一个静态 IP 地址可确保在系统重新启动过程中，OMIVV 设备的 IP 地址保持相同。
 - 确保 OMIVV 主机名条目存在于您 DNS 服务器的正向和反向查询区域中。

有关 vSphere 的 DNS 要求的更多信息，请参阅以下 VMware 链接：

- [vSphere 5.5 的 DNS 要求](#)
- [vSphere 6.0 的 DNS 要求](#)
- [vSphere 6.5 和平台服务控制器设备的 DNS 要求](#)
- 对于 OMIVV 设备模式，确保根据您的虚拟化环境在合适模式下部署 OMIVV。有关更多信息，请参阅 [配置部署模式](#)。
- 配置您的网络以匹配端口要求。有关更多信息，请参阅 [端口信息](#)。

硬件要求

OMIVV 为若干代 Dell EMC 服务器提供全面支持，为带有 iDRAC Express 或 Enterprise 的服务器提供完整功能支持。可在 [Dell.com/support/manuals](#) 上提供的 *OpenManage Integration for VMware vCenter Release Notes (OpenManage Integration for VMWare vCenter 发行说明)* 中了解大量关于平台要求的信息。要验证您的主机服务器是否符合要求，请参阅下列后续小节中的信息：

- 支持的服务器和最低 BIOS
- iDRAC 支持的版本（包括部署和管理）
- 对第 11 代和旧版服务器的 OMSA 支持和 ESXi 版本支持（包括部署和管理）

- 支持的 OMIVV 内存和空间

OMIVV 要求主板/网络子卡上的 LAN 能够同时访问 iDRAC 和 CMC 或 Management Module 系统管理网络和 vCenter 管理网络。

配置部署模式

关于此任务

确保满足所需部署模式的以下系统要求：

表. 1: 部署模式的系统要求

部署模式	主机数量	CPU 数	内存（以 GB 为单位）	最低存储
小	最多 250 个	2	8	44 GB
中	最多 500 个	4	16	44 GB
大	最多 1000 个	8	32	44 GB

① 注: 对于任何提及的部署模式，请确保通过使用保留为 OMIVV 虚拟设备保留足够的内存资源量。请参阅 vSphere 文档获取保留内存资源的相关步骤。

您可以选择相应的部署模式缩放 OMIVV 以匹配您环境中的节点数。

步骤

- 1 在设备管理页面中，向下滚动到**部署模式**。
此时会显示部署模式的配置值，例如**小**、**中**或**大**，默认情况下部署模式设置为**小**。
- 2 如果想要根据环境更新部署模式，请单击**编辑**。
- 3 在**编辑**模式下，确保前提条件得到满足后选择所需的部署模式。
- 4 单击**应用**。
系统会根据所设置部署模式所需的 CPU 和内存验证已分配的 CPU 和内存，然后会发生以下任一情况：
 - 如果验证失败，将会显示一条错误消息。
 - 如果验证成功，在您确认更改后，OMIVV 设备会重新启动，部署模式会更改。
 - 如果已设置所需的部署模式，则会显示一条消息。
- 5 如果部署模式已更改，请确认相关更改，然后继续重新引导 OMIVV 设备以便让部署模式更新。

① 注: 在 OMIVV 设备的引导过程中，系统会根据设置的部署模式验证分配的系统资源。如果分配的系统资源少于设置的部署模式，OMIVV 设备不会引导至登录屏幕。要引导 OMIVV 设备，请关闭 OMIVV 设备，将系统资源更新至现有设置的部署模式，然后按照**降级部署模式**任务操作。

降级部署模式

- 1 登录到管理控制台。
- 2 将部署模式更改到所需的级别。
- 3 关闭 OMIVV 设备并将系统资源更改到所需的级别。
- 4 开启 OMIVV 设备。

BIOS、iDRAC 和 Lifecycle Controller 版本

本节列出了启用 OpenManage Integration for VMware vCenter 的功能所需的 BIOS、iDRAC 和 Lifecycle Controller 版本。

建议您在使用 OMIVV 之前先通过使用 Repository Manager 或 Lifecycle Controller 的平台创建的可引导 ISO 将服务器更新至以下基本版本之一：

① 注：建议使用具有 OMIVV 4.3 的 Dell EMC OpenManage Enterprise-Modular 版本 1.00.01。

表. 2: PowerEdge 第 11 代服务器的 BIOS

服务器	最低版本
PowerEdge R210	1.8.2 或更高版本
PowerEdge R210II	1.3.1 或更高版本
PowerEdge R310	1.8.2 或更高版本
PowerEdge R410	1.9.0 或更高版本
PowerEdge R415	1.8.6 或更高版本
PowerEdge R510	1.9.0 或更高版本
PowerEdge R515	1.8.6 或更高版本
PowerEdge R610	6.1.0 或更高版本
PowerEdge R710	6.1.0 或更高版本
PowerEdge R710	6.1.0 或更高版本
PowerEdge R715	3.0.0 或更高版本
PowerEdge R810	2.5.0 或更高版本
PowerEdge R815	3.0.0 或更高版本
PowerEdge R910	2.5.0 或更高版本
PowerEdge M610	6.1.0 或更高版本
PowerEdge M610x	6.1.0 或更高版本
PowerEdge M710HD	5.0.1 或更高版本
PowerEdge M910	2.5.0 或更高版本
PowerEdge M915	2.6.0 或更高版本
PowerEdge T110 II	1.8.2 或更高版本
PowerEdge T310	1.8.2 或更高版本
PowerEdge T410	1.9.0 或更高版本
PowerEdge T610	6.1.0 或更高版本
PowerEdge T710	6.1.0 或更高版本

表. 3: PowerEdge 第 12 代服务器的 BIOS

服务器	最低版本
T320	1.0.1 或更高版本
T420	1.0.1 或更高版本
T620	1.2.6 或更高版本
M420	1.2.4 或更高版本

服务器	最低版本
M520	1.2.6 或更高版本
M620	1.2.6 或更高版本
M820	1.2.6 或更高版本
R220	1.0.3 或更高版本
R320	1.2.4 或更高版本
R420	1.2.4 或更高版本
R520	1.2.4 或更高版本
R620	1.2.6 或更高版本
R720	1.2.6 或更高版本
R720xd	1.2.6 或更高版本
R820	1.7.2 或更高版本
R920	1.1.0 或更高版本

表. 4: PowerEdge 第 13 代服务器的 BIOS

服务器	最低版本
R630	1.0.4 或更高版本
R730	1.0.4 或更高版本
R730xd	1.0.4 或更高版本
R430	1.0.4 或更高版本
R530	1.0.2 或更高版本
R830	1.0.2 或更高版本
R930	1.0.2 或更高版本
R230	1.0.2 或更高版本
R330	1.0.2 或更高版本
T630	1.0.2 或更高版本
T130	1.0.2 或更高版本
T330	1.0.2 或更高版本
T430	1.0.2 或更高版本
M630	1.0.0 或更高版本
M830	1.0.0 或更高版本
FC430	1.0.0 或更高版本
FC630	1.0.0 或更高版本
FC830	1.0.0 或更高版本

表. 5: PowerEdge 第 14 代服务器的 BIOS

服务器	最低版本
R940	1.0.0 或更高版本
R740	1.0.0 或更高版本
R740xd	1.0.0 或更高版本
R640	1.0.0 或更高版本
M640	1.0.0 或更高版本
T640	1.0.0 或更高版本
T440	1.0.0 或更高版本
R540	1.0.0 或更高版本
FC640	1.0.0 或更高版本
R6415	1.0.0 或更高版本
R7425	1.0.0 或更高版本
R7415	1.0.0 或更高版本
MX740C	1.0.0 或更高版本
MX840C	1.0.0 或更高版本

表. 6: 要部署的 iDRAC 和 Lifecycle Controller

代别	版本	
	iDRAC	Lifecycle Controller
PowerEdge 第 11 代服务器	模块式为 3.35，机架式或塔式为 1.85	1.5.2 或更高版本
PowerEdge 第 12 代服务器	2.30.30.30 或更高版本	2.30.30.30 或更高版本
PowerEdge 第 13 代服务器	2.30.30.30 或更高版本	2.30.30.30 或更高版本
PowerEdge 第 14 代服务器	3.00.00.00 和更高版本	3.00.00.00 和更高版本

表. 7: 云服务器的 BIOS 和 iDRAC 要求

型号	BIOS	带 Lifecycle Controller 的 iDRAC
C6320	1.0.2	2.30.30.30 或更高版本
C4130	1.0.2	2.30.30.30 或更高版本
C6420	1.0.0 或更高版本	3.00.00.00 或更高版本
C4140	1.0.0 或更高版本	3.00.00.00 或更高版本

PowerEdge 服务器支持的功能

由 OpenManage Integration for VMware vCenter 管理的主机支持以下功能：

表. 8: PowerEdge 服务器支持的功能

功能	平台		
	第 11 代	第 12 代和 13 代	第 14 代
硬件资源清册	是	是	是
事件和警报	是 (仅限 SNMP v1)	是 (SNMP v1 和 v2)	是 (SNMP v1 和 v2)
组件级运行状况监测*	是	是	是
BIOS/固件更新#	是	是	是
主动式高可用性\$	否	是	是
保修信息	是	是	是
主机符合性	是	是	是
自动/手动发现裸机服务器	是	是	是
裸机合规性	是	是	是
硬件配置	是	是	是
裸机虚拟机管理程序部署	是	是	是
服务器 LED 闪烁	是	是	是
查看/清除 SEL 日志	是	是	是
链接和启动 iDRAC	是	是	是
iDRAC 重设	是	是	是
系统锁定模式	否	否	是
系统配置文件	否	否	是
群集配置文件	否	是^	是
使用统一机箱 IP 的主机管理	否	否	Y®
支持 OEM 服务器	否	Y~	是

* 在配备 C6320 型号的云中，夹层卡不支持运行状况监测。

在配备 C6320 型号的云中，夹层卡不支持固件更新。

主动式高可用性功能仅适用于带有 ESXi 6.0 或更高版本的 vCenter 6.5 或更高版本。同样，具有嵌入式 PSU 的服务器和云服务器型号不支持主动式高可用性功能。

^ 群集配置文件中不支持配置偏移。

® 仅适用于 MX 机箱主机。资源清册、监测、主动式高可用性和固件更新功能均受支持。

~ 仅受第 13 代服务器支持。

PowerEdge 机箱支持的功能

本主题介绍了有关 PowerEdge 机箱支持的功能的信息。

表. 9: 模块化基础架构支持的功能

功能	M1000e	VRTX	FX2s	MX
SNMP 警报	是	是	是	是
硬件资源清册	是	是	是	是
链接并启动 CMC 或 Management Module	是	是	是	是
许可证信息	不适用	是	是	是
保修信息	是	是	是	是
运行状况报告	是	是	是	是
多机箱管理组关系信息	否	否	否	是

已配置存储所需的空間

OMIVV 虚拟设备至少需要 44 GB 磁盘空间用于已配置存储。

默认虚拟设备配置

OMIVV 虚拟设备使用 8 GB RAM 和 2 个虚拟 CPU (小型部署模式) 配置。

软件要求

确保 vSphere 环境满足虚拟设备、端口访问和监听端口要求。

VMware vSphere Web 客户端的要求

- 支持 vCenter 6.0 和更高版本
- 需要 vCenter Web 客户端服务 (不支持 vSphere Desktop 客户端)

有关特定软件要求的信息, 您也可以参阅位于 Dell.com/support/manuals 的 *OpenManage Integration for VMware vCenter Compatibility Matrix (OpenManage Integration for VMware vCenter 兼容性值表)*。

OpenManage Integration for VMware vCenter 要求

受管主机上支持的 ESXi 版本

下表提供了有关受管主机支持的 ESXi 版本的信息:

表. 10: 支持的 ESXi 版本

ESXi 版本支持	服务器代系			
	第 11 代	第 12 代	第 13 代	第 14 代
v5.1	是	是	否	否
v5.1 U1	是	是	否	否
v5.1 U2	是	是	是	否
v5.1 U3	是	是	是 (M830、FC830 和 FC430 除外)	否
v5.5	是	是	否	否
v5.5 U1	是	是	否	否
v5.5 U2	是	是	是	否
v5.5 U3	是	是	是	否
v6.0	是	是	是	否
v6.0 U1	是	是	是	否
v6.0 U2	是	是	是	否
v6.0 U3	是	是	是	是
v6.5	否	是	是	否
v6.5 U1	否	是	是	是
v6.5 U2	否	是	是	是
v6.7	否	是	是	是
v6.7 U1	否	是	是	是

① 注: 仅当使用 ESXi 6.5 U2 和更高版本时支持 MX 主机。

OpenManage Integration for VMware vCenter 支持以下所有 vCenter Server 版本 :

表. 11: 支持的 vCenter Server 版本

vCenter 版本	Web Client 支持
v6.0 U2	是
v6.0 U3	是
v6.5	是
v6.5 U1	是
v6.5 U2	是
v6.7	是
v6.7 U1	是

① 注: 有关注册 vCenter Server 的更多信息, 请参阅 Dell.com/support/manuals 上提供的 *OpenManage Integration for VMware vCenter Version 4.3 Web Client Install Guide* (OpenManage Integration for VMware vCenter 版本 4.3 Web 客户端安装指南)。

OpenManage Integration for VMware vCenter 版本 4.3 支持 VMware vRealize Operations Manager (vROPS) 版本 1.1 和 1.2。

端口信息

虚拟设备和受管节点

在 OMIVV 中，使用**修补不符合要求的 vSphere 主机向导**中提供的**修补不符合要求的主机**链接部署 OMSA 代理时，OMIVV 执行以下操作：

- 启动 HTTP Client 服务
- 启用端口 8080
- 使 ESXi 5.0 或更高版本的端口可用以下载并安装 OMSA VIB

在 OMSA VIB 安装完成后，该服务会自动停止并关闭此端口。

表. 12: 虚拟设备

端口号	协议	端口类型	最高加密级别	方向	目标	使用情况	说明
53	DNS	TCP	无	出	OMIVV 设备至 DNS 服务器	DNS 客户端	连接到 DNS 服务器或解析主机名。
69	TFTP	UDP	无	出	OMIVV 设备至 TFTP 服务器	TFTP 客户端	用于 11G 服务器（带有旧固件）的固件更新
80/443	HTTP 或 HTTPS	TCP	无	出	OMIVV 设备至互联网	Dell 联机数据访问	连接到联机（互联网）保修、固件和最新的 RPM 信息。
80	HTTP	TCP	无	进	ESXi 服务器至 OMIVV 设备	HTTP 服务器	在操作系统部署流程中使用，以便安装后脚本与 OMIVV 设备进行通信。
162	SNMP 代理	UDP	无	进	iDRAC/ESXi 至 OMIVV 设备	SNMP 代理（服务器）	接收来自受管节点的 SNMP 陷阱。
443	HTTPS	TCP	128 位	进	OMIVV UI 至 OMIVV 设备	HTTPS 服务器	OMIVV 提供的 Web 服务。vCenter Web 客户端和 Dell 管理门户会消耗这些 Web 服务。
443	WSMAN	TCP	128 位	进/出	OMIVV 设备至/从 iDRAC/OMSA	iDRAC/OMSA 通信	iDRAC、OMSA 和 CMC 通信，用于管理和监测受管节点。
445	SMB	TCP	128 位	出	OMIVV 设备至 CIFS	CIFS 通信	与 Windows 共享通信。
4433	HTTPS	TCP	128 位	进	iDRAC 至 OMIVV 设备	自动查找	配置服务器，用于自动查找受管节点。
2049	NFS	UDP/TCP	无	进/出	OMIVV 设备至 NFS	公共共享	对受管节点公开的 NFS 公共共享（由 OMIVV 设备呈现），用于固件更新和操作系统部署流程。
4001 至 4004	NFS	UDP/TCP	无	进/出	OMIVV 设备至 NFS	公共共享	这些端口必须保持开放，以通过 NFS 服务器的 v 2 和 V 3 协议运行 statd、quotd、lockd 和 mountd 服务。
11620	SNMP 代理	UDP	无	进	iDRAC 至 OMIVV 设备	SNMP 代理（服务器）	用于使用 UDP: 162 接收标准 SNMP 警报的端口。收到的 iDRAC、OMSA

端口号	协议	端口类型	最高加密级别	方向	目标	使用情况	说明
							和 CMC 数据或管理模块用于管理和监测受管节点。
用户定义的	任意	UDP/TCP	无	出	OMIVV 设备至代理服务器	代理	与代理服务器通信。

表. 13: 受管节点 (ESXi)

端口号	协议	端口类型	最高加密级别	方向	目标	使用情况	说明
162, 11620	SNMP	UDP	无	出	ESXi 至 OMIVV 设备	硬件事件	ESXi 发送的异步 SNMP 陷阱。此端口必须从 ESXi 中打开。
443	WSMAN	TCP	128 位	进	OMIVV 设备至 ESXi (OMSA)	iDRAC/OMSA 通信	用于向管理站提供信息。此端口必须从 ESXi 中打开。
443	HTTPS	TCP	128 位	进	OMIVV 设备至 ESXi	HTTPS 服务器	用于向管理站提供信息。此端口必须从 ESXi 中打开。
8080	HTTP	TCP	128 位	出	ESXi 至 OMIVV 设备	HTTP 服务器； 下载 OMSA VIB 并修复不符合要求的 vSphere 主机。	帮助 ESXi 下载 OMSA/驱动程序 VIB。

表. 14: 受管节点 (iDRAC 或 CMC 或管理模块)

端口号	协议	端口类型	最高加密级别	方向	目标	使用情况	说明
443	WSMAN/ HTTPS, REST/ HTTPS	TCP	128 位	进	OMIVV 设备到 iDRAC 或 CMC 或管理模块	iDRAC 通信	用于向管理站提供信息并通过使用 REST 或 HTTPS 协议与 MX 机箱通信。此端口必须从 iDRAC 和 CMC 或管理模块中打开。
4433	HTTPS	TCP	128 位	出	iDRAC 至 OMIVV 设备	自动查找	用于在管理站中自动查找 iDRAC (受管节点)。
2049	NFS	UDP	无	进/出	iDRAC 至/从 OMIVV	公共共享	用于 iDRAC 访问由 OMIVV 设备呈现的 NFS 公共共享。用于操作系统部署和固件更新。 从 OMIVV 中访问 iDRAC 配置。用于部署流量。
4001 至 4004	NFS	UDP	无	进/出	iDRAC 至/从 OMIVV	公共共享	用于 iDRAC 访问由 OMIVV 设备呈现的 NFS 公共共享。用于操作系统部署和固件更新。 从 OMIVV 中访问 iDRAC 配置。用于部署流量。
69	TFTP	UDP	128 位	进/出	iDRAC 至/从 OMIVV	普通文件传输	用于在管理站中成功管理 iDRAC。

前提条件核对表

开始安装产品前的核对表：

- 验证您是否有由 OMIVV 用于访问 vCenter Server 的用户名和密码。用户可以有拥有所有必需权限的管理员角色或拥有必需权限的非管理员用户。有关 OMIVV 操作所需权限列表的更多信息，请参阅[非管理员用户的所需权限](#)。
- 检查您是否有用于 ESXi 主机系统的 root 密码，或在主机上拥有管理权限的 Active Directory 凭据。
- 检查您是否有与在 iDRAC 上具有管理员权限的 iDRAC Express 或 Enterprise 关联的用户名和密码。
- 检查该 vCenter 服务器是否正在运行。
- 确定 OMIVV 安装目录的位置。
- 检查以确保 VMware vSphere 环境满足虚拟设备、端口访问和侦听端口要求。此外，还需在客户端系统上安装 Adobe Flash Player。有关受支持的 Flash Player 版本的更多信息，请参阅 [OpenManage Integration for VMware vCenter Compatibility Matrix \(OpenManage Integration for VMware vCenter 兼容性表\)](#)。

① **注：**该虚拟设备起到普通虚拟机的作用；任何中断或关机都会影响到该虚拟设备的整体功能。

① **注：**当 VMware 工具被部署在 ESXi 5.5 及更高版本上时，OMIVV 显示其正在运行（过时）。如有必要，可在成功部署 OMIVV 设备后或在其后任何时间升级 VMware 工具。

① **注：**建议让 OMIVV 和 vCenter Server 位于同一网络中。

① **注：**OMIVV 设备网络应具有 iDRAC、主机和 vCenter 的访问权限。

安装、配置和升级 OMIVV

先决条件

确保满足硬件要求，并且您正在运行所需的 VMware vCenter 软件。

关于此任务

以下高级步骤概述了 OMIVV 的整体安装和配置步骤：

步骤

- 1 从 Dell 支持网站 Dell.com/support 下载 *DellEMC_OpenManage_Integration_<版本号>.<内部版本号>.zip* 文件。有关下载 OMIVV 的更多信息，请参阅[下载 OpenManage Integration for VMware vCenter](#)。
- 2 导航至下载该文件的位置，然后解压其内容。
- 3 部署 Open Virtualization Format (OVF) 文件，该文件中包含使用 vSphere Web Client 的 OMIVV 设备。请参阅[部署 OMIVV OVF](#)。
- 4 上载许可证文件。有关许可的更多信息，请参阅[上传许可证](#)。
- 5 使用管理控制台在 OMIVV 设备上注册 vCenter 服务器。请参阅[注册 OMIVV 和导入许可证文件](#)。
- 6 要配置设备，请完成[初始配置向导](#)。请参阅[通过配置向导的配置任务](#)。

下载 OpenManage Integration for VMware vCenter

前提条件

保留您手边的 Dell EMC PowerEdge 服务器的服务标签。建议您使用服务标访问 Dell 支持网站上的所有支持。这确保您为您的平台下载相应版本的软件。

要下载 OMIVV：

步骤

- 1 转至 <https://www.dell.com/support>。
- 2 请执行以下操作之一：
 - 输入您的 Dell EMC PowerEdge 服务器的服务标签，然后选择搜索。

- 选择**浏览所有产品 > 服务器 > PowerEdge**。
- 3 在相应型号的 PowerEdge 服务器上。
 - 4 在您的服务器的支持页面上，选择**驱动程序和下载**。
 - 5 从**操作系统**列表中，选择相应版本的 VMware ESXi。
 - 6 从**类别**列表中，选择**系统管理**。
将显示支持的 OMIVV 版本。
 - 7 单击**下载**或选中复选框将软件添加到您的下载列表中。

使用 vSphere Web 客户端部署 OMIVV OVF

先决条件

确保您已从 Dell 网站下载并提取了产品 .zip 文件 (*Dell_OpenManage_Integration_<版本号>.<内部版本号>.zip*)。

步骤

- 1 找到您所下载并提取的 OMIVV 虚拟磁盘，然后运行 **Dell_OpenManage_Integration.exe**。
用于提取和运行 exe 的受支持客户端操作系统版本是 Windows 7 SP1 和更高版本。
用于提取和运行 exe 的受支持服务器操作系统版本是 Windows 2008 R2 和更高版本。
- 2 接受 **EULA**，然后保存 .OVF 文件。
- 3 将 .OVF 文件复制或移动至您要向其上传设备的 VMware vSphere 主机的可访问位置。
- 4 启动 **VMware vSphere Web Client**。
- 5 从 **VMware vSphere Web 客户端**中，选择主机，并在主菜单中单击**操作 > 部署 OVF 模板**。
您也可以右键单击主机并选择**部署 OVF 模板**。

此时将显示**部署 OVF 模板**向导。

- 6 在**选择源**窗口中，执行下列子任务：
 - a 如果要从 Internet 下载 OVF 软件包，请选择 **URL**。
 - b 如果要从本地系统选择 OVF 软件包，请选择**本地文件**并单击**浏览**。

注: 如果 OVF 软件包位于网络共享中，此安装可能需要 10-30 分钟。为加速安装，建议将 OVF 托管在本地驱动器中。

- 7 单击**下一步**。

查看详情窗口将显示以下信息：

- **产品**—显示 OVF 模板名称。
- **版本**—显示 OVF 模板版本。
- **供应商**—显示供应商名称。
- **发行商**—显示发行商详细信息。
- **下载大小**—显示 OVF 模板的实际大小（千兆字节）。
- **占用磁盘大小**—显示厚置和精简配置详细信息。
- **说明**—在此显示备注。

- 8 单击**下一步**。

将显示**选择名称和文件夹**窗口。

- 9 在**选择名称和文件夹**窗口中，执行下列子步骤：
 - a 在**名称**中，输入该模板名称。该名称可包含最多 80 个字符。
 - b 在**选择文件夹或数据中心**列表中，选择要部署模板的位置。

- 10 单击**下一步**。

此时将显示**选择存储**窗口。

- 11 在**选择存储**窗口中，执行下列子步骤：
 - a 在**选择虚拟磁盘格式**下拉列表中，选择以下任一格式：

- 厚置备（延迟置零）
- 厚置备（快速置零）
- 精简配置

建议您选择“厚置备（快速置零）”。

b 从**虚拟机存储策略**下拉列表中，选择一个策略。

12 单击**下一步**。

显示**设置网络**窗口，其包含关于源和目标网络的详细信息。

13 在**设置网络**窗口中，单击**下一步**。

注：建议让 OMIVV 设备和 vCenter Server 位于同一网络中。

14 在**即将完成**窗口，查看为 OVF 部署任务所选的选项，并单击**完成**。

该部署作业将运行并提供完成状态窗口，在该窗口中可跟踪作业进度。

生成证书签名请求

先决条件

确保您上传证书后再将 OMIVV 注册到 vCenter。

关于此任务

生成新证书签名请求 (CSR) 可阻止通过以前生成的 CSR 创建的证书上传到设备。要生成 CSR，请执行以下操作：

步骤

1 在**设备管理**页面中，单击 **HTTPS 证书** 区域中的**生成证书签名请求**。

此时将显示一条消息，表明如果生成新请求，则使用以前的 CSR 创建的证书无法再上传到设备。要继续请求，请单击**继续**，要取消请求，请单击**取消**。

2 如果继续请求，则在**生成证书签名请求**对话框中，为请求输入**通用名称、组织名称、组织单元、地点、州/省名称、国家/地区和电子邮件**。单击**继续**。

3 单击**下载**，然后将产生的证书请求保存到可访问的位置。

上传 HTTPS 证书

先决条件

确保证书使用 PEM 格式。

关于此任务

您可以使用 HTTPS 证书在虚拟设备和主机系统之间进行安全通信。要设置此类型的安全通信，必须将 CSR 发送到证书颁发机构，然后使用管理控制台上传所得证书。还有一个自签名的默认证书可用于安全通信；此证书对于每个安装来说都是唯一的。

注：可以使用 Microsoft Internet Explorer、Firefox 或 Chrome 上传证书。

步骤

1 在**设备管理**页面中，单击 **HTTPS 证书** 区域中的**上传证书**。

2 在**上传证书**对话框中单击**确定**。

3 要选择上传的证书，请单击**浏览**，然后单击**上传**。

4 如果要取消上传，请单击**取消**。

注：如果您想要为设备上传自定义证书，请务必先上传新证书，然后再进行 vCenter 注册。如果您在注册 vCenter 后上传新的自定义证书，Web 客户端会显示通信错误。要解决此问题，请取消注册，然后重新向 vCenter 注册设备。

还原默认的 HTTPS 证书

- 1 在设备管理页面中，单击 HTTPS 证书区域中的还原默认证书。
- 2 在还原默认证书对话框中，单击应用。

以非管理员用户的身份注册 vCenter 服务器

您可使用 vCenter 管理员凭据或具有 Dell 权限的非管理员用户为 OMIVV 设备注册 vCenter 服务器。

关于此任务

要使具有必要权限的非管理员用户能够注册 vCenter 服务器，请执行以下步骤：

步骤

- 1 要更改角色的所选权限，请添加角色并选择所需的权限或修改现有的角色。
请参阅 VMware vSphere 文档的创建或修改角色步骤，然后选择 vSphere Web 客户端中的权限所需的步骤。要选择角色所需的全部权限，请参阅[非管理员用户的所需权限](#)。
注：vCenter 管理员应添加或修改角色。
- 2 将用户分配到新创建的角色后，您定义角色，然后选择角色权限。
请参阅 VMware vSphere 文档，了解有关在 vSphere Web 客户端中分配权限的更多信息。
注：vCenter 管理员应在 vSphere 客户端中分配权限。
具有所需权限的 vCenter 服务器非管理员用户现在可以注册和/或取消注册 vCenter、修改凭据或更新证书。
- 3 使用具有必要权限的非管理员用户注册 vCenter 服务器。
- 4 将 Dell 权限分配给步骤 1 中创建或修改的角色。请参阅 [Assigning Dell privileges to the role in vSphere Web Client](#) (向 vSphere Web Client 中的角色分配 Dell 权限)。

具有所需权限的非管理员用户可体验 Dell EMC 主机的 OMIVV 功能。

所需的非管理员用户的权限

向 vCenter 注册 OMIVV，非管理员用户需要以下权限：

注：通过非管理员用户向 OMIVV 注册 vCenter 服务器时，如果未分配以下权限，则会显示一条错误消息：

- 警报
 - 创建警报
 - 修改警报
 - 移除警报
- 分机
 - 注册扩展名
 - 注销扩展名
 - 更新扩展名
- 全局
 - 取消任务
 - 日志事件
 - 设置

注：如果使用的是 VMware vCenter 6.5 或升级至 vCenter 6.5 或更高版本，分配以下运行状况更新权限：

- 运行状况更新提供程序
 - 注册
 - 注销
 - 更新
- 主机
 - CIM
 - CIM 交互
 - 配置
 - 高级设置
 - 连接
 - 维护
 - 网络配置
 - 查询补丁程序
 - 安全配置文件和防火墙

注: 如果使用的是 VMware vCenter 6.5 或升级至 vCenter 6.5 或更高版本，分配以下权限：

- Host.Config
 - 高级设置
 - 连接
 - 维护
 - 网络配置
 - 查询补丁程序
 - 安全配置文件和防火墙

- 资源清册
 - 将主机添加到群集
 - 添加独立主机
 - 修改群集

注: 如果您使用的是 vCenter 6.5 或升级至 vCenter 6.5 或更高版本，请确保您分配修改群集权限。

- 主机配置文件
 - 编辑
 - 查看
- 权限
 - 修改权限
 - 修改角色
- 会话
 - 验证会话
- 任务
 - 创建任务
 - 更新任务

注: 如果非管理员用户要尝试注册 vCenter 服务器，则必须向现有角色添加 Dell 权限。有关查找 Dell 权限的更多信息，请参阅[将 Dell 权限分配给现有角色](#)。

由具有所需权限的非管理员用户注册 vCenter 服务器

您可以通过使用具有所需权限的非管理员用户为 OMIVV 设备注册 vCenter 服务器。请参阅[注册 OpenManage Integration for VMware vCenter](#) 和[导入许可证文件](#)主题。了解有关通过非管理员用户或作为管理员注册 vCenter 服务器的信息。


将 Dell 权限分配给现有角色

关于此任务

您可以编辑现有角色以分配 Dell 权限。

① **注:** 确保您以具有管理员权限的用户登录。

步骤

- 1 使用拥有管理权限的帐户登录到 vSphere Web 客户端。
- 2 在左侧窗格中，点击 vSphere web 客户端中的**管理 → 角色**。
- 3 从**角色提供程序**下拉列表中选择 vCenter 服务器系统。
- 4 从**角色列表**中选择角色，然后单击 。
- 5 单击**权限**，展开 **Dell**，然后为所选角色选择以下 Dell 权限，之后单击**确定**：
 - Dell.Configuration
 - Dell.Deploy-Provisioning
 - Dell.Inventory
 - Dell.Monitoring
 - Dell.Reporting

有关 vCenter 内可用 OMIVV 角色的更多信息，请参阅 *OpenManage Integration for VMware vCenter User's Guide* (OpenManage Integration for VMware vCenter 用户指南) 中的“安全角色和权限”，地址为：Dell.com/support/manuals。

对权限和角色的更改会立即生效。现在，具有必要权限的用户可以执行 OpenManage Integration for VMware vCenter 操作。

① **注:** 对于所有 vCenter 操作，OMIVV 使用已注册用户的权限而不是已登录用户的权限。

① **注:** 如果访问 OMIVV 的特定页面时没有向登录用户分配 Dell 权限，则显示错误 2000000。

注册 OpenManage Integration for VMware vCenter 和导入许可证文件

先决条件

确保您的许可证可从 [Dell Digital Locker](#) 下载。如果您订购了多个许可证，这些许可证可能会在不同时间分别发放。您可以在[订单状态](#)中查看其他许可证项目的状态。许可证文件以 .XML 格式提供。

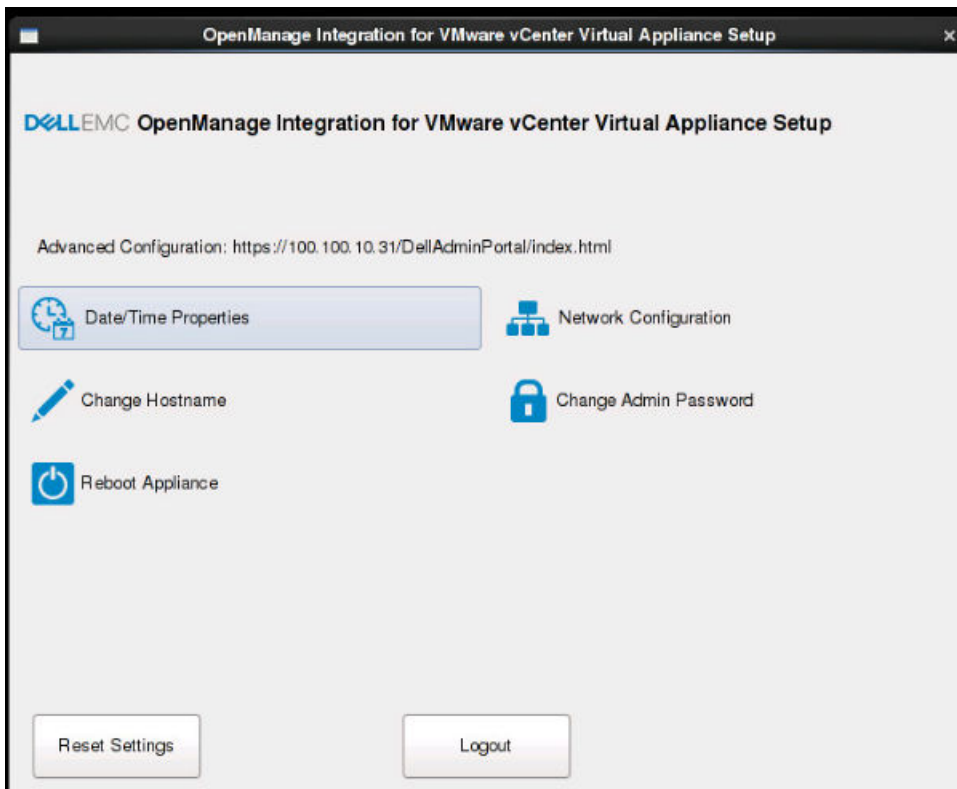
① **注:** 如果您想为您的设备上传自定义证书，请务必先上传新证书，然后再注册 vCenter。如果您在注册 vCenter 后上传新的自定义证书，Web 客户端会显示通信错误。要修复此问题，请取消注册，然后重新向 vCenter 注册设备。

步骤

- 1 从 vSphere Web 客户端，单击**主页 > 主机和群集**，然后在左面板中找到已部署的 OMIVV，再单击**开启虚拟机电源**。在部署期间如果选择**部署后开启电源**，则部署完成后将自动开启虚拟机电源。
- 2 要运行**管理控制台**，单击主 **VMware vCenter** 窗口中的**控制台**选项卡。
- 3 等待 OMIVV 完成引导，然后输入用户名 **Admin** (默认为 Admin) 并按 **Enter**。
- 4 输入新的管理员密码。确保管理员密码符合界面中显示的密码复杂性规则。按 **Enter** 键。

- 5 重新输入先前提提供的密码，然后按 **Enter**。
按 **Enter** 以配置 OMIVV 设备中的网络和时区信息。
- 6 要配置 OMIVV 时区信息，请单击**日期/时间属性**。

图 1: 控制台选项卡



- 7 在**日期和时间**选项卡中，选择**通过网络同步日期和时间**。
此时将显示 **NTP 服务器框**。
- 8 添加 vCenter 将要与其同步的有效 NTP 服务器的详细信息。
- 9 单击**时区**，并选择适当的时区，然后单击**确定**。
- 10 要对 OMIVV 设备配置静态 IP 地址，请单击**网络配置**，或跳至步骤 17。
- 11 选择 **Auto eth0**，然后单击**编辑**。
- 12 选择 **IPv4 设置**选项卡，然后在**方法**下拉列表中选择**手动**。
- 13 单击**添加**，然后添加有效的 IP、子网掩码和网关信息。
- 14 在 **DNS 服务器**字段中，提供 DNS 服务器详细信息。
- 15 单击**应用**。
- 16 要更改 OMIVV 设备的主机名，请单击**更改主机名**。
- 17 输入有效的主机名，然后单击**更新主机名**。

注: 更改主机名和 NTP 后，确保系统重新启动。

注: 如果在任何 vCenter 服务器中注册了 OMIVV 设备，请注销再重新注册所有 vCenter 实例。

打开管理控制台之前，确保手动更新设备的所有参考信息，如在 iDRAC、DRM 中配置服务器。

- 18 从支持的浏览器打开**管理控制台**。

要打开**管理控制台**，请在 OpenManage Integration for VMware vCenter 的**帮助和支持**选项卡中，单击**管理控制台**下的链接或启动 Web 浏览器，然后提供 `https://<ApplianceIP or Appliance hostname>` URL。

IP 地址是设备虚拟机的 IP 地址，而不是 ESXi 主机 IP 地址。可以使用控制台顶部提及的 URL 访问管理控制台。

例如：Https://10.210.126.120 或 Https://myesxihost

URL 不区分大小写。

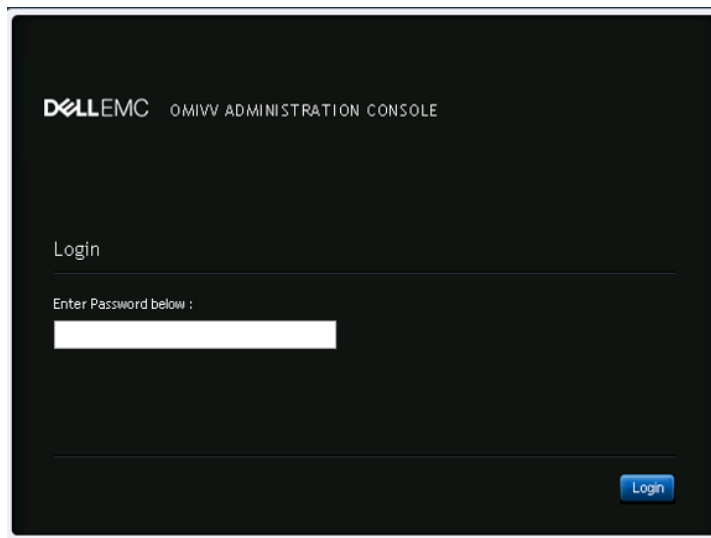


图 2: 管理控制台

- 19 在**管理控制台**登录窗口中，输入密码，然后单击**登录**。

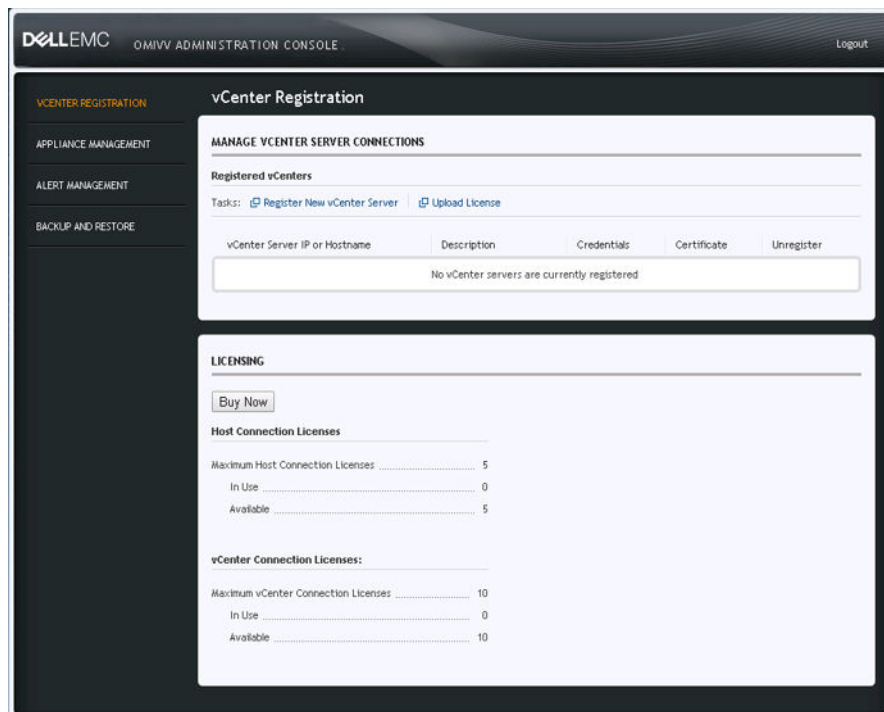


图 3: 管理控制台中的 vCenter 注册窗口

- 20 在 **vCenter 注册**窗口中，单击**注册新 vCenter 服务器**。
- 21 在**注册新 vCenter 服务器**窗口中，执行下列子步骤：

- a 在 **vCenter 名称** 下方的 **vCenter 服务器 IP 或主机名** 文本框中，输入服务器 IP 或主机名，然后在 **说明** 文本框中，输入说明。
“说明” 字段为可选项。

注: 建议使用完全限定域名 (FQDN) 向 VMware vCenter 注册 OpenManage Integration for VMware vCenter。确保 DNS 服务器可正确解析 vCenter 的主机名用于基于 FQDN 的注册。

- b 在 **vCenter 用户帐户** 下的 **vCenter 用户名** 中，输入管理员用户名或具有必要权限的用户名。
输入用户名作为 domain\user、domain/user 或 user@domain。OMIVV 使用管理员用户帐户或具有必要权限的用户进行 vCenter 管理。
- c 在 **密码** 中，输入密码。
- d 在 **确认密码** 中，再次输入密码。

22 单击**注册**。

注: 对于具有单个 vCenter 实例或多个 vCenter 服务器的大型部署模式，OpenManage Integration for VMware vCenter 目前使用链接的模式支持最多 1000 个主机。

23 请执行以下操作之一：

- 如果您使用的是 OMIVV 试用版本，则可查看 OMIVV 图标。
- 如果您使用的是完整的产品版本，则可以从 Dell Digital Locker (Dell Digital Locker) 上下载许可证文件，并将此许可证导入您的虚拟设备。要导入许可证文件，请单击**上传许可证**。

24 在**上传许可证**窗口中，单击**浏览**以导航至该许可证文件，然后单击**上传**以导入该许可证文件。

注: 如果您修改或编辑许可证文件，许可证文件 (.XML 文件) 将无法使用，您可以通过 Dell Digital Locker 下载 .XML 文件 (许可证密钥)。如果您无法下载许可证密钥，请转至**联系技术支持**找到您的产品对应的区域 Dell 支持电话号码，联系 Dell 支持部门。

在注册 OMIVV 后，OMIVV 图标将出现在 Web 客户端主页的**管理**类别下。

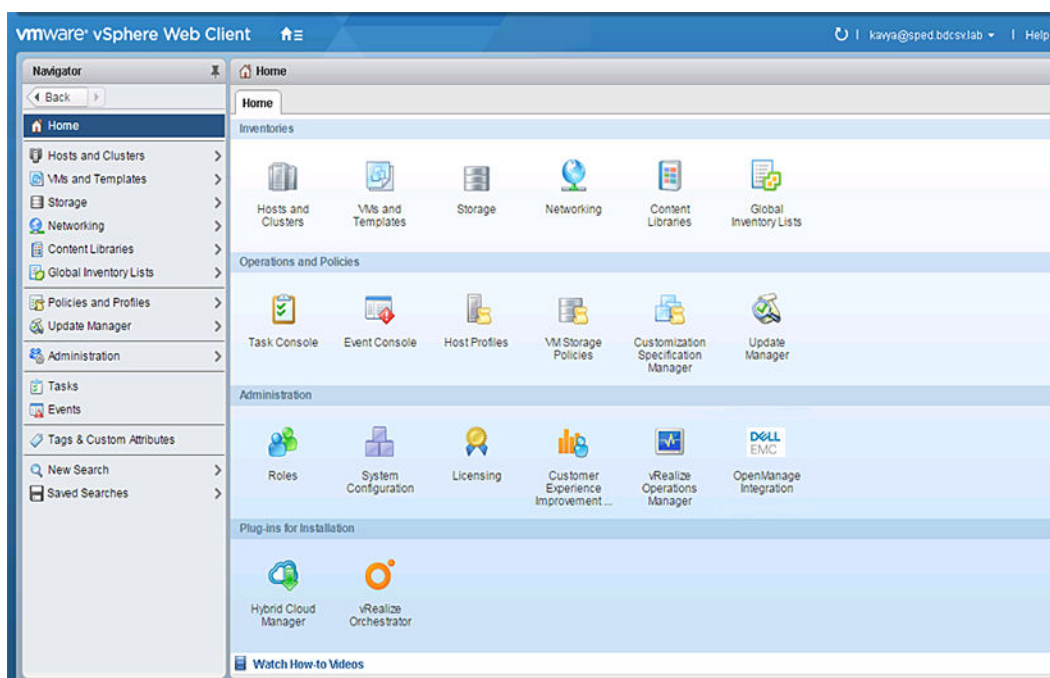


图 4: OpenManage Integration for VMware vCenter 已成功添加到 vCenter

实例

对于所有 vCenter 操作，OMIVV 使用已注册用户的权限而不是已登录用户的权限。

例如：具有必要权限的用户 X 向 vCenter 注册 OMIVV，用户 Y 仅具有 Dell 权限。用户 Y 现在可以登录到 vCenter 并且可以从 OMIVV 触发固件更新任务。在执行固件更新任务时，OMIVV 使用用户 X 的权限将计算机置于维护模式或重新引导主机。

升级已注册的 vCenter

升级注册的 vCenter 之后，请执行以下任务：

- 对于非管理员用户：
 - a 如有必要，向非管理员用户分配额外的权限。请参阅[所需的非管理员用户的权限](#)。例如，当从 vCenter 6.0 升级到 vCenter 6.5 时，分配额外的权限。
 - b 重新引导已注册的 OMIVV 设备。
- 对于管理员用户：
 - a 重新引导已注册的 OMIVV 设备。

验证安装

关于此任务

执行以下步骤可验证 OMIVV 是否已成功安装：

- 步骤**
- 1 关闭任何 vSphere 客户端窗口，并打开一个新 vSphere Web 客户端。
 - 2 确认 OMIVV 图标出现在 vSphere Web 客户端中。
 - 3 尝试从 vCenter Server 向虚拟设备 IP 地址或主机名发出 PING 命令来确保 vCenter 可与 OMIVV 进行通信。
 - 4 在 vSphere Web Client 中，单击**主页 > 管理 > 解决方案**，然后单击**插件管理**（在较旧 vCenter 版本中）或**客户端插件**（在较新版本中）。
有关访问**插件管理**或**客户端插件**页面限制的更多信息，请参阅 VMware 说明文件。
 - 5 在**插件管理**或**客户端插件**窗口中，验证 OMIVV 已安装并启用。

更新虚拟设备存储库位置和虚拟设备

先决条件

要确保所有数据受保护，请执行 OMIVV 数据库的备份后再更新虚拟设备。请参阅用户指南中的[管理备份和还原](#)主题。

步骤

- 1 在**设备管理**页面的**设备更新**部分中，确认当前的和可用的版本。

注：OMIVV 设备需要互联网连接来显示可用的升级机制和执行 RPM 升级。请确保 OMIVV 设备连接到互联网。根据网络设置，如果您的网络需要代理，则启用代理并提供代理设置。请参阅[用户指南](#)中的[设置 HTTP 代理](#)。

注：确保更新存储库路径有效。

有关可用的虚拟设备版本，适用的 RPM 和 OVF 虚拟设备升级机制会显示一个勾号。以下是可能的升级机制选项，您可以执行升级机制的任一项任务：

- 如果 RPM 旁显示了勾号，则可以将 RPM 从现有版本升级至最新的可用版本。请参阅[从现有版本升级至最新版本](#)。
 - 如果 OVF 旁显示勾号，则可以从现有版本备份 OMIVV 数据库，并在最新的可用设备版本中将其还原。请参阅[通过备份和还原更新设备](#)。
 - 如果 RPM 和 OVF 旁均显示勾号，则可以执行提及的任一选项以升级您的设备。在这种情况下，建议的选项是 RPM 升级。
- 2 要更新虚拟设备，请从 OMIVV 版本执行提及的适用升级机制任务。

注：确保您从所有 Web 客户端会话至 vCenter 服务器中注销。

① **注:** 确保登录到已注册的 vCenter 服务器之前，您在相同的平台服务控制器 (PSC) 下同时更新所有设备。否则，可能会在 OMIVV 实例上看到不一致信息。

3 单击**设备管理**并验证升级机制。

将 OMIVV 从现有版本升级至当前版本

1 在**设备管理**页面中，根据您的网络设置，如果网络需要代理，请启用代理并提供代理设置。请参阅**用户指南**中的**设置 HTTP 代理主题**。

2 要将 OpenManage Integration 插件从现有版本升级至当前版本，请执行以下步骤之一：

- 要使用**更新存储库路径**中可用的 RPM 进行升级，请确保**更新存储库路径**设置为路径：<https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/>。

如果路径不同，则在**设备管理**窗口中的**设备更新**窗口中，单击**编辑**，然后单击**应用**以便在**更新存储库路径**文本框中将路径更新到 <https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/>。

- 要使用最新下载的 RPM 文件夹或文件进行升级，如果没有互联网连接，则从 <https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/> 路径下载所有文件和文件夹并将其复制到 HTTP 共享中。

在**设备管理**窗口中的**设备更新**部分，单击**编辑**，然后在**更新存储库路径**文本框中，涵括脱机 HTTP 共享的路径，并单击**应用**。

3 比较可用虚拟设备版本和当前虚拟设备版本，并确保可用虚拟设备版本比当前虚拟设备版本高。

4 要将更新应用到虚拟设备，可在**设备设置**下，单击**更新虚拟设备**。

5 在**更新设备**对话框中，单击**更新**。

单击**更新**后，您会从**管理控制台**注销。

6 关闭 Web 浏览器。

① **注:** 在升级过程中，设备会重新启动一次或两次。

① **注:** 对设备进行 RPM 升级后，请确保执行以下操作：

- 先清除浏览器高速缓存再登录到 Dell 管理门户。
- 重新安装 VMware 工具。
要重新安装 VMware 工具，请执行以下操作：
 - a 右键单击 OMIVV 设备。
 - b 将鼠标指针悬停在来宾上，然后单击**安装/升级 VMware 工具**。
 - c 在**安装/升级 VMware 工具**对话框中，单击**自动工具升级**，然后单击**确定**。
您可以在**最近的任务**中查看安装状态。

① **注:** RPM 升级完成后，您可以在 OMIVV 控制台中查看登录屏幕。打开浏览器并提供 <https://<设备 IP/主机名>> 链接，然后导航至设备更新区域。您可以验证可用和当前虚拟设备版本是否相同。如果已在群集上启用主动式高可用性，OMIVV 为那些群集取消注册 Dell Inc 提供商，然后在升级后重新注册 Dell Inc 提供商。因此，直至升级完成后才能针对 Dell EMC 主机运行状况更新。

通过备份和还原更新设备

关于此任务

要将 OMIVV 设备从较旧版本更新至当前版本，请执行以下步骤：

步骤

1 对较旧版本的数据库进行备份。

2 从 vCenter 关闭较旧 OMIVV 设备。

① **注:** 请不要从 vCenter 注销 OMIVV 插件。如果从 vCenter 注销插件，将移除该插件在 vCenter 上注册的所有警报，并移除对这些警报执行的所有自定义设置（如动作等）。

- 3 部署新的 OpenManage Integration 设备 OVF。
- 4 开启 OpenManage Integration 新设备电源。
- 5 设置新设备的网络、时区等。

注: 确保新的 OpenManage Integration 设备与旧设备具有相同的 IP 地址。

注: 如果新设备的 IP 地址不同于旧设备上的 IP 地址，则 OMIVV 插件可能无法正常工作。在这种情况下，请先注销，然后再重新注册所有 vCenter 实例。

- 6 OMIVV 设备附带默认证书。如果您想为您的设备获取自定义证书，同样进行更新。请参阅[生成证书签名请求](#)和[上传 HTTPS 证书](#)。否则，请跳过此步骤。
- 7 将数据库还原到新的 OMIVV 设备。请参阅[用户指南](#)中的（从备份还原 OMIVV 数据库）[从备份还原 OMIVV 数据库](#)主题。
- 8 验证设备。请参阅 [Dell.com/support/manuals](#) 上提供的 *OpenManage Integration for VMware vCenter 安装指南* 中的“安装验证”。
- 9 对所有已注册的 vCenter 服务器运行[资源清册](#)。

注: Dell EMC 建议在升级后对插件管理的所有主机重新运行资源清册。要按需运行资源清册，请参阅 [Scheduling inventory jobs](#)（计划资源清册作业）。

注: 如果新 OMIVV 版本 y 的 IP 地址已从 OMIVV 版本 x 进行更改，请配置 SNMP 陷阱的陷阱目标以将鼠标悬停在新设备。对于第 12 代和更高代系的服务器，IP 更改是通过对这些主机运行资源清册进行修补。在第 12 代主机上运行资源清册时，如果 SNMP 陷阱不将鼠标悬停在新 IP，则那些主机将被列为不符合要求。对于兼容较早版本的第 12 代之前的主机，此 IP 更改会显示为不兼容并需要您配置 Dell EMC OpenManage Server Administrator (OMSA)。要修复 vSphere 主机符合性问题，请参阅 [用户指南](#) 中的 [Running the fix noncompliant vSphere hosts wizard](#)（运行修复不符合要求的 vSphere 主机向导）主题。

注: 从旧版 OMIVV 备份或还原至更高版本的 OMIVV 后，如果您发现 vCenter 上未显示 2 百万错误或 Dell EMC 徽标，请执行以下操作：

- 在 vCenter 服务器上重新启动 vSphere Web 客户端。
- 如果问题仍然存在：
 - 对于 VMware vCenter Server 设备，请转至 `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity`。对于 Windows vCenter，请转至 vCenter 设备中的 `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity` 文件夹，并查看已存在的旧数据，例如：`com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX`。
 - 手动删除与旧版 OMIVV 相应的文件夹。

注销较早版本的 OMIVV 后恢复 OMIVV

关于此任务

如果在备份较早版本数据库后注销了 OMIVV 插件，请在继续迁移前执行以下步骤：

注: 注销插件的操作会移除插件在已注册的警报上执行的所有自定义设置。以下步骤不会还原自定义。但是，默认状态下它将重新注册警报。

步骤

- 1 执行[通过备份和还原更新设备](#)中所述的步骤 3 至步骤 5。
- 2 向已在较早插件中注册的同一 vCenter 注册插件。
- 3 要完成迁移，请执行 [通过备份和还原更新设备](#) 中的步骤 6 至 9。

VMware vCenter 的设备配置

您完成 OMIVV 基础安装和 vCenter 注册后，单击 OMIVV 图标时，将显示**初始配置向导**。您可以继续通过使用以下方法之一配置设备：

- 通过**初始配置向导**配置设备。
- 通过 OMIVV 中的**设置选项卡**配置设备。

首次启动时，您可以使用**初始配置向导**配置 OMIVV 设备。在后续的实例中，请使用**设置选项卡**。

① | **注：**两个方法中的用户界面相似。

主题：

- [通过配置向导配置任务](#)
- [通过设置选项卡配置任务](#)
- [创建机箱配置文件](#)

通过配置向导配置任务

① | **注：**执行 OMIVV 相关的任务时，如果您在更改 DNS 设置后查看 Web 通信错误，请清除浏览器缓存，并从 Web 客户端注销，然后再次登录。

通过使用配置向导，您可以查看并执行以下任务：

- 查看配置向导欢迎页面。
- 选择 vCenter。请参阅[选择 vCenter](#)。
- 创建连接配置文件。请参阅[创建连接配置文件](#)。
- 创建机箱配置文件。需要使用机箱配置文件管理已禁用 iDRAC IPv4 的 MX 机箱中存在的主机。请参阅[创建机箱配置文件](#)。
- 配置事件和警报。请参阅[配置事件和警报](#)。
- 计划资源清册作业。请参阅[计划资源清册作业](#)。
- 运行保修检索作业。请参阅 [Running a warranty retrieval job](#)（运行保修检索作业）。

查看配置向导“欢迎”对话框

要在安装并注册到 vCenter 后配置 OMIVV，请执行以下步骤以查看**初始配置向导**：

- 1 在 vSphere Web 客户端中，单击**主页**，然后单击 **OpenManage Integration** 图标。
您可以执行以下任一选项以访问初始配置向导：
 - 首次单击 **OpenManage Integration** 图标，**初始配置向导**会自动显示。
 - 从 **OpenManage Integration > 入门**中，单击**开始初始配置向导**。
- 2 在**欢迎**对话框中，审阅各步骤，然后单击**下一步**。

选择 vCenter

关于此任务

在 **vCenter 选择** 对话框中，您可以配置以下的 vCenter：

- 特定的 vCenter
- 所有已注册的 vCenter

要访问 **vCenter 选择** 对话框，请执行以下操作：

步骤

- 1 在**初始配置向导的欢迎对话框**中，单击**下一步**。
- 2 从 **vCenter** 下拉式列表中选择 一个 vCenter 或所有已注册的 vCenter。
选择尚未配置的 vCenter 或者您已添加至环境的 vCenter。使用 **vCenter 选择** 页面，您可以选择一个或多个 vCenter 来配置设置。
- 3 要继续处理**连接配置文件说明对话框**，请单击**下一步**。

注：如果您具有多台属于同一单一登录 (SSO) 且使用相同 OMIVV 设备注册的 vCenter 服务器，并选择配置单台 vCenter 服务器，请重复执行第 1 至第 3 步，直至配置完每个 vCenter。

创建连接配置文件

前提条件

在结合使用 Active Directory 凭据与连接配置文件之前，请确保：

- Active Directory 用户的帐户存在于 Active Directory 中。
- 为 iDRAC 和主机配置基于 Active Directory 的验证。

关于此任务

连接配置文件存储 OMIVV 用来与 Dell EMC 服务器通信的 iDRAC 和主机凭据。每台 Dell EMC 服务器都必须与一个连接配置文件关联，以便 OMIVV 对其进行管理。您可以将多台服务器分配到单个连接配置文件。您可以使用配置向导创建连接配置文件，也可从 **OpenManage Integration for VMware vCenter > 设置选项卡** 创建。您可以使用 Active Directory 凭据登录 iDRAC 和主机。

注：Active Directory 凭据可以是相同或独立的 iDRAC 和主机。

注：如果添加的主机数超出用于创建连接配置文件的许可证限制，您将无法创建连接配置文件。

注：使用单个统一机箱管理 IP 管理 MX 机箱主机。要使用机箱配置文件管理 MX 机箱，请参阅 [Creating chassis profile](#)（创建机箱配置文件）。Dell EMC 建议管理具有 iDRAC IP 的 MX 机箱主机以获取完整的 OMIVV 功能。

步骤

- 1 在**连接配置文件说明对话框**中，单击**下一步**。
- 2 在**连接配置文件名称和凭据对话框**中，输入**连接配置文件名称**和可选的**连接配置文件说明**。
- 3 在**连接配置文件名称和凭据对话框**中的 **iDRAC 凭据**下，执行以下任一操作（具体取决于是否使用 Active Directory 配置 iDRAC）：

注：iDRAC 帐户需要用于更新固件、应用硬件配置文件、在第 14 代服务器中应用系统配置文件并部署虚拟机监控程序的管理权限。

- 对于已针对 Active Directory 配置和启用的 iDRAC IP（将在其上使用 Active Directory），请选择使用 **Active Directory**；否则，请向下滚动到配置 iDRAC 凭据步骤。
 - 1 在 Active Directory **用户名**中，键入用户名。按照下列格式之一键入用户名：**域\用户名**或**用户名@域**。用户名限制为 256。

- 2 在 Active Directory **密码**中，键入密码。密码不得超过 127 个字符。
- 3 在**验证密码**中，再次键入该密码。
- 4 根据您的要求，请执行以下操作之一：
 - 要下载和存储 iDRAC 证书并在将来的所有连接中对其进行验证，请选中**启用证书检查**。
 - 若要不存储 iDRAC 证书并且在将来的所有连接期间不对其进行验证，请清除**启用证书检查**。
- 要在无需 Active Directory 的情况下配置 iDRAC 凭据，请执行以下任务：
 - 1 在**用户名**中，键入用户名。用户名限制为 16 个字符。有关您所使用 iDRAC 版本的用户名限制的信息，请参阅 iDRAC 说明文件。
 - 2 在**密码**中，键入密码。密码不得超过 20 个字符。
 - 3 在**验证密码**中，再次键入该密码。
 - 4 请执行以下操作之一：
 - 要下载和存储 iDRAC 证书并在将来的所有连接中对其进行验证，请选中**启用证书检查**。
 - 若要不存储 iDRAC 证书并且在将来的所有连接期间不对其进行验证，请清除**启用证书检查**。
- 4 在**主机根**中，执行以下步骤之一：
 - 对于已针对 Active Directory 配置和启用的主机（将在其上使用 Active Directory），请选择使用 **Active Directory** 并执行以下步骤；否则，请配置主机凭据：
 - 1 在 Active Directory **用户名**中，键入用户名。按照下列格式之一键入用户名：**域\用户名**或**用户名@域**。用户名限制为 256 个字符。

注: 对于主机用户名和域限制，请参阅以下内容：

主机用户名要求：

 - 长度介于 1 和 64 个字符之间
 - 没有不可打印的字符

主机域要求：

 - 长度介于 1 和 64 个字符之间
 - 第一个字符必须为字母。
 - 不能包含空格。
 - 2 在 Active Directory **密码**中，键入密码。密码不得超过 127 个字符。
 - 3 在**验证密码**中，再次键入该密码。
 - 4 请执行以下操作之一：
 - 要下载和存储主机证书并在将来的所有连接中对其进行验证，请选中**启用证书检查**。
 - 若要不存储 iDRAC 证书并且在将来的所有连接期间不对其进行验证，请清除**启用证书检查**。
 - 要在不设置 Active Directory 的情况下配置主机凭据，请执行以下任务：
 - 1 在**用户名**中，用户名为 `root`，这是默认用户名，您无法更改。如果已设置 Active Directory，除了 `root`，您还可以选择任何 Active Directory 用户。
 - 2 在**密码**中，键入密码。密码不得超过 127 个字符。

注: OMSA 凭据与用于 ESXi 主机的凭据相同。
 - 3 在**验证密码**中，再次键入该密码。
 - 4 请执行以下操作之一：
 - 要下载和存储主机证书并在将来的所有连接中对其进行验证，请选中**启用证书检查**。
 - 若要不存储主机证书以及在将来的所有连接期间不进行检查，请清除**启用证书检查**。
- 5 单击**下一步**。
- 6 在**连接配置文件关联的主机**对话框中，选择连接配置文件的主机并单击**确定**。

注: 如果 OEM 主机未显示在选择主机窗口上，请通过使用添加 OEM 主机向导添加 OEM 主机。请参阅**用户指南**中的 **Adding OEM Hosts**（添加 OEM 主机）主题。
- 7 要测试连接配置文件，请选择一个或多个主机，然后单击**检测连接**。

- ① **注:** 此步骤是可选步骤，用于检查主机和 iDRAC 凭据。尽管此步骤为可选，Dell EMC 仍建议您测试连接配置文件。
- ① **注:** 如果对运行 ESXi 6.5 或更高版本的主机禁用 WBEM 服务，当您在那些主机上执行测试连接和资源清册时，将自动启用 WBEM。
- ① **注:** 创建连接配置文件时，如果您选择所有注册的 vCenter，请对运行已禁用 WBEM 服务的 ESXi 6.5 或更高版本的所有主机进行的测试连接失败。在这种情况下，建议完成连接配置文件向导操作、在主机上运行资源清册，然后再次测试连接配置文件。
- ① **注:** 您可能会看到主机的测试连接失败，并且即便在输入有效的凭据后仍表示输入了无效的凭据。由于 ESXi 阻止访问，因此发生此情况。请等待 15 分钟，然后重试测试连接。

8 要完成配置文件的创建，请单击下一步。

单击“下一步”后，系统将保存您在此向导中提供的所有详细信息，且您无法从此向导修改这些信息。您可以从**管理 > 配置文件连接配置文件**页面中为此 vCenter 详细信息修改连接配置文件或创建更多连接配置文件。请参阅 Dell.com/support/manuals 上提供的 *OpenManage Integration for VMware vCenter User's Guide* (*OpenManage Integration for VMware vCenter 用户指南*) 中的，查看本指南中的主题。。

① **注:** 对于既没有 iDRAC Express 也没有 Enterprise 卡的服务器，iDRAC 测试连接的结果不适用于此系统。

主机添加到连接配置文件后，OMIVV 的 IP 地址会自动设置为主机的 iDRAC 的 SNMP 陷阱目标，并且 OMIVV 会自动为运行 ESXi 6.5 和更高版本的主机启用基于 Web 的企业级管理 (WBEM) 服务。OMIVV 使用 WBEM 服务正确同步 ESXi 主机和 iDRAC 关系。如果为特定主机配置 SNMP 陷阱目标发生故障，并且/或者为特定主机启用 WBEM 服务发生故障，那么那些主机将被列为不符合要求。要查看需要重新配置 SNMP 陷阱目标并且/或者启用 WBEM 服务的不符合要求的主机，请参阅 Dell.com/support/manuals 上提供的 *OpenManage Integration for VMware vCenter User's Guide* (*OpenManage Integration for VMware vCenter 用户指南*) 中的**报告和修正 vSphere 主机的符合性**。。

计划资源清册作业

关于此任务

您可以使用配置向导或 **OpenManage Integration > 管理 > 设置选项卡**下的 OpenManage Integration 配置资源清册计划。

- ① **注:** 为确保 OMIVV 继续显示更新的信息，建议您计划一个周期性资源清册作业。资源清册作业消耗的资源很少，不会降低主机性能。
- ① **注:** 在对所有主机运行资源清册后，机箱将会被自动发现。如果将机箱添加到机箱配置文件中，则机箱资源清册会自动运行。在具有多个 vCenter 服务器的 SSO 环境中，当在计划时间对任何 vCenter 运行资源清册时，会自动对每一个 vCenter 运行机箱资源清册。
- ① **注:** 每次调用配置向导时，此页面中的设置都重设为默认值。如果您之前已配置资源清册计划，请确保先复制此页面中的先前计划，再完成向导功能，以便先前的计划不被默认设置覆盖。

步骤

- 1 在**初始配置向导的资源清册计划**对话框中，选择**启用资源清册数据检索**（如果其尚未启用）。**启用资源清册数据检索**默认启用。
- 2 在**资源清册数据检索计划**下，执行以下操作：
 - a 选中一周中要运行资源清册的日期旁边的复选框。
默认情况下，选中**所有天**。
 - b 在**数据检索时间**中以 HH:MM 格式输入时间。
输入的时间是当地时间。因此，如果您想要在虚拟设备的时区运行资源清册，请计算当地时间与虚拟设备时区之间的时差，然后输入适当的时间。
 - c 要应用更改并继续，请单击**下一步**。

单击“下一步”后，系统将保存您在此向导中提供的所有详细信息，且您无法从此向导修改这些信息。在配置向导中完成配置后，可以从**管理 > 设置选项卡**中修改资源清册计划详细信息。请参阅 Dell.com/support/manuals 上 *OpenManage Integration for VMware vCenter User's Guide* (*OpenManage Integration for VMware vCenter 用户指南*) 中的**修改资源清册作业计划**。

运行保修检索作业

关于此任务

保修检索作业配置位于 OMI VV 的“设置”选项卡中。此外，您还可从**作业队列 > 保修运行或计划保修检索作业**。计划的作业将列在作业队列中。在具有多个 vCenter 服务器的 SSO 环境中，当对任何 vCenter 运行保修时，会自动对每个 vCenter 运行机箱保修。但是，如果未将保修添加到机箱配置文件中，则保修不会自动运行。

① 注：每次调用配置向导时，此页面中的设置都重设为默认值。如果您之前已配置保修检索作业，请确保在此页面上先复制该计划保修检索作业，再完成向导功能，以便先前的保修检索不被默认设置覆盖。

步骤

- 1 在**保修计划**对话框中，选择**启用保修数据检索**。
- 2 在**保修数据检索计划**中，执行以下操作：
 - a 选中一周中要运行保修的日期旁边的复选框。
 - b 以 HH:MM 格式输入时间。
输入的时间是当地时间。因此，如果您想要在虚拟设备的时区运行资源清册，请计算当地时间与虚拟设备时区之间的时差，然后输入适当的时间。
- 3 要应用更改并继续，单击**下一步**，然后继续**事件和警报**设置。
单击“下一步”后，系统将保存您在此向导中提供的所有详细信息，且您无法从此向导修改这些信息。在配置向导中完成配置后，您可以从**设置**选项卡中修改保修作业计划。请参阅 Dell.com/support/manuals 上 *OpenManage Integration for VMware vCenter User's Guide (OpenManage Integration for VMware vCenter 用户指南)* 中的**修改保修作业计划**。

配置事件和警报

您可以使用**初始配置向导**或从**事件和警报**的**设置**选项卡来配置事件和警报。为了从服务器接收事件，OMI VV 被配置为陷阱目标。对于第 12 代及之后的主机，必须在 iDRAC 中设置 SNMP 陷阱目标。对于早于第 12 代的主机，请确保在 OMSA 中设置陷阱生成。

关于此任务

① 注：对于第 12 代或更高代系的主机，OMI VV 支持 SNMP v1 和 v2 警报；对于早于第 12 代的主机，仅支持 SNMP v1 警报。

步骤

- 1 在**初始配置向导**中的**事件发布级别**下，选择以下选项之一：
 - 不发布任何事件 — 阻止硬件事件
 - 发布所有事件 — 发布所有硬件事件
 - 仅发布严重和警告事件 — 仅发布严重和警告级别的硬件事件
 - 仅发布虚拟化相关的严重和警告事件 — 仅发布虚拟化相关的严重和警告事件，这是默认的事件发布级别
- 2 要启用所有硬件警报和事件，请选中对所有 **Dell EMC 主机启用警报**。

① 注：已启用警报的 Dell EMC 主机通过进入维护模式来响应某些特定的严重事件，您可以在需要时修改警报。

此时会显示**启用 Dell EMC 警报警告**对话框。
- 3 要接受更改，请单击**继续**，或取消更改，请单击**取消**。


① 注：选择对 Dell EMC 主机启用警报的情况下，确保您完成此步骤。
- 4 要恢复所有管理的 Dell EMC 服务器的默认 vCenter 警报设置，请单击**还原默认警报**。
可能需要片刻才能使更改生效。

① 注：恢复设备后，事件和警报设置未启用（即便在 GUI 中显示为启用）。您可以从设置选项卡重新启用可以从设置选项卡重新启用事件和警报设置。

① 注：BMC 陷阱没有消息 ID，因此警报在 OMI VV 中没有这些详细信息。

- 5 单击应用。

配置 SNMP 陷阱团体字符串

- 1 在 **OpenManage Integration for VMware vCenter** 页的**管理 > 设置**选项卡上，在**设备设置**下，单击对应于 **OMSA SNMP 陷阱团体字符串**的 。

此时将显示 **OMSA SNMP 陷阱团体字符串设置**对话框。默认情况下，**public** 显示在 SNMP 陷阱团体字符串中。

- 2 自定义任何字符串的公共文本，然后单击**应用**。

 **注:** 通过 OMIVV 安装或升级 OMSA 时，设置第 11 代 PowerEdge 服务器的 SNMP 陷阱团体字符串配置。

通过设置选项卡配置任务

使用设置选项卡，可以查看并执行以下配置任务：


- 启用 OMSA 链接。请参阅 [Enabling OMSA link](#) (启用 OMSA 链接)。
- 配置保修到期通知设置。请参阅 [Configuring warranty expiration notification settings](#) (配置保修到期通知设置)。
- 设置固件更新存储库。请参阅 [Setting up the firmware update repository](#) (设置固件更新存储库)。
- 配置最新设备版本通知。请参阅 [Configuring the latest appliance version notification](#) (配置最新设备版本通知)。
- 配置并查看事件和警报。请参阅 [配置事件和警报](#)。
- 查看资源清册和保修的数据检索计划。请参阅 [Viewing data retrieval schedules for inventory and warranty](#) (查看资源清册和保修的数据检索计划)。

设备设置

在本节中，请为 OMIVV 设备配置以下设置：

- 保修到期通知
- 固件更新存储库
- 最新设备版本通知
- 部署凭据

配置保修到期通知设置

- 1 在 **OpenManage Integration for VMware vCenter** 中的**管理 > 设置**选项卡上，在**设备设置**下单击**保修到期通知**。
- 2 展开**保修到期通知**以查看以下信息：
 - **保修到期通知** — 该设置是启用还是禁用
 - **警告** — 第一次警告设置的天数
 - **严重** — 严重警告设置的天数
- 3 配置保修到期阈值以警告保修到期，请单击  图标，位于**保修到期通知**右侧。
- 4 在**保修到期通知**对话框中，执行以下操作：
 - a 如果您希望启用该设置，请选择**为主机启用保修到期通知**。
选择该复选框将启用保修到期通知。
 - b 在**最少天数阈值警报**下，请执行以下操作：
 - 1 在**警告**下拉式列表中，选择您要提前获得保修到期警告的天数。
 - 2 在**严重**下拉式列表中，选择您要提前获得保修到期警告的天数。

5 单击应用。

设置固件更新存储库

关于此任务

可以在 OMIVV 设置选项卡上设置固件更新存储库。

注：您可以仅对于使用此存储库的非 VSAN 主机和群集更新固件。

步骤

- 1 在 OpenManage Integration for VMware vCenter 中的管理 > 设置选项卡上，在固件更新存储库右侧的设备设置下，单击  图标。
- 2 在固件更新存储库对话框中，选择以下选项之一：
 - **Dell 联机** — 固件更新默认存储库设置为 Dell 联机 (<https://downloads.dell.com>)。OMIVV 将从 Dell 存储库下载所选的固件更新并更新受管主机。
 - **Dell 定制联机** — OMIVV 从 Dell 定制联机下载所选固件更新并应用与受管主机（如有必要）。

注：根据网络设置，如果网络需要代理，则启用代理设置。

 - **共享网络文件夹** — 在基于 CIFS 或基于 NFS 的网络共享中，可以有一个本地的固件存储库。此存储库可以是 Dell 定期发布的 Server Update Utility (SUU) 的转储，或使用 DRM 创建的自定义存储库。OMIVV 应能访问此网络共享。

注：如果使用的是 CIFS 共享，则存储库密码不能超过 31 个字符。

注：确保使用最新的 Dell EMC Repository Manager (DRM) 版本 (3.0) 及更高版本。

 - a 如果您选择 **Dell 定制联机**，请按以下格式输入目录联机路径：
 - `http://share/filename.xml.gz`
 - `http://share/filename.gz`
 - `https://share/filename.xml.gz`
 - `https://share/filename.gz`
 - b 如果您选择**共享网络文件夹**，请使用以下格式输入目录文件位置：
 - XML 文件的 NFS 共享 — `host:/share/filename.xml`
 - GZ 文件的 NFS 共享 — `host:/share/filename.gz`
 - XML 文件的 CIFS 共享 — `\\host\share\filename.xml`
 - GZ 文件的 CIFS 共享 — `\\host\share\filename.gz`

注：OMIVV 仅支持基于服务器消息块 (SMB) 版本 1.0 和 SMB 版本 2.0 的 CIFS 共享。Dell EMC 建议使用基于 SMB 版本 2.0 的 CIFS 共享。

注：如果您使用的是 CIFS 共享，OMIVV 会提示您输入用户名和密码。
 - c 要验证给定的目录文件位置，请单击**开始测试**。此验证是进一步继续的必需步骤。
 -  — 表示测试连接成功。
 -  — 表示测试连接失败。
- 3 单击应用。

注：从源读取目录并更新 OMIVV 数据库可能需要长达 10 分钟。

使用 OMIVV 在 DRM 中创建目录

关于此任务

本节介绍了在 DRM 3.0 和更高版本中创建目录的流程。

步骤


- 1 在主页中，单击**添加新存储库**。
此时将显示**添加存储库**窗口。
- 2 在**添加存储库**窗口中，执行下列操作：
 - a 输入**存储库名称和说明**。
 - b 从**基础目录**下拉菜单中，选择一个目录。
 - c 从**集成类型**下拉菜单中，选择 **OpenManage Integration for VMware vCenter**。
- 3 在 **OpenManage Integration for VMware vCenter** 窗口中，输入**虚拟设备 IP**、**vCenter 服务器 IP**、**用户名和密码**，然后单击**连接**。
创建的目录显示在主页上。
- 4 要导出目录，选择一个目录，然后单击**导出**。

配置最新设备版本通知

关于此任务

要接收有关最新 OMIVV 版本 (RPM、OVF、RPM/OVF) 可用性的定期通知，请执行以下步骤以配置最新版本通知：

步骤

- 1 在 OpenManage Integration for VMware vCenter 中，在**管理**→**设置**选项卡的**设备设置**下，在**最新版本通知**的右侧，单击  图标。
默认情况下，最新版本通知处于禁用状态。
- 2 在**最新版本通知和检索计划**对话框中，执行以下操作：
 - a 如果想要启用最新版本通知，请选中**启用最新版本通知**复选框。
 - b 在**最新版本检索计划**下，为此作业选择一周当中的具体天数。
 - c 在**最新版本检索时间**中，指定所需的本地时间。
您提供的时间是您的本地时间。确保计算任何时间差，以便在正确的时间在 OMIVV 设备上运行此任务。
- 3 要保存设置，请单击**应用**；要重设设置，请单击**清除**；要中止操作，请单击**取消**。


配置部署凭据

使用部署凭据可以设置凭据来与通过自动查找发现的裸机系统进行安全通信，直至操作系统部署完成。为了与 iDRAC 安全地通信，OMIVV 从初始查找起直到部署过程结束，始终使用部署凭据。部署过程成功完成后，OMIVV 会将 iDRAC 凭据按连接配置文件中提供的进行更改。如果更改部署凭据，则从更改点起新查找到的所有系统将使用新凭据来配置。但是，部署凭据更改前查找到的服务器上的凭据不会受此更改的影响。

关于此任务

① | 注: OMIVV 用作配置服务器。在自动查找过程中，部署凭据允许您与使用 OMIVV 插件作为配置服务器的 iDRAC 进行通信。

步骤

- 1 在 OpenManage Integration for VMware vCenter 中的**管理** > **设置**选项卡上，在**部署凭据**右侧的**设备设置**下，单击  图标。
- 2 在**裸机服务器部署的凭据**中的**凭据**下，输入以下值：
 - 在**用户名**文本框中，输入用户名。
用户名不应该超过 16 个字符 (只能使用 ASCII 可打印字符)。

- 在 **密码** 文本框中，输入密码。
密码不应该超过 20 个字符（只能使用 ASCII 可打印字符）。
 - 在 **验证密码** 文本框中，再次输入密码。
确保密码匹配。
- 3 要保存指定的凭据，请单击**应用**。

vCenter 设置

在本节中，请配置以下 vCenter 设置：

- 启用 OMSA 链接。请参阅[启用 OMSA 链接](#)。
- 配置事件和警报。请参阅[配置事件和警报](#)。
- 配置资源清册和保修的数据检索计划。请参阅[查看资源清册和保修的数据检索计划](#)。

启用 OMSA 链接


先决条件

启用 OMSA 链接之前，安装并配置 OMSA Web 服务器。请参阅 *OpenManage Server Administrator Installation Guide*（OpenManage Server Administrator 安装指南）了解使用中的 OMSA 版本以及如何安装和配置 OMSA Web 服务器说明。

关于此任务

① | 注: 仅 Dell PowerEdge 第 11 代服务器需要 OMSA。

步骤

- 1 在 OpenManage Integration for VMware vCenter 中，在**管理 > 设置**选项卡上的 **vCenter 设置** 下，于 OMSA Web 服务器 URL 右侧，单击  图标。
- 2 在 **OMSA Web 服务器 URL** 对话框中，键入该 URL。
确保您包含完整的 URL 以及 HTTPS 和端口号 1311。

`https://<OMSA server IP or fqdn>:1311`

- 3 要将 OMSA URL 应用到所有 vCenter 服务器，请选择**将这些设置应用到所有 vCenter**。

① | 注: 如果未选中该复选框，OMSA URL 仅会应用到一个 vCenter。

- 4 要验证您提供的 OMSA URL 链接是否起作用，请导航至主机的**摘要**选项卡，然后检查 OMSA 控制台链接在 **OMIVV 主机信息** 部分中是否有效。

配置事件和警报

关于此任务


事件和警报对话框启用或禁用所有硬件警报。当前警报状态在 vCenter 警报选项卡上显示。严重事件表示实际或即将发生的数据损失或系统故障。警告事件并不一定是重大事件，但可表示将来可能的问题。

事件和警报还可以使用 VMware Alarm Manager 启用。事件在主机和群集视图中的 vCenter 任务和事件选项卡中显示。要接收来自服务器的事件，OMIVV 被配置为 SNMP 陷阱目标。对于第 12 代和更高版本的主机，SNMP 陷阱目标在 iDRAC 中设置。对于早于第 12 代的主机，陷阱目标在 OMSA 中设置。您可以使用**管理 > 设置**选项卡中的 OpenManage Integration for VMware vCenter 配置事件和警报。在 vCenter **设置** 下，展开**事件和警报**标题以显示 Dell EMC 主机的 vCenter 警报（已启用或已禁用）和事件发布级别。

① | 注: 对于第 12 代及之后的主机，OMIVV 支持 SNMP v1 和 v2 警报。对于早于第 12 代的主机，OMIVV 支持 SNMP v1 警报。

① | 注: 要接收 Dell 事件，请启用警报和事件。

步骤


- 1 在 Dell OpenManage Integration with VMware vCenter 中的**管理 > 设置**选项卡上，在 **vCenter 设置** 下展开**事件和警报**。此时会显示当前的 **Dell EMC 主机 vCenter 警报**（已启用或已禁用）和**事件发布级别**。
- 2 单击**事件和警报**右侧的图标。
- 3 要启用所有硬件警报和事件，请选中**对所有 Dell EMC 主机启用警报**。

注：已启用警报的 Dell EMC 主机通过进入维护模式来响应严重事件，您可以按需要修改警报。
- 4 要恢复所有管理的 Dell 服务器的默认 vCenter 警报设置，请单击**还原默认警报**。
此步骤可能需要片刻才能使更改生效，且选中**对所有 Dell EMC 主机启用警报**后才可用。
- 5 在**事件发布级别**中，选择“不发布任何事件”、“发布所有事件”、“仅发布严重和警告事件”或“仅发布虚拟化相关的严重和警告事件”。有关更多信息，请参阅 *OpenManage Integration for VMware vCenter User's Guide* (*OpenManage Integration for VMware vCenter 用户指南*) 中**事件、警报和运行状况监测**部分。
- 6 如果希望将这些设置应用到所有 vCenter，请选中**将这些设置应用到所有 vCenter**。

注：选中该选项后将覆盖所有 vCenter 的现有设置。

注：如果已从设置选项卡上的下拉式列表中选择所有已注册的 vCenter，该选项将不可用。
- 7 要进行保存，请单击**应用**。

查看资源清册和保修的数据检索计划

- 1 在 Dell OpenManage Integration with VMware vCenter 中的**管理 > 设置**选项卡上，在 **vCenter 设置** 下单击**数据检索计划**。单击后，“数据检索计划”展开以显示资源清册和保修的编辑选项。
- 2 单击图标，以防止**资源清册检索**或**保修检索**。
在**资源清册/保修数据检索**对话框中，您可以查看以下资源清册或保修检索的信息：
 - 资源清册和/或保修检索选项是启用还是禁用？
 - 启用的周中日期。
 - 启用的时间。
- 3 要编辑数据检索计划，请执行以下步骤：
 - a 在**资源清册/保修数据**下，选择**启用资源清册/保修数据检索**复选框。
 - b 在**资源清册/保修数据检索计划**下，为您的作业选择一周当中的具体天数。
 - c 在**资源清册/保修数据检索时间**文本框中，为此作业键入本地时间。
您可能需要考虑作业配置时间与作业实施时间之间的时间差。
 - d 要保存设置，请单击**应用**；要重设设置，请单击**清除**；要中止操作，请单击**取消**。
- 4 再次单击**数据检索计划**以确定资源清册和保修计划，并显示单行。

创建机箱配置文件

需要机箱配置文件来监测机箱。可以创建一个机箱凭据配置文件并将其与一个或多个机箱关联。

关于此任务

您可以使用 Active Directory 凭据登录 iDRAC 和主机。

步骤


- 1 在 OpenManage Integration for VMware vCenter 中，单击**管理**。
- 2 单击**配置文件**，然后单击**凭据配置文件**。
- 3 展开**凭据配置文件**，然后单击**机箱配置文件**选项卡。
- 4 在**机箱配置文件**页面，单击图标以创建一个**新机箱配置文件**。
- 5 在**机箱配置文件**向导页面，请执行以下操作：
在**名称和凭据**部分中的**机箱配置文件**下：

- a 在**配置文件名称**文本框中，输入配置文件名称。
- b 在**说明**文本框中，输入可选的说明。

在**凭据**部分中：

- a 在**用户名**文本框中，键入具有管理权限的用户名（通常用于登录到 Chassis Management Controller）。
- b 在**密码**文本框中，输入相应用户名的密码。
- c 在**验证密码**文本框中，输入在**密码**文本框中所输入的相同的密码。两个密码必须匹配。

注：该凭据可以是本地或 Active Directory 凭据。在结合使用 Active Directory 凭据和机箱配置文件之前，在 Active Directory 中必须存在 Active Directory 用户的帐户，并且必须为 Chassis Management Controller 配置基于 Active Directory 的验证。

- 6 单击 。将机箱与机箱配置文件关联。

注：只有在对机箱中存在的所有模块化主机成功运行资源清册之后，这些可供查找、可用并可用添加 MX 机箱手动添加的机箱才可与机箱配置文件相关联。

- 7 要选择一个机箱或多个机箱，请选择 **IP/主机名列**旁边的相应的复选框。

如果已选定的机箱是另一个配置文件的一部分，则会显示一条警告消息，指出所选的机箱与某个配置文件相关联。

例如，您有一个与机箱 A 相关联的配置文件**测试**。如果创建另一个配置文件**测试 1**并尝试将机箱 A 与**测试 1**关联，则会显示警告信息。

- 8 单击**确定**。


将显示**关联的机箱**页面。

- 9 必须进行测试连接，且为所选机箱自动运行。

测试连接将在以下情况下自动运行：

- 在首次选中机箱后
- 在您更改凭据时
- 如果该机箱为全新所选机箱

注：对于配置有 MCM 组的 MX 机箱，Dell EMC 建议使用主机箱管理所有主机箱和成员机箱。成员机箱测试连接操作将失败，并且测试结果显示为失败。单击主要机箱 IP，以查找完整的 MCM 组。

测试结果在**测试结果**列中显示为**通过**或**失败**。要手动测试机箱连接，请选择机箱并单击 。

注：如果主机在与添加的 MX 机箱关联的注册 vCenter 中不存在，相应的机箱测试连接将失败。

注：只有成功验证的机箱才会与机箱配置文件相关联。

- 10 要完成配置文件，请单击**完成**。

注：确保您至少拥有一个已成功验证的机箱，以完成向导。

要添加 MX 机箱管理模块 IP，请参阅**用户指南**中的**添加 MX 机箱 IP 或 FQDN**主题。

访问 Dell EMC 支持站点上的文档

您可以使用以下链接访问所需的文档：

- Dell EMC 企业系统管理文档 — www.dell.com/SoftwareSecurityManuals
- Dell EMC OpenManage 文档 — www.dell.com/OpenManageManuals
- Dell EMC 远程企业系统管理文档 — www.dell.com/esmmanuals
- iDRAC 和 Dell EMC 生命周期控制器文档 — www.dell.com/idracmanuals
- Dell EMC OpenManage 连接企业系统管理文档 — www.dell.com/OMConnectionsEnterpriseSystemsManagement
- Dell EMC 可维护性工具文档 — www.dell.com/ServiceabilityTools
- a 转至 www.dell.com/Support/Home。
- b 单击从所有产品中选择。
- c 从所有产品部分，单击软件和安全，然后单击以下部分中的所需链接：
 - 企业系统管理
 - 远程企业系统管理
 - 维护工具
 - Dell 客户端命令套件
 - Connections 客户端系统管理
- d 要查看文档，请单击所需的产品版本。
- 使用搜索引擎：
 - 在搜索框中键入文档的名称和版本。

相关说明文件

除本指南外，您还可以访问 [Dell.com/support](https://www.dell.com/support) 上提供的其他指南。单击**从所有产品中进行选择**，然后单击**软件和安全 > 虚拟化解决方案**。单击 **OpenManage Integration for VMware vCenter 4.3** 访问下列说明文件：

- *OpenManage Integration for VMware vCenter Version 4.3 Web Client User's Guide (OpenManage Integration for VMware vCenter 4.3 版 Web 客户端用户指南)*
- *OpenManage Integration for VMware vCenter Version 4.3 Release Notes (OpenManage Integration for VMware vCenter 4.3 版发行说明)*
- *OpenManage Integration for VMware vCenter Version 4.3 Compatibility Matrix (OpenManage Integration for VMware vCenter 4.3 版兼容性值表)*

您可以在 <https://www.dell.com/support> 上找到包括白皮书在内的技术资料。