

OpenManage Integration for VMware vCenter 版本 4.1

Web 客户端用户指南

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。

版权所有 © 2017 Dell Inc. 或其附属公司。保留所有权利。Dell、EMC 和其他商标均为 Dell Inc. 或其附属公司的商标。其他商标均为其各自所有者的商标。

1 简介.....	9
此版本中的新功能.....	9
OpenManage Integration for VMware vCenter 功能.....	9
2 关于管理控制台.....	11
使用管理门户.....	11
以非管理员用户的身份注册 vCenter 服务器.....	11
注册 vCenter 服务器.....	14
将许可证上传到管理控制台.....	15
管理虚拟设备.....	16
设置全局警报.....	20
管理备份和还原.....	21
关于 vSphere 客户端控制台.....	22
3 管理多个设备.....	25
4 从 Web 客户端访问 OpenManage Integration.....	26
在 VMware vCenter Web 客户端中导航.....	26
Web 客户端中的图标.....	27
查找软件版本.....	27
刷新屏幕内容.....	27
查看 Dell EMC 主机.....	28
查看 OpenManage Integration for VMware vCenter 许可选项卡.....	28
访问帮助和支持.....	28
下载故障排除包.....	29
重设 iDRAC.....	30
打开联机帮助.....	30
启动管理控制台.....	30
查看日志历史记录.....	31
查看日志.....	32
导出日志文件.....	32
5 OpenManage Integration for VMware vCenter 许可.....	33
购买并上传软件许可证.....	33
6 VMware vCenter 的设备配置.....	35
通过配置向导配置任务.....	35
查看配置向导“欢迎”对话框.....	35
选择 vCenter.....	36
创建连接配置文件.....	36

计划资源清册作业	38
运行保修检索作业.....	38
配置事件和警报	39
通过设置选项卡配置任务.....	39
设备设置.....	40
vCenter 设置.....	41
7 配置文件.....	44
关于连接配置文件.....	44
查看连接配置文件.....	44
创建连接配置文件.....	45
修改连接配置文件.....	46
删除连接配置文件.....	48
测试连接配置文件.....	48
关于机箱配置文件.....	48
查看机箱配置文件.....	49
创建机箱配置文件.....	49
编辑机箱配置文件.....	50
删除机箱配置文件.....	50
测试机箱配置文件.....	51
8 资源清册和保修管理.....	52
资源清册作业.....	52
查看主机资源清册.....	53
查看机箱资源清册.....	54
修改资源清册作业计划.....	54
运行资源清册作业.....	55
立即运行机箱资源清册作业.....	55
保修作业.....	55
查看保修历史.....	56
查看机箱保修.....	56
修改保修作业计划.....	57
立即运行主机保修作业.....	57
立即运行机箱保修作业.....	58
监测单个主机.....	58
查看主机摘要详细信息.....	58
查看单个主机的硬件详细信息.....	60
查看单个主机的存储设备详细信息.....	62
有关 Web 客户端中的系统事件日志.....	64
查看单个主机的其他硬件详细信息.....	65
监测群集和数据中心中的主机.....	66
查看数据中心和群集的概览.....	66
查看数据中心和群集的硬件详细信息.....	68
查看数据中心和群集的存储详细信息.....	69

查看数据中心和群集的其他硬件详细信息.....	71
设置物理服务器闪烁指示灯.....	72
配置系统锁定模式.....	73
9 关于固件更新.....	74
为单个主机运行固件更新向导.....	74
运行群集的固件更新向导.....	76
管理固件更新作业.....	77
10 事件、警报和运行状况监测.....	79
关于主机的事件和警报.....	79
About events and alarms for chassis.....	80
Viewing chassis events.....	80
Viewing chassis alarms.....	80
与虚拟化相关的事件.....	81
主动式高可用性事件.....	86
查看警报和事件设置.....	87
查看事件.....	87
硬件组件冗余运行状况 — 主动式高可用性.....	87
配置机架式和塔式服务器的主动式高可用性.....	88
启用群集的主动式高可用性.....	89
覆盖运行状况更新通知的严重性.....	90
启动管理控制台.....	90
启动远程访问控制台 (iDRAC).....	90
启动 OMSA 控制台.....	91
启动 Chassis Management Controller 控制台 (CMC).....	91
11 机箱管理.....	92
查看机箱摘要详细信息.....	92
查看机箱的硬件资源清册信息.....	93
查看机箱的其他硬件配置.....	95
查看机箱的关联主机.....	97
12 部署虚拟机监控程序.....	98
设备查找.....	99
手动查找.....	99
OpenManage Integration for VMware vCenter 中的自动查找.....	99
移除裸机服务器.....	102
配置.....	102
配置硬件配置文件.....	103
在参考服务器上启用 CSIOR.....	104
创建或自定义硬件配置文件.....	104
创建或克隆硬件配置文件.....	106
管理硬件配置文件.....	106

创建虚拟机监控程序配置文件.....	107
管理虚拟机监控程序配置文件.....	107
创建部署模板.....	108
管理部署模板.....	108
有关部署向导.....	109
VLAN 支持.....	109
运行部署向导.....	110
使用作业队列管理部署作业.....	112
部署作业时间.....	113
部署顺序中的服务器状态.....	113
下载自定义 Dell EMC ISO 映像.....	113
13 关于主机、裸机和 iDRAC 符合性.....	114
报告和修正 vSphere 主机的符合性.....	114
修补 vSphere 主机的 iDRAC 许可证符合性.....	116
对第 11 代服务器使用 OMSA.....	116
在 ESXi 系统上部署 OMSA 代理.....	116
设置 OMSA 陷阱目标.....	117
报告和修补裸机服务器的符合性.....	117
修补裸机服务器的 iDRAC 许可证符合性.....	118
刷新裸机服务器.....	118
14 安全角色和权限.....	119
数据完整性.....	119
访问控制验证、授权和角色.....	120
Dell 操作角色.....	120
Dell 基础架构部署角色.....	120
关于权限.....	120
15 故障排除.....	123
常见问题 (FAQ)	123
为什么在 Google Chrome 中“全部导出”按钮无法导出到 .csv 文件？.....	123
对于不兼容的 vSphere 主机，iDRAC 许可证类型和说明显示不正确.....	123
从较早的 OMIVV 版本注销 vCenter 后将不显示 Dell EMC 图标，然后用更高的 OMIVV 版本注册相同的 vCenter.....	124
每次调用时配置向导设置都会被默认设置覆盖.....	124
为什么 Dell Inc 未作为运行状况更新提供商显示.....	124
为什么在 ESXi 5.x 主机上资源清册执行固件更新失败？.....	125
主机资源清册或测试连接由于 iDRAC IP 无效或未知而导致失败。如何获得一个有效的 iDRAC IP？... ..	125
运行修复不兼容的 vSphere 主机向导时，为什么特定主机的状态显示为“未知”？.....	125
在注册 OMIVV 设备时分配的 Dell 权限，在取消注册 OMIVV 后不会删除.....	125
尝试筛选严重性类别时，Dell Management Center 不显示所有相关日志。我该如何查看所有日志？.. ..	126
如何解决 VMware 证书颁发机构 (VMCA) 导致的错误代码 2000000？.....	126
在管理控制台中，将设备重设为出厂设置后，为何更新存储库路径未设置为默认路径？.....	130

为什么不能对从作业队列页面中选择的所有 vCenter 应用保修和资源清册计划？	130
在 OMIVV 中更改 DNS 设置后在 vCenter Web 客户端中出现 Web 通信错误时该怎么办？	130
如果离开再返回设置页面，为何设置页面无法加载？	131
在初始配置向导的资源清册计划/保修计划页面中，为何会显示“无法计划在过去的时间执行任务”错误？	131
在固件页面中，一些固件的安装日期为何显示为 12/31/1969？	131
连续全局刷新会导致“最近的任务”窗口引发异常。如何解决此错误？	131
为什么在 IE 10 中少数 Dell 屏幕中的 Web 客户端 UI 会失真？	131
为何即使 OpenManage Integration 插件已成功注册到 vCenter，我在 Web 客户端上仍然看不到 OpenManage Integration 图标？	132
即便我的存储库中包含所选 11G 系统的捆绑包，为何固件更新显示没有固件更新的捆绑包？	132
如果使用 DHCP 值覆盖设备 IP 和 DNS 设置，为什么要在设备重新引导后将 DNS 配置设置到原始设置	132
不支持使用 OMIVV 更新固件版本为 13.5.2 的 Intel 网卡	132
由于 DUP 存在分段要求，使用 OMIVV 将 Intel 网卡从 14.5 或 15.0 更新至 16.x 失败	133
为什么在尝试使用无效的 DUP 执行固件更新时，尽管 LC 中的作业状态显示“失败”，但 vCenter 控制台上的硬件更新作业状态在数小时内既非失败也非超时？	133
为什么“管理控制台”显示无法获取更新存储库位置？	133
当我执行一对多固件更新时，为什么系统无法进入维护模式？	133
为什么在一些电源设备状态已变为严重时，机箱全局运行状况仍然为良好？	133
为什么在“系统概览”页面的“处理器视图”中处理器版本中为“不适用”？	134
OMIVV 配置和支持哪一代 Dell 服务器的 SNMP 陷阱？	134
OMIVV 管理哪些 vCenter 服务器？	134
OMIVV 是否支持处于链接模式的 vCenter？	134
什么是 OMIVV 所需的端口设置？	134
硬件配置文件或系统配置文件的用户具有 iDRAC 用户列表中的新更改凭据，在成功应用该配置文件后，用于裸机查找的相同用户的密码为什么未更改？	135
为什么无法在“vCenter 主机和群集”页面上查看新 iDRAC 版本的详细信息？	136
我如何使用 OMSA 模拟温度硬件故障来测试事件设置？	136
尽管 OMIVV 主机系统上已安装 OMSA 代理程序，我仍然收到 OMSA 未安装的错误消息。如何处理该错误？	136
OMIVV 已启用锁定模式的情况下是否支持 ESXi？	137
在我尝试使用锁定模式时失败	137
如果在使用参考服务器的情况下创建硬件配置文件失败该怎么办？	137
为什么尝试在服务器上部署 ESXi 失败？	137
为什么我的虚拟机监控程序在 Dell PowerEdge R210 II 机器上部署失败？	137
为什么部署向导中自动发现的系统未显示型号信息？	137
NFS 共享设置了 ESXi ISO，但装载共享位置错误造成部署失败	138
我如何强制移除虚拟设备？	138
在“立即备份”屏幕中输入密码时收到错误消息	138
在 vSphere Web 客户端中，单击 Dell Server Management Portlet 或 Dell 图标时返回 404 错误	138
如果固件更新失败应该怎么办？	138
如果 vCenter 注册失败，应该怎么办？	138
连接配置文件测试凭据的性能缓慢或没有响应	139

OMIVV 是否支持 VMware vCenter 服务器设备？	139
为什么在我使用“在下次重新引导时应用”选项执行了固件更新并且重新引导系统后，我的固件级别未更新？	139
为什么在从 vCenter 树中移除主机后主机仍显示在机箱下？	139
在管理控制台中，将设备重设为出厂设置后，为何更新存储库路径未设置为默认路径？	139
在备份和还原 OMIVV 后，为何警报设置没有被还原？	140
当在目标节点上启用 NIC 分区 (NPAR) 并且在系统配置文件中禁用该分区时，虚拟机监控程序部署失败。	140
当可用版本低于当前版本时，可用的虚拟设备版本显示错误信息	140
裸机部署问题	140
在新购买的系统上启用自动查找	140
16 相关说明文件	142
从 Dell 支持站点访问说明文件	142
附录 A: 系统特定属性	143
iDRACBIOSRAIDCNAFC	143
附录 B: 自定义属性	147
附录 C: 附加信息	148

简介

IT 管理员使用 VMware vCenter 作为主要控制台，以管理和监测 VMware vSphere ESX/ESXi 主机。OpenManage Integration for VMware vCenter (OMIVV) 提供增强的部署、管理、监测和升级功能，使您能够从 VMware web 客户端更好地管理 Dell 主机。

主题：

- [此版本中的新功能](#)
- [OpenManage Integration for VMware vCenter 功能](#)

此版本中的新功能

此版本的 OpenManage Integration for VMware vCenter 提供以下功能：

- 支持 vSphere 6.0 U3 和 6.5 U1
- 支持 OMSA 8.5。
- 支持第 14 代服务器的 iDRAC9 锁定模式
- 支持第 14 代服务器的系统配置文件 (SCP)
- 支持 SNMP 陷阱增强功能
- 支持第 14 代平台

OpenManage Integration for VMware vCenter 功能

以下是 OpenManage Integration for VMware vCenter (OMIVV) 设备功能：

表. 1: OMIVV 功能

功能	说明
资源清册	资源清册功能提供了以下选项： <ul style="list-style-type: none"> • PowerEdge 服务器详细信息，例如内存 — 数量和类型、NIC、PSU、处理器、RAC、保修信息、服务器、群集和数据中心级别视图。 • 机箱详细信息，比如机箱管理控制器信息、机箱电源、KVM 状态、风扇/散热详细信息、保修信息、闲置交换机/服务器详细信息。
监测和发送警报	监测和警报包括以下功能： <ul style="list-style-type: none"> • 检测关键硬件故障并执行虚拟化感知操作。例如，迁移工作负载或将主机置于维护模式。 • 提供情报（例如资源清册、事件、警报）来诊断服务器问题。 • 支持 VMware 主动式高可用性功能。
固件更新	将 Dell EMC 硬件更新到最新版本的 BIOS 和固件。

功能	说明
部署和配置	创建硬件配置文件、系统配置文件、虚拟机监控程序配置文件，并且使用 VMware vCenter（不使用 PXE）远程部署在裸机 PowerEdge 服务器上的操作系统。
服务信息	从 Dell 的保修数据库检索 Dell EMC 服务器及其关联机箱的保修信息，以便进行联机保修升级。
安全角色和权限	安全角色和权限包括以下功能： <ul style="list-style-type: none"> 与标准 vCenter 验证、规则和权限集成。 支持第 14 代服务器中的 iDRAC 锁定模式。

① **注:** 从 OMIVV 4.0 开始，仅支持 VMware vSphere Web 客户端，不支持 vSphere Desktop 客户端。

① **注:** 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。

① **注:** OMIVV 4.1 只是一个 OVF 发行版。对于一个 OVF 发行版，请确保您从现有版本备份 OMIVV 数据库，并将其在最新可用设备版本中还原。有关更多信息，请参阅[通过备份和还原更新设备](#)。

关于管理控制台

可以使用以下两个管理门户实现对 OpenManage Integration for VMware vCenter 及其虚拟环境的管理：

- 基于 Web 的 Administration Console
- 单个服务器的控制台视图（OMIVV 设备的虚拟机控制台）

使用管理门户

您可以使用管理控制台执行以下任务：

- 注册 vCenter 服务器。请参阅[注册 vCenter 服务器](#)。
- 修改 vCenter 登录凭据。请参阅[修改 vCenter 登录凭据](#)。
- 更新 SSL 证书。请参阅[更新已注册 vCenter 服务器的 SSL 证书](#)。
- 上传或购买许可证。如果您正在使用的是演示许可证，将显示[购买软件](#)链接。通过单击此链接，您可以购买用于管理多个主机的全版本许可证。请参阅[将许可证上传到管理控制台](#)。
- 更新 OMIVV。请参阅[更新虚拟设备存储库位置和虚拟设备](#)。
- 生成故障排除捆绑包。请参阅[下载故障排除包](#)。
- 重新启动 OMIVV。请参阅[重新启动虚拟设备](#)。
- 执行备份和还原。请参阅[通过备份和还原更新设备](#)。
- 配置警报。请参阅[设置全局警报](#)。

以非管理员用户的身份注册 vCenter 服务器

您可使用 vCenter 管理员凭据或具有必要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](#)。

① 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。

① 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。请参阅[使用具有所需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[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：

① 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

① 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
 - 查询补丁程序
 - 安全配置文件和防火墙

① 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
 - 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

① 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

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 vCenter 服务器](#)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: 确保以具有管理员权限的用户身份登录。

步骤

- 1 使用拥有管理权限的帐户登录到 vSphere Web 客户端。
- 2 在 vSphere Web 客户端中浏览至**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，并单击  图标。
- 5 为所选角色选择以下 Dell 权限，然后单击**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”[安全角色和权限](#)。

对权限和角色的更改立即生效。具有必需权限的用户现在可执行 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 vCenter 服务器

关于此任务

安装 OpenManage Integration for VMware vCenter 后，您可以注册 OMIVV 设备。OpenManage Integration for VMware vCenter 使用具有必要 vCenter 操作权限的管理员用户帐户或非管理员用户帐户。单个 OMIVV 设备实例可支持总共 10 台 vCenter 服务器和多达 1000 台 ESXi 主机。

要注册新 vCenter 服务器，请执行以下步骤：

步骤

- 1 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://<设备 IP|主机名>` URL。
- 2 在左侧窗格中，单击 **VCENTER 注册**，然后单击**注册新 vCenter 服务器**。
- 3 在**注册新 vCenter** 对话框中的 **vCenter 名称**下，执行以下步骤：
 - a 在 **vCenter 服务器 IP 或主机名**文本框中，输入 vCenter 的 IP 地址或主机的 FQDN。

① 注：建议使用完全限定域名 (FQDN) 通过 VMware vCenter 注册 OMIVV。对于所有注册，vCenter 的主机名应通过 DNS 服务器正确解析。建议您遵循以下建议的实践方法来使用 DNS 服务器：

 - 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。
 - b 在**说明**文本框中，输入说明（可选）。
- 4 在 **vCenter 用户帐户**下，请执行以下步骤：
 - a 在 **vCenter 用户名**文本框中，输入管理员的用户名或具有必要权限的非管理员用户名。
 - b 在 **密码**文本框中，输入密码。
 - c 在 **验证密码**文本框中，再次输入密码。
- 5 单击 **Register**（注册）。

注册 vCenter 服务器后，OMIVV 注册为 vCenter 插件，“Dell EMC OpenManage Integration”图标出现在 vSphere Web 客户端中，通过它可以访问 OMIVV 功能。

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。

实例

具有必要权限的用户 X 在 vCenter 中注册 OMIVV，用户 Y 仅有 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 的权限将主机置于维护模式或重新引导主机。

修改 vCenter 登录凭据

vCenter 登录凭据可由具有管理权限的用户或具有必要权限的非管理员用户修改。

- 1 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://<设备 IP|主机名>` URL。
- 2 在**登录**对话框中，键入密码并单击**登录**。
- 3 在左侧窗格中，单击 **VCENTER 注册**。
已注册的 vCenter 服务器将显示在 **MANAGE VCENTER SERVER CONNECTIONS** 窗口的右侧窗格中。要打开**修改用户帐户**窗口，请在**凭据**下单击已注册 vCenter 的**修改**。
- 4 输入 vCenter **用户名**、**密码**和**验证密码**；密码必须匹配。
- 5 要更改密码，请单击**应用**；或者要取消更改，请单击**取消**。

① **注:** 如果提供的用户没有所需的权限，则会显示一条错误消息。

更新已注册 vCenter 服务器的 SSL 证书

OpenManage Integration for VMware vCenter 通过使用 2048 位密钥长度的 RSA 加密标准，使用 OpenSSL API 创建证书签名请求 (CSR)。OMIVV 生成的 CSR 将从受信任的证书机构获得数字签名的证书。OpenManage Integration for VMware vCenter 使用数字证书在 Web 服务器上启用 SSL 以用于安全通信。

关于此任务

如果 vCenter 服务器上的 SSL 证书更改，请使用以下步骤导入 OpenManage Integration for VMware vCenter 的新证书：

- 步骤**
- 1 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://<设备 IP|主机名>` URL。
 - 2 在左侧窗格中，单击 **VCENTER 注册**。
已注册的 vCenter 服务器显示在右侧窗格中。
 - 3 要更新 vCenter 服务器 IP 或主机名的证书，请单击**更新**。

卸载 OpenManage Integration for VMware vCenter

关于此任务

要移除 OpenManage Integration for VMware vCenter，请使用管理控制台将 OMIVV 从 vCenter 服务器注销。

① **注:** 确保资源清册、保修或部署作业正在运行时不会从 vCenter 服务器注销 OMIVV。

- 步骤**
- 1 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://<设备 IP|主机名>` URL。
 - 2 在 **vCenter 注册**页面中，从 **vCenter 服务器 IP 或主机名表**，单击**注销**。
① **注:** 由于可能有多个 vCenter，请确保您选择正确的 vCenter。
 - 3 要确认注销所选的 vCenter 服务器，请在**注销 vCenter**对话框中单击**注销**。

① **注:** 如果已在群集上启用主动式高可用性，请确保在群集上禁用主动式高可用性。如需禁用主动式高可用性，请访问群集的主动式高可用性故障和响应屏幕，方法是：选择**配置 > 服务 > vSphere 可用性**，然后单击**编辑**。如需禁用主动式高可用性：在主动式高可用性故障和响应屏幕中，根据 Dell Inc 提供商清除此复选框。

将许可证上传到管理控制台

关于此任务

可以上传 OMIVV 许可证以更改受支持的并发已注册 vCenter 实例和受管主机数。如果需要添加更多主机，您也可以执行以下步骤以添加许可证：

- 步骤**
- 1 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://<设备 IP|主机名>` URL。
 - 2 在**登录**对话框中，键入密码。
 - 3 在左侧窗格中，单击 **VCENTER 注册**。
已注册的 vCenter 服务器显示在右侧窗格中。
 - 4 单击**上传许可证**。
 - 5 在**上传许可证**对话框中，单击**浏览**以导航至许可证文件，然后单击**上传**。

① | 注: 如果修改或编辑了许可证文件, 则 MOIVV 设备会将其视为已损坏并且许可证文件不会起作用。

管理虚拟设备

关于此任务

虚拟设备管理使您能够管理 OpenManage Integration for VMware vCenter 网络、版本、NTP 和 HTTPS 信息, 并可以让管理员:

- 重新启动虚拟设备。请参阅[重新启动虚拟设备](#)。
- 更新虚拟设备, 以及配置更新存储库位置。[更新虚拟设备存储库位置和虚拟设备](#)。
- 设置 NTP 服务器。请参阅[设置网络时间协议服务器](#)。
- 上传 HTTPS 证书。请参阅[上传 HTTPS 证书](#)。

在 OpenManage Integration for VMware vCenter 中, 请执行以下步骤以通过管理控制台访问[设备管理](#)页面:

步骤

- 1 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://<设备 IP|主机名>` URL。
- 2 在[登录](#)对话框中, 键入密码。
- 3 要配置设备管理部分, 请在左侧窗格中, 单击[设备管理](#)。

重新启动虚拟设备

- 1 在[设备管理](#)页面中, 单击[重新启动虚拟设备](#)。
- 2 要重新启动虚拟设备, 请在[重新启动虚拟设备](#)对话框中, 单击[应用](#), 或单击[取消](#)取消操作。

更改虚拟设备的主机名

关于此任务

执行以下步骤:

步骤

- 1 在[设备管理](#)页面, 单击[更改主机名](#)。
- 2 输入更新的主机名。
键入以下格式的域名: `<主机名>`。
- 3 单击[更新主机名](#)。
设备主机名已更新, 并返回主菜单。
- 4 要重新引导设备, 单击[重新引导设备](#)。

① | 注: 如果您已使用设备注册任何 vCenter 服务器, 则注销, 然后重新注册所有 vCenter 实例。

① | 注: 确保您手动更新其环境中的虚拟设备的所有参考信息, 如在 iDRAC、DRM 中配置服务器。

更新虚拟设备存储库位置和虚拟设备

前提条件

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[管理备份和还原](#)。

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。

① **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[设置 HTTP 代理](#)。

① **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。

① **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。

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[设置 HTTP 代理](#)。

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: <http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/>。如果路径不同, 则在[设备管理](#)窗口的[设备更新](#)区域中, 单击[编辑](#)以便在[更新存储库路径](#)文本框中将路径更新到 <http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/>。要进行保存, 请单击[应用](#)。
- 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 <http://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:** 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://<ApplianceIP>/hostname> 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 OMIVV 版本 x 更新至版本 y, 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 设备的电源。

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 版本 y OVF。

4 开启 OpenManage Integration 版本 y 设备电源。

5 设置版本 y 设备的网络、时区等。

① **注:** 确保新的 OpenManage Integration 版本 y 设备与旧设备具有相同的 IP 地址。

① **注:** 如果版本 y 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 将数据库还原到新的 OMIVV 设备。请参阅[从备份还原 OMIVV 数据库](#)。

7 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”。

8 对所有已注册的 vCenter 服务器运行[资源清册](#)。

① **注:** 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[计划资源清册作业](#)。

① **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 陷阱的陷阱目标以指向新设备。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 陷阱不指向新 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[运行修复不符合要求的 vSphere 主机向导](#)。

下载故障排除捆绑包

- 1 在设备管理页面中，单击生成故障排除捆绑包。
- 2 单击[下载故障排除捆绑包](#)链接。
- 3 单击关闭。

设置 HTTP 代理

- 1 在设备管理页面中，向下滚动至 HTTP 代理设置，然后单击编辑。
- 2 在编辑模式下执行以下操作：
 - a 选择已启用以启用 HTTP 代理设置的使用。
 - b 在代理服务器地址中输入代理服务器地址。
 - c 在代理服务器端口中输入代理服务器端口。
 - d 选择是以使用代理凭据。
 - e 如果使用代理凭据，请在用户名中输入用户名。
 - f 在密码中键入密码。
 - g 单击应用。

设置网络时间协议 (NTP) 服务器

关于此任务

可使用网络时间协议 (NTP) 同步虚拟设备时钟与 NTP 服务器的时钟。

步骤

- 1 在设备管理页面中，单击 NTP 设置区域中的编辑。
- 2 选中已启用。输入首选和次要 NTP 服务器的主机名或 IP 地址，然后单击应用。

① **注:** 虚拟设备时钟与 NTP 服务器同步可能约需 10 分钟。

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. 2: 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

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。

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 设备的电源。

生成证书签名请求

前提条件

确保您上传证书后再将 OMIVV 注册到 vCenter。

关于此任务

生成新的证书签名请求 (CSR) 可防止使用以前生成的 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**。

此时会显示一条消息，表述如果生成了新请求，使用以前的 CSR 创建的证书不能再上传到设备。要继续该请求，请单击**继续**，或单击**取消**以取消操作。

- 2 如果继续请求，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

前提条件

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。

① 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 如果要中止上传，请单击**取消**中止操作。

还原默认的 HTTPS 证书

关于此任务

① 注: 如果想为设备上传自定义证书，请确保在 vCenter 注册前上传新证书。如果是在 vCenter 注册后上传新的自定义证书，Web 客户端中将显示通信错误。要解决此问题，必须在 vCenter 中注销设备，然后再重新注册。

步骤

- 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**。

设置全局警报

关于此任务

警报管理功能允许您输入用于确定所有 vCenter 实例的警报存储方式的全局设置。

步骤

- 1 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://<设备 IP|主机名>` URL。
- 2 在**登录**对话框中，键入密码。
- 3 在左侧窗格中，单击**警报管理**。要输入新的 vCenter 警报设置，请单击**编辑**。
- 4 输入以下字段的数值：
 - **最大警报数**
 - **保留警报的天数**
 - **重复警报超时（秒数）**
- 5 要保存您的设置，请单击**应用**，或单击**取消**取消操作。

管理备份和还原

关于此任务

管理备份和还原在管理控制台完成。此页面上的任务包括：

- 配置备份和还原
- 计划自动备份
- 执行即时备份
- 从备份还原数据库

在 OpenManage Integration for VMware vCenter 中，请执行以下步骤以通过管理控制台访问**备份和还原设置**页面：

步骤

- 1 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://<设备 IP>主机名` URL。
- 2 在**登录**对话框中，键入密码。
- 3 在左侧窗格中，单击 **备份和还原**。

配置备份和还原

备份和还原功能将 OMIVV 数据库备份到远程位置，以后可从该位置进行还原。配置文件、模板和主机信息都包括在备份中。建议您计划自动备份以防止数据丢失。

关于此任务

注： NTP 设置未保存和还原。

步骤

- 1 在**备份和还原设置**页面中，单击**编辑**。
- 2 在突出显示的**设置和详细信息**区域，执行以下操作：
 - a 在**备份位置**，键入备份文件的路径。
 - b 在**用户名**中，键入用户名。
 - c 在**密码**中，键入密码。
 - d 在**输入用于加密备份的密码**中，在文本框中键入加密的密码。
加密密码可以包含字母数字字符和特殊字符，比如“!`@#$%*`”。
 - e 在**验证密码**中，重新键入加密的密码。
- 3 要保存这些设置，请单击 **应用**。
- 4 配置备份计划。请参阅**计划自动备份**。

后续步骤

此步骤后，配置备份计划。

计划自动备份

关于此任务

有关配置备份位置和凭据的更多信息，请参阅**配置备份和还原**。

步骤

- 1 在**备份和还原设置**页面中，单击**编辑自动计划的备份**。
相关字段已启用。
- 2 要启用备份，请单击**已启用**。
- 3 选中您要运行备份于每周的星期几的**备份星期**复选框。

- 4 在**备份时间（24 小时，HH:mm）**中，以 HH:mm 格式输入时间。
下一个备份将填充下一计划备份的日期和时间。
- 5 单击**应用**。

执行即时备份

- 1 在**备份和还原设置**页面中，单击**立即备份**。
- 2 要使用来自备份设置的位置和加密密码，请在**立即备份**对话框中，选中**立即备份**复选框。
- 3 输入**备份位置、用户名、密码和加密密码**的值。
加密密码可以包含字母数字字符和特殊字符，比如“!、@、#、\$、%、*”。不存在长度限制。
- 4 单击**备份**。

从备份还原 OMIVV 数据库

关于此任务

还原操作导致虚拟设备在还原完成后重新引导。

步骤

- 1 打开**备份和还原设置**页面。请参阅[管理备份和还原](#)。
- 2 在**备份和还原设置**页面中，单击**立即还原**。
- 3 在**立即还原**对话框中，输入**文件位置**的路径以及 .gz 备份文件（CIFS/NFS 格式）。
- 4 输入备份文件的**用户名、密码和加密密码**。
加密密码可以包含字母数字字符和特殊字符，比如“!、@、#、\$、%、*”。长度没有任何限制。
- 5 要保存您的更改，请单击**应用**。
该设备将重新引导。

① **注:** 如果设备重置为出厂设置，则确保您再次注册 OMIVV 设备。

关于 vSphere 客户端控制台

vSphere 客户端控制台在虚拟机的 vSphere 客户端中找到。控制台能够与管理控制台紧密关联。您可以使用控制台执行以下任务：

- 配置网络设置
- 更改虚拟设备密码
- 配置 NTP 并设置本地时区
- 重新引导虚拟设备
- 将虚拟设备重设为出厂设置
- 从控制台注销
- 使用只读用户角色

打开 OMIVV 虚拟机控制台

步骤

- 1 从 vSphere Web 客户端**主页**，单击**vCenter**。
- 2 在**资源清册列表**中，单击**虚拟机**，然后选择 OMIVV 虚拟设备。
- 3 请执行以下步骤之一：
 - 在**对象**选项卡上，选择**操作 → 打开控制台**。

- 右键单击您所选的虚拟设备，然后选择**打开控制台**。

后续步骤

打开虚拟机控制台并提供凭据（用户名：admin 和密码：部署设备时设置的密码）后，可以开始配置它。

配置网络设置

关于此任务

可以在 vSphere 客户端控制台中更改网络设置。

步骤

- 1 打开虚拟机控制台。请参阅[打开 vSphere 客户端控制台](#)。
- 2 在**控制台**窗口中，选择**配置网络**，然后按 **ENTER**。
- 3 在**编辑设备**或**编辑 DNS** 下输入所需的网络设置，然后单击**保存并退出**。要中止任何更改，请单击**退出**。

更改虚拟设备密码

关于此任务

可以在 vSphere Web 客户端中使用控制台更改虚拟设备密码。

步骤

- 1 打开虚拟机控制台。请参阅[打开 vSphere 客户端控制台](#)。
- 2 在**控制台**窗口中，使用箭头键选择**更改管理员密码**，然后按 **ENTER**。
- 3 在**当前管理员密码**中，输入值并按 **Enter**。
管理员密码应该至少为八个字符，并应包括一个特殊字符、一个数字、一个大写字母和一个小写字母。
- 4 针对**输入新的管理员密码**输入新密码，然后按 **ENTER**。
- 5 在**请确认管理员密码**中重新键入新密码，然后按 **Enter**。

配置 NTP 并设置本地时区

- 1 打开虚拟机控制台。请参阅[打开 vSphere 客户端控制台](#)。
- 2 要配置 OMIVV 时区信息，请单击**日期/时间属性**。
- 3 在**日期和时间**选项卡中，选择**通过网络同步日期和时间**。
此时会显示 **NTP 服务器**窗口。
- 4 要添加 NTP 服务器 IP 或主机名，请单击**添加**按钮，然后按下 **TAB** 键。
- 5 单击**时区**，选择适当的时区，然后单击**确定**。

重新引导虚拟设备

- 1 打开虚拟机控制台。请参阅[打开 vSphere 客户端控制台](#)。
- 2 单击**重新引导设备**。
- 3 要重新引导设备，请单击**是**，或单击**否**取消操作。

将虚拟设备重设为出厂设置

- 1 打开虚拟机控制台。请参阅[打开 vSphere 客户端控制台](#)。
- 2 单击**重设设置**。

随即显示以下消息：

All the settings in the appliance will be Reset to Factory Defaults and the appliance will be rebooted. Do you still wish to continue?

- 3 要重设设备，请单击是，或单击否取消操作。

如果单击“是”，OMIVV 设备会重设为原始出厂设置，所有其他设置和现有数据将会丢失。

① | 注：虚拟设备重设为出厂设置后，对网络配置进行的任何更新都将保留；这些设置不会重设。

从 vSphere 控制台中注销

要从 vSphere 控制台中注销，请单击**注销**。

只读用户角色

有一个具有外壳访问权限的只读用户角色，用于诊断目的。只读用户具有运行安装的有限权限。只读用户的密码设置为**只读**。在较早版本的 OMIVV 版本（OMIVV 版本 1.0 至 版本 2.3.1）中，只读用户角色的用户密码与管理密码相同，并且从 OMIVV 版本 3.0 向前更改以实现安全目的。

管理多个设备

您可以管理和监测多个用 vCenter 服务器注册的 OMIVV 设备。它们属于相同的平台服务控制器 (PSC) 和 vCenter 版本。

前提条件

如果页面缓存，建议您执行全局刷新。

步骤

- 1 在 VMware vCenter 主页中，单击 **OpenManage Integration** 图标。
- 2 在 **Dell EMC** 组下导航器中，单击 **OMIVV 设备**。
- 3 在 **OMIVV 设备** 选项卡上查看以下信息并监测设备：

注：在 Dell 设备选项卡上，列表中显示的设备优先级是预定的，并且高亮度显示的设备是处于活动状态的设备。

- **名称** — 显示使用各 OMIVV 设备 IP 地址或 FQDN 的链接。要查看和监测设备特定的信息，请单击特定设备名称链接。单击设备名称链接会将您带至 OMIVV 设备的主要内容窗格中。您可以管理 OMIVV 操作和监测特定设备的主机、数据中心和群集。

注：如果您使用多个设备，单击名称提示您在缓存页面上执行全局刷新后，将显示消息框。

要了解您管理 OMIVV 操作的设备，请执行以下操作：

- 1 在 OpenManage Integration for VMware vCenter 中，单击 **帮助和支持** 选项卡。
 - 2 在管理控制台，查看特定的 OMIVV 设备 IP。
- **版本** — 显示每个 OMIVV 设备的版本。
 - **合规性状态** — 指定设备是否兼容已加载的插件。
- 注：**当 OMIVV 设备与插件不兼容并且名称链接禁用时，设备的合规状态显示为不兼容。
- **可用性状态** — 显示指定您是否能从插件访问设备以及所需的 Web 服务是否正常运行 OMIVV 设备的状态。

注：当设备合规状态为不兼容并且设备可用性状态为是时，您可以选择一个设备。

- **已注册的 vCenter 服务器** — 显示所有您能访问的已登录会议的 vCenter，并使用设备进行注册。如果您使用多个 vCenter 注册设备，vCenter 显示为可展开和折叠的列表。单击 vCenter 链接会将您引导至所有 vCenter 均已列在导航器窗格中的 **vCenter 服务器** 页面。

从 Web 客户端访问 OpenManage Integration

安装 OMIVV 后，当您登录 VMware vCenter 并处于主页上的主页选项卡下时，**OpenManage Integration** 图标位于**管理组**下的主要内容区域中。您可以使用 **OpenManage Integration** 图标导航至 **OpenManage Integration for VMware vCenter** 页面。**Dell EMC** 组显示在**导航器**窗格中。

VMware vCenter 布局包括以下三个主要窗格：

表. 3: OpenManage Integration for VMware vCenter 窗格

窗格	说明
Navigator	访问控制台中的不同视图。OpenManage Integration for VMware vCenter 在 vCenter 菜单下有一个特别组，用作 OpenManage Integration for VMware vCenter 的主访问点。
主要内容	显示在导航器窗格中选择的视图。主要内容窗格是显示大多数内容的区域。
通知	显示 vCenter 警报、任务及正在进行的工作。OpenManage Integration for VMware vCenter 与警报、事件和任务系统集成在 vCenter 中，以在“通知”窗格中显示相关信息。

主题：

- 在 VMware vCenter Web 客户端中导航
- Web 客户端中的图标
- 查找软件版本
- 刷新屏幕内容
- 查看 Dell EMC 主机
- 查看 OpenManage Integration for VMware vCenter 许可选项卡
- 访问帮助和支持
- 查看日志历史记录

在 VMware vCenter Web 客户端中导航

OpenManage Integration for VMware vCenter 位于 VMware vCenter 中的特定 **Dell EMC** 组内。

- 1 登录 VMware vCenter。
- 2 在 VMware vCenter 主页中，单击 **OpenManage Integration** 图标。
在这里，可以：
 - 通过主要内容区域中的选项卡管理 OpenManage Integration for VMware vCenter 连接配置文件、产品设置，查看摘要页以及执行其他任务。
 - 从导航器窗格的 **vCenter 资源清册列表**下监测主机、数据中心和群集。选择想要调查的主机、数据中心或群集，然后在**对象**选项卡上，单击选择进行监测的对象。

Web 客户端中的图标

产品用户界面为您所执行的操作使用许多基于图标的操作按钮。

表. 4: 定义的图标按钮

图标按钮	定义
	添加或创建新内容
	将服务器添加到连接配置文件、数据中心和群集
	中止作业
	折叠列表
	展开列表
	删除对象
	更改计划
	编辑
	清除作业
	导出文件
	查看系统配置文件
	筛选

查找软件版本

在 OpenManage Integration for VMware vCenter 的**使用入门**选项卡上可以找到软件版本。

- 1 在 VMware vCenter 主页中，单击 **OpenManage Integration** 图标。
- 2 在 OpenManage Integration for VMware vCenter **使用入门**选项卡中，单击**版本信息**。
- 3 在**版本信息**对话框中，查看版本信息。
- 4 要关闭对话框，单击**确定**。

刷新屏幕内容

使用 VMware vCenter 的**刷新**图标可刷新屏幕。

- 1 选择您要刷新的页面。
- 2 在 VMware vCenter 标题栏中，单击**刷新 (Ctrl+Alt+R)** 按钮。
刷新图标位于“搜索”区域的右侧，看起来像是一个顺时针箭头。

查看 Dell EMC 主机

如您要仅快速查看 Dell EMC 主机，请在 OpenManage Integration for VMware vCenter 的导航器窗格中选择 **Dell EMC 主机**。

- 1 在 VMware vCenter 主页中，单击 **OpenManage Integration** 图标。
- 2 在导航器中的 **OpenManage Integration** 下，单击 **Dell EMC 主机**。
- 3 在 **Dell EMC 主机** 选项卡中，查看以下信息：
 - **主机名称** — 使用每台 Dell EMC 主机的 IP 地址显示链接。要查看 Dell EMC 主机信息，请单击特定主机链接。
 - **vCenter** — 显示此 Dell EMC 主机的 vCenter IP 地址。
 - **群集** — 如果 Dell EMC 主机在群集里，则显示群集名称。
 - **连接配置文件** — 显示连接配置文件的名称。

查看 OpenManage Integration for VMware vCenter 许可选项卡

安装 OpenManage Integration for VMware vCenter 许可证时，此选项卡将显示支持的主机和 vCenter 服务器的数量。您也可以在页面顶部查看 OpenManage Integration for VMware vCenter 的版本。

许可下面的页面显示 **购买许可证** 链接。

许可证管理部分显示：

- **产品许可门户（数字保险箱）**
- **iDRAC 许可门户**
- **管理控制台**

OpenManage Integration for VMware vCenter 的 **许可** 选项卡显示以下信息：

许可选项卡信息 说明

主机许可证

- 可用的许可证
显示可用的许可证数
- 使用中的许可证
显示使用中的许可证数

vCenter 许可证

- 可用的许可证
显示可用的许可证数
- 使用中的许可证
显示使用中的许可证数

访问帮助和支持

为了向您提供关于您产品的所需信息，OpenManage Integration for VMware vCenter 提供了 **帮助和支持** 选项卡。在此选项卡中，可以找到以下信息：

表. 5: 帮助和支持选项卡中的信息

名称	说明
产品帮助	<p>提供以下链接：</p> <ul style="list-style-type: none"> • OpenManage Integration for VMware vCenter 帮助 — 提供指向产品帮助的连接，该产品帮助位于产品内部。请使用目录或搜索功能查找所需的信息。 • 关于 — 此链接显示版本信息对话框。您可以在此处查看产品版本。
Dell EMC 手册	<p>提供指向以下内容的有效链接：</p> <ul style="list-style-type: none"> • 服务器手册 • OpenManage Integration for VMware vCenter 手册
管理控制台	提供指向管理控制台的链接。
附加帮助和支持	<p>提供指向以下内容的有效链接：</p> <ul style="list-style-type: none"> • 带 Lifecycle Controller 的 iDRAC 手册 • Dell VMware 说明文件 • OpenManage Integration for VMware vCenter 产品页面 • Dell 帮助和支持主页 • Dell TechCenter
支持呼叫提示	提供有关如何与 Dell 支持部门联系并正确路由呼叫信息的提示。
故障排除捆绑包	提供一个链接，用于创建和下载故障排除捆绑包。您可以在联系技术支持部门时提供或查看此捆绑包。有关更多信息，请参阅 下载故障排除捆绑包 。
Dell EMC 建议	提供指向 Dell Repository Manager (DRM) 的连接。请使用 DRM 查找和下载适用于您系统的所有固件更新。
iDRAC 重设	提供用于重设 iDRAC 的连接，可在 iDRAC 不响应时使用。此重设操作执行正常的 iDRAC 重新引导。

下载故障排除包

关于此任务

① 注: 要生成故障排除包，请确保您具有 OMIVV 写权限的用户登录到 vSphere Web 客户端。

可以使用故障排除捆绑包的信息来帮助您执行故障排除，或向技术支持部门发送信息。要获取故障排除信息，请执行以下步骤：

步骤

- 1 在 OpenManage Integration for VMware vCenter 中，单击**帮助和支持**选项卡。
- 2 在**故障排除捆绑包**下，单击**创建和下载故障排除捆绑包**。
- 3 单击**创建**按钮。
- 4 要保存文件，请单击**下载**。
- 5 在**文件下载**对话框中，单击**保存**。
- 6 在**另存为**对话框中，浏览到要保存文件的位置，然后单击**保存**。
- 7 要退出，请单击**关闭**。

重设 iDRAC

您可以在[帮助和支持](#)选项卡上找到 iDRAC 重设链接。重设 iDRAC 将执行正常的 iDRAC 重新引导操作。iDRAC 重新引导操作不会重新引导主机。您执行重设后，最多需花 2 分钟才能返回可用状态。如果 iDRAC 在 OpenManage Integration for VMware vCenter 中没有反应，请使用重设。

关于此任务

① 注: 建议您在重设 iDRAC 前将主机置于维护模式。您可以在作为连接配置文件一部分且已至少进行一次资源清册的主机上应用重设操作。该重设操作可能不会使 iDRAC 返回可用状况。在这种情况下，需要进行硬重设。要详细了解硬重设，请参阅 iDRAC 说明文件。

当 iDRAC 在重新引导时，可能会看到以下内容：

- OpenManage Integration for VMware vCenter 获取其运行状况时发生轻微通信错误延迟。
- 所有与 iDRAC 的当前会话关闭。
- iDRAC 的 DHCP 地址可能改变。

如果 iDRAC 使用 DHCP 作为其 IP 地址，则该 IP 地址可能改变。如果发生该情况，请重新运行主机资源清册作业，在资源清册数据中获取新的 iDRAC IP 地址。

步骤

- 1 在 OpenManage Integration for VMware vCenter 中，单击[帮助和支持](#)选项卡。
- 2 在“iDRAC 重设”下，单击**重设 iDRAC**。
- 3 在 **DRAC 重设**对话框中的“iDRAC 重设”下，键入主机 IP 地址/名称。
- 4 要确认您已了解 iDRAC 重设流程，请选择**我了解 iDRAC 重设。继续 iDRAC 重设**。
- 5 单击**重设 iDRAC**。

打开联机帮助

可以在[帮助和支持](#)选项卡上打开联机帮助。可以搜索说明文件以了解一个主题或一个步骤。

- 1 在 OpenManage Integration for VMware vCenter 中，在[帮助和支持](#)中的[产品帮助](#)下，单击 **OpenManage Integration for VMware vCenter 帮助**。
此时，联机帮助内容会显示在浏览器窗口中。
- 2 使用目录或搜索功能查找所选的主题。
- 3 要关闭联机帮助，请单击浏览器窗口右上角的 **X**。

启动管理控制台

可以在 VMware vCenter Web 客户端中启动 OpenManage Integration for VMware vCenter，并在[帮助和支持](#)选项卡上打开管理控制台。

- 1 在 OpenManage Integration for VMware vCenter 中[帮助和支持](#)选项卡的**管理控制台**下，单击指向控制台的链接。
- 2 在**管理控制台**登录对话框中，使用管理员密码登录。
可以在管理控制台中执行以下操作：
 - 注册或注销 vCenter、修改凭据或更新证书。
 - 上载许可证。
 - 查看已注册和可用 vCenter 数的摘要，以及关于已使用和可用的最大主机许可证数的摘要。
 - 重新启动虚拟设备。

- 更新或升级至最新版本。
- 显示网络设置（只读模式）。
- 配置 HTTP 代理设置，用于连接到 Dell EMC 服务器以进行设备升级或连接至 <http://downloads.dell.com/published/Pages/index.html>。
- 配置 NTP 设置，该设置允许您启用或禁用 NTP 服务器，以及配置首要和次要 NTP 服务器。
- 生成证书签名请求 (CSR)、上传证书或还原 HTTPS 证书的默认证书。
- 配置所有 vCenter 实例的警报存储方式的全局设置。您可以配置要存储警报的最大数量、警报的保留天数和重复警报的超时时间。
- 配置所有 vCenter 实例的警报存储方式的全局设置。
- 启动备份或还原。
- 配置网络共享的备份位置 and 该备份文件的加密密码（同时测试网络连接）。
- 计划定期备份。

查看日志历史记录

日志页面使让能够查看 OMI/V 生成的日志。

您可以使用两个下拉列表对此页面上的内容进行筛选和排序。第一个下拉列表允许您基于以下日志类型筛选和查看日志详细信息：

- 所有类别
- 信息
- 警告
- 错误

第二个下拉列表可帮助您根据以下日期和时间频率排序日志详细信息：

- Last Week（上周）
- Last Month（上个月）
- Last Year（去年）
- 自定义范围
 - 如果选择**自定义范围**，您可以根据自己希望的筛选内容指定开始和结束日期，然后单击**应用**。

该网格表显示以下信息：

- 类别 — 显示日志类别的类型
- 日期和时间 — 显示用户操作的日期和时间
- 说明 — 显示用户操作的说明

您可以单击列标题，使数据网格列按升序或降序排列。使用**筛选器**文本框，在内容中进行搜索。在页面网格底部，显示以下信息：

表. 6: 日志历史记录


日志信息	说明
总项目数	显示所有日志项目的总数。
每个屏幕上的项目数	显示所显示页面上的日志项目数。使用下拉框设置每个页面的项目数。
页面	当您在查看日志信息时显示所在的页面。在文本框中键入页码或使用 上一页 和 下一页 按钮，导航到所需的页面。
“上一页”或“下一页”按钮	指导您前往下一页或上一页。
“全部导出”图标	将日志内容导出到 CSV 文件。

查看日志

- 1 在 OpenManage Integration for VMware vCenter 中，单击**监测**选项卡。
- 2 在**日志**选项卡上，查看 OpenManage Integration for VMware vCenter 的用户操作日志。有关显示的日志信息，请参阅[日志历史记录](#)。
- 3 要为网格中的数据排序，请单击列标题。
- 4 要使用类别或时间块排序，请使用网格前面的下拉式列表。
- 5 要在日志项目页面之间翻页，请使用**上一页**和**下一页**按钮。

导出日志文件

OpenManage Integration for VMware vCenter 使用逗号分隔值 (CSV) 文件格式从数据表导出信息。

- 1 在 OpenManage Integration for VMware vCenter 中，单击**监测**选项卡。
- 2 要将日志内容导出到 CSV 文件，请在屏幕的右下角单击  图标。
- 3 在**选择下载位置**对话框中，浏览到保存日志信息的位置。
- 4 在**文件名**文本框中，接受默认名称 `ExportList.csv` 或键入自己的文件名，扩展名为 `.CSV`。
- 5 单击**保存**。

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 — OMIVV 版本 4.x 设备首次通电时，评估许可证会自动安装。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）。此许可证仅适用于 Dell EMC 第 11 代和更高版本的服务器，它是默认许可证，具有 90 天试用期。
- 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 商店下载许可证文件。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。

许可中将显示以下信息：

- 最大 vCenter 连接许可证数 — 可允许最多 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 商店 <http://www.dell.com/support/licensing> 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 www.dell.com/support/softwarecontacts 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。

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**进行上载。

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，请执行以下操作之一：
 - 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 商店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。

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](#)

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，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](#)。
- 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[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。
如果您尚未配置 vCenter，或者如果已向环境中添加了一个 vCenter，请选择一个 vCenter。“vCenter 选择”页面允许您选择一个或多个 vCenter 以配置设置。
- 3 要继续处理**连接配置文件说明**对话框，请单击**下一步**。

① **注：**如果您具有多台属于同一单一登录 (SSO) 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。

① **注：**Active Directory 凭据可以是相同或独立的 iDRAC 和主机。

① **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。

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）：

① **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**。用户名不得超过 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。用户名不得超过 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**。用户名不得超过 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
- 没有无效字符，比如 "/ \ [] ; | = , + * ? < > @

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。
- 没有无效字符，比如 "/ \ [] ; | = , + * ? < > @

- 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，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**。
 - 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**。

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，仍建议您测试连接配置文件。

① **注:** 对运行已禁用 WBEM 服务的 ESXi 6.5 和/或更高版本的所有主机进行的测试连接失败。对于这种主机，当您在那些主机上执行资源清册时，将自动启用 WBEM 服务。尽管测试连接失败，建议您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。

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 详细信息修改或创建新的连接配置文件。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。

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 ESXi 6.5 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 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，来配置资源清册计划。

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 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 OMIVV 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 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，OMIVV 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，OMIVV 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。
- 5 单击**应用**。

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 [启用 OMSA 链接](#)。
- 配置保修到期通知设置。请参阅 [配置保修到期通知设置](#)。
- 设置固件更新存储库。请参阅 [设置固件更新存储库](#)。
- 配置最新设备版本通知。请参阅 [配置最新设备版本通知](#)。
- 配置和查看事件和警报。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 [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。

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** — 您可以访问使用 Dell 固件更新存储库 (Ftp.dell.com) 的位置。OpenManage Integration for VMware vCenter 将从 Dell 存储库下载所选的固件更新并更新受管主机。
 -  **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。
- 3 如果选择**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

① **注:** 如果您配置使用 CIFS 共享, 而不是基于 CIFS 共享的服务器消息块 (SMB) 版本 1.0, 可能会导致潜在的服务中断, 因为 OMIVV 无法与诸如 CIFS 共享等通信。因此, 建议您使用基于仅基于 CIFS 共享的 SMB 版本 1.0。

① **注:** 如果您使用的是 CIFS 共享, OMIVV 会提示您输入用户名和密码。共享网络文件夹的用户名或密码不支持使用 @、% 和字符。

4 下载完成后单击**应用**。


① **注:** 从源读取目录并更新 OMIVV 数据库可能需要长达 60 至 90 分钟。

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


前提条件

启用 OMSA 链接之前，安装并配置 OMSA Web 服务器。请参阅 *OpenManage Server Administrator 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 代服务器或更早版本的服务器需要 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 。
- 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 **Dell EMC 主机信息** 部分中是否有效。

配置事件和警报

关于此任务

Dell EMC 管理中心事件和警报对话框可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**。

① | 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[事件、警报和运行状况监测](#)。


- 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**。

① | 注: 选中该选项后将覆盖所有 vCenter 的现有设置。


① | 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, 请参阅[修改资源清册作业计划](#)或[修改保修作业计划](#)。
- 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。

配置 SNMP 陷阱团体字符串

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

① | 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。

配置文件

使用**凭据配置文件**允许您管理和配置连接配置文件和机箱配置文件，而**部署模板**允许您管理和配置硬件和虚拟机监控程序配置文件。

关于连接配置文件

连接配置文件选项卡让您可以管理和配置连接包含被与 Dell EMC 服务器通信的虚拟设备所使用的凭据的配置文件。每个 Dell 服务器仅与一个连接配置文件关联，以用于 OpenManage Integration for VMware vCenter 进行管理。您可以将多个服务器分配到单个连接配置文件。运行**初始配置向导**后，您可以从 OpenManage Integration for VMware vCenter 管理连接配置文件，请执行以下任务：

- [查看连接配置文件](#)
- [创建连接配置文件](#)
- [修改连接配置文件](#)
- [删除连接配置文件](#)
- [测试连接配置文件](#)

查看连接配置文件

必须先创建连接配置文件和/或已有连接配置文件，才能进行查看。创建一个或多个连接配置文件后，可以在**连接配置文件**页面上查看这些文件。OpenManage Integration for VMware vCenter 使用配置文件中提供的凭据与 Dell 主机进行通信。

- 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**连接配置文件**选项卡。
可以查看您已创建的所有连接配置文件。

表. 7: 连接配置文件信息

连接配置文件字段	说明
配置文件名称	显示连接配置文件的名称
说明	显示说明（如果提供）
vCenter	根据上下文，显示 vCenter 的 FQDN 或主机名，或者 IP 地址
关联的主机	显示与连接配置文件关联的主机。如果多于一个，请使用展开图标显示全部。
iDRAC 证书检查	显示是启用还是禁用了“iDRAC 证书检查”
主机根证书检查	显示是启用还是禁用了“主机根证书检查”
创建日期	显示连接配置文件的创建日期
修改日期	显示连接配置文件的修改日期
上次修改者	显示修改连接配置文件的用户的详细信息


创建连接配置文件

关于此任务

您可以将多个主机关联至单一的连接配置文件。要创建连接配置文件，请执行以下步骤：

① 注：在此过程中列出的 vCenter 主机已使用相同的单点登录 (SSO) 对其进行了验证。如果未看到 vCenter 主机，则可能其位于不同的 SSO 上，或所用的 VMware vCenter 版本可能低于版本 5.5。

步骤

- 1 在 OpenManage Integration for VMware vCenter 中的 **管理** → **配置文件** → **凭据配置文件** → **连接配置文件** 选项卡上，单击  图标。
- 2 在 **欢迎** 页面中，单击 **下一步**。
- 3 在 **连接配置文件** 页面中，输入以下详细信息：
 - a 在 **配置文件** 下，键入 **配置文件名称** 和可选的 **说明**。
 - b 在 **vCenter** 中，从下拉式列表中选择要在其上创建配置文件的 vCenter 服务器。
此选项允许您为每个 vCenter 创建一个连接配置文件。
 - c 在 **iDRAC 凭据** 区域中，执行以下任务之一：

① 注： iDRAC 帐户需要用于更新固件、应用硬件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（将在其上使用 Active Directory），请选择 **使用 Active Directory**；否则，请跳到下一个选项。
 - 在 **Active Directory 用户名** 文本框中，键入用户名。以下列格式之一键入用户名，比如 **域\用户名** 或 **域@用户名**。用户名不得超过 256 个字符。有关用户名的限制信息，请参阅 Microsoft Active Directory 说明文件。
 - 在 **Active Directory 密码** 文本框中，键入密码。密码不得超过 127 个字符。
 - 在 **验证密码** 文本框中，再次键入密码。
 - 要验证 iDRAC 证书，请选择以下操作之一：
 - 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**。
 - 要不执行检查也不存储证书，请清除 **启用证书检查**。
- 要在不设置 Active Directory 的情况下配置 iDRAC 凭据，请执行以下操作：
 - 在 **用户名** 文本框中，键入用户名。用户名不得超过 16 个字符。有关您的 iDRAC 版本的用户名限制信息，请参阅 iDRAC 说明文件。

① 注：本地 iDRAC 帐户需要管理权限来更新固件、应用硬件配置文件和部署虚拟机监控程序。


- 在 **密码** 文本框中，键入密码。密码不得超过 20 个字符。
 - 在 **验证密码** 文本框中，再次键入密码。
 - 要验证 iDRAC 证书，请选择以下操作之一：
 - 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**。
 - 要不执行任何检查也不保存证书，请勿选择 **启用证书检查**。
- d 在 **主机根** 区域中，执行以下操作之一：
 - 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** 复选框；否则，请跳到配置主机凭据步骤。
 - 在 **Active Directory 用户名** 文本框中，键入用户名。以下列格式之一键入用户名，比如 **域\用户名** 或 **域@用户名**。用户名不得超过 256 个字符。有关用户名的限制信息，请参阅 Microsoft Active Directory 说明文件。
 - 在 **Active Directory 密码** 文本框中，键入密码。密码不得超过 127 个字符。
 - 在 **验证密码** 文本框中，再次键入密码。
 - 对于证书检查，请选择以下其中一项：

- 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**。
- 要不执行任何检查也不保存证书，请勿选中**启用证书检查**。
- 要在不设置 Active Directory 的情况下配置主机凭据，请执行以下操作：
 - 在**用户名**文本框中，用户名是根。
根用户名是默认用户名，无法更改。

① | 注: 如果已设置 Active Directory，则可以选择任何 Active Directory 用户名，而不是根。

- 在**密码**文本框中，键入密码。密码不得超过 127 个字符。
- 在**验证密码**文本框中，再次键入密码。
- 对于证书检查，请选择以下其中一项：
 - 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**。
 - 要不执行任何检查也不保存证书，请勿选中**启用证书检查**。

① | 注: OMSA 凭据与 ESXi 主机使用的凭据相同。

- 4 单击 **Next**（下一步）。
- 5 在**选择主机**对话框中，选择此连接配置文件的主机并单击 **OK**。
- 6 在**关联的主机**页面中，必要时为连接配置文件选择一个或多个主机。
要添加主机，请单击 **+** 图标，选择主机，然后单击 **确定**。
- 7 要测试连接配置文件，请选择一个或多个主机，然后单击  图标。

① | 注: 此步骤是可选步骤，用于验证主机和 iDRAC 凭据是否正确。尽管此步骤为可选，仍建议您测试连接配置文件。

① | 注: 对运行已禁用 WBEM 服务的 ESXi 6.5 和/或更高版本的所有主机进行的测试连接失败。对于这种主机，当您在那些主机上执行资源清册时，将自动启用 WBEM 服务。尽管测试连接失败，建议您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。

- 8 要完成配置文件创建，请单击**下一步**。
对于既没有 iDRAC Express 也没有 Enterprise 卡的服务器，iDRAC 测试连接的结果会表明**不适用于该系统**。

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 ESXi 6.5 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[运行修补不符合要求的 vSphere 主机向导](#)。


修改连接配置文件

创建连接配置文件后，您可以编辑配置文件名称、说明、关联的主机以及 iDRAC 和主机凭据。

关于此任务


- ① | 注:** 在此过程中列出的 vCenter 已使用相同的单点登录 (SSO) 对其进行了验证。如果未看到 vCenter 主机，则可能其位于不同的 SSO 上，或所用的 VMware vCenter 版本可能早于版本 5.5。
- ① | 注:** 确保资源清册、保修或部署作业正在运行时不会更新连接配置文件。
- ① | 注:** 确保资源清册、保修或部署作业正在运行时不会将与一个连接配置文件关联的主机移至另一连接配置文件或从连接配置文件中移除主机。

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**连接配置文件**。
- 4 选择配置文件并单击  图标。

- 5 在**连接配置文件**窗口的**欢迎**选项卡中，读取信息并单击**下一步**。
 - 6 在**名称和凭据**选项卡中，执行以下步骤：
 - a 在**配置文件**下，键入**配置文件名称**和可选的**说明**。
 - b 在**vCenter**下，查看与此连接配置文件相关联的主机。请参阅上文中有关为何您会看到此处显示的主机的说明。
 - c 在**iDRAC 凭据**下，执行以下步骤之一：
 - 对于已针对 Active Directory 配置和启用的 iDRAC 帐户（将在其上使用 Active Directory），请选择**使用 Active Directory**。
 - 在**Active Directory 用户名**文本框中，键入用户名。按照下列格式之一键入用户名：**域\用户名**、**域/用户名**或**用户名@域**。用户名不得超过 256 个字符。有关用户名的限制信息，请参阅 Microsoft Active Directory 说明文件。
 - 在**Active Directory 密码**文本框中，键入密码。密码不得超过 127 个字符。
 - 在**验证密码**文本框中，再次键入密码。
 - 对于证书检查，请选择以下其中一项：
 - 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**。
 - 要不执行检查也不存储证书，请勿选中**启用证书检查**。
 - 要在无需 Active Directory 的情况下配置 iDRAC 凭据，请输入以下项：
 - **用户名** — 以下列格式之一键入用户名，比如**域\用户名**或**域@用户名**。
用户名中可以使用的字符如下：/（正斜杠）、&（和号）、\（反斜杠）、.（句点）、"（引号）、@、%（百分号）（最多 127 个字符）。

域可以包含字母数字字符，比如 -（破折号）及 .（句点）（最多 254 个字符）。域的**第一个和最后一个字符必须是字母数字**。
 - **密码** — 键入密码。
密码中不允许使用的字符如下 /（正斜杠）、&（和号）、\（反斜杠）、.（句点）、"（引号）。
 - **验证密码** — 重新键入您的密码。
 - **启用证书检查** — 默认情况下，该复选框处于非选中状态。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**。如不执行证书检查也不保存证书，请勿选中**启用证书检查**复选框。
 - d 在**主机根**下，执行以下任务：
 - 要访问与 Active Directory 关联的所有控制台，请选中**使用 Active Directory**复选框。
 - **用户名** — 默认用户名为根且无法修改。如果选择了**使用 Active Directory**，则可以使用任何 Active Directory 用户名。
 - ① **注：**用户名为 **root**，如果不选择 **Active Directory**，则无法修改此输入。iDRAC 用户不必使用根凭据，如果设置了 **Active Directory**，则可以使用任何管理员权限。
 - **密码** — 键入密码。
密码中不允许使用以下字符：/（正斜杠）、&（和号）、\（句点）、"（引号）。
 - **验证密码** — 重新键入您的密码。
 - **启用证书检查** — 默认情况下，该复选框处于非选中状态。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**。若要不执行证书检查且不存储该证书，请勿选中**启用证书检查**复选框。
 - ① **注：**如果使用 **Active Directory**，请选择**启用证书检查**。
 - ① **注：**OMSA 凭据与 ESXi 主机使用的凭据相同。
 - ① **注：**对于既没有 iDRAC Express 也没有 Enterprise 卡的主机，iDRAC 测试连接的结果表示不适用于此系统。
- 7 单击**下一步**。
 - 8 在**选择主机**对话框中，选择此连接配置文件的主机。
 - 9 单击**确定**。
使用**关联的主机**对话框，可以在所选的服务器上测试 iDRAC 和主机凭据。
 - 10 请执行以下步骤之一：

- 要在不测试凭据的情况下创建连接配置文件，请单击**完成**。
- 要开始测试，请选择要检查的主机，然后单击图标。其他选项处于非活动状态。

注：对运行已禁用 WBEM 服务的 ESXi 6.5 和/或更高版本的所有主机进行的测试连接失败。对于这种主机，当您在那些主机上执行资源清册时，将自动启用 WBEM 服务。尽管测试连接失败，建议您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。

测试完成后，请单击**完成**。

- 要停止测试，请单击**中止所有测试**。在**中止测试**对话框中，单击**确定**，然后单击**完成**。


注：修改日期和上次修改者字段中包括您通过 Web 客户端界面为连接配置文件执行的更改。OMIVV 设备在各自的连接配置文件上执行的任何更改并不影响这两个字段的详细信息。

删除连接配置文件

关于此任务


注：确保资源清册、保修或部署作业正在运行时不会删除与主机关联的连接配置文件。

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**，单击**连接配置文件**选项卡，然后选择要删除的配置文件。
- 4 单击图标。
- 5 要移除配置文件，请对删除确认消息单击**是**，或者单击**否**取消删除操作。

注：OMIVV 不会管理是您删除的连接配置文件一部分的主机，直至这些主机添加到另一个连接配置文件。

测试连接配置文件

- 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**，单击**连接配置文件**选项卡，然后选择一个连接配置文件。
- 4 在**测试连接配置文件**对话框中，选择您要测试的主机，然后单击图标。
如果不选择连接配置文件，则运行测试连接会需要一些时间。
- 5 要中止所有选择的测试并取消测试，请单击**中止所有测试**。在**中止测试**对话框中，单击**确定**。
- 6 要退出，请单击**取消**。

关于机箱配置文件

OMIVV 可以监测所有与 Dell EMC 服务器相关联的 Dell EMC 机箱。需要机箱配置文件来监测机箱。您可以通过执行以下任务来管理机箱配置文件：

- 查看机箱配置文件。请参阅[查看机箱配置文件](#)。
- 创建机箱配置文件。请参阅[创建机箱配置文件](#)。
- 编辑机箱配置文件。请参阅[编辑机箱配置文件](#)。
- 删除机箱配置文件。请参阅[删除机箱配置文件](#)。
- 测试机箱配置文件。请参阅[测试机箱配置文件](#)。

查看机箱配置文件

前提条件

确保您创建机箱配置文件或在查看之前退出机箱配置文件。

关于此任务

创建一个或多个机箱配置文件后，您可以在机箱配置文件页面中进行查看。

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。
此时，会显示机箱配置文件。
- 4 要显示所有相关的机箱，请单击  图标，如果有多个机箱与机箱配置文件相关联。
- 5 在**机箱配置文件**页面中，查看机箱信息。

表. 8: 机箱配置文件信息

机箱字段	说明
配置文件名称	显示机箱配置文件的名称
说明	显示说明（如果提供）
机箱 IP/主机名	显示机箱的 IP 地址或主机名
机箱服务标签	显示分配给机箱的唯一标识符
修改日期	显示机箱配置文件的修改日期


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

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。

① **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**下一步**。

将显示**选择机箱**页面，其中显示所有可用的机箱。

① **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，这些机箱才可供查找，并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 要测试机箱的连接性，请选择机箱并单击图标，此操作会验证凭据，结果将在**测试结果**列中显示为**通过**或**失败**。

10 要完成配置文件，请单击**完成**。


编辑机箱配置文件

创建机箱配置文件后，可以编辑配置文件名称、说明、关联的机箱以及凭据。

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**，单击**机箱配置文件**选项卡，然后选择一个机箱配置文件。

4 单击主菜单上的图标。

此时将显示**编辑机箱配置文件**窗口。


5 在**机箱配置文件**中，您可以编辑**配置文件名称**和可选的**说明**。

6 在**凭据**区域下，可以编辑**用户名**、**密码**和**验证密码**。

您在**验证密码**中键入的密码必须与在**密码**字段中输入的密码相同。输入的凭据必须对机箱具有管理员权限。

7 要保存更改，请单击**应用**。

使用**关联的机箱**选项卡，让您测试机箱和所选机箱上的凭据。请执行以下步骤之一：

- 要开始测试，选择要检查的一个或多个机箱，然后单击图标。**测试结果**列显示检测连接是否成功。
- 您可以对某个机箱配置文件添加或删除一个或多个机箱。


① **注:** 如果未对机箱进行过资源清册，则仅会显示 IP/主机名称和服务标签。机箱名称和型号字段将在对机箱进行了资源清册后显示。

删除机箱配置文件

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 选择要删除的机箱配置文件，然后单击图标。


随即将显示一条警告消息。

5 要继续删除，请单击**是**，或单击**否**取消删除。

如果与某个机箱配置文件关联的所有机箱均被清除或移至不同的配置文件，则会显示删除确认消息，指出该机箱配置文件不存在任何关联机箱，且将被删除。要删除该机箱配置文件，请对删除确认消息单击**确定**。

① **注:** OMIVV 不会监测与您已删除的机箱配置文件关联的主机，直至这些机箱添加到另一个机箱配置文件。

测试机箱配置文件

- 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**并单击**机箱配置文件**选项卡，然后选择一个或多个机箱配置文件进行测试。完成此操作可能需要几分钟。
- 4 在**测试机箱配置文件**对话框中，选择要测试的机箱，然后单击图标。
- 5 要中止所有选择的测试并取消测试，请单击**中止所有测试**。在**中止测试**对话框中，单击**确定**。
- 6 要退出，请单击**取消**。

资源清册和保修管理

配置 OMIVV 后，可以在**监测**选项卡下监测资源清册、保修作业，管理部署作业以及管理固件更新作业。资源清册和保修是在**初始配置向导**中或从**设置**选项卡进行设置。

作业队列页面管理以下作业：

- 显示提交的服务器部署或固件更新作业。
- 刷新固件更新或部署作业，或是资源清册/保修历史队列。
- 计划资源清册或保修作业。
- 清除固件更新或部署作业队列条目。

① 注：要确保资源清册/保修包含最新的信息，计划资源清册/保修作业至少每周运行一次。

可以在此页面中执行的任务包括：

- [管理部署作业](#)
- [管理固件更新作业](#)
- [管理资源清册作业](#)
- [管理保修作业](#)

① 注：对于所有提及的作业，确保在设备时间更改为未来日期的情况下再次计划并恢复。

① 注：对于基本运行状况监测，确保重新引导 OMIVV 设备。对于扩展运行状况监测，确保禁用扩展监测，然后从 OMIVV 管理控制台将其启用。

主题：

- [资源清册作业](#)
- [保修作业](#)
- [监测单个主机](#)
- [监测群集和数据中心中的主机](#)
- [设置物理服务器闪烁指示灯](#)
- [配置系统锁定模式](#)

资源清册作业

资源清册作业通过**设置**选项卡或**初始配置向导**进行设置。请使用**资源清册历史**选项卡查看所有资源清册作业。从此选项卡可以执行的任务包括：

- [查看主机或机箱资源清册](#)
- [修改资源清册作业计划](#)
- [立即运行机箱资源清册作业](#)

查看主机资源清册

要收集数据，必须有成功完成的资源清册。资源清册完成后，便可以查看整个数据中心或单个主机系统的资源清册结果。您可以按升序或降序对资源清册视图的列进行排序。

关于此任务

注: 下面是无法检索和显示主机数据时几种可能的原因：

- 主机未与连接配置文件关联，因此您无法运行资源清册作业。
- 尚未在主机上运行用于收集数据的资源清册作业，因此没有可以显示的内容。
- 主机许可证数已超出，必须要有额外的可用许可证才能完成资源清册任务。
- 主机没有第 12 代及更高代 PowerEdge 服务器所需的正确 iDRAC 许可证，因此，请购买正确的 iDRAC 许可证。
- 凭据可能有误。
- 主机可能无法访问。

要查看主机资源清册详细信息，请执行以下操作：

步骤

- 1 在 OpenManage Integration for VMware vCenter 中，单击**监测**选项卡。
- 2 单击**作业队列**、展开**资源清册历史**，然后单击**主机资源清册**。
vCenter 信息将显示在上部的网格中。
- 3 要查看所选 vCenter 的主机信息，选择 vCenter 将显示所有关联的主机详细信息。
- 4 查看主机资源清册信息。

表. 9: vCenter, 主机信息

vCenter	
vCenter	显示 vCenter 地址
通过的主机	显示已通过的所有主机
上次资源清册	显示上次资源清册计划的运行日期和时间
下次资源清册	显示下次资源清册计划的运行日期和时间
主机	
主机	显示主机地址。
状态	显示状态。选项包括： <ul style="list-style-type: none">• 成功• 失败• 正在进行• 已计划
持续时间 (MM: SS)	显示作业的持续时间，以分钟和秒为单位
开始日期和时间	显示资源清册计划的开始日期和时间
结束日期和时间	显示资源清册计划的结束时间

查看机箱资源清册

要收集数据，必须有成功完成的资源清册。您可以按升序或降序对资源清册视图的列进行排序。

- 1 在 OpenManage Integration for VMware vCenter 中，单击**监测**选项卡。
- 2 单击**作业队列**、**资源清册历史记录**，然后单击**机箱资源清册**。
- 3 查看机箱资源清册信息。

表. 10: 机箱信息

机箱资源清册	
机箱 IP	显示机箱 IP 地址
服务标签	显示机箱的服务标签。服务标签是由制造商提供的唯一标识符，用于支持和维护
状态	显示机箱的状态
持续时间 (MM: SS)	显示作业的持续时间，以分钟和秒为单位
开始日期和时间	显示资源清册计划的开始日期和时间
结束日期和时间	显示资源清册计划的结束时间

修改资源清册作业计划

要确保有最新的主机信息，请计划至少每周运行一次资源清册作业。资源清册作业消耗最少的资源，且不会降低主机性能。您可以从**初始配置向导**或**监测**选项卡上更改资源清册作业计划。



关于此任务

资源清册作业计划设置运行资源清册作业的时间或日期，例如：

- 每周的选定日子和特定时间
- 按照设置的时间间隔

要在主机系统上执行资源清册，请创建提供通信和验证信息的连接配置文件。

步骤

- 1 在 OpenManage Integration for VMware vCenter 中，单击**监测**选项卡。
- 2 单击**作业队列**、**资源清册历史**，然后单击**主机资源清册**。
- 3 选择一个 vCenter，然后单击  图标。
- 4 在**资源清册数据检索**对话框中，执行以下操作：
 - a 在**资源清册数据**中，选择**启用资源清册数据检索**复选框。
 - b 在**资源清册数据检索计划**下，为您的作业选择日期。
 - c 在**资源清册数据检索时间**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。
- 5 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**。
- 6 要立即运行作业，请在 OpenManage Integration for VMware vCenter 中的**监测** > **作业队列**选项卡上，单击**资源清册历史** > **主机资源清册**。
- 7 单击 ，在**成功**对话框中，单击**关闭**。

① **注:** 当您运行模块化主机资源清册时, 会自动查找相应的机箱。如果机箱已经是机箱配置文件的一部分, 那么机箱资源清册将在主机资源清册后自动运行。

计划好资源清册作业后, 该资源清册作业现在已在队列中。您不能为单个主机运行资源清册。资源清册作业会对所有主机启动。

运行资源清册作业

- 1 一旦**配置向导**完成, 将针对添加到连接配置文件的所有主机自动触发资源清册作业。要后续按需运行资源清册作业, 请单击**作业队列 > 资源清册 > 立即运行**以运行资源清册作业。
- 2 要查看资源清册作业的状态, 可单击**刷新**。
- 3 导航至**主机和群集**视图, 单击任何 **Dell EMC 主机**, 然后单击 **OpenManage Integration** 选项卡。将提供以下信息:

- 概览页面
- 系统事件日志
- 硬件资源清册
- 存储
- 固件
- 电源监测

① **注:** 对于超出许可限值的主机, 将跳过资源清册作业, 并将其标记为失败。

可在 OpenManage Integration 选项卡内使用以下主机命令:


- 闪烁指示灯
- 运行固件更新向导
- 启动远程访问
- 启动 OMSA
- 启动 CMC
- 配置系统锁定模式

立即运行机箱资源清册作业

您可以在**机箱资源清册**选项卡查看并运行机箱资源清册作业。

- 1 在 OpenManage Integration for VMware vCenter 中, 单击**监测**选项卡。
- 2 单击**作业队列**、**资源清册历史**, 然后单击**机箱资源清册**。此时会显示机箱列表及其上次资源清册作业的状态。

① **注:** 计划的机箱资源清册与计划的主机资源清册同时运行。

- 3 单击 。此时会显示更新的已清册机箱列表, 每个机箱的状态为**成功**或**失败**。

保修作业

从“Dell 联机”检索硬件保修信息, 并通过 OMIVV 显示该信息。服务器的服务标签用于收集关于服务器的保修信息。保修数据检索作业是通过**初始配置向导**进行设置。

可以在此选项卡中执行的任务包括:

- [查看保修历史](#)
- [修改保修作业计划](#)
- [立即运行主机保修作业](#)

- [立即运行机箱保修作业](#)

查看保修历史

保修作业是一项计划任务，以通过 Support.dell.com 上获得所有系统的保修信息。您可以按升序或降序对资源清册视图的列进行排序。

关于此任务

① 注: OMIVV 设备需要互联网连接来以提取保修信息。请确保 OMIVV 设备连接到互联网。根据网络设置，OMIVV 可能需要代理信息以获得互联网可达性和保修信息。代理详细信息可在管理控制台中更新。请参阅 [设置 HTTP 代理](#)。

步骤

- 1 在 OpenManage Integration for VMware vCenter 中，单击**监测**选项卡。
- 2 单击**作业队列**，然后单击**保修历史**。
- 3 展开**保修历史**以显示**主机保修**和**机箱保修**。
- 4 要查看您相应的保修作业历史记录信息，请选择**主机保修**，然后选择 vCenter 将显示所有关联的主机详细信息。

表. 11: vCenter, 主机历史记录信息

vCenter 历史	
vCenter	显示 vCenter 的列表
通过的主机	显示通过的 vCenter 主机数
上次保修	显示上次保修作业运行的日期和时间
下次保修	显示下次保修作业的运行日期和时间
主机历史	
主机	显示主机地址
状态	显示状态。选项包括： <ul style="list-style-type: none"> • 成功 • 失败 • 正在进行 • 已计划
持续时间（分钟:秒）	显示保修作业的持续时间，格式为 MM:SS
开始日期和时间	显示保修作业的开始日期和时间
结束日期和时间	显示保修作业的结束时间

查看机箱保修

保修作业是在所有系统上从 support.dell.com 获取保修信息的计划任务。可以采用升序或降序对资源清册视图的列进行排序。


- 1 在 OpenManage Integration for VMware vCenter 中，单击**监测**选项卡。
- 2 单击**作业队列**，然后单击**保修历史**。
- 3 展开**保修历史**以显示**主机保修**和**机箱保修**。
- 4 单击**机箱保修**。
- 5 查看机箱保修详细信息。

表. 12: 机箱信息

机箱历史	
机箱 IP	显示机箱 IP 地址
服务标签	显示机箱的服务标签。服务标签是由制造商提供的用于支持和维护的唯一标识符
状态	显示机箱的状态
持续时间 (MM: SS)	显示保修作业的持续时间，格式为 MM:SS
开始日期和时间	显示保修作业的开始日期和时间
结束日期和时间	显示保修作业的结束时间


修改保修作业计划

保修作业最初在**初始配置向导**中配置。之后您可从**设置**选项卡修改保修作业计划。

- 1 在 OpenManage Integration for VMware vCenter 中，单击**监测**选项卡。
- 2 单击**作业队列**，然后单击**保修历史**。
- 3 展开**保修历史**以显示**主机保修**和**机箱保修**。
- 4 要查看您的相应保修作业历史信息，请选择**主机保修**或**机箱保修**。
- 5 单击  图标。
- 6 在**保修数据检索**对话框中，执行以下操作：
 - a 在**保修数据**下，选中**启用保修数据检索**复选框。
 - b 在**保修数据检索计划**下，为保修作业选择一周当中的具体天数。
 - c 在**保修数据检索时间**文本框中，为此作业键入本地时间。
您可能需要计算在正确时间运行此作业所需的时差。
- 7 单击**应用**。

立即运行主机保修作业


至少每周运行一次保修作业。

- 1 在 OpenManage Integration for VMware vCenter 中，单击**监测**选项卡。
- 2 单击**作业队列**，然后单击**保修历史**。
- 3 展开**保修历史**以显示**主机保修**和**机箱保修**。
- 4 要查看您的相应保修作业历史信息，请选择**主机保修**或**机箱保修**。
- 5 选择要运行的保修作业，然后单击立即  图标。
- 6 在**成功**对话框中，单击**关闭**。
保修作业此时会出现在队列中。

注: 当运行主机保修时，会自动为所有机箱运行机箱保修。在具有多个 vCenter 的 SSO 环境中，当手动运行任意 vCenter 的保修时，会自动对所有 vCenter 运行机箱保修。

立即运行机箱保修作业

至少每周运行一次保修作业。

- 1 在 OpenManage Integration for VMware vCenter 中，导航至**监测 > 作业队列**选项卡。
- 2 要选择想要运行的保修作业，请单击**保修历史**，然后单击**机箱保修**。
- 3 单击  图标。
- 4 在**成功**对话框中，单击**关闭**。
保修作业此时会出现在队列中。

监测单个主机

使用 OpenManage Integration for VMware vCenter 可查看单个主机的详细信息。您可以从导航器窗格中访问 VMware vCenter 中的主机，此操作将显示所有供应商的所有主机。要查看更多详细信息，请单击特定 Dell EMC 主机。要查看 Dell 主机的列表，请从 OpenManage Integration for VMware vCenter 的导航器窗格中，单击 **Dell EMC 主机**。

查看主机摘要详细信息

关于此任务

您可以在**主机摘要**页面上查看单个主机的主机摘要详细信息，其中显示了各种 Portlet。这些 Portlet 中有两种适用于 OpenManage Integration for VMware vCenter。这两种 Portlet 分别是：

- Dell EMC 主机运行状况
- Dell EMC 主机信息

像其他 Portlet 一样，您可以将这两种 Portlet 拖放到您希望的位置，并根据您的要求对这两种 Portlet 进行格式化和自定义。要查看主机摘要详细信息，请执行以下操作：

步骤

- 1 在 OpenManage Integration for VMware vCenter 中的导航器窗格中，单击**主机**。
- 2 在**对象**选项卡中，选择要查看的特定主机。
- 3 单击**摘要**选项卡。
- 4 查看主机摘要详细信息：

表. 13: 主机摘要信息

信息	说明
交替系统	状态区域下方和 Portlet 前面的黄色方框中显示 OpenManage Integration for VMware vCenter 的警报。
通知区域	在右侧面板区域中显示 Dell 产品集成信息，在该区域中可以查找关于以下内容的信息： <ul style="list-style-type: none">• 最近的任务• 正在进行的工作• 警报 Dell 警报信息显示在该通知区域 Portlet 中。

- 5 向下滚动可查看 Dell EMC Server Management Portlet。

表. 14: Dell EMC Server Management Portlet

信息	说明
服务标签	显示您的 PowerEdge 服务器的服务标签。在致电技术支持时需使用此 ID。
型号名称	显示服务器的型号名称。
故障恢复内存	<p>显示 BIOS 属性的状态。该 BIOS 属性在服务器的初始设置过程中已在 BIOS 中启用，它显示服务器的内存运行模式。在更改内存运行模式值时，请重新启动系统。这适用于支持故障恢复内存 (FRM) 选项且运行 ESXi 5.5 或更高版本的第 12 代或更高版本的 PowerEdge 服务器。该 BIOS 属性的 4 个不同的值为：</p> <ul style="list-style-type: none"> • 已启用并受保护：此值表示系统受支持，操作系统版本为 ESXi 5.5 或更高版本，并且 BIOS 中的内存运行模式已设置为 FRM。 • 已启用 NUMA 并受保护：此值表示系统受支持，操作系统版本为 ESXi 5.5 或更高版本，并且 BIOS 中的内存运行模式已设置为 NUMA FRM。 • 已启用但未受保护：此值表示，它支持具有低于 ESXi 5.5 的操作系统版本的系统。 • 已禁用：此值表示，它支持具有任何操作系统版本的有效系统，并且 BIOS 中的内存运行模式未设置为 FRM。 • 空白：如果 BIOS 中的内存运行模式不受支持，将不显示 FRM 属性。
系统锁定模式	显示第 14 代 PowerEdge 服务器的 iDRAC 锁定模式状态。封闭的锁表示 iDRAC 锁定模式处于开启状态，然而打开的锁表示 iDRAC 锁定模式已关闭。
识别	<p>将显示以下项：</p> <ul style="list-style-type: none"> • 主机名 — 显示 Dell EMC 主机的名称 • 电源状态 — 显示电源是打开还是关闭 • iDRAC IP — 显示 iDRAC IP 地址 • 管理 IP — 显示管理 IP 地址 • 连接配置文件 — 显示此主机的连接配置文件名称 • 型号 — 显示 Dell EMC 服务器型号 • 服务标签 — 显示服务器的服务标签 • 资产标签 — 显示的资产标签 • 保修剩余天数 — 显示保修的剩余天数 • 上次资源清册扫描 — 显示上次资源清册扫描的日期和时间
虚拟机监控程序和固件	<p>将显示以下项：</p> <ul style="list-style-type: none"> • 虚拟机监控程序 — 显示虚拟机监控程序版本 • BIOS 版本 — 显示 BIOS 版本 • 远程访问卡版本 — 显示远程访问卡版本
管理控制台	<p>管理控制台用于启动外部系统管理控制台，例如：</p> <ul style="list-style-type: none"> • 启动远程访问控制台 (iDRAC) — 启动 Integrated Dell Remote Access Controller (iDRAC) Web 用户界面。

信息	说明
	<ul style="list-style-type: none"> 启动 OMSA 控制台 — 启动 OMSA 控制台以访问 OpenManage Server Administrator 用户界面。
主机操作	要以各种时间间隔闪烁，请设置物理服务器以按各种时间间隔闪烁。请参阅 闪烁指示灯 。

6 查看 Dell EMC 主机运行状况 Portlet:

表. 15: Dell EMC 主机运行状况

信息	说明
Dell EMC 主机运行状况	<p>组件运行状况是所有主要主机服务器组件的状态的图示，包括服务器全局状态、服务器、电源设备、温度、电压、处理器、电池、侵入、硬件日志、电源管理，以及电源和内存。机箱运行状况参数适用于型号 VRTX 版本 1.0 及更高版本、M1000e 版本 4.4 及更高版本。对于低于 4.3 的版本，只显示两种运行状况标志，即正常和警告或严重（带橙色感叹号的倒三角）。总体运行状况基于具有最差运行状况参数的机箱来指示运行状况。选项包括：</p> <ul style="list-style-type: none"> 正常（绿色复选标记）— 组件正常运行。 警告（带有感叹号的黄色三角形）— 组件有非严重错误。 严重（红色 X）— 组件有严重故障。 未知（问号）— 组件的状态未知。

例如，如果有 5 个正常标志和 1 个警告标志，则总体运行状况显示为警告。

查看单个主机的硬件详细信息

关于此任务

您可以在 **Dell EMC 主机信息** 选项卡中查看单个主机的硬件详细信息。要使信息出现在本页面上，请运行资源清册作业。硬件视图直接报告来自 OMSA 和 iDRAC 的数据。请参阅[运行资源清册作业](#)。

步骤

- 1 在 OpenManage Integration for VMware vCenter 中的导航器窗格中，单击**主机**。
- 2 在**主机**选项卡上，选择要查看其硬件：<Component Name>详细信息的特定主机。
- 3 在**监测**选项卡中，选择 **Dell EMC 主机信息** 选项卡。

注: 如果系统锁定模式在第 14 代主机上开启，将在顶部显示带锁封闭图标的黄色条带。

在硬件：<Component Name>子选项卡上，查看各个组件的以下信息。

表. 16: 单个主机的硬件信息

硬件：组件	信息
硬件：FRU	<ul style="list-style-type: none"> 部件名 — 显示 FRU 部件名 部件号 — 显示 FRU 部件号 制造商 — 显示制造商的名称 序列号 — 显示制造商的序列号

硬件：组件	信息
	<ul style="list-style-type: none"> • 制造日期 — 显示制造日期
硬件：处理器	<ul style="list-style-type: none"> • 插槽 — 显示插槽编号 • 速度 — 显示当前速度 • 品牌 — 显示处理器品牌 • 版本 — 显示处理器版本 • 核心 — 显示此处理器中核心的数量
硬件：电源设备	<ul style="list-style-type: none"> • 类型 — 显示电源设备的类型。电源设备类型包括： <ul style="list-style-type: none"> • 未知 • 线性 • 切换 • BATTERY • UPS • 转换器 • 稳压器 • 交流 • 直流 • VRM • 位置 — 显示电源设备的位置，比如插槽 1 • 输出（瓦） — 显示功率，以瓦特为单位
硬件：内存	<ul style="list-style-type: none"> • 内存插槽 — 显示已使用、总计和可用内存计数 • 内存容量 — 显示已安装内存、总内存容量和可用内存 • 插槽 — 显示 DIMM 插槽 • 大小 — 显示内存大小 • 类型 — 显示内存类型
硬件：NIC	<ul style="list-style-type: none"> • 总计 — 显示可用网络接口卡的总计数 • 名称 — 显示 NIC 名称 • 制造商 — 仅显示制造商名称 • MAC 地址 — 显示 NIC MAC 地址
硬件：PCI 插槽	<ul style="list-style-type: none"> • PCI 插槽 — 显示已使用、总计和可用 PCI 插槽 • 插槽 — 显示插槽 • 制造商 — 显示 PCI 插槽的制造商名称 • 说明 — 显示 PCI 设备的说明 • 类型 — 显示 PCI 插槽类型 • 宽度 — 显示数据总线宽度（如果可用）
硬件：远程访问卡	<ul style="list-style-type: none"> • IP 地址 — 显示远程访问卡的 IP 地址 • MAC 地址 — 显示远程访问卡的 MAC 地址 • RAC 类型 — 显示远程访问卡的类型 • URL — 显示与此主机关联的 iDRAC 的有效 URL

查看单个主机的存储设备详细信息

关于此任务

您可以在 **Dell EMC 主机信息** 选项卡中查看单个主机的存储设备详细信息。要使信息出现在本页面上，请运行资源清册作业。硬件报告直接来自 OMSA 和 iDRAC 的数据。请参阅 [运行资源清册作业](#)。该页面会显示不同的选项，具体取决于从**视图**下拉式列表中选择的内容。如果选择**物理磁盘**，则会显示另一个下拉式列表。下一个下拉式列表称为筛选器，使用它可以筛选物理磁盘选项。要查看存储设备的详细信息，请执行以下操作：

步骤

- 1 在 OpenManage Integration for VMware vCenter 中的导航器窗格中，单击**主机**。
- 2 在**对象**选项卡上，选择要查看其“存储设备：物理磁盘”详细信息的特定主机。
- 3 在**监测**选项卡中，选择 **Dell EMC 主机信息** 选项卡。
在**存储**子选项卡上，查看以下内容：

表. 17: 单个主机的存储设备详细信息

组件	信息
存储时	显示虚拟磁盘、控制器、机柜和关联物理磁盘的数量，及全局热备份和专用热备份的计数。当您从“视图”下拉式列表中进行选择后，所选选项将突出显示。
查看	显示针对此主机要查看的选项： <ul style="list-style-type: none"> • 虚拟磁盘 • 物理磁盘 • 控制器 • 机柜

查看该视图选项的存储设备详细信息

主机**存储设备**页面上的存储设备选项取决于您在**视图**下拉式列表中所做的选择。从“视图”下拉式列表中选择所提及选项中的任意一项，然后查看以下内容：

表. 18: 单个主机的存储设备详细信息

信息	说明
虚拟磁盘	<ul style="list-style-type: none"> • 名称 — 显示虚拟磁盘的名称 • 设备 FQDD — 显示 FQDD • 物理磁盘 — 显示虚拟磁盘所处的物理磁盘 • 容量 — 显示虚拟磁盘的容量 • 布局 — 显示虚拟存储设备的布局类型，这表示为此虚拟磁盘配置的 RAID 的类型 • 介质类型 — 显示 SSD 或 HDD • 控制器 ID — 显示控制器 ID • 设备 ID — 显示设备 ID • 条带大小 — 显示条带大小，即每个条带在单个磁盘上所占的空间大小 • 总线协议 — 显示物理磁盘（包括在虚拟磁盘中）使用的技术。可能的值包括： <ul style="list-style-type: none"> • SCSI • SAS

信息	说明
	<ul style="list-style-type: none"> • SATA • 默认读取策略 — 显示控制器支持的默认读取策略。选项包括： <ul style="list-style-type: none"> • 预读 • 不预读 • 自适应预读 • 读取高速缓存已启用 • 读取高速缓存已禁用 • 默认写入策略 — 显示控制器支持的默认写入策略。选项包括： <ul style="list-style-type: none"> • 回写式 • 强制回写 • 回写已启用 • 直写 • 已保护启用的写入高速缓存 • 写入高速缓存已禁用 • 高速缓存策略 — 显示是否已启用高速缓存策略
<p>物理磁盘 — 当您选择此选项时，会显示筛选器下拉式列表。 可以基于以下选项筛选物理磁盘：</p> <ul style="list-style-type: none"> • 所有物理磁盘 • 全局热备用 • 专用热备用 • 最后一个选项显示自定义命名的虚拟磁盘 	<ul style="list-style-type: none"> • 名称 — 显示物理磁盘的名称 • 设备 FQDD — 显示设备 FQDD • 容量 — 显示物理磁盘容量 • 磁盘状态 — 显示物理磁盘状态。选项包括： <ul style="list-style-type: none"> • 联机 • 就绪 • 降级 • 故障 • 脱机 • 正在重建 • 不兼容 • 已移除 • 已清除 • 检测到 SMART 警报 • 未知 • 外来 • 不受支持 • 已配置 — 显示是否已配置磁盘 • 热备盘类型 — 显示热备盘类型。选项包括： <ul style="list-style-type: none"> • 否 — 没有热备用 • 全局 — 未使用的备份磁盘，它是磁盘组的一部分 • 专用 — 已分配给单个虚拟磁盘的未使用备份磁盘。如果虚拟磁盘中的某个物理磁盘发生故障，热备用就会启用以更换故障物理磁盘，而不用中断系统或需要用户干预。 • 虚拟磁盘 — 显示虚拟磁盘的名称 • 总线协议 — 显示总线协议 • 控制器 ID — 显示控制器 ID • 连接器 ID — 显示连接器 ID • 机柜 ID — 显示机柜 ID • 设备 ID — 显示设备 ID • 型号 — 显示物理存储磁盘的型号 • 部件号 — 显示存储设备部件号

信息	说明
	<ul style="list-style-type: none"> • 序列号 — 显示存储设备序列号 • 供应商 — 显示存储设备供应商名称
控制器	<ul style="list-style-type: none"> • 控制器 ID — 显示控制器 ID • 名称 — 显示控制器的名称 • 设备 FQDD — 显示设备的 FQDD • 固件版本 — 显示固件版本 • 所需最低固件 — 显示所需最低固件。如果固件过期并且有较新的版本可用，则此列会被填充 • 驱动程序版本 — 显示驱动程序版本 • 巡检读取模式 — 显示巡检读取模式 • 高速缓存大小 — 显示高速缓存大小
机柜	<ul style="list-style-type: none"> • 控制器 ID — 显示控制器 ID • 连接器 ID — 显示连接器 ID • 机柜 ID — 显示机柜 ID • 名称 — 显示机柜的名称 • 设备 FQDD — 显示设备 FQDD • 服务标签 — 显示服务标签

有关 Web 客户端中的系统事件日志

系统事件日志 (SEL) 提供由 OMIVV 查找到的硬件状态信息并根据以下条件显示信息：

状态	有多个状态图标：Informational（蓝色感叹号）、Warning（带有感叹号的黄色三角形）、错误（红色 XⓈ）和未知（带 ? 的框）。
时间（服务器时间）	表明事件发生的时间和日期。
搜索此页面	显示特定消息、服务器名称、配置设置等等。

严重性级别定义如下：

信息	OMIVV 操作已成功完成。
警告	OMIVV 操作部分失败，部分成功。
错误	OMIVV 操作失败。

可以将日志保存为外部 CSV 文件。请参阅[显示单个主机的系统事件日志](#)。


显示单个主机的事件日志

关于此任务

要显示事件，请执行以下步骤：

步骤

- 1 要访问[监测](#)选项卡和打开[系统事件日志](#)子选项卡，请执行以下任一步骤：

选项	说明
从 OMIVV	执行此选项的以下步骤： <ol style="list-style-type: none"> 在 OpenManage Integration for VMware vCenter 中的导航器窗格中，单击主机。 在对象选项卡上，双击您想要查看 SEL 日志的特定主机。
从主页页面	在主页页面中，单击 主机和群集 。
2	在 监测 选项卡上，选择 Dell EMC 主机信息 > 系统事件日志 。 最近的系统日志条目提供 10 个最近的系统事件日志条目。
3	要更新 系统事件日志 ，请执行全局刷新。
4	要限制（筛选）事件日志条目的数量，请选择以下选项之一： <ul style="list-style-type: none"> 在搜索筛选器文本框中，要动态筛选日志条目，请输入一个文本字符串。 要清除筛选器文本框，可单击 X，将显示所有事件日志条目。
5	要清除所有事件日志条目，可单击 清除日志 。 清除所有日志条目后，将显示一条消息指出已将其全部删除。然后您可以选择以下选项之一： <ul style="list-style-type: none"> 要同意清除日志条目，可单击清除日志。 要取消，可单击 取消。
6	要将事件日志导出到 CSV 文件，可单击  。
7	要浏览到位置和保存系统事件日志，请单击 保存 。

查看单个主机的其他硬件详细信息


关于此任务

您可在 **Dell EMC 主机信息**选项卡上查看单个主机的固件、电源监测、保修状态详细信息。要使信息出现在本页面上，请运行资源清册作业。硬件视图直接报告来自 OMSA 和 iDRAC 的数据。请参阅[立即运行机箱资源清册作业](#)。

步骤

- 在 OpenManage Integration for VMware vCenter 中的导航器窗格中，单击**主机**。
- 在**对象**选项卡上，选择您要查看 <Component Name> 详细信息的特定主机。
- 在**监测**选项卡中，选择 **Dell EMC 主机信息**选项卡。
在“硬件：<Component Name>”子选项卡上，查看各个组件的以下信息：

表. 19: 单个主机信息

组件	信息
固件 在主机页面中可以使用搜索、筛选器，以及导出固件信息的 CSV 文件	<ul style="list-style-type: none"> 名称 — 显示此主机上所有固件的名称 类型 — 显示固件的类型 版本 — 显示此主机上所有固件的版本 安装日期 — 显示安装日期
电源监测  注: 此处使用的主机时间是指主机所在位置的本地时间。	<ul style="list-style-type: none"> 常规信息 — 显示电源预算和当前配置文件名称 阈值 — 显示警告和故障阈值（以瓦特为单位） 保留电源容量 — 显示即时和峰值保留电源容量（以瓦特为单位） 能源统计信息 <ul style="list-style-type: none"> 类型 — 显示能耗统计信息类型 测量开始时间（主机时间） — 显示主机开始消耗电源的日期和时间

组件	信息
	<ul style="list-style-type: none"> • 测量结束时间（主机时间） — 显示主机停止消耗电源的日期和时间 • 读数 — 显示在一分钟时间内读数的平均值 • 峰值时间（主机时间） — 显示主机峰值安培的日期和时间 • 峰值读数 — 显示系统峰值功率统计信息，这是系统消耗的峰值功率（以瓦特为单位）
保修 ① 注： 要查看保修状态，请确保运行保修作业。请参阅 运行保修检索作业 。使用保修状态页面可以监测保修到期日期。保修设置通过启用或禁用保修计划，然后设置“最少天数阈值”警报，来控制何时可从 Dell 联机检索服务器保修信息。	<ul style="list-style-type: none"> • 提供商 — 显示保修提供商的名称 • 说明 - 显示说明 • 开始日期 — 显示保修开始日期 • 结束日期 — 显示保修结束日期 • 剩余天数 — 显示保修剩余天数 • 上次更新时间 — 上次更新保修的时间

监测群集和数据中心中的主机

使用 OpenManage Integration for VMware vCenter 可查看数据中心或群集中包括的所有主机的详细信息。您可以单击数据网格行标题来对数据进行排序。数据中心和群集页面支持将信息导出到 CSV 文件，并在数据网格上提供筛选或搜索功能。

查看数据中心和群集的概览

关于此任务

可在“Dell EMC 数据中心/群集信息”选项卡上查看数据中心或群集的主机详细信息。要使信息出现在本页面上，请运行资源清册作业。您看到的数据可能因访问数据的视图而异。硬件视图直接报告来自 OMSA 和 iDRAC 的数据。请参阅[运行资源清册作业](#)。

① **注：**数据中心和群集页面让您能将信息导出到 CSV 文件，并在数据网格上提供筛选或搜索功能。

步骤

- 1 在 OpenManage Integration for VMware vCenter 中的导航器窗格中，单击 **vCenter**。
- 2 单击**数据中心**或**群集**。
- 3 在**对象**选项卡中，选择您要查看其主机详细信息的特定数据中心或群集。
- 4 在**监测**选项卡中，选择 **Dell EMC 数据中心/群集信息 > 概览**选项卡，并查看详细信息。

① **注：**要显示详细信息的完整列表，请从数据网格选择特定主机。

表. 20: 数据中心和群集的概览

信息	说明
数据中心/群集信息	将显示以下项： <ul style="list-style-type: none"> • 数据中心/群集名称 • Dell 的受管主机数 • 总能耗
系统锁定模式	显示“iDRAC 锁定模式”的状态。主机总数的 iDRAC 锁定模式状态显示如下： <ul style="list-style-type: none"> • 已打开电源 • 关闭

信息	说明
	<ul style="list-style-type: none"> 不适用（仅适用于第 14 代服务器）
硬件资源	将显示以下项： <ul style="list-style-type: none"> 处理器总数 内存总量 虚拟磁盘容量
保修摘要	显示所选主机的保修状态。状态选项包括： <ul style="list-style-type: none"> 已过期保修 保修期内 未知保修
主机	显示主机名
服务标签	显示主机服务标签
型号	显示 PowerEdge 型号
资产标签	显示资产标签（如已配置）
机箱服务标签	显示机箱服务标签（如适用）
操作系统版本	显示 ESXi 操作系统版本
位置	仅刀片服务器：显示插槽位置。对于其他，显示“不适用”
系统锁定模式	仅适用于第 14 代 PowerEdge 服务器：显示主机的 iDRAC 锁定模式，开启、关闭或未知。 对于早于第 14 代的 PowerEdge 服务器，系统锁定模式将显示为不适用。
iDRAC IP	显示 iDRAC IP 地址
服务控制台 IP	显示服务控制台 IP
CMC URL	显示 CMC URL，即刀片服务器的机箱 URL；其他情况下，它将显示“不适用”
CPU	显示 CPU 数
内存	显示主机内存
电源状态	显示主机是否已加电
上次资源清册	显示上次资源清册作业的日期和时间
连接配置文件	显示连接配置文件的名称
远程访问卡版本	显示远程访问卡版本
BIOS 固件版本	显示 BIOS 固件版本

查看数据中心和群集的硬件详细信息

关于此任务

您可以在 **Dell EMC 数据中心/群集信息** 选项卡上查看单个主机的硬件详细信息。要使信息出现在本页面上，请运行资源清册作业。数据中心和群集页面让您能将信息导出到 CSV 文件，并在数据网络上提供筛选或搜索功能。您看到的数据可能因访问数据的视图而异。硬件视图直接报告来自 OMSA 和 iDRAC 的数据。请参阅[运行资源清册作业](#)。

步骤

- 1 在 OpenManage Integration for VMware vCenter 中的导航器窗格中，单击 **vCenter 资源清册列表**。
- 2 单击**数据中心**或**群集**。
- 3 在**对象**选项卡中，选择要查看其组件特定详细信息的特定数据中心或群集。
- 4 在**监测**选项卡中，选择 **Dell EMC 数据中心/群集信息** 选项卡。
在“硬件：<Component Name>”子选项卡上，查看各个组件的以下信息。

表. 21: 数据中心和群集的硬件信息

硬件：组件	信息
硬件：FRU	<ul style="list-style-type: none"> • 主机 — 显示主机名 • 服务标签 — 显示主机的服务标签 • 部件名 — 显示 FRU 部件名 • 部件号 — 显示 FRU 部件号 • 制造商 — 显示制造商的名称 • 序列号 — 显示制造商的序列号 • 制造日期 — 显示制造日期
硬件：处理器	<ul style="list-style-type: none"> • 主机 — 显示主机名 • 服务标签 — 显示主机的服务标签 • 插槽 — 显示插槽编号 • 速度 — 显示当前速度 • 品牌 — 显示处理器品牌 • 版本 — 显示处理器版本 • 核心 — 显示此处理器中核心的数量
硬件：电源设备	<ul style="list-style-type: none"> • 主机 — 显示主机名 • 服务标签 — 显示主机的服务标签 • 类型 — 显示电源设备的类型。电源设备类型包括： <ul style="list-style-type: none"> • 未知 • 线性 • 切换 • BATTERY • UPS • 转换器 • 稳压器 • 交流 • 直流 • VRM • 位置 — 显示电源设备的位置，比如插槽 1 • 输出（瓦） — 显示功率，以瓦特为单位

硬件：组件	信息
	<ul style="list-style-type: none"> • 状态— 显示电源设备状态。状态选项包括： <ul style="list-style-type: none"> • 其他 • 未知 • 正常 • 严重 • 不严重 • 可恢复 • 不可恢复 • 高 • 低
硬件：内存	<ul style="list-style-type: none"> • 主机— 显示主机名 • 服务标签— 显示主机的服务标签 • 插槽— 显示 DIMM 插槽 • 大小— 显示内存大小 • 类型— 显示内存类型
硬件：NIC	<ul style="list-style-type: none"> • 主机— 显示主机名 • 服务标签— 显示主机的服务标签 • 名称— 显示 NIC 名称 • 制造商— 仅显示制造商名称 • MAC 地址— 显示 NIC MAC 地址
硬件：PCI 插槽	<ul style="list-style-type: none"> • 主机— 显示主机名 • 服务标签— 显示主机的服务标签 • 插槽— 显示插槽 • 制造商— 显示 PCI 插槽的制造商名称 • 说明— 显示 PCI 设备的说明 • 类型— 显示 PCI 插槽类型 • 宽度— 显示数据总线宽度（如果可用）
硬件：远程访问卡	<ul style="list-style-type: none"> • 主机— 显示主机名 • 服务标签— 显示主机的服务标签 • IP 地址— 显示远程访问卡的 IP 地址 • MAC 地址— 显示远程访问卡的 MAC 地址 • RAC 类型— 显示远程访问卡的类型 • URL— 显示与此主机关联的 iDRAC 的有效 URL

查看数据中心和群集的存储详细信息

关于此任务


您可在 **数据中心/群集信息** 选项卡上查看数据中心或群集的物理存储详细信息。要使信息出现在本页面上，请运行资源清册作业。数据中心和群集页面让您能将信息导出到 CSV 文件，并在数据网络上提供筛选/搜索功能。硬件视图直接报告来自 OMSA 和 iDRAC 的数据。请参阅 [运行资源清册作业](#)。

步骤

- 1 在 OpenManage Integration for VMware vCenter 中的导航器窗格中，单击 **vCenter 资源清册列表**。
- 2 单击 **数据中心** 或 **群集**。

- 3 在**对象**选项卡中，选择特定数据中心或群集。
- 4 在**监测**选项卡中，选择 **Dell EMC 数据中心/群集信息**选项卡，然后导航至**存储 > 物理磁盘/虚拟磁盘**。
要显示详细信息的完整列表，请从数据网格选择特定主机。

表. 22: 数据中心和群集的存储详细信息

存储：磁盘	说明
物理磁盘	<ul style="list-style-type: none"> • 主机 — 显示主机名 • 服务标签 — 显示主机的服务标签 • 容量 — 显示物理磁盘容量 • 磁盘状态 — 显示物理磁盘状态。选项包括： <ul style="list-style-type: none"> • 联机 • 就绪 • 降级 • 故障 • 脱机 • 正在重建 • 不兼容 • 已移除 • 已清除 • SMART 警报检测 • 未知 • 外来 • 不受支持 <p style="margin-left: 20px;">  注: 有关这些警报含义的更多信息，请参阅 Dell EMC OpenManage Server Administrator 存储管理用户指南，位于：dell.com/support </p> <ul style="list-style-type: none"> • 型号 — 显示物理存储磁盘的型号 • 上次资源清册 — 显示已经运行的上次资源清册的日期、月份和时间 • 状态 — 显示主机状态 • 控制器 ID — 显示控制器 ID • 连接器 ID — 显示连接器 ID • 机柜 ID — 显示机柜 ID • 设备 ID — 显示设备 ID • 总线协议 — 显示总线协议 • 热备盘类型 — 显示热备盘类型。选项包括： <ul style="list-style-type: none"> • 否 — 没有热备盘 • 全局 — 未使用的备份磁盘，它是磁盘组的一部分 • 专用 — 已分配给单个虚拟磁盘的未使用备份磁盘。如果虚拟磁盘中的某个物理磁盘发生故障，热备用就会启用以更换故障物理磁盘，而不用中断系统或需要用户干预。 • 部件号 — 显示存储设备部件号 • 序列号 — 显示存储设备序列号 • 供应商名称 — 显示存储设备供应商名称
虚拟磁盘	<ul style="list-style-type: none"> • 主机 — 显示主机的名称 • 服务标签 — 显示主机的服务标签 • 名称 — 显示虚拟磁盘的名称 • 物理磁盘 — 显示虚拟磁盘所处的物理磁盘 • 容量 — 显示虚拟磁盘的容量

存储：磁盘	说明
	<ul style="list-style-type: none"> • 布局 — 显示虚拟存储设备的布局类型。这表示为此虚拟磁盘配置的 RAID 的类型 • 上次资源清册 — 显示上次运行资源清册操作的日期和时间 • 控制器 ID — 显示控制器 ID • 设备 ID — 显示设备 ID • 介质类型 — 显示 SSD 或 HDD • 总线协议 — 显示虚拟磁盘中包括的物理磁盘所使用的技术。可能的值包括： <ul style="list-style-type: none"> • SCSI • SAS • SATA • 条带大小 — 显示条带大小，即每个条带在单个磁盘上所占的空间大小 • 默认读取策略 — 显示控制器支持的默认读取策略。选项包括： <ul style="list-style-type: none"> • 预读 • 不预读 • 自适应预读 • 读取高速缓存已启用 • 读取高速缓存已禁用 • 默认写入策略 — 显示控制器支持的默认写入策略。选项包括： <ul style="list-style-type: none"> • 回写式 • 强制回写 • 回写已启用 • 直写 • 已保护启用的写入高速缓存 • 写入高速缓存已禁用 • 磁盘高速缓存策略 — 显示控制器支持的默认高速缓存策略。选项包括： <ul style="list-style-type: none"> • 已启用—高速缓存 I/O • 已禁用—直接 I/O

查看数据中心和群集的其他硬件详细信息

关于此任务

您可在 **Dell EMC 数据中心/群集信息** 选项卡上查看数据中心或群集的固件、电源监测、保修状态详细信息。要使信息出现在本页面上，请运行资源清册作业。数据中心和群集页面让您能将信息导出到 CSV 文件，并在数据网络上提供筛选/搜索功能。硬件视图直接报告来自 OMSA 和 iDRAC 的数据。请参阅[立即运行资源清册作业](#)。

步骤

- 1 在 OpenManage Integration for VMware vCenter 中的导航器窗格中，单击 **vCenter**。
- 2 单击**数据中心或群集**。
- 3 在**对象**选项卡中，选择要查看其主机组件详细信息的特定数据中心或群集。
- 4 在**监测**选项卡中，选择 **Dell EMC 数据中心/群集信息** 选项卡。
在 <Component Name> 子选项卡上，查看各个组件的以下信息：

表. 23: 单个主机信息

组件	信息
固件	<ul style="list-style-type: none"> • 主机 — 显示主机的名称 • 服务标签 — 显示主机的服务标签 • 名称 — 显示此主机上所有固件的名称

组件	信息
<p>电源监测</p> <p>① 注: 要显示详细信息的完整列表, 请从数据网格选择特定主机。</p>	<ul style="list-style-type: none"> • 版本 — 显示此主机上所有固件的版本 • 主机 — 显示主机的名称 • 服务标签 — 显示主机的服务标签 • 当前配置文件 — 显示电源配置文件以最大化您系统的性能并节省能源 • 能耗 — 显示主机的能耗 • 峰值保留容量 — 显示峰值电源保留容量 • 电源预算 — 显示此主机的功率上限 • 警告阈值 — 显示系统为温度探测器警告阈值配置的最大值 • 故障阈值 — 显示系统为温度探测器故障阈值配置的最大值 • 即时保留容量 — 显示主机瞬间余量容量 • 能耗开始日期 — 显示主机开始消耗电源的日期和时间 • 能耗结束日期 — 显示主机停止消耗电源的日期和时间 • 系统峰值功率 — 显示主机峰值功率 • 系统峰值功率开始日期 — 显示主机峰值功率开始的日期和时间 • 系统峰值功率结束日期 — 显示主机峰值功率结束的日期和时间 • 系统峰值安培 — 显示主机峰值安培 • 系统峰值安培开始日期 — 显示主机峰值安培的起始日期和时间 • 系统峰值安培结束日期 — 显示主机峰值安培的结束日期和时间
<p>保修摘要</p> <p>① 注: 要查看保修状态, 请确保运行保修作业。请参阅运行保修检索作业。使用保修摘要页面可以监测保修到期日期。保修设置通过启用或禁用保修计划, 然后设置“最少天数阈值”警报, 来控制何时可从 Dell 联机检索服务器保修信息。</p>	<ul style="list-style-type: none"> • 保修摘要 — 主机保修摘要将使用图标显示, 以虚拟方式显示处于各种状态类别的主机数量 • 主机 — 显示主机名 • 服务标签 — 显示主机的服务标签 • 说明 — 显示说明 • 保修状态 — 显示主机的保修状态。状态选项包括: <ul style="list-style-type: none"> • 活动 — 主机在保修期内, 尚未超过任何阈值 • 警告 — 主机处于活动状态, 但已超过警告阈值 • 严重 — 与警告相同, 但针对严重阈值 • 已过期 — 此主机保修已过期 • 未知 — OpenManage Integration for VMware vCenter 无法获得保修状态, 因为保修作业未运行、在获取数据时出错或系统没有参与保修 • 剩余天数 — 显示保修的剩余天数

设置物理服务器闪烁指示灯

关于此任务

要在大型数据中心环境中协助定位物理服务器, 可以设置正面指示灯在设定的时间段闪烁。

步骤

- 1 在 OpenManage Integration for VMware vCenter 中的导航器区域中, 在“资源清册列表”下, 单击**主机**。
- 2 在**对象**选项卡中, 双击所需的主机。
- 3 在**摘要**选项卡中, 向下滚动到 Dell EMC Server Management Portlet。
- 4 在**主机操作**下, 选择**闪烁指示灯**。

5 选择以下操作之一：

- 要开启闪烁并设置时间段，请在**指示灯**对话框中，单击**闪烁开**，使用“超时”下拉式列表选择超时增量，然后单击**确定**。
- 要关闭闪烁，请在**指示灯**对话框中，单击**闪烁关**，然后单击**确定**。

配置系统锁定模式

系统锁定模式设置在 PowerEdge 服务器的第 14 代 iDRAC 中可用。打开设置将锁定系统配置（包括固件更新）。该设置旨在保护系统被进行意外更改。您可以通过使用 OMIVV 设备或从 iDRAC 控制台打开或关闭受管主机的系统锁定模式。

关于此任务

从 OMIVV 版本 4.1 和更高版本中，您可以配置和监测服务器中 iDRAC 的锁定模式。您可以通过锁定或解锁主机或群集级别的主机或群集来配置系统锁定模式。系统锁定模式开启时，以下功能有如下限制：

- 所有配置任务，例如固件更新、操作系统部署、清除系统事件日志、重设 iDRAC 以及配置 iDRAC 陷阱位置。

要配置主机或群集级别的主机或群集的系统锁定模式，请执行以下步骤：

步骤

- 1 要启动配置系统锁定模式向导，请执行以下任一分步骤：
 - a 在**导航器**窗格中，单击**主机和群集**，选择并右键单击主机或群集，并单击**操作**下拉列表，然后选择**所有 OpenManage Integration 操作 > 配置系统锁定模式**。
 - b 在 OpenManage Integration 中，单击**主机**和**群集**页面，选择并右键单击主机或群集，或者选择一个主机或群集，然后单击**操作**下拉列表，然后选择**所有 OpenManage Integration 操作 > 配置系统锁定模式**。
 - c 在**导航器**窗格中，选择一个主机，然后单击**摘要 > Dell EMC 主机信息 > 配置系统锁定模式**。
 - d 在**导航器**窗格中，选择一个主机或群集，然后单击**监测 > Dell EMC 主机信息 > 固件 > 配置系统锁定模式**。
- 2 要启用系统锁定模式，请选择**开启**选项，或要禁用锁定模式，请选择**关闭**。
- 3 单击**应用**。

如果您尝试为第 11 代至第 13 代 PowerEdge 服务器配置系统锁定模式，将会有消息提示您此平台不支持该功能。

后续步骤

系统锁定配置完成后，您可以在**作业队列**页面中查看锁定模式的更新状态。有关锁定模式的作业队列信息仅在一个群集级别内有效。要访问作业队列页面，请在 OpenManage Integration 中，选择**监测 > 作业队列 > 系统锁定模式作业**。有关系统锁定模式的更多信息，请参阅 iDRAC 说明文件。

关于固件更新

OMIVV 设备允许您在受管主机上执行 BIOS 和固件更新作业。您可以跨多个群集或非群集主机执行并发固件更新作业。不允许在同一群集的两台主机上运行并发固件更新。

下表列出了在各种部署模式下可以同时运行的固件更新作业数量，但您可以计划任意数量的固件更新作业：

表. 24: 各种部署模式中的固件更新作业

小型部署模式	中型部署模式	大型部署模式
5	10	15

以下是执行固件更新的两种方法：

- 单一 DUP — 通过直接指向 DUP 位置（CIFS 或 NFS 共享）执行 iDRAC、BIOS 或 LC 固件更新。单一 DUP 方法只能在主机级别使用。
- 存储库 — 执行 BIOS 和所有支持的固件更新。该方法在主机级别和群集级别都可以使用。以下是两种存储库位置：
 - Dell 联机 — 该位置使用 Dell 的固件更新存储库 (ftp.dell.com)。OpenManage Integration for VMware vCenter 将从 Dell 存储库下载所选的固件更新，并更新受管的主机。

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 — 您可以在基于 CIFS 或 NFS 的网络共享中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) 转储或者使用 DRM 创建的自定义存储库。此网络共享应通过 OMIVV 访问。

注：如果使用的是 CIFS 共享，则存储库密码不能超过 31 个字符。请勿在密码中使用以下任何字符：@、&、%、'、"、,（逗号）、<、>。

有关设置固件更新存储库的信息，请参阅[设置固件更新存储库](#)。

固件更新向导始终检查 iDRAC、BIOS 和 Lifecycle Controller 的最低固件级别，并尝试将它们更新到所需的最低版本。有关 iDRAC、BIOS 和 Lifecycle Controller 的最低固件级别的更多信息，请参阅 *OpenManage Integration for VMware vCenter 兼容性值表*。一旦 iDRAC、Lifecycle Controller 和 BIOS 固件版本满足最低要求，固件更新流程将允许更新所有固件版本，包括：iDRAC、Lifecycle Controller、RAID、NIC/LOM、电源设备、BIOS 等等。

主题：

- [为单个主机运行固件更新向导](#)
- [运行群集的固件更新向导](#)
- [管理固件更新作业](#)

为单个主机运行固件更新向导

关于此任务

要执行单个主机的固件更新，请执行以下步骤：

注：固件更新过程中，建议不要删除以下内容：

- vCenter 中正在对其运行固件更新作业的主机。
- 正在对其运行固件更新作业的主机的连接配置文件。

步骤

1 要访问固件更新向导，请在 OpenManage Integration 中单击**主机**并执行以下任一操作：

- 右键单击一个主机，选择**所有 OpenManage Integration 操作 > 固件更新**。
- 在**主机**页面中，单击一个主机，然后选择**所有 OpenManage Integration 操作 > 固件更新**。
- 在**导航器**窗格中，选择一个主机，然后单击**摘要 > Dell EMC 主机信息 > 运行固件向导**。
- 在**导航器**窗格中，选择一个主机，然后单击**监测 > Dell EMC 主机信息 > 固件 > 运行固件向导**。

OMIVV 会检查主机的符合性，以及同一个群集内的任何主机中是否有其他固件更新作业正在进行。确认后，会显示**固件更新向导**，您会看到**欢迎**页面。

① 注：如果从较早版本的 OMIVV 升级到可用版本，并且已有计划好的固件更新作业，则可以在备份 OMIVV 数据库后在同一主机上启动固件更新向导并将其还原为可用版本。

2 单击**下一步**。

此时会显示**选择更新源**屏幕。

3 在**选择更新源**屏幕上，选择以下任一项：

- 选择**当前的存储库位置**，然后从**选择更新捆绑包**下拉式列表中选择固件更新捆绑包。

① 注：安装了 iDRAC 1.51 版本及更早版本的第 12 代主机不支持 64 位捆绑包。

① 注：安装了所有 iDRAC 版本的第 11 代主机不支持 64 位捆绑包。

① 注：OMIVV 支持 32 位和 64 位固件更新捆绑包。除这些捆绑包外，当目录中有发布 ID 相同的多个捆绑包时，OMIVV 还会创建一个混合捆绑包。

- 要从一个文件加载单个固件更新，请选择**单个 DUP**。单个 DUP 可以驻留在可由虚拟设备访问的 CIFS 或 NFS 共享上。按以下格式之一输入**文件位置**：

- NFS 共享 — <host>:/<share_path>/FileName.exe

- CIFS 共享 — \\<host accessible share path>\<FileName>.exe

对于 CIFS 共享，OMIVV 会提示您采用可以访问共享驱动器的域格式输入用户名和密码。

① 注：共享网络文件夹的用户名或密码不支持使用 @、% 和字符。

① 注：如果您配置使用 CIFS 共享，而不是基于 CIFS 共享的服务器消息块 (SMB) 版本 1.0，可能会导致潜在的服务中断，因为 OMIVV 无法与诸如 CIFS 共享等通信。因此，建议您使用基于仅基于 CIFS 共享的 SMB 版本 1.0。

4 如果选择**单个 DUP**，请转至第 7 步。

5 单击**下一步**。

显示**选择组件**屏幕，此屏幕列出了适用于组件的固件详细信息。该屏幕显示组件的详细信息，例如主机名、服务标签、型号名称、组件、版本、更新版本、严重程度、需要重新引导（是/否）以及所选主机的其他详细信息。

① 注：当从较早版本的 OMIVV 升级到可用版本时，“需要重新引导”字段会针对所有组件显示“否”，除非您刷新固件更新存储库。

6 使用复选框从列表中选择至少一个组件，然后单击**下一步**。

无法选择降级中或当前已计划进行更新的组件。您可以使用**筛选器**字段，从数据网格中各种组件的内容筛选逗号分隔值。您还可以在组件数据网格内拖放列。如要从向导中导出，请使用**导出至 CSV**按钮。如果选择**允许固件降级**复选框，请选择要列出进行降级的组件。

① 注：如果选择需要重新引导的组件，请确保以能够迁移工作负载的方式配置 vCenter 环境。

7 单击**下一步**。

此时会显示**计划固件更新**屏幕。

- a 在**固件更新作业名称**字段中指定作业名称，并在**固件更新说明**字段（可选）中指定说明。

固件更新作业名称是必需项，不能使用已在使用的名称。如果清除了固件更新作业名称，可以重新使用它。

- b 选择以下任一选项：

- 选择**立即更新**将立即开始固件更新作业。

- 要在稍后运行固件更新作业，请选择**计划更新**。您可以计划在当前时间 30 分钟后运行固件更新作业。
 - 在日历框中，选择月份和日期。
 - 在时间文本框中，以 HH:MM 格式键入时间。该时间是 OMIVV 设备时间。
- 要避免服务中断，请选择**在下次重新引导时应用更新**。
- 即使主机未处于维护模式，但仍要应用更新并重新引导，请选择**在不进入维护模式的情况下，应用更新并强制重新引导**。不建议使用此方法。

8 单击下一步。

此时，会显示**摘要**页面，其中提供关于所有组件固件更新的详细信息。

9 单击完成。

固件更新作业需要几分钟时间来完成，具体时间根据固件更新作业所包含的组件数而有所不同。您可以在**作业队列**页面中查看固件更新作业的状态。要访问作业队列页面，请在 OpenManage Integration 中，选择**监测 > 作业队列 > 固件更新**。固件更新任务完成后，如果在**计划固件更新**屏幕中选择了相关选项，资源清册会在所选主机上自动运行，且主机会自动退出维护模式。

运行群集的固件更新向导

OMIVV 允许您对群集上的所有主机执行 BIOS 和固件更新。向导仅更新属于连接配置文件，且在固件、CSIOR 状态、虚拟机管理程序和 OMSA 状态方面兼容的主机（仅限第 11 代服务器）。如果群集上启用了分布式资源调度 (DRS)，则 OMIVV 会通过主机进入/退出维护模式时迁移工作负载来执行支持群集的固件更新。

前提条件

确保满足以下条件后再运行固件更新向导：

- 已设置好固件更新存储库。有关设置固件更新存储库的信息，请参阅**设置固件更新存储库**。
- 要更新的群集下没有任何主机存在活动的固件更新。

关于此任务

① 注: VMware 建议使用相同的服务器硬件创建群集。

① 注: 固件更新过程中，建议不要删除以下内容：

- vCenter 中正在对其运行固件更新作业的群集中的主机。
- 正在对其运行固件更新作业的群集中主机的连接配置文件。

步骤

1 要启动固件更新向导，请在 OpenManage Integration 中单击**群集**并执行以下任一分步骤：

- 单击一个群集，选择**操作 > 所有 OpenManage Integration 操作 > 固件更新**。
- 在**对象**选项卡中，选择**操作 > 所有 OpenManage Integration 操作 > 固件更新**。
- 单击一个群集，选择**监测 > Dell EMC 群集信息 > 固件**。在**固件**屏幕中，单击**运行固件向导**链接。
- 右键单击一个群集，选择**操作 > 所有 OpenManage Integration 操作 > 固件更新**。

此时，会显示固件更新向导的**欢迎**页面。

2 查看**欢迎**页面，然后单击**下一步**。

此时，会显示**选择帐户**屏幕。

3 在**选择服务器**窗口中的**名称**树视图中，使用复选框选择主机。

4 单击**下一步**。

将显示可于其中选择捆绑包的**选择更新源**屏幕。还将显示存储库位置。

5 在**选择更新源**屏幕中，从**选择捆绑包**区域中显示的列表中选择所选主机的型号名称。

所选主机的每种型号在主机名旁有一个下拉式列表，可以从中选择所需的捆绑包。选择至少一个捆绑包进行固件更新。

① 注: OMIVV 支持 32 位和 64 位固件更新捆绑包。除这些捆绑包外，当目录中有发布 ID 相同的多个捆绑包时，OMIVV 还会创建一个混合捆绑包。

① 注: 安装了 iDRAC 1.51 版本及更早版本的第 12 代主机不支持 64 位捆绑包。

① **注:** 安装了所有 iDRAC 版本的第 11 代主机不支持 64 位捆绑包。

6 单击**下一步**。

此时会显示**选择组件**屏幕。该屏幕显示组件的详细信息，例如群集、型号、主机名、服务标签、组件、版本、更新版本、严重程度、需要重新引导（是/否）以及所选主机的其他详细信息。

7 在**选择组件**页面中，使用复选框从列表中选择至少一个组件，然后单击**下一步**继续。

您可以使用**筛选器**字段，从数据网格中各种组件的内容筛选逗号分隔值。您还可以在组件数据网格内拖放列。如要从向导中导出，请使用**导出至 CSV**按钮。通过选择**允许固件降级**复选框，可以选择早于当前版本的固件版本。

8 在**固件更新信息**页面中，查看所有固件更新详细信息。

9 单击**下一步**。

此时会显示**计划固件更新**屏幕。

a 在**固件更新作业名称**字段中输入固件更新作业名称。

固件更新作业名称是必需项，不能使用已在使用中的名称。如果清除了固件更新作业名称，可以重新使用它。

b 在**固件更新说明**字段中输入固件更新说明。

“说明”字段为可选项。

c 在**计划固件更新**下，从下面选择一个选项：

- 要立即运行更新作业，请单击**立即更新**。
- 要稍后运行更新作业，请单击**计划更新**，然后执行以下子任务：
 - a 在**日历**框中，选择月份和日期。
 - b 在**时间**文本框中，以 HH:MM 格式键入时间。

10 单击**下一步**。

将显示**摘要**页。

11 在**摘要**页面中，单击**完成**，此时会显示**已成功创建固件更新作业**消息。

固件更新作业需要几分钟时间来完成，具体时间根据所选的主机数和每个主机中的组件数而有所不同。您可以在**作业队列**页面中查看固件更新作业的状态。要访问作业队列页面，请在 OpenManage Integration 中，选择**监测 > 作业队列 > 固件更新**。固件更新任务完成后，资源清册会在所选主机上自动运行，且主机会自动退出维护模式。

管理固件更新作业

前提条件

要查看此页面中的信息，请运行群集的固件更新作业。请参阅[运行群集的固件更新向导](#)。

关于此任务

该页面显示所有固件更新作业。在此页面中，可以查看、刷新、清除或中止固件更新作业。

步骤

1 从 OpenManage Integration，选择**监测 > 作业队列 > 固件更新**。

2 要显示最新的信息，请单击**刷新**图标。

3 在数据网格中查看状态。


此网格提供有关固件更新作业的以下信息：

- 状态
- 计划的时间
- 名称
- 说明
- vCenter
- 集合大小（固件资源清册作业上的服务器数）
- 进度摘要（固件更新的进度详细信息）


4 要查看有关特定作业的更多详情，请在特定作业的数据网格内，选择作业。

在此您可以找到以下详细信息：

- 主机名
- 状态
- 开始时间
- 结束时间

5 如果您想要中止某个尚未运行的计划固件更新，请选择您要中止的作业，并单击 。

 **注：**如果您中止一个已提交至 iDRAC de 固件更新作业，固件可能仍在主机上更新，但 OMIVV 报告作业已取消。

6 如果要清除较早的固件更新作业或已计划的固件更新，请单击 。

此时会显示**清除固件更新作业**对话框。可以只清除已取消、成功的或失败的作业，不能清除计划的或处于活动状态的作业。

7 在**清除固件更新作业**对话框中，选择**早于**，然后单击**应用**。

然后，所选作业会从队列中清除。

事件、警报和运行状况监测

硬件管理的目标是提供系统运行状况和最新的基础架构信息，管理员需要这些信息以便在不离开 OMIVV 插件或 vCenter 的情况下，对严重硬件事件作出响应。

通过在 vCenter 中的机箱配置文件**任务**和**事件**选项卡上显示硬件（服务器和存储）和虚拟化相关的事件，数据中心和主机系统监测让管理员得以监测基础架构的运行状况。此外，严重硬件警报可以触发 OpenManage Integration for VMware vCenter 警报，为 Dell 虚拟化相关事件定义的少量警报可使受管主机系统进入维护模式。

要从服务器接收事件，OMIVV 配置为所有受监测设备上的陷阱目标，各种目标如下所示：

- 对于第 12 代及之后的主机，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。
- 对于机箱，陷阱目标在 CMC 中设置。

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。

要监测，请执行以下操作：

- 配置**事件和警报**设置。
- 必要时配置 SNMP OMSA 陷阱目标。
- 使用 vCenter 中的**任务**和**事件**选项卡查看事件信息。

主题：

- [关于主机的事件和警报](#)
- [About events and alarms for chassis](#)
- [与虚拟化相关的事件](#)
- [主动式高可用性事件](#)
- [查看警报和事件设置](#)
- [查看事件](#)
- [硬件组件冗余运行状况 — 主动式高可用性](#)
- [启动管理控制台](#)

关于主机的事件和警报

您可以在 OpenManage Integration for VMware vCenter 的**管理 > 设置**选项卡中编辑事件和警报。在该选项卡中，您可以选择事件发布级别、启用 Dell EMC 主机警报或恢复默认警报。您可以为每个 vCenter 配置事件和警报，或一次为所有已注册的 vCenter 配置事件和警报。

以下是四种事件发布级别：

表. 25: 事件发布级别

事件	说明
不发布任何事件	不允许 OpenManage Integration for VMware vCenter 向相关 vCenter 转发任何事件或警报。
发布所有事件	向相关 vCenter 发布所有事件（包括非正式的事件），OpenManage Integration for VMware vCenter 从受管 Dell EMC 主机接收这些事件。
仅发布严重和警告事件	仅将具有严重或警告危急程度的事件发布到相关的 vCenter。
仅发布虚拟化相关的严重和警告事件	将从主机收到的虚拟化相关事件发布到相关的 vCenter。虚拟化相关事件是 Dell 确定为对运行虚拟机的主机最严重的事件。

当您配置事件和警报时，可以启用它们。启用后，严重硬件警报可触发 OMIVV 设备将主机系统置于维护模式，并且在某些情况下，将虚拟机迁移到另一个主机系统。OpenManage Integration for VMware vCenter 会转发从管理的 Dell EMC 主机收到的事件，并创建这些事件的警报。使用这些警报可触发来自 vCenter 的操作，如重新引导、维护模式或迁移。

例如，当双电源设备发生故障并且创建警报后，导致的操作会让该机器进入维护模式，从而导致工作负载迁移到群集中的另一台主机上。

不在群集中，或在未启用 VMware 分布式资源调度 (DRS) 的群集中的所有主机，均可看到虚拟机由于严重事件而关闭。DRS 会持续监控跨资源池的使用并在虚拟机之间根据业务需求智能分配可用的资源。为确保虚拟机在发生严重硬件事件时自动迁移，请使用已配置 DRS 的群集与 Dell EMC 警报。详细的屏幕消息中列出此 vCenter 实例上可能会受影响的所有群集。请确认群集受影响后再启用事件和警报。

如果必须还原默认警报设置，您可使用**重设默认警报**按钮完成此操作。此按钮可以方便地还原默认警报配置而无需卸载和重新安装产品。如果有任何 Dell EMC 警报配置在安装后更改，则这些更改可使用此按钮恢复。

① **注:** 要接收 Dell 事件，请确保启用这些事件。

① **注:** OpenManage Integration for VMware vCenter 会预先选择对主机成功运行虚拟机来说至关重要的虚拟化相关事件。默认情况下，Dell 主机警报处于禁用状态。如果启用了 Dell 警报，群集应使用 DRS 确保发送严重事件的虚拟机自动迁移。

About events and alarms for chassis

The events and alarms corresponding to a chassis are shown only at the vCenter level. The events and alarms settings for hosts at every vCenter is also applicable at the chassis level. You can edit events and alarms settings from OpenManage Integration for VMware vCenter within the **Manage > Settings** tab. From here, you can select the event posting level, enable alarms for Dell EMC hosts and chassis, or restore default alarms. You can configure events and alarms for each vCenter or for all registered vCenters at once.

Viewing chassis events

- 1 In the left pane, select vCenter, and click the vCenter servers.
- 2 Click a specific vCenter.
- 3 Click the **Monitor > Events** tab.
- 4 To view more event details, select a specific event.

Viewing chassis alarms

- 1 In the left pane, select vCenter, and click the vCenter servers.
- 2 Click a specific vCenter.
The alarms are displayed. Only the first four alarms are displayed.

3 To view the complete list, click **Show All** to view the detailed list in the **Monitor** tab as **All Issues**.

4 In **Triggered Alarms**, click **Alarm** to view the alarm definition.

与虚拟化相关的事件

下表包含与虚拟化相关的严重和警告事件，并包括事件名称、说明、严重性级别和建议的操作。

表. 26: 虚拟化事件

事件名称	说明	严重性	建议操作
Dell-Current sensor detected a warning value	指定系统中的电流传感器超过警告阈值	警告	无操作
Dell-Current sensor detected a failure value	指定系统中的电流传感器超过故障阈值	错误	使系统进入维护模式
Dell-Current sensor detected a non-recoverable value	指定系统中的电流传感器检测到无法恢复的错误	错误	无操作
Dell-Redundancy regained	传感器已恢复正常值	信息	无操作
Dell-Redundancy degraded	指定系统中的冗余传感器检测到其中一个冗余装置组件发生故障，但该装置仍为冗余	警告	无操作
Dell - 冗余丢失	指定系统中的冗余传感器检测到其中一个冗余装置组件已经断开连接、发生故障或不存在	错误	使系统进入维护模式
Dell - 电源装置恢复正常	传感器已恢复正常值	信息	无操作
Dell - 电源装置检测到警告	指定系统中电源传感器的读数超过用户可定义警告阈值	警告	无操作
Dell - 电源装置检测到故障	电源设备已断开连接或失败。	错误	使系统进入维护模式
Dell - 电源装置传感器检测到不可恢复的值	指定系统中的电源传感器检测到无法恢复的错误。	错误	无操作
Dell - 内存设备状态警告	内存设备纠错率超过可接受值。	警告	无操作
Dell - 内存设备错误	内存设备纠错率超过可接受值，内存备用槽已激活或出现多位 ECC 错误。	错误	使系统进入维护模式
Dell - 风扇扩展柜插入到系统中	传感器已恢复正常值。	信息	无操作
Dell - 风扇扩展柜从系统中卸下	风扇罩已从指定系统中卸下。	警告	无操作
Dell - 风扇扩展柜从系统中卸下很长一段时间	风扇罩从指定系统中卸下已持续用户可定义的一段时间。	错误	无操作
Dell - 风扇扩展柜传感器检测到不可恢复的值	指定系统中的风扇罩传感器检测到无法恢复的错误。	错误	无操作
Dell - 交流电源已恢复	传感器已恢复正常值	信息	无操作
Dell - 交流电源中断警告	交流电源线已断电，但有足够的冗余将其分类为警告。	警告	无操作
Dell - 交流电源线已断电	交流电源线已断电，并且由于缺乏冗余，需将其分类为错误	错误	无操作

事件名称	说明	严重性	建议操作
Dell - 处理器传感器已恢复到正常值	传感器已恢复正常值	信息	无操作
Dell - 处理器传感器检测到警告值	指定系统中的处理器传感器处于限制状态	警告	无操作
Dell - 处理器传感器检测到故障值	指定系统中的处理器传感器已被禁用、有配置错误，或发生热断路	错误	无操作
Dell - 处理器传感器检测到不可恢复的值	指定系统中的处理器传感器发生故障。	错误	无操作
Dell - 设备配置错误	在指定系统中的可插拔设备上检测到配置错误	错误	无操作
Dell - 电池传感器已恢复到正常值	传感器已恢复正常值	信息	无操作
Dell - 电池传感器检测到警告值	指定系统中的电池传感器检测到电池处于潜在故障状态	警告	无操作
Dell - 电池传感器检测到故障值	指定系统中的电池传感器检测到电池发生故障	错误	无操作
Dell - 电池传感器检测到不可恢复的值	指定系统中的电池传感器检测到电池发生故障	错误	无操作
Dell - 热关机保护已启动	当系统被配置为发生错误事件即热关闭时，生成此消息。如果温度传感器读数超过为系统配置的错误阈值，则操作系统会关闭，系统关机。当风扇罩长时间从系统中卸下时，在指定系统中也会发生此事件。	错误	无操作
Dell - 温度传感器已恢复到正常值	传感器已恢复正常值	信息	无操作
Dell - 温度传感器检测到警告值	背板、系统板、CPU 或指定系统驱动器架上的温度传感器超过警告阈值	警告	无操作
Dell - 温度传感器检测到故障值	背板、系统板、CPU 或指定系统驱动器架上的温度传感器超过故障阈值	错误	使系统进入维护模式
Dell - 温度传感器检测到不可恢复的值	背板、系统板或指定系统驱动器架上的温度传感器检测到无法恢复的错误	错误	无操作
Dell - 风扇传感器已恢复到正常值	传感器已恢复正常值	信息	无操作
Dell - 风扇传感器检测到警告值	主机 <x> 上的风扇传感器读数超过警告阈值	警告	无操作
Dell - 风扇传感器检测到故障值	指定系统中的风扇传感器检测到一个或多个风扇故障	错误	使系统进入维护模式
Dell - 风扇传感器检测到不可恢复的值	风扇传感器检测到无法恢复的错误	错误	无操作
Dell - 电压传感器已恢复到正常值	传感器已恢复正常值	信息	无操作

事件名称	说明	严重性	建议操作
Dell - 电压传感器检测到警告值	指定系统中的电压传感器超过警告阈值	警告	无操作
Dell - 电压传感器检测到故障值	指定系统中的电压传感器超过故障阈值	错误	使系统进入维护模式
Dell - 电压传感器检测到不可恢复的值	指定系统中的电压传感器检测到无法恢复的错误	错误	无操作
Dell - 电流传感器已恢复到正常值	传感器已恢复正常值	信息	无操作
Dell - 存储：存储管理错误	存储管理检测到设备独立错误情况	错误	使系统进入维护模式
Dell - 存储：控制器警告	物理磁盘的一部分已损坏	警告	无操作
Dell - 存储：控制器故障	物理磁盘的一部分已损坏	错误	使系统进入维护模式
Dell - 存储：信道故障	信道故障	错误	使系统进入维护模式
Dell - 存储：扩展柜硬件信息	机柜硬件信息	信息	无操作
Dell - 存储：扩展柜硬件警告	机柜硬件警告	警告	无操作
Dell - 存储：扩展柜硬件故障	机柜硬件错误	错误	使系统进入维护模式
Dell - 存储：阵列磁盘故障	阵列磁盘故障	错误	使系统进入维护模式
Dell - 存储：EMM 故障	EMM 故障	错误	使系统进入维护模式
Dell - 存储：电源装置故障	电源设备故障	错误	使系统进入维护模式
Dell - 存储：温度探测器警告	物理磁盘温度探测器警告，太冷或太热	警告	无操作
Dell - 存储：温度探测器故障	物理磁盘温度探测器错误，太冷或太热。	错误	使系统进入维护模式
Dell - 存储：风扇故障	风扇故障	错误	使系统进入维护模式
Dell - 存储：电池警告	电池警告	警告	无操作
Dell - 存储：虚拟磁盘降级警告	虚拟磁盘降级警告	警告	无操作
Dell - 存储：虚拟磁盘降级故障	虚拟磁盘降级故障	错误	使系统进入维护模式
Dell - 存储：温度探测器信息	温度探测器信息	信息	无操作
Dell - 存储：阵列磁盘警告	阵列磁盘警告	警告	无操作
Dell - 存储：阵列磁盘信息	阵列磁盘信息	信息	无操作
Dell - 存储：电源装置警告	电源设备警告	警告	无操作
Dell - Fluid 高速缓存磁盘故障	Fluid 高速缓存磁盘故障	错误	使系统进入维护模式
Dell - 高速缓存故障或严重事件	电缆故障或严重事件	错误	使系统进入维护模式
Dell - Chassis Management Controller 检测到警告	Chassis Management Controller 检测到警告	警告	无操作
Dell - Chassis Management Controller 检测到错误	Chassis Management Controller 检测到错误	错误	使系统进入维护模式
Dell - IO 虚拟化故障或严重事件	IO 虚拟化失败或严重事件	错误	使系统进入维护模式
Dell - 链接状态警告	链接状态警告	警告	无操作

事件名称	说明	严重性	建议操作
Dell - 链接状态故障或严重事件	链接状态故障或严重事件	错误	使系统进入维护模式
Dell - 安全警告	安全警告	警告	无操作
Dell - 系统：软件配置警告	系统：软件配置警告	警告	无操作
Dell - 系统：软件配置故障	系统：软件配置失败	错误	使系统进入维护模式
Dell - 存储安全警告	存储安全警告	警告	无操作
Dell - 存储安全故障或严重事件	存储安全性故障或严重事件	错误	使系统进入维护模式
Dell - 软件更改更新警告	软件更改更新警告	警告	无操作
Dell - Chassis Management Controller 审核警告	Chassis Management Controller 审核警告	警告	无操作
Dell - Chassis Management Controller 审核故障或严重事件	Chassis Management Controller 审核故障或严重事件	错误	使系统进入维护模式
Dell - PCI 设备审核警告	PCI 设备审核警告	警告	无操作
Dell 电源装置审核警告	电源设备审核警告	警告	无操作
Dell - 电源装置审核故障或严重事件	电源设备审核故障或严重事件	错误	使系统进入维护模式
Dell - 功率使用审核警告	电源使用情况审核警告	警告	无操作
Dell - 功率使用审核故障或严重事件	电源使用情况审核故障或严重事件	错误	使系统进入维护模式
Dell - 安全配置警告	安全配置警告	警告	无操作
Dell - 配置：软件配置警告	配置：软件配置警告	警告	无操作
Dell - 配置：软件配置故障	配置：软件配置失败	错误	使系统进入维护模式
Dell - 虚拟磁盘分区失败	虚拟磁盘分区失败	错误	使系统进入维护模式
Dell - 虚拟磁盘分区警告	虚拟磁盘分区警告	警告	无操作

IDRAC 事件

① 注：对于属于群集的启用主动式高可用性的所有主机，以下虚拟化事件映射到主动式高可用性事件；但不映射事件“风扇没有冗余”和“电源设备没有冗余”。

风扇有冗余	无	信息	无操作
风扇冗余丢失	一个或多个风扇发生故障或已卸下，或者发生需要附加风扇的配置更改。	严重	卸下并重新安装故障的风扇或安装其它风扇。
风扇冗余降级	一个或多个风扇发生故障或已卸下，或者发生需要附加风扇的配置更改。	警告	卸下并重新安装故障的风扇或安装其它风扇。
风扇没有冗余	一个或多个风扇发生故障或已卸下，或者发生需要附加风扇的配置更改。	信息	卸下并重新安装故障的风扇或安装其它风扇。
风扇没有冗余。资源不足以维持正常操作	一个或多个风扇发生故障或已卸下，或者发生需要附加风扇的配置更改。	严重	卸下并重新安装故障的风扇或安装其它风扇。
电源设备冗余	无	信息	无操作

事件名称	说明	严重性	建议操作
电源设备冗余丢失	由于电源设备异常、电源设备资源清册变更或系统电源资源清册变更，当前电源运行模式为非冗余。系统之前在电源冗余模式下工作	严重	检查事件日志排查电源设备故障。查看系统配置和功耗
电源设备冗余降级	由于电源设备异常、电源设备资源清册变更或系统电源资源清册变更，当前电源运行模式为非冗余。系统之前在电源冗余模式下工作	警告	检查事件日志排查电源设备故障。查看系统配置和功耗
电源设备没有冗余	当前电源设备配置不符合启用冗余的平台要求。如果电源设备发生故障，系统可能会关机。	信息	如果是意外导致，则查看系统配置和功耗并据此安装电源设备。检查电源设备状态排查故障
电源设备并非冗余。资源不足以维持正常操作	系统可能关闭或在性能降级的状态下运行。	严重	检查事件日志排查电源设备故障。查看系统配置和功耗，并据此升级或安装电源设备
内部双 SD 模块冗余	无	信息	无操作
内部双 SD 模块冗余丢失	任一 SD 卡或两个 SD 卡工作不正常。	严重	更换有故障的 SD 卡。
内部双 SD 模块冗余降级	任一 SD 卡或两个 SD 卡工作不正常。	警告	更换有故障的 SD 卡。
内部双 SD 模块非冗余	无	信息	安装额外的 SD 卡并配置冗余（如果需要冗余）。
机箱事件			
电源设备冗余丢失	由于电源设备异常、电源设备资源清册变更或系统电源资源清册变更，当前电源运行模式为非冗余。系统之前在电源冗余模式下工作	严重	检查事件日志排查电源设备故障。查看系统配置和功耗
电源设备冗余降级	由于电源设备异常、电源设备资源清册变更或系统电源资源清册变更，当前电源运行模式为非冗余。系统之前在电源冗余模式下工作	警告	检查事件日志排查电源设备故障。查看系统配置和功耗
电源设备冗余	无	信息	无操作
电源设备没有冗余	当前电源设备配置不符合启用冗余的平台要求。如果电源设备发生故障，系统可能会关机。	信息	如果是意外导致，则查看系统配置和功耗并据此安装电源设备。检查电源设备状态排查故障
电源设备并非冗余。资源不足以维持正常操作	系统可能关闭或在性能降级的状态下运行。	严重	检查事件日志排查电源设备故障。查看系统配置和功耗，并据此升级或安装电源设备
风扇冗余丢失	一个或多个风扇发生故障或已卸下，或者发生需要附加风扇的配置更改。	严重	卸下并重新安装故障的风扇或安装其它风扇。
风扇冗余降级	一个或多个风扇发生故障或已卸下，或者发生需要附加风扇的配置更改。	警告	卸下并重新安装故障的风扇或安装其它风扇。

事件名称	说明	严重性	建议操作
风扇有冗余	无	信息	无操作
风扇没有冗余	一个或多个风扇发生故障或已卸下，或者发生需要附加风扇的配置更改。	信息	卸下并重新安装故障的风扇或安装其它风扇。
风扇没有冗余。资源不足以维持正常操作	一个或多个风扇发生故障或已卸下，或者发生需要附加风扇的配置更改。	严重	卸下并重新安装故障的风扇或安装其它风扇。

主动式高可用性事件

根据主动式高可用性 VMware 支持的组件，以下事件由 Dell Inc 提供商在注册 vCenter 过程中进行注册。

① **注:** 受支持的组件的主动式高可用性运行状况可以是正常（绿色）、或警告（黄色）或严重（红色）、或未知（灰色）状态。

表. 27: Dell 主动式高可用性事件

Dell Inc 提供商事件	组件类型	说明
DellFanRedundancy	风扇	风扇冗余事件
DellPowerRedundancy	电源设备 (PSU)	电源冗余事件
DellIDSDMRedundancy	存储	IDSDM 冗余事件

对于主动式高可用性启用主机，以下陷阱由 OMIVV 用作触发器以确定组件的冗余运行状况。根据冗余运行状况信息，主动式高可用性运行状况更新可能会发送至主机的 vCenter。这些陷阱不是直接转发至主动式高可用性主机的 vCenter。

表. 28: 主动式高可用性事件

事件名称	说明	严重性
风扇信息	风扇信息	信息
风扇警告	风扇警告	警告
风扇故障	风扇故障	严重
电源设备正常	电源设备恢复正常	信息
电源设备警告	电源装置检测到警告	警告
电源设备故障	电源设备检测到故障	严重
电源设备不存在	电源设备缺失	严重
冗余信息	冗余信息	信息
已降级冗余	已降级冗余	警告
冗余丢失	冗余丢失	严重
集成的双 SD 模块信息	集成的双 SD 模块 (IDSDM) 信息	信息
集成的双 SD 模块警告	集成的双 SD 模块警告	警告
集成的双 SD 模块故障	集成的双 SD 模块故障	严重
集成的双 SD 模块不存在	集成的双 SD 模块不存在	严重
集成的双 SD 模块冗余信息	集成的双 SD 模块冗余信息	信息
集成的双 SD 模块冗余降级	集成的双 SD 模块冗余降级	警告

事件名称	说明	严重性
集成的双 SD 模块冗余丢失	集成的双 SD 模块冗余丢失	严重
机箱事件		
风扇信息	风扇信息	信息
风扇警告	风扇警告	警告
风扇故障	风扇故障	严重
电源设备正常	电源设备恢复正常	信息
电源设备警告	电源装置检测到警告	警告
电源设备故障	电源设备检测到故障	严重
冗余信息	冗余信息	信息
已降级冗余	已降级冗余	警告
冗余丢失	冗余丢失	严重

查看警报和事件设置

关于此任务

配置警报和事件后，您可以查看是否为主机启用了 vCenter 警报，以及在“设置”选项卡上选择的事件发布级别。

步骤

- 1 在 OpenManage Integration for VMware vCenter 中，从**管理 > 设置**选项卡的 **vCenter 设置**下，展开**事件和警报**。此时将显示以下详细信息：
 - Dell EMC 主机的 vCenter 警报 — 显示**已启用**或**已禁用**。
 - 事件发布级别。
- 2 配置事件和警报。请参阅[配置事件和警报](#)。

后续步骤

要查看事件发布级别，请参阅[关于事件和警报](#)。

查看事件

前提条件

确保先配置事件，然后才能在**事件**选项卡上查看事件。请参阅[配置事件和警报](#)。

关于此任务

在“事件”选项卡上查看主机、群集或数据中心的事件。

步骤

- 1 在 OpenManage Integration for VMware vCenter 的导航器中，单击**主机**、**数据中心**或**群集**。
- 2 在**对象**选项卡上，选择您要查看其事件的特定主机、数据中心或群集。
- 3 在**监测**选项卡上，单击**事件**。
- 4 要查看事件详细信息，请选择特定事件。

硬件组件冗余运行状况 — 主动式高可用性

① **注:** 只有支持受支持的组件（电源、风扇和 IDSDM）的冗余运行状况的服务器才可使用主动式高可用性功能。

① **注:** 通过 OMIVV 配置全局警报时，主动式高可用性群集上已配置的主动式高可用性策略可能会受到影响。

① **注:** 主动式高可用性仅在支持电源、风扇和 IDSDM 的平台上可用。

主动式高可用性是与 OMIVV 配合使用的 vCenter (vCenter 6.5 及更高版本) 功能。启用主动式高可用性时, 该功能可通过在主机中的冗余组件发生故障期间主动采取措施来保证工作负载正常执行。

① 注: PowerEdge 第 12 代及更新代次, 以及 ESXi 版本 6.0 及更高版本中属于连接配置文件的一部分并成功进行资源清册的所有主机都可使用主动式高可用性功能。

评估受支持的主机组件的冗余运行状况状态后, OMIVV 设备将运行状况更新为 vCenter 服务器。受支持的组件 (电源设备、风扇和 IDSDM) 的冗余运行状况状态是:

- 正常 (信息) — 组件正常运行。
- 警告 (中度降级) — 组件有非严重错误。
- 严重 (严重降级) — 组件有严重故障。

① 注: 中度降级和严重降级状态在事件页面的类型列中表示为警告。

① 注: 未知运行状况表示来自 Dell Inc 提供商的任何主动式高可用性运行状况更新不可用。在下列情况下, 未知运行状况可能会发生:

- 已添加至主动式高可用性群集的所有主机可能会在数分钟内一直处于未知状态, 直到 OMIVV 用合适的状态对其初始化。
- vCenter 服务器重启可能会将主动式高可用性群集中的主机至于未知状态, 直到 OMIVV 再次用合适的状态对其初始化。

当 OMIVV 检测到受支持的组件的冗余运行状况发生更改时 (通过陷阱或轮询生成), 该组件的运行状况更新通知将发送至 vCenter 服务器。轮询每小时运行一次, 并且可作为故障保护机制用于防止陷阱丢失的可能性。

配置机架式和塔式服务器的主动式高可用性

要配置机架式和塔式服务器, 请执行以下步骤:

前提条件

确保所有主机已正确配置所有三个受支持的冗余组件 (电源设备、风扇和 IDSDM) 的冗余。

步骤

- 1 创建连接配置文件和关联主机与连接配置文件。请参阅[创建连接配置文件](#)。
- 2 验证主机资源清册是否已成功完成。请参阅[查看主机资源清册](#)。
- 3 验证 iDRAC 中的 SNMP 陷阱目标设置为 OMIVV 设备 IP 地址。

① 注: 确保从 OpenManage Integration > 显示器 > 日志选项卡中, 用户操作日志会确认主动式高可用性群集的主机的可用性。

- 4 在群集上启用主动式高可用性。请参阅[在群集上启用主动式高可用性](#)。

配置模块化服务器的主动式高可用性

要配置模块化服务器, 请执行以下步骤:

前提条件

配置模块化服务器的主动式高可用性之前, 请确保满足以下条件:

- 所有主机已正确配置所有三个支持的冗余组件 (电源设备、风扇和 IDSDM) 的冗余。
- 已成功完成主机和机箱的资源清册。

关于此任务

① 注: 建议主动式高可用性群集中所有模块化主机不应位于同一机箱中, 因为机箱故障会影响其所有刀片服务器。

步骤

- 1 创建连接配置文件和关联主机与连接配置文件。请参阅[创建连接配置文件](#)。
- 2 验证主机资源清册是否已成功完成。请参阅[查看主机资源清册](#)。

① **注:** 确保从 **OpenManage Integration > 显示器 > 日志选项卡** 中，用户操作日志会确认主动式高可用性群集的主机的可用性。

- 3 创建与机箱关联的机箱配置文件。请参阅[创建机箱配置文件](#)。
- 4 验证是否已成功完成机箱资源清册。请参阅[查看机箱资源清册](#)。
- 5 启动 CMC 并验证机箱的陷阱目标是否已设置为 OMIVV 设备 IP 地址。
- 6 在**机箱管理控制器**中，请转至**设置 > 常规**。
- 7 在**常规机箱设置**页面中，选择**启用增强型机箱日志记录和事件**。
- 8 在群集上启用主动式高可用性。请参阅[在群集上启用主动式高可用性](#)。

启用群集的主动式高可用性

前提条件

在群集上启用主动式高可用性之前，请确保满足以下条件：

- 启用 DRS 的群集在 vCenter 控制台中创建和配置。要在群集上启用 DRS，请参阅 VMware 文档。
- 属于群集的所有主机都应是连接配置文件的一部分并已成功进行资源清册，并且在适用情况下，机箱应具有机箱配置文件。

步骤

- 1 在 OpenManage Integration 中，单击**群集**。
- 2 在**群集**下，单击群集，选择**配置 > vSphere 可用性**，然后单击**编辑**。
此时会显示**编辑群集设置**向导。
- 3 单击**vSphere DRS**并选择**开启 vSphere DRS**（如果尚未选择）。
- 4 单击**vSphere 可用性**并选择**开启主动式高可用性**（如果尚未选择）。
- 5 在左侧窗格中的**vSphere 高可用性**下，单击**主动式高可用性故障和响应**。
主动式高可用性故障和响应屏幕将显示。
- 6 在**主动式高可用性故障和响应**屏幕中，展开**自动化级别**。
- 7 对于**自动化级别**，选择**手动**或**自动**。
- 8 对于**修复**，根据严重性状态选择**隔离模式**、**维护模式**或**隔离和维护模式（混合模式）**的组合。有关更多信息，请参阅 VMware 文档。
- 9 对于**主动式高可用性提供程序**，请使用复选框以选择群集的 Dell 提供程序。
- 10 针对所选 Dell 提供程序单击**编辑**。
此时将显示主动式高可用性提供程序的**编辑被阻止的故障条件**对话框。
- 11 要阻止故障条件发布事件，请从**故障条件**表中使用复选框来选择事件（通过陷阱或轮询生成）。
您可以使用**筛选器**字段筛选故障条件数据网格的内容，或者在故障条件数据网格中拖放列。故障条件可以在群集级别或主机级别应用。
- 12 要在群集中的所有当前和将来主机上应用，请中**群集级别**复选框。
- 13 要应用更改，请在**编辑被阻止的故障条件**中，单击**确定**，或者要取消，请单击**取消**。
- 14 要保存更改，请在**编辑群集设置**向导中，单击**确定**，或者要取消，请单击**取消**。

后续步骤

在群集上启用主动式高可用性后，OMIVV 扫描群集中所有主机并初始化所有支持的主机服务器组件的主动式高可用性运行状况。OMIVV 现在可以将支持的组件的运行状况更新通知发送至 vCenter 服务器。根据 OMIVV 的运行状况更新通知，vCenter 服务器会执行为**修复**选择的手动或自动操作。

要覆盖现有的严重性，请参阅[覆盖运行状况更新通知的严重性](#)。

覆盖运行状况更新通知的严重性

您可以配置用适合您环境的自定义严重性来覆盖 Dell EMC 主机及其组件的 Dell 主动式高可用性事件现有的严重性。

关于此任务

以下是应用至每件主动式高可用性事件的严重性级别：

- 信息
- 中度降级
- 严重降级

注：您不能使用信息严重性级别自定义主动式高可用性组件的严重性。

步骤

- 1 在 OpenManage Integration for VMware vCenter 的**管理**选项卡中，单击**主动式高可用性配置 > 主动式高可用性事件**。
- 2 单击以查看有关支持的事件列表中的信息。
数据网格显示所有受支持的主动式高可用性事件，并包括用于自定义主机及其组件严重性的列、事件 ID、事件说明、组件类型、默认严重性和覆盖严重性。
- 3 要更改主机及其组件的严重性，在**覆盖严重性**列中，从下拉列表中选择所需状态。
此策略应用于所有注册了 OMIVV 的 vCenter 服务器中所有主动式高可用性主机。
- 4 对必须自定义的所有事件重复步骤 3。
- 5 执行下面的任意一项操作：
 - a 要保存自定义，请单击**应用更改**。
 - b 要在选择严重性级别后恢复覆盖的严重性，请单击**取消**。
 - c 要对覆盖的严重性应用默认严重性，请单击**重设为默认值**。

启动管理控制台

可以从 Dell EMC Server Management Portlet 启动三个管理控制台。它们包括：

- 要访问 iDRAC 用户界面，请启动 Remote Access Console。请参阅[启动 Remote Access Console \(iDRAC\)](#)。
- 要访问 OpenManage Server Administrator 用户界面，请启动 OMSA 控制台。启动 OMSA 控制台之前，应在 Open Management Integration for VMware vCenter 中配置 OMSA URL。请参阅[启动 OMSA 控制台](#)。
- 要访问机箱用户界面，请单击刀片机箱控制台。请参阅[启动 Chassis Management Controller 控制台 \(CMC\)](#)。

注：如果您在刀片系统上，请启动 CMC 控制台以启动机箱管理控制器用户界面。如果您在刀片系统上，请启动 CMC 控制台以启动机箱管理控制器用户界面。

启动远程访问控制台 (iDRAC)

关于此任务

您可以从 Dell EMC Server Management Portlet 启动 iDRAC 用户界面。

步骤

- 1 在 OpenManage Integration for VMware vCenter 中的导航器区域中，在“资源清册列表”下，单击**主机**。
- 2 在**对象**选项卡上，双击所需的主机。
- 3 在**摘要**选项卡上，向下滚动到 Dell EMC Server Management Portlet。
- 4 单击**管理控制台 > 远程访问控制台 (iDRAC)**。

启动 OMSA 控制台

关于此任务

启动 OMSA 控制台之前，请确保设置 OMSA URL 并安装和配置 OMSA Web 服务器。您可以在**设置**选项卡中设置 OMSA URL。

① | 注: 请使用 **OpenManage Integration for VMware vCenter** 安装 OMSA 以监测和管理 PowerEdge 第 11 代服务器。

步骤

- 1 在 OpenManage Integration for VMware vCenter 中的导航器区域中，在“资源清册列表”下，单击**主机**。
- 2 在**对象**选项卡中，双击所需的主机。
- 3 在**摘要**选项卡中，向下滚动至 **Dell EMC 主机信息**。
- 4 在 **Dell EMC 主机信息**部分，单击 **OMSA 控制台**。

启动 Chassis Management Controller 控制台 (CMC)

关于此任务

可以从 Dell EMC Server Management Portlet 启动机箱用户界面。

步骤

- 1 在 OpenManage Integration for VMware vCenter 中的导航器区域中，在“资源清册列表”下，单击**主机**。
- 2 在**对象**选项卡中，双击您所需的刀片服务器。
- 3 在**摘要**选项卡中，向下滚动到 Dell EMC Server Management Portlet。
- 4 单击**管理控制台** > **Chassis Management Controller 控制台 (CMC)**。

机箱管理

OMIVV 允许您查看与模块化服务器关联的机箱的其他信息。在机箱信息选项卡中，您可以查看单个机箱的机箱概览详细信息，关于硬件资源清册、固件和管理控制器的信息、单个机箱组件的运行状况以及机箱保修信息。为每个机箱显示如下三个选项卡，并且不同机箱型号之间存在差异：

- “摘要”选项卡
- “监测”选项卡
- “管理”选项卡

① **注：**要查看所有信息，请确保机箱与机箱配置文件相关联，并成功完成机箱资源清册。请参阅[关于机箱配置文件的更多信息](#)。

主题：

- [查看机箱摘要详细信息](#)
- [查看机箱的硬件资源清册信息](#)
- [查看机箱的其他硬件配置](#)
- [查看机箱的关联主机](#)

查看机箱摘要详细信息

您可以在机箱摘要页面中查看单个机箱的机箱摘要详细信息。

- 1 在主页页面中，单击 **vCenter**。
- 2 在左侧窗格中，在 **OpenManage Integration** 下，单击 **Dell EMC 机箱**。
- 3 在左侧窗格中，选择相应的机箱 IP。
- 4 单击**摘要**选项卡。

此时会显示有关所选机箱的以下信息：

- 名称
- 型号
- 固件版本
- 服务标签
- CMC

① **注：**如果单击 **CMC** 链接，将显示 **Chassis Management Controller** 页面。

① **注：**如果未对机箱进行资源清册作业，则只能看到服务标签以及 CMC IP 地址。

- 5 查看与所选机箱关联的设备的运行状况。

主窗格显示机箱的总体运行状况。有效的运行状况标志包括**正常**、**警告**、**严重**和**不存在**。在**机箱运行状况**网格视图中，显示每个组件的运行状况。机箱运行状况参数适用于型号 VRTX 版本 1.0 及更高版本、M1000e 版本 4.4 及更高版本。对于低于 4.3 的版本，只显示两种运行状况标志，例如正常和警告或严重（带橙色感叹号的倒三角）。

① **注：**总体运行状况基于具有最差运行状况参数的机箱来指示运行状况。例如，如果有 5 个正常标志和 1 个警告标志，则总体运行状况显示为**警告**。

- 6 查看机箱的 **CMC Enterprise** 或 **Express** 以及许可证类型和过期日期。

上述详细信息不适用于 M1000e 机箱。

- 单击**保修**图标并查看剩余天数和已用于主机的天数。
如果您有多份保修，则使用最后一份保修的最后一天来计算保修剩余天数。
- 在机箱的**活动错误**表列表中查看错误，这些列表显示在**机箱运行状况**页面中。

① **注:** 对于 M1000e 版本 4.3 及更早版本，不会显示活动错误。

查看机箱的硬件资源清册信息

您可以查看有关所选机箱中硬件资源清册的信息。要在此页面中查看信息，请确保运行资源清册作业并导出含有组件信息的 CSV 文件。

- 在主页页面中，单击 **vCenter**。
- 在左侧窗格中，在 **OpenManage Integration** 下，单击 **Dell EMC 机箱**。
- 在左侧窗格中，选择相应的机箱 IP。
- 单击 **Monitor (监测)** 选项卡。

要查看相关组件信息，请通过 OMIVV 导航：

表. 29: 硬件资源清册信息

硬件资源清册：组件	通过 OMIVV 导航	信息
风扇	使用以下任一方法： <ul style="list-style-type: none"> 在概览选项卡中，单击风扇。 在监测选项卡中，展开左侧窗格，单击硬件资源清册，然后单击风扇。 	有关风扇的信息： <ul style="list-style-type: none"> 名称 存在 电源状态 读数 警告阈值 严重阈值 <ul style="list-style-type: none"> 最低 最高
电源设备	使用以下任一方法： <ul style="list-style-type: none"> 在概览选项卡中，单击电源设备。 在监测选项卡中，展开左侧窗格，单击硬件资源清册，然后单击电源设备。 	有关电源设备的信息： <ul style="list-style-type: none"> 名称 容量 存在 电源状态
温度传感器	使用以下任一方法： <ul style="list-style-type: none"> 在概览选项卡中，单击温度传感器。 在监测选项卡中，展开左侧窗格，单击硬件资源清册，然后单击温度传感器。 	有关温度传感器的信息： <ul style="list-style-type: none"> 位置 读数 警告阈值 <ul style="list-style-type: none"> 最高 最低 严重阈值 <ul style="list-style-type: none"> 最高 最低

硬件资源清册： 组件	通过 OMIVV 导航	信息
		<p>i 注: 对于 PowerEdge M1000e 机箱，仅会显示机箱的温度传感器的信息。对于其他型号的机箱，则会显示机箱和关联的模块化服务器的温度传感器信息。</p>
I/O 模块	<p>使用以下任一方法：</p> <ul style="list-style-type: none"> 在概览选项卡中，单击 I/O 模块。 在监测选项卡中，展开左侧窗格，单击硬件资源清册，然后单击 I/O 模块。 	<p>有关 I/O 模块的信息：</p> <ul style="list-style-type: none"> 插槽/位置 存在 名称 结构 服务标签 电源状态 <p>要查看附加的信息，请选择相应的 I/O 模块，即会显示以下信息：</p> <ul style="list-style-type: none"> Role（角色） 固件版本 硬件版本 IP 地址 子网掩码 网关 MAC 地址 DHCP 已启用
PCIe	<p>使用以下任一方法：</p> <ul style="list-style-type: none"> 在概览选项卡中，单击 PCIe。 在监测选项卡中，展开左侧窗格，单击硬件资源清册，然后单击 PCIe。 	<p>有关 PCIe 的信息：</p> <ul style="list-style-type: none"> PCIe 插槽 <ul style="list-style-type: none"> 插槽 名称 电源状态 结构 服务器插槽 <ul style="list-style-type: none"> 名称 编号 <p>要查看附加的信息，请选择相应的 PCIe，即会显示以下信息：</p> <ul style="list-style-type: none"> 插槽类型 服务器映射 分配状态 分配的插槽电源 PCI ID 厂商 ID <p>i 注: PCIe 信息不适用于 M1000e 机箱。</p>
iKVM	<p>使用以下任一方法：</p> <ul style="list-style-type: none"> 在概览选项卡中，单击 iKVM。 在监测选项卡中，展开左侧窗格，单击硬件资源清册，然后单击 iKVM。 	<p>有关 iKVM 的信息：</p> <ul style="list-style-type: none"> iKVM 名称 存在 固件版本 前面板 USB/视频已启用

硬件资源清册： 组件	通过 OMIVV 导航	信息
		<ul style="list-style-type: none"> 允许访问 CMC CLI <p>i 注: 只能查看有关 PowerEdge M1000e 机箱的 iKVM 的信息。</p> <p>i 注: 仅当机箱包含 iKVM 模块时, 才会显示 iKVM 选项卡。</p>

查看机箱的其他硬件配置

您可以查看有关所选机箱中的保修、存储、固件和管理控制器的信息。要在此页面中查看信息, 请确保运行资源清册作业并导出含有组件信息的 CSV 文件。

关于此任务

要查看机箱的保修、存储、固件和管理控制器详细信息, 请执行以下步骤:

步骤

- 1 在主页页面中, 单击 **vCenter**。
- 2 在左侧窗格中, 在 **OpenManage Integration** 下, 单击 **Dell EMC 机箱**。
- 3 在左侧窗格中, 选择相应的机箱 IP。
- 4 单击 **监测** 选项卡。

要查看保修、存储、固件和管理控制器的信息, 请通过 OMIVV 导航。

表. 30: 固件详细信息

硬件配置	通过 OMIVV 导航	信息
固件	<ol style="list-style-type: none"> a 在 监测 选项卡中, 单击双箭头标记并展开左侧窗格, 然后单击 固件。 b 在 监测 选项卡中, 如果您单击 启动 CMC, 则会显示 Chassis Management Controller 页面。 	有关固件的信息: <ul style="list-style-type: none"> 组件 当前版本

表. 31: 管理控制器详细信息

硬件配置	通过 OMIVV 导航	信息
管理控制器	<ol style="list-style-type: none"> a 在 监测 选项卡中, 单击双箭头标记并展开左侧窗格, 然后单击 管理控制器。 b 在 管理控制器 页面中, 要查看其他信息, 可单击箭头标记并展开左侧列。 	有关管理控制器的信息: <ul style="list-style-type: none"> 常规 <ul style="list-style-type: none"> 名称 固件版本 上次更新时间 CMC 位置 硬件版本 公用网络 <ul style="list-style-type: none"> DNS 域名 为 DNS 使用 DHCP MAC 地址 冗余模式 CMC IPv4 信息 <ul style="list-style-type: none"> IPv4 已启用

硬件配置	通过 OMIVV 导航	信息
		<ul style="list-style-type: none"> • DHCP 已启用 • IP 地址 • 子网掩码 • 网关 • 首选 DNS 服务器 • 备用 DNS 服务器

表. 32: 存储信息

硬件配置	通过 OMIVV 导航	信息
存储时	在 监测 选项卡上，单击 存储 。	<p>有关存储的信息：</p> <ul style="list-style-type: none"> • 虚拟磁盘 • 控制器 • 机柜 • 物理磁盘 • 热备盘 <p>注：当您单击存储下高亮显示的链接时，视图表会显示每个高亮显示项目的详细信息。在视图表中，如果单击每个行项目，则会显示每个高亮显示项目的附加信息。</p> <p>对于 M1000e 机箱，如果您有存储模块，则在网格视图中显示以下存储详细信息，而不含任何附加信息：</p> <ul style="list-style-type: none"> • 名称 • 型号 • 服务标签 • IP 地址（链接至存储设备） • 结构 • Group Name（组名称） • 组 IP 地址（链接至存储组）

表. 33: 保修信息

硬件配置	通过 OMIVV 导航	信息
保修	在 监测 选项卡上，单击 保修 。	<p>有关保修的信息：</p> <ul style="list-style-type: none"> • 提供商 • 说明 • 状态 • 开始日期 • 结束日期 • 剩余天数 • 上次更新 <p>注：要查看保修状态，请确保您运行保修作业。请参阅运行保修检索作业。</p>

查看机箱的关联主机

您可以在**管理**选项卡上查看所选机箱关联的主机的相关信息。

- 1 在**主页**页面中，单击 **vCenter**。
- 2 在左侧窗格中，在 **OpenManage Integration** 下，单击 **Dell EMC 机箱**。
- 3 在左侧窗格中，选择相应的机箱 IP。
- 4 单击**管理**选项卡。

此时会显示以下关于关联主机的信息：

- 主机名（如果您单击选定的主机 IP，则会显示关于该主机的详细信息。）
- 服务标签
- 型号
- iDRAC IP
- 插槽位置
- 上次资源清册

部署虚拟机监控程序

OMIVV 允许您在受支持的裸机服务器中配置以下组件，同时部署虚拟机监控程序并将其添加到 vCenter 中指定的数据中心和群集。

- 引导顺序设置
- RAID 配置
- BIOS 配置
- iDRAC 配置

您只需使用 VMware vCenter，不需要 PXE，就可以在 PowerEdge 裸机服务器上创建硬件配置文件、系统配置文件和虚拟机监控程序配置文件。

① 注: 部署虚拟机监控程序时，建议使用第 14 代及更新服务器的系统配置文件。

要配置硬件并执行部署，请确保在部署向导中显示物理服务器。确保所有物理服务器都满足以下要求：

- 满足在 *OpenManage Integration for VMware vCenter 兼容性值表* 中提供的具体硬件支持信息。
- 满足支持的最低版本的 iDRAC 固件、Lifecycle Controller 和 BIOS。有关具体的固件支持信息，请参阅 *OpenManage Integration for VMware vCenter 支持值表*。
- 在部署之后，手动配置 PCI 插槽中的 NIC。如果您使用的是扩展 NIC，则系统必须在主板 (LOM) 或网络子卡 (NDC) 上启用主机 LAN 并连接至网络。OMIVV 支持仅使用嵌入式/集成 LOM 进行部署。
- 满足 IDSDM 的存储规格。要了解 IDSDM 的存储规格，请参阅 VMware 文档。请确保先从 BIOS 启用 IDSDM，然后才能使用 OMIVV 部署虚拟机监控程序。OMIVV 允许在 IDSDM 或本地硬盘驱动器上进行部署。
- 如果 vCenter 和 iDRAC 连接到不同的网络，请确保 vCenter 和 iDRAC 网络之间存在路由。
- 请确保已启用重新引导时收集系统资源清册 (CSIOR)。另外，在启动自动/手动查找之前，请确保检索到的数据是最新的，检索方法是完全关闭系统，然后打开系统（硬重新引导）。
- 单击订购由工厂预先配置了自动查找和握手选项的 Dell 服务器。如果服务器没有预先配置这些选项，请手动输入 OMIVV 的 IP 地址，或者配置您的本地网络以提供此信息。
- 如果 OMIVV 未用于硬件配置，请确保启动虚拟机监控程序部署之前满足以下条件：
 - 在 BIOS 中启用虚拟化技术 (VT) 标志。
 - 将系统的引导顺序设置为可引导的虚拟磁盘或 IDSDM，以进行操作系统安装。
- 要验证如果使用 OMIVV 进行硬件配置，则尽管 BIOS 配置不是硬件配置文件的一部分，BIOS 的 VT 设置也会自动启用。如果虚拟磁盘没有出现在目标系统上，则需要进行 Express/Clone RAID 配置。
- 请确保包含所有 Dell 驱动程序自定义 ESXi 映像可部署。您可以从 support.dell.com 中找到正确的映像，方法是导航至 **Dell 驱动程序和下载** 页面，并将自定义映像保存到部署过程中 OMIVV 可以访问的 CIFS 或 NFS 共享位置。如需该版本支持的 ESXi 版本的最新列表，请参阅 *OpenManage Integration for VMware vCenter 兼容性值表*。要使用正确的映像，请参阅 [下载自定义 Dell ISO 映像](#)。
- 请确保在将虚拟机监控程序配置文件作为仅支持 BIOS 的 OMIVV 应用至目标服务器上的自动部署虚拟机监控程序之前，您已选择参考硬件配置文件中的 BIOS 模式。如果未选择硬件配置文件，请确保您手动配置引导模式为 BIOS 并在应用虚拟机监控程序配置文件之前重新引导服务器。

如果服务器来自早于 PowerEdge 第 12 代服务器的版本，则部署过程会执行以下任务：

- 在目标系统上安装 OMSA 软件包。
- 自动在 OMSA 中将 SNMP 陷阱目标配置为指向 OMIVV。

主题：

- 设备查找
- 配置
- 配置硬件配置文件
- 创建虚拟机监控程序配置文件
- 创建部署模板
- 有关部署向导
- 部署作业时间
- 下载自定义 Dell EMC ISO 映像


设备查找

查找是添加受支持的 PowerEdge 裸机服务器的过程。查找到服务器后，您可以将它用于虚拟机监控程序和硬件部署。如需部署所需的 PowerEdge 服务器列表，请参阅 *OpenManage Integration for VMware vCenter 兼容性值表*。需要从 Dell EMC 裸机服务器的 iDRAC 到 OMIVV 虚拟机的网络连接。

- ① **注:** 现已包含虚拟机监控程序的主机不应被查找并添加到 OMIVV 中，而应将它们添加到 vCenter。将它们添加到连接配置文件，然后使用主机符合性向导与 *OpenManage Integration for VMware vCenter* 进行协调。
- ① **注:** 如果在早于 OMIVV 4.0 检测到裸机服务器，则请确保从裸机服务器列表中删除这些服务器，并重新检测它们。
- ① **注:** 在第 12 代 Poweredge 裸机服务器的 SD 卡上执行 OS 部署，请确保已安装 iDRAC 2.30.30.30 及更高版本。

手动查找

您可以手动添加查找过程未添加的裸机服务器。添加之后，该服务器会显示在部署向导中的服务器列表中。

- 1 在 OpenManage Integration for VMware vCenter 中的 **管理 > 部署** 选项卡上，单击  图标。此时将显示 **添加服务器** 对话框。
- 2 在 **添加服务器** 对话框中，执行以下操作：
 - a 在 **iDRAC IP 地址** 文本框中，输入 iDRAC IP 地址。
 - b 在 **用户名** 文本框中，输入用户名。
 - c 在 **密码** 文本框中，输入密码。
- 3 单击 **添加服务器**。
完成添加服务器任务可能需要几分钟的时间。

OpenManage Integration for VMware vCenter 中的自动查找

查找是添加 PowerEdge 裸机服务器的过程。查找到服务器后，将它用于虚拟机监控程序和硬件部署。自动查找是一项 iDRAC 功能，它消除了从 OMIVV 中手动查找裸机服务器的需要。

自动查找前提条件

在尝试查找 PowerEdge 裸机服务器之前，请确保已安装 OMIVV。包含 iDRAC Express 或 iDRAC Enterprise 的 PowerEdge 服务器可被找到并加入裸机服务器池中。确保 Dell EMC 裸机服务器的 iDRAC 与 OMIVV 设备之间存在网络连接。

- ① **注:** 具有现有虚拟机监控程序的主机不应被找到并加入 OMIVV 中，而是将虚拟机监控程序添加到连接配置文件中，然后使用“主机符合性向导”与 OMIVV 进行协调。

为了进行自动查找，必须满足以下条件：

- 电源 — 请确保您将服务器连接至电源插座。服务器不需要开机。
- 网络连接 — 确保服务器的 iDRAC 具有网络连接并且通过端口 4433 与配置服务器进行通信。您可以使用 DHCP 服务器获取 IP 地址，或在 iDRAC 配置公用程序中手动指定 IP 地址。
- 附加网络设置 — 如果使用 DHCP，确保启用“从 DHCP 获取 DNS 服务器地址”设置，以便解析 DNS 名称。
- 配置服务器位置 — 确保 iDRAC 知道配置服务服务器的 IP 地址或主机名。请参阅[配置服务位置](#)。
- 已禁用帐户访问 — 确保启用对 iDRAC 的管理帐户访问，并且如果存在任何具有管理员权限的 iDRAC 帐户，请首先在 iDRAC Web 控制台中禁用这些帐户。自动查找成功完成后，将重新启用管理 iDRAC 帐户。
- 已启用自动查找 — 确保服务器的 iDRAC 已启用自动查找，以便开始自动查找流程。

配置服务器位置

使用下列选项可在自动查找过程中由 iDRAC 获取配置服务位置：

- 在 iDRAC 中手动指定 — 在 iDRAC 配置公用程序中的“LAN 用户配置”、“配置服务器”下手动指定位置。
- DHCP 作用域选项 — 使用 DHCP 作用域选项指定位置。
- DNS 服务记录 — 使用 DNS 服务记录指定位置。
- DNS 已知名称 — DNS 服务器指定具有已知名称 DCIMCredentialServer 的服务器的 IP 地址。

如果未在 iDRAC 控制台中手动指定配置服务值，iDRAC 会尝试使用 DHCP 作用域选项值。如果 DHCP 作用域选项不存在，iDRAC 会尝试使用 DNS 中的服务记录值。

有关如何配置 DHCP 作用域选项和 DNS 服务记录的详细信息，请参阅 Dell 自动查找网络设置规范，网址为 http://en.community.dell.com/techcenter/extras/m/white_papers/20178466。

启用或禁用 iDRAC 上的管理帐户

在设置自动查找之前，必须禁用除根帐户以外的所有管理帐户。在自动查找过程中，根帐户应该处于禁用状态。在您成功设置自动查找后，返回到 iDRAC GUI 并重新启用根以外已关闭的管理帐户。

关于此任务

① 注：若要防止自动查找失败，可以启用 iDRAC 上的非管理帐户。非管理帐户允许在自动查找失败时进行远程访问。

步骤

- 1 在浏览器中，键入 iDRAC IP 地址。
- 2 登录到 **Integrated Dell Remote Access Controller GUI**。
- 3 请执行以下操作之一：
 - 对于 iDRAC6：在左侧窗格中，选择 **iDRAC 设置 > 网络/安全 > 用户** 选项卡。
 - 对于 iDRAC7：在左侧窗格中，选择 **iDRAC 设置 > 用户验证 > 用户** 选项卡。
 - 对于 iDRAC8：在左侧窗格中，选择 **iDRAC 设置 > 用户验证 > 用户** 选项卡。
- 4 在**用户**选项卡中，找到除根以外的任何管理帐户。
- 5 要禁用该帐户，请在“用户 ID”下，选择 **ID**。
- 6 单击**下一步**。
- 7 在**用户配置**页面的**常规**下，清除**启用用户**复选框。
- 8 单击**应用**。
- 9 要重新启用每个管理帐户，请在成功设置自动查找后重复步骤 1 至 8，但现在选中**启用用户**复选框，然后单击**应用**。

手动配置 PowerEdge 第 11 代服务器以进行自动查找

前提条件

确保您有 iDRAC 和主机 IP 地址。

关于此任务

如果您尚未从工厂订购裸机设备以使用自动查找，您可以手动进行设置。

一旦裸机服务器的自动查找取得成功，将创建新的管理员帐户，或使用握手服务返回的凭据启用现有帐户。将不会启用在自动查找之前禁用的所有其他管理帐户。在自动查找成功后，请重新启用这些管理员帐户。请参阅[启用或禁用 iDRAC 上的管理帐户](#)。

注：如果由于某些原因，自动查找未成功完成，将没有办法远程连接到 iDRAC。远程连接需要您已在 iDRAC 上启用了非管理帐户。如果 iDRAC 上没有已启用的非管理帐户，则访问 iDRAC 的唯一方法是在本地登录到此对话框，然后在 iDRAC 上启用该帐户。

步骤

- 1 在浏览器中输入 iDRAC IP 地址。
- 2 登录到 iDRAC Enterprise GUI。
- 3 在 **Integrated Dell Remote Access Controller 6 — Enterprise > 系统摘要** 选项卡的“虚拟控制台预览”中，单击**启动**。
- 4 在**警告 — 安全性**对话框中，单击**是**。
- 5 在 iDRAC 公用程序控制台中，按 **F12** 一或两次。
此时将显示**需要验证**对话框。
- 6 在**需要验证**对话框中，查看显示的名称，然后按 **Enter** 键。
- 7 输入密码。
- 8 按 **Enter** 键。
- 9 当显示**关机/重启**对话框时，按 **F11**。
- 10 主机将重新启动，屏幕显示有关正在加载内存和 RAID 的信息。然后，屏幕显示 iDRAC 并指示按 **CTRL + E** 时，请立即按 **CTRL + E**。

如果您看到下面的对话框，说明操作成功，否则，请转到“电源”菜单，关机然后开机，并且重复此步骤。

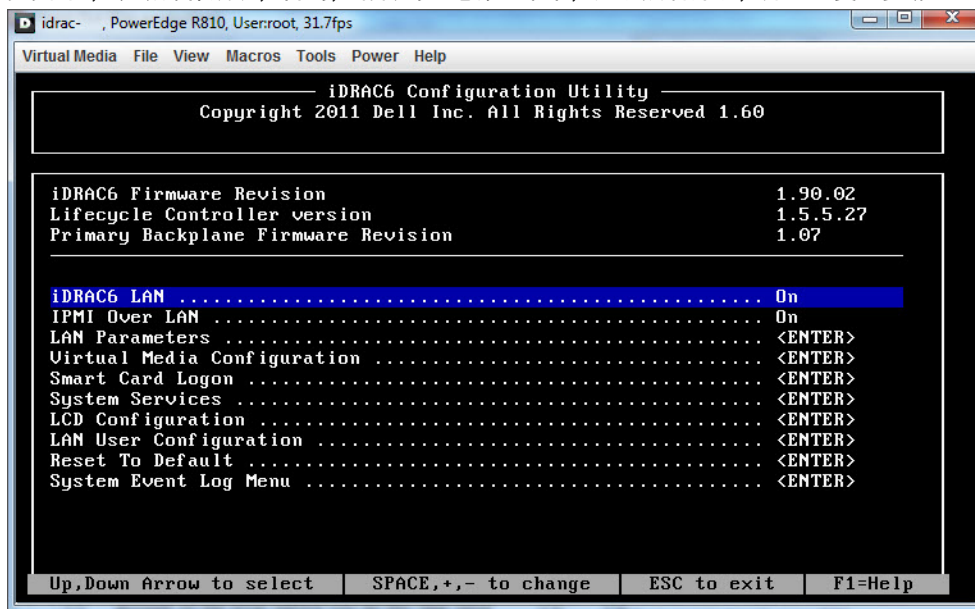


图 1: iDRAC 配置公用程序

- 11 在 iDRAC6 配置公用程序中，使用箭头键选择 **LAN 参数**。
- 12 按 **Enter** 键。
- 13 如果此主机为刀片，为了配置 NIC，请使用空格键将该选项切换到已启用。
- 14 如果您使用的是 DHCP，请使用箭头键选择从 **DHCP** 获取域名。
- 15 使用空格键将该选项切换到**开**。
- 16 如果您使用的是 DHCP，请使用箭头键导航到 IPv4 设置，然后选择从 **DHCP** 获取 DNS 服务器。
- 17 使用空格键将该选项切换到**开**。

- 18 若要退出，则在键盘上，按 **ESC** 键。
- 19 使用箭头键选择 **LAN 用户配置**。
- 20 使用箭头键选择 **配置服务器**。
- 21 按 **Enter** 键。
- 22 输入主机的 IP 地址。
- 23 按 **ESC** 键。
- 24 使用箭头键选择 **帐户访问**。
- 25 使用空格键将该选项切换到 **禁用**。
- 26 使用箭头键选择 **自动查找**。
- 27 使用空格键将该选项切换到 **已启用**。
- 28 从键盘中，按 **ESC** 键。
- 29 再次按 **ESC** 键。

手动配置 PowerEdge 第 12 代及更高版本服务器以进行自动查找

前提条件

确保您具有 iDRAC 地址。

关于此任务

从 Dell EMC 订购服务器时，您可以在提供配置服务器 IP 地址后要求在服务器上启用自动查找功能。配置服务器 IP 地址应是 OMIVV 的 IP 地址。因此，在收到 Dell 所提供的服务器后，当您安装并连接 iDRAC 电缆后，开启服务器电源时，服务器被自动查找，并列出现在“部署”向导的第一个页面中。

注：对于自动查找到的服务器，在管理 > 设置 > 部署凭据下提供的凭据设置为管理凭据，并用于与服务器进行进一步通信，直到操作系统部署完成。在操作系统成功部署后，设置在关联的连接配置文件中提供的 iDRAC 凭据。

要在目标机器上手动启用自动查找，请针对第 12 代及更高版本的服务器执行以下步骤：

步骤

- 1 要转到系统设置，请引导/重新引导目标系统，并在初始引导期间按 F2。
- 2 转至 **iDRAC 设置 > 用户配置** 并禁用根用户。当禁用根用户时，请确保该 iDRAC 地址上没有具有管理员权限的其他用户处于活动状态。
- 3 单击 **后退**，然后单击 **远程启用**。
- 4 将 **启用自动查找** 设置为 **启用**，并将 **配置服务器** 设置为 OMIVV 的 IP 地址。
- 5 保存设置。

在下次引导服务器时，自动查找服务器。在成功执行自动查找之后，根用户将启用，并且 **启用自动查找** 标志会自动禁用。

移除裸机服务器

您可以手动移除自动查找到的或手动添加的服务器。

- 1 在 OpenManage Integration for VMware vCenter 中，单击 **管理 > 部署** 选项卡。
- 2 在 **裸机服务器** 页面中，选择服务器，然后单击 **✗**。

配置

所有自动/手动查找到的符合要求的裸机系统均可供 OMIVV 用于进行硬件配置和虚拟机监控程序部署。要准备配置和部署，请执行以下操作：

表. 34: 准备部署

步骤	说明
创建系统配置文件	包含从第 14 代参考服务器搜集的系统配置设置，这些设置用于配置新服务器。
创建硬件配置文件	包含从参考服务器搜集的硬件设置，这些设置用于部署新服务器。请参阅 创建或自定义硬件配置文件 。 注: 建议使用第 13 代及更早期服务器的硬件配置文件。
创建虚拟机监控程序配置文件	包含 ESXi 部署所需的虚拟机监控程序安装信息。请参阅 创建虚拟机监控程序配置文件 。
创建部署模板	部署模板包含系统配置文件、硬件配置文件、虚拟机监控程序配置文件、系统配置文件和虚拟机监控程序配置文件的组合或者硬件配置文件和虚拟机监控程序配置文件的组合。您可以保存这些配置文件并根据需要将它们重复用于所有可用的数据中心服务器。

创建部署模板后，则使用部署向导搜集必要的信息，以创建在 vCenter 中配置服务器硬件并部署新主机的计划作业。有关运行部署向导的信息，请参阅[运行部署向导](#)。最后，通过作业队列查看作业状态，并对暂挂的部署作业进行更改。

配置硬件配置文件

要配置服务器硬件设置，请创建硬件配置文件。硬件配置文件是一种配置模板，可以将其应用到新查找到的基础架构组件，它需要以下信息：

表. 35: 创建硬件配置文件的要求

要求	说明
引导顺序	引导顺序是指引导设备序列和硬盘驱动器序列，仅当引导模式设置为 BIOS 时才能编辑该序列。
BIOS 设置	BIOS 设置包括：内存、处理器、SATA、集成设备、串行通信、嵌入式服务器管理、电源管理、系统安全以及杂项设置。 注: 无论参考服务器上的设置如何，OpenManage Integration for VMware vCenter 都会在所有部署的服务器上启用 BIOS 中的“处理器”组下的某些 BIOS 设置。在使用参考服务器创建新的硬件配置文件之前，它必须启用 CSIOR 设置，并进行重新引导以提供准确的资源清册和配置信息。
iDRAC 设置	iDRAC 设置包括网络、用户列表和用户配置。
RAID 配置	RAID 配置显示参考服务器上在提取硬件配置文件时的当前 RAID 拓扑。 注: 在硬件配置文件中配置了两个 RAID 配置选项： 1 应用 RAID1+ 创建专用热备用（如果适用）— 如果要为目标服务器应用默认 RAID 配置设置，则使用此选项。 2 从参考服务器克隆 RAID 配置 — 如果要克隆参考服务器设置，请使用此选项。请参阅 自定义参考服务器以创建硬件配置文件 。

创建硬件配置文件的任务包括：

- 在参考服务器上启用 CSIOR
- 自定义参考服务器以创建硬件配置文件
- 克隆硬件配置文件

在参考服务器上启用 CSIOR

前提条件

使用参考服务器创建硬件配置文件之前，启用重新引导时收集系统资源清册 (CSIOR) 设置并重新引导服务器以提供准确的资源清册和配置信息。

关于此任务

启用 CSIOR 有两种方法：

表. 36: 启用 CSIOR 的方法

方法	说明
本地	通过 Dell Lifecycle Controller United Server Configurator (USC) 用户界面使用单独的主机。
远程	使用 WS-Man 脚本。有关此功能脚本编写的详细信息，请参阅 <i>Dell TechCenter</i> (Dell 技术中心) 和 <i>DCIM Lifecycle Controller Management Profile</i> (DCIM Lifecycle Controller 管理配置文件)。

在参考服务器上本地启用 CSIOR：

步骤

- 1 打开系统，然后在自检期间按 **F2** 启动 USC。
- 2 选择**硬件配置 > 部件更换配置**。
- 3 启用 **主机重新引导时收集系统资源清册**设置，然后退出 USC。

创建或自定义硬件配置文件

步骤

- 1 在 OpenManage Integration for VMware vCenter 中，从**管理 > 部署**选项卡上，选择**部署模板 > 硬件配置文件**。
- 2 单击 **+** 图标。
- 3 在**硬件配置文件向导**中，在**欢迎**页面上单击**下一步**并执行以下操作：
 - 在**配置文件名称**文本框中，输入配置文件名称。
 - 在**说明**文本框中，键入说明。“说明”字段为可选项。
- 4 单击**下一步**。
此时将显示**参考服务器**对话框。您可以直接从该对话框中选择参考服务器，也可以通过“参考服务器”窗口中的“浏览”按钮选择参考服务器。
- 5 通过执行以下任一分步骤选择一个参考服务器：
 - 在**参考服务器**对话框中，选择所需的参考服务器，然后单击该参考服务器的**选择**链接。
此时将显示**提取确认**对话框，说明正在提取设置。要从参考服务器中提取硬件配置，请在**提取确认**对话框中，单击**是**，提取将在几分钟内完成。
 - 在**参考服务器**页面中，单击**浏览**以选择由 OMIVV 管理且已成功进行资源清册的符合要求的参考服务器，或者选择符合要求的裸机服务器。
要从参考服务器中提取硬件配置，请在**提取确认**对话框中，单击**是**。

所选服务器名称、iDRAC IP 地址、型号和服务标签将显示在**参考服务器**页面中。
- 6 在**参考服务器**页面中，要自定义参考服务器设置，请单击**自定义参考服务器设置**，然后选择可以选择性包括和自定义以下设置：
 - **RAID 设置**
 - **BIOS 设置**

- 引导顺序
 - iDRAC 设置
 - 网络设置
 - 用户列表
- 7 在 **RAID 配置** 窗口中，选择下列其中一项，然后单击**下一步**：
- **应用 RAID1 + 创建专用热备件（如果适用）** — 如果要为目标服务器应用默认 RAID 配置设置，则使用此选项。在支持 RAID1 的集成控制器的前两个驱动器上，RAID 配置任务默认为 RAID1。此外，如果候选驱动器符合 RAID 标准，那么将为 RAID1 阵列创建专用热备件。
 - **如下所示从参考服务器克隆 RAID 配置** — 如果要克隆参考服务器设置，请使用此选项。
- 8 在 **BIOS 设置** 页面中，要将 BIOS 设置信息包括在配置文件中，请展开类别以显示设置选项，然后单击**编辑**以更新以下选项之一：
- 系统信息
 - 内存设置
 - 处理器设置
 - SATA 设置
 - 引导设置
 - 一次性引导
 - 集成设备
 - 插槽禁用
 - 串行通信
 - 系统配置文件设置
 - 系统安全
 - 其他设置

一旦进行某个类别的所有更新后，请单击**下一步**以保存更改或单击**取消**以取消更改。

① 注：有关详细的 BIOS 信息（包括设置选项和说明），请参阅所选服务器的**硬件用户手册**。

- 9 在 **引导顺序** 页面中，执行以下操作，然后单击**下一步**：
- a 要显示引导顺序选项，请展开**引导顺序**，然后单击**编辑**进行更新：
 - 1 在**引导模式**列表中，选择 BIOS 或 UEFI。
 - 2 在**查看列表**中的**引导设备顺序**下，要对显示的引导设备顺序进行更改，请选择该设备并单击**上移**或**下移**。
 - 3 选择**启用重试引导顺序**，以让服务器自动重试引导顺序。
 - 4 要应用更改，请单击**确定**，或者要取消更改，请单击**取消**。
 - b 要显示硬盘驱动器顺序选项，请展开**硬盘驱动器顺序**，然后单击**编辑**。更新以下各项：
 - 1 要更改显示的硬盘驱动器顺序，请选择该设备并单击**上移**或**下移**。
 - 2 要应用更改，请单击**确定**，或者要取消更改，请单击**取消**。

① 注：对于第 13 代之前的服务器，显示 UEFI 和 BIOS 模式；对于第 13 代或更高代的服务器，显示 BIOS 或 UEFI 模式。

- 10 在 **iDRAC 设置** 页面中，执行以下操作：
- a 展开类别以显示设置选项，然后单击**编辑**：
更新下列其中一项：
 - 网络设置
 - 网络
 - 虚拟介质
 - b 在 iDRAC 本地 **用户列表** 中，执行以下操作之一：
 - **添加用户** — 手动输入一位 iDRAC 用户和所需的信息。完成后，单击**应用**以应用更改，或者单击**取消**以取消。
 - **删除用户** — 删除所选用户。要选择用户，请使用鼠标，然后单击**删除**。要确认操作，请单击**是**。
 - **编辑用户** — 手动编辑一位 iDRAC 用户的信息。完成后，单击**应用**以应用设置，或者单击**取消**以取消。

一旦进行某个类别的所有更新后，请单击**下一步**以保存更改或单击**取消**以取消更改。


① **注**: 有关详细的 iDRAC 信息（包括设置选项和说明），请参阅所选服务器的 *iDRAC 用户指南*。

- 11 单击**下一步**。
- 12 在**摘要**页面中，单击**完成**。

后续步骤

配置文件会自动保存并显示在**硬件配置文件**窗口中。

创建或克隆硬件配置文件

- 1 在 OpenManage Integration for VMware vCenter 中，从**管理 > 部署**选项卡上，选择**部署模板 > 硬件配置文件**。
- 2 单击  图标。
- 3 在**硬件配置文件向导**中，单击**欢迎**页面上的**下一步**，并执行以下操作：
 - 在**配置文件名称**文本框中，输入配置文件名称。
 - 在**说明**文本框中，键入说明。“说明”字段为可选项。
- 4 单击**下一步**。
- 5 要选择符合要求、由 vCenter 管理并且通过 Dell EMC OpenManage 插件成功进行资源清册的参考服务器，请在**参考服务器**页面中单击**浏览**。
- 6 要从参考服务器提取所有硬件设置，可单击**克隆参考服务器设置**选项。
- 7 单击**下一步**。
提取设置需要几分钟才能完成。
- 8 单击**下一步**。
将会填充设置，并且在参考服务器窗口中显示所选服务器的名称、iDRAC IP 地址和服务标签。


将保存配置文件，并在**硬件配置文件**窗口下的**可用配置文件**中显示。

管理硬件配置文件

硬件配置文件使用参考服务器来定义服务器的硬件配置。从 OpenManage Integration for VMware vCenter 中，您可以对现有的硬件配置文件执行多种管理操作，其中包括：

- 查看或编辑硬件配置文件
- 删除硬件配置文件

查看或编辑硬件配置文件

- 1 在 OpenManage Integration for VMware vCenter 中的**管理 > 部署**选项卡上，选择**部署模板 > 硬件配置文件**。
此时将显示硬件配置文件。
- 2 要编辑配置文件，请选择一个配置文件，然后单击  。
- 3 在**硬件配置文件向导**中，要使用不同的值进行配置，请单击**编辑**。
- 4 要应用更改，请单击**保存**，要取消更改，请单击**取消**。

删除硬件配置文件

关于此任务

① **注:** 删除属于正在运行的部署任务的硬件配置文件可能导致删除任务失败。

步骤

- 1 在 OpenManage Integration for VMware vCenter 的 **管理 > 部署** 选项卡上，选择 **部署模板** 硬件配置文件。
- 2 选择配置文件并单击 **X**。
- 3 要删除配置文件，请在确认对话框中，单击 **是**，或要取消删除，请单击 **否**。

创建虚拟机监控程序配置文件

前提条件

要向服务器部署并配置 ESXi，请创建虚拟机监控程序配置文件。虚拟机监控程序配置文件需要以下信息：

- Dell 自定义 ISO 软件介质在 NFS 或 CIFS 共享上的位置
- 管理部署的主机的 vCenter 实例和可选的主机配置文件
- vCenter 中插件在其中部署服务器的目标群集或数据中心

步骤

- 1 在 OpenManage Integration for VMware vCenter 的 **管理 > 部署** 选项卡上，选择 **部署模板 > 虚拟机监控程序配置文件**。
- 2 在 **虚拟机监控程序配置文件** 页面中，单击 **+** 图标。
- 3 在 **虚拟机监控程序配置文件** 对话框中，执行以下子任务：
 - 在 **配置文件名称** 文本框中，输入配置文件名称。
 - 在 **说明** 文本框中，输入说明，这是可选条目。
- 4 在 **选择参考 ISO 路径和版本** 下，在 **安装源 (ISO)** 文本框中，键入虚拟机监控程序共享位置的路径。
将修改一份虚拟机监控程序映像的副本以允许脚本安装。参考 ISO 位置可以是以下格式之一：

- **NFS 格式:** host:/share/hypervisor.iso
- **CIFS 格式:** \\host\share\hypervisor.iso

① **注:** 如果您配置使用 CIFS 共享，而不是基于 CIFS 共享的服务器消息块 (SMB) 版本 1.0，可能会导致潜在的服务中断，因为 OMIVV 无法与诸如 CIFS 共享等通信。因此，建议您使用基于仅基于 CIFS 共享的 SMB 版本 1.0。

如果使用 CIFS 共享，则输入 **用户名、密码和验证密码**。确保密码匹配。


- 5 在 **选择版本** 列表中，选择 ESXi 版本。
所有使用此虚拟机监控程序配置文件部署的服务器都有此映像，并且如果服务器版本早于第 12 代，则还会安装 OMSA 的最新推荐版本。
- 6 要确认路径和验证，请单击 **测试设置** 下的 **开始测试**。
- 7 单击 **应用**。

管理虚拟机监控程序配置文件

您可以对现有虚拟机监控程序配置文件执行多个管理操作，其中包括：

- 查看或编辑虚拟机监控程序配置文件
- 删除虚拟机监控程序配置文件

查看或编辑虚拟机监控程序配置文件


- 1 在 OpenManage Integration for VMware vCenter 的 **管理 > 部署** 选项卡上，选择 **部署模板 > 虚拟机监控程序配置文件**。此时，会显示虚拟机监控程序配置文件。
- 2 选择配置文件并单击  图标。
- 3 在 **虚拟机监控程序配置文件** 对话框中，提供更新的值。
- 4 要应用更改，请单击 **保存**，要取消更改，请单击 **取消**。

删除虚拟机监控程序配置文件

关于此任务

① | **注**: 删除属于正在运行的部署任务的虚拟机监控程序配置文件可能导致任务失败。

步骤


- 1 在 OpenManage Integration for VMware vCenter 的 **管理 > 部署** 选项卡上，选择 **部署模板 > 虚拟机监控程序配置文件**。
- 2 选择配置文件并单击  图标选择“高级”选项。
- 3 在确认对话框中，要移除配置文件，可单击 **删除**，或者单击 **取消** 以取消。

创建部署模板

关于此任务

部署模板包含系统配置文件、硬件配置文件、虚拟机监控程序配置文件、系统配置文件和虚拟机监控程序配置文件的组合或者硬件配置文件和虚拟机监控程序配置文件的组合。**部署向导**使用此模板在 vCenter 中配置服务器硬件并部署主机。

步骤

- 1 在 OpenManage Integration for VMware vCenter 的 **管理 > 部署** 选项卡上，请选择 **部署模板**。
- 2 单击  图标。
- 3 在 **部署模板** 对话框中，输入模板的名称。
- 4 在部署模板中输入可选的 **说明**。
- 5 单击 **系统配置文件** 或 **硬件配置文件**，然后从下拉菜单中选择相应的配置文件。

① | **注**: 建议使用第 14 代服务器的系统配置文件和第 13 代及更早期服务器的硬件配置文件。
- 6 从下拉菜单中选择 **虚拟机监控程序配置文件**。
- 7 要应用配置文件选择并保存更改，可单击 **保存**。要取消，可单击 **取消**。

管理部署模板

从 OpenManage Integration 中，可以对现有部署模板执行多种管理操作，其中包括：

- 查看或编辑部署模板
- 删除部署模板

查看或编辑部署模板

- 1 在 OpenManage Integration for VMware vCenter 的 **管理 > 部署** 选项卡上，请选择 **部署模板**。

将会显示部署模板配置文件。

- 2 在**部署模板**对话框中，输入该模板和说明的新名称。
确保模板具有唯一的名称。
- 3 从下拉菜单中选择**硬件配置文件**或**系统配置文件**。
- 4 从下拉菜单中更改**虚拟机监控程序配置文件**，并单击**保存**。

删除部署模板

- 1 在 OpenManage Integration for VMware vCenter 的**管理 > 部署**选项卡上，请选择**部署模板**。
- 2 在**部署模板**页面中，选择模板，然后单击  图标。
- 3 要确认模板删除，请在消息框上单击**删除**，或者要取消，请单击**取消**。

有关部署向导

部署向导说明部署过程，该过程如下所示：

- 选择符合要求的裸机服务器。
 - ① **注：**如果您选择第 14 代服务器用于部署，部署模板列表将包含硬件配置文件或系统配置文件或虚拟机监控程序配置文件或硬件与虚拟机监控程序的组合或系统与虚拟机监控程序配置文件的组合。
 - ① **注：**如果您选择非第 14 代服务器或第 14 代与非第 14 代服务器的组合，部署模板列表将包括一个硬件配置文件或虚拟机监控程序配置文件、或硬件配置文件与虚拟机监控程序配置文件的组合。
- 选择部署模板，其中包括硬件和虚拟机监控程序配置文件。
- 选择安装目标（硬盘或 iDSDM）。
部署系统管理程序时，您可以将其部署到内部双 SD 模块。应该先从 BIOS 中启用内部双 SD 模块，然后再使用 OMIVV 部署虚拟机监控程序。
- 选择要与主机关联的连接配置文件。
- 为每个主机分配网络详细信息。
- 选择 vCenter、目标数据中心或群集和可选的主机配置文件。
- 计划要运行的服务器部署作业。
 - ① **注：**如果您仅部署硬件配置文件，将跳过部署向导中的服务器标识、连接配置文件、网络详细信息选项，您将直接进入计划部署页面。
 - ① **注：**对于试用/评估许可证，只要许可证未过期，您可使用部署向导。

VLAN 支持

OMIVV 支持将虚拟机监控程序部署到可路由的 VLAN，您可以在部署向导中配置 VLAN 支持。在部署向导的此部分中，有一个指定使用 VLAN 和指定 VLAN ID 的选项。当提供 VLAN ID 时，会在部署期间将其应用于虚拟机监控程序的管理接口并使用 VLAN ID 标记所有流量。

确保在部署期间提供的 VLAN 可与虚拟设备和 vCenter 服务器通信。将虚拟机监控程序部署到 VLAN 但 VLAN 无法与这些目标的一个或两个通信会导致部署失败。

如果在单个部署作业中选择了多个裸机服务器，并要将相同的 VLAN ID 应用于所有服务器，则在部署向导的“服务器标识”部分中，使用**将设置应用于所有选定服务器**。此选项可用于将相同的 VLAN ID 以及其他网络设置应用于该部署作业的所有服务器中。

- ① **注：**OMIVV 不支持多宿主配置。将第二个网络接口添加到设备以与第二个网络通信会导致与虚拟机监控程序部署、服务器符合性和固件更新有关的工作流出现问题。

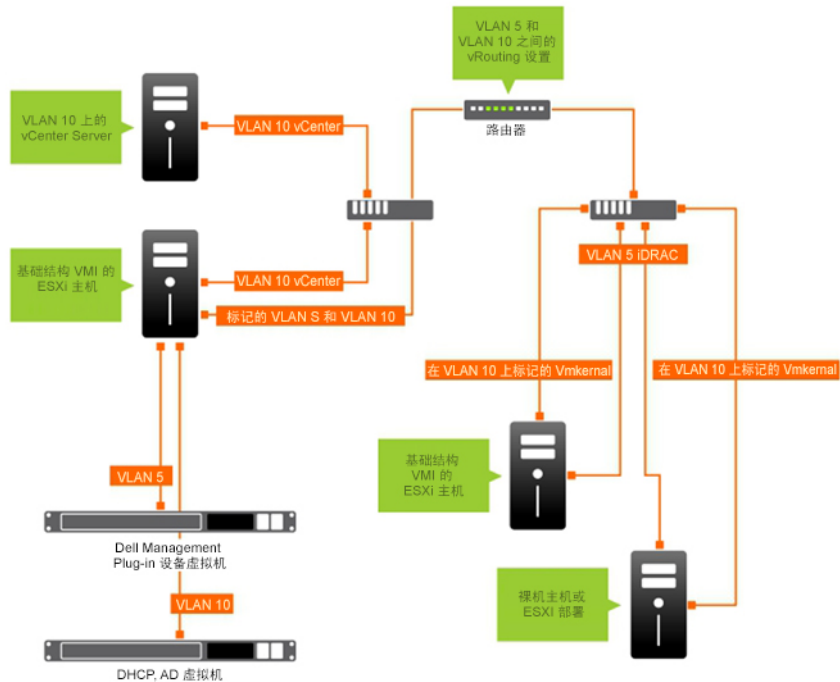


图 2: VLAN 网络。

在此示例网络中，OMIVV 设备位于 VLAN 5 上，而部署的 ESXi 主机的 vCenter 和 VMkernel 位于 VLAN 10 上。因为 OMIVV 不支持多 VLAN 宿主，所以 VLAN 5 必须路由到 VLAN 10，所有系统才能互相正常通信。如果在这些 VLAN 之间未启用路由，则部署将失败。

运行部署向导

前提条件

在运行部署向导之前，确保使用硬件配置文件、系统配置文件和虚拟机监控程序配置文件以及 vCenter 的连接配置文件创建部署模板。

关于此任务

要运行部署向导，请执行以下操作：

步骤

- 1 在 OpenManage Integration for VMware vCenter 中，选择**管理 > 部署**选项卡。
- 2 在**裸机服务器**窗口中，单击**运行部署向导**链接。
此时将显示部署向导的**欢迎**页面。
- 3 在**欢迎**页面中，查看信息，然后单击**下一步**。
- 4 在**选择服务器以进行部署**页面中，要将符合要求的裸机服务器分配给部署作业，请单击服务器列表旁边的复选框。
- 5 单击**下一步**。
- 6 在**选择模板/配置文件**页面中，执行以下分步骤：
 - a 在**部署模板**下，要将部署模板分配给所选服务器，请从**选择部署模板**中选择现有的部署模板。

注：仅当您在**选择服务器以进行部署**页面中选择第 14 代服务器时，才显示基于模板的系统配置文件。

您可以从下拉列表中选择以下其中一个部署模板：

- 如果您仅选择仅配置服务器硬件的部署模板的硬件配置文件或系统配置文件，请转至步骤 10。
- 如果您选择部署虚拟机监控程序的虚拟机监控程序配置文件部署模板，从步骤 6 往前继续。

① **注:** 如果您选择仅部署的硬件配置文件或系统配置文件, 您将被自动提示包括计划部署页面的信息。

b 在虚拟机监控程序安装下, 选择以下选项之一:

- **第一启动磁盘**- 在 RAID 控制器创建的硬盘 (HDD)、固态驱动器 (SSD)、虚拟磁盘上部署虚拟机监控程序。
- **内部双 SD 模块** — 在 IDSDM 上部署虚拟机监控程序。

① **注:** 如果 IDSDM 在至少一台所选服务器上可用, 将启用内部双 SD 模块选项。否则, 只有硬盘选项可用。

如果任何所选服务器不支持 IDSDM, 或 IDSDM 在部署期间不存在, 请执行以下操作之一:

- 如果要在服务器的第一启动磁盘上部署虚拟机监控程序, 则选中**将虚拟机监控程序部署到没有内部双 SD 模块的服务器**的第一启动磁盘复选框。

⚠ **小心:** 如果选中此选项并在服务器的第一启动磁盘驱动器上部署虚拟机监控程序, 则磁盘驱动器上的所有数据将被擦除。

- 要跳过在选定服务器上部署并在下一个服务器上继续执行虚拟机监控程序部署, 请清除**将虚拟机监控程序部署到没有内部双 SD 模块的服务器**的第一启动磁盘。

c 在**凭据配置文件**下, 执行以下操作之一:

- 选择**将此凭据配置文件用于所有服务器**选项按钮, 然后将要将所有服务器分配到同一个现有的配置文件, 请从下拉式列表中选择连接配置文件。
- 单击**为每个服务器选择一个连接配置文件**选项按钮, 然后从下拉式列表中为每个服务器选择单独的连接配置文件。

7 单击**下一步**。

此时将显示**服务器标识**页面。


服务器标识可通过以下两种方式提供:

- 输入网络信息 (IP 地址、子网掩码和网关) — 主机名的完全限定域名为必填项。不支持对 FQDN 使用 *localhost*。在将主机添加到 vCenter 时使用 FQDN。
- 使用动态主机配置协议 (DHCP) 配置 IP 地址、子网掩码、网关 IP、主机名和首选/备用 DNS 服务器 — 在将主机添加到 vCenter 时将使用 DHCP 分配的 IP 地址。在使用 DHCP 时, 建议对所选的 NIC MAC 地址使用 IP 保留。

① **注:** 对主机名而非 *localhost* 使用完全限定域名 (FQDN)。从 ESXi 5.1 开始, *localhost* 的值将会妨碍 OMIVV 插件处理主机发来的事件。创建使用 FQDN 解析 IP 地址的 DNS 记录。为正确标识 ESXi 5.1 发来的 SNMP 警报, 请将 DNS 服务器配置为支持逆向查找请求。在安排运行部署作业之前, 必须先提供 DHCP 保留和 DNS 主机名并对其进行验证。

8 在**服务器标识**页面中, 执行以下操作:

该页面提供了用于指定 VLAN ID 的选项。当提供 VLAN ID 时, 会在部署期间将其应用于虚拟机监控程序的管理接口并使用 VLAN ID 标记所有流量。服务器标识将新名称和网络标识分配至部署的服务器。请参阅 [VLAN 支持](#)。

- a 要展开并查看单个的服务器信息, 请在**所选服务器**下, 单击 。
- b 在 **主机名和 NIC** 下, 输入服务器的**完全限定主机名**。
- c 在**管理任务的 NIC** 下拉式列表中, 选择将用于管理服务器的 NIC。
- d 输入 IP 地址、子网掩码、默认网关和 DNS 详细信息, 或者选中**使用 DHCP 获取**复选框。
- e 如果部署到需要 VLAN ID 的网络, 请选中 **VLAN** 复选框, 然后输入 VLAN ID。
对于 VLAN ID, 请使用 1 到 4094 的数字。保留 VLAN ID 0 用于标记帧的优先级。
- f 对要部署的所有服务器重复步骤 a 到 h, 或者选中**将设置应用于所有选定服务器**复选框。
如果选择**将设置应用于所有选定服务器**, 请输入其他服务器的 FQDN 名称和 IP 地址。

① **注:** 在指定服务器的 FQDN 名称时, 请确保为每个服务器提供唯一的主机名。

9 单击**下一步**。

10 在**计划部署**页面中, 执行以下操作:

- a 输入**作业名称和作业说明**。
- b 对于 **vCenter 设置**, 请输入以下内容:
 - 1 在 **vCenter 实例**中, 选择部署后管理主机的服务器实例。
 - 2 在 **vCenter 目标容器**中, 单击**浏览**以搜索 vCenter 目标。

- 3 在 **vCenter 主机配置文件** 中，选择封装主机配置和帮助管理主机配置的配置文件（可选）。
- c 通过选择作业计划确定何时运行部署作业：
 - 1 选择**计划部署作业**
 - 使用日历控件选择日期。
 - 输入时间。
 - 2 要立即开始作业，请选择**立即运行部署作业**。

要在部署作业开始后转至作业队列，请选择**提交作业后转到作业队列**。

11 单击**完成**。

后续步骤

在部署向导任务完成后，您可以使用**作业队列**管理部署作业。。

使用作业队列管理部署作业

1 在 OpenManage Integration for VMware vCenter 中，在**监测 > 作业队列**选项卡上，单击**部署作业**。

以下有关部署作业的详细信息显示在上部的网格中：

- 名称
- 说明
- 计划的时间
- 状态
- 集合大小
- 进度摘要

2 要更新**部署作业详细信息**，请单击**刷新**图标。

3 要显示包含部署作业中服务器详细信息的部署作业详细信息，请选择上部网格中的部署作业。

以下细信息显示在下部的网格中：


- 服务标签
- iDRAC IP address (iDRAC IP 地址)
- 作业状态
- 警告
- 部署作业详细信息（有关鼠标悬停的更多信息）
- 开始和结束时间
- 更多详细信息


选择部署作业并将光标悬停在该作业的**详细信息**列上，可以以弹出式文本的方式查看关于该部署作业的完整信息。


有关基于系统配置文件作业故障的更多详细信息，请单击**更多详细信息**。**更多详细信息**页面显示以下信息：

- 组件的 FQDD
- 属性值
- 旧值
- 新值
- 关于故障的消息和消息 ID（未显示几种类型的错误）

当您单击**更多详细信息**时，一些显示在**应用系统配置文件故障详细信息**窗口的**属性名称**下的属性与系统配置文件的**属性名称**不相同。

要将详细信息导出到 CSV 文件，请在数据网格的右下角单击 。

4 要中止部署作业，请单击  图标。

- 当显示该消息时，请单击**中止作业**进行中止，或单击**请勿中止作业**取消操作。
- 要显示**清空部署作业队列**窗口，请单击。选择**早于日期和作业状态**，然后单击**应用**。然后，所选作业会从队列中清除。

部署作业时间

配置和部署裸机服务器可能需要 30 分钟到几个小时才能完成，具体视特定因素而定。开始部署作业后，建议您根据提供的指南计划部署时间。完成配置和部署所需的时间量因部署类型、复杂程度以及同时运行的部署作业数量而有所不同。下表提供了部署作业所用的大致时间：部署作业可以在最多五个并发服务器中分批运行以提高整体部署作业的时间。并行作业的确切数量视可用的资源而定。

表. 37: 大致部署时间

部署类型	每个部署的大致时间
仅系统管理程序	30 分钟到 130 分钟之间
虚拟机监控程序和硬件配置文件	1 - 4 小时
仅系统配置文件	5 - 6 分钟
系统配置文件和虚拟机监控程序配置文件	30 - 40 分钟

部署顺序中的服务器状态

当运行资源清册作业时，那些自动/手动查找到的裸机系统被分类成不同的状态，以此来帮助确定是否该服务器对数据中心是全新的，或者已有计划的待定部署作业。管理员能利用这些状态来决定是否应将某个服务器包含进部署作业当中。下面列出了这些状态：

表. 38: 部署顺序中的服务器状态

服务器状态	说明
未配置	服务器已经联系 OMIVV，正在等待得到配置。
已配置	该服务器已按照成功部署虚拟机监控程序需要的全部硬件信息配置完毕。

下载自定义 Dell EMC ISO 映像

前提条件

部署过程需要包含所有 Dell 驱动程序的自定义 ESXi 映像。

步骤

- 导航至 support.dell.com。
- 单击**从所有产品中选择 > 服务器、存储和网络**。。
- 在**选择产品**下，单击**PowerEdge**。
- 单击 PowerEdge 服务器型号。
- 单击服务器型号的**驱动程序和下载**页面。
- 单击**更改操作系统**链接，然后选择所需的 ESXi 系统。
- 单击**企业解决方案**。
- 在**企业解决方案**列表中，选择所需的 ISO 版本，然后单击**下载**。

关于主机、裸机和 iDRAC 符合性

要使用 OMIVV 管理主机、裸机服务器，每台主机都必须符合特定的最低标准。如果不符合要求，则无法通过 OMIVV 正确地管理它们。OMIVV 会显示有关裸机或主机的不符合要求的详细信息，并允许您修补不符合性问题（如果适用）。

在每种情况下，您可以通过运行以下操作之一查看并修补符合性问题：

- 要查看并修补 vSphere 主机符合性问题，请参阅[运行修补不符合要求的 vSphere 主机向导](#)。
- 要查看并修补有符合性问题的裸机服务器，请参阅[运行修补不符合要求的裸机服务器向导](#)。

主题：

- [报告和修正 vSphere 主机的符合性](#)
- [对第 11 代服务器使用 OMSA](#)
- [报告和修补裸机服务器的符合性](#)

报告和修正 vSphere 主机的符合性

前提条件

在以下情况下，主机主机不符合要求：

- 主机未分配给连接配置文件。
- 重新引导时收集系统资源清册 (CSIOR) 已禁用或尚未运行，需要手动重新引导。
- OMSA 代理未安装、已过时或没有正确配置。如果已为第 11 代服务器安装或更新 OMSA，则 ESXi 主机需要重新引导。
- 主机的 SNMP 陷阱目标未配置至 OMIVV 设备 IP 地址。连接配置文件中提供的 iDRAC 或主机凭据无效时，或者在 iDRAC 中没有可用槽或 iDRAC 锁定模式开启时（仅在第 14 代主机中），可能出现 SNMP 陷阱目标设置故障。
- OMIVV 无法在运行 ESXi 6.5 的主机上启用 WBEM 服务。

△ 小心：处于锁定模式下的主机在符合性检查中将不会显示，即使这些主机不符合要求也是如此。不显示的原因是无法确定其符合性状态。确保手动检查这些系统的符合性。在这种情况下，将会显示警告消息。

关于此任务

您可以运行“修补不符合要求的 vSphere 主机”向导来修补不符合要求的主机。某些不符合要求的 ESXi 主机需要重新引导。如果必须安装或更新 OMSA，则 ESXi 主机需要重新引导。此外，从未运行 CSIOR 的所有主机都需要重新引导。如果您选择自动重新引导 ESXi 主机，请进行以下操作：

- 对于 CSIOR 状态修补：
 - 如果 CSIOR 从未在主机上运行，则 CSIOR 将在主机上设置为**开启**，然后主机设置为维护模式并重新引导。
- 未安装 OMSA 或运行不受支持的 OMSA 版本的主机：
 - OMSA 已安装在主机上。
 - 主机设置为维护模式并重新引导。
 - 重新引导完成后，请配置 OMSA 以使更改生效。
 - 此时主机将脱离维护模式。
 - 系统将运行资源清册以刷新数据。
- 有关安装了受支持但必须配置的 OMSA 版本的 OMSA 状态修补：

- OMSA 已配置在主机上。
- 系统将运行资源清册以刷新数据。

要查看并修补不符合要求的主机，请执行以下操作：

步骤

- 1 在 OpenManage Integration for VMware vCenter 的**管理选项卡**中，单击**符合性 > vSphere 主机**。
 - a 在 **vSphere 主机** 页面中，查看不符合要求的主机列表。
将会显示一个表格，其中列出了不符合要求的主机以及主机 IP 或名称、型号、连接配置文件、CSIOR 状态、OMSA 状态、WBEM 状态、SNMP 陷阱状态、虚拟机监控程序和 iDRAC 许可证状态。
 - b 要查看不符合要求的主机的更多详细信息，请选择不符合要求的主机。
 - c 要交换表格中的列，请在数据网格中拖放列。
- 2 要修补不符合要求的主机，请单击**修补不符合要求的 vSphere 主机**。
启动**修补不符合要求的 vSphere 主机**向导。这是一个动态向导并仅显示与所选不符合要求主机相关的页面。

如果全部所选不符合要求的主机是 CSIOR 兼容，您可以查看向导中的**开启 CSIOR** 页面。
- 3 在**修补不符合要求的 vSphere 主机**向导中，在**欢迎**页面中单击**下一步**。
- 4 在**选择要修补符合性问题的 vSphere 主机**向导页面中，选中要修补的主机的复选框。
- 5 单击**下一步**。
如果有未分配给连接配置文件的选定主机，则会显示一条警告消息，提示您继续执行符合性向导或取消修补符合性向导。要解决连接配置文件不符合性问题，请执行以下操作之一：
 - 要从符合性向导中排除未分配给连接配置文件的主机，请单击**继续符合性向导**。
 - 要退出向导并从**连接配置文件**页面中修补系统，请单击**取消**。请参阅[创建连接配置文件](#)。创建连接配置文件后，您可以返回该向导。
- 6 如果您针对警告消息单击**继续符合性向导**，请在**开启 CSIOR** 窗口中，选中相应的复选框为选定主机开启 **CSIOR**。
- 7 单击**下一步**。
- 8 在 **修补 OMSA** 窗口中，选中复选框以修补所选主机的 **OMSA**。
- 9 单击**下一步**。
- 10 在 **重新引导主机**窗口中，查看必须重新引导的 ESXi 主机。
如果必须安装或更新 OMSA，则 ESXi 主机需要重新引导。此外，从未运行 CSIOR 的所有主机都需要重新引导。请执行以下操作之一：
 - 如果要将主机自动置于维护模式并在需要时重新引导，请选中**自动将主机置于维护模式并在需要时重新引导**复选框。
 - 如果要手动重新引导，请在安装 OMSA 之后重新引导主机，手动或通过符合性向导（在主机处于正在运行状态并且如果未配置 OMSA）配置 OMSA，然后再次运行资源清册。请参阅[运行资源清册作业](#)。请参阅[运行资源清册作业](#)。
- 11 单击**下一步**。
- 12 在**摘要**窗口中，查看针对不符合要求的主机执行的操作。
需要手动重新引导以使摘要页面上的操作生效。
- 13 单击**完成**。

当您通过在连接配置文件中提供有效信息或使前四个插槽在 iDRAC 陷阱目标中可用，或在 iDRAC 中禁用系统锁定模式，从而解决 iDRAC 或主机凭据后，向导将 SNMP 陷阱目标状态配置为**已配置**。

① | 注：系统锁定模式仅适用于第 14 代服务器。

如果具有 WBEM 不符合性的主机存在，请确保手动修复导致 WBEM 服务启用失败的这些主机的条件。您可以通过在用户日志中进行查看来修复错误条件，然后允许 OMIVV 在资源清册期间为这些主机启用 WBEM 服务。

修补 vSphere 主机的 iDRAC 许可证符合性

关于此任务

vSphere 主机符合性页面中列出的 vSphere 主机是不符合要求的，因为它们没有兼容的 iDRAC 许可证。该表显示 iDRAC 许可证的状态。您可以单击不符合要求的主机以查看更多详细信息，例如 iDRAC 许可证的剩余天数，那么您可以根据需要进行更新。如果 vSphere 主机页面中的运行资源清册作业链接已禁用，那么由于 iDRAC 许可证就没有不符合要求的 vSphere 主机。

步骤

- 1 在 OpenManage Integration for VMware vCenter 的**管理选项卡**中，单击**符合性 > vSphere 主机**。
- 2 选择 **iDRAC 许可证状态为不符合要求**的主机。
- 3 如果您的许可证已过时，请单击**购买/更新 iDRAC 许可证**链接。
- 4 登录到 **Dell 许可证管理**页面，然后更新或购买新的 iDRAC 许可证。
使用此页面上的信息标识并更新您的 iDRAC。
- 5 安装了 iDRAC 许可证后，运行 vSphere 主机的资源清册作业。然后当成功完成资源清册作业为主机符合要求后，返回至此页面。

对第 11 代服务器使用 OMSA

要管理 Dell PowerEdge 第 11 代服务器，OMIVV 需要在其上运行 OMSA。对于通过 OMIVV 部署的第 11 代主机，OMSA 将自动安装。手动部署的第 11 代主机，您可以选择以下任一操作：

- 使用 OMIVV 安装和配置 OMSA。请参阅 [设置 OMSA 陷阱目标](#)。
- 手动安装和配置 OMSA。请参阅 [在 ESXi 系统上部署 OMSA 代理](#)。

① **注:** 使用 OMIVV 部署 OMSA 代理时，OMIVV 会启动 httpClient 服务并启用端口 8080，在 ESXi 5.0 下载并安装 OMSA VIB 后释放该端口。在 OMSA 安装完成时，该服务会自动停止并关闭此端口。

① **注:** 除以上所列的选项之外，您可以使用 Web 客户端 Host Compliance，其会安装并配置 OMSA 代理。

在 ESXi 系统上部署 OMSA 代理

关于此任务

在 ESXi 系统上安装 OMSA VIB，以从系统收集资源清册和警报信息。

① **注:** Dell PowerEdge 第 12 代服务器之前的 Dell 主机上需要 OpenManage 代理。使用 OpenManage Integration for VMware vCenter 安装 OMSA 或手动安装到主机，然后再安装 OpenManage Integration for VMware vCenter。有关手动安装 OMSA 代理的详细信息可从以下网址获得：<http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.openmanage-server-administrator-omsa.aspx>

步骤

- 1 如果尚未安装 OMSA，请安装 vSphere 命令行工具 (vSphere CLI)，该工具可从 www.vmware.com 获取。

- 2 输入以下命令：

```
Vihostupdate.pl -server <IP Address of ESXi host> -i -b <OMSA version X.X>
```

① **注:** 安装 OMSA 可能需要几分钟时间。该命令需要您在完成后重新引导主机。

① **注:** 可以从**管理 > 设置 > 设备设置 > OMSA SNMP 陷阱团体字符串**中配置 SNMP 团体字符串。有关 SNMP 陷阱团体字符串的更多信息，请参阅[配置 SNMP 陷阱团体字符串](#)。

设置 OMSA 陷阱目标

关于此任务

所有第 11 代主机都必须配置 OMSA。

① **注:** 仅在第 12 代 PowerEdge 服务器之前的 Dell EMC 服务器上需要 OMSA。

要设置 OMSA 陷阱目标：

步骤

- 1 从 Web 浏览器中，通过提供 `https://<HostIP>:1311/` URL 导航至 OMSA 代理。
- 2 登录到界面，并选择**警报管理**选项卡。
- 3 选择**警报操作**，并确保所有被监测的事件都已设置**广播消息**选项，以便发布事件。
- 4 选择选项卡顶部的 **平台事件**项。
- 5 单击灰色的**配置目标**按钮，并单击**目标**链接。
- 6 选中 **启用目标**复选框。
- 7 在**目标 IP 地址**字段中输入 OMIVV 设备的 IP 地址。
- 8 单击**应用更改**。
- 9 重复步骤 1 到步骤 8 以配置额外事件。

① **注:** 可以从**管理 > 设置 > 设备设置 > OMSA SNMP 陷阱团体字符串**中配置 SNMP 团体字符串。有关 SNMP 陷阱团体字符串的更多信息，请参阅**配置 SNMP 陷阱团体字符串**。

报告和修补裸机服务器的符合性

前提条件


在下列情况下，裸机服务器不符合要求：

- 它不是受支持的服务器。
- 它没有受支持的 iDRAC 许可证（iDRAC Express 是最低要求）。
- 它没有受支持的 iDRAC、BIOS 或 LC 版本。
- 不存在 LOM 或 rNDC。
- 系统锁定模式已开启。

关于此任务

要查看并修补不符合要求的裸机服务器列表，请执行以下操作：

步骤

- 1 在 OpenManage Integration for VMware vCenter 中，选择**管理 > 部署**选项卡。
 - a 在**裸机服务器**页面中，查看不符合要求的服务器列表。
将会显示一个表格，其中列出了不符合要求的服务器及服务标签、型号、iDRAC Ip、服务器状态、系统锁定模式、符合性状态和 iDRAC 许可证状态。
 - b 要查看不符合要求的服务器的更多详细信息，请选择不符合要求的服务器。
 - c 要将服务器的不符合要求信息导出到 CSV 文件，请在表格的右下角中，单击图标。
 - d 要筛选的数据网格的内容，请单击列**筛选器**字段。
 - e 要交换表格中的列，请在数据网格中拖放列。
- 2 要修补不符合要求的服务器，请单击**修补不符合要求的服务器**。

① **注:** 修补不符合要求的服务器链接仅为第 11 代不符合要求的主机启用选择链接。

- 3 在**修补裸机符合性**向导中，在欢迎页面中单击**下一步**。
- 4 在**修补符合性**页面中，选中您要修补的服务器的复选框。

列出了不符合要求的服务器，且显示不符合要求的固件组件。列出的不符合要求的服务器需要更新以下至少一个固件组件：

- iDRAC IP

① 注：从 OMIVV 中，不能修补 iDRAC 许可证不符合要求的裸机服务器。确保在 OMIVV 外部将受支持的 iDRAC 许可证上传到那些服务器，然后单击刷新裸机服务器。请参阅[刷新裸机服务器](#)。

- BIOS
- LC
- 系统锁定模式

① 注：要从对应的 iDRAC 上查看不符合要求的裸机服务器的最新详细信息，请单击刷新裸机服务器详细信息。如果系统锁定模式已开启，则该服务器是不符合要求的，反之亦然。

5 要查看符合性问题详细信息，请单击符合性问题。

① 注：如果由于开启了系统锁定模式造成裸机服务器不符合要求，请确保您从 iDRAC 控制台上手动配置服务器的系统锁定模式。

6 单击下一步。

7 在摘要窗口中，查看针对不符合要求的裸机服务器的固件组件执行的操作。

8 单击完成。

修补裸机服务器的 iDRAC 许可证符合性

关于此任务

在裸机服务器页面中列出的裸机服务器是不符合要求的，因为它们没有兼容的 iDRAC 许可证。一张表显示 iDRAC 许可证的状态。您可以单击不符合要求的裸机服务器以查看更多详细信息，例如 iDRAC 许可证的剩余天数，那么您可以根据需要进行更新。如果刷新裸机服务器链接已在裸机服务器页面中启用，那么由于 iDRAC 许可证会有不符合要求的裸机主机。

步骤

- 1 在 OpenManage Integration for VMware vCenter 中，选择**管理 > 部署**选项卡。
在裸机服务器页面中，查看表中显示的不符合要求的服务器列表。
- 2 选择裸机服务器，其中 **iDRAC 许可证状态**为**不符合要求**或**未知**。
- 3 如果您的许可证已过时，请单击**购买/更新 iDRAC 许可证**链接。
- 4 登录到 **Dell 许可证管理**页面，然后更新或购买新的 iDRAC 许可证。
使用此页面上的信息标识并更新您的 iDRAC。
- 5 安装 iDRAC 许可证后，单击**刷新裸机服务器**。

刷新裸机服务器

- 1 在 **OpenManage Integration for VMware vCenter** 页面上，单击 **管理 > 部署 > 裸机服务器**，然后单击**刷新裸机服务器**。
- 2 在**刷新裸机服务器**窗口中，选择您想要刷新数据的服务器，然后单击**刷新所选的服务器**。

刷新裸机服务器数据可能需要几分钟。

在裸机服务器页面上，所有选定的裸机服务器数据将被刷新。

安全角色和权限

OpenManage Integration for VMware vCenter 以加密格式存储用户凭据。它不会向客户端应用程序提供任何密码，以避免任何不当请求。备份数据库使用自定义的安全短语进行完全加密，因此数据不会被滥用。

默认情况下，管理员组中的用户具有所有权限。管理员可在 VMware vSphere Web 客户端中使用 OpenManage Integration for VMware vCenter 的所有功能。如果您希望用户有管理产品的必要权限，请执行以下操作：

- 1 创建具有必要权限的角色
- 2 使用该用户注册 vCenter 服务器
- 3 包括 Dell 角色、Dell 操作角色和 Dell 基础架构部署角色。

主题：

- 数据完整性
- 访问控制验证、授权和角色
- Dell 操作角色
- Dell 基础架构部署角色
- 关于权限

数据完整性

OpenManage Integration for VMware vCenter、Administration Console 和 vCenter 之间的通信使用 SSL/HTTPS 完成。OpenManage Integration for VMware vCenter 生成一个用于 vCenter 和设备之间的可信通信的 SSL 证书。它还在通信和 OpenManage Integration for VMware vCenter 注册之前，验证和信任 vCenter 服务器的证书。当密钥在 Administration Console 与后端服务之间往返传输时，OpenManage Integration for VMware vCenter 的控制台选项卡使用安全步骤来避免不当请求。这种安全类型会使跨站点请求伪造失效。

安全 Administration Console 会话具有 5 分钟闲置超时，并且只有在当前浏览器窗口和/或选项卡中时此会话才有效。如果您尝试在新窗口或选项卡中打开会话，则会提示一个安全错误，要求有效的会话。此操作还会阻止用户单击任何可能会攻击 Administration Console 会话的恶意 URL。



图 3: 安全错误消息

访问控制验证、授权和角色

为了执行 vCenter 操作，OpenManage Integration for VMware vCenter 会使用 Web 客户端的当前用户会话和 OpenManage Integration 的已存储管理凭据。OpenManage Integration for VMware vCenter 使用 vCenter 服务器内置的角色和权限模式来授权用户对 OpenManage Integration 和 vCenter 管理的对象（主机和群集）执行操作。

Dell 操作角色

该角色包含权限/组以完成设备和 vCenter 服务器任务，其中包括固件更新、硬件资源清册、重新启动主机、将主机置于维护模式或创建 vCenter 服务器任务。

此角色包含以下权限组：

表. 39: 权限组

组名称	说明
权限组 — Dell.Configuration	执行主机相关任务、执行 vCenter 相关任务、配置 SelLog、配置 ConnectionProfile、配置 ClearLed、固件更新
权限组 — Dell.Inventory	配置资源清册、配置保修检索、配置只读
权限组 — Dell.Monitoring	配置监测、监测
权限组 — Dell.Reporting（未使用）	创建报告、运行报告

Dell 基础架构部署角色

该角色包含与虚拟机监控程序部署功能相关的权限。

此角色提供的权限为：创建模板、配置硬件配置配置文件、配置虚拟机监控程序部署配置文件、配置连接配置文件、分配标识、和部署。

权限组 — Dell.Deploy — 配置 创建模板、配置硬件配置配置文件、配置虚拟机监管程序部署配置文件、配置连接配置文件、分配标识、和部署

关于权限

OpenManage Integration for VMware vCenter 执行的每个操作均与权限相关联。以下部分列出了可用的操作和关联的权限：

- Dell.Configuration.Perform vCenter-related tasks
 - 退出和进入维护模式
 - 使 vCenter 用户组能查询权限
 - 注册和配置警报，例如，在事件设置页上启用/禁用警报
 - 将事件/警报发布到 vCenter
 - 在事件设置页上配置事件设置
 - 在事件设置页上恢复默认警报
 - 在配置警报/事件设置时检查群集的 DRS 状态
 - 在执行更新或其它配置操作后重新启动主机
 - 监测 vCenter 任务状态/进程

- 创建 vCenter 任务，例如：固件更新任务、主机配置任务和资源清册任务
- 更新 vCenter 任务状态/进程
- 获得主机配置文件
- 将主机添加到数据中心
- 将主机添加到群集
- 将配置文件应用到主机
- 获得 CIM 凭据
- 配置主机的兼容性
- 获得兼容性任务状态
- Dell.Inventory.Configure ReadOnly
 - 在配置连接配置文件时，获得所有 vCenter 主机来构建 vCenter 树
 - 在选定此选项卡时，检查该主机是否是 Dell 服务器
 - 获得 vCenter 的地址/IP
 - 获得主机 IP/地址
 - 基于 vSphere 客户端会话 ID，获得当前 vCenter 会话用户
 - 获得 vCenter 资源清册树以按照树结构显示 vCenter 资源清册
- Dell.Monitoring.Monitor
 - 获得用于发布事件的主机名
 - 执行事件日志操作，例如：获得事件计数，或更改事件日志设置
 - 注册、注销和配置事件/警报 — 接收 SNMP 陷阱和发布事件
- Dell.Configuration.Firmware Update
 - 执行固件更新
 - 在固件更新向导页上加载固件存储库和 DUP 文件信息
 - 查询固件资源清册
 - 配置固件存储库设置
 - 配置暂存文件夹和使用暂存功能执行更新
 - 测试网络和存储库连接
- Dell.Deploy-Provisioning.Create Template
 - 配置硬件配置的配置文件
 - 配置虚拟机监管程序部署配置文件
 - 配置连接配置文件
 - 分配标识
 - 部署
- Dell.Configuration.Perform host-related tasks
 - 从 Dell 服务器管理选项卡中闪烁 LED、清除 LED、配置 OMSA URL
 - 启动 OMSA 控制台
 - 启动 iDRAC 控制台
 - 显示和清除 SEL 日志
- Dell.Inventory.Configure Inventory
 - 在 Dell 服务器管理选项卡上显示系统资源清册
 - 获得存储详细信息
 - 获得电源监测详细信息

- 在连接配置文件页上的创建、显示、编辑、删除和测试连接配置文件
- 计划、更新和删除资源清册计划
- 在主机上运行资源清册

故障排除

通过本节内容查找故障排除问题的答案。本部分包括：

- [常见问题 \(FAQ\)](#)
- [裸机部署问题](#)

主题：

- [常见问题 \(FAQ\)](#)
- [裸机部署问题](#)

常见问题 (FAQ)

本节介绍一些常见问题及解决方案。

为什么在 Google Chrome 中“全部导出”按钮无法导出到 .csv 文件？

注册 vCenter 服务器后，如果您添加主机并创建连接配置文件，然后查看主机的资源清册详细信息，则**全部导出**按钮将返回失败。**全部导出**按钮不会将信息导出到 .csv 文件。

① 注：

在所有版本的 Google Chrome 浏览器中，**全部导出**按钮都不会在**匿名模式**中将信息导出到 .csv 文件。

解决方案：要在 Google Chrome 中使用**全部导出**按钮将信息导出到 .csv 文件，请在 Chrome 浏览器中禁用**匿名模式**。

受影响的版本：4.0

对于不兼容的 vSphere 主机，iDRAC 许可证类型和说明显示不正确

如果主机不兼容，则当 CSIOR 被禁用或尚未运行时，显示的 iDRAC 许可证信息将不正确，尽管有效的 iDRAC 许可证可用。因此，您可以在 vSphere 主机列表中查看主机，但当您单击主机查看详细信息时，**iDRAC 许可证类型**中显示的信息为空白，并且 **iDRAC 许可证说明**中显示“您的许可证需要升级”。

解决方案：要解决此问题，请在参考服务器上启用 CSIOR。

受影响的版本：4.0

从较早的 OMIVV 版本注销 vCenter 后将不显示 Dell EMC 图标，然后用更高的 OMIVV 版本注册相同的 vCenter

如果注销 vCenter 服务器的旧版 OMIVV 并在同一台 vCenter 服务器上注册更高版本的 OMIVV，则会在 vsphere-client-serenity 文件夹中出现一个条目，其中包含来自旧版 OMIVV 的旧数据。因此，在注册更高版本的 OMIVV 后不会显示 Dell 图标，因为特定于旧版 OMIVV 的旧数据仍在 vCenter 设备的 vsphere-client-serenity 文件夹中。

解决方案：执行以下步骤：

- 1 对于 VMware vCenter，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-3.0.0.197`
- 2 手动删除与旧版 OMIVV 相应的文件夹。
- 3 在 vCenter 服务器上重新启动 vSphere Web 客户端服务。

受影响的版本：所有

每次调用时配置向导设置都会被默认设置覆盖

配置资源清册后、保修检索计划、初始配置向导中的事件和警报后，再次重新启动配置向导，那么以前的资源清册和保修检索计划将不会保留。每次调用配置向导时，资源清册和保修计划会重设为默认设置，而事件和警报则保留已更新的设置。

解决方案/解决办法：在完成向导功能之前复制资源清册和保修计划页面中以前的计划，以便以前的计划不会被默认设置覆盖。

受影响的版本：3.0 及更高版本

为什么 Dell Inc 未作为运行状况更新提供商显示

使用 OMIVV 注册 vCenter 服务器并升级 vCenter 服务器版本（例如从 vCenter 6.0 升级到 vCenter 6.5）后，Dell 提供商未显示在**主动式高可用性提供商**列表中。

解决方案：您可以升级非管理员用户或管理员用户注册的 vCenter。要升级到最新版本的 vCenter 服务器，请参阅 VMware 说明文件，然后执行以下任一选项（如果适用）：

- 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](#)。
 - b 重新引导已注册的 OMIVV 设备。
 - c 从 Web 客户端注销，然后再次登录。
- 对于管理员用户：
 - a 重新引导已注册的 OMIVV 设备。
 - b 从 Web 客户端注销，然后再次登录。

Dell 提供商现在会列示在**主动式高可用性提供商**列表中。

受影响的版本：4.0

为什么在 ESXi 5.x 主机上资源清册执行固件更新失败？

注册 vCenter 服务器后，如果您在 ESXi 5.x 主机上执行固件更新任务并从**选择组件**屏幕中选择 iDRAC 作为组件，则主机中的 ESXi 可能不会与新的 iDRAC IP 同步，因此会导致向 OMIVV 提供无效的 iDRAC IP。因此，您将无法在该主机上成功运行资源清册。

解决方案：要解决此问题，请在 ESXi 主机上重新启动 sfcd 守护程序。有关详情，请参阅 https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2077693。

受影响的版本：4.0

主机资源清册或测试连接由于 iDRAC IP 无效或未知而导致失败。如何获得一个有效的 iDRAC IP？

关于此任务

主机资源清册或测试连接由于 iDRAC IP 无效或未知而导致失败并且您诸如以下错误消息，例如“网络延迟或无法获取主机”、“连接被拒绝”、“操作已超时”、“WSMAN”、“未路由到主机”以及“IP 地址：空值”。

步骤

- 1 打开 iDRAC 虚拟控制台。
- 2 按下 F2 并导航至**故障排除选项**。
- 3 在**故障排除选项**中，导航至**重新启动管理代理程序**。
- 4 要重新启动管理代理程序，按 F11 键。

现在将获得一个有效的 iDRAC IP。

① **注：**当 OMIVV 无法在运行 ESXi 6.5 的主机上启用 WBEM 服务时，主机资源清册也可能发生故障。有关 WBEM 服务的更多信息，请参阅[创建连接配置文件](#)。

运行修复不兼容的 vSphere 主机向导时，为什么特定主机的状态显示为“未知”？

运行修复不兼容的 vSphere 主机向导以修复不兼容的主机时，特定主机的状态显示为“未知”。无法访问 iDRAC 时，将会显示“未知状态”。

解决方案：验证主机的 iDRAC 连接，并确保成功运行资源清册。

受影响的版本：4.0

在注册 OMIVV 设备时分配的 Dell 权限，在取消注册 OMIVV 后不会删除

在注册 vCenter 与 OMIVV 设备后，多个 Dell 权限添加至 vCenter 权限列表。一旦您从 OMIVV 设备中注销 vCenter，Dell 权限不会删除。

① **注：**虽然 Dell 权限不会删除，这不会影响任何 OMIVV 操作。

受影响的版本：3.1 版

尝试筛选严重性类别时，Dell Management Center 不显示所有相关日志。我该如何查看所有日志？

当您从下拉菜单中选择**所有类别**以选择用于筛选日志数据的严重性类别时，会准确显示属于特定类别的所有日志。但如果通过从下拉列表中选择**信息**进行筛选，则不会显示固件更新日志，而只显示任务启动日志。

解决方案：要在 Dell Management Center 中查看所有日志，请从“筛选器”下拉列表中选择**所有类别**。

受影响的版本：3.1 版

如何解决 VMware 证书颁发机构 (VMCA) 导致的错误代码 2000000 ？

当您运行 vSphere 证书管理器和更换 vCenter 服务器或平台控制器服务 (PSC) 证书为新的 CA 证书和 vCenter 6.0 密钥时，OMIVV 显示错误代码 2000000 并引发异常。

解决方案：要解决此异常，您应更新服务的 ssl 锚。ssl 锚可通过在 PSC 上运行 `ls_update_certs.py` 脚本进行更新。脚本将旧证书记录指纹用作输入参数，且新证书已安装。旧证书是更换前的证书，新证书是更换后的证书。请访问 http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701 和 http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121689 了解更多信息。

在 Windows vSphere 6.0 中更新 ssl 锚

- 1 从 http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701 下载 `Istoolutil.py.zip` 文件。
- 2 将 `Istoolutil.py` 文件复制至 `%VMWARE_CIS_HOME%\VMware Identity Services\Istool\scripts\` 文件夹。

注：如果您正在使用 vSphere 6.0 Update 1，请勿更换 `Istoolutil.py` 文件。

您可以使用以下相关步骤更新 ssl 锚：

- 更新安装在 Windows 操作系统中的 vCenter ssl 锚：使用 vSphere 证书管理器公用程序更换 vCenter Windows 安装上的证书。请参阅 [更换 vCenter Windows 安装中的证书](#)。
- 更新 vCenter 服务器设备的 ssl 锚：使用 vSphere 证书管理器公用程序更换 vCenter 服务器设备的证书。请参阅 [更换 vCenter 服务器设备上的证书](#)。

从上述提及的步骤中获得的输出应分别显示更新了 24 项服务和更新了 26 项服务。如果输出显示更新了 0 项服务，旧证书指纹不正确。您可以执行以下步骤以检索旧证书指纹。如果未使用 **vCenter 证书管理器** 来更换证书，也请使用以下步骤以检索旧证书指纹：

注：使用获得的旧指纹运行 `ls_update_certs.py`。

- 1 检索管理对象浏览器 (MOB) 中的旧证书。请参阅 [检索管理对象浏览器 \(MOB\) 中的旧证书](#)。
- 2 从旧证书中提取指纹。请参阅 [从旧证书中提取指纹](#)。

受影响的版本：3.0 和更高版本，vCenter 6.0 和更高版本

更换 vCenter Windows 安装中的证书

关于此任务

如果在安装 vCenter Windows 时使用 vSphere Certificate Manager 公用程序更换证书，请执行以下步骤：

步骤

- 1 通过远程桌面连接连接到外部平台服务控制器。
- 2 在管理模式下打开命令提示符。
- 3 使用以下命令创建 c:\certificates 文件夹: `mkdir c:\certificates`
- 4 使用以下命令检索旧证书: `"%VMWARE_CIS_HOME%\vmafdd\vecs-cli entry getcert --store BACKUP_STORE --alias bkp__MACHINE_CERT --output c:\certificates\old_machine.crt`
- 5 使用以下命令检索旧证书的指纹记录: `"%VMWARE_OPENSSL_BIN%" x509 -in C:\certificates\old_machine.crt -noout -sha1 -fingerprint`

注: 检索到的证书指纹为以下格式: **SHA1 Fingerprint=13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88**

指纹由一系列数字和字母组成, 如下所示: 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88

- 6 使用以下命令检索新证书: `"%VMWARE_CIS_HOME%\vmafdd\vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT --output c:\certificates\new_machine.crt`
- 7 执行以下步骤:
 - a 使用命令 `"%VMWARE_PYTHON_BIN%" ls_update_certs.py --url 运行 ls_update_certs.py`
 - b 使用命令 `https://psc.vmware.com/lookupservice/sdk --fingerprint 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 --certfile c:\certificates\new_machine.crt --user Administrator@vsphere.local --password Password`, 将 `psc.vmware.com` 替换为 `Lookup_Service_FQDN_of_Platform_Services_Controller`, 将 `13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88` 指纹替换为在第 5 步中获得的指纹。

注: 确保提供有效的凭据。

- 8 在所有服务成功更新后, 注销并重新登录 vCenter Web 客户端。

后续步骤

OMIVV 现已成功启动。

更换 vCenter 服务器设备上的证书

关于此任务

如果使用 vSphere 证书管理器公用程序更换 vCenter 服务器设备上的证书, 请执行以下步骤:

步骤

- 1 通过控制台或 secure shell (SSH) 会话登录到外部平台服务控制器设备。
- 2 运行以下命令以启用访问 Bash shell: `shell.set --enabled true`
- 3 键入 `shell` 并按 **Enter** 键。
- 4 使用以下命令创建文件夹或证书: `mkdir /certificates`
- 5 使用以下命令检索旧证书: `/usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store BACKUP_STORE --alias bkp__MACHINE_CERT --output /certificates/old_machine.crt`
- 6 使用以下命令检索旧证书指纹: `openssl x509 -in /certificates/old_machine.crt -noout -sha1 -fingerprint`

注: 检索到的证书指纹为以下格式: **SHA1 Fingerprint=13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88**

指纹由一系列数字和字母组成, 如下所示: 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88

- 7 使用以下命令检索新证书: `/usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT --output /certificates/new_machine.crt`

- 8 运行以下命令切换目录：`cd /usr/lib/vmidentity/tools/scripts/`
- 9 执行以下步骤：
 - a 使用命令 `python ls_update_certs.py --url`，运行 `ls_update_certs.py`
 - b 使用命令 `https://psc.vmware.com/lookupservice/sdk --fingerprint 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 --certfile /certificates/new_machine.crt --user Administrator@vsphere.local --password "Password"`，将 `psc.vmware.com` 替换为 `Lookup_Service_FQDN_of_Platform_Services_Controller`，并将 `13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88` 指纹替换为在步骤 6 中获得的指纹

注：确保提供有效的凭据。

- 10 在所有服务成功更新后，注销并重新登录 vCenter Web 客户端。

后续步骤

OMIVV 现已成功启动。

检索管理对象浏览器 (MOB) 中的旧证书

您可以使用管理对象浏览器 (MOB) 连接平台服务控制器 (PSC)，以为 vCenter 中心系统检索旧证书。

关于此任务

要检索旧证书，您应执行以下步骤查找 `ArrayOfLookupServiceRegistrationInfo` 管理对象的 `sslTrust` 字段：

注：在本指南中，`C:\certificates\` 文件夹位置用于存储所有证书。

步骤

- 1 使用以下命令在 PSC 上创建 `C:\certificates\` 文件夹：`mkdir C:\certificates\`
- 2 在浏览器中打开以下链接：`https://<vCenter FQDN|IP 地址>/lookupservice/mob?moid=ServiceRegistration&method=List`
- 3 使用 `administrator@vsphere.local` 用户名登录，在出现提示时提供密码。

注：如果您的 vCenter 单一登录 (SSO) 域使用的是自定义名称，使用该用户名和密码。
- 4 在 `filterCriteria` 中，修改值字段为仅显示标签 `<filtercriteria></filtercriteria>`，然后单击调用方法。
- 5 根据您要更换的证书搜索以下主机名：

表. 40: 搜索条件信息

信任锚	搜索条件
vCenter 服务器	使用 Ctrl+F 在页面上搜索 <code>vc_hostname_or_IP.example.com</code>
平台服务控制器	使用 Ctrl+F 在页面上搜索 <code>psc_hostname_or_IP.example.com</code>

- 6 找到相应 `sslTrust` 字段的值。`sslTrust` 字段的值是旧证书的 Base64 编码字符串。
- 7 在更新平台服务控制器或 vCenter 服务器信任锚时，使用以下示例。

注：实际字符串明显缩短，以提高易读性。

- 对于 vCenter 服务器

表. 41: vCenter 服务器示例

名称	类型	值
<code>url</code>	<code>anyURI</code>	<code>https://vcenter.vmware.local:443/sdk</code>

- 对于平台服务控制器

表. 42: 平台服务控制器示例

名称	类型	值
url	anyURI	https://psc.vmware.local/sts/stsservice/vsphere.local

- 8 将 sslTrust 字段中的内容复制至文本文档，将文档保存为 old_machine.txt。
- 9 在文本编辑器中打开 old_machine.txt。
- 10 在 old_machine.txt 文件开头和结尾分别附加以下内容：
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
- 11 现在将 old_machine.txt 保存为 old_machine.crt。

后续步骤

您现在可以从该证书中提取指纹。

从旧证书中提取指纹

您可以使用下列选项，从旧证书中提取指纹并将其上传到平台服务：

- 使用证书查看器工具提取指纹。请参阅 [使用认证查看器工具提取证书指纹](#)。
- 在设备上使用命令行提取指纹。请参阅 [使用命令行提取指纹](#)。

使用认证查看器工具提取证书指纹

关于此任务

执行以下步骤以提取证书指纹：

步骤

- 1 在 Windows 中，双击 old_machine.txt 文件，以在 Windows 证书查看器中打开它。
- 2 在 Windows 证书查看器中，选择 **SHA1 指纹** 字段。
- 3 将指纹字符串复制到纯文本编辑器中，然后使用冒号更换空格或从字符串中移除空格。
例如，指纹字符串可显示为以下任何一种：
 - ea87e150bb96fbbe1fa95a3c1d75b48c30db7971
 - ea:87:e1:50:bb:96:fb:be:1f:a9:5a:3c:1d:75:b4:8c:30:db:79:71

使用命令行提取指纹

要在该设备上和安装 Windows 时使用命令行提取指纹，请参阅以下章节。

在 vCenter 服务器设备上使用命令行提取指纹

执行以下步骤：

- 1 在 C:\certificates\old_machine.crt 位置（在 [步骤 1: 检索旧证书的流程](#) 中创建）中，移动或上载 old_machine.crt 至 PSC。您可以使用 Windows Secure Copy (WinSCP) 或其他 SCP 客户端移动或上载证书。
- 2 通过 Secure Shell (SSH) 登录到外部平台服务控制器设备。
- 3 运行以下命令以启用对 Bash shell 的访问：shell.set --enabled true。
- 4 键入 shell 并按 **Enter** 键。
- 5 运行以下命令提取指纹：openssl x509 -in /certificates/old_machine.crt -noout -sha1 -fingerprint

① **注：**指纹显示为等号后的一系列数字和字母，如下所示：SHA1 Fingerprint= ea:87:e1:50:bb:96:fb:be:1f:a9:5a:3c:1d:75:b4:8c:30:db:79:71

安装 Windows 时使用命令行提取指纹

执行以下步骤：

- 1 在 C:\certificates\old_machine.crt 位置（在步骤 1：检索旧证书的流程中创建）中，移动或上载 old_machine.crt 至 PSC。您可以使用 Windows Secure Copy (WinSCP) 或其他 SCP 客户端移动或上载证书。
- 2 通过远程桌面连接连接到外部平台服务控制器。
- 3 在管理模式下打开命令提示符。
- 4 运行以下命令提取指纹：`"%VMWARE_OPENSSL_BIN%" x509 -in c:\certificates\old_machine.crt -noout -sha1 -fingerprint`

① **注：**指纹显示为等号后的一系列数字和字母，如下所示：SHA1 Fingerprint=09:0A:B7:53:7C:D9:D2:35:1B:4D:6D:B8:37:77:E8:2E:48:CD:12:1B

使用旧指纹运行 ls_update_certs.py。成功更新服务后，注销并登录到 vCenter Web 客户端。已成功启动 Dell 插件。

在管理控制台中，将设备重设为出厂设置后，为何更新存储库路径未设置为默认路径？

重设设备后，转至**管理控制台**，然后单击左侧窗格中的**设备管理**。在**设备设置**页面中，**更新存储库路径**未更改为默认路径。

解决方案：在**管理控制台**中，将**默认更新存储库**字段中的路径手动复制到**更新存储库路径**字段。

为什么不能对从作业队列页面中选择的所有 vCenter 应用保修和资源清册计划？

导航至 **Dell 主页 > 监测 > 作业队列 > 保修/资源清册历史记录 > 计划**。选择 vCenter，然后选择“修改计划”按钮。当显示对话框时，您可以看到一个复选框和**应用到所有已注册的 vCenter** 消息。当您选中此复选框并按**应用**时，设置即会应用到您最初选择的特定 vCenter 而不是所有 vCenter。从**作业队列**页面修改保修或资源清册计划时，**应用到所有已注册的 vCenter** 不适用。

解决方案：使用作业队列中的修改保修或资源清册计划时，仅修改选定的 vCenter。

受影响的版本：2.2 及更高版本

在 OMIVV 中更改 DNS 设置后在 vCenter Web 客户端中出现 Web 通信错误时该怎么办？

更改 DNS 设置后，如果您在执行任何 OMIVV 相关任务时在 vCenter Web 客户端中看到任何类型的 Web 通信错误，请执行以下操作之一：

- 清除浏览器高速缓存。
- 从 Web 客户端中注销，然后重新登录。

如果离开再返回设置页面，为何设置页面无法加载？

对于 vSphere v5.5，在 Web 客户端中，如果离开再返回设置页面，该页面可能无法加载，而微调框继续显示。无法加载是刷新问题，该页面未能正确刷新。

解决方案：单击全局刷新，屏幕将正确刷新。

受影响的版本：2.2 和 3.0

在初始配置向导的资源清册计划/保修计划页面中，为何会显示“无法计划在过去的时间内执行任务”错误？

在 Web 客户端中，在下列情况下会显示“无法计划在过去的时间内执行任务”错误：

- 如果您在“初始设置”向导中选择“所有已注册的 vCenter”，并且存在没有主机的 vCenter。
- 当 vCenter 中的一部分已计划资源清册或保修任务时。
- 当一部分 vCenter 尚未设置资源清册或保修计划时。

解决方案：再次分别从这些 vCenter 的设置页面运行资源清册和保修计划设置。

受影响的版本：2.2 及更高版本

在固件页面中，一些固件的安装日期为何显示为 12/31/1969？

在 Web 客户端中，主机固件页面上的一些固件项目的安装日期显示为 12/31/1969。如果固件安装日期不可用，将会显示该旧日期。

解决方案：如果看到任意固件组件显示该久远日期，则表示该组件的安装日期不可用。

受影响的版本：2.2 及更高版本

连续全局刷新会导致“最近的任务”窗口引发异常。如何解决此错误？

如果您反复按刷新按钮，VMware UI 可能会引发异常。

解决方案：您可以忽略此错误，并可继续。

受影响的版本：2.2 及更高版本

为什么在 IE 10 中少数 Dell 屏幕中的 Web 客户端 UI 会失真？

有时在显示弹出式对话框时，后台数据可能变为白色并且变形。

解决方案：关闭对话框，屏幕将恢复正常。

受影响的版本：2.2 及更高版本

为何即使 OpenManage Integration 插件已成功注册到 vCenter，我在 Web 客户端上仍然看不到 OpenManage Integration 图标？

OpenManage Integration 图标未显示在 Web 客户端中，除非 vCenter Web 客户端服务重新启动或 Box 重新引导。注册 OpenManage Integration for VMware vCenter 设备时，设备在桌面客户端和 Web 客户端均注册。如果注销设备后重新注册设备的相同版本或注册新版本，它可以成功注册两种客户端，但 Web 客户端中可能无法显示 Dell 图标。这是由于 VMware 的缓存问题。要解决该问题，请确保重新启动 vCenter 服务器上的 Web 客户端服务。然后，插件会在用户界面中显示。

解决方案：重新启动 vCenter 服务器上的 Web 客户端服务。

受影响的版本：2.2 及更高版本

即便我的存储库中包含所选 11G 系统的捆绑包，为何固件更新显示没有固件更新的捆绑包？

当我在锁定模式下将一个主机添加到连接配置文件时，资源清册开始，但随后失败，并指示“未找到远程访问控制器或在本主机上不支持资源清册”。资源清册应该可用于锁定模式的主机。

如果您将主机置于锁定模式或从锁定模式中移除主机，请确保等待 30 分钟后才能执行下一次操作。如果您使用第 11 代主机进行固件更新，则固件更新向导将不显示任何捆绑包，即使存储库有该系统的捆绑包。发生这种情况的原因可能是第 11 代主机尚未将 OMSA 配置向 OpenManage Integration 发送陷阱。

解决方案：通过使用 OpenManage Integration Web 客户端的主机符合性向导确保主机兼容。如果不兼容，则使用的修复主机兼容性来使其兼容。

受影响的版本：2.2 及更高版本

如果使用 DHCP 值覆盖设备 IP 和 DNS 设置，为什么要在设备重新引导后将 DNS 配置设置到原始设置

这是一个已知缺陷，其中静态分配的 DNS 设置将被 DHCP 中的值覆盖。使用 DHCP 获取 IP 设置并静态分配 DNS 值时会发生此问题。续订 DHCP 租赁或重新启动设备时，静态分配的 DNS 设置会被移除。

解决方案：当 DNS 服务器设置与 DHCP 不同时，静态分配 IP 设置。

受影响的版本：所有

不支持使用 OMIVV 更新固件版本为 13.5.2 的 Intel 网卡

这是 Dell PowerEdge 第 12 代服务器和固件版本为 13.5.2 的部分 Intel 网卡的已知问题。使用 Lifecycle Controller 应用固件更新时，更新具有此固件版本的部分 Intel 网卡会失败。使用此固件版本的客户必须使用操作系统更新网络驱动程序软件。如果 Intel 网卡的固件

版本是除 13.5.2 以外的其他版本，您可以使用 OMIVV 进行更新。有关更多信息，请参阅 <http://en.community.dell.com/techcenter/b/techcenter/archive/2013/03/20/intel-network-controller-card-with-v13-5-2-firmware-cannot-be-upgraded-using-lifecycle-controller-to-v13-5-6.aspx>

① **注：**当使用一对多固件更新时，请避免选择版本为 13.5.2 的 Intel 网络适配器，因为此时更新将会失败，并会阻止更新任务更新剩余的服务器。

由于 DUP 存在分段要求，使用 OMIVV 将 Intel 网卡从 14.5 或 15.0 更新至 16.x 失败

这是 NIC 14.5 和 15.0 中的已知问题。将固件更新到 16.x 之前，确保使用自定义目录将固件更新到 15.5.0。

受影响的版本：所有

为什么在尝试使用无效的 DUP 执行固件更新时，尽管 LC 中的作业状态显示“失败”，但 vCenter 控制台上的硬件更新作业状态在数小时内既非失败也非超时？

当选择了无效的 DUP 进行固件更新时，vCenter 控制台窗口中的任务状态保持为“正在进行”，但消息更改为失败原因。这是已知的 VMware 缺陷，将在未来的 VMware vCenter 版本中修复。

解决方案：必须手动取消该任务。

受影响的版本：所有

为什么“管理控制台”显示无法获取更新存储库位置？

如果您提供一个无法获取的更新存储库路径，则会在“设备更新”视图中显示。“失败：连接到 URL 时出错...”错误消息。但是，更新前，“更新存储库路径”未明确为该值。

解决方案：离开此页面进入另一个页面，并确保该页面刷新。

受影响的版本：所有

当我执行一对多固件更新时，为什么系统无法进入维护模式？

一些固件更新不需要重新引导主机。在该情况下，在执行固件更新时不会将主机置于维护模式。

为什么在一些电源设备状态已变为严重时，机箱全局运行状况仍然为良好？

有关机箱的全局运行状况在电源设备方面基于冗余策略以及机箱的电源需求是否满足仍联机并正常工作的 PSU。因此，即使有些 PSU 断电，仍然满足机箱的整体电源要求。因此，机箱的全局运行状况是良好。有关电源设备和电源管理的更多详细信息，请查找用户指南中的 Dell PowerEdge M1000e Chassis Management Controller 固件说明文件。

为什么在“系统概览”页面的“处理器视图”中处理器版本中为“不适用”？

在 PowerEdge 第 12 代 Dell 服务器和更高版本中，处理器版本列在“品牌”列中。在更低版本的服务器中，处理器版本显示在“版本”列中。

OMIVV 配置和支持哪一代 Dell 服务器的 SNMP 陷阱？

OMIVV 在 12 代以前的服务器上支持 OMSA SNMP 陷阱，在第 12 代服务器上支持 iDRAC 陷阱。

OMIVV 管理哪些 vCenter 服务器？

OMIVV 只管理已注册的 vCenter 服务器，处于链接模式或不在链接模式下皆可。

OMIVV 是否支持处于链接模式的 vCenter ？

是，OMIVV 支持最多 10 个 vCenter 服务器，处于链接模式或不在链接模式下皆可。有关 OMIVV 在链接模式下如何运行的更多信息，请参阅白色白皮书 *OpenManage Integration for VMware vCenter：在链接模式下运行* (www.dell.com)。

什么是 OMIVV 所需的端口设置？

① 注：在 OMIVV 中使用兼容性窗口中提供的修复不兼容的 vSphere 主机链接部署 OMSA 代理程序时，OMIVV 会在 ESXI 5.0 更高版本上启动 http 客户端服务并启用端口 8080，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。

使用 OMIVV 的以下端口设置：

表. 43: 虚拟设备端口

端口号	协议	端口类型	最大加密级别	方向	使用情况	可配置
21	FTP	TCP	无	出	FTP 命令客户端	否
53	DNS	TCP	无	出	DNS 客户端	否
80	HTTP	TCP	无	出	Dell 联机数据访问	否
80	HTTP	TCP	无	进	管理控制台	否
162	SNMP 代理	UDP	无	进	SNMP 代理（服务器）	否
11620	SNMP 代理	UDP	无	进	SNMP 代理（服务器）	否
443	HTTPS	TCP	128 位	进	HTTPS 服务器	否

端口号	协议	端口类型	最大加密级别	方向	使用情况	可配置
443	WSMAN	TCP	128 位	进/出	iDRAC/OMSA 通信	否
4433	HTTPS	TCP	128 位	进	自动查找	否
2049	NFS	UDP	无	进/出	公共共享	否
4001 - 4004	NFS	UDP	无	进/出	公共共享	否
11620	SNMP 代理	UDP	无	进	SNMP 代理 (服务器)	否

表. 44: 受管节点

端口号	协议	端口类型	最大加密级别	方向	使用情况	可配置
162, 11620	SNMP	UDP	无	出	硬件事件	否
443	WSMAN	TCP	128 位	进	iDRAC/OMSA 通信	否
2049	NFS	UDP	无	进/出	公共共享	否
4001 - 4004	NFS	UDP	无	进/出	公共共享	否
443	HTTPS	TCP	128 位	进	HTTPS 服务器	否
4433	HTTPS	TCP	128 位	出	自动查找	否
8080	HTTP	TCP		进	HTTP 服务器； 下载 OMSA VIB 并修复不符合要求的 vSphere 主机	否
50	RMCP	UDP/TCP	128 位	出	远程邮件检查协议	否
51	IMP	UDP/TCP	不适用	不适用	IMP 逻辑地址维护	否
5353	mDNS	UDP/TCP		进/出	多播 DNS	否
631	IPP	UDP/TCP	无	出	因特网打印协议 (IPP)	否
69	TFTP	UDP	128 位	进/出	普通文件传输	否
111	NFS	UDP/TCP	128 位	进	SUN 远程过程调用 (Portmap)	否
68	bootp	UDP	无	出	自举协议客户端	否

硬件配置文件或系统配置文件的用户具有 iDRAC 用户列表中的新更改凭据，在成功应用该配置文件后，用于裸机查找的相同用户的密码为什么未更改？

如果仅选择了硬件配置文件模板用于部署，则用于查找的用户的密码不会更改到新的凭据中。这是有意设置的，以便插件能够与 iDRAC 进行通信，从而用于满足未来的部署需求。

为什么无法在“vCenter 主机和群集”页面上查看新 iDRAC 版本的详细信息？

解决方案：在 vSphere Web 客户端中成功完成固件更新任务后，刷新**固件更新**页面并验证固件版本。如果页面显示旧版本，请转至 OpenManage Integration for VMware vCenter 中的**主机合规性**页面，然后查看主机的 CSIOR 状态。如果 CSIOR 未启用，请启用 CSIOR 并重新引导主机。如果已启用 CSIOR，请登录到 iDRAC 控制台、重设 iDRAC，并在等待几分钟后刷新**固件更新**页面。

我如何使用 OMSA 模拟温度硬件故障来测试事件设置？

关于此任务

要确保事件工作正常，请执行下列步骤：

步骤

- 1 在 OMSA 用户界面中，导航至**警报管理 > 平台事件**。
- 2 选中**启用平台事件筛选器警报**复选框。
- 3 向下滚动至底部，单击**应用更改**。
- 4 要确保启用特定事件（例如温度警告），请从左侧树中选择**主系统机箱**。
- 5 在**主系统机箱**下选择**温度**。
- 6 选择 **警报管理**选项卡，然后选择 **温度探测器警告**。
- 7 选择 **广播一条消息**复选框，然后选择 **应用更改**。
- 8 要引发温度警告事件，请从左侧的树视图中选择**主系统机箱**。
- 9 在 **主系统机箱**下选择 **温度**。
- 10 选择 **系统板环境温度**链接，然后选择 **设置为值**选项按钮。
- 11 将**最大警告阈值**设置为小于当前所列读数的值。
例如，如果当前读数为 27，则将阈值设为 **25**。
- 12 选择**应用更改**，并生成温度警告事件。
要造成另一个事件，请通过使用相同的**设置为值**选项来还原为原始设置。将事件生成成为警告后，再升级到正常状态。如果一切运行正常，则导航至 **vCenter 任务与事件**视图；系统上应显示温度探测器警告事件。

① **注：**有一个针对重复事件的筛选器；如果您连续尝试触发同一个事件，则只会收到一个事件。在不同事件之间至少保持 30 秒的间隔时间才能看到所有事件。

尽管 OMIVV 主机系统上已安装 OMSA 代理程序，我仍然收到 OMSA 未安装的错误消息。如何处理该错误？

关于此任务

要在第 11 代服务器上解决此问题，请执行以下操作：

步骤

- 1 在主机系统上安装包含有 **远程启用**组件的 **OMSA**。
- 2 如果您使用命令行安装 OMSA，请确保指定 **-c option**。如果已安装 OMSA，请使用 **-c option** 重新进行安装，并且重新启动服务：

```
srvadmin-install.sh -c
srvadmin-services.sh restart
```

对于 ESXi 主机，请确保使用 **VMware Remote CLI 工具**安装 **OMSA VIB**，然后重新引导系统。

OMIVV 已启用锁定模式的情况下是否支持 ESXi ?

可以。此版本支持 ESXi 5.0 及更高版本主机中的锁定模式。

在我尝试使用锁定模式时失败

当我在锁定模式下将一个主机添加到连接配置文件时，资源清册开始，但随后失败，并指示“未找到远程访问控制器或在本主机上不支持资源清册”。

如果您将主机置于锁定模式或从锁定模式中移除主机，请确保等待 30 分钟后才能对 OMIVV 执行下一次操作。

如果在使用参考服务器的情况下创建硬件配置文件失败该怎么办？

检查以确保已安装了建议的最低版本的 iDRAC 固件、Lifecycle Controller 固件和 BIOS。

为确保从参考服务器检索的数据是最新的，请启用**重新启动时收集系统资源清册 (CSIOR)**，并在重新启动参考服务器后再提取数据。

为什么尝试在服务器上部署 ESXi 失败？

- 1 确保 **ISO 位置 (NFS 路径)** 和**分级文件夹路径**准确无误。
- 2 确保在分配服务器标识时选择的 **NIC** 与虚拟设备在同一个网络上。
- 3 如果使用**静态 IP 地址**，请确保提供准确无误的网络信息（包括子网掩码和默认网关）。此外，请确保尚未在网络上分配 IP 地址。
- 4 请确保系统可以看到至少一个**虚拟磁盘**。
ESXi 也安装到内部 SD 卡。

为什么我的虚拟机监控程序在 Dell PowerEdge R210 II 机器上部署失败？

由于从所连接的 ISO 引导时 BIOS 发生故障，在 Dell PowerEdge R210 II 系统上的超时问题导致虚拟机监控程序部署失败错误。

解决方案：在机器上手动安装虚拟机监控程序。

为什么部署向导中自动发现的系统未显示型号信息？

这通常表示系统上安装的固件版本不符合建议的最低要求。有时，系统上可能未注册固件更新。

解决方案：冷引导系统或重新安装刀片可解决此问题。必须禁用 iDRAC 上新启用的帐户并重新初始化自动查找，以便向 OMIVV 提供型号信息和 NIC 信息。

NFS 共享设置了 ESXi ISO，但装载共享位置错误造成部署失败

关于此任务

要查找解决方案：

步骤

- 1 确保 iDRAC 能够 ping 到设备。
- 2 确保您的网络运行速度不是太慢。
- 3 确保端口：2049、4001 - 4004 打开，并相应调整了防火墙设置。

我如何强制移除虚拟设备？

- 1 转到 **Https://<vcenter_serverIPAddress>/mob**
- 2 输入 VMware vCenter 管理凭据。
- 3 单击**内容**。
- 4 单击 **ExtensionManager**。
- 5 单击 **UnregisterExtension**。
- 6 输入扩展密钥以注销 com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient，然后单击**调用方法**。
- 7 在 vSphere Web 客户端中，关闭 OMIVV 并将其删除。要注销的密钥必须适用于 Web 客户端。

在“立即备份”屏幕中输入密码时收到错误消息

如果您使用的是低分辨率显示器，则无法从“立即备份”窗口中看到“加密密码”字段。您必须向下滚动页面来输入加密密码。

在 vSphere Web 客户端中，单击 Dell Server Management Portlet 或 Dell 图标时返回 404 错误

检查 OMIVV 设备是否正在运行，否则，从 vSphere Web 客户端重新启动该设备。请等待几分钟以便虚拟设备 Web 服务启动，然后刷新页面。如果错误依然存在，则从命令行使用 IP 地址或完全限定域名尝试对该设备执行 ping 操作。如果 ping 操作未解决该问题，请查看您的网络设置，确保它们正确。

如果固件更新失败应该怎么办？

检查虚拟设备日志以查看任务是否已超时。如果是这样，必须通过执行冷重新引导重设 iDRAC。系统启动并运行后，请通过运行资源清册或使用**固件**选项卡进行检查以查看更新是否成功。

如果 vCenter 注册失败，应该怎么办？

vCenter 注册失败可能是因为通信问题，因此，如果您遇到这些问题，一种解决方案是使用静态 IP 地址。要使用静态 IP 地址，请在 OpenManage Integration for VMware vCenter 的“控制台”选项卡中，选择**配置网络 > 编辑设备**，然后输入正确的**网关**和**FQDN**（完全限定域名）。在“编辑 DNS 配置”下编辑 DNS 服务器名称。

① | 注: 确保虚拟设备可以解析您输入的 DNS 服务器。

连接配置文件测试凭据的性能缓慢或没有响应

关于此任务

服务器上的 iDRAC 只有一个用户（例如，仅 *root*），并且用户处于禁用状态，或者所有用户处于禁用状态。服务器通信处于禁用状态造成延迟。要解决此问题，您可以修复服务器禁用状态，或重设服务器上的 iDRAC 以将 *root* 用户重新启用为默认设置。

要修复禁用状态的服务器：

步骤

- 1 打开机箱管理控制器控制台并选择禁用的服务器。
- 2 要自动打开 iDRAC 控制台，请单击 **启动 iDRAC GUI**。
- 3 导航至 iDRAC 控制台内的用户列表，然后单击以下其中一项：
 - iDRAC 6：选择 **iDRAC 设置 > 网络/安全选项卡 > 用户选项卡**。
 - iDRAC 7：选择 **iDRAC 设置 > 用户选项卡**。
 - iDRAC 8：选择 **iDRAC 设置 > 用户选项卡**。
- 4 要编辑设置，在用户 ID 列中，单击 *admin (root)* 用户的链接。
- 5 单击 **配置用户**，然后单击 **下一步**。
- 6 在所选用户的 **用户配置** 页面中，选择“启用用户”旁边的复选框，然后单击 **应用**。

OMIVV 是否支持 VMware vCenter 服务器设备？

是，OMIVV 支持 VMware vCenter 服务器设备 v2.1 及更高版本。

为什么在我使用“在下次重新引导时应用”选项执行了固件更新并且重新引导系统后，我的固件级别未更新？

要更新固件，请在重新引导完成后在主机上运行资源清册。有时，重新引导事件未到达设备，因此没有自动触发资源清册。在这种情况下，您必须手动重新运行资源清册以获得更新的固件版本。

为什么在从 vCenter 树中移除主机后主机仍显示在机箱下？

机箱下的主机标识为机箱资源清册的一部分。成功执行机箱资源清册后，机箱下的主机列表已更新。因此，即使已从 vCenter 树中移除主机，机箱下也不会显示主机，直到下一次机箱资源清册运行。

在管理控制台中，将设备重设为出厂设置后，为何更新存储库路径未设置为默认路径？

重设设备后，转至**管理控制台**，然后单击左侧窗格中的**设备管理**。在**设备设置**页面中，**更新存储库路径**未更改为默认路径。

解决方案：在**管理控制台**中，将**默认更新存储库**字段中的路径手动复制到**更新存储库路径**字段。

在备份和还原 OMIVV 后，为何警报设置没有被还原？

还原 OMIVV 设备备份不会还原所有警报设置。但是，在 OpenManage Integration for VMware GUI 中，**警报和事件**字段会显示还原后的设置。

解决方案：在 OpenManage Integration for VMware GUI 的**管理 > 设置**选项卡中，手动更改**事件和警报**设置。

当在目标节点上启用 NIC 分区 (NPAR) 并且在系统配置文件中禁用该分区时，虚拟机监控程序部署失败。

当在目标机器上应用具有禁用 NPAR 的系统配置文件时，虚拟机监控程序部署失败。在此处，在目标节点上启用了 NPAR。并且除分区 1 以外，在通过部署向导进行部署的过程中，仅有其中一个分区 NIC 选作管理任务的 NIC。

解决方案：如果在部署期间您正通过系统配置文件更改 NPAR 状态，请确保您在部署向导中仅选择用于管理网络的第一个分区。

受影响的版本：4.1

当可用版本低于当前版本时，可用的虚拟设备版本显示错误信息

在 OMIVV 管理控制台的**设备管理**下，**可用虚拟设备版本**显示模式 RPM 与 OVF 为可用。

① **注：**建议更新存储库路径设置为最新版本，并且降级虚拟设备版本不受支持。

裸机部署问题

本节介绍部署过程中发现的问题。

自动查找和握手前提条件

- 在运行自动查找和握手之前，确保 iDRAC、Lifecycle Controller 固件和 BIOS 版本符合最低建议版本要求。
- CSIOR 必须已经至少在系统或 iDRAC 上运行过一次。

硬件配置故障

- 在初始化部署任务之前，确保系统已完成了 CSIOR 并且没有在重新引导过程中。
- BIOS 配置应当在克隆模式中运行，以便引用的服务器是相同的系统。
- 一些控制器不允许创建带有一个驱动器的 RAID 0 阵列。此功能仅在高端控制器上受支持，并且此类硬件配置文件的应用程序可能会造成故障。

在新购买的系统上启用自动查找

关于此任务

主机系统的自动查找功能在默认情况下未启用；而必须在购买时申请启用。如果在购买时未申请启用自动查找，则会在 iDRAC 上启用 DHCP 并且禁用 admin 帐户。无需配置 iDRAC 的静态 IP 地址。它会从网络上的 DHCP 服务器获得一个。要使用自动查找功能，必须配置 DHCP 服务器或 DNS 服务器（或两者）以支持查找过程。CSIOR 在出厂过程中应当已经运行。

如果在购买时未申请自动查找，则可以通过以下步骤启用：

步骤

- 1 在引导例行程序中按 **Ctrl + E**。
- 2 在 iDRAC 设置窗口中，启用 NIC（仅刀片服务器）。
- 3 启用自动查找。
- 4 启用 DHCP。
- 5 禁用 admin 帐户。
- 6 启用 **从 DHCP 获取 DNS 服务器地址**。
- 7 启用 **从 DHCP 获取 DNS 域名**。
- 8 在 **配置服务器** 字段中，输入：
`<OpenManage Integration virtual appliance IPAddress>:4433`

相关说明文件

除本指南外，您还可以访问 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 4.1** 访问下列说明文件：

- *OpenManage Integration for VMware vCenter 4.1 版 Web 客户端用户指南*
- *OpenManage Integration for VMware vCenter 4.1 版发行说明*
- *OpenManage Integration for VMware vCenter 4.1 版兼容性值表*

您可以在 delltechcenter.com 上找到包含白皮书的技术资料。在 Dell TechCenter Wiki 主页上，单击**系统管理 > OpenManage Integration for VMware vCenter** 可以访问这些文章。

从 Dell 支持站点访问说明文件

您可以通过以下方式之一访问所需的说明文件：

- 使用以下链接：
 - 所有企业系统管理说明文件 — Dell.com/SoftwareSecurityManuals
 - OpenManage 说明文件 — Dell.com/OpenManageManuals
 - 远程企业系统管理说明文件 — Dell.com/esmanuals
 - iDRAC 和 Lifecycle Controller 说明文件 — Dell.com/idracmanuals
 - OpenManage Connections 企业系统管理说明文件 — Dell.com/OMConnectionsEnterpriseSystemsManagement
 - 适用性工具说明文件 — Dell.com/ServiceabilityTools
 - 客户端命令套件系统管理说明文件 — Dell.com/DellClientCommandSuiteManuals
 - OpenManage 虚拟化解决方案说明文件 — Dell.com/VirtualizationSolutions
- 从 Dell 支持网站：
 - a 转至 Dell.com/Support/Home。
 - b 单击**查看产品**，在**选择产品**部分下，单击**软件和安全**。
 - c 在**软件和安全**组框中，通过以下项单击所需的链接：
 - **企业系统管理**
 - **远程企业系统管理**
 - **Serviceability Tools**
 - **Dell 客户端命令套件**
 - **Connections 客户端系统管理**
 - **虚拟化解决方案**
 - d 要查看说明文件，请单击所需的产品版本。
- 使用搜索引擎：
 - 在搜索框中键入说明文件的名称和版本。

系统特定属性

iDRAC

表. 45: 系统特定属性 iDRAC

属性名称	显示属性名称	组显示名称
DNS RAC 名称	DNS RAC 名称	NIC 信息
数据中心名称	数据中心名称	服务器拓扑
过道名称	过道名称	服务器拓扑
机架名称	机架名称	服务器拓扑
机架插槽	机架插槽	服务器拓扑
RAC 名称	Active Directory RAC 名称	Active Directory
DNS 域名	DNS 域名	NIC 静态信息
地址	IPv4 地址	Ipv4 静态信息
网络掩码	网络掩码	Ipv4 静态信息
网关	网关	Ipv4 静态信息
DNS1	DNS 服务器 1	Ipv4 静态信息
DNS2	DNS 服务器 2	Ipv4 静态信息
地址 1	IPv6 地址 1	IPv6 静态信息
网关	IPv6 网关	IPv6 静态信息
前缀长度	IPv6 链路本地前缀长度	IPv6 静态信息
DNS1	IPv6 DNS 服务器 1	IPv6 静态信息
DNS2	IPv6 DNS 服务器 2	IPv6 静态信息
DNSFromDHCP6	来自 DHCP6 的 DNS 服务器	IPv6 静态信息
主机名	服务器主机名称	服务器操作系统
房间名称	房间名称	服务器拓扑
节点 ID	系统节点 ID	服务器信息

BIOS

表. 46: BIOS 的系统特定属性

属性名称	显示属性名称	组显示名称
资产标签	资产标签	其他设置
lscsiDev1Con1Gateway	启动器网关	连接 1 设置
lscsiDev1Con1Ip	启动器 IP 地址	连接 1 设置
lscsiDev1Con1Mask	启动器子网掩码	连接 1 设置
lscsiDev1Con1TargetIp	目标 IP 地址	连接 1 设置
lscsiDev1Con1TargetName	目标名称	连接 1 设置
lscsiDev1Con2Gateway	启动器网关	连接 1 设置
lscsiDev1Con2Ip	启动器 IP 地址	连接 1 设置
lscsiDev1Con2Mask	启动器子网掩码	连接 1 设置
lscsiDev1Con2TargetIp	目标 IP 地址	连接 1 设置
lscsiDev1Con2TargetName	目标名称	连接 1 设置
lscsiInitiatorName	iSCSI 启动器名称	网络设置
Ndc1PcieLink1	集成网卡 1 PCIe 链路 1	集成设备
Ndc1PcieLink2	集成网卡 1 PCIe 链路 2	集成设备
Ndc1PcieLink3	集成网卡 1 PCIe 链路 3	集成设备
UEFI 引导顺序	UEFI 引导顺序	UEFI 引导设置

RAID

表. 47: RAID 的系统特定属性

属性名称	显示属性名称	组显示名称
机柜请求配置模式	不适用	不适用
机柜当前配置模式	不适用	不适用

CNA

表. 48: CNA 的系统特定属性

属性名称	显示属性名称	组显示名称
ChapMutualAuth	CHAP 相互验证	iSCSI 通用参数
ConnectFirstTgt	连接	iSCSI 第一个目标参数
ConnectSecondTgt	连接	iSCSI 第二个目标参数
FirstFCoEBootTargetLUN	引导 LUN	FCoE 配置

属性名称	显示属性名称	组显示名称
FirstFCoEWWPNTarget	全局端口名称目标	FCoE 配置
FirstTgtBootLun	引导 LUN	iSCSI 第一个目标参数
FirstTgtChapId	CHAP ID	iSCSI 第一个目标参数
FirstTgtChapPwd	CHAP 机密	iSCSI 第一个目标参数
FirstTgtIpAddress	IP 地址	iSCSI 第一个目标参数
FirstTgtIscsiName	iSCSI 名称	iSCSI 第一个目标参数
FirstTgtTcpPort	TCP 端口	iSCSI 第一个目标参数
IP 自动配置	IpAutoConfig	iSCSI 通用参数
IscsilInitiatorChapId	CHAP ID	iSCSI 启动器参数
IscsilInitiatorChapPwd	CHAP 机密	iSCSI 启动器参数
IscsilInitiatorGateway	默认网关	iSCSI 启动器参数
IscsilInitiatorIpAddr	IP 地址	iSCSI 启动器参数
IscsilInitiatorIpv4Addr	IPv4 地址	iSCSI 启动器参数
IscsilInitiatorIpv4Gateway	IPv4 默认网关	iSCSI 启动器参数
IscsilInitiatorIpv4PrimDns	IPv4 主要 DNS	iSCSI 启动器参数
IscsilInitiatorIpv4SecDns	IPv4 次要 DNS	iSCSI 启动器参数
IscsilInitiatorIpv6Addr	IPv6 地址	iSCSI 启动器参数
IscsilInitiatorIpv6Gateway	IPv6 默认网关	iSCSI 启动器参数
IscsilInitiatorIpv6PrimDns	IPv6 主要 DNS	iSCSI 启动器参数
IscsilInitiatorIpv6SecDns	IPv6 次要 DNS	iSCSI 启动器参数
IscsilInitiatorName	iSCSI 名称	iSCSI 启动器参数
IscsilInitiatorPrimDns	主要 DNS	iSCSI 启动器参数
IscsilInitiatorSecDns	次要 DNS	iSCSI 启动器参数
IscsilInitiatorSubnet	子网掩码	iSCSI 启动器参数
IscsilInitiatorSubnetPrefix	子网掩码前缀	iSCSI 启动器参数
SecondaryDeviceMacAddr	第二设备 MAC 地址	iSCSI 第二设备参数
SecondTgtBootLun	引导 LUN	iSCSI 第二个目标参数
SecondTgtChapPwd	CHAP 机密	iSCSI 第二个目标参数
SecondTgtIpAddress	IP 地址	iSCSI 第二个目标参数
SecondTgtIscsiName	iSCSI 名称	iSCSI 第二个目标参数
SecondTgtTcpPort	TCP 端口	iSCSI 第二个目标参数
UseIndTgtName	使用独立的目标名称	iSCSI 第二设备参数
UseIndTgtPortal	使用独立的目标门户	iSCSI 第二设备参数
VirtFIPMacAddr	虚拟 FIP MAC 地址	主配置页面

属性名称	显示属性名称	组显示名称
VirtIscsiMacAddr	虚拟 iSCSI 卸载 MAC 地址	主配置页面
VirtMacAddr	虚拟 MAC 地址	主配置页面
VirtMacAddr[分区: n]	虚拟 MAC 地址	分区 n 配置
VirtWWN	虚拟全局节点名称	主配置页面
VirtWWN[分区: n]	虚拟全局节点名称	分区 n 配置
VirtWWPN	虚拟全局端口名称	主配置页面
VirtWWPN[分区: n]	虚拟全局端口名称	分区 n 配置
全局节点名称	WWN	主配置页面
全局节点名称	WWN[分区: n]	分区 n 配置

FC

表. 49: FC 的系统特定属性

属性名称	显示属性名称	组显示名称
VirtualWWN	虚拟全局节点名称	端口配置页面
VirtualWWPN	虚拟全局端口名称	端口配置页面

自定义属性

表. 50: 自定义属性

FGDD	属性	OMIVV 自定义
BIOS	虚拟化技术	始终启用
iDRAC	重新启动时收集系统资源清册	始终启用
RAID	IncludedPhysicalDiskID	如果 IncludedPhysicalDiskID 值是自动选择，那么将移除该值
RAID	RAIDPDState	已移除
iDRAC	用户管理员密码 密码	仅启用 iDRAC 的用户将具有“密码”链接以输入密码。

附加信息

以下 Dell 技术白皮书和文件可在 delltechcenter.com 获得，其中提供有关系统配置文件配置模板、属性和工作流程的更多信息：

- *使用服务器配置文件的服务器克隆*
- *服务器配置 XML 文件*
- *配置 XML 工作流程*
- *配置 XML 工作流程脚本 133*
- *XML 配置文件示例*