

# OpenManage Integration for VMware vCenter

## 版本 5.2

### 用户指南

## 注意、小心和警告

 **注:** “注意” 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，并告诉您如何避免此类问题。

 **警告:** “警告” 表示可能会导致财产损失、人身伤害甚至死亡。

<b>章 1: 简介</b> .....	<b>10</b>
此版本中的新功能.....	10
OpenManage Integration for VMware vCenter 功能.....	10
<b>章 2: 登录到 Dell EMC OMIVV 管理控制台</b> .....	<b>12</b>
注册新 vCenter 服务器.....	12
使用非管理帐户注册 vCenter 服务器.....	13
所需的非管理员用户的权限.....	13
将 Dell 权限分配给现有角色.....	14
更新已注册 vCenter 服务器的证书.....	15
修改 vCenter 登录凭据.....	15
注销 OpenManage Integration for VMware vCenter.....	15
将许可证上传到 OMIVV 管理控制台.....	15
管理 OMIVV 设备.....	16
设置全局警报.....	23
关于 OMIVV 虚拟机控制台.....	23
<b>章 3: 使用仪表板监测主机和机箱</b> .....	<b>32</b>
<b>章 4: 使用主机凭据配置文件管理主机</b> .....	<b>35</b>
主机凭据配置文件.....	35
创建主机凭据配置文件.....	35
编辑主机凭据配置文件.....	36
查看主机凭据配置文件.....	37
测试主机凭据配置文件.....	38
删除主机凭据配置文件.....	38
<b>章 5: 使用机箱凭据配置文件管理机箱</b> .....	<b>39</b>
机箱凭据配置文件.....	39
创建机箱凭据配置文件.....	39
编辑机箱凭据配置文件.....	40
查看机箱凭据配置文件.....	40
测试机箱凭据配置文件.....	41
删除机箱凭据配置文件.....	41
<b>章 6: 使用存储库配置文件管理固件和驱动程序存储库</b> .....	<b>42</b>
存储库配置文件.....	42
创建存储库配置文件.....	42
编辑存储库配置文件.....	43
编辑或自定义 Dell 默认目录.....	43
编辑已验证的 MX 堆栈目录.....	44
与存储库位置同步.....	44
查看存储库配置文件.....	44

删除存储库配置文件.....	44
<b>章 7: 使用群集配置文件捕获基线配置.....</b>	<b>45</b>
群集配置文件.....	45
创建群集配置文件.....	45
编辑群集配置文件.....	46
查看群集配置文件.....	46
更新群集配置文件.....	46
删除群集配置文件.....	47
<b>章 8: 管理裸机服务器.....</b>	<b>48</b>
查看裸机服务器.....	48
设备查找.....	48
自动查找.....	48
自动查找前提条件.....	49
启用或禁用 iDRAC 上的管理帐户.....	49
手动配置 PowerEdge 服务器以进行自动查找.....	50
手动发现裸机服务器.....	50
删除裸机服务器.....	51
刷新裸机服务器.....	51
购买或续订 iDRAC 许可证.....	51
<b>章 9: 管理部署配置文件.....</b>	<b>52</b>
系统配置文件.....	52
创建系统配置文件.....	52
编辑系统配置文件.....	53
查看系统配置文件.....	54
删除系统配置文件.....	54
ISO 配置文件.....	54
创建 ISO 配置文件.....	55
编辑 ISO 配置文件.....	55
查看 ISO 配置文件.....	55
删除 ISO 配置文件.....	55
下载自定义 Dell EMC ISO 映像.....	56
<b>章 10: 系统配置文件和 ISO 配置文件部署.....</b>	<b>57</b>
部署任务清单.....	57
部署系统配置文件 ( 硬件配置 ) .....	58
部署 ISO 配置文件 ( ESXi 安装 ) .....	58
部署系统配置文件和 ISO 配置文件.....	60
VLAN 支持.....	60
部署作业时间.....	60
<b>章 11: 合规性.....</b>	<b>62</b>
管理合规性.....	62
查看非合规主机.....	62
修复非合规主机.....	63
配置合规性.....	64

查看配置合规性.....	64
查看偏移报告.....	65
<b>章 12: 管理 OMIVV 作业.....</b>	<b>67</b>
部署作业.....	67
发现作业.....	68
机箱固件更新作业.....	68
主机固件更新作业.....	69
系统锁定模式作业.....	69
偏移检测作业.....	70
查看主机资源清册作业.....	70
运行资源清册作业.....	71
修改主机资源清册作业.....	71
查看机箱资源清册作业.....	72
运行机箱资源清册作业.....	72
查看主机保修.....	72
修改主机保修作业.....	73
查看机箱保修.....	73
<b>章 13: 管理日志.....</b>	<b>74</b>
查看日志历史记录.....	74
<b>章 14: 管理 OMIVV 设备设置.....</b>	<b>75</b>
管理多个设备.....	75
配置保修到期通知.....	75
配置最新设备版本通知.....	75
配置部署凭据.....	76
硬件组件冗余运行状况 — 主动式高可用性.....	76
主动式高可用性事件.....	76
配置机架式和塔式服务器的主动式高可用性.....	77
在群集上启用主动式高可用性.....	78
覆盖运行状况更新通知的严重性.....	78
初始配置.....	79
查看初始配置状态.....	80
固件更新设置.....	80
查看许可证信息.....	80
OpenManage Integration for VMware vCenter (OMIVV) 许可.....	80
购买软件许可证.....	81
访问支持信息.....	81
创建和下载故障排除捆绑包.....	82
重设 iDRAC.....	82
<b>章 15: 管理 vCenter 设置.....</b>	<b>83</b>
有关事件和警报.....	83
配置事件和警报.....	83
查看机箱事件.....	84
查看机箱警报.....	84
查看警报和事件设置.....	84

与虚拟化相关的事件.....	84
管理数据检索计划.....	91
计划资源清册作业.....	91
计划保修检索作业.....	91
<b>章 16: 机箱管理.....</b>	<b>93</b>
查看 Dell EMC 机箱信息.....	93
查看机箱资源清册信息.....	93
查看机箱的硬件资源清册信息.....	93
查看固件资源清册信息.....	96
查看管理控制器信息.....	96
查看存储资源清册信息.....	97
查看保修信息.....	98
查看机箱的关联主机.....	98
查看相关的机箱信息.....	98
管理 PowerEdge MX 机箱.....	99
使用统一的机箱管理 IP 进行的机箱和主机管理.....	99
添加 PowerEdge MX 机箱.....	100
MX 机箱固件更新.....	100
<b>章 17: 主机管理.....</b>	<b>102</b>
查看 OMIVV 主机.....	102
监测单个主机.....	102
查看主机摘要信息.....	102
查看 OMIVV 主机信息.....	104
监测群集和数据中心中的主机.....	108
固件更新.....	113
更新 vSAN 主机上的固件和驱动程序.....	114
更新 vSAN 群集上的固件和驱动程序.....	116
更新 vSphere 主机上的固件.....	117
更新 vSphere 群集上的固件.....	119
更新相同的固件组件类型.....	120
vSphere 生命周期管理器概览.....	121
在 Dell EMC 管理控制台中查看 vSphere 生命周期管理器状态.....	121
在 Dell EMC 管理控制台中注册 vSphere 生命周期管理器.....	122
在 Dell EMC 管理控制台中注销 vSphere 生命周期管理器.....	122
使用 vSphere 生命周期管理器管理群集.....	122
在 vSphere 生命周期管理器中使用 OMIVV 作为固件加载项提供程序 — 用户界面.....	122
查看群集合规性状态.....	123
解决群集合规性问题.....	123
硬件兼容性检查.....	123
运行修复预检查.....	124
vSphere 生命周期管理器中的修复.....	124
在 vSphere 生命周期管理器中使用 OMIVV 作为固件加载项提供程序 — vSphere 自动化 vAPI.....	124
设置闪烁指示灯.....	128
配置系统锁定模式.....	128
<b>章 18: 安全角色和权限.....</b>	<b>129</b>
数据完整性.....	129

访问控制验证、授权和角色.....	129
Dell 操作角色.....	129
Dell 基础架构部署角色.....	130
关于权限.....	130
<b>章 19: 常见问题-FAQ.....</b>	<b>132</b>
常见问题-FAQ.....	132
对于不符合要求的 vSphere 主机，iDRAC 的许可证类型和说明显示不正确.....	132
Dell 提供程序未作为运行状况更新提供程序显示.....	132
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。.....	132
运行“修补不符合要求的 vSphere 主机”向导时，特定主机的状态显示为“未知”.....	133
在注册 OMIVV 设备时分配的 Dell 权限，在取消注册 OMIVV 后不会删除.....	133
如何解决 VMware 证书颁发机构 VMCA 导致的错误代码 2000000.....	133
在管理控制台中，将设备重设为出厂设置后，更新存储库路径未设置为默认路径.....	133
在 OMIVV 中更改 DNS 设置后在 vCenter HTML-5 客户端中出现 Web 通信错误时该怎么办.....	134
在固件页面中，一些固件的安装日期显示为 12/31/1969.....	134
即使 OpenManage Integration 插件已成功注册到 vCenter，我在 HTML-5 客户端上仍然看不到 OpenManage Integration 图标.....	134
如果设备 IP 和 DNS 设置被 DHCP 值覆盖，在设备重新启动后，为什么 DNS 配置设置将恢复到原始设置.....	134
运行固件更新可能会显示错误消息，固件存储库文件不存在或无效。.....	134
不支持使用 OMIVV 更新固件版本为 13.5.2 的 Intel 网卡.....	134
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.....	135
为什么管理门户显示无法访问的更新存储库位置.....	135
当我执行一对多固件更新时，系统无法进入维护模式.....	135
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.....	135
在“系统概览”页面的“处理器视图”中处理器版本中为“不适用”.....	135
OMIVV 在链接模式下是否支持 vCenter.....	135
什么是 OMIVV 所需的端口设置.....	135
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未更改.....	137
无法查看 vCenter 主机和群集页面上列出的新 iDRAC 版本详细信息.....	137
支持启用锁定模式的 ESX/ESXi.....	137
在我尝试使用锁定模式时失败.....	137
尝试在服务器上部署 ESXi 失败.....	137
在部署向导中看到自动查找到的系统没有型号信息.....	137
使用 ESXi ISO 设置了 NFS 共享，但装载共享位置出错，造成部署失败.....	137
我如何从 vCenter 上强制移除 OMIVV 设备.....	137
在“立即备份”屏幕中输入密码时收到错误消息.....	138
如果更新失败，应该怎么办.....	138
我的 vCenter 注册失败，该怎么办.....	138
主机凭据配置文件测试凭据期间的性能缓慢或无响应.....	138
OMIVV 是否支持 VMware vCenter 服务器设备.....	139
服务器可能显示为不符合 CSIOR 状态 - “未知”.....	139
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系统进行了重新引导后，但我的固件级别仍未更新.....	139
即使从 vCenter 树中删除了主机，主机仍显示在机箱下.....	139
备份和还原 OMIVV 后，警报设置未还原.....	139
当在目标节点上启用 NPAR 并且在系统配置文件中禁用该分区时，操作系统部署失败.....	139

当可用版本低于当前版本时，可用的 OMIVV 设备版本显示错误信息.....	139
添加第 12 代和更高版本的裸机服务器时引发 267027 异常.....	139
由于 iDRAC 错误，在部署过程中，系统配置文件应用失败.....	140
借助域用户身份验证进行配置时，OMIVV RPM 升级失败.....	140
无法应用 FX 机箱中有 PCIe 卡的系统配置文件.....	140
偏移检测显示在 FX 机箱中具有 PCIe 卡的模块化服务器的不合规情况.....	140
当 iDRAC 未填充所选 NIC 的 MAC 地址时无法在 PowerEdge 服务器上部署操作系统.....	140
为具有 ESXi 6.5U1 的主机创建主机凭据配置文件时，不在“选择主机”页面上显示主机的服务标签....	140
从旧版 OMIVV 备份或还原至更高版本的 OMIVV 后，将不显示 Dell EMC 图标.....	141
使用 OMIVV 升级或降级的一些 iDRAC 固件版本时，即使固件更新成功，OMIVV 仍可能显示作业失败。.....	141
在一个集群级别下配置系统锁定模式时有时会显示消息“该集群下没有主机具有成功的资源清册”.....	141
有时开机自检 OMIVV 设备的 RPM 升级，可以在 vCenter 最近任务中查看日志中的多个条目.....	141
注册 vCenter 后，OMIVV 的 Dell EMC 徽标不显示在 VMware 的主页上.....	141
在备份和还原后，非合规的 11G PowerEdge 服务器会保留在 OMIVV 资源清册中.....	142
升级 OMIVV 设备后无法从灵活客户端启动 vCenter.....	142
在 OMIVV 中添加或移除网络适配器时，现有 NIC 将从 OMIVV 控制台中消失.....	142
添加或移除第二个 NIC 后，“网络配置”页面显示三个 NIC.....	142
备份和还原到最新的 OMIVV 版本后，较早版本中状态为“未知”的服务器未列出在“裸机服务器”页面上.....	143
进行操作系统部署后，OMIVV 无法将 ESXi 主机添加到 vCenter、无法添加主机配置文件或主机进入维护模式失败.....	143
当 iDRAC IP 不可访问时，iDRAC 许可证状态在“管理合规性”页面上显示为“合规”.....	143
使用 OMIVV 成功部署操作系统后，ESXi 主机断开连接或处于无响应状态。.....	143
OMIVV 网络接口卡 (NIC) 未连接至 ESXi 主机网络时，部署作业超时.....	143
保修作业未针对某些主机运行.....	143
执行备份和还原后，主动高可用性初始化未发生.....	144
OMIVV 页面显示无效的会话、超时异常或 Firefox 浏览器中的 2000000 错误.....	144
在 vCenter 中，“最近任务”窗格不会显示一些 OMIVV 任务通知的详细信息列.....	144
使用 vCenter 6.5 U2 时，OMIVV 的所有页面中可能会显示 2000002 错误.....	144
在执行从较早的 OMIVV 版本到更新 OMIVV 版本的 RPM 升级或备份和恢复后，在 OMIVV 的所有页面中显示 2000002 错误。.....	144
有时，OMIVV 需要很长时间才能完成 vCenter 取消注册.....	144
更新 OMIVV 证书后，将显示“无法连接 OMIVV 设备。SSL 证书无效”错误消息。.....	145
OMIVV 中的部署作业失败.....	145
更改 vCenter 密码后，测试连接和清点操作在 OMIVV 中失败.....	145
在将 OMIVV 设备重置为出厂设置后，不会从 vCenter 中移除 OMIVV 实例.....	145
OMIVV 在“系统配置文件”的“配置文件设置”页面上仅显示 BIOS 和 iDRAC 属性.....	145
操作系统部署已完成，但出现未知错误.....	145
FX2 机箱中的机箱管理控制器 (CMC) 固件更新失败.....	146
OMIVV 中的 ISO 配置文件部署失败.....	146
裸机部署问题.....	146
在新购买的系统上启用自动查找.....	146
<b>附录 A: 系统特定属性.....</b>	<b>147</b>
<b>附录 B: 附加信息.....</b>	<b>151</b>
<b>附录 C: 自定义属性.....</b>	<b>152</b>

<b>附录 D: 组件与基线版本比较值表.....</b>	<b>153</b>
<b>附录 E: 响应代码.....</b>	<b>154</b>

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) 使您能够优化与在 vSphere 环境中管理和监视 Dell EMC 服务器基础架构相关的任务，从而降低管理数据中心的复杂性。

## 此版本中的新功能

此版本的 OpenManage Integration for VMware vCenter 5.2 提供以下功能：

- OMIVV RESTful API 简介  
有关更多信息，请参阅位于 <https://www.dell.com/support/> 的 *OpenManage Integration for VMware vCenter 5.2 API 指南*。
- 支持 vSphere 7.0 U1
- 支持 XE2420 PowerEdge 服务器
- 支持基于 IPv4 范围的裸机查找
- 安全性增强
- **Dell EMC 机箱和 Dell EMC 主机**页面上添加了筛选器选项，以根据运行状况筛选主机和机箱
- 用于具有多种或不同保修的主机的保修报告增强功能。

## 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	<p>资源清册功能提供了以下选项：</p> <p>PowerEdge 服务器详细信息，例如内存 — 数量和类型、NIC、PSU、处理器和远程访问控制器 (RAC)</p> <p>服务器、群集和数据中心级别的保修信息</p> <p>机箱详细信息，例如机箱管理控制器 (CMC) 或 Management Module 信息、机箱电源、KVM 状态、风扇或散热详细信息、保修信息、交换机、服务器和存储详细信息</p> <p>在多机箱管理 (MCM) 配置中支持 MX 机箱关系。</p> <p>MX 机箱 MCM 配置的结构信息</p> <p>MX 机箱的 QuickSync 硬件信息</p>
监测和发送警报	<p>监测和警报包括以下功能：</p> <p>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。</p> <p>提供情报（例如资源清册、事件、警报）来诊断服务器和机箱问题。</p> <p>支持 VMware Proactive HA 功能。</p>
固件更新	<p>支持群集的服务器固件更新包括以下：</p> <p>将支持的服务器更新到最新版本的 BIOS 和固件。</p>

表. 1: OMIVV 功能 (续)

功能	说明
	您还可以将 OMIVV 与 vSphere 生命周期管理器配合使用, 以执行固件更新 (适用于 vCenter 7.0 及更高版本)。
群集的偏移检测	群集的固件合规性 vSAN 群集的驱动程序合规性 硬件合规性 <b>i</b> 注: 硬件合规性不支持使用机箱凭据配置文件管理的主机。
驱动程序更新	vSAN 群集的驱动程序更新。
部署	部署包括以下: 创建和部署系统配置文件。 使用 VMware vCenter 在裸机服务器上远程部署操作系统, 而不使用 PXE。
服务信息	从 Dell 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: 与标准 vCenter 验证、规则和权限集成。 支持基于 iDRAC9 服务器中的 iDRAC 锁定模式。有关基于 iDRAC9 的服务器的列表, 请参阅兼容性值表。
支持 OEM 服务器	支持以下 OMIVV 功能: 资源清册 监测和发送警报 固件更新 部署 服务信息 安全角色和权限
MX 机箱固件更新	提供一个选项, 用于更新 MX 机箱的管理模块固件。

**i**注: 从 OMIVV 5.0 开始, 仅支持 VMware vSphere Client (HTML-5), 不支持 vSphere Desktop Client (FLEX)。

## 登录到 Dell EMC OMIVV 管理控制台

可以使用下面提到的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 的管理控制台
  - 单个服务器的控制台视图（OMIVV 设备的虚拟机控制台）
1. 转至 <https://<ApplianceIP/hostname/>>。  
帐户锁定持续时间为 1 分钟。  
帐户锁定时，无法启动新会话。但是，旧的活动会话将处于活动状态。
  2. 输入密码。  
输入无效密码将导致登录尝试失败。连续六次失败的登录尝试会导致帐户锁定。六次失败的登录尝试包括管理控制台或 REST API 中的失败登录尝试，或使用无效令牌访问 REST API。  
帐户锁定持续时间为 1 分钟。  
您不能在帐户锁定期间创建会话，但当前的活动会话仍保持活动状态。  
如果您是第一次登录，系统会提示您接受 EULA。
  3. 在 **Dell EMC 最终用户许可协议** 页面上，阅读条款和条件，然后选择**我接受许可协议中的条款**复选框。  
有关遥测 EULA 的详细信息，请单击 **DELL EMC 遥测 EULA**。
  4. 单击**接受**。

## 注册新 vCenter 服务器

您的 vCenter 帐户应具有创建用户所需的权限。有关所需权限的更多信息，请参阅[所需的非管理员用户的权限](#) 页面上的 13。

安装 OMIVV 后，您可以注册 OMIVV 设备。OMIVV 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 15 台 vCenter 服务器和多达 2,000 台 ESXi 主机。

如果您尝试注册超过 15 个 vcenter，将显示以下错误消息：

您的许可证仅允许 <x> 个 vcenter，并且它们均已注册。

要注册新 vCenter 服务器，请执行以下步骤：

1. 转至 <https://<ApplianceIP/hostname/>>。
2. 在 **vCenter 注册** 页面的右窗格中，单击**注册新 vCenter 服务器**。  
此时将显示**注册新 vCenter** 页面。
3. 在**注册新 vCenter** 对话框中的 **vCenter 名称** 下，执行以下任务：
  - a. 在 **vCenter 服务器 IP 或主机名** 框中，输入 vCenter 的 IP 地址或主机的 FQDN。  
Dell EMC 建议使用完全限定域名 (FQDN) 向 VMware vCenter 注册 OMIVV。对于所有注册，vCenter 的主机名必须可通过 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 设备时，会分配静态 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 主机名信息存在于 DNS 服务器的正向和反向查询区域中。
  - b. 在**说明**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** 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**框中，输入密码。
  - c. 在**验证密码**框中，再次输入密码。
  - d. 选中**注册 vSphere 生命周期管理器**复选框。  
选中**注册 vSphere 生命周期管理器**复选框可让您使用 vCenter 7.0 及更高版本中的 vSphere 生命周期管理器功能。
5. 单击**注册**。

如果 vCenter 注册失败，将显示以下错误消息：

由于凭据错误，无法与给定的 vCenter 服务器 <x> 联系。检查用户名和密码。

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

**注：**对于 OMIVV 设备中的所有 vCenter 操作，OMIVV 使用已注册用户的权限，而不是登录到 VMware vCenter 的用户或 OMIVV 设备本地帐户的权限。

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。

**注：**如果您想上传自定义证书颁发机构 (CA) 签名的至证书 OMIVV，请确保先上传新证书再注册 vCenter。如果您在注册 vCenter 后上传新的自定义证书，vSphere Client 会显示通信错误。要解决此问题，请取消注册，然后重新向 vCenter 注册设备。

## 使用非管理帐户注册 vCenter 服务器

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

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：

1. 创建角色或修改现有角色以使其具有所需权限。  
有关角色所需权限列表的更多信息，请参阅[非管理员用户的所需权限](#)。  
有关创建或修改角色以及在 vSphere Client (HTML-5) 中选择权限时所需的步骤，请参阅 VMware vSphere 说明文件
  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。  
有关分配具有权限的角色的更多信息，请参阅 VMware vSphere 说明文件。  
具有所需权限的 vCenter 服务器非管理员用户现在可以注册和/或取消注册 vCenter、修改凭据或更新证书。
  3. 使用具有必要权限的非管理员用户注册 vCenter 服务器。
  4. 注册完成后，将 Dell 权限分配给步骤 1 中创建或修改的角色。请参阅[将 Dell 权限分配给现有角色](#) 页面上的 14。
- 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，非管理员用户必须具有以下权限：

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
- 运行状况更新提供程序
  - 注册
  - 注销
  - 更新
- 主机
  - CIM
    - CIM 交互
- Host.Config

- 高级设置
- 更改设置
- 连接
- 维护
- 网络配置
- 查询补丁程序
- 安全配置文件和防火墙
- 资源清册
  - 将主机添加到群集
  - 添加独立主机
  - 修改群集
- 生命周期管理器：常规权限
  - 读取
- 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
  - 更新


**i 注：** vSphere 生命周期管理器常规权限仅适用于 vCenter 7.0 及更高版本。

**i 注：** 如果使用非管理员用户注册 vCenter 服务器以访问任何 OMIVV 功能，则非管理员用户必须具有 Dell 权限。有关查找 Dell 权限的更多信息，请参阅[将 Dell 权限分配给现有角色](#) 页面上的 14。

## 将 Dell 权限分配给现有角色

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。

您可以编辑现有角色以分配 Dell 权限。

1. 使用管理权限登录 vSphere Client (HTML-5)。
2. 在 vSphere Client (HTML-5) 中，**展开菜单**，然后单击**管理** → **角色**。
3. 从**角色提供程序**下拉列表中，选择 vCenter 服务器。
4. 从**角色列表**中，选择 **Dell 操作**，然后单击**权限**。
5. 要分配 Dell 权限，请编辑图标。此时将显示**编辑角色**页面。
6. 在左窗格中，单击 **Dell**，然后为所选角色选择以下 Dell 权限，之后单击**下一步**：
  - Dell.Configuration
  - Dell.Deploy-Provisioning
  - Dell.Inventory
  - Dell.Monitoring
  - Dell.Reporting

有关 vCenter 内可用的 OMIVV 角色的详细信息，请参阅 [安全角色和权限](#)。

7. 编辑角色名称，然后输入所选角色的说明（如果需要）。
8. 单击**完成**。  
从 vCenter 中注销，然后重新登录。现在，具有必要权限的用户可以执行 OMIVV 操作。

## 更新已注册 vCenter 服务器的证书

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。OMIVV 使用数字证书在 Web 服务器上启用 HTTPS 以进行安全通信。

如果 vCenter 服务器上的证书更改，请使用以下任务为 OMIVV 导入新证书：

1. 转至 <https://<ApplianceIP/hostname/>>。
2. 在左侧窗格中，单击 **VCENTER 注册**。  
已注册的 vCenter 服务器显示在工作窗格中。
3. 要更新 vCenter 服务器 IP 或主机名的证书，请单击**更新**。

## 修改 vCenter 登录凭据

您可以使用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 vCenter 登录凭据。

如果在群集上启用主动式高可用性功能，则您不得更改与其关联的用户。修改使用不同 vCenter 用户进行的注册将打破主动式高可用性功能。如果凭据需要修改，请取消注册旧凭据并通过使用新凭据进行注册。



1. 转至 <https://<ApplianceIP/hostname/>>。
2. 在**登录**对话框中，键入密码，然后单击**登录**。
3. 在左侧窗格中，单击 **VCENTER 注册**。  
已注册的 vCenter 服务器显示在工作窗格中。
4. 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**。
5. 如果输入了不正确的凭据，系统将会显示一条消息。输入有效的 vCenter 用户名、密码，然后重新输入密码以确认密码。
6. 要更改密码，请单击**应用**。要取消更新，请单击**取消**。

## 注销 OpenManage Integration for VMware vCenter

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。

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。要禁用主动式高可用性，请通过选择 **配置 > 服务 > vSphere 可用性**，然后单击 **编辑**，访问群集的**主动式高可用性故障和响应**屏幕。要禁用主动式高可用性，请在**主动式高可用性故障和响应**屏幕中，清除 **Dell Inc** 提供商旁边的复选框。

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. 转至 <https://<ApplianceIP/hostname/>>。
2. 在 **vCenter 注册**页面上的 **vCenter 服务器 IP 或主机名**表中，单击**注销**。  
 **注：** 确保选择正确的 vCenter，因为 OMIVV 可与多个 vCenter 相关联。
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**。  
 **注：** 注销 OMIVV 之后，注销并从 vSphere Client (HTML-5) 登录。如果 OMIVV 图标仍然可见，则重新启动 vSphere Client (HTML-5) 和 Web Client (FLEX) 的客户端服务。

## 将许可证上传到 OMIVV 管理控制台

确保您的许可证可从 <https://www.dell.com/support> 上的 Dell Digital Locker 下载。如果您订购了多个许可证，这些许可证可能会在不同时间分别发放。您可以在 <https://www.dell.com/support> 上的“订单状态”中查看其他许可证项目的状态。许可证文件以 .XML 格式提供。

1. 转至 <https://<ApplianceIP/hostname/>>。
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 服务器显示在工作窗格中。

4. 单击**上传许可证**。
5. 在**上传许可证**对话框中，单击**浏览**以转至许可证文件，然后单击**上传**。

**注**：如果修改或编辑许可证文件，则许可证文件（.XML 文件）将无效。可以通过 Dell Digital Locker 下载 XML 文件（许可证密钥）。如果您无法下载许可证密钥，请转至 <https://www.dell.com/support> 处的“联系技术支持”找到您的产品对应的区域 Dell 支持电话号码，联系 Dell 支持部门。

## 管理 OMIVV 设备

OMIVV 设备管理使您能够管理 OpenManage Integration for VMware vCenter 网络、NTP 和 HTTPS 信息，并可以让管理员执行以下操作：

- 重新启动 OMIVV 设备。请参阅[重新启动 OMIVV 设备](#) 页面上的 16。
- 更新 OMIVV 设备，并配置更新存储库位置。请参阅[升级 OMIVV 设备和存储库位置](#) 页面上的 16。
- 使用 RPM 升级 OMIVV 设备。请参阅[使用 RPM 升级 OMIVV 设备（使用 Internet）](#) 页面上的 17。
- 使用备份和还原升级 OMIVV 设备。请参阅[使用备份和还原升级 OMIVV 设备](#) 页面上的 18。
- 生成和下载故障排除捆绑包。请参阅[生成和下载故障排除捆绑包](#) 页面上的 20。
- 设置 HTTP 代理。请参阅[设置 HTTP 代理](#) 页面上的 20。
- 设置网络时间协议服务器。请参阅[设置网络时间协议 \(NTP\) 服务器](#) 页面上的 21。
- 配置部署模式。请参阅[配置部署模式](#) 页面上的 21。
- 扩展监测 请参阅[扩展监测](#) 页面上的 22。
- 生成证书签名请求 (CSR)。请参阅[生成证书签名请求 \(CSR\)](#) 页面上的 22。
- 上传 HTTPS 证书。请参阅[上传 HTTPS 证书](#) 页面上的 22。
- 设置全局警报。请参阅[设置全局警报](#) 页面上的 23。

## 访问设备管理

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：

1. 转至 <https://<ApplianceIP/hostname/>>。
2. 在**登录**对话框中，输入密码。
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 OMIVV 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 OMIVV 设备，请在**重新启动虚拟设备**对话框中，单击**应用**。

## 升级 OMIVV 设备和存储库位置

- 要确保所有数据受保护，请执行 OMIVV 数据库的备份后再更新 OMIVV 设备。请参阅[管理备份和还原](#) 页面上的 19。
- 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。如果您需要代理网络，请根据环境网络设置启用代理设置，然后输入代理数据。请参阅[设置 HTTP 代理](#)。
- 确保**更新存储库路径**有效。
- 确保您从所有 vSphere Client (HTML-5) 会话至 vCenter 服务器中注销。
- 在登录到已注册的 vCenter 服务器之前，确保您在相同的平台服务控制器 (PSC) 下同时更新所有设备。否则，可能会在 OMIVV 实例上看到不一致信息。

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 OMIVV 版本。

有关可用的 OMIVV 设备版本，适用的 RPM 和 OVF OMIVV 设备升级机制会显示一个勾选标记  ]。

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：

选项	说明
1	如果 RPM 旁显示了勾选标记，则可以将 RPM 从现有版本升级至最新的可用版本。请参阅 <a href="#">使用 RPM 升级 OMIVV 设备（使用 Internet）</a> 页面上的 17。
2	如果 OVF 旁显示勾选标记，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 <a href="#">使用备份和还原升级 OMIVV 设备</a> 页面上的 18。
3	如果 RPM 和 OVF 旁均显示勾选标记，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 OMIVV 设备，请从 OMIVV 版本执行提及的适用升级机制任务。

## OMIVV 升级选项

### 备份和恢复

您可以从 OMIVV 5.0 执行备份和恢复到最新版本（对于 vCenter 6.5 和更高版本）。

### RPM 升级

您可以执行从 OMIVV 5.0 到最新版本的 RPM 升级。

## 使用 RPM 升级 OMIVV 设备（使用 Internet）

确保您要升级到比当前设备更高的版本。

建议先截取设备快照，然后再升级 OMIVV 设备。

1. 在**设备管理**页面中，根据您的网络设置，启用代理并输入代理设置数据（如有必要）。请参阅用户指南[设置 HTTP 代理](#)中的。

有关可用的 OMIVV 设备版本，适用的 RPM 和 OVF OMIVV 设备升级机制会显示一个勾选标记 。

2. 要将 OMIVV 插件从现有版本升级至可用版本，请执行以下步骤之一：

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

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

3. 比较可用 OMIVV 设备版本和当前 OMIVV 设备版本。

4. 要将更新应用到 OMIVV 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**窗口注销。

6. 关闭 Web 浏览器。

在升级过程中，设备会重新启动一次或两次。RPM 升级设备后，请确保先清除浏览器高速缓存，然后再登录 Dell 管理员门户。

RPM 升级完成后，您可以在 OMIVV 控制台中查看登录屏幕。打开浏览器并输入 <https://<设备 IP | 主机名>> 链接，然后转至**设备更新**区域。您可以验证可用和当前 OMIVV 设备版本是否相同。

在 RPM 升级后，在面向 PHA 群集的已注册 Dell 警报和 Dell 运行状况更新提供程序上执行的所有自定义设置都将恢复为默认值。

## 使用 RPM 升级 OMIVV 设备（无 Internet）

创建 HTTP 或 HTTPS 共享。确保 HTTP 或 HTTPS 共享支持包含特殊字符（如 ++ 和空格）的文件名。

OMIVV 仅支持 HTTP 和 HTTPS 共享。

OMIVV 支持在没有互联网连接的情况下从版本 5.1 升级到 5.2。

1. 下载 <https://www.dell.com/support> 上提供的 RPM zip 软件包。

2. 提取 RPM zip 软件包，并将文件和文件夹从提取的位置复制到 HTTP 或 HTTPS 共享

3. 在**设备管理**页面的**设备更新**区域中，单击**编辑**，然后在**更新存储库路径**中输入共享位置路径。
4. 单击**应用**。
5. 比较可用 OMIVV 设备版本和当前 OMIVV 设备版本。
6. 要将更新应用到 OMIVV 设备，可在**设备设置**下，单击**更新虚拟设备**。
7. 在**更新设备**对话框中，单击**更新**。  
单击**更新**后，您会从 **OMIVV 管理控制台**窗口注销。  
完成更新可能需要大约 40 分钟，具体取决于您的网络速度。
8. 关闭 Web 浏览器。  
升级设备后，请确保先清除浏览器高速缓存，然后再登录 **OMIVV 管理员控制台**。

## 使用备份和还原升级 OMIVV 设备


建议不要在执行备份后且还原备份文件前更改或删除由 OMIVV 管理的群集或主机。如果更改或删除了由 OMIVV 管理的群集或主机，请在还原后重新配置与这些群集和主机关联的配置文件（例如，主机凭据配置文件、群集配置文件）。

请不要从 vCenter 注销 OMIVV 插件。如果从 vCenter 中注销插件，将移除 OMIVV 插件在 vCenter 上注册的主动高可用性群集的 Dell 运行状况更新提供程序。

建议先截取设备快照，然后再升级 OMIVV 设备。

要将 OMIVV 设备从较旧版本更新至当前版本，请执行以下步骤：

1. 备份早期版本的数据。
2. 从 vCenter 关闭较旧 OMIVV 设备。
3. 部署新的 OpenManage Integration 设备 OVF。
4. 开启 OpenManage Integration 新设备电源。
5. 设置新设备上的网络和时区。

 **注：**建议保留较早 OMIVV 设备的身份（IP 或 FQDN）以实现新的 OMIVV 设备。

6. OMIVV 设备附带默认证书。如果您想为您的设备获取自定义证书，同样进行更新。请参阅[生成证书签名请求 \(CSR\)](#) 页面上的 22 和[上传 HTTPS 证书](#) 页面上的 22。否则，请跳过此步骤。
7. 将数据库还原到新的 OMIVV 设备。请参阅[从备份还原 OMIVV 数据库](#)。
8. 验证设备。有关更多信息，请参阅[安装指南中的验证安装主题](#)
9. 在升级后，建议对 OMIVV 插件管理的所有主机重新运行资源清册。

在还原设备后，事件和警报设置未启用。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。

如果从早期版本的 OMIVV 升级到可用版本，所有已计划的作业将继续运行。

在执行备份和还原后，在面向 PHA 群集的已注册 Dell 警报和 Dell 运行状况更新提供程序上执行的所有自定义设置都将恢复为默认值。

从较早的 OMIVV 版本备份和恢复到更高版本的 OMIVV 后，如果您发现以下任何问题，请执行以下任务：

- 200000 消息
- 缺少 Dell EMC 徽标
- OMIVV UI 没有响应
- OMIVV 插件未从 vCenter 中移除
- SSL 证书无效

解决方案：

- 在 vCenter 服务器上为 vSphere Client (HTML-5) 和 vSphere Web Client (FLEX) 重新启动 vSphere Client 服务。
- 如果问题仍然存在：
  - 对于 VMware vCenter Server 设备：请转至 `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity`。对于 Windows vCenter，请转至 vCenter 设备中的以下文件夹，并检查是否存在与较早版本相对应的旧数据 - vCenter 设备中的 `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity` 文件夹，并查看是否存在旧数据，例如 `com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX`。
  - 手动删除与早期 OMIVV 版本对应的文件夹并重新启动 vSphere Client (HTML-5) 和 Web Client (FLEX) 的 vSphere Client 服务。

如果新设备的 IP 地址不同于旧设备的 IP 地址，请执行以下操作：

- 主动式高可用性功能可能无法正常运行。在这种情况下，请为存在 Dell EMC 主机的每个群集禁用并启用主动高可用性。
- 配置 SNMP 陷阱的陷阱目标以指向新设备。通过在主机上运行资源清册对身份更改进行修补。在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。要解决主机合规性问题，请参阅中的[修复非合规主机](#) 页面上的 63。

## 管理备份和还原

通过使用管理控制台，您可以执行备份和还原相关任务。

- [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](#)
- [重置备份和还原设置](#) 页面上的 20

在 OMIVV 中，请执行以下步骤以使用管理控制台访问[备份和还原设置](#)页面：

1. 转至 `https://<ApplianceIP|hostname>`。
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（NFS 和 CIFS），以后可从该位置进行还原。配置文件、配置和主机信息位于备份中。建议您计划自动备份以防止数据丢失。

 **注：** NTP 设置未保存和还原。

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，输入用户名。
  - c. 在[密码](#)中，输入密码。
  - d. 在[输入用于加密备份的密码](#)中，在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 “!、@、#、\$、% 和 \*”。
  - 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](#)。

此步骤后，配置备份计划。

## 计划自动备份

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](#)。

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. 选中您要运行备份作业于每周的星期几的[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**使用来自备份设置的位置和加密密码**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“!、@、#、\$、%和\*”。没有形成密码的字符限制。
4. 单击**备份**。

## 从备份还原 OMIVV 数据库

从以前的版本还原 OMIVV 之后：

- 不支持第 11 代服务器。在还原之后，仅保留第 12 代及更高版本的服务器。
- 不支持硬件配置文件和部署模板。建议使用系统配置文件来进行部署。
- 将会取消在第 11 代服务器上计划的部署任务和/或使用基于硬件配置文件的部署模板。
- 将从凭据配置文件中删除所有第 11 代服务器并会撤回所使用的许可证。
- 存储库配置文件将只使用 64 位捆绑包。
  - ① **注：**如果执行从 4.x 到 5.x 的备份和还原，群集配置文件名称将会显示警告符号，因为 OMIVV 不支持在 5.x 版中使用 32 位捆绑包。要对群集配置文件使用最新更改，请编辑群集配置文件。
- 将会取消在第 11 代服务器上计划的固件更新作业。

确保在执行恢复操作之前配置正确的部署模式。有关部署配置模式的更多信息，请参阅 [配置部署模式](#) 页面上的 21。

1. 在**备份和还原设置**页面中，单击**立即还原**。
2. 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 或 NFS 格式）。
3. 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“!、@、#、\$、%和\*”。
4. 要保存您的更改，请单击**应用**。  
还原操作导致 OMIVV 设备在还原完成后重新引导。要验证安装，请参阅安装指南中的“验证安装”主题。  
还原完成后，请关闭浏览器并清除浏览器缓存，然后再登录到管理员门户。

## 重置备份和还原设置

使用重置设置功能，您可以将设置重置为未配置状态。

1. 在**备份和还原设置**页面中，单击**重置设置**。
2. 在**重置设置**对话框中，单击**应用**。

## 生成和下载故障排除捆绑包

要生成故障排除捆绑包，请确保您登录到管理员门户。

故障排除捆绑包含有 OMIVV 日志记录信息，可用于帮助解决问题或将其发送给技术支持部门。

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**。

## 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. 选择**已启用**以启用 HTTP 代理设置的使用。
3. 在**代理服务器地址**中输入代理服务器地址。
4. 在**代理服务器端口**中输入代理服务器端口。
5. 选择**是**以使用代理凭据。
6. 如果使用代理凭据，请在**用户名**中输入用户名。
7. 在**密码**中键入密码。
8. 单击**应用**。

## 设置网络时间协议 (NTP) 服务器

可使用 NTP 同步 OMIVV 设备时钟与 NTP 服务器的时钟。

1. 在管理控制台中的**设备管理**页面上，单击 **NTP 设置**区域中的**编辑**。
2. 选择**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**。
3. 配置 NTP 后，启动终端控制台并选中**通过网络同步日期和时间**复选框。

**注:** OMIVV 时钟与 NTP 服务器同步可能需要几分钟时间。

**注:** 如果 OMIVV 管理员门户加载信息时间过长，请确保 NTP 设置正确，并且 OMIVV 虚拟机可以访问 NTP 服务器。

## 配置部署模式

对于任何提及的部署模式，请确保通过使用保留为 OMIVV 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。

通过分配这些资源到包含 OMIVV 的虚拟机，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 (GB)	最低存储
小	最多 250 个	2	8	95 GB
中	最多 500 个	4	16	95 GB
大	最多 1000 个	8	32	95 GB
超大模式	最多 2000 个	12	32	95 GB

**注:** MX 机箱固件更新功能仅在中、大和超大部署模式下受支持。

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。

要将 OpenManage Management Pack for vRealize operations (vROPS) 与 OMIVV 集成，所需的最低部署模式为**中等**。

1. 在**设备管理**页面中，向下滚动到**部署模式**。  
此时将显示部署模式的配置值，例如**小**、**中**、**大**和**特大**。默认情况下此模式设置为**小**。
2. 要基于某种环境编辑部署模式，请单击**编辑**。
3. 在**编辑**模式中，请确保满足这些前提条件并选择所需部署模式。
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。
  - 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，然后重启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页面。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，然后打开 OMIVV 设备。

## 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。

## 升级部署模式

1. 先清除浏览器高速缓存再登录到 Dell 管理门户。
2. 开启 OMIVV 设备。
3. 登录到管理控制台。
4. 将部署模式更改到所需的级别。

## 扩展监测

请确保启用扩展监测，以支持 OpenManage Management Pack for vRealize Operations Manager。建议通过“中型”部署模式执行扩展监测。

请确保启用 SNMP 陷阱监测，以支持 OpenManage Management Pack for vRealize Operations Manager 的 SNMP 警报。这允许用户实时监测服务器或机箱的运行状况。

1. 转至 <https://<ApplianceIP/hostname/>>。
2. 在左侧窗格中，单击**设备管理**。
3. 在**设备管理**页面中，向下滚动到**扩展监测**。
4. 要编辑扩展监测设置，请单击**编辑**。
5. 在编辑模式中，启用或禁用扩展监测和 SNMP 陷阱监测，然后单击**应用**。

## 生成证书签名请求 (CSR)

在将 OMIVV 注册到 vCenter 之前，请确保您上传 CSR。

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

1. 在**设备管理**页面中，单击 **HTTPS 证书** 区域中的**生成证书签名请求**。  
此时将显示一条消息，表明如果生成新请求，则使用以前的 CSR 创建的证书无法再上传到设备。要继续请求，请单击**继续**。
2. 如果继续请求，则在**生成证书签名请求**对话框中，输入通用名称、组织、地点、州/省、国家/地区和电子邮件地址。单击**继续**。
3. 单击**下载**，然后将所得 CSR 保存到可访问的位置。

## 上传 HTTPS 证书

确保证书使用 PEM 格式。

您可以使用 HTTPS 证书在 OMIVV 设备和主机系统或 vCenter 之间进行安全通信。要设置此类型的安全通信，请将 CSR 证书发送到签署机构，然后使用管理控制台上载生成的 CSR。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. 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. 要上传证书，请单击**浏览**，然后单击**上传**。  
要检查状态，请转至已注册 vCenter 的 vSphere Client 的**事件控制台**。

在上传证书时，OMIVV 管理控制台在最长 3 分钟内无响应。完成“上传 HTTPS 证书”任务后，关闭该浏览器会话，然后在新的浏览器会话中访问管理员门户。

## 还原默认的 HTTPS 证书

1. 在**设备管理**页面中，单击 **HTTPS 证书** 区域中的**还原默认证书**。
2. 在**还原默认证书**对话框中，单击**应用**。

在还原证书时，OMIVV 管理控制台在最长 3 分钟内无响应。在还原默认 HTTPS 证书任务完成后，关闭浏览器会话并在新的浏览器会话中访问管理员门户。

## 设置全局警报

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

1. 转至 <https://<ApplianceIP/hostname/>>。
2. 在**登录**对话框中，输入密码。
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. 在以下字段中输入数值：  
默认情况下，将显示当前警报数量的计数。
  - **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**。

## 关于 OMIVV 虚拟机控制台

OMIVV 虚拟机控制台在虚拟机的 vSphere 客户端中可用。控制台与管理控制台紧密协同工作。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 OMIVV 设备](#)
- [将 OMIVV 设备重置为出厂设置](#)
- [使用只读角色登录](#)
- [从控制台注销](#)

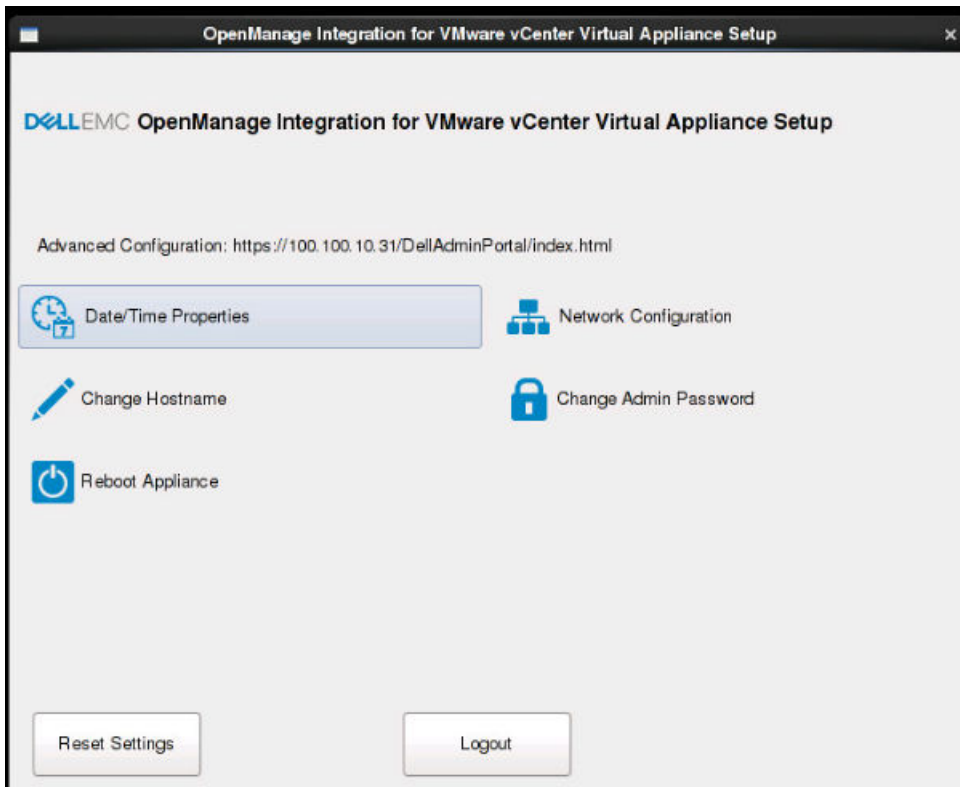
## 打开 OMIVV 虚拟机控制台

要打开 OMIVV 虚拟机控制台，请启动 OMIVV 设备的 Web 或远程控制台。

打开虚拟机控制台并输入凭据（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 OMIVV 设备

1. 为虚拟机通电。
2. 在右侧窗格中，单击**启动 Web 控制台**。
3. 以管理员身份登录（默认用户名为 admin）。
4. 如果您是第一次登录，请按照屏幕上的说明设置密码（管理员和只读用户）。
  - ① **注：**如果您忘记了管理员密码，则无法从 OpenManage Integration for VMware vCenter 设备中恢复。
5. 要配置 OMIVV 时区信息，请单击**日期/时间属性**。




**注:** OMIVV 设备无法从网络 (DHCP) 中检索 IP 地址时, 将会显示 0.0.0.0 作为 IP 地址。要解决此问题, 必须手动配置静态 IP。

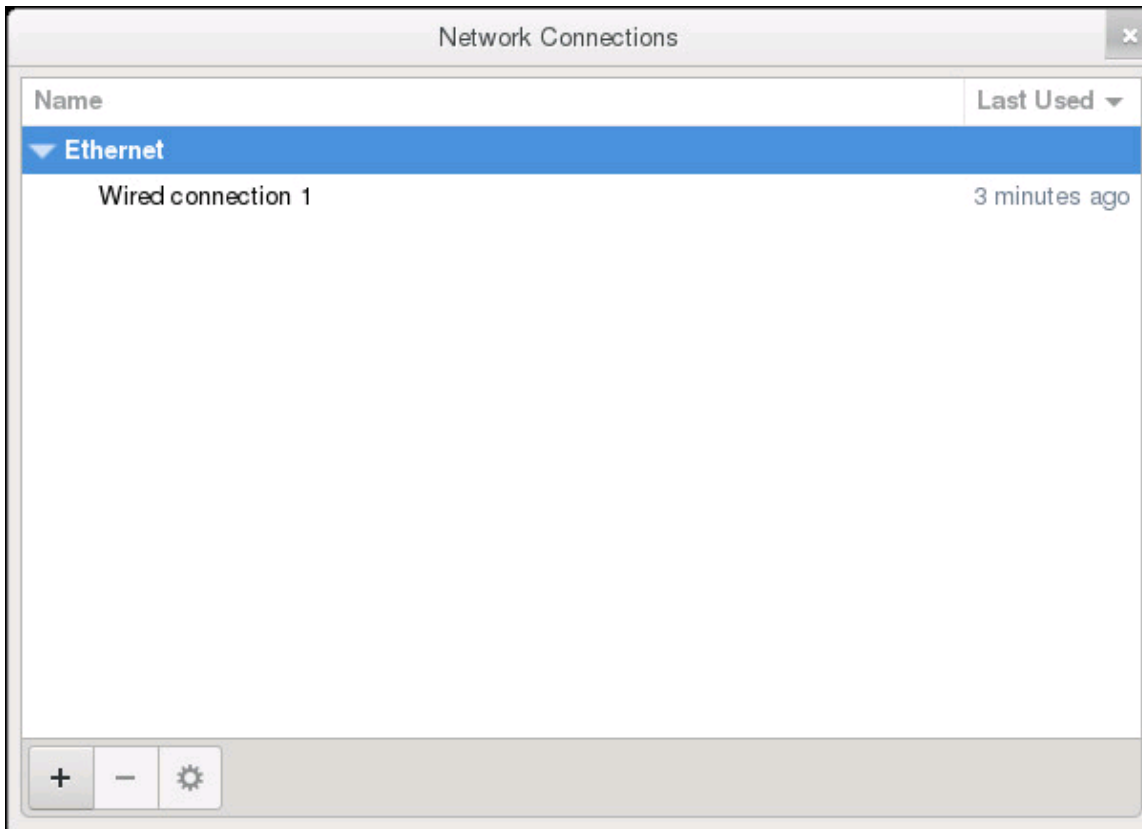
- a. 在**日期和时间**选项卡中, 选中**通过网络同步日期和时间**复选框。仅当使用管理员门户成功配置 NTP 之后, 才会启用**通过网络同步日期和时间**复选框。有关配置 NTP 的更多信息, 请参阅[设置网络时间协议 \(NTP\) 服务器](#) 页面上的 21。
  - b. 单击**时区**, 并选择适当的时区, 然后单击**确定**。
6. 要配置 OMIVV 设备的网络, 请单击**网络配置**。

要在 vSphere 环境中管理 Dell EMC 服务器, OMIVV 需要具有访问 vSphere 网络 (vCenter 和 ESXi 管理网络) 和带外网络 (iDRAC、CMC 和 OME-Modular) 的权限。

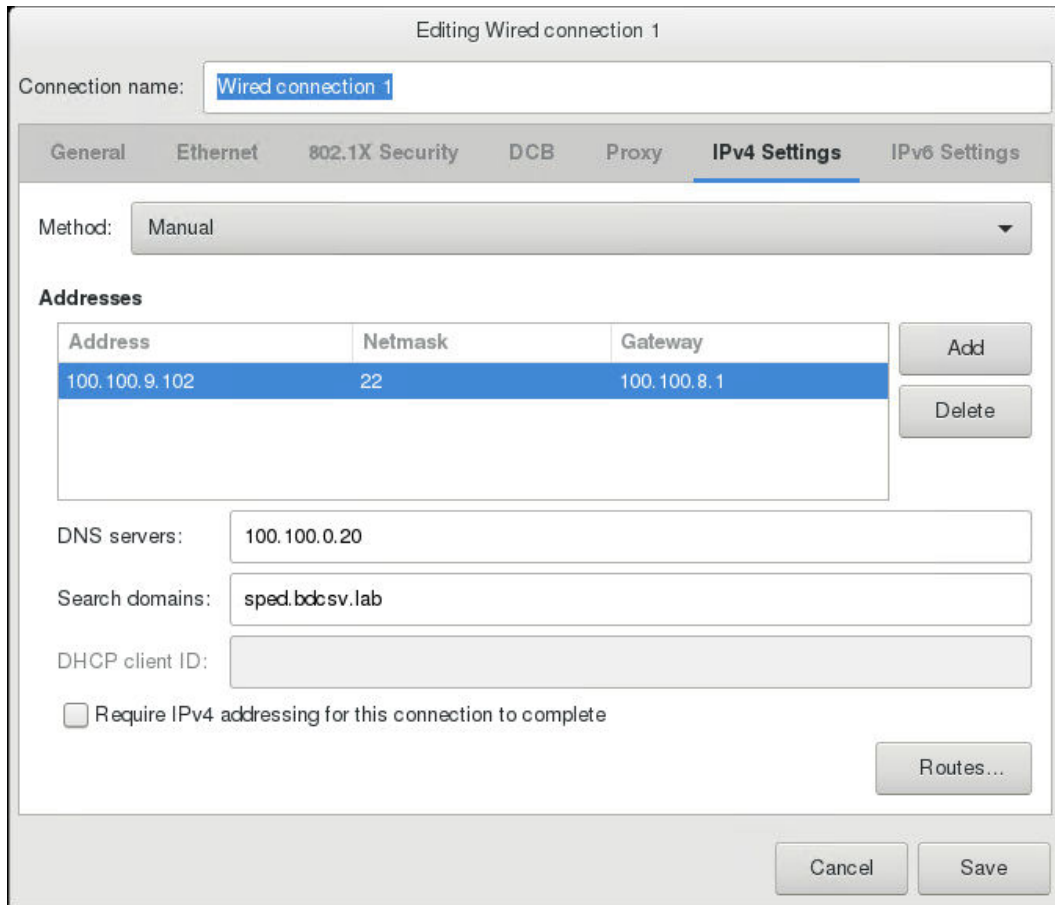
如果 vSphere 网络和带外网络在您的环境中作为单独的隔离网络进行维护, 则 OMIVV 需要具有访问这两个网络的权限。在这种情况下, OMIVV 设备必须配置两个网络适配器。建议在初始配置过程中配置两个网络。

如果您可以使用 vSphere 网络访问带外网络, 请不要为 OMIVV 设备配置两个网络适配器。有关配置 “第二个 NIC” 的更多信息, 请参阅[使用两个网络接口控制器 \(NIC\) 配置 OMIVV 设备](#) 页面上的 26。

7. 选择**有线连接 1**, 然后单击 。



- a. 单击 **IPv4 设置** 选项卡，从 **方法** 下拉列表中选择 **手动**，然后单击 **添加**。
  - ① **注:** 如果您选择“自动 (DHCP)”，则不要输入任何 IP 地址，因为在下一次重新启动过程中，OMIVV 设备会自动从 DHCP 服务器接收 IP。
- b. 输入有效的 IP、网络掩码（无类别域间路由 (CIDR) 格式）和网关信息。  
如果您在 **网络掩码** 框中输入 IP 地址，则它会自动转换为相应的 CIDR 格式。
- c. 分别在 **DNS 服务器** 和 **搜索域** 框中输入要搜索的 DNS 服务器 IP 和域。
- d. 选中 **需要 IPv4 地址才能完成此连接** 复选框，然后单击 **保存**。



**注:**

有时，使用静态 IP 配置 OMIVV 设备后，OMIVV 终端公用程序页面不会立即刷新并显示更新的 IP。要解决此问题，请退出 OMIVV 终端公用程序，然后再次登录。

8. 要更改 OMIVV 设备的主机名，请单击**更改主机名**。
  - a. 输入有效的主机名，然后单击**更新主机名**。

**注:** 如果在任何 vCenter 服务器中已注册了 OMIVV 设备，请注销再重新注册所有 vCenter 实例。有关详细信息，请参阅《安装指南》中的“管理取消注册和重新注册”主题。

9. 重新启动设备。

## 使用两个网络接口控制器 (NIC) 配置 OMIVV 设备

要在 vSphere 环境中管理 Dell EMC 服务器，OMIVV 需要具有访问 vSphere 网络（vCenter 和 ESXi 管理网络）和带外网络（iDRAC、CMC 和 OME-Modular）的权限。如果 vSphere 网络和带外网络在您的环境中作为单独的隔离网络进行维护，则 OMIVV 需要具有访问这两个网络的权限。在这种情况下，OMIVV 设备必须配置两个 NIC。如果可以使用 vSphere 网络访问带外网络，则不要为 OMIVV 设备配置两个 NIC。

确保您已准备好带外网络和 vSphere 网络的以下信息：

- 设备的 IP 地址、子网掩码（CIDR 格式）和网关（如果为静态）。
- 默认网关 - 必须将默认网关配置为具有互联网连接的唯一网络。建议将 vSphere 网络用作默认网关。
- 路由要求（网络 IP、子网掩码和网关）- 对于无法直接访问或无法使用默认网关访问的其他外部网络，请配置静态路由。
- DNS 要求 - OMIVV 只支持一个网络的 DNS 配置。有关 DNS 配置的更多信息，请转至本主题中的步骤 9 (b)。

1. 关闭 OMIVV 设备。
2. 使用 vSphere Client (HTML-5) 编辑虚拟机设置并添加附加的网络适配器。要编辑虚拟机设置，请右键单击虚拟机，然后单击**编辑设置**。
3. 单击**添加新设备**，选择**网络适配器**。

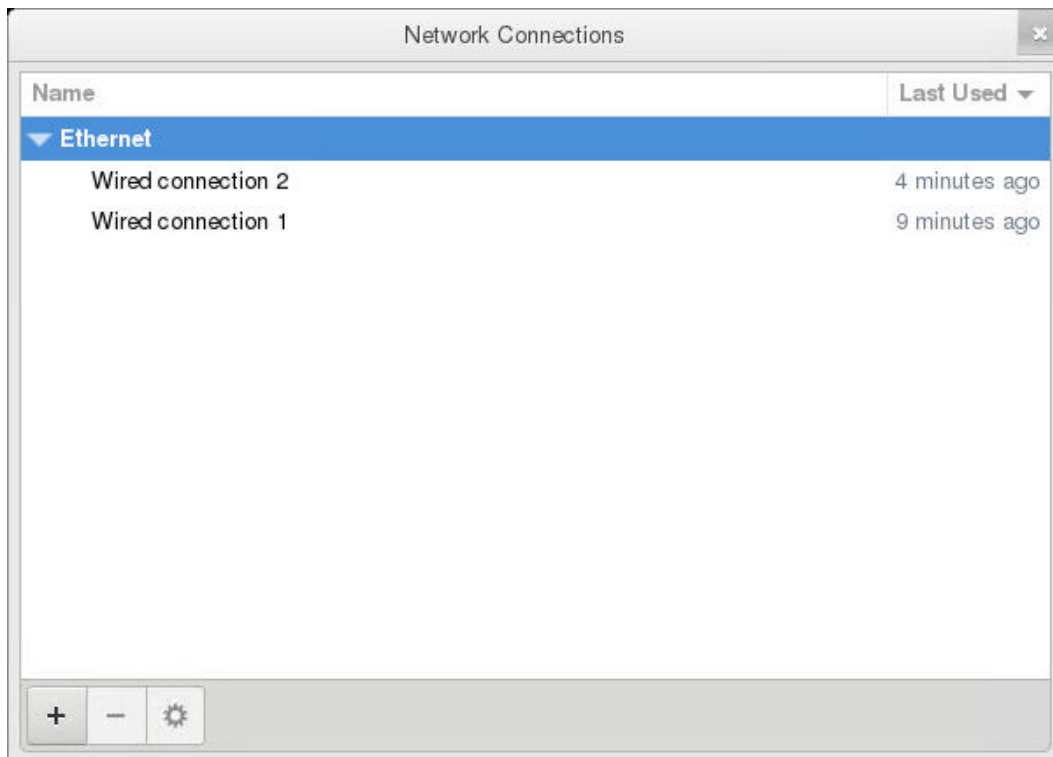
		ADD NEW DEVICE
> CPU	2	CD/DVD Drive Host USB Device Hard Disk RDM Disk Existing Hard Disk <b>Network Adapter</b> SCSI Controller USB Controller SATA Controller NVMe Controller Shared PCI Device PCI Device
> Memory	8 GB	
> Hard disk 1	85.436523437 GB	
> Network adapter 1	PGNet-IB Network	
> USB controller	USB 2.0	
> Video card	Specify custom settings	
VMCI device	Device on the virtual machine PCI bus that virtual machine communication interface	
> Other	Additional Hardware	


- a. 为 NIC 选择适当的网络，然后选中**在开机时连接**复选框。
- b. 从下拉菜单中选择 **VMXNET3** 适配器类型。


**注:** OMIVV 支持 VMXNET3 类型的 NIC。

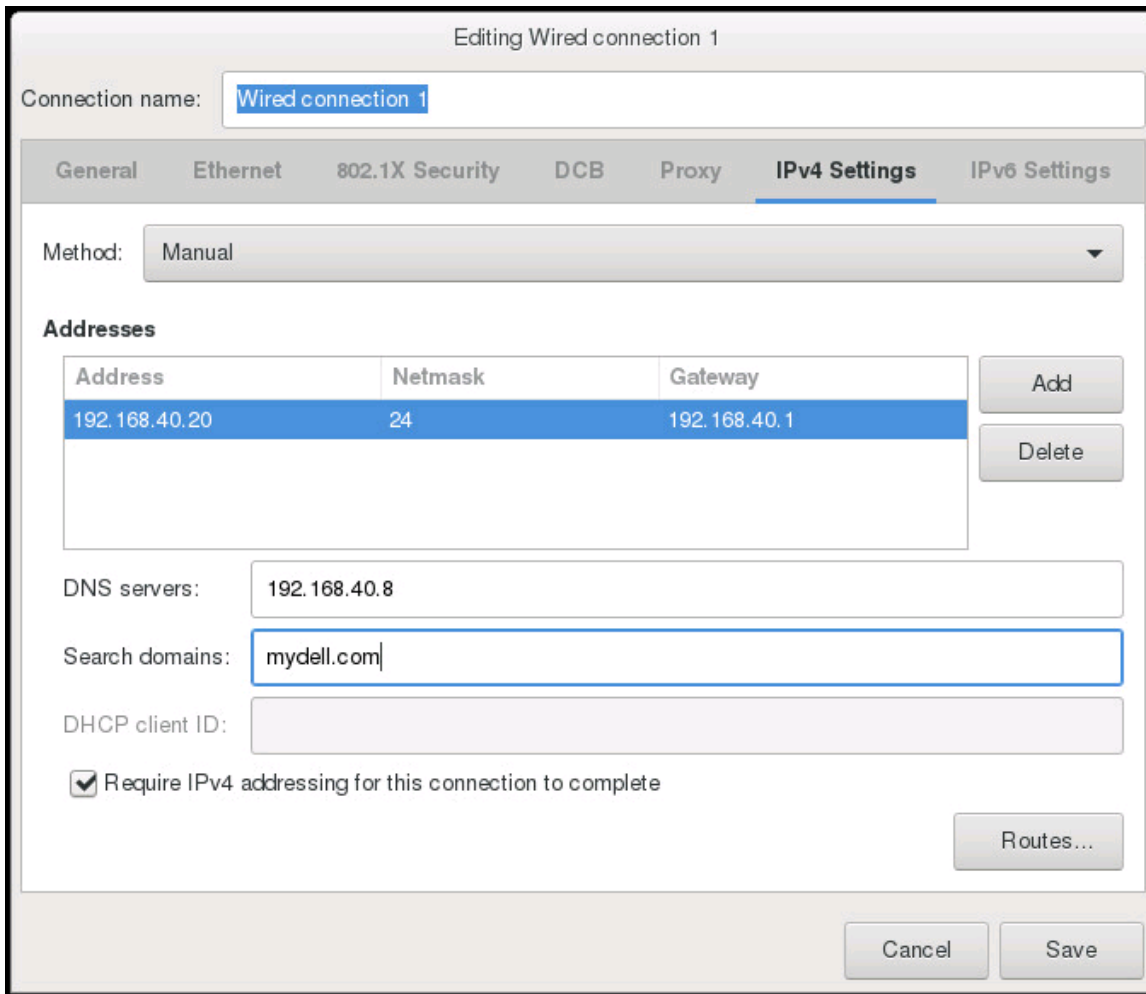
		ADD NEW DEVICE
> CPU	2	CANCEL <input type="button" value="OK"/>
> Memory	8 GB	
> Hard disk 1	85.436523437 GB	
> Network adapter 1	PGNet-IB Network <input checked="" type="checkbox"/> Connect...	
> New Network * Status	PvtNW_4_DualNIC <input checked="" type="checkbox"/> Connect At Power On	
Adapter Type	E1000	
MAC Address	Automatic	
> USB controller	USB 2.0	

4. 开启 OMIVV 设备。以管理员身份登录（默认用户名是 Admin），然后按 **Enter** 键。
5. 在 **OpenManage Integration for VMware vCenter 虚拟设备设置**实用程序中，单击**网络配置**。此时，**网络连接**页面会显示两个 NIC。

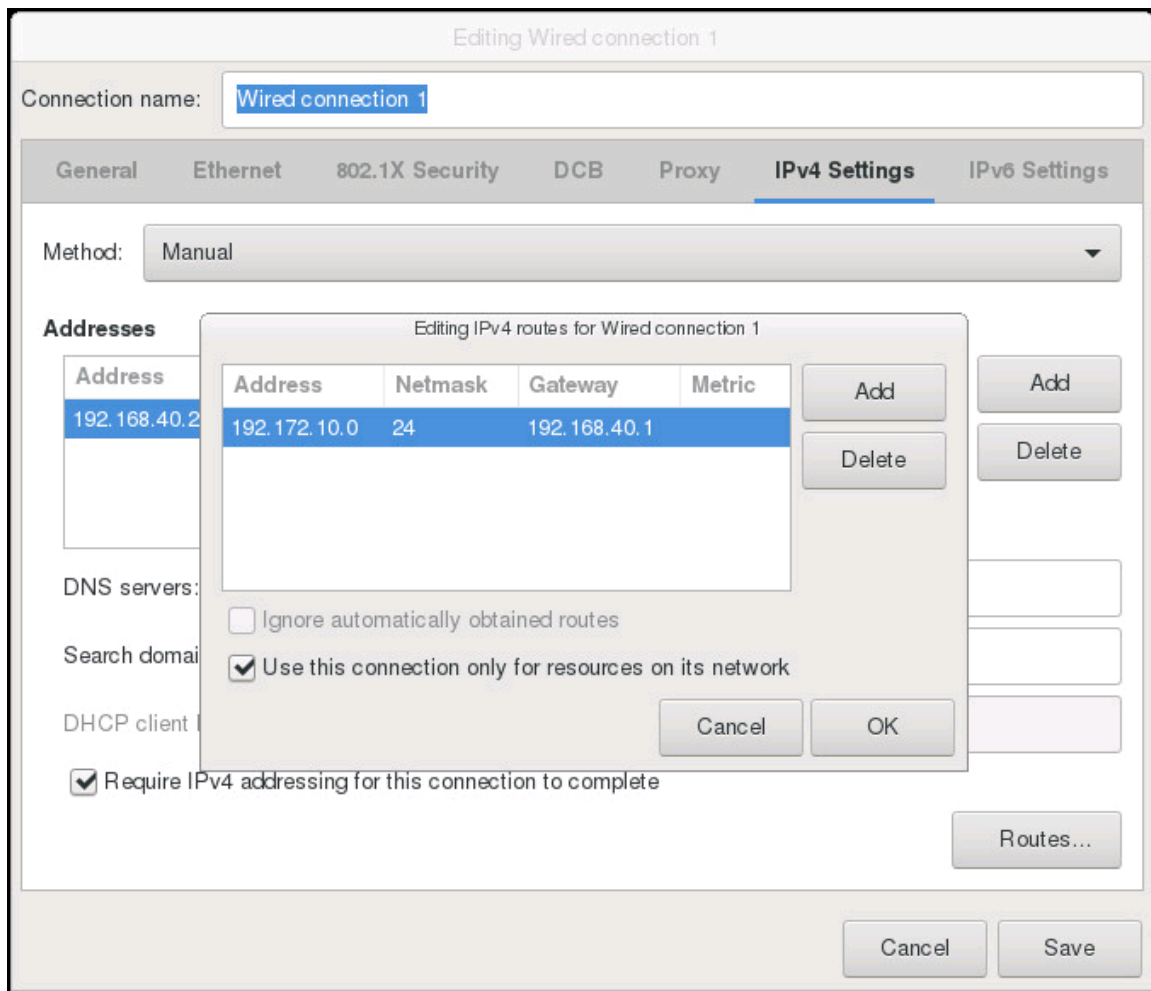


 **警告:** 不要使用 + 来添加任何新的网络接口。必须使用“vSphere 编辑设置”来添加 NIC。

6. 选择您要配置的 NIC 并单击 。
7. 要识别正确的 NIC，请使用在**以太网**选项卡上显示的 MAC ID，然后将它与 vSphere Client (HTML-5) 中显示的 MAC ID 进行比较。  
确保不要更改**以太网**选项卡中列出的默认 MAC 地址。
8. 单击**常规**选项卡并选中**当此网络可用时自动连接**复选框。
9. 单击**IPv4 设置**选项卡，执行下列操作之一：



- a. 从**方法**下拉列表中选择**手动或自动 (DHCP)**。
- b. 如果您选择**手动**方法，请单击**添加**，然后输入有效的 IP 地址、子网掩码（CIDR 格式）和网关详细信息。如果您想要控制 DNS 服务器的优先级（主要和次要 DNS 条目），建议使用静态 IP。  
 一般情况下，数据中心的 vSphere 元素（例如 vCenter 和 ESXi 主机）使用主机名或 FQDN 进行管理。iDRAC、CMC 和 OME-Modular 使用 IP 地址进行管理。在本示例中，建议您仅配置 vSphere 网络的 DNS 设置。  
 如果 vSphere 网络和 iDRAC 网络都使用主机名或 FQDN 进行管理，则 DNS 服务器的配置方式必须使它能够解析这两个网络的主机名或 FQDN。有关更多信息，请参阅 CentOS 说明文件。  
 ⓘ **注：**最后配置的 DNS 服务器将成为主要 DNS，不论您是为哪个网络配置 DNS 的。
- c. 分别在 **DNS 服务器**和**搜索域**框中输入要搜索的 DNS 服务器 IP 和域。
- d. 选中**需要 IPv4 地址才能完成此连接**复选框，然后单击**保存**。
- e. 如果不想将此网络用作默认网络（网关），请单击**路由**，然后选中**此连接仅用于其网络上的资源**复选框。  
 ⓘ **注：**将多个网络添加为默认网关可能会导致网络问题，并且 OMIVV 的功能可能会受影响。
- f. 如果您想要使用已知网关访问任何外部网络，请在同一页面上单击**添加**，然后添加网络 IP 地址、子网掩码（CIDR 格式）和网关详细信息。



一般情况下，已配置为默认网关的网络不需要任何手动路由配置，因为网关能够提供可访问性。但是，未配置默认网关的网络（其中已选中**此连接仅用于其网络上的资源**复选框），则可能需要手动路由配置。因为没有为此网络配置默认网关以访问外部网络，所有需要手动路由配置。

**注：** 不正确的路由配置可能会突然让网络接口停止响应。请确保路由条目配置合宜。

g. 单击**确定**。

10. 单击**保存**。要配置另一个 NIC，请重复任务 6–10。

11. 在 **OpenManage Integration for VMware vCenter 虚拟设备设置** 实用程序中，单击**重新引导设备**。只有在重新启动 OMIVV 设备之后，网络配置才能完成。

成功重新启动设备后，NIC 便会如配置那样开始工作。可以通过以**只读**用户身份登录并运行以下命令来查看 NIC 的状态：  
ifconfig、ping 和 route -n。

## 更改 OMIVV 设备密码



可以在 vSphere 客户端中使用控制台更改 OMIVV 设备密码。

1. 打开 OMIVV Web 控制台。
2. 在 **OpenManage Integration for VMware vCenter 虚拟设备设置** 实用程序中，单击**更改管理员密码**。  
按照屏幕上的说明设置密码。
3. 在**当前密码**文本框中，输入当前管理员密码。
4. 在**新密码**文本框中输入新密码。
5. 在**确认新密码**文本框中输入新密码。
6. 单击**更改管理员密码**。

## 配置网络时间协议 (NTP) 并设置本地时区

1. 打开 OMIVV Web 控制台。
2. 在 **OpenManage Integration for VMware vCenter 虚拟设备设置实用程序** 中，单击 **日期/时间属性**。  
确保在管理员控制台中输入 NTP 的详细信息。有关更多信息，请参阅 [设置网络时间协议 \(NTP\) 服务器](#) 页面上的 21。
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. 要添加其他 NTP 服务器 IP 或主机名（如果需要），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**。

## 更改 OMIVV 设备的主机名

1. 在 **OpenManage Integration for VMware vCenter 虚拟设备设置实用程序** 中，单击 **更改主机名**。  
 **注：**如果在任何 vCenter 服务器中注册了 OMIVV 设备，请注销再重新注册所有 vCenter 实例。
  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**。  
更新设备主机名，将显示主菜单页面。
  4. 要重新引导设备，单击 **重新引导设备**。
-  **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 和 Dell EMC Repository Manager (DRM) 中配置服务器。


## 重新引导 OMIVV 设备

1. 打开 OMIVV Web 控制台。
2. 在 **OpenManage Integration for VMware vCenter 虚拟设备设置实用程序** 中，单击 **重新引导设备**。
3. 要重新引导设备，单击 **是**。

## 将 OMIVV 设备重置为出厂设置

1. 打开 OMIVV Web 控制台。
2. 在 **OpenManage Integration for VMware vCenter 虚拟设备设置实用程序** 中，单击 **重置设置**。  
系统将显示以下消息：

```
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**。  
如果单击 **是**，OMIVV 设备会重设为出厂默认设置，所有其他设置和现有数据将会删除。  
完成恢复出厂设置后，再次将 vCenter 注册到 OMIVV 设备。
-  **注：**OMIVV 设备重置为出厂默认设置后，对网络配置进行的任何更新都将保留。这些设置不会重设。

## 只读用户角色

名为只读的无权限用户出于诊断目的具有 shell 访问权限。只读用户具有运行少数命令的有限权限。

## 使用仪表板监测主机和机箱

仪表板会显示以下内容：

- 主机和机箱的运行状况状态
- 主机和机箱的保修状态
- 主机和 vCenter 的许可证信息
- 主机的配置合规性状态
- 使用 OMIVV 安排的作业的状态
- 可用于部署的裸机服务器
- OMIVV 功能快速参考

### 运行状况

**运行状况**部分显示所有受 OMIVV 管理的主机和机箱的运行状况。此处显示的所有主机使用相同的平台服务控制器 (PSC) 进行配置。

从主机和机箱完成定期运行状况指标任务或 SNMP 事件（针对特定主机和机箱触发运行状况指标作业）后，每个主机和机箱的状态都会刷新。

默认情况下，运行状况指标任务每小时运行一次。显示的数据用于监测控制面板上服务器和机箱的主动式高可用性运行状况和运行状况更新。作业的详细信息将在日志中提供。

以下列表介绍了主机和机箱的不同状态：

- **正常** - 显示处于正常状态的主机和机箱的总数。
- **警告** - 显示需要采取纠正措施但不会立即影响系统的主机和机箱数量。
- **严重** - 显示主机或机箱中的一个或多个组件发生严重问题并且需要立即采取措施的主机和机箱数量。
- **未知** - 显示处于未知状态的主机和机箱的总数。当主机或机箱不可访问或运行状况未知时，主机或机箱会显示“未知”状态。

要查看有关主机的详细信息，请在**仪表板**页面上的**运行状况**部分下，单击**查看主机**。

要查看有关机箱的更多信息，请在**仪表板**页面上的**运行状况**部分下，单击**查看机箱**。

### 保修

在此保修类别下显示的主机数表示属于使用 PSC 的 vCenter 服务器的主机。要获取有关主机和机箱的保修信息，请确保您已在**设置**页面中启用保修到期通知。

对于具有“下一工作日 (NBD)”和“仅部件保修 (POW)”等保修类型的多种或不同的保修，OMIVV 将根据保修天数最低的保修类型显示状态。

**保修**部分提供了有关主机和机箱的以下信息：

- **正常** - 显示剩余保修天数高于警告阈值的主机和机箱数量。
- **警告** - 显示剩余保修天数低于警告阈值的主机和机箱数量。
- **严重** - 显示剩余保修天数低于严重阈值的主机和机箱数量。
- **未知** - 显示保修未知的主机和机箱的数量。

要识别处于**正常**、**警告**、**严重**和**未知**状态的主机，请执行以下操作：

1. 转到**主机和群集**。
2. 要在群集级别查看主机的运行状况，请选择群集，然后单击**监测 > OMIVV 群集信息 > 保修**。
3. 要在数据中心级别查看主机的运行状况，请选择数据中心，然后单击**监测 > OMIVV 数据中心信息 > 保修**。

# 许可证

许可证部分显示以下信息：

- 所有主机和 vCenter 许可证计数
- 可用主机和 vCenter 许可证计数
- 显示正在使用的主机和 vCenter 许可证的数量。

要购买许可证，请在**仪表盘**页面上的**许可证**部分下，单击**购买许可证**。

# 准备部署

本节仅列出使用 OMIVV 查找到的符合要求的裸机服务器。要部署裸机服务器，请单击**部署**。

# 配置合规性

此部分显示属于与群集配置文件相关联的群集一部分的主机。此处显示的主机使用相同的平台服务控制器 (PSC) 进行配置。

要查看主机的配置合规性状态，请单击**查看合规性**。

# 作业

此部分显示显示使用 OMIVV 计划的作业。您只能查看过去 7 天的作业详细信息。

饼图显示了处于**成功**、**正在进行**、**失败**、**已计划**和**已取消**状态的作业总数。要从饼图中筛选作业状态，请单击作业状态。

您可以查看处于**成功**、**进行中**、**失败**、**已计划**和**已取消**状态的以下作业的计数：

- 部署作业  
有关更多信息，请参阅 [部署作业](#) 页面上的 67。
- 主机固件更新作业  
有关更多信息，请参阅 [主机固件更新作业](#) 页面上的 69。
- 机箱固件更新作业  
有关更多信息，请参阅 [机箱固件更新作业](#) 页面上的 68。
- 系统锁定作业  
有关更多信息，请参阅 [系统锁定模式作业](#) 页面上的 69。

要查看所有作业的状态，请单击**查看所有作业**。

# 快速参考

本部分提供了以下功能的快速参考：

- 启动初始配置向导  
有关更多信息，请访问 [初始配置](#) 页面上的 79
- 主机凭据配置文件  
有关更多信息，请访问 [主机凭据配置文件](#) 页面上的 35
- 管理合规性  
有关更多信息，请访问 [管理合规性](#) 页面上的 62
- 机箱凭据配置文件  
有关更多信息，请访问 [机箱凭据配置文件](#) 页面上的 39
- 群集配置文件

- 有关更多信息，请访问 [群集配置文件](#) 页面上的 45 部署
- 有关更多信息，请访问 [部署任务清单](#) 页面上的 57

# 使用主机凭据配置文件管理主机

## 主机凭据配置文件

主机凭据配置文件存储 OMIVV 用来与服务器通信的 iDRAC 和主机凭据。OMIVV 管理与主机凭据配置文件关联的主机。您可以将多个服务器关联到单个主机凭据配置文件。

使用单个统一机箱管理 IP 管理 PowerEdge MX 机箱主机。需要使用机箱凭据配置文件管理已禁用 iDRAC IP 的 PowerEdge MX 机箱中存在的主机。要使用机箱凭据配置文件管理 PowerEdge MX 机箱，请参阅 [创建机箱凭据配置文件](#) 页面上的 39。建议管理具有 iDRAC IP 的 PowerEdge MX 机箱主机以使用主机凭据配置文件获取完整的 OMIVV 功能。

## 创建主机凭据配置文件

如果已添加的主机数量超出许可证限值，则无法创建主机凭据配置文件。

在结合使用 Active Directory (AD) 凭据与主机凭据配置文件之前，请确保：

- 用户帐户存在于 AD 中。
  - 为 iDRAC 和主机配置基于 AD 的验证。
1. 在 OMIVV 主页中，单击 **合规性和部署 > 主机凭据配置文件**。
  2. 在 **主机凭据配置文件** 页面中，单击 **创建新配置文件**。
  3. 在向导的 **机箱凭据配置文件** 页面中，阅读说明，然后单击 **开始**。
  4. 在 **名称和凭据** 页面中，请执行以下操作：
    - a. 编辑配置文件名称和说明。“说明”字段为可选项。
    - b. 从 **vCenter 名称** 列表中，选择您要在其上创建主机凭据配置文件的 vCenter 实例。
    - c. 在 **iDRAC 凭据** 区域中，输入 iDRAC 本地凭据或 AD 凭据。
      - 要输入 iDRAC 的本地凭据，请执行以下任务：
        - 在 **用户名** 框中输入用户名。用户名限制为 16 个字符。  
有关定义用户名的信息，请参阅 <https://www.dell.com/support> 上提供的 *iDRAC 用户指南*。
        - 输入密码。  
有关建议在用户名和密码中使用的字符的更多信息，请参阅 *iDRAC 用户指南*，网址为 <https://www.dell.com/support>。
      - 要下载和存储 iDRAC 证书并在未来的所有连接期间对其进行验证，请选中 **启用证书检查** 复选框。
      - 要输入已配置并已针对 AD 启用的 iDRAC 的凭据，请选中 **使用 Active Directory** 复选框。
 

**注：** iDRAC 帐户需要用于更新固件并部署操作系统 (OS) 的管理权限。

        - 在 **Active Directory 用户名** 框中输入用户名。  
以下列格式之一输入用户名，例如 `domain\username` 或 `username@domain`。用户名限制为 256 个字符。有关用户名的限制信息，请参阅 **Microsoft Active Directory 说明文件**。
        - 输入密码。  
AD 凭据可以是相同或独立的 iDRAC 和主机。
    - d. 在 **主机根** 区域中，输入本地主机凭据或 AD 凭据。  
默认用户名是 root。
      - 要输入本地主机凭据，请执行以下操作：

- 输入密码。

仅运行 ESXi 6.5 U3 及更早版本的主机需要主机密码。

要为 ESXi 6.7 及更高版本跳过此步骤，请确保清除**使用主机凭据**复选框。如果为运行 ESXi 6.7 和更高版本的主机输入了密码，密码将被忽略。

对于运行 ESXi 6.7 及更高版本的主机，不需要提供 ESXi 凭据。即使输入的主机凭据不正确，OMIVV 仍可将 iDRAC 与其 ESXi 主机配对。

- 要输入已配置并已针对 AD 启用的主机的凭据，请选中**使用 Active Directory** 复选框。
  - 在 **Active Directory 用户名**框中输入用户名。以下列格式之一输入用户名，例如 domain\username 或 username@domain。用户名限制为 256 个字符。有关用户名的限制信息，请参阅 **Microsoft Active Directory 说明文件**。
  - 输入密码。
- 要下载和存储主机证书并在未来的所有连接期间对其进行验证，请选中**启用证书检查**复选框。

#### 5. 单击**下一步**。

此时会显示**选择主机**页面。

#### 6. 在**选择主机**页面中，展开树视图并选择主机，然后单击**确定**。

- 要从**关联的主机**页面中添加或删除主机，请单击**添加主机**。

**注：**不要将已禁用 iDRAC IPv4 的 PowerEdge MX 服务器添加到主机凭据配置文件。这些服务器是使用机箱凭据配置文件管理的。

所选主机显示在**关联的主机**页面上。

#### 7. 要测试连接，请选择一个或多个主机，然后单击**开始测试**。

建议您测试所有已配置主机的连接。

在测试连接过程中，OMIVV 在运行 ESXi 6.5 及更高版本的主机上会启用 WBEM 服务，然后在检索 iDRAC IP 之后会禁用该服务。

**注：**当您输入有效的凭据之后，针对主机的测试连接操作也可能会失败，并显示一条消息，表明输入了无效的凭据。如果 ESXi 阻止了访问，则会观察到此问题。多次尝试使用错误的凭据连接 ESXi 会阻止访问 ESXi，阻止时长为 15 分钟。等待 15 分钟，然后重试此操作。

- 要停止测试连接过程，请单击**中止测试**。

您可以在**测试结果**部分中查看测试连接结果。

#### 8. 单击**完成**。

## 编辑主机凭据配置文件

您可以一次编辑多个主机凭据配置文件的凭据。

#### 1. 在**名称和凭据**页面中，请执行以下操作：

- a. 编辑配置文件的名称和说明。
- b. 在 **iDRAC 凭据**区域中，编辑 iDRAC 本地凭据或 AD 凭据。

- 要更改 iDRAC 的本地凭据，请执行以下任务：

- 在**用户名**框中更改用户名。用户名限制为 16 个字符。

有关定义用户名的信息，请参阅 [dell.com/support](http://dell.com/support) 上提供的 *iDRAC 用户指南*。

- 更改密码。
- 要下载和存储 iDRAC 证书并在未来的所有连接期间对其进行验证，请选中**启用证书检查**复选框。

- 要更改已配置并已针对 AD 启用的 iDRAC 的凭据，请选中**使用 Active Directory** 复选框。

**注：**iDRAC 帐户需要用于更新固件并部署操作系统 (OS) 的管理权限。

- 在 **Active Directory 用户名**框中更改用户名。

以下列格式之一输入用户名，例如 domain\username 或 username@domain。用户名限制为 256 个字符。有关定义用户名的更多信息，请参阅 *Microsoft Active Directory 说明文件*。

- 输入密码。

- 要下载和存储 iDRAC 证书并在未来的所有连接期间对其进行验证，请选中**启用证书检查**复选框。
- c. 在**主机根**区域中，修改本地主机凭据或 AD 凭据。
- 要输入本地主机凭据，请执行以下操作：
    - 默认用户名是 root。
    - 输入密码。
 

仅运行 ESXi 6.5 U3 及更早版本的主机需要主机密码。

要为 ESXi 6.7 及更高版本跳过此步骤，请确保清除**使用主机凭据**复选框。如果为运行 ESXi 6.7 和更高版本的主机输入了密码，密码将被忽略。

对于运行 ESXi 6.7 及更高版本的主机，不需要输入 ESXi 凭据。即使输入的主机凭据不正确，OMIVV 仍可将 iDRAC 与其 ESXi 主机配对。
  - 要更改已配置并已针对 AD 启用的主机的凭据，请选中**使用 Active Directory** 复选框。
    - 在 **Active Directory 用户名**框中更改用户名。
 




以下列格式之一输入用户名，例如 domain\username 或 username@domain。用户名限制为 256 个字符。有关维修的高级说明，请参阅 support.dell.com/manuals 上的有关用户名的限制信息，请参阅 *Microsoft Active Directory 说明文件*。
    - 更改密码。
  - 要下载和存储主机证书并在未来的所有连接期间对其进行验证，请选中**启用证书检查**复选框。
2. 单击**下一步**。  
将显示**关联的主机**页面。
3. 要在关联的主机列表中添加或删除主机，请在**关联的主机**页面中，单击**添加主机**。
- 注**：不要将已禁用 iDRAC IPv4 的 PowerEdge MX 服务器添加到主机凭据配置文件。这些服务器是使用机箱凭据配置文件管理的。
- 所选主机显示在**关联的主机**页面上。
4. 要测试连接，请选择一个或多个主机，然后单击**开始测试**。建议您测试所有已配置主机的连接。
- 注**：当您输入有效的凭据之后，针对主机的测试连接操作也可能会失败，并显示一条消息，表明输入了无效的凭据。如果 ESXi 阻止了访问，则会观察到此问题。多次尝试使用错误的凭据连接 ESXi 会阻止访问 ESXi，阻止时长为 15 分钟。等待 15 分钟，然后重试此操作。
- 要停止测试连接，请单击**中止测试**。
- 您可以在**测试结果**部分中查看测试连接结果。
- 在测试连接过程中，OMIVV 在运行 ESXi 6.5 及更高版本的主机上会启用 WBEM 服务，然后在检索 iDRAC IP 之后会禁用该服务。
5. 单击**完成**。
- 注**：修改日期和上次修改者字段中包括您使用 vSphere Client 界面为主机凭据配置文件执行的更改。OMIVV 设备在各自的主机凭据配置文件上执行的任何更改并不影响这两个字段。

## 查看主机凭据配置文件

1. 在 OMIVV 主页中，单击**合规性和部署 > 主机凭据配置文件**。  
表格显示所有主机凭据配置文件及以下信息：
  - **配置文件名称** — 主机凭据配置文件的名称
  - **说明** — 配置文件说明（如果提供）
  - **vCenter** — 关联 vCenter 的 FQDN 或主机名或 IP 地址
  - **关联的主机** — 与主机凭据配置文件关联的主机如果有多个关联的主机，请使用展开图标显示全部。
  - **iDRAC 证书检查** - 指示在创建主机凭据配置文件时是否验证 iDRAC 证书。
  - **主机根证书检查** - 指示在创建主机凭据配置文件时是否验证主机根证书。
  - **创建日期** — 创建主机凭据配置文件的日期
  - **修改日期** — 修改主机凭据配置文件的日期

- **上次修改者** — 修改主机凭据配置文件的用户的详细信息

**注:** 如果使用机箱凭据配置文件管理 PowerEdge MX 主机，则 OMIVV 会将其显示为与某个机箱凭据配置文件关联。有关更多信息，请参阅 [查看机箱凭据配置文件](#) 页面上的 40。

2. 如果您要从向导中移除或添加列名称，请单击 。  
默认情况下，**修改日期**和**上次修改日期**列未选中。要选择这些列，请单击 。
3. 要导出主机凭据配置文件信息，请单击 。

## 测试主机凭据配置文件

使用测试凭据配置文件功能，您可以测试主机和 iDRAC 凭据。建议您选择所有主机。

1. 在 OMIVV 主页中，选择具有关联主机的主机凭据配置文件，然后单击**测试**。  
此时将显示**测试主机凭据配置文件**页面。
2. 选择所有关联的主机并单击**开始测试**。
  - a. 要停止测试连接，请单击**中止测试**。  
将会显示 iDRAC 和主机凭据的测试连接结果。

## 删除主机凭据配置文件

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主机凭据配置文件。

OMIVV 不会管理是您删除的主机凭据配置文件一部分的主机，直至这些主机添加到另一个主机凭据配置文件。

1. 在**主机凭据配置文件**页面上，选择配置文件并单击**删除**。
2. 当提示确认时，单击**删除**。  
所选配置文件将从“主机凭据配置文件”列表中删除。

# 使用机箱凭据配置文件管理机箱

## 机箱凭据配置文件

“机箱凭据配置文件”存储 OMIVV 用来与机箱通信的机箱凭据。OMIVV 管理和监测与机箱凭据配置文件关联的机箱。可以将多个机箱分配到单个机箱凭据配置文件。

使用单个统一机箱管理 IP 管理 PowerEdge MX 机箱主机。需要使用机箱凭据配置文件管理已禁用 iDRAC IP 的 PowerEdge MX 机箱中存在的主机。建议管理具有 iDRAC IP 的 PowerEdge MX 机箱主机以使用主机凭据配置文件获取完整的 OMIVV 功能。有关管理 MX 机箱的更多信息，请参阅[管理 PowerEdge MX 机箱](#) 页面上的 99。

## 创建机箱凭据配置文件

- 要创建机箱凭据配置文件，您必须具有以下权限：
    - M1000e、VRTX 和 FX2 机箱 — 读取和设置 SNMP 陷阱目标
    - PowerEdge MX 机箱 — 管理员
  - 在结合使用 Active Directory (AD) 凭据与主机凭据配置文件之前，请确保：
    - 用户帐户存在于 AD 中。
    - CMC 或 OME 模块配置为基于 AD 的身份验证。
  - 对于 PowerEdge MX 机箱，请确保在注册的 vCenter 中至少有一个 MX 主机，以便成功完成测试连接。
1. 在 OMIVV 主页中，单击**合规性和部署 > 机箱凭据配置文件 > 创建新配置文件**。
  2. 在向导的**机箱凭据配置文件**页面中，阅读说明，然后单击**开始**。
  3. 在**名称和凭据**页面中，请执行以下操作：
    - a. 输入配置文件名称和说明。“说明”字段为可选项。
    - b. 在**用户名**文本框中，输入具有管理权限的用户名（通常用于登录到 Chassis Management Controller (CMC) 或者 OpenManage Enterprise-Modular (OME-Modular)）。
    - c. 在**密码**文本框中，输入密码。
    - d. 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。
  4. 在**选择机箱**页面中，使用**IP/主机名**列旁边的复选框选择单独的机箱或多个机箱，然后单击**确定**。所选主机显示在**关联的机箱**页面上。要从关联的机箱列表中添加或删除机箱，请单击**添加机箱**。

如果所选机箱已与机箱凭据配置文件相关联，则随后会显示一条消息：

选择当前与另一个配置文件关联的机箱将会从该机箱凭据配置文件中移除该机箱。将会删除没有关联机箱的机箱凭据配置文件。

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。

测试连接会为所选机箱自动运行。

测试连接将在以下情况下自动运行：

- 在首次选中机箱后。
- 在您更改凭据时
- 如果该机箱为全新所选机箱

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

对于配置有 MCM 组的 PowerEdge MX 机箱，建议您使用主机箱管理所有主机箱和成员机箱。成员机箱测试连接操作将失败，并且测试结果显示为**失败**。将会显示主要机箱 IP 链接。单击主要机箱 IP，以查找完整的 MCM 组。

5. 单击**完成**。

确保您至少拥有一个已成功验证的机箱，以完成向导中的任务。只有成功验证的机箱才可以与机箱凭据配置文件相关联。

要添加 PowerEdge MX 机箱，请参阅[添加 PowerEdge MX 机箱](#) 页面上的 100。

## 编辑机箱凭据配置文件

1. 在 OMIVV 主页中，单击**合规性和部署 > 机箱凭据配置文件**。
2. 在**机箱凭据配置文件**页面中，单击**编辑**。
3. 在**名称和凭据**页面中，请执行以下操作：
  - a. 编辑配置文件的名称和说明。“说明”字段为可选项。
  - b. 在**用户名**文本框中，更改具有管理权限的用户名（通常用于登录到 Chassis Management Controller (CMC) 或者 OpenManage Enterprise-Modular (OME-Modular)）。
  - c. 在**密码**文本框中，输入密码。  
如果将“密码”字段留空，OMIVV 将考虑在创建工作流期间输入的密码。
  - d. 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。
4. 在**选择机箱**页面中，使用**IP/主机名**列旁边的复选框选择或移除机箱，然后单击**确定**。  
所选主机显示在**关联的机箱**页面上。要从关联的机箱列表中添加或删除机箱，请单击**添加机箱**。

如果所选机箱已与某个主机凭据配置文件相关联，则会显示以下消息：

选择当前与另一个配置文件关联的机箱将会从该机箱凭据配置文件中移除该机箱。将会删除没有关联机箱的机箱凭据配置文件。

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。

测试连接会为所选机箱自动运行。

测试连接将在以下情况下自动运行：

- 在首次选中机箱后。
- 在您更改凭据时
- 如果该机箱为全新所选机箱

测试结果在**测试结果**部分中显示为**通过或失败**。要手动测试机箱连接，请选择机箱并单击**开始测试**。

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

**注：**如果主机不存于与添加的 PowerEdge MX 机箱关联的已注册 vCenter 中，则机箱的测试连接将会失败。

5. 单击**完成**。  
确保您至少拥有一个已成功验证的机箱，以完成向导中的任务。只有成功验证的机箱才可以与机箱凭据配置文件相关联。  
要添加 PowerEdge MX 机箱，请参阅[添加 PowerEdge MX 机箱](#) 页面上的 100。

## 查看机箱凭据配置文件

创建一个或多个机箱凭据配置文件后，可以在“机箱凭据配置文件”页面中查看机箱和关联的机箱。

1. 在 OMIVV 主页中，单击**合规性和部署 > 机箱凭据配置文件**。

表格显示所有机箱凭据配置文件及以下信息：


- **配置文件名称** — 机箱凭据配置文件的名称
- **说明** - 配置文件说明
- **机箱 IP/主机名** - 机箱 IP 或主机名链接。

对于多机箱管理 (MCM) 组，主机箱 (  ) 和成员机箱 (  ) 在层次结构中列出。

**注：**对于 MCM 配置中的 PowerEdge MX 机箱，OMIVV 仅使用主机箱来管理所有主机箱和成员机箱。所有主机箱和成员机箱都关联至与主机箱关联的同一机箱凭据配置文件。

对于 MCM 组中的成员机箱 (IPv4 处于禁用状态)，将会显示主机箱的 IPv4 地址。成员机箱的服务标签也显示在括号中。

- **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。
2. 以下有关关联主机的信息显示在上部网格中：
    - **配置文件名称**
    - **关联的主机**
    - **服务标签**
    - **机箱 IP/主机名**
    - **机箱服务标签**
  3. 要导出机箱凭据配置文件信息，请单击 。

## 测试机箱凭据配置文件

您可以使用机箱测试凭据配置文件功能来测试与机箱凭据配置文件关联的机箱的凭据。建议您选择所有机箱。

1. 在 OMIVV 主页中，单击**合规性和部署 > 机箱凭据配置文件**。
2. 选择一个机箱凭据配置文件，然后单击**测试**。
3. 在**测试机箱凭据配置文件**页面上，选择关联的机箱，然后单击**开始测试**。
  - a. 要停止测试连接，请单击**中止测试**。  
测试结果将显示在**测试结果**列中。

## 删除机箱凭据配置文件

删除机箱凭据配置文件之前，确保机箱实例不是 OMIVV 注册到的其它 vCenter 的一部分。

如果已删除机箱凭据配置文件，则在将机箱添加到另一个机箱凭据配置文件之前，OMIVV 不会监视已删除的机箱凭据配置文件中存在的机箱。

1. 在 OMIVV 主页中，单击**合规性和部署 > 机箱凭据配置文件 > 删除**。
2. 选择要删除的机箱凭据配置文件。
3. 当提示确认时，单击**删除**。

如果所有与机箱凭据配置文件关联的机箱均已移除或移至不同的配置文件，则会显示删除确认消息。该消息指示机箱凭据配置文件不存在任何关联机箱，并且将被删除。

要删除该机箱凭据配置文件，请在确认删除消息上单击**确定**。

# 使用存储库配置文件管理固件和驱动程序存储库

## 存储库配置文件

通过存储库配置文件，您可以创建和管理驱动程序或固件存储库。

您可以使用固件和驱动程序存储库配置文件来执行以下操作：

- 更新主机的固件
- 更新 vSAN 群集中主机的驱动程序版本。
- 创建群集配置文件并将这些群集作为基线。

默认的 OMIVV 固件目录为：

- **Dell EMC 默认目录**：出厂时创建的固件存储库配置文件，它使用 Dell EMC 联机目录获取最新的固件信息。如果设备没有互联网连接，请修改此存储库以指向基于 CIFS、NFS、HTTP 或 HTTPS 的本地共享。有关修改此目录的更多信息，请参阅[编辑或自定义 Dell 默认目录](#) 页面上的 43。

您可以选择“Dell EMC 默认目录”作为默认目录，以更新不与任何群集配置文件关联的 vSphere 主机的固件。

- **验证的 MX 堆栈目录**：出厂时创建的固件存储库配置文件，它使用 Dell EMC 联机目录获取 MX 机箱及其相应底座的已验证固件信息。有关修改此目录的更多信息，请参阅[编辑已验证的 MX 堆栈目录](#) 页面上的 44。有关“经验证的 MX 堆栈目录”的更多信息，请参阅技术白皮书，可从[MX7000 固件更新](#)中获得。

**注**：您不能使用“Dell EMC 默认目录”和“经验证的 MX 堆栈目录”存储库配置文件作为 vSAN 群集的基线。

## 创建存储库配置文件

1. 在 OMIVV 主页中，单击[合规性和部署](#) > [配置文件](#) > [存储库配置文件](#)。
2. 在向导的[存储库配置文件](#)页面中，阅读说明，然后单击**开始**。
3. 在[配置文件名称和说明](#)页面中，输入配置文件名称和说明。说明字段是可选的，限制为 255 个字符。
4. 单击**下一步**。  
将显示[配置文件设置](#)页面。
5. 在[配置文件设置](#)页面中，选择**固件**或**驱动程序**。

以下适用于驱动程序存储库配置文件：

- 驱动程序存储库配置文件最多可包含 10 个驱动程序。如果有更多的文件，驱动程序的选择将是随机的。
  - 仅使用脱机驱动程序捆绑包（.zip 文件）。
  - 下载并解压缩脱机驱动程序捆绑包（.zip 文件）并保存至共享位置，然后提供该共享位置的完整路径。OMIVV 会自动在 OMIVV 设备中创建目录。可从以下位置获取驱动程序捆绑包：<https://my.vmware.com/web/vmware/downloads>
  - OMIVV 需要 CIFS 或 NFS 的写入访问权限。
  - 将忽略子文件夹中的文件。
  - 将忽略大小超过 10 MB 的文件。
  - 驱动程序存储库仅适用于 vSAN 群集。
6. 在[存储库共享位置](#)区域中，执行下列任务：
    - a. 输入存储库共享位置（NFS 或 CIFS）。
    - b. 对于 CIFS，输入凭据。

OMIVV 仅支持基于服务器消息块 (SMB) 版本 1.0 和 SMB 版本 2.0 的 CIFS 共享。

**注**：如果用于驱动程序存储库的 SMB 1.0 共享，请在目录路径的末尾添加文件分隔符。

7. 要验证目录路径和凭据，请单击**开始测试**。


要继续创建存储库配置文件，您必须完成此验证过程。

将显示测试连接结果。

8. 单击**下一步**。  
此时将显示**与存储库位置同步**页面。
9. 单击**下一步**。  
此时会显示**摘要**页面，其中提供了有关存储库配置文件的信息。
10. 单击**完成**。  
创建目录后，目录会进行下载和分析，状态将显示在存储库配置文件的主页上。  
成功分析的存储库配置文件可在创建群集配置文件和固件更新期间使用。

## 编辑存储库配置文件

1. 在 OMIVV 主页中，单击**合规性与部署** > **存储库配置文件** > **编辑**。
2. 在**配置文件名称和说明**页面中，编辑配置文件名称和说明，然后单击**下一步**。
3. 在**配置文件设置**页面中，选择**固件**或**驱动程序**。  
以下适用于驱动程序存储库配置文件：
  - 驱动程序存储库配置文件最多可包含 10 个驱动程序。如果有更多的文件，驱动程序的选择将是随机的。
  - 仅使用脱机驱动程序捆绑包（.zip 文件）。
  - 下载并解压压缩脱机驱动程序捆绑包（.zip 文件）并保存至共享位置，然后提供该共享位置的完整路径。OMIVV 会自动在 OMIVV 设备中创建目录。可从以下位置获取驱动程序捆绑包：<https://my.vmware.com/web/vmware/downloads>
  - OMIVV 需要 CIFS 或 NFS 的写入访问权限。
  - 将忽略子文件夹中的文件。
  - 将忽略大小超过 10 MB 的文件。
  - 驱动程序存储库仅适用于 vSAN 群集。
4. 在**存储库共享位置**区域中，执行下列任务：
  - a. 输入存储库共享位置（NFS 或 CIFS）。
  - b. 对于 CIFS，输入凭据。

 **注：**OMIVV 仅支持基于服务器消息块 (SMB) 版本 1.0 和 SMB 版本 2.0 的 CIFS 共享。
5. 要验证目录路径和凭据，请单击**开始测试**。  
此验证是进一步继续的必需步骤。  
将显示测试连接结果。
6. 单击**下一步**。  
此时将显示**与存储库位置同步**页面。
7. 在**与存储库位置同步**页面中，选中**与存储库位置同步**复选框，然后单击**下一步**。  
要仅更新配置文件名称或查看信息，请取消选中**与存储库位置同步**复选框，以便目录在 OMIVV 中保持不变。有关与存储库位置同步的更多信息，请参阅**与存储库位置同步** 页面上的 44。
8. 在**摘要**页面上，检查配置文件信息，然后单击**完成**。

## 编辑或自定义 Dell 默认目录

1. 在**存储库配置文件**页面中，选择**Dell 默认目录**。
2. 在**配置文件名称和说明**页面中，编辑配置文件说明，然后单击**下一步**。
3. 在**指定存储卡位置**部分中，选择以下存储库位置之一：
  - **Dell 默认联机** - 存储库配置文件设置为 **Dell 联机** (<https://downloads.dell.com/catalog/Catalog.gz>)。OMIVV 使用“Dell EMC 联机”作为目录和更新软件包的源。
  - **自定义联机** - OMIVV 使用**自定义联机**（HTTP 或 HTTPS 共享）作为目录和更新包的源。使用 Server Update Utility (SUU) 创建自定义存储库时，请确保目录 `catalog.xml.gz.sign` 的签名文件存在于目录文件文件夹中。
  - **共享网络文件夹** - OMIVV 使用共享网络文件夹（CIFS 或 NFS）作为目录和更新软件包的源。
  - a. 如果您选择**自定义联机**，请输入目录联机路径。

- b. 如果您选择**共享网络文件夹**，请输入目录文件位置（NFS 或 CIFS）。
4. 要验证目录路径和凭据，请单击**开始测试**。  
将显示测试连接结果。
5. 在**与存储库位置同步**页面中，选中**与存储库位置同步**复选框，然后单击**下一步**。  
要仅更新配置文件名称或查看信息，请取消选中**与存储库位置同步**复选框，以便目录在 OMIVV 中保持不变。有关与存储库位置同步的更多信息，请参阅**与存储库位置同步** 页面上的 44。
6. 在**摘要**页面上，检查配置文件信息，然后单击**完成**。

## 编辑已验证的 MX 堆栈目录

1. 在**存储库配置文件**页面中，选择**已验证的 MX 堆栈目录**，然后单击**编辑**。
2. 您仅可以编辑以下：
  - a. 目录说明。
  - b. **与存储库位置同步**复选框。  
要仅更新配置文件名称或查看信息，请取消选中**与存储库位置同步**复选框，以便目录在 OMIVV 中保持不变。有关与存储库位置同步的更多信息，请参阅**与存储库位置同步** 页面上的 44。



## 与存储库位置同步

“Dell 默认目录”和“验证 MX 堆栈”存储库配置文件会每隔 24 小时或在每次重新引导时自动检查更改并自动更新。

要更新脱机目录，请完成以下步骤：

1. 使用 Dell EMC Repository Manager (DRM) 或 Server Update Utility (SUU) 更新脱机位置（CIFS 或 NFS）中的目录。如果有驱动程序，请更换驱动程序捆绑包。
2. 编辑存储库配置文件，然后选中**与存储库位置同步**复选框，以捕获 OMIVV 的更改以供参考。此过程需要几分钟时间。
3. 要更新配置合规性基线中的固件，请确保编辑相应的群集配置文件并保存。

## 查看存储库配置文件

1. 在 OMIVV 主页中，单击**合规性和部署 > 存储库配置文件**。  
表格显示所有存储库配置文件及以下信息：
  - **配置文件名称** — 存储库配置文件的名称
  - **说明** — 配置文件说明
  - **类型** — 存储库的类型（固件或驱动程序）
  - **共享路径** — NFS、CIFS、HTTP 或 HTTPS 路径
  - **上次成功更新时间** — 更新存储库配置文件的日期和时间
  - **上次刷新状态** — 目录下载和解析状态
2. 如果您要从向导中移除或添加列名称，请单击 。
3. 要导出存储库配置文件信息，请单击 。

## 删除存储库配置文件

在删除存储库配置文件之前，确保从关联的群集配置文件中取消关联存储库配置文件。

1. 在**存储库配置文件**页面中，选择一个存储库配置文件，然后单击**删除**。
2. 在删除确认对话框中，单击**删除**。


# 使用群集配置文件捕获基线配置

## 群集配置文件

通过群集配置文件，您可以捕获配置基线（硬件配置、固件或驱动程序版本），然后通过基于配置基线识别任何偏差来维护集群所需的状态。

要创建群集配置文件，请确保您拥有以下其中一个配置文件：系统配置文件、固件存储库配置文件、驱动程序存储库配置文件或其组合。建议对作为基线的群集使用同类服务器（相同的型号、相同的硬件配置和相同的固件级别）。

- 创建群集配置文件后，必须先分析固件和驱动程序存储库配置文件，然后才能将其用于创建群集配置文件。
- 在创建群集配置文件后，将会创建关联固件和驱动程序存储库的当前快照作为基线。如果原始存储库更改，则必须再次更新群集配置文件以反映更改。否则，针对存储库执行的任何更新不会更新到群集配置文件快照。
- 创建群集配置文件之后，它会触发偏移检测作业。
- 当任何群集与群集配置文件关联时，会覆盖以前的群集配置文件关联。
- 如果多个独立的 vCenter 注册到 OMIVV，建议您为每个 vCenter 创建不同的群集配置文件。
- 仅在 vSAN 群集上支持驱动程序基线。

 **注：**在 OMIVV 之外安装的驱动程序不会被视为基线。

## 创建群集配置文件

请确保：

- 您拥有以下其中一个配置文件：系统配置文件、固件存储库配置文件、驱动程序存储库配置文件或其组合。
  - 群集存在于 vCenter 中。
1. 在 OMIVV 主页上，选择**合规性和部署 > 配置文件 > 群集配置文件 > 创建新配置文件上**
  2. 在向导的**群集配置文件**页面中，阅读说明，然后单击**开始**。
  3. 在**配置文件名称和说明**页面中，输入配置文件名称和说明，然后单击**下一步**。  
配置文件名称最多可包含 200 个字符。说明最多可包含 400 个字符。
  4. 在**关联配置文件**页面中，选择以下任何一个配置文件或其组合：
    - 系统配置文件 - 选择系统配置文件会为群集中的主机设置配置基线。对于基本和高级系统配置文件类型，系统配置文件名称采用以下格式显示：Basic\_<系统配置文件名称>，Advanced\_<系统配置文件名称>
    - 固件存储库配置文件 - 选择固件存储库会为群集中的主机创建固件或 BIOS 基线。不支持为联机存储库创建 vSAN 群集基线。
    - 驱动程序存储库配置文件 - 选择驱动程序存储库会为群集中的主机创建驱动程序基线。一次最多可以将 10 个驱动程序关联到基线。仅在 vSAN 群集上支持驱动程序基线。
  5. 单击**下一步**。  
此时将显示**关联群集**页面。
  6. 在**关联群集**页面上，执行以下任务：
    - a. 选择已注册 vCenter 服务器的实例。
    - b. 要关联群集，请单击**浏览**。
    - c. 选择您要设为基线的群集。
    - d. 单击**确定**。  
所选群集显示在**关联群集**页面上。
    - e. 单击**下一步**。
  7. 在**计划偏移检测**页面上，选择日期和时间，然后单击**下一步**。  
此时会显示**摘要**页面，其中提供了有关群集配置文件的信息。
  8. 单击**完成**。  
偏移检测作业会在保存群集配置文件后立即运行，以后会在计划的时间运行。在“作业”页面中查看作业完成状态。

**注:** 如果在为群集创建群集配置文件之后修改了由 OMIVV 管理的节点的数量，则在后续偏移检测作业期间，集合大小会自动更新。

## 编辑群集配置文件

编辑群集配置文件将更改基线，这可能会导致重新计算合规性级别。

如果已更改关联的驱动程序存储库、固件存储库或系统配置文件，并且如果您想要使用群集配置文件的最新更改，请选择群集配置文件，单击**编辑**，然后在向导中单击**下一步**，然后单击**完成**。



1. 在 OMIVV 主页中，单击**合规性和部署 > 配置文件 > 群集配置文件**。
2. 选择群集配置文件并单击**编辑**。
3. 在**配置文件名称和说明**页面中，编辑说明，然后单击**下一步**。
4. 在**关联的配置文件**页面中，您可以更改配置文件组合。
5. 在**关联的群集**页面中，您可以更改 vCenter 实例和相关群集。
6. 在**偏移检测计划**页面中，您可以更改偏移检测计划。
7. 查看**摘要**页面上的更新信息，然后单击**完成**。  
偏移检测作业会在保存群集配置文件后立即运行，以后会在计划的时间运行。

## 查看群集配置文件

1. 在 OMIVV 页面中，单击**合规性和部署 > 配置文件 > 群集配置文件**。  
表格显示所有群集配置文件及以下信息：
  - **配置文件名称** - 群集配置文件的名称
  - **说明** — 配置文件说明
  - **关联系统配置文件** — 系统配置文件名称。对于基本和高级系统配置文件类型，系统配置文件名称采用以下格式显示：  
Basic\_<系统配置文件名称>，Advanced\_<系统配置文件名称>
  - **关联的固件存储库配置文件** — 关联的固件存储库配置文件名称
  - **关联的驱动程序存储库配置文件** — 关联的驱动程序存储库配置文件名称

**注:** 对于使用机箱凭据配置文件管理的 PowerEdge MX 主机，不计算配置偏移。

  - **vCenter** — 与群集配置文件关联的 vCenter 实例
  - **上次成功更新时间** — 更新群集配置文件的日期和时间。

**注:** 如果修改了关联的存储库配置文件（固件或驱动程序）或系统配置文件，则会显示带配置文件名称的警告符号。修改存储库或系统配置文件以更新基线中的更改后，必须更新群集配置文件。有关更新群集配置文件的更多信息，请参阅 [更新群集配置文件](#) 页面上的 46。
2. 如果您要从向导中移除或添加列名称，请单击 。
3. 要导出群集配置文件信息，请单击 。

## 更新群集配置文件

如果更新存储库配置文件（固件或驱动程序）和系统配置文件，则会在群集配置文件页面上的配置文件名称旁显示警告符号。更新配置文件可能会影响群集配置文件中关联群集的配置合规性和 vSphere 生命周期管理器中的固件合规性状态。您可以使用**更新配置文件**功能更新或重新调整群集配置文件的基线。

1. 在 OMIVV 主页中，单击**合规性和部署 > 配置文件 > 群集配置文件**。
2. 选择一个配置文件名称旁有警告符号的群集配置文件。
3. 单击**更新配置文件**。
4. 要将关联的配置文件更新到最新版本，请单击**确定**。  
更新配置文件后，将无法恢复此基线。  
当群集配置文件与更新的存储库配置文件或系统配置文件同步时，警告符号消失。

## 删除群集配置文件

1. 在 OMIVV 主页中，单击**合规性和部署** > **配置文件** > **群集配置文件**。
2. 选择群集配置文件，然后单击**删除**。
3. 在**删除确认**对话框中，单击**删除**。  
如果删除群集配置文件，则还会删除相应的偏移检测作业。

# 管理裸机服务器

## 查看裸机服务器

在**裸机服务器**页面中，您可以：

- 查看使用自动查找和手动查找功能查找到的裸机服务器。

将会显示诸如以下信息：**服务标签、型号名称、iDRAC IP、服务器状态、系统锁定模式、合规性状态和 iDRAC 许可证状态。**

以下是裸机服务器的不同状态：

- **未配置** - 以将服务器添加到 OMIVV，正在等待配置。
  - **已配置** - 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。
  - **已隔离** - 由于服务器已从任何 OMIVV 操作中排除，服务器无法执行操作系统部署和固件更新等任务。
- 查看裸机服务器的合规性状态。

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）。
  - 它没有安装受支持的 iDRAC、BIOS 或 LC 版本。
  - 不存在 LOM 或 NIC。
  - 系统锁定模式已开启。
- 要查看有关合规性问题的详细信息，请单击下部水平窗格中的**详细信息**。

您还可以在**裸机服务器**页面上执行以下任务：

- [手动发现裸机服务器](#)
- [删除裸机服务器](#)
- [系统配置文件和 ISO 配置文件部署](#)
- [刷新裸机服务器](#)
- [购买或续订 iDRAC 许可证](#)

## 设备查找

查找是添加受支持的裸机服务器的过程。查找到服务器后，您可以将它用于系统配置文件和 ISO 配置文件部署。有关受支持的服务器列表的更多信息，请参阅 *OpenManage Integration for VMware vCenter 兼容性表*。

前提条件：

- 需要从裸机服务器的 iDRAC 到 OMIVV 虚拟机的网络连接。
- 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。将它们添加到主机凭据配置文件。
- 要在 SD 卡上部署操作系统并使用第 12 代和第 13 代 PowerEdge 服务器中的系统配置文件功能，请确保已安装 iDRAC 2.50.50.50 和更高版本。

## 自动查找

自动查找是添加裸机服务器的过程。查找到服务器后，将它用于操作系统和硬件部署。自动查找是一项 iDRAC 功能，它消除了使用 OMIVV 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。

**注：**不应使用 OMIVV 来查找具有现有操作系统的主机，而是将操作系统添加到主机凭据配置文件中。

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 服务器获取配置服务器的 IP 地址，或在 iDRAC 配置公用程序中手动指定 IP 地址。
- 额外的网络设置 — 要解析 DNS 名称，请在 DHCP 设置中启用 Get DNS 服务器地址。
- 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 — 如果存在任何具有管理员权限的 iDRAC 帐户，请先从 iDRAC Web 控制台中禁用这些帐户。自动查找成功完成后，将使用在[设置](#)页面中输入的部署凭据重新启用管理 iDRAC 帐户。有关部署凭据的更多信息，请参阅[配置部署凭据](#) 页面上的 76。
- 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。有关更多信息，请参阅[启用或禁用 iDRAC 上的管理帐户](#) 页面上的 49。

## 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 Configuration Utility 中手动指定配置服务值，iDRAC Configuration Utility 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 <https://www.dell.com/support>。

## 启用或禁用 iDRAC 上的管理帐户

在设置自动查找之前，禁用除没有管理员访问权限以外的所有 iDRAC 帐户。自动查找后，可以启用除 Root 帐户以外的所有帐户。

**注：**在禁用管理员权限之前，建议您在 iDRAC 中创建非管理用户帐户。

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 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。
  - 对于 iDRAC9：请转至 **iDRAC 设置 > 用户 > 本地用户**。
4. 在 **本地用户** 选项卡中，找到除根用户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 服务器以进行自动查找

确保您具有 iDRAC 地址。

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。在收到 Dell EMC 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，并列在**裸机服务器**页面中。

**注：**对于自动查找到的服务器，在**设置 > 设备设置 > 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，设置在关联的主机凭据配置文件中提供的 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 PowerEdge 服务器执行以下步骤：

1. 在目标系统上，在初始引导期间按 F2 键。
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。

## 手动发现裸机服务器

确保通过具有管理员权限的 iDRAC 用户执行查找。

OMIVV 使您可以基于 IPv4 范围手动查找服务器。您可以使用基于 IPv4 的范围查找方法查找单个 IP 或 IP 组。

添加裸机服务器后，此服务器将显示在**裸机服务器**页面上的服务器列表中。

1. 在 OMIVV 主页中，单击**合规性与部署 > 部署 > 查找**。  
此时将显示**查找裸机服务器**页面。
2. 在**查找裸机服务器**页面中，执行以下任务：
  - a. 在**发现作业名称**字段中，输入作业名称。
  - b. 输入作业说明（可选）。
  - c. 要输入 IP 范围，请单击**添加范围数据**。

每个查找作业中可以提及多个范围。最多支持 1024 个 IP。可以在范围内配置的最大 IP 数为 256 个。

当您在范围的排除列表中添加特定的 IP 组，然后在另一个范围的包含列表中添加相同的 IP 时，包含的 IP 优先。

- d. 输入**起始 IP**。  
起始 IP 必须为 IPv4 地址格式。
- e. 输入**结束 IP**。  
结束 IP 必须是 IP 的最后一个八位位组，且大于起始 IP。
- f. 输入**全局排除列表**。

排除列表是要从列表中排除的 IP 的列表。

您在**排除列表**中输入的值必须在**起始 IP**和**结束 IP**范围内。值必须用逗号分隔，每个值可以是最后一个八位位组值或最后一个八位位组值（由 - 分隔）组成的范围。

例如：

要查找从 100.100.100.1 到 100.100.100.50 的所有 IP（排除从 100.100.100.25 到 100.100.100.30 以及 100.100.100.40 到 100.100.100.45 的 IP），请在**起始 IP**、**结束 IP**和**排除列表**中输入以下内容。

起始 IP：100.100.100.1

结束 IP：50

排除列表：25-30、40-45

- g. 要使用在**部署凭据**页面上输入的 iDRAC 凭据，请选中**使用部署凭据**复选框。  
有关部署凭据的更多信息，请参阅**配置部署凭据**页面上的 76。
- h. 如果未设置部署凭据，请输入用户名和密码。

默认情况下已设置部署凭据。如果您想要使用其他部署凭据，请输入 iDRAC 用户名和密码。您可以为每个范围设置单独的一组凭据。

用户名必须介于 1 到 16 个字符之间。不支持特殊字符 /、\、~ 和 '。

一个密码最多可包含 42 个字符。

3. 选择以下选项之一：

- **立即运行** - 立即运行作业时，将查找给定范围内提及的所有 IP。
- **稍后运行** - 计划作业稍后运行时，将查找给定范围内的 IP。

4. 单击**应用**。

查找作业的状态显示在**查找作业**页面上。有关更多信息，请参阅 [发现作业](#) 页面上的 68。

## 删除裸机服务器

您可以手动删除自动查找到的或手动添加的服务器。

1. 在 OMIVV 主页中，单击**合规性与部署 > 部署 > 删除**。
2. 选择裸机服务器，然后单击**确定**。

## 刷新裸机服务器

刷新操作通过连接到 iDRAC 并收集基本资源清册来重新发现裸机服务器。

**注：**如果针对“已配置”的裸机服务器执行刷新操作，则服务器状态将更改为“未配置”状态，因为刷新操作重新发现服务器。

1. 在 OMIVV 主页中，单击**合规性与部署 > 部署 > 刷新**。
2. 在**刷新裸机服务器**页面中，选择服务器，然后单击**确定**。  
刷新裸机服务器数据可能需要几分钟。当操作正在进行时，您可以关闭**刷新裸机服务器**页面，重新发现进程将在后台继续进行。重新发现的服务器显示在**裸机服务器**页面中。

## 购买或续订 iDRAC 许可证

当裸机服务器没有兼容的 iDRAC 许可证时，其状态显示不符合要求。一张表显示 iDRAC 许可证的状态。选择不符合要求的裸机服务器以查看有关 iDRAC 许可证的详细信息。

1. 要续订 iDRAC 许可证，请在 OMIVV 主页中，单击**合规性和部署 > 部署**。
2. 选择 iDRAC 许可证不符合要求的裸机服务器，然后单击**购买/续订 iDRAC 许可证**。
3. 登录到 Dell Digital Locker，然后更新或购买新的 iDRAC 许可证。
4. 安装 iDRAC 许可证后，单击**刷新**。

# 管理部署配置文件

## 系统配置文件

系统配置文件可捕获 iDRAC、BIOS、RAID、事件过滤器、FC 和 NIC 的组件级设置和配置。在裸机服务器上操作系统部署期间，将这些配置应用到其他相同的服务器。可以在群集配置文件中系统配置文件来保持配置的基线。

### 前提条件

在创建或编辑系统配置文件之前，请确保：

- 在参考服务器上启用 CSIOR 功能。启用 CSIOR 后，必须重新启动参考服务器，因此从 iDRAC 返回的数据是最新的。
- 每个由 vCenter 管理的参考主机的清点均取得成功。
- 裸机服务器已安装所需的最小 BIOS 和固件版本。有关更多信息，请参阅支持站点上的 *OMIVV 兼容性值表*。
- 参考服务器和目标服务器为同类（相同的型号、相同的硬件配置和相同的固件级别）。
- 硬件（例如 FC、NIC 和 RAID 控制器）存在于参考服务器和目标服务器的相同插槽中。
- 在从默认选择中包括或排除任何属性之前，将鼠标悬停在属性名称上以了解属性的详细信息。
- 在系统配置文件中配置 iDRAC 用户时，将选择用于查找 iDRAC 的 iDRAC 用户。
- **注：**请勿清除与用于查找裸机的 iDRAC 用户关联的属性，否则系统配置文件部署作业会失败。
- 您不能更改用于查找 iDRAC 的 iDRAC 用户的用户名。这会导致 iDRAC 存在连接问题，系统配置文件部署作业失败，而不应用任何属性。

在创建系统配置文件之前，建议您根据需要配置参考服务器属性和值。对所有必要的目标主机应用参考属性和值。

系统配置文件在应用配置文件时搜索确切实例 (FQDD)，该配置文件在机架式服务器（相同的）上成功运行，但在模块化服务器中可能受到一些限制。例如，在 FC640 中，由于 NIC 级别限制，从一台模块化服务器创建的系统配置文件无法在相同 FX 机箱中的其它模块化服务器上应用。在这种情况下，建议您从机箱的每个插槽获取一个参考系统配置文件。仅在机箱中为相应插槽应用这些系统配置文件。

**注：**系统配置文件不支持启用和禁用引导选项。

**注：**

- 使用系统配置文件时，可导出具有企业许可证的系统配置文件，而在服务器上导入具有 Express 许可证的相同系统配置文件失败。
- 您不能通过使用 iDRAC9 固件 3.00.00.00 的 Express 许可证导入系统配置文件。您必须具有企业版许可证。

## 创建系统配置文件

建议您使用 Google Chrome 创建或编辑系统配置文件。

使用超薄线缆连接 HBA、BOSS 和 PERC 的 PowerEdge R6515、R7515、R65125、R7525 和 C6515 服务器。在 OMIVV 中使用早于 4.30.30.30 的 iDRAC 版本创建的系统配置文件不能用于 iDRAC 4.30.30.30 及更高版本。使用 iDRAC 4.30.30.30 或更高版本创建新的系统配置文件，并在需要时使用它。

1. 在 OMIVV 主页中，单击 **合规性和部署 > 配置文件 > 系统配置文件 > 新建配置文件**。
2. 在向导的 **创建系统配置文件** 页面中，阅读说明，然后单击 **开始使用**。
3. 在 **名称和说明** 页面中，请执行以下操作：
  - a. 输入配置文件名称和说明。该说明字段是可选字段。
  - b. 请选择任何一种系统配置文件类型：
    - **基本** — 显示 iDRAC、BIOS、RAID、NIC 和 FC 的最小属性集。
    - **高级** — 显示 iDRAC、BIOS、RAID、NIC、FC 和 EventFilters 的所有属性。

4. 在**参考服务器**页面上，要选择主机或裸机作为参考服务器，请单击**选择**。

由于下列任何一个原因，服务器选择可能被禁用：

- 服务器是非合规主机或非合规裸机服务器。
- 部署作业已计划或正在服务器上运行。
- 服务器使用机箱凭据配置文件进行管理。

此时将显示**提取确认**对话框。

5. 要从参考服务器中提取系统配置，请单击**确定**。  
从参考服务器提取系统配置可能需要几分钟的时间。
6. 查看参考服务器详细信息，然后单击**下一步**。

- 要在**选择参考服务器**页面上更改参考服务器，请单击**浏览**。

如果参考服务器是裸机类型，则仅显示其 iDRAC IP。如果参考服务器本身是主机服务器，则会显示 iDRAC 和主机 (FQDN) IP。

将显示**配置文件设置**页面。

7. 在**配置文件设置**页面中，您可以根据参考服务器的配置查看或修改组件的配置文件设置（例如 iDRAC、BIOS、RAID、NIC、CNA、FCoE 和 EvenFilters）。

默认情况下，未列出平台特定属性和只读属性。有关平台特定属性的更多信息，请参阅**系统特定属性** 页面上的 147。

伪属性不会显示在系统配置文件中。有关详细信息，请参阅**服务器配置 XML 文件**文档。

在选择默认情况下选择的属性以外的属性之前，请检查属性、相关性和其他详细信息的性质。

如果您选择默认选择的属性以外的属性，将显示以下消息：

这些属性可能会影响其他相关属性、将来存在破坏性、分解服务器身份或影响目标服务器的安全性。

**注：**对于第 12 代和第 13 代 PowerEdge 服务器，某些属性可能无法在 OMIVV 中正确映射依赖关系。例如，BIOS 的内存操作电压组件为只读，除非在**系统 BIOS 设置**中将系统配置文件设置为**自定义**。

- a. 展开每个组件以查看设置选项，例如**实例**、**属性名称**、**值**、**破坏性**、**相关性**和**组**。

如果相关性文本不可用，则将显示相关性字段。

**注：**您可以使用**搜索**字段筛选除**值**以外的所有列的特定数据。

- b. 设置标有红色感叹号的属性值是必需进行的操作。此选项仅适用于已启用 iDRAC 并具有有效用户名的用户。

8. 单击**下一步**。

有关系统配置文件详细信息和系统配置的属性统计数据的信息的**摘要**页面将显示。

属性统计数据下将显示属性的总数、已启用属性的总数和破坏性属性的总数。

9. 单击**完成**。

**系统配置文件**页面上会显示保存的配置文件。

已覆盖一些系统配置文件以使 OMIVV 正常工作。有关自定义属性的更多信息，请参阅**自定义属性** 页面上的 152。有关系统配置文件配置模板、属性和工作流的更多信息，请参阅**附加信息** 页面上的 151。

## 编辑系统配置文件

建议您使用 Google Chrome 创建或编辑系统配置文件。

1. 在**创建系统配置文件**页面中，选择一个系统配置文件，然后单击**编辑**。
2. 在**名称和说明**页面中，更改配置文件名称和说明。“说明”字段为可选项。

**注：**创建基本或高级系统配置文件后，不能修改配置文件。

3. 在**参考服务器**页面上，要更改参考服务器（主机或裸机），请单击**选择**。

由于下列任何原因，服务器选择可能被禁用：

- 服务器是非合规主机或裸机服务器。
- 部署作业已计划或正在服务器上运行。
- 服务器使用机箱凭据配置文件进行管理。

此时将显示**提取确认**对话框。

4. 要从参考服务器中提取系统配置，请单击**确定**。  
从参考服务器提取系统配置可能需要几分钟的时间。
5. 查看参考服务器详细信息，然后单击**下一步**。
  - 要在**选择参考服务器**页面上更改参考服务器，请单击**浏览**。如果参考服务器是裸机类型，则仅显示其 iDRAC IP。如果参考服务器本身是主机服务器，则会显示 iDRAC 和主机 (FQDN) IP。

将显示**配置文件设置**页面。

6. 在**配置文件设置**页面中，您可以根据参考服务器的配置查看或修改组件的配置文件设置（例如 iDRAC、BIOS、RAID、NIC、CNA、FCoE 和 EvenFilters）。

默认情况下，未列出平台特定属性和只读属性。有关平台特定属性的更多信息，请参阅**系统特定属性** 页面上的 147。



如果您尝试修改少数属性，则会显示以下警告消息：

这些属性可能会影响其他相关属性、将来存在破坏性、分解服务器身份或影响目标服务器的安全性。

**注：**编辑系统配置文件后，如果修改了用于查找裸机服务器的 iDRAC 用户的密码，将忽略更新的密码。更新的密码将替换为用于查找裸机服务器的密码。

- a. 展开每个组件以查看设置选项，例如实例、属性名称、值、破坏性、相关性和组。  
如果相关性文本不可用，则将显示相关性字段。
  - b. 设置标有红色感叹号的属性值是必需进行的操作。此选项仅适用于已启用 iDRAC 并具有有效用户名用户。
7. 单击**下一步**。  
有关系统配置文件详细信息和系统配置的属性统计数据的信息的**摘要**页面将显示。  
属性统计数据下将显示属性的总数、已启用属性的总数和破坏性属性的总数。
  8. 单击**完成**。  
**系统配置文件**页面上会显示保存的配置文件。  
已覆盖一些系统配置文件以使 OMIVV 正常工作。有关自定义属性的更多信息，请参阅**自定义属性** 页面上的 152。有关系统配置文件配置模板、属性和工作流的更多信息，请参阅**附加信息** 页面上的 151。

## 查看系统配置文件

1. 在 OMIVV 主页中，单击**合规性和部署 > 系统配置文件**。  
表格显示所有系统配置文件及以下信息：
  - **配置文件名称** — 系统配置文件的名称
  - **说明** — 配置文件说明
  - **参考服务器** - 从中提取系统配置详细信息的 iDRAC IP。
  - **服务器型号** — 参考服务器的型号名称
2. 如果您要从向导中移除或添加列名称，请单击 .
3. 要导出系统配置文件信息，请单击 .

## 删除系统配置文件

删除属于正在运行的部署任务的系统配置文件可能导致删除作业失败。

1. 在**系统配置文件**页面中，选择一个配置文件，然后单击**删除**。
2. 在删除确认对话框中，单击**删除**。

## ISO 配置文件

ISO 配置文件包含在 NFS 或 CIFS 文件夹上保存的 Dell EMC 自定义 ESXi ISO 映像文件的文件夹路径。ISO 配置文件在部署向导中使用。

## 创建 ISO 配置文件



ISO 配置文件需要 NFS 或 CIFS 上的 Dell EMC 自定义的 ISO 文件位置。

1. 在 OMIVV 主页中，单击**合规性和部署 > 配置文件 > ISO 配置文件 > 创建新配置文件**。
2. 在向导 **ISO 配置文件** 页面中，阅读说明，然后单击**开始**。
3. 在**配置文件名称和说明**页面中，输入配置文件名称和说明。该说明是可选字段。
4. 在**安装源 (ISO)** 框中，输入 ISO 文件位置 (NFS 或 CIFS)。  
OMIVV 仅支持基于服务器消息块 (SMB) 版本 1.0 和 SMB 版本 2.0 的 CIFS 共享。
  - a. 如果使用 CIFS，请输入凭据。
5. 在 **ESXi 版本** 下拉列表中，选择 ESXi 版本。  
选择正确的 ESXi 版本，以便使用相应的安装引导脚本。如果您选择了不正确的 ESXi 版本，部署可能会失败。
6. 要验证 ISO 文件路径可访问性和凭据，请单击**开始测试**。  
将显示测试结果。
7. 单击**完成**。

## 编辑 ISO 配置文件

1. 在 OMIVV 主页中，单击**合规性和部署 > 配置文件 > ISO 配置文件**。
2. 选择 ISO 配置文件，单击**编辑**。
3. 在**配置文件名称和说明**页面中，编辑配置文件名称和说明。该说明是可选字段。
4. 在**安装源 (ISO)** 框中，更改 ISO 文件位置 (NFS 或 CIFS)。  
OMIVV 仅支持基于服务器消息块 (SMB) 版本 1.0 和 SMB 版本 2.0 的 CIFS 共享。
  - a. 如果使用 CIFS，请输入凭据。
5. 在 **ESXi 版本** 下拉列表中，选择 ESXi 版本。  
选择正确的 ESXi 版本，以便使用相应的安装引导脚本。如果您选择了不正确的 ESXi 版本，部署可能会失败。
6. 要验证 ISO 文件路径和身份验证，请单击**开始测试**。  
将显示测试结果。
7. 单击**完成**。

## 查看 ISO 配置文件

1. 在 OMIVV 主页中，单击**合规性和部署 > ISO 配置文件**。  
表格显示所有 ISO 配置文件及以下信息：
  - **配置文件名称** - 配置文件的名称
  - **说明** — 配置文件说明
  - **安装源** - ISO 文件位置 (NFS 或 CIFS)
  - **ESXi 基本版本** - ESXi 基本版本
2. 如果您要从向导中移除或添加列名称，请单击 。
3. 要导出 ISO 配置文件信息，请单击 。

## 删除 ISO 配置文件

如果您删除属于正在运行的部署任务的 ISO 配置文件，部署任务可能会失败。

1. 在 OMIVV 主页中，单击**合规性和部署 > 配置文件 > ISO 配置文件**。
2. 选择 ISO 配置文件，单击**删除**。
3. 在确认对话框中，单击**删除**。

# 下载自定义 Dell EMC ISO 映像

部署过程需要包含所有 Dell EMC 驱动程序自定义 ESXi 映像。

1. 打开浏览器并转至 **support.dell.com**。
2. 单击**浏览所有产品** > **服务器** > **PowerEdge**。
3. 单击 PowerEdge 服务器型号。
4. 单击服务器型号的**驱动程序和下载**页面。
5. 从**操作系统**下拉菜单中，选择 ESXi 版本。
6. 从**类别**下拉菜单中，选择**企业解决方案**。
7. 在**企业解决方案**列表中，选择所需的 ISO 版本，然后单击**下载**。

## 系统配置文件和 ISO 配置文件部署

要部署系统配置文件和 ISO 配置文件，请确保您的环境中的所有服务器满足以下要求：

- 所有服务器都显示在**系统配置文件和 ISO 配置文件部署**向导中。
- 满足在 *OpenManage Integration for VMware vCenter 兼容性值表* 中提到的具体硬件支持信息。
- 支持的最低版本的 iDRAC 固件和 BIOS 可用。  
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。
- IDSDM 存储规格可用。  
要了解 IDSDM 的存储规格，请参阅 VMware 文档。
- 先从 BIOS 启用 IDSDM，然后才能使用 OMIVV 部署操作系统。  
OMIVV 允许在 IDSDM 或本地硬盘驱动器或 BOSS 卡上进行部署。
- 如果 vCenter、OMIVV 和 iDRAC 连接到不同的网络，vCenter、OMIVV 和 iDRAC 网络之间存在路由。  
此要求仅适用于 OMIVV 设备未配置两个网络适配器的情况。
- 已启用重新引导时收集系统资源清册 (CSIOR)。
- 检索到的数据是最新的，方法是在启动自动或手动查找之前，在服务器上执行硬重启。
- 对于裸机服务器的自动查找，请订购由工厂预先配置了自动查找或信号交换选项的 Dell EMC 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，请确保部署操作系统之前满足以下条件：
  - 在 BIOS 中启用虚拟化技术 (VT) 标志。
  - 虚拟驱动程序、IDSDM 和 BOSS 设置为第一引导磁盘。
- 要验证如果使用 OMIVV 进行硬件配置，则尽管 BIOS 配置不是系统配置文件的一部分，BIOS 的 VT 设置也会自动启用。如果未在目标系统上配置虚拟驱动器，则需要快速或克隆 RAID 配置。
- 包含所有 Dell EMC 驱动程序的自定义 ESXi 映像可进行部署。  
从 [support.dell.com](http://support.dell.com) 上提供的**驱动程序和下载**部分下载正确的映像。有关下载自定义 Dell EMC ISO 映像的详细信息，请参阅 [下载自定义 Dell EMC ISO 映像](#) 页面上的 56。
- 将自定义映像保存到 CIFS 或 NFS 共享位置，在部署过程中 OMIVV 可以访问这些位置。  
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*。  
以下内容适用于部署具有双 NIC 的主机：
  - 主机可以在同一个网络中或在两个不同的网络中具有 iDRAC 和 vCenter 管理 NIC。
  - 可以将 ISO 映像保存在任何网络中。
  - 确保您选择适用于环境的正确 vCenter 网络和 OMIVV 网络。操作系统部署向导会显示两个 OMIVV 网络。

## 部署任务清单

部署系统配置文件和 ISO 配置文件之前，请确保以下各项可用：

- 主机凭据配置文件  
要创建主机凭据配置文件，请单击**创建**。有关创建主机凭据配置文件的更多信息，请参阅[创建主机凭据配置文件](#)页面上的 35。
- 裸机服务器  
要查找裸机服务器，请单击**查找**。有关查找裸机服务器的更多信息，请参阅[手动发现裸机服务器](#)页面上的 50。
- 系统配置文件  
要创建系统配置文件，请单击**创建**。有关创建系统配置文件的更多信息，请参阅[创建系统配置文件](#)页面上的 52。
- ISO 配置文件

要创建 ISO 配置文件，请单击**创建**。有关创建 ISO 配置文件的更多信息，请参阅[创建 ISO 配置文件](#) 页面上的 55。

通过使用**系统配置文件**和**ISO 配置文件部署**向导，您可以执行以下操作：

- 系统配置文件部署  
有关更多信息，请参阅 [部署系统配置文件（硬件配置）](#) 页面上的 58。
- ISO 配置文件部署  
有关更多信息，请参阅 [部署 ISO 配置文件（ESXi 安装）](#) 页面上的 58。
- 系统配置文件和 ISO 配置文件部署  
有关更多信息，请参阅 [部署系统配置文件和 ISO 配置文件](#) 页面上的 60。

## 部署系统配置文件（硬件配置）

1. 要启动部署向导，请转至**合规性与部署 > 部署 > 部署**。
2. 在部署向导的**系统配置文件和 ISO 配置文件部署检查清单**页面上，验证部署任务清单，然后单击**开始**。  
您只能在符合要求的裸机服务器上执行部署。有关更多信息，请参阅 [查看裸机服务器](#) 页面上的 48。
3. 在**选择服务器**页面上，选择一个或多个服务器。  
将显示**选择 RAID 级别**页面。
4. 在**选择部署选项**页面上，选择**系统配置文件（硬件配置）**。
5. 从**系统配置文件**下拉菜单中，选择适当的系统配置文件，然后单击**下一步**。  
对于基本和高级系统配置文件类型，系统配置文件名称采用以下格式显示：Basic\_<系统配置文件名称>，Advanced\_<系统配置文件名称>。

**配置预览**作业尝试根据所选主机比较或验证所选系统配置文件的兼容性。

6. 要在 iDRAC 上创建预览作业，请在**配置预览**页面上，选择一个 iDRAC IP，然后单击**预览**。配置预览是可选任务。  
系统配置文件预览操作可能需要几分钟才能完成。比较状态显示在**结果**列中。

比较结果如下：

- **已完成** — 预览作业已成功运行。有关比较结果的详细信息，请单击**详细信息**列中的**查看详细信息**。
  - **未完成** — 预览作业未在 iDRAC 上成功运行。如果需要，确保 iDRAC 可访问并执行 iDRAC 重设。有关作业的更多信息，请参阅 iDRAC 控制台上的 OMIVV 日志和日志。
7. 在**计划部署作业**页面中，执行以下操作：
    - a. 编辑部署作业名称和说明。该说明是可选字段。
    - b. 要立即运行部署作业，请单击**立即运行**。
    - c. 要将作业计划为稍后运行，请单击**计划稍后**，然后选择日期和时间。
    - d. 选中**在提交作业后转到作业页面**复选框。  
您可以在**作业**页面中跟踪作业状态。有关更多信息，请参阅 [部署作业](#) 页面上的 67。
  8. 单击**完成**。

## 部署 ISO 配置文件（ESXi 安装）

您只能在符合要求的裸机服务器上执行部署。有关更多信息，请参阅 [查看裸机服务器](#) 页面上的 48。

1. 要启动部署向导，请转至**合规性与部署 > 部署 > 部署**。
2. 在部署向导的**系统配置文件和 ISO 配置文件部署检查清单**页面上，验证部署任务清单，然后单击**开始**。
3. 在**选择服务器**页面上，选择一个或多个服务器。  
将显示**选择 RAID 级别**页面。
4. 在**选择部署选项**页面上，选择**ISO 配置文件（ESXi 安装）**。
5. 从**vCenter 名称**下拉菜单中，选择 vCenter 的实例。
6. 要选择 vCenter 目标容器，请单击**浏览**，然后选择要在其上部署操作系统的适当数据中心或群集。
7. 从**ISO 配置文件**下拉菜单中，选择一个适当的 ISO 配置文件。
8. 在**安装目标**下，选择以下其中一项：

- **第一启动磁盘** — 在由 RAID 控制器创建的硬盘、固态硬盘 (SSD)，或虚拟驱动器上部署操作系统。
- **内部双 SD 模块 (IDSDM)** — 在 IDSDM 上部署操作系统。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**第一启动磁盘**选项可用。
  - 如果任何一个选定服务器不支持 IDSDM 或 BOSS 模块，或者在部署过程中未在服务器中安装 IDSDM 或 BOSS，则会在这些服务器上跳过部署操作。  
要在服务器的第一启动磁盘上部署操作系统，请选中**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。

**i 注:** 第一引导磁盘安装目标不等同于 BIOS 硬盘驱动器顺序或 UEFI 引导顺序中的第一个条目。此选项会将操作系统部署到 ESXi 预操作系统标识的第一个磁盘。在选择了**第一引导磁盘**选项的情况下，请确保启用“硬盘故障转移”或“引导顺序重试”选项。

- **BOSS** — 在 BOSS 卡上部署操作系统。如果 BOSS 在至少一台所选服务器上可用，将启用 BOSS 选项。否则，只有**第一启动磁盘**选项可用。  
如果您使用 OMIVV 在 BOSS 控制器上部署操作系统，请确保从具有 BOSS VD 配置的参考服务器处捕获系统配置文件，并确保目标服务器必须具有相似配置的 BOSS。有关创建磁盘驱动器的更多信息，请参阅 *Dell EMC 引导优化服务器存储-S1 用户指南*，网址：[www.dell.com/support](http://www.dell.com/support)。

#### 9. 在选择主机凭据配置文件页面上，执行以下任务：

- 要对所有主机使用相同的主机凭据配置文件，请单击**是**，然后执行以下任务：

- 从下拉菜单中选择主机凭据配置文件。
- 输入密码。

在部署过程中，以下各项对于根用户适用：

- 对于 ESXi 6.5 及更早版本，将使用在主机凭据配置文件中输入的密码。
- 对于 ESXi 6.7 和更高版本，将使用在部署向导中输入的密码。
- 对于 ESXi 6.5 及更早版本，如果未在主机凭据配置文件中输入密码，将使用在部署向导中输入的密码。在主机凭据配置文件中更新 ESXi 凭据，以确保在操作系统 (OS) 部署后成功运行资源清册。

- 要为每个服务器选择单独的主机凭据配置文件，请单击**否**，然后执行以下任务：

- 从下拉菜单中选择主机凭据配置文件。
- 输入根密码。要查看输入的密码，请单击“眼睛”图标。

请确保输入正确的密码，因为“确认密码”选项不可用。

**i 注:** 如果在主机凭据配置文件中 AD 凭据用于 iDRAC 或 ESXi，则不会将那些配置文件视为操作系统部署。

**i 注:** 在主机凭据配置文件中，建议关联用于查找裸机的用户，否则在操作系统部署后，iDRAC 中已发现的用户将被禁用。

#### 10. 在配置网络设置页面中，执行以下任务：

- 输入服务器的完全限定主机名 (FQDN)。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。创建使用 FQDN 解析 IP 地址的 DNS 记录。配置 DNS 服务器以支持反向查找请求。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。

**i 注:** 如果 vCenter 使用 FQDN 向 OMIVV 注册，请确保 ESXi 主机可以使用 DNS 解析来解析该 FQDN。

- 选择用于管理网络的 NIC。确保 NIC 处于连接状态。

**i 注:** 确保根据与 OMIVV 的网络连接选择管理 NIC。**将设置应用到所有服务器**选项不适用于管理 NIC 选择。

- 选择有权访问 vCenter 的 OMIVV 网络实例。有关更多信息，请参阅 [系统配置文件和 ISO 配置文件部署](#) 页面上的 57。

- 选择以下其中一个网络选项：

- 对于静态，输入首选的 DNS 服务器、备用 DNS 服务器、IP 地址、子网掩码和默认网关。
- **使用 VLAN** — 当提供 VLAN ID 时，会在部署期间将其应用于操作系统的管理接口并使用 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。有关更多信息，请参阅 [VLAN 支持](#) 页面上的 60。
- **使用 DHCP** — 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。

#### 11. 在计划部署作业页面中，执行以下操作：

- 编辑部署作业名称和说明。

- b. 要立即运行部署作业，请单击**立即运行**。
- c. 要将作业计划为稍后运行，请单击**计划稍后**，然后选择日期和时间。
- d. 选中**在提交作业后转到作业页面**复选框。  
您可以在**作业**页面中跟踪作业状态。有关更多信息，请参阅 [部署作业](#) 页面上的 67。

## 12. 单击**完成**。

**i** **注：**在裸机服务器上执行操作系统部署后，OMIVV 会清除所有 iDRAC 作业。

在旧版本的 OMIVV 上安排的 ISO 配置文件部署作业在最新版本的 OMIVV 中无效。取消已安排的作业，并根据需要创建部署作业。

如果已安排的作业未取消，部署作业将会失败。在这种情况下，查找裸机服务器，然后创建 ISO 配置文件部署作业。

## 部署系统配置文件和 ISO 配置文件

您只能在符合要求的裸机服务器上执行部署。有关更多信息，请参阅 [查看裸机服务器](#) 页面上的 48。

1. 要启动部署向导，请转至**合规性与部署 > 部署 > 部署**。
2. 在部署向导的**系统配置文件和 ISO 配置文件部署检查清单**页面上，验证部署任务清单，然后单击**开始**。
3. 在**选择服务器**页面上，选择一个或多个服务器。  
将显示**选择 RAID 级别**页面。
4. 在**选择部署选项**页面上，选择**系统配置文件（硬件配置）**和**ISO 配置文件（ESXi 安装）**。
5. 从**vCenter 名称**下拉菜单中，选择 vCenter 的实例。
6. 要选择 vCenter 目标容器，请单击**浏览**，然后选择要在其上部署操作系统的适当数据中心或群集。
7. 要使用与群集配置文件关联的系统配置文件（其与所选群集关联），请单击**确认**。
  - 要选择任何其他系统配置文件，请单击**选择另一个**。建议选择与群集关联的系统配置文件，以避免配置合规性偏移。
8. 从**ISO 配置文件**下拉菜单中，选择适当的 ISO 配置文件，然后单击**下一步**。
9. 要在 iDRAC 上创建预览作业，请在**配置预览**页面上，选择一个 iDRAC IP，然后单击**预览**。配置预览是可选任务。系统配置文件预览操作可能需要几分钟才能完成。比较状态显示在**结果**列中。

比较结果如下：

- **已完成** — 预览作业已成功运行。有关比较结果的详细信息，请单击**详细信息**列中的**查看详细信息**。
- **未完成** — 预览作业未在 iDRAC 上成功运行。如果需要，确保 iDRAC 可访问并执行 iDRAC 重设。有关作业的更多信息，请参阅 iDRAC 控制台上的 OMIVV 日志和日志。

10. 完成**部署 ISO 配置文件（ESXi 安装）**页面上的 58 主题中列出的任务 7-10。

## VLAN 支持

OMIVV 支持将操作系统部署到可路由 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，有一个用于指定使用 VLAN ID 的 VLAN 的选项。当提供 VLAN ID 时，会在部署期间将其应用于操作系统的管理接口并使用 VLAN ID 标记所有流量。

确保在部署期间提供的 VLAN 可以与 OMIVV 设备和 vCenter 服务器进行通信。将操作系统部署到无法与这些目标中的一个或两个通信的 VLAN 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，并且想要将同一 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**将设置应用于所有服务器**。通过此选项，您可以将相同的 VLAN ID 以及其他网络设置应用于该部署作业中的所有服务器。

**i** **注：**确保根据与 OMIVV 的网络连接选择管理 NIC。**将设置应用到所有服务器**选项不适用于管理 NIC 选择。

## 部署作业时间

系统配置文件和 ISO 配置文件部署可能需要 30 分钟到几个小时才能完成，具体视多方面因素而定。开始部署作业后，建议您根据提供的指南计划部署时间。完成系统配置文件和 ISO 配置文件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。部署作业最多用五个并行的服务器批量运行，从而缩短整个部署作业的时间。并行作业的确切数量视可用的资源而定。

下表显示平均值，并且可能会因诸如服务器配置、服务器代次以及为部署计划的裸机服务器的数量等因素而有所差异：

**表. 3: 单个服务器的大致部署时间**

部署类型	每个部署的大致时间
仅 ISO 配置文件	30-130 之间
仅系统配置文件	5 - 6 分钟
系统配置文件和 ISO 配置文件	30 - 130 分钟

## 部署顺序中的服务器状态

在自动查找期间查找到或手动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。管理员可以使用这些状态来检查硬件配置状态。

**表. 4: 部署顺序中的服务器状态**

服务器状态	说明
未配置	服务器已经添加至 OMIVV，并正在等待得到配置。
已配置	该服务器已按照成功部署操作系统需要的全部硬件信息配置完毕。

## 管理合规性

要查看和管理 OMIVV 中的主机，每个主机都必须符合特定条件。如果主机不符合合规性标准，则 OMIVV 不会管理和监测它们。OMIVV 会显示有关非合规主机的详细信息，并让您要解决不合规问题（如果适用）。

在下列情况下，主机是非合规：

- 主机未关联到主机凭据配置文件。
- 重新引导时收集系统资源清册 (CSIOR) 功能已禁用或尚未运行，需要手动重新引导。
- **注：**当使用机箱管理主机时，CSIOR 状态不确定。
- 主机的 SNMP 陷阱目标未配置至 OMIVV 设备 IP 地址。在主机凭据中为 iDRAC 或主机凭据提供的配置文件无效时，SNMP 陷阱目标设置可能会失败。或者，iDRAC 没有可用的插槽，或 iDRAC 锁定模式已开启 - 仅在基于 iDRAC9 的服务器中。有关基于 iDRAC9 的服务器的列表，请参阅兼容性值表。
- OMIVV 无法在运行 ESXi 6.5 及更高版本的主机上启用 WBEM 服务。
- iDRAC 固件版本低于 2.50.50.50。仅在使用系统配置文件功能时，才需要 iDRAC 2.50.50.50 版或更高版本。
- iDRAC 许可证不兼容（iDRAC Express 是最低要求）。没有兼容 iDRAC 许可证的服务器不能用于监测和更新固件。

**小心：**即使非合规，处于锁定模式的主机也不在合规性测试中显示。确保手动检查合规性级别。手动检查时，将会显示一条消息。请忽略该消息。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。

在**管理合规性**页面上，您可以执行以下任务：

- 解决合规性问题。有关更多信息，请参阅 [修复非合规主机](#) 页面上的 63。
- 运行资源清册。如果任何一个与主机凭据配置文件关联的主机的 iDRAC 状态为**非合规**或**未知**，则运行资源清册作业链接处于活动状态。
- 续订 iDRAC 许可证。有关信息，请参阅 [解决 iDRAC 许可证合规性问题](#) 页面上的 63。
- 添加 OEM 主机。有关添加 OEM 主机的更多信息，请参阅 [添加 OEM 主机](#) 页面上的 64。

## 查看非合规主机

1. 在 OMIVV 主页中，单击**合规性和部署 > 管理合规性**。

表格显示所有非合规主机及以下信息：

- **主机** - 主机的 FQDN 或 IP 地址
- **型号** - 服务器的型号名称
- **凭据配置文件** - 主机凭据配置文件名称
- **CSIOR 状态** - CSIOR 状态（**打开**或**关闭**）对于使用机箱进行管理的主机，CSIOR 状态显示为**未确定**。
- **SNMP 陷阱状态** - SNMP 陷阱状态（**已配置**或**未配置**）。
- **虚拟机监控程序** - 虚拟机监控程序名称和版本
- **WBEM 状态** - WBEM 状态（**合规**或**非合规**）。对于使用机箱进行管理的主机，CSIOR 状态显示**不适用**。
- **iDRAC 固件版本** - iDRAC 固件版本
- **iDRAC 许可证状态** - iDRAC 许可证状态（**合规**或**非合规**）。

**注：**使用机箱凭据配置文件管理 PowerEdge MX 主机时，iDRAC 固件版本在**管理合规性**页面上显示为**不适用**。这是因为 iDRAC 固件合规性不适用于基于 iDRAC9 的服务器。有关基于 iDRAC9 的服务器的列表，请参阅兼容性值表。

## 修复非合规主机

在下列情况下，主机是非合规：

- 主机未关联到主机凭据配置文件。
- 重新引导时收集系统资源清册 (CSIOR) 功能已禁用或尚未运行，需要手动重新引导。
  - ① **注：**当使用机箱管理主机时，CSIOR 状态不确定。
- 主机的 SNMP 陷阱目标未配置至 OMIVV 设备 IP 地址。在主机凭据中为 iDRAC 或主机凭据提供的配置文件无效时，SNMP 陷阱目标设置可能会失败。或者，iDRAC 没有可用的插槽，或 iDRAC 锁定模式已开启 - 仅在基于 iDRAC9 的服务器中。有关基于 iDRAC9 的服务器的列表，请参阅兼容性值表。
- OMIVV 无法在运行 ESXi 6.5 及更高版本的主机上启用 WBEM 服务。
- iDRAC 固件版本低于 2.50.50.50。仅在使用系统配置文件功能时，才需要 iDRAC 2.50.50.50 版或更高版本。
- iDRAC 许可证不兼容 (iDRAC Express 是最低要求)。没有兼容 iDRAC 许可证的服务器不能用于监测和更新固件。

1. 在 OMIVV 主页中，单击**合规性和部署 > 管理合规性**。
2. 选择非合规主机，单击**修正合规性**。
3. 在向导的欢迎页面中，阅读说明，然后单击**开始**。
4. 在**选择主机**页面中，选择一个或多个非合规主机，然后单击**下一步**。

- 如果主机未与主机凭据配置文件关联，则会显示以下警告消息：

*有一些选择的主机未分配给主机凭据配置文件。要允许 OMIVV 运行合规性检查，必须将这些主机添加到主机凭据配置文件要排除未分配给主机凭据配置文件的主机，请单击**继续**。*

要将主机添加到“主机凭据配置文件”页面，请单击**取消**并转到“主机凭据配置文件”页面。有关创建主机凭据配置文件的更多信息，请参阅**创建主机凭据配置文件** 页面上的 35。

需要使用机箱凭据配置文件来管理已禁用 iDRAC IPv4 的 MX 机箱中存在的主机。将这些主机与机箱凭据配置文件关联，您必须使用 **Dell EMC 机箱** 页面中的“添加 MX 机箱”来添加机箱。

要更新 iDRAC 固件和 BIOS 版本：

- a. 在**更新 iDRAC 固件和 BIOS 版本**页面中，选择一个或多个要在其上更新固件版本的主机。
- b. 单击**下一步**。
- c. 在**重新引导主机**页面中，查看必须重新启动的 ESXi 主机。
- d. 如果您想要自动将主机置于维护模式，然后在需要时重新启动，请选中相应的复选框，然后单击**下一步**。
- e. 在**摘要**页面中，审核操作摘要，然后单击**完成**。

要打开 CSIOR：

- a. 在**选择主机**页面中，选择一个或多个非合规主机，然后单击**下一步**。
- b. 在**开启 CSIOR**页面中，选择一个或多个要为其开启 CSIOR 的主机，然后单击**下一步**。
- c. 在**摘要**页面中，审核操作摘要，然后单击**完成**。

当您通过在主机凭据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基于 iDRAC9 的服务器。

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。启用 OMIVV 可在资源清册期间为这些主机启用 WBEM 服务。

## 解决 iDRAC 许可证合规性问题

兼容 iDRAC 许可证是主机的合规性标准之一。如果主机没有兼容的 iDRAC 许可证，则这些主机在**管理合规性**页面上列为不符合要求的主机。

您可以单击不符合要求主机以查看详细信息，例如 iDRAC 到期日期、许可证类型和许可证说明。如果任何与主机凭据配置文件关联的主机的 iDRAC 合规性状态为**非合规**或**未知**，则**运行资源清册作业**处于活动状态。

1. 要修复 iDRAC 许可证合规性，请在 OMIVV 主页上，单击**合规性和部署 > 合规性 > 管理合规性**。
2. 选择 iDRAC 许可证不符合要求的主机，然后单击**续订 iDRAC 许可证**。

3. 登录到 Dell Digital Locker，然后更新或购买新的 iDRAC 许可证。  
安装 iDRAC 许可证后，运行主机的资源清册作业并在资源清册作业成功完成后返回到此页面。

## 支持 OEM 服务器

通过提供类似于 PowerEdge 服务器的功能或产品组合的 Dell EMC 合作伙伴提供 OEM 服务器。

- 从 OMIVV 4.3 开始，支持 OEM 机架式服务器。
- 通过使用**添加 OEM 主机**向导，添加 OEM 服务器。有关添加 OEM 主机的更多信息，请参阅**添加 OEM 主机**页面上的 64。  
**注：**如果已在 OEM 主机上启用 WBEM 服务并且添加至 vCenter，默认情况下，OMIVV 将那些 OEM 服务器添加到 OMIVV 管理的列表。将主机关联到主机凭据配置文件以管理这些服务器。有关创建机箱凭据配置文件的更多信息，请参阅**创建主机凭据配置文件**页面上的 35。
- 添加 OEM 服务器后，所有主机管理进程将类似于如何管理 Dell EMC PowerEdge 服务器。
- 使用 iDRAC 的 OEM 服务器也将支持裸机部署功能。

## 添加 OEM 主机

除了 Dell EMC PowerEdge 服务器，OMIVV 还支持更名和品牌屏蔽的服务器。有关 OEM 的更多信息，请参阅 <https://www.dell.com>。

如果 WBEM 服务已启用，则 OMIVV 会确定主机的 iDRAC 连接。如果连接可用，OMIVV 会将主机添加到受管列表。

如果 OMIVV 无法确定，则您必须手动选择**添加 OEM 主机**向导上的主机，以便将主机添加到 OMIVV 的受管列表。

如果已禁用 WBEM 服务或 iDRAC 不可访问，请使用**添加 OEM 主机**向导以便主机可以添加到 OMIVV 管理列表。

1. 在 OMIVV 主页中，单击**合规性和部署 > 合规性 > 管理合规性 > 添加 OEM 主机**。
2. 在**添加 OEM 主机**窗口中，从**vCenter 实例**下拉列表选择一个 vCenter 实例。
3. 从**主机凭据配置文件**下拉列表中，选择相应的主机凭据配置文件。
4. 要添加或移除关联的主机，请单击**添加主机**。  
此时将显示**选择主机**窗口。
5. 在**选择主机**窗口中，选择主机，然后单击**是**。

**注：**仅在**选择主机**窗口中显示不受 OMIVV 管理的主机。

OMIVV 会自动测试连接，测试连接结果将显示在**添加 OEM 主机**窗口中。

**iDRAC 测试**和**主机测试**列显示了 **iDRAC 凭据**和**主机凭据**的测试连接结果。

要停止所有测试连接，请单击**中止测试**。

6. 单击**确定**。  
所选主机将添加到选定的主机凭据配置文件中，并将触发资源清册。

## 配置合规性

**配置合规性**页显示合规性状态基于与群集配置文件关联的所有群集的偏移检测。在具有多个 vCenter 服务器的 PSC 环境中，配置合规性页面列出了属于在同一设备中注册的同一 PSC 的所有 vCenter 中的所有群集。

- 硬件配置合规性 — 显示在群集配置文件中中和属于群集的关联主机中使用的系统配置文件之间的属性偏移。
- 固件合规性 — 显示在固件配置文件中中和在属于群集的关联主机中使用的系统配置文件之间的固件版本偏移。
- 驱动程序合规性 — 显示在群集配置文件中中和在属于群集配置文件的关联 vSAN 主机中使用的驱动程序库存配置文件之间的驱动程序版本偏移。

## 查看配置合规性

1. 在 OMIVV 主页中，单击**合规性和部署 > 合规性 > 配置合规性**。  
表格显示具有关联群集配置文件、系统配置文件、固件存储库配置文件和驱动程序存储库配置文件的群集。

对于基本和高级系统配置文件类型，系统配置文件名称采用以下格式显示：Basic\_<系统配置文件名称>，Advanced\_<系统配置文件名称>。

2. 在**配置合规性**页面上，选择一个群集。  
此时将显示配置合规性信息和合规性状态。

以下信息将显示在**配置合规性**部分中：

- **群集名称** — 群集的名称
- **合规性状态** — 显示合规性状态（合规或非合规）。如果群集中的任何主机都不符合要求，则状态显示为非合规。
- **主机数** — 群集中存在的主机总数
- **下计划** — 计划下次偏移检测作业的日期和时间。
- **上次偏移检测时间** — 上次偏移检测作业完成时的日期和时间。

**合规性状态**部分显示硬件、固件和驱动程序组件的合规性状态。不同的合规性状态如下：

- **合规** — 显示与关联的硬件、固件和驱动程序组件兼容的主机数量。
- **非合规** — 显示与关联的硬件、固件和驱动程序组件不兼容的主机数量。
- **不适用** — 显示不适用的主机数。

硬件偏移不适用于使用机箱凭据配置文件管理的主机。

驱动程序偏移不适用于属于 vSphere 群集一部分的主机。

如果群集配置文件是使用联机目录创建的，则固件合规性不适用于 vSAN 群集。

3. 要查看偏移详细信息，请单击**查看偏移报告**。只有不符合要求的群集才会启用此链接。有关查看偏移报告的更多信息，请参阅[查看偏移报告](#) 页面上的 65。

## 查看偏移报告

**配置合规性报告**页面显示硬件、固件和驱动程序组件的偏移详细信息。

偏移检测作业状态显示在**摘要**部分中。

有关硬件：

- **主机名或 IP** — 表示主机 IP 或主机名。
- **服务标签** — 表示主机的服务标签。
- **偏移状态** — 表示偏移状态（不符合标准或失败）。
- **实例** — 表示硬件组件名称。
- **组** — 表示属性的组名称。
- **属性名称** — 表示属性名称。
- **当前值** — 表示主机中属性的当前值。
- **基线值** — 表示基线值。
- **偏移类型/错误** — 表示不合规的原因。有关偏移类型的更多信息，请参阅[组件与基线版本比较值表](#) 页面上的 153。

**注：**只有当主机或 iDRAC 无法访问时，偏移检测作业才会失败。如果主机或 iDRAC 资源清册成功，则偏移检测作业会显示成功。要检查任何其他偏移检测作业失败原因，请参阅偏移报告中的**偏移类型/错误**列。

对于固件和驱动程序：

- **主机名或 IP** — 表示主机 IP 或主机名。
- **服务标签** — 表示主机的服务标签。
- **偏移状态** — 表示偏移状态。
- **组件名称** — 显示组件的名称。
- **当前值** — 表示主机中属性的当前值。
- **基线值** — 表示基线值。
- **偏移类型/错误** — 表示不合规的原因。有关偏移类型的更多信息，请参阅[组件与基线版本比较值表](#) 页面上的 153。
- **严重程度（对于固件）** — 表示标识组件的更新版本的重要级别。
- **建议（对于驱动程序）** — 表示驱动程序组件的更新建议。

**注：**如果有多个固件版本可用，则始终将最新的固件版本用于合规性比较。

您可以使用过滤器选项来查看基于偏移状态的偏移详细信息。

- 注:** 32 位固件捆绑包在 5.x 版中不受支持。如果群集配置文件与 4.x 版中的 32 位固件捆绑包关联，则当您执行从 4.x 到 5.x 的备份和还原时，偏移状态显示为失败。将 64 位固件捆绑包用于群集配置文件，然后重新运行偏移检测作业。
- 注:** 您可能会看到 OMIVV 与 vSphere 生命周期管理器偏移报告之间存在不匹配。这是因为 vSphere 生命周期管理器始终显示实时偏移报告，而 OMIVV 会显示基于安排的日期和时间的偏移报告。如果在偏移报告之间看到不匹配，请在**偏移检测作业**页面上按需运行偏移检测作业。

## 管理 OMIVV 作业

作业页面会显示以下作业信息：

- 部署
- 查找
- 固件更新
- 系统锁定模式
- 漂移检测
- 资源清册
- 保修

当作业总数达到 500 时，OMIVV 会清除较旧的作业，包括用户创建的作业（例如，部署作业）和 OMIVV 创建的作业（例如，运行状况指标集合作业）。如果作业数超过 500，则会删除较旧的 500 个作业。

### 部署作业

部署任务完成后，您可以在**部署作业**页面上跟踪部署作业状态。

1. 在 OMIVV 主页中，单击**作业 > 部署作业**。

表格显示所有部署作业及以下信息：

- **名称** - 部署作业名称
- **说明** - 作业说明
- **计划的时间** - 计划作业时的日期和时间。
- **状态** - 部署作业的状态
- **集合大小** - 部署作业中的服务器数
- **进度摘要** - 部署作业的进度详细信息

2. 要查看有关部署作业中的服务器的更多信息，请选择部署作业。

以下信息会显示在下部窗格中：

- **服务标签**
- **iDRAC IP**
- **状态**
- **警告**
- **详细信息**
- **开始日期和时间**
- **结束日期和时间**
- **更多详细信息**

- a. 要查看关于部署作业的更多信息，请选择一个作业，然后将鼠标指针放置在**详细信息**列上。

- b. 要查看基于系统配置文件作业故障的更多信息，请单击**更多详细信息**。

此时会显示以下信息：

- 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。

3. 要停止部署作业，请单击**停止**。

4. 要清除部署作业，请单击**清除已完成**，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**部署作业**页面中清除。

## 发现作业

创建查找任务后，您可以在**查找作业**页面上跟踪作业状态。

1. 在 OMIVV 主页中，单击**作业 > 发现作业**。

表格显示所有发现作业及以下信息：

- **名称** - 发现作业名称
- **说明** - 作业说明
- **计划的时间** - 计划作业时的日期和时间。
- **状态** - 发现作业的状态。

成功查找到服务器后，作业状态显示成功。

如果作业失败，将显示失败的原因。

- **集合大小** - 发现作业中的服务器数
- **进度摘要** - 发现作业的进度详细信息

2. 要查看更多信息，请选择发现作业。

以下信息会显示在下部窗格中：

- **iDRAC IP**
- **状态**
- **详细信息**
- **开始日期和时间**
- **结束日期和时间**

3. 要清除发现作业队列，请单击**清除已完成**。

- a. 选择日期。

早于所选日期的作业将被删除。

- b. 选择作业的状况。
- c. 单击**应用**。

## 机箱固件更新作业

机箱固件更新任务完成后，您可以在**机箱固件更新作业**页面上查看固件更新作业的状态。

1. 在 OMIVV 主页中，单击**作业 > 固件更新 > 机箱固件更新**。

2. 要显示最新的日志信息，请单击刷新图标。

表格显示所有机箱固件配置文件及以下信息：

- **状态** - 固件更新作业的状态
- **计划的时间** - 固件更新作业计划的时间
- **名称** - 作业的名称
- **说明** - 固件更新作业说明
- **vCenter** - vCenter 名称
- **集合大小** - 固件更新作业中的机箱数。

机箱总数量仅包括主机箱和独立机箱。不包括成员机箱。

- **进度摘要** - 固件更新的进度详细信息

3. 要查看有关特定作业的详细信息，请选择作业。

以下信息会显示在下部窗格中：

- **机箱服务标签** - 机箱的服务标签
- **状态** - 作业的状态
- **开始时间** - 固件更新作业的开始时间
- **结束时间** - 固件更新作业的结束时间

4. 如果您想要停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**停止**。

 **警告:** 如果您停止一个已提交至 MX 机箱的固件更新作业, 固件可能仍在主机上更新。OMIVV 报告作业已取消。

5. 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**清除已完成**。此时会显示**清除固件更新作业**对话框。您可以只清除已取消、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。
6. 在**清除固件更新作业**对话框中, 选择**早于日期和作业状态**, 然后单击**确定**。然后, 所选作业会从**机箱固件更新作业**队列中清除。

## 主机固件更新作业

机箱固件更新任务完成后, 您可以在**主机固件更新作业**页面上查看固件更新作业的状态。


1. 在 OMIVV 主页中, 单击**作业 > 固件更新 > 主机固件更新**。

2. 要显示最新的日志信息, 请单击刷新图标。  
表格显示所有主机固件更新作业及以下信息:

- **状态** - 固件更新作业的状态
- **计划的时间** - 固件更新作业计划的时间
- **名称** - 作业的名称
- **说明** - 固件更新作业说明
- **vCenter** - vCenter 名称
- **集合大小** - 固件更新作业中包括的服务器数
- **进度摘要** - 固件更新的进度详细信息

3. 要查看有关特定作业的详细信息, 请选择作业。  
以下信息会显示在下部窗格中:

- **主机名称** - 主机的服务标签
- **状态** - 作业的状态
- **开始时间** - 固件更新作业的开始时间
- **结束时间** - 固件更新作业的结束时间

 **注:** 如果计划了使用多个 Dell 更新软件包的固件更新作业, 并且 OMIVV 无法下载某些选定的更新软件包, OMIVV 将继续更新成功下载的软件包。作业页面显示成功下载的软件包的状态。

4. 如果您想要停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**停止**。

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

5. 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**清除已完成**。此时会显示**清除固件更新作业**对话框。您可以只清除已取消、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。
6. 在**清除固件更新作业**对话框中, 选择**早于日期和作业状态**, 然后单击**确定**。然后, 所选作业会从**主机固件更新作业**队列中清除。

## 系统锁定模式作业

系统锁定模式设置仅受基于 iDRAC9 的服务器支持。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。从 OMIVV 4.1 版和更高版本中, 您可以配置和监测服务器中 iDRAC 的锁定模式。此外, iDRAC 必须具有企业版许可证才能启用锁定模式。

 **注:** 您无法更改使用机箱凭据配置文件管理的主机的系统锁定模式。

系统锁定配置完成后, 您可以在**系统锁定模式作业**页面中查看锁定模式的更新状态。

1. 在 OMIVV 主页中, 单击**作业 > 系统锁定模式**。

表格显示所有系统锁定模式及以下信息:

- **名称** - 系统锁定模式作业名称
- **说明** - 作业说明
- **计划时间** - 计划系统锁定模式作业时的日期和时间。
- **vCenter** - vCenter 名称
- **状态** - 系统锁定模式作业的状态
- **集合大小** - 系统锁定模式作业中包括的服务器的数量
- **进度摘要** - 系统锁定模式作业的作业进度详细信息

2. 要查看有关系统锁定模式作业中的服务器的详细信息，请选择系统锁定模式作业。以下信息会显示在下部窗格中：

- 服务标签
- iDRAC IP
- 主机名
- 状态
- 详细信息
- 开始日期和时间
- 结束日期和时间

要查看关于系统锁定模式作业的更多信息，请选择一个作业，然后将鼠标指针放置在**详细信息**列上。

3. 要清除系统锁定模式作业，请单击**清除已完成**，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**系统锁定模式**作业页面中清除。

## 偏移检测作业

运行偏移检测作业是为了了解验证的基线和服务器配置（包括硬件配置、固件和驱动程序版本）之间的对比。

**注：**只有当主机或 iDRAC 无法访问时，偏移检测作业才会失败。如果主机或 iDRAC 资源清册成功，则偏移检测作业将成功运行，您可以在偏移报告中查看偏移的详细信息。有关偏移报告的更多信息，请参阅[查看偏移报告](#) 页面上的 65。

1. 在 OMIVV 主页中，单击**作业 > 偏移检测**。

表格显示所有偏移检测作业及以下信息：

- **名称** - 偏移检测作业的名称
- **上次运行** - 上次运行偏移检测作业的日期和时间
- **下次运行** - 计划下次偏移检测作业的日期和时间
- **状态** - 偏移检测作业的状态
- **集合大小** - 偏移检测作业中的服务器数
- **进度摘要** - 偏移检测作业的进度详细信息

2. 要查看更新的偏移检测作业详细信息，请单击**刷新**。

3. 要查看有关偏移检测作业中的服务器的更多信息，请选择偏移检测作业。此时会显示以下信息：

- 服务标签
- iDRAC IP
- 主机名
- 群集
- vCenter
- 状态
- 开始日期和时间
- 结束日期和时间

4. 要按需运行**偏移检测**作业，请单击**立即运行**。

在基线群集中，将主机添加到主机凭据配置文件或机箱凭据配置文件后，偏移检测作业将在新添加的主机设备上自动运行。

## 查看主机资源清册作业

**主机资源清册**页面显示有关在与主机凭据配置文件关联的主机上运行的最新资源清册作业的信息。

1. 在 OMIVV 主页中，单击**作业 > 资源清册 > 主机资源清册**。

2. 选择 vCenter，以查看所有关联的主机资源清册作业的信息。

- **vCenter** — vCenter FQDN 或 IP 地址
- **通过的主机** — 成功运行了资源清册的主机计数
- **上次资源清册** — 上次运行资源清册的日期和时间
- **下次资源清册** — 下次资源清册计划运行的日期和时间

关联的主机详细信息显示在底部窗格中。

- **主机** — 主机的 FQDN 或 IP 地址

- **状态** — 主机的资源清册状态。选项包括：
  - 成功
  - 失败
  - 正在进行
- **持续时间（分钟:秒）** — 资源清册作业的持续时间，以分钟和秒为单位
- **开始日期和时间** - 显示资源清册作业开始时的日期和时间
- **结束日期和时间** - 资源清册作业完成时的日期和时间

## 运行资源清册作业

一旦初始配置完成，将针对添加到主机凭据配置文件的所有主机自动触发资源清册作业。

1. 要按需运行资源清册，请单击**作业 > 资源清册 > 主机资源清册**。
2. 单击**立即运行**。
3. 要查看资源清册作业的状态，可单击**刷新**。  
资源清册作业完成后，您可以在 **OMIVV 主机信息**页面上查看主机信息。
4. 要查看 OMIVV 主机信息，请展开**菜单**，然后选择**主机和群集**
5. 在左侧窗格中，选择任意主机。
6. 在右侧窗格中，选择**监测**，然后展开 **OMIVV 主机信息**。  
此时会显示以下信息：
  - 硬件资源清册
  - 存储
  - 固件
  - 电源监测
  - 保修
  - 系统事件日志

使用机箱凭据配置文件管理主机时，固件资源清册数据将显示少数几个额外的组件，例如 Lifecycle Controller 和软件 RAID。

**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。

7. 在**摘要**页面上的 **OMIVV 主机信息**部分中，您还可以执行以下操作：
  - 启动远程访问控制台 (iDRAC)
  - 让服务器 LED 指示灯闪烁
  - 配置系统锁定模式  
当机箱管理主机时，将不支持配置系统锁定模式。
  - 运行固件向导

## 修改主机资源清册作业

将主机关联到主机凭据配置文件之后，必须定期计划资源清册，以确保主机的资源清册信息是最新的。资源清册作业显示在主机上运行的资源清册作业的状态。

您还可以从**设置 > 数据检索计划 > 资源清册检索**页面修改资源清册计划。

1. 在**作业**页面中，选择 vCenter 实例，然后单击**编辑计划**。  
此时会显示**资源清册数据检索**对话框。
2. 在**资源清册数据**部分下，请执行以下操作：
  - a. 选中**启用资源清册数据检索（建议）**复选框。
  - b. 选择资源清册数据检索日期和时间，然后单击**应用**。
  - c. 要重设设置，请单击**清除**。
  - d. 要立即运行资源清册作业，请在**作业**页面中，单击**立即运行**。

**注：**对于没有 iDRAC Express 或 Enterprise 许可证的服务器，资源清册将会失败，因为 iDRAC 需要许可证升级。

**注：**当运行模块化主机资源清册时，系统会自动查找相应的机箱。如果机箱是机箱凭据配置文件的一部分，则会在主机资源清册后自动运行机箱资源清册。

## 查看机箱资源清册作业

机箱资源清册页面显示有关在与凭据配置文件关联的机箱上运行的最新资源清册作业的信息。

1. 在 OMIVV 主页中，单击**作业 > 资源清册 > 机箱资源清册**。
2. 要查看机箱资源清册信息，请选择机箱。
  - **机箱 IP/主机名** - 机箱的 IP 地址
  - **服务标签** - 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** - 显示资源清册作业开始时的日期和时间。
  - **结束日期和时间** - 资源清册作业完成时的日期和时间

在 MCM 组中，资源清册仅在主机箱上运行。资源清册信息提供有关主机箱和成员机箱的数据。

**注：**在以下 PowerEdge 服务器上不支持机箱资源清册作业：C6320P、C6320、C4130 和 C6420。

**注：**MX 机箱刀片式服务器仅对于 ESXi 版本 6.5U2 及更高版本受支持。如果在这些主机上部署较早的 ESXi 版本，则 OMIVV 中的资源清册作业将会失败。

## 运行机箱资源清册作业

1. 在 OMIVV 主页中，单击**作业 > 机箱资源清册**。
2. 选择机箱，然后单击**立即运行**。  
完成机箱资源清册后，您可以在**主机和机箱 > 机箱**页面上查看机箱信息。
3. 要查看机箱信息，请在**机箱**页面上选择一个机箱，然后单击**查看**。
  - 注：**在资源清册期间，陷阱目标和警报策略由 OMIVV 在 MCM 组中的主机箱上配置。
  - 注：**使用机箱管理主机时，运行机箱资源清册将会触发主机的主机资源清册。同样，运行主机资源清册也将触发机箱资源清册。

## 查看主机保修

保修作业是一项计划任务，以通过 [www.dell.com/support](http://www.dell.com/support) 上获得所有系统的保修信息。确保 OMIVV 设备具有互联网连接性来以提取保修信息。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。

1. 在 OMIVV 主页中，单击**作业 > 保修 > 主机保修**。
2. 选择 vCenter，以查看关联的主机信息。
  - **vCenter** — vCenter 的列表
  - **通过的主机** — 通过的 vCenter 主机数
  - **上次保修** — 上次保修作业运行的日期和时间。
  - **下次保修** — 下次保修作业的运行日期和时间。

关联的主机详细信息显示在底部窗格中。

- **主机** — 主机 IP 地址
- **状态** - 保修作业的状态，选项包括：
  - 成功
  - 失败
  - 正在进行
  - 已计划

- **持续时间 (MM:SS)** - 保修作业的持续时间，以分钟:秒为单位。
- **开始日期和时间** — 保修作业开始时的日期和时间
- **结束日期和时间** — 保修作业结束时的时间

3. 要按需运行主机箱保修，请单击**立即运行**。

## 修改主机保修作业

保修作业最初在**初始配置向导**中配置。您还可以在**设置 > 数据检索计划 > 保修检索**页面上修改保修作业计划。


1. 在**作业**页面上，展开**保修**，然后选择**主机保修**。
2. 选择 vCenter，然后单击**编辑计划**。
3. 在**保修数据**部分下，请执行以下操作：
  - a. 选中**启用保修数据检索 (建议)**复选框。
  - b. 选择保修数据检索日期和时间，然后单击**应用**。
  - c. 要重设设置，请单击**清除**。

## 查看机箱保修

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。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。

1. 在 OMIVV 主页中，单击**作业 > 保修 > 机箱保修**。  
表格会显示所有机箱保修作业信息。
  - **机箱 IP/主机名** - 主机 IP 地址
  - **服务标签** - 显示机箱的服务标签
  - **状态** - 保修作业的状态，选项包括：
    - 成功
    - 失败
    - 正在进行
    - 已计划
  - **持续时间 (MM:SS)** - 保修作业的持续时间，以分钟:秒为单位。
  - **开始日期和时间**： - 保修作业开始时的日期和时间。
  - **结束日期和时间** - 保修作业结束时的日期和时间。
2. 要按需运行机箱保修作业，请单击**立即运行**。

## 查看日志历史记录

1. 在 **OpenManage Integration for VMware vCenter** 页面中，要查看所有日志，请单击**日志**。  
OMIVV 日志检索过程将从其数据库中检索所有日志。这可能需要几秒钟，具体取决于日志大小。
  - 要导出日志数据，单击 。
  - 要为网格中的数据排序，请单击列标题。
  - 要在页面之间导航，请单击上一页和下一步图标。
  - 要刷新日志，请单击左上角的刷新图标。
2. 单击▼以根据以下类别或日期范围过滤日志：  
**类别：**
  - **所有类别**
  - **信息**
  - **警告**
  - **错误****日期：**
  - **上周**
  - **上个月**
  - **去年**
  - **自定义范围**：如果您选择此选项，请通过单击“日历”图标指定开始日期和结束日期。
3. 选择所需的类别和日期后，单击**应用**。  
您可以查看与所选类别和/或日期范围的相关的日志。日志数据表一次在一个页面上 100 个日志。
4. 要清除筛选后的数据，请单击**清除筛选器**。

## 管理 OMIVV 设备设置

在**设置**页面上，您可以执行以下任务：

- 配置保修到期通知设置。有关更多信息，请参阅 [配置保修到期通知](#) 页面上的 75。
- 配置最新设备版本通知。有关更多信息，请参阅 [配置最新设备版本通知](#) 页面上的 75。
- 覆盖主动式高可用性警报的严重性。有关更多信息，请参阅 [覆盖运行状况更新通知的严重性](#) 页面上的 78。
- 初始配置。有关更多信息，请访问 [初始配置](#) 页面上的 79
- 配置并查看事件和警报。有关更多信息，请参阅 [配置事件和警报](#) 页面上的 83。
- 计划或修改资源清册和保修的数据检索计划。有关更多信息，请参阅[计划资源清册作业](#) 页面上的 91 和[计划保修检索作业](#) 页面上的 91。

### 管理多个设备

如果多个 vCenter 实例共享相同的 PSC，并且如果这些 vCenter 向 OMIVV 设备的多个实例注册，则可使用交换机设备向导在 OMIVV 的不同实例之间切换。

您可以在主页上看到 OMIVV 的当前实例。

1. 在 **OMIVV** 主页中，单击**更改**。
  - **IP/名称** — OMIVV 设备 FQDN 或 IP
  - **版本** — OMIVV 设备的当前版本
  - **合规性状态** — 基于版本的 OMIVV 设备的状态（**合规或非合规**）
  - **可用性状态** — OMIVV 设备的可用性状态基于 OMIVV 服务是否正在运行。显示**正常**或**错误**以指示 OMIVV 的工作状态。
  - **已注册的 vCenter 服务器** — 已注册的 vCenter 服务器 FQDN 或 IP。
  - **操作**操作名称（**选择**或**选中**）。
2. 在**交换机 OMIVV 设备**页面中，单击**选择**。
3. 要确认，请单击**是**。  
您可以在主页上查看设备 IP 中的更改。

### 配置保修到期通知

启用保修到期通知，以便在任何主机的保修即将过期时收到通知。

1. 在 OMIVV 主页中，单击**设置 > 通知 > 保修到期通知**。
2. 选择**为主机启用保修到期通知**。
3. 选择在保修到期之前要接收到通知的天数。
4. 单击**应用**。

### 配置最新设备版本通知

要获取有关新 OMIVV 版本可用性的通知，请选中**启用最新版本通知（建议）**复选框。建议每周检查一次。要使用 OMIVV 的最新设备版本通知功能，您必须具有互联网连接。如果您的环境需要代理连接至互联网，请确保在管理员门户上配置代理设置。

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：

1. 在 OMIVV 主页中，单击**设置 > 设备设置 > 通知 > 最新版本通知**。
2. 选择**启用最新版本通知（建议）**复选框。
3. 要接收最新的设备版本通知，请选择日期和时间。

#### 4. 单击应用。

## 配置部署凭据

OMIVV 用作配置服务器。在自动查找过程中，部署凭据可让您与使用 OMIVV 插件作为配置服务器的 iDRAC 进行通信。部署凭据可让您设置 iDRAC 凭据以与使用自动查找来查找到的裸机服务器安全通信，直到操作系统部署完成为止。

操作系统部署过程成功完成后，OMIVV 会如在主机凭据配置文件中提供的那样更改 iDRAC 凭据。如果您更改部署凭据，则从该时间点开始使用自动查找来查找到的所有新系统都会使用新的 iDRAC 凭据调配。但是，在更改部署凭据之前已查找到的服务器上的凭据不受此更改影响。

1. 在 OMIVV 主页中，单击**设置 > 设备设置 > 部署凭据**。
2. 输入用户名和密码。默认用户名是 **root**，默认密码是 **calvin**。  
确保根据 iDRAC 中设置的 iDRAC 用户密码策略输入密码。此外，请确保使用 iDRAC 支持的字符。
3. 单击**应用**。

## 硬件组件冗余运行状况 — 主动式高可用性

主动式高可用性是与 OMIVV 配合使用的 vCenter 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。

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。中度降级状态在**事件**页面的**类型**列中表示为**警告**。
- 严重（严重降级） — 组件有严重故障。

**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。

**注：**

- 在配置事件时，建议选择“发布所有事件”选项作为事件发布级别。有关配置事件的更多信息，请参阅**配置事件和警报**页面上的 83。
- 主动式高可用性仅在支持电源、风扇和 iDSDM 的平台上可用。
- 主动式高可用性功能对于无法配置冗余的 PSU（例如，已连接电缆的 PSU）不受支持。

## 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。

表. 5: Dell 主动式高可用性事件

Dell Inc 提供商事件	组件类型	说明
DellFanRedundancy	Fan	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 <b>注：</b> 当主机添加到启用主动式高可用性的群集并且如果存在 IDSDM 组件时，

**表. 5: Dell 主动式高可用性事件 (续)**

Dell Inc 提供商事件	组件类型	说明
		请确保在 iDRAC 设置中将内部 SD 卡冗余配置为 <b>镜像</b> 。

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。

**表. 6: 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
集成的双 SD 模块冗余丢失	集成的双 SD 模块冗余丢失	严重
<b>机箱事件</b>		
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

## 配置机架式和塔式服务器的主动式高可用性

确保所有主机已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。

1. 创建主机凭据配置文件并将主机关联至主机凭据配置文件。请参阅[创建主机凭据配置文件](#) 页面上的 35。
2. 验证主机资源清册是否已成功完成。请参阅[查看主机资源清册作业](#) 页面上的 70。

3. 验证 iDRAC 中的 SNMP 陷阱目标设置为 OMIVV 设备 IP 地址。  
**注：** 确保根据日志数据确认主机可用于主动式高可用性群集。
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

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。
- 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，因为机箱组件（PSU 和风扇）故障会影响其所有关联服务器。
1. 创建主机凭据配置文件并将主机关联至主机凭据配置文件。请参阅[创建主机凭据配置文件](#) 页面上的 35。
  2. 验证主机资源清册是否已成功完成。请参阅[查看主机资源清册作业](#) 页面上的 70。  
**注：** 确保根据日志数据确认主机可用于主动式高可用性群集。
  3. 创建与机箱关联的机箱凭据配置文件。请参阅[创建机箱凭据配置文件](#) 页面上的 39。
  4. 验证是否已成功完成机箱资源清册。请参阅[查看机箱资源清册作业](#) 页面上的 72。
  5. 启动 CMC 或 OME-Modular 并验证机箱的陷阱目标是否已设置为 OMIVV 设备 IP 地址。有关配置陷阱的详细信息，请参阅 e CMC and OME-Modular User's Guide（CMC 和 OME 模块化用户指南），网址为：[dell.com/support](http://dell.com/support)。
  6. 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](#)。

## 在群集上启用主动式高可用性

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主机凭据配置文件的一部分并已成功进行资源清册。
  - 对于模块化服务器，必须将相应的机箱添加到机箱凭据配置文件并已成功进行资源清册。
1. 在 vSphere Client 中，展开**菜单**，然后选择**主机和群集**。  
所有主机和群集均显示在左侧窗格中。
  2. 选择一个群集，然后在右侧窗格中，单击 **vSphere DRS > 编辑**。
  3. 如果尚未选择 **vSphere DRS**，请选择它。
  4. 选择**配置 > vSphere 可用性 > 主动式高可用性 > 编辑**。  
此时会显示**编辑群集设置**页面。
  5. 在**编辑群集设置**页面中，选择**主动式高可用性**。
  6. 在**失败和响应**部分中，从下拉菜单中选择**手动**或**自动**自动化级别。
  7. 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。
  8. 单击**提供商**并选择 **Dell Inc** 作为群集的提供商。
  9. 单击**保存**。

在群集上启用主动式高可用性后，OMIVV 会初始化主动式高可用性运行状况和冗余状态并报告给 vCenter。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](#) 页面上的 78。

在 RPM 升级以及备份和恢复操作后，在面向 PHA 群集的已注册 Dell 运行状况更新提供程序上执行的所有自定义设置都将恢复为默认值。

## 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。

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

**i 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。

1. 在 OpenManage Integration for VMware vCenter 中，单击**设置 > 覆盖主动式高可用性事件的严重性**。  
数据网格显示所有受支持的主动式高可用性事件。数据网格列包括用于自定义主机及其组件严重性的列（如事件 ID、事件说明、组件类型、默认严重性和覆盖严重性列）。
2. 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。
3. 对必须自定义的所有事件重复步骤 2。
4. 执行下面的任意一项操作：
  - a. 要保存自定义工作，请单击**应用**。
  - b. 要取消覆盖严重性设置，请单击**取消**。
 要将覆盖严重性设置重设为默认值，请单击**重设为默认值**。

## 初始配置

您完成 OMIVV 基础安装和 vCenter 注册后，启动 vCenter 中的 OMIVV 时，将自动显示初始配置向导。

如果您想要稍后启动初始配置向导，请转至：

- **设置 > 初始配置向导 > 启动初始配置向导**
- **控制面板 > 快速参考 > 启动初始配置向导**

1. 在**欢迎**页面中，阅读说明，然后单击**开始**。
2. 在**选择 vCenter**页面的**vCenter**下拉菜单中，选择特定 vCenter 或**所有已注册的 vCenter**，然后单击**下一步**。  
**i 注:** 如果您具有多台属于同一 PSC 且使用相同 OMIVV 设备注册的 vCenter 服务器，并选择配置单台 vCenter 服务器，请重复执行第 2 步，直至配置完每个 vCenter。

3. 在**创建主机凭据配置文件**页面中，单击**创建主机凭据配置文件**。  
有关创建机箱凭据配置文件的更多信息，请参阅**创建主机凭据配置文件**页面上的 35。

将主机添加到主机凭据配置文件后，OMIVV 的 IP 地址会自动设置为主机 iDRAC 的 SNMP 陷阱目标。OMIVV 在运行 ESXi 6.5 及更高版本的主机上会启用 WBEM 服务，然后在检索 iDRAC IP 之后会禁用该服务。

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。要查看并修复非合规问题，请参阅**修复非合规主机**页面上的 63。

4. 在**配置其他设置**页面中，执行以下操作：
  - a. 计划资源清册作业。要获取有关计划资源清册数据的更多信息，请参阅**计划资源清册作业**页面上的 91。
  - b. 计划保修检索作业。要获取有关计划保修检索作业的更多信息，请参阅**计划保修检索作业**页面上的 91。  
如果您要修改资源清册作业计划，请转至**设置 > vCenter 设置 > 数据检索计划 > 资源清册检索或作业 > 资源清册 > 主机资源清册**。  
如果您要修改保修检索作业计划，请转至**设置 > vCenter 设置 > 数据检索计划 > 保修检索或作业 > 保修**。
  - c. 配置事件和警报。有关配置事件和警报的信息，请参阅**配置事件和警报**页面上的 83。
  - d. 要应用个别设置，请单独单击**应用**按钮，然后单击**下一步**。  
强烈建议启用所有附加设置。如果未应用任何附加设置，将显示一条消息，指出所有附加设置都是必需的。
5. 在**后续步骤**页面中，阅读说明，然后单击**完成**。

建议将 OMIVV 主机与配置基线相关联，因为它使您能够密切监控主机和关联群集中发生的配置更改。只要主机成功通过 OMIVV 进行管理，便可为任何群集创建配置基线。要创建配置基线，请执行以下操作：

- 创建固件和驱动程序的存储库配置文件 - 这有助于您定义基准的固件和驱动程序版本。
- 创建系统配置文件 - 这有助于您定义主机的基准硬件配置。
- 创建群集配置文件 - 要创建成功的基线，请选择群集并关联固件、驱动程序和硬件配置。
- 需要使用机箱凭据配置文件管理已禁用 iDRAC IPv4 的 PowerEdge MX 机箱中存在的主机。

## 查看初始配置状态

在“初始配置向导”页面上，您可以执行以下操作：

- 查看初始配置状态  
只有当所有 vCenter 均配置了主机凭据配置文件、事件和警报、清单和保修作业时，才会显示初始配置状态。
- 启动初始配置向导

## 固件更新设置

选中**清除 iDRAC 作业和重设 iDRAC**复选框，在更新主机上的固件之前，清除**作业队列**中的所有 iDRAC 作业，然后进行 iDRAC 重设。

在执行以下操作时，将使用**清除 iDRAC 作业和重设 iDRAC**设置：

- 使用 OMIVV 进行固件更新  
在使用 OMIVV 更新固件时可以覆盖此设置。但是，覆盖此设置不会对在**固件更新设置**页面上所做的设置产生任何影响。
  - 使用 vSphere 生命周期管理器进行固件修复  
在执行固件修复时，不能覆盖此设置。
1. 选中**清除 iDRAC 作业和重设 iDRAC**复选框。
  2. 单击**应用**。

## 查看许可证信息

上传 OMIVV 许可证时，此选项卡将显示支持的主机和 vCenter 服务器的数量。

要购买软件许可证，请单击**软件许可证**旁边的**购买许可证**。有关更多信息，请参阅[购买软件许可证](#) 页面上的 81。

将在**许可证**页面中显示以下信息：

许可证类型	说明
<b>主机许可证</b>	<ul style="list-style-type: none"><li>• 可用的许可证 显示可用的许可证数</li><li>• 使用中的许可证 显示使用中的许可证数</li></ul>
<b>vCenter 许可证</b>	<ul style="list-style-type: none"><li>• 可用的许可证 显示可用的许可证数</li><li>• 使用中的许可证 显示使用中的许可证数</li></ul>

**许可证管理**部分显示以下各项的链接：

- 产品许可门户（数字保险箱）
- 管理员控制台

## OpenManage Integration for VMware vCenter (OMIVV) 许可

OMIVV 有两种类型的许可证：

- 评估许可证 — 当 OMIVV 设备首次开机时，将自动安装评估许可证。试用版包含一个评估许可证，可由 OMIVV 管理五个主机（服务器）。此 90 天的试用版本是发货时随附的默认许可证。

- 标准许可证 — 您可以购买由 OMIVV 管理的任意数量的主机许可证。此许可证包括产品支持和 OMIVV 设备更新。标准许可证可使用三年或五年。购买的任何附加许可证都会延长现有许可证的期限。

单个 XML 密钥的许可证期限基于原始订单的销售日期计算。任何已上传新许可证将在任何先前的到期许可的 90 天宽限期结束后反映在计数中。

OMIVV 最多支持 15 个 vCenter 实例。从评估许可证升级到完整标准许可证后，您将收到一封订单确认电子邮件，然后便可从 Dell Digital Locker 下载许可证文件。将许可证 .XML 文件保存到您的本地系统，并使用**管理控制台**上传新的许可证文件。

购买许可证时，可从 Dell Digital Locker <https://www.dell.com/support> 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 <https://www.dell.com/support> 处的**联系订单支持**找到您的产品对应的区域 Dell 支持电话号码，联系 Dell 支持部门。

许可会在 OMIVV 管理控制台中显示以下信息：

- 最大 vCenter 连接许可证数 — 可启用最多 15 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（对于单个 OMIVV 实例，最多支持 2000 个主机）。
- 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。

在尝试将主机添加到主机凭据配置文件时，如果许可的主机的数量超出许可证数量，将无法添加更多主机。OMIVV 不支持管理超过主机许可证的数量的主机数。

**i** 注：任何活动许可证都可以用于 OMIVV 5.x 版本。从以前的 OMIVV 实例备份或从 Digital Locker 再次下载的许可证可以用于 OMIVV 的当前实例。

## 购买软件许可证

1. 转至**设置 > 许可 > 购买许可证或控制面板 > 购买许可证**，或者**管理员门户 > vCenter 注册 > 许可 > 立即购买**。此时将显示 Dell EMC 支持页面。
2. 下载许可证文件并将其保存到已知的位置。  
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。

## 访问支持信息

表. 7: 支持页面上的信息

名称	说明
文档支持	提供以下文档链接： <ul style="list-style-type: none"> <li>● PowerEdge 服务器</li> <li>● OMIVV 手册</li> <li>● 带 Lifecycle Controller 的 iDRAC</li> </ul>
管理控制台	提供指向管理控制台的链接。
一般帮助	提供 Dell EMC 支持网站的链接。
重设 iDRAC	提供用于重设 iDRAC 的链接，可在 iDRAC 不响应时使用。此重设操作执行正常的 iDRAC 重新引导。有关重设 iDRAC 的更多信息，请参阅 <a href="#">重设 iDRAC</a> 页面上的 82。
致电技术支持之前	提供有关如何与 Dell EMC 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 <a href="#">创建和下载故障排除捆绑包</a> 页面上的 82。
Dell EMC 建议	提供指向 Dell EMC Repository Manager (DRM) 支持页面的链接。DRM 用于创建自定义目录，后者可用于更新固件和偏移检测。

## 创建和下载故障排除捆绑包

要生成故障排除捆绑包，请确保您登录到管理员门户。

故障排除捆绑包含有 OMIVV 设备日志记录信息，可用于帮助解决问题或将其发送给技术支持部门。OMIVV 不会记录任何用户敏感数据。

1. 在**支持**页面上，单击**创建并下载故障排除捆绑包**。  
此时将显示**故障排除捆绑包**对话框。
2. 在**故障排除捆绑包**对话框中，单击**创建**。  
根据日志的大小，创建捆绑包可能需要一些时间。
3. 要保存文件，请单击**下载**。

## 重设 iDRAC

重设 iDRAC 将执行正常的 iDRAC 重新引导操作。重设 iDRAC 后，iDRAC 通常会重新启动，但是主机不会重新启动。重设后，要过几分钟才能使用 iDRAC。仅当 OMIVV 设备上的 iDRAC 无响应时重设。

- 您只能在作为主机凭据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。
- Dell EMC 建议您将主机切换到维护模式，然后重设 iDRAC。
- 重设 iDRAC 后，如果 iDRAC 变得不可用或停止响应，则硬重置 iDRAC。有关硬重置的信息，请参阅 iDRAC 用户指南，网址为：  
<https://www.dell.com/support/>。

当 iDRAC 在重新引导时，您可能会看到：

- 在 OMIVV 检索主机运行状况时通信延迟。
- 当前已打开的与 iDRAC 的所有会话均会结束。
- iDRAC 的 DHCP 地址更改。如果 iDRAC 使用 DHCP 生成其 IP 地址，则 iDRAC IP 地址可能会更改。在这种情况下，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。

1. 在**支持**页面上，单击**重设 iDRAC**。
2. 在**iDRAC 重设**页面上，输入主机名或 IP 地址。
3. 要确认您了解 iDRAC 重设过程，请选择**我了解 iDRAC 重设的后果**。继续在所选主机上重设 iDRAC 复选框。
4. 单击**重设 iDRAC**。

## 有关事件和警报

在**设置**页面中，您可以启用主机和机箱的事件和警报、选择事件发布级别和恢复默认警报。您可以为每个 vCenter 配置事件和警报，或为所有已注册的 vCenter 配置事件和警报。与机箱对应的事件和警报与 vCenter 关联。

以下是四种事件发布级别：

**表. 8: 事件发布级别**

事件	说明
不发布任何事件	不允许 OMIVV 将任何事件或警报转发到其关联的 vCenter。
发布所有事件	向关联的 vCenter 发布所有事件（包括非正式的事件），OMIVV 从受管 Dell EMC 主机接收这些事件。建议选择 <b>发布所有事件</b> 选项作为事件发布级别。
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关联的 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后，严重硬件警报可触发 OMIVV 设备将主机系统置于维护模式。在某些情况下，将虚拟机迁移到另一个主机系统。OMIVV 将从受管主机收到的事件转发到 vCenter 并为这些事件创建警报。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。Dell EMC 建议在启用 Dell 警报之前启用 DRS。有关更多信息，请参阅 VMware 说明文件。

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 警报。详细的屏幕消息中列出 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。

如果您想要还原默认警报设置，请选择**还原警报**选项。此选项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，则那些更改可使用**还原警报**选项恢复。

**注：**要接收 Dell 事件，请确保您在 iDRAC、CMC 和 Management Controller 中启用了所需的事件。

**注：**OMIVV 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 EMC 警报，群集应使用 DRS 确保发送严重事件的虚拟机自动迁移。

## 配置事件和警报

要接收来自服务器的事件，请确保在 iDRAC 中设置 SNMP 陷阱目标。OMIVV 支持 SNMP v1 和 v2 警报。

1. 在 OMIVV 主页中，单击**设置 > vCenter 事件 > 事件和警报**。

2. 要针对所有主机及其机箱启用警报，请单击**针对所有主机及其机箱启用警报**。

**启用 Dell EMC 警报警告** 页面显示了启用 Dell EMC 警报后可能会受影响的群集和非群集主机。

**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。

**注：**在 vCenter 6.7 U1 和 6.7 U2 中，编辑选项失败。要编辑警报定义，建议使用 Web Client (FLEX)。

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

3. 要接受更改，请单击**继续**。  
所有主机及其机箱的警报均已启用。
4. 选择以下任何一个事件发布级别：
  - **不发布任何事件** — 不将任何事件或警报转发到其关联的 vCenter。
  - **发布所有事件** — 将所有事件（包括信息性事件和从受管主机和机箱接收的事件）发布到其关联的 vCenter。建议选择“发布所有事件”选项作为事件发布级别。
  - **仅发布严重和警告事件** — 仅将严重和警告级别事件发布到其关联的 vCenter。
  - **仅发布虚拟化相关事件** — 将从主机收到的虚拟化相关事件发布到其关联的 vCenter。虚拟化相关事件是运行虚拟机的主机最严重的事件。

5. 要保存更改，请单击**应用**。

要还原所有主机及其机箱的默认 vCenter 警报设置，请单击**还原警报**。可能需要片刻才能使更改生效。

**还原警报**选项是还原默认警报配置而无需卸载和重新安装产品的便捷方式。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**还原警报**选项恢复。

**注:** 在还原设备后，事件和警报设置未启用。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。

## 查看机箱事件

1. 在 vSphere Client 中，展开**菜单**，然后选择**主机和群集**。
2. 在左侧窗格中，选择 vCenter 实例。
3. 在右侧窗格中，单击**监测 > 任务和事件 > 事件**。
4. 要查看更多信息，请选择特定事件。

**注:** 对于具有 MCM 配置的 PowerEdge MX 机箱，事件源将显示为主机箱，但是消息详细信息包含成员机箱的服务标签以供识别身份。

## 查看机箱警报

1. 在 vSphere Client 中，展开**菜单**，然后选择**主机和群集**。
2. 在左侧窗格中，选择 vCenter 实例。
3. 在右侧窗格中，单击**监测 > 问题和警报 > 已触发警报**。
4. 在**已触发警报**中，单击警报名称以查看警报定义。

## 查看警报和事件设置

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。

1. 在 OMIVV 主页中，单击**设置 > 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](#) 页面上的 83。  
要查看事件发布级别，请参阅[有关事件和警报](#) 页面上的 83。

## 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。

与虚拟化相关的事件以下列格式显示：

Dell-Message ID:<ID 号>, Message:<消息说明>。

机箱事件以下列格式显示：

Dell-Message:<消息说明>, Chassis name:<机箱名称>, Chassis Service Tag:<机箱服务编号>, Chassis Location:<机箱位置>

**表. 9: 虚拟化事件**

事件名称	说明	严重性	建议操作
Dell-alertHWCAuditWarning	硬件配置警告	警告	无操作
Dell-alertHWCAuditInformation	硬件配置信息	信息	无操作
Dell-alertLiquidCoolingLeakInformational	之前在设备上检测到的较小漏洞现已解决	信息	无操作
Dell-alertLiquidCoolingLeakWarning	在设备上检测到较小漏洞	警告	无操作
Dell-alertLiquidCoolingLeakFailure	在设备上检测到较大漏洞	严重	断开输入电源，然后立即联系您的服务提供商。
Dell-alertStorageSoftwareDefinedSubSystemFailure	软件定义的存储子系统故障	严重	验证消息中标识的硬盘的运行状况，然后重试该操作。要在 iDRAC GUI 上检查运行状况，请在 iDRAC 仪表板上单击 <b>存储 &gt; 物理磁盘</b> 。在命令行界面 (CLI) 中运行以下 RACADM 命令： <code>racadm raid get pdisks -o -p status</code>  将更多物理驱动器添加到存储池，然后重试此操作。
Dell-alertStorageSoftwareDefinedSubSystemWarning	软件定义的存储子系统警告	警告	无操作
Dell-alertTemperatureProbeReadWarning	无法读取温度传感器	警告	无操作
Dell-alertTemperatureProbeChangeFailure	温度升高错误	严重	检查机箱事件日志中的风扇问题并修复存在的任何问题。如果未检测到风扇问题，请检查机箱环境温度并确保温度在操作范围内。要检查机箱环境温度，请运行以下 RACADM 命令： <code>racadm getsensorinfo</code> 。
Dell-当前传感器检测到警告值	指定系统中的电流传感器超过警告阈值	警告	无操作
Dell-当前传感器检测故障值	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-当前传感器检测无法恢复的值	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-冗余恢复	传感器已恢复正常值	信息	无操作
Dell-冗余降级	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

表. 9: 虚拟化事件 (续)

事件名称	说明	严重性	建议操作
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
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

表. 9: 虚拟化事件 (续)

事件名称	说明	严重性	建议操作
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
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

表. 9: 虚拟化事件 (续)

事件名称	说明	严重性	建议操作
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
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

表. 9: 虚拟化事件 (续)

事件名称	说明	严重性	建议操作
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
<b>iDRAC 事件</b>			
<p><b>注：</b> 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”。</p>			
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
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

表. 9: 虚拟化事件 (续)

事件名称	说明	严重性	建议操作
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)。
<b>机箱事件</b>			
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	警告	卸下并重新安装故障的风扇或安装其它风扇。

表. 9: 虚拟化事件 (续)

事件名称	说明	严重性	建议操作
	发生需要附加风扇的配置更改。		
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。

## 管理数据检索计划

### 计划资源清册作业

要查看 OMIVV 上的最新资源清册数据, 您必须计划定期运行资源清册作业, 以确保主机或机箱的资源清册信息保持最新状态。建议每周运行一次资源清册作业。

**注:** 机箱在 OMIVV 上下文中进行管理。机箱管理中没有 vCenter 上下文。在计划的主机资源清册完成后, 将会为使用 OMIVV 管理的所有机箱触发机箱资源清册。

**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。

1. 在 OMIVV 主页上, 单击**设置 > vCenter 设置 > 数据检索计划 > 资源清册检索**。
2. 选中**启用资源清册数据检索 (建议)** 复选框。

在具有多个 vCenter 服务器的 PSC 环境中, 如果单个 vCenter 的计划不同, 并且您选择**所有已注册的 vCenter** 选项以更新资源清册计划, 则资源清册计划设置页面将显示默认计划。

3. 选择资源清册数据检索日期和时间, 然后单击**应用**。

**注:** 在具有多个 vCenter 服务器的 PSC 环境中, 如果更新**所有已注册 vCenter** 的资源清册计划, 则更新将覆盖单个 vCenter 资源清册计划设置。

### 计划保修检索作业

1. 要更新授权密钥, 请确保您有权访问索引目录 (<https://downloads.dell.com/catalog/CatalogIndex.gz>)。
2. 要获得保修报告, 请确保您有权访问 <https://apigtwb2c.us.dell.com>。
3. 确保已针对主机和机箱成功运行资源清册。
4. 要使用 OMIVV 的保修功能, 您必须具有互联网连接。如果您的环境需要代理才能访问互联网, 请确保在管理员门户上配置代理设置。

从 Dell 在线检索硬件保修信息, 并由 OMIVV 显示。只有服务标签会通过 Dell 在线发送和存储。

在具有多个 vCenter 服务器的 PSC 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凭据配置文件中, 则保修不会自动运行。

**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。

1. 在 OMIVV 主页上, 单击**设置 > vCenter 设置 > 数据检索计划 > 保修检索**。
2. 选中**启用保修数据检索 (建议)** 复选框。

在具有多个 vCenter 服务器的 PSC 环境中，如果单个 vCenter 的计划不同，并且您选择**所有已注册的 vCenter** 选项以更新保修计划，则保修计划设置页面将显示默认计划。

3. 选择保修数据检索日期和时间，然后单击**应用**。

**i** **注：**在具有多个 vCenter 服务器的 PSC 环境中，如果更新**所有已注册 vCenter** 的保修计划，则更新将覆盖单个 vCenter 保修计划设置。

## 查看 Dell EMC 机箱信息

您可以使用 OMIVV 查看已查找到并进行资源清册的机箱信息。Dell EMC 机箱列出由 OMIVV 管理的所有机箱。

1. 在 OMIVV 主页中，单击**主机和机箱 > 机箱 > 机箱列表**。

此时会显示以下信息：

- **名称** — 显示每个 Dell EMC 机箱的 IP 地址链接。
- **运行状况** — 显示机箱的运行状况。

要按每个 Dell EMC 机箱的运行状况进行筛选，请单击搜索旁边显示的筛选器图标。

- **IP 地址/FQDN** — 显示 vCenter IP 地址。
- **服务标签** — 显示机箱的服务标签。
- **机箱 URL** — 显示机箱 URL。
- **型号** — 显示型号名称。
- **角色** — 仅适用于 MX 机箱。显示机箱的角色（主机箱或成员机箱）。
- **上次资源清册** — 显示上次资源清册信息。
- **可用插槽** — 显示机箱中的可用插槽。
- **配置文件名称** — 显示机箱关联的机箱凭据配置文件名称。
- **位置** — 显示机箱的位置。

如果未运行资源清册，将不会显示**名称**、**上次资源清册信息**、**可用插槽**、**配置文件名称**、**位置**和机箱资源清册的信息。

**注：**对于 MCM 配置中的 PowerEdge MX 机箱，使用主机箱管理整个 MCM 基础架构。如果禁用成员机箱 IP 和 iDRAC IP 并更改机箱角色，Dell EMC 建议移除现有主机箱并再次添加新的主机箱 IP，然后与机箱凭据配置文件相关联。

2. 选择一个机箱以查看固件、许可证类型和保修相关信息。

如果未运行资源清册，将不显示**名称**、**固件**、**许可证类型**和**保修**信息。

## 查看机箱资源清册信息

1. 在 **Dell EMC 机箱**页面上，选择一个机箱或单击“服务标签”。

2. 在**机箱信息**部分中，单击**查看**。

**概览**页面显示机箱的运行状况、活动错误、机箱的组件级运行状况状态、硬件概览和机箱关系（仅适用于 MX 机箱）。

**注：**对于 M1000e 4.3 版及更早版本，不会显示活动错误。

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**未知**。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 1.0 版及更高版本、M1000e 4.4 版及更高版本。对于低于 4.3 的 M1000e 固件版本，只显示两种运行状况标志，例如正常和警告或严重。

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。

## 查看机箱的硬件资源清册信息

您可以查看有关所选机箱的硬件资源清册的信息。

1. 在 OMIVV 主页中，单击**主机和机箱 > 机箱 > 机箱列表**。

此时会显示 **Dell EMC 机箱**页面。

2. 选择机箱，单击“服务标签”链接。

此时会显示**概览**页面。

- 在**概览**页面中，单击**硬件**。

**表. 10: 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	<ul style="list-style-type: none"> <li>在 <b>Dell EMC 机箱</b> 页面上，单击 <b>机箱 &gt; 机箱列表</b>，然后单击服务标签链接。</li> <li>在<b>概览</b>页面上，选择<b>硬件</b>。</li> <li>在右侧窗格中，展开<b>风扇</b>。</li> </ul> <p><b>或</b></p> <ul style="list-style-type: none"> <li>在<b>概览</b>页面中，单击<b>风扇</b>。</li> </ul>	<p>有关风扇的信息：</p> <ul style="list-style-type: none"> <li>名称</li> <li>存在</li> <li>标识符（仅适用于 MX 机箱）</li> <li>电源状态</li> <li>读数 (RPM)</li> <li>警告阈值（不适用于 MX 机箱）</li> <li>严重阈值（不适用于 MX 机箱） <ul style="list-style-type: none"> <li>最低</li> <li>最高</li> </ul> </li> <li>脉冲宽度调制（仅适用于 MX 机箱）</li> </ul> <p><b>i 注:</b> 在 PowerEdge MX 机箱中，即使从机箱中卸下风扇，风扇是否存在也会显示为“是”。但是，<b>摘要</b>页面上的风扇运行状况显示为<b>严重</b>，并存在主动错误。</p>
电源设备	<ul style="list-style-type: none"> <li>在 <b>Dell EMC 机箱</b> 页面上，单击 <b>机箱 &gt; 机箱列表</b>，然后单击服务标签链接。</li> <li>在<b>概览</b>页面上，选择<b>硬件</b>。</li> <li>在右侧窗格中，展开<b>电源设备</b>。</li> </ul> <p><b>或</b></p> <ul style="list-style-type: none"> <li>在<b>概览</b>页面中，单击<b>电源设备</b>。</li> </ul>	<p>有关电源设备的信息：</p> <ul style="list-style-type: none"> <li>名称</li> <li>容量</li> <li>存在</li> <li>电源状态</li> <li>输入电压（仅适用于 PowerEdge MX 机箱）。</li> </ul>
温度传感器	<ul style="list-style-type: none"> <li>在 <b>Dell EMC 机箱</b> 页面上，单击 <b>机箱 &gt; 机箱列表</b>，然后单击服务标签链接。</li> <li>在<b>概览</b>页面上，选择<b>硬件</b>。</li> <li>在右侧窗格中，展开<b>温度传感器</b>。</li> </ul> <p><b>或</b></p> <ul style="list-style-type: none"> <li>在<b>概览</b>页面中，单击<b>温度传感器</b>。</li> </ul>	<p>有关温度传感器的信息：</p> <ul style="list-style-type: none"> <li>位置</li> <li>读数</li> <li>警告阈值 <ul style="list-style-type: none"> <li>最高</li> <li>最低</li> </ul> </li> <li>严重阈值 <ul style="list-style-type: none"> <li>最高</li> <li>最低</li> </ul> </li> </ul> <p><b>i 注:</b> 对于 PowerEdge M1000e 机箱，将显示机箱温度的信息。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>
输入/输出模块	<ul style="list-style-type: none"> <li>在 <b>Dell EMC 机箱</b> 页面上，单击 <b>机箱 &gt; 机箱列表</b>，然后单击服务标签链接。</li> <li>在<b>概览</b>页面上，选择<b>硬件</b>。</li> <li>在右侧窗格中，展开<b>I/O 模块</b>。</li> </ul> <p><b>或</b></p> <ul style="list-style-type: none"> <li>在<b>概览</b>页面中，单击<b>I/O 模块</b>。</li> </ul>	<p>有关 I/O 模块的信息：</p> <ul style="list-style-type: none"> <li>插槽/位置</li> <li>存在</li> <li>名称</li> <li>结构</li> <li>服务标签</li> <li>电源状态</li> <li>角色</li> <li>固件版本</li> <li>硬件版本</li> </ul>

表. 10: 硬件资源清册信息 (续)

硬件资源清册：组件	通过 OMIVV 导航	信息
		<ul style="list-style-type: none"> <li>IP 地址</li> <li>子网掩码</li> <li>网关</li> <li>MAC 地址</li> <li>DHCP 已启用</li> </ul>
结构 (仅适用于 PowerEdge MX 机箱)	<ul style="list-style-type: none"> <li>在 <b>Dell EMC 机箱</b> 页面上, 单击 <b>机箱 &gt; 机箱列表</b>, 然后单击服务标签链接。</li> <li>在 <b>概览</b> 页面上, 选择 <b>硬件</b>。</li> <li>在右侧窗格中, 展开 <b>结构</b>。</li> </ul> <p><b>或</b></p> <ul style="list-style-type: none"> <li>在 <b>概览</b> 页面中, 单击 <b>结构</b>。</li> </ul>	<p>有关结构组件的信息：</p> <ul style="list-style-type: none"> <li>运行状况</li> <li>结构</li> <li>说明</li> <li>交换机计数</li> <li>计算计数</li> <li>上行链路计数</li> </ul> <p>要查看与结构关联的交换机, 请选择一个结构的组件, 并会在下部网格中显示以下信息：</p> <ul style="list-style-type: none"> <li>交换机</li> <li>机箱</li> <li>插槽</li> <li>机箱角色</li> <li>交换机型号</li> </ul>
PCIe	<ul style="list-style-type: none"> <li>在 <b>Dell EMC 机箱</b> 页面上, 单击 <b>机箱 &gt; 机箱列表</b>, 然后单击服务标签链接。</li> <li>在 <b>概览</b> 页面上, 选择 <b>硬件</b>。</li> <li>在右侧窗格中, 展开 <b>PCIe</b>。</li> </ul> <p><b>或</b></p> <ul style="list-style-type: none"> <li>在 <b>概览</b> 页面中, 单击 <b>PCIe</b>。</li> </ul>	<p>有关 PCIe 的信息：</p> <ul style="list-style-type: none"> <li>PCIe 插槽 <ul style="list-style-type: none"> <li>插槽</li> <li>名称</li> <li>电源状态</li> <li>结构</li> </ul> </li> <li>服务器插槽 <ul style="list-style-type: none"> <li>名称</li> <li>编号</li> </ul> </li> <li>插槽类型</li> <li>服务器映射</li> <li>分配状态</li> <li>分配的插槽电源</li> <li>PCI ID</li> <li>厂商 ID</li> </ul> <p><b>i</b>   <b>注:</b> PCIe 信息不适用于 M1000e 机箱。</p>
iKVM - 仅适用于 PowerEdge M1000e	<ul style="list-style-type: none"> <li>在 <b>Dell EMC 机箱</b> 页面上, 单击 <b>机箱 &gt; 机箱列表</b>, 然后单击服务标签链接。</li> <li>在 <b>概览</b> 页面的左窗格中, 选择 <b>硬件</b>。在右侧窗格中, 展开 <b>iKVM</b>。</li> </ul> <p><b>或</b></p> <ul style="list-style-type: none"> <li>在 <b>概览</b> 页面中, 单击 <b>iKVM</b>。</li> </ul>	<p>有关 iKVM 的信息：</p> <ul style="list-style-type: none"> <li>iKVM 名称</li> <li>存在</li> <li>固件版本</li> <li>前面板 USB/视频已启用</li> <li>允许访问 CMC CLI。</li> </ul> <p><b>i</b>   <b>注:</b> 仅当机箱包含 iKVM 模块时, 才会显示 iKVM 选项卡。</p>

## 查看固件资源清册信息

您可以查看有关所选机箱的固件相关信息。

1. 在 OMIVV 主页中，单击**主机和机箱 > 机箱 > 机箱列表**。  
此时会显示 **Dell EMC 机箱** 页面。
2. 选择机箱，单击“服务标签”链接。  
此时会显示**概览**页面。
3. 在**概览**页面上，单击**固件**。  
此时将显示有关固件的以下信息：
  - 组件
  - 当前版本在此页面上，您还可以启动 OpenManage Enterprise Modular 和 CMC。

## 查看管理控制器信息

您可以查看有关所选机箱的管理控制器相关信息。

1. 在 OMIVV 主页中，单击**主机和机箱 > 机箱 > 机箱列表**。  
此时会显示 **Dell EMC 机箱** 页面。
2. 选择机箱，单击“服务标签”链接。  
此时会显示**概览**页面。
3. 在**概览**页面上，单击**管理控制器**。  
此时会显示以下关于管理控制器的信息：
  - 常规
    - 名称
    - 固件版本
    - 上次更新时间
    - 机箱位置
    - 硬件版本
  - 公用网络
    - DNS 域名
    - 为 DNS 使用 DHCP
    - MAC 地址
    - 冗余模式
    - 硬件版本
  - IPv4 信息
    - IPv4 已启用
    - 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
  - IPv6 信息
    - IPv6 已启用
    - DHCP 已启用
    - IP 地址
    - 链路本地地址
    - 网关
    - 首选 DNS 服务器
    - 备用 DNS 服务器
  - 本地访问配置

- 快速同步硬件存在
- LCD 存在
- LED 指示灯存在
- KVM 已启用

**注：**属于 MCM 配置一部分的成员机箱的网络相关信息的一些属性不显示在**管理控制器**部分中。

## 查看存储资源清册信息

您可以查看有关所选机箱的存储相关信息。

1. 在 OMIVV 主页中，单击**主机和机箱 > 机箱 > 机箱列表**。  
此时会显示 **Dell EMC 机箱** 页面。
2. 选择机箱，单击“服务标签”链接。  
此时会显示**概览**页面。
3. 在**概览**页面上，单击**存储**。

此时将显示有关存储的以下信息：

- 虚拟磁盘
- 物理磁盘
- 控制器
- 机柜
- 热备盘

对于 MX 机箱，将会显示以下信息：

- 插槽号
- 插槽名称
- 型号
- 服务标签
- 固件版本
- 资产标签
- 电源状态
- 分配模式

对于 MX 机箱，如果您要查看有关驱动器的信息，请单击存储底座。以下驱动器信息会显示在下部窗格中：

- 运行状况
- 状态
- 插槽
- 插槽分配
- 磁盘名称
- 容量
- 总线协议
- 介质

如果 PowerEdge MX 机箱中的磁盘未分配，则其插槽分配显示为**不适用**。

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：

- 名称
- 型号
- 服务标签
- IP 地址（链接至存储设备）
- 结构
- 组名称
- 组 IP 地址（链接至存储组）。

**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。

## 查看保修信息

您可以查看有关所选机箱的保修相关信息。

1. 在 OMIVV 主页中，单击**主机和机箱 > 机箱 > 机箱列表**。  
此时会显示 **Dell EMC 机箱** 页面。
2. 选择机箱，单击“服务标签”链接。  
此时会显示**概览**页面。
3. 在**概览**页面中，单击**保修**。

有关保修的信息：

- 提供商
- 说明
- 状态
- 授权类型
- 开始日期
- 结束日期
- 剩余天数
- 上次更新

 **注：**要查看保修状态，请确保您运行保修作业。请参阅[计划保修检索作业](#) 页面上的 91。

## 查看机箱的关联主机

您可以查看有关所选机箱的相关主机的信息。

1. 在 OMIVV 主页中，单击**主机和机箱 > 机箱 > 机箱列表**。  
此时会显示 **Dell EMC 机箱** 页面。
2. 选择机箱，单击“服务标签”链接。  
此时会显示**概览**页面。
3. 在**概览**页面上，单击**相关主机**。  
此时会显示以下关于关联主机的信息：

- 主机名
- 服务标签
- 型号
- iDRAC IP
- 位置
- 插槽位置
- 上次资源清册

4. 要查看有关主机的详细信息，请选择主机。

## 查看相关的机箱信息

**机箱关系**部分显示以 MCM 模式部署的 MX 机箱中机箱之间的关系。

 **注：**相关的机箱信息仅适用于在 MCM 组中配置的 PowerEdge MX 机箱。

1. 在 OMIVV 主页中，单击**主机和机箱 > 机箱 > 机箱列表**。  
此时会显示 **Dell EMC 机箱** 页面。
2. 选择机箱，单击“服务标签”链接。  
此时会显示**概览**页面。

在**概览**页面上，**机箱关系**部分显示主机箱和成员机箱的所有关联机箱信息。

# 管理 PowerEdge MX 机箱

管理 MX7000X 机箱的方式不同于管理其他 Dell EMC 机箱（例如 M1000e、VRTX 和 FX2）。

您可以在具有管理模块的公共 IP 和 iDRAC IP 的独立模式中管理 MX 机箱。此外，您还可以在具有一个主机箱和多个成员机箱的多机箱管理 (MCM) 模式中配置 MX 机箱。

Dell EMC OpenManage Enterprise-Modular 支持有线 MCM 组。在有线类型中，机箱通过管理模块上的冗余端口进行菊花链式或有线连接。您选择用于创建组的机箱必须以菊花链方式连接到至少一个机箱。有关创建机箱组的更多信息，请参阅 *PowerEdge MX7000 的 Dell EMC OpenManage Enterprise-Modular 用户指南*，网址为：[dell.com/support](http://dell.com/support)。

您可以通过以下两种方式管理 MX 机箱中存在的服务器：

1. **使用主机凭据配置文件管理服务器**：推荐用于管理服务器的标准方式，在其中，所有功能都受支持。在这种情况下，仅当完成 MX 主机资源清册之后查找机箱。有关创建机箱凭据配置文件的更多信息，请参阅[创建主机凭据配置文件](#) 页面上的 35。
2. **管理使用机箱凭据配置文件的服务器**：如果您选择使用机箱凭据配置文件管理您的主机，将支持 OMIVV 功能（如资源清册、监测、固件和驱动程序更新）。有关使用机箱凭据配置文件管理机箱和主机的更多信息，请参阅[创建机箱凭据配置文件](#) 页面上的 39。

**注**：OMIVV 不支持管理使用备份主机箱配置的 PowerEdge MX 机箱。

**注**：如果禁用了 iDRAC 的 IPv4 地址，您可以选择使用机箱凭据配置文件来管理服务器。如果您使用机箱凭据配置文件管理服务器，则不支持以下 OMIVV 功能：

- iDRAC 锁定模式
- 能够将此服务器用作参考服务器，以捕获系统配置文件
- 操作系统部署
- 获得或更新 CSIOR 状态
- 服务器配置合规性
- 少量资源清册相关信息

**注**：具有公共 IPv4 iDRAC IP 的主机也可以使用机箱凭据配置文件进行管理。但是，不建议使用此方法，因为上述功能不受支持。

## 使用统一的机箱管理 IP 进行的机箱和主机管理

如果已针对使用主机凭据配置文件管理的主机禁用 iDRAC IPv4，则主机资源清册会失败，并且不能查找到机箱。在此类情况下，必须手动添加机箱并应该关联到机箱凭据配置文件，以管理机箱及其关联的主机。

如果您选择使用统一的机箱管理 IP 管理您的主机，将支持 OMIVV 功能（如资源清册、监测、固件和驱动程序更新）。以下是使用统一的机箱管理 IP 管理主机和机箱的任务的高级别描述：

1. 添加 MX 机箱。  
有关添加 MX 机箱的信息，请参阅[添加 PowerEdge MX 机箱](#) 页面上的 100。
2. 创建机箱凭据配置文件并关联主机。  
有关创建机箱凭据配置文件的更多信息，请参阅[创建机箱凭据配置文件](#) 页面上的 39。
3. 查看使用机箱凭据配置文件管理的机箱和主机的作业。
4. 查看机箱和主机资源清册。  
有关主机和机箱资源清册的更多信息，请参阅[查看主机资源清册作业](#) 页面上的 70 和 [查看机箱资源清册作业](#) 页面上的 72。
5. 在使用机箱管理的主机上执行固件更新。  
有关固件更新的更多信息，请参阅[固件更新](#) 页面上的 113。

**注**：当使用机箱管理主机时，不支持裸机工作流程。

## 添加 PowerEdge MX 机箱

可将具有有效 IPv4 iDRAC IP 的主机添加到主机凭据配置文件，并且在主机资源清册期间，将自动查找到关联的 MX 机箱并显示在 **Dell EMC 机箱** 页面上。

如果已针对主机禁用 iDRAC IPv4，则主机资源清册会失败，并且不能查找到机箱。在此类情况下，必须手动添加 MX 机箱并应该关联到机箱凭据配置文件，以管理机箱及其关联的主机。

要手动添加 MX 机箱，请执行以下操作：

1. 在 **OMIVV** 主页中，单击**主机和机箱 > 机箱**。
2. 在 **Dell EMC 机箱** 页面中，单击**添加 MX 机箱**。
3. 输入管理模块 IPv4 或 FQDN 或主机名，然后单击**确定**。

如果您输入 IP，则系统会验证该 IP 是否由 OMIVV 管理。

**i** **注：**使用主机名或 FQDN 添加机箱前，请确保在 DNS 中创建有效的正向和反向查询条目。

**i** **注：**如果您输入 FQDN，则会显示机箱 URL 及 FQDN。

机箱将添加到 **Dell EMC 机箱** 页面。

4. 通过创建机箱凭据配置文件使主机与机箱凭据配置文件关联。有关创建机箱凭据配置文件的更多信息，请参阅[创建机箱凭据配置文件](#) 页面上的 39。

**i** **注：**如果您输入的 IP 并非 MX 机箱 IP，则测试连接将会失败，并且无效的条目会保留在 **Dell EMC 机箱** 页面上。只有成功验证的机箱才会与机箱凭据配置文件相关联。

**i** **注：**如果主机在与添加的 MX 机箱关联的注册 vCenter 中不存在，则测试连接失败。

**i** **注：**对于在 MCM 配置中配置的 PowerEdge MX 机箱，主机箱和成员机箱必须具有相同的凭据。

## MX 机箱固件更新

在计划固件更新之前，请确保环境满足以下条件：

- 确保 MX 机箱是机箱凭据配置文件的一部分并已成功进行资源清册。
- 如果其任何主机正在进行固件更新，则无法更新机箱固件。

**i** **注：**通过使用 MX 机箱固件更新功能，您只能更新管理模块固件。

1. 在 OMIVV 主页上，单击**主机和机箱 > 机箱 > 机箱列表 > MX 机箱固件更新**。
2. 在向导的**机箱固件更新**页面中，阅读说明，然后单击**开始**。
3. 从 **MX 机箱列表**中，选择一个或多个 MX 机箱，然后单击**下一步**。

如果环境未满足以下任一条件，则不会显示机箱：

- 正在从 OMIVV 进行机箱固件更新。
- 没有为机箱创建机箱凭据配置文件。
- 机箱的资源清册不成功。

对于采用 MCM 配置的 PowerEdge MX 机箱，只能选择主要机箱。系统会自动选择成员机箱。


4. 在**选择更新源**页面中，执行以下操作：
  - a. 从下拉菜单中选择相应的固件存储库配置文件。
  - b. 根据所选的机箱和固件存储库配置文件，从标识的系统类别中选择相应的捆绑包。
5. 在**选择固件组件**页面上，选择需要更新的固件组件，然后单击**下一步**。

无法选择版本低于目录中可用版本或其处于相同级别（最新）的组件。要选择以降级状态列出的组件，请单击**允许固件降级**。

在与 MCM 配置关联的 PowerEdge MX 机箱中，即使未选中**允许固件降级**复选框，也可以降级固件版本。

不能只选择成员机箱来进行更新或降级。选择主机箱将自动选择成员机箱。

要选择所有页面上的所有固件组件，请单击 。

要清除所有页面上的所有固件组件，请单击 。

6. 在**计划作业**页面中，执行以下操作：
  - a. 输入固件更新作业的名称和说明。该说明是可选字段。  
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. 选择相应的计划选项以应用更新。
7. 在**查看摘要**页面中，查看固件更新摘要，然后单击**完成**。

**表. 11: 正在针对每个部署模式的并行 MX 机箱固件更新总数**

部署模式	并行机箱固件更新数量
小	1
中	1
大	2
特大	2

## 查看 OMIVV 主机

您可以在 **OMIVV 主机** 页面上查看所有 OMIVV 管理的主机。

1. 在 OMIVV 主页中，单击**主机和机箱** > **主机**。
2. 在 **OMIVV 主机** 选项卡中，查看以下信息：
  - **主机名** — 显示主机的 IP 地址。要查看主机信息，请选择主机。
  - **运行状况** — 显示主机的运行状况。  
要按每台 Dell EMC 主机的运行状况进行筛选，请单击搜索旁边显示的筛选器图标。
  - **vCenter** — 显示此主机的 vCenter IP 地址。
  - **群集** — 如果 Dell EMC 主机在群集里，则显示群集名称。
  - **主机凭据配置文件** — 显示主机凭据配置文件的名称。

## 监测单个主机

OMIVV 可让您查看单个主机的详细信息。您可以在**主机和群集**页面上查看所有 OMIVV 主机。要查看更多信息，请选择特定的 OMIVV 管理的主机，然后转到**监测** > **OMIVV 主机信息**。

## 查看主机摘要信息

您可以在**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。有两个 portlet 适用于 OMIVV。这两种 Portlet 分别是：

- **OMIVV 主机运行状况**
- **OMIVV 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：

1. 在 OMIVV 主页上，展开**菜单**，然后选择**主机和群集**。
2. 在左侧窗格中，选择特定主机。
3. 在右侧窗格中，单击**摘要**。
4. 向下滚动可查看 OMIVV Server Management Portlet。

您可以在 **OMIVV 主机信息** 和 **OMIVV 主机运行状况** 部分中查看以下信息。

表. 12: OMIVV 主机信息

信息	说明
服务标签	显示服务器的服务标签。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	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 PowerEdge 服务器。该 BIOS 属性的 4 个不同的值为：

表. 12: OMIVV 主机信息 (续)

信息	说明
	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> <li>空白：如果 BIOS 中的内存运行模式不受支持，将不显示 FRM 属性。</li> </ul>
系统锁定模式	显示 iDRAC 8 和更高版本服务器的 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	将显示以下项： <ul style="list-style-type: none"> <li>主机名 — 显示 OMIVV 管理主机的名称</li> <li>电源状态 — 显示电源是打开还是关闭。</li> <li>iDRAC IP — 显示 iDRAC IP 地址</li> <li>管理 IP — 显示管理 IP 地址</li> <li>主机凭据配置文件 — 显示此主机的主机凭据配置文件名称</li> <li>型号 — 显示 Dell EMC 服务器型号</li> <li>服务标签 — 显示服务器的服务标签。</li> <li>资产标签 — 显示的资产标签</li> <li>保修剩余天数 — 显示保修的剩余天数</li> <li>上次资源清册扫描 — 显示上次资源清册扫描的日期和时间</li> </ul>
虚拟机监控程序和固件	将显示以下项： <ul style="list-style-type: none"> <li>虚拟机监控程序 — 显示虚拟机监控程序版本</li> <li>BIOS 版本 — 显示 BIOS 版本</li> <li>远程访问卡版本 — 显示远程访问卡版本</li> </ul>
管理控制台	显示用于启动 Remote Access Console (iDRAC) 的链接。
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 <a href="#">设置闪烁指示灯</a> 页面上的 128。

表. 13: OMIVV 主机运行状况

信息	说明
OMIVV 主机运行状况	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 1.0 版及更高版本、M1000e 4.4 版及更高版本。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： <ul style="list-style-type: none"> <li>正常（绿色复选标记）— 组件正常运行。</li> <li>警告（带有感叹号的黄色三角形）— 组件有非严重错误。</li> <li>严重（红色 X）— 组件有严重故障。</li> <li>未知（问号）— 组件的状态未知。</li> </ul>

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。

**注：**对于具有有线 PSU 的主机或模块化服务器，电源监测信息将不可用。

## 查看 OMIVV 主机信息

您可以在 **OMIVV 主机信息**页面上查看有关所有 OMIVV 托管主机的硬件、存储、固件、电源监测、保修和系统事件日志信息。

1. 在 OMIVV 主页中，展开**菜单**，然后选择**主机和群集**。
2. 在左侧窗格中，选择一个主机，然后单击**监测 > OMIVV 主机信息**。

## 查看主机的硬件信息

表. 14: 单个主机的硬件信息

硬件：组件	信息
FRU	<ul style="list-style-type: none"> <li>• <b>部件名</b> — 显示 FRU 部件名。</li> <li>• <b>部件号</b> — 显示 FRU 部件号。</li> <li>• <b>制造商</b> — 显示制造商的名称。</li> <li>• <b>序列号</b> — 显示制造商的序列号。</li> <li>• <b>制造日期</b> — 显示制造日期。</li> </ul>
处理器	<ul style="list-style-type: none"> <li>• <b>插槽</b> — 显示插槽编号。</li> <li>• <b>速度</b> — 显示当前速度。</li> <li>• <b>品牌</b> — 显示处理器品牌。</li> <li>• <b>版本</b> — 显示处理器版本。</li> <li>• <b>核心</b> — 显示此处理器中内核的数量。</li> </ul>
电源设备	<ul style="list-style-type: none"> <li>• <b>类型</b> — 显示电源设备的类型。电源设备类型包括： <ul style="list-style-type: none"> <li>○ 未知</li> <li>○ 线性</li> <li>○ 切换</li> <li>○ 电池</li> <li>○ UPS</li> <li>○ 转换器</li> <li>○ 稳压器</li> <li>○ 交流</li> <li>○ 直流</li> <li>○ VRM</li> </ul> </li> <li>• <b>位置</b> — 显示电源设备的位置，比如插槽 1。</li> <li>• <b>输出 (瓦)</b> — 显示功率，以瓦特为单位。</li> </ul>
内存	<ul style="list-style-type: none"> <li>• <b>内存插槽</b> — 显示已使用、总计和可用内存计数。</li> <li>• <b>内存容量</b> — 显示已安装内存、总内存容量和可用内存。</li> <li>• <b>插槽</b> — 显示 DIMM 插槽。</li> <li>• <b>大小</b> — 显示内存大小。</li> <li>• <b>类型</b> — 显示内存类型。</li> </ul>
NIC	<ul style="list-style-type: none"> <li>• <b>总计</b> — 显示可用网络接口卡的总计数。</li> <li>• <b>名称</b> — 显示 NIC 名称。</li> <li>• <b>制造商</b> — 仅显示制造商名称。</li> <li>• <b>MAC 地址</b> — 显示 NIC MAC 地址。</li> </ul>
PCI 插槽	<ul style="list-style-type: none"> <li>• <b>PCI 插槽</b> — 显示已使用、总计和可用 PCI 插槽。</li> <li>• <b>插槽</b> — 显示插槽。</li> <li>• <b>制造商</b> — 显示 PCI 插槽的制造商名称。</li> </ul>

表. 14: 单个主机的硬件信息 (续)

硬件：组件	信息
	<ul style="list-style-type: none"> <li>● <b>说明</b> — 显示 PCI 设备的说明。</li> <li>● <b>类型</b> — 显示 PCI 插槽类型。</li> <li>● <b>宽度</b> — 显示数据总线宽度 (如果可用)。</li> </ul>
远程访问控制器	<ul style="list-style-type: none"> <li>● <b>IP 地址</b> — 显示远程访问卡的 IP 地址。 如果使用统一 IP 地址管理主机，则此部分中不会显示 iDRAC IP。</li> <li>● <b>MAC 地址</b> — 显示远程访问卡的 MAC 地址。</li> <li>● <b>RAC 类型</b> — 显示远程访问卡的类型。</li> <li>● <b>URL</b> — 显示与此主机关联的 iDRAC 的有效 URL。</li> </ul>

## 查看主机的存储信息

您可以查看虚拟磁盘、控制器、机柜和关联物理磁盘的计数，及全局热备份和专用热备份的计数。要查看有关每个存储组件的更多信息，请从**查看**下拉菜单中选择特定组件。

对于使用机箱进行管理的主机，未显示完整的存储信息（即控制器、机柜、全局热备用和专用热备用）。

**i** **注：** 使用机箱配置文件管理主机时，如果您单击**存储**，然后从**查看**下拉菜单中选择以下项目：

- **机柜** — 存储机柜的控制器 ID 显示为 0 而不是正确的控制器 ID。
- **物理磁盘** — HDD 的介质类型显示为**磁性驱动器**而不是**硬盘驱动器**。

表. 15: 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"> <li>● <b>名称</b> — 显示虚拟驱动器的名称。</li> <li>● <b>设备 FQDD</b> — 显示 FQDD。</li> <li>● <b>物理磁盘</b> — 显示虚拟驱动器所处的物理磁盘。</li> <li>● <b>容量</b> — 显示虚拟驱动器的容量。</li> <li>● <b>布局</b> — 显示虚拟存储设备的布局类型，这表示为此虚拟驱动器配置的 RAID 的类型。</li> <li>● <b>介质类型</b> — 显示 SSD 或 HDD。</li> </ul> <p>要查看条带大小、总线协议和高速缓存策略等信息，请选择虚拟磁盘。</p> <ul style="list-style-type: none"> <li>● <b>控制器 ID</b> — 显示控制器 ID。</li> <li>● <b>设备 ID</b> — 显示设备 ID。</li> <li>● <b>条带大小</b> — 显示条带大小，即每个条带在单个磁盘上所占的空间大小。</li> <li>● <b>总线协议</b> — 显示物理磁盘（包括在虚拟驱动器中）使用的技术。可能的值包括： <ul style="list-style-type: none"> <li>○ SCSI</li> <li>○ SAS</li> <li>○ SATA</li> </ul> </li> <li>● <b>默认读取策略</b> — 显示控制器支持的默认读取策略。选项包括： <ul style="list-style-type: none"> <li>○ 预读</li> <li>○ 不预读</li> <li>○ 自适应预读</li> <li>○ 读取高速缓存已启用</li> <li>○ 读取高速缓存已禁用</li> </ul> </li> <li>● <b>默认写入策略</b> — 显示控制器支持的默认写入策略。选项包括： <ul style="list-style-type: none"> <li>○ 回写式</li> <li>○ 强制回写</li> </ul> </li> </ul>

表. 15: 单个主机的存储设备详细信息 (续)

信息	说明
	<ul style="list-style-type: none"> <li>○ 回写已启用</li> <li>○ 直写</li> <li>○ 已保护启用的写入高速缓存</li> <li>○ 写入高速缓存已禁用</li> <li>● <b>高速缓存策略</b> — 显示是否已启用高速缓存策略。</li> </ul>
<p><b>物理磁盘</b></p> <p>当您从查看下拉菜单中选择此选项时，将显示筛选下拉列表。</p> <p>筛选中提供了以下选项：</p> <ul style="list-style-type: none"> <li>● <b>所有物理磁盘</b></li> <li>● <b>全局热备用</b></li> <li>● <b>专用热备用</b></li> <li>● 最后一个选项显示虚拟驱动器的自定义名称。</li> </ul>	<ul style="list-style-type: none"> <li>● <b>名称</b> — 显示物理磁盘的名称。</li> <li>● <b>设备 FQDD</b> — 显示设备 FQDD。</li> <li>● <b>容量</b> — 显示物理磁盘容量。</li> <li>● <b>磁盘状态</b> — 显示物理磁盘状态。选项包括： <ul style="list-style-type: none"> <li>○ 联机</li> <li>○ 就绪</li> <li>○ 降级</li> <li>○ 故障</li> <li>○ 脱机</li> <li>○ 正在重建</li> <li>○ 不兼容</li> <li>○ 已移除</li> <li>○ 已清除</li> <li>○ 检测到 SMART 警报</li> <li>○ 未知</li> <li>○ 外来</li> <li>○ 不受支持</li> </ul> </li> <li>● <b>已配置</b> — 显示是否已配置磁盘。</li> <li>● <b>热备用类型</b> (不适用于 PCIe) — 显示热备用类型。选项包括： <ul style="list-style-type: none"> <li>○ 否 — 没有热备用。</li> <li>○ 全局 — 未使用的备份磁盘，它是磁盘组的一部分</li> <li>○ 专用 — 已分配给单个虚拟磁盘的未使用备份磁盘。如果虚拟驱动器中的某个物理磁盘崩溃，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。</li> </ul> </li> <li>● <b>虚拟磁盘</b> — 显示虚拟驱动器的名称。</li> <li>● <b>总线协议</b> — 显示总线协议。</li> <li>● <b>控制器 ID</b> — 显示控制器 ID。</li> <li>● <b>介质类型</b> — 显示 SSD 或 HDD。</li> <li>● <b>剩余额定写入耐久性</b> — 显示 SSD 剩余写入耐久性。</li> <li>● <b>连接器 ID</b> — 显示连接器 ID。</li> <li>● <b>机柜 ID</b> — 显示机柜 ID。</li> <li>● <b>设备 ID</b> — 显示设备 ID。</li> <li>● <b>型号</b> — 显示物理存储磁盘的型号。</li> <li>● <b>部件号</b> — 显示存储设备部件号。</li> <li>● <b>序列号</b> — 显示存储设备序列号。</li> <li>● <b>供应商</b> — 显示存储设备供应商名称。</li> </ul>
<p><b>控制器</b></p>	<ul style="list-style-type: none"> <li>● <b>控制器 ID</b> — 显示控制器 ID。</li> <li>● <b>名称</b> — 显示控制器的名称。</li> <li>● <b>设备 FQDD</b> — 显示设备的 FQDD。</li> <li>● <b>固件版本</b> — 显示固件版本。</li> <li>● <b>所需最低固件</b> — 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。</li> <li>● <b>驱动程序版本</b> — 显示驱动程序版本。</li> <li>● <b>巡检读取模式</b> — 显示巡检读取模式。</li> <li>● <b>高速缓存大小</b> — 显示高速缓存大小。</li> </ul>

表. 15: 单个主机的存储设备详细信息 (续)

信息	说明
	<p><b>注:</b> 此部分显示芯片组控制器信息。此信息不会显示在 iDRAC UI 的存储控制器部分中，但您可以查看有关 iDRAC 的资源清册页面的此信息。</p>
机柜	<ul style="list-style-type: none"> <li>• <b>控制器 ID</b> — 显示控制器 ID。</li> <li>• <b>连接器 ID</b> — 显示连接器 ID。</li> <li>• <b>机柜 ID</b> — 显示机柜 ID。</li> <li>• <b>名称</b> — 显示机柜的名称。</li> <li>• <b>设备 FQDD</b> — 显示设备 FQDD。</li> <li>• <b>服务标签</b> — 显示服务标签。</li> </ul>

## 查看单个主机的固件信息

将显示以下与固件相关的信息：

- **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。

**注:** 使用机箱凭据配置文件管理主机时，固件资源清册数据将显示少数几个额外的组件，例如 Life Cycle Controller 和软件 RAID。

您可以在此页面上启动固件更新和配置系统锁定模式向导。

## 查看单个主机的电源监测信息

您可以查看诸如以下信息：常规信息、阈值、保留功率容量和能耗统计信息。

- **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

- **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
- **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
- **注:** 此处使用的主机时间是指主机所在位置的本地时间。

**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）。

**注:** 对于具有有线 PSU 的主机或模块化服务器，电源监测信息将不可用。

**注:** 对于使用机箱管理的主机，不会显示完整的电源监测信息。

## 查看单个主机的保修信息

要查看保修状态，请确保运行保修作业。请参阅[计划保修检索作业](#) 页面上的 91。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。

- **提供商** — 显示保修提供商的名称。
- **说明** — 显示说明
- **状态** — 显示主机的保修状态。状态选项包括：
  - **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 — OMIVV 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。
- **授权类型**—显示以下状态：
  - 初始
  - 已延长
  - 已过期
- **开始日期** — 显示保修开始日期。
- **结束日期** — 显示保修结束日期。
- **到期天数** — 显示保修剩余天数。
- **上次更新时间** - 上次更新保修的时间。

## 查看单个主机的系统事件日志信息

系统事件日志 (SEL) 提供由 OMIVV 查找到的硬件状态信息并显示以下信息：

- **状态** — 有多个状态图标，例如通知（蓝色感叹号）、警告（带有感叹号的黄色三角形）、错误（红色 X）和未知（带 ? 的框）。  
严重性级别定义如下：
  - 信息
  - 警告
  - 错误
- **时间（服务器时间）** - 表明事件发生的时间和日期。

要清除所有系统事件日志，请单击**清除日志**。此时将显示一条消息，指示日志数据在清除日志后无法恢复。

## 监测群集和数据中心中的主机

OMIVV 可让您查看有关数据中心或群集中的所有主机的详细信息。

### 查看 OMIVV 数据中心和群集信息

#### 查看数据中心和群集的概览

您可以查看诸如以下信息：数据中心或群集信息、系统锁定模式、硬件资源和保修信息。要查看有关此页面的信息，请确保成功完成资源清册。OMIVV 数据中心和群集视图直接报告来自 iDRAC 的数据。

1. 在 OMIVV 主页中，展开**菜单**，然后选择**主机和群集**。
2. 在左侧窗格中，选择一个数据中心或群集，然后单击**监测 > OMIVV 群集或数据中心信息**。
3. 要查看详细信息，请选择特定主机。

iDRAC IP、机箱 URL、CPU 和内存等信息将显示在页面最下面的水平窗格中。

**表. 16: 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"> <li>● 数据中心/群集名称</li> <li>● 受管主机的数量</li> <li>● 总能耗</li> </ul>
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"> <li>● 已打开电源</li> </ul>

表. 16: 数据中心和群集的概览 (续)

信息	说明
	<ul style="list-style-type: none"> <li>• 关闭</li> <li>• 不适用 (仅适用于基于 iDRAC9 的服务器)</li> </ul> <p>有关基于 iDRAC9 的服务器的列表, 请参阅兼容性值表。</p>
硬件资源	<p>将显示以下项:</p> <ul style="list-style-type: none"> <li>• 处理器总数</li> <li>• 内存总量</li> <li>• 虚拟磁盘容量</li> </ul>
保修摘要	<p>显示所选主机的保修状态。状态选项包括:</p> <ul style="list-style-type: none"> <li>• 已过期保修</li> <li>• 保修期内</li> <li>• 超出警告阈值</li> <li>• 超出严重阈值</li> <li>• 未知保修</li> </ul> <p>对于具有多种或不同保修 (例如 ND 和 4DP 等服务级别代码) 的主机或机箱, OMIVV 将根据保修天数最低的保修类型来考虑状态。</p>
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	<p>仅适用于基于 iDRAC9 的服务器: 显示主机的 iDRAC 锁定模式, 开启、关闭或未知。</p> <p>对于所有早于基于 iDRAC9 的 PowerEdge 服务器, 系统锁定模式将显示为<b>不适用</b>。有关基于 iDRAC9 的服务器的列表, 请参阅兼容性值表。</p>
iDRAC IP	显示 iDRAC IP 地址
服务控制台 IP	显示服务控制台 IP
CMC 或管理模块 URL	显示 CMC 或 Management Module URL, 即模块化服务器的机箱 URL, 或者它将显示“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
主机凭据配置文件	显示主机凭据配置文件的名称
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信息

表. 17: 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"> <li>• <b>主机</b> — 显示主机名。</li> <li>• <b>服务标签</b> — 显示主机的服务标签</li> <li>• <b>部件名</b> — 显示 FRU 部件名。</li> <li>• <b>部件号</b> — 显示 FRU 部件号。</li> <li>• <b>制造商</b> — 显示制造商名称。</li> <li>• <b>序列号</b> — 显示制造商的序列号。</li> <li>• <b>制造日期</b> — 显示制造日期。</li> </ul>
硬件：处理器	<ul style="list-style-type: none"> <li>• <b>主机</b> — 显示主机名。</li> <li>• <b>服务标签</b> — 显示主机的服务标签</li> <li>• <b>插槽</b> — 显示插槽编号。</li> <li>• <b>速度</b> — 显示当前速度。</li> <li>• <b>品牌</b> — 显示处理器品牌。</li> <li>• <b>版本</b> — 显示处理器版本。</li> <li>• <b>核心</b> — 显示此处理器中内核的数量。</li> </ul>
硬件：电源设备	<ul style="list-style-type: none"> <li>• <b>主机</b> — 显示主机名。</li> <li>• <b>服务标签</b> — 显示主机的服务标签</li> <li>• <b>类型</b> — 显示电源设备的类型。电源设备类型包括： <ul style="list-style-type: none"> <li>○ 未知</li> <li>○ 线性</li> <li>○ 切换</li> <li>○ 电池</li> <li>○ UPS</li> <li>○ 转换器</li> <li>○ 稳压器</li> <li>○ 交流</li> <li>○ 直流</li> <li>○ VRM</li> </ul> </li> <li>• <b>位置</b> — 显示电源设备的位置，比如插槽 1。</li> <li>• <b>输出 (瓦)</b> — 显示功率，以瓦特为单位。</li> <li>• <b>状态</b> — 显示电源设备状态。状态选项包括： <ul style="list-style-type: none"> <li>○ 其他</li> <li>○ 未知</li> <li>○ 确定</li> <li>○ 严重</li> <li>○ 不严重</li> <li>○ 可恢复</li> <li>○ 不可恢复</li> <li>○ 高</li> <li>○ 低</li> </ul> </li> </ul>
硬件：内存	<ul style="list-style-type: none"> <li>• <b>主机</b> — 显示主机名。</li> <li>• <b>服务标签</b> — 显示主机的服务标签</li> <li>• <b>插槽</b> — 显示 DIMM 插槽。</li> <li>• <b>大小</b> — 显示内存大小。</li> <li>• <b>类型</b> — 显示内存类型。</li> </ul>
硬件：NIC	<ul style="list-style-type: none"> <li>• <b>主机</b> — 显示主机名。</li> <li>• <b>服务标签</b> — 显示主机的服务标签</li> </ul>

表. 17: 数据中心和群集的硬件信息 (续)

硬件：组件	信息
	<ul style="list-style-type: none"> <li>● <b>名称</b> — 显示 NIC 名称。</li> <li>● <b>制造商</b> — 仅显示制造商名称。</li> <li>● <b>MAC 地址</b> — 显示 NIC MAC 地址。</li> </ul>
硬件：PCI 插槽	<ul style="list-style-type: none"> <li>● <b>主机</b> — 显示主机名。</li> <li>● <b>服务标签</b> — 显示主机的服务标签</li> <li>● <b>插槽</b> — 显示插槽。</li> <li>● <b>制造商</b> — 显示 PCI 插槽的制造商名称。</li> <li>● <b>说明</b> — 显示 PCI 设备的说明。</li> <li>● <b>类型</b> — 显示 PCI 插槽类型。</li> <li>● <b>宽度</b> — 显示数据总线宽度 (如果可用)。</li> </ul>
硬件：远程访问卡	<ul style="list-style-type: none"> <li>● <b>主机</b> — 显示主机名。</li> <li>● <b>服务标签</b> — 显示主机的服务标签</li> <li>● <b>IP 地址</b> — 显示远程访问卡的 IP 地址。</li> <li>● <b>MAC 地址</b> — 显示远程访问卡的 MAC 地址。</li> <li>● <b>RAC 类型</b> — 显示远程访问卡的类型。</li> <li>● <b>URL</b> — 显示与此主机关联的 iDRAC 的有效 URL。</li> </ul>

查看数据中心和群集的存储信息

表. 18: 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"> <li>● <b>主机</b> — 显示主机名。</li> <li>● <b>服务标签</b> — 显示主机的服务标签</li> <li>● <b>容量</b> — 显示物理磁盘容量。</li> <li>● <b>磁盘状态</b> — 显示物理磁盘状态。选项包括： <ul style="list-style-type: none"> <li>○ 联机</li> <li>○ 就绪</li> <li>○ 降级</li> <li>○ 故障</li> <li>○ 脱机</li> <li>○ 正在重建</li> <li>○ 不兼容</li> <li>○ 已移除</li> <li>○ 已清除</li> <li>○ SMART 警报检测</li> <li>○ 未知</li> <li>○ 外来</li> <li>○ 不受支持</li> </ul> </li> </ul> <p><b>注:</b> 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，位置如下 <a href="http://dell.com/support">dell.com/support</a></p> <ul style="list-style-type: none"> <li>● <b>型号</b> — 显示物理存储磁盘的型号。</li> <li>● <b>上次资源清册</b> — 显示已经运行的上次资源清册的日期、月份和时间。</li> <li>● <b>状态</b> — 显示主机状态。</li> <li>● <b>控制器 ID</b> — 显示控制器 ID。</li> <li>● <b>连接器 ID</b> — 显示连接器 ID。</li> <li>● <b>机柜 ID</b> — 显示机柜 ID。</li> <li>● <b>设备 ID</b> — 显示设备 ID。</li> <li>● <b>总线协议</b> — 显示总线协议。</li> </ul>

表. 18: 数据中心和群集的存储详细信息 (续)

存储：磁盘	说明
	<ul style="list-style-type: none"> <li>● <b>剩余额定写入耐久性</b> — 显示 SSD 剩余写入耐久性。</li> <li>● <b>热备用类型</b> (不适用于 PCIe) — 显示热备用类型。选项包括：                             <ul style="list-style-type: none"> <li>○ 否 — 没有热备用。</li> <li>○ 全局 — 未使用的备份磁盘，它是磁盘组的一部分</li> <li>○ 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</li> </ul> </li> <li>● <b>部件号</b> — 显示存储设备部件号。</li> <li>● <b>序列号</b> — 显示存储设备序列号。</li> <li>● <b>供应商名称</b> — 显示存储设备供应商名称。</li> </ul>
虚拟磁盘	<ul style="list-style-type: none"> <li>● <b>主机</b> — 显示主机的名称。</li> <li>● <b>服务标签</b> — 显示主机的服务标签</li> <li>● <b>名称</b> — 显示虚拟驱动器的名称。</li> <li>● <b>物理磁盘</b> — 显示虚拟驱动器所处的物理磁盘。</li> <li>● <b>容量</b> — 显示虚拟驱动器的容量。</li> <li>● <b>布局</b> — 显示虚拟存储设备的布局类型。这表示为此虚拟驱动器配置的 RAID 的类型。</li> <li>● <b>上次资源清册</b> — 显示上次运行资源清册操作的日期和时间。</li> <li>● <b>控制器 ID</b> — 显示控制器 ID。</li> <li>● <b>设备 ID</b> — 显示设备 ID。</li> <li>● <b>介质类型</b> — 显示 SSD 或 HDD。</li> <li>● <b>总线协议</b> — 显示物理磁盘 (包括在虚拟驱动器中) 使用的技术。可能的值包括：                             <ul style="list-style-type: none"> <li>○ SCSI</li> <li>○ SAS</li> <li>○ SATA</li> <li>○ PCIe</li> </ul> </li> <li>● <b>条带大小</b> — 显示条带大小，即每个条带在单个磁盘上所占的空间大小。</li> <li>● <b>默认读取策略</b> — 显示控制器支持的默认读取策略。选项包括：                             <ul style="list-style-type: none"> <li>○ 预读</li> <li>○ 不预读</li> <li>○ 自适应预读</li> <li>○ 读取高速缓存已启用</li> <li>○ 读取高速缓存已禁用</li> </ul> </li> <li>● <b>默认写入策略</b> — 显示控制器支持的默认写入策略。选项包括：                             <ul style="list-style-type: none"> <li>○ 回写式</li> <li>○ 强制回写</li> <li>○ 回写已启用</li> <li>○ 直写</li> <li>○ 已保护启用的写入高速缓存</li> <li>○ 写入高速缓存已禁用</li> </ul> </li> <li>● <b>磁盘高速缓存策略</b> — 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"> <li>○ 已启用—高速缓存 I/O</li> <li>○ 已禁用—直接 I/O</li> </ul> </li> </ul>

### 查看数据中心和群集的固件信息

此时会显示以下关于每个固件组件的信息：

- **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。

- **版本** — 显示此主机上所有固件的版本。

## 查看数据中心和群集电源监测信息

- **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。

## 查看数据中心和群集的保修信息

要查看保修状态，请确保运行保修作业。请参阅[计划保修检索作业](#) 页面上的 91。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。

- **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：
  - **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。

## 固件更新

OMIVV 使您能针对受管主机执行 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。不允许针对同一群集的两台主机运行并发固件更新。

**注:** 在多设备环境中，要在群集或主机上执行固件更新，请确保已加载使用目标 vCenter 注册的设备。

下面是执行固件更新的两种方法：

- **单个 DUP** - 通过直接指向 DUP 位置 ( CIFS 或 NFS )，为 iDRAC 或 BIOS 执行固件更新。单个 DUP 方法只能在主机级别使用。
- **存储库配置文件** — 执行固件和驱动程序更新。该方法可以在主机级别和群集级别使用。

下面是用于固件和驱动程序更新的存储库配置文件：

- **固件存储库** — 使用固件目录获取固件信息的存储库配置文件。

下面是固件存储库的两种类型：

- **用户创建的固件存储库**

- 出厂时创建的固件存储库：以下是两种类型的出厂创建的目录：出厂创建的目录不适用于 vSAN 群集固件更新和基线。
  - Dell 默认目录：出厂时创建的固件存储库配置文件，它使用 Dell EMC 联机目录获取最新的固件信息。如果设备没有互联网连接，请修改此存储库以指向基于 CIFS 或 NFS 或 HTTP 或 HTTPS 的本地共享。
  - 验证的 MX 堆栈目录：出厂时创建的固件存储库配置文件，它使用 Dell EMC 联机目录获取 MX 机箱及其相应底座的已验证固件信息。
- 驱动程序存储库 — 存储库配置文件包含可用于更新 vSAN 群集的驱动程序的脱机捆绑包。

固件更新向导始终检查 iDRAC 和 BIOS 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 和 BIOS 最低固件版本的更多信息，请参阅 *OpenManage Integration for VMware vCenter 兼容性值表*。版本满足最低需求，固件更新过程将允许更新所有固件版本，包括：iDRAC、RAID Controller、NIC、BIOS 等等。

**注：**要更新 PowerEdge XR2 服务器，OMIVV 使用 Dell 联机目录中提供的 R440 固件组件。如果您想要创建自定义目录（使用 DRM）以用于离线固件存储库以支持 PowerEdge XR2，请使用适用于 PowerEdge R440 服务器的固件组件。

## 更新 vSAN 主机上的固件和驱动程序

在计划更新 vSAN 主机（启用 vSAN 的群集中的主机）的固件之前，请确保环境满足以下条件：

- 确保主机符合要求（启用 CSIOR 且主机必须支持 ESXi 版本）、与主机凭据配置文件关联且已成功进行资源清册。
  - 在计划固件更新之前，检查以下前提条件：
    - DRS 已启用。
    - 主机未处于维护模式。
    - vSAN 数据对象运行良好。
- 要跳过前提条件检查，请清除**计划更新**页面上的**检查前提条件**复选框。
- 对于存储控制器、HDD 和 SSD 组件，所选存储库中的所选驱动程序和固件版本符合基于 vSAN 版本的 VMware vSAN 准则。
  - 对于驱动程序，OMIVV 仅支持在“VMware 硬件兼容性列表”中列出的脱机捆绑包。
  - 群集满足所选数据迁移选项的 vSAN 要求。如果 vSAN 群集不满足所选数据迁移选项的要求，则更新将超时。
  - Dell EMC 建议选择基线（群集配置文件）固件或驱动程序存储库。
  - 确保要更新的群集下没有任何主机存在活动的固件更新。
  - 确保您指定“进入维护模式”作业的必需超时值。如果等待时间超过所指定的时间，更新作业将会失败。但是，在重新引导主机时，可能会自动更新组件。
  - 启用 vSAN 后再重新运行资源清册。

固件更新过程中，Dell EMC 建议不要删除或移动以下内容：

- 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主机凭据配置文件。
- 存储库位于 CIFS 或 NFS 中。

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。验证之后，将会显示固件更新向导。

1. 要启动固件更新向导，请在 OMIVV 主页中，展开**菜单**，选择**主机和群集**，然后执行以下任一操作：
  - 右键单击一个主机，选择 **OpenManage 主机操作 > 固件更新**。
  - 选择一个主机，在右侧窗格中，选择 **监测 > OMIVV 主机信息 > 固件 > 运行固件向导**。
  - 选择一个主机，在右侧窗格中，选择 **摘要**，然后转至 **OMIVV 主机信息 > 主机操作 > 运行固件向导**。
2. 在**固件更新核对表**页面上，确保所有前提条件均已在计划更新之前进行验证，然后单击**开始**。
3. 在**更新源**页面上，选择下列任一选项：
  - **存储库配置文件**
  - **单个 DUP**
4. 要从一个文件加载单个固件更新，请选择**单个 DUP**。
  - a. 单个 DUP 可以驻留在 OMIVV 设备可访问的 CIFS 或 NFS 共享上：按以下格式之一输入文件位置，然后转到步骤 9。
    - NFS — <host>:/<share\_path/FileName.exe
    - CIFS — \\<host accessible share path>\<FileName>.exe

**注：**确保用于单个组件 DUP 的文件名不包含任何空格。

对于 CIFS 共享，OMIVV 会提示您输入可以访问共享驱动器的用户名和密码。

5. 如果您选择**存储库配置文件**选项，请选择固件和驱动程序存储库配置文件。

如果群集配置文件与主机所在的群集相关联，默认情况下，将选择关联的固件和驱动程序存储库配置文件。

如果您更改固件或驱动程序存储库配置文件，将显示一条消息，指示所选存储库配置文件未关联到基线，并且使用不同的存储库可能会影响基线比较。

**注**：如果同时有驱动程序和固件存储库与群集配置文件关联，则建议同时更新驱动程序和固件。

如果您不想更新固件或驱动程序，或者固件或驱动程序已是最新，请从下拉菜单中选择**未选择任何存储库**。

存储库配置文件选项中不显示默认固件目录（Dell EMC 默认目录和经验证的 MX 堆栈目录）。要使用存储库配置文件，请在 OMIVV 中创建自定义存储库。

要创建自定义存储库配置文件，请执行以下操作：

- a. 转至 Dell EMC Repository Manager (DRM) 并创建目录。

有关使用 DRM 创建目录的更多信息，请参阅 [使用 OMIVV 在 Dell EMC Repository Manager \(DRM\) 中创建目录](#) 页面上的 116。

- b. 下载目录及相应的文件。

- c. 使用下载的目录在 OMIVV 中创建存储库配置文件。

有关创建存储库配置文件的更多信息，请参阅 [创建存储库配置文件](#) 页面上的 42。

6. 根据您选择的固件存储库配置文件，选择相应的捆绑包，然后单击**下一步**。仅支持 64 位捆绑包。

7. 在**选择驱动程序组件**页面上，选择需要更新的驱动程序组件，然后单击**下一步**。当您选择某个驱动程序组件进行更新时，将选择软件包中的所有组件。

您可以使用过滤器选项基于特定的列名称过滤数据。

8. 在**选择固件组件**页面上，选择需要更新的固件组件，然后单击**下一步**。

显示基于重要程度状态（如紧急、建议、可选和降级）的组件数量。

无法选择版本低于目录中可用版本或其处于相同级别（最新）的组件或已计划进行更新的组件。要选择版本低于可用版本的组件，请选中**允许固件降级**复选框。

要选择所有页面上的所有固件组件，请单击 。

要清除所有页面上的所有固件组件，请单击 。

9. 在**划更新**页面中，输入固件更新作业的名称和说明。该说明是可选字段。

固件更新作业名称是必填项。如果清除了固件更新作业名称，可以重新使用它。

10. 在**其他设置**部分下，请执行以下操作：

- a. 输入介于 60-1440 分钟的维护模式超时值。如果等待时间超过所指定的时间，更新作业将会失败，并且输入维护任务将被取消或超时。但是，在重新引导主机时，可能会自动更新组件。

- b. 在**进入维护模式选项**下拉菜单中，选择相应的数据迁移选项。有关数据迁移选项的详细信息，请参阅 VMware 说明文件。

**注**：如果群集配置不支持完整数据迁移或存储容量不足，进入维护模式任务将会失败。

默认情况下，会选择以下选项：

- **固件更新完成后退出维护模式** — 如果禁用此选项，主机将保留在维护模式。
- **将已关闭和暂停的虚拟机移动到群集中的其他主机** — 如果禁用此选项，则会断开虚拟机的连接，直至主机设备联机。

- c. 如果您在更新固件时遇到问题，请选中**删除作业队列并重设 iDRAC**复选框。这可能可以成功完成更新过程。这将增加完成作业所需的整体更新时间，取消在 iDRAC 上计划的任何挂起作业或活动并重设 iDRAC。

对于使用机箱凭据配置文件进行管理的主机，不支持删除作业队列。

默认情况下，选择**检查前提条件**选项。

11. 在**更新计划**部分中，选择以下选项之一：

- **立即更新**
- **计划更新**
- **在下次重新引导时应用更新**

12. 在**查看摘要**页面上，查看固件更新信息，然后单击**完成**。

固件更新作业可能需要几个小时，具体取决于所选服务器的组件和数量。您可以在**作业**页面中查看作业的状态。

固件更新任务完成后，如果在**计划更新**页面中选择了相关选项，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。

## 使用 OMIVV 在 Dell EMC Repository Manager (DRM) 中创建目录

本节介绍了在 DRM 3.0 和更高版本中创建目录的流程。

1. 转至[下载 DRM](#) 并下载 DRM。
2. 在 DRM 主页上，单击**添加新存储库**。  
此时将显示**添加存储库**窗口。
3. 在**添加存储库**窗口中，执行以下操作：
  - a. 输入**存储库名称和说明**。
  - b. 从**基础目录**下拉菜单中，选择一个目录。
  - c. 从**集成类型**下拉菜单中，选择 **OpenManage Integration for VMware vCenter**。
4. 在 **OpenManage Integration for VMware vCenter** 窗口中，输入**虚拟设备 IP**、**vCenter 服务器 IP**、**用户名和密码**，并单击**连接**。  
已创建的目录将显示在主页页面上。
5. 要导出目录，请选择一个目录，然后单击**导出**。

## 更新 vSAN 群集上的固件和驱动程序

在计划固件更新之前，请确保环境满足以下条件：

- 确保主机符合要求（启用 CSIOR 且主机必须支持 ESXi 版本）、与主机凭据配置文件关联且已成功进行资源清册。如果未列出主机，请从 OMIVV 中主机的管理合规性向导，然后使用固件更新向导。
- 在计划固件更新之前，检查以下前提条件：
  - DRS 已启用。
  - 主机未处于维护模式。
  - vSAN 数据对象运行良好。
- 对于存储控制器、HDD 和 SSD 组件，确保所选存储库中的所选驱动程序和固件版本符合基于 vSAN 版本的 VMware vSAN 准则。
- 对于驱动程序，OMIVV 仅支持在“VMware 硬件兼容性列表”中列出的脱机捆绑包。
- 群集满足所选数据迁移选项的 vSAN 要求。如果 vSAN 群集不满足所选数据迁移选项的要求，则更新将超时。
- Dell EMC 建议选择基线（群集配置文件）固件或驱动程序存储库。
- 确保要更新的群集下没有任何主机存在活动的固件更新。
- 确保您指定“进入维护模式”作业的必需超时值。如果等待时间超过所指定的时间，更新作业将会失败。但是，在重新引导主机时，可能会自动更新组件。
- 确保您在启用 vSAN 后重新运行资源清册。

固件更新过程中，Dell EMC 建议不要删除或移动以下内容：

- 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主机的主机凭据配置文件。
- 存储库位于 CIFS 或 NFS 中。

 **注：**VMware 建议使用相同的服务器硬件创建群集。

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。验证之后，将会显示固件更新向导。

1. 要启动固件更新向导，请在 OMIVV 主页中，展开**菜单**，选择**主机和群集**，然后执行以下任一操作：
  - 右键单击一个主机，选择 **OpenManage 群集操作 > 固件更新**。
  - 选择一个群集，在右侧窗格中，选择**监测 > OMIVV 群集信息 > 固件 > 运行固件向导**。
2. 在**固件更新核对表**页面上，确保所有前提条件均已在计划更新之前进行验证，然后单击**开始**。
3. 在**更新源**页面上，选择固件和驱动程序存储库配置文件。  
如果群集配置文件与主机所在的群集相关联，默认情况下，将选择关联的固件和驱动程序存储库配置文件。  
如果您更改固件或驱动程序存储库配置文件，将显示一条消息，指示所选存储库配置文件未关联到基线，并且使用不同的存储库可能会影响基线比较。

**注:** 如果同时有驱动程序和固件存储库与群集配置文件关联, 则建议同时更新驱动程序和固件。

如果您不想更新固件或驱动程序, 或者固件或驱动程序已是最新, 请从下拉菜单中选择**未选择任何存储库**。

存储库配置文件选项中不显示默认固件目录 ( Dell EMC 默认目录和经验证的 MX 堆栈目录 )。要使用存储库配置文件, 请在 OMIVV 中创建自定义存储库。

要创建自定义存储库配置文件, 请执行以下操作:

a. 转至 Dell EMC Repository Manager (DRM) 并创建目录。

有关使用 DRM 创建目录的更多信息, 请参阅 [使用 OMIVV 在 Dell EMC Repository Manager \(DRM\) 中创建目录](#) 页面上的 116。

b. 下载目录及相应的文件。

c. 使用下载的目录在 OMIVV 中创建存储库配置文件。

有关创建存储库配置文件的更多信息, 请参阅 [创建存储库配置文件](#) 页面上的 42。

4. 根据您选择的固件存储库配置文件, 选择相应的捆绑包, 然后单击**下一步**。仅支持 64 位捆绑包。

**注:** 仅可为 OEM ( 无品牌 ) 服务器选择一个捆绑包, 即使它们属于不同型号也是如此。即使捆绑包不适用于一个或多个 OEM 服务器, 固件更新向导的“组件”页面也会列出每个 OEM 服务器或固件组件对。如果给定固件组件对的固件更新失败, 请使用针对 OEM 服务器显示的备用捆绑包重试。

5. 在**选择驱动程序组件**页面上, 选择需要更新的驱动程序组件, 然后单击**下一步**。当您选择某个驱动程序组件进行更新时, 将选择软件包中的所有组件。

您可以使用过滤器选项基于特定的列名称过滤数据。

6. 在**选择固件组件**页面上, 选择需要更新的固件组件, 然后单击**下一步**。

显示基于重要程度状态 ( 如紧急、建议、可选和降级 ) 的组件数量。

您可以使用过滤器选项基于特定的列名称过滤数据。

无法选择版本低于目录中可用版本或其处于相同级别 ( 最新 ) 的组件或已计划进行更新的组件。要选择版本低于可用版本的组件, 请选中**允许固件降级**复选框。

要选择所有页面上的所有固件组件, 请单击 。

要清除所有页面上的所有固件组件, 请单击 。

7. 在**划更新**页面中, 输入固件更新作业的名称和说明。该说明是可选字段。

固件更新作业名称是必填项。如果清除了固件更新作业名称, 可以重新使用它。

8. 在**其他设置**部分下, 请执行以下操作:

a. 输入介于 60-1440 分钟的维护模式超时值。如果等待时间超过所指定的时间, 更新作业将会失败, 并且输入维护任务将被取消或超时。但是, 在重新引导主机时, 可能会自动更新组件。

b. 在**进入维护模式选项**下拉菜单中, 选择相应的数据迁移选项。有关数据迁移选项的详细信息, 请参阅 VMware 说明文件。

**注:** 如果群集配置不支持完整数据迁移或存储容量不足, 进入维护模式任务将会失败。

默认情况下, **将已关闭和暂挂的虚拟机移动到群集中的其他主机**选项处于选中状态。禁用此选项会断开虚拟机的连接, 直到主机设备处于联机状态为止。

c. 如果您在更新固件时遇到问题, 请选中**删除作业队列并重设 iDRAC**复选框。这可能可以成功完成更新过程。这将增加完成作业所需的整体更新时间, 取消在 iDRAC 上计划的任何挂起作业或活动并重设 iDRAC。

对于使用机箱凭据配置文件进行管理的主机, 不支持删除作业队列。

9. 在**更新计划**部分中, 选择以下选项之一:

- **立即更新**
- **计划更新**

10. 在**查看摘要**页面上, 查看固件更新信息, 然后单击**完成**。

固件更新作业可能需要几个小时, 具体取决于所选服务器的组件和数量。您可以在**作业**页面中查看作业的状态。

固件更新任务完成后, 如果在**计划更新**页面中选择了相关选项, 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。

## 更新 vSphere 主机上的固件

在计划更新 vSphere 主机 ( 仅限 ESXi ) 的固件之前, 请确保环境满足以下条件:

- 确保主机符合要求（启用 CSIOR 且主机必须支持 ESXi 版本）、与主机凭据配置文件关联且已成功进行资源清册。
- DRS 已启用。

**i** 注: 对于独立的主机, DRS 检查不适用。

要跳过前提条件检查, 请清除**计划更新**页面上的**检查前提条件**复选框。

**i** 注: vSphere 群集和主机上不支持驱动程序更新。

固件更新过程中, Dell EMC 建议不要删除或移动以下内容:

- 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主机凭据配置文件。
- 存储库位于 CIFS 或 NFS 中。

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。验证之后, 将会显示固件更新向导。

1. 要启动固件更新向导, 请在 OMIVV 主页中, 展开**菜单**, 选择**主机和群集**, 然后执行以下任一操作:

- 右键单击一个主机, 选择 **OpenManage 主机操作 > 固件更新**。
- 选择一个主机, 在右侧窗格中, 选择**监测 > OMIVV 主机信息 > 固件 > 运行固件向导**。
- 选择一个主机, 在右侧窗格中, 选择**摘要**, 然后转至 **OMIVV 主机信息 > 主机操作 > 运行固件向导**。

2. 在**固件更新核对表**页面上, 确保所有前提条件均已在计划更新之前进行验证, 然后单击**开始**。

3. 在**更新源**页面上, 选择下列任一选项:

- **存储库配置文件**
- **单个 DUP**

4. 要从一个文件加载单个固件更新, 请选择**单个 DUP**。

a. 单个 DUP 可以驻留在可由 OMIVV 设备访问的 CIFS 或 NFS 共享上。按以下格式之一输入文件位置, 然后转至步骤 8。

- NFS — <host>:/<share\_path/FileName.exe
- CIFS — \\<host accessible share path>\<FileName>.exe

**i** 注: 确保用于单个组件 DUP 的文件名不包含任何空格。

对于 CIFS 共享, OMIVV 会提示您输入可以访问共享驱动器的用户名和密码。

5. 如果您选择**存储库配置文件**选项, 请选择固件存储库配置文件。

如果群集配置文件与主机所在的群集相关联, 默认情况下, 将选择关联的固件存储库。否则, 将选择 **Dell 默认目录**。

如果您更改固件存储库配置文件, 将显示一条消息, 指示所选存储库配置文件未关联到基线, 并且使用不同的存储库可能会影响基线比较。

6. 根据您选择的固件存储库配置文件, 选择相应的捆绑包, 然后单击**下一步**。仅支持 64 位捆绑包。

7. 在**选择固件组件**页面上, 选择需要更新的固件组件, 然后单击**下一步**。

显示基于重要程度状态 (如紧急、建议、可选和降级) 的组件数量。

您可以使用过滤器选项基于特定的列名称过滤数据。

无法选择版本低于目录中可用版本或其处于相同级别 (最新) 的组件或已计划进行更新的组件。要选择版本低于可用版本的组件, 请选中**允许固件降级**复选框。

要选择所有页面上的所有固件组件, 请单击 。

要清除所有页面上的所有固件组件, 请单击 。

8. 在**划更新**页面中, 输入固件更新作业的名称和说明。该说明是可选字段。

固件更新作业名称是必填项。如果清除了固件更新作业名称, 可以重新使用它。

9. 在**其他设置**部分下, 请执行以下操作:

a. 输入介于 60-1440 分钟的维护模式超时值。如果等待时间超过所指定的时间, 更新作业将会失败, 并且输入维护任务将被取消或超时。但是, 在重新引导主机时, 可能会自动更新组件。

默认情况下, 会选择以下选项:

- **固件更新完成后退出维护模式** — 如果禁用此选项, 主机将保留在维护模式。
- **将已关闭和暂挂的虚拟机移动到群集中的其他主机** — 如果禁用此选项, 则会断开虚拟机的连接, 直至主机设备联机。

- b. 如果您在更新固件时遇到问题，请选中**删除作业队列并重设 iDRAC** 复选框。这可能可以成功完成更新过程。这将增加完成作业所需的整体更新时间，取消在 iDRAC 上计划的任何挂起作业或活动并重设 iDRAC。

对于使用机箱凭据配置文件进行管理的主机，不支持删除作业队列。

默认情况下，选择**检查前提条件**选项。

10. 在**更新计划**部分中，选择以下选项之一：

- **立即更新**
- **计划更新**
- **在下次重新引导时应用更新**
- **在不进入维护模式的情况下，应用更新并强制重新引导**

11. 在**查看摘要**页面上，查看固件更新信息，然后单击**完成**。

固件更新作业可能需要几个小时，具体取决于所选服务器的组件和数量。您可以在**作业**页面中查看作业的状态。

固件更新任务完成后，如果在**计划更新**页面中选择了相关选项，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。

## 更新 vSphere 群集上的固件

在计划固件更新之前，请确保环境满足以下条件：

- 确保主机符合要求（启用 CSIOR 且主机必须支持 ESXi 版本）、与主机凭据配置文件关联且已成功进行资源清册。如果未列出主机，请从 OMIVV 中主机的管理合规性向导，然后使用固件更新向导。
- DRS 已启用。
- 确保要更新的群集下没有任何主机存在活动的固件更新。
- 确保您指定“进入维护模式”作业的必需超市值。如果等待时间超过所指定的时间，更新作业将会失败。但是，在重新引导主机时，可能会自动更新组件。

**注：**vSphere 群集和主机上不支持驱动程序更新。

固件更新过程中，Dell EMC 建议不要删除或移动以下内容：

- 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主机的主机凭据配置文件。
- 存储库位于 CIFS 或 NFS 中

**注：**VMware 建议使用相同的服务器硬件创建群集。

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。验证之后，将会显示固件更新向导。

1. 要启动固件更新向导，请在 OMIVV 主页中，展开**菜单**，选择**主机和群集**，然后执行以下任一操作：

- 右键单击一个主机，选择 **OpenManage 群集操作 > 固件更新**。
- 选择一个群集，在右侧窗格中，选择**监测 > OMIVV 群集信息 > 固件 > 运行固件向导**。

2. 在**固件更新核对表**页面上，确保所有前提条件均已在计划更新之前进行验证，然后单击**开始**。

3. 在**更新源**页面上，如果群集配置文件与主机所在的群集相关联，默认情况下，将选择关联的固件存储库。否则，将选择 **Dell 默认目录**。

如果您更改固件存储库配置文件，将显示一条消息，指示所选存储库配置文件未关联到基线，并且使用不同的存储库可能会影响基线比较。

4. 根据您选择的固件存储库配置文件，选择相应的捆绑包，然后单击**下一步**。仅支持 64 位捆绑包。

**注：**仅可为 OEM（无品牌）服务器选择一个捆绑包，即使它们属于不同型号也是如此。即使捆绑包不适用于一个或多个 OEM 服务器，固件更新向导的“组件”页面也会列出每个 OEM 服务器或固件组件对。如果给定固件组件对的固件更新失败，请使用针对 OEM 服务器显示的备用捆绑包重试。

5. 在**选择固件组件**页面上，选择需要更新的固件组件，然后单击**下一步**。

显示基于重要程度状态（如紧急、建议、可选和降级）的组件数量。

无法选择版本低于目录中可用版本或其处于相同级别（最新）的组件或已计划进行更新的组件。要选择版本低于可用版本的组件，请选中**允许固件降级**复选框。

您可以使用过滤器选项基于特定的列名称过滤数据。

要选择所有页面上的所有固件组件，请单击 。

要清除所有页面上的所有固件组件，请单击 。

6. 在**划更新**页面中，输入固件更新作业的名称和说明。该说明是可选字段。  
固件更新作业名称是必填项。如果清除了固件更新作业名称，可以重新使用它。
7. 在**其他设置**部分下，请执行以下操作：
  - a. 输入介于 60-1440 分钟的维护模式超时值。如果等待时间超过所指定的时间，更新作业将会失败，并且输入维护任务将被取消或超时。但是，在重新引导主机时，可能会自动更新组件。  
默认情况下，**将已关闭和暂挂的虚拟机移动到群集中的其他主机**选项处于选中状态。禁用此选项会断开虚拟机的连接，直到主机设备处于联机状态为止。
  - b. 如果您在更新固件时遇到问题，请选中**删除作业队列并重设 iDRAC** 复选框。这可能可以成功完成更新过程。这将增加完成作业所需的整体更新时间，取消在 iDRAC 上计划的任何挂起作业或活动并重设 iDRAC。  
对于使用机箱凭据配置文件进行管理的主机，不支持删除作业队列。
8. 在**更新计划**部分中，选择以下选项之一：
  - **立即更新**
  - **计划更新**
9. 在**查看摘要**页面上，查看固件更新信息，然后单击**完成**。  
固件更新作业可能需要几个小时，具体取决于所选服务器的组件和数量。您可以在**作业**页面中查看作业的状态。  
固件更新任务完成后，如果在**计划更新**页面中选择了相关选项，资源清单会在所选主机上自动运行，且主机会自动退出维护模式。

## 更新相同的固件组件类型

下面是更新相同类型固件组件时需要记住的要点：

- 如果服务器中存在类型相同且版本相同的多个组件，则**选择固件组件**页面上只会显示该组件的一个版本。更新将应用到所有组件，并且仅针对组件的一个版本显示偏移详细信息。

例如，

**表. 19: 服务器中存在类型相同的多个组件的示例**

组件	当前版本	可用版本
HDD1	V1	V3
HDD2	V1	V3
HDD3	V1	V3

在这种情况下，**选择固件组件**页面会显示以下消息：

**表. 20: 服务器中存在版本相同的多个组件的示例**

组件	当前版本	可用版本
HDD1	V1	V3

- 如果服务器中存在类型相同但版本不同的多个组件，则将针对每个唯一的版本显示单个组件。在这种情况下，如果您选择了任何一个组件，则更新将应用到所有组件，而不考虑其当前固件版本。无论所有组件的当前固件版本如何，都会显示偏移详细信息。

例如，

**表. 21: 服务器中存在版本不同的多个组件的示例**

组件	当前版本	可用版本
HDD1	V1	V3
HDD2	V2	V3
HDD3	V2	V3

在这种情况下，**选择固件组件**页面会显示以下消息：

**表. 22: 服务器中存在版本不同的多个组件的示例**

组件	当前版本	可用版本
HDD1	V1	V3
HDD2	V2	V3

- 如果目录中包含多个可用版本，则建议仅选择组件类型的其中一个可用版本。然后，所选固件将应用到所有适用的组件，而不考虑其当前版本。

例如，

**表. 23: 目录中有多个可用版本的示例**

组件	当前版本	可用版本
HDD1	V1	V3
HDD2	V2	V3
HDD3	V2	V3
HDD1	V1	V4
HDD2	V2	V4
HDD3	V2	V4

在这种情况下，**选择固件组件**页面会显示以下消息：

**表. 24: 目录中有多个可用版本的示例**

组件	当前版本	可用版本
HDD1	V1	V3
HDD2	V2	V3
HDD1	V1	V4
HDD2	V2	V4

## vSphere 生命周期管理器概览

vSphere 生命周期管理器是一种在 vCenter 服务器中运行的服务（适用于 vCenter 7.0 及更高版本）。

vSphere 生命周期管理器允许您创建包含 ESXi 映像、固件和驱动程序的基线映像。通过执行法规遵从性检查，将确保群集中的每个主机都与基线映像对齐。如果有任何非法法规遵从性，则提供修复群集的选项。

在 vSphere 生命周期管理器中，OMIVV 充当固件加载项提供程序。有关 vSphere 生命周期管理器的更多信息，请参阅 VMware 说明文件。

要将 vSphere 生命周期管理器与 OMIVV 配合使用，必须进行 vCenter 注册。有关注册 vCenter 和 vSphere 生命周期管理器的详细信息，请参见[注册新 vCenter 服务器](#) 页面上的 12。

您可以在 vCenter 注册期间在 Dell EMC 管理控制台中注册 vSphere 生命周期管理（适用于 vCenter 7.0 及更高版本）。vCenter 注册成功后，您可以在 Dell EMC 管理控制台的 **VCENTER 注册** 页面上修改（注册或取消注册）vSphere 生命周期管理器的注册状态。有关更多信息，请参见在 [Dell EMC 管理控制台中注册 vSphere 生命周期管理器](#) 页面上的 122 和在 [Dell EMC 管理控制台中注销 vSphere 生命周期管理器](#) 页面上的 122。

## 在 Dell EMC 管理控制台中查看 vSphere 生命周期管理器状态

以下是可以在 **vSphere 生命周期管理器** 列中查看的 vSphere 生命周期管理器状态：

- **注册**（仅适用于 vCenter 7.0 及更高版本）— 在未注册 vSphere 生命周期管理器时显示。
- **取消注册**（仅适用于 vCenter 7.0 及更高版本）— 在已注册 vSphere 生命周期管理器时显示。
- **不适用** — 仅当注册的 vCenter 早于版本 7.0 时才显示。如果将 vCenter 升级到 7.0，状态仍为**不适用**。要反映应有状态，请重新启动 OMIVV 设备。

## 在 Dell EMC 管理控制台中注册 vSphere 生命周期管理器

vCenter 必须是 7.0 及更高版本。

1. 转至 <https://<ApplianceIP/hostname/>>。
2. 在 **VCENTER 注册** 页面上的 **vSphere 生命周期管理器** 下，单击 **注册**。  
将显示 **注册 VSPHERE 生命周期管理器** <vCenter 名称> 对话框。
3. 单击 **注册 vSphere 生命周期管理器**。  
将显示一则消息，指示成功注册了 vSphere 生命周期管理器。

## 在 Dell EMC 管理控制台中注销 vSphere 生命周期管理器

vCenter 必须是 7.0 及更高版本。

1. 转至 <https://<ApplianceIP/hostname/>>。
2. 在 **VCENTER 注册** 页面上的 **vSphere 生命周期管理器** 下，单击 **注销**。  
将显示 **注销 VSPHERE 生命周期管理器** <vCenter 名称> 对话框。
3. 单击 **注销**。  
将显示确认消息，指示成功取消注册了 vSphere 生命周期管理器。**DellEMC OMIVV** 将从 vSphere 生命周期管理器中的 **硬件支持管理器** 列表中删除。不会影响任何 OMIVV 功能。

## 使用 vSphere 生命周期管理器管理群集

**前提条件：**

使用 vSphere 生命周期管理器管理群集之前，请确保：

- 在 Dell EMC 管理控制台中启用了 vSphere 生命周期管理器。有关更多信息，请参阅 [在 Dell EMC 管理控制台中注册 vSphere 生命周期管理器](#) 页面上的 122。
- 群集中的主机符合管理要求。有关更多信息，请参阅 [管理合规性](#) 页面上的 62。
- 已为所选群集创建群集配置文件，并且群集配置文件与 OMIVV 中的固件存储库相关联。有关群集配置文件的更多信息，请参阅 [创建群集配置文件](#) 页面上的 45。

您可以在 vSphere 生命周期管理器中使用用户界面或 vSphere Automation API 管理群集。OMIVV 支持使用用户界面和 vSphere Automation API 管理群集。

 **注：**您可以在 vSphere 生命周期管理器管理的群集中使用 OMIVV 群集操作，例如系统锁定和固件更新，但这可能会影响基线报告。

## 在 vSphere 生命周期管理器中使用 OMIVV 作为固件加载项提供程序 — 用户界面

您可以将 OMIVV 与 vSphere 生命周期管理器结合使用，以作为固件加载项提供程序。

在 vSphere 生命周期管理器环境中，群集配置文件称为硬件支持包 (HSP)。在 OMIVV 中创建的群集配置文件在 vSphere 生命周期管理器中被选为 **固件和驱动程序加载项**。有关群集配置文件的更多信息，请参阅 [群集配置文件](#) 页面上的 45。

要为所选群集设置映像并将 OMIVV 关联为 **固件和驱动程序加载项**，请执行以下任务：

1. 在 vSphere Client 中，单击 **主机和群集**，然后选择要使用映像进行管理的群集。
2. 在 **更新** 页面的左侧窗格中，展开 **主机**，然后单击 **映像**。
3. 要选择固件和驱动程序加载项，请单击“选择”图标。  
**选择固件和驱动程序加载项** 页面将显示。
4. 在 **选择硬件支持管理器** 部分中，选择 **DellEMC OMIVV**。  
选择 **DellEMC OMIVV** 后，与固件存储库关联且连接到所选 vCenter 中的群集的所有群集配置文件都将列在 **选择固件和驱动程序加载项** 部分中。
5. 选择适用于所选群集的群集配置文件，然后单击 **选择**。  
要识别与所选群集关联的群集配置文件，请参阅群集配置文件中的说明。

**注:** 如果您尚未在 OMIVV 中创建任何群集配置文件，则会显示一个空列表。有关创建群集配置文件的更多信息，请参阅[创建群集配置文件](#) 页面上的 45。

- **加载项版本** — 指示群集配置文件的当前版本。如果群集配置文件已修改或版本在 OMIVV 中增加，请确保您在 vSphere 生命周期管理器中使用最新版本的群集配置文件。
  - 注:** 有时，vSphere 生命周期管理器会显示固件的不合规性。但是，vSphere 生命周期管理器中未列出不合规的固件。要解决此问题，请修复群集。修正群集不会导致 vSphere 生命周期管理器重新启动。
- **支持的 ESXi 版本** — 指明 OMIVV 支持的 ESXi 版本 (7.0.0)。

所选群集配置文件在[更新](#)页面上显示为固件加载项。

#### 6. 单击保存。

vSphere 生命周期管理器执行群集合规性检查。法规遵从性检查结果显示在 vSphere 生命周期管理器的[映像合规性](#)部分中。

总体合规性包含软件合规性和固件合规性。OMIVV 管理 vSphere 生命周期管理器任务的固件合规性部分。

## 查看群集合规性状态

以下是每个主机的可能固件合规性状态：

- **符合**：在主机上安装的所有固件组件的固件版本与 OMIVV 中群集配置文件中存在的固件版本相同时显示。
  - **不合规**：在主机上安装的一个或多个固件版本与 OMIVV 中的群集配置文件中的固件版本不同时显示。
    - 注:** 升级 OMIVV 设备后，对于使用旧版本的 OMIVV 创建的映像，vSphere 生命周期管理器检查合规性任务失败。要解决此问题，请使用最新版本的硬件支持包 (HSP) 保存映像。
  - **不兼容**：在以下情况下显示：
    - 在 vCenter 中选择的群集未与所选[驱动程序和固件加载项](#)（OMIVV 中的群集配置文件）相关联。
    - 如果在为所选群集保存 vSphere 生命周期管理器映像后更新了群集配置文件中的固件存储库。
  - **未知**：如果 OMIVV 中的主机未成功进行资源清册，则显示。有关更多信息，请参阅[主机凭据配置文件](#) 页面上的 35。
- 注:** 您可能会看到 OMIVV 与 vSphere 生命周期管理器偏移报告之间存在不匹配。这是因为 vSphere 生命周期管理器始终显示实时偏移报告，而 OMIVV 会显示基于安排的日期和时间的偏移报告。如果在偏移报告之间看到不匹配，请在 OMIVV 的[偏移检测作业](#)页面上按需运行偏移检测作业。

## 解决群集合规性问题

1. 如果主机状态为**合规**，则不需要对该主机执行任何进一步操作。
2. 如果主机状态为**不合规**，请继续进行修复操作。有关更多信息，请参阅[vSphere 生命周期管理器中的修复](#) 页面上的 124。
3. 如果主机状态**不兼容**，请执行以下操作：
  - a. 确保 vCenter 中的所选群集与群集配置文件关联。在 vSphere 生命周期管理器中选择与[固件和驱动程序加载项](#)相同的群集配置文件。
  - b. 编辑 vSphere 生命周期管理器映像并重新选择更新后的群集配置文件（固件和驱动程序加载项），然后保存映像。
4. 如果主机状态为**未知**，请确保主机已添加到 OMIVV 中的主机凭据配置文件中并且资源清册已成功运行。

## 硬件兼容性检查

vSphere 生命周期管理器提供了一个选项，用于在执行固件修复之前为 vSAN 群集执行硬件兼容性检查。硬件兼容性检查会将映像中列出的固件和驱动程序与 vSAN 硬件兼容性列表 (HCL) 中所列的硬件和支持的驱动程序进行比较。vSphere 生命周期管理器仅为存储控制器（PCIe 设备）执行硬件兼容性检查。有关支持的固件列表，请在 vSphere Client 中，转至[监控 > vSAN > Skyline 运行状况](#)。

要执行硬件兼容性检查，请在[映像合规性](#)部分中，单击[检查合规性](#)。

执行硬件兼容性检查时，OMIVV 会返回群集配置文件中存在的固件版本。

如果固件版本与硬件兼容性列表 (HCL) 中列出的固件兼容，vSphere 生命周期管理器会将合规性状态显示为**兼容**。有关合规性状态的详细信息，请参阅 VMware 说明文件。

硬件兼容性检查结果将显示在[硬件兼容性](#)页面上。

## 运行修复预检查

预检查操作将针对群集中的每个主机执行各种检查，以确保群集已准备好进行固件修复。

预检查是可在主机或群集级别执行的可选任务。

您可以跳过预检查操作，vSphere 生命周期管理器会在修复期间执行预检查。

作为预检查的一部分，OMIVV 将对以下项执行前提条件检查：

- iDRAC 可访问性
- iDRAC 锁定模式
- 从 OMIVV 为所选群集和任何主机触发的固件更新作业（如果有）的状态
- 已启用重新引导时收集系统资源清册 (CSIOR)。
- 连接到固件存储库和所需的固件组件。

要验证固件修复的前提条件，请单击**运行预检查**。

预检查任务状态和结果显示在**映像合规性**部分中。

如果任何主机的预检查失败，请修复相应问题，然后重新运行预检查或继续执行修复任务。

## vSphere 生命周期管理器中的修复

在**映像合规性**部分中，您可以一次修复群集中的单个主机或所有主机。

- a. 要为单个主机运行修复任务，在**映像合规性**部分中，单击主机旁边的垂直省略号图标，然后选择**修复**。
- b. 要为群集中的所有主机执行修复任务，请在**映像合规性**部分中单击**全部修复**。

建议您在运行固件更新之前执行 iDRAC 重置。执行 iDRAC 重置可减少出现故障的可能性。

要在使用每个主机上的 vSphere 生命周期管理器执行固件更新之前自动重置 iDRAC，请在 OMIVV 中启用**清除 iDRAC 作业和重设 iDRAC**复选框。有关更多信息，请参阅 [固件更新设置](#) 页面上的 80。

您可以通过单击**更新**页面上的**显示更多**来查看修复任务的状态。

您可以在 OMIVV 的**日志**页面上查看与 OMIVV 相关的日志。

## 在 vSphere 生命周期管理器中使用 OMIVV 作为固件加载项提供程序 — vSphere 自动化 vAPI

使用 vSphere Automation API 管理群集之前，请确保您已使用 vSphere 生命周期管理器用户界面完成以下任务：

- 选择硬件支持管理器作为 DellEMC OMIVV。
- 选择适用于所选群集的群集配置文件，然后保存映像。

## 扫描固件合规性

**命令**：POST https://{VC IP/FQDN}/api/esx/settings/clusters/{cluster ID}/software?vmw-task=true&action=scan

```
{
  "spec" : {
    "message": "test commit"
  }
}
```

**说明**：根据群集所需的状态扫描群集中的所有主机。此操作的结果可通过调用 `cis/tasks/{task-id}` 进行查询，其中 `task-id` 是此操作的响应。

**HTTP 响应代码**：200。有关所有响应代码的列表，请参阅[响应代码](#)页面上的 154。

**示例响应**：

```
{task ID}
```

## 获得兼容性任务状态

**命令** : GET https://{VC IP/FQDN}/rest/cis/tasks/{task ID}

**说明** : 返回有关任务的信息。

**HTTP 响应代码** : 200。有关所有响应代码的列表, 请参阅[响应代码](#) 页面上的 154。

**示例响应** : 以下示例仅包含非合规固件。

```
"result":
[
  {
    "value":
    [
      {
        "value":
        {
          "hardware_modules":
          [
            {
              "value":
              {
                "current":
                {
                  "version": "25.5.6.0009"
                },
                "details":
                {
                  "component_class": "PCI_DEVICE",
                  "description": "PERC H730 Mini"
                } "notifications":
                {
                  "info":
                  [
                    {
                      "id": "Different versions.",
                      "time": "2020-02-04T10:47:54.422Z",
                      "message":
                      {
                        "args": [],
                        "default_message": "Different versions.",
                        "id": "Different versions."
                      }
                    }
                  ],
                },
                "status": "NON_COMPLIANT",
                "target": {
                  "version": "25.5.5.0005"
                }
              }
            }
          ],
          "key": ""
        },
        "notifications":
        {
          "info":
          [
            {
              "id": "[vCenter:<vCenter IP/FQDN>][Cluster: <Cluster name>][Host: <host IP/FQDN>] The host is non-compliant",
              "time": "2020-02-04T10:47:54.423Z",
              "message":
              {
                "args": [],
                "default_message": "[vCenter:<vCenter IP/FQDN>][Cluster: <Cluster name>][Host: <host IP/FQDN>] The host is non-compliant",
                "id": "[vCenter:<vCenter IP/FQDN>][Cluster: <Cluster name>][Host: <host IP/FQDN>] The host is non-compliant"
              }
            }
          ]
        }
      }
    ]
  }
]
```

```
},
"status": "NON_COMPLIANT",
"target": {
"pkg": "<cluster profile name>",
"version": "0.0.0-0"
}
},
"key": "com.dell.plugin.OpenManager_HWSupportManager"
}
],
```

## 运行修复预检查

**命令** : POST https://{VC IP/FQDN}/api/esx/settings/clusters/{cluster ID}/software?vmw-task=true&action=check

**说明** : 先在群集上运行检查, 然后再在群集中的所有主机上应用所需状态。检查群集中的所有主机是否处于良好状态, 并可更新到所需状态。

**HTTP 响应代码** : 200。有关所有响应代码的列表, 请参阅[响应代码](#) 页面上的 154。

**示例响应** :

```
{task-id}
```

## 获取修复预检查任务状态

**命令** : GET https://{VC IP/FQDN}/rest/cis/tasks/{task ID}

**说明** : 返回有关任务的信息。

**HTTP 响应代码** : 200。有关所有响应代码的列表, 请参阅[响应代码](#) 页面上的 154。

**示例响应** :

```
{
  "value":
  {
    "parent": "",
    "cancelable": true,
    "end_time": "2020-02-12T18:03:59.391Z",
    "description":
    {
      "args": [],
      "default_message": "Task created by VMware vSphere Lifecycle Manager",
      "id": "com.vmware.vcIntegrity.lifecycle.Task.Description"
    },
    "target":
    {
      "id": "domain-c8",
      "type": "ClusterComputeResource"
    },
    "result":
    {
      "start_time": "2020-02-12T17:52:09.264Z",
      "commit": "",
      "end_time": "2020-02-12T18:03:59.386Z",
      "entity_results":
      [
        {
          "host": "host-47",
          "type": "HOST",
          "check_statuses": [],
          "status": "OK"
        }
        {
          "host": "host-41",
          "type": "HOST",
          "check_statuses": [],
          "status": "OK"
        }
      ]
    }
  }
}
```

```

},
{
  "host": "host-22",
  "type": "HOST",
  "check_statuses": [],
  "status": "OK"
},
{
  "host": "host-16",
  "type": "HOST",
  "check_statuses": [
    {
      "check":
      {
        "name":
        {
          "args": [],
          "default_message": "Host Hardware support check.",
          "id": "com.vmware.vcIntegrity.lifecycle.ClusterHealthCheckTask.HwSupportCheck.Name"
        },
        "description":
        {
          "args": [],
          "default_message": "Checks if the hardware update can be performed.",
          "id": "com.vmware.vcIntegrity.lifecycle.ClusterHealthCheckTask.HwSupportCheck.Description"
        },
        "check": "com.vmware.vcIntegrity.lifecycle.ClusterHealthCheckTask.HwSupportCheck"
      },
      "issues": [
        {
          "args": [],
          "default_message": "[vCenter: jpvc7dot0d5-2.sped.bdcsv.lab][Cluster: R6415_vSAN_AllFlash_ESXi7.0RC+][Host: 100.100.10.154][Update PreCheck Task] System Lockdown Mode is turned On for iDRAC IP, 172.20.5.5; hence Firmware update cannot continue.",
          "id": "[vCenter: jpvc7dot0d5-2.sped.bdcsv.lab][Cluster: R6415_vSAN_AllFlash_ESXi7.0RC+][Host: 100.100.10.154][Update PreCheck Task] System Lockdown Mode is turned On for iDRAC IP, 172.20.5.5; hence Firmware update cannot continue."
        }
      ],
      "status": "ERROR"
    }
  ],
  "status": "ERROR"
},
{
  "host": "host-19",
  "type": "HOST",
  "check_statuses": [],
  "status": "OK"
},
{
  "host": "host-13",
  "type": "HOST",
  "check_statuses": [],
  "status": "OK"
},

```

## 修复群集

**命令** : POST https://{{VC IP/FQDN}}/api/esx/settings/clusters/{cluster ID}/software?vmw-task=true&action=apply

```

{
  "accept_eula" : true
}

```

**说明** : 将与给定群集关联的所需状态应用到群集中的主机。

**HTTP 响应代码** : 200。有关所有响应代码的列表，请参阅[响应代码](#) 页面上的 154。

示例响应：

```
{task-id}
```


## 设置闪烁指示灯

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。

1. 要启动**让服务器 LED 指示灯闪烁**向导，请执行以下操作之一：
  - a. 在 OMIVV 主页中，展开**菜单**，选择**主机和群集**，右键单击某个主机或群集，然后转至**摘要 > OMIVV 主机信息 > 主机操作 > 让服务器 LED 指示灯闪烁**。
  - b. 右键单击某个主机，转至 **OMIVV 主机操作 > 让服务器 LED 指示灯闪烁**。
2. 在右侧窗格中，单击“摘要”，然后转至 **OMIVV 主机信息 > 主机操作 > 让服务器 LED 指示灯闪烁**。此时将显示**让服务器 LED 指示灯闪烁**对话框。
3. 选择以下任一操作：
  - a. 要打开服务器 LED 指示灯并设置时间段，请单击**打开**。
  - b. 要关闭服务器 LED 指示灯，请单击**关闭**。

## 配置系统锁定模式

系统锁定模式仅在具有企业许可证的基于 iDRAC9 的服务器上受支持。开启系统锁定模式时，锁定系统配置（包括固件更新）。系统锁定模式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。从 OMIVV 4.1 版和更高版本中，您可以配置和监测服务器中 iDRAC 的锁定模式。此外，iDRAC 必须具有企业版许可证才能启用锁定模式。

 **注：**您无法更改使用机箱凭据配置文件管理的主机的系统锁定模式。

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。
1. 要启动配置系统锁定模式向导，请执行以下操作：
    - a. 在 OMIVV 主页中，展开**菜单**，选择**主机和群集**，右键单击某个主机或群集，然后转至**摘要 > OMIVV 主机信息 > 主机操作 > 配置系统锁定模式**。
    - b. 右键单击某个主机或群集，转至 **OMIVV 主机操作 > 配置系统锁定模式**。
    - c. 选择某个主机或群集，转至**监测 > OMIVV 主机或群集信息 > 固件 > 配置系统锁定模式**。
  2. 对于群集级别，请输入系统锁定模式作业名称和说明。该说明是可选字段。
  3. 要启用系统锁定模式，请单击**打开**。此选项将限制对系统中系统配置（包括固件和 BIOS 版本）进行更改。
  4. 要禁用系统锁定模式，请单击**关闭**。此选项可允许对系统中系统配置（包括固件和 BIOS 版本）进行更改。  
如果您尝试为第 13 代及较早的 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。
  5. 单击**确定**。  
已成功创建用于配置系统锁定模式的作业。要检查作业状态，请转至**作业 > 系统锁定模式**。有关系统锁定模式作业的更多信息，请参阅**系统锁定模式作业** 页面上的 69。

## 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 操作角色和 Dell 基础架构部署角色。

## 数据完整性

OpenManage Integration for VMware vCenter、Administration Console 和 vCenter 之间的通信使用 HTTPS 完成。OpenManage Integration for VMware vCenter 生成一个用于在 vCenter 和设备之间进行受信通信的证书。它还在通信和 OpenManage Integration for VMware vCenter 注册之前，它还会验证和信任 vCenter 服务器的证书。

安全 Administration Console 会话具有 15 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 1: 安全错误消息

## 访问控制验证、授权和角色

为执行 vCenter 操作，OpenManage Integration for VMware vCenter 使用 vSphere 客户端的当前用户会话和 OpenManage Integration 的存储管理凭据。OpenManage Integration for VMware vCenter 采用 vCenter 服务器内置的角色和权限模型来授权用户在 OpenManage Integration 和 vCenter 托管对象（主机和群集）上执行的操作。

## 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. 25: 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

表. 25: 权限组 (续)

组名称	说明
权限组 - Dell. Reporting (Not used)	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“配置主机凭据配置文件”、“分配标识”和“部署”。

### 权限组 — Dell.Deploy-Provisioning

配置主机凭据配置文件、分配标识、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
  - 闪烁 LED、清除 LED
  - 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

## 常见问题-FAQ

使用本部分来查找故障排除问题的答案。本部分包括以下内容：

- [常见问题 \(FAQ\)](#)
- [裸机部署问题](#) 页面上的 146

### 常见问题-FAQ

本节包含一些常见问题及解决方案。

## 对于不符合要求的 vSphere 主机，iDRAC 的许可证类型和说明显示不正确

如果主机在 CSIOR 被禁用或尚未运行时不符合要求，则 iDRAC 许可证信息显示不正确，但有效的 iDRAC 许可证可用。因此，您可以在 vSphere 主机列表中查看主机，但是当您单击主机了解详细信息时，**iDRAC 许可证类型**中的信息将显示为空，**iDRAC 许可证说明**显示为“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 及更高版本

## Dell 提供程序未作为运行状况更新提供程序显示

当您为 vCenter 服务器与 OMIVV 一起注册，然后升级 vCenter 服务器版本时（例如，从 vCenter 6.0 升级到 vCenter 6.5），Dell 提供程序将不会显示在**主动高可用性提供程序**列表中。

解决方案：您可以为非管理员用户或管理员用户升级已注册的 vCenter。要升级至最新版本的 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：
  1. 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](#)页面上的 13。
  2. 重新引导已注册的 OMIVV 设备。
  3. 从 vSphere Client 中注销，然后再次登录。
- 对于管理员用户：
  1. 重新引导已注册的 OMIVV 设备。
  2. 从 vSphere Client 中注销，然后再次登录。

Dell 提供程序现在在**主动高可用性提供程序**列表中列出。

受影响的版本：4.0 及更高版本

## 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。

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”。

1. 打开 iDRAC 虚拟控制台。
2. 按下 F2 并转至**故障排除选项**。
3. 在**故障排除选项**中，转至**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。

**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[创建主机凭据配置文件](#) 页面上的 35。

## 运行“修补不符合要求的 vSphere 主机”向导时，特定主机的状态显示为“未知”

运行“修补不符合要求的 vSphere 主机”向导以修补不符合要求的主机时，特定主机的状态显示为“未知”。无法访问 iDRAC 时，将显示未知状态。

解决方案：验证主机的 iDRAC 连接并确保资源清册成功运行。

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

向 OMIVV 设备注册 vCenter 后，vCenter 权限列表中会增加几个 Dell 权限。从 OMIVV 设备中注销 vCenter 后，将不会移除 Dell 权限。

**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 及更高版本

## 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。有关更多信息，请参阅 [https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT\\_KB\\_1\\_1&externalId=2121701](https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701) 和 [https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT\\_KB\\_1\\_1&externalId=2121689](https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121689)。

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

有关更多信息，请参阅 <https://kb.vmware.com/s/article/2121689>。

## 更换 vCenter 服务器设备上的证书

有关更多信息，请参阅 <https://kb.vmware.com/s/article/2121689>。

## 检索管理对象浏览器 (MOB) 中的旧证书

有关更多信息，请参阅 <https://kb.vmware.com/s/article/2121701>。

## 从旧证书中提取指纹

有关更多信息，请参阅 <https://kb.vmware.com/s/article/2121701>。

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

在重设设备后，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 OMIVV 中更改 DNS 设置后在 vCenter HTML-5 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 HTML-5 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。
- 先进行注销，然后从 vSphere Client 中登录。

## 在固件页面中，一些固件的安装日期显示为 12/31/1969

在 vSphere Client 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

## 即使 OpenManage Integration 插件已成功注册到 vCenter，我在 HTML-5 客户端上仍然看不到 OpenManage Integration 图标

必须重新启动 vSphere 客户端服务，在 vSphere 客户端上才会显示 OpenManage Integration 图标。当用户注册 OpenManage Integration for VMware vCenter 设备时，将同时注册到 vSphere 客户端。如果用户注销设备，然后重新注册相同版本或新版本的设备，将成功注册，但是 OMIVV 图标可能不会出现在 vSphere 客户端中。这源自 VMware 的高速缓存问题。要解决此问题，用户需要重新启动 vCenter 服务器上的 vSphere 客户端服务。此后该插件才会出现在 UI 中。

解决方案：重新启动 vCenter 服务器上的 vSphere 客户端服务。

受影响的版本：2.2 及更高版本

## 如果设备 IP 和 DNS 设置被 DHCP 值覆盖，在设备重新启动后，为什么 DNS 配置设置将恢复到原始设置

存在一个已知缺陷，导致静态分配的 DNS 设置被 DHCP 中的值替换。当 DHCP 用于获取 IP 设置并且 DNS 值以静态方式分配时，可能会发生这种情况。当续订 DHCP 租赁或重新启动设备时，将移除静态分配的 DNS 设置。

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

受影响的版本：所有

## 运行固件更新可能会显示错误消息，固件存储库文件不存在或无效。

在群集级别运行“固件更新”向导时，可能会显示错误消息：**固件存储库文件不存在或无效**。这可能是由于每日后台进程无法从存储库下载和缓存目录文件。如果在后台进程运行时无法访问目录文件，则会发生这种情况。

解决方案：解决可能存在的任何目录连接问题之后，您可以通过更改固件存储库位置，然后将其设置回原始位置来重新启动后台进程。等待大约五分钟，以便后台进程完成。确保为 CIFS 提供的凭据中不存在 @ 字符。此外，请确保该 DUP 文件存在于共享位置。

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

Dell EMC PowerEdge 服务器和某些固件版本为 13.5.2 的 Intel 网卡出现已知问题。使用带有 Lifecycle Controller 的 iDRAC 应用固件更新时，更新此固件版本的某些型号的 Intel 网卡失败。具有此版本的固件的客户必须使用操作系统更新网络驱动程序软件。如果 Intel 网卡的固件版本不为 13.5.2，则您可以使用 OMIVV 进行更新。有关更多信息，请参阅 <http://en.community.dell.com/techcenter/b/>

**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

这对于 NIC 14.5 和 15.0 而言是一个已知问题。确保您使用自定义目录将固件更新至 15.5.0，然后再将固件更新至 16.x。  
受影响的版本：所有

## 为什么管理门户显示无法访问的更新存储库位置

如果提供无法访问的“更新存储库”路径，则“设备更新”视图顶部会显示“失败：连接到 URL 时出错。”错误消息。但在更新之前，“更新存储库路径”的值不会清除。

解决方案：离开此页面并进入另一个页面，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，系统无法进入维护模式

有些固件更新不需要重新启动主机。在这种情况下，无需将主机置于维护模式即可执行固件更新。

## 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

相对于电源设备的机箱全局运行状况是基于冗余策略和仍然处于在线状态并正常运行的 PSU 是否满足机箱电源需求。因此，即使某些 PSU 已失去功率，机箱电源总功率要求仍得到满足。因此，机箱全局运行状况仍然良好。有关“电源”和“电源管理”的更多详细信息，请参阅“用户指南”，获取 Dell PowerEdge M1000e 机箱管理控制器固件文档。

## 在“系统概览”页面的“处理器视图”中处理器版本中为“不适用”

在第 12 代和更高版本的服务器中，处理器版本显示在“品牌”列。如果是更低代次的服务器，处理器版本则显示在版本列。

## OMIVV 在链接模式下是否支持 vCenter

是，不管在链接模式还是非链接模式，OMIVV 均支持最多 10 台 vCenter 服务器。

## 什么是 OMIVV 所需的端口设置

使用 OMIVV 的以下端口设置：

表. 26: 虚拟设备

端口号	协议	端口类型	最高加密级别	方向	目标	使用情况	说明
53	DNS	TCP	无	出	OMIVV 设备至 DNS 服务器	DNS 客户端	连接到 DNS 服务器或解析主机名。
68	DHCP	UDP	无	进	DHCP 服务器至 OMIVV 设备	动态网络配置	获取网络详细信息，如 IP、网关、网络掩码和 DNS。

表. 26: 虚拟设备 (续)

端口号	协议	端口类型	最高加密级别	方向	目标	使用情况	说明
69	TFTP	UDP	128 位	出	OMIVV 至 iDRAC	普通文件传输	用于将裸机服务器更新至最低支持的固件版本。
123	NTP	UDP	无	进	NTP 至 OMIVV 设备	时间同步	与特定时区同步。
162	SNMP 代理	UDP	无	进	iDRAC、CMC 或 OME-Modular 至 OMIVV 设备	SNMP 代理 (服务器)	接收来自受管节点的 SNMP 陷阱。
80/443	HTTP 或 HTTPS	TCP	无	出	OMIVV 设备至互联网	Dell 联机数据访问	连接到联机 (互联网) 保修、固件和最新的 RPM 信息。
443	HTTPS	TCP	128 位	进	OMIVV UI 至 OMIVV 设备	HTTPS 服务器	OMIVV 提供的 Web 服务。vSphere Client 和 Dell 管理门户会消耗这些 Web 服务。
443	HTTPS	TCP	128 位	进	ESXi 服务器至 OMIVV 设备	HTTPS 服务器	在操作系统部署流程中使用, 以便安装后脚本与 OMIVV 设备进行通信。
443	HTTPS	TCP	128 位	进	iDRAC 至 OMIVV 设备	自动查找	配置服务器, 用于自动查找受管节点。
443	WSMAN	TCP	128 位	进/出	OMIVV 设备至或从 iDRAC	iDRAC 通信	用于管理和监测托管节点的 iDRAC、CMC 或 OME-Modular 通信。
445/139	SMB	TCP	128 位	出	OMIVV 设备至 CIFS	CIFS 通信	与 Windows 共享通信。
2049/111	NFS	UDP/TCP	无	进/出	OMIVV 设备至 NFS	公共共享	对受管节点公开的 NFS 公共共享 (由 OMIVV 设备呈现), 用于固件更新和操作系统部署流程。
4001 至 4004	NFS	UDP/TCP	无	进/出	OMIVV 设备至 NFS	公共共享	这些端口必须保持开放, 以通过 NFS 服务器的 V2 和 V3 协议运行 statd、quotd、lockd 和 mountd 服务。
用户定义的	任意	UDP/TCP	无	出	OMIVV 设备至代理服务器	代理	与代理服务器通信。

表. 27: 受管节点 (ESXi)

端口号	协议	端口类型	最高加密级别	方向	目标	使用情况	说明
162	SNMP	UDP	无	出	ESXi 至 OMIVV 设备	硬件事件	从 ESXi 发送的异步 SNMP 陷阱。此端口必须从 ESXi 中打开。
443	WSMAN	TCP	128 位	进	OMIVV 设备至 ESXi	iDRAC 通信	用于向管理站提供信息。此端口必须从 ESXi 中打开。
443	HTTPS	TCP	128 位	进	OMIVV 设备至 ESXi	HTTPS 服务器	用于向管理站提供信息。此端口必须从 ESXi 中打开。

有关 iDRAC 和 CMC 端口的详细信息, 请参阅 <https://www.dell.com/support> 上提供的 *Integrated Dell Remote Access Controller 用户指南* 和 *Dell Chassis Management Controller 用户指南*。

有关 OME-Modular 端口的详细信息, 请参阅 <https://www.dell.com/support> 上提供的 *Dell EMC OME-Modular 用户指南*。

**注:** 对于基于 iDRAC9 的服务器, iDRAC 会通过端口 2049 上的 TCP 装载 NFS。有关基于 iDRAC9 的服务器的列表, 请参阅兼容性值表。

## 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未更改

如果仅选择了系统配置文件（硬件配置）用于部署，则用于查找的用户的密码不会更改为新的凭据。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。

## 无法查看 vCenter 主机和群集页面上列出的新 iDRAC 版本详细信息

在 vSphere Web 客户端的最近任务窗格中成功完成固件更新任务之后，刷新**固件更新**页面并验证固件版本。如果页面显示旧版本，则转至 OpenManage Integration for VMware vCenter 的**主机符合性**页面，并检查主机的 CISO 状态。如果 CISO 尚未启用，则启用 CISO 并重新引导主机。如果 CISO 已启用，则登录到 iDRAC 控制台，重设 iDRAC，等待几分钟，然后在 vSphere Web 客户端中刷新**固件更新**页面。

## 支持启用锁定模式的 ESX/ESXI

可以。此版本支持 ESXi 6.0 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主机凭据配置文件时，清点开始，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清点”。

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

## 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. 确保在分配服务器身份时选择的 NIC 可被虚拟设备访问。
3. 确保根据与 OMIVV 的网络连接选择管理 NIC。
4. 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。
5. 请确保系统可以看到至少一个虚拟磁盘、iSDM 或 BOSS。

## 在部署向导中看到自动查找到的系统没有型号信息

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。在某些情况下，固件更新可能未在系统上注册。

解决方案：冷启动系统或重装刀片可修复此问题。iDRAC 上新启用的帐户必须已被禁用，并且已重新启动自动查找以将型号信息和 NIC 信息提供给。

## 使用 ESXi ISO 设置了 NFS 共享，但装载共享位置出错，造成部署失败

要查找解决方案：

1. 确保 iDRAC 可以对设备执行 ping 操作。
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。

## 我如何从 vCenter 上强制移除 OMIVV 设备

1. 转至 vSphere 客户端并为所有启用了主动式高可用性的群集清除 Dell 提供程序的复选框。
2. 转到 [https://<vcenter\\_serverIPAddress>/mob](https://<vcenter_serverIPAddress>/mob)

3. 输入 VMware vCenter 管理凭据。
4. 单击**主页 > 内容 > HealthUpdateManager**。
5. 单击 **QueryProviderList > 调用方法**。
6. 复制提供程序 ID 字符串值，然后关闭该窗口。
7. 单击 **UnregisterHealthUpdateProvider**，然后输入复制的提供程序 ID 字符串值。
8. 单击**调用方法**。
9. 转至**主页 > 内容**
10. 单击 **ExtensionManager**。
11. 单击 **UnregisterExtension**。
12. 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**。
13. 在 vSphere 客户端中，关闭 OMIVV 并将其删除。要注销的密钥必须适用于 vSphere 客户端。
14. 在 vCenter 中，清除 Serenity 条目并重新启动 vCenter 服务。

## 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。向下滚动页面来输入加密密码。

## 如果更新失败，应该怎么办

检查 OMIVV 设备日志了解任务是否已超时。如果超时，需要执行冷重新引导来重置 iDRAC。当系统启动和运行时，通过运行资源清册或使用**固件**选项卡，检查更新是否成功。

## 我的 vCenter 注册失败，该怎么办

vCenter 注册可能由于通信问题而失败，因此，遇到这些问题时的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”下输入 DNS 服务器名称。

 **注：** 确保虚拟设备可以解析您输入的 DNS 服务器。

## 主机凭据配置文件测试凭据期间的性能缓慢或无响应

服务器上的 iDRAC 只有一位用户（例如，仅 `root` 用户），并且该用户处于禁用状态，或所有用户处于禁用状态。与处于禁用状态的服务器通信会导致延迟。要解决此问题，您可以修复服务器的禁用状态，或在服务器上重置 iDRAC，以重新启用 `root` 用户的默认设置。

要修复禁用状态的服务器：

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，单击以下其中一项：
  - iDRAC7：选择 **iDRAC 设置 > 用户选项卡**。
  - iDRAC8：选择 **iDRAC 设置 > 用户选项卡**。
  - iDRAC9：选择 **iDRAC 设置 > 用户选项卡**。

对于 iDRAC 7 和 8：

- a. 要编辑设置，在用户 ID 列中，单击 `admin (root)` 用户的链接。
- b. 单击**配置用户**，然后单击**下一步**。
- c. 在所选用户的**用户配置**页中，选中“启用用户”旁边的复选框，然后单击**应用**。

对于 iDRAC 9：

- a. 选择 `root` 用户并单击**启用**。

## OMIVV 是否支持 VMware vCenter 服务器设备

是的，自 2.1 版本起，OMIVV 支持 VMware vCenter 服务器设备。

## 服务器可能显示为不符合 CSIOR 状态 - “未知”

解决方案：未知的 CSIOR 状态表示主机上的无响应 iDRAC。主机上的手动 iDRAC 重置将修复此问题。

受影响的版本：所有

## 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系统进行了重新引导后，但我的固件级别仍未更新

要更新固件，请在重新引导完成后在主机上运行资源清册。在某些情况下，在重新引导事件未到达设备时，资源清册不会自动触发。在这种情况下，必须手动重新运行资源清册以获得更新的固件版本。

## 即使从 vCenter 树中删除了主机，主机仍显示在机箱下

机箱下的主机将被视为机箱资源清册的一部分。在成功执行机箱资源清册后，将更新机箱下的主机列表。即使从 vCenter 树中移除主机，主机仍在机箱下显示，直至运行下一次资源清册。

## 备份和还原 OMIVV 后，警报设置未还原

还原 OMIVV 设备备份并不还原所有警报设置。但是，在 OMIVV GUI 中，**警报和事件**字段会显示还原的设置。

解决方案：在 OMIVV GUI 的**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 NPAR 并且在系统配置文件中禁用该分区时，操作系统部署失败


当在目标机器上应用具有禁用 NIC 分区 (NPAR) 的系统配置文件时，操作系统部署失败。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 及更高版本

## 当可用版本低于当前版本时，可用的 OMIVV 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。

 **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。

## 添加第 12 代和更高版本的裸机服务器时引发 267027 异常

在进行裸机查找的过程中，如果输入的凭据不正确，用户帐户会自动锁定几分钟。在此期间，iDRAC 变得无响应，并且需要几分钟才能恢复正常。

解决方案：等待几分钟，再重新输入用户凭据。

## 由于 iDRAC 错误，在部署过程中，系统配置文件应用失败

在部署过程中，OMIVV 将尝试在 iDRAC 中创建配置更新作业。但是，作业创建有时会失败，并显示一条消息，表示配置作业已创建。

**解决方案：**清除过时条目，然后重试部署。登录到 iDRAC 以清除作业。

## 借助域用户身份验证进行配置时，OMIVV RPM 升级失败

如果 OMIVV 设备使用代理配置来访问互联网，而代理使用 NTLM 身份验证进行验证，则由于底层 yum 工具问题，RPM 更新失败。

**受影响的版本：**OMIVV 4.0 及更高版本

**解决方案/解决办法：**执行备份和还原以更新 OMIVV 设备。

## 无法应用 FX 机箱中有 PCIe 卡的系统配置文件

使用 FX 机箱时，如果源服务器有 PCIe 卡信息，在目标服务器上部署操作系统将失败。源服务器上系统配置文件的 `fc.chassislot` ID 与目标服务器上的不同。OMIVV 尝试在目标服务器上部署同一 `fc.chassislot` ID 失败。系统配置文件在应用配置文件时搜索确切实例 (FQDD)，该配置文件在机架式服务器（相同的）上成功运行，但在模块化服务器中可能受到一些限制。例如，在 FC640 中，由于 NIC 级别限制，从一台模块化服务器创建的系统配置文件无法在相同 FX 机箱中的其它模块化服务器上应用。

**受影响的版本：**4.1 及更高版本。

**解决方案：**来自 FX2s 机箱插槽 1 中的 FC640 服务器的系统配置文件仅可在驻留在另一 FX2s 机箱插槽 1 中的另一 FC640 服务器上应用。

## 偏移检测显示在 FX 机箱中具有 PCIe 卡的模块化服务器的不合规情况

系统配置文件会在搜索确切实例 (FQDD) 的同时与基线进行比较，此方法在（完全相同的）机架式服务器上成功运行，但在模块化服务器中可能受到一些限制。例如，在 FC640 中，由于 FQDD 不匹配，从一台模块化服务器创建的系统配置文件（基线）显示与相同 FX 机箱中的其它模块化服务器有偏移。

**受影响的版本：**4.1 及更高版本。

**解决方案：**在创建系统配置文件时，清除与其他服务器不通用的 FQDD。

## 当 iDRAC 未填充所选 NIC 的 MAC 地址时无法在 PowerEdge 服务器上部署操作系统

当 iDRAC 未填充所选 NIC 端口的 MAC 地址时，在 PowerEdge 服务器上部署操作系统将会失败。

**解决方案：**分别将 NIC 固件和 iDRAC 固件更新到最新版本，并确保在 NIC 端口上填充 MAC 地址。

**受影响的版本：**4.3 及更高版本

## 为具有 ESXi 6.5U1 的主机创建主机凭据配置文件时，不在“选择主机”页面上显示主机的服务标签

当 OMIVV 查询 vCenter 以取得 ESXi 的服务标签时，vCenter 无法返回服务标签，因为“服务标签”值为 NULL。

**解决方案：**将 ESXi 版本更新到 ESXi 6.5U2 或 ESXi 6.7 U1。

**受影响的版本：**4.3 及更高版本

## 从旧版 OMIVV 备份或还原至更高版本的 OMIVV 后，将不显示 Dell EMC 图标

从旧版 OMIVV 备份或还原至更高版本的 OMIVV 后，将发现以下问题：

- vCenter 上未显示 Dell EMC 徽标。
- 2000000 错误
- 3001 错误

解决方案：

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

## 使用 OMIVV 升级或降级的一些 iDRAC 固件版本时，即使固件更新成功，OMIVV 仍可能显示作业失败。

在固件更新期间，当您降级或升级 iDRAC 版本（例如 3.20.20.20、3.21.21.21 和 3.21.21.22）时，即使该作业已成功运行，作业状态显示为发生故障。

解决方案：作业故障后，刷新资源清册，为其他组件重新运行作业。

受影响的版本：4.3

## 在一个集群级别下配置系统锁定模式时有时会显示消息“该集群下没有主机具有成功的资源清册”

在群集级别配置“系统锁定”模式时，有时会显示消息“群集下没有主机已成功清点”。即使群集已成功清点由 OMIVV 管理的基于 iDRAC9 的服务器，也会显示此消息。有关基于 iDRAC9 的服务器的列表，请参阅兼容性值表。

解决方案：重新引导 vCenter。

要重新引导的 vCenter，请执行以下操作：

1. 使用 vCenter 单点登录管理员帐户登录 vSphere Client。
2. 转至**管理 > 部署 > 部署 > 系统配置**。
3. 单击**节点**，选择 vCenter 服务器设备的节点，然后单击**相关对象**选项卡。
4. 重新引导 vCenter 设备。

## 有时开机自检 OMIVV 设备的 RPM 升级，可以在 vCenter 最近任务中查看日志中的多个条目

有时升级 RPM 后，在 vCenter 最近任务上查看时，将在日志中显示多个条目。

解决方案：重新启动 vCenter 服务。

受影响的版本：4.3

## 注册 vCenter 后，OMIVV 的 Dell EMC 徽标不显示在 VMware 的主页上

说明：OMIVV 的 Dell EMC 徽标可能不会显示在 VMware 的主页上，因为完成注册后不久，VMware vCenter 将验证插件。

解决方案：执行以下：

1. 刷新浏览器或清除浏览器缓存，或重新启动 vSphere 客户端 (HTML-5) 的客户端服务。
2. 从 vSphere Client 中注销，然后再次登录。

受影响的版本：5.0

## 在备份和还原后，非合规的 11G PowerEdge 服务器会保留在 OMIVV 资源清册中

在 OMIVV 中执行备份和还原操作后，非合规和非资源清册的 11G 主机仍然与主机凭据配置文件关联。但是，如果您尝试修复配置合规性并运行新的资源清册，作业将在不受支持的 11G 服务器上失败。

解决方案：OMIVV 5.0 不支持第 11 代服务器。手动从主机凭据配置文件中删除不受支持的第 11 代主机。

受影响的版本：5.0

## 升级 OMIVV 设备后无法从灵活客户端启动 vCenter

解决方法：有关解决方法，请参阅 VMware 知识库文章：<https://kb.vmware.com/s/article/54751>。

受影响的版本：5.0

## 在 OMIVV 中添加或删除网络适配器时，现有 NIC 将从 OMIVV 控制台中消失

有时，当您使用 vSphere Client 在 OMIVV 设备中添加或删除网络适配器时，现有 NIC 会从 OMIVV 控制台中消失。

解决方法：执行以下任务之一：

1.
  - a. 从终端控制台公用程序中移除所有网络适配器。
  - b. 关闭设备
  - c. 从设备中移除网络适配器。
  - d. 重新引导 OMIVV 设备。
  - e. 关闭设备
  - f. 添加所需的网络适配器并完成网络适配器配置。
  - g. 重新引导设备。
2.
  - a. 从管理员门户备份 OMIVV
  - b. 创建 OMIVV 设备。
  - c. 关闭设备
  - d. 添加所需的网络适配器并完成网络适配器配置。
  - e. 重新引导设备。
  - f. 恢复最新备份的数据。

受影响的版本：OMIVV 5.0

## 添加或删除第二个 NIC 后，“网络配置”页面显示三个 NIC

在您使用 vSphere 客户端在 OMIVV 设备中添加或删除 NIC 后，一旦您启动 OMIVV 设备并登录 OMIVV 终端控制台，有时网络配置页面会显示不一致的 NIC 数量。

解决方法：使用 MAC 地址来比较并配置正确的 NIC，并使用 - 按钮移除额外的 NIC。

受影响的版本：5.0

## 备份和还原到最新的 OMIVV 版本后，较早版本中状态为“未知”的服务器未列出在“裸机服务器”页面上

从较早版本还原备份后，不受支持的服务器（11G 及更早版本）将从裸机服务器资源清册中移除。还会移除在备份之前未通过较早版本确定代系的服务器。

解决方法：重新查找服务器。如果缺失的服务器受支持，则会在裸机服务器清单中列出。

受影响的版本：5.0

## 进行操作系统部署后，OMIVV 无法将 ESXi 主机添加到 vCenter、无法添加主机配置文件或主机进入维护模式失败

进行操作系统部署后，OMIVV 查询 vCenter 以执行主机操作（添加主机、添加主机配置文件或进入维护模式）。如果查询未在两分钟内收到响应，则表示 vCenter 上的特定操作超时，并且会在任务历史记录中显示一条消息，指出通信失败。但是，有时 vCenter 查询操作会成功。

解决方法：从任务历史记录中获取主机 IP 并手动添加。

## 当 iDRAC IP 不可访问时，iDRAC 许可证状态在“管理合规性”页面上显示为“合规”

在执行定期资源清册后，如果 iDRAC 无法访问，iDRAC 许可证状态在“管理合规性”页面上显示为“合规”。

解决方法：确保 iDRAC 可访问，并再次运行资源清册以获取正确的 iDRAC 许可证详细信息。

## 使用 OMIVV 成功部署操作系统后，ESXi 主机断开连接或处于无响应状态。

ESXi 主机无法将检测信号数据包发送至 vCenter，因为其 DNS 未正确配置为 vCenter 的查找 FQDN。

解决方案：执行以下任务：

1. 将 ESXi 主机从 vCenter 资源清册中移除。
2. 使用**添加主机**向导在 vCenter 中添加主机。
3. 创建主机凭据配置文件并运行资源清册。

## OMIVV 网络接口卡 (NIC) 未连接至 ESXi 主机网络时，部署作业超时

操作系统部署依赖 NIC 的选择。如果未选择正确的 NIC，则 OSD 作业超时。

解决方案：从部署向导的“配置主机设置”页面中，选择适当的“连接到主机的设备 NIC”。在操作系统安装过程中，OMIVV 需要执行此操作以访问 ESXi 网络。

## 保修作业未针对某些主机运行

在具有多个 vCenter 的 PSC 环境中，如果您将使用 FQDN 的主机添加到一个 vCenter 并将 IP 添加到另一个 vCenter，则保修作业将仅针对一个主机实例运行。

解决方法：从主机凭据配置文件中删除已断开连接的主机实例，然后运行资源清册和保修作业。

受影响的版本：5.0

## 执行备份和还原后，主动高可用性初始化未发生

当您从向 vSphere 客户端注册的先前版本还原 OMIVV 时，对于启用了主动高可用性的群集，Dell 提供程序断开连接。

解决方法：针对群集先禁用然后启用主动高可用性。

受影响的版本：5.0

## OMIVV 页面显示无效的会话、超时异常或 Firefox 浏览器中的 2000000 错误

如果 OMIVV 页面空闲一段时间（5-10 分钟），则会显示无效的会话或超时异常或 2000000 错误。

解决方案：刷新浏览器。如果问题仍然存在，请注销，然后从 vCenter 登录。

要在 OMIVV 中查看正确的数据，请确保您完成解决方案中列出的任务。

受影响的版本：5.0

## 在 vCenter 中，“最近任务”窗格不会显示一些 OMIVV 任务通知的详细信息列

解决方案：要在 vCenter 中查看任务通知，请转至 vCenter 的**任务控制台**。

受影响的版本：5.0

## 使用 vCenter 6.5 U2 时，OMIVV 的所有页面中可能会显示 2000002 错误

解决方案：将使用来自 VMware 的最新修补程序用于 6.5 U2，或者迁移到 6.5 U3 和更高版本。

受影响的版本：5.1

## 在执行从较早的 OMIVV 版本到更新 OMIVV 版本的 RPM 升级或备份和恢复后，在 OMIVV 的所有页面中显示 2000002 错误。

在注册当前版本之前，如果在 vCenter 服务器中有较早版本的 OMIVV，则 SSL 握手异常会导致新版本的 OMIVV 不再可访问，直到 vCenter 刷新新的插件数据。因为 vCenter 包含较早版本 OMIVV 的数据，这会以不同的方式处理 SSL 流量。

分辨率：

- 在 vCenter 服务器上重新启动 vSphere Client。
- 如果问题仍然存在：
  - 对于 VMware vCenter Server 设备，请转至 `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity`。对于 Windows vCenter，请转至 vCenter 设备中的 `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity` 文件夹，并查看已存在的旧数据，例如：`com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX`。
  - 手动删除与旧版 OMIVV 相应的文件夹。
  - 为 vSphere Client 重新启动 vSphere Client 服务 (HTML5)

受影响的版本：5.0 及更高版本

## 有时，OMIVV 需要很长时间才能完成 vCenter 取消注册

当您取消注册拥有大量主机（超过 300）的 vCenter 时，OMIVV 会长时间保持加载状态。

解决方案：刷新浏览器。

如果 vCenter 取消注册失败，请再次取消注册 vCenter。

受影响的版本：5.1

## 更新 OMIVV 证书后，将显示“无法连接 OMIVV 设备。SSL 证书无效”错误消息。

解决方案：重新启动 vCenter Client 服务。

受影响的版本：所有

## OMIVV 中的部署作业失败

部署作业失败，因为 LifeCycle Controller 正忙于完成挂起的作业或运行其他作业。

解决方案：执行以下：

1. 在 iDRAC 中清除 iDRAC 作业队列 [可选]
2. 重设 iDRAC
3. 再次运行部署作业

受影响的版本：所有

## 更改 vCenter 密码后，测试连接和清点操作在 OMIVV 中失败

对于 ESXi 版本 6.7 及更高版本，OMIVV 使用智能平台管理接口 (IPMI) 协议检索 ESXi 主机的 iDRAC IP，并且此操作不依赖于 WBEM。

如果由于任何原因 OMIVV 无法检索 iDRAC IP，OMIVV 会尝试使用依赖于 WBEM 状态的通用信息模型 (CIM) 协议（作为回退）。如果用于注册的 vCenter 用户密码已更改，则在运行测试连接和资源清册时可能会遇到与 WBEM 相关的问题。

解决方案：更改 vCenter 密码后，请在 OMIVV 管理控制台中修改 vCenter 凭据，然后在 vCenter 中执行任何操作。有关修改凭据的更多信息，请参阅[修改 vCenter 登录凭据](#) 页面上的 15。

受影响的版本：所有

## 在将 OMIVV 设备重置为出厂设置后，不会从 vCenter 中移除 OMIVV 实例

将设备重置为出厂设置时出现此问题。OMIVV 设备条目保留在 vCenter 的 vsphere-client-serenity 文件夹中，可防止在出厂重置后进行 vCenter 注册。

解决方案：从 vCenter 中移除 OMIVV 条目。有关更多信息，请参阅[我如何从 vCenter 上强制移除 OMIVV 设备](#) 页面上的 137。

受影响的版本：所有

## OMIVV 在“系统配置文件”的“配置文件设置”页面上仅显示 BIOS 和 iDRAC 属性

解决方案：将 Google Chrome 升级到最新版本。

受影响的版本：5.2

## 操作系统部署已完成，但出现未知错误

当您使用其他用户身份（而非用于发现服务器的用户身份）执行操作系统部署时，会出现此问题。OMIVV 日志页面上的错误消息显示未找到类错误。

解决方案：不适用，此问题不会影响 OMIVV 的功能。

受影响的版本：5.2

## FX2 机箱中的机箱管理控制器 (CMC) 固件更新失败

OMIVV 使您能够通过服务器 iDRAC 更新 FX2 机箱 CMC 固件。如果**允许通过操作系统和生命周期控制器更新 CMC** 选项在 iDRAC 中处于禁用状态，则 CMC 固件更新将会失败。

解决方案：在 iDRAC 中执行以下步骤：

1. 转至**设置 > 更新和回滚**。
2. 将**允许通过操作系统和生命周期控制器更新 CMC** 设置为**已启用**。

受影响的版本：5.2

## OMIVV 中的 ISO 配置文件部署失败

在旧版本的 OMIVV 上安排的 ISO 配置文件部署作业在最新版本的 OMIVV 中无效。

解决方案：取消已安排的作业，并根据需要创建部署作业。

如果已安排的作业未取消，部署作业将会失败。在这种情况下，查找裸机服务器，然后创建 ISO 配置文件部署作业。

受影响的版本：5.2

## 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。
- 应在克隆模式中运行 BIOS 配置，以便参考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

默认情况下，主机系统的自动查找功能未启用；而是必须在购买时请求启用。如果在购买时请求启用自动查找，则会在 iDRAC 上启用 DHCP，管理员帐户将被禁用。无需为 iDRAC 配置静态 IP 地址。它会从网络中的 DHCP 服务器获取一个地址。要使用自动查找功能，必须将 DHCP 服务器或 DNS 服务器（或两者）配置为支持查找过程。CSIOR 应在出厂过程中运行。

如果在购买时未申请自动查找，则可以通过以下步骤启用：

1. 在引导过程中按 **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
```

# 系统特定属性

## iDRAC

表. 28: 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
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
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. 29: 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
IscsiDev1Con1Gateway	启动器网关	连接 1 设置
IscsiDev1Con1Ip	启动器 IP 地址	连接 1 设置
IscsiDev1Con1Mask	启动器子网掩码	连接 1 设置
IscsiDev1Con1TargetIp	目标 IP 地址	连接 1 设置

表. 29: BIOS 的系统特定属性 (续)

属性名称	显示属性名称	组显示名称
IscsiDev1Con1TargetName	目标名称	连接 1 设置
IscsiDev1Con2Gateway	启动器网关	连接 1 设置
IscsiDev1Con2Ip	启动器 IP 地址	连接 1 设置
IscsiDev1Con2Mask	启动器子网掩码	连接 1 设置
IscsiDev1Con2TargetIp	目标 IP 地址	连接 1 设置
IscsiDev1Con2TargetName	目标名称	连接 1 设置
IsctlInitiatorName	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. 30: 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. 31: 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
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
IsctlInitiatorChapId	CHAP ID	iSCSI 启动器参数
IsctlInitiatorChapPwd	CHAP 机密	iSCSI 启动器参数

表. 31: CNA 的系统特定属性 (续)

属性名称	显示属性名称	组显示名称
IscsiInitiatorGateway	默认网关	iSCSI 启动器参数
IscsiInitiatorIpAddr	IP 地址	iSCSI 启动器参数
IscsiInitiatorIpv4Addr	IPv4 地址	iSCSI 启动器参数
IscsiInitiatorIpv4Gateway	IPv4 默认网关	iSCSI 启动器参数
IscsiInitiatorIpv4PrimDns	IPv4 主要 DNS	iSCSI 启动器参数
IscsiInitiatorIpv4SecDns	IPv4 次要 DNS	iSCSI 启动器参数
IscsiInitiatorIpv6Addr	IPv6 地址	iSCSI 启动器参数
IscsiInitiatorIpv6Gateway	IPv6 默认网关	iSCSI 启动器参数
IscsiInitiatorIpv6PrimDns	IPv6 主要 DNS	iSCSI 启动器参数
IscsiInitiatorIpv6SecDns	IPv6 次要 DNS	iSCSI 启动器参数
IscsiInitiatorName	iSCSI 名称	iSCSI 启动器参数
IscsiInitiatorPrimDns	主要 DNS	iSCSI 启动器参数
IscsiInitiatorSecDns	次要 DNS	iSCSI 启动器参数
IscsiInitiatorSubnet	子网掩码	iSCSI 启动器参数
IscsiInitiatorSubnetPrefix	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
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. 32: 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

## 附加信息

以下 Dell 技术白皮书和文件可在 [delltechcenter.com](http://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*

## 自定义属性

表. 33: 自定义属性

FQDD	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。
PCIeSSD	PCIeSSDSecureErase	始终禁用

## 组件与基线版本比较值表

表. 34: 组件与基线版本比较值表

偏移类型				
<b>硬件</b>	<b>关联的基线</b>	<b>目标组件</b>	<b>情况说明</b>	<b>合规性状态</b>
	可用	可用	硬件组件与关联的基线匹配。	合规
	可用	可用	组件的硬件属性与关联的基线不匹配。	非合规
	不可用	可用	不计算比较状态，予以忽略。	合规
	可用	不可用	硬件组件在关联的基线中可用，但是组件或属性在主机中不可用。	非合规
	不可用	不可用	不计算比较状态，予以忽略。	合规
<b>固件</b>	<b>关联的基线</b>	<b>目标组件</b>	<b>情况说明</b>	<b>合规性状态</b>
	可用	可用	固件组件版本与关联的基线匹配。	合规
	可用	可用	固件组件版本与关联的基线不匹配。	非合规
	不可用	可用	固件组件版本在关联的基线中不可用，但是组件在主机中可用。 不计算比较状态，予以忽略。	合规
	可用	不可用	不计算比较状态，予以忽略。	合规
	不可用	不可用	不计算比较状态，予以忽略。	合规
<b>驱动程序</b>	<b>关联的基线</b>	<b>目标组件</b>	<b>情况说明</b>	<b>合规性状态</b>
	可用	可用	驱动程序组件版本与关联的基线匹配。	合规
	可用	可用	驱动程序组件版本与关联的基线不匹配。	非合规
	不可用	可用	不计算比较状态，予以忽略。	合规
	可用	不可用	驱动程序组件版本在关联的基线中可用，但是组件在主机中不可用。	非合规
	不可用	不可用	不计算比较状态，予以忽略。	合规

# 响应代码

表. 35: 响应代码

响应代码	说明
200	成功生成/返回任务信息或任务列表。
202	成功启动任何任务。
400	错误请求
401	未经授权的请求
404	未找到
409	冲突
500	内部服务器错误
503	服务不可用