




**OpenManage Integration for VMware vCenter for
Desktop Client
User's Guide Version 3.2**



注、小心和警告

-  注：“注”表示可以帮助您更好地使用计算机的重要信息。
-  小心：“小心”表示可能会损坏硬件或致数据丢失，并说明如何避免此问题。
-  警告：“警告”表示可能会造成数据丢失、人身伤害甚至死亡。

版权所有 © 2016 Dell Inc. 保留所有权利。本产品受美国、国际版权和知识产权法律保护。Dell™和 Dell 徽标是 Dell Inc. 在美国和/或其他管辖区的商標。所有此提及的其他商標和品名可能是其各自所属公司的商標。

2017 - 04

Rev. A00

Contents

1 概	8
OpenManage Integration for VMware vCenter	8
主要功能	8
OpenManage Integration for VMware vCenter 如何助 vCenter Administration	8
OpenManage Integration for VMware vCenter 功能	8
What's new in this release	9
2 OpenManage Integration for VMware vCenter 配置	10
安全角色和限	10
数据完整性	10
控制、授和角色	10
Dell 操作角色	11
Dell 基构部署角色	11
理解限	12
3 配置或 OpenManage Integration for VMware vCenter 的步	14
OpenManage Integration for VMware vCenter 主	14
配置向迎	15
建新的接配置文件 [向]	15
配置事件和警 [向]	16
置代理服器 [向]	16
划源清册作 [向]	17
运行保修索作 [向]	17
配置部署凭据 [向]	17
置默固件更新存 [向]	18
启用 OMSA 接 [向]	18
配置 NFS 共享	19
置概	19
常置概	19
建新的接配置文件	20
配置事件和警	22
关于代理配置	23
运行源清册作	23
划保修作	24
看或部署凭据	24
置固件存	25
用于部署的服器安全置	25
关于主机、裸机和 iDRAC 符合性	26
运行修不符合要求的 vSphere 主机向	27
运行修不符合要求的裸机服器向	28
iDRAC 可符合性	28



升 OpenManage Integration for VMware vCenter.....	28
从用版升到完整品版本.....	29
OpenManage Integration for VMware vCenter 可.....	29

4 端到端硬件管理..... 30

数据中心和主机系.....	30
了解事件和警.....	30
vSphere 客端主机概.....	32
重 iDRAC.....	34
关于源清册划.....	34
修改源清册作划.....	34
Displaying The Inventory For A Single Host System in vCenter.....	35
源清册和可.....	36
看存源清册.....	37
看主机源.....	37
示整个数据中心的硬件配置.....	37
管理接配置文件.....	38
看或有的接配置文件.....	38
除接配置文件.....	40
接配置文件.....	40
刷新接配置文件.....	40
了解 vSphere 客端主机中的系事件日志.....	40
示 Dell Management Center 中的日志.....	41
示个主机的事件日志.....	41
关于固件更新.....	42
运行固件更新向.....	42
更新早的固件版本.....	43
运行群集和数据中心的更新固件向.....	43
使用 vCenter 行高主机管理.....	45
置物理服器正面指示灯.....	45
基于服器的管理工具.....	45
保修索.....	45

5 硬件管理..... 47

置概述.....	47
了解部署作.....	48
部署序中的服器状.....	48
下自定义 Dell ISO 映像.....	48
了解如何配置硬件配置文件.....	49
建新的硬件配置文件.....	49
克隆硬件配置文件.....	51
关于管理硬件配置文件.....	51
看或硬件配置文件.....	52
复制硬件配置文件.....	52
重命名硬件配置文件.....	52
除硬件配置文件.....	52

刷新硬件配置文件.....	52
□建新的虚□机□控程序配置文件.....	52
管理虚□机□控程序配置文件.....	53
VLAN 支持.....	54
□看或□□虚□机□控程序配置文件.....	54
复制虚□机□控程序配置文件.....	55
重命名虚□机□控程序配置文件.....	55
□除虚□机□控程序配置文件.....	55
刷新虚□机□控程序配置文件.....	55
构建新部署模板.....	55
管理部署模板.....	56
运行部署向□.....	56
部署向□ - 步□ 1 : □□服□器.....	57
部署向□步□ 2 : 部署模板.....	57
部署向□步□ 3 : 全局□置.....	57
部署向□步□ 4 : 服□器□□.....	58
部署向□步□ 5 : □接配置文件.....	58
部署向□步□ 6 : □划作□.....	59
了解作□□列.....	59
手□添加服□器.....	60
移除裸机服□器.....	60

6 控制台管理..... 61

基于 Web 的 Administration Console.....	61
使用管理控制台.....	61
使用具有必要□限的非管理□用□注册 vCenter 服□器.....	61
注册 vCenter 服□器.....	63
向管理控制台上□ OpenManage Integration for VMware vCenter □可□.....	66
虚□□□管理.....	66
重新启□虚□□□.....	66
更新存□□位置和虚□□□.....	66
更新虚□□□□件.....	67
下□故障排除包.....	67
□置 HTTP 代理.....	67
□置 NTP 服□器.....	67
生成□□□名□求.....	68
□置全局警□.....	68
管理□份和□原.....	69
配置□份和□原.....	69
□划自□□份.....	69
□行即□□份.....	70
从□份□原数据□.....	70
了解 vSphere Client 控制台.....	70
配置网□□置.....	71
更改虚□□□密□.....	71
□置本地□区.....	71



重新引导虚拟机.....	71
将虚拟机重置出厂设置.....	72
刷新控制台.....	72
从控制台注销.....	72
只读角色.....	72

7 故障排除.....73

常见问题 (FAQ)	73
在注册 OMIVV 分配的 Dell 限制, 在取消注册 OMIVV 后不会删除.....	73
如果 vCenter 处于空闲状态达数小时, OpenManage Integration 网卡和 Management Center 会将 OMIVV 的内容替换为“!”.....	73
如何操作来恢复会话?	73
如何查看重要性, Dell Management Center 不显示所有相关日志。我如何查看所有日志?	73
如何将 OMIVV 插件的状态更改为“已启用”?	73
运行 OpenManage Integration for VMware vCenter 原后, 如果 vSphere Client 中未显示 Dell Management Center 怎么办?	74
在更新后, “关于”屏幕未更新 OMIVV 版本.....	74
不支持使用 OpenManage Integration for VMware vCenter 更新固件版本 13.5.2 的 Intel 网卡。.....	74
在运行保修操作时, 保修操作状态未列在“保修操作列”页面中.....	74
由于 DUP 存在分段要求, 使用 OpenManage Integration for VMware vCenter 将 Intel 网卡从 14.5 或 15.0 更新至 16.x 失败.....	75
在更新使用无效的 DUP 运行固件更新, 尽管 LC 中的操作状态显示“失败”, 但 vCenter 控制台上的硬件更新操作状态在数小时内既非失败也非超时。为什么会发生这种情况?	75
管理仍然显示无法更新的更新存储位置。.....	75
如果使用 DHCP 运行 IP 和 DNS 覆盖, 在重启后, DNS 配置置何回到原始置?	75
当我运行一多固件更新, 为什么我的系统无法进入模式?	75
即便我的存储中包含所有 11G 系统的捆包, 为什么固件更新显示没有固件更新的捆包?	75
在具有 PERC S300 引导控制器的服务器上, 我的 ESXi 部署什么会失败?	76
在更新固件后, 为什么我会看到显示了一条消息?	76
OpenManage Integration for VMware vCenter 在哪一代 Dell 服务器上配置和支持 SNMP 陷阱?	76
OpenManage Integration for VMware vCenter 如何支持三个以上处于连接模式的 vCenter?	76
OpenManage Integration for VMware vCenter 是否支持处于连接模式的 vCenter?	77
什么是 OpenManage Integration for VMware vCenter 的必要端口置?	77
虚拟机成功安装和操作的最低要求是什么?	78
硬件配置文件的用户具有 iDRAC 用户列表中的新更改凭据, 在成功用配置文件后, 用于裸机找到的相同用户的密码什么未更改?	78
为什么在“系统概观”页面的“处理器”中处理器版本中“不适用”?	78
如果使用 DHCP 运行 IP 和 DNS 覆盖, 在重启后, DNS 配置置何回到原始置?	78
为什么我没有在“vCenter 主机和群集”页面上看到我的新 iDRAC 版本的信息?	79
我如何使用 OMSA 模拟温度硬件故障来测试事件置?	79
我在 Dell 主机系统上安装了 OMSA 代理程序, 但我仍然收到“OMSA 未安装”的消息。我怎么办?	79
OpenManage Integration for VMware vCenter 能否支持启用了定制模式的 ESXi?	79
在我使用定制模式失败。.....	79
在更新使用无效的 DUP 运行固件更新, 尽管 LC 中的操作状态显示“失败”, 但 vCenter 控制台上的硬件更新操作状态在数小时内既非失败也非超时。为什么会发生这种情况?	80
我将什么置用于 UserVars.CIMoeMProviderEnable With ESXi 4.1 U1?	80
我使用一台参考服务器构建硬件配置文件, 但构建失败。我怎么办?	80



我在刀片服务器上部署 ESXi，但部署失败。我该怎么办？	80
为什么我的虚拟机管理程序在 R210 II 机器上部署失败？	80
为什么我在部署向导中看到自己找到的系统没有型号信息？	80
使用 ESXi ISO 配置了 NFS 共享，但安装共享位置造成部署失败。	80
我如何限制移除虚拟机？	80
在“立即备份”屏幕中输入密码收到消息	81
我的固件更新失败，我该怎么办？	81
我的 vCenter 注册失败，该怎么办？	81
连接配置文件凭据期间的性能极慢或没有响应。	81
OpenManage Integration for VMware vCenter 是否支持 VMware vCenter 服务器？	81
OpenManage Integration for VMware vCenter 是否支持 vSphere Web 客户端？	81
在管理控制台中，将重新出厂置后，何更新存储路径未置默认路径？	81
在备份和还原 OpenManage Integration for VMware vCenter 后，何警告置没有被还原？	82
Bare Metal Deployment Issues	82
在新系统的系统上启用自己找	82
系统 Dell	82
OpenManage Integration for VMware vCenter 相关信息	83

8 Dell PowerEdge 服务器的虚拟化相关事件..... 84

附录 A: 了解自己找..... 91

自己找前提条件	91
启用或禁用 iDRAC 服务器上的管理	92
手动配置服务器以自行找（第 11 代 PowerEdge 服务器）	92
手动配置 PowerEdge 第 12 代及更高版本服务器以自行找	93



概览

OpenManage Integration for VMware vCenter

VMware vCenter 是 IT 管理员用来管理和监测 VMware vSphere ESXi 主机的主要控制台。在标准虚拟化环境中，VMware 警报和监测用于提示管理员启动另外的控制台来解决硬件问题。现在，管理员可以使用 OpenManage Integration for VMware vCenter 中的新功能来管理和监测虚拟化环境中的 Dell 硬件，例如：

- 警报和环境监测
- 单一服务器监测和报告
- 固件更新
- 增强的部署选项

主要功能

Dell 客户可以使用 OpenManage Integration for VMware vCenter 执行以下操作：

资源清册	资源清册主要资产、执行配置任务，以及提供 Dell 平台的群集和数据中心。
监测和警报	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）。
固件更新	将 Dell 硬件更新到最新版本的 BIOS 和固件
部署和配置	创建硬件配置文件、虚拟机监控程序配置文件，以及在裸机 Dell PowerEdge 服务器上远程或不通过 PXE 而使用 vCenter 部署两者的任何组合。
服务信息	从 Dell 联机检索保修信息。

OpenManage Integration for VMware vCenter 如何协助 vCenter Administration

OpenManage Integration for VMware vCenter 提供附加的虚拟化功能作为 vCenter 当前管理功能的补充：

- 压缩任务并将管理进程（诸如固件更新和裸机部署）添加至 vCenter Server Administration Console。
- 无需预引导执行环境 (PXE) 即可组织多个裸机服务器部署。
- 提供附加情报（资源清册、事件、警报）来诊断服务器问题。
- 与标准 vCenter 验证、规则和权限集成。

OpenManage Integration for VMware vCenter 功能

以下是 OpenManage Integration for VMware vCenter 的高级功能：

- 使用标准 vCenter 事件和警报子系统监测 Dell 服务器
- 执行高级硬件管理和配置

- 不使用 PXE，在裸机系统上执行 VMware ESXi 虚拟机监控程序的零接触部署
- 建立硬件和 VMware ESXi 虚拟机监控程序配置文件
- 执行固件更新
- 对基础结构问题进行故障排除
- 在数据中心和群集视图上生成报告 - 导出至 CSV 文件
- 将 OpenManage Integration for VMware vCenter 功能与标准 vCenter 角色和权限集成

What's new in this release

This release of OpenManage Integration for VMware vCenter provides the following features:

- Support for Dell OpenManage Server Administrator (OMSA) version 8.5
- Support for VMware vCenter server version 6.0 U3
- Support for VMware ESXi version 6.0 U3
- Support for PowerEdge R830 platform
- Support for Non-Uniform Memory Access (NUMA) Fault Resilient Memory (FRM)



OpenManage Integration for VMware vCenter 配置

以下几节提供 OpenManage Integration for VMware vCenter 初始配置的逐步说明，同时也提供了升级、卸载和安全角色信息等内容。

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，以避免任何可能会造成问题的不当请求。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 Client 或 Web Client 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，创建拥有必要权限的角色，分配角色给用户，使用此用户注册 vCenter，并包括以上两个 Dell 角色。

数据完整性

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

安全 Administration Console 会话具有五分钟闲置超时，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。如果用户尝试在新窗口或选项卡中打开会话，则会创建一个安全错误，要求有效的会话。此操作还会阻止用户单击任何可能会尝试攻击 Administration Console 会话的恶意 URL。



图 1: 错误消息

访问控制验证、授权和角色

OpenManage Integration for VMware vCenter 使用 vSphere 客户端的当前用户会话和为虚拟设备存储的管理凭据来执行 vCenter 操作。OpenManage Integration for VMware vCenter 使用 vCenter 服务器内置的角色和权限模式来授权用户对虚拟设备和 vCenter 管理的对象（主机和群集）执行操作。

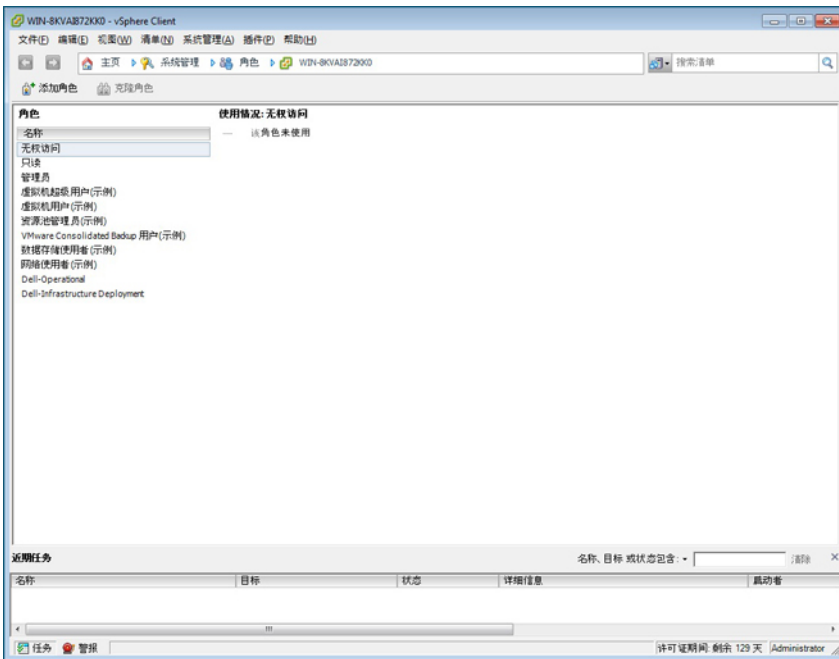


图 2: vCenter vSphere 客户端角色和权限

Dell 操作角色

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. 1: 权限组

Group Name (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、监测器
权限组 — Dell.Reporting (未使用)	创建报告、运行报告

Dell 基础结构部署角色

此角色包含专门与虚拟机监管程序部署功能相关的权限。



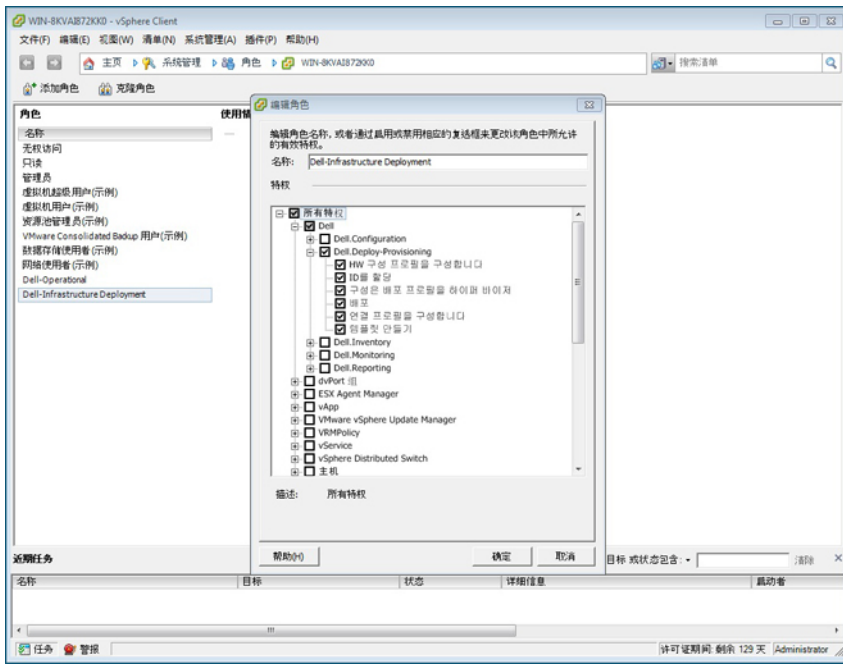


图 3: Dell 基础结构部署角色

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

Dell.Deploy — 配置 创建模板、配置硬件配置配置文件、配置虚拟机管理程序部署配置文件、配置连接配置文件、分配标识、和部署

理解权限

OpenManagement Integration for VMware vCenter 执行的每一项操作都有相关联的权限。以下几节列出了可用操作和关联的权限：

- Dell.Configuration.Perform vCenter-Related Tasks
 - 退出和进入维护模式
 - 使 vCenter 用户组能查询权限
 - 注册和配置警报，例如，在事件设置页上启用/禁用警报
 - 将事件/警报发布到 vCenter
 - 在事件设置页上配置事件设置
 - 在事件设置页上恢复默认警报
 - 在配置警报/事件设置时检查群集的 DRS 状态
 - 在执行更新或其它配置操作后重新启动主机
 - 监测 vCenter 任务状态/进程
 - 创建 vCenter 任务，例如：固件更新任务、主机配置任务和资源清册任务
 - 更新 vCenter 任务状态/进程
 - 获得主机配置文件
 - 将主机添加到数据中心
 - 将主机添加到群集
 - 将配置文件应用到主机
 - 获得 CIM 凭据

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



配置或编辑 OpenManage Integration for VMware vCenter 的步骤

完成 OpenManage Integration for VMware vCenter 的基本安装后，您可以继续运用本节中后续所述的以下方法之一来配置设备：

- 使用配置向导的配置任务
- 使用设置选项配置任务

两种方法中的用户界面类似，不同之处在于向导中是单击 *保存并继续*，而在“设置”选项中是单击 *应用*。

使用配置向导的配置任务

可以在使用配置向导配置 OpenManage Integration for VMware vCenter 时使用以下任务：

1. [配置向导欢迎页面](#)
2. [创建新的连接配置文件](#)
3. [配置事件和警报](#)
4. [设置代理服务器](#)
5. [计划资源清册作业](#)
6. [运行保修检索作业](#)
7. [配置部署凭据](#)
8. [设置默认固件更新存储库](#)
9. [启用 OMSA 链接](#)

使用设置选项配置任务

可使用以下任务来设置或编辑 OpenManage Integration for VMware vCenter 配置任务：

- [创建新的连接配置文件](#)
- [配置事件和警报](#)
- [设置代理服务器](#)
- [修改资源清册作业计划](#)
- [保修检索](#)
- [查看或编辑部署凭据](#)
- [设置固件存储库和凭据](#)
- [启用 OMSA 链接](#)

OpenManage Integration for VMware vCenter 主页

登录 OpenManage Integration for VMware vCenter 主页时，导航按钮位于左窗格中，而右窗格则提供有用的链接和信息。此种设计提供指向最常用任务的重要链接。尽管在左窗格导航下可以找到所有任务，但也能在“概览”页上找到它们，使用十分方便。此页面上提供的任务属于以下类别：

- **主机和服务器部署**
该部分提供关于主机和服务器部署的更多信息。
- **vSphere 主机和裸机服务器符合性**
该部分提供更多信息，并且可让您查看关于不符合要求的主机或裸机服务器，或如何运行向导以修补这些不符合要求问题的详细信息。
- **资源清册计划**
在该部分中，可以了解更多关于资源清册计划的信息。
- **保修数据检索计划**
该部分可让您了解更多信息或查看/更改保修计划。
- **许可**
在此部分可了解更多关于许可的信息。可使用链接转至各种许可任务。在“主机连接许可证”中，可以实时查看主机连接许可证。此外，还可以使用“立即购买”链接来购买完整版许可证以管理多个主机。只有在使用演示版许可证时，“立即购买”链接才会出现。在“vCenter 连接许可证”中，您可以查看与 VMware vCenter 连接许可证相关的信息。
- **事件和警报设置**
了解更多关于事件和警报设置的信息，或使用链接来配置它们。

配置向导欢迎页面

在安装 OMV 后，必须对其进行配置。

1. 在 **vSphere Client** 中，从主页上的**管理**选项卡，单击 **Dell Management Center** 图标。
初次单击 **Dell Management Center** 图标时，它将打开**配置向导**。您还可以在 **Dell Management Center** → **设置**页面中访问此向导。
2. 在**欢迎**选项卡中，审阅各步骤，然后单击**下一步**。

创建新的连接配置文件 [向导]

连接配置文件用于存储由虚拟设备用来与 Dell 服务器通信的凭据。每台 Dell 服务器都必须与一个连接配置文件关联，以便 OMV 对其进行管理。可以将多台服务器分配到单个连接配置文件。在配置向导中以及在 Dell Management Center 的**设置**选项卡下创建连接配置文件的过程类似。可以将 OMV 配置为使用 Active Directory 凭据连接到 iDRAC 和主机。在使用与连接配置文件关联的 Active Directory 凭据之前，Active Directory 中必须存在 Active Directory 用户帐户，并且必须为 iDRAC 和主机配置基于 Active Directory 的验证。iDRAC 和主机可以有相同的 Active Directory 凭据，也可以分别设置 Active Directory 凭据。用户凭据必须具有管理权限。

 **注:** 如果安装在使用第 12 代及更高代系的 Dell PowerEdge 服务器的主机上，则不需要安装 OMSA 代理程序。如果安装在第 11 代服务器上，则会在部署过程中自动安装 OMSA 代理程序。

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

要使用向导创建新的连接配置文件，请执行以下步骤：


1. 从 **连接配置文件**选项卡，单击 **新建**。
2. 在**配置文件名称与说明**面板中，输入配置文件名称以及可选的说明信息（用于帮助管理自定义的连接配置文件），然后单击**下一步**。
3. 在**关联的主机**部分中，选择要与连接配置文件关联的主机，然后单击**下一步**。
4. 查看关于凭据和连接协议的信息，然后单击 **下一步**。
5. 在 **iDRAC** 面板中，键入 iDRAC 凭据信息。
 - a. 对于要在其上使用 Active Directory 且已配置并启用 Active Directory 的 iDRAC，请选中**使用 Active Directory**复选框；否则，请配置 iDRAC 本地凭据。输入**用户名、密码和验证密码**。用户名最多可包含 16 个字符（包含空格）。密码必须匹配，并仅使用可打印的 ASCII 字符。
 - b. 对于 **证书检查**，选择 **启用**以下载并存储 iDRAC 证书，并且在将来所有的连接中对其进行验证，或者选择 **禁用**，从而不执行检查也不保存证书。



6. 单击 **Next**（下一步）。
7. 在**主机**面板中，执行以下操作：
 - a. 必须选中**使用 Active Directory** 复选框以启用 Active Directory 凭据。请输入“用户名”、“密码”和“验证密码”。
 - b. 如果未选中**使用 Active Directory**，则输入 **root** 用户的**密码**和**验证密码**。这些密码必须匹配。
 - c. 对于**证书检查**，选择**启用**以下载并存储 OMSA/ESXi 证书，并且在将来所有的连接中对其进行验证，或者选择**禁用**，从而不执行检查也不保存证书。
8. 单击**下一步**。
9. **测试连接**窗口将测试在选定服务器上输入的 iDRAC 和主机 root 凭据。测试连接是可选操作，但建议执行此操作。
 - 要开始测试，请选择主机，然后单击**测试选定项**。其他选项将被禁用。
 - 要在完成前中止所有测试，可单击**中止所有测试**。
10. 要完成配置文件，可单击 **保存**。
11. 要继续配置事件和警报，可单击 **保存并继续**。


配置事件和警报 [向导]


使用“配置向导”配置事件和警报，或从 Dell Management Center 中“事件”和“警报”的“设置”选项中进行配置。为了从服务器接收事件，OMIVV 被配置为陷阱目标。对于第 12 代及之后的主机，在 iDRAC 中设置 SNMP 陷阱目标。对于第 12 代之前的主机，陷阱生成在 OMSA 中设置。


 **注：对于第 12 代及之后的主机，OMIVV 支持 SNMP v1 和 v2 警报。对于第 12 代之前的主机，OMIVV 仅支持 SNMP v1 警报。**

要配置事件和警报，请执行以下步骤：

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

 **注：启用警报的 Dell 主机通过进入维护模式来响应严重事件。**
3. 在显示的对话框中，单击**继续**以接受此更改，或单击**取消**。

 **注：仅当选择对 Dell 主机启用警报时才会看到该步骤。**
4. 要恢复所有管理的 Dell 服务器的默认 vCenter 警报设置，可单击 **还原默认警报**。
可能需要片刻才能使更改生效。
5. 要继续向导，可单击 **保存并继续**。

 **注：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。要解决此问题，请在 OMIVV GUI 中的**管理** → **设置**选项卡上手动更改事件和警报设置。**

设置代理服务器 [向导]

在配置向导中设置代理服务器，或稍后使用 Dell Management Center **设置** → **代理**页面进行设置。


要设置代理服务器：

1. 在**配置 HTTP 代理**中，执行以下操作之一：
 - 若不使用代理服务器，可单击 **保存并继续**。
 - 要使用代理服务器，可在**设置**下输入**代理服务器地址**。
2. 输入**代理端口号**。

3. 如有必要，可选中**所需的凭据**复选框。
4. 如果选中**所需的凭据**，则执行以下操作：
 - a. 在**代理用户名**文本框中，键入代理用户名。
 - b. 在**代理密码**文本框中，键入代理密码。
 - c. 在**验证密码**文本框中，再次键入代理密码。
5. 在**代理下**，选中**使用代理**复选框。
6. 要保存这些选项并继续，可单击 **保存并继续**。

计划资源清册作业 [向导]

配置向导中的资源清册计划配置与 **Dell Management Center** → **设置**选项中的资源清册计划配置相类似。区别仅仅在于向导提供立即运行资源清册的选项。

 **注:** 为确保 OMIVV 继续显示更新的信息，建议您计划一个周期性资源清册作业。资源清册作业消耗最少的资源，且不会降低主机性能。

要计划资源清册作业：


1. 在 **配置向导的资源清册计划**窗口中，执行以下操作之一：
 - 要运行资源清册计划，可单击 **在选定的日期**。
 - 如果不运行资源清册计划，可选择 **请勿在 Dell 主机上运行资源清册**。
2. 如果选择**在选定的日期**，则执行以下操作：
 - a. 选中一周中要运行资源清册的日期旁边的复选框。
 - b. 在文本框中，以 HH:MM（小时：分钟）格式输入时间。
您输入的时间是当地时间。因此，如果您想要在虚拟设备的时区运行资源清册，请计算当地时间与虚拟设备时区之间的时差，然后输入适当的时间。
3. 要应用更改并继续，可单击 **保存并继续**。

运行保修检索作业 [向导]

向导中的保修检索作业配置与 **Dell Management Center** → **设置**选项中的配置类似。此外，可从作业队列立即运行保修检索作业。

要运行保修检索作业：


1. 在 **配置向导的保修计划**窗口中，执行以下操作之一：
 - 要运行保修计划，可单击 **在选定的日期**。
 - 要不运行保修计划，选择 **不检索保修数据**。
2. 如果选择 **在选定的日期**，则执行以下操作：
 - a. 选中一周中要运行保修作业的日期旁边的文本框。
 - b. 在文本框中，以 HH:MM（小时：分钟）格式输入时间。
您输入的时间是当地时间。因此，如果您想要在虚拟设备的时区运行资源清册，请计算当地时间与虚拟设备时区之间的时差，然后输入适当的时间。
3. 要应用更改并继续，可单击 **保存并继续**。

 **注:** OMIVV 连接到 Internet 以获取主机的保修信息。根据您的网络设置，您可能需要配置代理以成功运行保修作业。

配置部署凭据 [向导]

部署凭据用于与通过 AutoDiscovery 查找到的裸机系统安全通信。为了与 iDRAC 安全地通信，OMIVV 从初始查找起直到部署过程结束，始终使用部署凭据。部署完成后，这些凭据将更改为部署期间关联的连接配置文件中的凭据。如果更改了部署凭据，则从更改点起新查找到的所有系统将使用新凭据来配置；但是，更改前已查找到的服务器上的凭据不会受影响。



 **注: OMIVV 用作配置服务器。在 Auto Discovery 过程中, 部署凭据用于与使用插件作为配置服务器的 iDRAC 进行安全通信。**



配置部署凭据:

1. 在**部署凭据**窗口中, 可以查看或更改凭据。
2. 要更改这些凭据, 在**用于裸机服务器部署的凭据**下, 执行以下操作:
 - a. 在**用户名**文本框中, 编辑用户名。
 - b. 在**密码**文本框中, 编辑密码。
 - c. 在**验证密码**文本框中, 确认密码。
3. 要保存指定的凭据并继续配置向导, 请单击**保存并继续**。

设置默认固件更新存储库 [向导]


固件存储库设置包含用于更新部署的服务器的固件目录位置。可以先在向导中设置固件存储库, 或稍后从 Dell Management Center “设置”选项中进行设置。此外, 稍后您也可以从 OpenManage Integration 选项卡运行固件更新。

要设置默认固件更新存储库:

1. 要在**配置向导**中的**固件存储库**页面上选择固件更新的默认存储库, 可选择以下操作之一:
 - Dell 联机
默认固件存储库 (ftp.dell.com) 具有分级文件夹。OMIVV 下载选定的固件更新, 并将其存储在分级文件夹中, 然后在需要时应用它们。
 **注: OMIVV 连接到 Internet 以获取适用于您的主机的目录和固件软件包。根据您的网络设置, 您可能需要配置代理以从 Dell 联机成功运行固件更新任务。**
 - 本地/共享存储库
这些存储库使用 Dell Repository Manager 应用程序进行创建。此本地存储库应为网络共享。OMIVV 支持 NFS 和 CIFS 共享。
2. 如果选择**本地/共享存储库**, 则执行以下操作:
 - a. 使用以下格式输入**目录文件位置**:
 - xml 文件的 NFS 共享: host:/share/filename.xml
 - gz 文件的 NFS 共享: host:/share/filename.gz
 - xml 文件的 CIFS 共享: \\host\share\filename.xml
 - gz 文件的 CIFS 共享: \\host\share\filename.gz
 - b. 如果使用 CIFS 共享, 则输入**用户名、密码以及验证密码**, 密码必须匹配。这些字段只有在输入 CIFS 共享时处于活动状态。
 **注: 共享网络文件夹的用户名/密码中不支持 @ 字符。**
 - c. 要验证输入, 可单击**开始测试**。
3. 要保存该选择并继续**配置向导**, 可单击**保存并继续**。

启用 OMSA 链接 [向导]

要在 OMIVV 虚拟设备内启动 OMSA, 必须安装并配置 OMSA Web Server。有关如何安装和配置 Web Server 的说明, 请参阅 *Dell OpenManage Server Administrator Installation Guide* (Dell OpenManage Server Administrator 安装指南)。

 **注: 仅在 Dell 服务器第 12 代以前的版本上需要 OMSA。**

使用 OMSA 可以:

- 管理 vCenter 元素 (传感器/组件级别的详细运行状况信息)。

- 清除命令日志和系统事件日志 (SEL)。
 - 获取 NIC 统计数据。
 - 确保 OMIVV 从选定主机捕获事件。
1. 在 **配置向导** 中的 **OpenManage Server Admin** 页面上，使用 **OMSA Web 服务器 URL** 文本框输入 OMSA URL。必须输入包括 HTTPS 的完整 URL。
 2. 要保存该 URL 并完成配置向导，可单击 **完成**。

配置 NFS 共享

要将 NFS 共享配合 OMIVV 一起使用以进行备份和还原操作、固件更新以及作为分级文件夹，必须完成某些配置项目。CIFS 共享不需要额外配置。


配置 NFS 共享：

1. 在托管 NFS 共享的 Linux 或 Unix 操作系统的计算机上，编辑 `/etc/exports` 以添加：`/share/path <appliance IP> (rw) *(ro)`。

这将允许虚拟设备对共享的完全读写访问权限，但会将其他所有用户限制为只读。

2. 启动 nfs 服务：

```
service portmap start service nfs start service nfslock status
```

 **注：**上述步骤可能会因使用的 Linux 发行版而有所不同。

3. 如有任何服务已经运行：

```
exportfs -ra
```

设置概览

OpenManage Integration for VMware vCenter 的“设置”部分：

- 列出 OpenManage Integration for VMware vCenter 的配置设置。
- 启动初始“配置向导”，带领您逐步完成在 VMware vCenter 中管理和部署服务器时需使用的 OpenManage Integration for VMware vCenter 功能。
- 启动 OpenManage Integration for VMware vCenter 管理控制台，帮助您执行 vCenter 注册、虚拟设备管理、警报管理以及 OpenManage Integration for VMware vCenter 数据库备份/还原。

常规设置概览

常规设置用于：

- 定义 OpenManage Server Administrator (OMSA) URL。
- 启用或禁用保修期满通知。

可以执行以下任务：

可以执行以下任务：

- **常规：**设置 vCenter 中 Dell 主机选项卡上显示的 OMSA URL。您还可以启用或禁用保修期满通知。
- **事件和警报：**启用或禁用所有硬件警报（当前警报状态在 Alarms [警报] 选项卡上显示）。还可配置传入事件和警报过滤。
- **HTTP 代理：**在与 Internet 站点通信期间启用或禁用代理使用。
- **资源清册计划：**设置 vCenter 主机资源清册计划。
- **保修计划：**设置 Dell Online (Dell 在线) 的 Dell 主机保修信息检索计划。
- **部署凭据：**设置在自动查找和裸机服务器部署期间用于与 Dell 服务器通信的凭据。
- **固件存储库：**让您编辑固件存储库的存储位置。



- [安全防护](#)：提供限制服务器部署的服务器白名单。

在第 11 代 Dell PowerEdge 服务器上，要求 OMSA 代理以执行以下操作：

- 详细的主机资源清册。
- 从主机接收事件。
- 检索组件级运行状况信息。
- 清除命令日志和系统事件日志 (SEL)

 **注：仅在第 12 代 Dell PowerEdge 服务器以前的 Dell 服务器上需要 OMSA。**

保修期满通知可用于：

- 监测保修期满日期。
- 设置剩余最少保修天数阈值，超出该值将生成警告或严重警报。警报在主机的 OpenManage Integration 选项卡中显示为一个图标。

相关任务：

- [启用配置向导之外的 OMSA 链接](#)
- [启用或禁用服务器保修期满通知](#)

启用配置向导之外的 OMSA 链接

要在 OpenManage Integration for VMware vCenter 虚拟设备内启动 OpenManage Server Administrator (OMSA)，必须安装并配置 OMSA Web Server。有关如何安装和配置 Web Server 的说明，请参阅所使用的 OMSA 版本的 *Dell OpenManage Server Administrator Installation Guide*（Dell OpenManage Server Administrator 安装指南）。

 **注：仅在第 12 代 Dell PowerEdge 服务器以前的 Dell 服务器上需要 OMSA。**

启用 OMSA 链接：

1. 在 **Dell Management Center** 的 **设置** → **常规** 下的 OMSA 启动程序中，单击 **编辑**。
2. 使用 **OMSA Web 服务器 URL** 文本框输入 OMSA 的 URL。您必须输入带有 HTTPS 和端口号 1311 的完整 URL。
3. 要保存此 URL，请单击 **应用**。

 **注：有关设置 OMSA 陷阱目标的信息，请参阅[设置 OMSA 陷阱目标](#)。**

启用或禁用服务器保修期满通知

在控制保修设置时，可从 Dell 联机检索服务器保修信息。可使用此页面为主机和群集启用或禁用服务器保修到期通知。可在 Dell Management Center 的“设置”、“常规”页面设置或编辑此功能。

要启用或禁用服务器保修期满通知：

1. 在 **Dell Management Center** 中，单击 **设置** → **常规**。
2. 要启用通知，请单击 **常规** 页中右侧的“编辑”按钮。
3. 选中 **启用保修状态通知** 复选框。
4. 要设置 **最少天数阈值警报**，请执行以下操作：
 - a. 要设置警告，请在 **警告** 下拉列表中选择关于服务器保修状态警告的天数。
 - b. 要设置严重保修状态，请在 **严重** 下拉列表中选择针对严重服务器保修状态发出警告的天数。
5. 要应用更改，请单击 **应用**。

创建新的连接配置文件


连接配置文件存储虚拟设备用来与 Dell 服务器通信的凭据。每个 Dell 服务器只能与一个连接配置文件相关联，以便 OpenManage Integration for VMware vCenter 对其进行管理。可以将多个服务器分配给单个连接配置文件。在配置向导中创建

连接配置文件的过程与在 Dell Management Center 中创建连接配置文件的过程相似。可以在首次访问 Dell Management Console 时运行配置向导，或者稍后在“连接配置文件”窗口上运行配置向导。

 **注:** 有关许可的更多信息，请参阅“关于 OpenManage Integration for VMware vCenter 许可”。如果添加的主机数目超出许可证的限制，您将无法创建连接配置文件。

要创建新的连接配置文件：

1. 在 **OpenManage Integration for VMware vCenter** 中的左侧窗格中，单击**连接配置文件**。
2. 单击**新建链接**。
3. 在**配置文件名称与说明**页面中，输入**连接配置文件名称**以及可选的**连接配置文件说明**（它们用于帮助管理自定义的连接配置文件）。
4. 在**关联的主机**页面中，选择连接配置文件的主机并单击**下一步**。
5. 在**凭据**页面中，阅读凭据信息并单击**下一步**。
6. 在凭据下方的 iDRAC 页面中，请执行以下操作之一：

 **注:** iDRAC 帐户需要用于更新固件、应用硬件配置文件并部署虚拟机监控程序的管理权限。

- 对于已针对 Active Directory 配置和启用的 iDRAC（将在其上使用 Active Directory），请选择**使用 Active Directory** 复选框；否则，请跳到配置 iDRAC 凭据步骤。
 - 在 **Active Directory 用户名** 文本框中，键入用户名。按照下列格式之一键入用户名：域\用户名或域/用户名或用户名@域。用户名不得超过 256 个字符。有关用户名的限制信息，请参阅 Microsoft Active Directory 说明文件。
 - 在 **Active Directory 密码** 文本框中，键入密码。密码不得超过 127 个字符。
 - 在 **验证密码** 文本框中，再次键入密码。
 - 在“证书检查”下拉列表中，选择下列其中一项：
 - * 如需下载和存储 iDRAC 证书并在将来的所有连接中对其进行验证，请选择**启用**。
 - * 如不执行检查也不保存证书，请选择**禁用**。
- 要在无需 Active Directory 的情况下配置 iDRAC 凭据，请执行以下操作：
 - 在 **用户名** 文本框中，键入用户名。用户名不得超过 16 个字符。有关您的 iDRAC 版本的用户名限制信息，请参阅 iDRAC 说明文件。

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

- 在 **密码** 文本框中，键入密码。密码不得超过 20 个字符。
- 在 **验证密码** 文本框中，再次键入密码。
- 在“证书检查”下拉列表中，选择下列其中一项：
 - * 如需下载和存储 iDRAC 证书并在将来的所有连接中对其进行验证，请选择**启用**。
 - * 如不执行检查也不保存 iDRAC 证书，请选择**禁用**。

7. 单击**下一步**。
8. 在“凭据”下方的“主机凭据”页面中，请执行以下操作之一：
 - 对于已针对 Active Directory 配置和启用的主机（将在其上使用 Active Directory），请选择**使用 Active Directory** 复选框；否则，请跳到配置主机凭据步骤。
 - 在 **Active Directory 用户名** 文本框中，键入用户名。按照下列格式之一键入用户名：域\用户名或域/用户名或用户名@域。用户名不得超过 256 个字符。有关用户名的限制信息，请参阅 Microsoft Active Directory 说明文件。
 - 在 **Active Directory 密码** 文本框中，键入密码。密码不得超过 127 个字符。
 - 在 **验证密码** 文本框中，再次键入密码。



- 在“证书检查”下拉列表中，选择下列其中一项：
 - * 如需下载和存储主机证书并在将来的所有连接中对其进行验证，请选择**启用**。
 - * 如不执行检查也不保存主机证书，请选择**禁用**。
- 要在无需 Active Directory 的情况下配置主机凭据，请执行以下操作：
 - 在**密码**文本框中，键入 root 用户的密码。密码不得超过 127 个字符。
 - 在**验证密码**文本框中，再次键入密码。
 - 在“证书检查”下拉列表中，选择下列其中一项：
 - * 如需下载和存储主机证书并在将来的所有连接中对其进行验证，请选择**启用**。
 - * 如不执行检查也不保存主机证书，请选择**禁用**。

9. 单击**下一步**。

10. **测试选定项**链接可用于验证为选定服务器提供的 iDRAC 和主机凭据。

- 要开始测试，请选择主机，然后单击**测试选定项**。其他选项处于非活动状态。
- 要中止所有运行中的连接测试，单击**中止测试**。

 **注：**对于既没有 iDRAC Express 也没有 iDRAC Enterprise 的服务器，iDRAC 测试连接的结果表示不适用于该系统。

11. 要完成配置文件，可单击**保存**。

要管理连接配置文件，请参阅[管理连接配置文件](#)。

配置事件和警报

Dell Management Center Events and Alarms（Dell 管理中心事件和警报）页面可启用或禁用所有硬件警报。当前警报状态在 vCenter Alarms（vCenter 警报）选项卡上显示。严重事件表示实际或即将发生的数据损失或系统故障。警告事件并不一定是重大事件，但可表示将来可能的问题。事件和警报还可以使用 VMware Alarm Manager 启用。事件在“主机和群集”视图中的“vCenter 任务和事件”选项卡中显示。

 **注：**在版本早于第 12 代 Dell PowerEdge 服务器的主机上，该功能需要在 OMSA 中将虚拟设备配置为陷阱目标，以在 vCenter 中显示主机事件。有关 OMSA 的更多信息，请参阅[设置 OMSA 陷阱目标](#)。

您可以在事件和警报的设置选项下配置 Dell Management Center 中使用的事件和警报。

要配置事件和警报：

1. 在 Dell Management Center 中的**设置** → **事件和警报**下，单击**编辑**。
2. 在**事件发布等级**下，选择以下各项之一：
 - 不要发布任何事件 - 阻止硬件事件。
 - 发布所有事件 - 发布所有硬件事件。
 - 仅发布严重和警告事件 - 仅发布严重和警告级别的硬件事件。
 - 仅发布虚拟化相关的严重和警告事件 - 仅发布虚拟化相关的严重和警告事件；这是默认的事件发布级别。
3. 要启用所有硬件警报和事件，可选中 **对 Dell 主机启用警报**复选框。

 **注：**启用警报的 Dell 主机通过进入维护模式来响应严重事件。

4. 在显示的对话框中，单击**继续**以接受此更改，或单击**取消**。
5. 要恢复所有管理的 Dell 服务器的默认 vCenter 警报设置，可单击**还原默认警报**。可能要花费一分钟才能使更改生效。
6. 要保存，请单击**保存**。

关于代理配置

代理设置定义 HTTP 代理以及用于从 Web（包括从 Dell 在线）检索信息的任何所需凭据，例如：

- 启用或禁用代理服务器
- 输入所需的代理服务器和端口号
- 定义任何所需的凭据 - 用户名和密码

相关任务：

- [设置代理服务器](#)
- [使用 HTTP 代理检索基于 Web 的数据](#)
- [使用管理控制台设置 HTTP 代理](#)

设置代理服务器

OMIVV 可能需要使用代理信息来访问 Internet，具体取决于您的网络设置。代理设置可用于执行以下任务（如果适用）：

- 检索主机的保修信息
- 从 Dell 联机检索固件目录和相应的固件组件
- 在设备升级期间连接到 Dell 联机。

可在“配置向导”中设置代理服务器，或在以后使用设置选项“HTTP 代理”进行设置。

 **注：代理密码不能超过 31 个字符。**

要在 OMIVV 中设置代理的详细信息，请执行以下操作：

1. 在 **Dell Management Center** 中，选择**设置** → **HTTP 代理**，然后单击**编辑**。
2. 输入代理端口号。
3. 如有必要，可选中**所需的凭据**复选框。
4. 如果选中**所需的凭据**，则执行以下操作：
 - a. 在 **代理用户名**文本框中，输入代理用户名。
 - b. 在 **代理密码**文本框中，输入代理密码。
 - c. 在 **验证密码**文本框中，再次输入刚才输入的代理密码。
5. 在**代理**下，选中**使用代理**复选框。
6. 要保存这些选项，请单击**应用**。

使用 HTTP 代理检索基于 Web 的数据

要使用 HTTP 代理检索基于 Web 的数据：

1. 在 **Dell Management Center** 中，选择**设置 HTTP 代理**，然后单击**编辑**。
2. 选中 **使用代理**复选框。
3. 单击**应用**。
4. 要验证设置，可单击**测试连接**。

运行资源清册作业

要运行资源清册作业：

1. 一旦**配置向导**完成，将针对添加到连接配置文件的所有主机自动触发资源清册作业。要后续按需运行资源清册作业，请单击**作业队列** → **资源清册** → **立即运行**以运行资源清册作业。
2. 要查看资源清册作业的状态，可单击 **刷新**。



3. 导航至**主机和群集**视图，单击任何 **Dell 主机**，然后单击 **OpenManage Integration** 选项卡。将提供以下信息：

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

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

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


- 闪烁指示灯
- 运行固件更新向导
- 启动远程访问
- 启动 OMSA
- 启动 CMC

计划保修作业

可随时从 **Dell Management Center** → **设置** → **保修计划** 页面中运行保修作业计划。此时**保修检索**页面被禁用。此时，可从**作业队列** → **保修历史** 页面中运行保修检索作业。

计划保修检索作业：

1. 在 **Dell Management Center** 中，选择**设置** → **保修计划**。
2. 在 **保修计划** 窗口中，单击**编辑**。
3. 要配置计划，请执行以下操作之一：
 - a. 要运行保修计划，可单击 **在选定的日期**。
 - b. 如果不需要运行保修计划，请选择**不检索保修数据**。
4. 如果选择 **在选定的日期**，则执行以下操作：
 - a. 选中您要运行保修作业的每个星期几旁边的复选框。
 - b. 在文本框中，以 HH:MM（小时：分钟）格式输入时间。
输入的时间是当地时间。然后计算在正确的时间运行保修作业所需的时差。
5. 要立即运行保修作业，请导航到**作业队列** → **保修历史**，然后单击 **立即运行**。

 **注：**OMIVV 连接到 Internet 以获取主机的保修信息。根据您的网络设置，您可能需要配置代理以成功运行保修作业。

查看或编辑部署凭据

在 Dell Management Center 中，您可以编辑部署凭据。部署凭据用于在操作系统部署完成之前，与自动查找到的 Dell 裸机服务器进行安全通信。一旦部署完成，在成功执行操作系统部署后，将设置在相关联的连接配置文件中提供的 iDRAC 凭据。如果更改了部署凭据，则在凭证更改后查找到的裸机服务器将使用新凭据进行通信。在凭据更改前查找到的服务器上的凭据不会受此更改的影响。用户名长度不应超过 16 个字符（仅限 ASCII 可打印字符）。密码长度不应超过 20 个字符（仅限 ASCII 可打印字符）。

要查看或编辑部署凭据：

1. 在 **Dell Management Center** → **设置** → **部署凭据** 中，单击**编辑**。
2. 在 **裸机服务器部署的凭据** 中的 **凭据** 下，执行以下操作：
 - 在**用户名**文本框中，输入用户名。
用户名不应该超过 16 个字符（只能使用 ASCII 可打印字符）。

- 在**密码**文本框中，输入密码。
密码不应该超过 20 个字符（只能使用 ASCII 可打印字符）。
- 在**验证密码**文本框中，再次输入密码。
密码必须匹配。

3. 单击**应用**。


设置固件存储库

要设置固件存储库和凭据：

1. 在 **OpenManage Integration for VMware vCenter** 中，选择**设置** → **固件存储库**，然后单击**编辑**。
2. 要在**固件存储库**页面选择固件更新的默认存储库，可选择以下操作之一：
 - **Dell 联机**
这使用具有所需的暂存文件夹的 Dell 联机 (ftp.dell.com) 的默认固件更新存储库。OpenManage Integration for VMware vCenter 下载所选的固件更新，并将其存储在暂存文件夹中，然后在需要时应用它们。
 - **共享网络文件夹**
使用 Lifecycle Controller 的主机可以从托管在可访问网络共享文件夹中的自定义存储库进行更新。要创建自定义存储库，Dell 建议使用 Dell Repository Manager 创建该存储库，然后将其保存到主机和 OpenManage Integration 可以访问的共享位置。在下方输入存储库目录文件的位置。
3. 如果选择**共享网络文件夹**，则在**目录文件位置**字段中输入目录文件的完整路径。
4. 单击**开始测试**。
5. 单击**应用**。

用于部署的服务器安全设置

使用白名单限制可部署的服务器组。如果服务器位于白名单中，它会在自动查找和握手进程期间获得凭据，并在用于部署的服务器列表中显示。白名单通过手动添加服务器服务标签、删除服务标签或从 CSV 文件导入服务标签列表进行维护。

 **注：使用 CSV 分隔符的文件导入服务器。** 此文件在不同的行中包含多条记录，其中每条记录有一个或多个逗号分隔的服务标签。

要设置和管理白名单，请从以下各项中选择：

- [启用服务器白名单](#)
- [将服务器添加到白名单](#)
- [从白名单删除服务器](#)

启用可部署服务器白名单

有关可部署服务器安全设置的信息，请参阅[用于部署的服务器安全设置](#)。

要启用服务器白名单：

1. 在 **Dell Management Center** 的左侧窗格中，选择 **设置**。
2. 在右侧窗格中，选择**安全保护**。
3. 在 **安全保护**窗口中，单击 **编辑**。
4. 要使用白名单限制服务器部署，请选中 **强制服务器白名单**复选框。
5. 单击**应用**，服务器白名单设置将更改为“已启用”。

将可部署服务器添加到白名单

有关可部署服务器安全设置的信息，请参阅[用于部署的服务器安全设置](#)。强制执行时，只有服务器白名单上的 Dell 服务器可用于使用 OpenManage Integration for VMware vCenter 进行部署。您可以手动或使用列表导入，将可部署服务器添加到白名单。



要将可部署服务器添加到白名单：

1. 在 **Dell Management Center** 的左侧窗格中，选择 **设置** → **安全保护**。
2. 在 **服务器白名单**窗口中，单击 **编辑**，然后执行以下操作之一：
 - 要手动将服务器添加到白名单，请单击 **添加服务器**。
 - 在 **添加服务标签**对话框中，输入服务标签。
 - 要添加标签，请单击 **继续**。
 - 要导入服务标签列表，请单击 **导入白名单**。
 - 显示 **选择要上载的文件**对话框时，导航到 CSV 文件，然后单击**打开**。

ASDFG12

SDCNRD0

TESCVD3

AS243AS、ASWERF3、FGVCSD9

- 显示 **在您的文件中找到这些服务标签**对话框时，单击 **应用**。

此时，这些服务标签将在服务标签列表中显示。

从白名单删除可部署服务器

有关可部署服务器安全设置的信息，请参阅[用于部署的服务器安全设置](#)。


要从白名单删除可部署服务器：

1. 在 **Dell Management Center** 的左侧窗格中，选择**设置**。
2. 在右侧窗格中，选择**安全保护**。
3. 在 **安全保护**窗口中，单击 **编辑**。
4. 请执行以下操作之一：
 - 要删除单个服务器，请单击 **服务标签**复选框，然后单击 **删除所选项**。
 - 要删除所有服务器，请单击 **服务标签**复选框，然后单击 **删除所选项**。
5. 显示**是否确定要删除所选的服务标签**对话框时，单击 **应用**，或单击**取消**以取消。
6. 要完成更改，请单击 **应用**。

关于主机、裸机和 iDRAC 符合性问题

要使用 OpenManage Integration for VMware vCenter 管理主机、裸机服务器和 iDRAC，它们必须符合特定的最低标准。如果不符合要求，则无法通过 OpenManage Integration for VMware vCenter 正确地管理它们。使用 [Fix Non-Compliant Hosts, Bare Metal Server, and iDRAC](#)（修补不符合要求的主机、裸机服务器和 iDRAC）符合性链接查看您配置中的哪些主机/裸机服务器/iDRAC 不符合要求并进行修补。此向导显示主机/裸机服务器/iDRAC，其中：

- 主机未分配给连接配置文件。
如果连接配置文件没有分配到主机，将提供一个对话框让您转到连接配置文件屏幕。此配置在向导之外。稍后返回以运行此向导。
- 重新引导时收集系统资源清册（CSIOR）已禁用或尚未运行，需要手动重新引导。
- OMSA 代理（主机根凭据）未安装、已过时或没有正确配置。
- 裸机服务器有过时的集成的 Dell Remote Access Controller (iDRAC) 固件、Lifecycle Controller (LC) 固件或 BIOS 版本。

 **小心:** 处于 Lockdown (锁定) 模式下的主机在符合性检查中将不会显示 (如果这些主机不符合要求)。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。这种情况下将显示警告。

在每种情况下, 您都需要通过运行以下操作之一修补符合性问题:

- 要修补 vSphere 主机符合性问题, 请参阅 [运行修补不符合要求 vSphere 主机向导](#)
- 要修补有符合性问题的裸机服务器, 请参阅 [运行修补不符合要求裸机服务器向导](#)
- 要修补 iDRAC 符合性问题: [iDRAC 许可证符合性](#)

相关信息:

- [重新检查裸机服务器符合性](#)

运行修补不符合要求的 vSphere 主机向导

运行“修补不符合要求的 vSphere 主机向导”可修补不符合要求的主机。有关符合性的信息, 请参阅[关于主机和裸机符合性问题](#)。某些不符合要求的 ESXi 主机需要重新引导。如果必须安装或更新 OpenManage Server Administrator (OMSA), 则 ESXi 主机需要重新引导。此外, 从未运行 CSIOR 的所有主机都需要重新引导。如果您选择自动重新引导 ESXi 主机, 请进行以下操作:

- 对于 CSIOR 状态修补:
如果未在主机上启用 CSIOR, 您可以在主机上启用 CSIOR, 然后将该主机设为维护模式并重新引导。
- 对于 OMSA 状态修补:
 - a. OMSA 已安装在主机上。
 - b. 主机设置为维护模式并重新引导。
 - c. 重新引导完成后, 将配置 OMSA 以使更改生效。
 - d. 此时主机将脱离维护模式。
 - e. 系统将运行资源清册以刷新数据。

要运行修补不符合要求的 vSphere 主机向导:

1. 在 **Dell Management Center** 的左侧窗格中, 单击**符合性** → **vSphere 主机**。
2. 在 **vSphere 主机符合性**窗口中, 查看不符合要求的主机, 然后单击 **修补不符合要求的 vSphere 主机**。
3. 在 **修补不符合要求的 vSphere 主机**向导中, 选中您要修补的主机的复选框。
4. 单击 **Next (下一步)**。
5. 如果服务器没有连接配置文件, 您可以选择退出该向导并从**连接配置文件**页面修复这些系统, 或继续此向导。请参阅[创建新的连接配置文件](#)。完成后, 请返回至此向导。
6. 在 **开启 CSIOR**窗口中, 选中复选框以打开所选主机的 **CSIOR**。
7. 单击 **Next (下一步)**。
8. 在 **修补 OMSA**窗口中, 选中复选框以修补所选主机的 **OMSA**。
9. 单击 **Next (下一步)**。
10. 在 **重新引导主机**窗口中, 查看必须重新引导的 ESXi 主机。如果必须安装或更新 OMSA, 则 ESXi 主机需要重新引导。此外, 从未运行 CSIOR 的所有主机都需要重新引导。执行以下操作之一:
 - 如果要将主机自动置于维护模式并在需要时重新引导, 请选中**自动将主机置于维护模式并在需要时重新引导**复选框。
 - 如果要手动重新引导, 您必须执行以下操作:
 1. 一旦主机的 **安装 OMSA** 任务完成后, 就重新引导该主机。
 2. 一旦主机运行, 如果 OMSA 未配置, 请手动配置 OMSA 或使用符合性向导。
 3. 重新运行资源清册, 请参阅 [运行资源清册作业](#)。
11. 单击 **Next (下一步)**。
12. 在 **摘要**窗口中, 查看在不符合要求主机上进行的操作。需要手动重新引导才能使这些更改生效。
13. 单击**完成**。



运行修补不符合要求的裸机服务器向导

运行“修补不符合要求的裸机服务器”可修补不符合要求的裸机服务器。有关符合性的信息，请参阅[关于主机和裸机符合性问题](#)。

要运行修补不符合要求的裸机服务器向导：

1. 在 **Dell Management Center** 的左侧窗格中，单击 **符合性** → **裸机服务器**。
2. 在 **裸机服务器** 窗口中，查看不符合要求的主机，然后单击 **修补不符合要求的裸机服务器**。
3. 在 **修补裸机服务器** 向导中，选中您要修补的主机的复选框。
4. 单击 **Next (下一步)**。
5. 在 **摘要** 窗口中，查看在不符合要求裸机服务器上进行的操作。
6. 单击 **完成**。

重新检查裸机服务器符合性

对于在 OpenManage Integration for VMware vCenter 之外安装的服务器，必须运行该手动服务器符合性重新检查。可以在 Dell Management Center 的符合性下的裸机服务器页面上找到该内容。

要重新检查裸机服务器符合性：

1. 在 **Dell Management Center** → **符合性** → **裸机服务器** 页面中，单击 **重新检查符合性**。
2. 要在 **不符合要求的服务器** 窗口中刷新列表，可单击 **刷新**。
3. 要运行重新检查，可单击 **检查符合性**。
4. 要中止重新检查，可单击 **中止所有测试**。
5. 如果成功修复系统，将刷新列表，并且会从列表中移除系统。如果修复失败，则不符合要求的系统仍保留在列表上。
6. 完成时单击 **完成**。

 **注：**OMIVV 要求 BIOS、LC 和 iDRAC 固件至少达到 OMIVV 正常工作所需的最低符合性级别。对于其 BIOS、LC 或 iDRAC 固件低于所需符合性级别的 Dell 服务器，请参阅 *Using Dell™ Repository Manager to Create a Deployment Media (Bootable ISO) to Perform Systems Updates*（使用 Dell™ Repository Manager 创建部署介质 [可引导 ISO] 以执行系统更新）以手动更新固件。

iDRAC 许可证符合性


当您选择 iDRAC 许可证符合性页面时，它将运行符合性测试。此测试持续几分钟时间。此页面中列出的 vSphere 主机和裸机服务器不符合要求，因为它们没有兼容的 iDRAC 许可证。该表显示 iDRAC 许可证的状态。在此页面上，您可以查看许可证的剩余天数并根据需要进行更新。如果您的 [运行资源清册作业](#) 链接已禁用，这意味着没有由于 iDRAC 许可证导致不符合要求的 vSphere 主机。如果 [重新检查裸机服务器符合性](#) 链接已禁用，这意味着没有由于 iDRAC 许可证导致不符合要求的裸机服务器。

1. 在 **Dell Management Center** 的左侧窗格中，单击 **符合性**。
2. 展开 **符合性**，然后单击 **iDRAC 许可证**。
一旦您到达此页面，就会运行符合性测试。这与您单击 **刷新** 时运行的测试相同。
3. 如果您的许可证已过时，请单击 **购买/更新 iDRAC 许可证**。
4. 登录到 **Dell 许可证管理** 页面，然后更新或购买新的 iDRAC 许可证。
使用此页面上的信息标识并更新您的 iDRAC。
5. 安装 iDRAC 许可证后，运行 vSphere 主机的资源清册作业并在资源清册作业完成后返回到此页面。对于裸机服务器，请重新检查授权的裸机服务器符合性。

升级 OpenManage Integration for VMware vCenter

以下是 OpenManage Integration for VMware vCenter 的升级情况：

- [从试用版升级到完整产品版本](#)

 **注:** 开始升级之前执行设备备份。请参阅[执行即时备份](#)。

从试用版升级到完整产品版本

要从试用版升级到完整产品版本：

1. 转至 [Dell 网站](#) 并购买完整产品版本。
您还可以在 OpenManage Integration for VMware vCenter 中使用其中一个 **立即购买** 链接访问 Dell 网站，如位于管理门户的 **许可** 窗口中的链接。仅当您使用的是评估许可证时，此操作才适用。
2. 下载将包括新的完整版产品以及一个新的许可证文件。
3. 启动浏览器窗口并输入您要配置的虚拟机对应的 **vSphere vCenter Console** 选项卡中显示的 **Administration Console URL**，或使用来自 **Dell Management Console** → **设置** 页面的链接。该 URL 使用以下格式并且不区分大小写：**https://<设备 IP 地址>**
4. 在 **Administration Console** 登录窗口中，输入密码并单击 **登录**。
5. 要上载许可证文件，可单击 **上载**。
6. 在 **上载许可证** 窗口中，单击 **浏览** 导航到许可证文件。
7. 选择该许可证文件，然后单击 **上载**。

OpenManage Integration for VMware vCenter 许可

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

- 评估许可证 — 当 OMIVV 3.2 版本设备首次开机时，将自动安装评估许可证。试用版中包含一个评估许可证，可供 OpenManage Integration for VMware vCenter 管理的五个主机（服务器）使用。此许可证仅适用于 Dell 第 11 代和更高版本的服务器，它是默认许可证，具有 90 天试用期。
- 标准许可证 — 完整产品版本中包含一个标准许可证，可用于最多 10 个 vCenter 服务器。您可以购买任何数量的由 OMIVV 管理的主机连接。

从评估版许可证升级到完整标准版许可证时，您将收到一封有关订单确认的电子邮件，您可以从 Dell Digital 商店 <http://www.dell.com/support/licensing> 下载许可证文件。将许可证 .XML 文件保存到本地系统，然后使用 **管理控制台** 上载新的许可证文件。

许可中表达以下信息：

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

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

购买许可证时，可从 Dell Digital 商店 <http://www.dell.com/support/licensing> 下载 .XML 文件（许可证密钥）。如果您无法下载许可证密钥，请转至 www.dell.com/support/softwarecontacts 找到您的产品对应的区域 Dell 支持电话号码，联系 Dell 支持部门。



端到端硬件管理

端到端硬件管理的目标是提供系统运行状况和最新的基础结构信息，管理员需要这些信息以便在不离开 Dell Management Center 或 vCenter 的情况下，对严重硬件事件作出响应。OpenManage Integration for VMware vCenter 中的端到端硬件管理被分为四个单独的部分：

- 监测
- 资源清册
- 高级主机管理
- 保修检索

监测数据中心和主机系统

数据中心和主机系统监测通过在 vCenter 中的“任务和事件”选项卡上显示硬件（服务器和存储）和虚拟化相关事件，使管理员可以监测基础结构运行状况。此外，严重硬件警报可以触发 OpenManage Integration for VMware vCenter 警报。为 Dell 虚拟化相关事件定义的少量警报可使被管理的主机系统进入维护模式。

要执行监测：

1. 配置**事件和警报**设置。
2. 根据需要配置 **SNMP OMSA 陷阱目标**。
3. 使用 vCenter 中的**任务和事件**选项卡查看事件信息。

了解事件和警报

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

有四种事件发布级别。

表. 2: 事件发布级别说明

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

当您配置事件和警报时，可以启用它们。启用后，严重硬件警报可触发 OpenManage Integration for VMware vCenter 将主机系统置于维护模式，并且在某些情况下，将虚拟机迁移到另一个主机系统。OpenManage Integration for VMware vCenter 会转发


从管理的 Dell 主机收到的事件，并创建这些事件的警报。使用这些警报可触发来自 vCenter 的操作，如重新引导、维护模式或迁移。例如，当双电源设备发生故障并且创建警报后，导致的操作是将该计算机上的虚拟机迁移到一台新计算机。

仅当您请求时，主机才会进入或离开维护模式。如果主机进入维护模式时处于群集中，您可以选择清空关闭电源的虚拟机。如果选择此选项，则每个关闭电源的虚拟机都将迁移到另一台主机，除非群集中没有可用于虚拟机的兼容主机。处于维护模式时，主机不允许部署或打开虚拟机。在进入维护模式的主机上运行的虚拟机需要迁移到另一台主机或关闭，该操作可手动完成或通过 VMware 分布式资源调度 (DRS) 自动进行。

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


如果需要还原默认警报设置，您可使用 Reset Default Alarm（重置默认警报）按钮完成此操作。此按钮可以方便地还原默认警报配置而无需卸载和重新安装产品。如果有任何 Dell 警报配置在安装后更改，则这些更改可使用此按钮恢复。

 **注: 要接收 Dell 事件，必须启用这些事件。**

 **注: OpenManage Integration for VMware vCenter 会预先选择对主机成功运行虚拟机来说至关重要的虚拟化相关事件。默认情况下，Dell 主机警报已禁用。如果启用 Dell 警报，群集应使用 VMware Distributed Resource Scheduler (VMware 分布式资源计划程序) 确保发送严重事件的虚拟机自动迁移。**

了解第 11 代 Dell PowerEdge 主机的 OMSA

在第 12 代以前的 PowerEdge 服务器上，必须安装 OMSA 才能使用 OpenManage Integration for VMware vCenter。OMSA 将在部署期间自动安装在第 11 代 Dell PowerEdge 主机上。您也可以根据需要进行手动安装。

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

要在第 11 代 Dell PowerEdge 服务器上配置 OMSA，请选择以下项：

- [将 OMSA 代理部署到 ESXi 系统上](#)
- [设置 OMSA 陷阱目标](#)

将 OMSA 代理部署到 ESXi 系统

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

 **注: 在早于 Dell PowerEdge 第 12 代服务器的 Dell 主机需要 OpenManage 代理。使用 OpenManage Integration for VMware vCenter 安装 OMSA，或手动安装到主机，然后再安装 OpenManage Integration for VMware vCenter。有关手动安装代理的详细信息，请访问 <http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.openmanage-server-administrator-omsa.aspx>。**

1. 如果尚未安装，请安装 vSphere 命令行工具 (vSphere CLI)，该工具可从 <http://www.vmware.com> 获取。
2. 请输入以下命令：

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

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

设置 OMSA 陷阱目标

所有第 11 代主机都必须配置 OMSA。

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



要设置 OMSA 陷阱目标：

1. 使用 **设置** → **常规**中找到的指向 OMSA 用户界面的链接，或从 Web 浏览器导航至 OMSA 代理 (<https://<HostIP>:1311/>)。
2. 登录到界面，并选择 **警报管理**选项卡。
3. 选择**警报操作**，并确保所有被监测的事件都已设置**广播消息**选项，以便发送出事件。
4. 选择选项卡顶部的 **平台事件**项。
5. 单击灰色的 **配置目标**按钮，并单击 **目标**链接。
6. 选中 **启用目标**复选框。
7. 在**目标 IP 地址**字段中输入 OpenManage Integration for VMware vCenter 设备 IP 地址。
8. 单击**应用更改**。
9. 重复步骤 1 到步骤 8 以配置附加事件。

查看事件

要查看事件，执行以下操作之一：

- 导航至虚拟机并右键单击以显示 **vCenter** → **任务和事件**选项卡，然后单击 **事件**，以便显示所选等级的事件。
- 单击主机的父节点（群集或数据中心）或 vCenter 的根文件夹。

事件仅显示在 vSphere 树中的这些节点上。

vSphere 客户端主机概览

本概览提供关于主机服务器重要属性的信息，包括单个组件的运行状况、标识、虚拟机监控程序以及固件信息。

硬件组件运行状况

组件运行状况是所有主要主机服务器组件的状况的图示，包括系统机架、电源设备、温度、风扇、电压、处理器、电池、入侵、硬件日志、电源管理，以及内存。可用的状态表示有：

- 正常（绿色复选标记）— 组件正常运行
- 警告（带有感叹号的黄色三角形）— 组件有非严重错误
- 严重（红色 X）— 组件有严重故障
- 未知（问号）— 组件的状态未知

右上角的标题栏中将显示全局运行状况。

服务器信息

服务器信息提供标识、虚拟机监控程序和固件信息，例如：

- 主机名称、电源状态、iDRAC IP、管理 IP、使用中的连接配置文件、型号、服务标签和资产标签编号、剩余保修天数，以及最后一次执行资产清册扫描的时间。
- 虚拟机监控程序、BIOS 固件以及 iDRAC 固件版本。
- 十条最新的系统事件日志条目。单击“详细信息”以启动**系统事件日志**窗口，其中显示更多日志详细信息。

主机信息

在主机概览的左侧窗格中，可以找到指向以下主机信息类型的链接：

- 系统事件日志
显示硬件系统事件日志信息。请参阅[了解系统事件日志](#)。
- 硬件资源清册

显示关于以下硬件设备的信息：

- 现场可更换部件 (FRU)，如 DIMM、系统板、电源设备、背板、控制器卡等。
- 内存 — 可用插槽和使用中的插槽数量、最大容量和使用中的内存数量，以及单个 DIMM 的详细信息。
- 网络接口卡 (NIC) — 已安装的卡的数量，以及单个 NIC 的详细信息。
- PCI 插槽 — 可用的总数量、使用中的数量，以及单个插槽的详细信息。
- 电源设备 — 存在的数量和单个 PSU 的详细信息。
- 处理器 — 存在的数量和单个 CPU 的详细信息。
- 远程访问卡 — IP 地址信息、RAC 类型和 Web 界面 URL。

请参阅[关于资源清册作业](#)。

• 存储

主机系统存储提供图形化详细信息视图（关于连接到基于主机的存储控制器的存储器的物理和逻辑存储容量与类型），包括：

- 主机系统总存储量、未配置的量、已配置的量，以及全局的和专用的热备用磁盘容量
- 列出每个存储组件有多少出现在系统组件数据表（此表包含该组件的详细信息）中

• 固件

运行“固件更新向导”或查看固件版本。请参阅[固件更新](#)。

• 电源监测

主机系统电源监测提供常规电源信息、能量统计数据以及备用电源信息，包括：

- 当前电源预算、配置文件、警告和故障阈值
- 能耗、系统峰值电量，以及电流强度统计信息
- 备用电源，以及峰值备用容量

 **注：并非所有电源设备都支持该功能，并且不支持刀片机柜电源设备。**

• 保修

保修检索提供 Dell 服务器的以下信息：

- 仅传输主机服务标签时，更新的服务保修信息
- 按计划的间隔更新的保修信息
- 使用代理服务器和凭据进行安全传输
- 通过经测试的安全连接传输信息

请参阅[保修检索](#)。

主机操作

主机操作是在当前主机服务器上执行的命令，例如：

- 使用“闪烁指示灯”以使 LCD 前部指示灯闪烁。请参阅[设置物理服务器正面指示灯](#)。
- 使用“运行固件更新向导”以显示固件更新向导并更新主机服务器固件。请参阅[运行固件更新向导](#)。
- 使用 iDRAC 重设在不重新引导主机的情况下重设 iDRAC。

请参阅[重设 iDRAC](#)。

管理控制台

管理控制台用于启动外部系统管理控制台，例如：

- 单击“远程访问控制台”以启动 Integrated Dell Remote Access Controller (iDRAC) Web 用户界面。
- 如果已进行配置，则单击 OMSA 控制台以启动 OpenManage Server Administrator (OMSA) 用户界面。请参阅[启用 OMSA 链接](#)




- 单击“刀片机箱控制台”以启动 Chassis Management Controller (CMC) Web 用户界面。

重设 iDRAC

有时 iDRAC 可能不会响应 OpenManage Integration for VMware vCenter 发出的请求。从这种状态恢复的唯一方法是重设 iDRAC。iDRAC 重设执行 iDRAC 的正常重新引导。这样的重新引导不会重新引导主机。在执行重设之后，iDRAC 可能需花费 1 到 2 分钟才能恢复到可用状态。

当 iDRAC 在重新引导时，您可能会看到：

- OpenManage Integration for VMware vCenter 获取其运行状况时发生一些延迟或通信错误。
- 所有与 iDRAC 的当前会话关闭。
- iDRAC 的 DHCP 地址可能会改变。如果 iDRAC 使用 DHCP 作为其 IP 地址，则有可能该 IP 地址将改变。如果发生这种情况，请重新运行主机资源清册任务以捕获资源清册数据中的新 iDRAC IP

 **注：**有时软重设 iDRAC 可能无法让 iDRAC 恢复到可用状态。可能需要进行硬重设。要执行硬重设，请关闭服务器电源，卸下电源电缆 2 分钟再重新连接。有关重设 iDRAC 的更多信息，请参阅您的 iDRAC 版本的用户指南。

 **注：**Dell 建议您在重设 iDRAC 前将主机置于维护模式。


1. 在 vSphere 客户端中的资源清册标题下，选择主机和群集。
2. 从主机和群集中，在树形视图中选择主机系统，然后选择 **OpenManage Integration** 选项卡。
3. 在主机操作下，选择 **iDRAC 重设**。
4. 在 iDRAC 重设对话框上，选择**继续 iDRAC 重设**，然后单击**确定**。

关于资源清册计划

资源清册计划设置运行资源清册作业的时间/日期，例如：

- 每周的选定日子和特定时间
- 按照设置的时间间隔

大部分 OpenManage Integration for VMware vCenter 功能需要先完成资源清册以收集所需的数据。必须收集所有主机系统的资源清册以显示此信息。要执行主机系统上的资源清册，请创建提供通信和身份验证信息的连接配置文件。一旦资源清册完成，就可以查看单个主机系统的资源清册结果。

 **注：**要确保资源清册包含最新的信息，可计划至少每周运行一次资源清册作业。资源清册作业消耗的资源很少，不会降低主机性能。


相关任务：

- [运行资源清册作业](#)
- [修改资源清册作业计划](#)
- [显示单个主机系统的资源清册](#)
- [显示数据中心硬件配置和状态](#)

修改资源清册作业计划

资源清册计划设置运行资源清册作业的时间/日期，例如：

- 每周的特定时间和所选日期
- 需要按照设置的时间间隔完成资源清册，以收集大多数 OpenManage Integration for VMware vCenter 功能所需的数据。

 **注：**要确保资源清册包含最新的信息，应该至少每周运行一次资源清册作业。资源清册作业消耗的资源很少，不会降低主机性能。

要修改资源清册作业计划：

1. 从 Dell Management Center 选择 **设置** → **资源清册计划**。
2. 要更改当前计划，可单击 **编辑**。
3. 选择 **在选定的日期**选项按钮，然后选中一周中的日期的复选框，并且输入时间。单击 **清除**以清除条目。
4. 要更改资源清册计划，可单击 **应用**；要取消资源清册计划，则单击 **取消**。
5. 要立即运行作业，可从管理中心选择 **作业队列**，然后选择 **资源清册历史**选项卡。
6. 单击 **立即运行**。
7. 要更新 **上次资源清册作业**的详细信息，可单击 **刷新**。

Displaying The Inventory For A Single Host System in vCenter

To display the inventory for a single host system:

1. From the vSphere Client's Home, select **Hosts and Clusters**.
2. From **Hosts and Clusters**, in the left pane, select the host system, and then select the **OpenManage Integration** tab.
3. An overview of the selected host is displayed.

The overview provides information on key host server attributes, including individual component health, identification, hypervisor, and firmware information.

- Hardware Component Health is a graphical representation of the status of all major host server components: system chassis, power supply, temperature, fans, voltage, processors, batteries, intrusion, hardware log, power management, and memory. The available status states are:

- Healthy (green check mark) - component operating normally
- Warning (yellow triangle with exclamation point) - component has a non-critical error
- Critical (red X) - component has a critical failure
- Unknown (question mark) - status is unknown for the component

A global health status is displayed in the upper-right header bar.

- Server Information provides identification, hypervisor, and firmware information, such as:
 - Host name, power state, iDRAC IP address, Management IP address, connection profile in use, model, service tag and asset tag numbers, number of days left on the warranty, and when the last inventory scan was performed
 - Hypervisor, BIOS firmware, and iDRAC firmware versions
 - Fault Resilient Memory (FRM): This is a BIOS attribute and is enabled in the BIOS during initial setup of the sever and displays the memory operational mode of the server. You need to restart your system when you change memory operational mode value. This is applicable for R620, R720, T620, M620 and 13th generation servers with ESXi 5.5 or later version. The four different values are:
 - * Enabled and Protected: This value indicates that the system is supported and the operating system version is ESXi 5.5 or later, and the memory operational mode in BIOS is set to FRM.
 - * Enabled and Not Protected: This value indicates that the memory operational mode in BIOS is set to FRM, but the operating system does not have support for this feature.
 - * Disabled: This value indicates that it supports valid systems with any operating system version and here memory operational mode in BIOS is not set to FRM.
 - * Blank: If memory operational mode in BIOS is not supported the FRM attribute is not displayed.
 - Non-Uniform Memory Access (NUMA) Fault Resilient Memory (FRM): NUMA FRM is a new memory operating mode available on the BIOS settings of high-end Dell's 13th generation of PowerEdge systems with at least two or four processors. This mode establishes an area of memory that is fault-resilient on all CPUs, providing the same protection to the hypervisor against uncorrectable memory errors that would affect it, as well as maintaining NUMA memory functionality and performance. The four different values are:
 - * NUMA Enabled and Protected: This value indicates that the system is supported and the operating system version is ESXi 5.5 or later, and the memory operational mode in BIOS is set to NUMA FRM.



- * NUMA Enabled and Not Protected: This value indicates that the memory operational mode in BIOS is set to NUMA FRM, but the operating system does not have support for this feature.
 - * Disabled: This value indicates that it supports valid systems with any operating system version and here memory operational mode in BIOS is not set to NUMA FRM.
 - * Blank: If memory operational mode in BIOS is not supported the NUMA FRM attribute is not displayed.
- Recent System Log Entries provide the 10 most recent system event log entries. To launch the **System Event Log** window that displays additional log details, click **Details**.
4. Under **Host Information**, click **Hardware Inventory** to display a list and further details on all components installed in host system, including:
 - Field-replaceable units (FRUs) - DIMMS, system planar, power supplies, backplanes, controller cards, and so on.
 - Memory - Number of slots available and in use, maximum capacity and amount of memory in use, and details on individual DIMMs.
 - Network Interface Cards (NICs) - Number of installed cards and details on individual NICs.
 - PCI Slots - Total available and number in use, and details on individual slots.
 - Power Supplies - Number present and details on individual PSUs.
 - Processors - Number present and details on individual CPUs.
 - Remote Access Card - IP address information, RAC type, and Web interface URL.
 5. Under **Host Information**, click **Storage** to display a graphic and detailed view of the capacity and type of physical and virtual storage, including:
 - Host system total storage, unconfigured, configured, and global hot spare disk capacity.
 - List of how many of each storage component is present in the system.
 - Component data table that contains detailed information on that component.
 6. Under **Host Information**, click **Firmware** to display all Dell Lifecycle Controller firmware information including:
 - Update name - BIOS, Dell Lifecycle Controller, power supply, and so on.
 - Update type - BIOS, firmware, or application.
 - Individual update details - Version, installation time, if an update is in progress or the update status, and the update version. The update status and version only have data when an update is scheduled, and the update version is the firmware version to which the system will be updated.
 7. Under **Host Information**, click **Power Monitoring** to display general power information, energy statistics, and reserve power information, including:
 - Current power budget, profile, warning and failure thresholds.
 - Energy consumption, system peak power, and amperage statistics.
 - Reserve power and peak reserve capacity.
 8. Under **Host Information**, click **Warranty** to display system warranty information including:
 - Warranty provider name and description of the warranty.
 - Start and end dates and how many days are left on the warranty.
 - Status of the warranty (Active, Expired) and when the warranty information was last updated.

资源清册和许可

如果无法检索和显示服务器数据，可能有几种原因：

- 服务器没有与连接配置文件关联，因此无法完成资源清册任务。
- 未在服务器上运行用于收集数据的资源清册任务，因此没有内容可以显示。
- 已超过主机许可证的数量，必须拥有额外的可用许可证才能完成资源清册任务。
- 服务器没有第 12 代及更高版本服务器所需的正确 iDRAC 许可证，必须购买正确的 iDRAC 许可证。

“立即购买”链接用于首次购买产品，而不是用于升级。仅当使用评估许可证时，才会显示“立即购买”链接。

相关任务：

- [查看并编辑现有的连接配置文件](#)
- [修改资源清册作业计划](#)

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

- 评估许可证：试用版中包含一个演示许可证，可用于由 OpenManage Integration for VMware vCenter 管理的五个主机（服务器）。
- 标准许可证：完整产品版本中包含可用于 10 个 vCenter 的产品许可证，以及已购买的由 OpenManage Integration for VMware vCenter 管理的主机连接数。

相关任务：

- [关于 OpenManage Integration for VMware vCenter 许可](#)
- [向管理控制台上载 OpenManage Integration for VMware vCenter 许可证](#)

查看存储资源清册

主机系统存储提供图形化详细信息视图（关于连接到基于主机的存储控制器的存储器的物理和逻辑存储容量与类型），包括：

- 主机系统总存储量、未配置的量、已配置的量，以及全局热备用磁盘容量
- 列出每个存储组件有多少出现在系统中
- 包含该组件的详细信息的组件数据表

要查看存储数据：

1. 在 **vSphere 客户端** 中选择主机，然后选择 **OpenManage Integration** 选项卡。
2. 在左侧窗格中，单击**主机信息**下的**存储**。
3. 在 **存储**页面中，查看图形摘要，或使用表格以及 **查看**和 **筛选器**下拉列表以对资源清册信息进行排序。

查看主机电源监测

主机系统电源监测提供常规电源信息、能量统计数据以及备用电源信息，包括：

- 当前电源预算、配置文件、警告和故障阈值
- 能耗、系统峰值电量，以及电流强度统计信息
- 备用电源，以及峰值备用容量

要查看主机电源监测：

1. 在 **vSphere 客户端** 中选择主机，然后选择 **OpenManage Integration** 选项卡。
2. 在左窗格中，单击**主机信息**下的**电源监测**。
3. 在**电源监测**页面，查看此主机的电源。

显示整个数据中心的硬件配置

您必须完成资源清册作业，然后才能显示整个数据中心的硬件配置。一旦运行资源清册，即可以查看以下任何一项：

- 硬件：现场可替换部件
- 硬件：处理器
- 硬件：电源设备
- 硬件：内存
- 硬件：NIC
- 硬件：PCI 插槽
- 硬件：远程访问卡



- 存储：物理磁盘
- 存储：虚拟磁盘
- 固件
- 电源监测
- 保修

显示整个数据中心的硬件配置：

1. 从 **vSphere 客户端** 中的 **资源清册** 标题下，选择 **主机和群集**。
2. 在 **主机和群集** 中，在树形视图中选择一个数据中心，然后选择 **OpenManage Integration** 选项卡。
3. 此时将显示数据中心中所有主机的概览。使用 **查看** 下拉列表可查看资源清册类别。
4. 使用 **筛选器** 文本框可输入资源清册数据的筛选器。
5. 要刷新显示的 **资源清册**，可单击 **刷新**。

管理连接配置文件

连接配置文件将访问和部署凭据与一组主机系统关联并通常包含：

- 配置文件名称和唯一的说明（帮助进行配置文件管理）
- 与连接配置文件关联的主机列表
- iDRAC 凭据
- 主机凭据
- 创建日期
- 修改日期
- 最近修改的用户

运行 **配置向导** 后，通过 OpenManage Integration for VMware vCenter **管理选项卡** → **模板和配置文件** 使用以下操作管理凭据配置文件：


- [创建连接配置文件](#)
- [查看并编辑现有的连接配置文件](#)
- [删除连接配置文件](#)
- [测试连接配置文件](#)
- [刷新连接配置文件](#)

查看或编辑现有的连接配置文件

配置连接配置文件后，您可以编辑配置文件名称、说明、关联的主机以及 iDRAC 和 OMSA 代理凭据。

要查看或编辑现有的连接配置文件：

1. 在 OpenManage Integration for VMware vCenter 中，选择 **连接配置文件**。
2. 在 **可用的配置文件** 下，选择要查看或编辑的配置文件，然后单击 **编辑/查看**。
3. 在 **配置文件名称与说明** 页面中，输入 **连接配置文件名称** 以及可选的 **连接配置文件说明**（它们用于帮助管理自定义的连接配置文件）。
4. 在 **关联的主机** 页面中，选择连接配置文件的主机并单击 **下一步**。
5. 在 **凭据** 页面中，阅读凭据信息并单击 **下一步**。
6. 在凭据下方的 iDRAC 页面中，请执行以下操作之一：

 **注：** iDRAC 帐户需要用于更新固件、应用硬件配置文件并部署虚拟机监控程序的管理权限。

- 对于已针对 Active Directory 配置和启用的 iDRAC（将在其上使用 Active Directory），请选择**使用 Active Directory** 复选框；否则，请跳到配置 iDRAC 凭据步骤。
 - 在 **Active Directory 用户名** 文本框中，键入用户名。按照下列格式之一键入用户名：域\用户名或域/用户名或用户名@域。用户名不得超过 256 个字符。有关用户名的限制信息，请参阅 Microsoft Active Directory 说明文件。
 - 在 **Active Directory 密码** 文本框中，键入密码。密码不得超过 127 个字符。
 - 在 **验证密码** 文本框中，再次键入密码。
 - 在“证书检查”下拉列表中，选择下列其中一项：

- * 如需下载和存储 iDRAC 证书并在将来的所有连接中对其进行验证，请选择**启用**。
- * 如不执行检查也不保存证书，请选择**禁用**。

- 要在无需 Active Directory 的情况下配置 iDRAC 凭据，请执行以下操作：
 - 在**用户名**文本框中，键入用户名。用户名不得超过 16 个字符。有关您的 iDRAC 版本的用户名限制信息，请参阅 iDRAC 说明文件。

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

- 在**密码**文本框中，键入密码。密码不得超过 20 个字符。
- 在**验证密码**文本框中，再次键入密码。
- 在“证书检查”下拉列表中，选择下列其中一项：
 - * 如需下载和存储 iDRAC 证书并在将来的所有连接中对其进行验证，请选择**启用**。
 - * 如不执行检查也不保存 iDRAC 证书，请选择**禁用**。

7. 单击下一步。

8. 在凭据下方的 Host Credentials（主机凭据）页面中，请执行以下操作之一：

- 对于已针对 Active Directory 配置和启用的主机（将在其上使用 Active Directory），请选择**使用 Active Directory** 复选框；否则，请跳到配置主机凭据步骤。
 - 在 **Active Directory 用户名** 文本框中，键入用户名。按照下列格式之一键入用户名：域\用户名或域/用户名或用户名@域。用户名不得超过 256 个字符。有关用户名的限制信息，请参阅 Microsoft Active Directory 说明文件。
 - 在 **Active Directory 密码** 文本框中，键入密码。密码不得超过 127 个字符。
 - 在 **验证密码** 文本框中，再次键入密码。
 - 在“证书检查”下拉列表中，选择下列其中一项：

- * 如需下载和存储主机证书并在将来的所有连接中对其进行验证，请选择**启用**。
- * 如不执行检查也不保存主机证书，请选择**禁用**。

- 要在无需 Active Directory 的情况下配置主机凭据，请执行以下操作：

- 在**用户名**文本框中，键入用户名。该用户名必须为 root。
- 在**密码**文本框中，键入密码。密码不得超过 127 个字符。

 **注：对于既没有 iDRAC Express 也没有 Enterprise 卡的服务器，iDRAC 测试连接的结果表示不适用于该系统。**

 **注：OMSA 凭据与 ESXi 主机使用的凭据相同。**

- 在**验证密码**文本框中，再次键入密码。
- 在“证书检查”下拉列表中，选择下列其中一项：
 - * 如需下载和存储主机证书并在将来的所有连接中对其进行验证，请选择**启用**。

* 如不执行检查也不保存主机证书，请选择**禁用**。

9. 单击**保存**。

10. 要关闭窗口，请单击 **X**（右上角）。

删除连接配置文件

您可以从 OpenManage Integration for VMware vCenter 移除连接配置文件。

要删除连接配置文件：

1. 在 **OpenManage Integration for VMware vCenter** 中，单击**连接配置文件**。
2. 在**可用配置文件**下，选择要删除的配置文件，然后单击**删除**。
3. 在显示的消息上，单击**删除**删除配置文件，或单击**取消**取消删除操作。

测试连接配置文件

要测试连接配置文件：

1. 在 **OpenManage Integration for VMware vCenter** 中，选择**连接配置文件**。
2. 在**可用的配置文件**下，要测试所选服务器上输入的 iDRAC 和主机根凭据，可选择连接配置文件，然后单击 **测试连接**。
3. 使用复选框选择要测试的主机，然后单击**测试所选主机**。
4. 要中止所有选择的测试并取消测试，可单击**中止所有测试**。
5. 要退出，可单击**完成**。

刷新连接配置文件

在 OpenManage Integration for VMware vCenter 中的**管理** → **连接配置文件**选项卡上，单击 VMware vSphere Web 客户端标题栏上方的**刷新**图标。

 **注：**如果从 vCenter 中移除主机，则也会自动从连接配置文件中将其移除。

了解 vSphere 客户端主机视图中的系统事件日志

“系统事件日志”提供 OpenManage Integration for VMware vCenter 查找到的硬件的状态信息。

系统事件日志提供基于以下条件的信息：

状态	有几种状态图标：信息（蓝色感叹号），警告（带感叹号的黄色三角形），错误（红色 X）。
时间（服务器时间）	表明事件发生的日期和时间。
搜索此页面	显示特定消息、服务器名称、配置设置等等。

严重性级别定义如下：

信息	OpenManage Integration for VMware vCenter 操作已成功完成。
警告	OpenManage Integration for VMware vCenter 操作的一部分出现故障，并且是部分成功。
错误	OpenManage Integration for VMware vCenter 操作失败。
安全性	包含系统安全相关的信息。

可以将日志保存为外部 CSV 文件。

相关信息：

- [显示单个主机的系统事件日志](#)

显示 Dell Management Center 中的日志

Dell Management Center 日志包括已查找到的硬件的状态信息，以及用户操作的历史记录。

要显示 Dell Management Center 中的日志：

1. 从 **Dell Management Center** 的左窗格中，选择 **日志**。
2. 要使用最新的数据更新日志，可单击 **刷新**。
3. 要选择严重性类别以筛选日志数据，可在 **所有类别** 下拉列表中，选择以下内容之一：所有类别、信息、警告、错误或安全。
4. 要选择筛选日志数据的日期范围，可单击 **上周** 下拉列表，并选择以下内容之一：上周、上个月、去年或自定义范围。如果选择自定义范围，则会显示 **开始日期** 和 **结束日期** 下拉列表。
5. 如果选择自定义日期范围：
 - a. 单击日历以填充 **开始日期**。
 - b. 单击日历以填充 **结束日期**。
 - c. 要保存配置，可单击 **应用**。
6. 要控制日志显示的方式，可使用显示控件来设置 **每屏幕记录数**，转到所需的 **页面**，并使用向前和向后页面控件。
7. 要将日志内容导出为逗号分隔值的 (CSV) 文件，可单击 **导出**。
8. 在下载位置窗口中，浏览到保存日志的位置，然后单击 **保存**。

显示单个主机的事件日志

系统硬件事件日志提供基于以下条件的信息：

- **状态**
有几种状态图标：信息（蓝色感叹号），警告（带感叹号的黄色三角形），错误（红色 X）。
- **时间（服务器时间）**
显示事件发生的日期和时间。
- **搜索此页面**
显示特定消息、服务器名称、配置设置等等。

要显示单个主机的系统事件日志：

1. 从 **vSphere 客户端** 中的 **资源清册** 标题下，选择 **主机和群集**。
2. 在树形视图中，选择主机系统。
3. 选择 **OpenManage Integration** 选项卡。
4. 要启动 **系统事件日志** 窗口，可从 **最近的系统日志条目** 中，单击 **详细信息**。
5. 要更新 **系统事件日志**，单击 **刷新**。
6. 要限制（筛选）事件日志条目的数量，可选择以下选项之一：
 - 在搜索筛选器文本框中，输入文本字符串以对日志条目进行动态筛选。
 - 要清除筛选器文本框，可单击 **X**，将显示所有事件日志条目。
7. 要清除所有事件日志条目，可单击 **清除日志**。随即会显示一条消息，说明清除所有日志条目后，它们都将被删除。选择以下操作之一：
 - 要同意清除日志条目，可单击 **确定**。
 - 要取消，可单击 **取消**。
8. 要将事件日志导出到 CSV 文件，可单击 **导出**。
9. 浏览到保存系统事件日志的位置，然后单击 **保存**。




关于固件更新

服务器接收固件更新的位置是一项全局设置，可在 OpenManage Integration for VMware vCenter 中的“设置”选项卡上找到。

固件存储库设置包含用于更新已部署的服务器的固件目录位置。有两种位置类型：

Dell (ftp.dell.com) 使用 Dell (**ftp.dell.com**) 的固件更新存储库。OpenManage Integration for VMware vCenter 将从 Dell 存储库下载所选的固件更新。

共享网络文件夹 使用 Dell Repository Manager™ 创建。这些本地存储库位于 CIFS 或 NFS 文件共享上。

 **注：**一旦创建存储库，就会将其保存到注册的主机可以访问的位置。存储库密码不能超过 31 个字符。请勿在密码中使用以下任何字符：@、&、%、'、"、, (逗号)、<、>


“固件更新向导”始终检查 iDRAC、BIOS 和 Lifecycle Controller 的最低固件级别，并尝试将它们更新到所需的最低版本。一旦 iDRAC、Lifecycle Controller 和 BIOS 固件版本满足最低需求，则“固件更新向导”将允许更新所有固件，包括：iDRAC、Lifecycle Controller、RAID、NIC/LOM、电源设备、BIOS 等等。

相关信息：

- [设置固件存储库](#)

运行固件更新向导

此功能仅适用于具有 iDRAC Express 或 Enterprise 卡的第 11 代和更高代次的 Dell 服务器。

 **注：**为了避免发生浏览器超时问题，请将默认的超时值更改为 30 秒。有关更改默认超时设置的信息，请参阅 *用户指南* 中，故障排除部分的“为何我在单击固件更新链接后看到一条显示的错误消息？”。

 **注：**对于试用/评估许可证，只要许可证未过期，即可使用固件向导。

要运行固件更新向导：

1. 在 vSphere 客户端 → OpenManage Integration 选项卡 → 主机信息中，单击 **固件** → **运行固件更新向导**。

2. 要采用 **从文件载入单独的固件更新** 选项：

a. 以下列格式输入文件路径：

CIFS: \\<host accessible share path>\<FileName>.exe or
NFS: host:/share/filename.exe

b. 如果您有 NFS，请跳至步骤 7，或者采用可以访问共享驱动器的域格式输入 **用户名和密码**。

c. 继续到步骤 7。

或者，要采用 **从存储库更新** 选项：

a. 选择 **从存储库更新**。

b. 请确保您拥有可以访问 **ftp.dell.com** 的网络连接。

c. 单击 **Next (下一步)**。

3. 选择用于您的主机的软件包，然后单击 **下一步**。

 **注：**

- 安装了 iDRAC 1.51 版本及更早版本的第 12 代主机不支持 64 位捆绑包。
- 安装了所有 iDRAC 版本的第 11 代主机不支持 64 位捆绑包。

4. 选择所需的固件更新，然后单击 **下一步**。不能选择那些降级的、已经是最新的，或者当前已经计划更新的组件。如果您选中 **允许组件被降级** 复选框，请选择列为“降级”的选项。我们仅建议那些清楚固件降级含义的高级用户选择此选项。

5. 选择所需的重启选项。

- **进入维护模式，应用更新，然后重启。**

主机将进入维护模式。如果主机无法进入维护模式，那么主机将无法重启，更新会在下一次重新引导时应用。选中在 **固件更新完成后退出维护模式** 复选框，从而在更新后退出维护模式。

- 在下次重新引导时应用更新。
为了避免服务中断，我们建议在重新引导前，主机进入维护模式。
- 在不进入维护模式的情况下，应用更新并强制重新引导。
由此即使主机未处于维护模式，也可应用更新并进行重新引导。我们不建议此方法。

6. 单击完成。

7. 要验证是否成功更新了固件，在 Dell Management Center 中，选择作业队列 → 资源清册历史 → 立即运行，然后查看 Dell Management Center 概览页面上的新版本号。

更新较早的固件版本

固件必须达到运行固件更新向导所需的最低级别。如果不满足这一条件，则会在运行固件更新向导之前为您提供相关选项以帮助更新固件。2010 年 10 月 14 日之后更新的固件则运行固件更新向导。从 vSphere 客户端的主机 OpenManage Integration 选项卡上运行固件更新。要设置存储库，请参阅[设置固件存储库](#)。

要更新较早的固件版本：


1. 在 vSphere 客户端中的 OpenManage Integration 选项卡上，在主机操作下单击运行固件更新向导。
主机固件版本低于向导支持的最低版本时，将显示需要更新对话框。
2. 在需要更新对话框中，执行以下操作之一：
 - 要在固件更新之后自动退出维护模式，可选中完成固件更新后退出维护模式复选框。
 - 在将机器添加回群集之前，如果要进入维护模式以检查和/或测试机器，则请勿选中该复选框。
3. 单击更新。
4. 成功对话框说明更新正在进行。
如果选中固件更新完成后退出维护模式，则固件更新使主机进入维护模式，然后自动重新引导。否则它将停留在维护模式。
5. 请参考 vSphere 客户端的最近的任务区域，以观察更新进程。
在该程序之后，再次运行固件更新向导以确保固件已完成更新。

运行群集和数据中心的更新固件向导

此功能仅在带有 iDRAC Express 或 iDRAC Enterprise 的第 11 代和更高版本的 Dell 服务器上可用。如果您的固件安装于 2010 年 10 月 14 日或之后，则可以使用固件更新向导自动更新固件版本。该向导仅更新属于连接配置文件，且在固件、CSIOR 状态、虚拟机管理程序和 OMSA 状态方面兼容的主机（仅限第 11 代服务器）。如果您的主机没有被列出，请通过 OpenManage Integration for VMware vCenter 运行 vSphere 主机的符合性向导，或从“主机和群集”视图中选择未列出的主机并使用固件更新向导。更新每个主机的固件组件通常会花费 30 至 60 分钟时间。启用群集上的 DRS，以便在固件更新过程中当主机进入/退出维护模式时可以迁移虚拟机。一次只能计划或运行一个固件更新任务。

如果您要从该向导导出，请使用导出至 CSV 按钮。可用搜索功能确定数据网格中除“应用日期”外的特定群集、数据中心、主机或任何标题项。

 **注：请总是一起更新存储库捆绑中所有部件的固件：BIOS、iDRAC 和 Lifecycle Controller。**

 **注：有关更改默认超时设置的信息，请参阅用户指南中故障排除部分的“为何我在单击固件更新链接后看到一条显示的错误消息？”。**

您可以通过作业队列页面查看状态和管理固件更新作业。请参阅[查看群集和数据中心的固件更新状态](#)。

1. 在 vSphere 客户端中的资源清册标题下，选择主机和群集。
2. 在主机和群集中，在树形视图中选择数据中心或群集，然后选择 OpenManage Integration 选项卡。
3. 单击更新固件。
如果未启用此链接或在您单击此选项时出现一条弹出消息，则存在尚在进行中或已计划好的固件更新作业。请关闭该对话框，等待并稍后重试此操作。可在“作业队列”中的“固件更新作业”选项卡上查看所有作业的状态。
4. 在欢迎页面中，查看有关更新的信息，然后继续向导操作。
5. 单击 Next（下一步）。




6. 在**固件资源清册**页面中，查看系统上已安装的组件。
7. 单击 **Next**（下一步）。
8. 在**选择更新的捆绑包**页面中，使用复选框选择更新捆绑包。

 **注：**

- 安装了 iDRAC 1.51 版本及更早版本的第 12 代主机不支持 64 位捆绑包。
- 安装了所有 iDRAC 版本的第 11 代主机不支持 64 位捆绑包。

9. 单击 **Next**（下一步）。
10. 在“选择要更新的系统/组件”页面中，使用复选框选择要升级或降级的组件。如果您要降级，请选中**允许组件被降级**复选框。

 **注：如果您选中所有的组件而某些保留未选中状态，则意味着那些未选中的组件无升级可用。您可以选择那些组件进行降级操作。**

11. 单击 **Next**（下一步）。
12. 在**固件更新信息**页面中，查看您已选择进行升级或降级的组件。
13. 单击 **Next**（下一步）。

14. 在**计划固件更新**页面中的“作业名称”下，执行以下操作：

- a. 在固件更新作业名称文本框内，键入**固件更新作业名称**。
此为必填字段。如果留空，则此升级未被计划。请勿使用已经在使用中的名称。如果您清除此名称，您可以再次使用它。
- b. 在固件更新说明中，键入相应**说明**。

15. 在作业计划下，执行以下操作之一：

 **注：必须选中某个选项。如果未选中任何项，则该升级将被阻止。**

- 如果您要立即运行更新作业，请单击**立即更新**，然后单击**完成**。
- 如果您要稍后运行更新作业，请单击**计划更新**，然后执行以下操作：
 1. 在日历框中，选择**月份和日期**。
 2. 在时间文本框中，以 HH:MM（小时：分钟）格式键入**时间**，然后单击**完成**。

 **注：该时间为您的客户端实际所处的本地时区。无效的时间值会导致被阻止的更新操作。**

查看群集和数据中心的固件更新状态

为了在此页面显示信息，请运行群集或数据中心固件更新。此页面仅显示有关群集和数据中心固件更新的信息。请参阅[运行群集和数据中心更新固件向导](#)。

在此页上，您可以刷新、清除或中止固件更新作业。

1. 在 Dell Management Center 中，选择**作业队列** → **固件更新作业**。
2. 要显示最新的信息，请单击**刷新**。
3. 在数据网格中查看状态。此网格提供有关固件更新作业的以下信息：
 - 状态
 - 计划的时间
 - 名称
 - 说明
 - 集合大小

集合大小是此固件资源清册作业上的服务器数量。

- 进度摘要

进度摘要列出了此固件更新的进度详细情况。

4. 要查看有关特定作业的更多详情，在特定作业的数据网格内，单击**详细情况**。

在此您可以找到以下详细信息：

- 服务标签
 - iDRAC IP
 - 状态
 - 警告
 - 固件更新作业详细信息
 - 开始时间
 - 结束时间
5. 如果您要中止某个尚未运行的计划的固件更新作业，在您要中止的作业的同一行内，单击**中止**。
 6. 如果您要清除已计划的固件更新，请单击**清除作业队列**。
您可以仅清除已完成或计划的作业。
 7. 选择**早于日期和作业状态**，然后单击**应用**。选定的作业随即从队列中被清除。

使用 vCenter 进行高级主机管理

高级主机管理任务是基于主机系统的操作，让管理员识别数据中心环境中的物理服务器，启动基于服务器的管理工具，并显示服务器保修信息。所有这些操作都可以从 vCenter 中的 OpenManage Integration 选项卡中启动，或是通过右键单击单个主机系统的 **主机和群集** 视图中的主机来启动。

设置物理服务器正面指示灯

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

要设置物理服务器的正面指示灯：

1. 在 **vSphere 客户端** 中的 **资源清册** 标题下，选择 **主机和群集**。
2. 从 **主机和群集** 中，在树形视图中选择主机系统，然后选择 **OpenManage Integration** 选项卡。
3. 在 **主机操作** 下，选择 **闪烁指示灯**。
4. 选择以下操作之一：
 - 要开启闪烁并设置时间段，请在 **指示灯** 对话框中，单击 **闪烁开**，然后使用超时下拉列表选择超时增量，然后单击 **确定**。
 - 要关闭闪烁，请在 **指示灯** 对话框中，单击 **闪烁关**，然后单击 **确定**。

基于服务器的管理工具

有两种基于服务器的管理工具（即 iDRAC 和 OMSA）可从 **vSphere 客户端** → **OpenManage Integration** 选项卡启动。在左侧窗格中的管理控制台链接下，您可以访问：

- 启动远程访问。
使用此选项可启动 iDRAC 用户界面
- 启动 OMSA
使用此选项可在“使用初始”配置向导“期间或使用 **设置** → **常规** 启动输入管理中心的 OpenManage Server Administrator 用户界面 URL。您必须在基于 Windows 的管理站上安装服务器管理员 Web 服务器的 URL。
- 如果您在刀片系统上，请启动 CMC 以启动机箱管理控制器用户界面。如果您不在刀片系统上，该项将不会显示。


保修检索

保修检索提供 Dell 服务器的以下信息：

- 仅传输主机服务标签时，更新的服务保修信息



- 按计划的间隔更新的保修信息
- 使用代理服务器和凭据进行安全传输

 **注: Dell 不会存储传输的服务标签信息。**

相关任务:

- [运行保修检索作业](#)
- [查看单一主机的服务器保修信息](#)
- [查看整个数据中心的保修信息](#)

查看整个数据中心的服务器保修信息

一旦完成保修作业，就可以在 vSphere 客户端中的数据中心视图页面上查看服务器保修信息。
要查看整个数据中心的服务器保修信息：

1. 从 vSphere 客户端中的**资源清册**标题下，选择**主机和群集**。
2. 从**主机和群集**中，在树状视图中选择数据中心，并选择 **OpenManage Integration** 选项卡。
3. 将显示数据中心中的所有主机的概览。在视图下拉列表中，选择 **保修**。
4. 在 **筛选器**文本框中，输入担保数据的筛选器。
5. 要刷新显示的资源清册，可单击 **刷新**。
6. 要将资源清册导出为 CSV 文件，可单击 **导出**。在下载位置窗口中，浏览到要保存资源清册的位置，然后单击 **保存**。

查看单一主机的服务器保修信息


一旦保修作业完成，就可以在主机视图页面上查看 vSphere 客户端中单一主机的保修信息。
查看单一主机的服务器保修信息：

1. 在 vSphere 客户端的 **资源清册**标题下，选择**主机和群集**。
2. 从**主机和群集**中，在树形视图中选择主机系统，然后选择 **OpenManage Integration** 选项卡。
3. 要显示系统保修信息，请选择 **保修**。保修状态页面上的信息包括：
 - 保修提供商名称和保修说明
 - 开始和结束日期以及保修剩余天数
 - 保修状态（有效或失效）以及保修信息最后一次更新的时间

硬件管理

前提条件：

要成功执行硬件配置和部署，物理服务器必须出现在“部署向导”中。所有物理服务器都必须满足以下前提条件：

- 有关具体的硬件支持信息，请参阅 *OpenManage Integration for VMware vCenter Release Notes*（OpenManage Integration for VMware vCenter 发行说明）。
- 服务器必须至少具有支持的最低版本的 iDRAC 固件、Lifecycle Controller 和 BIOS。有关具体的硬件支持信息，请参阅 *OpenManage Integration for VMware vCenter Release Notes*（OpenManage Integration for VMware vCenter 发行说明）。
 -  **注：如果固件版本过时，可能需要两步式的升级流程。有关详细的升级说明，请参阅固件文档。**
- OpenManage Integration for VMware vCenter 支持仅使用嵌入式/集成 LOM 进行部署。在部署之后，可以手动配置 PCI 插槽中的 NIC。如果使用扩展 NIC，则系统必须启用主机 LOM。
- OpenManage Integration for VMware vCenter 允许部署到内部双 SD 模块（仅限虚拟机监控程序）或本地硬盘驱动器。在使用 OpenManage Integration for VMware vCenter 部署虚拟机监控程序之前，必须在 BIOS 中启用内部双 SD 模块。可以手动更改管理 NIC，并将系统添加到 vCenter。
 -  **注：有关支持的双 SD 模块的信息，请参阅相应服务器的产品说明文件。**
- 如果 iDRAC 处于专用模式，则必须启用其 NIC，以便与 OpenManage Integration for VMware vCenter 进行通信。
- 必须启用 CSIOR。此外，在启动自动查找之前，为了确保检索的数据为最新，系统必须完全关闭电源然后打开（硬重新引导）。
- 可以订购由工厂预先配置了自动查找和握手选项的 Dell 服务器。如果服务器没有预先配置这些选项，则必须手动输入 OpenManage Integration for VMware vCenter 的 IP 地址，或者配置本地网络以提供此信息。
- 如果没有使用 OpenManage Integration for VMware vCenter 进行硬件配置，则在启动虚拟机监控程序部署之前，请确保满足以下条件：
 - 在 BIOS 中启用 VT（虚拟化技术）标记。
 - 将系统的引导顺序设置为可引导虚拟磁盘或内部双 SD 模块，以进行操作系统安装。
- 如果使用 OpenManage Integration for VMware vCenter 进行硬件配置，则尽管 BIOS 配置不是硬件配置文件的一部分，VT 的 BIOS 设置也会自动启用。如果目标系统上尚不存在虚拟磁盘，则需要快速/克隆 RAID 配置。
- 如果服务器版本早于第 12 代 Dell PowerEdge 服务器，则部署流程会在目标系统上安装 OpenManage Server Administrator 程序包，并自动配置 SNMP 陷阱目标，以指向 OpenManage Integration for VMware vCenter。
- 需要包含所有 Dell 驱动程序自定义 ESXi 映像才能完成部署。您可通过进入 Dell Drivers & Downloads（Dell 驱动程序和下载）页面寻找正确的映像并将自定义映像保存在部署过程中可访问的位置。如需该版本支持的 ESXi 版本的最新列表，请参阅 Release Notes（发行说明）。
- *OpenManage Integration for VMware vCenter* 仅支持 BIOS 模式在目标服务器上自动部署虚拟机监控程序。请确保在参考硬件配置文件中选中 BIOS 模式，然后再应用虚拟机监控程序配置文件。如果不选中硬件配置文件，请务必将引导模式手动配置为 BIOS 并重新引导服务器，然后再应用虚拟机监控程序配置文件。

 **注：如果目标计算机的引导模式设置为 UEFI，从 OpenManage Integration for VMware and vCenter (OMIVV) 部署操作系统将失败**


设置概述

一旦完成数据中心的物理资源清册，所有自动查找到的裸机系统都可用于 OpenManage Integration for VMware vCenter 以进行零接触硬件配置和虚拟机监控程序部署。要准备配置和部署，必须执行以下操作：



- 创建硬件配置文件** 包含从参考服务器搜集的硬件设置，这些设置用于部署新服务器。请参阅 [创建新的硬件配置文件](#)。
- 创建虚拟机监控程序配置文件** 包含 ESXi 部署所需的虚拟机监控程序安装信息。请参阅 [创建新的虚拟机监控程序配置文件](#)。
- 创建部署模板** 可以选择性地包含硬件配置文件和/或虚拟机监控程序配置文件。可以根据需要保存这些配置文件并对所有可用的数据中心服务器重复使用它们。请参阅 [构建新部署模板](#)。

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

 **注：**不要计划连续运行超过两个部署作业。多个作业应该使用计划功能来安排交错部署执行。

了解部署作业时间

配置和部署裸机服务器可能需要 30 分钟到几个小时才能完成，具体视特定因素而定。开始部署作业后，建议您根据提供的指南计划部署时间。完成配置和部署所需的时间量因部署类型、复杂程度以及同时运行的部署作业数量而有所不同。下表提供了部署作业可能需要的大致时间的指南。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。

表. 3: 大致部署时间方案

部署类型	每个部署的大致时间
仅系统管理程序	30 分钟到 130 分钟之间
仅硬件	最多 2 小时，具体视复杂程度以及要配置的 RAID、BIOS 和引导选项而定
系统管理程序和硬件配置文件	1 到 4 小时


部署顺序中的服务器状态

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

- 未配置** 该服务器已经联系 OpenManage Integration for VMware vCenter，且正等待被配置。请参阅 [了解部署作业时间](#)。
- 已配置** 该服务器已按照成功部署虚拟机监控程序需要的全部硬件信息配置完毕。

下载自定义 Dell ISO 映像

部署过程要求包含所有 Dell 驱动程序的自定义 ESXi 映像。

 **注：**OpenManage Integration for VMware vCenter ISO 不包含在部署时所需的 ESXi ISO 映像。您必须将这些映像下载到部署期间可访问的位置，否则您的部署可能会失败。

1. 导航至 support.dell.com。
2. 浏览至采用您的首选语言的 **驱动程序和下载** 页面，然后执行以下操作之一：
 - 要使用服务标签或快速服务代码选择驱动程序，在 **是** 下的文本框中输入服务标签或快速服务代码，然后单击 **提交**。
 - 要使用另一个选项选择驱动程序，在 **否** 下选择以下各项之一：
 - 为我自动检测服务标签
 - 从我的产品和服务列表中选择

- 从所有 Dell 产品列表中选择

然后单击**继续**并按照所选选项的指示进行操作。




3. 在所选服务器的页面中，向下滚动到**精简您的结果**并在**操作系统**下使用下拉列表选择您所需的 ESXi 系统。
4. 单击**企业解决方案**。
5. 在**企业解决方案**列表中，选择所需的 ISO 版本，然后单击**下载文件**。

 **注:** 嵌入式 ISO 用于内部双 SD 模块上的系统管理程序安装。可安装的 ISO 用于硬盘上的安装。

6. 在对话框中，选择用于**通过浏览器的单一文件下载**，然后单击**立即下载**。
7. 在对话框中，浏览到存储用于部署的 ISO 映像的位置。

了解如何配置硬件配置文件

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

引导顺序	引导顺序是指引导设备序列和硬盘驱动器序列，仅当引导模式设置为 BIOS 时才能编辑该序列。
BIOS 设置	BIOS 设置包括：内存、处理器、SATA、集成设备、串行通信、嵌入式服务器管理、电源管理、系统安全以及杂项设置。
iDRAC 设置	iDRAC 设置包括：网络、用户列表以及用户配置（IPMI/iDRAC 特权）。  注: 对于具有 iDRAC Express 的系统，无法提取 iDRAC 配置，因此不应该将服务器用作参考服务器。如果它用作目标系统，则不会从参考服务器应用任何 iDRAC 配置。
RAID 配置	RAID 配置显示参考服务器上在提取硬件配置文件时的当前 RAID 拓扑。  注: 在硬件配置文件中配置了两个 RAID 配置选项： <ul style="list-style-type: none">• <i>应用 RAID1 + 创建专用热备用，适用。</i> 如果要为目标服务器应用默认 RAID 配置设置，则使用此选项。在支持 RAID1 的集成控制器的前两个驱动器上，RAID 配置任务默认为 RAID1。此外，如果存在符合标准的候选驱动器，则会为 RAID1 阵列创建专用热备用。• <i>如下所示从参考服务器克隆 RAID 配置。</i> 如果要克隆参考服务器设置，请使用此选项。请参阅 创建新的硬件配置文件。  注: 无论参考服务器上的设置如何，OpenManage Integration for VMware vCenter 都会在所有部署的服务器上启用 BIOS 中的“处理器”组下的某些 BIOS 设置。在使用参考服务器创建新的硬件配置文件之前，它必须启用“重新引导时收集系统资源清册 (CSIOR)”设置，并进行重新引导以提供准确的资源清册和配置信息。

创建硬件配置文件的任务包括：

- [在参考服务器上启用 CSIOR](#)
- [创建新的硬件配置文件](#)
- [克隆硬件配置文件](#)
- [关于管理硬件配置文件](#)


创建新的硬件配置文件

要创建新的硬件配置文件：

1. 在 Dell Management Center 中，选择**部署** → **部署模板** → **硬件配置文件**。
2. 单击**新建**。
3. 在**新硬件配置文件**页面中，执行以下操作：
 - 在**配置文件名称**文本框中，输入配置文件名称。



- 在说明文本框中，键入可选的说明。
4. 单击**保存**。
 5. 要继续，在左侧窗格中单击**参考服务器**。
 6. 在参考服务器窗口中，单击**编辑**。
 7. 要查找合规的、由 vCenter 管理并且通过 OpenManage Integration for VMware vCenter 成功进行资源清册的参考服务器，请单击**浏览**。
 8. 在**服务器**对话框中，向下滚动列表以查找正确的参考服务器，然后单击**选择**。
 9. 要自定义参考服务器设置作为默认值，请单击**来自参考服务器的自定义设置**，然后单击**保存**。
 10. 此时将显示一个对话框，表示提取设置需要几分钟时间。要填充设置，请单击**继续**。所选服务器的名称、iDRAC IP 地址和服务标签将在**参考服务器**窗口中显示。
 11. 在左侧窗格中，选择 **引导顺序**。要在配置文件中包含引导顺序信息，请选中 **在此硬件配置文件中包含引导顺序**复选框。
 12. 要显示引导顺序选项，展开 **引导顺序**，然后单击**编辑**进行更新：

 **注:** 对于 Dell 第 13 代 PowerEdge 服务器，只显示硬件配置文件的当前引导模式详细信息。

 **注:** 如果目标计算机的引导模式设置为 UEFI，从 OpenManage Integration for VMware and vCenter 部署操作系统将失败

- a. 在**引导模式**下拉列表中选择 BIOS 或 UEFI。
 - b. 要对显示的引导设备顺序进行更改，请在**查看/配置**下拉列表中的 **引导设备顺序**下，选择该设备并单击**上移**或**下移**。
 - c. 在**引导重试顺序**下拉列表中，选择 **已启用**以便服务器自动重试引导顺序，或选择 **已禁用**不重试该顺序。
 - d. 单击**保存**保存更改，或单击**取消**取消更改。
13. 如果选择了 **BIOS 引导模式**，您可以展开**硬盘驱动器顺序**以显示硬盘驱动器顺序选项，然后单击**编辑**进行更新：
 - 要对显示的硬盘驱动器顺序进行更改，请选择该设备并单击**上移**或**下移**。
 - 单击**保存**保存更改，或单击**取消**取消更改。
 14. 在左侧窗格中，选择 **BIOS 设置**。要在配置文件中包含 BIOS 设置信息，请选中 **在此硬件配置文件中包含 BIOS 设置**复选框。展开一个类别以显示设置选项，然后单击**编辑**对以下项之一进行更新：
 - Memory Settings（内存设置）
 - Processor Settings（处理器设置）
 - SATA Settings（SATA 设置）
 - Integrated Devices（集成设备）
 - Serial Communication（串行通信）
 - Embedded Server Management（嵌入式服务器管理）
 - Power Management（电源管理）
 - System Security（系统安全）
 - Miscellaneous Settings（其他设置）

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

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

15. 在左侧窗格中，选择 **iDRAC 设置**，然后选择**网络**。
16. 要在配置文件中包含网络设置信息，请选中 **在此硬件配置文件中包含网络设置**复选框。展开一个类别以显示设置选项，然后单击**编辑**对以下项之一进行更新：
 - Network（网络）
 - Network Settings（网络设置）
 - Virtual Media（虚拟介质）

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

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

17. 在左侧窗格中，选择 **iDRAC 设置** → **用户列表**。要在配置文件中包含用户列表信息，请选中**在此硬件配置文件中包含用户列表**复选框。在“iDRAC 本地用户列表”下，执行以下操作之一：

- a. **添加用户**：手动输入一位 iDRAC 用户和所需的信息。完成后，单击**保存**保存您的更改或单击**取消**以取消。
- b. **删除用户**：删除所选用户。选中该用户的复选框并单击**删除**，或单击**取消**以取消。
- c. **编辑用户**：手动编辑一位 iDRAC 用户的信息。完成后，单击**保存**保存您的更改或单击**取消**以取消。

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

18. 在左侧窗格中，选择 **RAID 配置**。要在配置文件中包含 RAID 配置信息，请选中 **在此硬件配置文件中包括 RAID 配置** 复选框。然后选择以下选项之一：
- 应用 RAID1 + 创建专用热备用（如适用）。
如果您希望将默认 RAID 配置设置应用于目标服务器，请使用此选项。RAID 配置默认为使用支持 RAID1 的集成控制器的前两个驱动器上的 RAID1。此外，如果存在满足条件的候选驱动器，则为 RAID1 阵列创建专用热备用。
 - 从参考服务器克隆 RAID 配置。
如果您要克隆参考服务器设置，请使用此选项。

配置文件会自动保存并显示在**硬件配置文件**窗口中的**可用配置文件**下。

在参考服务器上启用 CSIOR

使用参考服务器创建硬件配置文件之前，启用 Collect System Inventory On Reboot (CSIOR)（重新引导时收集系统资源清册 [CSIOR]）设置并重新引导服务器以提供准确的资源清册和配置信息。启用 CSIOR 有两种方法：

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

在参考服务器上本地启用 CSIOR：

1. 打开系统，然后在自检期间按 **<F10>** 启动 USC。
2. 选择 **硬件配置** → **部件更换配置**。
3. 启用 **主机重新引导时收集系统资源清册** 设置，然后退出 USC。

克隆硬件配置文件

要克隆新的硬件配置文件：

1. 在 Dell Management Center 中，选择 **部署** → **部署模板** → **硬件配置文件**。
2. 单击 **新建**。
3. 在 **新硬件配置文件** 页面中，执行以下操作：
 - 在 **配置文件名称** 文本框中，输入配置文件名称。
 - 在 **说明** 文本框中，输入可选的说明。
4. 单击 **保存**。
5. 在左侧窗格中单击 **参考服务器**。
6. 在 **参考服务器** 窗口中，单击 **编辑**。
7. 要从参考服务器提取所有硬件设置，可单击 **克隆参考服务器设置** 选项按钮。
8. 单击 **保存**。
9. 将显示一个对话框，表明提取设置将花费数分钟，然后单击 **继续**。将填充设置，并且在参考服务器窗口中显示所选服务器的名称、iDRAC IP 地址以及服务标记。
将保存配置文件，并在 **硬件配置文件** 窗口下的 **可用配置文件** 中显示。

关于管理硬件配置文件

硬件配置文件使用参考服务器定义服务器的硬件配置。在 Dell Management Center 中，您可以对现有的硬件配置文件执行多种管理操作，包括：



- [查看或编辑硬件配置文件](#)
- [复制硬件配置文件](#)
- [复制硬件配置文件](#)
- [删除硬件配置文件](#)
- [刷新硬件配置文件](#)

查看或编辑硬件配置文件

查看或编辑硬件配置文件：

1. 在 Dell Management Center 中，选择**部署** → **部署模板** → **硬件配置文件**。
2. 选择配置文件并单击 **查看/编辑**。
3. 在 **硬件配置文件**窗口中，要进行任何更改，请单击 **编辑**。
4. 单击 **保存**应用更改，或单击 **取消**取消更改。

复制硬件配置文件

要复制硬件配置文件：

1. 在 Dell Management Center 中，选择 **部署** → **部署模板** → **硬件配置文件**。
2. 在 **硬件配置文件**页面中，选择一个配置文件，然后单击 **复制**。
3. 在 **复制**对话框中，输入一个唯一的硬件配置文件名称。
4. 单击 **应用**使用新名称创建一份配置文件，或单击 **取消**以取消。


重命名硬件配置文件

要重命名硬件配置文件：

1. 在 Dell Management Center 中，选择**部署** → **部署模板** → **硬件配置文件**。
2. 在 **硬件配置文件**页面上，选择配置文件并单击 **重命名**。
3. 在 **重命名**对话框中，输入唯一的硬件配置文件名称。
4. 单击 **应用**使用新名称，或单击 **取消**取消。

删除硬件配置文件

要删除硬件配置文件：

 **注：**删除属于正在运行的部署任务的硬件配置文件可能导致任务失败。

1. 在 Dell Management Center 中，选择**部署** → **部署模板** → **硬件配置文件**。
2. 选择配置文件并单击**删除**。
3. 在消息对话框中，要移除配置文件，可单击 **删除**，或者单击 **取消**以取消。

刷新硬件配置文件

要刷新更新的硬件配置文件：

1. 在 Dell Management Center 中，选择**部署** → **部署模板** → **硬件配置文件**。
2. 单击**刷新**。
此时将显示更新的硬件配置文件信息。

创建新的虚拟机监控程序配置文件

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

- 可脚本化的参考 ISO 软件介质在 NFS 或 CIFS 共享上的位置
- 管理部署的主机的 vCenter 实例，加上可选的主机配置文件
- vCenter 中插件在其中部署服务器的目标群集或数据中心



注: 使用以下命名约定之一来为参考 ISO 文件命名:

NFS 格式: host:/share/hypervisor_image.iso

CIFS 格式: \\host\share\hypervisor.iso

要创建新的虚拟机监控程序配置文件:

1. 在 **Dell Management Center** 中，选择 **部署** → **部署模板** → **虚拟机监控程序配置文件**。
2. 在 **虚拟机监控程序配置文件** 页面中，单击 **新建**。
3. 在 **新的虚拟机监控程序配置文件** 页面中，执行以下操作:
 - 在 **配置文件名称** 文本框中，输入配置文件名称。
 - 在 **说明** 文本框中，输入可选的说明。
4. 在左窗格中，单击 **参考 ISO**，然后单击 **编辑**，并在 **虚拟机监控程序安装源** 对话框中输入以下信息:
 - 在 **虚拟机监控程序安装源** 文本框中，键入虚拟机监控程序共享位置的路径。将修改一份该虚拟机监控程序映像的副本以允许脚本安装。参考 ISO 位置必须是以下格式之一:
 - NFS 格式: host:/share/hypervisor_image.iso
 - CIFS 格式: \\host\share\hypervisor.iso
 - 在 **选择版本** 下拉列表中，选择 ESXi 版本。

所有使用该虚拟机监控程序配置文件部署的服务器都有该映像，并且如果服务器版本早于 12 代，将安装 OpenManage Server Administrator 的最新推荐版本。

5. 如果使用 CIFS 共享，则输入 **用户名**、**密码** 以及 **验证密码**。密码必须匹配。
6. 要向配置文件添加设置，可单击 **保存**。
7. 在左侧窗格中，单击 **vCenter 设置**，然后编辑所需的项目:
 - **vCenter 实例:** 显示部署后管理主机的服务器实例。
 - **vCenter 版本:** 显示当前版本。
 - **vCenter 目标容器:** 托管新物理服务器的数据中心或群集; 单击 **浏览搜索 vCenter 目标**。
 - **vCenter 主机配置文件:** 选择封装主机配置和帮助管理主机配置的配置文件。
8. 要向配置文件添加信息，可单击 **保存**。

有关管理虚拟机监控程序配置文件的的信息，请参阅 [管理虚拟机监控程序配置文件](#)。

管理虚拟机监控程序配置文件

您可以对现有虚拟机监控程序配置文件执行多个管理操作，包括:

- [了解 VLAN 支持](#)
- [查看或编辑虚拟机监控程序配置文件](#)
- [复制虚拟机监控程序配置文件](#)
- [重命名虚拟机监控程序配置文件](#)
- [删除虚拟机监控程序配置文件](#)
- [刷新虚拟机监控程序配置文件](#)



VLAN 支持

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

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

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

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

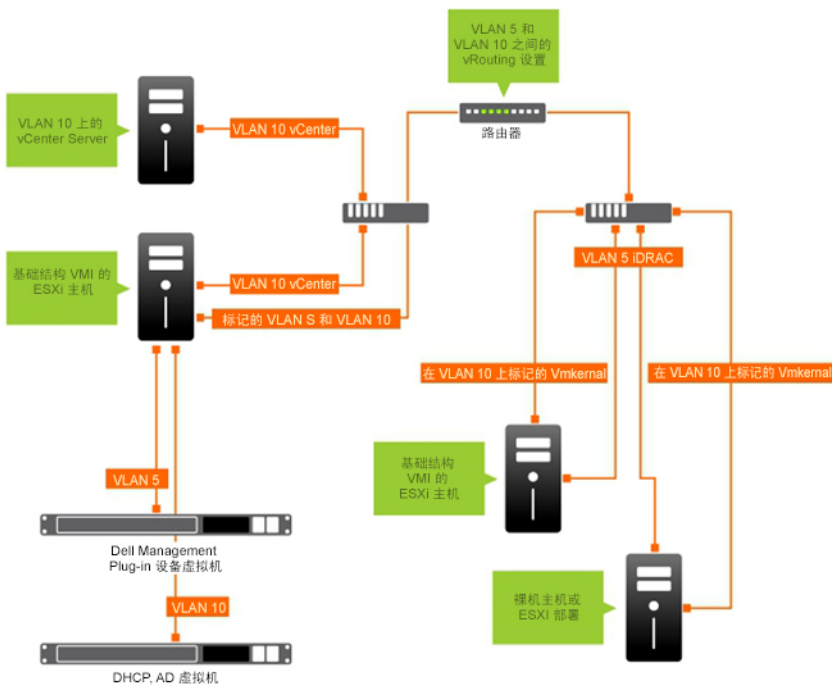


图 4: VLAN 网络示例。

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

查看或编辑虚拟机监控程序配置文件

要查看或编辑虚拟机监控程序配置文件：

1. 在 Dell Management Center 中，选择 **部署** → **部署模板** → **虚拟机监控程序配置文件** 窗口。
2. 选择配置文件并单击 **查看/编辑**。
3. 在 **虚拟机监控程序配置文件：配置文件名称** 窗口中，选择要显示或更改的配置文件部分，并进行必要的更改。
4. 单击 **保存应用更改**，或单击 **取消取消更改**。

复制虚拟机监控程序配置文件

要复制虚拟机监控程序配置文件：

1. 在 Dell Management Center 中，选择**部署** → **部署模板** → **虚拟机监控程序配置文件**。
2. 在**虚拟机监控程序配置文件**页面中，选择一个配置文件并单击**复制**。
3. 在**复制**对话框中，输入一个唯一的虚拟机监控程序配置文件名称。
4. 单击**应用**使用新名称创建一份配置文件，或单击**取消**以取消。

重命名虚拟机监控程序配置文件

要重命名虚拟机监控程序配置文件：

1. 在 Dell Management Center 中，选择**部署** → **部署模板** → **虚拟机监控程序配置文件**。
2. 在**虚拟机监控程序配置文件**页面中，选择一个配置文件并单击**重命名**。
3. 在**重命名**对话框中，输入一个唯一的虚拟机监控程序配置文件名称。
4. 单击**应用**使用新名称，或单击**取消**取消。

删除虚拟机监控程序配置文件

要删除虚拟机监控程序配置文件：

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

1. 在 Dell Management Center 中，选择**部署** → **部署模板** → **虚拟机监控程序配置文件**。
2. 选择配置文件并单击**删除**。
3. 在消息对话框中，单击**删除**以移除配置文件，或单击**取消**以取消。

刷新虚拟机监控程序配置文件

要刷新虚拟机监控程序配置文件：

1. 在 Dell Management Center 中，选择**部署** → **部署模板** → **虚拟机监控程序配置文件**。
2. 单击**刷新**。
此时将显示更新的虚拟机监控程序配置文件信息。

构建新部署模板

部署模板包含硬件配置文件和/或虚拟机监控程序配置文件。部署向导使用该模板在 vCenter 中配置服务器硬件并部署主机。

要构建新部署模板：

1. 在 Dell Management Center 中，选择**部署** → **部署模板**。
2. 在**可用的配置文件**下，单击**新建**。
3. 在**新建**窗口中，输入模板名称，然后单击**保存**。
4. 要完成模板，可单击**编辑**。
5. 在右侧窗格的**配置文件**下拉列表中，选择配置文件，然后执行以下操作之一：
 - 要显示所选配置文件的硬件/虚拟机监控程序配置文件设置，可单击**查看**。
 - 要创建新的硬件/虚拟机监控程序配置文件，可单击**新建**。
6. 为部署模板输入可选的**说明**，它有助于管理模板。
7. 要应用配置文件选择并保存更改，可单击**保存**。要取消，可单击**取消**。



管理部署模板

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

- [构建部署模板](#)
- [复制部署模板](#)
- [重命名部署模板](#)
- [删除部署模板](#)

复制部署模板

要复制部署模板：

1. 在 Dell Management Center 中，选择**部署** → **部署模板**。
2. 在部署模板页面上，选择模板，然后单击 **复制**。
3. 输入模板的新名称然后单击 **应用**。模板必须具有唯一的名称。

删除部署模板

要删除部署模板：

1. 在 Dell Management Center 中，选择**部署** → **部署模板**。
2. 在**部署模板**页面上，选择模板，然后单击**删除**。
3. 单击消息框上的**删除**以删除模板，或单击**取消**以取消。

重命名部署模板


要重命名部署模板：


1. 在 Dell Management Center 中，选择**部署** → **部署模板**。
2. 在**部署模板**页面中，选择一个模板，单击 **重命名**。
3. 输入模板的新名称然后单击 **应用**。模板必须具有唯一的名称。
4. 要显示所有部署模板，请从 **Dell Management Center** 中选择**部署** → **部署模板**，然后单击**刷新**。

运行部署向导

部署向导引导您逐步完成以下裸机服务器部署过程：

- 选择未部署的服务器。
部署虚拟机监控程序时，您可以部署到最少具备 1 GB 存储的内部双 SD 模块。必须先从 BIOS 启用内部双 SD 模块，然后才能使用 OpenManage Integration for VMware vCenter 部署虚拟机监控程序。
- 使用部署模板（硬件和虚拟机监控程序配置文件的组合）。
- 设置全局设置。此页面可让您选择将虚拟机监控程序部署到硬盘还是内部双 SD 模块。
- 将标识分配至部署的服务器。
- 将所需的连接配置文件与每台服务器相匹配。
- 计划要运行的服务器部署作业。
- 显示作业队列，您可在其中管理部署作业。

 **注：**如果仅部署硬件配置文件，则新的全局设置、服务器标识和连接配置文件页面都将跳过，您可直接转至计划作业页面。

 **注：**对于试用/评估许可证，只要许可证未过期，即可使用部署向导。

相关任务：

- [部署向导步骤 1: 选择服务器](#)
- [部署向导步骤 2: 部署模板](#)
- [部署向导步骤 3: 全局设置](#)
- [部署向导步骤 4: 服务器标识](#)
- [部署向导步骤 5: 连接配置文件](#)
- [部署向导步骤 6: 计划作业](#)

部署向导 - 步骤 1: 选择服务器

此页面介绍服务器部署。如果您要将系统管理程序部署到内部双 SD 模块，此页面将显示该选项是否可用。有关内部双 SD 模块的详细信息，请参阅[运行部署向导](#)。如果您要部署的服务器没有在步骤 2 的列表中显示，您可以手动添加服务器以使其在此步骤的列表中显示，请参阅[手动添加服务器](#)。

要选择服务器：

1. 在 **Dell Management Center** 中，选择 **部署** → **部署向导**。
2. 在 **选择服务器** 窗口中，要将未部署的服务器分配到此部署作业，请使用复选框选中 **服务器**。
3. 单击 **下一步**。

要继续任务的步骤 2，请单击 [部署向导步骤 2](#)。

部署向导步骤 2: 部署模板

部署到硬件配置文件与虚拟机监控程序部署有所不同。如果您要部署到硬件配置文件，请单击[部署向导步骤 6](#)。

要选择部署模板：


1. 部署模板通过以下多种方式之一选择/创建部署模板：
 - 在 **可用的模板** 下选择一个现有的部署模板。所选模板的信息将填充右侧窗格。
 - 选择一个现有的部署模板，然后单击 **编辑** 更改一个或两个关联的配置文件。
 - 单击 **新建** 定义一个新模板。
2. 选择以下选项之一：
 - 如果您要部署到硬件配置文件，单击 **下一步**，转至[部署向导步骤 6](#)。
 - 如果您要部署到系统管理程序配置文件，单击 **下一步**，转到 [部署向导步骤 3](#)。

部署向导步骤 3: 全局设置

可以将虚拟机管理程序部署到硬盘驱动器或内部双 SD 模块。如果至少一个所选服务器包含内部双 SD 模块，则默认会启用 **内部双 SD 模块** 选项。如果不存在，则 **硬盘** 和 **内部双 SD 模块** 选项都不会选中。

要部署虚拟机管理程序，请执行以下步骤：

1. 在“全局设置”页面中，选择以下选项之一：
 - **硬盘** - 在硬盘驱动器上部署虚拟机管理程序。
 - **内部双 SD 模块** - 在内部双 SD 模块上部署虚拟机管理程序。
2. 如果所有选中的服务器都不支持内部双 SD 模块，或者内部双 SD 模块在部署期间不存在，则执行以下操作之一：
 - 如果要在服务器的第一个硬盘上部署虚拟机管理程序，则选中 **将虚拟机管理程序部署到没有内部双 SD 模块的服务器的第一个硬盘** 复选框。

 **小心:** 如果选中此选项并在服务器的第一个硬盘驱动器上部署虚拟机管理程序，则磁盘驱动器上的所有数据将被擦除。

- 清除 **将虚拟机管理程序部署到没有内部双 SD 模块的服务器的第一个硬盘** 复选框，以跳过在这些服务器上的部署，并继续在下一个服务器上部署虚拟机管理程序。




3. 单击下一步。

要继续任务的步骤 4，请单击 [部署向导步骤 4：服务器标识](#)。

部署向导步骤 4：服务器标识

服务器标识可通过以下两种方式提供：

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

 **注：对主机名而非 localhost 使用完全限定域名 (FQDN)。**从 ESXi 5.1 开始，localhost 的值将会妨碍 OpenManage Integration for VMware vCenter 处理主机发来的事件。创建解析指向 FQDN 的 IP 地址的 DNS 记录。为正确标识 ESXi 5.1 发来的 SNMP 警报，请将 DNS 服务器配置为支持反向查找请求。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。

此屏幕提供指定 VLAN ID 的选项。当提供 VLAN ID 时，它会在部署期间应用于虚拟机监控程序的管理接口并使用 VLAN ID 标记所有流量。

要标识您的服务器：

1. 服务器标识为部署的服务器分配新名称和网络标识。要显示不符合最低固件、BIOS 要求或有其他问题的服务器列表，请单击 **不符合要求的服务器**。
2. 有关其他信息，请单击 **详细信息**。
3. 一旦系统更新，单击 **检查符合性** 重新检查并确认修复。要刷新该列表，请单击 **刷新**，然后单击 **中止所有测试** 取消测试。
4. 单击 **^** 展开并查看各服务器信息。
5. 在 **主机名和 NIC** 下，输入服务器的 **完全限定主机名**。
6. 在 **NIC 管理任务** 下拉列表中，选择将用于管理服务器的 NIC。
7. 输入 **IP 地址**、**子网掩码** 和其他网络信息，或选中 **使用 DHCP 获取** 复选框。
8. 如果部署到需要 VLAN ID 的网络，请选中 **VLAN** 复选框，然后输入 VLAN ID。
对于 VLAN ID，请使用 1 到 4094 的数字。保留 VLAN ID 0 用于标记帧的优先级。
9. 对要部署的所有服务器重复此操作，或选中 **将设置应用至所有选定服务器** 复选框。
10. 单击 **下一步**。

要继续任务的步骤 5，请单击 [部署向导步骤 5](#)。

部署向导步骤 5：连接配置文件

连接配置文件用于建立主机的连接凭据，方法是将其与 iDRAC 或主机根凭据关联。在连接配置文件窗口可以进行以下操作：

- 显示或编辑当前连接配置文件
- 删除连接配置文件
- 刷新连接配置文件列表以体现 vCenter 主机更改

创建连接配置文件：

1. 连接配置文件在部署作业完成后会将服务器自动分配给连接配置文件。
一旦选择连接配置文件，请单击 **下一步**。
2. 选择 **将所有服务器分配到同一连接配置文件** 选项按钮，然后从下拉列表选择连接配置文件以将所有服务器分配到同一现有配置文件。
3. 要创建新的配置文件，请单击 **新建**；要查看或编辑所选配置文件，请单击 **查看/编辑**。
4. 要显示所选连接配置文件设置，请单击 **查看**。
5. 选择 **为每个服务器选择一个连接配置文件** 选项按钮，然后从下拉列表中为每个服务器选择单独的连接配置文件。
6. 一旦选择连接配置文件，请单击 **下一步**。

要继续任务到步骤 6，请单击 [部署向导步骤 6](#)。

部署向导步骤 6：计划作业

计划可设置部署作业的计划。何时运行部署作业有以下几个选项：立即、计划部署作业以在所选日期和时间运行、保留部署作业和手动启动。

要设置计划：

1. 通过输入日期和时间确定何时运行部署作业：
 - a. 单击 **为部署计划服务器**。
 - b. 使用日历控件选择日期。
 - c. 输入一天当中的时间：
 - 立即：单击 **立即部署服务器**。
 - 推迟作业：单击 **创建部署作业**。
 - 暂停：使用此选项时，只能修改计划并且其他所有部署作业选项都无法更改。
2. 输入作业名称和作业说明。
3. 单击**完成**。
4. 现在，部署向导已完成，您可以使用**作业队列**管理部署作业。
5. 要显示必须进行固件更新然后才能完成向导的不符合要求的服务器列表，请单击 **不符合要求的服务器**。

相关任务：

- [使用部署作业队列管理部署作业](#)

了解作业队列

作业队列管理服务器部署和资源清册检索作业，例如：

- 显示提交的服务器部署作业。
- 刷新部署作业或资源清册/担保历史记录队列。
- 计划资源清册作业以更新当前 vCenter 中找到的 Dell 服务器属性。
- 清除部署作业队列条目。
- 管理群集和数据库的固件更新。

 **注：要确保资源清册/担保包中包含最新信息，请计划资源清册/担保作业至少每周运行一次。资源清册/担保作业将消耗资源极少并且不会降级主机性能。**

此页面上的任务包括：

- [使用部署作业队列管理部署作业](#)
- [运行资源清册作业](#)
- [修改资源清册作业计划](#)
- [查看群集和数据中心的固件更新状态](#)

使用部署作业队列管理部署作业

要使用部署作业队列管理部署作业：

1. 在 **Dell Management Center** 中，选择 **作业队列** → **部署作业**。
2. 要更新 **部署作业详细信息**，请单击 **刷新**。
3. 要显示部署作业详细信息对话框（其中包含部署作业中包括的服务器的详细信息），请单击 **详细信息**。此操作将显示以下详细信息：
 - 服务标签
 - iDRAC IP 地址



- 服务器状态
- 是否出现任何警告
- 部署作业详细信息
- 开始和结束时间

要显示对话框列表中每个项目的完整信息，将鼠标悬停在该项目上，此时将显示另一个弹出文本。

4. 要暂停所选作业或输入更新的计划，请单击 **修改**。
5. 单击 **中止** 中止部署作业。
6. 显示该消息时，单击 **中止作业** 中止，或单击 **请勿中止作业取消**。

 **注：正在进行的任何部署作业都无法中止。**

7. 要显示清空部署作业队列窗口，请单击 **清空作业队列**。选择 **早于日期和作业状态**，然后单击 **应用**。所选作业随即从队列中清空。

手动添加服务器

您可以手动添加没有通过查找进程添加的服务器。一旦添加后，该服务器将在部署向导的服务器列表中显示。

1. 在 Dell Management Center **部署** 中，单击 **部署向导**。
2. 在 **选择服务器** 选项卡中，单击 **添加服务器**。
3. 在 **添加服务器** 对话框中，执行以下操作：
 - a. 在 **iDRAC IP 地址** 文本框中，输入 iDRAC IP 地址。
 - b. 在 **用户名** 文本框中，输入用户名。
 - c. 在 **密码** 文本框中，输入密码。
4. 单击 **添加服务器**。这可能需要几分钟时间。

移除裸机服务器

您可以手动移除自动查找到的或手动添加的服务器。

1. 在 Dell Management Center **部署** 中，单击 **部署向导**。
2. 在 **选择服务器** 选项卡中，单击 **移除服务器**。
3. 在 **移除服务器** 对话框中，选中要移除的服务器的复选框。
4. 单击 **移除选定的服务器**。
5. 在 **选择服务器** 选项卡中，查看表格中列出的服务器以确认移除。

控制台管理

可通过使用两个附加的管理门户实现 OpenManage Integration for VMware vCenter 及其虚拟环境的管理：

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

通过使用这两个门户，可以跨所有 vCenter 实例输入并使用 vCenter 管理的全局设置、OpenManage Integration for VMware vCenter 数据库备份和还原以及重设/重新启动操作。

基于 Web 的 Administration Console

基于 Web 的 Administration Console 提供多项重要功能：vCenter 服务器注册和管理、虚拟设备管理、全局 vCenter 警报设置以及备份和还原设置。

使用管理控制台

从管理控制台中的“vCenter 注册”窗口中，您可以注册 vCenter 服务器，然后上载或购买许可证。如果您使用的是演示版许可证，将显示“购买软件”链接，您可通过该链接购买完整版许可证，以管理多台主机。您还可以在此部分中修改、更新和注销服务器。

相关任务：

- [使用具有必要权限的非管理员用户注册 vCenter 服务器](#)
- [注册 vCenter 服务器](#)
 - [修改 vCenter 登录名](#)
 - [更新已注册 vCenter 的 SSL 证书](#)
 - [从 vCenter 中卸载 OpenManage Integration for VMware vCenter](#)
- [上载 OpenManage Integration for VMware vCenter 许可证](#)

使用具有必要权限的非管理员用户注册 vCenter 服务器

您可使用具有 vCenter 服务器的 vCenter 管理员凭据的 OMIVV 设备或具有必要权限的非管理员用户注册 vCenter 服务器。

请执行以下步骤，使具有所需权限的用户能够注册 vCenter 服务器：

1. 添加角色并选择该角色的必要权限或修改现有角色以更改为该角色选择的权限。有关在 vSphere 客户端中创建或修改角色并选择权限所需的步骤，请参阅 VMware vSphere 说明文件。请参阅 [定义权限](#) 以选择该角色的所有必要权限。

 **注：vCenter 管理员应添加或修改角色。**

2. 定义角色并为该角色选择权限后，分配用户至新创建的角色。有关在 vSphere 客户端中分配权限的更多信息，请参阅 VMware vSphere 说明文件。具有必要权限的 vCenter 服务器非管理员用户现在可注册和/或注销 vCenter、修改凭据或更新证书。

 **注：vCenter 管理员应在 vSphere 客户端中分配权限。**

3. 使用具有必要权限的非管理员用户注册 vCenter 服务器。请参阅 [使用具有必要权限的非管理员用户注册 vCenter 服务器](#)。



4. 将 Dell 权限分配给步骤 1 中创建或修改的角色。请参阅 [分配 Dell 权限给角色](#)。

现在，具有必要权限的非管理员用户可体验 Dell 主机的 OMIVV 功能。

定义权限

要使具有必要权限的非管理员用户能够注册 vCenter 服务器，请选择以下权限：

- 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
- 主机
 - CIM
 - * CIM 交互
 - 配置
 - * 高级设置
 - * 连接
 - * 维护
 - * 查询补丁程序
 - * 安全配置文件和防火墙
 - 资源清册
 - * 将主机添加到群集
 - * 添加独立主机
- 主机配置文件
 - 编辑
 - 查看
- 权限
 - 修改权限
 - 修改角色
- 会话
 - 验证会话
- 任务
 - 创建任务
 - 更新任务

 **注:** 使用具有必要权限的非管理员用户注册 vCenter 服务器时，如果未分配上述权限，则会显示一条错误消息。

使用具有必要权限的非管理员用户注册 vCenter 服务器

您可使用具有必要权限的非管理员用户注册 OMIVV 设备的 vCenter 服务器。[注册 vCenter 服务器](#)有关注册 vCenter 服务器的更多信息。

分配 Dell 权限给角色

您可以编辑现有角色以分配 Dell 权限。

 **注:** 确保您以具有管理员权限的用户登录。

要分配 Dell 权限给现有角色，请执行以下操作：

1. 使用管理权限登录 vSphere 客户端。
2. 在 vSphere 客户端的**主页**，单击**角色**。
3. 右键单击该角色以编辑并选择**编辑角色**。
4. 选择以下权限，然后单击**确定**。
 - Dell
 - Dell.Configuration
 - Dell.Deploy-Provisioning
 - Dell.Inventory
 - Dell.Monitoring
 - Dell.Reporting

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

对权限和角色的更改立即生效。具有必需权限的非管理员现在可执行 OpenManage Integration for VMware vCenter 操作。

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

注册 vCenter 服务器

安装 OpenManage Integration for VMware vCenter 后，您可以注册 OpenManage Integration for VMware vCenter。OpenManage Integration for VMware vCenter 使用管理员用户帐户或具有所需权限的非管理员用户帐户进行 vCenter 操作。OpenManage Integration for VMware vCenter 当前支持每个 OMIVV 设备 10 个 vCenter，此数字以后可更改。

1. 打开**管理控制台**。
2. 要注册新 vCenter 服务器，请在左侧窗格中，单击 **VCENTER 注册**，然后单击 **注册新 vCenter 服务器**。
3. 在**注册新 vCenter** 对话框中的 **vCenter 名称** 下，执行以下操作：
 - a. 在 **vCenter 服务器 IP 或主机名** 文本框中，输入 vCenter 的 IP 地址或主机名 FQDN。

 **注:** 强烈建议使用全限定域名 (FQDN) 向 VMware vCenter 注册 OMIVV。对于所有注册，vCenter 的主机名应该可由 DNS 服务器正确解析。使用 DNS 服务器时，建议您遵循以下实践方法：

- 当您部署已有效注册 DNS 的 OMIVV 设备时，请分配一个静态 IP 地址和主机名。静态 IP 地址可确保在系统重新启动过程中，OMIVV 设备的 IP 地址保持不变。
 - 确保 OMIVV 主机名条目存在于正向和反向查询中。
- b. 在**说明**文本框中，输入可选的说明。
4. 在 **vCenter 用户帐户** 下，执行以下操作：
 - a. 在 **vCenter 用户名** 文本框中，输入管理员的用户名或具有必要权限的非管理员用户名。
 - b. 在 **密码** 文本框中，输入密码。
 - c. 在 **验证密码** 文本框中，再次输入密码。
 5. 单击 **Register**（注册）。



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

例如: 假设具有必要权限的用户 X 向 vCenter 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启动主机。

OpenManage Integration for VMware vCenter 要求

在前代服务器上, OpenManage Integration for VMware vCenter (OMIVV) 从 OpenManage 请求信息, 而较新的平台被限制为从支持较新芯片组的 vSphere 版本启动。因此, 给定 OMIVV 版本使用的 vSphere 版本将有一些限制。

表. 4: 受管主机上支持的 ESXi 版本

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

表. 5: 版本 3.2 的受支持的 vCenter Server 版本

vCenter 版本	Desktop Client 支持	Web Client 支持
v5.1 U2	是	否
v5.1 U3	是	否
v5.5 U1	是	是
v5.5 U2	是	是
v5.5 U3	是	是
v6.0	是	是
v6.0 U1	是	是
v6.0 U2	是	是
v6.0 U3	是	是

修改 vCenter 登录名

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

1. 在 OpenManage Integration for VMware vCenter 中的摘要选项卡上，使用相应链接打开**管理控制台**。
2. 在“登录”对话框中，键入密码。
3. 在左侧窗格中，单击 **VCENTER 注册**。注册的 vCenter 将在右侧窗格中显示。要打开**修改 vCenter 帐户**窗口，请在凭据下单击**修改**。
4. 输入 vCenter **用户名、密码和验证密码**；密码必须匹配。
5. 要更改密码，请单击 **应用**；或者要取消更改，请单击 **取消**。

 **注:** 如果没有为正在修改 vCenter 登录凭据的非管理员用户分配必要权限，将显示错误信息。

更新已注册 vCenter 服务器的 SSL 证书

如果 vCenter 服务器上的 SSL 证书已更改，则使用以下步骤导入 OpenManage Integration for VMware vCenter 的新证书。OpenManage Integration for VMware vCenter 使用此证书确保与其通信的 vCenter 服务器是正确的 vCenter 服务器而不是假冒者。

OpenManage Integration for VMware vCenter 使用 openssl API 创建证书签名请求 (CSR) (通过采用具有 2048 位密钥长度的 RSA 加密标准)。OpenManage Integration for VMware vCenter 所生成的 CSR 用于从受信任的证书颁发机构获取数字签名证书。OpenManage Integration for VMware vCenter 使用数字证书在 Web 服务器上启用 SSL 以进行安全的通信。

1. 启动 Web 浏览器中，然后输入 https://<ApplianceIPAddress>
2. 在左侧窗格中，单击 **VCENTER 注册**。注册的 vCenters 显示在右侧窗格中。要更新此证书，请单击**更新**。

卸载 OpenManage Integration for VMware vCenter


要移除 OpenManage Integration for VMware vCenter，必须首先使用管理控制台从 vCenter 服务器中将其取消注册。


1. 启动 Web 浏览器，然后输入 https://<ApplianceIPAddress>
2. 在 **vCenter 注册**页面中的 vCenter 服务器表下，通过单击**注销**来注销 OpenManage Integration for VMware vCenter。您可能有多个 vCenter，因此请确保已选择正确的 vCenter。
3. 在询问您是否确定要取消注册此服务器的 **取消注册 vCenter**对话框中，单击 **取消注册**。




向管理控制台上载 OpenManage Integration for VMware vCenter 许可证

1. 在 OpenManage Integration for VMware vCenter 中的“摘要”选项卡上，使用相应链接打开管理控制台。
2. 在“登录”对话框中，键入密码。
3. 在左侧窗格中，单击 **VCENTER 注册**。注册的 vCenter 将在表格中显示。要显示上载许可证对话框，请单击**上载许可证**。
4. 要导航到许可证文件，单击**浏览**按钮以导航到许可证文件，然后单击**上载**。

 **注:** 如果以任何形式修改或编辑了许可证文件，则设备会将其视为已损坏并且该文件将不起作用。

 **注:** 如果需要添加更多的主机，可添加许可证。请遵照上述过程添加更多许可证。

 **注:** 如果成功资源清册的第 11、12 和 13 代服务器数量等于已购买许可证的数量，可通过移除少量的第 11、12 或 13 代服务器来编辑现有连接配置文件。为移除的第 11、12 或 13 代服务器创建新的连接配置文件。

虚拟设备管理

虚拟设备管理中包含 OpenManage Integration for VMware vCenter 网络、版本、NTP 和 HTTPS 信息，并允许管理员：

- 重新启动虚拟设备
- 更新虚拟设备，以及配置更新存储库位置
- 生成包含设备日志记录信息的故障排除包。
- 输入网络时间协议 (NTP) 设置
- 上载并管理 HTTPS 证书

相关任务：

- [重新启动虚拟设备](#)
- [更新存储库位置并更新设备](#)
- [下载故障排除包](#)
- [设置 NTP 服务器](#)

重新启动虚拟设备

重新启动虚拟设备会让您从管理控制台上注销，并且 OpenManage Integration for VMware vCenter 将不可用，直到虚拟设备及其服务激活。

1. 在 OpenManage Integration for VMware vCenter 中的“管理控制台”下，使用链接打开管理控制台。
2. 在“登录”对话框中，键入密码。
3. 在左侧窗格中，单击**设备管理**。
4. 要重新启动 OpenManage Integration for VMware vCenter，请单击**重新启动虚拟设备**。
5. 在 **重新启动虚拟设备**对话框中，要重新启动虚拟设备，请单击 **应用**，或单击 **取消**以取消。

更新存储库位置和虚拟设备

在更新虚拟设备之前进行备份以确保所有数据都受到保护。请参阅[管理备份和还原](#)。

1. 在 OpenManage Integration for VMware vCenter 中的“管理控制台”下，使用链接打开管理控制台。
2. 在“登录”对话框中，键入密码。
3. 在左侧窗格中，单击**设备管理**。
4. 在设备更新旁边，单击 **编辑**。
5. 在**设备更新**窗口，输入**存储库位置 URL**，然后单击**应用**。

 **注:** 如果更新位置位于外部网络（例如 Dell FTP 站点）上，则必须在“HTTP 代理”区域中输入代理。

更新虚拟设备软件

为防止数据丢失，请在开始软件更新之前执行设备备份。

1. 启动 Web 浏览器中，然后输入 `https://<ApplianceIPAddress>`。
2. 在左侧窗格中，单击**设备管理**。
3. 要将虚拟设备更新为 **设备更新**下列出的软件版本，请单击**更新虚拟设备**。
4. 在**更新设备**对话框中，将列出当前和可用的版本。要开始更新，请单击 **更新**。
5. 系统将被锁定并置于维护模式。更新完成后，设备页面将显示新安装的版本。

下载故障排除包

使用此信息协助进行故障排除，或将信息发送给技术支持部门。

1. 启动 Web 浏览器中，然后输入 `https://<ApplianceIPAddress>`。
2. 在左侧窗格中，单击**设备管理**。
3. 要生成故障排除包对话框，请单击**生成故障排除包**。
4. 单击**下载故障排除捆绑包**链接。
5. 要退出，请单击**关闭**。

设置 HTTP 代理

您可以使用管理控制台设置 HTTP 代理设置。

1. 在 OpenManage Integration for VMware vCenter 中的“摘要”选项卡上，使用相应链接打开管理控制台。
2. 在“登录”对话框中，键入密码。
3. 在左侧窗格中，单击**设备管理**。
4. 在**设备管理**页面中，向下滚动至 **HTTP 代理设置**，然后单击**编辑**。
5. 在 **编辑**页面中，执行以下操作：
 - a. 要启用 HTTP 代理设置，在 **使用 HTTP 代理设置**旁边，选择 **启用**。
 - b. 在**代理服务器地址**文本框中，输入代理服务器地址。
 - c. 在**代理服务器端口**文本框中，输入代理服务器端口。
 - d. 要使用代理凭据，在 **使用代理凭据**旁边，选择**是**。
 - e. 如果要使用凭据，在 **用户名**文本框中，输入用户名。
 - f. 在 **密码**文本框中，键入密码。
6. 单击**应用**。

设置 NTP 服务器

可使用网络时间协议 (NTP) 同步虚拟设备时钟与 NTP 服务器的时钟。

1. 在 OpenManage Integration for VMware vCenter 中的“管理控制台”下，使用链接打开管理控制台。
2. 在“登录”对话框中，键入密码。
3. 在左侧窗格中，单击**设备管理**。
4. 单击 **NTP 设置**下的**编辑**。
5. 选中 **已启用**复选框。输入 **首选 NTP 服务器**和 **次要 NTP 服务器**的 **主机名或 IP 地址**，然后单击 **应用**。
6. 要退出，请单击 **取消**。

 **注:** 虚拟设备时钟与 NTP 服务器同步可能约需 10 分钟。



生成证书签名请求

 **注:** 向 vCenter 注册 OpenManage Integration for VMware vCenter 之前，必须上载证书。

生成新证书签名请求可阻止通过以前生成的 CSR 创建的证书上载到设备。


1. 在 OpenManage Integration for VMware vCenter 中的“管理控制台”下，使用链接打开管理控制台。
2. 在“登录”对话框中，键入密码。
3. 在左侧窗格中，单击**设备管理**。
4. 单击**生成 HTTPS 证书的证书签名请求**。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载到设备。要继续请求，请单击**继续**，或单击**取消取消**。
5. 输入请求的**通用名称、组织名称、组织单位、地点、省/州/市/自治区名称、国家/地区**和**电子邮件**。单击**继续**。
6. 单击**下载**，然后将产生的证书请求保存到可访问的位置。

上载 HTTPS 证书

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

 **注:** 您可以使用 Microsoft Internet Explorer、Firefox 或 Chrome 上载证书。

1. 在 OpenManage Integration for VMware vCenter 中的“摘要”选项卡上，使用相应链接打开管理控制台。
2. 在“登录”对话框中，键入密码。
3. 在左侧窗格中，单击**设备管理**。
4. 单击**上载 HTTPS 证书的证书**。
5. 在**上载证书**对话框中，单击**确定**。
6. 要选择上载的证书，请单击**浏览**，然后单击**上载**。
7. 如果要中止上载，请单击**取消**。

 **注:** 证书必须使用 PEM 格式。

还原默认的 HTTPS 证书

 **注:** 如果想为您的设备上载自定义证书，需要在 vCenter 注册前上载新证书。如果是在 vCenter 注册后上载新自定义证书，Web Client 中将显示通信错误。要解决此问题，需要注销并在 vCenter 中重新注册设备。

1. 在 OpenManage Integration for VMware vCenter 中的“摘要”选项卡上，使用相应链接打开管理控制台。
2. 在“登录”对话框中，键入密码。
3. 在左侧窗格中，单击**设备管理**。
4. 单击**HTTPS 证书**下的**还原默认证书**链接。
5. 在还原默认证书对话框中，单击**应用**。

设置全局警报

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

1. 在 OpenManage Integration for VMware vCenter 中的“管理控制台”下，使用链接打开管理控制台。
2. 在“登录”对话框中，键入密码。
3. 在左侧窗格中，单击**警报管理**。要输入新的 vCenter 警报设置，请单击**编辑**。
4. 输入以下各项的数值：
 - 最大警报数

- 保留警报的天数
 - 重复警报超时（秒数）
5. 要保存您的设置，请单击 **应用**，或单击 **取消**以取消。

管理备份和还原

管理备份和还原在 Administrative Console 完成。此页面上的任务包括：

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

配置备份和还原

备份和还原功能将 OpenManage Integration for VMware vCenter 数据库备份到远程位置，以后可从该位置进行还原。配置文件、模板和主机信息都包括在备份中。建议您计划自动备份以防止数据丢失。此步骤之后，您必须配置备份计划。

 **注: NTP 设置未保存和还原。**

1. 在 OpenManage Integration for VMware vCenter 中的“管理控制台”下，使用链接打开管理控制台。
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**。
4. 要编辑当前备份和还原设置，请单击 **编辑**。
5. 在 **设置和详细信息**页面中，执行以下操作：
 - a. 在 **备份位置**文本框中，键入指向备份文件的路径。
 - b. 在 **用户名**文本框中，键入用户名。
 - c. 在 **密码**文本框中，键入密码。
 - d. 在 **输入用于加密备份的密码**下，在文本框中键入加密的密码。
加密密码可包含字母数字字符和下列特殊字符：!@#%*。不存在长度限制。
 - e. 在 **验证密码**文本框中，重新键入加密的密码。
6. 要保存这些设置，请单击 **应用**。
7. 配置备份计划。有关详细信息，请参阅[计划自动备份](#)。

计划自动备份

这是配置备份和还原的第二部分。有关配置备份位置和凭据的详细信息，请参阅[配置备份和还原](#)。

计划自动备份：


1. 在 OpenManage Integration for VMware vCenter 中的“管理控制台”下，使用链接打开管理控制台。
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**。
4. 要编辑备份和还原设置，请单击 **编辑 自动计划的备份**（此操作将激活字段）。
5. 要启用备份，请单击**已启用**。
6. 选中您要运行备份于每周的星期几的复选框。
7. 在 **备份时间 [24 小时制, HH:mm]**文本框中，输入 HH:mm（小时：分钟）格式的时间。
下一个备份将填充下一计划的备份的日期和时间。
8. 单击**应用**。



执行即时备份

1. 在 OpenManage Integration for VMware vCenter 中的“管理控制台”下，使用链接打开管理控制台。
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**。
4. 单击 **立即备份**。
5. 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，选中该复选框。
6. 输入 **备份位置、用户名、密码和加密密码**。
加密密码可包含字母数字字符和下列特殊字符：!@#\$%*. 不存在长度限制。
7. 单击 **备份**。

从备份还原数据库

 **注:** 还原操作导致虚拟设备在该操作完成后重新引导。

1. 在 OpenManage Integration for VMware vCenter 中的“管理控制台”下，使用链接打开管理控制台。
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**，此时将显示当前备份和还原设置。
4. 单击 **立即还原**。
5. 在“立即还原”对话框中，输入文件位置以及 **backup.gz** 文件（CIFS/NFS 格式）。
6. 输入备份文件的 **用户名、密码和加密密码**。
加密密码可包含字母数字字符和下列特殊字符：!@#\$%*. 不存在长度限制。
7. 要保存您的更改，请单击**应用**。
单击应用之后，设备将重新引导或重新启动。

了解 vSphere Client 控制台

此 **vSphere Client 控制台** 位于虚拟机上的 vSphere Client 中。此**控制台**与管理控制台协同工作，提供以下功能：

- [配置网络设置](#)
- [更改虚拟设备密码](#)
- [设置本地时区](#)
- [重新启动虚拟设备](#)
- [将虚拟设备重设为出厂设置](#)
- [刷新控制台](#)
- [从控制台注销](#)
- [只读用户角色](#)
- [从 OMIVV 3.0 版本升级至当前版本](#)
- [从旧版本迁移至 OMIVV 3.1 版本](#)

使用箭头键向上或向下导航。选择所需选项后，立即按 **<ENTER>**。访问**控制台**屏幕后，VMware vSphere Client 便开始控制您的光标。要摆脱控制，请按 **<CTRL> + <ALT>**。

配置网络设置

在 vSphere Client 控制台中进行网络设置更改。

1. 在 vSphere Web 客户端的 Navigator 中，选择 **vCenter**。
2. 在 Navigator 中，选择您要管理的虚拟机。
3. 请执行以下操作之一：
 - 在“对象”选项卡上，选择操作 → **打开控制台**。
 - 右键单击您所选的虚拟设备，然后选择**打开控制台**。
4. 在 **控制台**窗口中，选择 **配置网络**，然后按 **<ENTER>**。
5. 在 **编辑设备**或 **编辑 DNS** 配置下输入所需的网络设置，然后单击 **保存并退出**。要中止任何更改，请单击 **退出**。

更改虚拟设备密码

可使用设备控制台在 vSphere Client 中更改虚拟设备密码。

要更改虚拟设备密码：

1. 登录部署了 OpenManage Integration for VMware vCenter 的 vCenter/ESXi 主机。选择 OpenManage Integration for VMware vCenter 虚拟机，然后单击**控制台**选项卡。
2. 使用用户名 admin 和之前设置的密码登录设备。
3. 在 OpenManage Integration for VMware vCenter“虚拟设备设置”窗口中，单击**更改管理员密码**。
4. 在**更改密码**窗口中，输入当前密码
5. 在**新密码**中输入新密码。
6. 在**确认新密码**中输入新密码，以进行确认。
7. 单击**更改密码**按钮
此时将显**密码更新成功**消息。
8. 单击**确定**。

设置本地时区

要设置本地时区：

 **注：**您仅可以编辑时区而非当前时间和日期。

1. 在 **vSphere 客户端**中选择 OpenManage Integration for VMware vCenter 虚拟机，然后单击**控制台**选项卡。
2. 选择 **设置时区**，然后按 **<ENTER>**。
3. 在 **时区选择**窗口中，选择所需的时区并单击 **确定**。要取消更改，请单击 **取消**。时区即完成更新。

重新引导虚拟设备

要重新引导虚拟设备：

1. 在 **vSphere 客户端**中选择 OpenManage Integration for VMware vCenter 虚拟机，然后单击**控制台**选项卡。
2. 选择 **重新引导此虚拟设备**，然后按 **<ENTER>**。
3. 随即显示以下消息：
`If there are any processes running on this appliance they will be terminated by this action. Are you sure you wish to do this?`
4. 输入 **y** 重新引导或输入 **n** 取消。设备将重新引导。



将虚拟设备重设为出厂设置

将虚拟设备重设为出厂设置：

1. 在 **vSphere Web 客户端** 中，选择 OpenManage Integration for VMware vCenter 虚拟机，然后单击**控制台**选项卡
2. 选择 **将此虚拟设备重设为出厂设置**并按 **<ENTER>**。
3. 此时将显示以下通知：

```
This operation is completely Irreversible if you continue you will completely reset
*this* appliance to its original settings. All changes you have made to this appliance
will be Lost. Are you sure you wish to Reset this Appliance to Factory Settings?
```

4. 输入 **y**（是）重设或输入 **n**（否）取消。

该设备将重设为原来的出厂设置，所有其他设置和保存的数据都将丢失。

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

刷新控制台视图

要刷新控制台视图，请选择 **刷新**，然后按 **<ENTER>**。

从控制台注销

要从控制台注销，单击您已登录帐户右上角的**注销**。

只读用户角色

名为只读的无权限用户角色出于诊断目的具有 shell 访问权限。只读用户具有运行安装的有限权限。只读用户的密码设置为**只读**。出于安全考虑，只读用户的密码已更改为非管理密码（对于 OMIVV v1.0 到 v3.2）。

故障排除

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](#)
- [联系 Dell](#)
- [相关产品信息](#)

常见问题（FAQ）

本节介绍一些常见问题及解决方案。

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

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

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

受影响的版本: 3.1 版

如果 vCenter 处于空闲状态长达数小时, 则单击 OpenManage Integration 选项卡和 Management Center 会将 OMIVV 的内容替换为“!”图标。应如何操作来恢复会话?

如果 vCenter 处于空闲状态长达数小时, 单击已进行过资源清册的主机的 **OpenManage Integration** 选项卡和 **Dell Management Center** 图标以执行任何操作时, 会将 OMIVV 的内容替换为“!”图标。

解决方案: 您可以通过关闭当前会话, 然后再次登录来恢复会话。

受影响的版本: 3.1、vCenter 6.0 及更高版本

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

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

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

受影响的版本: 3.1 版

如何将 OMIVV 插件的状态更改为“已启用”?

在安装 OMIVV 并通过 vCenter Server 进行注册后, 有时 OMIVV 插件显示的状态不是**已启用**状态, 而是**下载并安装**状态。要将 OMIVV 插件的状态更改为“已启用”, 请执行以下步骤:

1. 从 vSphere Client 和 vSphere Web Client 注销。
2. 引导 OMIVV 设备进入单一用户模式。



3. 编辑 `/etc/hosts` 文件：`<vCenterIP> <myvCenter.mydomain.com> <myvCenter>`，并为 vCenter Server 添加一个 DNS 条目。
例如 `10.35.210.126 myvCenter.us.dell.com myvCenter`
4. 重新引导 OMIVV 设备。根据 vCenter 设备的使用情况执行以下任一步骤。
 - a. 如果使用的是 Windows vCenter Server，请编辑 `c:\system\window32\drivers\etc\hosts` 中的主机文件，并为 OMIVV 设备添加一个 DNS 条目。
例如 `10.35.210.120 myomivv.us.dell.com myomivv`。

执行以下命令刷新 DNS：

```
ipconfig /flushdns
```
 - b. 如果使用的是 vCenter 设备，请编辑 `/etc/hosts` 文件，并为 OMIVV 设备添加一个 DNS 条目。
例如 `10.35.210.120 myomivv.us.dell.com myomivv`。

重新引导 vCenter 设备。
5. 单击**取消注册**以取消注册 OMIVV。
6. 重新登录到 vSphere Client 和 vSphere Web Client 以验证 OMIVV 插件是否显示**已启用**状态。

受影响的版本：3.0 版

执行 OpenManage Integration for VMware vCenter 还原后，如果 vSphere Client 中未显示 Dell Management Center 图标怎么办？

从以前创建的备份进行还原时，OpenManage Integration for VMware vCenter 可能不会显示 Dell Management Center 图标。

解决方案：您可以从 OMIVV 设备取消注册 vCenter Server，然后再次注册 vCenter Server。

受影响的版本：仅在执行从版本 OMIVV 3.0.0.173 到版本 OMIVV 3.0.0.197 的备份还原时，可能才出现这种问题。

在设备更新后，“关于”屏幕未更新 OMIVV 版本

这是 Internet Explorer 的已知问题，它仍在使用旧高速缓存值。清除 IE 的高速缓存可显示正确版本。

不支持使用 OpenManage Integration for VMware vCenter 更新固件版本为 13.5.2 的 Intel 网卡。

Dell PowerEdge 第 12 代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 Lifecycle Controller 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，则可以使用 OpenManage Integration for VMware vCenter 进行更新。有关更多信息，请参阅 <http://en.community.dell.com/techcenter/b/techcenter/archive/2013/03/20/intel-network-controller-card-with-v13-5-2-firmware-cannot-be-upgraded-using-lifecycle-controller-to-v13-5-6.aspx>

 **注：**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。

在运行保修检索作业时，保修作业状态未列在“保修作业队列”页面中

如果您的网络需要代理详细信息以连接到互联网，且未在 OMIVV 设备上设置代理，该保修检索作业失败，作业未列在保修作业队列中。

解决方案：设置代理的详细信息，并再次触发保修作业。

受影响的版本：所有

由于 DUP 存在分段要求，使用 OpenManage Integration for VMware vCenter 将 Intel 网卡从 14.5 或 15.0 更新至 16.x 失败

这对于 NIC 14.5 和 NIC 15.0 而言是一个已知问题。您必须先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

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

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

解决方案：必须手动取消该任务。

受影响的版本：所有

管理门户仍然显示无法访问的更新存储库位置。

如果用户提供了无法访问的更新存储库路径，在“设备更新”视图顶部会显示错误消息“Failed: Error while connecting to the URL ...”（失败：连接到 URL 时出错...），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

如果使用 DHCP 进行设备 IP 和 DNS 设置覆盖，在重启设备后，DNS 配置设置为何还原到原始设置？

存在一个已知缺陷：静态分配的 DNS 设置会被 DHCP 值取代。当使用 DHCP 获取 IP 设置并且静态分配 DNS 值时会发生这种情况。当 DHCP 租约延期或设备重新启动时，静态分配的 DNS 设置会被移除。解决方案：当 DNS 服务器设置将不同于 DHCP 时，静态分配 IP 设置。

受影响的版本：所有

当我执行一对多固件更新时，为什么我的系统无法进入维护模式？

一些固件更新不需要重新引导主机。在这种情况下，无需将主机置于维护模式即可执行固件更新。

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

当我在锁定模式下将一个主机添加到连接配置文件时，资源清册开始，但随后失败，并指示“No Remote Access Controller was found or Inventory is not supported on this host（未找到远程访问控制器或在本主机上不支持资源清册）”。资源清册应该可用于锁定模式的主机，对吗？

如果您将主机置于锁定模式或从锁定模式退出，必须等待 30 分钟后才能执行下一次操作。如果使用 11G 主机进行固件更新，则固件更新向导不会显示任何捆绑包，即使所提供的存储库包含该系统的捆绑包也是如此。当 11G 主机没有配置为通过 OMSA 向 OpenManage Integration 发送陷阱时，就会发生这种情况。

解决方案：使用 OpenManage Integration Desktop 客户端的主机“符合性”屏幕来确认主机的符合性。如果该主机不具备符合性，则使用“修复主机符合性”来使其具备符合性。

受影响的版本：2.2 及更高版本



在具有 PERC S300 引导控制器的服务器上，我的 ESXi 部署为什么会失败？

在包含 PERC S300 引导控制器的 Dell PowerEdge 服务器上使用不同的 ESXi 版本部署 OpenManage Integration for VMware vCenter 失败。Dell 定制的 ESXi 操作系统不含 PERC S300 引导控制器的驱动程序，这导致在操作系统安装过程中无法识别引导控制器/HDD。包含 PERC S300 引导控制器的服务器不支持用于 OpenManage Integration for VMware vCenter 部署。

在单击固件链接后，为什么我会看到显示了一条错误消息？

如果您的网络速度较慢 (9600 BPS)，您可能会收到通信错误消息。当您在 OpenManage Integration for VMware vCenter 的 vSphere 客户端中单击“固件”链接时，可能会显示此错误消息。当尝试获取软件资源清册列表时，如果连接超时，将会出现此错误。Microsoft Internet Explorer 会启动此超时。对于 Microsoft Internet Explorer 版本 9/10，默认的“接收超时”值设置为 10 秒。请通过以下步骤修复此问题。

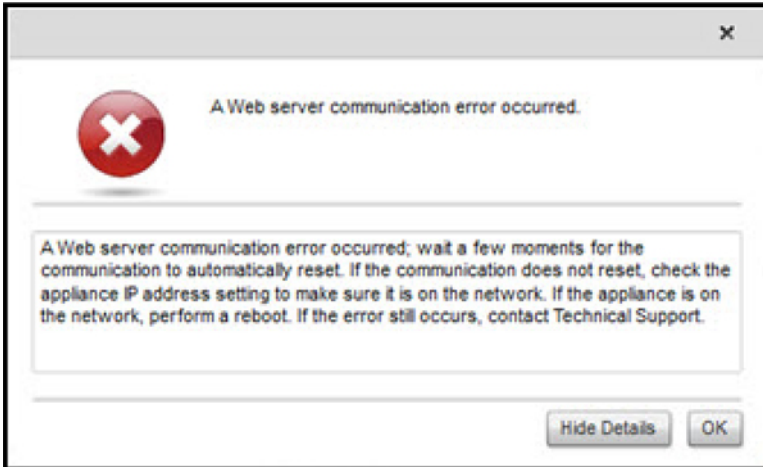



图 5: 固件链接通信错误

1. 打开 Microsoft 注册表编辑器 (Regedit)。
2. 导航至以下位置：
KHEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
3. 为 ReceiveTimeout 添加一个 DWORD 值。
4. 将该值设置为 30 秒 (30000) [在您的环境中，此值可能需要为更大的值]。
5. 退出 Regedit。
6. 重新启动 Internet Explorer。

 **注：仅仅打开新的 Internet Explorer 窗口还不够。请重新启动 Internet Explorer 浏览器。**

OpenManage Integration for VMware vCenter 在哪一代 Dell 服务器上配置和支持 SNMP 陷阱？

OpenManage Integration for VMware vCenter 在 12 代以前的服务器上支持 OMSA SNMP 陷阱，在第 12 代服务器上支持 iDRAC 陷阱。


OpenManage Integration for VMware vCenter 如何支持三个以上处于链接模式的 vCenter？

在链接模式下，每个虚拟设备最多支持三个 vCenter。如果您有十个以上的 vCenter，则需要为每十个具有关联许可的 vCenter 提供一个新的设备实例。

OpenManage Integration for VMware vCenter 是否支持处于链接模式的 vCenter?

是，OpenManage Integration for VMware vCenter 最多支持 10 个处于链接模式或非链接模式的 vCenter。有关 OpenManage Integration for VMware vCenter 如何在链接模式下工作的更多信息，请参阅 www.Dell.com 上的白皮书 *OpenManage Integration for VMware vCenter: Working in Linked Mode*（OpenManage Integration for VMware vCenter：在链接模式下工作）。

什么是 OpenManage Integration for VMware vCenter 的必要端口设置?

 **注：**在使用 OpenManage Integration for VMware vCenter 中的“符合性”窗口提供的 *修复不合规 vSphere 主机* 链接部署 OMSA 代理时，OpenManage Integration for VMware vCenter 将启动 http 客户端服务，启用 ESXI 5.0 之后版本的端口 8080，以下载 OMSA VIB 并安装它。当 OMSA 安装完成后，该服务将自动停止，端口也将关闭。

对 OpenManage Integration for VMware vCenter 使用这些端口设置。

表. 6: 虚拟设备端口

端口号	协议	端口类型	最大加密级别	方向	用途	可配置
21	FTP	TCP	无	出	FTP 命令客户端	否
53	DNS	TCP	无	出	DNS 客户端	否
80	HTTP	TCP	无	出	Dell 联机数据访问	否
80	HTTP	TCP	无	进	管理控制台	否
162	SNMP 代理	UDP	无	进	SNMP 代理（服务器）	否
11620	SNMP 代理	UDP	无	进	SNMP 代理（服务器）	否
443	HTTPS	TCP	128 位	进	HTTPS 服务器	否
443	WSMAN	TCP	128 位	进/出	iDRAC/OMSA 通信	否
4433	HTTPS	TCP	128 位	进	自动查找	否
2049	NFS	UDP	无	进/出	公共共享	否
4001–4004	NFS	UDP	无	进/出	公共共享	否
11620	SNMP 代理	UDP	无	进	SNMP 代理（服务器）	否

表. 7: 受管节点

端口号	协议	端口类型	最大加密级别	方向	用途	可配置
162、11620	SNMP	UDP	无	出	硬件事件	否
443	WSMAN	TCP	128 位	进	iDRAC/OMSA 通信	否
4433	HTTPS	TCP	128 位	出	自动查找	否
2049	NFS	UDP	无	进/出	公共共享	否
4001–4004	NFS	UDP	无	进/出	公共共享	否
443	HTTPS	TCP	128 位	进	HTTPS 服务器	否
8080	HTTP	TCP		进	HTTP 服务器； 下载 OMSA VIB 并修复不符合要	否

端口号	协议	端口类型	最大加密级别	方向	用途	可配置
50	RMCP	UDP/TCP	128 位	出	求的 vSphere 主机 远程邮件检查协议	否
51	IMP	UDP/TCP	不适用	不适用	IMP 逻辑地址维护	否
5353	mDNS	UDP/TCP		进/出	多播 DNS	否
631	IPP	UDP/TCP	无	出	因特网打印协议 (IPP)	否
69	TFTP	UDP	128 位	进/出	普通文件传输	否
111	NFS	UDP/TCP	128 位	进	SUN 远程过程调用 (Portmap)	否
68	bootp	UDP	无	出	自举协议客户端	否

虚拟设备成功安装和操作的最低要求是什么？

以下设置概述了最低设备要求：

- Google Chrome 版本 28 及更高版本
- Microsoft Internet Explorer 版本 9 和 10
- Mozilla Firefox 版本 22 及更高版本
- 保留内存：2 GB

 **注：为获得最佳性能，Dell 建议 3 GB。**

- 磁盘：43.5 GB。
- CPU：2 个虚拟 CPU。

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

如果仅选择了硬件配置文件模板用于部署，则用于查找的用户的密码不会更改到新的凭据中。这是有意这样做的，使得插件不能出于部署需要与 iDRAC 未来使用通信。

为什么在“系统概览”页面的“处理器视图”中处理器版本中为“不适用”？

如果是在第 12 代或更高的 PowerEdge Dell 服务器中，处理器版本显示在“品牌”列。如果是下一代服务器，处理器版本则显示在“版本”列。

如果使用 DHCP 进行设备 IP 和 DNS 设置覆盖，在重启设备后，DNS 配置设置为何还原到原始设置？

存在一个已知缺陷：静态分配的 DNS 设置会被 DHCP 值取代。当使用 DHCP 获取 IP 设置并且静态分配 DNS 值时会发生这种情况。当 DHCP 租约延期或设备重新启动时，静态分配的 DNS 设置会被移除。解决方案：当 DNS 服务器设置将不同于 DHCP 时，静态分配 IP 设置。

受影响的版本：所有


为什么我没有在“vCenter 主机和群集”页面上看到我的新 iDRAC 版本的详细信息？

在 vSphere Desktop 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 CSIOR 状态。如果 CSIOR 尚未启用，则启用 CSIOR 并重新引导主机。如果 CSIOR 已启用，则登录到 iDRAC 控制台，重设 iDRAC，等待几分钟，然后在 vSphere Desktop 客户端中刷新“固件更新”页面。

我如何使用 OMSA 模拟温度硬件故障来测试事件设置？

为确保事件工作正常：

1. 在 OMSA 用户界面中，导航至**警报管理** → **平台事件**。
2. 选中**启用平台事件筛选器警报**复选框。
3. 向下滚动至底部，单击**应用更改**。
4. 要确保启用特定事件（例如温度警告），请从左侧树中选择**主系统机箱**。
5. 在**主系统机箱**下选择**温度**。
6. 选择 **警报管理**选项卡，然后选择 **温度探测器警告**。
7. 选择 **广播一条消息**复选框，然后选择 **应用更改**。
8. 要引发温度警告事件，请从左侧的树视图中选择**主系统机箱**。
9. 在 **主系统机箱**下选择 **温度**。
10. 选择 **系统板环境温度**链接，然后选择 **设置为值**选项按钮。
11. 将 **最大警告阈值**设置为低于当前所列读数；例如，如果当前读数为 27，将阈值设为 25。
12. 选择 **应用更改**，温度警告事件即生成。要造成另一个事件，请使用相同的 **Set to Values（设置为值）**选项恢复原始设置。事件会生成为警告，之后恢复正常状态。如果一切工作正常，请导航至 **vCenter 任务与事件**视图；温度探测器警告事件应会显示。

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

我在 Dell 主机系统上安装了 OMSA 代理程序，但我仍然收到“OMSA 未安装”的错误消息。我该怎么办？

要在第 11 代服务器上解决此问题，请执行以下操作：

1. 在主机系统上安装包含有 **远程启用**组件的 **OMSA**。
2. 如果您使用命令行安装 OMSA，确保指定 **-c** 选项。如果 OMSA 已安装，请通过 **-c** 选项重新安装它并重新启动服务：

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

对于 ESXi 主机，您必须使用 **VMware Remote CLI 工具**安装 **OMSA VIB**，然后重新引导系统。

OpenManage Integration for VMware vCenter 能否支持启用了锁定模式的 ESXi？

可以。此版本支持 ESXi 5.0 及更高版本主机中的锁定模式。

在我尝试使用锁定模式时失败。

当我在锁定模式下将一个主机添加到连接配置文件时，资源清册开始，但随后失败，并指示“No Remote Access Controller was found or Inventory is not supported on this host（未找到远程访问控制器或在本主机上不支持资源清册）”。资源清册应该可用于锁定模式的主机，对吗？

如果您将主机置于锁定模式或从锁定模式中移除主机，需要等待 30 分钟后才能对 OpenManage Integration for VMware vCenter 执行下一次操作。



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

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

解决方案：必须手动取消该任务。

受影响的版本：所有

我应将什么设置用于 UserVars.CIMoeMProviderEnable With ESXi 4.1 U1？

将 `UserVars.CIMoeMProviderEnabled` 设置为 1。

我使用一台参考服务器创建硬件配置文件，但创建失败。我该怎么办？

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

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

我尝试在刀片服务器上部署 ESXi，但部署失败。我该怎么办？

1. 确保 **ISO 位置 (NFS 路径)** 和 **分级文件夹路径** 准确无误。
2. 确保在分配服务器标识时选择的 **NIC** 与虚拟设备在同一个网络上。
3. 如果使用的是 **静态 IP 地址**，确保提供的网络信息（包括子网掩码和默认网关）准确无误。此外，还要确保该 IP 地址尚未在网络上分配。
4. 确保系统至少可以看到一个 **虚拟磁盘**。ESXi 也安装到内部 RIPS SD 卡。

为何我的虚拟机监管程序在 R210 II 机器上部署失败？

由于 BIOS 从所连接的 ISO 引导故障，在 R210 II 系统上的超时问题造成虚拟机监管程序部署故障错误。要解决此问题，请在该机器上手动安装虚拟机监管程序。

为何我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。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 OpenManage Integration for VMware vCenter。

使用 ESXi ISO 设置了 NFS 共享，但装载共享位置错误造成部署失败。

要查找解决方案：

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

我如何强制移除虚拟设备？

1. 转到 `https://<vcenter_serverIPAddress>/mob`
2. 输入 VMware vCenter 管理凭据。
3. 单击内容。

4. 单击 **ExtensionManager**。
5. 单击 **UnregisterExtension**。
6. 输入扩展密钥 `com.dell.plugin.openManage_integration_for_VMware_vCenter`，然后单击**调用方法**。
7. 输入扩展密钥 `com.dell.plugin.openManage_integration_for_VMware_vCenter_WebClient`，然后单击**调用方法**。
8. 关闭 OpenManage Integration for VMware vCenter 虚拟设备后将其删除。

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的显示器，“加密密码”字段不会显示在“立即备份”窗口中。您必须向下滚动页面来输入加密密码。

我的固件更新失败，我怎么办？

检查虚拟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。

连接配置文件测试凭据期间的性能极慢或没有响应。

服务器上的 iDRAC 只有一个用户（例如，只有 `root`）并且该用户处于禁用状态，或所有用户处于禁用状态。与禁用状态的服务器通信会造成延迟。要修复此问题，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，选择以下其中一项：
 - iDRAC 6：选择 **iDRAC 设置** → **网络/安全选项卡** → **用户选项卡**。
 - iDRAC 7：选择 **iDRAC 设置** → **用户选项卡**。
 - iDRAC 8：选择 **iDRAC 设置** → **用户选项卡**。
4. 要编辑设置，在用户 ID 列中，单击 `admin (root)` 用户的链接。
5. 单击**配置用户**，然后单击**下一步**。
6. 在所选用户的“用户配置”页中，选择“启用用户”旁边的复选框，然后单击**应用**。

OpenManage Integration for VMware vCenter 是否支持 VMware vCenter 服务器设备？

是的，OpenManage Integration for VMware vCenter 支持 VMware vCenter 服务器设备。

OpenManage Integration for VMware vCenter 是否支持 vSphere Web 客户端？

是的，OpenManage Integration for VMware vCenter 支持 VMware vSphere Web 客户端。

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

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。

在备份和还原 OpenManage Integration for VMware vCenter 后，为何警报设置没有被还原？

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

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

Bare Metal Deployment Issues

This section deals with issues found during the deployment process.

Auto-Discovery and Handshake Prerequisites

- Prior to running auto-discovery and handshake, make sure that iDRAC and Lifecycle Controller firmware and BIOS versions meet the minimum recommendations.
- CSIOR must have run at least once on the system or iDRAC.

Hardware Configuration Failure

- Before initiating a deployment task, make sure the system has completed CSIOR and is not in the process of rebooting.
- It is highly recommended that BIOS configuration be run in Clone mode, so that the reference server is an identical system.
- Some controllers do not allow creation of a RAID 0 array with one drive. This feature is supported only on high-end controllers, and the application of such a hardware profile can cause failures.

OS deployment failure on PowerEdge servers running iDRAC version 2.35.35.35

- While deploying the ESXi operating system, the host fails to load all the ESXi packages from the OMIVV appliance, displaying the following message:

Fatal error: 33 (Inconsistent data)

- It is recommended that you update the iDRAC firmware to version 2.40.40.40 or later.


在新购买的系统上启用自动查找

主机系统的自动查找功能在默认情况下并未启用；而是必须在购买时申请启用。如果在购买时申请了启用自动查找，在 iDRAC 上会启用 DHCP，并且 admin 帐户被禁用。不需要为 iDRAC 配置静态 IP 地址。它会从网络上的 DHCP 服务器获得一个地址。要利用自动查找功能，DHCP 服务器或 DNS 服务器（或两者）必须被配置为支持查找进程。出厂过程已运行 CSIOR。

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`

联系 Dell

 **注：**如果没有活动的 Internet 连接，您可以在购货发票、装箱单、帐单或 Dell 产品目录上查找联系信息。

Dell 提供了若干联机及电话支持和服务选项。服务会因所在国家和地区以及产品的不同而有所差异，您所在的地区可能不提供某些服务。如要联系 Dell 解决有关销售、技术支持或客户服务问题：

1. 请转至 dell.com/support
2. 选择您的支持类别。
3. 在页面底部的**选择国家/地区**下拉列表中，确认您所在的国家或地区。
4. 根据您的需要，选择相应的服务或支持链接。

OpenManage Integration for VMware vCenter 相关信息

- 查看或下载 PowerEdge™ 服务器的 Dell 服务器说明文件：[Dell PowerEdge 手册](#)
- Dell OpenManage System Administrator 说明文件：[Dell OMSA 说明文件](#)
- Dell Lifecycle Controller 说明文件：[DLCI 说明文件](#)



Dell PowerEdge 服务器的虚拟化相关事件

下表列出了第 11 代、12 代和 13 代 PowerEdge 服务器的虚拟化相关严重和警告事件，包括事件名称、说明和严重性级别。

表. 8: 第 11 代、12 代和 13 代 PowerEdge 服务器的虚拟化相关事件

事件名称	说明	严重性	建议操作
Dell-Current sensor detected a warning value	指定系统中的电流传感器超过警告阈值。	警告	无操作
Dell-Current sensor detected a failure value	指定系统中的电流传感器超过故障阈值。	Error (错误)	使系统进入维护模式
Dell-Current sensor detected a non-recoverable value	指定系统中的电流传感器检测到无法恢复的错误	Error (错误)	无操作
Dell-Redundancy regained	传感器已恢复正常值	信息	无操作
Dell-Redundancy degraded	指定系统中的冗余传感器检测到其中一个冗余装置组件发生故障，但该装置仍为冗余。	警告	无操作
Dell - Redundancy lost	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。	Error (错误)	使系统进入维护模式
Dell - Power supply returned to normal	传感器已恢复正常值	信息	无操作
Dell - Power supply detected a warning	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 - Power supply detected a failure	电源设备已断开连接或失败。	Error (错误)	使系统进入维护模式
Dell - Power supply sensor detected a non-recoverable value	指定系统中的电源传感器检测到无法恢复的错误。	Error (错误)	无操作
Dell - Memory Device Status warning	内存设备纠错率超过可接受值。	警告	无操作
Dell - Memory Device error	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。	Error (错误)	使系统进入维护模式
Dell - Fan enclosure inserted into system	传感器已恢复正常值。	信息	无操作
Dell - Fan enclosure removed from system	风扇罩已从指定系统中卸下。	警告	无操作

事件名称	说明	严重性	建议操作
Dell - Fan enclosure removed from system for an extended amount of time	风扇罩从指定系统中卸下已持续用户可定义的一段时间。	Error (错误)	无操作
Dell - Fan enclosure sensor detected a non-recoverable value	指定系统中的风扇罩传感器检测到无法恢复的错误。	Error (错误)	无操作
Dell - AC power has been restored	传感器已恢复正常值。	信息	无操作
Dell - AC power has been lost warning	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 - An AC power cord has lost its power	交流电源线已断电，并且由于缺乏冗余，需将其分类为错误。	Error (错误)	无操作
Dell - Processor sensor returned to a normal value	传感器已恢复正常值	信息	无操作
Dell - Processor sensor detected a warning value	指定系统中的处理器传感器处于限制状态。	警告	无操作
Dell - Processor sensor detected a failure value	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。	Error (错误)	无操作
Dell - Processor sensor detected a non-recoverable value	指定系统中的处理器传感器发生故障。	Error (错误)	无操作
Dell - Device configuration error	在指定系统中的可插拔设备上检测到配置错误。	Error (错误)	无操作
Dell - Battery sensor returned to a normal value	传感器已恢复正常值	信息	无操作
Dell - Battery sensor detected a warning value	指定系统中的电池传感器检测到电池处于潜在故障状态。	警告	无操作
Dell - Battery sensor detected a failure value	指定系统中的电池传感器检测到电池发生故障。	Error (错误)	无操作
Dell - Battery sensor detected a nonrecoverable value	指定系统中的电池传感器检测到电池发生故障。	Error (错误)	无操作
Dell - Thermal shutdown protection has been initiated	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。	Error (错误)	无操作
Dell - Temperature sensor returned to a normal value	传感器已恢复正常值。	信息	无操作

事件名称	说明	严重性	建议操作
Dell - Temperature sensor detected a warning value	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 - Temperature sensor detected a failure value	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。	Error (错误)	使系统进入维护模式
Dell - Temperature sensor detected a non-recoverable value	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。	Error (错误)	无操作
Dell - Fan sensor returned to a normal value	传感器已恢复正常值	信息	无操作
Dell - Fan sensor detected a warning value	主机 <x> 上的风扇传感器读数超过警告阈值。	警告	无操作
Dell - Fan sensor detected a failure value	指定系统中的风扇传感器检测到一个或多个风扇故障。	Error (错误)	使系统进入维护模式
Dell - Fan sensor detected a nonrecoverable value	风扇传感器检测到无法恢复的错误。	Error (错误)	无操作
Dell - Voltage sensor returned to a normal value	传感器已恢复正常值	信息	无操作
Dell - Voltage sensor detected a warning value	指定系统中的电压传感器超过警告阈值	警告	无操作
Dell - Voltage sensor detected a failure value	指定系统中的电压传感器超过故障阈值。	Error (错误)	使系统进入维护模式
Dell - Voltage sensor detected a nonrecoverable value	指定系统中的电压传感器检测到无法恢复的错误。	Error (错误)	无操作
Dell - Current sensor returned to a normal value	传感器已恢复正常值。	信息	无操作
Dell - Storage: storage management error	存储管理检测到设备独立错误情况。	Error (错误)	使系统进入维护模式
Dell - Storage: Controller warning	控制器警告。请参阅 vSphere 客户端上的“任务和事件”选项卡了解详细信息。	警告	无操作
Dell - Storage: Controller failure	控制器故障。请参阅 vSphere 客户端上的“任务和事件”选项卡了解详细信息。	Error (错误)	使系统进入维护模式
Dell - Storage: Channel Failure	信道故障。	Error (错误)	使系统进入维护模式
Dell - Storage: Enclosure hardware information	机柜硬件信息。	信息	无操作
Dell - Storage: Enclosure hardware warning	机柜硬件警告。	警告	无操作
Dell - Storage: Enclosure hardware failure	机柜硬件错误。	Error (错误)	使系统进入维护模式

事件名称	说明	严重性	建议操作
Dell - Storage: Array disk failure	阵列磁盘故障。	Error (错误)	使系统进入维护模式
Dell - Storage: EMM failure	EMM 故障。	Error (错误)	使系统进入维护模式
Dell - Storage: power supply failure	电源设备故障。	Error (错误)	使系统进入维护模式
Dell - Storage: temperature probe warning	物理磁盘温度探测器警告, 太冷或太热	警告	无操作
Dell - Storage: temperature probe failure	物理磁盘温度探测器错误, 太冷或太热。	Error (错误)	使系统进入维护模式
Dell - Storage: Fan failure	风扇故障。	Error (错误)	使系统进入维护模式
Dell - Storage: Battery warning	电池警告。	警告	无操作
Dell - Storage: Virtual disk degraded warning	虚拟磁盘降级警告。	警告	无操作
Dell - Storage: Virtual disk degraded failure	虚拟磁盘降级故障	Error (错误)	使系统进入维护模式
Dell - Storage: Temperature probe information	温度探测器信息	信息	无操作
Dell - Storage: Array disk warning	阵列磁盘警告。	警告	无操作
Dell - Storage: Array disk information	阵列磁盘信息。	信息	无操作
Dell - Storage: Power supply warning	电源设备警告。	警告	无操作
Dell - 机箱侵入 - 物理安全性违规	机箱侵入 - 物理安全性违规	Error (错误)	无操作
Dell - 机箱侵入 (物理安全性违规) 事件已清除	机箱侵入 (物理安全性违规) 事件已清除	信息	无操作
Dell - CPU 存在 (检测到存在处理器)	CPU 存在 (检测到存在处理器)	信息	无操作
Dell - 系统事件日志 (SEL) 已满 (事件记录已禁用)	系统事件日志 (SEL) 已满 (事件记录已禁用)	Error (错误)	无操作
Dell - 系统事件日志 (SEL) 已清除	系统事件日志 (SEL) 已清除	信息	无操作
Dell - SD 卡冗余已恢复正常	SD 卡冗余已恢复正常	信息	无操作
Dell - SD 卡冗余已丢失	SD 卡冗余已丢失	Error (错误)	无操作
Dell - SD 卡冗余已降级	SD 卡冗余已降级	警告	无操作
Dell - 模块 SD 卡存在 (检测到存在 SD 卡)	模块 SD 卡存在 (检测到存在 SD 卡)	信息	无操作
Dell - 模块 SD 卡失败 (错误)	模块 SD 卡失败 (错误)	Error (错误)	无操作



事件名称	说明	严重性	建议操作
Dell - 模块 SD 卡写保护 (警告)	模块 SD 卡写保护 (警告)	警告	无操作
Dell - 模块 SD 卡不存在	模块 SD 卡不存在	信息	无操作
Dell - 监督计时器过期	监督计时器过期	Error (错误)	无操作
Dell - 已重设监督	已重设监督	Error (错误)	无操作
Dell - 关闭监督	关闭监督	Error (错误)	无操作
Dell - 关闭监督后再打开	关闭监督后再打开	Error (错误)	无操作
Dell - 系统电源超出 PSU 功率	系统电源超出 PSU 功率	Error (错误)	无操作
Dell - 已清除系统功率超出错误	已清除系统功率超出错误	信息	无操作
Dell - 已插入电源	已插入电源	信息	无操作
Dell - 内部双 SD 模块存在	内部双 SD 模块存在	信息	无操作
Dell - 内部双 SD 模块联机	内部双 SD 模块联机	信息	无操作
Dell - 内部双 SD 模块正常运行	内部双 SD 模块正常运行	信息	无操作
Dell - 内部双 SD 模块为写保护	内部双 SD 模块为写保护	警告	无操作
Dell - 内部双 SD 模块可写	内部双 SD 模块可写	信息	无操作
Dell - 集成的双 SD 模块不存在	集成的双 SD 模块不存在	Error (错误)	无操作
Dell - 集成的双 SD 模块冗余丢失	集成的双 SD 模块冗余丢失	Error (错误)	无操作
Dell - 内部双 SD 模块冗余	内部双 SD 模块冗余	信息	无操作
Dell - 内部双 SD 模块非冗余	内部双 SD 模块非冗余	信息	无操作
Dell - 集成的双 SD 模块故障	集成的双 SD 模块故障	Error (错误)	无操作
Dell - 内部双 SD 模块脱机	内部双 SD 模块脱机	警告	无操作
Dell - 集成的双 SD 模块冗余降级	集成的双 SD 模块冗余降级	警告	无操作
Dell - SD 卡设备已检测到警告	SD 卡设备已检测到警告	警告	无操作
Dell - SD 卡设备已检测到故障	SD 卡设备已检测到故障	Error (错误)	无操作
Dell - 集成的双 SD 模块警告	集成的双 SD 模块警告	警告	无操作
Dell - 集成的双 SD 模块信息	集成的双 SD 模块信息	信息	无操作
Dell - 集成的双 SD 模块冗余信息	集成的双 SD 模块冗余信息	信息	无操作
Dell - 网络故障或要严重事件	网络故障或要严重事件	Error (错误)	无操作
Dell - 网络警告	网络警告	警告	无操作

事件名称	说明	严重性	建议操作
Dell - 网络信息	网络信息	信息	无操作
Dell - 物理磁盘故障	物理磁盘故障	Error (错误)	无操作
Dell - 物理磁盘警告	物理磁盘警告	警告	无操作
Dell - 物理磁盘信息	物理磁盘信息	信息	无操作
Dell - 检测到 PCI 设备出现错误	检测到 PCI 设备出现错误	Error (错误)	无操作
Dell - 检测到 PCI 设备的警告事件	检测到 PCI 设备的警告事件	警告	无操作
Dell - 检测到 PCI 设备的信息事件	检测到 PCI 设备的信息事件	信息	无操作
Dell - Virtual Disk Partition failure.	虚拟磁盘分区失败。	Error (错误)	无操作
Dell - Virtual Disk Partition warning.	虚拟磁盘分区警告。	警告	无操作
Dell - Cable failure or critical event	电缆故障或严重事件	Error (错误)	无操作
Dell - Chassis Management Controller detected an error.	Chassis Management Controller 检测到错误。	Error (错误)	无操作
Dell - IO Virtualization failure or critical event.	IO 虚拟化失败或严重事件。	Error (错误)	无操作
Dell - Link status failure or critical event.	链接状态故障或严重事件。	Error (错误)	无操作
Dell - System: Software configuration failure.	系统：软件配置失败。	Error (错误)	无操作
Dell - Storage Security failure or critical event.	存储安全性故障或严重事件。	Error (错误)	无操作
Dell - Chassis Management Controller audit failure or critical event.	Chassis Management Controller 审核故障或严重事件。	Error (错误)	无操作
Dell - Power Supply audit failure or critical event.	电源设备审核故障或严重事件。	Error (错误)	无操作
Dell - Power usage audit failure or critical event.	电源使用情况审核故障或严重事件。	Error (错误)	无操作
Dell - Configuration: Software configuration failure.	配置：软件配置失败。	Error (错误)	无操作
Dell - Chassis Management Controller detected a warning.	Chassis Management Controller 检测到警告。	警告	无操作
Dell - Link status warning.	链接状态警告。	警告	无操作
Dell - Security warning.	安全警告。	警告	无操作


事件名称	说明	严重性	建议操作
Dell - System: Software configuration warning.	系统：软件配置警告。	警告	无操作
Dell - Storage Security warning.	存储安全警告。	警告	无操作
Dell - Software change update warning	软件更改更新警告	警告	无操作
Dell - Chassis Management Controller audit warning.	Chassis Management Controller 审核警告。	警告	无操作
Dell - PCI device audit warning.	PCI 设备审核警告。	警告	使系统进入维护模式
Dell - Power Supply audit warning.	电源设备审核警告。	警告	无操作
Dell - Power usage audit warning.	电源使用情况审核警告。	警告	无操作
Dell - Security configuration warning.	安全配置警告。	警告	无操作
Dell - Configuration: Software configuration warning.	配置：软件配置警告。	警告	无操作

了解自动查找

自动查找是指将 Dell PowerEdge 第 11 代、第 12 代或第 13 代裸机服务器添加到可用服务器池中以供 OpenManage Integration for VMware vCenter 使用的过程。查找到服务器后，即可将其用于虚拟机管理程序和硬件部署。此附录提供了有关自动查找的充足信息，以帮助您进行系统配置。自动查找是一项 Lifecycle Controller 功能，用于设置新服务器并使用控制台注册该服务器。使用此功能的优势包括不需要对新服务器执行烦琐的手动本地配置，以及为控制台查找已连接到网络并且插入电源的新服务器提供了一种自动化方法。

在执行相关流程后，自动查找有时也称为 *查找和握手*。当将启用了自动查找功能的新服务器插入交流电源并连接到网络时，Dell 服务器的 Lifecycle Controller 会尝试 *查找* 一个与 Dell 预配置服务器集成的部署控制台。然后，自动查找会在配置服务器与 Lifecycle Controller 之间启动 *握手*。

OpenManage Integration for VMware vCenter 是具有集成配置服务器的部署控制台。将使用不同的方法将配置服务器的位置提供给 iDRAC。配置服务器位置的 IP 地址或主机名称设置为 OpenManage Integration for VMware vCenter 设备虚拟机的 IP 地址或主机名称。

 **注：在 24 小时的期间内，配置用于自动查找的新服务器将每隔 90 秒尝试解析一次配置服务器的位置，之后，您可以手动重新启动自动查找。**


当 OpenManage Integration for VMware vCenter 收到自动查找请求时，它会验证 SSL 证书，然后启动任何可选配置的安全过程，如客户端安全证书和基于白名单的验证。新服务器提出的第二个验证请求将返回要在 iDRAC 上配置的临时用户名/密码凭据。随后的调用由 OpenManage Integration for VMware vCenter 启动，它收集有关服务器的信息，移除临时凭据，并配置用于管理访问的更多永久性用户定义的凭据。

如果自动查找成功，将在目标 iDRAC 上创建在查找时在 **设置** → **部署** 页面中提供的部署凭据。然后关闭自动查找功能。现在，服务器应该会在 OpenManage Integration for VMware vCenter 中“部署”下的可用裸机服务器池中显示。

目前可通过 vSphere Desktop 客户端执行自动查找。

自动查找前提条件

在尝试查找第 11 代、第 12 代或更高版本 Dell PowerEdge 裸机服务器之前，安装 OpenManage Integration for VMware vCenter。只有包含 iDRAC Express 或 iDRAC Enterprise 的第 11 代 Dell PowerEdge 或更高版本服务器可被找到并加入 OpenManage Integration for VMware vCenter 裸机服务器池中。在 Dell 裸机服务器的 iDRAC 与 OpenManage Integration for VMware vCenter 虚拟机之间需要存在网络连接。

 **注：现已包含虚拟机管理程序的主机不应被查找并添加到 OpenManage Integration for VMware vCenter 中，而是将虚拟机管理程序添加到连接配置文件中，然后使用主机符合性向导与 OpenManage Integration for VMware vCenter 进行协调。**

为了进行自动查找，必须满足以下条件：


- **电源：**将服务器连接到电源插座。不需要打开服务器。
- **网络连接：**服务器的 iDRAC 必须具有网络连接并且必须通过端口 4433 与配置服务器进行通信。您可以使用 DHCP 服务器获取 IP 地址，或在 iDRAC 配置公用程序中手动指定 IP 地址。
- **附加网络设置：**如果使用 DHCP，请启用从 *DHCP 获取 DNS 服务器地址* 设置，以便解析 DNS 名称。
- **配置服务器位置：**iDRAC 必须知道配置服务服务器的 IP 地址或主机名称。
- **已禁用帐户访问：**请启用对 iDRAC 的管理帐户访问。如果存在任何具有管理员权限的 iDRAC 帐户，请首先在 iDRAC Web 控制台中禁用这些帐户。自动查找成功完成后，将重新启用管理 iDRAC 帐户。



- **已启用自动查找：**服务器的 iDRAC 必须已启用自动查找，以便开始自动查找流程。

启用或禁用 iDRAC 服务器上的管理帐户

在设置自动查找之前，必须禁用除 root 帐户以外的所有管理帐户。在自动查找过程中，root 帐户处于禁用状态。在您成功设置自动查找后，返回到 Integrated Dell Remote Access Controller 6 GUI，然后重新启用已关闭的帐户。此程序适用于 Dell PowerEdge 第 11 代、12 代和 13 代服务器。

 **注：**若要防止自动查找失败，您可能希望启用 iDRAC 上的非管理帐户。这样，在自动查找失败时，仍然允许远程访问。


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

手动配置服务器以进行自动查找（第 11 代 PowerEdge 服务器）

您必须具有 iDRAC 和主机 IP 地址。

如果您尚未从工厂订购裸机设备以使用自动查找，您可以手动进行设置。iDRAC 具有两个用户界面，这两个界面均可以使用您要设置的 iDRAC 的 IP 地址进行访问。

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

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

在目标计算机上手动执行下列步骤以启用自动查找功能：

1. 引导/重新引导目标系统。
2. 当您看到在 **5 秒钟内按 <CTRL-E> 以远程访问设置...** 消息时，按 **CTRL + E** 以查看以下屏幕。

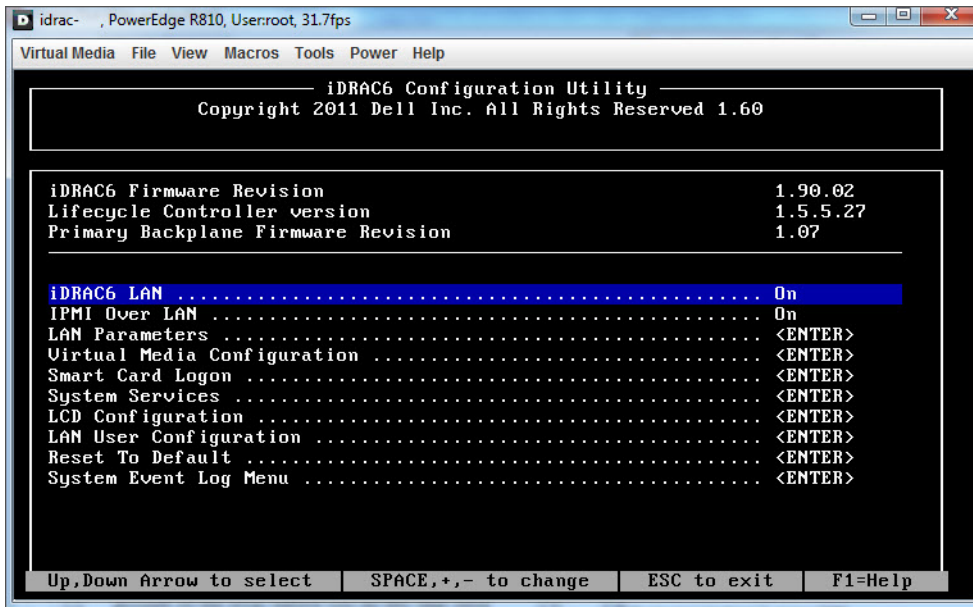


图 6: 按 CTRL+E 以激活此屏幕。

3. 在 iDRAC6 配置公用程序中，使用箭头键选择 **LAN 用户配置**。
4. 使用箭头键选择 **自动查找**。
5. 使用空格键将该选项切换到已启用。
6. 使用箭头键选择 **配置服务器**，然后按 **Enter** 键。
7. 输入 OMIVV 设备的 IP 地址。
8. 按 **ESC** 键。
9. 使用箭头键选择 **帐户访问**。
10. 使用空格键将该选项切换为禁用。
11. 从键盘中，按 **ESC** 键。
12. 再次按 **Esc** 键接收保存更改的通知并退出设置。
13. 选择 **保存更改并退出**，然后按 **Enter** 键。

在下次主机重新引导循环中自动查找到 iDRAC。

手动配置 PowerEdge 第 12 代及更高版本服务器以进行自动查找

您必须具有 iDRAC 和主机 IP 地址。

从 Dell 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 地址是 OMIVV 的 IP 地址。在此情况下，在收到 Dell 所提供的服务器后，当您安装并连接 iDRAC 电缆后，开启服务器电源时，服务器被自动查找。这些服务器将列在“部署”向导的第一个页面中。

注: 对于自动查找到的服务器，使用在 Dell Management Center → 设置 → 部署凭据下提供的凭据与服务器进行进一步通信，直到操作系统部署完成。在操作系统成功部署后，设置在关联的连接配置文件中提供的 iDRAC 凭据。

注: 确保服务器白名单已禁用，或者已将要自动查找的服务器的服务标签添加至 Dell Management Center → 设置 → 安全性下的服务器白名单中。

在目标计算机上手动执行下列步骤以启用自动查找功能：

1. 引导/重新引导目标系统，并在初始引导期间按 **F2** 键以进入“系统设置”
2. 转至 **iDRAC 设置** → **用户配置**并禁用 root 用户。请确保在禁用 root 用户时没有任何其他用户。在该 iDRAC 上，不应存在拥有有效管理员权限的任何用户。
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。
6. 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，root 用户将启用，并且**启用 Auto-Discovery** 标志会自动禁用。