

Dell EMC OpenManage Enterprise 版本 3.6.1 用户指南

注意、小心和警告

 **注:** “注意” 表示帮助您更好地使用该产品的重要信息。

 **小心:** “小心” 表示可能会损坏硬件或导致数据丢失，并告诉您如何避免此类问题。

 **警告:** “警告” 表示可能会导致财产损失、人身伤害甚至死亡。

表.....	9
章 1: 关于 Dell EMC OpenManage Enterprise.....	10
此发行版中的新功能.....	11
您可能需要的其他信息.....	11
联系 Dell EMC.....	11
OpenManage Enterprise 高级许可证.....	12
OpenManage Enterprise 中基于许可证的功能.....	12
章 2: OpenManage Enterprise 中的安全功能.....	13
OpenManage Enterprise 用户角色类型.....	13
OpenManage Enterprise 中基于角色和范围的访问控制.....	14
章 3: 安装 OpenManage Enterprise.....	17
安装的前提条件和最低要求.....	17
最低建议硬件.....	17
部署 OpenManage Enterprise 的最低系统要求.....	18
在 VMware vSphere 上部署 OpenManage Enterprise.....	18
在 Hyper-V 2012 R2 及更早版本的主机上部署 OpenManage Enterprise.....	18
在 Hyper-V 2016 主机上部署 OpenManage Enterprise.....	19
在 Hyper-V 2019 主机上部署 OpenManage Enterprise.....	20
通过使用基于内核的虚拟机部署 OpenManage Enterprise.....	20
以编程方式部署 OpenManage Enterprise.....	21
章 4: OpenManage Enterprise 使用入门.....	23
登录到 OpenManage Enterprise.....	23
使用文本用户界面配置 OpenManage Enterprise.....	23
配置 OpenManage Enterprise.....	25
获得最佳 OpenManage Enterprise 使用的建议的可扩展性和性能设置.....	26
OpenManage Enterprise 中支持的协议和端口.....	26
在 OpenManage Enterprise 中支持的协议和端口的使用案例链接.....	28
章 5: OpenManage Enterprise 图形用户界面概述.....	29
章 6: OpenManage Enterprise 门户主页.....	31
使用 OpenManage Enterprise 仪表盘监测设备.....	31
环形图.....	32
设备运行状况状态.....	33
章 7: 查找要监测或管理的设备.....	34
通过使用服务器启动的查找功能来自动查找服务器.....	35
.....	36
创建设备查找作业.....	36
启用设备.....	37

用于查找设备的协议支持值表.....	38
查看设备查找作业详细信息.....	39
编辑设备查找作业.....	39
运行设备查找作业.....	39
停止设备查找作业.....	40
通过从 .csv 文件导入数据来指定多个设备.....	40
全局排除范围.....	40
为创建服务器查找作业指定查找模式.....	41
创建服务器的自定义设备查找作业协议 - 查找协议的附加设置.....	41
为创建机箱查找作业指定查找模式.....	42
创建机箱的自定义设备查找作业协议 - 查找协议的附加设置.....	42
为创建戴尔存储设备查找作业指定查找模式.....	43
为创建网络交换机查找作业指定查找模式.....	43
创建 HTTPS 存储设备的自定义设备查找作业协议 - 查找协议的附加设置.....	44
为 SNMP 设备创建自定义设备查找作业模板.....	44
为创建 MULTIPLE 协议查找作业指定查找模式.....	44
删除设备查找作业.....	44

章 8: 管理设备和设备组.....46

将设备按组整理.....	46
创建自定义组（静态或查询）.....	47
创建静态设备组.....	48
创建查询设备组.....	48
编辑静态组.....	49
编辑查询组.....	49
重命名静态或查询组.....	50
删除静态或查询设备组.....	50
克隆静态或查询组.....	50
将设备添加到新组.....	50
将设备添加到现有组.....	51
在组上刷新运行状况.....	51
“所有设备” 页面 — 设备列表.....	51
“所有设备” 页面 — 设备列表操作.....	52
从 OpenManage Enterprise 删除设备.....	53
从 OpenManage Enterprise 中排除设备.....	53
在设备上运行资源清册.....	53
通过使用基线更新设备固件和驱动程序.....	54
刷新设备组的设备运行状况.....	54
在设备上刷新运行状况.....	55
回滚单个设备的固件版本.....	55
导出单个设备资源清册.....	55
在机箱和服务器的上执行更多操作.....	56
显示的 MX7000 机箱硬件信息.....	56
导出所有或所选数据.....	56
查看和配置各个设备.....	56
设备概述.....	57
设备硬件信息.....	57
运行并下载诊断报告.....	58
提取和下载 SupportAssist 报告.....	58
管理单个设备硬件日志.....	59

在各个设备上运行远程 RACADM 和 IPMI 命令.....	59
启动设备的管理应用程序 iDRAC.....	59
启动虚拟控制台.....	59
刷新单个设备的设备资源清册.....	60
章 9: 管理设备资源清册.....	61
创建资源清册作业.....	61
立即运行资源清册作业.....	62
停止资源清册作业.....	62
删除资源清册作业.....	62
编辑资源清册计划作业.....	63
章 10: 管理设备固件和驱动程序.....	64
管理固件和驱动程序目录.....	65
通过使用 Dell.com 添加目录.....	65
向本地网络添加目录.....	65
SSL 证书信息.....	66
更新目录.....	66
编辑目录.....	67
删除目录.....	67
创建固件/驱动程序基线.....	67
删除配置合规性基线.....	68
编辑基线.....	68
检查设备固件和驱动程序的合规性.....	68
查看基线合规性报告.....	69
使用基线合规性报告更新固件和/或驱动程序.....	70
章 11: 管理设备部署模板.....	72
要从参考设备创建部署模板.....	72
导入模板文件创建部署模板.....	73
查看部署模板信息.....	73
编辑服务器部署模板.....	73
编辑机箱部署模板.....	74
编辑 IOA 部署模板.....	75
编辑部署模板的网络属性.....	75
部署设备部署模板.....	75
部署 IOA 部署模板.....	76
克隆部署模板.....	77
在尚待发现的服务器或机箱上自动部署配置.....	77
创建自动部署目标.....	78
删除自动部署目标.....	78
将自动部署目标详细信息导出为不同的格式.....	79
无状态部署概览.....	79
管理标识池 - 无状态部署.....	79
创建标识池 — 池信息.....	79
定义网络.....	84
网络类型.....	84
编辑或删除配置的网络.....	84
导出 VLAN 定义.....	85

导入网络定义.....	85
章 12: 管理配置文件.....	86
创建配置文件.....	87
查看配置文件详细信息.....	87
配置文件—查看网络.....	87
编辑配置文件.....	88
分配配置文件.....	88
取消分配配置文件.....	89
重新部署配置文件.....	89
迁移配置文件.....	89
删除配置文件.....	90
以 HTML、CSV 或 PDF 格式导出配置文件数据.....	90
章 13: 管理设备配置合规性.....	91
管理合规性模板.....	91
从部署模板创建合规性模板.....	92
从参考设备创建合规性模板.....	92
通过从文件中导入以创建合规性模板.....	93
克隆合规性模板.....	93
编辑合规性模板.....	93
创建配置合规性基线.....	93
编辑配置合规性基线.....	94
删除配置合规性基线.....	95
刷新配置合规性基线的合规性.....	95
修正非合规设备.....	95
导出合规性基线报告.....	96
移除配置合规性基线.....	96
章 14: 监视和管理设备警报.....	97
查看警报日志.....	97
管理警报日志.....	98
警报策略.....	99
配置和管理警报策略.....	99
在插入和卸下底座上自动刷新 MX7000 机箱.....	103
警报定义.....	103
章 15: 监视审核日志.....	104
将审计日志转发到远程系统日志服务器.....	105
章 16: 使用作业进行设备控制.....	106
查看作业列表.....	106
作业状态和作业类型描述.....	107
OpenManage Enterprise 默认作业和计划.....	108
查看单个作业信息.....	109
创建作业以打开设备 LED.....	110
为管理电源设备创建作业.....	110
为管理设备创建远程命令作业.....	110
创建作业以更改虚拟控制台插件类型.....	111

选择目标设备和设备组.....	111
管理作业.....	111
章 17: 管理设备保修.....	113
查看和续订设备保修.....	113
章 18: 报告.....	115
运行报告.....	116
运行报告和通过电子邮件发送报告.....	116
编辑报告.....	117
复制报告.....	117
删除报告.....	117
创建报告.....	117
在创建报告时选择查询条件.....	118
导出所选报告.....	119
章 19: 管理 MIB 文件.....	120
导入 MIB 文件.....	120
编辑 MIB 陷阱.....	121
删除 MIB 文件.....	121
解析 MIB 类型.....	122
下载 OpenManage Enterprise MIB 文件.....	122
章 20: 管理 OpenManage Enterprise 设备设置.....	123
配置 OpenManage Enterprise 网络设置.....	123
管理 OpenManage Enterprise 用户.....	124
OpenManage Enterprise 中基于角色和范围的访问控制.....	125
添加和编辑 OpenManage Enterprise 用户.....	127
编辑 OpenManage Enterprise 用户属性.....	128
启用 OpenManage Enterprise 用户.....	128
禁用 OpenManage Enterprise 用户.....	128
删除 OpenManage Enterprise 用户.....	128
导入 AD 和 LDAP 组.....	129
设备管理者实体的所有权转移.....	129
终止用户会话.....	130
OpenManage Enterprise 中的目录服务集成.....	130
添加或编辑要用于目录服务的 Active Directory 组.....	131
添加或编辑要用于目录服务的轻量级目录访问协议组.....	131
删除目录服务.....	132
使用 OpenID Connect 提供程序登录 OpenManage Enterprise.....	133
将 OpenID Connect 提供程序添加到 OpenManage Enterprise.....	134
在 PingFederate 中配置 OpenID Connect 提供程序策略, 以提供基于角色的 OpenManage Enterprise 访问权限.....	134
在 Keycloak 中配置 OpenID Connect 提供程序策略, 以提供基于角色的 OpenManage Enterprise 访问权限.....	135
测试 OpenManage Enterprise 向 OpenID Connect 提供程序的注册状态.....	135
在 OpenManage Enterprise 中编辑 OpenID Connect 提供程序的详细信息.....	135
启用 OpenID Connect 提供程序.....	136
删除 OpenID Connect 提供程序.....	136

禁用 OpenID Connect 提供程序.....	136
安全证书.....	136
生成并下载的数字签名请求.....	136
使用 Microsoft Certificate Services 将 Web 服务器证书分配给 OpenManage Enterprise.....	136
设置登录安全性属性.....	137
管理控制台首选项.....	137
自定义警报显示.....	138
配置 SMTP、SNMP 和 Syslog 警报.....	139
管理传入警报.....	140
设置 SNMP 凭据.....	140
管理保修设置.....	140
检查并更新 OpenManage Enterprise 及可用插件的版本.....	141
OpenManage Enterprise 中的更新设置.....	141
更新 OpenManage Enterprise.....	141
从 Dell.com 更新.....	142
从内部网络共享更新.....	143
安装插件.....	144
禁用插件.....	144
卸载插件.....	144
启用插件.....	145
更新插件程序.....	145
执行远程命令和脚本.....	145
OpenManage Mobile 设置.....	146
启用或禁用 OpenManage Mobile 的警报通知.....	146
启用或禁用 OpenManage Mobile 订户.....	147
删除 OpenManage Mobile 订户.....	147
查看警报通知服务状态.....	147
通知服务状态.....	148
查看有关 OpenManage Mobile 订户的信息.....	148
OpenManage Mobile 订户信息.....	148
OpenManage Mobile 故障排除.....	149
章 21: 其他参考和字段说明.....	150
计划参考.....	150
固件基线字段定义.....	150
计划作业字段定义.....	150
EEMI 位置调整后的警报类别.....	151
远程脚本和警报策略中的标记替换.....	152
现场服务调试工作流程.....	152
取消阻止 FSD 功能.....	152
安装或授予已签署 FSD DAT.ini 文件.....	153
调用 FSD.....	153
禁用 FSD.....	153
目录管理字段定义.....	154
固件/驱动程序合规性基线报告 - 具有“未知”合规状态的设备.....	154
Dell EMC PowerEdge 服务器的通用命名惯例.....	154

1	您可能需要的其他信息.....	11
2	OpenManage Enterprise 用户角色类型.....	13
3	OpenManage Enterprise 中的基于角色的用户权限.....	14
4	最低建议硬件.....	17
5	最低要求.....	18
6	ovf_properties.config 中使用的参数.....	21
7	文本用户界面选项.....	23
8	OpenManage Enterprise 的可扩展性和性能注意事项.....	26
9	管理站上 OpenManage Enterprise 支持的协议和端口.....	26
10	受管节点上 OpenManage Enterprise 支持的协议和端口.....	28
11	在 OpenManage Enterprise 中支持的协议和端口的使用案例链接.....	28
12	OpenManage Enterprise 中的设备运行状况.....	33
13	用于查找的协议支持值表.....	38
14	支持的跨模板部署.....	77
15	网络类型.....	84
16	CSV 文件的 VLAN 定义格式.....	85
17	JSON 文件的 VLAN 定义格式.....	85
18	管理配置文件 - 字段定义.....	86
19	配置文件状态和可能的操作.....	86
20	警报清除.....	99
21	作业状态和说明.....	107
22	作业类型和说明.....	107
23	下表列出了 OpenManage Enterprise 默认作业名称及其计划。.....	108
24	用于管理 OpenManage Enterprise 上报告的基于角色的访问权限.....	115
25	用于生成 OpenManage Enterprise 报告的基于角色的访问权限.....	118
26	OpenManage Enterprise 中基于角色访问 MIB 文件.....	120
27	OpenManage Enterprise 中的基于角色的用户权限.....	125
28	LDAP 集成的 OpenManage Enterprise 前提条件/支持的属性.....	130
29	通知服务状态.....	148
30	OpenManage Mobile 订户信息.....	148
31	OpenManage Mobile 故障排除.....	149
32	OpenManage Enterprise 中的警报类别.....	151
33	OpenManage Enterprise 中支持的标记.....	152
34	固件/驱动程序合规性基线报告 — “错误” 合规设备.....	154
35	PowerEdge 服务器命名惯例和示例.....	155

关于 Dell EMC OpenManage Enterprise

OpenManage Enterprise 是作为虚拟设备提供的系统管理和监控 Web 应用程序。可以通过它全面了解企业网络中的 Dell EMC 服务器、机箱、存储设备和网络交换机。借助 OpenManage Enterprise，一个基于 Web 的可以集中管理多套系统的管理应用程序，用户可以：

- 查找数据中心环境中的设备。
- 查看硬件资源清册并监测设备运行状况。
- 查看和管理一体机收到的警报并配置警报策略。
- 监测固件/驱动程序版本，并对具有固件基线的设备上的固件/驱动程序更新进行管理。
- 管理设备上的远程任务（如电源控制）。
- 使用部署模板管理设备间的配置设置。
- 使用智能标识池管理设备间的虚拟标识设置。
- 使用配置基线检测和修正设备间的配置偏差。
- 检索和监测设备的保修信息。
- 将设备分组为静态或动态组。
- 创建和管理 OpenManage Enterprise 用户。

注:

- OpenManage Enterprise 的系统管理和监视最适合 Enterprise LAN，不建议在 WAN 上使用。
- 有关支持的浏览器的信息，请参阅支持站点上提供的 *OpenManage Enterprise 支持值表*。

OpenManage Enterprise 的一些安全功能包括：

- 基于角色的访问权限，用于限制对控制台设置和设备操作的访问。
- 基于范围的访问控制允许管理员限制设备管理者可以访问和管理的设备组。
- 通过 Security-Enhanced Linux (SELinux) 和内部防火墙加强的设备。
- 内部数据库中的敏感数据加密。
- 在设备之外使用加密通信 (HTTPS)。
- 创建和强制实施固件和配置相关的策略。
- 配置以配置和更新裸机服务器。

OpenManage Enterprise 具有基于域任务的 GUI，其设计导航时充分考虑主要由管理员和设备管理者使用的任务的顺序。将设备添加到环境中时，OpenManage Enterprise 会自动检测设备属性，将它置于相关的设备组中，并支持您管理设备：由 OpenManage Enterprise 用户执行的任务的典型顺序：

- [安装 OpenManage Enterprise](#) 页面上的 17
- [使用文本用户界面配置 OpenManage Enterprise](#) 页面上的 23
- [查找要监测或管理的设备](#) 页面上的 34
- [管理设备和设备组](#) 页面上的 46
- [使用 OpenManage Enterprise 仪表盘监测设备](#) 页面上的 31
- [将设备按组整理](#) 页面上的 46
- [管理设备固件和驱动程序](#) 页面上的 64
- [查看和配置各个设备](#) 页面上的 56
- [监视和管理设备警报](#) 页面上的 97
- [查看和续订设备保修](#) 页面上的 113
- [管理设备部署模板](#) 页面上的 72
- [管理设备配置合规性](#) 页面上的 91
- [管理合规性模板](#) 页面上的 91
- [监视审核日志](#) 页面上的 104
- [管理 OpenManage Enterprise 设备设置](#) 页面上的 123
- [立即运行资源清册作业](#) 页面上的 62
- [管理设备保修](#) 页面上的 113
- [报告](#) 页面上的 115
- [管理 MIB 文件](#) 页面上的 120
- [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14

- [OpenManage Enterprise 中的目录服务集成](#) 页面上的 130

主题:

- [此发行版中的新功能](#)
- [您可能需要的其他信息](#)
- [联系 Dell EMC](#)
- [OpenManage Enterprise 高级许可证](#)

此发行版中的新功能

- 基于范围的访问控制 (SBAC) 现在允许更高效、更安全地管理查找到的设备。管理员现在可以确定设备管理者预期将管理的设备组。
- 多机箱管理 (MCM) 机箱上的无缝固件更新，支持多达 20 个机箱及其底座。
- 可以在文本用户界面 (TUI) 页面上扫描和扩展设备磁盘大小。
- 支持的产品范围扩展至采用以下第 3 代 Intel® Xeon® 的 YX5X (15G) PowerEdge 服务器: R650、R750、R750xa、MX750c、C6520。

增强功能

- Redfish 协议支持在具有 iDRAC9 4.40.10.10 及更高版本的设备上查找、清点资源、监测和进行有限管理 (电源控制、闪烁、诊断和技术支持报告)。
- 在主页上添加了新的“资源利用率”小部件，用于以图形方式显示设备的 CPU 和内存利用率。
- “所有设备”页面上的附加环形图，用于显示所安装插件的数据。
- 添加到 SMTP 配置的测试电子邮件功能。
- 针对警报转发添加的 SNMPv3 支持。
- 添加至保修设置的保修筛选，用于自定义保修页面和报告。


您可能需要的其他信息

除了本指南以外，您可以访问以下能提供关于 OpenManage Enterprise 及其它相关产品的更多信息的说明文件。

表. 1: 您可能需要的其他信息

说明文件	说明	可用性
<i>Dell EMC OpenManage Enterprise 支持值表</i>	列出 OpenManage Enterprise 支持的设备。	<ol style="list-style-type: none"> 1. 转至 Dell.com/OpenManageManuals。 2. 单击 Dell OpenManage Enterprise，并选择所需的 OpenManage Enterprise 版本。 3. 单击文档以访问这些文档。
<i>Dell EMC OpenManage Enterprise 发行说明</i>	提供有关 OpenManage Enterprise 中的已知问题和解决方法的信息。	
<i>Dell EMC OpenManage Mobile 用户指南</i>	提供有关安装和使用 OpenManage Mobile 应用程序的信息。	
<i>Dell EMC Repository Manager 用户指南</i>	提供有关使用 Repository Manager 管理系统更新的信息。	
<i>Dell EMC OpenManage Enterprise and OpenManage Enterprise – Modular 版本 RESTful API 指南</i>	提供有关使用表述性状态转移 (REST) API 集成 OpenManage Enterprise 的信息，还包括使用 REST API 执行常见任务的示例。	
<i>Dell EMC SupportAssist Enterprise 用户指南</i>	提供有关安装、配置、使用和 SupportAssist Enterprise 故障排除的信息。	Dell.com/ServiceabilityTools

联系 Dell EMC

 **注:** 如果没有可用的互联网连接，可在购货发票、装箱单、帐单或 Dell EMC 产品目录上查找联系信息。

Dell EMC 提供多种在线和基于电话的支持和服务选项。具体的服务随您所在国家/地区以及产品的不同而不同，某些服务在您所在的地区可能不提供。如要联系 Dell EMC 解决有关销售、技术支持或客户服务问题：

1. 访问 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 Enterprise 高级许可证

注：安装和使用 OpenManage Enterprise 不需要 OpenManage Enterprise 高级许可证。仅限服务器配置管理功能 — 部署设备配置并验证服务器上的配置合规性需要在目标服务器上安装 OpenManage Enterprise 高级许可证。在服务器上创建部署模板时不需要此许可证。

OpenManage Enterprise 高级许可证是永久许可证，对服务器终生有效，并且一次只能绑定到一个服务器的服务标签。OpenManage Enterprise 提供一份内置报告以查看设备列表及其许可证。选择 **OpenManage Enterprise > 监测 > 报告 > 许可证报告**，然后单击**运行**。请参阅**运行报告** 页面上的 116。

注：在 OpenManage Enterprise 中启用服务器配置管理功能无需任何单独的许可证。如果在目标服务器上安装了 OpenManage Enterprise 高级许可证，则可以在该服务器上使用服务器配置管理功能。

OpenManage Enterprise 高级许可证 — 支持的服务器

您可以将 OpenManage Enterprise 高级许可证部署到以下 PowerEdge 服务器：

- YX3X 服务器，具有 iDRAC8 2.50.50.50 或更高固件版本。YX3X 固件版本向后兼容，可安装在 YX2X 硬件上。请参阅 [Dell EMC PowerEdge 服务器的通用命名惯例](#) 页面上的 154。
- YX4X 服务器，具有 iDRAC9 3.10.10.10 或更高固件版本。请参阅 [Dell EMC PowerEdge 服务器的通用命名惯例](#) 页面上的 154

购买 OpenManage Enterprise 高级许可证

您可以在购买服务器时或者联系销售代表来购买 OpenManage Enterprise 高级许可证。您可从位于 Dell.com/support/retail/lkm 的软件许可证管理门户下载购买的许可证。

验证许可证信息

OpenManage Enterprise 提供一份内置报告以查看受 OpenManage Enterprise 监测的设备列表及其许可证。单击 **OpenManage Enterprise > 监测 > 报告 > 许可证报告**。单击**运行**。请参阅**运行报告** 页面上的 116。

您可以通过以下方法来验证服务器上是否安装了 OpenManage Enterprise 高级许可证：

- 单击 **i** 符号（显示在 OpenManage Enterprise 所有页面的右上角），然后单击**许可证**。
- 在**许可证**对话框中，浏览消息并单击相应的链接以查看和下载 OpenManage Enterprise 相关的开源文件或其他开源许可证。

OpenManage Enterprise 中基于许可证的功能

需要 OpenManage Enterprise 高级许可证才能使用 OpenManage Enterprise 的以下功能：

- 服务器配置部署。
- 服务器配置合规性基线创建和补救。
- 引导至 ISO。
- 激活可用的插件（例如 Power Manager），以扩展一体机的功能。

注：要访问依赖 iDRAC 的 OpenManage Enterprise 功能（如虚拟控制台支持功能），则需要 iDRAC 企业许可证。有关详细信息，请参阅支持站点上提供的 *iDRAC 说明文件*。

OpenManage Enterprise 中的安全功能

OpenManage Enterprise 的一些安全功能包括：

- 基于角色的访问控制可为不同用户角色（管理员、设备管理者、查看者）提供不同的设备管理功能。
- 基于范围的访问控制允许管理员确定设备管理者预期将管理的设备组。
- 通过 Security-Enhanced Linux (SELinux) 和内部防火墙加强的设备。
- 内部数据库中的敏感数据加密。
- 在设备之外使用加密通信 (HTTPS)。
- 仅支持具有 256 位加密的浏览器。有关更多信息，请参阅，[部署 OpenManage Enterprise 的最低系统要求](#) 页面上的 18

警告： 未经授权的用户通过绕过 Dell EMC 的安全限制，可以获取 OpenManage Enterprise 设备的操作系统级别访问权限。一种可能是将 VMDK 作为辅助驱动器连接在另一个 Linux 虚拟机中，从而获得操作系统分区的访问权限，这样就有可能改变操作系统级别的登录凭据。Dell EMC 建议客户对驱动器（映像文件）进行加密，增加非授权访问的难度。客户还必须确保对于使用的任何加密机制，他们以后能够解密文件。否则设备将无法启动。

注：

- 对用户角色所做的任何更改都会立即生效，受影响的用户将从其活动会话中注销。
- 可以导入 AD 和 LDAP 目录用户并为其分配某个 OpenManage Enterprise 角色（管理员、设备管理者或查看者）。
- 执行设备管理操作需要对设备具有适当权限的帐户。

相关信息

[安装 OpenManage Enterprise](#) 页面上的 17

主题：

- [OpenManage Enterprise 用户角色类型](#)
- [OpenManage Enterprise 中基于角色和范围的访问控制](#)

OpenManage Enterprise 用户角色类型

注：

- 可以导入 AD 和 LDAP 目录用户并为其分配某个 OpenManage Enterprise 角色（管理员、设备管理者或查看者）。
- 在设备上运行操作需要该设备上的特权帐户。

表. 2: OpenManage Enterprise 用户角色类型

具有此角色的用户...	拥有以下用户权限
管理员	拥有所有可在控制台上执行的任务的完全访问权限。 <ul style="list-style-type: none"> • 完全访问（通过使用 GUI 和 REST）读取、查看、创建、编辑、删除、导出和移除与 OpenManage Enterprise 监测的设备和组相关的信息。 • 可以创建本地、Microsoft Active Directory (AD) 和 LDAP 用户并为其分配合适的角色 • 启用和禁用用户 • 修改现有用户的角色 • 删除用户 • 更改用户密码
设备管理者 (DM)	<ul style="list-style-type: none"> • 在管理员分配的设备（范围）上运行任务、策略和其他操作。

表. 2: OpenManage Enterprise 用户角色类型 (续)

具有此角色的用户...	拥有以下用户权限
查看者	<ul style="list-style-type: none"> 只能查看 OpenManage Enterprise 上显示的信息和运行报告。 默认情况下, 对控制台和所有组具有只读权限。 无法运行任务或创建和管理策略。

注:

- 如果将查看者或 DM 更改为管理员, 他们可获得完整的管理员权限。如果将查看者更改为 DM, 则查看者获得 DM 的权限。
- 对用户角色所做的任何更改都会立即生效, 受影响的用户将从其活动会话中注销。
- 在以下情况下将记录审核日志:
 - 分配组或更改访问权限时。
 - 修改用户角色时。

相关任务

安装 OpenManage Enterprise 页面上的 17

相关信息

OpenManage Enterprise 中基于角色和范围的访问控制 页面上的 14

OpenManage Enterprise 中基于角色和范围的访问控制

OpenManage Enterprise 具有基于角色的访问控制 (RBAC), 可明确定义三个内置角色 (管理员、设备管理者和查看者) 的用户权限。此外, 使用基于范围的访问控制 (SBAC), 管理员可以限制设备管理者有权访问的设备组。以下主题将进一步说明 RBAC 和 SBAC 功能。

OpenManage Enterprise 中基于角色的访问控制 (RBAC) 权限

分配给用户的角色决定其访问设备设置和设备管理功能的级别。此功能称之为基于角色的访问控制 (RBAC)。控制台会在允许操作之前强制实施某个操作所需的权限。有关在 OpenManage Enterprise 上管理用户的更多信息, 请参阅管理 OpenManage Enterprise 用户 页面上的 124。

此表列出为每个角色启用的各种权限。

表. 3: OpenManage Enterprise 中的基于角色的用户权限

OpenManage Enterprise 功能	权限描述	访问 OpenManage Enterprise 的用户级别		
		管理员	设备管理者	查看者
设备设置	涉及设置设备的全局设备设置。	是	否	否
安全设置	设备安全设置	是	否	否
警报管理	警报操作/管理	是	否	否
结构管理	结构操作/管理	是	否	否
网络管理	网络操作/管理	是	否	否
组管理	静态组和动态组的创建、读取、更新和删除 (CRUD)	是	否	否
查找管理	查找任务的 CRUD, 运行查找任务	是	否	否
资源清册管理	资源清册任务的 CRUD, 运行资源清册任务	是	否	否
陷阱管理	导入 MIB, 编辑陷阱	是	否	否

表. 3: OpenManage Enterprise 中的基于角色的用户权限 (续)

OpenManage Enterprise 功能	权限描述	访问 OpenManage Enterprise 的用户级别		
		管理员	设备管理者	查看者
自动部署管理	管理自动部署配置操作	是	否	否
监视设置	警报策略、转发、SupportAssist 等	是	是	否
电源控制	重新启动/重启设备电源	是	是	否
设备配置	设备配置、模板应用, 管理/迁移 IO 标识、存储映射 (用于存储设备) 等	是	是	否
操作系统部署	部署操作系统、映射到 LUN 等	是	是	否
设备更新	设备固件更新、应用更新的基线等	是	是	否
模板管理	创建/管理模板	是	是	否
基线管理	创建/管理固件/配置基线策略	是	是	否
电源管理	设置电源预算	是	是	否
作业管理	作业执行/管理	是	是	否
报告管理	报告上的 CRUD 操作	是	是	否
报告运行	运行报告	是	是	是
查看	查看所有数据、报告执行/管理等	是	是	是

OpenManage Enterprise 中基于范围的访问控制 (SBAC)

使用基于角色的访问控制 (RBAC) 功能, 管理员可以在创建用户时分配角色。角色确定其对设备设置和设备管理功能的访问权限级别。基于范围的访问控制 (SBAC) 是 RBAC 功能的扩展, 允许管理员将设备管理者角色限制为称为范围的设备组子集。

在创建或更新设备管理者 (DM) 用户时, 管理员可以分配范围以将 DM 的操作访问权限限制为一个或多个系统组、自定义组和/或插件组。

管理员和查看者角色具有无限范围。这意味着他们对所有设备和组实体具有 RBAC 权限指定的操作访问权限。

可以按如下所示实施范围:

1. 创建或编辑用户
2. 分配 DM 角色
3. 分配范围以限制操作访问权限

有关管理用户的更多信息, 请参阅[管理 OpenManage Enterprise 用户](#) 页面上的 124。

当具有所分配范围的设备管理者 (DM) 用户登录时, DM 只能查看和管理范围内设备。此外, 仅当 DM 拥有实体 (DM 创建了该实体或分配有该实体的所有权) 时, DM 才能查看和管理作业、固件或配置模板和基线、警报策略、配置文件等与范围内设备关联的实体。有关 DM 可以创建的实体的更多信息, 请参阅 [OpenManage Enterprise 中基于角色的访问控制 \(RBAC\) 权限](#)。

例如, 通过单击 **配置 > 模板**, DM 用户可以查看 DM 用户拥有的默认和自定义模板。此外, DM 用户还可以对拥有的模板执行 RBAC 授权的其他任务。

通过单击 **配置 > 标识池**, DM 用户可以查看管理员或 DM 用户创建的所有标识。DM 还可以对 RBAC 权限指定的标识执行操作。但是, DM 只能查看与 DM 范围下的设备相关联的标识的使用情况。

同样, 通过单击 **配置 > VLAN 池**, DM 可以查看管理员创建的所有 VLAN 并将其导出。DM 不能执行任何其他操作。如果 DM 有模板, 则可以编辑模板以使用 VLAN 网络, 但不能编辑 VLAN 网络。

在 OpenManage Enterprise 中, 可以在创建本地用户或导入 AD/LDAP 用户时分配范围。只能在 Open ID Connect (OIDC) 提供程序上完成 OIDC 用户的范围分配。

本地用户的 SBAC:

在创建或编辑具有 DM 角色的本地用户时, 管理员可以选择一个或多个定义 DM 范围的设备组。

例如，您（以管理员身份）创建名为 dm1 的 DM 用户并分配自定义组下的组 g1。那么，dm1 将仅拥有 g1 中的所有设备的操作访问权限。用户 dm1 将无法访问与任何其他设备相关的任何其他组或实体。

此外，借助 SBAC，dm1 也将无法查看其他 DM（假设 dm2）在同一个组 g1 中创建的实体。这意味着 DM 用户将只能查看用户拥有的实体。

例如，您（以管理员身份）创建另一个名为 dm2 的 DM 用户并分配自定义组下的相同组 g1。如果 dm2 为 g1 中的设备创建配置模板、配置基线或配置文件，则 dm1 将无权访问这些实体，反之亦然。

范围为“所有设备”的 DM 对 DM 拥有的所有设备和组实体具有 RBAC 权限指定的操作访问权限。

AD/LDAP 用户的 SBAC:

在导入或编辑 AD/LDAP 组时，管理员可以将范围分配给具有 DM 角色的用户组。如果用户是多个 AD 组（每个都有一个 DM 角色）的成员，并且每个 AD 组都具有不同的范围分配，则用户的范围是这些 AD 组的范围并集。

例如，

- 用户 dm1 是两个 AD 组 (*RR5-Floor1-LabAdmins* 和 *RR5-Floor3-LabAdmins*) 的成员。两个 AD 组都分配有 DM 角色，并且 AD 组的范围分配如下：*RR5-Floor1-LabAdmins* 获得 *ptlab-servers*，而 *RR5-Floor3-LabAdmins* 获得 *smclab-servers*。现在，DM dm1 的范围是 *ptlab-servers* 和 *smclab-servers* 的并集。
- 用户 dm1 是两个 AD 组 (*adg1* 和 *adg2*) 的成员。两个 AD 组均分配有 DM 角色，其中 AD 组的范围分配如下：*adg1* 具有 *g1* 的访问权限，而 *adg2* 具有 *g2* 的访问权限。如果 *g1* 是 *g2* 的超集，则 dm1 的范围是较大的范围 (*g1*、其所有子组和所有叶设备)。

如果用户是具有不同角色的多个 AD 组的成员，则功能更高的角色优先（按管理员、DM、查看者的顺序）。

具有无限范围的 DM 对所有设备和组实体具有 RBAC 权限指定的操作访问权限。

注：将 OpenManage Enterprise 升级到版本 3.6.x 后，AD/LDAP 和 OIDC (PingFederate 或 KeyCloak) 设备管理者需要重新创建所有有先前版本的实体，因为在升级后这些实体仅可供管理员使用。有关更多信息，请参阅发行说明，网址为 <https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs>。

OIDC 用户的 SBAC:

在 OME 控制台内不会进行 OIDC 用户的范围分配。在用户配置过程中，您可以在 OIDC 提供程序中为 OIDC 用户分配范围。当用户使用 OIDC 提供程序凭据登录时，角色和范围分配将可用于 OME。有关配置用户角色和范围的更多信息，请参阅在 [PingFederate 中配置 OpenID Connect 提供程序策略](#)，以提供基于角色的 OpenManage Enterprise 访问权限 页面上的 134。

注：如果要将 PingFederate 用作 OIDC 提供程序，则只能使用管理员角色。有关更多信息，请参阅在 [PingFederate 中配置 OpenID Connect 提供程序策略](#)，以提供基于角色的 OpenManage Enterprise 访问权限 页面上的 134 和发行说明（网址为 <https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs>）。

转移所有权：管理员可以将拥有的资源从一个设备管理者（源）转移给另一个设备管理者。例如，管理员可以将分配的资源从源 dm1 转移给 dm2。具有所有拥有实体（如固件和/或配置基线、配置模板、警报策略和配置文件）的设备管理者被视为合格源用户。“所有权转移”仅将实体而不是设备管理者拥有的设备组（范围）转移给另一个设备管理者。有关更多信息，请参阅 [设备管理者实体的所有权转移](#) 页面上的 129。

相关参考资料

[OpenManage Enterprise 用户角色类型](#) 页面上的 13

相关任务

[安装 OpenManage Enterprise](#) 页面上的 17

安装 OpenManage Enterprise

Dell EMC OpenManage Enterprise 作为一个设备提供，您可将其安装在虚拟机监控程序上并使用它来管理资源，从而最大程度减少停机时间。在文本用户界面 (TUI) 中进行首次网络调配后，您可从应用程序 Web 控制台配置虚拟设备。有关查看和更新控制台版本的步骤，请参阅[检查并更新 OpenManage Enterprise 及可用插件的版本](#) 页面上的 141。本章介绍安装前提条件和最低要求。

注：有关支持的浏览器的信息，请参阅支持站点上提供的 *OpenManage Enterprise 支持值表*。

相关参考资料

- OpenManage Enterprise [用户角色类型](#) 页面上的 13
- OpenManage Enterprise [图形用户界面概述](#) 页面上的 29
- OpenManage Enterprise [中的安全功能](#) 页面上的 13

相关信息

- OpenManage Enterprise [中基于角色和范围的访问控制](#) 页面上的 14

主题：

- 安装的前提条件和最低要求
- 在 VMware vSphere 上部署 OpenManage Enterprise
- 在 Hyper-V 2012 R2 及更早版本的主机上部署 OpenManage Enterprise
- 在 Hyper-V 2016 主机上部署 OpenManage Enterprise
- 在 Hyper-V 2019 主机上部署 OpenManage Enterprise
- 通过使用基于内核的虚拟机部署 OpenManage Enterprise
- 以编程方式部署 OpenManage Enterprise

安装的前提条件和最低要求

有关支持的平台、操作系统和浏览器的列表，请参阅支持站点和 Dell 技术中心上的 *Dell EMC OpenManage Enterprise 支持表*。

要安装 OpenManage Enterprise，您需要本地系统管理员权限，并且所使用的系统必须符合[最低建议硬件](#)和[安装 OpenManage Enterprise 的最低系统要求](#)中所述的标准。

最低建议硬件

该表介绍了 OpenManage Enterprise 的最低建议硬件。

表. 4: 最低建议硬件

最低建议硬件	大型部署	小型部署
可通过设备进行管理的设备数量	最多 8000	1000
RAM	32 GB	16 GB
处理器	共 8 核	共 4 核
硬盘驱动器	400 GB	400 GB

部署 OpenManage Enterprise 的最低系统要求

表. 5: 最低要求

特定	最低要求
支持的虚拟机监控程序	<ul style="list-style-type: none">VMware vSphere 版本:<ul style="list-style-type: none">vSphere ESXi 5.5 及更高支持 Microsoft Hyper-V:<ul style="list-style-type: none">Windows Server 2012 R2 及更高支持 KVM:<ul style="list-style-type: none">Red Hat Enterprise Linux 6.5 及更高
网络	可用的虚拟 NIC, 可以从 OpenManage Enterprise 访问要管理的所有设备的管理网络。
支持的浏览器	<ul style="list-style-type: none">Internet Explorer (64 位) 11 和更高版本Mozilla Firefox 52 和更高版本Google Chrome 58 和更高版本Microsoft Edge 41.16299 及更高版本
用户界面	基于 HTML 5、JS

注: 有关 OpenManage Enterprise 最低要求的最新更新, 请参阅支持站点上的 *Dell EMC OpenManage Enterprise 支持表*。

在 VMware vSphere 上部署 OpenManage Enterprise

注: 要对 OpenManage Enterprise 执行任何任务, 您必须有必要的用户权限。请参阅 *OpenManage Enterprise 中基于角色和范围的访问控制* 页面上的 14。

注: 如果辅助适配器是在首次开启设备电源之前添加的, 则该适配器将配置为禁用 IPv4 和 IPv6。在登录到 TUI, 接受 EULA 并更改管理员密码后, 该适配器将显示为**已禁用**, 并且必须由用户进行配置。

- 从支持站点下载 `openmanage_enterprise_ovf_format.zip` 文件并将文件解压到 VMware vSphere 客户端可访问的位置。建议使用本地驱动器或 CD/DVD, 因为从网络位置安装可能需要 30 分钟。
- 在 vSphere 客户端, 选择**文件 > 部署 OVF 模板**。此时将显示**部署 OVF 模板**向导。
- 在**源**页面上, 单击**浏览**, 然后选择 OVF 软件包。单击**下一步**。
- 在**OVF 模板详情**页面上, 查看所显示的信息。单击**下一步**。
- 在**最终用户许可协议**页面上, 读取许可协议并单击**接受**。要继续, 请单击**下一步**。
- 在**名称和位置**页面上, 名称最多可输入 80 个字符, 然后选择要存储模板的资源清册位置。单击**下一步**。
- 根据 vCenter 的配置, 将显示下列选项之一:
 - 如果已经配置了资源池** — 在**资源池**页面上选择虚拟服务器池来部署设备虚拟机。
 - 如果未配置资源池** — 在**主机/群集**页面上选择将要向其部署设备虚拟机的主机或群集。
- 如果主机上有多个数据存储可用, 则**数据存储**页面将显示此类数据存储。选择用于存储虚拟机 (VM) 文件的位置, 然后单击**下一步**。
- 在**磁盘格式**页面中, 单击**厚置备**以便在创建驱动器时将物理存储空间预分配给虚拟机。
- 在**已准备好完成**页面上, 查看您在以前页面上选择的选项, 然后单击**完成**以运行部署作业。完成状态窗口显示您可跟踪作业进度的位置。

在 Hyper-V 2012 R2 及更早版本的主机上部署 OpenManage Enterprise

注:

- 要对 OpenManage Enterprise 执行任何任务，您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14
 - 如果辅助适配器是在首次开启设备电源之前添加的，则该适配器将配置为禁用 IPv4 和 IPv6。在登录到 TUI，接受 EULA 并更改管理员密码后，该适配器将显示为**已禁用**，并且必须由用户进行配置。
 - 在安装或升级 Hyper-V 上的设备后，请关闭设备电源，卸下标准网络适配器并添加传统网络适配器，然后再开启设备电源。
1. 从支持站点下载 `openmanage_enterprise_vhd_format.zip` 文件。解压缩文件，然后将所附的 VHD 文件移动或复制到系统上要在其中存储 OpenManage Enterprise 虚拟驱动器的合适位置。
 2. 在 Windows Server 2012 R2 或更早版本中启动 **Hyper-V Manager**。Windows Hyper-V 应显示在 Hyper-V Manager 下。否则，请右键单击 **Hyper-V Manager**，然后选择**连接到服务器**。
 3. 单击**操作 > 新建 > 虚拟机**，启动**新建虚拟机向导**。
 4. 在最初的**准备开始**页面上，单击**下一步**。
 5. 在**指定名称和位置**页面
 - 提供**虚拟机名称**。
 - （可选）选中**在不同的位置存储虚拟机**复选框，以激活**位置**字段，然后浏览和导航，找到要存储该虚拟机的文件夹位置。

i 注：如果未选中该复选框，则虚拟机存储在默认文件夹中。
 6. 单击**下一步**。
 7. 在**指定代系**页面中，选择**第 1 代**，然后单击**下一步**。

i 注：OpenManage Enterprise 不支持第 2 代。
 8. 在**分配内存**页面上，在**启动内存**字段中输入启动内存，然后单击**下一步**。

i 注：确保最少分配 16,000 MB (16 GB)。
 9. 在**配置网络**页面上，在**连接**下拉列表中选择网络适配器。确保**虚拟交换机**已连接到网络。单击**下一步**。

i 注：如果设置为“未连接”，则第一次重新引导时 OME 将不工作；如果这种情况重复出现，就需要重新部署。
 10. 在**连接虚拟硬盘**页面上，单击**使用现有虚拟磁盘驱动器**，然后浏览到**第 1 步**中所述的复制 VHD 文件的位置。单击**下一步**。
 11. 完成屏幕上说明的操作。

i 注：确保具有 20 GB 的最低存储大小
 12. 打开新创建的虚拟机的**设置**并开启虚拟机。
 13. 在 TUI 屏幕上，在系统提示时接受 EULA，更改设备的密码，将网络参数设置为设备的 IP。

在 Hyper-V 2016 主机上部署 OpenManage Enterprise

- i 注：**
- 要对 OpenManage Enterprise 执行任何任务，您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14
 - 如果辅助适配器是在首次开启设备电源之前添加的，则该适配器将配置为禁用 IPv4 和 IPv6。在登录到 TUI，接受 EULA 并更改管理员密码后，该适配器将显示为**已禁用**，并且必须由用户进行配置。
 - 在安装或升级 Hyper-V 上的设备后，请关闭设备电源，卸下标准网络适配器并添加传统网络适配器，然后再开启设备电源。
1. 从支持站点下载 `openmanage_enterprise_vhd_format.zip` 文件。解压缩文件，然后将所附的 VHD 文件移动或复制到系统上要在其中存储 OpenManage Enterprise 虚拟驱动器的合适位置。
 2. 在 Windows Server 2016 中启动 **Hyper-V Manager**。Windows Hyper-V 应显示在 Hyper-V Manager 下。否则，请右键单击 **Hyper-V Manager**，然后选择**连接到服务器**。
 3. 单击**操作 > 新建 > 虚拟机**，启动**新建虚拟机向导**。
 4. 在最初的**准备开始**页面上，单击**下一步**。
 5. 在**指定名称和位置**页面
 - 提供**虚拟机名称**。
 - （可选）选中**在不同的位置存储虚拟机**复选框，以激活**位置**字段，然后浏览和导航，找到要存储该虚拟机的文件夹位置。

i 注：如果未选中该复选框，则虚拟机存储在默认文件夹中。
 6. 单击**下一步**。
 7. 在**指定代系**页面中，选择**第 1 代**，然后单击**下一步**。

注: OpenManage Enterprise 不支持第 2 代。

8. 在**分配内存**页面上, 在**启动内存**字段中输入启动内存, 然后单击**下一步**。

注: 确保最少分配 16,000 MB (16 GB)。

9. 在**配置网络**页面上, 在**连接**下拉列表中选择网络适配器。确保**虚拟交换机**已连接到网络。单击**下一步**。

注: 如果设置为“**未连接**”, 则第一次重新引导时 OME 将不工作; 如果这种情况重复出现, 就需要重新部署。

10. 在**连接虚拟硬盘**页面上, 单击**使用现有虚拟磁盘驱动器**, 然后浏览到第 1 步中所述的复制 VHD 文件的位置。单击**下一步**。

11. 完成屏幕上说明的操作。

注: 确保具有 20 GB 的最低存储大小

12. 打开新创建的虚拟机的**设置**并开启虚拟机。

13. 在 TUI 屏幕上, 在系统提示时接受 EULA, 更改设备的密码, 将网络参数设置为设备的 IP。

在 Hyper-V 2019 主机上部署 OpenManage Enterprise

注:

- 要对 OpenManage Enterprise 执行任何任务, 您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14
- 如果辅助适配器是在首次开启设备电源之前添加的, 则该适配器将配置为禁用 IPv4 和 IPv6。在登录到 TUI, 接受 EULA 并更改管理员密码后, 该适配器将显示为**已禁用**, 并且必须由用户进行配置。
- 在安装或升级 Hyper-V 上的设备后, 请关闭设备电源, 卸下标准网络适配器并添加传统网络适配器, 然后再开启设备电源。

1. 从支持站点下载 **openmanage_enterprise_vhd_format.zip** 文件。解压缩文件, 然后将所附的 VHD 文件移动或复制到系统上要

在其中存储 OpenManage Enterprise 虚拟驱动器的合适位置。

2. 在 Windows Server 2019 中启动 **Hyper-V Manager**。Windows Hyper-V 应显示在 Hyper-V Manager 下。否则, 请右键单击 **Hyper-V Manager**, 然后选择**连接到服务器**。

3. 单击**操作 > 新建 > 虚拟机**, 启动**新建虚拟机向导**。

4. 在最初的**准备开始**页面上, 单击**下一步**。

5. 在**指定名称和位置**页面

- 提供**虚拟机名称**。

- (可选) 选中在**不同的位置存储虚拟机**复选框, 以激活**位置**字段, 然后浏览和导航, 找到要存储该虚拟机的文件夹位置。

注: 如果未选中该复选框, 则虚拟机存储在默认文件夹中。

6. 单击**下一步**。

7. 在**指定代系**页面中, 选择**第 1 代**, 然后单击**下一步**。

注: OpenManage Enterprise 不支持第 2 代。

8. 在**分配内存**页面上, 在**启动内存**字段中输入启动内存, 然后单击**下一步**。

注: 确保最少分配 16,000 MB (16 GB)。

9. 在**配置网络**页面上, 在**连接**下拉列表中选择网络适配器。确保**虚拟交换机**已连接到网络。单击**下一步**。

注: 如果设置为“**未连接**”, 则第一次重新引导时 OME 将不工作; 如果这种情况重复出现, 就需要重新部署。

10. 在**连接虚拟硬盘**页面上, 单击**使用现有虚拟磁盘驱动器**, 然后浏览到第 1 步中所述的复制 VHD 文件的位置。单击**下一步**。

11. 完成屏幕上说明的操作。

注: 确保具有 20 GB 的最低存储大小

12. 打开新创建的虚拟机的**设置**并开启虚拟机。

13. 在 TUI 屏幕上, 在系统提示时接受 EULA, 更改设备的密码, 将网络参数设置为设备的 IP。

通过使用基于内核的虚拟机部署 OpenManage Enterprise

注:

- 要对 OpenManage Enterprise 执行任何任务, 您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14

- 如果辅助适配器是在首次开启设备电源之前添加的，则该适配器将配置为禁用 IPv4 和 IPv6。在登录到 TUI，接受 EULA 并更改管理员密码后，该适配器将显示为**已禁用**，并且必须由用户进行配置。

1. 安装操作系统时安装所需的虚拟化软件包。
2. 从支持站点下载 `openmanage_enterprise_kvm_format.zip` 文件。解压缩文件到将要在其中存储 OpenManage Enterprise 虚拟驱动器的合适位置。
3. 启动虚拟机管理器并选择**文件 > 属性**。
4. 在**网络接口**页面中，单击**添加**。
5. 选择**桥接**作为接口类型，然后单击**转发**。
6. 将启动模式设置为 **onboot** 并选中**立即激活**复选框。
7. 从列表中选择要桥接的接口，并确保属性与主机设备匹配，然后单击**完成**。
虚拟界面现已创建，您可以使用终端来配置防火墙设置了。
8. 在虚拟机管理器上，单击**文件 > 新建**。
9. 输入虚拟机的名称并选择**导入现有的磁盘映像**选项，然后单击**前进**。
10. 导航文件系统并选择在步骤 1 中下载的 QCOW2 文件，然后单击**前进**。
11. 分配 16 GB 作为内存并选择两个处理器内核，然后单击**前进**。
12. 为虚拟机分配所需的磁盘空间，然后单击**前进**。
13. 在**高级选项**下，确保已选择桥接的主机设备网络，并且已选择 KVM 作为“Virt 类型”。
14. 单击**完成**。

现在通过使用 KVM 部署 OpenManage Enterprise 设备。要开始使用 OpenManage Enterprise，请参阅[登录到 OpenManage Enterprise](#) 页面上的 23。

以编程方式部署 OpenManage Enterprise

在 VMware ESXi 版本 6.5 或更高版本上，OpenManage Enterprise 可以编程方式（使用脚本）部署。

注：编程/脚本式部署仅支持使用主要接口。

注：如果辅助适配器是在首次开启设备电源之前添加的，则该适配器将配置为禁用 IPv4 和 IPv6。在登录到 TUI，接受 EULA 并更改管理员密码后，该适配器将显示为**已禁用**，并且必须由用户进行配置。

注：您必须使用最新版本的 OVF 工具和 Python 3.0 或更高版本进行编程部署。

要以编程方式部署 OpenManage Enterprise，请执行以下操作：

1. 下载并解压缩 `openmanage_enterprise_ovf_format.zip` 文件，或者从支持站点单个下载以下 OVF 文件：
 - `openmanage_enterprise.x86_64-0.0.1-disk1.vmdk`
 - `openmanage_enterprise.x86_64-0.0.1.mf`
 - `openmanage_enterprise.x86_64-0.0.1.ovf`
 - `openmanage_enterprise.x86_64-0.0.1.vmx`
 - `ovf_properties.config`
 - `update_ovf_property.py`
2. 打开 `ovf_properties.config` 并设置以下参数：

表. 6: `ovf_properties.config` 中使用的参数

参数	接受的值	说明
<code>bEULATxt</code>	True 或 False	将此值设置为 True 即表示您同意最终用户许可协议 (EULA) 中的条款和条件。EULA 位于 <code>ovf_properties.config</code> 文件的底部。
<code>adminPassword</code>	必须包含至少一个以下字符：大写字母、小写字母、数字和特殊字符。例如，Dell123\$	键入 OpenManage Enterprise 的新管理员密码。
<code>bEnableDHCP</code>	True 或 False	如果您希望设备启用 IPv4 DHCP 而忽略静态 IPv4，请将此参数设置为 True。

表. 6: `ovf_properties.config` 中使用的参数 (续)

参数	接受的值	说明
<code>bEnableIpv6AutoConfig</code>	True 或 False	如果您希望设备启用 IPv6 自动配置而忽略静态 IPv6, 请将此参数设置为 True。
<code>staticIP</code>	CIDR 格式的静态 IP	可以是 IPv4 或 IPv6。(您不能同时设置 IPv4 和 IPv6 类型。)
<code>gateway</code>	IPv4 或 IPv6	您不能同时将静态网关设置为 IPv4 和 IPv6 类型。

3. 运行 `update_ovf_property.py` 脚本。

此脚本修改 `openmanage_enterprise.x86_64-0.0.1.ovf` 文件, 依据 `ovf_properties.config` 文件中设置的值进行部署。脚本执行完成后, 随即显示一个示例 `ovftool` 命令。该命令包含 `<DATASTORE>`, `<user>`, `<password>`, `<IP address>` 等标签, 您必须按照您的部署环境替换这些标签。这些设置定义了目标 ESXi 系统上使用的资源, 还有目标系统的凭据和 IP 地址。

注: 切记替换整个标签, 包括 `<` 和 `>` 符号。

4. 运行上一步中修改后的 `ovftool` 命令。

注: 运行 `ovftool` 命令必须附带 `--X:injectOvfEnv` 和 `--powerOn` 标志, 因为它们是编程部署所必需的。

运行 `ovftool` 命令后, 将会验证清单并开始部署。

OpenManage Enterprise 使用入门

主题:


- 登录到 OpenManage Enterprise
- 使用文本用户界面配置 OpenManage Enterprise
- 配置 OpenManage Enterprise
- 获得最佳 OpenManage Enterprise 使用的建议的可扩展性和性能设置
- OpenManage Enterprise 中支持的协议和端口
- 在 OpenManage Enterprise 中支持的协议和端口的使用案例链接

登录到 OpenManage Enterprise


首次从文本用户界面 (TUI) 中引导系统时，系统会提示您接受 EULA，然后更改管理员密码。如果您首次登录到 OpenManage Enterprise，您必须通过 TUI 设置用户凭据。请参阅[使用文本用户界面配置 OpenManage Enterprise](#) 页面上的 23。

 **小心:** 如果您忘记了管理员密码，则无法从 OpenManage Enterprise 设备中恢复。

1. 启动支持的浏览器。
2. 在地址框中，输入 OpenManage Enterprise 设备 IP 地址。
3. 在登录页面上，键入登录凭据，然后单击**登录**。

 **注:** 默认用户名为 admin。

如果您是首次登录 OpenManage Enterprise，将显示**欢迎使用 OpenManage Enterprise** 页面。单击**初始设置**并完成基本配置设置。请参阅[配置 OpenManage Enterprise](#) 页面上的 25。要查找设备，请单击**查找设备**。

 **注:** 默认情况下，在登录尝试失败三次后，您的 OpenManage Enterprise 帐户将被锁定，并且在帐户锁定时间结束之前您将无法登录。默认情况下，帐户锁定时间为 900 秒。要更改此持续时间，请参阅[设置登录安全性属性](#) 页面上的 137。

使用文本用户界面配置 OpenManage Enterprise

文本用户界面 (TUI) 工具提供一个文本界面，用于更改管理员密码、查看设备状态和网络配置、配置网络参数、启用现场服务调试请求、选择主要网络以及配置设备以自动查找您网络中的服务器。

当您第一次从 TUI 引导系统时，系统会提示您接受最终用户许可协议 (EULA)。接下来，更改管理员密码并为应用装置配置网络参数，然后在支持的浏览器中加载 Web 控制台以开始操作。只有具有 OpenManage 管理员权限的用户才能配置 OpenManage Enterprise。

在 TUI 界面上，使用箭头键或按 **Tab** 键以转至 TUI 上的下一选项，然后按 **Shift + Tab** 键返回到之前的选项。按 **Enter** 键选择选项。按 **Space** 键切换复选框的状态。

注:

- 要配置 IPv6，请确保其已由 vCenter 服务器配置。
- 默认情况下，OpenManage Enterprise 会使用最新查找到的设备的 IP 来执行所有操作。要让任何 IP 更改生效，您必须重新查找设备。

您可以通过使用 TUI 配置 OpenManage Enterprise。TUI 屏幕包含以下选项：

表. 7: 文本用户界面选项

选项	说明
更改管理员密码	选择 更改管理员密码 屏幕以输入新密码并确认该密码。 第一次登录后，您必须使用 TUI 屏幕上更改密码。

表. 7: 文本用户界面选项 (续)

选项	说明
显示当前设备状态	选择 显示当前设备状态 以查看设备的 URL 和状态。您还可以查看任务执行、事件处理、Tomcat、数据库和监测服务的状态。
显示当前网络配置	选择 显示当前网络配置 以查看 IP 配置详细信息。 选择网络适配器 菜单将列出所有可用的网络适配器。单击网络适配器将显示其当前设置。
设置一体机主机名称	选择 设置一体机主机名称 以在 DNS 上配置一体机的名称。此字段支持以下适用于主机名称的有效字符: 字母数字字符 (a-z、A-Z、0-9)、英文句号 (.) 和连字符 (-)。 注: 使用英文句号将指定域名信息。如果一体机的 DNS 信息采用的是静态配置, 而不是从 DHCP 获取域详细信息, 则必须使用完全限定域名 (FQDN) 配置主机名称, 以便可以填充域搜索信息。
设置网络参数	选择 设置网络参数 以重新配置网络适配器。 选择网络适配器 菜单将列出所有可用的网络适配器。选择一个网络适配器, 重新配置其网络参数, 然后选择 应用 以保存对相应接口的更改。 默认情况下, 在主要网络接口上仅启用 IPv4, 在设备中使用专用静态 IP。但是, 如果添加了新网络接口, 则同时启用 IPv4 和 IPv6 以便使用多宿主功能。 如果 OpenManage Enterprise 设备无法获得 IPv6 地址, 请检查环境是否已针对路由器广告进行配置以打开受管位 (M)。当此位打开时, 当前 Linux 发行版中的 Network Manager 会导致链路故障, 并且 DHCPv6 不可用。确保网络上已启用 DHCPv6, 或者禁用路由器广告的受管标志。 注: <ul style="list-style-type: none"> DNS 配置仅在主要网络接口上可用。如果此接口上需要 DNS 解决方案, 则所有主机名都必须可通过主要接口上配置的 DNS 服务器解析。
选择主要网络接口	选择主要网络接口 可指定主要网络。 主要接口选择会基于路由情况赋予所选接口优先级并将其用作默认路由。如果有不明确的情况, 此接口将具有路由优先级。主要接口预计也将是允许进行企业网络/互联网连接的“面向公众”的接口。将不同的防火墙规则应用于主要接口, 可允许实现更严格的访问控制, 如基于 IP 范围的访问限制。 注: 如果启用多宿主, 可从两个网络访问应用装置。在这种情况下, 使用代理设置时, 应用装置对于所有外部通信都使用主要接口。有关 OpenManage 上的多宿主的详细信息, 请参阅支持站点上的 <i>使用 Dell EMC OpenManage Enterprise 的远程脚本执行技术白皮书</i> 。
配置静态路由	如果网络需要将静态路由配置为通过 IPv4 和 IPv6 网络访问特定子网, 则选择 配置静态路由 。 注: 每个接口最多支持 20 个静态路由。
配置服务器启动的查找	选择 配置服务器启动的查找 , 以允许应用装置使用配置的 DNS 服务器自动注册所需的记录。 注: <ul style="list-style-type: none"> 确保设备已向 DNS 注册, 并且可动态更新记录。 目标系统必须配置为从 DNS 请求注册详细信息。

表. 7: 文本用户界面选项 (续)

选项	说明
	<ul style="list-style-type: none"> 要更改 DNS 域名, 请确保在 DNS 服务器上启用动态 DNS 注册。同样, 对于在 DNS 服务器上注册的设备, 请选择动态更新下的非安全和安全选项。
配置设备磁盘大小	<p>选择配置设备磁盘大小以扫描是否有磁盘空间或新磁盘, 然后根据需要为设备分配额外的磁盘空间或磁盘。</p> <p>注:</p> <ul style="list-style-type: none"> 强烈建议在应用任何磁盘配置更改之前, 拍摄控制台的虚拟机快照作为备份。 添加磁盘空间后, 不支持删除或缩减扩展磁盘空间。要删除新添加的磁盘或反转现有磁盘的大小增加, 必须恢复到之前的虚拟机快照。 如果初始扫描未检测到未分配的空间, 则在您的虚拟机管理程序上为控制台分配额外的磁盘空间或磁盘, 然后重新扫描。 磁盘空间的扫描和分配限制为最多四个磁盘。
启用现场服务调试 (FSD) 模式	<p>为控制台调试选择启用现场服务调试 (FSD) 模式。有关更多信息, 请参阅 现场服务调试工作流程 页面上的 152。</p>
重新启动服务	<p>使用以下选项选择重新启动服务, 以重新启动服务和网络:</p> <ul style="list-style-type: none"> 重新启动所有服务 重新启动网络
设置调试日志记录	<p>使用以下选项选择设置调试日志记录:</p> <ul style="list-style-type: none"> 启用调试日志 — 收集应用程序监测任务、事件和任务执行历史记录 of 调试日志。 禁用调试日志 — 禁用调试日志。 启用 SCP 保留 — 收集模板 XML 文件。 禁用 SCP 保留 — 禁用 SCP 保留。 <p>您可以通过在 OpenManage Enterprise 中单击监测 > 审核日志 > 导出 > 导出控制台日志来下载调试日志。</p>
更改键盘布局	<p>如有必要, 请选择更改键盘布局以更改键盘布局。</p>
重新引导设备	<p>选择重新启动设备以重新启动设备。</p> <p>注: 运行命令以重新启动服务后, TUI 可能会显示以下消息: NMI watchdog: BUG: soft lockup - CPU#0 stuck for 36s! [java:14439].</p> <p>可能由于虚拟机管理程序过载而出现软锁定问题。在这种情况下, 建议至少将 16 GB RAM 和 8000 MHz CPU 保留给 OpenManage Enterprise 设备。还建议在显示此消息时, 重新启动 OpenManage Enterprise 设备。</p>

配置 OpenManage Enterprise

如果您首次登录到 OpenManage Enterprise, 则会显示**欢迎使用 OpenManage Enterprise** 页面, 允许您设置时间 (手动或使用 NTP 时间同步) 和代理服务器配置。

1. 要手动配置时间, 请在**时间配置**部分中执行以下操作:

- 使用**时区** 下拉菜单选择适当的时区。
- 在**日期** 框中, 输入或选择一个日期。
- 在**时间** 框中, 填写时间。
- 单击**应用**保存设置。

2. 如果想要使用 NTP 服务器进行时间同步, 请在**时间配置**部分中执行以下操作:

注: NTP 服务器设置更新时，当前已登录的用户会自动从他们的 OpenManage Enterprise 会话中注销。

- 选中**使用 NTP** 复选框。
- 在**主要 NTP 服务器地址** 和**次要 NTP 服务器地址** (可选) 中输入 IP 地址或主机名以进行时间同步

3. 如果您想设置代理服务器进行外部通信，请在“代理服务器配置”部分中执行以下操作：

- 选中**启用 HTTP 代理设置** 复选框。
- 输入**代理服务器地址**。
- 输入代理服务器的**端口号**。
- 如果代理服务器需要凭据才能登录，请选中**启用代理身份验证** 复选框，并输入用户名和密码。
- 如果配置的代理截获 SSL 流量且不使用受信任的第三方证书，请选中**忽略证书验证**复选框。使用此选项将忽略用于保修和目录同步的内置证书检查。

4. 单击**应用**保存设置。

注: 有关支持的浏览器的信息，请参阅支持站点上提供的 *OpenManage Enterprise 支持值表*。

获得最佳 OpenManage Enterprise 使用的建议的可扩展性和性能设置

下表列出了在 OpenManage Enterprise 中支持的功能的性能参数。要确保 OpenManage Enterprise 的最佳性能，Dell EMC 建议在每个任务建议的最大设备数上以指定频率运行任务。

表. 8: OpenManage Enterprise 的可扩展性和性能注意事项

任务	运行任务所建议的频率	任务是否预制?	每个任务所建议的最大设备数。
查找	对于频繁网络变化的环境，一天一次。	否	每个任务 10,000
资源清册	OpenManage Enterprise 提供了能每天一次自动刷新资源清册的预制任务。	可以。您可以禁用此功能。	由 OpenManage Enterprise 监测的设备。
保修	OpenManage Enterprise 提供了能每天一次自动刷新保修的预制任务。	可以。您可以禁用此功能。	由 OpenManage Enterprise 监测的设备。
运行状况轮询	每隔一小时	可以。您可以更改此频率。	不适用
固件/驱动程序更新	根据需要		每个任务 150
配置资源清册	根据需要		1500/基线

OpenManage Enterprise 中支持的协议和端口

在管理站上支持的协议和端口

表. 9: 管理站上 OpenManage Enterprise 支持的协议和端口

端口号	协议	端口类型	最高加密级别	源	方向	目标	使用情况
22	SSH	TCP	256 位	管理站	进	OpenManage Enterprise 设备	<ul style="list-style-type: none"> • 仅当使用 FSD 时才需要传入。仅当与 Dell EMC 支持人员交互时，OpenManage Enterprise 管理员才需要启用。

表 9: 管理站上 OpenManage Enterprise 支持的协议和端口 (续)

端口号	协议	端口类型	最高加密级别	源	方向	目标	使用情况
25	SMTP	TCP	无	OpenManage Enterprise 设备	出	管理站	<ul style="list-style-type: none"> 要接收来自 OpenManage Enterprise 的电子邮件警报。
53	DNS	UDP/TCP	无	OpenManage Enterprise 设备	出	管理站	<ul style="list-style-type: none"> 适用于 DNS 查询。
68/546 (IPv6)	DHCP	UDP/TCP	无	OpenManage Enterprise 设备	出	管理站	<ul style="list-style-type: none"> 网络配置。
80*	HTTP	TCP	无	管理站	进	OpenManage Enterprise 设备	<ul style="list-style-type: none"> Web GUI 登录页面。这会将用户重定向到 HTTPS (端口 443)。
123	NTP	TCP	无	OpenManage Enterprise 设备	出	NTP 服务器	<ul style="list-style-type: none"> 时间同步 (如已启用)。
137、138、139、445	CIFS	UDP/TCP	无	iDRAC/CMC	进	OpenManage Enterprise 设备	<ul style="list-style-type: none"> 要上传或下载部署模板。 上传 TSR 和诊断日志。 下载固件/驱动程序 DUP 和 FSD 进程。 启动至网络 ISO。
				OpenManage Enterprise 设备	出	CIFS 共享	<ul style="list-style-type: none"> 从 CIFS 共享导入固件/驱动程序目录。
111、2049 (默认值)	NFS	UDP/TCP	无	OpenManage Enterprise 设备	出	外部 NFS 共享	<ul style="list-style-type: none"> 从 NFS 共享下载目录和 DUP 以进行固件更新。 用于从网络共享进行手动控制台升级。
162*	SNMP	UDP	无	管理站	进/出	OpenManage Enterprise 设备	<ul style="list-style-type: none"> 通过 SNMP 进行事件接收。仅当使用陷阱转发策略时，方向才是“传出”。
443 (默认)	HTTPS	TCP	128 位 SSL	管理站	进/出	OpenManage Enterprise 设备	<ul style="list-style-type: none"> Web GUI。 要从 Dell.com 下载更新和保修信息。与 OpenManage Enterprise 通信时允许使用 256 位加密：对 Web GUI 使用 HTTPS。 服务器发起的查找。
514	系统日志	TCP	无	OpenManage Enterprise 设备	出	Syslog 服务器	<ul style="list-style-type: none"> 将警报和审核日志信息发送到 Syslog 服务器。
3269	LDAPS	TCP	无	OpenManage Enterprise 设备	出	管理站	<ul style="list-style-type: none"> 全局编录的 AD/LDAP 登录。
636	LDAPS	TCP	无	OpenManage Enterprise 设备	出	管理站	<ul style="list-style-type: none"> 域控制器的 AD/LDAP 登录。

* 端口最多可配置为 499，不包括已分配的端口号。

在受管节点上支持的协议和端口

表. 10: 受管节点上 OpenManage Enterprise 支持的协议和端口

端口号	协议	端口类型	最高加密级别	源	方向	目标	使用情况
22	SSH	TCP	256 位	OpenManage Enterprise 设备	出	受管节点	<ul style="list-style-type: none"> 适用于 Linux OS、Windows 和 Hyper-V 查找。
161	SNMP	UDP	无	OpenManage Enterprise 设备	出	受管节点	<ul style="list-style-type: none"> 适用于 SNMP 查询。
162*	SNMP	UDP	无	OpenManage Enterprise 设备	输入/输出	受管节点	<ul style="list-style-type: none"> 发送和接收 SNMP 陷阱。
443	专用/ WS-Man/ Redfish	TCP	256 位	OpenManage Enterprise 设备	出	受管节点	<ul style="list-style-type: none"> iDRAC7 及更高版本的发现和资源清册。 用于 CMC 管理。
623	IPMI/ RMCP	UDP	无	OpenManage Enterprise 设备	出	受管节点	<ul style="list-style-type: none"> 通过 LAN 进行 IPMI 访问。
69	TFTP	UDP	无	CMC	进	管理站	<ul style="list-style-type: none"> 用于更新 CMC 固件。

* 端口最多可配置为 499，不包括已分配的端口号。

 注: 在 IPv6 环境中，必须启用 IPv6 并在 OpenManage Enterprise 设备中禁用 IPv4，以确保所有功能按预期工作。

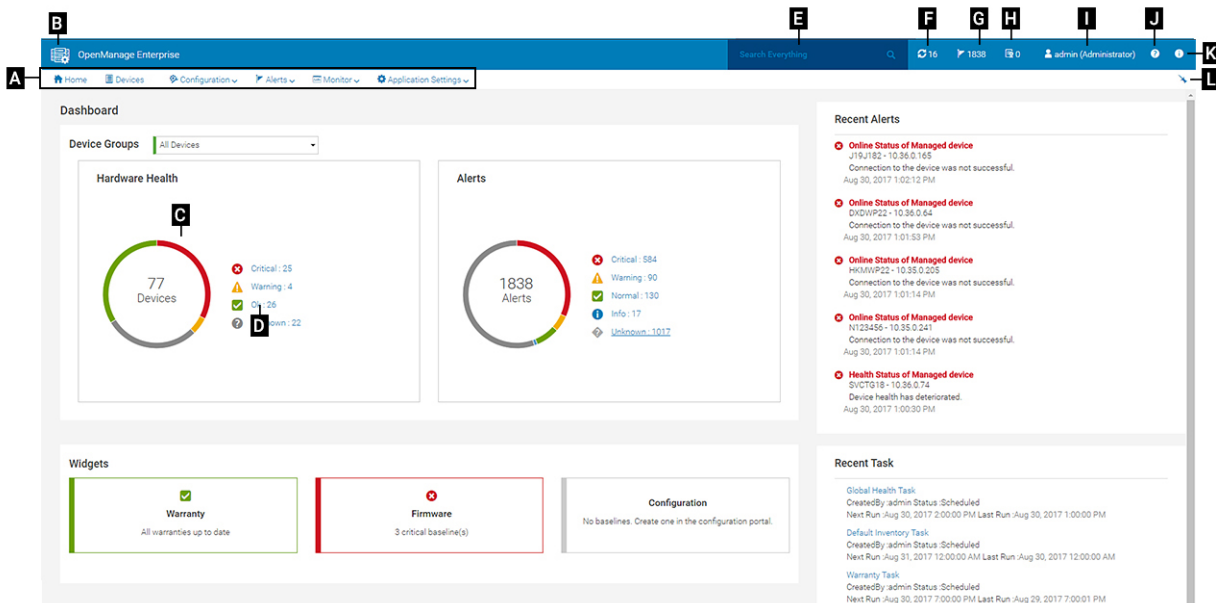
在 OpenManage Enterprise 中支持的协议和端口的使用案例链接

表. 11: 在 OpenManage Enterprise 中支持的协议和端口的使用案例链接

使用案例	URL
升级 OpenManage Enterprise 设备	https://downloads.dell.com/openmanage_enterprise/
访问设备保修	https://apigtwb2c.us.dell.com/PROD/sbil/eapi/v5/asset-entitlements
更新目录	https://downloads.dell.com/catalog/
使用 OpenManage Mobile 应用程序推送新的警报通知	https://openmanagecloud.dell.com

OpenManage Enterprise 图形用户界面概述

在 OpenManage Enterprise (GUI) 上, 您可以使用菜单项、链接、按钮、窗格、对话框、列表、选项卡、筛选框和页面以在页面与完成设备管理任务之间导航。诸如设备列表、环形图、审核日志、OpenManage Enterprise 设置、系统警报和固件/驱动程序更新等功能将显示在多个位置。建议您熟悉 GUI 元素, 以便轻松有效地使用 OpenManage Enterprise 管理您的数据中心设备。



- A — OpenManage Enterprise 所有页面上的 **OpenManage Enterprise** 菜单都提供了链接, 通过这些链接, 管理员可以查看仪表盘 (主页)、管理设备 (设备)、管理固件/驱动程序基线、模板和配置合规性基线 (配置)、创建和存储警报 (警报), 然后运行作业、查找、收集资源清册数据, 以及生成报告 (监测)。您还可以自定义 OpenManage Enterprise 的不同属性 (应用程序设置)。单击右上角的图钉符号, 将菜单项目固定, 使其在所有 OpenManage Enterprise 页面上显示。要解除固定, 请再次单击图钉符号。
- B — 仪表盘符号。单击此选项可从 OpenManage Enterprise 的任何页面中打开仪表盘页面。或者, 单击**主页**。请参阅**仪表盘**。
- C — 环形图提供由 OpenManage Enterprise 监测的所有设备运行状况的快照。使您能够对处于严重状态的设备快速执行操作。图中的每种颜色代表具有特定运行状况的设备组。单击相应的色带可查看设备列表中的各个设备。单击设备名称或 IP 地址以查看设备属性页面。请参阅**查看和配置各个设备** 页面上的 56。
- D — 用于表示设备运行状况的符号。请参阅**设备运行状况状态** 页面上的 33。
- E — 在**搜索所有内容**框中, 输入 OpenManage Enterprise 监测和显示的任何内容, 以查看结果, 如基于范围的访问控制 (SBAC) 定义的范围内的所有设备的设备 IP、作业名称、组名、固件/驱动程序基线和保修数据。您不能通过使用搜索所有功能排序或导出检索的数据。在单独的页面或对话框中, 输入或从**高级筛选器**部分中选择内容, 以细化您的搜索结果。
 - **不支持以下运算符: +、- 和 "。**
- F — 当前在队列中的 OpenManage Enterprise 作业数。与查找、资源清册、保修、固件和/或驱动程序更新等相关的作业。单击此选项可查看在“作业详细信息”页中的“运行状况”、“资源清册”和“报告”类别下运行的作业。要查看所有事件, 请单击**所有作业**。请参阅**使用作业进行设备控制** 页面上的 106。单击以刷新。
- G — 警报日志中生成的事件数量。另外, 根据您设置是否查看未确认的警报, 此部分中的警报数会有所不同。默认情况下, 仅显示未确认警报。要隐藏或取消隐藏已确认的警报, 请参阅**自定义警报显示** 页面上的 138。删除警报会降低计数。有关用于指示严重性状态的符号信息, 请参阅**设备运行状况状态** 页面上的 33。单击严重性符号可查看“警报”页中该严重性类别下的所有事件。要查看所有事件, 请单击**所有作业**。请参阅**管理设备警报**。
- H — 处于严重 (已过期) 和警告 (即将过期) 状态的设备保修的总数。请参阅**管理设备保修**。
- I — 当前登录的用户的名称。将指针暂停在用户名以查看分配给用户的角色。有关基于角色的用户的更多信息, 请参阅 **OpenManage Enterprise 中基于角色和范围的访问控制** 页面上的 14。单击以注销, 随后以不同的用户身份登录。
- J - 当前, 上下文相关帮助文件仅在您所在的页面显示, 而不在主页门户页面。单击此选项可查看基于任务的说明, 以便有效地使用 OpenManage Enterprise 中的链接、按钮、对话框、向导和页面。

- K — 单击以查看系统上安装 OpenManage Enterprise 的当前版本。单击**许可证**以浏览消息。单击相应的链接以查看和下载 OpenManage Enterprise 相关的开源文件，或其他开源许可证。
- L - 单击该符号以固定或解除固定菜单项目。解除固定后，要固定某个菜单项目，请展开 **OpenManage Enterprise** 菜单并单击图钉符号。

有关表中所列项目的的数据可以全面了解、一起导出或基于所选项目查看。请参阅[导出所有或所选数据](#) 页面上的 56。无论在同一窗口还是不同页面中打开，当显示为蓝色文本时，即可查看和更新表中关于该项目的详细信息。列表数据可以使用**高级筛选器**功能进行筛选。根据您查看的内容，筛选会有所不同。从字段中输入或选择数据。不完整的文本或数字将不能显示预期的输出。列表中显示符合筛选条件的数据。要移除筛选，请单击**清除全部筛选**。

要排序列表数据，请单击列标题。您不能通过使用搜索所有功能排序或导出检索的数据。

符号用于标识主要项目、仪表板、设备运行状况状态、警报类别、固件和驱动程序合规性状态、连接状态和电源状态等。单击浏览器的向前和向后按钮以在 OpenManage Enterprise 上的页面之间导航。有关支持的浏览器的信息，请参阅支持站点上提供的 *Dell EMC OpenManage Enterprise 支持值表*。

在适当情况下，页面会分为左侧窗格、工作窗格和右侧窗格以简化设备管理任务。如有必要，指针停在 GUI 元素时会显示联机说明和工具提示。

右侧窗格中显示有关设备的预览、作业、资源清册、固件/驱动程序基线、管理应用程序、虚拟控制台等。在工作窗格中选择一个项目，并在右侧窗格中单击**查看详细信息**以查看关于该项目的详细信息。

登录时会自动刷新所有页面。完成一体机部署后，在后续登录时，如果 OpenManage Enterprise 有更新版本可用，单击**更新**，您会立即收到更新版本提醒。具有所有 OpenManage Enterprise 权限的用户（管理员、设备管理者和查看者）可以查看消息，但只有管理员可以更新版本。管理员可以选择稍后提醒或取消消息。有关更新 OpenManage Enterprise 版本的更多信息，请参阅 [检查并更新 OpenManage Enterprise 及可用插件的版本](#) 页面上的 141。

对于 OpenManage Enterprise 执行的所有基于作业的操作，当创建或开始运行作业时，右下角会显示相应的消息。作业的详细信息可在[作业详细信息](#)页面中查看。请参阅[查看作业列表](#) 页面上的 106。

相关信息

[安装 OpenManage Enterprise](#) 页面上的 17

OpenManage Enterprise 门户主页

单击 **OpenManage Enterprise > 主页**，则会显示 OpenManage Enterprise 主页。在主页上：

- 查看仪表板以获取有关设备运行状况的实时快照，然后采取措施，如有必要。请参阅[仪表板](#)。
- 查看并解决严重和警告类别下的警报。请参阅[管理设备警报](#)。
- “小部件”部分列出了所有设备的汇总保修、固件/驱动程序合规性和配置合规性状态。有关“小部件”下面功能的更多信息，请参阅[使用 OpenManage Enterprise 仪表板监测设备](#) 页面上的 31。右侧窗格列出了 OpenManage Enterprise 生成的最近警报和任务。要查看有关该警报或任务的更多信息，请单击警报或任务标题。请参阅[监视和管理设备警报](#) 页面上的 97 和[使用作业进行设备控制](#) 页面上的 106。
- 如果有 OpenManage Enterprise 的更新版本可用，则更新一旦可用，您就会立即收到提示。要更新，请单击**更新**。有关更新 OpenManage Enterprise 版本的更多信息，请参阅[检查并更新 OpenManage Enterprise 及可用插件的版本](#) 页面上的 141。
- **最近警报**部分列出了受 OpenManage Enterprise 监测的设备生成的最近警报。单击警报标题以了解关于警报的详细信息。请参阅[管理设备警报](#)。
- **最近任务**部分列出了创建并运行的最近任务（作业）。单击任务标题以了解关于作业的详细信息。请参阅[查看作业列表](#) 页面上的 106。

注：如果以设备管理者的身份登录，则主页门户将显示有关 DM 拥有的设备/设备组的信息。此外，“设备组”下拉菜单仅列出设备管理者拥有操作访问权限的设备组。请参阅[OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

主题：

- [使用 OpenManage Enterprise 仪表板监测设备](#)
- [环形图](#)
- [设备运行状况状态](#)

使用 OpenManage Enterprise 仪表板监测设备

注：要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅[OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

除了首次登录之外，您后续每次登录 OpenManage Enterprise 时都将看到仪表板作为您的初始页面。

要从 OpenManage Enterprise 的任何页面中打开仪表板页面，请单击左上角的仪表板符号。或者，单击**主页**。

仪表板使用实时监测数据，显示数据中心环境中设备和设备组的设备运行状况、固件/驱动程序合规性、保修、警报以及其他方面。

任何可用的控制台更新也会在仪表板上显示。您可以立即升级 OpenManage Enterprise 版本，或者设置 OpenManage Enterprise 提醒您稍后升级。

默认情况下，首次启动应用程序时，仪表板页面显示为空。将设备添加到 OpenManage Enterprise，以便它们可以在仪表板上进行监测和显示。要添加设备，请参阅[查找要监测或管理的设备](#) 页面上的 34 和[将设备按组整理](#) 页面上的 46。

- [管理设备固件和驱动程序](#) 页面上的 64
- [管理设备警报](#)
- [查找设备](#)
- [创建报告](#)
- [管理 OpenManage Enterprise 设备设置](#) 页面上的 123

注：如果您在**设备组**下拉列表中选择任何设备组，则仪表板上显示的所有数据将仅适用于所选设备组。

默认情况下，**硬件运行状况**部分以环形图方式显示，其中显示了 OpenManage Enterprise 监测的所有设备的当前运行状况。单击环形图中的各部分，可以查看各自运行状况的设备信息。

警报部分的环形图列出了所选设备组中的设备接收的警报。请参阅[监视和管理设备警报](#) 页面上的 97。环形图中的警报总数会根据是否设置为查看未确认的警报而有所不同。默认情况下，仅显示未确认警报。请参阅[自定义警报显示](#) 页面上的 138。要查看每个类别下的警报，请单击相应的色带。在**警报**对话框中，“严重”部分列出了处于严重状态中的设备。要查看生成的所有警报，请单击**所有**。**源名称**列表表示生成警报的设备。单击名称可查看和配置设备属性。请参阅[查看和配置各个设备](#) 页面上的 56。

有关环形图的更多信息，请参阅[环形图](#) 页面上的 32 和[设备运行状况状态](#) 页面上的 33。要查看由 OpenManage Enterprise 监控的不同设备组中的设备摘要，请从[设备组](#) 下拉菜单中进行选择。要查看属于某种运行状况的[设备列表](#)，您可以单击与运行状况类别关联的色带，或单击环形图旁边的运行状况符号。

注：在“设备”列表中，单击设备名称或 IP 地址以查看设备配置数据，然后进行编辑。请参阅[查看和配置各个设备](#) 页面上的 56。




小部件部分提供了 OpenManage Enterprise 的一些主要功能的摘要。要查看每个类别下的摘要，请单击小部件标题。

- **保修：**显示保修即将过期的设备数量。这取决于[保修设置](#)。如果用户选择接收过期保修通知，则会显示保修已过期的设备数量。否则，将会显示即将过期或有效保修的数量。单击以在[保修](#)对话框中查看更多信息。有关管理设备保修的信息，请参阅[管理设备保修](#) 页面上的 113。将指针暂停在[保修](#)部分以读取本部分使用的符号的定义。
- **固件/驱动程序：**显示在 OpenManage Enterprise 上创建的设备基线的固件/驱动程序合规性状态。如果可用，本部分列出“严重”和“警告”固件/驱动程序基线。
 - 有关“汇总运行状况”状态的更多信息，请参阅 Dell 技术中心上提供的在 *Dell EMC 第 14 代及更高代别的 POWEREDGE 服务器上使用 iDRAC 管理汇总运行状况状态* 技术白皮书。
 - 单击以在[固件/驱动程序合规性](#)页面中查看更多信息。
 - 有关更新固件、创建固件目录、创建固件基线和生成基线合规性报告，请参阅[管理设备固件和驱动程序](#) 页面上的 64。
- **配置：**显示在 OpenManage Enterprise 上创建的配置合规性基线的汇总状态。如果可用，列出“严重”和“警告”配置基线。请参阅[管理合规性模板](#) 页面上的 91。
- **资源利用率：**显示设备的 CPU 和内存利用率。以下颜色编码检查用于指示各阶段的利用率：
 - 绿色 — 资源利用率低于 80%
 - 黄色 — 资源利用率超过 80% 但低于 95%
 - 红色 — 资源利用率超过 95%

注：总体资源利用率（显示为小部件左侧的颜色编码垂直条）是任何资源的最差情况汇总。


环形图

您可以在 OpenManage Enterprise 的不同部分查看环形图。环形图显示的输出取决于您在表格中所选的项目。环形图表示 OpenManage Enterprise 中的多种状态：

- 设备的运行状况：在仪表板页面上显示。环形图按比例分成不同的颜色，分别指示由 OpenManage Enterprise 监测的设备的运行状况。每种设备状态都用一个彩色符号表示。请参阅[设备运行状况状态](#) 页面上的 33。如果环形图指示该组中 279 个设备的运行状况，其中 131=严重、50=警告、95=正常，则该环由四个色带构成，每个分别代表这些数字所占的比例。
- **注：**单个设备的环形图由仅一个粗环构成，只使用一种颜色来表示设备的状态。例如，对于处于警告状态的设备，会显示黄色的圆圈。
- 设备的警报状态：表示为 OpenManage Enterprise 监测的设备生成的警报总数。请参阅[监视和管理设备警报](#) 页面上的 97。
 - **注：**环形图中的警报总数会根据是否设置为查看未确认的警报而有所不同。默认情况下，仅显示未确认警报。请参阅[自定义警报显示](#) 页面上的 138。
- 设备固件版本与目录版本的合规性：请参阅[管理设备固件和驱动程序](#) 页面上的 64。
- 设备和设备组的配置合规性基线：请参阅[管理设备配置合规性](#) 页面上的 91。
- **注：**所选设备的合规性级别由环形图表示。当多个设备与一个基线关联时，与基线合规性级别最差的设备的状态被指示为该基线的合规性级别。例如，如果有很多设备与一个固件基线关联，且少数设备的合规性级别为“良好”或“降级”，但如果该组中的一个设备的合规性为“降级”，固件基线的合规性级别指示为“升级”。汇总状态等于具有高严重性的设备的状态。有关“汇总运行状况”状态的更多信息，请参阅 Dell 技术中心上提供的 *MANAGING THE ROLLUP HEALTH STATUS BY USING iDRAC ON THE DELL EMC 14TH GENERATION AND LATER POWEREDGE SERVERS*（在 Dell EMC 第 14 代及更高代别的 POWEREDGE 服务器上使用 iDRAC 管理汇总运行状况状态）技术白皮书。
- **注：**单个设备的环形图由仅一个粗环构成，只使用一种颜色来表示设备固件合规性级别。例如，对于处于“严重”状态的设备，将显示一个红色的圆圈，表示必须更新设备固件。

设备运行状况状态

表. 12: OpenManage Enterprise 中的设备运行状况

运行状况	定义
严重 	表示设备或环境的重要方面出现故障。
警告 	设备即将发生故障。表示设备或环境的某些方面不正常。需要立即关注。
正常 	设备可以完全正常工作。
未知 	设备状态未知。

 **注:** 在仪表板中显示的数据视您在使用 OpenManage Enterprise 时的权限而定。有关用户的更多信息，请参阅[管理用户](#)。

查找要监测或管理的设备

通过单击 **OpenManage Enterprise > 监测 > 查找**，您可以在您的数据中心环境中查找设备，以针对您的业务关键型操作对其进行管理、提高其可用性和提高资源可用性。**查找**页面显示在任务中找到的设备数量，以及该设备的查找作业状态的相关信息。作业状态为“已排队”、“已完成”和“已停止”。右侧窗格中会显示关于任务的信息，例如可能的设备总数、通过设备类型查找的设备及其各自计数、下一次运行的时间（如已计划）以及最后一次查找的时间。右侧窗格中的**查看详细信息**会显示单个查找作业的详细信息。

注:

- 要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
- 为了支持使用域凭据的查找，OpenManage Enterprise 3.2 及更高版本将使用 OpenSSH 协议，而非以前版本中使用的 WSMAN 协议。因此，必须删除更新设备之前查找到的所有 Windows 和 Hyper-V 设备，并使用设备的 OpenSSH 凭据重新查找设备。请参阅 [Microsoft 说明文件](#)，以启用 Windows 和 Hyper-V 上的 OpenSSH。
- 在**查找和资源清册计划**页面上，计划作业的状态在**状态**列中被标识为**已排队**。但在**作业**页面上，同样的状态被标识为**已计划**。
- 默认情况下，OpenManage Enterprise 会使用最新查找到的设备的 IP 来执行所有操作。要让任何 IP 更改生效，您必须重新查找设备。
- 对于第三方设备，如果使用多个协议进行查找，则可能会看到重复条目。通过删除条目并仅使用 IPMI 协议重新查找设备，可以纠正此重复现象。

通过使用查找功能，您可以：

- 从全局排除列表中查看、添加和移除设备。请参阅[全局排除范围](#)页面上的 40。
- 创建、运行、编辑、删除和停止设备查找作业。

相关任务

- 删除设备查找作业 页面上的 44
- 查看设备查找作业详细信息 页面上的 39
- 停止设备查找作业 页面上的 40
- 运行设备查找作业 页面上的 39
- 为创建服务器查找作业指定查找模式 页面上的 41
- 创建服务器的自定义设备查找作业协议 - 查找协议的附加设置 页面上的 41
- 为创建戴尔存储设备查找作业指定查找模式 页面上的 43
- 为 SNMP 设备创建自定义设备查找作业模板 页面上的 44
- 为创建 MULTIPLE 协议查找作业指定查找模式 页面上的 44
- 编辑设备查找作业 页面上的 39

主题:

- [通过使用服务器启动的查找功能来自动查找服务器](#)
- [创建设备查找作业](#)
- [用于查找设备的协议支持值表](#)
- [查看设备查找作业详细信息](#)
- [编辑设备查找作业](#)
- [运行设备查找作业](#)
- [停止设备查找作业](#)
- [通过从 .csv 文件导入数据来指定多个设备](#)
- [全局排除范围](#)
- [为创建服务器查找作业指定查找模式](#)
- [创建服务器的自定义设备查找作业协议 - 查找协议的附加设置](#)
- [为创建机箱查找作业指定查找模式](#)

- [创建机箱的自定义设备查找作业协议 – 查找协议的附加设置](#)
- [为创建戴尔存储设备查找作业指定查找模式](#)
- [为创建网络交换机查找作业指定查找模式](#)
- [创建 HTTPS 存储设备的自定义设备查找作业协议 - 查找协议的附加设置](#)
- [为 SNMP 设备创建自定义设备查找作业模板](#)
- [为创建 MULTIPLE 协议查找作业指定查找模式](#)
- [删除设备查找作业](#)

通过使用服务器启动的查找功能来自动查找服务器

OpenManage Enterprise 允许自动查找具有 iDRAC 固件版本 4.00.00.00 或更高版本的服务器。可以将设备配置为允许这些服务器通过查询 DNS 来自动定位控制台并启动查找。

服务器启动的查找必须满足以下前提条件：

- 此功能仅适用于具有 iDRAC 固件版本 4.00.00.00 或更高版本的服务器。
- 服务器必须与 OpenManage Enterprise 位于同一域或子域中。
- OpenManage Enterprise 必须向 DNS 注册，才能使用 TUI 将配置信息添加到 DNS。较为理想的是 DNS 允许从 OpenManage Enterprise 自动更新。
- 应清除 DNS 上的应用装置控制台的旧记录（如果有），以避免来自服务器的多个通告。

注：基于范围的访问控制 (SBAC) 不影响 **监测 > 服务器启动的查找** 页面上的设备列表，并且设备管理者将在此页面上看到超出其范围的设备。

在 OpenManage Enterprise 中自动查找服务器时，请遵循以下步骤：

1. 使用以下方法之一在 DNS 上添加 OpenManage Enterprise 的配置信息：

- **TUI** — 通过 TUI 界面启用 **配置服务器启动的查找** 选项。有关更多信息，请参阅 [使用文本用户界面配置 OpenManage Enterprise](#) 页面上的 23。
- **手动** — 将以下四条记录添加到在设备上配置了接口的网络上的 DNS 服务器。确保将所有 <domain> 或 <subdomain.domain> 实例都替换为相应的 DNS 域和系统主机名。
 - <OME hostname>.<domain> 3600 A <OME IP address>
 - _dcimprovsrv._tcp.<domain> 3600 PTR ptr.dcimprovsrv._tcp.<domain>
 - ptr.dcimprovsrv._tcp.<domain> 3600 TXT URI=/api/DiscoveryConfigService/Actions/DiscoveryConfigService.SignalNodePresence
 - ptr.dcimprovsrv._tcp.<domain> 3600 SRV 0 0 443 <hostname>.<domain>

要在 Linux 中使用 nsupdate 创建记录，请使用以下命令：

- 要创建主机名记录

```
>update add omehost.example.com 3600 A XX.XX.XX.XX
```

- 要为服务器启动的查找添加记录

```
>update add _dcimprovsrv._tcp.example.com 3600 PTR ptr.dcimprovsrv._tcp.example.com.

>update add ptr.dcimprovsrv._tcp.example.com 3600 TXT URI=/api/DiscoveryConfigService/Actions/DiscoveryConfigService.SignalNodePresence

>update add ptr.dcimprovsrv._tcp.example.com 3600 SRV 0 0 443 omehost.example.com.
```

要在 Windows DNS 服务器上使用 dnscmd 创建记录，请使用以下命令：

- 要创建主机名记录

```
>dnscmd <DnsServer> /RecordAdd example.com omehost A XX.XX.XX.XX
```

- 要为服务器启动的查找添加记录

```
>dnscmd <DnsServer> /RecordAdd example.com _dcimprovsrv._tcp PTR ptr.dcimprovsrv._tcp.example.com

>dnscmd <DnsServer> /RecordAdd example.com ptr.dcimprovsrv._tcp TXT URI=/api/DiscoveryConfigService/Actions/DiscoveryConfigService.SignalNodePresence
```

```
>dnscmd <DnsServer> /RecordAdd example.com ptr.dcimprovsvr._tcp SRV 0 0 443  
omehost.example.com
```

2. 默认情况下，设备中的查找批准策略设置为自动，并将自动发现与控制台建立联系的服务器。要更改设置，请参阅 [管理控制台首选项](#) 页面上的 137。
3. 按照上述步骤中所述配置应用装置后，服务器可以通过查询 DNS 发起与 OpenManage Enterprise 的联系。在确保服务器的客户端证书由 Dell CA 签名后，应用装置会验证服务器。
注：如果服务器 IP 地址或 SSL 证书中存在任何更改，服务器将重新发起与 OpenManage Enterprise 的联系。
4. **监测 > 服务器启动的查找** 页面列出与控制台建立联系的服务器。此外，还列出了已在控制台中添加了其凭据但尚未发起联系的服务器。基于上述条件的服务器将显示以下状态：
 - 公布 — 服务器发起与控制台的联系，但是，服务器的凭据未添加到控制台。
 - 已添加凭据 — 在控制台中添加了服务器的凭据，但服务器未发起与控制台的联系。
 - 准备好查找 — 已添加服务器的凭据，并且服务器已发起联系。
注：设备每 10 分钟触发一次查找作业，以查找所有处于“准备好查找”状态的服务器。但是，如果设备中的查找批准策略设置为“手动”，则用户应该为每个服务器手动触发查找作业。有关更多信息，请访问 [管理控制台首选项](#) 页面上的 137
 - 已为查找提交作业 — 此状态表示已为服务器自动或手动启动查找作业。
 - 查找到 — 服务器已被查找到并在“所有设备”页面上列出。

可在**监测 > 服务器启动的查找**页面上执行以下任务：

1. **导入** — 要导入服务器凭据，请执行以下操作：
 - a. 单击**导入**。
 - b. 在“从文件导入”向导中，单击**上传服务编号文件**以导航并选择 .csv 文件。
要查看服务器凭据的样本 CSV 文件，请单击**下载样本 CSV 文件**。
 - c. 单击**完成**。
2. **发现** — 要手动查找“准备好查找”状态的服务器，请执行以下操作：
 - a. 选择“服务器启动的查找”页面上的“准备好查找”状态的服务器。
 - b. 单击**查找**。将触发查找作业以查找服务器，并在“所有设备”页面上列出这些服务器。
3. **删除** — 要删除“服务器启动的查找”页面上列出的服务器，请执行以下操作：
 - a. 在“服务器启动的查找”页面上选择已被查找到并列在“所有设备”页面上的服务器。
 - b. 单击**删除**。服务器将从“服务器启动的查找”页面中删除。
注：与查找到的服务器对应的条目在 30 天后自动清除。
4. **导出** — 要以 HTML、CSV 或 PDF 格式导出服务器凭据，请执行以下操作：
 - a. 在“服务器启动的查找”页面上选择一个或多个服务器。
 - b. 请单击**导出**。
 - c. 在“导出所有”向导中，选择以下输出格式中的任何一个：HTML、CSV 或 PDF。
 - d. 单击**完成**。将创建一个作业并将数据导出到所选位置。

创建设备查找作业

以下步骤介绍了如何在 OpenManage Enterprise 中启动设备查找作业，以使用“创建查找作业”向导查找数据中心内的设备。

- 注：**要对 OpenManage Enterprise 执行任何任务，您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
1. 要启动“创建查找作业”，您可以执行以下步骤之一：
 - 单击**监测 > 查找 > 创建**。
 - 或者，从“所有设备”页面（**OpenManage Enterprise > 设备**）中，单击**查找**下拉菜单并单击**查找设备**。
2. 在**创建查找作业**对话框中填入默认的作业名称。如需更改，请输入查找作业名称。
默认情况下，该对话框可让您一次定义类似设备的属性。

- 要将多个设备或范围添加到当前的查找作业，请单击**添加**。显示指定设备属性的另一组以下字段：类型、IP/主机名/范围和设置。

警告: 最多可以通过 OpenManage Enterprise 管理 8000 个设备。因此，请勿指定设备数超出 OpenManage Enterprise 所支持最大设备数的大型网络。否则可能会导致系统突然停止响应。

注: 在查找大量设备时，避免使用个别 IP 地址创建多个查找作业，应改用设备的 IP 范围。

- 从 .csv 文件中导入范围以查找设备。请参阅[通过从 .csv 文件导入数据来指定多个设备](#) 页面上的 40。
 - 要排除某些设备，移除已被排除的设备或查看从已被找到的结果中被排除的设备列表，请参阅[从查找结果中全局排除设备](#)。
3. 从**设备类型**下拉菜单中查找：
 - 服务器，选择**服务器**。请参阅[为创建服务器查找作业指定查找模式](#)。
 - 机箱，选择**机箱**。请参阅[为创建机箱查找作业指定查找模式](#)。
 - Dell EMC 存储设备或网络交换机，选择**Dell 存储或网络交换机**。请参阅[为创建存储、Dell 存储和网络交换机查找作业指定查找模式](#)。
 - 要使用多个协议查找设备，请选择**多个**。请参阅[为创建 MULTIPLE 协议查找作业指定查找模式](#) 页面上的 44。
 4. 在**IP/主机名/范围**框中，输入要查找或包含的 IP 地址、主机名或 IP 地址范围。有关您在该字段可以输入的数据的更多信息，请单击 **i** 符号。

注:

- 范围大小不得超过 16,385 (0x4001)。
- 也支持 IPv6 和 IPv6 CIDR 格式。

5. 在**设置**部分，输入用于查找范围的协议的用户名和密码。
6. 单击**附加设置**，选择不同的协议并更改设置。
7. 在**计划查找作业**部分，立即或计划以后运行作业。请参阅[计划作业字段定义](#) 页面上的 150。
8. 选择**启用查找 iDRAC 服务器和 MX7000 的陷阱接收**以便让 OpenManage Enterprise 接收来自查找到的服务器和 MX7000 机箱的传入陷阱。

注:

启用此设置将启用 iDRAC 上的警报（如果已禁用），并为 OpenManage Enterprise 服务器的 IP 地址设置警报目标。如果有需要启用的特定警报，则必须通过启用相应的警报文件管理器和 SNMP 陷阱来在 iDRAC 上配置它们。有关更多信息，请参阅 iDRAC 用户指南。

9. 选择**从应用程序设置中设置陷阱目标的团体字符串**。此选项仅适用于已查找到的 iDRAC 服务器和 MX7000 机箱。
10. 选择**完成时发送电子邮件**复选框，然后输入必须接收关于查找作业状态通知的电子邮件地址。如果未配置电子邮件，则会显示**转至 SMTP 设置**链接。单击该链接并配置 SMTP 设置。请参阅[配置 SMTP、SNMP 和 Syslog 警报](#) 页面上的 101。如果您选择此选项但不配置 SMTP，则不会显示**完成**按钮以继续执行任务。
11. 单击**完成**。如果字段填写不正确或未填写完整，则不会显示“完成”按钮。将会创建并运行查找作业。状态信息显示在**作业详细信息**页面上。

在设备查找过程中，将会针对在远程设备上启用的所有可用权限验证查找范围指定的用户帐户。如果用户身份验证通过，该设备会自动启用，或设备可以通过不同的用户凭据稍后启用。请参阅[启用设备](#) 页面上的 37。

注: 在 CMC 查找过程中，驻留在 CMC 上的服务器、IOM 和存储模块（将 IP 和设置为“公共”的 SNMP 配置为团体字符串）也会被找到和启用。如果您在 CMC 查找过程中启用陷阱接收，OpenManage Enterprise 会在所有服务器而不是机箱上被设置为陷阱目标。

注: 在 CMC 查找期间，不会查找可编程 MUX (PMUX) 模式下的 FN I/O 集合器。

启用设备

启用让服务器受管理，而不仅仅是受监测。

- 如果在查找期间提供管理员级别的凭据，则会启用服务器（在“所有设备”视图中，设备状态显示为“受管”）。
- 如果在查找期间提供较低级别权限的凭据，则不会启用服务器（在“所有设备”视图中，状态显示为“受监测”）。
- 如果控制台在服务器上也设置为陷阱接收器，那么其启用状态显示为“受警报管理”。
- **错误:** 表示在启用设备时出现问题。
- **代理:** 仅适用于 MX7000 机箱。表示设备通过 MX7000 机箱查找到（而不是直接查找）。

如果您想使用不同的用户帐户（不同于为查找指定的帐户）启用设备，或者因查找期间启用失败而要重试启用，请执行以下任务：

注:

- 已通过此向导启用的所有设备将保持通过此用户帐户启用的状态，在未来查找这些设备时，不会被查找用户帐户替代。

- 对于已查找到的设备，如果 SNMP 陷阱目标在 iDRAC 中“手动”设置为 OpenManage Enterprise，则设备将接收并处理警报。但是，设备在“所有设备”页面上显示的受管状态与其初始查找状态保持一致，即“受监测”、“受管”或“带警报的受管”。
- “所有设备”页面将所有已启用机箱的托管状态显示为“受管”，与在启用时使用的机箱用户角色凭据无关。如果机箱使用“只读”用户的凭据进行启用，则在机箱上执行的更新活动期间可能会出现故障。因此，建议使用机箱管理员的凭据来启用机箱以执行所有活动。
- 要对 OpenManage Enterprise 执行任何任务，您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

1. 在 **OpenManage Enterprise** 菜单的**设备**下面，单击**所有设备**。

环形图表示工作窗格中所有设备的状态。请参阅[环形图](#)。该表列出了所选设备的属性及其以下启用状态：

- **错误**：设备无法启用。尝试使用建议的权限登录。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
- **受管**：设备成功启用，并可通过 OpenManage Enterprise 控制台进行管理。
- **受监测**：设备没有管理选项（例如使用 SNMP 查找到的）。
- **带警报的受管**：设备已成功启用，并且 OpenManage Enterprise 控制台已在发现期间成功注册设备的 IP 地址，将其作为陷阱目标。

2. 在工作窗格中，选择与设备对应的复选框，单击**更多操作 > 启用**。

确保从所有设备页只选择支持启用的设备类型。您可在表格中搜索合适的设备，方式是单击**高级筛选器**，然后在筛选器框中选择或输入启用状态数据。

注：不支持启用已查找到的所有设备，仅支持 iDRAC 和 CMC 查找到的所有设备。确保您为支持的设备类型选择启用选项。

3. 在**启用**对话框中，输入 WS-Man 凭据 — 用户名和密码。

4. 在**连接设置**部分：

- 在**重试**框中，输入查找服务器必须重复尝试的次数。
- 在**超时**框中输入一个时间，在此时间之后作业必须停止运行。
注：如果输入的超时代数大于当前会话已过期时间，则您会自动注销 OpenManage Enterprise。但是，如果该值在当前会话过期超时段内，则会话会续而不会注销。
- 在**端口**框中，输入查找服务器必须使用的端口号。
- 可选字段。选择**启用常用名 (CN) 检查**。
- 可选字段。选择**启用证书颁发机构 (CA) 检查**并浏览到认证文件。

5. 单击**完成**。

注：启用从找到的接收陷阱复选框仅对使用 iDRAC 接口查找的服务器有效。该选择对其他服务器（例如使用操作系统查找功能找到的那些设备）无效。

用于查找设备的协议支持值表

下表提供用于查找设备的支持协议有关的信息。

注：所支持的协议查找、监测和管理附带 iDRAC6 的 PowerEdge YX1X 服务器的功能有限。有关详情，请参阅 [Dell EMC PowerEdge 服务器的通用命名惯例](#) 页面上的 154。

表. 13: 用于查找的协议支持值表

设备/操作系统	协议						
	Web Services-Management (WS-Man)	Redfish	简单网络管理协议 (SNMP)	Secure Shell (SSH)	智能平台管理接口 (IPMI)	ESXi (VMWare)	HTTPS
iDRAC6 和更高版本	支持	支持 仅适用于 iDRAC9 版本 4.40.10.00 及更高版本	不支持	不支持	不支持	不支持	不支持
		不支持					

表. 13: 用于查找的协议支持值表 (续)

设备/操作系统	协议						
	Web Services-Management (WS-Man)	Redfish	简单网络管理协议 (SNMP)	Secure Shell (SSH)	智能平台管理接口 (IPMI)	ESXi (VMWare)	HTTPS
PowerEdge C*	支持	不支持	不支持	不支持	不支持	不支持	不支持
PowerEdge 机箱 (CMC)	支持	不支持	不支持	不支持	不支持	不支持	不支持
PowerEdge MX7000 机箱	不支持	支持	不支持	不支持	不支持	不支持	不支持
存储设备	不支持	不支持	支持	不支持	不支持	不支持	不支持
以太网交换机	不支持	不支持	支持	不支持	不支持	不支持	不支持
ESXi	不支持	不支持	不支持	不支持	不支持	支持	不支持
Linux	不支持	不支持	不支持	支持	不支持	不支持	不支持
Windows	不支持	不支持	不支持	支持	不支持	不支持	不支持
Hyper-V	不支持	不支持	不支持	支持	不支持	不支持	不支持
非 Dell 服务器	不支持	不支持	不支持	不支持	支持	不支持	不支持
PowerVault ME	不支持	不支持	不支持	不支持	支持	不支持	支持

查看设备查找作业详细信息

1. 单击**监测 > 查找**。
2. 选择与查找作业名称对应的行，然后在右侧窗格中单击**查看详细信息**。
作业详细信息页面显示各自的查找作业信息。
3. 有关管理作业的更多信息，请参阅[使用作业进行设备控制](#) 页面上的 106。

相关信息

[查找要监测或管理的设备](#) 页面上的 34

编辑设备查找作业


您一次只能编辑一个设备查找作业。

1. 选择与您要编辑的查找作业对应的复选框，然后单击**编辑**。
2. 在**创建查找作业**对话框中，编辑属性。
有关此对话框中要执行的任务的信息，请参阅[创建设备查找作业](#)。

相关信息

[查找要监测或管理的设备](#) 页面上的 34

运行设备查找作业

 **注:** 您无法重新运行已在运行的作业。

运行设备查找作业:

1. 在现有设备查找作业列表中，选择与您要立即运行的作业对应的复选框。
2. 单击**运行**。
作业将会立即运行，右下角将会显示一条消息。

相关信息

[查找要监测或管理的设备](#) 页面上的 34

停止设备查找作业

您只能停止正在运行的作业。已完成或失败的查找作业无法停止。停止作业：

1. 在现有查找作业列表中，选择与您要停止的作业对应的复选框。

i | **注：**无法一次停止多个作业。

2. 单击**停止**。
作业停止，右下角将会显示一条消息。

相关信息

[查找要监测或管理的设备](#) 页面上的 34

通过从 .csv 文件导入数据来指定多个设备

1. 在**创建查找作业**对话框中，默认情况下查找作业名称填写在**查找作业名称**。如需更改，请键入查找作业名称。
2. 单击**导入**。

i | **注：**下载示例 .CSV 文件（如有必要）。

3. 在**导入**对话框中，单击**导入**，浏览到包含无效范围列表的 .CSV 文件，然后单击**确定**。

i | **注：**如果 .CSV 文件中包含无效范围，且在导入过程中排除了重复范围，则会显示一条错误消息。

全局排除范围

使用“全局排除范围”向导，您可以输入必须从 OpenManage Enterprise 监测和管理活动中排除的设备的地址或范围。以下步骤介绍了如何排除设备范围：

i | **注：**要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。
请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

i | **注：**目前，您无法通过主机名排除设备，仅可通过其 IP 地址或 FQDN 排除设备。

1. 要激活“全局排除范围”向导，可以执行以下操作之一：
 - 从“所有设备”页面（**OpenManage Enterprise > 设备**）的**查找**下拉菜单中，单击**编辑排除范围**。
 - 从**监测 > 查找**中，单击右上角的**全局排除列表**。
2. 在**全局排除范围**对话框中：
 - a. 在**排除范围说明**框中，输入关于排除范围的信息。
 - b. 在**输入排除范围**框中，输入要排除的地址或设备范围。该框一次最多可容纳 1000 个地址项目，但可通过换行符分隔。这意味着，每个排除范围必须输在框内的不同行中。
可被排除的范围与查找设备时适用的受支持的范围相同。请参阅[创建设备查找作业](#) 页面上的 36。

i | **注：**

- 范围大小不得超过 16,385 (0x4001)。
- 也支持 IPv6 和 IPv6 CIDR 格式。

3. 单击**添加**。

4. 显示提示时，单击**是**。
全局排除 IP 地址或范围，并将其显示在排除范围中。全局排除这些设备意味着它们将不再参与 OpenManage Enterprise 执行的任何活动。

注：全局排除的设备会在**作业详细信息**页面上清晰地标识为“全局排除”。

要从全局排除列表中删除设备，请执行以下操作：

- a. 选择此复选框并单击**从排除中删除**。
- b. 显示提示时，单击**是**。该设备已从全局排除列表中删除。但是，从全局排除列表中删除的设备不受 OpenManage Enterprise 自动监测。您必须查找设备以便 OpenManage Enterprise 启动监测。

注：

- 将控制台已知的设备（即控制台查找的设备）添加到全局排除列表中会将该设备从 OpenManage Enterprise 中删除。
- “全局排除列表”中新包括的设备将继续在“所有设备”网格中显示，直至下一个查找周期为止。为避免在此类设备上执行任务，强烈建议用户通过选中与设备对应的复选框，然后单击**排除**以从“所有设备”页面中手动排除这些设备。
- 全局排除列表中列出的设备将从控制台的所有任务中排除。如果设备的 IP 在全局排除列表中，在创建查找作业中查找范围包含该 IP，则该设备没有查找到。但是，在创建查找任务时，控制台上不会显示任何错误提示。如果您认为某个设备必须被查找却没有查找，那么您必须检查全局排除列表以查看该设备是否已包含在全局排除列表中。

为创建服务器查找作业指定查找模式

1. 从**设备类型**下拉菜单中选择**服务器**。
2. 当出现提示时，可选择：
 - **Dell iDRAC**：通过使用 iDRAC 查找。
 - **主机操作系统**：通过使用 VMware ESXi、Microsoft Windows Hyper-V 或 Linux 操作系统查找。
 - **非 Dell 服务器（通过 OOB）**：通过使用 IPMI 来查找第三方服务器。
3. 单击**确定**。
根据您的选择，**设置**下的字段将更改。
4. 在**IP/主机名/范围**中输入与协议相关的 IP 地址、主机名或 IP 范围。
5. 在**设置**下，输入要查找的服务器的用户名和密码。
6. 要通过单击**附加设置**自定义查找协议，请参阅 [Creating customized device discovery job template for servers](#)（为服务器创建自定义设备查找作业模板）。
7. 计划查找作业。请参阅[计划作业字段定义](#) 页面上的 150。
8. 单击**完成**。
查找作业即会创建并显示在查找作业列表中。

相关信息

[查找要监测或管理的设备](#) 页面上的 34

创建服务器的自定义设备查找作业协议 - 查找协议的附加设置

在**附加设置**对话框中，输入要用来查找服务器的适当协议的详细信息：

注：系统将根据初始输入自动预先选择相应协议。

1. **使用 WS-Man/Redfish (iDRAC、服务器和/或机箱) 查找**
 - a. 在“凭据”部分，输入**用户名和密码**。
 - b. 在**连接设置**部分：
 - 在**重试**框中，输入查找服务器必须重复尝试的次数。
 - 在**超时**框中输入一个时间，在此时间之后作业必须停止运行。
 - 在**端口**框中输入以编辑端口号。默认情况下，443 用于连接设备。有关支持的端口号，请参阅 [OpenManage Enterprise 中支持的协议和端口](#) 页面上的 26

- 如果设备的常用名与用于访问 OpenManage Enterprise 的主机名相同，则选择**启用常用名 (CN)** 复选框。
 - 如果需要，请选择**启用证书颁发机构 (CA)** 复选框。
2. **使用 IPMI (通过带外管理的非戴尔接口) 查找**
 - a. 在“凭据”部分，输入**用户名和密码**。
 - b. 在**连接设置**部分：
 - 在**重试**框中，输入查找服务器必须重复尝试的次数。
 - 在**超时**框中输入一个时间，在此时间之后作业必须停止运行。
 - 在**KgKey**框中，输入相应的值。
 3. **使用 SSH (Linux、Windows、Hyper-V) 查找**

i 注：仅支持 Windows 和 Hyper-V 上的 OpenSSH。Cygwin SSH 不受支持。

 - a. 在“凭据”部分，输入**用户名和密码**。
 - b. 在**连接设置**部分：
 - 在**重试**框中，输入查找服务器必须重复尝试的次数。
 - 在**超时**框中输入一个时间，在此时间之后作业必须停止运行。
 - 在**端口**框中输入以编辑端口号。默认情况下，22 用于连接设备。有关支持的端口号，请参阅 [OpenManage Enterprise 中支持的协议和端口](#) 页面上的 26
 - 选中**验证已知主机密钥**复选框，以根据已知的主机密钥验证主机。

i 注：已知的主机密钥通过 /DeviceService/HostKeys REST API 服务进行添加。有关如何管理主机密钥的更多信息，请参阅《[OpenManage Enterprise RESTful API 指南](#)》。
 - 如果首选 sudo 帐户，请选中**使用 SUDO 选项**复选框。

i 注：要使 sudo 帐户正常工作，必须配置服务器 /etc/sudoer 文件以使用 NOPASSWD。
 4. **使用 ESXi (VMware) 查找**
 - a. 在“凭据”部分，输入**用户名和密码**。
 - b. 在**连接设置**部分：
 - 在**重试**框中，输入查找服务器必须重复尝试的次数。
 - 在**超时**框中输入一个时间，在此时间之后作业必须停止运行。
 - 在**端口**框中输入以编辑端口号。默认情况下，443 用于连接设备。有关支持的端口号，请参阅 [OpenManage Enterprise 中支持的协议和端口](#) 页面上的 26
 - 如果设备的常用名与用于访问 OpenManage Enterprise 的主机名相同，则选择**启用常用名 (CN)** 复选框。
 - 如果需要，请选择**启用证书颁发机构 (CA)** 复选框。

相关信息

[查找要监测或管理的设备](#) 页面上的 34

为创建机箱查找作业指定查找模式

1. 从**设备类型**下拉菜单中，选择**机箱**。
根据您的选择，**设置**下的字段将更改。
 2. 在**IP/主机名/范围**中输入 IP 地址、主机名或 IP 范围。
 3. 在**设置**下，输入要检测的服务器的用户名和密码。
 4. 键入社区类型。
 5. 要通过单击**附加设置**创建自定义查找模板，请参阅[创建机箱的自定义设备查找作业协议 – 查找协议的附加设置](#) 页面上的 42。
- i** 注：目前，对于找到的任何 M1000e 机箱，硬件日志下时间戳列的日期在 CMC 5.1x 和更早的版本中显示为 2013 年 1 月 12 日。但在 CMC VRTX 和 FX2 机箱的所有版本中将显示正确的日期。
- i** 注：单独查找到机箱中的服务器时，有关服务器的插槽信息不显示在**机箱信息**部分中。不过，通过机箱查找到时，将会显示插槽信息。例如，MX7000 机箱中的 MX740c 服务器。

创建机箱的自定义设备查找作业协议 – 查找协议的附加设置

在**附加设置**对话框中：

1. 选择使用 **WS-Man/Redfish (iDRAC、服务器和/或机箱) 查找**。

注：对于机箱，使用 **WS-Man/Redfish 查找** 复选框默认处于选中状态。表示可通过这两种协议中的任意一种查找到机箱。M1000e、CMC VRTX 和 FX2 机箱支持 WS-Man 命令。MX7000 机箱支持 Redfish 协议。

2. 输入要检测的机箱的用户名和密码。

3. 在**连接设置**部分：

- a. 在**重试**框中，输入查找服务器必须重复尝试的次数。
- b. 在**超时**框中输入一个时间，在此时间之后作业必须停止运行。
- c. 在**端口**框中输入以编辑端口号。默认情况下，443 用于连接设备。关于支持的端口号，请参阅 [OpenManage Enterprise 中支持的协议和端口](#) 页面上的 26。
- d. 如果设备的常用名与用于访问 OpenManage Enterprise 的主机名相同，则选择**启用常用名 (CN) 检查**复选框。
- e. 选择**启用证书颁发机构 (CA) 检查**复选框。

4. 要查找 IO 模块，请选中**查找 IO 模块与机箱**复选框。

注：仅适用于 CMC VRTX、M1000e 和 FX2 机箱（型号 FN2210S、FN410T 和 FN410S）。对于 MX7000 机箱，IO 模块为自动检测。

注：仅在带有独立、PMUX（可编程 MUX）、VLT（虚拟链路主干聚合）模式的 IO 模块可查找。无法查找到完整的交换机和堆栈叠模式。

- a. 如果 M I/O 聚合器用户凭据与机箱凭据相同，则选择**使用机箱凭据**。
- b. 如果 M I/O 聚合器用户凭据与机箱凭据不同，请选择**使用不同的凭据**，并执行以下操作：

- 输入**用户名和密码**。
- 更改**重试次数、超时和端口**的默认值（如果需要）。
- 选中**验证已知主机密钥**，以根据已知的主机密钥验证主机。

注：已知的主机密钥通过 /DeviceService/HostKeys REST API 服务进行添加。有关如何管理主机密钥的更多信息，请参阅《[OpenManage Enterprise RESTful API 指南](#)》。

- 选择 **使用 SUDO 选项**（如果需要）。

5. 单击**完成**。

6. 完成 [创建设备查找作业](#) 页面上的 36 中的任务。

为创建戴尔存储设备查找作业指定查找模式

1. 从**设备类型** 下拉菜单中选择**戴尔存储设备**。

2. 当出现提示时，可选择：

- PowerVault ME：查找使用 HTTPS 协议的存储设备（如 PowerVault ME）。
- 其他：查找使用 SNMP 协议的存储设备。

根据您的选择，**设置**下的字段将更改。

3. 在 **IP/主机名/范围** 中输入 IP 地址、主机名或 IP 范围。

4. 在**设置**下，根据您的初始选择 — 对于存储 HTTPS，输入**用户名**和**密码**，或输入要检测设备的 **SNMP 版本**和**团体类型**。

5. 单击**其他设置**，自定义相应的查找协议。请参阅为 [SNMP 设备创建自定义设备查找作业模板](#) 或参阅[创建 HTTPS 存储设备的自定义设备查找作业协议 - 查找协议的附加设置](#) 页面上的 44。

6. 完成 [创建设备查找作业](#) 页面上的 36 中的任务。

相关信息

[查找要监测或管理的设备](#) 页面上的 34

为创建网络交换机查找作业指定查找模式

1. 从**设备类型** 下拉菜单中选择**网络交换机**。

2. 在 **IP/主机名/范围** 中输入 IP 地址、主机名或 IP 范围。

3. 在**设置**下，输入要检测的设备的 **SNMP 版本**和**团体类型**。

4. 单击**其他设置**，自定义相应的查找协议。请参阅为 [SNMP 设备创建自定义设备查找作业模板](#)

5. 完成 [创建设备查找作业](#) 页面上的 36 中的任务。

创建 HTTPS 存储设备的自定义设备查找作业协议 - 查找协议的附加设置

在**附加设置**对话框中：

1. 输入要检测的 PowerVault ME 的用户名和密码。
2. 在**连接设置**部分：
 - a. 在**重试**框中，输入查找服务器必须重复尝试的次数。
 - b. 在**超时**框中输入一个时间，在此时间之后作业必须停止运行。
 - c. 在**端口**框中输入以编辑端口号。默认情况下，443 用于连接设备。关于支持的端口号，请参阅 [OpenManage Enterprise 中支持的协议和端口](#) 页面上的 26。
 - d. 如果设备的常用名与用于访问 OpenManage Enterprise 的主机名相同，则选择**启用常用名 (CN) 检查**复选框。
 - e. 选择**启用证书颁发机构 (CA) 检查**复选框。
3. 单击**完成**。
4. 完成 [创建设备查找作业](#) 页面上的 36 中的任务。

为 SNMP 设备创建自定义设备查找作业模板

默认情况下，选择**使用 SNMP 查找**复选框以让您检测存储、网络或其他 SNMP 设备。

注：仅在带有独立、PMUX（可编程 MUX）、VLT（虚拟链路主干聚合）模式的 IO 模块可查找。无法查找到完整的交换机和堆栈叠模式。

1. 在**凭据**下，选择 SNMP 版本，然后输入社区类型。
2. 在**连接设置**部分：
 - a. 在**重试**框中，输入查找服务器必须重复尝试的次数。
 - b. 在**超时**框中输入一个时间，在此时间之后作业必须停止运行。
 - c. 在**端口**框中，输入查找服务器必须使用的端口号。

注：目前，**重试**框和**超时**框中的设置对 SNMP 设备的查找作业没有任何功能影响。因此，可以忽略这些设置。

3. 单击**完成**。
4. 完成 [创建设备查找作业](#) 页面上的 36 中的任务。

相关信息

[查找要监测或管理的设备](#) 页面上的 34

为创建 MULTIPLE 协议查找作业指定查找模式

1. 从**类型**下拉菜单中选择 **MULTIPLE**，使用多个协议查找设备。
2. 在 **IP/主机名/范围**中输入 IP 地址、主机名或 IP 范围。
3. 要通过单击**附加设置**创建自定义查找模板，请参阅[创建服务器的自定义设备查找作业协议 - 查找协议的附加设置](#) 页面上的 41。

相关信息


[查找要监测或管理的设备](#) 页面上的 34


删除设备查找作业

注：即使设备上有正在运行的任务也可以删除该设备。如果在完成之前设备已被删除，则在设备上启动任务失败。

要删除设备查找作业：

1. 选择与您要删除的查找作业对应的复选框，然后单击**删除**。
2. 当提示显示是否必须删除选定的作业时，请单击**是**。
删除查找作业，屏幕右下角会显示一条消息。

 **注：**如果删除查找作业，与该作业关联的设备不会被删除。如果您想要从控制台中删除查找作业所查找的设备，请从**所有设备**页面中将其删除。

 **注：**无法从**作业**页面中删除设备查找作业。

相关信息

[查找要监测或管理的设备](#) 页面上的 34

管理设备和设备组

通过单击 **OpenManage Enterprise > 设备**，您可以查看和管理 OpenManage Enterprise 中查找到的设备组和设备。如果您以设备管理者的身份登录，则只能查看和管理您范围内的设备组及其关联树。

左侧窗格显示设备组，如下所示：

- 所有设备 — 包含所有组的顶层根组。
- 系统组 — 由 OpenManage Enterprise 在发运时创建的默认组。
- 自定义组 — 由用户（例如管理员和设备管理者）创建的组。您可以在“自定义组”下创建“查询”组或“静态”组。
- 插件组 — 由插件创建的组。

您可以在这些父组下创建子组。有关更多信息，请参阅[设备组](#)。

在工作窗格顶部，环形图默认显示所有设备的运行状况和警报。但是，当在左侧窗格中选择组时，这些环形图将显示所选组的运行状况和警报。此外，如果安装了插件，则第三个环形图可能会显示所安装插件的数据。有关环形图的更多信息，请参阅[环形图](#)。

环形图后面的表格列出了设备，并显示其运行状况、电源状态、名称、IP 地址和标识符。默认情况下，会列出所有设备，但在左侧窗格中选择组时，仅显示该组的设备。有关设备列表的更多信息，请参阅[设备列表](#)。

高级筛选器可用于根据运行状况、电源状态、连接状态、名称、IP 地址、标识符、设备类型、托管状态等进一步缩小显示在“设备列表”中的设备。

当您在列表中选择设备，右侧窗格将显示关于所选设备的预览。当选择多个设备，将显示关于最后一个所选设备的预览。在**快速操作**下，将会列出关联到各自设备的管理链接。要清除选择，单击**清除选择**。

注：

- 将 OpenManage Enterprise 升级至最新版本后，将在重新运行查找作业后更新设备列表。
- 您在每个页面最多可以选择 25 个设备，并导航各页面以选择更多设备并执行任务。
- 您可以在“所有设备”页面上执行的某些与设备相关的任务，如固件更新、资源清册刷新、状态刷新、服务器控制操作，也可在相应[设备详细信息](#)页面中对各个设备执行。

主题：

- [将设备按组整理](#)
- [“所有设备”页面 — 设备列表](#)
- [“所有设备”页面 — 设备列表操作](#)
- [查看和配置各个设备](#)

将设备按组整理

在数据中心的，为实现高效快速的设备管理，您可以：

- 将设备分组。例如，您可以根据功能、操作系统、用户配置文件、位置、运行的作业，然后运行查询来将设备分组，方便管理设备。
- 在管理设备、更新固件、查找设备和管理警报策略和报告时筛选与设备相关的数据。
- 可以管理组中的设备的属性。请参阅[查看和配置各个设备](#) 页面上的 56。

OpenManage Enterprise 提供一份内置报告以获得受 OpenManage Enterprise 监测的设备概述。单击 **OpenManage Enterprise > 监测 > 报告 > 设备概述报告**。单击**运行**。请参阅[运行报告](#) 页面上的 116。

- 注：**要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

要查看与所选设备或组有关的仪表板数据，请从**设备组**下拉菜单中选择。

- 注：**相应的符号表示设备或组的运行状况。组的运行状况就是组中运行状况最严重的设备的运行状况。例如，在组的众多设备中，如果某个服务器的运行状况是“警告”，则组的运行状况也是“警告”。汇总状态等于具有高严重性的设备的状态。有关“汇总运行状况”状态的更多信息，请参阅 Dell 技术中心上提供的在 *Dell EMC 第 14 代及更高代别的 POWEREDGE 服务器上使用 iDRAC 管理汇总运行状况状态* 技术白皮书。

组可以具有父组和子组。组不能将它的父组用作它的子组。默认情况下，OpenManage Enterprise 随以下内置组提供。

系统组：由 OpenManage Enterprise 创建的默认组。您不能编辑或删除“系统组”，但可以基于用户权限查看。“系统组”的示例：

- **HCI 设备：**超融合设备，例如 VxRAIL 和 Dell EMC XC 系列设备
- **虚拟机管理程序系统：**Hyper-V 服务器和 VMware ESXi 服务器
- **模块化系统：**PowerEdge 机箱、PowerEdge FX2、PowerEdge 1000e 机箱、PowerEdge MX7000 机箱和 PowerEdge VRTX 机箱。
 - ① **注：**MX7000 机箱可以是主机箱、独立机箱或成员机箱。如果 MX7000 机箱是主机箱并有一个成员机箱，则后者将通过其主机箱的 IP 查找。MX7000 机箱使用以下语法之一进行标识：
 - **MCM 组** — 表示具有多个使用以下语法标识的机箱的多机箱管理 (MCM) 组：Group_<MCM group name>_<Lead_Chassis_Svctag>，其中：
 - <MCM group name>：MCM 组的名称
 - <Lead_Chassis_Svctag>：主机箱的服务标签。机箱、底座和网络 IOM 组成此组。
 - **独立机箱组** — 使用 <Chassis_Svctag> 语法进行标识。机箱、底座和网络 IOM 组成此组。
- **网络设备：**Dell Force10 网络交换机和光纤信道交换机
- **服务器：**Dell iDRAC 服务器、Linux 服务器、非 Dell 服务器、OEM 服务器和 Windows 服务器。
- **存储设备：**Dell Compellent 存储阵列、PowerVault MD 存储阵列和 PowerVault ME 存储阵列
- **查找组：**映射到查找任务范围的组。不能编辑或删除，因为该组受查找作业控制，查找作业中应用了包括/排除条件。请参阅[查找要监测或管理的设备](#) 页面上的 34。

① **注：**要展开组中的所有子组，右键单击组，然后单击**全部展开**。

自定义组：由管理员创建以满足特定需要。例如，对托管电子邮件服务的服务器分组。基于用户权限和组类型，用户可以查看、编辑和删除。

- **静态组：**由用户通过添加特定设备至组以手动创建。这些组仅在用户在组或子组中手动更改设备时才会更改。组中的项目将保持静态，直到编辑了父组或删除了子设备为止。
- **查询组：**通过匹配用户指定的条件动态定义的组。组中设备会根据使用条件查找到的设备的结果而发生变化。例如，运行一个查询以查找分配给财务部门的服务器。但是，“查询组”具有不含任何层次的平面结构。

① **注：**静态组和查询组：

- 不能有多个父组。这意味着不能将一个组作为子组添加在其父组下面。
- 当对静态组（添加或删除设备）或查询组（更新查询）进行更改时，与这些组关联的设备的固件/驱动程序合规性不会自动刷新。建议用户为此类实例中新添加/删除的设备启动固件和/或驱动程序合规性。

① **注：**在设备层次中创建更多自定义（查询）组会影响 OpenManage Enterprise 的整体性能。为了取得优化的性能，OpenManage Enterprise 每隔 10 秒捕获一次汇总运行状况 - 具有较多的“动态组”会影响此性能。

在**所有设备**页面上，在左侧窗格中，您可以在“静态组”和“查询组”父组下创建子组。请参阅[创建静态设备组](#) 页面上的 48 和[创建查询设备组](#) 页面上的 48。

① **注：**要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅[OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

要删除“静态组”或“查询组”的子组，请执行以下操作：

1. 右键单击“静态组”或“查询组”，然后单击**删除**。
2. 显示提示时，单击**是**。即会删除该组，并会更新组下面的列表。

插件组：安装 Support Assist Enterprise、Power Manager 等插件时将创建插件组。插件在安装后将具有自己的系统组，并且某些插件（例如 Power Manager 插件）允许用户在其下创建自定义组。

相关任务

从 [OpenManage Enterprise 删除设备](#) 页面上的 53

刷新单个设备的设备资源清册 页面上的 60

刷新设备组的设备运行状况 页面上的 54

创建自定义组（静态或查询）

在 **OpenManage Enterprise > 设备**（“所有设备”页面）中，您可以使用“创建自定义组”向导创建静态或查询组。

要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅[OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14


1. 要激活“创建自定义组”向导，您可以执行以下操作：
 - 在 **OpenManage Enterprise > 设备** 左侧窗格“自定义组”中，右键单击或单击三个点垂直菜单，然后单击**创建自定义组**。
 - 从“所有设备”页面的**组操作**下拉菜单中，单击**创建自定义组**。
2. 在“创建自定义组”向导中，选择以下某个自定义组：
 - a. **静态组**。
 - b. **查询组**
3. 单击**创建**。
根据您的选择（静态或查询），将激活**创建静态组向导**或**创建查询组向导**。

创建（静态或查询）组后，它会在“自定义组”的“静态”或“查询”组下面列出。

创建静态设备组

在“所有设备”页面（**OpenManage Enterprise > 设备**）上，您可以使用“创建静态组”向导创建静态组。静态组中的设备将保持静态，直到添加或删除组中的设备。


要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

1. 要激活“创建静态组”向导，请执行以下操作之一：
 - 在“自定义组”的**静态组**下，右键单击或单击三个垂直点菜单，然后单击**创建新静态组**。
 - 单击**组操作 > 创建自定义组 > 静态组**。
2. 在**创建静态组向导**对话框中，输入组的“名称”和“说明”（可选），然后选择必须在其下创建新静态组的父组。
 **注：**静态或动态组名称以及与服务器配置相关的名称在 OpenManage Enterprise 中必须是唯一的（不区分大小写）。例如，不能同时使用 *name1* 和 *Name1*。
3. 单击**下一步**。
4. 从“组成员选择”对话框中，选择必须包含在静态组中的设备。
5. 单击**完成**。

静态组已创建并在左侧窗格中列在父组下面。子组从其父组继承而来。

创建查询设备组

查询组是通过匹配一些用户指定条件来定义设备的动态组。组中设备会根据使用查询条件查找到的设备的结果而发生变化。在“所有设备”页面（**OpenManage Enterprise > 设备**）上，您可以使用“创建查询组”向导创建查询组。

 **注：**要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

1. 要激活“创建查询组”向导，可以执行以下操作之一：
 - 在“自定义组”下，右键单击**查询组**或单击查询组旁边的三个点垂直菜单，然后单击**创建新查询组**。
 - 单击**组操作 > 创建自定义组 > 查询组**。
2. 在**创建查询组向导**对话框中，输入组的**名称和说明**（可选）。
3. 单击**下一步**。
4. 在**查询条件选择**对话框中，从**选择要复制的现有查询**下拉菜单中选择查询，然后选择其他筛选条件。请参阅[选择查询条件](#) 页面上的 48。
5. 单击**完成**。
查询组已创建并在左侧窗格中列在“查询组”部分下面。

选择查询条件

创建查询条件时定义筛选条件：

- 生成自定义报告。请参阅[创建报告](#) 页面上的 117。
- 在自定义组下创建基于查询的设备组。请参阅[创建查询设备组](#) 页面上的 48。

使用两个选项定义查询条件：

- **选择现有查询以复制：**默认情况下，OpenManage Enterprise 提供一份您可以复制并构建您自己的查询条件的内置查询列表。定义查询时，最多可以使用 6 个条件（筛选条件）。要添加筛选条件，您必须从**选择类型**下拉菜单中选择。

- **选择类型**：使用下拉菜单列出的属性从头构建查询条件。菜单中的项目取决于受 OpenManage Enterprise 监测的设备。选择查询类型后，根据查询类型，仅显示相应的运算符，例如 =、>、< 和 null。建议使用此方法定义构建的自定义报告中的查询条件。

注：当评估具有多个条件的查询时，评估的顺序与 SQL 相同。要指定条件评估的特定顺序，请在定义查询时添加或删除括号。

注：选中后，只是以虚拟方式复制现有查询的筛选条件来构建新的查询条件。与现有查询条件关联的默认筛选条件将不更改。内置查询条件的定义（筛选条件）将用作构建自定义查询的起点。例如：

1. *查询1* 是一个内置查询条件，具有以下预定义的筛选条件：Task Enabled=Yes。
2. 复制 *查询1* 的筛选条件属性，创建 *查询2*，然后通过添加以下筛选条件自定义查询条件：Task Enabled=Yes 和 (Task Type=Discovery)。
3. 接下来，请打开 *查询1*。它的筛选条件仍为 Task Enabled=Yes。

1. 在**查询条件选择**对话框中，请基于您是否想要创建查询条件用于查询组或生成报告而从下拉菜单中选择。
2. 通过分别单击加号或垃圾箱符号添加或删除一个筛选条件。
3. 单击**完成**。
查询条件生成并保存在现有查询列表中。生成审计日志条目并让其显示在审计日志列表中。请参阅[监视审核日志](#) 页面上的 104。

相关信息

[管理设备配置合规性](#) 页面上的 91

[编辑配置合规性基线](#) 页面上的 94

[移除配置合规性基线](#) 页面上的 96

编辑静态组

在“所有设备”页面（OpenManage Enterprise > 设备）上，可以重命名或重新定位现有静态组，并且可以使用“编辑静态组”向导添加或删除静态组中的设备。

注：要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

1. 右键单击静态组或单击静态组旁边的三个垂直点菜单，然后单击**编辑**以激活“编辑静态组”向导。
2. 在“编辑静态组”向导中，您可以编辑“名称”、“说明”和“父组”。
3. 单击**下一步**。
4. 在“组成员选择”屏幕中，您可以选中或取消选中设备以在静态组中包含或排除它们。
5. 单击**完成**。

对静态组所做的更改已实施。

编辑查询组

在“所有设备”页面（OpenManage Enterprise > 所有设备）中，可以使用“编辑查询组”向导，编辑和重新定位现有查询组，并且可以编辑据以将设备包括在查询组中的查询条件。

要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

1. 在“自定义组”下，右键单击查询组，或单击查询组旁边的三个垂直点菜单，然后单击**编辑**。
2. 在“编辑查询组”向导中，根据需要更改“名称”和“说明”。
3. 单击**下一步**。
4. 在“查询条件选择”对话框中，从**选择要复制的现有查询**下拉菜单中选择查询，然后选择其他筛选条件。
5. 单击**完成**。

对查询组所做的更改已实施。

重命名静态或查询组

要在“所有设备”页面（OpenManage Enterprise > 设备）上重命名静态或查询组，请执行以下操作：

1. 在**自定义组**下，右键单击静态或查询组，或单击要重命名的组旁边的三个点，然后单击**重命名**。或者，选择一个组，然后单击**组操作 > 重命名组**。
2. 在**重命名组**对话框中，输入组的新名称。
3. 单击**完成**。
更新的名称将在左侧窗格中列出。

删除静态或查询设备组

在“所有设备”页面（OpenManage Enterprise > 设备）上，您可以删除现有静态或查询组，如下所示：

要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 OpenManage Enterprise 中[基于角色和范围的访问控制](#) 页面上的 14。

注：此过程仅适用于删除静态或查询组，但不会从“所有设备”页面中删除组中的设备。要从 OpenManage Enterprise 中删除设备，请参阅[OpenManage Enterprise 删除设备](#) 页面上的 53。

1. 在**自定义组**下，右键单击静态或查询组，或单击组旁边的三个点垂直菜单，然后单击**删除**。或者，选择要删除的组，然后从**组操作**下拉菜单中单击**删除组**。
2. 显示提示时，单击**是**。

已从“自定义组”中删除该组。

克隆静态或查询组

可以克隆现有静态或查询组并将其添加到“自定义组”。

注：要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 OpenManage Enterprise 中[基于角色和范围的访问控制](#) 页面上的 14。

1. 右键单击静态或查询组，或单击静态或查询组旁边的树点垂直菜单，然后单击**克隆**。
2. 在**克隆组**对话框中，输入组的名称和说明。此外，对于静态组，选择必须在其下创建所克隆静态组的父组。
3. 单击**完成**。
将创建克隆组，并在左侧窗格中将其在父组下面显示。

将设备添加到新组

您可以创建新组，然后从“所有设备”页面上提供的设备列表表格中在其中添加设备。

要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 OpenManage Enterprise 中[基于角色和范围的访问控制](#) 页面上的 14。

1. 从 **OpenManage Enterprise** 菜单中，单击**设备**。
此时将显示“所有设备”页面。
2. 在设备列表中，选中与设备对应的复选框，然后单击**组操作 > 添加到新组**。
 - a. 在**将设备添加到新组向导**对话框中，输入**名称**、**说明**（可选），然后选择将在其下创建新子组的**父组**。有关组的更多信息，请参阅[设备组](#)。
 - b. 要向组中添加更多设备，请单击**下一步**。否则，请转至步骤 3。
3. 在**组成员选择**对话框中，从**添加设备**列表中，选择更多的设备。
在**所有设备**选项卡中选择设备之后，已选设备将在**所有选定的设备**下列出。
4. 单击**完成**。
将会创建新组并将设备添加到所选组。

注：创建组或将设备添加到某个组时，必须遵循组的父子关系。请参阅[设备组](#)。

将设备添加到现有组

您可以从“所有设备”页面上提供的设备列表表格中将设备添加到现有组。

注: 要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

1. 从 **OpenManage Enterprise** 菜单中，单击**设备**。
此时将显示“所有设备”页面。
2. 在设备列表中，选中与设备对应的复选框，然后单击**组操作 > 添加到现有组**。
3. 在**将所选设备添加到现有组**对话框中，输入或选择数据。有关组的更多信息，请参阅[设备组](#)。
4. 单击**完成**。
设备便会添加到所选的现有组。

注: 创建组或将设备添加到某个组时，必须遵循组的父子关系。请参阅[设备组](#)。

在组上刷新运行状况

以下步骤介绍了如何刷新所选组的运行状况和在线状态。

注:

- 要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
- 对于使用 ESXi 和 Linux 操作系统查找到的带内设备，运行状况 (🔌) 显示为“未知” (❓)。

1. 单击 **OpenManage Enterprise > 设备**，以转到“所有设备”页面。
2. 在左侧窗格中，选择要刷新运行状况的组。
选择组后，设备列表将列出所选组的设备。
3. 单击**刷新运行状况**下拉菜单，然后单击**在组上刷新运行状况**。此时将显示“运行状况”向导。
4. 在“运行状况”向导中，**作业名称**显示了设备为刷新运行状况任务生成的作业名称。如果需要，您可以更改作业名称。
5. **选择组**下拉列表将显示您选择的组。
6. 从“计划”下拉列表中，您可以选择以下选项之一：
 - a. **立即运行** — 立即在所选组上运行“刷新运行状况”。
 - b. **稍后运行** — 您可以选择“稍后运行”，然后选择将运行组上的“刷新运行状况”作业的日期和时间。
 - c. **按计划运行** — 如果您要在每日或每周的特定时间在组上刷新运行状况，则可以选择此选项，选择“每天”或“每周”，然后选择时间。

用于刷新组的运行状况和在线状态的作业已创建。您可以在“作业”页面 (**OpenManage Enterprise > 监测 > 作业**) 上查看作业详细信息。

“所有设备”页面 — 设备列表

设备列表可显示设备属性，如 IP 地址和服务标签。您在每个页面最多可以选择 25 个设备，并导航各页面以选择更多设备并执行任务。有关在“所有设备”页面上可执行的任务的更多信息，请参阅 [“所有设备”页面 — 设备列表操作](#) 页面上的 52。

注: 默认情况下，“设备”列表显示在形成环形图时所考虑的所有设备。要查看属于特定运行状况的设备列表，请单击环形图中对应的色带，或单击运行状况符号。将会列出仅属于所选类别的设备。

- **运行状况**表示设备的工作状态。运行状况（正常、严重和警告）通过相应的颜色符号来标识。请参阅 [设备运行状况状态](#) 页面上的 33
- **电源状态**表示设备是打开还是关闭
- **连接状态**表示设备是否已连接至 OpenManage Enterprise
- **名称**表示设备名称。
- **IP 地址**表示设备上安装的 iDRAC 的 IP 地址
- **标识符**表示设备的服务编号
- **型号**表示型号
- **类型**表示设备的类型，即服务器、机箱、Dell 存储和网络交换机
- **机箱名称**表示机箱名称

- **插槽名称**表示机箱设备的插槽名称
- **托管状态**列表示是监测、托管还是代理设备。请参阅[查找要监测或管理的设备](#) 页面上的 34。

要筛选表中的数据，请单击**高级筛选器**或筛选器符号。要将数据导出为 HTML、CSV 或 PDF 文件格式，请单击右上角的导出符号。

- ① **注:** 在“设备”列表中，单击设备名称或 IP 地址以查看设备配置数据，然后进行编辑。请参阅[查看和配置各个设备](#) 页面上的 56。
- ① **注:** 工作窗格显示所选设备组的环形图。通过使用环形图，您可以查看该组中属于其他运行状况的设备列表。要查看属于其他运行状况的设备，请单击相应的环形图色带。表中的数据发生变化。有关使用环形图的更多信息，请参阅[环形图](#)。

“所有设备” 页面 — 设备列表操作

在“所有设备”页面 (**OpenManage Enterprise > 设备**) 的设备列表中，您可以执行各种设备操作。

操作按钮与从左侧树中选择的组以及在网格中选择的设备相关。因此，如果操作与组相关，例如组操作（如“在组上运行资源清册”和“在组上刷新运行状况”）将默认为所选组。所有设备操作都将默认为所选设备。但是，如果未做任何选择，查找等少数操作将始终适用。此外，每个设备可用的操作类型取决于所选设备的类型。

- ① **注:** 要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

- 在**组操作**下拉列表中，您可以：
 - 创建自定义设备组。请参阅[创建自定义组（静态或查询）](#) 页面上的 47。
 - 创建静态组。请参阅[创建静态设备组](#) 页面上的 48。
 - 创建查询组。请参阅[创建查询设备组](#) 页面上的 48
 - 编辑静态或查询组。请参阅[编辑静态组](#) 页面上的 49 和[编辑查询组](#) 页面上的 49。
 - 克隆组。请参阅[克隆静态或查询组](#) 页面上的 50。
 - 重命名组。请参阅[重命名静态或查询组](#) 页面上的 50。
 - 删除组。请参阅[删除静态或查询设备组](#) 页面上的 50。
 - 将设备添加到新组。请参阅[将设备添加到新组](#) 页面上的 50。
 - 将设备添加到现有组。请参阅[将设备添加到现有组](#) 页面上的 51。
- 在**查找**下拉列表中，您可以：
 - 查找和启用设备。请参阅[查找要监测或管理的设备](#) 页面上的 34 和[启用设备](#) 页面上的 37。
 - 排除设备。请参阅[从 OpenManage Enterprise 中排除设备](#) 页面上的 53。
 - 编辑排除范围。请参阅[全局排除范围](#) 页面上的 40。
- 在**资源清册**下拉列表中，您可以：
 - 在设备组上运行资源清册。请参阅[创建并运行资源清册作业](#)。
 - 在设备上运行资源清册。请参阅[在设备上运行资源清册](#) 页面上的 53。
- 在**刷新运行状况**下拉列表中，您可以：
 - 在组上刷新运行状况。请参阅[在组上刷新运行状况](#) 页面上的 51。
 - 在设备上刷新运行状况。请参阅[在设备上刷新运行状况](#) 页面上的 55。
- 从**更多操作**下拉列表中，您可以：
 - 打开 LED。请参阅[创建作业以打开设备 LED](#) 页面上的 110。
 - 关闭 LED。请参阅[创建作业以打开设备 LED](#) 页面上的 110。
 - 打开设备电源。请参阅[为管理电源设备创建作业](#) 页面上的 110。
 - 关闭设备电源。请参阅[为管理电源设备创建作业](#) 页面上的 110。
 - 正常关闭设备。请参阅[为管理电源设备创建作业](#) 页面上的 110。
 - 关闭系统电源后重启（冷引导）。请参阅[为管理电源设备创建作业](#) 页面上的 110。
 - 系统重置（热引导）。请参阅[为管理电源设备创建作业](#) 页面上的 110。
 - 在设备上执行 IPMI CLI 远程命令。请参阅[在各个设备上运行远程 RACADM 和 IPMI 命令](#) 页面上的 59。
 - 在设备上执行 RACADM CLI 远程命令。请参阅[在各个设备上运行远程 RACADM 和 IPMI 命令](#) 页面上的 59。
 - 从 OpenManage Enterprise 删除设备。请参阅[从 OpenManage Enterprise 删除设备](#) 页面上的 53。
 - 导出所有设备上的数据。请参阅[导出所有或所选数据](#) 页面上的 56
 - 导出所选设备上的数据。请参阅[导出所有或所选数据](#) 页面上的 56

从 OpenManage Enterprise 删除设备

以下步骤介绍了如何在 OpenManage Enterprise 中删除和禁用查找到的设备。

注:

- 要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
- 如果未从设备取消分配配置文件，则不能删除已分配配置文件的设备。有关更多信息，请参阅 [取消分配配置文件](#) 页面上的 89。
- 即使设备上有正在运行的任务也可以删除该设备。如果在任务完成之前设备已被删除，则在设备上启动的任务将失败。

要删除查找到的设备，请执行以下操作：

1. 单击 **OpenManage Enterprise > 设备**，以转到“所有设备”页面。
2. 从设备列表中，选中与要删除的设备对应的复选框。
3. 单击**更多操作**下拉菜单，然后单击**删除设备**。
4. 在指明将从 OpenManage Enterprise 中删除并禁用设备的提示符处，单击**是**。

将从 OpenManage Enterprise 中完全删除所选设备。设备经删除后，与被删除设备对应的所有启用信息也将被删除。如果用户凭据信息未与其他设备共享，则也会被自动删除。如果将 OpenManage Enterprise 设置为所删除设备上的陷阱目标，则您必须将 OpenManage Enterprise 控制台 IP 作为陷阱目标从设备中删除。

相关信息

[将设备按组整理](#) 页面上的 46

从 OpenManage Enterprise 中排除设备

在 OpenManage Enterprise 中进行设备查找和分组，以便高效处理重复的任务，例如固件更新、配置更新、资源清册生成和警报监测。但是，您也可以从所有 OpenManage Enterprise 查找、监测和管理活动中排除设备。以下步骤介绍了如何从 OpenManage Enterprise 中排除已查找到的设备。

注: 要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

1. 单击 **OpenManage Enterprise > 设备**，以转到“所有设备”页面。
2. 在左侧窗格中，选择必须排除其设备的系统组或自定义组。
3. 在设备列表中，选中与设备对应的复选框，然后从**查找**下拉菜单中单击**排除设备**。
4. 在指明将会完全删除设备并将其添加到“全局排除”列表的提示符处，单击**是**。

设备将被排除并添加到全局排除列表中，并且不再由 OpenManage Enterprise 监测。

注: 要从全局排除中删除设备，并使 OpenManage Enterprise 再次监测设备，必须从全局排除范围中删除设备，然后再重新查找。

在设备上运行资源清册

以下步骤介绍了如何在查找到的设备上启动资源清册收集。

要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14

1. 单击 **OpenManage Enterprise > 设备**，以转到“所有设备”页面。
2. 从设备列表中，选中与设备对应的复选框。
3. 从**资源清册**下拉列表中，单击**在设备上运行资源清册**。

将为所选设备的资源清册收集创建“资源清册”作业。您可以在“资源清册”页面 (**OpenManage Enterprise > 监测 > 资源清册**) 上查看此作业的状态。

通过使用基线更新设备固件和驱动程序

您可以在“所有设备”页面或从“固件/驱动程序合规性”页面中更新设备的固件和/或驱动程序版本（请参阅[使用基线合规性报告更新固件和/或驱动程序](#) 页面上的 70）。当更新单个设备的固件和/驱动程序时，建议使用“所有设备”页面进行更新。

注：

- 要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
- 驱动程序更新仅适用于与 64 位 Windows 版本关联的设备。
- 无法回滚设备上的驱动程序更新。
- 如果固件更新是使用“**下一个服务器重新引导阶段**”选项完成的，则必须在将程序包安装到远程设备后手动执行资源清册和基线检查。
- 如果设备不关联任何基线，**基线**下拉菜单不会填充。要将设备与基线关联，请参阅[创建固件基线](#)。
- 如果您选择多个设备，表中将只列出与所选基线关联的设备。

1. 从“所有设备”页面的**设备**列表中，选择设备，然后单击**更多操作 > 更新**。

注：当您选择设备时，确保它们与一个或多个固件基线相关联。否则，该设备不会显示在合规性报告中，因此无法更新。

2. 在**设备更新**对话框中：

a. 在**选择更新源**部分，选择下面其中一项：

- 从**基线**下拉菜单中，选择相应的基线。将显示与所选基线相关联的设备列表。“合规性”列中将显示每个设备的合规性级别。根据合规性级别，您可以更新固件和/或驱动程序版本。有关此页面上字段说明的信息，请参阅[查看设备固件合规性报告](#)。
 - i. 选择与必须更新的设备对应的复选框。
 - ii. 单击**下一步**。
- 您也可以使用单独的更新包来更新固件和/或驱动程序。单击**单独的软件包**，然后按屏幕上的说明操作。单击**下一步**。

b. 在**计划**部分：

• 在**计划更新**下，单击**其他信息**以查看重要信息，然后选择下面其中一项：

- a. **立即更新**：立即应用固件/驱动程序更新。
- b. **以后计划**：指定一个固件或驱动程序版本必须更新的日期和时间。如果不想打扰当前的任务，建议您使用此模式。

• 在**服务器选项**下，选择以下重新启动选项之一：

- a. 要在固件/驱动程序更新后立即重新启动服务器，请选择**立即重新启动服务器**，然后从下拉菜单中选择下面其中一项：
 - i. **正常重新引导而不强制关机**
 - ii. **正常重新引导并强制关机**
 - iii. **关机后重新开机**，用于设备的硬重置。
- b. 选择**下一个服务器重新引导阶段**，以在下次重新启动服务器时触发固件/驱动程序更新。如果选择此选项，则必须在将程序包安装到远程设备后手动执行资源清册和基线检查。

3. 单击**完成**。

将创建一个固件/驱动程序更新作业，并“作业”列表中列出。请参阅[使用作业进行设备控制](#) 页面上的 106。

刷新设备组的设备运行状况

默认情况下，设备会每小时自动刷新所有设备和设备组的运行状况，但也可以随时刷新设备和/或设备组的运行状况。以下步骤介绍了如何在“所有设备”页面上刷新所选设备组的运行状况和在线状态。

1. 在左侧的窗格中，选择设备所属的组。

将列出与该组关联的设备。

2. 选中与设备对应的复选框，然后单击**在组上刷新运行状况**。

作业已创建并在“作业”列表中列出，在“作业状态”列中标识为**新建**。

所选设备的最新工作状态将被收集并显示在仪表板和 OpenManage Enterprise 的其他相关部分。要下载设备资源清册，请参阅[导出单个设备资源清册](#) 页面上的 55。



相关信息

[将设备按组整理](#) 页面上的 46

在设备上刷新运行状况

默认情况下，设备会每小时自动刷新所有设备和设备组的运行状况，但也可以随时刷新设备和/或设备组的运行状况。以下步骤介绍了如何在“所有设备”页面上刷新所选设备的运行状况和在线状态。

注:

- 要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
- 对于使用 ESXi 和 Linux 操作系统查找到的带内设备，运行状况 () 显示为“未知” ()。

1. 单击 **OpenManage Enterprise > 设备**，以转到“所有设备”页面。
2. 从设备列表中选择要刷新运行状况的设备。
3. 单击**刷新运行状况**下拉菜单，然后单击**在设备上刷新运行状况**。

已为所选设备启动运行状况任务。您可以在“作业”页面 (**OpenManage > 监测 > 作业**) 上查看运行状况任务的状态。


回滚单个设备的固件版本

您可以回滚高于关联基线固件版本的设备固件版本此功能仅在您查看和配置单个设备的属性时可用。请参阅[查看和配置各个设备](#) 页面上的 56。您可以升级或回滚单个设备的固件版本。您一次只可以回滚一种设备的固件版本。

注:

- 回滚仅适用于固件。设备驱动程序一旦更新，就无法回滚到以前的版本。
- 回滚仅适用于从 OME 控制台更新的设备（对基线更新和单个 DUP 更新都适用）。
- 如果任何安装的 iDRAC 未处于就绪状态，即使已成功应用固件，也可能表示固件更新作业失败。查看未处于就绪状态的 iDRAC，然后在服务器引导期间按 F1 键继续。

此处没有列出任何通过使用 iDRAC GUI 进行更新的设备固件，且无法进行更新。有关创建基线的信息，请参阅[创建固件/驱动程序基线](#) 页面上的 67。

1. 在左侧窗格中，选择组，然后单击列表中的设备名称。
2. 在<设备名称>页面中，单击**固件/驱动程序**。
3. 从**基线**下拉菜单中选择该设备所属的基线。
列出与所选基线关联的所有设备。有关表中字段说明的信息，请参阅[查看基线合规性报告](#) 页面上的 69。
4. 选择与其固件版本必须回滚的设备对应的复选框，该设备由  标识。
5. 单击**回滚固件**。
6. 在**回滚固件**对话框，会显示以下信息：
 - **组件名称**：设备上组件的固件版本高于基线版本。
 - **当前版本**：组件的当前版本。
 - **回滚版本**：组件可以降级到建议的固件版本。
 - **回滚源**：单击**浏览**以选择可以下载固件版本的源位置。
7. 单击**完成**。回滚固件版本。

注: 当前，回滚功能仅跟踪回滚固件的版本号。回滚不考虑使用回滚功能（通过回滚版本）安装的固件版本。

导出单个设备资源清册

您每次只能导出一个设备的资源清册数据，并且只能导出为 .csv 格式。

1. 在左侧窗格中，选择设备组。组中设备的列表显示在“设备”列表中。
环形图表示工作窗格中的设备状态。请参阅[环形图](#)。该表列出了所选设备的属性。请参阅[设备列表](#)。
2. 在设备列表中，选中与设备对应的复选框，然后单击**导出资源清册**。
3. 在**另存为**对话框中，保存到已知的位置。

注: 导出为 .csv 格式时，GUI 上显示的一些数据未用描述性字符串枚举。

在机箱和服务器的执行更多操作

通过使用**更多操作**下拉菜单，在“所有设备”页面上可执行以下操作。选择设备，然后执行以下一项操作：

- **打开 LED**：打开设备的 LED，以便在数据中心中的一组设备内识别该设备。
- **关闭 LED**：关闭设备的 LED。
- **打开电源**：开启设备。
- **关闭电源**：关闭设备。
- **正常关机**：单击关闭目标系统。
- **关闭系统电源后重启（冷引导）**：单击可关闭然后重新引导系统。
- **系统重置（热引导）**：单击可强制关闭目标系统，然后关闭并重新引导操作系统。
- **代理**：仅为 MX7000 机箱显示。表示在多机箱管理 (MCM) 的情况下，设备通过 MX7000 主机箱查找到。
- **IPMI CLI**：单击可运行 IPMI 命令。请参阅[为管理设备创建远程命令作业](#) 页面上的 110。
- **RACADM CLI**：单击可运行 RACADM 命令。请参阅[为管理设备创建远程命令作业](#) 页面上的 110。
- **更新固件**：请参阅[通过使用基线更新设备固件和驱动程序](#) 页面上的 54。
- **启用**：请参阅[启用设备](#) 页面上的 37。
- **全部导出和导出所选项**：请参阅[导出所有或所选数据](#) 页面上的 56。

显示的 MX7000 机箱硬件信息

- **机箱电源设备** — 有关底座和其他组件中所使用电源设备 (PSU) 的信息。
- **机箱插槽** — 有关机箱和组件（如有，安装在插槽中）中可用插槽的信息。
- **机箱控制器** — 机箱管理控制器 (CMC) 及其版本。
- **风扇** — 有关机箱中所使用风扇及其工作状态的信息。
- **温度** — 机箱的温度状态和阈值。
- **FRU** — 机箱中安装的组件或现场可更换单元 (FRU)。

导出所有或所选数据

您可以执行以下操作：

- 导出您在设备组中查看的设备的相关数据，并执行策略和统计分析。
- 导出最多 1000 台设备的相关数据。
- 与系统警报、报告、审计日志、组资源清册、设备列表、保修信息、Support Assist 等相关。
- 将数据导出为以下文件格式：HTML、CSV 和 PDF。

i 注：

- 请避免将列包含长字符串或列太多的“宽”表导出为 PDF。由于 PDFMaker 库的限制，此类导出数据的最右侧部分将被截断或切断。
- 您只能将单个设备的资源清册导出为 .csv 格式。请参阅[导出单个设备资源清册](#) 页面上的 55
- 仅在报告的情况下，您可以一次只导出所选报告而不是所有报告。请参阅[导出所选报告](#) 页面上的 119。

1. 要导出数据，请选择**全部导出或导出所选**。
将创建一个作业并将数据导出到所选位置。
2. 如有必要，请下载该数据并执行策略和统计分析。
该数据将根据您的选择被成功打开或保存。

i 注：如果以 .csv 格式导出数据，则必须具有管理员级别凭据才能打开该文件。

查看和配置各个设备

i 注：在设备列表中，单击设备名称或 IP 地址以查看设备配置数据，然后按照本节所述编辑设备配置。

通过单击 **OpenManage Enterprise > 设备 > 选择设备列表中的设备 > 查看详细信息**，您可以执行以下操作：

- 查看运行状况和电源状态、设备 IP 以及服务标签的相关信息。

- 查看有关设备的一般信息，并执行服务器控制和故障排除任务。
- 查看设备信息，例如 RAID、PSU、操作系统、NIC、内存、处理器和存储机柜。OpenManage Enterprise 提供一份内置报告以获得关于在受 OpenManage Enterprise 监测的设备上使用的 NIC、BIOS、物理磁盘和虚拟磁盘的概述。单击 **OpenManage Enterprise > 监测 > 报告**。
- 更新或回滚与固件基线相关联的设备中组件的固件版本。请参阅[管理设备固件和驱动程序](#) 页面上的 64。
 ⓘ **注：**使用单个软件包工作流更新设备仅支持基于可执行 (EXE) 的 Dell Update Packages。更新 FX2 CMC 时，必须通过机箱中的一个底座安装可执行 DUP。
- 确认、导出、删除或忽略与设备相关的警报。请参阅[管理设备警报](#)。
- 查看和导出设备的硬件日志数据。请参阅[管理单个设备硬件日志](#) 页面上的 59。
- 查看和管理配置设备的资源清册以用于配置合规性。当针对设备运行配置资源清册时，将启动合规性比较。
- 针对设备相关的配置合规性基线查看其合规性级别。请参阅[管理设备配置合规性](#) 页面上的 91。

设备概述

- 在<设备名称>页中，**概述**下面将显示设备的运行状况、电源状态和服务标签。单击 IP 地址以打开 iDRAC 登录页面。请参阅 Dell 支持站点上提供的 *iDRAC 用户指南*。
 - **信息：**显示以下信息，如服务标签、DIMM 插槽、iDRAC DNS 名称、处理器、机箱、操作系统和数据中心名称。将会列出与设备关联的多个管理 IP 地址，并且可以单击以激活各自的界面。
 - **最近警报：**为设备生成的最近警报。
 - **最近活动：**设备上运行的最近活动的列表。单击**全部查看**可查看所有作业。请参阅[使用作业进行设备控制](#) 页面上的 106。
 - **远程控制台：**单击**启动 iDRAC** 以启动 iDRAC 应用程序。单击**启动虚拟控制台**以启动虚拟控制台。单击**刷新预览**符号以刷新概述页面。
 - **服务器子系统：**显示设备其他组件的运行状况，如 PSU、风扇、CPU 和电池。
 ⓘ **注：**收集使用 IPMI 发现的传感器组件的子系统数据所需的时间取决于网络连接、目标服务器和目标固件。如果在收集传感器数据时遇到超时，请重新启动目标服务器。
 - **上次更新部分**表示上次更新设备资源清册状态的时间。单击**刷新**按钮可更新状态。将启动资源清册作业并更新页面上的状态。
- 通过使用**电源控制**，可以打开、关闭、关机后再开机以及正常关闭设备。
- 通过使用**故障排除**：
 - 运行并下载诊断报告。请参阅[运行并下载诊断报告](#) 页面上的 58。
 - 重设 iDRAC。
 - 提取并下载 SupportAssist 报告。请参阅[提取和下载 SupportAssist 报告](#) 页面上的 58。
- 刷新设备状态。
- 刷新设备资源清册。
- 导出通过单击**刷新**收集的**资源清册**。请参阅[导出所有或所选数据](#) 页面上的 56。
- 在设备上运行远程 RACADM 和 IPMI 命令。请参阅[在各个设备上运行远程 RACADM 和 IPMI 命令](#) 页面上的 59。

OpenManage Enterprise 提供一份内置报告以获得受 OpenManage Enterprise 监测的设备概述。单击 **OpenManage Enterprise > 监测 > 报告 > 设备概述报告**。单击**运行**。请参阅[运行报告](#) 页面上的 116。

设备硬件信息

OpenManage Enterprise 提供一份关于组件及其符合固件合规性基线的内置报告。单击 **OpenManage Enterprise > 监测 > 报告 > 每个组件的固件合规性报告**。单击**运行**。请参阅[运行报告](#) 页面上的 116。

- **设备卡信息** — 有关设备中使用的插卡的信息。
- **已安装的软件** — 设备中不同组件上安装的固件和软件的列表。
- **处理器** — 处理器信息，如插槽、系列、速度、内核和型号。
- **RAID 控制器信息** — 存储设备上使用的 PERC 和 RAID 控制器。汇总状态等于具有高严重性的 RAID 的状态。有关“汇总运行状况”状态的更多信息，请参阅 Dell 技术中心上提供的在 *Dell EMC 第 14 代及更高代别的 POWEREDGE 服务器上使用 iDRAC 管理汇总运行状况状态白皮书*。
- **NIC 信息** — 有关设备中使用的 NIC 的信息。
- **内存信息** — 设备中使用的 DIMM 的数据。
- **阵列磁盘**：有关安装在设备上的驱动器的信息。OpenManage Enterprise 提供一份关于由 OpenManage Enterprise 监测的设备上可用的 HDD 或虚拟驱动器的内置报告。单击 **OpenManage Enterprise > 监测 > 报告 > 物理磁盘报告**。单击**运行**。请参阅[运行报告](#) 页面上的 116。
- **存储控制器**：安装在设备上的存储控制器。单击加号符号以查看单个控制器数据。

- **电源设备信息**：有关设备上安装的 PSU 的信息。
- **操作系统** — 设备上安装的操作系统。
- **许可证** — 设备中安装的不同许可证的运行状况。
- **存储机柜** — 存储机柜的状态和 EMM 版本。
- **虚拟闪存** - 虚拟闪存驱动器及其技术规格列表。
- **FRU** — 可由现场技术人员处理和维修的现场可更换单元 (FRU) 的列表。OpenManage Enterprise 提供一份关于在受 OpenManage Enterprise 监测的设备上安装的现场可更换单元 (FRU) 的内置报告。单击 **OpenManage Enterprise > 监测 > 报告 > FRU 报告**。单击**运行**。请参阅[运行报告](#) 页面上的 116。
- **设备管理信息** — 设备 (如果是服务器) 中安装的 iDRAC 的 IP 地址信息。
- **来宾信息** - 显示 OpenManage Enterprise 监测的来宾设备。UUID 是设备的通用唯一标识符。**来宾状态**列表表示来宾设备的工作状态。

运行并下载诊断报告

- i** **注**: 要在 OpenManage Enterprise 上执行任何任务, 您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14
- i** **注**: 请确保先在 **SMB 设置** 中启用 SMBv1, 然后才能在任何机箱上或具有 iDRAC 版本 2.50.50.50 及更早版本的 PowerEdge YX2X 和 YX3X 服务器上开始任何固件任务。有关详情, 请参阅[管理控制台首选项](#) 页面上的 137 和 [Dell EMC PowerEdge 服务器的通用命名惯例](#) 页面上的 154。
1. 在<**设备名称**>页面上, 从**故障排除**下拉菜单中选择**运行诊断程序**。
 2. 在**远程诊断类型**对话框中, 从**远程诊断类型**下拉菜单中选择以下操作之一以生成报告。
 - **快速**: 尽可能缩短时间。
 - **延长**: 以正常速度延长。
 - **长期运行**: 以慢速运行。

i **注**: 请参阅 https://en.community.dell.com/techcenter/extras/m/white_papers/20438187 上的**使用 WS-Man 和 RACADM 命令远程运行自动诊断技术白皮书**。
 3. 要立即生成诊断报告, 请选择**立即运行**。
 4. 单击**确定**。显示提示时, 单击**是**。

警告: 运行诊断报告会**自动重启服务器**。

作业即会创建并显示在**作业**页面上。要查看关于作业的信息, 请单击右侧窗格中的**查看详细信息**。请参阅[查看作业列表](#) 页面上的 106。作业状态在**最近活动**部分中也会显示。作业成功运行后, 作业状态标识为**诊断完成**, 且**下载**链接显示在**最近活动**部分中。

5. 要下载报告, 请单击**下载**链接, 然后下载<Servicetag-jobid>.TXT 诊断报告文件。
 - 否则, 请单击**故障排除 > 下载诊断报告**, 然后下载文件。
6. 在**下载远程诊断文件**对话框中单击 .TXT 文件链接, 然后下载报告。
7. 单击**确定**。

提取和下载 SupportAssist 报告

- i** **注**: 要在 OpenManage Enterprise 上执行任何任务, 您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14
- i** **注**: 请确保先在 **SMB 设置** 中启用 SMBv1, 然后才能在任何机箱上或具有 iDRAC 版本 2.50.50.50 及更早版本的 PowerEdge YX2X 和 YX3X 服务器上开始任何固件任务。有关详情, 请参阅[管理控制台首选项](#) 页面上的 137 和 [Dell EMC PowerEdge 服务器的通用命名惯例](#) 页面上的 154。
1. 在<**设备名称**>页面上, 请从**故障排除**下拉菜单中选择**提取 SupportAssist 报告**。
 2. 在**提取 SupportAssist 报告**对话框中:
 - a. 输入必须保存 SupportAssist 报告的文件名。
 - b. 选择与必须提取 SupportAssist 报告的日志类型对应的复选框。
 3. 单击**确定**。
作业即会创建并显示在**作业**页面上。要查看关于作业的信息, 请单击右侧窗格中的**查看详细信息**。请参阅[查看作业列表](#) 页面上的 106。作业状态在**最近活动**部分中也会显示。作业成功运行后, 作业状态标识为**诊断完成**, 且**下载**链接显示在**最近活动**部分中。

- 要下载报告，请单击**下载**链接，然后下载<服务标签>.<时间>.TXT SupportAssist 报告文件。
 - 否则，请单击**故障排除** > **下载 SupportAssist 报告**。
- 在**下载 SupportAssist 文件**对话框中单击 .TXT 文件链接，然后下载报告。每个链接代表所选日志类型。
- 单击**确定**。

管理单个设备硬件日志

- 注：** 硬件日志可用于 YX4X 服务器、MX7000 机箱和底座。有关详情，请参阅 [Dell EMC PowerEdge 服务器的通用命名惯例](#) 页面上的 154。
- 在<设备名称>页面中，单击**硬件日志**。所有为设备生成的事件和错误消息已列出。有关字段说明，请参阅[监视审核日志](#) 页面上的 104。
 - 对于机箱，关于硬件日志的实时数据将从该机箱检索。
 - 要添加注释，请单击**添加注释**。
 - 在对话框中键入注释，然后单击**保存**。保存注释后，用符号将其在**注释**列中标识。
 - 要将所选日志数据导出到 .CSV 文件，请选择相应的复选框，然后单击**导出导出所选**。
 - 要导出页面中所有日志，请单击**导出导出当前页面**。

在各个设备上运行远程 RACADM 和 IPMI 命令

可以通过“设备名称”页面将 RACADM 和 IPMI 命令发送到设备的 iDRAC，以远程管理相应的设备。

- 注：**
- RACADM CLI 一次只允许一个命令。
 - 不支持将以下特殊字符用作 RACADM 和 IPMI CLI 参数：[、;、|、\$、>、<、&、'、]、.、* 和 '。
- 选择与设备对应的复选框，然后单击**查看详细信息**。
 - 在<设备名称>页面中单击**远程命令行**，然后选择 **RACADM CLI** 或 **IPMI CLI**。

注： 以下服务器不显示 RACADM CLI 选项卡，因为相应任务在设备组中不可用 — MX740c、MX840c 和 MX5016S。
 - 在**发送远程命令**对话框中，键入命令。最多可以输入 100 个命令，每个命令必须位于单独的行中。要让结果显示在同一对话框中，请选择**发送后打开结果**复选框。

注： 采用以下语法输入 IPMI 命令：-I lanplus <command>。要结束命令，请输入“Exit”。
 - 单击**发送**。
作业即会创建并显示在对话框中。作业也将在“作业详细信息”中列出。请参阅[查看作业列表](#) 页面上的 106。
 - 单击**完成**。
最近警报部分显示作业完成状态。

启动设备的管理应用程序 iDRAC

- 选择与设备对应的复选框。
将会显示设备的工作状态、名称、类型、IP 和服务标签。
 - 在右侧窗格中，单击**启动管理应用程序**。
随即显示 iDRAC 登录页面。使用 iDRAC 凭据登录。
有关使用 iDRAC 的更多信息，请访问 [Dell.com/idracmanuals](#)。
- 注：** 您也可以通过单击设备列表中的 IP 地址启动管理应用程序。请参阅“[所有设备](#)”页面 — [设备列表](#) 页面上的 51。

启动虚拟控制台

虚拟控制台链接在 YX4X 服务器的 iDRAC Enterprise 许可下有效。该链接在 YX2X 和 YX3X 服务器的 iDRAC Enterprise 2.52.52.52 或更高版本的许可下有效。在虚拟控制台的当前插件类型为 Active X 时如果单击此链接，将出现一条消息，提示您需要更新控制台到 HTML 5 以实现更好的用户体验。有关详情，请参阅[创建作业以更改虚拟控制台插件类型](#) 页面上的 111 和 [Dell EMC PowerEdge 服务器的通用命名惯例](#) 页面上的 154。

1. 选择与设备对应的复选框。
将会显示设备的工作状态、名称、类型、IP 和服务标签。
2. 在右侧窗格中，单击**启动虚拟控制台**。
随即会显示服务器上的远程控制台页面。

刷新单个设备的设备资源清册

默认情况下，设备或设备组中的软件和硬件组件的资源清册将在每 24 小时后自动收集，（例如每天凌晨 12:00）。但是，无论在何时收集单个设备的资源清册报告，都请执行以下操作：

1. 在“所有设备”页面上，选中与设备对应的复选框（**OpenManage Enterprise > 设备**），然后单击右侧窗格中的**查看详细信息**。此时会显示设备的“概览”页面。
2. 单击**刷新资源清册**以启动资源清册作业。
资源清册作业的状态可在“资源清册”页面上进行查看（**OpenManage Enterprise > 监测 > 资源清册**）。选择资源清册作业，然后单击**查看详细信息**，以查看所选设备已收集的资源清册。要获取更多有关查看刷新资源清册数据的更多信息，请参阅[查看和配置各个设备](#) 页面上的 56。要下载设备资源清册，请参阅[导出单个设备资源清册](#) 页面上的 55。

相关信息

[将设备按组整理](#) 页面上的 46

管理设备资源清册

注：要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

通过单击 **OpenManage Enterprise > 监测 > 资源清册**，您可以生成设备资源清册报告，以更好地管理数据中心、减少维护、保持最小库存以及降低运营成本。通过使用 OpenManage Enterprise 中的“资源清册计划”功能，您可以在预定义时间运行计划的作业，然后生成报告。您可以在第 12 代及更高版本的 PowerEdge 服务器、网络设备、PowerEdge 机箱、EqualLogic 阵列、Compellent 阵列和 PowerVault 设备上计划资源清册作业。

在此页面上，您可以创建、编辑、运行、停止或删除资源清册计划。将显示现有资源清册计划作业的列表。

- **名称：**资源清册计划名称。
- **计划：**指明作业被计划成立即运行还是以后运行。
- **上次运行：**指明上次运行作业的时间。
- **状态：**指明作业是正在运行、已完成还是失败。

注：在[查找和资源清册计划](#)页面上，计划作业的状态由**状态**列中的**排队**标识。但在[作业](#)页面上，同样的状态被标识为**已计划**。

要预览作业信息，请单击与作业对应的行。右侧窗格会显示与资源清册任务相关的作业数据和目标组。要查看关于作业的信息，请单击[查看详细信息](#)。[作业详细信息](#)页面显示更多信息。请参阅[查看单个作业信息](#)页面上的 109。

相关任务

[立即运行资源清册作业](#) 页面上的 62

[停止资源清册作业](#) 页面上的 62

[删除资源清册作业](#) 页面上的 62

[创建资源清册作业](#) 页面上的 61

主题：

- [创建资源清册作业](#)
- [立即运行资源清册作业](#)
- [停止资源清册作业](#)
- [删除资源清册作业](#)
- [编辑资源清册计划作业](#)

创建资源清册作业

以下步骤介绍了如何在查找到的组上启动资源清册收集。

- 注：**
- 要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
 - 如果通过机箱设备管理对机箱存储底座进行管理，则 OpenManage Enterprise 中不支持机箱存储底座上的资源清册收集。

- 要启动“资源清册”向导，请执行以下操作之一：
 - 在“所有设备”页面（**OpenManage Enterprise > 设备**）上，从左侧窗格中选择一个组，然后从**资源清册**下拉菜单中单击在**组上运行资源清册**。
 - 在“资源清册”页面（**OpenManage Enterprise > 监测 > 资源清册**）上，单击**创建**。
- 在**资源清册计划**对话框中，**资源清册作业名称**中填入默认的资源清册作业名称。如需更改，请输入资源清册作业名称。
- 从**选择组**下拉菜单中选择必须运行资源清册的设备组。
如果在选择组后从“所有设备”页面启动了“资源清册”作业，则将使用所选组名称预填充“选择组”。有关设备组的信息，请参阅[将设备按组整理](#)页面上的 46。

4. 在**计划**部分，立即或计划以后运行作业。
请参阅[计划作业字段定义](#) 页面上的 150。
5. 在运行资源清册作业时，可以选择以下**附加选项**：
 - 选中**收集配置资源清册**复选框，以生成配置合规性基线的资源清册。
 - 选中**收集驱动程序资源清册**复选框，以从 Windows 服务器收集驱动程序资源清册信息。此外，如果服务器上不存在这些组件，则在 Windows 服务器上安装资源清册收集器和 Dell System Update。

注：

- “收集驱动程序资源清册”仅适用于作为 64 位 Windows 服务器而查找的设备。
- 仅支持使用 OpenSSH 完成基于 Windows 的设备资源清册收集。不支持 Windows 上的其他 SSH 实现，比如 CygWin SSH。

有关配置合规性基线的信息，请参阅[管理设备配置合规性](#) 页面上的 91。

6. 单击**完成**。
7. 该作业已创建并在队列中列出。
创建资源清册作业（显示在资源清册作业列表中）。**计划**列指定该作业为已计划或未计划的作业。请参阅[立即运行资源清册作业](#) 页面上的 62。

相关信息

[管理设备资源清册](#) 页面上的 61

立即运行资源清册作业

注： 您无法重新运行已在运行的作业。

1. 在现有的资源清册计划作业列表中，选择与您想要立即运行的资源清册作业对应的复选框。
2. 单击 **立即运行**。
作业会立即运行，右下角将会显示一条消息。

相关信息

[管理设备资源清册](#) 页面上的 61

停止资源清册作业

您只能停止正在运行的作业。已完成或失败的资源清册作业无法停止。停止作业：

1. 在现有的资源清册计划作业列表中，选择与您要停止的资源清册计划作业对应的复选框。
2. 单击**停止**。
作业停止，右下角将会显示一条消息。

相关信息

[管理设备资源清册](#) 页面上的 61

删除资源清册作业

注： 如果作业正在运行，则无法将其删除。

1. 在现有的资源清册计划作业列表中，选择与您想要删除的资源清册作业对应的复选框。
2. 单击**删除**。
作业被删除，右下角将会显示一条消息。

相关信息

[管理设备资源清册](#) 页面上的 61

编辑资源清册计划作业

1. 单击**编辑**。
2. 在**资源清册计划**对话框中，编辑**资源清册作业名称**中的资源清册作业名称。请参阅[创建资源清册作业](#) 页面上的 61。资源清册计划作业将会更新并显示在表格中。





管理设备固件和驱动程序

在 **OpenManage Enterprise > 配置 > 固件/驱动程序合规性** 页面上，您可以管理所有“受管”设备的固件。您还可以更新基于 64 位 Windows 的设备的驱动程序。

注:

- 要对 OpenManage Enterprise 执行任何任务，您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
- 如果设备固件或驱动程序版本早于基线版本，则不会自动更新，必须由用户启动更新。
- 建议在维护期内进行固件和驱动程序更新，以防设备或环境在工作时间脱机。
- 要管理设备的固件和/或驱动程序，系统的“启用”状态应为“受管”或“带警报的受管”。请参阅 [启用设备](#) 页面上的 37
- 目前，目录包含的驱动程序仅适用于基于 64 位 Windows 的设备。

通过使用固件/驱动程序功能，您可以：

- 直接使用 Dell.com 上的固件和驱动程序目录，或在网络路径上保存后使用。请参阅 [通过使用 Dell.com 添加目录](#) 页面上的 65 或 [使用本地网络创建固件目录](#)。
- 使用可用的目录创建固件和驱动程序基线。这些基线用作基准，对设备上的固件和驱动程序版本与目录中的版本进行比较。请参阅 [创建固件基线](#)。
- 运行合规性报告以检查与基线关联的设备是否符合基线固件和驱动程序版本。请参阅 [检查固件合规性](#)。合规性列中显示：
 - **OK**  — 如果目标设备的固件和/或驱动程序版本与基线相同。
 - **升级** — 如果目标设备具有一个或多个早于基线的固件或驱动程序版本的版本。请参阅 [更新设备固件版本](#)
 - **严重**  — 如果设备不符合基线要求，并指出它是重要升级且必须升级设备的固件和驱动程序以确保正常工作。
 - **警告**  — 如果设备固件和/或驱动程序不符合基线要求，并且可以升级设备固件以增强功能。
 - **降级**  — 如果设备固件和/或驱动程序晚于基线版本。
 - 导出统计和分析目的的合规性报告。
 - 通过使用基线更新设备固件和/或驱动程序版本。请参阅 [通过使用基线更新设备固件和驱动程序](#) 页面上的 54。

注:

- 当检查包含多个设备的固件/驱动程序基线是否满足合规性时，将仅记录来自该基线的一个随机、不符合要求的设备的“警报”页面上的警告警报 CDEV9000。
- 网络交换机、模块化 IOA 和戴尔存储设备的固件或驱动程序合规性状态显示为**未知**，因为它们无法使用戴尔目录进行更新。推荐使用各自的单独更新软件包为这些设备执行单独的固件或驱动程序更新。要执行单独的固件或驱动程序更新，请在所有设备页面上选择一个设备，然后单击 [查看详细信息 > 固件/驱动程序](#) 并选择单个软件包选项。有关不受支持设备列表的更多信息，请参阅 [固件/驱动程序合规性基线报告 - 具有“未知”合规状态的设备](#) 页面上的 154。

您还可以在以下位置更新设备固件版本：

- “所有设备”页面。请参阅 [更新设备固件版本](#)。
- “设备详细信息”页面。在“设备”列表中，单击设备名称或 IP 地址以查看设备配置数据，然后进行编辑。请参阅 [查看和配置各个设备](#) 页面上的 56。

注: 使用单个软件包工作流更新设备仅支持基于可执行 (EXE) 的 Dell Update Packages。更新 FX2 CMC 时，必须通过机箱中的一个底座安装可执行 DUP。

所有基线的摘要显示在工作窗格中，所选基线的合规性将通过环形图显示在右侧窗格中。基线中项目的环形图和列表将随您从基线列表中选择基线而变化。请参阅 [环形图](#)。

主题:

- [管理固件和驱动程序目录](#)
- [创建固件/驱动程序基线](#)
- [删除配置合规性基线](#)
- [编辑基线](#)

- [检查设备固件和驱动程序的合规性](#)

管理固件和驱动程序目录

目录是基于设备类型的固件和驱动程序捆绑包。验证所有可用的目录（更新软件包）并发布到 Dell.com。您可以直接从联机存储库使用目录，也可以将其下载到网络共享。

使用这些目录，您可以为查找到的设备创建固件/驱动程序基线并检查其合规性。这样可以减少管理员和设备管理员的额外工作量，并减少整体更新和维护时间。

管理员用户可以查看和访问 OpenManage Enterprise 中的所有目录，但设备管理者只能查看和管理自己创建并拥有的目录。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

有关目录管理页面上的字段定义，请参阅 [目录管理字段定义](#) 页面上的 154。您目前可以访问的目录来源有：

i 注：

- 使用 Dell.com 或本地网络路径管理的固件目录仅限于 Enterprise Server 目录。
- 在通过网络共享导入 OpenManage Enterprise 版本 3.5 中的目录时，可在不使用 Dell Update Packages (DUP) 的情况下使用指向 “Downloads.dell.com” 的基本位置的目录。在固件升级过程中，将直接从 <https://downloads.dell.com> 下载 DUP。
- **Dell.com 上的最新组件版本**：列出了设备的最新固件和驱动程序（64 位 Windows）版本。例如，经过严格测试并发布到 Dell.com 上的 iDRAC、BIOS、PSU 和 HDD。请参阅 [使用 Dell.com 创建固件目录](#)。
- **网络路径**：Dell Repository Manager (DRM) 下载固件和驱动程序目录并将其保存在网络共享中的位置。请参阅 [使用本地网络创建固件目录](#)。

通过使用 Dell.com 添加目录

i 注：要对 OpenManage Enterprise 执行任何任务，您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

i 注：请确保先在 **SMB 设置** 中启用 SMBv1，然后才能在任何机箱上或具有 iDRAC 版本 2.50.50.50 及更早版本的 PowerEdge YX2X 和 YX3X 服务器上开始任何固件任务。有关详情，请参阅 [管理控制台首选项](#) 页面上的 137 和 [Dell EMC PowerEdge 服务器的通用命名惯例](#) 页面上的 154。

1. 在 **目录管理** 页面中，单击 **添加**。
2. 在 **添加更新目录** 对话框中：
 - a. 在 **名称** 字段中，输入固件类别名称。
 - b. 对于 **目录源**，选择 **Dell.com 上的最新组件版本** 选项。
 - c. 在 **更新目录** 框中，选择 **手动** 或 **自动**。
 - d. 如果在 **更新目录** 框中选择了 **自动**，则需要为 **更新频率** 选择 **每天** 或 **每周**，后跟带上午/下午的 12 小时制时间格式。
 - e. 单击 **完成**。
只有在您输入了对话框中的所有字段之后，**完成** 按钮才会显示出来
一个新的固件目录将会创建并列在 **目录管理** 页面上的目录表中。
3. 要返回 **固件/驱动程序合规性** 页面，请单击 **返回到固件/驱动程序合规性**。

向本地网络添加目录

可以使用 Dell Repository Manager (DRM) 下载包含固件和驱动程序（64 位 Windows）的目录，并将其保存在网络共享上。

1. 在 **目录管理** 页面中，单击 **添加**。
2. 在 **添加更新目录** 对话框中：
 - a. 在 **名称** 框中，输入目录名称。
 - b. 对于 “**目录源**”，选择 **网络路径** 选项。
将显示 **共享类型** 下拉菜单。
 - c. 选择以下选项之一：
 - i** 注：请确保先在 **SMB 设置** 中启用 SMBv1，然后才能在任何机箱上或具有 iDRAC 版本 2.50.50.50 及更早版本的 PowerEdge YX2X 和 YX3X 服务器上开始任何固件任务。有关详情，请参阅 [管理控制台首选项](#) 页面上的 137 和 [Dell EMC PowerEdge 服务器的通用命名惯例](#) 页面上的 154。

- NFS
 - i. 在**共享地址**框中，输入在网络上存储固件目录的系统的 IP 地址。
 - ii. 在**目录文件路径**框中，输入目录文件位置的完整文件路径。示例路径：*nfsshare\catalog.xml*
- CIFS
 - i. 在**共享地址**框中，输入在网络上存储固件目录的系统的 IP 地址。
 - ii. 在**目录文件路径**框中，输入目录文件位置的完整文件路径。示例路径：*Firmware\m630sa\catalog.xml*
 - iii. 在**域**框中，输入设备的域名。
 - iv. 在**用户名**框中，输入存储目录所在设备的用户名。
 - v. 在**密码**框中，输入要访问共享的设备的密码。键入存储 *catalog.xml* 文件的共享文件夹的用户名和密码。
- HTTP
 - i. 在**共享地址**框中，输入在网络上存储固件目录的系统的 IP 地址。
 - ii. 在**目录文件路径**框中，输入目录文件位置的完整文件路径。示例路径：*compute/catalog.xml*。
- HTTPS
 - i. 在**共享地址**框中，输入在网络上存储固件目录的系统的 IP 地址。
 - ii. 在**目录文件路径**框中，输入目录文件位置的完整文件路径。示例路径：*compute/catalog.xml*。
 - iii. 在**用户名**框中，输入存储目录所在设备的用户名。
 - iv. 在**密码**框中，输入存储目录的设备的密码。
 - v. 选择**证书检查**复选框。

存储目录文件的设备的真实性已验证，并在**证书信息**对话框中生成和显示安全证书。

- d. 在您输入**共享地址**和**目录文件路径**后，将会显示**立即测试**链接。要验证与目录的连接，请单击**立即测试**。如果建立了与目录的连接，将会显示**连接成功**消息。如果未建立与共享地址或目录文件路径的连接，将会显示**连接到路径失败**错误消息。此步骤为可选。
 - e. 在**更新目录**框中，选择**手动**或**自动**。
如果选择**更新目录**为**自动**，请选择更新频率是**每天**还是**每周**，并以 12 小时制输入时间。
3. 单击**完成**。只有在您输入了对话框中的所有字段之后，**完成**按钮才会显示出来。
一个新的固件目录将会创建并列在**目录管理**页面上的目录表中。
 4. 要返回**固件/驱动程序合规性**页面，请单击**返回到固件/驱动程序合规性**。


相关任务

[删除目录](#) 页面上的 67

SSL 证书信息

可从 Dell 支持网站、Dell EMC Repository Manager (Repository Manager) 或组织网络内部网站下载固件和驱动程序更新的目录文件。

如果选择从组织网络内部网站下载目录文件，则可接受或拒绝 SSL 证书。可在**证书信息**窗口中查看 SSL 证书的详细信息。此信息包含有效期、证书颁发机构和向其颁发证书的实体的名称。

 **注：**从**创建基线**向导创建目录的情况下，才会显示**证书信息**窗口。

操作

接受	接受 SSL 证书，并允许您访问网站。
取消	关闭 证书信息 窗口而不接受 SSL 证书。

更新目录

可通过 Dell.com 网站（基本位置）更新现有的固件和驱动程序目录。

要更新目录，请执行以下操作：

1. 在“目录管理”页面上，选择一个目录。
2. 单击**检查更新**按钮，其位于**目录管理**页面的右侧窗格中。
3. 单击**是**。

如果所选目录是联机目录，它将被在 Dell.com 站点中维护的最新版本取代。对于本地网络目录，考虑使用基本位置中可用的所有最新固件和驱动程序来计算基线合规性。

编辑目录

1. 在**目录管理**页面上，选择一个目录。
目录详细信息显示在 <目录名称> 右窗格中。
2. 单击右侧窗格中的**编辑**。
3. 在**编辑更新目录**向导中编辑属性。
您不可编辑的属性显示为灰色。有关字段定义，请参阅[通过使用 Dell.com 添加目录](#) 页面上的 65 和 [向本地网络添加目录](#) 页面上的 65。
4. 输入**共享地址** 和 **目录文件路径**，此时会显示**立即测试** 链接。要验证与目录的连接，请单击**立即测试**。如果建立了与目录的连接，将会显示 Connection Successful 消息。如果未建立与共享地址或目录文件路径的连接，将会显示 Connection to path failed 错误消息。此步骤为可选。
5. 在**更新目录框**中，选择**手动**或**自动**。
如果选择**更新目录** 为**自动**，请选择更新频率是**每天** 还是**每周**，并以 12 小时制输入时间。
6. 单击**完成**。
立即创建并运行作业。**目录管理**页面的**存储库位置**列中显示作业状态。

删除目录

1. 在**目录管理**页面上，选择目录，然后单击**删除**。
此时会从列表中删除目录。
2. 要返回**固件/驱动程序合规性**页面，请单击**返回到固件/驱动程序合规性**。

注：如果目录链接到基线，则无法删除目录。

相关信息

[向本地网络添加目录](#) 页面上的 65

创建固件/驱动程序基线

基线是与固件/驱动程序目录关联的一批设备或一组设备。创建基线的目的是，依照目录中指定的版本，对该基线中的设备的固件和驱动程序进行合规性评估。要创建基线，请执行以下操作：

注：

- 要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
- 设备管理者用户只能查看和管理相应设备管理者创建并拥有的固件/驱动程序基线。此外，在创建基线时，仅显示在设备管理者范围内的目标组或设备（支持固件更新）。
- 升级到版本 3.6.x 后，仅将设备管理者在任何先前的 OpenManage Enterprise 版本中创建的任何固件/驱动程序基线分配给管理员。因此，设备管理者必须在升级后从先前版本重新创建固件/驱动程序基线。
- 固件和/或驱动程序版本早于目录版本的不合规设备不会自动更新。您必须更新固件版本。建议在维护期内更新设备固件，以防设备或环境在工作时间脱机。

1. 在**固件**下，单击**创建基线**。
2. 在**创建更新基线**对话框中：
 - a. 在**基线信息**部分：
 - i. 从**目录**下拉菜单中，选择一个目录。
 - ii. 要将目录添加到此列表，单击**添加**。请参阅[管理固件目录](#)。
 - iii. 在**基线名称**框中，输入一个基线名称，然后输入基线说明。
 - iv. 单击**下一步**。
 - b. 在**目标**部分：

- 要选择目标设备：
 - i. 选择**选择设备**，然后单击**选择设备**按钮。
 - ii. 在**选择设备**对话框中，OpenManage Enterprise 监测的所有设备、IOM 以及静态或查询组下面的设备都将显示在相应的组中。
 - iii. 在左侧窗格中，单击类别名称。该类别的设备将显示在工作窗格中。
 - iv. 选择与设备对应的复选框。选定的设备将在**所选设备**选项卡中列出。
 - 要选择目标设备组：
 - i. 选择**选择组**，然后单击**选择组**按钮。
 - ii. 在**选择组**对话框中，OpenManage Enterprise 监控的所有设备、IOM 以及静态或查询组下面的设备都将显示在相应的类别中。
 - iii. 在左侧窗格中，单击类别名称。该类别的设备将显示在工作窗格中。
 - iv. 选择与组对应的复选框。选定的组将在**所选组**选项卡中列出。
3. 单击**完成**。
将显示一条消息，指明已为创建基线创建作业。
在“基线”表中，将显示有关设备和基线作业的数据。有关字段定义，请参阅[固件基线字段定义](#) 页面上的 150。

删除配置合规性基线

您可以在**配置 > 配置合规性**页面上删除配置合规性基线，并从关联的基线中取消链接设备。

注：要对 OpenManage Enterprise 执行任何任务，您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14

要删除配置合规性基线，请执行以下操作：

1. 从“配置合规性”页面上列出的基线中选择基线。
2. 单击**删除**，并在确认提示窗口单击**是**。

已删除的配置基线将从“配置合规性”页面中删除。

编辑基线

配置 > 固件/驱动程序合规性页面上的基线可按如下方式编辑：

1. 选择一个基线，然后单击右侧窗格中的**编辑**。
2. 按照[创建固件基线](#)中所描述的修改数据。
更新的信息将显示在上部的网格中。
3. 要返回**固件/驱动程序合规性**页面，请单击**返回到固件/驱动程序合规性**。

检查设备固件和驱动程序的合规性

在**配置 > 固件/驱动程序合规性**页面上，您可以根据关联的目录检查基线设备的固件和驱动程序的合规性，查看报告，并更新不合规设备的固件和驱动程序。

注：

- 要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
- 基线中不合规设备的固件和驱动程序（64 位 Windows）不会自动更新，必须由用户进行更新。建议在维护期内更新设备固件和驱动程序，以防设备或环境在工作时间脱机。
- 要收集资源清册信息，Windows 服务器上必须有资源清册收集器和 Dell System Update。如果服务器上没有这些组件，则启动资源清册作业，然后选择**收集驱动程序资源清册**。查找作业还会收集驱动程序资源清册信息，但只有资源清册作业会在服务器上安装必要的组件。要收集驱动程序资源清册信息，请创建或编辑资源清册作业，然后选择**收集驱动程序资源清册**复选框。有关更多信息，请参阅[创建资源清册作业](#) 页面上的 61 和[编辑资源清册计划作业](#) 页面上的 63。

1. 选择与基线对应的复选框，然后单击**检查合规性**。
此时会运行基线合规性作业。

注: 如果设备未与目录关联, 则不验证合规性。仅为合规性表中关联并列出的设备创建作业。要将设备与目录关联, 请参阅 [创建固件基线](#)。

在“基线”表中, 将显示有关设备和基线作业的数据。有关字段定义, 请参阅 [固件基线字段定义](#) 页面上的 150。

2. 要查看合规性报告并升级设备的固件和驱动程序版本, 请单击右侧窗格中的 **查看报告**。

请参阅 [查看设备固件合规性报告](#)。

注: 不支持驱动程序回滚。

查看基线合规性报告

在 **配置 > 固件/驱动程序合规性** 页面上, 显示了基线的合规性状态。环形图提供了基线与其相应目录的符合性的摘要。当多个设备与一个基线关联时, 与基线的符合性最差的设备的状态被指示为该基线的合规性级别。例如, 其中只有一个设备的合规性为“严重”

的基线的合规性级别表示为“严重” , 即使大多数设备都合规也是如此。

您可以查看与基线相关联的各个设备的固件和驱动程序合规性, 并选择升级或降级该设备上的固件和/或驱动程序版本。要查看基线合规性报告:

- 选择与基线对应的复选框, 然后单击右窗格中的 **查看报告**。

在 **合规性报告** 页面上将会显示与基线相关联的设备列表及其合规性级别。默认情况下, 会显示处于 **严重** 和 **警告** 状态的设备。

注: 如果每台设备都有自己的状态, 则最高严重性状态将被视为该组的状态。有关“汇总运行状况”状态的更多信息, 请参阅 Dell 技术中心上提供的 [在 Dell EMC 第 14 代及更高代别的 POWEREDGE 服务器上使用 iDRAC 管理汇总运行状况状态白皮书](#)。

- 合规性:** 表示设备的合规性级别符合基线。有关用于设备固件/驱动程序合规性级别的符号的更多信息, 请参阅 [管理设备固件和驱动程序](#) 页面上的 64。

- 类型:** 生成合规性报告的设备类型。

- 设备名称/组件:** 默认情况下将会显示设备的服务标签。

- 要查看有关设备中组件的信息, 请单击 > 符号。

将会显示组件及其符合目录合规性的列表。


注: 对于完全符合关联固件基线的所有设备 (MX7000 机箱除外), 不显示 > 符号。

- 选择与固件合规性状态为“严重”且需要更新的设备对应的一个或多个复选框。

- 单击 **使合规**。请参阅 [使用基线合规性报告更新设备固件版本](#)。

- 服务标签:** 在 **<设备名称>** 页面上查看有关该设备的完整信息。有关可以在该页面上完成的任务的详细信息, 请参阅 [查看和配置各个设备](#) 页面上的 56。

- 重新启动要求:** 指示在更新固件后是否必须重新启动设备。

- 信息** : 与每个设备组件相对应的符号链接到可以从中更新固件/驱动程序的支持站点页面。单击此项以打开支持站点上相应的“驱动程序详细信息”页面。

- 当前版本:** 表示设备上固件的当前版本。

- 基线版本:** 表示关联目录中可用设备的相应固件和驱动程序版本。



- 要将合规性报告导出到 Excel 文件, 请选择与设备对应的复选框, 然后选择 **导出**。

- 要返回 **固件** 页面, 请单击 **返回固件**。

- 要根据列按列数据, 请单击列标题。

- 要在表格中搜索设备, 请单击 **高级筛选器**, 然后在筛选器框中选择或输入数据。请参阅 [OpenManage Enterprise 图形用户界面概述](#) 页面上的 29 中的“高级筛选器”。

使用基线合规性报告更新固件和/或驱动程序

运行固件或驱动程序合规性报告后，如果设备上的固件或驱动程序版本早于目录上的版本，则“合规性报告”页面会将设备固件或驱动程序状态指示为“升级”（ 或者 ）。

关联基线设备的固件和驱动程序版本不会自动更新，因此，用户必须启动更新。建议在维护期内更新设备固件和/或驱动程序，以防设备或环境在工作时间脱机。

设备管理者只能在其范围内的设备上运行固件/驱动程序更新。

注： 如果通过机箱设备管理对机箱存储底座进行管理，则 OpenManage Enterprise 中不支持机箱存储底座上的资源清册收集和固件更新。

前提条件：

- 要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
- 您必须创建入站防火墙规则，允许与端口 22 进行通信。
- 如果使用代理设置配置了 HTTP 和 HTTPS 共享，请在启动任何更新任务之前，确保这些本地 URL 包含在代理例外列表中。
- 在给定时间，只能在目标机器上启动一个更新任务。

注：

- MCM 机箱下处于“代理”启用状态的设备和仅更新设备驱动程序不支持重设 iDRAC 功能。有关管理作业的更多信息，请参阅 [启用设备](#) 页面上的 37。
- 网络交换机、模块化 IOA 和戴尔存储设备的固件或驱动程序合规性状态显示为“未知”，因为它们无法使用戴尔目录进行更新。推荐使用各自的单独更新软件包为这些设备执行单独的固件或驱动程序更新。要执行单独的固件或驱动程序更新，请在所有设备页面上选择一个设备，然后单击 [查看详细信息](#) > [固件/驱动程序](#) 并选择单个软件包选项。有关不受支持设备列表的详细信息，请参阅 [固件/驱动程序合规性基线报告 - 具有“未知”合规状态的设备](#) 页面上的 154

如果使用低于 1.30.00 的 OpenManage Enterprise-Modular 版本管理多机箱管理 (MCM) 组，则在更新 MX7000 机箱和底座的固件和/或驱动程序之前，必须考虑以下事项：

- 机箱和底座固件更新必须分别进行。
- 更新所有成员机箱后，作为最后一步，单独更新主机箱。
- 一次最多可为 9 个成员机箱更新固件。
- 无论启用状态是什么（受管或代理），一次最多支持 43 个底座的固件更新。

驱动程序更新仅在作为 64 位 Windows 服务器而查找到的设备上可用。在更新驱动程序之前，请执行以下操作：

- 请注意，不支持回滚驱动程序更新。
- 仅支持在使用 OpenSSH 的 Windows 上的带内驱动程序更新。不支持在 Windows 上托管的第三方 SSH（如 CygwinSSH）上的驱动程序更新。
- 要收集资源清册信息，Windows 服务器上必须有资源清册收集器和 Dell System Update。如果服务器上没有这些组件，则启动资源清册作业，然后选择 [收集驱动程序资源清册](#)。查找作业还会收集驱动程序资源清册信息，但只有资源清册作业会在服务器上安装必要的组件。要收集驱动程序资源清册信息，请创建或编辑资源清册作业，然后选择 [收集驱动程序资源清册](#) 复选框。有关更多信息，请参阅 [创建资源清册作业](#) 页面上的 61 和 [编辑资源清册计划作业](#) 页面上的 63。

要使用基线合规性报告更新设备固件和/或驱动程序，请执行以下操作：

1. 在 [配置](#) > [固件/驱动程序合规性](#) 页面上，选择与设备关联的基线对应的复选框，然后在右窗格中单击 [查看报告](#)。

在 [合规性报告](#) 页面上，将会显示与基线相关联的设备列表及其合规性级别。有关字段说明，请参阅 [查看基线合规性报告](#) 页面上的 69。

2. 选择与固件或驱动程序必须要更新的设备对应的复选框。您可以选择多个类似属性的设备。

3. 单击 [使合规](#)。

4. 在 [使设备合规](#) 对话框中，您可以执行以下操作：

- 在 [计划更新](#) 下，单击 [其他信息](#) 以查看重要信息，然后选择下面其中一项：

- a. **立即更新**：立即应用固件/驱动程序更新。

- b. **以后计划**：选择以指定固件和/或驱动程序版本必须更新的日期和时间。如果不想打扰当前的任务，建议您使用此模式。

- 在 [服务器选项](#) 下，选择以下重新启动选项之一：

- a. 要在固件/驱动程序更新后立即重新启动服务器，请选择 **立即重新启动服务器**，然后从下拉菜单中选择下面其中一项：

- i. **正常重新引导而不强制关机**

- ii. **正常重新引导并强制关机**

- iii. **关机后重新开机**，用于设备的硬重置。

- b. 选择 **下一个服务器重新引导阶段**，以在下次重新启动服务器时触发固件/驱动程序更新。

注: 如果使用“下一个服务器重新引导阶段”选项创建固件/驱动程序更新作业，则必须在将程序包安装到远程设备后手动执行资源清册和基线检查。

- **清除作业队列:** 选择此项，可在启动更新作业之前删除目标设备上的所有作业（已计划、已完成和已失败）。

注: 更新驱动程序不支持此功能。

- **重置 iDRAC:** 选择此项，可在启动更新作业之前启动 iDRAC 重新引导。

注: 更新驱动程序不支持此功能。

5. 单击**更新**。

此时创建固件/驱动程序更新作业，以更新设备的固件和/或驱动程序。您可以在**监视 > 作业**页面中查看作业的状态。

管理设备部署模板

通过 OpenManage Enterprise 中的设备部署模板，您可以设置服务器和机箱的配置属性，例如 BIOS、启动、网络属性等。

部署模板是系统配置设置（称为属性）的整合。部署模板允许快速、自动配置多个服务器或机箱，而不存在人为错误的风险。

模板使您能够优化数据中心资源，并缩短创建克隆和部署的周期时间。模板还增强了使用软件定义基础架构的融合基础架构中的关键业务级操作。

您可以使用预定义的部署模板，或者从参考设备或现有模板文件导入部署模板。要查看现有模板的列表，请从 OpenManage Enterprise 菜单中，单击**配置 > 模板**。

要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。[OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

设备管理者可以查看和执行默认模板上的任务，但只能查看和执行该设备管理者拥有的自定义模板上的任务。

主题：

- [要从参考设备创建部署模板](#)
- [导入模板文件创建部署模板](#)
- [查看部署模板信息](#)
- [编辑服务器部署模板](#)
- [编辑机箱部署模板](#)
- [编辑 IOA 部署模板](#)
- [编辑部署模板的网络属性](#)
- [部署设备部署模板](#)
- [部署 IOA 部署模板](#)
- [克隆部署模板](#)
- [在尚待发现的服务器或机箱上自动部署配置](#)
- [创建自动部署目标](#)
- [删除自动部署目标](#)
- [将自动部署目标详细信息导出为不同的格式](#)
- [无状态部署概览](#)
- [定义网络](#)
- [编辑或删除配置的网络](#)
- [导出 VLAN 定义](#)
- [导入网络定义](#)

要从参考设备创建部署模板

注：要对 OpenManage Enterprise 执行任何任务，您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

注：请确保先在 **SMB 设置** 中启用 SMBv1，然后才能在任何机箱上或具有 iDRAC 版本 2.50.50.50 及更早版本的 PowerEdge YX2X 和 YX3X 服务器上开始任何任务。请参阅 [管理控制台首选项](#) 页面上的 137 和 [Dell EMC PowerEdge 服务器的通用命名惯例](#) 页面上的 154。

您可以通过使用参考设备或从现有部署模板导入来创建或编辑部署模板。通过使用参考设备来创建：

1. 从 **OpenManage Enterprise** 菜单中，单击**配置 > 模板 > 创建模板**，然后选择**从参考设备**。
2. 在**创建模板**对话框中：
 - a. 在**模板信息**部分中，输入部署模板的名称和说明。
 - b. 选择部署模板类型：
 - **克隆参考服务器：**使您可以克隆现有服务器的配置。
 - **克隆参考机箱：**使您可以克隆现有机箱的配置。

- **克隆参考 IOA**：使您可以克隆现有 M I/O 聚集器的配置。

注：IOA 模板中属性不可编辑。只有 IOA 模板的**名称**和**说明**可编辑。

c. 单击**下一步**。

d. 在**参考设备**部分，单击**选择设备**以选择其配置属性必须用于创建新部署模板的设备。有关选择设备的更多信息，请参阅**选择目标设备和设备组**。

注：您只能选择一种设备作为参考设备。

注：只能克隆在机箱查找时间提取的 IOA 模板。请参阅 **创建服务器的自定义设备查找作业协议 - 查找协议的附加设置** 页面上的 41

e. 在**配置元素**部分，选择与您必须要克隆的设备元素对应的复选框。要通过使用服务器作为设备创建部署模板，您可以选择克隆服务器属性，例如 iDRAC、BIOS、Lifecycle Controller 和事件筛选器。默认情况下，将选择所有元素。

f. 单击**完成**。

创建成功后，作业将显示在列表中。部署模板创建作业已启动，状态显示在**状态**列中。

作业信息也会显示在**监测 > 作业**页面中。要查看作业的附加详细信息，请选择作业，然后单击工作窗格中的**查看详细信息**。在**作业详细信息**页面中，将显示作业的执行详细信息。在**结果**窗格中，单击**查看详细信息**以查看作业执行的详细信息。

导入模板文件创建部署模板

注：请确保先在 **SMB 设置**中启用 SMBv1，然后才能在任何机箱上或具有 iDRAC 版本 2.50.50.50 及更早版本的 PowerEdge YX2X 和 YX3X 服务器上开始任何任务。有关详情，请参阅**管理控制台首选项** 页面上的 137 和 **Dell EMC PowerEdge 服务器的通用命名惯例** 页面上的 154。

1. 从 **OpenManage Enterprise** 菜单中，单击**配置 > 模板 > 创建模板**，然后选择**从文件导入**。

2. 在**导入模板**对话框中：

- a. 输入新部署模板的名称。
- b. 单击**选择文件**，然后选择模板文件。
- c. 选择**服务器、机箱**或 **IOA** 以指明模板类型。

3. 单击**完成**。

将导入现有模板文件的属性并创建新部署模板。

● 要查看部署模板的信息，请选择复选框，然后单击右侧窗格中的**查看详细信息**。在**模板详细信息**页中，您可以部署或编辑部署模板。请参阅**部署设备部署模板** 页面上的 75 和 **要从参考设备创建部署模板** 页面上的 72。

● 要编辑部署模板：

1. 选择相应的复选框，然后单击**编辑**。
2. 在**编辑模板**对话框中，编辑部署模板名称，然后单击**完成**。更新的信息将显示在部署模板列表中。

查看部署模板信息

预定义、用户创建或克隆的设备部署模板列表将显示在**配置 > 模板**下。

1. 在部署模板列表中，选择与所需设备模板对应的复选框。

2. 在工作窗格中，单击**查看详细信息**。

在**模板详细信息**页面上，将显示部署模板名称、说明、用于创建部署模板的参考设备以及 OpenManage Enterprise 用户信息的上次更新日期。

3. 右键单击元素以展开或折叠**配置详细信息**部分中的所有子元素，从而显示用于创建部署模板的所有属性。您也可以展开特定于父元素的各个子元素。例如，如果您选择了 iDRAC 和 BIOS 元素必须用于目标设备上的克隆，则仅显示与这些元素相关的属性。

编辑服务器部署模板

内置部署模板不可编辑。只能编辑由用户创建且标识为“自定义”的部署模板。无论您是使用参考模板文件还是参考设备创建模板的，都可以编辑部署模板的属性。

1. 在**配置 > 模板**页面上，选择要求的自定义模板复选框，然后单击**编辑**。

2. 在**编辑模板**对话框中：

- a. 在**模板信息**部分，编辑部署模板名称和说明。无法编辑模板类型。

- b. 单击**下一步**。
- c. 在**编辑组件**部分中，将会在以下视图中显示部署模板属性：
 - **指导式视图** — 此属性视图仅显示按功能分组的通用属性。将显示以下类别的属性：
 - i. 在 **BIOS 设置**部分中，选择以下选项之一：
 - **手动**：可让您手动定义以下 BIOS 属性：
 - **系统配置文件**：从下拉菜单中，选择此选项可指定要在系统配置文件中实现的性能优化的类型。
 - **用户可访问的 USB 端口**：从下拉菜单中，选择此选项可指定用户可以访问的端口。
 - 默认情况下，使用逻辑处理器和带内可管理性均已启用。
 - **基于工作负载优化**：从下拉菜单中选择工作负载配置文件，选择此选项可指定您想要在配置文件上实现的工作负载性能优化的类型。
 - ii. 单击**引导**并定义引导模式：
 - 如果您选择 BIOS 作为引导模式，请执行以下操作：
 - 要重试引导顺序，请选中**已启用**复选框。
 - 拖动项目以设置引导顺序和硬盘驱动器顺序。
 - 如果您选择 UEFI 作为引导模式，则拖动项目以设置 UEFI 引导顺序。如果需要，选中该复选框以启用“安全引导”功能。
 - iii. 单击**网络**。与部署模板关联的所有网络都显示在**网络接口**下面。
 - 要使可选标识池与部署模板关联，请从**标识池**下拉菜单中选择。将显示与所选标识池关联的网络。如果在高级视图中编辑部署模板，则会对此部署模板禁用标识池选择。
 - 要查看网络属性，请展开网络。
 - 要编辑属性，请单击相应的笔形符号。
 - 选择要用于引导的协议。仅当您的网络支持该协议时才选择。
 - 选择要与网络关联的未标记的和已标记的网络
 - 将会显示我们早先创建的部署模板（配置文件）中的分区、最大带宽和最小带宽。
 - 单击**完成**。将会保存部署模板的网络设置。
 - **高级视图** — 此视图会列出可更改的所有部署模板属性（包括在指导式视图中显示的属性）。通过此视图，您不仅可以指定属性值（如指导式视图），而且可以指定将部署模板部署到目标设备时是否包含每个属性。

属性将按功能分组进行显示。特定于供应商的属性分组到其他属性下。显示每个单独的属性时，属性名称前面都会带有复选框。该复选框指示将部署模板部署到目标设备时是否包含此属性。由于属性依赖关系，如果您更改了关于是否部署特定属性的设置，可能会在目标设备上造成意外结果，或导致部署失败。每个组的名称左侧还有一个复选框。组复选框中的图标包含以下三个值之一：

- i. 选中 — 表示选择部署组中的所有属性。
- ii. 连字符 — 表示选择部署部分（但不是全部）属性。
- iii. 清除 — 表示未选择部署组中的任何属性

i 注：

- 使用此选项时务必谨慎，您需要熟悉属性以及属性之间的依赖关系，因为许多属性都要依靠其他属性中的值来确定自身行为。
- 您可以单击组图标，以切换组中所有属性的部署设置。
- 具有安全信息（如密码）的属性将隐藏，并在最初加载时显示为“空”，并且对这些安全属性值的更改不会显示。
- 如果配置文件已与部署模板关联，则无法更改模板的关联标识池。

3. 单击**下一步**。
在**摘要**部分中，将会显示您使用指导式和高级模式编辑的属性。
4. 这部分是只读字段。通读这些设置，然后单击**完成**。
更新的模板属性将保存到部署模板。

编辑机箱部署模板

可通过 OpenManage Enterprise 编辑机箱部署模板。

i 注：

- 要编辑机箱部署模板，您必须具有管理员或设备管理员的权限。有关更多详情，请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
- 无法在 MX7000 机箱和机箱管理控制器 (CMC) 部署模板上设置用户密码。

要编辑机箱部署模板：

1. 选择 **OpenManage Enterprise > 配置 > 模板** 以获取部署模板的列表。
2. 选择与所需机箱模板对应的复选框，然后单击 **编辑**。确保该部署模板标识为“自定义”。
3. 编辑 **模板信息** 部分中的 **模板名称和说明**。不能编辑 **模板类型**。
4. 单击 **下一步**。
5. 在 **高级视图** 下的 **编辑组件** 部分中，您可以选择或取消选择要包括在部署模板中或从模板中排除的属性。
6. 单击 **下一步**。
7. 您可以在 **摘要** 下查看对属性所做的更改。已更改属性旁边会显示一个圆圈。
8. 单击 **完成** 以保存对机箱部署模板所做的更改。

编辑 IOA 部署模板

IOA 部署模板中属性不可编辑。只有 IOA 部署模板的 **名称和说明** 可编辑。

注：

IOA 模板属性不能在一体机之外进行编辑，因为在部署过程中模板将被视为损坏的文件。

编辑部署模板的网络属性

在 **配置 > 模板** 页面上，您可以编辑包含适用 NIC 属性的部署模板的网络配置。

选择部署模板后，单击 **编辑网络** 以激活编辑网络向导并执行以下操作：

注： 即使 MX7000 机箱超出范围，也允许设备管理者在范围内“代理的”MX7000 底座上进行 VLAN 设置。

1. 单击 **IO 池分配**，并从 **标识池** 列表中选择部署模板的标识池。单击 **下一步**。
2. 在 **带宽** 部分中，编辑关联 NIC 的 **最小带宽 (%)** 和 **最大带宽 (%)**，然后单击 **下一步**。

注： 带宽设置仅适用于分区 NIC。
3. 在 **VLAN** 部分中（仅适用于模块化系统）：
 - a. 选择适当的 **NIC 组合** 选项。
 - b. 选中 **立即传播 VLAN 设置** 复选框，以便在不需要重新启动服务器的情况下立即在关联的模块化系统服务器上传播更改的 VLAN 设置。单击 **查看详细信息** 以查看受影响的设备。

注：

 - 仅当部署模板部署后，才能 **立即传播 VLAN 设置**。
 - 在传播 VLAN 设置之前，请确保已为结构中的模块化系统服务器创建了网络配置文件。
 - 如果选中了 **立即传播 VLAN 设置** 复选框，则会创建名为 **VLAN 传播** 的作业以应用更改。可以在 **监测 > 作业** 页面上检查作业的状态。
 - c. 选中 **使用严格检查** 复选框以匹配具有类似特征的 VLAN。如果未选中，则仅 VLAN 名称和 QoS 用于匹配。

注： 此选项仅适用于模块化系统底座。
 - d. 根据需要更改关联 NIC 的 **未标记网络** 和 **已标记网络** 的属性。
4. 单击 **完成** 以应用更改。

部署设备部署模板

您可以部署一个部署模板，该模板将包含一组特定设备的配置属性。在设备上部署设备部署模板可确保以一致的方式配置设备。

注：

- 要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
- 如果设备管理者正在部署模板，则仅显示该设备管理者范围内且可进行部署的目标组和设备。

在开始部署设备部署模板之前，请确保：

- 您已创建设备部署模板或克隆示例部署模板。请参阅[要从参考设备创建部署模板](#) 页面上的 72。
- 目标设备符合 [部署 OpenManage Enterprise 的最低系统要求](#) 页面上的 18 中指定的要求。
- 目标设备上已安装 OpenManage Enterprise 高级许可证。

小心：请确保只选择合适的设备进行部署。在重新利用和裸机设备上部署部署模板后，可能无法将设备恢复为其原始配置。

注：在部署 MX7000 机箱模板期间：

- 目标设备只能是主 MX7000 机箱。
- 如果从组中移除某个 MX7000 机箱，则必须在 OpenManage Enterprise 中重新发现它。
- MX7000 机箱上的用户将替换为在模板中配置的用户。
- 导入的 Active Directory 设置将替换为机箱配置文件中的值。

1. 从**部署 > 模板**的模板列表中，选中与要部署的部署模板对应的复选框，然后单击**部署模板**。

2. 在**部署模板：<模板名称>**对话框的**目标**下：

- a. 单击**选择**，然后选择**作业目标**对话框中的设备。请参阅[选择目标设备和设备组](#)。
- b. 在部署设备部署模板期间，配置更改可能需要强制重新引导服务器。如果您不想重新引导服务器，请选择**不强制重新引导主机操作系统**选项。
在选择**不强制重新引导主机操作系统**选项时，将尝试正常重新引导服务器。如果重新引导失败，您必须重新运行模板部署任务。
- c. 选中**使用严格检查**复选框以匹配具有类似特征的 VLAN。如果未选中，则仅 VLAN 名称和 QoS 用于匹配

注：仅当所选目标设备为模块化系统底座时，才会显示此选项。

d. 单击**下一步**。

3. 如果目标设备是服务器，则在**引导至网络 ISO**部分中：

- a. 选择**引导至网络 ISO**复选框。
- b. 选择 **CIFS** 或 **NFS** 作为共享类型，然后在 ISO 图像文件路径和存储 ISO 图像文件的共享位置等字段中输入信息。按照工具提示输入正确的语法。
- c. 选择**连接 ISO 的时间**下拉菜单选项，以设置网络 ISO 文件保持映射到目标设备的小时数。默认情况下，此值设置为 4 小时。
- d. 单击**下一步**。

4. 在**iDRAC 管理 IP**部分中，更改目标设备 IP 设置（如果需要），然后单击**下一步**。

注：

- 如果在模板部署期间将 DHCP 设置分配给最初使用静态 IP 查找到的目标设备，模板部署将会失败。
- 如果未在已查找到的 MX7000 底座上配置 IP 设置，则在模板部署期间，“引导至网络 ISO”操作无法正常工作。

5. 在**目标属性**部分中，可以在部署此部署模板之前更改特定于每个所选目标设备（例如位置属性和 IP 地址）的非虚拟标识属性。部署模板时，这些更改的目标属性仅在特定设备上实施。要更改特定于设备的非虚拟标识属性，请执行以下操作：

- a. 从显示先前选择的目标设备的列表中选择目标设备。
- b. 展开属性类别，然后选择或清除在目标设备上的模板部署过程中必须包含或排除的属性。
- c. 单击**下一步**。

6. 在**虚拟标识**部分中，单击**保留标识**。

此时会显示所选目标设备的 NIC 卡的已分配虚拟标识。要查看所选目标设备的身份标识池的所有已分配标识，请单击**查看所有 NIC 详细信息**。

注：如果已在设备外部分配标识，则除非将其清除，否则新部署将不会使用这些标识。有关更多信息，请访问 [标识池](#) 页面上的 80

7. 在**计划**部分，立即或计划以后运行作业。请参阅[计划作业字段定义](#) 页面上的 150。

8. 单击**完成**。查看警告消息并单击**是**。

设备配置作业创建完毕。请参阅[使用作业进行设备控制](#) 页面上的 106。

部署 IOA 部署模板

注：要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

在开始部署 IOA 部署模板之前，请确保：

- 您已经为部署创建了 IOA 部署模板。请参阅[要从参考设备创建部署模板](#) 页面上的 72。

- 目标设备符合 [部署 OpenManage Enterprise 的最低系统要求](#) 页面上的 18 中指定的要求。
- 目标设备的固件版本与 IOA 部署模板相同。
- 仅支持以下跨模板部署：

表. 14: 支持的跨模板部署

IOA 部署模板模式	目标的受支持 IOA 模板模式
独立	独立, PMUX
PMUX (可编程 MUX)	PMUX, 独立
VLT	VLT

 **小心:** 请确保只选择合适的设备进行部署。在重新利用和裸机设备上部署部署模板后，可能无法将设备恢复为其原始配置。

1. 从 **配置 > 模板** 上的部署模板列表中，选中与要部署的 IOA 模板对应的复选框，然后单击 **部署模板**。
2. 在 **部署模板: <模板名称>** 对话框的 **目标** 下：
 - a. 单击 **选择**，然后选择 **作业目标** 对话框中的设备。请参阅 [选择目标设备和设备组](#)。
 - b. 单击 **确定**。
3. 在 **主机名** 对话框中，您可以更改目标 IOA 设备的 **主机名**。单击 **下一步**。
4. 在 **高级选项** 对话框中，选择 **预览模式** 以模拟部署，或者选择 **在警告时继续** 以部署模板并忽略遇到的警告。单击 **下一步**。
5. 在 **计划** 部分，立即或计划以后运行作业。请参阅 [计划作业字段定义](#) 页面上的 150。
6. 单击 **完成**。查看警告消息并单击 **是**。
在作业下创建设备配置作业。请参阅 [使用作业进行设备控制](#) 页面上的 106。

克隆部署模板

1. 在 **OpenManage Enterprise** 菜单的 **配置** 下面，单击 **模板**。
将显示可用部署模板的列表。
2. 选中要克隆的模板的对应复选框。
3. 单击 **克隆**。
4. 输入新部署模板的名称，然后单击 **完成**。
克隆部署模板将会创建并显示在部署模板列表中。

在尚待发现的服务器或机箱上自动部署配置

可将 OpenManage Enterprise 中现有的部署模板分配给正在等待发现的服务器和机箱。当发现目标设备并配置入网时，这些部署模板自动部署到各自的设备上。

要访问 **自动部署** 页面，请单击 **OpenManage Enterprise > 配置 > 自动部署**。

此时会显示自动部署目标及其相应 **标识符**（服务标签或节点 ID）、**模板名称**、**模板类型**、**状态** 和 **引导至网络 ISO 状态**（针对服务器）。

可以使用列表顶部的高级筛选器 字段自定义 **自动部署** 目标列表。

“自动部署”页面的右侧区域显示所选自动部署目标的 **创建日期** 和 **创建者** 详细信息。当选择了多个项目时，该区域中显示最后选取项目的详细信息。

查找到自动部署目标后，将自动删除其在“自动部署”页面中的条目，并将其移至“所有设备”页面。此外，还会在“配置文件”页面上创建一个配置文件，其中包含设备的配置设置。

可以在“自动部署”页面上执行下列操作：

- **创建** 用于自动部署的模板。请参阅 [创建自动部署目标](#) 页面上的 78
- **删除** 不需要的模板。请参阅 [删除自动部署目标](#) 页面上的 78
- 将自动部署模板 **导出** 为不同的格式。请参阅 [将自动部署目标详细信息导出为不同的格式](#) 页面上的 79

注:

- 只有管理员才能在自动部署模板上执行创建、删除和导出任务。设备管理者只能“导出”自动部署模板。有关更多信息，请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

创建自动部署目标

注: 要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14

要创建自动部署目标，请执行以下操作：

1. 单击 **OpenManage Enterprise > 配置 > 自动部署 > 创建**
此时将显示**自动部署模板**向导。
2. 在**模板信息**页面上，选择部署模板类型（服务器或机箱）。
3. 从**选择模板**下拉菜单中，选择合适的模板。如果选择的模板具有未与任何虚拟身份标识池关联的身份标识属性，则会显示以下消息：*选择的模板具有身份标识属性，但尚未与虚拟身份标识池关联。部署此模板不会更改目标设备上的虚拟网络地址。*
4. 单击下一步。
此时将显示**目标信息**页面。
5. 在**目标信息**页面上，可以采用以下方法之一选择目标设备：
 - **手动输入**：输入服务标签或节点 ID 以标识目标设备。尽管可以按任何顺序输入标识符，但标识符必须用逗号进行分隔。单击“验证”以验证值的准确性。验证标识符是必选操作。
 - **导入 CSV**：单击**导入 CSV**，浏览文件夹并选择含有目标设备详细信息的相应 .csv 文件。此时将显示成功导入和无效条目数量的摘要。要查看导入结果的更详细视图，请单击**查看详细信息**。
CSV 文件中的条目必须采用以下格式：标识符必须在第一列中列出，每行一个，从第二行开始。对于模板 CSV 文件，请单击**下载样本 CSV 文件**。
6. 单击**下一步**。
7. 在**目标组信息**页面上，在**静态组**下（如果可用）指定一个子组。有关设备分组的更多信息，请参阅[将设备按组整理](#)页面上的 46。目标设备将放置在其查找上指定的目标组下
8. 单击**下一步**。
9. 如果目标设备是服务器，则在**引导至网络 ISO**页面上：
 - 选择**引导至网络 ISO**复选框。
 - 选择 **CIFS** 或 **NFS**。
 - 输入 ISO 映像文件存储位置的 **ISO 路径**。按照工具提示输入正确的语法。
 - 输入 **共享 IP 地址**、**工作组**、**用户名** 和 **密码**。
 - 选择**连接 ISO 的时间**下拉菜单选项，以设置网络 ISO 文件保持映射到目标设备的小时数。默认情况下，此值设置为 4 小时。
 - 单击**下一步**。
10. 在**虚拟标识**页面上，单击**保留标识**。
此时会显示所选目标设备的 NIC 卡的已分配虚拟标识。要查看所选目标设备的身份标识池的所有已分配标识，请单击**查看所有 NIC 详细信息**。
11. 在**目标属性**部分中，可以在部署此部署模板之前更改特定于每个所选目标设备（例如位置属性和 IP 地址）的非虚拟标识属性。部署模板时，这些更改的目标属性仅在特定设备上实施。要更改特定于设备的非虚拟标识属性，请执行以下操作：
 - a. 从显示先前选择的目标设备的列表中选择目标设备。
 - b. 展开属性类别，然后选择或清除在目标设备上的模板部署过程中必须包含或排除的属性。
 - c. 单击**下一步**。
12. 单击**完成**。
此时会显示警告消息：*部署模板可能导致数据丢失，并且可能导致设备重新启动。您确实要部署模板吗？*
13. 单击**是**。
此时会创建新的自动部署目标并在**自动部署**页面上列出。

删除自动部署目标

注: 要对 OpenManage Enterprise 执行任何任务，您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14

注: 如果通过 **OpenManage Enterprise > 配置 > 模板**页面删除与自动部署目标相关联的模板，则也会删除相关联的自动部署条目，而无论其当前状态如何。

要从**自动部署**列表中删除自动部署目标，请执行以下操作：

1. 通过单击 **OpenManage Enterprise > 配置 > 自动部署**，转到“自动部署”页面。

2. 从列表中选择自动部署目标。
3. 单击**删除**，然后单击**是** 确认。
此时会从“自动部署”页面中移除所选的自动部署目标。

将自动部署目标详细信息导出为不同的格式

1. 通过单击 **OpenManage Enterprise > 配置 > 自动部署**，转到“自动部署”页面。
2. 从列表中选择自动部署目标，然后单击**导出**。
3. 在**导出所有** 对话框中，选择格式为 HTML、CSV 或 PDF。单击**完成**。
将创建一个作业并以选定格式导出自动部署目标数据。

无状态部署概览

要在目标设备上部署包含虚拟标识属性的设备部署模板，请执行以下步骤：

1. **创建设备模板** — 单击**部署**选项卡下的**创建模板**任务以创建部署模板。您可以选择从配置文件或参考设备创建模板。
2. **创建标识池** — 单击**标识池**选项卡下的**创建**任务，以创建一个或多个类型的虚拟标识类型。
3. **将虚拟标识分配给设备模板** - 从**模板**窗格中选择部署模板，然后单击**编辑网络**以将标识池分配给部署模板。您也可以选择已标记的和未标记的网络，并将最小和最大带宽分配给端口。
4. **在目标设备上部署部署模板** — 使用**部署**选项卡下的**部署模板**任务，在目标设备上部署部署模板和虚拟标识。

管理标识池 - 无状态部署

服务器的 I/O 接口，例如 NIC 或 HBA，具有接口制造商分配的唯一标识属性。这些唯一的标识属性统称为服务器的 I/O 标识。I/O 标识唯一地标识网络上的服务器，还确定服务器使用特定协议和网络资源通信的方式。借助 OpenManage Enterprise，您可自动生成虚拟标识属性，并将其分配至服务器的 I/O 接口。

使用包含虚拟 I/O 标识的设备部署模板部署的服务器被称为“无状态”。无状态部署可用于创建动态且灵活的服务器环境。例如，通过在 SAN 引导的环境中部署包含虚拟 I/O 标识的服务器，您可以快速执行以下操作：

- 通过将服务器的 I/O 标识移动至另一备用服务器更换正在发生故障或已发生故障的服务器。
- 部署额外的服务器来增大高工作负载期间的计算能力。

使用 **OpenManage Enterprise > 配置 > 标识池** 页面，可以创建、编辑、删除或导出虚拟 I/O 池。

注：

- 要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。
[OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14
- 基于范围的限制不适用于标识池，因此所有标识池均可供所有用户类型查看和使用。但是，设备管理者分配标识后，设备管理者只能查看和使用这些标识。

创建标识池 — 池信息

标识池用于在服务器上基于模板的部署以虚拟化以下项的网络标识：

- 以太网
- iSCSI
- 基于以太网的光纤信道 (FCoE)
- 光纤信道 (FC)

在每个这些类别中最多可创建 5000 个标识池。

服务器部署过程提取池中下一个可用的标识，并在通过模板说明提供服务器时使用。然后可将配置文件从一台服务器迁移到另一台服务器，而不会丢失对您环境中网络或存储资源的访问。

您可以编辑池中的条目数。但是，不能减少低于那些分配或保留的条目数。也可删除未分配或保留的条目。

标识池

标识池是一个或多个虚拟标识类型的集合，这些类型为网络通信所必需。标识池可包含以下任何虚拟标识类型的组合：

- 以太网标识
此类标识由介质访问控制 (MAC) 地址定义。以太网 (LAN) 通信需要使用 MAC 地址。
- iSCSI 标识
此类标识由 iSCSI 限定名称 (IQN) 定义。需要使用 IQN 标识来支持使用 iSCSI 协议从 SAN 引导。
- 光纤信道 (FC) 标识
此类标识由全球节点名称 (WWNN) 和全球端口名称 (WWPN) 定义。WWNN 标识分配给 FC 结构中的节点 (设备) 并可通过设备的部分或全部端口共享。WWPN 标识分配给 FC 结构中的每个端口并对每个端口为唯一状态。需要 WWNN 和 WWPN 标识支持使用 FC 和以太网光纤信道 (FCoE) 协议的从 SAN 引导以及数据访问。
- 基于以太网的光纤信道 (FCoE) 标识
此类标识为 FCoE 操作提供唯一的虚拟标识。这些标识由 MAC 地址和 FC 地址 (即 WWNN 和 WWPN) 进行定义。需要 WWNN 和 WWPN 标识支持使用 FC 和以太网光纤信道 (FCoE) 协议的从 SAN 引导以及数据访问。

OpenManage Enterprise 使用标识池自动将虚拟标识分配至用于部署服务器的设备部署模板。

注:

- 对于属于现有标识池但在 OpenManage Enterprise 外部部署的标识，必须启动新的配置资源清册作业，以便在设备中识别并将其指定为“已分配”。
- 已分配的虚拟标识将不会用于新部署，除非这些标识被清除。

创建标识池

您可创建包含一个或多个虚拟标识类型的标识池。所有设备管理者都可以使用管理员创建的通用池。此外，管理员还可以查看正在使用的所有标识。设备管理者可以查看所有标识池，并对其执行所有操作（按 RBAC 指定），但在“使用情况”下，设备管理者只能查看关联到其范围内的设备的标识。

要创建虚拟标识类型的池：

1. 在配置页面上，单击**标识池**。
2. 单击**创建**。
3. 在**创建标识池**对话框中的**池信息**下：
 - a. 输入标识池的唯一名称和相应的说明。
 - b. 单击**下一步**。
4. 在**以太网**部分中：
 - a. 选中**包括以太网虚拟 MAC 地址**复选框以包括 MAC 地址。
 - b. 输入起始 MAC 地址并指定要创建的虚拟 MAC 标识数。
5. 在**iSCSI**部分中：
 - a. 选中**包括 iSCSI MAC 地址**复选框以包括 iSCSI MAC 地址。
 - b. 输入起始 MAC 地址并指定要创建的 iSCSI MAC 地址数。
 - c. 选择**配置 iSCSI 启动器**，然后输入 IQN 前缀。
 - d. 选择**启用 iSCSI 启动器 IP 池**，然后输入网络详细信息。
注: iSCSI 启动器 IP 池不支持 IPv6 地址。
6. 在**FCoE**部分中：
 - a. 选中**包括 FCoE 标识**复选框以包括 FCoE 标识。
 - b. 输入起始 MAC 地址并指定要创建的 FCoE 标识数。
注: WWPN 和 WWNN 地址通过分别向 MAC 地址添加 0x2001 和 0x2000 前缀来生成。
7. 在**光纤信道**部分中：
 - a. 选中**包括 FC 标识**复选框以包括 FC 标识。
 - b. 输入后缀八位位组 (6 个八位位组) 以及要创建的 WWPN 和 WWNN 地址数。

注: WWPN 和 WWNN 地址通过分别添加提供的后缀与 0x2001 和 0x2000 作为前缀来生成。

此时，标识池已创建并在**标识池**选项卡下列出。

创建标识池 — 光纤信道

可向标识池添加光纤信道 (FC) 地址。FC 由 WWPN/WWNN 地址组成。

- 包括 FC 标识** 选中该复选框以将 FC 地址添加到标识池。
- 后缀 (6 个八位位组)** 按以下格式之一输入后缀：
- AA:BB:CC:DD:EE:FF
 - AA-BB-CC-DD-EE-FF
 - AABB.CCDD.EEFF
- 后缀的最大长度为 50 个字符。只有在选中**包括 FC 标识**复选框时，才显示此选项。
- WWPN/WWNN 地址数** 选择 WWPN 或 WWNN 地址的数量。地址数介于 1 到 5000 之间。只有在选中**包括 FC 标识**复选框时，才显示此选项。

操作

- 上一个** 显示 FCoE 选项卡。
- 完成** 保存更改并显示配置页面。
- 取消** 关闭**创建标识池**向导而不保存更改。

创建标识池 — iSCSI

可在 iSCSI 选项卡中配置所需数目的 iSCSI MAC 地址。

注: 当 iSCSI 启动器在源模板中处于禁用状态时，才会应用 iSCSI 属性。

- 包括虚拟 iSCSI MAC 地址** 选中该复选框以将 iSCSI MAC 地址添加到标识池。
- 起始虚拟 MAC 地址** 按以下格式之一输入标识池的起始 MAC 地址：
- AA:BB:CC:DD:EE:FF
 - AA-BB-CC-DD-EE-FF
 - AABB.CCDD.EEFF
- MAC 地址的最大长度为 50 个字符。只有在选中**包括 iSCSI MAC 地址**复选框时，才显示此选项。
- iSCSI MAC 地址数** 输入 iSCSI MAC 地址的数量。MAC 地址数介于 1 到 5000 之间。只有在选中**包括 iSCSI MAC 地址**复选框时，才显示此选项。
- 配置 iSCSI 启动器** 选中该复选框以配置 iSCSI 启动器。只有在选中**包括 iSCSI MAC 地址**复选框时，才显示此选项。
- IQN 前缀** 输入 iSCSI 标识池的 IQN 前缀。IQN 前缀的最大长度为 200 个字符。系统通过向前缀附加生成的数字，自动生成 IQN 地址池。例如： <IQN Prefix>.<number>
- 只有在选中**配置 iSCSI 启动器**复选框时，才显示此选项。
- 注:** 如果引导模式为“BIOS”，则未在目标系统上部署使用标识池配置的 IQN。
- 注:** 如果 iSCSI 启动器名称显示在**标识池 > 使用情况 > iSCSI IQN** 字段中的单独行中，则它将指示 iSCSI IQN 只能在该 NIC 分区上启用。

启用 iSCSI 启动器 IP 池	选中该复选框以配置 iSCSI 启动器标识池。只有在选中 包括 iSCSI MAC 地址 复选框时，才显示此选项。
IP 地址范围	按以下格式之一输入 iSCSI 启动器池的 IP 地址范围： <ul style="list-style-type: none"> • A.B.C.D - W.X.Y.Z • A.B.C.D/E
子网掩码	从下拉列表中选择 iSCSI 池的子网掩码地址。
网关	输入 iSCSI 池的网关地址。
主要 DNS 服务器	输入主要 DNS 服务器地址。
次要 DNS 服务器	输入次要 DNS 服务器地址。

 **注：**IP 地址范围、网关、主要 DNS 服务器和次要 DNS 服务器必须为有效的 IPv4 地址。

操作

上一个	显示 以太网 选项卡。
下一个	显示 FCoE 选项卡。
完成	保存更改并显示 配置 页面。
取消	关闭 创建标识池 向导而不保存更改。

创建标识池 — 以太网光纤信道

可向标识池添加所需数量的以太网光纤信道 (FCoE) 初始化协议 (FIP) MAC 地址。全球端口名称 (WWPN)/全球节点名称 (WWNN) 值从这些 MAC 地址生成。

包括 FCoE 标识	选中该复选框以将 FCoE MAC 地址添加到标识池。
FIP MAC 地址	按以下格式之一输入标识池的起始 FCoE 初始化协议 (FIP) MAC 地址： <ul style="list-style-type: none"> • AA:BB:CC:DD:EE:FF • AA-BB-CC-DD-EE-FF • AABB.CCDD.EEFF <p>MAC 地址的最大长度为 50 个字符。只有在选中包括 FCoE 标识复选框时，才显示此选项。 WWPN/WWNN 值是从 MAC 地址生成。</p>
FCoE 标识数	选择所需的 FCoE 标识数。标识数介于 1 到 5000 之间。

操作

上一个	显示 iSCSI 选项卡。
下一个	显示 光纤信道 选项卡。
完成	保存更改并显示 标识池 页面。
取消	关闭 创建标识池 向导而不保存更改。

创建标识池 — 以太网

在**以太网**选项卡中，可将所需数量的 MAC 地址添加到标识池。

包括以太网虚拟 MAC 地址	选中该复选框以将虚拟 MAC 地址添加到标识池。
起始虚拟 MAC 地址	按以下格式之一输入起始虚拟 MAC 地址： <ul style="list-style-type: none"> • AA:BB:CC:DD:EE:FF • AA-BB-CC-DD-EE-FF • AABB.CCDD.EEFF MAC 地址的最大长度为 50 个字符。只有在选中 包括以太网虚拟 MAC 地址 复选框时，才显示此选项。
虚拟 MAC 标识数	选择虚拟 MAC 标识的数量。标识数介于 1 到 50 之间。只有在选中 包括以太网虚拟 MAC 地址 复选框时，才显示此选项。

操作

上一个	显示 池信息 选项卡。
下一个	显示 iSCSI 选项卡。
完成	保存更改并显示 标识池 页面。
取消	关闭 创建标识池 向导而不保存更改。

查看标识池的定义

要查看标识池的定义，请执行以下操作：

1. 在**配置**页面上，单击**标识池**。
2. 选择一个标识池，然后单击**摘要**。
此时，会列出标识池的各种标识定义。
3. 要查看这些标识定义的使用情况，请单击**使用情况**选项卡，然后选择**查看依据**筛选选项。

编辑标识池

您可以编辑标识池以添加您先前尚未指定的范围，添加一个标识类型或删除标识类型范围。

要编辑标识池的定义，请执行以下操作：

1. 在**配置**页面上，单击**标识池**。
2. 选择标识池，然后单击**编辑**。
此时会显示**编辑标识池**对话框。
3. 在相应的部分中进行更改，然后单击**完成**。

标识池现已修改完毕。

删除标识池

如果标识保留或分配给部署模板，则不能删除标识池。

要删除标识池，请执行以下操作：

1. 在**配置**页面上，单击**标识池**。
2. 选择标识池，然后单击**删除**。
3. 单击**是**。

此时，标识池已被删除，与一个或多个部署模板关联的已保留标识也已移除。

定义网络

在“VLAN”页面上，您可以输入设备可访问的环境中当前配置的网络的信息。

注：要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

1. 选择配置 > VLAN > 定义。
2. 在定义网络对话框中，输入名称和相应的说明。
3. 输入 VLAN ID，然后选择网络类型。
您可以选择仅用于 MX7000 机箱的网络类型。有关网络类型的更多信息，请参阅 [网络类型](#) 页面上的 84。
4. 单击完成。

您环境中当前配置的网络现已定义完毕，资源可以访问该网络。

注：基于范围的限制不适用于 VLAN，因为这些是常见资源池。管理员定义 VLAN 后，就可供所有设备管理者使用。

网络类型

注：您可以选择仅用于 MX7000 机箱的网络类型。

表. 15: 网络类型

网络类型	说明
一般用途 (铜牌)	用于低优先级数据流量
一般用途 (银牌)	用于标准或默认优先级数据流量
一般用途 (金牌)	用于高优先级数据流量
一般用途 (白金)	用于极高优先级数据流量
群集互连	用于群集检测信号 VLAN
虚拟机监控程序管理	用于虚拟机监控程序管理连接，比如 ESXi 管理 VLAN
存储 — iSCSI	用于 iSCSI VLAN
存储 — FCoE	用于 FCoE VLAN
存储 — 数据复制	用于支持存储数据复制的 VLAN，比如 VMware 虚拟存储区域网络 (VSAN)
VM 迁移	用于支持 vMotion 和类似技术的 VLAN
VMWare FT 日志记录	用于支持 VMware 容错功能的 VLAN

编辑或删除配置的网络

1. 通过单击配置 > VLAN 转到 VLAN 页面。
2. 从列表中选择一个网络，然后在右侧窗格中单击编辑以更改名称、说明、VLAN ID 或网络类型。
注：因为 M I/O 聚合器 (IOA) 和 FN I/O 模块不支持 IPv6 寻址，所以在 IPv6 基础设施中不支持 M1000e 和 FX2 机箱上的 VLAN 配置。
注：在运行无状态部署任务之后，不会在目标 MX7000 机箱上更新已更改的 VLAN 名称和 ID。
3. 要删除网络，请选择该网络并单击删除。

4. 单击是。

导出 VLAN 定义

OpenManage Enterprise 中可用的网络定义可以下载为 CSV 或 JASON 文件。

1. 要下载为 CSV 文件，请执行以下操作：
 - a. 单击配置 > VLAN > 导出，然后选择全部导出为 CSV。
2. 要下载为 JSON 文件，请执行以下操作：
 - a. 单击配置 > VLAN > 导出，然后选择全部导出为 JSON。

导入网络定义

可使用以下方法导入网络定义：

1. 从文件导入 VLAN 定义
要从文件导入 VLAN 定义，请执行以下操作：
 - a. 单击配置 > VLAN。
 - b. 单击导入，然后选择从文件导入。
 - c. 导航至文件位置，然后选择包含 VLAN 定义的现有 .json 或 .csv 文件，然后单击打开。

注：

- 文件中的无效条目或内容类型会被标记，并且不会导入。
- .csv 和 .json 文件中的 VLAN 定义必须按以下格式输入：

表. 16: CSV 文件的 VLAN 定义格式

名称	说明	VLANMin	VLANMax	类型
VLAN1	使用单个 ID 的 VLAN	1	1	1
VLAN2 (范围)	使用 ID 范围的 VLAN	2	10	2

和

表. 17: JSON 文件的 VLAN 定义格式

```
[{"Name":"VLAN1","Description":"VLAN with single ID", "VlanMinimum":1,"VlanMaximum":1,"Type":1}, {"Name":"VLAN2 (Range)","Description":"VLAN with an ID Range", "VlanMinimum":2,"VlanMaximum":10,"Type":2}]
```

- d. 单击完成。创建了名为 ImportVLANDefinitionsTask 的作业，以从所选文件导入网络。
2. 从机箱导入 VLAN 定义
要从现有 MX7000 机箱导入 VLAN 定义，请执行以下操作：
 - a. 单击配置 > VLAN。
 - b. 单击导入并选择从机箱导入 VLAN。
 - c. 在作业目标屏幕中，选择需要导入 VLAN 定义的机箱，然后单击确定。创建了名为 ImportVLANDefinitionsTask 的作业，以从所选机箱导入网络。

作业完成后，刷新配置 > VLAN 页面，以查看成功导入的 VLAN 定义。

要查看作业的执行详细信息和从机箱导入的每个网络的状态，请转至作业页面，方法是单击监测 > 作业，选择作业，然后单击查看详细信息。

管理配置文件

“配置文件”是现有部署模板的特定实例，它自定义了单个设备独有的属性。配置文件可在模板的部署/自动部署过程中隐式创建或从用户现有模板中创建。配置文件包含特定于目标的属性值和 BootToISO 选项，以及目标设备的 iDRAC 管理 IP 详细信息。它还可以包含服务器 NIC 端口的任何网络带宽和 VLAN 分配（如果适用）。配置文件链接到从中创建它的源模板。

在**配置 > 配置文件**页面中，显示登录用户范围内的所有配置文件。例如，管理员可以查看和管理所有配置文件，但范围有限的设备管理者只能查看和使用其创建并拥有的配置文件。

显示所列配置文件的下列详细信息：

表. 18: 管理配置文件 - 字段定义

字段名称	说明
已修改	初始分配后将显示“已修改”符号  ，以通知对关联的配置文件或模板属性进行任何修改或更改。如果在设备上重新部署修改后的配置文件，该符号将消失。
配置文件名称	配置文件的名称
模板名称	链接的源模板的名称
目标	分配了配置文件的设备的服务编号或 IP 地址。如果配置文件未分配给任何设备，则目标为空。
目标类型	分配了配置文件的设备类型（服务器或机箱）
机箱	当目标服务器被查找为机箱的一部分时机箱的机箱名称
配置文件状态	如果配置文件已分配，则配置文件状态将显示为“已分配给设备”，如果未分配，显示为“未分配”，如果配置文件已部署，显示为“已部署”。
上次操作状态	显示配置文件的上次操作状态，如中止、取消、完成、失败、新、未运行、暂停、排队、正在运行、计划、正在启动、停止、已完成但有错误。

可以使用**高级筛选器**自定义配置文件列表。

在右侧 —— 显示所选配置文件的说明、上次部署时间、上次修改时间、创建时间和创建者。单击查看标识可查看标记到该配置文件的 NIC 配置和虚拟标识。

根据不同的配置文件状态，可以在**配置 > 配置文件**页面上执行以下操作，如下所述：


 **注：**“创建”和“删除”操作不作为表格的一部分列出。

表. 19: 配置文件状态和可能的操作

配置文件状态	编辑	分配目标	取消分配目标	重新部署	迁移
取消分配的配置文件	是	是	否	否	否
分配至设备	是	否	是	否	否
已部署	是	否	是	是	是

- 创建配置文件并预先保留虚拟标识。请参阅 [创建配置文件](#) 页面上的 87
- 查看配置文件详细信息。请参阅 [查看配置文件详细信息](#) 页面上的 87
- 编辑配置文件属性和设置。请参阅 [编辑配置文件](#) 页面上的 88
- 将配置文件分配给设备或服务标签（通过自动部署）。请参阅 [分配配置文件](#) 页面上的 88
- 从设备或服务标签取消分配配置文件。请参阅 [取消分配配置文件](#) 页面上的 89
- 将配置文件更改重新部署到关联的目标设备。请参阅 [重新部署配置文件](#) 页面上的 89

- 将配置文件从一个目标（设备或服务标签）迁移到另一个目标。
- 删除配置文件。请参阅 [删除配置文件](#) 页面上的 90
- 导出配置文件，然后将其数据下载到 HTML、CSV 或 PDF。请参阅 [以 HTML、CSV 或 PDF 格式导出配置文件数据](#) 页面上的 90

主题：

- [创建配置文件](#)
- [查看配置文件详细信息](#)
- [配置文件—查看网络](#)
- [编辑配置文件](#)
- [分配配置文件](#)
- [取消分配配置文件](#)
- [重新部署配置文件](#)
- [迁移配置文件](#)
- [删除配置文件](#)
- [以 HTML、CSV 或 PDF 格式导出配置文件数据](#)

创建配置文件

可以使用现有的目标设备上的部署模板来创建配置文件，也可以为尚未查找到的设备保留以进行自动部署。

注：

- 只有具有 OpenManage Enterprise 管理员或设备管理器权限的用户可以执行配置文件管理任务。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
- 升级到版本 3.6.x 后，先前 OpenManage Enterprise 版本中由 AD/LDAP 和 OIDC（PingFederate 或 KeyCloak）设备管理者创建的所有配置文件仅分配给管理员。因此，设备管理者必须在升级后重新创建配置文件。

从现有部署模板创建配置文件：

1. 通过单击 **配置 > 配置文件** 转到配置文件页面。
2. 单击 **创建** 以激活创建配置文件向导。
3. 在模板部分，**模板类型** 选择为服务器或机箱，然后在 **选择模板** 下拉列表中选择部署模板。单击 **下一步**。
4. 在 **详细信息** 页面中，根据需要修改 **名称前缀** 并在 **说明框** 中提供说明。在 **配置文件数量** 框中，输入配置文件的数量。单击 **下一步**。
5. （可选）在 **引导至网络 ISO** 页面中，选中 **引导至网络 ISO** 复选框，并指定完整 ISO 路径、文件共享位置，然后选择 **附加 ISO 的时间** 选项以设置网络 ISO 文件保持映射到目标设备的小时数。
6. 单击 **完成**。

根据部署模板名称和所提供的数量创建配置文件。这些配置文件在配置文件页面中列出。

查看配置文件详细信息

如需只查看现有配置文件的详细信息而不进行编辑，请执行以下操作：

1. 从 **配置 > 配置文件** 页面上的配置文件列表选择一个配置文件。
2. 单击 **查看** 以激活查看配置文件向导。
3. 在向导的 **详细信息** 页面上，将显示源模板、名称、说明和目标信息。
4. 单击 **下一步**。在 **启动至网络 ISO** 页面上，如果配置文件最初是使用该首选项设置的，则会显示 ISO 映像文件路径、ISO 映像文件的共享位置和连接 ISO 值的时间。

配置文件—查看网络

要查看与配置文件相关联的 NIC 端口的网络带宽和 VLAN 分配，请执行以下操作：

1. 在 **配置 > 配置文件** 页面上选择一个配置文件。
2. 单击 **查看** 以激活查看配置文件向导。
3. **带宽** 部分显示分区 nic 的以下带宽设置：NIC 标识符、端口、分区、最小带宽 (%) 和最大带宽 (%)。单击 **下一步**。
4. **VLAN** 部分显示了以下 VLAN 配置文件的详细信息：NIC 分组、NIC 标识符、端口、组、未标记的网络和已标记的网络。

5. 单击**完成**关闭向导。

编辑配置文件

可在**配置 > 配置文件**页面上编辑现有配置文件。配置文件中的更改不会自动影响关联的目标系统。要使更改生效，必须在目标设备上重新部署修改后的配置文件。

注：要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14

要重命名、编辑网络或编辑现有配置文件的属性，请在配置文件页面上选择配置文件，然后单击**编辑**。可选择以下编辑选项：

1. 选择**重命名**，然后在重命名配置文件向导的**名称**框中编辑配置文件名称。
2. 选择**编辑配置文件**以激活编辑配置文件向导，然后编辑以下内容：
 - a. 在**详细信息**页面中，您可以编辑**名称**和**说明**。单击**下一步**。
 - b. 在**启动至网络 ISO**页面上，选中**启动至网络 ISO**复选框以指定完整 ISO 路径和共享位置，然后执行以下操作：
 - **共享类型**选择 CIFS 或 NFS。
 - 在**ISO 路径**框中，输入完整的 ISO 路径。按照工具提示输入正确的语法。
 - 提供**共享 IP 地址**、**用户名**和**密码**框中的详细信息。
 - 选择**连接 ISO 的时间**下拉菜单选项，以设置网络 ISO 文件保持映射到目标设备的小时数。默认情况下，此值设置为 4 小时。
 - 单击**下一步**。
 - c. 在**iDRAC 管理 IP**页面，选择以下任一项：
 - 不要更改 IP 设置。
 - 设置为 DHCP
 - 设置静态 IP 并提供相关的管理 IP、子网掩码和网关详细信息。
 - d. 在**目标属性**页面上，您可以选择和编辑配置文件的 BIOS、系统、NIC、iDRAC 和虚拟标识属性。
 - e. 单击**完成**以保存更改。

分配配置文件

通过**配置 > 配置文件**页面，未分配的配置文件可以部署在现有服务器上，也可以保留用于在尚未查找到的服务器上自动部署。

注：

- 要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
- 在部署配置文件的情况下，目标服务器的现有属性（如有）将被覆盖。
- 只有未与任何配置文件关联的设备可用于部署或自动部署。

1. 要**部署配置文件**：
 - a. 在**配置 > 配置文件**页面上选择一个未分配的配置文件，单击**分配 > 部署**以激活部署配置文件向导。
 - b. **详细信息**页面显示源模板、配置文件名称和说明。单击**下一步**。
 - c. 在**目标**页面上：
 - 单击**选择**，然后从设备列表中选择目标设备。

注：已分配配置文件的设备将显示为灰色，并且不能在目标列表中选择。
 - 如果在部署后需要重新启动，请选择**正常重新启动失败时不强制重新启动主机操作系统**复选框。
 - 单击**下一步**。
 - d. （可选）在**启动至网络 ISO**页面上，选中**启动至网络 ISO**复选框，并提供相关的 ISO 路径、共享位置详细信息和连接 ISO 的时间值。单击**下一步**。
 - e. 在**iDRAC 管理 IP**页面上，从以下选项中选择一项，并提供更多相关详细信息。
 - 不更改 IP 设置
 - 设置为 DHCP
 - 设置静态 IP
 - f. 在**目标属性**页面上，属性显示在 BIOS、系统、NIC 和 iDRAC 部分下。在部署之前，您可以选择、取消选择或编辑属性。
 - g. 在**虚拟标识**页面上，单击**保留标识**。此时会显示所选目标设备的 NIC 卡的已分配虚拟标识。要查看所选目标设备的身份标识池的所有已分配标识，请单击**查看所有 NIC 详细信息**。

- h. 在**计划**页面中，您可以选择立即**运行**以立即部署配置文件，或选择**启用计划**并为配置文件部署选择适当的日期和时间。
- i. 单击**完成**。

注：如果已在设备外部分配标识，则除非将其清除，否则新部署将不会使用这些标识。有关更多信息，请访问 [标识池](#) 页面上的 80

2. 要自动部署配置文件：

注：对于模块化设备，VLAN 定义的严格检查默认处于启用状态。

- a. 在**配置 > 配置文件**页面上选择一个未分配的配置文件，单击**分配 > 自动部署**以激活自动部署向导。
- b. 详细信息页面将显示配置文件的源模板、名称和说明（如有）。单击**下一步**。
- c. 在**目标**页面上，在**标识符**框中指定有待查找的设备的服务编号或节点 ID。单击**下一步**。
- d. （可选）在启动至网络 ISO 页面上，选中**启动至网络 ISO** 复选框，以指定完整的 ISO 路径和共享位置：
 - **共享类型**选择 CIFS 或 NFS。
 - 在 **ISO 路径**框中，输入完整的 ISO 路径。按照工具提示输入正确的语法。
 - 提供**共享 IP 地址**、**用户名**和**密码**框中的详细信息。
 - 选择**连接 ISO 的时间**下拉菜单选项，以设置网络 ISO 文件保持映射到目标设备的小时数。默认情况下，此值设置为 4 小时。
- e. 单击**完成**。

取消分配配置文件

使用**配置 > 配置文件 > 取消分配**，可以将已部署或自动部署的配置文件与其各自的目标解除关联。

要取消分配配置文件：

1. 从**配置 > 配置文件**页面上的配置文件列表中选择配置文件。
2. 单击**取消分配**。
3. 单击确认对话框中的**完成**。


这将取消分配所选的配置文件，并移除其相应目标中的标识。

注：对于已部署的目标设备，取消分配配置文件会将其恢复为工厂分配的标识。

重新部署配置文件

要使已经部署的配置文件的属性更改在关联的目标设备上生效，必须进行重新部署。对于模块化设备，可在重新部署期间配置 VLAN 定义，但匹配 VLAN 属性的严格检查将被禁用。

要重新部署配置文件，请执行以下操作：

1. 在**配置 > 配置文件**页面上，选择“已部署”和/或“已修改”（）的配置文件，然后单击**重新部署**。
2. 在重新部署向导的“属性部署选项”页面上，选择以下属性部署选项之一，然后单击**下一步**：
 - **仅修改的属性**：仅重新部署目标设备上的已修改属性。
 - **所有属性**：在目标设备上重新部署所有属性以及任何已修改的属性。
3. 在“计划”页面上，选择下面其中一个选项：
 - **立即运行**，立即实现更改。
 - **启用计划**并选择预定进行重新部署的日期和时间。
4. 单击**完成**以继续。

重新部署配置文件时，将执行**重新部署配置文件**作业。可以在**监测 > 作业**页面上查看作业的状态。

迁移配置文件

已部署或自动部署的配置文件可以从其现有目标设备或服务标签迁移到另一个相同的目标设备或服务标签。

迁移成功后，配置文件目标分配反映新目标。如果迁移是从目标设备到尚未看到的服务标签，则配置文件的状态变为“已分配”。

i 注:

- 要对 OpenManage Enterprise 执行任何任务，您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
- 迁移配置文件会将由配置文件定义的设置（包括已部署的虚拟标识）从源设备移动到目标设备。
- 即使无法联系到源设备，也可以强制执行配置文件的迁移。在这种情况下，用户必须确保没有虚拟标识冲突。
- 在迁移过程中，不会从“源”服务器回收真正的目标特定属性。因此，在迁移后，两台服务器上可能存在相同的资源清册详细信息。

要迁移配置文件，请执行以下操作：

1. 在 **配置 > 配置文件** 页面上，选择一个配置文件，然后单击 **迁移** 以激活“迁移配置文件”向导。
2. 在选择页面上：
 - a. 从 **选择源配置文件** 下拉菜单中，选择您想要迁移的配置文件
 - b. 单击 **选择目标**，从“作业目标”对话框中选择目标设备，然后单击 **确定**。
 - c. 如果需要，选择“即使无法联系源设备也强制迁移”复选框。

i 注: 您必须确保没有虚拟标识冲突。

- d. 单击 **下一步**。
3. 在“计划”页面上，选择以下任一项：
 - a. 选择 **立即更新**，立即将配置文件设置迁移到目标。
 - b. 选择预定进行迁移的 **日期和时间**。
 4. 单击 **完成**。

此时会创建一个作业，以将配置文件的设置迁移到新的目标设备。您可以在 **监视 > 作业** 页面中查看作业的状态。

删除配置文件

可从 **配置 > 配置文件** 页面删除现有的“未分配”配置文件：

i 注:

- 只有在已取消分配的情况下，才能从配置文件门户中删除已分配或已部署的配置文件。
- 删除保留了标识的未分配配置文件，会将这些标识返回到其来源的标识池。建议等待 10 分钟以将这些回收的标识用于未来的保留和部署。

要删除未分配的配置文件，请执行以下操作：

1. 在配置文件页面中选择未分配的配置文件。
2. 单击 **删除** 并在出现提示时单击 **确定** 进行确认。

以 HTML、CSV 或 PDF 格式导出配置文件数据

要将配置文件导出为 HTML、CSV 或 PDF 文件，请执行以下操作：

1. 在 **配置 > 配置文件** 页面上，选择配置文件。
2. 单击 **导出**，在“导出所选”对话框中，选择 HTML、CSV 或 PDF。
3. 单击 **完成**。将以选定的格式下载配置文件数据。

管理设备配置合规性

通过选择 **OpenManage Enterprise > 配置 > 配置合规性**，您可以使用内置的或用户创建的合规性模板创建配置基线。您可以从现有部署模板、参考设备或通过从文件导入来创建合规性模板。要使用此功能，您必须具有 OpenManage Enterprise 和 iDRAC 服务器的企业级许可证。机箱管理控制器不需要许可证。仅允许具有特定权限的使用此功能。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

在使用合规性模板创建配置基线后，每个基线的合规性级别摘要将在表中列出。与基线相关的每台设备都有自己的状态，但是最高严重性状态将被视为该基线的状态。有关“汇总运行状况”状态的更多信息，请参阅支持中心上提供的在 *Dell EMC 第 14 代及更高代别的 POWEREDGE 服务器上使用 iDRAC 管理汇总运行状况状态* 白皮书。

注：具有多个设备的基线有时会显示为永久不合规，因为少数属性值在所有目标中不一定相同。例如，iSCSI 目标 IQN、LUN ID、FCoE 目标 WWPN 等的启动控制属性在所有目标中不相同，并且可能会导致基线永久不合规。

“总体合规性摘要”报告将显示以下字段：

- **合规性：**设备的汇总合规性级别（参照配置合规性基线）。具有最低合规性（比如严重）的设备状态将标示为整个基线的状态。
- **名称：**配置合规性基线的名称。
- **模板：**基线使用的合规性模板的名称。
- **上次运行时间：**运行合规性基线的最近日期和时间。

要查看基线的配置合规性报告，请选择对应的复选框，然后单击右侧窗格中的**查看报告**。

使用查询构建器功能生成设备相对于选定基线的合规性级别。请参阅[选择查询条件](#) 页面上的 48。

OpenManage Enterprise 提供一份内置报告以查看受监测的设备列表及其配置合规性基线的合规性。选择 **OpenManage Enterprise > 监测 > 报告 > 每个模板合规性基线的设备**，然后单击**运行**。请参阅[运行报告](#) 页面上的 116。

相关任务

[创建配置合规性基线](#) 页面上的 93

[编辑配置合规性基线](#) 页面上的 94

[移除配置合规性基线](#) 页面上的 96

[管理合规性模板](#) 页面上的 91

[选择查询条件](#) 页面上的 48

主题：

- [管理合规性模板](#)
- [创建配置合规性基线](#)
- [编辑配置合规性基线](#)
- [删除配置合规性基线](#)
- [刷新配置合规性基线的合规性](#)
- [修正非合规设备](#)
- [移除配置合规性基线](#)

管理合规性模板

使用合规性模板来创建合规性基线，然后定期检查与基线关联的设备的配置合规性状态。请参阅[管理设备配置合规性](#) 页面上的 91。

要创建合规性模板，可以使用部署模板、参考设备或从文件导入。请参阅[管理合规性模板](#) 页面上的 91。

注：

- 要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

通过选择**配置 > 配置合规性 > 模板管理**，您可以根据 OpenManage Enterprise 中基于范围的访问权限来查看合规性模板的列表。例如，管理员可以查看和管理所有合规性模板，但设备管理者只能查看和管理自己创建且拥有的模板。在此页面上：

- 您可以通过以下方式创建合规性模板：
 - 使用部署模板。请参阅[从部署模板创建合规性模板](#) 页面上的 92。
 - 使用参考设备。请参阅[从参考设备创建合规性模板](#) 页面上的 92。
 - 从模板文件导入。请参阅[通过从文件中导入以创建合规性模板](#) 页面上的 93。
- 编辑合规性模板。请参阅[编辑合规性模板](#) 页面上的 93。
- 克隆合规性模板。请参阅[克隆合规性模板](#) 页面上的 93。
- 导出与合规性模板相关的报告。在[合规性模板](#)页面上，选中相应的复选框，然后单击**导出**。请参阅[导出所有或所选数据](#) 页面上的 56。
- 删除合规性模板。在[合规性模板](#)页面上，选中相应的复选框，然后单击**删除**。

配置合规性可扩展至最多 6000 个设备。要高效地管理大规模配置合规性活动，请执行以下操作：

- 禁用自动触发的默认配置资源清册任务，并在需要时手动运行。
- 使用数量较少的设备创建合规性基线。例如，6000 个设备必须划分为四个单独的基线，每个基线具有 1500 个设备。
- 不应同时检查所有基线的合规性。

注： 编辑合规性模板时，将自动触发与其关联的所有基线的配置合规性。如果存在频繁编辑模板的用例，则不支持上述规模环境，建议您为每个基线最多关联 100 个设备以获得最佳性能。

相关信息

[管理设备配置合规性](#) 页面上的 91

[编辑配置合规性基线](#) 页面上的 94

[移除配置合规性基线](#) 页面上的 96

[从部署模板创建合规性模板](#) 页面上的 92

[编辑合规性模板](#) 页面上的 93

从部署模板创建合规性模板

- 单击 **配置 > 配置合规性 > 模板管理 > 创建 > 从部署模板**。
- 在 **克隆部署模板** 对话框中，从 **模板** 下拉菜单中选择必须用作新模板参考的部署模板。
- 为合规性模板输入名称和说明。
- 单击 **完成**。
在合规性模板列表中创建并列出现合规性模板。

相关任务

[管理合规性模板](#) 页面上的 91

[克隆合规性模板](#) 页面上的 93

从参考设备创建合规性模板

要使用设备的配置属性作为用于创建配置基线的模板，此设备必须处于已启用状态。请参阅[启用设备](#) 页面上的 37。

- 单击 **配置 > 配置合规性 > 模板管理 > 创建 > 从参考设备**。
- 在 **创建合规性模板** 对话框中，输入合规性模板的名称和说明。
- 通过克隆服务器或机箱的属性，选择用于创建合规性模板的选项。
- 单击 **下一步**。
- 在 **参考设备** 部分中，选择必须用作创建合规性模板的参考设备。请参阅[选择目标设备和设备组](#) 页面上的 111。
 - 如果选择“服务器”作为参考设备，另请选择必须克隆的服务器配置属性。
- 单击 **完成**。
模板创建作业将被创建并运行。新创建的合规性模板在[合规性模板](#)页面中列出。

通过从文件中导入以创建合规性模板

1. 单击配置 > 配置合规性 > 模板管理 > 创建 > 从文件导入。
2. 在导入合规性模板对话框中，输入合规性模板的名称。
3. 选择服务器或机箱模板类型，然后单击**选择文件**以浏览到该文件并选择。
4. 单击**完成**。
创建并列出的合规性模板。

克隆合规性模板

1. 单击配置 > 配置合规性 > 模板管理。
2. 选择要克隆的合规性模板，然后单击**克隆**。
3. 在**克隆模板**对话框中，输入新合规性模板的名称。
4. 单击**完成**。
新合规性模板将创建成功并列在**合规性模板**下。

相关信息

[从部署模板创建合规性模板](#) 页面上的 92

[编辑合规性模板](#) 页面上的 93

编辑合规性模板

可在配置合规性 > 合规性模板页面上编辑合规性模板。

注:

- 编辑已与其他基线关联的合规性模板时，将自动触发所有使用该模板的基线上的所有设备的配置合规性。
 - 编辑链接至多个具有大量设备的基线的配置模板可能会导致会话超时，因为所有关联设备的配置合规性检查可能需要几分钟时间。会话超时不表示对合规性模板所做的更改有任何问题。
 - 当在包含 1000 个受管设备的大规模系统或最多 6000 个受管设备的配置资源清单上编辑合规性模板时，请确保没有其他配置资源清单或合规性操作在运行。此外，在**监测 > 作业**页面上**禁用**默认系统生成的配置资源清单作业（将源设置为“系统生成”）。
 - 为获得最佳性能，建议为每个基线关联最多 1500 个设备。
 - 如果存在频繁进行模板编辑的用例，建议您为每个基线关联最多 100 个设备，以获得最佳性能。
1. 在**合规性模板**页面上，选择相应的复选框，然后单击**编辑**。
 2. 在**模板详细信息**页中，将列出合规性模板的配置属性。
 3. 展开您要编辑的属性，然后在字段中输入或选择数据。
 - a. 要启用属性，请选择复选框（如果尚未启用）。
 4. 单击**保存**或**放弃**以实施或拒绝更改。
将编辑合规性模板并保存更新的信息。

相关任务

[管理合规性模板](#) 页面上的 91

[克隆合规性模板](#) 页面上的 93

创建配置合规性基线

配置合规性基线是与合规性模板相关联的设备列表。可以将 OpenManage Enterprise 中的设备分配给 10 个基线。您一次最多可以检查 250 个设备的合规性。。

要查看内置基线的列表，请单击 **OpenManage Enterprise > 配置 > 配置合规性**。

您可用的合规性基线列表取决于您在 OpenManage Enterprise 中的角色和基于范围的访问权限。例如，管理员可以查看和管理所有合规性基线，但设备管理者只能查看和管理该设备管理者创建并拥有的合规性基线。此外，设备管理者可用的目标设备会受到其各自范围内的设备/设备组的限制。

您可以通过以下方式创建配置合规性基线：

- 使用现有的部署模板。请参阅[管理设备配置合规性](#) 页面上的 91。
- 使用从支持的设备中捕获的模板。请参阅[从参考设备创建合规性模板](#) 页面上的 92。
- 使用从文件导入的模板。请参阅[通过从文件中导入以创建合规性模板](#) 页面上的 93。

在您选择用于创建基线的模板时，与模板关联的属性也会被选中。但是，您可以编辑基线属性。请参阅[编辑配置合规性基线](#) 页面上的 94。

小心：如果用于基线的合规性模板已与另一个基线关联，则编辑模板属性会更改已关联设备的基线合规性级别。阅读显示的错误和事件消息并采取相应的措施。有关错误和事件消息的更多信息，请参阅支持网站上提供的[错误和事件消息参考指南](#)。

注：创建配置合规性基线之前，请确保您已创建相应的合规性模板。

1. 选择配置 > 配置合规性 > 创建基线。

2. 在创建合规性基线对话框中：

- 在基线信息部分：
 - a. 从模板下拉菜单中，选择合规性模板。有关模板的更多信息，请参阅[管理设备配置合规性](#) 页面上的 91。
 - b. 输入合规性基线名称和说明。
 - c. 单击下一步。
- 在目标部分：
 - a. 选择设备或设备组。仅显示兼容设备。请参阅[选择目标设备和设备组](#) 页面上的 111。

注：仅列出兼容设备。如果您选择某个组，则与合规性模板不兼容的设备或者不支持配置合规性基线功能的设备将带有专有标识，可帮助您做出有效选择。

3. 单击完成。

合规性基线将会创建并列出。当创建或更新基线时，将启动合规性比较。基线的总体合规性级别显示在合规性列中。有关列表中的字段的信息，请参阅[管理设备配置合规性](#) 页面上的 91。

注：每次创建配置基线时，都会自动创建配置资源清册作业并由一体机运行，以收集与基线关联且资源清册数据不可用的设备的资源清册。这个新创建的配置资源清册作业包含与收集该资源清册的基线相同的名称。此外，在“配置合规性”页面上，相应的基线旁会显示指示资源清册作业进度的进度条。

相关信息

[管理设备配置合规性](#) 页面上的 91

[移除配置合规性基线](#) 页面上的 96

编辑配置合规性基线

您可以编辑与配置基线相关的设备、名称和其他属性。有关列表中显示的字段说明，请参阅[管理设备配置合规性](#) 页面上的 91。

小心：如果用于基线的合规性模板已与另一个基线关联，则编辑模板属性会更改已关联设备的基线合规性级别。请参阅[编辑合规性模板](#) 页面上的 93。阅读显示的错误和事件消息并采取相应的措施。有关错误和事件消息的更多信息，请参阅支持网站上提供的[错误和事件消息参考指南](#)。

1. 选择配置 > 配置合规性。

2. 从配置合规性基线列表中选择相应的复选框，然后单击编辑。

3. 在编辑合规性基线对话框中，更新该信息。请参阅[创建配置合规性基线](#) 页面上的 93。

注：每次编辑配置基线时，都会自动触发配置资源清册作业，以收集与基线关联且资源清册数据不可用的设备的资源清册。这个新创建的配置资源清册作业包含与收集该资源清册的基线相同的名称。此外，在“配置合规性”页面上，相应的基线旁会显示指示资源清册作业进度的进度条。

相关任务

[管理合规性模板](#) 页面上的 91

[选择查询条件](#) 页面上的 48

相关信息

[管理设备配置合规性](#) 页面上的 91

[移除配置合规性基线](#) 页面上的 96

删除配置合规性基线

您可以在 **配置 > 配置合规性** 页面上删除配置合规性基线，并从关联的基线中取消链接设备。

注： 要对 OpenManage Enterprise 执行任何任务，您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14

要删除配置合规性基线，请执行以下操作：

1. 从“配置合规性”页面上列出的基线中选择基线。
2. 单击**删除**，并在确认提示窗口单击**是**。

已删除的配置基线将从“配置合规性”页面中删除。

刷新配置合规性基线的合规性

如果对基线引用模板的属性做出更改或任何基线关联设备的配置资源清册进行了任何更改，则将自动触发合规性基线的合规性状态检查。

配置合规性基线的合规性状态是连接到该配置合规性基线的设备的汇总合规性级别。具有最低合规性（比如严重）的设备状态将标示为整个基线的状态。

所有配置基线的总体合规性摘要均在基线网格上方的圆环图上表示。合规性上次运行日期和时间显示在图表下方。

大型基线的合规性状态检查可能需要几分钟时间，但您可以单击**刷新合规性**，以便在执行大型基准合规性作业时按需获得设备的总体合规性摘要。

注： 当配置合规性处于“正在运行”状态时，不允许启动影响基线的新作业，如编辑合规性模板或基线。

要启动所有基线的总体合规性摘要刷新，请执行以下操作：

1. 单击**配置 > 配置合规性**，将显示“配置合规性”页面。
2. 单击**刷新合规性**。

将会启动合规性刷新作业（合规性负载摘要），显示当时的总体合规性摘要，以及更新合规性上次运行时间。

修正非合规设备

在基线的“合规性报告”页面上，您可以通过更改与关联基线属性相匹配的属性值来修正与关联的基线不匹配的设备。

“合规性报告”页面为与合规性模板基线关联的目标设备显示以下字段：

- **合规性：** 具有最低合规性（比如严重）的设备状态将标示为整个设备的状态。
- **设备名称：** 与基线关联的目标设备的名称。
- **IP 地址：** 目标设备的 IP 地址。
- **类型：** 关联的目标设备的类型。
- **型号：** 目标设备的型号名称。
- **服务标签：** 设备的服务标签。
- **上次运行时间：** 运行合规性基线的最近日期和时间。

您可以使用高级筛选器来快速查看非合规设备。此外，还可以对配置合规性结果使用“全选”和排序支持。要撤销筛选器，请单击**清除筛选器**。

要查看不合规的目标设备的偏离属性，请选择该设备并单击**查看报告**。相应目标装置的**合规性报告**列出了属性的属性名称、预期值和当前值。

要修复一个或多个非合规设备：

1. 选择**配置 > 配置合规性**。
2. 从配置合规性基线列表中，选中相应的复选框，然后单击**查看报告**。
3. 从不符合要求的设备列表中，选择一个或多个设备，然后单击**使其合规**。

4. 将配置更改计划为运行立即或以后运行，然后单击**完成**。

要在下一次重新引导服务器之后应用配置更改，您可以选择在**下一次重新引导时将配置更改部署到设备**选项。

将会运行新的配置资源清册任务，并会在**合规性**页面上更新基线的合规性状态。

导出合规性基线报告

与合规性模板基线关联的设备的完整或部分列表可以导出为 CSV 文件。

在配置基线的“合规性报告”页面

1. 单击**全部导出**以导出合规性基线中所有设备的详细信息。或者，
2. 从报告中选择各个所需设备后，单击**导出所选**。

移除配置合规性基线

您可以删除与配置基线关联的设备配置合规性级别。有关列表中显示的字段说明，请参阅[管理设备配置合规性](#) 页面上的 91。

 **小心:** 删除合规性基线或从合规性基线中删除设备时：

- 基线和/或设备的合规性数据将从 OpenManage Enterprise 数据中删除。
- 如果驱动器被删除，将不再检索其配置资源清册，已检索的信息也将被删除，除非该资源清册已与资源清册作业关联。

用作合规性基线的合规性模板如果与设备关联，则无法删除。在这种情况下将显示适当的消息。阅读显示的错误和事件消息并采取相应的措施。有关错误和事件消息的更多信息，请参阅支持网站上提供的[错误和事件消息参考指南](#)。

1. 单击**配置 > 配置合规性**。
2. 从配置合规性基线列表中选择相应的复选框，然后单击**删除**。
3. 询问您是否要删除时，单击**是**。
该合规性基线将被删除，同时会更新基线的**总体合规性摘要表**。

相关任务

[创建配置合规性基线](#) 页面上的 93

[选择查询条件](#) 页面上的 48

[管理合规性模板](#) 页面上的 91

[编辑配置合规性基线](#) 页面上的 94

相关信息

[管理设备配置合规性](#) 页面上的 91

监视和管理设备警报

通过选择 **OpenManage Enterprise > 警报**，您可以查看和管理管理系统环境中设备生成的警报。“警报”页面将显示以下选项卡：

- **警报日志**：您可以查看和管理在目标设备上生成的所有警报。
- **警报策略**：您可以创建警报策略，将在目标设备上生成的警报发送到电子邮件、手机、系统日志服务器等目标。
- **警报定义**：您可以查看为错误或信息用途生成的警报。

注：

- 要在 OpenManage Enterprise 上管理和监测设备警报，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
- 警报策略和警报日志由您在 OpenManage Enterprise 中基于范围的访问权限控制。例如，管理员可以查看和管理所有警报策略，但设备管理者只能查看和管理默认警报策略及其创建并拥有的策略。此外，设备管理者只能查看其范围内的设备的警报。
- 目前，OpenManage Enterprise 只会从以下 PowerEdge 服务器接收到 SNMPv1 和 SNMPv2 警报 — MX840c 和 MX5016s。
- OpenManage Enterprise 提供一份内置报告以查看受 OpenManage Enterprise 监测的设备列表和每个设备生成的警报列表。单击 **OpenManage Enterprise > 监测 > 报告 > 每个设备报告的警报计数**。单击**运行**。请参阅 [运行报告](#) 页面上的 116

相关概念

[查看警报日志](#) 页面上的 97

主题：

- [查看警报日志](#)
- [警报策略](#)
- [警报定义](#)

查看警报日志

警报日志页面显示在设备中发生的事件的警报日志列表。在 OpenManage Enterprise 中，单击**警报 > 警报日志**。此时将显示**警报日志**页面。

默认情况下，仅显示未确认警报。您可以使用下列两种方法之一来自定义警报列表：使用位于警报列表左侧顶部的高级过滤器，或者通过更改[应用程序设置](#)页面中的**警报显示设置**。请参阅[自定义警报显示](#)页面上的 138。您可以按如下所示查看警报详细信息：

- **确认**：如果警报已得到确认，则勾选标记会出现在**确认**下面。在**确认**下面的方括号内单击鼠标，以确认或取消确认警报。
- **时间**：生成警报的时间。
- **源名称**：生成警报的设备的操作系统主机名。单击源名称可查看和配置设备的属性。
- **注**：如果警报是从未查找到的设备生成或者是内部警报，则无法根据 IP 地址（源名称）过滤。
- **类别**：类别表示警报的类型。例如，系统运行状况和审核。
- **消息 ID**：所生成警报的 ID。
- **消息**：生成的警报。
- 右侧框中提供了其他信息，例如所选警报的详细描述和建议操作

注：OpenManage Enterprise 3.2 及更高版本会跟踪**上次更新操作者**数据点，但在以前的版本中未跟踪此数据点。因此，请注意警报日志是否使用**用户**高级筛选器字段进行细化，不会显示以前版本中的已确认警报。

选择警报以查看其他信息，例如“警报日志”页面右侧的详细描述和建议操作。您还可以在警报日志页上执行以下任务：

- 确认警报
- 取消确认警报
- 忽略警报
- 导出警报
- 删除警报

- 已存档的警报

相关信息

[监视和管理设备警报](#) 页面上的 97

管理警报日志

在**警报日志**页面上生成并显示警报日志后，您可以对其进行确认、取消确认、忽略、导出、删除和归档。

确认警报

在您查看警报并了解其内容之后，您可以确认已阅读警报消息。确认警报会阻止将同一个事件存储在系统中。例如，如果设备有噪音并且多次生成同一个事件，则您可以通过确认从该设备接收到的事件来忽略进一步记录该警报。另外，不会进一步记录同一类型的事件。


要确认警报，请在**警报日志**页面上，选中与警报对应的复选框，然后单击**确认**。

勾选标记将显示在**确认**列中。一旦确认警报，就会填充位于警报详细信息部分中的**上次更新操作者**字段。

取消确认警报

您可以取消确认已确认的警报日志。取消确认警报意味着会记录来自任何设备的所有事件，即使是相同的事件反复发生也不例外。默认情况下，将取消确认所有警报。

要取消确认警报，请选中与警报对应的复选框，然后单击**取消确认**按钮。另外，您也可以单击与每个警报对应的对号标记来取消确认。

 **注：**警报详细信息部分中的**上次更新操作者**字段将会保留上次确认该警报的用户的用户名。

忽略警报

忽略警报会创建警报策略，启用忽略情报并放弃该警报在以后出现的所有情况。选中与警报对应的复选框，然后单击**忽略**。将显示一条消息，指明正在创建作业，将忽略所选的警报。OpenManage Enterprise 标题行中显示的警报总数将会减少。

导出警报

您可以以 .csv 格式将警报日志导出到网络共享或您系统上的本地驱动器。

要导出警报日志，请在**警报日志**页面上，选择要导出的警报日志，然后单击**导出 > 导出所选**。您可以通过单击**导出 > 导出全部**导出所有警报日志。警报日志以 .csv 格式导出。

删除警报

您可以删除警报以永久移除控制台发出警报的情况。

选择与警报所对应的复选框，然后单击**删除**。将显示一条消息，提示您确认删除过程。单击**是**以删除警报。OpenManage Enterprise 标题行中显示的警报总数将会减少。

查看存档的警报

在 OpenManage Enterprise 中最多可生成和查看 50,000 个警报。在达到 50,000 限制的 95% (47,500) 时，OpenManage Enterprise 生成内部消息，表示当计数达到 50,000 时，OpenManage Enterprise 会自动清除 10% 的已存档警报 (5000 个)。下表列出了涉及警报清除的不同方案。

表. 20: 警报清除

工作流程	说明	结果
清除任务	在控制台上每 30 分钟后运行一次。	如果警报已达到最大容量 (即 50,000) , 检查并生成清除存档。
清除警报警告	生成内部清除警报警告。	如果警报超过 95% (即 475000) , 则生成内部清除警报, 清除 10% 的警报。
清除警报	从警报日志清除警报。	如果警报数超过 100%, 那么 10% 的旧警报将被清除, 以使警报数量恢复为 90% (即 45,000) 。
下载清除警报	下载已清除的警报。	可以从存档警报下载最近五个清除警报的存档。

下载存档的警报

存档警报是最旧的警报中的 10% (5000 个) , 当数量超过 50,000 时将被清除。这些最旧的 5000 个警报将从表中删除并存储在 .csv 文件中, 然后存档。下载存档的警报文件:

1. 单击存档的警报。

在**存档的警报**对话框中, 显示最后五个清除的存档警报。显示文件的大小、名称和存档日期。

2. 选择与警报文件对应的复选框, 并单击**完成**。该 .CSV 文件将下载到您选择的位置。

注: 要下载存档的警报, 您必须具有所需的权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

警报策略

本主题介绍警报策略的概念及其用途。有关创建、编辑、启用、禁用和删除警报策略的说明, 请参阅[配置和管理警报策略](#)。

通过警报策略, 您可以为特定设备或组件配置特定警报并将其发送到特定目标, 例如电子邮件、手机、系统日志服务器等。警报可帮助您有效监视和管理设备。

使用警报策略执行以下功能:

- 根据警报输入自动触发操作。
- 将警报发送到电子邮件地址。
- 通过短信或通知向手机发送警报。
- 通过 SNMP 陷阱发送警报。
- 将警报发送到系统日志服务器。
- 执行设备电源控制操作, 例如在生成预定义类别的警报时打开或关闭设备。
- 运行远程脚本。

要查看、创建、编辑、启用、禁用和删除警报策略, 请单击**警报 > 警报策略**。

相关任务

[配置和管理警报策略](#) 页面上的 99

配置和管理警报策略

本主题提供有关如何创建、编辑、启用、禁用和删除警报策略的说明。

注:

- 要在 OpenManage Enterprise 上执行任何任务, 您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

相关信息

[警报策略](#) 页面上的 99

[将审计日志转发到远程系统日志服务器](#) 页面上的 101

创建警报策略

您可以创建警报策略并将其启用以将警报发送到电子邮件地址、电话、SNMP 陷阱，以及执行设备控制操作，例如，在生成预定义类别的警报时打开或关闭设备、电源重启和正常关机。

注：升级到版本 3.6.x 后，仅将设备管理者在任何先前的 OpenManage Enterprise 版本中创建的任何警报策略分配给管理员。因此，在升级后，设备管理者必须重新创建警报策略，才能继续接收警报。

在**警报 > 警报策略**页面上，单击**创建**，然后执行以下操作：

1. 输入警报策略的名称和描述，然后单击**下一步**。默认情况下，**启用策略**复选框处于选中状态。
2. 通过选择任意或所有内置和导入的第三方管理信息库 (MIB) 类别来选择警报类别。
您可以展开每个类别以查看和选择子类别。要了解有关类别和子类别的详细信息，请参阅**警报定义** 页面上的 103。
3. 选择需要警报的设备或组，然后单击**下一步**。可对以下项目应用警报：
 - 一个设备或多个设备。
 - 一个设备组或多个设备组。
 - 通过输入 IP 地址或主机名指定的未查找到的设备。
 - 任何未查找到的设备。

注：不能在未查找到的设备上执行“远程脚本执行”和“电源操作”任务。

注：OpenManage Enterprise 会识别此类未查找到的（外部）设备发送的 SNMPv1、SNMPv2 和 SNMPv3 协议警报。
4. （可选）通过为**日期范围**、**时间间隔**和**天数**选择所需的值，指定警报策略适用的持续时间，然后单击**下一步**。
5. 选择警报的严重性，然后单击**下一步**。
要选择所有严重性类别，请选择**全选**复选框。
6. 选择一个或多个警报操作，然后单击**下一步**。可用的选项有：
 - 电子邮件 - 选择“电子邮件”以通过指定每个字段的信息并使用令牌（如果主题和消息需要）来向指定收件人发送电子邮件。请参阅**远程脚本和警报策略中的标记替换** 页面上的 152
 - **注：**针对同一类别、消息 ID 和内容的多个警报的电子邮件每 2 分钟只触发一次，以避免收件箱中收到重复或冗余的警报消息。
 - SNMP 陷阱转发（启用）— 单击启用以查看 SNMP 配置窗口，您可以在其中配置警报的 SNMP 设置。请参阅**配置 SMTP、SNMP 和 Syslog 警报** 页面上的 101。
 - 系统日志（启用）— 单击启用以查看系统日志配置窗口，您可以在其中配置警报的系统日志设置。请参阅**配置 SMTP、SNMP 和 Syslog 警报** 页面上的 101。
 - 选择忽略复选框以忽略警报消息，且不激活警报策略。
 - 发送短信至指定电话号码。
 - 电源控制 - 选中“电源控制”复选框可查看可以打开、关闭、关机再开机或正常关闭设备的操作。要在执行电源控制操作之前关闭操作系统，请选中**先关闭操作系统**复选框。
 - 远程脚本执行（启用）- 单击“启用”以查看“远程命令设置”窗口，您可在其中在远程节点上添加和运行远程命令。有关添加远程命令的详细信息，请参阅**执行远程命令和脚本** 页面上的 102。
从下拉菜单中，选择运行此警报策略时要运行的脚本。您也可以设置运行远程命令，如**管理 OpenManage Enterprise 设备设置** 页面上的 123 中所述。
 - 将通知发送到向 OpenManage Enterprise 注册的手机。请参阅**OpenManage Mobile 设置** 页面上的 146。
7. 在“摘要”选项卡中查看所创建警报策略的详细信息，然后单击**完成**。
警报策略已成功创建并且列在**警报策略**部分中。

管理警报策略

在**警报策略**页面上创建警报策略后，您可以编辑、启用、禁用和删除它们。此外，OME 提供内置警报策略，可在收到警报时触发关联的操作。您不能编辑或删除内置警报策略，而只能启用或禁用这些策略。

要查看创建的警报策略，请单击**警报 > 警报策略**。

要选择所有警报策略，请选中**已启用**左侧的复选框。选中警报策略旁边的一个或多个复选框，以执行下列操作：

- **编辑警报策略：**选择一个警报策略，然后单击**编辑**以在**配置和管理警报策略** 页面上的 99 对话框中编辑所需信息。

注：一次只能编辑一个警报策略。

注：默认情况下，对于版本 3.3.1 之前的 OpenManage Enterprise 版本的警报策略，时间间隔复选框处于禁用状态。升级后，启用“时间间隔”并更新字段以重新激活策略。

- **启用警报策略**：选择警报策略并单击**启用**。在启用警报策略后，**启用**列中会出现复选标记。已启用的警报策略的**启用**按钮显示为灰色。
- **禁用警报策略**：选择警报策略并单击**禁用**。警报策略已禁用，并且**已启用**列中的复选标记已被删除。
在创建警报策略时，通过清除“名称和描述”部分中的**启用策略**复选框，还可以禁用警报策略。
- **删除警报策略**：选择警报策略并单击**删除**。
您可以通过选择相应的复选框来一次删除多个警报策略。要选择或清除所有复选框，请选择**启用**旁边标题行中的复选框。

将审计日志转发到远程系统日志服务器

要从系统日志服务器监测 OpenManage Enterprise 的所有审计日志，您可以创建一个警报策略。可将所有审计日志（例如用户登录尝试、创建警报策略和运行不同的作业）转发到系统日志服务器。

要创建警报策略以将审计日志转发到系统日志服务器：

1. 选择**警报 > 警报策略 > 创建**。
2. 在**创建警报策略**对话框中的**名称和说明**部分，输入警报策略的名称和说明。
 - a. **启用策略**复选框默认处于选中状态，以指示一旦创建警报策略，就会启用它。要禁用警报策略，请清除复选框。有关在以后启用警报策略的更多信息，请参阅 [配置和管理警报策略](#) 页面上的 99。
 - b. 单击**下一步**。
3. 在**类别**部分中，展开**应用程序**并选择设备日志的类别和子类别。单击**下一步**。
4. 在**目标**部分中，**选择设备**选项默认处于选中状态。单击**选择设备**并从左窗格中选择设备。单击**下一步**。
 ⓘ **注**：将审计日志转发到系统日志服务器时，不能选择目标设备或组。
5. （可选）默认情况下，警报策略始终处于活动状态。要限制活动，在**日期和时间**部分，选择开始和结束日期，然后选择时间范围。
 - a. 选择与必须运行警报策略的天对应的复选框。
 - b. 单击**下一步**。
6. 在**严重性**部分，选择必须激活此策略的警报的严重性级别。
 - a. 要选择所有严重性类别，请选择**全选**复选框。
 - b. 单击**下一步**。
7. 在**操作**部分中，选择**系统日志**。
如果未在 OpenManage Enterprise 中配置系统日志服务器，请单击**启用**并输入系统日志服务器的目标 IP 地址或主机名。有关配置系统日志服务器的更多信息，请参阅[配置 SMTP、SNMP 和 Syslog 警报](#) 页面上的 101。
8. 单击**下一步**。
9. 在**摘要**部分，将显示您定义的警报策略的详细信息。请仔细阅读信息。
10. 单击**完成**。

警报策略已成功创建并且列在**警报策略**部分中。

相关任务

[配置和管理警报策略](#) 页面上的 99

[监视审核日志](#) 页面上的 104

配置 SMTP、SNMP 和 Syslog 警报

通过单击 **OpenManage Enterprise > 应用程序设置 > 警报**，您可以配置接收系统警报、SNMP 警报转发目标和 Syslog 转发属性的电子邮件 (SMTP) 地址。要管理这些设置，您必须具有 OpenManage Enterprise 管理员级凭据。

要配置和验证负责管理用户和 OpenManage Enterprise 之间电子邮件通信的 SMTP 服务器，请执行以下操作：

1. 展开**电子邮件配置**。
2. 输入发送电子邮件消息的 SMTP 服务器网络地址。
3. 要验证 SMTP 服务器，请选中**启用验证**复选框，然后输入用户名和密码。
4. 默认情况下，要访问的 SMTP 端口号为 25。必要时可进行编辑。
5. 选择**使用 SSL**复选框来保护您的 SMTP 事务。
6. 要测试 SMTP 服务器是否正常工作，请单击**发送测试电子邮件**复选框，然后输入**电子邮件收件人**。

7. 单击**应用**。
8. 要将设置重置为默认属性，请单击**放弃**。

要配置 SNMP 警报转发配置，请执行以下操作：

1. 展开 **SNMP 警报转发配置**。
2. 选择**启用**复选框以启用各自的 SNMP 陷阱以在发生预定义事件时发送警报。
3. 在**目标地址**框中，输入必须接收警报的目标设备的 IP 地址。
注：不允许输入控制台 IP，以避免出现重复的警报。
4. 从 **SNMP 版本**菜单中，选择 SNMP 版本类型为 SNMPv1、SNMPv2 或 SNMPv3 并填写以下字段：
 - a. 在社区字符串框中，输入必须接收警报的设备的 SNMP 社区字符串。
 - b. 根据需要编辑端口号。SNMP 陷阱的默认端口编号=162。请参阅 [OpenManage Enterprise 中支持的协议和端口](#) 页面上的 26。
 - c. 如果选择了 SNMPv3，请提供以下附加详细信息：
 - i. 用户名：提供用户名。
 - ii. 验证类型：从下拉列表中选择 SHA、MD_5 或“无”。
 - iii. 验证密码：提供至少包含八个字符的验证密码。
 - iv. 隐私类型：从下拉列表中选择 DES、AES_128 或“无”。
 - v. 隐私密码：提供至少包含八个字符的隐私密码。
5. 要测试 SNMP 消息，请单击相应陷阱的**发送**按钮。
6. 单击**应用**。要将设置重置为默认属性，请单击**放弃**。

要更新 Syslog 转发配置，请执行以下操作：

1. 展开 **Syslog 转发配置**。
2. 选择该复选框以在**服务器**列中各自的服务器上启用 Syslog 功能。
3. 在**目标地址/主机名称**框中，输入接收 Syslog 消息的设备的 IP 地址。
4. 使用 UDP 的默认端口编号=514。如有必要，可通过输入或从框中选择进行编辑。请参阅 [OpenManage Enterprise 中支持的协议和端口](#) 页面上的 26。
5. 单击**应用**。
6. 要将设置重置为默认属性，请单击**放弃**。

执行远程命令和脚本

当您获得 SNMP 陷阱时，您可以在 OpenManage Enterprise 上运行脚本。这会设置一个策略，其会在用于警报管理的第三方票证系统打开一个票证。您最多可以创建和存储**四个**远程命令。

注：不支持将以下特殊字符用作 RACADM 和 IPMI CLI 参数：[、;、|、\$、>、<、&、'、]、..、* 和 '。

1. 单击 **应用程序设置 > 脚本执行**。
2. 在**远程命令设置**部分中，执行以下操作：
 - a. 要添加远程命令，请单击**创建**。
 - b. 在**命令名称**框中，输入命令名称。
 - c. 选择以下任何一种命令类型：
 - i. 脚本
 - ii. RACADM
 - iii. IPMI 工具
 - d. 如果您选择**脚本**，请执行以下操作：
 - i. 在 **IP 地址**框中，输入 IP 地址。
 - ii. 选择身份验证方法：**密码**或 **SSH 密钥**。
 - iii. 输入 **SSH 密钥的用户名和密码**。
 - iv. 在**命令**框中，键入命令。
 - 最多可以键入 100 个命令，每个命令必须位于单独的行中。
 - 可以在脚本中实现标记替换。请参阅 [远程脚本和警报策略中的标记替换](#) 页面上的 152
 - v. 单击**完成**。
 - e. 如果您选择 **RACADM**，请执行以下操作：
 - i. 在**命令名称**框中，输入命令名称。
 - ii. 在**命令**框中，键入命令。最多可以键入 100 个命令，每个命令必须位于单独的行中。
 - iii. 单击**完成**。
 - f. 如果您选择 **IPMI 工具**，请执行以下操作：

- i. 在**命令名称**框中，输入命令名称。
 - ii. 在**命令**框中，键入命令。最多可以键入 100 个命令，每个命令必须位于单独的行中。
 - iii. 单击**完成**。
3. 要编辑远程命令设置，请选择命令，然后单击**编辑**。
 4. 要删除远程命令设置，请选择该命令，然后单击**删除**。

在插入和卸下底座上自动刷新 MX7000 机箱

在查找到或启用独立或主 MX7000 机箱后，OpenManage Enterprise 几乎可即时反映底座的添加或卸载。

使用 OpenManage Enterprise 版本 3.4 和更高版本查找到或启用独立或主 MX7000 机箱时，将在 MX7000 机箱上同时创建警报策略。有关在 OpenManage Enterprise 中查找和启用设备的详细信息，请参阅 [创建设备查找作业](#) 页面上的 36 和 [启用设备](#) 页面上的 37。

每次在 MX7000 机箱中插入、卸下或更换底座时，MX7000 OpenManage Enterprise-Modular 设备上自动创建的警报策略会在 OpenManage Enterprise 中触发名为**刷新机箱资源清册**的机箱资源清册刷新作业。

完成机箱资源清册刷新作业后，将在“所有设备”页面上显示 MX7000 的与底座相关的更改。

要成功创建自动警报策略，在启用 MX7000 时必须满足以下前提条件：

- MX7000 中必须已安装 OpenManage Enterprise-Modular 版本 1.2。
- MX7000 机箱应启用，并选择“**启用从查找到的 iDRAC 服务器和 MX7000 机箱的陷阱接收**”以及“**从应用程序设置中设置陷阱目标的团体字符串**”。
- OpenManage Enterprise 设备 IP 应成功注册为刚启用的 MX7000 中的四个可用警报目标之一。如果在启用时已配置 MX7000 中的所有警报目标，则自动创建警报策略将失败。

注：

- MX7000 上的警报策略仅特定于底座，不适用于机箱的其他组件，例如 IOM。
- 可以在 OpenManage Enterprise 中设置 MX7000 警报首选项，以接收来自 MX7000 机箱的所有警报，或者只接收机箱类别警报。有关更多信息，请参阅 [管理控制台首选项](#) 页面上的 137。
- 在实际操作底座与触发 OpenManage Enterprise 上的机箱资源清册刷新之间可能存在一些延迟。
- 如果从 OpenManage Enterprise 的设备资源清册中删除 MX7000 机箱，则自动创建的警报策略也会被删除。
- “所有设备”页面会将具有自动警报转发策略的已成功启用的 MX7000 机箱的**受管状态**列为“带警报的受管”。有关启用状态的详细信息，请参阅 [启用设备](#) 页面上的 37。

警报定义

通过单击 **OpenManage Enterprise > 警报 > 警报定义**，您可以查看因错误或出于参考目的而生成的警报。这些消息：

- 称为事件和错误消息。
- 显示在图形用户界面 (GUI) 以及 RACADM 和 WS-Man 命令行界面 (CLI) 上。
- 保存在日志文件中仅供参考。
- 已编号且明确定义，可使您有效地实施纠正和预防措施。

“事件”和“错误”消息包含：

- **消息 ID**：消息按 BIOS、电源 (PSU)、存储 (STR)、日志数据 (LOG) 和机箱管理控制器 (CMC) 等组件进行分类。
- **消息**：事件的实际原因。仅出于参考目的或因执行任务时出错而触发了警报。
- **类别**：错误消息所属的类别。有关类别的信息，请参阅支持站点上提供的 *Dell EMC PowerEdge 服务器的“事件”和“错误”消息参考指南*。
- **建议的措施**：使用 GUI、RACADM 或 WS-Man 命令解决错误。如有需要，建议您参考支持站点或技术中心的文档以获取更多信息。
- **详细说明**：可获取有关问题的更多信息，便于快速找到解决措施。

您可以通过使用筛选器（如消息 ID、消息文本、类别和子类别）查看有关警报的更多信息。查看警报定义：

1. 从 **OpenManage Enterprise** 菜单中，在**警报**下单击**警报定义**。

在**警报定义**下，将显示所有标准警报消息的列表。

2. 要快速搜索错误消息，请单击**高级筛选器**。

右窗格将会显示您在表中选择的消息 ID 的“错误”和“事件”消息信息。

监视审核日志

OpenManage Enterprise > 监测 > 审核日志页面列出了日志数据，可帮助您或 Dell EMC 支持团队进行故障处理和分析。在以下情况下将记录审核日志：

- 分配组或更改访问权限时。
- 修改用户角色时。
- 已在 OpenManage Enterprise 监测的设备上执行的操作。

审计日志文件可导出为 CSV 文件格式。请参阅[导出所有或所选数据](#) 页面上的 56。

注：

- 要对 OpenManage Enterprise 执行任何任务，您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
 - 基于范围的限制不适用于审核日志。
1. 要查看审核日志，请选择**监视 > 审核日志**。
将会显示 OpenManage Enterprise 存储的审计日志，其显示有关已执行的任务的信息。例如，用户登录尝试次数、警报策略创建和正在运行的不同作业。
 2. 要对任何列中的数据排序，请单击列标题。
 3. 要快速搜索关于审计日志的信息，单击**高级筛选器**。
将显示以下字段，可充当快速搜索数据的筛选器。
 4. 在以下字段中输入或选择数据：
 - **严重性**：选择日志数据的严重性级别。可用选项包括信息、警告和严重。
 - 严重：发生任何异常操作。需要立即关注。
 - 警告：该事件非常重要，但不需要立即关注。
 - 信息：已成功执行任何操作。
 - **开始时间和结束时间**：查看指定时间段的审核日志。
 - **用户**：查看来自特定用户的审核日志。例如，管理员、系统、设备管理者和查看者。
 - **源地址**：查看来自特定系统的审核日志。例如，您登录到 OpenManage Enterprise 的系统。
 - **类别**：查看审核或配置类型的审核日志。
 - 审核：在用户登录或注销 OpenManage Enterprise 设备时生成。
 - 配置：在目标设备上执行任何操作时生成。
 - **描述包含**：输入您正在搜索的日志数据中包含的文本或短语。显示所选文本的所有日志。例如，如果您输入 `warningSizeLimit`，将显示包含此文本的所有日志。
 - **消息 ID**：输入消息 ID。如果搜索条件相匹配，则仅显示具有匹配消息 ID 的项目。
 5. 要移除筛选，请单击**清除所有筛选**。
 6. 要导出某个审计日志或所有审计日志，请分别选择**导出 > 导出所选**或**导出 > 全部导出**。有关导出审核日志的更多信息，请参阅[导出所有或所选数据](#) 页面上的 56。
 7. 要将控制台日志导出为 .zip 文件，请单击**导出 > 导出控制台日志**。

注：

- 当前，对于已查找到的带有 5.1x 及更早版本的固件版本的所有 M1000e 机箱，硬件日志的 TIMESTAMP 列中的日期显示为 JAN 12, 2013。但在 VRTX 和 FX2 机箱的所有机箱版本中将显示正确的日期。
- 文件将无法立即可供下载，尤其是要收集大量日志的情况。收集过程在后台进行，在操作完成后会显示文件保存提示。

相关信息

将[审计日志转发到远程系统日志服务器](#) 页面上的 101

主题：

- [将审计日志转发到远程系统日志服务器](#)

将审计日志转发到远程系统日志服务器

要从系统日志服务器监测 OpenManage Enterprise 的所有审计日志，您可以创建一个警报策略。可将所有审计日志（例如用户登录尝试、创建警报策略和运行不同的作业）转发到系统日志服务器。

要创建警报策略以将审计日志转发到系统日志服务器：

1. 选择**警报 > 警报策略 > 创建**。
2. 在**创建警报策略**对话框中的**名称和说明**部分，输入警报策略的名称和说明。
 - a. **启用策略**复选框默认处于选中状态，以指示一旦创建警报策略，就会启用它。要禁用警报策略，请清除复选框。有关在以后启用警报策略的更多信息，请参阅 [配置和管理警报策略](#) 页面上的 99。
 - b. 单击**下一步**。
3. 在**类别**部分中，展开**应用程序**并选择设备日志的类别和子类别。单击**下一步**。
4. 在**目标**部分中，**选择设备**选项默认处于选中状态。单击**选择设备**并从左窗格中选择设备。单击**下一步**。

i **注：** 将审计日志转发到系统日志服务器时，不能选择目标设备或组。
5. （可选）默认情况下，警报策略始终处于活动状态。要限制活动，在**日期和时间**部分，选择开始和结束日期，然后选择时间范围。
 - a. 选择与必须运行警报策略的天对应的复选框。
 - b. 单击**下一步**。
6. 在**严重性**部分，选择必须激活此策略的警报的严重性级别。
 - a. 要选择所有严重性类别，请选择**全选**复选框。
 - b. 单击**下一步**。
7. 在**操作**部分中，选择**系统日志**。

如果未在 OpenManage Enterprise 中配置系统日志服务器，请单击**启用**并输入系统日志服务器的目标 IP 地址或主机名。有关配置系统日志服务器的更多信息，请参阅[配置 SMTP、SNMP 和 Syslog 警报](#) 页面上的 101。
8. 单击**下一步**。
9. 在**摘要**部分，将显示您定义的警报策略的详细信息。请仔细阅读信息。
10. 单击**完成**。

警报策略已成功创建并且列在**警报策略**部分中。

相关任务

[配置和管理警报策略](#) 页面上的 99

[监视审核日志](#) 页面上的 104

使用作业进行设备控制

作业是一组有关在一个或多个设备上执行任务的说明。这些作业包括查找、固件更新、设备的资源清册刷新、保修等。您可以在**作业**页面上查看在设备及其组件中启动的作业的状态和详细信息。OpenManage Enterprise 有许多内部维护作业，这些作业由设备按照设置的计划自动触发。有关“默认”作业及其计划的更多信息，请参阅 [OpenManage Enterprise 默认作业和计划](#) 页面上的 108。

前提条件：

创建和管理涉及设备选择任务的作业，例如闪烁、电源控制、管理固件基线、管理配置合规性基线等。

- 您必须具有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14
- 每个作业类型都限制为您必须具有以下项的设备：
 - 访问权限。
 - 能够完成所需的操作。

要创建和管理作业，请选择 **OpenManage Enterprise > 监视 > 作业**。还可以在**作业**页上执行以下任务：

- [查看](#)当前正在运行、发生故障和已成功完成的作业的列表。
- 创建作业以闪烁设备 LED、控制设备电源，并在设备上运行远程命令。请参阅[为管理设备创建远程命令作业](#) 页面上的 110，[为管理电源设备创建作业](#)和[创建作业以使设备 LED 闪烁](#)。您可以在设备详细信息页面的服务器上执行类似操作。请参阅[查看和配置各个设备](#) 页面上的 56。
- [管理作业](#)，例如运行、停止、启用、禁用或删除作业。

要查看关于作业的更多信息，请选择与作业相对应的复选框，然后单击右侧窗格中的[查看详细信息](#)。请参阅[查看作业信息](#)。

主题：

- [查看作业列表](#)
- [查看单个作业信息](#)
- [创建作业以打开设备 LED](#)
- [为管理电源设备创建作业](#)
- [为管理设备创建远程命令作业](#)
- [创建作业以更改虚拟控制台插件类型](#)
- [选择目标设备和设备组](#)
- [管理作业](#)

查看作业列表

在 OpenManage Enterprise 中，单击**监视 > 作业**以查看现有作业的列表。以下各列中提供了有关作业的信息：


- **作业状态**：提供作业的执行状态。
请参阅[作业状态和作业类型描述](#) 页面上的 107。
- **状态**：提供作业的状态。可用的选项包括“已启用”或“已禁用”。
- **作业名称**：作业的名称。
- **作业类型**：提供作业的类型。
请参阅[作业状态和作业类型描述](#) 页面上的 107。
- **描述**：作业的详细描述。
- **上次运行**：作业的上次运行期间。

通过在**高级筛选器**部分中输入或选择值，还可以筛选作业。可以提供以下其他信息用于筛选警报：

- **上次运行开始日期**：作业上次运行开始日期。
- **上次运行结束日期**：作业上次运行结束日期。
- **源**：可用的选项包括“全部”、“用户生成”（默认）和“系统”。

要查看关于作业的更多信息，请选择一个作业，然后单击右侧窗格中的[查看详细信息](#)。请参阅[查看单个作业信息](#) 页面上的 109。

OpenManage Enterprise 提供一份内置报告以查看计划的作业列表。单击 **OpenManage Enterprise > 监测 > 报告 > 计划作业报告**。单击**运行**。请参阅[运行报告](#) 页面上的 116。

 **注:** 在[查找和资源清册计划](#)页面上, 计划作业的状态由**状态**列中的**排队**标识。但在[作业](#)页面上, 同样的状态被标识为**已计划**。

作业状态和作业类型描述

表. 21: 作业状态和说明

作业状态	说明
已计划	作业计划在以后的日期或时间运行。
已排队	等待执行的作业。
正在启动	
运行中	使用 立即运行 触发了作业
已完成	作业已运行。
失败	作业运行不成功。
新建	作业已创建但未运行。
已完成, 但有错误	作业运行取得部分成功, 虽已完成, 但有错误。
已中止	用户暂停了作业运行。
已暂停	用户停止了作业运行。
停止	用户中断了作业运行。
已取消	
未运行	作业已排队或已计划, 但尚未运行。

作业可能属于以下任一类型:

表. 22: 作业类型和说明

作业类型	说明
运行状况	检查设备的运行状况。请参阅 设备运行状况状态 页面上的 33。
资源清册	创建设备的资源清册报告。请参阅 管理设备资源清册 页面上的 61。
设备配置	创建设备配置合规性基线。请参阅 管理设备配置合规性 页面上的 91。
Report_Task	使用内置的或自定义数据字段创建与设备相关的报告。请参阅 报告 页面上的 115。
保修	生成与设备的保修状态相关的数据。请参阅 管理设备保修 页面上的 113。
Onboarding_Task	配置查找到的设备入网。请参阅 启用设备 页面上的 37。
查找	查找设备。请参阅 查找要监测或管理的设备 页面上的 34。
控制台更新执行任务	正在使用此任务跟踪控制台升级作业, 此任务有助于确定升级是完成还是失败
备份	
机箱配置文件	
调试日志	收集应用程序监视任务、事件和任务执行历史记录调试日志。
设备操作	在设备上创建“打开 LED”、“关闭 LED”、“IPMI CLI”、“RACADM CLI”等操作。
Diagnostic_Task	下载/运行诊断/TSR 或 SupportAssist 任务与诊断任务相关。请参阅 运行并下载诊断报告 。
导入 VLAN 定义	从 Excel 或 MSM 导入 VLAN 定义。
OpenID Connect 提供程序	有关 OpenID 连接的配置。请参阅 使用 OpenID Connect 提供程序登录 OpenManage Enterprise 。使用 OpenID Connect 提供程序登录 OpenManage Enterprise 页面上的 133

表. 22: 作业类型和说明 (续)

作业类型	说明
PluginDownload_Task	正在跟踪“插件下载”任务，此任务有助于识别插件 RPM 下载是否已完成并准备好进行安装。请参阅 检查并更新 OpenManage Enterprise 及可用插件的版本 。
Post_Upgrade_Task	已跟踪 PostUpgrade 任务以设置在 N-1 或 N-2 版本中执行的设备设置，也会运行在以前版本中创建的查找任务，以确保列出所有设备。
Report_Task	当用户运行报告时（对于“预制”和“自定义”），将跟踪报告任务。
还原	
设置更新	当用户在“应用程序设置”选项卡下应用新设置时，将跟踪“设置更新”任务。
软件回滚	当用户在目标设备上执行回滚操作时，回滚是正在跟踪的任务。
更新	当用户在目标设备上执行固件或驱动程序更新时，正在跟踪更新任务。
Upgrade_Bundle_Download_Task	正在跟踪“升级捆绑下载”任务，此任务有助于识别是否下载 OMEnterprise RPM 已完成并准备好进行安装

OpenManage Enterprise 默认作业和计划

OpenManage Enterprise 有许多内部维护作业，这些作业由设备按照设置的计划自动触发。

表. 23: 下表列出了 OpenManage Enterprise 默认作业名称及其计划。

作业名称	Cron 表达式	Cron 表达式描述	示例
配置资源清册	0 0 0 1/1 * ? *	从每个月 1 日起，在每天 00:00:00 AM 执行	<ul style="list-style-type: none"> Tue May 18 00:00:00 UTC 2021 Wed May 19 00:00:00 UTC 2021
默认控制台更新任务	0 0 12 ? * MON *	在每个月每个周一 12:00:00 PM 执行	<ul style="list-style-type: none"> Mon May 24 12:00:00 UTC 2021 Mon May 31 12:00:00 UTC 2021
默认的资源清册任务	0 0 5 * * ? *	在每天 05:00:00 AM 执行	<ul style="list-style-type: none"> Tue May 18 05:00:00 UTC 2021 Wed May 19 05:00:00 UTC 2021
针对清理的设备配置清除任务	0 0/1 * * * ? *	从每个小时的 :00 分钟起，在每分钟的 :00 秒执行	<ul style="list-style-type: none"> Mon May 17 18:39:00 UTC 2021 Mon May 17 18:40:00 UTC 2021
针对共享利用率的文件清除任务	0 0 0 1/1 * ? *	从每个月 1 日起，在每天 00:00:00 AM 执行	<ul style="list-style-type: none"> Tue May 18 00:00:00 UTC 2021 Wed May 19 00:00:00 UTC 2021
针对单个 DUP 文件的文件清除任务	0 0 0/4 1/1 * ? *	自每个月 1 日起，从每天 00 AM 开始，每 4 小时在 :00 分钟 :00 秒钟执行	<ul style="list-style-type: none"> Mon May 17 20:00:00 UTC 2021 Tue May 18 00:00:00 UTC 2021 Tue May 18 04:00:00 UTC 2021 Tue May 18 04:00:00 UTC 2021
全局运行状况任务	0 0 0/1 1/1 * ? *	自每个月 1 日起，从每天 00 AM 开始，每个小时在 :00 分钟 :00 秒钟执行	<ul style="list-style-type: none"> Mon May 17 19:00:00 UTC 2021 Mon May 17 20:00:00 UTC 2021
内部同步任务	0 0/5 * 1/1 * ? *	自每个月 1 日起，从每天每个小时的 :00 分钟开始，每 5 分钟在 :00 秒钟执行	<ul style="list-style-type: none"> Mon May 17 18:45:00 UTC 2021 Mon May 17 18:50:00 UTC 2021
指标清除任务	0 0 * ? * *	在每个小时的 :00 分钟 :00 秒钟执行	<ul style="list-style-type: none"> Mon May 17 19:00:00 UTC 2021 Mon May 17 20:00:00 UTC 2021 Mon May 17 21:00:00 UTC 2021
指标任务	0 0/15 * 1/1 * ? *	自每个月 1 日起，从每天每个小时的 :00 分钟开始，每 15 分钟在 :00 秒钟执行	<ul style="list-style-type: none"> Mon May 17 18:45:00 UTC 2021 Mon May 17 19:00:00 UTC 2021
移动订阅任务	0 0/2 * 1/1 * ? *	自每个月 1 日起，从每天每个小时的 :00 分钟开始，每 2 分钟在 :00 秒钟执行	<ul style="list-style-type: none"> Mon May 17 18:54:00 UTC 2021 Mon May 17 18:56:00 UTC 2021

表. 23: 下表列出了 OpenManage Enterprise 默认作业名称及其计划。 (续)

作业名称	Cron 表达式	Cron 表达式描述	示例
节点启动的查找任务	0 0/10 * 1/1 * ? *	自每个月 1 日起, 从每天每个小时的 :00 分钟开始, 每 10 分钟在 :00 秒钟执行	<ul style="list-style-type: none"> Mon May 17 19:00:00 UTC 2021 Mon May 17 19:10:00 UTC 2021
密码轮换任务	0 0 0/6 1/1 * ? *	自每个月 1 日起, 从每天 00 AM 开始, 每 6 小时在 :00 分钟 :00 秒钟执行	<ul style="list-style-type: none"> Tue May 18 00:00:00 UTC 2021 Tue May 18 06:00:00 UTC 2021 Tue May 18 12:00:00 UTC 2021
定期指标注册	0 0 3 * * ?	在每天 03:00:00 AM 执行	<ul style="list-style-type: none"> Tue May 18 03:00:00 UTC 2021 Wed May 19 03:00:00 UTC 2021
针对任务表的按需清除运行状况任务	0 0 0/5 1/1 * ? *	自每个月 1 日起, 从每天 00 AM 开始, 每 5 小时在 :00 分钟 :00 秒钟执行	<ul style="list-style-type: none"> Tue May 18 00:00:00 UTC 2021 Tue May 18 05:00:00 UTC 2021 Tue May 18 10:00:00 UTC 2021
清除任务表: Event_Archive	0 0 18/12 ? * * *	从每天 18 PM 开始, 每 12 小时在 :00 分钟 :00 秒钟执行	<ul style="list-style-type: none"> Tue May 18 18:00:00 UTC 2021 Wed May 19 18:00:00 UTC 2021 Thu May 20 18:00:00 UTC 2021
清除任务表: Group_Audit	0 0 0 1/1 * ? *	从每个月 1 日起, 在每天 00:00:00 AM 执行	<ul style="list-style-type: none"> Tue May 18 00:00:00 UTC 2021 Wed May 19 00:00:00 UTC 2021 Thu May 20 00:00:00 UTC 2021
清除任务表: 任务	0 0 0 1/1 * ? *	从每个月 1 日起, 在每天 00:00:00 AM 执行	<ul style="list-style-type: none"> Tue May 18 00:00:00 UTC 2021 Wed May 19 00:00:00 UTC 2021 Thu May 20 00:00:00 UTC 2021
清除任务表: announced_target	0 0 0 1/1 * ? *	从每个月 1 日起, 在每天 00:00:00 AM 执行	<ul style="list-style-type: none"> Tue May 18 00:00:00 UTC 2021 Wed May 19 00:00:00 UTC 2021 Thu May 20 00:00:00 UTC 2021
针对核心应用程序日志表的清除任务	0 0 0/5 1/1 * ? *	自每个月 1 日起, 从每天 00 AM 开始, 每 5 小时在 :00 分钟 :00 秒钟执行	<ul style="list-style-type: none"> Tue May 18 00:00:00 UTC 2021 Tue May 18 05:00:00 UTC 2021
针对事件表的清除任务	0 0/30 * 1/1 * ? *	自每个月 1 日起, 从每天每个小时的 :00 分钟开始, 每 30 分钟在 :00 秒钟执行	<ul style="list-style-type: none"> Mon May 17 19:30:00 UTC 2021 Mon May 17 20:00:00 UTC 2021 Mon May 17 20:30:00 UTC 2021
针对基础架构设备表的清除任务	0 0/30 * 1/1 * ? *	自每个月 1 日起, 从每天每个小时的 :00 分钟开始, 每 30 分钟在 :00 秒钟执行	<ul style="list-style-type: none"> Mon May 17 19:30:00 UTC 2021 Mon May 17 20:00:00 UTC 2021 Mon May 17 20:30:00 UTC 2021
订阅轮询器任务	0 0/30 * 1/1 * ? *	自每个月 1 日起, 从每天每个小时的 :00 分钟开始, 每 30 分钟在 :00 秒钟执行	<ul style="list-style-type: none"> Mon May 17 19:30:00 UTC 2021 Mon May 17 20:00:00 UTC 2021 Mon May 17 20:30:00 UTC 2021

查看单个作业信息

1. 在**作业**页面中, 选择与作业对应的复选框。
2. 在右侧窗格中, 单击**查看详细信息**。
在**作业详细信息**页面上, 将显示作业信息。
3. 如果作业的状态为“停止”、“失败”或“新建”之一, 请单击**重新启动作业**。
消息指示作业已开始运行。

执行历史部分列出了有关作业已成功运行的信息。**执行详细信息**部分列出了运行作业的设备和所用的时间。

注: 如果停止某项配置补救任务, 则整体任务状态会指示为“已停止”, 但该任务会继续运行。但是, 在**执行历史**部分中, 状态会指示为“正在运行”。

4. 要将数据导出到 Excel 文件, 请选择对应的或全部复选框, 然后单击**导出**。请参阅**导出所有或所选数据** 页面上的 56。

创建作业以打开设备 LED

以下步骤介绍了如何使用“闪烁设备”向导来使指定设备的 LED 闪烁。

要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

1. 可以通过以下方式激活“闪烁设备”向导：
 - a. 从“作业”页面（OpenManage Enterprise > 监测 > 作业）中，单击**创建**，然后选择**闪烁设备**。
 - b. 从“所有设备”页面（OpenManage Enterprise > 设备）中，选择设备，单击**更多操作**下拉列表，然后单击**打开 LED 或关闭 LED**。
2. 在**闪烁设备向导**对话框中：
 - a. 在**选项**部分：
 - i. 在**作业名称**框中输入作业名称。
 - ii. 从**闪烁 LED 持续时间**下拉菜单中，选择可以使 LED 闪烁一段时间、亮起或熄灭的选项。
 - iii. 单击**下一步**。
 - b. 在**目标**部分中，选择目标设备或目标组，然后单击**下一步**。请参阅[选择目标设备和设备组](#)页面上的 111。
 - c. 在**计划**下拉列表中，选择**立即运行**、**稍后运行**或**按计划运行**。请参阅[计划作业字段定义](#)页面上的 150。
3. 单击**完成**。
闪烁 LED 作业已创建并在“作业”页面（OpenManage Enterprise > 监测 > 作业）**作业状态**列中列出。

为管理电源设备创建作业

注：电源控制操作只能在使用 iDRAC（带外）查找和管理的设备上执行。

1. 单击**创建**，然后选择**电源控制设备**。
2. 在**电源控制设备向导**对话框中：
 - a. 在**选项**部分：
 - i. 在**作业名称**中输入作业。
 - ii. 从**电源选项**下拉菜单中，选择其中一项任务：**开机**、**关机**或**关机后再开机**。
 - iii. 单击**下一步**。
 - b. 在**目标**部分，选择目标设备并单击**下一步**。请参阅[选择目标设备和设备组](#)页面上的 111。
 - c. 在**计划**部分，立即或计划以后运行作业。请参阅[计划作业字段定义](#)页面上的 150。
3. 单击**完成**。
该作业已创建并在“作业”列表中列出，在**作业状态**列中标识为相应的状态。
4. 如果作业已计划为以后运行，但您想要立即运行该作业：
 - 在作业页面中，选择与计划的作业对应的复选框。
 - 单击**立即运行**。作业已运行且状态已更新。
 - 要查看作业数据，请单击右侧窗格中的**查看详细信息**。请参阅[查看单个作业信息](#)页面上的 109。

为管理设备创建远程命令作业

您可以使用命令行作业向导创建远程命令作业，以远程管理目标设备。

1. 单击**创建**，然后选择**设备远程命令**。
2. 在**命令行作业向导**对话框中的**选项**部分中：
 - a. 在**作业名称**中输入作业。
 - b. 从“界面”下拉菜单中选择一个界面，具体取决于您要管理的目标设备：
 - **IPMI CLI** — 用于 iDRAC 和非 Dell 服务器。
 - **RACADM CLI** — 用于使用 WSMAN 协议查找到的 iDRAC。
 - **SSH CLI** — 用于使用 SSH 协议查找到的 Linux 服务器。
 - c. 在**自变量**框中，输入命令。最多可以键入 100 个命令，每个命令必须位于单独的行中。

注：“参数”框中的命令一次运行一个。

- d. 单击**下一步**。
选项旁边的绿色勾选标记表示已提供所需数据。
3. 在**目标**部分，选择目标设备并单击**下一步**。请参阅[选择目标设备和设备组](#) 页面上的 111。
4. 在**计划**部分，立即或计划以后运行作业。请参阅[计划作业字段定义](#) 页面上的 150。
5. 单击**完成**。
该作业已创建并在“作业”列表中列出，在**作业状态**列中标识为相应的状态。
6. 如果作业已计划为以后运行，但您想要立即运行该作业：
 - 在作业页面中，选择与计划的作业对应的复选框。
 - 单击**立即运行**。作业已运行且状态已更新。
 - 要查看作业数据，请单击右侧窗格中的**查看详细信息**。请参阅[查看单个作业信息](#) 页面上的 109。

创建作业以更改虚拟控制台插件类型

您可以在多台设备上将虚拟控制台插件类型更改为 HTML5。更新到 HTML5 可带来更好的浏览器体验。要进行更新，请执行以下操作：

1. 单击 **OpenManage Enterprise > 监测 > 作业**
2. 单击**创建**，然后选择**更改设备上的虚拟控制台插件**。
3. 在**更改虚拟控制台插件向导**对话框的**选项**部分中：
 - a. 在**作业名称**中输入作业。默认情况下，插件类型显示为 HTML5。
 - b. 单击**下一步**。
4. 在**目标作业**部分中，选择目标设备并单击**下一步**。请参阅[选择目标设备和设备组](#) 页面上的 111。
 - a. 单击**下一步**。
5. 在**计划**部分，立即或计划以后运行作业。请参阅[计划作业字段定义](#) 页面上的 150。
6. 单击**完成**。
该作业已创建并在“作业”列表中列出，在**作业状态**列中标识为相应的状态。
7. 如果作业已计划为以后运行，但您想要立即运行该作业：
 - 在作业页面中，选择与计划的作业对应的复选框。
 - 单击**立即运行**。作业已运行且状态已更新。
 - 要查看作业数据，请单击右侧窗格中的**查看详细信息**。请参阅[查看单个作业信息](#) 页面上的 109。

选择目标设备和设备组

默认情况下，**选择设备**选为表示可以在设备上运行作业。您可以通过选择**选择组**在设备组上运行作业。

注：显示的设备组和设备受用户对设备的基于范围的操作访问权限控制。有关更多信息，请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

1. 单击**选择设备**。
在**作业目标**对话框中，左侧窗格列出了受 OpenManage Enterprise 监测的设备。在工作窗格中，显示与每个组关联的设备列表和设备详细信息。有关字段说明，请参阅“[所有设备](#)” [页面 — 设备列表](#) 页面上的 51。有关设备组的信息，请参阅[将设备按组整理](#) 页面上的 46。
2. 选择与设备对应的复选框，然后单击**确定**。
所选设备将在选择组的**所有选定设备**部分中显示。

管理作业

在**作业**页面上创建并显示作业之后，您可以按如下方式对其进行管理。

- **运行作业：**选中与作业对应的复选框，然后单击**立即运行**以在目标设备上执行任务。您可以在作业处于已启用状态时运行它。
 - **启用作业：**选中与作业对应的复选框，然后单击**启用**。
 - **禁用作业：**选中与作业对应的复选框，然后单击**禁用**。
- 注：**只能禁用正在运行的“已计划”的作业。不能中途禁用处于活动状态以及“正在运行”状态的作业。

- **停止作业：**选中与作业对应的复选框，然后单击**停止**。您可以在作业处于正在运行状态时停止它。
- **删除：**选中与作业对应的复选框，然后单击**删除**。

管理设备保修




注：要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

通过单击 **OpenManage Enterprise > 监测 > 保修**，您可以查看受 OpenManage Enterprise 监测且在您范围内的所有设备的保修状态。例如，具有所有设备组的访问权限的管理员将看到所有设备的保修详细信息，但设备管理者将仅看到其各自范围内的设备的保修详细信息。

您还可以将所选数据或全部数据导出到 Excel 工作表以进行统计和分析。“保修”页面会显示以下详细信息：

- **保修的状态**

注：保修状态由管理员选择的设置来决定。请参阅 [管理保修设置](#) 页面上的 140

-  意味着**严重**，指示保修已过期。
-  意味着**警告**，表示保修临近过期。
-  意味着**正常**，表示保修处于活动状态。

- **服务标签**

- **设备型号**

- **设备类型**

- **保修类型：**

- 初始：购买 OpenManage Enterprise 附带提供的保修。
- 延长：延长保修，因为初始保修持续时间已过期。

- **服务级别说明：**表示与设备保修相关的服务级别协议 (SLA)。

- **剩余天数：**保修到期前剩余的天数。您可以设置在收到警报前剩余的天数。请参阅[管理保修设置](#) 页面上的 140。

OpenManage Enterprise 会提供一份关于即将在 30 天内过期的保修的内置报告。单击 **OpenManage Enterprise > 监测 > 报告 > 30 天保修期**。单击**运行**。请参阅[运行报告](#) 页面上的 116。

要筛选表中显示的数据，请单击**高级筛选器**。请参阅 [OpenManage Enterprise 图形用户界面概述](#) 页面上的 29 中的高级筛选器部分。

内置保修作业会每周自动收集所有查找到的设备的保修状态。您也可以通过单击右上角的**刷新保修**来手动启动保修作业。

要导出所有或所选的保修数据，请单击**导出**。请参阅[导出所有或所选数据](#) 页面上的 56。

相关任务

[查看和续订设备保修](#) 页面上的 113



主题：

- [查看和续订设备保修](#)

查看和续订设备保修

单击 **OpenManage Enterprise > 监测 > 保修** 以获取通过 OpenManage Enterprise 监测的所有设备的保修状态列表及其服务标签、型号名称、设备类型、关联的保修和服务级别信息。有关字段说明，请参阅[管理设备保修](#) 页面上的 113。

要查看保修信息和续订设备的保修，请执行以下操作：

- 选择与设备对应的复选框。在右侧窗格中，将会显示设备的保修状态和其他重要详细信息（例如服务级别代码、服务提供商、保修开始日期、保修结束日期等等）。
- 要查看已过期的保修，请单击 **Dell 设备保修续订**，这会您可以重定向到 Dell EMC 支持站点，以使您能够管理您的设备保修。
- 单击右上角中的**刷新保修**以刷新“保修”表。保修状态自动从严重  更改为正常 ，适用于续订保修的所有设备。每次单击**刷新保修**时，都会在控制台生成新的设备保修警报日志，其中包含已过期保修的总数。有关警报日志的信息，请参阅[查看警报日志](#)

- 要对表中的数据按列排序，请单击列标题。
- 单击**高级过滤器**按钮以进行自定义。

相关信息

[管理设备保修](#) 页面上的 113

通过单击 **OpenManage Enterprise > 监测 > 报告**，您就可以创建自定义报告以深入查看设备的详细信息。报告使您可以查看有关设备、作业、警报和数据中心其他元素的数据。报告是内置的且由用户定义。您只能编辑或删除用户定义的报告。用于内置报告的定义和条件不可编辑或删除。您从“报告列表”中选择的报告的预览将显示在右侧窗格中。

“报告”页面上显示的报告和数据取决于您在 OpenManage Enterprise 中拥有的基于范围的用户权限。例如，除了内置报告外，设备管理者只能访问他们创建的报告。此外，用户生成的报告将仅包含该用户范围内的设备中的数据。例如，管理员和“无限”设备管理者生成的报告将包含有关所有设备组的数据，但具有受限范围的设备管理者生成的报告将仅包含与其范围内的设备和/或设备组相关的数据。

注：要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

表. 24: 用于管理 OpenManage Enterprise 上报告的基于角色的访问权限

用户角色...	允许的报告任务...
管理员和设备管理者	运行、创建、编辑、复制、发送电子邮件、下载和导出
查看者	运行、发送电子邮件、导出、查看和下载

“报告”功能的优点：

- 使用最多 20 个筛选器构建报告条件
- 您可以筛选数据并按您选择的列名进行排列
- 可以查看、下载和通过电子邮件消息发送报告
- 将报告一次发送到最多 20-30 个收件人
- 如果您觉得生成报告太费时间，您可以停止该过程。
- 生成的报告会自动翻译成安装 OpenManage Enterprise 时设置的语言
- 只要您生成、编辑、删除或复制报告定义，就会创建一个审计日志条目

目前，可以生成以下内置报告来提取以下各项的信息：

- 设备类别：资产、FRU、固件、固件/驱动程序合规性、计划的作业、警报摘要、硬盘驱动器、模块化机柜、NIC、虚拟驱动器、保修和许可证。
- 警报类别：每周警报

相关任务

[运行报告](#) 页面上的 116

[运行报告和通过电子邮件发送报告](#) 页面上的 116

[编辑报告](#) 页面上的 117

[删除报告](#) 页面上的 117

主题：

- [运行报告](#)
- [运行报告和通过电子邮件发送报告](#)
- [编辑报告](#)
- [复制报告](#)
- [删除报告](#)
- [创建报告](#)
- [导出所选报告](#)

运行报告

在“报告”页面（OpenManage Enterprise > 监测 > 报告）中，您可以运行、查看和下载内置报告或已创建的报告。

当您运行报告时，将会显示前 20 行，可逐页浏览分页的结果。要一次性查看所有行，请下载报告。要编辑此值，请参阅[导出所有或所选数据](#) 页面上的 56。输出中显示的数据无法排序，因为这是在用于构建报告的查询中定义的。要对数据进行排序，请编辑报告查询，或将其导出到 Excel 表中。建议一次运行的报告不要超过五 (5) 个，因为报告会消耗系统资源。不过，五个报告这一值取决于找到的设备、使用的字段，以及为生成报告而加入的表格数。将创建一个报告作业，它将在请求生成报告时运行。有关用于生成报告的基于角色的权限，请参阅[创建报告](#) 页面上的 117。

注:

- 要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
- 设备管理者生成的报告将仅包含与其范围内的设备相关的数据。
- 不建议您经常运行报告，因为这会消耗处理和数据资源。
- 对于类别“设备”的报告，第一列默认为“设备名称”、“设备型号”和“设备服务标签”。在自定义报告时，可以排除一些列。

要运行报告，请选择报告，然后单击**运行**。在 **<报告名称> 报告** 页中，报告使用您为创建报告定义的字段，以表格的形式显示。

要下载报告：

1. 单击**下载**。
2. 在**下载报告**对话框中，选择输出文件类型，然后单击**完成**。将显示所选的输出文件。目前，您可将报告导出成 XML、PDF、Excel 和 CSV 文件格式。只要您生成、编辑、删除或复制报告定义，就会创建一个审计日志条目。

要通过电子邮件发送报告：

1. 单击**电子邮件**。
2. 在**电子邮件报告**对话框中，选择文件格式、键入收件人的电子邮件地址，然后单击**完成**。该报告将通过电子邮件发出。您一次可通过电子邮件将报告发给 20-30 个收件人。
3. 如果未配置电子邮件地址，请单击**转到 SMTP 设置**。有关设置 SMTP 属性的更多信息，请参阅[设置 SNMP 凭据](#) 页面上的 140。

注: 如果您在下载或运行已生成的报告，而另一个用户同时在尝试删除该报告，两个任务都会成功完成。

相关信息

[报告](#) 页面上的 115

运行报告和通过电子邮件发送报告

您可以运行报告，并通过电子邮件将其一次性发送给 20-30 个收件人。

注: 如果邮件大小超出 SMTP 服务器上设置的固定邮件大小，则电子邮件操作可能会失败，并生成大型报告。在此类情况下，请考虑重新设置 SMTP 服务器的邮件大小限制，然后重试。

1. 选择报告，然后单击**运行和发送电子邮件**。
2. 在**电子邮件报告**对话框中：
 - a. 从**格式**下拉菜单中，选择生成报告必须采用的某一种文件格式 — HTML、CSV、PDF 或 MS-Excel。
 - b. 在**收件人**框中，输入收件人的电子邮件地址。如果未配置电子邮件地址，请单击**转到 SMTP 设置**。有关设置 SMTP 属性的更多信息，请参阅[设置 SNMP 凭据](#) 页面上的 140。
 - c. 单击**完成**。
报告将会通过电子邮件发送并记录在审核日志中。

相关信息

[报告](#) 页面上的 115

编辑报告

只能编辑用户创建的报告。

1. 选择该报告，然后单击**编辑**。
2. 在**报告定义**对话框中，编辑设置。请参阅[创建报告](#)。
3. 单击**保存**。
保存更新的信息。只要您生成、编辑、删除或复制报告定义，就会创建一个审计日志条目。

注：在编辑自定义报告时，如果类别已更改，关联的字段也将被删除。

相关信息

[报告](#) 页面上的 115

复制报告

只能复制用户创建的报告。

1. 选择报告，单击**更多操作**，然后单击**复制**。
2. 在**复制报告定义**对话框中，输入复制报告的新名称。
3. 单击**保存**。
保存更新的信息。只要您生成、编辑、删除或复制报告定义，就会创建一个审计日志条目。

删除报告

只能删除用户定义报告。如果删除报告定义，关联的报告历史记录也将被删除，并且使用该报告定义运行的所有报告都将停止。

1. 从 **OpenManage Enterprise** 菜单，在**监测**下选择**报告**。
将显示设备可用报告的列表。
2. 选择报告，单击**更多操作**，然后单击**删除**。
注：如果您在下载或运行已生成的报告，而另一个用户同时在尝试删除该报告，两个任务都会成功完成。
3. 在**删除报告定义**对话框中，当提示是否必须删除报告时，请单击**是**。
该报告即从报告列表中删除，列表也会进行更新。只要您生成、编辑、删除或复制报告定义，就会创建一个审计日志条目。

相关信息

[报告](#) 页面上的 115

创建报告

注：

- 要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
- 设备管理者生成的报告将仅包含与其范围内的设备组相关的数据。
- 一些表包含特定于设备类型的数据，可有效地将报告锁定到该设备类型。对于不同类型（比如服务器和机箱）的多个特定于设备的表，其中的混合列将会导致没有任何结果的无效报告。

尽管内置报告具有用于生成报告的默认定义（筛选条件），您也可以自定义条件来创建自己的定义，然后生成自定义的报告。您要在报告中显示的字段或列取决于您选择的类别。一次只能选择一个类别。报告中的列布局可通过拖放操作改变。同时：

- 报告名称必须是唯一的。
- 报告定义必须至少有一个字段和一个类别
- 对于具有设备和警报类别的报告，其中一个必填字段必须是设备名称或设备组

默认情况下，已选择**设备**作为类别，设备名称、设备服务标签和设备型号列将显示在工作窗格中。如果在编辑报告条件时选择任何其他类别，将会显示一条消息，指示默认字段将被移除。每个类别都有可用作列标题的预定义属性，其中的数据可使用您定义的条件进行筛选。示例类别类型如下：

- 作业：任务名称、任务类型、任务状态和任务内部。
- 组：组状态、组说明、组成员资格类型、组名和组类型。
- 警报：警报状态、警报严重性级别、目录名称、警报类型、警报子类别和设备信息。
- 设备：警报、警报目录、机箱风扇、设备软件等。这些条件具有更详细的分类，可以基于这些分类筛选数据和生成报告。

表. 25: 用于生成 OpenManage Enterprise 报告的基于角色的访问权限

用户角色...	允许的报告任务...
管理员和设备管理者	运行、创建、编辑、复制、发送电子邮件、下载和导出
查看者	运行、发送电子邮件、导出、查看和下载

1. 单击**报告 > 创建**。
2. 在**报告定义**对话框中：
 - a. 键入要定义的新报告的名称和说明。
 - b. 单击**下一步**。
3. 在**报告构建器**部分：
 - a. 从**类别**下拉菜单中选择报告类别。
 - 如果您选择“设备”作为该类别，请同时选择该设备组。
 - 如有必要，请编辑筛选条件。请参阅**选择查询条件**页面上的 48。
 - b. 在**选择列**区域下，选中必须显示为报告列的字段的复选框。所选字段名称将在**列顺序**区域中显示。
 - c. 您可以自定义报告，具体方法是
 - 使用**排序依据**和**方向**框。
 - 在**列顺序**区域中向上或向下拖动字段。
4. 单击**完成**。
报告生成并在报告列表中列出。您可以导出报告进行分析。请参阅**导出所有或所选数据**页面上的 56。只要您生成、编辑、删除或复制报告定义，就会创建一个审计日志条目。

在创建报告时选择查询条件

创建查询条件时定义筛选条件：

- 生成自定义报告。请参阅**创建报告**页面上的 117。
- 在自定义组下创建基于查询的设备组。请参阅**创建查询设备组**页面上的 48。

使用两个选项定义查询条件：

- **选择现有查询以复制**：默认情况下，OpenManage Enterprise 提供一份您可以复制并构建您自己的查询条件的内置查询列表。定义查询时，最多可以使用 20 个条件（筛选条件）。要添加筛选条件，您必须从**选择类型**下拉菜单中选择。
- **选择类型**：使用下拉菜单列出的属性从头构建查询条件。菜单中的项目取决于受 OpenManage Enterprise 监测的设备。选择查询类型后，根据查询类型，仅显示相应的运算符，例如 =、>、< 和 null。建议使用此方法定义构建的自定义报告中的查询条件。

注：当评估具有多个条件的查询时，评估的顺序与 SQL 相同。要指定条件评估的特定顺序，请在定义查询时添加或删除括号。

注：选中后，只是以虚拟方式复制现有查询的筛选条件来构建新的查询条件。与现有查询条件关联的默认筛选条件将不更改。内置查询条件的定义（筛选条件）将用作构建自定义查询的起点。例如：

1. **查询1** 是一个内置查询条件，具有以下预定义的筛选条件：Task Enabled=Yes。
2. 复制**查询1**的筛选条件属性，创建**查询2**，然后通过添加以下筛选条件自定义查询条件：Task Enabled=Yes 和 (Task Type=Discovery)。
3. 接下来，请打开**查询1**。它的筛选条件仍为 Task Enabled=Yes。

1. 在**查询条件选择**对话框中，请基于您是否想要创建查询条件用于查询组或生成报告而从下拉菜单中选择。
2. 通过分别单击加号或垃圾箱符号添加或删除一个筛选条件。
3. 单击**完成**。
查询条件生成并保存在现有查询列表中。生成审计日志条目并让其显示在审计日志列表中。请参阅**监视审核日志**页面上的 104。

导出所选报告

1. 选择与要导出的报告对应的复选框，单击**更多操作**，然后单击**导出所选**。
当前，您无法一次导出所有报告。
2. 在**导出所选报告**对话框中，选择导出报告必须采用的某一种文件格式 — HTML、CSV 或 PDF。
3. 单击**完成**。
在该对话框中，将文件打开或保存到已知位置以进行分析和统计。

管理 MIB 文件

注: 要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

数据中心的第三方工具可能会产生对您的操作至关重要的警报。这些警报存储在由各自供应商工具定义和理解的管理信息库 (MIB) 文件中。但是，OpenManage Enterprise 也可以管理这些 MIB。因此 OpenManage Enterprise 可以导入、解析和使用非 Dell EMC MIB 进行设备管理。OpenManage Enterprise 支持 SMI1 和 SMI2。OpenManage Enterprise 提供可用于 Dell EMC 设备的内置 MIB 文件。这些是只读 MIB 且不可编辑。

注: OpenManage Enterprise 只处理具有陷阱的有效 MIB。

管理 MIB 可以通过：

- [导入 MIB 文件](#) 页面上的 120
- [删除 MIB 文件](#) 页面上的 121
- [解析 MIB 类型](#) 页面上的 122

通过单击 **OpenManage Enterprise > 检测 > MIB**，您可以管理在数据中心由 OpenManage Enterprise 和其他系统管理工具使用的 MIB 文件。表中列出了具有以下属性的可用 MIB 文件。单击列标题对数据进行排序。

表. 26: OpenManage Enterprise 中基于角色访问 MIB 文件

OpenManage Enterprise 功能	MIB 文件的基于角色的访问控制		
	管理员	设备管理者	查看者
查看陷阱或 MIB	是	是	是
导入 MIB。编辑陷阱。	是	否	否
移除 MIB	是	否	否
编辑陷阱	是	否	否

要从 OpenManage Enterprise 下载内置 MIB 文件，单击**下载 MIB**。将文件保存到指定的文件夹中。

主题:

- [导入 MIB 文件](#)
- [编辑 MIB 陷阱](#)
- [删除 MIB 文件](#)
- [解析 MIB 类型](#)
- [下载 OpenManage Enterprise MIB 文件](#)

导入 MIB 文件

理想的 MIB 导入流程是：**用户将 MIB 上传到 OpenManage Enterprise > OpenManage Enterprise 解析 MIB > OpenManage Enterprise 搜索数据库中已经可用的任何类似陷阱 > OpenManage Enterprise 显示 MIB 文件数据**。可以导入的最大 MIB 文件大小为 3 MB。每次导入和删除 MIB 时，OpenManage Enterprise 都会审核日志历史记录。

注:

- 要在 OpenManage Enterprise 上执行任何任务，您必须具有所需的基于角色的用户权限和设备的基于范围的操作访问权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14
- 一次只能导入一个 MIB 文件。

1. 单击 **MIB > 导入 MIB**。
2. 在**导入 MIB** 对话框的**上传 MIB 文件**部分，单击**选择文件**以选择 MIB 文件。

如果 MIB 已导入由外部 MIB 解析的语句，则会显示一条消息。

- a. 单击**解析类型**。解析 MIB 类型。请参阅[删除 MIB 文件](#) 页面上的 121。
 - b. 单击**完成**。如果 MIB 文件为 Dell EMC 所有，将显示一条消息，指明该 MIB 是产品附带的，不可修改。
3. 单击**下一步**。
 4. 在**查看陷阱**部分，将显示 MIB 文件列表及以下信息：
 - 陷阱的警报类别。您可以编辑该类别，使其与 OpenManage Enterprise 类别定义相符。请参阅[编辑 MIB 陷阱](#) 页面上的 121。
 - 陷阱名称为只读。由第三方设备定义。
 - 警报的严重性级别：严重、警告、信息和正常。
 - 与警报关联的警报消息。
 - 陷阱 OID 为只读且唯一。
 - “新”表示陷阱首次由 OpenManage Enterprise 导入。表示已导入的陷阱为“已导入”。“覆盖”表示陷阱的定义因导入操作而被覆盖。

要编辑 MIB 文件的默认警报类别或严重性级别，请参阅[编辑 MIB 陷阱](#) 页面上的 121。要删除 MIB 文件，请选择相应的复选框，然后单击**删除陷阱**。将删除 MIB 文件并更新 MIB 文件列表。

5. 单击**完成**。MIB 文件将被解析并导入到 OpenManage Enterprise 中，然后在**最小值**选项卡下面列出。

i **注**：如果您导入某个 MIB，然后再次将其导入，则 MIB 状态将显示为**已导入**。然而，如果您重新导入一个已删除的 MIB 文件，陷阱状态将标识为**新**。

i **注**：已导入到 OpenManage Enterprise 的陷阱不可导入。

i **注**：默认情况下附带 OpenManage Enterprise 的 MIB 文件不可导入。

i **注**：导入陷阱后生成的事件将被格式化并按新的定义显示。

编辑 MIB 陷阱

1. 选择该报告，然后单击**编辑**。
2. 在**编辑 MIB 陷阱**对话框中：
 - a. 在字段中选择或键入数据：
 - 选择要分配给警报的新警报类别。默认情况下，OpenManage Enterprise 显示几个内置的警报类别。
 - 键入警报组件。
 - 陷阱名称是只读的，因为它由第三方工具生成。
 - 选择要分配给警报的严重性。默认情况下，OpenManage Enterprise 显示几个内置的警报类别。
 - 一条描述警报的消息。
 - b. 单击**完成**。
陷阱将被编辑并且已更新陷阱列表将显示。
 - i** **注**：您一次无法编辑多个警报。已导入到 OpenManage Enterprise 的陷阱不可编辑。
3. 在**报告定义**对话框中，编辑设置。请参阅[创建报告](#)。
4. 单击**保存**。
保存更新的信息。

删除 MIB 文件

i **注**：您不能删除任何警报策略使用的陷阱定义的 MIB 文件。请参阅[警报策略](#) 页面上的 99。

i **注**：在删除 MIB 之前接收的事件不会受关联 MIB 删除的影响。但是，删除后生成的事件将会有未格式化的陷阱。

1. 在**MIB 文件名**列中，展开文件夹，然后选择 MIB 文件。
2. 单击**移除 MIB**。
3. 在**移除 MIB**对话框中，选择要移除的 MIB 的复选框。
4. 单击**移除**。

MIB 文件即被移除，且 MIB 表已更新。

解析 MIB 类型

1. 导入 MIB 文件。请参阅[导入 MIB 文件](#) 页面上的 120。
如果未解析 MIB 类型，则会在**未解析的类型**对话框中列出 MIB 类型，这说明只有解析后才能导入 MIB 类型。
2. 单击**解析类型**。
3. 在**解决类型**对话框中单击**选择文件**，然后选择缺失的文件。
4. 在**导入 MIB** 对话框中单击**下一步**。如果仍然存在缺失的 MIB 类型，则**未解决的类型**对话框会再次列出缺失的 MIB 类型。重复步骤 1-3。
5. 解析完所有未解析的 MIB 类型后，请单击**完成**。完成导入过程。请参阅[导入 MIB 文件](#) 页面上的 120。

下载 OpenManage Enterprise MIB 文件

1. 在**监测**页面上，单击 **MIB**。
2. 展开并选择一个 OpenManage Enterprise MIB 文件，然后单击**下载 MIB**。

 **注：**您只能下载与 OpenManage Enterprise 相关的 MIB 文件。

管理 OpenManage Enterprise 设备设置

注: 要对 OpenManage Enterprise 执行任何任务，您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

注: 有关支持的浏览器的信息，请参阅支持站点上提供的 [OpenManage Enterprise 支持表](#)。

通过单击 **OpenManage Enterprise > 应用程序设置**，您可以执行以下操作：

- 配置和管理 OpenManage Enterprise 网络设置，例如 IPv4、IPv6、时间和代理设置。请参阅 [配置网络设置](#)。
- 添加、启用、编辑和删除用户。请参阅 [管理用户](#)。
- 设置设备运行状况和仪表盘监测属性。请参阅 [管理控制台首选项](#)。
- 管理用户登录和锁定策略。请参阅 [设置登录安全性属性](#)。
- 查看当前 SSL 证书，然后生成一个 CSR 请求。请参阅 [生成并下载的证书签名请求](#) 页面上的 136。
- 配置电子邮件、SNMP 和警报管理的系统日志属性。请参阅 [配置 SMTP、SNMP 和 Syslog 警报](#) 页面上的 101。
- 设置 SNMP 侦听器 and 陷阱转发设置。请参阅 [管理传入警报](#)。
- 设置凭据和时间以接收有关保修到期的通知。请参阅 [管理保修设置](#)。
- 设置属性以检查更新版本的可用性，然后更新 OpenManage Enterprise 版本。请参阅 [检查并更新 OpenManage Enterprise 及可用插件的版本](#) 页面上的 141。
- 使用 RACADM 和 IPMI 设置用户凭据，以运行远程命令。请参阅 [执行远程命令和脚本](#)。
- 在您的手机上设置和接收警报通知。请参阅 [OpenManage Mobile 设置](#) 页面上的 146。

相关任务

[删除目录服务](#) 页面上的 132

主题：

- [配置 OpenManage Enterprise 网络设置](#)
- [管理 OpenManage Enterprise 用户](#)
- [终止用户会话](#)
- [OpenManage Enterprise 中的目录服务集成](#)
- [使用 OpenID Connect 提供程序登录 OpenManage Enterprise](#)
- [安全证书](#)
- [设置登录安全性属性](#)
- [管理控制台首选项](#)
- [自定义警报显示](#)
- [配置 SMTP、SNMP 和 Syslog 警报](#)
- [管理传入警报](#)
- [管理保修设置](#)
- [检查并更新 OpenManage Enterprise 及可用插件的版本](#)
- [执行远程命令和脚本](#)
- [OpenManage Mobile 设置](#)

配置 OpenManage Enterprise 网络设置

注: 要对 OpenManage Enterprise 执行任何任务，您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

1. 要仅查看 OpenManage Enterprise 的所有活动网络连接的当前网络设置，如 DNS 域名、FQDN 以及 IPv4 和 IPv6 设置，请展开 **当前设置**。
2. 要配置 OpenManage Enterprise API 和 Web 界面用户的会话超时和最大会话数，请展开 **会话非活动超时配置** 并执行以下操作：

- a. 选中**启用**复选框，激活通用超时并输入**非活动超时 (1-1440)**值。非活动超时值可以设置为1分钟到1440分钟（24小时）之间。默认情况下，通用超时呈灰色显示。启用通用超时将会禁用API和Web界面字段。
 - b. 更改API**非活动超时 (1-1440)**和**最大会话数 (1-100)**的值。默认情况下，这些属性分别设置为30分钟和100。
 - c. 更改Web界面**非活动超时 (1-1440)**和**最大会话数 (1-100)**的值。默认情况下，这些属性分别设置为30分钟和100。
 - d. 单击**应用**以保存设置，或单击**放弃**以保留默认值。
3. 将显示当前系统时间和来源本地时区或NTP服务器IP。要配置系统时区、日期、时间和NTP服务器同步，请展开**时间配置**。
- a. 从下拉式列表中选择时区。
 - b. 输入日期，或单击**日历**图标以选择日期。
 - c. 以hh:mm:ss格式输入时间。
 - d. 要与NTP服务器同步，请选中**使用NTP**复选框，然后输入主要NTP服务器的服务器地址。
您最多可以在OpenManage Enterprise中配置三个NTP服务器。
注：选择**使用NTP**选项时，**日期**和**时间**选项不可用。
 - e. 单击**应用**。
 - f. 要将设置重置为默认属性，请单击**放弃**。
4. 要配置OpenManage Enterprise代理设置，请展开**代理配置**。
- a. 选中**启用HTTP代理设置**复选框以配置HTTP代理，然后输入HTTP代理地址和HTTP端口号。
 - b. 选择**启用代理服务器身份验证**复选框以启用代理服务器凭据，然后输入用户名和密码。
 - c. 如果配置的代理截获SSL流量且不使用受信任的第三方证书，请选中**忽略证书验证**复选框。使用此选项将忽略用于保修和目录同步的内置证书检查。
 - d. 单击**应用**。
 - e. 要将设置重置为默认属性，请单击**放弃**。

要了解您可以通过使用应用程序设置功能执行的所有任务，请参阅[管理 OpenManage Enterprise 设备设置](#) 页面上的 123。

管理 OpenManage Enterprise 用户

注：

- 要对 OpenManage Enterprise 执行任何任务，您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
- 对用户角色所做的任何更改都不会影响受影响用户的活动会话，并且将在后续登录时生效。
- 如果设备管理者用户降级为查看者，则该 DM 将失去对全部已拥有的实体（如作业、固件或配置模板和基线、警报策略以及配置文件等）的访问权限。这些实体只能由管理员管理，即使同一用户从查看者“升级”为 DM，也无法恢复权限。

通过点击 **OpenManage Enterprise > 应用程序设置 > 用户**，您可以执行以下操作：

- 查看、添加、启用、编辑、禁用或删除 OpenManage Enterprise 本地用户。有关详细信息，请参阅[添加和编辑 OpenManage Enterprise 本地用户](#)
- 通过导入目录组，将 OpenManage Enterprise 角色分配给 Active Directory 用户。在 OpenManage Enterprise 中，可以为 AD 和 LDAP 目录用户分配管理员、设备管理者或查看者角色。有关更多信息，请访问[导入 AD 和 LDAP 组](#) 页面上的 129
- 查看有关已登录用户的详细信息，然后结束（终止）用户会话。
- 管理目录服务。有关更多信息，请访问[添加或编辑要用于目录服务的 Active Directory 组](#) 页面上的 131
- 查看、添加、启用、编辑、禁用或删除 OpenID 连接提供程序（PingFederate 和/或密钥遮蔽）。有关更多信息，请访问[使用 OpenID Connect 提供程序登录 OpenManage Enterprise](#) 页面上的 133

默认情况下，**用户**下面会显示用户的列表。右侧窗格即会显示您在工作窗格中所选用户名的属性。

- **用户名：**除了您创建的用户，OpenManage Enterprise 将显示以下默认用户角色，该角色无法编辑或删除 admin、system 和 root。但您可以通过选择默认用户名，然后单击**编辑**以编辑登录凭据。请参阅[启用 OpenManage Enterprise 用户](#) 页面上的 128。建议使用的用户名字符如下：
 - 0-9
 - A-Z
 - a-z
 - - ! # \$ % & () * / ; ? @ [\] ^ _ ` { | } ~ + < = >
 - 建议使用的密码字符如下：
 - 0-9
 - A-Z
 - a-z

▪ ' - ! " # \$ % & () * . / : ; ? @ [\] ^ _ ` { | } ~ + < = >

- **用户类型**: 指明用户是在本地还是远程登录。
- **已启用**: 用一个勾选标记表示已启用户来执行 OpenManage Enterprise 管理任务。请参阅[启用 OpenManage Enterprise 用户](#) 页面上的 128 和[禁用 OpenManage Enterprise 用户](#) 页面上的 128。
- **角色**: 表示使用 OpenManage Enterprise 时的用户角色。例如, OpenManage Enterprise 管理员和设备管理者。请参阅[OpenManage Enterprise 用户角色类型](#) 页面上的 13。

相关参考资料

[禁用 OpenManage Enterprise 用户](#) 页面上的 128
[启用 OpenManage Enterprise 用户](#) 页面上的 128

相关任务

[删除目录服务](#) 页面上的 132
[删除 OpenManage Enterprise 用户](#) 页面上的 128
[终止用户会话](#) 页面上的 130

OpenManage Enterprise 中基于角色和范围的访问控制

OpenManage Enterprise 具有基于角色的访问控制 (RBAC), 可明确定义三个内置角色 (管理员、设备管理者和查看者) 的用户权限。此外, 使用基于范围的访问控制 (SBAC), 管理员可以限制设备管理者有权访问的设备组。以下主题将进一步说明 RBAC 和 SBAC 功能。

OpenManage Enterprise 中基于角色的访问控制 (RBAC) 权限

分配给用户的角色决定其访问设备设置和设备管理功能的级别。此功能称之为基于角色的访问控制 (RBAC)。控制台会在允许操作之前强制实施某个操作所需的权限。有关在 OpenManage Enterprise 上管理用户的更多信息, 请参阅[管理 OpenManage Enterprise 用户](#) 页面上的 124。

此表列出为每个角色启用的各种权限。

表. 27: OpenManage Enterprise 中的基于角色的用户权限

OpenManage Enterprise 功能	权限描述	访问 OpenManage Enterprise 的用户级别		
		管理员	设备管理者	查看者
设备设置	涉及设置设备的全局设备设置。	是	否	否
安全设置	设备安全设置	是	否	否
警报管理	警报操作/管理	是	否	否
结构管理	结构操作/管理	是	否	否
网络管理	网络操作/管理	是	否	否
组管理	静态组和动态组的创建、读取、更新和删除 (CRUD)	是	否	否
查找管理	查找任务的 CRUD, 运行查找任务	是	否	否
资源清册管理	资源清册任务的 CRUD, 运行资源清册任务	是	否	否
陷阱管理	导入 MIB, 编辑陷阱	是	否	否
自动部署管理	管理自动部署配置操作	是	否	否
监视设置	警报策略、转发、SupportAssist 等	是	是	否
电源控制	重新启动/重启设备电源	是	是	否

表. 27: OpenManage Enterprise 中的基于角色的用户权限 (续)

OpenManage Enterprise 功能	权限描述	访问 OpenManage Enterprise 的用户级别		
		管理员	设备管理者	查看者
设备配置	设备配置、模板应用, 管理/迁移 IO 标识、存储映射 (用于存储设备) 等	是	是	否
操作系统部署	部署操作系统、映射到 LUN 等	是	是	否
设备更新	设备固件更新、应用更新的基线等	是	是	否
模板管理	创建/管理模板	是	是	否
基线管理	创建/管理固件/配置基线策略	是	是	否
电源管理	设置电源预算	是	是	否
作业管理	作业执行/管理	是	是	否
报告管理	报告上的 CRUD 操作	是	是	否
报告运行	运行报告	是	是	是
查看	查看所有数据、报告执行/管理等	是	是	是

OpenManage Enterprise 中基于范围的访问控制 (SBAC)

使用基于角色的访问控制 (RBAC) 功能, 管理员可以在创建用户时分配角色。角色确定其对设备设置和设备管理功能的访问权限级别。基于范围的访问控制 (SBAC) 是 RBAC 功能的扩展, 允许管理员将设备管理者角色限制为称为范围的设备组子集。

在创建或更新设备管理者 (DM) 用户时, 管理员可以分配范围以将 DM 的操作访问权限限制为一个或多个系统组、自定义组和/或插件组。

管理员和查看者角色具有无限范围。这意味着他们对所有设备和组实体具有 RBAC 权限指定的操作访问权限。

可以按如下所示实施范围:

1. 创建或编辑用户
2. 分配 DM 角色
3. 分配范围以限制操作访问权限

有关管理用户的更多信息, 请参阅[管理 OpenManage Enterprise 用户](#) 页面上的 124。

当具有所分配范围的设备管理者 (DM) 用户登录时, DM 只能查看和管理范围内设备。此外, 仅当 DM 拥有实体 (DM 创建了该实体或分配有该实体的所有权) 时, DM 才能查看和管理作业、固件或配置模板和基线、警报策略、配置文件等与范围内设备关联的实体。有关 DM 可以创建的实体的更多信息, 请参阅 [OpenManage Enterprise 中基于角色的访问控制 \(RBAC\) 权限](#)。

例如, 通过单击 **配置 > 模板**, DM 用户可以查看 DM 用户拥有的默认和自定义模板。此外, DM 用户还可以对拥有的模板执行 RBAC 授权的其他任务。

通过单击 **配置 > 标识池**, DM 用户可以查看管理员或 DM 用户创建的所有标识。DM 还可以对 RBAC 权限指定的标识执行操作。但是, DM 只能查看与 DM 范围下的设备相关联的标识的使用情况。

同样, 通过单击 **配置 > VLAN 池**, DM 可以查看管理员创建的所有 VLAN 并将其导出。DM 不能执行任何其他操作。如果 DM 有模板, 则可以编辑模板以使用 VLAN 网络, 但不能编辑 VLAN 网络。

在 OpenManage Enterprise 中, 可以在创建本地用户或导入 AD/LDAP 用户时分配范围。只能在 Open ID Connect (OIDC) 提供程序上完成 OIDC 用户的范围分配。

本地用户的 SBAC:

在创建或编辑具有 DM 角色的本地用户时, 管理员可以选择一个或多个定义 DM 范围的设备组。

例如, 您 (以管理员身份) 创建名为 dm1 的 DM 用户并分配自定义组下的组 g1。那么, dm1 将仅拥有 g1 中的所有设备的操作访问权限。用户 dm1 将无法访问与任何其他设备相关的任何其他组或实体。

此外, 借助 SBAC, dm1 也将无法查看其他 DM (假设 dm2) 在同一个组 g1 中创建的实体。这意味着 DM 用户将只能查看用户拥有的实体。

例如，您（以管理员身份）创建另一个名为 dm2 的 DM 用户并分配自定义组下的相同组 g1。如果 dm2 为 g1 中的设备创建配置模板、配置基线或配置文件，则 dm1 将无权访问这些实体，反之亦然。

范围为“所有设备”的 DM 对 DM 拥有的所有设备和组实体具有 RBAC 权限指定的操作访问权限。

AD/LDAP 用户的 SBAC:

在导入或编辑 AD/LDAP 组时，管理员可以将范围分配给具有 DM 角色的用户组。如果用户是多个 AD 组（每个都有一个 DM 角色）的成员，并且每个 AD 组都具有不同的范围分配，则用户的范围是这些 AD 组的范围并集。

例如，

- 用户 dm1 是两个 AD 组（RR5-Floor1-LabAdmins 和 RR5-Floor3-LabAdmins）的成员。两个 AD 组都分配有 DM 角色，并且 AD 组的范围分配如下：RR5-Floor1-LabAdmins 获得 ptlab-servers，而 RR5-Floor3-LabAdmins 获得 smdlab-servers。现在，DM dm1 的范围是 ptlab-servers 和 smdlab-servers 的并集。
- 用户 dm1 是两个 AD 组（adg1 和 adg2）的成员。两个 AD 组均分配有 DM 角色，其中 AD 组的范围分配如下：adg1 具有 g1 的访问权限，而 adg2 具有 g2 的访问权限。如果 g1 是 g2 的超集，则 dm1 的范围是较大的范围（g1、其所有子组和所有叶设备）。

如果用户是具有不同角色的多个 AD 组的成员，则功能更高的角色优先（按管理员、DM、查看者的顺序）。

具有无限范围的 DM 对所有设备和组实体具有 RBAC 权限指定的操作访问权限。

注：将 OpenManage Enterprise 升级到版本 3.6.x 后，AD/LDAP 和 OIDC（PingFederate 或 KeyCloak）设备管理者需要重新创建所有先前版本的实体，因为在升级后这些实体仅可供管理员使用。有关更多信息，请参阅发行说明，网址为 <https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs>。

OIDC 用户的 SBAC:

在 OME 控制台内不会进行 OIDC 用户的范围分配。在用户配置过程中，您可以在 OIDC 提供程序中为 OIDC 用户分配范围。当用户使用 OIDC 提供程序凭据登录时，角色和范围分配将可用于 OME。有关配置用户角色和范围的更多信息，请参阅在 PingFederate 中配置 OpenID Connect 提供程序策略，以提供基于角色的 OpenManage Enterprise 访问权限 页面上的 134。

注：如果要使用 PingFederate 作为 OIDC 提供程序，则只能使用管理员角色。有关更多信息，请参阅在 PingFederate 中配置 OpenID Connect 提供程序策略，以提供基于角色的 OpenManage Enterprise 访问权限 页面上的 134 和发行说明（网址为 <https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs>）。

转移所有权：管理员可以将拥有的资源从一个设备管理者（源）转移给另一个设备管理者。例如，管理员可以将分配的资源从源 dm1 转移给 dm2。具有所有拥有实体（如固件和/或配置基线、配置模板、警报策略和配置文件）的设备管理者被视为合格源用户。“所有权转移”仅将实体而不是设备管理者拥有的设备组（范围）转移给另一个设备管理者。有关更多信息，请参阅设备管理者实体的所有权转移 页面上的 129。

相关参考资料

OpenManage Enterprise 用户角色类型 页面上的 13

相关任务

安装 OpenManage Enterprise 页面上的 17

添加和编辑 OpenManage Enterprise 用户

此过程仅限于添加和编辑本地用户。在编辑本地用户时，您可以编辑所有用户属性。但是，对于目录用户，仅可以编辑角色和设备组（对于设备管理者而言）。要在 OpenManage Enterprise 中集成目录服务并导入目录用户，请参阅 OpenManage Enterprise 中的目录服务集成 页面上的 130 和导入 AD 和 LDAP 组 页面上的 129。

注：

- 要对 OpenManage Enterprise 执行任何任务，您必须有必要的用户权限。请参阅 OpenManage Enterprise 中基于角色和范围的访问控制 页面上的 14。
- 您无法启用、禁用或删除管理员/系统/ root 用户。您只能通过单击右侧窗格中的编辑来更改密码。

1. 选择设备设置 > 用户 > 用户 > 添加。
 2. 在添加新用户对话框中：
 - a. 在用户详细信息下，从用户角色下拉菜单中选择“管理员”、“设备管理者”或“查看者”。有关更多信息，请参阅 OpenManage Enterprise 中基于角色和范围的访问控制 页面上的 14。
- 默认情况下，启用复选框已选择，表示已为用户启用当前正在设置的用户权限。

- b. 对于设备管理者角色，范围默认为**所有设备**（无限制范围），但管理员可以通过选择**选择组**选项，然后选择设备组来限制范围。
- c. 在**用户凭证**下，输入**用户名、密码**，然后在**确认密码**字段中再次输入该密码。

注：用户名只能包含字母数字字符（但是允许下划线），密码必须包含至少一个以下字符：大写字母、小写字母、数字和特殊字符。

3. 单击**完成**。

将显示一条消息，表明该用户已成功保存。作业已启动以创建新用户。运行作业后，新用户将会创建并显示在用户列表中。

编辑 OpenManage Enterprise 用户属性

1. 在**应用程序设置**页面中，在**用户**下，选择与用户对应的复选框。
2. 完成**添加和编辑 OpenManage Enterprise 用户** 页面上的 127 中的任务。
保存更新的数据。

注：在您更改用户的角色时，可以自动应用新角色的可用权限。例如，如果您将设备管理者更改为管理员，则为管理员提供的访问权限和特权将自动为设备管理者启用。

启用 OpenManage Enterprise 用户

选择与用户名称对应的复选框，然后单击**启用**。用户已启用，并在**启用**列的对应单元格中显示勾选标记。如果该用户在创建用户名时已经启用，则**启用**按钮将显示为灰色。

相关任务

[删除目录服务](#) 页面上的 132

[删除 OpenManage Enterprise 用户](#) 页面上的 128

[终止用户会话](#) 页面上的 130

相关信息

[管理 OpenManage Enterprise 用户](#) 页面上的 124

禁用 OpenManage Enterprise 用户

选择与用户名对应的复选框，然后单击**禁用**。该用户将被禁用，**已禁用**列相应单元格中的勾选标记将消失。如果该用户在创建用户名时被禁用，则**禁用**按钮将显示为灰色。

相关任务

[删除目录服务](#) 页面上的 132

[删除 OpenManage Enterprise 用户](#) 页面上的 128

[终止用户会话](#) 页面上的 130

相关信息

[管理 OpenManage Enterprise 用户](#) 页面上的 124

删除 OpenManage Enterprise 用户

1. 选中与用户名对应的复选框，然后单击**删除**。
2. 显示提示时，单击**是**。

相关参考资料

[禁用 OpenManage Enterprise 用户](#) 页面上的 128

[启用 OpenManage Enterprise 用户](#) 页面上的 128

相关信息

管理 OpenManage Enterprise 用户 页面上的 124

导入 AD 和 LDAP 组

注:

- 没有管理员权限的用户无法启用或禁用 Active Directory (AD) 和轻量级目录访问协议 (LDAP) 用户。
- 在 OpenManage Enterprise 中导入 AD 组之前，必须在配置 AD 时将用户组包括通用组中。
- 可以导入 AD 和 LDAP 目录用户并为其分配某个 OpenManage Enterprise 角色（管理员、设备管理者或查看者）。在登录到控制台时单点登录 (SSO) 功能停止。在设备上运行操作需要该设备上的特权帐户。
- 将 OpenManage Enterprise 升级到版本 3.6.x 后，AD/LDAP 和 OIDC (PingFederate 或 KeyCloak) 设备管理者需要重新创建所有先前版本的实体，因为在升级后这些实体仅可供管理员使用。有关更多信息，请参阅发行说明，网址为 <https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs>

1. 单击**导入目录组**。
2. 在**导入 Active Directory** 对话框中：
 - a. 从**目录源**下拉菜单中，选择必须为添加组导入的 AD 或 LDAP 源。有关添加目录，请参阅[添加或编辑要用于目录服务的 Active Directory 组](#) 页面上的 131。
 - b. 单击**输入凭据**。
 - c. 在对话框中，键入目录所保存的域的用户名和密码。按照工具提示输入正确的语法。
 - d. 单击**完成**。
3. 在**可用组**部分中：
 - a. 在**查找组**框中，输入测试目录中可用的组名的前几个字母。开头为所输入文本的所有组名都会在“组名”下面列出。
 - b. 选择要导入的组的相应复选框，然后单击 **>>** 或 **<<** 按钮以添加或删除组。
4. 在**要导入的组**部分中：
 - a. 选中组的复选框，然后从“分配组角色”下拉菜单中选择一个角色。有关基于角色访问的更多信息，请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
 - b. 单击**分配角色**。
组中选定目录服务下的用户都会分配到所选的用户角色。
 - c. 对于“设备管理者”角色，范围默认为**所有设备**，但管理员可以通过选择**分配范围**选项，然后选择设备组来限制范围。
5. 重复第 3 和第 4 步，如有必要。
6. 单击**导入**。
导入目录组并让其显示在用户列表中。但是，那些组中的用户将使用他们的域用户名和凭据登录到 OpenManage Enterprise。

域用户（如 john_smith）是可以成为多个目录组和被分配到不同角色的组的成员。在这种情况下，将鼠标悬停在设备标头右边角的用户名上时，会显示设备管理者和查看者等多个角色。此类用户将获得用户所属的所有目录组的最高级别角色。

- 示例 1: 用户属于管理员、DM 和查看者这三个分组。在此情况下，用户将成为管理员。
- 示例 2: 用户属于三个 DM 组和一个查看者组。在此情况下，用户将成为 DM，可以访问三个 DM 角色内的设备组并集。

设备管理者实体的所有权转移

本主题介绍管理员如何将一个设备管理者创建的作业、固件或配置模板和基线、警报策略和配置文件等实体转移给另一个设备管理者。当设备管理者离开组织时，管理员可以启动“所有权转移”。

注:

- 要在 OpenManage Enterprise 上执行此任务，您必须拥有必要的用户权限。 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
- “所有权转移”仅将实体而不是设备管理者拥有的设备组（范围）转移给另一个设备管理者。
- 在启动实体的所有权转移之前，管理员必须先将先前设备管理者拥有的设备组重新分配给将接管的设备管理者。
- 如果将实体的所有权转移到 Active Directory 用户组，则会将所有权转移给该 AD 组的所有成员。

要将作业、固件或配置模板和基线等实体的所有权从一个设备管理者转移给另一个设备管理者，请执行以下操作：

1. 通过单击 **OpenManage Enterprise > 应用程序设置 > 用户 > 转移所有权**，启动“转移所有权”向导。
2. 从**源用户**下拉列表中，选择必须从中转移实体所有权的设备管理者。

注: 源用户将仅列出本地、Active Directory、OIDC 或已删除的设备管理者，这些设备管理者具有关联的作业、固件或配置模板、警报策略和配置文件等实体。

3. 从**目标用户**下拉列表中，选择要将实体转移到的设备管理者。
4. 单击**完成**，然后在提示消息中单击**是**。

所有拥有的实体（如作业、固件或配置模板、警报策略和配置文件）已从“源”设备管理者转移给“目标”设备管理者。

终止用户会话

1. 选择与用户名所对应的复选框，然后单击**终止**。
2. 当提示确认时，单击**是**。
所选用户会话结束，用户已注销。

相关参考资料

禁用 OpenManage Enterprise 用户 页面上的 128
启用 OpenManage Enterprise 用户 页面上的 128

相关信息

管理 OpenManage Enterprise 用户 页面上的 124

OpenManage Enterprise 中的目录服务集成

目录服务使您能够导入来自 AD 或 LDAP 的目录组以供在控制台上使用。OpenManage Enterprise 支持以下目录服务的集成：

1. Windows Active Directory
2. Windows AD/LDS
3. OpenLDAP
4. PHP LDAP

LDAP 集成的前提条件/支持的属性

表. 28: LDAP 集成的 OpenManage Enterprise 前提条件/支持的属性

	用户登录属性	组成员身份的属性	证书要求
AD/LDAP	Cn、sAMAccountName	Member	<ul style="list-style-type: none">• 根据域控制器证书的需要决定是否具有 FQDN。SAN 字段可以有 IPv4 和/或 IPv6 或 FQDN。• 仅支持 Base64 证书格式
OpenLDAP	uid、sn	Uniquemember	仅支持 PEM 证书格式
PHP LDAP	uid	MemberUid	

用于目录服务集成的用户前提条件

在开始使用目录服务集成之前，您必须确保满足以下用户前提条件：

1. BindDN 用户和用于“测试连接”的用户应相同。
2. 如果提供了用户登录的属性，则设备登录仅允许使用分配给该属性的相应用户名值。
3. 用于测试连接的用户应属于 LDAP 中的任何非默认组
4. 组成员资格的属性应具有用户的“userDN”或短名称（用于登录）。
5. 当 MemberUid 用作“组成员资格属性”时，在设备登录中使用的用户名在某些 LDAP 配置中将被视为区分大小写。
6. 在 LDAP 配置中使用搜索筛选器时，不允许不属于提及的搜索条件的用户登录。
7. 只有当组在所提供的组成员资格属性下分配了用户时，组搜索才会工作。

- 注:** 如果 OpenManage Enterprise 在 IPv6 网络上托管, 而将 IPv4 设置为 DNS 中的首选地址, 则使用 FQDN 对域控制器进行 SSL 身份验证将会失败。要避免这种失败, 请执行以下任一操作:
- 使用 FQDN 查询时, DNS 应设置为返回 IPv6 作为首选地址。
 - DC 证书的 SAN 字段中需要有 IPv6。

要使用目录服务:

- 添加目录连接。请参阅[添加或编辑要用于目录服务的 Active Directory 组](#) 页面上的 131。
- 导入目录组并将组中所有用户映射到特定角色。请参阅[导入 AD 和 LDAP 组](#) 页面上的 129。
- 对于 DM 用户, 编辑目录组以添加 DM 可以管理的组。请参阅[添加和编辑 OpenManage Enterprise 用户](#) 页面上的 127。

添加或编辑要用于目录服务的 Active Directory 组

1. 单击[应用程序设置](#) > [用户](#) > [目录服务](#), 然后单击**添加**。
2. 在[连接到目录服务](#)对话框中, **AD** 默认处于选中状态, 表示目录类型是 Active Directory (AD):
 - 注:** 要通过使用目录服务创建 LDAP 用户组, 请参阅[添加或编辑要用于目录服务的轻量级目录访问协议组](#) 页面上的 131。
- a. 输入 AD 目录的名称。
- b. 选择域控制器查找方法:
 - **DNS:** 在**方法**框中, 输入用于查询域控制器的 DNS 的域名。
 - **手动:** 在**方法**框中, 输入域控制器的 FQDN 或 IP 地址。对于多个服务器的情况, 最多支持三个服务器, 以逗号分隔。
- c. 在**组域**框中, 按照工具提示语法中的建议输入组域。
3. 在**高级选项**部分中:
 - a. 默认情况下, 填入全局编录地址端口号 3269。对于域控制器访问, 请输入 636 作为端口号。
 - 注:** 只支持 LDAPS 端口。
 - b. 以秒为单位输入网络超时和搜索超时持续时间。支持的最长超时持续时间为 300 秒。
 - c. 要上载 SSL 证书, 请选择**证书验证**, 并单击**选择文件**。证书应为以 Base64 格式编码的根 CA 证书。此时会显示**测试连接**页面。
4. 单击**测试连接**。
5. 在对话框中, 输入要连接的域的用户名和密码。
 - 注:** 用户名必须以 UPN (用户名@域) 格式或以 NetBIOS (域\用户名) 格式输入。
6. 单击**测试连接**。
此时, **目录服务信息**对话框中会显示一条消息, 表明连接成功。
7. 单击**确定**。
8. 单击**完成**。
此时会创建并运行一个作业, 将请求的目录添加到目录服务列表中。
1. 在**目录名称**列中, 选择该目录。此时, 目录服务属性会显示在右侧窗格中。
2. 单击**编辑**。
3. 在[连接到目录服务](#)对话框中, 编辑数据并单击**完成**。此时, 数据已更新并保存。

添加或编辑要用于目录服务的轻量级目录访问协议组

1. 单击[应用程序设置](#) > [用户](#) > [目录服务](#), 然后单击**添加**。
2. 在[连接到目录服务](#)对话框中, 选择 **LDAP** 作为目录类型。
 - 注:** 要通过使用目录服务创建 AD 用户组, 请参阅[添加或编辑要用于目录服务的 Active Directory 组](#) 页面上的 131。
- a. 输入 LDAP 目录的所需名称。
- b. 选择域控制器查找方法:

- **DNS**: 在**方法**框中, 输入用于查询域控制器的 DNS 的域名。
 - **手动**: 在**方法**框中, 输入域控制器的 FQDN 或 IP 地址。对于多个服务器的情况, 最多支持三个服务器, 以逗号分隔。
- c. 输入 LDAP Bind 可分辨名称 (DN) 和密码。
- i** **注**: AD LDS 不支持匿名绑定。
3. 在**高级选项**部分中:
- a. 默认情况下, 636 的 LDAP 端口号已填充。如需更改, 请输入端口号。
- i** **注**: 只支持 LDAPS 端口。
- b. 要匹配服务器上的 LDAP 配置, 请输入组的基本识别名以进行搜索。
- c. 输入 LDAP 系统中已配置的用户属性。建议此 UID 在所选基本可分辨名称中是唯一的。否则, 请配置搜索筛选器以确保它是唯一的。如果无法通过属性和搜索筛选器的搜索组合来唯一标识用户可分辨名称, 登录操作将会失败。
- i** **注**: 应该先在用于查询的 LDAP 系统中配置用户属性, 然后集成在目录服务上。
- i** **注**: 对于 AD LDS 配置, 您需要为用户属性输入 **cn** 或 **sAMAccountName**, 对于 LDAP 配置输入 **UID**。
- d. 在**组成员身份的属性**框中, 输入将组和成员信息存储在目录中的属性。
- e. 以秒为单位输入网络超时和搜索超时持续时间。支持的最长超时持续时间为 300 秒。
- f. 要上载 SSL 证书, 请选择**证书验证**, 并单击**选择文件**。证书应为以 Base64 格式编码的根 CA 证书。此时会启用**测试连接**按钮。
4. 单击**测试连接**, 然后输入要连接到的域的绑定用户凭据。
- i** **注**: 测试连接时, 请确保**测试用户名**是之前输入的**用户登录属性**的值。
5. 单击**测试连接**。
此时, **目录服务信息**对话框中会显示一条消息, 表明连接成功。
6. 单击**确定**。
7. 单击**完成**。
此时会创建并运行一个作业, 将请求的目录添加到目录服务列表中。
1. 在**目录名称**列中, 选择该目录。此时, 目录服务属性会显示在右侧窗格中。
 2. 单击**编辑**。
 3. 在**连接到目录服务**对话框中, 编辑数据并单击**完成**。此时, 数据已更新并保存。

删除目录服务

选择与要删除的目录服务对应的复选框, 然后单击**删除**。

相关参考资料

[禁用 OpenManage Enterprise 用户](#) 页面上的 128

[启用 OpenManage Enterprise 用户](#) 页面上的 128

相关信息

[管理 OpenManage Enterprise 设备设置](#) 页面上的 123

[管理 OpenManage Enterprise 用户](#) 页面上的 124

使用 OpenID Connect 提供程序登录 OpenManage Enterprise

您可以使用 OpenID Connect (OIDC) 提供程序进行登录。OpenID Connect 提供程序是允许用户安全地访问应用程序的身份和用户管理软件。目前，OpenManage Enterprise 为 PingFederate 和 Keycloak 提供支持。

警告: 在向 OIDC 提供程序 PingFederate (PingIdentity) 重新注册客户端时，用户角色和范围会重置为“默认值”。此问题可能导致将非管理员角色 (DM 与查看者) 的权限和范围重置为管理员的权限和范围。在设备升级、网络配置更改或 SSL 证书更改的情况下，将触发向 OIDC 提供程序重新注册设备控制台。

要在上述任何重新注册事件后避免出现安全问题，管理员必须在 PingFederate 站点上重新配置所有 OpenManage Enterprise 客户端 ID。此外，我们强烈建议使用 Pingfederate 仅为管理员用户创建客户端 ID，直到此问题得到解决为止。

注:

- 要对 OpenManage Enterprise 执行任何任务，您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。
- 在设备中，只能添加最多四个 OpenID Connect 提供程序 ID。
- 将 OpenManage Enterprise 升级到版本 3.6.x 后，AD/LDAP 和 OIDC (PingFederate 或 KeyCloak) 设备管理者需要重新创建所有先前版本的实体，因为在升级后这些实体仅可供管理员使用。有关更多信息，请参阅发行说明，网址为 <https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs>

前提条件:

启用 OpenID Connect 提供程序登录之前，必须执行以下操作:

- 在 OpenManage Enterprise 中添加 OIDC 提供程序:** 在 OpenManage Enterprise 应用程序设置中，添加 OpenID Connect 提供程序。添加 OpenID Connect 提供程序时，将为 OpenID Connect 提供程序生成客户端 ID。有关详情，请参阅: [将 OpenID Connect 提供程序添加到 OpenManage Enterprise](#) 页面上的 134。
- 使用客户端 ID 配置 OpenID Connect 提供程序:** 在 OpenID Connect 提供程序中，通过添加和映射名为 **dxqua** 的范围 (用户验证的戴尔扩展声明)，找到客户端 ID 并定义登录角色 (管理员、设备管理者或查看者)。有关更多信息，请参阅:
 - 在 PingFederate 中配置 OpenID Connect 提供程序策略，以提供基于角色的 OpenManage Enterprise 访问权限 页面上的 134
 - 在 Keycloak 中配置 OpenID Connect 提供程序策略，以提供基于角色的 OpenManage Enterprise 访问权限 页面上的 135

在 OpenManage Enterprise 中添加 OpenID Connect 提供程序后，它将在 **应用程序设置 > 用户 > OpenID Connect 提供程序** 页面中列出。将显示以下 OIDC 提供程序详细信息:

- 名称 - 在设备中添加 OpenID Connect 提供程序时的名称
- 启用 - 此字段中的对勾表示已在设备中启用了 OpenID Connect 提供程序
- 查找 URI — OpenID Connect 提供程序的 URI (统一资源标识符)
- 注册状态 - 可以是以下值之一:
 - 成功 - 表示向 OpenID Connect 提供程序注册成功
 - 失败 - 表示向 OpenID Connect 提供程序注册失败。如果 OpenID Connect 提供程序注册的状态为“失败”，即使其被启用也不会被允许。
 - 进行中 - 当设备尝试向 OpenID Connect 提供程序注册时会显示此状态。

在右侧窗格中，将显示所选 OpenID Connect 提供程序的客户端 ID、注册状态、查找 URI。您可以单击 [查看详细信息](#) 来查看 OpenID Connect 提供程序的证书详细信息。

在 **应用程序设置 > 用户 > OpenID Connect 提供程序** 页面中，您可以执行以下操作:

- 将 OpenID Connect 提供程序添加到 OpenManage Enterprise 页面上的 134
- 在 OpenManage Enterprise 中编辑 OpenID Connect 提供程序的详细信息 页面上的 135
- 测试 OpenManage Enterprise 向 OpenID Connect 提供程序的注册状态 页面上的 135
- 启用 OpenID Connect 提供程序 页面上的 136
- 禁用 OpenID Connect 提供程序 页面上的 136
- 删除 OpenID Connect 提供程序 页面上的 136

将 OpenID Connect 提供程序添加到 OpenManage Enterprise

添加、启用和注册 OpenID Connect 提供程序 (Keycloak 或 PingFederate) 可允许授权客户端登录 OpenManage Enterprise。这将生成客户端 ID。

要将 OpenID Connect 提供程序添加到 OpenManage Enterprise，请转至 **应用程序设置 > 用户 > OpenID Connect 提供程序** 页面并执行以下操作：

注：只能添加最多四个 OpenID Connect 提供程序客户端。

1. 单击**添加**以激活“添加新的 OpenID Connect 提供程序”页面。
2. 在相应的字段中填入以下信息：
 - a. 名称 - OIDC 客户端的名称。
 - b. 查找 URI - OIDC 提供程序的统一资源标识符
 - c. 验证类型 - 选择访问令牌必须用来访问设备的以下方法之一：
 - i. 初始访问令牌 - 提供初始访问令牌
 - ii. 用户名和密码 - 提供用户名和密码
 - d. (可选) 证书验证复选框 - 您可以选中该复选框然后上传 OIDC 提供程序的证书，方法是单击**浏览**并找到证书，或者将证书拖放到虚线框中。
 - e. (可选) 测试连接 - 单击**测试 URI 和 SSL 连接**以测试与 OpenID Connect 提供程序的连接。

注：测试连接不依赖于用户名和密码或初始访问令牌详细信息，因为它只检查提供的查找 URI 的有效性。
 - f. (可选) “启用”复选框 - 您可以选中该复选框以允许授权客户端访问令牌登录到设备。
3. 单击**完成**。

在“应用程序设置 > 用户 > OpenID Connect 提供程序”页面中列出了新添加的 OpenID Connect 提供程序，并且客户端 ID 可以位于右侧窗格中。

后续步骤：

在 PingFederate 中配置 OpenID Connect 提供程序策略，以提供基于角色的 OpenManage Enterprise 访问权限 页面上的 134

在 Keycloak 中配置 OpenID Connect 提供程序策略，以提供基于角色的 OpenManage Enterprise 访问权限 页面上的 135

在 PingFederate 中配置 OpenID Connect 提供程序策略，以提供基于角色的 OpenManage Enterprise 访问权限

要启用使用 PingFederate 的 OpenManage Enterprise OpenID Connect 登录，您必须添加范围 **dx cua** (用户验证的戴尔扩展声明) 并将其映射到客户端 ID，然后按如下所示定义用户权限：

警告：在向 OIDC 提供程序 PingFederate (PingIdentity) 重新注册客户端时，用户角色和范围会重置为“默认值”。此问题可能会将非管理员角色 (DM 与查看者) 的权限和范围重置为管理员的权限和范围。在设备升级、网络配置更改或 SSL 证书更改的情况下，将触发向 OIDC 提供程序重新注册设备控制台。

要在上述任何重新注册事件后避免出现安全问题，管理员必须在 PingFederate 站点上重新配置所有 OpenManage Enterprise 客户端 ID。此外，我们强烈建议使用 Pingfederate 仅为管理员用户创建客户端 ID，直到此问题得到解决为止。

注：

- 默认的分配算法应为 RS256 (使用 SHA-256 的 RSA 签名)。

1. 在 OAuth 设置中的“范围管理”下添加名为 **dx cua** 的“独占”或“默认”范围。
2. 按照以下步骤映射在 **OpenID Connect 策略 > 管理策略** 中创建的范围：
 - a. 启用**在令牌中包括用户信息**
 - b. 在属性范围中，添加范围和属性值为 **dx cua**。
 - c. 在“合同履行”中，添加 **dx cua** 并选择类型为“文本”。然后，使用以下属性之一定义 OpenManage Enterprise OpenID Connect 提供程序登录的用户权限：
 - i. 管理员: `dx cua : [{"Role": "AD"}]`
 - ii. 设备管理者: `dx cua : [{"Role": "DM"}]`

注：要将设备管理者的访问权限限制为选择设备组，假设 G1 和 G2，请在 OpenManage Enterprise 中使用 `dx cua : [{"Role": "DM", "Entity": "G1, G2"}]`
 - iii. 查看者: `dx cua : [{"Role": "VE"}]`

- d. 如果在 OpenManage Enterprise 中注册客户端后配置了“独占”范围，请在 PingFederate 中编辑已配置的客户端，并启用创建的“dxcua”独占范围。
3. 应在 PingFederate 中为 OpenManage Enterprise 客户端注册启用**动态客户端注册**。如果在 OpenID Connect 提供程序客户端设置中未选择“需要初始访问令牌”选项，注册将使用用户名和密码。如果启用了此选项，则注册将仅使用初始访问令牌。

在 Keycloak 中配置 OpenID Connect 提供程序策略，以提供基于角色的 OpenManage Enterprise 访问权限

要启用使用 Keycloak 的 OpenManage Enterprise OpenID Connect 登录，您必须先添加范围 **dxcua** 并将其映射到客户端 ID，然后按如下所示定义用户权限：

注：在 OpenID Connect 提供程序配置向导中指定的查找 URI 应具有列出的提供程序的有效端点。

1. 在 Keycloak 用户的属性部分中，使用以下属性之一为 OpenManage Enterprise 登录角色定义“键和值”：
 - 管理员：dxcua : [{"Role": "AD"}]
 - 设备管理者：dxcua : [{"Role": "DM"}]
 - 注：**要将设备管理者的访问权限限制为选择设备组，假设 G1 和 G2，请在 OpenManage Enterprise 中使用 dxcua : [{"Role": "DM", "Entity": "G1, G2"}]
 - 查看者：dxcua : [{"Role": "VE"}]
2. 在 Keycloak 中注册客户端后，在“映射器”部分中，添加具有以下值的“用户属性”映射器类型：
 - 名称：dxcua
 - 映射器类型：用户属性
 - 用户属性：dxcua
 - 令牌声明名称：dxcua
 - 声明 Json 类型：字符串
 - 添加到 ID 令牌：启用
 - 添加到访问令牌：启用
 - 添加到用户信息：启用

测试 OpenManage Enterprise 向 OpenID Connect 提供程序的注册状态

在**应用程序设置 > 用户 > OpenID Connect 提供程序**页面上，执行以下操作：

1. 选择 OpenID Connect 提供程序。
2. 在右侧窗格中，单击**测试注册状态**。

注：测试连接不依赖于用户名和密码或初始访问令牌详细信息，因为它只检查查找 URI 的有效性。

此时会更新 OIDC 提供程序的最新注册状态（“成功”或“失败”）。

在 OpenManage Enterprise 中编辑 OpenID Connect 提供程序的详细信息

在**应用程序设置 > 用户 > OpenID Connect 提供程序**页面上，执行以下操作：

1. 选择 OpenID Connect 提供程序。
2. 单击右侧窗格中的**编辑**。
3. 根据 OpenID Connect 提供程序客户端的注册状态，您可以执行以下操作：
 - a. 如果注册状态为“成功”，则仅可编辑证书验证、测试连接和“已启用”复选框。
 - b. 如果注册状态为“失败”，则您可以编辑用户名、密码、证书验证、测试连接和“已启用”复选框。
4. 单击**完成**以执行，或者单击**取消**放弃更改。

启用 OpenID Connect 提供程序

如果在将 OpenID Connect 提供程序添加到设备时未启用它的登录，则要激活登录，您必须在设备中“启用”登录。

在**应用程序设置 > 用户 > OpenID Connect 提供程序**页面上，执行以下操作：

1. 选择一个或多个 OpenID Connect 提供程序。
2. 单击**启用**。

在 OpenManage Enterprise 中启用 OpenID Connect 提供程序将允许授权客户端访问令牌登录到设备。

删除 OpenID Connect 提供程序

在**应用程序设置 > 用户 > OpenID Connect 提供程序**页面上，执行以下操作：

1. 选择一个或多个 OpenID Connect 提供程序。
2. 单击**删除**。

禁用 OpenID Connect 提供程序

在**应用程序设置 > 用户 > OpenID Connect 提供程序**页面上，执行以下操作：

1. 选择一个或多个 OpenID Connect 提供程序。
2. 单击**禁用**。

设备将拒绝“禁用”的 OIDC 提供程序的客户端访问令牌。

安全证书

通过单击**应用程序设置安全证书**，您可以查看有关设备的当前可用 SSL 证书的信息。

注：要对 OpenManage Enterprise 执行任何任务，您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

要生成证书签名请求 (CSR)，请参阅[生成并下载证书签名请求](#) 页面上的 136。

生成并下载证书签名请求

为设备生成证书签名请求 (CSR)，然后申请 SSL：

注：您只能从 OpenManage Enterprise 设备中生成 CSR。

1. 单击**生成证书签名请求**。
2. 在**生成证书签名请求**对话框中，在字段中输入信息。
3. 单击**生成**。
CSR 将会创建并显示在**证书签名请求**对话框中。也会向您请求中提供的电子邮件地址发送 CSR 副本。
4. 在**证书签名请求**对话框中，在申请 SSL 证书时，复制 CSR 数据并将它提交给认证机构 (CA)。
 - 要下载 CSR，请单击**下载证书签名请求**。
 - 单击**完成**。

使用 Microsoft Certificate Services 将 Web 服务器证书分配给 OpenManage Enterprise

1. 在 OpenManage Enterprise 中生成并下载证书签名请求 (CSR)。请参阅 [生成并下载证书签名请求](#) 页面上的 136
2. 打开到证书服务器 (<https://x.x.x.x/certsrv>) 的 Web 会话，然后单击**请求证书**链接。
3. 在“请求证书”页面上，单击**提交高级证书请求**链接。

4. 在“高级证书请求”页面上，单击使用 **Base 64 编码的 CMC 或 PKCS#10 文件提交证书请求**，或使用 **Base 64 编码 PKCS#7 文件提交续订请求**。
5. 在“提交证书请求或续订请求”页面上，执行以下操作：
 - a. 在 **Base 64 编码的证书请求 (CMC 或 PKCS#10 文件或 PKCS#7)** 字段中，复制并粘贴已下载 CSR 的所有内容。
 - b. 对于**证书模板**，请选择 **Web 服务器**。
 - c. 单击**提交**以颁发证书。
6. 在“颁发的证书”页面上，选择 **Base 64 编码**选项，然后单击**下载证书**链接以下载证书。
7. 通过导航至**应用程序设置 > 安全 > 证书**页面，然后单击**上传**，在 OpenManage 中上传证书。

设置登录安全性属性

注：要对 OpenManage Enterprise 执行任何任务，您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

注：可以导入 AD 和 LDAP 目录用户并为其分配某个 OpenManage Enterprise 角色（管理员、设备管理者或查看者）。

通过单击 **OpenManage Enterprise > 应用程序设置 > 安全性**，您可以通过指定**限制允许的 IP 范围**或**登录锁定策略**来保护您的 OpenManage Enterprise。

展开**限制允许的 IP 范围**：

注：在应用装置中配置“限制允许的 IP 范围”时，对于给定范围之外的设备，将阻止传入应用装置的任何连接，如警报接收、固件更新和网络标识。但是，从应用装置传出的任何连接将在所有设备上正常运行。

1. 要指定必须能够访问 OpenManage Enterprise 的 IP 地址范围，请选择**启用 IP 范围**复选框。
2. 在 **IP 地址范围 (CIDR)** 框中输入 IP 地址范围。

注：只允许输入一个 IP 范围。

3. 单击**应用**。要重设为默认属性，请单击**放弃**。

注：如果在 **IP 地址范围 (CIDR)** 框中输入了多个 IP 范围，将无法启用**应用**按钮。

展开**登录锁定策略**：

1. 选择**按用户名**复选框，以防特定用户名登录到 OpenManage Enterprise。
2. 选择**按 IP 地址**复选框，以防特定 IP 地址登录到 OpenManage Enterprise。
3. 在**锁定失败计数**框中输入不成功尝试的次数，超过该数字后，OpenManage Enterprise 必须阻止用户进一步登录。默认情况下，3 次尝试次数。
4. 在**锁定失败窗口**框中输入一个持续时间，在该时间内，OpenManage Enterprise 必须显示失败登录尝试的信息。
5. 在**锁定惩罚时间**框中，输入一个持续时间，如果用户多次登录尝试失败，则在该时间内不能再尝试登录。
6. 单击**应用**。要将设置重置为默认属性，请单击**放弃**。

管理控制台首选项

注：要对 OpenManage Enterprise 执行任何任务，您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

通过单击 **OpenManage Enterprise > 应用程序设置 > 控制台首选项**，您可以设置 OpenManage Enterprise GUI 的默认属性。例如，在仪表板上自动检查和更新设备运行状况的默认时间以及用于查找设备的首选设置。下列选项可用：

1. **报告设置：**要设置最大行数，您可以在 OpenManage Enterprise 上查看：
 - a. 展开**报告设置**。
 - b. 在**报告行限制**框中输入数字。默认限制设置为 1,000 行，但允许的最大行数为 2,000,000,000。
 - c. 单击**应用**。作业已运行且设置已应用。
2. **设备运行状况：**必须在 OpenManage Enterprise 仪表板上自动监测和更新设备的运行状况。在此之后，设置时间：
 - a. 展开**设备运行状况**。
 - b. 输入必须记录设备运行状况和存储数据的频率。
 - c. 选择：
 - **最后已知：**显示电源连接中断时最新记录的设备运行状况。
 - **未知：**显示设备状态变为“未知”时最新记录的设备运行状况。与 iDRAC 之间的连接中断且设备不再受 OpenManage Enterprise 监测时，设备对 OpenManage Enterprise “未知”。
 - d. 单击**应用**以保存对设置的更改，或单击**放弃**以将设置重置为默认属性。

3. **查找设置**：展开“查找设置”，通过使用**常规设备命名**和**服务器设备命名**设置，设置 OpenManage Enterprise 使用的设备命名，以标识查找到的 iDRAC 和其他设备。

注：“常规设备命名”和“服务器设备命名”中的设备命名选项彼此独立，彼此互不影响。

a. **常规设备命名**适用于 iDRAC 以外的其他所有已查找到的设备。选择以下命名模式之一：

- **DNS**，使用 DNS 名称。
- **Instrumentation (NetBIOS)**，使用 NetBIOS 名称。

注：

- 常规设备命名的默认设置为 **DNS**。
- 如果查找到的任何设备的 DNS 名称或 NetBIOS 名称无法满足该设置，则设备将使用这些设备的 IP 地址来标识这些设备。
- 如果在**常规设备命名**中选择了 **Instrumentation (NetBIOS)** 选项，则对于机箱设备，**机箱名称**会显示为“所有设备”页上的“设备名称”条目。

b. **服务器设备命名**仅适用于 iDRAC。为查找到的 iDRAC 选择以下命名模式之一：

- **iDRAC 主机名**，使用 iDRAC 主机名。
- **系统主机名**，使用系统主机名。

注：

- iDRAC 设备的默认命名首选项是**系统主机名**。
- 如果任何 iDRAC 所具有的 iDRAC 主机名或系统主机名无法满足该设置，则设备将使用此类 iDRAC 的 IP 地址来标识这些 iDRAC。

c. 指定无效的设备主机名和常见的 MAC 地址，请展开**高级设置**

- 在**无效设备主机名**中输入一个或多个由逗号分隔的无效主机名。默认情况下，填入无效设备主机名列表。
- 在**常见的 MAC 地址**中输入由逗号分隔的常见的 MAC 地址。默认情况下，填入常见的 MAC 地址列表。

d. 单击**应用**以保存对设置的更改，或单击**放弃**以将设置重置为默认属性。

4. **服务器发起的查找**。选择以下某个查找批准策略：

- **自动**：允许控制台自动查找具有 iDRAC 固件版本 4.00.00.00（与控制台位于同一网络）的服务器。
- **手动**：由用户手动查找服务器。
- 单击**应用**以保存更改，或单击**放弃**以将设置重置为默认属性。

5. **MX7000 启用首选项**：在启用 MX7000 机箱时指定以下一种警报转发行为：

- 接收所有警报
- 仅接收“机箱”类别警报

6. **SMB 设置**：选择一个必须用于网络通信的服务器消息块 (SMB) 版本。

- **禁用 V1**：SMBv1 已禁用。这是设备中的默认选项。
- **启用 V1**：启用 SMBv1。

注：请确保先在 **SMB 设置** 中启用 SMBv1，然后才能在任何机箱上或具有 iDRAC 版本 2.50.50.50 及更早版本的 PowerEdge YX2X 和 YX3X 服务器上开始任何任务。有关详情，请参阅**管理控制台首选项** 页面上的 137 和 **Dell EMC PowerEdge 服务器的通用命名惯例** 页面上的 154。

7. **电子邮件发件人设置**：要设置发送电子邮件消息的用户的地址：

- 在**发件人电子邮件 ID**框中输入电子邮件地址。
- 单击**应用**以保存更改，或单击**放弃**以将设置重置为默认属性。

8. **陷阱转发格式**：要设置陷阱转发格式 —

a. 选择下列选项之一

- **原始格式 (仅对 SNMP 陷阱有效)**：将陷阱数据保留原样。
- **标准化 (对所有事件有效)**：对陷阱数据进行标准化。当陷阱转发格式设置为“标准化”时，接收代理（例如 Syslog）会收到一个标签，其中包含转发警报来自的设备 IP。

b. 单击**应用**以保存更改，或单击**放弃**以将设置重置为默认属性。

9. **指标收集设置**：要设置 PowerManager 扩展数据维护和清除的频率，请执行以下操作：

- 在**数据清除间隔**框中，输入要删除 PowerManager 数据的频率。您可以输入介于 30 - 365 天内的值。
- 单击**应用**以保存更改，或单击**放弃**以将设置重置为默认属性。

自定义警报显示

1. 单击 **OpenManage Enterprise 应用程序设置 > 警报**，然后展开**警报显示设置**。

2. 选择以下选项之一：

- a. **全部** - 允许显示已确认和未确认的警报。
- b. **未确认** - 只允许显示未确认的警报。

注: 默认情况下，警报显示设置为未确认。

- c. **已确认** - 只允许显示已确认的警报。

3. 单击应用。

对“警报显示设置”的更改将会影响以下 OpenManage Enterprise 页面：

- 所有 OpenManage Enterprise 页面的右上角。请参阅 [OpenManage Enterprise 图形用户界面概述](#) 页面上的 29。
- 在“仪表盘”页面上。请参阅 [使用 OpenManage Enterprise 仪表盘监测设备](#) 页面上的 31。
- “设备”页面。请参阅 [环形图](#) 页面上的 32。
- **警报日志表**，在“警报”页面下。请参阅 [查看警报日志](#) 页面上的 97。

配置 SMTP、SNMP 和 Syslog 警报

通过单击 **OpenManage Enterprise > 应用程序设置 > 警报**，您可以配置接收系统警报、SNMP 警报转发目标和 Syslog 转发属性的电子邮件 (SMTP) 地址。要管理这些设置，您必须具有 OpenManage Enterprise 管理员级凭据。

要配置和验证负责管理用户和 OpenManage Enterprise 之间电子邮件通信的 SMTP 服务器，请执行以下操作：

1. 展开**电子邮件配置**。
2. 输入发送电子邮件消息的 SMTP 服务器网络地址。
3. 要验证 SMTP 服务器，请选中**启用验证**复选框，然后输入用户名和密码。
4. 默认情况下，要访问的 SMTP 端口号为 25。必要时可进行编辑。
5. 选择**使用 SSL**复选框来保护您的 SMTP 事务。
6. 要测试 SMTP 服务器是否正常工作，请单击**发送测试电子邮件**复选框，然后输入**电子邮件收件人**。
7. 单击**应用**。
8. 要将设置重置为默认属性，请单击**放弃**。

要配置 SNMP 警报转发配置，请执行以下操作：

1. 展开**SNMP 警报转发配置**。
2. 选择**启用**复选框以启用各自的 SNMP 陷阱以在发生预定义事件时发送警报。
3. 在**目标地址**框中，输入必须接收警报的目标设备的 IP 地址。

注: 不允许输入控制台 IP，以避免出现重复的警报。
4. 从**SNMP 版本**菜单中，选择 SNMP 版本类型为 SNMPv1、SNMPv2 或 SNMPv3 并填写以下字段：
 - a. 在社区字符串框中，输入必须接收警报的设备的 SNMP 社区字符串。
 - b. 根据需要编辑端口号。SNMP 陷阱的默认端口编号=162。请参阅 [OpenManage Enterprise 中支持的协议和端口](#) 页面上的 26。
 - c. 如果选择了 SNMPv3，请提供以下附加详细信息：
 - i. 用户名：提供用户名。
 - ii. 验证类型：从下拉列表中选择 SHA、MD_5 或“无”。
 - iii. 验证密码：提供至少包含八个字符的验证密码。
 - iv. 隐私类型：从下拉列表中选择 DES、AES_128 或“无”。
 - v. 隐私密码：提供至少包含八个字符的隐私密码。
5. 要测试 SNMP 消息，请单击相应陷阱的**发送**按钮。
6. 单击**应用**。要将设置重置为默认属性，请单击**放弃**。

要更新 Syslog 转发配置，请执行以下操作：

1. 展开**Syslog 转发配置**。
2. 选择该复选框以在**服务器**列中各自的服务器上启用 Syslog 功能。
3. 在**目标地址/主机名称**框中，输入接收 Syslog 消息的设备的 IP 地址。
4. 使用 UDP 的默认端口编号=514。如有必要，可通过输入或从框中选择进行编辑。请参阅 [OpenManage Enterprise 中支持的协议和端口](#) 页面上的 26。
5. 单击**应用**。
6. 要将设置重置为默认属性，请单击**放弃**。

管理传入警报

注: 要对 OpenManage Enterprise 执行任何任务，您必须有必要的用户权限。请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14。

通过单击 **OpenManage Enterprise > 应用程序设置 > 传入警报**，您可以设置 TrapForward 属性并定义接收传入 SNMPv3 警报的用户。

• 为传入警报设置 SNMP 凭据：

1. 选择 **SNMPV3 启用** 复选框。
2. 单击 **凭据**。
3. 在 **SNMP 凭据** 对话框中：
 - a. 在 **用户名** 框中，输入管理 OpenManage Enterprise 设置的用户的登录 ID。
 - b. 从 **验证类型** 下拉菜单中，选择 **SHA** 或 **MD_5** 算法作为验证类型。
 - c. 在 **验证密码** 框中，根据您的选择，输入与 SHA 或 MD_5 相关的密码。
 - d. 从 **隐私类型** 下拉菜单中，选择 **DES** 或 **AES_128** 作为您的加密标准。
 - e. 在 **隐私密码** 框中，根据您的隐私类型输入密码。
 - f. 单击 **保存**。
4. 在 **团体** 框中，输入团体字符串以接收 SNMP 陷阱。
5. 默认情况下，传入陷阱的 SNMP 端口号为 162。编辑以更改端口号。
6. 单击 **应用**。
SNMP 凭据和设置将被保存。
7. 要将设置重置为默认属性，请单击 **放弃**。

注: 如果在升级一体机之前已配置 SNMPv3 警报设置，您需要通过提供用户名、身份验证密码和隐私密码来重新配置此设置，以继续接收警报。如果问题仍然存在，请使用文本用户界面 (TUI) 重新启动服务。

8. 单击 **应用** 以保存更改，或单击 **放弃** 以重置为取消。


设置 SNMP 凭据

1. 单击 **凭据**。
2. 在 **SNMP 凭据** 对话框中：
 - a. 在 **用户名** 框中，输入管理 OpenManage Enterprise 设置的用户的登录 ID。
 - b. 从 **验证类型** 下拉菜单中，选择 **SHA** 或 **MD_5** 算法作为验证类型。
 - c. 在 **验证密码** 框中，根据您的选择，输入与 SHA 或 MD_5 相关的密码。
 - d. 从 **隐私类型** 下拉菜单中，选择 **DES** 或 **AES_128** 作为您的加密标准。
 - e. 在 **隐私密码** 框中，根据您的隐私类型输入密码。
3. 单击 **保存**。

管理保修设置

保修设置 确定在主页警报小部件、跨所有页面的警示牌、保修页面和报告中显示的 OpenManage Enterprise 保修统计数据。

要更改保修设置，请执行以下操作：

1. 单击 **OpenManage Enterprise > 应用程序设置 > 保修**
2. 单击 **保修设置** 以激活对话框。
3. 在 **如果保修即将过期则显示警告** 框中，输入天数。您可以输入 0-1000 的值（含这两个值）。默认值设为 90 天。基于此设置的保修即将过期表现为  在报告和小部件中。
4. 在 **隐藏过期的保修** 选项中，您可以选择以下选项之一：
 - a. **全部**：隐藏已过期的所有“初始”以及“延长”保修的显示。
 - b. **仅初始**：仅隐藏已过期的“初始”保修。
 - c. **无**：显示所有过期的保修。
5. 单击 **应用** 或 **放弃**，以保存保修设置，或放弃更改并保留旧设置。

检查并更新 OpenManage Enterprise 及可用插件的版本

要转到“控制台和插件”页面，请单击**应用程序设置 > 控制台和插件**。在“控制台和插件”页面上，您可以执行以下操作：

1. 查看 OpenManage Enterprise 的当前版本，检查是否有可用更新，然后再升级到较新版本。您可以单击**更新设置**按钮以执行以下操作：
 - a. 自动或手动检查更新。
 - b. 选择通过联机或脱机模式更新一体机。有关详情，请参阅 [OpenManage Enterprise 中的更新设置](#) 页面上的 141
2. 下载并安装更多插件（扩展），例如 Power Manager 插件，以增强一体机的功能。有关安装插件的更多信息，请参阅[插件](#)
i 注：要让插件在安装后完全正常工作，需要具备 OpenManage Enterprise 高级许可证。有关插件的更多详细信息，请参阅 Dell 支持网站上提供的相应文档。
i 注：在 OpenManage Enterprise 上安装插件将重新启动一体机服务。
3. 在安装好插件之后，您可以执行以下操作：
 - 单击**更多操作**下拉菜单可进一步了解插件，以及禁用、卸载、启用插件或更改插件设置。有关详细信息，请参阅[插件](#)、[插件](#)、[插件](#)
 - 当插件有可用新版本时，您可以单击**有可用更新**。

相关信息

从 [Dell.com 更新](#) 页面上的 142

从 [内部网络共享更新](#) 页面上的 143

OpenManage Enterprise 中的更新设置

通过单击控制台和扩展页面上的**更新设置（应用程序设置 > 控制台和扩展）**，可以选择以下更新设置：

1. **如何检查更新** — 从以下方法中进行选择：
 - a. **自动**：设备会在每个星期一从**在何处检查更新**中指定的源自动检查可用的更新。
 - b. **手动**：如果配置为“手动”，则用户必须从**在何处检查更新**中指定的源手动检查可用的更新。
2. **在何处检查更新** — 可以指定设备检查更新的位置。下列选项可用：
 - a. **Dell.com（联机）** — 选择此选项后，设备会直接从 https://downloads.dell.com/openmanage_enterprise 检查可用的更新。
 - b. **网络共享（脱机）** — 指定包含更新包的 NFS、HTTP 或 HTTPS 路径。单击**立即测试**以验证与指定的网络共享的连接。
i 注：对于脱机更新（网络共享），管理员应在下载更新包之前创建适当的文件夹结构，具体取决于是需要最小还是完全升级。有关将 OpenManage Enterprise 更新到最新版本和允许的更新文件夹结构的更多信息，请参阅支持网站上的升级 Dell EMC OpenManage Enterprise 设备版本技术白皮书 (https://downloads.dell.com/manuals/all-products/esuprt_software/esuprt_ent_sys_mgmt/dell-openmanage-enterprise-v321_white-papers10_en-us.pdf)。
3. 选中**下载完成后自动启动控制台更新**复选框，以在下载更新包后立即开始安装控制台更新。否则，可以手动启动更新。
i 注：根据更新设置，设备将检查是否有更新可用，如果有新版本可用，将显示包含新升级版本信息的横幅。在横幅上，管理员可以选择忽略通知、稍后提醒，也可以单击**立即查看**了解详细信息，例如[应用程序设置 > 控制台和扩展](#)页面上提供的可用更新的版本和大小等。OpenManage Enterprise 部分的控制台和扩展页面显示可用更新的所有新功能和增强功能。单击**安装更新**以开始更新。

更新 OpenManage Enterprise

根据更新设置（[应用程序设置 > 控制台和扩展 > 更新设置](#)），您的现有 OpenManage Enterprise 可以直接从 Dell.com 站点，或从网络共享中的已下载更新包中自动或手动更新。

当确定 OpenManage Enterprise 的新的可升级版本时，控制台和扩展页面上会显示更多详细信息，例如更新的版本、大小和新功能，并且有一个活动的**更新**按钮可用。此外，还会显示一条横幅，其中包含新版本的详细信息。所有用户都可以查看横幅，但只有具有管理员权限的用户可以选择稍后提醒或忽略消息选项。

i 注：

- 仅 OpenManage Enterprise 版本 3.4 及更高版本可通过**自动 > 联机**方法更新到版本 3.6.1。

- 必须先将低于 3.4 版本（如 3.3x 版本和 3.2 版本）的 OpenManage Enterprise 版本更新到 3.4 版本，再考虑升级到 3.6.1。
- 不支持直接从 OpenManage Enterprise—Tech Release 更新。TechRelease 版本应首先升级到 OpenManage Enterprise 3.0 或 3.1 版本。
- 在您升级到版本 3.6.x 后，现有设备管理者在默认情况下将拥有其范围内的所有设备。但是，如果需要，管理员可以使用 SBAC 功能编辑设备管理者范围。有关更多信息，请参阅 [OpenManage Enterprise 中基于角色和范围的访问控制](#) 页面上的 14 和 [管理 OpenManage Enterprise 用户](#) 页面上的 124。

更新到最新版本之前，管理员应：

- 将控制台的虚拟机快照作为一个备份，以防出现意外情况。为此分配更多停机时间，如有必要。
- 至少分配一个小时用于更新过程。如果必须使用低速网络连接下载更新，则需要分配更多时间。
- 确保在计划的停机时间内没有设备配置、部署或扩展（插件）任务正在运行或计划运行。在更新过程中，任何活动或计划的任务或策略都会终止，而不会出现进一步的警告。
- 通知待处理的计划更新的其他控制台用户。
- 如果升级失败，设备将重新启动。建议恢复虚拟机快照并再次升级。

对于从 OpenManage Enterprise 版本 3.5 进行升级，升级过程的结果将通过控制台页面上的横幅表明。默认情况下，横幅会在升级后显示 24 小时，但您可以通过单击横标最右边的“消除”来使其消失。当从 OpenManage Enterprise 版本 3.5 升级成功时，横标将显示为绿色，并包含指明一体机新版本号的“升级成功”消息。但是，如果升级失败，一体机将自动恢复到其以前的版本，并且横幅显示为橙色并显示“故障”消息。您可以单击横幅上的“查看详细消息”，以在“作业详细信息”页面上查看“升级”作业的执行历史记录。

i 注：

- 当您更新已发现设备数超过 8,000 个的 OpenManage Enterprise 时，更新任务需要两到三个小时才能完成。在此期间，服务可能会无响应。此后，建议您正常重启设备。重新启动后，设备会恢复正常功能。
- 只有在完成控制台升级后任务之后，才能添加第二个网络接口。在升级后任务进行过程中，尝试添加第二个 NIC 将是无效的。
- 您可在一体机更新后立即登录，无需等待整个资源清册查找完毕后再登录。更新后，查找任务将在后台运行，您可以偶尔查看进度。
- 单击**更新**将启动“升级捆绑包下载”作业。所有更新文件下载完毕且用户无法终止此作业时，此作业会自行结束。

1. 要从 Dell.com 进行联机更新，请参阅 [从 Dell.com 更新](#) 页面上的 142。
2. 要从 NFS 或 HTTPS 网络共享中已下载的更新包进行脱机更新，请参阅 [从内部网络共享更新](#) 页面上的 143。

i 注： 根据需要最小升级还是完全升级，管理员应在下载更新包之前创建适当的文件夹结构。有关允许的文件夹结构和将 OpenManage Enterprise 更新到最新版本的更多信息，请参阅支持网站上的 [升级 Dell EMC OpenManage Enterprise 设备版本技术白皮书](#)。

从 Dell.com 更新

您现有的 OpenManage Enterprise 可以通过 Dell.com (https://downloads.dell.com/openmanage_enterprise) 自动或手动更新。

联机更新前提条件：

- 将在何处**检查更新**更新设置指定为 Dell.com。有关详细信息，请参阅 [OpenManage Enterprise 中的更新设置](#) 页面上的 141。
- 您必须确保 OpenManage Enterprise 设备可以访问 Dell.com 和预期的更新。
- 开始更新之前，请务必备份控制台的虚拟机快照，以防出现意外情况。为此分配更多停机时间，如有必要。

当确定 OpenManage Enterprise 的新的可升级版本时，控制台和扩展页面上会显示更多详细信息，例如更新的版本、大小和新功能，并且有一个活动的**更新**按钮可用。此外，还会显示一条横幅，其中包含新版本的详细信息。所有用户都可以查看横标，但只有具有管理员权限的用户可以选择稍后提醒或忽略消息选项。

1. 单击**更新**，并执行更新。

i 注：

- 单击**更新**将启动“升级捆绑包下载”作业。所有更新文件下载完毕且无法终止此作业时，此作业会自行结束。
- 如果升级失败，设备将重新启动。建议恢复虚拟机快照并再次升级

2. 更新后登录并确认产品的工作情况与预期一致。检查关于更新的所有警告或错误的审计日志。如果出现任何错误，导出审计日志并保存以供技术支持使用。

更新一体机之后：

- 清除浏览器高速缓存。如果不清除浏览器高速缓存，可能导致更新后执行的新任务失败。

- 只有在完成控制台升级后任务之后，才能添加第二个网络接口。在升级后任务进行过程中，尝试添加第二个 NIC 将是无效的。
- 您可在一体机更新后立即登录，无需等待整个资源清单查找完毕后再登录。更新后，查找任务将在后台运行，您可以偶尔查看进度。

相关任务

检查并更新 OpenManage Enterprise 及可用插件的版本 页面上的 141

从内部网络共享更新

当您无法自动连接到 Dell.com 时，您必须设置本地网络共享并手动下载更新软件包。每次在您手动找到更新后，系统都会创建审核日志。

注:

- 对于版本 3.3x 和版本 3.2 等早于 3.4 的 OpenManage Enterprise 版本，在考虑通过共享的网络文件共享 (NFS) 升级到 3.6.x 之前，必须先更新到版本 3.4。
- 不支持直接从 OpenManage Enterprise—Tech Release 更新。TechRelease 版本应首先升级到 OpenManage Enterprise 3.0 或 3.1 版本。
- 对于脱机更新（网络共享），管理员应在下载更新包之前创建适当的文件夹结构，具体取决于是需要最小还是完全升级。有关将 OpenManage Enterprise 更新到最新版本和允许的更新文件夹结构的更多信息，请参阅支持网站上的升级 Dell EMC OpenManage Enterprise 设备版本技术白皮书 (https://downloads.dell.com/manuals/all-products/esuprt_software/esuprt_ent_sys_mgmt/dell-openmanage-enterprise-v321_white-papers10_en-us.pdf)。
- 当更新本地共享以手动升级没有安装任何扩展/插件的版本（如 3.1 和 3.2）时，审核日志会显示警告条目，如“无法检索扩展目录类型的源文件，因为文件不存在”以及“下载扩展目录的状态为失败”。这些错误消息对升级过程没有任何功能影响，可以忽略。

在开始更新之前，请执行以下操作：

- 请务必备份控制台的虚拟机快照，以防出现意外情况。（为此分配更多停机时间，如有必要）。
- 如果升级失败，设备将重新启动。建议恢复虚拟机快照并再次升级。
- 只有在完成控制台升级后任务之后，才能添加第二个网络接口。在升级后任务进行过程中，尝试添加第二个 NIC 将是无效的。
- 使用 HTTPS 更新方法时，您必须确保安全证书由受信任的第三方认证机构签署。

要更新 OpenManage Enterprise，请执行以下操作：

1. 从 <https://downloads.dell.com> 下载适用文件，并保存在可以通过控制台进行访问的保留相同文件夹结构的网络共享上。
2. 选择**手动和脱机**。
3. 输入保存已下载文件的本地路径信息，然后单击**立即检查**。路径示例：`nfs://<IP 地址>/<Folder_Name>`、`http://<IP 地址>/<Folder_Name>`、`https://<IP 地址>/<Folder_Name>`。
将会显示可用的更新版本及新功能的简要说明。
4. 要验证与目录的连接，请单击**立即测试**。如果建立了与目录的连接，将会显示**连接成功**消息。如果未建立与共享地址或目录文件路径的连接，将会显示**连接到路径失败**错误消息。此步骤为可选操作。
5. 单击**更新**，然后执行更新（适用于将来的升级）。

注:

- 单击**更新**将启动“升级捆绑包下载”作业。所有更新文件下载完毕且用户无法终止此作业时，此作业会自行结束
- 如果升级下载无法通过代理连接，请取消选中代理设置，然后下载。

更新后登录并确认产品的工作情况与预期一致。检查关于更新的任何警告或错误的审计日志。如果出现任何错误，导出审计日志并保存以供技术支持使用。

更新一体机之后：

- 清除浏览器高速缓存。如果不清除浏览器高速缓存，可能导致更新后执行的新任务失败。
- 如果从 OpenManage Enterprise 版本 3.1 进行升级，建议您重新配置或导入 Active Directory 组以增强性能。
- 您可在一体机更新后立即登录，无需等待整个资源清单查找完毕后再登录。更新后，查找任务将在后台运行，您可以偶尔查看进度。

相关任务

检查并更新 OpenManage Enterprise 及可用插件的版本 页面上的 141

安装插件

您可以根据要求安装 Power Manager、SupportAssist-Enterprise 和 Update Manager 插件，以增强 OpenManage Enterprise 的功能。

- 要从 Dell.com 安装 OpenManage Enterprise 插件程序，请确保 OpenManage Enterprise 设备可以访问 downloads.dell.com。
- 要从本地网络共享安装 OpenManage Enterprise 插件程序，您必须手动将软件包下载到网络共享，并在 OpenManage Enterprise 的“更新设置”页面上更新该位置。

有关更新设置配置的更多信息，请参阅 [OpenManage Enterprise 中的更新设置](#) 页面上的 141。

注：在 OpenManage Enterprise 上安装插件将重新启动一体机服务。

要安装插件，请执行以下步骤：

1. 在 OpenManage Enterprise 中，单击**应用程序设置 > 控制台和插件**。此时将显示**控制台和插件**页面。
2. 在**插件**部分中，针对要安装的插件单击**安装**。此时会显示**安装插件**向导。
3. 从**可用版本**列表中，选择要安装的版本。
4. 检查并确保您满足**前提条件**部分所述的前提条件列表，然后单击**下载插件**。

注：当您选择要安装的插件版本时，前提条件列表会发生变化。

安装操作会验证安装插件程序的前提条件。如果未满足安装前提条件，将显示相应的错误消息。

成功下载插件后，插件顶部显示的状态将从**可用**更改为**已下载**。

5. 要安装 OpenManage Enterprise 插件，请在**安装插件**向导中单击**安装插件**。
6. 此时将显示一个同意书，通知您最终用户许可协议 (EULA)。单击**接受**以继续安装插件程序。登录到 OpenManage Enterprise 的用户数、正在进行的任务和计划作业的详细信息将显示在**确认**对话框中。
7. 要确认安装，请选择**我同意在执行插件操作之前已捕获了 OpenManage Enterprise 设备的快照**选项，然后单击**确认安装**。此时会显示安装操作的状态。成功安装插件程序后，“插件程序”部分顶部显示的状态将从**可用**或**已下载**更改为**已安装**。

禁用插件

在 OpenManage Enterprise 上禁用所有插件功能。

注：在 OpenManage Enterprise 上禁用插件将重新启动设备服务。

1. 在 OpenManage Enterprise 中，单击**应用程序设置 > 控制台和插件**。此时将显示**控制台和插件程序**选项卡。
2. 在**插件**部分中，针对要禁用的插件单击**禁用**。此时将显示**禁用插件**向导。
3. 要禁用插件，请单击**禁用插件**。登录到 OpenManage Enterprise 的用户数、正在进行的任务和计划作业的详细信息将显示在**确认**对话框中。
4. 要确认，请选择**我同意在执行插件操作之前已捕获了 OpenManage Enterprise 设备的快照**选项，然后单击**确认禁用**。

注：禁用插件后，您将无法看到与 OpenManage Enterprise 上的插件相关的任何信息或页面。

卸载插件

卸载并删除插件收集的所有数据。

1. 在 OpenManage Enterprise 中，单击**应用程序设置 > 控制台和插件**。此时将显示**控制台和插件程序**选项卡。
2. 在**插件**部分，针对要卸载的插件单击**卸载**。此时将显示**卸载插件**向导。
3. 要从 OpenManage Enterprise 卸载插件，请单击**卸载插件**。登录到 OpenManage Enterprise 的用户数、正在进行的任务和计划作业的详细信息将显示在**确认**对话框中。
4. 要确认卸载，请选择**我同意在执行插件操作之前已捕获了 OpenManage Enterprise 设备的快照**选项，然后单击**确认卸载**。与插件关联的所有功能和数据都将被卸载。

启用插件

所有插件页面都将显示在 OpenManage Enterprise 上且已在 OpenManage Enterprise 上启用插件功能。

注: 在 OpenManage Enterprise 上启用插件将重新启动设备服务。

1. 在 OpenManage Enterprise 中，单击**应用程序设置 > 控制台和插件**。
此时将显示**控制台和插件程序**选项卡。
2. 在**插件**部分中，针对要启用的插件单击**启用**。
此时将显示**启用插件**向导。
3. 要启用插件，请单击**启用插件**。
登录到 OpenManage Enterprise 的用户数、正在进行的任务和计划作业的详细信息将显示在**确认**对话框中。
4. 要确认，请选择**我同意在执行插件操作之前已捕获了 OpenManage Enterprise 设备的快照**。选项，然后单击**确认启用**。

更新插件程序

根据更新设置，设备会检查已安装插件程序的更新是否可用。如果有可用的新版本，将显示包含新升级版本信息的横幅。在横幅上，管理员可以选择忽略通知、稍后提醒，也可以单击**立即查看**了解详细信息，例如**应用程序设置 > 控制台和插件程序**页面上提供的可用更新的版本和大小等。“控制台和插件程序”页面的“插件程序”部分显示可用插件程序更新的所有新功能和增强功能。

在您更新插件程序之前，请确保按 **OpenManage Enterprise 中的更新设置** 页面上的 141 中所述方式配置更新设置。

要更新插件程序，请执行以下操作：

1. 在“插件程序”部分中，针对要更新的插件程序单击**有可用更新**。
此时将显示**更新插件程序**页面。
2. 选择插件程序版本，然后单击**下载插件程序**。
此时插件程序已下载，并且下载状态显示为绿色色带。
3. 要更新插件程序，请单击**更新插件程序**。
在**确认**窗口中，选择**我同意在执行插件程序操作之前已捕获了 OpenManage Enterprise 设备的快照**选项，然后单击**更新**。

更新操作完成后，该版本将显示在“插件程序”部分中。

执行远程命令和脚本

当您获得 SNMP 陷阱时，您可以在 OpenManage Enterprise 上运行脚本。这会设置一个策略，其会在用于警报管理的第三方票证系统打开一个票证。您最多可以创建和存储**四个**远程命令。

注: 不支持将以下特殊字符用作 RACADM 和 IPMI CLI 参数：[、;、|、\$、>、<、&、'、]、.、* 和 '。

1. 单击 **应用程序设置 > 脚本执行**。
2. 在**远程命令设置**部分中，执行以下操作：
 - a. 要添加远程命令，请单击**创建**。
 - b. 在**命令名称**框中，输入命令名称。
 - c. 选择以下任何一种命令类型：
 - i. 脚本
 - ii. RACADM
 - iii. IPMI 工具
 - d. 如果您选择**脚本**，请执行以下操作：
 - i. 在**IP 地址**框中，输入 IP 地址。
 - ii. 选择身份验证方法：**密码**或**SSH 密钥**。
 - iii. 输入**SSH 密钥的用户名和密码**。
 - iv. 在**命令**框中，键入命令。
 - 最多可以键入 100 个命令，每个命令必须位于单独的行中。
 - 可以在脚本中实现标记替换。请参阅 **远程脚本和警报策略中的标记替换** 页面上的 152
 - v. 单击**完成**。
 - e. 如果您选择**RACADM**，请执行以下操作：
 - i. 在**命令名称**框中，输入命令名称。
 - ii. 在**命令**框中，键入命令。最多可以键入 100 个命令，每个命令必须位于单独的行中。

- iii. 单击**完成**。
- f. 如果您选择 **IPMI 工具**，请执行以下操作：
 - i. 在**命令名称**框中，输入命令名称。
 - ii. 在**命令**框中，键入命令。最多可以键入 100 个命令，每个命令必须位于单独的行中。
 - iii. 单击**完成**。
3. 要编辑远程命令设置，请选择命令，然后单击**编辑**。
4. 要删除远程命令设置，请选择该命令，然后单击**删除**。

OpenManage Mobile 设置

OpenManage Mobile (OMM) 是一款系统管理应用程序，可用于通过 Android 设备或 iOS 设备在一个或多个 OpenManage Enterprise 控制台和/或集成 Dell Remote Access Controller (iDRAC) 上安全地执行部分数据中心监测和修复任务。使用 OMM 您可以：

- 接收来自 OpenManage Enterprise 的警报通知。
- 查看组、设备、警报和日志信息。
- 开机、关机或重新启动服务器。

默认情况下，已针对所有警报和严重警报启用推送通知。本章提供了关于可通过使用 OpenManage Enterprise 配置的 OMM 设置的信息。此外还提供进行 OMM 故障排除所需的信息。

 **注：**有关安装和使用 OMM 的信息，请参阅位于 Dell.com/OpenManageManuals 的 *OpenManage Mobile 用户指南*。

相关任务


- [启用或禁用 OpenManage Mobile 的警报通知](#) 页面上的 146
- [启用或禁用 OpenManage Mobile 订户](#) 页面上的 147
- [删除 OpenManage Mobile 订户](#) 页面上的 147
- [查看警报通知服务状态](#) 页面上的 147
- [OpenManage Mobile 故障排除](#) 页面上的 149


相关信息

- [启用或禁用 OpenManage Mobile 的警报通知](#) 页面上的 146
- [启用或禁用 OpenManage Mobile 订户](#) 页面上的 147
- [OpenManage Mobile 故障排除](#) 页面上的 149

启用或禁用 OpenManage Mobile 的警报通知

默认情况下，OpenManage Enterprise 配置为向 OpenManage Mobile 应用程序发送警报通知。但是，仅在 OpenManage Mobile 用户向 OpenManage Mobile 应用程序添加 OpenManage Enterprise 时从 OpenManage Enterprise 发送警报通知。

 **注：**启用或禁用 OpenManage Mobile 的警报通知需要具有管理员权限。

 **注：**要让 OpenManage Enterprise 向 OpenManage Mobile 发送警报通知，请确保 OpenManage Enterprise 服务器具有出站 (HTTPS) 互联网接入。

要启用或禁用从 OpenManage Enterprise 发向 OpenManage Mobile 的警报通知，请执行以下操作：

1. 单击 **OpenManage Enterprise > 应用程序设置 > 移动**。
2. 选择**启用推送通知**复选框。
3. 单击**应用**。

相关任务

- [OpenManage Mobile 设置](#) 页面上的 146

相关信息

- [OpenManage Mobile 设置](#) 页面上的 146
- [删除 OpenManage Mobile 订户](#) 页面上的 147

启用或禁用 OpenManage Mobile 订户

使用**移动订户**列表中的**启用**列中的复选框可以启用或禁用向 OpenManage Mobile 订户传送警报通知。

注:

- 启用或禁用 OpenManage Mobile 订户需要具有管理员权限。
- 如果其移动服务提供商推送通知服务表示设备永远不可达，则 OpenManage Enterprise 会自动禁用 OpenManage Mobile 订户。
- 即使在**移动订户**列表中启用了 OpenManage Mobile 订户，他们也可以在其 OpenManage Mobile 应用程序设置中禁用接收警报通知。

要启用或禁用发向 OpenManage Mobile 订户的警报通知，请执行以下操作：

1. 单击 **OpenManage Enterprise > 应用程序设置 > 移动**。
2. 要启用，请选择相应的复选框并单击**启用**。要禁用，请选择复选框并单击**禁用**。
您可以一次选择多个订户。

相关任务

[OpenManage Mobile 设置](#) 页面上的 146

相关信息

[OpenManage Mobile 设置](#) 页面上的 146

[删除 OpenManage Mobile 订户](#) 页面上的 147

删除 OpenManage Mobile 订户

删除 OpenManage Mobile 订户会从移动订户列表中移除该用户，使其无法接收来自 OpenManage Enterprise 的警报通知。但是，OpenManage Mobile 用户以后可从 OpenManage Mobile 应用程序重新订阅警报通知。

注: 删除 OpenManage Mobile 订户需要具有管理员权限。

要删除 OpenManage Mobile 订户，请执行以下操作：

1. 单击 **OpenManage Enterprise 应用程序设置移动**。
2. 选中与订户名称对应的复选框，然后单击**删除**。
3. 显示提示时，单击**是**。

相关任务

[启用或禁用 OpenManage Mobile 的警报通知](#) 页面上的 146

[启用或禁用 OpenManage Mobile 订户](#) 页面上的 147

[删除 OpenManage Mobile 订户](#) 页面上的 147

[查看警报通知服务状态](#) 页面上的 147

相关信息

[OpenManage Mobile 设置](#) 页面上的 146

[删除 OpenManage Mobile 订户](#) 页面上的 147

查看警报通知服务状态

OpenManage Enterprise 通过订户各自的设备平台警报通知服务将警报通知转发至 OpenManage Mobile 订户。如果 OpenManage Mobile 订户未能收到警报通知，可以检查**通知服务状态**以排除警报通知传送故障。

要查看警报通知服务的状态，请单击**应用程序设置移动**。

相关任务

[查看警报通知服务状态](#) 页面上的 147




相关信息

[OpenManage Mobile 设置](#) 页面上的 146
[删除 OpenManage Mobile 订户](#) 页面上的 147
[查看警报通知服务状态](#) 页面上的 147

通知服务状态

下表提供关于[应用程序设置 > 移动](#) 页面中显示的**通知服务状态** 的信息。

表. 29: 通知服务状态

状态图标	状态说明
	该服务正在运行并且工作正常。 注: 此服务状态仅反映与平台通知服务成功通信。如果订户的设备未连接到 Internet 或蜂窝数据服务, 则在连接恢复之前不会发送通知。
	服务在传送消息时遇到错误, 这可能是暂时状况。如果问题一直存在, 请执行故障排除步骤或联系技术支持。
	服务在传送消息时遇到错误。请执行故障排除步骤或根据需要联系技术支持。

查看有关 OpenManage Mobile 订户的信息

在 OpenManage Mobile 用户成功添加 OpenManage Enterprise 后, 该用户即被添加到 OpenManage Enterprise 的**移动订户**表中。要查看有关移动订户的信息, 请在 OpenManage Enterprise 中单击[应用程序设置 > 移动](#)。

您也可以通过使用[导出](#)下拉列表将移动订户的相关信息导出为 .csv 文件。

OpenManage Mobile 订户信息

下表提供了关于[应用程序设置 > 移动](#) 页面中显示的**移动订户** 表的信息。

表. 30: OpenManage Mobile 订户信息

字段	说明
已启用	选择或清除复选框, 然后分别单击 启用 或 禁用 以启用或禁用发向 OpenManage 移动订户的警报通知。
状况	显示订户的状态, 指示 OpenManage Enterprise 能否将警报通知成功发送到警报转发服务。
状态消息	状态消息的状态说明。
用户名	OpenManage Mobile 用户的名称。
设备 ID	移动设备的唯一标识符。
说明	移动设备的说明。
筛选器	筛选器是订户为警报通知配置的策略。
上次出错	向 OpenManage Mobile 用户发送警报通知时上次发生错误的日期和时间。
上次推送	上次成功地从 OpenManage Enterprise 向警报转发服务发送警报通知的日期和时间。
上次连接	用户上次通过 OpenManage Mobile 访问 OpenManage Enterprise 的日期和时间。

表. 30: OpenManage Mobile 订户信息 (续)

字段	说明
注册	用户在 OpenManage Mobile 中添加 OpenManage Enterprise 的日期和时间。

OpenManage Mobile 故障排除

如果 OpenManage Enterprise 无法注册邮件转发服务或无法成功转发通知，可使用以下解决方案：

表. 31: OpenManage Mobile 故障排除

问题	原因	解决方案
OpenManage Enterprise 无法连接到 Dell 邮件转发服务。[代码 1001/1002]	出站互联网 (HTTPS) 连接中断。	使用 Web 浏览器检查出站互联网连接是否可用。 如果连接不可用，请完成以下网络故障排除任务： <ul style="list-style-type: none"> • 验证是否已连接网络电缆。 • 验证 IP 地址和 DNS 服务器设置。 • 验证防火墙是否配置为允许出站流量。 • 验证 ISP 网络是否运行正常。
	代理设置不正确。	根据要求设置代理主机、端口、用户名和密码。
	“邮件转发服务”暂时不可用。	等待该服务恢复可用。
“邮件转发服务”无法连接到设备平台通知服务。[代码 100-105、200-202、211-212]	平台提供商服务暂时对“邮件转发服务”不可用。	等待该服务恢复可用。
设备通信令牌已从平台提供商服务注销。[代码 203]	OpenManage Mobile 应用程序已更新、还原、卸载，或者设备操作系统已升级或还原。	在设备上重新安装 OpenManage Mobile，或者遵循在 <i>OpenManage Mobile 用户指南</i> 中指定的 OpenManage Mobile 故障排除步骤，然后将设备重新连接到 OpenManage Enterprise。 如果设备不再连接到 OpenManage Enterprise，则移除订户。
OpenManage Enterprise 注册被邮件转发服务拒绝。[代码 154]	正在使用过时的 OpenManage Enterprise 版本。	升级到较新版本的 OpenManage Enterprise。

相关任务

[OpenManage Mobile 设置](#) 页面上的 146

相关信息

[OpenManage Mobile 设置](#) 页面上的 146

其他参考和字段说明

本节列出和定义了关于一些在 OpenManage Enterprise 图形用户界面 (GUI) 上常见字段的定义。此外，还描述了其他有用信息以供进一步参考。

主题:

- [计划参考](#)
- [固件基线字段定义](#)
- [计划作业字段定义](#)
- [EEMI 位置调整后的警报类别](#)
- [远程脚本和警报策略中的标记替换](#)
- [现场服务调试工作流程](#)
- [取消阻止 FSD 功能](#)
- [安装或授予已签署 FSD DAT.ini 文件](#)
- [调用 FSD](#)
- [禁用 FSD](#)
- [目录管理字段定义](#)
- [固件/驱动程序合规性基线报告 - 具有“未知”合规状态的设备](#)
- [Dell EMC PowerEdge 服务器的通用命名惯例](#)

计划参考

- **立即更新:** 固件版本已更新并与相关目录上可用的版本相匹配。要使更新在下次设备重新启动期间生效，请选择**下一个服务器重新引导阶段**复选框。
- **以后计划:** 选择以指定一个固件版本必须更新的日期和时间。

固件基线字段定义

- **合规性:** 固件基线的运行状况状态。即使与固件基线关联的设备处于严重运行状况，基线运行状况也会声明为“严重”。这称为汇总运行状况状态，等于具有高严重性的基线的状态。有关“汇总运行状况”状态的更多信息，请参阅 Dell 技术中心上提供的在 *Dell EMC 第 14 代及更高代别的 POWEREDGE 服务器上使用 iDRAC 管理汇总运行状况状态白皮书*。
- **名称:** 固件基线名称。单击此选项可查看**合规性报告**页中的基线合规性报告。有关创建固件基线的更多信息，请参阅[创建固件/驱动程序基线](#) 页面上的 67。
- **目录:** 固件基线所属的固件目录。请参阅[管理固件和驱动程序目录](#) 页面上的 65。
- **上次运行时间:** 基线合规性报告中上次运行的时间。请参阅[检查设备固件和驱动程序的合规性](#) 页面上的 68。

计划作业字段定义

- **立即运行**以立即开始作业。
- **以后运行**以指定一个未来的日期和时间。
- **按计划运行**以根据所选频率重复运行。选择**每天**，然后选择相应的频率。

注: 默认情况下，每天上午 12:00 重设作业调度器时钟。cron 格式计算作业频率时不考虑作业创建时间。例如，如果作业在上午 10:00 点开始，此后每隔 10 小时运行，作业下一次运行是晚上 08:00。但是，随后的时间不是第二天的早上 06:00，而是上午 12:00。这是因为每天上午 12:00 重设调度器时钟。

EEMI 位置调整后的警报类别

EEMI 位置调整表

表. 32: OpenManage Enterprise 中的警报类别

以前的类别	以前的子类别	新类别	新子类别
审核	设备	系统运行状况	设备
审核	设备	配置	设备
审核	设备	配置	设备
审核	设备	配置	设备
审核	设备	配置	设备
审核	应用程序	配置	应用程序
审核	应用程序	配置	应用程序
审核	应用程序	配置	应用程序
审核	应用程序	配置	应用程序
审核	设备	审核	用户
审核	模板	配置	模板
审核	模板	配置	模板
审核	模板	配置	模板
审核	模板	配置	模板
审核	模板	配置	模板
配置	资源清册	配置	作业
配置	资源清册	配置	作业
配置	资源清册	配置	作业
配置	资源清册	配置	设备
配置	资源清册	配置	设备
配置	资源清册	配置	设备
配置	固件	配置	作业
配置	固件	配置	作业
其他	作业	配置	作业
其他	作业	配置	作业
其他	作业	配置	作业
其他	通用	配置	通用
其他	通用	配置	通用
其他	通用	配置	通用
其他	通用	配置	通用
其他	通用	配置	通用
其他	通用	配置	通用
其他	通用	配置	通用

表. 32: OpenManage Enterprise 中的警报类别 (续)

以前的类别	以前的子类别	新类别	新子类别
其他	通用	配置	通用
其他	设备	配置	设备
其他	设备	配置	设备
审核	安全性	配置	安全性
审核	安全性	配置	安全性
审核	安全性	配置	安全性

远程脚本和警报策略中的标记替换

OpenManage Enterprise 支持使用标记来增强远程脚本执行和警报策略创建。

表. 33: OpenManage Enterprise 中支持的标记

标记	说明
\$IP	设备 IP 地址
\$MSG	消息
\$DATE	日期
\$TIME	时间
\$SEVERITY	严重性
\$SERVICETAG	服务标签
\$RESOLUTION	建议的解决方案
\$CATEGORY	警报类别名称
\$ASSETTAG	资产标签
\$MODEL	型号名称

现场服务调试工作流程

在 OpenManage Enterprise, 您可以通过使用现场服务调试 (FSD) 选项来授权控制台调试。

通过使用 FSD, 您可以执行以下任务:

- 允许启用和复制调试日志
- 允许复制实时日志
- 允许备份或还原数据库到虚拟机。

每个任务中引用的主题会提供详细说明。要启用 FSD, 请执行以下任务:

1. 取消阻止 FSD 功能。请参阅[取消阻止 FSD 功能](#) 页面上的 152。
2. 安装或授予签署 FSD DAT.ini 文件。请参阅[安装或授予已签署 FSD DAT.ini 文件](#) 页面上的 153。
3. 调用 FSD。请参阅[调用 FSD](#) 页面上的 153。
4. 禁用 FSD。请参阅[禁用 FSD](#) 页面上的 153。

取消阻止 FSD 功能

您可以通过 TUI 屏幕取消阻止 FSD 功能。

1. 导航至 TUI 主菜单。
2. 在 TUI 屏幕上, 要使用 FSD 选项, 请选择[启用现场服务调试 \(FSD\) 模式](#)。

3. 要生成新的 FSD 取消阻止请求，在 **FSD 功能** 屏幕上选择 **取消阻止 FSD 功能**
4. 要确定所请求的调试功能的持续时间，请选择开始日期和结束日期。
5. 在 **选择请求的调试功能** 屏幕上，请从调试功能列表中选择唯一的调试功能与控制台对应。在右下角选择 **生成**。

注： 当前受支持的调试功能是 RootShell。

6. 在 **下载 DAT 文件** 屏幕上查看签字说明和 DAT.ini 文件所在的共享 URL 地址。
7. 使用外部客户端从步骤 6 中所述的共享 URL 地址中提取 DAT.ini 文件。

注： 下载共享目录具有只读权限，且一次只支持一个 DAT.ini 文件。

8. 执行以下任务，具体取决于您是否为外部用户或内部 Dell EMC 用户：
 - 如果您是外部用户，请将 DAT.ini 文件发送至 Dell EMC 联系人以供签字。
 - 将 DAT.ini 文件上传到相应的 Dell 现场服务调试验证中心 (FSDAF) 并提交。
9. 等待 Dell EMC 签字并许可 DAT.ini 文件返回。

安装或授予已签署 FSD DAT.ini 文件

确保您已收到由 Dell EMC 签字并批准的 DAT.ini 文件。

注： Dell EMC 批准 DAT.ini 文件后，您必须将文件上传到生成原始取消阻止命令的控制台设备上。

1. 要上传签署的 DAT.ini 文件，在 **FSD 功能** 屏幕中，请选择 **安装/授予签署 FSD DAT 文件**。

注： 上传共享目录具有只写权限，且一次只支持一个 DAT.ini 文件。DAT.ini 文件大小限制为 4 KB。

2. 在 **上传签署 DAT 文件** 屏幕上，请按照有关上传 DAT.ini 文件至给定的文件共享 URL 中的说明进行操作。
3. 使用外部客户端将 DAT.ini 文件上传到共享位置。
4. 在 **上传签署 DAT 文件** 屏幕上，请选择 **我已上传 FSD DAT 文件**。

如果在 DAT.ini 文件上传过程中没有出现错误，将会显示一条消息，确认证书安装成功。要继续，请单击 **确定**。

DAT.ini 文件上传可能会因以下任何一种原因失败：

- 上传共享目录没有足够的磁盘空间。
- 上传的 DAT.ini 文件未对应上一个调试功能请求。
- 由 Dell EMC 提供的 DAT.ini 文件的签名无效。

调用 FSD

确保 Dell EMC 签字并返回 DAT.ini 文件，然后上传至 OpenManage Enterprise。

1. 要调用调试功能，在 **FSD 功能** 屏幕上选择 **调用 FSD 功能**。
2. 在 **调用请求的调试功能** 屏幕上，请从 Dell EMC 签字的 DAT.ini 文件许可的调试功能列表中选择调试功能。在右下角单击 **调用**。

注： 当前受支持的调试功能是 RootShell。

运行 `invoke` 命令时，OpenManage Enterprise 可以启动 SSH 守护程序。外部 SSH 客户端可以与 OpenManage Enterprise 连接用于调试目的。

禁用 FSD

调用控制台上的调试功能后，它将继续运行，直至控制台重新启动，或调试功能停止。否则，由起始日期和结束日期确定的持续时间将超出范围。

1. 要停止调试功能，在 **FSD 功能** 屏幕上选择 **禁用调试功能**。
2. 在 **禁用调用调试功能** 屏幕上，选择调试功能或从当前已调用的调试功能列表中选择功能。在屏幕右下角选择 **禁用**。

确保您停止当前正在使用调试功能的任何 SSH 守护程序或 SSH 会话。

目录管理字段定义

目录名称：目录的名称。内置目录不可编辑。

下载：表示存储库文件夹中的目录的下载状态。状态有：已完成、正在运行和出现故障。

存储库：存储库类型，例如 Dell.com、CIFS 和 NFS。

存储库位置：保存目录的位置。例如 Dell.com、CIFS 和 NFS。还表示目录上运行的作业的完成状态。

目录文件：键入目录文件。

创建日期：创建目录文件的日期。

固件/驱动程序合规性基线报告 - 具有“未知”合规状态的设备

固件/驱动程序基线合规性报告中的以下存储、网络和超融合基础架构 (HCI) 设备的固件或驱动程序合规性状态显示为未知，因为戴尔固件/驱动程序目录不支持这些设备的固件或软件更新。

表. 34: 固件/驱动程序合规性基线报告 — “错误” 合规设备

设备类别	设备列表
存储	<ul style="list-style-type: none">• SC 系列• MD 系列• ME 系列
FX2、VRTX 和 M1000e 机箱中的网络设备	<ul style="list-style-type: none">• F10 交换机• IOA (输入/输出聚合器)• IOM (输入/输出模块)
超融合一体机 (HCI)	<ul style="list-style-type: none">• VXRail• XC 系列
可使用单个设备的 Dell Update Package (DUP) 对设备进行更新，但在戴尔目录上不直接支持	<ul style="list-style-type: none">• MX9116n 结构引擎• MX5108n 以太网交换机• PowerEdge MX5000s
无法使用戴尔目录或单个 DUP 进行更新的设备 注： 有关这些设备的固件/驱动程序更新，请参阅相应设备的“安装指南”。	<ul style="list-style-type: none">• MX7116n 结构扩展器模块• PowerEdge MX 25GbE PTM

注：有关 SC、MD、ME 和 XC 系列中的设备的完整列表，请参阅 https://topics-cdn.dell.com/pdf/dell-openmanage-enterprise_compatibility-matrix2_en-us.pdf

Dell EMC PowerEdge 服务器的通用命名惯例

为涵盖一系列服务器型号，现在使用通用命名惯例（而不是其代系）来指称 PowerEdge 服务器。

本主题介绍如何识别使用通用命名惯例指称的 PowerEdge 服务器的代系。

示例：

R740 服务器型号是一个拥有两个处理器的机架系统，它源于使用 Intel 处理器的第 14 代服务器。在本文档中，为指称 R740，使用了通用命名惯例 **YX4X** 服务器，其中：

- 字母 **Y** (字母) 用于表示以下服务器外形规格：
 - **C** = 云 — 适用于超规模环境的模块化服务器节点
 - **F** = 灵活 — 适用于基于机架的 FX2/FX2s 机柜的基于机架的混合底座
 - **M** 或 **MX *** = 模块化 — 适用于模块化机柜 MX7000、M1000e 和/或 VRTX 的刀片服务器
 - **R** = 机架式服务器

- T = 塔式服务器
- 字母 X (数字) 表示服务器的类 (处理器数量)。
- 数字 4 表示服务器的代系。
- 字母 X (数字) 表示处理器的构造。

表. 35: PowerEdge 服务器命名惯例和示例

YX3X 服务器	YX4X 系统
PowerEdge M630	PowerEdge M640
PowerEdge M830	PowerEdge R440
PowerEdge T130	PowerEdge R540