




适用于 Dell PowerEdge VRTX 的 Chassis
Management Controller 版本 1.25
用户指南



注、小心和警告

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

版权所有 © 2014 Dell Inc. 保留所有权利。本产品受美国、国际版权和知识产权法律保护。Dell™ 和 Dell 徽标是 Dell Inc. 在美国和 / 或其他管辖区域的商标。所有此处提及的其他商标和产品名称可能是其各自所属公司的商标。

2014 - 02

Rev. A00

目录

1 概览	13
本发行版中的新增功能	13
主要功能	14
管理功能	14
安全功能	15
机箱概览	15
支持的远程访问连接	18
支持的平台	18
支持的管理站操作系统和 Web 浏览器	19
管理许可证	19
许可证类型	19
获取许可证	19
许可证操作	19
许可证组件的状态或条件以及可用操作	20
使用 CMC Web 界面管理许可证	20
使用 RACADM 管理许可证	20
CMC 中的可授权功能	20
查看 CMC Web 界面的本地化版本	22
支持的管理控制台应用程序	22
如何使用本用户指南	22
您可能需要的其他说明文件	22
从 Dell 支持站点访问说明文件	23
2 安装和设置 CMC	25
开始之前	25
安装 CMC 硬件	25
设置机箱一览表	25
基本 CMC 网络连接	26
在管理站上安装远程访问软件	26
在 Linux 管理站上安装 RACADM	26
从 Linux 管理站卸载 RACADM	26
配置 Web 浏览器	26
代理服务器	27
Microsoft Phishing Filter	27
证书吊销列表 (CRL) 访存	28
使用 Internet Explorer 从 CMC 下载文件	28
允许在 Internet Explorer 中播放动画	28
设置对 CMC 的初始访问	28

配置初始 CMC 网络.....	29
访问 CMC 的界面和协议.....	31
使用其他系统管理工具启动 CMC.....	32
下载和更新 CMC 固件.....	32
设置机箱物理位置和机箱名称.....	32
使用 Web 界面设置机箱物理位置和机箱名称.....	33
使用 RACADM 设置机箱物理位置和机箱名称.....	33
设置 CMC 的日期和时间.....	33
使用 CMC Web 界面设置 CMC 的日期和时间.....	33
使用 RACADM 设置 CMC 的日期和时间.....	33
配置 LED 以识别机箱上的组件.....	33
使用 CMC Web 界面配置 LED 闪烁.....	33
使用 RACADM 配置 LED 闪烁.....	34
配置 CMC 属性.....	34
使用 CMC Web 界面配置 iDRAC 启动方法.....	34
使用 RACADM 配置 iDRAC 启动方法.....	35
使用 CMC Web 界面配置登录锁定策略属性	35
使用 RACADM 配置登录锁定策略属性.....	35
了解冗余 CMC 环境.....	36
关于待机 CMC.....	36
CMC 故障保护模式.....	36
活动 CMC 自举过程.....	37
获得冗余 CMC 的运行状况.....	37
配置前面板.....	37
配置电源按钮.....	37
配置 LCD.....	37
使用 KVM 访问服务器.....	38

3 登录 CMC..... 39

访问 CMC Web 界面.....	39
以本地用户、Active Directory 用户或 LDAP 用户身份登录 CMC.....	39
使用智能卡登录 CMC.....	40
使用单点登录来登录 CMC.....	41
使用串行、Telnet 或 SSH 控制台登录 CMC.....	41
使用 RACADM 访问 CMC.....	41
使用公共密钥验证登录 CMC.....	42
多个 CMC 会话.....	42
更改默认登录密码.....	42
使用 Web 界面更改默认登录密码.....	43
使用 RACADM 更改默认登录密码.....	43
启用或禁用默认密码警告消息	43
使用 Web 界面启用或禁用默认密码警告消息.....	43

使用 RACADM 启用或禁用警告消息以更改默认登录密码.....	43
更新输入/输出模块基础结构设备固件.....	44
使用 CMC Web 界面更新输入/输出模块基础结构设备固件.....	44
使用 RACADM 更新输入/输出模块基础结构设备固件.....	44
4 更新固件.....	45
下载 CMC 固件.....	45
查看当前安装的固件版本.....	45
使用 CMC Web 界面查看当前安装的固件版本.....	45
使用 RACADM 查看当前安装的固件版本.....	45
更新 CMC 固件.....	46
使用 RACADM 更新 CMC 固件.....	46
使用 Web 界面更新 CMC 固件.....	46
更新机箱基础结构固件.....	47
使用 CMC Web 界面更新机箱基础结构固件.....	47
使用 RACADM 更新机箱基础结构固件.....	47
更新服务器 iDRAC 固件.....	47
使用 Web 界面更新服务器 iDRAC 固件.....	48
使用 RACADM 更新服务器 iDRAC 固件.....	48
更新服务器组件固件.....	48
启用 Lifecycle Controller.....	49
筛选进行固件更新的组件.....	49
查看固件资源清册.....	51
使用 CMC Web 界面查看固件资源清册.....	52
使用 RACADM 查看固件资源清册.....	53
Lifecycle Controller 作业操作.....	53
重新安装服务器组件固件.....	53
回滚服务器组件固件.....	54
使用 CMC Web 界面回滚服务器组件固件.....	54
升级服务器组件固件.....	54
使用 CMC Web 界面升级服务器组件固件.....	55
删除计划的服务器组件固件作业.....	55
使用 Web 界面删除计划的服务器组件固件作业.....	55
使用 CMC Web 界面更新存储组件.....	55
使用 CMC 恢复 iDRAC 固件.....	56
5 查看机箱信息和监测机箱与组件运行状况.....	57
查看机箱和组件摘要.....	57
机箱图形.....	57
所选组件信息.....	58
查看服务器型号名称和服务标签.....	58
查看机箱摘要.....	59

查看机箱控制器信息和状态.....	59
查看所有服务器的信息和运行状况.....	59
查看单个服务器的运行状况和信息.....	59
查看 IOM 的信息和运行状况.....	59
查看单个输入/输出模块的信息和运行状况.....	60
查看风扇的信息和运行状况.....	60
配置风扇.....	61
查看前面板属性.....	62
查看 KVM 信息和运行状况.....	62
查看 LCD 信息和运行状况.....	62
查看温度传感器的信息和运行状况.....	62

6 配置 CMC..... 63

查看和修改 CMC 网络 LAN 设置.....	63
使用 CMC Web 界面查看和修改 CMC 网络 LAN 设置.....	64
使用 RACADM 查看和修改 CMC 网络 LAN 设置.....	64
启用 CMC 网络接口.....	64
为 CMC 网络接口地址启用或禁用 DHCP.....	65
对 DNS IP 地址启用或禁用 DHCP.....	65
设置静态 DNS IP 地址.....	65
配置 DNS 设置（IPv4 和 IPv6）.....	65
配置自动协商、双工模式和网络速度（IPv4 和 IPv6）.....	66
设置最大传输单元 (MTU)（IPv4 和 IPv6）.....	66
配置 CMC 网络和登录安全设置.....	66
使用 CMC Web 界面配置 IP 范围属性.....	66
使用 RACADM 配置 IP 范围属性.....	67
为 CMC 配置虚拟 LAN 标签属性.....	67
使用 RACADM 为 CMC 配置 VLAN 标签属性.....	67
使用 Web 界面为 CMC 配置虚拟 LAN 标签属性.....	68
配置服务.....	68
使用 CMC Web 界面配置服务.....	69
使用 RACADM 配置服务.....	69
配置 CMC 扩展存储卡.....	69
设置机箱组.....	70
将成员添加到机箱组.....	70
从主机箱中移除成员.....	71
解散机箱组.....	71
在成员机箱中禁用单个成员.....	71
启动成员机箱或服务器的 Web 页面.....	71
传播主机箱属性至成员机箱.....	72
MCM 组的刀片资源清册.....	72
保存服务器资源清册报告.....	72

机箱组资源清册和固件版本.....	73
查看机箱组资源清册	74
使用 Web 界面查看所选机箱的资源清册.....	74
使用 Web 界面查看所选服务器组件的固件版本.....	74
使用 RACADM 配置多个 CMC.....	74
创建 CMC 配置文件.....	75
分析规则.....	76
修改 CMC IP 地址.....	77
查看和结束 CMC 会话.....	77
使用 Web 界面查看和结束 CMC 会话.....	77
使用 RACADM 查看和结束 CMC 会话.....	78

7 配置服务器..... 79

配置插槽名称.....	79
配置 iDRAC 网络设置.....	80
配置 iDRAC 快速部署网络设置.....	80
修改单个服务器 iDRAC 的 iDRAC 网络设置.....	82
使用 RACADM 修改 iDRAC 网络设置.....	82
配置 iDRAC VLAN 标签设置.....	83
使用 RACADM 配置 iDRAC VLAN 标签设置.....	83
使用 Web 界面配置 iDRAC VLAN 标签设置.....	83
设置第一引导设备.....	84
使用 CMC Web 界面为多个服务器设置第一引导设备.....	84
使用 CMC Web 界面为单个服务器设置第一引导设备.....	84
使用 RACADM 设置第一引导设备.....	85
配置服务器 FlexAddress.....	85
配置远程文件共享.....	85
使用服务器配置复制功能配置配置文件设置.....	86
访问服务器配置文件页面.....	86
添加或保存配置文件.....	86
应用配置文件.....	87
导入配置文件.....	87
导出配置文件.....	87
编辑配置文件.....	88
查看配置文件设置.....	88
查看存储的配置文件设置.....	88
查看配置文件日志.....	88
完成状态和故障排除.....	88
配置文件的 Quick Deploy	89
将服务器配置文件分配给插槽	89
使用单点登录启动 iDRAC.....	89
启动远程控制台.....	90

8 配置 CMC 以发送警报.....	91
启用或禁用警报.....	91
使用 CMC Web 界面启用或禁用警报.....	91
使用 RACADM 启用或禁用警报.....	91
筛选警报.....	91
配置警报目标.....	92
配置 SNMP 陷阱警报目标.....	92
配置电子邮件警报设置.....	94
9 配置用户帐户和权限.....	97
用户的类型.....	97
修改根用户管理员帐户设置.....	100
配置本地用户.....	100
使用 CMC Web 界面配置本地用户.....	100
使用 RACADM 配置本地用户.....	101
配置 Active Directory 用户.....	102
支持的 Active Directory 验证机制.....	102
标准架构 Active Directory 概览.....	103
配置标准架构 Active Directory.....	103
扩展架构 Active Directory 概览.....	106
配置扩展架构 Active Directory.....	107
配置通用 LDAP 用户.....	114
配置通用 LDAP 目录以访问 CMC.....	114
使用 CMC Web 界面配置通用 LDAP 目录服务.....	115
使用 RACADM 配置通用 LDAP 目录服务.....	115
10 配置 CMC 进行单点登录或智能卡登录.....	117
系统要求.....	117
客户端系统.....	117
CMC.....	117
单点登录或智能卡登录的前提条件.....	118
生成 Kerberos Keytab 文件.....	118
配置 CMC 以使用 Active Directory 架构.....	118
配置浏览器以使用 SSO 登录.....	118
Internet Explorer.....	119
Mozilla Firefox	119
配置浏览器以使用智能卡登录.....	119
为 Active Directory 用户配置 CMC SSO 或智能卡登录.....	119
使用 Web 界面为 Active Directory 用户配置 CMC SSO 登录或智能卡登录.....	119
上载 Keytab 文件.....	120
使用 RACADM 为 Active Directory 用户配置 CMC SSO 登录或智能卡登录.....	120

11 配置 CMC 以使用命令行控制台.....	121
CMC 命令行控制台功能.....	121
CMC 命令行界面命令.....	121
将 Telnet 控制台与 CMC 配合使用.....	121
将 SSH 与 CMC 配合使用.....	122
支持的 SSH 加密方案.....	122
配置通过 SSH 的公共密钥验证.....	123
配置终端仿真软件.....	124
配置 Linux Minicom.....	124
使用 Connect 命令连接到服务器或 I/O 模块.....	125
为串行控制台重定向配置管理服务器 BIOS.....	126
配置 Windows 进行串行控制台重定向.....	127
配置 Linux 在引导期间进行服务器串行控制台重定向.....	127
配置 Linux 在引导后进行服务器串行控制台重定向.....	128
12 使用 FlexAddress 和 FlexAddress Plus 卡.....	129
关于 FlexAddress.....	129
关于 FlexAddress Plus.....	129
激活 FlexAddress.....	129
激活 FlexAddress Plus.....	130
验证 FlexAddress 激活.....	131
停用 FlexAddress.....	131
查看 FlexAddress 信息.....	132
查看机箱的 FlexAddress 信息.....	132
查看所有服务器的 FlexAddress 信息.....	132
查看单个服务器的 FlexAddress 信息.....	133
配置 FlexAddress.....	133
LAN 唤醒和 FlexAddress.....	134
为机箱级结构和插槽配置 FlexAddress.....	134
查看全局名称/介质访问控制 (WWN/MAC) ID.....	135
命令消息.....	135
FlexAddress DELL 软件许可协议.....	136
13 管理结构.....	139
无效配置.....	139
刷新开机场景.....	139
监测 IOM 运行状况.....	139
为 IOM 配置网络设置.....	139
使用 CMC Web 界面为 IOM 配置网络设置.....	140
使用 RACADM 为 IOM 配置网络设置.....	140
管理输入/输出模块的电源控制操作.....	140

启用或禁用输入/输出模块的 LED 闪烁.....	140
14 管理和监测电源.....	141
冗余策略.....	141
交流冗余策略.....	141
电源设备冗余策略.....	142
动态电源设备接入.....	142
默认冗余配置.....	143
交流冗余.....	143
电源设备冗余.....	143
硬件模块电源预算.....	143
服务器插槽电源优先级设置.....	144
为服务器分配优先级.....	145
使用 CMC Web 界面为服务器分配优先级.....	145
使用 RACADM 为服务器分配优先级.....	145
查看功耗状态.....	145
使用 CMC Web 界面查看功耗状态.....	145
使用 RACADM 查看功耗状态.....	145
使用 CMC Web 界面查看电源预算状态.....	146
使用 RACADM 查看电源预算状态.....	146
冗余状态和总体电源运行状况.....	146
PSU 出现故障后的电源管理。.....	146
卸下 PSU 后的电源管理.....	146
新的服务器接入策略.....	146
系统事件日志中的电源和冗余策略更改.....	147
配置电源预算和冗余.....	148
节能和电源预算.....	148
最大节能模式.....	148
减少服务器功率以维持功率预算.....	148
PSU 在 110V 交流电源下工作.....	149
远程日志记录.....	149
外部电源管理.....	149
使用 CMC Web 界面配置电源预算和冗余.....	149
使用 RACADM 配置电源预算和冗余.....	150
执行电源控制操作.....	152
对机箱执行电源控制操作.....	152
使用 Web 界面对机箱执行电源控制操作.....	152
使用 RACADM 对机箱执行电源控制操作.....	152
对服务器执行电源控制操作.....	152
使用 CMC Web 界面对多个服务器执行电源控制操作.....	153
对 IOM 执行电源控制操作.....	153
使用 CMC Web 界面对 IOM 执行电源控制操作.....	153

使用 RACADM 对 IOM 执行电源控制操作.....	153
15 管理机箱存储.....	155
查看存储组件的状态.....	155
查看存储拓扑.....	155
将虚拟适配器分配到插槽.....	155
使用 CMC Web 界面查看控制器属性.....	156
使用 RACADM 查看控制器属性.....	156
导入或清除外部配置.....	156
使用 CMC Web 界面查看物理磁盘属性.....	156
使用 RACADM 查看物理磁盘驱动器属性.....	157
识别物理磁盘和虚拟磁盘.....	157
使用 CMC Web 界面分配全局热备用.....	157
使用 RACADM 分配全局热备用.....	157
使用 CMC Web 界面查看虚拟磁盘属性.....	157
使用 RACADM 查看虚拟磁盘属性.....	158
使用 CMC Web 界面创建虚拟磁盘.....	158
为虚拟磁盘应用虚拟适配器访问策略.....	158
使用 CMC Web 界面修改虚拟磁盘属性.....	159
使用 CMC Web 界面查看机柜属性.....	159
16 管理 PCIe 插槽.....	161
使用 CMC Web 界面查看 PCIe 插槽属性.....	161
使用 CMC Web 界面将 PCIe 插槽分配至服务器.....	161
使用 RACADM 管理 PCIe 插槽.....	161
17 故障排除和恢复.....	163
使用 RACDUMP 收集配置信息、机箱状态和日志.....	163
支持的接口.....	163
下载 SNMP 管理信息库 (MIB) 文件.....	164
远程系统故障排除首先需要执行的步骤.....	164
电源故障排除.....	164
警报故障排除.....	165
查看事件日志.....	165
查看硬件日志.....	166
查看机箱日志.....	166
使用诊断控制台.....	167
重设组件.....	167
保存或还原机箱配置.....	167
网络时间协议 (NTP) 错误故障排除.....	168
LED 颜色和闪烁样式说明.....	168
无响应 CMC 的故障排除.....	170

观察 LED 隔离问题.....	170
从 DB-9 串行端口获取恢复信息.....	171
恢复固件映像.....	171
排除网络故障.....	171
控制器故障排除.....	172
18 使用 LCD 面板界面.....	173
LCD 导航.....	173
主菜单.....	174
KVM 映射菜单.....	174
DVD 映射.....	174
机柜菜单.....	174
IP 摘要菜单.....	175
设置.....	175
诊断程序.....	176
前面板 LCD 消息.....	176
LCD 模块与服务器状态信息.....	176
19 常见问题.....	179
RACADM.....	179
管理和恢复远程系统.....	179
Active Directory.....	180
FlexAddress 和 FlexAddressPlus.....	181
IOM.....	182

概览

Dell Chassis Management Controller (CMC) for Dell PowerEdge VRTX 是用于管理 **PowerEdge VRTX** 机箱的系统管理硬件和软件解决方案。CMC 具有自己的微处理器和内存，由其所插入的模块化机箱供电。

IT 管理员使用 CMC 可以：

- 查看资源清册
- 执行配置并监测任务
- 远程打开和关闭机箱和服务器的电源
- 支持针对服务器模块中的服务器和组件事件发出警报
- 查看和管理 VRTX 机箱中的存储控制器和硬盘驱动器
- 管理 VRTX 机箱中的 PCIe 子系统
- 为机箱中的 iDRAC 和 I/O 模块提供一对多管理界面

您可以为 PowerEdge VRTX 机箱配置单个 CMC 或冗余 CMC。在冗余 CMC 配置中，如果主要 CMC 与机箱或管理网络失去通信，则待机 CMC 会接管机箱管理。

CMC 为服务器提供多项系统管理功能。电源和温度管理是 CMC 的主要功能，下面列出了这些功能：

- 机柜级别电源和温度实时自动管理。
 - CMC 监测系统电源要求并支持可选的动态电源设备接入 (DPSE) 模式。此模式使 CMC 可以在服务器处于待机模式时设置电源设备，并动态管理负载和冗余要求，从而提高电源效率。
 - CMC 报告实时功耗，包括用时间戳记录的高点和低点。
 - CMC 支持设置可选的机柜最大功率限制（系统输入功率上限），一旦超过该限制就会触发警报和采取措施，例如限制服务器功耗和/或防止新服务器开机，以使机柜功率保持在规定的最大功率限制以内。
 - CMC 监测实际环境温度和内部温度测量值，并据此自动控制冷却风扇和鼓风机的运转。
 - CMC 提供全面的机柜资源清册和状态或错误报告。
- CMC 提供针对以下设置的集中配置机制：
 - Dell PowerEdge VRTX 机柜的网络和安全设置。
 - 电源冗余和电源上限设置。
 - I/O 交换机和 iDRAC 网络设置。
 - 服务器模块上的第一引导设备。
 - 检查 I/O 模块和服务器之间的 I/O 结构一致性。CMC 还可根据需要禁用组件，以保护系统硬件。
 - 用户访问安全保护。
 - 存储组件。
 - PCIe 插槽。

可以将 CMC 配置为在出现与温度、硬件误配置、电源故障、风扇速度和鼓风机等相关的警告或错误时，发送电子邮件警报或 SNMP 陷阱警报。

本发行版中的新增功能

此版本 Dell PowerEdge VRTX 的 CMC 支持：

- 对 M520 和 M620 服务器的 Ivy Bridge 支持
- 支持光纤信道 PCIe 卡
- 将 BIOS 配置文件保存至硬盘驱动器 (HDD) 用于还原至相同或不同的机箱
- 多机箱管理
- 从主机箱选择机箱配置属性并将这些属性应用到成员机箱的能力。
- 组成员机箱保持其机箱设置与主机箱同步的能力
- 不需重新启动服务器模块而从 CMC 重设 iDRAC
- 显示机箱服务器和机箱组的组件资源清册
- 配置文件到服务器的 Quick Deploy
- 通过配置文件管理服务器设置——备份、还原和复制
- 支持服务器配置文件的所有可用复制设置
- 默认检查凭据并通过 GUI、CLI 和 SNMP 警报向用户显示警告
- 阻止登录尝试失败的用户和 IP 地址
- 使用 DNS 名称启动 iDRAC
- 对 OMPC 的附加 WS-Man 支持
- 将 Linux 内核更新至版本 3.20

主要功能

CMC 功能分为管理功能和安全保护功能。

管理功能

CMC 提供以下管理功能：


- 冗余 CMC 环境。
- IPv4 和 IPv6 的动态域名系统 (DDNS) 注册。
- 本地用户、Active Directory 和 LDAP 的登录管理与配置。
- 可以启用高级冷却选项来提供附加冷却以改进性能，例如 ECM（增强冷却模式）和风扇偏移。
- 使用 SNMP、Web 界面、KVM、Telnet 或 SSH 连接进行远程系统管理和监测。
- 监测 - 允许访问系统信息和组件状态。
- 访问系统事件日志 - 允许访问硬件日志和机箱日志。
- 针对各种机箱组件的固件更新 - 允许更新 CMC、服务器上 iDRAC、机箱基础结构和机箱存储的固件。
- 使用 Lifecycle Controller，在机箱中的多个服务器上进行 BIOS、网络控制器和存储控制器等服务器组件的固件更新。
- Dell OpenManage 软件集成 - 使您能够从 Dell OpenManage Server Administrator 或 OpenManage Essentials (OME) 1.2 启动 CMC Web 界面。
- CMC 警报 - 通过远程系统日志电子邮件或 SNMP 陷阱对潜在管理节点问题发出警报。
- 远程电源管理 - 从管理控制台提供远程电源管理功能，如关机和重设任意机箱组件。
- 电源使用情况报告。
- 安全套接字层 (SSL) 加密 - 通过 Web 界面提供安全的远程系统管理。
- Integrated Dell Remote Access Controller (iDRAC) Web 界面的启动点。
- 支持 WS-Management。
- FlexAddress 功能 - 使用机箱为特定插槽分配的 WWN/MAC ID 替换出厂配置的全局名称/介质访问控制 (WWN/MAC) ID；可选升级。
- 机箱组件状态和运行状况的图形显示。

- 支持一个和多个插槽的服务器。
- LCD iDRAC 配置向导支持 iDRAC 网络配置。
- iDRAC 单点登录。
- 网络时间协议 (NTP) 支持。
- 增强的服务器摘要、电源报告和电源控制页面。
- 强制 CMC 故障转移，以及服务器的虚拟重置。
- 多机箱管理，可从主机箱查看最多 8 个其他机箱。
- 配置机箱中的存储组件。
- 将 PCIe 插槽映射到服务器及其标识。

安全功能

CMC 提供以下安全功能：

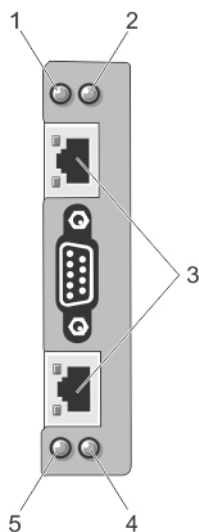
- 密码级别安全性管理 - 防止未经授权访问远程系统。
- 通过以下方式集中进行用户验证：
 - 使用标准架构或扩展架构（可选）的 Active Directory。
 - 存储于硬件的用户 ID 和密码。
- 基于角色的授权，使管理员能为每位用户配置特定权限。
- 通过 Web 界面配置用户 ID 和密码。Web 界面支持 128 位 SSL 3.0 加密和 40 位 SSL 3.0 加密（适用于不接受 128 位加密的国家/地区）。

 **注：** Telnet 不支持 SSL 加密技术。

- 可配置 IP 端口（如适用）。
- 每个 IP 地址的登录失败限制，在超过此限制时阻塞来自该 IP 地址的登录。
- 可配置会话自动超时和一个以上并发会话。
- 限制连接到 CMC 的客户端的 IP 地址范围。
- 使用加密层的 Secure Shell (SSH) 实现更高的安全保护。
- 单点登录、双重验证和公共密钥验证。

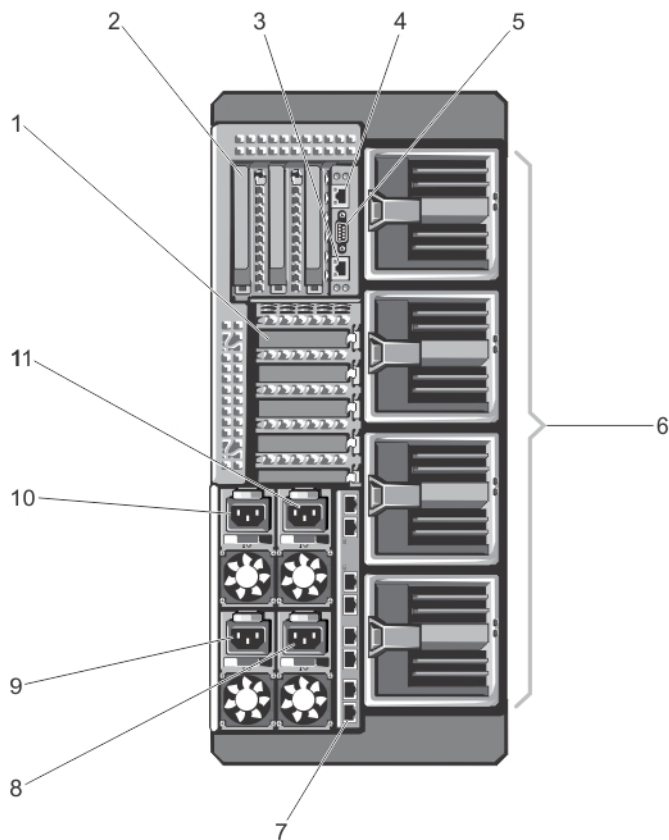
机箱概览

下图显示了 CMC 连接器视图。



项目	指示灯、按钮或连接器
1	状态/标识指示灯 (CMC 1)
2	电源指示灯 (CMC 1)
3	CMC 连接器端口 (2)
4	电源指示灯 (CMC 2)
5	状态/标识指示灯 (CMC 2)

这里显示了机箱的背面板视图，并在表格中列出了 CMC 中的可用部件和设备。



项目	指示灯、按钮或连接器
1	薄型 PCIe 扩展卡插槽 (5 个)
2	全高 PCIe 扩展卡插槽 (3 个)
3	CMC GB 以太网端口 (CMC-2)
4	CMC GB 以太网端口 (CMC-1)
5	串行连接器
6	鼓风机模块 (4 个)
7	I/O 模块端口

项目	指示灯、按钮或连接器
8	PSU 4
9	PSU 3
10	PSU 1
11	PSU 2

这里显示了机箱的前面板视图，并在表格中列出了 CMC 中的可用部件和设备。

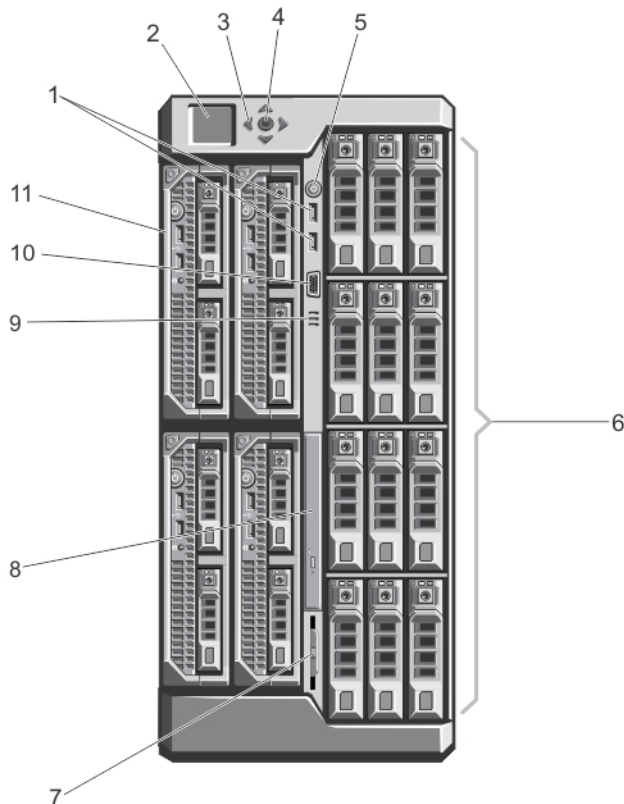



图 1: 前面板功能部件和指示灯 - 3.5 英寸硬盘驱动器机箱

项目	指示灯、按钮或连接器	说明
1	USB 连接器 (2 个)	用于将键盘和鼠标连接到系统。
2	LCD 面板	提供系统信息、状态和错误消息，以指示系统何时运行正常或何时需要注意。
3	LCD 菜单滚动按钮 (4 个)	使光标移动一格。
4	选择 (“选中”) 按钮	选择和保存 LCD 屏幕上的项目，以及移动到下一个屏幕。
5	机柜通电指示灯、电源按钮	通电指示灯在机柜接通电源时亮起。电源按钮控制 PSU 到系统的输出。

项目	指示灯、按钮或连接器	说明
6	硬盘驱动器 (HDD)	<p>2.5 英寸硬盘驱动器机柜 最多 25 个 2.5 英寸可热插拔硬盘驱动器。</p> <p>3.5 英寸硬盘驱动器机柜 最多 12 个 3.5 英寸可热插拔硬盘驱动器。</p>
7	信息标签	滑出式标签牌，可用于记录系统信息，例如服务标签、NIC、MAC 地址、系统电气额定值和全球管制机构标志。
8	光盘驱动器（可选）	一个可选的 SATA DVD-ROM 驱动器或 DVD+/-RW 驱动器。
9	通风孔	温度传感器的通风孔。  注: 为确保正常冷却，请确认通风孔未堵塞。
10	视频连接器	用于将显示器连接到系统。
11	服务器模块	最多 4 个专为机柜配置的 PowerEdge M520 或 M620 服务器模块。

支持的远程访问连接

下表列出支持的远程访问控制器。

表. 1: 支持的远程访问连接

连接	功能
CMC 网络接口端口	<ul style="list-style-type: none"> GB 端口：CMC Web 界面专用网络接口。 DHCP 支持。 SNMP 陷阱和电子邮件事件通知。 iDRAC 和输入/输出模块 (IOM) 的网络接口。 支持 Telnet/SSH 命令控制台和 RACADM CLI 命令，包括系统引导、重设、开机和关机命令。
串行端口	<ul style="list-style-type: none"> 支持串行控制台和 RACADM CLI 命令，包括系统引导、重设、开机和关机命令。 支持专门设计使用二进制协议与特定类型输入/输出模块通信的应用程序进行二进制交换。 通过 connect（或 racadm connect）命令，可将串行端口连接到内部服务器的串行控制台或 I/O 模块。 仅提供对活动 CMC 的访问。

支持的平台

CMC 支持为 PowerEdge VRTX 平台设计的模块化服务器。有关 CMC 兼容性的信息，请参阅设备的说明文件。有关最新支持的平台的信息，请参阅 dell.com/support/manuals 上的 *Dell Chassis Management Controller (CMC) Version 1.00 for Dell PowerEdge VRTX Release Notes*（Dell PowerEdge VRTX 的 Dell Chassis Management Controller (CMC) 1.00 版本发行说明）。

支持的管理站操作系统和 Web 浏览器

Dell PowerEdge VRTX 支持以下操作系统和 Web 浏览器：

- Microsoft Internet Explorer 9: Windows 7 (32 位)、Windows 7 (64 位)、Windows Server 2008、Windows Server 2008 (64 位) 和 Windows Server 2008 R2 (64 位)。
- Microsoft Internet Explorer 10: Windows 7 (32 位)、Windows 7 (64 位)、Windows 8 (32 位)、Windows 8 (64 位)、Windows Server 2008、Windows Server 2008 (64 位)、Windows Server 2008 R2 (64 位) 和 Windows 8 Server。
- Mozilla Firefox 20.0.1: Windows 7 (32 位)、Windows 7 (64 位)、Windows 8 (32 位)、Windows 8 (64 位)、Macintosh OSX Lion、Windows Server 2008、Windows Server 2008 (64 位)、Windows Server 2008 R2 (64 位) 和 Windows 8 Server。
- Google Chrome 26.0.1410: Windows 8 (32 位)、Windows 8 (64 位)。
- 原生的 Mozilla Firefox: SLES 10 SP4、SLES 11 SP2、SLES 11 SP3、RHEL 5.8 (32 位)、RHEL 5.8 (64 位)、RHEL 6.3、RHEL 6.4。

管理许可证

基于所购买的许可证 (CMC Express 或 CMC Enterprise) 提供 CMC 功能。界面中只提供已获得许可的功能，以允许您配置或使用 CMC。例如 CMC Web 界面、RACADM、WS-MAN 等。始终可通过 CMC Web 界面和 RACADM 访问 CMC 许可证管理和固件更新功能。

许可证类型

提供的许可证类型包括：

- 30 天评估和扩展 - 许可证在 30 天到期后可延长 30 天。评估许可证按持续时间计时，计时器在为系统通电时开始计时。
- 永久 - 许可证绑定到服务标签，而且是永久性的。


获取许可证

使用以下任何方法都可获取许可证：

- 电子邮件 - 从技术支持中心请求后，许可证会附加到发送的电子邮件中。
- 自助服务门户 - CMC 中提供了自助服务门户的链接。单击该链接可打开互联网上的许可自助服务门户，通过该门户可购买许可证。有关更多信息，请参阅自助服务门户页面的联机帮助。
- 销售点 - 订购系统时即可获得许可证。


许可证操作

在执行许可证管理任务之前，请确保获得许可证。有关详细信息，请参阅 support.dell.com 上提供的《概览和功能指南》。


 **注:** 如果您购买的系统已预先安装所有许可证，请无需进行许可证管理。

对于一对一许可证管理，您可以使用 CMC、RACADM 和 WS-MAN 执行以下许可操作；对于一对多许可证管理，您可以使用 Dell License Manager 执行以下许可操作：

- 查看 - 查看当前许可证信息。
- 导入 - 获取许可证后，将许可证存储在本地存储位置，并使用支持的界面之一将其导入 CMC。如果许可证通过验证检查，则会导入。

 **注:** 对于新功能，可能需要重新启动 CMC 才能启用功能。

- 导出 - 将已安装的许可证导出至外部存储设备进行备份，或者在更换维修部件后重新安装许可证。导出许可证的文件名和格式为 <EntitlementID>.xml。
- 删除 - 如果组件丢失，删除分配给组件的许可证。将许可证删除后，它不会存储在 CMC 中，并且基本产品功能会启用。
- 更换 - 将许可证更换为扩展评估许可证，更改许可证类型（如使用购买的许可证更改评估许可证），或者扩展过期的许可证。
- 您可以使用升级的评估许可证或购买的许可证更换评估许可证。
- 您可以使用更新的许可证或升级的许可证更换购买的许可证。
- 了解详情 - 了解已安装许可证或可供服务器上已安装组件使用的许可证的详细信息。

 **注:** 为了让 Learn More（了解详情）选项显示正确的页面，请确保在 Security Settings “安全设置”中已将 *.dell.com 添加到 Trusted Sites（受信任的站点）列表中。有关更多信息，请参阅“Internet Explorer 帮助”文档。

许可证组件的状态或条件以及可用操作

下表提供了基于许可证状态或条件的可用许可证操作列表。

表 1. 基于状态和条件的许可证操作

许可证/组件状态或条件	导入	导出	删除	替换	了解更多
非管理员登录	是	否	否	否	是
活动许可证	是	是	是	是	是
过期许可证	否	是	是	是	是
许可证已安装但组件丢失	否	是	是	否	是

使用 CMC Web 界面管理许可证

要使用 CMC Web 界面管理许可证，请转至 **机箱概览** → **设置 机箱概览** → **设置** → **许可证**。

导入许可证之前，确保将有效的许可证文件存储在本地系统或可从 CMC 访问的网络共享位置中。许可证可以是嵌入式的，或者是从 **自助服务 Web 门户** 或许可证密钥管理工具通过电子邮件发送的。

许可 页面显示与设备相关联的许可证，或者已安装但系统中不存在的设备的许可证。有关导入、导出、删除或替换许可证的更多信息，请参阅 **联机帮助**。

使用 RACADM 管理许可证

要使用 RACADM 命令管理许可证，请使用以下许可证子命令。

```
racadm license <license command type>
```

有关 RACADM 命令的更多信息，请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

CMC 中的可授权功能

此表中列出了基于您的许可证启用的 CMC 功能列表。

功能	Express	企业	注释
CMC 网络	是	是	
CMC 串行端口	是	是	
Active Directory 和 LDAP	否	是	
插槽和功能分配 (PCIe 和虚拟适配器)	否	是	
RACADM (SSH、本地和远程)	是	是	
CMC 设置备份	否	是	
CMC 设置还原	是	是	
WS-MAN	是	是	
SNMP	是	是	
Telnet	是	是	
SSH	是	是	
基于 Web 的界面	是	是	
电子邮件警报	是	是	
LCD 部署	是	是	
扩展的 iDRAC 管理	是	是	
机柜还原和备份	否	是	
服务器模块固件更新	否	是	
远程系统日志	否	是	
目录服务	否*	是	*对于非默认目录服务设置, Express 许可证仅允许“重设目录服务”操作。“重设目录服务”将目录服务重设为出厂默认值。
iDRAC 单一登录	否	是	
双重验证	否	是	
PK 验证	否	是	
机箱分组	否	是	
远程文件共享	是	是	
插槽资源管理	否	是	
机柜级功率上限	否*	是	*对于非默认电源上限设置, Express 许可证仅允许“还原功率上限”操作。“还原功率上限”将功率上限设置重设为出厂默认值。
动态电源设备接入	否*	是	*对于非默认 DPSE 设置, Express 许可证仅允许“还原 DPSE”操作。“还原 DPSE”将 DPSE 重设为出厂默认值。
多机箱管理	否	是	
高级配置	否	是	
机柜级备份	否	是	
FlexAddress 启用	否*	是	*对于非默认 FlexAddress 设置, Express 许可证仅允许“还原默认”操作。“还原默认”将 FlexAddress 设置重设为出厂默认值。

PCIe 适配器映射	是	是	*Express 许可证最多可为每个服务器分配两个 PCIe 适配器。
虚拟适配器至插槽的映射	否*	是	*对于非默认虚拟适配器映射，Express 许可证仅允许默认映射。“还原默认”将虚拟适配器映射更改为出厂默认值。
取消虚拟适配器至插槽的映射	是	是	
服务器克隆	否	是	
一对多服务器固件更新	否	是	
iDRAC 的一对多配置	否	是	

查看 CMC Web 界面的本地化版本

要查看 CMC Web 界面的本地化版本，请浏览 Web 浏览器的说明文件。

支持的管理控制台应用程序

CMC 支持与 Dell OpenManage Console 集成。有关更多信息，请参阅 dell.com/support/manuals 上的 OpenManage Console 说明文件。

如何使用本用户指南

本用户指南中的内容指导您使用以下工具执行任务：

- Web 界面：本指南只提供任务相关信息。有关字段和选项的信息，请参阅可通过 Web 界面打开的 *CMC for Dell PowerEdge VRTX 联机帮助*。
- RACADM 命令：本指南介绍您必须使用的 RACADM 命令或对象。有关 RACADM 命令的更多信息，请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

您可能需要的其他说明文件

可从 Dell 支持网站访问说明文件。除了本参考指南之外，还可以从 dell.com/support/manuals 访问以下指南。

- *VRTX CMC 联机帮助*提供有关使用 Web 界面的信息。要访问联机帮助，请在 CMC Web 界面上单击**帮助**。
- *Chassis Management Controller Version 1.0 for Dell PowerEdge VRTX RACADM Command Line Reference Guide*（Dell PowerEdge VRTX 的 Chassis Management Controller 1.0 版 RACADM 命令行参考指南）提供有关使用 VRTX 相关 RACADM 功能的信息。
- *Dell Chassis Management Controller (CMC) for Dell PowerEdge VRTX Version 1.00 Release Notes*（Dell PowerEdge VRTX 的 Dell Chassis Management Controller (CMC) 1.00 版本发行说明）提供系统或说明文件的最新更新，或者是面向有经验的用户或技术人员的高级技术参考资料。
- *Integrated Dell Remote Access Controller 7 (iDRAC7) User's Guide*（Integrated Dell Remote Access Controller 7 (iDRAC7) 用户指南）提供有关在管理系统中安装、配置和维护 iDRAC 的信息。
- *Dell OpenManage Server Administrator's User's Guide*（Dell OpenManage Server Administrator 用户指南）提供了有关安装和使用 Server Administrator 的信息。
- *Dell Update Packages User's Guide*（Dell Update Package 用户指南）提供了有关获取和作为系统更新策略的一部分使用 Dell Update Package 的信息。
- *Dell Shared PowerEdge RAID Controller (PERC) 8 User's Guide*（Dell Shared PowerEdge RAID Controller (PERC) 8 用户指南）提供有关部署 Shared PERC 8 卡和管理存储子系统的信息。此说明文件在 dell.com/storagecontrollermanuals 上在线提供。

- Dell 系统管理应用程序说明文件提供了关于安装和使用系统管理软件的信息。

以下系统说明文件提供关于安装 VRTX CMC 的系统的更多信息：

- 系统随附的安全说明提供了重要的安全和法规信息。其他法规信息请参阅法规合规性主页，网址是 dell.com/regulatory_compliance。保修信息可能包含于此说明文件中，也可能为单独的说明文件。
- 系统随附的 *Dell PowerEdge VRTX Getting Started Guide*（Dell PowerEdge VRTX 入门指南）提供系统功能概览、系统设置方法以及技术规格。
- 系统随附的设置单张说明文件提供有关初始系统设置和配置的信息。
- 服务器模块的 *用户手册* 提供有关服务器模块功能的信息，并介绍如何排除服务器模块故障，以及如何安装或更换服务器模块的组件。此说明文件在 dell.com/poweredgemanuals 上在线提供。
- 机架解决方案附带的机架说明文件介绍了如何将系统安装到机架中（如果需要）。
- 有关本说明文件中所用缩写或缩略词的全称，请参阅 dell.com/support/manuals 上的 Glossary（词汇表）。
- 系统管理软件说明文件介绍了软件的功能、要求、安装和基本操作。
- 单独购买的任何组件所附带的说明文件均提供有关配置和安装这些选件的信息。
- 系统随附的所有介质都提供了用于配置和管理系统的说明文件和工具，包括与随系统购买的操作系统、系统管理软件、系统更新以及系统组件相关的说明文件和工具。有关系统的更多信息，请扫描系统的快速资源定位器（QRL）以及系统随附的系统设置单张说明文件。从移动平台下载 QRL 应用，以便在您的移动设备上启用该应用。

系统有时附带更新，用于说明对系统、软件和/或说明文件所做的更改。请务必先阅读这些更新，因为这些更新通常会取代其他说明文件中的信息。

从 Dell 支持站点访问说明文件

您可以通过以下方式之一访问所需的说明文件：

- 从以下链接：
 - 所有系统管理说明文件 — dell.com/softwaresecuritymanuals
 - 企业系统管理说明文件 — dell.com/openmanagemanuals
 - 远程企业系统管理说明文件 — dell.com/esmmanuals
 - 适用性工具说明文件 - dell.com/serviceabilitytools
 - 客户端系统管理说明文件 — dell.com/OMConnectionsClient
 - OpenManage Connections Enterprise 系统管理说明文件 — dell.com/OMConnectionsEnterpriseSystemsManagement
 - OpenManage Connections Client 系统管理说明文件 — dell.com/OMConnectionsClient
- 从 Dell 支持站点，请按以下步骤进行：
 - 访问 dell.com/support/manuals。
 - 在 **Tell us about your Dell system**（向我们介绍您的 Dell 系统）部分中的 **No**（否）下，选择 **Choose from a list of all Dell products**（从 Dell 产品的完整列表中选择），然后单击 **Continue**（继续）。
 - 在 **Select your product type**（选择您的产品类型）部分，单击 **Software and Security**（软件和安全）。
 - 在 **Choose your Dell Software**（选择您的 Dell 软件）部分中，从以下项目中单击所需的链接：
 - * **Client System Management**
 - * **Enterprise System Management**
 - * **Remote Enterprise System Management**
 - * **Serviceability Tools**
 - 要查看说明文件，请单击所需的产品版本。

- 使用搜索引擎，请按以下步骤进行：
 - 在**搜索框**中键入说明文件的名称和版本。

安装和设置 CMC

本节介绍如何安装 CMC 硬件、建立对 CMC 的访问、配置您的管理环境以使用 CMC 并引导您完成配置 CMC 的任务：

- 设置对 CMC 的初始访问。
- 通过网络访问 CMC。
- 添加并配置 CMC 用户。
- 更新 CMC 固件。

有关安装和设置冗余 CMC 环境的更多信息，请参阅[了解冗余 CMC 环境](#)。

开始之前



在设置 CMC 环境之前，请从 dell.com/support/ 下载适用于 PowerEdge VRTX 的最新 CMC 固件版本。此外，确保您拥有系统随附的 *Dell Systems Management Tools and Documentation DVD*。

安装 CMC 硬件

CMC 已预先安装在机箱中，因此无需安装。可以安装第二个 CMC 作为活动 CMC 的备用。

设置机箱一览表

使用以下任务可准确设置机箱：

1. CMC 与使用浏览器的管理站必须位于相同的网络中，即管理网络。将以太网网络电缆从 CMC 活动端口连接至管理网络。
2. 在机箱中安装 I/O 模块，并将网络电缆连接到机箱。
3. 在机箱中插入服务器。
4. 将机箱与电源相连。
5. 在完成第 7 步中的任务之后，按电源按钮或者从 CMC Web 界面打开机箱电源。
 **注：**不要打开服务器电源。
6. 使用 LCD 面板，导航到“IP 摘要”并单击“选中”按钮选择。在管理系统浏览器（IE、Chrome 或 Mozilla）中使用 CMC 的 IP 地址。要设置 CMC 的 DHCP，请使用 LCD 面板，单击**主菜单** → **设置** → **网络设置**。
7. 使用 Web 浏览器通过键入默认用户名 (root) 和密码 (calvin) 连接到 CMC IP 地址。
8. 在 CMC Web 界面中为每个 iDRAC 提供一个 IP 地址并启用 LAN 和 IPMI 界面。
 **注：**一些服务器上默认显示 iDRAC LAN 界面。此信息可以在 CMC Web 界面的**服务器概览** → **设置**下找到。这可能是一个高级许可证选项；在此情况下必须为每个服务器使用**设置**功能。
9. 在 CMC Web 界面中为 IO 模块提供 IP 地址。您可以通过单击 **I/O 模块概览**然后单击**设置**来获取 IP 地址。
10. 通过 Web 浏览器连接到各 iDRAC 并提供 iDRAC 的最终配置。默认用户名是 root，密码是 calvin。
11. 使用 Web 浏览器连接到 I/O 模块并提供 I/O 模块的最终配置。

12. 打开服务器电源并安装操作系统。

基本 CMC 网络连接

为了提供最高的冗余度，请将每个可用的 CMC 连接到您的管理网络。

在管理站上安装远程访问软件

可使用远程访问软件（例如 Telnet、Secure Shell (SSH) 或操作系统上提供的串行控制台公用程序）或 Web 界面从管理站访问 CMC。


若要从管理站使用远程 RACADM，则使用系统随附的 *Dell Systems Management Tools and Documentation* DVD 安装远程 RACADM。这张 DVD 包括以下 Dell OpenManage 组件：

- DVD 根目录 - 包含 Dell Systems Build and Update Utility。
- SYSMGMT - 包含系统管理软件产品，其中包括 Dell OpenManage Server Administrator。
- DOCS - 包含系统、系统管理软件产品、外设和 RAID 控制器的说明文件。
- SERVICE - 包含配置系统所需的工具，并提供最新的诊断程序和 Dell 专为您的系统优化的驱动程序。

有关安装 Dell OpenManage 软件组件的信息，请参阅 DVD 或 dell.com/support/manuals 上提供的 *Dell OpenManage Installation and Security User's Guide*（Dell OpenManage 安装和安全用户指南）。您也可以从 support.dell.com 下载最新版本的 Dell DRAC 工具。

在 Linux 管理站上安装 RACADM


1. 以 root 用户身份登录到运行支持的 Red Hat Enterprise Linux 或 SUSE Linux Enterprise Server 操作系统的系统，从而在该系统中安装管理系统组件。
2. 将 *Dell Systems Management Tools and Documentation* DVD 插入 DVD 驱动器。
3. 若要将 DVD 装载到所需位置，则使用 mount 命令或类似命令。

 **注：**在 Red Hat Enterprise Linux 5 操作系统中，通过 `-noexec mount` 选项自动装载 DVD。该选项不允许从 DVD 运行任何可执行程序。您需要手动装载 DVD-ROM，然后运行命令。

4. 导航至 `SYSMGMT/ManagementStation/linux/rac` 目录。要安装 RAC 软件，请输入以下命令：

```
rpm -ivh *.rpm
```

5. 要查看 RACADM 命令帮助，请在运行前面的命令后键入 `racadm help`。有关 RACADM 的更多信息，请参阅 *Chassis Management Controller for Dell PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for Dell PowerEdge VRTX RACADM 命令行参考指南）。

 **注：**使用 RACADM 远程功能时，在使用涉及文件操作的 RACADM 子命令的文件夹上必须具有“写”权限。例如：`racadm getconfig -f <file name>`。

从 Linux 管理站卸载 RACADM


1. 以 root 用户身份登录到要卸载管理站功能的系统。
2. 运行以下 rpm 查询命令以确定安装的 DRAC 工具版本：

```
rpm -qa | grep mgmtst-racadm
```
3. 验证要卸载的软件包版本，通过使用 `rpm -e rpm -qa | grep mgmtst-racadm` 命令卸载该功能。


配置 Web 浏览器

您可以通过 Web 浏览器配置和管理机箱中安装的 CMC、服务器和模块。请参阅 dell.com/support/manuals 上的 *Dell Systems Software Support Matrix*（Dell 系统软件支持值表）中的“支持的浏览器”部分。

CMC 与使用浏览器的管理站必须位于相同的网络中，称之为 *管理网络*。根据安全性要求，管理网络可以是隔离且高度安全的网络。

 **注:** 确保管理网络上的安全措施（如防火墙和代理服务器）不会阻止您的 Web 浏览器访问 CMC。

一些浏览器功能会干扰连接或影响性能，特别是在管理网络没有到 Internet 的路由时。如果管理站在 Windows 操作系统上运行，有些 Internet Explorer 设置会干扰连接，即使使用命令行界面访问管理网络也不例外。

 **注:** 为解决安全性问题，Microsoft Internet Explorer 严格监测有关其 Cookie 管理的时间。为此，运行 Internet Explorer 的计算机上的时间必须与 CMC 上的时间同步。

代理服务器

要绕过无法访问管理网络的代理服务器进行浏览，可以将管理网络地址添加到浏览器的例外列表中。这样可以使浏览器在访问管理网络时绕过代理服务器。

Internet Explorer

要编辑 Internet Explorer 中的例外列表，请执行以下操作：

1. 启动 Internet Explorer。
2. 单击 **工具** → **Internet 选项** → **连接**。
3. 在 **局域网 (LAN) 设置** 部分，单击 **LAN 设置**。
4. 在 **代理服务器** 部分，选择为 **LAN 使用代理服务器**（这些设置不会应用于拨号或 VPN 连接）选项，然后单击 **高级**。
5. 在 **例外** 部分，将管理网络上的 CMC 和 iDRAC 地址添加到分号分隔的列表。可以在条目中使用 DNS 名称和通配符。

Mozilla Firefox

要在 Mozilla Firefox 版本 19.0 中编辑例外列表，请执行以下操作：

1. 启动 Mozilla Firefox。
2. 单击 **工具** → **选项**（对于运行 Windows 的系统），或者单击 **编辑** → **首选项**（对于运行 Linux 的系统）。
3. 单击 **高级**，然后单击 **网络** 选项卡。
4. 单击 **设置**。
5. 选择 **手动代理配置**。
6. 在 **不使用代理** 字段中，将管理网络上 CMC 和 iDRAC 的地址输入到逗号分隔的列表中。可以在条目中使用 DNS 名称和通配符。

Microsoft Phishing Filter

如果在管理系统上的 Internet Explorer 中启用 Microsoft Phishing Filter 且 CMC 不能访问 Internet，则对 CMC 的访问可能会延迟几秒钟。在使用浏览器或远程 RACADM 等其他界面时会发生这种延迟。要禁用 Phishing Filter，请执行以下操作：

1. 启动 Internet Explorer。
2. 单击 **工具** → **Phishing Filter**，然后单击 **Phishing Filter 设置**。
3. 选择 **禁用 Phishing Filter** 项选，然后单击 **确定**。

证书吊销列表 (CRL) 访存

如果 CMC 无法访问 Internet，请禁用 Internet Explorer 中的证书吊销列表 (CRL) 访存功能。该功能检测服务器（如 CMC Web 服务器）是否正在使用从 Internet 检索的已吊销证书列表中的证书。如果无法访问 Internet，那么当您使用浏览器或命令行界面（如远程 RACADM）访问 CMC 时，该功能可能导致数秒钟的延迟。

要禁用 CRL 访存，请执行以下操作：

1. 启动 Internet Explorer。
2. 单击**工具** → **Internet 选项**，然后单击**高级**。
3. 转至“安全性”部分，清除**检查发行商的证书是否吊销**选项，然后单击**确定**。

使用 Internet Explorer 从 CMC 下载文件

当使用 Internet Explorer 从 CMC 下载文件时，您可能会遇到**不将加密的页保存到磁盘**选项未启用的问题。

要启用**不将加密的页保存到磁盘**选项，请执行以下操作：

1. 启动 Internet Explorer。
2. 单击**工具** → **Internet 选项** → **高级**。
3. 在**安全**部分，选中**不将加密的页保存到磁盘**选项。

允许在 Internet Explorer 中播放动画


在 Web 界面之间传输文件时，文件传输图标将旋转以显示传输活动。在使用 Internet Explorer 时，您需要配置浏览器才能播放动画。

要将 Internet Explorer 配置为播放动画，请执行以下操作：

1. 启动 Internet Explorer。
2. 单击**工具** → **Internet 选项** → **高级**。
3. 转到**多媒体**部分，然后选中**播放网页中的动画**选项。

设置对 CMC 的初始访问

要远程管理 CMC，请将 CMC 连接到您的管理网络，然后配置 CMC 网络设置。

 **注：**要管理 PowerEdge VRTX 解决方案，它必须连接到您的管理网络。


有关配置 CMC 网络设置的信息，请参阅[配置初始 CMC 网络](#)。此初始配置将分配 TCP/IP 联网参数，以支持访问 CMC。

各服务器上的 CMC 和 iDRAC 以及交换机 I/O 模块上的网络管理端口都连接到 PowerEdge VRTX 机箱内的公共内部网络。这样可以将管理网络与服务器数据网络隔离。流量隔离对于不间断访问机箱管理功能至关重要。

CMC 连接到管理网络。所有对 CMC 和 iDRAC 的外部访问都通过 CMC 实现。对管理服务器的访问则通过与 I/O 模块 (IOM) 的网络连接实现。这使应用程序网络能够与管理网络相互隔离。

建议将机箱管理与数据网络相隔离。由于数据网络上可能存在流量，因此内部管理网络上的管理接口可能会因发送到服务器的流量而处于饱和状态。这将导致 CMC 和 iDRAC 通信发生延迟。这些延迟可能会使机箱发生意想不到的行为，例如，即使 iDRAC 已启动并运行，CMC 也会将其显示为脱机，这又会导致其他意料之外的行为。如果以物理方式隔离管理网络的做法不切实际，可以将 CMC 和 iDRAC 流量分离到单独的 VLAN。CMC 和各个 iDRAC 网络接口可配置为使用 VLAN。

配置初始 CMC 网络

 **注:**更改 CMC 网络设置可能会断开当前网络连接。

可以在 CMC 得到 IP 地址之前或之后执行初始网络配置。如果在得到 IP 地址之前配置 CMC 的初始网络设置，您可以使用以下两种界面中的任意一种：

- 机箱前面的 LCD 面板
- Dell CMC 串行控制台


如果在 CMC 得到 IP 地址后配置初始网络设置，可以使用以下任意界面：

- 命令行界面 (CLI)，如串行控制台、Telnet、SSH 或 Dell CMC 控制台。
- 远程 RACADM
- CMC Web 界面
- LCD 面板界面

CMC 同时支持 IPv4 和 IPv6 寻址模式。IPv4 和 IPv6 的配置设置相互独立。

使用 LCD 面板界面配置 CMC 网络

使用快速设置 (DHCP) 配置 CMC

 **注:**可以通过按下向上-向下按钮两秒钟来自定义 LCD 显示屏的方向（针对机架式或塔式）。或者，也可以使用向右-向左按钮。有关 CMC LCD 面板上的可用按钮的更多信息，请参阅 [LCD 导航](#)。

要使用 LCD 面板界面设置网络，请执行以下操作：

1. 按下机箱电源按钮打开机箱电源。开机过程中，LCD 面板将显示一系列初始化屏幕。
2. 在**主菜单**面板中，选择**设置**。
3. 在**LCD 语言**面板中，使用箭头按钮选择语言，然后按中央按钮。将显示**主菜单**面板。
4. 选择**设置**，然后选择**网络设置**。在**网络设置**面板中，当系统提示您选择通过使用 DHCP 快速设置 CMC 或通过高级设置模式设置时，使用箭头键并选择以下任意选项：

- **快速设置 (DHCP)**
- **高级设置**

5. 如果选择**快速设置 (DHCP)**，面板将显示以下消息。

```
About to get DHCP addresses. Ensure CMC network cable is connected.
```

按中央按钮，然后等待几分钟。面板将显示**请稍候**消息，然后 CMC IP 编号将显示在 **IP 摘要**面板上。

```
CMC IP4: <IP number>
```


按两下中央按钮。将显示**主菜单**面板。

使用高级设置配置 CMC

1. 在**网络设置**面板中，如果选择**高级设置**，则会显示以下消息，询问您是否要配置 CMC。

```
Configure CMC?
```
2. 要使用高级设置属性来配置 CMC，请单击中央按钮。转到步骤 4。另外，要配置 iDRAC，请转到步骤 14。
3. 如果系统提示您选择适当的网络速度，请使用相应按钮选择网络速度（**自动 (1Gb)**、**10Mb** 或 **100Mb**）。为获得有效的网络吞吐量，网络速度设置必须符合您的网络配置。将网络速度设置为低于您的网络配置速度会增加带宽消耗，并降低网络通信速度。确定您的网络是否支持上述网络速度并进行相应设置。如果网络配置不符合其中任何值，则建议选择**自动 (1Gb)**选项，或者参考您的网络设备制造商的用户说明文件。

4. 要选择**自动 (1Gb)**，请按两下中央按钮。转到步骤 7。否则，如果选择 **10Mb** 或 **100Mb**，请转到步骤 5。
5. 在**双工**面板上，选择符合网络环境的双工模式（**全双工**或**半双工**），按两下中央按钮。

 **注:** 如果**自动协商**设置为**开**，或者选择了**1000MB (1Gbps)**，则网络速度和双工模式设置不可用。如果为一个设备开启了自动协商，而另一个设备没有开启，则使用自动协商的设备可以决定另一个设备的网络速度，但不能决定双工模式。在这种情况下，选择半双工作为自动协商期间的双工模式。此双工不匹配会导致网络连接速度慢。
6. 在**协议**面板中，选择您要为 CMC 使用的 Internet 协议（**仅 IPv4**、**仅 IPv6** 或**两者**），按两下中央按钮。
7. 如果选择 **IPv4** 或**两者**，请转到步骤 9 或 10（根据您选择 **DHCP** 或**静态**模式）。否则，如果选择 **IPv6**，请转到本过程稍后的步骤 11。
8. 在**模式**面板中，选择 CMC 获取 NIC IP 地址的模式。如果选择 DHCP，CMC 自动从网络上的 DHCP 服务器检索 IP 配置（IP 地址、掩码和网关）。CMC 将得到您的网络中唯一的 IP 地址。如果选择 **DHCP**，请按两下中央按钮。将显示**配置 iDRAC** 面板。转到本过程稍后的步骤 12。
9. 如果选择**静态**，请按照 LCD 面板上的说明输入 IP 地址、网关和子网掩码。

将显示您输入的 IP 信息。按两下中央按钮。**CMC 配置**屏幕列出您输入的**静态 IP 地址**、**子网掩码**和**网关**设置。检查设置的准确性。要更正设置，请按相应的按钮。按两下中央按钮。将显示**是否注册 DNS?** 面板。
10. 要进行注册，请输入 DNS IP 地址，然后按中央按钮。转到步骤 12，然后选择是否要配置 iDRAC。
11. 如果选择不进行注册，请转到步骤 12。
12. 指出是否要配置 iDRAC:
 - **否**: 转到本过程稍后的步骤 17。
 - **是**: 按中央按钮。

您也可以从 CMC Web 界面配置 iDRAC。

13. 在**协议**面板中，选择要为服务器使用的 IP 类型（IPv4、IPv6 或两者）。如果选择 **IPv4** 或**两者**，请选择 **DHCP** 或**静态**，然后转到步骤 14。否则，如果选择 **IPv6**，请转到本过程稍后的步骤 17。

动态主机配置协议 (DHCP)

iDRAC 自动从网络上的 DHCP 服务器检索 IP 配置（IP 地址、掩码和网关）。iDRAC 将得到在您的网络中唯一的 IP 地址。按中央按钮，然后转到本过程的步骤 16。

静态

如果选择**静态**，请按照 LCD 屏幕上的说明手动输入 IP 地址、网关和子网掩码。

如果选择了**静态**选项，请按中央按钮，然后执行以下操作:

- a. 以下消息询问您是否在插槽 1 的 IP 的基础上自动增加。
IPs will auto-increment by slot number.
单击中央按钮。以下消息将要求您输入插槽 1 的 IP 编号。
Enter slot 1 (starting) IP
输入插槽 1 IP 编号，然后按中央按钮。
- b. 设置子网掩码，然后按中央按钮。
- c. 设置网关，然后按中央按钮。
- d. **网络摘要**屏幕列出您输入的**静态 IP 地址**、**子网掩码**和**网关**设置。检查设置的准确性。要更正设置，请按相应的按钮，然后按中央按钮。
- e. 确认所输入的设置准确性后，转到步骤 10。

14. 选择**启用**或**禁用**以指出是否要启用 IPMI over LAN。按中央按钮继续。

15. 在 **iDRAC 配置** 面板中，将显示以下消息。


Apply settings to installed servers?

要将所有 iDRAC 网络设置应用到已安装的服务器，请选择**是**，然后按中央按钮。否则，选择**否**并按中央按钮，然后转到本过程稍后的步骤 17。

16. 在接下来的 **iDRAC 配置** 面板中，将显示以下消息。
Auto-Apply settings to newly-inserted servers?
- 要将所有 iDRAC 网络设置应用到新安装的服务器，请选择**是**并按中央按钮。当机箱中插入新服务器时，LCD 会提示您是否使用之前配置的网络设置策略自动部署该服务器。如果您不想将 iDRAC 网络设置应用到新安装的服务器，请选择**否**并按中央按钮。当机箱中插入新服务器时，不会配置其 iDRAC 网络设置。
17. 在 **iDRAC 配置** 面板中，将显示以下消息。
Apply All Enclosure Settings?
- 要应用所有有机柜设置，请选择**是**并按中央按钮。否则，选择**否**并按中央按钮。
18. 在 **IP 摘要** 面板中，检查您提供的 IP 地址，以确保地址准确无误。要纠正设置，请按**后退**按钮，然后按中央按钮以返回该设置所在的屏幕。纠正 IP 地址后，请按中央按钮。
确认您输入的设置准确无误后，按两下中央按钮。将显示**主菜单**面板 ID。
现在网络上提供 CMC 和 iDRAC。可以使用 Web 界面或诸如串行控制台、Telnet 和 SSH 等 CLI 通过分配的 IP 地址访问 CMC。

访问 CMC 的界面和协议

配置完 CMC 网络设置后，可以通过各种界面远程访问 CMC。下表列出您可用于远程访问 CMC 的界面。

 **注:** 因为 Telnet 没有其他接口安全，所以默认禁用。通过使用 Web、SSH 或远程 RACADM 启用 Telnet。



 **注:** 同时使用一个以上的界面可能会产生意外的结果。

表. 2: CMC 界面

界面	说明
Web 界面	可使用图形用户界面远程访问 CMC。Web 界面构建在 CMC 固件中并从管理站上的受支持 Web 浏览器通过 NIC 接口访问。 有关所支持 Web 浏览器的列表，请参阅 dell.com/support/manuals 上 <i>Dell 系统软件支持值表</i> 中的“支持的浏览器”部分。
远程 RACADM 命令行界面	使用此命令行公用程序管理 CMC 及其组件。您可以使用远程或固件 RACADM: <ul style="list-style-type: none"> 远程 RACADM 是在管理站上运行的客户端公用程序。它使用带外网络接口在受管系统上运行 RACADM 命令，并且使用 HTTPS 通道。-r 选项在网络上运行 RACADM 命令。 固件 RACADM 可通过使用 SSH 或 Telnet 登录 CMC 来进行访问。您可以在不指定 CMC IP、用户名或密码的情况下运行固件 RACADM 命令。在输入 RACADM 提示符之后，您可以在不加 racadm 前缀的情况下直接运行命令。
机箱 LCD 面板	使用前面板上的 LCD 可以: <ul style="list-style-type: none"> 查看警报、CMC IP 或 MAC 地址、用户可编程字符串。 设置 DHCP。 配置 CMC 静态 IP 设置。
Telnet	提供命令行，用于通过网络访问 CMC。CMC 命令行提供 RACADM 命令行界面和 connect 命令，用于连接到服务器或 IO 模块的串行控制台。  注: Telnet 不是安全协议，并且在默认情况下处于禁用状态。Telnet 可传输所有数据，包括纯文本形式的密码。当传输敏感信息时，请使用 SSH 界面。

界面	说明
SSH	使用 SSH 运行 RACADM 命令。它所提供的功能与使用加密传输层的 Telnet 控制台相同，可提供更高的安全性。SSH 服务默认在 CMC 上处于启用状态，可以被禁用。
WS-MAN	<p>WSMAN 服务基于 Web 管理服务 (WSMAN) 协议，用于执行一对多系统管理任务。您必须通过 WS-MAN 客户端（如 WinRM 客户端 (Windows) 或 OpenWSMAN 客户端 (Linux)）来使用 LC 远程服务功能。您也可以使用 Power Shell 和 Python 来编写 WS-MAN 界面脚本。</p> <p>WSMAN 是用于系统管理的基于简单对象访问协议 (SOAP) 的协议。CMC 使用 WS - Management 传递分布式管理综合小组 (DMTF) 基于公用信息模型 (CIM) 的管理信息。CIM 信息定义了可在管理系统中修改的语义和信息类型。</p> <p>CMC WS-MAN 实施在端口 443 上采用 SSL 实现传输安全性，并且支持基本验证。通过 WS-Management 获得的数据由映射到 DMTF 配置文件和扩展名配置文件的 CMC 工具界面提供。</p> <p>有关更多信息，请参阅：</p> <ul style="list-style-type: none"> • MOF 和配置文件 - delltechcenter.com/page/DCIM.Library • DMTF 网站 - dmtof.org/standards/profiles/ • WS-MAN 发行说明文件。 • www.wbemsolutions.com/ws_management.html • DMTF WS-Management 规范：www.dmtf.org/standards/wbem/wsman <p>可以通过利用 Windows WinRM、Powershell CLI 等客户端基础结构、WSMANCLI 等开放源代码公用程序、以及 Microsoft .NET 等应用程序编程环境来使用 Web 服务界面。</p> <p>对于使用 Microsoft WinRM 的客户端连接，最低要求为 2.0 版本。有关更多信息，请参阅 support.microsoft.com/kb/968929 上的 Microsoft 文章。</p>

 **注:** CMC 用户名和密码的默认值分别是 `root` 和 `calvin`。

使用其他系统管理工具启动 CMC

您还可以从 Dell Server Administrator 或 Dell OpenManage Essentials 启动 CMC。

要使用 Dell Server Administrator 访问 CMC 界面，请启动管理站上的 Server Administrator。从 Server Administrator 主页的左侧窗格中，单击 **系统** → **主系统机箱** → **Remote Access Controller**。有关更多信息，请参阅 dell.com/support/manuals 上的 *Dell Server Administrator User's Guide*（Dell Server Administrator 用户指南）。

下载和更新 CMC 固件

要下载 CMC 固件，请参阅 [下载 CMC 固件](#)。

要更新 CMC 固件，请参阅 [更新 CMC 固件](#)。


设置机箱物理位置和机箱名称

您可以设置机箱在数据中心的位置，以及用于在网上标识机箱的机箱名称（默认名称为 **Dell Rack System**）。例如，对机箱名称的 SNMP 查询将返回您所配置的名称。

使用 Web 界面设置机箱物理位置和机箱名称

要使用 CMC Web 界面设置机箱位置和机箱名称，请执行以下操作：

1. 在左侧窗格中，转至**机箱概览**，然后单击**设置**。
2. 在**常规机箱设置**页面中，键入位置属性和机箱名称。有关设置机箱属性的更多信息，请参阅 *CMC 联机帮助*。

 **注：**机箱位置字段是可选字段。建议使用**数据中心**、**通道**、**机架**和**机架插槽**字段来表示机箱的物理位置。

3. 单击**应用**。将保存设置。

使用 RACADM 设置机箱物理位置和机箱名称

要通过使用命令行界面设置机箱名称、位置、日期和时间，请使用 **setsysinfo** 和 **setchassisname** 命令。有关更多信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

设置 CMC 的日期和时间

可手动设置日期和时间，也可将日期和时间与网络时间协议 (NTP) 服务器同步。

使用 CMC Web 界面设置 CMC 的日期和时间

要设置 CMC 上的日期和时间，请执行以下操作：


1. 在左侧窗格中，单击**机箱概览** → **设置** → **日期/时间**。
2. 要将日期和时间与网络时间协议 (NTP) 服务器同步，请在**日期/时间**页上，选择**启用 NTP**并最多指定三台 NTP 服务器。要手动设置日期和时间，请清除**启用 NTP**选项，然后编辑**日期**和**时间**字段。
3. 从下拉菜单中选择**时区**，然后单击**应用**。

使用 RACADM 设置 CMC 的日期和时间

要使用命令行界面设置日期和时间，请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）中的 **config** 命令和 `cfgRemoteHosts` 数据库属性组部分。

配置 LED 以识别机箱上的组件

可以让组件（机箱、服务器、物理磁盘驱动器、虚拟磁盘和 I/O 模块）的 LED 闪烁以识别机箱上的组件。


 **注：**要修改这些设置，必须具备**机箱配置管理员**权限。

使用 CMC Web 界面配置 LED 闪烁


要为一个、多个或所有组件 LED 启用闪烁，请执行以下操作：

- 在左侧窗格中，转至下列任意页面：
 - **机箱概览** → **故障排除**。
 - **机箱概览** → **故障排除**。

- 机箱概览 → 机箱控制器 → 故障排除。
- 机箱概览 → 服务器概览 → 故障排除。

 注: 只能在此页上选择服务器。

- 机箱概览 → I/O 模块概览 → 故障排除。
- 存储 → 故障排除。

 注: 在此页面上只能选择物理磁盘驱动器和虚拟磁盘。

要启用组件 LED 闪烁, 请选中与物理磁盘驱动器或虚拟磁盘相对应的**全选/取消全选**选项, 然后单击**闪烁**。要禁用组件 LED 闪烁, 请清除与 LED 相对应的**全选/取消全选**选项, 然后单击**取消闪烁**。

使用 RACADM 配置 LED 闪烁

打开到 CMC 的串行/Telnet/SSH 文本控制台, 登录并键入:

`racadm settled -m <module> [-l <ledState>]`, 其中 `<module>` 指定您要配置其 LED 的模块。配置选项包括:

- `server-n` 其中 $n=1-4$
- `switch-1`
- `cmc-active`

和 `<ledState>` 指定 LED 是否应该闪烁。配置选项包括:

- 0 - 不闪烁 (默认)
- 1 - 闪烁

`racadm raid <operation> <component FQDD>`, 其中 `operation` 的值为 `blink` 或 `unblink`, 而 FQDD 针对组件的物理磁盘驱动器和虚拟磁盘。


配置 CMC 属性

您可以使用 Web 界面或 RACADM 命令配置 CMC 属性, 如电源预算、网络设置、用户, 以及 SNMP 和电子邮件警报。

使用 CMC Web 界面配置 iDRAC 启动方法

要在**常规机箱设置**页面上配置 iDRAC 启动方法, 请执行以下操作:

1. 在左侧窗格中, 单击**机箱概览** → **设置**。
系统将显示**常规机箱设置**页面。
2. 在**iDRAC 启动方法**属性的下拉菜单中, 选择**IP 地址**或**DNS**。
3. 单击**应用**。


 注: 仅在以下情况下需要使用基于 DNS 的方法来启动任何特定 iDRAC:

- 机箱设置为 DNS。
- CMC 检测到特定 iDRAC 是使用 DNS 名称配置的。

使用 RACADM 配置 iDRAC 启动方法

要使用 RACADM 更新 CMC 固件，使用 `cfgRacTuneIdracDNSLaunchEnable` 子命令。有关更多信息，请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

使用 CMC Web 界面配置登录锁定策略属性

 **注:** 要执行以下任务，必须具备**机箱配置管理员**权限。

安全登录功能允许您使用 CMC Web 界面配置 CMC 登录的 IP 范围属性。要使用 CMC Web 界面配置 IP 范围属性，执行以下操作：

1. 在左侧窗格中，转至**机箱概览**并单击**网络** → **网络**。
将显示**网络配置**页面。
2. 在“IPv4 设置”部分，单击**高级设置**。或者，要访问**安全登录**页面，在左侧窗格中，转至**机箱概览**，然后单击**安全** → **登录**。
将显示**安全登录**页面。
3. 要启用用户阻止或 IP 地址阻止功能，请在**登录锁定策略**部分，选中**按用户名锁定**或**按 IP 地址 (IPv4) 锁定**。
设置其他登录锁定策略属性的选项将激活。
4. 在激活的字段 - **锁定失败次数**、**锁定失败窗口**和**锁定惩罚时间**中输入登录锁定策略属性必填值。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。
5. 要保存这些设置，请单击**应用**。

使用 RACADM 配置登录锁定策略属性

您可以针对以下功能使用 RACADM 配置登录锁定策略属性：

- 用户阻止
- IP 地址阻止
- 允许的登录尝试次数
- 锁定失败次数超限后的间隔时间
- 锁定惩罚时间
- 要启用用户阻止功能，请使用：

```
racadm config -g cfgRacTuning -o cfgRacTuneUserBlkEnable <0|1>
```
- 要启用 IP 阻止功能，请使用：

```
racadm config -g cfgRacTuning -o cfgRacTuneIPBlkEnable <0|1>
```
- 要指定登录尝试次数，请使用：

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount
```
- 要指定锁定失败次数超限后的间隔时间，请使用：

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow
```
- 要指定锁定惩罚时间的值，请使用：

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime
```


有关这些对象的更多信息，请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

了解冗余 CMC 环境

您可以安装待机 CMC，如果活动 CMC 停止工作，可以使用待机 CMC 继续工作。冗余 CMC 可以提前安装也可以之后安装。为确保完全冗余或最佳性能，有必要正确连接 CMC 网络电缆。

故障转移发生在以下时候：


- 运行 RACADM `cmchangeover` 命令。请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）中的 `cmchangeover` 命令部分。
- 在活动 CMC 上运行 RACADM `racreset` 命令。请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）中的 `racreset` 命令部分。
- 从 Web 界面重设活动的 CMC。请参阅[执行电源控制操作](#)中所述的**电源控制操作** `Reset CMC` 选项。
- 从活动 CMC 上卸下网络电缆。
- 从机箱中卸下活动 CMC。
- 在活动 CMC 上初始化 CMC 固件闪存。
- 有不再工作的活动 CMC。

 **注：**当 CMC 故障转移时，所有 iDRAC 连接和所有活动 CMC 会话都将注销。注销会话的用户必须重新连接到新的活动 CMC。

关于待机 CMC

待机 CMC 等同于活动 CMC 的镜像，并作为镜像进行维护。活动和待机 CMC 都必须安装相同的固件版本。如果固件版本不同，系统将报告为“冗余已降级”。

待机 CMC 采用与活动 CMC 相同的设置和属性。必须在两个 CMC 上维护相同的固件版本，但不需要在待机 CMC 上复制配置设置。

 **注：**有关安装 CMC 的信息，请参阅 *VRTX 用户手册*。有关在待机 CMC 上安装 CMC 固件的说明，请参阅[更新固件](#)。

CMC 故障保护模式

与冗余 CMC 提供的故障转移保护类似，PowerEdge VRTX 机柜启用故障保护模式以防服务器和 I/O 模块发生故障。故障保护模式在 CMC 没有控制机箱的情况下启用。在 CMC 故障转移期间或在单个 CMC 管理丢失期间：

- 您无法打开新安装服务器的电源。
- 您无法远程访问现有服务器。
- 服务器性能降低以限制功耗，直到 CMC 的管理恢复。

以下是可能导致 CMC 管理丢失的一些情况：

- CMC 移除 - 机箱管理会在更换 CMC 或故障转移至待机 CMC 之后恢复。
- 拔下 CMC 网络电缆或网络连接中断 - 机箱管理在机箱故障转移到待机 CMC 后恢复。网络故障转移只有在冗余 CMC 模式下才能启用。
- CMC 重设 - 机箱管理会在 CMC 重新引导或机箱故障转移至待机 CMC 之后恢复。
- CMC 故障转移命令已发出 - 机箱管理会在机箱故障转移至待机 CMC 之后恢复。

- CMC 固件更新 - 机箱管理会在 CMC 重新引导或机箱故障转移至待机 CMC 之后恢复。建议您首先更新待机 CMC，以便仅发生一次故障转移事件。
- CMC 错误检测和纠正 - 机箱管理会在 CMC 重设或机箱故障转移至待机 CMC 之后恢复。

 **注:** 您可以将机柜配置为使用一个 CMC 或冗余 CMC。在冗余 CMC 配置中，如果主 CMC 与机柜或管理网络失去通信，则待机 CMC 会接替机箱进行管理。

活动 CMC 自举过程

两个 CMC 插槽之间没有任何区别，即插槽不具有优先顺序。而首先安装或启动的 CMC 将担任活动 CMC 角色。如果接通交流电源时已安装了两个 CMC，则安装在 CMC 机箱插槽 1 中的 CMC 通常担任活动角色。活动 CMC 由蓝色 LED 表示。

如果将两个 CMC 插入已经打开电源的机箱，将需要最多两分钟来进行自动的活动/待机协商。协商完成后，将恢复正常的机箱运行。

获得冗余 CMC 的运行状况

可以在 Web 界面中查看待机 CMC 的运行状况。有关在 Web 界面中访问 CMC 运行状况的更多信息，请参阅[查看机箱信息和监测机箱及组件运行状况](#)。

配置前面板

您可以配置以下各项：

- 电源按钮
- LCD
- DVD 驱动器


配置电源按钮

要配置机箱电源按钮，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **前面板** → **设置**。
2. 在**前面板配置**页面的**电源按钮配置**部分下，选择**禁用机箱电源按钮**选项，然后单击**应用**。
机箱电源按钮即被禁用。

配置 LCD

1. 在左侧窗格中，单击**机箱概览** → **前面板** → **设置**。
2. 在**配置**页面的**LCD 配置**部分，执行以下操作：
 - 选择**锁定控制面板 LCD**选项以禁用使用 LCD 界面可执行的任何配置。
 - 从**LCD 语言**下拉菜单中，选择所需的语言。
 - 从**LCD 方向**下拉菜单中，选择所需的模式：**塔模式**或**机架模式**。

 **注:** 使用 LCD 向导配置机箱时，如果选择**将设置自动应用到新插入的服务器**选项，则无法通过使用基本许可证禁用**将设置自动应用到新插入的服务器**功能。如果您不希望该功能生效，请忽略 LCD 上显示的消息（它会自动消失）；或者按 LCD 上的**不接受**按钮，然后按中央按钮。

3. 单击**应用**。

使用 KVM 访问服务器

要通过 KVM 界面将服务器映射到 KVM 并启用到服务器远程控制台的访问，您可以使用 CMC Web 界面、RACADM 或 LCD 界面。

使用 CMC Web 界面将服务器映射到 KVM

确保 KVM 控制台连接到机箱。

要将服务器映射到 KVM，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **前面板** → **设置**。
2. 在**前面板配置**页上的**KVM 配置**部分下，从**KVM 映射**列表中选择必须映射到 KVM 的插槽，然后单击**应用**。

使用 LCD 将服务器映射到 KVM

确保 KVM 控制台连接到机箱。

使用 LCD 将服务器映射到 KVM - 从 LCD 上的**主菜单**屏幕转到**KVM 映射**，选择必须映射的服务器，然后按“确定”。

将服务器映射到 DVD 驱动器

要将服务器映射到机箱 DVD 驱动器，请执行以下操作：


1. 在左侧窗格中，单击**机箱概览** → **前面板** → **设置**。
2. 在**前面板配置**页上的**DVD 驱动器配置**部分：
从**DVD 映射**下拉菜单中选择一个服务器。选择机箱 DVD 驱动器访问所需的服务器。
3. 单击**应用**。

登录 CMC

您可以以 CMC 本地用户、Microsoft Active Directory 用户或 LDAP 用户身份登录 CMC。默认用户名和密码分别是 root 和 calvin。您还可以使用单点登录或智能卡进行登录。


访问 CMC Web 界面

在使用 Web 界面登录 CMC 之前，请确保已配置支持的 Web 浏览器（Internet Explorer 或 Firefox），并且已创建具有所需权限的用户帐户。

 **注:** 如果使用 Microsoft Internet Explorer，请通过代理连接，如果看到 The XML page cannot be displayed 错误，则必须禁用代理才能继续。


要访问 CMC Web 界面，请执行以下操作：

1. 打开您的系统支持的 Web 浏览器。
有关支持的 Web 浏览器的最新信息，请参阅 dell.com/support/manuals 上的 *Dell Systems Software Support Matrix*（Dell 系统软件支持值表）。
2. 在**地址**字段中键入下面的 URL，然后按 <Enter>：
 - 要访问使用 IPv4 地址的 CMC，请输入：`https://<CMC IP address>`
如果默认的 HTTPS 端口号（端口 443）已更改，请键入：`https://<CMC IP address>:<port number>`
 - 要访问使用 IPv6 地址的 CMC，请输入：`https://[<CMC IP address>]`
如果默认的 HTTPS 端口号（端口 443）已更改，请键入：`https://[<CMC IP address>]:<port number>`，其中 *<CMC IP address>* 是 CMC 的 IP 地址，*<port number>* 是 HTTPS 端口号。
此时将显示 **CMC 登录** 页面。

 **注:** 使用 IPv6 时，必须用方括号 ([]) 将 CMC IP 地址括起来。

以本地用户、Active Directory 用户或 LDAP 用户身份登录 CMC

要登录 CMC，您必须具有**登录 CMC** 权限的 CMC 帐户。默认 CMC 用户名是 root，密码是 calvin。root 帐户是随 CMC 一起提供的默认管理帐户。


 **注:** 为增加安全性，强烈建议您在首次设置时更改根帐户的默认密码。

CMC 不支持扩展的 ASCII 字符（如 ß、â、é、ü）或主要在非英语语言中使用的其他字符。


要以本地用户、Active Directory 用户或 LDAP 用户身份登录，请执行以下操作：

1. 在**用户名**字段中，键入您的用户名：

- CMC 用户名：<user name>
- Active Directory 用户名：<domain>\<user name>、<domain>/<user name> 或 <user>@<domain>。
- LDAP 用户名：<user name>

 **注：**此字段区分大小写。

2. 在**密码**字段中，键入用户密码。

 **注：**对于 Active Directory 用户，**用户名**字段区分大小写。

3. 另外，可选择会话超时。这是您在被自动注销前可保持登录状态但不进行任何操作的时段。默认值为 **Web 服务空闲超时**。

4. 单击**确定**。

您便以所需的用户权限登录 CMC。

不能在单个 workstation 上的多个浏览器窗口中使用不同的用户名登录到 Web 界面。

使用智能卡登录 CMC

要使用此功能，必须具有企业版许可证。可以使用智能卡登录 CMC。智能卡提供双重验证 (TFA)，该功能可实现双层安全性：

- 物理智能卡设备。
- 加密代码（例如密码或 PIN）。

用户必须使用智能卡和 PIN 验证其凭据。

 **注：**您不能使用 IP 地址通过智能卡登录来登录 CMC。Kerberos 基于完全限定域名 (FQDN) 验证您的凭据。


使用智能卡以 Active Directory 用户身份登录之前，请确保：

- 将受信任的证书颁发机构 (CA) 证书（证书颁发机构签发的 Active Directory 证书）上载到 CMC。
- 配置 DNS 服务器。
- 启用 Active Directory 登录。
- 启用智能卡登录。

要使用智能卡以 Active Directory 用户身份登录 CMC，请执行以下操作：

1. 使用链接 <https://<cmcname.domain-name>> 登录 CMC。


此时将显示 **CMC 登录** 页面，提示插入智能卡。

 **注：**如果您更改了默认 HTTPS 端口号（端口 80），则使用 <cmcname.domain-name>:<port number> 访问 CMC Web 页面，其中 cmcname 是 CMC 的主机名，domain-name 是域名，port number 是 HTTPS 端口号。

2. 插入智能卡并单击**登录**。

此时将显示 PIN 对话框。


3. 键入 PIN，并单击**提交**。

 **注：**如果 Active Directory 中存在该智能卡用户，则不需要输入 Active Directory 密码。否则，需要使用相应的用户名和密码进行登录。

您已使用 Active Directory 凭据登录到 CMC。

使用单点登录来登录 CMC

在启用单点登录 (SSO) 时，您可以登录到 CMC 而无需提供域用户验证凭据，如用户名和密码。要使用此功能，您必须有企业版许可证。


 **注:** 您不能使用 IP 地址登录 SSO。Kerberos 会根据完全限定域名 (FQDN) 验证您的凭据。

在使用 SSO 登录到 CMC 之前，请确保：

- 您已使用有效的 Active Directory 用户帐户登录到系统。
- 单点登录选项在 Active Directory 配置过程中已启用。

要使用 SSO 登录 CMC，请执行以骤操作：

1. 使用网络帐户登录客户端系统。
2. 通过 `https://<cmcname.domain-name>` 访问 CMC Web 界面
例如，`cmc-6G2WXF1.cmcad.lab`，其中 `cmc-6G2WXF1` 是 `cmcname`，`cmcad.lab` 是 `domain-name`。

 **注:** 如果您更改了默认 HTTPS 端口号（端口 80），则使用 `<cmcname.domain-name>:<port number>` 访问 CMC Web 界面，其中 `cmcname` 是 CMC 的 CMC 主机名，`domain-name` 是域名，`port number` 是 HTTPS 端口号。

CMC 会使用在您使用有效 Active Directory 帐户登录时浏览器高速缓存的 Kerberos 凭据来使您登录。如果登录失败，浏览器将重定向到正常的 CMC 登录页。

 **注:** 如果您不再登录 Active Directory 域并在使用 Internet Explorer 以外的浏览器，则登录将失败，并且浏览器仅显示空白页。

使用串行、Telnet 或 SSH 控制台登录 CMC

可以通过串行、Telnet 或 SSH 连接登录 CMC。

配置完管理站终端仿真软件和受管节点 BIOS 后，执行下列任务以登录到 CMC：

1. 使用管理站终端仿真软件连接到 CMC。
2. 键入 CMC 用户名和密码，然后按 <Enter>。
您即登录到 CMC。

使用 RACADM 访问 CMC

RACADM 提供了一组命令，允许您通过基于文本的界面来配置和管理 CMC。可以使用 Telnet/SSH 或串行连接、KVM 上的 Dell CMC 控制台访问 RACADM，或者通过安装在管理站上的 RACADM 命令行界面从远程访问。

RACADM 界面的分类如下：

- 远程 RACADM - 允许使用 `-r` 选项和 CMC 的 DNS 名称或 IP 地址在管理站上运行 RACADM 命令。
 **注:** 远程 RACADM 包含在 *Dell Systems Management Tools and Documentation DVD* 中，并已安装在管理站上。
- 固件 RACADM - 允许使用 Telnet、SSH 或串行连接登录到 CMC。利用固件 RACADM，可将 RACADM 作为 CMC 固件的一部分实现。

您可以在脚本中使用远程 RACADM 命令来配置多个 CMC。您不能直接在 CMC Web 界面上运行脚本，因为 CMC 不支持该操作。

有关 RACADM 的更多信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

有关配置多个 CMC 的更多信息，请参阅[使用 RACADM 配置多个 CMC](#)。

使用公共密钥验证登录 CMC

您可以通过 SSH 登录 CMC 而无需输入密码。您还可以将单一的 RACADM 命令作为命令行参数发送到 SSH 应用程序。由于该会话在命令完成时结束，因此该命令行选项的行为与远程 RACADM 类似。

在通过 SSH 登录 CMC 之前，确保上载了公共密钥。要使用此功能，您必须具有企业版许可证。

例如：

- **登录：** `ssh service@<domain>` 或 `ssh service@<IP_address>`，其中 `IP_address` 是 CMC IP 地址。
- **发送 RACADM 命令：** `ssh service@<domain> racadm getversion` 和 `ssh service@<domain> racadm getsel`

使用服务帐户登录时，如果在创建公共密钥或私人密钥时设置了密码，可能会提示您再次输入该密码。如果密码与密钥结合使用，运行 Windows 和 Linux 的客户端系统都提供相应方法来自动实现此方法。在运行 Windows 的客户端系统上，您可以使用 Pageant 应用程序。该应用程序在后台运行，使密码的输入变得透明。对于运行 Linux 的客户端系统，您可以使用 ssh 代理。有关如何设置和使用上述任一应用程序的信息，请参阅相应的产品说明文件。

多个 CMC 会话

此表列出了使用各种界面可建立的多个 CMC 会话的情况。

表.3: 多个 CMC 会话

界面	会话数
CMC Web 界面	4
RACADM	4
Telnet	4
SSH	4

更改默认登录密码

在以下情况下，系统会发送警告消息提示您更改默认密码：

- 您以**配置用户**权限登录到 CMC。
- 默认密码警告功能已启用。
- 当前启用的任何帐户的默认用户名和密码都分别是 `root` 和 `calvin`。

如果使用 Active Directory 或 LDAP 登录，会显示同一条警告消息。在确定是否有任何（本地）帐户将 `root` 和 `calvin` 作为凭据时，不考虑 Active Directory 和 LDAP 帐户。在使用 SSH、Telnet、远程 RACADM 或 Web 界面登录 CMC 时，也会显示警告消息。对于 Web 界面、SSH 和 Telnet，会为每个会话显示一条警告消息。对于远程 RACADM，会为每个命令显示警告消息。

要更改凭据，您必须拥有**配置用户**权限。

 **注：**如果在 CMC 登录页面上选中**不再显示该警告**选项，则会生成 CMC 日志消息。


使用 Web 界面更改默认登录密码

当您登录 CMC Web 界面时，如果显示**默认密码警告**页面，您可以更改密码。要更改密码，请执行以下操作：

1. 选择**更改默认密码**选项。
2. 在**新密码**字段中，输入新密码。
密码的最大字符数为 20。字符进行屏蔽处理。支持使用以下字符：

- 0-9
- A-Z
- a-z
- 特殊字符：+、&、?、>、-、}、|、\、!、(、'、\、_、[、"、@、#、)、*、;、\$、]、/、&、%、=、<、:、{、\、\

3. 在**确认密码**字段中，再次输入密码。
4. 单击**继续**。新密码即配置好并且您随后登录到 CMC。

 **注：**只有在**新密码**和**确认密码**字段匹配的情况下才会**继续**。

有关其他字段的信息，请参阅**联机帮助**。

使用 RACADM 更改默认登录密码

要更改密码，请运行以下 RACADM 命令：

```
racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i <index> <newpassword>
```

其中，<index> 是从 1 至 16 的值（代表用户帐户），<password> 是新的用户定义的密码。

有关更多信息，请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

启用或禁用默认密码警告消息

您可以启用或禁用默认密码警告消息的显示。要启用或禁用，您必须拥有**配置用户**权限。

使用 Web 界面启用或禁用默认密码警告消息

要在登录 iDRAC 后启用或禁用默认密码警告消息的显示，请执行以下操作：

1. 转至**机箱控制器** → **用户验证** → **本地用户**。
此时将显示**用户**页面。
2. 在**默认密码警告**部分，选择**启用**，然后单击**应用**以允许在登录到 CMC 时显示**默认密码警告**页面。否则，请选择**禁用**。
或者，如果此功能已启用并且您不希望为后续登录操作显示警告消息，请在**默认密码警告**页面上，选择**不再显示此警告**选项，然后单击**应用**。

使用 RACADM 启用或禁用警告消息以更改默认登录密码

要在使用 RACADM 更改默认登录密码时显示警告消息，使用 `racadm config -g cfgRacTuning -o cfgRacTuneDefCredentialWarningEnable<0> or <1>` 对象。有关更多信息，请参阅 dell.com/support/

manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南)。

更新输入/输出模块基础结构设备固件

通过执行此更新，IOM 模块设备组件的固件被更新，但 IOM 模块设备自身的固件不会被更新；组件是 IOM 模块设备与 CMC 之间的接口电路。组件的更新映像驻留在 CMC 文件系统中，只有当组件与 CMC 上组件映像的当前版本不匹配时，组件才在 CMC Web 界面上显示为可更新设备。

在更新 IOM 模块基础结构设备固件之前，确保 CMC 固件获得更新。

注:

只有当 CMC 检测到 IOM 模块基础结构设备固件 (IOMINF) 相对于 CMC 文件系统中包含的映像已经过时，CMC 才允许更新 IOMINF 固件。如果 IOMINF 固件是最新的，CMC 会阻止 IOMINF 更新。最新的 IOMINF 设备不会列为可更新设备。

使用 CMC Web 界面更新输入/输出模块基础结构设备固件

要在 CMC Web 界面中更新 IOM 模块基础结构设备固件，执行以下操作：

1. 转至 **机箱概览** → **输入/输出模块概览** → **更新**。

随即显示 **IOM 固件和软件** 页。


或者，请转至以下任一页：


- **机箱概览** → **更新**
- **机箱概览** → **机箱控制器** → **更新**

随即显示 **固件更新** 页，该页提供用以访问 **IOM 固件和软件** 页的链接。

2. 在 **IOM 固件和软件** 页，**IOM 固件** 部分，勾选要更新其固件的 IOM 模块的相应 **更新** 列并单击 **应用固件更新**。

在 **更新状态** 部分提供固件更新状态信息。当上传映像文件时，页面上将显示状态指示灯。文件传输时间因连接速度而异。当内部更新进程开始时，将自动刷新页面并显示固件更新计时器。

 **注:** 在文件传输过程中，请勿单击 **刷新** 图标或导航到另一页。

 **注:** 当更新 IOMINF 固件时，不会显示文件传输计时器。

更新完成后，与 IOM 模块设备的连接会短暂丧失，因为该设备会进行重置并且在 **IOM 固件和软件** 页上显示新固件。

使用 RACADM 更新输入/输出模块基础结构设备固件

要使用 RACADM 更新输入/输出模块基础结构设备固件，使用 **fwupdate** 子命令。有关更多信息，请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (适用于 PowerEdge VRTX RACADM 的机箱管理控制器的命令行参考指南)。

更新固件

可以为以下各项更新固件：

- CMC - 活动和待机
- 机箱基础结构
- I/O 模块
- iDRAC7

您可以更新以下服务器组件的固件：

- iDRAC
- BIOS
- Lifecycle Controller
- 32 位诊断程序
- 操作系统驱动程序包
- 网络接口控制器
- RAID 控制器

下载 CMC 固件

在开始固件更新之前，请从 support.dell.com 下载最新的固件版本，然后将其保存到本地系统。

查看当前安装的固件版本

可以使用 CMC Web 界面或 RACADM 查看当前安装的固件版本。

使用 CMC Web 界面查看当前安装的固件版本

在 CMC Web 界面，转至以下任一页查看当前固件版本：

- [机箱概览](#) → [更新](#)
- [机箱概览](#) → [机箱控制器](#) → [更新](#)
- [机箱概览](#) → [服务器概览](#) → [服务器组件更新](#)
- [机箱概览](#) → [I/O 模块概览](#) → [更新](#)
- [机箱概览](#) → [存储](#) → [存储组件更新](#)

固件更新页显示列出的每个组件的当前固件版本，并允许将固件更新到最新版本。

如果机箱中包含 iDRAC 处于恢复模式的早期服务器，或者如果 CMC 检测到 iDRAC 中有损坏的固件，则早期的 iDRAC 也将列在**固件更新**页中。


使用 RACADM 查看当前安装的固件版本

要使用 RACADM 查看 iDRAC 和 CMC 的 IP 信息，以及 CMC 服务或资产标签，请运行 `racadm getsysinfo` 子命令。有关其他 RACADM 命令的更多信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM*

Command Line Reference Guide (Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南)。

更新 CMC 固件

您可以使用 Web 界面或 RACADM 更新 CMC 固件。默认情况下，固件更新会保留当前的 CMC 设置。更新过程中，可以将 CMC 配置设置重设为出厂默认设置。

 **注:** 要更新 CMC 的固件，必须具备机箱配置管理员权限。

如果使用 Web 用户界面会话更新系统组件固件，则**空闲超时 (0、60-10800)** 设置必须设置为较大的值以便满足文件传输时间要求。在某些情况下，固件文件传输时间可能长达 30 分钟。要设置空闲超时值，请参阅[配置服务](#)。

在 CMC 固件更新期间，机箱中部分或全部风扇装置通常会全速旋转。

如果机箱中安装了冗余 CMC，建议通过一个操作同时将两个 CMC 更新到相同的固件版本。如果这两个 CMC 的固件版本不同并发生故障转移，可能会出现意外结果。

固件成功上载后，活动 CMC 将重设并暂时不可用。如果待机 CMC 存在，则待机和活动角色会转换。待机 CMC 成为活动 CMC。如果更新只应用到活动 CMC，则重设完成后，活动 CMC 不运行更新的映像，只有待机 CMC 运行该映像。一般来说，强烈建议为活动和待机 CMC 维护相同的固件版本。

当待机 CMC 更新完毕后，交换 CMC 的角色，使用刚更新的 CMC 作为活动 CMC 并将固件版本较低的 CMC 作为待机 CMC。有关转换角色的信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南) 中的 `cmcchangeover` 命令部分。运行此命令有助于您在更新第二个 CMC 中的固件前验证更新是否成功以及新固件是否正常工作。当两个 CMC 都更新后，可以使用 `cmcchangeover` 命令将 CMC 还原到以前的角色。CMC 固件版本 2.x 更新使用主要 CMC 和冗余 CMC，而不运行 `cmcchangeover` 命令。


为避免重设期间断开其他用户的连接，请通知可能登录到 CMC 的授权用户，并查看会话页中的活动会话。要打开会话页，请单击左侧窗格中的**机箱概览**，单击**网络**，然后单击**会话**。

当从 CMC 或向 CMC 传输文件时，文件传输图标将在传输期间旋转。如果该图标不显示动画，请确保浏览器配置为允许动画。有关在浏览器中允许播放动画的更多信息，请参阅[允许在 Internet Explorer 中播放动画](#)。

使用 RACADM 更新 CMC 固件

要使用 RACADM 更新 CMC 固件，请使用 `fwupdate` 子命令。有关 RACADM 命令的更多信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南)。


使用 Web 界面更新 CMC 固件

 **注:** 在更新 CMC 固件之前，请确保打开了机箱电源，但关闭了机箱中的所有服务器。

要使用 CMC Web 界面更新 CMC 固件，请执行以下操作：


1. 在左侧窗格中，转至下列任意页面：
 - **机箱概览** → **更新**
 - **机箱概览** → **机箱控制器** → **更新**
2. 在**固件更新**页的**CMC 固件**部分，在**更新目标**列下为要更新的一个 CMC 或多个（如果存在待机 CMC）选择所需的组件，然后单击**应用 CMC 更新**。
3. 在**固件映像**字段中，输入固件映像文件在管理站或共享网络中的路径，或者单击**浏览**以浏览到该文件位置。CMC 固件映像文件的默认名称是 `vrtx_cmc.bin`。

- 单击**开始固件更新**，然后单击**是**。**固件更新过程**部分提供固件更新状态信息。当上载映像文件时，页面上将显示状态指示灯。文件传输时间因连接速度而异。当内部更新过程开始时，页面将自动刷新并显示固件更新计时器。
- 对于待机 CMC，当完成更新时，**更新状态**字段将显示**完成**。对于活动 CMC，在固件更新过程的最后阶段，浏览器会话和与 CMC 的连接将在活动 CMC 断开网络连接时暂时丢失。您必须在几分钟后等活动 CMC 重新启动时再次登录。重设 CMC 后，新固件将显示在**固件更新**页上。

 **注:** 固件更新后，从 Web 浏览器高速缓存中删除文件。有关清除浏览器高速缓存的说明，请参阅 Web 浏览器的联机帮助。


附加说明：

- 在文件传输期间，不要单击**刷新**图标或者导致到其他页面。
- 要取消该进程，请选择**取消文件传输和更新**选项。该选项仅在文件传输过程中可用。
- 更新状态**字段显示固件更新状态。

 **注:** CMC 的更新过程可能需要几分钟时间。

更新机箱基础结构固件

机箱基础结构更新操作可更新主板和 PCIe 子系统管理固件等组件。

 **注:** 要更新机箱基础结构固件，请确保机箱已打开电源并且服务器已关机。

使用 CMC Web 界面更新机箱基础结构固件

- 转至以下任一页：
 - 机箱概览** → **更新**。
 - 机箱概览** → **机箱控制器** → **更新**。
- 在**固件更新**页上**机箱基础结构固件**部分的**更新目标**列中，选择该选项，然后单击**应用机箱基础结构固件**。
- 在**固件更新**页上，单击**浏览**，然后选择适当的机箱基础结构固件。
- 单击**开始固件更新**，然后单击**是**。

固件更新进度部分提供固件更新状态信息。在上载映像文件时，页面上将显示状态指示灯。文件传输时间取决于连接速度。当内部更新过程开始时，页面会自动刷新，并显示固件更新计时器。

要遵循的其他说明：

- 在文件传输过程中，请勿单击**刷新**图标或导航到另一页。
- 更新状态**字段显示固件更新状态。

更新完成后，与主板的连接会短暂丧失，因为该设备会进行重设并且在**固件更新**页上显示新固件。

使用 RACADM 更新机箱基础结构固件


要使用 RACADM 更新机箱基础结构固件，请使用 `fwupdate` 子命令。有关使用 RACADM 命令的更多信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

更新服务器 iDRAC 固件

您可以更新 iDRAC7 或更高版本的固件。要使用此功能，必须具有企业版许可证。

对于带有 iDRAC 的服务器，iDRAC 固件版本必须为 1.40.40 或更高版本。

更新固件后，iDRAC（服务器上）将重设并暂时不可用。

 **注:**要更新 iDRAC 固件，CMC 必须具有 SD 卡。

使用 Web 界面更新服务器 iDRAC 固件

要更新服务器中的 iDRAC 固件，请执行以下操作：


1. 转至以下任一页：
 - 机箱概览 → 更新。
 - 机箱概览 → 机箱控制器 → 更新。
 - 机箱概览 → I/O 模块概览 → 更新。

此时将显示**固件更新**页面。

 **注:**

您还可以使用**机箱概览** → **服务器概览** → **更新**来更新服务器 iDRAC 固件。有关更多信息，请参阅[更新服务器组件固件](#)。

2. 要更新 iDRAC7 固件，请在 **iDRAC7 固件** 部分，单击要更新其固件的服务器对应的**更新**链接。
此时将显示**服务器组件更新**页面。要继续，请参阅[更新服务器组件固件](#)。
3. 在**固件映像**字段中，输入管理站或共享网络上固件映像文件的路径，或单击**浏览**导航到文件位置。默认 iDRAC 固件映像名称为 **firring.imc**。
4. 单击**开始固件更新**，然后单击**是**。
固件更新进度部分提供固件更新状态信息。进度条会指示上载过程的状态。文件传输时间取决于连接速度。当内部更新过程开始时，页面会自动刷新，并显示固件更新计时器。

 **注:**要遵循的其他说明：

- 在文件传输过程中，请勿单击**刷新**图标或导航到另一页。
- 要取消该过程，请单击**取消文件传输和更新**。该选项仅在文件传输过程中可用。
- **更新状态**字段显示固件更新状态。

更新 iDRAC 固件最多需要十分钟。

使用 RACADM 更新服务器 iDRAC 固件


可通过运行 `fwupdate` 命令更新 iDRAC7 的固件。要执行此操作，必须具有企业版许可证。iDRAC7 版本必须为 1.40.40 或更高版本。有关该命令的更多信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

更新服务器组件固件

Lifecycle Controller 服务在每台服务器上提供，并且因 iDRAC 变得更简便。您可以使用 Lifecycle Controller 服务管理服务器上的组件和设备的固件。Lifecycle Controller 使用优化算法来更新固件，可有效减少重新启动次数。

Dell Update Package (DUP) 用于使用 Lifecycle Controller 执行固件更新。操作系统驱动程序包组件 DUP 超出此限制，并且必须使用扩展存储功能单独更新。

Lifecycle Controller 为 iDRAC6 和更新的服务器提供模块更新支持。iDRAC 固件必须为版本 2.3 或更高，才能使用 Lifecycle Controller 更新固件。

 **注:** 使用基于 Lifecycle Controller 的更新功能之前，必须更新服务器固件版本。在更新服务器组件固件模块之前，还必须更新 CMC 固件。

始终采用以下顺序更新服务器组件固件模块：

- BIOS
- Lifecycle Controller
- iDRAC

要使用 CMC Web 界面更新服务器组件固件，请单击 **机箱概览** → **服务器概览** → **更新** → **服务器组件更新**。

如果服务器不支持 Lifecycle Controller 服务，则**组件/设备固件资源清册**部分显示**不支持**。对于最新一代的服务器，请安装 Lifecycle Controller 固件并更新 iDRAC 固件，以在服务器上启用 Lifecycle Controller 服务。对于旧版服务器，此升级不可行。

通常，Lifecycle Controller 固件通过在服务器操作系统上执行的相应安装包进行安装。对于支持的服务器，可以使用文件扩展名为 **.usc** 的特殊修复或安装包。该文件使您可以通过本机 iDRAC Web 浏览器界面上提供的固件更新工具安装 Lifecycle Controller 固件。

您还可以通过在服务器操作系统上执行的相应安装软件包安装 Lifecycle Controller 固件。有关更多信息，请参阅 *Dell Lifecycle Controller User's Guide*（Dell Lifecycle Controller 用户指南）。

如果服务器上禁用了 Lifecycle Controller 服务，将显示**组件/设备固件资源清册**部分。

Lifecycle Controller may not be enabled.

启用 Lifecycle Controller

在打开服务器电源时，您可以启用 Lifecycle Controller 服务：

- 对于 iDRAC6 服务器，当显示以下消息时，在引导控制台上按 <CTRL><E>。
Press <CTRL-E> for Remote Access Setup within 5 sec.
。然后，在设置屏幕上单击**系统服务**。转到**系统设置主菜单**页并单击**完成**以保存设置。
- 对于 iDRAC7 服务器，在引导控制台中，按 <F2> 键访问**系统设置**。
- 在**系统设置主菜单**页上，转到 **iDRAC 设置** → **Lifecycle Controller**，单击**已启用**。转到**系统设置主菜单**页，并单击**完成**以保存设置。

“取消系统服务”可用于取消挂起的所有计划作业并将其从队列中移除。

有关 Lifecycle Controller 和支持的服务器组件以及设备固件管理的更多信息，请参阅：

- *Lifecycle Controller 远程服务快速入门指南*。
- delltechcenter.com/page/Lifecycle+Controller。


服务器组件更新页可以更新服务器上的各种固件组件。要使用此页面上的特性和功能，您必须拥有以下权限：

- 对于 CMC：**服务器管理员**权限。
- 对于 iDRAC：**配置 iDRAC** 权限和**登录到 iDRAC** 权限。

如果权限不足，则只能查看服务器上组件和设备的固件资源清册。您无法为服务器上任何类型的 Lifecycle Controller 操作选择任何组件或设备。


筛选进行固件更新的组件

可同时检索所有服务器上所有组件和设备的相关信息。为了管理这些数量庞大的信息，Lifecycle Controller 提供了各种筛选机制。

 **注:** 要使用此功能, 必须具有企业版许可证。

这些筛选器支持:

- 选择一个或多个组件或设备类别以便于查看。
- 对服务器的组件和设备的固件版本进行比较。
- 基于类型或型号缩小特定组件或设备类别的范围, 从而自动筛选所选组件和设备。

 **注:** 自动筛选功能在使用 Dell Update Package (DUP) 时非常重要。DUP 的更新编程可基于组件或设备的类型或型号。自动筛选行为旨在将进行初始选择后的后续选择决策减至最少。

以下是应用筛选机制的一些示例:

- 如果选定 BIOS 筛选器, 则只显示所有服务器的 BIOS 资源清册。如果服务器组包含许多服务器型号, 并且选定一台服务器用于 BIOS 更新, 则自动筛选逻辑会自动删除不匹配所选服务器型号的所有其他服务器。这将确保选择的 BIOS 固件更新映像 (DUP) 与正确的服务器型号兼容。
有时, BIOS 固件更新映像可能会与多个服务器型号兼容。此类优化将被忽略, 以防此兼容性在将来不再有效。
- 自动筛选对于网络接口控制器 (NIC) 和 RAID 控制器的固件更新非常重要。这些设备类别包含不同的类型和型号。同样, 固件更新映像 (DUP) 可能以优化形式提供, 即单个 DUP 设计为可以更新指定类别的多种设备类型或型号。

使用 CMC Web 界面筛选进行固件更新的组件

要筛选设备, 请执行以下操作:

1. 在左侧窗格中, 转至**服务器概览**, 然后单击**更新**。
2. 在**服务器组件更新**页面的**组件/设备更新筛选器**部分, 选择以下一项或多项:
 - BIOS
 - iDRAC
 - Lifecycle Controller
 - 32 位诊断程序
 - 操作系统驱动程序包
 - 网络 I/F 控制器
 - RAID 控制器

固件资源清册部分只显示机箱中存在的所有服务器的相关组件或设备。从下拉菜单中选择一项后, 列表中只显示与该项相关联的组件或设备。

筛选的组件和设备组在资源清册部分中显示后, 选择进行更新的组件或设备时, 可进行进一步筛选。例如, 如果选定 BIOS 筛选器, 则资源清册部分仅显示所有服务器及其 BIOS 组件。如果选定其中一台服务器上的 BIOS 组件, 则资源清册会进一步筛选以显示匹配选定服务器型号名称的服务器。

如果没有选择任何筛选器并在资源清册部分选择了要更新的组件或设备, 将自动启用与该选择关联的筛选器。可以进行进一步筛选, 即资源清册部分显示在型号、类型或某种标识方面与所选组件相匹配的所有服务器。例如, 如果选择更新其中一台服务器上的 BIOS 组件, 则筛选器自动设置为 BIOS, 并且资源清册部分显示与所选服务器的型号名称相匹配的服务器。

使用 RACADM 筛选进行固件更新的组件


要使用 RACADM 筛选进行固件更新的组件, 请使用 **getversion** 命令:

```
racadm getversion -l [-m <module>] [-f <filter>]
```

有关更多信息，请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

查看固件资源清册

您可以查看机箱中当前存在的所有服务器的所有组件和设备的固件版本摘要及其状态。

 **注:** 要使用此功能，必须具有企业版许可证。

使用 CMC Web 界面查看固件资源清册

要查看固件资源清册，请执行以下操作：

1. 在左侧窗格中，单击**服务器概览**，然后单击**更新**。
2. 在**服务器组件更新**页面的**组件/设备固件资源清册**部分，查看固件资源清册详情。在此页面中，可以查看以下信息：
 - 当前不支持 Lifecycle Controller 服务的服务器列为**不支持**。所提供的超链接可以导航到替代页，在此可以直接只更新 iDRAC 固件。此页面仅支持 iDRAC 固件更新，而不支持对服务器上的任何其他组件和设备进行更新。iDRAC 固件更新不依赖于 Lifecycle Controller 服务。
 - 如果服务器列为**尚未就绪**，则表示在检索固件资源清册时，服务器上的 iDRAC 仍然在初始化。请稍待片刻，让 iDRAC 充分运行，然后刷新页面以重新检索固件资源清册。
 - 如果组件和设备的资源清册没有反映服务器上实际安装的内容，则必须在服务器引导过程中调用 Lifecycle Controller。这可以帮助刷新内部组件和设备信息，并允许验证当前安装的组件和设备。符合以下条件时会出现这种情况：
 - * 更新服务器 iDRAC 固件以将 Lifecycle Controller 功能新引入至服务器管理。
 - * 新设备被插入服务器。

为自动执行此操作，iDRAC 设置公用程序（适用于 iDRAC7）提供可通过引导控制台访问的选项：

1. 对于 iDRAC7 服务器，在引导控制台中，按 <F2> 访问**系统设置**。
 2. 在**系统设置主菜单**页面中，单击 **iDRAC 设置** → **重新启动时收集系统资源清册**，选择**已启用**，返回**系统设置主菜单**页面，然后单击**完成**保存设置。
- 执行各种 Lifecycle Controller 操作（例如，“更新”、“回滚”、“重新安装”和“作业删除”）的选项均可用。一次只能执行一种类型的操作。不支持的组件和设备可能会作为资源清册的一部分列出，但不允许 Lifecycle Controller 操作。

下表显示服务器上的组件和设备信息：

表. 4: 组件和设备信息

字段	说明
插槽	显示机箱中服务器占用的插槽。插槽编号是顺序 ID，从 1 到 4（用于机箱中的 4 个可用插槽），它有助于识别服务器在机箱中的位置。如果占用插槽的服务器少于 4 个，则仅显示插有服务器的插槽。
名称	显示每个插槽中的服务器名称。
型号	显示服务器的型号。
组件/设备	显示服务器上组件或设备的说明。如果列宽过窄，鼠标悬停触发工具会提供说明视图。
当前版本	显示服务器上组件或设备的当前版本。
回滚版本	显示服务器上组件或设备的回滚版本。
作业状态	显示服务器上计划的任何操作的作业状态。作业状态会持续动态更新。如果作业完成并检测到状态为“已完成”，则服务器上的任何组件或设备的固件版本发生更改时，会自动刷新组件和设备的固件版本。当前状态旁还会显示信息图标，提供关于当前作业状态的附加信息。可通过单击或将鼠标悬停在图标上来查看此信息。
更新	单击可选择服务器上进行固件更新的组件或设备。


使用 RACADM 查看固件资源清册

要使用 RACADM 查看固件资源清册，请使用 `getversion` 命令：

```
racadm getversion -l [-m <module>] [-f <filter>]
```

有关更多信息，请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

Lifecycle Controller 作业操作

 **注：**要使用此功能，必须具有企业版许可证。

您可以执行 Lifecycle Controller 操作，例如：

- 重新安装
- 回滚
- 更新
- 删除作业

一次只能执行一种类型的操作。不支持的组件和设备可能会作为资源清册的一部分列出，但不允许 Lifecycle Controller 操作。

要执行 Lifecycle Controller 操作，您必须具有：

- 对于 CMC：服务器管理员权限。
- 对于 iDRAC：配置 iDRAC 权限和登录到 iDRAC 权限。

Lifecycle Controller 操作在服务器上计划后，可能需要 10 到 15 分钟才能完成。该过程涉及服务器的几次重新引导，在此期间将执行固件安装，还包括固件验证阶段。您可以使用服务器控制台查看此过程的进度。如果服务器上有多个组件或设备需要更新，您可以将所有更新整合为一个计划的操作，从而将所需的重新引导次数减至最少。

有时，当某项操作正提交并计划通过另一个会话或上下文完成时，会尝试进行另一项操作。在这种情况下，将显示确认消息，指出这种情况并且禁止提交该操作。等待正在进行的操作完成，然后再次提交该操作。

不要在已提交操作进行计划之后离开页面。如果尝试离开，将显示确认消息，允许取消离开页面的尝试。否则，操作将被中断。中断（尤其是在更新操作中）可能会导致固件映像文件上传操作在正确完成之前终止。提交操作进行计划之后，请确保确认表明操作已成功计划的确认消息。

重新安装服务器组件固件

您可以在一个或多个服务器上为所选的组件或设备重新安装当前已安装固件的固件映像。固件映像可在 Lifecycle Controller 中获得。

使用 Web 界面重新安装服务器组件固件


要重新安装服务器组件固件，请执行以下操作：

1. 在左侧窗格中，单击**服务器概览** → **更新**。
2. 在**服务器组件更新**页面中，筛选组件或设备（可选）。
3. 在**当前版本**列中，选择您要重新安装固件的组件或设备对应的选项。

4. 选择以下选项之一：
 - **立即重新引导** - 立即重新启动服务器。
 - **下一次重新引导时** - 稍后手动重新启动服务器。
5. 单击**重新安装**。将为所选组件或设备重新安装固件版本。

回滚服务器组件固件

您可以在一个或多个服务器上为所选的组件或设备安装以前已安装的固件的固件映像。固件映像可在回滚操作的 Lifecycle Controller 中获得。可用性受 Lifecycle Controller 的版本兼容性逻辑影响。它还假定 Lifecycle Controller 为以前的更新提供便利。

 **注:** 要使用此功能，必须具有企业版许可证。


使用 CMC Web 界面回滚服务器组件固件

要将服务器组件固件版本回滚到较早的版本，请执行以下操作：

1. 在左侧窗格中，单击**服务器概览**→ **更新**。
2. 在**服务器组件更新**页面中，筛选组件或设备（可选）。
3. 在**回滚版本**列中，选择您要为其回滚固件的组件或设备对应的选项。
4. 选择以下选项之一：
 - **立即重新引导** - 立即重新启动服务器。
 - **下一次重新引导时** - 稍后手动重新启动服务器。
5. 单击**回滚**。为所选组件或设备重新安装以前安装的固件版本。

升级服务器组件固件

您可以在一个或多个服务器上为所选的组件或设备安装下一个版本的固件映像。在 Lifecycle Controller 中提供了固件映像，以用于回滚操作。要使用此功能，必须具有企业版许可证。

 **注:** 对于 iDRAC 和操作系统驱动程序包固件更新，请确保已启用**扩展存储**功能。

建议在初始化服务器组件固件更新之前清除作业队列。在 **Lifecycle Controller 作业**页面上提供了服务器上所有作业列表。此页面允许删除单个或多个作业，或者清除服务器上的所有作业。

BIOS 更新特定于服务器的型号。有时，即使选择更新服务器上的单个网络接口控制器 (NIC) 设备的固件，更新也可能应用到该服务器上的所有 NIC 设备。这是 Lifecycle Controller 功能的固有行为，尤其是编程采用 Dell Update Package (DUP) 时。目前支持小于 48MB 的 Dell Update Package (DUP)。


如果更新文件映像的体积过大，则作业状态会指示下载失败。如果在服务器上尝试更新多个服务器组件，则所有固件更新文件的总大小也可能超过 48 MB。在这种情况下，更新文件被截断的某个组件更新会失败。要更新服务器上的多个组件，建议首先一起更新 Lifecycle Controller 和 32 位诊断程序组件。这些操作不需要重新引导服务器，而且完成速度相对较快。完成后可以一起更新其他组件。

通常，所有 Lifecycle Controller 更新都计划立即执行。不过，系统服务可延迟一段时间再执行更新。在这种情况下，会由于通过 CMC 托管的远程共享不再可用而导致更新失败。

使用 CMC Web 界面升级服务器组件固件


要将固件版本升级到下一版本，请执行以下操作：

1. 在左侧窗格中，单击**服务器概览**，然后单击**更新**。
2. 在**服务器组件更新**页面中，筛选组件或设备（可选）。
3. 在**更新**列中，选择要将其固件更新到下一个版本的组件或设备对应的选项。


 **注：**使用 <Ctrl> 键选择要在所有适用服务器上更新的组件或设备类型。按住 <Ctrl> 键以黄色高亮显示所有组件。按住 <Ctrl> 键的同时，通过选择**更新**列中的关联选项来选择所需的组件或设备。

此时将显示另一个表，其中列出所选类型的组件或设备，以及固件映像文件的选择器。对于每种类型的组件，会显示一个固件映像文件选择器。

网络接口控制器 (NIC) 和 RAID 控制器等少数设备包含许多类型和型号。更新选择逻辑会基于初始选定的设备自动筛选相关设备类型或型号。此自动筛选行为的主要理由是只能为该类别指定一个固件映像文件。


 **注：**如果已安装并启用扩展存储功能，则单个 DUP 或组合 DUP 的更新大小限制可忽略。有关启用扩展存储的信息，请参阅[配置 CMC 扩展存储卡](#)。

4. 为所选的组件或设备指定固件映像文件。这是一个适用于 Microsoft Windows 的 Dell Update Package (DUP) 文件。
5. 选择以下选项之一：
 - **立即重新引导** - 立即重新启动服务器。
 - **下一次重新引导时** - 稍后手动重新启动服务器。

 **注：**此任务对 Lifecycle Controller 和 32 位诊断程序固件更新无效。对这些设备会立即执行服务器重新启动操作。

6. 单击**更新**。系统会对所选的组件或设备更新固件版本。

删除计划的服务器组件固件作业

 **注：**要使用此功能，必须具有企业版许可证。

您可以删除为一个或多个服务器上所选组件和/或设备计划的作业。

使用 Web 界面删除计划的服务器组件固件作业

要删除计划的服务器组件固件作业，请执行以下操作：

1. 在左侧窗格中，单击**服务器概览**，然后单击**更新**。
2. 在**服务器组件更新**页面中，筛选组件或设备（可选）。
3. 在**作业状态**列中，如果作业状态旁边显示复选框，则表示 Lifecycle Controller 作业正在进行并且当前处于所指示的状态。可选择该作业进行作业删除操作。
4. 单击**删除作业**。将删除所选组件或设备的作业。

使用 CMC Web 界面更新存储组件

确保已下载所需存储组件的 DUP。

要更新存储组件，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **存储** → **更新**。
2. 在**存储组件更新**页面中，单击**浏览**，选择先前下载的 DUP，然后单击**上载**。
该 DUP 被上载到 CMC，并显示**固件更新状态**页面，其中包含以下信息：
 - 所耗时间
 - 目标组件
 - 当前固件版本
 - 更新状态

使用 CMC 恢复 iDRAC 固件

iDRAC 固件通常使用 iDRAC 界面更新，如 iDRAC Web 界面、SM-CLP 命令行界面或从 support.dell.com 下载的特
定操作系统更新软件包。有关更多信息，请参阅 *iDRAC User's Guide*（iDRAC 用户指南）。

较早几代的服务器可能包含使用最新 iDRAC 固件更新进程恢复的损坏固件。CMC 检测到损坏的 iDRAC 固件
时，将在**固件更新**页上列出服务器。请完成[更新服务器 iDRAC 固件](#)中所述的任务。

查看机箱信息和监测机箱与组件运行状况

您可以查看信息并监测以下各项的运行状况：

- 活动和待机 CMC
- 所有服务器和单个服务器
- IO 模块
- 风扇
- 电源设备 (PSU)
- 温度传感器
- 硬盘驱动器
- LCD 部件
- 存储控制器
- PCIe 设备

查看机箱和组件摘要

在登录 CMC Web 界面后，**机箱运行状况**页面会显示机箱及其组件的运行状况。该页面会显示机箱及其组件的图形视图。该视图动态更新，而且组件子图形覆盖标记和文本提示会自动更改以反映当前状态。



要查看机箱运行状况，请单击**机箱概览**。系统会显示机箱、活动和待机 CMC、服务器模块、IO 模块 (IOM)、风扇、鼓风机、电源设备装置 (PSU)、LCD 部件、存储控制器和 PCIe 设备的整体运行状况。单击每个组件可显示该组件的详情。此外，还会显示 CMC 硬件日志中的最新事件。有关更多信息，请参阅[联机帮助](#)。






如果将您的机箱配置为组主机箱，则在登录后显示**组运行状况**页面。该页面显示机箱级信息和警报。将显示所有活动、严重和非严重警报。

机箱图形

机箱分前后视图展示（分别为上图和下图）。服务器、DVD、HDD、KVM 和 LCD 在前视图中显示，其余组件在后视图中显示。选中组件显示为蓝色，并且单击所需组件的图像可进行相应控制。机箱中存在组件时，该组件

类型的图标在组件安装位置（插槽）的图形中显示。空位置显示为炭灰色背景。组件图标可指示组件的状态。其他组件显示图标代表具体组件。将光标悬停在组件上方将显示一个工具提示和有关该组件的附加信息。

表. 5: 服务器图标状态

图标	说明
	服务器存在、处于开启状态并正常工作。
	服务器存在但关闭。
	服务器存在，但报告一个非严重错误。
	服务器存在，但报告一个严重错误。
	服务器不存在。

所选组件信息

所选组件的信息在三个独立的部分中显示：

- 运行状况、性能和属性 - 显示硬件日志所示的活动严重和非严重事件以及随时间变化的性能数据。
- 属性 - 显示不会随时间变化或很少发生更改的组件属性。
- 快速链接 - 提供导航至常用页面以及常用操作的链接。只有适用于所选组件的链接才会在此部分显示。

查看服务器型号名称和服务标签

通过以下步骤可及时获得每台服务器的型号名称和服务标签：

1. 在左侧窗格中，单击**服务器概览**。所有服务器（SLOT-01 到 SLOT-04）将显示在服务器列表中。如果插槽中不存在服务器，则图形中相应的图像将以灰色显示。

2. 将光标悬停在服务器的插槽名称或插槽编号上，工具提示会显示服务器的型号名称和服务标签（如果可用）。

查看机箱摘要

要查看机箱摘要信息，请在左侧窗格中单击**机箱概览** → **属性** → **摘要**。
此时将显示**机箱摘要**页面。有关此页面的更多信息，请参阅**联机帮助**。

查看机箱控制器信息和状态

要查看机箱控制器的信息和状态，请在 CMC Web 界面中单击**机箱概览** → **机箱控制器**。
此时将显示**机箱控制器状态**页面。有关更多信息，请参阅**联机帮助**。

查看所有服务器的信息和运行状况

要查看所有服务器的运行状况，请执行以下任一操作：

- 单击**机箱概览**。**机箱运行状况**页面显示机箱中安装的所有服务器的图形概览。服务器运行状况由服务器子图形的覆盖标记指示。有关机箱运行状况的更多信息，请参阅**联机帮助**。
- 单击**机箱概览** → **服务器概览**。**服务器状态**页面提供机箱中的服务器概览。有关更多信息，请参阅**联机帮助**。

查看单个服务器的运行状况和信息

若要查看单个服务器的运行状况，请执行以下任一操作：

1. 转至**机箱概览** → **属性** → **运行状况**。

机箱运行状况页显示机箱中安装的所有服务器的图形概览。服务器运行状况由服务器子图形的覆盖标记指示。将光标移动到单个服务器子图形的上方。所显示的相应文本提示或屏幕提示提供该服务器的附加信息。单击服务器子图形可在右侧查看输入/输出模块信息。有关更多信息，请参阅**联机帮助**。

2. 在左侧窗格中，转至**机箱概述**并展开**服务器概述**。展开的列表中显示所有服务器 (1 - 4)。单击要查看的服务器（插槽）。

服务器状态页（与**服务器状态**页不同）提供该机箱中服务器的运行状况及 iDRAC Web 界面的启动点，即用于管理该服务器的固件。有关更多信息，请参阅**联机帮助**。

 **注：**要使用 iDRAC Web 界面，您必须拥有 iDRAC 用户名和密码。有关 iDRAC 和使用 iDRAC Web 界面的更多信息，请参阅 *Integrated Dell Remote Access Controller User's Guide*（Integrated Dell Remote Access Controller 用户指南）。

查看 IOM 的信息和运行状况

要在 CMC Web 界面中查看 IOM 的运行状况，请执行以下任一操作：

1. 单击**机箱概览**。

将显示**机箱运行状况**页。左侧窗格中的图形显示机箱的前视图、后视图和侧视图，并包含 IOM 的运行状况。IOM 运行状况由 IOM 子图形的重叠标记表示。将光标移到各个 IOM 子图形上方，文本提示将提供有关该 IOM 的附加信息。单击 IOM 子图形可在右窗格中查看 IOM 信息。

2. 转到**机箱概览** → **I/O 模块概览**。

I/O 模块状态页提供与机箱关联的 IOM 的概览。有关更多信息，请参阅**联机帮助**。

查看单个输入/输出模块的信息和运行状况

要查看单个输入/输出模块的运行状况，在 CMC Web 界面中，执行以下任一操作：

1. 转至**机箱概览** → **属性** → **运行状况**。

机箱运行状况页面出现。“机箱图形”的下半部分显示机箱的后视图并包含输入/输出模块的运行状况。输入/输出模块的运行状况由输入/输出模块子图形的覆盖标记指示。将光标移动到单个输入/输出模块子图形的上方。所显示的文本提示提供该输入/输出模块的附加信息。单击该输入/输出模块子图形可在右侧查看输入/输出模块信息。

2. 在系统树中转至**机箱概览**并展开输入/输出**模块概览**。展开的列表中显示所有输入/输出模块（1-6）。单击要查看的输入/输出模块。


此时将显示特定于该输入/输出模块的输入/输出**模块状态页**（与整体输入/输出**模块状态页**不同）。有关更多信息，请参阅**联机帮助**。

查看风扇的信息和运行状况

CMC 可根据系统事件来增减风扇速度，从而控制机箱风扇的速度。您可以以三种模式运行风扇：如低、中、高。有关配置风扇的更多信息，请参阅**联机帮助**。

要通过使用 RACADM 命令设置风扇的属性，请在 CLI 界面键入以下命令：


```
racadm fanoffset [-s <off|low|medium|high>]
```

 **注:** CMC 监测机箱中的温度传感器，并根据需要自动调整风扇速度。不过，您可以通过 `racadm fanoffset` 命令覆盖以维护最低风扇速度。在使用此命令覆盖时，CMC 将始终按选定的速度运行风扇，即使机箱风扇不需要按该速度运行。

有关 RACADM 命令的更多信息，请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

当发生以下事件时，CMC 生成警报并提高风扇速度：

- 超过 CMC 环境温度阈值。
- 风扇停止转动。
- 从机箱中卸下了一个风扇。

 **注:** 在服务器上的 CMC 或 iDRAC 固件更新期间，机箱中的部分或全部风扇装置会全速旋转。这是正常现象。

要在 CMC Web 界面中查看风扇的运行状况，请执行以下任一操作：

1. 转到**机箱概览**。

将显示**机箱运行状况**页。机箱图形的下半部分提供机箱的左视图并包含风扇的运行状况。风扇运行状况由风扇子图形的重叠标记表示。将光标移到风扇子图形上方，文本提示将提供有关风扇的附加信息。单击风扇子图形可在右窗格中查看风扇信息。

2. 转到**机箱概览** → **风扇**。

风扇状态页提供机箱中风扇的状态和速度测量值（以每分钟转数 (RPM) 为单位）和阈值。可以有一个或多个风扇。



注：在 CMC 和风扇装置间发生通信故障时，CMC 将无法获取或显示风扇装置的运行状况。



注：当两个风扇都不在插槽中或者一个风扇低速旋转时，将显示以下消息：

Fan <number> is less than the lower critical threshold.

有关更多信息，请参阅**联机帮助**。

配置风扇

风扇偏移 - 一种向机箱的存储和 PCIe 区域提供增强冷却效果的功能。使用此功能可以增加向 HDD、共享 PERC 控制器和 PCIe 卡插槽的气流输送。例如，在使用比平时需要更大冷却量的大功率或自定义 PCIe 卡时，就需要用到“风扇偏移”。“风扇偏移”功能有“关”、“低”、“中”和“高”选项。“低”、“中”和“高”设置分别对应于最高风扇速度偏移（增加）20%、50% 和 100%。每个选项还有最低速度设置，“低”、“中”和“高”分别对应于最低风扇速度偏移（增加）35%、65% 和 100%。

例如，将风扇偏移设置为“中”，风扇 1 - 6 的转速将比最高速度增加 50%。这一增加值是指高出系统已经基于安装的硬件配置而设置的冷却速度。

在启用“风扇偏移”的任一选项时，功耗都会增加。设置“低”偏移时，系统响声会加大，设置“中”偏移时，系统响声会明显加大，设置“高”偏移时，系统响声会显著加大。未启用“风扇偏移”选项时，风扇速度将降低到系统冷却安装的硬件配置所需的默认速度。

要设置偏移功能，请转到**机箱概览** → **风扇** → **设置**。在**高级风扇配置**页上，从与**风扇偏移**对应的值下拉菜单中进行适当选择。

有关“风扇偏移”功能的更多信息，请参阅**联机帮助**。

要通过使用 RACADM 命令设置这些功能，请使用以下命令：

```
racadm fanoffset [-s <off|low|medium|high>]
```

有关与风扇偏移相关的 RACADM 命令的更多信息，请参阅 dell.com/support/Manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

增强的冷却模式 (ECM) - 是 CMC 中的一项功能，能够提高 PowerEdge VRTX 机箱中安装的服务器的冷却能力。例如，在高温环境中或者使用安装了大功率（≥120W）CPU 的服务器时，就需要使用 ECM。该模式通过让四个机箱鼓风机模块以较高的速度运行来获得增强的冷却能力。因此，在启用 ECM 时，系统功耗和噪声级别可能会增加。

启用后，ECM 将只能增强机箱内服务器插槽的冷却能力。务必还要注意，ECM 并未设计为始终为这些服务器提供增强的冷却能力。即使启用 ECM，只能在需要增强冷却能力时才会看到鼓风机速度提高。这种情况的示例包括服务器利用率高/繁忙和高温环境。

默认情况下，ECM 处于关闭状态。当启用 ECM 时，鼓风机能够为每个刀片增加大约 20% 的气流量。

要设置 ECM 模式，请转到**机箱概览** → **风扇** → **设置**。在**高级风扇配置**页上，从与**增强的冷却模式**对应的值下拉菜单中进行适当选择。

有关 ECM 功能的更多信息，请参阅**联机帮助**。

查看前面板属性

要查看前面板属性，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **前面板**。
2. 在**属性**页上，您可以查看以下信息：
 - 电源按钮属性
 - LCD 属性
 - KVM 属性
 - DVD 驱动器属性

查看 KVM 信息和运行状况

要查看与机箱关联的 KVM 的运行状况，请执行以下任一操作：

1. 单击**机箱概览**。
此时将显示**机箱运行状况**页面。左侧窗格显示机箱的前视图，并包含 KVM 的运行状况。通过 KVM 子图形的覆盖标记指示 KVM 运行状况。将指针移到 KVM 子图形上方，即会显示相应的文本提示或屏幕提示。文本提示提供有关 KVM 的附加信息。单击 KVM 子图形可在右侧窗格中查看 KVM 信息。
2. 或者，单击**机箱概览** → **前面板**。
在**状态**页面的**KVM 属性**部分，可以查看与机箱关联的 KVM 的状态和属性。有关更多信息，请参阅**联机帮助**。

查看 LCD 信息和运行状况

要查看 LCD 的运行状况，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览**。
将显示**机箱运行状况**页。左侧窗格显示机箱的前视图。LCD 运行状况由 LCD 子图形的重叠标记表示。
2. 移动光标到 LCD 子图形上。相应的文本提示或屏幕提示会提供有关 LCD 的附加信息。
3. 单击 LCD 子图形可在右窗格中查看 LCD 信息。有关更多信息，请参阅**联机帮助**。
或者，转到**机箱概览** → **前面板** → **属性** → **状态**。在**状态**页的**LCD 属性**下，您可以查看机箱上可用 LCD 的状态。有关更多信息，请参阅**联机帮助**。

查看温度传感器的信息和运行状况

要查看温度传感器的运行状况，请执行以下操作：

在左侧窗格中，单击**机箱概览** → **温度传感器**。

温度传感器状态页显示整个机箱（机箱和服务器）上温度探测器的状态和读数。有关更多信息，请参阅**联机帮助**。




注：无法编辑温度探测器值。任何超过阈值的更改都会生成警报，从而造成风扇速度发生变化。例如，如果 CMC 环境温度探测器超过阈值，机箱的风扇速度会提高。

配置 CMC

使用 Chassis Management Controller 可以配置属性、设置用户和警报，以执行远程管理任务。


在开始配置 CMC 之前，必须首先配置 CMC 网络设置，以允许从远程管理 CMC。该初始配置分配 TCP/IP 联网参数，以允许访问 CMC。有关更多信息，请参阅[设置对 CMC 的初始访问](#)。

可以使用 Web 界面或 RACADM 来配置 CMC。

 **注:** 当首次配置 CMC 时，您必须以 root 用户登录，以在远程系统上执行 RACADM 命令。可创建另一个用户，使之具有配置 CMC 的权限。

在设置 CMC 并执行基本配置之后，可以执行以下操作：

- 根据需要修改网络设置。
- 配置访问 CMC 的界面。
- 配置 LCD 显示屏。
- 根据需要设置机箱组。
- 配置服务器、I/O 模块或前面板。
- 配置 VLAN 设置。
- 获取所需证书。
- 添加和配置具有权限的 CMC 用户。
- 配置并启用电子邮件警报和 SNMP 陷阱。
- 根据需要设置功率上限策略。

 **注:** 在两种 CMC 界面（GUI 和 CLI）的属性字符串中，不能使用以下字符：


- &#
- < 和 >
- ;（分号）

查看和修改 CMC 网络 LAN 设置

LAN 设置（如团体字符串和 SMTP 服务器 IP 地址）将影响 CMC 和机箱的外部设置。

如果机箱中有两个 CMC（活动和待机），并且它们均连接至网络，则在出现故障转移时，待机 CMC 自动继承活动 CMC 的网络设置。

如果在启动时启用 IPv6，则会每 4 秒发送三个路由器请求。如果外部网络交换机运行生成树协议 (STP)，则外部交换机端口可在发送 IPv6 路由器请求时阻塞 12 秒以上。在此情况下，IPv6 连接会在一段时间内受限，直到 IPv6 路由器无偿发送路由器广告。

 **注:** 更改 CMC 网络设置可能会断开当前网络连接。

 **注:** 必须具备**机箱配置管理员**权限才可以设置 CMC 网络设置。

使用 CMC Web 界面查看和修改 CMC 网络 LAN 设置

要使用 CMC Web 界面查看和修改 CMC 网络 LAN 设置，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览**，然后单击**网络**。**网络配置**页面将显示当前的网络设置。
2. 根据需要修改常规、IPv4 或 IPv6 设置。有关更多信息，请参阅**联机帮助**。
3. 单击各个部分的**应用更改**以应用这些设置。

使用 RACADM 查看和修改 CMC 网络 LAN 设置

要查看 IPv4 设置，请使用下列子命令和对象：

- getniccfg
- getconfig
- cfgCurrentLanNetworking

要查看 IPv6 设置，请使用下列子命令和对象：

- getconfig
- cfgIpv6LanNetworking


要查看机箱的 IPv4 和 IPv6 寻址信息，请使用 `getsysinfo` 子命令。

有关子命令和对象的更多信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

启用 CMC 网络接口


若要为 IPv4 和 IPv6 启用或禁用 CMC 网络接口，请键入：

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1 racadm config -g  
cfgLanNetworking -o cfgNicEnable 0
```

 **注：**默认情况下启用 CMC NIC。


要启用或禁用 CMC IPv4 寻址，请键入：

```
racadm config -g cfgLanNetworking -o cfgNicIPv4Enable 1 racadm config -g  
cfgLanNetworking -o cfgNicIPv4Enable 0
```

 **注：**默认情况下启用 CMC IPv4 寻址。

要启用或禁用 CMC IPv6 寻址，请键入：

```
racadm config -g cfgIpv6LanNetworking -o cfgIPv6Enable 1 racadm config -g  
cfgIpv6LanNetworking -o cfgIPv6Enable 0
```

 **注：**默认情况下禁用 CMC IPv6 寻址。

默认情况下，对于 IPv4，CMC 自动从动态主机配置协议 (DHCP) 服务器请求并获取 CMC IP 地址。您可以禁用 DHCP 功能并指定静态 CMC IP 地址、网关和子网掩码。

对于 IPv4 网络，要禁用 DHCP 并指定静态 CMC IP 地址、网关和子网掩码，请键入：

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0 racadm config -g  
cfgLanNetworking -o cfgNicIpAddress <static IP address> racadm config -g  
cfgLanNetworking -o cfgNicGateway <static gateway> racadm config -g  
cfgLanNetworking -o cfgNicNetmask <static subnet mask>
```

默认情况下，对于 IPv6，CMC 自动从 IPv6 自动配置机制请求并获取 CMC IP 地址。

对于 IPv6 网络，要禁用自动配置功能并指定静态 CMC IPv6 地址、网关和前缀长度，请键入：

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6AutoConfig 0 racadm config -g
cfgIPv6LanNetworking -o cfgIPv6Address <IPv6 address> racadm config -g
cfgIPv6LanNetworking -o cfgIPv6PrefixLength 64 racadm config -g
cfgIPv6LanNetworking -o cfgIPv6Gateway <IPv6 address>
```

为 CMC 网络接口地址启用或禁用 DHCP

当启用时，CMC 的 NIC 地址 DHCP 功能将自动从动态主机配置协议 (DHCP) 服务器请求和获取 IP 地址。默认启用此功能。

您可以禁用 NIC 地址 DHCP 功能并指定静态 IP 地址、子网掩码和网关。有关更多信息，请参阅[设置对 CMC 的初始访问](#)。

对 DNS IP 地址启用或禁用 DHCP

默认情况下，禁用 CMC 的 DNS 地址 DHCP 功能。当启用时，该功能将从 DHCP 服务器获取主要和次要 DNS 服务器地址。使用该功能，可以不用配置静态 DNS 服务器 IP 地址。


要启用 DNS 地址 DHCP 功能并指定静态首选和备用 DNS 服务器地址，请键入：

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
```

要启用 IPv6 的 DNS 地址 DHCP 功能并指定静态首选和备用 DNS 服务器地址，请键入：

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6DNSServersFromDHCP6 0
```

设置静态 DNS IP 地址

 **注：**只有在禁用 DNS 地址 DHCP 功能的情况下，静态 DNS IP 地址设置才有效。

对于 IPv4，要设置主要和次要 DNS IP 服务器地址，请键入：

```
racadm config -g cfgLanNetworking -o cfgDNSServer1 <IP-address> racadm config -g
cfgLanNetworking -o cfgDNSServer2 <IPv4-address>
```


对于 IPv6，要设置主要和次要 DNS IP 服务器地址，请键入：


```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6DNSServer1 <IPv6-address>
racadm config -g cfgIPv6LanNetworking -o cfgIPv6DNSServer2 <IPv6-address>
```

配置 DNS 设置 (IPv4 和 IPv6)

- **CMC 注册** - 若要在 DNS 服务器上注册 CMC，请键入：

```
racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1
```

 **注：**有些 DNS 服务器只注册 31 个或更少字符的名称。确保指定的名称在 DNS 要求的范围内。

 **注：**只有通过将 `cfgDNSRegisterRac` 设置为 1 在 DNS 服务器上注册 CMC，以下设置才有效。

- **CMC 名称** - 默认情况下，DNS 服务器上的 CMC 名称为 `cmc-<service tag>`。要更改 DNS 服务器上的 CMC 名称，请键入：

```
racadm config -g cfgLanNetworking -o cfgDNSRacName <name>
```

其中 `<name>` 为最多 63 个字母数字字符和连字符组成的字符串。例如，`cmc-1、d-345`。

- **DNS 域名** - 默认 DNS 域名是单个空字符。要设置 DNS 域名，请键入：

```
racadm config -g cfgLanNetworking -o cfgDNSDomainName <name>
```

其中 `<name>` 为最多 254 个字母数字字符和连字符组成的字符串。例如：`p45、a-tz-1、r-id-001`。

配置自动协商、双工模式和网络速度（IPv4 和 IPv6）

当启用时，自动协商功能确定 CMC 是否通过与最近的路由器或交换机通信来自动设置双工模式和网络速度。默认启用自动协商功能。

可以通过键入以下命令禁用自动协商并指定双工模式和网络速度：

```
racadm config -g cfgNetTuning -o cfgNetTuningNicAutoneg 0 racadm config -g  
cfgNetTuning -o cfgNetTuningNicFullDuplex <duplex mode>
```

其中：

<duplex mode>为 0（半双工）或 1（全双工，默认）

```
racadm config -g cfgNetTuning -o cfgNetTuningNicSpeed <speed>
```

其中：


<speed> 是 10 或 100（默认值）。

设置最大传输单元 (MTU)（IPv4 和 IPv6）

MTU 属性允许设置可以通过接口传输的最大数据包限制。要设置 MTU，请键入：


```
racadm config -g cfgNetTuning -o cfgNetTuningMtu <mtu>
```

其中 <mtu> 是 576 - 1500（包含起始值；默认值为 1500）之间的值。

 **注：**IPv6 要求的最小 MTU 是 1280。如果启用了 IPv6，并且 `cfgNetTuningMtu` 设置为更小的值，则 CMC 会使用 1280 的 MTU。


配置 CMC 网络和登录安全设置

CMC 中的 IP 地址阻止和用户阻止功能支持您阻止猜密码登录尝试引发的安全问题。此功能可用于阻止一定范围的 IP 地址和可以访问 CMC 的用户。默认情况下，CMC 中启用 IP 地址阻止功能。

 **注：**IP 地址阻止功能仅适用于 IPV4 地址。

您可以使用 CMC Web 界面或 RACADM 设置 IP 范围属性。要使用 IP 地址阻止和用户阻止功能，请使用 CMC Web 界面或 RACADM 启用相关选项。配置登录锁定策略设置，以便设置特定用户或 IP 地址的登录尝试失败次数。超过此次数限制，被阻止的用户只能等惩罚时间过后期后才能再登录。

使用 CMC Web 界面配置 IP 范围属性

 **注：**要执行以下任务，必须具备**机箱配置管理员**权限。

要使用 CMC Web 界面配置 IP 范围属性，执行以下操作：

1. 在左侧窗格中，转至**机箱概览**，单击**网络** → **网络**。**网络配置**页面随即显示。
2. 在“IPv4 设置”部分，单击**高级设置**。
将显示**安全登录**页面。
此外，要访问“安全登录”页面，在左侧窗格中，转至**机箱概览**，单击**安全** → **登录**。
3. 要启用 IP 范围检查功能，请在 **IP 范围**部分，选中**启用 IP 范围**选项。
将激活 **IP 范围地址**和 **IP 范围掩码**字段。
4. 在 **IP 范围地址**和 **IP 范围掩码**字段中，输入您要阻止访问 CMC 的 IP 地址的范围和 IP 范围掩码。
有关更多信息，请参阅**联机帮助**。

5. 单击**应用**保存设置。

使用 RACADM 配置 IP 范围属性

您可以使用 RACADM 配置 CMC 的以下 IP 范围属性：

- IP 范围检查功能
- 您希望禁止访问 CMC 的 IP 地址范围
- 您希望禁止访问 CMC 的 IP 范围掩码

IP 筛选功能会比较接入登录的 IP 地址与指定的 IP 地址范围。仅当以下两项相同时才允许接入 IP 地址登录：

- **cfgRacTuneIpRangeMask** 按位并有接入 IP 地址
- **cfgRacTuneIpRangeMask** 按位并有 **cfgRacTuneIpRangeAddr**

注：

- 要启用 IP 范围检查功能，请使用 `cfgRacTuning` 组中的以下属性：
`cfgRacTuneIpRangeEnable <0/1>`
- 要指定您希望禁止访问 CMC 的 IP 地址范围，请使用 `cfgRacTuning` 组中的以下属性：
`cfgRacTuneIpRangeAddr`
- 要指定您希望禁止访问 CMC 的 IP 范围掩码，请使用 `cfgRacTuning` 组中的以下属性：
`cfgRacTuneIpRangeMask`

为 CMC 配置虚拟 LAN 标签属性

VLAN 用于允许多个虚拟 LAN 共同存在于同一物理网络电缆上，并允许出于安全性和负载管理的目的而分离网络流量。启用 VLAN 功能时，将给每个网络信息包分配 VLAN 标签。

使用 RACADM 为 CMC 配置 VLAN 标签属性

1. 启用外部机箱管理网络的 VLAN 功能：

```
racadm config -g cfgLanNetworking -o cfgNicVlanEnable 1
```

2. 为外部机箱管理网络指定 VLAN ID：

```
racadm config -g cfgLanNetworking -o cfgNicVlanID <VLAN id>
```

`<VLAN id>` 的有效值为 1-4000 和 4021-4094。默认值为 1。

例如：

```
racadm config -g cfgLanNetworking -o cfgNicVlanID 1
```

3. 然后，为外部机箱管理网络指定 VLAN 优先级：

```
racadm config -g cfgLanNetworking -o cfgNicVlanPriority <VLAN priority>
```

`<VLAN priority>` 的有效值为 0-7。默认值为 0。

例如：

```
racadm config -g cfgLanNetworking -o cfgNicVlanPriority 7
```

也可用一个命令指定 VLAN ID 和 VLAN 优先级：

```
racadm setniccfg -v <VLAN id> <VLAN priority>
```

例如：

```
racadm setniccfg -v 1 7
```

- 若要移除 CMC VLAN，请禁用外部机箱管理网络的 VLAN 功能：

```
racadm config -g cfgLanNetworking -o cfgNicVlanEnable 0
```

也可用以下命令移除 CMC VLAN：

```
racadm setniccfg -v
```

使用 Web 界面为 CMC 配置虚拟 LAN 标签属性

要使用 CMC Web 界面为 CMC 配置 VLAN，请执行以下操作：

- 转至以下任一页：

- 在左侧窗格中，单击**机箱概览**，然后单击**网络** → **VLAN**。
- 在左侧窗格中，单击**机箱概览** → **服务器概览**，然后单击**网络** → **VLAN**。

此时将显示 **VLAN 标签设置** 页。VLAN 标签是机箱属性。即使拆下了组件，机箱仍然有这些标签。

- 在 **CMC** 部分，为 CMC 启用 VLAN，设置优先级并分配 ID。有关这些字段的更多信息，请参阅 [联机帮助](#)。

- 单击**应用**。将保存 VLAN 标签设置。

您也可以通过**机箱概览** → **服务器** → **设置** → **VLAN** 访问此页面。

配置服务


您可以在 CMC 上配置和启用以下服务：

- CMC 串行控制台 - 支持使用串行控制台访问 CMC。
- Web 服务器 - 支持访问 CMC Web 界面。禁用 Web 服务器也会禁用远程 RACADM。
- SSH - 支持通过固件 RACADM 访问 CMC。
- Telnet - 支持通过固件 RACADM 访问 CMC。
- RACADM - 支持使用 RACADM 访问 CMC。
- SNMP - 支持 CMC 发送事件的 SNMP 陷阱。
- 远程系统日志 - 支持 CMC 将事件记录到远程服务器。要使用此功能，必须具有企业版许可证。


CMC 包含 Web 服务器，它配置为使用行业标准 SSL 安全协议通过 Internet 接受来自客户端的加密数据，或者向客户端传输加密数据。Web 服务器包含 Dell 自签名的 SSL 数字证书（服务器 ID），并且负责接受和响应来自客户端的安全 HTTP 请求。Web 界面和远程 RACADM CLI 工具需要该服务与 CMC 进行通信。

如果 Web 服务器重设，请等待至少一分钟以使服务再次可用。Web 服务器重设通常是由以下某个事件所导致的：

- 通过 CMC Web 用户界面或 RACADM 更改了网络配置或网络安全属性。
- 通过 Web 用户界面或 RACADM 更改了 Web 服务器端口配置。
- CMC 重设。
- 上载了新的 SSL 服务器证书。

 **注：**要修改服务设置，您必须具有机箱配置管理员权限。

远程系统日志是 CMC 的附加日志目标。配置远程系统日志之后，CMC 生成的每个新日志条目都会转发至相应的目标。

 **注：**由于在转发日志条目时使用 UDP 进行网络传输，因此不能保证日志条目成功发送，CMC 也不会收到关于日志条目是否被成功接收的反馈。

使用 CMC Web 界面配置服务

要使用 CMC Web 界面配置 CMC 服务，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览**，然后单击**网络** → **服务**。此时将显示**服务管理**页面。
2. 根据需要配置以下服务：
 - CMC 串行
 - Web Server
 - SSH
 - Telnet
 - 远程 RACADM
 - SNMP
 - 远程系统日志

有关各字段的信息，请参阅**联机帮助**。

3. 单击**应用**，然后更新所有默认超时和最大超时限制。

使用 RACADM 配置服务

要启用和配置各种服务，请使用以下 RACADM 对象：

- `cfgRacTuning`
- `cfgRacTuneRemoteRacadmEnable`

有关这些对象的更多信息，请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

如果服务器上的固件不支持某项功能，则在配置与该功能相关的属性时将显示错误。例如，使用 RACADM 在不受支持的 iDRAC 启用远程系统日志时将显示一条错误信息。

同样，使用 RACADM `getconfig` 命令显示 iDRAC 属性时，对于服务器上不支持的功能，属性值显示为 N/A（不适用）。

例如：

```
$ racadm getconfig -g cfgSessionManagement -m server-1 #
cfgSsnMgtWebServerMaxSessions=N/A # cfgSsnMgtWebServerActiveSessions=N/A #
cfgSsnMgtWebServerTimeout=N/A # cfgSsnMgtSSHMaxSessions=N/A #
cfgSsnMgtSSHActiveSessions=N/A # cfgSsnMgtSSTimeout=N/A #
cfgSsnMgtTelnetMaxSessions=N/A # cfgSsnMgtTelnetActiveSessions=N/A #
cfgSsnMgtTelnetTimeout=N/A
```

配置 CMC 扩展存储卡

可以启用或修复可选的可移动闪存介质，以用于扩展的非易失性存储。某些 CMC 功能依赖于扩展的非易失性存储进行操作。

要使用 CMC Web 界面启用或修复可移动闪存介质，请执行以下操作：

1. 在左侧窗格中，转至**机箱概览**，然后单击**机箱控制器** → **闪存介质**。
2. 在**可移动闪存介质**页面中，根据需要从下拉菜单中选择以下选项之一：
 - **修复活动控制器介质**
 - **停止使用闪存介质存储机箱数据**

有关这些选项的更多信息，请参阅**联机帮助**。

3. 单击**应用**以应用所选的选项。

如果机箱中存在两个 CMC，则两个 CMC（活动和待机）都必须包含闪存介质；除非活动和待机 CMC 都包含闪存介质，否则扩展存储功能的性能会下降。

设置机箱组

CMC 可以从一个主机箱监测多个机箱。启用机箱组时，主机箱中的 CMC 会生成主机箱和机箱组中所有成员机箱的状态的图形显示。要使用此功能，必须具有企业版许可证。


机箱组功能为：

- 显示描绘每个机箱正面和背面的图像，主机箱一组，每个成员机箱一组。
- 有关主机箱和组成员的运行状况通过红色或黄色覆盖标记识别，并在有问题的组件上标识 X 或 ! 符号。单击机箱图像或**详情**按钮时，机箱图像下会显示详情。
- 快速启动链接可用于打开成员机箱或服务器的 Web 页面。
- 服务器和输入/输出资源清册对于组可用。
- 提供可选选项，以在新成员添加到组时令新成员的属性与主机箱属性同步。

机箱组最多可包含八个成员。此外，主机箱或成员只能加入一个组。不能将作为某个组的主机箱或成员的机箱加入到另一个组中。可以从组中删除机箱，然后再将其添加到不同组。

要使用 CMC Web 界面设置机箱组，请执行以下操作：

1. 以机箱管理员权限登录到主机箱。
2. 单击**设置** → **组管理**。
3. 在**机箱组**页面中的**角色**下，选择**主机箱**。此时将显示用于添加组名称的字段。
4. 在**组名称**字段中键入组名称，然后单击**应用**。


 **注：**适用于域名的相同规则也适用于组名称。

创建机箱组后，GUI 会自动切换到**机箱组**页面。左侧窗格按组名称和主机箱指示组，并且未填充的成员机箱会在左侧窗格中显示。

将成员添加到机箱组

设置机箱组后，通过以下步骤将成员添加到机箱组：

1. 以机箱管理员权限登录到主机箱。
2. 在树中选择主机箱。
3. 单击**设置** → **组管理**。
4. 在**组管理**下的**主机名/IP 地址**字段中输入成员的 IP 地址或 DNS 名称。
5. 在**用户名**字段中，输入具有该成员机箱的机箱管理员权限的用户名。
6. 在**密码**字段中键入相应的密码。
7. 另外，可选择 **Sync New Member with Leader Properties**（用**主机箱属性同步新成员**）以将主机箱属性推送至成员。

8. 单击**应用**。
9. 完成步骤 4 至步骤 8 中的任务可添加最多 8 个成员。新成员的机箱名称显示在**成员**对话框中。
 **注:** 为成员输入的凭据会以安全方式传递到成员机箱，以在成员与主机箱之间建立信任关系。凭据不会在任一机箱中保留，并且在建立初始信任关系后永远不会再次进行交换。

从主机箱中移除成员

可以从主机箱移除组中的成员。要移除成员，请执行以下操作：

1. 以机箱管理员权限登录到主机箱。
2. 在左侧窗格中，选择主机箱。
3. 单击**设置** → **组管理**。
4. 从**移除成员**列表中，选择要删除的成员的名称，然后单击**应用**。
主机箱随后会与已从组中移除的一个或多个成员机箱（如果选择多个）进行通信。成员名称即被移除。如果因为网络问题导致主机箱与成员机箱之间无法通信，则成员机箱可能无法收到该消息。在这种情况下，从成员机箱禁用该成员即可完成移除。

解散机箱组

要从主机箱解散机箱组，请执行以下操作：

1. 以管理员权限登录到主机箱。
2. 在左侧窗格中选择主机箱。
3. 单击**设置** → **组管理**。
4. 在**机箱组**页中的**角色**下，选择**无**，然后单击**应用**。
主机箱随后会与已从组中移除的所有成员通信。现在，可以将该主机箱分配为新组的主机箱或成员。
如果因为网络问题导致主机箱与成员之间无法联系，则成员机箱可能无法收到消息。在这种情况下，从成员机箱禁用该成员即可完成移除过程。

在成员机箱中禁用单个成员

有时，无法通过主机箱从组中移除成员。如果与该成员的网络连接丢失，则可能会发生此情况。要在成员机箱上从组中移除成员：

1. 以机箱管理员权限登录到成员机箱。
2. 在左侧窗格中，单击**机箱概览** → **设置** → **组管理**。
3. 选择**无**，然后单击**应用**。

启动成员机箱或服务器的 Web 页面

可通过主机箱组页面访问成员机箱的 Web 页面、服务器远程控制台或 iDRAC 服务器的 Web 页面。如果成员设备的登录凭据与主机箱相同，则可以使用相同的凭据来访问成员设备。

要导航到成员设备，请执行以下操作：

1. 登录到主机箱。
2. 在树中选择**组：名称**。

3. 如果成员 CMC 是所需的目标，请为所需机箱选择**启动 CMC**。
如果机箱中的服务器是所需目标：
 - a) 选择目标机箱的图像。
 - b) 在**运行状况**部分所显示的机箱图像中，选择服务器。
 - c) 在标记为**快速链接**的框中，选择目标设备。此时会显示带有目标页面或登录屏幕的新窗口。

传播主机箱属性至成员机箱

您可以将来自主机箱的属性应用至组中的成员机箱。要同步成员与主机箱属性，请执行以下操作：

1. 以管理员权限登录到主机箱。
2. 在树中选择主机箱。
3. 单击**设置** → **组管理**。
4. 在**机箱属性传播**部分，选择以下传播类型之一：
 - **动态变化传播** — 选择此选项以自动传播所选机箱属性设置。每当主机箱属性被更改时，该属性更改即被传播至所有当前的组成员。
 - **手动传播** — 选择此选项以手动传播组机箱主机箱属性至其成员。主机箱属性设置仅在主机箱管理员单击**传播**时，才传播至组的其他成员。
5. 在**传播属性**部分，选择将要被传播至成员机箱的主机箱配置属性的类别。
请仅选择那些您希望在机箱组的所有成员上采取同样配置的设置类别。例如，选择**日志和警报属性类**，以启用组中的所有机箱共享主机箱的日志和警报设置。
6. 单击**保存**。
如果选择**动态变化传播**，成员机箱将采用主机箱的属性。如果选择**手动传播**，在想要传播所选设置至成员机箱时，单击**传播**。有关将主机箱属性传播至成员机箱的更多信息，请参阅**联机帮助**。

MCM 组的刀片资源清册

组是包含 0 到 8 个机箱组成员的主机箱。**机箱组运行状况**页面显示所有成员机箱，并允许您使用标准浏览器下载功能将服务器资源清册报告保存到文件。该报告包含以下对象的数据：

- 当前在所有组机箱（包括主机箱）中的所有服务器。
- 空插槽和扩展插槽（包括全高和双宽服务器模块）。

保存服务器资源清册报告

要使用 CMC Web 界面保存服务器资源清册报告，请执行以下操作：

1. 在左侧窗格中，选择**组**。
2. 在**机箱组运行状况**页面中，单击**保存资源清册报告**。将显示**文件下载**对话框，提示您打开或保存文件。
3. 单击**保存**并指定服务器模块资源清册报告的路径和文件名。



注：机箱组主机箱和机箱组成员机箱以及关联机箱中的服务器模块必须接通电源，才能获得最准确的服务器模块资源清册报告。

导出的数据

服务器资源清册报告包含在机箱组主机箱的正常轮询期间（每 30 秒一次）由各个机箱组成员最近返回的数据。


要获得最准确的服务器资源清册报告：

- 机箱组主机箱和所有机箱组成员机箱必须处于**机箱电源状态开启**状态。

- 相关机箱中的所有服务器必须已开机。

如果机箱组成员机箱的子集为以下状态，则资源清册报告中可能会缺少相关机箱和服务器的资源清册数据：

- 机箱电源状态关闭状态
- 已关闭电源

 注: 如果在机箱电源关闭时插入服务器，则在机箱再次通电前不会在 Web 界面中的任何位置显示型号。

下表列出每个服务器要报告的具体数据字段以及字段的具体要求：

表. 6: 服务器模块资源清册字段说明

数据字段	示例
机箱名称	数据中心主机箱
机箱 IP 地址	192.168.0.1
插槽位置	1
插槽名称	SLOT-01
主机名	企业 Web 服务器  注: 需要在服务器上运行的服务器管理员代理；否则显示为空。
操作系统	Windows Server 2008  注: 需要在服务器上运行的服务器管理员代理；否则显示为空。
型号	PowerEdgeM610
服务标签	1PB8VF1
总系统内存	4.0 GB  注: 成员上需要 VRTX CMC 1.0 或更高版本；否则显示为空。
CPU 数量	2  注: 成员上需要 VRTX CMC 1.0 或更高版本；否则显示为空。
CPU 信息	Intel (R) Xeon (R) CPU E5502 @1.87GHz  注: 成员上需要 VRTX CMC 1.0 或更高版本；否则显示为空。


数据格式

资源清册报告以 .CSV 文件格式生成，以便于导入各种工具，例如 Microsoft Excel。可通过在 MS Excel 中选择 **数据** → **自文本** 将资源清册报告 .CSV 文件导入模板。在将资源清册报告导入至 MS Excel 后，如果显示一条消息提示需要附加信息，请选择逗号分隔以将文件导入至 MS Excel。

机箱组资源清册和固件版本

机箱组固件版本 页面显示机箱组资源清册与机箱中服务器和服务器组件的固件版本。您还可以在该页面上整理资源清册信息并筛选固件版本视图。将基于服务器或以下任何机箱服务器组件显示视图：

- BIOS
- iDRAC
- CPLD
- USC
- 诊断程序
- 操作系统驱动程序
- RAID
- NIC

 **注:** 每次添加或卸下组中的机箱后，显示的机箱组、成员机箱、服务器和服务器组件资源清册信息都会更新。

查看机箱组资源清册

要使用 CMC Web 界面查看机箱组，在左侧窗格中，选择**组**。单击**属性** → **固件版本**。**机箱组固件版本**页面将显示组中的所有机箱。

使用 Web 界面查看所选机箱的资源清册

要使用 CMC Web 界面查看所选机箱的资源清册，请执行以下操作：

1. 在系统树中，选择**组**。单击**属性** → **固件版本**。
机箱组固件版本页面将显示组中的所有机箱。
2. 在**选择机箱**部分，选择您要查看其资源清册的成员机箱。
固件视图筛选器部分将显示所选机箱的服务器资源清册和所有服务器组件的固件版本。

使用 Web 界面查看所选服务器组件的固件版本


要使用 CMC Web 界面查看所选服务器组件的固件版本，执行以下操作：

1. 在左侧窗格中，选择**组**。单击**属性** → **固件版本**。
机箱组固件版本页面将显示组中的所有机箱。
2. 在**选择机箱**部分，选择您要查看其资源清册的成员机箱。
3. 在**固件视图筛选器**部分，选择**组件**。
4. 在**组件**列表中，选择您要查看其固件版本的所需组件：BIOS、iDRAC、CPLD、USC、诊断程序、操作系统驱动程序、RAID 设备（最多 2 个）和 NIC 设备（最多 6 个）。
将显示所选成员机箱中所有服务器的所选组件的固件版本。


使用 RACADM 配置多个 CMC

使用 RACADM 可以配置一个或多个具有相同属性的 CMC。

使用组 ID 和对象 ID 查询特定 CMC 卡时，RACADM 从检索到的信息创建 `racadm.cfg` 配置文件。通过将文件导出到一个或多个 CMC，可以在最短时间内以相同属性配置控制器。


 **注:** 某些配置文件包含独特的 CMC 信息（如静态 IP 地址），在将文件导出到其他 CMC 之前必须修改这些信息。

1. 使用 RACADM 查询包含所需配置的目标 CMC。

 **注:** 生成的配置文件为 **myfile.cfg**。您可以重命名该文件。**.cfg** 文件不包含用户密码。在将 **.cfg** 文件上载到新 CMC 后，您必须重新添加所有密码。

2. 打开到 CMC 的 Telnet/SSH 文本控制台，登录并键入：

```
racadm getconfig -f myfile.cfg
```

 **注:** 仅远程 RACADM 界面支持使用 `getconfig -f` 将 CMC 配置重定向至文件。

3. 使用简单文本编辑器（可选）修改配置文件。配置文件中的任何特殊格式字符都可能损坏 RACADM 数据库。

4. 使用新创建的配置文件修改目标 CMC。在命令提示符处，键入：

```
racadm config -f myfile.cfg
```

5. 重设已配置的目标 RAC。在命令提示符处键入：

```
racadm reset
```

`getconfig -f myfile.cfg` 子命令为活动 CMC 请求 CMC 配置并生成 **myfile.cfg** 文件。如果需要，可以将文件重命名或将其保存到另一个位置。

可以运行 `getconfig` 命令来执行以下操作：

- 显示组中的所有配置属性（用组名称和索引指定）。
- 按用户名显示用户的所有配置属性。

`config` 子命令将信息载入其他 CMC。Server Administrator 使用 `config` 命令同步用户和密码数据库。

创建 CMC 配置文件

CMC 配置文件 **<filename>.cfg** 与 `racadm config -f <filename>.cfg` 命令一同使用可创建简单文本文件。该命令允许建立配置文件（类似于 `.ini` 文件），可通过该文件配置 CMC。

用户可以使用任意文件名，并且文件不一定要使用 **.cfg** 扩展名（尽管本小节中的指定值采用了此扩展名）。

 **注:** 有关 `getconfig` 子命令的更多信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

RACADM 在首次将 **.cfg** 文件载入 CMC 时对其进行分析，以验证是否存在有效的组和对象名称，以及是否遵守简单的语法规则。使用检测到错误的行号来标记错误，并且使用消息来解释问题。系统将分析整个文件以检查其正确性，并显示所有错误。如果在 **.cfg** 文件中发现错误，写入命令将不会传输到 CMC。必须先改正所有错误才能使配置生效。

要在创建配置文件之前检查错误，请在 `config` 子命令中使用 `-c` 选项。通过使用 `-c` 选项，`config` 仅验证语法而不会写入 CMC。

创建 **.cfg** 文件时，请遵循以下原则：

- 如果分析器遇到索引组，区分各个索引的将是锚定对象的值。
分析器将从 CMC 读入该组的所有索引。配置 CMC 时，该组内的任何对象已经修改。如果修改的对象代表新的索引，则将在配置过程中在 CMC 上创建该索引。
- 无法在 **.cfg** 文件中指定所需的索引。
可以创建和删除索引。经过一段时间后，组中可能会出现使用和未使用的索引碎片。如果索引存在，它将被修改。如果索引不存在，则使用第一个可用的索引。

此方法在添加索引条目时更加灵活，因为您不需要在所有管理的 CMC 之间进行精确索引匹配。新用户将被添加至第一个可用的索引。如果所有索引均已满并且必须添加新的用户，则在一个 CMC 上可以正确分析和运行的 .cfg 文件可能无法在另一个 CMC 上正确运行。

- 可以使用 racresetcfg 子命令为两个 CMC 配置相同的属性。

使用 racresetcfg 子命令将 CMC 重设为初始默认值，然后运行 racadm config -f <filename>.cfg 命令。确保 .cfg 文件中包含所有所需的对象、用户、索引和其他参数。有关对象和组的完整列表，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

 **小心:** 使用 racresetcfg 子命令可将数据库和 CMC 网络接口设置重设为初始默认设置，并移除所有用户和用户配置。根用户可用时，还会将其他用户设置重设为默认设置。

- 如果您键入 racadm getconfig -f <filename> .cfg，该命令将建立当前 CMC 配置的 .cfg 文件。此配置文件可用作示例并用作唯一的 .cfg 文件的起点。

分析规则

- 以井号 (#) 开始的行将视为注释。

注释行必须在第一列中开始。所有其他列中的 “#” 字符均只被视为 # 字符。

一些调制解调器参数可能在其字符串中包含 # 字符。不需要转义字符。您可能要从 racadm getconfig -f <filename>.cfg 命令生成 .cfg，然后对另一个 CMC 执行 racadm config -f <filename>.cfg 命令，而不添加转义字符。

例如：

```
# # This is a comment [cfgUserAdmin] cfgUserAdminPageModemInitString= <Modem
init # not a comment>
```

- 所有的组条目必须位于左方括号和右方括号 ([和]) 之内。

表示组名起始的 [字符必须位于第一列。此组名必须先于该组中的任何对象而被指定。没有关联组名的对象将导致错误。配置数据将组织成组，如 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（适用于 PowerEdge VRTX RACADM 的机箱管理控制器的命令行参考指南）的“数据库属性”一章中所定义。以下示例显示组名、对象以及对象的属性值：

```
[cfgLanNetworking] -{group name} cfgNicIpAddress=143.154.133.121 {object
name} {object value}
```

- 所有参数都指定为“对象=值”对，在对象、= 或值之间不留空格。值后的空格将忽略。值字符串内的空格保持不变。“=”右侧的所有字符（例如第二个 =、#、[和] 等）都将保留原样。这些字符都是有效的调制解调器对话脚本字符。

```
[cfgLanNetworking] -{group name} cfgNicIpAddress=143.154.133.121 {object
value}
```

- .cfg 分析器忽略索引对象条目。

用户无法指定使用哪个索引。如果索引已存在，则使用该索引，否则将在该组的第一个可用索引中创建新条目。

racadm getconfig -f <filename>.cfg 命令将注释放置在索引对象前，允许用户查看包含的注释。


 **注:** 可以使用以下命令手动创建索引组：

```
racadm config -g <groupname> -o <anchored object> -i <index 1-4> <unique
anchor name>
```

- 无法从 .cfg 文件中删除索引组的行。如果使用文本编辑器删除该行，则 RACADM 会在分析配置文件时停止并警告错误。

用户必须使用以下命令手动移除索引对象：

```
racadm config -g <groupname> -o <objectname> -i <index 1-4> ""
```

 **注:** NULL 字符串（两个"字符表示）指示 CMC 删除指定组的索引。

要查看索引组的内容，请运行以下命令：

```
racadm getconfig -g <groupname> -i <index 1-4>
```

- 对于索引组，对象定位器必须是 [] 对后的第一个对象。以下是当前索引组的示例：

```
[cfgUserAdmin] cfgUserAdminUserName= <USER_NAME>
```

- 使用远程 RACADM 将配置组捕获到文件中时，如果组内的关键属性未设置，则配置组不会保存为配置文件的一部分。如果需要将这些配置组克隆到其他 CMC，则在执行 `getconfig -f` 命令之前必须设置关键属性。或者，可以在运行 `getconfig -f` 命令之后手动将缺失的属性输入到配置文件中。对于所有 RACADM 索引组均如此。

这是表现出此行为的索引组及其相应的关键属性列表：

- cfgUserAdmin - cfgUserAdminUserName
- cfgEmailAlert - cfgEmailAlertAddress
- cfgTraps - cfgTrapsAlertDestIPAddr
- cfgStandardSchema - cfgSSADRoleGroupName
- cfgServerInfo - cfgServerBmcMacAddress

修改 CMC IP 地址

在配置文件中修改 CMC IP 地址时，移除所有不必要的 `<variable> = <value>` 条目。只有实际变量组标签带有 [和] 的保持不变，包括与 IP 地址更改有关的两个 `<variable> = <value>` 条目。

示例：


```
# # Object Group "cfgLanNetworking" # [cfgLanNetworking]
cfgNicIpAddress=10.35.10.110 cfgNicGateway=10.35.10.1
```

此文件更新如下：

```
# # Object Group "cfgLanNetworking" # [cfgLanNetworking]
cfgNicIpAddress=10.35.9.143 # comment, the rest of this line is ignored
cfgNicGateway=10.35.9.1
```


命令 `racadm config -f <myfile>.cfg` 分析文件并通过行号标识任何错误。正确的文件会更新适当的条目。此外，您可以使用与上一示例相同的 `getconfig` 命令确认更新。

使用此文件下载公司范围的更改或使用命令 `racadm getconfig -f <myfile>.cfg` 通过网络配置新系统。

 **注:** *Anchor* 是保留字，不应在 `.cfg` 文件中使用。

查看和结束 CMC 会话

您可以查看当前登录 iDRAC7 的用户数并结束用户会话。

 **注:** 要结束会话，必须具备 **机箱配置管理员** 权限。

使用 Web 界面查看和结束 CMC 会话

要使用 Web 界面查看或结束会话，执行以下操作：

1. 在左侧窗格中，转至 **机箱概览** 并单击 **网络** → **会话**。
会话页会显示会话 ID、用户名、IP 地址以及会话类型。有关这些属性的更多信息，请参阅 *联机帮助*。
2. 要结束会话，对会话单击 **终止**。

使用 RACADM 查看和结束 CMC 会话

您必须具有管理员权限才能使用 RACADM 结束 CMC 会话。

要查看当前用户会话，请使用 `getssninfo` 命令。

要结束用户会话，使用 `closesessn` 命令。

有关这些命令的更多信息，请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（适用于 PowerEdge VRTX RACADM 的机箱管理控制器的命令行参考指南）。

配置服务器


可以配置服务器的以下设置：

- 插槽名称
- iDRAC 网络设置
- DRAC VLAN 标签设置
- 第一引导设备
- 服务器 FlexAddress
- 远程文件共享
- 使用服务器克隆的 BIOS 设置

配置插槽名称

插槽名称用于标识单个服务器。当选择插槽名称时，将应用以下规则：

- 名称仅能包含最多 15 个非扩展的 ASCII 字符（ASCII 代码 32 到 126）。
- 插槽名称必须在机箱内唯一。各插槽不能具有相同的名称。
- 字符串不区分大小写。Server-1, server-1, and SERVER-1 是相同的名称。
- 插槽名称不得使用以下字符串开头：
 - Switch-
 - Fan-
 - PS-
 - DRAC-
 - MC-
 - Chassis
 - Housing-Left
 - Housing-Right
 - Housing-Center
- 可以使用字符串 Server-1 到 Server-4，但仅供相应的插槽使用。例如，Server-3 是插槽 3 的有效名称，但不是插槽 4 的有效名称。但是，Server-03 可以是任何插槽的有效名称。

 **注：**要更改插槽名称，您必须具备**机箱配置管理员**权限。

Web 界面中的插槽名称设置仅保存在 CMC 中。如果从机箱中卸下服务器，则服务器的插槽名称设置将不再保留。

CMC Web 界面中的插槽名称设置始终覆盖在 iDRAC 界面中对显示名称所做的任何更改。

要使用 CMC Web 界面编辑插槽名称，请执行以下操作：

1. 在左侧窗格中，转至**机箱概览** → **服务器概览** → **设置** → **插槽名称**。
2. 在**插槽名称**页面的**插槽名称**字段中编辑插槽名称。

3. 要将服务器的主机名用作插槽名称，请选择**插槽名称使用主机名**选项。如果服务器的主机名（或系统名称）可用，此选项将用该名称覆盖静态插槽名称。这要求 OMSA 代理安装在服务器上。有关 OMSA 代理的更多信息，请参阅 dell.com/support/manuals 上的 *Dell OpenManage Server Administrator User's Guide*（Dell OpenManage Server Administrator 用户指南）。
4. 要保存设置，请单击**应用**。

要还原服务器的默认插槽名称（SLOT-01 至 SLOT-4，基于服务器的插槽位置），请单击**还原默认值**。

配置 iDRAC 网络设置

要使用此功能，必须具有企业版许可证。您可以配置服务器的 iDRAC 网络配置设置。可以使用快速部署设置来配置以后要安装的服务器的默认 iDRAC 网络配置设置和根密码。这些默认设置是 iDRAC 快速部署设置。

有关 iDRAC 的更多信息，请参阅 dell.com/support/manuals 上的 *iDRAC7 用户指南*。


配置 iDRAC 快速部署网络设置

使用“快速部署设置”可为新插入的服务器配置网络设置。

要启用并设置 iDRAC 快速部署设置，请执行以下操作：

1. 在左侧窗格中，单击**服务器概览** → **设置** → **iDRAC**。
2. 在**部署 iDRAC**页面的**快速部署设置**部分中，指定在下表中提到的设置。有关这些字段的更多信息，请参阅**联机帮助**。


表. 7: 快速部署设置

设置	说明
启用快速部署	选择此选项可启用 快速部署 功能，将此页面上配置的 iDRAC 设置自动应用到新插入的服务器。必须在本地 LCD 面板上确认自动配置。
插入服务器时设置 iDRAC root 密码	选择此选项可在插入服务器时，更改 iDRAC 根密码以符合在 iDRAC 根密码 字段中提供的值。
iDRAC 根密码	选中 插入服务器时设置 iDRAC 根密码 和 启用快速部署 选项后，此密码值会在服务器插入机箱时分配给服务器的 iDRAC 根用户密码。此密码可包含 1 到 20 个可打印（含空格）字符。
确认 iDRAC 根密码	允许您重新输入在 密码 字段中提供的密码。
启用 iDRAC LAN	启用或禁用 iDRAC LAN 信道。默认情况下，清除此选项。
启用 iDRAC IPv4	启用或禁用 iDRAC 上的 IPv4。默认情况下，选中此选项。
启用 LAN 上 iDRAC IPMI	为机箱中存在的每个 iDRAC 启用或禁用 IPMI over LAN 信道。默认情况下，选中此选项。
启用 iDRAC IPv4 DHCP	为机箱中存在的每个 iDRAC 启用或禁用 DHCP。如果启用此选项，则字段 快速部署 IP 、 快速部署子网掩码 和 快速部署网关 都被禁用，并且无法修改，因为系统使用 DHCP 自动为每个 iDRAC 分配这些设置。要选择此选项，必须选择 启用 iDRAC IPv4 选项。
起始 iDRAC IPv4 地址（插槽 1）	指定机柜插槽 1 中服务器 iDRAC 的静态 IP 地址。从插槽 1 的静态 IP 地址开始，针对每个插槽，每个后续 iDRAC 的 IP 地址增加 1。如果 IP 地址加插槽编号大于子网掩码，会显示一个错误消息。  注： 子网掩码和网关不像 IP 地址那样增加。 例如，如果起始 IP 地址是 192.168.0.250 并且子网掩码是 255.255.0.0，则插槽 15 的快速部署 IP 地址是 192.168.0.265。如果子网掩码是 255.255.255.0，则将在单击 保存快速部署设置 或 使用快速部署设置自动填充 时显示 QuickDeploy IP address range is not fully within QuickDeploy Subnet 错误消息。
iDRAC IPv4 子网掩码	指定被分配到所有新插入服务器的快速部署子网掩码。


设置	说明
iDRAC IPv4 网关	指定分配给机箱中所有 iDRAC 的快速部署默认网关。
启用 iDRAC IPv6	为机箱中支持 IPv6 的每个 iDRAC 启用 IPv6 寻址。
启用 iDRAC IPv6 自动配置	使 iDRAC 能够从 DHCPv6 服务器获取 IPv6 设置（地址和前缀长度），还启用无状态地址自动配置。默认情况下，此选项被启用。
iDRAC IPv6 网关	指定要分配给 iDRAC 的默认 IPv6 网关。默认值是“..”。
iDRAC IPv6 前缀长度	指定要为 iDRAC 上的 IPv6 地址分配的前缀长度。默认值是 64。

- 单击**保存快速部署设置**以保存设置。如果您对 iDRAC 网络设置进行了更改，请单击**应用 iDRAC 网络设置**将设置部署到 iDRAC。

快速部署功能仅在启用并且服务器插入机箱中时执行。如果启用**插入服务器时设置 iDRAC 根密码**和**启用快速部署**，则在 LCD 界面中会提示用户允许或不允许更改密码。如果网络配置设置不同于当前的 iDRAC 设置，则提示用户接受或拒绝更改。

 **注:** 如果存在 LAN 或 IPMI over LAN 差异，则提示用户接受快速部署 IP 地址设置。如果差异是 DHCP 设置，则提示用户接受 DHCP 快速部署设置。

要将快速部署设置复制到 **iDRAC 网络设置**部分，请单击**使用快速部署设置自动填充**。快速部署网络配置设置将复制到 **iDRAC 网络配置设置**表中的相应字段。

 **注:** 对快速部署字段的更改立即生效，但对一个或多个 iDRAC 服务器网络配置设置的更改可能需要几分钟才能从 CMC 传播到 iDRAC。单击**刷新**太快时，可能只显示一个或多个 iDRAC 服务器的部分正确数据。

修改单个服务器 iDRAC 的 iDRAC 网络设置

使用此功能可以为每台已安装的服务器配置 iDRAC 网络配置设置。每个字段显示的初始值是从 iDRAC 读取的当前值。要使用此功能，必须具有企业版许可证。


要修改 iDRAC 网络设置，请执行以下操作：

- 在左侧窗格中，单击**服务器概览**，然后单击**设置**。在**部署 iDRAC**页面的**iDRAC 网络设置**部分，列出了所有已安装服务器的 iDRAC IPv4 和 IPv6 网络配置设置。
- 根据需要修改服务器的 iDRAC 网络设置。

 **注:** 您必须选择**启用 LAN**选项来指定 IPv4 或 IPv6 设置。有关这些字段的信息，请参阅**联机帮助**。

- 要将设置部署到 iDRAC，请单击**应用 iDRAC 网络设置**。对于**快速部署设置**做出的所有更改也会保存。

iDRAC 网络设置表反映未来的网络配置设置；为安装服务器显示的值不一定与当前安装的 iDRAC 网络配置设置相同。更改后单击**刷新更新 iDRAC 部署**页和每个安装的 iDRAC 网络配置设置。

 **注:** 对“快速部署”字段的更改立即生效，但对一个或多个 iDRAC 服务器网络配置设置的更改可能需要几分钟才能从 CMC 传送到 iDRAC。单击**刷新**太快时，可能只显示一台或多台 iDRAC 服务器的部分正确数据。

使用 RACADM 修改 iDRAC 网络设置

RACADM `config` 或 `getconfig` 命令支持以下配置组的 `-m <module>` 选项：

- `cfgLanNetworking`
- `cfgIpv6LanNetworking`
- `cfgRacTuning`
- `cfgRemoteHosts`
- `cfgSerial`
- `cfgSessionManagement`

有关属性默认值和范围的更多信息，请参阅 dell.com/support/manuals 上的 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）。

配置 iDRAC VLAN 标签设置

VLAN 用于允许多个虚拟 LAN 共同存在于同一物理网络电缆上，并允许出于安全性或负载管理的目的而分离网络流量。启用 VLAN 功能时，将给每个网络信息包分配 VLAN 标签。VLAN 标签是机箱属性。即使拆下了组件，机箱仍然保留这些标签。

使用 RACADM 配置 iDRAC VLAN 标签设置

- 用以下命令指定特定服务器的 VLAN ID 和优先级：
`racadm setniccfg -m server-<n> -v <4VLAN id> <VLAN priority>`

<n> 的有效值为 1 - 4。

<VLAN> 的有效值为 1-4000 和 4021-4094。默认值为 1。

<VLAN priority> 的有效值为 0-7。默认值为 0。

例如：

```
racadm setniccfg -m server-1 -v 1 7
```

例如：

- 若要删除服务器 VLAN，请禁用指定服务器网络的 VLAN 功能：

```
racadm setniccfg -m server-<n> -v
```

<n> 的有效值为 1 - 4。

例如：

```
racadm setniccfg -m server-1 -v
```

使用 Web 界面配置 iDRAC VLAN 标签设置


要为服务器配置 VLAN，请执行以下操作：

1. 转至以下任一页：
 - 在左侧窗格中，单击**机箱概览** → **网络** → **VLAN**。
 - 在左侧窗格中，单击**机箱概览** → **服务器概览**，然后单击**设置** → **VLAN**。
2. 在 **VLAN 标签设置** 页面的 **iDRAC** 部分，为服务器启用 VLAN，设置优先级并输入 ID。有关各字段的更多信息，请参阅 [联机帮助](#)。
3. 单击**应用**保存设置。

设置第一引导设备

可以为每台服务器指定 CMC 第一引导设备。该设备可能不是服务器的实际第一引导设备，甚至不代表该服务器中的设备。它代表 CMC 发送到服务器的设备，并用作它针对该服务器的第一引导设备。可以将此设备设置为默认第一引导设备或一次性引导设备，以便引导映像来执行任务，如运行诊断程序或重新安装操作系统。

您可以设置第一引导设备仅用于下次引导或用于所有后续重新引导。您可以设置服务器的第一引导设备。系统在下次和后续重新引导时会从所选设备引导，并保持作为 BIOS 引导顺序中的第一引导设备，直到从 CMC Web 界面或从 BIOS 引导顺序再次更改为止。

 **注:** CMC Web 界面中的第一引导设备设置会覆盖系统 BIOS 引导设置。


您指定的引导设备必须存在并且包含可引导介质。

可以将以下设备设置为第一引导设备。

表. 8: 引导设备

引导设备	说明
PXE	从网络接口卡上的预引导执行环境 (PXE) 协议引导。
硬盘驱动器	从服务器上的硬盘驱动器引导。
本地 CD/DVD	从服务器上的 CD 或 DVD 驱动器引导。
虚拟软盘	从虚拟软盘驱动器引导。软盘驱动器（或软盘映像）位于管理网络中另一台计算机上，并且使用 iDRAC GUI 控制台 Viewer 连接。
虚拟 CD/DVD	从虚拟 CD/DVD 驱动器或 CD/DVD ISO 映像引导。光盘驱动器或 ISO 映像文件位于管理网络中另一台计算机或另一个引导磁盘上，并且使用 iDRAC GUI 控制台查看器连接。
iSCSI	从 Internet 小型计算机系统接口 (iSCSI) 设备引导。
本地 SD 卡	从本地 SD（安全数字）卡引导 - 仅适用于支持 iDRAC6 和 iDRAC7 系统的服务器。
本地软盘	从本地软盘驱动器中的软盘引导。
远程文件共享	从远程文件共享 (RFS) 映像引导。映像文件使用 iDRAC GUI 控制台查看器连接。

使用 CMC Web 界面为多个服务器设置第一引导设备

 **注:** 要为服务器设置第一引导设备，必须具备**服务器管理员**权限或**机箱配置管理员**权限，以及 **iDRAC 登录** 权限。

要为多个服务器设置第一引导设备，请执行以下操作：

1. 在左侧窗格中，单击**服务器概览** → **设置** → **第一引导设备**。此时将显示服务器列表。
2. 在**第一引导设备**列中，从各服务器所对应的下拉菜单中选择要用于该服务器的引导设备。
3. 如果要服务器每次引导时都从选定的设备引导，请清除该服务器对应的**引导一次**选项。如果要服务器仅在下一个引导周期从选定的设备引导，请选中该服务器对应的**引导一次**选项。
4. 单击**应用**保存设置。

使用 CMC Web 界面为单个服务器设置第一引导设备

 **注:** 要为服务器设置第一引导设备，必须具备**服务器管理员**权限或**机箱配置管理员**权限和 **iDRAC 登录** 权限。

要为单个服务器设置第一引导设备，请执行以下操作：

1. 在左侧窗格中，单击**服务器概览**，然后单击要为其设置第一引导设备的服务器。
2. 转至**设置** → **第一引导设备**。此时将显示**第一引导设备**页面。
3. 在**第一引导设备**下拉菜单中，选择要用于每个服务器的引导设备。
4. 如果希望服务器每次引导时都从选定的设备引导，请清除该服务器对应的**引导一次**选项。如果要服务器仅在下一引导周期从选定的设备引导，请选中该服务器对应的**引导一次**选项。
5. 单击**应用**保存设置。

使用 RACADM 设置第一引导设备

要设置第一引导设备，请使用 `cfgServerFirstBootDevice` 对象。

要启用为设备引导一次，请使用 `cfgServerBootOnce` 对象。

有关这些对象的更多信息，请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

配置服务器 FlexAddress

有关为服务器配置 FlexAddress 的信息，请参阅[使用 CMC Web 界面为机箱级结构和插槽配置 FlexAddress](#)。要使用此功能，必须具有企业版许可证。

配置远程文件共享

远程虚拟介质文件共享功能通过 CMC 将网络上共享驱动器中的文件映射到一个或多个服务器，以部署或更新操作系统。连接后，可以像访问本地服务器文件那样访问远程文件。支持两种类型的介质：软盘驱动器和 CD/DVD 驱动器。

要执行远程文件共享操作（连接、断开连接或部署），您必须具有**机箱配置管理员**或**服务器管理员**权限。要使用此功能，必须具有企业版许可证。

要配置远程文件共享，请执行以下操作：

1. 在左侧窗格中，单击**服务器概览** → **设置** → **远程文件共享**。
2. 在**部署远程文件共享**页面中，在各字段中键入相应的数据。有关字段说明的更多信息，请参阅[联机帮助](#)。
3. 单击**连接**连接到远程文件共享。要连接远程文件共享，必须提供路径、用户名和密码。操作成功后将允许访问该介质。
单击**断开连接**可断开之前连接的远程文件共享。
单击**部署**可部署介质设备。



注：在单击**部署**按钮之前务必保存所有工作文件，因为此操作会使服务器重新启动。

单击**部署**后会执行以下任务：

- 连接远程文件共享。
- 将文件选择为服务器的第一引导设备。
- 重新启动服务器。
- 如果服务器已关机，则接通服务器电源。

使用服务器配置复制功能配置配置文件设置

服务器配置复制功能允许您将指定服务器的所有配置文件设置应用于一个或多个服务器。可以复制的配置文件设置是那些可以修改并且可以跨服务器复制的配置文件设置。将显示并且可以复制服务器的以下三个配置文件组：

- BIOS - 此组仅包含服务器的 BIOS 设置。这些配置文件从 CMC 针对 PowerEdge VRTX 版本 1.00 和更高版本所生成。
- BIOS 和引导 - 此组包括服务器的 BIOS 和引导设置。这些配置文件从 CMC 针对 PowerEdge VRTX 版本 1.00 和更高版本所生成。
- 所有设置 - 此版本包含该服务器及该服务器上组件的所有设置。这些配置文件从 CMC 针对 PowerEdge VRTX 版本 1.00 和更高版本，以及针对搭载 iDRAC7 和 Lifecycle Controller 2 版本 1.1 或更高版本的 12G 服务器所生成。

服务器配置复制功能支持 iDRAC7 服务器。上一代 RAC 服务器在主页上列出，但会显示为灰色，并且不能使用此功能来启用。

要使用服务器配置复制功能，请执行以下操作：

- iDRAC 至少必须具有要求的最低版本。iDRAC7 服务器要求版本 1.00.00。
- 服务器必须接通电源。

服务器版本和配置文件兼容性：

- iDRAC7 及 Lifecycle Controller 2 版本 1.1 可以接受任何版本的配置文件。
- 搭载 Lifecycle Controller 2 版本 1.0 的 iDRAC7 仅接受 BIOS 或 BIOS 和引导配置文件。
- 从搭载 Lifecycle Controller 2 版本 1.1 的 iDRAC7 服务器保存配置文件导致生成所有设置配置文件。

可执行以下操作：

- 查看服务器上或来自所保存配置文件的配置文件设置。
- 保存来自服务器的配置文件。
- 将配置文件应用于其他服务器。
- 从远程文件共享导入存储的配置文件。
- 编辑配置文件的名称和说明。
- 将存储的配置文件导出到远程文件共享。
- 删除已存储的配置文件。
- 使用 **Quick Deploy** 选项将所选配置文件部署到目标设备。
- 显示最近的服务器配置文件任务的日志活动。

访问服务器配置文件页面

您可以使用 **服务器配置文件** 页面添加和管理服务器配置文件，并将其应用于一个或多个服务器。


要使用 CMC Web 界面访问 **服务器配置文件** 页面，在左侧窗格中，转至 **机箱概览** → **服务器概览**。单击 **设置** → **配置文件**。系统将显示 **服务器配置文件** 页面。

添加或保存配置文件

克隆服务器属性之前，首先将属性捕捉到存储的配置文件中。创建存储的配置文件并为每个配置文件提供名称，还可以添加说明。您可以在 CMC 非易失性扩展存储介质上最多保存 16 个存储的配置文件。


卸下或禁用非易失性扩展存储介质会阻止对存储的配置文件进行访问，并禁用服务器克隆功能。

要添加或保存配置文件：


1. 转至**服务器配置文件**页面。在**服务器配置文件**部分，选择您要从其设置生成配置文件的服务器，然后单击**保存配置文件**。
将显示**保存服务器配置文件**部分。
2. 在**配置文件名称和说明**字段中，请输入配置文件名称和说明（可选），然后单击**保存配置文件**。
CMC 与 LC 通信以获取可用的服务器配置文件设置，并将它们存储为指定的配置文件。
进度指示器表示“保存”操作正在进行中。完成该操作后，会显示一条“操作成功”的消息。
 **注：**收集设置的进程在后台运行。因此，新配置文件可能需要过一段时间才能显示。如果不显示新配置文件，请检查配置文件日志中是否存在错误。

应用配置文件

仅当服务器配置文件存储在 CMC 上的非易失性介质上时，才能执行服务器克隆。要启动服务器克隆操作，您可以将存储的配置文件应用于一个或多个服务器。

 **注：**如果服务器不支持 Lifecycle Controller 或机箱的电源已关闭，则不能将配置文件应用于服务器。

要将配置文件应用到一个或多个服务器，请执行以下操作：

1. 转至**服务器配置文件**页面。在**保存和应用配置文件**部分，选择您要应用所选配置文件的一个或多个服务器。
选择配置文件下拉菜单此时被启用。
2. 从**选择配置文件**下拉菜单中，选择您要应用的配置文件。
应用配置文件选项此时被启用。
3. 单击**应用配置文件**。
会显示警告消息指示将应用新的服务器配置文件覆盖当前设置并重新引导所选服务器。系统会提示您确认是否要继续该操作。
 **注：**要在服务器上执行服务器克隆操作，必须为服务器启用 CSIOR 选项。如果已禁用 CSIOR 选项，会显示警告消息指示服务器未启用 CSIOR。要完成刀片克隆操作，请确保在服务器上启用 CSIOR 选项。
4. 单击**确定**以应用配置文件到选定的服务器。
服务器将应用所选配置文件，并且可能立即重新引导（如果需要）。有关更多信息，请参阅 *CMC Online Help*（CMC 联机帮助）。

导入配置文件

您可以将存储在远程文件共享上的服务器配置文件导入到 CMC。

要将远程文件共享上的存储配置文件导入到 CMC，请执行以下操作：

1. 在**服务器配置文件**页面上的**SD 卡上的配置文件**部分，单击**导入配置文件**。
将显示**导入服务器配置文件**部分。
2. 单击**浏览**从所需的位置访问该配置文件，然后单击**导入配置文件**。
有关更多信息，请参阅**联机帮助**。

导出配置文件

您可以将存储在 CMC 非易失性介质（SD 卡）上的服务器配置文件导出至远程文件共享上的指定路径。

要导出存储的配置文件：

1. 转至**服务器配置文件**页面。在 **SD 卡上的配置文件**部分，选择所需的配置文件，然后单击**导出配置文件**。随即会显示**文件下载**消息，询问您打开还是保存文件。
2. 单击**保存或打开**以导出配置文件至所需的位置。
有关更多信息，请参阅[联机帮助](#)。

编辑配置文件

您可以编辑存储在 CMC 非易失性介质（SD 卡）上的服务器配置文件的名称和说明。


要编辑存储配置文件：

1. 转至**服务器配置文件**页面。在 **SD 卡上的配置文件**部分，选择所需的配置文件，然后单击**编辑配置文件**。随即显示**编辑 BIOS 配置文件 - <配置文件名>**部分。
2. 按照要求编辑服务器配置文件的名称和说明，然后单击**编辑配置文件**。
有关更多信息，请参阅[联机帮助](#)。

查看配置文件设置

要查看选定服务器的**配置文件设置**，请转至**服务器配置文件**页面。在**服务器配置文件**部分，单击所需服务器的**服务器配置文件**列中的**查看**。将显示**查看设置**页面。

有关所显示设置的更多信息，请参阅[联机帮助](#)。

 **注：**只有**重新启动时收集系统资源清册 (CSIOR)** 选项启用时，CMC 服务器配置复制功能才会检索并显示特定服务器的设置。

要启用 CSIOR，在重新引导服务器后，从 **F2 设置**中，选择 **iDRAC 设置** → **Lifecycle Controller**，启用 **CSIOR** 并保存更改。

查看存储的配置文件设置

要查看存储在 CMC 非易失性介质（SD 卡）上的服务器配置文件的设置，请转至**服务器配置文件**页面。在 **SD 卡上的配置文件**部分，单击所需服务器的**查看配置文件**列中的**查看**。**查看设置**页面随即显示。有关所显示设置的更多信息，请参阅[联机帮助](#)。

查看配置文件日志

要查看配置文件日志，请在**服务器配置文件**页面中，查看**最近配置文件日志**部分。该部分列出服务器克隆操作直接生成的最近 10 个配置文件日志条目。每条日志记录均显示服务器配置复制操作的严重性、提交时间和日期，以及复制日志消息描述。日志条目还可以从 RAC 日志中查看。要查看其他可用条目，请单击**浏览配置文件日志**。**配置文件日志**页面随即显示。有关更多信息，请参阅[联机帮助](#)。

完成状态和故障排除

要检查应用的 BIOS 配置文件的完成状态，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **服务器概览** → **设置** → **配置文件**。
2. 在 **BIOS 配置文件**页面中，记下**最近配置文件日志**部分中已提交作业的作业 ID (JID)。
3. 在左侧窗格中，单击**服务器概览** → **故障排除** → **Lifecycle Controller 作业**。搜索作业表中的相同 JID。有关使用 CMC 执行 Lifecycle Controller 作业的更多信息，请参阅[Lifecycle Controller 作业操作](#)。

配置文件的 Quick Deploy

使用 Quick Deploy 功能可以将存储的配置文件分配给服务器插槽。插槽中插入的任何支持服务器配置复制的服务器都可以使用分配给该插槽的配置文件进行配置。仅当在**部署 iDRAC**页面中启用了**启用服务器配置文件部署**选项时，才能执行 Quick Deploy 操作。要转至**部署 iDRAC**页面，选择**服务器概览** → **设置** → **iDRAC**。可以部署的配置文件都包含在 SD 卡中。


注:


要设置用于快速部署的配置文件，您必须拥有**机箱管理员**权限。


将服务器配置文件分配给插槽

在**服务器配置文件**页面上可以将服务器配置文件分配给插槽。要将配置文件分配给机箱插槽，请执行以下操作：

1. 在**服务器配置文件**页面上，转至**用于快速部署的配置文件**部分。
在**服务器配置文件**列中包含的选择框中，将显示插槽的当前配置文件分配。
2. 从下拉菜单中，选择要分配给所需插槽的配置文件。可选择若干配置文件以应用于多个插槽。
3. 单击**分配**。
配置文件将应用于选定的插槽。

 **注:** 没有分配任何配置文件的插槽将在选择框中以“未选择配置文件”来指示。

 **注:** 要移除插槽的所有配置文件分配，在下拉菜单中，选中**未选择配置文件**。


 **注:** 当使用**快速部署配置文件**功能为服务器部署配置文件时，应用的过程和结果将记录在配置文件日志中。


使用单点登录启动 iDRAC

CMC 针对单个机箱组件（例如服务器）提供有限的管理。为了全面管理这些单个组件，CMC 提供基于 Web 的服务器管理控制器 (iDRAC) 界面启动点。

用户不需要再次登录即可启动 iDRAC Web 界面，因为此功能采用单点登录。单点登录策略如下：

- 拥有服务器管理权限的 CMC 用户会使用单点登录自动登录到 iDRAC。在 iDRAC 站点上，会自动授予此用户管理员权限。即便同一位用户没有在 iDRAC 上的帐户，或如果该帐户没有管理员权限，这也同样适用。
- CMC 用户如果**没有**服务器管理权限但拥有在 iDRAC 上的相同帐户，可使用单点登录自动登录到 iDRAC。在 iDRAC 站点上，授予此用户为 iDRAC 帐户创建的权限。
- CMC 用户如果没有服务器管理权限或在 iDRAC 上的相同帐户，则**不会**使用单点登录自动登录到 iDRAC。单击 **启动 iDRAC GUI** 可将此用户导航至 iDRAC 登录页。

 **注:** 在此情况下，术语“相同帐户”的含义是用户拥有 CMC 和 iDRAC 的相同登录名称以及匹配密码。用户拥有相同登录名称而没有匹配密码，也认为其拥有相同帐户。

 **注:** 可能提示用户登录到 iDRAC（请参阅上面的第三单点登录策略公告）。

 **注:** 如果禁用 iDRAC 网络 LAN（LAN 启用 = 否），单点登录不可用。

如果从机箱卸下服务器，iDRAC IP 地址会更改，或 iDRAC 网络连接遇到问题，单击“启动 iDRAC GUI”可能会显示一个错误页。

从服务器状态页启动 iDRAC

要为单个服务器启动 iDRAC 管理控制台，请执行以下操作：

1. 在左侧窗格中，展开**服务器概览**。在展开的**服务器概览**列表中，将显示所有四个服务器。
2. 单击要为其启动 iDRAC Web 界面的服务器。
3. 在**服务器状态**页面中，单击**启动 iDRAC GUI**。
此时将显示 iDRAC Web 界面。有关字段说明的信息，请参阅**联机帮助**。

从服务器状态页启动 iDRAC

要从**服务器状态**页启动 iDRAC 管理控制台，请执行以下操作：

1. 在左侧窗格中，单击**服务器概览**。
2. 在**服务器状态**页中，为要启动 iDRAC Web 界面的服务器单击**启动 iDRAC**。

启动远程控制台

您可以在服务器上直接启动键盘-视频-鼠标 (KVM) 会话。远程控制台功能仅在满足以下所有条件时可用：

- 机箱已开机。
- 支持 iDRAC 7 的服务器。
- 服务器上的 LAN 界面已启用。
- 主机系统安装有 JRE (Java Runtime Environment) 6 Update 16 或更高版本。
- 主机系统上的浏览器支持弹出窗口 (禁用弹出窗口阻止程序)。

也可从 iDRAC Web 界面启动远程控制台。有关更多详情，请参阅 dell.com/support/manuals 上的 *iDRAC 用户指南*。

从机箱运行状况页启动远程控制台

要从 CMC Web 界面启动远程控制台，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览**，然后单击**属性**。
2. 在**机箱运行状况**页面中，单击机箱图形中的指定服务器。
3. 在**快速链接**部分，单击**远程控制台**链接以启动远程控制台。

从服务器状态页启动远程控制台

要为单个服务器启动远程控制台，请执行以下操作：

1. 在左侧窗格中，展开**服务器概览**。在展开的服务器列表中，将显示所有四个服务器。
2. 单击要为其启动远程控制台的服务器。
3. 在**服务器状态**页面中，单击**启动远程控制台**。

从服务器状态页启动远程控制台

要从**服务器状态**页启动远程控制台，请执行以下操作：

1. 在左侧窗格中，转至**服务器概览**，然后单击**属性** → **状态**。此时将显示**服务器状态**页。
2. 单击**启动远程控制台**，为所需的服务器启动远程控制台。

配置 CMC 以发送警报

您可以为机箱上发生的某些事件设置警报和操作。当系统组件的状态超过预定义的条件时会触发事件。如果事件与事件筛选器匹配，并且您已将此筛选器配置为生成警报消息（电子邮件警报或 SNMP 陷阱），则系统会将警报发送到一个或多个配置的目标，例如电子邮件地址、IP 地址或外部服务器。

要配置 CMC 来发送警报，请执行以下操作：

1. 启用**机箱事件警报**选项。
2. 还可以根据类别或严重程度筛选警报。
3. 配置电子邮件警报或 SNMP 陷阱设置。
4. 启用机箱事件警报向已配置的目标发送电子邮件警报或 SNMP 陷阱。

启用或禁用警报

要将警报发送到配置的目标，您必须启用全局警报选项。该属性将覆盖单个警报设置。

确保将 SNMP 或电子邮件警报目标配置为接收警报。

使用 CMC Web 界面启用或禁用警报

要启用或禁用生成警报，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **警报**。
2. 在**机箱事件**页面的**机箱警报启用**部分，选择**启用机箱事件警报**选项以启用警报，或者清除该选项以禁用警报。
3. 要保存设置，请单击**应用**。

使用 RACADM 启用或禁用警报


要启用或禁用生成警报，请使用 `cfglpmiLanAlertEnable` RACADM 对象。有关更多信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

筛选警报

可以基于类别和严重性筛选警报。

使用 CMC Web 界面筛选警报

要基于类别和严重性筛选警报，请执行以下操作：

 **注:** 要应用机箱事件配置更改，必须具有警报配置权限。

1. 在左侧窗格中，单击**机箱概览** → **警报**。
2. 在**机箱事件**页面的**警报筛选**部分，选择下列一个或多个类别：
 - 系统运行状况
 - 存储
 - 配置
 - 审核
 - 更新
3. 选择下列一个或多个严重性等级：
 - 严重
 - 警告
 - 通知
4. 单击**应用**。

监测的警报部分显示基于所选类别和严重性的结果。有关此页面上的字段说明的信息，请参阅**联机帮助**。

使用 RACADM 设置事件警报

要设置事件警报，请运行 `eventfilters` 命令。有关更多信息，请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

配置警报目标

管理站使用简单网络管理协议 (SNMP) 接收 CMC 发来的数据。

您可以配置 IPv4 和 IPv6 警报目标、电子邮件设置和 SMTP 服务器设置，并测试这些设置。

在配置电子邮件警报或 SNMP 陷阱设置之前，请确保您具有机箱配置管理员权限。

配置 SNMP 陷阱警报目标

您可以配置 IPv6 或 IPv4 地址以接收 SNMP 陷阱。

使用 CMC Web 界面配置 SNMP 陷阱警报目标

要使用 CMC Web 界面配置 IPv4 或 IPv6 警报目标设置，请执行以下操作：


1. 在左侧窗格中，单击**机箱概览** → **警报** → **陷阱设置**。
2. 在**机箱事件警报目标**页面中，键入以下内容：
 - 在**目标**字段中，键入有效的 IP 地址。使用四点 IPv4 格式、标准 IPv6 地址表示法或 FQDN。例如：**123.123.123.123** 或 **2001:db8:85a3::8a2e:370:7334** 或 **dell.com**。
选择一种与您的联网技术或基础结构一致的格式。测试陷阱功能无法根据当前网络配置检测不正确的选择（例如，在仅支持 IPv4 的环境中使用 IPv6 目标）。
 - 在**团体字符串**字段中，输入目标管理站所属的有效团体名称。
该团体字符串与**机箱概览** → **网络** → **服务**页面上的团体字符串不同。SNMP 陷阱团体字符串是 CMC 用于以管理站为目标的出站陷阱的团体字符串。**机箱概览** → **网络** → **服务**页面上的团体字符串是管理站用于查询 CMC 上 SNMP 守护程序的团体字符串。
 - 在**已启用**下，选择与目标 IP 对应的选项，以允许该 IP 地址接收陷阱。您最多可以指定 4 个 IP 地址。

3. 单击**应用**保存设置。
4. 要测试 IP 地址是否接收 SNMP 陷阱，请单击**测试 SNMP 陷阱**列中的**发送**。
IP 警报目标即配置完成。

使用 RACADM 配置 SNMP 陷阱警报目标

要使用 RACADM 配置 IP 警报目标，请执行以下操作：

1. 打开到 CMC 的串行/Telnet/SSH 文本控制台并登录。

 **注：**只能为 SNMP 和电子邮件警报设置一个筛选器掩码。如果已经选择了筛选器掩码，则不要执行任务 2，而转至步骤 3。

2. 启用警报生成：

```
racadm config -g cfgAlerting -o cfgAlertingEnable 1
```

3. 通过运行 `racadm eventfilters set` 命令指定事件筛选器。

- a) 要清除所有可用的警报设置，请运行以下命令：`racadm eventfilters set -c cmc.alert.all -n none`
- b) 使用严重性作为参数进行配置。例如，为存储类别中的所有通知事件分配关闭电源操作，并分配电子邮件和 SNMP 通知：`racadm eventfilters set -c cmc.alert.storage.info -n email,snmp`
- c) 使用子类别作为参数进行配置。例如，为审核类别中的许可子类别下的所有配置分配关闭电源操作，并启用所有通知：`racadm eventfilters set -c cmc.alert.audit.lic -n all`
- d) 使用子类别和严重性作为参数进行配置。例如，为审核类别中的许可子类别下的所有通知事件分配关闭电源操作，并禁用所有通知：`racadm eventfilters set -c cmc.alert.audit.lic.info -n none`

4. 启用陷阱警报：

```
racadm config -g cfgTraps -o cfgTrapsEnable 1 -i <index>
```

其中 <index> 的值为 1-4。CMC 使用索引编号来区别最多四个用于陷阱警报的可配置目标。可以将目标指定为格式正确的数字地址（IPv6 或 IPv4）或完全限定域名（FQDN）。

5. 指定接收陷阱警报的目标 IP 地址：

```
racadm config -g cfgTraps -o cfgTrapsAlertDestIPAddr <IP address> -i <index>
```

其中 <IP address> 是有效目标，<index> 是在步骤 4 中指定的索引值。

6. 指定团体名称：

```
racadm config -g cfgTraps -o cfgTrapsCommunityName <community name> -i <index>
```

其中 <community name> 是机箱所属的 SNMP 团体，<index> 是在步骤 4 和 5 中指定的索引值。

最多可以配置四个接收陷阱警报的目标。要添加更多目标，请执行步骤 2 - 6 中的任务。

 **注：**步骤 2 - 6 中的命令会覆盖为指定索引 (1-4) 配置的所有现有设置。要确定某索引以前是否配置过值，请键入：`racadm getconfig -g cfgTraps -i <index>`。如果已配置该索引，则会显示 `cfgTrapsAlertDestIPAddr` 和 `cfgTrapsCommunityName` 对象的值。

7. 要测试警报目标的事件陷阱，请键入：

```
racadm testtrap -i <index>
```

其中 <index> 是 1-4 之间的值，代表想要测试的警报目标。


如果不确定索引号，请运行以下命令：

```
racadm getconfig -g cfgTraps -i <index>
```

配置电子邮件警报设置

当 CMC 检测到机箱事件时（如环境警告或组件故障），可以配置为向一个或多个电子邮件地址发送电子邮件警报。

必须配置 SMTP 电子邮件服务器才能接收来自 CMC IP 地址的中继电子邮件，该功能在大多数邮件服务器上通常由于安全原因而被关闭。有关以安全方式执行此操作的说明，请参阅随 SMTP 服务器一起提供的说明文件。

 **注:** 如果邮件服务器是 Microsoft Exchange Server 2007，确保为邮件服务器配置 iDRAC7 域名，以便从 iDRAC7 接收电子邮件警报。

 **注:** 电子邮件警报支持 IPv4 和 IPv6 地址。使用 IPv6 时必须指定 DRAC DNS 域名。

如果网络中存在不时释放并更新 IP 地址租用的 SMTP 服务器，并且每次更新后得到的地址不同，则可能会因为指定的 SMTP 服务器 IP 地址发生变化而导致该属性设置在一段时间内无法工作。这种情况下，请使用 DNS 名称。

使用 CMC Web 界面配置电子邮件警报设置

要使用 Web 界面配置电子邮件警报设置，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **警报** → **电子邮件警报设置**。
2. 指定 SMTP 电子邮件服务器设置和电子邮件地址以接收警报。有关字段说明的信息，请参阅[联机帮助](#)。
3. 单击**应用**保存设置。
4. 单击**测试电子邮件**下的**发送**，将测试电子邮件发送到指定的电子邮件警报目标。


使用 RACADM 配置电子邮件警报设置

要使用 RACADM 向电子邮件警报目标发送测试电子邮件，请执行以下操作：

1. 打开到 CMC 的串行/Telnet/SSH 文本控制台并登录。

2. 启用警报生成：

```
racadm config -g cfgAlerting -o cfgAlertingEnable 1
```

 **注:** 只能为 SNMP 和电子邮件警报设置一个筛选器掩码。如果已经设置了筛选器掩码，则不要执行步骤 3 中的任务。

3. 指定必须生成警报的事件：

```
racadm config -g cfgAlerting -o cfgAlertingFilterMask <mask value>
```

其中 <mask value> 是介于 0x0 和 0xfffff 之间的十六进制值，并且必须带有前导 0x 字符。事件陷阱筛选器掩码表提供针对每种事件类型的筛选器掩码。有关计算您想要启用的筛选器掩码十六进制值的说明，请参阅[使用 RACADM 配置 SNMP 陷阱警报目标](#)中的步骤 3。

4. 启用电子邮件警报生成：

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable 1 -i <index>
```

其中 <index> 为 1-4 之间的值。CMC 使用索引号来区分最多 4 个可配置的目标电子邮件地址。

5. 指定接收电子邮件警报的目标电子邮件地址：

```
racadm config -g cfgEmailAlert -o cfgEmailAlertAddress <email address> -i <index>
```

其中 <email address> 是有效的电子邮件地址，<index> 是在步骤 4 中指定的索引值。

6. 指定接收电子邮件警报的人员姓名:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEmailName <email name> -i <index>
```


其中 <email name> 是接收电子邮件警报的个人或组的名称, <index> 是在步骤 4 和步骤 5 中指定的索引值。电子邮件名称最多包含 32 个字母数字字符、破折号、下划线和句点。空格无效。

7. 设置 SMTP 主机:

```
racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr host.domain
```

其中 host.domain 是 FQDN。

最多可配置 4 个目标电子邮件地址以接收电子邮件警报。要添加更多电子邮件地址, 请执行步骤 2 到步骤 6 中的任务。

 **注:** 步骤 2-6 中的命令会覆盖为所指定索引 (1-4) 配置的任何现有设置。要确定某索引以前是否配置过值, 请键入: `racadm getconfig -g cfgEmailAlert -i <index>`。如果已配置该索引, 则会显示 `cfgEmailAlertAddress` 和 `cfgEmailAlertEmailName` 对象的值。

有关更多信息, 请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南)。

配置用户帐户和权限

您可以设置具有特定权限（基于角色的授权）的用户帐户以使用 CMC 管理系统和维护系统安全。默认情况下，CMC 配置了本地管理员帐户。此默认用户名为 `root`，密码为 `calvin`。作为管理员，您可以设置用户帐户，以允许其他用户访问 CMC。

您最多可以设置 16 个本地用户，或使用目录服务（例如 Microsoft Active Directory 或 LDAP）以设置附加用户帐户。使用目录服务可提供一个集中的位置来管理授权的用户帐户。

CMC 支持基于角色访问具有一组相关权限的用户。角色包括管理员、操作员、只读用户或无角色。角色定义可用的最大权限。

用户的类型

用户有两种类型：



- CMC 用户和机箱用户
- iDRAC 用户或服务器用户（自 iDRAC 驻留在服务器上后）

CMC 和 iDRAC 用户可以是本地用户或 Directory 服务用户。

除 CMC 用户拥有**服务器管理员**权限外，授予 CMC 用户的权限不会自动转移到服务器上的同一用户，因为服务器用户的创建是与 CMC 用户无关的。换言之，CMC Active Directory 用户和 iDRAC Active Directory 用户位于 Active Directory 树中两个不同的分支。要创建本地服务器用户，配置用户必须直接登录到服务器。配置用户不能从 CMC 创建服务器用户，反之亦然。该规则是为了保护服务器的安全性和完整性。

表. 9: 用户类型

权限	说明
CMC 登录用户	<p>用户可登录到 CMC 并查看所有 CMC 数据，但不能增加或修改数据或者执行命令。</p> <p>用户可能具备其他权限而不具备 CMC 登录用户权限。当需要暂时禁止用户登录时，该功能非常有用。当用户的 CMC 登录用户权限恢复后，用户仍将保留所有之前授予的其他权限。</p>
机箱配置管理员	<p>用户可添加或更改的数据有：</p> <ul style="list-style-type: none"> • 标识机箱的数据，例如机箱名称和机箱位置。 • 专门分配给机箱的数据，例如 IP 模式（静态或 DHCP）、静态 IP 地址、静态网关以及静态子网掩码。 • 为机箱提供服务的数据，例如日期和时间、固件更新以及 CMC 重设。 • 与机箱相关的数据，例如插槽名称和插槽优先级。尽管这些属性适用于服务器，但是严格地说它们是与插槽而非服务器本身相关的机箱属性。因此，不管服务器是否存在于插槽中，都可以添加或更改插槽名称和插槽优先级。 <p>当服务器移到不同的机箱中时，它会在新机箱中继承分配给它所占据的插槽的名称和优先级。以前的插槽名称和优先级与以前的机箱保持一致。</p>

权限	说明
用户配置管理员	<p> 注: 具有机箱配置管理员权限的 CMC 用户可配置电源设置。但是, 要执行机箱电源操作, 包括打开电源、关闭电源以及打开后再关闭电源, 则需要机箱控制管理员权限。</p> <p>用户可以:</p> <ul style="list-style-type: none"> • 添加新用户。 • 更改用户的密码。 • 更改用户的权限。 • 启用或禁用某个用户的登录权限, 但保留该用户在数据库中的名称和其他权限。
清除日志管理员	用户可清除硬件日志和 CMC 日志。
机箱控制管理员 (电源命令)	<p>拥有机箱电源管理员权限的 CMC 用户可以执行所有与电源相关的操作。他们可以控制机箱电源操作, 包括打开电源、关闭电源以及打开后再关闭电源。</p> <p> 注: 要配置电源设置, 需要机箱配置管理员权限。</p>
服务器管理员	<p>这是一种全面的权限, 赋予 CMC 用户在机箱中的所有服务器上执行任何操作的所有权利。</p> <p>当具有 CMC 服务器管理员权限的用户发起要在服务器上执行的操作时, CMC 固件将此命令发送给目标服务器, 而不会检查此用户在该服务器上的权限。换言之, 服务器管理员权限可覆盖服务器上缺少的任何管理员权限。</p> <p>如果没有服务器管理员权限, 只有在满足以下所有条件时, 机箱上创建的用户才能在服务器上执行命令:</p> <ul style="list-style-type: none"> • 此服务器上存在相同的用户名。 • 此服务器上相同的用户名的密码必须相同。 • 此用户必须具备执行命令的权限。 <p>当不具备服务器管理员权限的 CMC 用户发起要在服务器上执行的操作时, CMC 会将一条命令发送给具有此用户的登录名和密码的目标服务器。如果该服务器上不存在此用户, 或者密码不匹配, 则拒绝此用户执行操作。</p> <p>如果目标服务器上有此用户且密码匹配, 则该服务器将应答此用户在该服务器上具有的权限。根据服务器的权限响应, CMC 固件决定此用户是否有权执行操作。</p> <p>下面列出了服务器管理员在服务器上被授予的权限和可以进行的操作。只有在机箱用户未具备机箱上的服务器管理权限时, 才应用这些权限。</p> <p>服务器配置管理员:</p> <ul style="list-style-type: none"> • 设置 IP 地址 • 设置网关 • 设置子网掩码 • 设置第一引导设备 <p>配置用户:</p> <ul style="list-style-type: none"> • 设置 iDRAC 根密码 • iDRAC 重设

权限	说明
	服务器控制管理员： <ul style="list-style-type: none"> • 打开电源 • 关闭电源 • 打开电源后再关闭电源 • 正常关机 • 服务器重新引导
测试警报用户	用户可发送测试警报消息。
调试命令管理员	用户可执行系统诊断命令。
结构 A 管理员	用户可设置和配置结构 A IOM。
结构 B 管理员	用户可设置和配置结构 B，它对应于服务器中的第一个夹层卡，并且连接到主板上的共享 PCIe 子系统结构 B 电路。
结构 C 管理员	用户可设置和配置结构 C，它对应于服务器中的第二个夹层卡，并且连接到主板上的共享 PCIe 子系统结构 C 电路。

CMC 用户组提供具有预分配用户权限的一系列用户组。


 **注:** 如果选择“管理员”、“高级用户”或“来宾用户”，然后从预定义设置中添加或删除权限，则 CMC 组会自动更改为自定义。

表. 10: CMC 组权限

用户组	权限分配
管理员	<ul style="list-style-type: none"> • CMC 登录用户 • 机箱配置管理员 • 用户配置管理员 • 清除日志管理员 • 服务器管理员 • 测试警报用户 • 调试命令管理员 • 结构 A 管理员
高级用户	<ul style="list-style-type: none"> • 登录 • 清除日志管理员 • 机箱控制管理员（电源命令） • 服务器管理员 • 测试警报用户 • 结构 A 管理员
来宾用户	登录
自定义	选择以下权限的任意组合： <ul style="list-style-type: none"> • CMC 登录用户 • 机箱配置管理员 • 用户配置管理员 • 清除日志管理员


用户组	权限分配
	<ul style="list-style-type: none"> • 机箱控制管理员（电源命令） • 服务器管理员 • 测试警报用户 • 调试命令管理员 • 结构 A 管理员
无	没有分配权限

表. 11: CMC 管理员、高级用户和来宾用户的权限比较

权限集	管理员权限	高级用户权限	来宾用户权限
CMC 登录用户	是	是	是
机箱配置管理员	是	否	否
用户配置管理员	是	否	否
清除日志管理员	是	是	否
机箱控制管理员（电源命令）	是	是	否
服务器管理员	是	是	否
测试警报用户	是	是	否
调试命令管理员	是	否	否
结构 A 管理员	是	是	否

修改根用户管理员帐户设置


为了增强安全性，强烈建议您更改 root（用户 1）帐户的默认密码。root 帐户是 CMC 随附的默认管理帐户。要更改 root 帐户的默认密码，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览**，然后单击**用户验证**。
2. 在**用户**页面的**用户 ID**列中，单击**1**。
 **注:** 用户 ID 1 是 CMC 默认随附的根用户帐户。该帐户无法更改。
3. 在**用户配置**页面中，选择**更改密码**选项。
4. 在**密码**字段中键入新密码，然后在**确认密码**中键入相同的密码。
5. 单击**应用**。即会更改用户 ID 1 的密码。


配置本地用户

您可以在 CMC 中配置多达 16 个具有特定访问权限的本地用户。在创建 CMC 本地用户之前，请验证是否存在当前用户。您可以使用这些用户的权限设置用户名、密码和角色。这些用户名和密码可通过任何 CMC 安全界面（如 Web 界面、RACADM 和 WS-MAN）进行更改。


使用 CMC Web 界面配置本地用户

 **注:** 您必须具有**配置用户**权限才能创建 CMC 用户。


要添加和配置本地 CMC 用户，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览**，然后单击**用户验证**。
2. 在**本地用户**页面的**用户 ID**列中，单击某个用户 ID 号。此时将显示**用户配置**页面。
 **注：**用户 ID 1 是 CMC 默认随附的根用户帐户。该帐户无法更改。
3. 启用用户 ID 并指定用户名、密码和该用户的访问权限。有关选项的更多信息，请参阅**联机帮助**。
4. 单击**应用**。即会创建具有相应权限的用户。

使用 RACADM 配置本地用户


 **注：**必须以 root 用户登录才能在远程 Linux 系统上执行 RACADM 命令。

最多可以在 CMC 属性数据库中配置 16 个用户。手动启用 CMC 用户前，请验证当前用户是否存在。如果配置新 CMC 或使用了 `racadm racresetcfg` 命令，则当前唯一用户为 root，密码为 calvin。`racresetcfg` 子命令将所有配置参数重设为默认值。之前的所有更改将丢失。

 **注：**可以随时启用和禁用用户，并且禁用用户不会从数据库中删除该用户。

要验证某个用户是否存在，请打开到 CMC 的 Telnet/SSH 文本控制台，登录，然后为 1-16 的每个索引键入以下命令一次：

```
racadm getconfig -g cfgUserAdmin -i <index>
```

 **注：**您还可以键入 `racadm getconfig -f <myfile.cfg>`，查看或编辑 **myfile.cfg** 文件，该文件包含所有 CMC 配置参数。

多个参数和对象 ID 会与其当前值一起列出。其中两个重要的对象是：

```
# cfgUserAdminIndex=XX cfgUserAdminUserName=
```

如果 `cfgUserAdminUserName` 对象没有值，则可以使用 `cfgUserAdminIndex` 对象指示的索引编号。如果“=”后显示了名称，该索引即会被此用户名使用。

使用 `racadm config` 子命令手动启用或禁用用户时，必须使用 `-i` 选项指定索引。

命令对象中的“#”字符表示它是一个只读对象。同样，如果您使用 `racadm config -f racadm.cfg` 命令来指定要写入的任意数量的组/对象，则无法指定索引。新用户会添加到第一个可用的索引。这种行为允许使用与主 CMC 相同的设置来配置另一个 CMC，具备更大的灵活性。


使用 RACADM 添加 CMC 用户

要将新用户添加到 CMC 配置，请执行以下操作：

1. 设置用户名。
2. 设置密码。
3. 设置用户权限。有关用户权限的信息，请参阅**用户类型**。
4. 启用用户。

示例：

下面的示例说明如何添加密码为“123456”的新用户“John”，以及 CMC 的登录权限。

 **注：**有关特定用户权限的有效位掩码值的列表，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。默认权限值为 0，这表明用户没有启用权限。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 john racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456 racadm config -g
```

```
cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x00000001 racadm config -g
cfgUserAdmin -i 2 -o cfgUserAdminEnable 1
```

要验证是否成功地为用户添加了正确的权限，请运行以下命令：

```
racadm getconfig -g cfgUserAdmin -i 2
```

有关 RACADM 命令的更多信息，请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

禁用 CMC 用户

使用 RACADM 时，必须以手动方式逐个禁用用户。不能使用配置文件删除用户。

要删除 CMC 用户，命令语法如下：

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <index>"" racadm
config -g cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x0
```

双引号空字符串 ("") 指示 CMC 删除指定索引处的用户配置，然后将用户配置重设为出厂默认值。

启用具有权限的 CMC 用户

启用具有特定管理权限的用户（基于角色的授权）：

1. 使用命令语法找到可用的用户索引：

```
racadm getconfig -g cfgUserAdmin -i <index>
```

2. 使用新用户名和密码键入以下命令。

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <index> <user
privilege bitmask value>
```



注：有关特定用户权限的有效位掩码值列表，请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。默认权限值为 0，即表示用户没有启用任何权限。

配置 Active Directory 用户

如果您的公司使用 Microsoft Active Directory 软件，则可以配置该软件以提供访问 CMC 的权限，从而允许添加和控制目录服务中现有用户的 CMC 用户权限。这是获得许可的功能。



注：在以下操作系统上，您可以使用 Active Directory 识别 CMC 用户。

- Microsoft Windows 2000
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008

您可以通过 Active Directory 配置用户验证以登录到 CMC。您还可以提供基于角色的权限，从而使管理员可以为每位用户配置特定的权限。

支持的 Active Directory 验证机制

您可以通过两种方法使用 Active Directory 定义 CMC 用户访问权限：

- **标准架构解决方案**，仅使用 Microsoft 的默认 Active Directory 组对象。
- **扩展架构解决方案**，拥有 Dell 提供的自定义 Active Directory 对象。所有访问控制对象都在 Active Directory 中维护。它为在具有各种权限级别的不同 CMC 上配置用户访问权限提供了最大的灵活性。

标准架构 Active Directory 概览


如下图所示，为 Active Directory 集成使用标准架构需要在 Active Directory 和 CMC 上都进行配置。

在 Active Directory 中，标准组对象用作角色组。具有 CMC 访问权限的用户属于角色组的成员。要为此用户分配访问特定 CMC 卡的权限，需要在特定 CMC 卡上配置角色组名称及其域名。角色及权限级别在每个 CMC 卡（而不是 Active Directory 中）上进行定义。在每个 CMC 中，您最多可以配置五个角色组。下表显示了默认角色组的权限。

表. 12: 默认角色组权限

角色组	默认权限级别	授予的权限	位掩码
1	无	<ul style="list-style-type: none">CMC 登录用户机箱配置管理员用户配置管理员清除日志管理员机箱控制管理员（电源命令）服务器管理员测试警报用户调试命令管理员结构 A 管理员	0x00000fff
2	无	<ul style="list-style-type: none">CMC 登录用户清除日志管理员机箱控制管理员（电源命令）服务器管理员测试警报用户结构 A 管理员	0x00000ed9
3	无	CMC 登录用户	0x00000001
4	无	没有分配权限	0x00000000
5	无	没有分配权限	0x00000000

 注：“位掩码”值只有在用 RACADM 设置标准架构时才使用。


 注: 有关用户权限的更多信息，请参阅[用户类型](#)。

配置标准架构 Active Directory


要配置 CMC 以进行 Active Directory 登录访问，请执行以下操作：

1. 在 Active Directory 服务器（域控制器）上，打开 **Active Directory 用户和计算机管理单元**。
2. 使用 CMC Web 界面或 RACADM：
 - a) 创建组或选择现有组。
 - b) 配置角色权限。
3. 将 Active Directory 用户作为 Active Directory 组的成员进行添加，使其能够访问 CMC。


使用 CMC Web 界面配置具有标准架构的 Active Directory

 **注:** 有关各字段的信息, 请参阅 *CMC Online Help* (CMC 联机帮助)。

1. 在左侧窗格中, 转至**机箱概览**, 然后单击**用户验证** → **目录服务**。此时将显示**目录服务**页面。
2. 选择 **Microsoft Active Directory (标准架构)**。要为标准架构配置的设置显示在同一页上。
3. 指定以下各项:
 - 启用 Active Directory, 输入根域名称和超时值。
 - 如果要用定向调用搜索域控制器和全局编录, 请选择**搜索 AD 服务器以搜索 (可选)**选项, 然后指定域控制器和全局编录详情。
4. 单击**应用**保存设置。

 **注:** 您必须先应用设置才能继续。如果您不应用这些设置, 则导航至下一页时会丢失这些设置。

5. 在**标准架构设置**部分, 单击**角色组**。此时将显示**配置角色组**页。
6. 为角色组指定组名、域和权限。
7. 单击**应用**保存角色组设置, 然后单击**退回到配置**页。
8. 如果您启用了证书验证, 则必须将域目录林根证书颁发机构签发的证书上传到 CMC。在**管理证书**部分, 键入证书的文件路径, 或浏览到证书文件。单击**上传**将文件上传到 CMC。

 **注:** **文件路径**值显示上传的证书的相对文件路径。必须键入绝对文件路径, 包括全路径和完整文件名及文件扩展名。

域控制器的 SSL 证书必须是由根证书颁发机构签发的证书。访问 CMC 的管理站必须有根证书颁发机构签发的证书。

9. 如果您已经在 **Kerberos Keytab** 部分启用单点登录 (SSO), 请单击**浏览**, 指定 keytab 文件, 然后单击**上传**。上传完成后, 会显示一条消息, 指示上传成功或失败。
10. 单击**应用**。CMC Web 服务器将在单击**应用**后自动重新启动。
11. 注销, 然后登录 CMC 以完成 CMC Active Directory 配置。
12. 在系统树中选择**机箱**, 然后导航到**网络**选项卡。此时将显示**网络配置**页。
13. 如果在**网络设置**下选择了**使用 DHCP (用于 CMC 网络接口 IP 地址)**, 则选择**使用 DHCP 获取 DNS 服务器地址**。
要手动输入 DNS 服务器 IP 地址, 请取消选中**使用 DHCP 获取 DNS 服务器地址**并键入主要和备用 DNS 服务器 IP 地址。
14. 单击**应用更改**。
CMC 标准架构 Active Directory 功能配置完成。

使用 RACADM 配置具有标准架构的 Active Directory


在 RACADM 命令提示符处，运行以下命令：

- 使用 **config** 命令：


```
racadm config -g cfgActiveDirectory -o cfgADEnable 1 racadm config -g
cfgActiveDirectory -o cfgADType 2 racadm config -g cfgStandardSchema -i
<index> -o cfgSSADRoleGroupName <common name of the role group> racadm
config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupDomain <fully
qualified domain name> racadm config -g cfgStandardSchema -i <index> -o
cfgSSADRoleGroupPrivilege <Bit Mask Value for specific RoleGroup
permissions>
```


```
racadm config -g cfgActiveDirectory -o cfgADDomainController1 <fully
qualified domain name or IP address of the domain controller> racadm
config -g cfgActiveDirectory -o cfgADDomainController2 <fully qualified
domain name or IP address of the domain controller> racadm config -g
cfgActiveDirectory -o cfgADDomainController3 <fully qualified domain name
or IP address of the domain controller>
```

 **注：**输入域控制器的 FQDN，而不是域的 FQDN。例如，输入 `servername.dell.com` 而不是 `dell.com`。

 **注：**
至少需要配置三个地址中的一个。CMC 逐一尝试连接到配置的每个地址，直到成功建立连接。
使用标准架构时，这些是用户帐户和角色组所在域控制器的地址。

```
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog1 <fully
qualified domain name or IP address of the domain controller> racadm
config -g cfgActiveDirectory -o cfgADGlobalCatalog2 <fully qualified
domain name or IP address of the domain controller> racadm config -g
cfgActiveDirectory -o cfgADGlobalCatalog3 <fully qualified domain name or
IP address of the domain controller>
```

 **注：**
只有用户帐户和角色组位于不同的域中时，标准架构才需要全局编录服务器。在多个域的情况下，只能使用通用组。

 **注：**
如果您启用了证书验证，则在此字段中指定的 FQDN 或 IP 地址应与域控制器证书的 Subject（主题）或 Subject Alternative Name（主题备用名称）字段相符。

如果要禁用 SSL 握手过程中的证书验证，请运行以下 RACADM 命令：

- 使用 **config** 命令：`racadm config -g cfgActiveDirectory -o
cfgADCertValidationEnable 0`


在此情况下，无需上载认证机构 (CA) 证书。

在 SSL 握手过程中强制执行证书验证（可选）：

- 使用 **config** 命令：`racadm config -g cfgActiveDirectory -o
cfgADCertValidationEnable 1`

在此情况下，必须使用以下 RACADM 命令上载 CA 证书：

```
racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
```

 **注:** 如果证书验证已启用, 请指定域控制器服务器地址和全局编录 FQDN。确保已正确配置 DNS。

扩展架构 Active Directory 概览

使用扩展架构解决方案需要 Active Directory 架构扩展。

Active Directory 架构扩展

Active Directory 数据是属性和类的分布式数据库。Active Directory 架构包含确定可添加或包含在数据库中的数据类型的规则。例如, 数据库中存储的类可以是用户类; 用户类的属性可以是用户的名字、姓氏、电话号码等。

您可以通过添加自己独特的属性和类来扩展 Active Directory 数据库以满足特定需求。Dell 使用 Active Directory 扩展了该架构, 包括必要的更改以支持远程管理验证和授权。

添加到现有 Active Directory 架构的每个属性或类都必须使用唯一的 ID 定义。为了在整个行业内维护唯一的 ID, Microsoft 维护 Active Directory 对象标识符 (OID) 的数据库, 以便公司添加架构扩展时, 可以保证这些扩展唯一并且不会彼此冲突。要在 Microsoft 的 Active Directory 中扩展架构, 对于添加到目录服务中的属性和类, Dell 将收到唯一的 OID、唯一的扩展名和唯一链接的属性 ID。

- Dell 扩展名: dell
- Dell 基础 OID: 1.2.840.113556.1.8000.1280
- RAC LinkID 范围: 12070 至 12079


架构扩展概览

Dell 已扩展架构以包括关联、设备和权限属性。关联属性用于将用户或组与一组特定的权限一起链接到一个或多个 RAC 设备。此模型为网络上有各种用户、RAC 权限和 RAC 设备组合的管理员提供了最大的灵活性, 而无需繁琐操作。

当要与 Active Directory 集成以进行验证和授权的网络上有两个 CMC 时, 为其中每个 CMC 创建至少一个“关联”对象和一个“RAC 设备”对象。可以创建多个“关联”对象, 每个“关联”对象都可以链接到所需的任意多个用户、用户组或“RAC 设备”对象。用户和 RAC 设备对象可以是企业任何域中的成员。

不过, 每个“关联”对象只能链接 (或者可能链接用户、用户组或“RAC 设备”对象) 到一个“权限”对象。此示例允许管理员控制特定 CMC 上的每个用户权限。

RAC 设备对象就是到 RAC 固件的链接, 用于查询 Active Directory 以进行验证和授权。将 RAC 添加到网络后, 管理员必须使用 Active Directory 名称配置 RAC 及其设备对象, 以便用户可以使用 Active Directory 执行验证和授权。此外, 管理员还必须将 RAC 添加到至少一个“关联”对象以使用户能够验证。

 **注:** RAC 权限对象适用于 CMC。

您可以根据需要创建任意多个关联对象。但是, 您必须创建至少一个关联对象, 并且网络上要与 Active Directory 集成的每个 RAC (CMC) 都必须具有一个 RAC 设备对象。

关联对象允许任意多的用户和/或组以及 RAC 设备对象。但是, 每个关联对象仅包括一个权限对象。关联对象可连接在 RAC (CMC) 上拥有权限的用户。

此外, 可以在一个域或多个域中配置 Active Directory 对象。例如, 已有两个 CMC (RAC1 和 RAC2) 和三个现有 Active Directory 用户 (用户 1、用户 2 和用户 3)。您想要授予用户 1 和用户 2 对两个 CMC 的管理员权限并授予用户 3 对 RAC2 卡的登录权限。

添加来自不同域的通用组时, 将创建具有通用范围的关联对象。Dell Schema Extender 公用程序创建的默认关联对象是域本地组, 并且不能与来自其他域的通用组一起使用。

要为单域情况配置对象, 请执行以下操作:

1. 创建两个关联对象。
2. 创建两个“RAC 设备”对象 (RAC1 和 RAC2) 以代表两个 CMC。

3. 创建两个权限对象（权限 1 和权限 2），其中权限 1 具有所有权限（管理员），而权限 2 仅具有登录权限。
4. 将用户 1 和用户 2 归到组 1。
5. 将组 1 添加为关联对象 1 (A01) 的成员，权限 1 作为 A01 的权限对象，而 RAC1 和 RAC2 作为 A01 中的 RAC 设备。
6. 将用户 3 添加为关联对象 2 (A02) 的成员，权限 2 作为 A02 的权限对象，而 RAC2 作为 A02 中的 RAC 设备。

要为多域情况配置对象，请执行以下操作：

1. 确保域目录林功能处于本机或 Windows 2003 模式。
2. 在任意域中创建两个“关联”对象：A01（通用范围）和 A02。图“在多个域中设置 Active Directory 对象”显示域 2 中的对象。
3. 创建两个“RAC 设备”对象（RAC1 和 RAC2）以代表两个 CMC。
4. 创建两个权限对象（权限 1 和权限 2），其中权限 1 具有所有权限（管理员），而权限 2 仅具有登录权限。
5. 将用户 1 和用户 2 分组到组 1。组 1 的组范围必须是通用。
6. 将组 1 添加为关联对象 1 (A01) 的成员，权限 1 作为 A01 的权限对象，而 RAC1 和 RAC2 作为 A01 中的 RAC 设备。
7. 将用户 3 添加为关联对象 2 (A02) 的成员，权限 2 作为 A02 的权限对象，而 RAC2 作为 A02 中的 RAC 设备。

配置扩展架构 Active Directory

要配置 Active Directory 以访问 CMC，请执行以下操作：

1. 扩展 Active Directory 架构。
2. 扩展 Active Directory 用户和计算机管理单元。
3. 将 CMC 用户及其权限添加到 Active Directory。
4. 在各个域控制器上启用 SSL。
5. 使用 CMC Web 界面或 RACADM 配置 CMC Active Directory 属性。

扩展 Active Directory 架构

通过扩展您的 Active Directory 架构，可向 Active Directory 架构添加 Dell 组织单元、架构类和属性，以及示例权限与关联对象。在您扩展架构之前，确保您对域目录林的架构主机灵活单主机操作 (FSMO) 角色拥有者具有架构管理员权限。

可使用以下任一方法扩展架构：

- Dell Schema Extender 公用程序
- LDIF 脚本文件

如果使用 LDIF 脚本文件，则不会将 Dell 组织单元添加到架构中。

LDIF 文件和 Dell Schema Extender 分别位于 *Dell Systems Management Tools and Documentation* DVD 的以下目录中：

- DVDdrive:\SYSTEMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files
- <DVDdrive>\SYSTEMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema Extender

要使用 LDIF 文件，请参阅 LDIF_Files 目录中的发行说明中的说明。

可以从任意位置复制并运行 Schema Extender 或 LDIF 文件。

使用 Dell Schema Extender

 **小心:** Dell Schema Extender 使用 SchemaExtenderOem.ini 文件。要确保 Dell Schema Extender 公用程序正常工作，请勿修改此文件的名称。

1. 在欢迎屏幕中单击下一步。
2. 阅读并了解警告，然后单击下一步。
3. 选择**使用当前登录凭据**或输入具有架构管理员权限的用户名和密码。
4. 单击**下一步**运行 Dell Schema Extender。
5. 单击**完成**。
架构即得到扩展。要验证架构扩展，请使用 MMC 和 Active Directory 架构管理单元验证类和属性是否存在。有关类和属性的更多信息，请参阅[类和属性](#)。有关使用 MMC 和 Active Directory 架构管理单元的更多信息，请参阅 Microsoft 说明文件。

类和属性

表. 13: 添加到 Active Directory 架构中类的类定义

类名称	分配的对象标识号 (OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

表. 14: dellRacDevice 类

OID	1.2.840.113556.1.8000.1280.1.7.1.1
说明	代表 Dell RAC 设备。在 Active Directory 中必须将 RAC 配置为 delliDRACDevice。这种配置使 CMC 可将轻量级目录访问协议 (LDAP) 查询发送到 Active Directory。
类的类型	结构类
超类	dellProduct
属性	dellSchemaVersion dellRacType

表. 15: delliDRACAssociationObject 类

OID	1.2.840.113556.1.8000.1280.1.7.1.2
说明	代表 Dell 关联对象。关联对象用于提供用户与设备之间的连接。
类的类型	结构类
超类	组
属性	dellProductMembers dellPrivilegeMember

表. 16: dellRAC4Privileges 类

OID	1.2.840.113556.1.8000.1280.1.1.1.3
说明	定义 CMC 设备的权限（授权限）。
类的类型	辅助类
超类	无
属性	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsTestAlertUser dellIsDebugCommandAdmin dellPermissionMask1 dellPermissionMask2

表. 17: dellPrivileges 类

OID	1.2.840.113556.1.8000.1280.1.1.1.4
说明	用作 Dell 权限（授权限）的容器类。
类的类型	结构类
超类	用户
属性	dellRAC4Privileges

表. 18: dellProduct 类

OID	1.2.840.113556.1.8000.1280.1.1.1.5
说明	所有 Dell 产品派生所依据的主类。
类的类型	结构类
超类	计算机
属性	dellAssociationMembers

表. 19: 添加到 Active Directory 架构的属性的列表

分配的 OID/语法对象标识符	单值
属性: dellPrivilegeMember 说明: 属于此属性的 dellPrivilege 对象的列表。 OID: 1.2.840.113556.1.8000.1280.1.1.2.1 可分辨名称: (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
属性: dellProductMembers 说明: 属于此角色的 dellRacDevices 对象的列表。此属性是指向 dellAssociationMembers 反向链接的正向链接。 链接 ID: 12070	FALSE

分配的 OID/语法对象标识符	单值
OID: 1.2.840.113556.1.8000.1280.1.1.2.2 可分辨名称: (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
属性: dellIsCardConfigAdmin 说明: 如果用户具有设备的卡配置权限, 则为 TRUE。	TRUE
OID: 1.2.840.113556.1.8000.1280.1.1.2.4 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
属性: dellIsLoginUser 说明: 如果用户具有设备的登录权限, 则为 TRUE。	TRUE
OID: 1.2.840.113556.1.8000.1280.1.1.2.3 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
属性: dellIsUserConfigAdmin 说明: 如果用户具有设备的用户配置管理员权限, 则为 TRUE。	TRUE
OID: 1.2.840.113556.1.8000.1280.1.1.2.5 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
属性: delIsLogClearAdmin 说明: 如果用户具有设备的清除日志管理员权限, 则为 TRUE。	TRUE
OID: 1.2.840.113556.1.8000.1280.1.1.2.6 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
属性: dellIsServerResetUser 说明: 如果用户具有设备的服务器重设权限, 则为 TRUE。	TRUE
OID: 1.2.840.113556.1.8000.1280.1.1.2.7 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
属性: dellIsTestAlertUser 说明: 如果用户具有设备的测试警报用户权限, 则为 TRUE。	TRUE
OID: 1.2.840.113556.1.8000.1280.1.1.2.10 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
属性: dellIsDebugCommandAdmin 说明: 如果用户具有设备的调试命令管理员权限, 则为 TRUE。	TRUE
OID: 1.2.840.113556.1.8000.1280.1.1.2.11 布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
属性: dellSchemaVersion 说明: 当前架构版本用于更新架构。	TRUE
OID: 1.2.840.113556.1.8000.1280.1.1.2.12 忽略大小写字符串 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
属性: dellRacType	TRUE

分配的 OID/语法对象标识符	单值
<p>说明: 此属性是 dellRacDevice 对象的当前 Rac 类型和指向 dellAssociationObjectMembers 正向链接的反向链接。</p> <p>OID: 1.2.840.113556.1.8000.1280.1.1.2.13</p> <p>忽略大小写字符串 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)</p> <p>属性: dellAssociationMembers</p> <p>属性: 属于此产品的 dellAssociationObjectMembers 的列表。此属性是指向 dellProductMembers 链接属性的反向链接。</p> <p>链接 ID: 12071</p> <p>OID: 1.2.840.113556.1.8000.1280.1.1.2.14</p> <p>可分辨名称 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)</p> <p>属性: dellPermissionsMask1</p> <p>OID: 1.2.840.113556.1.8000.1280.1.6.2.1 整数 (LDAPTYPE_INTEGER)</p> <p>属性: dellPermissionsMask2</p> <p>OID: 1.2.840.113556.1.8000.1280.1.6.2.2 整数 (LDAPTYPE_INTEGER)</p>	FALSE

安装用于 Microsoft Active Directory 用户和计算机管理单元的 Dell 扩展

扩展 Active Directory 中的架构时，还必须扩展 Active Directory 用户和计算机管理单元，以使管理员能够管理 RAC (CMC) 设备、用户和用户组、RAC 关联和 RAC 权限。

使用 *Dell Systems Management Tools and Documentation DVD* 安装系统管理软件时，您可以通过在安装过程中选择 **Active Directory 用户和计算机管理单元** 选项来扩展管理单元。有关安装系统管理软件的其他说明，请参阅 *Dell OpenManage Software Quick Installation Guide* (Dell OpenManage 软件快速安装指南)。对于 64 位 Windows 操作系统，管理单元安装程序位于：<DVDdrive>\SYSMGMTManagementStation\support\OMActiveDirectory_SnapIn64

有关 Active Directory 用户和计算机管理单元的更多信息，请参阅 Microsoft 说明文件。

将 CMC 用户和权限添加到 Active Directory

使用 Dell 扩展的 Active Directory 用户和计算机管理单元，您可以通过创建 RAC 设备、关联和权限对象添加 CMC 用户和权限。要添加每个对象，请执行以下操作：

- 创建 RAC 设备对象
- 创建权限对象
- 创建关联对象
- 将对象添加到关联对象


创建 RAC 设备对象

要创建 RAC 设备对象，请执行以下操作：

1. 在 **MMC 控制台根目录** 窗口中，右键单击一个容器。
2. 选择 **新建** → **Dell 高级远程管理对象**。
3. 在 **新建对象** 页面中，键入新对象的名称。该名称必须与您在 [使用 Web 界面以标准架构配置 Active Directory](#) 中键入的 CMC 名称相同。
4. 选择 **RAC 设备对象**，然后单击 **确定**。

创建权限对象

要创建权限对象：

 **注:** 您必须在相关关联对象的同一个域中创建权限对象。

1. 在 **MMC 控制台根目录** 窗口中，右键单击一个容器。
2. 选择 **新建** → **Dell 高级远程管理对象**。
3. 在 **新建对象** 页面中，键入新对象的名称。
4. 选择 **权限对象**，然后单击 **确定**。
5. 右键单击已创建的权限对象，然后选择 **属性**。
6. 单击 **RAC 权限** 选项卡并为用户或组分配权限。有关 CMC 用户权限的更多信息，请参阅 [用户类型](#)。

创建关联对象

关联对象从组派生而来，必须包含组类型。关联范围指定关联对象的安全组类型。创建关联对象时，必须选择适用于要添加的对象类型的关联范围。例如：如果选择“通用”，则关联对象只有在 Active Directory 域以本机模式或更高模式运行时才可用。

要创建关联对象，请执行以下操作：

1. 在 **控制台根目录 (MMC)** 窗口中，右键单击一个容器。
2. 选择 **新建** → **Dell 高级远程管理对象**。
3. 在 **新建对象** 页面中，键入新对象的名称，然后选择 **关联对象**。
4. 选择 **关联对象** 的范围，然后单击 **确定**。

将对象添加到关联对象

使用 **关联对象属性** 窗口可以关联用户或用户组、权限对象和 RAC 设备或 RAC 设备组。如果系统运行 Windows 2000 操作系统或更高版本，请使用“通用组”以涵盖包含您的用户或 RAC 对象的域。

可以添加用户组和 RAC 设备组。

添加用户或用户组

要添加用户或用户组，请执行以下操作：

1. 右键单击 **关联对象** 并选择 **属性**。
2. 选择 **用户** 选项卡并单击 **添加**。
3. 输入用户或用户组名称并单击 **确定**。

添加权限

要添加权限，请执行以下操作：

1. 选择 **权限对象** 选项卡，然后单击 **添加**。
2. 输入权限对象名称并单击 **确定**。
单击 **权限对象** 选项卡以向关联对象添加权限对象，该关联对象定义了针对 RAC 设备验证时用户或用户组的权限。一个关联对象只能添加一个权限对象。


添加 RAC 设备或 RAC 设备组






要添加 RAC 设备或 RAC 设备组，请执行以下操作：

1. 选择 **产品** 选项卡并单击 **添加**。
2. 输入 RAC 设备或 RAC 设备组名称并单击 **确定**。
3. 在 **属性** 窗口中，依次单击 **应用**、**确定**。
单击 **产品** 选项卡将一个或多个 RAC 设备添加到关联设备。关联设备指定连接到网络的 RAC 设备，这些设备对于所定义的用户或用户组可用。可以将多个 RAC 设备添加到关联对象。


使用 CMC Web 界面配置具有扩展架构的 Active Directory

要使用 CMC Web 界面配置具有扩展架构的 Active Directory，请执行以下操作：

 **注：**有关各字段的信息，请参阅[联机帮助](#)。

1. 在左侧窗格中，单击**机箱概览** → **用户验证** → **机箱概览** → **目录服务**。
2. 选择 **Microsoft Active Directory (扩展架构)**。
针对扩展架构配置的设置显示在同一页面上。
3. 指定以下各项：
 - 启用 Active Directory，输入根域名和超时值。
 - 如果要启用定向调用搜索域控制器和全局编录，请选择**搜索 AD 服务器以搜索 (可选)**选项，然后指定域控制器和全局编录详情。
 -  **注：**将 IP 地址设置为 0.0.0.0 时，将禁止 CMC 搜索服务器。
 -  **注：**可以指定逗号分隔的一组域控制器或全局编录服务器。CMC 允许指定多达三个 IP 地址或主机名。
 -  **注：**如果未针对所有域和应用程序正确配置域控制器或全局编录服务器，可能导致在现有应用程序/域运行过程中产生无法预料的结果。
4. 单击**应用**保存设置。
 -  **注：**您必须先应用设置才能继续。如果您不应用这些设置，则导航至下一页时会丢失这些设置。
5. 在**扩展架构设置**部分，键入 CMC 设备名称和域名。
6. 如果您启用了证书验证，则必须将域目录林根证书颁发机构签发的证书上传到 CMC。在**管理证书**部分，键入证书的文件路径，或浏览到证书文件。单击**上传**将文件上传到 CMC。
 -  **注：**文件路径值显示上传的证书的相对文件路径。必须键入绝对文件路径，包括全路径和完整文件名及文件扩展名。

域控制器的 SSL 证书必须是由根证书颁发机构签发的证书。访问 CMC 的管理站必须有根证书颁发机构签发的证书。


 **小心：**默认需要 SSL 证书验证。不建议禁用此证书。
7. 如果您已经在 Kerberos Keytab 部分启用单点登录 (SSO)，请单击**浏览**，指定 keytab 文件，然后单击**上传**。当上传完成时，会显示一条消息，指示上传成功或失败。
8. 单击**应用**。
CMC Web 服务器将在您单击**应用**后自动重新启动。
9. 登录 CMC Web 界面。
10. 在系统树中选择**机箱**，单击**网络**选项卡，然后单击**网络子**选项卡。此时将显示**网络配置**页。
11. 如果启用**对 CMC 网络接口 IP 地址使用 DHCP**，请进行以下任一操作：
 - 选择**使用 DHCP 获取 DNS 服务器地址**使 DHCP 服务器能够自动获取 DNS 服务器地址。
 - 不选中**使用 DHCP 获取 DNS 服务器地址**复选框，然后在提供的字段中键入主和备用 DNS 服务器 IP 地址，手工配置 DNS 服务器 IP 地址。
12. 单击**应用更改**。
扩展架构的 Active Directory 设置配置完成。

使用 RACADM 配置具有扩展架构的 Active Directory

要使用 RACADM 命令配置具有扩展架构的 CMC Active Directory，请打开命令提示符，然后在命令提示符处输入以下命令：


```
racadm config -g cfgActiveDirectory -o cfgADEnable 1 racadm config -g  
cfgActiveDirectory -o cfgADType 1 racadm config -g cfgActiveDirectory -o
```

```
cfgADRRacName <RAC common name> racadm config -g cfgActiveDirectory -o
cfgADRRacDomain <fully qualified rac domain name> racadm config -g
cfgActiveDirectory -o cfgADDomainController1 <fully qualified domain name or IP
Address of the domain controller> racadm config -g cfgActiveDirectory -o
cfgADDomainController2 <fully qualified domain name or IP Address of the domain
controller> racadm config -g cfgActiveDirectory -o cfgADDomainController3
<fully qualified domain name or IP Address of the domain controller>
```

 **注:** 您必须至少配置三个地址中的一个。CMC 逐一尝试连接到每个配置的地址，直到成功建立连接。使用扩展架构时，这些是此 CMC 设备所在位置域控制器的 FQDN 或 IP 地址。

要在握手过程中禁用证书验证，请执行以下命令（可选）：

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
```


 **注:** 在此情况下，您无需上传 CA 证书。

在 SSL 握手过程中强制执行证书验证（可选）：

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

在此情况下，您必须上传 CA 证书：

```
racadm sslcertupload -t 0x2 -f < ADS root CA certificate >
```

 **注:** 如果证书验证已启用，请指定域控制器服务器地址和 FQDN。确保 DNS 已正确配置。

以下 RACADM 命令可选：

```
racadm sslcertdownload -t 0x1 -f <RAC SSL certificate>
```

配置通用 LDAP 用户

CMC 提供通用解决方案来支持基于轻量级目录访问协议 (LDAP) 的验证。此功能不需要在目录服务上进行任何架构扩展。

CMC 管理员现在可在 CMC 中集成 LDAP 服务器用户登录。此集成要求同时在 LDAP 和 CMC 服务器上配置。在 LDAP 服务器上，标准组对象用作角色组。具有 CMC 权限的用户将成为该角色组的成员。权限仍存储在 CMC 中用于验证，工作方式与具有 Active Directory 支持的标准架构设置类似。

若要支持 LDAP 用户访问特定的 CMC 卡，则必须在特定的 CMC 卡上配置角色组名称及其域名。每个 CMC 可配置最多 5 个角色组。用户可选择添加到目录服务内的多个组。如果用户是多个组的成员，则其获得所有所属组的权限。

有关角色组权限级别和默认角色组设置的信息，请参阅[用户类型](#)。

配置通用 LDAP 目录以访问 CMC

CMC 的通用 LDAP 实现在授予用户访问权限时分两阶段 - 先是用户验证，然后是用户授权。

LDAP 用户验证

一些目录服务器要求在特定 LDAP 服务器上进行任何搜索前完成绑定。

要验证用户，请执行以下操作：

1. 可以选择绑定到目录服务。默认为匿名绑定。
2. 根据用户登录搜索用户。默认属性为 uid。如果找到一个以上的对象，则该过程返回错误。
3. 解除绑定并以用户的 DN 和密码执行绑定。如果系统无法进行绑定，则登录将会失败。
4. 如果这些步骤成功完成，则用户通过验证。


LDAP 用户的授权

要对用户授权，请执行以下操作：


1. 在每个已配置的组中搜索该用户在 `member` 或 `uniqueMember` 属性中的域名。管理员可以配置用户域。
2. 对于该用户所属的每个用户组，授予该用户相应的用户访问权限和特权。

使用 CMC Web 界面配置通用 LDAP 目录服务

要配置通用 LDAP 目录服务，请执行以下操作：

 **注：**您必须具有**机箱配置管理员**权限。

1. 在左侧窗格中，单击**机箱概览** → **用户验证** → **目录服务**。
2. 选择**通用 LDAP**。
在同一页面上会显示可以为标准架构配置的设置。
3. 指定以下各项：

 **注：**有关各字段的信息，请参阅**联机帮助**。

- 常见设置

- 使用 LDAP 的服务器：

- * 静态服务器 - 指定 FQDN 或 IP 地址和 LDAP 端口号。
- * DNS 服务器 - 指定 DNS 服务器，以通过搜索其在 DNS 内的 SRV 记录来检索 LDAP 服务器列表。

为 SRV 记录执行以下 DNS 查询：


```
_[Service Name]._tcp.[Search Domain]
```

其中 `<Search Domain>` 是查询中使用的根级别域而 `<Service Name>` 是查询中使用的服务名称。

例如：

```
_ldap._tcp.dell.com
```


其中 `ldap` 是服务名称而 `dell.com` 是搜索域。

4. 单击**应用**保存设置。
 **注：**您必须先应用设置才能继续。如果您不应用这些设置，则导航至下一页时会丢失这些设置。
5. 在**组设置**部分，单击**角色组**。
6. 在**配置 LDAP 角色组**页面中，指定角色组的组域名和权限。
7. 单击**应用**保存角色组设置，单击**退回到配置页**，然后选择**通用 LDAP**。
8. 如果您选择了**启用 SSL 证书验证**选项，则在**管理证书**部分，指定 CA 证书以在 SSL 握手期间验证 LDAP 服务器证书，然后单击**上传**。证书便上传到 CMC 并会显示详细信息。
9. 单击**应用**。
通用 LDAP 目录服务即配置完成。

使用 RACADM 配置通用 LDAP 目录服务

要配置 LDAP 目录服务，请使用 `cfgLdap` 和 `cfgLdapRoleGroup` RACADM 组中的对象。

配置 LDAP 登录有多个选项。大多数情况下部分选项可使用其默认设置。

 **注:** 强烈建议使用 `racadm testfeature -f LDAP` 命令在第一次设置时测试 LDAP 设置。此功能支持 IPv4 和 IPv6。

所需属性更改包括启用 LDAP 登录、设置服务器 FQDN 或 IP 以及配置 LDAP 服务器的基础 DN。

- `$ racadm config -g cfgLDAP -o cfgLDAPEnable 1`
- `$ racadm config -g cfgLDAP -o cfgLDAPServer 192.168.0.1`
- `$ racadm config -g cfgLDAP -o cfgLDAPBaseDN dc= company,dc=com`

可对 CMC 进行配置，使其查询 DNS 服务器上的 SRV 记录（可选）。如果 `cfgLDAPSRVLookupEnable` 属性启用，则忽略 `cfgLDAPServer` 属性。以下查询可用于搜索 DNS 中的 SRV 记录：

```
_ldap._tcp.domainname.com
```

`ldap` 在上述查询中为 `cfgLDAPSRVLookupServiceName` 属性。

`cfgLDAPSRVLookupDomainName` 配置为 **domainname.com**。


有关 RACADM 命令的更多信息，请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

配置 CMC 进行单点登录或智能卡登录

此部分为 Active Directory 用户提供配置 CMC 进行智能卡登录和单点登录 (SSO) 的信息。

SSO 使用 Kerberos 作为验证方法，使已经登录的用户可以自动或单点登录到 Exchange 等后续应用程序。对于单点登录，CMC 使用客户端系统的凭据，您使用有效的 Active Directory 帐户登录之后，操作系统就会缓存这些凭据。

双重验证提供了更高级别的安全性，要求用户具有密码或 PIN 以及含有私钥或数字证书的实物卡。Kerberos 使用此双重验证机制来让系统可以证明用户的真实性。

 **注:** 选择登录方法不会设置与诸如 SSH 等其他登录界面相关的策略属性。您还必须设置其他登录界面的其他策略属性。如果您要禁用所有其他登录界面，请导航至 **服务** 页面并禁用所有（或某些）登录界面。

Microsoft Windows 2000、Windows XP、Windows Server 2003、Windows Vista、Windows 7 和 Windows Server 2008 可以使用 Kerberos 作为 SSO 和智能卡登录的验证机制。

有关 Kerberos 的信息，请参阅 Microsoft 网站。

系统要求

要使用 Kerberos 验证方法，网络必须包括：

- DNS 服务器
- Microsoft Active Directory 服务器

 **注:** 如果您使用 Windows 2003 上的 Active Directory，应确保客户端系统上安装了最新的 Service Pack 和增补软件。如果您使用 Windows 2008 上的 Active Directory，应确保安装了 SP1 和以下热补丁：
用于 KTPASS 公用程序的 **Windows6.0-KB951191-x86.msu**。如果没有此增补软件，该公用程序会生成错误 Keytab 文件。

Windows6.0-KB957072-x86.msu，用作在 LDAP 绑定过程中使用 GSS_API 和 SSL 事务处理。

- Kerberos Key Distribution Center（与 Active Directory Server 软件一起打包）。
- DHCP 服务器（推荐）。
- DNS 服务器反向区域必须有 Active Directory 服务器和 CMC 的条目。

客户端系统

- 对于只通过智能卡的登录，客户端系统必须具有 Microsoft Visual C++ 2005 Redistributable。有关更多信息，请参阅 www.microsoft.com/downloads/details.aspx?FamilyID=32BC1BEEA3F9-4C13-9C99-220B62A191EE&displaylang=en
- 对于单点登录或智能卡登录，客户端系统必须是 Active Directory 域和 Kerberos 领域的一部分。

CMC

- 每个 CMC 都必须有 Active Directory 帐户。
- CMC 必须是 Active Directory 域和 Kerberos 领域的一部分。

单点登录或智能卡登录的前提条件

配置 SSO 或智能卡登录的前提条件包括：

- 为 Active Directory (ksetup) 设置 kerberos 领域和密钥分发中心。
- 强健的 NTP 和 DNS 基础结构以避免时钟漂移和反向查询出现问题。
- 使用包含授权成员的 Active Directory 标准架构角色组配置 CMC。
- 对于智能卡，为每个 CMC 创建 Active Directory 用户，配置为使用 Kerberos DES 加密，而不是预验证。
- 配置浏览器实现 SSO 或智能卡登录。
- 使用 Ktpass 在密钥分发中心注册 CMC 用户（这也会将密钥上传到 CMC）。

生成 Kerberos Keytab 文件


为了支持 SSO 和智能卡登录验证，CMC 支持 Windows Kerberos 网络。ktpass 工具（Microsoft 在服务器安装 CD/DVD 中提供）用于创建与用户帐户的服务主体名称 (SPN) 绑定并将信任信息导出到 MIT-style Kerberos keytab 文件。有关 ktpass 公用程序的更多信息，请参阅 Microsoft 网站。

生成 keytab 文件之前，您必须创建一个 Active Directory 用户帐户，以便与 ktpass 命令的 **-mapuser** 选项一起使用。您必须使用与上载生成的 keytab 文件的 CMC DNS 名称相同的名称。


使用 ktpass 工具生成 keytab 文件：

1. 在希望将 CMC 映射到 Active Directory 中的用户帐户的域控制器（Active Directory 服务器）上运行 *ktpass* 公用程序。
2. 使用以下 ktpass 命令创建 Kerberos keytab 文件：

```
C:\>ktpass -princ HTTP/cmcname.domain_name.com@REALM_NAME.COM -mapuser  
dracname -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass * -out c:  
\krbkeytab
```

 **注：**RFC 要求 cmcname.domainname.com 必须小写，而 @REALM_NAME 必须大写。此外，CMC 支持 Kerberos 验证的 DES-CBC-MD5 类型的加密。

所生成的 keytab 文件必须上载到 CMC。

 **注：**keytab 包含加密密钥，必须妥善保管。有关 *ktpass* 公用程序的更多信息，请参阅 [Microsoft 网站](#)。


配置 CMC 以使用 Active Directory 架构

有关配置 CMC 以使用 Active Directory 标准架构的信息，请参阅[配置标准架构 Active Directory](#)。

有关配置 CMC 以使用扩展架构 Active Directory 的信息，请参阅[扩展架构 Active Directory 概览](#)。

配置浏览器以使用 SSO 登录


Internet Explorer 版本 6.0 和更高版本及 Firefox 版本 3.0 和更高版本支持单点登录 (SSO)。

 **注：**仅当 CMC 结合 Kerberos 验证使用单点登录时，以下说明才适用。

Internet Explorer

要配置 Internet Explorer 进行单点登录，请执行以下操作：

1. 在 Internet Explorer 中，选择**工具** → **Internet 选项**。
2. 在**安全**选项卡上的**选择要查看或更改安全设置的区域**下面，选择**本地 Intranet**。
3. 单击**站点**。
此时将显示**本地 Intranet**对话框。
4. 单击**高级**。
此时将显示**本地 Intranet 高级设置**对话框。
5. 在**将该网站添加到区域**中，键入 CMC 的名称和它所属的域，然后单击**添加**。

 **注：**您可以使用通配符 (*) 指定该域中的所有设备或用户。

Mozilla Firefox

1. 在 Firefox 中的“地址”栏中键入 **about:config**。
 **注：**如果浏览器显示**这样可能会失去质保警告**，请单击**我保证会小心**。
2. 在**筛选器**文本框中，键入 **negotiate**。
浏览器将显示首选项名称的列表，这些名称必须包含单词 negotiate。
3. 在该列表中，双击 **network.negotiate-auth.trusted-uris**。
4. 在**输入字符串值**对话框中，键入 CMC 的域名并单击**确定**。

配置浏览器以使用智能卡登录


Internet Explorer - 确保将 Internet 浏览器配置为下载 Active-X 插件。

为 Active Directory 用户配置 CMC SSO 或智能卡登录

您可以使用 CMC Web 界面或 RACADM 配置 CMC SSO 或智能卡登录。


使用 Web 界面为 Active Directory 用户配置 CMC SSO 登录或智能卡登录

要配置 CMC 的 Active Directory SSO 登录或智能卡登录，请执行以下操作：

 **注:** 有关各选项的信息, 请参阅 [联机帮助](#)。

1. 在配置 Active Directory 设置用户帐户时, 请执行以下附加步骤:

- 上载 Keytab 文件。
- 要启用 SSO, 请选择 **启用单点登录** 选项。
- 要启用智能卡登录, 请选择 **启用智能卡登录** 选项。

 **注:** 如果选择了这两个选项, 所有命令行带外接口, 包括 Secure Shell (SSH)、Telnet、串行和远程 RACADM 都保持不变。

2. 单击 **应用**。

将保存设置。

您可以使用 RACADM 命令测试使用 Kerberos 验证的 Active Directory:

```
testfeature -f adkrb -u <user>@<domain>
```

其中 *<user>* 是有效的 Active Directory 用户帐户。

命令成功表示 CMC 能够获得 Kerberos 凭据和访问用户的 Active Directory 帐户。如果命令不成功, 则解决错误并再次运行该命令。有关更多信息, 请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南)。

上载 Keytab 文件

Kerberos Keytab 文件用作 CMC 对于 Kerberos Data Center (KDC) 的用户名和密码凭据, KDC 又允许访问 Active Directory。Kerberos 领域中的每个 CMC 都必须在 Active Directory 注册, 而且必须有唯一的 Keytab 文件。

您可以上载在关联 Active Directory 服务器上生成的 Kerberos Keytab。您可以通过执行 **ktpass.exe** 公用程序从 Active Directory 服务器生成 Kerberos Keytab。此 keytab 会在 Active Directory 服务器和 CMC 之间建立真正的关系。

要上载 Keytab 文件, 请执行以下操作:

1. 在左侧窗格中, 单击 **机箱概览** → **用户验证** → **目录服务**。
2. 选择 **Microsoft Active Directory (标准架构)**。
3. 在 **Kerberos Keytab** 部分, 单击 **浏览**, 选择 keytab 文件, 然后单击 **上载**。

上载完成后, 会显示一条消息, 指出是否成功上载 keytab 文件。

使用 RACADM 为 Active Directory 用户配置 CMC SSO 登录或智能卡登录

除了配置 Active Directory 时执行的步骤以外, 还可运行以下命令启用 SSO:

```
racadm -g cfgActiveDirectory -o cfgADSSOEnable 1
```

除了配置 Active Directory 时执行的步骤以外, 还可使用以下对象启用智能卡登录:

- `cfgSmartCardLogonEnable`
- `cfgSmartCardCRLEnable`

配置 CMC 以使用命令行控制台

本部分提供有关 CMC 命令行控制台（或串行/Telnet/Secure Shell 控制台）功能的信息，并介绍如何设置系统以通过控制台执行系统管理操作。有关通过命令行控制台在 CMC 中使用 RACADM 命令的信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

CMC 命令行控制台功能

CMC 支持以下串行、Telnet 和 SSH 控制台功能：

- 一个串行客户端连接和最多四个并发 Telnet 客户端连接。
- 最多四个并发 Secure Shell (SSH) 客户端连接。
- RACADM 命令支持。
- 内置 connect 命令用于连接到服务器和 I/O 模块的串行控制台；也可使用 `racadm connect`。
- 命令行编辑和历史。
- 在所有控制台界面上的会话超时控制。

CMC 命令行界面命令

当连接到 CMC 命令行时，可以输入这些命令：

表. 20: CMC 命令行命令

命令	说明
<code>racadm</code>	RACADM 命令以关键字 <code>racadm</code> 开头，后接一个子命令。有关更多信息，请参阅 <i>Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide</i> （Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。
<code>connect</code>	连接到服务器或 I/O 模块的串行控制台。有关更多信息，请参阅 使用 Connect 命令连接到服务器或 I/O 模块 。  注: 您还可以使用 <code>connect RACADM</code> 命令。
<code>exit</code> 、 <code>logout</code> 和 <code>quit</code>	所有这些命令都执行相同操作，即结束当前会话并返回登录命令行界面。

将 Telnet 控制台与 CMC 配合使用


一次最多可以将四个 Telnet 会话与 CMC 配合使用。

如果管理站在运行 Microsoft Windows XP 或 Microsoft Windows Server 2003，则可能会在 CMC Telnet 会话中遇到字符问题。此问题会以冻结登录的方式发生，在这种情况下，回车键无响应并且不显示密码提示。


要修复此问题，请从 support.microsoft.com 下载热修复程序 824810。有关更多信息，也可参阅 Microsoft 知识库文章 824810。

将 SSH 与 CMC 配合使用

SSH 是一种命令行会话，包含与 Telnet 会话相同的功能，但还包含会话协商和加密功能以增强安全性。CMC 支持具有密码验证功能的 SSH 版本 2。CMC 上默认启用 SSH。

 **注:** CMC 不支持 SSH 版本 1。

如果在 CMC 登录过程中出现错误，SSH 客户端就会发出一条错误消息。此消息文本取决于客户端，不受 CMC 控制。查看 RACLog 消息以确定故障原因。

 **注:** 在 Windows 上，必须从 VT100 或 ANSI 终端仿真程序运行 OpenSSH。也可使用 **Putty.exe** 运行 OpenSSH。在 Windows 命令提示符处运行 OpenSSH 不能提供完整的功能（即有些键不响应并且不显示图形）。对于运行 Linux 的服务器，运行 SSH 客户端服务以使用任何 Shell 连接到 CMC。

同时支持四个并发 SSH 会话。通过 `cfgSsnMgtSshIdleTimeout` 属性控制会话超时。有关 RACADM 命令的更多信息，请参阅 dell.com/support/Manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

CMC 还支持通过 SSH 的公共密钥验证 (PKA)。此验证方法不再需要嵌入或提示输入用户 ID/密码，从而提高 SSH 脚本的自动化程度。有关更多信息，请参阅 [配置通过 SSH 的公共密钥验证](#)。

SSH 默认为启用。如果禁用了 SSH，可使用任何其他支持的界面启用。

要配置 SSH，请参阅 [配置服务](#)。

支持的 SSH 加密方案


要使用 SSH 协议与 CMC 通信，它支持下表中列出的多种加密方案。

表. 21: 加密方案

方案类型	方案
非对称加密	Diffie-Hellman DSA/DSS 512 – 1024（随机）位/NIST 规范
对称加密	<ul style="list-style-type: none">• AES256-CBC• RIJNDAEL256-CBC• AES192-CBC• RIJNDAEL192-CBC• AES128-CBC• RIJNDAEL128-CBC• BLOWFISH-128-CBC• 3DES-192-CBC• ARCFOUR-128
消息完整性	<ul style="list-style-type: none">• HMAC-SHA1-160• HMAC-SHA1-96• HMAC-MD5-128• HMAC-MD5-96
验证	密码

配置通过 SSH 的公共密钥验证

最多可以配置 6 个公共密钥，通过 SSH 接口与服务用户名一起使用。添加或删除公共密钥之前，务必使用 `view` 命令查看已设置了哪些密钥，这样就不会无意中覆盖或删除密钥。服务用户名是特殊用户帐户，可在通过 SSH 访问 CMC 时使用。在设置和正确使用 SSH 上的 PKA 时，无需输入用户名或密码即可登录到 CMC。这对于设置执行各种功能的自动化脚本非常有用。

 **注:** 不支持使用任何 GUI 管理此功能，您只能使用 RACADM。

添加新公共密钥时，确保现有密钥没有位于添加新密钥的索引处。CMC 在添加新密钥之前不检查是否删除了以前的密钥。添加了新密钥后，只要启用了 SSH 接口，新密钥就自动生效。

使用公共密钥的公共密钥注释部分时，请记住 CMC 仅使用前 16 个字符。在使用 RACADM `getssninfo` 命令时，CMC 使用公共密钥注释区分 SSH 用户，因为所有 PKA 用户均使用服务用户名登录。

例如，如果设置了两个公共密钥，一个公共密钥的注释是 PC1，另一个的注释是 PC2:

```
racadm getssninfo Type User IP Address Login Date/Time SSH PC1 x.x.x.x
06/16/2009 09:00:00 SSH PC2 x.x.x.x 06/16/2009 09:00:00
```

有关 `sshpkauth` 的更多信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南)。


为运行 Windows 的系统生成公共密钥

在添加帐户之前，通过 SSH 访问 CMC 的系统需要公共密钥。有两种方法可生成公共/私人密钥对：对于运行 Windows 的客户端使用 PuTTY Key Generator 应用程序，对于运行 Linux 的客户端使用 `ssh-keygen` CLI。

本节介绍使用这两个应用程序生成公共/私人密钥对的简单说明。有关这些工具的其他用法或高级用法，请参阅应用程序帮助。

要使用 PuTTY Key Generator 为运行 Windows 的客户端创建基本密钥，请执行以下操作：

1. 启动应用程序，根据要生成的密钥类型（不支持 SSH-1）选择 SSH-2 RSA 或 SSH-2 DSA。
2. 输入密钥的位数。位数应介于 768 和 4096 之间。

 **注:** 如果您添加的密钥小于 768 或大于 4096 位，CMC 可能不会显示消息，但在您尝试登录时，这些密钥会失败。

3. 单击**生成**，按指示在窗口中移动鼠标。
创建密钥后，您可以修改密钥注释字段。
还可以输入密码短语，来保证密钥的安全。确保将私人密钥保存起来。
4. 使用公共密钥时，有两个选项：
 - 将公共密钥保存到文件中以便稍后上载。
 - 使用文本选项添加帐户时，从**供粘贴的公共密钥**窗口中复制和粘贴文本。

为运行 Linux 的系统生成公共密钥

适用于 Linux 客户端的 `ssh-keygen` 应用程序是不带图形用户界面的命令行工具。打开终端窗口，然后在 Shell 提示符处键入：

```
ssh-keygen -t rsa -b 1024 -C testing
```

其中，

- `t` 必须为 `dsa` 或 `rsa`。
- `b` 指定介于 768 和 4096 之间的加密位数。
- `c` 允许修改公共密钥注释，并且是可选的。

<passphrase> 是可选的。命令完成后，使用公共文件传递到 RACADM 以便上传文件。

CMC 的 RACADM 语法注释

在使用 `racadm sshpkauth` 命令时确保：

- 对于 `-i` 选项，参数必须为 `svcacct`。`-i` 的所有其他参数都会在 CMC 中失败。`svcacct` 是 CMC 中基于 SSH 的公共密钥验证的特殊帐户。
- 若要登录到 CMC，用户必须为服务。其他类别的用户可使用 `sshpkauth` 命令访问输入的公共密钥。

查看公共密钥

要查看已经添加到 CMC 的公共密钥，请键入：

```
racadm sshpkauth -i svcacct -k all -v
```


要一次仅查看一个密钥，请将 `all` 替换为 1-6 中的一个数字。例如，要查看密钥 2，请键入：

```
racadm sshpkauth -i svcacct -k 2 -v
```

添加公共密钥

要使用文件上载 `-f` 选项将公共密钥添加至 CMC，请在命令行界面控制台中输入：

```
racadm sshpkauth -i svcacct -k 1 -p 0xffff -f <public key file>
```

 **注：**只有远程 RACADM 才允许使用文件上载选项。有关更多信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

要使用文本上载选项添加公共密钥，请输入：

```
racadm sshpkauth -i svcacct -k 1 -p 0xffff -t "<public key text>"
```

删除公共密钥

要删除某个公共密钥，请运行以下命令：

```
racadm sshpkauth -i svcacct -k 1 -d
```

要删除所有公共密钥，请运行以下命令：

```
racadm sshpkauth -i svcacct -k all -d
```

配置终端仿真软件

CMC 支持在运行以下某种终端仿真软件的管理站上使用串行文本控制台：

- Linux Minicom。
- Hilgraeve's HyperTerminal Private Edition（版本 6.3）。

完成以下小节中的任务以配置所需类型的终端软件。

配置 Linux Minicom

Minicom 是 Linux 的串行端口访问公用程序。以下步骤适用于配置 Minicom 版本 2.0。其他 Minicom 版本的配置步骤可能略有不同，但需要相同的基本设置。要配置 Minicom 的其他版本，请参阅本用户指南的“必需的 Minicom 设置”部分中的信息。

配置 Minicom 版本 2.0

 **注:** 为了获得最佳效果，将 `cfgSerialConsoleColumns` 属性设置为与列数匹配。请注意，提示符会占用两个字符。例如，对于 80 列的终端窗口：

```
racadm config -g cfgSerial -o cfgSerialConsoleColumns 80。
```

1. 如果没有 Minicom 配置文件，请转至下一步。如果您有 Minicom 配置文件，请键入 `minicom<Minicom config file name>`，然后转至步骤 12。
2. 在 Linux 命令提示符处，键入 `minicom -s`。
3. 选择 **串行端口设置** 并按 <Enter> 键。
4. 按 <a> 并选择相应的串行设备（例如，`/dev/ttyS0`）。
5. 按 <e> 并将 **Bps/Par/Bits（速率/奇偶校验位/数据位和停止位）** 选项设置为 **115200 8N1**。
6. 按 <f>，然后将 **硬件流量控制** 设置为 **是**，将 **软件流量控制** 设计为 **否**。要退出 **串行端口设置** 菜单，请按 <Enter>。
7. 选择 **调制解调器和拨号** 并按 <Enter>。
8. 在 **调制解调器拨号和参数设置** 菜单中，按 <Backspace> 清除 **初始化、重设、连接和挂断** 设置以使它们保留为空白，然后按 <Enter> 保存每个空白值。
9. 清除完所有指定字段后，按 <Enter> 退出 **调制解调器拨号和参数设置** 菜单。
10. 选择 **从 Minicom 退出** 并按 <Enter>。
11. 在命令解释程序提示符下，键入 `minicom <Minicom 配置文件名>`。
12. 要退出 Minicom，请按 <Ctrl><a>、<x>、<Enter>。

确保 Minicom 窗口显示一个登录提示符。如果显示登录提示符，说明连接成功。现在就可以登录和访问 CMC 命令行界面。

必需的 Minicom 设置

请参阅下表来配置任何版本的 Minicom。

表. 22: Minicom 设置

设置说明	所需设置
Bps/Par/Bits（速率/奇偶校验位/数据位和停止位）	115200 8N1
硬件流量控制	是
软件流量控制	否
终端仿真	ANSI
调制解调器拨号和参数设置	清除 初始化、重设、连接和挂断 设置以使它们保留为空白


使用 Connect 命令连接到服务器或 I/O 模块


CMC 可建立一个连接，以重定向服务器或 I/O 模块的串行控制台。


对于服务器，串行控制台重定向可以使用以下方法完成：

- CMC 命令行界面 (CLI) 或 `RACADM connect` 命令。有关运行 `RACADM` 命令的更多信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。
- iDRAC Web 界面串行控制台重定向功能。
- iDRAC Serial Over LAN (SOL) 功能。

在串行、Telnet、SSH 控制台中，CMC 支持 `connect` 命令以建立到服务器或 I/O 模块的串行连接。服务器串行控制台既包含 BIOS 引导和设置屏幕，也包含操作系统串行控制台。对于 I/O 模块，可使用交换机串行控制台。在机箱上有单个 IOM。

 **小心:** 从 CMC 串行控制台运行时，`connect -b` 选项将保持连接状态，直到 CMC 重设为止。此连接具有潜在的安全风险。

 **注:** `connect` 命令提供了 `-b`（二进制）选项。此 `-b` 选项传递原始二进制数据，而不使用 `cfgSerialConsoleQuitKey`。此外，当使用 CMC 串行控制台连接到服务器时，DTR 信号中的过渡（例如，如果卸下串行电缆而连接调试器）不会导致退出应用程序。

 **注:** 如果 IOM 不支持控制台重定向，则 `connect` 命令会显示闲置的控制台。在这种情况下，要返回到 CMC 控制台，请键入转义序列。默认控制台转义序列为 `<Ctrl><\>`。

要连接到 IOM，请执行以下命令：


```
connect switch-n
```


其中 `n` 为 IOM 标签 A1。

在 `connect` 命令中引用 IOM 时，IOM 将按照下表所示映射到交换机。

表. 23: 将 I/O 模块映射到交换机


I/O 模块标签	交换机
A1	交换机 a1 或交换机 1


 **注:** 每个机箱同一时间只能有一个 IOM 连接。

 **注:** 不能从串行控制台连接到直通设备。

要连接到管理服务器的串行控制台，请运行 `connect server-n` 命令，其中 `n` 为 1-4。也可以使用 `racadm connect server-n` 命令。使用 `-b` 选项连接到服务器时，假定为二进制通信且转义字符被禁用。如果 iDRAC 不可用，则会显示 `No route to host`（没有至主机的路由）错误消息。

`connect server-n` 命令允许用户访问服务器的串行端口。建立此连接后，用户能够看到服务器通过 CMC 串行端口的控制台重定向，该端口既包括 BIOS 串行控制台，也包括操作系统串行控制台。

 **注:** 要查看 BIOS 引导屏幕，必须在服务器的 BIOS 设置中启用串行重定向。此外，必须将终端仿真程序窗口设置为 80x25。否则，页面上的字符将无法正常显示。

 **注:** 在 BIOS 设置页面中，并非所有键都起作用。因此需提供针对 `<Ctrl>+<Alt>+<Delete>` 和其他键的相应键盘快捷键。初始重定向屏幕显示所需的键盘快捷键。

为串行控制台重定向配置管理服务器 BIOS

您可以使用 iDRAC7 Web 界面通过远程控制台会话连接到管理系统（请参阅 dell.com/support/manuals 上的 *iDRAC7 用户指南*）。

默认情况下，BIOS 中的串行通信为关闭。要将主机文本控制台数据重定向到 Serial over LAN，必须启用通过 COM1 进行控制台重定向。要更改 BIOS 设置，请执行以下操作：

1. 打开管理服务器电源。
2. 在开机自检过程中，按 `<F2>` 键进入 BIOS 设置公用程序。

3. 转到**串行通信**，然后按 <Enter> 键。在对话框中，串行通信列表将显示以下选项：

- 关
- 开，控制台重定向不启用
- 开，通过 COM1 进行控制台重定向

要在这些选项之间导航，请按相应的箭头键。

 **注：**确保选中了**开，通过 COM1 进行控制台重定向**选项。

4. 启用**引导后重定向**，默认值为**禁用**。选择此选项后，可在后续的重新引导后进行 BIOS 控制台重定向。


5. 保存更改并退出。
管理系统重新启动。

配置 Windows 进行串行控制台重定向

对于运行 Microsoft Windows Server（Windows Server 2003 以上版本）的服务器，不必进行任何配置。Windows 会接收来自 BIOS 的信息，并启用特别管理控制台 (SAC) 的一号控制台 COM1。

配置 Linux 在引导期间进行服务器串行控制台重定向

以下步骤特定于 Linux GRand Unified Bootloader (GRUB)。使用不同的引导加载程序需要类似的更改。

 **注：**在配置客户端 VT100 仿真窗口时，将显示重定向控制台的窗口或应用程序设置为 25 行 x 80 列，以确保文本正确显示。否则，有些文本屏幕可能会出现乱码。

按照以下说明编辑 `/etc/grub.conf` 文件：

1. 找到文件的常规设置部分并键入以下两个新行：

```
serial --unit=1 --speed=57600 terminal --timeout=10 serial
```

2. 在内核行上追加两个选项：

```
kernel console=ttyS1,57600
```

3. 如果 `/etc/grub.conf` 包含 `splashimage` 指令，应将其注释掉。

以下示例显示了此过程中说明的更改。

```
# grub.conf generated by anaconda # # Note that you do not have to rerun
grub after making changes # to this file # NOTICE: You do not have a /boot
partition. This means that # all kernel and initrd paths are relative to /,
e.g. # root (hd0,0) # kernel /boot/vmlinuz-version ro root= /dev/sda1 #
initrd /boot/initrd-version.img # #boot=/dev/sda default=0 timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz serial --unit=1 --speed=57600 terminal --timeout=10
serial title Red Hat Linux Advanced Server (2.4.9-e.3smp) root (hd0,0) kernel /
boot/vmlinuz-2.4.9-e.3smp ro root= /dev/sda1 hda=ide-scsi console=ttyS0
console= ttyS1,57600 initrd /boot/initrd-2.4.9-e.3smp.img title Red Hat
Linux Advanced Server-up (2.4.9-e.3) root (hd0,00) kernel /boot/
vmlinuz-2.4.9-e.3 ro root=/dev/sda1 initrd /boot/initrd-2.4.9-e.3.img
```

按照以下原则编辑 `/etc/grub.conf` 文件：

- 禁用 GRUB 的图形界面并使用基于文本的界面。否则，GRUB 屏幕不会在控制台重定向中显示。要禁用图形界面，请注释掉以 `splashimage` 开头的行。
- 要使用多个 GRUB 选项来通过串行连接启动控制台会话，将以下行添加到所有选项：

```
console=ttyS1,57600
```

此示例显示 `console=ttyS1,57600` 仅添加到第一个选项。

配置 Linux 在引导后进行服务器串行控制台重定向

按照以下说明编辑文件 `/etc/inittab`:

添加新行以在 COM2 串行端口上配置 `agetty`:

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

下例显示了带有新行的文件。

```
# # inittab This file describes how the INIT process # should set up the system
in a certain # run-level. # # Author: Miquel van Smoorenburg # Modified for RHS
Linux by Marc Ewing and # Donnie Barnes # # Default runlevel. The runlevels
used by RHS are: # 0 - halt (Do NOT set initdefault to this) # 1 - Single user
mode # 2 - Multiuser, without NFS (The same as 3, if you # do not have
networking) # 3 - Full multiuser mode # 4 - unused # 5 - X11 # 6 - reboot (Do
NOT set initdefault to this) # id:3:initdefault: # System initialization.
si::sysinit:/etc/rc.d/rc.sysinit 10:0:wait:/etc/rc.d/rc 0 11:1:wait:/etc/
rc.d/rc 1 12:2:wait:/etc/rc.d/rc 2 13:3:wait:/etc/rc.d/rc 3 14:4:wait:/etc/
rc.d/rc 4 15:5:wait:/etc/rc.d/rc 5 16:6:wait:/etc/rc.d/rc 6 # Things to run in
every runlevel. ud::once:/sbin/update # Trap CTRL-ALT-DELETE ca::ctrlaltdel:/
sbin/shutdown -t3 -r now # When our UPS tells us power has failed, assume we
have a few # minutes of power left. Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have power installed and your # UPS is
connected and working correctly. pf::powerfail:/sbin/shutdown -f -h +2 "Power
Failure; System Shutting Down" # If power was restored before the shutdown
kicked in, cancel it. pr:12345:powerokwait:/sbin/shutdown -c "Power Restored;
Shutdown Cancelled" # Run gettys in standard runlevels co:2345:respawn:/sbin/agetty -h -L
57600 ttyS1 ansi 1:2345:respawn:/sbin/mingetty tty1 2:2345:respawn:/sbin/mingetty
tty2 3:2345:respawn:/sbin/mingetty tty3 4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5 6:2345:respawn:/sbin/mingetty tty6 # Run xdm
in runlevel 5 # xdm is now a separate service x:5:respawn:/etc/X11/prefdm -
nodaemon
```

按照以下说明编辑文件 `/etc/securetty`:

添加新行, 带有 COM2 的串行 tty 名称:


```
ttyS1
```

以下示例显示带有新增行的示例文件。

```
vc/1 vc/2 vc/3 vc/4 vc/5 vc/6 vc/7 vc/8 vc/9 vc/10 vc/11 tty1 tty2 tty3 tty4
tty5 tty6 tty7 tty8 tty9 tty10 tty11 ttyS1
```


使用 FlexAddress 和 FlexAddress Plus 卡

此部分提供有关 FlexAddress 和 FlexAddress Plus 卡以及如何配置和使用这些卡的信息。

 **注:** FlexAddress 是一项许可功能，您必须具有企业版许可证才能使用此功能。

关于 FlexAddress

FlexAddress 功能是可选升级，它允许服务器模块使用由机箱提供的 WWN/MAC ID 替换出厂时分配的全局名称和介质访问控制 (WWN/MAC) 网络 ID。

在生产过程中，每个服务器模块都被分配了唯一的 WWN 和/或 MAC ID。在使用 FlexAddress 之前，如果需要使用另一个模块替换某个服务器模块，则 WWN/MAC ID 将会更改，并且需要重新配置以太网管理工具和 SAN 资源以标识新的服务器模块。

FlexAddress 允许 CMC 将 WWN/MAC ID 分配给特定的插槽并覆盖出厂 ID。因此，如果更换了服务器模块，则基于插槽的 WWN/MAC ID 保留不变。使用此功能便不需要为新服务器模块重新配置以太网网络管理工具和 SAN 资源。

此外，覆盖操作仅在将服务器模块插入支持 FlexAddress 的机箱时发生；对服务器模块没有进行永久性更改。如果服务器模块移到不支持 FlexAddress 的机箱，则使用出厂分配的 WWN/MAC ID。

FlexAddress 功能卡包含一个 MAC 地址范围。安装 FlexAddress 之前，可以通过将 SD 卡插入 USB 内存读卡器并查看文件 `pwwn_mac.xml` 来确定 FlexAddress 功能卡上包含的 MAC 地址范围。SD 卡上的该明文 XML 文件包含一个 XML 标签 `mac_start`，它代表用于该唯一 MAC 地址范围的第一个起始十六进制 MAC 地址。而 `mac_count` 标签是 SD 卡可以分配的 MAC 地址总数。已分配的总 MAC 范围可以根据以下公式计算：

$$\langle \text{mac_start} \rangle + 0 \times \text{CF} (208 - 1) = \text{mac_end}$$


其中 208 是 `mac_count`，公式为：

$$\langle \text{mac_start} \rangle + \langle \text{mac_start} \rangle - 1 = \langle \text{mac_end} \rangle$$

例如：

$$(\text{starting_mac})00188BFFDCFA + 0 \times \text{CF} = (\text{ending_mac})00188BFFDCC9$$

。

 **注:** 将 SD 卡插入 USB 内存读卡器之前先锁定 SD 卡，防止意外修改其中的任何内容。将 SD 卡插入 CMC 前，您必须解除锁定。

关于 FlexAddress Plus

FlexAddress Plus 是 2.0 版功能卡中的新增功能。它是 FlexAddress 功能卡 1.0 版的升级。FlexAddress Plus 的 MAC 地址多于 FlexAddress 功能。两个功能都允许机箱分配全局名称/介质访问控制 (WWN/MAC) 地址到光纤通道和以太网设备。机箱分配的 WWN/MAC 地址全局唯一且特定于服务器插槽。

激活 FlexAddress

通过安全数字 (SD) 卡提供 FlexAddress，必须将该卡插入 CMC 才能激活此功能。要激活 FlexAddress 功能，可能需要进行软件更新。如果不激活 FlexAddress，就不需要这些更新。下表中列出的更新包括服务器模块 BIOS 和

CMC 固件。必须应用这些更新才能启用 FlexAddress。如果没有应用这些更新，则 FlexAddress 功能可能无法如期发挥作用。



 **注:** 无法在 DELL 单片服务器上激活 FlexAddress。


表. 24: 激活 FlexAddress 的前提条件


组件	最低要求版本
服务器模块 BIOS	<ul style="list-style-type: none">• M620• M520 <p> 注: M520 和 M620 的 BIOS 版本必须是 1.7.6 或更高版本。</p>
iDRAC7	版本 1.40.40 和更高版本
LC - USC	版本 1.1.5 和更高版本
CMC	版本 1.0 或更高版本

为了保证正确部署 FlexAddress 功能，请按以下顺序更新 BIOS 和固件：

1. 更新服务器模块 BIOS。
2. 更新服务器模块上的 iDRAC 固件。
3. 更新机箱中的所有 CMC 固件；如果存在冗余 CMC，则保证两个 CMC 的固件都得到更新。
4. 将 SD 卡插入被动模块中以获得冗余 CMC 模块系统，或插入单个 CMC 模块中以获得非冗余系统。

 **注:** 如果未安装支持 FlexAddress 的 CMC 固件（版本 1.10 或更高版本），则无法激活此功能。有关安装 SD 卡的说明，请参阅 *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification*（Chassis Management Controller (CMC) 安全数字 (SD) 卡技术规范）说明文件。

 **注:** 该 SD 卡包含 FlexAddress 功能。SD 卡上包含的数据经过加密，不能以任何方式复制或修改，否则会妨碍系统功能并导致系统无法正常运行。


 **注:** 每张 SD 卡只能用于一个机箱。如果有多个机箱，则必须购买额外的 SD 卡。

FlexAddress 功能将在安装有 SD 功能卡的 CMC 重新启动后自动激活。激活后会将此功能绑定到当前机箱。如果在冗余 CMC 中安装了 SD 卡，则直到冗余 CMC 激活时才会激活 FlexAddress 功能。有关如何激活冗余 CMC 的信息，请参阅 *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification*（Chassis Management Controller (CMC) 安全数字 (SD) 卡技术规范）说明文件。

当 CMC 重新启动时，请验证激活过程。有关激活 FlexAddress 的更多信息，请参阅[验证 FlexAddress 激活](#)。

激活 FlexAddress Plus

FlexAddress Plus 在 FlexAddress Plus 安全数字 (SD) 卡上随 FlexAddress 功能一起提供。

 **注:** 标有 FlexAddress 的 SD 卡仅包含 FlexAddress，标有 FlexAddress Plus 的卡包含 FlexAddress 和 FlexAddress Plus。必须将卡插入 CMC 才能激活此功能。

某些服务器需要的 MAC 地址数可能超过 FA 可以提供给 CMC 的地址数，具体取决于其配置方式。对于这些服务器来说，升级到 FlexAddress Plus 可实现 WWN/MAC 配置的全面优化。请联系 Dell 以获得 FlexAddress Plus 功能的支持。

要激活 FlexAddress Plus 功能，需要更新以下软件：服务器 BIOS、服务器 iDRAC 和 CMC 固件。如果不应用这些更新，则只有 FlexAddress 功能可用。有关这些组件需要的最低版本的信息，请参阅 dell.com/support/manuals 上的 *Dell Chassis Management Controller (CMC) for Dell PowerEdge VRTX Version 1.00 Release Notes*（Dell PowerEdge VRTX 的 Dell Chassis Management Controller (CMC) 1.00 版本发行说明）。

验证 FlexAddress 激活

功能卡包含以下一项或多项功能：FlexAddress、FlexAddress Plus 和/或扩展存储。运行以下 RACADM 命令可验证 SD 功能卡及其状态：

```
racadm featurecard -s
```

表. 25: featurecard -s 命令返回的状态消息

状态消息	操作
No feature card inserted.	检查 CMC 以验证 SD 卡是否已正确插入。在冗余 CMC 配置中，确保安装了 SD 功能卡的 CMC 是活动 CMC，而不是待机 CMC。
The feature card inserted is valid and contains the following feature(s) FlexAddress: bound.	无需任何操作。
The feature card inserted is valid and contains the following feature(s) FlexAddress: bound to another chassis, svctag=ABC1234, SD card SN = 1122334455.	移除 SD 卡；找到当前机箱的 SD 卡并进行安装。
The feature card inserted is valid and contains the following feature(s) FlexAddress: not bound.	功能卡可以移到另一个机箱或在当前机箱上重新激活。要在当前机箱上重新激活，请输入 <code>racadm racreset</code> ，直到安装了功能卡的 CMC 模块变为活动为止。

使用以下 RACADM 命令显示机箱上所有激活的功能：

```
racadm feature -s
```

该命令返回以下状态消息：

```
Feature = FlexAddress Date Activated = 8 April 2008 - 10:39:40 Feature  
installed from SD-card SN = 01122334455
```

如果机箱中没有活动的功能，则此命令将返回消息：

```
racadm feature -s No features active on the chassis
```


Dell 功能卡可包含多个的功能。一旦 Dell 功能卡上的所有功能都已在一个机箱上激活，则 Dell 功能卡上所有其他功能都不能在其他机箱上激活。在此情况下，`racadm feature -s` 命令会显示受到影响的功能的以下消息：

```
ERROR: One or more features on the SD card are active on another chassis
```

有关 `feature` 和 `featurecard` 命令的更多信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

停用 FlexAddress

使用 RACADM 命令可以停用 FlexAddress 功能，并将 SD 卡还原到安装前的状态。Web 界面中没有停用功能。停用功能会将 SD 卡还原到原始状态，以便可以在另一个机箱上安装并激活。在此语境中，FlexAddress 一词指 FlexAddress 和 FlexAddressPlus。

 **注：**SD 卡必须实际安装在 CMC 中，并且在运行停用命令之前必须关闭机箱电源。

如果在未安装卡时运行停用命令，或者对安装在不同机箱上的卡运行该命令，则会停用该功能且不会对该卡进行任何更改。

要停用 FlexAddress 功能并还原 SD 卡，请执行以下操作：

```
racadm feature -d -c flexaddress
```

如果成功停用，该命令将返回以下状态消息：

```
feature FlexAddress is deactivated on the chassis successfully.
```

如果在运行命令前未关闭机箱电源，则该命令将显示以下错误消息：

```
ERROR: Unable to deactivate the feature because the chassis is powered ON
```

有关该命令的详情，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）的 **feature** 命令部分。

查看 FlexAddress 信息

可以查看整个机箱或单个服务器的状态信息。显示的信息包括：

- 结构配置。
- FlexAddress 是活动的或非活动的。
- 插槽编号和名称。
- 机箱分配的地址和服务器分配的地址。
- 使用中的地址。

查看机箱的 FlexAddress 信息

可以显示整个机箱的 FlexAddress 状态信息。状态信息包括功能是否激活以及每个服务器的 FlexAddress 状态概述。

要使用 CMC Web 界面查看机箱 FlexAddress 状态，请单击**机箱概览** → **设置**。

此时将显示**常规机箱设置**页。

FlexAddress 具有值**活动**或**非活动**。值**活动**表示此功能已安装在机箱中，**活动**表示机箱中未安装且未使用此功能。

运行以下 RACADM 命令以显示整个机箱的 FlexAddress 状态：

```
racadm getflexaddr
```

要显示特定插槽的 FlexAddress 状态，请执行以下操作：

```
racadm getflexaddr [-i <slot#>]
```

其中 *<slot#>* 值为 1-4。

有关 **getflexaddr** 命令的附加信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

查看所有服务器的 FlexAddress 信息

要查看所有服务器的 FlexAddress 状态，请单击**服务器概览** → **属性** → **WWN/MAC**。


WWN/MAC 摘要页面显示关于以下方面的信息：

- WWN 配置
- 机箱中所有插槽的 MAC 地址

结构配置

结构 A 显示所安装的输入/输出结构的类型。

iDRAC 显示服务器管理 MAC 地址。


 **注:** 如果结构 A 已启用，则未填充的插槽会显示机箱为结构 A 分配的 MAC 地址。

WWN/MAC 地址

显示机箱中每个插槽的 FlexAddress 配置。显示的信息包括：

- 插槽编号和位置。
- FlexAddress 是活动的或非活动的。
- 结构类型。
- 使用中的服务器分配的 WWN/MAC 地址和机箱分配的 WWN/MAC 地址。

绿色复选标记表示活动地址类型，可以是服务器分配或机箱分配。

 **注:** iDRAC 管理控制器不是结构，但其 FlexAddress 被视作结构。

有关各字段的信息，请参阅 [联机帮助](#)。


查看单个服务器的 FlexAddress 信息


要使用 CMC Web 界面查看特定服务器的 FlexAddress 信息，请执行以下操作：

1. 在左侧窗格中，展开 **服务器概览**。
此时会列出机箱中插入的所有服务器。
2. 单击想要查看的服务器。
此时将显示 **服务器状态** 页面。
3. 单击 **设置** 选项卡，然后单击 **FlexAddress**。
此时将显示 **FlexAddress** 页面，该页面提供所选服务器的 WWN 配置和 MAC 地址。有关更多信息，请参阅 [联机帮助](#)。

配置 FlexAddress

FlexAddress 是一种可选升级，它允许服务器模块使用由机箱提供的 WWN/MAC ID 替换工厂分配的 WWN/MAC ID。

 **注:** 在此部分，FlexAddress 一词还指 FlexAddress Plus。

 **注:** 通过使用 `racresetcfg` 子命令，您可以将 CMC 的 Flex Address 重设为其出厂默认设置，即“禁用”。RACADM 语法为：

```
racadm racresetcfg -c flex
```

有关 FlexAddress 相关的 RACADM 命令和其他出厂默认属性相关数据的更多信息，请参阅 [dell.com/support/manuals](#) 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（适用于 PowerEdge VRTX RACADM 命令行的机箱管理控制器参考指南）。

您必须购买和安装 FlexAddress 升级才可以配置 FlexAddress。如果尚未购买和安装升级，Web 界面上会显示以下文本：

未安装可选功能。有关基于机箱的 WWN 和 MAC 地址管理功能的信息，请参阅 *Dell Chassis Management Controller Users Guide*（Dell Chassis Management Controller 用户指南）。要购买此功能，请通过 [www.dell.com](#) 联系 Dell。

如果随机箱购买了 FlexAddress，则系统开机时，该功能已安装并且激活。如果单独购买 FlexAddress，则必须按照 [dell.com/support/manuals](#) 上的 *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical*

Specification (Chassis Management Controller (CMC) 安全数字 (SD) 卡技术规范) 说明文件中的说明安装 SD 功能卡。

开始配置前必须关闭服务器。可以基于每个结构启用或禁用 FlexAddress。此外，还可以基于每个插槽启用或禁用该功能。在基于每个结构启用该功能后，可以选择要启用的插槽。例如，如果已启用结构 A，则启用的任何插槽将仅在结构 A 上启用 FlexAddress。所有其他结构都使用服务器上工厂分配的 WWN/MAC。

LAN 唤醒和 FlexAddress

首次部署 FlexAddress 功能时，必须在服务器模块上完成电源关闭和电源打开顺序，FlexAddress 才会生效。以太网设备上的 FlexAddress 由服务器模块的 BIOS 编程。为了使服务器模块的 BIOS 能够对地址进行编程，它必须处于运行状态，这需要打开服务器模块的电源。当电源关闭和电源打开顺序完成后，机箱分配的 MAC ID 可用于 LAN 唤醒 (WOL) 功能。



为机箱级结构和插槽配置 FlexAddress

在机箱级别，可以启用或禁用结构和插槽的 FlexAddress 功能。基于每个结构启用 FlexAddress，然后选择参与该功能的插槽。必须同时启用结构和插槽才能成功配置 FlexAddress。

使用 CMC Web 界面为机箱级结构和插槽配置 FlexAddress

如果插槽中有服务器，请先将其关闭，然后再在该插槽上启用 FlexAddress 功能。

要使用 CMC Web 界面启用或禁用结构和插槽以便使用 FlexAddress 功能，请执行以下操作：

1. 在左侧窗格中，单击**服务器概览** → **设置** → **FlexAddress**。
2. 在**部署 FlexAddress** 页面的**为机箱分配的 WWN/MAC 选择结构**部分，选择要启用 FlexAddress 的结构类型（**结构 A** 或 **iDRAC**）。要将其禁用，请清除此选项。
 **注:** 如果没有选择结构，则会显示以下消息。
FlexAddress is not enabled for the selected slots.
3. 在**为机箱分配的 WWN/MAC 选择插槽**页面中，为您要启用 FlexAddress 的插槽选择**已启用**选项。要将其禁用，请清除此选项。
 **注:** 如果没有选择插槽，则不会为所选结构启用 FlexAddress。
4. 要保存设置，请单击**应用**。

使用 RACADM 为机箱级结构和插槽配置 FlexAddress

要启用或禁用结构，请使用以下 RACADM 命令：

```
racadm setflexaddr [-f <fabricName> <state>]
```

其中，<fabricName> = A or iDRAC 和 <state> = 0 or 1

0 表示禁用，1 表示启用。

要启用或禁用插槽，请使用以下 RACADM 命令：


```
racadm setflexaddr [-i <slot#> <state>]
```

其中，<slot#> = 1 or 4 和 <state> = 0 or 1

0 表示禁用，1 表示启用。

有关 **setflexaddr** 命令的更多信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南)。

 **注:** 如果随 Dell PowerEdge VRTX 购买 FlexAddress 或 FlexAddressPlus 功能，将预安装并为所有插槽和结构启用该功能。要购买该功能，请通过 dell.com 与 Dell 联系。

 **注:** 通过使用 `racresetcfg` 子命令, 您可以将 CMC 的 Flex Address 重设为其出厂默认设置, 即“禁用”。RACADM 语法为:

```
racadm racresetcfg -c flex
```


有关 FlexAddress 相关的 RACADM 命令和其他出厂默认属性相关数据的更多信息, 请参阅 dell.com/support/manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南)。

查看全局名称/介质访问控制 (WWN/MAC) ID

WWN/MAC 摘要页面可用于查看机箱中插槽的 WWN 配置和 MAC 地址。

结构配置

结构配置部分显示为结构 A 安装的输入/输出结构类型。绿色复选标记表示已为该结构启用 FlexAddress。FlexAddress 功能用于将机箱分配的插槽永久 WWN/MAC 地址部署到机箱内的各种结构和插槽。该功能基于结构和插槽启用。

 **注:** 有关 FlexAddress 功能的更多信息, 请参阅[关于 FlexAddress](#)。

命令消息

下表列出 RACADM 命令和常见 FlexAddress 情况的输出。

表. 26: FlexAddress 命令和输出

情况	命令	输出
活动 CMC 模块中的 SD 卡绑定到另一个服务标签。	<code>\$racadm featurecard -s</code>	The feature card inserted is valid and contains the following feature(s) FlexAddress: bound to another chassis, svctag = <Service tag Number> SD card SN = <Valid flex address serial number>
活动 CMC 模块中的 SD 卡绑定到相同的服务标签。	<code>\$racadm featurecard -s</code>	The feature card inserted is valid and contains the following feature(s) FlexAddress: bound
活动 CMC 模块中的 SD 卡未绑定到相同的服务标签。	<code>\$racadm featurecard -s</code>	The feature card inserted is valid and contains the following feature(s) FlexAddress: not bound
出于某种原因 (未插入 SD 卡/SD 卡损坏/功能停用后/SD 卡绑定到不同机箱), 机箱上的 FlexAddress 功能未处于活动状态。	<code>\$racadm setflexaddr [-f <fabricName> <slotState>]</code> <code>\$racadm setflexaddr [-i <slot#> <slotstate>]</code>	ERROR: Flexaddress feature is not active on the chassis
来宾用户尝试在插槽/结构上设置 FlexAddress。	<code>\$racadm setflexaddr [-f <fabricName> <slotState>]</code> <code>\$racadm setflexaddr [-i <slot#> <slotstate>]</code>	ERROR: Insufficient user privileges to perform operation
在机箱接通电源的情况下停用 FlexAddress 功能。	<code>\$racadm feature -d -c flexaddress</code>	ERROR: Unable to deactivate the feature

情况	命令	输出
来宾用户尝试停用机箱上的功能。	<pre>\$racadm feature -d -c flexaddress</pre>	because the chassis is powered ON ERROR: Insufficient user privileges to perform operation
服务器模块接通电源时更改插槽/结构 FlexAddress 设置。	<pre>\$racadm setflexaddr -i 1 1</pre>	ERROR: Unable to perform the set operation because it affects a powered ON server
未安装 CMC 企业版许可证的情况下更改插槽或结构的 Flexaddress 设置。	<pre>\$racadm setflexaddr -i <slotnum> <status> \$racadm setflexaddr -f <FabricName> <status></pre>	ERROR: SWC0242 : A required license is missing or expired. Obtain an appropriate license and try again, or contact your service provider for additional details.

 **注:** 要解决此问题，您必须具有 **FlexAddress Enablement** 许可证。

FlexAddress DELL 软件许可协议

本协议是您（用户）与 Dell Products L.P 或 Dell Global B.V. (“Dell”) 之间的法律协议。本协议涵盖了 Dell 产品附带的所有软件（统称“软件”），除此之外不存在您与软件制造商或所有者之间的任何单独许可协议。本协议并不代表销售软件或任何其他知识产权。所有与软件有关的所有权和知识产权均归软件的制造商或所有者所有。未在本协议中明确授予您的所有权利均由软件的制造商或所有者保留。一旦您打开或拆开本软件包装上的密封，安装或下载本软件，或者使用产品中预装或嵌入的软件，即表示您同意受本协议条款的约束。如果您不同意这些条款，请立即退回所有软件物品（包括磁盘、书面材料和包装），并且删除任何预装或嵌入的软件。

一份软件一次仅可在一台计算机上使用。如果您拥有多份软件许可证，则可以随时使用的软件份数与许可证份数相同。“使用”是指将本软件载入计算机上的临时存储器或永久性存储设备。如果在网络服务器上安装本软件以便将其分配给其他计算机，并且获分配本软件的每台计算机均具有单独的许可证，则不能将这种安装称为“使用”。您必须保证安装在网络服务器上的软件的使用人数不超过您拥有的许可证份数。如果网络服务器上安装的软件的用户数超过许可证数，则必须购买更多的软件许可证，使许可证份数与用户数相等，然后才能允许其他用户使用软件。如果您是 Dell 的商业客户或 Dell 会员，您特此授权 Dell 或 Dell 选定的代理商在正常工作时间内就您对本软件的使用情况进行核查，并且同意在核查期间与 Dell 合作并合理地提供与本软件使用相关的所有记录。核查行为仅限于验证您是否遵循本协议中的条款。

本软件受美国版权法和国际条约的保护。您可以复制一份软件以用于备份或存档；也可以将软件传送至某个硬盘，条件是将原始软件仅用于备份或存档目的。您不得出租或租用本软件，也不得复制本软件附带的书面材料，但是可以作为 Dell 产品销售或转让的一部分永久性地转让本软件及其附带的所有材料，条件是您不保留任何复制件，并且受转让者同意遵守本协议中的条款。任何转让必须包括最新的更新文件和所有先前的版本。不得对软件进行反向工程、反编译或分解。如果计算机附带的软件包装内含有光盘、3.5 英寸和/或 5.25 英寸磁盘，则仅可将适当的磁盘用于您的计算机。不得在另一台计算机或另一个网络上使用这些磁盘，也不得出借、出租、租赁或将它们转让给另一个用户（除非符合本协议的规定）。

有限担保

从您收到这些软件磁盘之日起九十 (90) 天内，Dell 保证这些软件磁盘在正常使用的情况下不会出现材料和工艺方面的缺陷。此担保仅适用于您本人，并且不能转让。任何暗示性担保均限制在从您收到本软件之日起九十 (90) 天之内。某些辖区不允许对暗示性担保的持续时间进行限制，因此上述限制可能不适用于您。Dell 及其供应商的全部责任以及您获得的唯一补偿是：(a) 退回购买本软件所付的款项，或者 (b) 更换不符合此担保要求的任何磁盘，但是您必须将磁盘与退回授权号一起发送至 Dell 并承担相关费用和 risk。此有限担保不适用于因意

外、滥用、误用或由非 Dell 授权人员维修或修改磁盘所导致的损坏。对于任何更换过的磁盘，其担保期为原始担保期的剩余时间或者三十 (30) 天，以较长的时间为准。

Dell 并不保证本软件的功能可以满足您的要求，也不保证本软件的操作不会中断或不出现错误。您自己负责选择本软件来满足您的特定用途，并且对本软件的使用及其产生的后果负责。

对于软件及其附带的所有书面材料，DELL 代表本公司及其供应商否认其他所有的明示或暗示担保，包括但不限于适销性和对某一特定用途适用性的暗示担保。本有限担保赋予您特定的法律权利；您可能还具有其他权利，视管辖区域的不同而有所差异。

无论在什么情况下，Dell 或其供应商对于因使用本软件或不能使用本软件所造成的任何损失（包括但不限于商业利润损失、业务中断、业务信息丢失或其他经济损失）概不负责，即使已得到可能出现此类损失的通知。由于某些辖区不允许对必然性或偶然性损失的责任进行排除或限制，因此上述限制可能不适用于您。

开放源代码软件

本 CD 的一部分可能包含开放式源代码软件，您可以按照在分发开放式源代码软件时所依据的特殊许可证的条款和条件使用该软件。

本开放源代码软件的发布旨在希望其将是有益的，但本软件按原样提供，无任何明示或暗示的担保，包括但不限于适销性或对于特定目的适用性的暗示担保。无论任何情况，Dell、版权所有者或其他责任者均不会对任何直接的、间接的、偶然的、特殊的、典型的或伴生的损失（包括但不限于替代产品或服务的采购、用途、数据和利润的损失，或业务中断）负责，无论如何引起、基于何种责任的推理、是否有合同、严格的义务或任何由于使用本软件所引发的民事侵权行为（包括疏忽或其他原因），即使已得到可能会有此类损失的提示。

美国政府限制权利

48 C.F.R. 2.101 中的条款规定软件和文档均属于“商品”，它由 48 C.F.R. 12.212 中所用的术语“商业计算机软件”和“商业计算机软件说明文件”组成。与 48 C.F.R. 12.212 和 48 C.F.R. 227.7202-1 到 227.7202-4 一致，所有获得本软件和文档的美国政府最终用户仅具有如前所述的权利。

签约商/制造商是 Dell Products, L.P., One Dell Way, Round Rock, Texas 78682。

一般信息


本许可在终止前持续有效。本许可会依据上述条件终止，或者如果您违反了本许可规定的任何条款，则本许可会被终止。许可终止后，您同意销毁本软件和随附材料，以及所有副本。本协议受德克萨斯州法律的管辖。本协议中的各项规定均具有可分割性。如果某一规定被认为无法实施，它并不会影响本协议中其他规定、条款或条件的有效性。本协议对本软件的继承者和受让者均有效。在法律允许的最大范围内，Dell 和您均同意放弃就本软件或本协议提起任何诉讼的权利。此放弃行为在某些辖区内可能无效，因此它可能不适用于您。您确认已阅读了本协议，并且理解和同意遵守其中的条款。另外，您还承认本协议是您与 Dell 之间就软件所签署的完整的、唯一的协议声明。

管理结构

机箱支持一种结构类型，即结构 A。结构 A 供单个 I/O 模块使用，并且始终连接到服务器的机载以太网适配器。

机箱只包含一个 I/O 模块 (IOM)，该 IOM 是直通或交换机模块。该 I/O 模块归类为组 A。

机箱 IOM 使用称为**结构**的独立数据路径，该结构命名为 A。结构 A 仅支持以太网。每个服务器 IO 适配器（夹层卡或 LOM）可以具有两个或四个端口，具体取决于性能。连接到 PCIe 卡（而不是 IO 模块）的 PCIe 扩展卡占用夹层卡插槽。在部署以太网、iSCSI 或光纤信道网络时，跨组 1 和组 2 建立冗余链路以获得最大可用性。利用结构标识符标识独立 IOM。

 **注:** 在 CMC CLI 中，IOM 按照惯例称为 switch。

无效配置

有三种无效配置类型：

- 无效的 MC 或 LOM 配置，新安装的服务器的结构类型与现有 IOM 结构不同，即单个服务器的 LOM 或 MC 不受其对应 IOM 的支持。在此情况下，机箱中的所有其他服务器都在运行，而 MC 卡不匹配的服务器无法开机。服务器上的电源按钮呈琥珀色闪烁以提示存在结构不匹配情况。
- 无效的 IOM-MC 配置，新安装 I/O 模块的结构类型与驻留的 MC 结构类型不匹配或不兼容。不匹配的 IOM 将保持关机状态。CMC 向 CMC 和硬件日志添加条目，注明无效配置并指定 IOM 名称。CMC 导致有问题的 IOM 的错误 LED 指示灯闪烁。如果将 CMC 配置为发送警报，则会发送关于此事件的电子邮件和/或 SNMP 警报。
- 无效 IOM-IOM 配置，新安装的 IOM 与组中已安装的 IOM 具有不同或不兼容的结构类型。CMC 将新安装的 IOM 保持在关机状态，从而导致 IOM 的错误 LED 指示灯闪烁，并在 CMC 和硬件日志中创建关于不匹配的条目。

刷新开机场景

当机箱插入并开机时，I/O 模块的优先级高于服务器。允许 IOM 比其他服务器先开机。此时不会执行它们的结构类型验证。

IOM 开机后，服务器开机，然后 CMC 验证服务器的结构一致性。

如果直通模块和交换机的结构相同，则允许它们位于相同的组中。即使交换机和直通模块由不同的供应商制造，也可存在于相同的组中。

监测 IOM 运行状况


有关监测 IOM 运行状况的信息，请参阅[查看 IOM 的信息和运行状况](#)。


为 IOM 配置网络设置

可以为用于管理 IOM 的接口指定网络设置。对于以太网交换机，可以配置带外的管理端口（IP 地址）。不能使用此界面配置带内管理端口（即 VLAN1）。

在为 IOM 配置网络设置之前，确保将 IOM 电源打开。

要为组 A 中的 IOM 配置网络设置，必须具有结构 A 管理员权限。

 **注:** 对于以太网交换机，带内 (VLAN1) 和带外管理 IP 地址不能相同或位于相同的网络；否则会导致无法设置带外 IP 地址。有关默认带内管理 IP 地址，请参阅 IOM 说明文件。

 **注:** 不要为以太网直通和 Infiniband 交换机配置 I/O 模块网络设置。


使用 CMC Web 界面为 IOM 配置网络设置

要为 I/O 模块配置网络设置，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览**，再单击**I/O 模块概览**，然后单击**设置**。或者，要配置唯一可用的 I/O 模块 A 的网络设置，请单击**千兆位以太网**，然后单击**设置**。


在**配置 I/O 模块网络设置**页面中，键入相应的数据，然后单击“应用”。

2. 如果允许，请键入 IOM 的根密码、SNMP RO 团体字符串和系统日志服务器 IP 地址。有关字段说明的更多信息，请参阅[联机帮助](#)。

 **注:** 从 CMC 设置的 IOM IP 地址不会保存到交换机的永久启动配置中。要永久保存 IP 地址配置，必须运行 `connect switch` 命令或 `racadm connect switch RACADM` 命令，或者使用到 IOM GUI 的直接界面将该地址保存到启动配置文件中。

3. 单击**应用**。

IOM 的网络设置已配置完成。

 **注:** 如果允许，可以将 VLAN、网络属性和 IO 端口重设为默认配置值。

使用 RACADM 为 IOM 配置网络设置

要使用 RACADM 为 IOM 配置网络设置，请设置日期和时间。请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）中的 `deploy` 命令部分。

您可以使用 RACADM `deploy` 命令为 IOM 设置用户名、密码和 SNMP 字符串：

```
racadm deploy -m switch -u <username> -p <password>
```

```
racadm deploy -m switch -u -p <password> -v SNMPv2 <snmpCommunityString> ro
```

```
racadm deploy -a [server|switch] -u <username> -p <password>
```

管理输入/输出模块的电源控制操作

有关为输入/输出模块设置电源控制操作的信息，请参阅[对 IOM 执行电源控制操作](#)。

启用或禁用输入/输出模块的 LED 闪烁

有关启用输入/输出模块的 LED 闪烁的信息，请参阅[配置 LED 以标识机箱上的组件](#)。

管理和监测电源

Dell PowerEdge VRTX 机箱是能效最高的模块化服务器机柜。它设计独特，包括高效率的电源设备和风扇，优化的布局使气流在系统内畅行无阻，并且机柜中处处包含优化能效的组件。优化的硬件设计配合内置于 Chassis Management Controller (CMC)、电源设备和 iDRAC 中的先进电源管理功能，使您能够进一步提高服务器环境的能效。

PowerEdge VRTX 的电源管理功能可帮助管理员配置机柜以减少功耗，调整功率以满足环境的特定需要。

PowerEdge VRTX 模块化机柜使用交流电源，并在所有当前活动的内部电源设备装置 (PSU) 之间进行负载分配。该系统最多能够提供 5000W 交流电源，分配给服务器模块和相关机柜基础结构。但是，该容量因您选择的电源冗余策略而异。


PowerEdge VRTX 机柜可针对影响 PSU 行为的两种冗余策略之一进行配置，并且可以决定如何向管理员报告机箱冗余状态。

您也可以通过 **OpenManage Power Center (OMPC)** 控制电源管理。当 OMPC 从外部控制电源时，CMC 可继续维护：

- 冗余策略
- 远程电源日志记录
- 动态电源设备接入 (DPSE)

于是 OMPC 管理：

- 服务器电源
- 服务器优先级
- 系统输入功率上限
- 最大节能模式

 **注：**实际电源供应取决于配置和工作负载。

可以使用 CMC Web 界面或 RACADM 管理和配置 CMC 电源控制：

- 查看电源分配情况、功耗以及机箱、服务器和 PSU 的状态。
- 配置机箱的电源预算和冗余策略。
- 执行机箱电源控制操作（开机、关机、系统重设、关机后再开机）。

冗余策略


冗余策略是一组可配置的属性，它可以确定 CMC 如何管理到机箱的电源。以下冗余策略可配置带或不带动态 PSU 接入：


- 交流冗余
- 电源设备冗余

交流冗余策略

交流冗余策略的目的是使模块化机柜系统能够在可承受交流电源故障的模式下运行。这些故障可能因交流电网、布线和传输或 PSU 本身而引起。

在为系统配置交流冗余时，PSU 划分到电网中：插槽 1 和 2 中的 PSU 位于第一个电网，而插槽 3 和 4 中的 PSU 位于第二个电网。CMC 管理电源，因此即使有一个电网发生故障，系统仍可在不降低性能的情况下继续运行。交流冗余也可承受单个 PSU 的故障。

 **注：**交流冗余的作用之一是在整个电网发生故障的情况下支持服务器的无缝运行，但在两个电网的供电能力大致相等时，大多数供电用于维持交流冗余。

 **注：**交流冗余仅在负载要求不超过供电能力最低的电网的容量时可实现。

交流冗余级别

每个电网中 1 个 PSU 是交流冗余必需的最低配置。也可使用其他所有组合配置，但在每个电网中至少要有 1 个 PSU。为了提供最大可用功率，各电网中 PSU 的总功率应尽可能相近。维持交流冗余时的功率上限是两个电网中供电能力较小的电网的可用功率。

如果 CMC 因某种原因无法维持交流冗余，则在配置了针对冗余丢失事件发出警报的情况下，会将电子邮件和/或 SNMP 警报发送给管理员。


如果此配置中的一个 PSU 出现故障，则故障电网中其余的 PSU 被标记为“联机”。在这种情况下，任意剩余 PSU 出现故障也不会导致系统操作中断。如果一个 PSU 出现故障，机箱运行状况将被标记为不严重。如果供电能力较小的电网不能支持全部机箱电源分配，则交流冗余状态将报告为**无冗余**，机箱运行状况显示为**严重**。

电源设备冗余策略

电源设备冗余策略在冗余电源电网不可用时发挥作用，但您可能希望防止因单个 PSU 出现故障而导致模块化机柜中的服务器停机。供电能力最高的 PSU 将为此目的而联机保留。这样就形成了电源设备冗余池。下图说明电源冗余模式。

超出功率和冗余所需的 PSU 仍可用并会在出现故障时添加到池。

与交流冗余不同的是，选择电源设备冗余后，CMC 不要求 PSU 设备存在于任何特定 PSU 插槽位置。

 **注：**动态电源设备接入 (DPSE) 允许将 PSU 置于待机状态。该待机状态表示 PSU 未接受供电的实际状态。启用 DPSE 时，可将额外的 PSU 置于待机模式，以提高效率和节约用电。

动态电源设备接入


在默认情况下，动态电源设备接入 (DPSE) 模式处于禁用状态。DPSE 可通过优化 PSU 向机箱供电的功效而节能。这样可延长 PSU 的使用寿命，减少热量产生。要使用此功能，必须具有企业版许可证。

CMC 监测总体机柜功率分配，并将 PSU 转到“待机”状态，从而通过更少的 PSU 提供机箱的总体电源分配。因为联机 PSU 以更高利用率运行时更高效，所以在延长待机 PSU 使用寿命的同时还会提高效率。

要让其余 PSU 在最大效率下工作，请使用以下电源冗余模式：

- 带有 DPSE 的 **PSU 冗余**模式也能提高电源效率。至少两个电源设备处于联机状态，其中一个 PSU 为配置提供电力，另一个在出现 PSU 故障时提供冗余。“PSU 冗余”模式可以在任何一个 PSU 出现故障时提供保护，但在交流电网停工时不提供保护。
- 带有 DPSE 的 **交流冗余**模式至少有两个 PSU 处于活动状态，每个电网中有一个。在部分负载的模块化机柜配置中，交流冗余也会在效率和最大可用性之间取得平衡。
- 禁用 DPSE 提供最低效率，因为全部六个电源都活动并共享负载，使每个电源的利用率降低。

可针对上面介绍的所有双电源设备冗余配置启用 DPSE - **电源设备冗余**和**交流冗余**。


 **注：**在双 PSU 配置模式中，服务器负载可能会阻止任何 PSU 更改为待机模式。

- 在**电源设备冗余**配置中，除了机柜开机所需的 PSU 之外，机柜始终保留一个附加的 PSU 处于开启状态并标记为**联机**。电源使用情况受到监测，根据总体系统负载，一个 PSU 可转到“待机”状态。在四个 PSU 的配置中，最少两个 PSU 始终保持开启。

因为采用**电源设备冗余**配置的机柜始终启用一个额外的 PSU，所以当一台联机 PSU 出现故障时，机柜仍能正常工作，并且仍能为安装的服务器模块提供充足的电力。当联机 PSU 出现故障时，一台待机 PSU 将变为联机状态。多个 PSU 同时出现故障可能导致某些服务器模块断电，同时待机 PSU 被开启。

- 在**交流冗余**配置中，机箱开机时所有 PSU 均启用。电源使用情况受到监测，如果系统配置和电源使用情况允许，PSU 将转到**待机**状态。因为电网中 PSU 的**联机**状态将镜像其他电网的联机状态，所以机柜可以承受整个电网断电，而不会中断为机柜供电。

交流冗余配置中功率要求的增加会造成 PSU 从**待机**状态接入。这保持双电网冗余所需的镜像配置。

 **注:** 当 DPSE 处于启用状态时，如果两种电源冗余策略模式中的电源需求增加，则待机 PSU 会转为**联机**以收回电源。

默认冗余配置


如表中所示，机箱的默认冗余配置取决于它所包含的 PSU 的数量。

表. 27: 默认冗余配置


PSU 配置	默认冗余策略	默认动态 PSU 接入设置
两个 PSU	直流冗余	已禁用
四个 PSU	直流冗余	已禁用

交流冗余

在具有四个 PSU 的交流冗余模式中，所有四个 PSU 都处于活动状态。其中两个 PSU 必须连接到一个交流电网，另外两个 PSU 连接到另一个交流电网。

 **小心:** 为了避免系统故障并让交流冗余有效工作，必须有均衡的 PSU 组正确连接到不同的交流电网。

如果一个交流电网出现故障，连接至正常运行的交流电网的 PSU 将接管供电任务，而不会中断服务器或基础结构。

 **小心:** 在交流冗余模式中，必须具有均衡的 PSU 组（每个电网至少有一个 PSU）。如果不能满足此条件，则不能实现交流冗余。

电源设备冗余

启用电源设备冗余时，机箱中的一个 PSU 保持备用状态，从而确保任何单个 PSU 故障不会导致服务器或机箱断电。电源设备冗余模式至少需要两个 PSU。启用 DPSE 后，如果存在额外的 PSU，会使用这些 PSU 来提高系统的电源效率。冗余丢失后，如果发生故障，可能会导致机箱中的服务器断电。

硬件模块电源预算

CMC 提供电源预算服务，它能够为机箱配置电源预算、冗余和动态电源。

电源管理服务能够优化功耗，并根据需要将电源重新分配到不同的模块。

CMC 为机柜保持电源预算，为所有安装的服务器和组件保留所需功率。

CMC 将功率分配给机箱中的 CMC 基础结构和服务器。CMC 基础结构由机箱中的组件组成，例如风扇、I/O 模块、存储适配器、PCIe 卡、物理磁盘和主板。机箱最多可承载 4 个服务器，这些服务器通过 iDRAC7 与机箱通信。有关更多信息，请参阅 dell.com/support/manuals 上的 *iDRAC7 用户指南*。


服务器开机之前，iDRAC 为 CMC 提供其功率范围需求。功率范围包含可以使服务器运行的最大功率需求和最小功率需求。iDRAC 的初始估计值以其对服务器中组件的初步了解为根据。在工作开始后发现其他组件时，iDRAC 可增加或降低其初始功率要求。

机柜中的服务器开机时，iDRAC 软件重新估算功率需求，并请求对功率范围做出后续调整。

CMC 为服务器提供所请求的功率，并且从可用预算中减去分配的功率。一旦批准服务器的功率请求，服务器的 iDRAC 软件就会持续监测实际功耗。根据实际功率要求，iDRAC 功率范围会随着时间推移而发生变化。如果服务器完全消耗所分配的功率，iDRAC 会请求提升功率。

在重负载下，可能会降低服务器处理器的性能，以确保功耗低于用户配置的系统输入功率上限。

PowerEdge VRTX 机柜可以为大多数服务器配置提供充足的功率以发挥峰值性能，但有许多服务器配置并不会消耗机柜所能提供的最大功率。为了帮助数据中心为其机柜分配电源，PowerEdge VRTX 允许您指定系统输入功率上限，以确保总体机箱交流电源消耗量保持在给定阈值之下。CMC 首先确保提供足够的电能来运行风扇、I/O 模块、存储适配器、物理磁盘驱动器、主板和 CMC 自身。这些电源分配被称为“分配给机箱基础结构的输入电源”。机柜中的服务器在机箱基础结构后开机。任何将系统输入功率上限设置为低于“功率负荷”的尝试都会失败。“功率负荷”是分配给基础结构的功率与分配给已开机服务器的最低功率之和。

 **注:** 要使用功率上限功能，必须具有企业版许可证。

为了保证总体电源预算始终低于系统输入功率上限的值，CMC 在必要时会为服务器分配低于其最大请求功率的值。系统基于服务器优先级设置为服务器分配功率，具有最高优先级的服务器获得最大功率，具有第 2 优先级的服务器在第 1 优先级服务器之后获得功率，依次类推。优先级较低的服务器获得的功率可能少于第 1 优先级服务器，这取决于系统输入最大功率上限和用户配置的系统输入功率上限设置。

如果发生诸如在机箱中增加服务器、共享 HDD 或 PCIe 卡之类的配置变化，可能需要提高系统输入功率上限。在温度条件发生变化并且需要风扇以更快速度运转时，会导致它们消耗更多电力，而模块化机柜中的电力需求也会随之增加。插入 I/O 模块和存储适配器、PCIe 卡、物理磁盘和主板以及 PSU 的数量、类型和配置变化也会增加模块化机柜的电力需求。即便是为了保持管理控制器运行而关闭服务器时，也会消耗极少量的电力。

只有在电力充足时才能打开模块化机柜中的更多服务器。可随时将系统输入功率上限提高到最大值 5000W，以允许启动额外的服务器。

模块化机柜中减少功率分配的变动为：

- 服务器关闭
- I/O 模块关闭
- 存储适配器、PCIe 卡、物理磁盘驱动器和主板关闭
- 机箱过渡到关闭


机箱打开或关闭时，都可以重新配置系统输入功率上限。

服务器插槽电源优先级设置

CMC 允许您为机柜中的四个服务器插槽分别设置电源优先级。优先级设置从 1（最高）到 9（最低）。这些设置被分配给机箱中的插槽，并且插槽的优先级将被插入该插槽的任何服务器继承。CMC 基于插槽优先级将电源预算优先分配给机柜中具有最高优先级的服务器。


根据默认服务器插槽优先级设置，电源将平均分配给所有插槽。更改插槽优先级允许管理员区分为哪些服务器优先分配电源。如果更重要的服务器模块保持它们的默认插槽优先级为 1，并且不太重要的服务器模块更改为更低的优先级值 2 或以上，优先级为 1 的服务器模块将首先开机。然后这些更高优先级服务器将获得最大电源分配，而可能不会为更低优先级服务器分配足够电源以便它们以最高性能运行，甚至根本不开机，这取决于设置的系统输入功率上限有多低以及服务器电源要求。


如果管理员先手动开启低优先级服务器模块，然后开启高优先级服务器模块，则系统首先将低优先级服务器模块的电源分配下调至最低值，以满足高优先级服务器的需求。因此，在可供分配的电源耗尽后，CMC 会从较低或同等优先级的服务器回收电源，直至达到其最低功率水平。

 **注:** I/O 模块、风扇、主板、物理磁盘驱动器和存储适配器具有最高优先级。CMC 仅回收低优先级设备的电源以满足高优先级设备或服务器的电源需求。

为服务器分配优先级

当需要额外电源时，服务器优先级决定 CMC 将从哪台服务器开始节电。

 **注:** 为服务器分配的优先级与服务器所在的插槽相关联，而不是服务器本身。如果将服务器移动到新插槽，必须为新插槽位置重新配置优先级。

 **注:** 要执行电源管理操作，必须具有**机箱配置管理员**权限。

使用 CMC Web 界面为服务器分配优先级

要分配优先级，请执行以下操作：

1. 在左侧窗格中，单击**服务器概览** → **电源** → **优先级**。
服务器优先级页面会列出机箱中的所有服务器。
2. 从**优先级**下拉菜单中，为一台、多台或全部服务器选择优先级（1-9，其中 1 代表最高优先级）。默认值为 1。可以为多台服务器分配相同的优先级。
3. 单击**应用**保存所做的更改。

使用 RACADM 为服务器分配优先级

打开到 CMC 的串行/Telnet/SSH 文本控制台，登录并键入：

```
racadm config -g cfgServerInfo -o cfgServerPriority -i <slot number> <priority level>
```

其中 *<slot number>* (1-4) 表示服务器位置，而 *<priority level>* 为 1-9 之间的值。

例如，要将插槽 4 中的服务器优先级设置为 1，请键入以下命令：


```
racadm config -g cfgServerInfo -o cfgServerPriority -i 4 1
```

查看功耗状态

CMC 为整个系统提供实际输入功耗。

使用 CMC Web 界面查看功耗状态

在左侧窗格中，单击**机箱概览** → **电源** → **电源监测**。“电源监测”页面将显示电源运行状况、系统电源状态、实时电源统计信息和实时能耗统计信息。有关更多信息，请参阅[联机帮助](#)。

 **注:** 您也可以在“电源设备”下查看电源冗余状态。

使用 RACADM 查看功耗状态

要使用 RACADM 查看功耗状态，请执行以下操作：

打开到 CMC 的串行/Telnet/SSH 文本控制台，登录并键入：

```
racadm getpminfo
```

使用 CMC Web 界面查看电源预算状态

要使用 CMC Web 界面查看电源预算状态，请在左侧窗格中转至**机箱概览**，然后单击**电源** → **预算状态**。**电源预算状态**页面显示系统电源策略配置、电源预算详情、为服务器模块分配的预算以及机箱电源设备详情。有关更多信息，请参阅[联机帮助](#)。

使用 RACADM 查看电源预算状态


打开到 CMC 的串行/Telnet/SSH 文本控制台，登录并键入：

```
racadm getpbinfo
```

有关 **getpbinfo** 的更多信息，包括输出详情，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）中的 **getpbinfo** 命令部分。

冗余状态和总体电源运行状况

冗余状态是确定总体电源运行状况的一个因素。例如，电源冗余策略设置为“交流冗余”，并且冗余状态指示系统正在运行并且有冗余时，总体电源运行状况通常是**正常**。但是，如果不符合以交流冗余模式运行的条件，则冗余状态会**是否**，而且总体电源运行状况会是**严重**。这是因为系统无法按照配置的冗余策略运行。

 **注：**将冗余策略更改为交流冗余或将交流冗余更改为其他策略时，CMC 不会预先检查这些条件。因此，配置冗余策略可能会直接导致冗余丢失或重新获得。

PSU 出现故障后的电源管理。

当发生电源不足的事件时（如 PSU 故障），CMC 将减少为服务器提供的电源设备。减少电源后，CMC 会重新评估机箱的电源需求。如果仍然不满足电源需求，CMC 会关闭优先级较低的服务器。但是，此操作是基于您在 CMC 上设置的电源冗余策略完成的。冗余服务器可承受电源损失，而不会影响服务器的性能。

具有较高优先级的服务器的电源逐步恢复，而电源需求会维持在电源预算内。要设置冗余策略，请参阅[电源预算和冗余](#)。

卸下 PSU 后的电源管理

当您卸下 PSU 或 PSU 交流电线时，CMC 可能会开始节电。CMC 会降低较低优先级服务器的供电，直到机箱中剩余的 PSU 能够支持电源分配。如果卸下多个 PSU，CMC 将在卸下第二个 PSU 时重新评估电源需求以确定固件响应。如果仍然不满足电源需求，CMC 可以关闭优先级较低的服务器。

限制

- CMC 不支持对较低优先级的服务器进行**自动**断电，从而允许较高优先级的服务器开机；但是，您可以执行用户发起的断电。
- 对 PSU 冗余策略的更改受限于机箱中的 PSU 数量。可以选择[默认冗余配置](#)中列出的两种 PSU 冗余配置设置中的任意一种。

新的服务器接入策略

当新服务器开机时，如果超出机箱的可用电源，CMC 可能需要降低对低优先级服务器的供电。如果管理员为机箱配置的功率限制低于为服务器分配全功率所需的功率，或者电源不足以满足机箱中所有服务器的更高功率需求时会发生这种情况。如果通过降低为较低优先级服务器分配的电源依旧无法腾出足够的电源，则新服务器将无法开机。

如果管理员为机箱配置的功率限制低于服务器的全功率分配，或者电源不足以满足服务器的高功率需求，则会发生这种情况。

下表提供在先前描述的情形下，当新服务器开机时 CMC 所采取的操作。

表. 28: 尝试打开服务器电源时的 CMC 响应

是否满足最差情况下的电源需求	CMC 响应	打开服务器电源
是	不需要节能	允许
否	执行节能： <ul style="list-style-type: none"> • 能够提供新服务器所需的电源 • 不能提供新服务器所需的电源 	允许 不允许

如果某个 PSU 出现故障，会导致非严重运行状况，并生成 PSU 故障事件。卸下 PSU 时，会生成 PSU 卸下事件。

如果任一事件导致冗余丢失，则根据电源分配情况，将生成冗余丢失事件。

如果随后的电源容量或用户电源容量大于服务器分配容量，服务器的性能会降低，在最坏情况下，服务器可能会关机。在这两种情况下都以逆优先级顺序进行，也就是优先级较低的服务器先关机。

下表介绍针对各种 PSU 冗余配置，固件对 PSU 关闭或卸下的响应。

表. 29: PSU 故障或卸下对机箱的影响

PSU 配置	动态 PSU 接入	固件响应
交流冗余	已禁用	CMC 警告您失去交流冗余。
电源设备冗余	已禁用	CMC 警告您失去电源设备冗余。
交流冗余	已启用	CMC 警告您失去交流冗余。将打开待机模式的 PSU（如果有）以补偿 PSU 故障或卸下造成的电源预算损失。
电源设备冗余	已启用	CMC 警告您失去电源设备冗余。将打开待机模式的 PSU（如果有）以补偿 PSU 故障或卸下造成的电源预算损失。

系统事件日志中的电源和冗余策略更改

将电源状态和电源冗余策略的更改记录为事件。在系统事件日志 (SEL) 中记录条目的有关电源的事件包括电源插入和卸下、电源输入插入和卸下以及电源输出确认和未确认。

下表列出与电源更改有关的 SEL 条目：

表. 30: 电源更改的 SEL 事件

电源事件	系统事件日志 (SEL) 条目
插入	电源设备存在。
卸下	电源设备缺失。
接受交流输入	电源设备的电源输入丢失。
交流输入丢失	电源设备的电源输入已恢复。
产生直流输出	电源设备工作正常。
直流输出丢失	电源设备发生故障。

与电源冗余状态变化相关并记录在 SEL 中的事件包括：冗余丢失以及冗余重新获得，这适用于配置为**交流冗余**电源策略或**电源设备冗余**电源策略的模块化机柜。下表列出有关电源冗余策略更改的 SEL 条目。

电源策略事件

冗余丢失
重新获取冗余

系统事件日志 (SEL) 条目

电源设备冗余丢失。
电源设备存在冗余。

配置电源预算和冗余

可以配置整个机箱（机箱、服务器、I/O 模块、KVM、CMC 和电源设备）的电源预算、冗余和动态电源。整个机箱使用四个电源设备装置 (PSU)。电源管理服务可优化功耗，并根据需求为不同模块重新分配电源。


您可以配置以下各项：

- 系统输入功率上限
- 冗余策略
- 启用动态电源设备接入
- 禁用机箱电源按钮
- 最大节能模式
- 远程电源日志记录
- 远程电源日志记录间隔
- 基于服务器的电源管理

节能和电源预算

当达到用户配置的最大功率限制时，CMC 开始节能。当电源需求超出用户配置的“系统输入功率上限”时，CMC 将按优先级从低到高的顺序减少为服务器提供的功率，以便为机箱中高优先级的服务器和其他模块腾出功率。

如果机箱中所有或多个插槽配置了相同的优先级，CMC 将按照插槽编号递增的顺序减少为服务器提供的功率。例如，如果插槽 1 和 2 中的服务器具有相同的优先级，则插槽 1 中的服务器将先于插槽 2 中的服务器减少供电。

 **注：**可以通过指定每台服务器从 1 到 9 的编号，为机箱中每台服务器分配一个优先级。所有服务器的默认优先级为 1。数字越低，优先级越高。

电源预算限制为两个 PSU 中最弱的 PSU 设置的最大值。如果尝试设置超过 *系统输入功率上限* 值的交流电源预算值，CMC 会显示消息。电源预算限制为 5000W。

最大节能模式

只有在选择交流冗余时才启用此模式。CMC 在以下情况下进入最大节能模式：

- 启用了最大节能模式
- 由 UPS 设备发出的自动命令行脚本启用最大节能模式。

在最大节能模式下，所有服务器都在最低电源水平下工作且所有后续服务器电源分配请求都会被拒绝。在此模式下，已开机服务器的性能可能下降。额外的服务器无论优先级如何都不能开机。

在清除最大节能模式后，系统恢复到最佳性能。

减少服务器功率以维持功率预算

为了让系统功耗保持在用户配置的系统输入功率上限内而需要额外功率时，CMC 将减少分配给较低优先级服务器的功率。例如，当接入新服务器时，CMC 可能会减少低优先级服务器的功率，以便为新服务器提供更多

功率。如果减少分配给较低优先级服务器的功率之后，功率量仍然不足，CMC 会降低服务器的性能，直到为新服务器腾出足够的功率为止。

CMC 在两种情况下会减少分配给服务器的功率：

- 总体功耗超过可配置的系统输入功率上限。
- 在非冗余配置中出现电源故障。

PSU 在 110V 交流电源下工作

默认情况下，PSU 可在 110V 交流输入下工作。但是，不支持在 110V 和 220V 组合交流输入下工作。如果 CMC 检测到同时输入这两种电压，则会选择其中一种电压值，并关闭连接到另一种电压电平的那些电源设备，并指示其无法工作。

远程日志记录

功耗可报告至远程系统日志服务器。可记录一段收集时间内的机箱总功耗、最小值、最大值和平均功耗。有关启用此功能和配置收集或日志记录间隔的更多信息，请参阅[管理和监测电源](#)。

外部电源管理

CMC 电源管理可选择由 OpenManage Power Center (OMPC) 控制。有关更多信息，请参阅 *OMPC 用户指南*。

当启用了外部电源管理时，OMPC 可管理：

- 第 12 代服务器的服务器电源
- 第 12 代服务器的服务器优先级
- 系统输入功率上限
- 最大节能模式

CMC 可继续维护或管理：


- 冗余策略
- 远程电源日志记录
- 服务器性能优先于电源冗余
- 动态电源设备接入

在将电源分配给机箱基础结构和前一代服务器节点之后，OMPC 基于可用预算管理机箱中第 12 代服务器节点的优先级和电源。远程电源日志记录不受外部电源管理的影响。


启用“基于服务器的电源管理模式”之后，机箱即为 PM3 管理准备就绪。所有第 12 代服务器优先级均被设为 1（高）。PM3 直接管理服务器电源和优先级。由于 PM3 控制兼容的服务器电源分配，因此 CMC 不再控制最大节能模式。因而此选择被禁用。

当启用**最大节能模式**时，CMC 会将“系统输入功率上限”设为机箱可处理的最大值。CMC 不允许功率超出最高容量。但是 PM3 可处理所有其他功率容量限制。

当禁用 PM3 电源管理时，CMC 会在启用外部管理之前恢复服务器优先级设置。

 **注：**当禁用 PM3 管理时，CMC 不会恢复最大机箱电源的先前设置。请参阅 **CMC 日志** 了解先前的设置以便手动恢复该值。


使用 CMC Web 界面配置电源预算和冗余

 **注：**要执行电源管理操作，必须具有**机箱配置管理员**权限。

要配置电源预算，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **电源** → **配置**。
2. 在**预算/冗余配置**页面中，根据需要选择以下任一或所有属性。有关字段说明的信息，请参阅[联机帮助](#)。
 - 启用基于服务器的电源管理
 - 系统输入功率上限
 - 冗余策略
 - 启用动态电源设备接入
 - 禁用机箱电源按钮
 - 最大节能模式
 - 启用远程电源日志记录
 - 远程电源日志记录间隔
3. 单击**应用**保存更改。

使用 RACADM 配置电源预算和冗余

 **注：**要执行电源管理操作，必须具有**机箱配置管理员**权限。

要启用和设置冗余策略，请执行以下操作：

1. 打开到 CMC 的串行/Telnet/SSH 文本控制台并登录。
2. 根据需要设置属性：

- 要选择冗余策略，请键入：

```
racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy <value>
```

其中 <value> 为 0（交流冗余）或 1（电源设备冗余）。默认值为 0。

例如，以下命令将冗余策略设置为 1：

```
racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy 1
```

- 要设置电源预算值，请键入：

```
racadm config -g cfgChassisPower -o cfgChassisPowerCap <value>
```

其中 <value> 为“当前运行时机箱负荷”和 5000 之间的数字，表示最大功率上限（瓦）。默认值为 5000。

例如，以下命令将最大电源预算设置为 5000 瓦：

```
racadm config -g cfgChassisPower -o cfgChassisPowerCap 5000
```

- 要启用或禁用动态 PSU 接入，请键入：

```
racadm config -g cfgChassisPower -o cfgChassisDynamicPSUEngagementEnable <value>
```

其中，<value> 为 0（禁用）或 1（启用）。默认值为 0。

例如，以下命令禁用动态 PSU 接入：

```
racadm config -g cfgChassisPower -o cfgChassisDynamicPSUEngagementEnable 0
```

- 要启用最大功率模式，请键入：

```
racadm config -g cfgChassisPower -o cfgChassisMaxPowerConservationMode 1
```

- 要恢复正常操作，请键入：

```
racadm config -g cfgChassisPower -o cfgChassisMaxPowerConservationMode 0
```

- 要启用电源远程日志记录功能，请输入以下命令：

```
racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingEnabled 1
```

- 要指定所需的日志记录间隔，请输入以下命令：

```
racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingInterval n
```

其中 n 为 1 至 1440 分钟。

- 要确定是否已启用电源远程日志记录功能，请输入以下命令：

```
racadm getconfig -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingEnabled
```

- 要确定电源远程日志记录间隔，请输入以下命令：

```
racadm getconfig -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingInterval
```

电源远程日志记录功能依赖于之前是否已在远程系统日志主机上配置此功能。必须启用登录到一台或多台远程系统日志主机，否则将记录功耗。可通过 Web GUI 或 RACADM CLI 完成此操作。有关更多信息，请参阅远程系统日志配置说明。

- 要启用通过 OpenManage Power Center (OPMC) 进行远程电源管理，请键入：

```
racadm config -g cfgChassisPower -o cfgChassisServerBasedPowerMgmtMode 1
```


- 要恢复 CMC 电源管理，请键入：

```
racadm config -g cfgChassisPower -o cfgChassisServerBasedPowerMgmtMode 0
```

有关机箱电源的 RACADM 命令的信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）中的 **config**、**getconfig**、**getpbinfo** 和 **cfgChassisPower** 部分。


执行电源控制操作

可以对机箱、服务器和 IOM 执行以下电源控制操作。

 **注:** 电源控制操作将影响整个机箱。

对机箱执行电源控制操作

CMC 能够对整个机箱（机箱、服务器、IOM 和 PSU）远程执行几项电源管理操作（如有序关机）。

 **注:** 要执行电源管理操作，必须具有**机箱配置管理员**权限。

使用 Web 界面对机箱执行电源控制操作

要使用 CMC Web 界面对机箱执行电源控制操作，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **电源** → **控制**。
此时将显示**机箱电源控制**页。
2. 选择以下任一电源控制操作。
有关各个选项的信息，请参阅**联机帮助**。
 - 打开系统电源
 - 关闭系统电源
 - 关闭系统电源后再开启（冷引导）
 - 重设 CMC（热引导）
 - 非正常关机
3. 单击**应用**。
将显示一个对话框，要求您进行确认。
4. 单击**确定**执行电源管理操作（例如，使系统重设）。

使用 RACADM 对机箱执行电源控制操作


打开到 CMC 的串行/Telnet/SSH 文本控制台，登录并键入：

```
racadm chassisaction -m chassis <action>
```

其中 *<action>* 为 powerup（开机）、powerdown（关机）、powercycle（关机后再开机）、nongraceshutdown（非正常关机）或 reset（重设）。

对服务器执行电源控制操作

可以一次对机箱中的多个服务器或对机箱中的单个服务器远程执行电源管理操作。

 **注:** 要执行电源管理操作，必须具有**机箱配置管理员**权限。

使用 CMC Web 界面对多个服务器执行电源控制操作

要使用 CMC Web 界面对多个服务器执行电源控制操作，请执行以下操作：


1. 在左侧窗格中，单击**服务器概览** → **电源**。
此时将显示**电源控制**页。
2. 在**操作**列中，从下拉菜单中为所需服务器选择以下任一电源控制操作：
 - 无操作
 - 打开服务器电源
 - 关闭服务器电源
 - 正常关机
 - 重设服务器（热引导）
 - 关闭服务器电源后再开启（冷引导）

有关各选项的信息，请参阅**联机帮助**。

3. 单击**应用**。
此时将显示要求确认的对话框。
4. 单击**确定**执行电源管理操作（例如，重设服务器）。

对 IOM 执行电源控制操作

您可以远程重设或开启 IOM。

 **注：**要执行电源管理操作，必须具有**机箱配置管理员**权限。

使用 CMC Web 界面对 IOM 执行电源控制操作

要对 I/O 模块执行电源控制操作，请执行以下步骤：

1. 在左侧窗格中，单击**机箱概览** → **I/O 模块概览** → **电源**。
2. 在**电源控制**页上，对于 IOM，从下拉菜单中选择希望执行的操作（关机后再开机）。
3. 单击**应用**。

使用 RACADM 对 IOM 执行电源控制操作

要使用 RACADM 对 IOM 执行电源控制操作，请打开至 CMC 的串行/Telnet/SSH 文本控制台，登录并键入：

```
racadm chassisaction -m switch <action>
```

其中 **<action>** 表示要执行的操作：power cycle。

管理机箱存储


在 Dell PowerEdge VRTX 上，可以执行以下操作：

- 查看物理磁盘驱动器和存储控制器的状态。
- 查看控制器、物理磁盘驱动器、虚拟磁盘和机柜的属性。
- 设置控制器、物理磁盘驱动器和虚拟磁盘。
- 分配虚拟适配器。
- 排除控制器、物理磁盘驱动器和虚拟磁盘故障。
- 更新存储组件。

查看存储组件的状态

要查看存储组件的状态，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **存储** → **属性** → **存储概览**。
2. 在**存储概览**页面中，可以执行以下操作：
 - 查看机箱中安装的物理磁盘驱动器的图形摘要及其状态。
 - 查看所有存储组件的摘要，包含指向其相应页面的链接。
 - 查看已用存储容量和总存储容量。
 - 查看控制器信息。
 - 查看最近记录的存储事件。

 **注：**有关更多信息，请参阅[联机帮助](#)。

查看存储拓扑


要查看存储拓扑，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **存储** → **属性** → **拓扑**。
2. 在**拓扑**页面中，单击 **<controller name>** 以查看相应页面。
3. 在每个已安装的控制器的下，单击**查看虚拟磁盘**、**<enclosure name>** 和**查看物理磁盘**链接以打开相应页面。

将虚拟适配器分配到插槽


可以通过先将虚拟磁盘映射到虚拟适配器 (VA)，再将虚拟适配器 (VA) 映射到服务器插槽来将虚拟磁盘映射到服务器插槽。

- 将 VA 分配到服务器插槽之前，请确保：
 - 服务器插槽为空，或者插槽中的服务器已关机。
 - 从服务器取消映射 VA。
- 系统将创建虚拟磁盘，并将其分配为**虚拟适配器 1**、**虚拟适配器 2**、**虚拟适配器 3** 或**虚拟适配器 4**。有关更多信息，请参阅[为虚拟磁盘应用虚拟适配器访问策略](#)。

 **注:** 每次只能将一个虚拟适配器映射到一个服务器。若没有适当的许可证，可以将 VA 映射到默认服务器，或者取消映射 VA 服务器分配。默认映射关系为 VA1-服务器插槽 1、VA2-服务器插槽 2、VA3-服务器插槽 3 和 VA4-服务器插槽 4。


使用虚拟适配器功能，可以与四个服务器共享已安装的存储。要从服务器插槽取消映射虚拟适配器，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **存储** → **设置** → **虚拟化**。
2. 在**存储虚拟化**页面上，从**操作**下拉菜单中选择**取消映射**，然后单击**应用**。
将取消该 VA 到所选服务器插槽的映射。

 **注:** 您可以通过选择**单一分配**或**多分配**模式来将虚拟磁盘分配到虚拟适配器。有关这些模式的更多信息，请参阅**联机帮助**。

使用 CMC Web 界面查看控制器属性

要查看控制器属性，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **控制器**。
2. 在**控制器**页面的**控制器**部分下，可以查看控制器的基本属性。但是，要查看高级属性，请单击 。有关控制器的更多信息，请参阅**联机帮助**。

使用 RACADM 查看控制器属性

要使用 RACADM 查看控制器属性，请运行命令 `racadm raid get controllers -o`

有关更多信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

导入或清除外部配置

必须将外部磁盘插入机箱。

要导入或清除外部配置，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **存储** → **控制器** → **设置**。
2. 在**控制器设置**页面的**外部配置**部分，针对各个控制器，单击：
 - **清除外部配置**以清除现有磁盘配置。
 - **导入/恢复**以导入具有外部配置的磁盘。

使用 CMC Web 界面查看物理磁盘属性

确保机箱中安装了物理磁盘。

要查看物理磁盘驱动器的属性，请执行以下操作：

1. 在左侧窗格中，转到**机箱概览** → **存储** → **物理磁盘**。
此时将显示**属性**页。
2. 要查看所有物理磁盘驱动器的属性，请在**物理磁盘**部分，单击 **+**。您也可以使用以下筛选器查看特定物理磁盘驱动器的属性：
 - 在**基本物理磁盘筛选器**选项下，从**分组依据**下拉菜单中，选择**虚拟磁盘**、**控制器**或**机柜**，然后单击**应用**。
 - 单击**高级筛选器**，选择各属性的值，然后单击**应用**。

使用 RACADM 查看物理磁盘驱动器属性

要使用 RACADM 查看物理磁盘驱动器的属性，请运行命令 `racadm raid get pdisks -o`

有关更多信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

识别物理磁盘和虚拟磁盘

有关启用或禁用 LED 闪烁功能的更多信息，请参阅：

- [使用 CMC Web 界面配置 LED 闪烁](#)
- [使用 RACADM 配置 LED 闪烁](#)

使用 CMC Web 界面分配全局热备用

要分配或取消分配全局热备用，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **存储** → **物理磁盘** → **设置**。
将显示**设置物理磁盘**页面。
2. 在**全局热备用分配**部分下的**热备用操作**下拉菜单中，为各个物理磁盘驱动器选择**未分配**或**全局热备用**，然后单击**应用**。或者，从**热备用操作 - 分配至所有**下拉菜单中选择**未分配**或**全局热备用**，然后单击**应用**。

使用 RACADM 分配全局热备用


要使用 RACADM 分配全局热备用，请运行命令 `racadm raid hotspare: -assign yes -type ghs`。

有关使用 RACADM 命令的更多信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

使用 CMC Web 界面查看虚拟磁盘属性

确保创建了虚拟磁盘。

要查看虚拟磁盘属性，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **存储** → **虚拟磁盘** → **属性**。
2. 在**属性**页面的**虚拟磁盘**部分，单击 。您也可以使用以下筛选器查看特定虚拟磁盘属性：
 - 在**基本虚拟磁盘筛选器**部分，从**控制器**下拉菜单中选择控制器名称，然后单击**应用**。
 - 单击**高级筛选器**，选择各属性的值，然后单击**应用**。


使用 RACADM 查看虚拟磁盘属性

要使用 RACADM 查看虚拟磁盘属性，请运行命令 `racadm raid get vdisks -o`

有关更多信息，请参阅 *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide*（Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南）。

使用 CMC Web 界面创建虚拟磁盘

确保在机箱中安装了物理磁盘。

 **注：**删除虚拟磁盘会将该虚拟磁盘从控制器配置中移除。

要创建虚拟磁盘，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **存储** → **虚拟磁盘** → **创建**。
2. 在**创建虚拟磁盘**页面的**设置**部分，键入相应数据，然后在**选择物理磁盘**部分，基于先前选择的 RAID 级别选择物理磁盘驱动器数目，然后单击**创建虚拟磁盘**。

为虚拟磁盘应用虚拟适配器访问策略

确保已安装物理磁盘驱动器，并且已创建虚拟磁盘。

要应用虚拟适配器访问策略，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **存储** → **虚拟磁盘** → **分配**。
2. 在**分配虚拟磁盘**页面的**虚拟适配器的访问策略**部分中，从**虚拟适配器 <number>**下拉菜单中为每个物理磁盘驱动器选择**完全访问**。
3. 单击**应用**。

现在可以将虚拟适配器分配到服务器插槽。有关更多信息，请参阅本用户指南中的“将虚拟适配器分配到插槽”部分。

使用 CMC Web 界面修改虚拟磁盘属性

要修改虚拟磁盘属性，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **存储** → **虚拟磁盘** → **管理**。
2. 在**管理虚拟磁盘**页上，从**虚拟磁盘操作**下拉菜单中选择下列操作之一，然后单击**应用**。
 - **重命名**
 - **删除**



注：如果选择“删除”，将显示以下消息，指示删除虚拟磁盘将永久删除该虚拟磁盘中的数据。

Deleting the virtual disk removes the virtual disk from the controller's configuration. Initializing the virtual disk permanently erases data from the virtual disk.




注：如果选择“删除”，将显示以下消息，指示删除虚拟磁盘将永久删除该虚拟磁盘中的数据。

Deleting the virtual disk removes the virtual disk from the controller's configuration. Initializing the virtual disk permanently erases data from the virtual disk.

- **编辑策略：读取高速缓存**
- **编辑策略：写入高速缓存**
- **编辑策略：磁盘高速缓存**
- **初始化：快速**
- **初始化：完全**

使用 CMC Web 界面查看机柜属性

要查看机柜属性，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **存储** → **机柜** → **属性**。
2. 在**属性**页面的**机柜**部分下，单击  可查看物理磁盘驱动器及其状态的图形视图、物理磁盘驱动器插槽摘要以及高级属性。

管理 PCIe 插槽

默认情况下，所有插槽均未映射。您可以执行以下操作：

- 查看机箱中所有 PCIe 插槽的状态。
- 向服务器分配或取消分配 PCIe 插槽。


在向服务器分配 PCIe 插槽之前请考虑以下因素：

- 不能将空 PCIe 插槽分配给开启的服务器。
- 如果当前被分配的服务器（源）处于开启状态，则适配器已分配给某一服务器的 PCIe 插槽不能分配给另一服务器。
- 不能将适配器已分配给某个服务器的 PCIe 插槽分配给另一个已经开启的（目标）服务器。


在从服务器取消分配 PCIe 插槽之前请考虑以下因素：

- 如果 PCIe 插槽为空，则可以从服务器取消分配该插槽，即使该服务器处于开启状态。
- 如果 PCIe 插槽有适配器且未开启，则可以从服务器取消分配该插槽，即使该服务器处于开启状态。当某个插槽为空，并且被分配的服务器处于开启状态，然后用户在空插槽中插入适配器时，可能会发生这种情况。

有关分配和取消分配 PCIe 插槽的更多信息，请参阅[联机帮助](#)。

 **注：**在没有许可证的情况下，最多可以向一台服务器分配两个 PCIe 设备。

使用 CMC Web 界面查看 PCIe 插槽属性

- 要查看全部八个 PCIe 插槽的信息，请在左侧窗格中单击**机箱概览** → **PCIe 概览**。单击  查看所需插槽的全部属性。
- 要查看一个 PCIe 插槽的信息，请单击 **机箱概览** → **PCIe 插槽 <number>** → **属性** → **状态**。

使用 CMC Web 界面将 PCIe 插槽分配至服务器

要将 PCIe 插槽分配至服务器，请执行以下操作：

- 在左侧窗格中，单击**机箱概览** → **PCIe 概览** → **设置** → **映射：从 PCIe 插槽到服务器插槽**。在**映射：从 PCIe 插槽到服务器插槽**页面中，在**操作列的操作**下拉菜单中选择相应的服务器名称，然后单击**应用**。

有关将 PCIe 设备分配至服务器的更多信息，请参阅[联机帮助](#)。

使用 RACADM 管理 PCIe 插槽

您可以使用 RACADM 命令向服务器分配或取消分配 PCIe 插槽。这里提供了一些命令。有关 RACADM 命令的更多信息，请参阅 dell.com/support/Manuals 上的 *Chassis Management Controller for PowerEdge VRTX RACADM*

Command Line Reference Guide (Chassis Management Controller for PowerEdge VRTX RACADM 命令行参考指南)。

- 要查看当前分配给服务器的 PCIe 设备，请运行以下命令：

```
racadm getpciecfg -a
```

- 要使用 FQDD 查看 PCIe 设备的属性，请运行以下命令：

```
racadm getpciecfg [-c <FQDD>]
```

例如，要查看 PCIe 设备 1 的属性，请运行以下命令：

```
racadm getpciecfg -c pcie.chassisslot.1
```

- 要将 PCIe 适配器插槽分配给服务器插槽，请运行以下命令：

```
racadm setpciecfg assign [-c <FQDD>] [i <server slot>]
```

- 例如，要将 PCIe 插槽 5 分配给服务器插槽 2，请运行以下命令：

```
racadm setpciecfg assign -c pcie.chassisslot.5 -i 2
```

- 要从服务器取消分配 PCIe 插槽 3，请运行以下命令：

```
racadm setpciecfg unassign -c pcie.chassisslot.3
```

故障排除和恢复

本部分介绍如何使用 CMC Web 界面执行与远程系统问题恢复和故障排除相关的任务。

- 查看机箱信息。
- 查看事件日志。
- 收集配置信息、错误状态和错误日志。
- 使用诊断控制台。
- 管理远程系统上的电源。
- 管理远程系统上的 Lifecycle Controller 作业。
- 重置组件。
- 网络时间协议 (NTP) 故障排除。
- 网络问题故障排除。
- 警报问题故障排除。
- 重设忘记的管理员密码。
- 保存并还原机箱配置设置和证书。
- 查看错误代码和日志。

使用 RACDUMP 收集配置信息、机箱状态和日志

`racdump` 子命令是获得全面机箱状态、配置状态信息和历史事件日志的单一命令。

`racdump` 子命令显示以下信息：

- 常规系统/RAC 信息
- CMC 信息
- 机箱信息
- 会话信息
- 传感器信息
- 固件版次信息

支持的接口

- CLI RACADM
- 远程 RACADM
- Telnet RACADM

`racdump` 包含以下子系统并聚集以下 RACADM 命令。有关 `racdump` 的更多信息，请参阅 *RACADM Command Line Reference Guide for CMC in PowerEdge VRTX*（适用于 PowerEdge VRTX 中的 CMC 的 RACADM 命令行参考指南）。

子系统	RACADM 命令
常规系统/RAC 信息	getsysinfo
会话信息	getssninfo
传感器信息	getsensorinfo
交换机信息 (IO 模块)	getioinfo
夹层卡信息 (子卡)	getdcinfo
所有模块信息	getmodinfo
电源预算信息	getpbinfo
KVM 信息	getkvminfo
NIC 信息 (CMC 模块)	getniccfg
冗余信息	getredundancymode
跟踪日志信息	gettraceolog
RAC 事件日志	getraclog
系统事件日志	getsel

下载 SNMP 管理信息库 (MIB) 文件

CMC SNMP MIB 文件定义机箱类型、事件和指示灯。使用 CMC 可以通过 Web 界面下载 MIB 文件。

要使用 CMC Web 界面下载 CMC 的 SNMP 管理信息库 (MIB) 文件，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **网络** → **服务** → **SNMP**。
2. 在 **SNMP 配置** 部分中，单击**保存**将 CMC MIB 文件下载到本地系统。
有关 SNMP MIB 文件的更多信息，请参阅 dell.com/support/manuals 上的 *Dell OpenManage Server Administrator SNMP Reference Guide* (Dell OpenManage Server Administrator SNMP 参考指南)。

远程系统故障排除首先需要执行的步骤

以下问题常用于管理系统中的高级别排除故障：

- 系统开机还是关机？
- 如果是开机，操作系统是正常运行、无响应还是停止运行？
- 如果是关机，电源是意外关闭的吗？

电源故障排除

以下信息可帮助您对电源设备和电源相关问题进行故障排除：

- **问题：**将**电源冗余策略**配置成了**交流冗余**，并发出电源设备冗余丢失事件。
 - **解决方案 A：**此配置要求在模块化机柜中，1 侧（左边 2 个插槽）至少有 1 个电源设备且 2 侧（右边 2 个插槽）至少有 1 个电源设备存在并且可正常运行。另外，每侧的容量必须足以支持机箱的总功率分配要求，以维持**交流冗余**。（为了获得完整的交流冗余，确保提供由 4 个电源设备组成的完整 PSU 配置。）
 - **解决方案 B：**检查确认所有电源设备是否正确连接到两个交流电网；1 侧的电源设备必须连接到一个交流电网；2 侧的电源设备必须连接到另一个交流电网；且两个交流电网都能正常工作。如果其中一个交流电网无法正常工作，则**交流冗余**会丢失。

- **问题：** PSU 状态显示为**失败（无交流）**，即使已连接交流电缆并且配电装置的交流输出良好。
 - **解决方案 A：** 检查并更换交流电缆。检查并确认为电源设备供电的配电装置是否按预期方式工作。如果故障依然存在，请致电 Dell 客户服务更换电源设备。
 - **解决方案 B：** 确认 PSU 连接的电压是否与其他 PSU 相同。如果 CMC 检测到在不同电压下工作的 PSU，则此 PSU 会被关闭并标记为“故障”。
- **问题：** 动态电源设备接入已启用，但**待机**状态中没有显示任何电源。
 - **解决方案 A：** 剩余功率不足。一个或多个电源设备仅会在机柜内的剩余功率超过至少一个电源设备的容量时进入待机状态。
 - **解决方案 B：** 机柜内的电源设备装置不足以完全支持动态电源设备接入。要确认是否属于这种情况，请使用 Web 界面关闭动态电源设备接入，然后再次打开。如果不能完全支持动态电源设备接入，则会显示一条消息。
- **问题：** 将新服务器插入供电充足的机柜，但服务器无法开机。
 - **解决方案 A：** 检查系统输入功率上限设置 - 它的配置可能太低，导致不允许任何附加服务器开机。
 - **解决方案 B：** 检查最大节能设置。如果设置了该模式，则会发生此问题。有关更多详情，请参阅电源配置设置。
 - **解决方案 C：** 检查与新插入服务器相关的插槽的服务器插槽电源优先级，确保它不低于任何其他服务器插槽的电源优先级。
- **问题：** 可用电源不断变化，即便没有更改模块化机柜配置。
 - **解决方案：** CMC 具有动态风扇电源管理功能，如果机柜在接近用户配置的功率上限峰值下运行时，则会暂时减少服务器的分配；这将导致通过降低服务器性能来为风扇分配电源，以保证输入功率低于**系统输入功率上限**。这是一种正常行为。
- **问题：** 报告有 <number>W 的**峰值性能盈余**。
 - **解决方案：** 机柜在当前配置中具有 <number>W 的盈余功率，并且**系统输入功率上限**可安全地降低报告的数值，而不会影响服务器性能。
- **问题：** 一部分服务器在交流电网故障后失去供电，即便机箱在带有四个电源设备的**交流冗余**配置下运行。
 - **解决方案：** 发生交流电网故障时，如果电源设备未正确连接到冗余交流电网，就会发生这种问题。**交流冗余策略**要求左侧的两个电源设备连接到一个交流电网，右侧的两个电源设备连接到另一个交流电网。如果未正确连接两个 PSU，例如将 PSU 2 和 PSU 3 连接到错误的交流电网，则交流电网故障会造成最低优先级服务器发生断电。
- **问题：** 最低优先权服务器在 PSU 故障后损失电源。
 - **解决方案：** 为了防止未来的电源设备故障导致服务器断电，请确保机箱至少有三个电源设备，并且配置了**电源设备冗余策略**，以防止 PSU 故障影响服务器运行。
- **问题：** 数据中心的室温提高时，总体服务器性能下降。
 - **解决方案：** 如果**系统输入功率上限**配置的值导致风扇的电源需求增加而将服务器的电源分配降低，则会发生这种问题。用户可将**系统输入功率上限**增加到更高的值，允许为风扇分配额外电源而不会影响服务器性能。

警报故障排除


使用 CMC 日志和跟踪日志进行 CMC 警报故障排除。每次成功或失败的电子邮件和/或 SNMP 陷阱传递尝试都会记录到 CMC 日志中。描述具体错误的附加信息将记录到跟踪日志中。但是，由于 SNMP 并不确认陷阱的传递，因此请使用网络分析器或 Microsoft 的 snmputil 等工具跟踪管理系统中的信息包。


查看事件日志

可以查看硬件和机箱日志，了解管理系统上发生的系统级严重事件的信息。

查看硬件日志

CMC 生成发生在机箱上的事件的硬件日志。可以使用 Web 界面和远程 RACADM 查看硬件日志。

 **注:**要清除硬件日志，必须具备**清除日志管理员**权限。

 **注:**可以配置 CMC 在发生特定事件时发送电子邮件或 SNMP 陷阱。有关配置 CMC 以发送警报的信息，请参阅[配置 CMC 以发送警报](#)。


硬件日志条目示例

```
critical System Software event: redundancy lost Wed May 09 15:26:28 2007 normal
System Software event: log cleared was asserted Wed May 09 16:06:00 2007
warning System Software event: predictive failure was asserted Wed May 09
15:26:31 2007 critical System Software event: log full was asserted Wed May 09
15:47:23 2007 unknown System Software event: unknown event
```


使用 CMC Web 界面查看硬件日志


您可以查看、保存和清除硬件日志。可以单击列标题基于“严重性”、“日期/时间”或“说明”对日志条目排序。

要使用 CMC Web 界面查看硬件日志，请在左侧窗格中单击**机箱概览** → **日志**。将显示**硬件日志**页面。要将硬件日志的副本保存到管理站或网络，请单击**保存日志**，然后指定日志的文本文件的位置。

 **注:**因为日志保存为文本文件，所以不会显示用于在用户界面中指示严重性的图形图像。在文本文件中，严重性以**正常**、**通知**、**未知**、**警告**和**严重**等词语表示。日期和时间条目以升序显示。如果在**日期/时间**列中出现 <SYSTEM BOOT>，则表示在任何模块开启或关闭时发生的事件，此时日期或时间不可用。

若要清除硬件日志，请单击**清除日志**。

 **注:**CMC 会创建一个新的日志条目表示日志已清除。

 **注:**要清除硬件日志，您必须具有**清除日志管理员**权限。

使用 RACADM 查看硬件日志

要使用 RACADM 查看硬件日志，请打开至 CMC 的串行/Telnet/SSH 文本控制台，登录并键入：


```
racadm getsel
```

要清除硬件日志，请键入：

```
racadm clrsel
```

查看机箱日志

CMC 生成与机箱相关事件的日志。

 **注:**要清除机箱日志，您必须具有**清除日志管理员**权限。

使用 RACADM 查看机箱日志

要使用 RACADM 查看机箱日志信息，请打开至 CMC 的串行、Telnet、SSH 文本控制台，登录并输入以下命令：

```
racadm chassislog view
```

此命令显示最近的 25 个机箱日志条目。

要显示查看机箱日志的可用选项，请运行以下命令：

```
racadm chassislog help view
```

使用 Web 界面查看机箱日志


您可以查看、保存和清除机箱日志。可以基于日志类型和筛选器筛选日志。此外，甚至还可以基于关键字执行搜索，或者查看指定天数的日志。

在左侧窗格中，单击**机箱概览** → **日志** → **机箱日志**。将显示**机箱日志**页。

要将机箱日志的副本保存到管理站或网络，请单击**保存日志**，然后指定保存日志文件的位置。

使用诊断控制台

如果您是一位高级用户或在技术支持指导下的用户，可以使用 CLI 命令诊断与机箱硬件相关的问题。


 **注:**要修改这些设置，您必须具有**调试命令管理员**权限。

要访问诊断控制台，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **故障排除** → **诊断**。
此时将显示**诊断控制台**页。
2. 在**命令**文本框中，输入命令并单击**提交**。
有关命令的信息，请参阅**联机帮助**。
此时将显示诊断结果页面。

重设组件

您可以重设活动的 CMC，或者虚拟重设服务器，使其产生如同被卸下并重新插入的效果。如果机箱有一个待机 CMC，重设活动的 CMC 会造成故障转移并且待机 CMC 变为活动状态。

 **注:**要重设组件，必须具备**调试命令管理员**权限。


要使用 CMC Web 界面重设组件，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **故障排除** → **重设组件**。
此时将显示**重设组件**页。
2. 要重设活动的 CMC，请在 **CMC 状态**部分，单击**重设/故障转移 CMC**。如果存在待机 CMC 并且机箱为完全冗余，则会发生故障转移，导致待机 CMC 变为活动状态。但是，如果不存在待机 CMC，则将重新引导可用的 CMC。
3. 要虚拟重置服务器，请在**虚拟重置服务器**部分，选择要重置的服务器，然后单击**应用选择**。
有关更多信息，请参阅**联机帮助**。
此操作使服务器产生如同卸下并重新插入的效果。

保存或还原机箱配置

这是一项许可功能。要使用 CMC Web 界面保存或还原机箱配置备份，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **设置** → **机箱备份**。将显示**机箱备份**页面。要保存机箱配置，请单击**保存**。覆盖默认文件路径（可选），然后单击**确定**保存文件。默认备份文件名包含机箱的服务标签。以后使用此备份文件只能还原此机箱的设置和证书。
2. 要还原机箱配置，在“还原”部分单击**浏览**，指定备份文件，然后单击**还原**。

 **注:**CMC 不会在还原配置时重设，不过，CMC 服务可能需要一些时间才能有效实施任何更改或新增的配置。成功完成后，所有当前会话都会关闭。

网络时间协议 (NTP) 错误故障排除

配置 CMC 将其时钟和网络上的远程时间服务器同步后，可能需要 2-3 分钟日期和时间才会发生改变。如果这段时间后仍没有改变，可能需要排除故障。出于以下原因，CMC 可能无法同步其时钟：

- NTP 服务器 1、NTP 服务器 2 和 NTP 服务器 3 设置有问题。
- 可能不小心输入了无效的主机名或 IP 地址。
- 网络连接问题，妨碍 CMC 与任一配置的 NTP 服务器进行通信。
- DNS 问题，妨碍解析任意 NTP 服务器主机名。

要解决与 NTP 相关的问题，请检查 CMC 跟踪日志中的信息。该日志包含与 NTP 相关的故障的错误消息。如果 CMC 未能与任何配置的远程 NTP 服务器同步，则 CMC 时间与本地系统时钟同步，并且跟踪日志包含与下面类似的条目：

```
Jan 8 20:02:40 cmc ntpd[1423]: synchronized to LOCAL(0), stratum 10
```

您还可以键入以下 `racadm` 命令检查 `ntpd` 状态：

```
racadm gettractime -n
```


如果配置的一台服务器没有显示 “*”，可能设置未正确配置。该命令的输出包含详细的 NTP 统计数据，在解决问题时，这些统计数据可能很有用。

如果您尝试配置基于 Windows 的 NTP 服务器，增大 `ntpd` 的 `MaxDist` 参数可能很有帮助。在更改此参数之前，请了解所有影响，因为默认设置必须足够大，才可配合多数 NTP 服务器运行。

要修改参数，请键入以下命令：

```
racadm config -g cfgRemoteHosts -o cfgRhostsNtpMaxDist 32
```

在进行更改后，禁用 NTP，等待 5-10 秒，然后再次启用 NTP：

 **注：**NTP 可能还要再等待 3 分钟才能再次同步。

要禁用 NTP，请键入：

```
racadm config -g cfgRemoteHosts -o cfgRhostsNtpEnable 0
```

要启用 NTP，请键入：

```
racadm config -g cfgRemoteHosts -o cfgRhostsNtpEnable 1
```

如果 NTP 服务器正确配置且此条目存在于追踪日志中，则此项确认 CMC 不能与任何已配置的 NTP 服务器同步。

如果未配置 NTP 服务器 IP 地址，可能会看到与以下内容类似的跟踪日志条目：

```
Jan 8 19:59:24 cmc ntpd[1423]: Cannot find existing interface for address 1.2.3.4 Jan 8 19:59:24 cmc ntpd[1423]: configuration of 1.2.3.4 failed
```

如果 NTP 服务器设置配置了一个无效的主机名，可能看到如下所示的跟踪日志条目：

```
Aug 21 14:34:27 cmc ntpd_initres[1298]: host name not found: blabla Aug 21 14:34:27 cmc ntpd_initres[1298]: couldn't resolve `blabla', giving up on it
```

有关如何使用 CMC Web 界面输入 `gettracelog` 命令查看跟踪日志的信息，请参阅[使用诊断控制台](#)。

LED 颜色和闪烁样式说明

机箱上的 LED 指示以下组件状态：

- 呈绿色稳定发光的 LED 表示组件已打开电源。如果绿色 LED 持续闪烁，则表示严重但属于例行程序的事件（如固件上载）。在此期间该装置无法工作，但不表示发生故障。

- 组件上持续闪烁的琥珀色 LED 表示该模块发生故障。
- 呈蓝色闪烁的 LED 可由用户配置并可用于标识。有关配置的更多信息，请参阅[下载 SNMP 管理信息库 MIB 文件](#)。


表. 31: LED 颜色和闪烁样式

组件	LED 颜色, 闪烁样式	状态
CMC	绿色, 稳定发光	已打开电源
	绿色, 闪烁	正在上载固件
	绿色, 暗色	已关闭电源
	蓝色, 稳定发光	活动
	蓝色, 闪烁	用户启用的模块标识符
	琥珀色, 稳定发光	未使用
	琥珀色, 闪烁	故障
	蓝色, 暗色	待机
服务器	绿色, 稳定发光	已打开电源
	绿色, 闪烁	正在上载固件
	绿色, 暗色	已关闭电源
	蓝色, 稳定发光	正常
	蓝色, 闪烁	用户启用的模块标识符
	琥珀色, 稳定发光	未使用
	琥珀色, 闪烁	故障
	蓝色, 暗色	无故障
IOM (常规)	绿色, 稳定发光	已打开电源
	绿色, 闪烁	正在上载固件
	绿色, 暗色	已关闭电源
	蓝色, 稳定发光	正常/堆栈主装置
	蓝色, 闪烁	用户启用的模块标识符
	琥珀色, 稳定发光	未使用
	琥珀色, 闪烁	故障
	蓝色, 暗色	无故障/堆栈从属装置
IOM (直通)	绿色, 稳定发光	已打开电源
	绿色, 闪烁	未使用
	绿色, 暗色	关机
	蓝色, 稳定发光	正常
	蓝色, 闪烁	用户启用的模块标识符

组件	LED 颜色, 闪烁样式	状态
鼓风机	琥珀色, 稳定发光	未使用
	琥珀色, 闪烁	故障
	蓝色, 暗色	无故障
	绿色, 稳定发光	风扇正在运行
	绿色, 闪烁	未使用
	绿色, 暗色	已关闭电源
	琥珀色, 稳定发光	无法识别风扇类型, 更新 CMC 固件
	琥珀色, 闪烁	风扇出现故障; 转速计超出范围
PSU	琥珀色, 暗色	未使用
	(椭圆) 绿色, 稳定发光	交流正常
	(椭圆) 绿色, 闪烁	未使用
	(椭圆) 绿色, 暗色	交流不正常
	琥珀色, 稳定发光	未使用
	琥珀色, 闪烁	故障
	琥珀色, 暗色	无故障
	(圆形) 绿色, 稳定发光	直流正常
(圆形) 绿色, 暗色	直流不正常	

无响应 CMC 的故障排除


如果使用任意界面（Web 界面、Telnet、SSH、远程 RACADM 或串行）都无法登录到 CMC，则可以通过观察 CMC 上的 LED、使用 DB-9 串行端口获取恢复信息或恢复 CMC 固件映像来验证 CMC 功能。

 **注:** 无法使用串行控制台登录待机 CMC。

观察 LED 隔离问题

插卡的左侧有两个 LED：

- 顶部 LED - 指示电源状态。如果该 LED 未亮：
 - 请验证至少有一个交流电源设备。
 - 验证 CMC 卡是否正确就位。可以释放或拉动排出器手柄，卸下 CMC，重新安装 CMC 以确保插板已插入到位且门锁正确关闭。
- 底部左侧 LED - 此 LED 有多种颜色。当 CMC 活动且正在运行时，如果没有问题，则底部 LED 是蓝色。如果是琥珀色，则表示检测到故障。故障可能由以下三种事件中的任意一种引发：
 - 核心故障。这种情况下，必须更换 CMC 板。
 - 自检故障。这种情况下，必须更换 CMC 板。
 - 映像损坏。这种情况下，可以通过上载 CMC 固件映像恢复 CMC。

 **注:** 正常进行 CMC 引导或重设时，需要花费一分钟时间才能完全引导操作系统并进入允许登录状态。蓝色 LED 在活动 CMC 上启用。在两个 CMC 的冗余配置中，待机 CMC 仅启用顶部右侧的绿色 LED。

从 DB-9 串行端口获取恢复信息

如果底部 LED 是琥珀色，则可以从位于 CMC 前方的 DB-9 串行端口获取恢复信息。

要获取恢复信息，请执行以下操作：

1. 在 CMC 系统和客户端系统之间安装零调制解调器电缆。
2. 打开您选择的终端仿真器（如 HyperTerminal 或 Minicom）。看到系统提示时输入以下规格：8 位、无奇偶校验、无流控制、波特率 115200。
核心内存故障每隔 5 秒钟显示一次错误消息。

3. 按 <Enter> 键。

如果出现恢复提示，则可以获得其他信息。该提示指示 CMC 插槽编号和故障类型。

要显示一些命令的故障原因和语法，请键入 `recover`，然后按 <Enter>。

示例提示：

```
recover1[self test] CMC 1 self test failure
recover2[Bad FW images] CMC2 has corrupted images
```


- 如果提示出现自检故障，CMC 中没有可维修的组件。CMC 损坏且必须退回 Dell。
- 如果提示指出 **Bad FW Images**（固件映像损坏），请完成[恢复固件映像](#)中的任务。


恢复固件映像

当 CMC 无法正常引导至操作时，它将进入恢复模式。在恢复模式下，提供少量命令子集以便通过上载固件更新文件 `firming.cmc` 对 Flash 设备重新编程。该文件与正常固件更新所使用的固件映像文件相同。恢复进程将显示其当前活动并在完成后引导至 CMC 操作系统。

当在 `recovery` 提示符下键入 `recover` 然后按下 <Enter> 时，将显示恢复原因和可用子命令。下面是一个恢复序列示例：

```
recover getniccfg recover setniccfg 192.168.0.120 255.255.255.0 192.168.0.1
recover ping 192.168.0.100 recover fwupdate -g -a 192.168.0.100
```

 **注:** 将网络电缆连接到最左侧的 RJ45。

 **注:** 在恢复模式下，因为没有活动网络堆栈，所以无法正常 ping CMC。`recover ping <TFTP server IP>` 命令可以对 TFTP 服务器执行 ping 命令以检验 LAN 连接。在一些系统上可能需要使用 `recover reset` 命令（在 `setniccfg` 命令后）。

排除网络故障

内部 CMC 跟踪日志可用于调试 CMC 警报和网络。可使用 CMC Web 界面或 RACADM 访问跟踪日志。请参阅 *RACADM Command Line Reference Guide for iDRAC7 and CMC*（适用于 iDRAC7 和 CMC 的 RACADM 命令行参考指南）中的 `gettracelog` 命令部分。

跟踪日志跟踪以下信息：


- DHCP - 跟踪发送到 DHCP 服务器和从 DHCP 服务器接收的数据包。
- DDNS - 跟踪动态 DNS 更新请求和响应。
- 对网络接口所做的配置更改。

跟踪日志还可能包含 CMC 固件特定的错误代码，与内部 CMC 固件有关，而不是管理系统的操作系统。

控制器故障排除

要排除控制器故障，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览** → **存储** → **控制器** → **故障排除**。
2. 在**控制器故障排除**页，从相应控制器的**操作**下拉列表中，选择下列任一选项，然后单击**应用**。
 - **重设配置** - 删除虚拟磁盘和热备用。不过，磁盘上的数据不会被擦除。
 - **导出 TTY 日志** - 存储控制器上的 TTY 调试日志导出到本地系统。

 **注:** 如果存在已驻留高速缓存，将显示清除选项。如果不存在已驻留高速缓存，将不显示此选项。

使用 LCD 面板界面

可以使用机箱中的 LCD 面板执行配置和诊断，并获取关于机箱及其组件的状态信息。

下图说明了 LCD 面板。LCD 屏幕显示菜单、图标、图片和消息。

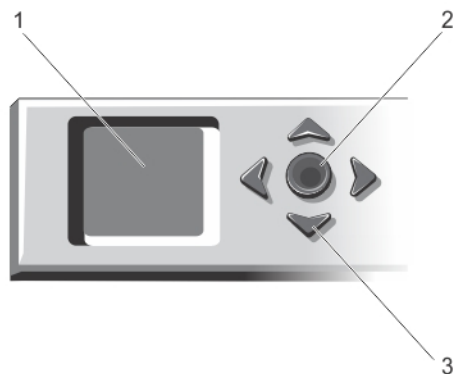


图 2: LCD 显示屏

- | | |
|--------------|---------------|
| 1. LCD 屏幕 | 2. 选择（“选中”）按钮 |
| 3. 滚动按钮（4 个） | |

LCD 导航

LCD 面板的右侧包含五个按钮：四个箭头按钮（向上、向下、向左和向右）以及一个中央按钮。

- 要在屏幕之间移动，请使用向右（下一屏）和向左（上一屏）箭头按钮。使用面板过程中的任意时刻，都可以返回到上一屏。
- 要在屏幕上的选项间滚动，请使用向下和向上箭头按钮。
- 要选择并保存屏幕上的某个项目并移动到下一屏，请使用中央按钮。

可以使用上、下、左和右箭头按钮更改屏幕上所选的菜单项或图标。所选项目以浅蓝色背景或边框显示。

当 LCD 屏幕上显示的消息长度超过屏幕长度，使用左和右箭头按钮向左右滚动文本。

下表说明的图标用于在 LCD 屏幕之间导航。

表. 32: LCD 面板导航图标

普通图标



高亮显示图标



图标名称和说明

后退 - 高亮显示并按下中央按钮可返回至上一个屏幕。

接受/是 - 高亮显示并按下中央按钮可接受更改并返回至上一个屏幕。




跳过/下一步 - 高亮显示并按下中央按钮可跳过任何更改并转到下一个屏幕。



否 - 高亮显示并按下中央按钮表示对问题回答“否”，并转到下一屏幕。



组件标识 - 组件上闪烁的蓝色 LED。

 **注:** 当启用“组件标识”时，此图标四周将出现不断闪烁的蓝色矩形框。

LCD 面板上的状态指示 LED 提供机箱及其组件的整体运行状况提示。

- 稳定蓝色表示运行状况良好。
- 不停闪烁的琥珀色表示至少一个组件处于故障状态。
- 不停闪烁的蓝色为 ID 信号，用于识别一组机箱中的某个机箱。

主菜单

从**主菜单**中，可导航至以下屏幕：

- **KVM 映射** - 包含在 KVM 与服务器之间进行映射或取消映射的选项。
- **DVD 映射** - 只有在安装了 DVD 驱动器的情况下，此选项才会显示在**主菜单**屏幕中。
- **机柜** - 显示机箱的状态信息。
- **IP 摘要** - 显示关于 CMC IPv4、CMC IPv6、iDRAC IPv4 和 iDRAC 4 IPv6 的信息。
- **设置** - 包含 **LCD 语言**、**机箱方向**、**默认 LCD 屏幕**和**网络设置**等选项。


KVM 映射菜单

通过此屏幕可以查看从 KVM 到服务器的映射信息、将另一台服务器映射到 KVM，或者取消映射现有连接。要为服务器使用 KVM，请从主菜单中选择 **KVM 映射**，导航至相应的服务器，然后按中央**选中**按钮。

DVD 映射

通过使用此页面，可以查看从 DVD 到服务器的映射信息、将另一个服务器映射到机箱上的 DVD 驱动器，或者取消映射现有连接。要使服务器能够访问 DVD，请从主菜单中选择 **DVD 映射**，导航至所需的服务器，然后按中间的**选中**按钮。

只有在服务器插槽已启用 DVD 的情况下，才能将 DVD 驱动器映射到该服务器插槽。也可以取消映射 DVD 驱动器，以防止任何服务器插槽使用该驱动器。如果 DVD 驱动器与主板之间的 SATA 电缆未正确连接，则 DVD 驱动器的运行状况将为严重。如果 DVD 驱动器的运行状况为严重，则服务器无法访问该 DVD 驱动器。

 **注:** 只有在安装了 DVD 驱动器的情况下，DVD 映射功能才会显示在 LCD **主菜单**屏幕中。

机柜菜单

从此屏幕可导航至以下屏幕：

- **正面状态**

- 背面
- 侧面
- 机柜状态

使用导航按钮高亮显示所需的项目（高亮显示**后退**图标返回**主菜单**），然后按下中央按钮。此时将显示所选的屏幕。

IP 摘要菜单

IP 摘要屏幕显示关于 CMC（IPv4 和 IPv6）以及机箱中安装的每个服务器的 IP 信息。

使用上下箭头按钮在列表中滚动。使用左右箭头按钮滚动超过屏幕长度的所选消息。

使用上下箭头按钮选择**后退**图标并按下中央按钮返回**机柜菜单**。

设置

设置菜单显示可配置项目的菜单：

- **LCD 语言** - 选择要用于 LCD 屏幕文字和消息的语言。
- **机箱方向** - 基于机箱的安装方向，选择**塔模式**或**机架模式**。
- **默认 LCD 屏幕** - 选择当 LCD 面板上没有任何活动时显示的屏幕（**主菜单**、**正面状态**、**背面状态**、**侧面状态**或**自定义**）。
- **网络设置** - 选择配置 CMC 的网络设置。有关此功能的更多信息，请参阅[使用 LCD 面板界面配置 CMC 网络](#)。

使用上箭头和下箭头按钮高亮显示菜单中的某个项目，或者如果想返回**主菜单**屏幕，可高亮显示**后退**图标。要激活您的选择，请按中央按钮。

LCD 语言

LCD 语言屏幕可用于选择 LCD 面板消息所使用的语言。当前活动语言以浅蓝色背景高亮显示。

1. 使用上、下、左和右箭头按钮高亮显示所需语言。
2. 按下中央按钮。**接受**图标出现并高亮显示。
3. 按下中央按钮确认更改。此时将显示 **LCD 设置**菜单。

默认屏幕

默认屏幕可用于更改面板上无任何活动时 LCD 面板显示的屏幕。出厂默认屏幕为**主菜单**。可选择显示以下屏幕：

- **主菜单**
- **正面状态**（机箱的正面图形视图）
- **背面状态**（机箱的背面图形视图）
- **侧面状态**（机箱的左侧图形视图）
- **自定义**（带机箱名称的 Dell 徽标）

当前活动默认屏幕以浅蓝色高亮显示。

1. 使用上箭头键和下箭头键高亮显示要设置为默认状态的屏幕。
2. 按下中央按钮。此时会高亮显示**接受**图标。
3. 再次按下中央按钮确认更改。将显示**默认屏幕**。

诊断程序

LCD 面板可帮助诊断机箱中任何服务器或模块的问题。如果机箱或机箱中任何服务器或其他模块发生问题或故障，则 LCD 面板状态指示灯呈琥珀色闪烁。在**主菜单**上，具有琥珀色背景的图标会显示在菜单项（机柜）旁边，该菜单项导向前、后、侧或机柜状况。

通过跟踪 LCD 菜单系统中的琥珀色图标，可以显示状态屏幕和发生问题项目的错误消息。

通过卸下导致问题的模块或服务器或通过清除该模块或服务器的硬件日志，可以移除 LCD 面板上的错误消息。对于服务器错误，使用 iDRAC Web 界面或命令行界面清除服务器的系统事件日志 (SEL)。对于机箱错误，使用 CMC Web 界面或命令行界面清除硬件日志。

前面板 LCD 消息

本节包括前面板 LCD 上显示错误和状态信息两个小节。

LCD 上的 *错误消息* 具有与从 CLI 或 Web 界面查看的系统事件日志 (SEL) 类似的格式。

错误部分中的表格列出各种 LCD 屏幕上显示的错误和警告消息以及可能的原因。尖括号 (< >) 中的文本表示该段文本可能会不一样。

LCD 上的 *状态信息* 包括关于机箱中各模块的说明性信息。此节中的表格说明了对每个组件显示的信息。

LCD 模块与服务器状态信息

本节中的表格说明了前面板 LCD 上显示的机箱中每种类型组件的状态项目。

表. 33: CMC 状态

项目	说明
示例: CMC1、CMC2	名称/位置。
无错误	如果没有出现错误则会显示“无错误”，否则列出错误消息。
固件版本	仅在活动 CMC 上显示。对于待机 CMC 显示“待机”。
IP4 <已启用, 已禁用>	仅在活动的 CMC 上显示当前 IPv4 启用状态。
IP4 地址: <地址, 获取中>	仅在 IPv4 只于活动 CMC 上启用时显示。
IP6 <已启用, 已禁用>	在活动的 CMC 上仅显示当前 IPv6 启用状态。
IP6 本地地址: <地址>	仅在 IPv6 只于活动 CMC 上启用时显示。
IP6 全局地址: <地址>	仅在 IPv6 只于活动 CMC 上启用时显示。

表. 34: 机箱或机柜状态

项目	说明
用户定义的名称	示例: “Dell Rack System”。可通过 CMC CLI 或 Web GUI 设置。
错误消息	如果没有错误，则显示“无错误”；否则列出错误信息，先列出严重错误，再列出警告。

项目	说明
型号	示例：“PowerEdgeM1000”
功耗	当前功耗（瓦）。
峰值功耗	峰值功耗（瓦）。
最小功耗	最小功耗（瓦）。
环境温度	当前环境温度（摄氏度）。
服务标签	工厂分配的服务标签。
CMC 冗余模式	非冗余或冗余。
PSU 冗余模式	非冗余、交流冗余或直流冗余。

表. 35: 风扇状态

项目	说明
名称/位置。	例如：Fan1、Fan2 等。
错误消息	如果没有错误，则显示“无错误”；否则列出错误信息，先列出严重错误，再列出警告。
RPM	当前风扇速度 (RPM)。



表. 36: PSU 状态

项目	说明
名称/位置。	例如：PSU1、PSU2 等。
错误消息	如果没有错误，则显示“无错误”；否则列出错误信息，先列出严重错误，再列出警告。
状态	脱机、联机或待机。
最大功率	PSU 可为系统提供的最大功率。

表. 37: IOM 状态

项目	说明
名称/位置。	IOM A
错误消息	如果没有错误，则显示“无错误”；否则列出错误信息，先列出严重错误，再列出警告。
状态	关或开。
型号	IOM 型号。
结构类型	网络类型。
IP 地址	只有当 IOM 打开时才显示。对于直通类型 IOM，此值为零。
服务标签	工厂分配的服务标签。

表. 38: 服务器状态

项目	说明
示例: Server 1、Server 2 等。	名称/位置。
无错误	如果没有错误, 则显示“无错误”; 否则列出错误消息。先列出严重错误, 再列出警告。有关更多信息, 请参阅“LCD 错误消息”。
插槽名称	机箱插槽名称。例如 SLOT-01。  注: 可通过 CMC CLI 或 Web GUI 设置此表。
名称	服务器名称, 用户可通过 Dell OpenManage 进行设置。只有 iDRAC 完成引导并且服务器支持此功能时才显示该名称, 否则显示 iDRAC 引导消息。
型号	如果 iDRAC 完成引导则显示。
服务标签	如果 iDRAC 完成引导则显示。
BIOS 版本	服务器 BIOS 固件版本。
最后一个开机自检代码	显示最后一个服务器 BIOS 开机自检代码消息字符串。
iDRAC 固件版本	如果 iDRAC 完成引导则显示。  注: iDRAC 版本 1.01 显示为 1.1。不存在 iDRAC 版本 1.10。
IP4 <已启用, 已禁用>	显示当前 IPv4 启用状态。
IP4 地址: <地址, 获取中>	仅当 IPv4 启用时显示。
IP6 <已启用, 已禁用>	仅当 iDRAC 支持 IPv6 时显示。显示当前 IPv6 启用状态。
IP6 本地地址: <地址>	仅当 iDRAC 支持 IPv6 且已启用 IPv6 时显示。
IP6 全局地址: <地址>	仅当 iDRAC 支持 IPv6 且已启用 IPv6 时显示。
在结构上启用了 Flex 地址	仅当已安装该功能时显示。列出为此服务器启用的结构 (即 A、B 和 C)。

动态更新表中的信息。如果服务器不支持此功能, 则不会出现以下信息, 否则服务器管理员使用以下选项:

- 选项“无” = LCD 上没有必须显示的字符串。
- 选项“默认值” = 无效果。
- 选项“自定义” = 允许为此服务器输入字符串名称。

仅当 iDRAC 完成引导后才显示此信息。有关此功能的更多信息, 请参阅 *RACADM Command Line Reference Guide for CMC in PowerEdge VRTX* (适用于 PowerEdge VRTX 中的 CMC 的 RACADM 命令行参考指南)。

常见问题

本部分列出了关于以下方面的常见问题：

- RACADM
- 管理和恢复远程系统
- Active Directory
- FlexAddress 和 FlexAddressPlus

RACADM

在执行 CMC 重设（使用 RACADM `racreset` 子命令）后，如果输入命令，则显示以下消息：

```
racadm <subcommand> Transport: ERROR: (RC=-1)
```

这条消息什么意思？

只有在 CMC 完成重设后，才能发出另一条命令。

使用 RACADM 子命令有时会显示以下一条或多条错误：

- 本地错误消息 - 诸如语法、印刷错误和错误名称等问题。例如：ERROR: <message>

使用 RACADM `help` 子命令可显示正确的语法和用法信息。例如，如果在清除机箱日志时出现错误，可以运行以下子命令。

```
racadm chassislog help clear
```

与 CMC 相关的错误消息 - CMC 无法执行操作的问题。显示以下错误消息

```
racadm command failed.
```

要查看有关机箱的信息，请键入以下命令。

```
racadm gettracelog
```

在使用固件 RACADM 时，提示符更改为 “>”，“\$” 提示符不再显示。

如果在命令中使用不匹配的双引号 (") 或不匹配的单引号 (')，则 CLI 会更改为 “>” 提示符并将所有命令排队。

要返回到 “\$” 提示符，请键入 <Ctrl> - d。

在使用 `$ logout` 和 `$ quit` 命令时，将显示错误消息：Not Found（未找到）。

管理和恢复远程系统

访问 CMC Web 界面时，显示一个安全警告，指出 SSL 证书的主机名与显示的 CMC 的主机名不匹配。

CMC 包括一个默认的 CMC 服务器证书，以确保 Web 界面和远程 RACADM 功能的网络安全。如果使用该证书，Web 浏览器就会显示一个安全警告，因为默认证书颁发给与 CMC 的主机名（例如，IP 地址）不匹配的 CMC 默认证书。

要解决此安全问题，应上载一个颁发给 CMC IP 地址的 CMC 服务器证书。生成用于颁发证书的证书签名请求 (CSR) 时，应确保 CSR 的常用名 (CN) 与 CMC 的 IP 地址（例如，192.168.0.120）或注册的 DNS CMC 名称匹配。

要确保 CSR 与注册的 DNS CMC 名称匹配，请执行以下操作：

1. 在左侧窗格中，单击**机箱概览**。
2. 单击**网络**。
此时将显示**网络配置**页面。
3. 选中在**DNS 上注册 CMC**选项。
4. 在**DNS CMC 名称**字段中输入 CMC 名称。
5. 单击**应用更改**。

为什么在属性更改后，远程 RACADM 和基于 Web 的服务会变得不可用？

CMC Web 服务器重置后，可能需要等待一分钟，远程 RACADM 服务和 Web 界面才会可用。

CMC Web 服务器会在发生以下情况后重置：

- 使用 CMC Web 用户界面更改网络配置或网络安全属性。
- 更改 `cfgRacTuneHttpsPort` 属性（包括通过 `config -f <配置文件>` 进行更改时）。
- 使用 `racresetcfg` 或还原机箱配置备份。
- CMC 重置。
- 上载了新的 SSL 服务器证书。

我的 DNS 服务器没有注册我的 CMC？

有些 DNS 服务器最多只能注册含有 31 个字符的名称。

访问 CMC Web 界面时，显示一个安全警告，指出该 SSL 证书是由一家不可信的证书颁发机构颁发的。

CMC 包括一个默认的 CMC 服务器证书，以确保 Web 界面和远程 RACADM 功能的网络安全。该证书不是由可信证书颁发机构颁发的。要解决此安全问题，请上载一个由可信证书颁发机构（例如 Thawte 或 Verisign）颁发的 CMC 服务器证书。

为何出于未知原因显示以下消息？

Remote Access: SNMP Authentication Failure

在查找过程中，IT Assistant 会尝试验证设备的 **get** 和 **set** 团体名称。在 IT Assistant 中，**get 团体名称 = public** 而 **set 团体名称 = private**。默认情况下，CMC 代理的团体名称是 public。当 IT Assistant 发出 set 请求时，CMC 代理会生成 SNMP 验证错误，因为它只接受来自**团体 = public** 的请求。

使用 RACADM 更改 CMC 团体名称。要查看 CMC 团体名称，请使用以下命令：

```
racadm getconfig -g cfgOobSnmp
```

要设置 CMC 团体名称，请使用以下命令：

```
racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <团体名称>
```

要防止生成 SNMP 验证陷阱，请输入代理接受的团体名称。因为 CMC 只允许使用一个团体名称，所以请为 IT Assistant 发现设置输入相同的 get 和 set 团体名称。

Active Directory

Active Directory 是否支持跨多个树进行 CMC 登录？

CMC 的 Active Directory 查询算法支持单个目录林中的多个树。

使用 Active Directory 登录到 CMC 的操作是否可以在混合模式下进行（也就是说，目录林中的域控制器运行着不同的操作系统，比如 Microsoft Windows 2000 或 Windows Server 2003）？

是。在混合模式中，CMC 查询过程使用的所有对象（比如用户、RAC 设备对象和关联对象）都必须处于同一域中。

如果处于混合模式，Dell 扩展的 Active Directory 用户和计算机管理单元将检查模式并限制用户以跨多个域创建对象。

配合使用 CMC 和 Active Directory 是否支持多个域环境？

是。域目录林功能级别必须处在本机 (Native) 或 Windows 2003 模式。此外，关联对象、RAC 用户对象和 RAC 设备对象（包括关联对象）的组都必须是通用组。

这些 Dell 扩展的对象（Dell 关联对象、Dell RAC 设备和 Dell 权限对象）是否可以位于不同的域？

关联对象和权限对象必须位于相同的域。Dell 扩展的 Active Directory 用户和计算机管理单元只允许您在相同的域中创建这两个对象。其他对象可以位于不同的域。

域控制器 SSL 配置是否有任何限制？

是。目录林中用于 Active Directory 服务器的所有 SSL 证书都必须由相同的根证书颁发机构签发，因为 CMC 只允许上传一个可信证书颁发机构签发的 SSL 证书。

只有在新 RAC 证书创建并上传后，Web 界面才会启动。

如果使用 Microsoft Certificate Services 生成 RAC 证书，则在创建证书时，可能使用了“用户证书”选项而不是“Web 证书”。

要进行恢复，请生成 CSR，从 Microsoft Certificate Services 创建新的 Web 证书并通过运行以下 RACADM 命令进行上传：

```
racadm sslcsrigen [-g] [-f {filename}]
racadm sslcertupload -t 1 -f {web_sslcert}
```

FlexAddress 和 FlexAddressPlus

如果取出功能卡，会发生什么情况？

取出功能卡后没有明显变化。可以取出功能卡并保存起来，或者将其留在原位。

如果取出某个机箱中使用的功能卡，并将它放入另一个机箱中，会发生什么情况？

Web 界面显示以下错误消息：

```
This feature card was activated with a different chassis. It must be removed
before accessing the FlexAddress feature.
```

```
Current Chassis Service Tag = XXXXXXXXX
```

```
Feature Card Chassis Service Tag = YYYYYYYY
```

```
An entry is added to the CMC log that states:
```

```
cmc <date timestamp> : feature 'FlexAddress@YYYYYYYY' not activated; chassis
ID='XXXXXXXX'
```

如果卸下功能卡并安装非 FlexAddress 卡，会发生什么情况？

不应激活或修改该卡。该卡被 CMC 忽略。在这种情况下，`$racadm featurecard -s` 命令会返回以下消息：

```
No feature card inserted
```

```
ERROR: can't open file
```

如果对机箱服务标签重新编程，并且有功能卡绑定到该机箱，会发生什么情况？

- 如果该机箱或任何其他机箱的活动 CMC 中存在原始功能卡，则 Web 界面会显示以下错误消息：

```
This feature card was activated with a different chassis. It must be removed
before accessing the FlexAddress feature.
Current Chassis Service Tag = XXXXXXXXX
Feature Card Chassis Service Tag = YYYYYYYY
```

原始功能卡不再适合在该机箱或任何其他机箱上停用，除非 Dell Service 将原始机箱服务标签重新编程到机箱中，并且包含原始功能卡的 CMC 在该机箱中激活。
- FlexAddress 功能在最初绑定的机箱上仍处于激活状态。该机箱功能绑定将更新，以反映新服务标签。

将两个功能卡安装到冗余 CMC 系统时是否显示一条错误消息？

活动 CMC 中的功能卡处于活动状态，并安装在机箱中。第二张卡被 CMC 忽略。

SD 卡上是否有写保护锁？

是。将 SD 卡安装到 CMC 模块之前，需要验证写保护锁是否处于“解除锁定”位置。如果 SD 卡受写保护，就不能激活 FlexAddress 功能。在这种情况下，`$racadm feature -s` 命令会返回以下消息：

```
No features active on the chassis. ERROR: read only file system
```

如果在活动 CMC 模块中没有 SD 卡，会发生什么情况？

`$racadm featurecard -s` 命令会返回以下消息：

```
No feature card inserted.
```

如果服务器 BIOS 从版本 1.xx 更新到版本 2.xx，FlexAddress 功能会发生什么情况？

服务器模块在使用 FlexAddress 之前必须关机。服务器 BIOS 更新完成后，服务器模块会在服务器关机再开机后获得机箱分配的地址。

如果对 FlexAddress 执行停用命令时 SD 卡不在机箱中，如何恢复使用该 SD 卡？


问题在于，如果停用 FlexAddress 时 SD 卡不在 CMC 中，就不能使用该 SD 卡在另一个机箱上安装 FlexAddress。要恢复使用该卡，请将卡插回其绑定的机箱的 CMC 中，重新安装 FlexAddress，然后停用 FlexAddress。

已正确安装 SD 卡并且已安装所有固件或软件更新。FlexAddress 处于活动状态，但服务器部署屏幕为何不显示部署选项？出了什么问题？

这是浏览器高速缓存问题。请从浏览器注销并重新启动。

如果我需要使用 RACADM 命令 `racresetcfg` 重设我的机箱配置，FlexAddress 会发生什么情况？

FlexAddress 功能仍然处于激活状态，随时可以使用。默认情况下会选择所有结构和插槽。

 **注：**在运行 RACADM 命令 `racresetcfg` 之前，强烈建议关闭机箱电源。

在仅禁用 FlexAddressPlus 功能（让 FlexAddress 仍然处于激活状态）之后，为何仍然活动的 CMC 上的 `racadm setflexaddr` 命令会失败？

如果 CMC 后来变为活动，而 FlexAddressPlus 功能卡仍然留在卡插槽中，则 FlexAddressPlus 功能将被再次激活，而且插槽或结构 Flexaddress 配置更改可恢复。

IOM

在配置更改后，有时 CMC 将 IP 地址显示为 0.0.0.0。

单击刷新图标了解交换机上的 IP 地址是否正确设置。如果 IP/掩码/网关设置有误，交换机不会设置 IP 地址并在所有字段中返回 0.0.0.0。

常见错误有：

- 将带外 IP 地址设置为与带内管理 IP 地址相同或位于相同的网络。
- 输入无效的子网掩码。
- 将默认网关设置为没有直接连接到该交换机的网络地址。