Dell Chassis Management Controller Firmware 版本 3.0 用户指南

注和小心

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"表示可能会导致财产损失、人身伤害甚至死亡。**

_____

2010 年 7 月

目录

使用 CMC 目录服务

Dell Chassis Management Controller Firmware 版本 3.0 用户指南

目录服务维护一个公用数据库，在其中存储用于控制网络用户、计算机、打印机等的所有必需信息。如果您的公司使用 Microsoft Active Directory 服务软件或 LDAP 目录服务软件，您可配置 CMC 根据用户验证使用目录。

将 CMC 用于 Microsoft Active Directory

注： 在 Microsoft Windows 2000 和 Windows Server 2003 操作系统上支持使用 Active Directory 识别 CMC 用户。只有 Windows 2008 支持基于 IPv6 的 Active Directory。

Active Directory 架构扩展

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

- 仅使用 Active Directory 组对象的标准架构解决方案。
- 使用由 Dell 定义的 Active Directory 对象的扩展架构解决方案。

标准架构与扩展架构

使用 Active Directory 配置到 CMC 的权限时，必须选择扩展架构或标准架构。

使用标准架构解决方案：

- 无需架构扩展，因为标准架构只使用标准 Active Directory 对象。
- Active Directory 的配置很简单。

使用扩展架构解决方案：

- 所有权限控制对象都在 Active Directory 中。
- 使用不同权限级别配置不同 CMC 上用户访问权限可提供最大灵活性。

标准架构 Active Directory 概述

使用标准架构进行 Active Directory 集成，需要对 Active Directory 和 CMC 都进行配置。

在 Active Directory 端，标准组对象用作角色组。具有 CMC 权限的用户是该角色组的成员。

为了授予该用户对特定 CMC 卡的权限，需要在特定 CMC 卡上配置角色组名称及其域名。与扩展架构不同，角色和权限级别定义在各个 CMC 卡上，而不是 Active Directory 中。每个 CMC 中可配置和定义多达五个角色组。 表 5-41 显示了角色组的权限级别而 表 8-1 显示了默认角色组设置。

图 8-1. 使用 Active Directory 和标准架构进行 CMC 配置

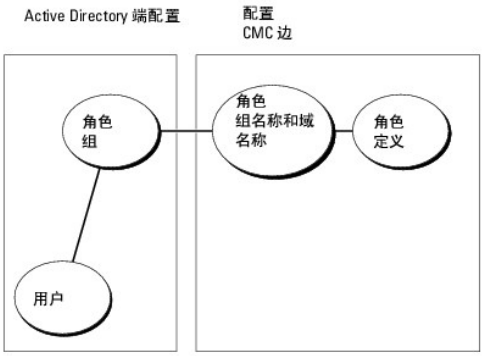


表 8-1. 默认角色组权限

角色组	默认权限级别	授予的权限	位掩码
1	无	• 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） • 高级用户 • 服务器管理员 • 检测警报用户 • 调试命令用户 • 结构 A 管理员 • 结构 B 管理员 • 结构 C 管理员	0x00000fff
2	无	• 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 • 检测警报用户 • 结构 A 管理员 • 结构 B 管理员 • 结构 C 管理员	0x000000f9
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 设置标准模式时才使用。

注： 有关用户权限的详情，请参阅 "用户类型"。

有两种方式启用标准架构 Active Directory：

- 使用 CMC Web 界面。请参阅"使用标准模式 Active Directory 和 Web 界面配置 CMC"。
- 用 RACADM CLI 工具。请参阅"使用标准模式 Active Directory 和 RACADM 配置 CMC"。

配置标准架构 Active Directory 访问 CMC

Active Directory 用户能访问 CMC 之前，需要执行以下步骤配置 Active Directory：

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. 创建组或选择现有组。必须通过 Web 界面或 RACADM 在 CMC 上配置组名和该域的名称。

   有关详细信息，请参阅"使用标准模式 Active Directory 和 Web 界面配置 CMC" 或 "使用标准模式 Active Directory 和 RACADM 配置 CMC"。

3. 添加 Active Directory 用户作为 Active Directory 组的成员以访问 CMC。

使用标准模式 Active Directory 和 Web 界面配置 CMC

1. 登录 CMC Web 界面。
2. 选择系统树中的**"Chassis"（机箱）**。
3. 单击**"User Authentication"（用户验证）**→ **"Directory Services"（目录服务）**。显示**"Directory Services"（目录服务）**页。
4. 选择 Microsoft Active Directory（标准架构）旁的单选按钮。**"Active Directory Configuration and Management"（Active Directory 配置与管理）**页会出现。
5. 在**"Common Settings"（常见设置）**部分：
   a. 选择**"Enable Active Directory"（启用 Active Directory）**复选框。
   b. 键入**"Root Domain Name"（Root 域名）**。

   注： **根域名**必须是使用 *x.y* 命名规范的有效域名，其中 *x* 是 1–256 个字符的 ASCII 字符串，字符之间不带空格，且 *y* 是有效的域类型，如 com、edu、gov、int、mil、net 或 org。

   c. 键入**超时**时间，以秒为单位。超时范围 **15–300** 秒。默认超时时间为 90 秒。
6. 如果要用定向调用搜索域控制器和全局编录，请选择**"Search AD Server to search (Optional)"（搜索 AD 服务器以搜索 [可选]）**复选框，然后执行以下操作：
   a. 在**"Domain Controller"（域控制器）**文本字段中，键入安装了 Active Directory 服务的服务器。
   b. 在**"Global Catalog"（全局编录）**文本字段中，键入全局编录在 Active Directory 域控制器上的位置。全局编录提供了搜索 Active Directory 森林的资源。
7. 单击**"Apply"（应用）**保存设置。

   注： 继续下一步前必须应用设置。如果不应用这些设置，则导航至下一页后会丢失这些输入的设置。
8. 在**"Standard Schema Settings"（标准架构设置）**部分，单击**"Role Group"（角色组）**。此时将显示**"Configure Role Group"（配置角色组）**页。
9. 键入**"Group Name"（组名称）**。组名称可标识与 CMC 卡相关联的 Active Directory 中的角色组。
10. 键入**"Group Domain"（组域）**。**"Group Domain"（组域）**是目录林的完全限定 Root 域名。
11. 在**"Role Group Privileges"（角色组权限）**页中，选择组的权限。

    如果修改任何权限，现有**"Role Group Privilege"（角色组权限）**（管理员、高级用户或客用户）会更改为自定义组或相应角色组权限。请参阅表 5-41。
12. 单击**"Apply"（应用）**保存角色组设置。
13. 单击**"Go Back To Configuration Page"（退回到配置页）**。
14. 将域目录林根认证机构签发的认证上载到 CMC。在**"Certificate Management"（证书管理）**部分键入认证的文件路径或浏览至认证文件。单击**"Upload"（上载）**按钮传输文件到 CMC。

    注： **"File Path"（文件路径）**值显示上载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 认证必须由根认证机构签名认证签名。在访问 CMC 的 management station 上必须提供根认证机构签发的认证。
15. 单击**"Apply"（应用）**。CMC Web 服务器将在单击**"Apply"（应用）**后自动重新启动。
16. 注销，然后登录 CMC 以完成 CMC Active Directory 功能配置。
17. 选择系统树中的**"Chassis"（机箱）**。
18. 单击**"Network"（网络）**选项卡。
19. 单击**"Network"（网络）**子选项卡。显示**"Network Configuration"（网络配置）**页。
20. 如果在**"Network Settings"（网络设置）**下选择了**"Use DHCP"（使用 DHCP）（用于 CMC 网络接口 IP 地址）**，则选择**"Use DHCP to obtain DNS server address"（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**"Use DHCP to obtain DNS server address"（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。

21. 单击**"Apply Changes"（应用更改）**。

    CMC 标准模式 Active Directory 功能配置完成。

使用标准模式 Active Directory 和 RACADM 配置 CMC

要使用 RACADM CLI 和标准架构 Active Directory 功能配置 CMC，可使用以下命令：

1. 打开到 CMC 的串行/远程登录/SSH 文本控制台，并键入：

   ```
   racadm config -g cfgActiveDirectory -o cfgADEnable 1

   racadm config -g cfgActiveDirectory -o cfgADType 2

   racadm config -g cfgActiveDirectory -o cfgADRootDomain <完全限定的 root 域名>

   racadm config -g cfgStandardSchema -i <索引> -o cfgSSADRoleGroupName <角色组的常用名>

   racadm config -g cfgStandardSchema -i <索引> -o cfgSSADRoleGroupDomain <完全限定域名>

   racadm config -g cfgStandardSchema -i <索引> -o cfgSSADRoleGroupPrivilege <针对特定用户权限的位掩码值>

   racadm sslcertupload -t 0x2 -f <ADS 根 CA 证书>

   racadm sslcertdownload -t 0x1 -f <RAC SSL 证书>
   ```

   注： 对于位掩码数字值，请参阅《*Dell Chassis Management Controller Administrator Reference Guide.*》的数据库属性一章中的表 3-1。

2. 使用以下选项之一指定 DNS 服务器：

   - 如果 CMC 上已启用 DHCP 并且您希望使用 DHCP 服务器自动获取的 DNS 地址，则键入以下命令：

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

   - 如果 CMC 上已禁用 DHCP，或想要手工输入 DNS IP 地址，则键入以下命令：

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

     racadm config -g cfgLanNetworking -o cfgDNSServer1 <主要 DNS IP 地址>

     racadm config -g cfgLanNetworking -o cfgDNSServer2 <次要 DNS IP 地址>
     ```

扩展架构概览

有两种方式在 Active Directory 中启用扩展架构：

- 使用 CMC Web 界面。有关说明，请参阅 "使用扩展架构 Active Directory 和 Web 界面配置 CMC"。
- 使用 RACADM CLI 工具。有关说明，请参阅 "使用扩展架构 Active Directory 和 RACADM 配置 CMC"。

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。

数据库中存储的类的一个示例就是用户类。用户类属性包括用户的名字、姓氏、电话号码等。

您可以通过添加自己独特的属性和类扩展 Active Directory 数据库以解决特定环境下的需求。Dell 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。

每个添加到现有 Active Directory 架构的属性或类都必须定义唯一的 ID。为在整个行业中保持唯一的 ID，Microsoft 维护着 Active Directory 对象标识符 (OID) 的数据库。为在 Microsoft 的 Active Directory 中扩展架构，Dell 为 Dell 特定的属性和类建立了唯一的 OID、唯一的名称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：12070–2079

RAC 架构扩展概览

Dell 提供了一组可以配置的属性。Dell 扩展架构包括关联、设备和权限属性。

关联属性可将具有一组特定权限的用户或组与一个或多个 RAC 设备链接起来。这种模式给管理员提供了极大的灵活性，可以对网络上的用户、RAC 权限和 RAC 设备进行各种组合而无需增加太多的复杂性。

Active Directory 对象概览

当要与 Active Directory 集成以进行验证和授权的网络上有两个 CMC 时，必须为其中每个 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。

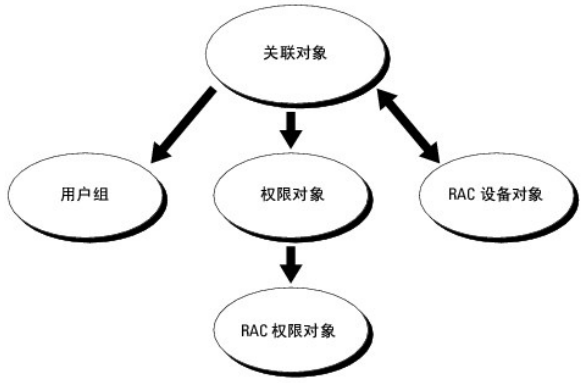
RAC 设备对象就是到 RAC 固件的链接，用于查询 Active Directory 以进行验证和授权。将 RAC 添加到网络后，管理员必须使用 Active Directory 名称配置 RAC 及其设备对象，以便用户可以使用 Active Directory 执行验证和授权。管理员还必须将 RAC 添加到至少一个"关联"对象以使用户能够验证。

图 8-2 说明关联对象提供了进行所有验证和授权所需的连接。

注： RAC 权限对象适用于 DRAC 4、DRAC 5 和 CMC。

可以根据需要创建任意数量的关联对象。然而，必须创建至少一个关联对象，对于网络上每一个想与 Active Directory 集成的 RAC (CMC) 来说，则必须有一个 RAC 设备对象。

图 8-2. Active Directory 对象的典型设置

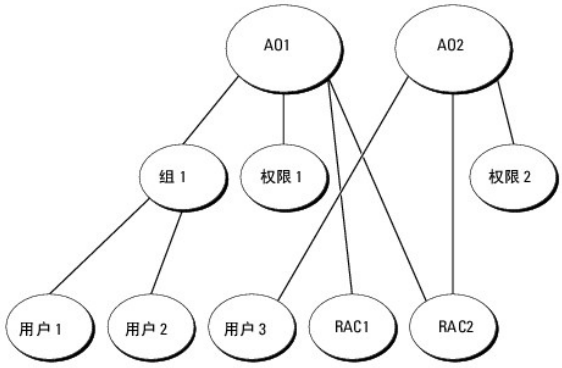


关联对象允许任意数量的用户和/或组以及 RAC 设备对象。然而，每个关联对象只有一个权限对象。"关联"对象连接那些对 RAC (CMC) 具有"权限"的"用户"。

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 Active Directory 现有用户（用户 1、用户 2 和 用户 3）。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。 图 8-3 显示了如何在此情况下设置 Active Directory 对象。

添加来自不同域的通用组时，请创建一个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，不能与来自其它域的通用组一起使用。

图 8-3. 在一个域中设置 Active Directory 对象



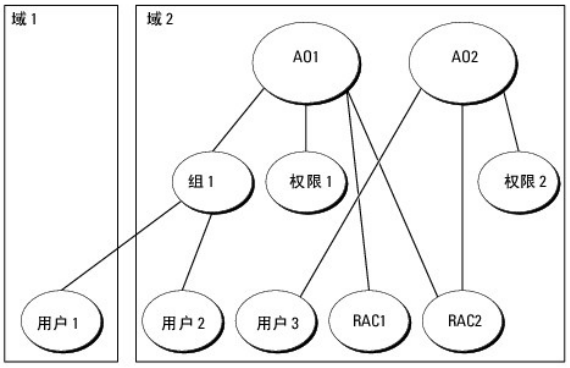
要为单域情况配置对象：

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

有关详细指导，请参阅 "将 CMC 用户和权限添加到 Active Directory"。

图 8-4 提供多个域中 Active Directory 对象的示例。在这种情况下，已有两个 CMC（RAC1 和 RAC2）和三个 Active Directory 现有用户（用户 1、用户 2 和用户 3）。用户 1 位于域 1 中，用户 2 和用户 3 位于域 2 中。在此情况下，配置用户 1 和用户 2 具有对两个 CMC 的管理员权限，配置用户 3 具有对 RAC2 卡的登录权限。

图 8-4. 在多个域中设置 Active Directory 对象



要为多域情况配置对象：

1. 确保域目录林功能处在本机或 Windows 2003 模式。
2. 在任意域中创建两个"关联"对象：A01（范围是 Universal）和 A02。

   图 8-4 显示域 2 中的对象。
3. 创建两个 RAC"设备"对象（RAC1 和 RAC2）用以代表两个 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 归到组 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 访问 CMC

使用 Active Directory 访问 CMC 之前，应配置 Active Directory 软件和 CMC：

1. 扩展 Active Directory 架构（请参阅"扩展 Active Directory 架构"）。

2. 扩展 Active Directory 用户和计算机管理单元（请参阅 "安装 Dell 对 Active Directory 用户和计算机管理单元的扩展"）。

3. 将 iDRAC 用户及其权限添加到 Active Directory（请参阅 "将 CMC 用户和权限添加到 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（请参阅 "使用扩展架构 Active Directory 和 Web 界面配置 CMC" 或 "使用扩展架构 Active Directory 和 RACADM 配置 CMC"）。

扩展 Active Directory 架构

扩展 Active Directory 架构将会在 Active Directory 架构中添加一个 Dell 组织单元、架构类和属性以及示例权限和关联对象。扩展架构前，必须在域目录林的"架构主机灵活单主机操作 (FSMO) 角色所有者"上具有架构管理权限。

可以使用以下方法之一扩展架构：

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

如果使用 LDIF 脚本，将不会把 Dell 组织单元添加到架构。

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

- **<DVD 驱动器>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\<安装类型>\LDIF Files**
- **<DVD 驱动器>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_ Tools\<安装类型>\Schema Extender**

要使用 LDIF 文件，请参阅 **LDIF_Files** 目录中自述文件中的说明。有关使用 Dell Schema Extender 扩展 Active Directory 架构的说明，请参阅 "使用 Dell Schema Extender"。

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

使用 Dell Schema Extender

Dell Schema Extender 使用 **SchemaExtenderOem.ini** 文件。要确保 Dell Schema Extender 公用程序运行正常，请勿修改该文件的名称。

1. 在**"Welcome"（欢迎）**屏幕中单击**"Next"（下一步）**。

2. 阅读并了解警告，单击**"Next"（下一步）**。

3. 选择**"Use Current Log In Credentials"（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**"Next"（下一步）**运行 Dell Schema Extender。

5. 单击**"Finish"（完成）**。

   架构将会扩展。要验证架构扩展，请使用 Microsoft 管理控制台 (MMC) 和 Active Directory 架构管理单元验证以下内容是否存在：

   - 类 — 请参阅 表 8-2 到 表 8-7
   - 属性 — 请参阅 表 8-8

请参阅 Microsoft 说明文件详细了解如何在 MMC 中启用和使用 Active Directory 架构管理单元。

表 8-2. 添加到 Active Directory 架构的类的类定义

类名称	分配的对象标识号 (OID)
dellRacDevice	1.2.840.113556.1.8000.1280.1.1.1.1
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2
dellRACPrivileges	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 8-3. dellRacDevice 类

OID	1.2.840.113556.1.8000.1280.1.1.1.1
说明	表示 Dell RAC 设备。RAC 设备必须在 Active Directory 中配置为 dellRacDevice。这种配置使 CMC 能够向 Active Directory 发送轻量级目录访问协议 (LDAP) 查询。
类的类型	结构类
超类	dellProduct
属性	**dellSchemaVersion** **dellRacType**

表 8-4. dellAssociationObject 类

OID	1.2.840.113556.1.8000.1280.1.1.1.2
说明	表示 Dell 关联对象。关联对象提供用户和设备之间的连接。
类的类型	结构类
超类	组
属性	**dellProductMembers** **dellPrivilegeMember**

表 8-5. dellRAC4Privileges 类

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

表 8-6. dellPrivileges 类

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

表 8-7. 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 8-8. 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** 后退链接的前进链接。 **链接 ID:** 12070	
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)	FALSE
属性：dellIsCardConfigAdmin **说明：**如果用户具有设备的卡配置权限，则为 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)	TRUE
属性：dellIsLoginUser **说明：**如果用户具有设备的登录权限，则为 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)	TRUE
属性：dellIsCardConfigAdmin **说明：**如果用户具有设备的卡配置权限，则为 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)	TRUE
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。	
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)	TRUE
属性：dellIsLogClearAdmin **说明：**如果用户具有设备的清除日志管理员权限，则为 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)	TRUE
属性：dellIsServerResetUser **说明：**如果用户具有设备的服务器重设权限，则为 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)	TRUE
属性：dellIsTestAlertUser **说明：**如果用户具有设备的检测警报用户权限，则为 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)	TRUE
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。	
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)	TRUE
属性：dellSchemaVersion **说明：**当前架构版本用于更新架构。	
OID：1.2.840.113556.1.8000.1280.1.1.2.12 大小写忽略字符串 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
属性：dellRacType **说明：**此属性是 dellRacDevice 对象的当前 Rac 类型和到 dellAssociationObjectMembers 前进链接的后退链接。	
OID：1.2.840.113556.1.8000.1280.1.1.2.13 大小写忽略字符串 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
属性：dellAssociationMembers **说明：**属于此产品的 dellAssociationObjectMembers 的列表。此属性是到 dellProductMembers 链接属性的后退链接。 链接 ID：12071	
OID：1.2.840.113556.1.8000.1280.1.1.2.14 可分辨名称 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
属性：dellPermissionsMask1	
OID：1.2.840.113556.1.8000.1280.1.6.2.1 整数 (LDAPTYPE_INTEGER)	
属性：dellPermissionsMask2	
OID：1.2.840.113556.1.8000.1280.1.6.2.2 整数 (LDAPTYPE_INTEGER)	

安装 Dell 对 Active Directory 用户和计算机管理单元的扩展

扩展 Active Directory 中的模式时，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，可以通过在安装过程中选择**"Dell Extension to the Active Directory User's and Computers Snap-In"（到 Active Directory 用户和计算机管理单元的 Dell 扩展）**选项来扩展管理单元。请参阅*《Dell OpenManage Software Quick Installation Guide》*进一步了解如何安装系统管理软件。

有关 Active Directory 用户和计算机管理单元的详情，请参阅 Microsoft 说明文件。

安装 Administrator Pack

必须在管理 Active Directory CMC 对象的每个系统上安装 Administrator Pack。如果不安装 Administrator Pack，将无法在容器中查看 Dell RAC 对象。

打开 Active Directory 用户和计算机管理单元

要打开 Active Directory 用户和计算机管理单元：

1. 如果登录到域控制器，则单击**"Start"（开始）→"Admin Tools"（管理工具）→"Active Directory Users and Computers"（Active Directory 用户和计算机）**。

   如果没有登录到域控制器上，则必须在本地系统上安装相应的 Microsoft Administrator Pack。要安装此 Administrator Pack，单击**"Start"（开始）→ "Run"（运行）**，键入 `MMC` 并按 <Enter>。

   Microsoft 管理控制台 (MMC) 显示。

2. 在**"Console 1"（控制台 1）**窗口中，单击**"File"（文件）**（如果是运行 Windows 2000 的系统，则单击**"Console"（控制台）**）。

3. 单击**"Add/Remove Snap-in"（添加/删除管理单元）**。

4. 选择**"Active Directory Users and Computers"（Active Directory 用户和计算机）**管理单元并单击**"Add"（添加）**。

5. 单击**"Close"（关闭）**并单击**"OK"（确定）**。

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，使您能够通过创建 RAC、关联和权限对象添加 CMC 用户和权限。要添加各种对象类型，请：

1. 创建 RAC 设备对象。
2. 创建权限对象。
3. 创建关联对象。
4. 将对象添加到关联对象。

创建 RAC 设备对象

1. 在 MMC 的**"Console Root"（控制台根目录）**窗口中，右键单击一个容器。
2. 选择**"New"（新建）**→ **"Dell RAC Object"（Dell RAC 对象）**。

   系统将显示**"New Object"（新建对象）**窗口。
3. 为新对象键入名称。该名称必须与准备在 "使用扩展架构 Active Directory 和 Web 界面配置 CMC" 步骤 8a 中键入的 CMC 名称相同。
4. 选择**"RAC Device Object"（RAC 设备对象）**。
5. 单击**"OK"（确定）**。

创建权限对象

注： 权限对象必须和相关关联对象创建在同一个域中。

1. 在**"Console Root"（控制台根目录）**(MMC) 窗口中，右键单击一个容器。
2. 选择**"New"（新建）**→ **"Dell RAC Object"（Dell RAC 对象）**。

   系统将显示**"New Object"（新建对象）**窗口。
3. 为新对象键入名称。
4. 选择**"Privilege Object"（权限对象）**。
5. 单击**"OK"（确定）**。
6. 右键单击创建的权限对象并选择**"Properties"（属性）**。
7. 单击**"RAC Privileges"（RAC 权限）**选项卡并选择要让用户拥有的权限。有关 CMC 用户权限的详情，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。关联范围为关联对象指定安全组类型。创建关联对象时，请选择适用于要添加对象的类型的关联范围。

例如，如果选择**"Universal"（通用）**，则关联对象仅当 Active Directory 域以本机模式或更高模式运行时才可用。

1. 在**"Console Root"（控制台根目录）**(MMC) 窗口中，右键单击一个容器。
2. 选择**"New"（新建）**→ **"Dell RAC Object"（Dell RAC 对象）**。

   这将打开**"New Object"（新建对象）**窗口。
3. 为新对象键入名称。
4. 选择**"Association Object"（关联对象）**。

5. 选择**"Association Object"（关联对象）**的范围。

6. 单击**"OK"（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 模式或更高模式，请使用通用组以跨越用户或 RAC 对象的域。

可以添加用户组和 RAC 设备组。创建 Dell 相关的组和非 Dell 相关的组的过程相同。

添加用户或用户组

1. 右键单击**"Association Object"（关联对象）**并选择**"Properties"（属性）**。

2. 选择**"Users"（用户）**选项卡并单击**"Add"（添加）**。

3. 键入用户或用户组名称并单击**"OK"（确定）**。

单击**"Privilege Object"（权限对象）**选项卡将权限对象添加到验证 RAC 设备时定义用户或用户组权限的关联。只能将一个权限对象添加到关联对象。

添加权限

1. 选择**"Privileges Object"（权限对象）**选项卡并单击**"Add"（添加）**。

2. 键入权限对象名称并单击**"OK"（确定）**。

单击**"Products"（产品）**选项卡将一个或多个 RAC 设备添加到关联。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。

添加 RAC 设备或 RAC 设备组

要添加 RAC 设备或 RAC 设备组：

1. 选择**"Products"（产品）**选项卡并单击**"Add"（添加）**。

2. 键入 RAC 设备或 RAC 设备组名称并单击**"OK"（确定）**。

3. 在**"Properties"（属性）**窗口中，单击**"Apply"（应用）**，并单击**"OK"（确定）**。

使用扩展架构 Active Directory 和 Web 界面配置 CMC

1. 登录 CMC Web 界面。

2. 选择系统树中的**"Chassis"（机箱）**。

3. 单击**"User Authentication"（用户验证）→ "Directory Services"（目录服务）**。

   随即显示**"Directory Services"（目录服务）**页面。

4. 选择 **Microsoft Active Directory（扩展架构）**。

5. 在**"Common Settings"（常见设置）**部分：

   a. 确认选中**"Enable Active Directory"（启用 Active Directory）**复选框。

   b. 键入**"Root Domain Name"（Root 域名）**。

注： **根域名**必须是使用 *x.y* 命名惯例的有效域名，其中，*x* 是一个 1–256 个字符的 ASCII 字符串，字符之间不含空格，*y* 是一种有效类型的域，例如 com、edu、gov、int、mil、net 或 org。

c. 键入**超时**时间，以秒为单位。**配置范围：** 15–300 秒。**默认：**90 秒

6. **可选项：**如果要用定向调用搜索域控制器和全局编录，请选择**"Search AD Server to search (Optional)"（搜索 AD 服务器以搜索 [可选]）**复选框，然后：

   a. 在**"Domain Controller"（域控制器）**文本字段中，键入安装了 Active Directory 服务的服务器。

   b. 在**"Global Catalog"（全局编录）**文本字段中，键入全局编录在 Active Directory 域控制器上的位置。全局编录提供了搜索 Active Directory 森林的资源。

   注： 将 IP 地址设置为 0.0.0.0 时，将禁止 CMC 搜索服务器。

   注： 可以指定一列域控制器或全局编录服务器，并用逗号分隔。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。

7. 在**"Extended Schema Settings"（扩展架构设置）**部分：

   a. 键入**"CMC Device Name"（CMC 设备名称）**。**CMC 名称**对 Active Directory 中的 CMC 卡进行唯一识别。**CMC 名称**必须与在域控制器中创建的新的 CMC 对象的常用名称相同。**CMC 名称**必须是 1–256 个字符的 ASCII 字符串，字符之间没有空格。

   b. 键入**"CMC Domain Name"（CMC 域名）**（例如：cmc.com）。**CMC 域名**是 Active Directory CMC 对象所在域的 DNS 名称（字符串）。名称必须是由 *x*.y 组成的有效域名，其中 *x* 是 1-256 个字符的 ASCII 字符串，字符之间没有空格，而 *y* 是有效域类型，如 com、edu、gov、int、mil、net 或 org。

8. 单击**"Apply"（应用）**保存设置。

   注： 在继续下一步，导航至另一页之前，必须先应用这些设置。如果不应用这些设置，则导航至下一页时会丢失这些输入的设置。

9. 在**"Manage Certificates"（管理证书）**部分于文本字段中输入证书的文件路径或单击**"Browse"（浏览）**选择证书文件。单击**"Upload"（上载）**按钮传输文件到 CMC。

   注： **"File Path"（文件路径）**值显示上载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。

   默认情况下要求 SSL 证书验证。**cfgActiveDirectory** RACADM 组中和 GUI 内有新设置，可禁用证书检查。

但禁用证书检查风险很高。

若要打开 SSL 证书验证（默认）：

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

若要关闭 SSL 证书验证：

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
```

域控制器 SSL 认证必须由根认证机构签名。在访问 CMC 的 management station 上必须提供根认证机构签发的认证。

10. 单击**"Apply"（应用）**。CMC Web 服务器将在您单击**"Apply"（应用）**后自动重新启动。

11. 登录到 CMC Web 界面。

12. 从系统树中选择**"Chassis"（机箱）**，单击**"Network"（网络）**选项卡，然后单击**"Network"（网络）**子选项卡。随即显示**"Network Configuration"（网络配置）**页面。

13. 如果启用（选中）**"Use DHCP (for CMC Network Interface IP Address)"（使用 DHCP [针对 CMC 网络接口 IP 地址]）**，请进行以下操作之一：

    - 选择**"Use DHCP to Obtain DNS Server Addresses"（使用 DHCP 获取 DNS 服务器地址）**使 DHCP 服务器自动获取 DNS 服务器地址，或
    - 不选中**"Use DHCP to Obtain DNS Server Addresses"（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。

14. 单击**"Apply Changes"（应用更改）**。

CMC 扩展模式 Active Directory 功能配置完成。

使用扩展架构 Active Directory 和 RACADM 配置 CMC

使用以下命令以通过 RACADM CLI 工具而不是 Web 界面配置 CMC Active Directory 的扩展架构。

1. 打开到 CMC 的串行/远程登录/SSH 文本控制台，登录并键入：

   ```
   racadm config -g cfgActiveDirectory -o cfgADEnable 1
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgADType 1
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgADRacDomain <完全限定的 CMC 域名>
   ```

```
racadm config -g cfgActiveDirectory -o cfgADRootDomain <完全限定的 root 域名>

racadm config -g cfgActiveDirectory -o cfgADRacName <CMC 常用名>

racadm sslcertupload -t 0x2 -f <ADS 根 CA 认证 -r

racadm sslcertdownload -t 0x1 -f <CMC SSL 认证>
```

注： 只能通过远程 RACADM 使用此命令。有关远程 RACADM 的详细信息，请参阅 "远程访问 RACADM"。

可选项：如果想指定 LDAP 或全局编录服务器，而不是使用由 DNS 服务器返回的服务器来搜索用户名，则键入以下命令启用**"Specify Server"（指定服务器）**选项：

```
racadm config -g cfgActiveDirectory -o cfgADSpecifyServerEnable 1
```

注： 当使用**"Specify Server"（指定服务器）**选项时，认证机构签名认证中的主机名与指定服务器的名称不匹配。如果您是 CMC 管理员，这样尤为有用，因为可以让您输入主机名和 IP 地址。

启用**"Specify Server"（指定服务器）**选项后，可使用服务器的 IP 地址或完全限定的域名 (FQDN) 指定 LDAP 服务器和全局编录。FQDN 包含服务器的主机名和域名。

要指定 LDAP 服务器，键入：

```
racadm config -g cfgActiveDirectory -o cfgADDomainController <AD 域控制器 IP 地址>
```

要指定全局编目服务器，键入：

```
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog <AD 全局编录 IP 地址>
```

注： 将 IP 地址设置为 0.0.0.0 时，将禁止 CMC 搜索服务器。

注： 可以用逗号分隔来指定一列 LDAP 或全局编目服务器。CMC 允许指定多达三个 IP 地址或主机名。

注： 所有域和应用程序的一个或多个 LDAP 未正确配置可能导致现有应用程序/域运作时，产生无法预料的结果。

2. 使用以下选项之一指定 DNS 服务器：

   - 如果 CMC 上已启用 DHCP 并且您希望使用 DHCP 服务器自动获取的 DNS 地址，则键入以下命令：

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

   - 如果 CMC 上已禁用 DHCP，或如果已启用 DHCP 但想要手工指定 DNS IP 地址，则键入以下命令：

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

     racadm config -g cfgLanNetworking -o cfgDNSServer1 <主要 DNS IP 地址>

     racadm config -g cfgLanNetworking -o cfgDNSServer2 <次要 DNS IP 地址>
     ```

扩展架构功能配置完成。

常见问题

表 8-9. 将 CMC 用于 Active Directory：常见问题

问题	解答
我能否使用 Active Directory 跨越多个树登录 CMC？	是。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会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强制您在相同的域中创建这两个对象。其它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 认证都必须由相同的根认证机构签发的认证签名，因为 CMC 只允许上载一个可信认证机构签发的 SSL 认证。
我创建并上载了一个新 RAC 证书，然而现在 Web 界面不启动。	如果使用 Microsoft Certificate Services 生成 RAC 认证，则您可能在创建认证时不小心选择了**"User Certificate"（用户认证）**，而不是**"Web Certificate"（Web 认证）**。 要进行恢复，请生成 CSR，然后从 Microsoft Certificate Services 创建新的 Web 证书并使用以下 RACADM 命令进行上载：

	racadm sslcsrgen [-g] [-f {filename (文件名称)}] racadm sslcertupload -t 1 -f {web_sslcert}
如果不能使用 Active Directory 验证方法登录到 CMC，应该怎么办？我如何排除这个问题？	1. 确保在登录期间使用正确的用户域名，而不是 NetBIOS 名称。 2. 如果具有本地 CMC 用户帐户，请使用本地凭据登录 CMC。 登录后，执行以下步骤： a. 确保已选中 CMC Active Directory 配置页上的**"Enable Active Directory"（启用 Active Directory）**复选框。 b. 确保 CMC 联网配置页上的 DNS 设置正确。 c. 确保已从 Active Directory 根认证机构签发的认证将 Active Directory 认证上载到 CMC。 d. 检查域控制器 SSL 证书以确保没有过期。 e. 确保 **CMC 名称**、**Root 域名**和 **CMC 域名**与 Active Directory 环境配置匹配。 f. 确保 CMC 密码最多有 127 个字符。虽然 CMC 可以支持多达 256 个字符的密码，但 Active Directory 只支持最大长度为 127 个字符的密码。

配置单一登录

Microsoft Windows 2000、Windows XP、Windows Server 2003、Windows Vista 和 Windows Server 2008 可以使用网络验证协议 Kerberos 作为验证方法，使已经登录到域的用户可以自动或单一登录到 Exchange 等随后的应用程序。

从 CMC 版本 2.10 开始，CMC 可以使用 Kerberos 支持其它两种类型的登录机制 — 单一登录和 Smart Card 登录。对于单一登录，CMC 使用客户端系统的证书，您使用有效的 Active Directory 帐户登录之后操作系统就会高速缓存这些凭据。

注： 选择登录方法不会设置与诸如 SSH 等其它登录界面相关的策略属性。您还必须设置其它登录界面的其它策略属性。如果您要禁用所有其它登录界面，请导航至**"Services"（服务）**页并禁用所有（或某些）登录界面。

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

- 对于仅通过 Smart Card 登录，客户端系统必须有 Microsoft Visual C++ 2005 Redistributable。有关详情，请参阅 **www.microsoft.com/downloads/details.aspx?FamilyID=32BC1BEEA3F9-4C13-9C99-220B62A191EE&displaylang=en**
- 对于单一登录和 Smart Card 登录，客户端系统必须是 Active Directory 域和 Kerberos 领域的一部分。

CMC

- CMC 必须有固件版本 2.10 或更高版本
- 每个 CMC 都必须有 Active Directory 帐户
- CMC 必须是 Active Directory 域和 Kerberos Realm 的一部分

配置设置

前提条件

- 已经设置了 Active Directory (AD) 的 Kerberos 领域和 Key Distribution Center (KDC) (ksetup)
- 强健的 NTP 和 DNS 基础设施以避免时钟漂移和反向查询出现问题
- 具有授权成员的 CMC 标准模式角色组

配置 Active Directory

在**"CMC Properties"（CMC 属性）**对话框的**"Accounts"（帐户）**选项部分下面，配置以下设置：

- **"Account is trusted for delegation"（帐户可以委派其它帐户）**— 在选择此选项时，当前 CMC 不使用创建的已转发凭据。能否选择此选项视其它服务要求而定。
- **"Account is sensitive and cannot be delegated"（敏感帐户，不能被委派）**— 能否选择此选项视其它服务要求而定。
- **"User Kerberos DES encryption types for the account"（帐户的用户 Kerberos DES 加密类型）**— 选择此选项。
- **"Do not require Kerberos preauthentication"（不要求 Kerberos 预验证）**— 不选择此选项。

在用来将 CMC 映射到 Active Directory 中的用户帐户的域控制器上，运行 ktpass 公用程序（Microsoft Windows 的一部分）。例如：

```
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 名称 @REALM_NAME 必须大写。此外，CMC 支持 Kerberos 验证的 DES-CBC-MD5 类型的加密。

此过程会生成一个 Keytab 文件，必须将该文件上载到 CMC。

注： Keytab 包含加密密钥，因此必须保管好。有关 ktpass 公用程序的详情，请参阅 Microsoft 网站：**technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true**。

配置 CMC

注： 本节中介绍的配置步骤仅适用于 CMC 的 Web 访问。

将 CMC 配置为使用在 Active Directory 中设置的标准模式角色组。有关详情，请参阅"配置标准架构 Active Directory 访问 CMC"。

上载 Kerberos 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。

要上载 Keytab 文件：

1. 导航至**"User Authentication"（用户验证）**选项卡→ **"Directory Services"（目录服务）**子选项卡。确保选择 **Microsoft Active Directory 标准**或**扩展架构**。否则选择首选项并单击**"Apply"（应用）**。
2. 单击**"Kerberos Keytab Upload"（Kerberos Keytab 上载）**部分中的**"Browse"（浏览）**，导航至保存 Keytab 文件的文件夹并单击**"Upload"（上载）**。

   上载完成后，将显示一个信息框，说明上载成功或失败。

启用单一登录

1. 单击**"Chassis Management Controller Network Security"（机箱管理控制器网络安全）**选项卡→ **Active Directory**→ **"Configure Active Directory"（配置 Active Directory）**。

   随即显示**"Active Directory Configuration and Management"（Active Directory 配置与管理）**页。
2. 在**"Active Directory Configuration and Management"（Active Directory 配置和管理）**页上，选择：
   - "Single Sign-On"（单一登录）— 此选项使您能够使用登录 Active Directory 时获得的高速缓存的凭据登录 CMC。

   注： 对于此选项，所有命令行带外接口，包括 Secure Shell (SSH)、远程登录、串行和远程 RACADM 都保持不变。
3. 滚动到页面底部，然后单击**"Apply"（应用）**。

您可以使用 CLI 命令 test feature 检测使用 Kerberos 验证的 Active Directory。

键入：

`testfeature -f adkrb -u <用户>@<域>`

其中用户是有效的 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，则解决错误并重复该命令。有关详情，请参阅 **support.dell.com/manuals** 上的《*Chassis Management Controller Administrator Reference Guide*》。

配置浏览器以使用单一登录

Internet Explorer 版本 6.0 和更高版本及 Firefox 版本 3.0 和更高版本支持单一登录。

注： 仅当 CMC 结合使用单一登录和 Kerberos 验证时，以下说明才适用。

Internet Explorer

1. 在 Internet Explorer 中，选择**"Tools"（工具）→"Internet Options"（Internet 选项）**。
2. 在**"Security"（安全）**选项卡的**"Select a zone to view or change security settings"（选择要查看或更改安全设置的区域）**下面，选择**"Local Intranet"（本地 Intranet）**。
3. 单击**"Sites"（站点）**。

   此时将显示**"Local Intranet"（本地 Intranet）**对话框。
4. 单击**"Advanced"（高级）**。

   此时将显示**"Local Intranet Advance Settings"（本地 Intranet 高级设置）**对话框。
5. 在**"Add this site to the zone"（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**"Add"（添加）**。

   注： 您可以使用通配符 (*) 指定该域中的所有设备/用户。

Mozilla Firefox

1. 在 Firefox 中的"Address"（地址）栏中键入 **about:config**。

   注： 如果浏览器显示**"This might void your warranty"（这样可能会失去质保）**警告，单击**"I'll be careful. I promise"（我保证会小心）**。
2. 在**"Filter"（过滤器）**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**"Enter string value"（输入字符串的值）**对话框中，键入 CMC 的域名并单击**"OK"（确定）**。

使用单一登录来登录到 CMC

注： 您不能使用 IP 地址进行单一登录或 Smart Card 登录。Kerberos 根据完全限定域名 (FQDN) 验证凭据。

1. 使用网络帐户登录客户端系统。
2. 使用以下方式访问 CMC Web 页面

   https://<*CMC 名称.域名*>

   例如，`cmc-6G2WXF1.cmcad.lab`

   其中，`cmc-6G2WXF1` 是 CMC 名称

   `cmcad.lab` 是域名。

注： 如果您更改了默认 HTTPS 端口号（端口 80），则使用 ***<CMC 名称.域名>:<端口号>*** 访问 CMC Web 页面，其中 ***CMC 名称***是 CMC 的 CMC 主机名，***域名***是域名，***端口号***是 HTTPS 端口号。

将显示CMC**"Single Sign-On"（单一登录）**页。

3. 单击**"Login"（登录）**。

   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，浏览器将重定向至正常的 CMC 登录页。

   注： 如果您没有登录到 Active Directory 域，而且使用的是除 Internet Explorer 以外的浏览器，则登录将失败，而且浏览器仅显示空白页。

配置 Smart Card 双重验证

传统的验证模式使用用户名和密码来验证用户。而双重验证则提供了更高的安全性，要求用户具有密码或 PIN 以及含有私人密钥和数字证书的实物卡。Kerberos 是一种使用此双重验证机制的网络验证协议，使系统可以证明其真实性。Microsoft Windows 2000、Windows XP、Windows Server 2003、Windows Vista 和 Windows Server 2008 将 Kerberos 用作首选的验证方法。从 CMC 版本 2.10 开始，CMC 可以使用 Kerberos 支持 Smart Card 登录。

注： 选择登录方法不会设置与诸如 SSH 等其它登录界面相关的策略属性。您还必须设置其它登录界面的其它策略属性。如果您要禁用所有其它登录界面，请导航至**"Services"（服务）**页并禁用所有（或某些）登录界面。

系统要求

Smart Card 的 "系统要求" 与单一登录相同。

配置设置

Smart Card 的 "前提条件" 与单一登录相同。

配置 Active Directory

1. 如果 Active Directory 的 Kerberos 领域和 Key Distribution Center (KDC) 尚未配置，则进行设置 (ksetup)。

   注： 确保具有强健的 NTP 和 DNS 基础设施，以避免时钟漂移和反向查询出现问题。

2. 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。

3. 使用 Ktpass 在 Key Distribution Center 注册 CMC 用户（这也会将一个密钥上载到 CMC）。

配置 CMC

注： 本节中介绍的配置步骤仅适用于 CMC 的 Web 访问。

将 CMC 配置为使用在 Active Directory 中设置的标准模式角色组。有关详情，请参阅"配置标准架构 Active Directory 访问 CMC"。

上载 Kerberos 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。

要上载 Keytab 文件：

1. 导航至**"User Authentication"（用户验证）**选项卡→ **"Directory Services"（目录服务）**子选项卡。确保选择 **Microsoft Active Directory 标准**或**扩展架构**。否则选择首选项并单击**"Apply"（应用）**。

2. 单击**"Kerberos Keytab Upload"（Kerberos Keytab 上载）**部分中的**"Browse"（浏览）**，导航至保存 Keytab 文件的文件夹并单击**"Upload"**（上载）。

   上载完成后，将显示一个信息框，说明上载成功或失败。

启用 Smart Card 验证

1. 导航至**"User Authentication"（用户验证）**选项卡→ **"Directory Services"（目录服务）**子选项卡。确保选择 **Microsoft Active Directory 标准**或**扩展架构**。
2. 在**"Common Settings"（常见设置）**部分中选择：
   - Smart Card — 此选项要求将 Smart Card 插入阅读器并输入 PIN 码。

   注： 对于此选项，所有命令行带外接口，包括 Secure Shell (SSH)、远程登录、串行和远程 RACADM 都保持不变。
3. 滚动到页面底部，然后单击**"Apply"（应用）**。

您可以使用 CLI 命令 testfeature 检测使用 Kerberos 验证的 Active Directory。

键入：

`testfeature -f adkrb -u <用户>@<域>`

其中用户是有效的 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，则解决错误并重复该命令。有关详情，请参阅 RACADM 命令 testfeature 文档。

配置浏览器以使用 Smart Card 登录

Mozilla Firefox

CMC 2.10 不支持通过 Firefox 浏览器进行 Smart Card 登录。

Internet Explorer

确保 Internet 浏览器配置为下载 Active-X 插件。

使用 Smart Card 登录 CMC

注： 您不能使用 IP 地址进行单一登录或 Smart Card 登录。Kerberos 根据完全限定域名 (FQDN) 验证凭据。

1. 使用网络帐户登录客户端系统。
2. 使用以下方式访问 CMC Web 页面。

   https:// *<CMC 名称.域名>*

   例如，cmc-6G2WXF1.cmcad.lab

   其中，cmc-6G2WXF1 是 CMC 名称

   cmcad.lab 是域名。

   注： 如果您更改默认 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 CMC 主机名，***domain-name*** 是域名，***port number*** 是 HTTPS 端口号。

   将显示 **CMC "Single Sign-On"（单一登录）**页，提示插入 Smart Card。
3. 将 Smart Card 插入阅读器并单击**"OK"（确定）**。

   将显示 **PIN 弹出**对话框。
4. 另外，可选择会话超时。这是登录后可保持无活动状态的时间。默认值为 Web 服务会话空闲超时。有关详情，请参阅"配置服务"。
5. 输入 PIN，并单击**"OK"（确定）**。

Smart Card 登录故障排除

以下提示可帮助您调试无法访问的 Smart Card：

ActiveX 插件无法检测到 Smart Card 阅读器

确保 Microsoft Windows 操作系统支持 Smart Card。Windows 支持有限的几种智能卡加密服务提供程序 (CSP)。

提示：在常规检查过程中，要查看 Smart Card CSP 是否位于特定客户端上，在出现 Windows 登录 (Ctrl-Alt-Del) 屏幕时将 Smart Card 插入阅读器并检查 Windows 是否检测到 Smart Card 并显示 PIN 对话框。

不正确的智能卡 PIN

检查智能卡是否因为用不正确的 PIN 尝试太多次而已锁定。在这种情况下，组织中的智能卡颁发者应能够帮助获得新的智能卡。

无法以 Active Directory 用户的身份登录 CMC

如果无法以 Active Directory 用户的身份登录 CMC，则尝试在不启用 Smart Card 登录的情况下登录 CMC。还可以选择用以下命令通过本地 RACADM 禁用 Smart Card 登录：

racadm config -g cfgActiveDirectory -o cfgADSCLEnable 0

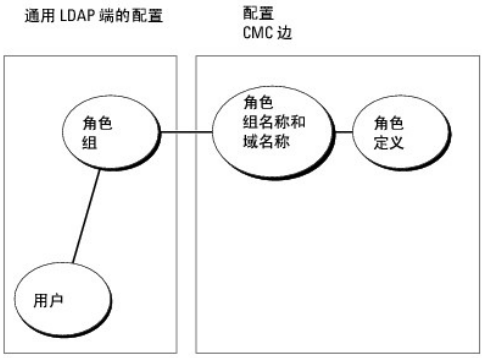
racadm config -g cfgActiveDirectory -o cfgADSSOEnable 0

使用 CMC 及通用 LDAP

CMC 管理员现在可集成 LDAP 服务器用户登录和 CMC。此集成要求在 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 权限的用户将是该角色组的成员。权限仍储存于 CMC 上用于授权，类似于 Active Directory 支持下标准架构的工作方式。

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。 表 5-41 显示了角色组的权限级别而 表 8-1 显示了默认角色组设置。

图 8-5. 配置 CMC 及通用 LDAP



配置通用 LDAP 目录访问 CMC

CMC 的通用 LDAP 实施在授予用户访问权限时分两阶段。第 1 阶段从用户验证开始，而第 2 阶段则为用户授权。

LDAP 用户的验证和授权

有些域服务器要求在特定 LDAP 服务器上进行搜索前完成绑定。验证的步骤为：

1. 可选绑定到目录服务。默认为匿名绑定。
2. 根据用户登录搜索用户。默认属性为 **uid**。
3. 如果找到一个以上的对象，则返回错误。
4. 解除绑定并以用户的 DN 和密码进行绑定。

5. 如果绑定失败，则登录失败。

如果这些步骤成功完成，则用户通过验证。下一阶段是授权。CMC 最多储存 5 个组及其相应的权限。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。

授权步骤为：

1. 在各配置的组中于**成员**或**唯一成员**属性中搜索用户的 DN。管理员可配置此字段。

2. 对于用户作为其成员的每个组累加其权限。

使用 CMC 基于 Web 的界面配置通用 LDAP 目录服务

您可使用通用轻型目录访问协议 (LDAP) 服务配置软件提供到 CMC 的访问。LDAP 允许您添加和控制现有用户的 CMC 用户权限。

注： 要为 CMC 配置 LDAP 设置，必须具备**机箱配置管理员**权限。

有关 LDAP 配置和配置通用 LDAP 的详情，请参阅 "使用 CMC 及通用 LDAP"。

若要查看和配置 LDAP，请执行以下步骤：

1. 登录到 Web 界面。

2. 单击**"User Authentication"（用户验证）**选项卡，然后单击**"Directory Services"（目录服务）**子选项卡。随即出现**"Directory Services"（目录服务）**页。

3. 单击通用 LDAP 的单选按钮。

4. 配置显示的选项并单击**"Apply"（应用）**。

可用配置选项如下：

表 8-10. 常见设置

设置	说明
启用通用 LDAP	在 CMC 上启用通用 LDAP 服务。
用可分辨名称搜索组成员资格	指定允许其成员访问设备的 LDAP 组的可分辨名称 (DN)。
启用 SSL 证书验证	如果选择，CMC 使用 CA 证书验证 SSL 握手期间的 LDAP 服务器证书
绑定 DN	在搜索登录用户的 DN 时，指定绑定到服务器的用户的可分辨名称。如果未提供，则使用匿名绑定。
密码	与绑定 DN 一起使用的绑定密码。 绑定密码属于敏感数据，应予以正确保护。
用于搜索的基础 DN	目录分支的域名，所有搜索都从此处开始。
用户登录的属性	指定要搜索的属性。如果未配置，默认使用 uid。推荐在选择的基础 DN 内唯一，否则必须配置搜索筛选器以保证登录用户的唯一性。如果用户 DN 不能通过搜索属性和搜索筛选器组合而唯一识别，则登录失败并报错。
组成员资格属性	指定用于检查组成员资格的 LDAP 属性。必须是一个组类属性。如果未指定，则使用成员和唯一成员属性。
搜索筛选器	指定有效的 LDAP 搜索筛选器。如果用户属性不能在所选基础 DN 中唯一标识登录用户，将使用此功能。如果未指定，默认为 objectClass=*，显示搜索树中的所有对象。此属性的最大长度为 1024 个字符。
网络超时（秒）	设置空闲的 LDAP 会话在等待多少秒后自动关闭。
搜索超时（秒）	设置搜索在等待多少秒后自动关闭。

选择 LDAP 服务器

用通用 LDAP 配置服务器有两种方式。静态服务器允许管理员在字段内加入 FQDN 或 IP 地址。另外，也可通过在 DNS 内查询其 SRV 记录而读取 LDAP 服务器列表。

以下是 LDAP 服务器部分中的属性：

- Use Static LDAP Servers（使用静态 LDAP 服务器） - 选择此选项可让 LDAP 服务使用提供端口号的指定服务器（详情见下）。

  注： 必须选择静态或 DNS。

- LDAP Server Address（LDAP 服务器地址） - 指定 LDAP 服务器的 FQDN 或 IP 地址。要指定位于相同域的多个冗余 LDAP 服务器，请提供所有服务器的列表（用逗号隔开）。CMC 会尝试依次连接到每个服务器，直到建立连接为止。

- LDAP Server Port（LDAP 服务器端口） - LDAP 在 SSL 上的端口，如未配置，则默认为 636。CMC 版本 3.0 不支持非 SSL 端口，因没有 SSL 就不能传输密码。
- Use DNS to find LDAP Servers（用 DNS 查找 LDAP 服务器） - 选择此选项可让 LDAP 通过 DNS 使用搜索域和服务名称。必须选择静态或 DNS。

会为 SRV 记录进行以下 DNS 查询：

_<服务名称>._tcp.<搜索域>

其中 <*搜索域*> 是查询中使用的根域而 <*服务名称*> 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。

管理 LDAP 组设置

"组设置"部分表中列出了角色组，为已配置的所有角色组显示相关名称、域和权限。

- 若要配置新角色组，则单击没有列出名称、域和权限的角色组名称。
- 若要为现有角色组更改设置，则单击角色组名称。

在单击角色组名称时，显示**"Configure Role Group"（配置角色组）**页。通过页面右上角的**"Help"（帮助）**链接可以访问该页的帮助。

管理 LDAP 安全证书

此部分显示最近上传到 CMC 的 LDAP 证书的属性。如果已上传证书，则用此信息验证证书有效且没有过期。

注： 默认情况下，CMC 没有认证机构颁发的 Active Directory 服务器认证。您必须上载当前的、认证机构签字的服务器认证。

会显示证书的以下属性：

- 序列号 - 证书的序列号。
- 接收者信息 - 证书的接收者（经认证人员的姓名或公司的名称）。
- 颁发者信息 - 证书的颁发者（发证机构的名称）。
- 有效期自 - 证书的起始日期。
- 有效期至 - 证书的失效日期。

用以下控件上传和下载此证书：

- 上传 - 发起证书的上传过程。该证书可从 LDAP 获取，授予对 CMC 的访问权限。
- 下载 - 发起下载过程。会提示您确定保存文件的位置。选择该选项后，单击**"Next"（下一步）**，系统出现"File Download"（文件下载）对话框。通过该对话框指定服务器认证在 management station 或共享网络的位置。

使用 RACADM 配置通用 LDAP 目录服务

注： 此功能支持 IPv4 和 IPv6。

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： 强烈推荐使用"racadm testfeature -f LDAP"目录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

CMC 可配置为随意查询 SRV 记录 DNS 服务器。如果 **cfgLDAPSRVLookupEnable** 属性启用，则忽略 **cfgLDAPServer**属性。以下查询可用于为 SRV 记录搜索 DNS 服务器：

_ldap._tcp.domainname.com

ldap 在上述查询中为 **cfgLDAPSRVLookupServiceName** 的属性。

cfgLDAPSRVLookupDomainName 配置为 **domainname.com**。

用途

若要用 LDAP 用户登录到 CMC，则在登录提示屏幕使用用户名并在密码提示屏幕使用用户密码。如果 LDAP 用户因任何原因而不能登录，CMC 会返回用相同用户名和密码尝试本地登录。这样可以在网络故障或 LDAP 服务器不可用时允许用户登录。

获得帮助

CMC 的追踪日志含用户为什么不能登录的部分信息。若要对 LDAP 登录故障分类，则推荐使用 `racadm testfeature -f LDAP` 命令并打开调试。

目录

目录

配置 CMC 使用命令行控制台

Dell Chassis Management Controller Firmware 版本 3.0 用户指南

本节提供了有关 CMC 命令行控制台（或串行/远程登录/SSH 控制台）功能的信息，并解释要通过控制台执行系统管理操作该如何设置系统。有关通过命令行控制台在 CMC 中使用 RACADM 命令的信息，请参阅 "使用 RACADM 命令行界面"。

CMC 上的命令行控制台功能

CMC 支持以下串行、远程登录和 SSH 控制台功能：

- 存在一个串行客户连接和最多四个并发远程登录客户连接
- 最多四个 SSH 客户端同时连接
- RACADM 命令支持
- 内置 **connect** 命令连接到服务器和 I/O 模块的串行控制台；也可用作 **racadm connect**
- 命令行编辑和历史
- 在所有控制台接口上的会话超时控制

使用串行、远程登录或 SSH 控制台

当连接到 CMC 命令行时，可以输入这些命令：

表 3-1. CMC 命令行命令

命令	说明
racadm	RACADM 命令以关键字 **racadm** 开始，后接一个子命令，如 **getconfig**、**serveraction** 或 **getsensorinfo**。有关使用 RACADM 的详情，请参阅 "使用 RACADM 命令行界面"。
connect	连接到服务器或 I/O 模块的串行控制台。请参阅 "使用 Connect 命令连接到服务器或 I/O 模块" 获得使用 **connect** 命令的帮助。 **注：** 也可使用 **racadm connect** 命令。
exit、logout 和 quit	这些命令都执行相同操作：结束当前会话并返回一个登录提示符。

将远程登录控制台与 CMC 配合使用

任何时刻可以有多达四个远程登录客户系统和四个 SSH 客户端连接。

如果 Management Station 运行 Windows XP 或 Windows 2003，可能会遇到 CMC 远程登录会话中的字符问题。此问题可能表现为冻结登录，即回车键没有反应且密码提示符不出现。

要解决此问题，请从 Microsoft 支持网站 **support.microsoft.com** 下载热修复程序 824810。请参阅 Microsoft 知识库文章 824810 了解有关详情。

将 SSH 与 CMC 配合使用

SSH 是一个命令行会话，具有与远程登录会话相同的功能，不过还具有会话协商和加密功能以提高安全保护级别。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。

如果在登录过程中出现错误，SSH 客户端就会发出一条错误信息。此信息文本依赖于客户端，不受 CMC 控制。查看 RACLog 信息以确定故障原因。

注： OpenSSH 应该从 Windows 上的 VT100 或 ANSI 终端仿真程序中运行。也可用 Putty.exe 运行 OpenSSH。在 Windows 命令提示符处运行 OpenSSH 不会提供完整的功能（即，有些键不响应并且不显示任何图形）。对于 Linux，运行 SSH 客户端服务以使用任何 shell 连接到 CMC。

在任何给定时刻可支持四个同时 SSH 会话。会话超时由 cfgSsnMgtSshIdleTimeout 属性（请参阅《*Dell Chassis Management Controller 管理员参考指南*》的"数据库属性"一章）或 Web 界面的**"Services Management"（服务管理）**页控制（请参阅 "配置服务"）。

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供用户 ID/密码，从而提高了 SSH 脚本编写的自动化程度。有关详情，请参阅"使用 RACADM 配置通过 SSH 的公共密钥验证"。

启用 CMC 上的 SSH

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。

有关使用 RACADM 在 CMC 上启用 SSH 连接的说明，请参阅《*Dell Chassis Management Controller* 管理员参考指南》中的 **config** 命令部分和 **cfgSerial** 数据库属性部分。有关使用 Web 界面在 CMC 上启用 SSH 连接的说明，请参阅 "配置服务"。

更改 SSH 端口

要更改 SSH 端口，使用以下命令：

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort <端口号>
```

有关 cfgSerialSshEnable 和 cfgRacTuneSshPort 属性的详情，请参阅《*Dell Chassis Management Controller 管理员参考指南*》的数据库属性一章。

CMC SSH 实施支持多种加密模式，如表 3-2 中所示。

表 3-2. 加密模式

模式类型	模式
非对称加密	Diffie-Hellman DSA/DSS 512-1024（随机）位/NIST 规范
对称加密	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
信息完整性	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
验证	"Password"（密码）

启用至 iKVM 连接的前面板

有关使用 iKVM 前面板端口的信息和说明，请参阅"启用或禁用前面板"。

配置终端仿真软件

CMC 支持在运行以下一种终端仿真软件的管理工作台上使用串行文本控制台：

- Linux Minicom
- Hilgraeve's HyperTerminal Private Edition（版本 6.3）

执行以下小节中的步骤以配置所用终端软件。

配置 Linux Minicom

Minicom 是 Linux 的串行端口访问公用程序。以下步骤可用于配置 Minicom 版本 2.0。其它 Minicom 版本可能略有不同，但需要相同的基本设置。使用 "必需的 Minicom 设置" 中的信息配置其它版本的 Minicom。

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，键入：`racadm config -g cfgSerial -o cfgSerialConsoleColumns 80`。

1. 如果没有 Minicom 配置文件，则转至下一步。

   如果有 Minicom 配置文件，则键入 `minicom <Minicom config 文件名>` 并跳至 步骤 13。

2. 在 Linux 命令提示符处，键入 `minicom -s`。

3. 选择**"Serial Port Setup"（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> 并将**"Hardware Flow Control"（硬件流控制）**设置为**"Yes"（是）**，将**"Software Flow Control"（软件流控制）**设置为**"No"（否）**。

   要退出**"Serial Port Setup"（串行端口设置）**菜单，按 <Enter>。

7. 选择**"Modem and Dialing"（调制解调器和拨号）**并按 <Enter>。

8. 在**"Modem Dialing and Parameter Setup"（调制解调器拨号和参数设置）**菜单中，按 <Backspace> 清除**"init"（初始化）**、**"reset"（重设）**、**"connect"（连接）**和**"hangup"（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**"Modem Dialing and Parameter Setup"（调制解调器拨号和参数设置）**菜单。

10. 选择**"Save setup as config_name"（将设置另存为 config_name）**并按 <Enter>。

11. 选择**"Exit From Minicom"（从 Minicom 退出）**并按 <Enter>。

12. 在命令解释程序提示符处键入 `minicom <Minicom 配置文件名>`。

13. 按 <Ctrl+a>、<x>、<Enter> 以退出 Minicom。

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

根据表 3-3 配置任何版本的 Minicom。

表 3-3. 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
"Hardware flow control"（硬件流控制）	是
"Software flow control"（软件流控制）	否
"Terminal emulation"（终端仿真）	ANSI
"Modem dialing and parameter settings"（调制解调器拨号和参数设置）	清除**"init"（初始化）**、**"reset"（重设）**、**"connect"（连接）**和**"hangup"（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，可采用几种方式完成串行控制台重定向：

- 使用 CMC 命令行和 **connect** 或 **racadm connect** 命令。有关 **connect** 的详情，请参阅《*Dell Chassis Management Controller 管理员参考指南*》中的 **racadm connect** 命令部分。
- 使用 iDRAC Web 界面串行控制台重定向功能。
- 使用 iDRAC 串行 LAN (SOL) 功能。

在串行/远程登录/SSH 控制台中，CMC 支持 **connect** 命令以建立到服务器或 IOM 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。

小心： 当从 CMC 串行控制台执行时，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 串行控制台连接到一个服务器时，DTR 信号中的过渡（例如，如果拆下串行电缆而连接调试器）不会导致注销。

注： 如果某个 IOM 不支持控制台重定向，则 **connect** 命令将显示闲置的控制台。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>\。

Managed System 上最多有六个 IOM。要连接到一个 IOM，键入：

```
connect switch-n
```

其中 *n* 为 IOM 标签 a1、a2、b1、b2、c1 和 c2。

IOM 标签为 A1、A2、B1、B2、C1 和 C2。（请参阅 图 11-1 获得在机箱中安放 IOM 的图示说明。）当在 **connect** 命令中引用 IOM 时，IOM 将按照 表 3-4所示映射到交换机。

表 3-4. 将 I/O 模块映射到交换机

输入/输出模块标签	交换机
A1	switch-a1
A2	switch-a2
B1	switch-b1
B2	switch-b2
C1	switch-c1
C2	switch-c2

注： 每个机箱每次只能有一个 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串行控制台，请使用命令 **connect server-n**，其中 *-n* 是服务器的插槽编号；也可使用 **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，会看到No route to host（没有至主机的路由）错误信息。

命令 **connect server-n** 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： 为了看到 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，屏幕会出现乱码。

注： 在 BIOS 设置屏幕中，并非所有键都起作用，因此需提供针对 **CTRL+ALT+DEL** 的相应转义序列和其它转义序列。初始重定向屏幕显示所需的转义序列。

为串行控制台重定向配置受管服务器 BIOS

必须使用 iKVM 连接到受管服务器（请参阅 "使用 iKVM 管理服务器"），或从 iDRAC Web GUI 建立远程控制台会话（请参阅 **support.dell.com/manuals** 上的《*iDRAC 用户指南*》）。

默认情况下，BIOS 中的串行通信为"OFF"（关）。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：

1. 引导受管服务器。
2. 在开机自检过程中，按 <F2> 进入 BIOS 设置公用程序。
3. 向下滚动到**"Serial Communication"（串行通信）**并按 <Enter>。在弹出对话框中，串行通信列表显示以下选项：
   - off
   - on without console redirection（开，控制台重定向不启用）
   - on with console redirection via COM1（开，通过 COM1 进行控制台重定向）

   可使用箭头键在这些选项之间导航。

4. 保证启用了**"On with console redirection via COM1"（开，通过 COM1 进行控制台重定向）**。

5. 启用**"Redirection After Boot"（引导后重定向）**（默认值是**"disabled"[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。

6. 保存更改并退出。

7. 受管服务器重新引导。

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 将接收来自 BIOS 的信息，并启用 Special Administration Console (SAC) 控制台一 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)。如果使用不同的引导加载程序，可能需要进行相似的更改。

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添加以下两行新命令：

   ```
   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 (grub.conf 由 anaconda 生成)
#
# 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/sdal
#          initrd /boot/initrd-version.img
#

# (请注意，更改
# 这个文件后，你不必重新运行 grub.
# 注意：你不具备 /boot 分区。这意味着
#       所有的内核 和initrd 路径是相对于 /，例如，
#       root (hd0,0)
#       kernel /boot/vmlinuz-version ro root=/dev/sdal
#       initrd /boot/initrd-version.img)

#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz


#(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
```

```
(串行 --unit=1 --speed=57600
终端 --timeout=10 serial

标题 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
标题 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)
```

编辑 **/etc/grub.conf** 文件时，应遵循以下原则：

- 禁用 GRUB 的图形界面并使用基于文本的界面；否则，GRUB 屏幕将不会显示在控制台重定向中。要禁用图形界面，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=ttzyS1,57600
  ```

  此示例中，`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 (此文件说明如何进行 INIT 过程)
#          should set up the system in a certain (应该将系统设置为特定)
#          run-level. (运行级别。)
#
# Author:  Miquel van Smoorenburg
#          Modified for RHS Linux by Marc Ewing and (由 Marc Ewing 和 Donnie Barnes 为 RHS Linux 修改)
#          Donnie Barnes
#
# Default runlevel.The runlevels used by RHS are:
# (默认运行级别。RHS 使用的运行级别有：)
#   0 - halt (Do NOT set initdefault to this)
#   (0 - 终止 （请勿将此设置为 initdefault）)
#   1 - Single user mode
#   (1 - 单用户模式)
#   2 - Multiuser, without NFS (The same as 3, if you#do not have networking)
#   (2 - 多用户，无 NFS（与 3 相同，如果
#        没有网络连接）)
#   3 - Full multiuser mode
#   (3 - 完全多用户模式)
#   4 - unused
#   (4 - 未使用)
#   5 - X11
#   (5 - X11)
#   6 - reboot (Do NOT set initdefault to this)
#   (6 - 重新启动 （请勿将此设置为 initdefault）)
#
id:3:initdefault:

# System initialization.
# (系统初始化)
si::sysinit:/etc/rc.d/rc.sysinit


l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6

# Things to run in every runlevel.
# (在每个运行级别需要运行的东西。)
ud::once:/sbin/update

# Trap CTRL-ALT-DELETE
# (陷阱 CTRL-ALT-删除)
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"
# (当 UPS 提示我们电源发生故障时，假设还有几 # 分钟的电量余留。请准备从现在起 2 分钟后关机。

# 当然，这是假设你安装有电源以及 # UPS 连接好且工作正常。

# 如果在关机前电源恢复，请取消它。)

# Run gettys in standard runlevels
# (在标准级别运行 gettys)
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
# (在运行级别 5 运行 xdm.)
# xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
# (xdm 现在是一个独立的服务)
```

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
  ```

以例显示含有新行的示例文件。

```
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
```

目录

目录

使用 FlexAddress Plus

Dell Chassis Management Controller Firmware 版本 3.0 用户指南

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 WWN/MAC（全球名称/介质访问控制）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 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 卡只包含 FlexAddress，而标有 FlexAddress Plus 的卡包含 FlexAddress 和 FlexAddress Plus。该卡必须插入 CMC，功能才能激活。

PowerEdge M710HD 等服务器要求多于 FA 提供给 CMC 的 MAC 地址。对于这些服务器来说，升级到 FA+ 可支持 WWN/MAC 配置的全面优化。请联系 Dell 获得 FlexAddress Plus 功能的支持。

若要激活 FlexAddress Plus 功能，则要求更新以下软件：服务器 BIOS、服务器 iDRAC 和 CMC 固件。如果不执行这些更新，则 FlexAddress 功能不可用。

表 7-1. Flexadress Plus 要求的更新

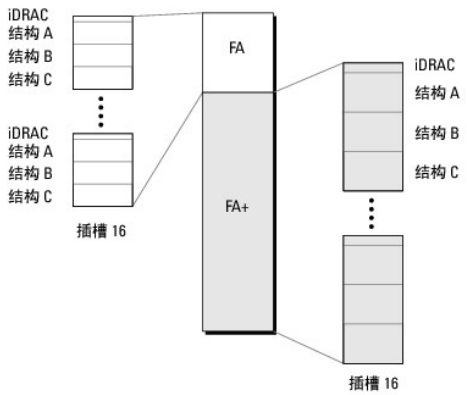
组件	最低要求版本
服务器模块 BIOS	PowerEdge M710hd
iDRAC	版本 3.0 或更高版本
CMC	版本 3.0 或更高版本

FlexAddress 和 FlexAddress Plus 对比

FlexAddress 有 208 个地址分配到 16 个服务器插槽，因此每个插槽分配到 13 个 MAC 地址。FlexAddress Plus 有 2928 个地址分配到 16 个服务器插槽，因此每个插槽分配到 183 个 MAC 地址。下表显示了两种功能下分别提供的 MAC 地址。

	结构 A	结构 B	结构 C	iDRAC 管理	MAC 总数
FlexAddress	4	4	4	1	13
FlexAddress Plus	60	60	60	3	183

图 7-1. FlexAdress (FA) 和 FlexPlusAddress (FA+) 功能对比



MAC 地址分配方案 1 和 2

为了与 FA 向后兼容，FA+ 中的地址分为两组：第一组有 208 个地址，第二组有 2928 个地址。第一组中，13 个 MAC 以与 FA 相同的方式分配到 16 个插槽中的每一个。第二组中，183 个 MAC 被分配到各插槽。

每个服务器第一组的 13 个 MAC 的分配如下：1 个用于 iDRAC，每个结构（A、B、C）各 4 个。在每个结构（A、B、C）内，两个地址分配到端口 1，两个地址分配到端口 2。结果是：

- 1 个 MAC 用于 iDRAC 管理
- 4 个 MAC 用于结构 A（2 个 MAC 用于端口 1，2 个 MAC 用于端口 2）
- 4 个 MAC 用于结构 B（2 个 MAC 用于端口 1，2 个 MAC 用于端口 2）
- 4 个 MAC 用于结构 C（2 个 MAC 用于端口 1，2 个 MAC 用于端口 2）

方便起见，此 MAC 地址分配方式叫做方案 1。

每个服务器第二组的 183 个 MAC 的分配如下：3 个用于 iDRAC，每个结构（A、B、C）各 60 个。在每个结构内，30 个地址分配到端口 1，30 个地址分配到端口 2。结果是：

- 1 个 MAC 用于 iDRAC 管理
- 60 个 MAC 用于结构 A（30 个 MAC 用于端口 1，30 个 MAC 用于端口 2）
- 60 个 MAC 用于结构 B（30 个 MAC 用于端口 1，30 个 MAC 用于端口 2）
- 60 个 MAC 用于结构 C（30 个 MAC 用于端口 1，30 个 MAC 用于端口 2）

方便起见，此 MAC 地址分配方式叫做方案 2。

MAC 地址分配的常用方式是首先根据方案 1 为每结构分配 MAC 地址。如果一个结构要求的地址数超出方案 1 提供的数目，则根据方案 2 为每个结构额外分配 2 个 MAC 地址。

当机箱仅采用 FA 激活且其服务器网络配置要求的地址数超出方案 1 提供的数目时，额外的地址不可用。状态显示为"Not Installed"（未安装）。

如果机箱已激活 FA，则无需禁用 FA 即可增加 FA+。

在此情况下 MAC 地址的具体分配如下：

- 方案 1 分配的 MAC 地址来自功能卡 1.0 的 FA。之前的 WWN/MAC 配置无需更改。
- 方案 2 分配的额外 MAC 地址来自 FA+ 的方案 2 地址。

MAC 地址分配示例

假设 FA 中 MAC 的起始地址为 00:FA:AE:58:59:2B，FA+ 的方案 2 中 MAC 的起始地址为 00:FB:AE:58:59:FB。服务器在插槽 1 中，服务器的网络配置为：

- 1 个MAC 用于 iDRAC
- 8 个 MAC 用于结构 A
- 4 个 MAC 用于结构 B
- 4 个 MAC 用于结构 C

因结构 A 需要的 MAC 地址比方案 1 可提供的多 4 个 ，则前 4 个 MAC 地址根据方案 1 分配自 FA，2 个 MAC 用于端口 1，2 个 MAC 用于端口 2。额外的 4 个 MAC 地址根据方案 2 分配自 FA+，2 个 MAC 用于端口 1，2 个 MAC 用于端口 2。结构 B 和 C 的 iDRAC 的 MAC 地址根据方案 1 分配自 FA。

来自 FA+ 的结构 A 端口 1 的起始地址为 00:23:AE:58:59:FE，因为前 3 个 MAC 地址为 iDRAC 保留。因此机箱为服务器分配的 MAC 地址为：

iDRAC	00:FA:AE:58:59:2B（自 FA）
结构 A 端口 1：	00:FA:AE:58:59:2C（自 FA） 00:FA:AE:58:59:2D（自 FA） 00:FB:AE:58:59:FE（自 FA+） 00:FB:AE:58:59:FF（自 FA+）
结构 A 端口 2：	00:FA:AE:58:59:2E（自 FA） 00:FA:AE:58:59:2F（自 FA） 00:FB:AE:58:5A:00（自 FA+） 00:FB:AE:58:5A:01（自 FA+）
结构 B 端口 1：	00:FA:AE:58:59:30（自 FA） 00:FA:AE:58:59:31（自 FA）

结构 B 端口 2：	00:FA:AE:58:59:32（自 FA） 00:FA:AE:58:59:33（自 FA）
结构 C 端口 1：	00:FA:AE:58:59:34（自 FA） 00:FA:AE:58:59:35（自 FA）
结构 C 端口 2：	00:FA:AE:58:59:36（自 FA） 00:FA:AE:58:59:37（自 FA）

在使用之前无 FA 的机箱 — 或从未激活或曾激活但又禁用 — 且其服务器网络配置要求的地址数超出方案 1 提供数目时，方案 1 分配获得来自 FA 的方案 1 的地址，而方案 2 分配获得来自 FA+ 的方案 2 的地址。

根据上例，此情况下同一服务器由机箱分配的 MAC 地址为：

iDRAC	00:FB:AE:58:59:2B (FA)
结构 A 端口 1：	00:FB:AE:58:59:2C (FA) 00:FB:AE:58:59:2D (FA) 00:FB:AE:58:59:FE (FA+) 00:FB:AE:58:59:FF (FA+)
结构 A 端口 2：	00:FB:AE:58:59:2E (FA) 00:FB:AE:58:59:2F (FA) 00:FB:AE:58:5A:00 (FA+) 00:FB:AE:58:5A:01 (FA+)
结构 B 端口 1：	00:FB:AE:58:59:30 (FA) 00:FB:AE:58:59:31 (FA)
结构 B 端口 2：	00:FB:AE:58:59:32 (FA) 00:FB:AE:58:59:33 (FA)
结构 C 端口 1：	00:FB:AE:58:59:34 (FA) 00:FB:AE:58:59:35 (FA)
结构 C 端口 2：	00:FB:AE:58:59:36 (FA) 00:FB:AE:58:59:37 (FA)

目录

目录

使用 FlexAddress

Dell Chassis Management Controller Firmware 版本 3.0 用户指南

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 替换工厂分配的全球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 资源以感知新的服务器模块。

FlexAddress 允许 CMC 分配 WWN/MAC ID 到特定插槽并*取代*工厂 ID。如果更换服务器模块，基于插槽的 WWN/MAC ID 将保持相同。该功能可以避免为新服务器模块重新配置以太网管理工具和 SAN 资源的麻烦。

此外，*取代操作*仅当服务器模块插入启用 FlexAddress 的机箱时发生；并且不会对服务器模块进行任何永久更改。如果将服务器模块移动到不支持 FlexAddress 的机箱，则将使用工厂分配的 WWN/MAC ID。

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 文件将包含 XML 标签 *mac_start*，它代表将被用于该唯一 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：

<*mac_start*> + 0xCF (208 - 1) = mac_end

其中 208 是 mac_count，公式为
<mac_start> + <mac_count> - 1 = <mac_end>

例如：（起始 MAC）00188BFFDCFA + 0xCF =（终止 MAC）00188BFFDDC9。

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*。

激活 FlexAddress

安全数字 (SD) 卡上提供了 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、I/O 夹层 BIOS 或固件，以及 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 功能可能无法按照预期方式工作。

组件	最低要求版本
以太网夹层卡 - Broadcom M5708t，5709，5710	引导代码固件 4.4.1 或更高版本 iSCSI 引导固件 2.7.11 或更高版本 PXE 固件 4.4.3 或更高版本
FC 夹层卡 - QLogic QME2472，FC8	BIOS 2.04 或更高版本
FC 夹层卡 - Emulex LPe1105-M4，FC8	BIOS 3.03a3 和固件 2.72A2 或更高版本
服务器模块 BIOS	PowerEdge M600 - BIOS 2.02 或更高版本 PowerEdge M605 - BIOS 2.03 或更高版本 PowerEdge M805 PowerEdge M905 PowerEdge M610 PowerEdge M710 PowerEdge M710hd
PowerEdgeM600/M605 主板上的 LAN (LOM)	引导代码固件 4.4.1 或更高版本 iSCSI 引导固件 2.7.11 或更高版本
iDRAC	对于 PowerEdge *xx*0*x* 系统，为版本 1.50 或更高版本

	对于 PowerEdge *xx*1*x* 系统，为版本 2.10 或更高版本
CMC	版本 1.10 或更高版本

注： 2008 年 6 月以后订购的任何系统都拥有正确的固件版本。

为了保证正确部署 FlexAddress 功能，请按以下顺序更新 BIOS 和固件：

1. 更新所有夹层卡固件和 BIOS。
2. 更新服务器模块 BIOS。
3. 更新服务器模块上的 iDRAC 固件。
4. 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。
5. 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 SD 卡的安装说明，请参阅*机箱管理控制器 (CMC) 安全数字 (SD) 卡技术规格*文件。

注： SD 卡含有 FlexAddress 功能。SD 卡上含有的数据经过加密，不能以任何方式复制或修改，因为会禁止系统功能并导致系统出现故障。

注： 一张 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 中已安装 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*机箱管理控制器 (CMC) 安全数字 (SD) 卡技术规格*说明文件。

当重启 CMC 时，使用下一节"验证 FlexAddress 激活"中介绍的步骤验证激活过程。

验证 FlexAddress 激活

要确保正确激活 FlexAddress，可以使用 RACADM 命令验证 SD 功能卡和 FlexAddress 激活。

使用以下 RACADM 命令验证 SD 功能卡及其状态：

```
racadm featurecard -s
```

表 6-1. 通过 featurecard -s 命令返回状态信息

状态信息	操作
未插入功能卡。	检查 CMC 以验证 SD 卡已正确插入。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。
插入的功能卡有效且包含以下功能 FlexAddress：功能卡绑定到此机箱。	无需任何操作。
插入的功能卡有效且包含以下功能 FlexAddress：功能卡绑定到另一个机箱。 svctag = ABC1234, SD card SN = 01122334455	拆下 SD 卡；为当前机箱找到并安装 SD 卡。
插入的功能卡有效且包含以下功能 FlexAddress：功能卡未绑定到任何机箱。	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 racadm racreset，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
```

此命令将返回以下状态信息：

```
Feature = FlexAddress
(功能 = FlexAddress)

Date Activated = 8 April 2008 - 10:39:40
(激活日期 = 2008 年 4 月 8 日 - 10：39：40)

Feature installed from SD-card SN = 01122334455
(从 SD-卡 SN 上安装的功能 = 01122334455)
```

如果机箱中没有激活的功能，则此命令将返回信息：

```
racadm feature -s
```

(Racadm 功能 -s)

机箱中没有激活的功能。

Dell 功能卡可含一个以上的功能。一旦 Dell 功能卡上的任一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信息：

ERROR: One or more features on the SD card are active on another chassis（错误：SD 卡的一个或多个功能已在其他机箱上激活。）

有关 RACADM 命令的详情，请参阅《*Dell Chassis Management Controller* 管理员参考指南》中的 **feature** 和 **featurecard** 命令部分。

取消激活 FlexAddress

使用 RACADM 命令可以取消激活 FlexAddress 功能，并将 SD 卡还原到安装前的状态。Web 界面中没有取消激活功能。取消激活将把 SD 卡还原到原始状态，以便可以在另一个机箱上安装和激活。

注： SD 卡必须物理安装在 CMC 中，并且在执行取消激活命令之前必须关闭机箱电源。

如果在未安装卡时执行取消激活命令，或者对安装在不同机箱上的卡执行该命令，则将取消激活该功能且无法恢复对该卡所做的任何更改。

取消激活 FlexAddress

使用以下 RACADM 命令取消激活 FlexAddress 功能并恢复 SD 卡：

racadm feature -d -c flexaddress

成功取消激活后，该命令将返回以下状态信息：

"feature FlexAddress is deactivated on the chassis successfully."（功能 FlexAddress 在机箱上取消激活成功。）

如果在执行命令前未关闭机箱电源，则该命令将失败并出现以下错误信息：

"ERROR: Unable to deactivate the feature because the chassis is powered ON"（错误：因为机箱电源打开，所以无法取消激活该功能）

有关命令的详情，请参阅《*Dell Chassis Management Controller* 管理员参考指南》中的 **feature** 命令部分。

使用 CLI 配置 FlexAddress

注： 插槽和结构都必须启用，才能将机箱分配的 MAC 地址推送到 iDRAC。

注： 也可以使用图形用户界面查看 FlexAddress 状态。有关详情，请参阅"FlexAddress"。

可以使用命令行界面在每个结构的基础上启用或禁用 FlexAddress。此外，还可以在每个插槽的基础上启用/禁用该功能。在每结构基础上启用该功能后，可以选择要启用的插槽。例如，如果仅启用结构 A，则启用的任何插槽将仅在结构 A 上启用 FlexAddress。所有其他结构将使用服务器上工厂分配的 WWN/MAC。为了使此功能起作用，必须启用结构，而且必须将服务器关机。

已启用的插槽将会为所有已启用的结构启用 FlexAddress。例如，如果启用结构 A 和 B，要在结构 A 的插槽 1 上启用 FlexAddress，而不在结构 B 的插槽 1 上启用 FlexAddress，这是不可能的。

使用以下 RACADM 命令启用或禁用结构：

racadm setflexaddr [-f <结构名称> <状态>]

<结构名称> = A, B, C 或 iDRAC

<状态> = 0 或 1

其中 **0** 表示禁用，**1** 表示启用。

使用以下 RACADM 命令启用或禁用结构：

racadm setflexaddr [-i <插槽编号> <状态>]

<插槽编号> = 1 至 16

<状态> = 0 或 1

其中 **0** 表示禁用，**1** 表示启用。

有关命令的其它信息，请参阅《*Dell Chassis Management Controller* 管理员参考指南》中的 **setflexaddr** 命令部分。

用于 Linux 的其他 FlexAddress 配置

当在基于 Linux 的操作系统上将服务器分配的 MAC ID 更改为机箱分配的 MAC ID 时，可能需要执行其它配置步骤：

- SUSE Linux Enterprise Server 9 和 10：您可能需要在 Linux 系统上运行 YAST (Yet another Setup Tool) 来配置网络设备，然后重新启动网络服务。
- Red Hat Enterprise Linux 4(RHEL) 和 RHEL 5：运行 Kudzu，该公用程序用于检测和配置系统上的新硬件/更改的硬件。Kudzu 为您提供"硬件发现菜单"，拆下硬件和添加新硬件时，它会检测 MAC 地址变化。

使用 CLI 查看 FlexAddress 状态

可以使用命令行界面查看 FlexAddress 状态信息。可以查看整个机箱或特定插槽的状态信息。显示的信息包括：

- 结构配置
- 启用/禁用 FlexAddress
- 插槽数量和名称
- 机箱分配的地址和服务器分配的地址
- 使用中的地址

使用以下 RACADM 命令显示整个机箱的 FlexAddress 状态：

```
racadm getflexaddr
```

要显示特定插槽的 FlexAddress 状态：

```
racadm getflexaddr [-i <插槽编号>]
```

<插槽编号> = 1 至 16

有关 FlexAddress 配置的其它详情，请参阅 "使用 CLI 配置 FlexAddress"。有关命令的其它信息，请参阅《*Dell Chassis Management Controller 管理员参考指南*》中的 **getflexaddr** 命令部分。

使用 GUI 配置 FlexAddress

Wake-On-LAN 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 可用于通过 LAN 唤醒 (WOL) 功能。

FlexAddress 故障排除

本节包含 FlexAddress 故障排除信息。

1. 如果取出功能卡，会发生什么情况？

   什么也不会发生。功能卡可以取出和存储，或者原样不动。

2. 如果取出某台机箱中使用的功能卡，并将它放入另一台机箱中，会发生什么情况？

   Web 界面将显示错误消息表明：

   This feature card was activated with a different chassis. It must be removed before accessing the FlexAddress feature.（该功能卡已在另一台机箱中激活。在访问 FlexAddress 功能前必须先取出功能卡。）

   Current Chassis Service Tag = XXXXXXXX （当前机箱服务标签 = XXXXXXXX）

   Feature Card Chassis Service Tag = YYYYYYYY （功能卡机箱服务标签 = YYYYYYYY）

   CMC 日志中将添加一项条目表明：

   cmc <日期时间戳> : feature 'FlexAddress@XXXXXXX' not activated; chassis ID='YYYYYYY'

3. 如果取出功能卡并安装非 FlexAddress 卡，会发生什么情况？

不会激活或修改该卡。CMC 将忽略该卡。在这种情况下，**$racadm featurecard -s** 将返回消息：

"No feature card inserted"（未插入功能卡）

"ERROR: can't open file"（错误：无法打开文件）

4. 如果重新编程机箱服务标签，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它机箱上的活动 CMC 中存在原始功能卡，Web 界面将显示以下错误：

     This feature card was activated with a different chassis. It must be removed before accessing the FlexAddress feature. (该功能卡已在另一台机箱中激活。在访问 FlexAddress 功能前必须先取出功能卡。)

     Current Chassis Service Tag = XXXXXXXX (当前机箱服务标签 = XXXXXXXX)

     Feature Card Chassis Service Tag = YYYYYYYY (功能卡机箱服务标签 = YYYYYYYY)

     原始功能卡不能再在该机箱或任何其它机箱上取消激活，除非 Dell 服务人员重新将原始机箱服务标签设置回机箱中，并且具有原始功能卡的 CMC 在该机箱中设为活动。

   - FlexAddress 功能在原来绑定的机箱上仍处于激活状态。将更新*该机箱绑定*功能，以反映新服务标签。

5. 如果在冗余 CMC 系统中安装两块功能卡，会发生什么情况？我是否会得到错误消息？

   活动 CMC 中的功能卡将被激活并安装在机箱中。CMC 将忽略第二块卡。

6. SD 卡上是否具有写保护锁？

   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** 命令将返回以下信息：

   No features active on the chassis. ERROR: read only file system（机箱中没有激活的功能。错误：只读文件系统）

7. 如果在活动的 CMC 模块中没有 SD 卡，会发生什么情况？

   $racadm featurecard -s 命令将返回以下信息：

   No feature card inserted. （未插入功能卡。）

8. 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？

   服务器模块需要在使用 FlexAddress 之前关闭电源。服务器 BIOS 更新完成后，服务器模块将在服务器关闭电源再打开电源之后获得机箱分配的地址。

9. 如果具有单个 CMC 的机箱将固件版本降级到 1.10 之前的版本会发生什么情况？

   - 将从机箱删除 FlexAddress 功能和配置。
   - 用于激活此机箱上的功能的功能卡不变，而且仍然绑定到该机箱。随后将机箱的 CMC 固件升级到版本 1.10 或更高版本时，通过重新插入原始功能卡（如有必要），重设 CMC（如果在固件升级完成之后插入功能卡）和重新配置功能来重新激活 FlexAddress 功能。

10. 在带有冗余 CMC 的机箱中，如果将 CMC 单元更换为固件版本早于 1.10 的 CMC 单元，必须执行以下过程确保当前 FlexAddress 功能和配置不会被删除。

    a. 确保活动 CMC 固件始终为版本 1.10 或更高。

    b. 删除待机 CMC 并在其位置上插入新的 CMC。

    c. 从活动 CMC 中，将待机 CMC 固件升级到 1.10 或更高版本。

    注： 如果您没有将待机 CMC 的固件更新到 1.10 或更高版本，发生故障转移时，则将无法配置 FlexAddress 功能，而且您需要重新激活和重新配置该功能。

11. 我对 FlexAddress 执行取消激活命令时，SD 卡不在机箱中。我现在该如何恢复我的 SD 卡？

    问题在于，如果取消激活 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，请将卡插回其绑定到的机箱的 CMC 中，重新安装 FlexAddress，然后重新取消激活 FlexAddress。

12. 我已正确安装了 SD 卡和所有固件/软件更新。我看到 FlexAddress 处于活动状态，但没有在服务器部署屏幕上看到任何可以部署的卡？问题出在哪里？

    这是浏览器缓冲问题；请关闭浏览器并重新启动。

13. 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。默认情况下将选择所有结构和插槽。

    注： 在发出 RACADM 命令 racresetcfg 之前，强烈建议关闭机箱电源。

命令信息

下表列出 RACADM 命令和常见 FlexAddress 情况的输出。

表 6-2. 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	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature (s) FlexAddress: The feature card is bound to another chassis, svctag = J310TF1 SD card SN =0188BFFE03A`
活动 CMC 模块中的 SD 卡绑定到相同的服务标签	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature (s) FlexAddress: The feature card is bound to this chassis`
活动 CMC 模块中的 SD 卡绑定到任意服务标签	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature (s) FlexAddress: The feature card is not bound to any chassis`
由于某些原因（未插入 SD 卡/损坏 SD 卡/功能取消激活后/SD 卡绑定到不同机箱），机箱上的 FlexAddress 功能未活动	`$racadm setflexaddr [-f <fabricName> <slotState>]` 或 `$racadm setflexaddr [-i <slot#> <slotState>]`	`ERROR: Flexaddress feature is not active on the chassis`
来宾用户尝试在插槽/结构上设置 FlexAddress	`$racadm setflexaddr [-f <fabricName> <slotState>]` `$racadm setflexaddr [-i <slot#> <slotState>]`	`ERROR: Insufficient user privileges to perform operation`
电源处于打开状态的机箱无法取消激活 FlexAddress 功能	`$racadm feature -d -c flexaddress`	`ERROR: Unable to deactivate the feature because the chassis is powered ON`
来宾用户尝试取消激活机箱上的功能	`$racadm feature -d -c flexaddress`	`ERROR: Insufficient user privileges to perform operation`
服务器模块电源打开时更改插槽/结构 FlexAddress 设置	`$racadm setflexaddr -i 1 1`	`ERROR: Unable to perform the set operation because it affects a powered ON server`

FlexAddress DELL 软件许可协议

本协议是您（用户）与 Dell Products L.P 或 Dell 全球 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它知识产权。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，则可以随时使用的软件份数与许可份数相同。"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它计算机，并且获分配本软件的每台计算机均具有单独的许可，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份数。如果安装在网络服务器上的软件的用户数超过许可份数，则必须购买更多的软件许可，使许可份数与用户数相等，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了本协议中的条款。

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

Dell 保证本软件磁盘在您收到之日起九十 (90) 天内，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 并承担费用和风险。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它所有的明示或暗示担保，包括但不限于可销售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；您可能还具有其它权利，视管辖区域的不同而有所不同。

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、业务信息丢失或其它经济损失）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。

本开放源软件的发布旨在希望其将是有用的，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负责（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（包括疏忽或其它原因），即使已得到可能会有此类损失的提示。

美国 政府有限权利

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"商业计算机软件文档" 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。本许可将依据上述条件终止，或者如果您违反了本许可规定的任何条款，则本许可将会被终止。一旦终止，您同意销毁本软件及其附带材料以及它们的所有复制件。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它规定、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。

目录

目录

使用 iKVM 模块

Dell Chassis Management Controller Firmware 版本 3.0 用户指南

概览

Dell M1000e 服务器机箱的本地访问 KVM 模块称为 Avocent 集成 KVM 交换机模块，或 iKVM。iKVM 是一种插入机箱中的模拟键盘、视频和鼠标交换机。它是机箱的可选热插拔模块，提供至机箱中的服务器和活动 CMC 命令行的本地键盘、鼠标和视频访问。

iKVM 用户界面

iKVM 使用屏上配置和报告 (OSCAR) 图形用户界面，可通过热键激活。OSCAR 允许用户选择要通过本地键盘、显示器和鼠标访问的其中一个服务器或 Dell CMC 命令行。

每个机箱只允许有一个 iKVM 会话。

安全保护

OSCAR 用户界面允许用户使用屏幕保护程序密码保护自己的系统。在经过用户定义的一段时间后，屏幕保护程序模式启用，访问将被禁止，直到输入相应密码重新激活 OSCAR 为止。

扫描

当 OSCAR 处于扫描模式时，OSCAR 允许用户选择一组按所选次序显示的服务器。

服务器标识

CMC 为机箱中所有服务器分配插槽名称。虽然您可通过分层连接使用 OSCAR 界面为服务器分配名称，但是 CMC 分配的名称具有优先权，使用 OSCAR 为服务器分配的任何新名称都将被改写。

CMC 通过向插槽分配唯一名称来识别插槽。要使用 CMC Web 界面更改插槽名称，请参阅"编辑插槽名称"。要使用 RACADM 更改插槽名称，请参阅《*Dell Chassis Management Controller 管理员参考指南*》中的 **setslotname** 部分。

显卡

iKVM 视频连接可支持从 640 x 480（60 赫兹）到 1280 x 1024（60 赫兹）的视频显示分辨率。

即插即用

iKVM 支持显示数据信道 (DDC) 即插即用功能，可自动进行视频显示器配置，并符合 VESA DDC2B 标准。

FLASH 可升级

您可以使用 CMC Web 界面或 RACADM **fwupdate** 命令更新 iKVM 固件。有关详情，请参阅"从 CMC 管理 iKVM"。

物理连接接口

您可以从机箱前面板、模拟控制台接口 (ACI) 和机箱后面板通过 iKVM 连接到服务器或 CMC CLI 控制台。

注： 机箱正面控制面板上的端口专门为 iKVM 设计，为可选组件。如果没有 iKVM，则无法使用前控制面板端口。

iKVM 连接优先次序

一次只能有一个 iKVM 连接。iKVM 向每种类型连接分配优先次序，以便当存在多个连接时，只有一个连接可用，其他连接均被禁用。

iKVM 连接的优先次序如下所示：

1. 前面板
2. ACI
3. 后面板

例如，如果前面板和 ACI 中有 iKVM 连接，则前面板连接保持活动，而 ACI 连接被禁用。如果有 ACI 和后面板连接，则 ACI 连接具有优先权。

通过 ACI 连接分层

iKVM 允许与服务器和 iKVM 的 CMC 命令行控制台建立分层连接，既可以通过远程控制台交换机端口本地实现，也可以通过 Dell RCS 软件远程实现。 iKVM 支持从以下产品进行 ACI 连接：

- 180AS、2160AS、2161DS*、2161DS-2 或 4161DS Dell 远程控制台交换机
- Avocent AutoView 交换系统
- Avocent DSR 交换系统
- Avocent AMX 交换系统

* 不支持 Dell CMC 控制台连接。

注： iKVM 还支持至 Dell 180ES 和 2160ES 的 ACI 连接，但不是无缝分层。此连接要求一个至 PS2 SIP 的 USB。

使用 OSCAR

本节提供了 OSCAR 界面的概览。

导航基础知识

表 10-1. OSCAR 键盘和鼠标导航

键或键顺序	结果
• <Print Screen>-<Print Screen> • <Shift>-<Shift> • <Alt>-<Alt> • <Ctrl>-<Ctrl>	任何这些键顺序都可以打开 OSCAR，取决于用户的 **"Invoke OSCAR"（调用 OSCAR）**设置。可通过选择**"Main"（主菜单）**对话框**"Invoke OSCAR"（调用 OSCAR）**部分中的各框，然后单击**"OK"（确定）**，启用两个、三个或全部这些键顺序。
<F1> 键	打开当前对话框的**"Help"（帮助）**屏幕。
<Esc> 键	不保存更改而关闭当前对话框，并返回到上一个对话框。 在**"Main"（主菜单）**对话框中，<Esc> 将关闭 OSCAR 界面并返回到所选服务器。 在信息框中，它将关闭弹出框并返回到当前对话框。
<Alt>	当与下划线字母或其他指定字符配合使用时，将打开对话框，选择或勾选选项，并执行操作。
<Alt>+<X>	关闭当前对话框并返回到上一个对话框。
<Alt>+<O>	选择**"OK"（确定）**按钮，然后返回到上一个对话框。
<Enter>	完成**"Main"（主菜单）**对话框中的切换操作，并退出 OSCAR。
单击，<Enter>	在文本框中,选择要编辑的文本并启用左箭头键和右箭头键移动光标。再次按下 <Enter> 退出编辑模式。

<Print Screen>, <Backspace>	如果没有其他按键操作，则切换回上一个选择。
<Print Screen>, <Alt>+<0>	立刻断开用户与服务器的连接；不选择服务器。状况标志显示可用。（此操作只适用于键盘而非小键盘上的 =<0>。）
<Print Screen>, <Pause>	如果该特定控制台采用了密码保护，使用该键可立刻打开屏幕保护程序模式并阻止对该控制台的访问。
上/下箭头键	在列表的行间移动光标。
右/左箭头键	编辑文本框时，在列间移动光标。
<Home>/<End>	移动光标至列表的顶部 (Home) 或底部 (End)。
<Delete>	删除文本框中的字符。
数字键	从键盘或小键盘键入数字。
<Caps Lock>	禁用。要更改大小写，使用 <Shift> 键。

配置 OSCAR

表 10-2. OSCAR 设置菜单功能

功能	用途
菜单	按插槽号以数字顺序或按名称以字母顺序更改服务器排列。
安全保护	• 设置限制对服务器访问的密码。 • 启用屏幕保护程序并设置屏幕保护程序出现之前的非活动时间，然后设置屏幕保护模式。
标志	更改状况标志的显示、时间、颜色或位置。
语言	更改所有 OSCAR 屏幕的语言。
广播	设置通过键盘和鼠标操作同时控制多个服务器。
扫描	为多达 16 个服务器设置自定义扫描样式。

要访问**"Setup"（设置）**对话框：

1. 按 <Print Screen> 键启动 OSCAR 界面。随即显示**"Main"（主菜单）**对话框。
2. 单击**"Setup"（设置）**。**"Setup"（设置）**对话框会出现。

更改显示行为

使用**"Menu"（菜单）**对话框更改服务器的显示次序并设置 OSCAR 的屏幕延迟时间。

要访问**"Menu"（菜单）**对话框：

1. 按下 <Print Screen> 启动 OSCAR。随即显示**"Main"（主菜单）**对话框。
2. 单击**"Setup"（设置）**，然后单击**"Menu"（菜单）**。随即显示**"Menu"**（菜单）对话框。

要在**"Main"（主菜单）**对话框中选择服务器的默认显示次序：

1. 选择**"Name"（名称）**，按名称以字母顺序显示服务器。

   或

   选择**"Slot"**（插槽）以按插槽编号的数字顺序显示服务器。
2. 单击**"OK"（确定）**。

要为 OSCAR 激活分配一个或多个键顺序：

1. 从**"Invoke OSCAR"（调用 OSCAR）**菜单中选择一个键顺序。
2. 单击**"OK"（确定）**。

调用 OSCAR 的默认键为 <Print Screen>。

要为 OSCAR 设置屏幕延迟时间：

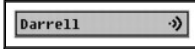
1. 输入按下 <Print Screen> 后使 OSCAR 延迟显示的秒数（0 到 9）。输入 <0> 无延迟启动 OSCAR。
2. 单击**"OK"（确定）**。

设置 OSCAR 延迟显示时间可允许用户完成一次软切换。要执行软切换，请参阅 "软切换"。

控制状况标志

状况标志会显示在桌面上，说明所选服务器的名称或所选插槽的状况。使用**"Flag"（标志）**对话框配置要按服务器显示的标志或更改桌面上标志的颜色、不透明度、显示时间和位置。

表 10-3. OSCAR 状态标志

标志	说明
	按名称划分的标志类型
	表示用户已从所有系统断开连接的标志
	表示广播模式已启用的标志

要访问**"Flag"（标志）**对话框：

1. 按下 <Print Screen>。随即显示**"Main"（主菜单）**对话框。
2. 单击**"Setup"（设置）**，然后单击**"Flag"（标志）**。**"Flag"（标志）**对话框会出现。

要指定如何显示状况标志：

1. 选择**"Displayed"（已显示）**使标志始终显示，或选择**"Displayed and Timed"（已显示和计时）**使标志在交换后只显示 5 秒钟。

   注： 如果选择**"Timed"（已计时）**，则标志不会显示。

2. 从**"Display Color"（显示颜色）**部分选择一种标志颜色。选项为黑色、红色、蓝色和紫色。
3. 在**"Display Mode"（显示模式）**中，选择**"Opaque"（不透明）**用于不透明颜色标志，或选择**"Transparent"（透明）**可通过标志看到桌面。
4. 要在桌面上安排状态标志的位置：
   a. 单击**"Set Position"（设置位置）。 "Set Position Flag"（设置位置标志）**会显示。
   b. 左击标题栏并将它拖到桌面上的所需位置。
   c. 右击返回到**"Flag"（标志）**对话框。

注： 只有当单击**"Flag"（标志）**对话框中的**"OK"（确定）**后，对标志位置进行的更改才会被保存。

5. 单击**"OK"（确定）**保存设置。

   要不保存更改而退出，单击  。

使用 iKVM 管理服务器

iKVM 是一种可支持多达 16 个服务器的模拟交换机。iKVM 交换机使用 OSCAR 用户界面选择和配置服务器。此外，iKVM 还包括一个系统输入，可与 CMC 建立 CMC 命令行控制台连接。

外围设备兼容性与支持

iKVM 与以下外围设备兼容：

- 采用 QWERTY、QWERTZ、AZERTY 和日式 109 布局的标准 PC USB 键盘。
- 配备 DDC 支持的 VGA 显示器。

- 标准 USB 定点设备。
- 连接到 iKVM 上本地 USB 端口的自备电源 USB 1.1 集线器。
- 连接到 Dell M1000e 机箱前面板控制台的 Powered USB 2.0 集线器。

注： 可以在 iKVM 本地 USB 端口上使用多个键盘和鼠标。iKVM 将汇集输入信号。如果存在来自多个 USB 键盘或鼠标的同时输入信号，则可能产生不可预测的结果。

注： USB 连接专用于支持的键盘、鼠标和 USB 集线器。iKVM 不支持来自其他 USB 外围设备的数据传输。

查看并选择服务器

使用 OSCAR **"Main"（主菜单）**对话框通过 iKVM 查看、配置和管理服务器。可以按名称或插槽查看服务器。插槽编号是服务器所占用的机箱插槽编号。**"Slot"**（插槽）列指示安装服务器的插槽编号。

注： Dell CMC 命令行占用插槽 17。选择此插槽显示 CMC 命令行，其中您可执行 RACADM 命令或连接到服务器或 I/O 模块的串行控制台。

注： 服务器名称和插槽编号由 CMC 分配。

访问 **"Main"（主菜单）**对话框的步骤：

按 <Print Screen> 键启动 OSCAR 界面。随即显示**"Main"（主菜单）**对话框。

或

如果已指定密码，屏幕将显示 **Password**（密码）对话框。请键入您的密码，然后单击**"OK"（确定）**。随即显示**"Main"（主菜单）**对话框。

有关设置密码的详情，请参阅 "设置控制台安全性"。

注： 有四个选项可以调用 OSCAR。可通过选择**"Main"（主菜单）**对话框**"Invoke OSCAR"（调用 OSCAR）**部分中的各框，然后单击**"OK"（确定）**，启用一个、多个或全部这些键顺序。

查看服务器状况

机箱中服务器的状况显示在**"Main"（主菜单）**对话框的右侧几列中。下表说明了状况符号。

表 10-4. OSCAR 界面状况符号

符号	说明
	（绿点。）服务器联机。
	（红 X。）服务器脱机或不在机箱中。
	（黄点。）服务器不可用。
	（绿色 A 或 B。）服务器正被由字母表示的用户信道访问：A=后面板、B=前面板。

选择服务器

使用**"Main"（主菜单）**对话框选择服务器。选择服务器时，iKVM 将重新配置键盘和鼠标，使之符合该服务器的正确设置。

- 要选择服务器：

  双击服务器名称或插槽号。

  或

  如果服务器列表的显示次序是按插槽排列（即，**"Slot"（插槽）**按钮按下），则键入插槽号并按下 <Enter>。

  或

  如果服务器列表的显示次序是按名称排列（即，**"Name"（名称）**按钮按下），则键入服务器名称的前几个字符，将其建立为唯一名称，然后按两次 <Enter>。

- 要选择上一个服务器：

  按下 <Print Screen>，然后按下 <Backspace>。此组合键在上一个和当前连接之间进行切换。

- 要从服务器上断开用户：

  按下 <Print Screen> 访问 OSCAR，然后单击**"Disconnect"（断开连接）**。

或

按下 <Print Screen>，然后按下 <Alt><0>。这将使用户处于可用状态，而未选择任何服务器。桌面上如果有激活的状态标志，则显示为"Free"（可用）。请参阅"控制状况标志"。

软切换

软切换是使用热键顺序的服务器之间的切换。通过按下 <Print Screen> 键并键入服务器名称或编号的前几个字符，即可软切换至该服务器。如果以前设置了**延迟时间**（从按下 <Print Screen> 后到**"Main"（主菜单）**对话框显示前所间隔的秒数），又在该时间结束前按下了键序列，则 OSCAR 界面不会显示。

要将 OSCAR 配置为软切换：

1. 按 <Print Screen> 键启动 OSCAR 界面。随即显示**"Main"（主菜单）**对话框。
2. 单击**"Setup"（设置）**，然后单击**"Menu"（菜单）**。随即显示"**Menu**"（菜单）对话框。
3. 为显示/排序键选择**"Name"（名称）**或**"Slot"（插槽）**。
4. 在**"Screen Delay Time"（屏幕延迟时间）**字段中键入所需延迟秒数。
5. 单击**"OK"（确定）**。

要软切换到一个服务器：

- 要选择服务器，按下 <Print Screen>。

  如果服务器列表的显示次序为在步骤 3 中选择的按插槽排列（即，**"Slot"（插槽）**按钮被按下），则键入插槽号并按下 <Enter>。

  或

  如果服务器列表的显示次序为在步骤 3 中选择的按名称排列（即，**"Name"（名称）**按钮被按下），则键入服务器名称的前几个字符，将其建立为唯一名称，然后按下 <Enter>。

- 要切换回到上一个服务器，按下 <Print Screen>，然后按下 <Backspace>。

视频连接

iKVM 在机箱的前面板和后面板上有视频连接。前面板连接信号优先于后面板连接信号。当显示器连接到前面板时，视频连接不会传递到后面板，会显示一条后面板 KVM 和 ACI 连接均已禁用的 OSCAR 信息。如果显示器被禁用（即，被从前面板上卸下或被 CMC 命令禁用），则 ACI 连接成为活动的，而后面板 KVM 仍被禁用。（有关连接优先顺序的信息，请参阅"iKVM 连接优先次序"。）

有关启用或禁用前面板连接的信息，请参阅"启用或禁用前面板"。

抢占警告

通常，一个通过 iKVM 连接到服务器模块的用户与另一个通过 iDRAC GUI 控制台重定向功能连接到同一个服务器控制台的用户，均具有对该控制台的访问权并可以同时键入信息。

要防止这种情况，在开始 iDRAC GUI 控制台重定向之前，远程用户可以禁用 iDRAC Web 界面中的本地控制台。本地 iKVM 用户会看到一条该连接将在指定时间中被抢占使用的 OSCAR 信息。本地用户应在至服务器的 iKVM 连接终止之前完成工作。

未向 iKVM 用户提供任何占先功能。

注： 如果某个远程 iDRAC 用户已禁用某个特定服务器的本地视频，则该服务器的视频、键盘和鼠标对 iKVM 不可用。服务器状态在 OSCAR 菜单中以一个黄点标记，表示它已被锁定或无法在本地使用（请参阅"查看服务器状况"）。

设置控制台安全性

OSCAR 允许用户配置 iKVM 控制台上的安全性设置。用户可以建立一个屏幕保护程序模式，如果在指定延迟时间内始终未使用控制台，则启用该模式。一旦启用，控制台将保持锁定状态，直到按下任一键或移动鼠标后为止。输入屏幕保护程序密码可继续操作。

在**"Security"（安全性）**对话框中，可使用密码保护锁定控制台，设置或更改密码，或启用屏幕保护程序。

注： 如果丢失或忘记了 iKVM 密码，可使用 CMC Web 界面或 RACADM 将其重设为 iKVM 出厂默认值。请参阅"清除丢失或忘记的密码"。

访问"Security"（安全性）对话框

1. 按下 <Print Screen>。随即显示**"Main"（主菜单）**对话框。
2. 单击**"Setup"（设置）**，然后单击**"Security"（安全性）**。**"Security"（安全性）**对话框会出现。

设置或更改密码

1. 单击并按下 <Enter> 或双击**"New"（新建）**字段。
2. 在**"New"（新建）**字段中键入新密码，然后按下 <Enter>。密码有大小写之分并要求为 5-12 个字符。密码必须至少包含一个字母和一个数字。合法字符为：A-Z、a-z、0-9、空格和连字符。
3. 在**"Repeat"（重复）**字段中，再次键入该密码，然后按下 <Enter>。
4. 如果只想要更改密码，则单击**"OK"（确定）**，然后关闭对话框。

为控制台提供密码保护

1. 按照上述步骤中的说明设置密码。
2. 选择**"Enable Screen Saver"（启用屏幕保护程序）**框。
3. 键入延迟密码保护和屏幕保护程序激活的**"Inactivity Time"（非活动时间）**的分钟数（从 1 到 99）。
4. 对于**"Mode"（模式）**：如果显示器符合 ENERGY STAR，则选择**"Energy"（能量）**；否则，选择**"Screen"（屏幕）**。

   注： 如果模式设置为**"Energy"（能量）**，则设备将使显示器进入睡眠模式。这通常以显示器关机和琥珀色灯光取代绿色电源 LED 表示。如果模式设置为**"Screen"（屏幕）**，则在检测过程中 OSCAR 标志会在屏幕上跳动。检测开始之前，警告弹出框会显示以下信息："Engery 模式可能会损坏非 ENERGY STAR 类型的显示器。但是，一旦开始，可通过鼠标或键盘干涉立刻放弃检测。"

小心： 对非 Energy Star 类型的显示器使用 Energy 模式可能导致显示器损坏。

5. 可选项：要启动屏幕保护程序检测，单击**"Test"（检测）**。**"Screen Saver Test"（屏幕保护程序检测）**对话框会出现。单击**"OK"（确定）**开始检测。

   检测需要 10 秒钟。检测结束时，将返回到**"Security"（安全性）**对话框。

登录

1. 按下 <Print Screen> 启动 OSCAR。**"Password"（密码）**对话框会出现。
2. 键入密码并单击**"OK"（确定）**。随即显示**"Main"（主菜单）**对话框。

设置自动注销

您可以将 OSCAR 设置为一段非活动时期后自动从服务器注销。

1. 在**"Main"（主菜单）**对话框中，单击**"Setup"（设置）**，然后单击**"Security"（安全性）**。
2. 在**"Inactivity Time"（非活动时间）**字段中，输入希望在自动断开连接前要与服务器保持连接的时间长短。
3. 单击**"OK"（确定）**。

从控制台删除密码保护

1. 从**"Main"（主菜单）**对话框，单击**"Setup"（设置）**，然后单击**"Security"（安全性）**。
2. 在**"Security"（安全性）**对话框中，单击并按下 <Enter>，或双击**"New"（新建）**字段。
3. 让**"New"（新建）**字段保持空白，按下 <Enter>。
4. 单击并按下 <Enter>，或双击**"Repeat"（重复）**字段。

5. 让**"Repeat"（重复）**字段保持空白，按下 <Enter>。

6. 如果只想删除密码，单击**"OK"（确定）**。

启用无密码保护的屏幕保护程序模式

注： 如果控制台有密码保护，必须先删除密码保护。请先执行上述过程的步骤，然后再执行以下步骤。

1. 选择**"Enable Screen Saver"（启用屏幕保护程序）**。

2. 键入将屏幕保护程序延迟激活的分钟数（1 到 99）。

3. 如果显示器为 ENERGY STAR 类型，选择**"Energy"（能量）**；否则，选择**"Screen"（屏幕）**。

小心： 对非 Energy Star 类型的显示器使用 Energy 模式可能导致显示器损坏。

4. 可选项：要启动屏幕保护程序检测，单击**"Test"（检测）**。**"Screen Saver Test"（屏幕保护程序检测）**对话框会出现。单击**"OK"（确定）**开始检测。

   检测需要 10 秒钟。检测结束时，将返回到**"Security"（安全性）**对话框。

   注： 启用屏幕保护程序模式将使用户从服务器断开连接；不选择任何服务器。状况标志显示为可用。

退出屏幕保护程序模式

要退出屏幕保护程序模式并返回到**"Main"（主菜单）**对话框，按下任意键或移动鼠标。

要关闭屏幕保护程序：

1. 在**"Security"（安全性）**对话框中，清除**"Enable Screen Saver"（启用屏幕保护程序）**框。

2. 单击**"OK"（确定）**。

要立刻打开屏幕保护程序，按下 <Print Screen>，然后按下 <Pause>。

清除丢失或忘记的密码

当丢失或忘记了 iKVM 密码时，可将其重设为 iKVM 出厂默认值，然后更改密码。可使用 CMC Web 界面或 RACADM 重设密码。

要使用 CMC Web 界面重设丢失或忘记的 iKVM 密码：

1. 登录 CMC Web 界面。

2. 从机箱子菜单中选择**iKVM**。

3. 单击**"Setup"（设置）**选项卡。显示 **iKVM Configuration（iKVM 配置）**页面。

4. 单击**"Restore Default Values"（恢复默认值）**。

然后可使用 OSCAR 从默认值更改密码。请参阅"设置或更改密码"。

要使用 RACADM 重设丢失或忘记的密码，打开一个至 CMC 的串行/远程登录/SSH 文本控制台，登录并键入：

```
racadm racresetcfg -m kvm
```

注： 如果与默认值不同，则使用 **racresetcfg** 命令重设"Front Panel Enable"（前面板启用）和"Dell CMC Console Enable"（Dell CMC 控制台启用）设置。

有关 **racresetcfg** 子命令的详情，请参阅*《Dell Chassis Management Controller 管理员参考指南》*中的 racresetcfg 部分。

更改语言

使用**"Language"（语言）**对话框更改 OSCAR 文本以任何支持语言的显示。所有 OSCAR 屏幕上的文本会立刻更改为所选语言。

要更改 OSCAR 语言：

1. 按下 <Print Screen>。随即显示**"Main"（主菜单）**对话框。
2. 单击**"Setup"（设置）**，然后单击**"Language"（语言）**。**"Language"（语言）**对话框会出现。
3. 单击所需语言的单选按钮，然后单击**"OK"（确定）**。

显示版本信息

使用**"Version"（版本）**对话框显示 iKVM 固件和硬件版本，并识别语言和键盘配置。

要显示版本信息：

1. 按下 <Print Screen>。随即显示**"Main"（主菜单）**对话框。
2. 单击**"Command"（命令）**，然后单击**"Display Versions"（显示版本）**。**"Version"（版本）**对话框会出现。

   "Version"（版本）对话框的上半部分会列出设备中的子系统版本。
3. 单击 ☒ 或按下 <Esc> 关闭**"Version"（版本）**对话框。

扫描系统

在扫描模式中，iKVM 自动对逐个插槽（逐个服务器）进行扫描。通过指定要扫描的服务器和每个服务器的显示秒数，可扫描多达 16 个服务器。

要将服务器添加到扫描列表中：

1. 按下 <Print Screen>。随即显示**"Main"（主菜单）**对话框。
2. 单击**"Setup"（设置）**，然后单击**"Scan"（扫描）**。**"Scan"（扫描）**对话框会出现，列出机箱中的所有服务器。
3. 选择要扫描服务器旁边的框。

   或

   双击该服务器名称或插槽。

   或

   按下 <Alt > 和希望扫描的服务器编号。可选择多达 16 个服务器。
4. 在**"Time"（时间）**字段中，输入希望 iKVM 在扫描移动到序列中下个服务器之前将等待的秒数（3 到 99）。
5. 单击**"Add/Remove"（添加/删除）**按钮，然后单击**"OK"（确定）**。

要从**"Scan"（扫描）**列表中删除一个服务器：

1. 在**"Scan"（扫描）**对话框中，选择要删除的服务器旁边的框。

   或

   双击该服务器名称或插槽。

   或

   单击**"Clear"（清除）**按钮从**"Scan"（扫描）**列表中删除所有服务器。
2. 单击**"Add/Remove"（添加/删除）**按钮，然后单击**"OK"（确定）**。

要启动扫描模式：

1. 按下 <Print Screen>。随即显示**"Main"（主菜单）**对话框。
2. 单击**"Commands"（命令）**。**"Command"（命令）**对话框会出现。
3. 选择**"Scan Enable"（扫描启用）**框。

4. 单击**"OK"（确定）**。会出现一条鼠标和键盘均已重设的信息。

5. 单击 关闭该信息框。

要取消扫描模式：

1. 如果 OSCAR 打开且**"Main"（主菜单）**对话框已显示，选择列表中的一个服务器。

   或

   如果 OSCAR *未*打开，移动鼠标或按下键盘上的任一键。扫描停止在当前所选服务器处。

   或

   按下 <Print Screen>。**"Main"（主菜单）**对话框会出现；选择列表中的一个服务器。

2. 单击**"Commands"（命令）**按钮。**"Commands"（命令）**对话框会出现。

3. 清除**"Scan Enable"（扫描启用）**方框。

广播至服务器

您可以同时控制系统中的多个服务器，确保全部所选服务器都接受相同的输入。您可以选择自行广播击键操作和/或鼠标移动。

注： 一次可广播多达 16 个服务器。

要广播至服务器：

1. 按下 <Print Screen>。随即显示**"Main"（主菜单）**对话框。

2. 单击**"Setup"（设置）**，然后单击**"Broadcast"（广播）**。**"Broadcast"（广播）**对话框会出现。

   注： 广播击键操作：当使用击键操作时，接收一个要给予相同解释的击键操作广播的所有服务器的键盘状态必须相同。具体说，所有键盘上的 <Caps Lock> 和 <Num Lock> 模式必须相同。当 iKVM 尝试向所选服务器同时发送击键操作时，某些服务器可能会禁止并进而延迟传输。

   注： 广播鼠标移动：要使鼠标准确工作，所有服务器必须具有相同的鼠标驱动程序、桌面（如一致放置的图标）和视频分辨率。鼠标在所有屏幕上也必须完全处于相同位置。由于这些条件很难实现，所以向多个服务器广播鼠标移动可能会导致不可预测的结果。

3. 通过选择方框启用要接收广播命令的服务器的鼠标和/或键盘。

   或

   按上下箭头键使鼠标移动到一个目标服务器。然后按下 <Alt><K> 选择键盘框和/或按下 <Alt><M> 选择鼠标框。对其他服务器重复这一操作。

4. 单击**"OK"（确定）**保存设置并返回到**"Setup"（设置）**对话框。单击 或按下 <Escape> 返回到**"Main"（主菜单）**对话框。

5. 单击**"Commands"（命令）**。**"Commands"（命令）**对话框会出现。

6. 单击**"Broadcast Enable"（广播启用）**框激活广播。**"Broadcast Warning"（广播警告）**对话框会出现。

7. 单击"O**K"（确定）**启用广播。

   要取消并返回到**"Commands"（命令）**对话框，请单击 或按下 <Esc>。

8. 如果已启用广播，键入要从 Management Station 广播的信息和/或执行要从 Management Station 广播的鼠标运动。只有列表中的服务器可以访问。

要关闭广播：

从**"Commands"（命令）**对话框，清除**"Broadcast Enable"（广播启用）**框。

从 CMC 管理 iKVM

启用或禁用前面板

要使用 RACADM 启用或禁用从前面板对 iKVM 的访问功能，打开一个至 CMC 的串行/远程登录/SSH 文本控制台，登录并键入：

```
racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable <值>
```

其中，<*值*> 为 1（启用）或 0（禁用）。

有关 **config** 子命令的详情，请参阅《*Dell Chassis Management Controller 管理员参考指南*》中的 config 命令部分。

要使用 Web 界面启用或禁用从前面板对 iKVM 的访问功能：

1. 登录 CMC Web 界面。
2. 选择系统树中的 iKVM。随即显示 **iKVM Status（iKVM 状态）**页面。
3. 单击**"Setup"（设置）**选项卡。显示 **iKVM Configuration（iKVM 配置）**页面。
4. 要启用，选择**"Front Panel USB/Video Enabled"（已启用前面板 USB/视频）**复选框。

   要禁用，清除**"Front Panel USB/Video Enabled"（已启用前面板 USB/视频）**复选框。
5. 单击 **Apply（应用）**以保存设置。

通过 iKVM 启用 Dell CMC 控制台

要使用 RACADM 启用 iKVM 对 Dell CMC 控制台的访问功能，打开一个至 CMC 的串行/远程登录/SSH 文本控制台，登录并键入：

```
racadm config -g cfgKVMInfo -o cfgKVMAccessToCMCEnable 1
```

要使用 Web 界面启用 Dell CMC 控制台：

1. 登录 CMC Web 界面。
2. 选择系统树中的 iKVM。随即显示 **iKVM Status（iKVM 状态）**页面。
3. 单击**"Setup"（设置）**选项卡。显示 **iKVM Configuration（iKVM 配置）**页面。
4. 选择**"Allow access to CMC CLI from iKVM"（允许从 iKVM 访问 CMC CLI）**复选框。
5. 单击 **Apply（应用）**以保存设置。

查看 iKVM 状况和属性

Dell M1000e 服务器机箱的本地访问 KVM 模块称为 Avocent 集成 KVM 交换机模块，或 iKVM。与机箱相关联的 iKVM 的运行状况可以在**"Chassis Graphics"（机箱图形）**部分的**"Chassis Properties Health"（机箱属性运行状况）**页中查看。

要使用**"Chassis Graphics"（机箱图形）**查看 iKVM 的运行状况：

1. 登录 CMC Web 界面。
2. 将显示**"Chassis Status"（机箱状态）**页。**"Chassis Graphics"（机箱图形）**的右侧部分描述机箱的后视图并包含 iKVM 的运行状况。iKVM 运行状况以 iKVM 子图形的颜色表示：
   - 绿色 — iKVM 存在，电源打开并且正在与 CMC 通信；这表示不存在不利条件。
   - 琥珀色 — iKVM 存在，但电源可能未打开，或者可能无法与 CMC 通信；可能存在不利条件。
   - 灰色 — iKVM 存在且电源未打开。它当前未与 CMC 通信且不存在不利条件。
3. 将光标停留在 iKVM 子图形上方将显示相应的文本提示或屏幕提示。文本提示提供有关该 iKVM 的其它信息。
4. iKVM 子图形是到相应 CMC GUI 页的超链接，以便立即导航到**"iKVM Status"（iKVM 状态）**页。

有关 iKVM 的详情，请参阅"使用 iKVM 模块"。

要使用**"iKVM Status"（iKVM 状态）**页查看 iKVM 的状态：

1. 登录 CMC Web 界面。

2. 选择系统树中的 **iKVM**。随即显示 **iKVM Status**（iKVM 状态）页面。

表 10-5. iKVM 状态信息

项目	说明
"Presence"（存在）	显示 iKVM 模块是**"Present"（存在）**还是**"Absent"（不存在）**。
"Power State"（电源状态）	显示 iKVM 的电源状态：**"On"（开）**、**"Off"（关）**或**"N/A"（不可用）**（不存在）。
"Name"（名称）	显示 iKVM 的产品名称。
"Manufacturer"（制造商）	显示 iKVM 的制造商。
"Part Number"（部件号）	显示 iKVM 的部件号。部件号是供应商提供的唯一标识符。
"Firmware Version"（固件版本）	显示 iKVM 的固件版本。
"Hardware Version"（硬件版本）	显示 iKVM 的硬件版本。
"Front Panel Connected"（前面板已连接）	显示显示器是否**已连接**至前面板 VGA 连接器（**"Yes"[是]**或**"No"[否]**）。系统将该信息提供给 CMC，这样 CMC 可以确定是否有本地用户通过前面板访问机箱。
"Rear Panel Connected"（后面板已连接）	指示显示器是否**已 连接**至后面板 VGA 连接器（**"Yes"[是]**或**"No"[否]**）。系统将该信息提供给 CMC，这样 CMC 可以确定是否有本地用户通过后面板访问机箱。
"Tiering Port Connected"（分层端口已连接）	iKVM 支持使用内置硬件从 Dell 和 Avocent 无缝层接外部 KVM 设备。如 iKVM 已分层，可以通过外部 KVM 交换机（ iKVM 从该交换机分层）的屏幕显示器访问机箱中的服务器。
"Front Panel USB/Video Enabled"（前面板 USB/视频已启用）	显示是否已启用前面板 VGA 连接器（**"Yes"[是]** 或"No"[否]）。
"Allow access to CMC from iKVM"（允许从 iKVM 访问 CMC）	指示是否已通过 iKVM 启用 CMC 命令（**"Yes"[是]** 或"No"[否]）。

更新 iKVM 固件

可使用 CMC Web 界面或 RACADM 更新 iKVM 固件。

要使用 CMC Web 界面更新 iKVM 固件：

1. 登录 CMC Web 界面。
2. 单击系统树中的**"Chassis"（机箱）**。
3. 单击 **"Update"（更新）**选项卡。**"Updatable Components"（可更新组件）**页会显示。
4. 单击 iKVM 名称。显示**"Firmware Update"（固件更新）**页面。
5. 在**"Firmware Image"（固件映像）**字段中，在 management station 或共享网络上输入固件映像文件的路径，或单击**"Browse"（浏览）**导航到文件位置。

注： 默认 iKVM 固件映像名是 i**kvm.bin**；但用户可以更改 iKVM 固件映像名。

6. 单击**"Begin Firmware Update"（开始固件更新）**。将显示一个对话框，要求您确认该操作。
7. 单击 **Yes**（是）以继续。在**"Firmware Update Progress"（固件更新过程）**部分提供固件更新状态信息。当上载映像时，页面上将显示状态指示灯。文件传输时间根据连接速度而显著不同。当内部更新过程开始时，将自动刷新页面并显示固件更新计时器。其它注意事项：
   - 在文传输过程中，请勿使用**"Refresh"（刷新）**按钮或导航到其它页。
   - 要取消进程，请单击**"Cancel File Transfer and Update"（取消文件传输和更新）** — 该选项仅可在文件传输过程中可用。
   - 更新状态显示在**"Update State"（更新状态）**字段中；在文件传输过程中将自动更新该字段。某些版本较低的浏览器不支持这些自动更新。要手动刷新**"Update State"（更新状态）**字段，请单击**"Refresh"（刷新）**。

注： 更新 iKVM 大约最多需要一分钟。

当更新完成时，iKVM 将重设且更新的新固件将显示在**"Updatable Components"（可更新组件）**页。

要使用 RACADM 更新 iKVM 固件，打开一个至 CMC 的 串行/远程登录/SSH 文本控制台，登录并键入：

```
racadm fwupdate -g -u -a <TFTP 服务器 IP 地址或 FQDN> -d <文件路径/文件名> -m kvm
```

例如：

```
racadm fwupdate -gua 192.168.0.10 -d ikvm.bin -m kvm
```

有关 **fwupdate** 子命令的详情，请参阅《*Dell Chassis Management Controller 管理员参考指南*》中的 **fwupdate** 命令部分。

故障排除

注： 如果有活动控制台重定向会话并且 iKVM 连接了较低分辨率的显示器，在本地控制台选择了服务器的情况下，可能会重设服务器控制台分辨率。如果服务器运行 Linux 操作系统，本地显示器上可能无法查看 X11 控制台。在 iKVM 上按 <Ctrl><Alt><F1> 会将 Linux 切换为文本控制台。

表 10-6. iKVM 故障排除

问题	可能原因和解决方案
连接到前面板的显示器上显示 "User has been disabled by CMC control"（用户已被 CMC 控制禁用）信息。	前面板连接已被 CMC 禁用。 可以使用 CMC Web 界面或 RACADM 启用前面板。 要使用 Web 界面启用前面板： 1. 登录 CMC Web 界面。 2. 选择系统树中的 iKVM。 3. 单击**"Setup"（设置）**选项卡。 4. 选择**"Front Panel USB/Video Enabled"（已启用前面板 USB/视频）**复选框。 5. 单击 **Apply（应用）**以保存设置。 要使用 RACADM 启用前面板，打开一个至 CMC 的串行/远程登录/SSH 文本控制台，登录并键入： `racadm config -g cfgKVMInfo -o cfgKVMAccesToCMCEnable 1`。
后面板访问不起作用。	前面板设置已被 CMC 启用，且有一个显示器当前正连接到前面板。 每次只允许有一个连接。前面板连接优先于 ACI 和后面板。有关连接优先顺序的详情，请参阅"iKVM 连接优先次序"。
连接到后面板的显示器上会出现"User has been disabled as another appliance is currently tiered"（用户已被禁用，因为另一个设备当前被分层）信息。	网络电缆已连接到 iKVM ACI 端口连接器和次 KVM 设备。 每次只允许有一个连接。ACI 分层连接优先于后面板显示器连接。优先次序为前面板、ACI，然后是后面板。
iKVM 的琥珀色 LED 指示灯正在闪烁。	有三种可能原因： **iKVM 出现了问题**，需要重新编程。要修复此问题，请遵照 iKVM 固件更新说明操作（请参阅"更新 iKVM 固件"）。 **iKVM 正在重新编程 CMC 控制台界面。**在这种情况下，CMC 控制台暂时不可用并由 OSCAR 界面中的一个黄点表示。此过程最多需要 15 分钟。 **iKVM 固件检测到一个硬件错误。**有关的其他信息，请查看 iKVM 状况。 要使用 Web 界面查看 iKVM 状况： 1. 登录 CMC Web 界面。 2. 选择系统树中的 iKVM。 要使用 RACADM 查看 iKVM 状况，打开一个至 CMC 的串行/远程登录/SSH 文本控制台，登录并键入： `racadm getkvminfo`
我的 iKVM 通过 ACI 端口分层到外部 KVM 交换机，但是 ACI 连接的所有条目都不可用。 所有状态都在 OSCAR 界面中显示一个黄点。	前面板连接已启用并已连接一个显示器。因为前面板优先于所有其他 iKVM 连接，所以 ACI 和后面板连接器均被禁用。 要启用 ACI 端口连接，必须先禁用前面板访问或卸下连接到前面板的显示器。外部 KVM 交换机 OSCAR 条目将变成活动和可访问。 要使用 Web 界面禁用前面板： 1. 登录 CMC Web 界面。 2. 选择系统树中的 iKVM。 3. 单击**"Setup"（设置）**选项卡。 4. 清除（取消勾选）**"Front Panel USB/Video Enabled"（已启用前面板 USB/视频）**复选框。 5. 单击 **Apply（应用）**以保存设置。 要使用 RACADM 禁用前面板，打开一个至 CMC 的串行/远程登录/SSH 文本控制台，登录并键入： `racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable 0`
在 OSCAR 菜单中，Dell CMC 连接显示一个红色 X，我无法连接到 CMC。	有两种可能原因：

	Dell CMC 控制台已被禁用。在这种情况下，可使用 CMC Web 界面或 RACADM 启用它。 要使用 Web 界面启用 Dell CMC 控制台： 1. 登录 CMC Web 界面。 2. 选择系统树中的 **iKVM**。 3. 单击**"Setup"（设置）**选项卡。 4. 选择**"Allow access to CMC CLI from iKVM"（允许从 iKVM 访问 CMC CLI）**复选框。 5. 单击 **Apply（应用）**以保存设置。 要使用 RACADM 启用 Dell CMC 连接，打开一个至 CMC 的串行/远程登录/SSH 文本控制台，登录并键入： `racadm config -g cfgKVMInfo -o cfgKVMAccessToCMCEnable 1` **CMC 不可用，因为它正在初始化、正在切换到待机 CMC 或正在重新编程。**在这种情况下，只需等待 CMC 完成初始化即可。
一个服务器的插槽名称在 OSCAR 中显示为 "正在初始化"，我无法选择它。	服务器正在初始化或该服务器上的 iDRAC 初始化失败。 首先，等待 60 秒钟。如果服务器仍在进行初始化，则初始化一完成就会显示插槽名称，您可以选择服务器。 如果经过 60 秒钟后，OSCAR 仍表示插槽正在初始化，则应卸下服务器，然后将服务器重新插入机箱。此操作允许 iDRAC 重新初始化。

目录

目录

安装和设置 CMC

Dell Chassis Management Controller Firmware 版本 3.0 用户指南

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 并引导您完成随后的 CMC 配置步骤：

- 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 环境的详情，请参阅 "理解冗余 CMC 环境"。

开始之前

在开始设置 CMC 环境之前，请首先从 Dell 支持网站 **support.dell.com** 下载 CMC 固件的最新版本。

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 在机箱上预安装，因此无需安装。可以安装第二个 CMC 作为活动 CMC 的后备。有关使用待机 CMC 的详情，请参阅"理解冗余 CMC 环境"。

机箱集成一览表

使用以下步骤可准确设置机箱：

1. CMC 与使用浏览器的 management station 必须位于相同的网络中，即管理网络。用电缆将标有 **GB** 的 CMC 以太网端口连接到管理网络。

   注： 不要将电缆插入标有 **STK** 的 CMC 以太网端口。有关用电缆连接 STK 端口的详情，请参阅 "理解冗余 CMC 环境"。

2. 对于机架机箱，在机箱中安装 IO 模块并用电缆互相连接。
3. 在机箱中插入服务器。
4. 连接机箱到电源。
5. 在完成 步骤 7 后按下机箱旁的电源按钮，或者从 CMC GUI 使机箱开机。

   注： 不要使服务器开机。

6. 使用系统前端的 LCD 面板，为 CMC 提供静态 IP 地址或配置为 DHCP。
7. 用默认用户名（root）和密码（calvin）通过网络浏览器连接到 CMC IP 地址。
8. 在 CMC GUI 中为每个 iDRAC 提供一个 IP 地址并启用 LAN 和 IPMI 接口。

   注： 有些服务器上的 iDRAC LAN 接口默认禁用。

9. 在 CMC GUI 中为每个 IO 模块提供一个 IP 地址。
10. 通过网络浏览器连接到各 iDRAC 并提供 iDRAC 的最终配置。默认用户名是 root，密码是 calvin。

11. 通过网络浏览器连接到各 IO 模块并提供 IO 模块的最终配置。

12. 给服务器供电并安装操作系统。

基本 CMC 网络连接

为了提供最高的冗余度，请将每个 CMC 连接到您的管理网络。如果机箱只有一个 CMC，请建立一个到管理网络的连接。如果机箱有冗余 CMC，则建立两个到管理网络的连接。

每个 CMC 包含两个 RJ-45 以太网端口，分别标记为 **GB**（*上行*端口）和 **STK** （*堆栈*或电缆合并端口）。通过基本布线，您可以将 GB 端口连接到管理网络并保留不使用 STK 端口。

△ **小心： 将 STK 端口连接到管理网络会出现无法预测的结果。用电缆连接 GB 和 STK 到相同网络（广播域）会引发广播风暴。**

菊花链式 CMC 网络连接

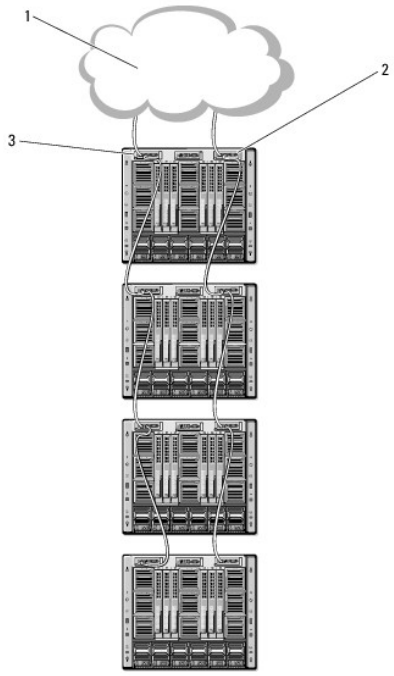
如果机架中有多个机箱，可以通过将四个机箱以菊花链式连接起来以减少到管理网络的连接数量。如果四个机箱中的每一个都包含冗余 CMC，则通过菊花链式连接，您可以将管理网络必要连接数从八个减少到两个。如果每个机箱只有一个 CMC，则您可以将必要连接数从四个减少到一个。

当采用菊花链式机箱连接时，GB 是"上行"端口，而 STK 是"堆栈"（电缆合并）端口。连接 GB 端口到管理网络或到更接近网络的机箱中 CMC 的 STK 端口。必须仅连接 STK 端口到 GB 端口才能扩展链或网络。

在活动的 CMC 插槽和第二 CMC 插槽中为 CMC 创建单独的链。

图 2-1 说明了四个采用菊花链式连接的机箱的电缆布线，每个都有活动和待机 CMC。

图 2-1. 菊花链式 CMC 网络连接



1	管理网络	2	待机 CMC
3	活动 CMC		

图 2-2、图 2-3 和 图 2-4 显示了 CMC 的**错误**布线示例。

图 2-2. CMC 网络连接布线错误 - 2 个 CMC

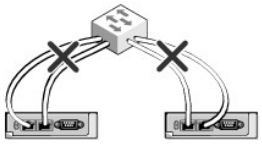


图 2-3. CMC 网络连接布线错误 - 单个 CMC

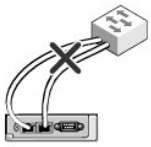
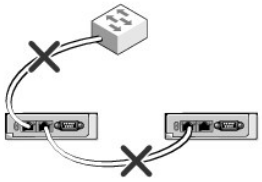


图 2-4. CMC 网络连接布线错误 - 2 个 CMC



执行以下步骤将四个机箱以菊花链式连接：

1. 将第一个机箱活动 CMC 的 GB 端口连接到管理网络。
2. 将第二个机箱活动 CMC 的 GB 端口连接到第一个机箱活动 CMC 的 STK 端口。
3. 如果有第三个机箱，请将其活动 CMC 的 GB 端口连接到第二个机箱活动 CMC 的 STK 端口。
4. 如果有第四个机箱，请将其活动 CMC 的 GB 端口连接到第三个机箱的 STK 端口。
5. 如果机箱中有冗余 CMC，请使用相同的方式进行连接。

小心： 任何 CMC 上的 STK 端口都决不能连接到管理网络。它只能连接到其它机箱的 GB 端口。将 STK 端口连接到管理网络会破坏网络并导致数据丢失。用电缆连接 GB 和 STK 到相同网络（广播域）会引发广播风暴。

注： 绝不要连接活动 CMC 到待机 CMC。

注： 重设 STK 端口链接至另一个 CMC 的 CMC 可能会中断链接后面 CMC 的网络。子 CMC 可能会记录信息表明网络连接已掉失，且它们可能故障切换到冗余 CMC。

要开始使用 CMC，请参阅 "在 Management Station 上安装远程访问软件"。

在 Management Station 上安装远程访问软件

可使用远程访问软件从 Management Station 访问 CMC，例如远程登录、Secure Shell (SSH) 或操作系统上提供的串行控制台实用程序或使用 Web 界面。

若要从管理工作站使用远程 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 上或 **support.dell.com/manuals** 提供的《*Dell OpenManage 安装和安全性用户指南*》。可以从 Dell 支持网站 **support.dell.com** 下载 Dell DRAC Tools 的最新版本。

在 Linux Management Station 上安装 RACADM

1. 以 root 身份登录至运行支持的 Red Hat Enterprise Linux 或 SUSE Linux Enterprise Server 操作系统的系统，以在该系统中安装 Managed System 组件。
2. 将 *Dell Systems Management Tools and Documentation DVD* 插入 DVD 驱动器中。
3. 若要将 DVD 安装到所需位置，则使用 `mount` 命令或类似命令。

   注： 在 Red Hat Enterprise Linux 5 操作系统上，DVD 会由 `-noexec mount` 选项自动安装。此选项不允许您从 DVD 上运行任何可执行文件。需要手动安装 DVD-ROM，然后运行可执行文件。

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. 要获得 RACADM 命令的帮助，请在运行前面的命令后键入 `racadm help`。有关使用 RACADM 的详情，请参阅"使用 RACADM 命令行界面"。

   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 <文件名>
   ```

有关远程 `racadm` 的详情，请参阅 "远程访问 RACADM" 和后续部分。

从 Linux Management Station 卸载 RACADM

1. 以 root 身份登录到要安装 Management Station 功能的系统上。
2. 使用以下 `rpm` 查询命令确定已安装的是哪个版本的 DRAC 工具：

   ```
   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

可以通过 Web 浏览器配置和管理 CMC 和服务器，以及安装在机箱中的模块。请在 Dell 支持网站 **support.dell.com/manuals** 参阅《*Dell 系统软件支持值表*》中的"*支持的浏览器*"一节。

CMC 与使用浏览器的 management station 必须位于相同的网络中，即*管理网络*。根据安全性要求，管理网络应该是隔离的、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 Web 浏览器访问 CMC。

一些浏览器功能会干扰连接或性能，特别是当管理网络没有到 Internet 的路由时。如果 management station 运行在 Windows 操作系统上，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时也会如此。

代理服务器

如果使用无法访问管理网络的代理服务器浏览，可以将管理网络地址添加到浏览器的排除列表。这样可以使浏览器在访问管理网络时不经过代理服务器。

Internet Explorer

执行以下步骤编辑 Internet Explorer 中的排除列表：

1. 启动 Internet Explorer。

2. 单击**"Tools"（工具）→ "Internet Options"（Internet 选项）→ "Connections"（连接）**。
3. 在**"Local Area Network (LAN) settings"（局域网 [LAN] 设置）**部分，单击**"LAN Settings"（LAN 设置）**。
4. 在**"Proxy server"（代理服务器）**部分，单击**"Advanced"（高级）**。
5. 在**"Exceptions"（排除）**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 3.0 中编辑例外列表：

1. 启动 Mozilla Firefox。
2. 单击**"Tools"（工具）→"Options"（选项）**(Windows) 或单击**"Edit"（编辑）→"Preferences"（首选项）**(Linux)**。**
3. 单击**"Advanced"（高级）**，然后单击**"Network"（网络）**选项卡。
4. 单击**"Settings"（设置）**。
5. 选择**"Manual proxy configuration"（手动代理配置）。**
6. 在**"No Proxy for"（不使用代理）**部分，将管理网络上的 CMC 和 iDRAC 地址输入到逗号分隔的列表。可以在条目中使用 DNS 名称和通配符。

Microsoft Phishing Filter

如果在管理系统的 Internet Explorer 7 上启用 Microsoft Phishing Filter 且 CMC 不能接入因特网，则到 CMC 的访问可能会延迟几秒钟。在使用浏览器或远程 RACADM 等其他接口时会发生这种延迟。执行以下步骤禁用 Phishing Filter：

1. 启动 Internet Explorer。
2. 单击**"Tools"（工具）→ Phishing Filter**，然后单击**"Phishing Filter Settings"（Phishing Filter 设置）**。
3. 选中**"Disable Phishing Filter"（禁用 Phishing Filter）**复选框。
4. 单击**"OK"（确定）**。

证书撤回列表 (CRL) 访存

如果 CMC 没有到因特网的路由，您应该禁用 Internet Explorer 中的证书撤回列表 (CRL) 访存功能。该功能检测服务器（诸如 CMC Web 服务器）是否正在使用位于因特网已撤回证书检索列表中的证书。如果无法访问 Internet，那么当您使用浏览器或如远程 RACADM 等命令行界面访问 CMC 时，该功能可能导致数秒钟的延迟。

执行以下步骤禁用 CRL 访存：

1. 启动 Internet Explorer。
2. 单击**"Tools"（工具）→ "Internet Options"（Internet 选项）**，然后单击 **"Advanced"（高级）**。
3. 滚动到"Security"（安全性）部分，并取消选取**"Check for publisher's certificate revocation"（检查钓鱼者证书撤回）**。
4. 单击**"OK"（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**"Do not save encrypted pages to disk"（请勿将加密页保存至磁盘）**选项未启用的问题。

请按照如下步骤启用**"Do not save encrypted pages to disk"（请勿将加密页保存至磁盘）**选项：

1. 启动 Internet Explorer。

2. 单击**"Tools"（工具）→ "Internet Options"（Internet 选项）**，然后单击 **"Advanced"（高级）**。

3. 滚动到"Security"（安全性）部分，并选中**"Do not save encrypted pages to disk"（不将加密的页存盘）**。

允许在 Internet Explorer 中播放动画

当把文件传输到 Web 界面和从 Web 界面传输文件时，将出现旋转的文件传输图标以表明传输活动。对于 Internet Explorer，该功能要求浏览器配置为能够播放动画，同时这也是默认设置。

执行以下步骤配置 Internet Explorer 允许播放动画：

1. 启动 Internet Explorer。

2. 单击**"Tools"（工具）→ "Internet Options"（Internet 选项）**，然后单击 **"Advanced"（高级）**。

3. 滚动到"Multimedia"（安全性）部分，并复选**"Play animations in web pages"（允许在网页中播放动画）**。

设置对 CMC 的初始访问

为远程管理 CMC，请将 CMC 连接到您的管理网络并配置 CMC 网络设置。

注： 若要管理 M1000e 解决方案，它必须连接到管理网络。

有关如何配置 CMC 网络设置的信息，请参阅 "配置 CMC 网络"。此初始配置分配启用对 CMC 进行访问的 TCP/IP 网络参数。

各服务器上的 CMC 和 iDRAC 以及所有交换机 I/O 模块上的网络管理端口连接到 M1000e 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。流量隔离对于机箱管理的不间断访问非常重要。

CMC 连接到管理网络。所有对 CMC 和 iDRAC 的访问都通过 CMC 完成。对受管服务器的访问则通过与输入/输出模块 (IOM) 的连接网络完成。这使应用程序网络能够与管理网络相互隔离。

注： 建议将机箱管理与数据网络隔离。Dell 不支持或保证您不正确集成的机箱的运行时间。由于数据网络的潜在流量，内部管理网络的管理接口会因服务器流量而饱和。这会导致 CMC 和 iDRAC 通信延迟。延迟会使机箱发生无法预测的行为，例如，即使 iDRAC 启动并在运行，CMC 也会将其显示为脱机，这又会导致其它不必要的行为。如果物理隔离管理网络的做法不切实际，可以将 CMC 和 iDRAC 通信分离到单独的 VLAN。CMC 和各个 iDRAC 网络接口可配置为使用 racadm setniccfg 命令的 VLAN。有关详情，请参阅 *《Dell Chassis Management Controller 管理员参考指南》*。

如果您有一个机箱，请将 CMC 和待机 CMC 连接到管理网络。如果有一个冗余 CMC，则使用另一条网络电缆并连接 **GB** CMC 端口到管理网络的第二个端口。

如果有多个机箱，您可以在基本连接（将每个 CMC 连接到管理网络）或菊花链式机箱连接（多个机箱串联起来，只有一个 CMC 连接到管理网络）中选择。基本连接类型使用管理网络上更多的端口，并提供更好的冗余。菊花链式连接类型使用管理网络上较少的端口，但增加了 CMC 间的相关性，降低了系统的冗余。

有关菊花链式连接的详情，请参阅 "菊花链式 CMC 网络连接"。

注： 不能在冗余配置中正确连接 CMC 的电缆会失去管理控制和引发广播风暴。

配置 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*为 CMC 配置初始网络设置，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，可以使用以下任意接口：

- 命令行界面 (CLI) 如串行控制台、远程登录、SSH 或通过 iKVM 连接的 Dell CMC 控制台
- 远程 RACADM
- 使用 CMC Web 界面

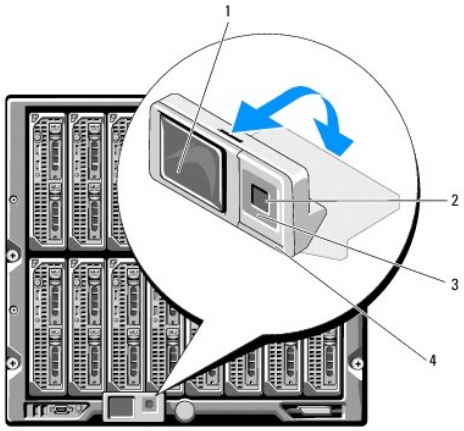
使用 LCD 配置向导配置网络

注： 只有当部署 CMC 或更改默认密码后使用 LCD 配置向导配置服务器的选项才可用。如果未更改密码，仍然可以使用 LCD 重新配置 CMC，但会可能导致安全风险。

LCD 位于机箱前方左下角。

图 2-5 图示说明了 LCD 面板。

图 2-5. LCD 显示屏



1	LCD 屏幕	2	选择（"选中"）按钮
3	滚动按钮（4 个）	4	状况标志 LED

LCD 屏幕显示菜单、图标、图像和信息。

LCD 面板上的状况标志 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。

在 LCD 屏幕中导航

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。使用配置向导过程中的任意时刻，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。

有关使用 LCD 面板的详细信息，请参阅《*Dell Chassis Management Controller 管理员参考指南*》中的 LCD 面板部分。

使用 LCD 配置向导

1. 如果尚未开机，请按下机箱电源按钮开机。

   通电时，LCD 屏幕将显示一系列初始化屏幕。就绪后，将显示**语言设置**屏幕。

2. 使用箭头按钮选择语言，然后按下中央按钮以选择**"Accept/Yes"（接受/是）**，并再次按下中央按钮。

3. **机柜**屏幕显示以下问题：**"Configure Enclosure?"（是否配置机柜？）**

   a. 按下中央按钮继续到**"CMC Network Settings"（CMC 网络设置）**屏幕。请参阅步骤 4。

   b. 要退出**"Configure Enclosure"（配置机柜）**菜单，请选择"No"（否）图标并按下中央按钮。请参阅步骤 9。

4. 按下中央按钮继续到**"CMC Network Settings"（CMC 网络设置）**屏幕。

5. 使用向下箭头按钮选择网络速度（10Mbps、100Mbps、自动 [1Gbps]）。

注： "Network Speed"（网络速度）设置必须同有效网络吞吐量的网络配置相匹配。将"Network Speed"（网络速度）设置为低于网络配置的速度会增加带宽消耗，并使网络通信变慢。**确定您的网络是否支持以上网络速度并进行相应设置。**如果您的网络配置与这些值的任何一个均不匹配，Dell 建议使用"Auto Negotiation"（自动协商）（**"Auto"（自动）**选项）或咨询您的网络设备制造商。

按下中央按钮继续到下一个**"CMC Network Settings"（CMC 网络设置）**屏幕。

6. 选择匹配网络环境的双工模式（半双工或全双工）。

注： 如果"Auto Negotiation"（自动协商）设置为"On"（开启）或选择 1000MB (1Gbps)，则网络速度和双工模式设置不可用。

注： 如果为一个设备打开了自动协商，但没有为另一个设备打开该协议，则使用自动协商的设备可以确定其它设备的网络速度，但不能确定双工模式；此时，双工模式将在自动协商期间默认为半双工设置。这种双工的不匹配会造成网络连接较慢。

按下中央按钮继续到下一个**"CMC Network Settings"（CMC 网络设置）**屏幕。

7. 选择要用于 CMC 的 Internet 协议（IPv4、IPv6 或两者）。

按下中央按钮继续到下一个**"CMC Network Settings"（CMC 网络设置）**屏幕。

8. 选择希望 CMC 以何种方式获得 NIC IP 地址：

动态主机配置协议	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 将得到网络中唯一的 IP 地址。如果已经选择了 DHCP 选项，请按下中央按钮。**"Configure iDRAC?"**（是否**配置 iDRAC？）**屏幕出现；转到 步骤 10。
静态	在随即出现的屏幕中手动输入 IP 地址、网关和子网掩码。 如果已经选择**"Static"（静态）**选项，请按下中央按钮继续到下一步 **CMC 网络设置**屏幕，然后： a. 通过使用向右或向左箭头键在位置间移动，并使用向上和向下箭头为每个位置选择编号来设置**"Static IP Address"（静态 IP 地址）**。当您已经完成**"Static IP Address"（静态 IP 地址）**设置后，按下中央按钮继续。 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。随即显示**"Network Summary"（网络摘要）**屏幕。 **"Network Summary"（网络摘要）**屏幕将列出已输入的**"Static IP Address"（静态 IP 地址）**、**"Subnet Mask"（子网掩码）**和**"Gateway"（网关）**设置。查看设置的准确性。要更正设置，可以导航至左侧箭头按钮，并按下中央键返回该设置屏幕。更正后，请按下中央按钮。 a. 当您已经确认了已输入设置的精确性后，请按中央按钮。随即将显示**" Register DNS?"（是否注册 DNS？）**屏幕。

注： 如果为 CMC IP 配置选择动态主机配置协议 (DHCP) 模式，则在默认情况下还将启用 DNS 注册。

9. 如果在上一步中选择了 **DHCP**，请转至步骤 8。

要注册 DNS 服务器的 IP 地址，按下中央按钮继续。如果没有 DNS，请按向右箭头键。随即将显示**" Register DNS?"（是否注册 DNS？）**屏幕将出现；转至步骤 10。

通过使用向右或向左箭头键在位置间移动，并使用向上和向下箭头为每个位置选择编号来设置**"DNS IP Address"（DNS IP 地址）**。当您已经完成"DNS IP Address"（DNS IP 地址）设置后，按下中央按钮继续。

10. 表明您是否希望配置 iDRAC：

- **否：**请跳至步骤 13。
- **是：** 请按下中央按钮继续。

也可从 CMC GUI 配置 iDRAC。

11. 选择要用于服务器的 Internet 协议（IPv4、IPv6 或两者）。

动态主机配置协议	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 将得到网络中唯一的 IP 地址。请按下中央按钮。
静态	在随即出现的屏幕中手动输入 IP 地址、网关和子网掩码。 如果已经选择**"Static"（静态）**选项，请按下中央按钮转到下一**"iDRAC Network Settings"（CMC 网络设置）**屏幕，然后： a. 通过使用向右或向左箭头键在位置间移动，并使用向上和向下箭头为每个位置选择编号来设置**"Static IP Address"（静态 IP 地址）**。此地址是第一个插槽中的 iDRAC 的静态 IP 地址。随着此 IP 地址的插槽号增加，将计算每个后续 iDRAC 的静态 IP 地址。当您已经完成**"Static IP Address"（静态 IP 地址）**设置后，按下中央按钮继续。 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。

a. 选择是**启用**还是**禁用** IPMI LAN 信道。请按下中央按钮继续。

b. 在**"iDRAC Configuration"（配置）**屏幕上，将所有 iDRAC 网络设置应用到安装的服务器，突出显示**"Accept/Yes"（接受/是）**图标并按中间按钮。如果不将

iDRAC 网络设置应用到安装的服务器，请突出显示**"No"（否）**图标并按下中央按钮，然后继续步骤 c。

c. 在下一个**"iDRAC Configuration"（配置）**屏幕上，将所有 iDRAC 网络设置应用到新安装的服务器，突出显示**"Accept/Yes"（接受/是）**图标并按中央按钮；如果将新服务器插入机箱，LCD 将提示用户是否使用之前配置的网络设置/策略自动部署服务器。如果不将 iDRAC 网络设置应用到新安装的服务器，请突出显示**"No"（否）**图标并按下中央按钮；如果新服务器插入机箱中，将不会配置 iDRAC 网络设置。

l. 在**"Enclosure"（机柜）** 屏幕上，要应用所有机柜设置，请突出显示**"Accept/Yes"（接受/是）**图标并按中央按钮。如不应用机柜设置，请突出显示**"No"（否）**图标并按中央按钮。

m. 在**"IP Summary"（IP 摘要）** 屏幕，检查您提供的 IP 地址以确保地址正确。要更正设置，可以导航至左侧箭头按钮，然后按下中央键返回该设置屏幕。更正后，请按下中央按钮。如果有必要，可以导航至右箭头按钮，然后按下中央键返回**"IP Summary"（IP 摘要）**屏幕。

当您确认输入的设置正确之后，按下中央按钮。配置向导将关闭并返回到**"Main Menu"（主菜单）**屏幕。

注： 如果您选择了**"Yes/Accept"（是/接受）**，在显示**"IP Summary"（IP 摘要）**屏幕之前，将显示**"Wait"（等待）**屏幕。

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、远程登录和 SSH 等 CLI 通过分配的 IP 地址访问 CMC。

注： 通过 LCD 配置向导完成网络设置后，该向导将不再可用。

通过网络访问 CMC

配置完 CMC 网络设置后，可以通过以下界面远程访问 CMC：

- Web 界面
- 远程登录控制台
- SSH
- 远程 RACADM

注： 因 Telnet 没有其他接口安全，所以默认禁用。启用使用 Web、ssh 或远程 RACADM 的 Telnet。

表 2-1. CMC 界面

接口	说明
Web 界面	提供了使用图形用户界面到 CMC 的远程访问。Web 界面构建在 CMC 固件中并从 Management Station 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 支持网站 **support.dell.com/manuals** 上的*《Dell 系统软件支持值表》*中的"支持的浏览器"一节。
远程 RACADM 命令行界面	使用命令行界面 (CLI) 从 Management Station 提供到 CMC 的远程访问。远程 RACADM 使用 **racadam -r** 选项加 CMC 的 IP 地址执行对 CMC 的命令。 有关远程 racadm 的详细信息，请参阅 "远程访问 RACADM" 和后续部分。
Telnet	通过网络提供对 CMC 的命令行访问。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 是一种以明文传送所有数据（包括密码）的非安全协议。发送敏感信息时，应使用 SSH 接口。
SSH	提供与远程登录相同的能力，同时使用加密传输层提高安全性。

注： CMC 默认用户名是 **root**，默认密码是 **calvin**。

可以使用支持的 Web 浏览器通过 CMC 网络接口访问 CMC 和 iDRAC Web 界面；还可以从 Dell Server Administrator 或 Dell OpenManage IT Assistant 启动该界面。

有关所支持 Web 浏览器的列表，请参阅 Dell 支持网站 **support.dell.com/manuals** 上的*《Dell 系统软件支持值表》*中的"支持的浏览器"一节。有关使用支持的 Web 浏览器访问 CMC 的信息，请参阅 "访问 CMC Web 界面"。有关 Dell OpenManage IT Assistant 的信息，请参阅 "在 Management Station 上安装远程访问软件"。

要使用 Dell Server Administrator 访问 CMC 界面，请启动 Management Station 上的 Server Administrator。从 Server Administrator 主页左窗格的系统树上，单击**"System"（系统）** →**"Main System Chassis"（主系统机箱）** →**Remote Access Controller**。有关详情，请参阅《*Dell Server Administrator 用户指南*》。

有关通过远程登录或 SSH 访问 CMC 命令行的信息，请参阅 "配置 CMC 使用命令行控制台"。

有关使用 RACADM 的详情，请参阅"使用 RACADM 命令行界面"。

有关使用 **connect** 或 **racadm connect** 命令连接服务器和 IO 模块的信息，请参阅 "使用 Connect 命令连接到服务器或 I/O 模块"。

安装或更新 CMC 固件

下载 CMC 固件

开始更新固件之前，请先从 Dell Support 网站 **support.dell.com** 下载最新固件并将该文件保存到本地系统。

CMC 固件包包含以下软件组件：

- 编译的 CMC 固件代码和数据
- Web 的界面、JPEG 和其它用户界面数据文件
- 默认配置文件

注： 在 CMC 固件更新期间，机箱中部分或所有风扇装置通常以 100% 速率旋转。

注： 按默认，固件更新将保留当前 CMC 设置。更新过程中，可以选择将 CMC 配置设置重设为出厂默认设置。

注： 如果机箱中安装了冗余 CMC，将两者都更新到相同的固件版本非常重要。如果 CMC 的固件版本不同将发生故障转移，可能发生不可预见的结果。

可使用 RACADM **getsysinfo** 命令（请参阅《*DellChassis Management Controller 管理员参考指南*》中的 **getsysinfo** 命令部分）或**"Chassis Summary"（机箱摘要）**页面（请参阅 "查看当前固件版本"），查看机箱中安装的 CMC 的当前固件版本。

如果有待机 CMC，建议通过一次操作同时更新两个 CMC。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。（请参阅《*Dell Chassis Management Controller 固件管理员参考指南*》中的 **cmcchangeover** 命令部分获得关于切换角色的帮助。）这允许您在更新第二个 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 恢复到以前的角色.CMC 固件版本 2.x 更新使用主要 CMC 和冗余 CMC，而不使用 **cmcchangeover** 命令。

使用 Web 界面更新 CMC 固件

有关使用 Web 界面更新 CMC 固件的说明，请参阅 "更新 CMC 固件"。

使用 RACADM 更新 CMC 固件

有关使用 RACADM **fwupdate** 子命令更新 CMC 固件的说明，请参阅《*Dell Chassis Management Controller 管理员参考指南*》中的 **fwupdate** 命令部分。

配置 CMC 属性

可以使用 Web 界面或 RACADM 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。

有关使用 Web 界面的详情，请参阅"访问 CMC Web 界面"。有关使用 RACADM 的详情，请参阅 "使用 RACADM 命令行界面"。

小心： 同时使用一个以上的 CMC 配置工具可能会产生意外的结果。

配置电源预算

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。

有关 CMC 电源管理的详情，请参阅 "电源管理"。

有关使用 Web 界面配置电源预算和其它电源设置的详情，请参阅 "配置电源预算"。

配置 CMC 网络设置

注： 更改 CMC 网络设置可能会断开当前网络连接。

可以使用以下配置工具中的一种配置 CMC 网络设置：

- RACADM — 有关详情，请参阅 "在多个机箱中配置多个 CMC"。

注： 如果准备在 Linux 环境中部署 CMC，请参阅 "在 Linux Management Station 上安装 RACADM"。

- Web 接口 — 有关详情，请参阅 "配置 CMC 网络属性"。

添加并配置用户

可以使用 RACADM 或 CMC Web 界面添加并配置 CMC 用户。还可以使用 Microsoft Active Directory 来管理用户。

有关使用 RACADM 为 CMC 添加和配置公共密钥用户的说明，请参阅 "使用 RACADM 配置通过 SSH 的公共密钥验证"。有关使用 Web 接口添加和配置用户的说明，请参阅 "添加和配置 CMC 用户"。

有关与 CMC 一同使用 Active Directory 的说明，请参阅 "使用 CMC 目录服务"。

添加 SNMP 和电子邮件警报

可以将 CMC 配置为发生某些机箱事件时生成 SNMP 或电子邮件警报。有关详情，请参阅"配置 SNMP 警报"和"配置电子邮件警报"。

配置远程系统日志

通过 CMC GUI 或 *racadm* 命令激活和配置**远程系统日志**功能。配置选项包括 CMC 转发日志条目时使用的系统日志服务器名称（或 IP 地址）和 UDP 端口。在配置中最多可以指定 3 个不同的系统日志服务器目标。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目标。

注： 由于在所转发日志条目的网络传输过程中采用 UDP，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已经被成功接收的反馈。

要配置 CMC 服务：

1. 登录 CMC Web 界面。
2. 单击**"Network"（网络）**选项卡。
3. 单击**"Services"（服务）**子选项卡。随即出现**"Services"（服务）**页。

有关配置远程系统日志的详情，请参阅表 5-56。

理解冗余 CMC 环境

如果活动 CMC 失败，可以安装待机 CMC 接替。冗余 CMC 可预先安装或随后添加。CMC 网络电缆连接正确对确保完全冗余或最佳性能至关重要。

故障转移发生在以下时候：

- 运行 RACADM **cmcchangeover** 命令。（请参阅《*Dell Chassis Management Controller* 管理员参考指南》中的 **cmcchangeover** 命令部分。）
- 在活动 CMC 上运行 RACADM **racreset** 命令。（请参阅《*Dell Chassis Management Controller* 管理员参考指南》中的 **racreset** 命令部分。）
- 从 Web 界面重设活动的 CMC。（请参阅**"Power Control Operations"（电源控制操作）**的**"Reset CMC"（重设 CMC）** 选项，如 "执行机箱电源控制操作"中所述。）
- 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 会话都将丢失。丢失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，并作为镜像维护。活动和待机 CMC 必须都安装相同的固件修订。如果固件修订不同，系统将报告已降级冗余。

待机 CMC 假定与活动 CMC 具有相同的设置和属性。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： 有关安装待机 CMC 的信息，请参阅 *硬件用户手册*。有关在待机 CMC 上安装 CMC 固件的说明，请遵照 "安装或更新 CMC 固件" 中的说明。

活动 CMC 自举过程

两个 CMC 插槽之间没有任何区别，插槽并不表明优先级。而首先安装或启动的 CMC 假定为活动 CMC 的角色。如果将 AC 电源应用于已安装的两个 CMC，安装在 CMC 机箱插槽 1（左侧）的 CMC 通常假定为活动角色。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。当协商完成时，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 运行状况的详情，请参阅 "查看机箱和组件摘要"。

目录

目录

I/O 结构管理

Dell Chassis Management Controller Firmware 版本 3.0 用户指南

机箱可以容纳六个输入/输出模块 (IOM)，每个模块都可以是直通或交换模块。

IOM 分为三个组 - A、B 和 C。每组有两个插槽 - 插槽 1 和插槽 2。插槽使用字母标记，自左至右，在机箱后侧：A1 | B1 | C1 | C2 | B2 | A2。每台服务器都有两个用于连接 IOM 的夹层插卡 (MC) 插槽。MC 和相应的 IOM 必须具备相同的结构。

机箱 IO 按照字母 A、B 和 C 分为 3 个独立的数据路径。这些路径称为"结构"并支持以太网、光纤通道或 InfiniBand。这些独立的结构路径分为 2 个 IO"组"：组 1 和组 2。每个服务器 IO 适配卡（夹层卡或 LOM）根据容量可有 2 或 4 个端口。这些端口平分到 IOM 组 1 和 2 以允许冗余。在部署以太网、iSCSI 或光纤通道网络时，在组 1 和组 2 上跨越冗余链接可获得最大可用性。我们用结构识别符和组号表示不连续的 IOM。

例如："A1" 表示组"1"中的结构"A"。"C2"表示组"2"中的结构"C"。

机箱支持三种结构或协议类型。同组的 IOM 和夹层卡必须具有相同或兼容的结构类型。

- **组 A** IOMS 始终连接至服务器的机载以太网适配器；组 A 的 结构类型始终是以太网。
- 对于**组 B，**IOM 插槽永久性连接到每个服务器模块中的**第一个 MC（夹层卡）**插槽。
- 对于**组 C，**IOM 插槽永久性连接到每个服务器模块中的**第二个 MC（夹层卡）**插槽。

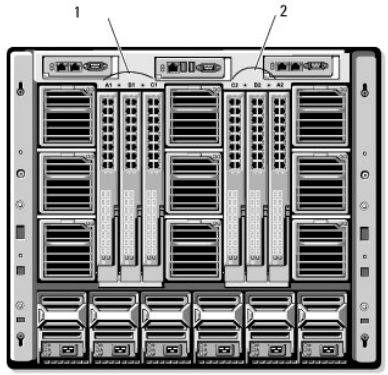
注： 在 CMC CLI 中，IOM 按照惯例称为 switch-*n*：
A1=switch-1、A2=switch-2、B1=switch-3、B2=switch-4、C1=switch-5 和 C2=switch-6。

结构管理

结构管理有助于避免由于安装了与机箱既定结构类型不兼容结构类型的 IOM 或 MC，从而造成有关电气、配置或连接问题。无效硬件配置将会给机箱或其组件带来电气或功能问题。结构管理仅阻止打开无效配置。

图 11-1 显示机箱中 IOM 的位置。各 IOM 的位置按组号（A、B 或 C）表示。这些独立的结构路径分为 2 个 IO 组：组 1 和组 2。在机箱上，IOM 插槽名称标记为 A1、A2、B1、B2、C1 或 C2。

图 11-1. 机箱后视图，显示 IOM 的位置



1	组 1（插槽 A1、B1、C1）	2	组 2（插槽 A2、B2、C2）

CMC 将在硬件日志和 CMC 日志中为无效硬件配置创建条目。

例如：

- 已连接到光纤信道 IOM 的以太网 MC 是无效配置。然而，连接到以太网交换机和安装在相同 IOM 组中以太网直通 IOM 的以太网 MC 是有效连接。
- 如果所有服务器上的第一个 MC 也是光纤信道，则插槽 B1 和 B2 中的光纤信道直通 IOM 和光纤信道交换机 IOM 是有效配置。在这种情况中，CMC 将开启 IOM 和服务器。不过，某些光纤信道冗余软件可能不支持此配置；并非全部有效的配置都是必要的支持配置。

注： 只有当机箱开机时，才能对服务器 IOM 和 MC 执行结构验证。当机箱处于电源待机状态时，服务器模块上的 iDRAC 仍处于关机状态，因此它无法报告服务器的 MC 结构类型。在服务器上的 iDRAC 开机之前， CMC 用户界面中可能不会报告 MC 结构类型。另外，如果机箱开机，则在插入服务器或 IOM（可选）时进行结构认证。如果检测到不匹配结构，则允许服务器或 IOM 开机且状态 LED 闪烁**琥珀**色。

无效配置

有三种无效配置类型：

- 无效 MC 或 LOM 配置，新安装的服务器结构类型与现有 IOM 结构不同
- 无效 IOM-MC 配置，新安装的 IOM 结构类型和驻留的 MC 光纤类型不匹配或不兼容
- 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

无效夹层卡 (MC) 配置

无效 MC 配置发生在单独服务器的 LOM 或 MC 不受相应 IOM 支持的时候。在这种情况，机箱中的所有其他服务器都能运行，但不允许带有不匹配 MC 卡的服务器开机。服务器上的电源按钮将闪烁琥珀色以提示结构不匹配。

有关 CMC 和硬件日志的信息，请参阅 "查看事件日志"。

无效 IOM 夹层卡 (MC) 配置

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 还将使无效配置 IOM 上的错误 LED 闪烁。如果将 CMC 配置为发送警报，则它将为该事件发送电子邮件和/或 SNMP 警报。

有关 CMC 和硬件日志的详情，请参阅 "查看事件日志"。

无效 IOM-IOM 配置

CMC 保持新安装的 IOM 处于关机状态，从而导致 IOM 的错误 LED 闪烁，并在 CMC 和硬件日志中创建关于不匹配的条目。

有关 CMC 和硬件日志的详情，请参阅 "查看事件日志"。

刷新开机场景

当输入/输出模块插入机箱并开机时，其优先权高于服务器。每个组中的第一个 IOM 允许比其它 IOM 先开机。此时，不会执行它们的结构类型验证。如果一个组的第一个插槽上没有 IOM，该组第二个插槽上的模块将开机。如果两个插槽上都有 IOM，第二个插槽中的模块将与第一个插槽中的模块比较一致性。

IOM 开机之后，服务器开机，然后 CMC 将验证服务器的结构一致性。

只要直通模块和交换机的结构等同，则允许将它们在相同的组中。甚至当交换机和直通模块由不同的供应商制造时，也可存在于相同的组中。

监控 IOM 运行状况

IOM 的运行状况可以用两种方法查看：从**"Chassis Status"（机箱状态）**页页上的**"Chassis Graphics"（机箱图形）**部分查看，或者从**"I/O Modules Status"（I/O 模块状态）**页查看。**"Chassis Graphics"（机箱图形）**页提供已安装在机箱中的 IOM 的图形概览。

要使用机箱图形查看 IOM 的运行状况：

1. 登录 CMC Web 界面。
2. 将显示**"Chassis Status"（机箱状态）**页。**"Chassis Graphics"（机箱图形）**的右侧部分描述机箱的后视图并包含 IOM 的运行状态。IOM 运行状态由 IOM 子图形的颜色表示：
   - 绿色 — IOM 存在，电源打开并且正在与 CMC 通信；这表示不存在不利条件。
   - 琥珀色 — IOM 存在，但电源可能未打开，或者可能无法与 CMC 通信；可能存在不利条件。
   - 灰色 — IOM 存在且电源未打开。它当前未与 CMC 通信且不存在不利条件。
3. 将光标停留在单个 IOM 子图形上方将显示相应的文本提示或屏幕提示。文本提示提供有关该 IOM 的其它信息。
4. IOM 子图形超链接到相应的 CMC GUI 页，以便立即导航到与该 IOM 相关联的**"I/O Module Status"（I/O 模块状态）**页。

要使用**"I/O Modules Status"（I/O 模块状态）**页查看所有 IOM 的运行状况：

1. 登录 CMC Web 界面。
2. 在系统树的 **"Chassis"（机箱）**菜单中选择 **"I/O Modules"（I/O 模块）**。
3. 单击**"Properties"（属性）**选项卡。
4. 单击**"Status"（状态）**子选项卡。将显示**"I/O Modules Status"（I/O 模块状态）**页。

项目	说明		
插槽	按结构号（A、B 或 C）和组（1 或 2）显示 I/O 模块在机箱中的位置。IOM 枚举：**A1**、**A2**、**B1**、**B2**、**C1** 或 **C2**。		
"Present"（存在）	显示 IOM 是否存在（**"Yes"[是]** 或 **"No"[否]**）。		
"Health"（运行状况）		"OK"（良好）	表示 IOM 存在且正在与 CMC 通信。在 CMC 和服务器间发生通讯故障时，CMC 将无法获取或显示 IOM 的运行状况。
		"Informational"（通知）	当运行状况（ " OK"[正常]、 "Warning"[警告]、" Severe"[严重]）没有发生变化时，显示关于 IOM 的信息。
		"Warning"（警告）	表示发出的警告警报，以及**必须采取的修正操作。**如果没有采取补救操作，将可能发生影响 IOM 完整性的严重故障。 导致警告的条件示例：IOM 结构与服务器的夹层卡结构不匹配；无效 IOM 配置，同一组中新安装的 IOM 与现有 IOM 不匹配。
		"Severe"（严重）	指示至少已发出一个故障警报。严重状况表示 IOM 上发生系统故障，**必须立即采取补救措施**。 导致严重状况的条件示例：检测 IOM 失败；IOM 已卸下。
	注： 运行状况的任何变化都会记录到硬件和 CMC 日志。有关详情，请参阅"查看事件日志"。		
"Fabric"（结构）	显示 IOM 的结构类型：Gigabit Ethernet、10GE XAUI、10GE KR、10GE XAUI KR、FC 4 Gbps、FC 8 Gbps、SAS 3 Gbps、SAS 6 Gbps、Infiniband SDR、Infiniband DDR、Infiniband QDR、PCIe Bypass Generation 1、PCIe Bypass Generation 2。 **注：** 了解机箱中 IOM 的结构类型对防止同组中 IOM 不匹配的情况非常关键。有关 I/O 结构的信息，请参阅 "I/O 结构管理"。		
"Name"（名称）	显示 IOM 产品名称。		
启动 IOM 管理控制台		如果存在特定 I/O 模块的按钮，单击它可在新浏览器窗口或选项卡中为该 IOM 模块启动 I/O 管理控制台。 **注：** 此选项仅用于管理型交换机 I/O 模块。不能用于直通 I/O 模块或非管理型 Infiniband 交换机。 **注：** 如果一个 I/O 模块由于关闭而无法访问，则其 LAN 接口被禁用，或者没有为模块制定一个有效 IP 地址，没有为该 I/O 模块显示"Launch IOM GUI"（启动 IOM GUI）选项。 **注：** 将提示您登录 I/O 模块管理界面。 **注：** 可使用 CMC GUI 配置 I/O 模块 IP 地址，如 "为单个	

	IOM 配置网络设置"中所述。
角色	当 I/O 模块链接在一起时，角色显示 I/O 模块堆栈成员关系。**"Member"（成员）**表示模块是堆栈组的一部分。**"Master"（主要）**表示模块是主要访问点。
"Power Status"（电源状况）	显示 IOM 的电源状况：**"On"（开）**、**"Off"（关）**或**"N/A"（无）**。
服务标签	显示 IOM 的服务标签。服务标签是由 Dell 提供的用于支持和维护的唯一标识符。 运行状况的任何变化都会记录到硬件和 CMC 日志。有关详情，请参阅"查看事件日志"。 **注：** 直通模块没有服务标签。只有交换机才有服务标签。

查看所有单独 IOM 的运行状况

"I/O Module Status"（I/O 模块状况）页（与*"I/O Modules "[I/O 模块]***状态**页不同）提供单个 IOM 的概览。

查看所有单独 IOM 的运行状况：

1. 登录 CMC Web 界面。
2. 展开系统树中的**" I/O Modules "（输入/输出模块）**。展开的**"I/O Modules"（I/O 模块）**列表中将列出所有的 IOM (1-6)。
3. 在系统树**"I/O Modules"（I/O 模块）**列表中单击您想查看的 IOM。
4. 单击**"Status"（状态）**子选项卡。将显示**"I/O Modules Status"（I/O 模块状态）**页。

项目	说明		
"Location"（位置）	按组号（A、B 或 C）和插槽号（1 或 2）显示 IOM 在机箱中的位置。插槽名称：**A1**、**A2**、**B1**、**B2**、**C1** 或 **C2**。		
"Name"（名称）	显示 IOM 的名称。		
"Present"（存在）	显示 IOM 是**"Present"（存在）**还是**无**。		
"Health"（运行状况）		"OK"（良好）	表示 IOM 存在且正在与 CMC 通信。在 CMC 和服务器间发生通讯故障时，CMC 将无法获取或显示 IOM 的运行状况。
		"Informational"（通知）	当运行状况（ " OK"[正常]、 " Warning"[警告]、" Severe"[严重]）没有发生变化时，显示关于 IOM 的信息。 产生通知状况的条件示例：检测到存在 IOM；用户请求 IOM 关机后再开机。
		"Warning"（警告）	表示发出的警告警报，以及**必须采取的修正操作**。如果没有采取补救操作，将可能发生影响 IOM 完整性的严重故障。 例如，在这些情况下会引发警告：IOM 结构与服务器的夹层卡结构不匹配；无效 IOM 配置，新安装的 IOM 与同一组中现有 IOM 不匹配。
		"Severe"（严重）	指示至少已发出一个故障警报。严重状况表示 IOM 上发生系统故障，**必须立即采取补救措施**。 导致严重状况的条件示例：检测 IOM 失败；IOM 已卸下。
	注： 运行状况的任何变化都会记录到硬件和 CMC 日志。有关查看日志的信息，请参阅 "查看硬件日志" 和 "查看 CMC 日志"。		
"Power Status"（电源状况）	显示 IOM 的电源状况：**"On"（开）**、**"Off"（关）**或**"N/A"（无）**。		

服务标签	显示 IOM 的服务标签。服务标签是由 Dell 提供的用于支持和维护的唯一标识符。
"Fabric"（结构）	显示 IOM 的结构类型：Gigabit Ethernet、10GE XAUI、10GE KR、10GE XAUI KR、FC 4 Gbps、FC 8 Gbps、SAS 3 Gbps、SAS 6 Gbps、Infiniband SDR、Infiniband DDR、Infiniband QDR、PCIe Bypass Generation 1、PCIe Bypass Generation 2。 **注：** 了解机箱中 IOM 的结构类型对防止同组中 IOM 不匹配的情况非常关键。有关 I/O 结构的信息，请参阅 "I/O 结构管理"。
"MAC Address"（MAC 地址）	显示 IOM 的 MAC 地址。MAC 地址是硬件供应商分配给设备的作为标识之用的唯一地址。 **注：** 直通模块没有 MAC 地址。只有交换机才有 MAC 地址。
角色	当模块相互连接时，显示 I/O 模块"堆栈"关系： ○ **"Member"（成员）** — 模块是堆栈设置的一部分 ○ **"Master"（主要）** — 模块是主要访问点。

为单个 IOM 配置网络设置

通过"I/O Modules Setup"（输入/输出模块设置）页，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）。

注： 要更改"I/O Modules Configuration"（I/O 模块配置）页的设置，您必须具有结构 A 管理员权限以配置组 A 中的 IOM；结构 B 管理员权限以配置组 B 中的 IOM；或结构 C 管理员权限以配置组 C 中的 IOM。

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；这将导致无法设置带外 IP 地址。请参阅默认带内管理 IP 地址的 IOM 说明文件。

注： 仅显示机箱中存在的 IOM。

注： 不要为以太网直通和 Infiniband 交换机配置 I/O 模块网络设置。

要为单个 IOM 配置网络设置：

1. 登录 CMC Web 界面。
2. 展开系统树中的**"I/O Modules"（I/O 模块）**。单击**"Setup"（设置）**子选项卡。随即显示**"Configuring I/O Modules Network Settings"（配置 I/O 模块网络设置）**页。
3. 要配置 I/O 模块的网络设置，可以为以下属性键入/选择值，然后单击**"Apply"（应用）**。

   注： 仅可配置电源打开的 IOM。

   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，您必须输入 connect switch-n 或 racadm connect switch -n RACADM 命令，或使用到 IOM GUI 的直接界面将该地址保存到启动配置文件中。

项目	说明
插槽	按组号（A、B 或 C）和插槽号（1 或 2）显示 IOM 在机箱中的位置。插槽名称：A1、A2、B1、B2、C1 或 C2。（不能更改插槽值。）
"Name"（名称）	显示 IOM 产品名称。（不能更改 IOM 名称。）
"Power State"（电源状态）	显示 IOM 的电源状态。（不能从该页更改电源状态。）
"DHCP Enabled"（已启用 DHCP）	启用机箱上的 IOM 从动态主机配置协议 (DHCP) 服务器自动请求并获取 IP 地址。 默认：选中（已启用）。 如果选中该选项，IOM 将自动从网络中的 DHCP 服务器检索 IP 配置（IP 地址、子网掩码和网关）。 **注：** 当启用该功能时，"IP Address"（IP 地址）、"Gateway"（网关）和"Subnet Mask"（子网掩码）属性

	字段（紧跟在该选项后面）处于未激活状态，而且以前为这些属性输入的任何值都被忽略。 如果未选中该选项，您必须在紧跟在该选项后面的相应文本字段中手动输入有效的 IP 地址、网关和子网掩码。
"IP Address"（IP 地址）	为 IOM 网络接口指定 IP 地址。
"Subnet Mask"（子网掩码）	为 IOM 网络接口指定子网掩码。
"Gateway"（网关）	为 IOM 网络接口指定网关。

IOM 网络设置故障排除

下表包括 IOM 网络设置的故障排除项：

- 配置更改后 CMC 可能过快地读取 IP 地址设置；单击**"Apply"（应用）** 后将显示 **0.0.0.0**。您必须按刷新按钮以便查看交换机上的 IP 地址是否设置正确。
- 如果在设置 IP/掩码/网关时发生错误，则交换机将不会设置 IP 地址并将在所有字段中返回 **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。

有关 IOM 网络设置的详情，请参阅 *Dell™ PowerConnect™ M6220 Switch Important Information* document 和 *Dell™ PowerConnect™ 6220 Series Port Aggregator White Paper*。

目录

目录

概览

Dell Chassis Management Controller Firmware 版本 3.0 用户指南

Dell Chassis Management Controller (CMC) 是一种热插拔系统管理硬件和软件解决方案，专门用于为 Dell PowerEdge M1000e 机箱系统提供远程管理功能和电源控制功能。

可以配置 CMC 为：出现与温度、硬件误配置、电源故障和风扇速度相关的警告或错误时，发送电子邮件警报或 SNMP 陷阱警报。

CMC 自身具备微处理器和内存，它由所插入的模块化机箱供电。要开始使用 CMC，请参阅 "安装和设置 CMC"。

此版本的新功能

此版本的 CMC 支持以下功能：

- 支持 10GB 以太网
- 全新 M710HD 虚拟化环境优化服务器
- 全新和更高效的风扇
- iDRAC6 和 CMC 支持轻型目录访问协议 (LDAP)
  - 通过 Linux 社区使用的开放标准和在大型企业中跨平台提供基于目录的验证和访问授权
- 改进的 2.0 CMC Web 界面
  - 直观、重要的信息和目录一目了然
  - 大部分常用操作可通过一次单击完成
- 机箱可在由 UPS 或其他备用电源供电时以最大节能模式运行，从而延长供电时间
- 服务器温度传感器摘要在单个页面上显示累计温度和运行状态
- 操作系统分配的服务器主机名称在 CMC GUI 中作为插槽名称
- 用于服务器的虚拟键盘-视频-鼠标（远程控制台）会话
- CMC Web 界面登录特定于一次会话的超时时间

CMC 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
- 使用 SNMP、Web 界面、iKVM 或远程登录/SSH 连接进行远程系统管理和监控
- 支持 Microsoft Active Directory 验证 — 在 Active Directory 中使用标准架构或扩展架构集中管理 CMC 用户 ID 和密码
- 监控 — 允许访问系统信息和组件状况
- 访问系统事件日志 — 提供对硬件日志和 CMC 日志的访问
- 不同组件的固件更新 — 支持更新 CMC、服务器、iKVM 和 I/O 模块基础设施设备的固件
- Dell OpenManage 软件集成 — 使您能够从 Dell OpenManage Server Administrator 或 IT Assistant 启动 CMC Web 界面
- CMC 警报 — 通过电子邮件信息或SNMP 陷阱提供潜在管理节点问题
- 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
- 密码级别安全性管理 — 防止未授权访问远程系统

- 基于角色的权限 — 为不同的系统管理任务提供可分配的权限
- Integrated Dell Remote Access Controller (iDRAC) Web 界面的启动位置
- 支持 WS-Management
- FlexAddress 功能 — 使用机箱为特定插槽分配的 WWN/MAC ID 替换工厂分配的全球名称/介质访问控制 (WWN/MAC) ID；可选升级。有关详情，请参阅 "使用 FlexAddress"
- 机箱组件状态和运行状况的图形显示
- 支持一个或多个插槽的服务器
- 一次更新多个 iDRAC 管理控制台固件
- LCD iDRAC 配置向导支持 iDRAC 网络配置
- iDRAC 单次登录
- 网络时间协议 (NTP) 支持
- 增强服务器摘要、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*重新就位*

安全保护功能

CMC 提供以下安全保护功能：

- 通过 Active Directory（可选）或硬件存储的用户 ID 和密码对用户进行验证
- 基于角色的权限，使管理员能为每个用户配置特定权限
- 通过 Web 界面配置用户 ID 和密码
- Web 界面支持 128 位 SSL 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）

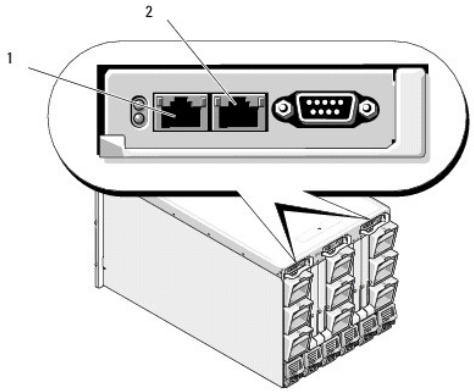
  注： Telnet 不支持 SSL 加密技术。

- 可配置 IP 端口（如适用）
- 每个 IP 地址的登录失败限制，在超过此限制时阻止来自该 IP 地址的登录
- 可配置会话自动超时和一个以上并发会话
- 连接 CMC客户端的有限 IP 地址范围
- 使用加密层的 Secure Shell (SSH) 实现更高的安全保护
- 单一登录、双重验证和公共密钥验证

机箱概览

图 1-1 显示 CMC（插入件）的前侧和 CMC 插槽在机箱中的位置。

图 1-1. Dell M1000e 机箱和 CMC



1	GB 端口	2	STK 端口

硬件规格

TCP / IP 端口

当为远程访问 CMC 开启防火墙时，必须提供端口信息。

表 1-1. CMC 服务器侦听端口

端口号	功能
22*	SSH
23*	Telnet
80*	HTTP
161	SNMP 代理
443*	HTTPS
* 可配置端口	

表 1-2. CMC 客户端端口

端口号	功能
25	SMTP
53	DNS
68	DHCP 分配的 IP 地址
69	TFTP
162	SNMP 陷阱
514*	远程系统日志
636	LDAPS
3269	全局编录 (GC) LDAPS
* 可配置端口	

支持的远程访问连接

表 1-3. 支持的远程访问连接

连接	功能
CMC 网络接口端口	• 两个 10/100 GB 端口，一个用于管理，另一个用于机箱到机箱电缆通信 • 10Mbps/100Mbps/1Gbps 以太网，通过 CMC GbE 端口 • DHCP 支持 • SNMP 陷阱和电子邮件事件通知 • GB 端口：CMC Web 界面专用网络接口 • STK：机箱到机箱管理网络电缆通信的上行端口 • iDRAC 和输入/输出模块 (IOM) 网络接口 • 支持远程登录/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	• 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 • 为专门设计用于使用二进制协议与特定类型 IOM 通信的应用程序提供二进制交换支持 • 通过 connect（或 racadm connect）命令，可将串行端口连接到服务器的串行控制台或 I/O 模块
其它连接	• 通过 Avocent 集成 KVM 交换机模块 (iKVM) 访问 Dell CMC 控制台

支持的平台

CMC 支持为 M1000e 平台设计的模块化系统。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，请参阅 Dell 支持网站 **support.dell.com / manuals** 上的*《Dell 系统软件支持值表》*。

支持的 Web 浏览器

CMC3.0 支持以下网络浏览器：

- Windows 7、Windows Vista、Windows XP 和 Windows Server 2003 系列的 Microsoft Internet Explorer 8.0。
- Windows 7、Windows Vista、Windows XP 和 Windows Server 2003 系列的 Microsoft Internet Explorer 7.0。
- Mozilla Firefox 1.5（32-位） - 功能受限。

要查看 CMC Web 界面的本地化版本：

1. 打开 Windows**"Control Panel"（控制面板）**。
2. 双击**"Regional Options"（区域选项）**图标。
3. 从**"Your locale (location)"（您的区域设置 [位置]）**下拉菜单选择所需区域设置。

支持的管理控制台应用程序

CMC 支持与 Dell OpenManage IT Assistant 集成。有关详情，请参阅 Dell 支持网站 **support.dell.com / manuals** 上的 IT Assistant 说明文件集。

WS-Management 支持

Web Services for Management (WS-MAN) 是用于系统管理的基于简单对象访问协议 (SOAP) 的协议。WS-MAN 提供一种可互操作的协议，使设备可以在网络之间共享和交换数据。CMC 使用 WS-MAN 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 信息定义了可在受控系统中操作的语义和信息类型。Dell 嵌入式服务器平台管理界面按配置文件进行组织，其中每个配置文件定义某个管理域或功能区域的特定界面。此外，Dell 定义了多个模型和配置文件扩展，为附加功能提供界面。

要访问 WS-Management，需要使用本地用户权限登录并在端口 443 使用安全套接层 (SSL) 协议进行基本验证。有关设置用户帐户的信息，请参阅*《Dell Chassis Management Controller 固件管理员参考指南》*中的"会话管理数据库属性"部分。

通过 WS-Management 获得的数据是由映射到以下 DMTF 配置文件版本 1.0.0 的 CMC 工具界面所提供的数据的子集：

- 分配功能配置文件
- 基础度量配置文件
- 基础服务器配置文件
- 计算机系统配置文件
- 模块化系统配置文件
- 物理资产配置文件
- Dell 电源分配配置文件
- Dell 电源配置文件
- Dell 电源拓扑配置文件
- 电源状态管理配置文件
- 配置文件注册配置文件
- 记录日志配置文件
- 资源分配配置文件
- 基于角色授权配置文件
- 传感器配置文件
- 服务处理器配置文件
- 简单标识管理配置文件
- Dell Active Directory 客户端配置文件

- 引导控制配置文件
- Dell 简单 NIC 配置文件

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。有关设置用户帐户的信息，请参阅《*Dell Chassis Management Controller 固件管理员参考指南*》中的 "cfgSessionManagement 数据库属性"部分。可以通过利用 Windows WinRM、Powershell CLI 等客户端基础设施、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。

对于使用 Microsoft WinRM 的客户端连接，最低要求为 2.0 版本。有关详情，请参阅 **Microsoft 文章 <http://support.microsoft.com/kb/968929>。**

Dell 技术中心 **www.delltechcenter.com** 上提供了其它实施指南、白皮书、配置文件和代码样例。有关详情，请参阅：

- DTMF Web 站点：**www.dmtf.org/standards/profiles/**
- WS-MAN 版本注释或自述文件。
- **www.wbemsolutions.com/ws_management.html**
- DMTF WS-Management 规范：**www.dmtf.org/standards/wbem/wsman**

您可能需要的其它说明文件

除了该指南之外，还可以在 Dell 支持网站 support.dell.com/manuals 上找到以下指南。在"Manuals"（手册）页上，单击**"Software"（软件）→"Systems Management"（系统管理）**。单击右侧的相应产品链接访问文档：

- *CMC 联机帮助*提供了有关使用 Web 界面的信息。
- *机箱管理控制器 (CMC) 安全数字 (SD) 卡技术规范*提供最低 BIOS 和固件版本、安装和使用情况的信息。
- 《*Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise 刀片服务器版用户指南*》提供有关在 Managed System 中安装、配置和维护 iDRAC 的信息。
- 《*Dell OpenManage IT Assistant 用户指南*》提供关于 IT Assistant 的信息。
- 针对第三方管理控制台应用程序的说明文件。
- 《*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 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。

以下系统说明文件还提供了更多有关 CMC 所安装的系统的信息：

- 系统附带的安全说明提供了重要的安全与管制信息。有关其它管制信息，请参阅 **www.dell.com/regulatory_compliance** 上的"Regulatory Compliance"（管制遵循）主页。保修信息可能包括在该说明文件中，也可能作为单独的说明文件提供。
- 机架解决方案中的《*机架安装指南*》和《*机架安装说明*》介绍如何将系统安装到机架中。
- 《*硬件用户手册*》提供了有关系统功能的信息，并说明了如何排除系统故障以及安装或更换系统组件。
- 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。

  注： 请始终先阅读这些更新，因为这些更新通常会取代其它说明文件中的信息。

- 系统可能附带版本注释或自述文件，提供对系统或说明文件所做的最新更新，或者为有经验的用户或技术人员提供高级技术参考资料。
- 有关 IOM 网络设置的详情，请参阅《*Dell PowerConnect M6220 交换机重要信息*》说明文件和《*Dell PowerConnect 6220 系列端口聚合器白皮书*》。

目录

目录

电源管理

Dell Chassis Management Controller Firmware 版本 3.0 用户指南

概览

Dell PowerEdge M1000e 服务器机柜是市场上最具有能源效率的模块化服务器。它设计独特，包括高效率的电源设备和风扇，拥有优化的布局以便空气更轻松地流过系统，并且机柜中处处包含经能源优化的组件。最优化的硬件设计配合内置到机箱管理控制器 (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能源效率并全面控制电源环境。

PowerEdge M1000e 模块化机柜包括交流电源，并在所有活动的内部电源设备 (PSU) 上进行负载分配。系统最多提供分配到服务器模块和相关机柜基础设施的 11637 瓦交流电源。

注： 实际电源传输基于配置和工作负载。

M1000e 的电源管理功能可帮助管理员配置机柜以减少功耗，并根据他们独特的要求和环境定制电源管理。

PowerEdge M1000e 机柜可针对影响 PSU 行为的三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。

交流冗余模式

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。

在为交流冗余配置系统时，PSU 按电网划分：插槽 1、2 和 3 中 PSU 在第一个电网，而插槽 4、5 和 6 中 PSU 在第二个电网。CMC 管理电源，这样即使有一个电网故障，系统仍可在不降低性能的情况下运行。交流冗余也可承受单个 PSU 的故障。

注： 因为交流冗余的作用之一是在整个电网故障的情况下支持服务器的无缝运行，因此在两个电网的供电能力大约相等时大多数供电用于保持交流冗余性。

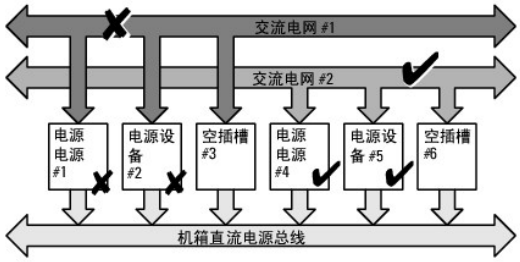
注： 交流冗余仅在负载要求不超过供电能力最低的电网的容量时可实现。

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。也可进行其他配置，但每个组合中至少在每个电网中有 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当。维护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 因某种原因不能维持交流冗余，则会在配置冗余掉失事件提示时通过电子邮件和/或 SNMP 警报提示管理员。

图 9-1. 图 8-2.每个电网 2 个 PSU 和电网 1 上一个供电故障



注： 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"Online"（联机）。在这种情况，任一剩余 PSU 出现故障也不会中断系统的操作。如果一个 PSU 出现故障，机箱运行状况将被标记为不严重。如果供电能力更小的电网不能支持全部机箱电源分配，交流冗余状态将报告为"No Redundancy"（无冗余），机箱运行状况显示为"Critical"（严重）。

电源冗余模式

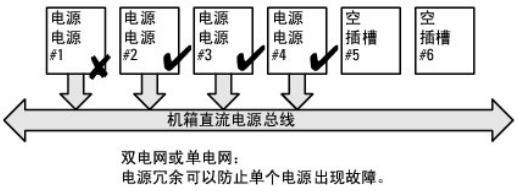
电源设备冗余模式在冗余电源电网不可用时发挥作用，但您可能希望防止因单个 PSU 出现故障而导致模块化机柜中的服务器停机。供电能力最高的 PSU 将为此目的而联机保留。这样就形成了电源设备冗余池。

超出功率和冗余所需的 PSU 仍可用并会在故障时增加到冗余池。

与交流冗余不同的是，选择电源冗余后，CMC 不要求 PSU 设备存在于任何指定 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。待机状态指示物理状态，而不是电源的。启用 DPSE 时，额外的 PSU 置于待机模式，以提高效率，节约用电。

图 9-2. 电源设备冗余：合计 4 个 PSU，其中 1 个 PSU 故障。



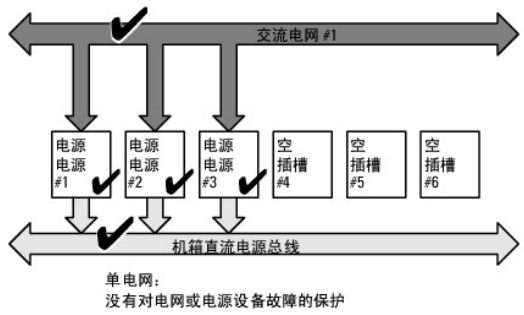
无冗余模式

*无冗余模式*是 3 PSU 配置的出厂默认设置，表示机箱没有配置任何电源冗余。在这种配置下，机箱的总体冗余状态始终表示为**"No Redundancy"（无冗余）**。

"No Redundancy"（无冗余）配置时，CMC 不要求 PSU 设备存在于任何指定的 PSU 插槽位置。

注： 如果在**"No Redundancy"（无冗余）**模式中禁用 DPSE，则机箱中的所有 PSU 均列为**"Online"（联机）**。在 DPSE 启用时，机箱中所有活动的 PSU 均列为**"Online"（联机）**且其他 PSU 可转为**"Standby"（待机）**以提高系统功效。

图 9-3. 机箱中 3 个 PSU 且无冗余



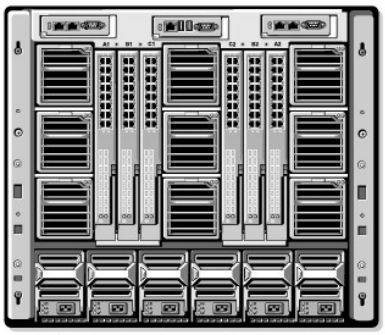
一个 PSU 出现故障时，系统会根据需要使其它 PSU 退出待机模式，以便支持机箱的电源分配。如果有 4 个 PSU 而只要求 3 个，则在 1 个 PSU 出现故障时第 4 个 PSU 会被联机。一个机箱可让所有 6 个 PSU 均联机。

启用 DPSE 时，额外的 PSU 置于待机模式，以提高效率，节约用电。有关详情，请参阅"动态电源设备接入"。

硬件模块电源预算

图 9-4 显示包含六个 PSU 配置的机箱。PSU 的编号从机柜左侧开始分别为 1-6。

图 9-4. 配备六个 PSU 的机箱



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瓦特数。

CMC 将电源分配给机箱中的 CMC 基础设施和服务器。CMC 基础设施由机箱中的组件组成，例如风扇、输入/输出模块和 iKVM（如果存在）。机箱最多可以有 16 个服务器，这些服务器通过 iDRAC 与机箱通信。有关详情，请参阅 **support.dell.com / manuals** 上的《*iDRAC User's Guide*》。

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 软件重新估计功率需求，并请求随后对功率范围做出调整。

CMC 准许服务器请求的功率，并且从可用预算中减去分配的瓦特数。一旦准许服务器的一个功率请求，服务器的 iDRAC 软件就对实际功耗进行连续监控。iDRAC 功率范围会根据实际功率需求而随时间发生变化。只有服务器完全消耗分配的电源时，iDRAC 才会请求升高功率。

在重负载下，可降低服务器处理器的性能以确保功耗低于用户配置的**"System Input Power Cap"（系统输入功率上限）**。

PowerEdge M1000e 机柜可以为大部分服务器配置的峰值性能提供充足的电能，但许多可用的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它们的机柜提供电源，M1000e 允许您指定**"System Input Power Cap"（系统输入电源上限）**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源以运行风扇、IO 模块、iKVM（如存在）和 CMC 自身。此电源分配称作**"Input Power Allocated to Chassis Infrastructure"（分配给机箱基础设施的输入电源）**。机柜中的服务器在机箱基础设施后开机。任何设置**"System Input Power Cap"（系统输入功率上限）**低于实际功耗的尝试都会失败。

如果需要总体电源预算始终低于**"System Input Power Cap"（系统输入电源上限）**的值，CMC 将为服务器分配一个小于它们最大请求功率的值。服务器根据其**"Server Priority"（服务器优先权）**设置获得分配的电力，拥有优先权 1 的服务器获得最大电力，拥有优先权 2 的在拥有优先权 1 的服务器之后获得电力，以此类推。优先权较低的服务器获得的电力可能少于拥有优先权 1 的服务器，这取决于**"System Input Max Power Capacity"（系统输入最大电源容量）**和用户配置的**"System Input Power Cap"（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等配置变化，可能需要提高**"System Input Power Cap"（系统输入电源上限）**。在热条件变化并且需要风扇以更快速度运转时，都会造成它们消耗更多电力，模块化机柜中的电力需求也会随之增加。插入输入/输出模块和 iKVM 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，也会消耗相当少量的电力。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**"System Input Power Cap"（系统输入功率上限）**提高到 11637 瓦的最大值，以允许额外的服务器开机。

模块化机柜中减少功率分配的变动为：

- 服务器电源关闭
- 服务器
- I/O 模块、
- iKVM 拆卸
- 机箱过渡到断电状态

机箱打开或关闭时均可重新配置**"System Input Power Cap"（系统输入电源上限）**。

服务器插槽电源优先级设置

CMC 允许您为机柜中十六个服务器插槽的每一个设置电源优先权。优先权设置从 **1**（最高）到 **9**（最低）。这些设置被分配给机箱中的插槽，并且插槽的优先权将被插入该插槽中的任何服务器继承。CMC 使用插槽优先权将电源优先预算为机柜中的最高优先权服务器。

根据默认服务器插槽优先权设置，功率将平均分配给所有插槽。更改插槽优先权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权值 2 或以上，优先权为 1 的服务器模块将首先开机。然后这些更高优先权服务器将获得最大电源分配，而可能不会为更低优先权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。

如果管理员在更高优先权服务器之前为低优先权服务器模块手动开机，低优先权服务器模块将首先成为让它们的电源分配下降到最小调节值的模块，以适应更高优先权的服务器。所以在可供分配的功率耗尽后，CMC 会从较低或同等优先级服务器中收回功率分配直到其达到最低功耗水平。

注： 输入/输出模块、风扇和 iKVM（如果存在）具有最高优先权。CMC 收回电源只是为了满足优先权更高的模块或服务器的电源需求。

动态电源设备接入

在默认情况下，动态电源设备接入 (DPSE) 模式是禁用的。DPSE 可通过优化 PSU 向机箱供电的功效而节电。这样可延长 PSU 的使用寿命、减少热量产生

CMC 将监控总体机柜电源分配，并将 PSU 转到**"Standby"（待机）**状态，从而通过更少的 PSU 提供机箱的总体电源分配。因为以更高利用率运行时联机 PSU 更有效率，所以在提高效率的同时还会延长待机 PSU 的使用寿命。

若要其余 PSU 在最大效率下工作：

- **带有 DPSE 的"No Redundancy"（无冗余）**模式具有更高的电源效率，且有最佳数目的 PSU 处于联机状态。不需要的 PSU 置于待机模式。
- **带有 DPSE 的"PSU Redundancy"（PSU 冗余）**模式也具有电源效率。至少两个电源设备处于活动状态，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 Redundancy"（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"AC Redundancy"（交流冗余）**模式（至少有两个电源设备处于活动状态，每个电网中有一个）在部分负载模块化机柜配置的效率和最大可用性之间提供出色的平衡。
- 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。

可针对所有上述三个电源设备冗余配置启用 DPSE —**"No Redundancy"（无冗余）**、**"Power Supply Redundancy"（电源设备冗余）**和**"AC Redundancy"（交流冗余）**。

- 在使用 DPSE 的**"No Redundancy"（无冗余）**配置中，M1000e 最多可让五个电源设备处于**"Standby"（待机）**状态。在六个 PSU 的配置中，有些 PSU 装置将处于"Standby"（待机）模式并保持不使用状态，以便提高电源效率。拆卸或此配置中的联机 PSU 出现故障时，会导致处于**"Standby"（待机）**状态的 PSU 变为**"Online"（联机）**；不过，待机 PSU 最多需要 2 秒才能变为活动，所以部分服务器模块在**"No Redundancy"（无冗余）**配置中的过渡期间可能丢失电源。

注： 在三 PSU 配置中，服务器负载可能阻止任何 PSU 过渡到**"Standby"（待机）**。

- 在**"Power Supply Redundancy"（电源设备冗余）**配置中，除了机柜开机所需的 PSU 之外，机柜始终保持一个附加的 PSU 处于开启状态并标记为**"Online"（联机）**。电源利用情况受到监控，根据总体系统负载，最多四个 PSU 可转到**"Standby"（待机）**状态。在六个 PSU 的配置中，最少两个电源设备始终保持开启。

  因为采用**"Power Supply Redundancy"（电源设备冗余）**配置的机柜始终启用一个额外的 PSU，所以当一个联机 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 故障时，一个待机 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的电源丢失，同时待机 PSU 开机。

- 在**"AC Redundancy"（交流冗余）**模式下，机箱开机时所有电源设备均启用。电源利用得到监控，并且如果系统配置和电源利用允许，PSU 将转到 **"Standby"（待机）状态**。因为电网中 PSU 的**"Online"（联机）**状态将镜像其他电网，所以机柜能承受整个电网的电源损失而不会中断机柜的电源。

  "**AC Redundancy"（交流冗余）**配置中功率要求的增加将造成 PSU 从"**Standby"（待机）**状态接入。这保持双电网冗余所需的镜像配置。

注： 启用了 DPSE 时，在三种电源冗余策略模式中，当电源需求增加时，待机 PSU 都会转为**"Online"（联机）**以收回电源。

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
- 无冗余

机箱的默认冗余配置取决于它包含的 PSU 数量，如 表 9-1 中所示。

表 9-1. 默认冗余配置

PSU 配置	默认冗余策略	默认动态 PSU 接入设置
六 PSU	交流冗余	已禁用
三 PSU	无冗余	已禁用

交流冗余

在具有六个 PSU 的交流冗余模式中，所有六个 PSU 都处于活动状态。左侧的三个 PSU 必须连接至一个交流电网，同时右侧的三个 PSU 连接到另一个交流电网。

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 将接替供电任务，而不会中断服务器或基础设施。

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）。如果此条件不能满足，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 保持为备用状态，确保任何一个 PSU 的故障不会造成服务器或机箱断电。电源设备冗余模式最多需要四个 PSU。启用 DPSE 后，如果存在额外的 PSU，将使用该 PSU 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。

无冗余

最多三个 PSU 电源可以用于为整个机箱供电。因此，在 6 PSU 机箱中，如果任意 3 个 PSU 出现故障，机箱将继续以全容量运行。

小心： "No Redundancy"（无冗余）模式仅使用最少的 PSU 数目且没有备用。任何一个活动的 PSU 发生故障都将导致服务器掉电和数据丢失。

节能和电源预算更改

当达到用户配置的最大电源限制时，CMC 能够执行节能。当电源需求超出用户配置的**"System Input Power Cap"（系统输入电源上限）**时，CMC 将按优先权从低到高的顺序减少为服务器提供的电源，以便为机箱中高优先权的服务器和其它模块腾出电源。

如果机箱中所有或多个插槽配置了相同的优先权，CMC 将按照插槽编号递增的顺序减少为服务器提供的电源。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 的数字，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。

有关分配服务器优先级的说明，请参阅使用 "使用 RACADM"。

您可以使用 GUI 分配服务器优先权：

1. 单击系统树中的**"Servers"（服务器）**。
2. 单击**"Power"（电源）→ "Priority"（优先权）**。

节能和最大节能模式

CMC 在以下情况下进入最大节能模式：

- 用户通过 Web 接口或 RACADM 选择最大节能模式。
- 由 UPS 设备发出的自动命令行脚本选择最大节能模式。

在最大节能模式下，所有服务器都在最低功耗水平下工作且所有后续服务器功率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权如何都不能开机。

系统在用户或自动命令行脚本取消选择最大节能模式时恢复到最大性能。

使用 Web 界面

您可用 GUI 选择或取消选择最大节能模式：

1. 在系统树中选择**"Chassis Overview"（机箱概览）**。
2. 单击**"Power"（电源）→"Configuration"（配置）**。
3. 选择**"Max Power Conservation Mode"（最大节能模式）**框以启用最大节能模式，然后单击**"Apply"（应用）**。
4. 取消选择**"Max Power Conservation Mode"（最大节能模式）**框可恢复正常工作，然后单击**"Apply"（应用）**。

使用 RACADM

打开到 CMC 的串行/远程登录/SSH 控制台，并登录。

- 若要启用最大节能模式，键入：

```
racadm config -g cfgChassisPower -o cfgChassisMaxPowerConservationMode 1
```

- 若要恢复正常工作，键入：

```
racadm config -g cfgChassisPower -o cfgChassisMaxPowerConservationMode 0
```

110V PSU 的工作

部分 PSU 可在 110V 交流输入下工作。此输入可超出分支电路的允许值。如果有 PSU 连接到 110V 交流，则用户需要设置 CMC 才能让机柜正常工作。如果未设置且检测到 110V 的

PSU，则所有后续服务器功率分配请求都会被拒绝。在此情况下，额外的服务器无论优先权如何都不能开机。您可通过 Web 接口或 RACADM 设置 CMC 使用 110 V 的 PSU。

使用 Web 界面

确认 110 V 电路是预期电流的额定值，然后执行以下步骤：

1. 在系统树中选择**"Chassis Overview"（机箱概览）**。
2. 单击**"Power"（电源）→"Configuration"（配置）**。
3. 选择**"Allow 110 VAC Operation"（允许 110 V 交流工作）**并单击**"Apply"（应用）**。

使用 RACADM

确认 110 V 电路是预期电流的额定值，然后执行以下步骤：

1. 打开到 CMC 的串行/远程登录/SSH 文本控制台，并登录。
2. 启用 110 V 交流的 PSU：

```
racadm config -g cfgChassisPower -o cfgChassisAllow110VACOperation 1
```

PSU 故障与降级或无冗余策略

在节能模式中，当发生电源不足的事件时（如 PSU 故障），CMC 将减少为服务器供电。减少服务器的电源后，CMC 重新评估机箱的电源需求。如果功率要求仍未满足，则 CMC 会关闭低优先权服务器。

在电源需求仍维持在电源预算范围内时，高优先级服务器的电源将逐渐恢复。

注： 要设置冗余策略，请参阅 "配置电源预算和冗余"。

新的服务器接入策略

当新服务器开机时，如果添加此新服务器后超出机箱可用的电源，CMC 可能需要降低对低优先级服务器的供电，以便为新服务器提供更多电源。如果管理员为机箱配置的电源限制低于为服务器分配全功率所需的电源，或者电源不足以在最坏情况下为机箱中所有服务器提供电源时会发生这种情况。如果通过降低为较低优先级服务器分配的电源无法腾出足够的电源，则新服务器可能无法开机。

运行机箱和所有服务器（包括新添加的服务器）所需的最高持续电源即最坏情况下的电源需求。如果可以提供该电源量，则不会为任何服务器分配低于最坏情况下所需的电源，并且允许新服务器开机。

如果无法满足最坏情况下的电源需求，则会降低较低优先级服务器的电源，直到能够为新服务器节省出足够的电源为止。

表 9-2 说明了当新服务器在上述场景中打开电源时 CMC 会采取的操作。

表 9-2. 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	最大数量
否	执行节能： • 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	最大数量 不允许

如果一个 PSU 出现故障，会导致不严重运行状况，并生成 PSU 故障事件。拆下 PSU 时，会生成 PSU 拆下事件。

如果任一事件导致冗余丢失，根据电源分配，将生成*冗余掉失*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，服务器的性能将降低，在最坏情况下，服务器可能会断电。在这两种条件下都以相反优先级的顺序进行，也就是优先权较低的服务器先断电。

表 9-3 说明应用各种 PSU 冗余配置后固件对 PSU 断电或卸载的固件响应。

表 9-3. PSU 故障或卸载对机箱的影响

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。
无冗余	已禁用	如果需要，可以减少为优先级较低的服务器分配的电源。
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 故障或卸载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 故障或卸载造成的电源预算损失。
无冗余	已启用	如果需要，可以减少为优先级较低的服务器分配的电源。

PSU 拆下与降级或无冗余策略

当您拆下 PSU 或 PSU 交流电线时，CMC 可能会启动节电功能。CMC 会降低较低优先级服务器的供电，直到机箱中剩余的 PSU 能够支持功耗。如果拆下多个 PSU，CMC 将在拆下第二个 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 可以关闭优先权较低的服务器。

限制

- CMC 不支持对较低优先级的服务器进行*自动*断电，从而为较高优先级的服务器提供足够的电源；但是，它支持执行用户初始化的断电。
- 对 PSU 冗余策略的更改受限于机箱中的 PSU 数量。可以选择 "冗余策略" 中列出的三种 PSU 冗余配置设置中的任意一种。

系统事件记录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。在系统事件记录 (SEL) 中记录条目的有关电源的事件是电源插入和拆卸、电源输入插入和拆卸以及电源输出确认和未确认。 表 9-4 列出与电源设备变化相关的 SEL 条目。

表 9-4. 电源更改的 SEL 事件

电源事件	系统事件记录 (SEL) 条目
插入	电源存在确认
卸下	电源存在未确认
接受交流输入	电源输入掉失未确认
交流输入掉失	电源输入掉失确认
产生直流输出	电源故障未确认
直流输出掉失	电源故障确认
检测到未认可的 110V 工作状态	电源输入低压 (110) 确认
110V 工作认可	电源输入低压 (110) 未确认

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**"AC Redundancy"（交流冗余）**电源策略或**"Power Supply Redundancy"（电源设备冗余）**电源策略的模块化机柜。 表 9-5 列出有关电源冗余策略更改的 SEL 条目。

表 9-5. 电源冗余状态变化的 SEL 事件

电源策略事件	系统事件记录 (SEL) 条目
冗余掉失	冗余掉失确认
重新获取冗余	冗余掉失未确认

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"AC Redundancy"（交流冗余），并且冗余状态指示系统正在运行并且有冗余时，总体电源运行状况一般是**"OK"（良好）**。但是，如果不符合以交流冗余模式运行的条件，冗余状态将是**"No"（否）**，而且总体电源运行状况是**"Critical"（严重）**。这是因为系统无法按照配置的冗余策略运行。

注： 当您将冗余策略更改为交流冗余或将交流冗余更改为其它策略时，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。

配置和管理电源

可以使用基于 Web 的界面和 RACADM 界面管理和配置 CMC 上的电源控制。具体说来，可以：

- 查看电源分配情况、功耗和机箱、服务器和 PSU 的状态
- 配置机箱的系统输入电源上限和冗余策略
- 执行机箱电源控制操作（开机、关机、系统重设、关机后再开机）

查看 PSU 的运行状况

"Power Supply Status"（电源设备状况）页显示与 PSU 与机箱相关的状况和读数。

使用 Web 界面

PSU 的运行状态可以通过两种方法查看：从**"Chassis Status"（机箱状态）**页上的**"Chassis Graphics"（机箱图形）**，或者从**"Power Supply Status"（电源设备状况）**页。**"Chassis Graphics"（机箱图形）**页提供机箱中所有 PSU 的图形概览。

要使用**"Chassis Graphics"（机箱图形）**查看所有 PSU 的运行状况：

1. 登录 CMC Web 界面。
2. 将显示**"Chassis Status"（机箱状态）**页。"**Chassis Graphics"（机箱图形）**的下半部分描述机箱的后视图并包含所有 PSU 的运行状况。PSU 运行状态由 PSU 子图形的颜色表示：
   - 绿色 — PSU 存在，电源打开并且正在与 CMC 通信；不存在不利条件。
   - 琥珀色 — 表示 PSU 出现故障。有关故障状况的详情，请参阅 CMC 日志。
   - 灰色 — PSU 初始化中、PSU 设置为待机时、机箱开机中或 PSU 插入中发生。PSU 存在且电源未打开。不存在不利条件。
3. 将光标停留在单个 PSU 子图形上方将显示相应的文本提示或屏幕提示。文本提示提供有关该 PSU 的其它信息。
4. PSU 子图形超链接到相应的 CMC GUI 页，以便可以立即导航到所有 PSU 的**"Power Supply Status"（电源设备状态）**页。

要使用**"Power Supply Status"（电源设备状况）**查看 PSU 的运行状况：

1. 登录 CMC Web 界面。
2. 选择系统树中的**"Power Supplies"（电源设备）**。随即显示**"Power Supply Status"（电源设备状态）**页。

表 8-6 和 8-7 提供"Power Supply Status"（电源设备状况） 页中所提供信息的说明。

表 9-6. 电源设备

项目	说明		
"Name"（名称）	显示电源设备名称：PS-[n]，其中 [n] 是电源设备编号。		
"Present"（存在）	表示 PSU 是**"Present"（存在）**还是**无**。		
运行状况		"OK"（良好）	指示 PSU 存在并且与 CMC 通信。在 CMC 和电源之间通信失败的情况下，CMC 无法获得或显示 PSU 的运行状况。
		"Warning"（警告）	表示仅发出了警告警报，必须采取更正措施。如果没有采取纠正措施，将可能发生影响机箱完整性的严重电源故障。
		"Severe"（严重）	指示至少为电源发出了一个故障警报。严重状况表示机箱上发生电源故障，**必须立即采取补救措施**。
"Power Status"（电源状况）	显示电源设备的电源状态（以下之一）：**"Initializing"（正在初始化）**、**"Online"（联机）**、**"Stand By"（待机）**、**"In Diagnostics"（诊断中）**、**"Failed"（故障）**、**"Offline"（脱机）**、**"Unknown"（未知）**或**"Absent"（缺失）**。		
容量	显示以瓦特为单位的电源容量。		

表 9-7. 系统电源状况

项目	说明
"Overall Power Health"（总体电源运	显示整个机箱的电源管理运行状况（**"OK"[良好]**、**"Non-Critical"[不严重]**、**"Critical"[严重]**、**"Non-Recoverable"[不可恢**

行状况）	**复]、"Other"[其它]、"Unknown"[未知]**）。
系统电源状况	显示机箱的电源状态（**"On"[开]** 、**"Off"[关]**、**"Powering On"[正在开机]**、**"Powering Off"[正在关机]**）。
"Redundancy"（冗余）	显示电源设备冗余状态。值包括： **"No"（否）**：电源设备并非冗余。 **"Yes"（是）**：完全冗余有效。

使用 RACADM

打开到 CMC 的串行/远程登录/SSH 文本控制台，登录并键入：

```
racadm getpminfo
```

有关 **getpminfo** 的详情（包括输出详情），请参阅 Dell 支持网站 **support.dell.com** 上的《*Chassis Management Controller Administrator Reference Guide*》。

查看功耗状态

CMC 在**"Power Consumption Status"（功耗状态）**页上提供整个系统的实际输入功耗。

使用 Web 界面

注： 要执行电源管理操作，必须具有**机箱配置管理员**权限。

1. 登录 CMC Web 界面。
2. 在系统树中选择**"Chassis Overview"**（机箱概览）。
3. 单击**"Power"（电源）**→**"Power Consumption"（功耗）**。随即出现**"Power Consumption"（功耗）**页。

表 9-8 到 表 9-11 说明**"Power Consumption"（功耗）**页中显示的信息。

注： 您还可以在**"System"（系统）**树 →**"Status"（状态）**选项卡中的**"Power Supplies"（电源设备）**下查看电源冗余状态。

使用 RACADM

打开到 CMC 的串行/远程登录/SSH 文本控制台，登录并键入：

```
racadm getpminfo
```

表 9-8. 实时电源统计信息

项目	说明
系统输入功率	表示从 PSU 的交流输入端测量得到的机箱中所有模块电流累积交流功耗。系统输入功率的值同时用瓦特和 BTU/h 为单位表示。
系统峰值功率	显示自上次清除该值后最大系统级别输入功耗。此属性使您能够按系统（机箱和模块）跟踪一段时间内记录的最大功耗。单击表下方的**"Reset Peak/Min Power Statistics"（重设峰值/最小电源统计信息）**按钮重设该值。系统峰值功率的值同时用瓦特和 BTU/h 为单位表示。
系统峰值功耗开始时间	显示上次清除系统峰值功耗值时记录的日期和时间。时间戳以 **hh:mm:ss MM/DD/YYYY** 格式显示，其中 **hh** 代表小时 (0-24)、**mm** 代表分钟 (00-60)、**ss** 代表秒钟 (00-60)、**MM** 代表月 (1-12)、**DD** 代表天 (1-31)，而 **YYYY** 代表年。可以使用**"Reset Peak/Min Power Statistics"（重设峰值/最小电源统计信息）**按钮重设该值，并且当 CMC 重设或故障转移后也将重设该值。
"Peak System Power Timestamp"（系统峰值功耗时间戳）	出现记录时间段内系统峰值功耗时的日期和时间。时间戳以 **hh:mm:ss MM/DD/YYYY** 格式显示，其中 **hh** 代表小时 (0-24)、**mm** 代表分钟 (00-60)、**ss** 代表秒数 (00-60)、**MM** 代表月 (1-12)、**DD** 代表日 (1-31)、**YYYY** 代表年。
系统最低功耗	显示自用户上次清除该值之后系统级别最低交流功耗（以瓦特为单位）。此属性使您能够按系统（机箱和模块）跟踪一段时间内记录的最低功耗。单击表下方的**"Reset Peak/Min Power Statistics"（重设峰值/最小电源统计信息）**按钮重设该值。系统最低功耗的值同时用瓦特和 BTU/h 为单位表示。可以使用**"Reset Peak/Min Power Statistics"（重设峰值/最小电源统计信息）**按钮重设该值，并且当 CMC 重设或发生故障后也将重设该值。
系统最低功耗开始时间	显示上次清除系统最低功耗值时记录的日期和时间。时间戳以 **hh:mm:ss MM/DD/YYYY** 格式显示，其中 **hh** 代表小时 (0-24)、**mm** 代表分钟 (00-60)、**ss** 代表秒钟 (00-60)、**MM** 代表月 (1-12)、**DD** 代表天 (1-31)，而 **YYYY** 代表年。可以使用**"Reset Peak/Min Power Statistics"（重设峰值/最小电源统计信息）**按钮重设该值，并且当 CMC 重设或发生故障后也将重设该值。
系统最低功耗时间戳	显示当记录期间出现系统最低功耗时记录的日期和时间。时间戳格式与**"Peak System Power Timestamp"（系统峰值功耗时间戳）**相同。
系统空闲功耗	显示系统处于空闲状态时机箱的大约功耗。空闲状态定义为电源打开时机箱所处的状态，并且在空闲状态时所有模块都会消耗电源。*这是估计值而不是测量值。* 根据分配给机箱基础设施组件（I/O 模块、风扇、iKVM、iDRAC 控制器和前面板 LCD）的累计电源，以及所有分配电源且处于电源打开状态中所有服务器的最低功率进行计算。系统空闲功耗的值同时用瓦特和 BTU/h 为单位表示。

系统潜在功耗	显示当机箱在最大功耗条件下工作时的大约功耗。最大功耗定义为当机箱电源打开且所有模块都处于最大功耗时的功耗。*这是从系统配置的历史总功耗得出的估计值，而不是测量值*。计算依据的是分配给机箱基础设施组件（输入/输出模块、风扇、iKVM、iDRAC 控制器和前面板 LCD）的累计电源，以及分配了电源且处于开机状态中的所有服务器的最大电源需求。系统潜在功耗的值同时用瓦特和 BTU/h 为单位表示。
系统输入电流读数	根据机箱中各个 PSU 模块的输入电流消耗量总和，显示机箱的总计输入电流消耗量。系统输入电流读数以 Amps（安培）为单位表示。

表 9-9. 实时能耗统计状态

项目	说明
系统能耗	表示从电源输入端测量得到的机箱中所有模块电流累积能耗。该值以 KWh 为单位表示，并且是累积值。
系统能耗开始时间	显示上次清除系统能耗值并开始新的测量周期时记录的日期和时间。时间戳以 **hh:mm:ss MM/DD/YYYY** 格式显示，其中 **hh** 代表小时（0-24）、**mm** 代表分钟（00-60）、**ss** 代表秒钟（00-60）、**MM** 代表月（1-12）、**DD** 代表天（1-31）而 **YYYY** 代表年。使用**"Reset Energy Statistics"（重设能耗统计信息）**按钮重设该值，但 CMC 重设或发生故障后仍将保留该值。
系统能耗时间戳	显示计算系统能耗时的日期和时间。时间戳以 **hh:mm:ss MM/DD/YYYY** 格式显示，其中 **hh** 代表小时（0-24）、**mm** 代表分钟（00-60）、**ss** 代表秒钟（00-60）、**MM** 代表月（1-12）、**DD** 代表天（1-31）而 **YYYY** 代表年。

表 9-10. 系统电源状况

项目	说明
"Overall Power Health"（总体电源运行状况）	指示机箱电源子系统的运行状况： • 绿色对勾图标，**"OK"（良好）** • 黄色惊叹号图标，**"Non-Critical"（不严重）** • 红色 X 图标，**"Critical"（严重）**
系统电源状况	显示机箱的电源状态（**"On"[开]**、**"Off"[关]**、**"Powering On"[正在开机]**、**"Powering Off"[正在关机]**）。
"Redundancy"（冗余）	显示冗余状态。有效值为： **No** — PSU 不冗余 **Yes** — 完全冗余有效

表 9-11. 服务器模块

项目	说明
插槽	显示服务器模块的位置。**"Slot"（插槽）**是在机箱中按服务器模块位置对其进行标识的序列号 (1-16)。
"Name"（名称）	显示服务器名称。用户可以重新定义服务器名称。
"Present"（存在）	显示插槽中是否存在服务器（**"Yes"[存在]** 或**"No"[无]**）。如果该字段显示**"Extension of #"（# 的扩展）**（其中 # 为 1-8），则后面的编号是多插槽服务器的主要插槽。
实际（交流）	服务器实际功耗的实时测量。以交流瓦特显示的测量值。
累计功率开始时间	自**"Start Time"（开始时间）**字段中显示的时间开始，服务器消耗的累计功率的实时测量结果。以千瓦小时 (kWh) 为单位表示测量值。
峰值功耗时间戳	显示服务器一次消耗的峰值功率。在**"Time Stamp"（时间戳）**字段中记录峰值功耗发生的时间。测量值以瓦特为单位显示。

查看电源预算状况

CMC 在**"Power Budget Status"（电源预算状态）**页上提供电源子系统的电源状态概览。

使用 Web 界面

注： 要执行电源管理操作，必须具有**机箱配置管理员**权限。

1. 登录 CMC Web 界面。
2. 在系统树中选择**"Chassis Overview"（机箱概览）**。
3. 单击**"Power"（电源）→ "Budget Status"（预算状况）**。

显示 **Power Budget Status（电源预算状态）**页面。

表 9-12 到 表 9-15 说明**"Power Budget Status"（电源预算状况）**页中显示的信息。

有关为该信息配置设置的信息，请参阅 "配置电源预算和冗余"。

使用 RACADM

打开到 CMC 的串行/远程登录/SSH 文本控制台，登录并键入：

```
racadm getpbinfo
```

有关 **getpbinfo** 的详情（包括输出详情），请参阅《*Chassis Management Controller Administrator Reference Guide*》中的 **getpbinfo** 命令部分。

表 9-12. 系统电源策略配置

项目	说明
"System Input Power Cap"（系统输入功率上限）	显示用户配置的整个系统（机箱、CMC、服务器、输入/输出模块、电源设备、iKVM 和风扇）的最大功耗限制。CMC 将通过降低服务器电源分配或关闭较低优先级服务器模块的电源强制实施该限制。系统输入功率上限的值以瓦、BTU/h 和百分比为单位显示。 如果机箱功耗超过**"System Input Power Cap"（系统输入功率上限）**，则较低优先级服务器的性能将降低，直到总功耗降到上限水平之下。 在服务器都设置为**相同**优先级的情况下，将根据服务器插槽编号顺序选择采取降低服务器电源或关闭电源操作的服务器。例如，首先选择插槽 1 中的服务器，最后选择插槽 16 中的服务器。
"Redundancy Policy"（冗余策略）	显示当前的冗余配置：**"AC Redundancy"（交流冗余）**、**"Power Supply Redundancy"（电源设备冗余）**和**"No Redundancy"（无冗余）**。 **"AC Redundancy"（交流冗余）**— 电源输入在所有 PSU 之间负载平衡。应将所有 PSU 中的一半连接到一个交流电网，另一半连接到另一个电网。当系统以"AC Redundancy"（交流冗余）模式处于最佳运行状态时，电量在所有活动电源设备上进行负载平衡。在交流电网发生故障的情况下，运作交流电网上的 PSU 将不间断接管。 **"Power Supply Redundancy"（电源设备冗余）**— 保留机箱中定额最高的 PSU 的容量，以确保任意一个 PSU 出现故障都不会导致服务器模块或机箱断电。 **"Power Supply Redundancy"（电源设备冗余）**不会使用所有 6 个 PSU；它使用足够数目的 PSU 保证任何一个 PSU 故障时其余 PSU 仍可继续向机箱供电。如果启用 DPSE，则其他 PSU 可处于待机模式。 **"No Redundancy"（无冗余）** — 所有活动的 PSU 足以为整个机箱供电，包括机箱、服务器、I/O 模块、iKVM 和 CMC。如果启用 DPSE，则其他 PSU 可处于待机模式。 △ **小心： "No Redundancy"（无冗余）一次仅使用最低要求数目的 PSU，无备用。任意一个使用中的 PSU 发生故障都会导致服务器模块断电或损失数据。**
动态电源设备接入	显示是启用还是禁用**"Dynamic Power Supply Engagement"（动态电源设备接入）**。启用该功能将使 CMC 能够根据系统电源需求和设置的冗余策略将未使用的 PSU 置于待机模式。将未使用的 PSU 置于待机模式能够提高联机 PSU 的利用率和效率，从而省电。

表 9-13. 电源预算

项目	说明
"System DC Max Power Capacity"（系统最大直流电源容量）	电源设备能够为系统提供的最大可用输入电源（以瓦为单位）。
"Input Redundancy Reserve"（输入冗余备用）	表示可以用于交流电网或电源设备 (PSU) 故障情况中的备用冗余电源量（以瓦特为单位）。 当机箱配置为在**"AC Redundancy"（交流冗余）**模式下工作时，**"Input Redundancy Reserve"（输入冗余备用）**就是在发生交流电网故障时可以使用的备用电源量。 当机箱配置为在**"Power Supply Redundancy "（电源设备冗余）**模式下运行时，**"Input Redundancy Reserve"（输入冗余备用）**就是在发生 PSU 故障时可以使用的备用电源量。
"Input Power Allocated to Servers"（分配给服务器的输入电源）	显示 CMC 根据其配置分配给服务器的累积输入功率（以瓦特为单位）。
"Input Power Allocated to Chassis Infrastructure"（分配给机箱基础设施的输入电源）	显示（以瓦为单位）CMC 分配给机箱基础设施（风扇、IO 模块、iKVM、CMC、服务器上的待机 CMC 和 iDRAC）的累积输入功率。
"Total Input Power Available for Allocation"（可用于分配的输入电源总数）	显示仍可用于分配的机箱电源总功率（以瓦特为单位）。
"Standby Input Power Capacity"（待机输入电源容量）	显示可以用于电源设备故障或从系统中卸载电源设备的情况中待机输入电源的容量（以瓦为单位）。当系统有多个电源设备时且已启用电源设备动态接入时，该字段可能会显示读数。

	注： 有时可以看到 PSU 处于待机模式，但不提供待机输入电源容量值。在这种情况下，来自该 PSU 的电源累积到**"Total Input Power Available for Allocation"（可用于分配的输入电源总数）**值。

表 9-14. 服务器模块

项目	说明
插槽	显示服务器模块的位置。**"Slot"（插槽）**是在机箱中按服务器模块位置对其进行标识的序列号 (1-16)。
"Name"（名称）	显示服务器名称。服务器名称由用户定义。
"Type"（类型）	显示服务器的类型。
优先级	显示为机箱中服务器插槽分配的电源预算优先级。当根据用户定义的电源限制或者电源或电网故障必须减少或重新分配电源时，CMC 将在计算中使用该值。 **"Priority levels"（优先级）：1（最高）到 9（最低）** 默认：**1** **注：** 服务器插槽优先级与服务器插槽关联 — 而不是与插入插槽的服务器关联。如果将服务器移动到机箱中的不同插槽，与新插槽关联的以前的优先级将确定换位服务器的优先权。
"Power State"（电源状态）	显示服务器的电源状态： ○ **"N/A"（无）：**CMC 尚未确定服务器的电源状态。 ○ **"Off"（关）：**服务器或机箱关闭。 ○ **"On"（开）：**机箱和服务器都打开。 ○ **"Powering On"（电源打开）：**关闭和打开之间的临时状态。当开机操作完成后，电源状态将更改为"On"（开）。 ○ **"Powering Off"（电源关闭）：**打开和关闭之间的临时状态。当关机操作完成后，电源状态将更改为"Off"（关）。
预算分配 - 实际	指示服务器模块的电源预算分配。 • **实际：**每台服务器当前的电源预算分配。

表 9-15. 机箱电源

项目	说明
"Name"（名称）	显示 PSU 的名称，格式为 PS-*n*，其中 *n* 为 PSU 的编号。
"Power State"（电源状态）	显示 PSU 的电源状态 — **"Initializing"（正在初始化）**、**"Online"（联机）**、**"Stand By"（待机）**、**"In Diagnostics"（诊断中）**、**"Failed"（故障）**、**"Unknown"（未知）**或**"Absent"（缺失）**（丢失）。
"Input Volts"（输入电压）	显示电源设备的输入电压。
"Input Current"（输入电流）	显示电源设备的输入电流。
"Output Rated Power"（额定输出电源）	显示电源设备的最大输出电源额定值。

配置电源预算和冗余

CMC 的电源管理服务优化整个机箱（机箱、服务器、IOM、iKVM、CMC 和 PSU）的功耗，并根据需求为不同的模块重新分配电源。

使用 Web 界面

注： 要执行电源管理操作，必须具有**机箱配置管理员**权限。

1. 登录 CMC Web 界面。
2. 在系统树中选择**"Chassis Overview"（机箱概览）**。
3. 单击**"Power"（电源）→"Configuration"（配置）**。

   显示 **Budget/Redundancy Configuration（预算/冗余配置）**页面。
4. 根据需要设置表 9-16 中说明的任意或所有属性。

5. 单击**"Apply"（应用）**保存您所做的更改。

要刷新**"Budget/Redundancy Configuration"（预算/冗余配置）**页上的内容，请单击**"Refresh"（刷新）**。要打印此内容，请单击**"Print"（打印）**。

表 9-16. 可配置的电源预算/冗余属性

项目	说明
"System Input Power Cap"（系统输入功率上限）	系统输入功率上限是系统允许分配给服务器和机箱基础设施的最大交流电源。用户可以为它配置任何**超过** 开机服务器和机箱基础设施所需的最低电源之和的值；配置低于服务器和机箱基础设施所需最低电源的值将会发生故障。 分配给服务器和机箱基础设施的电源可以在用户界面**"Chassis"（机箱）→"Power"（电源）→"Power Budget"（电源预算）**状态页的**"Power Budgeting"（电源预算）**部分下面，或通过 CLI RACADM 公用程序命令 (racadm getpbinfo) 查看。 用户可以关闭一台或多台服务器以降低当前功耗，并为**"System Input Power Cap"（系统输入功率上限）**重新尝试设置较低的值（如果希望），或者只需在打开服务器电源之前配置上限。 要更改该设置，可以使用任何单位输入值。当应用这些更改时，界面会确保提交最后一次更改的单位字段值。 **注：** 有关容量规划的信息，请参阅 **www.dell.com/calc** 的数据中心容量规划工具 (DCCP)。 **注：** 当以瓦特指定值更改时，提交的值将准确反映实际应用的值。但是，当提交的更改是以 BTU/h 或百分比为单位时，提交的值可能不能准确反映实际应用的值。这是因为这些单位将转换为瓦特后再应用；而转化容易出现取舍误差。
"Redundancy Policy"（冗余策略）	该选项允许您选择以下一个选项： • **"No Redundancy"（无冗余）：** 电源为整个机箱供电，包括机箱、服务器、I/O 模块、iKVM 和 CMC。不必储备电源。 **注：** **"No Redundancy"（无冗余）**模式一次仅使用最低要求数目的 PSU。如果安装最低要求数目的 PSU，则无备用可用。如果使用中的三个电源设备之一出现故障，将会导致服务器断电和/或丢失数据。如果存在超过最低要求数目的 PSU，则其他 PSU 可在启用 DPSE 时处于待机模式以提高功效。 • **"Power Supply Redundancy"（电源设备冗余）**：机箱中定额最高的电源设备的容量保留为备用，以确保任意一个电源设备出现故障都不会导致服务器模块或机箱断电（热备份）。 **"Power Supply Redundancy"（电源设备冗余）**模式不可利用所有安装的电源。启用 DPSE 后，如有任何附加电源设备，会将这些电源设备置于待机模式以便提高电源效率。如果机箱的功耗超过额定功耗，**"Power Supply Redundancy"（电源设备冗余）**模式将阻止服务器模块开机。在此模式下，如果**两个**电源设备出现故障，可能会导致机箱中的部分或全部服务器模块断电。在此模式下，不会降低服务器模块的性能。 • **"AC Redundancy"（交流冗余）：**该模式将 PSU 分成两个电网（例如，PSU 1-3 组成电网 1，PSU 4-6 组成电网 2）。一个 PSU 出现故障或一个电网的交流电源断电时，会将冗余状态报告为丢失。
启用动态电源设备接入	选择后启用动态电源管理。在**"Dynamic Engagement"（动态接入）**模式中，电源设备将根据功耗**打开**（联机）或**关闭**（待机），从而优化整个机箱的能耗。 例如，电源预算是 5000 瓦，冗余策略设置为交流冗余模式，并且有六个电源设备。CMC 确定四个电源设备可以管理交流冗余，而其他两个电源处于待机模式。如果新安装的服务器需要额外 2000W 电源，或者必须提高现有系统配置的电源效率，那么两个待机电源设备将接入。
"Disable Chassis Power Button"（禁用机箱电源按钮）	选择后禁用机箱电源按钮。如果选择了此复选框，并且您尝试通过按下机箱电源按钮更改机箱的电源状态，该操作将被忽略。
允许 110 V 交流工作	选择后如果任一电源设备连接到 110 V 交流输入则允许正常工作。有关详情，请参阅"110V PSU 的工作"。
最大节能模式	选择后立即进入最大节能模式。有关详情，请参阅"节能和最大节能模式"。

使用 RACADM

要启用冗余并设置冗余策略：

注： 要执行电源管理操作，必须具有**机箱配置管理员**权限。

1. 打开到 CMC 的串行/远程登录/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 <值>
     ```

     其中<*值*>为**0**（无冗余）、1（交流冗余）、**2**（电源设备冗余）。默认为 0。

例如，以下命令：

```
racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy 1
```

将冗余策略设置为 1。

- 要启用或禁用动态 PSU 接入，请键入：

```
racadm config -g cfgChassisPower -o cfgChassisDynamicPSUEngagementEnable <值>
```

其中<*值*>为**0**（禁用）、1（启用）。默认为 0。

例如，以下命令：

```
racadm config -g cfgChassisPower -o cfgChassisDynamicPSUEngagementEnable 0
```

禁用动态 PSU 接入。

有关机箱电源的 RACADM 命令的信息，请参阅《*CMC Administrator Reference Guide*》中的 **config**、**getconfig**、**getpbinfo** 和 **cfgChassisPower** 部分。

为服务器分配优先级

服务器优先级确定当需要额外电源时，CMC 将从哪台服务器开始节电。

注： 为服务器分配的优先权取决于插槽而不是服务器本身。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权。

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

1. 登录 CMC Web 界面。
2. 在系统树中选择**"Server Overview"（服务器概览）**。随即出现**"Server Status"（服务器状况）**页。
3. 单击**"Power"（电源）**→ **"Server Priority"（服务器优先级）**。

   随即出现**"Server Priority"（服务器优先级）**页，其中列出了机箱中的所有服务器。
4. 为一台、多台或全部服务器选择优先级（1-9，1 代表最高优先权）。默认值为 1。可以为多台服务器设定相同的优先级。
5. 单击**"Apply"（应用）**保存您所做的更改。

使用 RACADM

打开到 CMC 的串行/远程登录/SSH 文本控制台，登录并键入：

```
racadm config -g cfgServerInfo -o cfgServer Priority -i <插槽号> <优先级>
```

其中 <*插槽号*> (1-16) 指代服务器位置，而<*优先级*>为 1-9 之间的值。

例如，以下命令：

```
racadm config -g cfgServerInfo -o cfgServerPriority -i 5 1
```

将插槽 5 中的服务器优先级设置为 1。

设置电源预算

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

1. 登录 CMC Web 界面。
2. 在系统树中选择**"Chassis Overview"（机箱概览）**。随即显示**"Chassis Health"（机箱运行状况）**页。

3. 单击**"Power"（电源）**选项卡。

   随即出现**"Power Consumption Status"（功耗状态）**页。

4. 单击**"Configuration"（配置）**子选项卡。

   随即出现**"Budget / Redundancy Configuration"（预算 / 冗余配置）**页。

5. 在**"System Input Power Cap"（系统输入功率上限）**文本字段键入预算值，最高 11637 瓦特。

   注： 机箱功率限值为 11637 瓦特。如果尝试设置超过机箱电源容量的交流电源预算值，CMC 将显示故障信息。

   注： 当以瓦特指定值更改时，提交的值将准确反映实际应用的内容。但是，当提交的更改是以 BTU/h 或百分比为单位时，提交的值可能不能准确反映实际应用的内容。这是因为这些单位将转换为瓦特后再应用；而转化容易出现取舍误差。

6. 单击**"Apply"（应用）**保存您所做的更改。

使用 RACADM

打开到 CMC 的串行/远程登录/SSH 文本控制台，登录并键入：

```
racadm config -g cfgChassisPower -o cfgChassisPowerCap <值>
```

其中<值>是 2715-11637 的数字，代表以瓦特为单位的最大电源限制。默认值为 11637。

例如，以下命令：

```
racadm config -g cfgChassisPower -o cfgChassisPowerCap 5400
```

将最大电源预算设置为 5400 瓦特。

注： 机箱功率限值为 11637 瓦特。如果尝试设置超过机箱电源容量的交流电源预算值，CMC 将显示故障信息。

减少服务器电源以维持电源预算

当为了将系统功耗保持在用户配置的**"System Input Power Cap"（系统输入电源上限）**内而需要额外电源时，CMC 将减少分配给较低优先级服务器的电源。例如，当接入新服务器时，CMC 可能会减少低优先权服务器的电源，以便为新服务器提供更多电源。如果减少分配给较低优先权服务器的电源之后，电源量仍然不足，CMC 将降低服务器的性能，直到能够为新服务器供电而释放出足够的电源为止。

CMC 在两种情况下会减少分配给服务器的电源：

- 总体功耗超过可配置的**"System Input Power Cap"（系统输入功率上限）**（请参阅 "设置电源预算"。）
- 在非冗余配置中出现电源故障

有关为服务器分配优先级的信息，请参阅 "执行机箱电源控制操作"。

执行机箱电源控制操作

注： 要执行电源管理操作，必须具有**机箱配置管理员**权限。

注： 电源控制操作将影响整个机箱。有关 IOM 上的电源控制操作的信息，请参阅 "执行 IOM 电源控制操作"。有关服务器上的电源控制操作的信息，请参阅 "执行服务器电源控制操作"。

CMC 能够远程执行几项对整个机箱（机箱、服务器、IOM、iKVM 和 PSU）的电源管理操作（如按顺序关机）。

使用 Web 界面

1. 登录 CMC Web 界面。
2. 在系统树中选择**"Chassis Overview"（机箱概览）**。
3. 单击**"Power"（电源）**选项卡。

   随即出现**"Power Consumption Status"（功耗状态）**页。

4. 单击**"Control"（控制）**子选项卡。

随即出现**"Chassis Power Control"（机箱电源控制）**页。

5. 单击相应单选按钮选择以下**"Power Control Operations"（电源控制操作）**之一：

- **"Power On System"（打开系统电源）**— 打开机箱电源（相当于在机箱电源**关闭**时按下电源按钮）。如果机箱电源已经**打开**，则该选项处于禁用状态。

注： 该操作将打开机箱和其他子系统（服务器上的 iDRAC、IOM 和 iKVM）的电源。服务器将无法开机。

- **"Power Off System"（关闭系统电源）**— 关闭机箱电源。如果服务器已经**"OFF"（关闭）**，则禁用该选项。

注： 此操作关闭机箱电源（机箱、服务器、IOM、iKVM 和电源设备）。CMC 仍然保持电源打开，但处于虚拟待机状态，电源设备和风扇为该状态中的 CMC 提供冷却。电源设备还将为低速运转的风扇提供电源。

- **"Power Cycle System (cold boot)"（系统关机后再开机[冷引导]）**— 关机然后重新引导服务器（冷引导）。如果服务器已经**"OFF"（关闭）**，则禁用该选项。

注： 此操作将关闭电源，然后重新引导整个机箱（机箱、配置为始终打开电源的服务器、IOM、iKVM 和电源设备）。

- **"Reset CMC"（重设 CMC）**— 在不关机的情况下重设 CMC（温引导）。（如果 CMC 已经关机，则禁用该选项）。

注： 此操作仅重设 CMC。不影响其它组件。

- **"Non-Graceful Shutdown"（非正常关机）**— 此操作强制整个机箱（机箱、服务器、IOM、iKVM 和电源设备）非正常关机。该操作不会在关闭电源之前尝试正常关闭服务器的操作系统。

- 单击**"Apply"（应用）**。对话框会显示要求确认。
- 单击**"OK"（确定）**执行电源管理操作（例如，使系统重设）。

使用 RACADM

打开到 CMC 的串行/远程登录/SSH 文本控制台，登录并键入：

```
racadm chassisaction -m chassis <操作>
```

其中<*操作*>为"powerup"（开机）、"powerdown"（关机）、"powercycle"（关机后再开机）、"nongraceshutdown"（非正常关机）或"reset"（重设）。

执行 IOM 电源控制操作

可以远程对单个 IOM 执行重设或关机后再开机操作。

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 Web 界面

1. 登录 CMC Web 界面。
2. 选择**"I/O Modules Overview"（输入/输出模块概览）**。

   将显示"**I/O Modules Status**"（I/O 模块状态）页。
3. 单击**"Power"（电源）**选项卡。

   随即出现**"Power Control"（电源控制）**页。
4. 从列表中 IOM 旁边的下拉菜单中选择想要执行的操作（**"reset"（重设）** 或**"power cycle"（关机后再开机）**）。
5. 单击**"Apply"（应用）**。

   对话框会显示要求确认。
6. 单击**"OK"（确定）**执行电源管理操作（例如，使 IOM 关机后再开机）。

使用 RACADM

打开到 CMC 的串行/远程登录/SSH 文本控制台，登录并键入：

```
racadm chassisaction -m switch<n> <操作>
```

其中 *<n>* 是数字 1-6，并指定 IOM（A1、A2、B1、B2、C1、C2），*<操作>* 表示您要执行的操作："powercycle"（**关机后再开机**）或"reset"（**重设**）。

执行服务器电源控制操作

注： 要执行电源管理操作，必须具有**机箱配置管理员**权限。

CMC 使您能够对机箱中的单独服务器远程执行几项电源管理操作，例如按顺序关机。

使用 Web 界面

1. 登录 CMC Web 界面。
2. 展开系统树中的**"Server Overview"（服务器概览）**，然后选择希望执行电源控制操作的服务器。随即显示**"Server Status"（服务器状态）**页。
3. 单击**"Power"（电源）**选项卡。

   随即显示**"Server Power Management"（服务器电源管理）**页。
4. **"Power Status"（电源状态）**显示服务器的电源状态（以下某个值）：
   - **无 —** CMC 尚未确定服务器的电源状态。
   - **关 —** 服务器关闭或机箱关闭。
   - **开** — 机箱和服务器都打开。
   - **正在开机 —** 关闭和打开之间的临时状态。当成功地完成操作后，**电源状态**将显示**开**。
   - **正在关机** - 打开和关闭之间的临时状态。当成功地完成操作后，**电源状态**将显示**关**。
5. 通过单击单选按钮选择以下**电源控制操作**中的一项：
   - **"Power On System"（打开系统电源）**— 打开系统电源（相当于系统电源关闭时按电源按钮）。如果服务器已经打开电源，则禁用该选项。
   - **"Power Off System"（关闭系统电源）**— 关闭系统电源（与系统电源打开时按电源按钮等效）。
   - **"Graceful Shutdown"（正常关闭系统）** — 关机并重新引导服务器。
   - **"Reset System (warm boot)"（重设系统 [温引导]）**— 在不关机的情况下重新引导服务器。如果服务器已关机则该选项禁用。
   - **"Power Cycle System (cold boot)"（系统关机后再开机[冷 引导]）**— 关机然后重新引导服务器。如果服务器已关机则该选项禁用。
6. 单击**"Apply"（应用）**。对话框会显示要求确认。
7. 单击**"OK"（确定）**执行电源管理操作（例如，使服务器重设）。

注： 可以从**"Servers"（服务器）**→**"Power"（电源）**→**"Control"（控制）**页对多台服务器执行所有电源控制操作。

使用 RACADM

打开到 CMC 的串行/远程登录/SSH 文本控制台，登录并键入：

```
racadm serveraction -m <模块> <操作>
```

其中*<模块>*根据机箱中的插槽号（服务器-1 到 服务器-16）指定服务器，而*<操作>*表示想要执行的操作："powerup"（开机）、"powerdown"（关机）、"powercycle"（关机后再开机）或"hardreset"（硬重设）。

110V 工作

部分电源设备 (PSU) 型号能够在 220V 主电源以及 110V 主电源下工作。110V 电源功率有限；因此在检测到 110V 连接时，机箱不会批准额外的服务器功率申请，直到用户通过改变功率配置属性而认可在 110V 下工作。用户必须在认可前确认使用的 110V 电路能够为机箱配置提供所需功率。认可后，机箱会授予未来所有相应的服务器功率申请，并使用所有可用电源容量。

用户可在初次安装后可随时从 GUI 或 RACADM 重设 110V 认可。检测到和卸下 110V 电源时会在 SEL 日志中记录电源设备条目。用户认可和取消认可时也会在 SEL 中记录。

当机箱处于 110V 下且用户未认可 110V 时，整体功率运行状况至少为不严重状态。不严重状态下 GUI 主界面上显示"警告"图标。

不支持 110V 和 220V 的混合操作。如果 CMC 检测到使用两种电压，则会选择一个电压并关闭连接到另一个电压的电源设备并将其标记为故障。

故障排除

有关电源和电源相关问题的故障排除，请参阅 "故障排除和恢复"。

目录

目录

使用 RACADM 命令行界面

Dell Chassis Management Controller Firmware 版本 3.0 用户指南

RACADM 提供一组可以通过基于文本的界面配置和管理 CMC 的命令。RACADM 可以通过远程登录/SSH 或串行连接访问、通过 iKVM 上的 Dell CMC 控制台访问、或者使用安装在 Management Station 上的 RACADM 命令行界面远程访问。

RACADM 接口的分类如下：

注： 远程 RACADM 包含在 *Dell Systems Management Tools and Documentation DVD* 中，并已安装在 Management Station 上。

- 远程 RACADM — 允许在 Management Station 上带有 **-r** 选项和 CMC 的 DNS 名称或 IP 地址执行 RACADM 命令。
- 固件 RACADM — 允许使用远程登录、SSH、串行连接或 iKVM 登录到 CMC。使用固件 RACADM 后，可运行作为 CMC 固件一部分的 RACADM 实现。

可以在脚本中使用远程 RACADM 命令以配置多个 CMC。CMC 不支持脚本，所以无法直接在 CMC 上运行脚本。有关配置多个 CMC 的详情，请参阅 "在多个机箱中配置多个 CMC"。

使用串行、远程登录或 SSH 控制台

可以通过串行或远程登录/SSH 连接，或者 iKVM 上的 Dell CMC 控制台登录到 CMC。要配置串行或远程访问 CMC，请参阅 "配置 CMC 使用命令行控制台"。表 4-2 中列出了常用的子命令选项。RACADM 子命令的完整列表在《*Dell Chassis Management Controller 管理员参考指南*》中的"RACADM 子命令"一章列出。

登录 CMC

配置完 Management Station 终端仿真软件和受管节点 BIOS 后，执行下列步骤登录到 CMC：

1. 使用 Management Station 终端仿真软件连接到 CMC。
2. 键入 CMC 用户名和密码，然后按 <Enter>。

   随后登录到 CMC。

启动文本控制台

可以使用远程登录或 SSH 通过网络、串行端口，或 iKVM 上的 Dell CMC 控制台登录到 CMC。打开远程登录或 SSH 会话，连接并登录到 CMC。

有关通过 iKVM 连接到 CMC 的信息，请参阅 "使用 iKVM 模块"。

使用 RACADM

可以通过串行、远程登录或 SSH 控制台命令提示符或通过正常的命令提示符远程运行 RACADM 子命令。

使用 RACADM 子命令配置 CMC 属性并执行远程管理任务。要显示 RACADM 子命令列表，请键入：

```
racadm help
```

当不带选项或子命令运行时，RACADM 将显示语法信息和如何访问子命令及帮助的说明。要列出单独子命令的语法和命令行选项，请键入：

```
racadm help <子命令>
```

RACADM 子命令

表 4-1 提供了 RACADM 中常用子命令的简要列表。有关 RACADM 子命令的完整列表（包括语法和有效条目），请参阅《*Dell Chassis Management Controller 管理员参考指南*》中的"RACADM 子命令"一章。

注： **connect** 命令有两种形式 — RACADM 命令和 CMC 内置命令。**exit**、**quit** 和 **logout** 命令是 CMC 内置命令，不是 RACADM 命令。这些命令都不能在远程 RACADM 中使用。有关使用这些命令的详情，请参阅 "使用 Connect 命令连接到服务器或 I/O 模块"。

表 4-1. RACADM 子命令

命令	说明
help	列出 CMC 子命令说明。
help <*子命令*>	列出指定子命令的用法摘要。
?	列出 CMC 子命令说明。
?<*子命令*>	列出指定子命令的用法摘要。
arp	显示 ARP 表的内容。ARP 表条目不能被添加或删除。
chassisaction	在机箱、交换机和 KVM 上执行开机、关机、重设和关机后再开机操作。
closessn	关闭会话。
clrraclog	清除 CMC 日志并创建单独输入项，表明清除日志的用户和时间。
clrsel	清除系统事件日志条目。
cmcchangeover	在冗余 CMC 环境中将 CMC 的状态从活动更改为待机，或者相反。
config	配置 CMC。
connect	连接到服务器或 I/O 模块的串行控制台。请参阅 "使用 Connect 命令连接到服务器或 I/O 模块" 获得使用 connect 子命令的帮助。
deploy	通过指定需要的属性部署服务器。
feature	显示活动功能和功能取消激活。
featurecard	显示功能卡状态信息。
fwupdate	执行系统组件固件更新并显示固件更新状态。
getassettag	显示机箱的资产标签。
getchassisname	显示机箱名称。
getconfig	显示当前 CMC 配置属性。
getdcinfo	显示常规输入/输出模块和子卡误配置信息。
getflexaddr	显示每个插槽/结构基础上已启用/已禁用的弹性地址。如果使用 -i 选项，该命令将显示特定插槽的 WWN 和 MAC 地址。
getioinfo	显示常规输入/输出模块信息。
getkvminfo	显示关于 iKVM 的信息。
getled	显示模块的 LED 设置。
getmacaddress	显示服务器的 MAC 地址。
getmodinfo	显示模块配置和状况信息。
getniccfg	显示控制器的当前 IP 配置。
getpbinfo	显示电源预算状况信息。
getpminfo	显示电源管理状况信息。
getraclog	显示 CMC 日志。
getractime	显示 CMC 时间。
getredundancymode	显示 CMC 的冗余模式。
getsel	显示系统事件日志（硬件日志）。
getsensorinfo	显示关于系统传感器的信息。
getslotname	显示机箱中插槽的名称。
getssninfo	显示关于活动会话的信息。
getsvctag	显示服务标签。
getsysinfo	显示一般 CMC 和系统信息。
gettracelog	显示 CMCtrace 日志。如果与 -i 选项一同使用，则该命令显示 CMC 跟踪日志中的条目数。
getversion	显示当前软件版本、型号信息以及是否可更新设备。
ifconfig	显示当前 CMC 的 IP 配置。
krbkeytabupload	上载 Kerberos Keytab 到 CMC。
netstat	显示路由表和当前连接。
ping	验证是否可以使用当前路由表内容从 CMC 访问目标 IPv4 地址。
ping6	验证是否可以使用当前路由表内容从 CMC 访问目标 IPv6 地址。
racdump	显示全面的机箱状态和配置状态信息，以及历史事件日志。用于后期部署配置验证和调试会话过程。
racreset	重设 CMC。
racresetcfg	将 CMC 重设为默认配置。
remoteimage	连接、断开连接或部署远程服务器上的介质文件。

serveraction	在 Managed System 上执行电源管理操作。
setassettag	设置机箱的资产标签。
setchassisname	设置机箱名称。
setflexaddr	当机箱上的 FlexAddress 功能激活时，启用/禁用特定插槽/结构上的 FlexAddress。
setled	设置模块的 LED 设置。
setniccfg	设置控制器的 IP 配置。
setractime	设置 CMC 时间。
setslotname	设置机箱中插槽的名称。
setsysinfo	设置机箱的名称和位置。
sshpkauth	上载最多 6 个不同的 SSH 公共密钥、删除现有密钥和查看 CMC 中已经存在的密钥。
sslcertdownload	下载认证机构的签名证书。
sslcertupload	上载认证机构的签名证书或服务器证书到 CMC。
sslcertview	查看 CMC 中的认证机构的签名证书或服务器证书。
sslcsrgen	生成并下载 SSL CSR。
sslresetcfg	通过 CMC Web GUI 重新生成自签证书。
testemail	强制 CMC 通过 CMC NIC 发送电子邮件。
testfeature	允许您验证特定功能的配置参数。例如，它支持使用简单验证方法（用户名和密码）检测 Active Directory 配置，或使用 Kerberos 验证方法（单一登录或 Smart Card 登录）检测 Active Directory 配置。
testtrap	强制 CMC 通过 CMC 网络接口发送 SNMP。
traceroute	打印 IPv4 信息包到达网络节点所经过的路由。
traceroute6	打印 IPv6 信息包到达网络节点所经过的路由。

远程访问 RACADM

表 4-2. 远程 RACADM 子命令选项

选项	说明
-r <*racIpAddr*> -r <*racIpAddr*>:<*端口*>	指定控制器的远程 IP 地址。 如果 CMC 端口号不是默认端口 (443)，请使用<*端口号*>。
-i	指示 RACADM 向用户交互查询用户名和密码。
-u <*用户名*>	指定用于验证命令事务处理的用户名。如果使用 -u 选项，则必须使用 -p 选项，并且不允许使用 -i 选项（交互）。
-p <*密码*>	指定用于验证命令事务处理的密码。如果使用 -p 选项，则不允许使用 -i 选项。

要远程访问 RACADM，键入以下命令：

```
racadm -r <CMC IP 地址> -u <用户名> -p <密码> <子命令> <子命令选项>
```

```
racadm -i -r <CMC IP 地址> <子命令> <子命令选项>
```

注： **-i** 选项指示 RACADM 交互式提示用户名和密码。如果不使用 **-i** 选项，则必须在命令中使用 **-u** 和 **-p** 选项提供用户名和密码。

例如：

```
racadm -r 192.168.0.120 -u root -p calvin getsysinfo
```

```
racadm -i -r 192.168.0.120 getsysinfo
```

如果 CMC 的 HTTPS 端口号更改为非默认端口 (443) 的自定义端口，则必须使用下面的语法：

```
racadm -r <CMC IP 地址>:<端口> -u <用户名> -p <密码> <子命令> <子命令选项>
```

```
racadm -i -r <CMC IP 地址>:<端口> <子命令> <子命令选项>
```

启用和禁用 RACADM 远程功能

注： Dell 建议在机箱上运行这些命令。

CMC 上的 RACADM 远程功能默认情况下为启用。在以下命令中，**-g** 指定对象所属的配置组，**-o** 指定要配置的配置对象。

要禁用 RACADM 远程功能，请键入：

```
racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 0
```

要重新启用 RACADM 远程功能，请键入：

```
racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 1
```

远程使用 RACADM

注： 使用 RACADM 远程功能前请配置 CMC 上的 IP 地址。有关设置 CMC 的详情，请参阅 "安装和设置 CMC"。

RACADM 控制台远程选项 (-r) 允许从远程控制台或 Management Station 连接到 Managed System 并执行 RACADM 子命令。要使用远程功能，您需要有效的用户名（-u 选项）和密码（-p 选项），以及 CMC 的 IP 地址。

尝试远程访问 RACADM 之前，请确认具备相应的权限。要显示用户权限，请键入：

```
racadm getconfig -g cfguseradmin -i n
```

其中 *n* 为用户 ID (1-16)。

如果不知道用户 ID，请尝试使用不同的 *n* 值。

注： 仅支持在 Management Station 上通过支持的浏览器使用 RACADM 远程功能。有关详情，请参阅 Dell 支持网站 **support.dell.com / manuals** 上的《*Dell 系统软件支持值表*》中的"支持的浏览器"一节。

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入权限。例如：

```
racadm getconfig -f <文件名> -r <IP 地址>
```

或

```
racadm sslcertupload -t 1 -f c:\cert\cert.txt
```

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没有设置，配置组将不会保存为配置文件的一部分。如果需要将这些配置组复制到其它 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` 命令之后手动将缺少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

RACADM 错误信息

关于 RACADM CLI 错误信息，请参阅 "故障排除"。

使用 RACADM 配置 CMC

注： 为了首次配置 CMC， 必须以用户 **root** 登录才能在远程系统上执行 RACADM 命令。将创建另一个用户，并为他或她分配配置 CMC 的权限。

CMC Web 界面是配置 CMC 的最快方法（请参阅 "使用 CMC Web 界面"）。但是，如果选择 CLI 或脚本配置或需要配置多个 CMC，请使用 Management Station 上随 CMC 代理安装的远程 RACADM。

配置 CMC 网络属性

在配置 CMC 之前，必须首先配置 CMC 网络设置以便远程管理 CMC。此初始配置分配可启用 CMC 访问的 TCP/IP 网络参数。

设置对 CMC 的初始访问

本节解释如何使用 RACADM 命令执行初始 CMC 网络配置。本节中说明的所有配置都可以通过前面板 LCD 执行。请参阅"使用 LCD 配置向导配置网络"。

小心： 更改 CMC 网络设置屏幕上的设置可能断开您当前的网络连接。

有关网络子命令的详情，请参阅《*Dell Chassis Management Controller* 管理员参考指南》的"RACADM 子命令"和"属性数据库组和对象定义"章节。

注： 必须具备**机箱配置管理员**权限才可以设置 CMC 网络设置。

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

查看当前 IPv4 网络设置

要查看 NIC、DHCP、网络速度和双工设置的摘要，请键入：

```
racadm getniccfg
```

或

```
racadm getconfig -g cfgCurrentLanNetworking
```

查看当前 IPv6 网络设置

要查看网络设置的摘要，请键入：

```
racadm getconfig -g cfgIpv6LanNetworking
```

要查看机箱类型的 IPv4 和 IPv6 寻址信息，请键入：

```
racadm getsysinfo
```

默认情况下，CMC 自动从动态主机配置协议服务器请求并获取 CMC IP 地址。

可以禁用此功能并指定静态 CMC IP 地址、网关和子网掩码。

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 <静态 IP 地址>
```

```
racadm config -g cfgLanNetworking -o cfgNicGateway <静态网关>
```

```
racadm config -g cfgLanNetworking -o cfgNicNetmask <静态子网掩码>
```

查看当前网络设置

要查看 NIC、DHCP、网络速度和双工设置的摘要，请键入：

```
racadm getniccfg
```

或

```
racadm getconfig -g cfgCurrentLanNetworking
```

要查看机箱的 IP 地址和 DHCP、MAC 地址和 DNS 信息，请键入：

```
racadm getsysinfo
```

配置网络 LAN 设置

注： 要执行以下步骤，必须具备**机箱配置管理员**权限。

注： 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。

注： 如果您的机箱具有两个 CMC（活动和待机），且他们均连接至网络，则在出现故障时待机 CMC 自动承继活动 CMC 的网络设置。

注： 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 (SPT)，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，当 IPv6 连接受限时，IPv6 路由器无偿发送路由器广告时会等待一段时间。

启用 CMC 网络接口

若要为 IPv4 和 IPv6 启用/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/禁用 CMC IPv4 寻址，请键入：

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

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

注： 默认启用 CMC IPv4 寻址。

要启用/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。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 <静态 IP 地址>
```

```
racadm config -g cfgLanNetworking -o cfgNicGateway <静态网关>
```

```
racadm config -g cfgLanNetworking -o cfgNicNetmask <静态子网掩码>
```

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 IP 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 地址>
```

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6PrefixLength 64
```

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6Gateway <IPv6 地址>
```

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。此功能默认启用。

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。有关详情，请参阅"设置对 CMC 的初始访问"。

启用或禁用 DNS IP 地址 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。

要禁用 DNS 地址 DHCP 功能并指定静态主要和备用 DNS 服务器地址，请键入：

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

要禁用 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： 静态 DNS 服务器 IP 地址设置在禁用 DNS 地址的 DCHP 功能时才有效。

对于 IPv4，要设置首选主要和次要 DNS IP 服务器地址，请键入：

```
racadm config -g cfgLanNetworking -o cfgDNSServer1 <IP 地址>
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer2 <IPv4 地址>
```

对于 IPv6，要设置首选和次要 DNS IP 服务器地址，请键入：

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6DNSServer1 <IPv6 地址>
```

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6DNSServer2 <IPv6 地址>
```

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： 某些 DNS 服务器仅可注册 31 个字符或更少字符的名称。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 Name"（CMC 名称）。**默认情况下，DNS 服务器上的 CMC 名称为 cmc-<服务标签>。要更改 DNS 服务器上的 CMC 名称，请键入：

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

  其中 <*名称*> 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 Domain Name"（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 <名称>
  ```

  其中 <*名称*> 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。默认情况下启用自动协商。

可以通过键入以下命令禁用自动协议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 <双工模式>
```

其中

<*双工模式*>为 0（半双工）或 1（全双工，默认）

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

其中

<*速度*> 是 10 或 100（默认值）。

设置 CMC VLAN（IPv4 和 IPv6）

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> 的有效值是 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 优先权：

   ```
   racadm config -g cfgLanNetworking -o cfgNicVLanPriority <VLAN 优先权>
   ```

   <VLAN 优先权> 的有效值是 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 优先权：

```
racadm setniccfg -v <VLAN id> <VLAN 优先权>
```

例如：

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

删除 CMC VLAN

若要删除 CMC VLAN，禁用外部机箱管理网络的 VLAN 功能：

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

也可用以下命令删除 CMC VLAN：

```
racadm setniccfg -v
```

设置服务器 VLAN

用以下命令指定特定服务器的 VLAN ID 和优先权：

```
racadm setniccfg -m server-<n> -v <VLAN id> <VLAN 优先权>
```

<n> 的有效值是 1 - 16。

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

<VLAN 优先权> 的有效值是 0-7。默认值为 0。

例如：

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

删除服务器 VLAN

若要删除服务器 VLAN，禁用指定服务器网络的 VLAN 功能：

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

<n> 的有效值是 1 - 16。

例如：

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

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；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 将使用 1280 的 MTU。

设置 SMTP 服务器 IP 地址（IPv4 和 IPv6）

可以启用 CMC 使用简单邮件传输协议 (SMTP) 向指定 IP 地址发送电子邮件警报。要启用此功能，请键入：

```
racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr <SMTP IP 地址>
```

其中 <*SMTP IP 地址*>是网络 SMTP 服务器的 IP 地址。

注： 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，使用 DNS 名称。

配置网络安全设置（仅 IPv4）

注： 要执行以下步骤，必须具备**机箱配置管理员**权限。

启用 IP 范围检查（仅 IPv4）

IP 筛选将接入登录的 IP 地址与以下 **cfgRacTuning** 属性中指定的 IP 地址范围相比较：

- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask

仅当下列两项相同时，才允许从接入 IP 地址登录：

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

使用 RACADM 配置用户

开始之前

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 或运行 RACADM racresetcfg 命令，则当前唯一用户为 root 密码 calvin。racresetcfg 子命令将 CMC 重设回原始默认值。

小心： 使用 racresetcfg 命令时请小心，因为它将把*所有* 配置参数重设为初始默认值。任何之前的更改将丢失。

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。

若要验证用户是否存在，则打开到 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 <索引>
```

系统将显示有些参数和对象 ID 以及它们的当前值。受关注的两个对象为：

```
# cfgUserAdminIndex=XX

cfgUserAdminUserName=
```

如果 cfgUserAdminUserName 对象没有值，则可以使用由 cfgUserAdminIndex 对象表示的索引编号。如果"="后有名称，则该索引由该用户名占用。

注： 使用 RACADM config 子命令手动启用或禁用用户时，*必须*通过 -i 选项指定索引。请注意上一示例中显示的 cfgUserAdminIndex 对象带有 # 字符。另外，如果使用 **racadm** config -f racadm.cfg 命令指定任意数量的要写入的组/对象，将无法指定索引。新用户将被添加至第一个可用的索引。该行为允许更灵活地为第二个 CMC 配置与主 CMC 相同的设置。

添加 CMC 用户

要将新用户添加到 CMC 配置，可以使用一些基本命令。请执行以下步骤：

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《*Dell Chassis Management Controller 管理员参考指南*》的"数据库属性"一章中的 表 5-40 和 表 5-41。
4. 启用用户。

示例

下面的示例说明如何添加新用户"John" 密码"123456"，对 CMC 具有登录权限。

注： 请参阅《*Dell Chassis Management Controller 固件管理员参考指南*》的数据库属性一章中的表 3-1，查看特定用户权限的有效位掩码值的列表。默认权限值为 0，表示用户没有启用任何权限。

```
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
```

为验证是否成功地为用户添加了正确的权限，键入以下命令：

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

使用 RACADM 配置通过 SSH 的公共密钥验证

开始之前

最多可以配置 6 个公共密钥，通过 SSH 接口与服务用户名结合使用。添加或删除公共密钥之前，务必使用查看命令查看已设置了什么密钥，这样就不会无意改写或删除密钥。服务用户名是在通过 SSH 访问 CMC 时可以使用的特殊用户帐户。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脚本非常有用。

准备好设置此功能时，注意以下事项：

- 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，确保现有密钥不位于添加新密钥的索引处。CMC 不检查在添加新密钥之前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 (racadm getssninfo)

  Type User IP Address Login Date/Time

  (类型) (用户) (IP 地址) (登录日期/时间)

  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` 的详情，请参阅《*Dell Chassis Management Controller 管理员参考指南*》。

生成在 Windows 中使用的公共密钥

在添加帐户之前，在将通过 SSH 访问 CMC 的系统中必须有公共密钥。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。有关这些工具的其它用法或高级用法，请参阅应用程序帮助。

要使用适用于 Windows 客户端的 PuTTY Key Generator 创建基本密钥：

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： 如果您添加的密钥少于 768 位或超过 4096 位，CMC 可能不会显示信息，但您尝试登录时，这些密钥将出现故障。

3. 单击**"Generate"（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**"Public key for pasting..."（供粘贴的公共密钥...）**窗口中复制和粘贴文本。

生成在 Linux 中使用的公共密钥

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 提示符中键入：

```
ssh-keygen -t rsa -b 1024 -C testing
```

其中，

-t 选项必须为 dsa 或 rsa。

-b 选项指定介于 768 和 4096 之间的加密位数。

-C 选项允许修改公共密钥注释，该选项是可选的。

密码短语是可选的。

请按照说明进行操作。命令完成后，使用公共文件传递到 RACADM 以便上载文件。

CMC 的 RACADM 语句注释

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 SSH 上公共密钥验证的特殊帐号。
- 若要登录到 CMC，用户必须为 **service**。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，请键入：

```
racadm sshpkauth -i svcacct -k 1 -p 0xfff -f <公共密钥文件>
```

注： 只有远程 RACADM 才允许使用文件上载选项。有关详情，请参阅 "远程访问 RACADM" 和后续部分。

有关公共密钥权限，请参阅《*Dell Chassis Management Controller 管理员参考指南*》的"数据库属性"一章中的表 3-1。

要使用文本上载选项添加公共密钥，请键入：

```
racadm sshpkauth -i svcacct -k 1 -p 0xfff -t "<公共密钥文本>"
```

删除公共密钥

要删除公共密钥，请键入：

```
racadm sshpkauth -i svcacct -k 1 -d
```

要删除所有公共密钥，请键入：

```
racadm sshpkauth -i svcacct -k all -d
```

使用公共密钥验证方法登录

上载公共密钥之后，您不必输入密码就能够通过 SSH 登录 CMC。您还可以选择以命令行参数的形式发送单个 RACADM 命令到 SSH 应用程序。命令行选项的效果就像远程 RACADM 一样，因为会话在命令完成之后结束。例如：

登录：

```
ssh service@<域>
```

或

```
ssh service@<IP 地址>
```

其中，<IP 地址> 是 CMC 的 IP 地址。

发送 racadm 命令：

```
ssh service@<域> racadm getversion

ssh service@<域> racadm getsel
```

使用服务帐户登录时，如果在创建公共/私人密钥对时设置了密码短语，可能会提示您再次输入该密码短语。如果密码短语与密钥结合使用，Windows 和 Linux 客户端都提供相应方法来使之自动实现。在 Windows 客户端上，您可以使用 Pageant 应用程序。该应用程序在后台运行，使密码短语的输入变得透明。在 Linux 客户端上，您可以使用 ssh-agent。有关如何设置和使用上述任一应用程序，请参阅该应用程序提供的说明文件。

启用带有权限的 CMC 用户

要启用具有特定管理权限（基于角色授权）的用户，首先请通过执行 "开始之前" 中的步骤找到一个可用用户索引。然后输入以下命令行，并在其中输入新的用户名和密码。

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <索引> <用户权限位掩码值>
```

注： 请参阅《*Dell Chassis Management Controller* 管理员参考指南》的"数据库属性"一章中的表 3-1，查看特定用户权限的有效位掩码值的列表。默认权限值为 0，表示用户没有启用任何权限。

禁用 CMC 用户

通过使用 RACADM，可以手动只禁用单个 CMC 用户。不能使用配置文件删除用户。

下面的示例说明可用于删除 CMC 用户的命令语法：

```
racadm config -g cfgUserAdmin -i 2 cfgUserAdminPrivilege 0x0
```

配置 SNMP 和电子邮件警报

可以配置 CMC 在发生特定机箱事件时发送 SNMP 事件陷阱和/或电子邮件警报。有关详情和说明，请参阅 "配置 SNMP 警报" 和 "配置电子邮件警报"。

可以将陷阱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)。选择一种与您的组网技术/基础设施一致的格式。

注： **"Test TRAP"（检测陷阱）**功能不会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。

在多个机箱中配置多个 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），在将文件导出到其它 CMC 之前必须修改这些信息。

1. 使用 RACADM 查询包含相应配置的目标 CMC。

   注： 生成的配置文件是 **myfile.cfg**。可以文件重命名。

   注： **.cfg** 文件不包含用户密码。当 **.cfg** 文件上载至新 CMC 时，必须重新添加所有的密码。

2. 打开到 CMC 的远程登录/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。有关详情，请参阅"远程访问 RACADM"。

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. 请使用新创建的配置文件修改目标 CMC。

   在命令提示符下键入：

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

5. 重设已配置的目标 RAC。在命令提示符下键入：

```
racadm reset
```

getconfig -f myfile.cfg 子命令（步骤 1）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。

可以使用 **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它 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（**<***文件名***>.cfg**）是使用 `racadm config -f <文件名>.cfg` 命令创建的简单文本文件。该命令允许建立配置文件（类似于 **.ini** 文件）并从该文件中配置 CMC。

用户可以使用任意文件名，并且不一定要使用 **.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** 子命令的详情，请参阅《*Dell Chassis Management Controller 管理员参考指南*》。

RACADM 在首次将 **.cfg** 文件载入 CMC 时会对其进行分析，以验证有效组和对象名称是否存在以及是否遵守某些简单的语法规则。错误标记有在其中检测到错误的行号，并且有一条信息解释该问题。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** 文件中找到错误，写入命令将不传输到 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** 文件时请使用以下原则：

- 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，因为用户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 <文件名>.cfg` 命令。确保 **.cfg** 文件中包含所有所需的对象、用户、索引和其它参数。请参阅《*Dell Chassis Management Controller 管理员参考指南*》的数据库属性一章，查看对象和组的完整列表。

小心： 使用 racresetcfg 子命令将数据库和 CMC 网络接口设置重设为初始默认设置并删除所有用户和用户配置。尽管根用户可用，但也会将其他用户的设置重设为默认设置。

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。所有其它列中的"`#`"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 <文件名>.cfg` 命令生成 **.cfg**，然后对另一个 CMC 执行 `racadm config -f <文件名>.cfg` 命令，而不添加转义字符。

  例如：

```
#
# This is a comment (这是一条注释。)
[cfgUserAdmin]
cfgUserAdminPageModemInitString=<Modem init # not a comment (调制解调器初始化字符串中的 # 不是注释)>
```

- 所有的组条目必须位于左方括号和右方括号（`[` 和 `]`）之内。

  表示组名的起始的 `[` 字符*必须*从第一列开始。此组名称*必须*在该组中的任何对象之前指定。没有关联组名称的对象将导致错误。配置数据是根据《*Dell Chassis Management Controller 管理员参考指南*》的数据库属性一章中的定义进行分组的。

  以下示例显示了组名称、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 <*文件名*>.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 <定位标记对象> -i <索引 1-16> <唯一的定位标记名称>
  ```

- *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 将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删除索引对象：

  ```
  racadm config -g <组名> -o <对象名> -i <索引 1-16> ""
  ```

  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，请使用以下命令：

  ```
  racadm getconfig -g <组名> -i <索引 1 至 16>
  ```

- 对于索引组，对象定位标记*必须* 是 [ ] 对后的第一个对象。

  下面是当前索引组的示例：

  ```
  [cfgUserAdmin]
  cfgUserAdminUserName=<用户名>
  ```

  如果键入 racadm getconfig -f <*myexample*>.cfg，则命令将为当前 CMC 配置生成一个 **.cfg** 文件。此配置文件可用作一个示例，基于该文件来开始创建独特的 **.cfg** 文件。

修改 CMC IP 地址

修改配置文件中的 CMCIP 地址时，请删除所有不需要的<*变量*>=<*值*>条目。只保留带有 [和] 的实际变量组标签，包括两个与 IP 地址更改相关的 <*变量*>=<*值*> 条目。

示例：

```
#
# Object Group (对象组) "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
cfgNicGateway=10.35.10.1
```

此文件将更新为如下内容：

```
#
# Object Group (对象组) "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.9.143
# comment, the rest of this line is ignored (注释，此行的其余部分将被忽略)
cfgNicGateway=10.35.9.1
```

命令 racadm config -f <*myfile*>.cfg 分析文件并按行号识别错误。正确的文件将更新适当的条目。此外，可以使用上面示例中的 getconfig 命令确认更新。

使用该文件下载公司范围内的更改或使用命令 racadm getconfig -f <*myfile*>.cfg 通过网络配置新系统。

注： *"定位标记"*是保留字，不能在 **.cfg** 文件中使用。

使用 RACADM 配置 iDRAC 上的属性

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

- cfgLanNetworking
- cfgIPv6LanNetworking
- cfgRacTuning
- cfgRemoteHosts
- cfgSerial
- cfgSessionManagement

注： 有关属性默认值和范围的详情，请参阅《*Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise 刀片服务器版用户指南*》。

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

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*"（无）。

例如：

```
$ racadm getconfig -g cfgSessionManagement -m server-1

# cfgSsnMgtWebServerMaxSessions=N/A

# cfgSsnMgtWebServerActiveSessions=N/A

# cfgSsnMgtWebServerTimeout=N/A

# cfgSsnMgtSSHMaxSessions=N/A

# cfgSsnMgtSSHActiveSessions=N/A

# cfgSsnMgtSSHTimeout=N/A

# cfgSsnMgtTelnetMaxSessions=N/A

# cfgSsnMgtTelnetActiveSessions=N/A

# cfgSsnMgtTelnetTimeout=N/A
```

故障排除

表 4-3 列出与远程 RACADM 相关的常见问题。

表 4-3. 使用串行/ RACADM 命令：常见问题

问题	解答
执行 CMC 重设后（使用 RACADM **racreset** 子命令），我输入一个命令，结果显示以下信息： racadm <*子命令*> 传输：错误：(RC=-1) 这条信息是什么意思？	必须等待 CMC 完成重设，然后才能发出另一个命令。
当我使用 RACADM 子命令时，我得到一些无法理解的错误。	可能在使用 RACADM 时遇到以下一个或多个错误： - 本地错误信息 — 诸如语法、印刷错误和错误名称等问题。示例： ERROR: <消息> 使用 RACADM **help** 子命令显示正确的语法和用法信息。 - CMC 相关错误信息 — CMC 无法执行某项操作的问题。也可能显示为"racadm command failed"（**racadm 命令失败**）。 键入 **racadm gettracelog** 获取调试信息。
当我使用远程 RACADM 时，提示符更改为">"而我无法返回到"$"提示符。	如果在命令中输入不匹配的双引号 (") 或不匹配的单引号 ('), CLI 会更改为 ">" 提示并将所有命令排队。

	要返回到"$"提示符，请键入 <Ctrl>-d。

我尝试使用以下命令并接收显示"Not Found"（未发现）的错误：
 	
$ logout
 	
$ quit
	在 CMC CLI 界面中不支持 logout 和 quit 命令。

目录

目录

故障排除和恢复

Dell Chassis Management Controller Firmware 版本 3.0 用户指南

概览

本节介绍如何使用 CMC Web 界面执行与远程系统问题恢复和故障排除有关的任务。

- 收集配置信息、错误状态和错误日志
- 管理远程系统上的电源
- 查看机箱信息
- 查看事件日志
- 使用诊断控制台
- 重设组件
- 排除网络时间协议 (NTP) 故障
- 排除网络故障
- 排除警报故障
- 重置遗忘的管理员密码
- 错误代码和日志

机箱监测工具

收集配置信息和机箱状态及日志

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。

用途

```
racadm racdump
```

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 命令可以通过串行、远程登录或 SSH 控制台命令提示符或通过正常的命令提示符远程运行。

要列出 RACDUMP 子命令的语法和命令行选项，请键入：

```
racadm help <racdump>
```

CLI RACDUMP

Racdump 包括以下子系统，并组合了以下 RACADM 命令：

子系统	RACADM 命令
常规系统/RAC 信息	getsysinfo
会话信息	getssinfo
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	gettracelog
RAC 事件日志	gettraclog
系统事件日志	getsel

用途

```
racadm racdump
```

远程 RACDUMP

远程 RACADM 是一种客户端公用程序，可用于从 Management Station 通过带外网络接口执行。提供了远程功能选项 (-r)，可以允许连接到 Managed System 和从远程控制台或 Management Station 执行 RACADM 子命令。要使用远程功能，需要有效的用户名（-u 选项）和密码（-p 选项），以及 CMC IP 地址。

注： 使用 RACADM 远程功能时，须在使用有关文件操作的 RACADM 子命令的文件夹上具有写权限，例如：

- `racadm getconfig -f <文件名>`
- `racadm sslcertdownload -t <类型> [-f <文件名>]`

远程 RACDUMP 用法

若要远程使用 RACDUMP 子命令，请键入以下命令：

```
racadm -r <CMC IP 地址> -u <用户名> -p <密码>
```

```
<子命令> <子命令选项>
```

```
racadm -i -r <CMC IP 地址> <子命令> <子命令
```

选项>

注： -i 选项指示 RACADM 交互式提示用户名和密码。如果不使用 -i 选项，则必须在命令中使用 -u 和 -p 选项提供用户名和密码。

例如：

```
racadm -r 192.168.0.120 -u root -p calvin racdump
```

```
racadm -i -r 192.168.0.120 racdump
```

如果 CMC 的 HTTPS 端口号更改为非默认端口 (443) 的自定义端口，则必须使用下面的语法：

```
racadm -r <CMC IP 地址>:<端口> -u <用户名> -p <密码> <子命令> <子命令选项>

racadm -i -r <CMC IP 地址>:<端口> <子命令> <子命令选项>
```

Telnet RACDUMP

SSH/Telnet RACADM 用于从 SSH 或 Telnet 提示符下使用 RACADM 命令。

有关 RACDUMP 说明的详情，请参阅 "使用 RACADM 命令行界面" 部分和"*CMC 管理员参考指南*"。

配置 LED 以识别机箱上的组件

可以为全部或单个组件（机箱、服务器和 IOM）设置组件 LED 闪烁作为识别机箱上组件的一种方法。

注： 要修改这些设置，必须具备**机箱控制管理员**权限。

使用 Web 界面

要为一个、多个或所有组件 LED 启用闪烁：

1. 登录 CMC Web 界面。
2. 单击系统树中的**"Chassis"（机箱）**。
3. 单击**"Troubleshooting"（故障排除）**选项卡。
4. 单击**"Identify"（标识）**子选项卡。随即显示**"Identify"（标识）**页，其中列出了机箱上所有组件的列表。
5. 要为组件 LED 启用闪烁，可以选中设备名称旁边的方框，然后单击**"Blink"（闪烁）**。
6. 要为组件 LED 禁用闪烁，可以选中设备名称旁边的方框，然后单击**"UnBlink"（不闪烁）**。

使用 RACADM

打开到 CMC 的串行/远程登录/SSH 文本控制台，登录并键入：

```
racadm setled -m <模块> [-l <ledState>]
```

其中<*模块*>指定想要配置 LED 的模块。配置选项：

- `server-n` 其中 *n*=1-16
- `switch-n` 其中 *n*=1-6
- `cmc-active`

和 <*ledState*> 指定 LED 是否应该闪烁。配置选项：

- 0 — 不闪烁（默认）
- 1 — 闪烁

配置 SNMP 警报

简单网络管理协议 (SNMP) 陷阱，或*事件陷阱*，与电子邮件事件警报相似。Management Station 使用它们从 CMC 接收未请求数据。

可以配置 CMC 生成事件陷阱。 表 12-2 提供触发器 SNMP 和电子邮件警报的事件概览。有关电子邮件警报的信息，请参阅"配置电子邮件警报"。

注： 从 CMC 版本 2.10 开始，SNMP 现在支持 IPv6。您可以在事件警报的目标中包括 IPv6 地址或完全限定域名 (FQDN)。

表 12-2. 可生成 SNMP 的机箱事件

事件	说明
风扇探测器故障	风扇转动速度太慢，或根本没有转动。
电池探测器警告	电池停止运作。
温度探测器警告	温度接近最高或最低限制。
温度探测器故障	温度太高或太低，无法正常工作。
已降级冗余	风扇和（或）电源设备的冗余已经减少。
冗余掉失	风扇和（或）电源设备没有保留冗余。
电源设备警告	电源设备临近故障状况。
电源设备故障	电源设备已失败。
电源设备不存在	预期的电源不存在。
硬件日志故障	硬件日志不运作。
硬件日志警告	硬件日志几乎写满。
服务器不存在	预期的服务器不存在。
服务器故障	服务器无法运作。
KVM 不存在	预期的 KVM 不存在。
KVM 故障	KVM 无法运作。
IOM 不存在	预期的 IOM 不存在。
IOM 故障	IOM 无法运作。
固件版本不匹配	机箱或服务器固件的固件不匹配。
机箱电源阈值错误	机箱中的功耗达到系统输入电源上限。

可以使用 Web 界面或 RACADM 添加和配置 SNMP 警报。

使用 Web 界面

注： 要添加或配置 SNMP 警报，您必须具有**机箱配置管理员**权限。

注： 为了增加安全性，Dell 强烈建议您更改 root（用户 1）帐户的默认密码。root 帐户是与 CMC 一并提供的默认管理帐户。要更改 root 帐户的默认密码，请单击"User ID 1"（用户 ID 1），打开"**User Configuration**"（用户配置）页面。通过页面右上角的**"Help"（帮助）**链接可以访问该页的帮助。

1. 登录 CMC Web 界面。
2. 选择系统树中的**"Chassis"（机箱）**。
3. 单击**"Alerts"（警报）**标签。随即出现**"Chassis Events"（机箱事件）**页。
4. 启用警报：
   a. 选择想要启用警报的事件的复选框。要启用所有警报事件，请选择**"Select All"（全选）**复选框。
   b. 单击**"Apply"（应用）**保存设置。
5. 单击**"Traps Settings"（陷阱设置）**子选项卡。随即显示**"Chassis Event Alert Destinations"（机箱事件警报目标）** 页。
6. 在空白的**"Destination"（目标）**字段中键入有效地址。

   注： 有效地址是接收陷阱警报的地址。使用"四点"IPv4 格式、标准 IPv6 地址表示法或 FQDN。例如：123.123.123.123、2001:db8:85a3::8a2e:370:7334 或 dell.com
7. 键入目标 Management Station 所属的**" SNMP Community String"（SNMP 团体字符串）**。

   注： **"Chassis Event Alert Destinations"（机箱事件警报目标）**页上的团体字符串与**"Chassis"（机箱）→ "Network"（网络）→ "Services"（服务）**页上的团体字符串不同。SNMP 陷阱团体字符串是 CMC 用于出站陷阱到 Management Station 的团体。**"Chassis"（机箱）→ "Network"（网络）→ "Services"（服务）**页上的团体字符串是 Management Station 用于查询 CMC 上 SNMP 守护程序的团体字符串。
8. 单击"**Apply**"（应用）保存您所做的更改。

要检测警报目标的事件陷阱：

1. 登录 CMC Web 界面。

2. 选择系统树中的**"Chassis"（机箱）**。

3. 单击**"Alerts"（警报）**标签。随即显示**"Chassis Events"（机箱事件）**页。

4. 单击**"Traps Settings"（陷阱设置）**选项卡。随即显示**"Chassis Event Alert Destinations"（机箱事件警报目标）**页。

5. 单击位于目的地旁边的**"Test Trap"（测试陷阱）**列中的**"Send"（发送）**。

注： 将陷阱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)。选择一种与您的组网技术/基础设施一致的格式。**"Test Trap"（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）。

使用 RACADM

1. 打开到 CMC 的串行/远程登录/SSH 文本控制台，并登录。

   注： 仅可同时对 SNMP 和电子邮件警报设置一个筛选器掩码。如果已经选定筛选器掩码，则可以跳过步骤 2。

2. 通过键入以下命令启用警报：

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

3. 通过键入以下命令指定希望 CMC 生成警报的事件：

   ```
   racadm config -g cfgAlerting -o cfgAlertingFilterMask <掩码值>
   ```

   其中 <*掩码值*> 是 0x0 和 0x017fffdf 之间的十六进制值。

   要获得掩码值，请使用十六进制模式的科学计算器，并使用 <OR> 键加上各个掩码（1、2、4 等）的第二个值。

   例如，要为电池探测器警告 (0x2)、电源设备故障 (0x1000) 和 KVM 故障 (0x80000) 启用陷阱警报，键入 2 <OR> 1000 <OR> 200000 并按下 <=> 键。

   结果十六进制值为 208002，则用于 RACADM 命令的掩码值为 0x208002。

表 12-3. 事件陷阱筛选器掩码

事件	筛选器掩码值
风扇探测器故障	0x1
电池探测器警告	0x2
温度探测器警告	0x8
温度探测器故障	0x10
已降级冗余	0x40
冗余掉失	0x80
电源设备警告	0x800
电源设备故障	0x1000
电源设备不存在	0x2000
硬件日志故障	0x4000
硬件日志警告	0x8000
服务器不存在	0x10000
服务器故障	0x20000
KVM 不存在	0x40000
KVM 故障	0x80000
IOM 不存在	0x100000
IOM 故障	0x200000
固件版本不匹配	0x00400000
机箱电源阈值错误	0x01000000

4. 通过键入以下命令启用陷阱：

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

   其中<*索引*>值为 1-4。CMC 使用索引号码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. 通过键入以下命令指定接收陷阱警报的目标 IP 地址：

   ```
   racadm config -g cfgTraps -o cfgTrapsAlertDestIPAddr <IP 地址> -i <索引>
   ```

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

6. 通过键入以下命令指定团体名称：

   ```
   racadm config -g cfgTraps -o cfgTrapsCommunityName <团体名称> -i <索引>
   ```

   其中 *<团体名称>* 是机箱所属的 SNMP 团体，*<索引>* 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，请重复步骤 2-6。

注： 步骤 2-6 中的命令将覆盖任何为指定索引 (1-4) 配置的现有设置。要确定某索引以前是否配置过值，请键入：**racadm get config -g cfgTraps -i** *<索引>*。如果已配置该索引，则会出现 **cfgTrapsAlertDestIPAddr** 和 **cfgTrapsCommunityName** 对象的值。

要检测警报目标的事件陷阱，请键入：

```
racadm testtrap -i <索引>
```

其中*<索引>*是代表想要测试的警报目的地的值 1-4。如果不确定索引号码，请键入：

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

配置电子邮件警报

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。

表 12-2 提供触发器电子邮件和 SNMP 警报的事件概览。有关电子邮件警报的信息，请参阅 "配置 SNMP 警报"。

可以使用 Web 界面或 RACADM 添加和配置电子邮件警报。

使用 Web 界面

注： 要添加或配置电子邮件警报，您必须具有**机箱配置管理员**权限。

1. 登录 CMC Web 界面。
2. 选择系统树中的**"Chassis"（机箱）**。
3. 单击**"Alerts"（警报）**标签。随即出现**"Chassis Events"（机箱事件）**页。
4. 启用警报：
   a. 选择想要启用警报的事件的复选框。要启用所有警报事件，请选择**"Select All"（全选）**复选框。
   b. 单击**"Apply"（应用）**保存设置。
5. 单击**"Email Alert Settings"（电子邮件警报设置）**子选项卡。随即显示**"Email Alert Destinations"（电子邮件警报目标）**页。
6. 指定 SMTP 服务器 IP 地址：
   a. 定位到**"SMTP (Email) Server"（SMTP [电子邮件] 服务器）**字段，然后键入 SMTP 地址。

   注： 必须配置 SMTP 电子邮件服务器才能接受来自 CMC 的 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。有关如何以安全的方式完成此目标的说明，请参考随 SMTP 服务器提供的说明文件。

   b. 输入希望使用的警报发件人电子邮件，或保持空白以使用默认电子邮件发件人。默认值是 cmc@<IP 地址>，其中<IP 地址>是 CMC 的 IP 地址。如果输入值，则电子邮件名称的语法是 <电子邮件名称>[@<域>]，并且可以选择是否指定电子邮件域。

      如果未指定 @<域> 且只有一个活动 CMC 网络域，则将使用电子邮件地址<电子邮件名称>@<cmc 域>作为源电子邮件。如果未指定@<域>且 CMC 无活动网络域，则将使用 CMC 的 IP 地址（例如<电子邮件名称>@<IP 地址>）。

   c. 单击**"Apply"**（应用）保存您所做的更改。
7. 指定接收警报的电子邮件地址：
   a. 在空白的**"Destination Email Address"（目标电子邮件地址）**字段中键入有效的电子邮件地址。
   b. 输入可选的**"Name"（名称）**。这是接收电子邮件实体的名称。如果输入的名称为无效电子地址，则它将被忽略。

c. 单击**"Apply"（应用）**保存设置。

要将测试电子邮件发送到一个电子邮件警报的目标电子邮件地址：

1. 登录 CMC Web 界面。
2. 选择系统树中的**"Chassis"（机箱）**。
3. 单击**"Alerts"（警报）**标签。随即出现**"Chassis Events"（机箱事件）**页。
4. 单击**"Email Alert Settings"（电子邮件警报设置）**子选项卡。随即显示**"Email Alert Destinations"（电子邮件警报目标）**页。
5. 单击位于目的地旁边的**"Destination Email Address "（目标电子邮件地址）**列的**"Send"（发送）**。

使用 RACADM

1. 打开到 CMC 的串行/远程登录/SSH 文本控制台，并登录。
2. 通过键入以下命令启用警报：

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

   注： 仅可同时对 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，则可以跳过步骤 3。

3. 通过键入以下命令指定希望 CMC 生成警报的事件：

   ```
   racadm config -g cfgAlerting -o cfgAlertingFilterMask <掩码值>
   ```

   其中 *<掩码值>* 是介于 0x0 和 0x017fffdf 之间的十六进制值，并且必须带有前导 *0x* 字符。 表 12-3 为每种事件类型提供筛选器掩码。有关计算想要启用的筛选器掩码十六进制值的说明，请参阅"使用 RACADM"的步骤 3。

4. 通过键入以下命令启用电子邮件警报：

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

   其中*<索引>*值为 1-4。CMC 使用索引号码来区别最多四个可配置目标电子邮件地址。

5. 通过键入以下命令指定要接收电子邮件警报的目标电子邮件地址：

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertAddress <电子邮件地址> -i <索引>
   ```

   其中*<电子邮件地址>*是有效电子邮件地址，*<索引>*是在步骤 4 中指定的索引值。

6. 通过键入以下命令指定接收电子邮件警报的团体名称：

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEmailName <电子邮件名称> -i <索引>
   ```

   其中*<电子邮件名称>*是接收电子邮件警报的个人或组的名称，*<索引>*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、连字符、下划线和句点。空格无效。

7. 通过键入以下命令配置 cfgRhostsSmtpServerIpAddr 数据库属性以设置 SMTP 主机：

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

   其中 host.domain 是完全限定域名。

最多可配置四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，请重复步骤 步骤 2-步骤 6。

注： 步骤 2-6 中的命令将覆盖任何为指定索引 (1-4) 配置的现有设置。要确定某索引以前是否配置过值，请键入：**racadm getconfig -g cfgEmailAlert -i** *<索引>*。如果已配置该索引，则会出现 **cfgEmailAlertAddress** 和 **cfgEmailAlertEmailName** 对象的值。

排除远程系统故障首先需要进行的步骤

以下是在排除 Managed System 高级别故障时常见的一些问题：

1. 系统开机还是关机？

2. 如果是开机，操作系统是运作正常、崩溃，或者只是冻结？

3. 如果是关机，电源是意外关闭的吗？

监测机箱电源并执行电源控制命令

可以使用 Web 界面或 RACADM 完成：

- 查看系统的当前电源状态。
- 当重新引导、打开或关闭系统电源时，通过操作系统执行秩序关机。

有关 CMC 上电源管理和配置电源预算、冗余和电源控制的信息，请参阅"电源管理"。

查看电源预算状况

有关使用 Web 界面或 RACADM 查看机箱、服务器和 PSU 电源预算状态的说明，请参阅 "查看功耗状态"。

执行电源控制操作

有关使用 CMC Web 接口或 RACADM 开机、关机、重设、关机后再开机的说明，请参阅"执行机箱电源控制操作"、"执行 IOM 电源控制操作"和"执行服务器电源控制操作"。

电源故障排除

使用下面的项目帮助排除电源故障并解决有关电源的问题：

- **问题：**将**"Power Redundancy Policy"（电源冗余策略）**配置成了**"AC Redundancy"（交流冗余）**，并发出电源设备冗余掉失事件。
  - **解决方案 A：**此配置要求 1 侧（左边 3 个插槽）至少有 1 个电源且 2 侧（右边 3 个插槽）至少有 1 个电源存在于模块化机柜中并可正常运行。另外，每侧的容量必须足以支持机箱的合计功率分配以维持**交流冗余**。（为了获得完整的交流冗余，确保提供由 6 个电源设备组成的完整 PSU 配置。）
  - **解决方案 B：**确认所有电源设备是否正确连接到两个交流电网；1 侧的电源设备需要连接到一个交流电网；2 侧的电源设备需要连接到一个交流电网；且两个交流电网都需要能正常运行。如果一个交流电网不工作，则**交流冗余**丢失。
- **问题：**即使已连接交流线并且配电装置的交流输出良好，PSU 状态也显示为**"Failed (No AC)"（失败 [无交流]）**。
  - **解决方案 A：**检查并更换交流电缆。检查并确认为电源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。
  - **解决方案 B：**确认 PSU 连接的电压是否与其他 PSU 相同。如果 CMC 检测到一个 PSU 在不同电压下工作，则此 PSU 会被关闭并标记为"Failed"（故障）。
- **问题：**动态电源设备接入已启用，但**"Standby"（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：**机柜内的电源设备不完全支持动态电源设备接入。要确认是否是此情况，用 Web 界面关闭动态电源设备接入，然后再次打开。如果不完全支持动态电源设备接入，则会看到一条消息。
- **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：**检查系统输入电源上限设置 - 它的配置可能太低，不允许任何额外服务器开机。
  - **解决方案 B：**检查是否在 110V 下工作。如果任何电源设备连接到 110V 分支电路，则在允许服务器开机前必须认可这是有效的配置。有关详情，请参阅"电源配置设置"。
  - **解决方案 C：**检查最大节能设置。如果设置了这个，则服务器不会开机。有关详情，请参阅"电源配置设置"。
  - **解决方案 D：**检查与新插入服务器相关的插槽的服务器插槽电源优先权，确保它不低于任何其他服务器插槽电源优先权。
- **问题：**可用电源不断变化，即便没有更改模块机柜配置
  - **解决方案：**CMC 1.2 和更高版本拥有动态风扇电源管理功能，如果机柜在接近峰值用户配置的电源上限操作，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为风扇分配电源，以保证输入电源消耗低于**"System Input Power Cap"（系统输入电源上限）**。这是正常现象。
- **问题：**报告 2000 W 作为**"Surplus for Peak Performance"（峰值性能盈余）**。
  - **解决方案：**机柜在当前配置中提供 2000 W 剩余电源，并且**"System Input Power Cap"（系统输入电源上限）**可安全地降低报告的此数值，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断电，甚至当机箱在带有六个电源设备的**"AC Redundancy"（交流冗余）**配置中运行时也是如此。
  - **解决方案：**发生交流电网故障时，如果电源未正确连接到冗余交流电网，则会发生这种问题。**"AC Redundancy"（交流冗余）**策略需要左侧的三个电源连接到一个交流电网，右侧的三个电源连接到其他交流电网。如果未正确连接两个 PSU，例如将 PSU3 和 PSU4 连接到错误的交流电网，交流电网故障会造成最低优先权服务器断电。
- **问题：**最低优先权服务器在 PSU 故障后损失电源。
  - **解决方案：**如果机柜电源策略配置为**"No Redundancy"（无冗余）**，则这是预期现象。为了防止未来的电源故障导致服务器断电，确保机箱至少有四个电源且为**"Power**

Supply Redundancy"（电源冗余）策略配置，以防止产生影响服务器操作的 PSU 故障。

- **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**"System Input Power Cap"（系统输入电源上限）**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**"System Input Power Cap"（系统输入电源上限）**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。

查看机箱摘要

CMC 提供机箱、活动和待机 CMC、iKVM、风扇、温度传感器和输入/输出模块 (IOM) 的滚动概览。

使用 Web 界面

要查看机箱、CMC、iKVM 和 IOM 的摘要：

1. 登录 CMC Web 界面。
2. 选择系统树中的**"Chassis"（机箱）**。
3. 单击**"Summary"（摘要）**标签。随即显示**"Chassis Summary"（机箱摘要）**页。

表 12-4、表 12-5、表 12-6和表 12-7说明提供的信息。

表 12-4. 机箱摘要

项目	说明
"Name"（名称）	显示机箱名称。该名称用于识别网络上的机箱。有关设置机箱名称的信息，请参阅"编辑插槽名称"。
"Model"（型号）	显示机箱型号或制造商。例如，PowerEdge 2900。
"Service Tag"（服务标签）	显示机箱的服务标签。服务标签是制造商提供的用于支持和维修的唯一标识符。
"Asset Tag"（资产标签）	显示机箱的资产标签。
"Location"（位置）	显示机箱的位置。
"CMC Failover Ready"（CMC 故障转移就绪）	显示（**"Yes"（是）**，**"No"（否）**）待机 CMC（如果存在）是否具备在发生故障时进行完成故障转移的能力。
"System Power Status"系统电源状况	显示系统电源状态。

表 12-5. CMC 摘要

项目	说明
活动 CMC 信息	
"Name"（名称）	显示 CMC 的名称。例如，活动 CMC 或待机 CMC。
"Description"（说明）	提供 CMC 目标的简要说明。
"Date/Time"（日期/时间）	显示在活动 CMC 上当前设置的日期和时间。
"Active CMC Location"（活动 CMC 的位置）	显示活动 CMC 的插槽位置。
"Redundancy Mode"（冗余模式）	如果机箱中出现待机 CMC，则显示。
"Primary Firmware Version"（主要固件版本）	显示活动 CMC 的固件版本。
"Firmware Last Updated"（上次更新固件）	显示上次更新固件的时间。如果未发生更新，则该属性显示**"N/A"（暂无）**。
"Hardware Version"（硬件版本）	显示活动 CMC 的硬件版本。
"MAC Address"（MAC 地址）	显示 CMC 网络接口的 MAC 地址。MAC 地址是 CMC 在整个网络中的唯一标识符。
"IP Address"（IP 地址）	显示 CMC 网络接口的 IP 地址。
"Gateway"（网关）	显示 CMC 网络接口的网关。
"Subnet Mask"（子网掩码）	显示 CMC 网络接口的子网掩码。
"Use DHCP (for CMC Network Interface IP Address)"（使用 DHCP [针对 CMC 网络接口 IP 地址]）	显示是否启用 CMC 自动从动态主机配置协议服务器请求和获取 IP 地址**（"Yes"（是）或"No"（否））。该属性的默认设置是"No"（否）。**
"Primary DNS Server"（主要 DNS 服务器）	显示主要 DNS 服务器名称。
"Alternate DNS Server"（备用 DNS 服务器）	显示次要 DNS 服务器名称。

"Use DHCP for DNS Domain Name"（使用 DHCP 来设置 DNS 域名）	显示使用 DHCP 获取 DNS 域名（**"Yes"（是）**、**"No"（否）**）。
"DNS Domain Name"（DNS 域名）	显示 DNS 域名。
"Standby CMC Information"（备用 CMC 信息）	
"Present"（存在）	显示（**"Yes"（是）**、**"No"（否）**）是否安装第二（待机）CMC。
"Standby Firmware Version"（备用固件版本）	显示安装在待机 CMC 上的 CMC 固件版本。

表 12-6. iKVM 摘要

项目	说明
"Present"（存在）	显示是否存在 iKVM 模块（"Yes"[是] 或"No"[否]）。
"Name"（名称）	显示 iKVM 的名称。名称用于识别网络上的 iKVM。
"Manufacturer"（制造商）	显示 iKVM 型号或制造商。
"Part Number"（部件号）	显示 iKVM 的部件号。部件号是供应商提供的唯一标识符。部件号命名习惯随供应商而有所差别。
"Firmware Version"（固件版本）	显示 iKVM 的固件版本。
"Hardware Version"（硬件版本）	显示 iKVM 的硬件版本。
"Power Status"（电源状况）	显示 iKVM 的电源状况：**"On"（开）**、**"Off"（关）**以及**"N/A"（不可用）**（不存在）。
"Front Panel USB/Video Enabled"（前面板 USB/视频已启用）	显示是否已启用前面板 VGA 和 USB 连接器（**"Yes"[是]**或**"No"[否]**）。
"Allow Access to CMC CLI from iKVM"（允许从 iKVM 访问 CMC CLI）	显示在 iKVM 上已启用 CLI 访问（**"Yes"[是]**或**"No"[否]**）。

表 12-7. IOM 摘要

项目	说明
"Location"（位置）	显示 IOM 占用的插槽。六个插槽靠组名称（A、B 或 C）和插槽号（1 或 2）识别。插槽名称：**A-1**、**A-2**、**B-1**、**B-2**、**C-1** 或 **C-2**。
"Present"（存在）	显示 IOM 是否存在（**"Yes"[是]** 或**"No"[否]**）。
"Name"（名称）	显示 IOM 名称。
"Fabric"（结构）	显示结构的类型。
"Power Status"（电源状况）	显示 IOM 的电源状况：**"On"（开）**、**"Off"（关）**或**"N/A"（无）**。
"Service Tag"（服务标签）	显示 IOM 的服务标签。服务标签是由制造商提供的用于支持和维护的唯一标识符。

使用 RACADM

1. 打开到 CMC 的串行/远程登录/SSH 文本控制台，并登录。
2. 要查看机箱和 CMC 摘要，键入：

   ```
   racadm getsysinfo
   ```

3. 要查看 iKVM 摘要，键入：

   ```
   racadm getkvminfo
   ```

4. 要查看 IOM 摘要，键入：

   ```
   racadm getioinfo
   ```

查看机箱和组件运行状况

使用 Web 界面

要查看机箱和组件运行状况摘要：

1. 登录 CMC Web 界面。
2. 选择系统树中的**"Chassis"（机箱）**。随即显示**"Chassis Health"（机箱运行状况）**页。

   "Chassis Graphics"（机箱图形）部分提供机箱前面板和后面板的图形视图。该图形表示提供机箱内安装的组件即其相应状态的可视化概览。

   每个图形显示实时代表已安装的组件。通过组件子图形的重叠表示指示组件状态。

   - 无重叠 — 组件存在，电源打开并且正在与 CMC 通信；这指示不存在不利条件。
   - 琥珀色小心标记 - 指示只发出警告警报并且必须采取纠正措施。
   - 红色 X - 指示至少存在一次故障。这表明 CMC 仍然能够同组件通信，且运行状况报告为严重。
   - 灰色且不可选 - 指示组件存在但未开机。它当前未与 CMC 通信且不存在不利条件。

   当把鼠标停放在组件子图形上方时，所有组件都将显示相应的文本提示或屏幕提示。组件状态会动态更新，并且组件子图形的颜色和文本提示将自动更改以反映当前状态。

   单击组件子图形可选择组件的信息和快速链接，在机箱图形的下方显示。

   "CMC 硬件日志"部分提供最新的 10 条 CMC 硬件日志条目用于参考（请参阅"查看硬件日志"）。

使用 RACADM

打开到 CMC 的串行/远程登录/SSH 文本控制台，登录并键入：

```
racadm getmodinfo
```

查看事件日志

"Hardware Log and CMC Log"（硬件日志和 CMC 日志）页显示 Managed System 上发生的严重系统事件。

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 在发生指定事件时发送电子邮件或 SNMP 陷阱。有关配置 CMC 发送警报的信息，请参阅 "配置 SNMP 警报" 和 "配置电子邮件警报"。

硬件日志条目范例

```
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 Web 界面

可以在 CMC Web 界面中查看、保存和清除硬件日志的文本文件版本。

表 12-8 提供 CMC Web 界面中**"Hardware Log"（硬件日志）**页所提供信息的说明。

要查看硬件日志：

1. 登录 CMC Web 界面。
2. 单击系统树中的**"Chassis"（机箱）**。
3. 单击**"Logs"（日志）**选项卡。
4. 单击**"Hardware Log"（硬件日志）**子选项卡。随即显示**"Hardware Log"（硬件日志）**页。

要将硬件日志的副本保存到 Managed Station 或网络：

1. 单击**"Save Log"（保存日志）**。

   对话框打开。

2. 为日志的文本文件选择位置。

注： 因为日志保存为文本文件，所以不会在用户接口中出现图形来指示严重性。在文本文件中，严重性以"OK"（良好）、"Informational"（通知）、"Unknown"（未知）"Warning"（警告）和"Severe"（严重）等词语表示。
日期和时间条目以升序显示。如果在"Date/Time"（日期/时间）列中出现<"SYSTEM BOOT"（系统引导）>，这表示在任何模块关闭或启动时发生事件，此时时间或日期不可用。

若要清除硬件日志，单击**"Clear Log"（清除日志）**。

注： CMC 将创建一个新的日志条目表示日志已清除。

表 12-8. 硬件日志信息

项目	说明		
严重性		"OK"（良好）	指示正常事件，无需采取修正操作。
		"Informational"（通知）	指示事件上的通知条目，其中严重性状况未更改。
		"Unknown"（未知）	指示不严重事件，**应该尽快采取修正操作**以避免系统故障。
		"Warning"（警告）	指示严重事件，要求立即采取修正操作以避免系统故障。
		"Severe"（严重）	指示**要求立即采取纠正操作**以避免系统故障的严重事件。
"Date/Time"（日期/时间）	显示发生事件的确切日期和时间（例如，"Wed May 02 16:26:55 2007"[2007 年 5 月 2 日，周三，16:26:55]）。如果未出现日期/时间，则该事件在系统引导时出现。		
"Description"（说明）	提供 CMC 生成的事件的简单说明（例如，Redundancy lost, Server inserted.（冗余掉失、插入服务器））。		

使用 RACADM

1. 打开到 CMC 的串行/远程登录/SSH 文本控制台，并登录。

2. 要查看硬件日志，键入：

   ```
   racadm getsel
   ```

   要清除硬件日志，键入：

   ```
   racadm clrsel
   ```

查看 CMC 日志

CMC 生成与机箱相关事件的日志。

注： 要清除硬件日志，必须具备**清除日志管理员**权限。

使用 Web 界面

可以在 CMC Web 界面中查看、保存和清除 CMC 日志的文本文件版本。

可以通过单击列标题按照"Source"（来源）、"Date/Time"（日期/时间）或"Description"（说明）对日志条目重新排序。接着再单击列标题会反向排序。

表 12-9 提供 CMC Web 界面中**"CMC Log"（CMC 日志）**页所提供信息的说明。

要查看 CMC 日志：

1. 登录 CMC Web 界面。
2. 单击系统树中的**"Chassis"（机箱）**。
3. 单击**"Logs"（日志）**选项卡。
4. 单击**"CMC Log"（CMC 日志）**子选项卡。随即显示**"CMC Log"（CMC 日志）**页。
5. 要将 CMC 日志的副本保存到 Managed Station 或网络，请单击**"Save Log"（保存日志）**。

   随即打开对话框：选择日志文本文件的位置。

表 12-9. CMC 日志信息

命令	结果
"Source"（来源）	显示导致该事件的接口（例如 CMC）。
"Date/Time"（日期/时间）	显示发生事件的确切日期和时间（例如，"Wed May 02 16:26:55 2007"[2007 年 5 月 2 日，周三，16:26:55]）。
"Description"（说明）	提供该操作的简短说明，例如登录或注销、登录失败或清除日志。说明由 CMC 生成。

使用 RACADM

1. 打开到 CMC 的串行/远程登录/SSH 文本控制台，并登录。
2. 要查看硬件日志，键入：

   ```
   racadm getraclog
   ```

   要清除硬件日志，键入：

   ```
   racadm clrraclog
   ```

使用诊断控制台

"Diagnostic Console"（诊断控制台）页使高级用户或在技术支持指导下的用户能够使用 CLI 命令诊断与机箱硬件相关的问题。

注： 要修改这些设置，必须具备**调试命令管理员**权限。

要访问**"Diagnostic Console"（诊断控制台）**页：

1. 登录 CMC Web 界面。
2. 单击系统树中的**"Chassis"（机箱）**。
3. 单击**"Troubleshooting"（故障排除）**选项卡。
4. 单击**"Diagnostic"（诊断）**子选项卡。随即显示**"Diagnostic Console"（诊断控制台）**页。

要执行诊断 CLI 命令，在**"Enter RACADM Command"（输入 RACADM 命令）**字段中键入命令，并随后单击**"Submit"（提交）**执行诊断命令。诊断结果页将会显示。

要返回到**"Diagnostic Console"（诊断控制台）**页，单击**"Go Back to Diagnostic Console Page"（返回诊断控制台页）**或**"Refresh"（刷新）**。

诊断控制台支持 表 12-10 中列出的命令和 RACADM 命令。

表 12-10. 支持的诊断命令

命令	结果
arp	显示地址解析协议 (ARP) 表的内容。ARP 条目不能添加或删除。
ifconfig	显示网络接口表的内容。

netstat	显示路由表的内容。
ping <*IP 地址*>	验证使用当前路由表中的内容可以从 CMC 到达目标 <*IP 地址*>。目标 IP 地址必须输入至该选项右侧的字段。根据当前的路由表内容，将 Internet 控制报文协议 (ICMP) 回音数据包发送到目标 IP 地址。
gettracelog	显示跟踪日志（可能需要几秒钟显示日志）。**gettracelog -i** 命令返回跟踪日志中的记录数。 **注：** 有关 gettracelog 命令的详情，请参阅《*Dell Chassis Management Controller 管理员参考指南*》中的 gettracelog 命令部分。

重设组件

"Reset Components"（重设组件）页面允许用户重设活动的 CMC，或者虚拟重置服务器，使其产生如同被拆卸并重新插入的效果。如果机箱有一个待机 CMC，重设活动的 CMC 将造成故障转移并且待机 CMC 将变为活动状态。

注： 要重设组件，必须具备**调试命令管理员**权限。

要访问**"Diagnostic Console"（诊断控制台）**页：

1. 登录 CMC Web 界面。
2. 单击系统树中的**"Chassis"（机箱）**。
3. 单击**"Troubleshooting"（故障排除）**选项卡。
4. 单击**"Reset Components"（重设组件）**子选项卡。**"Reset Components"（重设组件）**页会显示。**"CMC Summary"（CMC 摘要）**部分（"**Reset Components"[重设组件]**）页显示以下信息：

表 12-11. CMC 摘要

属性	说明		
运行状况		"OK"（良好）	CMC 存在并通过其组件通信。
		"Informational"（通知）	如果运行状况没有更改（良好、警告、严重），则显示有关 CMC 的信息。
		"Warning"（警告）	发出了警告警报，**必须采取更正措施**。如果未采取纠正措施，则可发生影响 CMC 完整性的严重故障。
		"Severe"（严重）	已至少发出一个故障警报。严重状况表示发生 CMC 系统故障，**必须立即采取补救措施**。
"Date/Time"（日期/时间）	显示 CMC 的日期和时间，格式为 *MM/DD/YYYY*，其中 *MM* 代表月，*DD* 代表日期，*YYYY* 代表年。		
"Active CMC Location"（活动 CMC 的位置）	显示活动 CMC 的位置。		
"Redundancy Mode"（冗余模式）	如果机箱中存在待机 CMC，则显示**"Redundant"（冗余）**，如果机箱中不存在待机 CMC，则显示**"No Redundancy"（无冗余）**。		

5. "**Virtual Reseat Server"（虚拟重置服务器）**部分**（"Reset Components"[重设组件]）**页显示以下信息：

表 12-12. 虚拟重置服务器

属性	说明		
"Slot"（插槽）	显示机箱中服务器占用的插槽。插槽名称是从 1 到 16 的连续 ID，帮助确定机箱中服务器的位置。		
"Name"（名称）	显示每个插槽中的服务器名称。		
"Present"（存在）	显示插槽中是否存在服务器（**"Yes"[存在]** 或**"No"[无]**）。		
"Health"（运行状况）		"OK"（良好）	服务器存在并且与 CMC 通信。在 CMC 和服务器间发生通信故障时，CMC 将无法获取或显示服务器的运行状况。
		"Informational"（通知）	如果运行状况没有更改（良好、警告、严重），则显示有关服务器的信息。

	⚠	"Warning"（警告）	发出了警告警报，**必须采取更正措施**。如果未采取更正措施，则可发生影响服务器完整性的严重故障。
	✖	"Severe"（严重）	已至少发出一个故障警报。严重状况表示发生 CMC 系统故障，**必须立即采取补救措施**。
iDRAC 状态	显示嵌入管理控制器的服务器 iDRAC 的状态： • **"N/A"（无）**- 服务器不存在，或机箱没有开机。 • **"Ready"（就绪）**- iDRAC 已就绪并正常操作。 • **"Corrupted"（已损坏）**- iDRAC 固件损坏。使用 iDRAC 固件更新实用程序维修固件。 • **"Failed"（已失败）**- 无法和 iDRAC 通信。使用"Virtual Reseat"（虚拟重置）复选框清除错误。如果此操作失败，请手动拆卸并更换服务器以清除错误。 • **"FW Update"（固件更新）**- 正在进行 iDRAC 固件更新；尝试任何操作前请先完成更新。 • **"Initializing"（初始化）**- 正在重设 iDRAC；尝试任何操作前请等待控制器完成开机。	
"Power State"（电源状态）	显示服务器电源状态。 • **"N/A"（无）—** CMC 尚未确定服务器的电源状态。 • **"Off"（关）**- 服务器或机箱关闭。 • **"On"（开）**— 机箱和服务器都打开。 • **正在开机 —** 关闭和打开之间的临时状态。当开机操作完成后，"Power State"（电源状态）将更改为"On"（开）。 • **正在关机** - 打开和关闭之间的临时状态。当关机操作完成后，"Power State"（电源状态）将更改为"Off"（关）。	
虚拟重置	选中该复选框虚拟重置该服务器。	

6. 要虚拟重置服务器，请单击要重置的服务器的复选框，然后选择**"Apply Selections"（应用选择）**。执行此操作后，服务器的行为与执行拆卸并重新插入操作后的行为相同。

7. 选择**"Reset/Failover CMC"（重设/故障转移 CMC）**会重设活动的 CMC。如果存在待机 CMC 并且机箱完全冗余，发生的故障转移会使待机 CMC 变为活动状态。

排除网络时间协议 (NTP) 错误故障

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改变，可能需要排除故障。CMC 无法同步其时钟的几种原因包括：

- NTP 服务器 1、NTP 服务器 2 和 NTP 服务器 3 设置可能出现问题。
- 可能不小心输入了无效的主机名或 IP 地址。
- 可能出现网络连通性问题，使 CMC 无法与配置的任何 NTP 服务器通信。
- 可能出现 DNS 问题，阻止解析任何 NTP 服务器主机名称。

CMC 提供工具以排除这些问题故障，主要故障排除信息的来源是 CMC 跟踪日志。此日志包含有关 NTP 故障的错误信息。如果 CMC 无法与配置的任何远程 NTP 服务器同步，则将从本地系统时钟导出其定时。

如果 CMC 同步到本地系统时钟而非远程时间服务器，跟踪日志将包含如下所示的条目：

```
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 getractime -n
```

如果配置的一台服务器没有显示 `*'，可能有些内容没有正确设置。上述命令的输出还包含详细的 NTP 统计数据，在针对服务器不同步情况进行调试时，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 参数可能会有所帮助。更改此参数之前，阅读并理解执行此操作的可能后果，因为默认设置应足够大到能配合多数 NTP 服务器的运行。要修改参数，请键入以下命令：

```
racadm config -g cfgRemoteHosts -o cfgRhostsNtpMaxDist 32
```

做出更改之后，禁用 NTP，等待 5-10 秒，然后重新启用 NTP，来重新启动 ntpd。

注： NTP 还需要 3 分钟来尝试和重新同步。

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，则确认 CMC 不能与任何已配置的 NTP 服务器同步。

可能有其他 NTP 相关的跟踪日志为您的故障排除工作提供帮助。如果是 NTP 服务器 IP 地址误配置问题，可能看到如下所示的条目：

```
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
```

请参阅"使用诊断控制台"了解如何输入 `gettracelog` 命令以使用 CMC GUI 查看跟踪日志的信息。

LED 颜色和闪烁样式说明

机箱上的 LED 可以通过颜色和闪烁/不闪烁提供信息：

- 稳定发光、绿色的 LED 表示组件已打开电源。如果绿色 LED 正在闪烁，则表示一件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。它不表示故障。
- 组件上正在闪烁的琥珀色 LED 表示该模块发生故障。
- 蓝色、闪烁 LED 可由用户配置并可用于标识（请参阅 "配置 LED 以识别机箱上的组件"）。

表 12-13. LED 颜色和闪烁样式

组件	LED 颜色、闪烁样式	含义
CMC	绿色、稳定发光	打开电源
	绿色、正在闪烁	正在上载固件
	绿色、不发光	关机
	蓝色、稳定发光	活动
	蓝色、正在闪烁	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、不发光	待机
iKVM	绿色、稳定发光	打开电源
	绿色、正在闪烁	正在上载固件
	绿色、不发光	关机
	琥珀色、稳定发光	未使用
	琥珀色，闪烁	故障
	琥珀色、不发光	无故障
服务器	绿色、稳定发光	打开电源
	绿色、正在闪烁	正在上载固件
	绿色、不发光	关机
	蓝色、稳定发光	正常
	蓝色、正在闪烁	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、不发光	无故障
IOM（常规）	绿色、稳定发光	打开电源
	绿色、正在闪烁	正在上载固件
	绿色、不发光	关机
	蓝色、稳定发光	正常/堆栈主
	蓝色、正在闪烁	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、不发光	无故障/堆栈从属
IOM （直通）	绿色、稳定发光	打开电源
	绿色、正在闪烁	未使用
	绿色、不发光	关机
	蓝色、稳定发光	正常
	蓝色、正在闪烁	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、不发光	无故障

风扇	绿色、稳定发光	风扇正在工作
	绿色、正在闪烁	未使用
	绿色、不发光	关机
	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：转速计超过范围
	琥珀色、不发光	未使用
PSU	（椭圆）绿色、稳定发光	交流正常
	（椭圆）绿色、正在闪烁	未使用
	（椭圆）绿色、不发光	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、不发光	无故障
	（圆形）绿色、稳定发光	直流正常
	（圆形）绿色、不发光	直流不正常

排除无响应 CMC 故障

注： 无法使用串行控制台登录待机 CMC。

如果使用任何界面（Web 界面、远程登录、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。

观察 LED 隔离问题

正对安装在机箱中的 CMC 前方，可以看到插卡的左侧有两个 LED。

顶部 LED — 顶部的绿色 LED 指示电源。如果该 LED 未发光：

1. 验证至少有一个电源有交流电。
2. 验证 CMC 卡正确接入。可以释放/拉动排出器手柄，卸下 CMC，重新安装 CMC 以确保插板已安装到位且闩锁正确关闭。

底部 LED — 底部 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 为蓝色。如果是琥珀色，则表示检测到故障。故障可能有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/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。在冗余、两个 CMC 配置中，待机 CMC 仅启用顶部绿色的 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：

1. 在 CMC 和客户端计算机之间安装 NULL 调制解调器电缆。
2. 打开选择的（如 HyperTerminal 或 Minicom）终端仿真器。设置：8 位、无奇偶校验、无流控制、波特率 115200。

   核心内存故障将每隔 5 秒钟显示一次错误信息。
3. 按 <Enter> 键。如果出现**"recovery"（恢复）**提示，则可以获得其它信息。该提示将指示 CMC 插槽号和故障类型。

   要显示故障原因和一些命令的语法，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

- 如果提示表明"self test failure"（自检故障），则 CMC 上没有能够提供服务的组件。CMC 已损坏，必须返回给 Dell。
- 如果提示表明**"Bad FW Images"（固件映像损坏）**，则按照 "恢复固件映像" 中的步骤修复问题。

恢复固件映像

当 CMC 无法正常引导到操作系统时，它将进入恢复模式。在恢复模式中，提供少量命令子集以便通过上载固件更新文件 **firmimg.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。

当键入 recover 然后按下 <Enter> 时，（在 **recovery** 提示符下）将显示恢复原因和可用子命令。一个恢复顺序示例：

```
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： 在恢复模式中，因为没有活动网络堆栈，所以无法正常 ping CMC。**recover ping <TFTP 服务器 IP>** 命令能够 ping TFTP 服务器以检验 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 跟踪日志允许调试 CMC 警报和网络。可使用 CMC Web 界面（请参阅"使用诊断控制台"）或 RACADM（请参阅"使用 RACADM 命令行界面"和《*Dell Chassis Management Controller 管理员参考指南*》中的 **gettracelog** 命令部分）访问跟踪日志。

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 managed system 的操作系统。

重置遗忘的管理员密码

小心： 多数维修只能由经认证的维修技术人员进行。您只能根据产品说明文件中的授权，或者在联机或电话服务和支持小组的指导下，进行故障排除和简单的维修。未经 Dell 授权的维修所造成的损坏不在保修范围之内。请阅读并遵循产品附带的安全说明。

要执行管理活动，用户必须具有**"Administrator"（管理员）**权限。CMC 软件具有用户帐户密码保护安全功能，如果忘记了管理员账户密码，可以禁用该帐户。如果忘记了管理员账户密码，可以使用 CMC 板上的 PASSWORD_RSET 跳线恢复密码。

CMC 板具有双插针密码重设连接器，如 图 12-1 所示。如果跳线安装在重设连接器中，则将启用默认管理员帐户和密码并设置为默认值，即**用户名：root** 和**密码：calvin**。无论帐户是否已删除或密码是否已更改，都将重设管理员帐户。

注： 开始之前，请确保 CMC 模块处于被动状态。

要执行管理活动，用户必须具有"Administrator"（管理员）权限。如果忘记了管理员账户密码，可以使用 CMC 板上的 PASSWORD_RST 跳线重置密码。

PASSWORD_RST 跳线使用两针接头，如 图 12-1 所示。

安装 PASSWORD_RST 跳线时，启用默认管理员帐户和密码且设置为以下默认值：

用户名：root

密码：calvin

如果删除管理员帐户或改变密码，管理员帐户也会临时重置。

注： 在安装 PASSWORD_RST 跳线后，则采用默认串行控制台配置（而不是配置属性值），具体如下：

```
cfgSerialBaudRate=115200

cfgSerialConsoleEnable=1
```

```
cfgSerialConsoleQuitKey=^\

cfgSerialConsoleIdleTimeout=0

cfgSerialConsoleNoAuth=0

cfgSerialConsoleCommand=""

cfgSerialConsoleColumns=0
```

1. 按下手柄上的 CMC 松开锁，并移动手柄使其从模块前面板松开。将 CMC 模块滑出机柜。

注： 静电放电 (ESD) 事件可损坏 CMC。在某些情况下，ESD 会在您身体上或在物体上积累，然后释放到 CMC 中。为了防止 ESD 损害，必须采取预防措施以防止您在机箱外处理和接触 CMC 时身体释放静电。

2. 从密码重设连接器中取出跳线插头，并插入 2 插针跳线以启用默认管理员账户。要在 CMC 板上找到密码跳线，请参阅 图 12-1。

图 12-1. 密码重设跳线位置

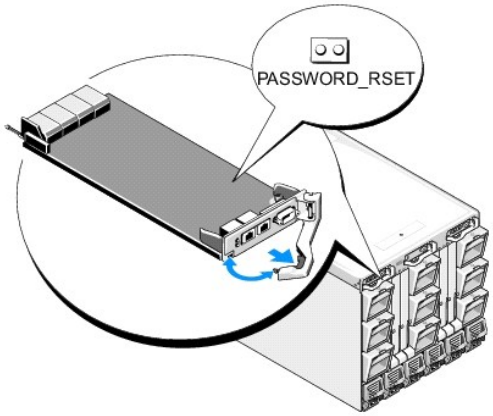


表 12-14. CMC 密码跳线设置

PASSWORD_RSET	（默认设置）	已禁用密码重设功能。
		已启用密码重设功能。

3. 将 CMC 模块滑入机柜中。将任何断开的电缆重新连接起来。

注： 确保 CMC 模块成为活动 CMC，并在剩余步骤完成前保持为活动的 CMC。

4. 如果跳线后的 CMC 模块只是 CMC，那么只需等待其完成重启。如果机箱中有冗余 CMC，则会发起切换使跳线后的 CMC 活动。使用 GUI 界面执行以下步骤：
   a. 导航至**"Chassis"（机箱）**页，单击**"Power Management"（电源管理）**选项卡→ **"Control"（控制）**子选项卡。
   b. 选择**"Reset CMC (warm boot)"（重设 CMC [温引导]）**按钮。
   c. 单击**"Apply"（应用）**。

   CMC 自动故障转移到冗余模块，该模块现在就变为活动模块。

5. 使用默认管理员名 **root** 和密码 **calvin** 登录到活动 CMC，并重设任何所需的用户帐户设置。现有账户和密码未禁用，仍处于活动状态。

6. 执行任何所需的管理操作，包括创建新管理员密码以替代忘记的密码。

7. 取出 2 针 PASSWORD_RST 跳线并重新插上跳线插头。
   a. 按下手柄上的 CMC 松开锁，并移动手柄使其从模块前面板松开。将 CMC 模块滑出机柜。
   b. 取出 2 插针跳线并更换跳线插头。
   c. 将 CMC 模块滑入机柜中。将任何断开的电缆重新连接起来。重复 步骤 4 以确保未跳线的 CMC 模块成为活动 CMC。

排除警报故障

使用 CMC 日志和跟踪日志对 CMC 警报进行故障排除。每次成功或失败的电子邮件和/或 SNMP 陷阱传递尝试都将记录到 CMC 日志。描述特定错误的其他信息将记录到跟踪日志中。但是，由于 SNMP 并不确认陷阱的传输，因此请使用网络分析器或 Microsoft 的 **snmputil** 等工具跟踪 managed system 中的信息包。

可以使用 Web 界面配置 SNMP 警报。有关详情，请参阅"配置 SNMP 警报"。

目录

目录

使用 CMC Web 界面

Dell Chassis Management Controller Firmware
版本 3.0 用户指南

CMC 提供 Web 界面，可以使用它配置 CMC 属性和用户、执行远程管理任务并对远程（管理型）系统问题进行故障排除。CMC Web 界面还可用于机箱日常管理。本章提供关于如何使用 CMC Web 界面执行常规机箱管理任务的信息。

还可以使用本地 RACADM 命令或命令行控制台（串行控制台、远程登录或 SSH）执行所有配置任务。有关使用本地 RACADM 的详情，请参阅 "使用 RACADM 命令行界面"。有关使用命令行控制台的信息，请参阅 "配置 CMC 使用命令行控制台"。

注： 如果使用 Microsoft Internet Explorer，通过代理连接时得到"The XML page cannot be displayed"（无法显示 XML 页）的错误，则需要禁用代理以继续。

访问 CMC Web 界面

要通过 IPv4 访问 CMC Web 界面：

1. 打开支持的 Web 浏览器窗口。

   有关支持的 Web 浏览器的最新信息，请参阅 Dell 支持网站 **support.dell.com/manuals** 上的《*Dell 系统软件支持值表*》。

2. 在"Address"（地址）字段中键入以下 URL，然后按 <Enter>：

   `https://<CMC IP 地址>`

   如果默认 HTTPS 端口号（端口 443）已更改，请键入：

   `https://<IP 地址>:<端口号>`

   其中 <CMC IP 地址> 是 CMC 的 IP 地址，而 <端口号> 是 HTTPS 端口号。

   随即显示 CMC**"Login"（登录）**页。

要通过 IPv6 访问 CMC Web 界面：

1. 打开支持的 Web 浏览器窗口。

   有关支持的 Web 浏览器的最新信息，请参阅 Dell 支持网站 **support.dell.com/manuals 上的**《*Dell 系统软件支持值表*》。

2. 在**"Address"（地址）**字段中键入以下 URL，然后按 <Enter>：

   `https://[<CMC IP 地址>]`

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

   如果您仍然使用默认值 (443)，则可以根据情况决定是否在 URL 中指定 HTTPS 端口号。否则，必须指定端口号。如果指定端口号，IPv6 CMC URL 语法是：

   `https://[<CMC IP 地址>]:<端口号>`

   其中 <*CMC IP 地址*> 是 CMC 的 IP 地址，而 <*端口号*> 是 HTTPS 端口号。

随即显示 **CMC"Login"（登录）**页。

登录

注： 要登录到 CMC，必须拥有具备**登录到 CMC** 权限的 CMC 帐户。

注： 默认 CMC 用户名是 **root**，默认密码是 **calvin**。root 帐户是与 CMC 一并提供的默认管理帐户。为增加安全性，强烈建议您在首次设置时更改 root 帐号的默认密码。

注： CMC 不支持扩展的 ASCII 字符（如 、、é、ü）或主要在非英语语言中使用的其它字符。

注： 不能在单个工作站上的多个浏览器窗口中使用不同的用户名登录到 Web 界面。

您可以作为 CMC 用户或 Directory 用户登录。

要登录：

1. 在**"Username"（用户名）**字段中，键入您的用户名：
   - CMC 用户名：<*用户名*>
   - Active Directory 用户名：<*域*>\<*用户名*>、<*域*>/<*用户名*>或<用户>@<域>。
   - LDAP 用户名：<用户名>

   注： 此字段区分大小写。
2. 在**"Password"（密码）**字段，键入您的 CMC 用户密码或 Active Directory 用户密码。

   注： 此字段区分大小写。
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间。默认值为 Web 服务会话空闲超时。有关详情，请参阅"配置服务"。
4. 单击**"OK"（确定）**或按 <Enter>。

注销

当登录到 Web 界面后，可以随时通过单击任意页面右上角的**"Logout"（注销）**注销。

注： 应用（保存）页面上输入的设置或信息时请小心。如果没有应用更改就注销或导航到其它页面，则更改将丢失。

配置基本的 CMC 设置

设置机箱名称

可以设置用于识别网络中机箱的名称。（默认名称是"Dell 机架系统"。）例如，对机箱名称进行 SNMP 查询时，将返回您配置的名称。

要设置机箱名称：

1. 登录 CMC Web 界面。随即显示**"Chassis Health"（机箱运行状况）**页。
2. 单击**"Setup"（设置）**选项卡。随即显示**"General Chassis Settings"（常规机箱设置）**页。
3. 在**"Chassis Name"（机箱名称）**字段中键入新名称，然后单击**"Apply"（应用）**。

设置 CMC 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。

1. 登录 CMC Web 界面。随即显示**"Chassis Health"（机箱运行状况）**页。
2. 单击**"Setup"（设置）**选项卡。随即显示**"General Chassis Settings"（常规机箱设置）**页。

3. 单击**"Date/Time"（日期/时间）**子选项卡。随即显示**"Date/Time"（日期/时间）**页。

4. 要将日期和时间与网络时间协议 (NTP) 服务器同步，请选中**"Enable NTP"（启用 NTP）**并最多指定三台 NTP 服务器。

5. 要手动设置日期和时间，请取消选中**"Enable NTP"（启用 NTP）** 并编辑**"Date"（日期）**和**"Time"（时间）**字段，从下拉菜单选择**"Time Zone"（时区）**，然后单击**"Apply"（应用）**。

要使用命令行界面设置日期和时间，请参阅*《Dell Chassis Management Controller 管理员参考指南》*中的 `config` 命令和 `cfgRemoteHosts` 数据库属性组部分。

机箱运行状况页

登录到 CMC 后，**显示"Chassis Health"（机箱运行状况）**页（**"Chassis Overview"（机箱概览）→ "Properties"（属性）→ "Health"（运行状况）**）。此页提供常用信息和操作。

"Chassis Health"（机箱运行状况）页显示机箱及其组件的实时图形视图以及组件详情。根据选择的组件，可提供各种操作或到其他页面的链接。另外，也会显示 CMC 硬件日志中的最新事件。

"Chassis Health"（机箱运行状况）页中的所有信息都会动态更新。此页面由两个主要部分组成：顶部的**"Chassis Component Summary（机箱组件摘要）**和下面的**"Recent CMC Hardware Log Events"（最近 CMC 硬件日志事件）**列表。

"Chassis Component Summary（机箱组件摘要）部分（在显示整体机箱信息时标题也可为"机箱运行状况"）显示图形及其相关信息。您可单击**"Close"（关闭）**图标整体隐藏这个部分。

"Chassis Component Summary（机箱组件摘要）的左半部分显示图形和机箱快速链接。右半部分显示与所选组件相关的信息、链接和操作。单击组件的图形化表示即可选择此组件。图形在选择后呈蓝色。

"Recent CMC Hardware Log Events"（最新 CMC 硬件日志事件）列表显示此日志中最新的 10 个事件。此部分的内容动态更新且列表顶部显示最近发生的事件。有关 CMC 硬件日志条目详情，请参阅 "查看事件日志"。

机箱组件摘要

机箱图形

机箱由前后视图展示（分别为上图和下图）。服务器和 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。服务器图标在 表 5-1 中作为示例。其他组件显示图标代表具体组件。服务器和 IOM 的图标在安装双倍规格组件时可跨越多个插槽。将鼠标放在组件上可显示工具提示，提供该组件的附加信息。

表 5-1. 服务器图标状态

图标	说明
	服务器开机和工作正常。
	服务器关闭。
	服务器报告不严重错误。

	服务器报告严重错误。
	无服务器。

机箱快速链接在机箱图形下显示。

表 5-2. 机箱快速链接

字段	说明
"Configure Users"（配置用户）	导航至"Chassis Overview"（机箱概览）→"User Authentication"（用户验证）→"Local Users"（本地用户）
网络配置	导航至"Chassis Overview"（机箱概览）→"Network"（网络）→"Network"（网络）
电源配置	导航至"Chassis Overview"（机箱概览）→"Power"（电源）→ "Configuration"（配置)
固件更新	导航至"Chassis Overview"（机箱概览）→ "Update"（更新）→"Firmware Update"（固件更新）

机箱运行状况

在此页面第一次显示时，页面右侧含机箱级别信息和警报。所有活动的严重和不严重警报都会显示。

单击组件后，机箱级别信息会被所选组件的信息替换。若要返回到机箱级别信息，则单击右上角的**"Return to Chassis Health"（返回到机箱运行状况）**。

表 5-3. 机箱页面信息

字段	说明
"Model"（型号）	显示机箱 LCD 面板的型号。
Firmware（固件）	显示活动 CMC 的固件版本。
Service Tag（服务标签）	显示机箱的服务标签。服务标签是制造商提供的用于支持和维修的唯一标识符。
Asset Tag（资产标签）	显示机箱的资产标签。
Input Power（输入功率）	机箱目前消耗的功率。
Power Cap（功率上限）	用户分配的允许消耗的最大输入功率。在机箱达到此限值后，服务器开始节流以防止所需输入功率进一步上升。
Power Policy（电源策略）	用户为协调多个供电装置分配的首选项。
Health（运行状况）	显示机箱电源子系统的整体运行状况。

Selected Component Information（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

  在此显示硬件日志显示的活动的严重和不严重事件（如有）。随时间变化的性能数据也在此显示。

- Properties（属性）

  在此显示不随时间变化或仅偶尔更改的组件属性。

- Quick Links（快速链接）

  "快速链接"部分提供导航至常用页面以及常用操作的便捷方式。只有适用于所选组件的链接才会在此部分显示。

表 5-4. 运行状况和性能信息 - 服务器

项目	说明
"Power State"（电源状态）	服务器的开/关状态。有关各种类型电源状态的详情，请参阅"表 5-23"。
"Health"（运行状况）	显示相当于运行状况图标的文本。
"Power Consumption"（功耗）	服务器目前消耗的功率。
"Power Allocated"（分配功率）	服务器预算的电源数量。
"Temperature"（温度）	服务器温度传感器的读数。

表 5-5. 服务器属性

项目	说明
"Name"（名称）	用户分配的插槽名称。
"Model"（型号）	服务器型号，例如"PowerEdge M600"或"PowerEdge M605"。
"Service Tag"（服务标签）	服务器的服务标签。服务标签是制造商提供的用于支持和维修的唯一标识符。如果没有服务器，此字段为空。
操作系统	服务器上的操作系统。
"Host Name"（主机名）	操作系统确定的服务器名称。
iDRAC	服务器上 iDRAC 固件的版本。
BIOS	服务器 BIOS 版本。
CPLD	服务器的复杂可编程逻辑器件 (CPLD) 的版本号。

表 5-6. 快速链接 - 服务器

项目	说明
服务器状况	导航至**"Server Overview"（服务器概览）→** <*所选服务器*>**→ "Properties"（属性）→ "Status"（状态）**
启动远程控制台	在服务器上启动键盘-视频-鼠标 (KVM)会话（如果服务器支持此操作）。
启动 iDRAC GUI	为服务器启动 iDRAC 管理控制台。
服务器开机	为处于"关闭"状态的服务器供电。
关闭服务器	为处于"打开"状态的服务器断电。
远程文件共享	导航至**"Server Overview"（服务器概览）→ "Setup"（设置）→ "Remote File Share"（远程文件共享）**
部署 iDRAC 网络	导航至**"Server Overview"（服务器概览）→ "Setup"（设置）→ iDRAC**（部署 iDRAC）

表 5-7. IOM 运行状况和性能

项目	说明
"Power State"（电源状态）	显示 I/O 模块的电源状况：开、关或未知（不存在）。
"Role"（角色）	在链接 I/O 模块时显示 I/O 模块的堆栈成员关系。"Member"（成员）指示模块是堆栈组的一部分。"Master"（主要）指示模块是主要访问点。

表 5-8. IOM 属性

项目	说明
"Model"（型号）	显示 I/O 模块产品名称。
"Service Tag"（服务标签）	显示 I/O 模块的服务标签。服务标签是由 Dell 提供的用于支持和维护的唯一标识符。

表 5-9. 快速链接 - I/O 模块

项目	说明
IOM 状况	导航至**"I/O Modules"（输入/输出模块）→** <*所选 IOM*>**→ "Properties"（属性）→ "Status"（状态）**
启动 IOM GUI	如果存在特定 I/O 模块的"*启动 IOM GUI*"链接，单击它可在新浏览器窗口或选项卡中为该 IOM 模块启动 I/O 管理控制台。

表 5-10. 活动的 CMC 运行状况和性能

项目	说明
"Redundancy Mode"（冗余模式）	显示待机 CMC 的故障转移就绪程度。如果 CMC 固件不匹配或 CMC 未正确连接到管理网络，则冗余会不可用。

"MAC Address"（MAC 地址）	显示 CMC 网络接口卡 (NIC) 的 MAC 地址。MAC 地址是 CMC 在整个网络中的唯一标识符。
IPv4	显示 CMC 网络接口的当前 IPv4 地址。
IPv6	显示 CMC 网络接口的第一个 IPv6 地址。

表 5-11. CMC 属性

项目	说明
固件	显示活动 CMC 的固件版本。
待机固件	显示安装在待机 CMC 上的固件版本。如果未安装第二个 CMC，则此字段显示"NA"（不可用）。
上次更新	显示上次更新固件的时间。如果未更新，则此字段显示"NA"（不可用）。
硬件	显示活动 CMC 的硬件版本。

表 5-12. 快速链接 - CMC

项目	说明
CMC 状态	导航至**"Chassis Controller"（机箱控制器）→ "Properties"（属性） → "Status"（状态）**
网络	导航至**"Chassis Overview"（机箱概览）→ "Network"（网络） → "Network"（网络）**
固件更新	导航至**"Chassis Overview"（机箱概览）→ "Update"（更新）→ "Firmware Update"（固件更新）**

表 5-13. iKVM 运行状况和性能

项目	说明
OSCAR 控制台	显示是否启用后面板 VGA 接头（"Yes"（是）或"No"（否））访问 CMC。

表 5-14. iKVM 属性

项目	说明
"Name"（名称）	显示 iKVM 的名称。
"Part Number"（部件号）	显示 iKVM 的部件号。部件号是供应商提供的唯一标识符。部件号命名习惯随供应商而有所差别。
"Firmware"（固件）	显示 iKVM 的固件版本。
"Hardware"（硬件）	显示 iKVM 的硬件版本。

表 5-15. 快速链接 - iKVM

项目	说明
iKVM 状态	导航至 **iKVM→ "Properties"（属性）→ "Status"（状态）**
固件更新	导航至**"Chassis Overview"（机箱概览）→ "Update"（更新）→ "Firmware Update"（固件更新）**

表 5-16. 风扇运行状况和性能

项目	说明
速率	按每分钟转数 (RPM) 显示风扇速度。

表 5-17. 风扇属性

项目	说明
临界阈值下限	低于此速度即视为风扇故障。
临界阈值上限	高于此速度即视为风扇故障。

表 5-18. 快速链接 - 风扇

项目	说明
风扇状态	导航至**"Fans"（风扇）→ "Properties"（属性）→ "Status"（状态）**

表 5-19. PSU 运行状况和性能

项目	说明
"Power Status"（电源状况）	显示电源设备的电源状态（以下之一）："Initializing"（正在初始化）、"Online"（联机）、"Standby"（待机）、"In Diagnostics"（诊断中）、"Failed"（故障）、"Updating,"（更新中）、"Offline"（脱机）或"Unknown"（未知）。

表 5-20. PSU 属性

项目	说明
容量	显示电源设备容量（瓦特）。

表 5-21. 快速链接 - PSU

项目	说明
"Power Supply Status"（电源设备状态）	导航至**"Power Supplies"（电源设备）→"Properties"（属性）→ "Status"（状态）**
"Power Consumption"（功耗）	导航至**"Chassis Overview"（机箱概览）→ "Power"（电源）→ "Power Consumption"（功耗）**
"System Budget"（系统预算）	导航至**"Chassis Overview"（机箱概览）→ "Power"（电源）→ "Budget Status"（预算状况）**

表 5-22. LCD 运行状况和性能

项目	说明
LCD 运行状况	显示 LCD 面板的存在和运行状况
机箱运行状况	显示机箱运行状况的文字说明。

LCD 无快速链接。

监测系统运行状况

查看机箱和组件摘要

CMC 显示**"Chassis Health"（机箱运行状况）**页面上代表机箱的图形，该图形提供已安装组件状态的可视概览。**"Chassis Health"（机箱运行状况）**页将动态更新，并且组件子图形的覆盖标记和文本提示会自动更改以反映当前状态。

图 5-1. Web 界面中的机箱图形示例

"Chassis Health"（机箱运行状况）页提供机箱、活动和待机 CMC、服务器模块、IO 模块 (IOM)、风扇、iKVM、电源 (PSU) 和 LCD 的总体运行状况。单击组件即可显示该组件的详情。有关查看机箱和组件摘要的说明，请参阅 "查看机箱摘要"。

查看电源预算状况

"Power Budget Status"（电源预算状况）页显示机箱、服务器和机箱电源设备装置 (PSU) 的电源预算状况。

有关查看电源预算状态的说明，请参阅 "查看功耗状态"。有关 CMC 电源管理的详情，请参阅 "电源管理"。

查看服务器型号名称和服务标签

使用以下步骤可及时获得每台服务器的型号名称和服务标签。

- 展开系统树中的"Servers"（服务器）。展开的"Servers"（服务器）列表中显示所有服务器 (1–16)。没有服务器的插槽名称将变灰。
- 将光标放在服务器的插槽名称或插槽编号上，工具提示会提示服务器的型号名称和服务标签（如果可用）。

查看所有服务器的运行状况

您可从**"Chassis Health"（机箱运行状况）**页面或**"Server Status"（服务器状况）**页面的**"Chassis Graphics"（机箱图形）**选项查看所有服务器的运行状况。

"Chassis Graphics"（机箱图形）提供已安装在机箱中的所有服务器的图形概览。

要使用"Chassis Graphics"（机箱图形）查看所有服务器的运行状况：

1. 登录 CMC Web 界面。

   将显示**"Chassis Health"（机箱运行状况）**页。**"Chassis Graphics"（机箱图形）**的左侧部分描述机箱的前视图并包含所有服务器的运行状况。服务器运行状况由服务器子图形的覆盖标记指示：

   - 无覆盖标记 — 服务器存在，电源打开并且正在与 CMC 通信；不存在不利条件。
   - 琥珀色小心标记 - 指示只发出警告警报并且必须采取纠正措施。
   - 红色 X - 指示至少存在一次故障。这表明 CMC 仍然能够同组件通信，且运行状况报告为严重。
   - 灰色且不可选 - 指示组件存在但未开机。它当前未与 CMC 通信且不存在不利条件。

"Servers Status"（服务器状况）页提供机箱中服务器的概览。若要使用"Servers Status"（服务器状况）页查看所有服务器的运行状况：

1. 登录 CMC Web 界面。
2. 在系统树中选择**"Server Overview"（服务器概览）**。随即出现**"Server Status"（服务器状况）**页。

表 5-23. 所有服务器状态信息

项目	说明		
插槽	显示服务器的位置。插槽号是顺序号，按机箱中的位置标识服务器。		
"Name"（名称）	显示服务器的名称，默认情况下由其所在的**插槽名称**（插槽-01 到插槽-16）确定。 **注：** 可更改默认服务器名称。有关说明，请参阅"编辑插槽名称"。		
"Model"（型号）	显示服务器型号名称。如果此字段空白，则服务器不存在。如果此字段显示"Extension of #"（# 的扩展）（其中 # 值为 1-8），则编号 # 是多插槽服务器的主要插槽。		
运行状况		"OK"（良好）	显示服务器存在并能与 CMC 通讯。
		"Informational"（通知）	如果运行状况没有更改，则显示有关服务器的信息。
		"Warning"（警告）	显示仅发出了警告警报，*必须采取纠正措施* 。如果未采取纠正措施，则可发生影响设备完整性的严重故障。
		"Critical"（严重）	显示至少已发出一个故障警报。严重状态表示服务器上发生系统故障，**必须立即采取纠正措施**。
		"No value"（无值）	当插槽中没有服务器时，不提供运行状况信息。
启动远程控制台	在服务器上于新浏览器窗口或选项卡中单击启动键盘-视频-鼠标 (KVM)会话 只有满足以下所有条件时，才会为服务器显示此图标： - 服务器为 PowerEdge M610、M610X、M710、M710HD 或 M910 - 机箱已开机 - 服务器上的 LAN 界面已启用 - iDRAC 版本为 2.20 或以上 此功能仅在满足以下条件时正确工作：		

	• 主机系统安装有 JRE（Java Runtime Environment）6 Update 16 或以上版本 • 主机上浏览器支持弹出窗口 （禁用弹出窗口阻止程序）
启动 iDRAC GUI	左键单击按钮，在新浏览器窗口或选项卡中启动服务器的 iDRAC 管理控制台。只有满足以下所有条件时，才会为服务器显示此图标： • 存在服务器 • 机箱已开机 • 服务器上的 LAN 界面已启用 此功能仅在满足以下条件时正确工作： • 主机上浏览器支持弹出窗口 （禁用弹出窗口阻止程序） **注：** 如果从机箱卸下服务器、iDRAC 的 IP 地址被更改或 iDRAC 上的网络连接遇到任何问题，则单击**"Launch iDRAC GUI"（启动 iDRAC GUI）**图标将显示有关 iDRAC LAN 界面的错误页。
"Power State"（电源状态）	显示服务器的电源状态： • **"N/A"（无）—** CMC 尚未确定服务器的电源状态。 • **关 —** 服务器关闭或机箱关闭。 • **开** — 机箱和服务器都打开。 • **正在开机 —** 关闭和打开之间的临时状态。当成功地完成操作后，**电源状态**将显示**开**。 • **正在关机** - 打开和关闭之间的临时状态。当成功地完成操作后，**电源状态**将显示**关**。
服务标签	显示服务器的服务标签。服务标签是制造商提供的用于支持和维修的唯一标识符。如果没有服务器，此字段为空。

有关如何启动 iDRAC 管理控制台和单次登录策略的信息，请参阅"使用单次登录启动 iDRAC"。

编辑插槽名称

"Slot Names"（插槽名称）页允许更新机箱中的插槽名称。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。不能有两个插槽具有相同的名称。
- 字符串不区分大小写。`Server-1`、`server-1` 和 `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-`
  - `KVM`
  - `DRAC-`
  - `MC-`
  - `Chassis`
  - `Housing-Left`
  - `Housing-Right`
  - `Housing-Center`
- 可以使用字符串 `Server-1` 到 `Server-16`，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。请注意 `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。

注： 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存在。

注： 插槽名称设置不会扩展到可选的 iKVM。插槽名称信息通过 iKVM FRU 提供。

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

要编辑插槽名称：

1. 登录 CMC Web 界面。
2. 选择系统树中**"Chassis"（机箱）**菜单中的**"Server Overview"（服务器概览）**。
3. 单击**"Setup"（设置）** → **"Slot Names"（插槽名称）**。随即显示**"Slot Names"（插槽名称）**页。

4. 在**"Slot Name"（插槽名称）**字段中键入插槽的更新名称或新名称。为每个想要重命名的插槽重复此操作。

5. 单击**"Apply"（应用）**。

6. 要将默认插槽名称（**SLOT-01** 到 **SLOT-16**，根据服务器的插槽位置）恢复到服务器，请按**"Restore Default Value"（恢复默认值）**。

用服务器的主机名称作为插槽名称。

"Slot Names"（插槽名称）页允许用服务器的主机名称（或系统名称）覆盖静态插槽名称。这要求服务器上安装 OMSA 代理。OMSA 代理的详情参见*Dell OpenManage 服务器管理员用户手册*。

若要用服务器的主机名称作为插槽名称：

1. 登录 CMC Web 界面。

2. 选择系统树中**"Chassis"（机箱）**菜单中的**"Server Overview"（服务器概览）**。

3. 单击**"Setup"（设置）** → **"Slot Names"（插槽名称）**。随即显示**"Slot Names"（插槽名称）**页。

4. 选择**"Use Host Name for the Slot Name "（用服务器主机名称作插槽名称）**复选框。

5. 单击**"Apply"（应用）**。

设置服务器的首个引导设备

"First Boot Device"（第一个引导设备）页允许为每台服务器指定 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，甚至不代表服务器中的设备，相反它代表会被 CMC 发送的设备，以及用作该服务器的第一引导设备。

可以设置默认引导设备，也可设置执行一次的引导设备，以便引导特殊映像来执行任务，如运行诊断或重新安装操作系统。

所指定的引导设备必须存在且包含可引导的介质。

表 5-24. 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
"Hard Drive"（硬盘驱动器）	从服务器的硬盘驱动器引导。
"Local CD/DVD"（本地 CD/DVD）	从服务器上的 CD/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。
"Virtual CD/DVD"（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磁盘上，并且使用 iDRAC GUI 控制台 Viewer 连接。
iSCSI	从因特网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 — 仅针对 M610/M710/M805/M905 系统。
"Floppy"（软盘）	从本地软盘驱动器中的软盘引导。

注： 要设置服务器的第一个引导设备，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。

在机箱中为部分或全部服务器设置首个引导设备的步骤：

1. 登录 CMC Web 界面。

2. 单击系统树中的**"Servers Overview"（服务器概览）**，然后单击**"Setup"（设置）→ "First Boot Device"（第一个引导设备）**。随即显示服务器列表，每行一个服务器。

3. 从列表框中选择每个服务器要使用的引导设备。

4. 如果要服务器每次引导时都从选中的设备引导，请取消选择服务器的 **Boot Once**（引导一次）复选框。

   如果要服务器只在下一个引导周期从选中的设备引导，请选择服务器的 **Boot Once**（引导一次）复选框。

5. 单击**"Apply"（应用）**。

查看所有单个服务器的运行状况

单个服务器的运行状况可以通过两种方法查看：从**"Chassis Health"（机箱运行情况）**页上的**"Chassis Graphics"（机箱图形）**部分，或者从**"Server Status"（服务器状态）**页。

"Chassis Graphics"（机箱图形）页提供机箱中单个服务器的图形概览。

要使用"Chassis Graphics"（机箱图形）查看单个服务器的运行状况：

1. 登录 CMC Web 界面。

   将显示**"Chassis Health"（机箱运行状况）**页。**"Chassis Graphics"（机箱图形）**的上半部分描述机箱的前视图并包含单个服务器的运行状况。服务器运行状况由服务器子图形的覆盖标记指示：

   - 无覆盖标记 — 指示服务器存在，电源打开并且正在与 CMC 通信；不存在不利条件。
   - 琥珀色小心标记 - 指示只发出警告警报并且必须采取纠正措施。
   - 红色 X - 指示至少存在一次故障。这表明 CMC 仍然能够同组件通信，且运行状况报告为严重。
   - 灰色且不可选 - 指示组件存在但未开机。它当前未与 CMC 通信且不存在不利条件。

- 移动光标到一个服务器子图形上。

  即会显示相应的文本提示或屏幕提示。文本提示提供有关该服务器的其它信息。

3. 单击服务器子图形可选择该服务器信息，并在机箱图形右侧显示快速链接。

"Server Status"（服务器状态）页（与*服务器***"Status"[状态]** 页不在同一页）提供服务器概览和指向集成 Dell 远程访问控制器 (iDRAC) Web 界面的启动位置，该界面即用于管理服务器的固件。

注： 要使用 iDRAC 用户界面，必须具有 iDRAC 用户名和密码。有关 iDRAC 和使用 iDRAC Web 界面的详情，请参阅 *Integrated Dell Remote Access Controller 固件用户指南*。

查看所有单个服务器的运行状况：

1. 登录 CMC Web 界面。
2. 在系统树中展开**"Server Overview"（服务器概览）。**展开的**"Servers"（服务器）**列表中出现的所有服务器 (1–16)。
3. 单击想要查看的服务器（插槽）。随即显示**"Server Status"（服务器状况）**页。

也可单击页面右侧服务器快速链接中的状况链接，查看服务状况页。

表 5-25. 单独 服务器状态 - 属性

项目	说明		
"Slot"（插槽）	显示机箱上服务器占用的插槽。插槽号是顺序 ID，从 1 到 16（机箱中有 16 个可用插槽），它有助于标识机箱中服务器的位置。		
" Slot Name"（插槽名称）	显示服务器所在插槽的名称。		
"Present"（存在）	显示插槽中是否存在服务器（"Yes"[存在] 或"No"[无]）。当服务器状态为无时，服务器的运行状况、电源状态和服务标签信息为未知（不显示）。		
运行状况		"OK"（良好）	显示服务器存在并能与 CMC 通讯。在 CMC 和服务器间发生通讯故障时，CMC 将无法获取或显示服务器的运行状况。
		"Informational"（通知）	如果运行状况没有变化（良好、警告、严重），则显示有关服务器的信息。
		"Warning"（警告）	显示仅发出了警告警报，*必须采取纠正措施* 。如果未采取纠正措施，则可发生影响服务器完整性的严重故障。
		"Critical"（严重）	显示至少已发出一个故障警报。严重状态表示服务器上发生系统故障，*必须立即采取纠正措施*。
		"No value"（无值）	当插槽中没有服务器时，不提供运行状况信息。
"Server Model"（服务器型号）	显示机箱中服务器的型号。示例：**PowerEdge M600**、**PowerEdge M605**。		
"Service Tag"（服务标签）	显示服务器的服务标签。服务标签是由制造商提供的用于支持和维护的唯一标识符。如果没有服务器，此字段为空。		
"iDRAC Firmware"（iDRAC 固件）	显示当前安装在服务器上的 iDRAC 版本。		
"CPLD Version"（CPLD 版本）	显示服务器的复杂可编程逻辑器件 (CPLD) 的版本号。		

"BIOS version"（BIOS 版本）	显示服务器上的 BIOS 版本。
"Operating System"（操作系统）	显示服务器上的操作系统。

表 5-26. 单独服务器状态 - iDRAC 系统事件日志

项目	说明		
严重性		"OK"（良好）	指示正常事件，无需采取修正操作。
		"Informational"（通知）	指示与严重性状态未发生变化的某个事件相关的通知项。
		未知	指示未知/未分类的事件。
		"Warning"（警告）	指示不严重事件，必须尽快采取纠正措施以避免系统故障。
		"Critical"（严重）	指示严重事件，要求立即采取修正操作以避免系统故障。
"Date/Time"（日期/时间）	显示发生事件的确切日期和时间（例如，"Wed May 02 16:26:55 2007"[2007 年 5 月 2 日，周三，16:26:55]）。		
说明	提供事件的简要说明。		

表 5-27. 单独服务器状态 - iDRAC 网络设置

项目	说明
"LAN Enabled"（LAN 已启用）	指示 LAN 信道是启用（**"Yes"[是]**）还是禁用（**"No"[否]**）。

表 5-28. 单独服务器状态 - IPv4 iDRAC 网络设置

项目	说明
已启用	指示是否在 LAN 中使用了 IPv4 协议（"Yes"[是]）。如果服务器不支持 IPv6，则 IPv4 协议总是处于启用状态，而且此设置不显示出来。
"DHCP Enabled"（已启用 DHCP）	指示动态主机配置协议 (DHCP) 是启用（**"Yes"[是]**）还是禁用（**"No"[否]**）。 如果启用（**"Yes"[是]**）该选项，服务器将自动从网络中的 DHCP 服务器检索 IP 配置（IP 地址、子网掩码和网关）。服务器将始终分配到网络中唯一的 IP 地址。
"IPMI over LAN Enabled"（LAN 上 IPMI 已启用）	指示 IPMI LAN 信道是启用（**"Yes"[是]**）还是禁用（**"No"[否]**）。
"IP Address"（IP 地址）	为 iDRAC 网络接口指定 IP 地址。
"Subnet Mask"（子网掩码）	为 iDRAC 网络接口指定子网掩码。
"Gateway"（网关）	为 iDRAC 网络接口指定网关。

表 5-29. 单独服务器状态 - IPv6 iDRAC 网络设置

项目	说明
已启用	指示在 LAN 上是否使用了 IPv6 协议（"Yes"[是]）。
"Autoconfiguration Enabled"（已启用自动配置）	指示是否已启用 IPv6 的自动配置（"Yes"[是]）。 如果已启用自动配置，服务器将自动从网络中的 IPv6 路由器检索 IPv6 配置（**IPv6 地址、前缀长度**和 **IPv6 网关**）。服务器始终具有网络中唯一的 IPv6 地址，最多可以给服务器指定 16 个 IPv6 地址。
"Link Local Address"（链路本地地址）	根据 CMC 的 MAC 地址给 CMC 分配的 IPv6 地址。
"Gateway"（网关）	显示 iDRAC 网络接口的 IPv6 网关。
"IPv6 Address"（IPv6 地址）	显示 iDRAC 网络接口的 IPv6 地址。最多可以有 16 个 IPv6 地址。如果前缀长度不是零，则在正斜杠 ("/") 后面指定。

表 5-30. 单独服务器状态 - WWN/MAC 地址

项目	说明

"Slot"（插槽）	显示机箱上服务器占用的插槽。
"Location"（位置）	显示输入/输出模块占用的位置。这六个位置由组名称（A、B 或 C）和插槽编号（1 或 2）的组合标识。位置名称：A1、A2、B1、B2、C1 或 C2。
"Fabric"（结构）	显示 I/O 结构的类型。
"Server-Assigned"（服务器分配）	显示嵌入控制器硬件中服务器分配的 WWN/MAC 地址。WWN/MAC 地址显示"N/A"（无），表示没有为指定结构安装接口。
"Chassis-Assigned"（机箱分配）	显示机箱分配的用于特定插槽的 WWN/MAC 地址。WWN/MAC 地址显示"N/A"（无），表示没有安装 FlexAddress 功能。 **注：** **"Server-Assigned"（服务器分配）**和**"Chassis-Assigned"（机箱分配）**列中的绿色复选标记表示活动地址的类型。 **注：** 启用 FlexAddress 时，没有安装服务器的插槽将显示机箱为嵌入以太网控制器（结构 A）分配的 MAC/WWN 任务。结构 B 和 C 的机箱分配地址显示"N/A"（无），除非这些结构在填充插槽中的服务器上使用；假设将在未填充的插槽中部署相同的结构类型。

有关如何启动 iDRAC 管理控制台和单次登录策略的信息，请参阅 "使用单次登录启动 iDRAC"。

查看 IOM 的运行状况

IOM 的运行状况可以用两种方法查看：从**"Chassis Health"（机箱运行状况）**页面上的**"Chassis Component Summary"（机箱组件摘要）**部分查看，或者从**"I/O Modules Status"（I/O 模块状态）**页查看。**"Chassis Health"（机箱运行状况）**页提供已安装在机箱中的 IOM 的图形概览。

要使用机箱图形查看 IOM 的运行状况：

1. 登录 CMC Web 界面。

   将显示**"Chassis Health"（机箱运行状况）**页。**"Chassis Graphics"（机箱图形）**的下半部分描述机箱的后视图并包含 IOM 的运行状况。IOM 运行状态由 IOM 子图形的覆盖标记表示：

   - 无覆盖标记 — IOM 存在，电源打开并且正在与 CMC 通信；不存在不利条件。
   - 琥珀色小心标记 - 指示只发出警告警报并且必须采取纠正措施。
   - 红色 X - 指示至少存在一次故障。这表明 CMC 仍然能够同组件通信，且运行状况报告为严重。
   - 灰色且不可选 - 指示 IOM 存在但未开机。它当前未与 CMC 通信且不存在不利条件。

2. 移动光标到一个 IOM 子图形上。

   即会显示文本提示或屏幕提示。文本提示提供有关该 IOM 的其它信息。

3. 单击 IOM 子图形可选择 IOM 的信息和快速链接，在机箱图形的右侧显示。。

"I/O Modules Status"（输入/输出模块状态）页提供与机箱关联的所有 IOM 的概览。有关通过 Web 界面或 RACADM 查看 IOM 运行状况的说明，请参阅 "监控 IOM 运行状况"。

查看风扇的运行状况

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 100% 旋转。这是正常现象。

风扇的运行状态可以通过两种方法查看：从**"Chassis Health"（机箱运行状况）**页上的**"Chassis Component Summary"（机箱组件摘要）**，或者从**"Fans Status"（风扇状态）**页。**"Chassis Health"（机箱运行状况）**页提供机箱中安装的所有风扇的图形概览。要使用**"Chassis Graphics"（机箱图形）**查看所有风扇的运行状况：

1. 登录 CMC Web 界面。

   将显示**"Chassis Health"（机箱运行状况）**页。**"Chassis Graphics"（机箱图形）**的下半部分描述机箱的后视图并包含所有风扇的运行状况。风扇运行状况由风扇子图形的覆盖标记表示：

   - 无覆盖标记 — 风扇存在且运行；不存在不利条件。
   - 琥珀色小心标记 - 指示只发出警告警报并且必须采取纠正措施。
   - 红色 X - 指示至少存在一次故障。这表示运行状况报告为严重。
   - 灰色且不可选 - 指示风扇存在但未开机。不存在不利条件。

2. 移动光标到一个风扇子图形上。

   即会显示文本提示或屏幕提示。文本提示提供有关该风扇的其它信息。

3. 单击风扇子图形可选择风扇的信息和快速链接，在机箱图形的右侧显示。。

"Fans Status"（风扇状况）页提供机箱中风扇的状况和速度测量值（以每分钟旋转次数或 RPM 为单位）。可以有一个或多个风扇。

控制风扇速度的 CMC 将根据系统范围内的事件自动提高或降低风扇速度。当发生以下事件时，CMC 将生成警报并提高风扇速度。

- 超过 CMC 机箱内温度阈值。
- 风扇故障。
- 从机箱中卸下风扇。

要查看风扇装置的运行状况：

1. 登录 CMC Web 界面。
2. 选择系统树中的**"Fans"（风扇）**。随即显示**"Fans Status"（风扇状况）**页。

也可单击页面右侧风扇信息快速链接中的状况链接，查看**"Fan Status"（风扇状况）**页。

表 5-31. 风扇运行状况信息

项目	说明		
"Name"（名称）	以 **FAN**-*n* 格式显示风扇名称，其中 n 为风扇编号。		
"Present"（存在）	指示风扇设备是否存在（**"Yes"[是]**或**"No"[否]**）。		
运行状况		"OK"（良好）	表示风扇装置存在并能与 CMC 通讯。在 CMC 和风扇装置间发生通讯故障时，CMC 将无法获取或显示风扇装置的运行状况。
		"Critical"（严重）	指示至少已发出一个故障警报。严重状况代表风扇装置出现系统故障，并且必须立即采取纠正措施以防止过热和系统关机。
		"Unknown"（未知）	当机箱首先开机时显示。在 CMC 和风扇装置间发生通讯故障时，CMC 将无法获取或显示风扇装置的运行状况。
"Speed"（速率）	表示以 RPM 为单位的风扇转速。		

查看 iKVM 状况

Dell M1000e 服务器机箱的本地访问 KVM 模块称为 Avocent 集成 KVM 交换机模块，或 iKVM。与机箱关联的 iKVM 的运行状况可以在**"Chassis Health"（机箱运行状况）**页查看。

要使用**"Chassis Graphics"（机箱图形）**查看 iKVM 的运行状况：

1. 登录 CMC Web 界面。

   将显示**"Chassis Health"（机箱运行状况）**页。**"Chassis Graphics"（机箱图形）**的下半部分描述机箱的后视图并包含 iKVM 的运行状况。iKVM 运行状况由 iKVM 子图形的覆盖标记表示：

   - 无覆盖标记 — iKVM 存在，电源打开并且正在与 CMC 通信；不存在不利条件。
   - 琥珀色小心标记 - 指示只发出警告警报并且必须采取纠正措施。
   - 红色 X - 指示至少存在一次故障。这表明 CMC 仍然能够同 iKVM 通信，且运行状况报告为严重。
   - 灰色且不可选 - 指示 iKVM 存在但未开机。它当前未与 CMC 通信且不存在不利条件。

- 移动鼠标到 iKVM 子图形上。

  即会显示文本提示或屏幕提示。文本提示提供有关该 iKVM 的其它信息。

3. 单击 iKVM 子图形可选择 iKVM 的信息和快速链接，在机箱图形的右侧显示。。

也可单击页面右侧 iKVM 快速链接中的状况链接，查看**"iKVM Status"（iKVM 状况）**页面。

有关查看 iKVM 状况和 iKVM 设置属性的说明，请参阅：

- "查看 iKVM 状况和属性"
- "启用或禁用前面板"
- "通过 iKVM 启用 Dell CMC 控制台"
- "更新 iKVM 固件"

有关 iKVM 的详情，请参阅 "使用 iKVM 模块"。

查看 PSU 的运行状况

与机箱相关联的 PSU 运行状况可以用两种方法查看：从**"Chassis Health"（机箱运行状况）**页的**"Chassis 组件摘要"（机箱Component Summary）**部分查看，或者从**"Power Supply Status"（电源状态）**页查看。**"Chassis Health"（机箱运行状况）**页提供机箱中安装的所有 PSU 的图形概览。

要使用**"Chassis Graphics"（机箱图形）**查看所有 PSU 的运行状况：

1. 登录 CMC Web 界面。

   将显示**"Chassis Health"（机箱运行状况）**页。**"Chassis Graphics"（机箱图形）**的下半部分描述机箱的后视图并包含所有 PSU 的运行状况。PSU 运行状态由 PSU 子图形的覆盖标记表示：

   - 无覆盖标记 — PSU 存在，电源打开并且正在与 CMC 通信；不存在不利条件。
   - 琥珀色小心标记 - 指示只发出警告警报并且必须采取纠正措施。
   - 红色 X - 指示至少存在一次故障。这表明 CMC 仍然能够同 PSU 通信，且运行状况报告为严重。
   - 灰色且不可选 - 指示 PSU 存在但未开机。它当前未与 CMC 通信且不存在不利条件。

2. 将光标停留在单个 PSU 子图形上方将显示相应的文本提示或屏幕提示。文本提示提供有关该 PSU 的其它信息。

3. 单击 PSU 子图形可选择 PSU 的信息和快速链接，在机箱图形的右侧显示。

"Power Supply Status"（电源设备状况）页显示与 PSU 与机箱相关的状况和读数。有关 CMC 电源管理的详情，请参阅 "电源管理"。

要查看 PSU 的运行状况：

1. 登录 CMC Web 界面。

2. 选择系统树中的**"Power Supplies"（电源设备）**。随即将显示**"Power Supply Status"（电源设备状况）**页。

也可单击页面右侧 PSU 快速链接中的状况链接，查看**"PSU Status"（PSU 状况）**页。

表 5-32. 电源设备运行状况信息

项目	说明		
"Name"（名称）	显示 PSU 的名称：*PS-n*，其中 *n* 为电源编号。		
"Present"（存在）	指示电源设备是否存在**（"Yes"[是]**或**"No"[否]**）。		
运行状况		"OK"（良好）	指示 PSU 存在并且与 CMC 通信。指示 PSU 的运行状况良好。在 CMC 和风扇单元通信失败的情况下，CMC 无法获得或显示 PSU 的运行状况。
		"Critical"（严重）	指示 PSU 发生故障，并且运行状况很严重。**必须立即采取修正操作。**如果执行此操作失败，可能是由电源损耗造成组件关闭。
		"Unknown"（未知）	当机箱首先开机时显示。在 CMC 和 PSU 之间发生通信故障时，CMC 不能获取或显示 PSU 的运行状况。
"Power Status"（电源状况）	表示 PSU 的电源状态：**"Online"（联机）**、**"Off"（关机）**或**"Slot Empty"（插槽空）**。		
容量	显示以瓦特为单位的电源功率。		

表 5-33. 系统电源状况

项目	说明
"Overall Power Health"（总体电源运行状况）	显示整个机箱的电源管理运行状况（**"OK"[良好]**、**"Non-Critical"[不严重]**、**"Critical"[严重]**、**"Non-Recoverable"[不可恢复]**、**"Other"[其它]**、**"Unknown"[未知]**）。
"System Power Status"（系统电源状况）	显示机箱的电源状态（"On"[开] 、"Off"[关]、"Powering On"[正在开机]、"Powering Off"[正在关机]）。
"Redundancy"（冗余）	显示电源设备冗余状态。值包括： **"No"（否）**：电源设备并非冗余。 **"Yes"（是）**：完全冗余有效。

查看温度传感器的状况

"**Temperature Sensors Status"（温度传感器状况）**页显示整个机箱（机箱和服务器）上温度探测器的状况和读数。

注： 温度探测器值不可编辑。任何超过阈值的更改都会生成警报，从而造成风扇速度变化。例如，如果 CMC 环境温度探测器超过阈值，机箱上风扇的速度将会提高。

要查看温度探测器的运行状况：

1. 登录 CMC Web 界面。
2. 选择系统树中的**"Temperature Sensors "（温度传感器）**。随即显示**"Temperature Sensors Status"（温度传感器状况）**页。

表 5-34. 温度传感器运行状况信息

项目	说明		
ID	显示温度传感器的位置。		
"Name"（名称）	显示机箱和服务器各温度传感器的名称。		
"Present"（存在）	指示机箱中的模块是存在 (Yes) 还是无 (No)。		
运行状况		"OK"（良好）	指示模块存在并能与 CMC 通讯。在 CMC 和服务器间发生通信故障时，CMC 将无法获取或显示服务器的运行状况。
		"Warning"（警告）	表示仅发出了警告警报，必须采取纠正措施。如果未采取纠正措施，则可发生影响模块完整性的严重故障。
		"Severe"（严重）	指示已发出一个故障警报。严重状况表示模块上发生系统故障，必须立即采取补救措施。
		"Unknown"（未知）	指示与模块的通信未建立。这通常是因为机箱电源关闭或机箱未完成初始化。
"Reading"（读数）	显示当前摄氏和华氏温度。		
"Threshold Maximum"（最大阈值）	显示允许的最高摄氏和华氏温度，达到这一温度时会发出故障警报。		

查看 LCD 的状况

LCD 的运行状况可通过**"Chassis Health"（机箱运行状况）**页上与机箱相关的机箱图形查看。

若要查看 LCD 的运行状况：

1. 登录 CMC Web 界面。

   将显示**"Chassis Health"（机箱运行状况）**页。机箱图形的上半部分显示机箱的前视图。LCD 运行状况由 LCD 子图形的覆盖标记表示：

   - 无覆盖标记 - LCD 存在、开机且与 CMC 通信。无不利条件。
   - 琥珀色小心标记 - 警告警报发出且必须采取纠正措施。
   - 红色 X - 至少存在一次故障。运行状况为严重。
   - 灰色且不可选 - LCD 存在但未开机。它当前未与 CMC 通信且不存在不利条件。

2. 移动光标到 LCD 子图形上。显示提供 LCD 附加信息的对应文本提示或屏幕提示。
3. 单击 LCD 子图形可选择 LCD 的信息并在机箱图形右侧显示。

查看全球名称/介质访问控制 (WWN/MAC) ID

"WWN/MAC Summary page"（WWN/MAC 摘要页）可以查看机箱中的 WWN 配置和插槽的 MAC 地址。

结构配置

"Fabric Configuration section"（结构配置部分）显示为结构 A、结构 B 和结构 C 安装的输入/输出结构类型。绿色复选标记表示该结构已启用 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。该功能以结构和插槽为单位启用。

注： 有关 FlexAddress 功能的详情，请参阅"使用 FlexAddress"。

WWN/MAC 地址

"WWN/MAC Address"（WWN/MAC 地址）部分显示分配给所有服务器的 WWN/MAC 信息，即便那些服务器插槽当前为空。**"Location"（位置）**显示输入/输出模块占用的插槽位置。这六个插槽由组名（A、B 或 C）和插槽编号（1 或 2）的组合标识：插槽名称 A1、A2、B1、B2、C1 或 C2。iDRAC 是服务器的集成管理控制器。**"Fabric"（结构）**显示 I/O 结构的类型。**"Server-Assigned"（服务器分配）**显示服务器分配的嵌入式控制器硬件的 WWN/MAC 地址。**"Chassis-Assigned"（机箱分配）**显示机箱分配的用于特定插槽的 WWN/MAC 地址。在**"Server-Assigned"（服务器分配）**或**"Chassis-Assigned"（机箱分配）**列中的绿色复选标记表示活动地址的类型。机箱分配地址当 FlexAddress 在机箱上激活时分配，并代表插槽永久地址。选中机箱分配地址时，将使用那些地址，即便一台服务器被另一台服务器取代。

配置 CMC 网络属性

注： 更改网络配置会导致当前网络登录的连接丢失。

设置对 CMC 的初始访问

在配置 CMC 之前，必须首先配置 CMC 网络设置以便远程管理 CMC。此初始配置分配可启用 CMC 访问的 TCP/IP 网络参数。

注： 必须具备**机箱配置管理员**权限才可以设置 CMC 网络设置。

1. 登录到 Web 界面。
2. 在系统树中选择**"Chassis Overview"（机箱概览）**。
3. 单击**"Network"（网络）**选项卡。显示**"Network Configuration"（网络配置）**页。
4. 通过选择或取消选择**"Use DHCP (For CMC Network Interface IP Address)"（使用 DHCP [获取 CMC 网络接口 IP 地址]）**复选框为 CMC 启用或禁用 DHCP。
5. 如果要禁用 DHCP，则请键入 IP 地址、网关和子网掩码。
6. 单击页面底部的**"Apply Changes"（应用更改）**。

配置网络 LAN 设置

注： 必须具备**机箱配置管理员**权限才可以设置 CMC 网络设置。

注： **"Network Configuration"（网络配置）**页中的设置（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。

注： 如果您的机箱具有两个 CMC（活动和待机），且他们均连接至网络，则在主 CMC 出现故障时备用 CMC 自动承继网络设置。

1. 登录到 Web 界面。
2. 单击**"Network"（网络）**选项卡。
3. 按照表 5-35 至表 5-37 中的说明配置 CMC 网络设置。
4. 单击**"Apply Changes"（应用更改）**。

要配置 IP 范围和 IP 阻塞设置，请单击**"Advanced Settings"（高级设置）**按钮（请参阅"配置 CMC 网络安全设置"）。

要刷新**"Network Configuration"（网络配置）**页中的内容，请单击**"Refresh"（刷新）**。

要打印**"Network Configuration"（网络配置）**页中的内容，请单击**"Print"（打印）**。

表 5-35. 网络设置

设置	说明
"CMC MAC Address"（BMC MAC 地址）	显示机箱的 MAC 地址，这是机箱在计算机网络中的唯一标识符。
启用 CMC 网络接口	启用 CMC 的网络接口。

	默认："Enabled"（已启用）。如果该选项被选中： • CMC 与之通信且通过计算机网络可以访问。 • 可以使用与 CMC 相关的 Web 界面、CLI（远程 RACADM）、WSMAN、远程登录和 SSH。 如果该选项未被选中： • CMC 网络接口不能在网络上通信。 • 无法通过 CMC 与机箱通信。 • 不能使用与 CMC 相关的 Web 界面、CLI（远程 RACADM）、WSMAN、远程登录和 SSH。 • 仍可访问服务器 iDRAC Web 界面、本地 CLI、输入/输出模块和 iKVM。 • 这种情况下，可以从机箱的 LCD 获取 iDRAC 和 CMC 的网络地址。 **注：** 机箱上的网络禁用（或掉失）时，不影响对机箱中其它可访问组件的访问。
"Register CMC on DNS"（在 DNS 上注册 CMC）	该属性在 DNS 服务器上注册 CMC 名称。 **"Default"（默认值）：**默认取消选取（禁用） **注：** 某些 DNS 服务器仅注册含有 31 个字符或更少字符的名称。确保指定的名称在 DNS 要求的范围内。
"DNS CMC Name"（DNS CMC 名称）	仅当选择 **"Register CMC on DNS"（在 DNS 上注册 CMC）**后才会显示 CMC 名称。默认 CMC 名称为 *CMC_service_tag*，其中 *service tag* 为机箱的服务标签。最多 63 个字符。第一个字符必须是字母 (a-z, A-Z)，其后可以是字母数字 (a-z, A-Z, 0-9) 或连字符 (-)。
"Use DHCP for DNS Domain Name"（使用 DHCP 来设置 DNS 域名）	使用默认 DNS 域名。仅当选择**"Use DHCP (For CMC Network InterfaceIP Address)"（使用 DHCP [获取 CMC 网络接口 IP 地址]）**时才可激活该复选框。 **默认：**"Enabled"（已启用）
"DNS Domain Name"（DNS 域名）	默认 DNS 域名是空字符。仅当选择了**"Use DHCP for DNS Domain Name"（使用 DHCP 设置 DNS 域名）**复选框时，才可编辑该字段。
自动协议 (1 Gb)	确定 CMC 是否通过与最近的路由器或交换机自动设置双工模式和网络速度（**"On"[开]**）或允许用户手动设置双工模式和网络速度（**"Off"[关]**）。 **默认**："On"（开） **如果"Auto Negotiation"（自动协议）为"On"（开）**，CMC 自动与最近的路由器或交换机通信并且以 1 Gb 速度操作。 **如果"Auto Negotiation"（自动协议）为"Off"（关），**则必须手动设置"Duplex Mode"（双工模式）和"Network Speed"（网络速度）。
"Network Speed"（网络速度）	将网络速度设置为 100 Mbps 或 10 Mbps 以匹配网络环境。 **注：** "Network Speed"（网络速度）设置必须同有效网络吞吐量的网络配置相匹配。将"Network Speed"（网络速度）设置为低于网络配置的速度会增加带宽消耗，并使网络通信变慢。**确定您的网络是否支持以上网络速度并进行相应设置。**如果您的网络配置与这些值的任何一个均不匹配， 建议使用**"Auto Negotiation"（自动协商）**或咨询您的网络设备制造商。 **注：** 要使用 1000 Mb 或 1 Gb 速度，请选择**"Auto Negotiation"（自动协议）**。
"Duplex Mode"（双工模式）	将"Duplex Mode"（双工模式）设置为"Full"（完全）或"Half"（半）以同您的网络环境相匹配。 **提示:：**如果某个设备的**"Auto Negotiation"（自动协议）**为"On"（开），而其它设备没有打开，则使用自动协议的设备可以确定其它设备的网络速度，但不能确定双工模式。这种情况下，双工模式将在自动协商期间默认为半双工设置。这种双工的不匹配会造成网络连接较慢。 **注：** 如果"Auto Negotiation"（自动协议）设置为"On"（开），则网络速度和双工模式设置不可用。
MTU	设置最大传输单元 (MTU) 的大小，即能够通过该接口传输的最大数据包。 **配置范围：** 576–1500。 **默认值：**1500。 **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 将使用 1280 的 MTU。

表 5-36. IPv4 设置

设置	说明
"Enable IPv4"（启用 IPv4）	允许 CMC 使用 IPv4 协议在网络中通信。取消选择该框不会阻止 IPv6 组网发生。默认：选中（启用）
"DHCP Enable"（启用 DHCP）	使 CMC 能够从 IPv4 动态主机配置协议 (DHCP) 服务器请求并自动获取 IP 地址。默认：选中（启用）

	如果选中该选项，CMC 将自动从网络中的 DHCP 服务器检索 IPv4 配置（IP 地址、子网掩码和网关）。CMC 将始终被分配网络中唯一的 IP 地址。 **注：** 当启用该功能时，将禁用**"Static IP Address"（静态 IP 地址）**、**"Static Subnet Mask"（静态子网掩码）**和**"Static Gateway"（静态网关）**属性字段（位于**"Network Configuration"[网络配置]** 页中该选项的正下方），并且之前为这些属性输入的任何值都将被忽略。 如果未选中该选项，则必须在**"Network Configuration"（网络配置）**页中该选项正下方的文本字段中手动键入**"Static IP Address"（静态 IP 地址）**、**"Static Subnet Mask"（静态子网掩码）**和**"Static Gateway"（静态网关）**。
"Static IP Address"（静态 IP 地址）	为 CMC 网络接口指定 IPv4 地址。
"Static Subnet Mask"（静态子网掩码）	为 CMC NIC 指定静态 IPv4 子网掩码。
"Static Gateway"（静态网关）	为 CMC 网络接口指定 IPv4 网关。 **注：** **"Static IP Address"（静态 IP 地址）**、**"Static Subnet Mask"（静态子网掩码）**和**"Static Gateway"（静态网关）**字段仅在禁用（取消选中）了**"DHCP Enable"（启用 DHCP）**（在上述字段前面的属性字段）时才激活。在这种情况下，必须手动键入 CMC 的**"Static IP Address"（静态 IP 地址）**、**"Static Subnet Mask"（静态子网掩码）**和**"Static Gateway"（静态网关）**，才能在网络中使用 CMC。 **注：** **"Static IP Address"（静态 IP 地址）**、**"Static Subnet Mask"（静态子网掩码）**和**"Static Gateway"（静态网关）**字段仅适用于机箱设备。这些字段不影响机箱解决方案中的其它网络可访问组件，例如服务器网络、本地访问、输入/输出模块和 iKVM。
"Use DHCP to obtain DNS server addresses"（使用 DHCP 获取 DNS 服务器地址）	从 DHCP 服务器获得主要 DNS 服务器地址和备用 DNS 服务器地址，而不是静态设置。 **默认：**默认已选中（启用） **注：** 如果启用**"Use DHCP (For CMC Network Interface IP Address)"（使用 DHCP [获取 CMC 网络接口 IP 地址]）**，则启用**"Use DHCP to obtain DNS server addresses"（使用 DHCP 获取 DNS 服务器地址）**属性。 **如果选中该选项**，CMC 将自动从网络中 DHCP 服务器上检索其 DNS IP 地址。 **注：** 当启用该属性时，"Static Preferred DNS Server"（静态首选 DNS 服务器）和"Static Alternate DNS Server"（静态备用 DNS 服务器）属性字段（位于"Network Configuration"[网络配置] 页中该选项的下方）将不被激活，并且之前在这些属性中输入的值都将被忽略。 如果该选项**未**选中，则 CMC 将从静态首选 DNS 服务器和静态备用 DNS 服务器检索 DNS IP 地址。这些服务器的地址在**"Network Configuration"（网络配置）**页中该选项下方的文本字段中指定。
"Static Preferred DNS Server"（静态首选 DNS 服务器）	指定首选 DNS 服务器的静态 IP 地址。静态首选 DNS 服务器仅当禁用**"Use DHCP to Obtain DNS Server Addresses"（使用 DHCP 获取 DNS 服务器地址）**时才可实现。
"Static Alternate DNS Server"（静态备用 DNS 服务器）	指定备用 DNS 服务器的静态 IP 地址。静态首选 DNS 服务器仅当禁用**"Use DHCP to Obtain DNS Server Addresses"（使用 DHCP 获取 DNS 服务器地址）**时才可实现。如果您没有备用 DNS 服务器，键入 IP 地址 0.0.0.0。

表 5-37. IPv6 设置

设置	说明
"Enable IPv6"（启用 IPv6）	允许 CMC 使用 IPv6 协议在网络中通信。取消选中该框不会阻止 IPv4 组网发生。默认：选中（启用）
"AutoConfiguration Enable"（启用自动配置）	允许 CMC 使用 IPv6 协议从配置用于提供 IPv6 相关地址和网关设置的 IPv6 路由器获取此信息。然后，CMC 将具有网络中唯一的 IPv6 地址。**默认：**选中（启用） **注：** 当启用该功能时，将禁用**"Static IPv6 Address"（静态 IPv6 地址）**、**"Static Prefix Length"（静态前缀长度）**和**"Static Gateway"（静态网关）**属性字段（位于**"Network Configuration"[网络配置]** 页中该选项的正下方），并且之前为这些属性输入的任何值都将被忽略。 如果未选中该选项，则必须在**"Network Configuration"（网络配置）**页中该选项正下方的文本字段中手动键入"Static IPv6 Address"（静态 IPv6 地址）、"Static Prefix Length"（静态前缀长度）和"Static Gateway"（静态网关）。
"Static IPv6 Address"（静态 IPv6 地址）	未启用自动配置时，为 CMC 网络接口指定 IPv6 地址。
"Static Prefix Length"（静态前缀长度）	未启用自动配置时，为 CMC 网络接口指定 IPv6 前缀长度。
"Static Gateway"（静态网关）	未启用自动配置时，为 CMC 网络接口指定静态 IPv6 网关。

	注： **"Static IPv6 Addres"（静态 IPv6 地址）**、**"Static Prefix Length"（静态前缀长度）**和**"Static Gateway"（静态网关）**字段仅在禁用（取消选中）了**"AutoConfiguration Enable"（启用自动配置）**（在上述字段前面的属性字段）时才激活。在这种情况下，必须手动键入 CMC 的**"Static IPv6 Address"（静态 IPv6 地址）**、**"Static Prefix Length"（静态前缀长度）**和**"Static Gateway"（静态网关）**，才能在 IPv6 网络中使用 CMC。 **注：** **"Static IPv6 Address"（静态 IPv6 地址）**、**"Static Prefix Length"（静态前缀长度）**和**"Static Gateway"（静态网关）**字段仅适用于机箱设备。这些字段不影响机箱解决方案中的其它网络可访问组件，例如服务器网络、本地访问、输入/输出模块和 iKVM。
"Static Preferred DNS Server"（静态首选 DNS 服务器）	指定首选 DNS 服务器的静态 IPv6 地址。仅当禁用或取消选中了**"Use DHCP to Obtain DNS Server Addresses"（使用 DHCP 获取 DNS 服务器地址）**时，才考虑"Static Preferred DNS Server"（静态首选 DNS 服务器）条目。在 IPv4 和 IPv6 配置区域中都有此服务器的条目。
"Static Alternate DNS Server"（静态备用 DNS 服务器）	指定备用 DNS 服务器的静态 IPv6 地址。如果您没有备用 DNS 服务器，则键入 IPv6 地址 "::"。仅当禁用或取消选中了**"Use DHCP to Obtain DNS Server Addresses"（使用 DHCP 获取 DNS 服务器地址）**时，才考虑"Static Alternate DNS Server"（静态备用 DNS 服务器）条目。在 IPv4 和 IPv6 配置区域中都有此服务器的条目。

配置 CMC 网络安全设置

注： 要执行以下步骤，必须具备**机箱配置管理员**权限。

1. 登录到 Web 界面。
2. 单击**"Network"（网络）**选项卡。

   随即显示**"Network Configuration"（网络配置）**页。
3. 单击**"Advanced Settings"（高级设置）**按钮。

   随即显示**"Network Security"（网络安全性）**页。
4. 配置 CMC 网络安全设置。

   表 5-38 说明**"Network Security"（网络安全性）**页中的**设置**。

   注： IP 范围和 IP 阻塞设置仅适用于 IPv4。

表 5-38. 网络安全性页设置

设置	说明
"IP Range Enabled"（IP 范围已启用）	启用 IP 范围检查功能，定义了可以访问 CMC 的特定范围 IP 地址。
"IP Range Address"（IP 范围地址）	为范围检查确定基础 IP 地址。
"IP Range Mask"（IP 范围掩码）	定义可以访问 CMC 的特定 IP 地址范围，这是称为 IP 范围检查的过程。 IP 范围检查允许只从 IP 地址在用户指定范围内的客户端或 Management Station 访问 CMC。所有其它登录都将被拒绝。 例如： IP 范围掩码：255.255.255.0 (11111111.11111111.11111111.00000000) IP 地址范围：192.168.0.255 (11000000.10101000.00000000.11111111) 结果 IP 地址范围是 192.168.0 中包含的任意地址，从 192.168.0.0 到 192.168.0.255 之间的任意地址。
"IP Blocking Enabled"（IP 阻塞已启用）	启用 IP 地址阻塞功能，限制在预先选定的时间段内来自特定 IP 地址的失败登录尝试数。
• **"IP Blocking Fail Count"（IP 阻塞失败计数）**	设置拒绝某个 IP 地址的登录尝试前允许登录失败的次数。
• **"IP Blocking Fail Window"（IP 阻塞失败时间范围）**	决定一个时间范围（以秒为单位），在该范围内必须发生 IP 阻塞故障计数的故障才能触发 IP 阻塞惩罚时间。
• **"IP Blocking Penalty Time"（IP 阻塞惩罚时间）**	一个时间范围（以秒为单位），在该范围内拒绝失败次数过多的某个 IP 地址的登录尝试。

	注： "IP Blocking Fail Count"（IP 阻塞失败计数）、"IP Blocking Fail Window"（IP 阻塞失败窗口）和"IP Blocking Penalty Time"（IP 阻塞惩罚时间）字段只有在"IP Blocking Enabled"（IP 阻塞启用）复选框（这些字段前面的属性字段）选中（启用）时才有效。在该情况下，必须手动键入"IP Blocking Fail Count"（IP 阻塞失败计数）、"IP Blocking Fail Window"（IP 阻塞失败窗口）和"IP Blocking Penalty Time"（IP 阻塞惩罚时间）属性。

5. 单击**"Apply"（应用）**保存设置。

要刷新**"Network Security"（网络安全性）**页中的内容，请单击**"Refresh"（刷新）**。

要打印**"Network Security"（网络安全性）**页中的内容，请单击**"Print"（打印）**。

配置 VLAN

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通信流。启用 VLAN 功能时，将给每个网络信息包分配 VLAN 标签。

1. 登录到 Web 界面。
2. 单击**"Network"（网络）**选项卡→**VLAN** 子选项卡。

   将显示**"VLAN Tag Settings"（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。

3. 配置 CMC/iDRAC VLAN 设置。

   表 5-39 说明**"Network Security"（网络安全性）**页中的**设置**。

表 5-39. VLAN 标签设置

设置	说明
插槽	显示机箱中服务器占用的插槽。插槽号是顺序 ID，从 1 到 16（用于机箱中的 16 个可用插槽），它有助于识别机箱中服务器的位置。
Name（名称）	显示每个插槽中的服务器名称。
启用	如果选择了该复选框，则启用 VLAN。默认情况下，VLAN 处于禁用状态。
优先级	指示帧优先级，可用于将不同类型的通信（语音、视频和数据）区分优先级。有效优先级是 0 至 7；其中 0（默认值）最小，7 最大。
ID	显示 VLAN ID（标识）。有效的 VLAN ID 是：1 至 4000 和 4021 至 4094。默认 VLAN ID 是 1。

4. 单击**"Apply"（应用）**保存设置。

您还可以从**"Chassis Overview"（机箱概览）**→**"Servers"（服务器）**→**"Setup"（设置）**选项卡 → **VLAN** 子选项卡访问此页。

添加和配置 CMC 用户

要用 CMC 管理系统并维护系统安全性，请创建具有特定管理权限（或*基于角色的权限*）的唯一用户。要增强安全性，还可以配置警报以便在发生特定系统事件时通过电子邮件通知特定用户。

用户类型

有两种用户类型：CMC 用户和 iDRAC 用户。CMC 用户也称为"机箱用户"。因为 iDRAC 位于服务器中，所以 iDRAC 用户也称为"服务器用户"。

CMC 用户可以是本地用户或 Directory 服务用户。iDRAC 用户也可以是本地用户或 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，因为服务器用户由 CMC 用户自行创建。换句话说，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 5-40. 用户类型

权限	说明
CMC 登录用户	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。 用户可能具备其它权限而不具备 CMC 登录用户登录权限。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分配的其它权限。

机箱配置管理员	用户可添加或更改的数据有： • 识别机箱的数据，例如机箱名称和机箱位置。 • 分配给机箱的特定数据，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相关的属性而不是服务器本身的属性。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。 当服务器移到不同的插槽中时，它会在新机箱中继承分配给此插槽的名称和优先级。以前的插槽名称和优先级保持和以前的机箱一致。
用户配置管理员	用户可以： • 添加新用户 • 删除现有用户 • 更改用户密码 • 更改用户权限 • 启用或禁用用户的登录权限，但保留用户的名称和在数据库中的其它权限。
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）	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： • 控制机箱电源操作，包括打开电源、关闭电源以及开机后再关闭电源
服务器管理员	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权利。 当拥有**服务器管理员**权限的用户发出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服务器上的权限。换言之，**服务器管理员**权限拥有服务器上的任何管理员权限。 如果没有**服务器管理员**权限，在满足以下条件时，机箱上创建的用户只能在某个服务器上执行命令： • 此服务器上存在相同的用户名 • 此服务器上相同的用户名必须有完全相同的密码 • 此用户必须具备执行命令的权限 当不具备**服务器管理员**权限的 CMC 用户发出要在服务器上执行的操作时，CMC 将发送一条命令给有此用户的用户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，或者如果密码不匹配，则拒绝此用户执行操作。
	如果目标服务器上有此用户且密码匹配，则服务器对在此服务器上具备权限的用户做出响应。根据服务器对权限的响应，CMC 固件决定此用户是否有权执行操作。 下面列出了**服务器管理员**在服务器上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，方适用这些权利。
服务器管理员（续）	服务器配置管理员： • 设置 IP 地址 • 设置网关 • 设置子网掩码 • 设置第一个引导设备 配置用户： • 设置 iDRAC 根密码 • iDRAC 重设 服务器控制管理员： • 打开电源 • 电源关闭 • 打开电源再关闭电源 • 正常关机 • 服务器重新引导
检测警报用户	用户可发送检测警报消息。
调试命令管理员	用户可执行系统诊断命令。
结构 A 管理员	用户可设置和配置位于 I/O 插槽 A1 或 A2 的结构 A IOM。
结构 B 管理员	用户可设置和配置位于 I/O 插槽 B1 或 B2 的结构 B IOM。
结构 C 管理员	用户可设置和配置位于 I/O 插槽 C1 或 C2 的结构 C IOM。
高级用户	用户拥有对 CMC 的根目录访问权以及**用户配置管理员**和**登录到 CMC 用户**的权限。只有具有**超级用户**权限的用户可授予新的或现有用户**纠错命令管理员**和**超级用户**权限。

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"Administrator"（管理员）、"Power User"（高级用户）或"Guest User"（客用户），然后从预定义集添加或删除权限，则 CMC 组会自动更改为"Custom"（自定义）。

。

表 5-41. CMC 组权限

用户组	权限分配
管理员	• 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 • 检测警报用户 • 调试命令管理员 • 结构 A 管理员 • 结构 B 管理员 • 结构 C 管理员
高级用户	• 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 • 检测警报用户 • 结构 A 管理员 • 结构 B 管理员 • 结构 C 管理员
客用户	登录
自定义	选择以下权限的任意组合： • 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） • 高级用户 • 服务器管理员 • 检测警报用户 • 调试命令管理员 • 结构 A 管理员 • 结构 B 管理员 • 结构 C 管理员
无	无分配的权限。

表 5-42. CMC 管理员、高级用户和客用户的权限比较

权限集	管理员权限	高级用户许可	客用户许可
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）	✔	✔	✖
高级用户	✔	✖	✖
服务器管理员	✔	✔	✖
检测警报用户	✔	✔	✖
调试命令管理员	✔	✖	✖
结构 A 管理员	✔	✔	✖
结构 B 管理员	✔	✔	✖

结构 C 管理员	✔	✔	✖

添加并管理用户

从 Web 界面的**"Users"（用户）**和**"User Configuration"（用户配置）**页中，可以查看关于 CMC 用户、添加新用户和更改现有用户设置的信息。

最多可以配置 16 个本地用户。如果需要更多的用户，并且您的公司使用 Microsoft Active Directory 或通用轻型目录访问协议 (LDAP) 服务，您可对其进行配置以访问 CMC。除了 16 个本地用户外，Active Directory 配置允许在 Active Directory 软件中添加并控制现有用户的 CMC 用户权限。有关详情，请参阅"使用 CMC 目录服务"。有关 LDAP 的详情，请参阅"使用 CMC 和轻型目录访问协议服务"部分。

用户可以通过 Web 界面、远程登录串行、SSH 和 iKVM 会话登录。用户之间最多可区分 22 个激活的会话（Web 界面、远程登录串行、SSH 和 iKVM，以任意组合）。

注： 为增加安全性，强烈建议您更改 root（用户 1）帐户的默认密码。root 帐户是与 CMC 一并提供的默认管理帐户。要更改 root 帐户的默认密码，请单击 **"User ID" 1（用户 ID 1）**，打开 **"User Configuration"（用户配置）**页面。通过页面右上角的"Help"（帮助）链接可以访问该页的帮助。

要添加并配置 CMC 用户：

注： 您必须具有**"Configure Users"（配置用户）**权限才能执行以下步骤。

1. 登录到 Web 界面。
2. 单击**"User Authentication"（用户验证）**选项卡。随即出现**"Local Users"（本地用户）**页，其中列出每个用户的用户 ID、用户名、CMC 权限和登录状态，包括 root 用户的这些信息。可以配置的用户 ID 不显示用户信息。
3. 单击可用的用户 ID 编号。显示 **"User Configuration"（用户配置）**页面。

   要刷新 **"Users"（用户）**页面的内容，请单击 **"Refresh"（刷新）**。要打印 **"Users"（用户）**页面的内容，请单击 **"Print"（打印）**。
4. 为用户选择常规设置。

表 5-43. 配置新的或现有 CMC 用户名和密码的常规用户设置

属性	说明
"User ID"（用户 ID）	"(Read only)"（[只读]）使用 16 个用于 CLI 脚本目的的预置、顺序编号当中的一个来标识一位用户。当通过 CLI 工具 (RACADM) 配置该用户时使用该用户 ID 标识用户。不能编辑用户 ID。 如果您编辑用户 root 的信息，则此字段为静态字段。不能编辑 root 用户的用户名。
"Enable User"（启用用户）	启用或禁用用户访问 CMC。
"User Name"（用户名）	设置或显示与用户相关的唯一 CMC 用户名。用户名最多包含 16 个字符。CMC 用户名不能包括正斜杠 (/) 或句点 (.) 字符。 **注：** 如果更改了用户名，在下次登录之前，新用户名不会出现在用户界面上。在应用新用户名之后登录的任意用户将能够立即看到该更改。
"Change Password"（更改密码）	允许更改现有用户的密码。在**"New Password"（新密码）**字段输入新密码。 配置新用户时，**"Change Password"（更改密码）**复选框不可选。仅当更改现有用户设置时才可选择该复选框。
"Password"（密码）	为现有用户设置新密码。要更改密码，还必须选择**"Change Password"（更改密码）**复选框。密码可包含最多 20 个字符，键入时显示为点。
"Confirm Password"（确认密码）	验证在**"New Password"（新密码）**字段中输入的密码。 **注：** **"New Password"（新密码）**和**"Confirm New Password"（确认新密码）**字段仅在两种情况下可以编辑：(1) 配置新用户；或 (2) 编辑现有用户设置，并且选定**"Change Password"（更改密码）**复选框。

5. 分配用户到 CMC 用户组。表 5-40 说明 CMC 用户权限。

   从"CMC Group"（CMC 组）下拉菜单选择用户权限设置时，已启用的权限将根据该组的预定义设置显示（在列表中作为复选框显示）。

   可通过选中或取消选中复选框来定制用户的权限设置。选择"CMC Group"（CMC 组）或"Custom"（自定义）用户权限后，单击 **"Apply Changes"（应用更改）**保存设置。
6. 单击**"Apply Changes"（应用更改）**。

要刷新**"User Configuration"（用户配置）**页中的内容，请单击**"Refresh"（刷新）**。

要打印**"User Configuration"（用户配置）**页中的内容，请单击**"Print"（打印）**。

配置和管理 Microsoft Active Directory 认证

注： 要为 CMC 配置 Active Directory 设置，必须具备**机箱配置管理员**权限。

注： 有关 Active Directory 配置和如何配置标准架构和扩展架构的 Active Directory 的详情，请参阅 "使用 CMC 目录服务"。

使用 MicrosoftActive Directory 服务配置软件以提供对 CMC 的访问。Active Directory 服务允许您添加和控制现有用户的 CMC 用户权限。

要访问**"Active Directory Main Menu"（Active Directory 主菜单）**页：

1. 登录到 Web 界面。
2. 单击**"User Authentication"（用户验证）**选项卡，然后单击**"Directory Services"（目录服务）**子选项卡。选择用于 Microsoft Active Directory 标准架构或扩展架构的单选按钮。出现 Active Directory 表。

常见设置

此选项允许您为 CMC 配置和查看常见的 Active Directory 设置。

表 5-44. 常见设置

字段	说明
"Enable Active Directory"（启用 Active Directory）	启动 Active Directory 登录到 CMC。必须为 Active Directory 服务器安装由相同证书机构签发的 SSL 证书并上传到 CMC。
启用智能卡登录	启用基于 Dell 提供、自安装的浏览器插件的 Kerberos 验证的 Active Directory 互操作和智能卡的使用。若要启用智能卡，则选择复选框。若要禁用智能卡，则取消选择复选框。如果启用智能卡，则必须配置 Microsoft Windows 客户端工作站正确使用智能卡读卡器功能。这涉及到为使用的智能卡读卡器安装正确的驱动程序，以及为实际使用的智能卡安装正确的驱动程序。智能卡的驱动程序由供应商提供。智能卡必须用相应 Active Directory 服务器提供的智能卡登记服务采用必要凭据正确编程。 **注：** 智能卡登录和单一登录选项相互排斥。一次只能配置一项。
启用单一登录	启用 CMC 采用 **Active Directory**。若要启用**单一登录**，则选择复选框。若要禁用**单一登录**，则取消选择复选框。如果启用**单一登录**，则也必须设置 **Active Directory** 属性和选择要使用的架构。 **注：** 智能卡登录和单一登录选项相互排斥。一次只能配置一项。
启用 SSL 证书验证	为 CMC 的 Active Directory SSL 连接启用 SSL 证书验证。若要禁用 SSL 证书验证，则取消选择复选框。 **警告：**禁用此功能可能会暴露验证而受到中间人攻击。 浏览器操作要求 CMC 通过含用于 CMC 的完全合格域地址的 HTTP URL 访问，即 **http://cmc-6g2wxf1.dom.net**。普通 IP 地址用于 CMC 不会产生正确的单一登录操作。若要支持完全合格的域地址，则必须在 Active Directory 服务器的域名服务中登记 CMC。 如果单一登录浏览器验证不成功，则会自动采用普通本地或 Active Directory 用户名/密码浏览器验证方法。同样，成功单一登录后的注销操作也可采用用户名/密码方法。单一登录旨在提供方便而并不强制要求。 **注：** 基于智能卡的浏览器验证仅支持 Microsoft Windows 客户端和 Internet Explorer 浏览器。 Dell 提供、自安装的浏览器插件（ActiveX 控件）依赖于预安装 Microsoft Visual C++ 2005 Redistributable Package (x86) 运行时组件的 Microsoft Windows 客户端操作系统。此组件可通过以下链接下载：**http://www.microsoft.com/downloads/details.aspx?FamilyID=32BC1BEE-A3F9-4C13-9C99-220B62A191EE&displaylang=en**.Windows 客户端需要"提升"权限才能成功安装 ActiveX 控件。同样，浏览器配置要求接受"未签名"ActiveX 控件的能力。
	启用智能卡可为浏览器验证强制执行仅使用智能卡的策略。普通本地或 Active Directory 用户名/密码验证等所有其他浏览器验证方法均会被禁用。如果采用仅使用智能卡的强制策略，则必须在禁用 CMC 的所有其他访问方法前完全验证智能卡是否正确工作。否则可能会意外锁定所有到 CMC 的访问。
"Root Domain Name"（根域名）	指定 Active Directory 使用的域名。根域名就是完全合格的森林的根域名。 **注：** Root 域名必须是使用 x.y 命名规范的有效域名，其中 x 是 1–256 个字符的 ASCII 字符串，字符之间不带空格，且 y 是有效的域类型，如 com、edu、gov、int、mil、net 或 org。
"AD Timeout"（AD 超时）	设置空闲的 Active Directory 会话在等待多少秒后自动关闭。 有效值：15-300 秒。 默认：90 秒

指定要搜索的 AD 服务器（可选）	启用（勾选时）对域控制器和全局编录的直接调用。如果启用此选项，还必须在如下设置中指定域控制器和全局编录的位置。 **注：** Active Directory CA 认证上的名称不会匹配指定的 Active Directory 服务器或全局编录服务器。
"Domain Controller"（域控制器）	指定安装了 Active Directory 服务的服务器。此选项只在启用了 **"Specify AD Server to search (Optional)"（指定要搜索的 AD 服务器 [可选]）** 时有效。
"Global Catalog"（全局编录）	指定全局编录在 Active Directory 域控制器上的位置。全局编录提供了搜索 Active Directory 森林的资源。 此选项只在启用了 **"Specify AD Server to search (Optional)"（指定要搜索的 AD 服务器 [可选]）** 时有效。

"Standard Schema Settings"（标准架构设置）

此部分在选择 Microsoft Active Directory（标准架构）时显示，提供所有已配置的角色组以及相关名称、域和权限。

要更改角色组设置，单击角色组列表中相应的角色组按钮。

注： 如果在应用新设置之前单击角色组链接，则会丢失这些设置。要避免丢失任何新设置，可以在单击角色组按钮前单击**"Apply"（应用）**。

随即显示"Configure Role Group"（配置角色组）页：

- "Group Name"（组名称） – 在 Active Directory 中标识 CMC 卡相关角色组的名称。
- "Group Domain"（组域） – 组所在的域。
- "Group Privilege"（组特权） – 组的特权级别。

单击**"Apply"（应用）**保存设置。

单击**"Go Back To Configuration Page"（退回到配置页）**可返回到**"Directory Services"（目录服务）**页。

要刷新**"Directory Services"（目录服务）**页中的内容，请单击**"Refresh"（刷新）**。

要打印**"Directory Services"（目录服务）**页中的内容，请单击**"Print"（打印）**。

"Extended Schema Settings"（扩展架构设置）

此部分在选择 Microsoft Active Directory（扩展架构）时显示，提供以下属性：

- CMC 设备名称 - 显示为 CMC 创建的 RAC 设备对象的名称。CMC 设备名称对 Active Directory 中的 CMC 卡进行唯一识别。CMC 设备名称必须与在域控制器中创建的新的 RAC 设备对象的常用名称相同。CMC 名称必须是 1-256 个字符的 ASCII 字符串，字符之间没有空格。有关 RAC 设备对象的详情，请参阅 CMC 用户指南。
- CMC 域名 - 显示 Active Directory RAC 设备对象所在域的 DNS 名称（字符串）。MC 域名必须是 *x.y* 格式的有效域名，其中 *x* 是 1-256 个字符的 ASCII 字符串，字符之间没有空格，而 *y* 是有效域类型，例如 com、edu、gov、int、mil、net、org。

管理 Active Directory 证书

此部分显示最近上传到 CMC 的 Active Directory 证书的属性。如果已上传证书，则用此信息验证证书有效且没有过期。

注： 默认情况下，CMC 没有认证机构颁发的 Active Directory 服务器认证。您必须上载当前的、认证机构签字的服务器认证。

会显示证书的以下属性：

- 序列号 - 证书的序列号。
- 接收者信息 - 证书的接收者（经认证人员的姓名或公司的名称）。
- 颁发者信息 - 证书的颁发者（发证机构的名称）。
- 有效期自 - 证书的起始日期。
- 有效期至 - 证书的失效日期。

用以下控件上传和下载此证书：

- 上传 - 发起证书的上传过程。该认证可从 Active Directory 获取，授予对 CMC 的访问权限。
- 下载 - 发起下载过程。会提示您确定保存文件的位置。选择该选项后，单击**"Next"（下一步）**，系统出现"File Download"（文件下载）对话框。通过该对话框指定服务器认证在 management station 或共享网络的位置。

注： 默认情况下，CMC 没有认证机构颁发的 Active Directory 服务器认证。您必须上载当前的、认证机构签字的服务器认证。

Kerberos Keytab

您可上传相关 Active Directory 服务器上生成的 Kerberos Keytab。您可以执行 **ktpass.exe** 公用程序，以从 Active Directory 服务器生成 Kerberos Keytab。此 Keytab 在 Active Directory 服务器和 CMC 之间建立信任关系。

注： CMC 没有适用于 Active Directory 的 Kerberos Keytab。您必须上载当前生成的 Kerberos Keytab。有关详细信息，请参阅"配置单一登录"。

允许以下操作：

- 浏览 - 打开**"浏览"**对话框，然后从中选择想要上传的服务器证书。
- 上传 - 用指定的文件路径发起证书的上传流程。

配置和管理通用轻型目录访问协议服务

您可使用通用轻型目录访问协议 (LDAP) 服务配置软件提供到 CMC 的访问。LDAP 允许您添加和控制现有用户的 CMC 用户权限。

注： 要为 CMC 配置 LDAP 设置，必须具备**机箱配置管理员**权限。

若要查看和配置 LDAP：

1. 登录到 Web 界面。
2. 单击**"User Authentication"（用户验证）**选项卡，然后单击**"Directory Services"（目录服务）**子选项卡。随即出现**"Directory Services"（目录服务）**页。
3. 单击通用 LDAP 的单选按钮。
4. 配置显示的选项并单击**"Apply"（应用）**。

可用配置选项如下：

表 5-45. 常见设置

设置	说明
启用通用 LDAP	在 CMC 上启用通用 LDAP 服务。有关 LDAP 详情请，参阅《CMC 用户指南》。
用可分辨名称搜索组成员资格	指定允许其成员访问设备的 LDAP 组的可分辨名称 (DN)。
启用 SSL 证书验证	如果选择，CMC 使用 CA 证书验证 SSL 握手期间的 LDAP 服务器证书
"Bind DN"（绑定 DN）	在搜索登录用户的 DN 时，指定绑定到服务器的用户的可分辨名称。如果未提供，则使用匿名绑定。
"Password"（密码）	与绑定 DN 一起使用的绑定密码。 绑定密码属于敏感数据，应予以正确保护。
用于搜索的基础 DN	目录分支的域名，所有搜索都从此处开始。
用户登录的属性	指定要搜索的属性。如果未配置，默认使用 uid。推荐在选择的基础 DN 内唯一，否则必须配置搜索筛选器以保证登录用户的唯一性。如果用户 DN 不能通过搜索属性和搜索筛选器组合而唯一识别，则登录失败并报错。
组成员资格属性	指定用于检查组成员资格的 LDAP 属性。必须是一个组类属性。如果未指定，则使用成员和唯一成员属性。
搜索筛选器	指定有效的 LDAP 搜索筛选器。如果用户属性不能在所选基础 DN 中唯一标识登录用户，将使用此功能。如果未指定，默认为 objectClass=*，显示搜索树中的所有对象。此属性的最大长度为 1024 个字符。
网络超时（秒）	设置空闲的 LDAP 会话在等待多少秒后自动关闭。
搜索超时（秒）	设置搜索在等待多少秒后自动关闭。

选择 LDAP 服务器

用通用 LDAP 配置服务器有两种方式。静态服务器允许管理员在字段内加入 FQDN 或 IP 地址。另外，也可通过在 DNS 内查询其 SRV 记录而读取 LDAP 服务器列表。以下是 LDAP 服务器部分中的属性：

- "Use Static LDAP Servers"（使用静态 LDAP 服务器） - 选择此选项可使 LDAP 服务使用提供端口号的指定服务器（详情请参阅下面）。

  注： 必须选择静态或 DNS。

- "LDAP Server Address"（LDAP 服务器地址） - 指定 LDAP 服务器的 FQDN 或 IP 地址。要指定位于相同域的多个冗余 LDAP 服务器，请提供所有服务器的列表（用逗号隔

开）。CMC 会尝试依次连接到每个服务器，直到建立连接为止。

- "LDAP Server Port"（LDAP 服务器端口） - LDAP 在 SSL 上的端口，如未配置，则默认为 636。CMC 版本 3.0 不支持非 SSL 端口，因没有 SSL 就不能传输密码。
- "Use DNS to find LDAP Servers"（用 DNS 查找 LDAP 服务器） - 选择此选项可使 LDAP 通过 DNS 使用搜索域和服务名称。必须选择静态或 DNS。

会为 SRV 记录进行以下 DNS 查询：

```
_[Service Name]._tcp.[搜索域]
```

其中 <*搜索域*> 是查询中使用的根域而 <*服务名称*> 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。

管理 LDAP 组设置

"组设置"部分表中列出了角色组，为已配置的所有角色组显示相关名称、域和权限。

- 若要配置新角色组，则单击没有列出名称、域和权限的角色组名称。
- 若要为现有角色组更改设置，则单击角色组名称。

在单击角色组名称时，显示**"Configure Role Group"（配置角色组）**页。通过页面右上角的**"Help"（帮助）**链接可以访问该页的帮助。

管理 LDAP 安全证书

此部分显示最近上传到 CMC 的 LDAP 证书的属性。如果已上传证书，则用此信息验证证书有效且没有过期。

注： 默认情况下，CMC 没有认证机构颁发的 Active Directory 服务器认证。您必须上载当前的、认证机构签字的服务器认证。

会显示证书的以下属性：

- 序列号 - 证书的序列号。
- 接收者信息 - 证书的接收者（经认证人员的姓名或公司的名称）。
- 颁发者信息 - 证书的颁发者（发证机构的名称）。
- 有效期自 - 证书的起始日期。
- 有效期至 - 证书的失效日期。

用以下控件上传和下载此证书：

- 上传 - 发起证书的上传过程。该证书可从 LDAP 获取，授予对 CMC 的访问权限。
- 下载 - 发起下载过程。会提示您确定保存文件的位置。选择该选项后，单击**"Next"（下一步）**，系统出现"File Download"（文件下载）对话框。通过该对话框指定服务器认证在 management station 或共享网络的位置。

使用 SSL 和数字认证确保 CMC 通信

本小节提供关于 CMC中包括的以下数据安全性功能的信息：

- 安全套接字层 (SSL)
- 证书签名请求 (CSR)
- 访问 SSL 主菜单
- 生成新 CSR
- 上载服务器证书
- 查看服务器证书

安全套接字层 (SSL)

CMC 包括 Web 服务器，通过配置 Web 服务器可使用行业标准的 SSL 安全协议在因特网上传输加密数据。基于公共密钥和私人密钥加密技术构建的 SSL 是广泛接受的技术，用于在客户端和服务器之间提供验证和加密的通信，以防止网络上的窃听现象。

SSL 允许启用 SSL 的系统执行以下任务：

- 向启用 SSL 的客户端验证自身
- 允许客户端向服务器验证自身
- 允许两个系统建立加密连接

此加密过程提供高级别数据保护。CMC 使用 128 位 SSL 加密标准，北美互联网浏览器常用的最安全加密方式。

CMC Web 服务器包括 Dell 自签字的 SSL 数字认证 (Server ID)。要确保互联网上的高安全性，请向 CMC 提交请求生成新的认证签名请求 (CSR) 来更换 Web 服务器 SSL 认证。

证书签名请求 (CSR)

CSR 是向认证机构（Web 界面中称为 CA）请求安全服务器认证的数字请求。安全服务器认证可以确保远程系统的身份，并确保与远程系统交换的信息不会被他人查看或更改。要确保 CMC 的安全性，强烈建议生成 CSR、将 CSR 提交给认证机构，并上载认证机构返回的认证。

认证机构是 IT 行业认可的企业实体，可满足高标准的可靠性审查、识别和其它重要安全标准。例如，Thwate 和 VeriSign 均为 CA。认证机构接收 CSR 之后将查看并验证 CSR 包含的信息。如果申请人符合认证机构的安全性标准，认证机构会向申请人签发认证，该认证唯一标识网络或因特网上交易的申请人。

认证机构批准 CSR 并发送认证后，必须将认证上载到 CMC 固件。存储在 CMC 固件中的 CSR 信息必须与证书中包含的信息匹配。

访问 SSL 主菜单

注： 要为 CMC 配置 SSL 设置，必须具备**机箱配置管理员**权限。

注： 您上载的任何服务器认证必须为当期（未过期）并且由认证机构签字。

1. 登录到 Web 界面。
2. 单击**"Network"（网络）**选项卡，然后单击 **SSL** 子选项卡。随即出现**"SSL Main Menu"（SSL 主菜单）**页。

使用**"SSL Main Menu"（SSL 主菜单）**页选项生成要发送到认证机构的 CSR。CSR 信息存储在 CMC 固件中。

生成新的证书签名请求

要确保安全性，强烈建议您获取安全的服务器认证并将其上载到 CMC。安全服务器认证可以确保远程系统的身份且他人无法查看或更改与远程系统交换的信息。没有安全的服务器认证，CMC 易受未经授权的用户访问。

表 5-46. SSL 主菜单选项

字段	说明
"Generate a New Certificate Signing Request (CSR)"（生成新的证书签名请求 [CSR]）	选择该选项并单击**"Next"（下一步）**打开"Generate Certificate Signing Request (CSR)"（生成认证签名请求 [CSR]）页，可以在该页上为安全 Web 认证生成一个可以提交到认证机构的 CSR 请求。 **注：** 每个新的 CSR 都会改写 CMC 上任何原有的 CSR。对于接受您的 CSR 的认证机构，CMC 中的 CSR 必须同认证机构中返回的认证相匹配。
"Upload Server Certificate Based on Generated CSR"（根据生成的 CSR 上载服务器证书）	选择该选项并单击**"Next"（下一步）**可显示**"Certificate Upload"（上载证书）**页，您可在该页中上载您的公司所拥有的并用来控制 CMC 访问的现有证书。 **注：** 只有 X509，Base 64 编码认证才能被 iDRAC 接受。不接受 DER 编码证书。上载新的认证，取代您通过 CMC 接收的默认认证。
"Upload Webserver key and Certificate"（上载 Webserver 密钥和证书）	选择该选项并单击**"Next"（下一步）**可打开**"Webserver Key and Certificate Upload"（上载 Webserver 密钥和证书）**页，您可在该页中上载您的公司所拥有的并用来控制 CMC 访问的现有 Web 服务器密钥和服务器证书。 **注：** CMC 仅接受 Base 64 编码的 X.509 证书。不接受二进制 DER 编码证书。上载新的认证，取代您通过 CMC 接收的默认认证。
"View Server Certificate"（查看服务器证书）	选择选项并单击**"Next"（下一步）**按钮打开**"View Server Certificate"（查看服务器认证）**页，可以通过该页查看当前服务器认证。

要获取安全的服务器认证，您必须将认证签名请求 (CSR) 提交给您所选择的认证机构。CSR 是数字请求，请求一份包含组织信息和唯一识别码的、经签字的安全服务器证书。

当从**"Generate Certificate Signing Request (CSR)"（生成证书签名请求 [CSR]）**页生成 CSR 时，将提示您将副本保存在 Management Station 或共享网络上，用于生成

CSR 的唯一信息存储在 CMC 上。该信息用于以后验证您从认证机构接收的服务器认证。收到认证机构的服务器证书后，必须将其上载到 CMC。

注： 为了使 CMC 能够接受由认证机构返回的服务器认证，新认证中包含的验证信息必须与生成 CSR 时存储在 CMC 上的信息匹配。

小心： 生成新的 CSR 后，它会覆盖 CMC 上任何以前的 CSR。如果挂起的 CSR 在认证机构分配服务器认证之前被覆盖，则 CMC 将不会接受服务器认证，因为用于验证认证的信息已经掉失。生成 CSR 之前需特别注意以防覆盖任何未完成的 CSR。

要生成 CSR：

1. 从**"SSL Main Menu "**（**SSL 主菜单**）页上选择 **"Generate a New Certificate Signing Request (CSR)"（生成新的认证签名请求 [CSR]）**，并单击**"Next"（下一步）**。随即显示**"Generate Certificate Signing Request (CSR)"（生成认证签名请求 [CSR]）**页。

2. 为每个 CSR 属性值键入一个值。

3. 单击**"**Generate"（生成）。出现**"File Download"（文件下载）**对话框。

4. 将 **csr.txt** 文件保存到 Management Station 或共享网络。（您也可以在此时打开文件并稍后保存。）您将稍后提交该文件到认证机构。

表 5-47. 生成证书签名请求 (CSR) 页选项

字段	说明
"Common Name"（常用名）	认证的确切名（通常是 Web Server 的域名，例如 **www.xyzcompany.com**）。 **有效**：字母数字字符（A–Z、a–z、0–9）连字符、下划线和句点。 **无效**：上列有效字符之外的非字母数字字符（包括但不限于 @ # $ % & *）；主要用于非英语语言的字符，如 、、é、ü。
"Organization Name"（组织名称）	与组织相关联的名称，（例如，**"XYZ Corporation"[XYZ 公司]**）。 **有效**：字母数字字符（A–Z、a–z、0–9）；连字符、下划线、句点和空格。 **无效**：上列有效字符之外的非字母数字字符（包括但不限于，@ # $ % & *）。
"Organization Unit"（组织单位）	与组织机构相关联的名称，例如某部门（例如"Enterprise Group"[企业组]）。 **有效**：字母数字字符（A–Z、a–z、0–9）；连字符、下划线、句点和空格。 **无效**：上列有效字符之外的非字母数字字符（包括但不限于，@ # $ % & *）。
"Locality"（地点）	组织所在城市或其它地方（例如**亚特兰大**、**香港**）。 **有效**：字母数字字符（A–Z、a–z、0–9）和空格。 **无效**：上列有效字符之外的非字母数字字符（包括但不限于 @ # $ % & *）。
"State"（状态）	州、省或申请认证的实体所在的区域（例如**德克萨斯**、**新南威尔士**、**安得拉邦**）。 **注：** 不要使用缩写。 **有效**：字母数字字符（大写和小写字母；0–9）；和空格。 **无效**：上列有效字符之外的非字母数字字符（包括但不限于 @ # $ % & *）。
"Country"（国家/地区）	申请认证的组织所在的国家/地区。
"Email"（电子邮件）	您所在组织的电子邮件地址。可以键入希望与 CSR 关联的任何电子邮件地址。电子邮件地址必须有效，包含 (@) 符号（示例：**name@xyzcompany.com**）。 **注：** 此电子邮件地址是可选字段。

上载服务器证书

1. 从**"SSL Main Menu"（SSL 主菜单）**页中选择**"Upload Server Certificate Based on Generated CSR"（上载基于生成的 CSR 的服务器证书）**并单击**"Next"（下一步）**。随即显示**"Certificate Upload"（证书上载）**页。

2. 在文本字段中键入文件路径，或单击**"Browse"（浏览）**选择文件。

3. 单击**"Apply"（应用）**。如果认证无效，则会显示错误信息。

注： **"File Path"（文件路径）**值显示上载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。

要刷新**"Certificate Upload "（认证上载）**页中的内容，请单击**"Refresh"（刷新）**。

要打印**"Certificate Upload "（认证上载）**页中的内容，请单击**"Print"（打印）**。

"Upload Webserver key and Certificate"（上传 Webserver 密钥和证书）

1. 选择**"Upload Webserver key and Certificate"（上传 Webserver 密钥和证书）**选项，然后单击**"Next"（下一步）**。
2. 用浏览菜单输入 Private Key File（私人密码文件）。
3. 用浏览菜单输入证书文件。
4. 上传两个文件后单击**"Apply"（应用）**。如果 Webserver 密钥和证书不匹配，则会显示一条错误消息。

注： 只有 Base-64 编码的 X509 证书才能被 CMC 接受。不会接受使用 DER 等其他编码方式的证书。上载新的认证，取代您通过 CMC 接收的默认认证。

注： 若要上传 Webserver 密钥和证书，则必须具有机箱配置管理员权限。

注： 成功上传证书后，CMC 将重设并暂时不可用。要在重设时避免与其他用户断开连接，通知可能登入 CMC 的授权用户，并通过查看"Network"（网络）选项卡下的"Sessions"（会话）页检查活动的会话。

查看服务器证书

从**"SSL Main Menu"（SSL 主菜单）**页中选择**"View Server Certificate"（查看服务器认证）**并单击**"Next"（下一步）**。显示**"View Server Certificate"（查看服务器认证）**页。

表 5-48 说明**"Certificate"（证书）**窗口中列出的字段及相关说明。

表 5-48. 认证信息

字段	说明
串行	证书序列号
主题	按主题输入的证书属性
颁发者	按颁发者返回的证书属性
"notBefore"（颁发日期）	证书的颁发日期
"notAfter"（失效日期）	证书的期满日期

要刷新**"View Server Certificate"（查看服务器认证）** 页中的内容，请单击**"Refresh"（刷新）**。

要打印**"View Server Certificate"（查看服务器认证）**页中的内容，请单击**"Print"（打印）**。

管理会话

"Sessions"（会话）页显示所有当前连接到机箱的实例，并允许终止任意激活的会话。

注： 要终止会话，必须具备**机箱配置管理员**权限。

要管理或终止会话：

1. 通过 Web 登录到 CMC。
2. 单击**"Network"（网络）**选项卡，然后单击**"Sessions"（会话）**子选项卡。
3. 在**"Sessions"（会话）**页上，找到要终止的会话，然后单击相应按钮。

表 5-49. 会话属性

属性	说明

"Session ID"（会话 ID）	显示为每个登录实例顺序生成的 ID 号。
"Username"（用户名）	显示用户的登录名称（本地用户或 Active Directory 用户）。Active Directory 用户名的例子有 *name@domain.com*、*domain.com/name*、*domain.com\name*。
"IP Address"（IP 地址）	显示用户的 IP 地址。
"Session Type"（会话类型）	说明会话类型：Telnet、serial、SSH、Remote RACADM、SMASH CLP、WSMAN 或 GUI 会话。
"Terminate"（终止）	允许终止除自己的会话外列出的任意会话。单击此按钮终止相关会话。只有在具备**机箱配置管理员**权限时方显示此栏。

配置服务

CMC 包含 Web Server，配置使用行业标准 SSL 安全协议通过因特网接受和传输来自客户端的加密数据。Web server 包含 Dell 自签名 SSL 数字证书 (Server ID) 并负责接受和响应来自客户端的安全 HTTP 请求。该服务是用于与 CMC 通信的 Web 界面和远程 CLI 工具所必需的服务。

注： 远程 (RACADM) CLI 工具和 Web 界面使用 Web server。在 Web Server 不活动的情况下，不可操作远程 RACADM 和 Web 界面。

注： 在 Web server 重设时，等待至少一分钟以使服务再次可用。Web Server 重设通常由以下事件引起：通过 CMC Web 用户界面或 RACADM 更改网络配置或网络安全性属性；通过 Web 用户界面或 RACADM 更改 Web Server 端口配置；重设 CMC；上载了新的 SSL 服务器证书。

注： 要修改服务设置，必须具备**机箱配置管理员**权限。

要配置 CMC 服务：

1. 登录 CMC Web 界面。
2. 单击**"Network"（网络）**选项卡。
3. 单击**"Services"（服务）**子选项卡。随即出现**"Services"（服务）**页。
4. 根据需要配置以下服务：
   - CMC 串行控制台（表 5-50）
   - Web Server（表 5-51）
   - SSH（表 5-52）
   - Telnet（表 5-53）
   - 远程 RACADM（表 5-54）
   - SNMP (表 5-55)
   - 远程系统日志 (表 5-56)
5. 单击**"Apply"（应用）**，然后更新所有默认超时和最大超时限制。

表 5-50. CMC 串行控制台设置

设置	说明
已启用	在 CMC 上启用 Telnet 控制台界面。 **默认值**：取消选取（禁用）
"Redirect Enabled"（已启用重定向）	通过串行/远程登录/SSH 客户端从 CMC 启用串行/文本控制台重定向到服务器。CMC 连接到与服务器 COM2 端口在内部相连的 iDRAC。 **配置选项：**选中（启用），取消选中（禁用） **默认：**选中（启用）
"Idle Timeout"（空闲超时）	显示空闲串行会话自动断开连接前等待的秒数。对**"Timeout"（超时）**设置的更改在下次登录时生效；它不影响当前会话。 **"Timeout Range"（超时范围）**：0 或 60 至 10800 秒。要禁用"Timeout"（超时）功能，请输入 0。 **默认值**：1800 秒
"Baud Rate"（波特率）	显示 CMC 上外部串行端口的数据速度。 **配置选项：** 9600、19200、28800、38400、57600 和 115200 bps。 **默认值**：115200 bps
验证已禁用	启用 CMC 串行控制台登录验证。

	默认值：取消选取（禁用）
"Escape Key"（Esc 键）	允许指定 Escape 键组合，用于在使用 **connect 或 racadm connect** 命令时终止串行/文本控制台重定向。 **默认值：** ^\ （按住 <Ctrl> 并键入反斜杠 (\) 字符） **注：** 脱字符号 ^ 代表 <Ctrl> 键。 配置选项： • 十进制值（例如：95） • 十六进制值（例如：0x12） • 八进制值（例如：007） • ASCII 值（例如：^a） ASCII 值可以使用以下 Esc 键代码表示： • Esc 后跟字母 (a-z, A-Z) • Esc 后跟特殊字符：[ ] \ ^ _ • 最大允许长度： 4
"History Size Buffer"（历史缓冲区大小）	显示串行历史记录缓冲区的最大值，保存最后写入串行控制台的字符。 **默认：**8192 个字符
"Login Command"（登录命令）	指定用户登录 CMC 串行控制台界面时自动执行的串行命令。 **示例：** connect server-1 **默认值：** [Null]

表 5-51. Web Server 设置

设置	说明
已启用	启用 CMC Web Server 服务（通过远程 RACADM 和 Web 界面访问）。 **默认**：选中（启用）。
"Max Sessions"（最大会话数）	显示机箱允许的最大并发 Web 用户界面会话数。**最大会话数**属性的更改会在下次登录时生效；不会影响当前**激活的会话数**（包含您自己的）。远程 RACADM 不受 Web Server **最大会话数**属性的影响。 允许范围：1–4 **默认值**：4 **注：** 如果将**"Max Sessions"（最大会话）**属性的值更改到小于当前激活的会话数并注销，则在其它会话终止或过期之前，您将无法再次登录。
"Idle Timeout"（空闲超时）	显示空闲 Web 用户界面会话自动断开连接前等待的秒数。对**"Timeout"（超时）**设置的更改在下次登录时生效；它不影响当前会话。 **超时范围**：60 至 10800 秒。 **默认值**：1800 秒
"HTTP Port Number"（HTTP 端口号）	显示 CMC 用来监听服务器连接的默认端口。 **注：** 在浏览器上提供 HTTP 地址时，Web Server 会自动重定向并使用 HTTPS。 如果更改了默认 HTTP 端口号 (80)，则必须在浏览器地址字段的地址中包含端口号，如下所示： http://<*IP 地址*>:<*端口号*> 其中 *IP 地址*是机箱的 IP 地址，而*端口号*是默认值 80 以外的 HTTP 端口号。 **配置范围：** 10–65535。 **默认值**：80
"HTTPS Port Number"（HTTPS 端口号）	显示 CMC 用来监听安全服务器连接的默认端口。 如果默认 HTTPS 端口号 (443) 已更改，必须在浏览器地址字段将端口号包括在地址中，如下所示： https://<*IP 地址*>:<*端口号*>

	其中 *IP 地址*是机箱的 IP 地址，而*端口号*是默认值 443 以外的 HTTPS 端口号。 **配置范围：** 10–65535。 **默认值**：443

表 5-52. SSH 设置

设置	说明
已启用	启用 CMC 上的 SSH **默认**：选中（启用）。
"Max Sessions"（最大会话数）	机箱允许的最大并发 SSH 会话数。该属性的更改会在下次登录时生效；不会影响当前激活的会话数（包含您自己的）。 **配置范围：** 1–4。 **默认值**：4 **注：** 如果将**"Max Sessions"（最大会话）**属性的值更改到小于当前**"Active Sessions"（活动会话）**数并注销，则在其它会话终止或过期之前，您将无法再次登录。
"Idle Timeout"（空闲超时）	显示空闲 SSH 会话自动断开连接前等待的秒数。对**"Timeout"（超时）**设置的更改在下次登录时生效；它不影响当前会话。 **"Timeout Range"（超时范围）**：0 或 60 – 10800 秒。要禁用"Timeout"（超时）功能，请输入 0。 **默认值**：1800 秒
"Port Number"（端口号）	CMC 用来侦听服务器连接的端口。 **配置范围：** 10–65535。 **默认值**：22

表 5-53. Telnet 设置

设置	说明
已启用	在 CMC 上启用 Telnet 控制台界面。 **默认值**：取消选取（禁用）
"Max Sessions"（最大会话数）	显示机箱允许的最大并发 Telnet 会话数。该属性的更改会在下次登录时生效；不会影响当前激活的会话数（包含您自己的）。 **允许范围** ：1–4 **默认值**：4 **注：** 如果将"Max Sessions"（最大会话）属性的值更改到小于当前"Active Sessions"（活动会话）数并注销，则在其它会话终止或过期之前，您将无法再次登录。
"Idle Timeout"（空闲超时）	显示空闲 Telnet 会话自动断开连接前等待的秒数。对"Timeout"（超时）设置的更改在下次登录时生效；它不影响当前会话。 **"Timeout Range"（超时范围）**：0 或 60 – 10800 秒。要禁用"Timeout"（超时）功能，请输入 0。 **默认值**：1800 秒
"Port Number"（端口号）	显示 CMC 用来监听服务器连接的端口。 **默认值**：23

表 5-54. 远程 RACADM 设置

设置	说明
已启用	启用远程 RACADM 公用程序访问 CMC。 **默认**：选中（启用）。

"Max Sessions"（最大会话数）	显示机箱允许的最大并发 RACADM 会话数。该属性的更改会在下次登录时生效；不会影响当前**激活的会话**数（包含您自己的）。 **允许范围** ：1–4 **默认值**：4 **注：** 如果将"Max Sessions"（最大会话）属性的值更改到小于当前"Active Sessions"（活动会话）数并注销，则在其它会话终止或过期之前，您将无法再次登录。
"Idle Timeout"（空闲超时）	显示空闲 racadm 会话自动断开连接前等待的秒数。"Idle Timeout"（空闲超时）设置的更改会在下次登录生效；不会影响当前会话。要禁用"Idle Timeout"（空闲超时）功能，请输入 0。 **"Timeout Range"（超时范围）**：0 或 10 至 1920 秒。要禁用"Timeout"（超时）功能，请输入 0。 **默认**：30 秒

表 5-55. SNMP 配置

设置	说明
已启用	在 CMC 上启用 SNMP。 **有效值**：选中（启用），取消选中（禁用） **默认值**：取消选中（禁用）
"Community Name"（团体名称）	显示用于从 CMC 的 SNMP 守护程序获得数据的团体字符串。

表 5-56. 远程系统日志配置

设置	说明
已启用	启用 CMC 日志和硬件日志条目到指定服务器的传输和远程采集。 **有效值**：选中（启用），取消选中（禁用） **默认值**：取消选中（禁用）
"Syslog Server 1"（系统日志服务器 1）	有可能运行 CMC 副本和硬件日志条目的三个服务器中的第一个。指定为主机名、IPv6 地址或 IPv4 地址。
"Syslog Server 2"（系统日志服务器 2）	有可能运行 CMC 副本和硬件日志条目的三个服务器中的第二个。指定为主机名、IPv6 地址或 IPv4 地址。
"Syslog Server 3"（系统日志服务器 3）	有可能运行 CMC 副本和硬件日志条目的三个服务器中的第三个。指定为主机名、IPv6 地址或 IPv4 地址。
"Syslog Port Number"（系统日志端口号）	指定接收 CMC 副本和硬件日志条目的远程服务器端口号。三台服务器均使用相同的端口号。有效的系统日志端口号在 10-65535 范围内。 **默认值**：514

配置电源预算

CMC 允许预算并管理机箱电源。电源管理服务根据需要优化电源消耗并对不同模块重新分配电源。

有关通过 CMC 配置电源的说明，请参阅 "配置和管理电源"。

有关 CMC 电源管理服务的详情，请参阅 "电源管理"。

管理固件更新

本节说明如何使用 Web 界面更新固件。可以使用 GUI 或 RACADM 命令更新以下机箱组件：

- CMC — 活动和待机
- iKVM
- iDRAC
- IOM 基础设施设备

当更新固件时，遵守推荐流程可以防止更新失败时服务掉失。有关使用本节中说明之前所需遵守的的指导原则，请参阅 "安装或更新 CMC 固件"。

查看当前固件版本

"Update"（更新）页显示机箱中所有可更新组件的当前版本。这些可能包括 iKVM 固件、活动 CMC 固件、（如适用）待机 CMC 固件、iDRAC 固件和 IOM 基础设施设备固件。有关详情，请参阅"更新 IOM 基础设施设备固件"。

要为所选设备打开更新页面：

1. 单击设备名称或选择**"Select / Deselect All"（选择全部/取消全部选择）**复选框。
2. 单击**"Apply Update"（应用更新）**。

   显示选定设备的更新页。

如果机箱中包含 iDRAC 处于恢复模式的上一代服务器，或者 CMC 检测到 iDRAC 中有已损坏的固件，则上一代 iDRAC 也将列在"Firmware Update"（固件更新）页中。有关使用 CMC 恢复 iDRAC 固件的步骤，请参阅 "使用 CMC 恢复iDRAC 固件"。

要查看可更新的机箱组件：

1. 登录到 Web 界面。有关详情，请参阅"访问 CMC Web 界面"。
2. 在系统树中选择**"Chassis Overview"（机箱概览）**。
3. 单击 **"Update"（更新）**选项卡。显示**"Firmware Update"（固件更新）**页面。

要查看可更新服务器组件：

1. 登录到 Web 界面。有关详情，请参阅"访问 CMC Web 界面"。
2. 在系统树中单击**"Server Overview"（服务器概览）**。
3. 单击 **Update**（更新）选项卡。显示**"Server Component Update"（服务器组件更新）**页面。

更新固件

注： 要更新 CMC 的固件，必须具备**机箱配置管理员**权限。

注： 固件更新保存当前 CMC 和 iKVM 设置。

注： 如果使用 Web 用户界面会话更新系统组件固件，则**"Idle Timeout"（空闲超时）**设置必须设置为足够大的值以便适应文件传输时间。在某些情况下，固件文件传输时间可能长达 30 分钟。要设置**"Idle Timeout"（空闲超时）**值，请参阅"配置服务"。

"Firmware Update"（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修订。更新设备固件的基本步骤包括：

- 选择要更新的设备
- 单击组合下面的**"Apply"（应用）**按钮
- 单击**"Browse"（浏览）**选择固件映像
- 单击**"Begin Firmware Update"（开始固件更新）**开始更新过程。显示说明**"Transferring file image"（正在传送文件映像）**的消息，后面是状态进度页。

注： 确保您具有最新的固件版本。您可以从 Dell 支持网站 support.dell.com 下载最新版本的固件映像文件。

更新 CMC 固件

注： 在服务器 CMC 固件或 iDRAC 固件更新期间，机箱中部分或所有风扇装置都将以 100% 速率旋转。这是正常现象。

注： 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交换。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 将不运行更新的映像，只有待机 CMC 会运行该映像。一般来说，强烈推荐为活动和待机 CMC 维护相同的固件版本。

注： 要在重设时避免与其他用户断开连接，通知可能登入 CMC 的授权用户，并查看**"Sessions"（会话）**页中活动的会话。要打开**"Sessions"（会话）**页，选择树中的**"Chassis"（机箱）**，单击**"Network"（网络）**选项卡，然后单击**"Sessions"（会话）**子选项卡。通过页面右上角的**"Help"（帮助）**链接可以访问该页的帮助。

注： 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。有关说明，请参阅 "允许在 Internet Explorer 中播放动画"。

注： 如果在使用 Internet Explorer 从 CMC 下载文件时遇到问题，请启用**"Do not save encrypted pages to disk"（不将加密的页存盘）**选项。有关说明，请参阅 "使用 Internet Explorer 从 CMC 下载文件"。

1. 在**"Firmware Update"（固件更新）**页上，通过选中 CMC 的**"Update Targets"（更新目标）**复选框选择要更新的 CMC。可以同时更新两个 CMC。

2. 单击 CMC 组件列表下面的**"Apply CMC Update"（应用 CMC 更新）**按钮。

   注： 默认 CMC 固件映像名称是 **firmimg.cmc**。在更新 IOM 基础设施设备固件之前，应该首先更新 CMC 固件。

3. 在**"Firmware Image"（固件映像）**字段中，在 management station 或共享网络上输入固件映像文件的路径，或单击**"Browse"（浏览）**导航到文件位置。

4. 单击**"Begin Firmware Update"（开始固件更新）**。在**"Firmware Update Progress"（固件更新过程）**部分提供固件更新状态信息。当上载映像时，页面上将显示状态指示灯。文件传输时间根据连接速度而显著不同。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。其它注意事项：

   - 在文传输过程中，请勿使用**"Refresh"（刷新）**按钮或导航到其它页。
   - 要取消进程，请单击**"Cancel File Transfer and Update"（取消文件传输和更新）** — 该选项仅可在文件传输过程中可用。
   - 更新状态显示在**"Update State"（更新状态）**字段中；在文件传输过程中将自动更新该字段。

注： 更新 CMC 可能会花费几分钟。

5. 对于待机 CMC，当完成更新时，**"Update State"（更新状态）**字段将显示"Done"（完成）。对于活动 CMC，在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 离线时掉失。必须在几分钟后等活动 CMC 重新启动时再次登录。

   重设 CMC 后，新的固件将显示在**"Firmware Update"（固件更新）**页上。

注： 固件更新后，清除 Web 浏览器高速缓存。有关如何清除浏览器缓存的说明，请参阅 Web 浏览器联机帮助。

更新 iKVM 固件

注： 成功上传固件后，iKVM 将重设并暂时不可用。

1. 登录到 CMC Web 界面。

2. 在系统树中选择**"Chassis Overview"（机箱概览）**。

3. 单击 **"Update"（更新）**选项卡。显示**"Firmware Update"（固件更新）**页面。

4. 通过选中 iKVM 的**"Update Targets"（更新目标）**复选框选择要更新的 iKVM。

5. 单击 iKVM 组件列表下面的**"Apply iKVM Update"（应用 iKVM 更新）**按钮。

6. 在**"Firmware Image"（固件映像）**字段中，在 management station 或共享网络上输入固件映像文件的路径，或单击**"Browse"（浏览）**导航到文件位置。

注： 默认 iKVM 固件映像名是 i**kvm.bin**；但用户可以更改 iKVM 固件映像名以避免与之前的映像混淆。

7. 单击**"Begin Firmware Update"（开始固件更新）**。

8. 单击 **Yes**（是）以继续。在**"Firmware Update Progress"（固件更新过程）**部分提供固件更新状态信息。当上载映像时，页面上将显示状态指示灯。文件传输时间根据连接速度而显著不同。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。其它注意事项：

   - 在文传输过程中，请勿使用**"Refresh"（刷新）**按钮或导航到其它页。
   - 要取消进程，请单击**"Cancel File Transfer and Update"（取消文件传输和更新）** — 该选项仅可在文件传输过程中可用。
   - 更新状态显示在**"Update State"（更新状态）**字段中；在文件传输过程中将自动更新该字段。

注： 更新 iKVM 最多需要两分钟。

当更新完成时，iKVM 将重设且新固件将显示在**"Firmware Update"（固件更新）**页上。

更新 IOM 基础设施设备固件

通过执行此更新，会更新 IOM 设备组件的固件，但不会更新 IOM 设备自身的固件；组件是 IOM 设备和 CMC 之间的接口电路。组件的更新映像驻留在 CMC 文件系统中，如果组件和 CMC 上组件映像的当前版本不匹配，组件仅显示为 CMC Web GUI 上的可更新设备。

1. 登录到 CMC Web 界面。

2. 在系统树中选择"**Chassis Overview"（机箱概览）**。

3. 单击 **"Update"（更新）**选项卡。显示**"Firmware Update"（固件更新）**页面。

4. 通过选择该 IOM 设备的**"Update Targets"（更新目标）**复选框选择要更新的 IOM 设备。

5. 单击 IOM 组件列表下面的**"Apply IOM Update"（应用 IOM 更新）**按钮。

   注： 对于 IOM 基础设施设备 (IOMINF) 目标，不显示**"Firmware Image"（固件映像）**字段，因为必要的映像保存在 CMC 上。在更新 IOMINF 基础设施设备固件之前，应该先更新 CMC 固件。

   如果 CMC 检测到 IOMINF 固件对于 CMC 文件系统中包含的映像已经过时，则 CMC 允许更新 IOMINF。如果 IOMINF 固件是最新的，CMC 将阻止 IOMINF 更新。最新的 IOMINF 设备列为可更新设备。

6. 单击**"Begin Firmware Update"（开始固件更新）**。在**"Firmware Update Progress"（固件更新过程）**部分提供固件更新状态信息。当上载映像时，页面上将显示状态指示灯。文件传输时间根据连接速度而显著不同。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。其它注意事项：

   - 在文件传输过程中，请勿使用**"Refresh"（刷新）**按钮或导航到其它页。
   - 更新状态显示在**"Update State"（更新状态）**字段中；在文件传输过程中将自动更新该字段。

注： 当更新 IOMINF 固件时，不会显示文件传输计时器。更新过程将导致暂时失去到 IOM 设备的连接，因为当更新完成时设备将执行重新启动。更新完成后，显示新固件且更新后的系统不再于**"Firmware Update"（固件更新）**页面上显示。

更新服务器 iDRAC 固件

注： 成功上载固件更新后，iDRAC（服务器上）将重设并暂时不可用。

注： 对于带有 iDRAC 的服务器，iDRAC 固件必须为版本 1.4 或更高版本，对于带有 iDRAC6 Enterprise 的服务器，必须为版本 2.0 或更高版本。

1. 登录到 CMC Web 界面。
2. 在系统树中选择**"Chassis Overview"（机箱概览）**。
3. 单击 **Update（更新）**选项卡。显示**"Firmware Update"（固件更新）**页面。
4. 通过选择那些设备的**"Update Targets"（更新目标）**，选择要更新的 iDRAC。
5. 单击 iDRAC 组件列表下面的**"Apply iDRAC Update"（应用 iDRAC 更新）**按钮。
6. 在**"Firmware Image"（固件映像）**字段中，在 management station 或共享网络上输入固件映像文件的路径，或单击**"Browse"（浏览）**导航到文件位置。
7. 单击**"Begin Firmware Update"（开始固件更新）**。在**"Firmware Update Progress"（固件更新过程）**部分提供固件更新状态信息。当上载映像时，页面上将显示状态指示灯。文件传输时间根据连接速度而显著不同。当内部更新过程开始时，将自动刷新页面并显示固件更新计时器。其它注意事项：
   - 在文件传输过程中，请勿使用**"Refresh"（刷新）**按钮或导航到其它页。
   - 要取消进程，请单击**"Cancel File Transfer and Update"（取消文件传输和更新）** — 该选项仅可在文件传输过程中可用。
   - 更新状态显示在**"Update State"（更新状态）**字段中；在文件传输过程中将自动更新该字段。

注： 更新 CMC 或服务器可能会花费几分钟。

使用 CMC 恢复iDRAC 固件

iDRAC 固件通常使用 iDRAC 工具更新，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。请参阅《*iDRAC 固件用户指南*》了解更新 iDRAC 固件的说明。

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**"Firmware Update"（固件更新）**页上列出服务器。

请按以下步骤更新 iDRAC 固件。

1. 从 **support.dell.com** 将最新的 iDRAC 固件下载到管理计算机上。
2. 登录到 Web 界面（请参阅 "访问 CMC Web 界面"）。
3. 在系统树中选择**"Chassis Overview"（机箱概览）**。
4. 单击 **"Update"（更新）**选项卡。显示**"Firmware Update"（固件更新）**页面。
5. 通过选择那些设备的**"Update Targets"（更新目标）**，选择要更新的相同型号的 iDRAC。

6. 单击 iDRAC 组件列表下面的**"Apply iDRAC Update"（应用 iDRAC 更新）**按钮。

7. 单击**"Browse"（浏览）**，浏览到下载的 iDRAC 固件映像，并单击**"Open"（打开）**。

   注： 默认 iDRAC 固件映像名称是 **firmimg.imc**。在更新 IOM 基础设施设备固件之前，应该首先更新 CMC 固件。

8. 单击**"Begin Firmware Update"（开始固件更新）**。其它注意事项：
   - 在文件传输过程中，请勿使用**"Refresh"（刷新）**按钮或导航到其它页。
   - 要取消进程，请单击**"Cancel File Transfer and Update"（取消文件传输和更新）** — 该选项仅可在文件传输过程中可用。
   - 更新状态显示在**"Update State"（更新状态）**字段中；在文件传输过程中将自动更新该字段。

注： 更新 iDRAC 固件需要大约十分钟。

管理 iDRAC

CMC 提供"Deploy iDRAC"（部署 iDRAC）页，允许用户配置安装和新插入的服务器的 iDRAC 网络设置。用户可从此页配置安装的一个或多个 iDRAC 设备。用户也可为今后将要安装的服务器配置默认的 iDRAC 网络配置设置和根密码；这些默认设置是**"iDRAC QuickDeploy"（iDRAC 快速部署）**设置。

有关 iDRAC 行为的详情，请参阅 Dell 支持网站 **support.dell.com/manuals** 上的*《iDRAC 用户指南》*。

iDRAC 快速部署

"Deploy iDRAC"（部署 iDRAC）页的**"iDRAC QuickDeploy"（iDRAC 快速部署）**部分包含适用于新插入服务器的网络配置设置。可使用这些设置自动填充"QuickDeploy"（快速部署）部分下面的**"iDRAC Network Settings"（iDRAC 网络设置）**表。一旦启用快速部署，快速部署设置将适用于安装服务器时的服务器。请参阅"使用 LCD 配置向导配置网络"中的步骤 8，了解有关"iDRAC QuickDeploy"（iDRAC 快速部署）设置的详细信息。

按照这些步骤启用并设置**"iDRAC QuickDeploy"（iDRAC 快速部署）**设置：

1. 登录 CMC Web 界面。
2. 在系统树中选择**"Server Overview"（服务器概览）**。
3. 单击**"Setup"（设置）**选项卡。显示**"Deploy iDRAC"（部署 iDRAC）**页。
4. 相应地设置快速部署设置。

表 5-57. 快速部署设置

设置	说明
启用快速部署	启用/禁用将此页上配置的 iDRAC 设置自动应用到新插入服务器的**"QuickDeploy"（快速部署）**功能；*必须*在本地 LCD 面板上确认自动配置。 **注：** 如果选中**"Set iDRAC Root Password on Server Insertion"（插入服务器时设置 iDRAC 根密码）**框，则包括根用户密码。 **默认值**：取消选取（禁用）
插入服务器时设置 iDRAC 根密码	插入服务器时，指定服务器的 iDRAC 根密码是否应该改为**"iDRAC Root Password"（iDRAC 根密码）**文本框中提供的值。
iDRAC 根密码	选中**"Set iDRAC Root Password on Server Insertion"（插入服务器时设置 iDRAC 根密码）**和**"QuickDeploy Enabled"（启用快速部署）后**，将服务器插入机箱时此密码值被分配到服务器的 iDRAC 根用户密码。此密码包括 1 到 20 个可打印（含空格）字符。
确认 iDRAC 根密码	验证输入**"iDRAC Root Password"（iDRAC 根密码）**字段的密码。
启用 iDRAC LAN	启用/禁用 iDRAC LAN 信道。 **默认值**：取消选取（禁用）
启用 iDRAC IPv4	启用/禁用 iDRAC 上的 IPv4。默认设置为已启用。
启用 LAN 上 iDRAC IPMI	为机箱中存在的每个 iDRAC 启用/禁用 LAN 上的 IPMI 信道。 **默认值**：取消选取（禁用）
启用 iDRAC DHCP	为机箱中存在的每个 iDRAC 启用/禁用 DHCP。如果启用此选项，则禁用字段**"QuickDeploy IP"（快速部署 IP）**、**"QuickDeploy Subnet Mask"（快速部署子网掩码）**和**"QuickDeploy Gateway"（快速部署网关）**，且无法修改，因为将使用 DHCP 自动为每个 iDRAC 分配这些设置。

	默认值：取消选取（禁用）
"Starting iDRAC IPv4 Address (Slot 1)"（起始 iDRAC IPv4 地址 [插槽 1]）	指定机壳插槽 1 中服务器 iDRAC 的静态 IP 地址。从插槽 1 的静态 IP 地址开始，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，则将在按下**"Save QuickDeploy Settings"（保存快速部署设置）**或**"Auto-Populate Using QuickDeploy Settings"（使用快速部署设置自动填充）**按钮时显示"QuickDeploy IP address range is not fully within QuickDeploy Subnet"（快速部署 IP 地址范围没有完全在快速部署子网内）错误消息。
"iDRAC IPv4 Netmask"（iDRAC IPv4 网络掩码）	指定被分配到所有新插入服务器的快速部署子网掩码。
"iDRAC IPv4 Gateway"（iDRAC IPv4 网关）	指定被分配到机箱中所有 iDRAC 的快速部署默认网关。
"Enable iDRAC IPv6"（启用 iDRAC IPv6）	为机箱中支持 IPv6 的每个 iDRAC 启用 IPv6 寻址。
"Enable iDRAC IPv6 Autoconfiguration"（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。默认设置为已启用。
"iDRAC IPv6 Gateway"（iDRAC IPv6 网关）	指定要分配给 iDRAC 的默认 IPv6 网关。默认设置是 "::"。
"iDRAC IPv6 Prefix Length"（iDRAC IPv6 前缀长度）	指定要为 iDRAC 上的 IPv6 地址分配的前缀长度。默认设置是 64。

5. 要保存选择，单击**"Save QuickDeploy Settings"（保存快速部署设置）**按钮。如果更改 iDRAC 网络设置，单击**"Apply iDRAC Network Settings"（应用 iDRAC 网络设置）**按钮将设置部署到 iDRAC。

6. 要将表格更新为上次保存的快速部署设置，并且将安装的各台服务器的 iDRAC 网络设置恢复为当前值，请单击**"Refresh"（刷新）**。

注： 单击**"Refresh"（刷新）**按钮删除所有未保存的 iDRAC 快速部署和 iDRAC 网络配置设置。

快速部署功能仅在启用并且服务器插入机箱中时执行。如果选中**"Set iDRAC Root Password on Server Insertion"（插入服务器时设置 iDRAC 根密码）**和**"QuickDeploy Enabled"（启用快速部署）**，则在 LCD 界面中会提示用户允许或不允许密码更改。如果网络配置设置不同于当前的 iDRAC 设置，则提示用户接受或不接受更改。

注： 如果存在 LAN 或 LAN 上 IPMI 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 Network Settings"（iDRAC 网络设置）**部分，请单击**"Auto-Populate Using QuickDeploy Settings"（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 Network Configuration Settings"（iDRAC 网络配置设置）**表中的相应字段。

注： 对"QuickDeploy"（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。按下**"Refresh"（刷新）**按钮太快时，可能只显示一台或多台 iDRAC 服务器的部分正确数据。

iDRAC 网络设置

"Deploy iDRAC"（部署 iDRAC）页的**"iDRAC Network Settings"（iDRAC 网络设置）**部分包含一个表格，列出所有已安装服务器的 iDRAC IPv4 和 IPv6 网络配置设置。使用此表格，您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。更改字段并单击**"Apply iDRAC Network Settings"（应用 iDRAC 网络设置）**会将更改的字段保存到 iDRAC。按照这些步骤启用并设置**"iDRAC Network Settings"（iDRAC 网络设置）**：

1. 登录 CMC Web 界面。

2. 在系统树中选择**"Server Overview"（服务器概览）**。

3. 单击**"Setup"（设置）**选项卡。

   显示"**Deploy iDRAC"（部署 iDRAC）**页。

4. 选中**"QuickDeploy Enabled"（启用快速部署）**复选框启用快速部署设置。

5. 相应设置其余的**"iDRAC Network Settings"（iDRAC 网络设置）**。

表 5-58. iDRAC 网络设置

设置	说明
插槽	显示机箱中服务器占用的插槽。插槽号是顺序 ID，从 1 到 16（机箱中有 16 个可用插槽），它有助于识别机箱中服务器的位置。

	注： 如果占用插槽的服务器少于 16 台，则仅显示插有服务器的插槽。
Name（名称）	显示每个插槽中服务器的服务器名称。在默认情况下，插槽的名称从 **SLOT-01** 到 **SLOT-16**。 **注：** 插槽名称不能为空或 NULL。
"Enable LAN"（启用 LAN）	启用（选中时）或禁用（取消选中时）LAN 信道。 **注：** 没有选中（禁用）LAN 时，不会使用所有其他网络配置设置（**LAN 上 IPMI**、**DHCP**、**IP 地址子网掩码**和**网关**）。这些字段不可访问。
更改根密码	启用（选中时）更改 iDRAC 根用户密码的功能。必须提供**"iDRAC Root Password"（iDRAC 根密码）**和**"Confirm iDRAC Root Password"（确认 iDRAC 根密码）**字段，此操作才能成功。
DHCP	如果选中的 DHCP 用于获取 iDRAC IP 地址，则子网掩码是默认网关，否则使用 iDRAC 网络配置字段中定义的值。必须启用 LAN 才能设置此字段
"IPMI over LAN"（LAN 上 IPMI）	启用（选中时）或禁用（取消选取时）IPMI LAN 信道。必须启用 LAN 才能设置此字段。
IP 地址	给位于此插槽中的 iDRAC 分配的静态 IPv4 或 IPv6 地址。
Subnet Mask（子网掩码）	指定分配到此插槽中安装的 iDRAC 的子网掩码。
网关	指定分配到将安装到此插槽中的 iDRAC 的默认网关。
"Enable IPv4"（启用 IPv4）	允许插槽中的 iDRAC 在网络中使用 IPv4 协议。您必须选择**"Enable LAN"（启用 LAN）**选项，此选项才会激活。默认设置为已启用。
"Enable IPv6"（启用 IPv6）	允许插槽中的 iDRAC 在网络中使用 IPv6 协议。您必须选择**"Enable LAN"（启用 LAN）**选项并取消选择**"Autoconfiguration"（自动配置）**选项，此选项才会激活。默认设置为已禁用。 **注：** 只有服务器支持 IPv6 时，此选项才可用。
"Autoconfiguration"（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。 **注：** 只有服务器支持 IPv6 时，此选项才可用。
"Prefix Length"（前缀长度）	指定 iDRAC 所属的 IPv6 子网的长度（以位为单位）。

6. 要将设置部署到 iDRAC，单击**"Apply iDRAC Network Settings"（应用 iDRAC 网络设置）**按钮。如果您对快速部署设置做出了更改，也会保存这些设置。

7. 要将"iDRAC Network"（iDRAC 网络）设置恢复为安装的各服务器的当前值，并将快速部署表更新为上次保存的快速部署设置，请单击**"Refresh"（刷新）**。

注： 单击**"Refresh"（刷新）**按钮将删除所有未保存的 iDRAC 快速部署和 iDRAC 网络配置设置。

"**iDRAC Network Settings"（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可能或不可能与当前安装的 iDRAC 网络配置设置相同。更改后按**"Refresh"（刷新）**按钮更新**"iDRAC Deploy"（iDRAC 部署）**页和每个安装的 iDRAC 网络配置设置。

注： 对"QuickDeploy"（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。按**"Refresh"（刷新）**按钮太快时，可能只显示一台或多台 iDRAC 服务器的部分正确数据。

从 CMC GUI 启动远程控制台

此功能允许从服务器直接启动键盘-视频-鼠标 (KVM) 会话。

若要从 CMC GUI 主页启动服务器远程控制台：

1. 单击机箱图形中的指定服务器。

2. 在**"Quicklinks"（快速链接）**上，单击**"Launch Remote Console"（启动远程控制台）**链接。

若要从**"Server Status"（服务器状况）**页启动服务器远程控制台：

1. 在系统树上选择**"Server Overview"（服务器概览）**。

2. 单击表中指定服务器的**"Launch Remote Console"（启动远程控制台）**。

若要为一个服务器启动服务器远程控制台：

1. 在系统树中展开**"Server Overview"（服务器概览）**。展开的"Servers"（服务器）列表中显示所有服务器 (1–16)。

2. 在系统树上单击要查看的服务器。随即显示**"Server Status"（服务器状态）**页。

3. 单击**"Launch Remote Console"（启动远程控制台）**。

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。
- 服务器为 PowerEdge M610、M610X、M710、M710HD 或 M910。
- 服务器上的 LAN 界面已启用。
- iDRAC 版本为 2.20 或以上。
- 主机系统安装有 JRE（Java Runtime Environment）6 Update 16 或以上版本。
- 主机上的浏览器支持弹出窗口（禁用弹出窗口阻止程序）。

注： 远程控制台也可从 iDRAC GUI 启动。有关详情，请参阅 iDRAC GUI。

使用单次登录启动 iDRAC

CMC 提供单独机箱组件（例如服务器）的有限管理。为了全面管理这些单独组件，CMC 为基于 Web 界面的服务器管理控制器 (iDRAC) 提供一个启动位置。

要从**"Servers"（服务器）**页面启动 iDRAC 管理控制台，请使用以下步骤：

1. 登录 CMC Web 界面。

2. 在系统树中选择**"Server Overview"（服务器概览）**。随即出现**"Server Status"（服务器状况）**页。

3. 单击您要管理的服务器的**"Launch iDRAC GUI"（启动 iDRAC GUI）按钮**。

要启动单独服务器的 iDRAC 管理控制台：

1. 登录 CMC Web 界面。

2. 在系统树中展开**"Server Overview"（服务器概览）**。展开的**"Servers"（服务器）**列表中出现的所有服务器 (1–16)。

3. 单击想要查看的服务器。随即显示**"Server Status"（服务器状况）**页。

4. 单击**"Launch iDRAC GUI"（启动 iDRAC GUI）按钮**。

用户不需要二次登录即可启动 iDRAC GUI，因为此功能利用单次登录。下面介绍单次登录策略。

- 拥有服务器管理权限的 CMC 用户将使用单次登录自动登录到 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，将使用单次登录自动登录到 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，将**不**会使用单次登录自动登录到 iDRAC。单击**"Launch iDRAC GUI"（启动 iDRAC GUI）**按钮可将此用户导航至 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，则不会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次登录策略公告）。

注： 如果禁用 iDRAC 网络 LAN（LAN 启用 = 否），单次登录不可用。

注： 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，然后单击"Launch iDRAC GUI"（启动 iDRAC GUI）图标可能显示一个错误页。

FlexAddress

本节介绍 FlexAddress 功能 Web 界面屏幕。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： 您必须购买和安装 FlexAddress 升级才可以访问该配置屏幕。如果尚未购买和安装升级，Web 界面上将显示以下文本：

```
"Optional feature not installed."（未安装可选功能。） See the Dell Chassis Management Controller Users Guide for information on the chassis-based WWN and MAC address administration feature. (有关基于机箱的 WWN 和 MAC 地址管理功能的信息，请参阅 Dell 机箱管理控制器用户指南。)

To purchase this feature, please contact Dell at www.dell.com. (要购买该功能，请通过 www.dell.com 联系 Dell。)
```

查看 FlexAddress 状态

可以使用 Web 界面查看 FlexAddress 状态信息。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 激活/未激活
- 插槽数量和名称
- 机箱分配的地址和服务器分配的地址
- 使用中的地址

注： 也可以使用命令行界面查看 FlexAddress 状态。有关命令详情，请参阅"使用 FlexAddress"。

查看机箱 FlexAddress 状态

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 状态概览。

使用以下步骤查看机箱的 FlexAddress 是否激活：

1. 登录到 Web 界面（请参阅 "访问 CMC Web 界面"）。
2. 在系统树中选择**"Chassis Overview"（机箱概览）**。
3. 单击**"Setup"（设置）**选项卡。随即出现**"General Setup"（一般设置）**页。FlexAddress 输入项的值为**"Active"（激活）**或**"Not Active"（未激活）**；值为激活表示机箱上已安装此功能。值为未激活表示机箱上未安装此功能且机箱中未使用此功能。.

使用以下步骤显示每个服务器模块的 FlexAddress 状态概览。

1. 登录到 Web 界面("访问 CMC Web 界面")。
2. 在系统树中单击**"Server Overview"（服务器概览）**。单击**"Properties"（属性）→ WWN/MAC（日期/时间）**。
3. 随即显示**"FlexAddress Summary"（FlexAddress 摘要）**页。本页允许查看机箱中所有插槽的 WWN 配置和 MAC 地址。

   状态页显示以下信息：

结构配置	**"Fabric A"（结构 A）**、**"Fabric B"（结构 B）**和**"Fabric C"（结构 C）**显示已安装输入/输出结构的类型。 **iDRAC** 显示服务器管理 MAC 地址。 **注：** 如果启用结构 A，未填充的插槽会显示机箱为结构 A 分配的 MAC 地址；如果它们被填充的插槽使用，则会显示结构 B 和 C 的 MAC 或 WWN。
WWN/MAC 地址	显示机箱中每个插槽的 FlexAddress 配置。显示的信息包括： • iDRAC 管理控制器不是结构，但其 FlexAddress 被视为一个结构。 • 插槽编号和位置 • FlexAddress 激活/未激活状态 • 连接结构类型 • 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。

4. 有关详情，请单击**"Help"（帮助）**链接并查看"使用 FlexAddress"。

查看服务器 FlexAddress 状态

还可以显示单个服务器的 FlexAddress 状态信息。服务器级别信息显示服务器的 FlexAddress 状态概览。

使用以下步骤查看 FlexAddress 服务器信息：

1. 登录到 Web 界面（请参阅 "访问 CMC Web 界面"）。

2. 在系统树中展开**"Server Overview"（服务器概览）**。展开的**"Servers"（服务器）**列表中出现的所有服务器 (1–16)。

3. 单击想要查看的服务器。随即显示**"Server Status"（服务器状况）**页。

4. 单击**"Setup"（设置）**选项卡和 **FlexAddress** 子选项卡。随即显示**"Deploy FlexAddress**"（部署 FlexAddress）页。本页允许查看选定服务器的 WWN 配置和 MAC 地址。

   状态页显示以下信息：

"FlexAddress Enabled"（已启用 FlexAddress）	显示特定插槽的 FlexAddress 功能是否激活。		
当前状态	显示当前 FlexAddress 配置： • **"Chassis-Assigned"（机箱分配）** — 选定的插槽地址是通过使用 FlexAddress 得到的机箱分配的地址。即使插入新的服务器，基于插槽的 WWN/MAC 地址仍保持相同。 • **"Server-Assigned"（服务器分配）** - 服务器使用由服务器分配的地址，或者嵌入控制器硬件中的默认地址。		
"Power State"（电源状态）	显示当前服务器的电源状态；值为**"On"（开）**、**"Powering On"（电源打开）**、**"Powering Off"（电源关闭）**、**"Off"（关）**和 **"N/A"（无）**（如果服务器不存在）。		
运行状况		OK（良好）	表示 FlexAddress 存在并提供 CMC 状态。在 CMC 和 FlexAddress 之间发生通信故障时，CMC 不能获取或显示 FlexAddress 的运行状况。
		"Informational"（通知）	当运行状况（"OK"[正常]、"Warning"[警告]、"Critical"[严重]）没有发生变化时，显示关于 FlexAddress 的信息。
		"Warning"（警告）	表示仅发出了警告警报，**必须采取纠正措施。**如果未采取纠正措施，则可发生影响服务器完整性的严重故障。
		"Critical"（严重）	指示至少已发出一个故障警报。严重状态表示服务器上发生系统故障，**必须立即采取纠正措施**。
		"No value"（无值）	当 FlexAddress 不存在时，不提供运行状况信息。
"iDRAC firmware"（iDRAC 固件）	显示当前安装在服务器上的 iDRAC 版本。		
"BIOS Version"（BIOS 版本）	显示服务器模块的当前 BIOS 版本。		
"Slot"（插槽）	与结构位置相关联的服务器插槽编号。		
"Location"（位置）	按组号（A、B 或 C）和插槽号（1 或 2）表示输入/输出 (I/O) 模块在机箱中的位置。插槽名称：A1、A2、B1、B2、C1 或 C2。		
"Fabric"（结构）	显示结构的类型。		
"Server-Assigned"（服务器分配）	显示嵌入控制器硬件的服务器分配的 WWN/MAC 地址。		
"Chassis-Assigned"（机箱分配）	显示机箱分配的用于特定插槽的 WWN/MAC 地址。		

5. 有关详情，请单击**"Help"**链接并查看 "使用 FlexAddress"。

配置 FlexAddress

如果随机箱购买了 FlexAddress，则系统中已安装 FlexAddress 且在启动系统时便是活动的。如果单独购买 FlexAddress，则必须按照*《机箱管理控制器 (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。有关此说明文件的详情，请查看 **support.dell.com / manuals**。

开始配置前必须关闭服务器。可以启用或禁用每个结构上的 FlexAddress。此外，还可以在每个插槽的基础上启用/禁用该功能。在每结构基础上启用该功能后，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。所有其他结构将使用服务器上工厂分配的 WWN/MAC。

选定的插槽将会为所有已启用的结构启用 FlexAddress。例如，如果启用结构 A 和 B，要在结构 A 的插槽 1 上启用 FlexAddress，而不在结构 B 的插槽 1 上启用 FlexAddress，这是不可能的。

注： 也可以使用命令行界面配置 FlexAddress。有关命令详情，请参阅"使用 FlexAddress"。

机箱级别结构和插槽 FlexAddress 配置

在机箱级别，可以启用或禁用结构和插槽的 FlexAddress 功能。FlexAddress 在每个结构的基础上启用，然后选择参与该功能的插槽。必须启用结构和插槽才能成功配置 FlexAddress。

执行以下启用或禁用结构和插槽的步骤以便使用 FlexAddress 功能：

1. 登录到 Web 界面（请参阅 "访问 CMC Web 界面"）。
2. 在系统树中单击**"Server Overview"（服务器概览）**。
3. 单击**"Setup"（设置）**选项卡 →**FlexAddress** 子选项卡。随即显示**"Deploy FlexAddress"（部署 FlexAddress）**页。
4. "**Select Fabrics for Chassis-Assigned WWN/MACs"（为机箱分配的 WWN/MAC 选择结构）**显示**"Fabric A"（结构 A）**、**"Fabric B"（结构 B）**、**"Fabric C"（结构 C）**和 **iDRAC 的复选框。**
5. 为希望启用 FlexAddress 功能的每个结构单击复选框。要禁用结构，请单击复选框以清除选择。

注： 如果没有选定的结构，则不会为选择的插槽启用 FlexAddress。

"Select Slots for Chassis-Assigned WWN/MACs"（为机箱分配的 WWN/MAC 选择插槽）页为机箱中的每个插槽 (1 - 16) 显示**"Enabled"（启用）**复选框。

6. 为希望启用 FlexAddress 功能的每个插槽单击**"Enabled"（启用）**复选框。如果希望选择所有插槽，可以使用**"Select/Deselect All"（选择全部/取消全部选择）**复选框。要禁用某插槽，可以单击**"Enabled"（启用）**复选框以清除选择。

注： 如果插槽中存在服务器，则需要关闭服务器电源，才能在该插槽启用 FlexAddress 功能。

注： 如果没有选择插槽，则不会为选定的结构启用 FlexAddress。

7. 单击**"Apply"（应用）**保存更改**。**

   有关详情，请单击**"Help"（帮助）**链接并查看"使用 FlexAddress"。

服务器级别插槽 FlexAddress 配置

在服务器级别，可以启用或禁用单独插槽的 FlexAddress 功能。

使用以下步骤启用或禁用插槽以便使用 FlexAddress 功能：

1. 登录到 Web 界面（请参阅 "访问 CMC Web 界面"）。
2. 在系统树中展开**"Server Overview"（服务器概览）**。展开的**"Servers"（服务器）**列表中显示所有服务器 (1–16)。
3. 单击想要查看的服务器。随即显示**"Server Status"（服务器状况）**页。
4. 单击**"Setup"（设置）**选项卡和 **FlexAddress** 子选项卡。随即显示**"FlexAddress Status"（FlexAddress 状态）**页。
5. 使用**"FlexAddress Enabled"（启用 FlexAddress）**下拉菜单进行选择；选择**"Yes"（是）**启用 FlexAddress 或者选择**"No"（否）**禁用 FlexAddress。
6. 单击**"Apply"（应用）**保存更改。有关详情，请单击**"Help"（帮助）**链接并查看"使用 FlexAddress"。

远程文件共享

"Remote Virtual Media File Share"（远程虚拟介质文件共享）选项通过 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，以便部署或更新操作系统。连接后，远程文件可以像本地系统文件一样访问。支持两种类型的介质：软盘驱动器和 CD/DVD 驱动器。

1. 登录到 Web 界面（请参阅 "访问 CMC Web 界面"）。
2. 在系统树中单击**"Server Overview"（服务器概览）**。
3. 单击**"Setup"（设置）**选项卡和**"Remote File Sharing"（远程文件共享）**子选项卡。随即显示**"Deploy Remote File Share"（部署远程文件共享）**页。
4. 设置远程文件共享设置。

表 5-59. 远程文件共享设置

设置	说明
"Image File Path"（映像文件路径）	只有连接和部署操作才需要映像文件路径。它不适用于断开连接操作。网络驱动器的路径名称通过 Windows SMB 或 Linux/Unix NFS 协议安装到服务器。 例如，要连接到 CIFS，请键入： //<IP 用于连接 CIFS 文件系统>/<文件路径>/<映像名称> 要连接到 NFS，请键入： //<IP 用于连接 NFS 文件系统>:/<文件路径>/<映像名称> 以 **.img** 结尾的文件名以虚拟软盘的形式连接。以 **.iso** 结尾的文件名以虚拟 CD/DVD 的形式连接。最多 511 个字符。
"User Name"（用户名）	只有连接和部署操作才需要用户名。它不适用于断开连接操作。在此字段中最多可以指定 40 个字符。
"Password"（密码）	只有连接和部署操作才需要密码。它不适用于断开连接操作。在此字段中最多可以指定 40 个字符。
"Slot"（插槽）	标识插槽的位置。插槽号是有序的，从 1 到 16（用于机箱中的 16 个可用插槽）。
"Name"（名称）	显示插槽的名称。插槽的命名依据是它们在机箱中的位置。
"Model"（型号）	显示服务器的型号名称。
"Power State"（电源状态）	显示服务器的电源状态： **"N/A"（无）**- CMC 尚未确定服务器的电源状态。 **"Off"（关）**- 服务器关闭或机箱关闭。 **"On"（开）**- 机箱和服务器都打开。 **"Powering On"（正在开机）**- 关闭和打开之间的临时状态。成功后，"Power State"（电源状态）是"On"（开）。 **"Powering Off"（正在关机）**- 打开和关闭之间的临时状态。成功后，"Power State"（电源状态）是"Off"（关）。
"Connect Status"（连接状态）	显示远程文件共享连接状态。
"Select/Deselect All"（全选/取消全选）	在启动远程文件共享操作之前选择此选项。远程文件共享操作是："Connect"（连接）、"Disconnect"（断开连接）和"Deploy"（部署）。

5. 单击**"Connect"（连接）**可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，就可以访问介质。

   单击**"Disconnect"（断开连接）**可断开之前连接的远程文件共享。

   单击**"Deploy"（部署）**可部署介质设备。

   注： 在执行"部署"命令之前应保存所有工作文件，因为此操作会使服务器重新启动。

   此命令涉及以下操作：

   - 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。
   - 如果服务器已关闭，则将服务器通电。

常见问题

表 5-60 列出管理或恢复远程系统时的常见问题。

。

表 5-60. 管理和恢复远程系统

问题	解答
访问 CMC Web 界面时，我得到一个安全警告，指出 SSL 认证的主机名与 CMC 的主机名不匹配。	CMC 包括了一个默认的 CMC 服务器认证以确保 Web 界面和远程 RACADM 配置的网络安全。如果使用该认证，Web 浏览器就会显示一个安全警告，因为默认的认证是颁发给 **CMC 默认认证**的，它与 CMC 的主机名不匹配（例如，IP 地址）。 要解决这个安全问题，应上载一个颁发给 CMC IP 地址的 CMC 服务器认证。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 DNS CMC 名称匹配： 1. 在**系统**树中，单击**"Chassis Overview"（机箱概览）**。 2. 单击**"Network"（网络）**选项卡，然后单击**"Network"（网络）**。显示**"Network Configuration"（网络配置）**页。 3. 选择**"Register CMC on DNS"（在 DNS 上注册 CMC）**复选框。 4. 在**"DNS CMC Name"（DNS CMC 名称）**字段中输入 CMC 名称。 5. 单击**"Apply Changes"（应用更改）**。 有关生成 CSR 和颁发认证的详情，请参阅 "使用 SSL 和数字认证确保 CMC 通信"。
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？	重设 CMC Web Server 后，可能需要等待几分钟，远程 RACADM 服务和基于 Web 的界面才会可用。 CMC Web Server 会在发生以下情况后重设： • 使用 CMC Web 用户界面更改网络配置或网络安全性属性时 • 更改 **cfgRacTuneHttpsPort** 属性时（包括 config -f *配置文件*> 更改它时） • 使用 **racresetcfg** 时 • CMC 重设时 • 上载新的 SSL 服务器证书时
为什么我的 DNS 服务器没有注册 CMC？	有些 DNS 服务器只能注册含有 31 个或更少字符的名称。
访问 CMC Web 界面时，我得到一个安全警告，指出该 SSL 认证是由一个不可信的认证机构颁发的。	CMC 包括了一个默认的 CMC 服务器认证以确保 Web 界面和远程 RACADM 配置的网络安全。该认证*不*是由信任认证机构颁发的认证。要解决这个安全问题，上载一个由可信认证机构（例如 Thawte 或 Verisign）颁发的 CMC 服务器认证。有关颁发认证的详情，请参阅 "使用 SSL 和数字认证确保 CMC 通信"。

由于未知原因而显示以下信息：
 	
"Remote Access: SNMP Authentication Failure"（远程访问：SNMP 验证故障）
 	
为什么会发生这种情况？
	在发现过程中，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。
	
	可以使用 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，必须输入将由代理接受的团体名称。由于 CMC 只允许一个团体名称，因此必须为 IT Assistant 查找设置输入相同的 **get** 和 **set** 团体名称。

CMC 故障排除

CMC Web 界面提供用于识别、诊断和修补机箱问题的工具。有关故障排除的详情，请参阅"故障排除和恢复"。

目录