Dell EMC OpenManage Server Administrator 9.1.2 版

用户指南

DELL EMC

注、小心和警告

注：“注”表示帮助您更好地使用该产品的重要信息。

小心：“小心”表示可能会损坏硬件或导致数据丢失，并说明如何避免此类问题。

警告：“警告”表示可能会造成财产损失、人身伤害甚至死亡。

2018 - 09

Rev. A00

目录

1

简介

Server Administrator 通过两种方式提供了全面的、一对一的系统管理解决方案：一是通过集成的、基于 Web 浏览器的图形用户界面 (GUI)；二是通过操作系统的命令行界面 (CLI)。Server Administrator 使系统管理员可在本地或远程管理网络中管理系统。通过提供全面的一对一系统管理，Server Administrator 使系统管理员可以专注于管理整个网络。在 Server Administrator 的环境中，系统是指一个独立的系统，带有单独机箱网络存储单元连接的系统，或在一个模块化的机柜中包含一个或多个服务器模块的模块化系统。Server Administrator 提供以下信息：

- 正常运行的系统和出现故障的系统
- 需要执行远程恢复操作的系统

Server Administrator 通过一组全面的集成式管理服务，提供易于使用的、本地和远程系统监管。Server Administrator 是在被管理的系统上唯一需要的安装程序，可以通过 **Server Administrator** 主页进行本地和远程访问。可以通过拨入、LAN 或无线连接方式访问受监测的远程系统。Server Administrator 通过基于角色的访问控制 (RBAC)、验证和安全套接字层 (SSL) 加密技术来确保其管理连接的安全。

主题：

安装

您可以使用 *Dell EMC Systems Management Tools and Documentation 软件*来安装 Server Administrator。该软件提供安装程序来安装、升级和卸载 Server Administrator、受管系统和管理站软件组件。此外，您可以通过网际无人值守方式在多个系统上安装 Server Administrator。Server Administrator 安装程序提供安装脚本和 RPM 软件包以安装、卸载受管系统上的 Server Administrator 和其他受管系统软件组件。有关更多信息，请参阅 **dell.com/opemanagemanuals** 上的 *Dell EMC Server Administrator 安装指南*和*管理站软件安装指南*。

注: 如果通过 *Dell EMC Systems Management Tools and Documentation* 软件安装开源软件包，则会将相应的许可证文件自动复制到系统中。当您移除这些软件包时，相应的许可证文件也会被移除。

注: 如果有模块化系统，则在机箱中所装的每个服务器模块上安装 Server Administrator。

本发行版中的新增功能

OpenManage Server Administrator 的发行亮点：

- 支持以下操作系统：
  - Red Hat Enterprise Linux 7.5
  - VMware ESXi 6.7
  - **注: Server Administrator 和 Storage Management 的 Citrix Xenserver 操作系统支持已降低。**
- 支持以下浏览器：
  - Internet Explorer - 10、11
  - Google Chrome - 62、63
  - Safari - 10.x
  - Mozilla Firefox - 57、58
- 支持的网卡：
  - Harbor 通道 - Intel (R) 以太网 25G 2P XXV710 适配器（25GBE PCIe 适配器）
  - QLogic Dundee - LP - QLogic 4x10GE QL41164HxRJ CNA
  - QLogic Dundee - FH - QLogic 4x10GE QL41164HxRJ CNA
  - QLogic Delray – FH - QLogic 4x10GE QL41164HFCU CNA
  - Emulex LightPulse LPE1200x FC8 HBA
  - Emulex LightPulse LPe31000-M6-D 单端口 16Gb 光纤信道适配器
  - Emulex LightPulse LPe31002-M6-D 双端口 16Gb 光纤信道适配器
  - Emulex LightPulse LPe32002-M2-D 双端口 32Gb 光纤信道适配器

注: 此版本仅支持新 Dell EMC MX 平台 - PowerEdge MX740c、MX840c 服务器和 MX5016s 存储底座。有关支持的操作系统和戴尔服务器列表，请参阅 dell.com/openmanagemanuals 上所需版本的 OpenManage 软件的 *Dell EMC OpenManage 软件支持值表*。

更新各个系统组件

要更新各个系统组件，请使用特定于组件的 Dell 更新包。使用 *Dell Server Update Utility* DVD 查看完整的版本报告以及更新整个系统。Server Update Utility (SUU) 可识别并应用系统的必需更新。SUU 也可以从 **support.dell.com** 下载。

注: 有关获取并使用 Server Update Utility (SUU) 更新系统或查看存储库中所列全部系统的可用更新的更多信息，请参阅位于 dell.com/openmanagemanuals 上的 *Dell Server Update Utility User's Guide*（Dell Server Update Utility 用户指南）。

存储管理服务

Storage Management Service 以集成图形视图方式向用户提供存储管理信息。

注: 有关 Storage Management Service 的更多信息，请参阅 dell.com/openmanagemanuals 上的 *Dell EMC Server Administrator Storage Management 用户指南*。

Instrumentation Service

Instrumentation Service 使您可以快速查看由行业标准系统管理代理收集的详细故障和性能信息，并且允许对受监测系统进行远程管理（包括关闭系统、启动和安全保护）。

Remote Access Controller

Remote Access Controller 为配备有 Baseboard Management Controller (BMC)/Integrated Dell Remote Access Controller (iDRAC) 解决方案的系统提供完整的远程系统管理解决方案。Remote Access Controller 使您可以远程访问不能运行的系统，使其尽快启动并运行。

Remote Access Controller 还可在系统停机时提供警报通知，并允许您远程重新启动系统。此外，Remote Access Controller 还将记录系统故障的可能原因并保存最近一次的崩溃屏幕。

日志

Server Administrator 将显示以下项的日志：向（由）系统发出的命令、受监测的硬件事件和系统警报。您可以在主页上查看、打印日志，或将其保存为报告，并将其通过电子邮件发送给指定的服务联系人。

系统管理标准可用性

Server Administrator 支持下列系统管理协议：

- 安全超文本传输协议 (HTTPS)
- 公用信息模型 (CIM)
- 简单网络管理协议 (SNMP)

如果系统支持 SNMP，则必须在操作系统上安装和启用该服务。如果操作系统提供了 SNMP 服务，Server Administrator 安装程序会安装 SNMP 的支持代理程序。

所有操作系统都支持 HTTPS。对 CIM 和 SNMP 的支持取决于操作系统，在某些情况下还取决于操作系统版本。

注: 有关涉及 SNMP 安全问题的信息，请参阅 Server Administrator 发行说明文件（与 Server Administrator 应用程序打包在一起），或者位于 dell.com/openmanagemanuals 上。必须从操作系统的主要 SNMP 代理程序应用更新，以确保 SNMP 子代理程序的安全。

在支持的操作系统上的可用性

在支持的 Microsoft Windows 操作系统上，Server Administrator 支持两种系统管理标准：CIM/Windows 管理工具 (WMI) 和 SNMP，而在支持的 Red Hat Enterprise Linux 及 SUSE Linux Enterprise Server 操作系统上，Server Administrator 支持 SNMP 系统管理标准。

Server Administrator 显著提升了这些系统管理标准的安全性。所有属性集操作（例如，更改资产标签的值）必须在已登录并拥有所需权限的情况下通过 Dell EMC OpenManage Essentials 来执行。

下表显示了每个支持的操作系统可用的系统管理标准。

表. 1: 系统管理标准可用性

操作系统	SNMP	CIM
Windows Server 2012 R2 系列	可通过操作系统安装介质获得	始终安装
Red Hat Enterprise Linux	可通过操作系统安装介质中的 net-snmp 软件包获得	不可用
SUSE Linux Enterprise Server	可通过操作系统安装介质中的 net-snmp 软件包获得	不可用
VMWare ESXi	可获得 SNMP 陷阱支持 **注: 尽管 ESXi 支持 SNMP 陷阱，但不支持通过 SNMP 获得硬件资源清册。**	可用

Server Administrator 主页

Server Administrator 主页提供了易于设置且易于使用的基于 Web 浏览器的系统管理任务，可通过 LAN、拨号服务或无线网络从管理系统或从远程主机执行这些任务。已在受管系统上安装并配置 Systems Management Server Administrator 连接服务 (DSM SA 连接服

务）时，您可以从具有受支持的 Web 浏览器和连接的任何系统执行远程管理功能。此外，Server Administrator 主页还提供了详尽的上下文相关联机帮助。

您可能需要的其他说明文件

除了本指南以外，您还可以访问 **dell.com/softwaresecuritymanuals** 上的以下指南。

- *Dell EMC Systems Software Support Matrix*（Dell EMC 系统软件支持值表）提供有关各种系统、这些系统支持的操作系统以及可以安装在这些系统上的组件的信息。
- *Dell EMC OpenManage Server Administrator Installation Guide*（Dell EMC OpenManage Server Administrator 安装指南）包含帮助安装 Dell EMC OpenManage Server Administrator 的说明。
- *Dell EMC OpenManage Management Station Software Installation Guide*（Dell EMC OpenManage 管理站软件安装指南）包含可帮助您安装 Dell EMC OpenManage 管理站软件的说明。
- *Dell EMC OpenManage SNMP Reference Guide*（Dell EMC OpenManage SNMP 参考指南）介绍了简单网络管理协议 (SNMP) 管理信息库 (MIB)。
- *Dell EMC OpenManage Server Administrator CIM Reference Guide*（Dell EMC OpenManage Server Administrator CIM 参考指南）介绍了公用信息模型 (CIM) 提供程序，它是标准管理对象格式 (MOF) 文件的扩展。
- *Dell EMC Messages Reference Guide*（Dell EMC 消息参考指南）列出了 Server Administrator 主页警报日志或操作系统事件查看器中显示的消息。
- *Dell EMC OpenManage Server Administrator Command Line Interface Guide*（Dell EMC OpenManage Server Administrator 命令行界面指南）介绍了 Server Administrator 的完整命令行界面。
- *Dell Remote Access Controller User's Guide*（Dell Remote Access Controller 用户指南）提供了有关使用 RACADM 命令行公用程序配置 DRAC 的完整信息。
- *Dell EMC Chassis Management Controller User's Guide*（Dell EMC Chassis Management Controller 用户指南）提供了有关使用控制器（管理含有系统的机箱中的所有模块）的信息。
- *Command Line Reference Guide for iDRAC 6 and CMC*（iDRAC 6 和 CMC 命令行参考指南）提供了关于 iDRAC6 和 CMC 的 RACADM 子命令、支持的界面、属性数据库组和对象定义的信息。
- *Integrated Dell Remote Access Controller 7 (iDRAC7) User's Guide*（Integrated Dell Remote Access Controller 7 (iDRAC7) 用户指南）介绍如何配置 iDRAC7 并将其用于 12G 机架式、塔式和刀片式服务器，以通过网络来远程管理和监测系统及其共享资源。
- *Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers User Guide（集成的 Dell 远程访问控制器 6 (iDRAC6) Enterprise 刀片服务器版用户指南）*提供了有关配置和使用 iDRAC6 11G 刀片服务器版通过网络远程管理和监测系统及其共享资源的信息。
- *Integrated Dell Remote Access Controller 6 (iDRAC6) User Guide*（集成的 Dell 远程访问控制器 6 (iDRAC6) 用户指南）提供了有关配置和使用 iDRAC6 11G 塔式和机架式服务器版，通过网络来远程管理和监测系统及其共享资源的完整信息。
- *Dell Online Diagnostics User's Guide*（Dell Online Diagnostics 用户指南）提供了有关在系统中安装并使用联机诊断程序的完整信息。
- *Dell OpenManage Baseboard Management Controller Utilities User's Guide*（Dell OpenManage Baseboard Management Controller 公用程序用户指南），提供了有关使用 Server Administrator 来配置和管理系统的 BMC 的更多信息。
- *Dell EMC OpenManage Server Administrator Storage Management User's Guide*（Dell EMC OpenManage Server Administrator 存储管理用户指南）为配置和管理与系统连接的本地和远程存储设备提供了全面的参考指南。
- *Dell Remote Access Controller Racadm User's Guide*（Dell Remote Access Controller Racadm 用户指南）提供了有关使用 racadm 命令行公用程序的信息。
- *Dell Remote Access Controller User's Guide*（Dell Remote Access Controller 用户指南）提供了有关安装和配置 DRAC 控制器以及使用 DRAC 远程访问不能运行的系统的完整信息。
- *Dell Update Packages User's Guide*（Dell Update Packages 用户指南）提供了有关作为系统更新战略的一部分获取和使用 Dell Update Packages 的信息。
- *Dell EMC OpenManage Server Update Utility User's Guide*（Dell EMC OpenManage Server Update Utility 用户指南）介绍了如何获取并使用 Server Update Utility (SUU) 更新系统或查看存储库中所列系统的可用更新。
- *Dell Management Console User's Guide*（Dell Management Console 用户指南）提供了有关安装、配置和使用 Dell Management Console 的信息。
- *Dell Lifecycle Controller User Guide*（Dell Lifecycle Controller 用户指南）提供了关于设置和使用 Unified Server Configurator 的信息，以便在系统的整个生命周期中执行各项系统和存储管理任务。
- *Dell License Manager User's Guide*（Dell License Manager 用户指南）提供有关管理 12G 服务器的组件服务器许可证的信息。
- *词汇表*提供本说明文件中所使用术语的相关信息。

访问 Dell EMC 支持站点上的文档

您可以使用以下链接访问所需的文档：

- Dell EMC 企业系统管理文档 — www.dell.com/SoftwareSecurityManuals
- Dell EMC OpenManage 文档 — www.dell.com/OpenManageManuals
- Dell EMC 远程企业系统管理文档 — www.dell.com/esmmanuals
- iDRAC 和 Dell EMC 生命周期控制器文档 — www.dell.com/idracmanuals
- Dell EMC OpenManage 连接企业系统管理文档 — www.dell.com/OMConnectionsEnterpriseSystemsManagement
- Dell EMC 可维护性工具文档 — www.dell.com/ServiceabilityTools
- a 转至 www.dell.com/Support/Home。

  b 单击**从所有产品中选择。**

  c 从**所有产品**部分，单击**软件和安全**，然后单击以下部分中的所需链接：
  - **企业系统管理**
  - **远程企业系统管理**
  - **维护工具**
  - **Dell 客户端命令套件**
  - **Connections 客户端系统管理**

  d 要查看文档，请单击所需的产品版本。
- 使用搜索引擎：

  – 在搜索框中键入文档的名称和版本。

获得技术协助

如果在任何时候您对本指南中的步骤不明白，或者如果您的产品未按预期运行，则还有不同类型的帮助工具可供利用。有关这些帮助工具的更多信息，请参阅您系统的 *Hardware Owner's Manual*（硬件用户手册）中的 **获得帮助**。

此外，还可以充分利用“企业培训和认证”服务；有关更多信息，请访问 dell.com/training。此项服务可能并不是在所有地区都提供。

联系 Dell EMC

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

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

访问 **Dell.com/contactdell**。

2

设置和管理

Server Administrator 通过基于角色的访问控制 (RBAC)、验证和加密为基于 Web 的界面和命令行界面提供安全保护。

主题：

基于角色的访问控制

RBAC 通过确定可以由具有特定角色的人员执行的操作来管理安全性。会给每位用户分配一个或多个角色，并给每个角色分配一个或多个授予具有该角色的用户权限。通过 RBAC，安全管理紧密对应组织结构。

用户权限

Server Administrator 根据分配给用户的组权限赋予用户不同的访问权限。四种用户权限级别为：用户、高级用户、管理员和提升管理员。

表. 2: 用户权限

用户权限级别	访问类型		说明
	查看	管理	
用户	是	否	*用户*可以查看大多数信息。
高级用户	是	是	*高级用户*可以设置警告阈值，并配置出现警告或故障事件时采取的警报操作。
管理员	是	是	*管理员*可以配置和执行关机操作，配置在操作系统不响应时系统的自动恢复操作，以及清除硬件、事件和命令日志。管理员还可以配置系统以发送电子邮件。
提升管理员（仅限于 Linux）	是	是	*提升管理员*可以查看和管理信息。

访问 Server Administrator 服务的权限级别

下表总结了哪些用户级别有权访问和管理 Server Administrator 服务。

Server Administrator 赋予以用户权限登录的用户只读访问权限；赋予以高级用户权限登录的用户读写访问权限；赋予以*管理员*和*提升管理员*权限登录的用户读、写和管理员访问权限。

表. 3: 所需权限以管理 Server Administrator 服务

服务	所需用户权限级别	
	查看	管理
仪器	用户、高级用户、管理员、提升管理员	高级用户、管理员、提升管理员
远程访问	用户、高级用户、管理员、提升管理员	管理员、提升管理员
存储管理	用户、高级用户、管理员、提升管理员	管理员、提升管理员

验证

Server Administrator 验证方案确保可以将正确的访问类型分配给正确的用户权限。另外，当调用命令行界面 (CLI) 时，Server Administrator 验证方案将验证包含当前运行进程的环境。该验证方案确保可以正确验证所有 Server Administrator 功能（无论通过 Server Administrator 主页还是通过 CLI 进行访问）。

Microsoft Windows 验证

在支持的 Microsoft Windows 操作系统上，Server Administrator 使用集成 Windows 验证（旧称 NTLM）进行验证。该验证系统使得 Server Administrator 的安全保护可以纳入用户网络的整体安全保护方案中。

Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 验证

在支持的 Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统上，Server Administrator 使用基于可插拔验证模块 (PAM) 库的各种验证方法。用户可以使用不同的帐户管理协议（比如 LDAP、NIS、Kerberos 和 Winbind）从本地或远程登录 Server Administrator。

VMware ESXi Server 验证

ESXi Server 使用 vSphere/VI 客户端或软件开发工具包 (SDK) 来验证访问 ESXi 主机的用户。ESXi 的默认安装将本地密码数据库用于验证。与 Server Administrator 的 ESXi 验证事务也会导致与 **vmware-hostd** 进程交互。为了确保验证在您的站点中能够高效工作，请执行诸如以下的基本任务：设置用户、组、权限和角色；配置用户属性；添加您自己的证书；以及确定您是否要使用 SSL 等。

注: 在运行 VMware ESXi Server 操作系统的系统上，要登录 Server Administrator，所有用户都需要“管理员”权限。有关分配角色的信息，请参阅 VMware 说明文件。

加密

通过使用安全套接字层 (SSL) 技术的安全 HTTPS 连接访问 Server Administrator 可以确保并保护正在管理的系统的身份。用户访问 **Server Administrator** 主页时，支持的 Microsoft Windows、Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统使用 Java 安全套接字扩展 (JSSE) 保护用户凭据和其他通过套接字连接传输的机密数据。

分配用户权限

为了确保重要系统组件的安全，在安装 OpenManage 软件之前给所有 OpenManage 软件用户分配用户权限。新用户可以使用其操作系统用户权限登录 OpenManage 软件。

小心: 要保护对重要系统组件的访问，请为可以访问 OpenManage 软件的每个用户帐户分配密码。

小心: 禁用支持 Windows 操作系统的来宾帐户以保护对重要系统组件的访问。请考虑重命名来宾帐户，以使远程脚本无法通过默认来宾帐户名称启用这些帐户。

注: 有关为每个所支持操作系统分配用户权限的说明，请参阅您的操作系统说明文件。

注: 要向 OpenManage 软件添加用户，将新用户添加到操作系统中。不需要从 OpenManage 软件中创建新用户。

向 Windows 操作系统上的域添加用户

注: 要执行这些步骤，系统中必须已安装 Microsoft Active Directory。有关使用 Active Directory 的更多信息，请参阅使用 Active Directory 登录。

1 导航到**控制面板** > **管理工具** > **Active Directory 用户和计算机**。
2 在控制台树中，右键单击**用户**，或者右键单击要在其中添加新用户的容器，然后指向**新建** > **用户**。
3 在对话框中键入相应的用户名信息并单击**下一步**。
4 单击**下一步**，然后单击**完成**。
5 双击表示您刚创建的用户的图标。
6 单击**成员**选项卡。
7 单击**添加**。
8 选择相应的组并单击**添加**。
9 单击**确定**，然后再次单击**确定**。

注: 新用户可使用为其组和域分配的用户权限登录至 OpenManage。

在支持的 Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统中创建 Server Administrator 用户

“管理员”访问权限将分配给以根用户身份登录的用户。有关创建用户和用户组的信息，请参阅操作系统说明文件。

注: 要执行这些步骤，必须以根或等同的用户身份登录。

注: 要执行这些步骤，系统中必须已安装 useradd 公用程序。

相关链接

- 创建具有用户权限的用户
- 创建具有高级用户权限的用户

创建具有用户权限的用户

1 通过命令行运行以下命令： `useradd -d <home-directory> -g <group> <username>`，其中 `<group>` 不是 `root`。

注: 如果 <group> 不存在，则使用 groupadd 命令创建它。

2 键入 `passwd <username>` 并按 <Enter>。
3 屏幕出现提示时，输入新用户的密码。

注: 为可以访问 Server Administrator 的每个用户帐户设定密码，以保护对重要系统组件的访问。

现在，新用户可以使用“用户”组权限登录至 Server Administrator。

创建具有高级用户权限的用户

1 通过命令行运行以下命令：`useradd -d <home-directory> -g <group> <username>`

注: 将 root 设置为主要组。

2 键入 `passwd <username>` 并按 <Enter>。

3 屏幕出现提示时，输入新用户的密码。

注: 为可以访问 Server Administrator 的每个用户帐户设定密码，以保护对重要系统组件的访问。

现在，新用户可以使用“高级用户”组权限登录至 Server Administrator。

在 Linux 操作系统上编辑 Server Administrator 用户权限

注: 您必须以根或等同的用户身份登录。

1 打开位于 /opt/dell/srvadmin/etc/omarolemap 的 **omarolemap** 文件。

2 在文件中添加以下内容： `<User_Name>[Tab]<Host_Name>[Tab]<Rights>`

下表列出了向 **omarolemap** 添加角色定义的说明

表. 4: 在 Server Administrator 中添加角色定义的说明

<User_Name>	<Host_Name>	<Rights>
用户名	主机名	管理员
(+) 组名	域	用户
通配符 (*)	通配符 (*)	用户

`[Tab] = \t (tab character)`

下表列出了向 **omarolemap** 文件添加角色定义的示例。

表. 5: 在 Server Administrator 中添加角色定义的示例

<User_Name>	<Host_Name>	<Rights>
Bob	Ahost	高级用户
+根	Bhost	管理员
+根	Chost	管理员
Bob	*.aus.amer.com	高级用户
Mike	192.168.2.3	高级用户

3 保存更改，然后关闭文件。

使用 omarolemap 文件的最佳做法

下面列出了使用 **omarolemap** 文件的最佳做法：

- 请勿删除 **omarolemap** 文件中的以下默认条目。

表. 6: omarolemap 文件的最佳做法

root	管理员
+根	* Poweruser
*	* User

- 请勿更改 **omarolemap** 文件权限或文件格式。
- 不要为 *<Host_Name>* 使用环回地址，例如：localhost 或 127.0.0.1。
- 连接服务重新启动后如果 **omarolemap** 文件的更改没有生效，请参阅命令日志查找错误。
- 将 **omarolemap** 文件从一台计算机复制到另一台计算机后，需要重新检查文件权限和文件的条目。
- 在 *Group Name* 前加上 *+*。
- 在下列情况中，Server Administrator 使用默认操作系统用户权限：
  - 用户在 **omarolemap** 文件中被降级
  - 存在具有相同 的重复用户名条目或用户组条目 *<Host_Name>*
- 您还可以使用 `Space` 作为列分隔符，而不使用 `[Tab]`。

为 VMware ESXi 6.*X* 创建 Server Administrator 用户

要向“用户”表添加用户，请执行以下操作：

1. 使用 vSphere 客户端登录到主机。
2. 单击**用户和组**选项卡，然后单击**用户**。
3. 右键单击“用户”表中的任意位置，然后单击**添加**以打开**添加新用户**对话框。
4. 输入登录、用户名、数字用户 ID (UID) 及密码；指定用户名和 UID 是可选操作。如果不指定 UID，vSphere 客户端会分配下一个可用的 UID。
5. 要使用户能够通过命令 Shell 访问 ESXi 主机，请选中**为此用户授予 Shell 访问权限**。只通过 vSphere 客户端访问主机的用户不需要 Shell 访问权限。
6. 要将用户添加到某个组，请从**组**下拉菜单中选择组名称并单击**添加**。
7. 单击**确定**。

在支持的 Windows 操作系统中禁用来宾和匿名帐户

注: 您必须以管理员权限登录。

1. 打开**计算机管理**窗口。
2. 在控制台树中，展开**本地用户和组**并单击**用户**。
3. 双击**来宾**或 **IUSR_system** name 用户帐户，查看这些用户的属性，或右键单击**来宾**或 **IUSR_***system name* 用户帐户，然后选择**属性**。
4. 选择**帐户已禁用**，然后单击**确定**。
   用户名上将显示一个带 X 的红圈，表示该帐户已被禁用。

配置 SNMP 代理程序

在所有支持的操作系统上，Server Administrator 均支持简单网络管理协议（SNMP，一种系统管理标准）。能否安装 SNMP 支持，将视您的操作系统和操作系统安装的方式而定。在大多数情况下，SNMP 作为操作系统的一部分进行安装。安装 Server Administrator 之前，需要先安装所支持的系统管理协议标准（例如 SNMP）。

您可以配置 SNMP 代理程序以更改团体名称，并将陷阱发送给管理站。要配置 SNMP 代理程序以正确地与管理应用程序（例如 OpenManage Essentials）进行交互，请执行以下各节中说明的步骤。

注：默认 SNMP 代理程序配置通常包括 SNMP 团体名称，比如“公共”。出于安全考虑，必须重命名默认的 SNMP 团体名称。有关重命名 SNMP 团体名称的信息，请参阅更改 SNMP 团体名称。

注：为了使 OpenManage Essentials 可以从运行 Server Administrator 的系统检索管理信息，OpenManage Essentials 所使用的团体名称必须与运行 Server Administrator 的系统上的团体名称匹配。为了使 OpenManage Essentials 可以在运行 Server Administrator 的系统上修改信息或执行操作，OpenManage Essentials 所使用的团体名称必须与运行 Server Administrator 的系统上允许 Set 操作的团体名称匹配。为了使 OpenManage Essentials 可以从运行 Server Administrator 的系统上接收陷阱（异步事件通知），必须将运行 Server Administrator 的系统配置为将陷阱发送至运行 OpenManage Essentials 的系统。

以下步骤提供了在每个支持的操作系统上配置 SNMP 代理程序的逐步说明：

- 为运行支持的 Windows 操作系统的系统中配置 SNMP 代理程序
- 在运行支持的 Red Hat Enterprise Linux 的系统上配置 SNMP 代理程序
- 在运行支持的 SUSE Linux Enterprise Server 的系统中配置 SNMP 代理程序
- 在运行受支持的 VMware ESXi 5.X 和 ESXi 6.X 操作系统的系统上配置 SNMP 代理程序
- 在运行支持的 Ubuntu Server 的系统中配置 SNMP 代理程序

在运行支持的 Windows 操作系统的系统上配置 SNMP 代理程序

Server Administrator 使用 Windows SNMP 代理程序提供的 SNMP 服务。您可以配置 SNMP 代理程序以更改团体名称，并将陷阱发送给管理站。要配置 SNMP 代理程序以正确地与管理应用程序（例如 OpenManage Essentials）进行交互，请执行以下各节中说明的步骤。

注：有关 SNMP 配置的附加详细信息，请参阅操作系统说明文件。

更改 SNMP 团体名称

注：您不能从 Server Administrator 设置 SNMP 团体名称。请使用操作系统 SNMP 工具设置团体名称。

配置 SNMP 团体名称可确定哪些系统能够通过 SNMP 管理您的系统。管理应用程序使用的 SNMP 团体名称必须与在运行 Server Administrator 的系统上所配置的 SNMP 团体名称匹配，以便管理应用程序可以从 Server Administrator 检索管理信息。

1 打开**计算机管理**窗口。
2 如果有必要，请展开窗口中的**计算机管理**图标。
3 展开**服务和应用程序**图标并单击**服务**。
4 向下滚动服务列表，直至找到 **SNMP 服务**，右键单击 **SNMP 服务**，然后单击**属性**。
SNMP 服务属性窗口处于禁用状态。
5 单击**安全**选项卡以添加或编辑团体名称。
要添加团体名称，请执行以下操作：

a 在**接受的团体名称**列表下单击**添加**。
将显示 **SNMP 服务配置**窗口。
b 在**团体名称**框中键入系统（能够管理您的系统）的团体名称（默认设置为 public），然后单击**添加**。
将显示 **SNMP 服务属性**窗口。

要编辑团体名称，请执行以下操作：

a 在**接受的团体名称**列表中选择一个团体名称，然后单击**编辑**。
将显示 **SNMP 服务配置**窗口。
b 在**团体名称**框中编辑团体名称，然后单击**确定**。

将显示 **SNMP 服务属性**窗口。

6 单击**确定**以保存更改。

配置您的系统以向管理站发送 SNMP 陷阱

Server Administrator 生成 SNMP 陷阱，以响应传感器状况和其他被监测参数的更改。您必须在运行 Server Administrator 的系统上配置一个或多个陷阱目标才能向管理站发送 SNMP 陷阱。

1 打开**计算机管理**窗口。

2 如果需要，请展开窗口中的**计算机管理**图标。

3 展开**服务和应用程序**图标，然后单击**服务**。

4 向下滚动服务列表，直至找到 **SNMP 服务**。右键单击 **SNMP 服务**，然后单击**属性**。

随即显示 **SNMP 服务属性**窗口。

5 单击**陷阱**选项卡以添加陷阱团体，或添加陷阱团体的陷阱目标。

a 要添加陷阱团体，请在**团体名称**框中键入团体名称，然后单击**团体名称**框旁边的**添加到列表**。

b 要添加陷阱团体的陷阱目标，请从**团体名称**下拉框中选择团体名称，然后单击**陷阱目标**框下的**添加**。

此时将显示 **SNMP 服务配置**窗口。

c 在**主机名称，IP 或 IPX 地址框**中，键入陷阱目标，**添加**。

随即显示 **SNMP 服务属性**窗口。

6 单击**确定**保存更改。

在运行支持的 Red Hat Enterprise Linux 的系统上配置 SNMP 代理程序

Server Administrator 使用 **net-snmp** SNMP 代理程序提供的 SNMP 服务。您可以配置 SNMP 代理程序以更改团体名称，并将陷阱发送给管理站。要配置 SNMP 代理程序以正确地与管理应用程序（例如 OpenManage Essentials）进行交互，请执行以下各节中说明的步骤。

注: 有关 SNMP 配置的附加详细信息，请参阅操作系统说明文件。

SNMP 代理访问控制配置

由 Server Administrator 实施的管理信息库 (MIB) 分支由对象标识符 (OID) 1.3.6.1.4.1.674 标识。管理应用程序必须能够访问 MIB 树分支，从而能管理运行 Server Administrator 的系统。

对于 Red Hat Enterprise Linux 和 VMware ESXi 操作系统，默认 SNMP 代理配置仅提供 MIB 树的 MIB-II *系统*分支（由 1.3.6.1.2.1.1 OID 标识）的公*共*团体的只读权限。此配置不允许管理应用程序检索或更改 Server Administrator 或 MIB-II *系统*分支之外的其他系统管理信息。

Server Administrator SNMP 代理安装操作

如果 Server Administrator 在安装期间检测到默认 SNMP 配置，它将尝试修改 SNMP 代理程序配置，以给予 public 团体对整个 MIB 树的只读访问权限。Server Administrator 通过以下方式修改 SNMP 代理程序配置文件 **/etc/snmp/snmpd.conf**：

- 通过添加以下行（如果它不存在）创建整个 MIB 树的视图：`view all included`
- 修改默认访问权限行，给予 public 团体整个 MIB 树的只读访问权限。Server Administrator 会查找以下行：`access notConfigGroup "" any noauth exact systemview none none`
- 如果 Server Administrator 找到上述行，它会将其修改为：`access notConfigGroup "" any noauth exact all none none`

注: 为确保 Server Administrator 能够修改 SNMP 代理配置以提供对系统管理数据的适当访问权限，建议在安装 Server Administrator 之后再对任何其他 SNMP 代理程序配置进行修改。

Server Administrator SNMP 使用 SNMP 多路复用 (SMUX) 协议与 SNMP 代理程序进行通信。当 Server Administrator SNMP 连接至 SNMP 代理程序时，它发送一个对象标识符至 SNMP 代理程序，以将自己标识为 SMUX 对等体。由于此对象标识符必须使用 SNMP 代理程序配置，因此，Server Administrator 在安装过程中将以下行（如果不存在）添加至 SNMP 代理程序配置文件 **/etc/snmp/snmpd.conf**：

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

更改 SNMP 团体名称

配置 SNMP 团体名称可确定哪些系统能够通过 SNMP 管理您的系统。管理应用程序使用的 SNMP 团体名称必须与运行 Server Administrator 的系统上所配置的 SNMP 团体名称匹配，以便管理应用程序可以从 Server Administrator 检索管理信息。
要更改用于从运行 Server Administrator 的系统检索管理信息的 SNMP 团体名称，请执行以下操作：

1 打开 SNMP 代理程序配置文件 **/etc/snmp/snmpd.conf**。
2 查找以下行：`com2sec publicsec default public` 或 `com2sec notConfigUser default public`.

注: 对于 IPv6，查找行 `com2sec6 notConfigUser default public`。此外，在文件中添加文本 `agentaddress udp6:161`。

3 编辑此行，将 `public` 替换为新的 SNMP 团体名称。编辑后，新行应为：`com2sec publicsec default community_name` 或 `com2sec notConfigUser default community_name`.
4 要启用 SNMP 配置更改，请通过键入以下命令重新启动 SNMP 代理程序：`systemctl restart snmpd` .

配置您的系统以向管理站发送陷阱

Server Administrator 生成 SNMP 陷阱，以响应传感器状况和其他受监测参数的变化。必须在运行 Server Administrator 的系统上配置一个或多个陷阱目标，才能向管理站发送 SNMP 陷阱。
要配置运行 Server Administrator 的系统以发送陷阱到管理站，编辑 SNMP 代理程序配置文件 **/etc/snmp/snmpd.conf**，并执行以下步骤：

1 向文件添加以下行：`trapsink IP_address community_name`，其中 `IP_address` 是管理站的 IP 地址，`community_name` 是 SNMP 团体名称。
2 要启用 SNMP 配置更改，请通过键入以下命令重新启动 SNMP 代理程序：`systemctl restart snmpd` 。

在运行支持的 SUSE Linux Enterprise Server 的系统中配置 SNMP 代理

Server Administrator 使用 net-snmp 代理程序提供的 SNMP 服务。您可以配置 SNMP 代理程序以从远程主机启用 SNMP 访问，更改团体名称，启用设置操作，并将陷阱发送给管理站。要配置 SNMP 代理程序以正确地与管理应用程序（例如 OpenManage Essentials）进行交互，请执行以下各节中说明的步骤。

注: 有关 SNMP 配置的附加详细信息，请参阅操作系统说明文件。

Sever Administrator SNMP 安装操作

Server Administrator SNMP 使用 SMUX 协议与 SNMP 代理程序进行通信。当 Server Administrator SNMP 连接至 SNMP 代理程序时，它发送一个对象标识符至 SNMP 代理程序，以将自己标识为 SMUX 对等体。此对象标识符必须使用 SNMP 代理程序配置，因此，Server Administrator 在安装过程中将以下行（如果不存在）添加至 SNMP 代理程序配置文件 **/etc/snmp/snmpd.conf**：

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

从远程主机启用 SNMP 访问

SUSE Linux Enterprise Server 操作系统中的默认 SNMP 代理程序配置对 public 团体只给予从本地主机访问整个 MIB 树的只读访问权限。此配置不允许在其他主机上运行的 SNMP 管理应用程序（例如 OpenManage Essentials）正确查找和管理 Server Administrator 系统。如果 Server Administrator 在安装期间检测到此配置，它将消息记录到操作系统日志文件 **/var/log/messages**，以表明 SNMP 访问权限仅限于本地主机。如果计划使用 SNMP 管理应用程序从远程主机管理系统，则必须配置 SNMP 代理程序以启用从远程主机进行 SNMP 访问。

注: 出于安全原因，建议在可能的情况下将 SNMP 访问限制在特定的远程主机。

要启用从特定远程主机对运行 Server Administrator 的系统的 SNMP 访问，请编辑 SNMP 代理程序配置文件 **/etc/snmp/snmpd.conf**，并执行以下步骤：

1 查找以下行：`rocommunity public 127.0.0.1`。

2 编辑或复制该行，以将 127.0.0.1 替换为该远程主机 IP 地址。编辑后，新行应为：`rocommunity public IP_address`。

注: 您可以通过为各个远程主机添加 `rocommunity` 指令来启用从多个特定远程主机进行 SNMP 访问。

3 要启用 SNMP 配置更改，请通过键入以下命令重新启动 SNMP 代理程序：`systemctl restart snmpd` 。

更改 SNMP 团体名称

配置 SNMP 团体名称可确定哪些管理站能够通过 SNMP 管理您的系统。管理应用程序使用的 SNMP 团体名称必须与运行 Server Administrator 的系统上所配置的 SNMP 团体名称匹配，以便管理应用程序可以从 Server Administrator 检索管理信息。

要更改用于从运行 Server Administrator 的系统检索管理信息的默认 SNMP 团体名称，请执行以下操作：

1 打开 SNMP 代理程序配置文件 **/etc/snmp/snmpd.conf**。

2 查找以下行：`rocommunity public 127.0.0.1.`

3 编辑此行，将 `public` 替换为新的 SNMP 团体名称。编辑后，新行应为：`rocommunity community_name 127.0.0.1.`

4 要启用 SNMP 配置更改，请通过键入以下命令重新启动 SNMP 代理程序：**systemctl restart snmpd**。

在运行支持的 Ubuntu Server 的系统中配置 SNMP 代理程序

Server Administrator 使用 net-snmp 代理程序提供的 SNMP 服务。您可以配置 SNMP 代理程序以从远程主机启用 SNMP 访问，更改团体名称，并将陷阱发送给管理站。要配置 SNMP 代理程序以正确地与管理应用程序（例如 OpenManage Essentials）进行交互，请执行以下各节中说明的步骤。

注: 有关 SNMP 配置的附加详细信息，请参阅操作系统说明文件。

Sever Administrator SNMP 安装操作

Server Administrator SNMP 使用 SMUX 协议与 SNMP 代理程序进行通信。当 Server Administrator SNMP 连接至 SNMP 代理程序时，它发送一个对象标识符至 SNMP 代理程序，以将自己标识为 SMUX 对等体。要支持 SMUX，对象标识符必须使用 SNMP 代理程序进行配置。要让 Server Administrator 使用 SMUX 协议，您需要按照以下步骤操作，以启用 SNMP 代理程序配置文件。

- 打开 SNMP 代理程序配置文件 **./etc/default/snmpd**。
- 配置文件中可用的默认选项为：**SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux,mteTrigger,mteTriggerConf -p /run/snmpd.pid'**
- 使用上述默认配置，便可禁用 SMUX 模块。
- 要支持 snmpd 以支持 SMUX，将配置更改为：**SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -p /run/snmpd.pid'**

在 SNMP 代理程序配置文件中添加 **./etc/snmp/snmpd.conf**

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

- 要启用 SNMP 配置更改，请通过使用以下命令重新启动 SNMP 代理程序：**systemctl restart snmpd。**

更改 SNMP 团体名称

配置 SNMP 团体名称可确定哪些管理站能够通过 SNMP 管理您的系统。管理应用程序使用的 SNMP 团体名称必须与运行 Server Administrator 的系统上所配置的 SNMP 团体名称匹配，以便管理应用程序可以从 Server Administrator 检索管理信息。

要更改用于从运行 Server Administrator 的系统检索管理信息的默认 SNMP 团体名称，请执行以下操作：

1. 打开 SNMP 代理程序配置文件 **/etc/snmp/snmpd.conf。**
2. 查找以下行：`rocommunity public 127.0.0.1.`
3. 编辑此行，将 `public` 替换为新的 SNMP 团体名称。编辑后，新行应为：`rocommunity community_name 127.0.0.1.`
4. 要启用 SNMP 配置更改，请通过键入以下命令重新启动 SNMP 代理程序：**systemctl restart snmpd。**

在运行受支持的 VMware ESXi 6.X 操作系统的系统上配置 SNMP 代理程序

Server Administrator 支持 Vmware ESXi 6.X 上的 SNMP 陷阱。如果仅存在单机许可证，则 VMware ESXi 操作系统上的 SNMP 配置会失败。Server Administrator 不支持 VMWare ESXi 6.X 上的 SNMP Get 和 Set 操作，因为所需的 SNMP 支持不可用。通过 VMware vSphere 命令行界面 (CLI)，可将运行 VMware ESXi 6.X 的系统配置为向管理站发送 SNMP 陷阱。

注: 有关使用 VMware vSphere CLI 的更多信息，请参阅 vmware.com/support。

配置您的系统以向管理站发送陷阱

Server Administrator 生成 SNMP 陷阱，以响应传感器状况的更改和其他受监测参数的更改。您必须在运行 Server Administrator 的系统上为将要发送至管理站的 SNMP 陷阱配置一个或多个陷阱目标。

要配置运行 Server Administrator 的 ESXi 系统将陷阱发送到管理站：

1. 安装 VMware vSphere CLI。
2. 在安装了 VMware vSphere CLI 的系统上打开命令提示符。
3. 更改到安装了 VMware vSphere CLI 的目录。Linux 上的默认位置是 **/usr/bin。**Windows 上的默认位置是 **C:\Program Files\VMware\VMware vSphere CLI\bin。**
4. 运行以下命令：`vicfg-snmp.pl --server <server> --username <username> --password <password> -c <community> -t <hostname> @162/<community>`

   其中，`<server>` 是 ESXi 系统的主机名或 IP 地址，`<username>` 是 ESXi 系统上的用户，`<community>` 是 SNMP 团体名称，`<hostname>` 是管理站的主机名或 IP 地址。

   注: 在 Linux 上，不要求提供 .pl 扩展名。

   注: 如果没有指定用户名和密码，系统将会提示您。

SNMP 陷阱配置会立即生效，而无须重新启动任何服务。

在运行支持的 Red Hat Enterprise Linux 操作系统和 SUSE Linux Enterprise Server 的系统上配置防火墙

如果在安装 Red Hat Enterprise Linux/SUSE Linux 时启用了防火墙安全保护，则默认情况下，所有外部网络接口上的 SNMP 端口都将处于关闭状态。要启用 SNMP 管理应用程序（例如 OpenManage Essentials）以从 Server Administrator 查找和检索信息，至少一个外

部网络接口上的 SNMP 端口必须打开。如果 Server Administrator 检测到防火墙中未打开任何外部网络接口的 SNMP 端口，则将显示警告消息，并在系统日志中记录消息。

通过禁用防火墙、打开防火墙中的整个外部网络接口或打开防火墙中至少一个外部网络接口的 SNMP 端口，您可以打开 SNMP 端口。您可以在启动 Server Administrator 之前或之后执行此操作。

要使用上述方法之一打开 Red Hat Enterprise Linux 上的 SNMP 端口，请执行以下操作：

1 在 Red Hat Enterprise Linux 命令提示符下，键入 `setup` 并按 <Enter> 以启动文本模式安装实用程序。

注: 只有在执行了默认的操作系统安装之后，此命令才可用。

选择工具菜单将显示。

2 使用向下箭头选择**防火墙配置**，并按 <Enter>。

此时会显示**防火墙配置**屏幕。

3 按 <Tab> 选择**安全级别**，然后按空格键选择您想要设置的安全级别。所选**安全级别**用星号表示。

注: 有关防火墙安全级别的更多信息，请按 <F1>。默认 SNMP 端口号为 161。如果您使用的是 X Window 系统图形用户界面，按 <F1> 可能不提供有关较新版本的 Red Hat Enterprise Linux 上的防火墙安全级别的信息。

a 要禁用防火墙，选择**无防火墙**或**禁用**并转至步骤 7。

b 要打开整个网络接口或 SNMP 端口，请选择**高、中**或**已启用**，然后继续执行步骤 4。

4 按 <Tab> 键以转到“自定义”，然后按 <Enter> 键。

此时会显示**防火墙配置-自定义**屏幕。

5 选择打开整个网络接口还是仅打开所有网络接口上的 SNMP 端口。

a 要打开整个网络接口，按 <Tab> 以转到一个受信任的设备并按空格键。设备名称左侧框中的星号表示将打开整个接口。

b 要打开所有网络接口上的 SNMP 端口，请按 <Tab> 以转到其他端口和类型 `snmp:udp`。

6 按 <**Tab**> 键以选择**确定**，然后按 <**Enter**> 键。

此时会显示**防火墙配置**屏幕。

7 按 <**Tab**> 键以选择**确定**，然后按 <**Enter**> 键。

选择工具菜单将显示。

8 按 <**Tab**> 键以选择**退出**，然后按 <**Enter**> 键。

防火墙配置

要在 SUSE Linux Enterprise Server 上打开 SNMP 端口：

1 通过在控制台上运行以下命令配置 SuSEfirewall2 `a.# yast2 firewall`

2 使用箭头键导航至**允许的服务**。

3 按 <Alt><d> 键打开**其他允许的端口**对话框。

4 按 <Alt><T> 键移动光标到 **TCP 端口**文本框。

5 在文本框中键入 **snmp**。

6 按 <Alt><O> <Alt><N> 键转至下一屏幕。

7 按 <Alt><A> 键接受并应用更改。

3

使用 Server Administrator

要启动 Server Administrator 会话，请双击桌面上的 **Server Administrator** 图标。

此时将显示 **Server Administrator 登录**屏幕。Server Administrator 的默认端口是 1311。您可以根据需要更改端口。有关设置服务器首选项的说明，请参阅系统管理服务器管理连接服务和安全设置。

主题：

登录和注销

Server Administrator 提供以下类型的登录方式：

- Server Administrator 本地系统登录
- Server Administrator 受管系统登录 — 使用桌面图标
- Server Administrator 受管系统登录 — 使用 Web 浏览器
- Central Web Server 登录

Server Administrator 本地系统登录

只有在 Server Instrumentation 和 Server Administrator Web Server 组件均已安装在本地系统上时，才可以使用 Server Administrator 本地系统登录。

注: Server Administrator 本地系统登录对于运行 XenServer 6.5 的服务器不可用。

要在本地系统上登录 Server Administrator，请执行以下操作：

1. 在系统管理的**登录**窗口的相应字段中键入预先分配的**用户名**和**密码**。
   如果要通过已定义的域访问 Server Administrator，还必须指定正确的域名。
2. 选中 **Active Directory 登录**复选框使用 Microsoft Active Directory 登录。请参阅使用 Active Directory 登录。
3. 单击**提交**。

要结束 Server Administrator 会话，请单击每个 **Server Administrator** 主页右上角的**注销**。

注: 有关使用 CLI 在系统上配置 Active Directory 的信息，请参阅 dell.com/openmanagemanuals 上的 *Management Station Software Installation Guide*（管理站软件安装指南）。

Server Administrator 受管系统登录 — 使用桌面图标

只有在系统上安装了 Server Administrator Web Server 组件时，才能使用此登录。要登录 Server Administrator 以管理远程系统：

1 双击桌面上的 **Server Administrator** 图标。
2 键入管理系统的 IP 地址、系统名称或完全限定域名 (FQDN)。

注: 如果已经提供系统名称或 FQDN，Server Administrator Web Server 主机会将系统名称或 FQDN 转换为管理系统的 IP 地址。您还可以通过以下格式提供管理系统的端口号进行连接：主机名:端口号，或者 IP 地址:端口号。

3 如果您使用的是内联网，请选择**忽略证书警告**。
4 选择 **Active Directory 登录**以使用 Microsoft Active Directory 验证进行登录。如果未使用 Active Directory 软件控制网络的访问权，请勿选择 **Active Directory 登录**。请参阅使用 Active Directory 登录。
5 单击**提交**。

Server Administrator 受管系统登录 — 使用 Web 浏览器

注: 要登录至 Server Administrator，您必须具有预先分配的用户权限。请参阅设置和管理了解有关设置新用户的说明。

1 打开 Web 浏览器。
2 在地址字段中键入以下项之一：
- `https://hostname:1311`，其中 hostname 是为受管系统分配的名称，1311 是默认端口号。
- `https://IP address:1311`，其中 IP address 是受管系统的 IP 地址，1311 是默认端口号。

注: 请确保在地址字段中输入 `https://`（而非 `http://`）。

3 按下 <Enter>。

Central Web Server 登录

只有在系统上安装了 Server Administrator Web Server 组件时，才能使用此登录。使用此登录管理 Server Administrator Central Web Server：

1 双击桌面上的 **Server Administrator** 图标。将显示远程登录页。

小心: 登录屏幕上显示忽略证书警告复选框。您应谨慎地使用此选项。强烈建议仅在可信企业内部网环境中使用此选项。

2 单击屏幕右上角的**管理 Web 服务器**链接。
3 输入**用户名**、**密码**和**域名**（如果从定义的域访问 Server Administrator），然后单击**提交**。
4 选择 **Active Directory 登录**以使用 Microsoft Active Directory 登录。请参阅使用 Active Directory 登录。
5 单击**提交**。

要结束 Server Administrator 会话，请单击全局导航栏上的**注销**。

注: 当使用 Mozilla Firefox 或 Microsoft Internet Explorer 启动 Server Administrator 时，会显示一个中间警告页指出安全证书的问题。为了确保系统安全，建议您生成新的 X.509 证书、重新使用现有的 X.509 证书或导入来自证书颁发机构 (CA) 的证书链。为避免遇到此类有关证书的警告消息，使用的证书必须来自可靠 CA。有关 X.509 证书管理的更多信息，请参阅 X.509 证书管理。

注: 为了确保系统安全，建议从证书颁发机构 (CA) 导入证书链。有关更多信息，请参阅 VMware 说明文件。

注: 如果受管系统上的证书颁发机构有效，但 Server Administrator Web 服务器仍然报告不可信证书错误，则仍然可以使用 certutil.exe 文件将受管系统的 CA 设置为可信。有关访问此 .exe 文件的信息，请参阅操作系统说明文件。在支持的 Windows 操作系统上，还可以使用证书管理单元选项导入证书。

使用 Active Directory 登录

应选中 **Active Directory 登录**以使用 Active Directory 中的 Dell 扩展架构解决方案登录。

使用此解决方案可以提供对 Server Administrator 的访问；可以为 Active Directory 软件中的现有用户添加/控制 Server Administrator 用户和权限。 有关更多信息，请参阅 **dell.com/openmanagemanuals** 上 *Server Administrator Installation Guide*（Server Administrator 安装指南）中的“使用 Microsoft Active Directory”。

单一登录

Windows 操作系统中的“单一登录”选项使所有已登录用户能够通过单击桌面上的 **Server Administrator** 图标跳过登录页并访问 Server Administrator Web 应用程序。

注: 有关单一登录的更多信息，请参阅位于 support.microsoft.com/default.aspx?scid=kb;en-us;Q258063 的知识库文章。

对于本地计算机访问，必须在计算机上拥有具备相应权限的帐户（用户、高级用户或管理员）。其他用户根据 Microsoft Active Directory 进行验证。为了根据 Microsoft Active Directory 使用单一登录验证启动 Server Administrator，还必须传递以下参数：

```
authType=ntlm&application=[plugin name]
```

其中 `plugin name = omsa, ita,` ，以此类推。

例如：

```
https://localhost:1311/?authType=ntlm&application=omsa
```

为了根据本地计算机用户帐户使用单一登录验证启动 Server Administrator，还必须传递以下参数：

```
authType=ntlm&application=[plugin name]&locallogin=true
```

其中 `plugin name = omsa, ita` ，以此类推。

例如：

```
https://localhost:1311/?authType=ntlm&application=omsa&locallogin=true
```

Server Administrator 也已经过扩展，以允许其他产品（比如 Dell EMC OpenManage Essentials）直接访问 Server Administrator Web 页面，而不用通过登录页（如果目前已登录并具有相应的权限）。

在运行支持的 Microsoft Windows 操作系统的系统上配置安全设置

必须配置浏览器的安全设置，才能从运行支持的 Microsoft Windows 操作系统的远程管理系统登录到 Server Administrator。

浏览器的安全性设置可能会使 Server Administrator 使用的客户端脚本不能执行。 要启用客户端脚本使用，请在远程管理系统上执行以下步骤。

注: 如果还没有将浏览器配置为使用客户端脚本，在登录 Server Administrator 时可能会看到一个空白屏幕。在这种情况下，将会显示错误消息来指导您配置浏览器设置。

在 Internet Explorer 上启用客户端脚本的使用

1 在 Web 浏览器中，单击**工具** > **Internet 选项** > **安全**
此时会显示 **Internet 选项**窗口。
2 在**选择要查看的区域或更改安全设置**下，单击**可信站点**，然后单击**站点**。
3 在**将该网站添加到区域**字段中，粘贴用来访问远程受管系统的该 Web 地址。
4 单击**添加**。
5 将用来访问远程受管系统的 Web 地址从浏览器的地址栏复制并粘贴到**将该网站添加到区域字段**中。
6 在**此区域的安全级别**中，单击**自定义**级别
7 单击**确定**保存新设置。
8 关闭浏览器并登录 Server Administrator。

在 Internet Explorer 上启用针对 Server Administrator 的单一登录

要允许不提示用户凭据的 Server Administrator 单一登录：

1 在 Web 浏览器中，单击**工具** > **Internet 选项** > **安全**
2 在**选择要查看的区域或更改安全设置**下面，单击**受信的站点**，然后单击**站点**。
3 在**将该网站添加到区域**字段中，粘贴用于访问远程受管系统的 Web 地址。
4 单击**添加**。
5 单击 **自定义级别**。
6 在**用户验证**下面，选择**自动使用当前用户名和密码登录**。
7 单击**确定**保存新设置。
8 关闭浏览器并登录 Server Administrator。

在 Mozilla Firefox 上启用客户端脚本的使用

1 打开您的浏览器。
2 单击**编辑** > **首选项**。
3 单击**高级** > **脚本和插件**。
4 在“为以下组件启用 Javascript”下，请确保选中位于**为以下组件启用 Javascript** 下的 **Navigator** 复选框。
5 单击**确定**保存新设置。
6 关闭浏览器。
7 登录到 Server Administrator。

Server Administrator 主页

注: 在使用 Server Administrator 时不要使用 Web 浏览器工具栏按钮（例如后退和刷新）。仅使用 Server Administrator 导航工具。

除个别例外情况之外，Server Administrator 主页包括三个主要区域：

- 全局导航栏提供常规服务的链接。
- 系统树基于用户访问权限显示所有可见的系统对象。
- 操作窗口显示基于用户访问权限可对选定的系统树对象进行的管理操作。操作窗口包含 3 个功能区域：
  - 操作选项卡，显示基于用户访问权限可对选定对象进行的主要操作或操作类别。

- 操作选项卡包含的子类别，显示操作选项卡基于用户访问权限的所有可用次选项。
- 数据区域基于用户访问权限显示有关选定的系统树对象、操作选项卡和子类别的信息。

此外，登录至 **Server Administrator** 主页时，窗口右上角将显示系统型号、分配的系统名称以及当前用户的用户名和用户权限。

Server Administrator 安装在系统后， 下表列出 **GUI** 字段名称和可应用的系统。

表. 7: GUI 字段名称和可应用的系统

GUI 字段名称	适用的系统
模块化机柜	模块化系统
服务器模块	模块化系统
主系统	模块化系统
系统	非模块化系统
主系统机箱	非模块化系统

下图显示具有管理员权限的用户在非模块化系统上登录时的 Server Administrator 主页布局示例。

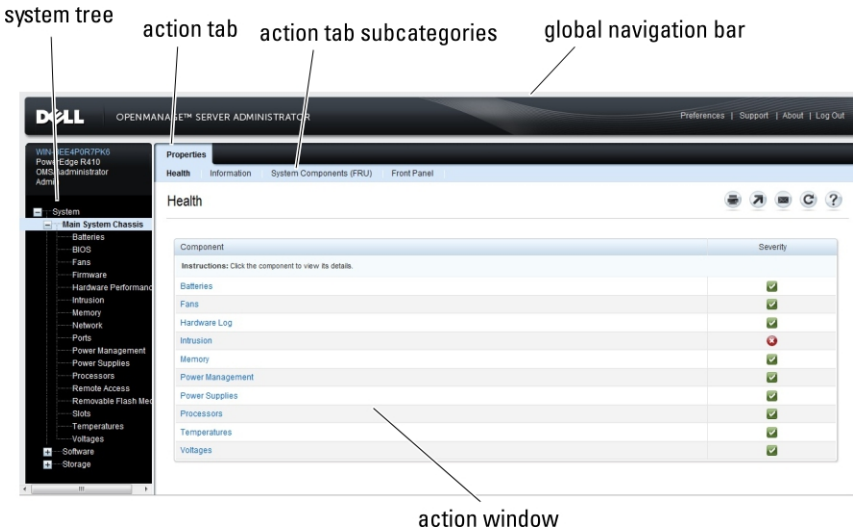

图 1: Server Administrator 主页示例 — 非模块化系统

下图显示具有管理员权限的用户在模块化系统上登录时的 Server Administrator 主页布局示例。

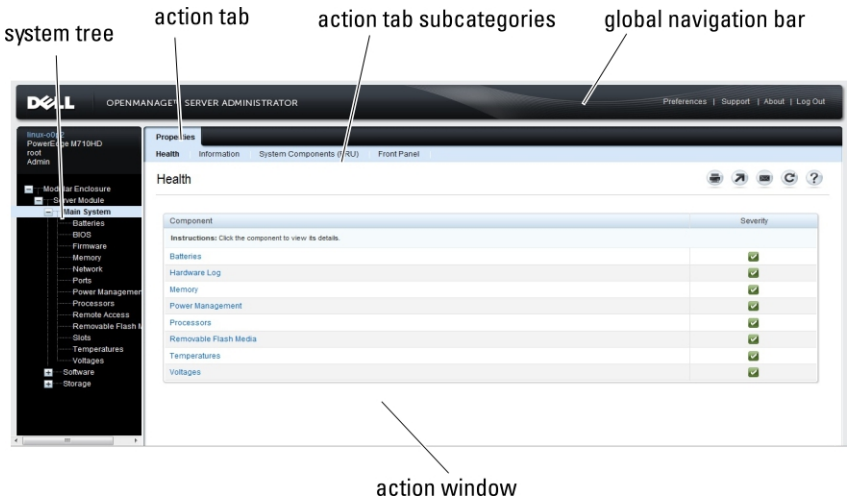

图 2: Server Administrator 主页示例 — 模块化系统

单击系统树中的对象将打开该对象的相应操作窗口。您可以浏览操作窗口，方法是：单击操作选项卡以选择主类别，单击操作选项卡子类别以访问更详细的信息或更具体的操作。操作窗口数据区域显示的信息可以是从系统日志到状况指示器和系统探测器计量表。操作窗口数据区域中带下划线的项目表示更高级别的功能。单击带下划线的项目将在操作窗口中创建包含更详细信息的数据区域。例如，单击**属性**操作选项卡的**运行状况**子类别下的**主系统机箱/主系统**，将列出“主系统机箱/主系统”对象包含的运行状况受监测的所有组件的运行状况。

注: 要查看大部分可配置的系统树对象、系统组件、操作选项卡和数据区域功能，用户必须具有“管理员”或“高级用户”权限。同时，只有以“管理员”权限登录的用户才能访问重要的系统功能，例如关机选项卡中的关闭系统功能。

模块化系统和非模块化系统的 Server Administrator 用户界面差异

下表列出模块化系统和非模块化系统中各种 Server Administrator 功能的可用性。

表. 8: 模块化系统和非模块化系统的 Server Administrator 用户界面差异

功能	模块化系统	非模块化系统
电池	✓	✓
电源设备	✗	✓
风扇	✗	✓
硬件性能	✗	✓
侵入	✗	✓
内存	✓	✓
网络	✓	✓
端口	✓	✓

功能	模块化系统	非模块化系统
Power Management（电源管理）	✓	✓
处理器	✓	✓
远程访问	✓	✓
可移除闪存介质	✓	✓
插槽	✓	✓
温度	✓	✓
电压	✓	✓
模块化机柜（机箱信息和 CMC 信息）	✓	✗

全局导航栏

全局导航栏及其链接可供程序中的所有用户级别使用。

- 单击**首选项**以打开**首选项**主页。请参阅使用首选项主页。
- 单击**支持**以连接到 Dell EMC 支持网站。
- 单击**关于**以显示 Server Administrator 版本和版权信息。
- 单击**注销**结束当前的 Server Administrator 程序会话。

系统树

系统树显示在 Server Administrator 主页的左侧，列出了可以查看的系统组件。系统组件按组件类型进行分类。展开称为**模块化机柜** > **系统/服务器模块**的主对象时，可能显示的系统/服务器模块组件的主要类别为**主系统机箱/主系统**、**软件**和**存储**。

要展开树的分支，请单击对象左侧的加号（ + ）或者双击该对象。减号（ − ）表示不能被进一步展开的已展开条目。

操作窗口

单击系统树中的项目时，操作窗口的数据区域将显示有关该组件或对象的详细信息。单击操作选项卡将以子类别列表的形式显示所有可用的用户选项。

单击系统/服务器模块树中的对象将打开该组件的操作窗口，显示可用的操作选项卡。 默认情况下，数据区域将显示选定对象第一个操作选项卡的预先选定子类别。

预先选定子类别通常为第一个选项。例如，单击**主系统机箱/主系统**对象将打开一个操作窗口，其中的数据区域将显示**属性**操作选项卡和**运行状况**子类别。

数据区域

数据区域位于主页右侧操作选项卡的下方。数据区域用于执行任务或查看有关系统组件的详细信息。窗口的内容取决于当前选择的系统树对象和操作选项卡。例如，从系统树中选择 **BIOS** 后，**属性**选项卡将被默认选定，并在数据区域中显示系统 BIOS 的版本信息。操作窗口的数据区域包含许多公用功能，包括状况指示器、任务按钮、带下划线的项目和计量表标志。

Server Administrator 用户界面以 <mm/dd/yyyy> 格式显示日期。

系统或服务器模块组件状态指示器

组件名称旁边显示的图标说明了组件的状况（即页面最后刷新时的状况）。

表. 9: 系统或服务器模块组件状态指示器

图标	说明
	组件运行状况良好（正常）。
	组件处于警告（非严重）状态。探测器或其他监测工具检测到组件的读数位于特定最小值和最大值范围时，将出现警告状况。警告状况需要及时处理。
	组件处于故障或严重状态。探测器或其他监测工具检测到组件的读数位于特定最小值和最大值范围时，将出现严重状况。严重状况需要立即进行处理。
	组件的运行状况未知。

任务按钮

大多数从 Server Administrator 主页打开的窗口均至少包含五个任务按钮：**打印**、**导出**、**电子邮件**、**帮助**和**刷新**。特定 Server Administrator 窗口还会包括许多其他任务按钮。例如，**日志**窗口还包含**另存为**和**清除日志**任务按钮。

- 单击**打印**（ ）将在默认打印机上打印打开的窗口。
- 单击**导出**（ ）会生成一个文本文件，列出打开窗口中各个数据字段的值。该导出文件将保存到指定的位置。有关自定义数据字段值分隔符的信息，请参阅“设置用户”和“系统首选项”。
- 单击**电子邮件**（ ）创建电子邮件信息，地址为指定的电子邮件收件人。有关设置电子邮件服务器和默认电子邮件收件人的说明，请参阅“设置用户”和“系统首选项”。
- 单击**刷新**（ ）将在操作窗口数据区域中重新载入系统组件的状况信息。
- 单击**另存为**将以 **.zip** 文件形式保存操作窗口的 HTML 文件。
- 单击**清除日志**将从操作窗口数据区域中显示的日志中删除所有事件。
- 单击**帮助**（ ）提供您正在查看的特定窗口或任务按钮的详细信息。

注: 导出、电子邮件和另存为按钮只有当用户以“高级用户”或“管理员”权限登录时才可见。清除日志按钮仅对具有“管理员”权限的用户可见。

带下划线的项目

单击操作窗口数据区域中带下划线的项目将显示有关该项目的其他详细信息。

计量表标志

温度探测器、风扇探测器和电压探测器分别由各自的计量表标志表示。例如，下图显示了系统 CPU 风扇探测器的读数。

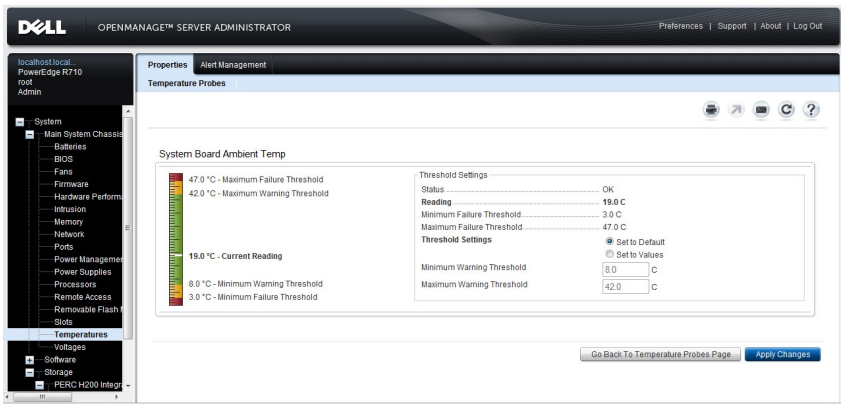

图 3: 计量表标志

使用联机帮助

Server Administrator 主页的每个窗口都有上下文相关联机帮助。 单击**帮助**将打开单独显示的帮助窗口，其中显示您正在查看的特定窗口的详细信息。 联机帮助涵盖 Server Administrator 服务的各个方面，可指导您完成相应的特定操作。 您可以查看的所有窗口（取决于 Server Administrator 在系统中查找到的软件组和硬件组以及您的用户权限级别）均可使用联机帮助。

使用首选项主页

首选项主页的左窗格（在 Server Administrator 主页上显示系统树）将显示系统树窗口中的所有可用配置选项。

“首选项”主页的可用配置选项如下：

- 常规设置
- 服务器管理员

为了管理远程系统而登录后，可以查看**首选项**选项卡。 为了管理 Server Administrator Web Server 或管理本地系统而登录后，此选项卡也可用。

与 Server Administrator 主页一样，**首选项**主页也有三个主要区域：

- 全局导航栏提供常规服务的链接。
  - 单击**主页**可返回到 Server Administrator 主页。
- **首选项**主页的左窗格（在 Server Administrator 主页上显示系统树）将显示管理系统或 Server Administrator Web Server 的首选项类别。
- 操作窗口显示管理系统或 Server Administrator Web Server 的可用设置和首选项。

管理系统首选项

登录远程系统时，“首选项”主页默认为**首选项**选项卡下的**节点配置**窗口。

单击 Server Administrator 对象使您能够启用或禁用具有“用户”或“高级用户”权限的用户的访问。根据用户组权限的不同，Server Administrator 对象操作窗口可包含**首选项**选项卡。

在**首选项**选项卡下，您可以：

- 启用或禁用具有“用户”或“高级用户”权限的那些用户的访问
- 选择警报消息的格式

  注: 可能的格式为传统和增强格式。默认的格式是传统格式，也就是传统的格式。
- 启用自动备份并清除 ESM 日志条目。
  默认情况下，此功能处于禁用状态。启用此功能可为 ESM 日志创建自动备份。创建备份后，Server Administrator 的 ESM 日志以及 iDRAC/BMC 的 SEL 条目将被清除。每当日志一满便会重复执行此过程。

  备份保存在以下位置:

  Windows：**<Install_root>\omsa\log\omsellog.xml**

  Linux 和 ESXi：**<Install_root>/var/log/openmanage/omsellog.xml**

  注: 此功能仅可用于第 10 代和第 11 代 PowerEdge 系统。从第 12 代 PowerEdge 服务器或更高版本开始，iDRAC 提供了自动备份和 SEL 日志清除功能。
- 选中或清除操作系统主要事件日志中记录的日志条目严重性。可以选择的值有：**记录严重**、**记录警告**或**记录信息性**

  注: 所有选项默认为处于选中状态。如安装了操作系统日志记录筛选器组件，则可使用操作系统日志记录筛选器功能。
- 选择**启用**记录所有不受监测的 ESM 传感器事件。通过启用此功能，Server Administrator 将生成所有不受监测传感器的 SNMP 陷阱、操作系统日志和警报。
- 配置命令日志大小
- 配置 SNMP

Server Administrator Web Server 首选项

当为了管理 Server Administrator Web Server 而登录时，首选项主页默认为**首选项**选项卡下的用户首选项窗口。

由于 Server Administrator Web Server 与管理系统分离，因此，当使用“管理 Web Server”链接登录 Server Administrator Web Server 时，将显示以下选项：

- Web Server 首选项
- X.509 证书管理

有关访问这些功能的更多信息，请参阅 Server Administrator 服务概述。

系统管理服务器管理连接服务和安全设置

设置用户和服务器首选项

您可以在**首选项**主页中设置用户和 webserver 首选项。

注: 要设置或重设用户或系统首选项，您必须以“管理员”权限登录。

设置用户首选项：

1 单击全局导航栏上的**首选项**。
将显示**首选项**主页。
2 单击**常规设置**。
3 要添加预先选定的电子邮件收件人，请在**邮件发送至：**字段中键入指定服务联系人的电子邮件地址，然后单击**应用**。

注: 在任意窗口中单击电子邮件（  **）可将电子邮件信息和附加的该窗口的 HTML 文件发送至指定的电子邮件地址。**

注: 如果重新启动 Server Administrator 服务或已安装 Server Administrator 的系统，则不会保留 Web Server URL。使用 omconfig 命令以重新输入该 URL。

Webserver 首选项

要设置 webserver 首选项，请执行以下操作：

1 单击全局导航栏上的**首选项**。
系统将显示**首选项**主页。
2 单击**常规设置**。
3 在**服务器首选项**窗口中根据需要设置选项。

- **会话超时（分钟）**功能可以用于设置 Server Administrator 会话保持活动状态的时间限制。选择**启用**，如果在指定分钟数内没有用户交互，则允许 Server Administrator 超时。会话超时的用户必须再次登录才能继续。选择**禁用**，将禁用 Server Administrator **会话超时（分钟）**功能。
- **HTTPS 端口**字段可指定 Server Administrator 的端口。Server Administrator 的默认安全端口是 1311。

  注: 将端口编号更改为无效或正在使用的端口编号可能会妨碍其他应用程序或浏览器访问管理系统上的 Server Administrator。有关默认端口列表，请参阅可在 dell.com/openmanagemanuals 上获得的 *Server Administrator Installation Guide*（Server Administrator 安装指南）。
- **要绑定到的 IP 地址**字段指定启动会话时，Server Administrator 所绑定到的管理系统的的 IP 地址。选择**所有**将绑定到所有适用于您的系统的 IP 地址。选择**特定**将绑定到特定 IP 地址。

  注: 将要绑定到的 IP 地址的值更改为除所有以外的值，可能会妨碍其他应用程序或浏览器访问管理系统上的 Server Administrator。
- **收件人**字段指定您想要默认向其发送有关更新的电子邮件的地址。您可以配置多个电子邮件地址并使用逗号分隔各地址。
- **SMTP 服务器名称（或 IP 地址）**和 **SMTP 服务器的 DNS 后缀**字段用于指定您的公司或组织的简单邮件传输协议 (SMTP) 和域名服务器 (DNS) 后缀。要启用 Server Administrator 以发送电子邮件，在相应字段中键入您公司或组织的 SMTP 服务器的 IP 地址和 DNS 后缀。

  注: 出于安全保护的原因，您的公司或组织可能不允许通过 SMTP 服务器向外部帐户发送电子邮件。
- **命令日志大小**字段可指定命令日志文件的最大文件大小（以 MB 为单位）。

  注: 仅在为了管理 Server Administrator Web Server 而登录时，才会显示此字段。
- **支持链接**字段可指定为管理系统提供支持的企业实体的 URL。
- **自定义分隔符**字段指定使用**导出**按钮创建的文件中用于分隔数据字段的字符。；字符是默认的分隔符。其它选项有 **!**、**@**、**#**、**$**、**%**、**^**、*、**~**、**?**、**|** 和 **,**。
- **SSL 密码**字段 在 Web 服务器和浏览器之间指定了一个安全连接。在配置时选择支持 Web 服务器的密码。如果设置了无效的密码组，连接服务不会启动。默认情况下，密码组的值如下：

  ```
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

  ,TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,
  ```

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,

TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,

TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,

TLS_ECDH_RSA_WITH_AES_128_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA

注: 如果设置了不正确的密码值，并且连接服务启动失败，请使用 CLI 命令提示符或手动设置有效的密码，然后重新启动连接服务。

注: 由于安全原因，升级到 Server Administrator 9.1 将不会保留现有的 Web 服务器密码设置。

- **SSL 协议**字段允许您从 Web 服务器列出的 SSL 协议进行设置，来建立 HTTPS 连接。可能的值包括： `TLSv1.1`、`TLSv1.2` 和 `(TLSv1.1, TLSv1.2)`。默认情况下，SSL 协议的值设为 `(TLSv1.1, TLSv1.2)`。更改会在 Web 服务器重新启动后生效。

注: 如果默认设置不支持该协议，请从浏览器设置中启用 SSL 协议。

- **密钥签名算法（对于自签名证书）** - 允许您选择支持的签名算法。如果选择 **SHA 512** 或 **SHA 256**，请确保操作系统/浏览器支持该算法。如果您选择这些选项之一，但没有所需的操作系统/浏览器支持，Server Administrator 将显示 `cannot display the webpage` 错误。此字段专用于 Server Administrator 自动生成的自签名证书。如果将新证书导入 Server Administrator 或在其中生成新证书，下拉列表将呈灰色。

- **Java Runtime Environment** — 允许您选择下列选项之一：
  - **捆绑的 JRE** — 启用与 System Administrator 一起提供的 JRE
  - **系统 JRE** - 启用已安装在系统上的 JRE。从下拉列表中选择所需的版本。

注: 不建议将 Server Administrator 升级到 Java Runtime Environment (JRE) 的主要版本，它被限制为安全补丁和最低 JRE 版本。有关更多详细信息，请参阅 Server Administrator 的发行说明（与 Server Administrator 应用程序打包在一起）或访问 dell.com/openmanagemanuals。

注: 如果当前运行 Server Administrator 的系统上不存在 JRE，则使用随 Server Administrator 提供的 JRE。

4 在**服务器首选项**窗口中完成选项设置后，请单击**应用**。

注: 您必须重新启动 Server Administrator Web Server 以使更改生效。

X.509 证书管理

注: 要执行证书管理，必须以“管理员”权限登录。

Web 证书需要确保远程系统的身份并确保与远程系统交换的信息无法由他人查看或更改。为了确保系统安全，建议

- 您生成新的 X.509 证书、重复使用现有的 X.509 证书或导入来自认证机构 (CA) 的证书链。
- 所有安装了 Server Administrator 的系统均有唯一的主机名。

要通过**首选项**主页管理 X.509 证书，请单击**常规设置**，单击 **Web Server** 选项卡，然后单击 **X.509 证书**。

可用选项如下：

- **生成新证书** — 生成新的自签名证书，用于运行 Server Administrator 的服务器与浏览器之间的 SSL 通信。

  注: 使用自签名证书时，大多数 Web 浏览器会显示一个*不受信任*警告，因为自签名证书没有被操作系统信任的认证机构 (CA) 签名。一些安全浏览器设置也会阻止自签名 SSL 证书。Server Administrator Web GUI 需要用于此类安全浏览器的 CA 签名证书。
- **证书维护** — 可让您生成证书签名请求 (CSR)，其中包含 CA 自动创建受信任 SSL Web 证书需要的所有主机相关信息。您可以按照证书签名请求 (CSR) 页上的指示，或将 CSR 页上文本框中的整个文本复制并粘贴到 CA 提交表中，检索必要的 CSR 文件。此文本必须采用 Base64 编码格式。

  注: 您也有查看证书信息，以及导出目前以 Base64 编码格式使用的证书的选项，该格式可被导入至其他网页服务中。
- **导入证书链** — 可让您导入信任 CA 签署的证书链（采用 PKCS#7 格式）。证书可以为 DER 或 Base64 编码格式。
- **导入 PKCS12 密钥库** — 可让您导入 PKCS # 12 密钥库，该密钥库取代 Server Administrator Web 服务器中使用的密钥和证书。PKCS# 12 是一个公共密钥库，包含一个私钥以及用于 Web 服务器的证书。Server Administrator 使用 Java 密钥库 (JKS) 格式存储 SSL 证书及其私钥。将 PKCS# 12 密钥库导入 Server Administrator 将删除密钥库条目，并会将私钥和证书条目导入到 Server Administrator JKS。

  注: 如果您选择了无效的 PKCS 文件或者键入了不正确的密码，则将显示一条错误消息。

SSL 服务器证书

Server Administrator Web 服务器配置为使用行业标准的 SSL 安全协议通过网络来传输加密数据。SSL 建立在非对称加密技术基础之上，是一种广泛接受的加密技术，用于在客户端与服务器之间提供经过验证和加密的通信，防止遭到网络上的窃听。

启用 SSL 的系统可以执行下列任务：

- 向启用 SSL 的客户端验证自身
- 允许两个系统建立加密的连接

加密过程提供高级别数据保护。Server Administrator 使用了北美地区常见互联网浏览器中提供的最安全加密方式。

默认情况下，Server Administrator Web 服务器包含自签名的唯一 SSL 数字证书。您可以用知名证书颁发机构 (CA) 签名的证书替换默认的 SSL 证书。证书颁发机构是一个企业实体，在信息技术行业中满足高标准的可靠筛选、标识和其他重要安全标准。CA 的示例包括 Thawte 和 VeriSign。要启动用于获取 CA 签名证书的过程，请使用 Server Administrator Web 界面生成包含您公司信息的证书签名请求 (CSR)。然后，将生成的 CSR 提交给 CA，例如 VeriSign 或 Thawte。CA 可以是根 CA 或中间 CA。在收到 CA 签名的 SSL 证书后，将其上载到 Server Administrator。

对于每个得到管理站信任的 Server Administrator，其 SSL 证书必须放在管理站的证书库中。在管理站上安装了 SSL 证书后，支持的浏览器可以访问 Server Administrator 而不会显示证书警告。

Server Administrator Web Server 操作选项卡

以下为登录以管理 Server Administrator Web 服务器时显示的操作选项卡：

- 属性
- 关机
- 日志
- 警报管理
- 会话管理

更新 Web 服务器

△ | 小心: **Web 服务器更新后就无法进行出厂重置。如需出厂重置，请重新安装 Server Administrator。**

您可以在需要时使用 **omwsupdateutility**，升级 Apache Tomcat Web 服务器，而不会影响 Server Administrator 功能。该实用程序允许升级到 Web 服务器的次要版本，但不支持升级到主要版本。例如，支持从版本 A.*x* 升级到 A.*y*，但是不支持从 A.*x* 升级到 B.*x* 或 B.*y*。此外，您可以使用该实用程序将 Web 服务器替换为较早的版本，前提条件该版本为次要版本。该实用程序将在 Web 服务器安装过程中被保存到以下默认位置：

- 在运行 Windows 操作系统的系统上：`C:\Program Files\Dell\SysMgt\omsa\wsupdate`
- 在运行 Linux 操作系统的系统上：`/opt/dell/srvadmin/lib64/openmanage/wsupdate`

您可以下载 Tomcat Web 服务器软件包的所需版本，并通过命令提示符运行上述实用程序。从 **tomcat.apache.org** 下载 Tomcat Web 服务器核心分发软件包。分发软件包必须是 .zip 或 .tar.gz 文件；Windows 安装程序包装包不受支持。

要更新 Web 服务器，浏览至 **wsupdate** 文件夹并随即运行以下命令：

- 在 Windows 上：`omwsupdate.bat [SysMgt folder path] [apache-tomcat.zip/.tar.gz file path]`
- 在 Linux 上 `omwsupdate.sh [srvadmin folder path] [apache-tomcat.zip/.tar.gz file path]`

默认的 **SysMgt** 文件夹路径为 **C：\Program Files\Dell\SysMgt** 而 **srvadmin** 文件夹路径为 **/opt/dell/srvadmin**。

使用 Server Administrator 命令行界面

Server Administrator 命令行界面 (CLI) 使用户可以通过被监测系统的操作系统命令提示符执行基本的系统管理任务。

CLI 使有非常明确任务的用户能够快速检索关于系统的信息。例如，管理员可以使用 CLI 命令编写批处理程序或脚本，以在特定时间执行。这些程序可以在执行时捕获感兴趣的组件报告，例如风扇 RPM。使用附加脚本时，CLI 可以用于捕获系统高使用率期间的数据，以与系统低使用率时的相同测量数据进行比较。命令结果可以发送到一个文件，以便以后进行分析。该报告可以帮助管理员获得有关信息，以用于调整使用方案，判断是否需要购买新的系统资源或了解故障组件的运行状况。

有关 CLI 功能和用法的完整说明，请参阅 **dell.com/openmanagemanuals** 上的 *Server Administrator Command Line Interface Guide*（Server Administrator 命令行界面指南）。

4

Server Administrator 服务

Server Administrator Instrumentation Service 可以监测系统的运行状况，并使您可以快速查看业界标准的系统管理代理程序收集的详细故障和性能信息。利用其报告和查看功能，可以检索构成系统的各个机箱的整体运行状况。在子系统级别中，可以查看系统关键位置的电压、温度、风扇转速和内存运行的信息。在摘要视图中，可以查看系统各相关物主成本 (COO) 的详细说明。也可以检索有关 BIOS、固件、操作系统和所有已安装系统管理软件的版本信息。

此外，系统管理员还可以使用 Instrumentation Service 执行以下重要任务：

- 指定某些关键组件的最小值和最大值。 这些值（称为阈值）用于确定组件发生警告事件的范围（最小和最大故障值由系统制造商指定）。
- 指定系统在发生警告或故障事件时如何响应。 用户可以配置系统对警告事件和故障事件的通知采取的响应措施。 另外，进行 24 小时监测的用户可以指定系统不采取任何措施，而根据用户自己的判断来选择对事件的最佳响应措施。
- 填写所有用户可以指定的系统值，例如系统名称、系统主要用户的电话号码、折旧方式以及系统是租赁还是购买。

注: 有关配置 SNMP 的更多信息，请参阅 在运行受支持的 Windows 操作系统的系统上配置 SNMP 代理程序。

主题：

管理系统

默认情况下，Server Administrator 主页将显示系统树视图的系统对象。**系统**对象将打开**属性**选项卡下的**运行状况**组件。

默认情况下，**首选项**主页将打开**节点配置**。

在**首选项**主页中，您可以限制具有“用户”和“高级用户”权限的用户的访问，设置 SNMP 密码，以及配置用户设置和 SM SA 连接服务设置。

注: Server Administrator 主页的每个窗口都有上下文相关的联机帮助。单击帮助（ ）可打开单独显示的帮助窗口，其中显示您正在查看的特定窗口的详细信息。联机帮助涵盖 Server Administrator 服务的各个方面，可指导您完成相应的特定操作。您可以查看的所有窗口（取决于 Server Administrator 在系统中查找到的软件组和硬件组以及您的用户权限级别）均可使用联机帮助。

注: 要查看诸多可配置的系统树对象、系统组件、操作选项卡和数据区域功能，用户必须具有“管理员”或“高级用户”权限。此外，只有以“管理员”权限登录的用户才能访问重要的系统功能，例如关机选项卡中的关闭系统功能。

管理系统或服务器模块树对象

Server Administrator 系统或服务器模块树基于 Server Administrator 在管理系统上发现的软件和硬件组以及用户访问权限显示所有可见的系统对象。系统组件按组件类型进行分类。当您展开主对象时 - **模块化机柜** - **系统/服务器模块** - 可能显示的系统组件的主要类别为**主系统机箱/主系统**、**软件**和**存储**。

如果已经安装了 Storage Management Service，则根据系统所连接的控制器和存储，存储树对象将会展开以显示各个对象。

有关 Storage Management Service 组件的详细信息，请参阅 **dell.com/openmanagemanuals** 上的 *Storage Management User's Guide*（Storage Management 用户指南）。

Server Administrator 主页系统树对象

本节提供 Server Administrator 主页上系统树中对象的相关信息。由于 ESXi 操作系统的限制，某些在 Server Administrator 早期版本中可用的功能在此版本中不再提供。

ESXi 不支持的功能有：

- FCoE 型和 iSoE 型信息。
- 警报管理 – 警报措施
- 网络接口 — 管理状况、DMA、Internet 协议 (IP) 地址，
- 网络接口 – 运行状况
- 远程关机 – 先关闭操作系统，然后关闭系统电源后再开启
- 关于详细信息 - Server Administrator 组件详细信息未列在**详细信息**选项卡下
- 角色图

注: Server Administrator 始终以 *<mm/dd/yyyy>* 格式显示日期。

注: 要查看诸多可配置的系统树对象、系统组件、操作选项卡和数据区域功能，用户必须具有“管理员”或“高级用户”权限。此外，只有以“管理员”权限登录的用户才能访问重要的系统功能，例如关机选项卡中的关闭系统功能。

模块化机柜

注: 对于 Server Administrator 来说，模块化机柜是包含一个或多个模块化系统的系统，在系统树中显示为独立的“服务器模块”。与独立“服务器模块”类似，模块化机柜包含系统的所有基本组件。唯一的不同是在更大的容器里有至少两个服务器模块的插槽，并且分别都是一个像系统一样完整的服务器模块。

要查看模块化系统的机箱信息和 Chassis Management Controller (CMC) 信息，单击**模块化机柜**对象。

- **选项卡：属性**
- **子选项卡：信息**

在属性选项卡下，您可以：

- 查看所监测模块化系统的机箱信息。
- 查看所监测模块化系统的详细 Chassis Management Controller (CMC) 信息。

访问并使用 Chassis Management Controller

要从 Server Administrator 主页启动 Chassis Management Controller **登录**窗口，请执行以下操作：

1 单击**模块化机柜**对象

2 单击 **CMC 信息选项卡**，然后单击**启动 CMC Web 界面**。随即显示 CMC **登录**窗口。

连接到 CMC 后，可以监测并管理模块化机柜。

系统或服务器模块属性

系统或服务器模块对象包含三个主要的系统组件组：主系统机箱/主系统、软件和存储。Server Administrator 主页默认为系统树视图的**系统**对象。通过**系统/服务器模块**对象操作窗口可以管理大部分管理功能。根据用户组权限的不同，**系统/服务器模块**对象操作窗口包含以下选项卡：**许可**、**属性**、**关机**、**日志**、**警报管理**和**会话管理**

许可

子选项卡：信息 | 许可

在许可子选项卡下，您可以：

- 设定使用 Integrated Dell Remote Access Controller (iDRAC) 的首选项以导入、导出、删除、或替换硬件的数字许可证。
- 查看所用设备的详细情况。详细情况包括许可证状态、许可证说明、授权 ID 和许可证过期日期。

注: Server Administrator 支持第 12 代 PowerEdge 系统以上版本的许可功能。该功能仅当所需的最低版本 iDRAC（即 iDRAC 1.30.30）已安装时才可用。

注: 该功能仅在安装所需的最低版本的 iDRAC 时可用。

属性

子选项卡：运行状况 | 摘要 | 资产信息 | 自动恢复

在**属性**选项卡下，您可以：

- 查看**主系统机箱/主系统**对象和**存储**对象中硬件和软件组件的当前运行状况警报状态。
- 查看所监测系统中所有组件的详细摘要信息。
- 查看和配置所监测系统的资产信息。
- 查看并为所监测的系统设置自动系统恢复（操作系统监督计时器）操作。

注: 自动系统恢复选项可能会由于已在 BIOS 中启用操作系统监督计时器而不可用。要配置自动恢复选项，必须禁用操作系统监督计时器。

注: 当监督器确认系统停止响应时，“自动系统恢复”操作可能不会完全按超时期限（n 秒）运行。操作执行时间范围介于 n-h+1 至 n+1 秒，其中 n 是超时期限，而 h 是心跳间隔。心跳间隔值在 n ≤ 30 时是 7 秒，在 n > 30 时是 15 秒。

注: 在系统 DRAM Bank_1 中出现不可纠正内存事件时无法保证监督计时器的功能。如果在此位置出现不可纠正内存事件，则可能是位于此处的 BIOS 代码损坏。由于监督功能使用对 BIOS 的调用来影响关闭系统或重新启动行为，此功能可能运行不正常。如果发生这种情况，必须手动重新启动系统。监督计时器的时间限制最多可设置为 720 秒。

关机

子选项卡：远程关机 | 热关机 | Web Server 关机

在**关机**选项卡下，您可以：

- 配置操作系统关机和远程关机选项
- 设置热关机严重性级别以便在温度传感器发回警告或故障时关闭系统。

注: 只有在传感器报告的温度高于温度阈值时，才会发生热关机。如果传感器报告的温度低于温度阈值，不会发生热关机。

- 关闭 DSM SA 连接服务（Web Server）。

注: DSM SA 连接服务关闭时，Server Administrator 通过命令行界面 (CLI) 仍可用。CLI 功能不需要运行 DSM SA 连接服务。

日志

子选项卡：硬件 | 警报 | 命令

在**日志**选项卡下，您可以：

- 查看嵌入式系统管理 (ESM) 日志或系统事件日志 (SEL)，以获得与系统硬件组件有关的所有事件列表。当日志文件达到 80% 的容量时，日志名称旁的状态标志图标会从正常状态 () 更改为非严重状态 ()。在 Dell PowerEdge 11G 系统上，当日志文件达到 100% 的容量时，日志名称旁边的状态标志图标将变为严重状态 ()。

  注: 通过启用自动备份并清除 ESM 日志条目功能，可为 ESM 日志创建自动备份。此功能仅可用于第 10 代和第 11 代 PowerEdge 服务器。从第 12 代 PowerEdge 服务器和更高版本开始，iDRAC 提供了自动备份和 SEL 日志清除功能。所提及的位置中仅提供最新版本的 XML 备份文件。
- 查看警报日志，以获得因响应传感器状态更改和其他被监测参数更改而由 Server Administrator Instrumentation Service 生成的所有事件的列表。

  注: 有关每个警报事件 ID 和相应的说明、严重性级别和原因的更多信息，请参阅 dell.com/openmanagemanuals 上的 *Server Administrator Messages Reference Guide*（Server Administrator 消息参考指南）。
- 查看命令日志，以获得在 **Server Administrator** 主页或其命令行界面运行过的所有命令的列表。

  注: 有关查看、打印、保存和电子邮件日志的说明，请参阅“Server Administrator 日志”。

警报管理

子选项卡：警报措施 | 平台事件 | SNMP 陷阱

在**警报管理**选项卡下，您可以：

- 查看当前警报措施设置，并设置当系统组件传感器返回警告或故障值时您希望系统执行的警报措施。
- 查看当前“平台事件筛选器”设置，并设置当系统组件传感器返回警告或故障值时您希望系统执行的平台事件筛选措施。 也可以使用**配置目标**选项选择平台事件警报要发送到的目标（IPv4 或 IPv6 地址）。

  注: Server Administrator 将不会在图形用户界面中显示 IPv6 地址的范围 ID。
- 查看当前 SNMP 陷阱警报阈值并为配备工具的系统组件设置警报阈值级别。 如果系统生成属于所选严重性级别的相应事件，则将触发选定的陷阱。
  - **SNMP 测试陷阱**可从显示的已配置目标列表发送陷阱到选定的目标。应当安装 Server Administrator SNMP 组件，才能发送测试陷阱。管理员应在操作系统 SNMP 服务或配置文件中配置 IP 地址/ FQDN，以便获取陷阱目标列表。

    注: VMware ESXi 不支持这项功能。
  - **启用 SNMP 陷阱**支持通过复选框和单选按钮来配置组件的设置。选中单选按钮会改变相应复选框的状态，而取消选中单选按钮同样会改变相应复选框的状态。

  注: 即使系统中不存在该组件传感器，警报操作窗口中也会列出所有可能存在的系统组件传感器的警报操作。为系统中不存在的系统组件传感器设置的警报操作无效。

  注: 在任何 Microsoft Windows 操作系统上，必须禁用操作系统中的高级系统设置 > 高级恢复选项，以确保生成 Server Administrator 自动系统恢复警报。

会话管理

子选项卡：会话

在**会话管理**选项卡下，您可以：

- 查看已登录到 Server Administrator 的当前用户的会话信息。
- 终止用户会话。

注：只有具有管理员权限的用户可以查看会话管理页及终止已登录用户的会话。

主系统机箱或主系统

单击**主系统机箱**或**主系统**对象以管理系统的重要硬件和软件组件。

可用的组件有：

- 电池
- BIOS
- 风扇
- 固件
- 硬件性能
- 侵入
- 内存
- 网络
- 端口
- 电源管理
- 电源
- 处理器
- 远程访问
- 可移除闪存介质
- 插槽
- 温度
- 电压

注：电源选项在 PowerEdge 1900 中不可用。电源监测和电源监测功能仅适用于安装有两个或多个冗余热插拔电源设备的系统。对于缺乏电源管理电路的、永久安装的非冗余电源，这些功能不可用。

主系统机箱或主系统属性

系统/服务器模块可能包含一个主系统机箱或多个机箱。主系统机箱/主系统包含系统的重要组件。**主系统机箱/主系统**对象操作窗口包括以下内容：

属性

子选项卡：运行状况 | 信息 | 系统组件 (FRU) | 前面板

在**属性**选项卡下，您可以：

- 查看硬件组件和传感器的运行状况或状态。每个列出的组件在其名称旁有系统/服务器模块组件状态指示器图标。表示组件运行状况良好（正常）。表示组件处于警告（不严重）状态并需要及时关注。表示组件处在故障（严重）状况下，需要立即关注。表示组件的运行状况未知。可用的受监测组件包括：
  - 电池
  - 风扇
  - 硬件日志
  - 侵入
  - 网络
  - 电源管理
  - 电源设备
  - 处理器
  - 温度
  - 电压

注: 电池仅在第 10 代 PowerEdge 系统上受支持。PowerEdge 1900 不提供电源。Power Management 仅在有限的第 10 代 PowerEdge 系统上受支持。电源设备监测和电源监测功能仅适用于安装有两个或多个冗余热插拔电源的系统。对于缺乏电源管理电路的、永久安装的非冗余电源，这些功能不可用。

注: 如果在第 12 代 PowerEdge 系统上安装了 QLogic QLE2460 4Gb 单端口光纤信道 HBA、QLogic QLE2462 4Gb 双端口光纤信道 HBA、Qlogic QLE2562 双端口 FC8 适配器或 Qlogic QLE2560 单端口 FC8 适配器卡，将不显示系统组件 (FRU) 屏幕。

- 查看关于主系统机箱属性的信息，例如：主机名称、iDRAC 版本、Lifecycle Controller 版本、机箱型号、机箱锁定、机箱服务标签、快速服务代码和机箱资产标签。快速服务代码 (ESC) 属性完全由系统服务标签的 11 位数字转换而来。当致电 Dell EMC 技术支持时，您可以键入快速服务代码进行自动呼叫路由。
- 查看有关系统中安装的现场可更换单元 (FRU) 的详细信息（在**系统组件** (**FRU**) 子选项卡下）。
- 启用或禁用受管系统的前面板按钮，即电源按钮和非屏蔽中断 (NMI) 按钮（如果系统上有）。此外，选择受管系统的 LCD 安全访问级别。可以从下拉菜单中选择受管系统的 LCD 信息。还可以从**前面板**子选项卡启用远程 KVM 指示会话。

电池

单击**电池**对象查看有关系统所装电池的信息。当系统关闭时，电池维持其日期和时间。电池保存系统的 BIOS 设置信息，从而使系统有效地重新引导。根据用户组权限的不同，电池对象操作窗口可包含以下选项卡：**属性**和**警报管理**。

属性

子选项卡：电池

在**属性**选项卡下，您可以查看系统电池的当前读数和状况。

警报管理

子选项卡：警报操作 | SNMP 陷阱

在**警报管理选项卡**下，您可以：

- 查看当前警报操作设置。
- 配置在电池出现警告或严重/故障事件时希望生成的警报。

BIOS

单击 **BIOS** 对象以管理系统 BIOS 的主要功能。系统的 BIOS 包含存储在闪存存储器芯片组中的程序，这些程序控制着微处理器和外围设备（例如键盘和视频适配器）之间的通信以及其他各种功能（例如系统消息）。根据用户的组权限不同，**BIOS** 对象操作窗口可具有以下选项卡：

属性和**设置**

属性

子选项卡：信息

在**属性**选项卡下，您可以查看 BIOS 信息。

设置

子选项卡：BIOS

注: 您系统上的“BIOS 设置”选项卡只显示系统上支持的 BIOS 功能。

在**设置**选项卡下，可以设置每个 BIOS 设置对象的状态。

您可以修改多个 BIOS 设置功能的状态，这些功能包括（但不限于）串行端口、硬盘驱动器顺序、用户可访问 USB 端口、CPU 虚拟化技术、CPU 超线程、交流电恢复模式、嵌入式 SATA 控制器、系统配置文件、控制台重定向和控制台重定向故障自动保护波特率。您还可以配置内部 USB 设备、光盘驱动器控制器设置、自动系统恢复 (ASR) 监督计时器、嵌入式虚拟机监控程序和主板上其他 LAN 网络端口的信息。不仅如此，您还可以查看可信平台模块 (TPM) 和可信加密模块 (TCM) 的设置。

根据特定系统配置的情况，可能显示其他的设置项。但是，某些 BIOS 设置选项可能显示在 BIOS 设置屏幕中，它在 Server Administrator 中却不可访问。

在第 12 代 PowerEdge 及更高版本的系统上，可配置的 BIOS 功能按特定的类别分组。这些类别包括调试菜单、系统信息、内存设置、处理器设置、SATA 设置、引导设置、引导选项设置、一次性引导、网络设置、集成设备、插槽禁用、串行通信、系统配置文件设置、系统安全以及其他设置。例如，在**系统 BIOS 设置**页面上，如果单击**内存设置**链接，将显示与系统内存相关的功能。您可以导航到相应的类别来查看或修改设置。

注: 第 13 代 PowerEdge 系统不支持“一次性引导”类别。

可配置的 BIOS 功能按特定的类别分组。这些类别包括调试菜单、系统信息、内存设置、处理器设置、SATA 设置、引导设置、引导选项设置、网络设置、集成设备、插槽禁用、串行通信、系统配置文件设置、系统安全以及其他设置。例如，在**系统 BIOS 设置**页面上，如果单击**内存设置**链接，将显示与系统内存相关的功能。您可以导航到相应的类别来查看或修改设置。

您可以在**系统安全**页面上设定“BIOS 设置”密码。如果已设定“BIOS 设置”的密码，请输入此密码以启用和修改 BIOS 设置。此外，BIOS 设置将以只读模式显示。设置密码后必须重新启动系统。

如果上一会话存在待处理的值或者从带外接口禁用了带内配置，Server Administrator 将不允许配置 BIOS 设置。

注: Server Administrator BIOS 设置中的 NIC 配置信息对于嵌入式 NIC 来说可能不准确。使用 BIOS 设置屏幕启用或禁用 NIC 可能会产生无法预料的结果。建议通过实际的“系统设置”屏幕（在系统引导期间按 <F2> 获得）执行所有的嵌入式 NIC 配置。

完整的电源关闭后重启 - 此新功能将允许服务器管理员使用 OpenManage GUI 或 CLI 对设备执行电源关闭后重启操作。**完整的电源关闭后重启**允许管理员先后执行直流电源关闭后重启和交流电源关闭后重启。

直流电源关闭后重启 - 重新启动服务器，但不中断辅助设备。
交流电源关闭后重启 - 重新启动辅助设备并将用户连接到服务器。

完整的电源关闭后重启包括以下设备的电源关闭后重启：

- 服务器

- BMC/iDRAC
- CPLD
- 传感器
- LCD
- 现场可更换部件
- Titan
- 网络子卡

虚拟交流电源关闭后重启

要设置虚拟交流电源关闭后重启：

1 在 Server Administrator 窗口中，展开**系统** > **主系统机箱**。
2 单击 **BIOS**。
此时会显示 **BIOS 属性**窗口。
3 单击**设置**选项卡。
此时会显示**系统 BIOS 设置**窗口。
4 单击**其他设置**链接。
5 在**电源关闭后重启请求**下，选择**虚拟交流电源**。
6 单击**应用**。

注: 重新启动服务器以成功更改电源关闭后重启设置。

风扇

单击**风扇**对象可以管理系统的风扇。Server Administrator 可以通过测量风扇 RPM 监测每个系统风扇的状况。风扇探测器向 Server Administrator Instrumentation Service 报告 RPM。

从设备树中选择风扇后，Server Administrator 主页右侧窗格的数据区中将显示详细信息。根据用户组权限的不同，风扇对象操作窗口可包含以下选项卡：**属性**和**警报管理**。

属性

子选项卡：风扇探测器

在**属性**选项卡下，您可以：

- 查看系统风扇探测器的当前读数并配置风扇探测器最大和最小警告阈值。

注: 根据系统具有的固件类型（例如：BMC 或 ESM），某些风扇探测器字段会有所不同。有些阈值在基于 BMC 的系统上是不可编辑的。

- 选择风扇控制选项。

警报管理

子选项卡：警报操作 | SNMP 陷阱

在**警报管理**选项卡下，您可以：

- 查看当前警报措施设置，并设置风扇返回警告或故障值时您希望系统执行的警报措施。
- 设置风扇的警报阈值级别。

固件

单击**固件**对象管理系统固件。固件由已写入 ROM 的程序或数据组成。固件可以引导和操作设备。每个控制器均包含有助于提供控制器功能的固件。根据用户的组权限不同，**固件**对象操作窗口可具有以下选项卡：**属性**。

属性

子选项卡：信息

在**属性**选项卡下，您可以查看系统的固件信息。

硬件性能

单击**硬件性能**对象查看状况以及造成系统性能降级的原因。根据用户组权限的不同，**硬件性能**对象操作窗口可包含以下选项卡：**属性**。

属性

子选项卡：信息

在**属性**选项卡下，可以查看系统性能降级的详情。

下表列出可能的状况值和探测原因：

表. 10: 可能的状况值和探测原因

状况值	原因值
降级	用户配置 功率不足 未知原因
正常	不适用

侵入

单击**侵入**对象管理系统的机箱侵入状况。作为一项安全措施，Server Administrator 将监测系统的机箱侵入状况，以防止未经授权的用户访问系统的关键组件。机箱侵入表明有人正在打开或已经打开系统机箱盖。根据用户组权限的不同，**侵入**对象操作窗口可包含以下选项卡：**属性**和**警报管理**

属性

子选项卡：侵入

在**属性**选项卡下，您可以查看机箱侵入状况。

警报管理

子选项卡：警报操作 | SNMP 陷阱

在**警报管理**选项卡下，您可以：

- 查看该当前警报措施设置，并设置侵入传感器返回警告或故障值时您希望系统执行的警报措施。
- 查看该当前 SNMP 陷阱警报阈值并为侵入传感器设置警报阈值级别。如果系统生成属于所选严重性级别的相应事件，则将触发选定的陷阱。

内存

单击**内存**对象管理系统的内存设备。Server Administrator 可以监测所监测系统中每个内存模块的内存设备状态。内存设备预故障传感器通过计算 ECC 内存校正数来监测内存模块。如果您的系统支持内存冗余功能，Server Administrator 还可以监测内存冗余信息。根据用户组权限的不同，**内存**对象操作窗口可包含以下选项卡：**属性**和**警报管理**。

属性

子选项卡：内存

在**属性**选项卡下，可以查看内存冗余状况、内存阵列属性、内存阵列总容量、内存阵列详情、内存设备详情、以及内存设备状况。内存设备详情提供连接器上内存设备的详细情况，例如，状态、设备名称、大小、类型、速度、列，以及故障。列为一行动态随机访问存储器 (DRAM) 设备，其中每个双列直插式内存模块 (DIMM) 包含 64 位数据。列的可能值为 `single`, `dual`, `quad`, `octal`,（单、双、四、八）和 `hexa`（十六）。列显示 DIMM 的列并有助于轻松维护服务器上的 DIMM。

注: 如果启用了备用内存区的系统进入了 冗余丢失状态，那么可能并不容易看出是哪个内存模块的问题。如果无法确定要更换哪个 DIMM，请参阅 ESM 系统日志中的“检测到 *切换*至备用内存区”日志条目，以找出是哪个内存模块出现了故障。

警报管理

子选项卡：警报操作 | SNMP 陷阱

在**警报管理**选项卡下，您可以：

- 查看该当前警报措施设置，并设置内存模块返回警告或故障值时您希望系统执行的警报措施。
- 查看该当前 SNMP 陷阱警报阈值并为内存模块设置警报阈值级别。如果系统生成属于所选严重性级别的相应事件，则将触发选定的陷阱。

网络

单击**网络**对象以管理系统的 NIC。Server Administrator 可以监测系统中每个 NIC 的状态，以确保持续的远程连接。Server Administrator 报告 NIC 的 FCoE 和 iSoE 功能。此外还会报告 NIC 组队详细信息（如果已在系统上进行了配置）。两个或多个物理 NIC 可以组成单个逻辑 NIC，管理员可以为其分配 IP 地址。通过使用 NIC 供应商工具可以配置组队。例如，Broadcom - BACS。如果一个物理 NIC 出现故障，此 IP 地址仍然可以访问，因为它绑定到逻辑 NIC，而不是单个物理 NIC。如果配置了组队接口，将显示详细的组队属性。如果物理 NIC 是组队接口的成员，还会报告这些物理 NIC 和组队接口之间的关系，反之亦然。

在 Windows2008 虚拟机监管程序操作系统上，Server Administrator 不会报告用于分配虚拟机 IP 的物理 NIC 端口的 IP 地址。

注: 不保证设备的检测顺序与设备的物理端口顺序一致。 单击“接口名称”下面的超链接可查看 NIC 信息。

在 ESXi 操作系统中，网络设备被视为一个组。例如，由服务控制台 (vswif) 使用的虚拟以太网接口，以及由 ESXi 上的 vmknic 设备使用的虚拟网络接口。

注: 服务器管理员仅支持物理网络接口的资源清册及其属性。Server Administrator 不支持逻辑接口（如 VLAN 和绑定）的资源清册。

根据用户组权限的不同，**网络**对象操作串口可具有以下选项卡：**属性**。

属性

子选项卡：信息

在**属性**选项卡下，可以查看有关系统中安装的物理 NIC 接口以及组接口的信息。

注: 在“IPv6 地址”部分中，除了链路本地地址外，Server Administrator 仅显示两个地址。

注: 在运行 Linux 操作系统且内核版本早于 3.10 版的系统上，组队接口速度不会显示。

端口

单击**端口**对象以管理系统的外部端口。Server Administrator 监测系统中现有的每个外部端口的状况。

注: Server Administrator 不枚举连接刀片服务器的 CMC USB 端口。

根据用户的组权限不同，**端口**对象操作窗口可具有以下选项卡：**属性**。

子选项卡：信息

属性

在**属性**选项卡下，您可以查看有关系统内部和外部端口的信息。

Power Management（电源管理）

注: 电源设备监测和电源监测功能仅适用于安装有两个或多个冗余热插拔电源设备的系统。对于缺乏电源管理电路的、永久安装的非冗余电源设备，这些功能不可用。

监测

子选项卡：消耗 | 统计信息

在**消耗**选项卡下，可以查看并管理系统的“功耗”信息，单位为瓦特和 BTU/小时。

BTU/小时 = 瓦特 X 3.413（数值舍入为最接近的整数值）

Server Administrator 监测电源消耗状况、安培数并跟踪电源统计详细信息。

还可以查看“系统瞬间余量”和“系统峰值余量”。这些值同时以瓦特和 BTU/小时（英制热量单位）为单位显示。功率阈值可以按瓦特和 BTU/小时设置。

“统计信息”选项卡使用户能够查看并重设系统功率跟踪统计信息，比如能耗、系统峰值功率和系统峰值安培。

管理

子选项卡：预算 | 配置文件

预算选项卡使用户能够查看“功率资源清册”属性，比如“系统空闲功率”和“系统最大潜在功率（瓦特和 BTU/小时）”。还可以使用“功率预算”选项为系统“启用功率限额”和设置“功率限额”。

配置文件选项卡使用户能够选择功率配置文件来尽量提高系统性能并节约能源。

警报管理

子选项卡：警报操作 | SNMP 陷阱

使用**警报措施**选项卡设置各种系统事件警报措施，比如“系统功率探测器警报”和“系统峰值功率”。

使用 **SNMP 陷阱**选项卡为系统配置 SNMP 陷阱。

有些“电源管理”功能只在启用了“电源管理总线 (PMBus)”的系统上可用。

电源设备

单击**电源设备**对象可管理系统的电源设备。Server Administrator 可以监测电源设备的状况（包括冗余），以确保系统中的每个电源设备都能正常运转。

根据用户组权限的不同，“电源设备”对象操作窗口可包含以下选项卡：**属性**和**警报管理**。

注: 电源设备监测和电源监测功能仅适用于安装有两个或多个冗余热插拔电源设备的系统。 对于缺乏电源管理电路的、永久安装的非冗余电源设备，这些功能不可用。

属性

子选项卡：要素

在**属性**选项卡下，您可以：

- 查看有关电源设备冗余属性的信息。
- 检查各个电源元件的状态，包括电源设备的固件版本和最大输出功率。
- 检查各个电源元件的状态，包括电源的固件版本、额定输入功率和最大输出功率。 “额定输入功率”属性只在 11G 和版本更高的 PMBus 系统上显示。

警报管理

子选项卡：警报操作 | SNMP 陷阱

在警报管理选项卡下，您可以：

- 查看当前警报操作设置，并设置系统电源返回警告或故障值时您希望系统执行的警报操作。
- 配置 IPv6 地址平台事件警报目标。
- 查看当前 SNMP 陷阱警报阈值并为系统功率设置警报阈值级别。如果系统生成属于所选严重性级别的相应事件，则将触发选定的陷阱。

注: “系统峰值功率”陷阱将只生成严重性为通知的事件。

处理器

单击**处理器**对象管理系统的微处理器。处理器是系统中的主要计算芯片，用于控制算术函数和逻辑函数的解释和执行。根据用户组权限的不同，处理器对象操作窗口可包含以下选项卡：**属性**和**警报管理**。

子选项卡：信息

属性

在**属性**选项卡下，您可以查看有关系统微处理器的信息，也可以查看有关高速缓存的详细信息。

警报管理

子选项卡：警报措施

在**警报管理**选项卡下，可以查看当前警报措施设置，并设置处理器返回警告或故障值时您希望系统执行的警报措施。

远程访问

单击**远程访问**对象以管理 Baseboard Management Controller (BMC) 或 Integrated Dell Remote Access Controller (iDRAC) 功能和 Remote Access Controller 功能。

选择“远程访问”选项卡可以管理 BMC/iDRAC 功能，比如 BMC/iDRAC 上的一般信息。 也可以管理局域网 (LAN) 上的 BMC/iDRAC 配置、BMC/iDRAC 的串行端口、串行端口的终端模式设置、LAN 上串行连接的 BMC/iDRAC 和 BMC/iDRAC 用户。

注: 如果在 Server Administrator 正在运行时使用 Server Administrator 之外的应用程序配置 BMC/iDRAC，则由 Server Administrator 显示的 BMC/iDRAC 配置数据可能与 BMC/iDRAC 不同步。 建议在 Server Administrator 正在运行时使用 Server Administrator 配置 BMC/iDRAC。

DRAC 使用户可以访问系统的远程系统管理功能。 Server Administrator DRAC 可以远程访问未运行的系统、在系统停机时发出警报通知以及重新启动系统。

根据用户的组权限不同，**远程访问**对象操作窗口可包含以下选项卡：**属性**、**配置**和**用户**。

子选项卡：信息

属性

在**属性**选项卡下，可以查看远程访问设备的常规信息。还可以查看 IPv4 和 IPv6 地址的属性。

单击**重设为默认值**可以将所有属性重设为系统默认值。

子选项卡：LAN | 串行端口 | LAN 上串行 | 附加配置

配置

在已配置 BMC/iDRAC 的情况下，可以在配置选项卡下配置 LAN 上的 BMC/iDRAC、BMC/iDRAC 的串行端口和 LAN 上串行连接的 BMC/iDRAC。

注: 附加配置选项卡仅在安装了 iDRAC 的系统上可用。

配置 DRAC 后，可在**配置**选项卡下配置网络属性。

在**附加配置**选项卡下，可以启用或禁用 IPv4/IPv6 属性。

注: 仅在双堆栈环境（IPv4 和 IPv6 堆栈均载入）中启用/禁用 IPv4/IPv6。

用户

子选项卡：用户

在**用户**选项卡下，您可以修改远程访问用户配置。您可以添加、配置和查看有关 Remote Access Controller 用户的信息。

可移除闪存介质

单击**可移动闪存介质**对象以查看内部 SD 模块和 vFlash 介质的运行状况和冗余状态。 “可移动闪存介质”操作窗口具有**属性**选项卡。

属性

子选项卡：信息

在**属性**选项卡下，可以查看有关可移动闪存介质和内部 SD 模块的信息。这包括有关“连接器名称”、其状态以及存储大小的详细信息。

警报管理

子选项卡：警报操作 | SNMP 陷阱

在**警报管理**选项卡下，您可以：

- 查看当前警报措施设置，并设置可移动闪存介质探测器返回警告或故障值时您希望系统执行的警报措施。

- 查看当前 SNMP 陷阱警报阈值，并为可移动闪存介质探测器设置警报阈值级别。如果系统生成属于所选严重性级别的相应事件，则将触发选定的陷阱。

警报管理为内部 SD 模块和 vFlash 所共用。 为 SD 模块配置警报措施/SNMP/PEF 将自动为 vFlash 配置这些内容，为 vFlash 配置警报措施/SNMP/PEF 将自动为 SD 模块配置这些内容。

插槽

单击**插槽**对象，可以管理系统板上用于插入印刷电路板（例如扩充卡）的连接器或插孔。插槽对象操作窗口具有**属性**选项卡。

属性

子选项卡：信息

在**属性**选项卡下，您可以查看有关各个插槽和安装的适配器的信息。

温度

单击**温度**对象可以管理系统温度，以防止系统内部组件因过热而损坏。Server Administrator 可以监测系统机箱内各个位置的温度，以确保机箱内部温度不会变得太高。

根据用户组权限的不同，**温度**对象操作窗口会显示以下选项卡：**属性**和**警报管理**。

子选项卡：温度探测器

在**属性**选项卡下，您可以查看系统温度探测器的当前读数和状态，以及配置温度探测器警告的最小和最大阈值。

注: 根据系统具有的固件类型（例如：BMC 或 ESM），某些温度探测器字段会有所不同。有些阈值在基于 BMC 的系统上是不可编辑的。分配探测器阈值时，Server Administrator 有时会将您输入的最小或最大值舍入为最接近的可分配值。

警报管理

子选项卡：警报操作 | SNMP 陷阱

在**警报管理**选项卡下，您可以：

- 查看该当前警报措施设置，并设置温度探测器返回警告或故障值时您希望系统执行的警报措施。
- 查看该当前 SNMP 陷阱警报阈值，并为温度探测器设置警报阈值级别。如果系统生成属于所选严重性级别的相应事件，则将触发选定的陷阱。

注: 仅可以将外部机箱的最小和最大温度探测器阈值设置为整数。 如果尝试将最小或最大温度探测器阈值设置为包含小数的数字，则只有小数位前的整数被保存为阈值设置。

电压

单击**电压**对象管理系统中的电压级别。Server Administrator 可以监测机箱内各处关键组件的电压。根据用户组权限的不同，**电压**对象操作窗口可包含以下选项卡：**属性**和**警报管理**。

属性

子选项卡：电压探测器

在**属性**选项卡下，您可以查看系统电压探测器的当前读数和状态，以及配置电压探测器警告阈值的最小和最大值。

注: 根据系统具有的固件类型（BMC 或 ESM），某些电压探测器字段会有所不同。有些阈值在基于 BMC 的系统上是不可编辑的。

警报管理

子选项卡：警报操作 | SNMP 陷阱

在**警报管理**选项卡下，您可以：

- 查看该当前警报措施设置，并设置当系统电压传感器返回警告或故障值时您希望系统执行的警报措施。
- 查看该当前 SNMP 陷阱警报阈值并为电压传感器设置警报阈值级别。如果系统生成属于所选严重性级别的相应事件，则将触发选定的陷阱。

软件

单击**软件**对象，则可以查看管理系统的重要软件组件（例如操作系统和系统管理软件）的详细版本信息。根据用户组权限的不同，软件对象操作窗口可包含以下选项卡：**属性**。

子选项卡：摘要

属性

在**属性**选项卡下，您可以查看所监测系统的操作系统和系统管理软件的摘要信息。

操作系统

单击**操作系统**对象，则可以查看有关操作系统的基本信息。依据用户的组权限，操作系统对象操作窗口可具有以下选项卡：**属性**。

属性

子选项卡：信息

在**属性**选项卡下，您可以查看有关操作系统的基本信息。

存储

Server Administrator 提供了 Storage Management Service：

Storage Management Service 提供了用于配置存储设备的功能。大多数情况下，使用**典型安装**安装 Storage Management Service。Storage Management Service 在 Microsoft Windows、Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统上可用。

当安装了 Storage Management Service 时，单击**存储**对象可以查看各种所连阵列存储设备、系统磁盘等的状态和设置。

在 Storage Management Service 中，根据用户组权限的不同，存储对象操作窗口可包含以下选项卡：**属性**。

属性

子选项卡：运行状况

在**属性**选项卡下，您可以查看连接的存储设备组件和传感器（如阵列子系统、操作系统磁盘和卷）的运行状况或状况。

管理首选项主页配置选项

首选项主页的左窗格（在 Server Administrator 主页上显示系统树）将显示系统树窗口中的所有可用配置选项。显示的选项基于管理系统上安装的系统管理软件。

首选项主页的可用配置选项如下：

- 常规设置
- 服务器管理员

常规设置

单击**常规设置**对象使您能够为所选的 Server Administrator 功能设置用户和 DSM SA 连接服务 (Web Server) 首选项。根据用户组权限的不同，“常规设置”对象操作窗口可包含以下选项卡：**用户**和 **Web Server**。

子选项卡：属性

用户

在**用户**选项卡下，您可以设置用户首选项，例如主页外观和**电子邮件**按钮的默认电子邮件地址。

- **Web Server**
- **子选项卡：属性 | X.509 认证**

在 Web Server 选项卡下，您可以：

- 设置 DSM SA 连接服务首选项。有关配置服务器首选项的说明，请参阅 Dell EMC 系统管理服务器管理连接服务和安全设置。
- 配置 SMTP 服务器地址并以 IPv4 或 IPv6 寻址模式绑定 IP 地址。
- 执行 X.509 证书管理的方式有：生成新的 X.509 证书、重新使用现有的 X.509 证书，或导入来自认证机构 (CA) 的证书链。有关证书管理的更多信息，请参阅 X.509 证书管理。

服务器管理员

单击 **Server Administrator** 对象使您能够启用或禁用具有“用户”或“高级用户”权限的那些用户的访问。根据用户组权限的不同，**Server Administrator** 对象操作窗口可包含以下选项卡：**首选项**。

子选项卡：访问配置

首选项

在**首选项**选项卡下，您可以启用或禁用具有“用户”或“高级用户”权限的那些用户的访问。

5

Server Administrator 日志

Server Administrator 使您可以查看和管理硬件、警报和命令日志。所有用户均可以通过 Server Administrator 主页或其命令行界面查看日志并打印报告。用户必须以“管理员”权限登录才能清除日志，或者必须以“管理员”或“高级用户”权限登录才能将日志通过电子邮件发送给指定的服务联络人。

有关通过命令行查看日志和创建报表的信息，请参阅 **dell.com/openmanagemanuals** 上的 *Server Administrator Command Line Interface Guide*（Server Administrator 命令行界面指南）。

查看 Server Administrator 日志时，您可以单击**帮助**（  ），以获得有关您正在查看的特定窗口的详细信息。用户可查看的所有窗口（取决于用户权限级别和 Server Administrator 在受管系统中查找到的特定硬件和软件组）均可使用 Server Administrator 日志帮助。

主题：

集成功能

单击列标题可按该列进行排序或更改该列的排序方向。 此外，每个日志窗口均包含若干任务按钮，用于管理和支持您的系统。

日志窗口任务按钮

下表列出了“日志”窗口任务按钮。

表. 11: 日志窗口任务按钮

名称	说明
打印	要打印一份日志到默认打印机。
导出	要将含有日志数据的文本文件（各个数据字段的值由可自定义分隔符隔开）保存到指定目的地。
电子邮件	要创建包含日志内容（作为附件）的电子邮件信息。
Clear Log（清除日志）	要删除日志中的所有事件。
另存为	要将日志内容保存在 .zip 文件中。
刷新	要在操作窗口数据区域中重新载入日志内容。

注: 有关使用任务按钮的其他信息，请参阅任务按钮。

Server Administrator 日志

Server Administrator 提供以下日志：

- 硬件日志
- 警报日志
- 命令日志

硬件日志

在第 11 代 PowerEdge 系统上，使用硬件日志可查找系统硬件组件的潜在问题。硬件日志状态标志将在日志文件达到 100% 的容量时变为严重状态 ()。硬件日志有两种（视您的系统而定）：嵌入式系统管理 (ESM) 日志和系统事件日志 (SEL)。ESM 日志和 SEL 均为一组嵌入式指令，可以向系统管理软件发送硬件状态消息。日志中列出的每个组件的名称旁边均有一个状态标志图标。下表列出了状态标志。

表. 12: 硬件日志状态标志

状态	说明
绿色复选标记 ()	表示组件运行状况良好（正常）。
包含感叹号的黄色三角形 ()	表示组件处于警告（不严重）状态并需要及时关注。
红色的 X ()	表示组件处在故障（严重）状态下，需要立即关注。
问号 ()	表示组件的运行状况未知。

要访问命令日志，请单击**系统**，单击**日志**选项卡，然后单击**硬件**。

ESM 和 SEL 日志中显示的信息包括：

- 事件的严重性级别
- 捕获事件的日期和时间
- 事件说明

维护硬件日志

Server Administrator 主页上日志名称旁的状况标志图标会从正常状况 () 更改为非严重状态  前提是当日志文件达到 80% 的容量时。请确保在硬件日志达到 80% 的容量时清除日志。如果日志允许达到 100% 的容量，最新的事件将记录不到日志中。

要清除硬件日志，请在**硬件日志**页面上单击**清除日志**链接。

警报日志

注: 如果警报日志显示无效的 XML 数据（例如，当为选项生成的 XML 数据没有很好形成时），可以单击清除日志，之后重新显示日志信息。

注: 警报日志文件的大小受到限制。要捕获最大警报日志，应启用所有操作系统日志筛选器。

使用警报日志可以监测各种不同的系统事件。Server Administrator 生成事件以响应传感器状况的更改和其他受监测参数的更改。警报日志中记录的每个状况更改事件均由特定事件源类别的唯一标识符（称为事件 ID）和事件消息（用于说明事件）组成。事件 ID 和事件消息提供对事件严重性和事件起因的唯一说明，并提供其他相关信息，例如事件的位置和受监测组件的先前状况。

要访问警报日志，请单击**系统**，单击**日志**选项卡，然后单击**警报**。

警报日志中显示的信息包括：

- 事件的严重性级别
- 事件 ID
- 捕获事件的日期和时间
- 事件的类别
- 事件说明

注：以后排除故障和进行诊断时可能需要日志历史记录。因此，建议您保存日志文件。

注：OMSA 可能会在警报日志页或操作系统日志文件中发送重复的 SNMP 陷阱或记录重复的事件。在操作系统重新引导后手动重新启动 OMSA 服务时，或设备传感器在 OMSA 服务启动后仍表示非正常状态时，都会记录重复的陷阱和事件。

有关警报消息的详细信息，请参阅 **dell.com/openmanagemanuals** 上的 *Server Administrator Messages Reference Guide*（Server Administrator 消息参考指南）。

命令日志

注：如果命令日志显示无效的 XML 数据（例如，当为选项生成的 XML 数据没有很好形成时），可以单击清除日志，之后重新显示日志信息。

使用命令日志可监测 Server Administrator 用户发出的所有命令。命令日志可以跟踪登录、注销、系统管理软件初始化和通过系统管理软件进行的关闭系统操作，并记录上次清除日志的时间。命令日志文件的大小可根据您的需要指定。

要访问命令日志，请单击**系统**，单击**日志**选项卡，然后单击**命令**。

命令日志中显示的信息包括：

- 调用命令的日期和时间
- 当前登录至 Server Administrator 主页或 CLI 的用户
- 命令及其相关值的说明

注：以后排除故障和进行诊断时可能需要日志记录。 因此，建议您保存日志文件。

6

使用 Remote Access Controller

系统 Baseboard Management Controller (BMC)/Integrated Dell Remote Access Controller (iDRAC) 通过与系统板上的各个传感器进行通信来监测系统是否发生严重事件，并在某些参数超出预置阈值时发送警报和日志事件。BMC/iDRAC 支持工业标准的智能平台管理界面 (IPMI) 规范，可让您远程配置、监测和恢复系统。

注: Integrated Dell Remote Access Controller (iDRAC) 在第 10 代 PowerEdge 和更高版本的系统上受支持。

DRAC 是一种系统管理硬件和软件解决方案，专门用于为系统提供远程管理功能、崩溃系统恢复和电源控制功能。

通过与系统的 Baseboard Management Controller (BMC)/Integrated Dell Remote Access Controller (iDRAC) 通信，可以配置 DRAC，使其发送与电压、温度和风扇速度相关的警告或错误的电子邮件警报。DRAC 也会记录事件数据和最新故障屏幕（仅限运行 Microsoft Windows 操作系统的系统）来帮助诊断系统故障的可能原因。

Remote Access Controller 使您可以远程访问不能运行的系统，使其尽快启动并运行。Remote Access Controller 还可在系统停机时提供警报通知，并允许您远程重新启动系统。此外，Remote Access Controller 还将记录系统故障的可能原因并保存*最近一次的崩溃屏幕*。

您可以通过 Server Administrator 主页或使用支持的浏览器直接访问控制器的 IP 地址来登录至 Remote Access Controller。

使用 Remote Access Controller 时，单击**帮助**可以获得有关正在查看的特定窗口的详细信息。用户可查看的所有窗口（取决于用户权限级别和 Server Administrator 在受管系统中查找到的特定硬件和软件组）均可使用 Remote Access Controller 帮助。

注: 有关 BMC 的更多信息，请参阅 dell.com/systemsecuritymanuals 上的 *Dell EMC OpenManage Baseboard Management Controller User's Guide*（Dell EMC OpenManage Baseboard Management Controller 用户指南）。

注: 有关配置和使用 iDRAC 的详细信息，请参阅 dell.com/systemsecuritymanuals 上的 *Integrated Dell Remote Access Controller User's Guide*（Integrated Dell Remote Access Controller 用户指南）。

下表列出了在 Server Administrator 安装于系统后的图形用户界面 (GUI) 字段名称和适用的系统。

表. 13: GUI 字段名称和适用的系统

GUI 字段名称	适用的系统
模块化机柜	模块化系统
服务器模块	模块化系统
主系统	模块化系统
系统	非模块化系统
主系统机箱	非模块化系统

有关对远程访问设备的系统支持的更多信息，请参阅可在 **dell.com/openmanagemanuals** 上获得的 *Dell EMC Systems Software Support Matrix*（Dell EMC 系统软件支持值表）。

Server Administrator 允许远程、带内访问事件日志、电源控制和传感器状态信息，并提供配置 BMC/iDRAC 的能力。要通过 Server Administrator 图形用户界面 (GUI) 管理 BMC/iDRAC 和 DRAC，请单击**远程访问**对象，该对象为**主系统机箱/主系统**组的一个子组件。

可以执行以下任务：

- 查看基本信息

- 将远程访问设备配置为使用 LAN 连接
- 将远程访问设备配置为使用 LAN 上串行连接
- 配置远程访问设备使用串行端口连接
- iDRAC 的附加配置
- 配置远程访问设备用户
- 设置平台事件筛选器警报

可根据哪个硬件提供了对系统的远程访问功能来查看 BMC/iDRAC 或 DRAC 信息。

也可以使用 `omreport/omconfig chassis remoteaccess` 命令行界面 (CLI) 命令管理 BMC/iDRAC 和 DRAC 的报告和配置。

另外，可以使用 Server Administrator Instrumentation Service 管理平台事件筛选器 (PEF) 参数和警报目标。

主题：

- 查看基本信息
- 将远程访问设备配置为使用 LAN 连接
- 配置远程访问设备使用串行端口连接
- 将远程访问设备配置为使用 LAN 上串行连接
- iDRAC 的附加配置
- 配置远程访问设备用户
- 设置平台事件筛选器警报

查看基本信息

可以查看有关 BMC/iDRAC、IPv4 地址和 DRAC 的基本信息。还可以将 Remote Access Controller 设置重设为默认值。要执行此操作：

注: 您必须以“管理员”权限登录才能重设 BMC 设置。

单击**模块化机柜** > **系统/服务器模块** > **主系统机箱/主系统** > **远程访问**

远程访问 页显示以下系统 BMC 的基本信息：

远程访问设备

- 设备类型
- IPMI 版本
- 系统 GUID
- 可能活动的会话数
- 目前活动的会话数
- LAN 已启用
- SOL 已启用
- MAC 地址

IPv4 地址

- IP 地址源
- IP 地址
- IP 子网
- IP 网关

IPv6 地址

- IP 地址源
- IPv6 地址 1
- 默认网关
- IPv6 地址 2
- 链接本地地址
- DNS 地址源
- 首选 DNS 服务器
- 备用 DNS 服务器

注: 只有在远程访问选项卡的附加配置下启用 IPv4 和 IPv6 地址属性后，才能查看 IPv4 和 IPv6 地址详细信息。

将远程访问设备配置为使用 LAN 连接

要将远程访问设备配置为通过 LAN 连接进行通信，请执行以下操作：

1 单击**模块化机柜** > **系统/服务器模块** > **主系统机箱/主系统** > **远程访问**对象。
2 单击 **Configuration**（配置）选项卡。
3 单击 **LAN**。
LAN 配置窗口会出现。

注: 如果主板上的 LAN (LOM) 配有任何网络适配器外插卡，则 BMC/iDRAC 管理通信将不会正常工作。

4 指定以下 NIC 配置详细信息：
- 启用 NIC（选择此选项以进行 NIC 组对。）

注: 您的 DRAC 包含集成 10BASE-T/100BASE-T 以太网 NIC，并支持 TCP/IP。 NIC 的默认地址为 192.168.20.1，默认网关为 192.168.20.1。

注: 如果您为 DRAC 配置的 IP 地址与同一网络上另一个 NIC 的 IP 地址相同，则会出现 IP 地址冲突。DRAC 将停止响应网络命令，直至在 DRAC 上更改了 IP 地址。即使已通过更改其他 NIC 的 IP 地址解决了 IP 地址冲突问题，也必须重设 DRAC。

注: 更改 DRAC 的 IP 地址会使 DRAC 重设。由于在 DRAC 初始化之前没有传送正确的温度，因此如果 SNMP 在 DRAC 初始化之前轮询 DRAC，系统将记录温度警告。

- NIC 选择

注: 不能在模块化系统上配置 NIC 选择

注: “NIC 选择”选项仅在 11G 和更早的系统上可用。

- 主要网络和故障转移网络选项

对于 12G 系统，用于 Remote Management (iDRAC7) NIC 的主要网络选项包括：LOM1、LOM2、LOM3、LOM4 和 Dedicated (专用)。故障转移网络选项包括：LOM1、LOM2、LOM3、LOM4、All LOMs(所有 LOM) 和 None (无)。

注: Dedicated （专用）选项仅在 iDRAC7 Enterprise 许可证存在并且有效时可用。LOM 的数量因具体系统或硬件配置而异。

- 启用 LAN 上 IPMI
- IP 地址源
- IP 地址
- 子网掩码
- 网关地址

- 信道权限级别限制
- 新密钥

5 配置以下可选 VLAN 配置详细信息：

注: VLAN 配置在具有 iDRAC 的系统上不可用。

- 启用 VLAN ID
- VLAN ID
- 优先级

6 配置以下 IPv4 属性：

- IP 地址源
- IP 地址
- 子网掩码
- 网关地址

7 配置以下 IPv6 属性：

- IP 地址源
- IP 地址
- 前缀长度
- 默认网关
- DNS 地址源
- 首选 DNS 服务器
- 备用 DNS 服务器

注: 只有在附加配置下启用 IPv4 和 IPv6 属性后，才能配置 IPv4 和 IPv6 地址详细信息。

8 单击**应用更改**。

配置远程访问设备使用串行端口连接

要配置 BMC 以通过串行端口连接进行通信，请执行以下操作：

1 单击**模块化机柜** > **系统/服务器模块** > **主系统机箱/主系统** > **远程访问**。

2 单击**配置**选项卡。

3 单击**串行端口**。

串行端口配置窗口会出现。

4 配置以下详细信息：

- 连接模式设置
- 波特率
- 流控制
- 信道权限级别限制

5 单击**应用更改**。

6 单击**终端模式设置**。

在终端模式设置窗口中，您可以配置该串行端口的终端模式设置。

终端模式用于在串行端口上使用可打印 ASCII 字符进行智能平台界面管理 (IPMI) 消息传递。 终端模式也支持有限的文本命令来支持传统的基于文本的环境。 这个环境的设计目的就是可以使用简单的终端或终端仿真程序。

7 指定以下定制来提高现有终端的兼容性：

- 行编辑
- 删除控制
- 回声控制

- 符号交换控制
- 新行序列
- 输入新行序列

8 单击**应用更改**。

9 单击**返回串行端口配置窗口**以返回到**串行端口配置**窗口。

将远程访问设备配置为使用 LAN 上串行连接

要配置 BMC/iDRAC 以通过 LAN 上串行 (SOL) 连接进行通信，请执行以下操作：

1 单击**模块化机柜** > **系统/服务器模块** > **主系统机箱/主系统** > **远程访问对象**。

2 单击 **Configuration**（配置）选项卡。

3 单击 **LAN 上串行**。

LAN 上串行配置窗口会出现。

4 配置以下详细信息：

- 启用 LAN 上串行
- 波特率
- 所需的最小权限

5 单击**应用更改**。

6 单击**高级设置**进一步配置 BMC。

7 在 **LAN 上串行配置高级设置**窗口中，可以配置以下信息：

- 字符积累间隔时间
- 字符发送阈值

8 单击**应用更改**。

9 单击**返回 LAN 上串行配置**返回到 **LAN 上串行配置**窗口。

iDRAC 的附加配置

要使用**附加配置**选项卡配置 IPv4 和 IPv6 属性，请执行以下操作：

1 单击**模块化机柜 → 系统/服务器模块 → 主系统机箱/主系统 → 远程访问对象**

2 单击 **Configuration**（配置）选项卡。

3 单击**附加配置**。

4 将 IPv4 和 IPv6 属性配置为**已启用**或**已禁用**。

5 单击**应用更改**。

注: 有关许可证管理的信息，请参阅 dell.com/openmanagemanuals 上的 *Dell License Manager User's Guide*（Dell License Manager 用户指南）。

配置远程访问设备用户

要使用远程访问页面配置远程访问设备，请执行以下操作：

1 单击**模块化机柜** > **系统/服务器模块** > **主系统机箱/主系统** > **远程访问对象**。

2 单击**用户**选项卡。

远程访问用户窗口显示可配置为 BMC/iDRAC 用户的用户相关信息。

3 单击**用户 ID** 配置一个新的或现有的 BMC/iDRAC 用户。

远程访问用户配置窗口允许您配置具体的 BMC/iDRAC 用户。

4 指定以下一般信息：

- 选择**启用用户**以启用该用户。
- 在**用户名**字段中输入用户的名称。
- 选中**更改密码**复选框。
- 在**新密码**字段中键入新密码。
- 在**确认新密码**字段中重新键入新密码。

5 指定以下用户权限：
- 选择最大 LAN 用户权限级别限制。
- 选择准予的最大串行端口用户权限。

6 为 DRAC/iDRAC 用户权限指定用户组。

7 单击**应用更改**以保存更改。

8 单击**返回至远程访问用户窗口**以返回至**远程访问用户**窗口。

注: 当安装了 DRAC 时，有六个附加的用户项可配置。这造成共 16 个用户。BMC/iDRAC 和 RAC 用户使用相同的用户名和密码规则。当安装了 DRAC/iDRAC6 时，所有 16 个用户项都分配给 DRAC。

设置平台事件筛选器警报

要使用 Server Administrator Instrumentation Service 配置最相关的 BMC 功能（例如平台事件筛选器 (PEF) 参数和警报目标）：

1 单击**系统**对象。

2 单击**警报管理**选项卡。

3 单击**平台事件**。

平台事件窗口可让针对特定的平台事件采取单独的措施。您可以选择要对其执行关闭操作的事件并针对所选操作生成警报。您也可以将警报发送到所选的特定 IP 地址目标。

注: 您必须以管理员权限登录才能配置 BMC PEF 警报。

注: 启用平台事件筛选器警报设置可以禁用或启用 PEF 警报生成。此设置独立于各个平台事件警报设置。

注: 倘若没有 PMBus 支持，虽然 Server Administrator 允许您配置，但系统电源探测器警告和系统电源探测器故障在 PowerEdge 系统上不受支持。

4 选择要对其执行关闭操作的平台事件或针对所选操作生成警报，然后单击**设置平台事件**。

设置平台事件窗口允许您指定在因平台事件而要关闭系统时所要执行的操作。

5 选择以下操作之一：
- **无**
- **重新引导系统**

  关闭操作系统并启动系统，执行 BIOS 检查并重新载入操作系统。
- **关闭系统电源**

  关闭系统的电源。
- **系统电源关闭后重启**

  将系统电源关闭、暂停、打开电源，然后重新引导系统。在需要重新初始化系统组件（比如硬盘驱动器）时，关机后再开机非常有用。
- **功率缩减**

  调节 CPU。

小心: 如果为“平台事件”关闭操作选择除“无”或“功率减小”以外的其他值，系统将在出现指定的事件时强制关闭。这种关机由固件启动，并且在执行时不会首先关闭操作系统或任何正在运行的应用程序。

注: 并不是所有系统都支持功率缩减。电源监测和电源监测功能仅适用于安装有两个或多个冗余热插拔电源设备的系统。对于缺乏电源管理电路的、永久安装的非冗余电源，这些功能不可用。

6 选择**生成警报**复选框以发送警报。

注: 要生成警报，您必须选择生成警报和启用平台事件警报设置。

7 单击**应用**。

8 单击**应用于平台事件页**以返回到**平台事件筛选器**窗口。

设置平台事件警报目标

也可使用平台事件筛选器窗口选择平台事件警报要发送到的目标。根据显示的目标数，您可以为每个目标地址配置单独的 IP 地址。平台事件警报将发送到您配置的每个目标 IP 地址。

1 单击平台事件筛选器窗口中的**配置目标**。

2 单击您想配置的目标数。

注: 在给定系统上可以配置的目标数会有所差异。

3 选中 **启用目标**复选框。

4 单击**目标数字**为该目标输入一个单独的 IP 地址。 这个 IP 地址是平台事件警报将要发送到的 IP 地址。

注: 在使用 iDRAC7 特定版本的 12G 系统上，可以将平台事件目标设置为 IPv4、IPv6 或 FQDN。

5 在**团体字符串**字段中输入一个值，以用作密码来验证在管理站和受管系统之间发送的消息。团体字符串（也称为团体名称）是在管理站和受管系统间的每个数据包中发送的。

6 单击**应用**。

7 单击**返回平台事件页**以返回到**平台事件筛选器**窗口。

7

设置警报措施

对运行支持的 Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统的系统设置警报措施

设置事件的警报措施时，可以将操作指定为在服务器上显示警报。为了执行此操作，Server Administrator 会将消息写入 **/dev/console**。如果 Server Administrator 系统运行的是 X Window 系统，则不显示该消息。要在运行 X Window 系统时查看 Red Hat Enterprise Linux 系统上的警报消息，在事件发生之前必须启动 **xconsole** 或 **xterm -C**。要在运行 X Window 系统时查看 SUSE Linux Enterprise Server 系统上的警报消息，在事件发生之前必须启动终端，例如：**xterm -C**。

为事件设置警报措施时，可以指定用于**广播消息**的操作。为了执行此操作，Server Administrator 会执行 wall 命令，该命令将消息发送到已登录且消息权限设为**是**的每个人。如果 Server Administrator 系统正在运行 X Window 系统，则默认情况下不会显示该消息。要在 X Window 系统运行时查看广播消息，必须在发生事件前启动诸如 **xterm** 或 **gnome-terminal** 之类的终端。

设置事件的警报措施时，您可以将操作指定为**执行应用程序**。对 Server Administrator 可以执行的应用程序有一些限制。 要确保正确执行应用程序：

- 不要指定基于 X Window 系统的应用程序， 因为 Server Administrator 无法正确执行此类应用程序。
- 不要指定需要用户输入信息的应用程序，因为 Server Administrator 无法正确执行此类应用程序。
- 指定应用程序时，请将 **stdout** 和 **stderr** 重定向至文件，以便查看所有输出或错误消息。
- 如果希望为警报执行多个应用程序（或命令），请创建一个脚本，并将脚本的完整路径放入**应用程序的绝对路径框**中。

示例 1：`ps -ef >/tmp/psout.txt 2>&1`

示例 1 中的命令执行应用程序 ps，将 stdout 重定向至文件 **/tmp/psout.txt**，并将 **stderr** 重定向至 **stdout** 所重定向的同一文件。

示例 2：`mail -s "Server Alert" admin </tmp/alertmsg.txt>/tmp/mailout.txt 2>&1`

示例 2 中的命令执行邮件应用程序，将文件 /tmp/alertmsg.txt 中包含的消息以 **Server Alert（服务器警报）**为主题发送至 Red Hat Enterprise Linux 用户或 SUSE Linux Enterprise Server 用户和管理员。用户必须在事件发生之前创建文件 **/tmp/alertmsg.txt**。此外，出现错误时，**stdout** 和 **stderr** 将重定向至文件 /tmp/mailout.txt。

在 Windows Server 中设置警报措施执行应用程序

在 Windows 中，默认情况下禁用**交互式服务检测**。必须在 **Regedit** 中激活**交互式服务检测**才可启用可执行应用程序。

要启用**交互式服务检测**，请按照下述步骤操作：

1 Modifying the **NoInteractiveServices**

1 打开 **Regedit**。

2 导航至 HKLM\SYSTEM\CurrentControlSet\Control\Windows\。

3 右键单击 **NoInteractiveServices**，然后单击 **修改**。

4 在**值数据**中输入 **0**，然后单击**确定**。

5 关闭 **Regedit**

6 要将用户添加到某个组，请从**组**下拉菜单中选择组名称并单击**添加**。

7 单击**确定**。

2 Enabling the **Interactive Service Detection**

8 打开 **Services.msc**。
9 导航至**交互式服务检测**。
10 右键单击**交互式服务检测**，然后单击**属性**。
11 在**常规**选项卡中，将**启动类型**更改为**自动**，然后单击**应用**。
12 在“服务状态”中单击**启动**。
3 Allowing the service to interact
13 导航至 **DSM SA Data Manager**，右键单击，然后单击**属性**。
14 在**登录**选项卡中，启用**允许服务与桌面交互**，然后单击**确定**。
15 单击**确定**。

重新启动 **DSM SA Data Manager** 以启用**交互式服务检测**。

交互式应用程序 — 交互式应用程序的示例是具有图形用户界面 (GUI) 的应用程序，或能提示用户以某种方式输入（如批处理文件中的 pause 命令）。

注: 查看交互式应用程序时，会显示一条弹出式消息：交互式服务检测，并显示如下消息：A program running on this computer is trying to display a message，单击查看消息即可继续。

BMC 或 iDRAC 平台事件筛选器警报消息

下表列出了所有可能的平台事件筛选器 (PEF) 消息，以及有关每个事件的说明。

表. 14: PEF 警报事件

事件	说明
风扇探测器故障	风扇转动速度太慢或根本不转动。
电压探测器故障	电压太低，无法正常工作。
电池探测器警告	电池在推荐的电量以下工作。
电池探测器故障	电池发生了故障。
分离电压探测器故障	电压太低，无法正常工作。
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。
检测到机箱侵入	系统机箱已被打开。
冗余（电源设备或风扇）降级	风扇和/或电源设备的冗余已经减少。
冗余（电源设备或风扇）丢失	系统的风扇和/或电源设备不再备有冗余。
处理器警告	处理器的运行速度低于峰值性能或速度。
处理器故障	处理器已经发生故障。
没有处理器	处理器已被卸下。
PS/VRM/D2D 警告	电源设备、调压器模块或直流对直流转换器即将出现故障状况。
PS/VRM/D2D 故障	电源设备、调压器模块或直流对直流转换器已经发生故障。
硬件日志已满或清空	硬件日志为空或已满，需要管理员注意。
自动系统恢复	系统已挂起或没有响应，并正在采取由自动系统恢复配置的措施。
系统电源探测器警告	功耗接近故障阈值。
系统电源探测器故障	功耗超过最高可接受限值并导致故障。
没有可移动闪存介质	可移动闪存介质已卸除。
可移动闪存介质故障	可移动闪存介质即将出现故障状况。

事件	说明
可移动闪存介质警告	可移动闪存介质处于故障状态。
内部双 SD 模块卡-严重	内部双 SD 模块卡出现故障。
内部双 SD 模块卡-警告	内部双 SD 模块卡处于故障状态。
内部双 SD 模块卡冗余丢失	内部双 SD 模块卡无冗余。
内部双 SD 模块卡-缺失	内部双 SD 模块卡已卸除。

8

故障排除

连接服务故障

在 Red Hat Enterprise Linux 上，当 `SELinux is set to enforced mode` 时，Systems Management Server Administrator (SMSA) 连接服务启动失败。执行以下任一步骤并启动此服务：

- 将 `SELinux` 设置为 `Disabled` 模式或 `Permissive` 模式。
- 将 SELinux 的 **allow_execstack** 属性更改为 **ON（开）**状态。运行以下命令：
  `setsebool allow_execstack on`
- 更改 SM SA 连接服务的安全上下文。运行以下命令：`chcon -t unconfined_execmem_t /opt/dell/srvadmin/sbin/dsm_om_connsvcd`

主题：

登录失败情况

在以下情形中，可能无法登录受管系统：

- 输入无效或不正确的 IP 地址。
- 输入不正确的凭据（用户名和密码）。
- 受管系统处于关闭状态。
- 由于 IP 地址无效或发生 DNS 错误，无法访问受管系统。
- 受管系统具有不可信的证书，而且用户没有在登录页中选择**忽略证书警告**
- VMware ESXi 系统中未启用 Server Administrator 服务。有关如何在 VMware ESXi 系统中启用 Server Administrator 服务的信息，请参阅 **dell.com/openmanagemanuals** 上的 *Server Administrator Installation Guide*（Server Administrator 安装指南）。
- VMware ESXi 系统上占用很少资源的 CIM 代理守护程序 (SFCBD) 服务没有运行。
- 管理系统上的 Web 服务器管理服务没有运行。
- 如果没有选中**忽略证书警告**复选框，则应输入管理系统的 IP 地址而不是主机名。
- 未在受管系统中配置 WinRM 授权功能（远程启用）。 有关此功能的信息，请参阅 **dell.com/openmanagemanuals** 上的 *Server Administrator Installation Guide*（Server Administrator 安装指南）。
- 连接到 VMware ESXi 5.0 操作系统时验证失败，这可能是由以下任何一种原因引起的：
  a 登录服务器或登录 Server Administrator 时启用了 `lockdown` 模式。 有关 `lockdown` 模式的更多信息，请参阅 VMware 说明文件。
  b 登录 Server Administrator 时更改了密码。
  c 以没有管理员权限的普通用户身份登录 Server Administrator。 有关更多信息，请参阅关于分配角色的 VMware 说明文件。

在支持的 Windows 操作系统上修复出现故障的 Server Administrator 安装

通过强制重新安装 Server Administrator 并接着进行卸载，可修复出现故障的安装。

要强制进行重新安装，请执行以下操作：

1 检查以前安装的 Server Administrator 的版本。
2 从 **support.dell.com** 下载该版本的安装软件包。
3 在 srvadmin\windows\SystemsManagement 目录下找到 SysMgmt.msi。
4 在命令提示符处输入以下命令以强制进行重新安装

```
msiexec /i SysMgmt.msi REINSTALL=ALL

REINSTALLMODE=vamus
```

5 选择**自定义安装**并选择原来安装的所有功能。如果您不能肯定已安装了哪些功能，则可选择所有功能并执行安装。

注: 如果在非默认目录中安装了 Server Administrator，请确保同时在自定义设置中更改它。

注: 安装了应用程序后，可以使用添加/删除程序卸载 Server Administrator。

Server Administrator 服务

下表列出 Server Administrator 用于提供系统管理信息的服务，以及这些服务发生故障时的影响。

表. 15: Server Administrator 服务

服务名称	说明	故障影响	恢复机制	严重性
Windows：SM SA 连接服务 Linux：`dsm_om_connsvc`（此服务随 Server Administrator Web 服务器一起安装。）	提供从具有支持的 Web 浏览器和网络连接的任何系统对 Server Administrator 进行的远程/本地访问。	用户将无法通过 Web 用户界面登录 Server Administrator 和执行任何操作。但是，仍然可以使用 CLI。	重新启动服务	严重
Windows：SM SA 共享服务 Linux：`dsm_om_shrsvc`（此服务在受管系统上运行。）	启动时运行资源清册收集程序，对将由 Server Administrator 的 SNMP 和 CIM 提供程序使用的系统执行软件资源清册，以便使用 System Management Console 和 Dell OpenManage Essentials 执行远程软件更新。	使用 OpenManage Essentials 无法进行软件更新。但是，仍然可以使用单个 Dell Update 软件包在本地和 Server Administrator 之外执行更新。仍可使用第三方工具（例如 MSSMS、Altiris 和 Novell ZENworks）执行更新。	重新启动服务	警告

注: Server Administrator 可能会在警报日志页或操作系统日志文件中发送重复的 SNMP 陷阱或记录重复的事件。在操作系统重新引导后手动重新启动 Server Administrator 服务时，或设备传感器在 Server Administrator 服务启动后仍指示非正常状态时，都会记录重复的陷阱和事件。

注: 使用 Dell Update Packages 更新 Dell 控制台需要资源清册收集程序。

注: 有些资源清册收集程序功能在 Server Administrator（64 位）上不被支持。

Windows：SM SA Data Manager Linux：`dsm_sa_datamgrd`（托管于 dataeng 服务下）（此服务在受管系统上运行。）	监测系统，提供对详细故障和性能信息的快速访问，并允许远程管理受监测的系统，包括关机、启动和安全保护。	如果这些服务没有运行，用户将无法在 GUI/CLI 上配置/查看硬件级详细信息。	重新启动服务	严重
SM SA Event Manager (Windows) Linux：`dsm_sa_eventmgrd`（托管于 dataeng 服务	为系统管理提供操作系统和文件事件记录服务，同时被事件日志分析程序使用。	如果停止此服务，事件记录功能将无法正常运行。	重新启动服务	警告

服务名称	说明	故障影响	恢复机制	严重性
下）（此服务在受管系统上运行。）				
Linux：`dsm_sa_snmpd`（托管于 dataeng 服务下）（此服务在受管系统上运行。）	数据引擎 Linux SNMP 接口	来自 Management Station 的 SNMP get/set /陷阱请求将不能运行。	重新启动服务	严重
Windows： `mr2kserv`（此服务在受管系统上运行。）	Storage Management Service 提供存储管理信息和高级功能，用于配置连接到系统的本地或远程存储设备。	用户将无法为所有受支持的 RAID 和非 RAID 控制器执行存储功能。	重新启动服务	严重

9

常见问题

本节列出有关 Server Administrator 的常见问题。

注: 下列问题并不特定于此版本的 Server Administrator。

1 **安装 Server Administrator 所需的最低权限级别是什么？**

要安装 Server Administrator，您必须具有管理员级别的权限。高级用户和用户没有安装 Server Administrator 的权限。

2 **如何确定适用于我系统的最新 Server Administrator 版本？**

登录到：**support.dell.com** → Software & Security → Enterprise System Management → OpenManage Server Administrator。

此页面显示所有可用的 Server Administrator 版本。

3 **如何得知自己系统上运行的 Server Administrator 的版本？**

登录到 Server Administrator 后，导航至**属性 → 摘要**。可以在**系统管理**列中找到系统上安装的 Server Administrator 的版本。

4 **用户除了 1311 外是否还可以使用其他端口？**

是，可以设置首选 https 端口。导航至**首选项 → 常规设置 → Web Server → HTTPS 端口**

不选择**使用默认值**，而是选择**使用**单选按钮设置首选端口。

注: 将端口编号更改为无效或正在使用的端口编号可能会妨碍其他应用程序或浏览器访问管理系统上的 Server Administrator。有关默认端口列表，请参阅可在 dell.com/openmanagemanuals 上获得的 *Server Administrator Installation Guide*（Server Administrator 安装指南）。

5 **是否可以在 Fedora、College Linux、Mint、Ubuntu、Sabayon 或 PClinux 上安装 Server Administrator？**

不可以，Server Administrator 不支持这些操作系统。

6 **Server Administrator 能否在出现问题时发送电子邮件？**

不能，Server Administrator 并没有设计为在出现问题时发送电子邮件。

7 **是否需要 SNMP 才能在 PowerEdge 系统上进行 ITA 查找、资源清册和软件更新？能否单独使用 CIM 进行查找、资源清册和更新还是需要 SNMP？**

ITA *与 Linux 系统通信*：

Linux 系统上需要 SNMP 才能进行查找、状态轮询和资源清册。

软件更新通过 SSH 会话和安全 FTP 来完成，因此单独执行、设置或请求此操作时需要 root 用户级别的权限/凭据。不一定要具有查找范围的凭据。

ITA *与 Windows 系统通信*：

对于服务器（运行 Windows Server 操作系统的系统），系统会配置为使用 SNMP 和/或 CIM 进行 ITA 查找。资源清册需要 CIM。

软件更新，同 Linux 中一样，与查找、轮询和所用协议无关。

使用计划和执行更新时要求的管理员级别凭据，在目标系统上建立管理（驱动器）共享，并从其他地方（可能是其他网络共享）复制文件到目标系统。随即调用 WMI 功能执行软件更新。

由于在客户端/工作站上没有安装 Server Administrator，因此在目标运行 OpenManage Client Instrumentation 时使用 CIM 查找。

对于许多其他设备，比如网络打印机，标准是使用 SNMP 与设备通信（主要是查找）。

像 EMC 存储这样的设备具有专用协议。查看使用的端口可以了解有关此环境的某些信息。

8 **是否有任何 SNMP v3 支持计划？**

不是，没有任何 SNMP v3 支持计划。

9 **域名中含有下划线字符是否会造成 Server Admin 登录问题？**

是，域名中的下划线字符是无效的。除连字符以外，所有其他特殊字符都是无效的。仅使用区分大小写的字母和数字。

10 **选择/取消选中 Server Administrator 登录页上的 'Active Directory' 对权限级别有什么影响？**

如果不选中 Active Directory 复选框，则您仅具有在 Microsoft Active Directory 中配置的访问权限。您无法使用 Microsoft Active Directory 中的扩展架构解决方案登录。

使用此解决方案可以提供对 Server Administrator 的访问；可为 Active Directory 软件中的现有用户添加/控制 Server Administrator 用户和权限。有关更多信息，请参阅可在 **dell.com/openmanagemanuals** 上获得的 *Server Administrator Installation Guide*Server Administrator 安装指南）中的" Using Microsoft Active Directory"（使用 Microsoft Active Directory）。

11 **我在执行 Kerberos 验证和尝试从 Web Server 登录时应该执行什么操作？**

要进行验证，必须将受管节点上的文件 **/etc/pam.d/openwsman** 和 **/etc/pam.d/sfcb** 的内容替换为以下内容：

```
auth required pam_stack.so service=system-auth auth required /lib64/security/pam_nologin.so
account required pam_stack.so service=system-auth
```

12 **Server Administrator 警报不会显示在 SNMP 陷阱中，如何配置以启用 SNMP 陷阱？**

按照设置 SNMP 配置的步骤以启用 Server Administrator 警报：

- `esxcli system snmp set --communities public`
- `esxcli network firewall ruleset set --ruleset-id snmp --allowed-all true`
- `esxcli network firewall ruleset set --ruleset-id snmp --enabled true`
- `esxcli system snmp set -t <target_ip>@162/public`
- `esxcli system snmp set --enable true`