Dell OpenManage Server Administrator 版本 6.4 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”表示可能会损坏硬件或导致数据丢失，并说明如何避免此类问题。

2010 年 12 月

返回目录页面

设置警报措施

Dell OpenManage Server Administrator 版本 6.4 用户指南

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 会将信息写入 **/dev/console**。如果 Server Administrator 系统运行的是 X Window 系统，则默认情况下无法看到该信息。要在运行 X Window 系统时查看 Red Hat Enterprise Linux 系统上的警报信息，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 系统上的警报信息，在事件发生之前必须启动 **xterm -C**。

设置事件的警报措施时，您可以将操作指定为“**广播信息**”。为了执行该操作，Server Administrator 将执行 **wall** 命令，该命令将信息发送至所有在登录时将信息许可设置为“**是**”的用户。如果 Server Administrator 系统运行的是 X Window 系统，则默认情况下无法看到该信息。要在运行 X Window 系统时查看广播信息，则在事件发生之前必须启动 **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。请遵循以下原则以确保正确执行应用程序：

- 由于 Server Administrator 无法正确执行基于 X Window 系统的应用程序，因此请勿指定此类应用程序。
- 由于 Server Administrator 无法正确执行需要用户输入信息的应用程序，因此请勿指定此类应用程序。
- 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信息。
- 如果想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“**Absolute path to the application**”（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** 中包含的信息以“**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 Microsoft Windows Server 2003 和 Windows Server 2008 中设置警报措施

指定警报操作时，Visual Basic 脚本不会由 Execute Application（执行应用程序）功能自动解释，尽管可以通过只指定文件作为警报操作来运行 .cmd、.com、.bat 或 .exe 文件。

要解决此问题，首先调用命令处理器 cmd.exe 启动脚本。例如，执行应用程序的警报操作值可以设置为：

```
c:\winnt\system32\cmd.exe /c d:\example\example1.vbs
```

其中 d:\example\example1.vbs 是脚本文件的完整路径。

请勿在应用程序绝对路径字段中设置交互式应用程序（具有图形用户界面或需要用户输入的应用程序）的路径。交互式应用程序在有些操作系统上可能不会按预想的方式工作。

注：应指定到 cmd.exe 文件和脚本文件的路径。

在 Windows Server 2008 中设置警报措施执行应用程序

出于安全原因，Windows Server 2008 配置为不允许交互式服务。在 Windows Server 2008 上将某个服务作为交互式服务安装时，操作系统会在 Windows 系统日志中记录一条有关将这个服务标记为交互式服务的错误信息。

当您使用 Server Administrator 为某个事件配置警报措施时，可以将措施指定为*执行应用程序*。要使交互式应用程序能够为警报措施正常执行，Dell Systems Management Server Administrator（DSM SA）Data Manager 服务必须配置为交互式服务。举例来说，具有图形用户界面（GUI）的应用程序或以某种方式提示用户输入的应用程序（如批处理文件中的 *pause* 命令）便是交互式应用程序。

在 Microsoft Windows Server 2008 上安装 Server Administrator 时，DSM SA Data Manager 服务将作为非交互式服务进行安装，这意味着它默认配置为不得与桌面进行交互。这意味着当为警报措施执行交互式应用程序时，未正确地执行。如果在这种情况下为警报措施执行交互式应用程序，应用程序将被暂挂，并等待输入。应用程序界面/提示对用户不可见，即使

在启动 Interactive Services Detection 服务后，也仍然不可见。**任务管理器**中的**进程**选项卡显示交互式应用程序每个执行的应用程序进程项。

如果需要在 Microsoft Windows Server 2008 上为警报措施执行交互式应用程序，必须将 DSM SA Data Manager 服务配置为允许与桌面进行交互。

要允许与桌面进行交互：

1. 右键单击**服务控制面板**中的 DSM SA Data Manager 服务，然后选择“属性”。
2. 在“**Log On**”（登录）选项卡中，启用“**Allow service to interact with desktop**”（允许服务与桌面交互），然后单击“**OK**”（确定）。
3. 重新启动 DSM SA Data Manager 服务，以便使更改生效。

当 DSM SA Data Manager 服务带有此项更改而重新启动后，Service Control Manager 会在系统日志中记录以下信息："The DSM SA Data Manager service is marked as an interactive service.However, the system is configured to not allow interactive services.This service may not function properly"（DSM SA Data Manager 服务标记为交互式服务。但是，系统配置为不允许交互式服务。此服务可能无法正常运行）。此项更改使 DSM SA Data Manager 服务可以为警报措施正确执行交互式应用程序。还要确保 Interactive Services Detection 服务已运行，以查看交互式应用程序显示的界面/提示。这些更改完成后，操作系统即会显示“**Interactive services dialog detection**”（交互式服务对话检测）对话框，以提供对交互式应用程序界面/提示的访问。

BMC/iDRAC 平台事件筛选器警报信息

所有可能的平台事件过滤器（PEF）消息以及每个事件的说明均在表 7-1 中列出。

表 7-1. 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。
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。
温度探测器故障	温度太高或太低，无法正常运行。
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降低。
冗余（电源设备或风扇）掉失	系统风扇和（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。
PPS/VRM/DCtoDC 警告	电源设备、稳压器模块或 DC 到 DC 转换器将要发生故障。
电源设备/VRM/D2D 故障	电源设备、稳压器模块或 DC 到 DC 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。
可移动闪存介质存在	可移动闪存介质存在。
可移动闪存介质故障	可移动闪存介质处于故障状态。
可移动闪存介质警告	可移动闪存介质存在。

了解服务名称

以下服务的可执行服务和显示名称已更改：

表 7-2. 服务名称

用途	服务名称	上一版本（版本 5.0 之前）	当前版本
Web Server	显示名称	安全端口服务器	DSM SA 连接服务
	可执行文件名称	Omaws[32|64]	dsm_om_connsvc
			dsm_om_connsvc
计划或通知	显示名称	OM 公共服务	DSM SA Shared Services

	可执行文件名称	Omsad[32|64]	dsm_om_shrsvc
			dsm_om_shrsvc

返回目录页面

返回目录页面

故障排除

Dell OpenManage Server Administrator 版本 6.4 用户指南

连接服务故障

在 Red Hat Enterprise Linux 上，SELinux 设置为强化模式时，Dell Systems Management Server Administrator（DSM SA）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）”（已禁用模式或“Permissive”（允许）模式。
- 将 SELinux **allow_execstack** 属性更改为“**ON**”（开）状态。运行以下命令：

  ```
  setsebool allow_execstack on
  ```

- 更改 DSM 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
  ```

登录失败情况

在以下情形中，可能无法登录 Managed System：

- 输入无效/不正确的 IP 地址。
- 输入不正确的凭据（用户名和密码）。
- Managed System 处于“OFF”（关）状态。
- 由于 IP 地址无效或发生 DNS 错误，无法访问 Managed System。
- Managed System 具有不可信的证书，而且用户没有在登录页中选择“**Ignore Certificate Warning**”（忽略证书警告）。
- 在 VMware ESX/ESXi 系统中没有启用 Server Administrator 服务。有关如何在 ESX/ESXi 系统中启用 Server Administrator 服务的信息，请参阅《Dell OpenManage Server Administrator 安装指南》。
- VMware ESX/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。
- Managed System 上的 Web 服务器管理服务没有运行。
- 在没有选中“**Ignore Certificate Warning**”（忽略证书警告）复选框的情况下输入 Managed System 的 IP 地址而不是主机名。
- 没有在 Managed System 中配置 WinRM 授权功能（远程启用）。有关此功能的信息，请参阅《Dell OpenManage Server Administrator 安装指南》。
- 连接到 VMware ESXi 4.1/ESX 4.1 操作系统时验证失败，这可能是以下任何原因引起的：
  - 登录服务器或登录 Server Administrator 时，就启用锁定模式。有关锁定模式的详情，请参阅 VMware 说明文件。
  - 登录 Server Administrator 时，就会更改密码。
  - 以没有管理员权限的普通用户身份登录 Server Administrator。有关详情，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，可修补出现故障的安装。

强制进行重新安装：

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“**Custom Setup**”（自定义安装）并选择原来安装的所有功能。如果不确定安装过哪些功能，请选择所有功能并执行安装过程。

   注：如果在非默认目录中安装了 Server Administrator，请确保同时在“Custom Setup”（自定义设置）中更改它。

6. 安装了应用程序后，可以使用“**Add/Remove**”（添加/删除程序）卸载 Server Administrator。

OpenManage 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 A-1. OpenManage Server Administrator 服务

服务名称	说明	故障影响	恢复机制	Severity（严重性）
Windows: DSM 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	“Critical”（严重）
常见服务				
Windows: DSM SA Shared Services（服务） Linux: dsm_om_shrsvc （此服务在 Managed System 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 Dell System Management Console 和 Dell IT Assistant（ITA）执行远程软件更新。	使用 ITA 无法进行软件更新。但是，仍然可以使用单独的 Dell Update 软件包在本地和 Server Administrator 之外执行更新。仍然可以通过第三方工具（例如，MSSMS、 Altiris 和 Novell ZENworks）执行更新。	重新启动服务	“Warning”（警告）
注：如果在 64 位 Linux 系统上没有安装 32 位兼容库，共享服务将无法启动资源清册收集程序，显示错误信息“libstdc++.so.5 is required to run the Inventory Collector”（需要 libstdc++.so.5 才能运行资源清册收集程序）。srvadmin-cm.rpm 为资源清册收集程序提供二进制文件。有关 srvadmin-cm 所依赖 RPM 的列表，请参阅《Dell OpenManage Server Administrator 安装指南》。				
Instrumentation Service				
Windows: DSM SA 数据管理器 Linux: dsm_sa_datamgrd （在 dataeng 服务下面） （此服务在 Managed System 上运行。）	监控系统，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控的系统，包括关机、启动和安全。	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	“Critical”（严重）
DSM SA 事件管理器（Windows） Linux: dsm_sa_eventmgrd （在 dataeng 服务下面） （此服务在 Managed System 上运行。）	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	“Warning”（警告）
Linux: dsm_sa_snmpd （在 dataeng 服务下面） （此服务在 Managed System 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	“Critical”（严重）
Storage Management Service				
Windows：mr2kserv（此服务在 Managed System 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。	用户将无法为所有支持的 RAID 和非 RAID 控制器执行存储功能。	重新启动服务	“Critical”（严重）

返回目录页面

返回目录页面

常见问题

Dell OpenManage Server Administrator 版本 6.4 用户指南

本节列出有关 Dell OpenManage Server Administrator 的常见问题：

注：这些问题并不特定于此版本的 Server Administrator。

1. **为什么从 OpenManage Server Administrator 启动的 ESXi 4.0.x（4.0 U1/U2）主机重新引导功能失败？**

   此问题是归咎于 VMware 单机许可证（SAL）密钥。有关详细信息，请参阅位于 kb.vmware.com/kb/1026060 上的知识库文章。

2. **将 VMware ESX 4.1 操作系统添加到 Active Directory 域后需要执行什么任务？**

   将 VMware ESX 4.1 操作系统添加到 Active Directory 域后，Active Directory 用户必须执行以下操作：

   - 将 VMware ESX 4.1 操作系统用作 Server Administrator 时，登录 Server Administrator，然后重新启动 DSM SA 连接服务。
   - 将 VMware ESX 4.1 操作系统用作远程启用代理时，登录远程节点。大约等待 5 分钟，让 sfcbd 进程为新用户添加权限。

3. **用户安装 Server Administrator 所需的最低权限级别是什么？**

   至少需要“**Administrator**”（管理员）权限级别才能安装 Server Administrator。“Power Users”（高级用户）和“Users”（用户）没有安装 Server Administrator 的权限。

4. **是否需要升级路径来安装 Server Administrator?**

   对于具有 Server Administrator 版本 4.3 的系统，无需升级路径。对于早于版本 4.3 的系统，需要先升级到版本 4.3，然后再升级到版本 6.x（x 表示要升级到的 Server Administrator 版本）。

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

   登录到：**support.dell.com**→ “**Enterprise IT**”（企业 IT）→ “**Manuals**”（手册）→ “**Software**”（软件）→ “**Systems Management**”（系统管理）→ **Dell OpenManage Server Administrator**

   最新的说明文件版本显示适用于您的 OpenManage Server Administrator 版本。

6. **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“**Properties**”（属性）→ “Summary”（摘要）。可以在“**Systems Management**”（系统管理）列中找到系统上安装的 Server Administrator 的版本。

7. **用户除了 1311 外是否还可以使用其它端口？**

   是，可以设置首选 https 端口。导航至“**Preferences**”（首选项）→ “**General Settings**”（常规设置）→ **Web Server** → “**HTTPS Port**”（HTTPS 端口）。

   不选择“**Use default**”（使用默认值），而是单击“**Use radio button to set your preferred port**”（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 managed system 上的 Server Administrator。请参阅《Dell OpenManage 安装和安全性用户指南》查看默认端口列表。

8. **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。

9. **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。

10. **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。

    Dell 软件更新通过 SSH 会话和安全 FTP 进行，因此单独执行、设置或请求此操作时需要根级别权限/凭据。不会假定采用查找范围的凭据。

    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 或 CIM 或者使用两者进行 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，并从其它地方（可能是其它网络共享）复制文件到目标系统。随后会调用 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。

对于许多其它设备，比如网络打印机，标准仍是使用 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。查阅 OpenManage 说明文件中的端口使用表可以了解有关此环境的某些信息。

11. **是否有任何 SNMP v3 支持计划？**

    不是，没有任何 SNMP v3 支持计划。

12. **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。其它所有特殊字符（连字符除外）都是无效的。仅使用不区分大小写的字母和数字。

13. **选中/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，则您只具有在 Microsoft Active Directory 中配置的访问权限。您无法使用 Microsoft 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。有关详情，请参阅《Dell OpenManage Server Administrator 安装指南》中的“使用 Microsoft Active Directory”。

14. **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：

    对于 32 位：

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

    对于 64 位：

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

返回目录页面

返回目录页面

Server Administrator 服务

Dell OpenManage Server Administrator 版本 6.4 用户指南

概览

Dell OpenManage Server Administrator Instrumentation Service 可以监测系统的运行状况，并使您可以快速查看行业标准系统管理代理收集的详细故障和性能信息。利用其报告和查看功能，可以检索包含系统的各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状况的信息。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。可以方便地检索有关 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等。

注：对于运行 Microsoft Windows Server 2003 的 Managed System 和网络 Management Station，都必须配置简单网络管理协议（SNMP）服务才能接受 SNMP 数据包。有关详细信息，请参阅“在运行支持的 Windows 操作系统的系统中配置 SNMP 代理”。

管理系统

默认情况下，Server Administrator 主页将显示系统树视图的“**System**”（系统）对象。“**System**”（系统）对象将打开“**Properties**”（属性）选项卡下的“**Health**”（运行状况）组件。

默认情况下，访问“**Preference**”（首选项）主页时将显示“**Preference**”（首选项）选项卡下的“**Access Configuration**”（访问配置）窗口。

在“**Preferences**”（首选项）主页中，您可以限制对具有“User”（用户）和“Power User”（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 DSM SA 连接服务设置。

注：Server Administrator 主页的每个窗口都有上下文相关联机帮助。单击“**Help**”（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“**Shutdown**”（关机）选项卡中的关闭系统功能。

管理系统 / 服务器模块树对象

Server Administrator 系统/服务器模块树将根据 Server Administrator 在 managed system 中查找到的软件和硬件组以及用户的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。展开主对象时一“**模块化机柜**”“**System / Server Module**（系统/服务器模块）”—可能显示的系统组件的主类别为“**Main System Chassis / Main System（主系统机箱/主系统）**”、“**Software（软件）**”和“**Storage（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 组件的详情，请参阅 **support.dell.com / manuals** 上的《Dell OpenManage Server Administrator Storage Management 用户指南》。

Server Administrator 主页系统树对象

不支持的 OpenManage Server Administrator 功能

由于 VMware ESXi 版本 4.X 操作系统的限制，较早版本 OpenManage Server Administrator 提供的某些功能在此版本中不可用。这些功能是：

ESXi 4.X 上不支持的功能

- 警报管理 – 警报措施
- 网络接口 – 管理状态
- 网络接口 – DMA
- 网络接口 – Internet 协议（IP）地址
- 网络接口 – 最大传输单元
- 网络接口 – 运行状态
- 首选项 – SNMP 配置
- 远程关机 – 先关闭操作系统，然后系统关机后再开机
- 关于详细信息 – Server Administrator 组件详细信息未列在“Details”（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“**Shutdown**”（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机箱管理控制器（CMC）信息，单击**模块化机柜**对象。

Properties（属性）

子选项卡：信息

在“**Properties**”（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机箱管理控制器（CMC）信息。

访问并使用机箱管理控制器

要从 Server Administrator 主页链接到 Chassis Management Controller“**Log in**”（登录）窗口：

1. 单击“**Modular Enclosure**”（模块化机柜）对象
2. 单击“**CMC Information**”（CMC 信息）选项卡，然后单击“**Launch the CMC Web Interface**”（启动 CMC Web 界面）。系统将显示 CMC“**Log in**”（登录）窗口。

连接到 CMC 后，可以监测并管理模块化机柜。

System/Server Module（系统/服务器模块）

“System/Server Module”（系统/服务器模块）对象包含三个主要的系统组件组：“Main System Chassis/Main System（主系统机箱/主系统）”、“Software（软件）”和“Storage（存储）”。Server Administrator 主页默认为系统树视图的“**System**”（系统）对象。通过“**System/Server Module**”（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，“**System/Server Module**”（系统/服务器模块）对象操作窗口包含以下选项卡：“**Properties**”（属性）、“**Shutdown**”（关机）、“**Logs**”（日志）、“**Alert Management**”（警报管理）和“**Session Management**”（会话管理）。

Properties（属性）

子选项卡：“Health”（运行状况）|“Summary”（摘要）|“Asset Information”（资产信息）|“Auto Recovery”（自动恢复）

在“**Properties**”（属性）选项卡下，您可以：

- 查看“**Main System Chassis/Main System**”（主系统机箱/主系统）对象和“**Storage**”（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：由于 BIOS 中已启用操作系统监督计时器，自动系统恢复选项可能不可用。要配置自动恢复选项，操作系统监督计时器必须禁用。

  注：当监督器确认有停止响应的系统时，自动系统恢复操作可能不会完全按超时期限（n 秒）执行。操作执行时间范围介于 $n-h+1$ 到 $n+1$ 秒，其中 n 是超时期限，而 h 是心跳间隔。心跳间隔值在 $n \leq 30$ 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引导行为，此功能可能运行不正常。如果发生这种情况，必须手动重新引导系统。

Shutdown（关机）

子选项卡：“Remote Shutdown”（远程关机）|“Thermal Shutdown”（热关机）|“Web Server Shutdown”（Web Server 关机）

在“**Shutdown**”（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 仍可用来使用命令行界面（CLI）。CLI 功能不需要运行 DSM SA 连接服务。

Logs（日志）

子选项卡：“Hardware”（硬件）|“Alert”（警报）|“Command”（命令）

在“**Logs**”（日志）选项卡下，您可以：

- 查看嵌入式 System Management（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，日志名称旁的状况标志图标会从正常状态（ ）更改为不严重状态（ ）。在 Dell PowerEdge *x8xx*、*x9xx* 和 *xx1x* 系统上，当日志文件达到 100% 的容量时，日志名旁边的状态标志图标将变为严重状态（ ）。

  注：建议在硬件日志达到 80% 的容量时清理硬件日志。如果允许日志达到 100% 的容量，将从日志中丢弃最新的事件。

- 查看警报日志，以获得因响应传感器状况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 的相应描述、严重性级别和原因的完整说明，请参阅《Server Administrator 信息参考指南》。

- 查看命令日志，以获得在 **Server Administrator** 主页或其命令行界面执行过的所有命令的列表。

注：请参阅“Server Administrator 日志”；了解有关查看、打印、保存和电子邮件日志的完整说明。

Alert Management（警报管理）

子选项卡：“Alert Actions”（警报措施）|“Platform Events”（平台事件）|“SNMP Traps”（SNMP 陷阱）

在“**Alert Management**”（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“**Configure Destination**”（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。

  注：即使系统中不存在该组件传感器，“Alert Actions”（警报措施）窗口中也将列出所有可能存在的系统组件传感器的警报措施。为系统中不存在的系统组件传感器设置的警报措施无效。

Session Management（会话管理）

子选项卡：“Session”（会话）

在“**Session Management**”（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。

Main System Chassis / Main System（主系统机箱 / 主系统）

单击“**Main System Chassis / Main System**”（主系统机箱/主系统）对象，可以管理系统的重要硬件和软件组件。

可用的组件有：

- Batteries（电池）
- BIOS
- Fans（风扇）
- “Firmware”（固件）
- Hardware Performance（硬件性能）
- Intrusion（侵入）
- Memory（内存）
- Network（网络）
- Ports（端口）
- Power Management（电源管理）
- Power Supplies（电源设备）
- Processors（处理器）
- Remote Access（远程访问）
- Removable Flash Media（可移动闪存介质）
- Slots（插槽）
- Temperatures（温度）
- Voltages（电压）

注：硬件性能只在 Dell *xx0x* 系统上受支持。电源设备在 Dell PowerEdge 1900 系统上不可用。电源管理在有限的 Dell *xx0x* 和版本更高的系统上受支持。

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。“**Main System Chassis/Main System**”（主系统机箱/主系统）对象操作窗口具有以下选项卡：“**Properties**”（属性）。

Properties（属性）

子选项卡：“Health”（运行状况）|“Information”（信息）|“System Components（FRU）”（系统组件 [FRU]）|“Front Panel”（前面板）

在“**Properties**”（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况。每个列出的组件在其名称旁有“系统/服务器模块组件状况指示器”图标。  表示组件运行状况良好（正常）。  表示组件处于警告（非严重）状态并需要及时关注。  表示组件处于故障（严重）状态并需要立即关注。  表示组件的运行状况未知。可用的被监测组件包括：
  - Batteries（电池）
  - Fans（风扇）
  - 硬件日志
  - Intrusion（侵入）
  - Memory（内存）
  - Network（网络）
  - Power Management（电源管理）
  - Power Supplies（电源设备）
  - Processors（处理器）
  - Temperatures（温度）
  - Voltages（电压）

  注：电池只在 Dell PowerEdge *x9xx* 和 Dell *xx0x* 系统上受支持。电源设备在 Dell PowerEdge 1900 系统上不可用。电源管理在有限的 Dell *xx0x* 系统上受支持。
- 查看关于主系统机箱属性的信息，例如：主机名称、iDRAC 版本、生命周期控制器版本、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）属性是 Dell 系统服务标签的 11 位仅数字的转换。当致电 Dell 技术支持进行自动呼叫路由选择时，您可以将此属性在电话上键入。对于存储（DAS）不存在快速服务代码属性。
- 查看有关系统中安装的现场可更换单元（FRU）的详细信息（在“**System Components（FRU）**”（系统组件（FRU））子选项卡下）。
- 启用或禁用 Managed System 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 Managed System 的 LCD 安全访问级别。可以从下拉菜单中选择 Managed System 的 LCD 信息。还可以从“**Front Panel**”（前面板）子选项卡启用远程 KVM 指示会话。

Batteries（电池）

单击“**Batteries**”（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，“**Batteries**”（电池）对象操作窗口可包含以下选项卡：“**Properties**”（属性）和“**Alert Management**”（警报管理）。

Properties（属性）

子选项卡：“Information”（信息）

在“**Properties**”（属性）选项卡下，您可以查看系统电池的当前读数和状况。

Alert Management（警报管理）

在“**Alert Management**”（警报管理）选项卡下，可配置想要在出现电池警告或严重/故障事件时生效的警报。

BIOS

单击 **BIOS** 对象管理系统 BIOS 的主要功能。系统的 BIOS 包含存储在快擦写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（例如系统信息）。根据用户组权限的不同，**BIOS** 对象操作窗口可包含以下选项卡：“**Properties**”（属性）和“**Setup**”（设置）。

Properties（属性）

子选项卡：“Information”（信息）

在“**Properties**”（属性）选项卡下，您可以查看 BIOS 信息。

Setup（设置）

子选项卡：BIOS

在“**Setup**”（设置）选项卡下，可以设置每个 BIOS 设置对象的状态。

可修改多个 BIOS 设置功能的状态，这些功能包括（但不限于）串行端口、网络接口控制器卡、引导顺序、硬盘驱动器顺序、用户可拆卸 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、控制台重定向和控制台重定向故障自动保护波特率。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、嵌入式系统管理程序和主板上其它 LAN 网络端口的信息。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 F2 BIOS 设置屏幕，它在 Server Administrator 中却不可访问。

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“System Setup”（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。

注：您系统上的 BIOS 设置选项卡只显示系统上支持的 BIOS 功能。

Fans（风扇）

单击“**Fans**”（风扇）对象管理系统风扇。Server Administrator 通过测量风扇转速来监测每个系统风扇的状况。风扇探测器向 Server Administrator Instrumentation Service 报告风扇转速。从设备树中选择“**Fans**”（风扇）后，Server Administrator 主页右侧窗格的数据区域中将显示有关风扇的详细信息。根据用户组权限的不同，“**Fans**”（风扇）对象操作窗口可包含以下选项卡：“**Properties**”（属性）和“**Alert Management**”（警报管理）。

Properties（属性）

子选项卡：风扇探测器

在“**Properties**”（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（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。

Alert Management（警报管理）

子选项卡：“Alert Actions”（警报措施）|“SNMP Traps”（SNMP 陷阱）

在“**Alert Management**”（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。
- 查看当前 SNMP 陷阱警报阈值并为风扇设置警报阈值级别。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。

“Firmware”（固件）

单击“**Firmware**”（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。根据用户组权限的不同，“**Firmware**”（固件）对象操作窗口可包含以下选项卡：“**Properties**”（属性）。

Properties（属性）

子选项卡：“Information”（信息）

在“**Properties**”（属性）选项卡下，您可以查看系统的固件信息。

Hardware Performance（硬件性能）

单击“**Hardware Performance**”（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，“**Hardware Performance**”（硬件性能）对象操作窗口可包含以下选项卡：“**Properties**”（属性）。

表 4-1 列出可能的状况值和检测原因：

表 4-1. 可能的状况值和检测原因

状况值	原因值
降级	用户配置
	电源容量不足
	未知原因
正常	[N/A]

Properties（属性）

子选项卡：“Information”（信息）

在“**Properties**”（属性）选项卡下，可以查看系统性能降级的详情。

Intrusion（侵入）

单击“**Intrusion**”（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，“**Intrusion**”（侵入）对象操作窗口可包含以下选项卡：“**Properties**”（属性）和“**Alert Management**”（警报管理）。

Properties（属性）

子选项卡：“Intrusion”（侵入）

在“**Properties**”（属性）选项卡下，您可以查看机箱侵入状况。

Alert Management（警报管理）

子选项卡：“Alert Actions”（警报措施）|“SNMP Traps”（SNMP 陷阱）

在“**Alert Management**”（警报管理）选项卡下，您可以：

- 查看当前警报措施设置，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。

Memory（内存）

单击“**Memory**”（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，“**Memory**”（内存）对象操作窗口可包含以下选项卡：“**Properties**”（属性）和“**Alert Management**”（警报管理）。

Properties（属性）

子选项卡：“Memory”（内存）

在“**Properties**”（属性）选项卡下，您可以查看内存属性、内存设备详细信息和内存设备状况。

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

Alert Management（警报管理）

子选项卡：“Alert Actions”（警报措施）|“SNMP Traps”（SNMP 陷阱）

在“**Alert Management**”（警报管理）选项卡下，您可以：

- 查看当前警报措施设置，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。

Network（网络）

单击“**Network**”（网络） 对象可以管理系统的 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。Dell OpenManage Server Administrator 已在系统上配置时将报告 NIC 协作详情。两个或多个物理 NIC 可以组成单个逻辑 NIC，管理员可以给其分配 IP 地址。可以使用 NIC 供应商工具配置协作。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。如果配置了组接口，将显示详细的组属性。如果物理 NIC 是组接口的成员，还会报告这些物理 NIC 和组接口之间的关系，反之亦然。根据用户组权限的不同，“**Network**”（网络）对象操作串口可具有以下选项卡：“**Properties**”（属性）。

Properties（属性）

子选项卡：“Information”（信息）

在“**Properties**”（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 Addresses”（IPv6 地址）部分中，除了链路本地地址外，Server Administrator 仅显示两个地址。

Ports（端口）

单击“**Ports**”（端口）对象可以管理系统的外部端口。Server Administrator 可以监测系统中每个外部端口的状态。根据用户组权限的不同，“**Ports**”（端口）对象操作窗口可包含以下选项卡“**Properties**”（属性）。

Properties（属性）

子选项卡：“Information”（信息）

在“**Properties**”（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：电源管理功能仅对具有可热交换电源设备的 PowerEdge 系统可用，对安装了固定、非冗余电源设备的系统不可用。

Monitoring（监测）

子选项卡：“Consumption”（消耗）| “Statistics “（统计信息）

在“Consumption”（消耗）选项卡下，可以查看并管理系统的“Power Consumption”（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情。

还可以查看“System Instantaneous Headroom”（系统瞬间余量）和“System Peak Headroom”（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。

“Statistics”（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。

Management（管理）

子选项卡：“Budget”（预算） | “Profiles”（配置文件）

“Budget”（预算）选项卡使用户能够查看“Power Inventory”（功率资源清册）属性，比如“System Idle Power”（系统空闲功率）和“System Maximum Potential Power in Watts and BTU/hr”（系统最大潜在功率 [瓦特和 BTU/小时]）。还可以使用“Power Budget”（功率预算）选项为系统“Enable Power Cap”（启用功率限额）和设置“Power Cap”（功率限额）。

“Profiles”（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。

Alert Management（警报管理）

子选项卡：“Alert Actions”（警报措施） | “SNMP Traps”（SNMP 陷阱）

使用“Alert Actions”（警报措施）选项卡设置各种系统事件警报措施，比如“System Power Probe Warning”（系统功率探测器警报）和“System Peak Power”（系统峰值功率）。

使用“SNMP Traps”（SNMP 陷阱）选项卡为系统配置 SNMP 陷阱。

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

Power Supplies（电源设备）

单击“Power Supplies”（电源设备）对象可管理系统电源设备。Server Administrator 可以监测电源设备的状况（包括冗余），以确保系统中的所有电源设备都能正常运转。根据用户组权限的不同，“Power Supplies”（电源设备）对象操作窗口可包含以下选项卡：“**Properties**”（属性）和“**Alert Management**”（警报管理）。

Properties（属性）

子选项卡：“Elements”（要素）

在“**Properties**”（属性）选项卡下，您可以：

· 查看有关电源设备冗余属性的信息。

· 检查各个电源设备组件的状况，包括“Rated Input Wattage”（额定输入瓦特）和“Maximum Output Wattage”（最大输出瓦特）。“Rated Input Wattage”（额定输入瓦特）属性只在 *xx1x* 以后的 PMBus 系统上显示。

Alert Management（警报管理）

子选项卡：“Alert Actions”（警报措施）|“SNMP Traps”（SNMP 陷阱）

在“**Alert Management**”（警报管理）选项卡下，您可以：

- 查看当前警报措施设置，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措施。
- 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：“System Peak Power”（系统峰值功率）陷阱将只生成严重性为通知的事件。

Processors（处理器）

单击“**Processors**”（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，“**Processors**”（处理器）对象操作窗口可包含以下选项卡：“**Properties**”（属性）和“**Alert Management**”（警报管理）。

Properties（属性）

子选项卡：“Information”（信息）

在“**Properties**”（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。

Alert Management（警报管理）

子选项卡：“Alert Actions”（警报措施）

在**Alert Management**（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。

Remote Access（远程访问）

单击“**Remote Access**”（远程访问）对象管理底板管理控制器（BMC）或 Integrated Dell Remote Access Controller（iDRAC）功能和 Remote Access Controller 功能。

选择“Remote Access”（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：BMC 在 Dell PowerEdge *x8xx* 和 *x9xx* 系统中受支持，而 iDRAC 只在 Dell *xx0x* 和 *xx1x* 系统中受支持。

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。

根据用户组权限的不同，“**Remote Access**”（远程访问）对象操作窗口可包含以下选项卡：“**Properties**”（属性）、“**Configuration**”（配置）和“**Users**”（用户）。

Properties（属性）

子选项卡：“Information”（信息）

在“**Properties**”（属性）选项卡下，可以查看远程访问设备的一般信息。还可以查看 IPv4 和 IPv6 地址的属性。

单击“**Reset to Defaults**”（重设为默认值）可以将所有属性重设为系统默认值。

Configuration（配置）

子选项卡：LAN |“Serial Port”（串行端口）|“Serial Over LAN”（LAN 上串行）|“Additional Configuration”（其他配置）

在已配置 BMC/iDRAC 的情况下，可以在“**Configuration**”（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：“**Additional configuration**”（其它配置）选项卡仅在安装了 iDRAC 的系统上可用。

在已配置 DRAC 的情况下，可以在“**Configuration**”（配置）选项卡执行以下操作：

配置网络属性

注：启用网卡、NIC 选择和密钥字段只在 Dell PowerEdge *x9xx* 系统上显示。

在“Additional Configuration”（其它配置）选项卡下，可以启用或禁用 IPv4/IPv6 属性。

注：只能双堆栈环境（IPv4 和 IPv6 堆栈都载入）中启用/禁用 IPv4/IPv6。

Users（用户）

子选项卡：“Users”（用户）

在“**Users**”（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。

注：在 Dell PowerEdge *x9xx* 系统上：
- 显示十个用户 ID。如果装有 DRAC 卡，则显示十六个用户 ID。
- 显示 LAN 上串行有效载荷列。

Removable Flash Media（可移动闪存介质）

单击“**Removable Flash Media**”（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。“Removable Flash Media”（可移动闪存介质）操作窗口具有“**Properties**”（属性）选项卡。

Properties（属性）

子选项卡：“Information”（信息）

在“**Properties**”（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“Connector Name”（连接器名称）、其状态以及存储大小的详细信息。

Alert Management（警报管理）

子选项卡：“Alert Actions”（警报措施）|“SNMP Traps”（SNMP 陷阱）

在“**Alert Management**”（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。

Slots（插槽）

单击“**Slots**”（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。“**Slots**”（插槽）对象措施窗口具有“**Properties**”（属性）选项卡。

Properties（属性）

子选项卡：“Information”（信息）

在“**Properties**”（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。

Temperatures（温度）

单击“**Temperatures**”（温度）对象可以管理系统温度，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部各处的温度，以确保机箱内部温度不会太高。根据用户组权限的不同，“**Temperatures**<”（温度）对象操作窗口会显示以下选项卡：“**Properties**”（属性）和“**Alert Management**”（警报管理）。

Properties（属性）

子选项卡：“Temperature Probes”（温度探测器）

在“**Properties**”（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（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。

Alert Management（警报管理）

子选项卡：“Alert Actions”（警报措施）|“SNMP Traps”（SNMP 陷阱）

“**Alert Management**”（警报管理）选项卡下，您可以：

- 查看当前警报措施设置，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。

Voltages（电压）

单击“**Voltages**”（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，“**Voltages**”（电压）对象操作窗口可包含以下选项卡：“**Properties**”（属性）和“**Alert Management**”（警报管理）。

Properties（属性）

子选项卡：“Voltage Probes”（电压探测器）

在“**Properties**”（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。

Alert Management（警报管理）

子选项卡：“Alert Actions”（警报措施）|“SNMP Traps”（SNMP 陷阱）

在“**Alert Management**”（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。

Software（软件）

单击“**Software**”（软件）对象，则可以查看 managed system 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，“**Software**”（软件）对象操作窗口可包含以下选项卡：“**Properties**”（属性）。

Properties（属性）

子选项卡：“Summary”（摘要）

在“**Properties**”（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。

Operating System（操作系统）

单击“**Operating System**”（操作系统）对象，则可以查看有关操作系统的基本信息。根据用户组权限的不同，“**Operating System**”（操作系统）对象操作窗口可包含以下选项卡：“**Properties**”（属性）。

Properties（属性）

子选项卡：“Information”（信息）

在“**Properties**”（属性）选项卡下，您可以查看有关操作系统的基本信息。

Storage（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“**Typical Setup**”（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“**Storage**”（存储）对象可以查看各种所连阵列存储设备、卷、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，“**Storage**”（存储）对象操作窗口可包含以下选项卡：“**Properties**”（属性）。

Properties（属性）

子选项卡：“Health”（运行状况）

在“**Properties**”（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

“Preferences”（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 managed system 上安装的系统管理软件。

“Preferences”（首选项）主页的可用配置选项如下：

- General Settings（常规设置）
- Server Administrator

General Settings（常规设置）

单击“**General Settings**”（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，“**General Settings**”（常规设置）对象操作窗口可包含以下选项卡：“**User**”（用户）和 **Web Server**。

User（用户）

子选项卡：“Properties”（属性）

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

Web Server

子选项卡：“Properties”（属性）| “X.509 Certificate”（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。请参阅“Dell Systems Management Server 管理连接服务和安全设置”了解如何配置服务器首选项。
- 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，或导入认证机构（CA）颁发的根证书或证书链。有关证书管理的详情，请参阅X.509 认证管理。

Server Administrator

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并配置 SNMP root 密码。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：“**Preferences**”（首选项）。

Preferences（首选项）

子选项卡：“Access Configuration”（访问配置）| “SNMP Configuration”（SNMP 配置）

在“**Preferences**”（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。
- 配置 SNMP root 密码。

  注：默认的 SNMP 配置用户是 `root`，密码是 `calvin`。

- 配置 SNMP Set 操作。

  注：配置 SNMP Set 操作后，必须重新启动服务才能使更改生效。在运行所支持 Microsoft Windows 操作系统的系统上，必须重新启动 Windows SNMP Service。在运行受支持的 Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统的系统上，Server Administrator 服务必须通过运行 `srvadmin-services.sh restart` 命令来重新启动。

返回目录页面

返回目录页面

简介

Dell OpenManage Server Administrator 版本 6.4 用户指南

概览

Dell OpenManage Server Administrator（OMSA）通过两种方式提供了全面的、一对一的系统管理解决方案：通过集成的、基于 Web 浏览器的图形用户界面（GUI）和通过操作系统的命令行界面（CLI）。Server Administrator 适合系统管理员在本地或远程管理网络中的系统。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。

对于 Server Administrator 来说，系统可以是独立的系统、在单独机箱中连接有网络存储单元的系统，或者是由模块化机柜中的一个或多个服务器模块组成的模块化系统。

Server Administrator 可以提供以下信息：

- 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管理服务提供了易于使用的对本地和远程系统的管理和监控。Server Administrator 是被管理的系统上唯一的安装，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远程监测的系统。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。

安装

可以使用 *Dell Systems Management Tools and Documentation DVD*（*OM DVD*）安装 Server Administrator。该 DVD 提供了安装程序，用于安装、升级和卸载 Server Administrator、Managed System 及 management station 软件组件。此外，您还可以在无人值守的情况下，通过网络在多个系统上安装 Server Administrator。

Dell OpenManage 安装程序提供了在 Managed System 上安装和卸载 Dell OpenManage Server Administrator 和其它 Managed System 软件组件的安装脚本和 RPM 软件包。有关详情，请参阅《Dell OpenManage Server Administrator 安装指南》和《Dell OpenManage Management Station 软件安装指南》。您可以在 **support.dell.com / manuals** 访问这些文档。

注：当您从 OM DVD 安装开放源软件包时，对应的许可证文件会自动复制到系统。当您移除这些软件包时，对应的文件也会被移除。

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

更新各个系统组件

要更新各个系统组件，请使用组件特定的 Dell Update Packages。使用 *Dell Server Updates DVD* 查看完整的版本报告和更新整个系统。Server Update Utility 是一个基于 DVD-ROM 的应用程序，用于识别并应用对系统的更新。Server Update Utility 可以从 **support.dell.com** 下载。

请参阅《Server Update Utility 用户指南》，详细了解如何获取并使用 Server Update Utility（SUU）更新 Dell 系统或查看存储库中所列服务器的可用更新。

Storage Management Service

Storage Management Service 以集成图形视图方式提供 Storage Management 信息。

有关 Storage Management Service 的详情，请参阅 **support.dell.com / manuals** 上的《Dell OpenManage 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 为装有 Dell Remote Access Controller（DRAC）或底板管理控制器（BMC）/Integrated Dell Remote Access Controller（iDRAC）解决方案的系

统提供了全面的远程系统管理解决方案。Remote Access Controller 使您可以远程访问未运行的系统，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 还将记录系统崩溃的可能原因并保存最近一次的崩溃屏幕。

日志

Server Administrator 可以显示以下记录：向系统发送的命令或由系统发出的命令、受监测硬件的事件和系统警报。您可以在主页上查看记录，打印记录或将记录保存为报告，以及通过电子邮件将其发送到指定服务联络地址。

6.4 版新增功能

OpenManage Server Administrator 6.4 的发行亮点：

- 重新设计 Dell OpenManage Server Administrator 用户界面，改善整体用户体验，包括：
  - 如果登录页面中存在错误状况（例如错误的用户名或密码），则该错误信息会显示 30 秒，然后显示登录提示。要在 30 秒前获取登录提示，请单击“**Try Again**”（重试）。
  - “**Back to Server Administrator**”（返回到 Server Administrator）按钮重命名为“**Home**”（主页）。
  - 登录页面中的“**OK**”（确定）按钮重命名为“**Submit**”（提交）按钮。
  - “**Emai**”（电子邮件）、“**Export**”（导出）、“**Refresh**”（刷新）按钮现在显示为图标。
  - “**Help**”（帮助）图标与“**Email**”（电子邮件）、“**Export**”（导出）、“**Refresh**”（刷新）图标一起显示在页面的右上角。
  - 自定义图标（如“**Save as**”（另存为）、“**Clear Log**”（清除日志）、“**Restart**”（重新启动）和“**Reset to Default**”（重设为默认设置）分组在“**Options**”（选项）部分下。
  - “**User Rights**”（用户权限）和“**Host Name**”（主机名称）按钮现在显示在页面的左上角而不是右上角。
  - “**Manage Remote Node**”（管理远程节点）“、“**About**”（关于）和“**Support**”（支持）链接显示在登录页面的底部。
  - 所有按钮（例如“**Print**”（打印）、“**Export**”（导出）等等）都显示在所有 OMSA 页面上。仅适用于某个特定页面的按钮会启用，而其余按钮则呈灰色显示。
  - 数据区域中的按钮和链接具有工具提示功能。
  - 在“**System Summary**”（系统摘要）和“**Summary of Asset Information**”（资产信息摘要）页面中，“**Jump to**”（跳转到）和“**Back to top**”（返回顶部）链接不可用。但是，您可以展开和折叠页面中的每个部分。
  - “**About**”（关于）页面中的“**Details**”（详细信息）按钮不再存在。所有详细信息显示在同一个页面中。
- 增加了快速服务代码（ESC）属性。
- 增加了对以下操作系统的支持：
  - Microsoft Windows 2008 HPC Edition Server R2
  - Red Hat Enterprise Linux 6
  - VMware ESX 4.0 U2
  - VMware ESXi 4.0 U2
- 取消了对以下操作系统的支持：
  - Red Hat Enterprise Linux 4.8
  - VMware ESX 4.0 U1
  - VMware ESXi 4.0 U1
- 弃用外观首选项功能。
- 弃用页面级运行状态图标功能。

有关所支持的操作系统列表，请参阅 **support.dell.com/manuals** 上的《Dell 系统软件支持值表》。

有关此版本推出的功能的详情，请参阅 Server Administrator 上下文相关联机帮助。

系统管理标准可用性

Dell OpenManage Server Administrator 支持下列主要的系统管理协议：

- 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。

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。

有关 SNMP 安全性顾虑的信息，请参阅 Dell OpenManage Server Administrator **自述**文件（与 Server Administrator 应用程序打包在一起），**support.dell.com/manuals** 上也提供了该文件。必须从操作系统的主 SNMP 代理应用更新，以确保 Dell SNMP 子代理的安全。

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/WMI（Windows 管理工具）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 OpenManage IT Assistant 来执行。

表 1-1 说明了每个支持的操作系统可用的系统管理标准。

表 1-1. 系统管理标准可用性

操作系统	SNMP	CIM
Windows Server 2008 系列和 Windows Server 2003 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 ESX	可通过操作系统安装的 **net-snmp**软件包获得	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
Citrix XenServer 5.6.	可通过操作系统安装介质中的 **net-snmp** 软件包获得	不可用

Server Administrator 主页

Server Administrator 主页提供了易于设置和使用的、基于 Web 浏览器的系统管理任务，可以从 Managed System 或从远程主机（通过 LAN、拨号服务或无线网络）对系统进行管理。在 Managed System 上安装并配置 Dell Systems Management Server Administrator 连接服务（DSM SA 连接服务）后，可以从具有所支持 Web 浏览器和连接的任何系统执行远程管理功能。此外，**Server Administrator** 主页还提供了广泛的、上下文相关的联机帮助。

您可能需要的其它说明文件

除了本指南，您可以在 **support.dell.com/manuals** 中获取如下指南。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以访问文档。

- 《Dell 系统软件支持值表》提供了有关各种 Dell 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 Dell OpenManage 组件的信息。
- 《Dell OpenManage Server Administrator 安装指南》包*含帮助安装 Dell OpenManage Server Administrator 的说明*。
- 《Dell OpenManage Management Station 软件安装指南》包*含帮助安装 Dell OpenManage Management Station 软件的说明*，该软件中包括 Baseboard Management Utility、DRAC 工具和 Active Directory 管理单元。
- 《Dell OpenManage Server Administrator SNMP 参考指南》介绍了简单网络管理协议（SNMP）管理信息库（MIB）。SNMP MIB 定义了标准 MIB 之外的变量，以涵盖系统管理代理功能。
- 《Dell 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。CIM 提供程序 MOF 介绍了支持的管理对象的类。
- 《Dell OpenManage Server Administrator 信息参考指南》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信息。该指南解释了 Server Administrator 发出的每个 Instrumentation Service 警报信息的内容、严重性和原因。
- 《Dell OpenManage Server Administrator 命令行界面用户指南》介绍了 Server Administrator 的完整命令行界面，包括对查看系统状况、访问日志、创建报告、配置各种组件参数和设置临界阈值的 CLI 命令的解释。
- 《Integrated Dell Remote Access Controller 用户指南》提供了有关配置和使用 iDRAC 的详细信息。
- 《Dell Chassis Management Controller 用户指南》提供了有关安装、配置和使用 CMC 的详细信息。
- 《Dell 联机诊断程序用户指南》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 底板管理控制器公用程序用户指南》提供了有关使用 Server Administrator 来配置和管理系统的 BMC 的其他信息。
- 《Dell OpenManage Server Administrator Storage Management 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 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 5 用户指南》提供了有关安装和配置 DRAC 5 控制器以及使用 DRAC 5 远程访问不运行系统的完整信息。
- 《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 OpenManage Server Update Utility 用户指南》介绍了如何获取并使用 Server Update Utility（SUU）更新 Dell 系统或查看存储库中所列系统的可用更新。
- 《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 Management Console 是基于 Web 的系统管理软件，利用它可以查找网络上的设备并编制资源清册。它还提供高级功能，例如联网设备的运行状况和性能监控，以及 Dell 系统的增补软件管理功能。
- 《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。Unified Server Configurator 可以用于部署操作系统、配置独立磁盘冗余阵列（RAID），以及运行诊断程序来验证系统和连接的硬件。远程服务功能实现了通过管理控制台进行自动化系统平台发现，并增强了远程操作系统部署功能。这些功能均通过由 Lifecycle Controller 固件提供的基于 Web 服务的硬件管理界面公开。
- 包含本说明文件中所使用术语相关信息的*词汇表*。

获得技术帮助

如果没有理解本指南中介绍的程序或者产品没有按照预期的方式运行，可以使用一些帮助工具来予以协助。有关这些帮助工具的详情，请参阅系统《硬件用户手册》中的“获得帮助”。

另外，Dell 可以提供企业培训和认证；有关详情，请参阅 **dell.com/training**。此服务可能并非在所有地区都有提供。

返回目录页面

返回目录页面

Server Administrator 日志

Dell OpenManage Server Administrator 版本 6.4 用户指南

概览

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“Administrator”（管理员）权限登录才能清除日志，或者必须以“Administrator”（管理员）或“Power User”（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。

请参阅《Dell OpenManage Server Administrator 命令行界面用户指南》，了解有关从命令行查看日志和创建报告的信息。

查看 Server Administrator 日志时，您可以单击“**Help**”（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。

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

- 单击“**Print**”（打印）可将一份日志打印至默认打印机。
- 单击“**Export**”（导出）可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。
- 单击“**Email**”（电子邮件）可创建包含日志内容（作为附件）的电子邮件信息。
- 单击“**Clear Log**”（清除日志）可删除日志中的所有事件。
- 单击“**Save As**”（另存为）可将日志内容保存在 **.zip** 文件中。
- 单击“**Refresh**”（刷新）可在操作窗口数据区域中重新载入日志内容。

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

使用硬件日志可查找系统硬件组件的潜在故障。在 Dell PowerEdge *x8xx*、*x9xx* 和 *xx1x* 系统上，硬件日志状况标志将在日志文件达到 100% 的容量时变为严重状况（ ）。硬件日志有两种（取决于您的系统）：嵌入式 System Management（ESM）日志和系统事件日志（SEL）。ESM 日志和 SEL 日志均为一组嵌入式指令，可以向系统管理软件发送硬件状况信息。日志中列出的每个组件的名称旁边均有一个状况标志图标。绿色复选标记（ ）表示组件状况良好（正常）。包含感叹号的黄色三角形（ ）表示组件处于警告（不严重）状况并需要及时处理。红色的 X（ ）表示组件处于故障（严重）状况并需要立即处理。空白的（ ）表示组件的运行状况未知。

要访问硬件日志，请单击“**System**”（系统），单击“**Logs**”（日志）选项卡，然后单击“**Hardware**”（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

当日志文件达到 80% 的容量时，Server Administrator 主页上日志名称旁的状况标志图标会从正常状态（  ）更改为非严重状态（  ）。请确保在硬件日志达到 80% 容量时清理日志。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。

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“**Clear Log**”（清除日志），之后重新显示日志信息。

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的标识符（称为事件 ID）和事件信息（用于说明事件）组成。事件 ID 和事件信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。

要查看警报日志，请单击“**System**”（系统），单击“**Logs**”（日志）选项卡，然后单击“**Alert**”（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记录。因此，建议您保存日志文件。

有关警报信息的详细信息，请参阅《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“**Clear Log**”（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“**System**”（系统），单击“**Logs**”（日志）选项卡，然后单击“**Command**”（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。

返回目录页面

返回目录页面

使用 Remote Access Controller

Dell OpenManage Server Administrator 版本 6.4 用户指南

注：*底板管理控制器（BMC）*在 Dell PowerEdge *x8xx* 和 *x9xx* 系统中受支持，而 *Integrated Dell Remote Access Controller（iDRAC）*在 Dell *xx0x* 和 *xx1x* 系统中受支持。

概览

本章介绍有关访问和使用 BMC/iDRAC 和 DRAC 的远程访问功能的信息。

Dell 系统底板管理控制器（BMC）/Dell 集成远程访问控制器（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。

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

通过与系统的底板管理控制器（BMC）/Dell 集成远程访问控制器（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崩溃屏幕（仅限运行 Microsoft Windows 操作系统的系统）来帮助诊断系统崩溃的可能原因。

Remote Access Controller 使您可以远程访问未运行的系统，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 还将记录系统崩溃的可能原因并保存*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“**Help**”（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：请参阅《Dell OpenManage 底板管理控制器公用程序用户指南》以了解 BMC 的详情。

注：请参阅《Dell Remote Access Controller 4 用户指南》了解使用 DRAC 4 的更多信息，或参阅《Dell Remote Access Controller 5 用户指南》了解使用DRAC 5 的更多信息。

注：请参阅《Integrated Dell Remote Access Controller 用户指南》了解有关配置和使用 iDRAC 的详细信息。

Server Administrator 安装在系统后，表 5-1 列出 GUI 字段名称和可应用的系统。

表 5-1. 以下 GUI 字段名称的系统可用性

GUI 字段名称	可应用的系统
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

请参阅《Dell 系统软件支持值表》了解有关远程访问设备系统支持的详情。

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。单击 **Remote Access** 对象（“**Main System Chassis/Main System**”（主系统机箱/主系统）组的一个子组件），可通过 Server Administrator 图形用户界面管理 BMC/iDRAC 和 DRAC。

可以执行以下任务：

- 查看基本信息
- 配置 LAN 连接上的远程访问设备
- 配置 LAN 上串行连接上的远程访问设备
- 配置串行端口连接上的远程访问设备
- 配置其它远程访问设备属性

- 配置远程访问设备上的用户
- 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` 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。

注：您只能在 Dell PowerEdge *x8xx* 和 *x9xx* 系统上查看 BMC 数据。

查看基本信息

可以查看有关 BMC/iDRAC、IPv4 地址和 DRAC 的基本信息。还可以将远程访问控制器设置重设为默认值。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“**Modular Enclosure**”（模块化机柜）→“**System / Server Module**”（系统/服务器模块）→“**Main System Chassis / Main System**”（主系统机箱/主系统）→ **Remote Access**。

Remote Access 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
- 可能激活的会话数
- 目前激活的会话数
- “LAN Enabled”（LAN 已启用）
- “SOL Enabled”（SOL 已启用）
- “MAC Address”（MAC 地址）

“IPv4 Address”（IPv4 地址）

- “IP Address Source”（IP 地址源）
- “IP Address”（IP 地址）
- IP Subnet（IP 子网）
- IP Gateway（IP 网关）

“IPv6 Address”（IPv6 地址）

- “IP Address Source”（IP 地址源）
- IPv6 Address 1（IPv6 地址 1）
- “Default Gateway”（默认网关）
- IPv6 Address 2（IPv6 地址 2）
- “Link Local Address”（链路本地地址）
- “DNS Address Source”（DNS 地址源）
- “Preferred DNS Server”（首选 DNS 服务器）
- “Alternate DNS Server”（备用 DNS 服务器）

注：只有在“**Remote Access**”（远程访问）选项卡的“**Additional Configuration**”（其它配置）下启用 IPv4 和 IPv6 地址属性后，才能查看 IPv4 和 IPv6 地址详情。

配置远程访问设备使用 LAN 连接

可以配置远程访问设备通过 LAN 连接进行通信。

1. 单击“**Modular Enclosure**”（模块化机柜）→“**System / Server Module**”（系统/服务器模块）→“**Main System Chassis / Main System**”（主系统机箱/主系统）→ **Remote Access** 对象。
2. 单击“**Configuration**”（配置）选项卡。

3. 单击 **LAN**。

“**LAN Configuration**”（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 配置详情：

- 启用网卡（此选项在 Dell PowerEdge *x9xx* 系统上且在已装有 DRAC 的情况下可用。选择此选项以进行网卡分组。在 Dell PowerEdge *x9xx* 系统中，可将 NIC 组合起来以增加冗余。）

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 地址与同一网络上其他 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 Selection”（NIC 选择）

注：不能在模块化系统上配置“**NIC Selection**”（NIC 选择）。

- “Enable IPMI Over LAN”（启用 LAN 上 IPMI）
- “IP Address Source”（IP 地址源）
- IP 地址
- Subnet Mask（子网掩码）
- Gateway Address（网关地址）
- “Channel Privilege Level Limit”（信道权限级别限制）
- 新密钥（此选项在 Dell PowerEdge *x9xx* 系统中可用。）

5. 配置以下可选 VLAN 配置详情：

注：VLAN 配置在具有 iDRAC 的系统上不可用

- “Enable VLAN ID”（启用 VLAN ID）
- VLAN ID
- 优先权

6. 配置以下 IPv4 属性：

- “IP Address Source”（IP 地址源）
- “IP Address”（IP 地址）
- Subnet Mask（子网掩码）
- Gateway Address（网关地址）

7. 配置以下 IPv6 属性：

- “IP Address Source”（IP 地址源）
- “IP Address”（IP 地址）
- “Prefix Length”（前缀长度）
- “Default Gateway”（默认网关）
- “DNS Address Source”（DNS 地址源）
- “Preferred DNS Server”（首选 DNS 服务器）
- “Alternate DNS Server”（备用 DNS 服务器）

注：只有在“Additional Configuration”（其它配置）下启用 IPv4 和 IPv6 属性后，才能配置 IPv4 和 IPv6 地址详情。

8. 单击“**Apply Changes**”（应用更改）。

配置远程访问设备使用串行端口连接

您可以在串行端口连接上配置 BMC 以用于通信。要执行此操作：

1. 单击“**Modular Enclosure**”（模块化机柜）→“**System/Server Module**”（系统/服务器模块）→“**Main System Chassis/Main System**”（主系统机箱/主系统）→ **Remote Access**。
2. 单击“**Configuration**”（配置）选项卡。
3. 单击“**Serial Port**”（串行端口）。

   “**Serial Port Configuration**”（串行端口配置）窗口会出现。
4. 配置以下详情：
   - 连接模式设置
   - “Baud Rate”（波特率）
   - “Flow Control”（流控制）
   - “Channel Privilege Level Limit”（信道权限级别限制）
5. 单击“**Apply Changes**”（应用更改）。
6. 单击“**Terminal Mode Settings**”（终端模式设置）。

   在“**Terminal Mode Settings**”（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）信息传递。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：
   - “Line Editing”（行编辑）
   - “Delete Control”（删除控制）
   - “Echo Control”（回声控制）
   - “Handshaking Control”（符号交换控制）
   - “New Line Sequence”（新行序列）
   - “Input New Line Sequence”（输入新行序列）
8. 单击“**Apply Changes**”（应用更改）。
9. 单击“**Back To Serial Port Configuration Window**”（返回串行端口配置窗口）以返回到“**Serial Port Configuration**”（串行端口配置）窗口。

配置远程访问设备使用 LAN 上串行连接

您可以在 LAN 上串行（SOL）连接配置 BMC/iDRAC 以用于通信。要执行此操作：

1. 单击“**Modular Enclosure**”（模块化机柜）→ ”**System/Server Module**”（系统/服务器模块）→ ”**Main System Chassis/Main System**”（主系统机箱/主系统）→ **Remote Access**。
2. 单击“**Configuration**”（配置）选项卡。
3. 单击“**Serial Over LAN**”（LAN 上串行）。

   “**Serial Over LAN Configuration**”（LAN 上串行配置）窗口会出现。
4. 配置以下详情：
   - “Enable Serial Over LAN”（启用 LAN 上串行）
   - “Baud Rate”（波特率）
   - 所需的最小权限

5. 单击“**Apply Changes**”（应用更改）。
6. 单击“**Advanced Settings**”（高级设置）进一步配置 BMC。
7. 在“**Serial Over LAN Configuration Advanced Settings**”（LAN 上串行配置高级设置）窗口中，可以配置以下信息：
   - “Character Accumulate Interval”（字符积累间隔时间）
   - “Character Send Threshold”（字符发送阈值）
8. 单击“**Apply Changes**”（应用更改）。
9. 单击“**Go Back to Serial Over LAN Configuration**”（返回 LAN 上串行配置）以返回到“**Serial Over LAN Configuration**”（LAN 上串行配置）窗口。

---

iDRAC 的其它配置

可以使用“**Additional Configuration**”（其它配置）选项卡配置 IPv4 和 IPv6 属性。要执行此操作：

1. 单击“**Modular Enclosure**”（模块化机柜）→ ”**System/Server Module**”（系统/服务器模块）→ ”**Main System Chassis/Main System**”（主系统机箱/主系统）→ **Remote Access** 对象。
2. 单击“**Configuration**”（配置）选项卡。
3. 单击“**Additional Configuration**”（其它配置）。
4. 将 IPv4 和 IPv6 属性配置为”**已**”**Enabled**”（启用）或”**Disabled**”（已禁用）。
5. 单击“**Apply Changes**”（应用更改）。

配置远程访问设备用户

可以使用“**Remote Access**”（远程访问）页配置远程访问设备用户。要访问此页：

1. 单击“**Modular Enclosure**”（模块化机柜）→“**System/Server Module**”（系统/服务器模块）→“**Main System Chassis/Main System**”（主系统机箱/主系统）→ **Remote Access** 对象。
2. 单击“**User**”（用户）选项卡。

   “**Remote Access Users**”（Remote Access 用户）窗口显示可配置为 BMC/iDRAC 用户的用户的信息。
3. 单击“**User ID**”（用户 ID）可以配置一个新的或现有的 BMC/iDRAC 用户。

   “**Remote Access User Configuration**”（Remote Access 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“**Enable User**”（启用用户）以启用该用户。
   - 在“**User Name**”（用户名）字段中输入用户的名称。
   - 选择“**Change Password**”（更改密码）复选框。
   - 在“**New Password**”（新密码）字段中键入新密码。
   - 在“**Confirm New Password**”（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。
   - 在 Dell PowerEdge *x9xx* 系统中，选择“**Enable Serial Over LAN**”（启用 LAN 上串行）以启用 LAN 上串行。
6. 为 DRAC/iDRAC 用户权限指定用户组。
7. 单击“**Apply Changes**”（应用更改）以保存更改。

8. 单击“**Back to Remote Access User Window**”（返回至 Remote Access 用户窗口）以返回至“**Remote Access Users**”（Remote Access 用户）窗口。

注：当安装了 DRAC 时，有六个附加的用户项可配置。这导致出现总共 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

您可以使用 Server Administrator Instrumentation Service 配置最密切相关的 BMC 功能，如平台事件筛选器（PEF）参数和警报目标。要执行此操作：

1. 单击“**System**”（系统）对象。
2. 单击“**Alert Management**”（警报管理）选项卡。
3. 单击“**Platform Events**”（平台事件）。

   “**Platform Events**”（平台事件）窗口可以让您针对具体平台事件采取单独措施。您可以选择那些想要为其执行关机操作，并为所选操作生成警报的事件。您也可以将警报发送到选定的 IP 地址目标。

   注：必须以“管理员”权限登录才能配置 BMC PEF 警报。

   注：“Enable Platform Event Filters Alerts”（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。它是独立的平台事件警报设置。

   注：“**System Power Probe Warning**”（系统电源探测器警告）和“**System Power Probe Failure**”（系统电源探测器故障）在没有 PMBus 支持的 Dell 系统上得不到支持，即使 Server Administrator 允许用户配置亦然。

   注：在 Dell PowerEdge 1900 系统上，不支持 **PS/VRM/D2D 警告**、**PS/VRM/D2D 故障**和没**有电源设备**等平台事件筛选器，即使 Server Administrator 允许配置这些事件筛选器。

4. 选择想要为其执行关机操作或为所选操作生成警报的事件，然后单击“**Set Platform Events**”（设置平台事件）。

   “**Set Platform Events**”（设置平台事件）窗口可以让您指定系统在关机以响应平台事件时采取的措施。

5. 选择以下一项措施：

   - **None（无）**
     操作系统挂起或崩溃时不采取任何措施。
   - **Reboot System（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。
   - **Power Cycle System（关闭并打开系统电源）**
     关闭系统电源、暂停、打开电源并重新引导系统。如果您想重新初始化系统组件（例如硬盘驱动器），关闭并打开系统电源会非常有用。
   - **Power Off System（关闭系统电源）**
     关闭系统的电源。
   - **Power Reduction（功率降低）**
     调节 CPU。

注：所有系统均不支持低功率运行。

小心: 如果选择平台事件关机操作而不是无操作或功率降低，在指定事件发生时系统将会强制关闭。该关闭系统操作是由固件启动的，完成执行无需事先关闭操作系统或任何运行的应用程序。

6. 选择要发送警报的“**Generate Alert**”（生成警报）复选框。

   注：要生成一个警报，必须选择“Generate Alert”（生成警报）和“Enable Platform Events Alerts”（启用平台事件警报）设置。

7. 单击“**Apply Changes**”（应用更改）。
8. 单击“**Go Back to Platform Events Page**”（返回平台事件页）以返回到“**Platform Event Filters**”（平台事件筛选器）窗口。

设置平台事件警报目标

您也可以使用 “**Platform Event Filters**”（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一个单独的 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“**Platform Event Filters**”（平台事件筛选器）窗口中的“**Configure Destinations**”（配置目标）。

   “**Configure Destinations**”（配置目标）窗口显示了许多目标。

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. 选择“**Enable Destination**”（启用目标）复选框。

4. 单击“**Destination Number**”（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。

5. 在“**Community String**”（团体字符串）字段中输入一个值用作验证 management station 和 managed system 之间所发出信息的密码。团体字符串（也称团体名称）在 management station 和 managed system 之间的每个数据包内发送。

6. 单击“**Apply Changes**”（应用更改）。

7. 单击“**Go Back to Platform Events Page**”（返回平台事件页）以返回到“**Platform Event Filters**”（平台事件筛选器）窗口。

返回目录页面

返回目录页面

设置和管理

Dell OpenManage Server Administrator 版本 6.4 用户指南

安全管理

Dell OpenManage 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。

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的用户权限。通过 RBAC，安全管理与组织的结构密切相关。

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。四种用户级别为：“User”（用户）、“Power User”（高级用户）、“Administrator”（管理员）和“Elevated Administrator”（提升管理员）。

- “*User*”（用户）可以查看大多数信息。
- “*Power User*”（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措施。
- “*Administrator*”（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。
- “*Elevated Administrators*”（提升管理员）可以查看和管理信息。

Server Administrator 赋予以“*User*”（用户）权限登录的用户只读访问权限；赋予以“*Power User*”（高级用户）权限登录的用户读写访问权限；赋予以“*Administrator*”（管理员）和“*Elevated Administrator*”（提升管理员）权限登录的用户读、写和管理员访问权限。请参阅 2-1。

表 2-1. 用户权限

用户权限	访问类型	
	视图	管理
User（用户）	是	否
高级用户	是	是
管理员	是	是
提升管理员（仅 Linux）	是	是

访问 Server Administrator 服务的权限级别

表 2-2 总结了哪些用户级别有权访问和管理 Server Administrator 服务。

表 2-2. Server Administrator 用户权限级别

服务	所需用户权限级别	
	视图	管理

工具	U, P, A, EA	P, A, EA
远程访问	U, P, A, EA	A, EA
存储管理	U, P, A, EA	A, EA

表 2-3 定义了在表 2-2 中使用的用户权限级别缩写。

表 2-3. Server Administrator 用户权限级别说明

U	User（用户）
P	高级用户
A	管理员
EA	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，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上下文。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

对于支持的 Microsoft Windows 操作系统，Server Administrator 验证使用集成 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

对于支持的 Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统，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客户管理协议（比如 LDAP、NIS、Kerberos 和 Winbind）从本地或远程登录 Server Administrator。

VMware ESX Server 4.X

当用户访问 ESX Server 主机时，VMware ESX Server 使用可插拔验证模块（PAM）结构进行验证。VMware 服务的 PAM 配置位于用于存储验证模块的路径的 /etc/pam.d/vmware-authd 中。

ESX Server 的默认安装使用 /etc/passwd 验证，与 Linux 的验证方式完全相同，但可以将 ESX Server 配置为使用其它分布式验证机制。

注：在运行 VMware ESX Server 4.1 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。

VMware ESXi Server 4.X

ESXi Server 使用 vSphere/VI Client 或 Software Development Kit（SDK）验证访问 ESXi 主机的用户。ESXi 的默认安装使用本地密码数据库进行验证。ESXi 与 Server Administrator 的验证事务也是与 **vmware-hostd** 进程的直接交互。要确保验证能够为站点高效工作，请执行设置用户、组、权限和角色，配置用户属性，添加自己的证书，以及确定是否要使用 SSL 等基本任务。

注：在运行 VMware ESXi Server 4.1 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）保护用户凭据和其它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 Dell OpenManage 软件之前给所有 Dell 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 Dell OpenManage 软件。

小心：要保护对重要系统组件的访问，请为可以访问 Dell OpenManage 软件的每个用户帐户分配密码。根据操作系统的设计，没有分配密码的用户不能登录运行 Windows Server 2003 的系统上的 Dell OpenManage 软件。

小心：禁用所支持 Windows 操作系统的宾客帐户以保护对重要系统组件的访问。考虑重命名帐户，这样远程脚本无法使用该名称启用帐户。

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：如果要向 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：要执行以下步骤，系统上必须装有 Microsoft Active Directory。有关使用 Active Directory 的详情，请参阅使用 Active Directory 登录。

1. 导航到“**Control Pane**”（控制面板）→“**Administrative Tools**”（管理工具）→“**Active Directory Users and Computers**”（Active Directory 用户和计算机）。
2. 在控制台树中，右键单击“**Users**”（用户），或者右键单击想向其中添加新用户的容器，然后指向“**New**”（新建）→“**User**”（用户）。
3. 在对话框中键入相应的用户名信息并单击“**Next**”（下一步）。
4. 单击“**Next**”（下一步），然后单击“**Finish**”（完成）。
5. 双击表示刚创建的用户的图标。
6. 单击“**Member of**”（成员）选项卡。
7. 单击 **Add**（添加）。
8. 选择相应的组并单击“**Add**”（添加）。
9. 单击“**OK**”（确定），然后再次单击“**OK**”（确定）。

   新用户可使用为其组和域分配的用户权限登录至 Dell OpenManage 软件。

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

“Administrator”（管理员）访问权限将分配给以 root 登录的用户。要创建具有“User”（用户）和“Power User”（高级用户）权限的用户，请执行以下步骤。

注：要执行以下步骤，必须以 root 或等同的用户身份登录。

注：要执行以下步骤，系统中必须已安装 **useradd** 公用程序。

创建用户

注：有关创建用户和用户组的信息，请参阅您的操作系统说明文件。

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 <*主目录*> -g <*组*> <*用户名*>

   其中 <*组*> 不是 root

   注：如果 <组> 不存在，则用 **groupadd** 命令创建它。

2. 键入 passwd <*用户名*> 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“Power User”（高级用户）权限的用户

1. 通过命令行运行以下命令：

   useradd -d <主目录> -g root <*用户名*>

   注：将 root 设置为主要组。

2. 键入 passwd <*用户名*> 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：以 root 或具有同等权限的用户身份登录才能执行这些步骤。

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>*

   表 2-4 列出向 *omarolemap* 文件添加角色定义的说明

表 2-4. 在 OpenManage Server Administrator 中添加角色定义的说明

<User_Name>	**<Host_Name>**	**<Rights>**
用户名	“Host Name ”（主机名）	管理员
(+）组名	域	User（用户）
通配符（*）	通配符（*）	User（用户）
[Tab] = \t（tab 字符）		

表 2-5 列出向 *omarolemap* 文件添加角色定义的说明

表 2-5. 在 OpenManage Server Administrator 中添加角色定义的说明

<User_Name>	**<Host_Name>**	**<Rights>**
Bob	Ahost	高级用户
+root	Bhost	管理员
+root	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

以下列出使用 **omarolemap** 文件的最佳做法：

- 请勿删除 **omarolemap** 文件中的以下默认条目。

• root	*	管理员
• +root	*	高级用户
• *	*	User（用户）

- 请勿更改 **omarolemap** 文件权限或文件格式。
- 如果用户在 **omarolemap** 文件中降级，Server Administrator 会使用默认操作系统用户权限。
- 请勿为 *<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** 文件从一个机器复制到另一个机器后，需要重新检查文件权限和文件的条目。
- 在*组名*前加上 +。
- 如果有重复的用户名或用户组条目以及相同的 *<Host_Name>*，Server Administrator 会使用默认的操作系统用户权限。
- 还可以不使用 [Tab]，而使用空格作为列分隔符。

为 VMware ESX 4.X 和 ESXi 4.X 创建 Server Administrator 用户

要向用户表添加用户：

1. 使用 vSphere 客户端登录到主机。
2. 单击“**Users & Groups**”（用户和组）选项卡，然后单击“**Users**”（用户）。
3. 右键单击“Users”（用户）表中的任意位置，然后单击“**Add**”（添加）以打开“**Add New User**”（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 ESX/ESXi 主机，请选中“**Grant shell access to this user**”（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“**Group**”（组）下拉式菜单中选择组名称并单击“**Add**”（添加）。
7. 单击 **OK**（确定）。

在支持的 Windows 操作系统中禁用来宾和匿名帐户

注：必须以“Administrator”（管理员）权限登录才能执行此步骤。

1. 打开“**Computer Management**”（计算机管理）窗口。
2. 在控制台树中，展开“**Local Users and Groups**”（本地用户和组）并单击“**Users**”（用户）。
3. 双击“**Guest**”（来宾）或 **IUSR_system** 名称用户帐户，查看这些用户的属性，或右键单击“**Guest**”（来宾）或 **IUSR_system** 名称用户帐户，然后选择“**Properties**”（属性）。
4. 选择“**Account is disabled**”（帐户已禁用），然后单击“**OK**”（确定）。

   带有 X 的红圈会显示在用户名上。该帐户已禁用。

配置 SNMP 代理

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，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，以更改团体名称、启用 Set 操作及向 Management Station（管理站）发送陷阱。要配置 SNMP 代理以正确地与管理应用程序（例如 Dell OpenManage IT Assistant）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 **public**。由于安全原因，更改 SNMP 团体名称的默认值。有关更改 SNMP 团体名称的信息，请参阅以下相关章节。

注：SNMP Set 默认情况下在 Server Administrator 5.2 或更高版本中禁用。Server Administrator 提供了相关支持来在 Server Administrator 中启动或禁用 SNMP Set 操作。可以使用“**Preferences**”（首选项）下的 **Server Administrator SNMP 配置**页或 Server Administrator 命令行界面（CLI）来启动或禁用 Server Administrator 中的 SNMP Set 操作。有关 Server Administrator CLI 的详细信息，请参阅《Dell OpenManage Server Administrator 命令行界面用户指南》。

注：为了使 IT Assistant 可以从运行 Server Administrator 的系统检索管理信息，IT Assistant 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 IT Assistant 可以在运行 Server Administrator 的系统上修改信息或执行操作，IT Assistant 所使用的团体名称必须与运行 Server Administrator 的系统上允许设置操作的团体名称匹配。为了使 IT Assistant 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 IT Assistant 的系统。

以下步骤提供了在每个支持的操作系统上配置 SNMP 代理的逐步说明：

- “在运行支持的 Windows 操作系统的系统中配置 SNMP 代理”
- “在运行支持的 Red Hat Enterprise Linux 的系统上配置 SNMP 代理”
- “在运行支持的 SUSE Linux Enterprise Server 的系统中配置 SNMP 代理”
- “在运行支持的 VMware ESX 4.X 操作系统的系统上将 SNMP 代理配置为代理 VMware MIB”
- “在运行支持的 VMware ESXi 4.X 操作系统的系统上配置 SNMP 代理”

在运行支持的 Windows 操作系统的系统中配置 SNMP 代理

Server Administrator 使用 Windows SNMP 代理提供的 SNMP 服务。您可以配置 SNMP 代理，以更改团体名称、启用 Set 操作及向 Management Station 发送陷阱。要配置 SNMP 代理以正确地与管理应用程序（例如 IT Assistant）进行交互，请执行以下各节中说明的步骤。

注：有关 SNMP 配置的其它详细信息，请参阅操作系统说明文件。

通过远程主机启用 SNMP 访问

默认情况下，Windows Server 2003 不接受来自远程主机的 SNMP 数据包。对于运行 Windows Server 2003 的系统，如果您打算使用远程主机上的 SNMP 管理应用程序来管理系统，则必须配置 SNMP 服务接受来自远程主机的 SNMP 数据包。

要使运行 Windows Server 2003 操作系统的系统能够接收来自远程主机的 SNMP 数据包，请执行下列步骤：

1. 打开“**Computer Management**”（计算机管理）窗口。
2. 如果有必要，请展开窗口中的“**Computer Management**”（计算机管理）图标。
3. 展开“**Services and Applications**”（服务和应用程序）图标并单击“**Services**”（服务）。
4. 向下滚动服务列表，直至找到“**SNMP Service**”（SNMP 服务），右键单击“**SNMP Service**”（SNMP 服务），然后单击“**Properties**”（属性）。

   将显示“**SNMP Service Properties**”（SNMP 服务属性）窗口。
5. 单击“**Security**”（安全）选项卡。
6. 选择“**Accept SNMP packets from any host**”（接受来自所有主机的 SNMP 数据包），或将该远程主机添加到“**Accept SNMP packets from these hosts**”（接受这些来自主机的 SNMP 数据包） 列表。

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 团体名称必须与在 Server Administrator 系统上配置的 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“**Computer Management**”（计算机管理）窗口。
2. 如果有必要，请展开窗口中的“**Computer Management**”（计算机管理）图标。
3. 展开“**Services and Applications**”（服务和应用程序）图标并单击“**Services**”（服务）。
4. 向下滚动服务列表，直至找到“**SNMP Service**”（SNMP 服务）。右键单击“**SNMP Service**”（SNMP 服务），然后单击“**Properties**”（属性）。

   将显示“**SNMP Service Properties**”（SNMP 服务属性）窗口。
5. 单击“**Security**”（安全）选项卡以添加或编辑团体名称。
   a. 要添加团体名称，请单击“**Accepted Community Names**”（接受的团体名称）列表下的“**Add**”（添加）。

      将显示“**SNMP Service Configuration**”（SNMP 服务配置）窗口。
   b. 在“**Community Name**”（团体名称）文本框中键入系统（能够管理您的系统）的团体名称（默认设置为 public），然后单击“**Add**”（添加）。

      将显示“**SNMP Service Properties**”（SNMP 服务属性）窗口。
   c. 要更改团体名称，请在“**Accepted Community Names**”（接受的团体名称）列表中选择团体名称，然后单击“**Edit**”（编辑）。

将显示“**SNMP Service Configuration**”（SNMP 服务配置）窗口。

d. 在“**Community Name**”（团体名称）文本框中对系统（能够管理您的系统）的团体名称执行所有必要的编辑操作，然后单击“**OK**”（确定）。

系统将显示“**SNMP Service Properties**”（SNMP 服务属性）窗口。

6. 单击“**OK**”（确定）以保存更改。

启用 SNMP 设置操作

为使用 IT Assistant 更改 Server Administrator 属性，必须在 Server Administrator 系统上启用 SNMP 设置操作。

1. 打开“**Computer Management**”（计算机管理）窗口。
2. 如果有必要，请展开窗口中的“**Computer Management**”（计算机管理）图标。
3. 展开“**Services and Applications**”（服务和应用程序）图标，然后单击“**Services**”（服务）。
4. 向下滚动服务列表，直至找到“**SNMP Service**”（SNMP 服务），右键单击“**SNMP Service**”（SNMP 服务），然后单击“**Properties**”（属性）。

   将显示“**SNMP Service Properties**”（SNMP 服务属性）窗口。
5. 单击“**Security**”（安全）选项卡以更改团体的访问权限。
6. 在“**Accepted Community Names**”（接受的团体名称）列表中选择一个团体名称，然后单击“**Edit**”（编辑）。

   将显示“**SNMP Service Configuration**”（SNMP 服务配置）窗口。
7. 将“**Community Rights**”（团体权限）设置为“**READ WRITE**”（读写）或“**READ CREATE**”（读创建），然后单击“**OK**”（确定）。

   将显示“**SNMP Service Properties**”（SNMP 服务属性）窗口。
8. 单击“**OK**”（确定）以保存更改。

配置您的系统以向 Management Station 发送 SNMP 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 Server Administrator 系统上为将要发送至 management station 的 SNMP 陷阱配置一个或多个陷阱目标。

1. 打开“**Computer Management**”（计算机管理）窗口。
2. 如果有必要，请展开窗口中的“**Computer Management**”（计算机管理）图标。
3. 展开“**Services and Applications**”（服务和应用程序）图标并单击“**Services**”（服务）。
4. 向下滚动服务列表，直至找到“**SNMP Service**”（SNMP 服务）。右键单击“**SNMP Service**”（SNMP 服务），然后单击“**Properties**”（属性）。

   将显示“**SNMP Service Properties**”（SNMP 服务属性）窗口。
5. 单击“**Traps**”（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“**Community Name**”（团体名称）框中键入团体名称，然后单击“**Community Name**”（团体名称）框旁边的“**Add to list**”（添加到列表）。

   b. 要添加陷阱团体的陷阱目标，请从“**Community Name**”（团体名称）下拉框中选择团体名称，然后单击“**Trap Destinations**”（陷阱目标）框下的“**Add**”（添加）。

   c. 将显示“**SNMP Service Configuration**”（SNMP 服务配置）窗口。

   键入陷阱目标并单击“**Add**”（添加）。

   将显示“**SNMP Service Properties**”（SNMP 服务属性）窗口。
6. 单击“**OK**”（确定）以保存更改。

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

Server Administrator 使用 ***net-snmp*** SNMP 代理提供的 SNMP 服务。您可以配置 SNMP 代理，以更改团体名称、启用 Set 操作及向 Management Station（管理站）发送陷阱。要配置 SNMP 代理以正确地与管理应用程序（例如 IT Assistant）进行交互，请执行以下各节中说明的步骤。

注：有关 SNMP 配置的其它详细信息，请参阅操作系统说明文件。

SNMP Agent Access Control 配置

Server Administrator 实现的 MIB（Management Information Base [管理信息库]）分支标有对象标识符（OID）1.3.6.1.4.1.674。管理应用程序必须能够访问 MIB 树的这个分支才能管理运行 Server Administrator 的系统。

对于 Red Hat Enterprise Linux 和 VMware ESXi 4.0 操作系统，默认 SNMP 代理配置只给予“*public*”团体对 MIB 树 MIB-II “*system*”分支（标有 1.3.6.1.2.1.1 OID）的只读访问权限。这项配置不允许管理应用程序检索或更改 Server Administrator 或 MIB-II “system”分支之外的其他*系统*管理信息。

Server Administrator SNMP 代理程序安装操作

如果 Server Administrator 在安装期间检测到默认 SNMP 配置，将尝试修改 SNMP 代理配置，以给予“*public*”团体对整个 MIB 树的只读访问权限。Server Administrator 以两种方式修改 **/etc/snmp/snmpd.conf** SNMP 代理配置文件：

第一种更改是，通过添加下列行来创建一个查看整个 MIB 树的视图（如果不存在）：

```
view all included.1
```

第二种更改是，修改默认 *access* 行，给予 *public* 团体对整个 MIB 树的只读访问权限。Server Administrator 会查看以下行：

```
access notConfigGroup "" any noauth exact systemview none none
```

如果 Server Administrator 找到上面的行，它会修改该行以便读取：

```
access notConfigGroup "" any noauth exact all none none
```

这些对默认 SNMP 代理程序配置的更改给予 *public* 团体对整个 MIB 树的只读访问权限。

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 之后再对其它所有 SNMP 代理配置进行修改。

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 代理时，它发送一个对象标识符至 SNMP 代理，以将其标为 SMUX 同级。因为必须用 SNMP 代理程序配置对象标识符，因此在安装期间如果它不存在，则 Server Administrator 将下列行添加至 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 团体名称必须与在 Server Administrator 系统上配置的 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：

   ```
   com2sec publicsec default public
   ```

   或

   ```
   com2sec notConfigUser default public
   ```

2. 编辑此行，用新的 SNMP 团体名称替换 `public`。编辑后，新行应为：

   ```
   com2sec publicsec default community_name
   ```

   或

   ```
   com2sec notConfigUser default community_name
   ```

3. 要启用已更改的 SNMP 配置，请通过键入以下命令重新启动 SNMP 代理程序：

   ```
   service snmpd restart
   ```

启用 SNMP 设置操作

为使用 IT Assistant 更改 Server Administrator 属性，必须在运行 Server Administrator 的系统上启用 SNMP Set 操作。

要在运行 Server Administrator 的系统上启用 SNMP 设置操作，请编辑 SNMP 代理配置文件 **/etc/snmp/snmpd.conf** 并执行以下步骤：

1. 查找以下行：

   ```
   access publicgroup "" any noauth exact all none none
   ```

   或

   ```
   access notConfigGroup "" any noauth exact all none none
   ```

2. 编辑此行，用 `all` 替换第一个 none。编辑后，新行应为：

   ```
   access publicgroup "" any noauth exact all all none
   ```

   或

   ```
   access notConfigGroup "" any noauth exact all all none
   ```

3. 要启用已更改的 SNMP 配置，请通过键入以下命令重新启动 SNMP 代理程序：

   ```
   service snmpd restart
   ```

配置您的系统以向 Management Station 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 的系统以向 management station 发送陷阱，请编辑 SNMP 代理配置文件 **/etc/snmp/snmpd.conf** 并执行以下步骤：

1. 向文件添加以下命令行：

   ```
   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. 要启用已更改的 SNMP 配置，请通过键入以下命令重新启动 SNMP 代理程序：

   ```
   service snmpd restart
   ```

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*** 代理提供的 SNMP 服务。可配置 SNMP 代理以启用从远程主机进行 SNMP 访问，更改团体名称，启用 Set 操作，以及发送陷阱到 Management Station。要配置 SNMP 代理以正确地与管理应用程序（例如 IT Assistant）进行交互，请执行以下各节中说明的步骤。

注：有关 SNMP 配置的其他详细信息，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 代理进行通信。当 Server Administrator SNMP 连接至 SNMP 代理时，它发送一个对象标识符至 SNMP 代理，以将其标为 SMUX 同级。必须用 SNMP 代理配置该对象标识符，因此如果它不存在，则在安装期间 Server Administrator 将下列行添加至 SNMP 代理配置文件（**/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 SNMP 管理应用程序（例如在其他主机上运行的 IT Assistant）正确发现和管理 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**，以指出 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：出于安全性原因，建议在可能的情况下，将 SNMP 访问限制在特定的远程主机。

要启用从特定的远程主机对运行 Server Administrator 的系统的 SNMP 访问，请编辑 SNMP 代理配置文件 **/etc/snmp/snmpd.conf**，并执行下列步骤：

1. 查找以下行：

   ```
   rocommunity public 127.0.0.1
   ```

2. 编辑或复制该行，以使用远程主机 IP 地址来替换 127.0.0.1。编辑后，新行应为：

   ```
   rocommunity public IP_address
   ```

   注：通过为每个远程主机添加 rocommunity 指令，可从多个特定的远程主机启用 SNMP 访问。

3. 要启用已更改的 SNMP 配置，请通过键入以下命令重新启动 SNMP 代理程序：

   ```
   /etc/init.d/snmpd restart
   ```

要启用从所有远程主机对运行 Server Administrator 的系统的 SNMP 访问，请编辑 SNMP 代理配置文件 **/etc/snmp/snmpd.conf**，并执行下列步骤：

1. 查找以下行：

   ```
   rocommunity public 127.0.0.1
   ```

2. 通过删除 127.0.0.1 来编辑此行。编辑后，新行应为：

   ```
   rocommunity public
   ```

3. 要启用已更改的 SNMP 配置，请通过键入以下命令重新启动 SNMP 代理程序：

   ```
   /etc/init.d/snmpd restart
   ```

更改 SNMP 团体名称

配置 SNMP 团体名称可确定哪些 Management Station 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 Server Administrator 系统上配置的 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，请编辑 SNMP 代理配置文件 **/etc/snmp/snmpd.conf**，并执行以下步骤：

1. 查找以下行：

   ```
   rocommunity public 127.0.0.1
   ```

2. 编辑此行，用新 SNMP 团体名称替换 public。编辑后，新行应为：

   ```
   rocommunity community_name 127.0.0.1
   ```

3. 要启用已更改的 SNMP 配置，请通过键入以下命令重新启动 SNMP 代理程序：

   ```
   /etc/init.d/snmpd restart
   ```

启用 SNMP 设置操作

为使用 IT Assistant 更改 Server Administrator 属性，必须在运行 Server Administrator 的系统上启用 SNMP Set 操作。要从 IT Assistant 来远程地关闭系统，SNMP Set 操作必须已启用。

注：重新引导系统以更改管理功能不需要 SNMP Set 操作。

要在运行 Server Administrator 的系统上启用 SNMP Set 操作，请编辑 SNMP 代理配置文件 **/etc/snmp/snmpd.conf**，并执行以下步骤：

1. 查找以下行：

   ```
   rocommunity public 127.0.0.1
   ```

2. 编辑此行，用 rwcommunity 替换 rocommunity。编辑后，新行应为：

   ```
   rwcommunity public 127.0.0.1
   ```

3. 要启用已更改的 SNMP 配置，请通过键入以下命令重新启动 SNMP 代理程序：

   ```
   /etc/init.d/snmpd restart
   ```

配置您的系统以向 Management Station 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 的系统以向 Management Station 发送陷阱，请编辑 SNMP 代理配置文件 **/etc/snmp/snmpd.conf** 并执行以下步骤：

1. 向文件添加以下命令行：

   `trapsink IP_address community_name`

   其中，“IP_address”（IP 地址）是管理站的 IP 地址，“community_name”（团体名称） 是 SNMP 团体名称

2. 要启用已更改的 SNMP 配置，请通过键入以下命令重新启动 SNMP 代理程序：

   `/etc/init.d/snmpd restart`

在运行支持的 VMware ESX 4.X 操作系统的系统上将 SNMP 代理配置为代理 VMware MIB

ESX 4.X 服务器可以通过单一默认端口 161 使用 SNMP 协议进行管理。为此，将 snmpd 配置为使用默认端口 161，将 vmwarehostd 配置为使用其它（未用）端口，例如：167。VMWare MIB 分支上的任何 SNMP 请求都将使用 ***snmpd*** 守护程序的代理功能重新路由至 ***vmware-hostd***。

VMWare SNMP 配置文件可以手动在 ESX 服务器上修改，也可以通过从远程系统（Windows 或 Linux）运行 VMWare 远程命令行界面（RCLI）命令 ***vicfg-snmp*** 进行修改。RCLI 工具可以从 VMware 网站（**vmware.com/download/vi/drivers_tools.html**）下载。

以下是配置前的必备步骤。

1. 以手动方式或通过运行以下 vicfg-snmp 命令来编辑 VMWare SNMP 配置文件（**/etc/vmware/snmp.xml**），以修改 SNMP 配置设置。这包括 SNMP 侦听端口、团体字符串、陷阱目标 IP 地址/端口以及陷阱团体名称，然后启用 VMWare SNMP 服务。

   a. `vicfg-snmp.pl --server <ESX_IP_addr> --username root --password <密码> -c <团体名称> -p X Ct <DMC_IP_Address>@162/<团体名称>`

   其中 X 表示未使用的端口。要查找未用端口，可以查看 **/etc/services** 文件中已定义系统服务的端口分配。此外，为确保所选端口当前未被任何应用程序/服务占用，请在 ESX 服务器上运行以下命令：netstat Ca 命令

   注：可以使用逗号分隔列表输入多个 IP 地址。

   b. 要启用 VMWare SNMP 服务，请运行以下命令：

   `vicfg-snmp.pl --server <ESX_IP_addr> --username root --password <密码>`

   `-E`

   c. 要查看配置设置，请运行以下命令：

   `vicfg-snmp.pl --server <ESX_IP_addr> --username root --password <密码>`

   `-s`

   修改后的配置文件内容与以下类似：

   ```
   <?xml version="1.0">
   <config>
   <snmpSettings>
   <enable>true</enable>
   <communities>public</communities>
   <targets>143.166.152.248@162/public</targets>
   <port>167</port>
   </snmpSettings>
   </config>
   ```

2. 如果 SNMP 服务已经运行在系统上，则输入以下命令停止该服务：

   `service snmpd stop`

3. 在 **/etc/snmp/snmpd.conf** 结尾添加以下行：

   ```
   proxy -v 1 -c public udp:127.0.0.1:X .1.3.6.1.4.1.6876
   ```

   其中 *X* 表示上面指定的配置 SNMP 时未使用的端口。

4. 使用以下命令配置陷阱目标：<目标 IP 地址> <团体名称>

   必须指定 trapsink 值，才能发送专有 MIB 中定义的陷阱。

5. 使用以下命令重新启动 mgmt-vmware 服务：

   ```
   service mgmt-vmware restart
   ```

6. 使用以下命令重新启动 snmpd 服务：

   ```
   service snmpd start
   ```

   注：如果 srvadmin 已安装并且服务已启动，则重新启动服务，因为它们依赖于 ***snmpd*** 服务。

7. 运行以下命令，让 snmpd 守护程序在每次重新引导时都启动：

   ```
   chkconfig snmpd on
   ```

8. 运行以下命令，以确保在向 management station 发送陷阱之前，SNMP 端口处于打开状态。

   ```
   esxcfg-firewall -e snmpd
   ```

在运行支持的 VMware ESXi 4.X 操作系统的系统上配置 SNMP 代理

Server Administrator 支持 VMware ESXi 4.X 上的 SNMP 陷阱。Server Administrator 不支持 VMWare ESXi 4.x 上的 SNMP Get 和 Set 操作，因为所需的 SNMP 支持不可用。VMware vSphere 命令行界面（CLI）用于配置运行 VMware ESXi 4.X 的系统，向 Management Station 发送 SNMP 陷阱。

注：有关使用 VMware vSphere CLI 的详情，请参阅 VMware 支持网站 vmware.com/support。

配置您的系统以向 Management Station 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。

要将运行 Server Administrator 的 ESXi 系统配置为向 management station 发送陷阱，请执行下列步骤：

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. 执行以下命令：

   ```
   vicfg-snmp.pl --server <服务器> --username <用户名> --password <密码> -c <团体> -t <主机名>/<团体>
   ```

   其中，<服务器> 是 ESXi 系统的主机名或 IP 地址，<用户名> 是 ESXi 系统上的用户，<密码> 是 ESXi 用户的密码，<团体> 是 SNMP 团体名称，<主机名> 是 Management Station 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。

运行支持的 Red Hat Enterprise Linux 操作系统和 SUSE Linux Enterprise Server 的系统上的防火墙配置

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况。要启用 SNMP 管理应用程序（例

如 IT Assistant），从 Server Administrator 查找和检索信息，至少一个外部网络接口上的 SNMP 端口必须处于打开状态。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，则将显示警告信息，并在系统日志中记录信息。

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，请执行以下步骤：

1. 在 Red Hat Enterprise Linux 命令提示符下，键入 setup 并按 **<Enter>** 键，以启动文本模式设置公用程序。

   注：只有在执行了默认的操作系统安装之后这个命令才可用。

   系统将显示“**Choose a Tool**”（选择工具）菜单。

2. 使用下箭头键选择“**Firewall Configuration**”（防火墙配置）并按 **<Enter>** 键。

   系统将显示“**Firewall Configuration**”（防火墙配置）屏幕。

3. 按 **<Tab>** 以选择“**Security Level**”（安全级别），然后按空格键以选择要设置的安全级别。所选“Security Level”（安全级别）将以星号表示。

   注：有关防火墙安全保护级别的详细信息，请按 <F1> 键。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> 不会提供有关新版 Red Hat Enterprise Linux 防火墙安全级别的信息。

   a. 要禁用防火墙，请选择“**No firewall**”（无防火墙）或“**Disabled**”（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“**High**”（高级）、“**Medium**”（中级）或“**Enabled**”（已启用），然后继续执行步骤 4。

4. 按 **<Tab>** 键以转到“**Customize**”（自定义），然后按 **<Enter>** 键。

   系统将显示“**Firewall Configuration - Customize**”（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，请按 **<Tab>** 键跳至信任的设备之一并按空格键。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>** 跳至“**Other ports**”（其它端口），然后键入 snmp:udp。

6. 按 **<Tab>** 键以选择“**OK**”（确定）并按 **<Enter>**。

   系统将显示“**Firewall Configuration**”（防火墙配置）屏幕。

7. 按 **<Tab>** 键以选择“**OK**”（确定）并按 **<Enter>**。

   系统将显示“**Choose a Tool**”（选择工具）菜单。

8. 按 **<Tab>** 键以选择“**Quit**”（退出）并按 **<Enter>**。

要在 SUSE Linux Enterprise Server 上打开 SNMP 端口，请执行以下步骤：

1. 通过在控制台上执行此命令配置 SuSEfirewall2
   a.# yast2 firewall

2. 使用箭头键导航至“**Allowed Services**”（允许的服务）。

3. 输入 **Alt+d** 打开“**Additional Allowed Ports**”（其它允许的端口）对话框。

4. 输入 **Alt+T** 移动光标到“**TCP Ports**”（TCP 端口）文本框。

5. 在文本框中输入 **snmp**。

6. 输入 **Alt-O** 和 **'Alt-N'** 以转至下一屏幕。

7. 输入 **Alt-A** 以接受并应用更改。

返回目录页面

返回目录页面

使用 Server Administrator

Dell OpenManage Server Administrator 版本 6.4 用户指南

启动 Server Administrator 会话

要启动 Server Administrator 会话，请单击桌面上的 **Dell OpenManage Server Administrator** 图标。

将显示 **Server Administrator** “**Log in**”（登录）屏幕。Dell OpenManage Server Administrator 的默认端口是 1311。可以在需要时更改端口。请参阅 “Dell Systems Management Server 管理连接服务和安全设置”了解有关设置系统首选项的说明。

登录和注销

OpenManage Server Administrator 提供三种类型的登录。这些功能是：

- Server Administrator 本地系统登录
- Server Administrator Managed System 登录
- Central Web Server 登录

Server Administrator 本地系统登录

只有在本地系统上安装了 Server Instrumentation 和 Server Administrator Web Server 组件时，才能使用此登录。

使用此登录窗口登录本地系统上的 Server Administrator：

1. 在系统管理的 “**Log in**”（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，您还必须指定正确的**域**名。

2. 如果系统运行 Microsoft Windows 操作系统并且是 Windows 域的成员，则从域列表中选择一个域。
3. 选中 “**Active Directory Login**”（Active Directory 登录）复选框使用 Microsoft Active Directory 登录。请参阅使用 Active Directory 登录。
4. 单击 “**Submit**”（提交）。

要结束 Server Administrator 会话，请单击每个 **Server Administrator** 主页右上角的 “**Log Out**”（注销）。

注：有关使用 CLI 配置系统上 Active Directory 的信息，请参阅《Dell OpenManage Management Station 软件安装指南》。

Server Administrator Managed System 登录

只有安装了 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，请执行以下步骤：

方法 1

1. 单击桌面上的 **Dell OpenManage Server Administrator** 图标。
2. 键入 Managed System 的 IP 地址或系统名称或完全限定域名（FQDN）。

注：如果已输入系统名称或 FQDN，Dell OpenManage Server Administrator Web Server 主机会将系统名称或 FQDN 转换为 Managed System 的 IP 地址。还可以输入 Managed System 的端口号。例如，“主机名:端口号”或“IP 地址:端口号”。如果连接到 Citrix XenServer 5.6 受管节点，则以格式“主机名:端口号”或“IP 地址:端口号”使用端口 5986。

3. 如果使用的是企业内部网连接，则选中“**Ignore Certificate Warnings**”（忽略证书警告）复选框。
4. 选中“**Active Directory Login**”（Active Directory 登录）复选框 。选中此选项即可使用 Microsoft Active Directory 验证登录。如果没有使用 Active Directory 软件控制网络访问，则请勿选中此复选框。请参阅使用 Active Directory 登录。
5. 单击“**Submit**”（提交）。

方法 2

打开 Web 浏览器，在地址字段中键入以下一项，然后按 <Enter>：

`https ://hostname:1311`

其中，主机名是为受管节点系统设定的名称，1311 是默认端口号。

或

`https ://IP address:1311`

其中，IP address 是 managed system 的 IP 地址，1311 是默认端口号。您必须在地址字段中键入 `https ://`（而不是 `http://`）才能在浏览器中收到有效响应。

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。

Central Web Server 登录

只有安装了 Server Administrator Web Server 组件时，才能使用此登录。使用此登录管理 OpenManage Server Administrator Central Web Server：

1. 单击桌面上的 **Dell OpenManage Server Administrator** 图标。将显示远程登录页。

小心：登录屏幕上有“Ignore certificate warnings”（忽略证书警告）复选框。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“**Manage Web Server**”（管理 Web Server）链接。
3. 输入“**User Name**”（用户名）、“**Password**”（密码）和“**Domain name**”（域名）（如果从定义的域访问 Server Administrator），然后单击“**Submit**”（提交）。
4. 选择“**Active Directory Login**”（Active Directory 登录）复选框使用 Microsoft Active Directory 登录。请参阅使用 Active Directory 登录。
5. 单击“**Submit**”（提交）。

要结束 Server Administrator 会话，单击“全局导航栏”上的“**Log Out**”（注销）。“**Log Out**”（注销）按钮位于每个 **Server Administrator** 主页的右上角。

注：使用 Mozilla Firefox 版本 3.0 和 3.5 或 Microsoft Internet Explorer 版本 7.0 或 8.0 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，强烈建议您生成新的 X.509 认证、重新使用现有的 X.509 认证或导入来自认证机构（CA）的根认证或认证链。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 证书管理的详情，请参阅“X.509 认证管理”。

为了确保系统安全性，强烈建议您导入从认证机构（CA）收到的根证书或证书链。有关详情，请参阅 VMware 说明文件。

注：如果 Managed System 上的认证机构有效，但 Server Administrator Web Server 仍然报告不可信证书错误，则仍然可以使用 **certutil.exe** 将 Managed System 的 CA 设置为可信。有关访问此 **.exe** 的详情，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 Login**”（Active Directory 登录）复选框以使用 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。有关详情，请参阅《Dell OpenManage 安装和安全用户指南》中的“*使用 Microsoft Active Directory*”。

单一登录

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

注：有关单一登录的详细信息，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=[插件名称]
```

其中*插件名称* = *omsa*、*ita* 等。

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=[插件名称]&locallogin=true
```

其中*插件名称* = *omsa*、*ita* 等。

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 OpenManage IT Assistant）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 时可能会得到一个空白屏幕。在这种情况下，将会显示错误信息来指导您配置浏览器设置。

Internet Explorer

1. 在 Web 浏览器中，单击“**Tools**”（工具）→“**Internet Option**”（Internet 选项）→“**Security**”（安全）。
2. 单击“**Trusted Sites**”（受信任的站点）图标。
3. 单击“**Sites**”（站点）。
4. 将用来访问远程 managed system 的 Web 地址从浏览器的地址栏复制并粘贴到“**Add this Web Site to the Zone**”（将该网站添加到区域中）字段。
5. 单击“**Custom Level**”（自定义级别）。

   对于 Windows Server 2003：

   - 在“**Miscellaneous**”（其他）下面，选择“**Allow Meta Refresh**”（允许 META REFRESH）单选按钮。
   - 在“**Active Scripting**”（活动脚本）下面，选择“**Enable**”（启用）单选按钮。
   - 在“**Active Scripting**”（活动脚本）下面，选择“**Allow scripting of Internet Explorer web browser controls**”（允许 Internet Explorer Web 浏览器控件脚本）单选按钮。
6. 单击“**OK**”（确定）保存新设置。关闭浏览器并登录 Server Administrator。

要允许 Server Administrator 不提示输入用户凭据的单一登录，执行下列步骤：

1. 在 Web 浏览器中，单击“**Tools**”（工具）→“**Internet Options**”（Internet 选项）→“**Security**”（安全）。
2. 单击“**Trusted Sites**”（受信任的站点）图标。
3. 单击“**Sites**”（站点）。
4. 将用来访问远程 managed system 的 Web 地址从浏览器的地址栏复制并粘贴到“**Add this Web Site to the Zone**”（将该网站添加到区域中）字段。
5. 单击“**Custom Level**”（自定义级别）。

6. 在“**User Authentication**”（用户验证）下面，选择“**Automatic Logon with current username and password**”（自动使用当前用户名和密码登录）单选按钮。
7. 单击“**OK**”（确定）保存新设置。关闭浏览器并登录 Server Administrator。

Mozilla Firefox

1. 启动浏览器。
2. 单击“**Edit**”（编辑）→“**Preferences**”（首选项）。
3. 单击“**Advanced**”（高级）→“**Scripts and Plugins**”（脚本和插件）。
4. 确保在“**Enable JavaScript for**”（为以下组件启用 JavaScript）下选中 **Navigator** 复选框。
5. 单击“**OK**”（确定）保存新设置。
6. 关闭浏览器。
7. 登录到 Server Administrator。

Server Administrator 主页

注：使用 Server Administrator 时，请勿使用 Web 浏览器的工具条按钮（比如“**Back**”（后退）和“**Refresh**”（刷新））。请只使用 Server Administrator 定位工具。

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

- 全局导航栏提供了常规服务的链接。
- 系统树显示基于用户访问权限的所有可见系统对象。
- 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。操作窗口包含三个功能区域：
  - 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，表 3-1列出 GUI 字段名称和可应用的系统。

表 3-1. 以下 GUI 字段名称的系统可用性

GUI 字段名称	可应用的系统
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

图 3-1 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 主页的样式。

图 3-1. Server Administrator 主页示例 — 非模块化系统

图 3-2 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 主页的样式。

图 3-2. 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新数据区域。例如，单击“**Properties**”（属性）操作选项卡的“**Health**”（运行状况）子类别下的“**Main System Chassis/Main System**”（主系统机箱/主系统），将列出“Main System Chassis/Main System object”（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“**Shutdown**”（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

表 3-2 列出模块化系统和非模块化系统中 Server Administrator 功能的可用性。勾选标记表示该功能可用，而删除符号表示该功能不可用。

表 3-2. 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	✗	✓ （从 *xx0x* 系统开始）
侵入	✗	✓
内存	✓	✓
网络	✓	✓
端口	✓	✓
电源管理	✓	✓

		（从 *xx0x* 系统开始）
处理器	✓	✓
远程访问	✓	✓
可移动闪存介质	✓	✓
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对程序中各个用户级别都可用。

- 单击“**Preferences**”（首选项）可打开“**Preferences**”（首选项）主页。请参阅“使用首选项主页”。
- 单击“**Support**”可连接到 Dell 支持网站。
- 单击“**About**”（关于）可显示 Server Administrator 版本和版权信息。
- 单击“**Log Out**”（注销）可结束当前 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“**Modular Enclosure**”（模块化机柜）→“**System/Server Module**”（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“**Main System Chassis/Main System**”（主系统机箱/主系统）、“**Software**”（软件）和“**Storage**”（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（⊟）表示该条目已被展开，不能进一步展开。

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“**Main System Chassis/Main System**”（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“**Properties**”（属性）操作选项卡和“**Health**”（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，“**Properties**”（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/服务器模块组件状况指示器

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 3-3. 系统/服务器模块组件状况指示器

✓	表示组件运行状况良好（正常）。
⚠	表示组件处于警告（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。警告状况需要立即进行处理。
✗	表示组件处于故障（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。
?	表示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：“**Print**”（打印）、“**Export**”（导出）、“**Email**”（电子邮件）、“**Help**”（帮助）和“**Refresh**”（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“**Save As**”（另存为）和“**Clear Log**”（清除日志）任务按钮。

- 单击“**Print**”（打印）（）将在默认打印机上打印打开的窗口。
- 单击“**Export**”（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。请参阅“设置用户和服务器首选项”了解有关自定义数据字段值分隔符的说明°
- 单击“**Email**”（电子邮件）（）将创建电子邮件信息，地址为指定的电子邮件收件人。请参阅“设置用户和服务器首选项”了解有关设置电子邮件服务器和默认电子邮件收件人的说明。
- 单击“**Refresh**”（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“**Save As**”（另存为）将保存操作窗口 HTML 文件（以 **.zip** 文件形式）。
- 单击“**Clear Log**”（清除日志）将从操作窗口数据区域显示的日志中删除所有事件。
- 单击“**Help**”（帮助）（）提供您正在查看的特定窗口或任务的详细信息。

注：“**Export**”（导出）、“**Email**”（电子邮件）、“**Save As**”（另存为）和“**Clear Log**”（清除日志）按钮只有当用户以“高级用户”或“管理员”权限登录时才可见。

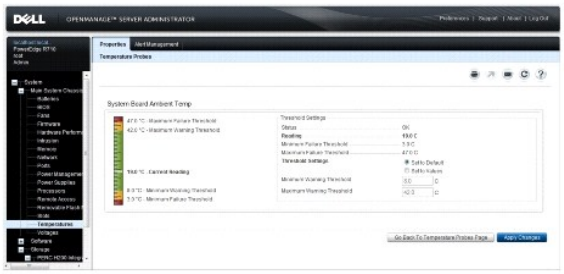
带下划线的项目

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，图 3-3显示了系统 CPU 风扇探测器的读数。

图 3-3. 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“**Help**”（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，可指导您完成所需的特定操作。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

“**Preferences**”（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。

“Preferences”（首选项）主页的可用配置选项如下：

- 常规设置
- Server Administrator

为了管理远程系统而登录后，可以查看“**Preferences**”（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，“**Preferences**”（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“**Home**”（主页）可返回到 Server Administrator 主页。

- “**Preferences**”（首选项）主页的左窗格（在 Server Administrator 主页上显示系统树）将显示 Managed System 或 Server Administrator Web Server 的首选项类别。
- 操作窗口显示 Managed System 或 Server Administrator Web Server 的可用设置和首选项。

图 3-4 显示首选项主页布局的样例。

图 3-4. 首选项主页的样例 - Managed System

Managed System 首选项

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

单击 Server Administrator 对象可以启用或禁用对具有“User”（用户）或“Power User”（高级用户）权限的用户的访问。Server Administrator 对象操作窗口可能有“**Preferences**”（首选项）选项卡，具体视用户的组权限而定。

在“Preferences”（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。
- 配置命令日志大小
- 配置 SNMP

Server Administrator Web Server 首选项

为管理 Server Administrator Web Server 而登录时，“**Preferences**”（首选项）主页默认为“Preferences”（首选项）选项卡下的“**User Preferences**”（用户首选项）窗口。

由于 Server Administrator Web Server 与 Managed System 分离，因此，当使用“Manage Web Server”（管理 Web Server）链接登录 Server Administrator Web Server 时，将显示以下选项：

- Web Server Preferences（Web Server 首选项）
- X.509 认证管理

有关访问这些功能的详情，请参阅“Server Administrator 服务”。

Dell Systems Management Server 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 “**Preferences**”（首选项）主页中设置用户和安全端口系统首选项。

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。

要设置用户首选项，请执行以下步骤：

1. 单击全局导航栏上的“**Preferences**”（首选项）。

   系统将显示“**Preferences**”（首选项）主页。

2. 单击“**General Settings**”（常规设置）。

3. 要添加预先选定的电子邮件收件人，请在“**Mail To:**”（邮件发送至：）字段中键入指定服务联络的电子邮件地址，然后单击“**Apply Changes**”（应用更改）。

注：在任意窗口中单击“Email”（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。

4. 要更改主页外观，请在“**skin**”（外观）或“**scheme**”（方案）字段中选择替换值，然后单击“**Apply Changes**”（应用更改）。

要设置安全端口系统首选项，请执行以下步骤：

1. 单击全局导航栏上的“**Preferences**”（首选项）。

   系统将显示“**Preferences**”（首选项）主页。

2. 单击“**General Settings**”（常规设置）和 **Web Server** 选项卡。

3. 在“**Server Preferences**”（服务器首选项）窗口中根据需要设置选项。

   - “**Session Timeout**”（会话超时）功能可以设置 Server Administrator 会话保持激活状况的时间限制。选择“**Enable**”（启用）单选按钮将允许 Server Administrator 在指定时间内无用户交互活动的情况下超时。会话超时的用户必须重新登录以继续。选择“**Disable**”（禁用）单选按钮将禁用 Server Administrator 会话超时功能。
   - “**HTTPS Port**”（HTTPS 端口）字段可以为 Server Administrator 指定安全端口。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 managed system 上的 Server Administrator。请参阅《Dell OpenManage 安装和安全性用户指南》查看默认端口列表。

   - “**IP Address to Bind to**”（要绑定到的 IP 地址）字段可指定启动会话时 Server Administrator 所绑定到的 managed system 的 IP 地址。选择“**All**”（所有）单选按钮将绑定到所有适用于系统的 IP 地址。选择“**Specific**”（特定）单选按钮将绑定到特定 IP 地址。

   注：将“**IP Address to Bind to**”（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 managed system 上的 Server Administrator。

   - “**SMTP Server name**”（SMTP 服务器名称）和“**DNS Suffix for SMTP Server**”（SMTP 服务器的 DNS 后缀）字段可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，您必须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。

   - “**Command Log Size**”（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。

   - “**Support Link**”（支持链接）字段可指定为 managed system 提供支持的企业实体的 URL。
   - “**Custom Delimiter**”（自定义分隔符）字段指定用于分隔数据字段的字符，以便分隔那些使用“**Export**”（导出）按钮创建的文件中的字段。**;** 字符是默认分隔符。其他选项有 **!**、**@**、**#**、**$**、**%**、**^**、*、**~**、**?**、**|** 和 **,**。
   - “**SSL Encryption**”（SSL 加密）字段指定安全 HTTPS 会话的加密级别。可用加密级别包括**自动协商**和**128 位或更高**。
     - “**Auto Negotiate**”（自动协商）— 允许具有任何加密长度的浏览器的连接。浏览器自动与 Server Administrator Web Server 协商并为会话使用可用的最高加密级别。具有较弱加密的旧式浏览器可以连接到 Server Administrator。
     - “**128-bit or higher**”（128 位或更高）— 允许具有 128 位或更长加密长度的浏览器的连接。根据任何已建立会话的浏览器，会使用以下一种加密方案：

     SSL_RSA_WITH_RC4_128_SHA

     SSL_RSA_WITH_RC4_128_MD5

     SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA

     TLS_DHE_RSA_WITH_AES_128_CBC_SHA

     SSL_RSA_WITH_3DES_EDE_CBC_SHA

     TLS_RSA_WITH_AES_128_CBC_SHA

     TLS_DHE_DSS_WITH_AES_128_CBC_SHA

     SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA

   - **密钥签署算法**显示支持的签署算法。从下拉列表中选择算法。如果选择 SHA 512 或 SHA 256，请确保操作系统/浏览器支持该算法。如果选择的其中一个选项没有必备的操作系统/浏览器支持，Server Administrator 会显示“无法显示网页”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。

   注：128 位或更高选项不允许具有较低 SSL 加密强度（比如 40 位和 56 位）的浏览器的连接。

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

   注：如果加密级别设置为 **128 位或更高**，可以使用具有相同或更高加密级别的浏览器访问或修改 Server Administrator 设置。

4. 在“**Server Preferences**”（服务器首选项）窗口中完成选项设置后，请单击“**Apply Changes**”（应用更改）。

X.509 认证管理

Web 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。为保证系统安全，强烈建议：

- 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）的根证书或证书链。
- 所有安装了 Server Administrator 的系统均有唯一的主机名。

注：要执行认证管理，必须以“Administrator”（管理员）权限登录。

要通过“Preferences”（首选项）主页管理 X.509 证书，请单击“**General Settings**”（常规设置），单击 **Web Server** 选项卡，然后单击“**X.509 Certificate**”（X.509 证书）。

此选项可用于：

- “**Generate a new X.509 certificate**”（生成新的 X.509 证书）— 此选项用于为访问 Server Administrator 创建证书。
- “**Certificate Maintenance**”（证书保留）— 此选项选择公司拥有的现有证书，并使用该证书控制对 Server Administrator 的访问。
- “**Import a root certificate**”（导入根证书）— 使用此选项可以导入根证书以及从可信认证机构收到的证书响应（采用 PKCS#7 格式）。
- “**Import certificate chain from a CA**”（导入来自 CA 的证书链）— 使用此选项可以导入来自可信认证机构的证书响应（采用 PKCS#7 格式）。Verisign、Thawte 和 Entrust 均为可信赖的认证机构。

Server Administrator Web Server 操作选项卡

为了管理 Server Administrator Web Server 而登录时，将显示以下操作选项卡：

- 关机
- 日志
- 会话管理

管理 Server Administrator

每次重新引导 managed system 时，Server Administrator 都将自动启动。要手动启动、停止或重新启动 Server Administrator，请按照以下说明进行。

注：要管理 Server Administrator，必须以管理员权限登录（对于支持的 Citrix XenServer、Red Hat Enterprise Linux 或 SUSE Linux Enterprise Server 操作系统，以 root 登录）。

启动 Server Administrator

所支持的 Microsoft Windows 操作系统

要在运行所支持的 Windows 操作系统的系统上启动 Server Administrator，请执行以下步骤：

1. 打开“**Services**”（服务）窗口。
2. 右键单击 **Dell Systems Management Server Administration（DSM SA）Connection Service** 图标。
3. 单击 “**Start**”（开始）。

支持的 Citrix XenServer、Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统

要在运行支持的 Citrix XenServer、Red Hat Enterprise Linux 或 SUSE Linux Enterprise Server 操作系统的系统中启动 Server Administrator，请通过命令行运行以下命令：

```
dsm_om_connsvc start
```

停止 Server Administrator

所支持的 Microsoft Windows 操作系统

要停止 Server Administrator，请执行以下步骤：

1. 打开“**Services**”（服务）窗口。
2. 右击 **DSM SA Connection Service** 图标。
3. 单击“**Stop**”（停止）。

支持的 Citrix XenServer、Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统

要在运行支持的 Citrix XenServer、Red Hat Enterprise Linux 或 SUSE Linux Enterprise Server 操作系统的系统中停止 Server Administrator，请通过命令行运行以下命令：

```
dsm_om_connsvc stop
```

重新启动 Server Administrator

所支持的 Microsoft Windows 操作系统

要重新启动 Server Administrator，请执行以下步骤：

1. 打开“**Services**”（服务）窗口。
2. 右击 **DSM SA Connection Service** 图标。
3. 单击“**Restart**”（重新启动）。

支持的 Citrix XenServer、Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统

要在运行支持的 Citrix XenServer、Red Hat Enterprise Linux 或 SUSE Linux Enterprise Server 操作系统的系统中重新启动 Server Administrator，请通过命令行运行以下命令：

```
dsm_om_connsvc restart
```

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关注故障组件的运行状况。

有关 CLI 功能和使用的完整说明，请参阅《Dell OpenManage Server Administrator 命令行界面用户指南》。

返回目录页面