

Dell OpenManage Server Administrator 版本 5.5 用户指南

[简介](#)

[版本 5.5 的新功能](#)

[设置和管理](#)

[安装 Server Administrator](#)

[使用 Server Administrator](#)

[Remote Access Controller](#)

[Instrumentation Service](#)

[使用底板管理控制器/Integrated Dell Remote Access Controller](#)

[Storage Management Service](#)


[Server Administrator 日志](#)


[设置警报措施](#)

[故障排除](#)

[词汇表](#)

"注"和"注意"

 **注：** "注"表示可以帮助您更好地使用计算机的重要信息。

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

本说明文件中的信息如有更改，恕不另行通知。
© 2008 Dell Inc. 版权所有，翻印必究。

未经 Dell Inc. 书面许可，严禁以任何形式进行复制。

本文中使用的商标，Dell、DELL 徽标、PowerEdge、PowerVault 和 OpenManage 是 Dell Inc. 的商标；Microsoft、Windows、MS-DOS、Active Directory、Windows Server 和 Windows NT 是 Microsoft Corporation 在美国和/或其它国家或地区的商标或注册商标；Novell 和 ConsoleOne 是 Novell, Inc. 的注册商标；SUSE 是 Novell, Inc. 在美国和其它国家或地区的注册商标；Intel 和 Pentium 是 Intel Corporation 的注册商标；Intel386 是 Intel Corporation 的商标；Red Hat 和 Red Hat Enterprise Linux 是 Red Hat, Inc. 的注册商标；VESA 是 Video Electronics Standards Association 的注册商标；UNIX 是 The Open Group 在美国和其它国家或地区的注册商标；OS/2 是 International Business Machines Corporation 的注册商标；VMware 是 VMware Inc 的注册商标；ESX Server 是 VMware Inc 的商标；AMD 是 Advanced Micro Devices, Inc. 的商标；Citrix 是 Citrix Systems, Inc. 在美国和/或其它国家或地区的注册商标或商标。

Server Administrator 包含由 Apache Software Foundation (www.apache.org) 开发的软件。Server Administrator 使用 OverLIB JavaScript 程序库。该程序库可以从 www.bosrup.com 获得。

本说明文件中提及的其它商标和产品名称是指拥有相应商标和产品名称的公司或其制造的产品。Dell Inc. 对本公司的商标和产品名称之外的其它商标和产品名称不拥有任何专有权。

2008 年 7 月

设置警报措施


Dell OpenManage Server Administrator 版本 5.5 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](#)
- [在 Microsoft Windows 2000、Windows Server 2003 和 Windows Server 2008 中设置警报操作](#)
- [BMC 平台事件筛选器警报信息](#)
- [了解服务名称](#)

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“Display an alert on the server”（**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，则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，则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“Broadcast a message”（**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。

 **注：** 在 SUSE Linux Enterprise Server (版本 9) 中，`wall` 发送的信息由 `xterm` 终端程序而非 `Konsole` 终端程序显示。

设置事件的警报措施时，您可以将操作指定为“Execute application”（**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：

- 1 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。
- 1 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。
- 1 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。
- 1 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 2000、Windows Server 2003 和 Windows Server 2008 中设置警报操作

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。

BMC 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 11-1 中列出。

表 11-1. BMC 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制。
温度探测器故障	温度太高或太低，无法正常工作。
检测到机箱侵入	系统机箱已被打开。
冗余（电源设备或风扇）降级	风扇和（或）电源设备的冗余已经减少。
冗余（电源设备或风扇）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。

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 11-2. 服务名称

用途	服务名称	上一版本	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	Omaaws[32 64]	dsm_om_connsvc[32 64]
			dsm_om_connsvc
计划或通知			
	显示名称	OM 公共服务	DSM SA 共享服务
	可执行文件名称	Omsad[32 64]	dsm_om_shrsvc[32 64]
			dsm_om_shrsvc

[目录](#)

故障排除

Dell OpenManage Server Administrator 版本 5.5 用户指南


- [在支持的 Windows 操作系统上修复出现故障的 Server Administrator 安装](#)
- [OpenManage Server Administrator 服务](#)

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. 找出以前安装的 Server Administrator 的版本。
2. 从 Dell™ 支持网站 support.dell.com 下载该版本的安装软件包。
3. 在 `srvadmin\windows\SystemManagement` 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，则可使用“Add/Remove”（添加/删除程序）卸载 Server Administrator。

OpenManage Server Administrator 服务

此表列出 OMSA 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.

服务名称	说明	故障影响	恢复机制	严重性
Windows: DSM SA 连接服务 Linux: dsm_om_connsvc	提供从具有支持的 Web 浏览器和网络连接的任何系统对 OMSA 进行的远程/本地访问。	提供从具有支持的 Web 浏览器和网络连接的任何系统对 OMSA 进行的远程/本地访问。	重新启动服务	Critical (严重)
常见服务				
Windows: DSM SA Shared 服务 Linux: dsm_om_shrsvc	启动时运行资源清册收集程序，对将由 OMSA 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 系统管理控制台 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 OMSA 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）
Instrumentation Service				
Windows: DSM SA 数据管理器 Linux: dsm_sa_datamgr32d (在 dataeng 服务下面)	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_eventmgr32d (在 dataeng 服务下面)	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工作。	重新启动服务	“Warning”（警告）
Linux: dsm_sa_snmp32d	数据引擎 Linux SNMP	来自 Management Station 的 SNMP get/set /陷阱请求将不能起作用。	重新启动	Critical (严重)

(在 dataeng 服务下面)	接口		服务	
Storage Management Service				
Windows: mr2kserv	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)
Remote Access Controller 服务				
Windows: Remote Access Controller (RAC) 服务 Linux: racsrvc	RAC 服务用于创建/监控 PPP 连接并处理从 RAC 固件异步收到的 RAC 事件。	如果此服务没有运行，则不处理来自固件的事件。控制台不能重定向。使用本地 racadm 公用程序无法升级 RAC 卡上的固件。但是，可以使用远程 racadm 公用程序或软盘进行升级。	重新启动服务	Critical (严重)
Windows: RAC Win VNC Service Linux: racXvnc	此服务用于将控制台重定向到远程用户。	控制台不能重定向。	重新启动服务	"Warning" (警告)
Linux: racser	建立与 RAC 卡的点对点 (PPP) 连接。	控制台不能重定向。使用 racadm 公用程序无法升级 RAC 卡上的固件。 但是，可以使用远程 racadm 公用程序或软盘进行升级。	重新启动服务	Critical (严重)
Remote Access Controller 服务 (RIALTO)				
Windows: Remote Access Controller 4 (RAC4) Linux: Racsvc	RAC 服务主要用于处理 RAC Virtual UART 上的 SPCMP 序列信息，并处理从固件异步收到的 RAC 事件。	如果此服务没有运行，则不处理来自固件的事件。用户使用本地 racadm 无法配置 DRAC。使用本地 racadm 公用程序无法升级 RAC 卡上的固件。 但是，可以使用远程 racadm 公用程序进行升级或配置。软盘公用程序也可以用于固件刷写。	重新启动服务	Critical (严重)

[目录](#)

[目录](#)

词汇表

Dell OpenManage Server Administrator 版本 5.5 用户指南

下面的列表定义或标识了系统说明文件中使用的技术术语、缩写词和缩略词。

ACL

访问控制列表 (access control list) 的缩写。ACL 文件是文本文件，它包含的列表定义了哪些人可以访问存储在 Novell® Web Server 上的资源。

ADB

指定数据库 (assign database) 的缩写。

AGP

高级图形端口 (Advanced Graphics Port) 的缩写。

ASIC

专用集成电路 (application-specific integrated circuit) 的缩写。

ASPI

高级 SCSI 编程接口 (advanced SCSI programming interface) 的缩写。

autoexec.bat 文件

autoexec.bat 文件在引导系统时执行（在执行完 **config.sys** 文件中的所有命令之后）。该启动文件包含的命令定义了所有连接至系统的设备的特性，并且可以查找和执行未存储在当前目录中的程序。

BGA

球栅阵列 (Ball Grid Array) 的缩写，一种集成电路 (IC) 封装技术，使用一组焊球（而不是插针）连接至系统板。

BMC

底板管理控制器 (baseboard management controller) 的缩写，是一个在 IPMI 结构中提供智能控制的控制器。

bpi

位/英寸 (bits per inch) 的缩写。

bps

位/秒 (bits per second) 的缩写。

BTU

英制热量单位 (British thermal unit) 的缩写。

CA

认证机构 (certification authority) 的缩写。

CDRAM

高速缓存 DRAM (cached DRAM) 的缩写, 是 Mitsubishi 开发的一种高速 DRAM 内存芯片, 其中包含了一个小型的 SRAM 高速缓存。

CHAP

竞争握手验证协议 (Challenge-Handshake Authentication Protocol) 的缩写, 是 PPP 服务器使用的验证方案, 可在连接时或连接之后的任意时间验证连接创立者的身份。

CI/O

综合输入/输出 (comprehensive input/output) 的缩写。

CIM

公用信息模型 (Common Information Model) 的缩写, 一种说明 DMTF 管理信息的模型。CIM 可独立执行, 允许不同的管理应用程序从各种资源中收集所需的数据。CIM 包括用于系统、网络、应用程序和设备的模式, 并且可以添加新模式。它提供了映射技术, 用于 CIM 数据与 SNMP 代理中的 MIB 数据进行交换。

CIMOM

公用信息模型对象管理器 (common information model object manager) 的缩写。

CLI

命令行界面 (command line interface) 的缩写。

CMC

机箱管理控制器 (Chassis Management Controller) 的缩写。

CMOS

互补金属氧化物半导体 (complementary metal-oxide semiconductor) 的缩写。在系统中, CMOS 存储器芯片通常用于 NVRAM 存储。

COM n

系统中第一个串行端口至第四个串行端口的设备名称分别为 COM1、COM2、COM3 和 COM4。COM1 和 COM3 的默认中断为 IRQ4, COM2 和 COM4 的默认中断为 IRQ3。因此, 配置运行串行设备的软件时请务必小心, 以免导致中断冲突。

config.sys 文件

文件 **config.sys** 在引导系统时执行 (在执行 **autoexec.bat** 文件中的命令之前)。该启动文件包含的命令指定了要安装的设备 and 要使用的驱动程序。该文件还包含确定操作系统如何使用内存和控制文件的命令。

ConsoleOne

Novell ConsoleOne 为那些从各个不同位置和平台管理网络资源的图形化公用程序提供一个基于 Java 的基础平台。ConsoleOne 为所有 Novell 和外部产品提供了单点控制。

COO

物主成本 (cost of ownership) 的缩写。

cpi

字符/英寸 (characters per inch) 的缩写。

CRC

循环冗余代码 (cyclic redundancy code) 的缩写，它是从数据块中导出的数字，并且存储在数据块中或随数据块一起传输，以检测损坏的数据。通过重新计算 CRC 并将其与原来传输的值相比较，接收器可以检测到某些类型的传输错误。

CSR

认证签名请求 (certificate signing request) 的缩写。

DAT

数字音频磁带 (digital audio tape) 的缩写。

dB

分贝 (decibel) 的缩写。

dBA

调整分贝 (adjusted decibel) 的缩写。

DBS

按需切换 (Demand Based Switching) 的缩写。DBS 通过在处理器使用率低时切换到低电源状态 (频率和电压) 来执行电源管理。它在保证应用程序性能的同时降低平均系统电源。

DHCP

动态主机配置协议 (Dynamic Host Configuration Protocol) 的缩写，通过该协议给 LAN 上的计算机动态分配 IP 地址。

DIMM

双列直插式内存模块 (dual in-line memory module) 的缩写。包含 DRAM 芯片的小型电路板，与系统板相连接。

DIN

德国工业标准 (Deutsche Industrie Norm) 的缩写，德国的标准制订组织。DIN 连接器是一种符合 DIN 制订的众多标准之一的连接器。DIN 连接器广泛用于个人计算机。例如，个人计算机的键盘连接器是 DIN 连接器。

DIP

双列直插式封装 (dual in-line package) 的缩写。一种电路板，例如系统板或扩充卡，可能包含用于配置电路板的 DIP 开关。DIP 开关均为切换开关，具有开和关两种状态。

DKS

动态内核支持 (dynamic kernel support) 的缩写。

DMA

直接内存访问 (direct memory access) 的缩写。DMA 通道使某些类型的数据可以绕过微处理器而直接在 RAM 和设备之间进行传输。

DMTF

分布式管理任务组 (Distributed Management Task Force) 的缩写，代表硬件和软件提供商的公司社团。

dpi

点/英寸 (dots per inch) 的缩写。

DPMS

显示器电源管理信号 (Display Power Management Signaling) 的缩写。一种由视频电子标准协会 (VESA®) 制定的标准，定义了视频控制器发出的、用于激活显示器电源管理状态的硬件信号。如果显示器在接收到来自系统视频控制器的相应信号后进入某一电源管理状态，则称该显示器为 DPMS 兼容显示器。

DRAC 4

Dell™ 远程访问控制器 4 (Dell™ Remote Access Controller 4) 的缩写。

DRAC 5

Dell 远程访问控制器 5 (Dell Remote Access Controller 5) 的缩写。

DRAC II

Dell OpenManage™ 远程访问卡 II (Dell OpenManage™ Remote Access Card II) 的缩写。

DRAC III

Dell 远程访问卡 III (Dell Remote Access Card III) 的缩写。

DRAC III/XT

Dell 远程访问卡 III/XT (Dell Remote Access Card III/XT) 的缩写。

DRAM

动态随机访问内存 (dynamic random-access memory) 的缩写。系统的 RAM 通常全部由 DRAM 芯片组成。由于 DRAM 芯片无法永久性地存储电荷，系统将不断刷新系统中的每个 DRAM 芯片。

DSM SA 连接服务

Dell Systems Management Server Administration 的缩写。一种应用程序，使 Web 页面能够通过使用 HTTPS 协议的浏览器查看。请参阅“[Web Server](#)”。

DTE

数据终端设备 (data terminal equipment) 的缩写。任何能够通过电缆或通信线路以数字形式发送数据的设备，例如计算机系统。DTE 通过数据通信设备 (DCE) (例如调制解调器) 连接至电缆或通信线路。

ECC

差错校验 (error checking and correction) 的缩写。

ECP

扩展功能端口 (Extended Capabilities Port) 的缩写。

EDO

扩展数据输出 (extended data output) 动态随机存取内存的缩写，是一种 DRAM，但是比常规 DRAM 快。EDO RAM 在将前一数据块发送到微处理器的同时就能开始获取内存中的下一数据块。

EEPROM

电可擦可编程只读存储器 (electrically erasable programmable read-only memory) 的缩写。

EIDE

增强型集成驱动电子设备 (enhanced integrated drive electronics) 的缩写。与传统 IDE 标准相比, EIDE 设备增加了以下一个或多个增强功能:

- 1 数据传输速率可达 16 MB/秒
- 1 不仅支持硬盘驱动器, 还支持 CD 驱动器和磁带驱动器等其他驱动器
- 1 支持容量大于 528 MB 的硬盘驱动器
- 1 最多可支持两个控制器, 每个控制器最多可连接两个设备

EISA

扩展工业标准体系结构 (Extended Industry-Standard Architecture) 的缩写, 32 位扩充总线设计。EISA 系统中的扩充卡连接器也与 8 或 16 位 ISA 扩充卡兼容。

要在安装 EISA 扩充卡时避免配置冲突, 您必须使用 EISA 配置公用程序。此公用程序使您可以指定在哪个扩充槽中包含 EISA 卡并从相应的 EISA 配置文件中获得有关 EISA 卡所需系统资源的信息。

EMC

电磁兼容性 (electromagnetic compatibility) 的缩写。

EMI

电磁干扰 (electromagnetic interference) 的缩写。

EMM

扩充内存管理器 (expanded memory manager) 的缩写。一种公用程序, 在配备有 Intel386™ 或更高级别微处理器的系统上, 使用扩展内存来模拟扩充内存。

EMS

扩充内存规范 (Expanded Memory Specification) 的缩写。

EPP

增强型并行端口 (Enhanced Parallel Port) 的缩写, 可提供增强的双向数据传输。许多设备均设计为可以使用 EPP 标准, 尤其是连接至便携式计算机并行端口的设备, 例如网络适配器或 SCSI 适配器。

EPROM

可擦可编程只读存储器 (erasable programmable read-only memory) 的缩写。

ERA

嵌入式远程访问 (embedded remote access) 的缩写。

ERA/MC

嵌入式远程访问模块化计算机 (embedded remote access modular computer) 的缩写。请参阅[模块化系统](#)。

ERA/O

嵌入式远程访问选项 (embedded remote access option) 的缩写。

ESD

静电释放 (electrostatic discharge) 的缩写。

ESM

嵌入式系统管理 (embedded systems management) 的缩写。

F

华氏 (Fahrenheit) 的缩写。

FAT

文件分配表 (file allocation table) 的缩写。FAT 和 FAT32 均是文件系统，它们的定义如下：

- 1 **FAT** — 一个由 MS-DOS、Windows 3.x、Windows 95 和 Windows 98 使用的文件系统。Windows NT® 和 Windows 2000 也可以使用 FAT 文件系统。操作系统维护文件分配表以记录用于存储文件的磁盘空间各段的状态。
- 1 **FAT32** — 一种从 FAT 派生出来的文件系统。与 FAT 相比，FAT32 可支持尺寸更小的簇，因此可以为 FAT32 驱动器提供更有有效的空间分配。

FCC

美国联邦通信委员会 (Federal Communications Commission) 的缩写。

FEPROM

快擦写可编程只读存储器 (flash erasable programmable read-only memory) 的缩写。快擦写存储器是一种类似于 EEPROM 的非易失性存储设备，但擦除只能在内存块或整个芯片中进行。

FPBGA

现场可编程门阵列 (field programmable gate array) 的缩写，一种具有高密度门的可编程逻辑芯片 (PLD)。

FRU

现场可更换单元 (field replaceable unit) 的缩写。

FTP

文件传输协议 (file transfer protocol) 的缩写。

G

重力 (gravities) 的缩写。

gcc

gnu C 编译器的缩写。

GUI

图形用户界面 (graphical user interface) 的缩写。

h

十六进制 (hexadecimal) 的缩写。以 16 为基的记数系统，在编程中通常用于识别系统 RAM 的地址和设备的 I/O 内存地址。例如，十进制中数字序列 0 至 16 在十六进制记数法中表示为：0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, 10。在文本中，十六进制数字前面通常带有 h。

HBA

主机总线适配器 (host bus adapter) 的缩写。驻留在系统中的 PCI 适配卡，其唯一的功能便是将数据命令从 PCI 总线格式转换为存储设备互连格式（例如 SCSI、光纤信道）并且直接与硬盘、磁带驱动器、CD 驱动器或其他存储设备进行通信。

HMA

高端内存区 (high memory area) 的缩写。1 MB 以上扩展内存的第一个 64 KB。一个符合 XMS 的内存管理器，使 HMA 成为常规内存的直接扩展。另请参阅 XMM。

HPFS

Windows NT 操作系统中高性能文件系统 (High Performance File System) 选项的缩写。

HTTP

超文本传输协议 (Hypertext Transfer Protocol) 的缩写。HTTP 是万维网上用于交换 HTML 文档的客户端-服务器 TCP/IP 协议。

HTTPS

超文本传输安全协议 (HyperText Transmission Protocol, Secure) 的缩写。HTTPS 是 HTTP 的一种变型，Web 浏览器用来处理安全事务。HTTPS 是一种独特的协议，也就是 HTTP 下的 SSL。需要使用“https://”访问带有 SSL 的 HTTP URL，同时还可以继续使用“http://”访问不带 SSL 的 HTTP URL。

Hz

赫兹 (hertz) 的缩写。

I/O

输入/输出 (input/output) 的缩写。键盘是输入设备，打印机是输出设备。通常，I/O 活动和计算活动是可以区分开的。例如，当程序向打印机发送文档时，它进行的是输出活动；当程序对术语列表进行排序时，它进行的则是计算活动。

ICES

设备引起干扰标准 (Interference Causing Equipment Standard, 加拿大) 的缩写。

ICMP

因特网信报控制协议 (Internet Control Message Protocol) 的缩写。ICMP 是一种 TCP/IP 协议，用于发送错误和控制信息。

ICU

ISA 配置公用程序 (ISA Configuration Utility) 的缩写。

ID

标识 (identification) 的缩写。

IDE

集成驱动电子设备 (Integrated Drive Electronics) 的缩写。IDE 是一种计算机系统接口，主要用于硬盘驱动器和 CD。

IDRAC

集成 Dell 远程访问控制器 (Integrated Dell Remote Access Controller) 的缩写。

IHV

独立硬件厂商 (Independent hardware vendor) 的缩写。IHV 通常为其生产的组件开发自己的 MIB。

IP 地址

网际协议地址 (Internet Protocol address) 的缩写。请参阅 TCP/IP。

IPMI

智能平台管理界面 (Intelligent Platform Management Interface) 的缩写，它是管理基于 Intel® 结构的企业系统中使用外围设备采用的一种工业标准。IPMI 的重要特点是资源清册、监测、日志记录和恢复控制功能均独立于主处理器、BIOS 和操作系统。

IPX

互联网信息包交换 (Internetwork packet exchange) 的缩写。

IRQ

中断请求 (Interrupt request) 的缩写。一种信号，表示数据将要发送到外围设备或者外围设备将要接收数据，它通过 IRQ 线路传送到微处理器。必须为每个已连接的外围设备分配一个 IRQ 号码。例如，默认情况下，系统中的第一个串行端口 (COM1) 被分配至 IRQ4。虽然两个设备可以共享同一个 IRQ 分配，但是您不能同时运行这两个设备。

ISA

工业标准体系结构 (Industry-Standard Architecture) 的缩写。ISA 是 16 位扩充总线设计。ISA 系统中的扩充卡连接器也与 8 位 ISA 扩充卡兼容。

iSCSI

互联网 SCSI (Internet SCSI) 的缩写。一种基于 IP 的存储网络标准，用于链接数据存储设备。通过在 IP 网络上执行 SCSI 命令，iSCSI 用于通过内部网协助数据传输以及在长距离管理存储。

ISV

独立软件商 (Independent software vendor) 的缩写。

ITE

信息技术设备 (information technology equipment) 的缩写。

Java

Sun Microsystems 开发的跨平台编程语言。

JSSE

Java 安全套接字扩展 (Java Secure Socket Extension) 的缩写。

K

千 (kilo) 的缩写，表示 1000。

KB

千字节 (kilobyte) 的缩写, 1 KB 等于 1024 字节。

KB/sec

千位/秒 (kilobit per second) 的缩写。

Kbit(s)

千位 (kilobit) 的缩写, 1 千位等于 1024 位。

Kerberos

一种网络验证协议。此协议旨在通过使用密钥加密技术, 为客户/服务器应用程序提供强有力的验证。

KHz

千赫兹 (kilohertz) 的缩写, 1 千赫兹等于 1000 赫兹。

LAN

局域网 (local area network) 的缩写。LAN 系统通常限制于同一座建筑物或几座相邻建筑物之内, 所有设备通过专用线路连接至 LAN。

LCC

有引线芯片载体 (leadless chip carrier) 或无引线芯片载体 (leadless chip carrier) 的缩写。

LDAP

轻量目录访问协议 (Lightweight Directory Access Protocol) 的缩写。一种用于查询并修改 TCP/IP 上运行的目录服务的网络协议。

LED

发光二极管 (light-emitting diode) 的缩写。一种电流通过时亮起的电子设备。

LIF

低插入力 (low insertion force) 的缩写。某些系统使用 LIF 插槽和连接器以便在安装或卸下设备 (例如微处理器芯片) 时, 作用于设备上的力为最小。

LOM

主板 LAN (LAN on motherboard) 的缩写词。

LPT_n

系统中第一个并行打印机端口至第三个并行打印机端口的设备名称分别为 LPT1、LPT2 和 LPT3。

LRA

本地响应代理 (local response agent) 的缩写。

mA

毫安 (milliampere) 的缩写。

mAh

毫安小时 (milliampere-hour) 的缩写。

Managed System

managed system 是通过 Server Administrator 所监测和管理的系统。可以在本地或通过支持的 Web 浏览器远程管理运行 Server Administrator 的系统。请参阅远程管理系统。

Mb

兆位 (megabit) 的缩写。

MB

兆字节 (megabyte) 的缩写。兆字节一词表示 1,048,576 字节；但是指硬盘驱动器存储时，通常将其四舍五入以表示 1,000,000 字节。

MB/sec

兆字节/秒 (megabyte per second) 的缩写。

Mbps

兆位/秒 (megabit per second) 的缩写。

MBR

主引导记录 (master boot record) 的缩写。

MCA

微通道体系结构 (Micro Channel Architecture) 的缩写，用于多处理。MCA 可以消除安装新外围设备时可能发生的冲突。MCA 与 EISA 或 XT 总线体系结构不兼容，因此早期的插卡不能与 MCA 一起使用。

MHz

兆赫兹 (megahertz) 的缩写。

MIB

管理信息库 (management information base) 的缩写。MIB 用于从或者向 SNMP 管理的设备发送详细的状态/命令。

MIDI

乐器数字化接口 (musical instrument digital interface) 的缩写。

MOF

受管对象格式 (managed object format) 的缩写，是一个包含正式 CIM 模式定义的 ASCII 文件。

MPEG

运动图像专家组 (Motion Picture Experts Group) 的缩略词。MPEG 是一种数字视频文件格式。

ms

毫秒 (millisecond) 的缩写。

MS-DOS

Microsoft 磁盘操作系统 (Microsoft Disk Operating System) 的缩写。

MTBF

平均故障间隔时间 (mean time between failures) 的缩写。

mV

毫伏 (millivolt) 的缩写。

name

对象或变量的名称是在 SNMP 管理信息库 (MIB) 文件或 CIM 管理对象文件 (MOF) 中用来对其进行标识的字符串。

NDIS

网络驱动程序接口规范 (Network Driver Interface Specification) 的缩写。

NIC

网络接口控制器 (network interface controller) 的缩写。

NIF

网络接口功能 (network interface function) 的缩写。该术语等同于 NIC。

NIS

网络信息系统 (network information system) 的缩写。NIS 是用于小型网络的网络命名和管理系统。任意主机上的用户都可以使用单一用户标识和密码访问网络中任何主机上的文件或应用程序。

NMI

不可屏蔽中断 (nonmaskable interrupt) 的缩写。设备向微处理器发送 NMI，以通知有关硬件的错误（例如奇偶校验错误）。

ns

纳秒 (nanosecond) 的缩写，一纳秒等于十亿分之一秒。

NTFS

Windows NT 操作系统中 Windows NT 文件系统 (Windows NT File System) 选项的缩写。NTFS 是一种高级文件系统，专用于 Windows NT 操作系统。它支持文件系统恢复、超大容量存储介质和长文件名。通过使用用户定义和系统定义的属性将所有文件作为对象处理，它还支持面向对象的应用程序。另请参阅 FAT 和 FAT32。

NLTM

Windows NT LAN 管理器 (Windows NT LAN Manager) 的缩写。NLTM 是 Windows NT 操作系统的安全保护协议。

NuBus

Apple Macintosh 个人计算机上使用的专用扩充总线。

NVRAM

非易失性随机存取存储器 (nonvolatile random-access memory) 的缩写。系统关闭后不会丢失其内容的存储器。NVRAM 用于维护日期、时间和系统配置信息。

OID

对象标识符 (object identifier) 的缩写。针对执行的整数或指针，用于唯一地标识对象。

OSWDT

操作系统监测计时器 (Operating System Watch Dog Timer) 的缩写。监测计时器是一种计算机硬件计时设备，如果操作系统没有反应会触发系统重置。

OTP

一次可编程 (one-time programmable) 的缩写。

PAM

可插入式验证模块 (Pluggable Authentication Modules) 的缩写。PAM 使系统管理员无需重新编译验证程序即可设置验证规定。

PC 卡

一种符合 PCMCIA 标准的可移动模块，比信用卡稍大，用于便携式计算机。PC 卡也称为“PCMCIA 卡”。PC 卡是 16 位设备，用于将调制解调器、网络适配器、声卡、无线电收发机、固态硬盘和硬盘驱动器连接至便携式计算机。PC 卡是“即插即用”设备，可以由 Card Services 软件自动配置。

PCI

外围组件互连 (Peripheral Component Interconnect) 的缩写。由 Intel Corporation 开发的占主导地位的 32 位或 64 位本地总线标准。

PCMCIA

个人计算机内存卡国际协会 (Personal Computer Memory Card International Association)。一个国际组织，开发可以插入便携式计算机的设备（例如调制解调器和外部硬盘驱动器）的标准。

PERC

可扩充 RAID 控制器 (Expandable RAID controller) 的缩写。

PGA

插针栅极阵列 (pin grid array) 的缩写，一种允许卸下微处理器芯片的微处理器插槽。

PIC

可编程中断控制器 (programmable interrupt controller) 的缩写。

PIP

外围交换程序 (peripheral interchange program) 的缩写。

PKCS #7

公共密钥加密标准 #7 (Public Key Cryptography Standard #7) 的缩写。PKCS #7 是 RSA Data Security, Inc. 的一种标准, 用于封装签名数据, 比如认证链。

PKIS

Novell 公开密钥基础设施服务 (Novell Public Key Infrastructure Services) 的缩写。

PLCC

塑料有引线芯片载体 (plastic leaded chip carrier) 的缩写。

PME

电源管理事件 (Power Management Event) 的缩写。PME 是外围设备组件连接上的一个插针, 使 PCI 设备能够确定唤醒事件。

POST

开机自检 (power-on self-test) 的缩写。在打开系统后、载入操作系统之前, POST 将检测各种系统组件, 例如 RAM、磁盘驱动器和键盘。

ppm

页/分钟 (pages per minute) 的缩写。

PPP

点对点协议 (Point-to-Point Protocol) 的缩写。

PQFP

塑料四边引出扁平封装 (plastic quad flat pack) 的缩写, 一种微处理器插槽, 微处理器芯片可以永久性地安装在此插槽中。

PS

电源设备 (power supply) 的缩写。

PS/2

个人系统/2 (Personal System/2) 的缩写。

PXE

预引导执行环境 (Pre-boot eXecution Environment) 的缩写。

QFP

四边引出扁平封装 (quad flat pack) 的缩写。

RAC

远程访问控制器 (remote access controller) 的缩略词。

RAID

单独磁盘冗余阵列 (redundant array of independent disks) 的缩写。

RAM

随机存取存储器 (random-access memory) 的缩写词。系统的主要暂时存储区域，用于存储程序指令和数据。RAM 中的每一位置均由称为内存地址的数字标识。关闭系统后，RAM 中存储的所有信息都将丢失。

RAMDAC

随机存取存储器数模转换器 (random-access memory digital-to-analog converter) 的缩写。

RBAC

基于角色的访问控制 (role-based access control) 的缩写。

RDRAM

Rambus DRAM 的缩写。Rambus, Inc. 提供的动态 RAM 芯片技术。Direct RDRAMs 使用在系统中。计算机中使用了 Direct RDRAM。Direct RDRAM 芯片位于 RIMM 模块中，它们类似于 DIMM，但具有不同的插针设置。该芯片可设计为双通道，使传输速率增加一倍，达到 3.2 GB/秒。

RFI

射频干扰 (radio frequency interference) 的缩写。

RGB

红/绿/蓝 (red/green/blue) 的缩写。

RIMM

Rambus 直插式内存模块 (Rambus In-line Memory Module) 的缩写，与 DIMM 模块相当的 Rambus 模块。

RMI

远程方法调用 (Remote Method Invocation) 的缩写。RMI 是 Java 编程语言库的一部分，使一个系统上运行的 Java 程序能够访问另一个系统上运行的 Java 程序的对象和方法。

ROM

只读存储器 (read-only memory) 的缩写。您的系统包含一些对系统运行至关重要的程序，以 ROM 代码的形式存在。与 RAM 不一样，ROM 芯片即使在关闭系统后仍然保留其中的内容。例如，ROM 代码中包括启动系统引导例行程序和 POST 的程序。

RPM

转/分钟 (revolutions per minute) 的缩写。

RPM

Red Hat® 软件包管理程序 (Red Hat® Package Manager) 的缩写。

RTC

实时时钟 (real-time clock) 的缩写。系统中使用电池供电的时钟电路，用于在系统关闭后保持日期和时间。

SAN

存储区域网络 (storage area network) 的缩写。

SAS

安全验证服务 (Secure Authentication Service) 或串行连接 SCSI (Serial-attached SCSI) 的缩写。当指安全性协议或验证时, SAS 是指安全验证服务。当指某些采用串行(一次一个位)即通过细电缆进行的数字数据传输方式的计算机外围设备时, SAS 是串行连接 SCSI。

SCA

单连接器连接 (single connector attachment) 的缩写。

SCSI

小型计算机系统接口 (small computer system interface) 的缩写。一种 I/O 总线接口, 其数据传输速率比标准端口更快。一个 SCSI 接口最多可连接七个设备(某些较新型的 SCSI 接口可连接 15 个设备)。

SDMS

SCSI 设备管理系统 (SCSI device management system) 的缩写。

sec

秒 (second) 的缩写。

SEC

单边接触 (single-edge contact) 的缩写。

SEL

系统事件日志 (system event log) 的缩写。

SGRAM

同步图形 RAM (synchronous graphics RAM) 的缩写。

shadowing 效率增强技术

计算机的系统和视频 BIOS 代码, 通常存储在 ROM 芯片中。Shadowing 效率增强技术表示一种性能增强技术, 即在引导例行程序期间将 BIOS 代码复制到上端内存区 (640 KB 之上) 中较快的 RAM 芯片中。

SIMD

单指令多数据 (Single Instruction Multiple Data) 的缩写。

SIMM

单列直插式内存模块 (single in-line memory module) 的缩写。包含 DRAM 芯片的小型电路板, 与系统板相连接。

SIP

单列直插式组件 (single in-line package) 的缩写。一种封装电子组件的类型, 其中所有的连接插针都从组件的一侧引出。SIP 也称为单列直插针式组件 (SIPP)。

SKU

库存单元 (stock keeping unit) 的缩写。

SMART

自我监测分析和报告技术 (Self-Monitoring Analysis and Reporting Technology) 的缩写。一种技术，使硬盘驱动器可以向系统 BIOS 报告错误和故障，然后在屏幕上显示错误信息。要使用这种技术，必须具备 SMART 兼容的硬盘驱动器和系统 BIOS 的正确支持。

SMBIOS

系统管理 BIOS (system management BIOS) 的缩写。

SMD

表面封装设备 (surface mount device) 的缩写。

SMTP

简单邮件传输协议 (Simple Mail Transfer Protocol) 的缩写。

SNMP

简单网络管理协议 (Simple Network Management Protocol) 的缩写。SNMP 是一种常用的网络控制和监测协议，是原有的 TCP/IP 协议组的一部分。SNMP 提供了有关不同网络设备（例如网络服务器或路由器）的重要信息发送至管理应用程序的格式。

SODIMM

小型 DIMM (small outline-DIMM) 的缩写。一种 DIMM 模块，由于使用 TSOP 芯片封装而变得更薄。SODIMM 广泛用于便携式计算机。

SOIC

小型 IC (Small Outline IC) 的缩写，一种小尺寸、塑料、矩形表面芯片封装技术，使用延伸至外部的翼形插针。

SOJ

小尺寸 J 形引线封装 (small outline package J-lead) 的缩写，一种小尺寸、塑料、矩形表面芯片封装技术，在两个长边上有 j 形插针。

SRAM

静态随机存取存储器 (static random-access memory) 的缩写。由于 SRAM 芯片不要求连续刷新，所以比 DRAM 芯片快得多。

SSL

安全套接字层 (secure socket layer) 的缩写。

SVGA

超级视频图形阵列 (super video graphics array) 的缩写。VGA 和 SVGA 是视频适配器的视频标准。与以前的标准相比，它们的分辨率更高，颜色显示能力更强。

要以特定的分辨率显示程序，您必须安装相应的视频驱动程序，并且显示器必须支持此分辨率。同样，程序能够显示的颜色数取决于显示器和视频驱动程序的性能，以及系统中安装的视频内存的容量。

system.ini 文件

Windows 操作系统的启动文件。启动 Windows 时，Windows 将查询 **system.ini** 文件以确定 Windows 运行环境的各个选项。另外 **system.ini** 文件还记录了 Windows 中安装了哪一个视频、鼠标和键盘驱动程序。

运行控制面板或 Windows 安装程序可能会更改 **system.ini** 文件中的选项。有时，您可能需要使用文本编辑器（例如记事本）手动更改 **system.ini** 文件的选项或向其中添加选项。

TCP/IP

传输控制协议/网际协议 (Transmission Control Protocol/Internet Protocol) 的缩写。一种用于在包含不同系统（例如运行 Windows 和 UNIX 的系统）的计算机网络中传输信息的系统。

TFTP

小型文件传输协议 (Trivial File Transfer Protocol) 的缩写。TFTP 是一种 TCP/IP FTP 协议，不具有目录或密码功能。

tpi

磁道/英寸 (tracks per inch) 的缩写。

TPM

可信平台模块 (Trusted Platform Module) 的缩写

TQFP

薄型四边引出扁平封装 (thin quad flat pack) 的缩写。

TSOP

薄型小尺寸封装 (thin small outline package) 的缩写。一种很薄的、塑料、矩形表面芯片封装技术，在两个短边上有翼形插针。

TSR

内存驻留程序 (terminate-and-stay-resident) 的缩写。TSR 程序在“后台”运行。大多数 TSR 程序可以执行预定义的组合键（有时称为热键），使您可以在运行其它程序时激活 TSR 程序的界面。TSR 程序使用完毕后，您可以返回其它应用程序，并将 TSR 程序驻留在内存中以备稍后使用。TSR 程序有时会引起内存冲突。在进行故障排除时，通过不启动任何 TSR 程序重新引导系统可以排除发生这种冲突的可能性。

UART

通用异步收发机 (universal asynchronous receiver transmitter) 的缩略词，组成串行端口的电子电路。

UDP

用户数据报协议 (user datagram protocol) 的缩写。

UL

Underwriters Laboratories 的缩写。

UMB

上端内存块 (upper memory blocks) 的缩写。

unicode

由 Unicode Consortium 开发和维护 的定宽、16 位世界通行的字符编码。

UPS

不间断电源设备 (uninterruptible power supply) 的缩写。能够在断电时自动为系统供电的电池电源设备。

URL

统一资源定位器 (Uniform Resource Locator [早先为 Universal Resource Locator]) 的缩写。

USB

通用串行总线 (Universal Serial Bus) 缩写。USB 连接器可为多个 USB 兼容设备 (例如鼠标、键盘、打印机和计算机扬声器) 提供单一连接点。USB 设备也可在系统运行时进行连接或断开连接。

UTP

非屏蔽双绞线 (unshielded twisted pair) 的缩写。

UUID

通用唯一标识 (Universal Unique Identification) 的缩写。

V

伏特 (volt) 的缩写。

VAC

交流电压 (volt alternating current) 的缩写。

VCCI

干扰自愿控制委员会 (Voluntary Control Council for Interference) 的缩写。

VDC

直流电压 (volt direct current) 的缩写。

VESA

视频电子标准协会 (Video Electronics Standards Association) 的缩写。

VGA

视频图形阵列 (video graphics array) 的缩写。VGA 和 SVGA 是视频适配器的视频标准。与以前的标准相比，它们的分辨率更高，颜色显示能力更强。要以特定的分辨率显示程序，您必须安装相应的视频驱动程序，并且显示器必须支持此分辨率。同样，程序能够显示的颜色数取决于显示器和视频驱动程序的性能，以及为视频适配器安装的视频内存的容量。

VGA 功能连接器

在一些带有内置 VGA 视频适配器的系统上，VGA 功能连接器使可以向系统添加增强型适配器 (例如视频加速器)。VGA 功能连接器也称为 VGA 通道连接器。

VLSI

超大规模集成电路 (very-large-scale integration) 的缩写。

VLVESA

超低压企业系统体系结构 (very low voltage enterprise system architecture) 的缩写。

vpp

峰值电压 (peak-point voltage) 的缩写。

VRAM

视频随机存取存储器 (video random-access memory) 的缩写。有些视频适配器使用 VRAM 芯片 (或组合使用 VRAM 和 DRAM) 来提高视频性能。VRAM 为双端口, 使视频适配器能够同时更新屏幕并接收新的图像数据。

VRM

稳压器模块 (voltage regulator module) 的缩写。

W

瓦特 (watt) 的缩写。

Web Server

一种应用程序, 使 Web 页面能够通过使用 HTTP 协议的 Web 浏览器查看。

WH

瓦特小时 (watt-hour) 的缩写。

win.ini 文件

Windows 操作系统的启动文件。启动 Windows 时, Windows 将查询 **win.ini** 文件以确定 Windows 运行环境的各个选项。另外, **win.ini** 文件还记录了为 Windows 安装的打印机和字体。**win.ini** 文件通常还包括硬盘驱动器中安装的 Windows 应用程序的可选设置。运行控制面板或 Windows 安装程序可能会更改 **win.ini** 文件中的选项。其它情况下, 您可能需要用文本编辑器 (例如记事本) 来进行更改或将选项手动添加至 **win.ini** 文件。

Winbind

一种程序, 使异构网络中的用户能够使用具有 UNIX 或 Windows NT 操作系统的工作站登录。该程序使 NT 对于每个 UNIX 工作站看起来像是 UNIX, 从而使用 UNIX 的工作站能够在 NT 域中运行。

Windows 95

一种集成而完整的 Microsoft Windows 操作系统, 不需要 MS-DOS。它增强了操作系统性能、易用性、工作组功能, 并简化了文件的管理和浏览。

Windows NT

由 Microsoft 开发的高性能服务器和工作站操作系统软件, 专为技术、工程和财务应用程序而设计。

WMI

Windows 管理工具 (Windows Management Instrumentation) 的缩写。WMI 提供 CIM 对象管理器服务。

X Window 系统

Red Hat Enterprise Linux® 环境中使用的图形用户界面。

X.509 认证

X.509 认证将公用密钥与主体本身或主体的其他属性结合起来。主体可以是人、应用程序代码 (例如签名的小程序) 或任何其他可唯一标识的实体 (例如安全端口服务器或 Web Server)。

Xen

Xen 是 x86 系统的一种虚拟计算机监视器。

XMM

扩展内存管理器 (extended memory manager) 的缩写，一种公用程序，使应用程序和操作系统可以按照 XMS 使用扩展内存。

XMS

扩展内存规范 (eXtended Memory Specification) 的缩写。

ZIF

零插入力 (zero insertion force) 的缩写。某些系统使用 ZIF 插槽和连接器，以便在安装或卸下设备（例如微处理器芯片）时无需用力。

ZIP

Iomega 生产的 3.5 英寸可移动磁盘驱动器。它最初可提供 100 MB 可移动磁盘，这种驱动器配有软件，可以对磁盘进行编目并锁定文件以保证安全。250 MB 的 Zip 驱动器也可以对 100 MB Zip 卡盒进行读写操作。

保护模式

一种 80286 或更高级别的微处理器支持的运行模式，保护模式使操作系统可以实现：

- 1 16 MB (80286 微处理器) 至 4 GB (Intel386 或更高级别微处理器) 内存地址空间
- 1 多任务处理
- 1 虚拟内存，一种使用硬盘驱动器增加可寻址内存的方法

Windows NT、OS/2® 和 UNIX® 32 位操作系统均以保护模式运行。MS-DOS 无法以保护模式运行；但是，某些可以从 MS-DOS 启动的程序（例如 Windows 操作系统）可以将系统置入保护模式。

本地总线

在具有本地总线扩充功能的系统上，有些外围设备（比如视频适配器电路）可以设计得比在传统扩充总线上运行得更快。有些本地总线设计使外围设备能够以系统微处理器的速度和数据通路宽度运行。

哔声代码

系统扬声器以哔声形式发出的一种诊断信息。例如，哔声代码 1-1-3 表示一声哔声，接着是第二声哔声，然后连续发出三声哔声。

变量

管理型目标的组件。例如，温度探测器的变量用于说明其性能、运行状况以及某些可以帮助您确定温度探测器正确位置的指针。

变量绑定

一种用于分配对象标识符 (OID) 的算法。变量绑定制订了唯一标识某个企业的十进制前缀的规则，并制订了公式，为在该企业的 MIB 中定义的对象指定唯一标识符。

表

在 SNMP MIB 中，表是描述组成管理型对象的变量的二维数组。

并行端口

一种输入/输出端口，通常用于将并行打印机连接至系统。通常，可以根据其 25 孔连接器来识别系统中的并行端口。

病毒

一种自启动程序，旨在引起不便。病毒程序会破坏存储在硬盘驱动器中的文件，或复制自身直至用尽计算机系统或网络的内存。病毒程序通常通过“被感染的”软盘从一个系统转到另一个系统，它们通过软盘将自身复制到硬盘驱动器。为防止病毒程序，应当注意以下几点：

- 1 定期运行系统硬盘驱动器中的病毒检查公用程序
- 1 使用任何软盘（包括市面上出售的软件）之前，请始终运行病毒检查公用程序

波特率

数据传输速率的度量单位。例如，调制解调器就是通过系统的 COM（串行）端口以一个或多个指定的波特率传输数据。

参数

为某个程序指定的值或选项。参数有时称为参数选项符或自变量。

常规内存

RAM 的第一个 640 KB。所有系统中均有常规内存。除非经过特殊设计，否则 MS-DOS® 程序只能在常规内存中运行。

超时

指定的一段时间，如果系统在该时间段内无活动，则会激活节能功能。

串行端口

一种输入/输出端口，经常用于将调制解调器连接至系统。通常，您可以根据其 9 针连接器来识别系统中的串行端口。

电源设备

一种电子系统，将墙上电源插座的交流电转变为系统电路所需的直流电。个人计算机中的电源设备一般可以提供多种电压。

电源装置

系统机箱中的一组电源设备。

多频显示器

一种支持若干种视频标准的显示器。多频显示器可以调整至来自多种视频适配器的信号的频率范围。

分区

可以使用 fdisk 命令将硬盘驱动器分成多个称为分区的物理部分。每个分区都可以包含多个逻辑驱动器。硬盘驱动器分区后，您必须使用 format 命令对每个逻辑驱动器进行格式化。

服务标签号码

条形码标签，当需要致电寻求客户支持或技术支持时，用于识别每个系统。

服务器模块

一个作为独立系统运行的模块化系统组件。要作为一个系统运行，将服务器模块插入机箱，其中带有电源设备、风扇、系统管理模块并且至少一个网络交换模块。电源设备、风扇、系统管理模块和网络交换模块是机箱中各个服务器模块的共享资源。请参阅[模块化系统](#)。

高速缓存

一种高速存储区域，用于保存数据或指令的副本以进行快速数据检索。例如，系统的 BIOS 可以将 ROM 代码高速缓存到速度更快的 RAM 中。或者，磁盘高速缓存公用程序可以保留

RAM，在其中存储系统磁盘驱动器经常访问的信息；如果程序请求访问磁盘驱动器中的数据且该数据位于高速缓存中，磁盘高速缓存公用程序就可以从 RAM 中检索数据，这比从磁盘驱动器检索数据更快。

格式化

准备硬盘驱动器或软盘以用于存储文件的过程。无条件格式化将删除存储在磁盘中的所有数据。

隔行扫描

一种提高视频分辨率的技术，它仅更新屏幕上相隔的水平行。由于隔行扫描会导致明显的屏幕闪烁，因此大多数用户更倾向于逐行扫描视频适配器分辨率。

公用程序

用于管理系统资源（例如内存、磁盘驱动器或打印机）的程序。

公用程序分区

硬盘驱动器上的可引导分区，提供用于硬件和软件的公用程序和诊断程序。该分区在激活时将作为分区的公用程序引导并提供可执行环境。

功能

表示某个对象可以执行的操作，或者针对某个管理型对象执行的操作。例如，如果某个插卡可以热插拔，则可以在系统电源处于接通状态时更换该插卡。

固件

已经写到只读内存 (ROM) 上的软件（程序或数据）。固件可以引导和操作设备。每个控制器均包含固件，以帮助提供控制器功能。

光纤信道

一种数据传输接口技术，允许单连接技术中的高速输入/输出和联网功能。光纤信道标准支持若干种拓扑，包括光纤信道点对点、光纤信道网（通用交换拓扑）和光纤信道仲裁环路 (FC_AL)。

即插即用

一种行业标准规格，使在个人计算机中添加硬件设备变得更容易。即插即用可以提供自动安装和配置、与现有硬件的兼容以及对可移动计算环境的动态支持。

架构

类定义的集合，用于说明特定环境中的管理型对象。一组类定义的架构，用于表示所有管理环境中公用的受管对象，这就是 CIM 被称为公用信息模型的原因。

交换机

系统板上的开关用于控制计算机系统中的各种电路或功能。这些开关就是 DIP 开关，它们通常与两个或多个开关一起封装在一个塑料盒中。系统板上通常使用两种 DIP 开关：滑动式开关和插压式开关。开关的名称取决于更改开关设置（开和关）的方式。

可引导软盘

可以从软盘启动系统。要制作可引导软盘，请将软盘插入软盘驱动器，在命令提示符后键入 `sys a:` 然后按 <Enter>。如果系统不能从硬盘驱动器引导，请使用该可引导软盘。

控制面板

系统的一部分，包含指示灯和控件，例如电源开关、硬盘驱动器访问指示灯和电源指示灯。

控制器

一种芯片，用于控制微处理器与内存之间或微处理器与外围设备（例如磁盘驱动器或键盘）之间的数据传输。

快擦写 BIOS

一种 BIOS，存储在快擦写存储器中，而不是 ROM 中。快擦写 BIOS 芯片可以直接更新，而 ROM BIOS 则必须更换为新的芯片。

快擦写存储器

一种 EEPROM 芯片，即使仍然安装在系统中，也可以通过软盘中的公用程序重新进行编程；大多数 EEPROM 芯片只能通过特殊的编程设备进行重写。

扩充卡连接器

一种位于系统的系统板或提升板上的连接器，用于插接扩充卡。

扩充内存

一种用于访问 1 MB 以上 RAM 的技术。要启用系统上的扩充内存，必须使用 EMM。只有在您运行的应用程序可以使用（或者需要）扩充内存时，才需要将系统配置为支持扩充内存。

扩充总线

系统包含一条扩充总线，使微处理器能够与外围设备（例如网卡或内置调制解调器）的控制器进行通信。

扩展内存

1 MB 以上的 RAM。可以使用扩展内存的大多数软件（例如 Windows 操作系统）都要求 XMM 控制扩展内存。

冷却装置

系统机箱中的风扇或其他冷却设备。

模块化系统

可以包括多个服务器模块的系统。每个服务器模块都作为一个独立的系统运行。要作为一个系统运行，将服务器模块插入机箱，其中带有电源设备、风扇、系统管理模块并且至少一个网络交换模块。电源设备、风扇、系统管理模块和网络交换模块是机箱中各个服务器模块的共享资源。请参阅[服务器模块](#)。

目录

目录以层次化、“倒置树状”结构维护磁盘上相关的文件。每个磁盘都有一个“根”目录：例如，`C:\>` 提示符通常表示您位于硬盘驱动器 C 的根目录。其他从根目录分支出去的目录都称为子目录。子目录还可以包含由其分支出的其它目录。

内部 USB

内部 USB 快擦写驱动器和设备是一种附加存储。内部 USB 会增强虚拟化功能。

内部微处理器高速缓存

内置于微处理器的指令和数据高速缓存。Intel Pentium 微处理器包括 16 KB 内部高速缓存，设置为 8 KB 只读指令高速缓存和 8 KB 读/写数据高速缓存。

内存

系统可以包含几种不同的内存，比如 RAM、ROM 和视频内存。内存一词经常用作 RAM 的同义词；例如，不规范的语句“系统具有 16 MB 内存”是指系统具有 16 MB RAM。

内存地址

系统 RAM 中的特定位置，通常以十六进制数字表示。

内存管理器

一种公用程序，控制除常规内存之外内存（例如扩展内存或扩充内存）的执行。

内存模块

包含 DRAM 芯片的小型电路板，与系统板相连接。

嵌入式系统管理程序

请参阅 *内部 USB*

驱动器型号

系统可以识别许多特定的硬盘驱动器。每个硬盘驱动器都分配有一个驱动器型号，该型号存储在 NVRAM 中。系统的系统设置程序中所指定的硬盘驱动器必须与系统中实际安装的驱动器相匹配。系统设置程序还使您可以为驱动器类型列表（存储在 NVRAM 中）中没有包括的驱动器指定物理参数（逻辑磁柱、逻辑磁头、磁柱数和每组的逻辑扇区）。

热插拔

可在系统运行时卸下和更换冗余部件的功能。也称为“热备用”。

散热器

带有金属钉或凸片的金属板，这些金属钉或凸片有助于释放热量。大多数微处理器都包括一个散热器。

上端内存区

位于 640 KB 和 1 MB 之间的 384 KB RAM。如果系统配备了 Intel386 或更高版本的微处理器，名为内存管理器的公用程序便可在上端内存区中创建 UMB，可以在其中载入设备驱动程序和内存驻留程序。

设备驱动程序

一种程序，使操作系统或某些其他程序能够与外围设备（例如打印机）正确接合。某些设备驱动程序（例如网络驱动程序）必须从 config.sys 文件（具有 device= 语句）载入，或者作为内存驻留程序（通常通过 autoexec.bat 文件）载入。其他驱动程序（例如视频驱动程序）则必须在启动使用该驱动程序的程序时载入。

设置

设置是可管理对象的状态，有助于确定在组件中检测到某一值时会发生的情况。例如，用户可以将温度探测器的临界阈值上限设置为 75 摄氏度。如果温度探测器达到这个温度，该设置将向管理系统送警报，以使用户能够采取措施。某些设置在达到其值后可以使系统关闭或引发防止系统损坏的其它响应。

实模式

一种 80286 或更高版本的微处理器支持的运行模式，模仿 8086 微处理器的体系结构。

视频分辨率

视频分辨率表示为横向像素数乘以纵向像素数，例如 800 x 600。要以特定的图形分辨率显示程序，必须安装相应的视频驱动程序，并且显示器必须支持此分辨率。

视频模式

视频适配器通常支持多种文本和图形显示模式。基于字符的软件以文本模式显示。文本模式可以定义为 x 列乘 y 行字符。基于图形的软件以图形模式显示，这种模式可以定义为 x 个水平像素 y 个垂直像素乘 z 种颜色。

视频内存

大多数 VGA 和 SVGA 视频适配器在系统 RAM 之外另外带有存储器芯片。如果视频驱动程序和显示器性能配备得当，程序能够显示的颜色数主要受所安装的视频内存容量的影响。

视频驱动程序

一种程序，允许按照选定分辨率和所需颜色数来显示图形模式的应用程序和操作系统。软件包可能包含一些“一般”视频驱动程序。可能需要其他视频驱动程序，以与系统中安装的视频适配器相匹配。

视频适配器

配合显示器提供系统视频功能的逻辑电路。视频适配器支持的功能可能多于或少于特定显示器提供的功能。通常，视频适配器会附带视频驱动程序，用于以多种视频模式显示常见应用程序和操作系统。

在一些系统中，视频适配器被集成至系统板。还有许多插入扩充卡连接器的视频适配卡可供使用。

视频适配器通常包括与系统板上的 RAM 相互独立的内存。视频内存的容量与适配器的视频驱动程序会影响可以同时显示的颜色数。视频适配器还可包括自身的协处理器，以加速图形渲染。

适配卡

一种扩充卡，插在系统的系统板上的扩充卡连接器中。通过提供扩充总线 and 外围设备之间的接口，适配卡可以为系统添加某些专门功能。适配卡的例子包括：网卡、声卡和 SCSI 适配器。

数学协处理器

请参阅协处理器。

刷新率

显示器刷新显示器屏幕上视频图像的速率。更准确地说，刷新率是屏幕的水平线更新的频率（有时也称为垂直频率），以 Hz 为单位。刷新率越高，人眼觉察到的图像闪烁越小。较高的刷新率即是逐行扫描。

套装程序软盘

您可以使用这套软盘执行操作系统或应用程序的完整安装。重新配置程序时，您通常会需要该程序的套装程序软盘。

提供者

提供者是 CIM 模式的扩展，可以与管理型对象进行通信并访问多种资源的数据和事件通告。提供者将这些信息转发至 CIM 对象管理器以进行综合和翻译。

跳线

跳线是电路板上带有两个或多个突起插针的小块。带电线的塑料插头可插在插针上。电线连接至插针后即可形成电路。跳线提供了一种更改印刷电路板中电路的方法，简单易行而又便于恢复。

调制解调器

使系统可以通过电话线与其他系统进行通信的设备。

通过 LAN 唤醒

一种功能，即通过网络打开客户端站点的电源。远程唤醒可在无人看管的情况下在用户的机器上执行软件升级和其它管理任务。它还可使远程用户可以访问已关闭的计算机。Intel 将远程唤醒称为“通过 LAN 唤醒”。

图形模式

一种视频模式，可以定义为 x 个水平像素乘 y 个垂直像素乘 z 种颜色。

图形协处理器

请参阅协处理器。

外部高速缓存

一种使用 SRAM 芯片的 RAM 高速缓存。由于 SRAM 芯片的运行速率是 DRAM 芯片的几倍，因此微处理器从外部高速缓存检索数据和指令的速度要比从 RAM 进行检索更快。

外围设备

连接至系统的内部或外部设备，例如打印机、磁盘驱动器或键盘。

微处理器

系统中的主要计算芯片，用于控制算术和逻辑函数的解释和执行。通常，针对一种微处理器编写的软件必须经过修改后才能和其它微处理器上运行。CPU 是微处理器的同义词。

文本编辑器

一种应用程序，用于编辑只包含 ASCII 字符的文本文件。例如，Windows 记事本就是文本编辑器。虽然某些微处理器能够对文本文件进行读和写，但大多数微处理器都使用包含二进制字符的专有文件格式。

文本模式

一种视频模式，可定义为 x 列乘 y 行字符。

物理内存阵列

物理内存阵列是系统的全部物理内存。物理内存阵列的变量包括最大容量、母板上内存插槽的总数和所使用插槽的总数。

系统板

作为主要的电路板，系统板通常包含系统的大部分集成组件，例如：

- 1 微处理器
- 1 RAM
- 1 标准外围设备（例如键盘）的控制器
- 1 各种 ROM 芯片

常用的系统板的同义词有母板和逻辑板。

系统内存

系统内存是 RAM 的同义词。

系统配置信息

内存中存储的数据，告知系统安装了哪些硬件，以及应当如何配置系统以运行这些硬件。

系统软盘

系统软盘是可引导软盘的同义词。

系统设置程序

一种基于 BIOS 的程序，使您可以配置系统硬件并通过设置密码保护和能源管理等功能自定义系统的运行。系统设置程序中的某些选项要求重新引导系统（或者系统可能自动重新引导）以更改硬件配置。由于系统设置程序存储在 NVRAM 中，所有设置均保持有效，直至您再次更改这些设置。

显示适配卡

请参阅视频适配器。

像素

视频显示屏上的一个点。像素按行和列排列生成图像。视频分辨率表示为横向像素数乘以纵向像素数，例如 640 x 480。

协处理器

一种芯片，可以帮助系统微处理器执行特定的处理任务。例如，数学协处理器执行数字处理。图形协处理器控制视频透视图。例如 Intel® Pentium® 微处理器包括一个内置数学协处理器。

写保护

只读文件被称为写保护文件。您可以对 3.5 英寸软盘进行写保护，方法是：将其写保护挡片滑至打开位置，或者在系统设置程序中设置写保护功能。

虚拟内存

一种通过使用硬盘驱动器来增加可定址 RAM 的方法。例如，当系统具有 16 MB RAM 并在硬盘驱动器中设置了 16 MB 虚拟内存时，操作系统将按照该系统具有 32 MB 物理 RAM 的情况来管理系统。

验证

Server Administrator Remote Access Controller 具有两种验证用户权限的方法：

RAC 验证和本地操作系统验证。RAC 验证始终处于已启用状态。管理员可以设置用于访问 RAC 的特定用户帐户和密码。

管理员还需要为操作系统定义不同的用户和用户帐户级别；不同的用户级别具有不同的权限。如果管理员不想在为操作系统中的用户定义一组权限后再定义一组单独用于 RAC 的用户和帐户，则可以选择在 RAC 上进行本地操作系统验证。如果您为 RAC 启用了本地操作系统验证，则操作系统中任何处于 Administrator（管理员）状况的用户均可登录到 RAC。

引导例行程序

当启动系统时，引导例行程序将清除所有内存，初始化设备，并载入操作系统。当操作系统无法响应时，您可以通过按 Ctrl+<Alt>+ 来重新引导（也称热启动）计算机；否则您必须通过按复位按钮或关机后重新开机来执行冷启动。

映射的物理内存阵列

映射的物理内存阵列表示物理内存分隔的方式。

例如，一个映射区可能为 640 KB，另一个映射区可能在 1 MB 和 127 MB 之间。

语法

一种要求在键入命令或指令时必须遵循的规则，以使系统可以识别。变量的语法表明其数据类型。

阈值

系统通常配备多种传感器来监测温度、电压、电流和风扇速度。传感器阈值指定的范围（最小和最大值）用于确定传感器是否在正常、非临界、临界或严重状态下运行。Server Administrator 支持的阈值包括：

- 1 严重阈值上限
- 1 临界阈值上限
- 1 非临界阈值上限
- 1 正常
- 1 非临界阈值下限
- 1 临界阈值下限
- 1 严重阈值下限

原始

未经处理。该术语表示传递至输入/输出设备时未经解释的数据。相反，已处理表示传递至输入/输出设备之前已经处理过的数据。它通常表示不以任何专用格式保存的未压缩文本。该术语出自 UNIX，对于输出至终端的数据，UNIX 支持已处理模式和原始模式。

远程管理系统

远程管理系统是使用支持的 Web 浏览器从远程位置访问受管系统的 Server Administrator 主页的系统。请参阅受管系统。

在线访问服务

一种服务，通常提供对因特网、电子邮件、公告栏、聊天室和文件库的访问。

只读文件

只读文件是一种禁止编辑或删除的文件。文件在下列情况时处于只读状态：

- 1 已启用只读属性。
- 1 驻留在物理写保护的软盘上，或驻留在写保护驱动器中的软盘上。
- 1 位于网络目录中，而系统管理员给分配了该目录的只读权限。

终结处理

某些设备（例如 SCSI 电缆两端的最后一个设备）必须进行终结处理，以防止电缆中的反射和乱真信号。将此类设备连接至序列中时，您可能需要启用或禁用这些设备上的终结处理。方法是更改设备上的跳线或开关设置，或者更改设备配置软件中的设置。

逐行扫描

按顺序刷新屏幕上的每一水平行以减少屏幕闪烁的技术。

主机适配器

主机适配器实现系统总线与外围设备的控制器之间的通信。（硬盘驱动器控制器子系统包括集成的主机适配器电路。）要在系统中添加 SCSI 扩充总线，您必须安装或连接相应的主机适配器。

状态

表示具有一种以上状态的对象状态。例如，某个对象可能处于“未就绪”状态。

状态

表示对象的运行状况或功能。例如，当温度探测器测量的温度在可以接受的范围内时，该探测器即处于正常状况。当探测器测量的温度超过用户设置的极限时，则该探测器将报告严重状况。

资产标签代码

分配给系统的独立代码（通常由系统管理员分配），用于安全保护和跟踪。

自述文件

软件包或硬件产品附带的文本文件，包含软件或硬件说明文件的补充或更新信息。通常，自述文件提供安装信息、介绍未写入说明文件的新产品增强功能或更正，并列出了已知问题或使用软件或硬件时需要注意的其它事宜。

总线

系统组件之间的信息通道。系统包含一条扩充总线，使微处理器可以与所有控制器（用于控制连接至系统的各种外围设备）进行通信。系统中还包含一条地址总线以及一条数据总线，用于微处理器和 RAM 之间的通信。

组合键

要求您同时按多个键的命令。例如，您可以通过按下 <Ctrl><Alt> 组合键来重新引导系统。

[目录](#)

安装 Server Administrator

Dell OpenManage Server Administrator 版本 5.5 用户指南

- [概览](#)
- [开始之前](#)
- [安装要求](#)
- [安装过程](#)

概览

可以使用多种方式来安装 Server Administrator。Dell™ *Systems Management Tools and Documentation DVD* 提供了可用于在 managed system 上安装、升级和卸载 Server Administrator 和其它 managed system 软件组件的安装程序。Dell *Systems Management Tools and Documentation DVD* 提供了可用于在 management station 上安装、升级和卸载 Management Station 软件组件的安装程序。此外，您还可以在无人值守安装情况下，通过网络在多个系统上安装 Server Administrator。Dell OpenManage™ 产品现在使用操作系统本机的安装过程进行安装。请遵循配置向导设置 Server Administrator。有关详情，请参阅《Dell OpenManage 安装和安全性用户指南》。

无人值守和无提示安装

可以使用 Dell™ *Systems Management Tools and Documentation DVD* 在运行支持的 Microsoft Windows、Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统的系统中执行 Server Administrator 的无人值守安装和卸载。此外，可以使用命令行在运行支持的 Microsoft Windows、Red Hat Enterprise Linux 和 SUSE LINUX Enterprise Server 操作系统的系统中安装和卸载 Server Administrator。

升级 Server Administrator

Dell OpenManage 软件允许使用 *Dell Systems Management Tools and Documentation DVD* 从版本 4.3 或更高版本升级至版本 5.5。

在 Dell OpenManage 5.5 中支持 Service Pack 升级。

 **注：** 如果有早于 4.3 的 Dell OpenManage 版本，则先卸载，然后重新安装 Dell OpenManage 5.5。有关详情，请参阅《Dell OpenManage 安装和安全性用户指南》。

要从 Dell OpenManage 4.3 或更高版本升级到 Dell OpenManage 5.5，请使用 **setup.exe** 或键入：

```
msiexec /i SysMgmt.msi /qn  
(对于全新安装或升级安装。例如，从 Dell OpenManage 版本 4.3 升级至版本 5.5。)
```


对于小型升级，比如从 Dell OpenManage 版本 4.3 升级至版本 4.4，请输入：

```
msiexec /i SysMgmt.msi REINSTALL=ALL REINSTALLMODE=vomus /qn
```

升级 MSI 引擎

Dell OpenManage 软件允许您在执行交互式安装时对 MSI 引擎进行升级。对于无提示安装，必须添加适当的命令到安装脚本。

在部署脚本中使用以下命令来升级 MSI 引擎（如有需要）及安装/升级系统管理软件。

 **注：** Dell OpenManage Systems Management 和 Management Station 安装程序要求 MSI 为 3.1 或更高版本。如果使用的是运行 Windows Server® 2003（无 Service Pack）、Windows 2000 Server 或 Windows XP 操作系统的系统，则应更新 MSI 引擎。如果您使用的是运行 Windows Server 2003 SP2 或 Windows Server 2003 x64 操作系统的系统，则不必更新 MSI 引擎。

```
:retry  
start /wait msiexec /i SysMgmt.msi /qn  
if %errorlevel% == 1613 (  
REM UPGRADE THE WINDOWS INSTALLER ENGINE  
start /wait WindowsInstaller-KB893803-v2-x86.exe /quiet /norestart  
goto retry  
)  
if %errorlevel% == 1638 (  
REM THIS IS A MINOR UPGRADE  
start /wait msiexec /i SysMgmt.msi REINSTALL=ALL REINSTALLMODE=vomus/qn  
)
```

请参阅《Dell OpenManage 安装和安全性用户指南》了解在各种所支持的操作系统中的安装过程以及有关安装、升级和卸载 Server Administrator 的各步说明的信息。

开始之前

- 1 阅读《Dell 系统软件支持值表》。
- 1 阅读并遵循“[设置和管理](#)”中的相应说明。

- 1 阅读安装要求，以确保您的系统可满足或超出最低要求。
- 1 阅读《Dell OpenManage 安装和安全保护用户指南》了解在各个所支持的操作系统上安装、升级和卸载 Server Administrator 的各步说明的信息。
- 1 阅读《Server Administrator 兼容性指南》。此说明文件包含有关在运行支持的 Microsoft Windows、Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统的各种硬件平台（或系统）中安装和运行 Server Administrator 的兼容性信息。
- 1 阅读 *Dell Systems Management Tools and Documentation DVD* 上的 Dell OpenManage Install 自述文件。此文件包含有关新功能的最新信息，以及已知问题方面的信息。
- 1 阅读 *Dell Systems Management Tools and Documentation DVD* 上的 Server Administrator 自述文件。除有关已知问题的信息外，该文件还包含有关软件、固件及驱动程序版本的最新信息。
- 1 阅读操作系统的安装说明。

安装要求

以下各节介绍了 Server Administrator 的一般要求。针对操作系统的安装必备要求被列为安装过程的一部分。

支持的操作系统

请参阅 *Dell Systems Management Tools and Documentation DVD* 上的 Server Administrator 自述文件或《Dell 系统软件支持值表》，了解各受支持操作系统上支持的 Server Administrator 服务的最新列表。

支持的 Web 浏览器

请参阅 *Dell Systems Management Tools and Documentation DVD* 上的 Server Administrator 自述文件或《Dell 系统软件支持值表》，了解各受支持 Web 浏览器上支持的 Server Administrator 服务的最新详细列表。

系统要求

必须在每个需要管理的系统中均安装 Server Administrator。这样，您便可以在本地或通过支持的 Web 浏览器远程管理每个运行 Server Administrator 的系统。

Dell Systems Management Tools and Documentation DVD 上的前提条件检查程序 (**setup.exe**) 会自动分析系统以确定是否已满足系统要求。有关详情，请参阅“[Windows 的前提条件检查程序](#)”。

受管系统要求


- 1 以下其中一个“[支持的操作系统](#)”。
 - 1 至少 128 MB RAM。
 - 1 至少 256 MB 硬盘驱动器可用空间。
 - 1 管理员权限。
 - 1 监测的系统和远程系统间的 TCP/IP 连接，以便于远程系统管理。
 - 1 以下其中一个“[支持的 Web 浏览器](#)”。
 - 1 以下其中一个“[支持的系统管理协议标准](#)”。
 - 1 鼠标、键盘和显示器，用于在本地管理系统。显示器要求屏幕分辨率最低为 800 x 600。建议的屏幕分辨率设置为 1024 x 768。
 - 1 Server Administrator Remote Access Controller 要求在要管理的系统上安装 Dell Remote Access Controller (DRAC)。有关完整的软件和硬件要求，请参阅“[Remote Access Controller](#)”和“[可能需要的其他说明文件](#)”查找相应的《Dell Remote Access Controller 用户指南》。
-  **注：** 如果 managed system 满足 DRAC 的所有安装前提条件，则在通过 *Dell Systems Management Tools and Documentation DVD* 安装 managed system 软件时，DRAC 软件将作为“**Typical Setup**”（**典型安装**）和“**Custom Setup**”（**自定义安装**）安装选项的一部分进行安装。有关完整的软件和硬件要求，请参阅“[Remote Access Controller](#)”和“[可能需要的其他说明文件](#)”查找相应的《Dell Remote Access Controller 用户指南》。
- 1 默认情况下，通过使用“**Typical Setup**”（**典型安装**）将 Storage Management Service 安装在运行支持的 Windows 操作系统的系统中。
-  **注：** 在 Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 系统中，可通过 Red Hat Package Manager (RPM) 安装 Storage Management Service，或使用 `srvadmin-install.sh` 脚本—是菜单驱动脚本，它根据选择的选项安装相应的 RPM。

远程管理系统要求

- 1 使用任何一种“[支持的 Web 浏览器](#)”从 Server Administrator 主页远程管理系统。
- 1 managed system 和远程系统间的 TCP/IP 连接，以便于远程系统管理。
- 1 屏幕分辨率最低为 800 x 600。建议的屏幕分辨率设置为 1024 x 768。

支持的系统管理协议标准

安装 Server Administrator 之前，受管系统中必须已安装支持的系统管理协议标准。在支持的 Microsoft Windows 操作系统中，Server Administrator 支持两个系统管理标准：公用信息模型/Windows 管理规范 (CIM/WMI) 和简单网络管理协议 (SNMP)。在支持的 Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统中，Server Administrator 支持 SNMP 系统管理标准。

 **注：** 有关在 managed system 中安装支持的系统管理协议标准的信息，请参阅操作系统说明文件。

[表 4-1](#) 说明了每个支持的操作系统可用的系统管理标准。

表 4-1. 操作系统可用的系统管理协议

操作系统	SNMP	CIM/WMI
所支持的 Microsoft Windows 操作系统	可通过操作系统安装介质获得。	始终安装。
所支持的 Red Hat Enterprise Linux 操作系统	您必须安装随操作系统提供的 SNMP 信息包。	不可用。
SUSE Linux Enterprise Server 操作系统	您必须安装随操作系统提供的 SNMP 信息包。	不可用。

Windows 的前提条件检查程序

setup.exe 前提条件检查程序位于 *Dell Systems Management Tools and Documentation DVD* 上的 Windows 目录中，该程序无需启动实际安装程序就能够检查软件组件的前提条件状况。此程序会显示一个状况窗口，其中提供了有关某些软件组件运行所需系统硬件的信息。

前提条件检查可以使用 `runprereqcheck.exe /s` 无提示执行。

安装过程

请参阅《*Dell OpenManage 安装和安全性用户指南*》了解在各种所支持的操作系统上的安装过程以及有关安装、升级和卸载 Server Administrator 的逐步说明的信息。

结合使用 Dell OpenManage 和 Citrix XenServer Dell Edition

Dell OpenManage Server Administrator 预安装在 Citrix® XenServer Dell Edition™ 中，因此无须执行安装步骤。有关结合使用 Dell OpenManage 和 Citrix XenServer Dell Edition 的详细信息，请参阅位于 <http://support.dell.com/support/edocs/software/Citrix/> 的《Citrix XenServer Dell Edition 解决方案指南》。

结合使用 Dell OpenManage 和 Citrix Application Server

有关结合使用 Dell OpenManage 和 Citrix Application Server 的详细信息，请参阅《*Dell OpenManage 安装和安全性用户指南*》。

安装 Storage Management Service 之前的注意事项

Storage Management 与 Server Administrator 集成在一起。Dell OpenManage Storage Management 是 Array Manager 的替换产品。

如果安装 Storage Management Service 2.0，则任何以前安装的 Storage Management Service 将被卸载。

安装 Storage Management Service 时的 PERC 控制台和 FAST 兼容性问题

在装有 FAST 或 PERC 控制台的系统上安装 Storage Management 是一项不受支持的配置。特别是，您会发现如果在装有 FAST 的系统上使用 Storage Management Service，则在运行时禁用 Storage Management Service 或 FAST 功能。因此，建议您卸载 FAST 和 PERC 控制台之后再安装 Storage Management Service。

Dell OpenManage Storage Management 会取代由 FAST 和 PERC 控制台提供的所有 Storage Management 功能。此外，Storage Management Service 也有些功能是 FAST 和 PERC 控制台没有的。

安装 Storage Management Service 时的 Linux 公用程序兼容性

建议您不要在已装有 Dell 或其他厂商所提供 RAID Storage Management 公用程序的 Linux 系统上安装 Storage Management Service。您应卸载这些公用程序后再安装 Storage Management Service。Storage Management Service 会取代这些公用程序提供的 Storage Management 功能。Dell 或其他厂商提供的 Linux 公用程序示例包括：

- 1 LinFlash
- 1 DellMgr
- 1 DellMON
- 1 LINLib
- 1 MegaMgr
- 1 MegaMON

Linux 上的前提条件驱动程序和固件与 Storage Management Service

在 Linux 上，Storage Management 安装无法检测到系统上的驱动程序和固件是否处于安装和使用 Storage Management 的所需级别。在 Linux 上安装时，无论这些驱动程序和固件版本是否符合要求，您将能够完成安装。但是，如果驱动程序和固件版本不符合要求，您可能无法访问由 Storage Management 提供的全部功能。在 Storage Management Service 运行时，请检查应用程序日志文件是否有过期固件版本的通知。请参阅 Storage Management 自述文件 (readme_sm.txt) 了解支持的控制器固件和驱动程序版本的完整列表。

文件系统分层标准 v2.3 支持

文件系统分层系统 (FHS) 是大型 Linux Standards Base 定义的一部分。在此版本中，Server Administrator 支持文件的重新排列。

典型安装会将所有文件置于以下目录：`/opt/dell/srvadmin`

受影响的相应目录为：

- 1 可共享（静态）文件位于：`/opt/dell/srvadmin`
- 1 主机特定文件（用户可修改）：`/etc/opt/dell/srvadmin` 和 `/etc/opt//srvadmin`
- 1 动态（日志）文件：`/var/tmp/dell/srvadmin`、`/var/tmp//srvadmin` 和 `/var/log/dell/srvadmin /var/log//srvadmin`

有关详情，请参阅《Dell OpenManage 安装和安全性用户指南》。

[目录](#)

Instrumentation Service

Dell OpenManage Server Administrator 版本 5.5 用户指南

- [管理系统](#)
- [管理系统/服务器模块树对象](#)
- [Server Administrator 主页系统树对象](#)
- [管理首选项: 主页配置选项](#)

概览

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。还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：

- 1 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）。
- 1 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。
- 1 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。

Server Administrator 安装在系统后，[表 7-1](#)列出 GUI 字段名称和可应用的系统。

表 7-1. 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
BMC	Dell PowerEdge x8xx 和 x9xx 系统
iDRAC	Dell xx0x 系统

图 7-1. Server Administrator 主页示例 — 非模块化系统



图 7-2. Server Administrator 主页示例 — 模块化系统



注： Server Administrator 主页的每个窗口都有上下文相关联机帮助。单击全局导航栏上的“Help”（帮助）将打开单独显示的帮助窗口，其中显示当前所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。

默认情况下，访问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，您可以限制具有“用户”和“高级用户”权限用户的访问、设置 SNMP 密码及配置用户设置和安全端口服务器设置。

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—“模块化机柜”—“系统/服务器模块”—可能显示的系统组件的主类别为“主系统机箱/主系统”、“Software（软件）”和“存储时”。

如果已经安装了 Storage Management Service，则根据系统所连的控制器和存储设备，存储树对象将会展开来显示以下对象：

- | | |
|---------|-------------|
| 1 控制器 | 1 风扇 |
| 1 电池 | 1 电源设备 |
| 1 连接器 | 1 温度 |
| 1 机柜或背板 | 1 虚拟磁盘 |
| 1 物理磁盘 | 1 固件/驱动程序版本 |
| 1 EMM | |

Server Administrator 主页系统树对象

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，并且分别都是一个完整的服务器模块。

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“Modular Enclosure”（模块化机柜）对象。

属性

子选项卡：信息

在“Properties”（属性）选项卡下，您可以：

- 1 查看所监测模块化系统的机箱信息。
- 1 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 主页链接到机箱管理控制器“Log in”（登录）窗口，单击“Modular Enclosure”（模块化机柜）对象，单击“CMC Information”（CMC 信息）选项

卡，并随后单击“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。

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：“主系统机箱/主系统”、“Software（软件）”和“存储时”。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）。

 **注：** Server Administrator 2.0 或更低版本上支持更新功能。Dell™ Server Update Utility 和 Dell Update Packages 可从 Dell 支持网站 support.dell.com 下载。这些在 Microsoft Windows®、Red Hat® Enterprise Linux® 和 SUSE® Linux Enterprise Server 操作系统中受支持。


 **注：** Dell Server Update Utility 或 Dell Update Packages 必须从要更新的系统启动。


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：

- 1 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况。
- 1 查看所监测系统中所有组件的详细摘要信息。
- 1 查看和配置所监测系统的资产信息。
- 1 查看并为所监测系统设置自动系统恢复（OS 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。

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：

- 1 配置操作系统关机和远程关机选项。
- 1 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。

- 1 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 DSM SA 连接服务运行。

 **注：** DSM SA 连接服务会在重新引导后自动启动，因此每次系统启动后必须关闭 DSM SA 连接服务。

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：


- 1 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 和 x9xx 系统上，当日志文件达到 100% 的容量时，日志名旁边的状况标志图标将变为严重状况 (✗)。

 **注：** 建议在硬件日志达到 80% 的容量时清理硬件日志。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。

- 1 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》。

- 1 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。

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:

- 1 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。
- 1 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。您也可以使用"Configure Destination" (配置目标) 选项选择平台事件警报要发送到的目标。
- 1 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。

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:

- 1 查看已登录到 Server Administrator 的当前用户的会话信息。
- 1 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。

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:

- o [交流开关](#)
- o [端口](#)
- o [电池](#)
- o [电源监控](#)
- o [BIOS](#)
- o [电源设备](#)
- o [风扇](#)
- o [处理器](#)
- o [固件](#)
- o [远程访问](#)
- o [硬件性能](#)
- o [插槽](#)
- o [侵入](#)
- o [温度](#)
- o [内存](#)
- o [电压](#)
- o [网络](#)

 **注:** "AC Switch" (交流开关) 只在有限的系统上受支持。

 **注:** "Batteries" (电池) 只在 Dell PowerEdge x9xx 和 Dell xx0x 系统上受支持。

 **注:** "Hardware Performance" (硬件性能) 只在 Dell xx0x 系统上受支持。

 **注:** "Power Supplies" (电源设备) 在 Dell PowerEdge 1900 系统上不可用。

 **注:** "Power Monitoring" (电源监测) 在有限的 Dell xx0x 系统上受支持。

系统/服务器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)。

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:

- 1 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。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) 状态并需要及时处理。空白的 () 表示组件的运行状况未知。可用的被监测组件包括:

- o [交流开关](#)
- o [网络](#)
- o [电池](#)
- o [电源监控](#)

- [风扇](#)
- [电源设备](#)
- [硬件日志](#)
- [处理器](#)
- [侵入](#)
- [温度](#)
- [内存](#)
- [电压](#)

-  **注：** "AC Switch"（**交流开关**）只在有限的系统上受支持。
-  **注：** "Batteries"（**电池**）只在 Dell PowerEdge x9xx 和 Dell xx0x 系统上受支持。
-  **注：** "Power Supplies"（**电源设备**）在 Dell PowerEdge 1900 系统上不可用。
-  **注：** "Power Monitoring"（**电源监测**）在有限的 Dell xx0x 系统上受支持。

- 1 查看有关主系统机箱属性的信息。
- 1 查看有关系统中安装的现场更换用装置 (FRU) 的详细信息（在 "System Components [FRU]" [系统组件 (FRU)] 子选项卡下）。请注意，仅列出具有电子零件标识符 (PPID) 的 FRU。
- 1 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）。

交流开关

单击"AC Switch"（**交流开关**）对象使您能够显示系统交流故障转移开关的重要功能。根据用户组权限的不同，"AC Switch"（**交流开关**）对象操作窗口可包含以下选项卡："Properties"（**属性**）。

属性

子选项卡："Information"（**信息**）

在"Properties"（**属性**）选项卡下，可以查看交流开关的冗余信息以及查看有关交流电线的信息。

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**）。

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。

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**）。

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。

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。

-  **注：** 在"Setup"（**设置**）选项卡的"Device List"（**设备列表**）设置引导顺序会产生以下引导顺序：软盘、IDE CD 驱动器、硬盘、可选 ROM（如果这些设备是可用的）。

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、双网络接口控制器卡、引导顺序、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、可信平台模块 (TPM) 设置、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他 LAN 网络端口的信息。

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。

 **注意：** 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。

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）。

属性

子选项卡：“Fan Probes”（风扇探测器） | “Fan Control”（风扇控制）

在“Properties”（属性）选项卡下，您可以：

- 1 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。

- 1 选择风扇控制选项。

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：

- 1 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。
- 1 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。

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）。

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 7-2](#) 列出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]

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。

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)。

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。

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:

- 1 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。
- 1 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。


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况。内存设备预防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)。

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"冗余丢失"状态, 那么可能并不容易看出是哪个内存模块的问题。如果无法确定更换哪个 DIMM, 请参阅 ESM 系统日志中的*切换到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。

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:

- 1 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。
- 1 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。

网络

单击"Network" (网络) 对象管理系统的 NIC。Server Administrator 可以监测系统中每个 NIC 的状况, 以保持持续的远程连接。根据用户组权限的不同, "Network" (网络) 对象操作窗口可具有以下选项卡: "Properties" (属性)。

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中安装的 NIC 的信息。

端口

单击"Ports" (端口) 对象可以管理系统的外部端口。Server Administrator 可以监测系统中所有外部端口的状况。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)。

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。

电源监控

单击"Power Monitoring" (电源监测) 对象管理系统的电源消耗。Server Administrator 监测电源消耗状况、安培数并跟踪电源统计详情。根据用户组权限的不同, "Power Monitoring" (电源监控) 对象操作窗口可包含以下选项卡: "Properties" (属性) 和"Alert Management" (警报管理)。

属性

子选项卡: "Power Consumption" (电源消耗)

在"Properties" (属性) 选项卡下, 您可以:

- 1 查看有关系统电源消耗属性的信息。
- 1 查看有关当前组件属性的信息。
- 1 查看有关能耗的跟踪统计数据并记录系统峰值功率

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:

- 1 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。
- 1 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。

电源设备

单击"Power Supplies" (电源设备) 对象管理电源设备。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)。

属性

子选项卡: "Elements" (要素)

在"Properties" (属性) 选项卡下, 您可以:

- 1 查看有关电源设备冗余属性的信息。
- 1 检查单个电源设备要素的状况。

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:

- 1 查看当前警报措施设置, 并设置电源设备返回警告或故障值时您希望系统执行的警报措施。
- 1 查看当前 SNMP 陷阱警报阈值并为电源设备设置警报阈值级别。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。

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)。

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。

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:


- 1 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。
- 1 查看当前 SNMP 陷阱警报阈值并为处理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。

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。

如果选择 BMC/iDRAC, 则可管理 BMC/iDRAC 功能, 比如, BMC/iDRAC 上的常规信息。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 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。

如果选择 DRAC, 则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）。

属性

子选项卡：“Information”（信息）

在“Properties”（属性）选项卡下，您可以查看常规 BMC/iDRAC 或 DRAC 信息。单击“Reset to Defaults”（重置为默认值）可以将所有属性重置为系统默认值。


配置

子选项卡：LAN | “Serial Port”（串行端口） | “Serial Over LAN”（LAN 上串行）

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。

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


- 1 配置网络属性
- 1 配置 SNMP 陷阱
- 1 配置请求拨出条目
- 1 配置拨入用户
- 1 配置远程引导参数一类的远程属性
- 1 配置调制解调器属性

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

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 Service 用户的信息。

 **注：** 在 Dell PowerEdge x9xx 系统上：

- 1 显示十个用户 ID。如果装有 DRAC 卡，则显示十六个用户 ID。
- 1 显示 LAN 上串行有效载荷列。

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）的连接器和插孔。“Slots”（插槽）对象措施窗口具有“Properties”（属性）选项卡。

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。


温度

单击“Temperatures”（温度）对象，则可以管理系统温度，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）对象操作窗口可包含以下选项卡：“Properties”（属性）和“Alert Management”（警报管理）。

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。

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：

- 1 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时您希望系统执行的警报措施。
- 1 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：** 用户可以将外部机箱的最小和最大温度探测器阈值仅设置为整数。如果用户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，则仅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)。

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。

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：

- 1 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。
- 1 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)。

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。

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)。

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。

存储时

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)。

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。

Storage Management Service

如果是 Storage Management Service，单击“**Storage**” (存储) 对象可以查看系统上所连被支持控制器的状态和设置。控制器对象会展开来显示控制器所连的存储设备。

根据系统所连的控制器和存储设备，展开的“**Storage**” (存储) 对象可能会显示以下较低级别对象：

1 控制器

1 风扇


1 电池	1 电源设备
1 连接器	1 温度
1 机柜或背板	1 虚拟磁盘
1 物理磁盘	1 固件/驱动程序版本
1 EMM	

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）。

属性

子选项卡：“Health”（运行状况）

在“Properties”（属性）选项卡的“Health”（运行状况）窗口中，可以查看存储控制板信息。存储控制板列出系统上所有的控制器。可以使用“Available Tasks”（可用任务）下拉菜单配置控制器。在存储控制板页中，还可以查看虚拟磁盘详情和控制器的运行状况。

 **注：** 必须作为管理员登录才能执行存储控制板中的“Available Tasks”（可用任务）。

子选项卡：“Information/Configuration”（信息/配置）

在“Properties”（属性）选项卡的“Information/Configuration”（信息/配置）窗口中，您可以查看系统所选控制器的属性。您也可以执行适用于所有控制器的全局任务。

控制器

单击“Controller”（控制器）对象可以查看关于控制器及控制器上所述各种组件的信息。控制器上所连组件可以包括电池、虚拟磁盘等。根据用户组权限的不同，“Controller”（控制器）对象操作窗口可包含以下选项卡：“Health”（运行状况）和“Information/Configuration”（信息/配置）。

运行状况

在“Health”（运行状况）选项卡下，您可以查看电池、虚拟磁盘及控制器所连其他存储组件的当前状态。该状态会用“[存储组件严重性](#)”中所述的图标标出来。

信息/配置

在“Information/Configuration”（信息/配置）选项卡下，您可以查看控制器及控制器所连组件的属性信息。您也可以执行此选项卡中的控制器任务。

连接器

单击“Connector”（连接器）对象可以查看关于连接器及连接器所连机柜或背板的信息。根据用户组权限的不同，“Connector”（连接器）对象操作窗口可包含以下选项卡：“Health”（运行状况）和“Information/Configuration”（信息/配置）。

运行状况

在“Health”（运行状况）选项卡下，您可以查看连接器及连接器所连机柜或背板的当前状态。该状态会用“[存储组件严重性](#)”中所述的图标标出来。

配置/信息

在“Configuration/Information”（配置/信息）选项卡下，您可以查看连接器及连接器所连机柜或背板的属性信息。您也可以执行此选项卡中的连接器任务。

机柜或背板

单击“Enclosure or Backplane”（机柜或背板）对象可以查看有关物理磁盘、温度探测器以及机柜或背板上所连接的其他组件的信息。根据用户组权限的不同，“Enclosure or Backplane”（机柜或背板）对象操作窗口可包含以下选项卡：“Health”（运行状况）和“Configuration/Information”（配置/信息）。

运行状况

在“Health”（运行状况）选项卡下，可以查看物理磁盘及机柜或背板所连接的其他组件的当前状态。例如，机柜的风扇、电源、温度探测器等设备的状态会显示在这个选项卡中。背板所连接的物理磁盘的状态也会显示在此处。该状态会用“[存储组件严重性](#)”中所述的图标标出来。

配置/信息

在“Configuration/Information”（配置/信息）选项卡下，可以查看物理磁盘、温度探测器、EMM（机柜管理模块）及机柜或背板上所连接的其他组件的属性信息。对于机柜，也可以执行此选项卡中的机柜任务。

物理磁盘

单击“Physical Disks”（物理磁盘）对象可以查看关于机柜或背板所连接的物理磁盘的信息。根据用户组权限的不同，“Physical Disks”（物理磁盘）对象操作窗口可包含以下选项卡：“Configuration/Information”（配置/信息）。

配置/信息

在"Configuration/Information" (**配置/信息**) 选项卡下, 可以查看机柜或背板所连接的物理磁盘的当前状态和属性信息。该状态会用[存储组件严重性](#)中所述的图标标出来。属性信息包括名称、状态、容量、已用和可用磁盘空间及其他信息。也可以执行此选项卡中的物理磁盘任务。

EMM

单击 EMM 对象可以查看有关机柜管理模块 (EMM) 的信息。根据用户组权限的不同, EMM 对象操作窗口可包含以下选项卡: "Configuration/Information" (**配置/信息**)。

配置/信息

在"Configuration/Information" (**配置/信息**) 选项卡下, 您可以查看 EMM 的当前状态和属性信息。该状态会用[存储组件严重性](#)中所述的图标标出来。

属性信息包括名称、状态、部件号、固件版本及 SCSI 速率。

风扇

单击"Fans" (**风扇**) 对象查看关于机柜风扇的信息。根据用户组权限的不同, **风扇**对象操作窗口可包含以下选项卡: "Configuration/Information" (**配置/信息**)。

配置/信息

在"Configuration/Information" (**配置/信息**) 选项卡下, 您可以查看风扇的当前状态和属性信息。该状态会用[存储组件严重性](#)中所述的图标标出来。

属性信息包括风扇名称、状态、部件号和速度。

电源设备

单击"Power Supplies" (**电源设备**) 对象可以查看关于机柜电源的信息。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: "Configuration/Information" (**配置/信息**)。

配置/信息

在"Configuration/Information" (**配置/信息**) 选项卡下, 您可以查看机柜电源设备的当前状态和属性信息。该状态会用[存储组件严重性](#)中所述的图标标出来。

属性信息包括名称、状态和部件号。

温度

单击"Temperatures" (**温度**) 对象可以查看关于机柜温度探测器的信息。根据用户组权限的不同, **温度**对象操作窗口可包含以下选项卡: "Configuration/Information" (**配置/信息**)。

配置/信息

在"Configuration/Information" (**配置/信息**) 选项卡下, 您可以查看机柜温度探测器的当前状态和属性信息。该状态会用[存储组件严重性](#)中所述的图标标出来。

属性信息包括名称、状态和读数 (当前温度)。温度探测器"Warning" (**警告**) 和"Failure" (**故障**) 阈值的最小和最大值设置也会在这个选项卡下面显示。

虚拟磁盘

单击"Virtual Disks" (**虚拟磁盘**) 对象可以查看关于控制器上所配置虚拟磁盘的信息。根据用户组权限的不同, "Virtual Disks" (**虚拟磁盘**) 对象操作窗口可包含以下选项卡: "Configuration/Information" (**配置/信息**)。

配置/信息

在"Configuration/Information" (**配置/信息**) 选项卡下, 您可以查看关于控制器上所配置虚拟磁盘的属性信息。属性信息包括名称、状态和布局 (RAID 级别)。读取、写入和高速缓存策略及条带大小也会被显示。您也可以执行此选项卡中的虚拟磁盘任务。

固件/驱动程序版本

单击"Firmware/Driver Version" (**固件/驱动程序版本**) 对象可以查看有关控制器上当前安装的驱动程序和固件版本的信息。固件和驱动程序属性可根据控制器的型号而有所不同。

固件和驱动程序属性可包括:

- 1 固件版本
- 1 所需的最低固件版本
- 1 驱动程序版本
- 1 所需的最低驱动程序版本

存储组件严重性




一个组件的状态被评定为不同严重程度。每个严重程度要求您采取不同的响应。例如，您必须立即采取修复措施响应“Warning”（警告）或“Critical/Failure”（严重/故障）状态以避免任何数据损失。

查看一下说明组件为何出现“Warning”（警告）或“Critical”（严重）状态的事件警报日志可能会有用。有关更多的故障排除信息，请参阅 Storage Management 联机帮助。

 **注：** 显示的状态反映浏览器第一次显示该页时的状态。如果您认为状态已更改并且想要更新显示的信息，请单击措施窗口右上角的“Refresh”（刷新）按钮。有些存储配置更改只有当您执行控制器**重新扫描**后才能被检测到；单击所需控制器内的“Information/Configuration”（信息/配置）选项卡，然后单击“Rescan”（重新扫描）。

表 7-3 介绍不同的严重性级别及相应的组件状态。

表 7-3. 严重性级别和组件状态


严重性级别	组件状况
	Normal/OK（正常/良好）。组件工作正常。
	Noncritical/Warning（不严重/警告）。探测器或其他监视设备检测到组件的读数超出或低于可接受的范围。组件仍然可以工作，但可能会发生故障。组件也可能是在故障的状态下工作。数据可能会丢失。
	Critical/Failure/Error（严重/故障/错误）。组件已经发生故障，或故障就要发生。组件需要立即采取措施，可能需要更换它。数据可能已经丢失。

设置存储事件警报

可以使用 Server Administrator Instrumentation Service 配置最常用的存储功能，比如“Storage Event”（存储事件）警报操作参数。


1. 单击“System”（系统）对象。
2. 单击“Alert Management”（警报管理）选项卡。
3. 单击“Alert Action”（警报操作）。
4. 单击“Storage Event”（存储事件）。

“Storage Event”（存储事件）窗口允许对特定存储事件分别采取操作。

 **注：** 必须以“管理员”权限登录才能配置“Storage Event Alerts”（存储事件警报）。

您可以配置以下存储事件。

1 存储系统警告	1 虚拟磁盘警告
1 存储系统故障	1 虚拟磁盘故障
1 存储控制器警告	1 机柜警告
1 存储控制器故障	1 机柜故障
1 物理磁盘警告	1 存储控制器电池警告
1 物理磁盘故障	1 存储控制器电池故障

 **注：** “Storage Controller Battery Warning”（存储控制器电池警告）和“Storage Controller Battery Failure”（存储控制器电池故障）事件在模块化系统上不可用。

5. 选择存储事件为其针对所选操作生成警报。
6. 单击“Apply Changes”（应用更改）。
7. 单击“Go Back to Alert Action Page”（返回警告操作页）返回“Alert Action Information”（警告操作信息）窗口。

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。

请参阅 [表 7-4](#) 了解可用的首选项主页配置选项。

表 7-4. 首选项主页配置选项

	*****	常规设置
	*****	Server Administrator

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**。

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：

- 1 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。
- 1 执行 X.509 认证管理的方式有：生成新的 X.509 认证，重新使用现有的 X.509 认证，或导入证书颁发机构 (CA) 颁发的根目录认证或认证链。有关证书管理的详细信息，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：

- 1 启用或禁用具有“用户”或“高级用户”权限的那些用户的访问。
- 1 配置 SNMP root 密码。

 **注：** 默认的 SNMP 配置用户是 root 且密码是 calvin。

- 1 配置 SNMP Set 操作。

 **注：** 配置 SNMP Set 操作后，必须重启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。

[目录](#)

[目录](#)


简介

Dell OpenManage Server Administrator 版本 5.5 用户指南

- [概览](#)
- [集成功能](#)
- [可能需要的其他说明文件](#)
- [获得技术帮助](#)

概览

Server Administrator 通过两种方式提供了全面的、一对一的系统管理解决方案：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、一对一的系统管理，Server Administrator 使系统管理员可以专注于管理整个网络。

 **注：** 对于 Server Administrator 来说，系统可以是一个独立的系统，一个连接有独立机箱中网络存储单元的系统，或者是一个在机箱中包含一个或多个服务器模块的模块化系统。

Server Administrator 可以提供以下信息：

- 1 正常运行的系统和出现故障的系统
- 1 需要执行远程恢复操作的系统


 **注：** 要进行远程恢复，必须安装 Dell™ Remote Access Controller。


集成功能

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)、验证和行业标准安全套接字层 (SSL) 加密技术来确保其管理连接的安全。

安装

可以使用多种方式来安装 Server Administrator。Dell® Systems Management Tools and Documentation DVD 提供了安装程序，用于在 managed system 上安装、升级和卸载 Server Administrator 和其它 managed system 软件组件。该 DVD 还提供了安装程序在 management station 上安装、升级和卸载 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。

 **注：** 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。

 **注：** 有关无人值守 Server Administrator 安装/卸载的详情，请参阅《Dell OpenManage™ 安装和安全性用户指南》。

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，用于识别并应用对服务器的更新。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。


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。

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系统进行远程管理（包括关闭系统、启动和安全保护）。

Remote Access Controller

 **注：** Remote Access Controller 在模块化系统上不可用。可直接连接至模块化机箱上的 Dell Embedded Remote Access/Modular Chassis Controller (ERA/MC)。有关详情，请参阅《Dell Embedded Remote Access/MC 用户指南》。

Remote Access Controller 为装有 Dell Remote Access Controller (DRAC) 解决方案的系统提供了一个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。

Storage Management Service

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


Server Administrator 的 Storage Management Service:


- 1 可以让您查看被监视系统上所连本地和远程存储设备的状态
- 1 支持 SCSI、SATA、ATA 和 SAS。不支持光纤信道。
- 1 可以让您通过一个图形或命令行界面为所有支持的 RAID 和非 RAID 控制器和机柜执行控制器和机柜功能，而不必使用控制器 BIOS 公用程序。
- 1 通过配置数据冗余、分配热备份或重建故障驱动器来保护数据
- 1 提供了用于配置存储器的功能。


在支持的 Microsoft® Windows® 操作系统中，使用“Typical Setup”（典型安装）安装 Storage Management。

在运行支持的 Red Hat® Enterprise Linux® 和 SUSE® Linux Enterprise Server 操作系统的系统中，可以通过 Red Hat Package Manager (RPM) 安装 Storage Management Service，或使用 `srvadmin-install.sh` 脚本安装它。该脚本是菜单驱动脚本，它根据选择的选项安装相应的 RPM。

有关 Storage Management Service 的详细信息，请参阅 Storage Management 联机帮助和《Dell OpenManage Server Administrator Storage Management 用户指南》。要了解如何启动联机帮助，请参阅“[显示联机帮助](#)”。

 **注意：** Dell OpenManage Array Manager 不再受支持。如果升级装有 Array Manager 的系统（装有 Dell OpenManage 4.3 或更高版本），Array Manager 会在升级过程中删除。可使用 Storage Management 来代替。

 **注：** 安装 Storage Management 会取代系统上驻留的任何先前安装的 Array Manager managed system（服务器软件）和控制台（客户机软件）。如果系统上只安装了 Array Manager 控制台，则安装 Storage Management 不会取代 Array Manager 控制台。

 **注：** 只有当检测到先前的 Dell OpenManage Management Station 软件（装有 Array Manager 控制台），Dell OpenManage Array Manager 控制台（对于 Management Station）在 Windows 上才可用。它只可用于升级。

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。

可能需要的其他说明文件

除**用户指南**外，还可以在 [Dell 支持网站 support.dell.com](http://support.dell.com) 或 *Dell Systems Management Tools and Documentation DVD* 上找到以下指南：

- 1 《Dell 系统软件支持值表》介绍了各种 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。
- 1 《Dell OpenManage 安装和安全性用户指南》提供了在各种支持的操作系统中的安装过程以及有关安装、升级和卸载 Server Administrator 逐步说明的完整信息。
- 1 《Dell OpenManage 软件快速安装指南》概述了可以安装在 management station（控制台）和 managed system 上的应用程序，并介绍了在运行支持的操作系统上的安装控制台和 managed system 应用程序的步骤。
- 1 《Dell OpenManage Server Administrator 兼容性指南》提供了有关在运行所支持 Microsoft Windows、Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统的各种硬件平台（或系统）上安装和操作 Server Administrator 的兼容性信息。
- 1 《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。
- 1 《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 文档介绍了管理对象支持的类。
- 1 《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。
- 1 《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。
- 1 《Dell Integrated Remote Access Controller 用户指南》提供了有关配置和使用 iDRAC 的详细信息。
- 1 《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。
- 1 《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。
- 1 《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。
- 1 《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。
- 1 《Dell Remote Access Controller 安装和设置指南》提供了有关安装和配置 DRAC III、DRAC III/XT 和 ERA/O 控制器、配置 ERA 控制器和使用 RAC 远程访问未运行系统的完整信息。
- 1 《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。
- 1 《Dell Remote Access Controller 4 用户指南》提供了有关安装和配置 DRAC 4 以及使用 DRAC 4 远程访问不运行系统的完整信息。
- 1 《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。
- 1 《Dell Embedded Remote Access/MC Controller 用户指南》，提供了有关配置和使用 ERA/MC 控制器来通过网络远程管理和监测模块化系统及其共享资源的完整信息。

- 1 《Dell OpenManage 远程安装用户指南》，提供了有关利用基于映像的技术实现无人值守的并发支持和配置解决方案的信息。
- 1 《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。
- 1 《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 Systems Management Tools and Documentation DVD 包含了 Server Administrator 的自述文件及其上的大部分其它应用程序。

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更多信息，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 www.dell.com/training。此服务并非在所有国家和地区提供。

[目录](#)

[目录](#)

Server Administrator 日志

Dell OpenManage Server Administrator 版本 5.5 用户指南

- [概览](#)
- [集成功能](#)
- [Server Administrator 日志](#)

概览

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

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，您可以单击全局导航栏上的“**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

单击列标题可以按列进行排序或更改列的排序顺序。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

- 1 单击“Print”（打印）可将一份日志打印至默认打印机。
- 1 单击“Export”（导出）将包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。
- 1 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。
- 1 单击“Clear Log”（清除日志）可删除日志中的所有事件。
- 1 单击“Save As”（另存为）可将日志内容保存在 .zip 文件中。
- 1 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：

- 1 [“硬件日志”](#)
- 1 [“警报日志”](#)
- 1 [“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 和 x9xx 系统上，系统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 X (❌)。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。

要查看硬件日志，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：


- 1 事件的严重性级别
- 1 捕获事件的日期和时间
- 1 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态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：

- 1 事件的严重性级别
- 1 事件 ID
- 1 捕获事件的日期和时间
- 1 事件的类别
- 1 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：

- 1 调用命令的日期和时间
- 1 当前登录至 Server Administrator 主页或 CLI 的用户
- 1 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。

[目录](#)

使用底板管理控制器/Integrated Dell Remote Access Controller

Dell OpenManage Server Administrator 版本 5.5 用户指南

- [概览](#)
- [查看基本 BMC 信息](#)
- [配置 BMC/iDRAC 用户](#)
- [设置 BMC 平台事件筛选器警报](#)
- [配置 BMC/iDRAC 使用 LAN 上串行 \(SOL\) 连接](#)
- [配置 BMC 使用串行端口连接](#)
- [配置 BMC/iDRAC 使用 LAN 连接](#)
- [访问和使用 Integrated Dell Remote Access Controller](#)

 **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) 只在 Dell xx0x 系统中受支持。

概览

Dell 系统底板管理控制器 (BMC)/Integrated Dell Remote Access Controller (iDRAC) 通过与系统板上不同传感器进行通信，并在某些参数超出其预设阈值时发送警报和日志事件来监测发生严重事件的系统。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。

Server Administrator 安装在系统后，表 8-1 列出 GUI 字段名称和可应用的系统。

表 8-1. 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
BMC	Dell PowerEdge x8xx 和 x9xx 系统
iDRAC	Dell xx0x 系统


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。您可以执行以下 BMC 相关任务：

- 1 查看基本 BMC/iDRAC 信息
- 1 配置 BMC/iDRAC 用户
- 1 设置 BMC/iDRAC 平台事件筛选器警报
- 1 在 LAN 上串行连接上配置 BMC/iDRAC
- 1 在串行端口连接上配置 BMC
- 1 在虚拟 LAN 连接上配置 BMC

不过，在 Dell PowerEdge x8xx 和 x9xx 系统中，BMC 和 RAC 会组合成一个称为 Remote Access ("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) 的对象。可根据哪个硬件提供了对系统的远程访问功能来查看 BMC 或 RAC 信息。在 Dell xx0x 系统中，RAC 只是一个逻辑实体，因此不能与 iDRAC 组合。

也可以使用 `omconfig chassis remoteaccess` CLI 命令管理 BMC/iDRAC 和 DRAC 的报告和配置。


另外，您可以使用 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。其他系统只允许您安装和卸载 BMC。在 Dell PowerEdge x6xx 和 x7xx 系统上使用 BMC 或 ESM，只能提供有限的传感器数据。

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。

查看基本 BMC 信息

您可以查看 BMC 的基本信息，也可以将 BMC 设置重设为默认值。

 **注：** 您必须以“管理员”权限登录才能重置 BMC 设置。

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。

Remote Access 页显示以下系统 BMC 的基本信息:

1	BMC 名称/iDRAC 名称	1	SOL 已启用
1	IPMI 版本	1	IP 地址源
1	系统 GUID	1	IP 地址
1	可能激活的会话数	1	IP 子网
1	目前激活的会话数	1	IP 网关
1	LAN 上 IPMI 已启用	1	MAC 地址

配置 BMC/iDRAC 用户

BMC/iDRAC 用户可以通过 Remote Access 页进行配置, 通过浏览以下路径可以访问到该页。

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:


- 1 选择"Enable User" (启用用户) 以启用该用户。
- 1 在"User Name" (用户名) 字段中输入用户的名称。
- 1 选择"Change Password" (更改密码) 复选框。
- 1 在"New Password" (新密码) 字段中键入新密码。
- 1 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:

- 1 选择最大 LAN 用户权限级别限制。
- 1 选择准予的最大串行端口用户权限。
- 1 在 Dell PowerEdge x9xx 系统中, 选择"Enable Serial Over LAN" (启用 LAN 上串行) 启动 LAN 上串行。

6. 单击"Apply Changes" (应用更改) 以保存更改。

7. 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 RAC 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 5 时, 所有 16 个用户项将分配给 RAC。

设置 BMC 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。

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 平台事件筛选器警报。

您可以配置以下平台事件：

1 风扇探测器故障	1 处理器不存在
1 电压探测器故障	1 处理器警告
1 分离电压探测器故障	1 处理器故障
1 温度探测器警告	1 PS/VRM/DcToDc 警告
1 温度探测器故障	1 PS/VRM/DcToDc 故障
1 检测到机箱侵入	1 硬件日志故障
1 已降级冗余	1 自动系统恢复
1 冗余掉失	1 电池探测器警告
1 系统电源探测器警告	1 电池探测器故障
1 系统电源探测器故障	1 电源不存在

 **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平台事件筛选器警报生成。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 OMSA 允许您配置。

 **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：

- 1 **无**
操作系统挂起或崩溃时不采取任何措施。
- 1 **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。
- 1 **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。
- 1 **关闭系统**
关闭系统的电源。
- 1 **性能降低**
降低系统的性能。

如果选择平台事件关机操作而不是**无操作或性能降低**，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。

配置 BMC/iDRAC 使用 LAN 上串行 (SOL) 连接

您可以在 LAN 上串行 (SOL) 连接配置 BMC/iDRAC 以用于通信。

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"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：
 - 1 启用 LAN 上串行
 - 1 波特率
 - 1 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，可指定以下信息：
 - 1 字符积累间隔时间
 - 1 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。

配置 BMC 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。

1. 单击"System"（系统）→ "Main System Chassis"（主系统机箱）→ Remote Access 对象。
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：
 - 1 连接模式设置
 - 1 波特率
 - 1 数据流控制

- 1 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:
 - 1 行编辑
 - 1 删除控制
 - 1 回声控制
 - 1 符号交换控制
 - 1 新行序列
 - 1 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 BMC/iDRAC 使用 LAN 连接

 **注:** LAN 配置字段如果对带内用户配置为"disabled" (已禁用), 则会显示为只读。

您可以在 LAN 连接上配置 BMC/iDRAC 以用于通信。

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) 配有网络适配器添加式插卡, 则 BMC/iDRAC 管理通信将不会正常工作。

4. 指定以下 NIC 配置详情:
 - 1 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, 可对网卡分组以增加冗余。)
 - 1 NIC 选择

 **注:** "Enable NIC" (启用 NIC) 和"NIC Selection" (NIC 选择) 不能在装有 iDRAC 的系统上配置。

1 MAC 地址	1 子网掩码
1 启用 LAN 上 IPMI	1 网关地址
1 IP 地址源	1 信道权限级别限制
1 IP 地址	1 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

- 1 启用 VLAN ID
- 1 VLAN ID
- 1 优先权

- 1 单击"Apply Changes" (应用更改)。

访问和使用 Integrated Dell Remote Access Controller

要从 Server Administrator 主页链接到 Remote Access Controller iDRAC "Log in" (登录) 窗口, 请依次单击"Main System Chassis/Main System" (主系统机箱/主系统) 对象、"Remote Access Controller" (远程访问控制器) 对象、"Remote Connect" (远程连接) 选项卡和"Launch the iDRAC Web Interface" (启动 iDRAC Web 界面)。系统将显示 iDRAC "Log in" (登录) 窗口。

连接到 iDRAC 后就可以监测并管理系统, 包括访问系统和会话信息、管理 iDRAC 配置和在 managed system 上执行远程访问功能。

[目录](#)

Remote Access Controller

Dell OpenManage Server Administrator 版本 5.5 用户指南

- [概览](#)
- [硬件前提条件](#)
- [软件前提条件](#)
- [添加和配置 DRAC 用户](#)
- [配置现有 DRAC 用户](#)
- [配置 DRAC 网络属性](#)
- [配置 DRAC 警报属性](#)
- [配置 DRAC III 拨入 \(PPP\) 用户和调制解调器设置](#)
- [配置 DRAC 远程功能属性](#)
- [配置 DRAC 安全](#)
- [访问和使用 Dell Remote Access Controller](#)

概览

Server Administrator Remote Access Controller 为配备了 Dell™ Remote Access Card (DRAC) III、DRAC III/XT、Embedded Remote Access(ERA) 控制器或 ERA Option (ERA/O) 卡的 SNMP 和 CIM 工具系统提供了一种全面的远程系统管理解决方案。这些硬件和软件解决方案统称为 Dell Remote Access Controller (DRAC)。DRAC 4 和 DRAC 5 还允许从 Dell OpenManage® Server Administrator 执行基本的管理任务；根据已安装的 DRAC 卡，可从 Server Administrator 图形用户界面连接至 DRAC 4 或 DRAC 5。

DRAC 4 和 DRAC 5 是一个专为 Dell 系统提供远程管理功能、崩溃系统恢复和电源控制功能而设计的系统管理硬件和软件解决方案。

通过与系统的底板管理控制器 (BMC) Integrated Dell Remote Access Card (iDRAC) 通信，可以配置 DRAC 4 和 DRAC 5 发送电压、温度和风扇速度相关警告或错误的电子邮件警报。DRAC 4 和 DRAC 5 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。

- 📌 **注：** BMC 在 Dell PowerEdge™ x8xx 和 x9xx 系统中受支持，而 iDRAC 只在 Dell xx0x 系统中受支持。
- 📌 **注：** LAN 配置字段如果对带内用户配置为“disabled”（已禁用），则会显示为只读。

根据您的系统，DRAC 4 硬件是一个系统卡 (DRAC 4/I) 或一个较短的 PCI 卡 (DRAC 4/P)。除硬件差异之外，DRAC 4/I 和 DRAC 4/P 都是相同的。

DRAC 5 硬件是一个嵌入式的系统卡。

DRAC 4 和 DRAC 5 有它们各自的微处理器和内存，并且由它们所在的系统提供电源。DRAC 4 和 DRAC 5 可以预安装在系统中，也可以在套件中单独提供。

- 📌 **注：** 这一部分中包含的信息适用于以前的几代 DRAC。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。

Remote Access Controller 使您可以通过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。

请参阅《Dell OpenManage Server Administrator 命令行界面用户指南》和《Dell Remote Access Controller Racadm 用户指南》，了解有关从命令行运行 Remote Access Controller (DRAC III) 的详细信息。

使用 Remote Access Controller 时，单击全局导航栏上的“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。

- ➡ **注意：** 当 DRAC 5 卡在重新设置或执行固件更新时，切勿使用 Server Administrator 在远程或在本地查询或配置它。在重设期间，DRAC 5 卡将脱机一小段时间。在重设期间拆卸 DRAC 5 卡可能导致图形用户界面或命令行界面 (CLI) 中显示的数据出现故障。
- 📌 **注：** Remote Access Controller 在模块化系统上不可用。您必须直接连接到模块化系统的 DRAC 上。请参阅《Dell Embedded Remote Access/MC 控制器用户指南》以了解详细信息。
- 📌 **注：** 有关安装和配置 DRAC III、DRAC III/XT、ERA 或 ERA/O 控制器和使用 DRAC 远程访问未运行系统的完整信息，请参阅《Dell Remote Access Controller 安装和设置指南》。请参阅《Dell Embedded Remote Access/MC 控制器用户指南》，了解有关配置和使用 ERA/MC 控制器来通过网络远程管理和监测模块化系统及其共享资源的完整信息。

Server Administrator 安装在系统后，[表 6-1](#) 列出 GUI 字段名称和可应用的系统。


表 6-1. 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
BMC	Dell PowerEdge x8xx 和 x9xx 系统
iDRAC	Dell xx0x 系统

硬件前提条件


要使用 Remote Access Controller，则必须在受管系统上安装 DRAC。

有关 DRAC 的具体硬件要求列表，请参阅 *Dell Systems Management Tools and Documentation DVD* 上的 Remote Access Controller 自述文件和《*Dell Remote Access Controller 安装和设置指南*》或《*Dell Embedded Remote Access/MC 控制器用户指南*》。

 **注：** 如果 Managed System 满足 DRAC 的所有安装前提条件，则在通过 *Dell Systems Management Tools and Documentation DVD* 安装 Managed System 软件时，DRAC 软件将作为“Typical Setup”（典型安装）和“Custom Setup”（自定义安装）安装选项的一部分进行安装。请参阅相应的 DRAC 说明文件，以了解有关软件和硬件要求的完整信息。

软件前提条件

managed system 必须安装 DRAC 软件。请参阅《*Dell Remote Access Controller 安装和设置指南*》或《*Dell Embedded Remote Access/MC 控制器用户指南*》以了解关于软件安装前提条件的详细信息。

 **注：** 如果 Managed System 满足 DRAC 的所有安装前提条件，则在通过 *Dell Systems Management Tools and Documentation DVD* 安装 Managed System 软件时，DRAC 软件将作为“Typical Setup”（典型安装）和“Custom Setup”（自定义安装）安装选项的一部分进行安装。请参阅相应的 DRAC 说明文件，以了解有关软件和硬件要求的完整信息。

添加和配置 DRAC 用户

 **注：** 要使用 Remote Access Controller，您必须在 Server Administrator 中具有“管理员”权限。

DRAC 最多可存储 16 个用户的信息。Remote Access Controller 通过要求用户在建立远程连接之前提供用户名和密码来提供安全保护。Remote Access Controller 还可以提供寻呼服务，以在系统崩溃、断电或遇到一系列已定义的其他事件时通知用户。仅 DRAC III 卡可使用寻呼服务。

 **注：** 某些配置功能只在装有 DRAC III、DRAC III/XT、ERA 和 ERA/O 的系统上提供，而不在装有 DRAC 4 或 DRAC 5 的系统上提供。要配置 DRAC 4 或 DRAC 5，使用“Launch the Remote Connect Interface”（启用远程连接界面）并且对于 iDRAC 使用“RAC Properties”（RAC 属性）窗口中的“Launch the iDRAC Interface”（启动 iDRAC 界面）选项。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。

要创建 DRAC 用户，请执行以下步骤：

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” 并随后单击“Users”（用户）选项卡。

系统将显示“Remote Access Users”（Remote Access 用户）窗口。

2. 单击 Add（添加）。

系统将显示“Add Remote Access User”（添加 Remote Access 用户）窗口。

3. 在“User Name”（用户名）字段中键入用户名。

4. 在“New Password”（新密码）字段中键入新密码。

5. 在“Confirm Password”（确认密码）字段中再次键入新密码。

6. 配置数字寻呼（仅限于 DRAC III 用户）：

- a. 单击“Enable Numeric Paging”（启用数字寻呼）旁边的复选框，并在“Pager Number”（寻呼机号码）字段中输入寻呼机号码。
- b. 在“Numeric Message”（数字信息）字段中，输入 DRAC 接收到某些事件时向您发送的数字信息。

7. 配置电子邮件寻呼：

- a. 单击“Enable Email Paging”（启用电子邮件寻呼）旁边的复选框，并在“Email Address”（电子邮件地址）字段中输入电子邮件地址。
- b. 在“Message”（信息）字段中，输入 DRAC 接收到某些事件时向您发送的信息。

8. 配置字母数字寻呼（仅限于 DRAC III 用户）：

- a. 单击“Enable Alpha-Numeric Paging”（启用字母数字寻呼）旁边的复选框，并在“Pager Number”（寻呼机号码）字段中输入寻呼机号码。
- b. 选择寻呼机的服务供应商使用的字母数字协议：7EO 或 8N1。
- c. 选择寻呼机的波特率：300 或 1200。
- d. 在“Custom Message”（自定义信息）字段中，输入 DRAC 接收到某些事件时向您发送的信息。
- e. 在“Pager ID”（寻呼机 ID）字段中，输入寻呼机的 PIN，然后必要时在“Pager Password”（寻呼机密码）字段中输入寻呼机密码。

f. 单击窗口底部的“Apply Changes”（应用更改）。

9. 在“Severity Configuration”（严重性配置）下，指定陷阱以及陷阱必须从 DRAC 触发寻呼操作的严重性。


陷阱使您能够将 DRAC 配置为响应来自系统的 ESM 硬件的警报状况或响应其他状况，例如操作系统崩溃或出现电源故障。

复选框的第一（最左侧的）列对应严重性级别“Informational”（通知），第二列对应严重性级别“Warning”（警告），第三列对应严重性级别“Critical”（严重）。最后七个事件只能报告严重性级别“Informational”（通知）。

10. 单击“Apply Changes”（应用更改），然后单击“OK”（确定），以将警报、寻呼和用户配置保存到 Server Administrator 数据资源库。

Server Administrator 将返回到“Users”（用户）选项卡。您刚刚创建和配置的用户将显示在“User Name”（用户名）列表中。

配置现有 DRAC 用户

 **注：** 要使用 Remote Access Controller，您必须在 Server Administrator 中具有“管理员”权限。

要配置现有的 DRAC 用户，请执行以下步骤：

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 并随后单击“Users”（用户）选项卡。

系统将显示“Remote Access Users”（Remote Access 用户）窗口。

2. 单击您要配置的用户的用户名。

3. 更改密码：

- 单击“Change Password”（更改密码）旁边的复选框，并在“Password”（密码）字段中键入新密码。
- 在“Confirm Password”（确认密码）字段中再次键入新密码。

4. 配置数字寻呼（仅限于 DRAC III 用户）：

- 选择“Enable Numeric Paging”（启用数字寻呼）旁边的复选框，并在“Pager Number”（寻呼机号码）字段中输入寻呼机号码。
- 在“Numeric Message”（数字信息）字段中，输入 DRAC 接收到某些事件时向您发送的数字信息。

5. 配置电子邮件寻呼：

- 选择“Enable Email Paging”（启用电子邮件寻呼）旁边的复选框，并在“Email Address”（电子邮件地址）字段中输入电子邮件地址。
- 在“Message”（信息）字段中，输入 DRAC 接收到某些事件时向您发送的信息。

6. 配置字母数字寻呼（仅限于 DRAC III 用户）：

- 选择“Enable Alpha-Numeric Paging”（启用字母数字寻呼）旁边的复选框，并在“Pager Number”（寻呼机号码）字段中输入寻呼机号码。
- 选择寻呼机的服务供应商使用的字母数字协议：7EO 或 8N1。
- 选择寻呼机的波特率：300 或 1200。
- 在“Custom Message”（自定义信息）字段中，输入 DRAC 接收到某些事件时向您发送的信息。
- 在“Pager ID”（寻呼机 ID）字段中，输入寻呼机的 PIN，然后必要时在“Pager Password”（寻呼机密码）字段中输入寻呼机密码。
- 单击窗口底部的“Apply Changes”（应用更改）。

7. 在“Severity Configuration”（严重性配置）下，指定陷阱以及陷阱必须从 DRAC 触发寻呼操作的严重性。


陷阱使您能够将 DRAC 配置为响应来自系统的 ESM 硬件的警报状况或响应其他状况，例如操作系统崩溃或出现电源故障。

复选框的第一（最左侧的）列对应严重性级别“Informational”（通知），第二列对应严重性级别“Warning”（警告），第三列对应严重性级别“Critical”（严重）。最后七个事件只能报告严重性级别“Informational”（通知）。


8. 单击“Apply Changes”（应用更改），然后单击“OK”（确定），以将警报、寻呼和用户配置保存到 Server Administrator 数据资源库。


Server Administrator 将使您返回到“Users”（用户）选项卡。

配置 DRAC 网络属性

 **注：** 要使用 Remote Access Controller，您必须在 Server Administrator 中具有“管理员”权限。

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，直至您在 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，也必须重新启动 DRAC。

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

要配置您的 DRAC 的网络属性，请执行以下步骤：

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 并随后单击"Configuration"（**配置**）选项卡。

"LAN Configuration"（**LAN 配置**）窗口会出现。

2. 选择"Enable NIC"（**启用 NIC**）旁边的复选框（此选项在默认情况下处于选中状况）。
3. 要让 DHCP 系统分配 NIC 信息，请选择"Use DHCP (For NIC IP Address)"（**使用 DHCP [对于 NIC IP 地址]**）旁边的复选框。否则，请取消选择此复选框，并在"Static IP Address"（**静态 IP 地址**）、"Static Subnet Mask"（**静态子网掩码**）和"Static Gateway Address"（**静态网关地址**）字段中输入 DRAC 的 NIC 信息。
4. 启用拨入网络（仅限于 DRAC III 用户）：
 - a. 选择"Enable Dial-In"（**启用拨入**）旁边的复选框（此选项在默认情况下处于选中状况）。
 - b. 要让 DHCP 系统分配拨入信息，请选择"Use DHCP (For Dial-In IP Address)"（**使用 DHCP [对于拨入 IP 地址]**）旁边的复选框。否则，请取消选择此复选框，并在"Base IP Address"（**基本 IP 地址**）字段中输入 DRAC III 调制解调器的基本 IP 地址。
 - c. 指定拨入连接要求的"Dial-In Authentication"（**拨入验证**）设置：
 - o "Any"（**任何**）— 允许连接使用任何类型的加密，包括不加密
 - o "Encrypted"（**加密**）— 要求连接使用某些类型的加密
 - o CHAP — 要求连接使用 CHAP
5. 要启用 SMTP 服务器地址控件，请单击"Enable SMTP"（**启用 SMTP**）旁边的复选框，并在"SMTP (Email) Server Address"（**SMTP [电子邮件] 服务器地址**）字段中键入 SMTP 服务器地址。
6. 单击"Apply Changes"（**应用更改**），并单击"OK"（**确定**）保存您所作的更改。


配置 DRAC 警报属性

DRAC 可配置为响应来自系统的 ESM 的警报状况或响应其他状况，例如操作系统崩溃或出现电源故障。

DRAC 提供以下类型的警报措施：

- 1 字母数字寻呼（仅限于 DRAC III）（请参阅[添加和配置 DRAC 用户](#)了解有关配置这种警报操作的信息。）
- 1 数字寻呼（仅限于 DRAC III）（请参阅[添加和配置 DRAC 用户](#)了解有关配置这种警报操作的信息。）
- 1 电子邮件（请参阅[添加和配置 DRAC 用户](#)了解有关配置这种警报操作的信息。）
- 1 SNMP 陷阱（有关如何配置此类警报措施的信息，请参阅下一小节。）

配置 SNMP 警报属性

 **注：** 要使用 Remote Access Controller，您必须在 Server Administrator 中具有"管理员"权限。

要配置 Remote Access Controller 警报属性，请执行以下步骤：

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 并随后单击"Configuration"（**配置**）选项卡。
2. 单击 SNMP。
3. 单击"Add"（**添加**）或单击"Destination IP Address"（**目标 IP 地址**），以编辑现有 SNMP 警报属性。
4. 选择"Enable SNMP Trap"（**启用 SNMP 陷阱**）旁的复选框，如果尚未选中。
5. 在"Community"（**团体**）字段中，输入目标 management station 所属的 SNMP 团体名称。
6. 在"IP Address"（**IP 地址**）字段中，输入发生事件时您希望 DRAC 向其发送 SNMP 陷阱的 management station 的目标 IP 地址。
7. 使用"Severity Configuration"（**严重性配置**）下的复选框，指定事件及其必须从 DRAC 触发警报措施的严重性级别。


复选框的第一（最左侧的）列对应严重性级别“Informational”（通知），第二列对应严重性级别“Warning”（警告），第三列对应严重性级别“Critical”（严重）。最后七个事件只能报告严重性级别“Informational”（通知）。

- 单击“Apply Changes”（应用更改），并单击“OK”（确定）保存您所作的更改。


配置 DRAC III 拨入 (PPP) 用户和调制解调器设置

拨入 (PPP) 用户和调制解调器功能目前仅限于 DRAC III。

添加和配置 DRAC III 拨入 (PPP) 用户

 **注：** 要使用 Remote Access Controller，您必须在 Server Administrator 中具有“管理员”权限。

本节将介绍如何添加和配置拨入 (PPP) 用户。验证拨入用户后，拨入用户必须在 Remote Access Controller 登录屏幕中输入 DRAC 用户验证，以访问 DRAC III。

 **注：** Server Administrator Managed-System PPP 客户端使用 192.168.234.235 网络与已安装的 DRAC III 进行会话。此网络 IP 地址很可能已经由其他系统或应用程序使用。如果出现这种情况，PPP 连接将出现故障。如果此地址已被使用，则需要用户将受管系统 PPP 客户端 IP 地址更改为其他数字。要更改受管系统 PPP 服务器 IP 地址以使用其他网络并避免发生冲突，您必须使用 racadm 公用程序。有关使用 racadm 公用程序的信息，请参阅《Dell Remote Access Controller Racadm 用户指南》。

要添加和配置拨入用户，请执行以下步骤：


- 单击“Modular Enclosure”（模块化机框）→ “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 并随后单击“Configuration”（配置）选项卡。
- 单击“Dial-In Users”（拨入用户）。
- 单击 Add（添加）。
- 在“User Name”（用户名）字段中键入用户名。
- 在“Password”（密码）字段中键入新密码。

- 在“Callback Number”（回叫号码）字段中键入回叫号码。


此号码是将“Callback Type”（回叫类型）设置为“Preset”（预设）时 Remote Access Controller 拨打的号码。

- 从“Callback Type”（回叫类型）下拉式菜单中选择一种设置：
 - “None”（无）— 呼叫时，Remote Access Controller 不会断开连接和回拨；连接保持活动状态。
 - “Preset”（预设）— 呼叫时，Remote Access Controller 断开连接，并拨打在“Callback Number”（回叫号码）字段中指定的号码，此设置将激活回叫号码控件。
 - “User Specified”（用户指定）— 接到呼叫时，Remote Access Controller 向用户询问回叫号码。然后，Remote Access Controller 断开连接，并拨打用户指定的号码。
- 单击“Apply Changes”（应用更改），并单击“OK”（确定）保存您所作的更改。

添加和配置 DRAC III 请求拨出条目

 **注：** 要使用 Remote Access Controller，您必须在 Server Administrator 中具有“管理员”权限。

将拨入 (PPP) 设置为“Preset”（预设）时，请求拨出条目可使 Remote Access Controller 断开连接，并以预设号码回叫 management station。回叫时，必须提供 DRAC 用户验证才能访问 Remote Access Service。


 **注：** DRAC III Managed System Software 使用 PPP 连接来与安装的 DRAC 进行会话。PPP 连接的 IP 地址是 192.168.234.235。此网络 IP 地址很可能已经由其他系统或应用程序使用。如果出现这种情况，PPP 连接将出现故障。如果此地址已被使用，则用户需要将 Managed System PPP 客户端 IP 地址更改为其它数字。要更改 Managed System PPP 服务器 IP 地址以使用另一个网络并避免发生冲突，必须使用 racadm 公用程序。有关使用 racadm 公用程序的信息，请参阅《Dell Remote Access Controller Racadm 用户指南》。

要添加请求拨出条目，请执行以下步骤：

- 单击“System”（系统）→ “Main System Chassis”（主系统机箱）→ Remote Access 并随后单击“Configuration”（配置）选项卡。
- 选择“Demand Dial-Out”（请求拨出）。

3. 单击 **Add (添加)**。
4. 输入由此用户呼叫时 Remote Access Controller 回叫的 management station IP 地址。
5. 在 **"Phone Number" (电话号码)** 字段中, 输入系统的调制解调器使用的电话号码。
6. 在 **"User Name" (用户名)** 字段中, 输入请求拨出用户的用户名。
7. 在 **"Password" (密码)** 字段中, 输入请求拨出用户的用户名。
8. 从 **"Authentication" (验证)** 下拉式菜单中选择一种设置:
 - 1 **"Any" (任何)** — 允许连接使用任何类型的加密, 包括不加密
 - 1 **"Encrypted" (加密)** — 要求连接使用某些类型的加密
 - 1 **CHAP** — 要求连接使用 CHAP
9. 单击 **"Apply Changes" (应用更改)**, 并单击 **"OK" (确定)** 保存您所作的更改。

配置 DRAC III 调制解调器设置


 **注:** 要使用 Remote Access Controller, 您必须在 Server Administrator 中具有“管理员”权限。

如果您的 DRAC III 套件中包含可选的 PCMCIA 调制解调器, 则必须在使用之前配置调制解调器。

要配置 DRAC III 调制解调器, 请执行以下步骤:

1. 单击 **"System" (系统)** → **"Main System Chassis" (主系统机箱)** → **Remote Access** 并随后单击 **"Configuration" (配置)** 选项卡。
2. 单击 **"Modem" (调制解调器)**。
3. 对于 **"Dial Mode" (拨号方式)**, 请选择 **"Pulse" (脉冲)** 或 **"Tone" (音频)**。
4. 从 **"Country Code" (国家代码)** 下拉式菜单中选择 DRAC III 所在的国家。
5. 对于 **"Initialization String" (初始字符串)**, 在文本字段中输入 DRAC III 调制解调器所需的初始字符串。
6. 从下拉式菜单中选择 **"Baud Rate" (波特率)** 设置 (默认值为 **38400**)。
7. 单击 **"Apply Changes" (应用更改)**, 并单击 **"OK" (确定)** 保存您所作的更改。

配置 DRAC 远程功能属性

 **注:** 要使用 Remote Access Controller, 您必须在 Server Administrator 中具有“管理员”权限。

如果受管系统上的本地引导映像已损坏, 则 DRAC 能够使用从小型文件传输协议 (TFTP) 服务器下载的软盘引导映像引导其主机服务器。此功能称为远程软盘引导。DRAC 还可以使用位于 TFTP 服务器上的固件映像更新其固件。此功能称为远程固件更新, 其过程与快擦写系统 BIOS 相似。

要配置您的 DRAC 的远程软盘引导功能和远程固件更新功能, 请执行以下步骤:


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** 并随后单击 **"Configuration" (配置)** 选项卡。

屏幕将显示 **"Configure Network Properties" (配置网络属性)** 窗口。
2. 单击 **"Remote Features" (远程功能)**。

系统将显示 **"Remote Properties" (远程属性)** 窗口。
3. 选择 **"Enable Remote Floppy Boot" (启用远程软盘引导)** 旁边的复选框, 以配置远程引导参数。
4. 配置 DRAC 的远程引导参数:
 - a. 单击 **"Enable Remote Floppy Boot" (启用远程软盘引导)** 旁边的复选框。
 - b. 在 **"Remote Floppy TFTP Address" (远程软盘 TFTP 地址)** 字段中, 键入 TFTP 服务器的 IP 地址。

- c. 在"Remote Floppy TFTP Path" (远程软盘 TFTP 路径) 字段中, 键入引导映像文件名。该路径必须相对于 TFTP 服务器的根目录。
5. 配置 DRAC 的固件更新参数:
 - a. 单击"Enable Remote Firmware Update" (启用远程固件更新) 旁边的复选框。
 - b. 在"Remote Firmware TFTP Address" (远程固件 TFTP 地址) 字段中, 键入 TFTP 服务器的 IP 地址。
 - c. 在"Remote Firmware Update Path" (远程固件更新路径) 字段中, 键入固件映像文件名。该路径必须相对于 TFTP 服务器的根目录。
 6. 单击"Apply Changes" (应用更改), 并单击"OK" (确定) 保存您所作的更改。

配置 DRAC 安全

 **注:** 要使用 Remote Access Controller, 您必须在 Server Administrator 中具有"管理员"权限。

 **注:** 有关 DRAC 安全功能的详细信息, 请参阅《Dell Remote Access Controller 安装和设置指南》。

要从 Server Administrator 主页配置 DRAC 安全, 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 并随后单击"Security" (安全) 选项卡。在"Security" (安全) 选项卡下, 可以执行 CSR 认证管理并设置 DRAC 用户登录验证选项。

 **注:** 有些 DRAC 认证管理操作使用 FTP 协议与 DRAC 固件通信。如果系统上安装了防火墙软件, 则这些操作可能会失败。

认证管理

使用"Certificate Management" (认证管理) 窗口可以生成认证签名请求 (CSR)、将服务器认证或认证机构 (CA) 认证上载到 DRAC 固件或查看现有服务器认证或 CA 认证。在"Certificate Management" (认证管理) 窗口中, 您可以使用以下选项:

- 1 [生成 CSR](#)
- 1 [上载认证](#)
- 1 [查看认证](#)

CSR 是发送至 CA 的数字请求, 用于获得安全服务器认证。安全服务器认证可以确保远程系统的身份, 并确保与远程系统交换的信息不会被他人查看或更改。要确保 DRAC 的安全, 强烈建议您生成 CSR, 并将 CSR 提交至 CA, 然后上载从 CA 返回的认证。

认证机构是 IT 行业认可的企业实体, 可满足高标准的可靠性审查、识别和其它重要安全标准。例如, Thwate 和 VeriSign 均为 CA。CA 收到您的 CSR 后, 将对 CSR 中包含的信息进行检查和验证。如果申请者符合 CA 的安全标准, CA 将向申请者颁发认证, 以在通过网络和互联网进行事务处理时唯一标识该申请者。

CA 批准 CSR 并向您发送认证后, 您必须将认证上载至 DRAC 固件。保存在 DRAC 固件上的 CSR 信息必须与认证中包含的信息相匹配。

生成 CSR

 **注意:** 每个新的 CSR 都会改写固件上任何原有的 CSR。固件上的 CSR 与从 CA 返回的认证相匹配是非常重要的。

1. 在"Certificate Management" (认证管理) 窗口中, 选择"Generate a new CSR" (生成新 CSR) 选项并单击"Next" (下一步)。

系统将显示"Certificate Signing Request (CSR) Generation" (认证签名请求 [CSR] 生成) 窗口。

2. 为每个列出的属性键入一个值或从下拉式菜单中选择一个值, 然后单击"Generate" (生成)。

系统将显示一条信息, 说明 CSR 已成功生成并给出保存路径。

3. 此时便可以向 CA 发送您的 CSR。

上载认证

要将服务器认证或 CA 认证上载到 DRAC 固件, 认证必须位于 DRAC 的主机服务器上。必须指定 CSR 类型、确切的文件名和认证在服务器上的绝对文件路径。然后单击"Upload" (上载)。

 **注:** 未输入认证在主机服务器上的正确路径并不会产生警告信息。


1. 在"Certificate Management" (认证管理) 窗口中, 选择"Upload certificate" (上载认证) 选项并单击"Next" (下一步)。

系统将显示"Upload Certificate" (上载认证) 窗口。

2. 从下拉式菜单中选择认证类型。

选项包括“Server Certificate”（服务器认证）和“CA Certificate”（CA 认证）。


3. 键入要上传认证的确切路径和文件名。

 **注：** 如果完全限定路径或文件名中包含空格，则必须使用双引号将字符串括起。例如，如果文件包含在 c:\security files\certificates\sslcert.cer 中，由于“security”和“files”之间有一个空格，所以必须将完全限定路径名和文件名放在双引号中。例如：c:\security files\certificates\sslcert.cer

4. 单击“Upload”（上传）。

系统将显示信息，说明认证已成功上传至 DRAC 固件。

5. 重设 DRAC 以启用新认证。

 **注：** 上传认证后必须重设 DRAC 以确保使用新认证。

查看认证

在“View Server Certificate”（查看服务器认证）和“View CA Certificate”（查看 CA 认证）窗口中均包含以下信息。请参阅表 6-2。

表 6-2. 认证信息

属性	值
类型	认证类型，是服务器认证还是 CA 认证
串行	认证序列号
密钥大小	密钥大小
有效期自	认证的颁发日期
有效期至	认证的期满日期
主题	按照主题输入的认证属性
颁发者	按照颁发者返回的认证属性

配置远程连接验证选项

使用“Remote Connect Authentication Options”（远程连接验证选项）窗口设置 DRAC 用户登录验证选项。将 DRAC 配置为：仅允许通过 Remote Access Controller 创建的用户（DRAC 用户）登录，或允许以通过 Remote Access Controller 和本地操作系统创建的用户登录 DRAC。

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 并随后单击“Security”（安全）选项卡。


系统将显示“Certificate Management”（认证管理）窗口。

2. 单击“Authentication Options”（验证选项）。

将显示“Remote Connect Authentication Options”（远程连接验证选项）窗口。共有两个配置选项，每个前面都带有复选框。

“RAC Authentication”（RAC 验证）复选框默认情况下为选中，并且不能取消选择。此设置使那些通过 DRAC 创建的用户（DRAC 用户）能够登录到 DRAC。

选中“Local Operating System Authentication”（本地操作系统验证）复选框以使那些通过本地操作系统创建的用户也能够登录到 DRAC。

 **注：** “Local Operating System Authentication”（本地操作系统验证）复选框默认情况下为灰显并且对于 DRAC 固件 3.20 或更高版本不能被选中或被取消选择。为 DRAC 固件 3.20 或更高版本使用 Active Directory 验证。请参阅《Dell Remote Access Controller 安装和设置指南》了解有关一起使用 Microsoft Active Directory 和 Dell Remote Access Controller (DRAC III、DRAC III/XT、ERA 和 ERA/O) 的信息。

3. 单击“Apply Changes”（应用更改），并单击“OK”（确定）保存您所作的更改。

访问和使用 Dell Remote Access Controller

要从 Server Administrator 主页链接到 Remote Access Controller DRAC “Log in”（登录）窗口，请依次单击“Main System Chassis/Main System”（主系统机箱/主系统）对象、Remote Access Controller 对象、“Remote Connect”（远程连接）选项卡和“Launch the Remote Connect Interface”（启动远程连接界面）。系统将显示 DRAC “Log in”（登录）窗口。

连接到 DRAC 后就可以监测并管理系统，包括访问系统和会话信息、管理 DRAC 配置和在受管系统上执行远程访问功能。请参阅《Dell Remote Access Controller 安装和设置指南》以了解如何使用 DRAC。

[目录](#)

设置和管理

Dell OpenManage Server Administrator 版本 5.5 用户指南

- [安全管理](#)
- [分配用户权限](#)
- [在支持的 Windows 操作系统中禁用来宾和匿名帐户](#)
- [配置 SNMP 代理](#)
- [在运行支持的 Red Hat Enterprise Linux 操作系统的系统中的防火墙配置](#)

安全管理

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

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。每位用户分配有一个或多个角色，每个角色分配有一个或多个可以由该角色用户执行的用户权限。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。用户级别有三种：用户、高级用户和 管理员。

- 1 “User” (用户) 可以查看大多数信息。
- 1 “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。
- 1 “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。

Server Administrator 赋予以“用户”权限登录的用户只读访问权限；赋予以“高级用户”权限登录的用户读写访问权限；赋予以“管理员”权限登录的用户读、写和管理员访问权限。请参阅 [表 3-1](#)。

表 3-1. 用户权限

用户权限	访问类型		
	管理员	写	读
用户			X
高级用户		X	X
管理员	X	X	X

读访问可以查看 Server Administrator 报告的数据。读访问不允许更改或设置受管系统上的值。

写访问可以更改或设置受管系统上的值。

Administrator 访问权还可以关闭 managed system 。

访问 Server Administrator 服务的权限级别

[表 3-2](#) 总结了哪些用户级别有权访问和管理 Server Administrator services。

表 3-2. Server Administrator 用户权限级别

服务	所需用户权限级别	
	查看	管理
工具	U、P、A	P、A

远程访问	U、P、A	A
存储设备管理	U、P、A	A

表 3-3 定义了在中使用的用户权限级别缩写表 3-2。

表 3-3. Server Administrator 用户权限级别说明

U	用户
P	高级用户
A	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（无论是通过 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 验证会使用集成 Windows 验证（以前称为 NTLM）来进行验证。该验证系统使 Server Administrator 安全保护可以并入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 使用多种基于可插拔验证模块 (PAM) 库的验证方法。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。





 **注：** 在 SUSE Linux Enterprise Server (版本 9 Service Pack 3) 上不支持使用 Winbind 和 Kerberos 的 Server Administrator 验证，因为操作系统中没有 Winbind 和 Kerberos 的 32 位兼容程序库。

加密

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

分配用户权限

要确保重要系统组件安全，安装 Dell OpenManage 软件前将用户权限分配给所有 Dell® OpenManage® 软件用户。新用户可以使用其操作系统用户权限登录 Dell OpenManage 软件。

-  **注意：** 要保护对重要系统组件的访问，您必须为可以访问 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。
-  **注意：** 禁用所支持 Windows 操作系统的来宾帐户以保护对重要系统组件的访问。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®。请参阅“Microsoft Active Directory”了解使用 Active Directory 的详情。

1. 导航到“Control Panel”（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），或者在想向其中添加新用户的分支上单击右键，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:** 您必须以 root 登录才能执行这些步骤。

 **注:** 要执行下面的步骤, 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, 则必须用 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。


您必须为可以访问 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:** 您必须将 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。

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

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

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

 **注:** 您必须以 root 登录才能执行这些步骤。

1. 打开位于 `/etc` 的 `omarolemap` 文件。
2. 在文件中添加以下内容：

```
<User_Name>[Tab]<Host_Name>[Tab]<Rights>
```

[表 3-4](#)列出向 `omarolemap` 文件添加角色定义的说明

表 3-4. 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	用户
通配符 (*)	通配符 (*)	用户
[Tab] = \t (tab 字符)		


[表 3-5](#)列出向 `omarolemap` 文件添加角色定义的说明

表 3-5. 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。
4. 从命令行运行以下命令重新启动连接服务：

```
service dsm_om_connsvc restart
```

 **注：** 确保重新启动连接服务以使更改生效。

使用 `omarolemap` 文件的最佳做法


以下列出使用 `omarolemap` 文件的最佳做法：

- 1 请勿删除 `omarolemap` 文件中的以下默认条目。

1	root	*	管理员
1	+root	*	高级用户
1	*	*	用户

- 1 请勿更改 `omarolemap` 文件权限或文件格式。
- 1 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。
- 1 请勿为 `<Host_Name>` 使用环回地址，例如：`localhost` 或 `127.0.0.1`。
- 1 连接服务重新启动后如果 `/etc/omarolemap` 文件的更改没有生效，请参阅命令日志查找错误。
- 1 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。
- 1 在组名前加上 `+`。
- 1 如果有重复的用户名称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
- 1 除了 [Tab] 以外，空格还可以用作列分隔符

在支持的 Windows 操作系统中禁用来宾和匿名帐户

 **注：** 您必须以“管理员”权限登录才能执行此步骤。

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. 单击“Guest”（来宾）或“IUSR_system name”（IUSR_系统名称）用户帐户。
4. 单击“Action”（操作）并指向“Properties”（属性）。
5. 选择“Account is disabled”（帐户已停用），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，需要安装支持的系统管理协议标准（例如 SNMP）。有关详情，请参阅“[安装要求](#)”。

您可以配置 SNMP 代理，以更改团体名称、启用设置操作以及向管理站发送陷阱。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。有关其他原则，请参阅《Dell Power Solutions》杂志 2003 年 5 月的“[Securing an SNMP Environment](#)”一文。该杂志还可在 www.dell.com/powersolutions 找到。
-  **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：

- 1 “[在运行支持的 Windows 操作系统的系统中配置 SNMP 代理](#)”
- 1 “[在运行支持的 Red Hat Enterprise Linux 的系统上配置 SNMP 代理](#)”
- 1 “[在运行支持的 SUSE Linux Enterprise Server 操作系统的系统中配置 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、启用设置操作以及向管理站发送陷阱。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 配置的其他详细信息，请参阅您的操作系统说明文件。

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）。
系统将显示“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 团体名称可确定哪个系统能够通过 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）。
系统将显示“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）。
系统将显示“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）。
系统将显示“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）。
系统将显示“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）。
系统将显示“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）列表中选择团体名称，然后单击“Edit”（编辑）。
系统将显示“SNMP Service Configuration”（SNMP 服务配置）窗口。
7. 将“Community Rights”（团体权利）设置为“READ WRITE”（读写）或“READ CREATE”（读创建），然后单击“OK”（确定）。
系统将显示“SNMP Service Properties”（SNMP 服务属性）窗口。
8. 单击“OK”（确定）以保存更改。

配置您的系统以向管理站发送 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）。

系统将显示“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. 系统将显示“SNMP Service Configuration”（SNMP 服务配置）窗口。


键入陷阱目标并单击“Add”（添加）。

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。

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

Server Administrator 使用 ucd-snmp 或 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、启用设置操作及向 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 配置的其他详细信息，请参阅您的操作系统说明文件。

SNMP Agent Access Control 配置

Server Administrator 实现的 MIB (Management Information Base [管理信息库]) 分支标有 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 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 代理配置的修改给予“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 之后再对其他所有 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 团体名称可确定哪个系统能够通过 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 团体名称
```

或

```
com2sec notConfigUser default 团体名称
```

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 设置操作。

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
```

配置您的系统以向管理站发送陷阱

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

要配置运行 Server Administrator 的系统以向 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 Management Station 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 操作系统的系统中配置 SNMP 代理

Server Administrator 使用 ucd-snmp 或 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：** 在 SUSE Linux Enterprise Server（版本 9）中，SNMP 代理配置文件位于 `/etc/snmpd.conf`。在 SUSE Linux Enterprise Server（版本 10）上，SNMP 代理配置文件位于 `/etc/snmp/snmpd.conf`。

 **注：** 有关 SNMP 配置的其他详细信息，请参阅操作系统说明文件。


Server Administrator SNMP 安装操作

Server Administrator SNMP 使用 SNMP 多路复用 (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/snmpd.conf` 或 `/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。


要启用从一个特定远程主机向运行 Server Administrator 的系统的 SNMP 访问，应编辑以下 SNMP 代理配置文件，`/etc/snmpd.conf` 或 `/etc/snmp/snmpd.conf`，并执行以下步骤：

1. 查找以下行：

```
rocommunity public 127.0.0.1
```

2. 编辑或复制该行，以使用远程主机 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向运行 Server Administrator 的系统的 SNMP 访问，应编辑以下 SNMP 代理配置文件，`/etc/snmpd.conf` 或 `/etc/snmp/snmpd.conf`，并执行以下步骤：

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/snmpd.conf` 或 `/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

必须在运行 Server Administrator 的系统上启用“SNMP 设置”操作，以便使用 IT Assistant 更改 Server Administrator 属性。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 设置操作，请编辑 SNMP 代理配置文件 `/etc/snmpd.conf` 或 `/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
```

配置您的系统以向管理站发送陷阱

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

要将运行 Server Administrator 的系统配置为向管理站发送陷阱，请编辑 SNMP 代理配置文件 `/etc/snmpd.conf` 或 `/etc/snmp/snmpd.conf`，并执行下列步骤：

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 Red Hat Enterprise Linux 操作系统的系统中的防火墙配置

如果在安装 Red Hat Enterprise 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）以从 Server Administrator 查找和检索信息，则至少一个外部网络接口上的 SNMP 端口必须处于打开状况。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 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。

- 按 <Tab> 以选择"Security Level" (**安全级别**)，然后按空格键以选择您要设置的安全级别。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。

- 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](#)。
- 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[步骤 4](#)。

- 按 <Tab> 以转到"**Customize**" (**自定义**) 并按 <Enter>。

系统将显示"**Firewall Configuration - Customize**" (**防火墙配置 - 自定义**) 屏幕。

- 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。
 - 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网络接口。
 - 要打开所有网络接口上的 SNMP 端口，请按 <Tab> 跳至"**Other ports**" (**其他端口**)，然后键入 `snmp:udp`。

- 按 <Tab> 键以选择"**OK**" (**确定**) 并 <Enter>。

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

- 按 <Tab> 键以选择"**OK**" (**确定**) 并 <Enter>。

系统将显示"**Choose a Tool**" (**选择工具**) 菜单。

- 按 <Tab> 键以选择"**Quit**" (**退出**) 并按 <Enter>。

[目录](#)

[目录](#)

Storage Management Service

Dell OpenManage Server Administrator 版本 5.5 用户指南

- [概览](#)
- [软件前提条件](#)
- [硬件前提条件](#)
- [Storage Management Service](#)
- [从 Array Manager 迁移至 Storage Management](#)
- [Storage Management 命令行界面](#)
- [显示联机帮助](#)

概览

Storage Management Service 提供了与 Server Administrator 集成的 RAID 和非 RAID 存储管理。在 Microsoft® Windows®、Red Hat® Enterprise Linux® 和 SUSE™ Linux Enterprise Server 中，使用“Typical Setup”（典型安装）或“Custom Setup”（自定义安装）安装 Storage Management Service。Storage Management Service 以集成图形视图方式提供 Storage Management 信息。

Storage Management Service:

- 1 可以让您通过一个图形或命令行界面为所有支持的 RAID 和非 RAID 控制器和机柜执行控制器和机柜功能，而不必使用控制器 BIOS 公用程序。
- 1 可以让您查看被监测系统上所连本地和远程存储设备的状态。
- 1 支持 SCSI、SATA、ATA 和 SAS；但是，光纤信道不受支持。
- 1 通过配置数据冗余、分配热备份或重建故障驱动器来保护数据。
- 1 提供了一个图形界面，以向导方式为新用户和高级用户提供了功能及详细的联机帮助。
- 1 提供了一个全功能和可编写脚本的命令行界面。
- 1 提供了详细的联机帮助。

有关从命令行运行 Storage Management 的信息，请参阅《Server Administrator 命令行界面用户指南》。

- 🔔 **注意：** Storage Management Service (Storage Management) 可以让您执行具有数据破坏性功能的存储任务。Storage Management 应由熟悉其存储环境的经验丰富的管理员使用。
- 📖 **注：** 有关 Storage Management 的完整说明文件，请参阅 Storage Management 联机帮助或《Dell™ OpenManage™ Server Administrator Storage Management 用户指南》。
- 📖 **注：** Storage Management Service 在运行 Microsoft Windows、Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统的系统中可用。

使用 Storage Management 时，单击全局导航栏上的“**Help**”（帮助），可以获得有关当前正在查看的特定窗口的详细信息。用户可查看所有窗口（取决于用户权限级别和 Server Administrator 在 managed system 中查找到的特定硬件和软件组）均可使用帮助。

软件前提条件

请参阅 Storage Management 自述文件 ([readme_sm.txt](#)) 和 Server Administrator 自述文件 ([readme_sa.txt](#)) 了解完整的软件和硬件要求。这些文件可在 *Dell Systems Management Tools and Documentation DVD* 上找到。

硬件前提条件

在一个没有支持的控制器或者控制器没有连接到存储设备的系统上安装 Storage Management 是一项不支持的配置。要了解所支持控制器的列表和有关 Storage Management Service 硬件要求的其它信息，请参阅 *Dell Systems Management Tools and Documentation DVD* 上的 Server Administrator 自述文件 ([readme_sa.txt](#)) 和 Storage Management 自述文件 ([readme_sm.txt](#))。

Storage Management Service

安装 Storage Management 会取代系统上驻留的任何先前安装的 Array Manager managed system（服务器软件）和控制台（客户机软件）。如果系统上只安装了 Array Manager 控制台，则安装 Storage Management 不会取代 Array Manager 控制台。

Storage Management Service 提供了用于配置系统本地所连 RAID 和非 RAID 磁盘存储的高级功能。Storage Management 使您能够通过 Server Administrator 图形界面为所有支持的 RAID 和非 RAID 控制器、PowerVault™ 2xxS、PowerVault MD1120 和 PowerVault MD1000 机柜执行控制器和机柜功能，而不必使用控制器 BIOS 公用程序。

使用 Storage Management Service，您可以通过配置数据冗余、分配热备份或重建故障驱动器来保护数据。您还可执行具有数据破坏性功能的任务，如删除虚拟磁盘或重设控制器配置。所有 Storage Management Service 用户应熟悉其存储环境和 Storage Management。

除 Server Administrator 界面功能之外，Storage Management Service 还以向导方式为新用户和高级用户提供了一些功能和详细的联机帮助。

Storage Management 命令行界面 (CLI) 提供了用于 Server Administrator **omreport** 和 **omconfig** 命令的扩展选项。这些选项提供了一个全功能和可编写脚本的命令行界面。

Storage Management Service 支持 SCSI、SATA、ATA 和 SAS；但不支持光纤信道。

Storage Management Service 和 Array Manager

Dell OpenManage Storage Management 是 Array Manager 的替换产品。Storage Management Service 提供与 Array Manager 相似的 Storage Management 和配置功能。在操作系统支持和其他功能方面也有所不同。请务必阅读 [“从 Array Manager 迁移至 Storage Management”](#) 中的详情并参阅 《Storage Management 用户》了解详情。

Storage Management 树对象


如果已经安装，则通过在 Server Administrator 图形用户界面上选择“Storage”（存储）树对象可以访问 Storage Management Service。“Storage”（存储）对象展开后会显示系统上所连支持的控制器的树对象。控制器对象会展开来显示控制器所连的存储设备。

根据系统所连的控制器和存储设备，展开的“Storage”（存储）对象可能会显示以下低级别对象：

- | | |
|---------------|-------------|
| 1 控制器 | 1 风扇 |
| 1 电池 | 1 电源设备 |
| 1 连接器 | 1 温度 |
| 1 机柜或背板 | 1 固件/驱动程序版本 |
| 1 物理磁盘 | 1 虚拟磁盘 |
| 1 EMM（机柜管理模块） | |

“Health”（运行状况）选项卡

各个树对象的“Health”（运行状况）选项卡显示存储控制板信息。“Storage Dashboard”（存储控制板）会列出系统上所有可用的控制器。可以使用“Available Tasks”（可用任务）下拉菜单配置控制器。在“Storage Dashboard”（存储控制板）页中，还可以查看虚拟磁盘详情以及控制器的运行状况。


 **注：** 必须作为管理员登录才能执行存储控制板中的“Available Tasks”（可用任务）。

“Information/Configuration”（信息/配置）选项卡

“Information/Configuration”（信息/配置）选项卡显示所选树对象的属性信息。使用 Storage Management Service 时，“Information/Configuration”（信息/配置）选项卡也会有用于执行存储任务和启动向导的下拉菜单和按钮。

Storage Management 任务

Storage Management Service 具有用于执行 Storage Management 和配置任务的下拉菜单和向导。本节将介绍 Storage Management Service 提供的一些常见的存储任务和向导。

 **注：** 要获得 Storage Management 存储任务和其他功能的完整说明文件，请参阅 Storage Management 联机帮助。

创建虚拟磁盘向导

Storage Management Service 提供了快速和高级创建虚拟磁盘向导。“快速向导”会根据可用的空间和控制器情况计算相应的虚拟磁盘配置。使用“快速向导”时，您可以选择虚拟磁盘的 RAID 级别和大小。“快速向导”会选择一个符合所选 RAID 级别和大小的建议磁盘配置。“快速向导”不需要用户进行太多输入，建议新用户使用。

“创建虚拟磁盘高级向导”可以让您指定虚拟磁盘的读取、写入和高速缓存策略。也可以选择要使用的物理磁盘和控制器连接器。您需要熟悉 RAID 级别和硬件才能使用“高级向导”。建议高级用户使用此向导。

要启动快速和高级创建虚拟磁盘向导：

1. 展开“Storage”（存储）树对象以显示控制器对象。
2. 展开控制器对象。
3. 选择“Virtual Disks”（虚拟磁盘）对象。
4. 单击“Goto Create Virtual Disk Wizard”（转到创建虚拟磁盘向导）。
5. 请参阅 Storage Management 联机帮助了解详情。

重新配置虚拟磁盘向导

"重新配置虚拟磁盘向导"可以让您更改虚拟磁盘配置。使用此任务，可以通过添加物理磁盘更改 RAID 级别或增加虚拟磁盘容量。

要启动"重新配置虚拟磁盘向导"：

1. 展开"Storage"（**存储**）树对象以显示控制器对象。
2. 展开控制器对象。
3. 选择"Virtual Disks"（**虚拟磁盘**）对象。
4. 从"Available Tasks"（**可用任务**）下拉菜单选择"Reconfigure"（**重新配置**）。
5. 单击"Execute"（**执行**）。
6. 请参阅 Storage Management 联机帮助了解详情。

保持冗余虚拟磁盘的完整性

如果已经创建了冗余虚拟磁盘，"Check Consistency"（**检查一致性**）任务可以验证冗余（奇偶校验）信息的准确性。此任务只适用于冗余虚拟磁盘。必要时，"Check Consistency"（**检查一致性**）可以重建冗余数据。

要启动"Check Consistency"（**检查一致性**）任务：

1. 展开"Storage"（**存储**）树对象以显示控制器对象。
2. 展开控制器对象。
3. 选择"Virtual Disks"（**虚拟磁盘**）对象。
4. 从"Available Tasks"（**可用任务**）下拉菜单选择"Check Consistency"（**检查一致性**）。
5. 单击"Execute"（**执行**）。
6. 请参阅 Storage Management 联机帮助了解详情。

分配和取消全局热备份

全局热备份是一个未使用的备份磁盘，它是阵列组的一部分。热备份保持待机模式。当在虚拟磁盘中使用的物理磁盘发生故障时，会激活分配的热备份来替换故障的物理磁盘，而不会中断系统或需要您的干预。当热备份被激活时，它会为所有使用故障物理磁盘的冗余虚拟磁盘重建数据。

通过取消分配某一磁盘并根据需要选择另一磁盘，可更改热备份的分配。还可以分配一个以上的物理磁盘作为全局热备份。

全局热备份必须手动分配和取消。它们不分配到特定的虚拟磁盘。如果想要将一个热备份分配到虚拟磁盘（它将取代虚拟磁盘中出现故障的任何物理磁盘），则使用指令对专用热备份进行分配和取消分配。

分配专用热备份

1. 在"Connector"（**连接器**）（信道或端口）表中选择您要用作专用热备份的磁盘。在某些控制器上，可选择多个磁盘。您选作专用热备份的磁盘将显示在"Disks currently configured as dedicated hot spare"（**当前配置为专用热备份的磁盘**）表中。
2. 在准备好后单击"Apply Changes"（**应用更改**）。

取消专用热备份

1. 单击"Disks currently configured as dedicated hot spare"（**当前配置为专用热备份的磁盘**）表中的磁盘以取消分配。单击该磁盘会将其从"Disks currently configured as dedicated hot spare"（**当前配置为专用热备份的磁盘**）表中除去，并将其返回至"连接器"（信道或端口）表中。
2. 在准备好后单击"Apply Changes"（**应用更改**）。

在 Storage Management 中查找该磁盘

1. 展开"Storage" (存储) 树对象以显示控制器对象。
2. 展开控制器对象。
3. 选择"Virtual Disks" (虚拟磁盘) 对象。
4. 从"Available Tasks" (可用任务) 下拉菜单中选择 "Assign/Unassign Dedicated Hot Spare" (分配/取消专用热备份)。
5. 单击"Execute" (执行) 。
6. 请参阅 Storage Management 联机帮助了解详情。

重建故障的物理磁盘

如果故障的物理磁盘是冗余虚拟磁盘的一部分，如果立即更换，物理磁盘故障应不会造成数据损失。在选定"Physical Disks" (物理磁盘) 对象时即可使用重建任务。请参阅 Storage Management 联机帮助了解详情。

全局任务

在选定存储对象时即可使用以下全局任务。请参阅 Storage Management 联机帮助了解详情。

- 1 **全局重新扫描**：全局重新扫描可以更新所有控制器及其所连组件的配置更改（如新的或删除的设备）。
- 1 **启用和禁用 SMART 热关机**：默认情况下，在 PV220S 和 PV221S 机柜达到 0 或 50 摄氏度临界温度时操作系统和服务器关闭。但是，使用"Enable Smart Thermal Shutdown" (启用智能热关机) 任务，您可以指定当机柜达到临界温度时，机柜关机，而非操作系统和服务器关机。要将系统恢复到默认设置，请使用"Disable Smart Thermal Shutdown" (禁用智能热关机) 任务。

控制器任务

在选定"Controller" (控制器) 对象时即可使用以下控制器任务。请参阅 Storage Management 联机帮助了解详情。

- 1 **重新扫描控制器**：重新扫描控制器可以更新控制器所连所有组件的配置更改（如新的或删除的设备）。
- 1 **创建虚拟磁盘**：请参阅 [创建虚拟磁盘向导](#)。
- 1 **启用、禁用、静音和检测警报**：这些任务使用户能够管理控制器警报。例如，您可以设置警报在设备故障时响起，或者在警报响起后静音。
- 1 **设置重建率**：重建率指有多少系统资源专门用于重建失败的物理磁盘。此任务可以让您调整这一设置。
- 1 **重置配置**：此任务会擦除控制器上的所有信息，因此可以执行全新配置。此操作会破坏控制器上的所有虚拟磁盘。
- 1 **导出日志文件**：此任务会将控制器日志导出到一个文本文件。
- 1 **导入外部配置**：此任务会对移自其他控制器的物理磁盘上的虚拟磁盘进行导入。
- 1 **清除外部配置**：使用清除外部配置任务从新近连接的物理磁盘上清除或擦除虚拟磁盘信息。
- 1 **设置后台初始化率**：此任务更改专门用于后台初始化任务的系统资源数量。
- 1 **设置检查一致性率**：此任务更改专门用于检查一致性任务的系统资源数量。
- 1 **设置重新构建率**：此任务更改专门用于重新构建任务的系统资源数量。
- 1 **设置巡检读取模式**：此功能可识别磁盘错误以避免磁盘故障和数据丢失或损坏。
- 1 **启动和停止巡检读取**：这些任务使用户可以在巡检读取模式设置为手动时启动巡检读取任务或停止运行的任务。
- 1 **管理正在使用的高速缓存**：在回写策略中，数据先写入高速缓存中，然后写入物理磁盘中。如果虚拟磁盘由于任何原因变为脱机或被删除，高速缓存中的数据会丢失。发生意外电缆或电源故障时，高速缓存中的数据也可能会丢失。发生这种故障时，存储控制器会保留在正在使用的或未清除的高速缓存上写入的数据，直到用户恢复虚拟磁盘或清除高速缓存为止。
- 1 **导入/恢复外部配置**：此任务会对移自其它控制器的物理磁盘上的虚拟磁盘进行导入和恢复。
- 1 **外部配置操作**：此任务提供可以导入的外部配置的预览。固件版本为 6.1 和更高版本的 PERC 6 控制器上提供了此任务。
- 1 **清除外部配置**：使用此任务可以从新连接的物理磁盘中清除或擦除虚拟磁盘信息。
- 1 **更改控制器属性**：此任务使用户能够同时更改多个控制器属性。固件版本为 6.1 和更高版本的 PERC 6 控制器上提供了此任务。
- 1 **负载均衡**：此任务能够自动使用两个连接到同一机柜的控制器端口或连接器来发送 I/O 请求。只有固件版本为 6.1 和更高版本的 PERC 6 控制器上才提供此任务。
- 1 **可恢复热备份**：此任务能够实现自动将数据从物理磁盘复制到热备份（发生预测故障时）或从热备份复制到物理磁盘（更换降级磁盘时）。固件版本为 6.1 和更高版本的 PERC 6 控制器上提供了此任务。
- 1 **发生预测故障时自动更换**：发生预测故障时，此任务能够自动将数据从物理磁盘复制到热备份。此属性与"Revertible Hot Spare" (可恢复热备份) 属性结合使用。固件版本为 6.1 和更高版本的 PERC 6 控制器上提供了此任务。

电池任务

在选定“Battery”（**电池**）对象时即可使用以下电池任务。此任务只供那些电池需要复原的控制器使用。请参阅 [Storage Management 联机帮助](#) 了解详情。

- 1 **复原电池**：此任务会对控制器电池进行完全放电并重新充电。
- 1 **启动记忆循环**：使用启动记忆循环任务开始电池记忆循环。
- 1 **电池延迟记忆循环**：使用此任务延迟记忆循环启动时间长达七天。

连接器任务

在选定“Connector”（**连接器**）对象时即可使用以下连接器任务。请参阅 [Storage Management 联机帮助](#) 了解详情。

- 1 **重新扫描连接器**：此任务重新扫描控制器连接器来验证当前连接的设备，或者识别已添加到连接器的新设备。在连接器上执行重新扫描与在控制器上执行重新扫描相似。

机柜任务

在选定“Enclosure”（**机柜**）对象时即可使用以下机柜任务。请参阅 [Storage Management 联机帮助](#) 了解详情。

- 1 **启用并禁用警报**：使用这些任务管理机柜警报。如果启用，则当机柜遇到错误情况下会发出警报。
- 1 **设置资产数据**：使用此任务更改机柜的资产标签和资产名称。
- 1 **设置温度探测器值**：温度探测器监测机柜的温度。每个温度探测器都有一个“警告”和“故障”阈值。“警告”阈值表示机柜正在接近异常的高温或低温。使用此任务可以修改“警告”阈值。
- 1 **闪烁**：使用“闪烁”任务以使机柜上的发光二极管（LED）闪烁。您可能需要使用此任务来查找某一机柜。机柜上的 LED 可显示不同的颜色和闪烁样式。

温度任务


在选定“Temperatures”（**温度**）对象时即可使用以下温度探测器任务。请参阅 [Storage Management 联机帮助](#) 了解详情。

- 1 **设置温度探测器值**：温度探测器监测机柜的温度。每个温度探测器都有一个“警告”和“故障”阈值。“警告”阈值表示机柜正在接近异常的高温或低温。使用此任务可以修改“警告”阈值。

物理磁盘任务

在选定“Physical Disks”（**物理磁盘**）对象时即可使用以下物理磁盘任务。请参阅 [Storage Management 联机帮助](#) 了解详情。

- 1 **闪烁和取消闪烁**：闪烁任务使用户可以通过闪烁磁盘上的某个发光二极管（LED）来查找机柜中的磁盘。“Unblink”（取消闪烁）任务取消“Blink”（闪烁）任务。
- 1 **卸下死段**：在某些环境中，此任务使用户能够恢复当前不可用的磁盘空间。
- 1 **分配和取消分配全局热备份**：请参阅 [“分配和取消全局热备份”](#)。
- 1 **准备卸下**：在从机柜卸下磁盘前使用此任务。

 **注意**：要防止数据丢失，应确保执行此任务。

- 1 **联机和脱机**：在卸下前使用脱机任务取消激活磁盘。使用“Online”（联机）任务可以重新启用脱机的磁盘。
- 1 **初始化**：在有些控制器上，“Initialize”（初始化）任务准备将物理磁盘用作虚拟磁盘的一员。
- 1 **重建**：请参阅 [“重建故障的物理磁盘”](#)。
- 1 **取消重建**：使用取消重建任务取消正在进行的重建。
- 1 **清除物理磁盘和取消清除**：使用清除物理磁盘任务擦除物理磁盘上的数据。

虚拟磁盘任务

在选定“Virtual Disks”（**虚拟磁盘**）对象时即可使用以下虚拟磁盘任务。请参阅 [Storage Management 联机帮助](#) 了解详情。

- 1 **重新配置**：请参阅 [“重新配置虚拟磁盘向导”](#)。
- 1 **取消重建**：使用取消重建任务取消正在进行的重建。
- 1 **取消重新配置**：使用取消重新配置任务取消正在进行的虚拟磁盘重新配置。
- 1 **格式化和初始化；慢速和快速初始化**：使用格式化或初始化；慢速和快速初始化任务在虚拟磁盘上擦除文件并删除文件系统。
- 1 **取消后台初始化**：在有些控制器上，冗余虚拟磁盘的后台初始化在虚拟磁盘创建后自动开始。如果您需要取消后台初始化则可以使用此任务。

- 1 **恢复死段：**使用恢复死段任务从已损坏的 RAID-5 虚拟磁盘恢复数据。
- 1 **"Delete"（删除）。**使用此任务可以删除虚拟磁盘上的所有数据。
- 1 **分配和取消分配全局热备份：**请参阅[分配和取消全局热备份](#)。
- 1 **检查一致性、取消一致性检查、暂停一致性检查和恢复一致性检查：**请参阅[保持冗余虚拟磁盘的完整性](#)。
- 1 **闪烁和取消闪烁：**闪烁和取消闪烁任务会闪烁或取消闪烁虚拟磁盘中物理磁盘上的指示灯。
- 1 **重命名：**使用此任务重命名虚拟磁盘。
- 1 **更改策略：**使用此任务可以更改虚拟磁盘的读、写、高速缓存或磁盘高速缓存策略。
- 1 **分割镜像：**使用此任务可以分开原来被配置为 RAID 1、RAID 1 连锁或 RAID 10 虚拟磁盘的镜像数据。
- 1 **取消镜像：**使用此任务可以分开镜像数据，并将一半镜像恢复到可用的空间。
- 1 **更换成员磁盘：**使用此任务可以通过提供更换成员配置选项，将数据从属于虚拟磁盘成员的物理磁盘复制到另一个物理磁盘。可以启动多个从不同阵列组复制数据的操作。

其他 Storage Management 功能和说明文件

有关 Storage Management Service 的完整说明文件，请参阅 Storage Management 联机帮助和《Dell OpenManage Server Administrator Storage Management 用户指南》。要了解如何启动联机帮助，请参阅[显示联机帮助](#)。

从 Array Manager 迁移至 Storage Management

如果用 Storage Management 来取代现有的 Array Manager 安装，则考虑以下迁移注意事项：

- 1 **虚拟磁盘保留：**从 Array Manager 迁移到 Storage Management 时可以保留虚拟磁盘名称。但是，为了这样做，您务必不能在安装 Storage Management 之前卸载 Array Manager。如果在安装 Storage Management 之前已卸载 Array Manager，则 Storage Management 将对用 Array Manager 创建的虚拟磁盘进行重命名。不管是否已卸载 Array Manager，Storage Management 均可识别和管理用 Array Manager 创建的虚拟磁盘。
- 1 **SNMP 陷阱：**用于处理 SNMP 陷阱和管理信息库 (Management Information Base, MIB) 的体系结构在 Storage Management 与 Array Manager 中是不同的。您必须修改已自定义为从 Array Manager 中接收 SNMP 陷阱的应用程序。
- 1 **事件编号：**Storage Management 警报或事件的编号方案与用于相应 Array Manager 事件的编号不同。请参阅 Storage Management 联机帮助了解详情。

Storage Management 命令行界面

有关从命令行运行 Storage Management Service 的信息，请参阅《Server Administrator 命令行界面用户指南》。如果已安装 Storage Management，您也可以参阅联机帮助来获得扩展的 **omreport** 和 **omconfig** 命令行选项的信息。

显示联机帮助

Server Administrator 提供了上下文相关的联机帮助。要访问联机帮助，请单击全局导航栏上的“**Help**”（帮助）。用户可查看的所有窗口（取决于用户权限级别和 Server Administrator 在 managed system 中查找到的特定硬件和软件组）均可使用此导航。

Storage Management 提供了更多的联机帮助。选定“**Storage**”（存储）或低级别树对象时即可使用帮助。

Storage Management Service 的联机帮助：

- 1 提供存储概念信息，如虚拟磁盘、RAID 等
- 1 介绍应用程序不同的窗口中的图形用户界面组件
- 1 提供您可以在图形用户界面中执行任务的详细说明
- 1 介绍可用的 CLI 命令及其子命令

Storage Management 联机帮助备有两种格式：

- 1 **上下文相关帮助：**要访问上下文相关联机帮助，单击全局导航栏上的“**Help**”（帮助）。
- 1 **目录：**上下文相关帮助的帮助屏幕包含联机帮助目录的链接。要访问目录，请先单击全局导航栏上的“**Help**”（帮助）。然后，单击“**Back to Storage Management Contents Page**”（返回到 Storage Management 目录页）链接以显示目录。此链接显示在每个帮助屏幕的上部和底部。使用“Table of Contents”（目录）可以访问联机帮助中包括的所有主题。

[目录](#)

[目录](#)

使用 Server Administrator

Dell OpenManage Server Administrator 版本 5.5 用户指南

- [启动 Server Administrator 会话](#)
- [登录和注销](#)
- [Server Administrator 主页](#)
- [使用联机帮助](#)
- [使用首选项主页](#)
- [使用 Server Administrator 命令行界面](#)
- [Dell Systems Management Server 管理连接服务和安全设置](#)
- [控制 Server Administrator](#)

启动 Server Administrator 会话

要在本地系统中启动 Server Administrator 会话，请单击桌面上的 Dell™ OpenManage™ Server Administrator 图标。

要在远程系统上启动 Server Administrator 会话，打开 Web 浏览器并在地址字段中输入下面的任一地址，然后按 <Enter> 键：

```
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 地址是 managed system 的 IP 地址，1311 是默认端口号。

Server Administrator 日志登录窗口出现。


 **注：** 您必须在地址字段中键入 https://（而不是 http://）以在浏览器中接收有效响应。

 **注：** Dell™ OpenManage™ Server Administrator 的默认端口是 1311。您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。


 **注：** 使用 Internet Explorer 版本 7.0 启动 Server Administrator 时，会立即显示一个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](#)”。

登录和注销

要登录到 Server Administrator，需将预先分配的“Username”（用户名）和“Password”（密码）输入系统管理“Log in”（登录）窗口的相应字段。请参阅“[单一登录](#)”了解如何通过单击桌面上的 Dell OpenManage Server Administrator 图标跳过登录页并访问 Server Administrator Web 应用程序。

 **注：** 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。

如果要通过已定义的域访问 Server Administrator，您还需要指定正确的“Domain”（域）名。


 **注：** “Application”（应用程序）下拉菜单将作为系统的不可选字段出现，该菜单只能访问一个 Dell OpenManage Server Administrator 组件。只有在 managed system 上有两个或多个 Dell OpenManage Server Administrator 组件时，该下拉菜单才可用。

选择“Active Directory Login”（Active Directory 登录）复选框使用 Microsoft® Active Directory® 登录。

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。

单一登录

Microsoft Windows® 系统上的“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：** 请参阅知识库文章 <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q258063> 了解有关单一登录的详情。

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）。

运行支持的 Microsoft Windows Server 2003 操作系统的系统

必须配置浏览器的安全设置，才能从运行支持的 Microsoft Windows Server® 2003 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. 启动浏览器。
2. 单击“Tools”（工具）→ “Internet Options”（Internet 选项）→ “Security”（安全）。
3. 单击“Trusted Sites”（受信任的站点）图标。
4. 单击 Sites（站点）。
5. 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。
6. 单击“Custom Level”（自定义级别）。

对于 Windows 2000:

- 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。

对于 Windows 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。

- 1 单击“OK”（确定）保存新设置。
- 1 关闭浏览器。
- 1 登录到 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. 启动浏览器。
2. 单击“Tools”（工具）→ “Internet Options”（Internet 选项）→ “Security”（安全）。
3. 单击“Trusted Sites”（受信任的站点）图标。
4. 单击 Sites（站点）。

5. 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。
6. 单击“Custom Level”（自定义级别）。
7. 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。
8. 单击“OK”（确定）保存新设置。
9. 关闭浏览器。
10. 登录到 Server Administrator。

Mozilla

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，Server Administrator 主页包括三个主要区域：

1. [全局导航栏](#) 提供了常规服务的链接。
1. [系统树](#) 显示基于用户访问权限的所有可见系统对象。
1. [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、设定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 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
BMC	Dell PowerEdge x8xx 和 x9xx 系统
iDRAC	Dell xx0x 系统

[图 5-1](#) 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 5-1. Server Administrator 主页示例 — 非模块化系统



图 5-2 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 5-2. 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区数据区域。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。

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。

- 1 单击“Preferences”（首选项）将打开“Preferences”（首选项）主页。请参阅[使用首选项主页](#)。
- 1 单击“Support”（支持）将连接至 Dell 支持网站。
- 1 单击“Help”（帮助）将打开上下文相关联机帮助窗口。请参阅[使用联机帮助](#)。
- 1 单击“About”（关于）将显示 Server Administrator 的版本和版权信息。
- 1 单击“Log Out”（注销）将结束当前的 Server Administrator 程序会话。

系统树

系统树显示在 Server Administrator 主页的左侧，列出了可以查看的系统组件。系统组件按组件类型进行分类。展开称为“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。

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 5-2. 系统/服务器模块组件状况指示器

	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（非严重）状况。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。警告状态需要尽快处理。
	红色的 X 表示组件处于故障（严重）状况。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。
	空白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四个任务按钮：“Print”（打印）、“Export”（导出）、“Email”（电子邮件）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。有关单个任务按钮的特定信息，请单击任意 Server Administrator 主页窗口的“Help”（帮助）以获得有关正在查看的特定窗口的详细信息。

- 1 单击“Print”（打印）将在默认打印机上打印打开的窗口。
- 1 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。
- 1 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。
- 1 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。
- 1 单击“Save As”（另存为）将保存操作窗口 HTML 文件（以 .zip 文件形式）。
- 1 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。

 **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。

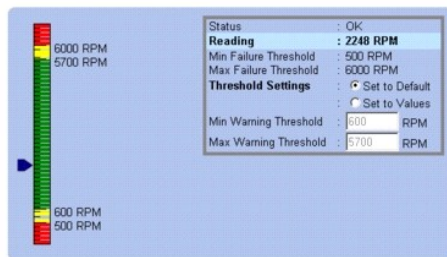
带下划线的项目

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 5-3](#)显示了系统 CPU 风扇探测器的读数。

图 5-3. 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。单击全局导航栏上的“Help”（帮助）将打开单独显示的帮助窗口，其中显示当前所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

默认情况下，访问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。

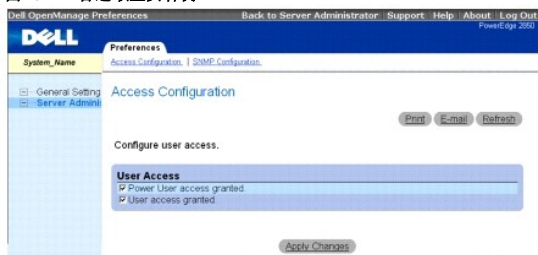
在首选项主页中，您可以限制具有“用户”和“高级用户”权限用户的访问，设置简单网络管理协议（SNMP）密码及配置用户设置和安全端口系统设置。

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

- 1 全局导航栏提供常规服务的链接。
 - o 单击“Back to Server Administrator”（返回 Server Administrator）将使您返回到 Server Administrator 主页。
- 1 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 的首选类别。
- 1 操作窗口显示 managed system 的可用设置和首选项。

图 5-4 显示首选项主页布局的样例。

图 5-4. 首选项主页样例



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。

在许多情况下，CLI 使有非常明确任务的用户可以快速检索系统信息。例如，管理员可以使用 CLI 命令编写批处理程序或脚本，以在指定时间执行。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，与系统低使用率时的同一测量数据进行比较。命令结果可以发送到一个文件，以便以后进行分析。该报告可以帮助管理员获得有关信息，以用于调整使用方案、判断是否需要购买新的系统资源或了解故障组件的运行状况。

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

Dell Systems Management Server 管理连接服务和安全设置

本节包括以下主题：

- 1 [设置用户和服务器首选项](#)
- 1 [X.509 认证管理](#)

设置用户和服务器首选项

您可以在“Preference”（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“Preference”（首选项）。
系统将显示“Preference”（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。

- 1 "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。


- 1 "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。

- 1 "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。

- 1 "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。

- 1 "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)。

- 1 "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。

- 1 "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 ,。

- 1 "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-bit or higher" (128 位或更高)。

o 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。

o "128-bit or higher" (128 位或更高): 允许具有 128 位或更高加密长度的浏览器的连接。根据建立会话的浏览器,会使用以下某种加密方案:

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

 **注:** "128-bit or higher" (128 位或更高) 选项不允许具有较低 SSL 加密强度 (比如 40 位、56 位) 的浏览器的连接。

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


 **注意:** 如果加密级别设置为 "128-bit or higher" (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:

- 1 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。
- 1 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，您必须以 "Administrator"（管理员）权限登录。


要通过首选项主页管理 X.509 认证，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 认证）。

此选项可用于：

1. **生成新的 X.509 证书** - 此选项用于为访问 Server Administrator 创建证书。
1. **重复使用现有的 X.509 证书** - 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。
1. **导入根证书** - 此选项使您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）。
1. **导入来自 CA 的证书链** - 此选项使您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。

控制 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：** 要控制 Server Administrator，必须以管理员权限登录（对于支持的 Red Hat® Enterprise Linux® 或 SUSE® Linux Enterprise Server 操作系统，则以 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 Microsoft 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 Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统

要在运行支持的 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 Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统

要在运行支持的 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 Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统

要在运行支持的 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
```

[目录](#)


[目录](#)

版本 5.5 的新功能

Dell OpenManage Server Administrator 版本 5.5 用户指南

此版本的 Server Administrator 中有以下新增功能:

- 1 支持以下 Storage Management Service 功能:
 - 1 控制器任务 - 管理正在使用的高速缓存、外部配置导入预览、外部配置操作、清除外部策略、更改控制器属性、负载均衡、可恢复热备份、发生预测故障时自动更换
 - 1 虚拟磁盘任务 - 更换成员磁盘、更改策略 (磁盘高速缓存策略)

 **注:** 有关支持的操作系统列表, 请参阅 Dell 所提供介质的 DVD_Drive\docs\readme\PEOSOM 上或 Dell 支持网站 support.dell.com 上的《Dell 系统软件支持值表》。

5.5 DVD 结构

5.5 Systems Management Tools and Documentation DVD 包含:

目录	Version
Systems Build and Update Utility	1.0.7
ISO 映像 (Dell Systems Build and Update Utility)	1.0
ISO 映像 (Dell Systems and Console Agent CD (Dell OpenManage 软件))	5.3.0.1

可以使用 DVD 根目录中的 ISO 映像为没有 DVD 驱动器的系统创建 CD。

但是, 如果需要 1.0.7 版 Dell Systems Build and Update Utility (以支持 x6xx 和 x7xx Dell 系统以及 Windows Server 2008 操作系统), 可从 Dell 支持网站 support.dell.com 下载 ISO 映像。还可以从 Dell 支持网站 support.dell.com 下载 5.5 版 Dell OpenManage Server Administrator 和 Dell OpenManage Management Station 软件的 Web 软件包。可以为没有 DVD 驱动器的系统将这些 Web 软件包的内容传输到 CD 或 USB 闪存盘。

[目录](#)