

安装指南

[简介](#)

[Dell OpenManage 安全保护](#)

[设置和管理](#)

[Server Administrator 的部署情况](#)

[在 Microsoft Windows 操作系统上安装 Managed System Software](#)

[在 Microsoft Windows Server 2008 Core 和 Microsoft Hyper-V Server 上安装 Dell OpenManage 软件](#)

[在支持的 Linux 操作系统上安装 Managed System Software](#)

[VMware ESXi 上的 Dell OpenManage](#)


[使用 Microsoft Active Directory](#)

[前提条件检查程序](#)

[常见问题](#)

[OpenManage Linux 安装程序软件包](#)

注和小心

 **注：**“注”表示可以帮助您更好地使用计算机的重要信息。

 **小心：**“注意”表示如果不遵循说明，就有可能损坏硬件或导致数据丢失。

本说明文件中的信息如有更改，恕不另行通知。
© 2010 Dell Inc. 版权所有，翻印必究。

未经 Dell Inc. 书面许可，严禁以任何形式复制这些材料。

本文中使用的商标：Dell、DELL 徽标、OpenManage、PowerEdge、PowerConnect 和 PowerVault 是 Dell Inc. 的商标；Microsoft、Windows、Windows NT、Windows Server、Vista、Hyper-V 和 Active Directory 是 Microsoft Corporation 在美国和/或其它国家/地区的商标或注册商标；Red Hat 和 Red Hat Enterprise Linux 是 Red Hat, Inc. 在美国和其它国家/地区的注册商标；VMware 是 VMware Inc 在美国和/或其它管辖区的注册商标；ESX Server 是其商标；Novell、SUSE 和 ConsoleOne 是 Novell, Inc. 在美国和其它国家/地区的注册商标；Linux 是 Linus Torvalds 的注册商标；UNIX 是 The Open Group 在美国和其它国家/地区的注册商标；Intel 是 Intel Corporation 在美国 和其它国家/地区的注册商标；Citrix 和 XenServer 是 Citrix Systems, Inc. 在美国和/或其它国家/地区的注册商标或商标。

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. 对其它公司的商标和产品名称不拥有任何所有权。

2010 年 4 月

Server Administrator 的部署情况

安装指南

● [Managed System 上的 Server Administrator 组件](#)

您可以以下方法安装 Dell™ OpenManage™ Server Administrator:

- 1 在任何系统（Dell PowerEdge 系统、膝上型计算机或台式机）上安装 Server Administrator Web Server，并在另一个支持的 Dell PowerEdge™ 系统上安装 Server Instrumentation


采用此方法时，Server Administrator Web Server 执行中央 Web Server 的功能，您可以使用它监控众多 Managed System。采用此方法可以减少 Server Administrator 在 Managed System 上占用的资源。

- 1 继续在同一系统上安装 Server Administrator Web Server 和 Server Instrumentation

[表 4-1](#) 列出安装和使用 Server Administrator 的部署情况，并帮助您在选择各个安装选项时做出正确的选择：

表 4-1. 部署情况

目的	选择
从系统（可能是膝上型计算机、台式机或服务器）远程管理和监测 Managed System 的整个网络。	Server Administrator Web Server。然后，必须在 Managed System 上安装 Server Instrumentation。
管理和监测当前系统。	Server Administrator Web Server + Server Instrumentation。
使用其它一些远程系统管理和监测当前系统。	Remote Enablement 对于在 Microsoft Windows 上运行的系统，Remote Enablement 位于 Server Instrumentation 选项下面。然后，必须在远程系统上安装 Server Administrator Web Server。
查看连接到 Managed System 的本地存储设备和远程存储设备的状态，并在集成图形视图中获得存储设备管理信息。	Storage Management。
远程访问无法运行的系统、当系统停机时接收警报通知和远程重新启动系统。	Remote Access Controller。

 **注：** 在安装 Managed System Software 之前使用操作系统介质在 Managed System 上安装 SNMP 代理程序。

Managed System 上的 Server Administrator 组件

安装程序既提供“Custom Setup”（自定义安装）选项，也提供“Typical Setup”（典型安装）选项。

“Custom Setup”（自定义安装）选项使您可以选择要安装的软件组件。[表 4-2](#) 列出在自定义安装过程中可以安装的各个 Managed System Software 组件。有关自定义安装选项的详情，请参阅[“自定义安装”](#)。

表 4-2. Managed System Software 组件

组件	安装内容	部署情况	安装到的系统
Server Administrator Web Server	允许您本地或远程管理系统的基于 Web 的系统管理功能	如果想从系统远程监测 Managed System，则仅安装 Server Administrator Web Server。不需要实际接触到 Managed System。	任何系统。例如，膝上型计算机、台式机或 Dell PowerEdge 系
注： 如果要远程管理在 Windows 和 Linux 操作系统上运行的多个系统，建议在 Windows 操作系统上安装 Server Administrator Web Server。			
Server Instrumentation	Server Administrator CLI + Instrumentation Service	安装 Server Instrumentation 以便将系统用作 Managed System。安装 Server Instrumentation 和 Server Administrator Web Server 时，将会安装 Server Administrator。可以使用 Server Administrator 监测、配置和管理系统。 注： 如果选择仅安装 Server Instrumentation（没有选择 Remote Enablement），则还必须安装 Server Administrator Web Server。	支持的 Dell PowerEdge 系统。有关支持的 Dell PowerEdge 请参阅 Dell 支持网站 support.dell.com/support/edocs/software/omswarel 上的《Dell 系统软件支持值表》。
存储设备管理	Server Administrator Storage Management	安装 Storage Management 以实现硬件 RAID 解决方案并配置连接到系统的存储组件。有关 Storage Management 的详情，请参阅 docs 目录或 Dell 支持网站 support.dell.com/support/edocs/software/omswarel/index.htm 上的《Dell OpenManage Server Administrator Storage Management 用户指南》。	仅限于安装了 Server Instrumentation 或 Remote Enabler 系统。
Remote Enablement	Server Administrator CLI + Instrumentation Service + CIM 提	安装 Remote Enablement 以执行远程系统管理任务。可以在系统上安装 Remote Enablement，而在另一个系统（比如系统 X）上仅安装 Server Administrator Web Server。然后，可以使用系统 X 远程监测和管理您的系统。可以使用系统 X 管理任意个安装了 Remote Enablement 的系统。	支持的 Dell PowerEdge 系统。有关支持的 Dell PowerEdge 请参阅 Dell 支持网站 support.dell.com/support/edocs/software/omswarel 上的《Dell 系统软件支持值表》。

	供程序		
Remote Access Controller	Server Administrator CLI + Instrumentation Service + iDRAC 或 DRAC 5 或 DRAC 4 (取决于 Dell PowerEdge 系统的类型)	安装 Remote Access Service 以接收与电压、温度和风扇速度相关警告或错误的电子邮件警报。Remote Access Service 还可记录事件数据和最近一次的崩溃屏幕 (仅在运行 Microsoft Windows 操作系统的系统上提供) 以帮助诊断系统崩溃的可能原因。	仅限于安装了 Server Instrumentation 或 Remote Enabler 系统。
Intel SNMP Agent	Intel SNMP Agent	安装此 SNMP 代理程序以使 Server Administrator 能够获取有关网络接口卡 (NIC) 的信息。此 SNMP 代理程序有助于识别 NIC。	仅在安装了 Server Instrumentation 且运行 Microsoft Windows 的 Dell PowerEdge 系统上。
Broadcom SNMP Agent	Broadcom SNMP Agent	安装此 SNMP 代理程序以使 Server Administrator 能够获取有关 NIC 的信息。此 SNMP 代理程序有助于识别 NIC。	仅在安装了 Server Instrumentation 且运行 Microsoft Windows 的 Dell PowerEdge 系统上。

[目录](#)

[目录](#)

常见问题

安装指南

- [一般信息](#)
- [Microsoft® Windows®](#)
- [Red Hat® Enterprise Linux® 或 SUSE® Linux Enterprise Server](#)

一般信息

如何安装只具有 CLI 功能的 Dell OpenManage Server Administrator?

通过选择不安装 Server Administrator Web Server, 将只得到 CLI 功能。

Dell OpenManage 应用程序使用哪些端口?

Server Administrator 使用的默认端口是 1311。Dell OpenManage™ IT Assistant 使用的默认端口是 2607 (用于连接服务) 和 2606 (用于网络监测服务)。这些端口均可以配置。有关特定组件的端口信息, 请参阅该相应组件的《用户指南》。

当在低带宽和存在延迟的情况下通过广域网 (WAN) 在 DRAC 控制器上运行虚拟介质时, 在虚拟介质上直接启动 OpenManage 安装程序时失败, 我该怎么办?

如果出现故障, 首先将 Web 安装软件包 (可从 support.dell.com 获得) 直接复制到本地系统, 然后从本地系统直接启动 Dell OpenManage 安装程序。

我是否需要安装 Server Administrator Storage Management Service 之前先卸载已安装在系统上的 Adaptec Fast Console 应用程序?

是的, 如果系统上已安装 Adaptec Fast Console, 则必须在安装 Server Administrator Storage Management Service 之前卸载该应用程序。


Microsoft® Windows®

如何修补 Server Administrator 的安装故障?

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。
- 1 从 Dell 支持网站 support.dell.com 中下载该版本的安装软件包。
- 1 从 `SYSGMT\sradmin\windows\SystemManagement` 目录中找到 `SysMgmt.msi`, 并在命令提示符处输入以下命令以强制执行重新安装。

```
msiexec /i SysMgmt.msi REINSTALL=ALL REINSTALLMODE=vomus
```
- 1 选择“Custom Setup” (自定义安装) 并选择原来安装的所有功能。如果您不能肯定最初安装的是哪些功能, 则可选择所有功能并进行安装。

 **注:** 如果 Server Administrator 安装在非默认目录下, 则一定也要在“Custom Setup” (自定义安装) 中更改。

一旦应用程序安装后, 可从“Add/Remove Programs” (添加/删除程序) 中进行卸载。

当创建 WinRM listener 失败并显示错误信息“The CertificateThumbprint property must be empty when the SSL configuration will be shared with another service” (当 SSL 配置将与其它服务共享时 CertificateThumbprint 属性必须为空) 时, 我该怎么办?

当已经安装 Internet Information Server (IIS) 并配置 HTTPS 通信时会遇到上述错误。有关 IIS 和 WinRM 共存的详情, 请参阅: technet.microsoft.com/en-us/library/cc782312.aspx。

在这种情况下, 可以通过以下命令使用 `CertificateThumbprint empty` 创建 HTTPS 侦听器。

例如: `winrm create winrm/config/Listener?Address=*&Transport=HTTPS @{Hostname=<主机名称>;CertificateThumbprint=""}`

需要为 WinRM 进行哪些防火墙相关的配置?

在防火墙打开 (ON) 的情况下, 需要将 WinRM 添加到防火墙排除列表以允许 HTTPS 通信所需的 TCP 端口 443。

当启动 Dell OpenManage 安装程序时, 可能会显示错误信息, 表明载入特定程序库失败、拒绝访问或初始化错误。Dell OpenManage 安装期间出现安装失败的例子: “failed to load OMIL32.DLL.” (载入 OMIL32.DLL 失败)。我该怎么办?

原因很可能是由于系统上的 COM 权限不足。请参阅以下文章处理这种情况: support.installshield.com/kb/view.asp?articleid=Q104986

如果以前安装 Dell OpenManage 系统管理软件或其它软件产品不成功, 则 Dell OpenManage 安装也可能失败。可以删除临时 Windows 安装程序注册表项, 这有可能帮助解决 Dell OpenManage 安装故障问题。如果出现以下注册表项, 可以删除该项:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Installer\InProgress
```

我在 Dell OpenManage 安装过程中收到误导的警告/错误信息。

如果 Windows 系统驱动器上的磁盘空间不足，则运行 Dell OpenManage 安装程序时可能会遇到误导的警告或错误信息。另外，Windows 安装程序还需要一些磁盘空间以便将安装程序软件包临时解压到 %TEMP% 文件夹。运行 Dell OpenManage 安装程序之前请确保系统驱动器拥有足够的磁盘空间（100 MB 或更多）。

启动 Dell OpenManage 安装程序时，我收到错误信息“An older version of Server Administrator software is detected on this system.You must uninstall all previous versions of Server Administrator applications before installing this version”（在此系统中检测到较早版本的 Server Administrator 软件。在安装此版本之前，必须卸载所有以前版本的 Server Administrator 应用程序），我该怎么办？

如果在尝试启动 Dell OpenManage 安装程序时看到此错误，建议您运行 SYSMGMT\sradmin\support\OMClean 目录下的 OMClean.exe 程序，以便删除系统上较早版本的 Server Administrator。

在安装 Citrix Metaframe 之前是否需要卸载以前版本的 Server Administrator？

是。在安装 Citrix Metaframe（所有版本）之前必须卸载以前版本的 Server Administrator。因为 Citrix Metaframe 安装后注册表中可能会存在错误，所以需要重新安装 Server Administrator。

运行 Dell OpenManage 安装程序时，前提条件检查信息屏幕上为什么会出难以理解的字符？

当运行英语、德语、法语或西班牙语的 Dell OpenManage 安装程序并在“Prerequisite Check Information”（前提条件检查信息）屏幕出现难以理解的字符时，请确保浏览器编码包含默认的字符集。重设浏览器编码以使用默认字符集可以解决这个问题。

在相同目录中安装 Server Administrator 和 Dell Online Diagnostics 后，Dell Online Diagnostics 无法工作，我该怎么办？

如果在相同的目录中安装 Server Administrator 和 Online Diagnostics，则 Online Diagnostics 可能无法正常工作。而且稍后卸载 Server Administrator 之后，还可能丢失所有 Online Diagnostics 文件。要避免出现该问题，请在不同的目录中安装 Server Administrator 和 Online Diagnostics。一般情况下，建议不要在相同的目录中安装多个应用程序。

我已使用部署在 Windows Server 2008 上的远程 Server Administrator 安装 Server Administrator，但为何在桌面上看不到 Server Administrator 图标？

使用部署在运行 Windows 2008 的服务器上的远程 Server Administrator 首次安装 Server Administrator 后（OMSA 推送），Server Administrator 图标将在手工刷新桌面后才显示。例如，可以通过按 <F5> 键刷新桌面。

在 Microsoft Windows Server 2008 上卸载 Server Administrator 的过程中，为什么安装程序尝试删除快捷方式链接时，我会看到警告信息？

在卸载 Microsoft Windows Server 2008 上的 Server Administrator 的过程中，安装程序尝试删除快捷方式链接时可能会看到警告信息。请单击警告信息上的“OK”（确定）继续卸载。

在哪里可以找到 MSI 日志文件？

默认情况下，MSI 日志文件存储在 %TEMP% 环境变量定义的路径中。

我从 Dell 支持网站下载了用于 Windows 的 Server Administrator 文件并将其复制到自己的介质上。当尝试启动 SysMgmt.msi 文件时失败。问题出在哪里？

如果 MSI 文件没有位于 DVD 的根目录，则 MSI 要求所有的安装程序都要指定 MEDIAPACKAGEPATH 属性。

对于 Managed System Software MSI 软件包，此属性设置为 SYSMGMT\sradmin\windows\SystemManagement。如果决定制作自己的 DVD，必须确保 DVD 布局保持一致。SysMgmt.msi 文件必须位于 SYSMGMT\sradmin\windows\SystemManagement 中。有关更多的详细信息，请转至 msdn.microsoft.com 并搜索：MEDIAPACKAGEPATH Property。

Dell OpenManage 安装程序是否支持 Windows 通告安装？

否。Dell OpenManage 安装程序不支持 Windows 的“通告”安装 - 通过 Windows 组策略自动分发程序到客户端计算机进行安装的过程。

如何在自定义安装过程中检查磁盘空间的可用性？

在“Custom Setup”（自定义设置）屏幕上，必须单击某个激活的功能以查看硬盘驱动器空间可用性或更改安装目录。例如，如果选择安装功能 A（激活）而功能 B 未激活，则单击功能 B 时“Change”（更改）和“Space”（空间）按钮将禁用。单击功能 A 可以查看空间可用性或更改安装目录。

当看到当前版本已安装的信息时，我该怎么办？

如果使用 MSP 从版本“X”升级到版本“Y”，然后尝试使用版本“Y”DVD（完整安装），则版本“Y”DVD上的前提条件检查程序将提示您当前版本已安装。如果继续，安装将不会运行在“Maintenance”（维护）模式且您将无法选择“Modify”（更改）、“Repair”（修复）或“Remove”（删除）选项。继续安装将删除 MSP 并创建版本“Y”软件包中存在的 MSI 文件的高速缓存。第二次运行时，安装程序将在“Maintenance”（维护）模式下运行。

使用前提条件检查程序信息的最佳方式是什么？

前提条件检查程序可用于 Windows。有关如何使用前提条件检查程序的详细信息，请参阅 *Dell Systems Management Tools and Documentation* DVD 上 SYSMGMT\sradmin\windows\PreReqChecker\readme.txt 中的自述文件。

在前提条件检查程序屏幕中，得到信息“An error occurred while attempting to execute a Visual Basic Script.Please confirm that Visual Basic files are installed correctly.”（尝试执行 Visual Basic 脚本时出错。请确认 Visual Basic 文件安装正确。）应该如何解决这个问题？

当前前提条件检查程序调用 Dell OpenManage 脚本 vbstest.vbs（visual basic 脚本）验证安装环境时会出现此错误，并且脚本失败。

可能的原因有：

- 1 错误的 Internet Explorer 安全设置。

请确保“Tools”（工具）→“Internet Options”（Internet 选项）→“Security”（安全）→“Custom Level”（自定义级别）→“Scripting”（脚本）→“Active Scripting”（活动脚本）设置为“Enable”（启用）。

请确保“Tools”（工具）→“Internet Options”（Internet 选项）→“Security”（安全）→“Custom Level”（自定义级别）→“Scripting”（脚本）→“Scripting of Java Applets”（Java 小程序脚本）设置为“Enable”（启用）。

- 1 Windows Scripting Host (WSH) 已禁用 VBS 脚本的运行。默认情况下, WSH 在操作系统安装期间安装。可以将 WSH 配置为阻止具有 .VBS 扩展名的脚本运行。
 - e. 右击桌面上的“My Computer”（我的电脑）并单击“Open”（打开）→ “Tools”（工具）→ “Folder Options”（文件夹选项）→ “File Types”（文件类型）。
 - f. 寻找 VBS 文件扩展名并确保“File Types”（文件类型）设置为“VBScript Script File”（VBScript 脚本文件）。
 - g. 如果没有, 则单击“Change”（更改）并选择 Microsoft Windows Based Script Host 作为进行调用以运行脚本的应用程序。
- 1 WSH 是错误的版本、已损坏或未安装。默认情况下, WSH 在操作系统安装期间安装。从 msdn.microsoft.com 下载 WSH。

Windows Installer Services 在安装/卸载过程中显示的时间是否准确?

否。在安装/卸载过程中, Windows Installer Service 会显示完成当前任务的剩余时间。这只是 Windows 安装程序引擎根据各种因素得出的近似值。

是否可以在不运行前提条件检查程序的情况下启动安装? 如何做到?

是, 可以。例如, 您可以直接从 `SYSMGMT\srvadmin\Windows\SystemManagement` 运行 Managed System Software 的 MSI。一般来说, 跳过前提条件检查信息不是个好主意, 因为其中可能包含您并不知道的重要信息。

如何得知系统上所装 Systems Management Software 的版本?

转至“Start”（开始）→ “Settings”（设置）→ “Control Panel”（控制面板）→ “Add/Remove programs”（添加/删除程序）并选择 Dell OpenManage Server Administrator。选择[支持信息](#)的链接。

升级 Dell OpenManage 后是否需要重新引导系统?

如果要升级的文件正在使用中, 可能需要重新引导才能升级。这是 Windows 安装程序的典型行为。在出现此类提示时, 建议重新引导系统。

在哪里可以查看到目前系统上已安装的 Server Administrator 功能?

请参阅 Windows 的“Add/Remove Programs”（添加/删除程序）了解当前已安装 Server Administrator 功能。

Dell OpenManage 的各项功能在 Windows 中的名称是什么?

下表列出了所有 Dell OpenManage 功能的名称以及在 Windows 中的相应名称。

表 11-1. Windows 下的 Dell OpenManage 功能

部件	Windows 中的名称
Managed System Services	
Server Administrator Instrumentation Service	DSM SA 数据管理器 DSM SA 事件管理器
Server Administrator	DSM SA 连接服务 DSM SA 共享服务
Server Administrator Storage Management Service	Mr2kserv
Remote Access Controller 控制台 (DRAC 4)	Remote Access Controller 4 (DRAC 4)

Red Hat® Enterprise Linux® 或 SUSE® Linux Enterprise Server

安装 Server Administrator 后, 我无法登录。

安装 Server Administrator 后, 先注销, 然后重新登录以访问 Server Administrator 命令行界面 (CLI)。

我尝试在来宾 Linux 操作系统上安装 Server Administrator 时, 看到以下信息: ./srvadmin-install.sh: line 2295 : [: ==: unary operator expected (./srvadmin-install.sh: line 2295 : [: ==: 应为一元运算符)

在来宾 Linux 操作系统上安装 Dell OpenManage 组件时, 可能会显示警告信息。但是, 安装会继续进行和完成, 而不会丢失任何功能。

我手动安装了 Red Hat Enterprise Linux 4 - x86_64 操作系统, 并在尝试安装 Server Administrator 时可以看到 RPM 相关性。在哪里能找到这些相关 RPM 文件?

对于 Red Hat Enterprise Linux 而言, 相关 RPM 文件位于 Red Hat Enterprise Linux 安装介质中。所有其它 RPM 位于 `/SYSMGMT/srvadmin/linux/RPMS/supportRPMS/opensource-components` 目录中。

要安装或更新所有相关 RPM 文件, 应执行以下命令:

```
rpm -ivh /SYSMGMT/srvadmin/linux/RPMS/
supportRPMS/opensource-components
```

然后就可以继续 Server Administrator 安装了。

我使用 Linux 操作系统介质执行 Linux 操作系统的非默认安装, 在安装 Server Administrator 时看到丢失的 RPM 文件相关性该怎么办?

Server Administrator 是 32 位应用程序。当安装在运行 Enterprise Linux 64 位版本操作系统的系统上时，Server Administrator 仍然是 32 位应用程序，而 Server Administrator 安装的设备驱动程序是 64 位。如果尝试为 Intel EM64T 在运行 Red Hat Enterprise Linux (版本 4 和版本 5) 的系统上安装 Server Administrator，请确保安装丢失 RPM 文件相关性的相应 32 位版本。32 位 RPM 版本的文件扩展名中总是包含 **i386**。您还可能会遇到共享目标文件（文件扩展名中包含 **so**）相关性失败。在这种情况下，可以通过使用 `RPM --whatprovides` 开关确定安装共享对象时需要哪个 RPM。例如：

```
rpm -q --whatprovides libpam.so.0
```

应该返回 RPM 名称（如 **pam-0.75-64**），因此您可以获取并安装 **pam-0.75-64.i386.rpm**。当 Server Administrator 安装在运行 64 位版本 Linux 操作系统的系统上时，请确保安装 **compat-libstdc++-<版本>.i386.rpm** RPM 软件包。需要通过从 Linux 操作系统介质安装丢失的 RPM 文件手工解决相关性问题。

注： 如果使用支持的 Linux 操作系统的更高版本，并且兼容 DVD `SYSMGMT/srvadmin/linux/RPMS/supportRPMS` 目录中提供的 RPM 文件，则可以使用来自操作系统介质中的最新 RPM。

在哪里可以找到开放源代码 RPM 的源软件包？

开放源代码 RPM 的源软件包可从订购的 DVD 映像中获得。

当由于缺少 RPM 文件而导致 Management Station RAC 公用程序安装失败时，该怎么办？

在安装 Management Station RAC 公用程序（*Dell Systems Management Tools and Documentation* DVD 上 `SYSMGMT/ManagementStation/linux/rac` 目录下的 `mgmtst-racadm` RPM）过程中，可能会由于 `libstdc++.so` 程序库缺少 RPM 文件相关性而导致安装失败。可以通过安装同一目录下的 **compat-libstdc++ rpm** 解决相关性问题并重新安装。

当使用 `rpm -e 'rpm -qa | grep srvadmin'` 命令删除 Dell OpenManage 系统管理软件时，一些 RPM 公用程序版本可能会按照错误的顺序卸载，这将导致用户收到误导的警告或错误信息。有什么解决方法？

解决方法是使用 DVD 上提供的 Dell OpenManage 卸载脚本 `srvadmin-uninstall.sh`。

当要求使用 root 用户帐户进行身份验证时，我该做什么？

Dell Systems Build and Update Utility 向 root 用户的 `.bash_profile` 文件添加了一个脚本，它将提示安装 Dell OpenManage 系统管理软件。该脚本可能会干预使用系统 root 用户帐户进行身份验证的远程客户端应用程序，但无法处理用户提示。要解除该限制，可以编辑 `.bash_profile` 文件并注释以下行：`[S{SHLVL}...`

在卸载过程中，显示 `error: %preun(srvadmin-NAME-X.Y.Z-N.i386) scriptlet failed, exit status 1` 错误信息。

手工 RPM 升级未成功之后，卸载 Server Administrator 时可能出现该问题。您将看到以下错误信息：

```
"error: %preun(srvadmin-NAME-X.Y.Z-N.i386) scriptlet failed, exit status 1" (错误: %preun(srvadmin-NAME-X.Y.Z-N.i386) Scriptlet 失败, 退出状态 1)
```

在这种情况下，NAME 表示功能名称，例如 `omacore`。X.Y.Z-N 是该功能的版本和内部版本号。可以解决该问题的解决方法有：

1. 尝试再次卸载。例如，使用以下命令：

```
rpm -e srvadmin-NAME-X.Y.Z-N.i386
```

2. 如果 `/etc/omreg.cfg` 文件中存在“`upgrade.relocation=bad`”行，则删除该行后尝试再次卸载。

为什么在安装期间得到一条关于 RPM 软件包密钥的警告？

RPM 文件使用数字签名进行了签名。要避免此警告，应安装介质或软件包，并使用如下的命令导入密钥：

```
rpm --import /mnt/dvdrom/SYSMGMT/srvadmin/linux/RPM-GPG-KEY
```

Red Hat Enterprise Linux 或 SUSE Linux Enterprise Server 下所有 Dell OpenManage 功能的名称都是什么？

下表列出了 Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统下所有 Dell OpenManage 功能及其相应 init 脚本的名称：

表 11-2. Red Hat Enterprise Linux 下 Dell OpenManage 功能 SUSE LINUX Enterprise Server

部件	在 VMware ESX、Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 中的名称
Managed System Services 功能	功能 init 脚本名称
DSM SA 设备驱动程序	<code>instsvcdrv</code>
DSM SA Data Engine 服务	<code>dataeng</code>
DSM SA 共享服务	<code>dsm_om_shrsvc</code>
DSM SA 连接服务	<code>dsm_om_connsvc</code>
DSM SM LSI 管理器	<code>mpctl</code>
集成的 Dell Remote Access Controller (iDRAC)	无
Remote Access Controller (DRAC 4)	<code>racsvc</code>
Remote Access Controller (DRAC 5)	无

srvadmin/linux/custom/<操作系统> 下目录中包含什么内容？

下表列出了 SYSMGMT/srvadmin/linux/custom/<操作系统> 目录中各目录的名称。

表 11-3. srvadmin/linux/custom/<操作系统> 目录下各目录的名称

RPM 的名称	说明	其它需要的 Server Administrator RPM
Server-Instrumentation — 这是 Server Administrator 的核心代码。它提供主板警报并包含用于监控和控制 Server Administrator 的 CLI，如 omconfig、omdiag 和 omreport。除独立 DRAC 支持外，所有外围设备软件包都需要安装此目录中的全部或多数 RPM。  注： 为确保功能正常，可能还需要安装 IPMI 驱动程序。		
srvadmin-om	Server Administrator 资源注册收集程序 — 系统管理更改管理资源注册收集程序。	srvadmin-omilcore、srvadmin-deng 和 srvadmin-omacore。
srvadmin-deng	Server Administrator Data Engine — 系统管理为系统管理软件提供一个数据管理框架。	srvadmin-omilcore
srvadmin-hapi	Server Administrator 硬件应用程序编程接口 — 此系统管理软件包提供系统管理软件访问所支持系统中硬件信息所需的设备驱动程序和程序库。	srvadmin-omilcore
srvadmin-isvc	Server Administrator Instrumentation Service — Server Administrator 提供一整套使网络上所支持系统保持良好运行状况的系统管理信息。Server Administrator Instrumentation Service 为管理应用程序提供故障管理信息、故障前兆信息以及资产和库存信息。Instrumentation Service 监控系统的运行状况并提供对所支持系统上硬件的详细故障和性能信息的快速访问。Instrumentation Service 要求安装系统管理设备驱动程序。	srvadmin-omilcore、srvadmin-deng 和 srvadmin-hapi
srvadmin-omacore	Server Administrator — 由系统管理的管理型模式核心和 CLI。	srvadmin-omilcore 和 srvadmin-deng
srvadmin-omhip	Server Administrator Instrumentation Service Integration Layer — 提供设备 CLI。	srvadmin-omilcore、srvadmin-deng、srvadmin-hapi、srvadmin-isvc 和 srvadmin-omacore
srvadmin-omilcore	Server Administrator Install Core — 它是核心安装软件包，提供其它系统管理安装软件包所需的工具。所有 Server Administrator RPM 都需要此 RPM。	
srvadmin-syscheck	检查 OpenManage 支持级别的软件包。	srvadmin-omilcore
add-iDRAC — 用于第三代 Remote Access Controller 的远程管理软件。 例如：iDRAC。		
srvadmin-idrac-components	集成的 Dell Remote Access Card Data Populator Remote Access Controller 组件。	srvadmin-omilcore、srvadmin-deng、srvadmin-hapi 和 srvadmin-racser
srvadmin-idracadm	iDRAC 命令界面 — Integrated Dell Remote Access Controller 的命令行用户界面。	srvadmin-omilcore
srvadmin-idracrsc	iDRAC Integration Layer — Server Administrator 的 Integrated Dell Remote Access CLI 和 Web 插件	srvadmin-omilcore、srvadmin-deng、srvadmin-rac4 组件和 srvadmin-omacore
add-RAC4 — 用于第四代 Remote Access Controller 的远程管理软件。 如：DRAC 4。		
srvadmin-rac4-components	远程访问卡 Data Populator — Remote Access Controller 组件。	srvadmin-omilcore、srvadmin-deng、srvadmin-hapi 和 srvadmin-racsvc
srvadmin-racadm4	RAC 命令界面 — Remote Access Controller (RAC) 的命令行用户界面。	srvadmin-omilcore
srvadmin-racdrsc4	DRAC 4 Integration Layer — 用于 Server Administrator 的远程访问 CLI 和 Web 插件。	srvadmin-omilcore、srvadmin-deng、srvadmin-rac4 组件和 srvadmin-omacore
srvadmin-racsvc	远程访问卡管理型节点 — 支持服务器群集的中央管理和分布式资源远程管理的 Remote Access Controller (RAC) 服务。	srvadmin-omilcore
add-RAC5 — 用于第五代 Remote Access Controller 的远程管理软件。 如：DRAC 5。		
srvadmin-rac5-components	远程访问卡 Data Populator、DRAC 5 和 Remote Access Controller 组件，DRAC 5。	srvadmin-omilcore、srvadmin-deng 和 srvadmin-hapi
srvadmin-racadm5	RAC 命令界面 — Remote Access Controller (RAC) 的命令行用户界面。	srvadmin-omilcore 和 srvadmin-hapi
srvadmin-racdrsc5	DRAC 5 Integration Layer — 用于 Server Administrator 的远程访问 CLI 和 Web 插件	srvadmin-omilcore、srvadmin-deng、srvadmin-omacore 和 srvadmin-rac5 组件
add-StorageManagement — Storage Management RAID 配置公用程序和存储警报软件		
srvadmin-storage	Storage Management — 提供系统管理存储服务。	srvadmin-omilcore、srvadmin-deng、srvadmin-omacore 和 srvadmin-odf
SA-WebServer — 提供对服务器管理的 Web 访问		
srvadmin-hapi	Server Administrator 硬件应用程序编程接口 — 此系统管理软件包提供系统管理软件访问所支持系统中硬件信息所需的设备驱动程序和程序库。	srvadmin-omilcore
srvadmin-iws	安全端口服务器 — 系统管理型节点 Web Server 软件包。	srvadmin-omilcore、srvadmin-

		deng、srvadmin-omacore 和 srvadmin-jre
srvadmin-jre	Server Administrator Sun Java Runtime 环境 — 由系统管理所管理的节点 Java 运行时间。	srvadmin-omilcore、srvadmin-deng 和 srvadmin-omacore
srvadmin-omauth	提供验证文件。	srvadmin-omilcore
srvadmin-omcommon	提供 Server Administrator 所需的通用框架。	srvadmin-omilcore
srvadmin-omilcore	Server Administrator Web Server Install Core — 这是核心安装软件包。所有 Server Administrator Web Server RPM 都需要该 RPM。	
srvadmin-wsmanclient	操作系统特定的 WSMan 客户端软件包。	srvadmin-omcommon 和 srvadmin-omauth
Remote-Enablement — 使用其它一些远程系统管理和监测当前系统		
srvadmin-cm	Server Administrator 资源注册收集程序 — 系统管理更改管理资源注册收集程序。	srvadmin-omilcore、srvadmin-deng 和 srvadmin-omacore。
srvadmin-deng	Server Administrator Data Engine — 系统管理为系统管理软件提供一个数据管理框架。	srvadmin-omilcore
srvadmin-hapi	Server Administrator 硬件应用程序编程接口 — 此系统管理软件包提供系统管理软件访问所支持系统中硬件信息所需的设备驱动程序和程序库。	srvadmin-omilcore
srvadmin-iscv	Server Administrator Instrumentation Service — Server Administrator 提供一整套使网络上所支持系统保持良好运行状况的系统管理信息。Server Administrator Instrumentation Service 为管理应用程序提供故障管理信息、故障前兆信息以及资产和库存信息。Instrumentation Service 监控系统的运行状况并提供对所支持系统上硬件的详细故障和性能信息的快速访问。Instrumentation Service 要求安装系统管理设备驱动程序。	srvadmin-omilcore、srvadmin-deng 和 srvadmin-hapi
srvadmin-omacore	Server Administrator — 由系统管理的管理型模式核心和 CLI。	srvadmin-omilcore 和 srvadmin-deng
srvadmin-omcommon	提供 Server Administrator 所需的 Common Framework。	srvadmin-omilcore
srvadmin-omhip	Server Administrator Instrumentation Service Integration Layer — 提供设备 CLI。	srvadmin-omilcore、srvadmin-deng、srvadmin-hapi、srvadmin-iscv 和 srvadmin-omacore
srvadmin-omilcore	Server Administrator Install Core — 它是核心安装软件包，提供其它系统管理安装软件包所需的工具。所有 Server Administrator RPM 都需要此 RPM。	
srvadmin-ssa	实现从安装 Server Administrator Web Server 的远程系统通过 WS-Man 界面管理系统。	srvadmin-omacore、srvadmin-omhip 和 srvadmin-iscv。
srvadmin-syscheck	检查 OpenManage 支持级别的软件包。	srvadmin-omilcore

已安装 Server Administrator 的系统上还可安装哪些附加组件？

已安装 Server Administrator 的系统上还可以安装一些附加组件。例如，可以在以前已安装 Managed System Software 的系统上安装 Online Diagnostics。在这种系统上卸载 Server Administrator 时，仅卸载任何新安装的组件都不需要的那些 RPM 软件包。在上面的示例中，

Online Diagnostics 需要一些软件包，例如 -

srvadmin-omilcore-X.Y.Z-N 和 **srvadmin-hapi-X.Y.Z-N**。在 Server Administrator 卸载过程中将不会卸载这些软件包。

在这种情况下，如果稍后通过运行

```
sh srvadmin-install.sh
```

命令尝试安装 Server Administrator，将得到以下信息：

Server Administrator version X.Y.Z is currently installed. (当前已安装 Server Administrator 版本 X.Y.Z。)

Installed Components are: (已安装的组件包括:)

```
1 srvadmin-omilcore-X.Y.Z-N
```

```
1 srvadmin-hapi-X.Y.Z-N
```

Do you want to upgrade Server Administrator to X.Y.Z? (是否要将 Server Administrator 升级到 X.Y.Z?) Press (y for yes | Enter to exit): (按 [y 代表是" | Enter 代表"退出"]：)

按 **y** 后，仅升级系统上存在的 Server Administrator 软件包（在上例中为 **srvadmin-omilcore-X.Y.Z-N** 和 **srvadmin-hapi-X.Y.Z-N**）。

如果还必须安装其它 Dell OpenManage 组件，则需要再次运行以下命令：

```
sh srvadmin-install.sh
```

如果在不支持的系统或不支持的操作系统上安装 RPM 软件包将会发生什么情况？

如果尝试在不支持的系统或不支持的操作系统上安装 RPM 软件包，在安装、卸载或使用 RPM 软件包过程中可能会遇到不可预知的行为。大多数 RPM 软件包都针对 Dell PowerEdge™ 系统和自述文件中列出的 Linux 版本编写和测试。

Server Administrator 启动后，在 Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统上运行的守护程序是什么？

在 Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统上运行何种守护程序取决于具体安装了哪些程序以及哪些程序允许运行。下表显示完全安装情况下通常运行的守护程序：

表 11-4. 一旦 Server Administrator 启动后，在 Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 上运行的守护程序

守护程序名称	Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 中的名称
对于 srvadmin-base 目录中的 RPM	
dsm_sa_datamgr32d	DSM SA Data Manager — 由 DSM SA Data Engine 服务启动的 Server Administrator 数据管理器守护程序。
dsm_sa_eventmgr32d	DSM SA Event Manager — 由 DSM SA Data Engine 服务启动的 Server Administrator 事件和登录守护程序。
dsm_sa_snmp32d	DSM SA SNMP 守护程序 — 由 DSM SA Data Engine 服务启动的 Server Administrator SNMP 守护程序。
dsm_om_shrsvc32d	DSM SA 共享服务 — Server Administrator 核心守护程序。
对于 SA-WebServer 目录中的 RPM	
dsm_om_connsvc32d	DSM SA 连接服务 — Server Administrator Web server 守护程序。
对于支持 DRAC 4 的系统：add-RAC4	
racsvc	DRAC 4 管理员守护程序

Server Administrator 启动时载入的内核模块是什么？

这取决于系统设备的类型。下表显示了 Server Administrator 启动时载入的内核模块。

表 11-5. Server Administrator 服务启动时载入的内核模块

驱动程序名称	说明
对于有 IPMI 的系统	
dell_rbu	Dell BIOS 更新驱动程序
ipmi_devintf	IPMI 设备驱动程序
ipmi_msghandler	IPMI 设备驱动程序
ipmi_si	IPMI 设备驱动程序 — 针对运行 Red Hat Enterprise Linux (版本 4) 或 SUSE Linux Enterprise Server (版本 10) 的系统
对于 TVM 系统	
dcdbas	Dell Systems Management 基本驱动程序
dell_rbu	Dell BIOS 更新驱动程序
对于 ESM 系统	
dcdbas	Dell Systems Management 基本驱动程序
dell_rbu	Dell BIOS 更新驱动程序
对于 Server Administrator 存储系统的支持	
mptctl	LSI RAID 的设备驱动程序

[目录](#)

[目录](#)

VMware ESXi 上的 Dell OpenManage

安装指南

- [VMware ESXi 4.0 更新 1 和 ESXi 4.1 上的 Dell OpenManage](#)
- [在 Managed System 上启用 Server Administrator 服务](#)
- [在运行 VMware ESXi 4/ESXi 4.1 的系统上配置 SNMP 代理](#)

有些 Dell™ 系统在工厂预装了 VMware ESXi。有关这些系统的列表，请参阅 Dell 支持网站 support.dell.com/support/edocs/software/omswrels/index.htm 上的最新《Dell 系统软件支持值表》。您可以使用 Server Administrator Web Server 版本 6.3 访问 VMware ESXi 4.0 更新 1 和 VMware ESXi 4.1 系统。

VMware ESXi 4.0 更新 1 和 ESXi 4.1 上的 Dell OpenManage

Dell OpenManage Server Administrator 以 .zip 文件 ([oem-dell-openmanage-esxi_6.3.0-A00.zip](#)) 的形式提供，可安装在运行 VMware ESXi 4.0 更新 1 和 ESXi 4.1 的系统上。在 Dell 支持网站 support.dell.com 上可以下载 [oem-dell-openmanage-esxi_6.3.0-A00.zip](#) 文件。

从 vmware.com 下载 VMware vSphere 命令行界面 (vSphere CLI) 并安装在 Microsoft Windows 或 Linux 系统上。此外，可以将 VMware vSphere Management Assistant (vMA) 导入到 ESXi 4 或 ESXi 4.1 主机中。

使用 vSphere CLI


1. 将 [oem-dell-openmanage-esxi_6.3.0-A00.zip](#) 文件复制到系统上的一个目录中。
2. 如果您使用 Microsoft Windows，则导航至已安装 vSphere CLI 公用程序的目录，执行步骤 4 提及的命令。

如果您使用 Linux 上的 vSphere CLI，则可以从任何目录执行步骤 4 中的命令。

3. 关闭 ESXi 主机上的所有来宾操作系统，并将 ESXi 主机置于维护模式。

4. 执行以下命令：

```
vihostupdate.pl --server <ESXi 主机的 IP 地址> -i -b <Dell OpenManage 文件路径>
```

 **注：** 如果您使用 Linux 上的 vSphere CLI，则不需要 .pl 扩展名。

5. 出现提示时，输入 ESXi 主机的 root 用户名和密码。

命令输出显示更新成功或失败。如果更新失败，请参阅“[故障排除](#)”。

6. 重新启动 ESXi 主机系统。

使用 VMware vSphere Management Assistant

vSphere Management Assistant (vMA) 使管理员和开发人员可以运行脚本和代理程序来管理 ESX/ESXi 系统。有关 vMA 的详情，请参阅 vmware.com/support/developer/vma/。

1. 以管理员的身份登录 vMA，在出现提示时提供密码。
2. 将 [oem-dell-openmanage-esxi_6.3.0-A00.zip](#) 文件复制到 vMA 上的一个目录中。
3. 关闭 ESXi 主机上的所有来宾操作系统，并将 ESXi 主机置于维护模式。

4. 在 vMA 中，执行以下命令：

```
vihostupdate --server <ESXi 主机的 IP 地址> -i -b <Dell OpenManage 文件路径>
```

5. 出现提示时，输入 ESXi 主机的 root 用户名和密码。

命令输出显示更新成功或失败。如果更新失败，请参阅“[故障排除](#)”。

6. 重新启动 ESXi 主机系统。

运行命令时，将在系统上安装以下组件：

- 1 Server Administrator Instrumentation Service
- 1 Remote Enablement
- 1 Server Administrator Storage Management
- 1 Remote Access Controller

必须在 Management Station 上单独安装 Server Administrator Web Server。有关安装 Server Administrator Web Server 的信息，请参阅“在 [Microsoft Windows 操作系统上安装 Managed System Software](#)”和“在支持的 Linux 操作系统上安装 Managed System Software”。

 **注：** 确保仅安装 Server Administrator Web Server 版本 6.1 和更高版本。VMware ESXi 4.0 和更高版本不支持 Server Administrator Web Server 版本 6.0.3。

安装 Server Administrator 后，必须启用 Server Administrator 服务。有关启用这些服务的信息，请参阅“在 [Managed System 上启用 Server Administrator 服务](#)”。

故障排除

- 1 尝试使用 vhostupdate 命令时，可能会显示以下错误：

```
unpacking c:\oem-dell-openmanage-esxi_6.3.0-A00.zip (正在解压缩 c:\oem-dell-openmanage-esxi_6.3.0-A00.zip)
```

```
metadata.zip.sig does not exist (metadata.zip.sig 不存在)
```

```
signature mismatch : metadata.zip (签名不匹配: metadata.zip)
```

```
Unable to unpack update package. (无法解压缩更新软件包。)
```

如果您使用较早版本的远程 CLI，就会显示此错误。下载并安装 vSphere 版本的 CLI。

- 1 尝试使用 vhostupdate 命令时，可能会显示以下错误：

```
Unable to create, write or read a file as expected.I/O Error (28) on file : [Errno 28] No space left on device.
```

(无法按预期创建、写入或读取文件。文件出现 I/O 错误 (28)：[错误 28] 设备上没有剩余空间。)

请参阅 kb.vmware.com 上的 VMware 知识库文章 1012640 以修复此错误。

在 Managed System 上启用 Server Administrator 服务

Server Administrator Web Server 通过 Server Administrator 通用接口模型 (CIM) 提供程序与 VMware ESXi 系统通信。Server Administrator CIM 提供程序是 VMware ESXi 系统上的 OEM 提供程序。默认情况下，CIM OEM 提供程序在 VMware ESXi 中被禁用。必须在 VMware ESXi 4.0/ESXi 4.1 系统上启用 CIM OEM 提供程序，才能使用 Server Administrator Web Server 访问它。

使用 vSphere 客户端 (对于 VMware ESXi 4.0/ESXi 4.1) 启用 CIM OEM 提供程序

要使用 VMware vSphere 客户端启用 CIM OEM 提供程序，需要安装 vSphere 客户端工具。可以从 <https://<ESXi 主机的 IP 地址>> 下载和安装该工具，其中 <IP 地址> 是 VMware ESXi 系统的 IP 地址。

要使用 vSphere 客户端在 VMware ESXi 系统上启用 CIM OEM 提供程序：

1. 使用 vSphere 客户端登录 VMware ESXi 主机系统。
2. 单击“Configuration”（配置）选项卡。
3. 在左侧的“Software”（软件）部分下面，单击“Advanced Settings”（高级设置）。
4. 在“Advanced Settings”（高级设置）对话框中，单击左窗格中的 UserVars。
5. 将 CIMOEMProvidersEnabled 字段的值更改为 1。
6. 单击“OK”（确定）。
7. 要使更改在无需重新启动系统的情况下生效，可以在 VMware ESXi 系统本地控制台的直接控制台用户界面 (DCUI) 中使用“Restart Management Agents”（重新启动管理代理程序）选项。

如果更改无效，并且您使用 Server Administrator 无法连接到 VMware ESXi 主机，则重新启动 VMware ESXi 主机系统。

使用 vSphere CLI（对于 VMware ESXi 4.0/ESXi 4.1）启用 CIM OEM 提供程序

1. 如果您使用 Microsoft Windows 上的 vSphere CLI，则导航至已安装 vSphere CLI 公用程序的目录。

如果您使用 Linux 上的 vSphere CLI，则可以从任何目录执行步骤 2 中的命令。

2. 执行以下命令：

```
vicfg-advcfg.pl --server <ESXi 主机的 IP 地址> --username <用户名> --password <密码> --set 1 UserVars.CIMOEMProvidersEnabled
```

 **注：** 如果您使用 Linux 上的 vSphere CLI，则不需要 .pl 扩展名。

3. 要使更改在无需重新启动系统的情况下生效，可以在 VMware ESXi 系统本地控制台的直接控制台用户界面 (DCUI) 中使用“Restart Management Agents”（重新启动管理代理程序）选项。

如果更改无效，并且您使用 Server Administrator 无法连接到 VMware ESXi 主机，则重新启动 VMware ESXi 主机系统。

使用 vMA（对于 VMware ESXi 4.0/ESXi 4.1）启用 CIM OEM 提供程序

1. 以管理员的身份登录 vMA，在出现提示时提供密码。

2. 执行以下命令：

```
vicfg-advcfg --server <ESXi 主机的 IP_地址> --username <用户名> --password <密码> --set 1 UserVars.CIMOEMProvidersEnabled
```

3. 要使更改在无需重新启动系统的情况下生效，可以在 VMware ESXi 系统本地控制台的直接控制台用户界面 (DCUI) 中使用“Restart Management Agents”（重新启动管理代理程序）选项。

如果更改无效，并且您使用 Server Administrator 无法连接到 VMware ESXi 主机，则重新启动 VMware ESXi 主机系统。

在运行 VMware ESXi 4/ESXi 4.1 的系统上配置 SNMP 代理

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 的系统上配置一个或多个陷阱目标才能向 Management Station 发送 SNMP 陷阱。

Server Administrator 支持 VMware ESXi 上的 SNMP 陷阱，但不支持 SNMP Get 和 Set 操作，因为 VMware ESXi 不提供所需的 SNMP 支持。您可以使用 VMware vSphere CLI 配置运行 VMware ESXi 的系统，向诸如 IT Assistant 等管理应用程序发送 SNMP 陷阱。

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


使用 vSphere CLI 配置系统以向 Management Station 发送陷阱

1. 安装 VMware vSphere CLI。
2. 在安装了 vSphere CLI 的系统上打开命令提示符。
3. 导航至安装了 vSphere CLI 的目录。在 Linux 上，默认位置是 `/usr/bin`；在 Windows 上，默认位置是 `C:\Program Files\VMware\VMware vSphere CLI\bin`。

4. 使用以下命令配置 SNMP 设置：

```
vicfg-snmp.pl --server <服务器> --username <用户名> --password <密码> -c <团体> -t <主机名>@162/<团体>
```

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

 **注：** 如果没有指定用户名和密码，系统将会提示您指定这两项。

5. 使用以下命令启用 SNMP：

```
vicfg-snmp.pl --server <服务器> --username <用户名> --password <密码> -E
```

6. 使用以下命令查看 SNMP 配置：

```
vicfg-snmp.pl --server <服务器> --username <用户名> --password <密码> -s
```

7. 使用以下命令测试 SNMP 配置:

```
vicfg-snmp.pl --server <服务器> --username <用户名> --password <密码> -T
```

 **注:** 如果您使用 Linux 上的 vSphere CLI 或使用 vMA, 则不需要 **.pl** 扩展名。

[目录](#)

在支持的 Linux 操作系统上安装 Managed System Software

- [概览](#)
- [软件许可协议](#)
- [Server Administrator 设备驱动程序](#)
- [动态内核支持](#)
- [OpenIPMI 设备驱动程序](#)
- [安装受管系统软件](#)
- [Remote Enablement 的相关 RPM](#)
- [Remote Enablement 安装后配置](#)
- [卸载 Managed System Software](#)
- [结合使用 Dell OpenManage 和 Citrix XenServer](#)
- [使用第三方部署软件进行 Managed System Software 安装](#)

概览

Dell™ OpenManage™ 安装程序对于 32 位和 64 位体系结构都支持。下表说明 OpenManage 的操作系统安装值表。

表 7-1. OpenManage 的操作系统安装值表

操作系统	RHEL 4		RHEL 5		SLES 10		SLES 11		ESX	
	32 位	64-bit (64 位)	32 位	64-bit (64 位)	32 位	64-bit (64 位)	32 位	64-bit (64 位)	32 位	64-bit (64 位)
OpenManage 6.3 (32 位)	UP	U/UP	UP	U/UP	NS	U/UP	NS	U/UP	NS	U/UP
OpenManage 6.3 (64 位)	NS	I	NS	I	NS	I	NS	I	NS	NS

UP - 升级; U/UP - 卸载并升级; I - 安装; NS - 不支持

- **注:** 在 OpenManage 升级时, 建议升级到 DVD 提供的最新开放源代码组件。
- **注:** `srvadmin-cm` RPM 是与 64 位 OpenManage Server Administrator RPM 一起安装的 32 位 RPM。此 RPM 需要 32 位版本的 `zlib` 和 `compat-libstdc++` 程序库。确保在系统上安装了这些程序库。
- **注:** 如果您要将操作系统升级到主要版本 (例如, SLES 10 至 SLES 11), 您必须卸载现有版本的 OpenManage 并安装支持的版本。
- **注:** 在迁移到 64 位 OpenManage 之前, 您必须卸载以下各项:
 - 1 安装的 32 位 OpenManage, 以及
 - 1 作为 32 位 OpenManage 的一部分安装的其他开放源代码组件 (`openwsman-server`, `openwsman-client`, `libwsman1`, `sblim-sfcb`, `sblim-sfcc`, `libcmptCpplmpio`, `libsmbios2`, `smbios-utils-bin`)

提供专门针对您的操作系统的安装脚本和 RPM 软件包, 可以安装和卸载 Dell OpenManage Server Administrator 和其它 Managed System Software 组件。这些安装脚本和 RPM 位于 *Dell Systems Management Tools and Documentation DVD* 的 `SYSMGMT/srvadmin/linux/` 目录中。

自定义安装脚本 `srvadmin-install.sh` 允许自定义和交互安装。通过将 `srvadmin-install.sh` 脚本包括到 Linux 脚本中, 您可以在本地或网络上的一个或多个系统上安装 Server Administrator。

第二种安装方法使用自定义目录中提供的 Server Administrator RPM 软件包和 Linux `rpm` 命令。您可以编写 Linux 脚本, 使之能在本地或网络上的一个或多个系统上安装 Server Administrator。

建议您不要将这两种安装方法一起使用, 这可能需要用 Linux `rpm` 命令手工安装自定义目录中提供的所需 Server Administrator RPM 软件包。

有关支持的平台和支持的操作系统的信息, 请参阅 Dell 支持网站 support.dell.com/support/edocs/software/omswrels/index.htm 上的《Dell 系统软件支持值表》。

软件许可协议

Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 版本的 Dell OpenManage 软件 的软件许可证位于 *Dell Systems Management Tools and Documentation DVD* 上。请阅读 `license.txt` 文件。通过安装或复制 Dell 提供的介质上的任何文件, 即表示您同意此文件中的条款。此文件也会被复制到软件树的根目录 (选择在其上安装 Dell OpenManage 软件)。

Server Administrator 设备驱动程序

Server Administrator 包括两个用于 Linux 的设备驱动程序: 系统管理基本驱动程序 (`dcdbas`) 和 BIOS 更新驱动程序 (`dell_rbu`)。Server Administrator 使用这些驱动程序在支持的 Linux 操作系统上执行系统管理功能。根据具体的系统, Server Administrator 在需要的时候载入这些驱动程序中的一个或两个。

用于 Linux 的设备驱动程序已根据 GNU 通用公共许可证版本 2.0 发布为开放源代码。这些驱动程序从内核 2.6.14 版本开始就内置于 `kernel.org` 的 Linux 内核中。

如果随操作系统提供了 Server Administrator 驱动程序, 则 Server Administrator 将使用这些版本的驱动程序。如果没有随操作系统提供 Server Administrator 驱动程序, 则 Server Administrator 将在需要的时候使用动态内核支持 (DKS) 功能生成驱动程序。有关 DKS 的详情, 请参阅“[动态内核支持](#)”一节。

动态内核支持


Server Administrator 包括 DKS，在需要的时候，Server Administrator 使用此功能自动为运行内核生成设备驱动程序。

如果在 Server Administrator 设备驱动程序启动期间看到以下信息，则表示 Server Administrator 已尝试使用其 DKS 功能，但是由于不满足某些前提条件而不能使用此功能：

```
Building <driver> using DKS... [FAILED]

(正在使用 DKS 建立 <驱动程序>... [FAILED])

其中，<驱动程序>是 dcdbas 或 dell_rbu
```

 **注：** Server Administrator 将信息记录到 `/var/log/messages` 日志文件中。

要使用 DKS，请识别在受管系统上运行的是哪个内核，并检查 DKS 前提条件。

确定运行的内核

1. 作为 root 登录。
2. 在控制台上键入以下命令并按 <Enter>：

```
uname -r
```

系统会显示标识运行内核的信息。

动态内核支持前提条件

要使 Managed System Software 使用 DKS，必须符合以下相关性才能启动 Server Administrator。

- 1 运行的内核必须已启用可载入模块支持。
- 1 `/lib/modules/`uname -r`/build` 中必须有用于为运行内核建立内核模块的源代码。在运行 SUSE Linux Enterprise Server 的系统上，`kernel-source` RPM 提供必要的内核源代码。在运行 Red Hat Enterprise Linux 的系统上，`kernel-devel` RPM 提供构建内核模块所需的内核源代码。
- 1 必须安装 GNU make 公用程序。`make` RPM 提供该公用程序。
- 1 必须安装 GNU C 编译器 (gcc)。`gcc` RPM 提供该编译器。
- 1 必须安装 GNU 链接器 (ld)。`binutils` RPM 提供该链接器。

满足这些前提条件后，DKS 就会在 Server Administrator 启动期间根据需要自动建立设备驱动程序。

在安装 Server Administrator 后使用动态内核支持

要使 Server Administrator 能够支持预编译设备驱动程序不支持的、在安装 Server Administrator 之后载入的内核，请执行以下步骤：确保在要管理的系统上已满足 DKS 前提条件并在该系统上引导新的内核。

Server Administrator 在载入内核后首次启动时将系统运行的内核建立设备驱动程序。默认情况下，Server Administrator 将在系统启动期间启动。

将动态建立的设备驱动程序复制到运行相同内核的系统


当 Server Administrator 以动态方式为运行内核建立设备驱动程序时，它将设备驱动程序安装到 `/lib/modules/<内核>/kernel/drivers/firmware` 目录中，其中 `<内核>` 是（键入 `uname -r` 后所返回的）内核名称。如果系统运行着为其构建设备驱动程序的相同内核，则可以将新构建的设备驱动程序复制到其它系统的 `/var/omsa/dks/<内核>` 目录中以供 Server Administrator 使用。此操作使 Server Administrator 能够在多个系统上使用 DKS，而不用在每个系统上都安装内核源代码。


以下情况就是一个示例：系统 A 正在运行一个内核，但其中一个 Server Administrator 预编译设备驱动程序不支持该内核。系统 B 正在运行相同的内核。要在系统 A 中建立设备驱动程序并将该设备驱动程序复制到系统 B 以供 Server Administrator 使用，请执行以下步骤：

1. 确保在系统 A 上满足 DKS 前提条件。
2. 在系统 A 中启动 Server Administrator。

在启动期间，Server Administrator 将为系统 A 中运行的内核建立设备驱动程序。


3. 在系统 A 上键入 `uname -r` 以确定运行内核的名称。
4. 将系统 A 上的 `/lib/modules/<kernel>/kernel/drivers/firmware` 目录中的任何 `dcdbas.*` 或 `dell_rbu.*` 文件都复制到系统 B 上的 `/var/omsa/dks/<内核>` 目录中，其中 `<内核>` 为第三步中键入 `uname -r` 后所返回的内核名称。

 **注：** The `/lib/modules/<内核>/kernel/drivers/firmware` 目录中可能会包含下列一个或多个文件：`dcdbas.*` 或 `dell_rbu.*`

 **注：** 可能需要在系统 B 上创建 `/var/omsa/dks/<内核>` 目录。例如，如果内核名称是 `1.2.3-4smp`，可以通过键入以下命令创建目录：`mkdir -p /var/omsa/dks/1.2.3-4smp`

5. 在系统 B 中启动 Server Administrator。

Server Administrator 检测出您复制到 `/var/omsa/dks/<内核>` 目录的设备驱动程序支持正在运行的内核并将使用该设备驱动程序。

 **注：** 当从系统 B 中卸载了 Server Administrator 后，`/var/omsa/dks/<内核>/*.` 复制到系统 B 的文件将不会删除。如果不再需要，则必须删除这些文件。

OpenIPMI 设备驱动程序

Server Administrator 的 Server Instrumentation 功能需要 OpenIPMI 设备驱动程序以提供基于 IPMI 的信息和功能。

所有支持的 Linux 系统都在默认内核本身就包含了所需版本的 IPMI 模块。您不必安装 IPMI RPM。有关所支持系统的信息，请参阅 Dell 支持网站 support.dell.com/support/edocs/software/oms wre ls/index.htm 上的《Dell 系统软件支持值表》。

Server Administrator Instrumentation Service 启动时功能降级

Server Administrator 安装后，无论何时启动，Server Administrator Instrumentation Service 都会对 OpenIPMI 设备驱动程序进行一次运行时间检查。每当运行 `srvadmin-services.sh start` 或 `srvadmin-services.sh restart` 命令时，或每当重新启动系统时（在此期间 Server Administrator Instrumentation Service 也会启动），Server Administrator Instrumentation Service 就会启动。


如果系统上当前未安装相应版本的 OpenIPMI 设备驱动程序，则 Server Administrator 安装会阻止 Server Administrator 软件包的安装。然而，仍有可能（尽管一般不能）在安装 Server Administrator 之后卸载或更换足够高版本的 OpenIPMI 设备驱动程序。Server Administrator 无法阻止此操作。

考虑到 Server Administrator 已安装后用户会卸载或更换足够高版本的 OpenIPMI 设备驱动程序，每当 Server Administrator Instrumentation Service 启动时，都会检查 OpenIPMI 设备驱动程序版本。如果未找到足够高版本的 OpenIPMI 设备驱动程序，则 Server Administrator Instrumentation Service 就会让自身功能降级，以便不提供任何基于其 IPMI 的信息或功能。基本上，这意味着它不会提供任何探测器数据（如风扇、温度和电压探测器数据）。

安装受管系统软件

本节说明如何使用以下安装选项安装受管系统软件：

- 1 使用 `srvadmin-install.sh` Shell 脚本进行快速安装或自定义安装


 **注：** 如果已从 Dell 支持网站 support.dell.com 下载了 Managed System Software 安装程序（.tar.gz 文件），`srvadmin-install.sh` 外壳脚本会在根目录中显示为 `setup.sh`。

- 1 使用 RPM 命令进行自定义安装

要了解 Dell OpenManage 版本 6.3 中提供的 Server Administrator 的各个组件的信息和帮助您选择所需的组件进行安装，请参阅“[Server Administrator 的部署情况](#)”。

安装 Managed System Software 的前提条件

- 1 必须作为 root 登录。
- 1 运行的内核必须已启用可加载模块支持。
- 1 `/opt` 目录必须至少有 250 MB 可用空间，而 `/tmp`、`/etc` 和 `/var` 目录必须分别至少有 20 MB 可用空间。
- 1 如果使用 SNMP 管理服务器，则必须安装随操作系统提供的 `ucd-snmp` 或 `net-snmp` 软件包。如果想要使用 `ucd-snmp` 或 `net-snmp` 代理的支持代理，则必须在安装 Server Administrator 之前安装支持 SNMP 标准的操作系统。有关安装 SNMP 的详细信息，请参阅系统中运行的操作系统的安装说明。

 **注：** 当在 VMware ESX、Red Hat Enterprise Linux 或 SUSE Linux Enterprise Server 中安装 RPM 软件包时，为避免出现与 RPM-GPG 密钥相关的警告，应使用类似以下的命令导入密钥：

```
rpm --import /mnt/dvdrom/SYSGMT/srvadmin/  
linux/RPM-GPG-KEY
```

- 1 必须安装所有必需的 RPM 才能成功进行安装。


如果系统在工厂预装了 VMware ESX（版本 4 或 4.1）、Red Hat Enterprise Linux（版本 4 和 5）或 SUSE Linux Enterprise Server（版本 10 和 11），请参

参阅“[Remote Enablement 的相关 RPM](#)”一节，了解有关在安装 Managed System Software 之前需要手动安装的任何 RPM 的信息。一般情况下，不需要手动安装任何 RPM。

如果系统没有在工厂预装 Linux 操作系统，而您也没有使用 Dell Systems Build and Update Utility 安装 VMware ESX（版本 4 或 4.1）、Red Hat Enterprise Linux（版本 4 和 5）或 SUSE Linux Enterprise Server（版本 10 和 11）操作系统，则在安装 Managed System Software 之前就需要手动安装必需的 RPM。Dell Systems Management Tools and Documentation DVD 上提供了这些 RPM 文件。导航至 `SYSMGMT/srvadmin/linux/RPMS/supportRPMS/srvadmin/<操作系统>/<架构>` 找到适用于 Linux 操作系统的 RPM 文件。安装 managed system software 前，使用 `rpm -ivh <RPM 名称>` 安装相应的 RPM。

使用 Dell 提供的介质安装 Managed System Software

Dell OpenManage 安装程序使用 RPM 安装每个组件。为便于自定义安装，该介质 (DVD) 分为若干子目录。

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

如果安装前希望查看软件，请执行以下步骤：

1. 将 *Dell Systems Management Tools and Documentation* DVD 插入系统的 DVD 驱动器。
2. 如果有必要，使用以下命令利用命令安装 DVD：

```
mount /dev/dvdr0m /mnt/dvdr0m
```
3. 安装完 DVD 后，请导航至：


```
cd /mnt/dvdr0m/SYSMGMT/srvadmin/linux/
```
4. 使用 `ls` 命令获得目录列表。

介质上属于 VMware ESX、Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 的目录如下：

- 1 SYSMGMT/srvadmin/linux/custom
- 1 SYSMGMT/srvadmin/linux/RPMS
- 1 SYSMGMT/srvadmin/linux/supportscripts

快速安装

使用所提供的外壳脚本进行快速安装。

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

1. 以 root 身份登录至运行支持的 Red Hat Enterprise Linux 或 SUSE Linux Enterprise Server 操作系统的系统，以在该系统中安装 Managed System 组件。
2. 将 *Dell Systems Management Tools and Documentation* DVD 插入 DVD 驱动器中。
3. 如果有必要，使用以下命令利用命令安装 DVD：

```
mount /dev/dvdr0m /mnt/dvdr0m
```
4. 导航至 `SYSMGMT/srvadmin/linux/supportscripts` 目录。
5. 如下所示运行 `srvadmin-install.sh` 外壳脚本，这会执行快速安装。安装程序将安装以下 Managed System Software 功能：

- 1 Server Administrator Web Server
- 1 Server Instrumentation
- 1 存储设备管理
- 1 Remote Access Controller

```
sh srvadmin-install.sh --express
```

或

```
sh srvadmin-install.sh -x
```

Server Administrator 服务不会自动启动。

6. 请在安装后使用 `srvadmin-services.sh` 脚本启动 Server Administrator 服务，方法是使用 `sh srvadmin-services start` 命令。

自定义安装

Managed System Software 提供了两种自定义安装方法。一种是基于 RPM 的，使用预配置的自定义目录，而另一种是基于外壳脚本的。

使用预配置的自定义目录执行自定义安装

针对特定操作系统的所有 RPM 按 [表 7-2](#) 中所列组合在一起。您可以通过预配置的自定义目录使用这些 RPM 执行自定义安装。

表 7-2. 使用预配置的目录进行自定义安装

目录	详细信息
要进行基于 RPM 的自定义安装，请添加以下目录的 RPM：	
SYSMGMT/srvadmin/linux/custom/ESX40/<架构>	包含针对 VMware ESX（版本 4）的使用命令行界面的 Server Administrator
SYSMGMT/srvadmin/linux/custom/ESX41/<架构>	包含针对 VMware ESX（版本 4.1）的使用命令行界面的 Server Administrator
SYSMGMT/srvadmin/linux/custom/RHEL4/<架构>	包含针对 Red Hat Enterprise Linux（版本 4）的使用命令行界面的 Server Administrator
SYSMGMT/srvadmin/linux/custom/RHEL5/<架构>	包含针对 Red Hat Enterprise Linux（版本 5）的使用命令行界面的 Server Administrator
SYSMGMT/srvadmin/linux/custom/SLES10/<架构>	包含针对 SUSE Linux Enterprise Server（版本 10）的使用命令行界面的 Server Administrator
SYSMGMT/srvadmin/linux/custom/SLES11/<架构>	包含针对 SUSE Linux Enterprise Server（版本 11）的使用命令行界面的 Server Administrator
例如，如果您运行的是 Red Hat Enterprise Linux（版本 4），可通过添加以下目录的 RPM 来自定义安装：	
SYSMGMT/srvadmin/linux/custom/RHEL4/add-StorageManagement/<架构>	适于 Red Hat Enterprise Linux（版本 4）的 Storage Management 组件软件包
SYSMGMT/srvadmin/linux/custom/RHEL4/SA-WebServer/<架构>	适于 Red Hat Enterprise Linux（版本 4）的 Server Administrator Web Server 组件软件包
SYSMGMT/srvadmin/linux/custom/RHEL4/Server-Instrumentation/<架构>	适于 Red Hat Enterprise Linux（版本 4）的 Server Instrumentation 软件包

DVD 提供的 RPM 可以通过 Yum、Zypper 和 Rug 等客户端进行基于存储库的安装。有些 RPM 可以整组安装，或者您可以选择单独 RPM 以安装特定组件。RPM 位于：

SYSMGMT/srvadmin/linux/RPMS/supportRPMS/metaRPMS


 **注：** 有关 RPM 的完整列表及其说明，请参阅“[OpenManage Linux 安装程序软件包](#)”一节。

以下 RPM 列表依次允许安装特定 RPM 组。

表 7-3. 元 RPM

元 RPM	详细信息
srvadmin-all	安装所有组件
srvadmin-base	安装 Server Instrumentation 组件。必须先安装此组件，才能安装任何其它特定组件。
srvadmin-idrac	安装 iDRAC 组件
srvadmin-rac4	安装 DRAC 4 组件
srvadmin-rac5	安装 DRAC 5 组件
srvadmin-standardAgent	安装 Remote Enablement 组件
srvadmin-storageservices	安装存储服务组件
srvadmin-webserver	安装 Web Server 组件

以下是 Server Administrator 基于 RPM 的自定义安装的示例，其中包括安装 Remote Enablement 功能和 Storage Management Service 组件。

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


- 以 root 身份登录至运行支持的 VMware ESX、Red Hat Enterprise Linux 或 SUSE Linux Enterprise Server 操作系统的系统，以便在系统中安装 Managed System 组件。
- 将 *Dell Systems Management Tools and Documentation* DVD 插入 DVD 驱动器中。
- 如果有必要，使用以下命令安装 DVD：


```
mount /dev/dvdrom /mnt/dvdrom.
```
- 导航至 `SYSMGMT/srvadmin/linux/custom/<操作系统>/<架构>`，其中 `<操作系统>` 是 `ESX41`、`ESX40`、`RHEL4`、`RHEL5`、`SLES10` 或 `SLES11`，`<架构>` 是 32 位或 64 位。ESX 仅支持 32 位，而 RHEL 和 SLES 支持 32 位和 64 位。进入对应您的系统的操作系统特定目录。

5. 键入以下命令：

```
rpm -ihv Server-Instrumentation/*.rpm
add-StorageManagement/*.rpm RemoteEnablement/*.rpm
```


Server Administrator 服务不会自动启动。

 **注：** 确保先安装 Server Administrator Web Server、Remote Enablement 或 Server Instrumentation，然后再安装 Remote Access Controller 或 Storage Management。

 **注：** 如果选择安装 Remote Enablement 功能，则确保先安装相关的 RPM，然后再安装此功能。有关安装相关 RPM 的详情，请参阅“[Remote Enablement 的相关 RPM](#)”。

6. 安装后使用此命令启动 Server Administrator 服务：

```
sh srvadmin-services start
```

 **注：** 您可以在符合操作系统相关性的任何系统上安装 Server Administrator。但是，在安装之后，在不支持的系统上可能无法启动某些 Server Administrator 服务。

 **注：** 在系统上安装 Dell OpenManage Server Administrator 时，可能会出现与 RPM 相关的相关性问题。要解决这些问题，请从 [SYSMGMT/srvadmin/linux/RPMS/supportRPMS/opensource-components](#) 安装缺少的 RPM。如果该目录中不存在这些 RPM，则从操作系统介质中安装这些 RPM。如果介质上不存在这些 RPM，则在因特网上搜索这些 RPM。

使用外壳脚本执行自定义安装

可以采用交互模式运行 Server Administrator 自定义安装脚本。

此脚本的基本用法如下：

```
srvadmin-install.sh [选项]...
```

Server Administrator 自定义安装公用程序

如果不指定任何选项，此公用程序将以交互模式运行；如果提供一个或多个选项，则以无提示方式运行。

选项包括：

[-x|--express] 安装所有组件（包括 RAC，如果可用），传递的任何其它选项将被忽略。

[-d|--dellagent] 安装 Server Instrumentation 组件。

[-c|--cimagent] 安装 Remote Enablement 组件。

[-s|--storage] 安装 Storage Management，包括 Server Instrumentation。

[-r|--rac] 安装合适的 RAC 组件，包括 Server Instrumentation。


[-w|--web] 安装 Server Administrator Web Server。

[-u|--update] 更新合适的 Server Administrator 组件。

[-h|--help] 显示此帮助文本。

以下选项可以与上述选项一起使用：

[-p|--preserve] 保留屏幕信息而不清除。

 **注：** 如果在自定义安装过程中没有使用 **[-p|--preserve]** 选项，屏幕上的历史记录信息将被清除。

[-a|--autostart] 在组件安装后启动已安装服务。

使用外壳脚本以交互模式执行自定义安装

此过程使用安装外壳脚本在安装过程中提示安装特定组件。

1. 以 root 身份登录至运行支持的 Red Hat Enterprise Linux 或 SUSE Linux Enterprise Server 操作系统的系统，以在该系统中安装 Managed System 组件。
2. 将 *Dell Systems Management Tools and Documentation DVD* 插入 DVD 驱动器中。
3. 如果有必要，使用以下命令安装 DVD：

```
mount /dev/dvdrom /mnt/dvdrom
```
4. 如果您使用的是 DVD，导航至 [SYSMGMT/srvadmin/linux/supportscripts](#)。
5. 使用 `sh srvadmin-install.sh` 命令执行脚本，并接受最终用户许可协议的条款。

执行该命令时，会显示组件选项列表。如果已经安装了任何组件，则这些组件会分别列出，旁边带有复选标记。将会显示 Server Administrator 自定义安装选项。

6. 选择 <c> 可进行复制, <i> 可进行安装, <r> 可进行重置并重新启动, 或 <q> 可退出。如果选择 <c>, 系统会提示您输入绝对目的地路径。

安装完成后, 脚本将具有启动服务的选项。

7. 选择 <n> 可退出。您可以之后手工启动这些服务。

使用自定义安装脚本以无提示模式运行


以下为使用 `srvadmin-install.sh` 外壳脚本进行无提示自定义安装的一个示例:

1. 以 `root` 身份登录至运行支持的 Red Hat Enterprise Linux 或 SUSE Linux Enterprise Server 操作系统的系统, 以在该系统中安装 Managed System 组件。
2. 将 *Dell Systems Management Tools and Documentation DVD* 插入 DVD 驱动器中。
3. 如果有必要, 使用如下命令安装 DVD: `mount /dev/dvdrom /mnt/dvdrom`。
4. 导航至 `SYSMGMT/srvadmin/linux/supportscripts`。
5. 要安装 Storage Management Service 组件, 请键入以下命令。

```
sh srvadmin-install.sh --storage (这些是长选项)
```

或


```
sh srvadmin-install.sh -s (这些是短选项)
```

 **注:** 长选项可与短选项组合使用, 反之亦然。

Server Administrator 服务不会自动启动。

6. 安装后使用此命令启动 Server Administrator 服务:

```
sh srvadmin-services start
```


 **注:** 安装 Server Administrator 后, 先注销, 然后重新登录以访问 Server Administrator 命令行界面 (CLI)。

Remote Enablement 的相关 RPM

如果选择安装 Remote Enablement 功能, 则在安装此功能之前, 必须安装某些相关 RPM 并配置这些 RPM。

相关 RPM 位于 *Dell Systems Management Tools and Documentation DVD* 的 `srvadmin/linux/RPMS/supportRPMS/opensource-components/<操作系统>/<架构>` 中。安装以下 RPM:

- 1 `libcmptCpplmpIO`
- 1 `libwsman1`
- 1 `openwsman-server`
- 1 `sblim-sfcb`
- 1 `sblim-sfcc`

 **注:** 在 SLES 11 SP1 的情形中, 建议从操作系统介质安装上述 RPM。

安装相关 RPM

1. 检查是否已安装相关 RPM。如果是, 则删除已安装的 RPM。
2. 确保卸载了 Pegasus RPM。
3. 使用 `make-install` 检查是否已安装 `openwsmand` 和 `sfcbd` 二进制文件。可以通过运行以下命令检查:

```
openwsman
```

或

```
sfcbd
```

或

可以检查 `/usr/local/sbin` 目录中是否存在上述二进制文件。

4. 如果已安装二进制文件，则卸载这些二进制文件。
5. 检查表 7-4 中列出的 `openwsman` 和 `sfcbd` RPM 所需的相关性。

表 7-4. 所需的主资源

软件包	Red Hat Enterprise Server	SUSE Linux Enterprise Server
Openwsman	<ul style="list-style-type: none">1 OpenSSL1 LibXML1 Pkgconfig1 CURL1 Chkconfig1 Initscript1 SBLIM-SFCC	<ul style="list-style-type: none">1 LibOpenSSL1 LibXML1 Pkg-config1 libCURL1 aaa_base1 aaa_base1 SBLIM-SFCC
SBLIM SFCC	CURL	LibCURL
SBLIM SFCB	<ul style="list-style-type: none">1 zlib1 CURL1 PAM1 OpenSSL1 Chkconfig1 Initscript	<ul style="list-style-type: none">1 zlib1 LibCURL1 PAM1 LibOpenSSL1 aaa_base1 aaa_base

6. 安装相关 RPM。

可以使用单个命令安装所有 RPM。

```
rpm -ivh rpm1 rpm2 rpm3 rpm4 ... rpmN
```

也可以逐个安装 RPM。

 **注：** 如果逐个安装 RPM，可以使用下面的顺序。

```
rpm -ivh sblim-sfcb-x.x.x.rpm
```

```
rpm -ivh sblim-sfcc-x.x.x.rpm
```

 **注：** `libwsman` 和 `openwsman` 客户端 RPM 应同时安装，因为它们具有循环相关性。

```
rpm -ivh libwsman1-x.x.x.rpm openwsman-client-x.x.x.rpm
```

```
rpm -ivh openwsman-server-x.x.x.rpm
```

Remote Enablement 安装后配置

本节详细说明安装 Remote Enablement 功能之后配置相关 RPM 的步骤。


安装后配置脚本位于服务器文件系统的 `/opt/dell/srvadmin/etc/`。

安装完所有相关 RPM 和 Remote Enablement 功能后，执行 `autoconf_cim_component.sh` 脚本。

在执行 `autoconf_cim_component.sh` 脚本前，请确保已安装 Dell OpenManage。有关安装 Dell OpenManage 的信息，请参阅“[安装受管系统软件](#)”。

执行以下命令根据默认配置来配置 `sfbc` 和 `openwsman`。

```
./ autoconf_cim_component.sh
```

 **注：** 要在受管节点上将 `Openwsman` 配置为在另一个端口上运行，请使用 `-p <端口>` 选项和 `autoconf_cim_component.sh`。这是可选配置，默认情况下，`Openwsman` 将被配置为在端口 443 上运行。

为 WSMAN 创建服务器证书

可以为 WSMAN 创建新证书，也可以重复使用现有的证书。

创建新证书

可以通过执行位于 `/etc/openwsman` 中的 `owsmangencert.sh` 脚本，为 WSMAN 创建新服务器证书。此脚本由 `openwsman` RPM 提供。执行向导中的步骤创建服务器证书。


重复使用现有的证书

如果有自签证书或认证机构签署的证书，则可以通过以下方法为 `openwsman` 服务器使用相同的证书：使用现有的证书值更新 `/etc/openwsman/openwsman.conf` 中 `[server]` 标记分组内的 `ssl_cert_file` 和 `ssl_key_file` 值。

为 openwsman 客户端配置 CRL

您需要配置 Server Administrator Web Server 使用的证书撤回列表 (CRL)。要执行此操作：

1. 描述 `/etc/openwsman/openwsman_client.conf` 中的有效 CRL 文件。
2. 如果保留空白，则忽略 CRL 检查。

 **注：** 只有 SUSE Linux Enterprise Server 版本 11 和 Red Hat Enterprise Linux Server 版本 5 更新 5 才支持 CRL。对于其它操作系统，与操作系统供应商联系以提供支持 CRL 的所需 CURL 程序库。

运行 sfcbl 和 openwsman

运行 `sfcbl` 和 `openwsman`：

```
1 /etc/init.d/sfcbl start
1 /etc/init.d/openwsmand start
```

Managed System 已配置并已准备就绪可供 Server Administrator Web Server 使用。

用于 Red Hat Enterprise Linux 操作系统 openwsman 和 sfcbl 的 Winbind 配置

按照下述说明在 32 位 OMI 安装上配置 `openwsman` 和 `sfcbl`。在 64 位安装的情形中，将 `"lib"` 替换为 `"lib64"`。

1. 备份以下文件：

```
1 /etc/pam.d/openwsman
1 /etc/pam.d/sfcbl
1 /etc/pam.d/system-auth
```

2. 将 `/etc/pam.d/openwsman` 和 `/etc/pam.d/sfcbl` 的内容替换为：

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

3. 将 `/etc/pam.d/system-auth` 的内容替换为：

```
%PAM-1.0
This file is auto-generated.
User changes will be destroyed the next time authconfig is run.
auth required /lib/security/$ISA/pam_env.so
auth sufficient /lib/security/$ISA/pam_unix.so likeauth nullok
auth sufficient /lib/security/$ISA/pam_krb5.so use_first_pass
auth sufficient /lib/security/$ISA/pam_winbind.so use_first_pass
auth required /lib/security/$ISA/pam_deny.so
account required /lib/security/$ISA/pam_unix.so broken_shadow
account sufficient /lib/security/$ISA/pam_succeed_if.so uid 100 quiet
```

```

account [default=bad success=ok user_unknown=ignore] /lib/security/$ISA/pam_krb5.so
account [default=bad success=ok user_unknown=ignore] /lib/security/$ISA/pam_winbind.so

account required /lib/security/$ISA/pam_permit.so

password requisite /lib/security/$ISA/pam_cracklib.so retry=3

password sufficient /lib/security/$ISA/pam_unix.so nullok use_authtok md5 shadow

password sufficient /lib/security/$ISA/pam_krb5.so use_authtok

password sufficient /lib/security/$ISA/pam_winbind.so use_authtok

password required /lib/security/$ISA/pam_deny.so

session required /lib/security/$ISA/pam_limits.so

session required /lib/security/$ISA/pam_unix.so

session optional /lib/security/$ISA/pam_krb5.so

```

用于 SUSE Linux Enterprise Server 操作系统 openwsman 和 sfcbl 的 Winbind 配置

按照下述说明在 32 位 OMI 安装上配置 openwsman 和 sfcbl。在 64 位安装的情形中，将 "lib" 替换为 "lib64"。

1. 备份以下文件：

```

1 /etc/pam.d/openwsman
1 /etc/pam.d/sfcbl
1 /etc/pam.d/system-auth
1 /etc/pam.d/common-account

```

2. 将 /etc/pam.d/openwsman/ 和 /etc/pam.d/sfcbl 的内容替换为：

```

%PAM-1.0

auth include common-auth

auth required /lib/security/pam_nologin.so

account include common-account

```

3. 将 /etc/pam.d/common-auth 的内容替换为：

```

auth required pam_env.so

auth sufficient pam_unix2.so debug

auth sufficient pam_winbind.so use_first_pass debug

```

4. 将 /etc/pam.d/common-account 的内容替换为：

```

account sufficient pam_unix2.so

account sufficient pam_winbind.so

```

Libssl 问题的解决方法

如果系统中已经存在 openwsman 所需的必要程序库，则可以使用 `autoconf_cim_component.sh` 脚本尝试解决 `libssl.so` 问题。但是，如果该程序库不存在，则脚本将报告此情况。检查系统上是否已安装最新版本的 `libssl` 程序库，然后创建 `libssl.so` 的软链接。

例如：在 32 位 OpenManage 安装上，如果 `/usr/lib` 中已经包含 `libssl.so.0.9.8a` 和 `libssl.so.0.9.8b`，则创建最新的 `libssl.so.0.9.8b` 的软链接：

```

1 ln -sf /usr/lib/libssl.so.0.9.8b /usr/lib/libssl.so
1 ldconfig

```

在 64 位 OpenManage 安装上，如果 `/usr/lib` 中已经包含 `libssl.so.0.9.8a` 和 `libssl.so.0.9.8b`，则创建最新的 `libssl.so.0.9.8b` 的软链接：

```

1 ln -sf /usr/lib64/libssl.so.0.9.8b /usr/lib64/libssl.so
1 ldconfig

```

卸载 Managed System Software

您可以从 Red Hat Enterprise Linux、SUSE Linux Enterprise Server 或 VMware ESX 命令行卸载 Managed System Software。

卸载 Managed System Software 的前提条件

必须作为 root 登录。

从 Red Hat Enterprise Linux 或 SUSE Linux Enterprise Server 命令行卸载 Managed System Software。

安装 Server Administrator 时，还会安装一个卸载脚本。您可以通过键入 `srvadmin-uninstall.sh` 然后按下 <Enter> 执行该脚本。

自定义卸载特定组件

可卸载 Dell OpenManage 一些个别组件而无需卸载全部 Dell OpenManage。示例如下：

要只卸载 Server Administrator Web Server，请使用此命令：

```
rpm -e `rpm -qa | grep srvadmin-iws`
```

要卸载存储组件，请使用此命令：


```
rpm -e `rpm -qa | grep srvadmin-storage`
```

在卸载过程中，会使用 `.rpmsave` 文件扩展名保留已进行用户设置的文件。在卸载之后，还会保留日志文件。

结合使用 Dell OpenManage 和 Citrix XenServer

Dell OpenManage Server Administrator 可通过 OpenManage Supplemental Pack 安装在 Citrix® XenServer 中。OpenManage Supplemental Pack for XenServer 5.6 有两种安装方法：

- 1 在安装 XenServer 过程中
 - a. 照常开始安装 XenServer，按照屏幕上的说明操作。
 - b. 在 XenServer 安装过程中较早出现的问题之一是，如果要安装任何 Supplemental Pack，则选择“**Yes**”（是）并继续进行安装过程。
 - c. 安装基本 XenServer 映像（5-10 分钟，具体情况视系统速度而定）之后，将提示您插入 Supplemental Pack CD。从光盘驱动器弹出 XenServer 安装 CD，插入 OpenManage Supplemental Pack CD，然后单击“**OK**”（确定）。此时显示提示“OpenManage Supplemental Pack was found”（找到 OpenManage Supplemental Pack）。要确认安装，选择“**Use**”（使用）并单击“**OK**”（确定）。

 **注：** 如果您有多个 Supplemental Pack（Citrix 提供的 Linux Supplemental Pack，或者其它第三方应用程序），您可以按任何顺序安装，不过建议最后安装 OpenManage Supplemental Pack。

- d. OpenManage Supplemental Pack 安装完毕（2-5 分钟，具体情况视系统速度而定）之后，将提示您安装其它 Supplemental Pack。如果没有，选择“**Skip**”（跳过）并按 **Enter**。XenServer 已成功安装。

- 1 在运行的系统上
 - a. 将 Supplemental Pack ISO 文件刻录到 CD 或将 ISO 文件下载到服务器。
 - b. 如果您下载 ISO 文件，则将该文件安装到临时目录

```
$ mount -o loop <openmanage-supplemental-pack-文件名>.iso /mnt
```

如果您已将 ISO 文件刻录到 CD，则将 CD 插入光盘驱动器中并运行

```
$ mount /dev/cdrom /mnt
```


- c. 安装 Supplemental Pack。

```
$ cd /mnt
```

```
$ ./install
```

- d. 安装完成后，卸下 ISO 文件或取出 CD。

```
$ cd ..  
  
$ umount /mnt
```

 **小心：** Dell 或 Citrix 不支持删除 OpenManage Supplemental Pack 或任何 OpenManage RPM，因此不建议删除。手动删除任何 RPM，都会使系统处于不一致状态，从而导致任何潜在问题调试工作都难以或无法进行。未来的 Supplemental Pack 版本将支持删除 OpenManage Supplemental Pack。

今后发布新 OpenManage Supplemental Pack 版本时，将允许和支持升级现有安装。

如果 XenServer 映像升级到较新的 XenServer 更新或版本，则必须重新安装 OpenManage Supplemental Pack，因为新 XenServer 映像将放在另一个分区中，而不是放在原来的分区。在这种情况下，按照前文所述的安装说明操作。但是，服务器上保存的所有 OpenManage 配置设置都将丢失。

请参阅 support.dell.com/support/edocs/software/Citrix/ 上的《Citrix XenServer Dell Edition 解决方案指南》，了解有关结合使用 Dell OpenManage 和 Citrix XenServer Dell Edition 的详情。

 **注：** 如果使用 Server Administrator Web Server 连接到 XenServer™ 5.6 受管节点，则以格式“主机名:端口号”或“IP 地址:端口号”使用端口 5986。

使用第三方部署软件进行 Managed System Software 安装

可以使用第三方部署软件，比如 Altiris Deployment Solution，来将 Managed System Software 安装到所支持的 Dell 服务器上。要使用 Altiris 分发和安装 Managed System Software，请启动您的 Altiris 应用程序并导入位于 *Dell Systems Management Tools and Documentation* DVD 上 `SYSMGMT\svadmin\support\Altiris` 中的 `OpenManage_Jobs.bin`。指定要将 `OpenManage_Jobs.bin` 导入到的工作文件夹。可能需要修改“Run Script”（运行脚本）和“Copy File”（复制文件）任务来与部署环境相匹配。完成后，可以安排工作在 Altiris Deployment Solution 管理的支持的 Dell 系统上运行。

[目录](#)

在 Microsoft Windows 操作系统上安装 Managed System Software

- [概览](#)
- [安装过程前提条件检查程序](#)
- [Remote Enablement 要求](#)
- [安装和升级 Server Administrator](#)
- [升级 Managed System Software](#)
- [安装失败时的系统恢复](#)
- [Windows 安装程序日志记录](#)
- [执行 Managed System Software 的无人值守安装](#)
- [卸载 Managed System Software](#)
- [使用第三方部署软件进行 Managed System Software 安装](#)

概览

本节包含在运行 Microsoft® Windows® 操作系统的系统上安装 Managed System Software 的过程。


在 Microsoft Windows 操作系统上，插入 *Dell Systems Management Tools and Documentation DVD* 时将显示自动运行公用程序。该公用程序使您可以选择要在系统上安装的系统管理软件。

如果自动运行程序没有自动启动，可以使用 *Dell Systems Management Tools and Documentation DVD* 上 `SYSMGMT\srvadmin\windows` 目录中的安装程序。您可以通过操作系统卸载功能。请参阅《*Dell 系统软件支持值表*》了解当前支持的操作系统列表。

无人值守和脚本化无提示安装

可以使用 *Dell Systems Management Tools and Documentation DVD* 执行 Managed System Software 的无人值守和脚本化无提示安装。另外，还可以从命令行安装和卸载功能。

安装过程前提条件检查程序

 **注：** 如果想使用简单网络管理协议 (SNMP) 的支持代理，则必须在安装 Server Administrator 前后安装对 SNMP 标准的操作系统支持。有关安装 SNMP 的详细信息，请参阅系统中运行的操作系统的安装说明。

安装程序（位于 `\SYSMGMT\srvadmin\windows`）会启动前提条件检查程序。前提条件检查程序在不启动实际的安装程序的情况下检查是否符合软件组件的前提条件要求。此程序显示一个状态窗口，提供可能影响软件功能安装和运行的系统硬件和软件的信息。

前提条件检查程序显示三种类型信息：通知、警告和错误。

通知信息说明一种情况，但这种情况并不妨碍功能的安装。

警告信息说明在典型安装过程中阻止安装软件产品的情况。建议先解决引起警告的情况，然后再继续安装软件。如果决定继续，可选择并使用自定义安装来安装软件。例如，如果在系统上没有检测到 Intel 网络接口卡 (NIC)，将会显示以下信息：

```
An Intel(R) NIC was not detected on this system. This will disable the "Typical" installation of the Intel(R) SNMP Agent.  
  
Use the "Custom" installation setup type later during installation to select this feature if you have an Intel(R) NIC installed.
```

（此系统上没有检测到 Intel(R) NIC。这将会禁用 Intel(R) SNMP 代理的“Typical”[典型] 安装。

在后面的安装过程中使用“Custom”[自定义] 安装类型以在装有 Intel(R) NIC 的情况下选择此功能。）

错误信息说明阻止安装软件功能的情况。必须解决引起错误的情况，然后才可继续安装该软件功能。如果不解决这个问题，将不会安装该软件功能。

使用 `RunPreReqChecks.exe /s` 命令（位于 `\SYSMGMT\srvadmin\windows\PreReqChecker`）以无提示的方式运行前提条件检查。有关详情，请参阅“[前提条件检查程序](#)。”

Remote Enablement 要求

要安装 Remote Enablement 功能，必须在系统上配置以下各项：

- 1 Windows 远程管理 (WinRM)
- 1 认证机构签署/自签证书
- 1 WinRM HTTPS 侦听器端
- 1 WinRM 和 Windows Management Instrumentation (WMI) 服务器授权

安装 WinRM

如果使用 Windows Server 2003 操作系统，则安装 WinRM 版本 1.1。可以从 microsoft.com/downloads/details.aspx?familyid=845289ca-16cc-4c73-8934-

[dd46b5ed1d33&displaylang=en](#) 下载和安装 WinRM 版本 1.1

默认情况下，在 Windows Server 2008 R2 和 Win7 上安装 WinRM 版本 2.0。默认情况下，会在 Windows Server 2008 上安装 WinRM 版本 1.1。

认证机构签署/自签证书

需要认证机构 (CA) 签署的证书或自签证书才能在系统上安装和配置 Remote Enablement 功能。建议使用 CA 签署的证书。还可以使用 SelfSSL 工具生成自签证书。

使用认证机构签署的证书

1. [申请认证机构签署的有效证书](#)
2. [使用认证机构签署的有效证书创建 HTTPS 侦听器](#)

申请认证机构签署的有效证书

1. 单击 **Start (开始)** → **Run (运行)**。
2. 键入 `mmc`，然后单击 **OK (确定)**。
3. 单击 **File (文件)** → **Add/Remove Snap-in (添加/删除管理单元)**。
4. 选择证书并将其移到右侧。
5. 在新对话框中，选择 **Computer Account (计算机帐户)**，单击 **Next (下一步)**，然后单击 **Finish (完成)**。
6. 单击 **OK (确定)**。
7. 从新添加的树中展开 **Certificates (证书)**。
8. 右键单击 **Personal (个人)**，选择 **All Tasks (所有任务)** → **Request New Certificate (申请新证书)**。
9. 单击 **Next (下一步)**。
10. 选择合适的证书类型，一般是 **Computer (计算机)**，然后单击 **Enroll (登记)**。
11. 单击 **Finish (完成)**。

使用认证机构签署的有效证书创建 HTTPS 侦听器

运行安装程序，单击前提条件检查程序上的链接以创建 HTTPS 侦听器。

使用 SelfSSL 工具生成自签署证书

1. [创建证书](#)
2. [添加证书和记录指纹](#)
3. [创建 WinRM HTTPS 侦听器](#)
4. [为 WinRM 配置信封大小](#)

创建证书

1. 从 microsoft.com/downloads/details.aspx?FamilyID=56fc92ee-a71a-4c73-b628-ade629c89499&displaylang 下载 **IIS 资源套件**。

2. 运行 `iis60rkt.exe`。
3. 单击"Next" (下一步)。
4. 选择"End-User License Agreement" (最终用户许可协议) 屏幕中的"I Agree" (我同意), 并单击"Next" (下一步)。
5. 单击"Next" (下一步)。
6. 在"Select Type" (选择类型) 屏幕中, 选择"Custom" (自定义) 并单击"Next" (下一步)。
7. 单击"Next" (下一步)。
8. 在"Select Features" (选择功能) 屏幕中, 选择 SelfSSL 1.0 并单击"Next" (下一步)。
9. 单击"Next" (下一步)。
10. 单击 "Finish" (完成)。
将安装 SelfSSI。
11. 单击"Start" (开始) → "Programs" (程序) → "IIS Resource" (IIS 资源) → SelfSSL → SelfSSL。
12. Type (类型)
`selfssl /T /N:CN=<计算机名称或域名>`

添加证书和记录指纹

如果系统上已经安装了 Internet 信息服务 (IIS), 则 `CertificateThumbprint` 的值必须是空字符串, 而且您不必执行本节中的步骤。例如:

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname=  
'<主机名>';CertificateThumbprint=""}
```

1. 单击 Start (开始) → Run (运行)。
2. 键入 `mmc`, 然后单击"OK" (确定)。
3. 单击"File" (文件) → "Add/Remove Snap-in" (添加/删除管理单元)。
4. 单击 "Add" (添加)。
5. 选择"Certificates" (证书) 并单击"Add" (添加)。
6. 选择"Computer account" (计算机帐户) 选项并单击"Next" (下一步)。
7. 选择"Local Computer" (本地计算机) 并单击"Finish" (完成)。
8. 单击 Close (关闭)。
9. 单击 "OK" (确定)。
10. 在"Console" (控制台) 屏幕中, 展开左侧导航窗格中的"Certificates (Local Computer)" (证书 [本地计算机])。
11. 展开"Personal" (个人)。
12. 选择"Certificates" (证书)。
13. 在右窗格中, 双击所需的证书。
将显示"Certificate" (证书) 屏幕。
14. 单击"Details" (详细信息) 选项卡。
15. 选择"Thumbprint" (指纹)。
将指纹复制到剪贴板。在创建 HTTP 侦听器时可以使用此参数。

16. 单击“OK”（确定）。


创建 WinRM HTTPS 侦听器

要在 WinRM 中启用 HTTPS 侦听器，请键入以下命令：

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname=  
'<主机名>';CertificateThumbprint="6e132c546767bf16a8acf4fe0e713d5b2da43013"}
```

如果您使用 Windows 2008 Small Business Server，则按如下将 CertificateThumbprint 的值保留空白：


```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname=  
'<主机名>';CertificateThumbprint=""}
```


 **注：** 确保 Hostname 和 CertificateThumbprint 的值正确无误。

默认情况下，HTTP 侦听器已启用并在端口 80 侦听。

为 WinRM 和 WMI 服务器 配置用户授权

要提供对 WinRM 和 WMI 服务的访问权限，必须为用户显式添加适当的访问级别。

 **注：** 必须使用管理员权限登录才能为 WinRM 和 WMI 服务器配置用户授权。

 **注：** 默认情况下将配置管理员。

WinRM:

1. 单击“Start”（开始）并单击“Run”（运行）。
2. 键入 winrm configsdll 并单击“OK”（确定）。

如果您使用 WinRM 版本 2.0，则键入 winrm configsdll default。

3. 单击“Add”（添加）并向列表中添加必要的用户或组（本地/域）。
4. 分别为用户提供适当的权限并单击“OK”（确定）。

WMI:

1. 单击“Start”（开始）并单击“Run”（运行）。
2. 键入 wmicmt.msc 并单击“OK”（确定）。

将显示 Windows Management Infrastructure (WMI) 屏幕。

3. 右键单击左窗格中的“WMI Control (Local)”（WMI 控制 [本地]）节点并单击“Properties”（属性）。
- 将显示“WMI Control (Local) Properties”（WMI 控制 [本地] 属性）屏幕。

4. 单击“Security”（安全）并展开命名空间树中的“Root”（根）节点。
5. 导航至“Root”（根）→ DCIM → sysman。
6. 单击“Security”（安全）。

将显示“Security”（安全）屏幕。

7. 单击“Add”（添加）并向列表中添加必要的用户或组（本地/域）。
8. 分别为用户提供适当的权限并单击“OK”（确定）。

9. 单击 "OK" (确定)。
10. 关闭 Windows Management Infrastructure (WMI) 屏幕。

为 WinRM 配置 Windows 防火墙

1. 打开控制面板。
2. 单击"Windows Firewall" (Windows 防火墙)。
3. 单击 Exceptions (例外) 选项卡。
4. 选择"Windows Remote Management" (Windows 远程管理) 复选框。如果看不到该复选框, 请单击"Add Program" (添加程序) 按钮以添加 Windows 远程管理。

为 WinRM 配置信封大小

1. 打开命令提示符。
2. 键入 winrm g winrm/config。
3. 检查 MaxEnvelopeSizekb 属性的值。如果该值小于 4608, 键入以下命令:

```
winrm s winrm/config @{MaxEnvelopeSizekb="4608"}
```
4. 将 MaxTimeoutms 的值设置为 3 分钟:

```
winrm s winrm/config @{MaxTimeoutms="180000"}
```


在 WinRM 版本 2.0 上, 启用 WinRM 版本 2.0 的兼容模式以使用端口 443。默认情况下, WinRM 版本 2.0 使用端口 5986。要启用兼容模式, 请使用以下命令:


```
winrm s winrm/config/Service @{EnableCompatibilityHttpsListener="true"}
```

安装和升级 Server Administrator


本节解释如何使用以下两个安装选项安装 Server Administrator:

- 1 使用 *Dell Systems Management Tools and Documentation DVD* 上 `\SYSMGMT\sradmin\windows` 中的安装程序安装 Server Administrator 和其它 Managed System Software。
- 1 通过 Windows 安装程序引擎 `msiexec.exe` (请参阅表 5-1), 使用无人值守安装方法在多个系统上安装 Server Administrator 和其它 Managed System Software。

 **注:** 在系统管理安装和卸载过程中, 将停止和启动简单网络管理协议 (SNMP) 服务。因此, 诸如 DSM IT Assistant 连接服务、DSM IT Assistant 网络监控服务和其它第三方服务等依赖于 SNMP 的服务将停止。在系统管理安装或卸载结束后, 将启动 IT Assistant 服务, 如果停止了第三方服务, 则需要手动重新启动这些第三方服务。

 **注:** 对于模块化系统, 必须为机箱中所装的每个服务器模块安装 Server Administrator。

 **注:** 在 PowerEdge 800、830、850 和 1800 系统上安装 Server Administrator 后, 如果选择安装 Storage Management Service, 系统可能会提示重新引导系统。

 **注:** 在支持的 Windows 系统上安装 Server Administrator 过程中, 如果出现 Out of Memory (内存不足) 错误信息, 则必须退出安装并释放内存。关闭其它应用程序或执行任何其它可以释放内存的任务, 然后再重试尝试安装 Server Administrator。

安装程序会调用前提条件检查程序, 后者使用系统的 PCI 总线搜索控制器卡等已安装硬件。

Dell OpenManage 安装程序为安装 Server Administrator 和其它 Managed System Software 提供了 "Typical Setup" (典型安装) 选项和 "Custom Setup" (自定义安装) 选项。

要了解 Dell OpenManage 中提供的 Server Administrator 的各个组件的信息并且帮助您选择所需的安装组件, 请参阅 ["Server Administrator 的部署情况"](#)。


典型安装


当前提条件检查程序启动 Server Administrator 安装程序并选择 "Typical Setup" (典型安装) 选项时, 安装程序将安装以下 Managed System Software 功能:

- 1 Server Administrator Web Server
- 1 Server Instrumentation
- 1 Remote Access Controller

- 1 Intel SNMP Agent
- 1 Broadcom SNMP Agent。


在**典型**安装期间，各个管理站服务不会安装在不符合服务特定硬件和软件要求的受管系统上。例如，如果受管系统未安装 Remote Access Controller，则在**"Typical"（典型）**安装过程中不会安装 Dell OpenManage Server Administrator Remote Access Controller 服务软件模块。不过，可以转至**"Custom Setup"（自定义安装）**并选择安装 **Remote Access Controller** 软件模块。

 **注：** 只有使用**"Custom Setup"（自定义安装）**选项才提供 Remote Enablement 功能。

 **注：** Server Administrator 安装还会在系统上安装一些必要的 Visual C++ 运行时组件。

自定义安装

以下各节说明了如何使用**"Custom Setup"（自定义安装）**选项安装 Server Administrator 和其它受管系统软件。

 **注：** Management Station 和 Managed System 服务既可以安装在相同目录也可以安装在不同目录。您可以选择安装目录。

1. 以内置管理员权限登录到要安装系统管理软件的系统上。
2. 关闭所有打开的应用程序并禁用任何病毒扫描软件。
3. 将 *Dell Systems Management Tools and Documentation DVD* 插入系统的 DVD 驱动器。系统将显示自动运行菜单。
4. 从自动运行菜单中选择 **Dell OpenManage Server Administrator**，然后单击**"Install"（安装）**。

如果自动运行程序不自动启动，则转至 DVD 上的 `SYSMGMT\srvadmin\windows` 目录，然后运行 `setup.exe` 文件。

"Dell OpenManage Server Administrator prerequisite"（Dell OpenManage Server Administrator 前提条件） 状况屏幕会打开并对受管系统运行前提条件检查。系统会显示任何相关的通知、警告或错误信息。解决任何出现的错误和警告情况。

5. 单击**"Install, Modify, Repair, or Remove Server Administrator"（安装、修改、修复或删除 Server Administrator）**选项。

"Welcome to the Install Wizard for Dell OpenManage Server Administrator "（欢迎使用 Dell OpenManage Server Administrator 安装向导） 屏幕会打开。

6. 单击**"Next"（下一步）**。

Dell 软件许可协议将会出现。

7. 如果同意，单击**"I accept the terms in the license agreement"（我接受许可协议中的条款）**并单击**"Next"（下一步）**。

"Setup Type"（安装类型）对话框会打开。

8. 选择**"Custom"（自定义）**并单击**"Next"（下一步）**。

"Custom Setup"（自定义安装）对话框会打开。

请参阅[表 4-1](#)和[表 4-2](#) 以便帮助您为系统选择 Server Administrator 组件。


如果在非 Dell PowerEdge 系统上安装 Server Administrator，安装程序将仅显示 **Server Administrator Web Server** 选项。

所选功能的旁边有一个硬盘驱动器图标。未选功能旁边有一个红色的 **X**。默认情况下，如果前提条件检查程序发现没有支持硬件的软件功能，检查程序会取消选择它们。

要接受安装 Managed System Software 的默认目录路径，请单击**"Next"（下一步）**。否则，请单击**"Change"（更改）**并浏览至要安装 Managed System Software 的目录，然后单击**"OK"（确认）**。您将返回到**"Custom Setup"（自定义安装）**对话框。

9. 单击**"Next"（下一步）**接受要安装的所选软件功能。

"Ready to Install the Program"（准备安装程序）对话框将会显示。

 **注：** 可以单击**"Cancel"（取消）**取消安装过程。安装将回滚所作的更改。如果在安装过程的某个时刻以后单击**"Cancel"（取消）**，安装可能不会正确回滚，从而给系统留下不完整的安装。请参阅[安装失败时的系统恢复](#)。


10. 单击**"Install"（安装）**以安装选定的软件功能。

"Installing Dell OpenManage Server Administrator"（安装 Dell OpenManage Server Administrator） 屏幕将会出现并提供所安装软件功能的状况和进度。所选组件安装后，**"Install Wizard Completed"（安装向导已完成）**对话框将会打开。

11. 单击**"Finish"（完成）**退出 Server Administrator 安装。

如果提示重新引导系统，请重新引导它以便使安装的 Managed System Software 服务可以使用。如果提示重新引导系统，请选择一种重新引导选项：

- 1 是，现在重新引导系统。
- 1 否，稍后重新引导系统。

 **注：** 如果在安装过程中选择了 **Remote Enablement**，在 Windows 事件日志中将记录错误信息“A provider, WinTunnel, has been registered in the Windows Management Instrumentation namespace ROOT\dcim\sysman to use the LocalSystem account. This account is privileged and the provider may cause a security violation if it does not correctly impersonate user requests.”（提供程序 WinTunnel 已在 Windows 管理规范名称空间 ROOT\dcim\sysman 中注册以使用 LocalSystem 帐户。该帐户享有特权，如果提供程序不正确地模拟用户请求，可能会导致违反安全保护。）您可以放心忽略此信息并继续安装。

合并安装 Server Administrator 与 Citrix Application Server

Citrix 会在安装后重新映射所有硬盘驱动器号。例如，如果在驱动器 C: 上安装 Server Administrator，然后再安装 Citrix，则它会将驱动器号 C: 更改为 M:。由于进行了重新映射，Server Administrator 可能无法正常工作。

为避免此问题，请选择以下选项之一：

选项 1：

- 1. 卸载 Server Administrator。
- 2. 安装 Citrix。
- 3. 重新安装 Server Administrator。

选项 2：

安装完 Citrix 后，键入以下命令：


```
msiexec.exe /fa SysMgmt.msi
```


升级 Managed System Software

Dell OpenManage 安装程序为 Server Administrator 和其它 Managed System Software 的升级提供了“Upgrade”（升级）选项。

安装程序会运行**前提条件检查程序**，后者则使用系统的 PCI 总线搜索控制器卡等已安装硬件。

安装程序会安装或升级所有适合特定系统硬件配置的 Managed System Software 功能。

 **小心：** Dell OpenManage Array Manager 不再受支持。如果升级装有 Array Manager 的系统（装有 Dell OpenManage 5.0 或更高版本），则在升级过程中将会删除 Array Manager。但您可以使用 Storage Management Service。

 **注：** 升级时将保留所有用户设置。

以下程序说明了如何升级 Server Administrator 和其它 Managed System Software。

升级原则

- 1 无法将早于版本 5.0 的 Server Administrator 升级到版本 6.3。必须升级到 Server Administrator 5.0 或更高版本，然后再升级到 Server Administrator 版本 6.3。
- 1 如果已经在 Managed System 上安装了 Server Instrumentation，请确保安装 Server Administrator Web Server 版本 6.1 或更高版本。安装较早版本的 Server Administrator Web Server 可能会显示错误。
- 1 如果已经安装了 Server Administrator Web Server 版本 6.3，请确保在 Managed System 上安装 Server Instrumentation 版本 6.3。使用 Server Administrator Web Server 版本 6.3 访问较早版本的 Server Administrator 可能会显示错误。

升级

- 1. 将 *Dell Systems Management Tools and Documentation DVD* 插入系统的 DVD 驱动器。系统将显示自动运行菜单。
- 2. 选择 **Dell OpenManage Server Administrator** 并单击“Install”（安装）。

如果自动运行程序不自动启动，转至 DVD 上的 `SYSMGMT\srvadmin\windows` 目录，然后运行 `setup.exe` 文件。

“Dell OpenManage Server Administrator prerequisite”（Dell OpenManage Server Administrator 前提条件）状况屏幕会打开并对 Managed Station 运行前提条件检查。系统会显示任何相关的通知、警告或错误信息。

3. 单击"Install, Modify, Repair, or Remove Server Administrator" (**安装、修改、修复或删除 Server Administrator**) 选项。
"Welcome to the Install Wizard for Dell OpenManage Server Administrator " (欢迎使用 Dell OpenManage Server Administrator 安装向导) 屏幕会打开。
4. 单击"Next" (**下一步**)。

Dell 软件许可协议将会出现。
5. 如果同意, 单击"I accept the terms in the license agreement" (**我接受许可协议中的条款**) 并单击"Next" (**下一步**)。

"Setup Type" (**安装类型**) 对话框会打开。
6. 按自定义安装一节所述从 [步骤 8](#) 开始继续安装。

修改

如果要添加/删除 Server Administrator 组件:

1. 导航至 Windows **控制面板**。
2. 双击"Add/Remove Programs" (**添加/删除程序**)。
3. 单击 Dell OpenManage Server Administrator 并单击"Change" (**更改**)。

"Welcome to the Install Wizard for Dell OpenManage Server Administrator " (欢迎使用 Dell OpenManage Server Administrator **安装向导**) 对话框会打开。
4. 单击"Next" (**下一步**)。

"Program Maintenance" (**程序维护**) 对话框将会打开。
5. 选择"Modify" (**修改**) 选项并单击"Next" (**下一步**)。

"Custom Setup" (**自定义安装**) 对话框会打开。
6. 要选择特定的 Managed System Software 应用程序, 单击所列功能旁边的下拉箭头并选择"This feature will be installed..." (**此功能将会安装...**) 来安装该功能, 或者选择"This feature will not be available" (**此功能将不可用**) 不进行安装。


所选功能的旁边有一个硬盘驱动器图标。未选功能旁边有一个红色的 X。默认情况下, 如果前提条件检查程序发现没有支持硬件的软件功能, 则检查程序会取消选中该功能。
7. 单击"Next" (**下一步**) 接受要安装的所选软件功能。

"Ready to Modify the Program" (**准备修改程序**) 对话框将会显示。
8. 单击"Install" (**安装**) 以安装选定的软件功能。

"Installing Dell OpenManage Server Administrator" (**安装 Dell OpenManage Server Administrator**) 屏幕将会打开。信息将提供所安装软件功能的状况和进程。

安装所选功能后, 会出现"Install Wizard Completed" (**安装向导已完成**) 对话框。
9. 单击"Finish" (**完成**) 退出 Server Administrator 安装。

如果提示重新引导系统, 则必须重新引导它以使安装的 Managed System Software 服务可以使用。如果提示重新引导系统, 请选择一种重新引导选项:
 - 1 是, 现在重新引导系统。
 - 1 否, 稍后重新引导系统。

 **注:** 如果您从另一个系统运行安装程序并使用"Modify" (**修改**) 选项尝试安装组件, 安装程序可能会显示错误。此错误可能是因为系统上从其运行安装程序的源已损坏。您可以检查以下注册表项, 验证此情况: HKLM\Software\Classes\Installer\Products\<GUID>\sourcelist\lastusedsource。如果 lastusedsource 的值是负数, 则表示源已损坏。

修复

如果要修复可能损坏的已安装 Server Administrator 组件:

1. 导航至 Windows **控制面板**。

2. 双击"Add/Remove Programs" (添加/删除程序)。
3. 单击 Dell Server Administrator 并单击"Change" (更改)。

"Welcome to the Install Wizard for Dell OpenManage Server Administrator " (欢迎使用 Dell OpenManage Server Administrator 安装向导) 对话框会打开。

4. 单击"Next" (下一步)。

"Program Maintenance" (程序维护) 对话框将会打开。

5. 选择"Repair" (修复) 选项并单击"Next" (下一步)。

"Ready to Repair the Program" (准备修复程序) 对话框将会显示。

6. 单击"Install" (安装) 以安装选定的软件功能。

"Installing Dell OpenManage Server Administrator" (安装 Dell OpenManage Server Administrator) 屏幕将会打开。显示的信息会提供所安装软件功能的状态和进度。

安装所选功能后, 会出现"Install Wizard Completed" (安装向导已完成) 对话框。

7. 单击"Finish" (完成) 退出 Server Administrator 安装。

如果提示重新引导系统, 请选择一种重新引导选项:

- 1 是, 现在重新引导系统。
- 1 否, 稍后重新引导系统。


安装失败时的系统恢复


Microsoft Software Installer (MSI) 提供了一种功能, 使系统能够在安装失败后返回到完全正常的状态。MSI 通过为安装、升级或卸载期间执行的每个标准操作都保留一个撤消操作来实现这一点。此操作包括恢复删除或改写的文件、注册表项和其它资源。Windows 会临时保存在安装或卸载期间删除或改写的任何文件以便在需要时恢复, 这是一种回滚。成功完成安装后, Windows 会删除所有临时的备份文件。

除了回滚 MSI 标准操作外, Dell OpenManage 库还能够在回滚时撤消 INI 文件中列出的各个应用程序的命令。Dell OpenManage 安装操作修改的所有文件将在回滚时恢复到原始状态。

MSI 引擎执行安装序列时, 会忽略计划为回滚操作的所有操作。如果自定义操作、MSI 标准操作或 Dell OpenManage 安装操作失败, 回滚就会开始。

安装一旦完成即不可回滚; 事务处理安装的目的只是在安装会话期间作为保护系统的安全网。例如, 如果要卸下安装的应用程序, 则只需卸载该应用程序就可以了。

 **注:** 驱动程序安装和卸载都不是安装事务处理的一部分, 因此如果在执行期间出现严重错误就不能回滚。

 **注:** 在安装程序清除期间或安装事务完成后取消的安装、卸载和升级将不能回滚。

失败的更新

供应商提供的 MSI 修补程序和更新程序必须应用到供应商提供的原 MSI 软件包中。如果有意或无意中重新打包了 MSI 软件包, 或直接进行了更改, 修补程序和更新程序可能会失败。MSI 软件包不得重新封装, 否则将更改功能结构和 GUID, 从而中断任何提供的修补程序或更新程序。当有必要对供应商提供的 MSI 软件包进行更改时, 应始终使用 .mst 转换文件。

Windows 安装程序日志记录

Windows 带有一种注册表激活的日志记录服务以帮助诊断 Windows 安装程序问题。要在无提示安装过程中启用这种日志记录服务, 打开注册表编辑器并创建以下路径和密钥:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer
Reg_SZ: 日志记录
值: voicewarmup
```

值字段中的字母可以是任何顺序。每个字母打开一种不同的日志记录模式。每个字母的实际作用如以下 MSI 版本 3.1 中所示:

- v - 详细输出
- o - 磁盘空间已满信息
- i - 状况信息
- c - 初始 UI 参数
- e - 所有错误信息
- w - 非严重警告
- a - 操作启动
- r - 操作特定的记录
- m - 内存不足或严重退出信息

u - 用户请求
p - 终端属性
+ - 附加到现有文件
! - 将每一行刷新到日志
*** - 通配符，记录除 v 选项之外的所有信息。要包括 v 选项，指定 "/!*v"。

一旦激活，就可以找到 %TEMP% 目录中生成的日志文件。此目录中生成的日志文件有：

- 1 受管系统安装
 - o SysMgmt.log
- 1 管理站安装
 - o MgmtSt.log

如果前提条件检查程序用户界面 (UI) 正在运行，会默认创建这些特定日志文件。

执行 Managed System Software 的无人值守安装


Dell OpenManage 安装程序为无人值守安装过程提供了“Typical Setup”（典型安装）选项和“Custom Setup”（自定义安装）选项。

无人值守安装使您可以在多个系统上同时安装 Server Administrator。您可以通过创建包含所有必需的 Managed System Software 文件的无人值守安装软件包来执行无人值守安装。无人值守安装选项还提供了一些功能，使用户可以配置、验证和查看有关无人值守安装的信息。

无人值守安装软件包使用独立软件供应商 (ISV) 的软件分发工具分发至远程系统。软件包分发完毕后，安装脚本将执行软件安装。

创建和分发典型无人值守安装软件包

无人值守安装的“Typical Setup”（典型安装）选项将 *Dell Systems Management Tools and Documentation* DVD 用作无人值守安装软件包。msiexec.exe /i SysMgmt.msi /qb 命令会访问 DVD 以接受软件许可协议并在所选远程系统上安装所有必要的 Server Administrator 功能。msiexec.exe /i SysMgmt.msi /qb 命令将根据系统硬件配置在每个远程系统上安装 Server Administrator 功能。

 **注：** 无人值守安装完成后，为了使用 Server Administrator 的命令行界面 (CLI) 功能，必须打开新的控制台窗口并在那里执行 CLI 命令。从安装 Server Administrator 的同一控制台窗口执行 CLI 命令不会起作用。

可以将 DVD 映像提供给远程系统，方法是通过分发介质的整个内容，也可以通过从目标系统到 DVD 映像的位置映射驱动器。

映射驱动器以用作典型无人值守安装软件包

1. 将 *Dell Systems Management Tools and Documentation* DVD 映像与要安装 Server Administrator 的每个远程系统进行共享。

您可以通过直接共享 DVD 或将整个 DVD 复制到驱动器并共享备份来完成此任务。

2. 创建一个脚本，该脚本从远程系统到 [步骤 1](#) 中说明的共享驱动器映射一个驱动器。此脚本应在驱动器映射后执行 msiexec.exe /i Mapped Drive\SYSTEMGMT\svradmin\windows\SystemManagement\SysMgmt.msi /qb 。

3. 配置 ISV 分发软件以分发和执行 [步骤 2](#) 中创建的脚本。

4. 使用 ISV 软件分发工具将该脚本分发至目标系统。

此脚本在每个远程系统上执行以安装 Server Administrator。

5. 重新引导每个远程系统以启用 Server Administrator。

分发整个 DVD 以用作典型无人值守安装软件包

1. 将 *Dell Systems Management Tools and Documentation* DVD 的整个映像分发至目标系统。

2. 配置 ISV 分发软件以从 DVD 映像执行 msiexec.exe /i DVD Drive\SYSTEMGMT\svradmin\windows\SystemManagement\SysMgmt.msi /qb 命令。


此程序在每个远程系统上执行以安装 Server Administrator。

3. 重新引导每个远程系统以启用 Server Administrator。

创建和分发自定义无人值守安装软件包

要创建自定义无人值守安装软件包，请执行以下步骤：

1. 将 `SYSMGMT\srvadmin\windows` 目录从 DVD 复制到系统硬盘驱动器。
2. 创建将使用 Windows 安装程序引擎 (`msiexec.exe`) 执行安装的批处理脚本。

 **注：** 对于自定义无人值守安装，每个所需功能都必须作为命令行界面 (CLI) 参数包括在内才能被安装。

例如，`msiexec.exe /i SysMgmt.msi ADDLOCAL=SA,IWS,BRCM /qb`。（有关更多详情和可用功能标识，请参阅“[自定义参数](#)”。）

3. 将该批处理脚本放在系统硬盘驱动器上的 `windows` 目录中。

分发自定义无人值守安装软件包

 **注：** “Custom Setup”（自定义安装）无人值守安装（请参阅“[创建和分发自定义无人值守安装软件包](#)”）中使用的 Server Administrator 的 `SysMgmt.msi` 安装软件包位于 DVD 的 `SYSMGMT\srvadmin\windows\SystemManagement` 目录中。

1. 配置 ISV 分发软件在分发安装软件包后执行批处理脚本。
2. 使用 ISV 分发软件将自定义无人值守安装软件包分发至远程系统。
批处理脚本在每个远程系统上安装 Server Administrator 以及特定的功能。
3. 重新引导每个远程系统以启用 Server Administrator。

指定日志文件位置

对于受管系统 MSI 安装，运行以下命令执行无人值守安装，同时指定日志文件位置：

```
msiexec.exe /i SysMgmt.msi /l*v "C:\openmanage\logs\SysMgmt.log"
```

无人值守安装功能

无人值守安装提供以下功能：

- 1 一组可选的命令行设置，用于自定义无人值守安装
- 1 自定义参数，用于指定要安装的特定软件功能。
- 1 前提条件检查程序，用于检查所选软件功能的相关性状况，而无需执行实际的安装。

可选命令行设置

[表 5-1](#) 显示了为 `msiexec.exe` MSI 安装程序提供的可选设置。在命令行上，在 `msiexec.exe` 后面键入可选的设置，各个设置间带一个空格。


 **注：** 请参阅 support.microsoft.com 详细了解 Windows 安装程序工具所有的命令行开关。

表 5-1. MSI 安装程序命令行设置

设置	结果
<code>/i <软件包 产品代码></code>	此命令安装或配置产品。 <code>/i SysMgmt.msi</code> - 安装 Server Administrator 软件。
<code>/i SysMgmt.msi /qn</code>	此命令将执行版本 6.1 的全新安装。
<code>/x <软件包 产品代码></code>	此命令卸载产品。 <code>/x SysMgmt.msi</code> - 卸载 Server Administrator 软件。
<code>/q[n b z f]</code>	此命令设置用户界面 (UI) 级别。 <code>/q</code> 或 <code>/qn</code> - 无 UI。此选项用于无提示和无人值守安装。

	<p>/qb - 基本 UI。此选项用于无人值守安装，但不是无提示安装。</p> <p>/qr - 精简的 UI。此选项用于无人值守安装，同时显示一个指示安装进度的模式对话框。</p> <p>/qf - 完全 UI。此选项用于标准有人值守安装。</p>
/f[p o e d c a u m s v] 软件包 产品代码>	<p>此命令修复产品。</p> <p>/fp - 此选项只在缺少文件时重新安装产品。</p> <p>/fo - 此选项在缺少文件或安装了较旧版本的文件时重新安装产品。</p> <p>/fe - 此选项在缺少文件或安装了相同或较旧版本的文件时重新安装产品。</p> <p>/fd - 此选项在缺少文件或安装了不同版本的文件时重新安装产品。</p> <p>/fc - 此选项在缺少文件或存储的校验和值与计算值不匹配时重新安装产品。</p> <p>/fa - 此选项强制重新安装所有文件。</p> <p>/fu - 此选项重写所有必需的用户特定注册表项。</p> <p>/fm - 此选项重写所有必需的系统特定注册表项。</p> <p>/fs - 此选项会覆盖所有现有的快捷方式。</p> <p>/fv - 此选项从源程序运行并更新本地软件包高速缓存。对于一个应用程序或功能的首次安装，不要使用 /fv 重新安装选项。</p>
INSTALLDIR=<路径>	<p>此命令将产品安装到特定的位置。如果用此开关指定安装目录，则必须在执行 CLI 安装命令前手工创建，否则命令将会失败，并且不会显示为什么会失败的错误或信息。</p> <p>/i SysMgmt.msi INSTALLDIR=c:\OpenManage /qn - 以 c:\OpenManage 为安装位置，将产品安装到这个特定位置。</p>

例如，运行 `msiexec.exe /i SysMgmt.msi /qn` 会在每个远程系统上基于系统硬件配置安装 Server Administrator 功能。此安装会以无提示并且无人值守的方式完成。

自定义参数

 **注：** 键入大写的 REINSTALL 和 REMOVE CLI 参数，它们可以区分大小写。

通过 **REINSTALL** 和 **REMOVE** 自定义 CLI 参数，可以自定义在无提示或无人值守运行时要安装、重新安装或卸载的确切软件功能。借助自定义参数，可以使用相同的无人值守安装软件包为不同的系统选择性安装、重新安装或卸载软件功能。例如，可以在一组特定服务器上选择安装 Server Administrator，而不安装 Remote Access Controller 服务，在另一组服务器上选择安装 Server Administrator，而不安装 Storage Management Service。还可以选择在一组特定服务器上卸载一个或多个功能。



 **注：** [表 5-2](#) 中所述的软件功能 ID 区分大小写。

表 5-2. 软件功能 ID

功能 ID	说明
ALL	所有功能
BRCM	Broadcom NIC 代理
INTEL	Intel NIC 代理
IWS	Dell OpenManage Server Administrator Web Server
OMSM	Server Administrator Storage Management Service
RmtMgmt	Remote Enablement
RAC4	Remote Access Controller (DRAC 4)
RAC5	Remote Access Controller (DRAC 5)
iDRAC	Integrated Dell Remote Access Controller
SA	Server Administrator

 **注：** xx1x 系统仅支持 iDRAC6。

可以在命令行中包含 **REINSTALL** 自定义参数，并指定要重新安装的软件功能的一个或多个功能 ID。比如

```
msiexec.exe /i SysMgmt.msi REINSTALL=BRCM /qb.
```

此命令会运行 Dell OpenManage Systems Management 的安装，并只重新安装 Broadcom 代理，模式为无人值守，但不是无提示。

可以在命令行中包含 **REMOVE** 自定义参数，指定要卸载的软件功能的一个或多个功能 ID。比如

```
msiexec.exe /i SysMgmt.msi REMOVE=BRCM /qb.
```

此命令会运行 Dell OpenManage Systems Management 的安装，并只卸载 Broadcom 代理，模式为无人值守，但不是无提示。

还可以选择运行 `msiexec.exe` 程序一次性安装、重新安装和卸载功能。比如

```
msiexec.exe /i SysMgmt.msi REMOVE=BRCM /qb
```

此命令会运行 Managed System 软件的安装，并卸载 Broadcom 代理程序。将会在无人值守但不是无提示模式下执行。

注： 全局唯一标识符 (GUID) 有 128 位长，用于生成 GUID 的算法保证了每个 GUID 都是唯一的。产品 GUID 唯一标识应用程序。在这种情况下，Server Administrator 的产品 GUID 是 {54C04D53-C3C3-46EA-A75F-7AFF4BEB727C}。

MSI 返回代码

应用程序事件记录项记录在 `SysMgmt.log` 文件中。表 5-3 显示了 `msiexec.exe` Windows 安装程序引擎返回的一些错误代码。

表 5-3. Windows 安装程序返回代码

错误代码	值	说明
ERROR_SUCCESS	0	操作成功完成。
ERROR_INVALID_PARAMETER	87	其中一个参数无效。
ERROR_INSTALL_USEREXIT	1602	用户取消了安装。
ERROR_SUCCESS_REBOOT_REQUIRED	3010	需要重新启动以完成安装。此信息表示成功安装。

注： 请参阅 support.microsoft.com 详细了解 `msiexec.exe` 和 `InstMsi.exe` Windows 安装程序功能返回的所有错误代码。

卸载 Managed System Software

可以通过使用 *Dell Systems Management Tools and Documentation DVD* 或操作系统卸载受管系统软件功能。此外，您还可以在多个系统上同时执行无人值守卸载。

使用 Dell 提供的介质卸载 Managed System Software

1. 将 *Dell Systems Management Tools and Documentation DVD* 插入系统的 DVD 驱动器。

如果安装程序不自动启动，运行 DVD 上 `SYSMGMT\sradmin\windows` 目录中的 `setup.exe`。

"Dell OpenManage Server Administrator prerequisite" (Dell OpenManage Server Administrator 前提条件) 状况屏幕会打开并对受管系统运行前提条件检查。将会显示检查期间检测到的任何相关的通知、警告或错误信息。

2. 单击 "Install, Modify, Repair, or Remove Server Administrator" (安装、修改、修复或删除 Server Administrator) 选项。

"Welcome to the Install Wizard for Dell OpenManage Server Administrator" (欢迎使用 Dell OpenManage Server Administrator 安装向导) 屏幕会打开。

3. 单击 "Next" (下一步)。

"Program Maintenance" (程序维护) 对话框将会打开。

此对话框使您能够修改、修复或删除程序。

4. 选择 "Remove" (删除) 选项并单击 "Next" (下一步)。

"Remove the Program" (删除程序) 对话框将会打开。

5. 单击 "Remove" (删除)。

"Uninstalling Dell OpenManage Server Administrator" (卸载 Dell OpenManage Server Administrator) 屏幕将会出现并提供正在被卸载的软件功能的状况和进度。

所选功能卸载后，"Install Wizard Completed" (安装向导已完成) 对话框将会打开。

6. 单击 "Finish" (完成) 退出 Server Administrator 卸载。

如果提示重新引导系统，则必须重新引导系统才能成功卸载。如果提示重新引导系统，请选择一种重新引导选项：

- 1 是，现在重新引导系统。
- 1 否，稍后重新引导系统。

将卸载所有 Server Administrator 功能。

使用操作系统卸载 Managed System Software 功能

1. 导航至 Windows **控制面板**。
2. 双击“Add/Remove Programs”（**添加/删除程序**）。
3. 单击 **Dell OpenManage Server Administrator** 并单击“Remove”（**删除**）。

“Add or Remove Programs”（**添加或删除程序**）对话框会打开。

4. 单击“**Yes**”（**是**）确认卸载 Server Administrator。

Dell OpenManage Server Administrator 屏幕将会打开并提供正在被卸载的软件功能的状况和进度。

如果提示重新引导系统，则必须重新引导才能成功卸载。如果提示重新引导系统，请选择一种重新引导选项：

- 1 **是，现在重新引导系统。**
- 1 **否，稍后重新引导系统。**

将卸载所有 Server Administrator 功能。

使用产品 GUID 进行无人值守卸载

如果卸载时没有可用的安装 DVD 或 MSI 软件包，可使用以下命令行在运行 Windows 的 Managed System 或 Management Station 上卸载 Dell OpenManage 系统管理软件。对于这些情况，可使用软件包 GUID 卸载产品。

对于受管系统，使用此命令：

```
msiexec.exe /x {54C04D53-C3C3-46EA-A75F-7AFF4BEB727C}
```

执行无人值守的 Managed System Software 卸载

Dell OpenManage 安装程序提供了无人值守卸载过程。无人值守卸载使您可以从多个系统同时卸载 Managed System Software。无人值守卸载软件包使用 ISV 软件分发工具分发至远程系统。软件包分发完毕后，卸载脚本将执行以卸载软件。

分发无人值守卸载软件包

Dell Systems Management Tools and Documentation DVD 已经过预先配置可作为无人值守卸载软件包。要将该软件包分发至一个或多个系统，请执行以下步骤：

1. 配置 ISV 分发软件以
在分发无人值守卸载软件包后执行 `msiexec.exe /x DVD Drive\SYSTEM\svradmin\windows\SystemManagement\SystemMgmt.msi /qb` 命令（如果使用的是 DVD）。

2. 使用 ISV 分发软件将典型无人值守卸载软件包分发至远程系统。

此程序在每个远程系统上执行以卸载 Managed System Software。

3. 重新引导每个远程系统以完成卸载过程。

无人值守卸载命令行设置

[表 5-1](#) 显示无人值守卸载可用的无人值守卸载命令行设置。在命令中，在 `msiexec.exe /x SysMgmt.msi` 后面键入可选的设置，各个设置间带一个空格。

例如，运行 `msiexec.exe /x SysMgmt.msi /qb` 将会运行无人值守卸载，并在运行时显示无人值守安装状况。

运行 `msiexec.exe /x SysMgmt.msi /qn` 将运行无人值守无提示（不显示窗口）的卸载。

使用第三方部署软件进行 Managed System Software 安装

您可以使用第三方部署软件，比如 Altiris Deployment Solution，将 Managed System Software 安装到所支持的 Dell 系统上。要使用 Altiris 分发和安装 Server

Administrator, 请启动 Altiris 应用程序并导入位于 *Dell Systems Management Tools and Documentation* DVD 上: `SYSMGMT\sradmin\support\Altiris` 中的 **OpenManage_Jobs.bin**。指定要导入 **OpenManage_Jobs.bin** 的工作文件夹。可能需要修改"Run Script" (运行脚本) 和"Copy File" (复制文件) 任务来与部署环境相匹配。完成后, 还可安排将在 Altiris Deployment Solution 中管理的所支持 Dell 系统上运行的工作。

[目录](#)

[目录](#)

简介 安装指南

- [概览](#)
- [Dell OpenManage Systems Management Software](#)
- [可能需要的其它说明文件](#)
- [获得技术帮助](#)


概览

本指南包含的信息可以帮助您在 Managed System 上安装 Dell™ OpenManage™ Server Administrator。Managed System 装有支持的工具代理程序，允许通过 Server Administrator 对系统进行查找并轮询其状态。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。有关 Server Administrator 的详情，请参阅“[Dell OpenManage Server Administrator](#)”。

本说明文件还包含关于安装和使用 Dell OpenManage Server Administrator 的 **Remote Enablement** 功能的信息。包含关于使用 Dell OpenManage Server Administrator Web Server 管理远程系统的信息。目前，Microsoft® Windows®、Microsoft Hyper-V™、Hyper-V Server、Red Hat Enterprise Linux®、Suse Enterprise Linux®、VMware® ESXi、ESX 和 Citrix™ XenServer™ 5.6 操作系统支持 **Remote Enablement** 功能。

此外，本指南提供了在部署或升级之前或期间配置系统的信息和说明。本说明文件包含以下主题：

- 1 [Dell OpenManage 安全保护](#)
- 1 [设置和管理](#)
- 1 [Server Administrator 的部署情况](#)
- 1 [在 Microsoft Windows 操作系统上安装 Managed System Software](#)
- 1 [在 Microsoft Windows Server 2008 Core 和 Microsoft Hyper-V Server 上安装 Dell OpenManage 软件](#)
- 1 [在支持的 Linux 操作系统上安装 Managed System Software](#)
- 1 [VMware ESXi 上的 Dell OpenManage](#)
- 1 [使用 Microsoft Active Directory](#)
- 1 [前提条件检查程序](#)
- 1 [常见问题](#)

 **注：** 如果在同一系统上安装 Management Station 和 Managed System Software，应安装相同版本的软件以避免系统冲突。

Dell OpenManage Systems Management Software

Dell OpenManage Systems Management Software 是一套针对 Dell 系统的应用程序。此软件使用户能够通过主动监测、诊断、通知和远程访问来管理系统。

Dell Systems Management Software 由 3 张 DVD 组成：

- 1 *Dell Systems Management Tools and Documentation* DVD
- 1 *Dell Server Updates* DVD
- 1 *Dell Management Console* DVD

Dell Systems Management Tools and Documentation DVD

根据 *Dell Systems Management Tools and Documentation* DVD 的用途可以将系统分为：

- 1 Managed System

Managed System 是任何使用 Dell OpenManage Server Administrator (DVD 上的系统管理工具之一) 监控和管理的系统。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。有关 Server Administrator 的详情，请参阅“[Dell OpenManage Server Administrator](#)”。

- 1 Management Station

Management Station 是用于从集中位置远程管理一台或多台 Managed System 的计算机 (膝上型计算机、台式机或服务器)。以下应用程序包含 Dell Management Station Software，您可以使用 *Dell Systems Management Tools and Documentation* DVD 安装该软件：

- 1 Active Directory 管理单元
- 1 BMC 应用程序
- 1 DRAC 工具

有关安装这些应用程序的信息，请参阅 *Dell Systems Management Tools and Documentation DVD* 或 support.dell.com/support/edocs/software/omswrels/index.htm 上的《*Dell OpenManage Management Station 软件安装指南*》。此链接还包含 Dell OpenManage 应用程序的用户说明文件。

Dell Systems Management Tools and Documentation DVD 还包含以下产品：

Dell Systems Build and Update Utility

功能

可以使用 Dell Systems Build and Update Utility 执行以下操作：

- 1 更新系统固件和安装操作系统。
- 1 在多系统的预操作系统环境中更新固件和 BIOS。
- 1 配置系统硬件。
- 1 自定义 Server Update Utility (SUU) 并使用它更新系统。

有关执行这些任务的信息和 Dell Systems Build and Update Utility 的详情，请参阅 support.dell.com/support/edocs/software/omswrels/index.htm 上的《*Dell Systems Build and Update Utility 用户指南*》。

在 DVD 中的位置

<DVD root>

Dell OpenManage Server Administrator

功能

Dell OpenManage Server Administrator 提供了一组全面的集成管理服务，它专为系统管理员设计，用于在本地管理系统或在网络上远程管理系统。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。

有关安装 Server Administrator 的信息，请参阅“在 [Microsoft Windows 操作系统上安装 Managed System Software](#)”或“在 [支持的 Linux 操作系统上安装 Managed System Software](#)”。

有关使用 Server Administrator 的详情，请参阅 support.dell.com/support/edocs/software/omswrels/index.htm 上的《*Dell OpenManage Server Administrator 用户指南*》。

Storage Management Service 提供用于管理系统本地连接 RAID 和非 RAID 磁盘存储器的增强功能。

Storage Management Service 提供以下功能：

- 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 SAS、SCSI、SATA 和 ATA，但不支持光纤信道。
- 1 可以让您通过单一图形界面或 CLI 对所有支持的 RAID 和非 RAID 控制器和机柜执行控制器和机柜功能，而无需使用控制器 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。

在 DVD 中的位置

<DVD 驱动器>\SYSMGMT\svradmin

Dell Server Updates DVD

Dell Server Updates DVD 以及 *Dell Systems Management Tools and Documentation DVD* 是 Dell OpenManage 订购服务套件的一部分。*Dell Server Updates DVD* 仅提供给已订阅了订阅服务的客户。

Dell Server Updates DVD 包含 Dell Update Package (DUP) 和 Dell OpenManage Server Update Utility (SUU)。DUP 允许管理员同时更新大量的系统组件，并将脚本应用到一组类似的 Dell 系统，以便将系统软件组件升级到相同的版本级别。

SUU 是确定并应用更新到系统的应用程序。可以使用 SUU 更新 Dell 系统或查看 SUU 支持的任何系统的可用更新。

除了帮助您安装、配置和更新程序和操作系统外，*Dell Server Updates DVD* 还为系统提供更新版本的软件。

有关 DUP 和 SUU 的详情, 请参阅 support.dell.com/support/edocs/software/omswarels/index.htm 上的《Dell Update Package 用户指南》和《Dell OpenManage Server Update Utility 用户指南》。

有关订阅服务的详情, 请参阅 www.dell.com/openmanagesubscription 或联系销售代表。

Dell Management Console DVD

Dell Management Console 是基于 Web 的系统管理软件, 该软件使您能够发现网络中的设备并对其进行资源清册。它还提供高级功能, 例如联网设备的运行状况和性能监测, 以及 Dell 系统的增补软件管理功能。

Dell Management Console DVD 随所有 Dell xx0x 及更高版本的系统提供。也可以从 www.dell.com/openmanage 下载 Dell Management Console。

可能需要的其它说明文件

除本指南外, 还可以在 *Dell Systems Management Tools and Documentation DVD* 或 Dell 支持网站 support.dell.com/manuals 上访问以下指南。在“Manuals”（手册）页上, 单击“Software”（软件）→“Systems Management”（系统管理）。单击右侧的相应产品链接以访问文档。

- 1 《Dell Unified Server Configurator 用户指南》提供了有关使用 Unified Server Configurator 的信息。
- 1 《Dell Management Console 用户指南》包含有关安装、配置和使用 Dell Management Console 的信息。Dell Management Console 是基于 Web 的系统管理软件, 该软件使您可以查找网络上的设备并对其进行资源清册。它还提供高级功能, 例如联网设备的运行状况和性能监测, 以及 Dell 系统的增补软件管理功能。
- 1 《Dell Systems Build and Update Utility 用户指南》提供了有关使用 Systems Build and Update Utility 的信息。
- 1 《Dell 系统软件支持值表》提供了有关各种 Dell 系统、这些系统支持的操作系统以及可以安装在这些系统上的 Dell OpenManage 组件的信息。
- 1 《Dell OpenManage Server Administrator 用户指南》介绍了 Server Administrator 的安装和使用。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。
- 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。此指南说明了支持的各种管理对象类。
- 1 《Dell OpenManage Server Administrator 消息参考指南》列出了 Server Administrator 主页警报日志或操作系统事件查看器中显示的信息。该指南解释了 Server Administrator 发出的每个警报信息的内容、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 OpenManage IT Assistant 用户指南》提供有关安装、配置和使用 IT Assistant 的信息。IT Assistant 提供了一个中央访问点来监控和管理局域网 (LAN) 或广域网 (WAN) 上的系统。通过为管理员提供一个整个企业的综合视图, IT Assistant 可以增加系统运行时间、自动化重复任务并防止中断重要业务操作。
- 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 远程访问不能运行的系统的完整信息。
- 1 《Integrated Dell Remote Access Controller 用户指南》提供了有关配置和使用 Integrated Dell Remote Access Controller 来通过网络远程管理和监测系统及其共享资源的完整信息。
- 1 《Dell Update Packages 用户指南》提供了有关获取 Dell Update Package 和作为系统更新策略的一部分将 Dell Update Package 用于 Windows 和 Linux 的信息。
- 1 《Dell OpenManage Server Update Utility 用户指南》提供了有关使用 Dell OpenManage Server Update Utility 的信息。
- 1 软件套件 (DVD) 包含可以在介质上找到的应用程序的自述文件。

获得技术帮助

如果不明白本指南中说明的程序或者您的产品没有按照预期运行, 您可以随时寻求各种帮助。有关详情, 请参阅系统《硬件用户手册》中“获得帮助”一节。

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。并非在所有地区均提供此项服务。

[目录](#)

[目录](#)

使用 Microsoft Active Directory

安装指南

- [控制对网络的访问](#)
- [扩展 Active Directory 架构](#)

控制对网络的访问

如果使用 Active Directory® 服务软件，可以配置它以控制对网络的访问。Dell 修改了 Active Directory 数据库以支持远程管理身份验证和授权。Dell™ OpenManage™ IT Assistant、Dell OpenManage Server Administrator、Integrated Dell Remote Access Controller (iDRAC) 和 Dell Remote Access Controllers (DRAC) 现在能够与 Active Directory 交互。借助此工具，可以从一个中央数据库添加并控制用户和权限。

Active Directory 架构扩展

Active Directory 数据存放在一个“Attributes”（属性）和“Classes”（类）的分布式数据库中。一种 Active Directory “Class”（类）的示例为“User”（用户）类。一些用户类的示例“Attributes”（属性）可为用户的名、姓和电话号码等。添加到现有 Active Directory 架构中的每个属性或类都必须用一个唯一 ID 定义。要在整个业界中保证唯一 ID，Microsoft 维护着一个 Active Directory 对象标识符 (OID) 数据库。

Active Directory 架构定义了规定哪些数据可以包括在数据库中的规则。要扩展 Active Directory 中的架构，Dell 接收了目录服务中新属性和类的唯一 OID、唯一名称扩展名和唯一链接属性 ID。

Dell 扩展名是：dell

Dell 基础 OID 是：1.2.840.113556.1.8000.1280

Dell LinkID 范围是：12070 到 12079

Microsoft 维护的 Active Directory OID 数据库可以通过输入扩展 Dell，在 msdn.microsoft.com/certification/ADAcctInfo.asp 查看。

Active Directory 架构扩展概览

Dell 创建了类或对象组，可以由用户配置以满足特定需求。架构中的新类包括关联、产品和权限类。关联对象将用户或组链接到一组给定的权限以及网络中的系统（产品对象）。这种模式使管理员能够控制网络上用户、权限和系统的不同组合或 RAC 设备，而不增加复杂性。

Active Directory 对象概览

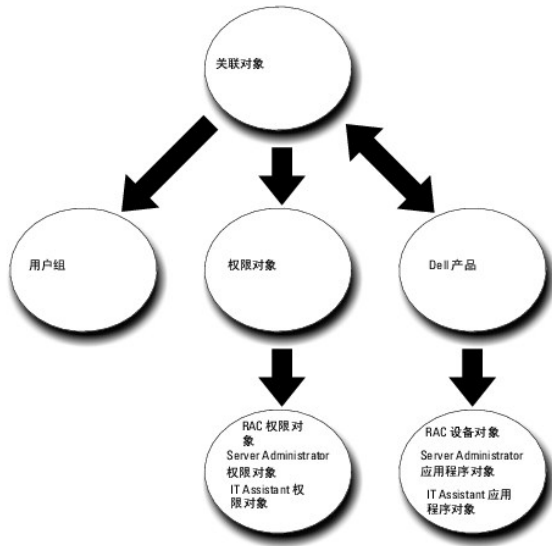
对于每个要与 Active Directory 集成以进行验证和授权的系统，至少必须有一个关联对象和一个产品对象。产品对象代表系统。关联对象将其与用户和权限相链接。您可以根据需要创建任意多个关联对象。

每个关联对象都可以根据需要链接到任意多个用户、用户组和产品对象。用户和产品对象可以来自任何域。不过，每个关联对象只能链接到一个权限对象。此行为使管理员能够控制哪些用户对于特定系统具有什么样的权限。

产品对象将系统链接到 Active Directory 以进行验证和授权查询。将系统添加到网络后，管理员必须使用 Active Directory 名称配置系统及其产品对象以便用户可以使用 Active Directory 执行验证和授权。管理员还必须将系统添加到至少一个关联对象以使用户能够验证。

[图 9-1](#) 说明关联对象提供了进行所有验证和授权所需的连接。

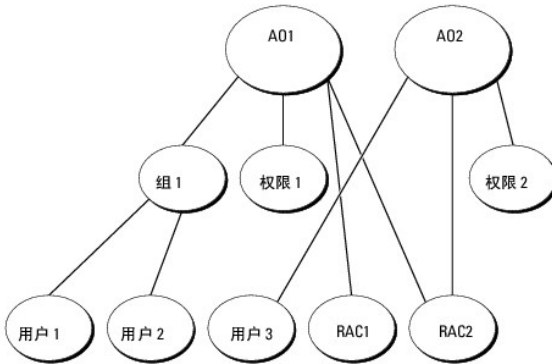
图 9-1. Active Directory 对象的典型设置



此外，可以在一个域或多个域中设置 Active Directory 对象。在一个域中设置对象并没有什么不同，无论是设置 RAC、Server Administrator，还是 IT Assistant 对象。不过，涉及到多个域时，就有些不同了。

例如，您有两个 DRAC 4 卡（RAC1 和 RAC2）以及三个现有 Active Directory 用户（用户 1、用户 2 和用户 3）。想给用户 1 和用户 2 对两个 DRAC 4 卡的管理员权限，而给用户 3 对 RAC2 卡的登录权限。[图 9-2](#) 显示了如何在此情况下设置 Active Directory 对象。

图 9-2. 在一个域中设置 Active Directory 对象



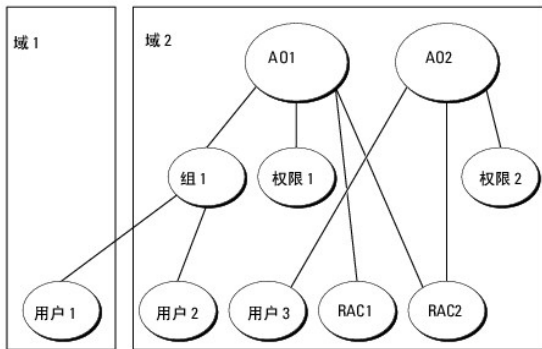
要为一个域的情况设置对象，应执行以下任务：

1. 创建两个关联对象。
2. 创建两个 RAC 产品对象（RAC1 和 RAC2）来表示这两个 DRAC 4 卡。
3. 创建两个权限对象（权限 1 和权限 2），其中权限 1 具有所有权限（管理员），而权限 2 具有登录权限。
4. 将用户 1 和用户 2 分組到组 1。
5. 将组 1 添加为关联对象 1 (A01) 中的成员，权限 1 作为 A01 中的权限对象，而 RAC1 和 RAC2 作为 A01 中的 RAC 产品。
6. 将用户 3 添加为关联对象 2 (A02) 中的成员，权限 2 作为 A02 中的权限对象，而 RAC2 作为 A02 中的 RAC 产品。

有关详细说明，请参阅[“将用户和权限添加到 Active Directory”](#)。

[图 9-3](#) 显示了如何在 RAC 的多个域中设置 Active Directory 对象。在这种情况下，您有两个 DRAC 4 卡（RAC1 和 RAC2）以及三个现有 Active Directory 用户（用户 1、用户 2 和用户 3）。用户 1 位于域 1，但用户 2 和用户 3 则位于域 2。想给用户 1 和用户 2 对 RAC1 和 RAC2 卡的管理员权限，而给用户 3 对 RAC2 卡的登录权限。

图 9-3. 在多个域中设置 RAC Active Directory 对象

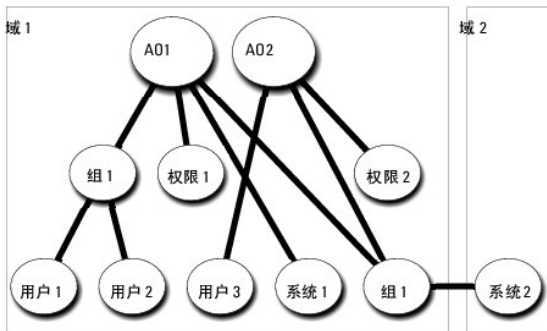


要为此多个域的情况设置对象，应执行以下任务：

1. 确保域目录林功能处在本机或 Windows 2003 模式。
2. 在任何域中创建两个关联对象 AO1（通用范围）和 AO2。此图显示了域 2 中的对象。
3. 创建两个 RAC 设备对象（RAC1 和 RAC2）来表示这两个远程系统。
4. 创建两个权限对象（权限 1 和权限 2），其中权限 1 具有所有权限（管理员），而权限 2 具有登录权限。
5. 将用户 1 和用户 2 分组到组 1。组 1 的组范围必须是通用。
6. 将组 1 添加为关联对象 1 (AO1) 中的成员，权限 1 作为 AO1 中的权限对象，而 RAC1 和 RAC2 作为 AO1 中的产品。
7. 将用户 3 添加为关联对象 2 (AO2) 中的成员，权限 2 作为 AO2 中的权限对象，而 RAC2 作为 AO2 中的产品。

对于 Server Administrator 或 IT Assistant，另一方面，一个关联中的用户可以位于不同的域中，而无需添加到通用组中。以下是一个非常相似的示例，显示不同域中的 Server Administrator 或 IT Assistant 系统如何影响目录对象的设置。除了 RAC 设备，将有两个运行 Server Administrator 的系统（Server Administrator 产品系统 1 和系统 2）。系统 1 和系统 2 位于不同的域中。可以使用 Active Directory 中任何现有用户或组。[图 9-4](#) 显示了如何为此示例设置 Server Administrator Active Directory 对象。

图 9-4. 在多个域中设置 Server Administrator Active Directory 对象



要为此多个域的情况设置对象，应执行以下任务：

1. 确保域目录林功能处在本机或 Windows 2003 模式。
2. 在任意域中创建两个关联对象（AO1 和 AO2）。此图显示了域 1 中的对象。
3. 创建两个 Server Administrator 产品（系统 1 和系统 2）来表示两个系统。系统 1 位于域 1 而系统 2 位于域 2 中。
4. 创建两个权限对象（权限 1 和权限 2），其中权限 1 具有所有权限（管理员），而权限 2 具有登录权限。
5. 将系统 2 分组到组 1。组 1 的组范围必须是通用。
6. 将用户 1 和用户 2 添加为关联对象 1 (AO1) 的成员，权限 1 作为 AO1 中的权限对象，而系统 1 和组 1 作为 AO1 中的产品。

7. 将用户 3 添加为关联对象 2 (AO2) 的成员, 权限 2 作为 AO2 中的权限对象, 而组 1 作为 AO2 中的产品。

请注意在此情况下每个关联对象都不需要是通用范围。

配置 Active Directory 访问系统

在使用 Active Directory 访问系统前, 必须配置好 Active Directory 软件和系统。

1. 扩展 Active Directory 架构 (请参阅[“扩展 Active Directory 架构”](#))。
2. 扩展 Active Directory 用户和计算机管理单元 (请参阅[“安装 Dell 对 Active Directory 用户和计算机管理单元的扩展”](#))。
3. 将系统用户及其权限添加到 Active Directory (请参阅[“将用户和权限添加到 Active Directory”](#))。
4. 仅对于 RAC 系统, 在每个域控制器上启用 SSL。
5. 使用基于 Web 的界面或 CLI 配置系统的 Active Directory 属性 (请参阅[“配置系统或设备”](#))。

配置 Active Directory 产品名称

要配置 Active Directory 产品名称:

1. 在安装目录中找到 `omsaoem.ini` 文件。
2. 编辑该文件以添加 `adproductname=text` (`adproductname=文本`) 行, 其中文本是在 Active Directory 中创建的产品对象的名称。例如, 如果 Active Directory 产品名称配置为 `omsaApp`, `omsaoem.ini` 文件将包含以下语法。

```
productname=Server Administrator

startmenu=Dell OpenManage Applications

autdbid=omsa

accessmask=3


adsupport=true

adproductname=omsaApp
```


3. 保存 `omsaoem.ini` 文件后, 重新启动 **DSM SA 连接服务**。

扩展 Active Directory 架构

可以使用 RAC、Server Administrator 和 IT Assistant 架构扩展。只需为要使用的软件或硬件扩展架构。必须单独应用每个扩展以得到其软件特定设置的好处。扩展 Active Directory 架构将会为架构添加架构类和属性、示例权限和关联对象, 以及 Dell 组织单元。

 **注:** 扩展架构前, 必须在域目录林的架构主灵活单主机操作 (FSMO) 角色物主上拥有“Schema Admin” (架构管理员) 权限。

可以用两种不同方法扩展架构。可以使用 Dell Schema Extender 公用程序, 或者可使用轻型目录交换格式 (LDIF) 脚本文件。

 **注:** 如果使用 LDIF 脚本文件, 将不会添加 Dell 组织单元。

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

- 1 <DVD 驱动器>:\SYSTEMGMT\ManagementStation\support\OMActiveDirectory_Tools\
<安装类型>\LDIF 文件
- 1 <DVD 驱动器>:\SYSTEMGMT\ManagementStation\support\OMActiveDirectory_Tools\
<安装类型>\Schema Extender

[表 9-1](#) 列出文件夹名称和 <安装类型>。

表 9-1. 文件夹名称和 安装类型

文件夹名称	安装类型
-------	------

ITA7	IT Assistant 7.0 或更高版本
OMSA	Dell OpenManage Server Administrator
Remote_Management	xxOx 模块化系统上的 RAC 4、RAC 5、CMC 和 iDRAC
Remote_Management_Advanced	xx1x 系统上的 iDRAC 注： xx1x 系统仅支持 iDRAC6。

要使用 LDIF 文件，请参阅 LDIF 文件目录中自述文件的说明。要使用 Dell Schema Extender 扩展 Active Directory 架构，应执行“[使用 Dell Schema Extender](#)”中的步骤。

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

使用 Dell Schema Extender

 **小心：** Dell Schema Extender 使用 SchemaExtenderOem.ini 文件。要确保 Dell Schema Extender 公用程序运作正常，请勿修改此文件的名称或内容。

1. 单击“Welcome”（欢迎）屏幕上的“Next”（下一步）。
2. 阅读警告并再次单击“Next”（下一步）。
3. 既可以选择“Use Current Log In Credentials”（使用当前登录凭据）也可以输入具有架构管理员权限的用户名和密码。
4. 单击“Next”（下一步）运行 Dell Schema Extender。
5. 单击“Finish”（完成）。

要验证架构扩展，请使用 Microsoft Management Console (MMC) 中的 Active Directory 架构管理单元验证是否存在以下类（列于[表 9-2](#)、[表 9-5](#)、[表 9-7](#)、[表 9-8](#)、[表 9-9](#)和[表 9-10](#)）和属性（列于[表 9-11](#)和[表 9-12](#)）。请参阅 Microsoft 说明文件详细了解如何启用和使用 Active Directory 架构。MMC 中的管理单元。

有关 DRAC 的类定义的详情，请参阅《Dell Remote Access Controller 4 用户指南》和《Dell Remote Access Controller 5 用户指南》。

有关 iDRAC 的类定义的详情，请参阅《Integrated Dell Remote Access Controller 用户指南》。

表 9-2. 添加到 Active Directory 类的类定义架构

类名称	分配的对象标识号 (OID)	类的类型
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2	结构类
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4	结构类
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5	结构类
dellOmsa2AuxClass	1.2.840.113556.1.8000.1280.1.2.1.1	辅助类
dellOmsaApplication	1.2.840.113556.1.8000.1280.1.2.1.2	结构类
dellIta7AuxClass	1.2.840.113556.1.8000.1280.1.3.1.1	辅助类
dellItaApplication	1.2.840.113556.1.8000.1280.1.3.1.2	结构类

表 9-3. dellAssociationObject 类

OID	1.2.840.113556.1.8000.1280.1.1.1.2
说明	这种类表示 Dell 关联对象。关联对象提供了用户和设备或产品之间的连接。
类的类型	结构类
超类	组
属性	dellProductMembers dellPrivilegeMember

表 9-4. dellPrivileges 类

OID	1.2.840.113556.1.8000.1280.1.1.1.4
说明	这种类用作 Dell 权限（授权权限）的容器类。
类的类型	结构类
超类	用户
属性	dellIRAC4Privileges

dellRAC3Privileges
dellOmsaAuxClass
dellItaAuxClass

表 9-5. dellProduct 类

OID	1.2.840.113556.1.8000.1280.1.1.1.5
说明	这是所有 Dell 产品所派生的主类。
类的类型	结构类
超类	计算机
属性	dellAssociationMembers

表 9-6. dellOmsa2AuxClass 类

OID	1.2.840.113556.1.8000.1280.1.2.1.1
说明	这种类用于为 Server Administrator 定义权限（授权权限）。
类的类型	辅助类
超类	无
属性	dellOmsaIsReadOnlyUser dellOmsaIsReadWriteUser dellOmsaIsAdminUser

表 9-7. dellOmsaApplication 类

OID	1.2.840.113556.1.8000.1280.1.2.1.2
说明	这种类代表 Server Administrator 应用程序。Server Administrator 必须在 Active Directory 中配置为 dellOmsaApplication。此配置启用 Server Administrator 应用程序将 LDAP 查询发送到 Active Directory。
类的类型	结构类
超类	dellProduct
属性	dellAssociationMembers

表 9-8. dellIta7AuxClass 类

OID	1.2.840.113556.1.8000.1280.1.3.1.1
说明	这种类用于为 IT Assistant 定义权限（授权权限）。
类的类型	辅助类
超类	无
属性	dellItaIsReadOnlyUser dellItaIsReadWriteUser dellItaIsAdminUser

表 9-9. dellItaApplication 类

OID	1.2.840.113556.1.8000.1280.1.3.1.2
说明	这种类代表 IT Assistant 应用程序。IT Assistant 必须在 Active Directory 中配置为 dellItaApplication。此配置启用 IT Assistant 将 LDAP 查询发送到 Active Directory。
类的类型	结构类
超类	dellProduct
属性	dellAssociationMembers

表 9-10. 添加到 Active Directory 架构中的常规属性

属性名称/说明	分配的 OID/语法对象标识符	单值
dellPrivilegeMember 属于此属性的 dellPrivilege 对象的列表。	1.2.840.113556.1.8000.1280.1.1.2.1 可分辨名称 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers 属于此角色的 dellRacDevices 对象的列表。此属性是指向 dellAssociationMembers 后退链接的前进链	1.2.840.113556.1.8000.1280.1.1.2.2 可分辨名称 (LDAPTYPE_DN	FALSE

接。	1.3.6.1.4.1.1466.115.121.1.12)	
链接 ID: 12070		
dellAssociationMembers	1.2.840.113556.1.8000.1280.1.1.2.14	FALSE
属于此产品的 dellAssociationObjectMembers 的列表。此属性是到 dellProductMembers 链接属性的后退链接。	可分辨名称 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
链接 ID: 12071		

表 9-11. 添加到 Active Directory 架构的 Server Administrator 特定属性 Directory Schema 的类定义

属性名称/说明	分配的 OID/语法对象标识符	单值
dellOMSAIsReadOnlyUser	1.2.840.113556.1.8000.1280.1.2.2.1	TRUE
如果用户在 Server Administrator 中具有只读权限，则为 TRUE	布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellOMSAIsReadWriteUser	1.2.840.113556.1.8000.1280.1.2.2.2	TRUE
如果用户在 Server Administrator 中具有读写权限，则为 TRUE	布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellOMSAIsAdminUser	1.2.840.113556.1.8000.1280.1.2.2.3	TRUE
如果用户在 Server Administrator 中具有管理员权限，则为 TRUE	布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	

表 9-12. 添加到 Active Directory 架构的 IT Assistant 特有属性 Directory Schema 的类定义

属性名称/说明	分配的 OID/语法对象标识符	单值
dellItaIsReadWriteUser	1.2.840.113556.1.8000.1280.1.3.2.1	TRUE
如果用户在 IT Assistant 中具有读写权限，则为 TRUE	布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellItaIsAdminUser	1.2.840.113556.1.8000.1280.1.3.2.2	TRUE
如果用户在 IT Assistant 中具有管理员权限，则为 TRUE	布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellItaIsReadOnlyUser	1.2.840.113556.1.8000.1280.1.3.2.3	TRUE
如果用户在 IT Assistant 中具有只读权限，则为 TRUE	布尔值 (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	

Active Directory 用户和计算机管理单元

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

在 Active Directory 中扩展架构时，也必须扩展 Active Directory 用户和计算机管理单元以便管理员可以管理产品、用户和用户组、关联和权限。只需扩展一次管理单元，即使已经添加了一个以上的架构扩展。必须在每个准备用于管理这些对象的系统上安装管理单元。

使用 *Dell Systems Management Tools and Documentation DVD* 安装系统管理软件时，可以通过在安装过程中选择“Active Directory Snap-in”（Active Directory 管理单元）选项安装该管理单元。

对于 64 位 Windows 操作系统，管理单元安装程序位于 <DVD 驱动器>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64。

注： 必须在管理新 Active Directory 对象的每个管理站上都安装 Administrator Pack。下一节“[打开 Active Directory 用户和计算机管理单元](#)”介绍了安装过程。如果不安装 Administrator Pack，则无法查看容器中的新对象。

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

打开 Active Directory 用户和计算机管理单元

注： 在 Windows 2000 Server 上，可以扩展架构，但无法将 Dell 扩展安装到管理单元。

为了在运行 Windows 2000 的域控制器上管理扩展架构，请执行以下步骤：

从另一个域控制器连接到 Windows 2000 Server 域控制器

1. 单击“Start”（开始）→“Admin Tools”（管理工具）→“Active Directory Users and Computers”（Active Directory 用户和计算机）。

2. 在左窗格中，右键单击“Active Directory Users and Computers”（Active Directory 用户和计算机）。
3. 单击“Connect to Domain Controller”（连接到域控制器）以连接到另一个域控制器。
4. 输入 Windows 2000 域控制器的名称。

从本地系统连接到 Windows 2000 Server 域控制器

1. 本地系统上必须安装有合适的 Microsoft Administrator Pack。
2. 要安装此 Administrator Pack，请单击“Start”（开始）→“Run”（运行），键入 MMC 并按 <Enter>。
将显示 Microsoft Management Console (MMC) 窗口。
3. 单击“File”（文件）。
4. 单击“Add/Remove Snap-in”（添加/删除管理单元）。
5. 单击“Add”（添加）。
6. 选择“Active Directory Users and Computers”（Active Directory 用户和计算机）管理单元并单击“Add”（添加）。
7. 单击“Close”（关闭）并单击“OK”（确定）。

此时将连接到当前域控制器。如果此域控制器不是 Windows 2000 域控制器，则继续执行[从另一个域控制器连接到 Windows 2000 Server 域控制器](#)下描述的步骤。



要打开 Active Directory 用户和计算机管理单元，应执行以下步骤：

1. 如果在域控制器上，则单击“Start”（开始）→“Admin Tools”（管理工具）→“Active Directory Users and Computers”（Active Directory 用户和计算机）。如果不在域控制器上，必须在本地系统上安装相应的 Microsoft Administrator Pack。要安装此 Administrator Pack，请单击“Start”（开始）→“Run”（运行），键入 MMC 并按 Enter。
这会打开 Microsoft Management Console (MMC) 窗口。
2. 单击“Console 1”（控制台 1）窗口中的“File”（文件）。
3. 单击“Add/Remove Snap-in”（添加/删除管理单元）。
4. 单击“Add”（添加）。
5. 选择“Active Directory Users and Computers”（Active Directory 用户和计算机）管理单元并单击“Add”（添加）。
6. 单击“Close”（关闭）并单击“OK”（确定）。

将用户和权限添加到 Active Directory

Dell 扩展的 Active Directory 用户和计算机管理单元使您能够通过创建 RAC、关联和权限对象来添加 DRAC、Server Administrator 和 IT Assistant 用户和权限。要添加对象，请执行相应小节中的步骤。

创建产品对象

-  **注：** Server Administrator 和 IT Assistant 用户必须使用通用类型产品组用其产品对象来跨越域。
-  **注：** 当添加来自不同域的通用类型产品组时，需要用通用范围创建一个关联对象。由 Dell Schema Extender 公用程序创建的默认关联对象为域本地组，并且不能与来自其它域的通用类型产品组一起使用。

在“Console Root”（控制台根节点）(MMC) 窗口中，右击一个容器。

1. 选择“New”（新建）。
2. 根据安装情况，选择 RAC、Server Administrator 或 IT Assistant 对象。

系统将显示“New Object”（新建对象）窗口。

3. 键入新对象的名称。此名称必须与“[在运行 Server Administrator 的系统上使用 CLI 配置 Active Directory](#)”中讨论的 Active Directory 产品名称匹配。
4. 选择相应的“Product Object”（产品对象）。
5. 单击“OK”（确定）。

创建权限对象

权限对象必须创建在与其关联的关联对象的相同域中。

1. 在“Console Root”（控制台根目录）(MMC) 窗口中，右键单击一个容器。
2. 选择“New”（新建）。
3. 根据安装情况，选择 RAC、Server Administrator 或 IT Assistant 对象。

系统将显示“New Object”（新建对象）窗口。

4. 键入新对象的名称。
5. 选择相应的“Privilege Object”（权限对象）。
6. 单击“OK”（确定）。
7. 右击创建的权限对象并选择“Properties”（属性）。
8. 单击相应的“Privileges”（权限）选项卡并选择希望用户具有的权限（有关详情请参阅[表 9-2](#)和[表 9-8](#)）。

创建关联对象

关联对象从组派生而来，必须包含组类型。关联范围为关联对象指定安全组类型。创建关联对象时，必须选择适用于要添加的对象类型的关联范围。例如，选择“Universal”（通用）表示关联对象只有在 Active Directory 域以本机或更高模式运行时才可用。


1. 在“Console Root”（控制台根节点）(MMC) 窗口中，右击一个容器。
2. 选择“New”（新建）。
3. 根据安装情况，选择 RAC、Server Administrator 或 IT Assistant 对象。

系统将显示“New Object”（新建对象）窗口。

4. 键入新对象的名称。
5. 选择“Association Object”（关联对象）。
6. 选择“Association Object”（关联对象）的范围。
7. 单击“OK”（确定）。

将对象添加到关联对象

通过使用“Association Object Properties”（关联对象属性）窗口，可以关联用户或用户组、权限对象、系统、RAC 设备以及系统或设备组。


 **注：** RAC 用户必须使用通用组用其用户或 RAC 对象跨越域。

可以添加用户组和产品组。可以采用与创建其它组相同的方法创建与 Dell 相关的组。

要添加用户或用户组：

1. 右键单击"Association Object" (关联对象) 并选择"Properties" (属性)。
2. 选择"Users" (用户) 选项卡并单击"Add" (添加)。
3. 键入用户或用户组名称或浏览选择一个并单击"OK" (确定)。


单击"Privilege Object" (权限对象) 选项卡将权限对象添加到验证系统时定义用户或用户组权限的关联。

 **注：** 只能将一个权限对象添加到关联对象。

要添加权限：

1. 选择"Privileges Object" (权限对象) 选项卡并单击"Add" (添加)。
2. 键入权限对象名称或浏览选择一个并单击"OK" (确定)。

单击"Products" (产品) 选项卡将一个或多个系统或设备添加到关联。关联的对象指定连接到网络的已定义用户或用户组可用的产品。


 **注：** 可以将多个系统或 RAC 设备添加到关联对象。

要添加产品：

1. 选择"Products" (产品) 选项卡并单击"Add" (添加)。
2. 键入系统、设备或组名称并单击"OK" (确定)。
3. 在"Properties" (属性) 窗口中，单击"Apply" (应用)，然后单击"OK" (确定)。


配置系统或设备


有关如何使用 CLI 命令配置 Server Administrator 或 IT Assistant 系统的说明，请参阅[“在运行 Server Administrator 的系统上使用 CLI 配置 Active Directory”](#)。对于 DRAC 用户，请参阅《Dell Remote Access Controller 4 用户指南》或《Dell Remote Access Controller 5 用户指南》。对于 iDRAC 用户，请参阅《Integrated Dell Remote Access Controller 用户指南》。

 **注：** 装有 Server Administrator 和/或 IT Assistant 的系统必须是 Active Directory 域的一部分并且在该域中还应具有计算机帐户。

在运行 Server Administrator 的系统上使用 CLI 配置 Active Directory

可以使用 `omconfig preferences dirservice` 命令配置 Active Directory 服务。`产品 oem.ini` 文件会修改以反映这些更改。如果 `adproductname` 没有出现在 `产品 oem.ini` 文件中，则会分配一个默认名称。默认值是 `系统名称-软件-产品名称`，其中 `系统名称` 是运行 Server Administrator 的系统的名称，而 `软件-产品名称` 是指 `omprv32.ini` (即，`计算机名称-omsa`) 中定义的软件产品的名称。

 **注：** 此命令只能适用于运行 Windows 操作系统的系统。

 **注：** 配置完 Active Directory 后重新启动 Server Administrator 服务。

[表 9-13](#) 显示该命令的有效参数。

表 9-13. Active Directory 服务配置参数

名称=值对	说明
<code>prodname=<文本></code>	指定要应用 Active Directory 配置更改的软件产品。 <code>Prodname</code> 是指在 <code>omprv32.ini</code> 中定义的产品名称。对于 Server Administrator，为 <code>omsa</code> 。
<code>enable=<true false></code>	true: 启用 Active Directory 服务验证支持。 false: 禁用 Active Directory 服务验证支持。
<code>adprodname=<文本></code>	指定 Active Directory 服务中定义的产品名称。此名称将产品与用于用户鉴别的 Active Directory 权限数据相链接。

[目录](#)

前提条件检查程序

安装指南

● [前提条件检查程序的命令行操作](#)

前提条件检查程序的命令行操作

可以通过从 *Dell Systems Management Tools and Documentation DVD* 上的 `SYSMGMT\svadmin\windows\PreReqChecker` 目录中执行 `runprereqchecks.exe /s`，无提示运行前提条件检查。运行前提条件检查后，将在 `%Temp%` 目录中创建一个 HTML 文件 (`omprereq.htm`)。此文件包含前提条件检查结果。`Temp` 目录通常不是 `X:\Temp`，而是 `X:\Documents and Settings\Username\Local Settings\Temp`。要查找 `%TEMP%`，转至命令行提示符并键入 `echo %TEMP%`。

对于受管系统，这些结果写在以下密钥之下：

`HKEY_LOCAL_MACHINE\Software\Dell Computer Corporation\OpenManage\PreReqChecks\MN\`

无提示运行前提条件检查时，来自 `runprereqchecks.exe` 的返回代码是与所有软件产品最高严重性情况相关的数字。返回代码数字与注册表中使用的相同。[表 10-1](#) 返回代码的详细信息。

表 10-1. 无提示运行前提条件检查时返回的代码

返回代码	说明
0	没有条件与软件相关。
1	一个（或多个）通知条件与软件相关。它不阻止安装软件产品。
2	一个（或多个）警告条件与软件相关。建议先解决引起警告的情况，然后再继续安装软件
3	一个（或多个）错误条件与软件相关。需要先解决引起错误的情况，然后才可继续安装该软件。如果不解决这些问题，将不会安装软件。
-1	Microsoft® Windows® Script Host (WSH) 错误。前提条件检查程序将不会运行。
-2	操作系统不受支持。前提条件检查程序将不会运行。
-3	用户不具有管理员权限。前提条件检查程序将不会运行。
-4	不是一个实现的返回代码。
-5	用户未能将工作目录更改为 <code>%TEMP%</code> 。前提条件检查程序将不会运行。
-6	目标目录不存在。前提条件检查程序将不会运行。
-7	出现内部错误。前提条件检查程序将不会运行。
-8	软件已在运行。前提条件检查程序将不会运行。
-9	Windows Script Host 损坏、版本错误或未安装。前提条件检查程序将不会运行。
-10	脚本环境出现错误。前提条件检查程序将不会运行。

运行完前提条件检查后，各个软件产品都设置了相关值。[表 10-2](#) 提供每种软件功能的功能 ID 的列表。功能 ID 是 2 至 5 个字符的指定值。


 **注：** [表 10-2](#) 中所述的软件功能 ID 区分大小写。

表 10-2. Managed Systems Software 的软件功能 ID

功能 ID	说明
ALL	所有功能
BRCM	Broadcom NIC 代理
INTEL	Intel® NIC 代理
IWS	Dell OpenManage Server Administrator Web Server
OMSM	Server Administrator Storage Management Service
RAC4	Remote Access Controller (DRAC 4)
RAC5	Dell 远程访问控制器 (DRAC) 5
iDRAC	Integrated Dell Remote Access Controller
SA	Server Administrator
RmtMgmt	Remote Enablement

OpenManage Linux 安装程序软件包 安装指南

本附录列出了 OpenManage Linux 安装程序软件包。

表 A-1. 元 RPM

RPM	说明	相关软件包	以下项需要	OM 6.1	OM 6.2	OM 6.3
srvadmin-all	用于安装所有 Server Administrator 功能的元软件包	所有元 RPM	Server Administrator 完整功能	是	是	是
srvadmin-base	用于安装 Server Agent 的元软件包	srvadmin-omacore srvadmin-smcommon srvadmin-cm	Server Instrumentation、SNMP 监控和 Server Administrator CLI	是	是	是
srvadmin-standardAgent	用于安装 Standard Server Agent 的元软件包	srvadmin-itunnelprovider srvadmin-cm srvadmin-smcommon	实现使用 Server Administrator Web Server 进行远程管理	是	是	是
srvadmin-webserver	用于安装 Server Administrator Web Server 功能的元软件包	srvadmin-iws srvadmin-smcommon srvadmin-smweb	用于本地和远程节点管理的 Server Administrator Web Server	是	是	是
srvadmin-storageservices	用于安装 Server Administrator Storage Services 功能的元软件包	srvadmin-storage srvadmin-smcommon srvadmin-cm srvadmin-megalib (仅适用于 32 位安装) srvadmin-fsa (在 6.3 中已删除) srvadmin-storelib srvadmin-storage-populator srvadmin-sysfsutils	使用 Server Administrator GUI/CLI 进行存储设备管理	是	是	是
srvadmin-rac4	RAC4 组件的元 RPM	srvadmin-omilcore srvadmin-racadm4 srvadmin-racdrsc4 srvadmin-racsvc srvadmin-rac4-populator* srvadmin-rac-components* srvadmin-racdrsc* * - 6.3 软件包	使用 Server Administrator GUI/CLI、RAC4 工具进行的 RAC 4 管理	是	是	是
srvadmin-rac5	RAC5 组件的元 RPM	srvadmin-omilcore srvadmin-racdrsc5 srvadmin-racadm5 srvadmin-racdrsc* srvadmin-rac-components* * - 6.3 软件包	使用 Server Administrator GUI/CLI、RAC5 工具进行的 RAC 5 管理	是	是	是
srvadmin-idrac	IDRAC 组件的元 RPM	srvadmin-omilcore srvadmin-idracdrsc srvadmin-idracadm srvadmin-racdrsc* srvadmin-rac-components* srvadmin-argtable2* * - 6.3 软件包	使用 Server Administrator GUI/CLI、IDRAC 工具进行的 IDRAC 管理	是	是	是

表 A-2. Server Instrumentation 和 SNMP 监控

RPM	说明	OM 相关软件包	以下项需要	OM 6.1	OM 6.2	OM 6.3
srvadmin-omilcore	为系统管理安装软件包提供工具的核心安装软件包	smbios-utils-bin libsmbios	Server Administrator 的安装和运行	是	是	是
srvadmin-syscheck	用于检查系统 ID 并验证 OpenManage 支持的软件包	无	无	是	陈旧	陈旧
srvadmin-deng	Data Engine 存储和管理系统管理的对象	srvadmin-omilcore	Server Instrumentation 和 SNMP 监控	是	是	是
srvadmin-hapi	为系统管理提供底层硬件接口	无	Server Instrumentation	是	是	是
srvadmin-isvc	为本地和远程系统管理提供系统管理接口	srvadmin-omilcore srvadmin-deng srvadmin-hapi	Server Instrumentation 和 SNMP 监控	是	是	是
srvadmin-ipmi	-	-	-	陈旧	陈旧	陈旧
libsmbios	提供 SMBIOS 库用来获取标准 BIOS 表	无	使用 ITA 进行安装和软件更新	否	是	是
smbios-utils-bin	提供 SMBIOS 公用程序以获取系统信息	无	安装	否	是	是

表 A-3. GUI 和 CLI 组件使用的本地管理所需的软件包

RPM	说明	OM 相关软件包	以下项需要	OM 6.1	OM 6.2	OM 6.3
srvadmin-omcommon	GUI/CLI 的通用框架/库	srvadmin-omilcore	服务器管理器 GUI/CLI	是	是	是
srvadmin-omacore	提供充当后端和 GUI/CLI 之间接口的插件。还提供 OM CLI 工具。	srvadmin-omilcore srvadmin-deng srvadmin-omcommon srvadmin-xmlsup libsmbios	服务器管理器 GUI/CLI 和基础设施，用于通过 ITA 进行软件更新	是	是	是
srvadmin-omhip	为工具提供数据访问器	无	服务器管理器 GUI/CLI	是	陈旧。与 srvadmin-omacore 合并	陈旧
srvadmin-xmlsup	XML 支持库	srvadmin-libxslt (仅限于 VmWare ESX) libxslt (由操作系统供应商在其它 Linux 版本上提供)	服务器管理器 GUI/CLI	否	是	是
srvadmin-libxslt	XSLT 支持库 * 仅在 VmWare ESX 上适用	无	服务器管理器 GUI/CLI	否	是	是
srvadmin-cm	更改管理资源注册收集程序。向 ITA 等 Management Station 应用程序提供软件资源注册数据	srvadmin-omacore	使用 ITA 进行软件资源注册和更新			

表 A-4. 用于本地和远程管理的 Server Administrator Web Server (GUI)

RPM	说明	相关软件包	以下项需要	OM 6.1	OM 6.2	OM 6.3
srvadmin-jre	为 Web Server 提供 JAVA 运行时	srvadmin-omilcore	Server Administrator GUI	是	是	是
srvadmin-iws	Server Administrator Web Server 和 GUI 软件包	srvadmin-omilcore srvadmin-omcommon srvadmin-jre openwsman-client libwsman1	Server Administrator GUI	是	是	是
srvadmin-omauth	为 GUI 提供验证文件	无	Server Administrator GUI	是	陈旧。与 srvadmin-iws 合并	陈旧
openwsman-client	Openwsman 客户端库	无	Server Administrator GUI，用于通过 WSMAN 管理远程节点	是	是	是
libwsman1	客户端和服务组件使用的 Openwsman 库	无	Openwsman 支持库	是	是	是

表 A-5. Server Administrator Remote Enablement (标准代理)

RPM	说明	OM 相关软件包	以下项需要	OM 6.1	OM 6.2	OM 6.3
srvadmin-wsmanclient	实现远程系统管理的 WSMAN 客户端软件包	无	无	是	陈旧。由 openwsman-client 和 libwsman1 软件包取代	陈旧
srvadmin-ssa	实现从安装 Server Administrator Web Server 的远程系统通过 WS-Man 界面管理系统。	无	无	是	陈旧	陈旧
srvadmin-itunnelprovider	实现服务器远程管理的 OpenManage SFCB 提供程序	sblim-sfcb >= 1.3.2 sblim-sfcc >= 2.1.0 openwsman-client >= 2.1.5 openwsman-server >= 2.1.5 libwsman1 >= 2.1.5 libcmpiCpplmp10 >= 2.0.0	实现服务器远程管理	否	是	是
libwsman1	客户端和服务组件使用的 Openwsman 库	无	Openwsman 支持库	是	是	是
openwsman-server	Openwsman 服务器和服务库 * 在 VmWare ESX 上不适用	无	实现服务器远程管理	是	是	是
sblim-sfcb	轻量级 CIM 后台程序 (sfcb) - 符合 CIM Operations over HTTP 协议的 CIM 服务器。 * 在 VmWare ESX 上不适用	无	实现服务器远程管理	是	是	是
sblim-sfcc	轻量级 CIM 客户端库 (sfcc) 运行时库	无	实现服务器远程管理	是	是	是

	*在 VmWare ESX 上不适用					
libcmplCpplImpl0	提供助手库以便将 CMPI C++ 插件实施到 SFCB 中 *在 VmWare ESX 上不适用	无	实现服务器远程管理	否	是	是
mod_wsman	一个实现 WSMAN 接口的 Apache 模块	无	无	是	陈旧	陈旧

表 A-6. Storage Instrumentation、SNMP 监控、GUI 和 CLI 插件

RPM	说明	OM 相关软件包	以下项需要	OM 6.1	OM 6.2	OM 6.3
srvadmin-storage	用于存储设备管理的核心接口库	srvadmin-omilcore srvadmin-deng srvadmin-isvc srvadmin-omcommon srvadmin-xmlsup	Storage Instrumentation、SNMP 监控和 CLI (用于存储设备管理)	是	是	是
srvadmin-storage-populator	低层库，用于发现和监控存储设备	srvadmin-omilcore srvadmin-deng srvadmin-isvc srvadmin-storage	Storage Instrumentation	否	是	是
srvadmin-storelib	用于存储设备管理的 LSI 公用程序库	srvadmin-storelib-sysfs	Storage Instrumentation	否	是	是
srvadmin-storelib-libpci	内核的 PCI 公用程序。由 storelib 库使用	无	Storage Instrumentation	否	是	陈旧
srvadmin-storelib-sysfs	提供库，以便与内核的 sys 文件系统连接。由 LSI storelib 库使用 *对 VmWare ESX 不适用	无	Storage Instrumentation	否	是	是
srvadmin-sysfsutils	提供公用程序，以便与 sysfs 文件系统连接。由 OM Storage Management 库使用	无	Storage Instrumentation	否	是	是
srvadmin-megalib	用于 PERC 4 控制器的存储设备管理的 LSI 公用程序库 *对 64 位 OMSA 安装以及 VmWare ESX 不适用。	无	PERC 4 控制器的 Storage Instrumentation	否	是	是
sradmin-fsa	Adaptec 公用程序库，用于管理 Adaptec 控制器	无	Storage Instrumentation	否	是	陈旧
srvadmin-smcommon	GUI/CLI 的通用框架/库 (用于存储设备管理)	无	使用 Server Administrator GUI/CLI 进行存储设备管理	否	是	是
srvadmin-smweb	用于存储设备管理的 GUI 插件	srvadmin-omcommon	使用 Server Administrator GUI 进行存储设备管理	否	是	是

表 A-7. RAC Instrumentation、SNMP 监控、GUI 和 CLI 插件

RPM	说明	OM 相关软件包	以下项需要	OM 6.1	OM 6.2	OM 6.3
srvadmin-racsvc	RAC 服务，用于管理 DRAC 4	srvadmin-omilcore	DRAC 4 Instrumentation	是	是	是
srvadmin-rac4-components	DRAC 4 的 RAC Data Populator	srvadmin-omilcore srvadmin-hapi srvadmin-deng srvadmin-racsvc	DRAC 4 Instrumentation 和 SNMP 监控	是	是	陈旧。合并到 srvadmin-rac-components
srvadmin-racadm4	提供用于 DRAC 4 管理的 CLI 工具	srvadmin-omilcore	DRAC 4 的 RAC CLI 工具	是	是	是
srvadmin-racdrsc4	DRAC 4 的 Server Administrator 的 RAC CLI 和 Web 插件	srvadmin-omilcore srvadmin-deng srvadmin-omcommon srvadmin-omacore srvadmin-rac4-components	使用 Server Administrator GUI/CLI 进行 DRAC 4 管理	是	是	陈旧。合并到 srvadmin-racdrsc
srvadmin-rac5-components	DRAC 5 的 RAC Data Populator	srvadmin-omilcore srvadmin-hapi srvadmin-deng	DRAC 5 Instrumentation 和 SNMP 监控	是	是	陈旧。合并到 srvadmin-rac-components

srvadmin-racadm5	提供用于 DRAC 5 管理的 CLI 工具	srvadmin-omilcore srvadmin-hapi	DRAC 5 的 RAC CLI 工具	是	是	是
srvadmin-racdrsc5	DRAC 5 的 Server Administrator 的 RAC CLI 和 Web 插件	srvadmin-omilcore srvadmin-deng srvadmin-omcommon srvadmin-omacore srvadmin-rac5-components	使用 Server Administrator GUI/CLI 进行 DRAC 5 管理	是	是	陈旧。合并到 srvadmin-racdrsc
srvadmin-idrac-components	iDRAC 的 RAC Data Populator	srvadmin-omilcore srvadmin-hapi srvadmin-deng	iDRAC Instrumentation 和 SNMP 监控	是	是	陈旧。合并到 srvadmin-rac-components
srvadmin-idracadm	提供用于 iDRAC 管理的 CLI 工具	srvadmin-omilcore srvadmin-hapi	iDRAC 的 RAC CLI 工具	是	是	是
srvadmin-idracdrsc	iDRAC 的 Server Administrator 的 RAC CLI 和 Web 插件	srvadmin-omilcore srvadmin-deng srvadmin-omcommon srvadmin-omacore srvadmin-idrac-components	使用 Server Administrator GUI/CLI 进行 iDRAC 管理	是	是	陈旧。合并到 srvadmin-racdrsc
srvadmin-racdrsc	RAC 4、5 和 iDRAC 的 Server Administrator 的 RAC CLI 和 Web 插件	srvadmin-deng srvadmin-omcommon	使用 Server Administrator GUI/CLI 进行 RAC 管理	否	否	是
srvadmin-rac-components	RAC 4、5 和 iDRAC 的 RAC SNMP 组件	srvadmin-deng	RAC Instrumentation 和 SNMP 监控	否	否	是
srvadmin-rac4-populator-	DRAC 4 的 RAC Data Populator	srvadmin-hapi srvadmin-deng srvadmin-racadm4	DRAC 4 Instrumentation	否	否	是
srvadmin-argtable2	用于分析 GNU 式命令行参数的库。由 RAC 5 和 iDRAC 软件包使用	srvadmin-racadm5 srvadmin-idracadm5	用于 RAC 5 和 iDRAC 管理的 RAC CLI 工具	否	否	是
srvadmin-idrac-ivmcli	提供 CLI 工具，从而从 Management Station 向远程模块化系统中的 iDRAC 提供虚拟介质功能	无	RAC CLI 工具，用于提供虚拟介质功能	否	否	是
srvadmin-idrac-vmcli	提供 CLI 工具，从而从 Management Station 向远程非模块化系统中的 iDRAC 提供虚拟介质功能	无	RAC CLI 工具，用于提供虚拟介质功能	否	否	是

表 A-8. 实现使用 IT Assistant 进行软件资源注册和更新

RPM	说明	OM 相关软件包	以下项需要	OM 6.1	OM 6.2	OM 6.3
srvadmin-cm	更改管理资源注册收集程序。向 ITA 等 Management Station 应用程序提供软件资源清单数据	srvadmin-omacore	使用 ITA 进行软件资源注册和更新	是	是	是

[目录](#)

Dell OpenManage 安全保护


安装指南

- [安全功能](#)
- [安全管理](#)


安全功能

Dell™ OpenManage™ System Management Software 组件提供了以下安全功能：

- 1 通过硬件中存储的用户 ID 和密码或者通过使用可选的 Microsoft® Active Directory® 来验证用户身份。
- 1 对于 Linux 操作系统，支持网络信息服务 (NIS)、Winbind、Kerberos 和轻型目录访问协议 (LDAP) 验证协议。
- 1 基于角色的授权，允许为每个用户配置具体权限。
- 1 在多数情况下，通过基于 Web 的界面或命令行界面 (CLI) 配置用户 ID 和密码。
- 1 128 位和 40 位（用于不接受 128 位的国家/地区）SSL 加密技术。

 **注：** Telnet 不支持 SSL 加密技术。

- 1 通过基于 Web 的界面或命令行界面 (CLI) 配置会话超时（分钟）。
- 1 端口配置 - 必须正确配置端口，Dell OpenManage Systems Management Software 才能通过防火墙连接到远程设备。

 **注：** 有关各个 Dell OpenManage 系统管理组件所用端口的信息，请参阅该组件的用户指南。

安全管理

Dell 通过基于角色的访问控制 (RBAC)、验证和加密，或通过 Active Directory（或通过 Linux 操作系统上的 Winbind、Kerberos、LDAP 或 NIS），为基于 Web 的界面和命令行界面提供安全和访问管理。

RBAC

RBAC 通过确定可以由特定角色用户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。借助 RBAC，安全管理可以与组织结构紧密相关。有关设置用户的信息，请参阅操作系统说明文件。

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。三种用户级别为：“用户”、“高级用户”和“管理员”。

“User”（用户）可以查看大多数信息。

“Power User”（高级用户）可以设置警告阈值，并配置出现警告或故障事件时采取的警报措施。

“Administrator”（管理员）可以配置和执行关机操作，配置在操作系统不响应时系统的自动恢复操作，以及清除硬件、事件和命令日志。“Administrator”（管理员）可以配置警报措施，例如当生成警报时发送电子邮件信息。

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

表 2-1. 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

管理员访问权限允许关闭受管系统。

写访问权限可以修改或设置受管系统上的值。

读访问权限允许查看 Server Administrator 报告的数据。读访问权限不允许更改或设置的值。

访问 Server Administrator 服务的权限级别

[表 2-2](#) 概括了具有访问和管理 Server Administrator 服务权限的用户级别。

表 2-2. Server Administrator 用户权限级别

服务	所需用户权限级别	
	视图	管理
工具	U、P、A	P、A
远程访问	U、P、A	A
更新	U、P、A	A
存储设备管理	U、P、A	A

[表 2-3](#) 定义了[表 2-2](#)中使用的用户权限级别缩写。

表 2-3. Server Administrator 用户权限级别说明

U	用户
P	高级用户
A	管理员

验证

Server Administrator 验证方案确保可以将访问类型分配给正确的用户权限。此外，调用 CLI 时，Server Administrator 验证方案会验证当前过程运行的环境。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 Windows 操作系统，Server Administrator 验证使用集成 Windows 验证（旧称 NTLM）进行验证。该验证系统使 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 验证基于可插拔验证模块（PAM）库。此公开的功能程序库使管理员可以确定各应用程序验证用户的方法。

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 时，支持的 Windows、Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server 操作系统可使用 Java 安全套接字扩展（JSSE）来保护用户凭据和其它通过套接字连接传输的敏感数据。

Microsoft Active Directory

Active Directory Service (ADS) 软件可作为网络安全性的中央机构。ADS 使操作系统可以验证用户身份并控制该用户对网络资源的访问。对于在支持的 Windows 平台上运行的 Dell OpenManage 应用程序，Dell 为客户提供了可以修改其 Active Directory 数据库的架构扩展，以支持远程管理验证和授权。IT Assistant、Server Administrator 和 Dell Remote Access Controller 可以与 Active Directory 交互，以便从一个中央数据库添加并控制用户和权限。有关使用 Active Directory 的信息，请参阅[使用 Microsoft Active Directory](#)。

Linux 操作系统的验证协议

Dell OpenManage 应用程序（版本 5.2 及更高版本）支持 Linux 操作系统的网络信息服务（NIS）、Winbind、Kerberos 和轻型目录访问协议（LDAP）验证协议。

在 Microsoft Windows Server 2008 Core 和 Microsoft Hyper-V Server 上安装 Dell OpenManage 软件

安装指南

- [简介](#)
- [安装 Managed System 和 Management Station 软件](#)

简介

Microsoft® Windows Server® 2008 和 Hyper-V™ Server 操作系统的 Server Core 安装选项为运行特定服务器角色提供了最低环境，降低了这些服务器角色的维护和管理要求并缩小了受攻击面。Windows Server 2008 Core 或 Hyper-V Server 安装仅安装支持的服务器角色所需的二进制文件。例如，Explorer shell 不作为 Windows Server 2008 Core 或 Hyper-V Server 安装的一部分安装。相反，Windows Server 2008 Core 或 Hyper-V Server 安装的默认用户界面是命令提示符。

- **注：** Windows Server 2008 Core 或 Hyper-V Server 操作系统不支持基于图形用户界面 (GUI) 的 Dell™ OpenManage™ 软件组件的安装。需要在 Server Core 上的命令行界面 (CLI) 模式中安装 OpenManage 软件。有关 Server Core 的详细信息，请访问 Microsoft 网站。
- **注：** 在 Windows 2007 上，要成功安装 Systems Management Software，您必须使用属于“Administrators Group”（管理员组）的帐户登录，而且应使用右键菜单上的“Run as administrator”（以管理员身份运行）选项执行 setup.exe。
- **注：** 必须以内置管理员身份登录才能在 Windows Server 2008 和 Windows Vista® 上安装系统管理软件。请参阅 Windows Server 2008 帮助了解有关内置 Administrator 帐户的信息。

安装 Managed System 和 Management Station 软件

本节提供有关在 Windows Server 2008 Core 或 Hyper-V Server 操作系统上的 CLI 模式中安装 managed system 和 management station 软件的说明。

在 CLI 模式中运行 PreReqChecker

在安装 Dell OpenManage 软件之前运行 PreReqChecker。有关在 CLI 模式中运行前提条件检查程序的详情，请参阅[“前提条件检查程序”](#)。

在 Windows Server 2008 Core 或 Hyper-V Server 上，因为无 GUI 可用，所以需要以 CLI 模式运行前提条件检查程序。

- 1 **Managed System 软件：** 在命令提示符中键入 `runprereqchecks.exe /s`。文件 `runprereqchecks.exe` 位于 *Dell Systems Management Tools and Documentation* DVD 上 `SYSMGMT\srvadmin\windows\prereqchecker` 中。

- **注：** 返回代码为负 (-1 至 -10) 表示在运行前提条件检查程序工具本身自身故障。导致返回代码为负的一些可能原因包括软件策略限制、脚本限制、缺乏文件夹许可以及大小限制。有关 PreReqChecker 返回代码的详情，请参阅[“无提示运行前提条件检查时返回的代码”](#)。
- **注：** 如果遇到返回代码为 2 或 3，建议检查 Windows 临时文件夹 `%TEMP%` 中的 `omprereq.htm` 文件。要查找 `%TEMP%`，运行 `echo %TEMP%` 命令。
- **注：** `omprereq.htm` 是一个 html 文件。将此文件传输至另一台装有浏览器的计算机以阅读此文件。

从前提条件检查程序返回值 2 的常见原因：

- 1 其中一个存储器控制器或驱动程序的固件或驱动程序已过期。请参阅 `firmwaredriverversions_<lang>.html`（其中 `<lang>` 代表语言）或在 `%TEMP%` 文件夹中找到的 `firmwaredriverversions.txt`。要查找 `%TEMP%`，运行 `echo %TEMP%` 命令。
- 1 除非在系统上检测到设备，否则不选择默认安装 RAC 组件软件版本 4。在这种情况下，前提条件检查程序会生成一个警告信息。
- 1 仅当检测到系统上的相应设备时，才会选择默认安装 Intel® 和 Broadcom® 代理。如果未找到相应设备，前提条件检查程序会生成一个警告信息。
- 1 运行在系统上的 DNS 或 WINS 服务器可导致 RAC 软件产生警告条件。有关详情，请参阅 Server Administrator 自述文件中相关章节。
- 1 请勿在相同系统上安装 managed system 和 management station RAC 组件。仅安装 managed system RAC 组件，因为它提供了所需功能。

从前提条件检查程序返回代码 3（故障）的常见原因：

- 1 您未以内置管理员权限登录。
- 1 MSI 软件包损坏或其中一个所需的 XML 文件损坏。
- 1 从 DVD 复制时出现错误以及从网络共享复制时出现网络访问问题。
- 1 前提条件检查程序检测到另一个 MSI 软件包安装正在运行或重新引导挂起：
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\InProgress` 表示另一个 MSI 软件包安装正在进行中。
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations` 表示重新引导挂起。
- 1 运行 Windows 2008 Core 的 x64 版本，因为有些组件已被禁用而无法安装。

确保在继续安装 Dell OpenManage 软件组件之前纠正任何错误或警告情况。


以 CLI 模式安装 Managed System 软件

1. 确保安装 managed system 组件之前纠正 PreReqChecker 检测到的所有错误或警告。
2. 使用 `msiexec /i SysMgmt.msi` 命令从命令提示符启动 MSI 文件。MSI 文件 `SysMgmt.msi` 位于 *Dell Systems Management Tools and Documentation DVD* 上 `SYSMGMT\sradmin\windows\SystemManagement` 中。

要安装 managed system 软件的本地化版本，请在命令提示符下

键入 `msiexec /I SysMgmt.msi TRANSFORMS= <language_transform>.mst`。用相应的语言文件替换 `<language_transform>.mst`：

- 1 **1031.mst** (德语)
- 1 **1034.mst** (西班牙语)
- 1 **1036.mst** (法语)
- 1 **1041.mst** (日语)
- 1 **2052.mst** (简体中文)

 **注：** 有关 MSI 安装程序可选命令行设置的详情，请参阅“[MSI 安装程序命令行设置](#)”。

卸载系统管理软件

要卸载 managed system 软件，在命令提示符下执行 `msiexec /x sysmgmt.msi` 命令。

[目录](#)

设置和管理

安装指南

- [开始之前](#)
- [安装要求](#)
- [配置支持的 Web 浏览器](#)
- [配置 SNMP 代理](#)
- [安全端口服务器和安全性设置](#)

开始之前

- 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 阅读位于 Dell 支持网站 support.dell.com/support/edocs/software/omswrels/index.htm 上适用的 Dell OpenManage 自述文件和《Dell 系统软件支持值表》。除有关已知问题的信息外，这些文件还包含有关软件、固件和驱动程序版本的最新信息。
- 1 如果正在运行介质上的任何应用程序，则应先关闭该应用程序，然后再安装 Server Administrator 应用程序。
- 1 阅读操作系统的安装说明。
- 1 在 Linux 操作系统上，确保 Server Administrator RPM 所需的所有操作系统 RPM 软件包均已安装。

安装要求

本节介绍了 Dell OpenManage Server Administrator 的一般要求并包括以下信息：

- 1 “[支持的操作系统和 Web 浏览器](#)”
- 1 “[系统要求](#)”

具体操作系统的必备要求被列为安装过程的一部分。

支持的操作系统和 Web 浏览器

有关所支持的操作系统和 Web 浏览器，请参阅 Dell 支持网站 support.dell.com/support/edocs/software/omswrels/index.htm 上的《Dell 系统软件支持值表》。


- ❗ **注：** Dell OpenManage 安装程序在 Microsoft Windows Storage Server™ 2003 R2、Microsoft Windows Storage Server 2003 R2、Express x64 Edition with Unified Storage、Microsoft Windows Storage Server 2003 R2、Workgroup x64 Edition with Unified Storage 以及 Windows Server 2008（包括 x86 和 x64）R2 操作系统上提供多语言用户界面支持。多语言用户界面软件包是一组特定语言的资源文件，可添加到所支持 Windows 操作系统的英文版本中。然而，Dell OpenManage 6.3 安装程序只支持六种语言：英语、德语、西班牙语、法语、简体中文和日语。
- ❗ **注：** 当多语言用户界面 (MUI) 设置为诸如简体中文或日语等非 Unicode 语言时，将系统区域设置为简体中文或日语。这样就能够显示前提条件检查程序信息。这是因为只有将系统区域（在 XP 上也称为“**非 Unicode 程序的语言**”）设置为与应用程序的语言一致时，任何非 Unicode 应用程序才能运行。

系统要求


Dell OpenManage Server Administrator 必须安装在每个需要管理的系统上。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。

Managed System 要求

- 1 其中一个“[支持的操作系统和 Web 浏览器](#)”
- 1 至少 2 GB RAM
- 1 至少 512 MB 硬盘驱动器可用空间
- 1 管理员权限
- 1 受管系统和远程系统间的 TCP/IP 连接，以便于远程系统管理。
- 1 任何一种 [支持的系统管理协议标准](#)（请参阅“[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。建议的屏幕分辨率为 1024 x 768
- 1 Server Administrator Remote Access Controller 服务要求在要管理的系统上安装 Remote Access Controller (RAC)。有关完整的软件和硬件要求，请参阅相应的《Dell Remote Access Controller 用户指南》


 **注：** 如果受管系统满足 RAC 的所有安装前提条件，则在安装 Managed System Software 时，RAC 软件将作为“**Typical Setup**”（**典型安装**）安装选项的一部分进行安装。有关完整的软件和硬件要求，请参阅相应的《Dell Remote Access Controller 用户指南》。

- 1 Server Administrator Storage Management Service 要求将 Dell OpenManage Server Administrator 安装在系统上才能正确管理。请参阅《Dell OpenManage Server Administrator Storage Management 用户指南》了解软件和硬件的全部要求。
- 1 Microsoft Software Installer (MSI) 3.1 或更高版本

 **注：** Dell OpenManage 软件检测系统上的 MSI 版本。如果版本低于 3.1，则前提条件检查程序将给出升级到 MSI 版本 3.1 的提示。将 MSI 升级到版本 3.1 之后，可能需要重新引导系统，以便安装诸如 Microsoft SQL Server 等其它软件应用程序。

支持的系统管理协议标准

必须在受管系统上安装支持的系统管理协议，才能安装 Management Station 或 Managed System 软件。在支持的 Windows 和 Linux 操作系统上，Dell OpenManage 软件支持：公用信息模型 (CIM)、Windows 管理工具 (WMI) 和简单网络管理协议 (SNMP)。您必须安装随操作系统提供的 SNMP 信息包。

 **注：** 有关在受管系统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 3-1](#) 说明了每个支持的操作系统的系统管理标准。

表 3-1. 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
支持的 Red Hat Enterprise Linux 操作系统。	安装随操作系统提供的 SNMP 软件包。	可用。安装 <i>Dell Systems Management Tools and Documentation</i> DVD 上提供的 CIM 软件包 - SFCB/SFCC/CMPI-Devel
支持的 SUSE Linux Enterprise Server 操作系统。	安装随操作系统提供的 SNMP 软件包。	可用。安装 <i>Dell Systems Management Tools and Documentation</i> DVD 上提供的 CIM 软件包 - SFCB/SFCC/CMPI-Devel

Windows Server 2003 R2 和 R2 IPMI 设备驱动程序

本节中的内容仅适用于 Dell PowerVault x00 系统和 Dell PowerEdge x8xx 系统和更高版本。

Windows Server 2003 R2 和 Windows Storage Server R2 包含一个名为 Hardware Management 的可选组件。此组件包含一个 IPMI 驱动程序。在安装过程中，该组件安装并启用其 IPMI 驱动程序。

当 Server Administrator 启动时，它首先确定 Windows Server 2003 R2 IPMI 驱动程序是否已启用。如果该驱动程序已启用，则 Server Administrator 使用 Windows Server 2003 R2 IPMI 驱动程序提供其基于 IPMI 的功能。如果 Windows Server 2003 R2 IPMI 驱动程序没有启用，则 Server Administrator 使用其内部 IPMI 支持来提供其基于 IPMI 的功能。对于 Server Administrator，建议您最好使用 Windows Server 2003 R2 IPMI 驱动程序，而不要使用内部 IPMI 支持。如果系统运行的是 Windows Server 2003 R2 或 Windows Storage Server R2，建议在安装 Server Administrator 后，还安装 R2 的可选 Hardware Management 组件。

要在 Dell PowerVault x00 系统上安装 Windows Server 2003 R2 IPMI 驱动程序，请执行以下附加步骤：

- 1 从命令外壳中，执行以下命令：

```
Rundll32 ipmisetp.dll, AddTheDevice
```

安装 Windows Server 2003 R2 的 Hardware Management 组件后，重新启动 **DSM SA Data Manager** 服务，使 Server Administrator 能从使用其内部 IPMI 支持切换到使用 Windows Server 2003 R2 IPMI 驱动程序。要重新启动该服务，既可手工重新启动该服务，也可重新引导系统。


如果以后通过手工方式卸载或通过卸载 Hardware Management 组件（这将卸载驱动程序）而卸载 Windows Server 2003 R2 IPMI 驱动程序，请重新启动 **DSM SA Data Manager** 服务，以便使 Server Administrator 能从使用 Windows Server 2003 R2 IPMI 驱动程序切换到使用其内部 IPMI 支持。要重新启动该服务，既可手工重新启动该服务，也可重新引导系统。

数字证书

所有用于 Microsoft 的 Server Administrator 软件包都使用 Dell 认证进行数字签名，该认证有助于确保软件包安装的完整性。如果对这些软件包重新封装、编辑或以其它方式处理，则数字签名将失效。这种处理会生成不受支持的安装软件包并且前提条件检查程序不允许安装软件。

配置支持的 Web 浏览器

如需查阅支持的 Web 浏览器的列表，请参阅“[支持的操作系统和 Web 浏览器](#)”。

 **注：** 确保将 Web 浏览器设置为对于本地地址不使用代理服务器。

查看本地化版本的基于 Web 的界面

在运行 Windows 操作系统的系统上，使用 Windows **控制面板** 中的“Regional and Language Options”（**区域和语言选项**）查看本地化版本的基于 Web 的界面。


Microsoft Active Directory

如果使用 Active Directory 服务软件，可以配置它以控制对网络的访问。Dell 修改了 Active Directory 数据库以支持远程管理身份验证和授权。Dell OpenManage Server Administrator、IT Assistant 和 Dell Remote Access Controllers 可以与 Active Directory 交互。借助此工具，可以从一个中央数据库添加并控制用户和权限。如果使用 Active Directory 控制用户对网络的访问，请参阅[使用 Microsoft Active Directory](#)。

配置 SNMP 代理

在所有支持的操作系统中，Dell OpenManage 软件均支持 SNMP 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。安装 Dell OpenManage 软件之前，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 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，请更改默认 SNMP 团体名称。有关更改 SNMP 团体名称的信息，请参阅针对您的操作系统的以下相应章节。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。

以下部分提供了有关为每种支持的操作系统配置 SNMP 代理的逐步说明：

- 1 [为运行支持的 Windows 操作系统的系统配置 SNMP 代理](#)
- 1 [在运行支持的 Red Hat Enterprise Linux 操作系统的系统上配置 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](#)


为运行支持的 Windows 操作系统的系统配置 SNMP 代理

Dell OpenManage 软件使用 Windows SNMP 代理提供的 SNMP 服务。在支持的连接到 System Administrator 会话的两种方式中，SNMP 是一种，另一种是 CIM/WMI。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。

通过 Windows Server 2003 上的远程主机启用 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。

 **注：** 为更改管理功能而重新引导系统不需要 SNMP Set 操作。

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 IT Assistant 主机添加到“Accept SNMP packets from these hosts”（**接受来自这些主机的 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。管理站应用程序使用的 SNMP 团体名称必须与在 Dell OpenManage 软件系统上配置的 SNMP 团体名称匹配，以

便管理应用程序可以从 Dell OpenManage 软件检索系统管理信息。

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）文本框中键入管理站的团体名称（默认为 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）文本框中编辑管理站的团体名称，然后单击“OK”（确定）。

系统将显示 $\circ \times$ SNMP Service Properties”（SNMP 服务属性） $\times \circ \square \circ \text{£}$
6. 单击“OK”（确定）以保存更改。

启用 SNMP 设置操作

在运行 Dell OpenManage 软件的系统上启用 SNMP Set 操作，以便使用 IT Assistant 更改 Dell OpenManage 软件属性。要从 IT Assistant 启用系统的远程关机，请启用 SNMP Set 操作。

 **注：** 为更改管理功能而重新引导系统不需要 SNMP Set 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”（团体权限）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。

 **注：** 在 Dell OpenManage Server Administrator 版本 5.3 和更高版本中，Server Administrator 中默认禁用了 SNMP Set 操作。Server Administrator 提供对启用或禁用 SNMP Set 操作的支持。您可以使用“Preferences”（首选项）下的 Server Administrator SNMP 配置页或 Server Administrator 命令行界面（CLI）来启用或禁用 SNMP Set 操作。有关在 Server Administrator 中启用或禁用 SNMP Set 操作的详细信息，请参阅《Dell OpenManage Server Administrator 用户指南》或《Dell OpenManage Server Administrator 命令行界面用户指南》。

配置您的系统以向管理站发送 SNMP 陷阱

Dell OpenManage 软件生成 SNMP 陷阱，以响应传感器状况的更改和其它受监测参数的更改。您必须在 Dell OpenManage 软件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。

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. 要添加陷阱的团体，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）。

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


- c. 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 操作系统的系统上配置 SNMP 代理

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

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

SNMP Agent Access Control 配置

Server Administrator 实现的 MIB (Management Information Base [管理信息库]) 分支标有 1.3.6.1.4.1.674 OID。管理站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。

对于支持的 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 遇到这一行，会将此行修改为：

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

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

 **注：** 为确保 Server Administrator 能够修改 SNMP 代理配置以提供对系统管理数据的适当访问权限，建议在安装 Server Administrator 之后再对其他所有 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。系统管理应用程序使用的 SNMP 团体名称必须与一个在 Server Administrator 软件系统上配置的 SNMP 团体名称匹配，以便系统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

必须在运行 Server Administrator 的系统上启用 SNMP Set 操作才能使用 IT Assistant 更改 Server Administrator 软件属性。要从 IT Assistant 启用系统的远程关机，请启用 SNMP Set 操作。

 **注：** 为更改管理功能而重新引导系统不需要 SNMP Set 操作。

要在运行 Server Administrator 的系统上启用 SNMP Set 操作，请编辑 `/etc/snmp/snmpd.conf` SNMP 代理配置文件并执行下列步骤：

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_地址 团体_名称
```

其中，`IP_地址` 是 Management Station 的 IP 地址，`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：

```
service snmpd restart
```


在运行支持的 Red Hat Enterprise Linux 操作系统的系统中配置防火墙

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态。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，至少一个外部网络接口上的 SNMP 端口必须处于打开状态。如果 Server Administrator 检测到防火墙中未打开任何外部网络接口的 SNMP 端口，则 Server Administrator 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。

3. 选择“Security Level”（**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 Windows GUI，则按 `<F1>` 不会提供有关新版 Red Hat Enterprise Linux 操作系统防火墙安全级别的信息。

- a. 要禁用防火墙，请选择“**No firewall**”（**无防火墙**）或“**Disabled**”（**禁用**）并转至**步骤 7**。
- b. 要打开整个网络接口或 SNMP 端口，请选择“**High**”（**高级**）、“**Medium**”（**中级**）或“**Enabled**”（**已启用**）。

- d. 选择“**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。

5. 选择打开整个网络接口还是仅打开所有网络接口上的 SNMP 端口。

- a. 要打开整个网络接口，请选择“**Trusted Devices**”（**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。
- b. 要打开所有网络接口上的 SNMP 端口，请选择“**Other ports**”（**其它端口**），然后键入 `snmp:udp`。

6. 选择“**OK**”（**确定**）并按 `<Enter>`。

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


7. 选择“**OK**”（**确定**）并按 `<Enter>`。

系统将显示“Choose a Tool”（**选择工具**）菜单。

8. 选择“**Quit**”（**退出**）并按 `<Enter>`。

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 代理以正确地与系统管理应用程序（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 10）中，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。因为该对象标识符必须用 SNMP 代理来配置，所以在安装过程中，Server Administrator 会将 `/etc/snmpd.conf` 或 `/etc/snmp/snmpd.conf` 一行添加到 SNMP 代理配置文件中（如果该行不存在的话）：


```
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。此项配置不允许在其它主机上运行的 IT Assistant 等 SNMP 管理应用程序正常搜索和管理 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。


要启用从特定的远程主机对运行 Server Administrator 的系统的 SNMP 访问，请编辑 SNMP 代理配置文件 `/etc/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. 编辑或复制该行，以使用远程主机 IP 地址来替换 127.0.0.1。编辑后，新行应为：

```
rocommunity public IP_address
```

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

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

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

要启用从所有远程主机对运行 Server Administrator 的系统的 SNMP 访问，请编辑 SNMP 代理配置文件 `/etc/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. 通过删除 127.0.0.1 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 的系统中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 团体_名称 127.0.0.1
```

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

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

启用 SNMP 设置操作

为使用 IT Assistant 更改 Server Administrator 属性，应在运行 Server Administrator 的系统上启用 SNMP 设置操作。要从 IT Assistant 启用系统的远程关机，请启用 SNMP Set 操作。

 **注：** 为更改管理功能而重新引导系统不需要 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`，并执行以下步骤：

1. 查找以下行：

```
rocommunity public 127.0.0.1
```

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

```
rwcommunity public 127.0.0.1
```

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

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

配置您的系统以向管理站发送陷阱

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_地址 团体_名称
```

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
```


安全端口服务器和安全性设置

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

您可以从相应“Preferences”（**首选项**）页面为 Server Administrator 和 IT Assistant 设置用户和安全端口服务器首选项。单击“General Settings”（**常规设置**）并单击“User”（**用户**）选项卡或 Web Server 选项卡。

 **注：** 要设置或重设用户或服务器首选项，您必须以 Administrator（管理员）权限登录。

要设置用户首选项，请执行以下步骤：

1. 单击全局导航栏上的“Preferences”（**首选项**）。

系统将显示“Preferences”（**首选项**）主页。

2. 单击“General Settings”（**常规设置**）。

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

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

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

要设置安全端口服务器首选项，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**）功能可以设置会话保持活动的时间限制。选择“Enable”（**启用**）单选按钮启用在指定分钟内没有用户交互情况下的超时。会话超时的用户必须再次登录才能继续。选择“Disable”（**禁用**）单选按钮禁用 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受管系统上的 Server Administrator。

- 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 所绑定到的受管系统的 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：** 具有管理员权限的用户在远程登录系统时不能使用 Server Administrator。

 **注：** 将“IP Address to Bind to”（**要绑定到的 IP 地址**）的值更改为除“All”（**所有**）以外的值可能会妨碍其它应用程序或浏览器远程访问受管系统上的 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**）字段可指定您单位的简单邮件传输协议（SMTP）和域名服务器（DNS）后缀。要启用 Server Administrator 发送电子邮件，您必须在相应字段中键入您单位的 SMTP 服务器的 IP 地址和 DNS 后缀。

 **注：** 出于安全保护的原因，您的单位可能不允许通过 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**）字段可指定为受管系统提供支持的企业实体的 Web 地址。

- 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。其它选项有 !、@、#、\$、%、^、*、-、?、:、| 和 ,。

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。

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

可以从相应“Preferences”（**首选项**）页面中管理 Server Administrator 和 IT Assistant 的 X.509 证书。单击“General Settings”（**常规设置**），选择 Web Server 选项卡，并单击“X.509 Certificate”（**X.509 认证**）。使用 X.509 认证工具生成新的 X.509 认证、重新使用现有的 X.509 认证或通过 CA 导入根认证或认证链。已授权的 CA 包括 Verisign、Entrust 和 Thawte。

X.509 证书管理的最佳实践

为确保在使用 server administrator 时系统安全不受影响，应始终遵循以下要点：

- 1 **唯一的主机名：** 所有装有 server administrator 的系统都应具有唯一主机名。
- 1 **更改 'localhost' 为唯一：** 所有主机名设为 'localhost' 的系统都应更改为唯一主机名。

[目录](#)