Dell OpenManage™ IT Assistant 7.2 版用户指南

注和注意

注： “注”表示可以帮助您更好地使用计算机的重要信息。

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

本说明文件中的信息如有更改，恕不另行通知。
© 2005 Dell Inc. 版权所有，翻印必究。

未经 Dell Inc. 书面许可，严禁以任何形式进行复制。

本文中使用的商标：*Dell*、*DELL* 徽标、*Dell OpenManage*、*OptiPlex*、*PowerEdge* 和 *PowerConnect* 是 Dell Inc. 的商标；*Microsoft* 和 *Windows* 是 Microsoft Corporation 的注册商标；*Novell* 和 *NetWare* 是 Novell, Inc. 的注册商标；*Red Hat* 是 Red Hat, Inc. 的注册商标；*Intel* 是 Intel Corporation 的注册商标。

本说明文件中述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。

2005 年 12 月

返回目录页

配置协议将信息发送给 IT Assistant

Dell OpenManage™ IT Assistant 7.2 版用户指南

Dell OpenManage™ IT Assistant 使用两个系统管理协议 — 简单网络管理协议 (SNMP) 和公用信息模型 (CIM)。 此附录提供 SNMP 和 CIM 的配置信息。 这些系统管理协议可让 IT Assistant 使用服务器代理程序或 Dell OpenManage Client Instrumentation (OMCI) 获得 Dell™ 系统的状态。 此附录包括配置用于支持查找、状况和陷阱信息的 SNMP 和 CIM 的程序。 下表汇总了可由 IT Assistant 管理的支持操作系统和相应的 SNMP 和 CIM 协议的可用性。

表 A-1. Managed System 上支持的操作系统和系统管理协议

操作系统	SNMP	CIM
Microsoft® Windows® 操作系统	在操作系统安装介质中可用	在操作系统安装介质中可用
Red Hat® Linux 操作系统	您必须安装随操作系统提供的 SNMP 信息包。	不可用
Novell® NetWare® 操作系统	始终安装。	不可用

配置 SNMP 服务

为正确安装和运行 IT Assistant，它必须安装在安装并运行 SNMP 服务的支持的 Microsoft 操作系统上。 除非在安装之后进行了修改，否则 Microsoft 操作系统 SNMP 服务应无需附加配置。 尽管 IT Assistant 系统上的 SNMP 服务无需特殊配置，但系统上将管理的 SNMP 服务需要特殊配置。 此外，尽管 IT Assistant 只能安装在支持的 Microsoft 操作系统上，但它可以管理运行支持的 Microsoft、Novell NetWare 和 Red Hat Linux 操作系统的系统。 本节说明如何在这些 Managed System 上配置 SNMP。

使用 SNMP 协议与 IT Assistant 进行通信的每个 Managed System 必须具有设定的读/写和只读团体名称。 如果要您的 IT Assistant 能够从这些 Managed System 接收陷阱，您还必须配置通过主机名或 IP 地址定义的 SNMP 陷阱目标。

IT Assistant 和 Server Administrator 中的 SNMP 团体名称

要使 IT Assistant 能够在运行 Dell OpenManage Server Administrator（Dell 建议的服务器代理程序）和/或其它支持的代理程序的系统上成功读取信息、修改信息和执行操作，IT Assistant 使用的团体名称必须与 Managed System 上相应的团体只读 (Get) 和读/写 (Set) 团体名称相匹配。 此外，为使 IT Assistant 能够从运行 Server Administrator 的系统中接收陷阱（异步事件通知），系统必须被配置为将陷阱发送至运行 IT Assistant 的系统。

团体名称必须安全

Get 和 Set 团体名称存在操作系统默认名称。 为安全考虑，应该更改这些名称。 在为您的网络选择团体名称时，请遵照以下原则：

- 将 Get 和 Set 名称更改为难以猜中的密码。
- 避免使用字符串，例如，您公司的名称或电话号码或有关您本人的任何公开个人信息。
- 使用包括字母和数字的字母数字字符串，混合使用大写和小写字母；团体名称区分大小写。
- 使用长度至少为六个字符的字符串。

在运行支持的 Windows 操作系统的系统上配置 SNMP 服务

运行 IT Assistant

IT Assistant 可以安装在具有以下任何操作系统的系统上：Windows 2000、Windows XP Professional 或 Windows Server™ 2003。 有关支持的操作系统详情和硬件配置的最新信息，请参阅自述文件。

要在 IT Assistant 系统上安装 SNMP，请执行以下步骤：

1. 单击“**Start**”（开始）按钮，指向“**Settings**”（设置），并选择“**Control Panel**”（控制面板）。
2. 双击“**Add/Remove Programs**”（添加/删除程序）图标。
3. 在左手窗格中，单击“**Add/Remove Windows Components**”（添加/删除 Windows 组件）。
4. 选择“**Management and Monitoring Tools**”（管理和监视工具），单击“**Details**”（详细信息），选择“**Simple Network Management Protocol**”（简单网络管理协议），然后单击“**OK**”（确定）。
5. 单击“**Next**”（下一步）。

   “**Windows Optional Networking Components Wizard**”（Windows 可选网络组件向导）将安装 SNMP。

在运行支持的 Windows 操作系统的 IT Assistant Managed System 上配置 SNMP 服务

Server Administrator 和 Dell PowerConnect™ 交换机等某些其它 Managed System 代理程序使用 SNMP 协议与 IT Assistant 进行通信。 要启用此通信，必须正确配置 Windows SNMP 服务，以便启用 Get 和 Set 操作并将陷阱发送至服务系统。

注：有关 SNMP 配置的其它详情，请参阅操作系统说明文件。

注：对于被查找的运行 Windows Server 2003 的系统，Windows Server 2003 上的 Microsoft 标准 SNMP 配置需要将 SNMP 配置为从 IT Assistant 主机接受软件包。

更改 SNMP 团体名称

配置 SNMP 团体名称可以确定哪些系统能够通过 SNMP 管理您的系统。

1. 如果您的系统运行的是 Windows Server 2003，请单击“**Start**”（开始）按钮，右键单击“**My Computer**”（我的电脑），并指向“**Manage**”（管理）。 如果您的系统运行的是 Windows 2000，请右键单击“**My Computer**”（我的电脑），并指向“**Manage**”（管理）。

   出现“**Computer Management**”（计算机管理）窗口。
2. 展开该窗口中的“**Computer Management**”（计算机管理）图标（如有必要）。
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，直到您找到“**SNMP Service**”（SNMP 服务），右键单击“**SNMP Service**”（SNMP 服务），然后单击“**Properties**”（属性）。

   出现“**SNMP Service**”（SNMP 服务）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，请在“**Accepted Community Names**”（接受的团体名称）列表下面单击“**Add**”（添加）。

      出现“**SNMP Service Configuration**”（SNMP 服务配置）窗口。
   b. 在“**Community Name**”（团体名称）文本框中键入能够管理您系统的系统的团体名称（默认值为 public），并单击“**Add**”（添加）。

      出现“**SNMP Service**”（SNMP 服务）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）。

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

d. 在“**Community Name**”（**团体名称**）文本框中对能够管理您系统的系统的团体名称进行所有必要的编辑，然后单击“**OK**”（**确定**）。

出现“**SNMP Service**”（**SNMP 服务**）窗口。

6. 单击“**OK**”（**确定**）以保存所做的更改。

启用 SNMP 设置操作

必须在 Managed System 上启用“SNMP 设置”操作，以便使用 IT Assistant 更改 Server Administrator 属性。

1. 如果您的系统运行的是 Windows Server 2003，请单击“**Start**”（**开始**）按钮，右键单击“**My Computer**”（**我的电脑**），并指向“**Manage**”（**管理**）。 如果您的系统运行的是 Windows 2000，请右键单击“**My Computer**”（**我的电脑**），并指向“**Manage**”（**管理**）。

出现“**Computer Management**”（**计算机管理**）窗口。

2. 展开该窗口中的“**Computer Management**”（**计算机管理**）图标（如有必要）。
3. 展开“**Services and Applications**”（**服务和应用程序**）图标，然后单击“**Services**”（**服务**）。
4. 向下滚动服务列表，直到您找到“**SNMP Service**”（**SNMP 服**务），右键单击“**SNMP Service**”（**SNMP 服务**），然后单击“**Properties**”（**属性**）。

出现“**SNMP Service**”（**SNMP 服务**）窗口。

5. 单击“**Security**”（**安全**）选项卡以更改对团体的访问权限。
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**）。

出现“**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**”（**读取创建**），然后单击“**OK**”（**确定**）。

出现“**SNMP Service**”（**SNMP 服务**）窗口。

8. 单击“**OK**”（**确定**）以保存所做的更改。

配置系统发送 SNMP 陷阱

Server Administrator 等 Managed System 代理程序生成 SNMP 陷阱以响应传感器状态和其它所监测参数的变化。 您必须在 Managed System 上为要发送至 IT Assistant 系统的这些陷阱配置一个或多个陷阱目标。

1. 如果您的系统运行的是 Windows Server 2003，请单击“**Start**”（**开始**）按钮，右键单击“**My Computer**”（**我的电脑**），并指向“**Manage**”（**管理**）。 如果您的系统运行的是 Windows 2000，请右键单击“**My Computer**”（**我的电脑**），并指向“**Manage**”（**管理**）。

出现“**Computer Management**”（**计算机管理**）窗口。

2. 展开该窗口中的“**Computer Management**”（**计算机管理**）图标（如有必要）。
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，直到您找到“**SNMP Service**”（**SNMP 服务**），右键单击“**SNMP Service**”（**SNMP 服务**），然后单击“**Properties**”（**属性**）。

出现“**SNMP Service**”（**SNMP 服务**）窗口。

5. 单击“**Traps**”（**陷阱**）选项卡，以便为陷阱添加团体，或为陷阱团体添加陷阱目标。
6. 要为陷阱添加团体，请在“**Community Name**”（**团体名称**）框中键入团体名称，并单击“**Add to list**”（**添加至列表**）。
7. 要为陷阱团体添加陷阱目标，请从“**Community Name**”（**团体名称**）下拉式菜单中选择团体名称并单击“**Add**”（**添加**）。

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

8. 键入陷阱目标并单击“**Add**”（**添加**）。

出现“**SNMP Service**”（**SNMP 服务**）窗口。

9. 单击“**OK**”（**确定**）以保存所做的更改。

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

Server Administrator 等 Managed System 代理程序使用 ucd-snmp 或 net-snmp SNMP 代理程序提供的 SNMP 服务。 您可以配置 SNMP 代理程序以更改团体名称、启用 Set（设置）操作，并将陷阱发送至 IT Assistant 系统。 要配置 SNMP 代理程序与 IT Assistant 正确交互，请执行以下各节中描述的步骤。

注：有关 SNMP 配置的其它详情，请参阅操作系统说明文件。

更改 SNMP 团体名称

正确配置 SNMP 团体名称可以确定能够在您网络中与 Managed System 进行通信的 IT Assistant 服务系统。 IT Assistant 使用的 SNMP 团体名称必须与 Managed System 上配置的 SNMP 团体名称相匹配，以便 IT Assistant 可以在您网络中的 Managed System 上成功读取、写入和执行操作。

要更改 SNMP 团体名称，请通过执行以下步骤编辑 SNMP 代理程序配置文件 **/etc/snmp/snmpd.conf**：

1. 找到下行：

```
com2sec publicsec default public
```

或

```
com2sec notConfigUser default public
```

2. 通过将 public 替换为新的 SNMP 团体名称，编辑此行。 编辑后，该行应为：

```
com2sec publicsec default 团体名称
```

或

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

启用 SNMP 设置操作

必须在运行 Server Administrator 的系统上启用“SNMP 设置”操作，以便使用 IT Assistant 更改 Server Administrator 属性。 要在运行 Server Administrator 的系统上启用“SNMP 设置”操作，请编辑 SNMP 代理程序配置文件 **/etc/snmp/snmpd.conf** 并执行以下步骤：

1. 找到下行：

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

或

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

2. 编辑此行，将第一个 none 替换为 all。 编辑后，该行应为：

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

或

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

对于 Red Hat Enterprise Linux（版本 7.3 或更高）和 Red Hat Enterprise Linux AS（版本 2.1 或更高）操作系统， sysLocation 和 sysContact 变量的默认 SNMP 权限已经更改为只读。 IT Assistant 使用这些变量的访问权限来确定是否可以通过 SNMP 执行某些操作。 这些变量必须配置有读写权限以在 IT Assistant 中启用“sets”（设置）或系统配置设置更改。 要配置这些变量，必须在 Red Hat Enterprise Linux SNMP 配置文件中注释掉 sysContact 和 sysLocation 值。

1. 查找以 sysContact 开始的行。
2. 将行更改为 #sysContact。
3. 查找以 sysLocation开始的行。
4. 将行更改为 #sysLocation。

配置 Managed System 发送陷阱到 IT Assistant

Server Administrator 等 Managed System 代理程序生成 SNMP 陷阱以响应传感器状态和 Managed System 上其它所监测参数的变化。 为使 IT Assistant 接收这些陷阱，必须在 Managed System 上配置一个或多个陷阱目标。

要将运行 Server Administrator 的系统配置为将陷阱发送至服务系统，请通过执行以下步骤编辑 SNMP 代理程序配置文件 **/etc/snmp/snmpd.conf**：

1. 将以下行添加至文件：

```
trapsink IP_address community_name
```

其中，*IP_address*（*IP 地址*）是服务系统的 IP 地址，*community_name*（*团体名称*）是 SNMP 团体名称。

2. 保存 **snmpd.conf** 文件并重新启动 snmpd 服务。

在运行支持的 NetWare 操作系统上配置 SNMP 代理程序

Server Administrator 等 Managed System 代理程序使用 NetWare SNMP 代理程序提供的 SNMP 服务。 您可以配置 SNMP 代理程序以更改团体名称、启用“Set”（设置）操作，并将陷阱发送至服务系统。 要配置 SNMP 代理程序与 IT Assistant 正确交互，请执行以下各节中描述的任务。

注：有关 SNMP 配置的其它详情，请参阅操作系统说明文件。

注：所有团体名称均区分大小写。

更改 SNMP 团体名称

IT Assistant 使用的 SNMP 团体名称必须与所有 Managed System 上配置的 SNMP 团体名称相匹配。 IT Assistant 需要从 Server Administrator 和任何其它支持的代理程序中检索管理信息。

要在 Managed System 上更改 SNMP 团体名称，请执行以下步骤：

1. 在 NetWare 命令行控制台中，键入 inetcfg 并按 <Enter>。

   出现 **“Internetworking Configuration”（联网配置）**菜单。

   注： 如果这是您首次使用 inetcfg 命令，系统可能会提示您下列问题：Do you want to transfer LAN drivers, protocol, and remote access commands?（您是否要传输 LAN 驱动程序、协议和远程访问命令？） Dell 建议您对此信息回答 **“Yes”（是）**。 有关此提示的附加信息，请参阅 Novell 网站。 选择 **“Yes”（是）**时，系统将会强制重新启动。 系统重新启动之后，请返回控制台并再次键入 inetcfg 命令。 这时弹出的屏幕将显示以下提示：Do you want to use the fast setup method or the standard method?（您想使用快速设置方法还是标准方法？）Dell 建议您选择标准方法来执行 SNMP 设置。 选择标准方法之后，请参阅下一步。

2. 选择 **“Manage Configuration”（管理配置）**。

   出现 **“Manage Configuration”（管理配置）**菜单。

3. 选择 **“Configure SNMP Parameters”（配置 SNMP 参数）**。

   出现 **“SNMP Parameters”（SNMP 参数）**菜单。

4. 选择 **“Monitor State”（监测状态）**以配置读取（或 Get）团体名称。

   出现 **“Monitor Community Handling”（监测团体处理）**菜单，包含以下选项：

   - 可以读取的任何团体
   - 保留为默认设置
   - 不可读取的团体
   - 可以读取的指定团体

   注： 有关 **“Monitor State”（监测状态）**的详情，请按 <F1>。 按 <Esc> 可以清除帮助窗口。

5. 选择 **“Specified Community May Read”（可以读取的指定团体）**。
6. 在 **“Monitor Community”（监测团体）**下面，输入读取团体名称。
7. 选择 **“Control State”（控制状态）**以配置写入（或设置）团体名称。

   出现包含以下选项的 **“Control Community Handling”（控制团体处理）**菜单：

   - 可以写入的任何团体
   - 保留为默认设置
   - 不可写入的团体
   - 可以写入的指定团体

   注： 有关 **“Control State”（控制状态）**的详情，请按 <F1>。 按 <Esc> 可以清除帮助窗口。

8. 选择 **“Specified Community May Write”（可以写入的指定团体）**。
9. 在 **“Control Community”（控制团体）**下面，输入写入团体名称。
10. 选择 **“Trap State”（陷阱状态）**以配置陷阱团体处理。

    出现包含以下选项的 **“Trap Handling”（陷阱处理）**菜单选项：

    - 请勿发送陷阱
    - 保留为默认设置
    - 发送包含指定团体的陷阱

11. 选择 **“Send Traps With Specified Community”（发送包含指定团体的陷阱）**。

12. 在“**Trap Community**”（**陷阱团体**）下面，输入要陷阱包含的团体名称。

   注：有关“**Trap State**”（**陷阱状态**）的详情，请按 <F1>。 按 <Esc> 可以清除帮助窗口。

13. 按 <Esc> 以退出“**SNMP Parameters**”（**SNMP 参数**）菜单。

   出现信息框，提示您保存更改。

14. 选择“**Yes**”（**是**）。

   出现“**Manage Configuration**”（**管理配置**）菜单。

15. 按 <Esc> 以退出“**Manage Configuration**”（**管理配置**）菜单。

   出现“**Internetworking Configuration**”（**联网配置**）菜单。

16. 选择“**Protocols**”（**协议**）。

   出现“**Protocol Configuration**”（**协议配置**）菜单。

17. 选择 **TCP/IP**。

   出现“**TCP/IP Protocol Configuration**”（**TCP/IP 协议配置**）菜单。

18. 选择“**SNMP Manager Table**”（**SNMP 管理器表**）。

   出现包含以下选项的“**SNMP Manager Table**”（**SNMP 管理器表**）菜单：

   - 按 <Ins> 添加 SNMP 陷阱目标。
   - 按 <Enter> 修改 SNMP 陷阱目标。
   - 按 <Del> 删除 SNMP 陷阱目标。

   注：有关“**SNMP Manager Table**”（**SNMP 管理器表**）的详情，请按 <F1>。 按 <Esc> 可以清除帮助窗口。

19. 选择“**SNMP Manager Table**”（**SNMP 管理器表**）菜单选项之一。
20. 按 <Esc> 以退出“**SNMP Manager Table**”（**SNMP 管理器表**）菜单。

   出现信息框，提示您更新数据库。

21. 选择“**Yes**”（**是**）。

   出现“**TCP/IP Protocol Configuration**”（**TCP/IP 协议配置**）菜单。

22. 按两次 <Esc> 以退出“**TCP/IP Protocol Configuration**”（**TCP/IP 协议配置**）菜单。

   出现“**Internetworking Configuration**”（**联网配置**）菜单。

23. 重新启用您的系统以使配置更改生效。

设置 CIM

CIM 仅适用于支持的 Microsoft Windows 操作系统。

在您的 Managed System 上设置 CIM

本小节提供在运行支持的 Windows 操作系统的 Managed System 上设置 CIM 的步骤。

创建域管理员的建议

尽管以下步骤描述如何将本地管理员添加至支持的 Windows 操作系统，但 Dell 建议您在 IT Assistant 所管理的每个系统上创建域管理员，而不是创建用户。 创建域用户帐户还将有助于防止因在输入的查找范围内发现 IT Assistant 登录系统失败而锁定帐户。 例如，查找范围 192.168.0.* 会导致试图登录到所有 253 个系统。 如果传递至任何一个 Managed System 的凭证未验证，则帐户将锁定。 另外，Windows XP 中增强的安全性要求 IT Assistant 系统和客户必须位于相同的域中。 Windows XP 还要求用户名具有非空密码。 有关创建 Windows 域用户帐户的详情，请参阅 Microsoft 说明文件。

注：IT Assistant 需要在 Managed System 上建立的具有管理员权限的 CIM 用户名和密码。 如果您正在使用域用户，确保在用户名字段中指定正确的域。 用户名必须始终使用域来限定,或使用 **localhost**（如果没有域）。 格式可以是**域\用户**或 **localhost\用户**。

注：CIM 查找需要正确的用户 ID 和密码凭证。 无法在为 CIM 查找配置的子网上提供正确的凭证可能会导致帐户锁定。

对于运行 Windows 2000 的 Managed System

注：默认情况下，WMI 内核已随 Windows 2000 一起安装。

1. 单击**“Start”（开始）→“Settings”（设置）→“Control Panel”（控制面板）→“Administrative Tools”（管理工具）→“Computer Management”（计算机管理）**。
2. 在**“Computer Management (Local)”（计算机管理 [本地]）**树中，展开**“Local Users and Groups”（本地用户和组）**分支，并单击**“Users”（用户）**文件夹。
3. 在菜单栏上，单击**“Actions”（操作）**，然后单击**“New User”（新用户）**。
   a. 在**“New User”（新用户）**对话框中，在必填信息字段中填入用户名和密码，例如 CIMUser 和 DELL。 （这些只是用于说明的示例，您应根据企业设置相应的用户名和密码。）
   b. 确保清除（取消选择）**“User must change password at next logon”（用户下次登录时须更改密码）**复选框。
   c. 单击**“Create”（创建）**。
4. 在**“Computer Management”（计算机管理）**对话框的右窗格中，双击 **CIMUser**。

   您可能必须滚动列表以定位 **CIMUser**。
5. 在**“CIMUser Properties”（CIMUser 属性）**对话框中，单击**“Member Of”（成员）**选项卡。
6. 单击**“Add”（添加）**。
7. 单击**“Administrators”（管理员）**，单击**“Add”（添加）**，然后单击**“OK”（确定）**。
8. 再次单击**“OK”（确定）**，然后关闭**“Computer Management”（计算机管理）**对话框。
9. 安装 Client Instrumentation 7.*x* 或 Server Administrator，视系统是客户机还是服务器而定。
10. 重新启动系统。

对于运行 Windows XP Professional 的 Managed System

如上所述，Windows XP 中增强的安全性要求 IT Assistant 系统和客户必须位于相同的域中。 另外，设置自己的用户名和密码时，请勿指定空密码。

以下步骤详细描述如何创建本地用户。 Dell 强烈建议您创建具有管理权限的域用户，这样一来，您不需手动添加用户至每个客户机。 这将简化在 IT Assistant 中创建查找范围的过程。

1. 单击**“Start”（开始）→“Settings”（设置）→“Control Panel”（控制面板）→“Administrative Tools”（管理工具）→“Computer Management”（计算机管理）**。
2. 在**“Computer Management (Local)”（计算机管理 [本地]）**树中，展开**“Local Users”（本地用户）和“Groups”（组）**分支，并单击**“Users”（用户）**文件夹。
3. 在菜单栏上，单击**“Actions”（操作）**，然后单击**“New User”（新用户）**。
   a. 在**“New User”（新用户）**对话框中，在必填信息字段中填入用户名 CIMUser 和密码 DELL。

b. 确保清除（取消选择）**“User must change password at next logon”（用户下次登录时须更改密码）**复选框。

c. 单击**“Create”（创建）**。

4. 在**“Computer Management”（计算机管理）**对话框的右窗格中，双击 **CIMUser**。

您可能必须滚动列表以定位 **CIMUser**。

5. 在**“CIMUser Properties”（CIMUser 属性）**对话框中，单击**“Member Of”（成员）**选项卡。
6. 单击**“Add”（添加）**。
7. 单击**“Administrators”（管理员）**，单击**“Add”（添加）**，然后单击**“OK”（确定）**。
8. 再次单击**“OK”（确定）**，然后关闭**“Computer Management”（计算机管理）**对话框。

注： Windows XP Professional 仅支持用于 IT Assistant 客户机系统。

9. 安装 Client Instrumentation 7.*x* 或 Server Administrator，视系统是客户机还是服务器而定。
10. 重新启动系统。

对于运行 Windows Server 2003 的 Managed System

1. 单击**“Start”（开始）**→**“Settings”（设置）**→**“Control Panel”（控制面板）**→**“Administrative Tools”（管理工具）**→**“Computer Management”（计算机管理）**。
2. 在**“Computer Management (Local)”（计算机管理 [本地]）**树中，展开**“Local Users and Groups”**（本地用户和组）分支，并单击**“Users”（用户）**文件夹。
3. 在菜单栏上，单击**“Actions”（操作）**，然后单击**“New User”（新用户）**。

a. 在**“New User”（新用户）**对话框中，在必填信息字段中填入用户名 CIMUser 和密码 DELL。

b. 确保清除（取消选择）**“User must change password at next logon”（用户下次登录时须更改密码）**复选框。

c. 单击**“Create”（创建）**。

4. 在**“Computer Management”（计算机管理）**对话框的右窗格中，双击 **CIMUser**。

您可能必须滚动列表以定位 **CIMUser**。

5. 在**“CIMUser Properties”（CIMUser 属性）**对话框中，单击**“Member Of”（成员）**选项卡。
6. 单击**“Add”（添加）**。
7. 单击**“Administrators”（管理员）**，单击**“Add”（添加）**，然后单击**“OK”（确定）**。
8. 再次单击**“OK”（确定）**，然后关闭**“Computer Management”（计算机管理）**对话框。
9. 安装 Client Instrumentation 7.*x* 或 Server Administrator，视系统是客户机还是服务器而定。
10. 重新启动系统。

返回目录页

返回目录页

IT Assistant 简介

Dell OpenManage™ IT Assistant 7.2 版用户指南

Dell OpenManage™ IT Assistant 提供了一个用于监测和管理局域网 (LAN) 或广域网 (WAN) 上系统的集中访问点。 通过允许管理员对企业的全面查看，IT Assistant 能够增加系统运行时间、自动化处理重复任务并防止中断重要的业务操作。

简化系统管理

通过使用 IT Assistant，您能够：

- 标识要远程管理的系统组。
- 集中查看所有系统，为您提供了集中管理这些系统的起始点。
- 创建警报筛选器和操作，在系统运行时间受到影响时自动通知您。
- 创建自定义的企业范围报告，提供了各系统的详情资源清册。
- 创建自定义任务，使您能够在整个企业中协调配置管理，包括软件更新、设备控制（关机/唤醒）和命令行执行。

标识远程管理的系统组

IT Assistant 执行基本的查找和状况轮询，从而使系统管理员能够在网络上按照主机名、IP 地址或 IP 子网范围来识别系统和设备。 在状况轮询期间，IT Assistant 查询系统及其组件的运行状况或*状况*。 在查找和状况轮询期间收集的信息显示在管理控制台中，并写入 IT Assistant 数据库。 默认数据库为 Microsoft® Database Engine (MSDE) 2000。 需要功能更强大的数据库的用户可以使用 Microsoft SQL Server。

合并所有系统的视图

IT Assistant 可以让系统管理员从管理控制台中对 Managed System 执行操作。 通过使用 IT Assistant，可以创建适用于单个系统或组中各个系统的任务，创建动态系统组以便于管理，以及在任何系统上执行资源清册。 此外，IT Assistant 为以下 Dell™ 系统管理应用程序和设备提供了一个统一的起始点：Dell OpenManage Server Administrator、 Dell OpenManage Array Manager、Remote Access Console、Dell PowerConnect™ 和数字化键盘/视频/鼠标 (KVM)。

创建警报筛选器和操作

可以使用 IT Assistant 创建警报*筛选器*隔离系统管理员特别关心的警报。 系统管理员可以随后创建相应的警报*措施*，当符合用于定义警报筛选器的条件时触发该操作。 例如，IT Assistant 可以在服务器风扇处于警告或严重状态时对系统管理员发出警报。 通过创建具有相应电子邮件操作的筛选器，在风扇出现定义的状况时会给管理员发出电子邮件通知。 管理员可以随后针对通知采取行动，如有必要，使用 IT Assistant 关闭系统，或启动 Server Administrator 对问题进行故障排除。

创建自定义查找和资源清册报告

通过使用 IT Assistant 的报告向导，可以为整个企业的任何设备或组创建自定义报告。 这些报告可以包含基于多种属性选择的设备资源清册信息。 例如，可以创建报告，其中列出了组中所有服务器的各个设备卡的详细情况，包括总线速度和宽度、制造商和插槽长度和/或号码。 IT Assistant 还提供了一系列预先设置好格式的报告，这些报告收集了企业中的常用信息。

创建任务实现从中央控制台进行配置管理

IT Assistant 还使用户能够从单一的控制台在整个企业中执行常用的配置管理任务。 通过使用 IT Assistant 基于向导的用户界面 (UI) 设置简单的任务，可以在所管理组的任何系统上执行设备控制任务（关机/唤醒）、软件更新或运行命令行任务。 IT Assistant 使您能够将 Dell Update Packages 和系统更新集载入中央存储库，然后对企业中的服务器运行一致性检查。系统管理员可以随后指示 IT Assistant 立即执行更新或根据规定的计划执行更新。

注：要执行软件更新，必须在目标设备上安装相应的代理程序软件。 有关代理程序的详情，请参阅“要监测的系统上的代理程序”。

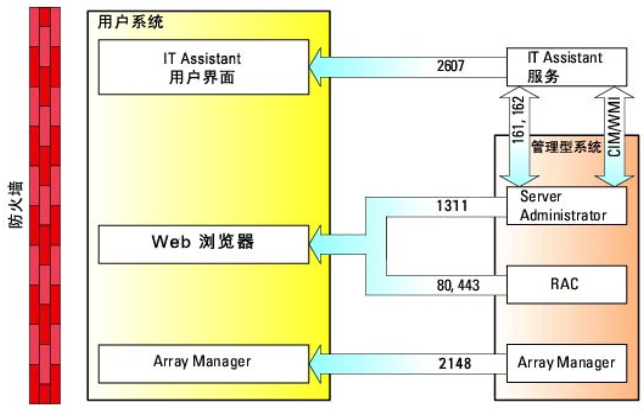
了解 IT Assistant 的组件

要了解此文档的其它章节，您必须了解 IT Assistant 的以下组件：

- IT Assistant UI
- IT Assistant 服务层（网络监测服务、连接服务和数据库）
- Managed System

IT Assistant 用户界面以图形化用户界面的形式显示 IT Assistant 服务层收集的信息。 此信息展示所管理组中各系统的整体运行状况和配置详情。 IT Assistant 监测的所管理组中的系统被称为 *Managed System*；运行 IT Assistant 用户界面的系统通常称为*网络 Management Station*。

图 1-1. IT Assistant 用户界面、服务系统和 Managed System



注：图 1-1 中的数字是 IT Assistant 用来与 Managed System 通信的端口号。

用户界面

从 IT Assistant UI，用户可以执行各种配置和管理任务，比如指定要查找的系统、创建警报筛选器和操作以及系统关机后再开机。

IT Assistant 用户界面基于 Sun Java 技术。 远程访问是通过 Web 浏览器（Microsoft Windows® 上的 Internet Explorer，以及 Red Hat® Enterprise Linux 系统上的 Mozilla 或 Firefox）或终端服务会话来实现的。

IT Assistant 服务

IT Assistant 服务层作为标准安装的一部分安装。 从技术上说，服务层由网络监测服务、连接服务和数据库组成。 在高度自定义的安装中，一些用户可以将数据库安装在独立的系统上。如果您正在 Managed System 上配置 SNMP 代理程序，SNMP 服务的陷阱目标必须指向安装 IT Assistant 的主机名或 IP 地址。

术语：Managed System 和 IT Assistant 系统

对于 IT Assistant 而言，*Managed System* 是指安装了支持的工具或代理程序以允许查找和轮询系统状况的系统。 IT Assistant 通过允许管理员从一个管理控制台监测多个 Managed System 来简化它们的系统管理。

在本指南中，术语 *IT Assistant 系统*或*网络 Management Station* 用于标识装有 IT Assistant 软件的系统。

集成的功能

本机安装

Dell OpenManage 系统管理软件产品使用操作系统的本机安装过程进行安装。

用户界面设计和联机帮助

IT Assistant 用户界面 (UI) 包括用于执行多种标准任务的基于向导的对话框。 IT Assistant 菜单栏选项已更改，因此以前的用户需要花一点时间来熟悉新布局。

现在提供了全面的联机帮助，既可以从 IT Assistant 窗口右上角的**“Help”（帮助）**链接访问，也可以从各个对话框和向导的上下文特定**“Help”（帮助）**按钮访问。

该用户界面完全基于 Web，使用 Sun Microsystems Java 技术，并且支持 Linux 系统。

DMI 支持

IT Assistant 不再支持桌面管理接口 (DMI) 协议。 因此，使用 Dell OpenManage Server Agent 4.5.1（和更低版本）和 Dell OpenManage Client Instrumentation 6.0（和更低版本）运行 DMI 的系统不会被 IT Assistant 查找。

新拓朴视图

在用户界面中，可以选择**“Views”（视图）→ “Topology”（拓扑）**查看网络中设备的图形化表示。 要双击图标查看组时，您可以下移层次结构。 此外，可以将光标移到各图标上显示详细的设备信息。 还可以在此视图中的设备上执行任务，比如应用程序启动、刷新资源清册和状况，以及故障排除。

动态组

可以创建动态设备组帮助您更有效地管理和监测。 有关详情，请参阅 IT Assistant 联机帮助中的组配置主题。

注：可以在其它模块中重新使用在某个 IT Assistant 模块中创建的设备选择查询。 例如，在搜索设备模块中创建的查询在您创建或编辑报告、警报筛选器或任务时还可以使用。

应用程序启动

IT Assistant 为以下 Dell 系统管理应用程序提供了一个统一的起始点：Server Administrator、Array Manager、Remote Access Console、PowerConnect 和数字化 KVM（键盘/视频/键盘）。 有关详情，请参阅 IT Assistant 联机帮助中的应用程序启动主题。

注：网络地址转换 (NAT) 不是 IT Assistant 上支持的配置。 因此，即使 IT Assistant 能够成功找到 Managed System，应用程序启动也不能和 NAT 一起使用。 应使用 IT Assistant 只连接到找到系统的 IP 地址。 系统上其它可用的 IP 地址无法由 IT Assistant 访问。 在许多实现中，比如服务器场或负载平衡器实现中，系统会位于 NAT 后面。 在这种情况下，IT Assistant 将无法连接到这些系统上运行的 Server Administrator。

报告

IT Assistant 提供了一种可自定义的报告功能，从 Microsoft Data Engine (MSDE) 或 SQL Server 数据库收集数据。 报告结果基于上次查找和/或资源清册收集的数据。

报告界面向导旨在帮助您选择 IT Assistant 数据库中的实际字段。 可以创建包含以下信息的报告：

- IT Assistant 管理的硬件设备的详情，包括系统、交换机和存储设备
- BIOS、固件和驱动程序版本
- 其它资产或物主成本详情

还可以指定输出格式，比如 HTML、XML 或逗号分隔的值 (CSV)。 CSV 通常用于电子表格工具中，比如 Microsoft Excel。 IT Assistant 会保存报告定义以便日后使用和检索。

要使用 IT Assistant 报告向导，选择**“Views”（视图）→“Reports”（报告）**。 使用报告向导的完整功能和步骤说明可在 IT Assistant 联机帮助中获得。

软件更新

IT Assistant 允许将 Dell 更新软件包和系统更新集载入中央存储库，然后将软件包与企业系统上当前运行软件的版本进行比较。 随后可以决定是否更新那些不一致的系统，既可以立即更新也可以按照计划运行。

还可以按照操作系统、系统类型、组件名和软件类型自定义软件包信息的视图。

要使用软件更新功能，选择**“Manage”（管理）→“Software Updates”（软件更新）**。 有关详情，请参阅 IT Assistant 联机帮助中的软件更新主题。

管理任务

IT Assistant 提供一种更新任务功能，允许在企业中的所有系统上设置和远程运行某些任务，包括设备控制（关机和唤醒）、软件更新和命令行执行。

要使用该任务功能，选择**“Manage”（管理）→“Tasks”（任务）**。 有关详情，请参阅 IT Assistant 联机帮助中的任务主题。

故障排除工具

可以从**“Tools”（工具）→“Troubleshooting Tool”（故障排除工具）**使用图形化故障排除工具来诊断并解决查找和配置问题，包括简单网络管理协议 (SNMP) 和公用信息模型 (CIM) 问题。 还可以使用此工具检测设备和电子邮件连接。

有关详情，请参阅 IT Assistant 联机帮助。

用户身份验证

对于 IT Assistant 的以前用户，IT Assistant 现在使用基于操作系统或域的身份验证；IT Assistant 6.*x* 读/写密码不再使用。 有关 Active Directory 架构以及如何配置以用于 IT Assistant 的信息，包括如何安装所需的管理单元，请参阅*《Dell OpenManage 安装和安全性用户指南》*。

增强的资源清册

IT Assistant 会收集有关软件和固件版本的资源清册信息，以及与设备有关的信息，比如内存、处理器、电源设备、PCI 卡和嵌入式设备以及存储。 有关 IT Assistant 收集并存储在数据库中的资源清册信息的详情，请参阅联机帮助中的“添加报告 — 使用 IT Assistant 报告系统”。 有关配置资源清册设置，请参阅联机帮助中的“资源清册轮询设置 — 配置 IT Assistant 执行资源清册”。

单一登录

支持 Windows 系统上的“单一登录”。 使用“单一登录”通过单击桌面上的 **IT Assistant** 图标跳过登录页并访问 IT Assistant。 桌面图标会查询注册表以查看 Internet Explorer 中是否启用了借助当前用户名和密码进行自动登录选项。 如果启用了此选项，就会执行单一登录；否则将会显示正常的登录页。 有关如何设置这些选项的详情，请参阅“单一登录”。

用户首选项

用户首选项独立于用户权限。 可以使用此功能自定义设备组视图。 可以从 **“Tools”（工具）→ “User Preferences”（用户首选项）** 访问此功能。 有关如何使用此功能的详情，请参阅联机帮助中的“用户首选项 — 自定义 IT Assistant 用户界面”。

可能需要的其它信息

本*用户指南*旨在显示 IT Assistant 的高级视图。 本说明文件中并没有显示所有配置和功能。 不过，IT Assistant 用户界面中的联机帮助对每个功能都有全面的说明。

此外，以下资源还可以从 Dell 支持网站 **support.dell.com** 或说明文件 CD 上找到：

- *《Dell OpenManage Server Administrator 用户指南》*介绍了构成 Dell 一对一服务器管理工具主要套件的功能、安装和服务。
- *《Dell OpenManage Server Administrator SNMP 参考指南》*介绍了 SNMP 管理信息库 (MIB)。 SNMP MIB 定义了扩展标准 MIB 的变量，以涵盖系统管理代理的各项功能。
- *《Dell OpenManage Server Administrator CIM 参考指南》*介绍了 CIM 提供程序，它是标准管理对象格式 (MOF) 文件的扩展。 CIM 提供程序 MOF 记录了支持的管理对象类。
- *《Dell OpenManage 安装和安全性用户指南》*介绍了如何在系统上安装 Dell OpenManage Systems Management Software，以及如何为 IT Assistant 配置 Active Directory 并扩展架构。

可以在两个位置找到 IT Assistant 联机帮助：通过单击浏览器窗口右上角的 **“Help”（帮助）** 链接，或通过单击所用对话框或向导中的 **“Help”（帮助）** 按钮。

返回目录页

返回目录页

计划 IT Assistant 安装

Dell OpenManage™ IT Assistant 7.2 版用户指南

在安装 Dell OpenManage™ IT Assistant 之前进行计划是很重要的。 根据公司的网络管理目标，可能想将 IT Assistant 主要用作查找和状况轮询工具，快速扫描网络检索 Managed System 的信息。 在另一方面，可能想要 IT Assistant 只对特定 Managed System 的问题进行接收并给支持人员转发警报。 或者也许需要这两种功能组合。

安装之前的决策

确定网络大小和网络管理目标之后，必须执行特定于网络管理目标的配置决策。 如果您的网络建立得很好，并且已经正确定义了 IT Assistant 管理计划，则其中的许多决策点可能已经解决。 安装前计划包括进行以下选择：

- 事件过滤和通知策略
- 用于存储 IT Assistant 数据的数据库
- 硬件配置
- 操作系统
- 系统管理协议
- Managed System 的代理程序

注：本文档假定您的系统通过 TCP/IP 网络连接，而不管网络的复杂性或者您是否已经使用任何系统管理应用程序。 此外，也不管系统类型以及您网络上存在的设备。 请参阅“安装、卸载和升级 IT Assistant”了解所有安装、卸载和升级程序。

主要计划问题

不同企业具有不同的系统类型和网络管理目标。 回答以下问题可以更好地准备 IT Assistant 的安装，以支持您公司网络管理目标。 阅读本节之后，请在安装前参阅表 2-4。

1. 安装 IT Assistant 的基本硬件和操作系统要求是什么？ 我的企业是否符合这些要求？
2. 在安装 IT Assistant 时，在所支持的操作系统中选择特定操作系统是否有任何原因？
3. 在安装 IT Assistant 时，是否存在选择特定硬件配置的任何原因？
4. 是否要使用默认安装数据库 (MSDE) 或者是否应安装 Microsoft® SQL Server 数据库？
   - 要查找或管理多少系统？
   - 希望网络上的事件通信量的密度如何？
5. 应计划安装或启用哪些系统管理协议？
   - 要管理什么类型的系统？
   - 目前在我的 Managed System 上安装了什么代理程序和工具？
   - 最终要在我的 Managed System 上运行什么代理程序？
   - 这些代理程序需要或支持什么协议？
6. 如果正在子网上使用多个系统管理协议，应如何组织 Managed System 的 IP 地址？

选择操作系统

您可以在运行表 2-1 中其中一个操作系统的任何系统上安装 IT Assistant。

表 2-1. IT Assistant 最低支持的操作系统要求

小型企业（最多 500 个 Managed System）	大型企业（500 个以上的 Managed System）
Microsoft Windows® XP Professional，带有 SP2	Windows Server 2003，带有 SP1
Windows 2000，带有 SP4	Windows 2000，带有 SP4
Windows Server™ 2003，带有 SP1	Windows 2000，带有 SP4

注：IT Assistant 在 Microsoft Windows Small Business Server 2003 上不受支持。

注：在安装和配置终端服务或远程桌面时，请参阅 Microsoft 操作系统说明文件。

注：IT Assistant 无法安装在运行 Red Hat® Enterprise Linux 操作系统的 Dell™ 服务器上。 不过这些服务器可以通过支持的浏览器（Mozilla 1.7.3 和更高版本，以及 Firefox 1.0.1 或更高版本）启动 IT Assistant。

选择硬件配置

选择的硬件配置必须符合或超过 IT Assistant 的推荐配置。 视您的特定 IT Assistant 部署和您的网络环境而定，建议您超过处理器速度、内存大小和硬盘空间的建议配置。 例如，如果是以下情况，则最好超过或选择最高建议配置：

- 预计具有大量的 Managed System 警报通信量
- 具有配置了警报措施的复杂警报过滤器
- 经常执行查找、资源清册和状况轮询
- 运行配置为最大性能的 Microsoft SQL Server

表 2-2 中显示了 IT Assistant 的最低建议硬件配置。

表 2-2. IT Assistant 的最低建议硬件配置（按企业规模）

组件	小型企业（最多 500 个Managed System ）	大型企业（500 个以上的Managed System ）
处理器	1 个处理器（最低 1.8 GHz）	2 到 4 个处理器（最低 800 MHz）
内存	512 MB	1-2 GB
磁盘空间	至少 1 GB	最多可达 5 GB

注：如果导入多个更新软件包，磁盘空间的数量可能需要增加。

选择 MSDE 默认数据库或 SQL 2000 Server

通常，预计管理的系统数以及预计从 Managed System 中获得的警报数决定与 IT Assistant 配合使用的数据库。 如果准备管理 500 个以下的系统，IT Assistant 配备的兼容 SQL Server 的默认数据库 Microsoft Data Engine (MSDE) 2000 很可能是一个比较合适的数据存储库。 但是，如果您准备管理 500 个或更多的系统和/或每秒接收多个警报，应将 Microsoft SQL Server 2000 或更高版本用作您的数据库。 此外，如果准备执行频繁的查找或状况轮询，则相对于 MSDE 2000，SQL Server 2000 提供的更高性能将非常有用。

注：您可以配置 IT Assistant 版本 6.3 和更高版本，以便使用在专用远程服务器上而不是 IT Assistant 系统上运行的 Microsoft SQL Server。 请参阅 **www.dell.com/openmanage** 上相应的标题为“远程 Microsoft SQL Server 与 IT Assistant 配合使用的逐步说明”的 Dell 白皮书。

电子邮件通知功能

电子邮件警报措施在系统管理员不想使用 IT Assistant 用户界面以可视方式监测 Managed System 状态的环境中非常有用。 通过将电子邮件警报措施与警报措施筛选器相结合，在特定系统将警报发送给 IT Assistant 网络 Management Station 时，管理员可以确定将以电子方式得到通知的人员。 此人员然后可以选择为该系统采取适当的纠正措施。 通过在警报筛选器中配置相应的警报措施，将无需 IT Assistant 持续监测系统状态，因为设置了每当满足事件条件时将会发生电子邮件通知。

确定系统管理协议

在计划 IT Assistant 安装中，其中一个最重要的决策是确定将与 IT Assistant 一起使用的协议。 通常，通过要监测的系统以及它们所支持的相应代理程序协议来确定要选择的协议。 如果要监测的系统具有使用简单网络管理协议 (SNMP) 或公用信息模型 (CIM) 协议的代理程序，这些也必须在 IT Assistant 中配置。

支持的协议

IT Assistant 支持两种系统管理协议：SNMP 和 CIM。 这些协议允许在您网络上的 IT Assistant 网络 Management Station 和 Managed System 之间进行通信。 要在 IT Assistant 和每个 Managed System 之间成功进行通信，必须在您要管理的每个系统上安装代理程序（工具）。 对于服务器管理，强烈建议您启用并配置这两个协议。

注：如果在 Managed System 上没有正确配置相应的协议，IT Assistant 将不能正确区分系统，故而会限制对这些系统的管理。

SNMP

为了成功执行 IT Assistant 安装，必须安装并启用操作系统 SNMP 服务。

CIM

CIM 用于管理客户机和服务器系统。 也可以用于监测网络上不允许 SNMP 管理的 Server Instrumentation。

影响协议选择的因素

影响协议选择的两个因素：

- 要监测的系统
- 要监测的系统上的代理程序

要监测的系统

您的网络可能由客户机和服务器系统的组合组成，包括便携式计算机、台式机、工作站和独立服务器，比如打印和文件服务器、服务器模块（或刀片式）、群集服务器或机架上密集分布的数以百计的服务器。 在计划 IT Assistant 安装时，您将调查这些系统以及计划添加至网络的任何系统，并确定要监测的系统。 在此评估期间，您不仅会查看客户机和服务器系统数，而且查看在这些系统上安装的任何系统管理代理程序和操作系统。 以下部分讨论您可能需要在 IT Assistant 中配置的代理程序和相应的协议。 要成功管理您的网络，需在 IT Assistant 内正确配置这些协议。

要监测的系统上的代理程序

在 Managed System 上运行的代理程序可能支持特定的系统管理协议。 如果要保留已在这些系统上安装的代理程序，必须继续使用各自的协议对它们进行管理。 如果特定代理程序使用的协议是旧协议，在大多数情况下，您可以选择使用支持新协议的代理程序更换或升级这些代理程序。 表 2-3 列出了可能在 Dell 客户机和服务器上安装的众多代理程序和工具。 只要在 IT Assistant 中启用了相应的协议，便可以在您的网络上查找和管理这些系统。

*代理程序*是一个适用于系统管理设备软件组件的常规术语。 下表介绍了 IT Assistant 支持的管理和警报代理程序。 各代理程序的支持级别各不相同。 例如，IT Assistant 可以自动查找、显示、接收来自 Dell OpenManage Server Administrator 所管理系统的警报并可在这些系统上执行操作，但是 IT Assistant 只能接收来自某些存储设备代理的警报。

注： IT Assistant 不再支持桌面管理接口 (DMI) 协议。 因此，使用 Dell OpenManage Server Agent 4.5.1（和更低版本）和 OMCI 6.0（和更低版本）运行 DMI 的系统不会被 IT Assistant 查找到。

表 2-3. IT Assistant 支持的代理程序

设备	支持的版本	可自动查找	报警
Dell PowerEdge™ 代理程序*			
Server Administrator	1.0-2.2	是	是
Server Agent	4.2-4.5	是	是
Array Manager	2.5-3.7	是	是
DRAC 4	1.0-1.30	是	是
DRAC III, DRAC III/XT	1.0-3.50	是	是
ERA, ERA/O	1.0-3.50	是	是
ERA/MC	1.0-3.50	是	是
PowerEdge 1655MC/1855MC 集成交换机	暂无	是	是
* IT Assistant 需要 Server Administrator 2.0 或更高版本以进行远程软件更新。			
Dell PowerVault™ 代理程序			
PowerVault 701N	暂无	是	是
PowerVault 705N	暂无	是	是
PowerVault 735N	暂无	是	是
PowerVault 750N	暂无	是	是
PowerVault 755N	暂无	是	是
PowerVault 715N	暂无	是	是
PowerVault 725N	暂无	是	是
PowerVault 770N	暂无	是	是
PowerVault 775N	暂无	是	是
Adaptec CIO	4.02	否	是
IT Assistant 支持的 Dell PowerConnect™ 代理程序和 PowerConnect 固件版本			
PowerConnect 3024	5.2.5.*x*, 6.0.4.*x*, 6.1.2.*x*	是	是
PowerConnect 3048	5.2.5.*x*, 6.0.4.*x*, 6.1.2.*x*	是	是
PowerConnect 3248	1.0.1.*x*, 2.0.0.*x*, 2.1.0.*x*	是	是
PowerConnect 3324	1.0.0.*x*, 1.1.0.*x*, 1.2.0.*x*	是	是
PowerConnect 3348	1.0.0.*x*, 1.1.0.*x*, 1.2.0.*x*	是	是
PowerConnect 5012	5.2.5.*x*, 6.0.4.*x*, 6.1.2.*x*	是	是
PowerConnect 5212	1.0.0.*x*, 3.1.0.*x*	是	是
PowerConnect 5224	1.0.1.*x*, 2.0.0.*x*, 2.1.0.*x, 3.1.0*	是	是
PowerConnect 5316M	1.0.0.*x*	是	是
PowerConnect 5324	1.0.1.*x*	是	是
PowerConnect 6024	1.0.2.*x*	是	是
PowerConnect 6024F	1.0.2.*x*	是	是
Digital KVM 代理程序			
2161 DS	暂无	是	是
网络适配器代理程序			
Intel® PRO	暂无	否	是
Broadcom	暂无	否	是
ASF	1	否	是
客户代理程序			
Dell OpenManage Client Instrumentation	7.*x*	是	是

安装前决策摘要

本节列出了在安装和使用 IT Assistant 在网络上管理系统之前必须考虑的主要因素。 表 2-4 汇总了前面部分提出的问题、可用选项和操作，以及可以在本指南中找到的执行该操作相应过程的章节。

表 2-4. 安装前问题、选项和操作

问题	选项/操作	选项/操作	下一步
在安装 IT Assistant 时，在所支持的操作系统中选择特定操作系统是否有任何原因？	确保您所安装的 IT Assistant 的组件支持该操作系统。	对于大型网络，请在一个基于服务器的操作系统上安装 IT Assistant。	请参阅 Dell Support 站点 **support.dell.com** 或 *Dell Systems Management Consoles* CD 上最新的 IT Assistant **readme.txt**。
在安装 IT Assistant 时，是否存在选择特定硬件配置的任何原因？	确保硬件配置符合或超过将在系统上安装的 IT Assistant 组件的建议要求。		
我是否要使用默认安装数据库 (MSDE) 或者是否应安装 Microsoft SQL Server 数据库？	通常，如果要管理的系统不足 500 个，使用 MSDE 就足够了。 但是，如果存在大量的事件通信量或需要更高的性能，则需选择 SQL Server。	对于需要较高处理器速度和/或额外处理器、更多内存和更大硬盘空间以确保 IT Assistant 性能的环境，选择 SQL 数据库和大量的事件通信量是不错的选择。	
应计划安装或启用哪些系统管理协议？	调查要在您的 Managed System 上运行的代理程序，并找出它们所支持的协议；考虑正在管理的系统类型。		请参阅 “安装、卸载和升级 IT Assistant”和 “配置 IT Assistant 监视系统” 。
如果正在子网上使用多个系统管理协议，应如何组织 Managed System 的 IP 地址？	只要可能，将使用相同系统管理协议的系统分组为连接的子网。 这种策略会增加在创建 IT Assistant 查找范围期间的可管理性。		
我是否将在 IT Assistant 中使用基于角色的访问分配用户级别？	IT Assistant 支持标准的基于角色的访问级别。 支持的三种级别有 User（用户）、Power User（高级用户）和 Administrator（管理员）。	在企业中使用这些访问角色可以进一步加强安全性。	请参阅 “确保安全 Dell OpenManage IT Assistant 安装”

返回目录页

返回目录页

安装、卸载和升级 IT Assistant

Dell OpenManage™ IT Assistant 7.2 版用户指南

安装要求

安装 Dell OpenManage™ IT Assistant 时，一定要查看 *Dell Systems Management Consoles* CD 或 Dell™ 支持网站 **support.dell.com** 上最新的 **readme.txt** 文件。 此文件定义 IT Assistant 最新的支持操作系统和硬件要求。 除了满足这些要求外，还有其它 IT Assistant 安装要求以及将由 IT Assistant 管理的系统的要求。 请参阅 “规划 IT Assistant 安装”了解有关详情。

TCP/IP 协议支持

为使 IT Assistant 正常工作，您的网络必须支持 TCP/IP 协议。

设置或启用代理程序通信的协议

安装 IT Assistant 前，必须安装操作系统的简单网络管理协议 (SNMP) 服务。 此外，为确保系统对于 IT Assistant 查找和资源清册运作可见，应保证 Managed System 上的代理程序和设备可以通过公用信息模型 (CIM) 协议访问。

注：默认情况下，会在 Microsoft® Windows® 2000、Windows Server™ 2003 和 Windows XP Professional 上安装 CIM。

在 IT Assistant 系统上安装 SNMP

必须在 IT Assistant 系统上安装和运行 SNMP 服务。 SNMP（或 CIM）也必须安装在要查找和管理的系统上。

注：以下示例使用 Windows 2000 Advanced Server。

1. 单击 **“Start”（开始）**按钮，指向 **“Settings”（设置）**，并双击 **“Control Panel”（控制面板）**。
2. 双击 **“Add/Remove Programs”（添加/删除程序）**图标。

   这将启动 **“Add/Remove Programs”（添加/删除程序）**窗口。
3. 单击左菜单栏上的 **“Add/Remove Windows Components”（添加/删除 Windows 组件）**图标。

   这将启动 **“Windows Components Wizard”（Windows 组件向导）**窗口。
4. 在 **“Components”（组件）**下面的 **“Windows Components Wizard”（Windows 组件向导）**窗口中，滚动至 **“Management and Monitoring Tools”（管理和监视工具）**。
5. 选择 **“Management and Monitoring Tools”（管理和监视工具）**，单击 **“Details”（详细情况）**，选择并复选 **“Simple Network Management Protocol”（简单网络管理协议）**，并单击 **“OK”（确定）**。

6. 单击“**Windows Components Wizard**”（**Windows 组件向导**）窗口中的“**Next**”（**下一步**）。

   “**Windows Components Wizard**”（**Windows 组件向导**）将安装 SNMP。

7. 一旦完成安装，单击“**Finish**”（**完成**）。
8. 关闭“**Add/Remove Programs**”（**添加/删除程序**）窗口。

   SNMP 现已安装在您的系统上。

仅在运行 Windows 2000、Windows XP Professional 或 Windows Server 2003 的系统上安装 IT Assistant。 有关如何在运行 Microsoft Windows、Red Hat® Linux 或 Novell® NetWare® 操作系统的 Managed System 上安装并配置 SNMP 的信息，请参阅“配置协议将信息发送给 IT Assistant”。

启用 CIM

默认情况下，在 Windows 2000、Windows Server 2003 和 Windows XP Professional 上会安装 CIM/WMI (Windows Management Instrumentation) 服务。 CIM 查找需要正确的用户 ID 和密码凭据。 无法在为 CIM 查找配置的子网上提供正确的凭证可能会导致帐户锁定。

有关如何设置 CIM 的示例，请参阅“配置协议将信息发送给 IT Assistant”。

设置 RBAC 用户信息

IT Assistant 支持基于角色的访问控制 (RBAC) 以定义每个用户可以执行的具体操作。 不过，IT Assistant 安装过程不需要这些用户角色在安装前就已设定好。 要在安装 IT Assistant 前/后设置 RBAC 用户，请参阅“确保安全 Dell OpenManage IT Assistant 安装”。

安装 IT Assistant

如果是第一次安装 IT Assistant，应遵循此处显示的步骤。 如果是从以前版本升级，请参阅“从以前版本的 IT Assistant 升级”。

您可以从 *Dell Systems Management Consoles* CD 安装 IT Assistant，或从 Dell 支持网站 **support.dell.com** 下载并安装 IT Assistant。 Dell OpenManage Management Station 安装程序用于安装 IT Assistant 和其它 Dell OpenManage 软件。 要安装 IT Assistant 以外的产品，请参阅特定于该产品的安装说明。

要第一次安装 IT Assistant：

1. 将 *Dell Systems Management Consoles* CD 放入驱动器中。

   如果安装程序没有自动启动，应浏览到 **/windows** 目录并单击 **setup.exe**。 **Dell OpenManage Management Station** 屏幕将会显示。

   安装程序会自动扫描系统查找任何相关性，比如是否安装了 SNMP 或具有支持的数据库应用程序。 如果找到相关性，会显示信息窗口并提示您安装所需的软件包。

2. 如果没有找到相关性，则单击“**Install, Modify, Repair or Remove Management Station**”（**安装、修改、修复或删除 Management Station**）。

   将会显示 Dell OpenManage Management Station 安装向导。 单击“**Next**”（**下一步**）。

3. 如果同意 Dell Inc. 软件许可协议，则单击“**Next**”（**下一步**）。
4. 从“**Setup Type**”（**安装类型**）窗口选择“**Express**”（**快速**）或“**Custom**”（**自定义**）安装。

选择 **"Custom"（自定义）**使您能够选择要安装的特定 Dell OpenManage 应用程序并更改 IT Assistant 的安装目录路径和端口设置。

选择 **"Express"（快速）**会使用预先选择的默认位置和端口设置安装所有通过相关性检查的 Dell OpenManage 应用程序（包括 IT Assistant）。 如果选择 **"Express"（快速）**，会跳到最后一步。

5. 确保在可安装组件列表中选中 **IT Assistant**，然后单击 **"Next"（下一步）**。
6. 如果选择 **"Custom"（自定义）**安装选项，应输入端口设置或接受默认值。 如果选择 **"Express"（快速）**安装选项，此对话不会出现。
7. 单击 **"Next"（下一步）**。
8. 确保将 **IT Assistant** 包括在安装摘要窗口中，然后单击 **"Install"（安装）**开始安装。

从以前版本的 IT Assistant 升级

注：只有 IT Assistant 6.2 和更高版本支持从以前版本升级。 Dell OpenManage Management Station 安装程序会检测系统上当前是否有可升级版本的 IT Assistant。

要升级 IT Assistant：

1. 将 *Dell Systems Management Consoles* CD 放入 CD 驱动器中。

   如果安装程序没有自动启动，应浏览到 **/windows** 目录并单击 **setup.exe**。 **Dell OpenManage Management Station** 屏幕将会显示。

2. 安装程序会自动扫描系统查找任何相关性，比如是否安装了 SNMP 或具有支持的数据库应用程序。 如果找到相关性，会显示信息窗口并提示您安装所需的软件包。

   注：如果拥有 IT Assistant 版本 6.*x*，应先安装 IT Assistant 7.0 然后再安装 7.1 或更高版本。 IT Assistant 7.0 安装程序会删除所有以前的 Management Station 应用程序并重新安装所选应用程序。所有的 Dell OpenManage Server Administrator 应用程序也会删除。

   注：如果具有 IT Assistant 7.0 或更高版本，安装程序会将 IT Assistant 7.2 作为 Service Pack 安装。

3. 如果没有找到相关性，则单击 **"Install, Modify, Repair or Remove Management Station"（安装、修改、修复或删除 Management Station）**。

   将会显示 Dell OpenManage Management Station 安装向导。 单击 **"Next"（下一步）**。

4. 如果同意 Dell Inc. 软件许可协议，则单击 **"Next"（下一步）**。
5. 从 **"Setup Type"（安装类型）**窗口选择 **"Express"（快速）**或 **"Custom"（自定义）**安装。

   选择 **"Custom"（自定义）**使您能够选择要安装的特定 Dell OpenManage 应用程序并更改 IT Assistant 的安装目录路径和端口设置。

   选择 **"Express"（快速）**会使用预先选择的默认位置和端口设置安装所有 Dell OpenManage 应用程序（包括 IT Assistant）。

6. 确保在可安装组件列表中选中 **IT Assistant**，然后单击 **"Next"（下一步）**。
7. 如果选择 **"Custom"（自定义）**安装选项，应输入端口设置或接受默认值。 如果选择 **"Express"（快速）**安装选项，此对话不会出现。
8. 默认情况下，会选中 **"Migrate IT Assistant Database Settings"（迁移 IT Assistant 数据库设置）**。 选中此选项后，现有 IT Assistant 安装中的以下数据库设置会保留在新的安装中：
   - 全局配置
   - 事件存储操作
   - 查找配置
9. 单击 **"Next"（下一步）**。
10. 确保将 **IT Assistant** 包括在安装摘要窗口中并且单击 **"Install"（安装）**开始安装。

注： 从 IT Assistant 版本 6.*x* 升级到版本 7.2 时，必须限定 CIM 用户名。 这种限定是必要的，因为 CIM 只根据查找范围启用/禁用，并且要求每个 CIM 用户用一个域限定，或者如果没有配置可信域，则使用本地主机限定。 通过查找范围（例如，*<域\用户名>* 或 *<本地主机\用户名>*）配置 CIM 以验证和使用 CIM 协议时，提供这种限定很有必要。

卸载 IT Assistant

卸载 IT Assistant：

1. 单击“**Start**”（开始）按钮，指向“**Settings**”（设置），并双击“**Control Panel**”（控制面板）。
2. 双击“**Add/Remove Programs**”（添加/删除程序）。
3. 从当前所装程序列表中选择 **Management Station** 并单击“**Change**”（更改）按钮。

   注：要卸载整个产品 Management Station 套件（包括 IT Assistant），在上一步中选择“**Remove**”（删除）。 选择“**Remove**”（删除）后，如果 IT Assistant 正在执行查找或轮询，卸载过程可能会有几分钟没有响应。

   Management Station 安装向导会出现。 单击“**Next**”（下一步）。
4. 在“**Program Maintenance**”（程序维护）窗口，选择“**Modify**”（修改）并单击“**Next**”（下一步）。
5. 在“Custom Setup”（自定义设置）屏幕，取消选择 IT Assistant 并单击“**Next**”（下一步）。
6. 在摘要屏幕中，确保将 IT Assistant 包括在要删除的应用程序的列表中。 单击“**Install**”（安装）。
7. 完成卸载后，单击“**Finish**”（完成）。
8. 重新引导系统。

远程 Microsoft SQL Server 和 IT Assistant

请参阅 **www.dell.com/openmanage** 上的白皮书“远程 Microsoft SQL Server 与 IT Assistant 配合使用的逐步说明”，该白皮书介绍了如何配置 IT Assistant 6.3 和更高版本，以便将正在远程服务器上运行的 Microsoft SQL Server 用作 IT Assistant 数据库。

返回目录页

返回目录页

配置 IT Assistant 监测系统

Dell OpenManage™ IT Assistant 7.2 版用户指南

Dell OpenManage™ IT Assistant 可以为企业中的每个系统查找、资源清册并执行各种更改管理任务。 Managed System 可以包括各种客户系统（台式机、便携式计算机和工作站）、服务器、带有远程访问卡的系统、Dell™ PowerConnect™ 交换机和高密度机架系统使用的数字键盘/视频/鼠标 (KVM) 交换机。

现实用户方案中的 IT Assistant

本节讨论如何在两种不同的客户方案中使用 IT Assistant。

- 中小型公司
- 大型企业环境

虽然是虚构的，但是本节介绍的这两种方案都解释了负责管理网络环境的管理员应如何配置 IT Assistant。 尽管这两种方案的许多 IT Assistant 配置概念完全相同，但其它配置取决于所管理系统的类型和数量。 将最符合您情况的方案作为您配置 IT Assistant 的常规指导。

不管您的网络有多大，仔细研究一下两种方案以充分了解 IT Assistant 的程序和概念是非常有用的。

注：本节中的两个方案都不旨在展示 IT Assistant 的全部功能。 根据您企业的具体情况，可能需要选择此处没有展示的 IT Assistant 选项和功能。 有关 IT Assistant 全部功能的详情，请参阅 IT Assistant 联机帮助。

确保安装并运行代理程序和设备

无论大还是小，所有由 IT Assistant 管理的网络都有一个基本要求：网络中的所有 Managed System 都必须安装并运行 Dell Systems Management 代理程序（设备）。 Managed System 需要的 Dell 代理程序包含在 Dell OpenManage Server Administrator 中；客户系统（工作站、台式机和便携式计算机）需要的 Dell 代理程序包含在 Dell OpenManage Client Instrumentation (OMCI) 中。

这些代理程序会从所装系统的 BIOS 或其它固件收集状况信息，然后将此信息提供给 IT Assistant。 IT Assistant 监测的系统通常称为 *Managed System* --管理它们的系统称为*网络 Management Station* 或 *IT Assistant 系统*。

如果没有安装这两个代理程序，请先参阅 *Dell OpenManage Server Administrator* 和 *Dell OpenManage Client Instrumentation* 说明文件，然后再继续 IT Assistant 配置。 如果两个都已安装并正确运行，则启动 IT Assistant 并继续阅读。

启动 IT Assistant

注：IT Assistant 支持基于角色的访问控制 (RBAC) 以定义每个用户可以执行的具体操作。 要设置 RBAC 用户，请参阅“确保安全 Dell OpenManage IT Assistant 安装”。

要登录 IT Assistant：

1. 双击系统桌面上的 **IT Assistant** 图标。
2. **"Log in"（登录）**对话框会出现。（如果按照"确保安全 Dell OpenManage IT Assistant 安装"配置了单一登录，**"Log in"（登录）**对话框将不会出现。）
3. 输入用户名和密码。
4. 如果使用 Active Directory 插件程序配置了用户信息，则选择 **"Active Directory Login"（Active Directory 登录）**。在 IT Assistant 中的权限取决于定义的用户设置。

   注： 有关设置基于角色的权限的详情，请参阅"确保安全 Dell OpenManage IT Assistant 安装"。有关安装 Active Directory 插件程序和为 IT Assistant 扩展 Active Directory 架构的信息，请参阅《*Dell OpenManage 安装和安全性用户指南*》。

   注：要远程访问 IT Assistant，必须输入 `https://<`*主机名*`>:<`*段口号*`>`。默认端口号为 2607。

5. 输入密码。

   注：IT Assistant 启动时，会出现一个验证认证弹出框。必须在 5 分钟内单击 **"OK"（确定）**接受这些认证，否则 IT Assistant 不会正确载入并且某些重要功能将不会运作。

   注：在 IT Assistant 启动期间可能会看到几个弹出框。可以避免看到这些要求接受授权认证的弹出框，方法是选择 **"View Certificate"（查看认证）→ "Install Certificate"（安装认证）**（如果可用）或选择 **"Always"（始终）**以响应要求接受认证的请求。

为系统可管理性配置 SNMP

为系统可管理性配置 SNMP 前，让我们先看看本节中用于说明 IT Assistant 的两个应用方案：

两位系统管理员（让我们称呼他们为 Jane 和 Tom）负责管理两个不同的网络环境。Jane 代表中小型公司（50 个服务器，外加 200 多个客户系统），Tom 则代表较大型的企业（1,000 个服务器）。尽管 Jane 和 Tom 都使用 IT Assistant 查找并管理系统，他们配置和使用 IT Assistant 的方式会有很大不同。不过在重点指出这些不同前，让我们看一下两人都要执行的一些基本步骤。

Jane 和 Tom 均必须配置简单网络管理协议 (SNMP) 系统管理协议以查找系统和接收陷阱（异步、警报通知）以报告其组件的状态。在 Managed System 上，Server Administrator 代理程序生成 SNMP 陷阱以响应 Managed System 上传感器和其它所监测参数的状态变化。要正确发送这些陷阱，操作系统的 SNMP 服务必须配置一个或多个陷阱目标，与安装 IT Assistant 的系统相对应。

配置 SNMP 服务的详情

有关 IT Assistant 系统和所有支持的 Managed System 操作系统的 SNMP 配置的详细信息，请参阅"配置协议将信息发送给 IT Assistant"。

在要管理的系统上配置 SNMP

除了在 IT Assistant 系统上安装和运行 SNMP 服务以外，每个 Managed System 的操作系统必须配置 SNMP 服务或守护程序。

SNMP 最佳做法

在配置 SNMP 时，您必须遵守以下要求：

- 将主机名或静态 IP 地址用于 IT Assistant 系统。
- 在所有 Managed System 上，将静态 IP 地址或主机名配置为 SNMP 陷阱目标。如果将主机名用作 SNMP 陷阱目标（IT Assistant 系统名称），则必须在您的网络上正确配置 DNS。
- 确保 SNMP 的 **Get** 和 **Set** 团体名称不同。
- 在将团体名称分配给 Managed System 时，确保不同团体名称的总数较低。团体名称越少，管理网络越容易。

需要 Managed System 上的信息来优化 SNMP 配置

对于使用 SNMP 协议查找和管理的每个系统，确保：

- 安装了 SNMP。
- IT Assistant 系统的名称或 IP 地址列在“SNMP Service Properties”（SNMP 服务属性）窗口 →“Security”（安全性）选项卡 →**“Accept SNMP packets from these hosts”（接受来自这些主机的 SNMP 数据包）**单选按钮。 需要在 Managed System 上配置此值。
- 如果 Managed System 准备将陷阱发送给 IT Assistant，则 IT Assistant 系统的主机名或 IP 地址必须列为**“SNMP Service Properties”（SNMP 服务属性）**窗口上**“Trap”（陷阱）**选项卡上**的 “Trap destination”陷阱目标）**。
- 必须在**“SNMP Service Properties”（SNMP 服务属性）**窗口的**“Trap”（陷阱）**和**“Security”（安全性）**选项卡上分配有效的团体名称。

要设置的两个团体名称为 **Get**（或读取）团体名称和 **Set**（或写入）团体名称。 读取团体名称，有时标记为*只读*，可让 IT Assistant 从 Managed System 中读取信息，而写入团体名称，有时标记为*读写*，可让 IT Assistant 读取信息并将其写入 Managed System。

注：团体名称区分大小写。

注：尽管您可以将一个团体名称设置为读取和读/写，但建议为每种创建单独的名称，以便限制对写入操作的访问。

当您设置 SNMP 查找范围时，在操作系统中为 Managed System SNMP 分配的团体名称还必须记录在 IT Assistant 中。

在协议部分下面的**“Discovery Range”（查找范围）**对话框中，确保输入所有 Managed System 的 **Get**（或读取）和 **Set**（或写入）团体名称。 如果每个字段存在多个团体名称，则使用逗号分隔每个团体名称。

为可管理性配置 CIM

根据您所在的网络环境，配置 CIM 可能是一个必需任务。 CIM 是新客户机工具的首选系统管理协议，需要装有 OMCI 7.*x* 版的 Dell 系统工具。 CIM 也用于执行远程 Windows 软件更新。

在 Jane 的中小型网络中，必须安装、启用和配置 CIM 才能够管理运行最新客户机工具 (OMCI 7.*x*) 的客户机系统。 虽然 Tom 的 Managed System 组完全由服务器组成，他也要安装并启用 CIM。 一般来说，如果企业包括任何运行 Microsoft® Windows® 操作系统的 Managed System，则应启用 CIM。

在操作系统中配置 CIM

IT Assistant 使用 Windows Management Interface (WMI) 内核进行 CIM 连接。 WMI 内核使用 Microsoft 网络安全保护防止他人擅自访问 CIM 工具。

有关操作系统 CIM 配置的详情，请参阅“配置协议将信息发送给 IT Assistant”。

注：IT Assistant 需要在Managed System 上建立的具有管理员权限的 CIM 用户名和密码。 如果您正在使用域用户，确保在用户名字段中指定正确的域。 用户名必须始终使用域来限定,或使用 **localhost**（如果没有域）。 格式可以是**域\用户**或 **localhost\用户**。

注：CIM 查找需要正确的用户 ID 和密码凭证。 无法在为 CIM 查找配置的子网上提供正确的凭证可能会导致帐户锁定。

设置查找目标的最佳做法

不管网络的大小，下表介绍了 Dell 在设置查找目标方面的最佳做法建议。 IT Assistant 用户在网络上定义查找目标系统和范围，以标识他们要确定并记入数据库的系统。 当您在 IT Assistant 中设置查找目标和范围时，您可以选择主机名、IP 地址或子网范围，以便标识要 IT Assistant 查找的系统。 本节显示最适合您所具有网络环境的查找类型。

表 4-1. 设置查找目标的最佳做法建议

首选查找范围类型	DHCP	主要静态 IP 地址

主机名	建议	如果 DNS 存在，并且 IP 地址分布于多个不同网络段中，则建议
IP 地址	不建议	如果 IP 地址分布于多个不同的网络段中，则建议
IP 范围	如果位于一个或多个网络段中，则建议	如果位于一个或多个网络段中，则建议

Jane 的中小型公司中的查找

Jane 想在网络上查找所有系统。 查找是 IT Assistant 标识每个系统并将该标识信息记录在 IT Assistant 数据库中的一个过程。

正如我们前面提到的，Jane 是一个混合系统网络的唯一系统管理员，该网络包括：

- 50 个 Dell PowerEdge™ 系统
- 200 个 Dell OptiPlex™ 台式机
- 10 个 Dell PowerConnect 交换机

Jane 准备使用 IT Assistant 来监测其系统的全局状态，并且当网络上的 PowerEdge 系统或 PowerConnect 交换机处于警告或严重状态时收到通知。 当其中一个桌面系统生成警报时，Jane 不计划使用 IT Assistant 对她作出通知。

确定混合服务器-客户机系统的要求

使用 IT Assistant 配置查找前，Jane 需要就她的网络做一些基本的决定。 具体地说，她必须决定：

- 在网络上管理系统和设备所需的系统管理协议
- 要由 SNMP 管理的系统的团体名称和陷阱目标
- PowerConnect 交换机的 SNMP 要求
- 验证的 CIM 凭证
- Jane 要监测的系统的主机名、IP 地址或 IP 子网范围

Jane 的网络需要的系统管理协议

在计划配置查找中，Jane 具有混合的系统类型（服务器、客户机和交换机）。 Jane 管理这些联网系统和设备所需的系统管理协议是：

- 用于 PowerEdge 系统和 PowerConnect 交换机的 SNMP
- 用于运行 Windows 的系统的 CIM，假定 Jane 在客户机系统上安装了与 CIM 兼容的新客户机工具

要了解协议要求，请参阅“配置协议将信息发送给 IT Assistant”。

团体名称和陷阱目标

Jane 在其Managed System 上为 SNMP 配置 **Get** 和 **Set** 团体名称和陷阱目标的要求不受公司大小的影响。 对于与服务器相关联的 SNMP 配置要求，请参阅“配置协议将信息发送给 IT Assistant”。

为 PowerConnect 交换机配置 SNMP

Jane 可以通过使用 IT Assistant 监测 10 个 PowerConnect 交换机。 每种型号的 PowerConnect 交换机均具有说明文件，提供了为该交换机设置 SNMP 服务的以下信息：

- 团体名称

- 陷阱目标
- 交换机将从中接受 SNMP 信息包的主机

用于在 Jane 的网络上查找系统的初始任务

现在 Jane 已经检查了有关查找配置的前提条件信息，她准备执行首次查找配置。 Jane 必须执行以下任务：

- 在Managed System 上配置通信协议。
- 配置查找设置。
- 输入所有查找范围。

使用 IT Assistant 查找并管理 Jane 的网络系统

如果这是 IT Assistant 自安装以来的首次运行，Jane 会看到一个欢迎屏幕，指出 IT Assistant 尚未配置。 下面列出的是四个基本配置步骤：

步骤 1：查找配置 – 控制 IT Assistant 多长时间轮询一次网络以查找新添加的系统

步骤 2：资源清册配置 – 控制 IT Assistant 多长时间检索一次所有已查找系统的详细资源清册

步骤 3：状况轮询 – 控制 IT Assistant 多长时间检索一次已查找系统的运行状况和网络连接状况

步骤 4：范围 – 标识 IT Assistant 的范围以限制或扩展查找、资源清册或轮询任务的范围

单击任何一个步骤都会将她带到 IT Assistant 中 **“Discovery and Monitoring”（查找和监测）**菜单栏下的相应对话框。 步骤 1 到 3 都是单窗口对话框；步骤 4 是一个用于定义查找范围的基于向导的程序。

配置查找设置

Jane 首先使用 **“Discovery Configuration Settings”（查找配置设置）**对话框为系统配置查找设置。 此对话框既会在 IT Assistant 中单击 *“Step 1: Discovery Configuration”（步骤 1：查找配置）*时自动显示，也会通过从菜单栏选择 **“Discovery Configuration”（查找配置）**来显示。 Jane 在此处输入 IT Assistant 将用于查找的信息。这些值将保持不变并且会应用到她以后在此过程中创建的相应查找范围。 不过，她可以随时更改这些值。

要配置 IT Assistant 中的查找设置：

1. 从 IT Assistant 菜单栏选择 **“Discovery and Monitoring”（查找和监测）→“Discovery Configuration”（查找配置）**。

   出现 **“Discovery Configuration Settings”（查找/配置设置）**对话框。 默认情况下，会选中 **“Enable Device Discovery”（启用设备查找）**。

2. 在 **“Initiate Device Discovery”（启动设备查找）**下的对话框中，选择何时要 IT Assistant 执行查找。

   Jane 选择在每周所有七天的 6:00:00 AM 执行查找，因为她需要所有日子的数据，但她要选择非高峰期间。

注：Dell 建议您安排在非高峰时查找。

3. 在 **“Discovery Speed”（查找速度）**下面，使用滑动条表示您要分配给查找多少网络带宽和系统资源。

   注：设置的查找速度越快，查找消耗的网络资源越多。 更快的查找速度可能会影响网络性能。

4. 在**“Discover”（查找）**下，选择是查找**“All Devices”（所有设备）**还是**“Only Instrumented Devices”（仅限配备工具的设备）**。

   Jane 选择了**“Only Instrumented Devices”（仅限配备工具的设备）**，因为她希望 IT Assistant 只查找那些具有 SNMP 或 CIM 工具的设备。 如果希望查找所有能够响应 **ping** 命令的设备，则应该选择**“All Devices”（所有设备）**。 有关所支持代理程序的列表，请参阅“IT Assistant 支持的代理程序”。

   注： Dell 建议，如果在您的网络上配置了域名系统 (DNS)，请选择默认的**“DNS Name Resolution”（DNS 名称解析）**。

5. 在**“Name Resolution”（名称解析）**下，选择**“DNS Name Resolution”（DNS 名称解析）**或**“Instrumentation Name Resolution”（设备名称解析）**。

   DNS 名称解析将系统的 IP 地址与主机名匹配。 工具名称解析为其名称查询Managed System 的代理程序工具。 有关如何配置工具名称解析的详情，请参阅设备或系统说明文件。

   注： Dell 建议，如果在您的网络上配置了 DNS，请选择默认的**“DNS Name Resolution”（DNS 名称解析）**。

6. 单击**“OK”（确定）**。

配置资源清册设置

接下来，Jane 需要输入资源清册设置。 IT Assistant 会收集有关软件和固件版本的资源清册信息，以及与设备有关的信息，比如内存、处理器、电源设备、PCI 卡和嵌入式设备以及存储。 此信息会存储在 IT Assistant 数据库中并且可以用来生成自定义报告。

要设置资源清册设置：

1. 从菜单栏选择**“Discovery and Monitoring”（查找和监测）→“Inventory Configuration”（资源清册配置）**。

   会显示**“Inventory Poll Settings”（资源清册轮询设置）**对话框。 默认情况下**“Enable Inventory”（启用资源清册）**为选中。

2. 在**“Initiate Inventory”（启动资源清册）**下面，选择希望 IT Assistant 何时执行资源清册。

   Jane 选择了每星期的所有七天，在早上 6:00:00 的网络通信非高峰时段。

3. 在**“Inventory Speed”（资源清册速度）**下面，使用滑动条表示您要分配给资源清册多少网络带宽和系统资源。

   注：设置的资源清册速度越快，查找消耗的网络资源越多。 更快的资源清册速度可能会影响网络性能。

4. 单击**“OK”（确定）**。

配置状况轮询设置

接下来，Jane 会为系统定义状况轮询设置。 IT Assistant 会为查找的设备执行电源和连接运行状况检查，确定设备是否运行正常，是处在非正常状态，还是已断电。 IT Assistant 中的状况信息包括 *“healthy”（运行良好）*、*“warning”（警告）*、*“critical”（严重）*和 *“powered down”（断电）*。 状况图标还会表示系统是否已配备好工具，没有系统的信息，或者系统最后一次断电前所处的状态。

要设置状况轮询设置：

1. 从菜单栏选择**“Discovery and Monitoring”（查找和监测）→“Status Polling Configuration”（状况轮询配置）**。

   “Status Polling Configuration Settings”（状况轮询配置设置）对话框会显示。 默认情况下，会选中**“Enable Status Polling”（启用状况轮询）**。

2. 在**“Status Polling Inventory”（状况轮询资源清册）**下，选择要 IT Assistant 执行状况轮询的间隔。
3. 在**“Status Polling Speed”（状况轮询速度）**下面，使用滑动条表示您要分配给状况轮询多少网络带宽和系统资源。

   注：设置的状况轮询速度越快，查找消耗的网络资源越多。 更快的速度可能会影响网络性能。

4. 单击**“OK”（确定）**。

配置查找范围

IT Assistant 维护着一个网络段注册表，用于查找设备。 查找范围可以是子网、子网上的 IP 地址范围、单个 IP 地址或单个主机名。

要向 IT Assistant 标识系统，Jane 必须定义一个查找范围。

要标识包含范围：

1. 从菜单栏选择**“Discovery and Monitoring”（查找和监测）→“Ranges”（范围）**。

   “Discovery Ranges”（查找范围）导航树显示在 IT Assistant 窗口的左边。

2. 扩展**“Discovery Ranges”（查找范围）**，右击**“Include Ranges”（包含范围）**并选择**“New Include Range”（新建包含范围）**。

   “New Discovery Wizard”（新建查找向导）将会启动。

   注：要从查找中*排除*某个系统或主机名，右击**“Discovery Ranges”（查找范围）**导航树中的**“Exclude Range”（排除范围）**并输入系统的名称或 IP 地址。 在大多数类似 Jane 的中小型公司中，不使用此选项。

3. 在向导的步骤 1 中，输入 IP 地址（或范围）或主机名，然后单击**“Next”（下一步）**进入下一步骤。

   注：包含范围的可接受值为单个系统的子网范围、主机名或 IP 地址。 Jane 引用她为服务器、台式机系统和交换机记下的 IP 子网范围。 在 Jane 的列表中，Jane 可能具有 192.166.153.* 和 192.166.154.*，其中第一个子网范围用于 Jane 的服务器，第二个子网范围用于 Jane 的台式机，交换机扩展至这两个子网。

   注：导入节点列表公用程序提供了一种便捷的方法，可以为 IT Assistant 指定要查找的一列主机名、IP 地址和子网范围。 请参阅 IT Assistant 联机帮助了解如何从命令行运行公用程序。 **importnodelist.exe** 文件位于 **/bin** 目录。

4. 在向导的步骤 2 中，为该范围的因特网控制信息协议 (ICMP) 超时和重试使用默认值。 使用故障排除工具确定这些值。
5. 在向导的步骤 3 中，配置在查找期间将要使用的 SNMP 参数：
   - 确保选中**“Enable SNMP Discovery”（启用 SNMP 查找）**选项。
   - 为**“Get Community”（Get 团体）**名称输入区分大小写的值。

     Jane 的考虑事项：

     Jane 正在管理 50 台服务器，因此她要配置 SNMP。 **“Get Community”（Get 团体）**名称是一个只读密码，SNMP 代理程序将其安装在Managed System 上用于验证。 Jane 在选择**“Get Community”（Get 团体）**名称时考虑了以下事项：

     每个 SNMP Managed System 均具有**“Get Community”（Get 团体）**名称。 Jane 确保在要管理的所有系统上列出每个团体名称。 如果 Jane 的 Managed System 具有多个团体名称，可以在**“Get Community”（Get 团体）**名称字段中输入多个以逗号分隔的团体名称。

     尽管**“Get Community”（Get 团体）**名称影响 IT Assistant 从 Managed System 中检索的只读信息（例如，查找的结果、状况轮询和警报日志），但 Jane 要限制对此只读数据的访问。 因此，她将默认的**“Get Community”（Get 团体）**名称 (**public**) 更改为只有她自己和指定后备同事知道的名称。

     注：在 SNMP Get 和 Set 团体名称字段中为 Managed System 操作系统输入的团体名称必须与 IT Assistant 中分配的 Get 团体和 Set 团体名称相匹配。

   - 为**“Set Community”（Set 团体）**名称输入区分大小写的值。

     Jane 的考虑事项：

“Set Community”（Set 团体）名称是一个读写密码，允许访问 Managed System。 Managed System 上运行的 SNMP 代理程序在系统上尝试操作时使用此密码进行验证，这些操作包括关闭、配置警报措施和更新软件。

注：尽管 Dell 服务器工具在 SNMP Set 团体名称上具有验证层（需要主机名和密码），但许多 SNMP 代理程序没有。 对于没有添加此安全保护层的代理程序，知道 SNMP Set 团体名称的任何用户均可以获得对 Managed System 的控制。

Jane 选择了一个与所管理系统上 SNMP Set 团体值匹配的**“Set Community”（Set 团体）**名称。 还确保选择的名称符合公司的安全密码标准。

注： 如果要在单个查找范围中指定多个 SNMP Get 或 Set 团体名称（例如，为每个 IP 子网范围指定一个团体名称），则用逗号分隔团体名称。

- 输入 SNMP 查找范围的超时和重试值。 在 Jane 的这种网络中，默认值通常是不错的选择。

6. 在向导的步骤 4 中，配置在查找期间将要使用的 CIM 参数。

由于在 Jane 运行 Windows 的管理组中混合有服务器和客户系统，因此需要配置 CIM。

- 确保选中**“Enable CIM Discovery”（启用 CIM 查找）**。
- 在**“Domain\User Name”（域\用户名）**中，输入用于在 Managed System 上配置 CIM 的名称。
- 输入用于在 Managed System 上配置 CIM 的**“Password”（密码）**。

7. 在向导的步骤 5 中，选择 IT Assistant 在向导完成时将采取什么操作。
8. 在向导的步骤 6 中，查看选择并选择**“Finish”（完成）**完成向导或**“Back”（返回）**更改选择。

在初始设置后更改查找、资源清册和状况轮询设置

可以随时返回**“Discovery and Monitoring”（查找和监测）**菜单编辑输入的设置。 输入的新设置将在下一次执行相应操作时生效。

为 Jane 的中小型公司创建警报措施筛选器和警报措施

Jane 在 IT Assistant 中通过指定一组条件来创建 *“Alert Action Filter”（警报措施筛选器）*。 当与 *“Alert Action”（警报措施）*关联后，IT Assistant 会自动执行 Jane 定义的操作。

IT Assistant 有三种警报筛选器：

“Alert Action Filters”（警报措施筛选器） – 用于在符合警报条件时触发操作

“Ignore/Exclude Filters”（忽略/排除筛选器） – 用于在收到时忽略 SNMP 陷阱和 CIM 提示

“Alert View Filters”（警报视图筛选器） – 用于自定义警报日志视图

Jane 选择在 IT Assistant 中使用警报措施筛选器来为服务器和 PowerConnect 交换机筛选*警告*和*严重*事件。 这样，她就能够创建警报措施，在服务器和交换机组件进入这些状态时自动向她发送电子邮件通知。 她可以随后采取措施来避免更严重的事件，比如系统故障。 由于是唯一的网络系统管理员，Jane 必须能够选择监测哪些系统，以及选择创建警报措施筛选器。她于是决定只将这些筛选器和操作用于最关键的设备和最严重的事件。

创建警报措施筛选器

1. 从菜单栏选择**“Alerts”（警报）→ “Filters”（筛选器）**。

“Alert Filters”（警报筛选器）窗口将会出现。

2. 在导航树中展开警报筛选器并右击**“Alert Action Filters”（警报措施筛选器）**。 选择**“New Action Alert Filter”（新建警报措施筛选器）**。

“Add Filter Wizard”（添加筛选器向导）将会出现。

3. 为筛选器输入说明名称。 例如，*Jane 的网络警告和严重*。
4. 在**“Severity”（严重性）**下面，选择要接收警报和日志的事件的严重性。

   Jane 选择**“Warning”（警告）**和**“Critical”（严重）**。

   单击**“Next”（下一步）**。
5. 在**“Alert Category Configuration”（警报类别配置）**下，选中**“Select All”（全选）**或选择要在警报筛选器中包括的事件类别。

   Jane 选取**“Select All”（全选）**，因为她想得知影响网络交换机或服务器的任何警报或严重事件。
6. 在**“Device/Group Configuration”（设备/组配置）**下，选择与新警报措施筛选器相关的设备或组。

   Jane 选取**“Servers and Network Devices”（服务器和网络设备）**。
7. 在**“Date/Time Range Configuration”（日期/时间范围配置）**下，为任何或所有可选类别输入值。

   Jane 将这些选项都保留为未选中，因为她想在所有时间都应用筛选器。
8. 在**“Alert Action Associations”（警报措施关联）**下，选择是否要筛选器捕获的事件触发警报或写入日志文件。

   Jane 选择**“Alert”（警报）**获取控制台通知。
9. **“New Filter Summary”（新筛选器摘要）**显示了选择。 单击**“Finish”（完成）**接受，或单击**“Back”（返回）**进行更改。
10. 验证在向导步骤 3 中创建的筛选器名称是否出现在**“Summary of Alert Action Filters”（警报措施筛选器摘要）**窗口中。

创建警报措施

现在，Jane 想创建由刚刚设置的警报措施筛选器触发的警报措施。

创建警报措施：

1. 从菜单栏选择**“Alerts”（警报）→“Actions”（措施）**。
2. 右击导航中的**“Alert Actions”（警报措施）**并选择**“New Alert Action”（新建警报措施）**。

   “Add Alert Action Wizard”（添加警报措施向导）将会出现。
3. 在**“Name”（名称）**字段中给该操作取一个合理的名称。
4. 从**“Type”（类型）**下拉式菜单中，选择**“Email”（电子邮件）**。

   注：Jane 也可以从操作类型下拉式菜单中选择**“Trap Forwarding”（陷阱转发）**或**“Application Launch”（应用程序启动）**。 **“Trap Forwarding”（陷阱转发）**使大型企业的管理者能够将 SNMP 陷阱发送到特定的 IP 地址和主机。 **“Application Launch”（应用程序启动）**使管理员能够指定在符合警报措施筛选器时运行的可执行文件。

   注： 由 IT Assistant 转发的任何陷阱都不具有源陷阱的 EnterpriseOID、Generic TrapId 和特定陷阱 ID。 这些值会显示在所转发陷阱的说明中。
5. 在**“E-mail Configuration”（电子邮件配置）**对话框中，指定有效的电子邮件地址（在企业的 SMTP 服务器组中）以接收自动通知。

   注：Jane 可以使用**“Test Action”（检测操作）**按钮检测她指定的电子邮件配置。 将会发出成功/失败消息。 成功表示 IT Assistant 发送了信息，而不是接收者收到了信息。 有关使用**“Test Action”（检测操作）**按钮的详情，请参阅 IT Assistant 联机帮助中的故障排除主题。

6. 在**“Alert Filter Associations”（警报筛选器关联）**中，标识将要触发此电子邮件的警报措施筛选器。

   在 Jane 的情况中，她选择了 *Jane 的网络警告和严重--* 她前面给警报措施筛选器取的名称。

7. 摘要对话框会显示您的选择。 单击**“Finish”（完成）**接受，或单击**“Back”（返回）**进行更改。

   验证在步骤 3 中分配的警报措施的名称是否出现在**“Summary of Alert Actions”（警报措施摘要）**窗口中。

作为 Jane 在 IT Assistant 中配置警报措施筛选器和警报措施的结果，这里是将要发生的情况：

- IT Assistant 会一直监测 Jane 网络上的所有服务器和网络交换机。
- 当任何服务器或网络交换机出现警告或严重状态时，Jane 在 IT Assistant 中设置的警报措施筛选器将会自动触发相关的警报措施。
- 警报措施会按照指定的地址向 Jane 发送一个电子邮件通知。
- Jane 于是决定对受影响的系统采取何种措施，比如对系统关机后再开机、关闭系统或使用其它 IT Assistant 功能运行远程命令。

在 IT Assistant 中可以使用的功能还有很多，此处就不再一一列出。 单击 IT Assistant 中相应对话框的**“Help”（帮助）**按钮以查看有关该功能的详细联机帮助。

现在让我们来看一看在大型企业中如何使用 IT Assistant 来完成 Jane 在小企业中所完成的基本相同的任务。

Tom 的企业级公司中的查找

在较大企业级公司（情况 2）中，Tom 是 1,000 个服务器网络的系统管理员。 Tom 还负责监管四位协助他的技术人员，当通知发生严重或警告时，对服务器采取纠正措施。 Tom 的四位技术人员的责任如下：

- 一位管理员负责所有远程系统
- 一位技术人员负责第一班（12 小时）
- 一位技术人员负责第二班（12 小时）
- 一位技术人员在周末工作，工作 24 小时，但仅响应严重和警告事件。

配置查找周期

由于 Tom 正在监测没有客户机的服务器网络，因此首选的系统管理协议是 SNMP。 不过，由于他也管理运行 Windows 的系统，所以也要启用 CIM（和 Jane 一样）。

要为他的服务器配置查找周期，他将需要执行以下任务：

- 为要监测的服务器确定子网范围、IP 地址和/或主机名。
- 确定不想监测的子网范围、主机名或 IP 地址。
- 确定将用于其网络的 SNMP 公共 (Get) 和专用 (Set) 团体名称。
- 在要监测的每个系统上安装并配置 SNMP 代理程序和操作系统 SNMP 服务。
- 为网络确定相应的查找超时值。

服务器的 IP 子网范围

Tom 的第一个决定是确定他要使用 IT Assistant 监测的 1,000 个服务器。 Tom 可能要记录他要在其查找中包括的每个子网的 IP 子网范围，他要从查找中排除的任何系统或范围，在每个子网上使用的相应团体名称，以及他确定的任何与网络相关的其它数据。 表 4-2 中显示了获取此数据的表格实例。 请注意，Tom 可以根据子网范围、主机名或 IP 地址监测系统。 尽管建议限制网络中使用的团体名称数量，但 Tom 还可以在其网络环境中定义多个公共和专用团体名称。 例如，Tom 可以决定他要为此网络上的所有系统定义公用 Get 团体名称，但为特定数据中心定义唯一的专用团体名称。

注：IT Assistant 提供了一个故障排除工具，在收集系统信息和子网范围时很有用。 从菜单栏选择“Tools”（工具）→“Troubleshooting Tool”（故障排除工具）可以使用该工具。 有关详情，请打开“Troubleshooting Tool”（故障排除工具）对话框并单击“Help”（帮助）。

在每个 Managed System 上配置 SNMP

在配置查找之前，Tom 需要确定他要用于其网络的 Get 和 Set 团体名称，然后安装和配置要管理的每个服务器的 SNMP 代理程序和操作系统 SNMP 服务。 请参阅“配置 SNMP 以实现服务器可管理性（两种情况下）”。

表 4-2 提供了有关 Tom 正在监测的远程系统的信息。

表 4-2. 数据中心和远程服务器的子网范围、IP 地址或主机名和相应信息的实例

系统组名称	包括子网范围	排除主机或子网范围	公共/专用团体名称	子网上服务器的名称	子网上观察到的最长 Ping 响应时间
数据中心服务器 1	192.166.153.*	192.166.153.2	dcp123/dcsecure01	100	64
数据中心服务器 2	192.166.154.*	examplehost	dcp123/dcsecure02	100	128
数据中心服务器 3	192.166.155.*	192.166.155.10-25	dcp123/dcxprivall	100	78
数据中心服务器 4	192.166.156.*		dcp123/dcxprivall	100	32
数据中心服务器 5	192.166.157.*		dcp123/dcxprivall	100	146
数据中心服务器 6	192.166.158.*		dcp123/dcxprivall	100	148
数据中心服务器 7	192.166.159.*		dcp123/dcxprivall	100	132
数据中心服务器 8	192.166.160.*		dcp123/dcxprivall	100	59
数据中心服务器 9	192.166.161.*		dcp123/dcxprivall	50	128
远程服务器 1	10.9.72.*		dcp123/dcxprivrem	50	5600
远程服务器 2	10.9.73.*		dcp123/dcxprivrem	100	2400

为网络选择适当的查找超时值

由于 Tom 正通过 WAN 监测远程系统，本地系统和那些进一步删除的系统的超时值可能会有很大的不同。 在这种情况下，建议 Tom 为位于 WAN 上的系统查找确定并设置适当的超时。

在具有较长网络等待时间的环境中，比如全球 WAN，Tom 可能需要考虑在企业中增加 Ping 超时值。 通过使用**“Tools”（工具）→“Troubleshooting Tool”（故障排除工具）**并选择**“Device Connectivity”（设备连接）**选项卡，他可以确定显示最长网络等待时间的系统 Ping 时间。 这样，Tom 就可以检测长等待时间系统的连接以决定是否应该增加具体的 ping 时间来实现更好的 WAN 性能。

在企业网络中首次配置查找设置

与 Jane 一样，如果这是 IT Assistant 自安装以来的首次运行，Tom 会看到一个欢迎屏幕，指出 IT Assistant 尚未配置。 下面列出的是四个基本配置步骤：

步骤 1：查找配置

步骤 2：资源清册配置

步骤 3：状况轮询

步骤 4：范围

单击任何一个步骤都会将他带到 IT Assistant 中**“Discovery and Monitoring”（查找和监测）**菜单栏下的相应对话框。 步骤 1 到 3 都是单窗口对话框；步骤 4 是一个用于定义查找范围的基于向导的程序。

配置查找设置

Tom 首先也使用 **“Discovery Configuration Settings”（查找配置设置）**对话框为系统配置查找设置。 此对话框既会在 IT Assistant 欢迎屏幕中单击 *“Step 1: Discovery Configuration”（步骤 1：查找配置）*时自动显示，也会通过从菜单栏选择 **“Discovery Configuration”（查找配置）**来显示。 Tom 在此处输入 IT Assistant 将用于查找的信息。 这些值将保持不变并且会应用到他以后在此过程中创建的相应查找范围。 当然，他可以使用此对话框随时更改这些值。

要为大型企业配置 IT Assistant 查找设置：

1. 从 IT Assistant 菜单栏选择 **“Discovery and Monitoring”（查找和监测）→“Discovery Configuration”（查找配置）**。

   出现 **“Discovery Configuration Settings”（查找/配置设置）**对话框。 默认情况下，会选中 **“Enable Device Discovery”（启用设备查找）**。

2. 在 **“Initiate Device Discovery”（启动设备查找）**中，选择希望 IT Assistant 何时执行查找。

   Tom 希望每天执行查找，因此选择了 **“Every Week On”（每星期）**，每天，早上 2:00 作为开始时间。 网络通信量在此时最少。

3. 在**查找速度**下面，使用滑动条表示您要分配给查找多少网络带宽和系统资源。

   Tom 将查找速度设置为 **“Fast”（快速）**（最右边）。 Tom 要快速查找准备使用 IT Assistant 管理的所有系统，并将它们放入数据库。 在以后的查找中，如果 Tom 发现尝试在系统上执行其它任务时此设置对系统性能影响很大，他可以更改 **“Discovery Speed”（查找速度）**来占用较少的网络资源。

4. 在 **“Discover”（查找）**下，选择是查找所有设备还是仅查找配备工具的设备。
5. 在 **“Name Resolution”（名称解析）**下，选择 **“DNS Name Resolution”（DNS 名称解析）**或 **“Instrumentation Name Resolution”（设备名称解析）**。

   域名系统 (DNS) 名称解析将系统的 IP 地址与主机名匹配。 工具名称解析为其名称查询 Managed System 的代理程序工具。 有关如何配置工具名称解析的详情，请参阅设备或系统说明文件。

   注：如果正在管理群集，则必须使用设备名称解析才能标识各个独立节点（系统）；否则，推荐使用 DNS 名称解析。

6. 单击 **“OK”（确定）**。

配置资源清册设置

接下来，Tom 输入资源清册设置。 IT Assistant 会收集有关软件和固件版本的资源清册信息，以及与设备有关的信息，比如内存、处理器、电源设备、PCI 卡和嵌入式设备以及存储。 此信息会存储在 IT Assistant 数据库中并且可以用来生成自定义报告。

要设置资源清册设置：

1. 从菜单栏选择 **“Discovery and Monitoring”（查找和监测）→“Inventory Configuration”（资源清册配置）**。

   会显示 **“Inventory Poll Settings”（资源清册轮询设置）**对话框。 默认情况下 **“Enable Inventory”（启用资源清册）**为选中。

2. 在 **“Initiate Inventory”（启动资源清册）**下的对话框中，选择何时要 IT Assistant 执行资源清册。

   Tom 将资源清册设置为每周星期六早上 3:00。

3. 在 **“Inventory Speed”（资源清册速度）**下面，使用滑动条表示您要分配给资源清册多少网络带宽和系统资源。

   注：设置的资源清册速度越快，查找消耗的网络资源越多。 更快的资源清册速度可能会对网络性能产生不利影响。

4. 单击 **“OK”（确定）**。

配置状况轮询设置

接下来，Tom 会为系统定义状况轮询设置。 IT Assistant 会为查找的设备执行电源和连接运行状况检查，确定设备是否运行正常，是处在非正常状态，还是已断电。 IT Assistant 中的状况信息包括 *"healthy"（运行良好）*、*"warning"（警告）*、*"critical"（严重）*和 *"powered down"（断电）*。 状况图标还会表示系统是否已配备好工具，没有系统的信息,或者系统断电时所处的状态。

要设置状况轮询设置：

1. 从菜单栏选择 **"Discovery and Monitoring"（查找和监测）→"Status Polling Configuration"（状况轮询配置）**。

   "Status Polling Configuration Settings"（状况轮询配置设置）对话框会显示。 默认情况下，会选中 **"Enable Status Polling"（启用状况轮询）**。

2. 在 **"Status Polling Inventory"（状况轮询资源清册）**下，选择要 IT Assistant 执行状况轮询的间隔。
3. 在 **"Status Polling Speed"（状况轮询速度）**下面，使用滑动条表示您要分配给状况轮询多少网络带宽和系统资源。

   注：设置的状况轮询速度越快，查找消耗的网络资源越多。 更快的速度可能会影响网络性能。

4. 单击 **"OK"（确定）**。

配置查找范围

IT Assistant 维护着一个网络段注册表，用于查找设备。 查找范围可以是子网、子网上的 IP 地址范围、单个 IP 地址或单个主机名。

Tom 的企业网络被划分为许多子网。 在数据中心具有 850 个服务器，并且具有 150 个远程服务器。 Tom 参阅他为其服务器记下的 IP 子网范围（请参阅表 4-2）。

Tom 的数据中心服务器分为八个独立的子网，并且他的远程服务器分为两个子网。

要向 IT Assistant 标识系统，Tom 必须定义一个查找范围。

要标识包含范围：

1. 从菜单栏选择 **"Discovery and Monitoring"（查找和监测）→"Ranges"（范围）**。

   "Discovery Ranges"（查找范围）导航树显示在 IT Assistant 窗口的左边。

2. 扩展 **"Discovery Ranges"（查找范围）**，右击 **"Include Ranges"（包含范围）**并选择 **"New Include Range"（新建包含范围）**。

   "New Discovery Wizard"（新建查找向导）将会启动。

3. 在向导的步骤 1 中，输入 IP 地址（或范围）或主机名，然后单击 **"Next"（下一步）**进入下一步骤。

   根据表 4-2 中有关 Tom 系统的信息，必须完成该向导两次才能包括所有系统。 第一次，输入：

   192.166.153-161.*

   第二次，输入：

   10.9.72-73.*

注：导入节点列表公用程序提供了一种便捷的方法，可以为 IT Assistant 指定要查找的一列主机名、IP 地址和子网范围。 请参阅 IT Assistant 联机帮助了解如何从命令行运行公用程序。 **importnodelist.exe** 文件位于 **/bin** 目录。

4. 在向导的步骤 2 中，为该范围的因特网控制信息协议 (ICMP) 超时和重试输入默认值。
5. 在向导的步骤 3 中，配置在查找期间将要使用的 SNMP 参数：
   - 确保选中**“Enable SNMP Discovery”（启用 SNMP 查找）**选项。
   - 为**“Get Community”（Get 团体）**名称输入区分大小写的值。 **“Get Community”（Get 团体）**名称是一个只读密码，SNMP 代理程序安装在 Managed System 上用于验证。

     Tom 的考虑事项：

     Tom 在选择**“Get Community”（Get 团体）**名称时考虑了以下事项：

     每个 SNMP Managed System 均具有**“Get Community”（Get 团体）**名称。 Tom 确保在要管理的所有系统上列出每个团体名称。 如果 Tom 的 Managed System 具有多个团体名称，可以在**“Get Community”（Get 团体）**名称字段中输入多个以逗号分隔的团体名称。

     尽管**“Get Community”（Get 团体）**名称影响 IT Assistant 从 Managed System 中检索的只读信息（例如，查找的结果、状况轮询和警报日志），但 Tom 要限制对此只读数据的访问。 因此，会将默认 **“Get Community”（Get 团体）**名称 **(public)** 更改为只有他及其管理员知道的名称。

   注：在 SNMP Get 和 Set 团体名称字段中为 Managed System 操作系统输入的团体名称必须与 IT Assistant 中分配的 Get 团体和 Set 团体名称相匹配。

   - 为**“Set Community”（Set 团体）**名称输入区分大小写的值。

     Tom 的考虑事项：

     “Set Community”（Set 团体）名称是一个读写密码，允许访问 Managed System。 Managed System 上运行的 SNMP 代理程序在系统上尝试操作时使用此密码进行验证，这些操作包括关机、配置警报措施和更新软件。

   注：尽管 Dell 服务器工具在 SNMP Set 团体名称上具有验证层（需要主机名和密码），但许多 SNMP 代理程序没有。 对于没有添加此安全保护层的代理程序，知道 SNMP Set 团体名称的任何用户均可以获得对 Managed System 的控制。

     Tom 选择了一个与所管理系统上 SNMP Set 团体值匹配的**“Set Community”（Set 团体）**名称。 还确保选择的名称符合公司的安全密码标准。

   注： 如果要在单个查找范围中指定多个 SNMP Get 或 Set 团体名称（例如，为每个 IP 子网范围指定一个团体名称），则用逗号分隔团体名称。

   - 输入 SNMP 查找范围的超时和重试值。 在 Tom 的这种网络中，默认值通常是不错的选择。
6. 在向导的步骤 4 中，配置在查找期间将要使用的 CIM 参数。

   由于 Tom 还有运行 Windows 的系统，因此需要配置 CIM。
   - 确保选中**“Enable CIM Discovery”（启用 CIM 查找）**。
   - 在**“Domain\User Name”（域\用户名）**中，输入用于在 Managed System 上配置 CIM 的名称。
   - 输入用于在 Managed System 上配置 CIM 的**“Password”（密码）**。
7. 在向导的步骤 5 中，选择 IT Assistant 在向导完成时将采取什么操作。
8. 在向导的步骤 6 中，查看选择并选择**“Finish”（完成）**完成向导或**“Back”（返回）**更改选择。

从查找中排除系统

IT Assistant 还提供了将特定系统从查找中排除的功能。 此功能通常用于大型企业环境以提高速度，隔离具有问题代理程序的系统，或增强安全性和便利性。

Tom 的企业中有一个系统包含高度机密的信息。 这些信息特别机密，事实上，他甚至不想其系统管理员看到该系统。 因此，他设置了一个**“Exclude Range”（排除范围）**将该系统从日

常网络查找中隔离开。

1. Tom 从菜单栏选择 **“Discovery and Monitoring”（查找和监测）→“Ranges”（范围）**。

   “Discovery Ranges”（查找范围）导航树显示在 IT Assistant 窗口的左边。

2. 展开 **“Discovery Ranges”（查找范围）**，右击 **“Exclude Ranges”（排除范围）**并选择 **“New Exclude Range”（新建排除范围）**。

   出现 **“New Exclude Range”（新建排除范围）**对话框。

3. 输入系统的 IP 地址并单击 **“OK”（确定）**。

   这样，该系统就从 IT Assistant 的日常查找中隐藏起来。

在初始设置后更改查找、资源清册和状况轮询设置

Tom 可以随时返回 **“Discovery and Monitoring”（查找和监测）**菜单编辑输入的设置。 新设置将在下一次执行相应操作时生效。

为 Tom 的大型企业创建警报措施筛选器和警报措施

IT Assistant 使 Tom 能够设置指定一组系统条件的警报措施筛选器。 符合这些条件时，Tom 还可以在 IT Assistant 中创建由该警报措施筛选器触发的警报措施。 警报措施会执行 Tom 定义的任何操作。

IT Assistant 有三种筛选器：

“Alert Action Filters”（警报措施筛选器） – 用于在符合警报条件时触发操作

“Ignore/Exclude Filters”（忽略/排除筛选器） – 用于在收到时忽略 SNMP 陷阱和 CIM 提示

“Alert View Filters”（警报视图筛选器） – 用于自定义警报日志视图

在 Tom 为其 1,000 服务器环境创建警报措施筛选器或警报措施前，他创建了两个自定义组以更好地实现事件通知。 按照上面概述的情况，Tom 的大多数服务器位于数据中心，而其它服务器则位于远程位置。 Tom 在设置 IT Assistant 时在此策略上的决定。

他决定：

1. 为数据中心服务器创建一个自定义组，为远程服务器创建一个自定义组。
2. 为在不同日期和不同班次帮助 Tom 管理远程和数据中心服务器的四个管理员分别创建警报措施筛选器。
3. 创建能够由相应的警报措施筛选器触发的警报措施以自动给在相应日期和时间值班的管理员发送电子邮件。

Tom 的管理员

Tom 有三位管理员：这三位负责保持数据中心服务器的操作，他们的工作时间如下：

- Bob 在第一班现场办公，从星期一至星期五（早上 7 点至晚上 7 点）
- John 在第二班现场办公，从星期一至星期五（晚上 7 点至早上 7 点）
- Jill 在周末随呼办公，从星期五晚上 7 点到星期一早上 7 点

因此，Tom 希望将 IT Assistant 配置为：

- 任何时候数据中心服务器出现警告或严重事件时通过电子邮件通知 Bob、John 和他自己
- 通过电子邮件向 Jill 报告任何警告或严重事件，不过仅限于她随呼办公期间发生的事件

创建自定义组

Tom 需要两个自定义组来管理将对 1,000 个服务器的严重和警告事件执行操作的四位技术人员的通知。 自定义组是远程服务器和数据中心服务器。

1. 从 IT Assistant 菜单栏，选择**“Views”（视图）→“Devices”（设备）。**
2. 右击 IT Assistant 导航树中的顶层根节点，然后选择**“New Group”（新建组）**。

   “Add Group Wizard”（添加组向导）将会出现。
3. 输入想要添加组的名称和说明。

   Tom 将该组命名为**数据中心服务器**。
4. 在**“Group Membership”（组成员）**对话框中，选择要包括到新组的设备，或者，如果是基于查询的组，则从下拉式菜单选择查询。
5. 在摘要屏幕中查看选择并选择**“Finish”（完成）**完成向导或**“Back”（返回）**更改选择。
6. 重复前面的步骤创建第二个组，名为**远程服务器**。

创建警报措施筛选器

现在，Tom 将创建一个警报措施筛选器，包括为他工作的四个管理员中的每位。 在以下步骤中，您可以看到为这两种服务器创建自定义组如何使创建筛选器更方便。

创建警报措施筛选器：

1. 从菜单栏选择**“Alerts”（警报）→“Filters”（筛选器）**。

   “Alert Filters”（警报筛选器）窗口将会出现。
2. 在导航树中展开警报筛选器并右击**“Alert Action Filters”（警报措施筛选器）**。 选择**“New Action Alert Filter”（新建警报措施筛选器）**。

   “Add Filter Wizard”（添加筛选器向导）将会出现。

   Tom 计划创建三个筛选器，分别用于他准备为每个管理员创建的通知事件操作。 Tom 必须依次创建三个筛选器。 Tom 为以下计划创建筛选器：

   - 数据中心第一班（星期一至星期五，早上 7 至晚上 7）
   - 数据中心第二班（星期一至星期五，晚上 7 至早上 7）
   - 周末管理员（星期六和星期日，24 小时）
3. 为筛选器输入说明名称。

   Tom 选择将 **DC 第一班**作为第一个筛选器的名称。 为其它两个筛选器选择的名称分别是 **DC 第二班**和**周末管理员**。
4. 在**“Severity”（严重性）**下面，选择要接收警报和日志的事件的严重性。

   对于 DC 第一班筛选器，Tom 选择**“Warning”（警告）**和**“Critical”（严重）**。

单击“**Next**”（下一步）。

5. 在“**Alert Category Configuration**”（警报类别配置）下，选中“**Select All**”（全选）或选择要在警报筛选器中包括的事件类别。

   Tom 选中“**Select All**”（全选），因为他想监测企业中的所有服务器。

6. 在“**Device/Group Configuration**”（设备/组配置）下，选择与新操作警报筛选器相关的设备或组的名称。

   Tom 选择**数据中心服务器**，这是他在前面创建的一个自定义组的名称。

7. 在“**Date/Time Range Configuration**”（日期/时间范围配置）下，为任何或所有可选类别输入值。

   Tom 分别为三个筛选器选择不同的时间和星期值。 Tom 不选择日期筛选器，但如果要为假期、外部服务供应商或其它特殊情况创建筛选器和操作，则可以使用此值。

   对于 DC 第一班筛选器，Tom 启用的时间范围是早上 7:00:00 点至晚上 7:00:00 点，启用的日期是星期一至星期五。

   对于 DC 第二班筛选器，Tom 启用的时间范围是晚上 7:00:00 点至早上 7:00:00 点，启用的日期是星期一至星期五。

   对于周末管理员筛选器，Tom 启用的时间范围是早上 12:00:00 点至晚上 12:00:00 点，启用的日期是星期六和星期日。

8. 在“**Alert Action Associations**”（警报措施关联）下，选择是否要筛选器捕获的事件触发警报或写入日志文件。

   Tom 选择“**Alert**”（警报），因为他想让 IT Assistant 在系统进入严重或警告状态时通过电子邮件通知所选的管理员。

9. “**New Filter Summary**”（新筛选器摘要）显示了选择。 单击“**Finish**”（完成）接受，或单击“**Back**”（返回）进行更改。
10. 验证在步骤 3 中分配的筛选器的名称是否出现在“**Summary of Alert Actions Filters**”（警报措施筛选器摘要）窗口中。

企业环境中的通知警报措施

已配置 Tom 的警报措施筛选器和组，他现在可以为他及三位管理员设置电子邮件警报措施实现自动通知。 Tom 的策略如下：

- 设置 IT Assistant 在出现任何警告或严重事件时向管理员发送电子邮件，具体根据各位管理员的随呼或班次状况
- 给他自己抄送所有信息以便能够始终了解所有服务器事件

Tom 准备为他自己、第一和第二班的数据中心管理员以及周末管理员配置电子邮件。 因此，需要重复以下程序四次 -- 为他自己、Bob、John 和 Jill。

注：要通过 IT Assistant 发送电子邮件，企业的 SMTP 服务器必须正确配置。 要配置 SMTP 服务器，转至顶部导航栏上的“**Preferences**”（首选项）→ **Web Server**，然后配置“**SMTP Server Name (or IP Address)**”（SMTP 服务器名称[或 IP 地址]）和“**DNS Suffix for SMTP Server**”（SMTP 服务器的 DNS 后缀）。

创建警报措施

创建警报措施：

1. 从菜单栏选择“**Alerts**”（警报）→ “**Actions**”（措施）。
2. 右击导航中的“**Alert Actions**”（警报措施）并选择“**New Alert Action**”（新建警报措施）。

   “**Add Alert Action Wizard**”（添加警报措施向导）将会出现。

3. 在“**Name**”（名称）字段中给该操作取一个合理的名称。

Tom 准备为自己、Bob、John 和 Jill 配置单独的警报措施。 每次重复此程序时，他都在**“Name”（名称）**字段使用以下名称：

- Tom ADMIN MGR 电子邮件
- DC 第一班 Bob 电子邮件
- DC 第二班 Bob 电子邮件
- 周末管理员 Jill 电子邮件

4. 从**“Type”（类型）**下拉式菜单中，选择**“Email”（电子邮件）**。
5. 在**“E-mail Configuration”（电子邮件配置）**对话框中，指定有效的电子邮件地址（在企业的 SMTP 服务器组中）以接收自动通知。

注：Tom 可以使用**“Test Action”（检测操作）**按钮检测他指定的电子邮件配置。 将会发出成功/失败消息。

6. 在**“Alert Filter Association”（警报筛选器关联）**中，标识将要触发此电子邮件的警报措施筛选器。

Tom 每次执行此步骤时都会提供他在前面程序中设置的警报筛选器的名称，**DC 第一班**、**DC 第二班**或**周末管理员**。

7. 摘要对话框会显示您的选择。 单击**“Finish”（完成）**接受，或单击**“Back”（返回）**进行更改。

验证在步骤 3 中定义的警报措施是否出现在**“Summary of Alert Actions”（警报措施摘要）**窗口中。

作为 Tom 在 IT Assistant 中配置警报措施筛选器和警报措施的结果，这里是将要发生的情况：

- IT Assistant 会一直监测 Tom 网络上的所有服务器。
- 当任何服务器出现警告或严重状态，IT Assistant 会自动按照警报措施向导中指定的地址给 Tom 发送电子邮件通知。
- 当任何服务器出现警告或严重状态，IT Assistant 会自动按照警报措施筛选器向导中指定的日期范围给 Bob、John 或 Jill 发送电子邮件通知。

摘要

本章涵盖了中小型公司和大型企业网络环境中的 IT Assistant 配置。 参照此处介绍的示例将会使您能够更成功地配置 IT Assistant。

在 IT Assistant 中可以使用的功能还有很多，此处就不再一一列出。 单击 IT Assistant 中相应对话框的**“Help”（帮助）**按钮以查看有关该功能的详细联机帮助。

返回目录页

返回目录页

报告和任务管理

Dell OpenManage™ IT Assistant 7.2 版用户指南

Dell OpenManage™ IT Assistant 使用户能够：

- 为企业中的所有系统创建自定义报告
- 从中央控制台在所管理的设备上进行命令行执行，包括关机和唤醒
- 在各个 Managed System 上执行软件一致性检查和更新

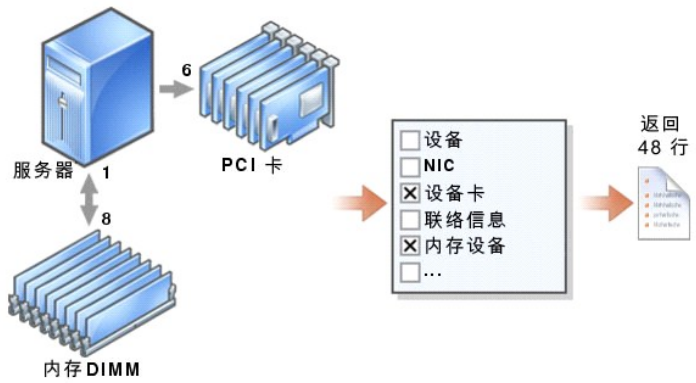
此处通过使用“配置 IT Assistant 以监视系统”中相同的用户情形展示了这些功能的基本特点。 有关这些主题的更详细信息，请参阅 IT Assistant 联机帮助。

自定义报告

IT Assistant 使用来自 Microsoft® Data Engine (MSDE) 或 SQL Server 数据库的数据创建自定义报告。 这些报告基于查找和资源清册期间收集的数据。

选择包括在报告中的设备或组对应于 IT Assistant 数据库中的字段。 执行报告时，会创建数据库查询。 下图提供了一个示例。

图 5-1. IT Assistant 中的自定义报告



例如，可以编制包含以下内容的报告：

- IT Assistant 管理的硬件设备的详情，包括服务器、交换机和存储设备
- 特定设备上的 BIOS、固件和驱动程序版本
- 其它资产或物主成本详情

可以为报告指定不同的输出格式，比如 HTML、XML 或 CSV（逗号分隔的值）。 创建的任何自定义报告模板都可以保存并以后使用。

创建新报告

要说明 IT Assistant 的报告功能，让我们再看一下 Jane 的企业：

在她的 Managed System 组中，有 50 个 Dell™ PowerEdge™ 服务器。 不过，她并不是很清楚哪些服务器装有哪种网络接口卡。 通过使用 IT Assistant 的报告工具，可以很快地回答该问题：

从 IT Assistant，Jane 会：

1. 选择**“Views”（视图）→“Reports”（报告）**，然后右击左边导航窗格中的**“All Reports”（所有报告）**。
2. 选择**“New Report”（新建报告）**。

   “Add Report”（添加报告）向导将会启动。

   她然后指定以下内容：

   - 报告的**“Name”（名称）**，名称不超过 64 个字符
   - 可选的**“Description”（说明）**
3. 在这种情况下，将选择**“Select devices/groups from the tree below”（从以下树中选择设备/组）**，然后从可用设备列表选择**“Servers”（服务器）**。

注：在设备列表中选择顶层属性会自动选中下面的所有属性。 展开树中的属性使您能够选择要包括的具体属性。 组选择的具有灰色背景的复选标记表示已在组中单独进行了选择。 具有白色背景的复选标记表示已选择了整个组。 因此，随着组成员的更改，选择将对应于修改的组成员。

4. 在**“Select Attributes”（选择属性）**下，选择了 **NIC**。
5. 然后，指定了一个首选的**“Sort by”（排序方式）**顺序。
6. 在**“Summary”（摘要）**中，既可以接受选择也可以返回进行更改。
7. 确认配置后，转至 IT Assistant 中的报告窗口并右击创建的报告名称，选择**“Execute”（执行）→“HTML Reports”（HTML 报告）**。

   将会显示一个基于 HTML 的报告，其中显示了企业中 50 个 Poweredge 服务器各自 NIC 设备的信息。

选择基于查询的报告：

Jane 还可以选择基于查询的报告。 除了在报告向导中选择**“Select devices/groups from the tree below”（从以下树中选择设备/组）**，可以转而选择**“Select a query”（选择查询）**。 然后，既可以选择先前创建的查询，也可以通过单击**“New”（新建）**按钮新建查询。 可以如下表所示指定查询报告的参数：

表 5-1. 查询报告参数

“Name of the Query”（查询的名称）	指定查询的名称。
“Query Criteria”（查询条件）	指定查询条件。 例如，要创建带有对应子网所有设备的查询条件的新查询，应指定： 其中：IP 地址以 143.166.155 开始 查询操作符有： - “Contains”（包含） — 指定查询条件字符串包含一组特定的字符。 - “Ends With”（结尾为） — 指定查询条件字符串的结尾为一组特定的字符。 - “Is”（是） — 指定查询条件字符串完全匹配这些字符。 - “Starts With”（起始为） — 指定查询条件字符串以这些字符开头。 可以将查询扩展为最多 10 个子查询，这些子查询一起组成完整的查询。 通过使用 AND/OR 操作符联接子查询。 **注：**如果在编辑现有查询期间进行了任何更改并保存了该查询，将会替换原查询。
“Run Query”（运行查询）	运行查询并显示结果。
“Save Query”（保存查询）	保存查询。
“Cancel”（取消）	关闭**“Query Editor”（查询编辑器）**窗口，而不保存输入。

注：可以单击**“Run Query”（运行查询）**在保存前检测查询。

注：如果想在 RAC 设备上运行报告，并选择**“RAC type”（RAC 类型）**作为一种包括进报告的属性，生成的报告会根据 RAC 类型列而列出 2、8 或 16 等值。 这些值映射如下：
2 = DRAC II
8 = DRAC III/DRAC 4
16 = 底板管理控制器 (BMC)

编辑、删除或运行报告

无论创建了哪种报告，Jane 都可以通过右击**“Reports”（报告）**窗口中的报告名称来编辑、删除、重命名或运行它。

预定义的报告

IT Assistant 提供了几种预定义的报告，可以立即拿来使用。 这些报告会显示在**“Reports”（报告）**窗口的左边。 单击报告的名称查看该报告所要收集的信息的摘要。

IT Assistant 数据库架构信息

设备表中的行表示网络中的设备。 IT Assistant 收集的数据存储在相关表中并且由 **DeviceId** 这种内部标识符来链接。

相关数据存储在以下表中。

注：表的主键用星号 (*) 标记。

表 5-2. IT Assistant 数据库架构

列名	数据类型	数据大小	允许空值	说明
设备表				
DeviceId*	int	4	否	在所有相关表中用作外键的内部设备标识。
DeviceName	nvarchar	256	是	IT Assistant 用于标识设备的名称，是在用户界面 (UI) 的**“Device Tree”（设备树）**中显示的名称。
DeviceInstrumentationName	nvarchar	256	是	从 MIB II SysName 或 CIM 检索的设备的名称。
DeviceDNSName	nvarchar	256	是	计算机系统名称
DeviceType	int	4	是	设备的类型。 工作站 = 3 服务器 = 4 台式机 = 5 便携式计算机 = 6 网络交换机 = 8 RAC = 9 KVM = 10 未知 = 2 或任何未列出的值
DeviceInventoryTime	datetime	8	是	IT Assistant 从设备收集资源清册数据的最后时间。
DeviceStatusedTime	datetime	8	是	IT Assistant 上次从设备收集全局运行状况数据的时间。
DeviceDiscoveredTime	datetime	8	是	IT Assistant 上次查询系统以确定有哪些代理程序的时间。
DeviceProtocols	int	4	是	位掩码指明设备支持哪些协议。 位 1 = SNMP 位 4 = CIM
DevicePreferredProtocol	int	4	是	远程设备首选的管理协议。 1 = SNMP 2 = CIM
DeviceAssetTag	nvarchar	64	是	此属性定义设备的资产标签。

DeviceServiceTag	nvarchar	64	是	此属性定义设备的服务标签。
DeviceSystemId	int	4	是	制造商的系统型号 ID。
DeviceSystemModelType	nvarchar	64	是	制造商的型号名称。
DeviceLocation	nvarchar	256	是	从远程代理程序检索的设备位置。
DellSystem	int	4	是	此布尔值标志指示设备是否是 Dell 启用的代理程序。
SubnetLastDiscoveredOn	nvarchar	256	是	用于查找设备的上一个查找范围。
代理程序表				
DeviceId*	int	4	否	到设备表的外键。
AgentName*	nvarchar	256	否	代理程序的名称。
AgentVersion	nvarchar	64	是	代理程序的版本。
AgentManufacturer	nvarchar	64	是	代理程序的制造商。
AgentDescription	nvarchar	256	是	代理程序所管理内容的简短说明。
AgentGlobalStatus	int	4	是	代理程序的全局状况。 不知道 = 0 未知 = 1 正常 = 4 警告 = 8 严重 = 16
AgentInstallTime	datetime	8	是	代理程序的安装时间（如果有的话）。
AgentId	int	4	是	用于在代理程序间相互区别的内部 ID。 RAC 带外代理程序 = 1 Server Administrator = 2 Microsoft WMI =3 OMCI = 4 DRAC II = 5 Array Manager = 6 Storage Manager = 7 Dell PowerEdge 1655MC 交换机 = 8 Dell PowerConnect™ 3248 = 9 PowerConnect 5224 = 10 PowerConnect 3024 = 11 PowerConnect 5012 = 12 PowerConnect 3048 = 13 PowerConnect 3000MIB = 14 KVM = 15 资源清册代理程序 = 16 RAC 带内代理程序 = 17
AgentURL	nvarchar	256	是	管理应用程序的 Web 地址（如果代理程序支持 Web 地址）。
AgentData	ntext	16	是	扩展代理程序数据；仅供内部使用。
阵列磁盘表				
DeviceId*	int	4	否	到设备表的外键。
ArrayDiskNumber*	int	4	否	该阵列磁盘项的实例号。
ArrayDiskName	nvarchar	256	是	Storage Management 中表示的阵列磁盘名称。
ArrayDiskVendorName	nvarchar	64	是	阵列磁盘转售商的名称。
ArrayDiskModelNumber	nvarchar	64	是	阵列磁盘的型号。
ArrayDiskSerialNumber	nvarchar	64	是	制造商设置的阵列磁盘唯一标识号。
ArrayDiskRevision	nvarchar	64	是	阵列磁盘的固件版本。
ArrayDiskEnclosureId	nvarchar	64	是	阵列磁盘所属机柜处理器的 SCSI ID。
ArrayDiskChannel	int	4	是	此阵列磁盘连接的总线。
ArrayDiskLength	int	4	是	阵列磁盘的大小（兆字节）。 如果大小是 0，则它比一个兆字节要小。
ArrayDiskBusType	nvarchar	64	是	阵列磁盘的总线类型。 可能的值：SCSI、IDE、Fibre Channel、SSA、USB 和 SATA。
ArrayDiskTargetId	int	4	是	此阵列磁盘分配的 SCSI 目标 ID。
ArrayDiskLUNId	int	4	是	此阵列磁盘的持久唯一 ID。
控制器表				
DeviceId*	int	4	否	到设备表的外键。
ControllerNumber*	int	4	否	该控制器项的实例号。
ControllerName	nvarchar	64	是	Storage Management 中表示的该子系统中控制器的名称。 包括控制器类型和实例，例如：PERC 3/QC 1。
ControllerVendor	nvarchar	64	是	控制器转售商的名称。
ControllerType	nvarchar	64	是	控制器的类型。
ControllerState	nvarchar	64	是	控制器子系统的当前情况。
ControllerStatus	int	4	是	控制器的状态
ControllerFWVersion	nvarchar	64	是	控制器的当前固件版本。
ControllerCacheSize	int	4	是	控制器的当前高速缓存内存量。

ControllerPhysicalDeviceCount	int	4	是	控制器通道上物理设备的数目，包括磁盘和控制器。
ControllerLogicalDeviceCount	int	4	是	控制器上虚拟磁盘数。
ControllerPartnerStatus	nvarchar	64	是	表示冗余配置中冗余控制器的可用性情况。
ControllerMemorySize	int	4	是	控制器上内存数量。
ControllerDriveChannelCount	int	4	是	冗余控制器驱动器信道数。
ControllerChargeCount	int	4	是	此控制器上电池充电的次数。
ControllerDriverVersion	nvarchar	64	是	此控制器当前所装驱动程序版本。
机柜表				
DeviceId*	int	4	否	到设备表的外键。
EnclosureNumber*	int	4	否	该机柜项的实例号。
EnclosureName	nvarchar	256	是	机柜的名称。
EnclosureVendor	nvarchar	256	是	机柜转售商的名称。
EnclosureId	int	4	是	处理器的 SCSI 地址。
EnclosureServiceTag	nvarchar	64	是	咨询客户支持部门时使用的机柜标识。
EnclosureAssetTag	nvarchar	64	是	机柜的用户可定义资产标签。
EnclosureAssetName	nvarchar	64	是	机柜的用户可定义的资产名称。
EnclosureProductId	nvarchar	64	是	机柜的产品标识，也对应于机柜类型。
EnclosureType	nvarchar	64	是	机柜类型。
EnclosureChannelNumber	int	4	是	机柜连接的通道号或总线。
EnclosureBackplanePartNum	nvarchar	64	是	机柜背板的部件号。
EnclosureSCSIId	int	4	是	此机柜所连控制器的 SCSI ID。
机柜管理模块表				
DeviceId*	int	4	否	到设备表的外键。
EMMNumber*	int	4	否	该机柜管理模块的实例号。
EMMName	nvarchar	256	是	机柜的名称。
EMMVendor	nvarchar	256	是	管理模块转售商的名称。
EMMPartNumber	nvarchar	64	是	该机柜内存模块的部件号。
EMMFWVersion	nvarchar	64	是	机柜内存模块的固件版本。
虚拟磁盘表				
DeviceId*	int	4	否	到设备表的外键。
VirtualDiskNumber*	int	4	否	该虚拟磁盘项的实例号。
VirtualDiskName	nvarchar	256	是	由 Storage Management 生成的或由用户输入的虚拟磁盘标签。
VirtualDiskDeviceName	nvarchar	256	是	该虚拟磁盘的成员磁盘使用的设备名称。
VirtualDiskLength	int	4	是	虚拟磁盘的大小 (MB)。
VirtualDiskWritePolicy	nvarchar	64	是	表示在写入虚拟磁盘时是否将使用控制器的写入高速缓存。
VirtualDiskReadPolicy	nvarchar	64	是	表示在从虚拟磁盘读取时是否将使用控制器的读取高速缓存。
VirtualDiskCachePolicy	nvarchar	64	是	表示在对虚拟磁盘进行读取或写入时是否将使用控制器的高速缓存。
VirtualDiskLayout	nvarchar	64	是	虚拟磁盘的 RAID 类型。
VirtualDiskStripeSize	int	4	是	虚拟磁盘的条带大小（以字节为单位）。
VirtualDiskTargetId	int	4	是	虚拟磁盘的唯一 ID。
卷表				
DeviceId*	int	4	否	到设备表的外键。
VolumeNumber*	int	4	是	卷项的实例号。
VolumeDriveLetter	nvarchar	64	是	根据操作系统的卷路径（或驱动器号）。
VolumeLabel	nvarchar	256	是	此卷的用户可定义标签。
VolumeSize	int	4	是	卷的大小 (MB)。
固件表				
DeviceId*	int	4	否	到设备表的外键。
FirmwareChassisIndex*	int	4	否	固件机箱索引（基于零）。
FirmwareIndex*	int	4	否	固件索引（基于 0）。
FirmwareType	nvarchar	64	是	固件类型。
FirmwareName	nvarchar	64	是	固件的名称。
FirmwareVersion	nvarchar	64	是	固件版本。

内存设备表				
DeviceId*	int	4	否	到设备表的外键。
MemoryDeviceChassisIndex*	int	4	否	此属性定义相关机箱的索引（基于 1）。
MemoryDeviceIndex*	int	4	否	此属性定义内存设备的索引（基于 1）。
MemoryDeviceName	nvarchar	256	是	此属性定义内存设备的位置。
MemoryDeviceBankName	nvarchar	256	是	此属性定义内存设备内存区的位置。
MemoryDeviceType	nvarchar	256	是	此属性定义内存设备的类型。
MemoryDeviceFormFactor	nvarchar	256	是	此属性定义内存设备的外形尺寸。
MemoryDeviceSize	int	4	是	此属性定义内存设备的大小。
MemoryDeviceFailureMode	nvarchar	256	是	此属性定义内存设备的故障模式。
NIC 表				
DeviceId*	int	4	否	到设备表的外键。
NICId*	int	4	否	NIC 的唯一实例 ID。
NICIPAddress	nvarchar	40	是	分配给 NIC 的 IP 地址。
NICNetmask	nvarchar	40	是	分配给 NIC 的子网掩码。
NICMACAddress	nvarchar	24	是	NIC 的 MAC 地址。
NICManufacturer	nvarchar	256	是	NIC 的转售商。
NICPingable	int	4	是	表示 IT Assistant 使用此 IP 地址与设备通信的标志。
操作系统表				
DeviceId*	int	4	否	到设备表的外键。
OSId*	int	4	否	操作系统的实例 ID。
OSName	nvarchar	64	是	操作系统的名称。
OSRevision	nvarchar	64	是	操作系统修订（例如，Microsoft Windows® Service Pack 或 Linux 内核版本）
OSTotalPhysicalMemory	int	4	是	操作系统报告的总物理内存 (MB)。
OSLocale	nvarchar	64	是	操作系统的区域设置。
OSType	int	4	是	操作系统的类型。
电源设备表				
DeviceId*	int	4	否	到设备表的外键。
PowerSupplyChassisIndex*	int	4	否	此属性定义机箱的索引（基于 1）。
PowerSupplyIndex*	int	4	否	此属性定义电源设备的索引（基于 1）。
PowerSupplyType	nvarchar	256	是	此属性定义电源设备的类型。
PowerSupplyLocation	nvarchar	256	是	此属性定义电源设备的位置。
PowerSupplyOutputWatts	int	4	是	此属性定义电源设备的最大持续输出瓦数（十分之一瓦为单位）。
处理器表				
DeviceId*	int	4	否	到设备表的外键。
ProcessorChassisIndex*	int	4	否	此属性定义机箱的索引（基于 1）。
ProcessorCores	int	4	是	此属性定义为处理器设备检测的处理器核心数。
ProcessorIndex*	int	4	否	此属性定义处理器的索引（基于 1）。
ProcessorFamily	nvarchar	256	是	此属性定义处理器设备的系列。
ProcessorCurrentSpeed	int	4	是	此属性定义处理器设备的当前速度 (MHz)。 零表示当前速度未知。
ProcessorSlotNumber	int	4	是	此属性定义处理器占用的插槽。
SMBIOS 表				
DeviceId*	int	4	否	到设备表的外键。
ParallelPortConfiguration	nvarchar	64	是	定义并行端口配置。
ParallelPortMode	nvarchar	64	是	并行端口的模式。
SerialPortYesConfiguration	nvarchar	64	是	定义串行端口 1 配置。
SerialPort2Configuration	nvarchar	64	是	定义串行端口 2 配置。
IDEController	nvarchar	64	是	定义 IDE 控制器是已启用还是已禁用。
BuiltinNIC	nvarchar	64	是	定义内置 NIC 是已启用还是已禁用。
BuiltinFloppy	nvarchar	64	是	定义内置软盘控制器是已启用、自动，还是只读。
BuiltinPointingDevice	nvarchar	64	是	定义内置定点设备（鼠标）端口是已启用还是已禁用。
WakeupOnLAN	nvarchar	64	是	定义通过 LAN 唤醒是禁用，仅为机载 NIC 启用，还是仅为添加式 NIC 启用。 如果选中 **“Enabled with boot to NIC”（启用引导至 NIC）**选项，则系统会在远程唤醒时从 NIC 引导 ROM 启动。

WakeupOnLANMethod	nvarchar	64	是	定义系统支持的通过 LAN 唤醒方法。
AutoOn	nvarchar	64	是	定义自动启动配置：禁用、每天或工作日（星期一-星期五）。
AutoOnHour	nvarchar	64	是	定义系统开机时的小时 (0-23)。
AutoOnMinute	nvarchar	64	是	定义系统开机时的分钟 (0-23)。
BootSequence	nvarchar	64	是	定义下次系统引导的引导顺序。
ChassisIntrusionStatus	nvarchar	64	是	报告系统有关**“Chassis Intrusion”（机箱侵入）**的状况（**“Detected”[已检测到]**或**“Not Detected”[未检测到]**）。 **“Unknown”（未知）**值表示本系统不支持机箱侵入检测，或者用户已禁用机箱侵入事件报告。 如果值是**“Detected”（已检测到）**，可以将其设置为**“Not Detected”（未检测到）**以使系统能够接收下一个事件并从现在起停止生成事件。
IntegratedAudio	nvarchar	64	是	系统内置声音设备的状态。
PCISlots	nvarchar	64	是	系统添加式 PCI 插槽的状态（已启用/已禁用）。
USBPorts	nvarchar	64	是	USB 端口的状态（on/off [开/关]）。
软件资源清册表				
DeviceId*	int	4	否	到设备表的外键。
ComponentId	nvarchar	64	是	软件的组件标识符。
InstanceId*	nvarchar	32	否	硬件的实例标识符。
HWDeviceId	nvarchar	16	是	PCI ID 的硬件设备标识符。
HWVendorId	nvarchar	16	是	PCI ID 的硬件供应商标识符。
HWSubDeviceId	nvarchar	16	是	PCI ID 的硬件子设备标识符。
HWSubVendorId	nvarchar	16	是	PCI ID 的硬件子供应商标识符。
SubComponentId	nvarchar	64	是	硬件的子组件标识符。
HWDescription	nvarchar	128	是	硬件的说明。
SoftwareType	nvarchar	64	是	软件的类型，例如，驱动程序 (DRVR)，固件 (FRMW) 等。
SoftwareVersion	nvarchar	64	是	软件版本号。
SoftwareDescription	nvarchar	128	是	软件的说明。
软件资源清册操作系统表				
DeviceId*	int	4	否	到设备表的外键。
OSVendor	nvarchar	64	是	操作系统供应商的名称。
OSMajorVersion	nvarchar	16	是	操作系统的主要版本。
OSMinorVersion	nvarchar	16	是	操作系统的次要版本。
OSSPMajorVersion	nvarchar	16	是	Service Pack 主要版本。
OSSPMinorVersion	nvarchar	16	是	Service Pack 次要版本。
交换机设备表				
DeviceId*	int	4	否	到设备表的外键。
SwitchIndex*	int	4	否	交换机的索引。
SwitchAssetTag	nvarchar	255	是	交换机的资产标签。
SwitchServiceTag	nvarchar	255	是	交换机的服务标签。
SwitchSerialNumber	nvarchar	255	是	交换机的序列号。
物主成本表				
DeviceId*	int	4	否	到设备表的外键。
CooIndex*	int	4	否	物主成本的索引。
PurchaseCost	nvarchar	64	是	系统的初始购买成本。
WayBillNumber	nvarchar	64	是	运货单号。
InstallationDate	nvarchar	64	是	系统安装日期。
PurchaseOrderNumber	nvarchar	64	是	订单号。
PurchaseDate	nvarchar	64	是	系统购买日期。
SigningAuthorityName	nvarchar	64	是	签署机构引用。
OriginalMachineConfigurationExpensed	nvarchar	64	是	支出的原始系统配置。
OriginalMachineConfigurationVendorName	nvarchar	64	是	原始系统配置供应商名称。
CostCenterInformationVendorName	nvarchar	64	是	成本中心信息供应商名称。
UserInformationUserName	nvarchar	64	是	用户名。
ExtendedWarrantyStartDate	nvarchar	64	是	延长保修开始日期。
ExtendedWarrantyEndDate	nvarchar	64	是	延长保修结束日期。
ExtendedWarrantyCost	nvarchar	64	是	延长保修成本。
ExtendedWarrantyProviderName	nvarchar	64	是	延长保修供应商名称。
OwnershipCode	nvarchar	64	是	所有权代码。

CorporateOwnerName	nvarchar	64	是	物主姓名。
HazardousWasteCodeName	nvarchar	64	是	有害废物代码名称。
DeploymentDateLength	nvarchar	64	是	部署日期长度。
DeploymentDurationUnitType	nvarchar	64	是	部署期限单位类型。
TrainingName	nvarchar	64	是	培训名称。
OutsourcingProblemDescription	nvarchar	64	是	外包问题说明。
OutsourcingServiceFee	nvarchar	64	是	外包服务费。
OutsourcingSigningAuthority	nvarchar	64	是	外包签署机构。
OutsourcingProviderFee	nvarchar	64	是	外包供应商费。
OutsourcingProviderServiceLevel	nvarchar	64	是	外包供应商服务级别。
InsuranceCompanyName	nvarchar	64	是	保险公司名称。
BoxAssetTagName	nvarchar	64	是	设备资产标签。
BoxSystemName	nvarchar	64	是	设备的操作系统名称。
BoxCPUSerialNumberName	nvarchar	64	是	设备的 CPU 序列号。
DepreciationDuration	nvarchar	64	是	折旧期限。
DepreciationDurationUnitType	nvarchar	64	是	折旧期限单位。
DepreciationPercentage	nvarchar	64	是	折旧百分比。
DepreciationMethod	nvarchar	64	是	折旧方法。
RegistrationIsRegistered	nvarchar	64	是	已注册。
联络信息表				
DeviceId*	int	4	否	到设备表的外键。
ContactName*	nvarchar	64	否	联系人姓名。
ContactInformation	nvarchar	64	是	此联系人的信息。
ContactDescription	nvarchar	64	是	此联系人的说明。
群集表				
DeviceId*	int	4	否	到设备表的外键。
ClusterIndex*	int	4	否	群集索引。
ClusterType	int	4	是	群集类型。
ClusterTypeName	nvarchar	64	是	群集类型名称。
ClusterName	nvarchar	255	是	群集名称。
ClusterDescription	nvarchar	255	是	群集说明。

软件更新

IT Assistant 提供了一种集中软件更新功能。 可以将 Dell Update Packages 和系统更新集载入中央存储库，然后使用该更新软件包对企业中的所有系统运行一致性检查。 系统更新集是一个 Dell Update Packages 逻辑集，旨在启用软件包排序并尽量减少系统重新引导。 Dell Update Packages 可从 Dell 支持站点 **support.dell.com** 或 *Dell PowerEdge Updates* CD 获得。 该 CD 可从 Dell OpenManage Subscription Service 获得或作为 ISO 映像从 **support.dell.com** 下载。 可以下载从 **www.dell.com** 订购的 OpenManage Subscription Service。

Dell PowerEdge Updates CD 包含 Dell Update Packages 和系统更新集（特定 PowerEdge 平台的已认证软件包集）的季度更新。

要在 IT Assistant 中使用 Dell Update Packages，应执行下列步骤：

1. 导航到 **“Manage”（管理）→ “Software Updates”（软件更新）**
2. 右击根节点（**“Software Update Repositories”[软件更新存储库]**）并选择 **“Open Repository (Update CD)...”（打开存储库 [Update CD]...）**。
3. 将 *Dell PowerEdge Updates* CD 插入 CD 驱动器。
4. 导航到 CD 位置并定位存储库目录。
5. 选择 **catalog.xml** 并单击 **“Open”（打开）**。
   Dell PowerEdge Updates CD 中的内容将能在 IT Assistant 中使用。 随后可以执行一些操作，比如导入软件包，执行一致性检查和执行软件更新。

在 IT Assistant 中使用软件更新

让我们来看看 Jane 如何在企业中使用这种功能。

Jane 已从 Dell 支持站点 **support.dell.com** 下载了更新软件包。 她知道有些系统需要其中包含的固件升级，不过她想确定是哪些系统而不用对 50 个服务器逐一手动检查。 可以通过 IT Assistant 快速找出这些信息。

这里是她将要采取的步骤：

1. 选择“**Manage**”（管理）→ “**Software Updates**”（软件更新）。
2. 右击左边导航窗格中的“**IT Assistant Repository**”（**IT Assistant** 存储库）并选择“**Add**”（添加）。

   Jane 浏览到系统上下载有更新软件包的位置。 该软件包可能在 CD 上是 **catalog.xml** 文件或另一个文件名。 当高亮度显示该文件名并单击“**Open**”（打开）时，IT Assistant 将它添加到窗口中。
3. 单击左手窗格中的更新软件包名称会在右手窗格中显示其内容摘要。
4. 单击“**Compliance**”（一致性）选项卡，然后选择使用软件包检查的一组具体设备（或查询）。
5. 单击“**Compare**”（比较）根据更新软件包内容检查所选设备。

   IT Assistant 会执行比较并生成一致性报告，报告中以图标形式显示找到的差异、所选设备的完整版本信息，以及可以帮助标识不兼容系统或设备的其它信息。
6. 如果 IT Assistant 找到需要更新的服务器或设备，Jane 可以选择需要更新哪些并单击“**Update**”（更新）按钮。 这会自动启动“**Software Updates**”（软件更新）任务向导。

注：不能在运行 IT Assistant 的系统上升级固件。 要升级此系统上的固件，从另一个系统运行软件更新。

管理任务

IT Assistant 也允许远程在企业的 Managed System 上运行某些任务。 这些任务包括：

- 常用命令行执行（如果启用了 Dell OpenManage 4.3 或更高版本设备，还支持远程调用 Dell OpenManage Server Administrator 命令行界面）
- 设备控制，包括关机和唤醒
- 计划的软件更新
- 能够远程执行智能平台管理接口 (IPMI) 命令
- 能够远程执行远程客户设备命令

注：如果 IT Assistant 没有检测到 IT Assistant 服务层装有必需的组件，IPMI 和远程客户设备命令行选项可能不可用。

可以配置这些任务按特定计划运行或立即执行。 有关详情，请参阅 IT Assistant 联机帮助。

创建设备控制任务

例如，Jane 想重新引导一个有问题的服务器（该服务器已通过 IT Assistant 发送了几次电子邮件警报）。 要在 IT Assistant 中执行此任务，需要：

1. 在左边导航窗格中选择“**Manage**”（管理）→ “**Tasks**”（任务）并右击“**Device Control**”（设备控制）。
2. 选择“**New Task**”（新建任务）。

   “Task Creation”（任务创建）向导将会启动。
3. Jane 会输入“**Task Name**”（任务名称），然后从“**Task Type**”（任务类型）下拉式菜单选择“**Shutdown Device**”（关闭设备）。
4. 从“**Select Shutdown Type**”（选择关闭类型）窗口选择“**Reboot**”（重新引导）。
5. 在“**Select Devices**”（选择设备）窗口，展开“**Servers**”（服务器）设备列表并只选择要重新引导的服务器。

6. 在**“Select Schedule”（选择计划）**中，选择**“Run Now”（立即运行）**。
7. 如果准备重新引导启用 SNMP 的系统，必须在**“Enter Credentials”（输入凭据）**窗口输入设备用户名和密码。 如果系统启用了 CIM，则必须输入完全限定域用户名和密码。
8. 在**“Summary”（摘要）**窗口中，既可以确认选择也可以选择**“Back”（返回）**进行更改。

指定的服务器将会在选择**“Finish”（完成）**后立即重新引导。

Jane 也可以选择对组中的设备加电，方法是在**“Task Creation”（任务创建）**向导中选择**“Wake Up Device”（唤醒设备）**作为**“Task Type”（任务类型）**。 也可以计划任务在指定时间运行，而不是立即运行。

IT Assistant 中可用的其它任务

IT Assistant 中可用的其它任务包括：

常用命令行

从下拉式菜单选择**“Generic Command Line”（常用命令行）**使您能够在网络中执行命令。 **“Remote Server Administrator Command Line”（远程 Server Administrator 命令行）**使您能够远程执行 Server Administrator 命令行界面 (CLI) 命令。

有关 IT Assistant 接受的参数的完整列表，请参阅联机帮助。

软件更新

选择**“Server Software Upgrade”（服务器软件升级）**使您能够完全自定义 Managed System 上的软件升级过程，包括为升级的每个组件定义单独的计划。

有关各个任务及其功能的完整说明，请参阅 IT Assistant 联机帮助。

IPMI 命令行

从下拉式菜单选择**“IPMI Command Line”（IPMI 命令行）**使您能够执行 IPM 命令。

有关其它信息，请参阅联机帮助。

远程客户设备命令行

选择**“Remote Client Instrumentation Command Line”（远程客户工具命令行）**使您能够远程执行客户设备命令。

有关其它信息，请参阅联机帮助。

返回目录页

返回目录页

确保安全 Dell OpenManage IT Assistant 安装

Dell OpenManage™ IT Assistant 7.2 版用户指南

本节讨论几个具体的主题，这些主题对于实现更安全的 Dell OpenManage™ IT Assistant 安装很有好处。 IT Assistant 采用了 HTTPS 进行安全通信，并且采用了 Microsoft® Active Directory 实现基于角色的访问。

有关 Dell OpenManage 平台安全性的详情，包括 IT Assistant，请参阅《*Dell OpenManage 安装和安全性用户指南*》。

TCP/IP 信息包端口安全

TCP/IP 信息包将请求传递给目标系统。 此信息包中包括的是一个与特定应用程序相关的端口号。 IT Assistant 通过指定 `https://<主机名>:<端口号>`来访问。 默认端口号为 2607。 使用 `https` 需要所用的应用程序按照安全套接层 (SSL) 规范对数据进行加密，以便观察者无法通过在网络上监测信息包来取得和读取密码等敏感信息。 然后通过 IT Assistant 登录页并根据在 Active Directory 或本地操作系统映射的用户角色检查用户凭据来对用户进行验证。 有关 IT Assistant 支持的三种角色的信息，请参阅 “基于角色的访问安全性管理”。

注：IT Assistant 用户界面通过端口 2607 与 IT 服务层通信。

保护管理型台式机、便携式计算机和工作站的安全

保护 Managed System 操作系统的安全

促进安全网络环境的第一步是确保所有 Managed System 操作系统在运行最新的 Service Pack 和/或任何附加的关键安全修补程序。 为简化此进程，Microsoft 推出了 Software Update Services。 请参阅 **Microsoft 网站**。 为其它 Managed System 的操作系统执行相同的更新。

会话超时

IT Assistant 用户界面会话可以配置为在一段定义的非活动期后超时。 要配置会话超时间隔，单击 IT Assistant 导航栏顶部的 **“Preferences”（首选项）**并选择 **“Web Server Properties”（Web Server 属性）**。 既可以完全禁用会话超时，也可以允许多达 30 分钟的非活动时间。

ASF 和 SNMP 协议

从 Dell™ OptiPlex™ GX260 系统开始，最后一个安全考虑是为警报标准格式 (ASF) 提供支持的集成网络接口控制器 (NIC)。 ASF 发出与系统状况和安全问题相对应的平台事件陷阱 (PET)。 由于 SNMP 协议支持这些陷阱，因此 Managed System NIC 必须配置运行 IT Assistant 的 Management Station 的 IP 地址和团体字符串。

总之，要按照以上段落中介绍的安全措施成功安全地管理台式机、便携式计算机和工作站，系统管理员应遵守以下最佳做法：

- 确保操作系统是最新的，并且具有最新的操作系统安全修补程序。
- 对于具备 ASF 功能的台式机，禁用 ASF 或实现不容易猜中的 SNMP 团体名称。

保护管理型服务器系统的安全

保护 Managed System 操作系统的安全

对于台式机和工作站，服务器安全的第一步是确保它在运行最新的 Service Pack，并且安装了相应的关键修补程序。 上节中提到的 Microsoft Software Update Services 也应用于 Microsoft Windows® 2000 和 Windows Server™ 2003 服务器。 应为 Red Hat® Linux 和 Novell® NetWare® 检查类似服务。

选择最安全的 Managed System 服务器协议

Dell OpenManage Server Administrator 是当前的 Dell 服务器工具软件，使用可在自定义安装期间配置的 SNMP 和 CIM 协议。

CIM 监测、DCOM 和 Windows 验证

使用 DCOM 安全的 CIM 协议可以利用 Windows 挑战/响应（用户 ID/密码）验证。 此外，通过在每个所配置 IT Assistant 查找范围中指定的域/用户 ID/密码帐户建立与 Managed System 的通信。 这些帐户的格式为 **<域名>\<用户名>**或 **localhost\<用户名>**。

注：可以使用 **dcomcnfg.exe**、**wmimgmt.msc** 和 **wbemcntl** 等公用程序更改 WMI 安全。 但是，由于可能存在不希望的负面效果，建议不要通过这些方法实现更改。 有关详情，请参阅 Microsoft 网站。

注：即使在仅使用 CIM 进行监测的环境中，通常也启用 SNMP，因为 Server Administrator 仅使用 SNMP 陷阱提供错误通知。

安全和 SNMP 协议

您可以执行多个操作，使用 SNMP 协议进一步提高环境的安全性。 尽管以下实例适用于 Microsoft Windows 操作系统，但可以为 Red Hat Linux 和 Novell NetWare 操作系统执行类似的步骤。 默认情况下，安装 SNMP 时，团体名称设为 **public**。 此字符串应像密码一样处理，并且在选择中应使用类似的规则 — 字符串足够长，不容易猜中，并且最好由字母和数字混合而成。 在 Windows 操作系统中，可以通过 SNMP 服务 **“Property”（属性）**对话框的 **“Security”（安全）**选项卡配置 SNMP 团体名称。

作为辅助预防措施，SNMP 还应设为 **“Read Only”（只读）**，以防止未授权配置和控制操作。 这可以通过在安装 Server Administrator 时通过使用 **snmpsets=no** 选项强制实现。 也仍然可以通过 Server Administrator 的用户界面或命令行界面 (CLI) 进行更改。 此外，还可以将 SNMP 服务配置为仅从特定服务器（此时为运行 IT Assistant 的系统）接受请求。 这还可以在 Windows **“Security”（安全）**选项卡上进行配置，方法是选择标记为 **“Accept SNMP packets from these hosts”（从这些主机接受 SNMP 信息包）**的单选按钮，然后单击 **“Add”（添加）**以输入运行 IT Assistant 的系统的地址或名称。

注：为确保正确配置所有系统，建议您使用 Group Policies in Active Directory 等工具强制执行这些 SNMP 设置。

作为最终的安全步骤，Server Administrator 应配置为拒绝访问用户和可能的高级用户帐户，从而仅限制对管理员帐户的访问。 这可以通过选择 **“Preference”（首选项）**，然后取消复选 **“User Access”（用户访问）**框，通过 Server Administrator 顶部导航栏来实现。 您还可以使用 Server Administrator CLI 命令 **omconfig preferences useraccess enable= admin** 限制用户访问。 有关详情，请参阅 **support.dell.com** 或说明文件 CD 上的 *Server Administrator 命令行界面用户指南*。

总之，要按照此处介绍的安全措施成功正确地管理服务器，系统管理员应遵守以下最佳做法：

- 确保操作系统是最新的，并且具有最新的操作系统安全修补程序。
- 使用 SNMP 和 CIM (Server Administrator) 协议。
- 实现不容易猜中的 SNMP 团体名称。
- 将 SNMP 配置为**只读**，以便将配置、更新和高级控制仅限于 Server Administrator。
- 配置 SNMP 以便仅从运行 IT Assistant 的系统的 IP 地址接受请求。
- 使用 Group Policies in Active Directory 等工具强制所有要管理服务器的 SNMP 设置。
- 将 Server Administrator 配置为拒绝用户级访问。

在使用 IT Assistant 时确保数据库安全

如果在安装 IT Assistant 时未检测到 SQL Server 数据库，则该进程将安装 MSDE 2000 的副本，它设置为仅限于信任或 Windows 的验证模式。 但是，可能以前已安装 MSDE 或 SQL Server 的其它应用程序，包括 IT Assistant 的以前版本，往往会选择 SQL 的验证模式或混合模式，它允许 SQL Server 管理自己的用户 ID 和密码。 在 IT Assistant 的早期版本中，高级用户或帐户密码设置为 null 或 dell。 至少，通过将这些密码更改为符合上述最佳做法要求的字符串，可以降低网络入侵的可能性。 较好的一种选择是将数据库验证模式更改为仅限于信任或 Windows。

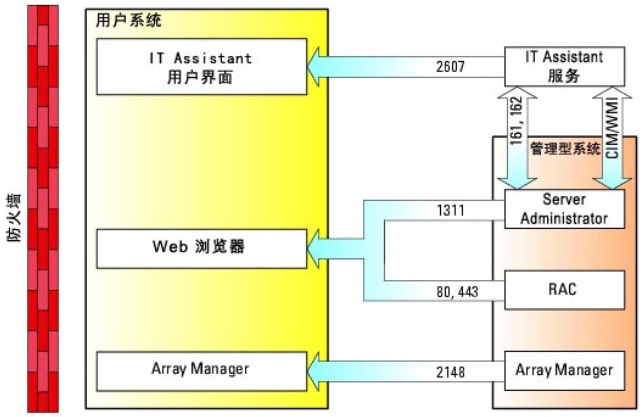
在防火墙后面运行 IT Assistant

图 6-1 显示了 IT Assistant 和所管理系统驻留在防火墙后面的典型安装。 防火墙将所保护网络和外界之间在指定端口上的通信隔断，而与此同时仍然允许管理员与 IT Assistant 和 Managed System 自由通信。

在防火墙后面环境中运行 IT Assistant 的系统的典型安全包括：

- 使用信任的帐户，而不是数据库的指定或混合帐户。
- 将用户接口连接限制到已知系统。

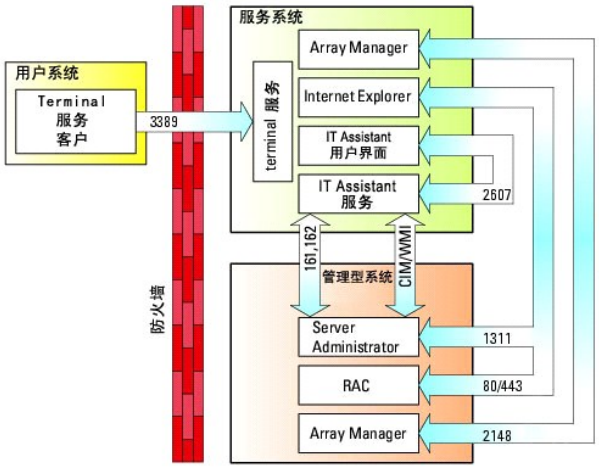
图 6-1. 防火墙后面的典型安装



为 IT Assistant 访问设置附加安全

本节到此，已讨论了有关 IT Assistant 和 Managed System 之间现有 TCP/IP 连接的安全问题。 除了这些安全预防措施外，Microsoft 终端服务仅允许具有管理员帐户（管理模式）的用户随意远程连接，它还可用于限制用户界面连接到运行 IT Assistant 用户界面和服务的系统。 图 6-2 中显示了利用终端服务的网络实例。

图 6-2. 使用终端服务取得附加安全



在图 6-2 中，用户可以通过本地安装的终端服务客户机或 Windows XP 远程桌面连接，连接到 IT Assistant Management Station 。 此连接需要有效的域/用户 ID/密码。 有关详情，请参阅 Microsoft 网站。

通过在所有 Managed System 上将限制设置为仅从运行 IT Assistant 用户界面（[UI] 即网络 Management Station）的系统的 IP 地址中接受 SNMP 通信量来实现附加的安全级别。 由于终端服务和远程桌面会话仿真直接来自网络 Management Station 的通信量，因此对 IT Assistant 的访问仅限于终端服务客户机或本地网络 Management Station 用户。 任何其它连接，例如，另一个远程 IT Assistant 用户界面安装，将无法与网络中正确配置的 Managed System 进行有效通信，因为标识为源自非网络 Management Station 系统的通信量将被拒绝。

注：终端服务是可以在管理员或应用程序模式中安装的 Microsoft Windows 2000 和 Microsoft Windows Server 2003 的可选组件。

注：如果以管理模式安装终端服务，最多两个用户可以登录（只要他们是管理员组的成员）。 如果以应用程序模式安装终端服务，则非管理员组可以登录，并且支持两个以上的会话。 但是，应用程序模式安装涉及附加许可。 当以应用程序模式在运行终端服务的系统上安装 IT Assistant 时，必须本地执行而不能通过终端会话执行安装。

保护 IT Assistant 和其它支持的 Dell OpenManage 应用程序端口的安全

可以使用 IP Security (IPSec) 保护 IT Assistant 服务层端口 2607 和 Managed System 端口 1311、161 和 162 的安全。 要列出当前在您的服务器上运行的端口，您可以从命令提示符中使用命令 **netstat -an** 来显示您系统上所有端口的状态。 此命令的结果应表示 IT Assistant Management Station 只应接受从管理 IT Assistant 用户界面的服务器到端口 2607 的连接（将通过终端服务进行连接）。 同样，Managed System 应配置为仅接受来自 Management Station 端口 1311、161 和 162 的连接。

单一登录

Windows 系统上的单一登录选项使所有的登录用户通过单击桌面上的 **IT Assistant** 图标跳过登录页并访问 IT Assistant。 桌面图标会查询注册表以查看 Internet Explorer 中是否启用了借助当前用户名和密码进行自动登录选项。 如果启用了此选项，就会执行单一登录；否则将会显示正常的登录页。 不能在 Windows 网络上禁用 NT LAN Manager (NTLM) 验证。

要启用“自动使用当前用户名和密码登录”选项，应在 Internet Explorer 中执行下列步骤：

1. 单击 **“Tools”（工具）**菜单上的 **“Internet Options”（Internet 选项）**。
2. 单击 **“Security”（安全）**选项卡
3. 选择 IT Assistant 系统处于的安全区域，即 **“Trusted sites”（受信任的站点）**，并单击 **“Custom Level”（自定义级别）**。
4. 在 **“Security Setting”（安全设置）**对话框中，在 **“User Authentication”（用户验证）**下，选择 **“Automatic Logon with current username and password”（自动使用当前用户名和密码登录）**。
5. 单击 **“OK”（确定）**两次，然后重新启动 Internet Explorer。

对于本地系统访问，必须具有提供该系统相应权限的帐户（User[用户]、Power User[高级用户] 或 Administrator[管理员]）。 其它用户都使用 Microsoft Active Directory 验证。

要通过 Microsoft Active Directory 使用单一式验证启动 IT Assistant，必须设置以下参数：

```
authType=ntlm&application=[ita]
```

例如：

```
https://localhost:2607/?authType=ntlm&application=ita
```

要通过本地系统用户帐户使用单一式验证启动 IT Assistant，必须设置以下参数：

```
authType=ntlm&application=[ita]&locallogin=true
```

例如：

```
https://localhost:2607/?authType=ntlm&application=ita&locallogin=true
```

基于角色的访问安全性管理

IT Assistant 通过基于角色的访问控制 (RBAC)、身份验证和加密来提供安全。

基于角色的访问控制

RBAC 通过确定可以由具有特定角色的人员执行的操作来管理安全性。 每位用户分配有一个或多个角色，每个角色分配有一个或多个可以由该角色用户执行的用户权限。 通过 RBAC，安全管理与组织的结构密切相关。

用户权限

IT Assistant 根据为用户分配的组权限来授予各种访问权限。 支持的三种用户级别有 User（用户）、Power User（高级用户）和 Administrator（管理员）。

*Users（用户）*对所有 IT Assistant 信息具有只读权限。

*Power Users（高级用户）*可以创建立即执行的任务。 不能修改查找配置设置、修改警报管理设置，或者计划或删除任务。

*Administrators（管理员）*可以执行所有 IT Assistant 任务和功能。

Microsoft Windows 身份验证

对于支持的 Windows 操作系统，IT Assistant 验证基于操作系统的用户身份验证系统，使用 Windows NT® LAN Manager (NTLM) 模块进行验证。 这种基础验证系统使 IT Assistant 安全性能够集成到网络的整个安全模式。

分配用户权限

安装 IT Assistant 前，不必将用户权限分配给 IT Assistant 用户。

以下程序按步骤介绍了如何为 Windows 操作系统创建 IT Assistant 用户并分配用户权限：

注意：应该为支持的 Microsoft Windows 操作系统禁用来宾帐户以保护对重要系统组件的访问。 请参阅“禁用来宾和匿名帐户”了解相关说明。

为支持的 Windows 操作系统创建 IT Assistant 用户

注：必须以管理员权限登录才能执行这些程序。

为支持的 Windows Server 2003 操作系统创建用户并分配用户权限

注：有关创建用户并分配用户组权限的问题或了解详细的指导，请参阅操作系统说明文件。

1. 单击**“Start”（开始）**按钮，右击**“My Computer”（我的电脑）**并指向**“Manage”（管理）**。
2. 在控制台树中，展开**“Local Users and Groups”（本地用户和组）**，然后单击**“Users”（用户）**。
3. 单击**“Action”（操作）**，然后单击**“New User”（新建用户）**。
4. 在对话框中键入相应的信息，选择或清除相应的复选框，然后单击**“Create”（创建）**。

注意：必须给每个可以访问 IT Assistant 的用户帐户分配一个密码以保护对重要系统组件的访问。 此外，由于操作系统限制，没有分配密码的用户在运行 Windows Server 2003 的系统上不能登录 IT Assistant。

5. 在控制台树中，在**“Local Users and Groups”（本地用户和组）**中，单击**“Groups”（组）**。
6. 单击要添加新用户的组：**“Users”（用户）**、**“Power Users”（高级用户）**或**“Administrators”（管理员）**。
7. 单击**“Action”（操作）**，然后单击**“Properties”（属性）**。
8. 单击**“Add”（添加）**。
9. 键入要添加的用户名并单击**“Check Names”（检查名称）**进行验证。
10. 单击**“OK”（确定）**。

新用户可以使用其所分配组的用户权限登录 IT Assistant。

为支持的 Windows 2000 操作系统创建用户并分配用户权限

注：有关创建用户并分配用户组权限的问题或了解详细的指导，请参阅操作系统说明文件。

1. 右击**“My Computer”（我的电脑）**并指向**“Manage”（管理）**。
2. 在控制台树中，展开**“Local Users and Groups”（本地用户和组）**，然后单击**“Users”（用户）**。
3. 单击**“Action”（操作）**，然后单击**“New User”（新建用户）**。
4. 在对话框中键入相应的信息，选择或清除相应的复选框，然后单击**“Create”（创建）**。

注意：必须给每个可以访问 IT Assistant 的用户帐户分配一个密码以保护对重要系统组件的访问。 此外，由于操作系统限制，没有分配密码的用户在运行 Windows Server 2003 的系统上不能登录 IT Assistant。

5. 在控制台树中，在**“Local Users and Groups”（本地用户和组）**中，单击**“Groups”（组）**。
6. 单击要添加新用户的组：**“Users”（用户）**、**“Power Users”（高级用户）**或**“Administrators”（管理员）**。
7. 单击**“Action”（操作）**，然后单击**“Properties”（属性）**。
8. 单击**“Add”（添加）**。
9. 单击要添加的用户的名称，然后单击**“Add”（添加）**。
10. 单击**“Check Names”（检查名称）**验证要添加的用户名。

11. 单击“**OK**”（**确定**）。

新用户可以使用其所分配组的用户权限登录 IT Assistant。

将用户添加到域

注：有关创建用户并分配用户组权限的问题或了解详细的指导，请参阅操作系统说明文件。

注：必须在系统上安装 Active Directory 以执行以下程序。

1. 单击“Start”（开始）按钮，然后指向“**Control Panel**”（**控制面板**）→“**Administrative Tools**”（**管理工具**）→“**Active Directory Users and Computers**”（**Active Directory 用户和计算机**）。
2. 在控制台树中，右击“**Users**”（**用户**）或右击要添加新用户的容器，然后指向“**New**”（**新建**）→“**User**”（**用户**）。
3. 在对话框中键入相应的用户名信息，然后单击“**Next**”（**下一步**）。

注意：必须给每个可以访问 IT Assistant 的用户帐户分配一个密码以保护对重要系统组件的访问。 此外，由于操作系统限制，没有分配密码的用户在运行 Windows Server 2003 的系统上不能登录 IT Assistant。

4. 单击“**Next**”（**下一步**），然后单击“**Finish**”（**完成**）。
5. 双击表示刚创建用户的图标。
6. 单击“**Member of**”（**成员**）选项卡。
7. 单击“**Add**”（**添加**）。
8. 选择相应的组并单击“**Add**”（**添加**）。
9. 单击“**OK**”（**确定**），然后再次单击“**OK**”（**确定**）。

新用户可以使用其所分配组和域的用户权限登录 IT Assistant。

禁用来宾和匿名帐户

注：必须以管理员权限登录才能执行此程序。

1. 如果您的系统运行的是 Windows Server 2003，请单击“**Start**”（**开始**）按钮，右键单击“**My Computer**”（**我的电脑**），并指向“**Manage**”（**管理**）。 如果您的系统运行的是 Windows 2000，请右键单击“**My Computer**”（**我的电脑**），并指向“**Manage**”（**管理**）。
2. 在控制台树中，展开“**Local Users and Groups**”（**本地用户和组**），然后单击“**Users**”（**用户**）。
3. 单击“**Guest**”（**来宾**）或“**IUSR_*system name*”（IUSR _*系统名称*）**用户帐户。
4. 单击“**Action**”（**操作**）并指向“**Properties**”（**属性**）。
5. 选择“**Account is disabled**”（**帐户已禁用**）并单击“**OK**”（**确定**）。

带有 X 的红圈会显示在用户名上。 该帐户已禁用。

返回目录页

返回目录页

Dell OpenManage™ IT Assistant 7.2 版用户指南

注：“注”表示可以帮助您更好地使用计算机的重要信息。

注意：“注意”表示可能会损坏硬件或导致数据丢失，并告诉您如何避免此类问题。

本说明文件中的信息如有更改，恕不另行通知。
© 2005 Dell Inc. 版权所有，翻印必究。

未经 Dell Inc. 书面许可，严禁以任何形式进行复制。

本文中使用的商标：*Dell*、*DELL* 徽标、*Dell OpenManage*、*OptiPlex*、*PowerEdge* 和 *PowerConnect* 是 Dell Inc. 的商标；*Microsoft* 和 *Windows* 是 Microsoft Corporation 的注册商标；*Novell* 和 *NetWare* 是 Novell, Inc. 的注册商标；*Red Hat* 是 Red Hat, Inc. 的注册商标；*Intel* 是 Intel Corporation 的注册商标。

本说明文件中述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。

2005 年 12 月

返回目录页