# LANDesk® System Manager 8.7

用户指南

# 封面

本文档中的任何内容都不具任何明示或暗示的保证、担保或许可。对于此类保证、担保和许可，LANDesk 不负担任何责任，内含但不限于：适合特定用途、适销性、不侵犯任何第三方或 LANDesk 的知识产权或其他权利、补偿以及其他一切保证。LANDesk 产品并非专为医疗、挽救或延续生命而设计。忠告读者：第三方可能拥有与本文档和在此讨论的技术有关的知识产权；如果发生侵权行为，需要诉诸法律解决，LANDesk 不负任何责任。

LANDesk 可以随时更改本文档以及相关的产品规范和说明，恕不另行通知。LANDesk 对本文档的使用不作任何担保，对文档中可能出现的错误不负任何责任，也没有义务要更新此处包含的信息。



LANDesk、Autobahn、NewRoad、Peer Download 和 Targeted Multicast 是 LANDesk Software, Ltd. 或其所控附属机构在美国和/或其他国家/地区的注册商标或商标。

* 其他品牌和名称是其各自所有者的财产。

# 内容

# 概述

## 关于 LANDesk® System Manager

欢迎使用 LANDesk® System Manager8.70，这是一个独立的管理应用程序，能帮助您维护服务器（包括运行 Windows、Linux、HP-UX 和 AIX 的服务器）的可靠运行。它还可以与 LANDeskManagement Suite 同时安装和使用，并且与 Management Suite 使用相同的核心数据库，以简化 IT 方面的报告。

由于设计时强调了低资源影响，本产品拥有多个仅在需要时才运行的“按需”代理和服务，从而为其他任务节省了内存和 CPU 周期。LANDesk 了解设备的可靠运行对于公司来说是至关重要的，所以设计本产品时强调了稳定性，保证一周 7 天，每天 24 小时不间断运行。它允许您管理在设备上运行的软件。您可以安装完整代理、选择特定组件或在不安装任何代理的情况下将设备移动到设备列表。

为了正确显示对话框和窗口，必须将 System Manager 网站添加到浏览器的弹出阻止功能的允许列表中。

### 8.70 版的新增功能

下列功能已被添加或从 System Manager 的先前版本进行了升级：

**无代理设备管理：**当设备启用带外管理技术（如 Intel* AMT、IPMI 或 DRAC）后，即可在**我的设备**视图中管理设备，无需在设备上安装管理代理。

**计划任务中的自定义组：**可以将任务划分到自定义组中，以便执行。

**初学者模式：**可以在工具栏上显示按钮的标签，因而更加便于新用户了解按钮的用途。同样，可以选择不显示标签（工具提示仍显示在鼠标上）。

**硬件配置：**使用这种新工具，可以为具有 Intel* AMT 功能的设备配置选项。可以生成用于部署 Intel AMT 设备的 ID、查看生成的 ID 以及更改与 Intel AMT 设备部署相关的配置选项。还可以定义用于检测和阻止设备上可疑网络活动的断路器策略。

**对活动管理技术的增强支持：**现在，这种产品支持 Intel* 活动管理技术第 2 版（除了第 1 版之外）。AMT 第 2 版还支持无代理管理和自动搜寻 Intel* AMT 2 设备。

### 产品功能

使用 System Manager 可选择管理覆盖范围的级别，从简单信息收集到扩展性能分析、安全和配置控制。System Manager 具有以下功能：

**易用的 Web 控制台：**在任何时间、任何地点，使用新设计的基于 Web 的控制台运行产品，在易于使用的界面中查看丰富的数据。您可以从主工作站或机房中的工作站运行 !ServerName!，不需要安装 !ServerName!。而只需浏览产品的 URL，http://*coreserver*/LDSM。通过将设备放入**目标设备**列表，针对特定操作（如软件分发）设置“目标”设备，这类似于许多 Web 应用程序中的“购物车”模型。

**扩展操作系统支持：**在一个集成控制台上管理各种服务器环境。除管理 Windows 2000 和 2003 服务器之外，System Manager 还支持 Linux 和 Unix 的多个版本：

- Red Hat Enterprise Linux v3 (ES) 32 位 - U6
- Red Hat Enterprise Linux v3 (ES) EM64t - U6
- Red Hat Enterprise Linux v3 WS 32 位 - U6
- Red Hat Enterprise Linux v3 WS EM64t - U6
- Red Hat Enterprise Linux v3 (AS) 32 位 - U6
- Red Hat Enterprise Linux v3 (AS) EM64t - U6
- Red Hat Enterprise Linux v4 (ES) 32 位 - U2
- Red Hat Enterprise Linux v4 (ES) EM64t - U2
- Red Hat Enterprise Linux v4 (AS) 32 位 - U2
- Red Hat Enterprise Linux v4 (AS) EM64t - U2
- Red Hat Enterprise Linux v4 WS 32 位 - U2
- Red Hat Enterprise Linux v4 WS EM64t - U2
- SUSE* Linux Server 9 ES 32 位 SP2
- SUSE Linux Server 9 EM64t SP2
- SUSE Linux Professional 9.3
- SUSE Linux Professional 9.3 EM64t
- HP-UX 11.1
- Unix AIX

**计划任务视图：**从一个位置查看所有已计划或已完成的代理部署、漏洞、软件分发、搜寻、OSD、软件更新和自定义脚本任务。可以重新计划、修改任务或使它成为重复事件。

**Intel* AMT 支持：**支持 Intel* 活动管理技术版本 1 和 2。Intel AMT 可以通过带外 (OOB) 通信在任何系统状态下远程管理网络设备，即便在操作系统没有反应或设备关闭的情况下也是这样。对设备端的唯一要求是与企业网络相连并且配有备用电源。

**IPMI 支持：**本产品支持已启动“智能平台管理界面 (IPMI)”（版本 1.5 或 2.0）的服务器，允许带外远程恢复已关闭的服务器，即便在操作系统或处理器不运行的情况下也能查看自动管理数据。

**脚本编写工具：**可以通过创建本地调度程序脚本在设备上执行自定义任务。

**性能监控：**您可以使用多种属性来监控受管的企业或刀片服务器的实时性能。甚至可以跟踪这些属性并查看数天内报告的性能数据历史记录。您可以监控已安装监控代理的设备，还可以在没有代理的情况下，监控带外的已启动 IPMI 的服务器。

**刀片服务器支持：**支持 IBM 刀片机箱和刀片服务器，包括搜寻、机箱检测、清单、软件分发和修补程序管理功能。利用本产品工具，您可以按功能、机箱、机架或其他标准对刀片服务器进行分组，从而更有效地收集数据。

**报告：**您可以针对数据库中的任何设备运行报告，显示使用率统计数据、资源分配和许多其他测量结果。本产品包括多个预定义（预制定）报告。这些报告通过直接访问数据库快速地运行并收集信息，并在二维或三维饼形和条形图中表示数据。通过创建自定义查询，您可以创建附加报告。

**健全性监控/警报：**监控设备的整体健全性非常简单。您可以设置测量阈值，如磁盘空间或 CPU 使用率，还可以配置超出阈值时的报警方式。您可以查看选定设备的健全性状态，并在任何用户察觉到速度变慢前或由于该故障而导致机器关机前启动操作来解决故障。

**软件更新：**可以接收 System Manager 和 Intel* 硬件的软件更新。可以使用软件分发功能手动部署所选的更新。

**基于角色的管理：**添加用户，并根据用户的管理角色为他们配置对工具和其他设备的访问权限。利用基于角色的管理功能，可以指定范围来确定用户能查看和管理的设备，给用户分配权限来确定他们能执行的任务，如仅能查看报告的用户。

**清单：**使用清单扫描工具，本产品可将大量的硬件和软件信息编译到核心数据库中。您可以查看、打印和导出这些数据。

**设备搜寻：**确定网络中的各个设备。设备搜寻收集您的环境中所有设备和其他设备的基本信息，从而实现对目标设备的更高效的控制并加快代理的部署速度。

**支持 Active System Console：**支持 Active System Console，这样在设备上安装 Active System Console 代理后，便可快速提供系统健全性的概要状况。您可以一眼看出所选的硬件元素是否正常工作，是否有任何潜在问题需要加以处理。  您也可以查看详细的系统性能指标及查看系统组件列表，包括硬件、软件、日志和有关 Intel* AMT 和 IPMI（如果该设备启用了其中的一个）的信息。

**执行控制板：**使主管人员能够监控业务的健全性或状态的一组工具（信息图表、图示、刻度和计量）。

**帮助：**本产品包括 入门指南，以及上下文相关帮助主题。

## 产品术语

- **核心服务器：**管理域的中心。产品的所有重要文件和服务都在核心服务器上。一个管理域只有一个核心服务器。核心服务器可以是新服务器，也可以是重定目标的服务器。
- **控制台：**作为主产品界面的基于浏览器的控制台。
- 核心数据库：该产品在核心服务器上创建一个 MSDE 数据库用以存储管理数据。
- **受管设备：**网络中安装产品代理的设备。“设备”包括台式机、服务器、笔记本电脑/移动计算机、刀片机箱等等。核心服务器可管理成千个设备。
- **公共：**对所有用户都可见的项（如组、分发程序包或任务）。用户修改公共项时，修改保持为“公共”。公共组由具备管理员权限的用户创建。

- **私有**或**用户**：由当前登录的用户创建的项。其他用户看不到这些项。私有项或用户项显示在**我的传送方式**、**我的程序包**和**我的任务**树下。具有管理员权限的用户可以看到私有组、用户程序包和任务。
- **通用**：对其他用户可见的项。用户拥有通用项的所有权（通过修改）时，该项分成两项：通用项保持不变，用户项保存在“Users”文件夹中。该项的用户实例不再对其他用户可见。用户可以标记对他们可见的任何通用任务进行标记，从而与其他用户进行共享。一旦用户清除了该项的属性的“通用”选项，则该任务仅在用户的用户任务组中可见。

# 入门



## 概述

欢迎使用 LANDesk® System Manager，这是一个独立的设备管理应用程序，它可以快速有效地管理设备，从而最大限度地节省您的宝贵时间，为您和您的公司节省时间和金钱。通过 System Manager，您可以在中心位置管理设备，根据操作（如冷开机、漏洞评估或配置警报）对其进行分组，远程排除任何故障、保持网络安全并用最新的修补程序不断更新设备。

本指南的用途是，通过配置服务、运行控制台、搜寻设备、将设备移到我的设备列表、配置受管设备以执行操作，帮助您很快使用 System Manager。

System Manager 是一个 Web 应用程序，您可以使用浏览器来访问它，这样就可以从远程工作站管理服务器，它的运作类似于您已经熟悉的许多 Web 应用程序，但还包含若干个高级的 Windows 类型的控制，以增强您的可使用性体验。例如，可将鼠标指针悬停在某个控件上，然后双击或右键单击该控件（就像您在 Windows 应用程序中所做的那样）。例如，在我的设备列表中，您可以双击一个设备名称以访问其详细信息，或右击查看可用操作。

下面的步骤将指导您启动并运行 System Manager、在网络中搜寻设备、选择要移动到我的设备列表的服务器、部署代理以及为各种任务指定目标设备的操作过程。

## 运行安装程序

在安装过程中，请在 Autorun 页面上选择 LANDesk® System Manager。详细安装说明，请参阅安装和部署指南的第 2 阶段。

完成 System Manager 安装后，便可以开始使用本产品。以下部分将指导您完成几个必须执行的任务：运行核心激活实用程序、配置服务、搜寻计算机、通过将设备移入我的设备列表指定有效管理哪些设备、对设备进行分组、添加用户以及部署代理。一旦完成这些任务，便可开始探究 System Manager 的这些强大功能如何才能帮助您管理设备。

## 激活核心服务器

只有激活核心服务器才能运行本产品。

使用核心服务器激活实用程序：

- 第一次激活新的 System Manager 核心服务器
- 更新现有的 System Manager 核心服务器或升级到 Management Suite 或 System Manager

每个核心服务器必须有一个唯一的授权证书。

此实用程序会在第一次重新启动时自动运行。

将核心服务器连接到 Internet，

1. 单击开始|所有程序|核心服务器激活。
2. 键入购买许可证时　提供的唯一的用户名和密码。
3. 单击激活。

核心服务器通过 HTTP 与　Software 授权服务器通信。如果您使用代理服务器，请单击该实用程序的代理选项卡并输入您的代理信息。如果您的核心有 Internet 连接，则与授权服务器之间的通信是自动的，并且不要求您进行任何干预。如果未连接核心，请在重新启动时单击关闭，并通过电子邮件将授权文件发送到 licensing@landesk.com。

核心服务器会定期在“\Program Files\LANDesk\Authorization Files\LANDesk.usage”文件中生成节点数验证信息。此文件定期发送到 LANDesk Software 授权服务器。此文件是 XML 格式的，并被数字签名和加密。任何对此文件进行的手动更改都将使其内容和下一次向 Software 授权服务器发送的使用情况报告无效。

- “核心服务器激活”实用程序不会自动启动拨号 Internet 连接，但是如果您手动启动了拨号连接并运行激活实用程序，该实用程序可以使用拨号连接报告使用情况数据。
- 还可以通过电子邮件激活核心服务器。将位于 Program Files\LANDesk\Authorization 下扩展名为 .TXT 的文件发送到 licensing@landesk.com。LANDesk 客户支持将用有关将文件复制到核心服务器以完成激活过程的文件和说明回复电子邮件。

# 添加用户

System Manager 用户是指可以登录到控制台并对网络中的特定设备执行特定任务的用户。可以使用基于角色的管理功能管理用户。通过基于角色的管理，可以根据产品用户的权限和范围，为这些用户分配特殊的管理角色。权限决定了用户能够查看和利用的产品工具和功能。范围决定用户可以查看和管理的设备范围。可以创建各种用户，并自定义其权限和范围以适合管理要求。例如，可以创建一个用户，赋予它帮助中心角色所需的权限，使其承担这个角色。有关详细信息，请参阅用户指南中基于角色的管理一章 System Manager。

安装产品时，将自动创建两个用户帐户（请参阅下文）。如果您希望添加更多的用户，可以手动进行添加。用户实际上不是在控制台中创建的。而是当用户被添加到核心服务器上 Windows NT 用户环境中的 LANDesk Management Suite 组后，这些用户才会出现在“用户”组中（单击左侧导航窗格中的用户）。“用户”组显示了目前保存在核心服务器的 LANDesk Management Suite 组内的所有用户。

“用户”组中有两个默认用户。一个用户是默认管理员。这是在安装产品时登录到服务器上的管理用户。

另一默认用户是默认模板用户。此用户包含一个用户属性（权限和范围）模板，将新用户添加到 Management Suite 组时，可使用该模板对新用户进行配置。换句话说，当您将某用户添加到 Windows NT 环境中的该组时，该用户会继承当前在“默认模板用户”属性中定义的权限和范围。假定“默认模板用户”选定了所有权限并选定了“默认范围 - 所有机器”，那么任何新加到 LANDesk Management Suite 组内的用户被加到“用户”组中时，其权限是能使用所有产品工具，范围是能够访问所有设备。

通过选择“默认模板用户”并单击编辑可更改其属性设置。例如，若要同时添加大量用户，但不想让他们能访问所有工具或设备，可先更改“默认模板用户”设置，然后将用户添加到 LANDesk Management Suite 组中（请参见下面的步骤）。“默认模板用户”不能删除。

当您在 Windows NT 中将某用户添加到 LANDesk Management Suite 组后，系统会自动将该用户读入用户窗口中的“用户”组中，该用户将继承当前“默认模板用户”的权限和范围。系统将显示该用户的名称、范围和权限。此外，还会在“用户设备”、“用户查询”、“用户报告”和“用户脚本”组中创建新的用户子组，这些子组以相应用户的唯一登录 ID 命名（注意，只有管理员才能查看“用户”组）。

相反，如果您从 LANDesk Management Suite 组中删除某用户，该用户将不再出现在用户列表中。不过，该用户的帐户仍会保存在您的核心服务器上，您随时可将其添回到 LANDesk Management Suite 组中。另外，还会保存该用户在“用户设备”、“用户查询”、“用户报告”和“用户脚本”下面的子组，因此，可以恢复用户且不丢失其数据，并可以将数据复制给其他用户。

按 F5 刷新 System Manager 控制台中的用户框。有关如何将用户或域组添加到 LANDesk Management Suite 组或如何创建新用户帐户的信息，请参阅 System Manager *用户指南*的基于角色的管理一章中的“添加产品用户”。

将用户或域组添加到 LANDesk Management Suite 组

1. 浏览并找到服务器的**管理工具|计算机管理|本地用户和组|组**实用程序。
2. 右击 **LANDesk Management Suite 组**，然后单击**添加到组**。
3. 单击**添加**，然后键入用户或在列表中选择用户。
4. 单击**添加**，然后单击**确定**。

**注意：**使用以下方法也可以将用户添加到 LANDesk Management Suite 组中：在**用户**列表中右击相应的用户帐户，单击**属性|该组的成员**，然后单击**添加**来选择该组并添加该用户。

如果用户帐户已不在服务器中，则必须先在服务器上创建它们。

创建新的用户帐户

1. 浏览并找到服务器的**管理工具|计算机管理|本地用户和组|用户**实用程序。
2. 右击**用户**，然后单击**新建用户**。
3. 在**新建用户**对话框中，输入名称和密码。
4. 指定密码设置。
5. 单击**创建**。**新建用户**对话框始终处于打开状态，因此，您可以创建其他用户。
6. 单击**关闭**，退出该对话框。

将用户添加到 LANDesk Management Suite 组中，使他们出现在控制台上的“用户”组中。

## 配置服务和凭证

在您管理网络上的设备之前，必须向 System Manager 提供必要的设备凭证。使用核心服务器上的配置服务实用程序 (SVCCFG.EXE) 指定所需的操作系统、Intel* AMT 和 IPMI BMC 凭证。还可以指定额外的设置，例如，清单默认值，PXE 暂存查询设置和 LANDesk 数据库设置。

使用配置服务进行配置：

- 数据库名、用户名和密码。（安装时设置。）
- 用于向受管设备安排作业的凭证。（您可以输入多组管理员凭证。）
- 用于配置 IPMI BMC 的凭证。（仅能输入一组 BMC 凭证。）
- 用于配置启用了 Intel AMT 设备的凭证。（仅能输入一组 Intel AMT 凭证。）
- 服务器软件扫描时间间隔、维护、保持清单扫描的天数以及登录历史记录的长度。
- 复制设备 ID 的处理方式。
- 调度程序配置，包括调度的作业和查询评估时间间隔。
- 自定义作业配置，包括远程执行超时。

1. 在核心服务器中单击开始 | 所有程序 | LANDesk | LANDesk 配置服务。
2. 单击调度程序选项卡。
3. 单击更改登录按钮。
4. 在受管设备上输入服务要使用的凭证，通常是域管理员帐户。
5. 单击添加。如果不是全部的受管设备都启用了相同的管理员用户名帐户，请根据需要添加其他凭证。
6. 单击应用。

7. 如果您的环境中有启用 IPMI 的服务器，请单击 BMC 密码选项卡。在密码文本框中键入密码，在确认密码文本框中重新键入密码，然后单击确定。（所有受管 IPMI 服务器必须共享相同的 BMC 用户名和密码。）
8. 如果您有启用 Intel AMT 的设备，则单击 Intel AMT 配置选项卡。在用户名文本框中输入当前配置的 Intel AMT 用户名，然后在密码文本框中输入当前配置的密码。在确认密码文本框中再次输入密码，然后单击确定。
9. 根据需要设定其他设置，如软件扫描时间间隔。
10. 单击确定以保存更改。

有关详细信息，请单击每个配置服务选项卡上的**帮助**。

## 运行控制台

System Manager 中含有大量的工具，可用来查看、配置、管理和保护网络上的设备。控制台是输入点，您可以通过它使用这些工具。

控制台中的顶部窗格显示了您正在登录的服务器以及可用作登录身份的用户。我的设备列表是控制台的主窗口，也是执行绝大多数功能的起始点。左侧窗格显示可用工具。控制台中的右侧窗格会显示对话框和屏幕，您可以借助它们完成管理任务。

控制台的方便之处在于，您可以从远程位置（如您的工作站）执行它的所有功能，这样您就不需要走到服务器房间或走近每台受管设备来执行例行的维护或排除故障。

可以用三种方式启动控制台：

- 在核心服务器中，单击开始|所有程序|LANDesk|System Manager。
- 在远程工作站的浏览器中，输入 URL http://coreserver/LDSM。

## 搜寻设备

使用**搜寻配置**选项卡可以创建新的搜寻配置，编辑和删除现有配置，以及安排搜寻配置的时间。每个搜寻配置都包括一个描述名称、要扫描的 IP 范围和搜寻类型。

创建配置之后，可使用**安排搜寻**对话框配置运行搜寻的时间。

1. 在左侧导航窗格中，单击**设备搜寻**。
2. 在**搜寻配置**选项卡中，单击**新建**按钮。
3. 填充下列所述字段。完成创建操作后，单击**添加**按钮，然后单击**确定**。

下面的文本介绍了**搜寻配置**对话框的各个部分。

- **配置名称：**键入该配置的名称。为配置取一个有意义的名称，以便您轻松记住此配置。配置名称最长可达 255 个字符，而且不应包含以下字符：″、+、#、& 或 %。任何这些字符之后的配置名称将无法显示。

- **标准网络扫描：**通过将 ICMP 数据包发送到指定范围内的 IP 地址，可以查找设备。这是最彻底的搜寻，但速度最慢。默认情况下，此选项使用 NetBIOS 收集设备的有关信息。

  网络扫描选项中包含一个 **IP 特征**选项，利用此选项，设备搜寻尝试通过 TCP 数据包响应来搜寻操作系统类型。“IP 特征”选项会或多或少地减慢搜寻速度。

  网络扫描选项中还包含一个**使用 SNMP** 选项，可用于配置使用 SNMP 进行扫描。单击**配置**以键入有关您的 SNMP 配置的信息。
- **LANDesk CBA 搜寻**在设备中查找标准管理代理[以前在 Management Suite 中称作通用基本代理 (CBA)]。)标准管理代理允许核心服务器搜寻网络上的客户端并与之通信。此选项可用于搜寻安装了产品代理的设备。路由器阻塞了标准管理代理和 PDS2 之间的通信。为了跨多个子网运行标准 CBA 搜寻，必须配置路由器，以允许多个子网之间进行定向广播。

  CBA 搜寻选项还有一个 **LANDesk PDS2 搜寻**选项，利用该选项，设备搜寻将在设备上查找 LANDesk Ping 搜寻服务 (PDS2)。LANDesk Software 产品，如 LANDesk® System Manager、Server Manager 和 LANDesk 客户端管理器使用 PDS2 代理。如果您网络上的设备已安装了这些产品，请选择此选项。CBA 搜寻对 Linux 机器不支持，但如果选择了 PDS2，则可搜寻到装有代理的 Linux 机器。
- **IPMI：**搜索已启动 IPMI 的服务器。IPMI 是由 Intel、* H-P、* NEC、* 和 Dell* 开发的一种规范，用来为可管理的硬件定义消息和系统界面。IPMI 具有监视和恢复功能，不管设备处于开机或关机状态、也不管操作系统处于何种状态，都可访问这些功能。请注意，如果底板管理控制器未进行配置，则无法响应产品用于搜寻 IPMI 的 ASF ping。也就是说，您不得不将其搜寻为普通计算机。当“推”客户端时，ServerConfig 将会扫描系统并检测到这是 IPMI 并配置 BMC。
- **服务器机箱：**查找刀片式服务器机箱管理模块 (CMM)。服务器机箱中的刀片式服务器将作为普通服务器被检测。
- **Intel* AMT：**查找支持 Intel 活动管理技术的设备。
- **起始 IP：**输入您要扫描的地址范围的起始 IP 地址。
- **结束 IP：**输入您要扫描的地址范围的结束 IP 地址。
- **子网掩码：**输入您要扫描的 IP 地址范围的子网掩码。
- **添加：**在对话框底部的工作队列中添加 IP 地址范围。
- **清除：**清除 IP 地址范围字段。
- **编辑：**在工作队列中选择 IP 地址范围，然后单击**编辑**。范围显示在工作队列上面的文本框中，您可以在其中编辑范围，并将新范围添加到工作队列中。
- **删除：**从工作队列中删除所选的 IP 地址范围。
- **全部删除：**从工作队列中删除全部 IP 地址范围。

配置搜寻任务后，您就可以安排运行搜寻任务的时间来搜寻连接到网络的设备。

## 安排并运行搜寻任务

使用搜寻设备选项卡上的计划按钮，可显示安排搜寻的时间对话框。搜寻运行时，可使用此对话框进行计划。您可以安排搜寻任务立即运行、在将来的某个时间运行、将此作为一个重复执行的计划，或者仅运行一次计划，而不必担心重复执行。

计划一个搜寻任务后，可在搜寻任务选项卡中查看搜寻状态。通过自动搜寻网络上出现的新设备，安排重新搜寻任务可为您提供帮助。

安排搜寻的时间对话框包括以下这些选项。

- 保持不计划：使任务保持不计划，但在搜寻配置列表中保留任务供未来使用。
- 立即开始：尽快运行任务。开始任务可能需要一分钟时间。
- 在预定时间开始：在指定的时间开始任务。单击此选项后，必须输入下列内容：
  - 时间：要启动任务的时间。
  - 日期：要开始任务的日期。根据您所在位置的不同，日期顺序将采用日-月-年或月-日-年的方式。
  - 重复间隔：想要重复任务，请选择按每天、每周或每月重复。如果选择了每月和某个并非所有月都有的日期（例如，31 号），则任务将只按照包含此日期的月来运行。

安排搜寻任务

1. 在左侧导航窗格中，单击搜寻的设备。
2. 在搜寻配置选项卡上，选择需要的配置，然后单击计划。配置搜寻计划，单击保存。
3. 在搜寻任务选项卡中监控搜寻进度。单击刷新更新此状态。
4. 搜寻完成后，单击不受管在上方的搜寻到的设备窗格中查看所有搜寻到的设备（该窗格不自动刷新）。

## 查看搜寻到的设备

在搜寻到的设备窗格中按设备类型对搜寻到的设备分类。默认情况下显示计算机文件夹。单击左侧窗格中的文件夹查看不同类别的设备。单击不受管查看搜寻操作返回的所有设备。

- 刀片服务器机箱出现在机箱文件夹中。
- 标准企业设备出现在计算机文件夹中。
- 路由器和其他设备出现在基础设施文件夹中。
- 启用了 Intel AMT 的设备出现在 Intel AMT 文件夹中。
- 已启用 IPMI 的服务器出现在 IPMI 文件夹中。
- 未分类的设备出现在其他文件夹中。
- 打印机出现在打印机文件夹中。

注意：某些 Linux 服务器作为操作系统名称与通用的“Unix”显示在一起（有时甚至显示为“其他”）。部署标准的管理代理时，这些服务器将更新我的设备列表中的操作系统名称条目，并显示完整的清单。　　查看搜寻到的服务器

1. 在设备搜寻页面的左侧窗格中，单击计算机或要查看的其他类型的设备。搜寻结果将显示在右窗格中。
2. 要过滤结果，单击“过滤”图标  ，至少键入要搜索的内容的一部分，单击查找。

## 分配名称

进行网络扫描搜寻时，会返回一些空节点名（或主机名）的服务器。运行 Linux 的服务器最容易出现这种情况。使用管理将设备移动到我的设备列表前，必须为该设备分配一个名称。

1. 在设备搜寻页面中，单击带空白名称的设备。（必须单击节点名称列中的空白区域。）
2. 在工具栏中单击分配名称。
3. 键入名称并单击确定。

在设备上安装产品代理时，它将自动扫描主机名，并用正确的信息更新核心数据库。

# 将设备移动到“我的设备”列表

搜寻设备后，您必须手动地设置要管理的目标设备，并将其移动到我的设备列表。移动设备时不会向设备安装任何软件。它仅使设备可在我的设备列表中进行查询、分组和排序。您针对特定操作设置“目标”设备，类似于许多 Web 应用程序中的“购物车”模型。

1. 在搜寻到的设备视图中，单击要移动到我的设备列表中的设备。您可以通过按 SHIFT+单击或 CTRL+ 单击来选择多个设备。
2. 单击目标按钮。如果此按钮未显示，请单击工具栏上的 <<。该按钮位于工具栏的最右侧。或者右键单击选择的服务器并单击目标。
3. 在窗格底部，单击管理选项卡。
4. 选择将已选定的设备移动到管理数据库中，或选择移动目标设备。
5. 单击移动。

单击移动将设备移动到我的设备列表，并将设备的信息放在数据库中。信息放入数据库后，您可以在数据库中运行受限的查询和报告（例如按设备名、IP 地址或操作系统进行查询和报告）。

# 根据操作将设备分组

您可能希望将设备分组，如按地理位置或功能分组，这样在这些设备上执行操作可以更为快捷。例如，您可能希望查看特定位置的所有设备的处理器速度。

1. 在我的设备列表中，单击私有组或公共组，然后单击添加组。
2. 在组名称框中键入组名。
3. 单击要创建的组类型。
   - 静态：已经添加到该组中的设备。它们将一直保留在该组中，直到将其删除或不再对其进行管理。
   - 动态：满足由查询定义的一个或多个条件的设备。例如，一个组可以包含当前处于“警告”状态的所有服务器。如果它们满足为该组定义的条件，则将一直保留在该组中。满足组查询条件时，设备自动添加到动态组。
4. 操作完成后，单击确定。
5. 要将设备添加到静态组，请单击我的设备列表右侧窗格中的设备，单击移动/复制，选择组，单击确定。

# 配置设备进行管理

搜寻设备本身无法对设备进行管理。在使用控制台完全管理设备和接收健全性警报之前，应首先在设备上安装管理代理。您可以选择安装默认代理配置（安装所有管理代理）或在设备上安装自定义的代理配置。（代理配置必须包括监视代理，以接收健全性警报。）

可以通过以下方式安装管理代理：

- 在我的设备列表中选择目标设备，然后安排代理配置任务来远程地在设备上安装代理。（以下步骤）
- 映射到核心服务器的 LDlogon 共享目录 (//coreserver/ldlogon)，然后运行 SERVERCONFIG.EXE。（有关步骤，请参阅 System Manager 用户指南设备代理安装和配置一章中的“‘拉’代理”）
- 创建自解压设备安装程序包。在设备上本地运行此程序包来安装代理。必须以具有管理员权限的用户登录才能完成此操作。 （有关步骤，请参阅 System Manager 用户指南设备代理安装和配置一章中的“使用安装程序包安装代理”）

**将代理推向以下目标：**

1. 我的设备列表中的目标设备（如“将设备移动到我的设备列表”所述）
2. 在左侧导航窗格中，单击代理配置，右键单击您要推送的配置，然后单击计划任务。
3. 在左窗格中，单击目标设备，然后单击添加目标列表按钮。
4. 单击计划任务，单击立即开始即可立即开始执行任务，或单击稍后开始，设置任务的开始日期和时间，然后单击保存。

您可以在配置任务选项卡中查看任务的状态。

## 安装 Linux 服务器代理

您可以远程地在 Linux 服务器上部署和安装 Linux 代理和 RPM。必须正确配置您的 Linux 服务器来完成此操作。有关正确配置 Linux 服务器的说明，请参阅 *System Manager 用户指南*设备代理安装和配置一章中的“安装服务器代理”。

# 设置警报

当设备上出现某个问题或其他事件时（例如设备磁盘空间不足），System Manager 会发出警报。选择安全性级别或会触发警报的阈值可自定义这些警报。警报将被发送到控制台，可对这些警报进行配置，以便执行特定的操作。可以为许多事件或潜在问题设置警报。产品附带了默认警报规则集，安装监控组件后，会将此规则集安装到受管设备。此警报规则集向 控制台发送健全性状态反馈。默认的规则集包括的警报有：

- 添加或删除磁盘
- 驱动器空间
- 内存使用情况
- 温度、风扇和电压

- 性能监控
- IPMI 事件（需要适当的硬件）

要了解警告的更多信息，请参阅 System Manager 用户指南的“警报配置”一章。

## 设置警报

当设备上出现某个问题或其他事件时（例如设备磁盘空间不足），System Manager 会发出警报。选择安全性级别或会触发警报的阈值可自定义这些警报。警报将被发送到控制台，可对这些警报进行配置，以便执行特定的操作。可以为许多事件或潜在问题设置警报。产品附带了默认警报规则集，安装监控组件后，会将此规则集安装到受管设备。此警报规则集向 控制台发送健全性状态反馈。默认的规则集包括的警报有：

- 添加或删除磁盘
- 驱动器空间
- 内存使用情况
- 温度、风扇和电压
- 性能监控

要了解警告的更多信息，请参阅 System Manager *用户指南*的“警报配置”一章。

## 下一步怎么办？

您现在已经启动并运行 Server Manager。您仅仅使用了 Server Manager 中的一部分功能，您确实只用了一部分功能（如设备搜寻和代理配置）。手册指南（*安装和部署指南*与*用户指南*）可以提供所有产品功能的深层信息。功能包括：

**软件更新：**为网络中的受管服务器建立不间断的修补程序级别的安全保障。该工具可以自动执行以下重复性工作：维护当前漏洞信息、评估在受管设备上运行的各种操作系统的漏洞、下载合适的修补程序可执行文件、通过在受影响的设备上部署和安装必要的修补程序来修补漏洞、验证修补程序的安装是否成功等。

**警报：**在任何设备达到特定阈值时确保向您发出警报。警报是监控相关功能，可以通过许多方式通知您。例如，如果需要了解设备上的存储量达到 95% 的时间，可以选择被警报的方式（代理可以发送电子邮件或寻呼机消息、重启或关闭设备或者将信息添加到警报日志）。

**查询：**通过在基于特定系统或用户标准的核心数据库中搜寻和组织设备来管理您的网络。您可以查询受管设备列表，查找那些满足特定标准的设备（如所有处在公司办公室或所有具有 256k RAM 设备），并将其分组用于各种操作。这些组可以是静态的（组成员只能手动更改），也可以是动态的（在设备满足或不满足特定标准时更改组成员）。

**软件分发：**创建任务将软件包（一个或多个 MSI 文件、一个可执行文件、一个批文件、RPM 文件 (Linux) 或用 LANDesk 程序包生成器创建的包）发送到目标设备。

**监测：**通过使用一种支持的监视类型（直接 ASIC 监视、带内 IPMI、带外 IPMI、CIM 等）监视设备的健全性状态。使用监视功能，您可以跟踪设备上的许多数据，例如使用级别、操作系统事件、

进程和服务、性能历史记录以及硬件传感器（风扇、电压、温度等）。警报是使用监视代理启动警报操作的相关功能。

**报告：**生成各种专门的报告，这些报告提供有关网络中受管设备的关键信息。Server Manager 使用清单扫描实用程序将设备（和收集的有关这些设备的硬件与软件数据）添加到核心数据库中。可以从设备清单视图中查看、打印此清单数据，还可以利用它定义查询并对设备进行分组。此报告工具通过收集并按实用的报告格式管理这些数据，可进一步利用此扫描的清单数据，有助于为管理报告收集并格式化数据。

**不受管的设备搜寻:**查找控制台没有管理的设备。搜寻是对将新机器快速进行管理的第一步。您可以设置搜寻任务，每月扫描一次新机器。

**软件授权监视：**跟踪许可证遵从的总体情况。软件许可证监视代理收集数据（如设备上所有已安装应用程序的总使用分钟数、启动数和上次启动日期），并将这些数据存储在设备的注册表中。您可以使用这些数据监视产品使用情况及拒绝倾向。代理使用最少的网络带宽被动监视设备上的产品使用情况。对于未与网络连接的移动设备，代理将持续监视其使用情况。

**操作系统部署：**使用基于 PXE 的部署工具将操作系统映像部署到网络设备上。通过此方法可以为带有空硬盘或其操作系统无法使用的设备部署映像。使用轻型 PXE 代表，就无需在每个子网上设立一个专用 PXE 服务器。操作系统部署简化了新设备的部署过程，部署一旦开始，便不需要其他最终用户和 IT 人员的参与。

# 许可

通过运行不间断的验证进程，本许可进程将有助于确保您的组织遵守许可的节点协议。使用此方法，您还可以在定义的用户帐户下使用多台核心服务器。此许可进程用后端数据库创建和管理用户帐户。此“许可进程”是一个简单的、从核心服务器到后端进程的请求和回复过程，运行此进程可以更新核心服务器，以在下一个周期内继续使用。

安装后运行本产品（或任何附加软件）时，您可以激活试用期的评估许可证，或输入用户名和密码来激活从 LANDesk 销售部门购买的许可证。对于现有帐户，可使用同一个用户名和密码来激活所有核心服务器。

对于评估和购买产品来说，激活过程在本质上是相同的。设备具有 Internet 连接时，此过程只是简单的信息交换。未连接 Internet 时，必须手动将一个文件通过电子邮件发送到 LANDesk，然后将返回的文件保存到核心服务器。此激活过程如下：

1. 用户运行 Activate Core 实用程序。
2. 创建一个包含服务器和使用情况信息的文件。该文件使用核心服务器的私钥签名，并使用 LANDesk 公钥进行加密。
3. 如果存在 Internet 连接，核心服务器将建立与 LANDesk 服务器的通信并上传激活文件。后端进程处理信息并发送回激活信息，该信息将直接写入数据库中。
4. 如果不存在 Internet 连接，您可以通过电子邮件将 \Program Files\LANDesk\Authorization Files 中的文件发送到 licensing@landesk.com。

# 添加许可证

是否可以通过控制台使用某一功能将取决于授权密钥。可通过添加新授权密钥来访问其附加功能，或更新用户数量。安装期间，会生成 45 天的试用许可证。通过控制台添加有效的许可证后，临时许可证将被删除。

**要添加授权密钥，请执行以下操作：**

1. 在左侧导航窗格中，单击**首选项**。
2. 单击**许可证**选项卡。
3. 单击屏幕底部的链接 http:/www.landesk.com/contactus/。

如果无法使用以上链接，可能是未将浏览器的安全级别设置为“中”。您应在 Internet Explorer（**工具 > Internet 选项 > 安全 > Internet > 默认级别**）中将默认的 Internet 安全级别更改为“中”。

# 控制台

## 启动控制台

**启动控制台**

1. 在核心服务器上，单击**开始 | 所有程序 | LANDesk | LANDesk System Manager**。

   或者

   在远程工作站上，打开浏览器并键入控制台地址。此地址的格式将是 http://*corename*/ldsm。

2. 输入有效的用户名和密码。

   若要连接到远程核心服务器，请遵循标准的 Windows 远程登录规则（即，如果用户是核心服务器的本地用户，只输入用户名即可；如果用户是域用户，则输入域名\用户名）。
3. 单击“确定”。

启动控制台后，如果不显示设备列表和按钮，您可能需要激活核心服务器。

### 关于 System Manager“登录”对话框

使用该对话框可启动控制台并连接到核心服务器。

- **用户名：**标识用户。这个用户可以是管理员用户或具有有限权限的某些其他类型的产品用户（有关详细信息，请参阅 基于角色的管理）。该用户必须是核心服务器的 LANDesk Management Suite 组中的成员。如果要连接远程核心服务器，请输入域名和用户名。
- **密码：**用户的密码。

# 目标设备

**目标设备**列表有助于您在所选设备上完成任务，如部署代理或向选定的设备组扫描软件更新。

建议添加到该列表的设备数量不应超过 250 个。设备将一直留在列表中，直到您的控制台会话超时（处于无操作状态 20 分钟之后）。

通过从任何设备列表中选择设备，将设备添加到**目标设备**列表中。如果看不到想要的设备，则使用工具栏上的**查找**按钮。可搜索某个具体的设备，也可使用通配符 % 或 * 搜索多个设备。单击**目标**工具栏按钮将设备添加到**目标设备**列表。如果看不到此按钮，请单击 << 按钮。

如果找到多个设备，请选择希望添加到列表中的设备，然后单击**目标**。如果搜索返回的设备列表跨多页显示，则必须在每页上单击**目标**。即使选中了多页中的设备，如果只单击一次该按钮，是无法

添加所有设备的。单击最右侧工具栏下的向下箭头，您可以设置每页要显示的设备数。每页最多可显示 500 台设备。要更改列表中显示的设备数量，请参阅**首选项**下的 页面设置。

利用**目标设备**列表中的一个或多个设备，您可以完成任务，如向每个目标设备部署代理配置，或者将不受管的设备移至**我的设备**列表。

**确定目标设备**

1. 在**我的设备**列表或**搜寻到的设备**视图中，单击希望用作操作目标的设备。使用标准的多项选择方法（SHIFT + 单击或 CTRL + 单击）可以选择多个设备。
2. 单击**目标**按钮。如果此按钮未显示，请单击工具栏上的 <<。该按钮位于工具栏的最右侧。

在下方的窗格中，所选设备列在了**目标设备**选项卡下面。一旦将它们列在此选项卡下面，您就可以打开工具（如代理部署），并安排可以应用到目标设备的任务。如果有不受管的目标设备，则您可以单击**管理**选项卡，并将其移至**我的设备**列表。

# 过滤显示列表

使用**我的设备**列表中的过滤图标，可以确定哪些设备将出现在列表中。可以按照其中的一个标准进行过滤（按设备名称或 IP 地址），也可以结合多个标准进行过滤以得到一个计算机子集。

**过滤显示列表**

1. 在**我的设备**列表中，双击**所有设备**或导航到一个组。
2. 单击工具栏上的**过滤**  。
3. 在下拉列表中，选择**设备名称**或 **IP 地址**。
4. 在文本框中键入标准，可设置指定标准的参数。**查找**框中不支持下列扩展字符：<、>、″、’、!。

   如果按设备名过滤，则键入主机名或计算机名的范围。可输入通配符来查找某些计算机名（例如，*srv）。

5. 单击**查找**。

# 使用组

将设备分组可简化管理。您可以创建组，根据职能、地理位置、部门、设备属性或任何其他符合要求的类别来组织设备。例如，可以为配置为 Web 服务器的所有服务器创建一个 Web 服务器组，或创建一个包含运行特定操作系统的所有设备的组。右击一个组可打开或删除该组，或者将组内包含的所有设备设置为执行特定操作（如警报规则集和代理部署）的目标设备。

**我的设备**主视图包含以下组：

- **所有设备**：基于用户的范围，在平面列表（无子组）中列出当前登录用户可以看到的所有设备。对于管理员，**所有设备**列出所有已扫描的或移动到核心数据库中的设备。当清单扫描器将配置标准管理代理的设备扫描到核心数据库以后，**所有设备**组 / 文件夹中会自动显示这些设备。用户（包括管理员）无法在**所有设备**中创建组。
- **公共组**：列出管理员从**所有设备**组中添加的组 / 设备，以及刀片机箱组。管理员（具有管理员权限的用户）可以看到该组中的所有设备，而其他用户只能看到其范围允许的设备。只有管理员可以在**公共组**下创建组。
- **私有组**：基于用户范围列出当前登录用户的组 / 设备。用户只能在**私有组**下创建设备子组。用户可以从**公共组**和**所有设备**组中通过移动或复制，在其**私有组**或任何子组中添加设备。所有用户都可以在**私有组**中创建组。

---

有关用户可以查看和管理设备视图中哪些设备以及可以使用的管理工具的更多信息，请参阅“基于角色的管理”。

---

# 组类型

可创建和管理两种类型的组：

- **静态组**。*静态组*由手动添加至其中的设备构成。只能通过手动添加或删除设备来更改静态组。
- **动态组**。*动态组*由符合筛选条件或查询定义的计算机构成。每次展开该组时，都会解析查询并显示结果。例如，动态组可以包含当前处于“警告”状态的所有设备。计算机会根据状态的变化移入或移出此组。

### 创建静态组

1. 在控制台的设备视图中，双击父组（例如，**私有组**），然后单击**添加组**。
2. 输入新组的名称。
3. 选择**静态**，然后单击**确定**。

创建静态组后，通过从列表中选择设备，并单击工具栏中的**移动 / 复制**，可以将设备移动或复制到静态组中。可以从**所有设备**列表中将设备复制到组中，也可以从其它组中移动/复制。

### 创建动态组

1. 在控制台的设备视图中，双击父组（例如，**私有组**），然后单击**添加组**。
2. 输入新组的名称。
3. 选择**动态**，然后单击**确定**。

创建动态组后，必须为其创建过滤器，以确定哪些计算机将出现在此组中。可以指定新的过滤器，或基于现有查询进行过滤。

### 新建过滤器

1. 选择新建的动态组（此操作在底部窗格中显示**组属性**）。

2. 在**组属性**中，选择**新建过滤器**，然后单击**新建过滤器**。
3. 选择要使用的过滤标准，然后单击**确定**。

**根据现有查询创建过滤器**

1. 选择新建的动态组（此操作在底部窗格中显示**组属性**）。
2. 在**组属性**中，选择**根据现有查询创建过滤器**
3. 选择要用于过滤组的现有查询，并单击**新建过滤器**。
4. 添加要使用的任何其他过滤标准，然后单击**确定**。

如果基于现有查询进行过滤，而在稍候由您或其他用户修改了此查询，则基于此查询的过滤不会动态地更改，以匹配修改的查询。

# 使用操作选项卡

使用**操作**选项卡在所选设备和目标设备上执行操作。可以从受管计算机列表中删除设备，打开、关闭和重新启动设备及监控与受管设备的连接。

- 删除设备
- 电源选项
- 设备监视器

## 删除设备

使用**删除设备**，您可以从受管计算机列表中删除所选设备或目标设备。删除功能可以删除 System Manager 中任何组（默认组或用户创建组）内的单台或多台设备。从组中删除某设备后，该设备将彻底地从所有受管/清单设备列表（包括默认的**所有设备**组）中删除。

如果您正删除大量设备，操作可能会超时。如果操作超时，尝试将操作分为几个较小操作。

## 电源选项

使用**电源选项**，您可以关闭、重启和（在使用受管 IPMI 机器的情况下）打开远程设备。在使用非 IPMI 服务器的情况下，设备必须部署 LANDesk 代理才能执行重新启动和关机功能。使用 IPMI 计算机，必须具有正确的 IPMI 证书才能执行开/关机和重新启动功能。如果 IPMI 框中已部署了 LANDesk 代理，则可以执行关机和重新启动功能而不需要 IPMI 证书。使用 配置服务实用程序可设置用于管理 IPMI 服务器的 IPMI BMC 密码。

**要使用电源选项，请执行以下操作：**

1. 在**我的设备**列表中，单击某设备或选择 目标设备列表。
2. 在底部窗格中，单击**操作**选项卡。
3. 单击**电源选项**。
4. 选择是在 目标设备中的设备上执行此操作，还是仅在选定的设备上执行此操作。

5. 从以下选项中进行选择：
   - 重新启动
   - 关闭电源
   - 打开电源（适用于启用 IPMI 和启用 Wake on LAN 的设备上）

6. 单击**显示控制台重定向窗口**可以使用启动器来启动超薄容器（对 EM64T 而言，该启动器将比 TTY 控制更易于重新编译）。

   打开或重新启动受管 IPMI 服务器时，可以打开控制台重定向窗口，该窗口显示了服务器的启动信息。如果您要验证该服务器是否正在重新启动，则可以使用该窗口。您也可以使用控制台窗口暂停启动进程更改受管服务器上的 BIOS 设置。

   要查看控制台重定向窗口，服务器必须在其 BIOS 设置中启用串行端口的“控制台重定向”。控制台数据发送到串行端口。如果服务器和管理员控制台之间通过串行电缆连接，则控制台重定向将通过该电缆传输。否则，System Manager 会启动 serial over LAN (SOL) 连接，将数据从串行端口重定向到 LAN 连接。只要控制台窗口打开，SOL 连接将保持打开状态。控制台显示完毕后应关闭窗口。

   控制台窗口打开时，会打开另一个消息窗口。您可以关闭该消息窗口。在控制台窗口打开之后，控制台显示启动顺序之前，您可以在该窗口中看到随机字符。出现这些字符的原因是服务器的 MBMC 正在发送检测信号消息，该消息通过与管理员控制台的连接传送。这些字符在控制台显示启动屏幕时不会出现，但可能会在启动进程完成后重新出现。

## 设备监视器

使用设备监视器检查所选设备的连接性。如果设备失去网络连接，则此服务器无法向核心服务器发送警报。“设备监视器”检查设备是否仍然可以在网络上通信。

1. 在**所有设备**列表中，单击某设备或选择 目标设备列表。
2. 在底部窗格中，单击**操作**选项卡，然后单击**设备监视器**。
3. 要查看当前监视的设备的列表，请单击**显示监视的设备**。
4. 键入 ping 扫描之间的分钟数和产品尝试与设备建立通信的次数。
5. 选择是否对 目标设备列表中的设备或**所有设备**组中的所有设备执行操作。
6. 要停止监视所有设备，选择**从不 ping 设备**。
7. 单击**应用**。

只监视最后一组目标设备。例如，如果以设备 A 和设备 B 为目标并对其应用设备监视，则只有设备 A 和设备 B 将被核心服务器 ping。那么，如果您以设备 C 和设备 D 为目标，并对其应用设备监视，则仅监视设备 C 和设备 D；不再监视设备 A 和设备 B。

# 自定义列

使用**自定义列**修改列名和字段。“名称”是列名，“字段”包含出现在列中的属性（如果存在属性）。其他用户无法看到您对列所做的任何更改。可以在**我的设备**视图中看到对自定义列的更改。

此产品包括一个含有七列的默认列集。您不能编辑默认集合，但您可以定义自定义列集，将其用作默认值。

不建议创建可能存在多个字段名的自定义列。例如，如果要创建 Computer.Software.Package.Name 字段，而设备上安装了多个软件包，则 System Manager 将每行只列出一个软件包名称，即使同一设备上有不同的软件包名称。这样，同一设备在**所有设备**列表中将有多个条目。

### 创建自定义列集

1. 在左侧导航窗格中，单击**首选项**。
2. 单击**自定义列**选项卡。
3. 单击**新建**。
4. 请为列集输入名称。
5. 在顶部框中，在列集中选择想要的每个列标题，然后单击**添加**。

   该框将显示一个列表，其中列出了数据库中当前所存在的所有清单数据。展开此列表，选择要显示在查询结果列表中的属性。请记住，要选择那些有助于确定查询中返回的客户端的属性。如果找不到要显示的属性，您可以在 自定义属性对话框中添加属性。但是，必须在这些属性出现在查询对话框中之前将这些属性指定给机器。

   **注：**如果在有 1:* 关系的数据库中选择属性，将会得到设备的重复条目。选择 1:1 关系的属性（只有一个可能属性，如 Computer.System.Asset Tag）时，不会得到重复条目。

6. 要更改列顺序，选择列标题并单击**上移**或**下移**。
7. 要删除列，请在底部框中选中该列，然后单击**删除**。
8. 要更改为列显示的标题，请在底部框中选中该标题，单击**编辑**并进行相应修改，然后按 Enter。不支持下列扩展字符：〈，〉，’，″，!.
9. 单击**确定**保存列集。
10. 要在查看**所有设备**列表时使用自定义列集，请选中该列集，然后单击工具栏上的**设置为当前列集**。

### 编辑自定义列集

1. 在左侧导航窗格中，单击**首选项**。
2. 单击**自定义列**选项卡。
3. 选择自定义列集，然后单击**编辑**。
4. 在顶部框中，选择列标题，然后单击**添加**添加列（请参阅上述步骤 5 下的注）。
5. 要删除列，请在底部框中选中该列，然后单击**删除**。

6. 要更改为列显示的标题，请在底部框中选中该标题，单击**编辑**并进行相应修改，然后按 Enter。不支持下列扩展字符：〈，〉，’，″，!.
7. 要更改列顺序，选择列标题并单击**上移**或**下移**。
8. 单击**确定**以保存更改。

# 自定义属性

属性是设备拥有的特征或特性。在数据库中，设备的属性越多，就越容易唯一地标识该设备。您只有在以管理员权限使用 LANDesk® Server Manager 时，才能创建自定义属性。如果创建了自定义属性并已添加到核心数据库，您可以将这些属性的值分配给受管设备。如果尚未向核心数据库添加任何自定义属性，则**分配属性**选项不会显示在**操作**选项卡下。

## 向设备分配自定义属性

1. 在**所有设备**列表中，选择一台或多台设备。
2. 在底部窗格中，单击**操作**选项卡。
3. 从左侧窗格中选择**分配属性**。
4. 每个“属性名称”都有一个包含值的下拉列表。在属性名称的下拉列表中选择一个值，必要情况下重复操作。单击**选定的设备**。
5. 单击**分配**，然后单击**确定**。

还可以向已被指定为目标设备的多台设备分配自定义属性。如果目标列表中存在设备，请在上述第 4 步中单击**目标设备**。

# 页面设置

使用**页面设置**可以设置列出设备或显示图形的页面的显示首选项。

1. 在左侧导航窗格中，单击**首选项**。
2. 单击**页面设置**选项卡。
3. 在**图形类型**下拉列表中，选择希望在**报告**中显示的图形类型。
4. 在**项目数/页**框中，键入每个使用页码的页面中要显示的最大项目数。该值必须小于或等于 500 个项目。

## 初学者模式

可以在工具栏上的按钮旁边显示文本，从而帮助新用户识别功能。 如果不选择此选项，则仅在工具栏上显示图标。当鼠标停留在图标上时才显示文本。

1. 要在工具栏上的按钮旁边显示文本，请单击**显示工具栏文本**复选框。
2. 单击**更新**。

# 查看服务器信息控制台

使用服务器信息控制台可查看设备的顶层一览表信息、查看系统信息（如 CPU 或风扇信息）、监控健全性状态和设备关键组件的阈值、管理漏洞、以及打开、关闭或重启设备。左侧导航窗格中列出了“服务器”信息控制台的以下部分。

- 系统信息
- 软件更新
- 监控
- 规则集
- 电源选项
- 硬件配置

为了查看某设备的服务器信息控制台，必须首先在该设备上部署标准管理代理（请参见 配置代理）。此外，在安装代理后必须重新启动该设备，服务器信息控制台才能正常工作。在核心服务器以及受管设备上安装代理时，需要执行上述的重新启动操作。

**查看服务器信息控制台**

1. 在**我的设备**视图中，双击设备名称。

   控制台将在新的浏览器窗口中打开，默认情况下显示**健全性一览表**页面。

2. 单击左侧导航窗格中的按钮可查看服务器信息以及使用可用的工具。

## 系统信息

**系统信息**包含有关设备健全性的一览表数据，以及有关硬件和软件的信息、系统日志和其他数据（如资产和网络信息）。

## 健全性一览表

**健全性一览表**页面可快速提供该设备系统健全性的概要状况。您可以一眼看出所选的硬件元素是否正常工作，是否有任何潜在问题需要加以处理。

当任何健全性元素处于警告或严重状态时，相应的按钮将包含一个黄色（警告）或红色（严重）图标来指示存在问题。单击该按钮可查看导致警告或严重警报的事件说明。

## 系统一览表

使用**系统一览表**页面可查看有关所选设备的重要信息。根据设备上配置的硬件和软件类型，该页面上列出的信息可包括下列内容。

- **健全性：**您设置的条件和参数所定义的设备整体健全性。
- **类型：**设备的类型，例如：打印、应用程序或数据库。
- **制造商：**设备制造商。
- **型号：**设备的型号。
- **BIOS 版本：**设备 BIOS 的版本。
- **操作系统：**设备的操作系统。
- **操作系统版本：**操作系统的版本号。

- **CPU**：设备处理器的制造商、型号和运行速度。
- **漏洞扫描器**：漏洞扫描器的版本。
- **远程控制**：远程控制代理的版本。
- **软件分发**：软件分发代理的版本。
- **清单扫描器**：清单扫描器的版本。
- **IPMI 类型，IPMI 版本**：设备正在使用的 IPMI 的类型和版本号。
- **SDR 版本**：设备 BMC 中传感器数据记录的版本。
- **BMC 版本**：设备底板管理控制器的版本。
- **内核**：对于 Linux 设备，已安装的内核的版本号。
- **监测**：设备上监视代理的版本号。
- **CPU 使用**：处理器当前的使用率百分比。
- **使用的物理内存***：在设备上总共使用的物理内存的百分比。
- **使用的虚拟内存***：在设备上总共使用的虚拟内存的百分比。
- **上次重启时间***：设备上次重启的日期和时间（按数据库所处的时区计）。
- **驱动器**：设备上的驱动器以及驱动器空间总量和已用空间百分比。

对于 Windows，此信息来自注册表；对于 Linux，此信息来自配置文件。

*设备上安装代理后会出现此信息。

## 硬件

使用**硬件**页面可查看有关设备硬件配置的详细信息。**硬件**列表中的各项可分为以下类别。请注意，并非所有设备都会显示全部类别。例如，如果设备没有风扇和温度传感器，则该列表中不会显示**冷却设备**类别。

- **CPU**：处理器和高速缓存
- **存储设备**：逻辑驱动器、物理驱动器、可移动介质和存储适配器
- **内存**：使用信息和内存模块
- **机箱**：服务器的机箱；查看机壳是打开还是关闭的
- **输入设备**：键盘、鼠标和其他设备
- **主板**：主板、扩展槽和 BIOS
- **冷却设备**：风扇和温度传感器
- **电源**：电源和电压

### 为硬件项目设置警报阈值

**硬件**列表中的某些项表示来自设备中的传感器（如温度传感器）的数据。如果受管设备包含的组件带有支持的传感器，则可以更改将会触发警报的传感器读数。例如，CPU 温度传感器可以具有触发警告和严重警报的温度下限和上限读数。通常，阈值是基于制造商建议的设置，但是，您可以使用**阈值**对话框更改上限和下限设置。

1. 在服务器信息控制台中，单击**系统信息**。
2. 展开**硬件**文件夹，然后逐级展开，找到所需的硬件元素（如**冷却设备|温度**）。
3. 在传感器列表中，双击要设置阈值的传感器。

4. 在下限阈值和/或上限阈值文本框中输入值，或者向左或向右拖动跟踪条上的滑块来更改值。
5. 单击**更新**以保存更改。
6. 要返回阈值的原始值，请单击**恢复默认值**。

## 日志

“日志”页面显示本地系统日志、IPMI 设备的系统事件日志 (SEL) 和警报日志。

本地日志（如应用程序、安全性和系统日志）不包含从控制台清除日志的按钮，但可以使用“Windows 计算机管理”查看和清除日志。

如果该设备的 BIOS 可以清除 SMBIOS 日志，请单击**清除日志**按钮删除所有日志条目。如果 BIOS 不支持此项操作，则该按钮不可用。

## 软件

**软件**页面显示有关此设备上的进程、服务和程序包的摘要信息以及当前环境变量的列表。

- **进程：**显示正在运行的进程；选择一个进程并单击**杀掉进程**将其终止
- **服务：**显示设备上可用的服务及其状态；选择一项服务并单击**停止**、**启动**或**重新启动**进行更改
- **程序包：**列出已安装的程序包以及版本号和供应商名称
- **环境：**列出设备上当前设置的环境变量

## 其他

**其他**页面显示资产信息以及网络硬件和连接的摘要信息。

- **资产信息：**查看和编辑资产管理信息，如位置和资产标签号；还可以查看系统信息，如序列号、制造商和机箱类型
- **网络信息：**查看已安装网络硬件的列表、网络活动统计数据、配置一览表（包括 IP 地址、默认网关地址以及 WINS、DHCP 和 DNS 服务器信息）以及当前网络连接（映射的驱动器）的列表

# 软件更新

使用**软件更新**页面可扫描选定设备上已检测到的漏洞。

### 检查已检测到的漏洞

1. 在**我的设备**视图中，双击要配置的设备。在新浏览器窗口中将打开服务器信息控制台。

2. 在左侧导航窗格中，单击**软件更新**。

**列说明**

- **ID**：通过一个由供应商定义的唯一字母数字代码来标识漏洞。
- **严重性**：指示漏洞的严重级别。可能的严重级别包括：Service Pack、严重、高级、中级、低级、不适用和未知。
- **标题**：采用简短的文本字符串描述漏洞的性质或目标。
- **语言**：指示已受漏洞影响的操作系统的语言。
- **发布日期**：指示供应商发布漏洞的日期。
- **无提示安装**：指示是否无提示安装与漏洞相关的修补程序文件（不与用户交互）。某些漏洞可能有多个修补程序。如果该漏洞的任一个修补程序无法进行无提示安装，漏洞的**无提示安装**属性将显示为**否**。
- **可修复的**：指示是否可以通过修补程序文件部署和安装修复漏洞。可能的值为：“是”、“否”和“某些”（对于包含多个检测规则的漏洞，且并非所有检测到的漏洞都可以修复）。

# 监控

使用**监控**可查看性能计数器和图形，并设置设备组件的阈值。有关此功能的详细信息，请参见 设备监控部分。

**选择要监视的性能计数器**

1. 在**我的设备**视图中，双击要配置的设备。在新浏览器窗口中将打开服务器信息控制台。
2. 在左侧导航窗格中，单击**监视**。
3. 单击**性能计数器设置**选项卡。
4. 在**对象**列中，选择要监视的对象。
5. 如果适用，在**实例**列中，选择要监视对象的实例。
6. 在**计数器**列中，选择要监视的特定计数器。
7. 指定轮询频率以及要保留计数器历史记录的天数。
8. 在**计数器超出范围后报警**文本框中，指定生成警报前允许的计数器超出阈值的次数。
9. 指定阈值上限和 / 或下限。
10. 单击**应用**。

**查看受监视计数器的性能图形**

1. 单击**活动性能计数器**选项卡。
2. 从列表中选择一个计数器。
3. 在**计数器**列表中，选择您要查看性能图形的计数器。
4. 选择**查看实时数据**以显示当前性能的图形。或者选择**查看历史记录数据**以显示选定计数器时指定的（保存历史记录）时期的性能图形。

在性能图形中，水平轴表示已经过的时间。垂直轴代表测量的单位，如字节/秒（例如，在监控文件传输时）、百分比（监控 CPU 使用率百分比时）或可用字节（监控硬盘驱动器空间时）。

# 规则集

使用**规则集**页面可查看指定给选定设备的警报和监视规则集配置列表，并查看每个警报的详细信息。

**查看警报规则集**

1. 在**我的设备**视图中，双击要配置的设备。控制台将在新浏览器窗口中打开。
2. 在左侧导航窗格中，单击**规则集**。
3. 单击**警报规则集**选项卡。

下面介绍提供的关于每个警报的详细信息。有关修改这些详细信息的更多信息，请参见 使用警报。

- **状态达到时：**当警报状态达到显示的状态时，将生成警报。
- **影响健全性：**如果警报状态到达指定的阈值，将影响设备的整体健全性状态。影响健全性的警报的选择在“警报规则集”对话框中确定。
- **规则集名称：**警报规则集的名称，在 警报规则集对话框中定义。
- **警报类型：**生成的警报类型，例如电子邮件、SNMP 陷阱或执行程序。
- **操作配置：**当生成警报时发生的操作，在 操作规则集对话框中定义。
- **警报处理程序：**与警报相关的处理程序，例如电子邮件处理程序。
- **实例：**指示警报的特定源。

**查看监视规则集**

1. 在**我的设备**视图中，双击要配置的设备。在新浏览器窗口中将打开服务器信息控制台。
2. 在左侧导航窗格中，单击**规则集**。
3. 单击**监视规则集**选项卡。

下面介绍提供的关于每个监视规则集的详细信息。有关修改这些详细信息的更多信息，请参见 关于监视。

- **名称：**在 监视页面中定义的规则集配置的名称。
- **规则集名称：**规则集是否为默认规则集。
- **启用：**规则集是否已在设备上启用为可执行。
- **警告阈值：**在超出该阈值后，设备将向核心服务器发送警告消息。
- **严重阈值：**在超出该阈值后，设备将向核心服务器发送严重消息。
- **检查频率：**监视项目的频率。

# 电源选项

使用**电源选项**，您可以关闭、重启和（在使用受管 IPMI 和 Intel AMT 设备的情况下）打开远程设备。在使用非 IPMI 服务器的情况下，服务器必须部署 LANDesk 代理才能执行重新启动和关机功能。

使用 IPMI 和 Intel AMT 设备，则必须配置了正确的证书才能执行开机/关机和重新启动功能。如果 IPMI 或 Intel AMT 设备已部署了 LANDesk 代理，则可以执行关机和重新启动功能而无需 IPMI 或 Intel AMT 证书。要配置 IPMI 设备的 BMC 凭证或 Intel AMT 设备凭证，请使用配置服务实用程序（请参见 配置服务和凭证）。

**使用所选设备上的电源选项**

1. 在**我的设备**视图中，双击要配置的设备。控制台将在新浏览器窗口中打开。
2. 在左侧导航窗格中，单击**电源选项**。
3. 从以下选项中进行选择：

   -  重新启动
   -  关机
   -  打开电源

## 硬件配置

使用**硬件配置**工具，可以为具有 IPMI 或 Intel* AMT 功能的设备配置选项。此工具以及所有选项仅显示在具有相应硬件的设备上（例如，仅当设备被识别为 IPMI 设备时，才会显示 IPMI 选项）。

可以生成用于部署 Intel AMT 设备的 ID、查看生成的 ID 以及更改与 Intel AMT 设备部署相关的配置选项。还可以定义用于检测和阻止设备上可疑网络活动的断路器策略，并且可以启用代理存在监控功能以确保设备上的管理代理连续运行。（有关详细信息，请参阅 Intel AMT 支持。）

对于 IPMI 设备，可以自定义配置选项，例如监视计计时器、电源选项和 BMC 用户设置。还可以配置如何使用 LAN 通道或 serial over LAN，以保持与 IPMI 设备的带外通信。（有关详细信息，请参阅 IPMI BMC 配置。）

对于具有 Dell* DRAC（远程访问控制器）的设备，可以查看 Dell DRAC 日志以及编辑用于访问 OpenManage Server Administrator 的用户名。（有关详细信息，请参阅 管理 Dell DRAC 设备。）

# 管理 Intel AMT 设备

搜寻到 Intel* AMT 设备并将其添加到核心数据库进行管理之后，即使该设备没有安装 LANDesk 代理，也能以有限的方式对其进行管理。（有关搜寻设备并将其移动到核心数据库的信息，请参阅搜寻 Intel* AMT 设备。）

与安装了 Intel AMT 和 System Manager 管理代理的设备相比，仅有 Intel AMT 的设备的可用管理选项见下表。

| | 仅有 Intel AMT | Intel AMT 和代理 | 仅有代理 |
|---|---|---|---|
| 清单 | 一览表 | X | X |
| 事件日志 | X | X | X |
| 远程启动管理器 | X | X | |
| 禁用操作系统网络 | | X | |
| 启用操作系统网络 | | X | |
| 重新启动时强制运行 vulscan | | X | |
| 清单历史记录 | | X | X |
| 远程控制 | | X | X |
| 对话 | | X | X |
| 文件传输 | | X | X |
| 远程执行 | | X | X |
| 唤醒 | | X | X |

| | 仅有 Intel AMT | Intel AMT 和代理 | 仅有代理 |
|---|---|---|---|
| 关闭 | | X | X |
| 重新启动 | | X | X |
| 清单扫描 | | X | X |
| 计划任务和策略 | 有限的 | X | X |
| 组选项 | | X | X |
| 运行清单报告 | | X | X |
| Intel AMT 警报 | | X | X |

**查看某设备的 Intel AMT 清单一览表**

1. 在**所有设备**列表上双击设备。
2. 在服务器信息控制台中，单击 **Intel AMT 选项**。
3. 单击**清单一览表**。

此一览表显示设备的 GUID、产品和制造商、序列号、BIOS、处理器、内存一览表和 Intel AMT 版本号。如果缺少任何信息，可单击**更新清单**来刷新数据。

## 访问以企业模式部署的设备

当以企业模式部署 Intel AMT 设备时，核心服务器会在该设备上安装证书，用以进行安全通信。如果该设备将由另一个核心服务器管理，必须对设备取消部署，然后由新的核心服务器重新部署。否则，该设备的 Intel AMT 访问将会由于新的核心服务器不具有匹配的证书而无法响应。同样，如果任何其它计算机尝试访问该设备上的 Intel AMT 功能，也将会由于它不具有匹配的证书而导致失败。（有关部署模式的信息，请参阅 Intel* AMT 支持。）

## Intel AMT 事件日志

使用 System Manager 可查看 Intel AMT 设备生成的事件日志。具体的设置决定了在此日志中捕获哪些事件。从中可查看事件的日期/时间、事件来源（实体列）、说明以及 Intel AMT 设置所决定的严重性（严重或不严重）。还能以逗号分隔值 (CSV) 的格式导出日志数据。

**查看 Intel AMT 事件日志**

1. 在**所有设备**列表上双击设备。
2. 在服务器信息控制台中，单击**系统信息**。
3. 展开**日志**，单击 **Intel AMT 日志**。
4. 要将日志导出到 CSV 格式的文件，请单击工具栏上的**导出**按钮并指定保存该文件的位置。
5. 要清除日志中的所有数据，请单击工具栏上的**清除日志**按钮。
6. 要更新日志条目，请单击工具栏上的**刷新日志**按钮。

## Intel AMT 电源选项

System Manager 包含可开关 Intel AMT 设备电源的选项。只要设备接入网络并且配有备用电源，那么即便设备操作系统没有响应，也能使用这些选项。

System Manager 启动电源选项命令时，某些情况下可能无法验证接收此命令的硬件是否支持这些命令。Intel AMT 的某些设备可能不支持所有电源选项功能（例如，设备可能支持 IDE-R 从 CD 重新启动但不支持从软盘重新启动）。如果某一电源选项在特定设备上不可用，则请参阅硬件供应商文档。如果电源选项未按要求执行，则可以对设备从 Intel 升级的任何固件或 BIOS 进行检查。

您可简单地打开或关闭设备电源，或者重新启动并指定设备重新启动的方式。选项说明见下表。

| | |
|---|---|
| 关闭电源 | 关闭设备电源 |
| 打开电源 | 打开设备电源 |
| 重新启动 | 先关闭设备电源再打开其电源 |
| 正常启动 | 使用设备默认设置的任何启动顺序启动设备 |
| 从本地硬盘启动 | 无论设备默认何种启动模式，均强制从设备硬盘启动 |
| 从本地 CD/DVD 驱动器启动 | 无论设备默认何种启动模式，均强制从 CD 或 DVD 驱动器启动 |
| PXE 启动 | 重新启动时，支持 PXE 的设备会在网络上搜索 PXE 服务器，如果找到该服务器，则会在设备上启动 PXE 启动会话。 |

| | |
|---|---|
| IDE-R 启动 | 使用选定的 IDE 重定向选项重新启动设备（请参阅下文） |
| 进入 BIOS 设置 | 设备启动后，用户可进入 BIOS 设置 |
| 显示控制台重定向窗口 | 启动设备时，以 serial over LAN 模式启动以显示控制台重定向窗口。 |
| IDE 重定向：从软盘重新启动 | 设备启动时，会从软盘驱动器或指定映像启动（软盘映像文件必须为 .img 格式；请参阅下文说明） |
| IDE 重定向：从 CD/DVD 重新启动 | 启动设备时，从 CD 驱动器或指定映像启动（CD 映像文件必须为 .iso 格式；请参阅下文说明） |
| IDE 重定向：从指定的映像文件启动 | 设备启动时，它将从指定的映像文件启动（请参阅以下说明） |

**使用 Intel AMT 电源选项**

1. 在**所有设备**列表上双击设备。
2. 在服务器信息控制台中，单击**电源选项**。
3. 选择电源命令。如果选择**重新启动**，请选择一个启动选项。
4. 单击**发送**以启动该命令。

## 有关使用 IDE 重定向选项的说明

要使用 IDE 重定向选项，则必须同时指定启动软盘或软盘映象文件和启动 CD/DVD 或 CD/DVD 映像文件。软盘映像文件必须为.img 格式；CD 映像文件必须为 .iso 格式。某些 BIOS 可能要求 CD 映像位于硬盘上。

Intel AMT 通常记住最后一次的 IDE-R 设置，但是 System Manager 在 45 秒后清除了这些设置。因此，后续启动时系统将不会重新启动 IDE-R 功能。Intel AMT 设备上的 IDE-R 会话将持续 6 个小时或到 System Manager 控制台关闭为止。6 小时后仍在进行中的任何 IDE-R 操作将被终止。

## 在 Intel AMT 机器上强制执行漏洞扫描并禁用网络访问

配置 Intel AMT 的设备在安装 LANDesk 代理后，该代理便能够帮助您解决恶意软件或其它阻止您访问设备的问题。

amtmon.exe 服务会随 LANDesk 代理一起安装。如果此服务在设备上运行，则在下次重新启动时可以强制执行漏洞扫描　　以尝试识别设备上的任何恶意软件。如果与设备的通信失败，那么即便在操作系统不能使用的情况下（如恶意软件通过消耗全部 CPU 周期而使操作系统无法使用）仍能禁用设备的网络连接。通过禁用网络连接，可以防止设备通过网络发送多余的数据包。

LANDesk 代理安装到 Intel AMT 设备上后，就可以使用 **Intel AMT 选项**页面上的以下选项：

- **操作系统网络连接：**单击**禁用**可禁用操作系统网络堆栈以停止访问网络；如果操作系统的网络访问已经禁用，则可以单击**启用**将其启用。
- **重新启动后扫描漏洞：**设备下次重新启动时强制运行漏洞扫描器。

当设备未作出响应或者设备上可能运行着恶意软件时，建议在下次重新启动时先运行漏洞扫描，以尝试识别该问题。如果该问题持续发生且机器正感染/攻击网络，或者无法访问设备，则可选择禁用操作系统 NIC。

**重新启动后强制执行漏洞扫描**

1. 在**所有设备**列表上双击设备。
2. 在设备控制台窗口中，单击 **Intel AMT 选项**。
3. 单击**配置选项**，然后再单击**扫描**。设备随即显示一条消息，说明下次重新启动时将运行扫描。
4. 要关闭或重新启动设备，请使用以上所述的 Intel AMT 远程启动管理器功能。

**在没有反应的设备上启用或禁用网络连接**

1. 在**所有设备**列表上双击设备。
2. 在设备控制台窗口中，单击 **Intel AMT 选项**。
3. 要禁用设备的网卡以停止其与网络上其它设备的通信，请单击**禁用**。如果网络连接已禁用，设备上将显示一条消息，说明网卡已禁用。
4. 如果设备可以安全地重新接入网络，请单击**启用**。如果连接已恢复，设备上将显示一条消息，说明网卡已重新启用。

## 打开 Intel AMT 配置屏幕

System Manager 含有一个可打开 Intel AMT 配置屏幕的链接。这是 Intel 提供的一个界面，可用于查看设备状态、硬件信息、Intel AMT 事件日志、远程启动设置和网络设置。您还可以用其添加和编辑设备的 Intel AMT 用户帐户。显示此屏幕的窗口独立于 System Manager 控制台。有关使用此界面的任何问题可咨询该设备制造商的技术支持。

**打开 Intel AMT 配置屏幕**

1. 在**所有设备**列表上双击设备。
2. 在设备控制台窗口中，单击 **Intel AMT 选项**。
3. 单击 **Intel AMT 控制台**，然后单击**启动 Intel AMT web 控制台**。

# 基于角色的管理

## 关于基于角色的管理

使用基于角色的管理可以根据用户在系统中的管理角色来配置用户访问产品工具和其他设备的权限。利用基于角色的管理功能，可以指定用户范围来确定用户能查看和管理的设备，给用户分配权限来确定他们能执行的任务。

管理员（具有管理员权限的用户）通过单击左侧导航窗格中的**用户**，即可访问基于角色的管理工具。

通过基于角色的管理，可以根据产品用户的权限和范围，为这些用户分配特殊的管理角色。*权限*决定了用户能够查看和利用的产品工具和功能。*范围*决定用户可以查看和管理的设备范围。

您可以根据用户的职责、您希望他们能执行的管理任务以及想让他们看到、访问和管理的设备来为他们创建角色。您可以将用户能访问的设备限定在某个地理位置，例如国家、地区、州（省）、城市甚至一个办公室或部门。也可以将访问限定为特定的平台、处理器类型或某些其他设备硬件或软件属性。通过使用基于角色的管理，您可以全权掌握要创建多少个不同的角色，哪些用户可以充当这些角色，他们的设备访问范围应该有多大或多小。

### 管理角色示例

下表列出了一些您可能要实施的管理角色、用户要执行的常见任务，以及用户有效行使该角色的职责所需的权限。

| 角色 | 任务 | 所需的权限 |
|---|---|---|
| 管理员 | 配置核心服务器、管理用户、配置警报、集成其他公司产品等（当然，具有全部权限的管理员可以执行任何管理任务。） | 管理员<br>（意味着拥有所有权限） |
| 资产管理员 | 搜寻设备、配置设备、运行清单扫描器、启用清单历史记录跟踪等 | 设备搜寻、软件分发和公共查询管理 |
| 报告管理员 | 运行预定义报告、打印报告等。 | 报告（所有报告都必需） |

这些只是角色示例。基于角色的管理非常灵活，因此，您可以根据自己的需要创建任意多个自定义角色。您可以给不同的用户分配一些相同的权限，但将他们的访问权限限制为范围较窄的一组设备。甚至可以用范围来限制管理员，使他们实质上只是某地理区域或某类受管设备的管理员。如何利用基于角色的管理取决于您的网络、人力资源以及您的具体需要。

要贯彻实施基于角色的管理，只需将当前的本地 Windows 用户指定为产品用户，或创建和添加新的本地 Windows 用户并将其指定为产品用户，将用户添加到 Management Suite 用户组，然后给他们分配必要的权限（以利用产品功能）和范围（以访问受管设备）。请按照下列步骤进行操作：

## 了解权限

权限授予用户对特定工具和功能的访问。用户必须具有所需的权限才能执行相应的任务。例如，要远程控制其范围内的设备，用户必须具有“远程控制”权限。如果您安装了多个 LANDesk 管理产品，就可从任何控制台将权限分配给用户，并且这些权限在所有控制台中都是有效的。

当未将某权限授予用户时，此用户在产品控制台中将看不到与该权限关联的工具。例如，如果用户不具有报告权限，则报告项将不显示在左侧导航窗格中。下表显示了用户需要具有哪些权限才可以使工具显示出来。

| 工具 | 要在左侧导航窗格中显示工具，用户需要具有的权限 |
|---|---|
| 我的设备 | Basic Web console |
| 代理配置 | 管理员 |
| 警报 | 警报和监视 |
| 设备搜寻 | 设备搜寻 |
| 监控 | 警报和监视 |
| 查询 | 基本 Web 控制台、公共查询管理、报告 |
| 报告 | 报告、修补程序管理 |
| 计划任务 | 设备搜寻 |
| 脚本 | 修补程序管理 |
| 用户 | 管理员 |
| 软件更新 | 修补程序管理 |

| 工具 | 要在左侧导航窗格中显示工具，用户需要具有的权限 |
|---|---|
| 首选项 | Basic Web console |
| 硬件配置 | 管理员 |

要了解每种产品权限以及如何使用权限来创建管理角色的详细信息，请参阅下面的说明。

**范围控制对设备的访问**
在使用这些权限授予的功能时，用户始终被限制在其范围（他们能够看到和操纵的设备）之内。

## 管理员

管理员权限的用户能完全访问所有产品工具（但是，这些工具的使用仍然仅限于该管理员范围中包含的设备）。

这是默认授予新加用户的授权，除非您修改了“默认模板用户”的设置。

具备管理员权限的用户能够：

- 在左侧导航窗格中看到和访问**用户**工具
- 在左侧导航窗格的**首选项**中查看产品许可。
- 执行下面列出的其它权限允许的所有产品任务

**建议您不要删除“管理员”用户。**如果您是登录特定 LDSM 控制台的最后一个管理员，并进入“Windows 计算机管理”及从 Management Suite 组删除“管理员”用户，则当您重新进入此控制台时可能会遇到问题。大约过 20 分钟左右（这是默认的会话超时），您仍可作为管理员登录，但当您启动任何操作或刷新您作为管理员登录的控制台浏览器（用 F5 键）时，仅属于管理员的任何权限将不再可用。建议您在任何情况下都不要删除最后一个“管理员”用户。

**权限和工具的相关说明**
管理员权限与**用户**工具具有排他关联性。如果用户没有管理员权限，则该用户的控制台中就不会显示这个工具。

产品控制台中的所有工具均与相应的权限相关联（如下所述）。

## 设备搜寻

具备“设备搜寻”权限的用户能够：

- 在网络上查找未将清单扫描提交至产品核心数据库的设备，提交清单扫描的方式包括网络扫描、标准管理代理搜寻和 IPMI 搜寻
- 安排定期搜寻时间
- 将设备从“搜寻的”移动到“受管的”

### 公共查询管理

具备“公共查询管理”权限的用户能够：

- 创建所有用户都可以使用的查询
- 创建或删除公共查询
- 修改 / 编辑现有公共查询

### 报告

具备“报告”权限的用户能够：

- 在左侧导航窗格中看到和访问**报告**工具
- 运行预定义的报告

### 修补程序管理

“修补程序管理”权限专用于漏洞扫描功能。有关详细信息，请参阅“使用软件更新工具”。

### Basic Web console

具备“基本 Web 控制台”权限的用户能够使用与此权限相关联的各种功能。这些功能如下所示，其中包括功能中的所有例外情况。

- **我的设备**（此权限不允许更新公共组，也不允许删除**操作**选项卡下的设备）
- 更改首选项（而不是自定义属性）

### 警报和监视

具备“警报和监视”权限的用户能够：

- 监视驱动器、处理器、内存、进程、系统的 Web 服务器每秒传输的字节等系统和操作系统组件的性能
- 跟踪所有受管设备的确切健全性
- 自定义达到某种严重级别（严重、警告、信息、良好、未知）或阈值（例如，如果硬盘使用率超过硬盘容量的 90%）时要发送的警报
- 选择警报超过阈值时要采取的操作（将信息添加到日志、通过电子邮件发送通知、在核心设备或单个设备上运行程序，或通过网络将 SNMP 陷阱发送到 SNMP 管理控制台）

## 添加产品用户

产品用户是指可以登录到产品控制台并对网络中的特定设备执行特定任务的用户。

产品用户实际上不是在控制台中创建的。而是在将用户添加到核心服务器上 Windows 用户环境下的 LANDesk Management Suite 组后，它们将显示在**用户**选项卡中（在左侧导航窗格中，单击**用户**）。**用户**组显示了目前保存在核心服务器的 LANDesk Management Suite 组内的所有用户。

**用户**组中有两个默认用户：

- **默认模板用户**：此用户基本上是用户属性（权限和范围）的模板，在将新用户添加到 LANDesk Management Suite 组时，可使用该模板对新用户进行配置。换句话说，当您将某用户添加到 Windows 环境中的该组时，该用户会继承当前在“默认模板用户”属性中定义的权限和范围。如果“默认模板用户”选定了所有权限并选定了“默认范围 - 所有机器”，则任何新加到 LANDesk Management Suite 组内的用户被加到**用户**组中时，其权限是能使用所有产品工具，范围是能够访问所有设备。

  通过右击“默认模板用户”并单击**编辑权限**，可以更改其属性设置。例如，若要同时添加大量用户，但不希望他们能访问所有工具或设备，可先更改“默认模板用户”的设置，然后将用户添加到 LANDesk Management Suite 组中（请参见下面的步骤）。

  “默认模板用户”不能删除。

- **默认管理员**：这是在安装此产品的核心组件时登录到服务器上的管理用户。

当您在 Windows 中将某用户添加到 LANDesk Management Suite 组后，系统会自动将该用户读入**用户**窗口中的**所有用户**组中，该用户将继承当前“默认模板用户”的相同权限和范围。系统将显示该用户的名称、范围和权限。

如果您在 Windows 用户环境中将某用户从 LANDesk Management Suite 组中删除，则该用户将不再处于活动状态，并且可以从**用户**组中将其删除。不过，该用户的帐户仍会保存在您的服务器上，您随时可将其添回到 LANDesk Management Suite 组中。另外，还会在**用户设备**、**用户查询**、**用户报告**和**用户脚本**下保留该用户的子组；因此，可以恢复用户且不丢失其数据，并可以将数据复制给其他用户。

要刷新**用户**列表以显示任何新添加的用户，请单击**用户**，然后单击浏览器上的**刷新**按钮。

### 将用户或域组添加到 LANDesk Management Suite 组

1. 浏览并找到服务器的**管理工具|计算机管理|本地用户和组|组**实用程序。
2. 右击 **LANDesk Management Suite** 组，然后单击**添加到组**。
3. 单击**添加**，然后键入用户或在列表中选择用户。
4. 单击**添加**，然后单击**确定**。

---

**注意：**使用以下方法也可以将用户添加到 LANDesk Management Suite 组中：在“用户”列表中右击相应的用户帐户，单击**属性|该组的成员**，然后单击**添加**来选择该组并添加该用户。

---

如果用户帐户在 Windows 中尚不存在，则必须先在服务器上创建它们。

**创建新的用户帐户**

1. 浏览并找到服务器的**管理工具|计算机管理|本地用户和组|用户**实用程序。
2. 右击**用户**，然后单击**新建用户**。
3. 在“新建用户”对话框中，输入名称和密码。
4. 指定密码设置。
5. 单击**创建**。“新建用户”对话框会一直处于打开状态，因此，您可以创建其他的用户。
6. 单击**关闭**，退出该对话框。
7. 将用户添加到 LANDesk Management Suite 组中，使他们出现在控制台上的“用户”组中。

现在，可以给产品用户分配权限和范围了。

# 创建范围

范围定义产品用户能够查看和管理的设备。如果您安装了多个 LANDesk 管理产品，就可从任何控制台将范围分配给用户，并且这些范围在所有控制台中都是有效的。

根据您的需要，范围可大可小，可以包含已扫描到核心数据库中的所有受管设备、只包含一个设备或不包含设备。正是这种灵活性加上模块化的工具访问，使基于角色的管理成为用途如此广泛的管理功能。

## 默认范围

基于角色的管理包括两个默认的范围。在配置默认模板用户的用户属性时，这两个预定义的范围很有用。

- **（默认）无机器范围：**排除数据库中的所有设备。
- **（默认）所有机器范围：**包括数据库中的所有设备。

不能编辑或删除默认范围。

## 自定义范围

可创建以下类型的自定义范围，然后将它们分配给用户：

- **基于查询的范围：**仅控制对符合自定义查询搜索的设备的访问。您可以选择现有的查询来定义范围，也可以在**查询**对话框中创建新的查询来定义范围。有关创建查询的详细信息，请参阅“创建数据库查询”。
- **基于组的查询：**仅控制对位于选定组中的服务器的访问。可以从**组范围属性**对话框中选择组来定义范围。

可以为任何用户指定多个范围。为用户指定多个范围后，累积有效范围（即，可作为指定范围的组合的结果来访问和管理的整个设备范围）是一个简单组合。

通过随时添加和删除范围，可以自定义用户的有效范围。可结合使用所有范围类型。

**创建范围**

1. 在左侧导航窗格中，单击**用户**。
2. 在**范围**选项卡上，单击**新建查询范围**或者**新建组范围**工具栏按钮。
3. 输入新范围的名称。
4. 选定基于查询的范围之后，选择一个现有查询，或单击**定义**来创建新的查询。单击“确定”。
5. 选定基于组的范围之后，选择一个组，然后单击**确定**。
6. 单击**确定**保存范围，并关闭该对话框。

# 为用户分配权限和范围

- 关于“用户权限/范围”对话框
- 关于“远程控制设置”对话框

添加了产品用户，了解了权限和他们如何控制对功能和工具的访问，而且创建了允许或限制对受管设备的访问的设备范围后，建立基于角色的管理的下一步就是给每个用户分配适当的权限和范围。

您可以随时修改用户的权限和范围。

如果您修改了某个用户的权限或范围，这些更改将在该用户下次登录控制台后生效。

**为用户分配权限和范围**

1. 在左侧导航窗格中，单击**用户**。
2. 展开用户的列表，查看当前作为核心服务器的 Windows NT 环境中 LANDesk Management Suite 组内成员的所有用户。

   该列表显示用户名和分配的权限（选中字符表示此权限处于启用或活动状态）。

3. 右击一个用户，然后单击**编辑**。
4. 在**用户权限/范围**对话框中，根据需要选中或清除权限。
5. 单击**范围**选项卡，并从**分配范围列表**中选择范围。
6. 单击**应用**。

新的权限会显示在列表中相应用户名的旁边，当该用户下次连接到核心服务器时，这些权限就会生效。

**删除范围**

1. 在左侧导航窗格中，单击**用户**。
2. 在**范围**选项卡上，单击要删除的范围，然后单击**删除**。单击“确定”。

删除范围时需特别注意。分配到这些范围内的用户将可以访问以前该范围禁止的权限。

## 关于“用户权限/范围”对话框

使用此对话框可查看和修改用户的分配权限和范围。通过选择某个用户并单击**编辑**来打开对话框。

**“权限”选项卡：**列出分配给用户的权限。

- **管理员**
- **设备搜寻**
- **公共查询管理**
- **报告**
- **修补程序管理**
- Basic Web console
- **警报和监视**

**“范围”选项卡：**列出分配给用户的范围。

- **分配的范围：**指明用户的当前范围。
- **添加：**打开**添加范围**对话框，您可以在其中选择要为用户添加的范围。
- **删除：**删除所选范围。
- **取消：**关闭对话框，但并不保存更改。

# 设备搜寻

## 使用设备搜寻

“设备搜寻”可在网络上找到未安装搜寻核心服务器代理并且未将清单扫描提交到该核心数据库的设备。设备搜寻有多种方式来查找网络上的设备。

- **网络扫描：**通过执行 ICMP ping 扫描来查找计算机。这是最彻底的搜寻，但耗时较长（如果使用 IP 指纹方式）。可以将搜索限制在某些 IP 和子网范围之内。默认情况下，此选项使用 NetBIOS 收集设备的有关信息。还可以选择“IP 特征”，在多数情况下，该特征也可以提供操作系统类型。网络扫描选项中也有一个**使用 SNMP** 选项，可以用于配置使用 SNMP 对 SNMP 设备（如某些打印机等）进行扫描。
- **CBA 搜寻：**在计算机中查找标准管理代理（以前在 Management Suite 中称作通用基本代理 [CBA]）。此选项搜寻通过 Server Manager、System Manager 等进行管理的计算机。还可以选择 PDS2 选项来搜寻使用旧版 LANDesk PDS2 代理的设备。CBA 搜寻对 Linux 机器不支持，但如果选择了 PDS2，则可搜寻到装有代理的 Linux 机器。
- **IPMI：**查找启用了 智能型平台管理界面的服务器，该界面允许访问底板管理控制器 (BMC) 而无需考虑服务器是否打开或者操作系统所处的状态。
- **服务器机箱：**查找刀片式服务器机箱管理模块 (CMM)。服务器机箱中的刀片式服务器将作为普通服务器被检测。
- **Intel* AMT：**查找采用 Intel 活动管理技术（版本 1）的设备，该技术允许限制管理功能而无需考虑服务器是否打开或者操作系统所处的状态。

设备搜寻尝试搜寻与每个设备相关的基本信息。并非下面的所有信息都可适用于每台设备。

- **节点名称：**搜寻到的设备的名称（如果有）。
- **IP 地址：**搜寻到的 IP 地址。
- **子网掩码：**搜寻到的子网掩码。
- **类别：**设备所属的设备搜寻组。
- **操作系统名称：**搜寻到的操作系统说明（如果有）。

当设备搜寻第一次找到设备后，会搜索核心数据库，查看该数据库**我的设备**列表中是否已有该设备的 IP 地址和名称。对**未管理**列表中的设备会进行重新搜寻，有可能会获得更多数据。如果有相匹配的信息，设备搜寻会忽略该设备。如果没有相匹配的信息，设备搜寻会将该设备添加到**不受管**设备表。**未管理**表中的设备不使用 System Manager 许可证。一旦设备将清单扫描发送到核心数据库，就认为该设备是受管理的设备。将设备移动到**所有设备**组中后，该设备不再显示在**搜寻到的设备**列表中。

IPMI 设备必须具有 BMC（底板管理控制器），其配置将设备搜寻为 IPMI 设备，并可使用完全 IPMI 功能。如果没有配置 BMC，设备则搜寻为计算机。然后可将设备添加到受管设备列表，并运行硬件配置功能来配置 BMC 密码。本产品随后便可识别设备的 IPMI 功能。请注意，BMC 的 IP 地址不一定与操作系统的 IP 地址相同，因此可能无法直接将代理推到 BMC 的 IP 地址。可能需

要重新搜寻标准 IP 才能获得标准代理并下“推”到 BMC 的 IP。BMC IP 应该能够进行 IP 代理推。

启用 Intel* AMT（版本 1）的设备应该以 Intel AMT 用户名和密码进行配置，这样才能被识别和搜寻为 Intel AMT 设备。搜寻到设备后，可以运行硬件配置功能来配置 Intel AMT 设置并以小企业模式或安全企业模式部署设备。

要使设备搜寻自动化，可以安排搜寻操作定期执行。例如，可以按子网划分网络，每天晚上安排对不同的子网执行 ping 扫描。在所有搜寻中，都由核心服务器执行搜寻。

要搜寻和管理网络上的设备，请完成下列任务：

- 创建搜寻配置
- 计划并运行搜寻
- 查看搜寻到的设备
- 将搜寻到的设备移动到**我的设备**列表

## 在带有防火墙的设备上使用“不受管的设备搜寻”

注意，除非手动配置防火墙，否则不受管的设备搜寻通常无法发现使用防火墙的设备，如 Windows 防火墙。必须打开以下端口。要更改这些设置，请通过 Windows“控制面板”进入 Windows 防火墙。

**受管服务器：**

- 文件和打印机共享：TCP 139、445；UDP 137、138（无此设置，“推”无法进行）
- 软件分发：TCP 9595（无此设置，“推”无法进行）
- 高级 - ICMP：“允许传入的回显请求”（不启用此设置则搜寻不到）

**核心服务器：**

- 清单： 5007
- 远程控制： 9535

# 创建搜寻配置

使用**搜寻配置**选项卡可以创建新的搜寻配置，编辑和删除现有配置，以及安排搜寻配置的时间。每个搜寻配置都包括一个描述名称、要扫描的 IP 范围和搜寻类型。

创建配置之后，可使用**安排搜寻**对话框配置运行搜寻的时间。

1. 在左侧导航窗格中，单击**设备搜寻**。
2. 在**搜寻配置**选项卡中，单击**新建**按钮。
3. 填充下列所述字段。完成创建操作后，单击**添加**按钮，然后单击**确定**。

下面的文本介绍了**搜寻配置**对话框的各个部分。

- **配置名称：**键入该配置的名称。为配置取一个有意义的名称，以便您轻松记住此配置。配置名称最长可达 255 个字符，而且不应包含以下字符：″、+、#、& 或 %。任何这些字符之后的配置名称将无法显示。
- **标准网络扫描：**通过将 ICMP 数据包发送到指定范围内的 IP 地址，可以查找设备。这是最彻底的搜寻，但速度最慢。默认情况下，此选项使用 NetBIOS 收集设备的有关信息。

  网络扫描选项中包含一个 **IP 特征**选项，利用此选项，设备搜寻尝试通过 TCP 数据包响应来搜寻操作系统类型。“IP 特征”选项会或多或少地减慢搜寻速度。

  网络扫描选项中还包含一个**使用 SNMP** 选项，可用于配置使用 SNMP 进行扫描。单击**配置**以键入有关您的 SNMP 配置的信息。有关详细信息，请参阅“配置 SNMP 扫描”。
- **LANDesk CBA 搜寻**在设备中查找标准管理代理[以前在 Management Suite 中称作通用基本代理 (CBA)]。)标准管理代理允许核心服务器搜寻网络上的客户端并与之通信。此选项可用于搜寻安装了产品代理的设备。路由器阻塞了标准管理代理和 PDS2 之间的通信。为了跨多个子网运行标准 CBA 搜寻，必须配置路由器，以允许多个子网之间进行定向广播。

  CBA 搜寻选项还有一个 **LANDesk PDS2 搜寻**选项，利用该选项，设备搜寻将在设备上查找 LANDesk Ping 搜寻服务 (PDS2)。LANDesk Software 产品，如 LANDeskÂ® System Manager、Server Manager 和 LANDesk 客户端管理器使用 PDS2 代理。如果您网络上的设备已安装了这些产品，请选择此选项。CBA 搜寻对 Linux 机器不支持，但如果选择了 PDS2，则可搜寻到装有代理的 Linux 机器。
- **IPMI：**搜索已启动 IPMI 的服务器。IPMI 是由 Intel、* H-P、* NEC、* 和 Dell* 开发的一种规范，用来为可管理的硬件定义消息和系统界面。IPMI 具有监视和恢复功能，不管设备处于开机或关机状态、也不管操作系统处于何种状态，都可访问这些功能。请注意，如果底板管理控制器未进行配置，则无法响应产品用于搜寻 IPMI 的 ASF ping。也就是说，您不得不将其搜寻为普通计算机。当“推”客户端时，ServerConfig 将会扫描系统并检测到这是 IPMI 并配置 BMC。有关 IPMI 的概述，请参阅 IPMI 支持。
- **服务器机箱：**查找刀片式服务器机箱管理模块 (CMM)。服务器机箱中的刀片式服务器将作为普通服务器被检测。
- **Intel* AMT：**查找支持 Intel 活动管理技术的设备。
- **起始 IP：**输入您要扫描的地址范围的起始 IP 地址。
- **结束 IP：**输入您要扫描的地址范围的结束 IP 地址。
- **子网掩码：**输入您要扫描的 IP 地址范围的子网掩码。
- **添加：**在对话框底部的工作队列中添加 IP 地址范围。
- **清除：** 清除 IP 地址范围字段。
- **编辑：**在工作队列中选择 IP 地址范围，然后单击**编辑**。范围显示在工作队列上面的文本框中，您可以在其中编辑范围，并将新范围添加到工作队列中。
- **删除：**从工作队列中删除所选的 IP 地址范围。
- **全部删除：**从工作队列中删除全部 IP 地址范围。

**编辑或删除配置**

- 在**搜寻配置**选项卡上，单击需要的配置，然后单击**编辑**或**删除**。

## 配置 SNMP 扫描

网络扫描搜寻可以使用 SNMP。根据您的 SNMP 配置，您可能需要在搜寻配置中输入其它 SNMP 信息。单击 **SNMP** 选项旁的**配置**，打开 **SNMP 配置**对话框，该对话框的选项如下：

- **重试次数：**设备搜寻重试 SNMP 连接的次数。
- **等待响应的秒数：**设备搜寻应该等待的 SNMP 响应时间。
- **端口：**设备搜寻发送 SNMP 查询应使用的端口。
- **社团名称：**设备搜寻应该使用的 SNMP 社团名称。
- **配置 SNMP V3：**设备搜寻也支持 SNMP V3。单击此按钮以在 **SNMP V3 配置**对话框中配置 SNMP V3 选项。

**SNMP V3 配置**对话框有以下选项：

- **用户名：**设备搜寻用于与远程 SNMP 服务进行身份验证的用户名。
- **密码：**远程 SNMP 服务的密码。
- **身份验证类型：**SNMP 使用的身份验证类型。可以是 **MD5**、**SHA** 或**无**。
- 加密**类型：**SNMP 服务使用的加密方法。可以是 **DES**、**AES128** 或**无**。
- 加密**密码：**用于指定加密类别的密码。在选择保密性类别**无**时无此项。

# 计划并运行搜寻

使用**搜索配置**选项卡上的**计划**按钮，可显示**计划任务**对话框。当搜寻配置运行时，可使用此对话框进行计划。可以计划搜寻配置立即运行、在将来的某个时间运行、重复运行，或者只运行一次。

可从**搜寻任务**选项卡中重新计划或删除搜寻任务。计划搜寻之后，请参见**搜寻任务**选项卡获得有关搜寻状态的信息。还可以在**计划任务**工具中访问搜寻任务的状态。搜寻任务完成后，尚未存在于核心数据库中的新设备将添加到已搜寻到的设备类别中。

**计划任务**对话框包括以下这些选项。

- **在常见任务中显示：**让其他用户看到该任务。当其他用户编辑或运行任务时，该用户成为任务实例的所有者。
- **所有者：**任务所有者。
- **保持不计划：**（默认）保留任务列表中的任务，以后再计划。
- **立即开始：**尽快运行任务。开始任务可能需要一分钟时间。
- **在预定时间开始：**在指定的时间开始任务。单击此选项后，必须输入下列内容：
  - **日期：**要开始任务的日期。根据您所在位置的不同，日期顺序将采用日-月-年或月-日-年的方式。
  - **时间：**要启动任务的时间。
  - **重复间隔：**如果要重复执行任务，请选择频率（每天、每周或每月）。如果选择了每月和某个并非所有月都有的日期（例如，31 号），则任务将只按照包含此日期的月来运行。

### 计划搜寻的时间

1. 在左侧导航窗格中，单击**设备搜寻**。
2. 在**搜寻配置**选项卡上，选择需要的配置，然后单击**计划**。配置搜寻计划。完成后，单击**保存**。
3. 在**搜寻任务**选项卡中监控搜寻进度。
4. 完成搜寻后，请在**搜寻到的设备**的上窗格中查看搜寻结果。双击搜寻任务时，设备的数量和百分比均为零，这是因为这些数字依赖于目标设备，而搜寻任务没有目标。

**搜寻任务**选项卡显示搜寻作业的状态。其状态包括以下内容：

- 搜寻配置的名称。
- 任务状态，这些状态可以是“正在进行”、“全部完成”、“未完成”或“失败”。
- 运行上一次任务的时间。
- 任务运行的类型。

### 删除或重新计划搜寻

如果要想从列表中删除某个任务，无论该任务是否已经运行，都可以通过先单击该任务然后单击**删除**来将其删除。如果任务还未运行或该任务是一个重复执行的任务，应删除该任务以免将来运行。

还可以通过单击该任务然后单击**编辑**，选择**计划**并重置计划来在列表中重新计划要再次运行或在另一时间运行的搜寻任务。要立即重新运行任务，请选择任务然后单击**立即开始**。

### 查看搜寻任务状态

1. 在左侧导航窗格中，单击**搜寻的设备**。
2. 单击**搜寻任务**选项卡或单击该窗格工具栏中的**刷新**按钮。

# 查看搜寻到的设备

在**设备搜寻**顶部窗格中查看所有搜寻到的设备。此窗格中列出了所有已运行搜寻的结果。当运行一个新的搜寻时，可将任何找到的设备添加到此列表中。

当设备搜寻找到一个设备时，将尝试识别其设备类型，以便将该设备添加到以下类别之一：

- **机箱：**包含刀片式服务器机箱管理模块 (CMM)。
- **计算机：**包含计算机。在**操作系统名称**列中，Linux 系统可能标为 Unix 系统。
- **基础设施：**包含路由器和其他网络硬件。
- **Intel AMT：**包含支持 Intel*活动管理技术的设备。
- **IPMI：**包含启用 IPMI 的设备。
- **其他：**包含未标识的设备。
- **打印机：**包含打印机。

这些类别有助于组织**设备搜寻**列表，使您更容易找到需要的设备。单击任一列标题，即可按该列标题对设备列表进行排序。“设备搜寻”可能无法每次都正确地对设备分类。通过以下操作可以轻松地将标识有误的设备移动到正确的组：右击需要移动的设备，接着单击**移动**，再选择正确的类别，然后单击**确定。**

偶尔会两次列出核心服务器。原因是通过不同的搜寻机制（例如 CBA、IPMI、CMM、PDS1 和 PDS2）发现了同一台机器并且将该机器的信息添加到了数据库的对应机制中。

将代理部署到某个搜寻到的设备，且该设备已将清单扫描发送到核心服务器之后，则此搜寻到的设备将从搜寻到的设备列表中删除。

## 过滤设备列表

使用工具栏中的**过滤依据**字段查找符合指定搜索条件的设备。可以按节点名称、IP 地址、子网掩码、类别或操作系统名称进行过滤。使用过滤器时，根据过滤所依据的属性按字母顺序对设备进行排序。

**过滤设备列表**

1. 在左侧导航窗格中，单击**设备搜寻**。
2. 在**不受管理的设备**树中，单击需要过滤的组。
3. 在**过滤依据**中，单击您要作为过滤依据的属性。（如果**过滤依据**不可见，单击>>将其扩展。）
4. 在属性旁边的框中，输入您要作为过滤依据的文本。
5. 单击**查找**。

## 添加类别

您可以创建设备类别，对不受管的设备分类。如果将某个设备移到另一个类别，以后当设备搜寻检测到此设备时，它将在该组中显示。将已知的不使用 Web 控制台管理的设备移动到其所属组中，可以使您更轻松地在**计算机**组中看到新的设备。

如果删除包含设备的组，设备搜寻会将设备移到**其他**组。

**添加设备种类**

1. 在**设备搜寻**视图中，单击**添加类别**。
2. 在**类别名称**框中键入组名，然后单击**确定**。
3. 要删除已添加的类别，选择该类别，单击**删除类别**，然后单击**确定**以确认删除。

# 将搜寻到的设备移动到“我的设备”列表

搜寻到设备后，可将其移动到**我的设备**列表。在移动设备的过程中，设备的信息被添加到数据库。将信息添加到数据库后，即可部署代理配置，运行与该信息有关的查询和报告，并执行许多其他管理任务。

对于可以带外管理的设备（具有 IPMI、Intel AMT 或 DRAC 功能的设备），也可以选择不部署代理进行设备管理。如果选择这种管理，则设备信息将保存在数据库中，而且设备的 BMC 将配置为可以使用设备带外管理硬件所提供的管理功能。

**将搜寻到的设备移动到“我的设备”列表**

1. 在**设备搜寻**视图中，单击要移动到**我的设备**列表中的设备。您可以通过按 SHIFT+单击或 CTRL+单击来选择多个设备。
2. 单击**目标**按钮。选定的设备会列入**目标列表**选项卡。
3. 单击**管理**选项卡。
4. 选择**移动目标设备**。
5. 如果设备可以带外管理而且您不希望为其部署管理代理，请选择**无代理管理带外启用的设备**。
6. 单击**移动**。

设备将从不受管设备列表中删除，并出现在**我的设备**列表中。

如果选择带外管理选项，可以通过单击下方窗格中的**移动状态**选项卡来查看移动过程的状态。配置中的任何错误均会在此注明。要将启用 IPMI 的设备移动到**我的设备**列表中，必须先在 配置服务实用程序中提供正确的 BMC 凭证，这样核心服务器才能成功地向设备验证身份。

将机箱管理模块 (CMM) 移动到**我的设备**列表后，此模块将显示在**所有设备**列表中，并显示为**公共组**列表中的一个组。组详细信息显示了 CMM 和机箱中的可用凹槽列表，以及凹槽中的刀片服务器名称。还将刀片服务器作为单独的服务器进行检测和管理。

# 搜寻 Intel AMT 设备

System Manager 包含的选项可用于搜寻以 Intel* Active Management Technology (Intel* AMT) 1 版配置的设备。只有在访问了设备上的 Intel AMT 配置屏幕并将制造商的默认密码更改为安全密码后，才能将设备作为 Intel AMT 设备搜寻。（有关访问 Intel AMT 配置屏幕的信息，请参阅制造商文档。）如果您尚未执行此操作，则虽可搜寻到设备，但不会将之标识为 Intel AMT 设备，并且也无法查看到与您这样做时能查看到的相同清单一览表信息。

---

Intel AMT 2 版设备无法使用此过程搜寻。在 Intel AMT 配置屏幕上输入部署 ID 以及核心服务器的 IP 地址后，会自动搜寻该设备。有关使用 2 版的详细信息，请参阅 配置 Intel AMT 设备。

---

### 搜寻 Intel AMT 设备

1. 在左侧导航窗格中，单击**设备搜寻**。
2. 单击**新建**创建新配置，然后键入配置的名称。或者单击现有的配置，然后单击**编辑**修改配置。
3. 选中**搜寻 Intel AMT 设备**。
4. 输入起始和结束 IP 地址来扫描地址范围，然后输入子网掩码。
5. 单击**添加**，然后单击**确定**。
6. 选择配置并单击**计划**。设置计划选项，或单击**立即开始**，然后单击**保存**。
7. 要查看扫描的进度，请单击**搜寻任务**选项卡。

以 Intel AMT 配置的设备在标有 **Intel AMT** 的文件夹中显示。可以从此文件夹选择设备并将其移动至受管设备列表中。

要将设备添加至核心数据库以便对其进行管理，设备的用户名/密码必须与“配置服务”实用程序中的用户名/密码匹配，该实用程序允许 System Manager 向设备验证身份。当您将密码配置保存至“配置服务”实用程序时，它将信息存储在核心数据库中，因此 System Manager 就能够向 Intel AMT 设备验证身份。

如果您的 Intel AMT 设备具有不同的凭证，您将需要确保每个设备的凭证与“配置服务”实用程序中的设备凭证匹配，然后才能对其进行管理。

当搜寻到 Intel AMT 设备并将其移动到**我的设备**列表时，它将使用您以“配置服务”实用程序选择的模式自动部署。“小型企业”模式提供基本的管理，没有网络基础结构服务，是不安全的；而“企业”模式旨在用于大型企业，提供了基于诸如 DHCP 和 DNS 的网络服务以及 TLS 证书授权服务的安全性。

如果核心使用代理服务器，该代理服务器必须支持“简要身份验证”才能搜寻 Intel AMT 设备。

### 配置 Intel AMT 密码

1. 单击**开始|所有程序| LANDesk |配置服务**。单击 **Intel AMT 配置**选项卡。
2. 输入当前用户名和密码。这些用户名和密码必须与 Intel AMT 配置屏幕（可在计算机 BIOS 设置中访问）中配置的用户名和密码匹配，以便对 Intel AMT 设备进行管理。
3. 要更改用户名和密码，请完成**新 Intel AMT 密码**部分。
4. 当您要将设备添加到核心数据库中对其进行管理时，选择您要用于部署设备的模式（**小企业**或**企业**）。
5. 单击“确定”。此更改将在运行客户端配置时生效。

### 将搜寻到的 Intel AMT 设备移动到受管设备列表中

1. 单击未管理设备列表中的一个或多个设备名称。
2. 单击工具栏上的**目标**按钮。

3. 在下面的窗格上单击**管理**按钮，选择**移动目标设备**，然后单击**移动**。

   如果希望管理的所有设备都在此列表中，则可以选择这些设备，单击下窗格上的**管理**按钮，选择**移动选定设备**，然后单击**移动**。

此设备将从不受管设备列表中删除，并出现在**所有设备**列表中。请注意，当您将设备移动到**我的设备**列表时，Intel AMT 部署在另一个后台进程中运行。发生这样的情况时，您可以继续进行其它搜寻或管理任务。

有关管理 Intel AMT 设备的详细信息，请参阅 管理 Intel* AMT 设备和 Intel* AMT 支持。

# 设备代理安装和配置

## 代理安装和配置概览

为了使用控制台完全管理设备，必须在设备上安装管理代理。您可以选择安装默认代理配置（安装所有产品代理）或在设备上安装自定义的代理配置。System Manager 的安装并不在核心服务器上自动安装代理；您也必须将代理安装在核心服务器上，然后手动重新启动核心服务器。代理配置必须包括监视代理，以接收健全性警报。

可以通过下列一种方法来安装管理代理：

- 部署代理。在**我的设备**列表中选择目标设备，然后安排代理配置任务来远程地在设备上安装代理。
- 使用安装程序包安装代理。创建自解压设备安装程序包。在设备上本地运行此程序包来安装代理。必须以具有管理员权限的用户登录才能完成此操作。
- “拉”代理。映射到核心服务器的 ldlogon 共享目录（*//服务器名*/ldlogon），然后在带有可移动 USB 驱动器的设备上手动运行 SERVERCONFIG.EXE（请参见 使用安装程序包安装代理）。
-

有关代理安装和配置的另一种资源是*《用户指南》*中的 设备搜寻一章。

**注意：**在**代理配置**页中选择一个设备配置并单击**设置为默认**，可使该配置成为默认配置。仅 IPMI BMC 配置不能作为默认配置。不能删除默认配置。

对于 Windows 系统，以下端口设置需要手动配置防火墙，才能获得全部产品功能。要更改这些设置，请通过 Windows 的“控制面板”访问 Windows 防火墙。

**受管服务器：**

- 文件和打印机共享：TCP 139，445；UDP 137，138（无此设置，“推”无法进行）
- 软件分发：TCP 9595（无此设置，“推”无法进行）
- 高级：ICMP -“允许传入的回显请求”（不启用此设置则搜寻不到。）

**核心服务器：**

- 清单： 5007
- 远程控制： 9535

要执行此操作，请单击**开始**|**控制面板**|**安全**。

# 更新已有的代理

即使标准管理或远程控制代理尚未安装，您也可以将代理配置“推”至设备。有关配置凭证的信息，请参见*《用户指南》*中的 配置服务和凭证。

如果您已安装了代理程序包，安装过程中将删除旧的代理而替换为新的代理。要卸载一个代理，可以通过新建一个不包含要删除的代理的代理程序包来完成。

# 卸载代理

如果需要从服务器卸载代理，请遵循以下步骤。

**警告：**默认情况下，卸载代理后，Uninstallwinclient.exe 将重新启动设备，除非在命令行使用 /noreboot 开关。必须重新启动才能完成卸载。如果已开始重新启动，服务器将重新启动但不会发出通知，并且所有其他应用程序被强制退出。/noreboot 开关使服务器继续运行，不执行重新启动。

### 从服务器卸载代理

1. 以管理员身份登录服务器。
2. 将某个驱动器映射到核心服务器的 ldmain 共享目录下。
3. 打开命令提示窗口，转至 ldmain 文件夹的驱动器盘符，然后输入以下命令：

   ```
   uninstallwinclient.exe /noreboot
   ```

卸载程序将无提示运行，并移除所有代理。

您还可以选择**开始 > 运行 >*核心服务器名称*\ldmain\uninstallwinclient.exe /noreboot**。

### 从 Linux 服务器卸载代理

1. 将文件 linuxuninstall.tar.gz 复制到 Linux 设备上的临时目录。这可以在核心服务器的 ManagementSuite 共享文件夹中找到。

   Linux 设备可能尚未安装/配置 Samba，因此您将无法直接复制该文件；您可以从核心服务器 pscp，将其复制到 ldlogon 文件夹，也可以将其复制到可移动介质。
2. 从 shell 提示（在 Linux 机器上），使用 tar 和 x、z 和 f 选项解包该文件。

   ```
   tar -xzf linuxuninstall.tar.gz
   ```
3. 该文件解包后，在 shell 提示从当前目录运行 linuxuninstall 脚本：

   ```
   ./linuxuninstall.sh
   ```

# 配置代理

为了使用控制台完全管理设备，必须在设备上安装管理代理。System Manager 的安装并不在核心服务器上自动安装代理；您也必须将代理安装在核心服务器上，然后手动重新启动核心服务器。无论是使用某种默认代理配置还是在控制台中创建代理配置，在 Windows 或 Linux 设备上安装代理都有三种方法：

- 创建代理配置，在**我的设备**列表中选择目标设备，然后安排代理配置任务来远程地在设备上安装代理。
- 创建自解压安装程序包。在设备上本地运行此程序包来安装代理。必须以具有管理员权限的用户登录才能完成此操作。有关更多信息，请参见“使用安装程序包安装代理”。
- 从 Windows 设备上，映射到核心服务器的 ldlogon 共享目录 (*我的服务器*\ldlogon)，然后运行 SERVERCONFIG.EXE。

**创建代理配置**

1. 在左侧导航窗格中，单击**代理配置**。
2. 单击**新建**。
3. 在**配置名称**框中输入新建配置的名称。

   输入名称，该名称说明正在进行的配置。这可以是现有的配置名称，也可以是一个新名称。

4. 选择平台进行配置。
5. 选择配置的安装类型（用户已选或仅 IPMI BMC）。选择**配置**下的**仅 IPMI BMC**，以便在启用 IPMI 的设备上配置底板管理控制器 (BMC)（请参见下面第 9 步的注释）。

   仅 IPMI BMC 配置为带外访问配置底板管理控制器，执行完整清单扫描，然后自行删除。仅 IPMI BMC 配置不能作为默认配置。创建仅 IPMI BMC 配置时，请注意在下列步骤中描述的大部分编辑选项不可用。

6. 选择刚创建的配置并单击**编辑**。

   在选项卡中，某些选项呈灰色，因为对于您所选的配置来说，它们是不可配置的。
7. 在**代理**选项卡中选择要部署的代理。

   - **All:**在选定的设备上安装所有代理。
   - **标准管理代理：**构成了设备和核心服务器之间通信的基础。这是必需代理（仅 BMC 配置除外）。此代理的大多数过程是按需的。
   - **软件更新：**安装软件更新扫描器。安装了此代理后，即可配置扫描器的运行方式。这不是按需代理。
   - **监视：**在选定的服务器上安装监视代理。监视代理可进行多种类型的监视，包括直接 ASIC 监视、带内 IPMI、带外 IPMI 和 CIM。这不是按需代理。

- **Active System Console：**安装代理能让您通过界面或菜单从 System Manager 访问 Active System Console。仅在带有 Intel 主板的设备上，才支持此代理。

8. 在**配置**系统类型框中，选择类型。如果该项变暗，表明您已经选择了类型。

9. 选择**重新启动**选项。

   手动重新启动说明在安装后设备不会重新启动。完成代理配置后不需要重新启动设备。您必须手动重新启动该设备。

   重新启动（如有必要）将导致代理更新在更新文件被锁定时重新启动。

10. 在清单选项卡中，设置“清单扫描器”配置设置。说明如下。
    - **自动更新：**在软件扫描期间远程设备从核心服务器中读取软件列表。如果设置了此选项，每台设备必须有一个驱动器映射到核心服务器上的 LDLOGON 目录，这样，这些设备就可以访问软件列表。对软件列表的更改将立即传递到设备中。
    - **手动更新：**软件扫描期间用于排除标题的软件列表将加载到每个远程设备。每次从控制台更改软件列表后，都必须将它重新手动发送给远程设备。
    - **清单扫描器设置：**清单运行的时间。您可以选择频率，也可以指定始终在启动时运行。从受管服务器可手动运行扫描器；从开始|程序|LANDesk Management |清单扫描也可启动扫描器。在 Linux 中，应该以根用户身份登录，然后从命令行运行：`/usr/LANDesk/ldms/ldiscan -ntt`

      - **始终在启动时运行：**在设备启动时运行清单扫描器。如果要创建 HP-UX 配置，则该按钮会因为将 HP-UX 扫描器设置为 cron 作业而变暗，该作业将按每天、每周或每月的间隔来运行。无法修改此操作。
      - **开始时间：**指定扫描器需在多少个小时内运行一次。如果一台设备在您指定的时间范围内登录，则清单扫描会自动运行。如果设备已经登录，一旦到了开始时间，清单扫描会自动运行。如果您想要错开对设备的清单扫描使它们不同时发送扫描，此选项非常有用。
      - **重复间隔：**输入表示增量的数字（如 1、2 或 3），以及计量单位（分钟、小时或天）。
      - **限制：**限制清单扫描器运行的可用天数和时间。单击**一天中的时间**、**一周中的天数**或**一个月中的天数**，然后输入包含的参数。例如，给**一个月中的天数**输入 10，给**一天中的时间**输入 1:00 AM 和 3:00 AM，让清单扫描器在每月第 10 天的 1:00 AM 至 3:00 AM 之间运行。

    - 在**软件更新**选项卡中，设置希望软件更新扫描器运行的日期和时间。扫描器将自动运行，事先不要求计划的任务。 **始终在启动时运行：**在设备启动时运行软件更新扫描器。

- **开始时间：**指定扫描器需在多少个小时内运行一次。如果一台设备在您指定的时间范围内登录，则软件更新扫描会自动运行。如果设备已经登录，一旦到了开始时间，软件更新扫描会自动运行。如果您想要错开对设备的扫描使它们不同时发送扫描，此选项非常有用。
- **重复间隔：**输入表示增量的数字（如 1、2 或 3），以及计量单位（分钟、小时或天）。
- **限制：**限制软件更新扫描器运行的可用天数和时间。单击**一天中的时间**、**一周中的天数**或**一个月中的天数**，然后输入包含的参数。例如，给**一个月中的天数**输入 10，给**一天中的时间**输入 1:00 AM 和 3:00 AM，让清单扫描器在每月第 10 天的 1:00 AM 至 3:00 AM 之间运行。

12. 在**规则集**选项卡中，选择要在配置中包括的所有监视和/或警报规则集。这些规则集存储在 ldlogon/alertrules 文件夹中。在**监视**或**警报**中可创建新的规则集。要在下拉列表中显示新创建的规则集，必须为自定义规则集生成 XML。
13. 单击**保存更改**将信息保存到数据库。单击**另存为文件**可将配置另存为一个可分发的程序包。

**注意：**在**代理配置**页中选择一个代理配置并单击**设置为默认**，可使该配置成为默认配置。不能删除默认配置。

**计划代理配置任务**

1. 在左侧导航窗格中，单击**代理配置**。
2. 单击代理配置，然后单击**计划任务**。
3. 编辑 目标设备和任务计划列表。
4. 单击**保存**。

单击**计划任务**后，即创建了一个任务（它没有目标设备且未计划）。如果取消该代理配置任务但不进行保存，请注意它仍是已创建任务并且显示在**任务**列表中，状态为“未计划”。您可以从**我的任务**列表中将其删除。

代理配置任务完成后，必须重新启动设备，才能在控制台中查看有关设备的详细信息（请参见 查看服务器信息控制台）。在核心服务器以及受管设备上安装代理时，需要执行上述的重新启动操作。代理配置过程允许选择何时重新启动，以便重新启动不会影响服务器的使用。

# 将代理部署到受管的设备

搜寻到设备后，您可以将代理部署到这些设备中。仅能将代理部署到受支持的 Windows、Linux 和 HP-UX 设备。在 Windows 设备上部署代理须具有管理员权限，在 Linux 和 HP-UX 设备上则须具有根权限。

您可以按以下方法之一将代理部署到不受管的设备：

- 使用搜寻作业和为处理搜寻作业的调度程序服务配置的域管理帐户进行基于“推”的部署。此域管理帐户授予调度程序服务安装服务器代理所需的权限。这适用于 Windows NT 系列服务器。

- 使用标准管理代理进行基于“推”的部署。如果服务器已安装标准管理代理（此代理用于许多 LANDesk 软件产品），则您可以在不需要域管理帐户的情况下将代理部署到这些服务器。

向搜寻到的设备进行部署时，请使用**不受管的设备**树的**过滤依据**选项。可依据 IP 地址进行过滤来找到设备。

对于 Windows 系统，以下端口设置需要手动配置防火墙，才能获得全部产品功能。要更改这些设置，请通过 Windows“控制面板”进入 Windows 防火墙。

**受管服务器：**

- 文件和打印机共享：TCP 139、445；UDP 137、138（无此设置，“推”无法进行）
- 软件分发：TCP 9594、9595（无此设置，“推”无法进行）
- 高级 - ICMP：“允许传入的回显请求”（不启用此设置则搜寻不到。）

**核心服务器：**

- 清单： 5007
- 远程控制： 9535

## 配置设备验证凭证

安装了标准管理代理的不受管设备不需要验证凭证就可以进行代理部署。要在没有安装标准管理代理的 Windows 操作系统服务器上安装代理，则必须指定控制台设备上的调度程序服务获取所需权限所使用的凭证。

要在不受管的设备上安装设备代理，调度程序服务需要能够使用管理帐户连接至设备。调度程序服务使用的默认帐户是 LocalSystem。LocalSystem 凭证一般用于域外设备。

如果设备在域中，必须指定域管理员帐户。如果您正在配置多个域中的不受管设备，必须每次在一个域中配置这些设备，因为调度程序服务使用一组凭证进行验证，而每个域都需要不同的域管理员帐户。

核心服务器包括“配置服务”实用程序，您可以使用该程序来自定义清单选项。此实用程序只能在核心服务器上运行。

**配置调度程序登录凭证**

1. 要启动“配置服务”实用程序，请在核心服务器上单击**开始|程序文件| LANDesk |配置服务**。
2. 单击**调度程序**选项卡。
3. 单击**更改登录**按钮。
4. 在客户端输入服务要使用的凭证，通常是输入域管理员帐户。

# 安装代理

在控制台中创建代理配置后，需将其安装到设备中。System Manager 的安装并不在核心服务器上自动安装代理；您也必须将代理安装在核心服务器上，然后手动重新启动核心服务器。

客户端代理程序包是一个自解压的可执行程序文件。默认情况下，它们存储在核心服务器的 \Program Files\LANDesk\ManagementSuite\ldlogon 文件夹中。运行该可执行程序后，并不需要与用户进行交互，而是以无提示方式在后台安装客户端代理。在目标设备上并非必须有浏览器才能成功安装代理。

## 安装代理

通过创建新的客户端配置并从控制台分发配置，可以更新代理，也可将代理直接安装到非受管的设备。

安装了一个客户端代理程序包后，再安装其他客户端代理程序包时，会删除所有代理而安装明确选定的代理。要卸载一个代理，可以通过新建一个不包含要删除的代理的客户端代理程序包来完成。

## 卸载代理

如果需要从设备中卸载代理，请参见“代理安装和配置概览”。

# 用安装程序包安装代理

安装代理的方法之一为使用自解压设备代理程序包。这允许您将文件复制到一张 CD 上或者 USB 驱动器上以手动安装代理。可以通过单击**配置**对话框底部的**另存为文件**创建这些程序包。

1. 单击**代理配置**，然后双击一个配置名称。
2. 在**代理配置**对话框中，单击**另存为文件**，然后单击**关闭**。

单击**另存为文件**，创建一个文件名与指定的配置名称匹配的自解压可执行程序包。在核心服务器的 \Program Files\LANDesk\ManagementSuite\ldlogon\ConfigPackages 文件夹中创建程序包可能需要几分钟时间。

运行该可执行程序以安装代理（不需要与用户进行交互）。必须以管理员的身份登录。

---

如果用户无法使用管理员权限登录以安装程序包，您可以通过电子邮件、Web 下载、登录脚本或从共享部署程序包。

---

# 拉代理

本节包含有关从命令行部署代理的详细信息。可使用 SERVERCONFIG.EXE 命令行参数来控制在设备上安装哪些组件。可以以独立模式启动 SERVERCONFIG.EXE。该程序位于 *http:\\coreserver\LDLogon* 共享目录中，可从任何 Windows 服务器读取该目录。

SERVERCONFIG.EXE 使用 SERVERCONFIG.INI 来配置设备。

## 了解 SERVERCONFIG.EXE

SERVERCONFIG.EXE 使用以下过程来配置 Windows NT 系列服务器以进行管理：

1. 使用 SERVERCONFIG 确定计算机先前是否已配置管理代理。如果已配置，则 SERVERCONFIG 将删除所有组件并重新安装选定的组件。
2. SERVERCONFIG 将加载相应的初始化文件 (SERVERCONFIG.INI) 并执行其中的指令。

SERVERCONFIG.EXE 可以使用以下命令行参数：

| 参数 | 说明 |
|---|---|
| /I | 要包含的组件（包括引号）：<br><br>"Common Base Agent"<br><br>"Inventory Scanner"<br><br>"Alerting"<br><br>"Vulnerability Scanner"<br><br>"Server Monitor"<br><br>可在同一命令行上组合这些组件。例如：<br><br>`SERVERCONFIG.EXE /I="Alerting" /I="Vulnerability Scanner"` |
| /L 或 /Log= | CFG_YES 和 CFG_NO 日志文件的路径。该日志文件记录已配置和未配置的服务器 |
| /LOGON | 执行带 [LOGON] 前缀的命令 |
| /N 或 /NOUI | 不显示用户界面 |

| 参数 | 说明 |
| --- | --- |
| /NOREBOOT | 完成后不重新启动服务器（默认） |
| /REBOOT | 运行后强制重新启动 |
| /X= | 要排除的组件。例如：<br><br>`SERVERCONFIG.EXE /X=SD` |
| /CONFIG=<br><br>/[CONFIG]= | 指定要使用的服务器配置文件替代默认的 SERVERCONFIG.INI 文件。<br><br>例如，如果已创建名为 NTTEST.INI 的配置文件，请使用以下语法：<br><br>`SERVERCONFIG.EXE /CONFIG=TEST.INI`<br><br>自定义的 .INI 文件应和 SERVERCONFIG.EXE 位于同一个目录中，另外，请注意：/config 参数使用没有 NT 前缀的文件名。 |
| /? 或 /H | 显示帮助菜单 |

## 创建代理配置

使用**代理配置**可创建和更新服务器代理配置（例如安装了或管理着哪些代理）。可以根据各组的具体需要创建不同的配置。例如，可为 Web 服务器创建一个配置，为应用程序服务器创建另一个配置。

要将配置“推”到服务器，需要执行以下操作：

- **创建代理配置**：为服务器设置特定的配置。
- **计划代理配置**：将配置“推”到服务器，或从服务器“推”出配置，然后从核心服务器的 LDLogon 共享目录中运行 SERVERCONFIG.EXE。

### 创建代理配置

1. 在控制台中，单击**代理配置**。
2. 单击**新建**工具栏按钮。
3. 输入**配置名称**并选择操作系统，然后单击**确定**。
4. 单击新的配置名称，然后单击**编辑**。
5. 选择要部署的代理。
6. 使用对话框顶部的选项卡导航至与所选组件相关的选项。必要时，可自定义选定的选项。
7. 单击**保存更改**，然后关闭对话框。
8. 如果要使配置成为默认配置，请单击**设置为默认**。

# 拉 Linux 代理配置

**拉 Linux 代理配置**

1. 在您的 Linux 设备上创建临时目录（例如 /tmp/ldcfg），将以下文件复制到目录中：
    1. LDLOGON\unix\linux 目录中的所有文件。
    2. 将以该配置命名的 shell 脚本（<*配置名称*>.sh）复制到临时目录中。
    3. 将以该配置命名的 *.0 文件复制到临时目录中。* 为 8 个字符（0-9、a-f）。
    4. 将 <*配置名称*>.ini 文件中列出的所有文件复制到临时目录中。要找到这些文件，在 .INI 文件中搜索 "FILE*xx*"，其中，*xx* 是数字。查找的大多数条目将在第 1 步复制到客户端，但是您要查找必须复制的 .XML 文件。文件名应该保持不变，但有以下例外：
        - alertrules\<*任何文本*>.ruleset.xml 应该被重命名为 internal.ruleset.xml
        - monitorrules\<*任何文本*>.ruleset.monitor.xml 应该被重命名为 masterconfig.ruleset.monitor.xml
2. 如果设备具有 IPMI 和一个 BMC（安装中包括监视程序），则在命令行中键入下列内容：

    ```
    export BMCPW="(bmc 密码)"
    ```

3. 以根用户身份运行，执行配置的 shell 脚本。例如，如果将脚本命名为“pull”，则可以使用下面的完整路径：

    ```
    /tmp/ldcfg/pull.sh
    ```

4. 删除临时目录及其所有内容。

注意：应注意到如果您将某代理推或拉至一台 Linux 设备，然后运行

```
./linuxuninstall.sh -f ALL
```

要将其清除，然后再次执行推或拉操作，则带该 GUID 的文件是此操作完成后设备上留下的唯一文件。

-f 选项会删除产品所拥有的所有目录。有关详细信息，请参阅 Linux 卸载文档。

# 创建独立的代理配置程序包

通常，可使用代理配置实用程序 SERVERCONFIG.EXE 配置受管设备上的代理。若有必要，可使用**代理配置**窗口创建自解压的单个可执行文件，该文件可在其运行的服务器上安装代理配置。如果要从光盘或可移动 USB 驱动器安装代理，则此方法很有帮助。

## 将代理配置“推”到设备

**推代理配置**

1. 在控制台中，选择要部署代理的设备，然后单击**目标**。
2. 在左侧导航窗格中，单击**代理配置**。
3. 右键单击要“推”出的代理配置，然后单击**计划任务。**
4. 单击**计划任务属性**对话框中的**目标设备**，然后单击**添加目标列表**。
5. 单击**计划任务**。
6. 指定部署代理的时间，然后单击**保存**。

# 安装 Linux 服务器代理

您可以远程地在 Linux 服务器上部署和安装 Linux 代理和 RPM。必须正确配置您的 Linux 服务器来完成此操作。要在 Linux 服务器中安装代理，必须具有根权限。

默认 Linux 安装（Red Hat 3 和 4 以及 SUSE）包括 Linux 标准管理代理所需的 RPM。如果在**代理配置**中选择监视代理，则需要额外的 RPM (sysstat)。有关该产品所需要的 RPM 完整列表，请参见*《System Manager 部署指南》*。

对于初始的 Linux 代理配置，核心服务器使用 SSH 连接与目标 Linux 服务器建立连接。您必须具有一个带用户名/密码验证的有效 SSH 连接。本产品不支持公钥/私钥验证。核心服务器和 Linux 服务器之间的任何防火墙都必须预留 SSH 端口。考虑测试核心服务器与第三方 SSH 应用程序之间的 SSH 连接。

Linux 代理安装程序包包含一个 shell 脚本、代理 tarball、.INI 代理配置和代理验证证书。这些文件存储在核心服务器的 LDLogon 共享目录下。shell 脚本从 tarball 中解压缩文件、安装 RPM 并配置服务器加载代理，以您在代理配置中指定的时间间隔定期地运行清单扫描器。文件位于 /usr/landesk 下。

还必须在核心服务器上配置调度程序服务，以便在 Linux 服务器上使用 SSH 验证凭证（用户名/密码）。调度程序服务使用这些凭证在您的服务器上安装代理。使用 配置服务实用程序输入调度程序服务作为备用凭证使用的 SSH 凭证。系统会提示您重新启动调度程序服务。如果系统没有提示您重新启动，请在**调度程序**选项卡上单击**停止**，然后单击**启动**重新启动服务。此操作将激活您所做的更改。

## 部署 Linux 代理

配置您的 Linux 服务器并将 Linux 凭证添加至核心服务器后，必须将服务器添加至**我的设备**列表，这样才能部署 Linux 代理。向服务器部署代理前，您必须将服务器添加至**我的设备**列表。使用**设备搜寻**搜寻您的 Linux 服务器来完成此操作。

### 搜寻 Linux 服务器

1. 在**设备搜寻**中，为每台 Linux 服务器都创建一个搜寻作业。使用标准网络扫描并输入起始和结束 IP 范围内的 Linux 服务器的 IP 地址。如果有许多 Linux 服务器，请输入一个 IP 地址范围。添加搜索 IP 范围后，请单击**确定**。
2. 安排刚刚创建的搜寻任务，方法是单击任务，然后单击**计划**。任务完成后，验证搜寻过程是否已找到要管理的 Linux 服务器。
3. 在**设备搜寻**中，选择希望管理的服务器，然后单击**目标**，将所选设备添加到目标列表中。单击窗口下半部分中的**管理**选项卡。单击**移动选定的设备**并单击**移动**。此操作将服务器添加至**我的设备**列表，这样就可以部署这些服务器。

### 创建 Linux 代理配置

1. 在**代理配置**中，单击**新建**。
2. 输入配置名称，单击 **HP-UX** 或 **Linux Server Edition**，选择安装类型（服务器或台式机），然后单击**确定**。
3. 选择刚创建的配置并单击**编辑**。
4. 选择需要的代理。
5. 在**清单**选项卡中，选择选项和需要的扫描器频率时间间隔。安装脚本将添加一个 cron 作业，此作业以您选择的时间间隔运行扫描器。
6. 在**规则集**选项卡中，选择要在配置中包括的所有监视和/或警报规则集。这些规则集存储在 ldlogon/alertrules 文件夹中。
7. 单击**保存更改**。

要部署代理配置，在**代理配置**中选择该配置，然后单击**计划任务**。配置任务并在**配置任务**中监视任务进度。

**注意：**在清单扫描器完成其安装后的第一次扫描之前，您不会收到有关 Linux 设备的任何健全性信息。

### 拉 Linux 代理配置

1. 在您的 Linux 设备上创建临时目录（例如 /tmp/ldcfg），并将以下文件复制到该临时目录中：
   - LDLOGON\unix\linux 目录中的所有文件。
   - 以该配置命名的 shell 脚本 (<*配置名称*>.sh)。
   - 以该配置命名的 *.0 文件。* 为 8 个字符（0-9、a-f）。
   - <*配置名称*>.ini 文件中列出的所有文件。要找到这些文件，在 .INI 文件中搜索“FILE*xx*”，其中 *xx* 是数字。查找的大多数条目将在第 1 步复制到客户端，但是您要查找必须复制的 .XML 文件。文件名应该保持不变，但有以下例外：
     - alertrules\<*任何文本*>.ruleset.xml 应该被重命名为 internal.ruleset.xml
     - monitorrules\<*任何文本*>.ruleset.monitor.xml 应该被重命名为 masterconfig.ruleset.monitor.xml

2. 如果设备拥有 IPMI 和 BMC（安装中包括监视程序），则在命令行中键入下列内容：

   ```
   export BMCPW="(bmc 密码)"
   ```

3. 以根用户身份运行，使用下面的完整路径执行配置的 shell 脚本：

   ```
   /tmp/ldcfg/lsminstall.sh
   ```

4. 删除临时目录及其所有内容。

**注意：**应注意到如果您将某代理推或拉至一台 Linux 设备上，然后运行

```
./linuxuninstall.sh -f ALL
```

将其清除之后再次执行推或拉操作，则带该 GUID 的文件是此操作完成后设备上留下的唯一文件。

`-f` 选项会删除产品所拥有的所有目录。有关其他信息，请参阅 Linux 卸载文档。

# 清单扫描器命令行参数

清单扫描器 ldiscan 具有多个命令行参数，用于指定扫描器的运行方式。有关每个参数的详细说明，请参阅“ldiscan -h”或“man ldiscan”。每个选项之前均可加上 "-" 或 "/"。

| 参数 | 说明 |
|---|---|
| -d=Dir | 在 Dir 目录（而非根目录）下启动软件扫描。默认情况下，在根目录下启动扫描。 |
| -f | 强制运行软件扫描。如果没有指定 -f，则扫描器会以在控制台的**配置|服务|清单|扫描器设置**中指定的日期间隔（默认为每天）执行软件扫描。 |
| -f- | 禁用软件扫描。 |
| -i=ConfName | 指定配置文件名。默认值为 /etc/ldappl.conf。 |
| -ntt=address:port | 核心服务器的主机名或 IP 地址。端口是可选项。 |
| -o=File | 将清单信息写入指定的输出文件。 |
| -s=Server | 指定核心服务器。此命令是可选的，仅用来实现向后兼容。 |
| -stdout | 将清单信息写入标准输出中。 |
| -v | 在扫描期间启用详细状态消息。 |
| -h 或 -? | 显示帮助屏幕。 |

## 示例

要将数据输出到文本文件，请键入：

```
ldiscan -o=data.out -v
```

要将数据发送到核心服务器，请键入：

```
ldiscan -ntt=ServerIPName -v
```

## Linux 清单扫描器文件

| 文件 | 说明 |
| --- | --- |
| ldiscan | 运行时带有命令行参数的可执行文件，指示要采取的操作。所有运行扫描器的用户均需要足够的权限才能执行该文件。<br><br>此文件的版本将根据上述支持的每个平台而改变。 |
| /etc/ldiscan.conf | 该文件始终位于 /etc 下，其中包含以下信息：<br><br>• 清单分配的唯一 ID<br>• 上次执行硬件扫描的时间<br>• 上次执行软件扫描的时间<br><br>所有运行扫描器的用户均需要该文件的读和写属性。<br>/etc/ldiscan.conf 中的唯一 ID 是第一次运行清单扫描器时分配给计算机的唯一编号。该号码可用来标识这台计算机。一旦更改了该号码，核心服务器会将其视为不同的计算机，这样就会导致数据库中出现重复条目。<br><br>**警告：**不要在创建唯一 ID 号后更改该 ID 号或删除 ldiscan.conf 文件。 |
| /etc/ldappl.conf | 在此文件中，您可以自定义运行软件扫描时，清单扫描器将报告的可执行文件的列表。该文件中包含一些示例，您需要为自己使用的软件包添加条目。搜索条件的基本要素为文件名和文件大小。虽然该文件通常位于 /etc 下，但扫描器可以通过 -i= 命令行参数来使用替代文件。 |
| ldiscan.8 | ldiscan 的手册页。 |

# 控制台集成

在将 Linux 计算机扫描到核心数据库后，可以执行以下操作：

- 查询由 Linux 清单扫描器返回给核心数据库的任何属性。
- 使用报告功能生成报告，报告中包含 Linux 扫描器收集的信息。例如，在操作系统一览表报告中，Linux 将显示为操作系统类型。
- 查看 Linux 计算机的清单信息。

**查询“系统正常运行时间”按字母顺序排序，会返回未预期的结果**
如果要执行查询来确定有多少台计算机的运行时间超过了一定的天数（如 10 天），请查询“系统启动”，而不是“系统正常运行时间”。查询“系统正常运行时间”可能会返回意外的结果，因为系统正常运行时间只是一个格式为“x 天，y 小时，z 分钟，j 秒”的字符串。排序依据是字母顺序，而不是时间间隔。

**控制台中不显示 ldappl.conf 中引用的配置文件的路径**
ldappl.conf 文件中的 ConfFile 条目必须包含路径。

# 设备监控

## 关于监视

System Manager 提供了若干种监视设备健全性状态的方法。监视功能从各种来源收集数据，帮助跟踪有关您的设备的多项数据，例如：

- 使用级别
- 操作系统事件
- 进程和服务
- 性能历史记录
- 硬件传感器（风扇、电压、温度等）

本章包括有关监视受管设备的不同功能的信息：

- 在设备上 安装监视代理，创建可部署到设备的监视规则集
- 在设备上设置性能计数器，监视性能数据
- 当发生更改时，通过警报 监视配置更改
- 定期 ping 设备，以便使用**设备监视器**功能 监视连接情况

警报是使用监视代理启动警报操作（如电子邮件或寻呼消息）、重新启动或关闭设备、或将信息添加到警报日志的相关功能。您可以从可被监视的任何设备事件生成警报。有关详细信息，请参阅“使用警报”。

**注意：**

- 与监视代理建立的通信都是以 GET、POST 或 XML 请求的形式使用 TCP/IP 通过 HTTP 进行的。对请求的响应在 XML 或 HTML 表文档中。
- 要运行并存储有关设备健全性状态的查询 (Computer.Health.State)，应注意数据库中的状态按编号显示。与以下状态相对应的数字：4=严重，3=警告，2=正常，1=信息，或 0=未知。
- 硬件监视有赖于安装在设备上的硬件功能，还有赖于硬件的正确配置。例如，如果在某一设备上安装了具有 S.M.A.R.T. 监视功能的硬盘驱动器，但是此设备的 BIOS 设置中未启用 S.M.A.R.T. 检测，或者此设备的 BIOS 不支持 S.M.A.R.T. 驱动器，则无法使用监视数据。
- 如果来自某台机器的报告似乎已停止，则您可以使用 LDCLIENT 文件夹中的 restartmon.exe 来重新启动收集器和所有监控提供程序。该实用程序适用于已安装了报告但报告已停止的机器。使用该实用程序可重新启动收集器和提供程序而无需重新启动设备。

## 将监视代理部署到设备

设备上安装了监视代理时，System Manager 将提供设备健全性的即时概览。监视代理是可在受管设备上安装的六个代理中的一个。它定期检查设备的硬件和配置，并反映设备的健全性状态的任何

变化。此信息由**我的设备**列表中的状态图标显示，详细信息显示在日志条目（在设备的**系统信息**一览表中显示）和图形（在设备的**监视**一览表页面中显示）中。

例如，磁盘驱动器占满的被监视设备可以在磁盘填满程度达到 90% 时显示警告状态图标，当磁盘填满程度达到 95% 时更改为严重状态图标。如果设备的警报规则集包括驱动器空间警报的规则，您还可以接收同一个磁盘驱动器状态的警报。

可将默认监视规则集部署到设备。或者，如果您愿意，可以创建只包括您关心的健全性项的自定义规则集。

## 创建监视规则集

您可以通过创建监视规则集（定义在设备上检查哪些监视代理）选择对设备上的哪些内容进行监视。您可以将规则集部署到一个设备或一组目标设备。例如，您可以为专用于存储的服务器定义一个规则集，而对 Web 服务器使用另一个规则集。

默认监视规则集包括 16 项。创建规则集时，可以打开或关闭这些项中的任何一个，指定检查这些项的频率，为某些项设置性能阈值。还可以选择设备上运行的要监视的服务。

创建和部署警报规则集的全部过程如下：

1. 选择打算部署规则集的目标设备，然后单击**目标**将其添加到**目标设备**列表。
2. 创建和编辑监视规则集。请注意，必须选中每个要在规则集中监视的事件的复选框以打开监视功能。不默认监视所有的事件.某些事件（如服务）还需选中要监视的每个服务。（请参见下面的详细步骤。）
3. 将规则集部署到目标设备。如果需要，可以在部署规则集前确定其他目标设备。（请参见下面的详细步骤。）

**创建监视规则集**

1. 在左侧导航窗格中，单击**监视**。
2. 单击**新建**，键入配置的名称和说明，单击**确定**。
3. 从左列选择配置。
4. 在项列表中，单击要更改的项，然后单击**编辑**。
5. 要关闭项的监视，请取消选中复选框，然后单击**更新**。
6. 要更改监视某项的频率，请选择**秒**或**分钟**，在文本框中指定一个数字。
7. 如果需要，设置警告和严重状态的阈值百分比。
8. 对于**服务**监视，从下拉列表中选择操作系统。选择要监视的一个或多个服务（使用 CTRL + 单击可多选），单击 >> 将服务添加到右侧的列表。
9. 对于您要修改的每项，单击**更新**，将更改应用于配置。如果修改项后决定不更改，则单击**恢复**以恢复原设置。

在核心服务器上的监视配置中编辑服务时，**可用服务**列表将显示清单数据库中的已知服务。只有 LANDesk 代理已部署到一个或多个设备且向核心服务器返回一个清单扫描后才能在**可用服务**列表框中显示服务。例如，要从列表选择 Linux 服务，则必须首先将一个代理部署到 Linux 设备。

**部署监视规则集**

1. 在左侧导航窗格中，单击**我的设备**，然后单击**所有设备**组。
2. 选择要对其部署规则集的设备，然后单击**目标**将设备放置在**目标设备**列表中。
3. 在左侧导航窗格中，单击**监视**，然后单击**部署规则集**选项卡。
4. 在**监视规则集**框中，选择要部署的规则集。
5. 单击链接查看**目标设备**列表。要从该列表中删除设备，请右键单击该设备，然后单击**删除**。（要添加设备，必须将它们添加到第 2 步中说明的目标列表。）
6. 单击**部署**，将所选规则集部署到目标设备。

作为部署过程的一部分，将创建一个 XML 页面，其中会列出部署的规则集和在其上部署规则集的设备。此报告将保存在核心服务器的 LDLOGON 目录中，并使用数据库所分配的序列号来命名。如果您希望在部署规则集过程以外查看此 XML 页面，请单击**生成 XML** 按钮，然后单击该链接即可查看 XML 文件。生成 XML 规则集还可以在 **代理配置**设置的可用规则集列表中显示该规则集。

## 关闭 ModemView 服务

ModemView 服务是监视调制解调器呼叫（传入和传出）的服务/驱动程序，如果发现呼叫，则并生成警报。此服务使用约 10 Mb 的内存，因为它使用 MFC。您可能不希望它运行，尤其是在设备没有调制解调器的情况下。

**关闭 ModemView 服务**

1. 在设备上（直接或通过远程控制）单击**开始** > **控制面板** > **管理工具** > **服务**。
2. 双击 **LANDesk Message Handler Service**。
3. 在**启动类型**下，选择**手动**，然后单击**确定**。

您还可以在**服务状态**下单击**停止**。

# 监视性能

使用**监视**页面，您可以监视各种系统对象的性能。可以监视特定的硬件组件，如驱动器、处理器和内存，还可以监视操作系统组件，如进程或系统 Web 服务器传输的字节 / 秒。**监视**页面包括显示计数器实时或历史数据的图形。

为了监视性能计数器，必须先选择计数器，并将其添加到受监视的计数器列表中。添加计数器后，还要指定轮询条目的频率，并设置性能阈值和生成警报前允许的突破阈值次数。有关选择计数器的详细信息，请参阅“设置性能计数器”。

**查看受监视计数器的性能图形**

1. 在**我的设备**视图中，双击要配置的设备。在另一浏览器窗口中将打开服务器信息控制台。
2. 在左侧导航窗格中，单击**监视**。
3. 如果需要，请单击**活动性能计数器**选项卡。

4. 在**计数器**下拉列表中，选择要查看其性能图形的计数器。
5. 选择**查看实时数据**以显示实时性能的图形。

   或者

   选择**查看历史记录数据**显示选定计数器时指定的（保存历史记录）时期的性能图形。

在性能图形中，水平轴表示已经过的时间。垂直轴代表测量的单位，如字节/秒（例如，在监控文件传输时）、百分比（监控 CPU 使用率百分比时）或可用字节（监控硬盘驱动器空间时）。行高不是固定单位。行高根据数据中的极限值而变化；对于某一计数器，垂直轴可能代表 1 至 100，而对于另一计数器，垂直轴可能代表 1 至 500,000。当数据的变化范围较大时，微小的变化将显示为一条直线。

**注意：**

- 选择其他计数器时图形将刷新，并重置测量单位。
- 单击**刷新**  清除图形并重新打开图形。
- 如果收到列表中的计数器生成的警报，请右键单击该计数器，然后单击**确认**，清除警报。

**停止监视性能计数器**

1. 在**我的设备**视图中，双击要配置的设备。在另一浏览器窗口中将打开服务器信息控制台。
2. 在左侧导航窗格中，单击**监视**。
3. 如果需要，请单击**活动性能计数器**选项卡。
4. 在**受监控的性能计数器**中，右键单击计数器，然后单击**删除**。

# 监视配置更改

如果设备的硬件或软件配置发生更改且设备上安装了监视代理，则此产品可以 生成警报。这些更改会影响设备的性能和稳定性或导致标准安装出现故障。通过监视设备的重要部分，此产品可降低总体拥有成本 (TCO)。

将生成警报的设备配置更改包括：

- **安装或卸载应用程序：**您可以看到哪些用户安装或删除了应用程序。此功能在跟踪许可证或员工生产率时非常有用。在控制面板的 Windows“添加/删除程序”区域中注册的应用程序被监视。其他应用程序将被忽略。Windows“添加/删除程序”中使用的应用程序名是出现在通知日志或警报弹出窗口中的应用程序名。
- **添加或删除内存：**此产品检测和监视安装的内存数量和类型。如果配置更改，则生成警报。
- **添加或删除硬盘驱动器：**此产品检测和监视设备上安装的驱动器的类型和大小。如果配置更改，则生成警报。
- **添加、删除或修改处理器：**此产品检测和监视处理器的数量、类型和速度。如果配置更改，则生成警报。

- **添加或移除网卡：**此产品检测和监视设备上的网络接口卡的数量和类型，并在配置更改时生成警报。

要查看配置更改的警报记录，请在服务器的信息控制台上检查警报日志。有关详细信息，请参阅“查看警报日志”。

# 监视连接性

在大多数情况下，出现严重情况时，例如硬盘已满或风扇停止，设备会报警。但是，在某些情况下，设备会在发送警报前进入脱机状态。例如，开关或路由器中断网络通信，或者设备电源出现故障。

在这些情况下，此产品可以定期检查设备，以确定它们是否在网络上可用。如果设备不响应 ping，则其健全性状态会下次刷新**我的设备**列表时更改为严重。

必须设置设备监视器 ping 目标设备或**所有设备**组中的全部设备。

**设置设备监视器**

1. 在**我的设备**列表中，选择要监视的设备。可以从**所有设备**、公共组或私有组中选择设备。
2. 单击**目标**。
3. 在底部窗格中，单击**操作**，然后单击**设备监视器**。
4. 要查看当前监视的设备的列表，请单击**显示监视的设备**。
5. 键入 ping 扫描之间的分钟数和产品尝试与设备建立通信的次数。
6. 选择是否对 目标设备列表中的设备或**所有设备**组中的所有设备执行操作。
7. 要停止监视所有设备，选择**从不 ping 设备**。
8. 单击**应用**。

只监视最后一组目标设备。例如，如果以设备 A 和设备 B 为目标并对其应用设备监视，则只有设备 A 和设备 B 将被核心服务器 ping。那么，如果您以设备 C 和设备 D 为目标，并对其应用设备监视，则仅监视设备 C 和设备 D；不再监视设备 A 和设备 B。

# 报警配置

## 使用警报

当设备上出现某个问题或其他事件时（例如设备磁盘空间不足），System Manager 会发出警报。选择安全性级别或会触发警报的阈值可自定义这些警报。警报将被发送到控制台，可对这些警报进行配置，以便执行特定的操作。本章将介绍警报的工作原理。



### 我如何查看警报？

本产品可通过以下方式通知您出现的问题或其他计算机事件：

- 将信息添加到日志
- 通过电子邮件发送通知或将消息发送到寻呼机
- 在核心设备或个人设备上运行程序
- 将 SNMP 陷阱发送到网络上的 SNMP 管理控制台
- 重新启动或关闭设备

请注意，分配到计算机组的某些警报可以同时生成大量的响应。例如，您可以设置警报“计算机配置更改”并使其与电子邮件操作相关联。如果软件分发修补程序被应用到包含此警报设置的计算机中，核心服务器将会生成与应用修补程序的计算机的数量相同的电子邮件，很可能“充满”您的电子邮件服务器。这种情况下，可选用另外的一种警报处理方式，即将警报写入核心日志而不发送电子邮件。

### 哪几种设备问题可以生成警报？

本产品包含一个详尽的事件列表，其中列出了可以生成警报的事件。有些是需要立即关注的问题；也有些属于配置更改，它们可能是也可能不是问题，但可以为系统管理员提供有用的信息。（有关详细信息，请参见“监控配置更改”。）设备必须配备了适当的硬件才可以生成警报。例如，只有配备了合适传感器的设备才可以生成传感器读数警报。

以下列出了可以监控的事件类型：

- **硬件更改：**处理器、内存、驱动器或板卡等组件的增减。
- **添加或删除应用程序：**在设备上安装或卸载了应用程序。
- **服务事件：**已在设备上启动或停止服务。
- **性能：**驱动器容量、可用内存等性能阈值已被超出。
- **IPMI 事件：**在 IPMI 设备上发生了可检测的事件，包括控制器、传感器、日志等的更改。

- **调制解调器使用：**已使用系统调制解调器，或增减了调制解调器。
- **物理安全性：**发生了机箱侵入窃密检测、电源循环或其他物理变更。
- **程序包安装：**目标计算机上已安装了程序包。
- **远程控制活动：**发生了远程控制会话活动，包括启动、停止或失败。

生成警报的硬件监视取决于安装在设备上的硬件功能，还取决于硬件的正确配置。例如，如果在某一设备上安装了具有 S.M.A.R.T. 监视功能的硬盘驱动器，但是此设备的 BIOS 设置中未启用 S.M.A.R.T. 检测，或者此设备的 BIOS 不支持 S.M.A.R.T. 驱动器，则无法从 S.M.A.R.T. 驱动器监视生成警报。

## 配置事件的安全性级别

设备问题或事件可能与以下显示的部分或所有安全性级别相关。

- **信息：**支持配置更改或制造商在各自的计算机系统中附带的计算机事件。此严重级别不影响设备健全性。
- **确定：**指示状态处于可接受的级别。
- **警告：**在问题变为严重之前给予一些预先警告。
- **严重：**指示该问题需要您立即关注。
- **未知：**无法确定警报状态，或未在设备上安装监控代理。

依据事件或服务器问题的性质，某些安全性级别将不适用且不包括在内。例如，对于侵入窃密检测事件，设备的机箱或是被打开，或是被关闭。如果机箱已打开，则此事件可触发安全性级别为“警告”的报警。其他事件（例如，磁盘空间和虚拟内存）包括三个安全性级别（良好、警告、严重）。

可以选择会触发某些警报的安全性级别或阈值。例如，您可以为“警告”或“严重”等警报状态选择不同的处理操作。“未知”状态不能被选作警报触发状态，它只是表明该状态无法被识别。

## 配置自定义警报规则集的过程

您可以配置警报规则集，并将其部署到单个设备或一组目标设备中。每个受管设备上必须首先安装有产品监控组件，然后才可以向核心服务器发送警报。（有关详细信息，请参见“配置代理”。）

在受管设备上安装监控组件后，该组件可提供默认的警报规则集，并向控制台发送健全性状态反馈。默认的规则集包括的警报有：

- 添加或删除磁盘
- 驱动器空间
- 内存使用情况
- 温度、风扇和电压
- 性能监控
- IPMI 事件（需要适当的硬件）

除默认的规则集外，还可以配置和部署自定义的警报规则集。可以包含自定义的警报操作以对特定事件做出响应。例如，如果风扇停止转动，可以触发一个警报并将一封电子邮件发送到您的硬件支持组。

创建和部署警报规则集的全部过程如下：

1. 选择打算部署规则集的目标设备，然后单击**目标**将其添加到**目标设备**列表。
2. 创建要使用的警报操作规则集。这些操作规则集定义了警报可触发的操作种类。（有关更多信息，请参见“配置警报操作”。）
3. 创建自定义警报规则集。执行此操作时，可以选择先前定义的操作。（有关详细信息，请参见“配置警报规则集”。）
4. 将规则集部署到目标设备。部署规则集前，可以将附加设备作为目标。（有关详细信息，请参见“部署规则集”。）

下面是此过程的一个简单例子。

## 示例：针对磁盘空间问题配置警报规则集

1. 在左侧导航窗格中，单击**我的设备**，然后双击**所有设备**组。
2. 选择要为其设置警报的设备，然后单击**目标**将设备放置在**目标设备**列表中。
3. 单击**警报**，然后单击**操作规则集**选项卡。
4. 在**操作**下拉列表中，选择要配置的操作（例如**发送电子邮件/页面**）。单击**新建**，在**名称**字段中键入名称，然后单击**确定**。
5. 返回**操作规则集**页面，选择刚刚命名的规则集，并单击**编辑操作**。根据需要在文本框中指定数据。完成时单击**保存**。
6. 单击**警报规则集**选项卡。
7. 单击**新建**，在**名称**字段中输入“磁盘空间问题”或其他类似信息，在**说明**字段中输入说明，然后单击**确定**。
8. 单击刚命名的警报规则集并单击**编辑规则集**。
9. 单击**新建**按钮。
10. 在**警报类型**下拉列表中，单击**驱动器空间**。
11. 选中要发出警报的状态：**良好**、**警告**或**严重**。（如果希望对多个状态采取相同的操作，则选择多个状态。如果希望对每种状态都采取不同的操作，则为每种状态都创建一个单独的配置，以便能够对不同的状态级别触发不同的操作。）
12. 在**操作**下拉列表中，选择符合步骤 6 和步骤 7 中指定的条件时要出现的操作。如果您希望执行的操作没有出现在列表中，可以使用**操作规则集**页面 创建一个。（如果警报操作规则集尚未创建，则它不会出现在列表中。）
13. 在**警报操作**下拉列表中，选择需要的配置。
14. 如果希望当警报显示在**所有设备**列表时，该警报能够应用于服务器的健全性状态，可选中**影响设备健全性**。如果警报的严重级别仅为**信息**，则该警报不会影响设备健全性。
15. 单击**添加**。
16. 重复步骤 6-12，可继续将其它警报添加到规则集中。
17. 完成后，单击**关闭**。
18. 如果要在规则集中更改任何警报类型，选择警报类型，然后单击**编辑**进行更改，单击**更新**，然后单击**关闭**。

19. 定义警报规则集后，将规则集应用至目标设备：单击**部署规则集**，选择规则集，然后单击**部署**。

# 配置报警

使用**操作规则集**页面提供有关选择操作后所希望的操作方式的其他信息。超出阈值时会生成警报。警报可以与某一操作相关联，如发送电子邮件。每个操作都有各自的配置，必须单独设置。

**创建操作规则集**

1. 在左侧导航窗格中，单击**警报**，然后单击**操作规则集**选项卡。
2. 在**操作**下拉列表中，选择要配置的操作。每个操作都具备各自的唯一配置列表。
3. 单击**新建**，在**名称**字段中键入名称，然后单击**确定**。
4. 返回**操作规则集**页面，选择刚刚命名的规则集，并单击**编辑操作**。
5. 如果选择**在核心服务器执行程序**或**在客户端执行程序**，请键入或粘贴出现警报时要执行程序的路径，然后单击**保存**。选择任一**执行程序**操作时，请注意程序可能不会按预期显示在桌面上。当程序运行时，它是作为 Windows 中的服务启动的，因此不会如常规应用程序那样显示。通过这种方式运行的程序不应包含需要交互操作的用户界面。要清楚判定程序是否执行，请检查 Windows 任务管理器中的进程。

   如果您选择**发送电子邮件/页面**，在**收件人**字段中键入电子邮件接收者的完整电子邮件地址；在**发件人**字段中键入有效的电子邮件地址；在**主题**字段中键入主题；在**正文**字段中键入消息；选择发送邮件的日期或时间；并在 **SMTP 服务器**字段中键入 SMTP 服务器的位置。单击**帮助**框学习如何将邮件发送给多个收件人和如何在邮件中使用变量。完成时单击**保存**。

   如果您选择**发送 SNMP 陷阱**，请键入主机名、选择版本并在**通讯字符串**框中键入通讯字符串，然后单击**保存**。

**注意：**

- 分配到计算机组的某些警报可以同时生成大量的响应。例如，您可以设置警报“计算机配置更改”并使其与电子邮件操作相关联。如果软件分发修补程序被应用到包含此警报设置的计算机中，核心服务器将会生成与应用修补程序的计算机的数量相同的电子邮件，很可能“充满”您的电子邮件服务器。这种情况下，可选用另外的一种警报处理方式，即将警报写入核心日志而不发送电子邮件。
- 一些警报操作不会影响设备健全性。这些操作包括“在客户端运行程序”、“关机/重新启动”以及仅属于信息性的任何警报。但是，如果其中的任何操作与其他确实影响设备健全性的警报操作组合，则生成的所有警报都将影响设备健全性，并将显示在警报日志中。
- 电子邮件中的**发件人**字段必须包含有效的电子邮件地址，以便 SMTP 警报发挥作用。
- 标识为版本 1 的 SNMP 陷阱将被处理，而那些标识为版本 3 的只会被转发。
- 对于 SNMP 陷阱，严重级别会在陷阱的“特定陷阱类型”字段中予以报告。值为 1 = 未知、2 = 信息、3 = 确定、4 = 警告、5 = 严重。

# 配置警报规则集

使用**警报规则集**页面可创建新的警报规则集。配置警报前，必须配置操作。（有关更多信息，请参见“配置警报操作”。）

默认情况下，**警报规则集**页面上会出现两个警报规则集：

- **核心警报规则集**：此规则集确保在启用**设备监视器**功能后（请参阅 监视连接性），警报发送至核心服务器。规则集包含预定义的警报类型组，包括设备监视器、AMT 断路器警报以及 Serial Over LAN 会话警报类型。可以编辑核心服务器警报类型的状态、操作、警报操作以及健全性设置，但是如果试图进行任何其他更改，则忽略这些信息。
- **默认规则集**：此规则集部署至所有受管设备，包含许多警报类型，大多数的网络管理员通常会使用这些警报类型。您可以编辑此规则集以添加其它警报类型和更改默认警报类型的设置。您在任何时候编辑此规则集，更改都会部署至所有受管设备，即使您未明确地重新部署规则集也同样如此。

除了这些规则集，您还可创建自定义规则集以应用至受管设备的目标组。这些规则集必须以 .XML 格式生成才能在**代理配置**中显示。

为设备创建自定义规则集时，请注意，如果默认规则集已经部署到设备，则有可能出现重叠或冲突的警报规则。如果配置受管设备时部署默认规则集，然后部署自定义规则集，则这两个规则集都将在设备上执行。例如，如果这两个规则集生成类型相同的警报，但各自采用不同的操作，则结果会产生重复或不可预料的警报操作。已部署的默认规则集无法删除，要想更改默认规则集的任何部分，可以编辑默认规则集。

### 创建警报规则集

1. 在左侧导航窗格中，单击**警报**，然后单击**警报规则集**选项卡（如有必要）。
2. 单击**新建**，在**名称**字段中输入名称，在**说明**字段中输入对该警报的说明，然后单击**确定**。
3. 单击刚命名的规则集并单击**编辑规则集**。
4. 单击**新建**。
5. 在**警报类型**下拉列表中，选择要接收警报的组件、操作或事件类型。
6. 选中要发出警报的每个状态：**信息**、**良好**、**警告**或**严重**。例如，如果希望当在步骤 5 中选择的类型达到严重阈值时接收到警报，可选中**严重**。
7. 在**操作**下拉列表中，选择符合步骤 5 和步骤 6 中指定的条件时要出现的操作。这些操作是预先设置的；如果您希望执行的操作没有出现在列表中，可以使用**操作规则集**页面 创建一个。

   **注意：**分配到计算机组的某些警报可以同时生成大量的响应。例如，您可以设置警报“计算机配置更改”并使其与电子邮件操作相关联。如果软件分发修补程序被应用到包含此警报设置的计算机中，核心服务器将会生成与应用修补程序的计算机的数量相同的电子邮件，很可能“充满”您的电子邮件服务器。这种情况下，可选用另外的一种警报处理方式，即将警报写入核心日志而不发送电子邮件。

8. 在**警报操作**下拉列表中，选择配置。可能只有一个配置可用（此列表的内容会随您在步骤 7 中所做的选择而变化）。
9. 如果希望当警报显示在**所有设备**列表时，该警报能够应用于服务器的健全性状态，可选中**影响设备健全性**。如果警报的严重级别仅为**信息**，则该警报不会影响设备健全性。
10. 单击**添加**。
11. 重复步骤 5-10，将其他警报添加到规则集中。
12. 完成后，单击**关闭**。

要编辑警报规则集，选择规则集（第 3 步），单击**编辑规则集**，然后继续以上步骤。

创建或编辑完规则集几分钟后，规则集部署服务将自动尝试更新之前已部署有该规则集的所有计算机。或者，要立即部署规则集，可单击**部署规则集**选项卡，然后单击**部署。**

# 部署规则集

使用**部署规则集**页面将所选警报规则集移到目标设备。

要将规则集部署到受管设备，必须先在该设备上安装管理代理。部署标准管理代理时，会部署默认规则集。完成代理设置时，可以更新或部署新的规则集。首先应确定希望部署规则集的目标设备。

**部署警报规则集**

1. 在左侧导航窗格中，单击**我的设备**，然后单击**所有设备**组。
2. 选择要对其部署警报规则集的设备，然后单击**目标**将设备放置在**目标设备**列表中。
3. 在左侧导航窗格中，单击**警报**，然后单击**部署规则集**选项卡。
4. 在**警报规则集**框中，选择要部署的规则集。
5. 单击链接查看目标设备列表。要从该列表中删除设备，请右键单击该设备，然后单击**删除**。要删除所有设备，右击任何设备名称，然后单击**重置**。要添加设备，您必须将其添加到 目标列表中（上述步骤 1-2）。
6. 关闭**目标列表**窗口，然后单击**部署**将所选配置部署到目标设备。

作为部署过程的一部分，将创建一个 XML 页面，其中会列出部署的规则集和在其上部署规则集的设备。此报告将保存在核心服务器的 \ldlogon\alertrules 目录中，并使用数据库所分配的序列号来命名。如果您希望在部署规则集过程以外查看此 XML 页面，请单击**生成 XML** 按钮，然后单击该链接即可查看 XML 文件。

注意，任何时候受管设备上都只能有一个自定义规则集生效。如果您已经在同一台设备上部署了一个自定义规则集，然后又部署了第二个规则集，则第一个规则集将被覆盖，而第二个规则集生效。

# 查看设备的警报规则集

使用**警报规则集**页面可查看指定给选定设备的警报规则集列表，并查看每个警报的详细信息。

**查看警报规则集**

1. 在**我的设备**视图中，双击要配置的设备。在另一浏览器窗口中将打开服务器信息控制台。
2. 在左侧导航窗格中，单击**规则集**。
3. 单击**警报规则集**选项卡。

下面介绍提供的关于每个规则集的详细信息。有关修改这些详细信息的更多信息，请参见 使用警报。

- **状态达到时：**当警报状态达到显示的状态时，将生成警报。
- **影响健全性：**指示显示在**所有设备**列表中的警报状态是否将应用到服务器的健全性状态。
- **规则集名称：**警报规则集的名称，在 警报规则集对话框中定义。
- **警报类型：**警报来源的说明（硬件、软件、事件等）。
- **操作配置：**当生成警报时发生的操作，在 操作配置对话框中定义。
- **警报处理程序：**生成的警报类型，例如电子邮件、SNMP 陷阱或执行程序。
- **实例：**指示警报的特定源。

也可单击**警报日志**按钮转至设备警报日志并查看有关警报的详细信息。（有关详细信息，请参阅查看警报日志。）

# 查看警报日志

使用**警报日志**页面可以查看发送到核心设备（全局警报日志）或受管设备中的警报。日志按“时间”(GMT) 排序，最新的记录位于日志顶部。

警报日志包含以下列：

- **警报名称：**与警报相关的名称，在**警报配置**页面中定义。
- **时间：**警报生成的日期和时间 (GMT)。
- **状态：**警报的状态可以是以下一种状态：
  - **未知：**此状态无法确定。
  - **信息：**支持配置更改或制造商在各自的计算机系统中附带的计算机事件。
  - **确定：**指示状态处于可接受的级别。
  - **警告：**在问题变为严重之前给予一些预先警告。
  - **严重：**指示该问题需要您立即关注。
- **实例：**指示警报的特定源。
- **设备名称：**生成警报的设备名称。应该是完全规范的域名。（仅全局警报日志。）
- **IP 地址：**生成警报的设备的 IP 地址。（仅全局警报日志。）

如果此设备名称未显示为完全规范的域名，这是因为本产品无法为此设备解析完全规范的域名。

**查看全局警报日志**

1. 在左侧导航窗格中，单击**日志**。
2. 要按时间、名称、状态或实例排序条目，请单击列标题。

3. 要查看警报的详细说明，请双击**警报名称**栏中的条目。
4. 要按名称、状态或实例列出日志条目，请在过滤器的下拉列表中选择过滤标准。例如，选择**警报名称**并键入一个完整的名称（如 Performance）或带有通配符的部分名称（如 Remote*）。要按日期搜索，请选择**启用日期过滤**，输入带开始日期和结束日期的范围，然后单击**查找**。
5. 要清除警报的健全性状态，请通过单击**警报名称**栏中的编号来选择警报，然后单击**清除警报**，最后单击**确定**。要删除日志条目，请选择警报然后单击**删除条目**。
6. 要删除日志中的所有条目，请单击**清除日志**。

**查看特定设备的警报日志**

1. 在**我的设备**列表中双击该设备。
2. 在左侧导航窗格中，单击**系统信息**。
3. 单击**日志**，然后双击**警报日志**。
4. 要按时间、名称、状态或实例排序条目，请单击列标题。
5. 要查看警报的详细说明，请单击**警报名称**栏中的条目。
6. 要按名称、状态或实例列出日志条目，请单击工具栏上的**过滤**按钮，并选择过滤标准。例如，选择**警报名称**并键入一个完整的名称（如 Performance）或带有通配符的部分名称（如 Remote*）。然后单击工具栏上的“查找”查看与所选过滤选项相关的警报。
7. 要查看某一日期范围内的日志条目，请清除**显示所有日期的事件**复选框，并选择一个日期范围。单击**刷新**查看仅该日期范围内的警报。

# 软件更新

System Manager 含有一个软件更新工具，您可以搜索管理软件、操作系统软件和设备驱动程序的更新。您可以下载这些类型的更新并通过部署和安装相应的更新（也称修补程序）修补受影响的设备。

阅读本章后，您将了解以下内容：

- 软件更新概述
- 关于软件更新窗口
- 配置软件更新扫描的设备
- 更新漏洞定义
- 计划软件更新下载
- 查看软件更新和检测规则信息
- 清除软件更新信息
- 为软件更新扫描设备
- 查看检测到的更新
- 下载修补程序
- 修补软件更新

## 软件更新概述

软件更新工具能让您保持网络中受管设备的软件版本的最新性。您可以让维护当前软件、下载相关更新文件以及在受影响设备上部署和安装所需更新的过程自动反复进行。

本产品使用标准的基于角色的管理功能，使用户可以访问软件更新工具。基于角色的管理是该产品的访问和安全模型，使管理员可限制对工具和设备的访问。每个用户都指定了特定的权限和范围，决定他们可以使用哪些功能以及可以使用哪些设备。管理员将这些权限指定给其他用户（详细信息请参阅 关于基于角色的管理）。要使用软件更新工具，必须以具有修补程序管理、基本 Web 控制台和报告权限的用户身份登录。

## 支持的服务器平台

软件更新功能支持大多数标准的服务器平台，使您能够扫描更新并将其部署到运行以下操作系统的受管服务器上：

- Windows 2000 Server SP4
- Windows 2000 Advanced Server SP4
- Windows 2000 Professional SP4
- Windows 2003 Standard Edition SP1
- Windows 2003 Enterprise Edition SP1
- Windows XP Pro SP2
- RedHat Enterprise Linux ES/AS 3

- SUSE Linux Server 9（Professional、Enterprise 和 Advanced）

## 关于软件更新窗口

拥有修补程序管理权限的用户将可以看到控制台左侧导航窗格中的**软件更新**工具。当您单击**软件更新**时，窗口右侧会显示一个工具栏和两个窗格。左窗格显示软件更新组的层次结构树视图。单击一个组可以在右窗格中查看其内容。右窗格的列列表中将显示软件更新定义的详细说明。在顶部它包含一个**查找**按钮，可以快速搜索指定的标准。**查找**框中不支持下列扩展字符：〈，〉，’，″，!.

## 工具栏按钮

- **更新：**打开**更新漏洞设置**对话框，在此对话框中您可以指定要更新其软件更新信息的平台和语言。还可以配置是否将更新放入**扫描**组、是否同时下载相关的修补程序、修补程序的下载位置以及代理服务器设置。
- **计划下载：**在可以配置任务选项的**计划任务**对话框中打开下载任务。单击**保存**后，下载任务被放入**计划任务窗口**中和**漏洞任务**选项卡下。
- **计划修补程序任务：**打开**计划漏洞扫描**对话框，您可在该对话框中输入名称并配置扫描器选项。
- **刷新：**更新右侧窗格中的列表，显示最新下载的更新信息。
- **清除：**打开**清除安全性和修补程序定义**对话框，在此对话框中可以指定要从核心数据库删除其漏洞信息的平台和语言。

## 左侧窗格（树视图）

窗口的左窗格显示以下组：

- **扫描：**列出当软件更新工具在受管设备上运行时搜索到的所有更新。换言之，如果此组中包含更新，则该更新将成为下一扫描操作的一部分；否则，即不是扫描的一部分。

  “扫描”是三种漏洞状态之一，另两种状态分别为“不扫描”和“未分配”。就此而言，一个软件更新一次只能属于这三组之一。每种状态的更新都以独特的图标进行识别：问号 (?) 图标代表“未分配”，红色 X 图标代表“不扫描”，正常的漏洞图标代表“扫描”。将更新从一个组移动到另一个组将自动更改其状态。

  要将软件更新从一个组移动到另一个，请右键单击该更新并选择要将其移动到的组。

  通过将更新移动到“扫描”组中，可以控制下次软件更新扫描的具体特征和大小。

  如果在**更新漏洞设置**对话框中选择了**将新定义放入“扫描”组**选项，还可以在更新过程中将新的更新自动添加到“扫描”组中。

  **从“扫描”组中移出软件更新时的注意事项**
  将软件更新从“扫描”组中移到“不扫描”组中时，核心数据库中有关哪一被扫描设备检测到更新的当前信息将从此数据库中删除，且不再出现在“软件更新属性”对话框或“扫描过的服务器信息”对话框中。要恢复该评估信息，必须将软件更新重新移到“扫描”组中，并再次运行扫描。

- **不扫描：**列出扫描器下次在设备上运行时不搜索的软件更新。如上所述，如果某个更新在该组中，则它不能同时存在于“扫描”组或“未分配”组中。您可以将更新移动到该组中，以将其从软件更新扫描中删除。

- **已检测到：**列出在前一次扫描作业中对所有包括的目标设备进行扫描时检测到的所有软件更新。无论只扫描了一台设备还是扫描了多台设备，该组中的内容始终由上次进行的软件更新扫描决定。

  “已检测到”列表中包含最近一次扫描中检测到的所有软件更新。“已扫描”列和“已检测到”列分别显示扫描了多少设备以及在其中多少台设备上检测到软件更新。要查看具体在哪些服务器上检测到更新，请右击定义，然后选择**查看受影响的计算机**。请注意，您也可以在服务器的 服务器信息控制台对话框中查看特定服务器的更新信息。

  只能将软件更新从“已检测到”组中移到“未分配”组或“不扫描”组中。

- **未分配：**列出所有不属于“扫描”或“不扫描”组中的所有软件更新。“未分配”组实质上是所收集的更新在您决定是否扫描它们之前的存储区域。

  默认情况下，所收集的软件更新将在更新过程中添加到“扫描”组中。

  可以将软件更新从“未分配”组移动到“扫描”组或“不扫描”组中。

- **按操作系统查看：**按特定设备操作系统子组列出所有已下载的软件更新。这些子组可以帮助您按操作系统类别找出更新。您可以使用这些操作系统子组将一组更新复制到“扫描”组中，从而进行特定于操作系统的扫描。

  可以将操作系统组中的软件更新复制到“扫描”、“不扫描”或“未分配”组中。更新可以同时存在于多个平台或产品组中。

- **按产品查看：**按特定产品子组列出所有已下载的软件更新。这些子组可以帮助您按产品类别找出更新。您可以使用这些产品子组将更新复制到“扫描”组中，从而进行特定于产品的扫描。

## 右侧窗格（列表视图）

该窗口的右侧窗格将显示以下软件更新详细信息，这些信息列在可排序的列中：

- **ID：**通过一个由供应商定义的唯一字母数字代码来标识更新。
- **严重性：**指示更新的严重级别。可能的严重级别包括：Service Pack、严重、高级、中级、低级、不适用和未知。
- **标题：**采用简短的文本字符串描述理的性质或目标。
- **语言：**指示受更新影响的操作系统的语言。
- **发布日期：**指示供应商发布软件更新的日期。
- **无提示安装：**指示是否无提示安装与更新相关的修补程序文件（不与用户交互）。某些更新可能有多个修补程序。如果更新的任一个修补程序无法进行无提示安装，该更新的“无提示安装”属性将为“否”。
- **可修复的：**指示是否可以通过修补程序文件部署和安装修复更新。可能的值为：“是”、“否”和“某些”（对于包含多个检测规则的更新，且并非所有检测到的更新都可以修复）。

双击更新 ID 可在其属性对话框中查看更详细的信息。在软件更新属性对话框中，可以查看该更新的检测规则、下载相关修补程序文件，还可以单击该规则查看其详细的属性对话框。

# 配置软件更新扫描的设备

必须先在受管设备上安装软件更新代理，然后它们才能扫描漏洞和接收修补程序部署。

在多台受管设备上部署软件更新代理的最简便方法：创建一个新的代理配置，选中软件更新代理（默认设置），然后使用**计划任务**为所需的目标设备计划该配置。

在对设备进行配置使之能支持软件更新时，会在目标设备上安装软件更新扫描和修补（即修补程序的部署和安装）所需的文件。

# 更新软件更新定义

您的网络会不断面临软件更新和错误修复等维护问题。由于软件更新工具让您能通过 LANDesk 提供的数据库来更新软件，所以它加快并简化了收集最新的已知修补程序信息的过程。此服务将来自多个可信的行业/供应商源的已知更新合并在一起。

通过建立和维护最新的修补程序信息，您能够更好地了解支持的每个服务器操作系统所需的软件更新的性质与程度。第一步就是掌握最新的已知更新信息。

您可以配置并即时执行漏洞更新，或者安排一个更新任务在规定的时间执行或重复执行。

**更新软件更新信息**

1. 在左侧导航窗格中，单击**软件更新**。（有关此对话框的说明，请参见 关于软件更新窗口。）
2. 单击**更新**工具栏按钮。
3. 从可用内容服务器列表中选择下载源站点。
4. 选择要更新其软件更新信息的平台。可以从列表中选择一个或多个平台。选择的平台越多，更新所需的时间就越长。
5. 为指定的平台中选择要更新其软件更新信息的语言。可以从列表中选择一种或多种语言。选择的语言越多，更新所需的时间就越长。
6. 如果希望新的软件更新定义（数据库中尚未存在的定义）会自动放入“未分配”组中，而不是默认情况下放入“扫描”组中，请取消选中**将新定义放入“扫描”组**复选框。
    - 如果要自动下载实际修补程序可执行文件，请选中**为以上选定的定义下载修补程序**复选框，然后单击下载选项之一。
      **只针对已检测到的漏洞定义：**只下载与上次软件更新扫描检测到的软件更新（即：当前存在于“已检测到”组中的更新）相关的修补程序。
    - **针对所有引用的定义：**下载与当前存在于“扫描”组中的软件更新相关的所有修补程序。这将需要很长时间。

修补程序将下载到该对话框的“修补程序设置”部分中指定的位置（见以下步骤）。

8. 如果网络中有用于外部 Internet 传输（这是更新软件更新信息和下载修补程序的必需途径）的代理服务器，则单击**代理设置**选项卡并选中**使用代理服务器**选项框。指定该服务器的地址和端口号，如果访问该代理服务器必须登录，还应指定身份验证凭据。
9. 可随时单击**应用**保存设置。
10. 单击**立即更新**运行软件更新。**更新安全性和修补程序定义**对话框会显示当前的操作和状态。
11. 更新完毕后，单击**关闭**。请注意，如果在更新完成前单击**取消**，则只有此刻前已被处理的软件更新信息会被下载到核心数据库中。您需要再次运行更新以获取所有剩余的信息。

**注意：**当更新进程正在运行时不要关闭控制台，否则该进程将终止。但对计划的下载任务而言，这一点并不适用。

如果已在同一台核心服务器上安装了 System Manager 和 LANDesk® Management Suite，则这两种产品会使用相同的设置文件来确定更新哪些类型的漏洞。在某些情况下，运行更新时，可以在 System Manager 中看到只能从 Management Suite 配置的更新。例如，如果您已在 Management Suite 中将安全威胁选择为更新选项，然后在 System Manager 中选择更新软件更新，则当您在 System Manager 中运行更新时，可以在已更新的项目中同时看到软件更新和安全威胁。

**配置修补程序下载位置**

1. 在**更新漏洞设置**对话框中，单击**修补程序设置**选项卡。
2. 输入要将修补程序文件复制到的 UNC 路径。默认位置为核心服务器的 \LDLogon\Patch 目录。
3. 如果前面输入的 UNC 路径是核心服务器以外的位置，则输入访问该位置时用于验明身份的有效用户名和密码。

   文件夹必须启用文件和 web 共享且支持匿名访问。

4. 输入 Web URL，服务器通过该 URL 可以访问已下载修补程序以进行部署。Web URL 应与上面的 UNC 路径相符。
5. 您可以单击**测试设置**来检查能否连接到前面指定的 Web 地址。
6. 如果要将 UNC 路径和 Web URL 恢复为其默认位置，请单击**重置修补程序设置**。默认位置为核心服务器的 \LDLogon\Patch 目录。

## 计划软件更新下载

您也可以将软件更新配置为计划任务，以便在将来的设定时间自动执行或重复执行该任务。要执行此操作，单击**计划下载**工具栏按钮，打开**计划任务属性**对话框，从中指定任务并配置其选项。单击**保存**后，该任务将出现在“计划任务”窗口中。

所有计划的软件更新任务都将使用**更新漏洞设置**对话框中的当前设置。因此，如果要更改某更新作业的源站点、平台、语言、修补程序下载站点或代理服务器设置，则必须在安排任务运行之前首先更改**更新漏洞设置**对话框中的这些设置。

**配置计划下载任务**

1. 在左侧导航窗格中，单击**软件更新**。
2. 单击**计划下载**。
3. 在**计划任务**页面中，配置 计划。
4. 单击**保存**。

单击**计划任务**后，则创建了一个任务（该任务无目标设备也未计划）。如果取消此**计划任务**过程，则请注意，该任务仍为已创建且显示在**我的任务**列表中。

# 查看软件更新和检测规则信息

从 LANDesk 安全服务中使用最新信息对软件更新进行更新后，可以从控制台中查看软件更新列表，按平台和产品查看这些更新，并将它们移入不同的状态组中。有关窗口中各个组的信息以及如何使用这些组，请参见本章前面的 关于软件更新窗口。

要查看软件更新的详细信息，双击一个软件更新 ID 可打开其“属性”对话框。在这一对话框中，也可以通过双击**检测规则**列表中的一个修补程序文件名打开修补程序属性对话框的方式（请参见 关于修补程序属性对话框）来获得检测规则详细信息。

该信息可帮助您确定哪些更新与您的网络支持的服务器平台相关、更新检测规则如何检查漏洞的存在、哪些修补程序可以使用以及如何为受影响的设备配置和执行修补任务。

还可以直接从控制台中查看特定于已扫描设备的软件更新定义和检测规则信息，方法是从**我的设备**中访问服务器信息控制台，然后在左侧导航窗格中单击**软件更新**。

# 清除软件更新信息

如果确定某一条软件更新信息与您的环境无关，可以从软件更新窗口（并随后从核心数据库）中清除该信息。

清除软件更新信息时，相关的检测规则信息也将同时从数据库中删除。不过，该过程并不删除实际修补程序的可执行文件。必须从通常位于核心服务器上的本地资料档案库中手动删除修补程序文件。

### 清除软件更新信息

1. 单击**清除**工具栏按钮。（有关此对话框的说明，请参见“关于‘清除安全和修补程序定义’对话框”。）
2. 选择要删除其软件更新信息的平台。可以从列表中选择一个或多个平台。

   如果某个更新与多个平台相关联，则必须选择与其关联的所有平台，才能删除该更新的信息。

3. 选择要删除其更新信息的语言（与上面指定的平台相关联）。

   如果在上述过程中选择了 Windows 平台，则应指定要删除哪些语言更新信息。如果选择的是 UNIX 平台，则必须指定“中性语言”选项，以便删除多种语言的更新信息。

4. 单击**删除**。

# 为软件更新扫描设备

软件更新评估是指根据当前已知的最新软件更新，在设备上检查操作系统特定文件的当前安装版本和注册表项，以确定服务器的更新需求。在查看了已知的软件更新信息（更新自行业源）并确定要

扫描哪些更新之后，您可以在已安装软件更新代理的受管设备上执行自定义评估。（有关配置设备进行扫描和修补程序部署的信息，请参见本章前面的“配置设备以进行软件更新扫描”。）

每次运行时，软件更新扫描器都会读取“扫描”组的内容并扫描这些特定的更新。扫描服务器更新前，应始终确保只有希望扫描的软件更新包含在该组中。可以将软件更新移入或移出“扫描”组，从而自定义扫描的特性和大小。

## 运行软件更新扫描器

可以从控制台将软件更新扫描器作为计划的扫描任务“推”向设备。

**创建软件更新扫描任务**

1. 在左侧导航窗格中，单击**软件更新**。
2. 确保最近已更新了软件更新定义。
3. 确保“扫描”组仅包含需要扫描的那些更新。
4. 单击**计划修补程序任务**工具栏按钮。（有关此对话框的说明，请参见“关于‘计划漏洞扫描’对话框”。）
5. 输入此次扫描的唯一名称。如果任务脚本已经存在，可以选择是否覆盖现有脚本。
6. 指定是否希望软件更新扫描器在目标设备上显示进程对话框。还可指定是否要在扫描器对话框中显示“取消”按钮，以便最终用户能够取消扫描。
7. 指定当目标设备上的软件更新扫描器完成运行后将如何关闭对话框。可以指定需要用户输入，也可以设置对话框在指定的超时时间后关闭。
8. 单击**确定**。
9. 在底部窗格中（**漏洞任务**下）选择任务，然后单击**编辑**。设置目标和 计划参数，然后单击**保存**。

# 查看检测到的更新

如果软件更新扫描器在任意目标设备上发现属于已启用软件更新的任意更新，则会将相应信息报告给核心服务器并添加到**已检测到**列表。

运行软件更新扫描后，可以使用以下任一方法查看检测到的更新：

## 按照“已检测到”组

从软件更新窗口中选择**已检测到**组可以查看最近一次扫描中检测到的所有更新。

## 按照单个设备

在**我的设备**中双击一个设备名，然后单击**软件更新**可查看该设备的详细软件更新评估信息。

# 下载修补程序

要在已检测到软件更新的设备上部署修补程序，必须先将修补程序可执行文件下载到网络中的本地修补程序资料档案库中。下载修补程序文件的默认位置是核心服务器上的 /LDLogon 目录。可以在**更新漏洞设置**对话框的**修补程序设置**选项卡中更改此位置。

**修补程序下载位置和代理服务器设置**
下载修补程序时始终使用**更新漏洞设置**对话框内**修补程序设置**选项卡中的当前下载位置设置。另请注意，如果您的网络通过代理服务器访问 Internet，则必须先在**更新漏洞设置**对话框的**代理设置**选项卡中配置代理服务器的设置，然后才能下载修补程序文件。

本产品首先尝试从“修补程序属性”对话框中所显示的 URL 下载修补程序文件。如果无法建立连接，或者该修补程序由于某些原因不可用，则本产品将从 LANDesk 安全服务（即公司提供的包含来自可信行业源的修补程序的数据库）下载修补程序。

可以一次下载一个修补程序，也可以一次同时下载一组修补程序。

### 下载单个修补程序

1. 双击一个软件更新名称打开其**属性**对话框。
2. 在**检测规则**部分，选择要下载的检测规则修补程序文件，然后单击**下载选定的修补程序**。
3. **正在下载修补程序**对话框中将显示下载操作和状态。可以随时单击**取消**来停止整个下载过程。
4. 下载完成后，单击**关闭**按钮。

### 下载多个修补程序

所有计划的软件更新任务都将使用**更新漏洞设置**对话框中的当前设置。因此，如果要更改某更新作业的源站点、平台、语言、修补程序下载站点或代理服务器设置，则必须在安排任务运行之前首先更改**更新漏洞设置**对话框中的这些设置。

1. 在左侧导航窗格中，单击**软件更新**。
2. 单击**计划下载**。
3. 在**计划任务**页面中，配置计划。
4. 单击**保存**。

# 删除修补程序文件

要删除修补程序文件，必须从修补程序资料档案库（通常是核心服务器的 LDLogon 目录）中手动删除文件。

# 修补软件更新

更新软件更新定义、将要扫描的更新放入“扫描”组中、在受管设备上运行扫描、确定哪些软件更新需要处理并下载必要的修补程序之后，下一个步骤便是通过在受影响的设备上部署和安装必要的修补程序，执行软件更新修补。

软件更新修补针对单个软件更新逐一进行。换句话说，您可以为特定软件更新创建一个修补任务，部署和安装必要的修补程序文件。

请注意，与软件更新扫描相似，您只能在已使用软件更新代理进行配置的设备上修补更新。有关详细信息，请参见本章前面的 配置设备以进行软件更新扫描。

支持 Linux 修补。您可以使用软件更新工具在 Linux 设备中搜寻漏洞，然后决定是否修补更新。如果希望如此操作，则可以使用 Linux 厂商的支持预订来下载所需的 RPM，然后将 RPM 部署到设备。

**警告：**许多修补程序都会在修补完成后自动重新启动设备。

### 创建自定义修补脚本

1. 在左侧导航窗格中，单击**软件更新**。
2. 选择**已检测到**组查看最近一次扫描检测到的软件更新。（没有必要选择该组。如果要针对未扫描或未检测到的更新创建自定义修补脚本，可以单击其他任何漏洞组，查看其内容并选择具体的漏洞。）
3. 右击定义，然后选择**查看受影响的设备**查看受此软件更新影响的设备。
4. 右击定义，然后选择**创建修补任务**。
5. （可选）在**任务名称**文本框中修改名称。
6. 从选项中进行选择，然后单击**确定**。
    - **将受影响的计算机复制到目标车：**将受软件更新影响的计算机复制到目标车以进行修补。
    - **运行时显示进度：**扫描器在最终用户设备上运行时，允许其显示信息。如果要显示扫描器活动，并在此对话框中配置其他显示和交互选项，可单击此选项。如果不单击此选项，此对话框中的其他选项均无法配置，扫描器将在设备上透明运行。
    - **关闭漏洞扫描对话框前需要用户输入：**如果希望在扫描器的显示对话框在设备上关闭前提示最终用户，则单击此选项。如果选择此选项，而最终用户没有响应，则对话框将保持打开状态，这将导致其它计划任务超时。
    - **超时后自动关闭对话框：**如果希望扫描器的显示对话框在经过指定时间后关闭，则单击此选项。

# 脚本

## 管理脚本

本产品使用脚本在设备上执行自定义任务。完成脚本创建对话框后，将生成 Windows INI 格式的 ASCII 文本文件，扩展名为 .INI。这些脚本存储在核心服务器的 \Program Files\LANDesk\ManagementSuite\Scripts 文件夹中。脚本文件名即为控制台中的脚本名。可以使用**脚本**窗口为 Windows 设备创建本地调度程序脚本（在左侧导航窗格中，单击**脚本**），也可以编写自己的脚本文件并将其保存到“脚本”文件夹中。

**脚本**窗口将脚本分为下列类别：

- **我的脚本**：与此组关联的脚本。
- **所有其他脚本**：核心服务器上的所有脚本。
- **用户脚本**（只有管理员可以看见）：由所有产品用户创建的脚本。这些脚本按照创建者排序。

可以在**我的脚本**项下创建组，将您的脚本进一步分类。要创建新的本地调度程序脚本，单击**本地**按钮。

创建脚本之后，可以在该脚本的快捷菜单中单击**计划**。在**我的设备**窗口中，可以指定应运行任务的设备，然后可以从**计划任务**窗口中安排应运行任务的时间。有关计划任务的详细信息，请参阅“计划任务”一节。

### 针对先前版本的 Management Suite 用户脚本和任务所有权的变化

对于 Management Suite8.70 之前的版本，所有脚本都是全局脚本，所有用户都可以看到。现在，只有脚本创建者和管理员可以看到脚本。

**脚本**窗口包含“状态”列。如果所有用户都可以看到该脚本，则“状态”列显示为“公共”；如果只有创建脚本的用户或管理员可以看到该脚本，则显示为“私有”。用户可以右键单击自己创建的脚本，然后单击“私有”或“公共”来更改脚本的状态。管理员可以更该任意脚本的状态。

默认值为 DOS PE。如果选择任何其他 PE，则无法创建命令脚本。对于 Windows 和 Linux PE，只能生成捕获脚本或部署脚本。

如果选择 Linux PE，则只能使用 LANDesk 或其他映像工具选项。如果选择 Windows PE，则可以使用 LANDesk、其他和 Microsoft* XImage。

### 创建本地调度程序脚本

本地调度程序是在设备上运行的一种服务。在部署代理配置时作为标准管理代理的一部分安装。通常本地调度程序处理产品任务，例如定期运行清单扫描器。您安排的其他任务是由核心服务器而不

是本地调度程序处理的。您可以使用本地调度程序安排自己的任务以在设备上定期运行。创建了本地调度程序脚本之后，可以将其部署到受管设备上，就像任何其他脚本一样。

本地调度程序为每个任务分配一个 ID 号。本地调度程序脚本的 ID 范围与产品使用的默认本地调度程序脚本的 ID 范围不同。在每个设备上仅可有一个自定义调度程序脚本是活动的。如果您创建了一个新的脚本并将其部署到设备，它将替换旧的脚本（自定义本地调度程序 ID 范围内的任何脚本）而不影响默认的本地调度程序脚本，例如本地清单扫描计划。

选择脚本的计划选项时，要注意各个选项的限制。例如，如果您选择“星期一”作为每周的某天，“17”作为每月的某天，则该任务将仅在同时是 17 日的星期一执行，这种情况很少发生。

您可以创建一个脚本，以立即或随时在本地机器上运行 restartmon.exe。如果来自某台机器的报告似乎已停止，则您可以使用 LDClient 文件夹中的 restartmon.exe 来重新启动收集器和所有监控提供程序。该实用程序适用于已安装了报告但报告已停止的机器。使用该实用程序可重新启动收集器和提供程序而无需重新启动设备。

1. 在左侧导航窗格中，单击**脚本**。
2. 单击**本地**。
3. 输入脚本名称。
4. 单击**添加**定义脚本的选项。
5. 如刚才所述配置本地调度程序选项。完成后，单击**保存**。
6. 单击**保存**以保存脚本。
7. 在**我的脚本**组中选择脚本，然后单击**计划**，将所创建的脚本部署到设备。

## 了解带宽选项

当配置本地调度程序命令时，您可以指定要执行任务，受管设备必须拥有的最小带宽。当到任务执行的时间时，每个运行本地调度程序任务的设备将向您指定的计算机发送少量的 ICMP 网络流量并评估传输性能。如果测试目标计算机不可用，则该任务将不执行。

您可以选择以下带宽选项：

- **RAS**：当设备到目标计算机的网络连接至少为 RAS 或拨号速度时，任务才会执行。选择此选项一般来说意味着只要设备有任何种类的网络连接，任务都将会运行。
- **WAN**：当设备到目标计算机的连接至少为 WAN 速度时，任务才会执行。WAN 速度为非 RAS 连接速度，它比 LAN 阈值低。
- **LAN**：当设备到目标计算机的连接超过 LAN 速度设置时，任务才会执行。默认情况下，LAN 速度为 262,144 bps。

## 安排脚本任务

**计划任务**窗口显示计划任务的状态：任务正在运行、任务已完成。调度程序服务以两种方式与设备进行通信：

- 通过标准管理代理（必须已安装在设备上）。

- 通过域级系统帐户。所选的帐户必须已使用服务权限登录，并且必须在“配置服务”实用程序中指定了凭证。有关配置调度程序帐户的详细信息，请参阅“配置调度程序服务”。

LANDesk 安装多个标准脚本，可安排执行日常维护任务的脚本，例如，对选定的设备进行清单扫描。在左侧导航窗格中单击**脚本**，然后单击**所有其他脚本**以查看并安排这些脚本。

**计划任务**

1. 在左侧导航窗格中，单击**脚本**。
2. 单击可以导航到脚本组。
3. 单击某个脚本，然后单击**计划**。
4. 键入任务的名称，然后单击**确定**。
5. 在**自定义脚本任务**选项卡中，单击**所有任务**，再单击第 3 步中命名的任务，然后单击**编辑**。
6. 填充自定义脚本任务的页面。有关任何页面的帮助，请单击“帮助”按钮，或参阅 任务调度程序帮助。

单击**计划**后，便创建了一个任务（该任务无目标设备也未计划）。如果取消此计划任务过程，则请注意，该任务仍然会创建，而且会显示在“任务”列表中。

## 使用默认脚本

本产品附带了两种默认的脚本。可以使用它们来帮助您完成某些典型的任务。这些脚本显示在**脚本**窗口的**所有其他脚本**树下（左侧导航窗格|**脚本**）下。

- **清单扫描器：**对选定的设备运行清单扫描器。此脚本包含说明如何编写脚本文件的文档。有关正确使用命令和参数的详细信息，请阅读或打印此脚本文件。
- **恢复客户端记录：**对选定的设备运行清单扫描器，但该扫描器报告到配置该设备的核心。在多核心环境中，如果您必须重新设置数据库，此任务可以帮助您将设备添加回正确的核心数据库中。

# 计划任务

## 计划任务



**计划任务**工具是代理配置、软件更新、脚本和设备搜寻的通用工具。任务在特定功能页面下方的窗格中被过滤，只显示相关任务。例如，如果打开**设备搜寻**工具，搜寻任务将显示在下半窗格的**搜寻任务**选项卡上。所有任务通过**计划任务**工具仍然保持可见。您可以在此处安排配置立即运行、在未来的某个时间点运行或重复运行，或者只运行一次。

**计划任务**页的左窗格显示了这些任务组：

- **我的任务**：已计划的任务。只有您和管理用户可以查看到这些任务。
- **全部任务**：包括您的任务和标记为公共的任务。
- **常见任务**：用户标记为常见的任务。在这一组中编辑或计划某个任务的任何用户都将成为该任务的所有者。该任务将保留在“常见任务”组中，同时该用户还可在“用户任务”组中看到他自己所计划的任务。
- **用户任务**（仅管理用户）：任务用户已创建。

单击**我的任务**、**公共任务**或**所有任务**时，右侧窗格将显示以下信息：

- **任务**：任务名称。
- **开始时间**：计划运行该任务的时间。单击某任务名，然后单击**编辑**，即可编辑开始时间或重新计划该任务。
- **状态**：整体任务状态。查看右侧窗格的“状态”列可获得更多详细信息。右侧窗格列显示任务状态，这些状态可以是“正在进行”、“全部完成”、“未完成”或“失败”。
- **分发程序包**：任务分发的程序包名称。该字段适用于软件分发。
- **传送方式**：任务使用的传送方式。该字段适用于软件分发。
- **所有者**：最初创建任务使用脚本的用户的姓名。

双击一个计划任务时，右侧窗格将显示以下摘要信息：

- **名称**：任务状态名称。
- **数量**：每个任务状态中的设备数量。
- **百分比**：每个任务状态中的设备百分比。

为设备计划任务前，该设备必须安装适当的代理，并且必须位于清单数据库中。服务器配置出现异常。可确定没有安装标准管理代理的设备的位置。可以在“任务”选项卡中重新安排（编辑）或删除任务。安排任务后，可在“任务”选项卡中查看任务状态。

您可以选择要编辑的任务，然后单击**编辑**来编辑任务。该任务在打开的时候带有适用于该任务的编辑选项。

## 自定义任务组

可以针对**我的任务**、**所有任务**和**公共任务**等任务类型创建自定义组。通过自定义组，可以将漏洞扫描和运行脚本等相关任务分组。组和子组可以有 20 层深。

1. **创建自定义任务组**在左侧导航窗格中，单击**计划任务**。

2. 在左侧窗格中，单击创建组时希望使用的任务类型。
3. 在工具栏上单击**新建组**。
4. 在**组名**文本框中键入一个名称，然后单击**确定**

创建自定义组后，从列表中选择任务或其他组，并单击工具栏中的**移动**，可以将它们移动或复制到该组中。

## 关于目标设备页面

使用此页面添加设备，您配置的任务将在这些设备上运行。在此选项卡中还可查看任务的目标设备、查询和设备组。如果安装了多个 LANDesk 管理产品，则可以在所有控制台中查看任何一个产品控制台中创建的设备组。设备搜寻任务不需要此页。

- **添加目标列表：**从**我的设备**添加以前放在目标列表中的设备。
- **添加查询：**为先前创建的查询结果确定目标。
- **删除：**删除选定的目标。

---

尽管本页显示目标设备组，但请注意仅在核心服务器上安装 LANDesk Management Suite 时才会显示组。如果在 Management Suite 中运行 Server Manager、System Manager 或 Web 控制台，则设备组不会成为目标组。相反，如果选择一个组并将其作为目标组，则该组中的单台设备会添加到这个目标设备列表中，而且还会在**目标设备**而非**目标组**下显示。

---

## 关于计划任务页面

调度程序包含**计划任务 - 属性**选项卡，它具有以下选项。

- **保持不计划：**（默认）保留任务列表中的任务，以后再计划。
- **立即开始：**尽快运行任务。开始任务可能需要一分钟时间，具体取决于另一设置。
- **在预定时间开始：**在指定的时间开始任务。单击此选项后，必须输入下列内容：
    - **日期：**要开始任务的日期。根据您所在位置的不同，日期顺序将采用日-月-年或月-日-年的方式。
    - **时间：**要启动任务的时间。
    - **重复间隔：**如果希望任务重复执行，则单击选择希望每**小时**、**日**、**周**或**月**重复一次。如果选择了**月**或者某个并非所有月都有的日期（例如，31 号），则任务将只按照包含此日期的月来运行。

- **计划这些设备：**如果任务初次运行，应保留默认的“正在等待或当前正在工作”。对于已运行过的任务，可从“全部”、“未成功的设备”或“未尝试运行该任务的设备”中选择。下文将详细解释这些选项。
  - **未成功的设备：**如果仅希望在首次执行任务时失败的设备上运行该任务，可选择此选项。这将排除具有“成功”状态的设备。任务将在处于其他状态的设备上执行，包括“正在等待”或“活动”。如果希望在尽可能多的未成功设备上运行该任务，但只需在每台设备上成功运行一次该任务，则可考虑使用此选项。
  - **正在等待或当前正在工作：**如果希望在等待处理或当前正在处理的设备上运行任务，则选择此选项。
  - **全部：**如果希望在所有设备上运行该任务（无论其处于何种状态），可选择此选项。如果某一任务，特别是重复性的任务，需要在尽可能多的设备上运行，可考虑使用此选项。
  - **没有执行此任务的设备：**如果仅希望在没有完成该任务（而非无法运行）的设备上运行该任务，可选择此选项。这将排除处于“关机”、“忙碌”、“已失败”或“已取消”状态的设备。如果有许多目标设备没有完成此任务，并且这些任务不如目标重要，则可考虑使用此选项。

## 关于“自定义脚本”页面

- **当前选定的自定义脚本：**选择要安排的脚本。

# 报告

## 关于报告

System Manager 包括一个报告工具，利用此报告工具可以生成各种专门的报告，这些报告提供有关网络中受管设备的关键信息。

System Manager 使用清单扫描实用程序将设备（和收集的有关这些设备的硬件与软件数据）添加到核心数据库中。可以从设备清单视图中查看、打印此清单数据，还可以利用它定义查询并对设备进行分组。此报告工具通过收集并按实用的报告格式管理这些数据，可进一步利用此扫描的清单数据。

您可以使用预定义的服务报告和清单资产报告。运行报告后，可以从控制台查看此报告。

如果同时安装了 Server Manager 和 Management Suite，则在 Server Manager 中运行的报告仅包括服务器。如果运行查询，您将同时包括服务器和其他设备，除非已配置了该查询排除了其他设备。

如果来自某台机器的报告似乎已停止，则您可以使用 LDCLIENT 文件夹中的 restartmon.exe 来重新启动收集器和所有监控提供程序。该实用程序适用于已安装了报告但报告已停止的机器。使用该实用程序可重新启动收集器和提供程序而无需重新启动设备。

### 了解报告组和预定义报告

在“报告”窗口（左侧窗格|**报告**）中，**报告**是以组的方式组织的。管理员可以查看所有报告组的内容。System Manager 包括一个特定的角色（称作报告），利用该角色，其他人可以在不具备对其他管理功能的访问权限情况下查看报告。（有关详细信息，请参阅“基于角色的管理”。）具有报告访问权限的用户也可以查看和运行报告，但只能在其范围内的设备上进行。

**报告**窗口中包含下列报告组：

- 硬件
- 软件

## 查看报告

您可以从**报告**窗口运行任何报告。

在**报告**窗口中，选择一个报告组，然后单击要运行的报告。**报告视图**中将显示报告数据。

# 关于“报告视图”窗口

报告可使您以图表方式迅速查看客户端计算机的资产。报告由扫描器存储在数据库中的数据生成。可以通过浏览器查看报告或打印报告。

**查看报告**

1. 在左侧导航窗格中，单击**报告**。报告类别将显示在右侧窗格中。单击类别标题以查看报告列表。每个报告旁边的图标指示报告类型。

    如果报告旁边有图表图标，该报告将显示为饼图或条形图（二维或三维）。可在图表中单击任一彩色条或饼图扇区，展开一个一览表。

    如果报告旁边有文档图标，该报告将显示为文本。

2. 单击报告名称可查看该报告。
3. 要查看硬件或软件扫描日期一览表，请单击开始和结束日期以设置期限，然后单击**运行**。

“磁盘空间一览表”报告仅包含基于 Windows 的设备的数据。

要打印报告，请右击该页，然后单击**打印**。在“打印”对话框上，单击**打印**。如果报告不止一页，则必须在每一页中右击才能完整地打印报告。

**分发报告**

- 要通过电子邮件发送报告，推荐将其打印为 .PDF 文件，然后粘贴为邮件的附件。

控制台将以饼图或条形图显示报告图表。要设置图表类型，请单击报告图表中的下拉列表，然后更改图表类型。

必须安装 Macromedia Flash Player* 7，方可查看多数报表中显示的交互式条形和饼形图。

# 查询

## 使用查询

查询是对核心数据库执行的自定义搜索。本产品提供的工具可以为核心数据库中的设备创建数据库查询。核心数据库查询是在控制台的**查询**视图中创建的。可以在 LANDesk® Management Suite 中查看 System Manager 公共查询，反之亦然（如果两者同时使用）。

阅读本节后，您将了解以下内容：

- 查询概述
- 查询组
- 创建数据库查询
- 运行查询
- 导入和导出查询

### 查询概述

借助于查询，您可以根据特定的系统或用户标准，搜索和组织核心数据库中的设备，从而协助您管理网络。

例如，您可以创建并运行一个查询，它只查找以下这种设备：处理器的时钟频率低于 166 MHz，或 RAM 小于 64 MB，或硬盘驱动器小于 2 GB。创建一条或多条表示这些条件的语句，并使用标准逻辑运算符将它们相互关联起来。运行查询后，可以打印查询的结果，并访问和管理相应的设备。

### 查询组

查询可以关联**我的设备**视图中的组。这些组称作动态组，动态组的内容是与此动态组相关联的查询的结果。例如，包含某地理区域中所有设备的组可以与有关内存、硬盘大小等项的查询相关联。

有关如何**所有设备**视图中显示查询组和查询以及使用它们可以完成哪些任务的详细信息，请参阅“对设备分组操作”。

### 创建数据库查询

在**新建查询**对话框中，通过选择属性、关系运算符和属性值可以构建查询。选择清单属性，然后将其与适当的值关联起来，这样可以构建查询语句。将查询语句彼此之间进行逻辑上的关联，以确保在将这些语句与其他语句或组关联之前，可将它们作为组进行求值。

#### 创建数据库查询

1. 在控制台的**查询**视图中，单击**新建**。
2. 从清单属性列表中选择**组件**。

3. 在**第 1 步：搜索条件**下，单击**编辑**。
    1. 展开此列表，选择要用作搜索条件的属性。例如，如果要查找运行某一特定类型的软件的所有客户端，则应选择 "Computer.Software.Package.Name"。
    2. 选择属性之后，您将看到窗口的右侧出现了一系列的字段。从这些字段中选择运算符和值，以完成搜索条件。例如，如果要查找运行 Internet Explorer 5.0 的所有客户端，则属性应该是“Computer.Software.Package.Name”，运算符为“=”，而值为“Internet Explorer 5”。
    3. 在窗口底部，单击**添加**将您所创建的搜索条件填充到空字段中。
    4. 通过创建其他搜索条件，然后使用布尔运算符（AND 或 OR）将其添加到第一个搜索条件中，可以进一步完善查询。也可以使用按钮来添加、删除、替换、组合（或取消组合）您所创建的搜索条件。
    5. 操作完成后，单击**确定**。
5. 在**第 2 步：要显示的属性**下，单击**编辑**。
    1. 展开此列表，选择要显示在查询结果列表中的属性。请记住，要选择那些有助于确定查询中返回的客户端的属性。如果找不到要显示的属性，您可以在 自定义属性对话框中添加属性。但是，必须在这些属性出现在查询对话框中之前将这些属性指定给机器。

    2. 选定属性后，单击**添加**将它移至窗口右侧的空白字段中。如果要列举查询结果列表，可单击**包括计数**。
    3. 如果要添加更多属性，请重复上述过程。使用**删除**按钮删除属性，然后单击**向上移动/向下移动**，更改属性顺序。
    4. 单击**使结果可命中**来启用查询结果为所指定的任何操作的可命中目标。
    5. 操作完成后，单击**确定**。
6. （可选）在**第 3 步：按属性排序结果**下，单击**编辑**自定义查询结果的顺序。
7. 如果要更多次运行该查询，单击**保存查询**，然后为查询输入唯一的名称。如果在保存之前运行查询，查询参数将丢失，必须重构才能再次运行相同的查询。
8. 在**第 4 步：运行查询**下，单击**运行查询**。

**以显示的顺序执行查询语句**

如果未进行分组，该对话框中列出的查询语句将按自下至上的顺序执行。请确保将相关的查询项分成一组，以便按组对这些项进行求值，否则，查询的结果可能会出乎意料。

# 运行查询

**运行查询**

1. 在左侧导航窗格中，单击**查询**。

2. 选择查询，并单击**运行**。

   或

   要在运行之前更改查询，双击查询，接着单击**编辑**，修改第 1-3 步，然后单击**运行查询**。

   **注**：如果修改查询后要保存更改，请单击**保存查询**以保存更改，或者单击**将查询另存为**为修改后的查询指定新名称。在运行查询之前执行此操作。如果在运行查询之前未保存更改，对查询的更改将无法保存。

3. 结果（匹配的设备）显示在**所有设备**视图的右侧窗格中。

## 导入和导出查询

可以使用导入和导出功能将查询从一个核心数据库传输到另一个核心数据库。导出的查询另保存为 .XML 文件。

**导入查询**

1. 右击将放置所导入的查询的查询组。
2. 从快捷菜单中选择**导入**。
3. 浏览至要导入的查询并选中它。
4. 单击**打开**，将该查询添加到**所有设备**视图中的所选查询组。

**导出查询**

1. 右击要导出的查询。
2. 从快捷菜单中选择**导出**。
3. 浏览到要将该查询保存为 .XML 文件的位置。
4. 键入查询的名称。
5. 单击**保存**，导出查询。

# 了解自定义查询

要获得有关您的设备上安装的硬件和软件的详细清单信息，可以使用自定义查询。使用自定义查询可以生成具有相似清单的计算机列表。自定义查询还可用于定义组和范围。

**自定义查询**页（单击左侧导航窗格中的**查询**）显示已保存的查询列表。要运行已保存的查询，选择该查询，然后选择**运行**。

---

如果查询列表跨多页，请使用页面顶部的箭头浏览至每一页。输入每页显示的条目数，然后单击**设置**。

# 创建自定义查询

要获得有关您的设备上安装的硬件和软件的详细清单信息，可以使用自定义查询。使用自定义查询可以生成具有类似清单的设备列表。例如，如果想要将所有设备升级到至少 750 MHz 处理器，可以查询您的数据库中处理器速度低于 750 MHz 的所有设备。自定义查询还可用于定义组和范围。

您可以查询清单扫描器存储在数据库中的任何清单项（称为“属性”）以及任何自定义属性。

## 管理查询

在**查询**视图中管理查询。可使用此视图来创建、编辑或删除查询：

- 要运行现有的查询，请选择它然后单击**运行**。
- 要创建新查询，请单击**新建**。创建并保存查询后，其名称将显示在本页的列表中。
- 要编辑列表中的查询，请双击它。**编辑查询**页面将显示可以编辑的查询参数。
- 要编辑最新的查询，请单击**编辑当前查询**。
- 要删除一个查询，请选择该查询并单击**删除**。

创建查询的过程分为四步：

1. **创建搜索条件**：指定一组清单属性作为查询的基础。
2. **选择要显示的属性：**优化或“筛选”查询，以便在查询结果中显示您最需要的属性，如 IP 地址或计算机设备名。
3. **按属性对结果排序（可选）**：选择想要的查询结果排序方式。（仅当在第 2 步中选择在查询结果中显示多种属性类型时才执行此步骤。）
4. **运行查询**：运行刚创建的查询。也可以保存该查询备用，或者清除所有查询信息重新开始查询。

# 第 1 步：创建搜索条件（必需的）

搜索条件是您所要查询的一组清单属性和相关值。您可使用一个搜索条件或将多个搜索条件组合起来，从而形成查询的基础。

以下步骤在**编辑查询**页中执行。从**运行查询**视图中，单击**新建**或选择一个现有查询，然后单击**编辑**。

### 创建搜索条件

1. 在**第 1 步**中，单击**编辑**。此时将显示一个窗口，其中列出了数据库中当前所存在的所有清单数据。
2. 展开此列表，选择要用作搜索条件的属性。例如，如果要查找运行某一特定类型的软件的所有客户端，则应选择 "Computer.Software.Package.Name"。

3. 选择属性之后，您将看到窗口的右侧出现了一系列的字段。从这些字段中选择运算符和值，以完成搜索条件。例如，如果要查找运行 Internet Explorer 5.0 的所有客户端，则属性应该是“Computer.Software.Package.Name”，运算符为“=”，而值为“Internet Explorer 5”。
4. 在窗口底部，单击**添加**将您所创建的搜索条件填充到空字段中。
5. 通过创建其他搜索条件，然后使用布尔运算符（AND 或 OR）将其添加到第一个搜索条件中，可以进一步完善查询。也可以使用按钮来添加、删除、替换、组合（或取消组合）您所创建的搜索条件。
6. 操作完成后，单击**确定**。

要运行并存储有关服务器健全性状态的查询 (Computer.Health.State)，应注意数据库中的状态按编号显示。使用下表创建搜索条件。例如，要针对健全性为“未知”的计算机创建搜索条件，请使用操作符“NOT EXIST”（不存在）。

| 健全性条件 | 操作符 |
|---|---|
| 未知 | NOT EXIST |
| 正常 | 2 |
| 警告 | 3 |
| 严重 | 4 |

# 第 2 步：选择要显示的属性（必需的）

在第 2 步中，选择最有助于确定查询结果中返回的计算机的属性。例如，如果希望搜索结果有助于找到所有符合第 1 步中设置的搜索条件的计算机，则可以指定以下属性：如每台计算机的显示名称 (Computer.DisplayName) 或 IP 地址 (Computer.Network.TCPIP.Address)。

以下步骤在**编辑查询**页中执行。

**选择要显示的属性**

1. 在**第 2 步**中，单击**编辑**。此时将显示一个窗口，其中列出了数据库中当前所存在的所有清单数据。

2. 展开此列表，选择要显示在查询结果列表中的属性。请记住，要选择那些有助于确定查询中返回的客户端的属性。如果找不到要显示的属性，您可以在 自定义属性对话框中添加属性。但是，必须在这些属性出现在查询对话框中之前将这些属性指定给机器。

   **注意：**如果您使用的是 Oracle 数据库，务必要至少选择一个由清单扫描器自己定义的属性（如 Computer.Display Name、Computer.Device Name、Computer.Device ID、Computer.Login Name 等等）。

3. 选定属性后，单击 >> 将它移至窗口右侧的空白字段。如果要列举查询结果列表，可单击**包括计数**。
4. 如果要添加更多属性，请重复上述过程。使用箭头按钮添加或删除属性，然后单击**向上移动/向下移动**可更改属性顺序。
5. 单击**使结果可命中**来启用查询结果为所指定的任何操作的可命中目标。
6. 操作完成后，单击**确定**。

也可以在查询结果列表中添加列标题。

**更改列标题（可选）**

1. 在**第 2 步**中，单击**编辑**。
2. 在底部框中，单击列标题，然后单击**编辑**。编辑标题，然后按 Enter 键。如有必要请重复此步骤。
3. 单击“确定”。

此时，您可能想保存查询。查询创建过程的下一步是可选的，它只适用于查询多列的结果。要保存您的查询，请单击页面顶部的**保存查询**。此时将出现一个窗口，提示您键入查询名称。键入名称后单击窗口右上角的**保存**。

# 第 3 步：按属性排序结果（可选）

只有当在第 2 步中定义了多个属性和列标题，并且现在想要在某一列中按字母顺序或数字顺序对结果进行排序时，才需要执行此步骤。

例如，假设您指定了在查询结果中显示两个不同的属性：每个返回的计算机的 IP 地址和处理器类型。在第 3 步中，可以按处理器类型的字母顺序对结果进行排序。

如果跳过此步骤，查询将自动按照第 2 步中选择的第一个属性排序。

**按属性排序结果**

1. 在**第 3 步**中，单击**编辑**。将出现一个窗口，显示您在**第 2** 步中选择的属性。
2. 选择您要作为排序依据的属性，然后单击 >> 将其移至空文本框。
3. 单击“确定”。

# 第 4 步：运行查询

创建查询后，您可以运行、保存查询或将它清除掉再重新创建。

要保存查询供将来使用，请单击**保存**工具栏按钮。该查询将立即显示在**自定义查询**页的列表中。如果当前查询是通过修改另一查询得到的，请单击**另存为**工具栏按钮为其指定新名称。

默认情况下，只有保存查询的用户能看到已保存的查询。如果保存之前选中了**公共查询**，则所有用户都能看到已保存查询。仅具有公共查询管理权限的管理员可以进行公共查询。

如果您安装了多个系列产品，则产品之间将共享查询。如果在一个产品的控制台保存了查询，则该查询也将显示在其他产品的控制台中。

要查看查询结果，请单击**运行**工具栏按钮。

要从**编辑查询**页中清除查询参数，请单击**清除**工具栏按钮。如果查询已保存，则会从此页中清除该查询，但它仍会保留在**自定义查询**列表中。

# 查看查询结果

查询结果符合您在查询构建过程中指定的搜索条件。如果查询结果不是所需内容，可返回**编辑查询**页优化搜索条件。

要展开以获得有关查询结果列表中某台设备的详细信息，请双击查询数据，或者右击然后单击结果菜单中的**查看计算机**。

在**查询结果**页上，可以单击**另存为 CSV** 工具栏按钮，将查询结果导出到与电子表格和其他应用程序兼容的格式。

要打印查询结果，请在查询结果页面中单击**打印视图**。

# 查看展开查询结果

查询结果符合您在查询构建过程中指定的搜索条件。如果查询结果不是所需内容，可返回**编辑查询**页优化搜索条件。

要展开以获得有关查询结果列表中某台设备的详细信息，请双击查询数据，或者右击然后单击结果菜单中的**查看计算机**。

# 将查询结果导出至 CSV 文件中

要使用电子表格应用程序查看查询的结果，请将数据导出为逗号分隔值 (CSV) 文件。在**查询结果**页面中，单击**另存为 CSV** 工具栏图标，将信息另存为 CSV 文件。然后就可以使用 Microsoft Excel* 之类的应用程序来导入并处理该 CSV 文件。

# 更改查询列标题

1. 打开现有查询或新建查询。
2. 在底部框中，单击列标题，然后单击**编辑**。编辑标题，然后按 Enter 键。如有必要请重复此步骤。
3. 单击“确定”。

# 导出和导入查询

可以导出和导入创建的查询。所有查询均导出为 XML 文件。如果多次导出同一查询文件名，则现有文件将被覆盖。为避免出现这种情况，可以在文件导出后将其复制到另一个位置。

在以下两种情况中，可借助导出和导入功能。

- 如果需要重新安装数据库，可以使用导出/导入功能来保存现有查询，以备在新数据库中使用。

  例如，可以导出查询，然后将它们移到不受重新安装数据库影响的目录中。重新安装数据库后，可以将这些查询移回 Web 服务器上的查询目录下，然后再将它们导入新数据库。
- 可以使用导出/导入功能将查询复制到其他数据库中。

  例如，可以将查询导出至 Web 服务器的查询目录中，然后通过电子邮件或 FTP 传送给其他人。随后，他就可以将这些查询放到另一台 Web 服务器的查询目录下，再将它们导入到另外一个数据库。也可以映射驱动器，直接将查询复制到另一台 Web 服务器的查询目录下。

**导出查询**

要导出查询，先连接到包含要导出的查询的数据库，然后执行以下步骤。

1. 在左侧导航窗格中，单击**查询**。
2. 在**自定义查询**页面中，单击要导出的查询名称。单击**编辑**。
3. 在**编辑查询**页面中，单击**导出**工具栏按钮将查询导出至磁盘。
4. 在**已导出查询**页面中，右键单击查询，将其作为 XML 文件下载到选定的目录中。查询变成 XML 文件。

注意，如果多次导出同一查询文件名，则现有文件将被覆盖。为避免出现这种情况，可以在文件导出后将其复制到另一个位置。

如果最终要将查询导入回数据库中，则必须将其移到 Web 服务器可以识别的查询目录中，默认情况下为 c:\inetpub\wwwroot\LANDesk\LDSM\queries。

### 导入查询

要导入查询，先连接到要将查询导入的数据库，然后执行以下步骤。

1. 在左侧导航窗格中，单击**查询**。
2. 在**自定义查询**页面中，单击**新建**。
3. 在**编辑查询**页面中，单击**导入**工具栏按钮。
4. 选择要导入的查询。如果要在导入之前验证该查询的参数，单击**查看**。
5. 单击**导入**将查询加载到**编辑查询**页面中。
6. 查询加载完毕后，向下滚动并单击**保存查询**将其保存在该数据库中。

# 清单管理

使用清单扫描实用程序向核心数据库添加设备，并收集设备的硬件和软件数据。您可以查看、打印和导出清单数据。还可以使用它来定义查询，对设备进行分组，以及生成专门报告。

阅读本节后，您将了解以下内容：

- 清单扫描概述
- 查看清单数据

# 清单扫描概述

如果使用设备安装功能对设备进行配置，清单扫描器便是安装在设备上的组件之一。当创建客户端配置时，可以指定清单扫描器在设备上运行的时间。

第一次配置设备后，清单扫描器将自动运行。扫描器可执行文件的名称为 LDISCAN32.EXE（对于 Windows）和 LDISCAN（对于 Linux）。清单扫描器收集硬件和软件数据，并将这些数据输入核心数据库。随后，设备每次启动时将运行硬件扫描，而软件扫描仅按指定的时间间隔运行。要配置软件扫描设置，请在核心服务器上单击**开始|程序文件| LANDesk | LANDesk 配置服务**。

有关配置清单服务的详细信息，请参阅附录 C 中的“配置清单服务”。

进行第一次扫描后，可以将清单扫描器作为计划任务从控制台运行。必须在远程设备上运行标准管理代理，以便对这些设备安排进行清单扫描。

**注意：**通过搜寻功能向核心数据库添加设备时，该设备的清单数据并未扫描到核心数据库中。必须在每个设备上运行清单扫描，才能显示该设备的完整清单数据。

您可以查看清单数据，并使用它们来完成以下操作：

- 自定义**所有设备**列表列来显示特定清单属性
- 在核心数据库中查询具有特定清单属性的服务器
- 对设备进行分组，以加速执行管理任务
- 基于清单属性生成专门报告
- 跟踪设备上的硬件和软件更改，并在发生此类更改时生成警报或日志文件条目。

阅读以下各节可了解有关清单扫描器工作方式的详细信息。

## 增量扫描

在设备上初次运行完全扫描后，随后运行的清单扫描器将只捕获增量更改，并将这些更改发送到核心数据库。使用扫描器选项 /RSS 从 Windows 注册表中收集软件信息。

## 强制完全扫描

如果要强制对设备的硬件和软件数据进行完全扫描，则可以删除现有的 delta 扫描文件，并更改**配置 LANDesk 软件服务**小程序中的设置。

1. 删除服务器上的 **invdelta.dat** 文件。最新清单扫描数据的副本将以隐藏文件形式存储在本地硬盘驱动器的根目录下，文件名为 invdelta.dat。（LDMS_LOCAL_DIR 环境变量指定该文件的位置。）
2. 在清单扫描器实用程序的命令行中添加 **/sync** 选项。要编辑命令行，请单击**开始|所有程序|LANDesk 管理**，右击**清单扫描**快捷方式，选择**属性|快捷方式**，然后编辑**目标**路径。
3. 在核心服务器中单击**开始 | 所有程序 | LANDesk | LANDesk 配置服务**。
4. 单击**清单**选项卡，然后单击**高级设置**。
5. 单击 **Do Delta** 设置。在**值**框中，键入 **0**。
6. 连续单击两次**确定**，然后单击提示符上的**是**重新启动该服务。

## 扫描压缩

默认情况下，Windows 清单扫描器 (LDISCAN32.EXE) 执行清单扫描时将压缩扫描结果。扫描器按大约 8:1 的压缩比来压缩完全扫描和增量扫描的结果。首先在内存中生成完整的扫描数据，然后将数据压缩成一个较大的数据包并传输到核心服务器。扫描压缩可减少数据包的数量，从而减少带宽占用量。

## 扫描加密

可以对清单扫描进行加密（仅限 TCP/IP 扫描）。通过更改 LANDesk 配置服务小程序中的设置可以禁用清单扫描加密。

1. 在核心服务器中单击**开始 | 所有程序 | LANDesk | LANDesk 配置服务**。
2. 单击**清单**选项卡，然后单击**高级设置**。
3. 单击 **Disable Encryption** 设置。在**值**框中，键入 **1**。
4. 单击**设置**，然后单击**确定**。
5. 单击**确定**，然后单击提示符上的**是**重新启动该服务。

# 查看清单数据

一旦清单扫描器扫描了设备，您就可以在控制台中查看设备的系统信息。

设备清单存储在核心数据库中，其内容包括硬件、设备驱动程序、软件、内存和环境信息。这些清单数据有助于您管理和配置设备，并快速识别系统问题。

可以通过以下方法查看清单数据：

- 清单一览表
- 完整清单

- 查看属性的特性
- 系统信息

还可以在生成的报告中查看清单数据。有关详细信息，请参阅“报告概述”。

## 从服务器信息控制台查看清单一览表

清单一览表位于服务器信息控制台的**一览表**页面上，用于快速查看设备的基本操作系统配置和系统信息。

**注意：**使用搜寻工具向核心数据库添加设备时，该设备的清单数据并未扫描到核心数据库中。必须在服务器上运行清单扫描才能成功实现清单一览表功能。

**查看清单一览表**

1. 在控制台的**所有设备**视图中，双击一个设备。
2. 在左侧导航窗格中，单击**系统信息**，然后单击**系统一览表**。

### Windows 2000/2003 服务器汇总数据

当您查看 Windows 2000/2003 服务器的清单一览表时，将显示以下这些信息。

- **健全性：**服务器当前的健全性状态。
- **类型：**服务器的类型，例如：应用程序、文件、电子邮件等。
- **制造商：**服务器制造商。
- **型号：**服务器的型号类型。
- **BIOS 版本：**ROM BIOS 的版本。
- **操作系统：**服务器上运行的 Windows 或 Linux 操作系统：2000、2003 或 Red Hat。
- **操作系统版本：**服务器上运行的 Windows 2000/2003 或 Linux 操作系统的版本号。
- **CPU：**服务器上运行的一个或多个处理器的类型。
- **漏洞扫描器：**已安装的代理的版本。
- **清单扫描器：**已安装的代理的版本。
- **监控：**已安装的监控扫描器的版本
- **上次重启时间：**服务器上次重启的时间。
- **CPU 使用：**当前处理器的使用率百分比。
- **使用的物理内存：**服务器上的可用 RAM 数量。
- **使用的虚拟内存：**服务器的可用内存数量，包括 RAM 和交换文件内存。
- **使用的驱动器空间：**驱动器空间当前的使用率百分比。如果硬盘驱动器不止一个，则会列出所有驱动器。

已启用 IPMI 的服务器将显示附加的 IPMI 详细数据。Linux 服务器也将在**一览表**视图中显示类似的信息。

## 查看完整清单

完整清单提供设备的详细硬件组件和软件组件的完整列表。此列表包含对象和对象属性。

**查看完整清单**

1. 在控制台的**所有设备**视图中，单击一个设备。
2. 在**属性**选项卡中，单击**查看清单**。

## 查看属性的特性

您可以从清单列表中查看设备清单对象的属性特性。属性特性可提供清单对象的特征和值。您还可以创建新的自定义属性和编辑用户定义的属性。

要查看属性的特征，请在左侧窗格中单击该属性。

要在 Internet Explorer 中打印此信息，请在框中单击右键，然后单击**打印**。要在 Mozilla 中打印，请在框中单击右键，然后单击**本图文框|将图文框另存为**，再单击**保存**，随后在应用程序中打开文件并单击**打印**。

## 系统信息

从服务器信息控制台，可以查看和修改设备的系统信息。**硬件**、**软件**、**日志**和**其他**类别的信息为存储的数据或实时数据。单击信息链接时，可以查看所选组件的详细信息，而且在适当的情况下，还可以设置阈值并输入信息。

1. 在控制台的**所有设备**视图中，双击一个设备。
2. 在服务器信息控制台的左侧导航窗格中，单击**系统信息**。
3. 展开组，然后单击要查看的信息链接。

# 自定义清单选项

控制台包括一个“配置服务”实用程序，您可以使用该程序来自定义清单选项。大多数选项可以采用默认设置，但如果需要更改默认设置，可以运行该实用程序。要启动“配置服务”小应用程序，请在核心服务器上单击**开始|程序文件| LANDesk | LANDesk 配置服务**。（该实用程序的文件名为 svccfg.exe。）

使用“配置服务”实用程序来配置：

- 数据库名、用户名和密码
- 设备软件扫描时间间隔、维护、保持清单扫描的天数以及客户端登录历史记录的长度
- 重复设备 ID 的处理方式
- 调度程序配置，包括调度的作业和查询评估时间间隔
- 自定义作业配置，包括远程执行超时

有关详细信息，请单击“配置服务”实用程序中各个选项卡的**帮助**。

# 编辑 LDAPPL3.TEMPLATE 文件

与扫描器的清单参数相关的特定信息都包含在 LDAPPL3.TEMPLATE 文件中。此模板文件使用 LDAPPL3.INI 文件来标识设备的软件清单。此文件作为代理配置的一部分放置在受管的 Windows 设备上。其参数可在 代理配置的清单选项卡中设置。

在 Linux 设备上，类似的配置文件 (/etc/ldappl.conf) 包含有关扫描器参数的信息。可以编辑此文件，更改扫描器的操作方式。此文件包含有关如何修改 Linux 扫描器操作的说明。

您可以编辑该模板文件的 [LANDesk Inventory] 部分，配置相应的参数来确定扫描器如何识别软件清单。默认情况下，LDAPPL3.TEMPLATE 文件位于核心服务器的 LDLogon 共享目录下。

下表可以指导您在文本编辑器中对 [LANDesk Inventory] 部分进行编辑。

| 选项 | 说明 |
| --- | --- |
| Mode | 确定扫描器在设备上扫描软件的方式。默认设置为 Listed。具体设置如下：<br><br>• **Listed:**记录在 LDAPPL3 中列出的文件。<br>• **Unlisted:**记录其扩展名已在 ScanExtensions 行中列出，但未在 LDAPPL3 中定义的所有文件的名称和日期。此模式可帮助您搜寻网络上的未授权软件。<br>• **All:**搜寻列出的文件和未列出的文件。 |
| Duplicate | 重复记录文件。如果将该值设置为 OFF，将只记录一次；如果设置为 ON，则所有检测到的文件都会记录。默认设置为 ON。 |
| ScanExtensions | 设置要扫描的文件扩展名（.EXE、.COM 和 .CFG 等）。各个文件扩展名之间用空格隔开。默认情况下只扫描 .EXE 文件。 |
| 版本 | LDAPPL3 文件的版本号。 |
| Revision | LDAPPL3 文件的修订号，可帮助您确保其未来兼容性。 |
| CfgFiles 1-4 | 记录所指定的文件的日期、时间、大小和内容。如果要排除所有本地驱动器，您可以省去驱动器盘符（如 c:）。在这四行中的每一行都可以指定多个文件，但每行的长度不能超过 80 个字符。<br><br>同一行上的各个路径名之间用空格隔开。 |

| 选项 | 说明 |
| --- | --- |
| | 扫描器会将当前文件的日期和大小与上一次的扫描数据进行比较。如果日期和大小与上次的扫描数据不匹配，则扫描器会将文件内容作为新的修订版本予以记录。 |
| ExcludeDir 1-3 | 将特定的目录排除在扫描范围之外。如果要排除所有本地驱动器，您可以省去驱动器盘符（如 c:）。枚举必须从 1 开始并且必须是连续的。每行必须用“\”结尾。 |
| MifPath | 指定 MIF 文件在客户端本地驱动器上的存储位置。默认位置为 c:\DMI\DOS\MIFS。 |
| UseDefaultVersion | 如果将其设置为 TRUE，当某个文件与 LDAPPL3 中某一条目的文件名和文件大小完全匹配时，扫描器会报告文件名匹配（版本报告为 EXISTS）。这样一来，如果这些应用程序与一个未知应用程序共享一个同样的文件名，就会导致不真实的匹配报告。在产品所附的 LDAPPL3.TEMPLATE 文件中，此参数设置为 FALSE；这意味着，如果完全匹配，只添加一个条目。如果未设置此参数，将会默认为 TRUE。 |
| SendExtraFileData | 如果设置为 TRUE，扫描器会将额外的文件数据发送到核心服务器。默认设置为 FALSE。这意味着在默认情况下，只将路径、名称和版本输入到核心数据库中。 |

**编辑 LDAPPL3.TEMPLATE 文件**

1. 在核心服务器上，转到 \Program Files\LANDesk\ManagementSuite\LDLogon 目录，然后在记事本或其他文本编辑器中打开 LDAPPL3.TEMPLATE。
2. 向下滚动文件，找到您想更新的参数，然后进行更改。
3. 保存该文件。

## 更新应用程序列表

应用程序列表 DEFAULTS.XML 中的数据存储在核心数据库中。因为常用软件应用程序的名称和版本号会经常更改，所以 LANDesk 每年都会多次发布一个新的 DEFAULTS.XML（在 LANDesk 软件的以前版本中，此文件被命名为 LDAPPL.INI）。

**更新应用程序列表**

1. 从 http://www.landesk.com/support/downloads 中下载新的 DEFAULTS.XML 或 LDAPPL3.TEMPLATE 文件。选择产品并单击**软件更新**下载该文件。
2. 将文件保存至 LDLOGON 目录。
3. 按照“发布应用程序列表”中的步骤发布新的 LDAPPL3.INI。

## 发布应用程序列表

“发布应用程序列表”包括将 DEFAULTS.XML 的最新应用程序列表导入数据库，然后结合应用程序列表和 LDAPPL3.TEMPLATE 的内容生成最新的 LDAPPL3.INI 文件。\Program Files\LANDesk\ManagementSuite 目录中有一个单独的实用程序 COREDBUTIL.EXE，用于自动执行上述两个步骤。

**要发布应用程序列表**

1. 启动 CoreDBUtil.exe
2. 单击**发布应用程序列表**按钮。

应在修改或下载最新版本的 LDAPPL3.TEMPLATE 或 DEFAULTS.XML 后发布应用程序列表。

# 硬件配置

## Intel AMT 支持

System Manager 支持使用 Intel* 活动管理技术 (Intel* AMT) 的设备，该技术为一种启用远程设备管理的硬件和固件功能。Intel AMT 使用带外 (OOB) 通信访问设备，无需考虑操作系统的状态或设备的供电情况。

本产品的 Intel AMT 支持包括 1 版和 2 版。部署 Intel AMT 2 设备的过程包括 1 版中未发现的一些新功能。有关部署 2 版的详细信息，请参阅 配置 Intel AMT 设备。除非说明，否则本节中的信息对两个版本都适用。

硬件配置工具包括管理 Intel AMT 设备的以下功能：

- 自动生成部署 ID（PID 和 PPS）（2 版）
- 更改受管设备的用户名和密码
- 配置和启用断路器策略（2 版）
- 配置和启用代理存在监控（2 版）

### 管理有/无管理代理的设备

设备配置 Intel AMT 后，即便未安装 LANDesk 代理也能使用有限数量的管理功能。只要设备接入网络并且配有备用电源，它们便可被找到并添加到清单，从而与网络上的其他设备一起得到管理。

如果某一设备有 Intel AMT 但未安装管理代理，则可以使用未管理的设备搜寻对其进行搜寻，并移动至清单数据库，然后在**我的设备**列表中查看。但是，许多 System Manager 管理选项均不可用。这些选项只有在安装 LANDesk 代理后才可用。配置了 Intel AMT 的设备提供的管理功能包括：

- **清单一览表：**即便在设备关闭的情况下仍能实时查询和查看设备的正常清单数据子集。
- **事件日志：**包含特定于 Intel AMT 的事件的日志，其中显示事件严重性和说明，并可实时查看。
- **远程启动管理器：**不考虑设备操作系统或电源，便可从远程管理控制台启动冷开机和若干启动选项。可用的选项基于设备对这些选项的支持。某些设备可能不支持所有启动选项。
- **强制执行漏洞扫描和禁用操作系统网络：**如果设备似乎运行了恶意软件，则会在下次重新启动时运行漏洞扫描；如有必要，将禁用设备操作系统级别的访问以防止有害数据包在网络上传播。

有关管理选项的详细信息，请参阅 管理 Intel AMT 设备。

### Intel AMT 1 版部署要求

只有在访问了设备上的 Intel AMT 配置屏幕并将制造商的默认密码更改为安全密码后，才能将设备作为 Intel AMT 设备搜寻。（有关访问 Intel AMT 配置屏幕的信息，请参阅制造商文档。）如

果您尚未执行此操作，则虽可搜寻到设备，但不会将之标识为 Intel AMT 设备，并且也无法查看到与您这样做时能查看到的相同清单一览表信息。

为了使核心服务器验证搜寻到的 Intel AMT 设备，则用户名/密码凭证必须与您使用“配置服务”实用程序配置的凭证相匹配。您可以使用 Intel AMT 配置屏幕更改凭证。

将 Intel AMT 设备添加到核心数据库进行管理时，System Manager 会以配置服务实用程序中选定的模式自动对该设备进行部署，而不管它是否已经部署。“小型企业”模式提供基本的管理，没有网络基础结构服务，是不安全的；而“企业”模式旨在用于大型企业，使用 DHCP、DNS 以及 TLS 证书授权服务确保受管设备和核心服务器之间安全通信。

当以企业模式部署 Intel AMT 设备时，核心服务器会在该设备上安装证书，用以进行安全通信。如果该设备将由另一个核心服务器管理，必须对设备取消部署，然后由新的核心服务器重新部署。否则，该设备的 Intel AMT 访问将会由于新的核心服务器不具有匹配的证书而无法响应。同样，如果任何其它计算机尝试访问该设备上的 Intel AMT 功能，也将会由于它不具有匹配的证书而导致失败。

# 配置 Intel AMT 设备

首次安装配备了 Intel AMT 功能的设备并打开电源时，应对其进行配置。部署过程包含若干安全措施，确保只有授权用户具有 Intel AMT 管理功能的访问权限。

Intel AMT 设备可以与网络上的部署服务器通信。部署服务器在网络上监听 Intel AMT 设备的消息，允许 IT 人员通过带外通信管理服务器，而不管该设备操作系统所处的状态。System Manager 充当了 Intel AMT 设备的部署服务器，具有有助于您在安装设备时部署设备的功能。然后，您就可以使用或不使用其他 System Manager 管理代理来管理设备。

本部分概述了新的 Intel AMT（版本 2）设备的建议配置过程。在此过程中，您将使用 System Manager 来生成一组部署 ID（PID 和 PPS）。在设备的 Intel AMT 配置屏幕上输入这些 ID 时，可以确保与支持这些 ID 的部署服务器进行安全连接，以便 Intel AMT 设备可以完成它的初始部署过程。

配备了 Intel AMT 1 版的设备采用类似的过程，但不使用 PID 和 PPS 密钥。有关详细信息，请参阅本部分结尾处的注释。

## 部署 Intel AMT 2 设备

收到 Intel AMT 2 设备后，IT 技术人员会组装计算机并打开电源。打开该设备的电源后，技术人员会登录到基于 BIOS 的 Intel ME (Management Engine) 配置屏幕，将默认密码 (admin) 更改为强密码。这样就可以访问 Intel AMT 配置屏幕了。

在 Intel AMT 配置屏幕中，输入了以下预部署信息：

- 部署 ID (PID)
- 预部署密钥 (PPS)，也称为预共享密钥 (PSK)

- 部署服务器的 IP 地址
- 端口 9982 为与部署服务器通信的端口
- 应选择企业模式
- Intel AMT 设备的主机名

PPS 必须为部署服务器和受管设备所知，但为安全起见，无法在网络上进行传输。需要在设备上将其手动输入（在 Intel AMT 配置屏幕上），并存储到部署服务器上。在这种情况下，它也就是 System Manager 的核心服务器。PID/PPS 对由 System Manager 生成，存储在数据库中。您可以打印已生成 ID 对的列表，在部署时使用。

IT 技术人员应输入 System Manager 核心服务器（作为部署服务器）的 IP 地址，并指定端口 9982。否则，默认情况下，Intel AMT 设备会在配置服务器在端口 9971 上监听时发送可以接收的常规广播。

访问 Intel AMT 配置屏幕的默认用户名和密码是“admin”和“admin”。他们会在部署过程中被更改。用户名可以保持不变，但密码必须更改为强密码。在 System Manager 附带的配置服务实用程序中输入新的用户名/密码组合，如下面的步骤中所述。配置完所有设备后，可以单独更改每台设备的用户名/密码，但为了部署目的，要使用配置服务中找到的用户名/密码。

在 Intel AMT 配置屏幕上输入以上信息后，该设备会在首次连接到网络时发送“hello”消息，尝试与部署服务器通信。如果部署服务器收到此消息，部署过程将在服务器与受管设备建立连接时将开始。

核心服务器收到“hello”消息并验证 PID/PPS 密钥时，它会将 Intel AMT 设备部署到 TLS 模式。部署完成时，TLS（传输层安全）模式在核心服务器和受管服务器之间会建立安全的通信渠道。此过程包括用设备的 UUID 和加密凭证在数据库中创建记录。设备的数据在数据库中时，设备显示在未管理设备列表中。

Intel AMT 设备被核心服务器部署后，它只能用 Intel AMT 功能进行管理。可以在未管理设备列表中选择该设备，然后将其添加到受管设备中。也可以将 System Manager 管理代理部署到该设备，以使用更多的管理功能。

使用 System Manager 部署 Intel AMT 2 设备的建议过程如下。第 1 项和第 2 项的详细说明在以下步骤中提供。

1. 运行配置服务实用程序，指定新的强密码，对 Intel AMT 设备进行部署。（请参见下面的详细步骤。）
2. 使用 System Manager 生成一批 Intel AMT 部署 ID（PID 和 PPS），然后打印密钥列表。（请参见下面的详细步骤。）
3. 从 BIOS 登录到设备的 Intel ME 配置屏幕，将默认密码更改为强密码。
4. 登录到 Intel AMT 配置屏幕。从打印的部署 ID 列表中输入 PID/PPS 密钥对。输入核心服务器（部署服务器）的 IP 地址，指定端口 9982。确保已为部署选择企业模式。输入 Intel AMT 设备的主机名。
5. 退出 BIOS 屏幕后，该设备将开始发送“hello”消息。
6. 核心服务器收到“hello”消息，对照已生成密钥列表检查 PID/PPS。如果有匹配，则将设备部署到 TLS 模式。

7. 随即将设备添加到未管理设备搜寻列表中。
8. 选择设备，将其添加到受管设备中。默认情况下，会将该设备作为无代理设备进行管理，也可以对其部署管理代理。

**在配置服务中设置 Intel AMT 用户名和密码**

1. 在核心服务器上，单击**开始**|LANDesk|**配置服务**。
2. 单击 **Intel AMT 配置**选项卡。
3. 键入 **admin**，将其作为**当前 Intel AMT 凭证**下的用户名和密码。
4. 在**使用新的 Intel AMT 凭证部署**下键入新的用户名（可选）和强密码。
5. 单击“确定”。

必须先在此处字段输入用户名和密码，然后才能生成一批部署 ID。

**生成一批 Intel AMT 部署 ID**

1. 在核心服务器上，单击左侧导航窗格中的**硬件配置**。
2. 展开 **AMT**，然后将**部署**逐级展开，找到**生成 AMT ID**。
3. 键入要生成的 ID 数（通常是计划部署的设备数）。
4. 如果要对 PID 使用不同的前缀，则在 **PID 前缀**文本框中键入该前缀。此前缀只能包含 ASCII 字符集中的大写字母字符和数字。一个前缀最多可以输入 7 个字符。
5. 键入批名称，标识此组已生成 ID。
6. 选中**显示生成的 AMT ID**，显示列表中的已生成 ID。如果不选中此框，则会生成 ID 并保存在数据库中，但不在此处显示。
7. 单击**生成 ID**。
8. 生成 ID 后，单击**打印 ID 列表**，打开新窗口，打印 ID 列表。（新窗口中仅显示列表中当前显示的 ID。）使用浏览器的打印功能打印列表。
9. 要查看以前生成的所有 ID，请将**批名称**框留空，然后单击**查看批 ID**。
10. 要查看一批已生成 ID，请在**批名称**文本框中键入批名称，然后单击**查看批 ID**。

可以立即生成任意数量的部署密钥。密钥存储在数据库中，已备将来部署新的 Intel AMT 设备时参考。部署设备并使用部署密钥时，**生成 AMT ID** 页将对已经使用的 ID 进行明暗显示，以便您可以对已使用的 ID 进行跟踪。

添加 PID 前缀是为了您方便将 ID 标识为 PID，但是并不要求您使用前缀。我们建议使用 0-4 个字符。前缀最多可以使用 7 个字符。

要标识若干批部署密钥，请指定批名称。此名称应该是描述性的名称，表示 ID 所代表的设备。例如，您可以为贵公司的每个组织生成批，将这些批命名为“开发”、“市场”、“财务”等等。如果以后希望查看所生成的 ID，则可以键入批名称，单击**查看批 ID** 以查看只含有这些 ID 的列表。

## 强密码

Intel AMT 要求使用强密码以进行安全通信。密码应满足以下要求：

- 长度至少为 8 个字符
- 至少包括一个数字字符 (0-9)
- 至少包括一个非字母数字 ASCII 字符（如 !、&、%）
- 包含大小写拉丁文字符或非 ASCII 字符（UTF+00800 以上）

## 部署过程中的错误

如果输入未正确配对的 PID 和 PPS（即 PPS 应该与不同的 PID 配对），则会在警告日志中看到错误消息，该设备的部署将停止。您需要重新启动该设备，然后在 Intel AMT 配置屏幕上重新输入正确的 PID/PPS 对。

键入 PID 时，如果 Intel AMT 配置屏幕显示错误消息，则表示您键入的 PID 错误。系统会执行校验和，确保 PID 正确无误。

## 搜寻 Intel AMT 1.0 设备

执行设备搜寻扫描时，会搜寻 Intel AMT 1 版设备，将其添加到“Intel AMT”文件夹中的**未管理设备**列表。如果使用安全用户名和密码配置这些设备，替换制造商设置的默认值，则会将这些设备视作 Intel AMT 设备。

在 Intel AMT 配置屏幕上添加安全用户名和密码时，也可以输入部署服务器的 IP 地址，指定端口 9982，与 Intel AMT 2 设备一样。但是，在部署 Intel AMT 1 设备时不使用 PID/PPS 对。如果指定部署服务器的 IP 地址，则核心服务器将充当部署服务器。您可以将该设备作为无代理设备进行管理。

注意：Intel AMT 1 版不使用与 2 版相同的安全级别。Intel 建议在隔离的安全网络上配置 1 版设备。配置完成后，可以将它们移至安全性较低的网络中进行管理。

# 更改 Intel AMT 设备的用户名和密码

部署新的 Intel AMT（版本 1）设备必需有安全的用户名和密码。对要用 System Manager 管理的设备而言，您在 Intel AMT 配置屏幕中输入的用户名和密码应与您在 System Manager 配置服务实用程序中输入的用户名和密码一样。配置服务实用程序中的用户名和密码保存在数据库中，并全局应用于部署 Intel AMT 设备。

Intel AMT 要求使用强密码以进行安全通信。密码应满足以下要求：

- 长度至少为 8 个字符
- 至少包括一个数字字符 (0-9)
- 至少包括一个非字母数字 ASCII 字符（如 !、&、%）
- 包含大小写拉丁文字符或非 ASCII 字符（UTF+00800 以上）

部署完成后，应将定期更改用户名和密码作为 IT 维护的一部分。可以对每台 Intel AMT 设备使用不同的用户名/密码组合，或者将用户名/密码组合应用到多台设备。您在“硬件配置”页中输入

的新用户名/密码组合存储在数据库中，由 System Manager 用来与受管的 Intel AMT 设备进行安全通信。

**更改 Intel AMT 设备的用户名和密码**

1. 在核心服务器上，单击左侧导航窗格中的**硬件配置**。
2. 展开 **AMT**，然后逐级展开，找到**配置**。
3. 在**所有设备**列表中，选择一台或多台要更改用户名和密码的设备。单击工具栏上的**目标**。
4. 在下方的窗格中，键入新用户名，然后键入并确认新密码。
5. 单击**目标设备**，然后单击**应用**。

   对于同一列表中的单台或多台设备，可以选择设备，单击**选定的设备**，然后单击**应用**。

# 配置断路器策略

Intel AMT* 2.0 具有断路器功能，可以在具有 Intel AMT 2.0 功能的设备上实施网络安全策略。您可以使用**硬件配置**工具为受管设备选择并应用断路器策略。

在 Intel AMT 设备上应用断路器策略后，该设备会根据定义的策略过滤收发网络数据包。网络流量与过滤器中定义的警报条件一致时，就会生成警报，该设备的网络访问就会受阻。然后，该设备就会与网络隔断，直到最终针对该策略完成修补步骤。

System Manager 包含可以应用到 Intel AMT 设备的预定义断路器策略。每个策略都包含一组过滤器，用来定义不允许哪一类网络流量以及在流量与过滤器的条件一致时需要采取的相应措施。选择和应用策略的步骤如下：

1. 将一个或多个受管设备设置为目标
2. 选择要应用的断路器策略；根据需要，编辑该策略
3. 将策略应用到目标设备

在受管设备上启用断路器策略时，该设备会监视所有收发网络流量。如果检测到过滤器的条件，就会出现以下情况：

1. 受管设备向核心服务器发送一条 ASF 警报，就会有一个条目添加到警报日志
2. 核心服务器确定违反了哪条策略，并关闭受管设备上的网络访问
3. 将该设备加入断路器修补队列（在**硬件配置**工具中）
4. 为了恢复该设备上的网络访问，管理员会遵循相应的修补步骤，之后会从修补队列中删除该设备；这样就会恢复该设备上的原始断路器策略

以下部分对此过程进行了更加详细的说明。

# 选择和应用断路器策略

System Manager 包含以下可应用到 Intel AMT 2.0 设备的预定义断路器策略。策略是用参数定义的，如端口号、数据包类型以及特定时段内的数据包数量。策略在启用时会在所选设备上的 Intel AMT 中进行注册。策略在受管设备上以 XML 文件格式保存在 CircuitBreakerConfig 文件夹中。

- **BlockFTPSrvr**：此策略禁止流量通过 FTP 端口。在 FTP 端口 21 上收发数据包时会丢失数据包，从而暂停网络访问。
- **LDCBKillNics**：除以下管理端口外，此策略会阻塞所有网络端口上的流量：

| 端口说明 | 号码范围 | 流向 | 协议 |
|---|---|---|---|
| LANDesk 管理 | 9593-9595 | 发送/接收 | TCP、UDP |
| Intel AMT 管理 | 16992-16993 | 发送/接收 | 仅 TCP |
| DNS | 53 | 发送/接收 | 仅 UDP |
| DHCP | 67-68 | 发送/接收 | 仅 UDP |

核心服务器关闭受管设备上的网络访问时，实际是将该策略应用到该设备上了。然后，在将设备从修补队列中删除时，原始策略就会重新应用到该设备上了。

- **LDCBSYNFlood**：此策略会检测到 SYN 大规模拒绝服务攻击：它每分钟只允许收发 10,000 个启用 SYN 标志的 TCP 数据包。超过该数字时，网络访问就会暂停。
- **UDPFloodPolicy**：此策略会检测到 UDP 大规模拒绝服务攻击：在 0 到 1023 之间的端口上，它每分钟只允许收发 20,000 个 UDP 数据包。超过该数字时，网络访问就会暂停。

**选择断路器策略**

1. 单击左侧导航窗格中的**硬件配置**。
2. 单击 **AMT**，然后将树逐级展开，找到 **CB 策略**。
3. 在设备列表中，选择要应用策略的设备（使用 Ctrl 或 Shift 选择多台设备）。
4. 单击工具栏上的**目标**，将设备添加到**目标设备**列表。
5. 在下方窗格中，从下拉列表选择一个策略。
6. 单击**目标设备**，然后单击**应用**。

# 恢复修补队列中设备的网络访问

如果设备的网络访问因断路器策略而暂停，则会将该设备加入修补队列中。它会一直保留在队列中，直到从该列表中删除为止，从而在该设备上恢复当前策略。进行此操作之前，需要解决将设备加入队列中的问题。例如，如果检测到 FTP 流量，则需要验证是否采用了相应的措施来防止设备上的更多 FTP 流量。

**从修补队列中删除设备**

1. 单击左侧导航窗格中的**硬件配置**。
2. 单击 **AMT**，然后将树逐级展开，找到 **CB 修补**。
3. 选择可以恢复原始断路器策略的设备，然后单击**删除**。

# Intel AMT 代理存在配置

Intel* AMT 2.0 配备了一个可以监控受管设备上是否存在软件代理的代理存在安全工具。您可以启用代理存在监控，确保设备上的管理代理连续运行。在代理停止运行时，甚至在其他基于软件的代理无法检测到问题时，发出警报。

System Manager 使用 Intel AMT 代理存在来监控两个代理：标准管理代理及监控服务。在没有正常监控通信的情况下，它非常有用。例如，设备的通信层无法正常工作或者监控代理本身可能已停止运行。默认情况下，代理存在也会监控自身的监控进程，所以如果它停止运行，就会向您发出警报。

代理存在监控是通过配置一个用来监听设备上管理代理的“心跳”信息的计时器实现的，可以验证代理是否正在运行。如果计时器由于未收到心跳信息过期，Intel AMT 就会向核心服务器发送一个警报。

设置代理存在配置时，设备上的代理在 Intel AMT 中注册，将心跳直接发送到 Intel AMT。如果心跳停止，Intel AMT 就会通过设备代理不响应的带外通信向核心服务器发警报。Intel AMT 将平台事件陷阱 (PET) 警报发送到核心服务器，同时提供更改状态的说明。默认情况下，此警报在记录时会同时记录设备健全性情况。可以配置收到此警报时要启动的其他警报操作。（有关配置警报操作的信息，请参阅 配置警报操作）。

配置代理存在监控后，即可启用或禁用两个代理的监控并设置以下值：

- **心跳**：心跳信号之间间隔的最长时间（秒）。如果超出此时间限制，但没有收到新的心跳，则认为代理不响应。标准管理代理的默认值为 120 秒，监控服务的默认值为 180 秒；两者的最小值为 30 秒。
- **启动时间**：操作系统启动后必须从代理收到心跳前间隔的最长时间（秒）。如果超出此时间限制，则认为代理不响应。安装代理时要在 Intel AMT 上配置代理监控，因此应该会留下足够的时间，以便代理开始运行并发送第一个心跳。默认值为 360 秒；最小值为 30 秒。

**编辑 Intel AMT 代理存在配置**

1. 单击左侧导航窗格中的**硬件配置**。
2. 展开 **AMT**，然后将树逐级展开，找到 **AP 配置**。
3. 要在 Intel AMT 2.0 设备上禁用代理存在监控，请清除**启用代理存在监视**复选框。
4. 要对特定代理禁用监控，请清除该代理名称旁边的复选框。（即使这两个复选框都被清除，代理存在只要启用就会继续监控自己的监控进程。）
5. 在**心跳**文本框中键入新值，更改心跳之间允许的最长时间（最小 30 秒）。

6. 在**启动时间**文本框中键入新值，更改在设备上启动操作系统后代理发送第一个心跳允许的最长时间（最小 30 秒；建议 120 秒）。

# IPMI 支持

System Manager 包括对“智能平台管理界面 (IPMI)”1.5 和 2.0 版本的支持。IPMI 是由 Intel、* H-P、* NEC、* 和 Dell* 开发的一种规范，用来为可管理的硬件定义消息和系统界面。IPMI 包含监视和恢复功能，它们允许您访问许多功能，而不论计算机是否开机以及操作系统目前处于何种状态。有关 IPMI 的更多信息，请访问 Intel 的 Web 站点。

IPMI 监控由 BMC（Baseboard Management Controller，底板管理控制器）处理。BMC 依靠备用电源运作，并自动轮询系统健康状态。如果 BMC 检测到任何元件超出范围，您可以配置产生的 IPMI 操作，例如登录事件、生成警报或执行自动恢复操作（如关闭系统电源或重新启动系统）。

要在系统中检测到 BMC，必须在该系统中安装 SMBIOS 2.3.1 或更高版本。如果在系统中未检测到 BMC，您将无法在报告、导出等中看到某些 IPMI 信息。

IPMI 可定义硬件的常用界面，用来监控物理健康特征（例如温度、电压、风扇、电源和机箱开启感应）。除健康监控之外，IPMI 还包括其他系统管理功能，包括自动报警、自动关闭系统和重启系统、远程重启和电源控制功能以及资产跟踪。

依操作系统的状态而定，启用了 IPMI 的设备上的 System Manager 菜单选项也会略有不同。

# 已启动 IPMI 的设备的管理功能

监视能力取决于被监视的设备上安装的内容以及设备的状态。任何安装了底板管理控制器 (BMC) 并启用 IPMI 的设备都可通过管理员控制台以有限的方式来监控，不需要在配置 BMC 后添加管理代理。当设备被关闭或操作系统不能正常工作时，这包括带外管理。如果安装了管理代理、BMC 存在、设备已开机且操作系统工作正常，则可以使用功能全面的管理。下表将可用功能与这些不同的配置进行比较。

| | 仅限 BMC* | BMC + 代理 | 代理（无 IPMI） |
|---|---|---|---|
| 启用带外管理 | X | X | |
| 启用带内管理 | | X | X |
| 可搜寻到设备** | X | X | X |
| 读取环境传感器 | X | X | 与硬件相关 |
| 远程启动/关闭 | X | X | X |
| 读取 & 清除事件日志 | X | X | |
| 配置警报 | X | X | X |
| 读取操作系统信息 | | X | X |
| 延时关机 | | X | X |
| 读取 SMBIOS 信息（处理器、插槽、内存） | | X | X |
| IP 同步（操作系统到 BMC） | | X | |
| 监视计时钟 | | X | |
| BMC 与核心服务器通信 | X | X | |

| | 仅限 BMC* | BMC + 代理 | 代理（无 IPMI） |
|---|---|---|---|
| 本地 System Manager 组件与核心服务器之间通信 | | X | X |
| 全套 System Manager 管理功能 | | X | |

*Standard BMC.小 BMC 是底板管理控制器的精简版本。该版本中提供了上面列出的所有功能，但有以下局限：

- 不支持 serial over LAN (SOL) redirection
- 仅有一个用于 BMC 管理的用户名
- 只使用一个频道与 BMC 通信
- 有一个较小型的系统事件日志 (SEL) 资料档案库

**如果尚未配置 BMC，则无法响应产品用于搜寻 IPMI 的 ASF ping。也就是说，您不得不将其搜寻为普通计算机。部署管理代理时，服务器配置可执行文件将扫描系统、检测它是否 IPMI 并配置 BMC。

## 与其它 IPMI 驱动程序之间的冲突

如果您在希望使用 System Manager 管理的设备上安装了含有 IPMI 驱动程序的其它管理软件，则需要先卸载这些产品，然后才能部署带有 IPMI 管理功能的 Management Suite 代理。

例如，Microsoft* Windows* Server 2003 通过安装 Windows Remote Management (WinRM) 提供 IPMI 支持。WinRM 包括 Windows Management Instrumentation (WMI) 提供程序和 IPMI 驱动程序。但是，System Manager 不支持安装该 IPMI 驱动程序，而是安装自己的 IPMI 驱动程序。如果在希望使用 System Manager 管理的设备上安装了 WinRM，则必须首先通过 Windows“添加/删除程序”卸载 WinRM（**开始|控制面板|添加或删除程序|添加/删除 Windows 组件|管理和监视工具**|清除**硬件管理**复选框|单击**确定**）。

# IPMI BMC 配置

使用 **IPMI BMC 配置**页可以自定义与启用 IPMI 的设备进行通信的设置。如下所述的功能适用于带内设备；如果是带外设备，则只能使用电源配置和 BMC 用户设置。

**注意**：强烈建议您不要更改 IPMI 设置，除非您熟悉 IPMI 规范并了解与这些设置有关的技术。如果这些配置选项使用不当，可能会使 System Manager 无法成功地与启用 IPMI 的设备进行通信。

可以使用下列配置选项：

- 监视计时钟
- 电源配置
- 用户设置

- BMC 密码
- LAN 配置
- SOL 配置
- 更改 IMM 配置

## 更改监视程序计时器设置

IPMI 为 BMC 监视程序计时器提供接口。此计时器可以设置为定时过期，并可以配置为在过期时执行特定操作（例如冷开机）。System Manager 配置为定期重置计时器，使其不会过期；如果设备不可用（例如关闭或挂起），计时器无法重置，因此将会过期，从而执行相应操作。

可以指定允许计时器在多长时间之后过期并选择在过期时要执行的操作。可以选择不采取措施，对设备进行硬重置（关闭和重新启动）、适度给设备断电或进行电源循环（适度断电，然后再次启动）。

也可以设置 BMC，在启用监视程序计时器时停止广播 ARP（地址解析协议）消息，这可以减少生成的网络通信量。如果挂起 ARP，则他们会在监视程序计时器过期时自动恢复。

**更改监视程序计时器设置**

1. 在**我的设备**视图中，双击要配置的设备。
2. 在服务器信息控制台的左侧导航窗格中，单击**硬件配置**。
3. 展开 **IPMI BMC 配置**，然后单击**监视程序计时器**。
4. 选中**打开监视程序计时器**以启用计时器。
5. 指定检查计时器的频率（分钟数或秒数）。
6. 选择在监视程序计时器过期时要执行的操作。
7. 如果希望 BMC 在启用监视程序计时器时停止广播 ARP 消息，选中**暂停 BMC ARP**。
8. 单击**应用**。
9. 如果已更改监视计计时器设置，可以单击**还原默认设置**来恢复默认设置。

## 更改电源配置设置

您可指定支持 IPMI 的计算机停电后，在电源恢复时将执行哪些操作。建议将计算机恢复为停电时的状态，不过也可保持关闭状态或一直接通电源。

**更改电源配置设置**

1. 在**我的设备**视图中，双击要配置的设备。
2. 在服务器信息控制台的左侧导航窗格中，单击**硬件配置**。
3. 展开 **IPMI BMC 配置**，然后单击**电源配置**。
4. 为电源恢复选择一个选项。
5. 单击**应用**。
6. 如果更改了电源配置设置，可以单击**恢复默认值**来恢复默认设置。

# 更改 BMC 用户设置

System Manager 使用对 BMC 唯一的用户名/密码组合（独立于任何其他 System Manager 用户名）向 BMC 验证身份。System Manager 保留第一个用户名，以便始终可以与 BMC 进行通信。如果 BMC 允许定义其他用户名，可以为 BMC 身份验证定义用户名和密码。

也可以为每个用户指定权限级别。对于高级 IMM，可以为每个渠道指定协议权限级别（telnet、http 和 https）。

**注意：**更改设置时应格外小心。错误设置将使设备 BMC 与此产品无法通信。

**更改 BMC 用户设置**

1. 在**我的设备**视图中，双击要配置的设备。
2. 在服务器信息控制台的左侧导航窗格中，单击**硬件配置**。
3. 展开 **IPMI BMC 配置**，然后单击**用户设置**。
4. 要清除用户名的数据，单击索引号，然后单击**清除**。
5. 要添加或更改用户名，请单击索引号，然后单击**编辑**。
6. 键入用户名。
7. 要设置密码，请选中**设置密码**复选框，然后键入密码并予以确认。
8. 选择 LAN 和串行访问使用的权限级别。
9. 单击**保存更改**。

# 更改 BMC 密码

System Manager 使用默认用户名（用户 1）和密码向设备的 BMC 验证身份。您不能更改用户名，但可以更改其密码。更改此密码设置时，更改保存在数据库中和 BMC 上。

**更改默认 BMC 密码**

1. 在**我的设备**视图中，双击要配置的设备。
2. 在服务器信息控制台的左侧导航窗格中，单击**硬件配置**。
3. 展开 **IPMI BMC 配置**，然后单击**密码**。
4. 键入新密码，并予以确认。
5. 单击**应用**。

# 更改 LAN 配置

IPMI 消息除了可以通过设备的系统接口获取之外，还可以直接通过 LAN 接口从 BMC 获取。启用了 LAN 通信后，即使设备关闭，核心服务器仍可以接收 IPMI 特定的警报。只要设备与有效的网络地址建立了物理网络连接，并且设备的主电源保持连通，核心服务器就会保留此通信。

**注意：**如果想设定与 BMC 的 LAN 或串行通信的自定义配置，则在更改设置时应格外小心。错误设置将使设备 BMC 与此产品无法通信。

如果定义了 LAN 渠道，则可以对设备的 BMC 使用默认设置，或更改 IP 地址和网关设置。使用这些选项对 BMC 为每个平台事件陷阱 (PET) 事件发送的 SNMP 陷阱配置目的地。

也可以更改 SNMP 通讯字符串设置，通过 LAN 发送警报。配置这些设置时，必须指定用于 SNMP 验证的 SNMP 通讯字符串。对于每项配置，可以编辑陷阱目标信息以指定陷阱发送的地点和方式以及陷阱的确认与否。

**设置 LAN 通道配置的属性**

1. 在**我的设备**视图中，双击要配置的设备。
2. 在服务器信息控制台的左侧导航窗格中，单击**硬件配置**。
3. 展开 **IPMI BMC 配置**，然后单击 **LAN 配置**。
4. 在 LAN 通信下拉列表中选择**始终可用**，确保始终可以访问 BMC。如果选择**禁用**，则设备处于带外时，您将没有 BMC 的 LAN 访问权限。
5. 选择用于渠道的用户权限级别：**管理员级别**具备所有命令的访问权限，而**用户级别**仅限于只读访问权限（如果选择用户级别，则将具有有限的功能设置）。
6. 选中**永久关闭 BMC ARP**，关闭 BMC 中的“地址解析协议”消息。此操作可以减少网络通信，但在设备处于带外时会阻碍与 BMC 的通信。
7. 选中 **Turn off ARP 响应**阻止 BMC 在操作系统不可用时发送 ARP 消息响应。如果启用此设置，就可能会在设备处于带外时阻止与 BMC 的通信。
8. 如果 BMC 与操作系统通道同步，则 LAN 通道的 IP 设置会自动设置。如果没有自动设置，则会启用 **IP 设置**选项卡下的复选框。您可以选中该框，使用自动提供的 DHCP 设置，或取消选中该框，用静态设置编辑文本字段。通常更愿意使用自动设置。
9. 单击**通过 LAN 发送警报**选项卡配置 SNMP 通讯字符串设置（请参阅下面的详细信息）。
10. 单击**应用**以保存更改。

**更改通过 LAN 发送警报的属性**

1. 打开 **LAN 配置**页（上述步骤 1-3）。
2. 单击**通过 LAN 发送警报**选项卡。
3. 选中**已启用**复选框，启用发送 SNMP 警报。
4. 指定用于 SNMP 验证的 **SNMP 通讯字符串**。
5. 要配置陷阱目的地，请双击索引号打开**属性**对话框。
6. 指定 BMC 发送警报的目标 IP 地址，以及相应的 MAC 地址。
7. 指定重试的次数、重试的频率以及要使用的首选网关。
8. 如果希望确认警报（这会增加生成的网络通信量），则选中**确认警报**复选框。
9. 单击“确定”。
10. 在 LAN 配置页，完成所有设置后单击**应用**。

## 更改 Serial Over LAN (SOL) 配置

使用 SOL (Serial Over LAN) 配置选项自定义用于特殊用途（如将 BIOS POST 消息重定向至串行端口）的串行调制解调器设置。如果需要 BMC 通过调制解调器连接拨出，则必须指定特定调制解调器设置（如初始化字符串和拨号字符串）。

使用串行调制解调器时，可能需要配置设备板的 BIOS 和跳线设置。有关详细信息，请参阅特定设备的文档。

**注意：**如果想设定与 BMC 的 LAN 或串行通信的自定义配置，则在更改设置时应格外小心。错误设置将使设备 BMC 与此产品无法通信。

**更改 SOL 配置设置**

1. 在**我的设备**视图中，双击要配置的设备。
2. 在服务器信息控制台的左侧导航窗格中，单击**硬件配置**。
3. 展开 **IPMI BMC 配置**，然后单击 **SOL 配置**。
4. 选中**启用 Serial-over-LAN 通信**启用 SOL。
5. 选择最小的**用户级别要求激活 SOL**。
6. 选择设备硬件配置相应的 **SOL 会话的波特率**。
7. 单击**应用**。

## 更改 IMM 配置

只有配备了高级 IMM 内插附件卡的 IPMI 设备方能显示 **IMM 配置**页面。使用该页面上的选项可以启用或禁用那些与启用 IMM 的设备相关的协议和功能。在更改这些设置前，请查阅 IMM 制造商文档。

**更改 IMM 配置设置**

1. 在**我的设备**视图中，双击要配置的设备。
2. 在服务器信息控制台的左侧导航窗格中，单击**硬件配置**。
3. 展开 **IPMI BMC 配置**，然后单击 **IMM 配置**。
4. 选中希望启用的协议和功能所对应的选项框，并添加任何必需的设置。可用选项包括：
   - KVM
   - SNMP
   - telnet
   - SMTP 警报
   - HTTP
   - HTTPS
5. 单击**应用**

## 管理 Dell* DRAC 设备

本产品与具有 Dell* DRAC（远程访问控制器）的设备进行了管理集成。DRAC 是一个远程硬件控制器，可以为 Dell 设备上符合 IPMI 标准的服务器管理硬件提供接口。DRAC 具有指定的 IP 地址，用来在设备搜寻和设备管理中识别 DRAC 设备。

可以使用与管理其他符合 IPMI 标准的设备同样的功能管理包含 Dell DRAC 的设备。搜寻到设备并将其添加到受管设备列表中时，该设备与任何其他设备一样得到管理。另外，System Manager 还具有独特的 Dell DRAC 功能。

OpenManage Server Administrator 是 Dell 提供的基于 Web 的控制台，用来管理 Dell DRAC 设备。通常，在浏览器中键入 DRAC 的 IP 地址，以用户名和密码登录，即可访问该设备。用 System Manager 管理 Dell DRAC 设备时，也可以从 System Manager 界面直接打开此实用程序。

另外，使用 System Manager 可以管理用户名和密码，以访问 OpenManager Server Administrator，并在服务器信息控制台中通过此实用程序显示三个日志。

**打开 Dell DRAC 设备的 OpenManage Server Administrator**

1. 在**所有设备**列表上双击设备。
2. 在服务器信息控制台中，展开**硬件**，然后单击 **Dell DRAC**。随即显示设备的 IP 地址及其它标识信息。
3. 单击**启动 Dell DRAC 实用程序**，在新窗口中打开设备的 OpenManage Server Administrator。

## System Manager 中的 Dell DRAC 日志

OpenManage Server Administrator 实用程序的三个日志显示在 System Manager 服务器信息控制台中。

- **Dell DRAC 日志**：查看 Server Administrator 记录的所有事件，如登录活动、会话状态、固件更新状态以及 DRAC 和其他设备组件之间的交互。System Manager 中显示的信息包括事件的严重性、说明以及建议的错误纠正操作。
- **Dell DRAC 命令日志**：跟踪向 Server Administrator 发出的所有命令。它说明谁在什么时候执行了什么命令，包括登录和注销的尝试以及访问错误。
- **Dell DRAC 跟踪日志**：对跟踪网络通信事件的详细信息非常有用，如 DRAC 的警报、寻呼或网络连接。

**查看 Dell DRAC 设备的日志**

1. 在**所有设备**列表上双击设备。
2. 在服务器信息控制台，展开**日志**。
3. 单击 **Dell DRAC 日志**、**Dell DRAC 命令日志**或 **Dell DRAC 跟踪日志**。

## 管理启用 Dell DRAC 的设备的用户名

要访问 OpenManage Server Administrator 界面，可以使用为设备定义的用户名和密码登录。默认 **root** 用户是列表中的第一个用户，无法被删除，但可以更改它的密码。最多可以再添加 15 个用户。DRAC 用户名可以有不同的访问级别，System Manager 只定义管理员级别的用户名。

**添加或编辑启用 DRAC 的设备的用户名和密码**

1. 在**所有设备**列表上双击设备。
2. 在服务器信息控制台中，单击**硬件配置**。
3. 在硬件配置控制台中，展开 **Dell DRAC 配置**，然后单击 **Dell DRAC 用户**。随即显示当前定义的用户的列表。
4. 要更改用户密码，请单击用户编号，然后单击**更改密码**。键入并确认新密码，然后单击**应用**。（要将同一密码分配给多个用户，请使用 Ctrl 或 Shift 进行选择。）
5. 要添加用户，请单击**添加用户**。键入用户名和密码，并确认该密码，然后单击**应用**。随即将该用户添加到列表中。

   **注意：**如果键入列表中已经存在的用户名，则指定的新密码将覆盖该用户名的现有密码；同名的另一个用户不会被添加到该列表中。

6. 要删除用户，请单击该用户的编号，然后单击**删除用户**，然后单击**确定**。（要删除多个用户，请使用 Ctrl 或 Shift 进行选择。）

此列表中的所有用户都有访问 OpenManage Server Administrator 的管理员级别权限。

# 核心数据库安装和维护

## 核心数据库安装

此产品的默认安装会在核心服务器上安装 Microsoft MSDE 数据库。这是 System Manager 可用的数据库唯一选项，并且只能安装一个核心数据库。应该将该数据库安装在独立的服务器上。

数据库架构支持 Microsoft SQL Server 2000 with SP4。所有数据库服务器都需要安装 MDAC 2.8。

在核心服务器上安装的数据库必须是全新的数据库。如果在以前安装 LANDesk® Management Suite 或 Server Manager 的服务器上安装 System Manager，则无法使用 System Manager 安装版本的现有数据库结构。

LANDesk 配置服务实用程序包含一个界面，可用于配置各种服务。此实用程序中的“常规”选项卡显示了当前服务器名称、数据库名称以及访问核心数据库所需的用户名/密码。这些凭证可供所有访问核心数据库的服务使用。由于 System Manager 只能使用一个核心数据库，因此不需要更改服务器或数据库名称。如果需要，可以更改凭证。有关详细信息，请参阅 附录 C：配置服务。

# 附录 A：系统要求和端口使用

核心服务器必须具备一个静态的 IP 地址。



## Administrative Core

Administrative Core 支持以下操作系统：

- Microsoft Windows 2000 Server（已安装 SP4）
- Microsoft Windows 2000 Advanced Server（已安装 SP4）
- Microsoft Windows 2003 Server Standard Edition（已安装 SP1）
- Microsoft Windows 2003 Server Enterprise Edition（已安装 SP1）

## 服务器支持（代理）

- Microsoft Windows 2000 Server（已安装 SP4）
- Microsoft Windows 2000 Advanced Server（已安装 SP4）
- Microsoft Windows 2000 Professional（已安装 SP4）
- Microsoft Windows 2003 Server Standard Edition x86（已安装 SP1）
- Microsoft Windows 2003 Server Standard x64 Edition（已安装 SP1）
- Microsoft Windows 2003 Server Enterprise Edition x86（已安装 SP1）
- Microsoft Windows 2003 Server Enterprise x64 Edition（已安装 SP1）
- ~~Microsoft Windows XP Professional（已安装 SP2）~~
- ~~Microsoft Windows XP Professional x64（已安装 SP2）~~
- Windows Small Business Server 2000（已安装 SP4）
- Windows Small Business Server 2003（已安装 SP1）
- Red Hat Enterprise Linux v3 (ES) 32 位 - U6
- Red Hat Enterprise Linux v3 (ES) EM64t - U6
- Red Hat Enterprise Linux v3 WS 32 位 - U6
- Red Hat Enterprise Linux v3 WS EM64t - U6
- Red Hat Enterprise Linux v3 (AS) 32 位 - U6
- Red Hat Enterprise Linux v3 (AS) EM64t - U6
- Red Hat Enterprise Linux v4 (ES) 32 位 - U2
- Red Hat Enterprise Linux v4 (ES) EM64t - U2
- Red Hat Enterprise Linux v4 (AS) 32 位 - U2
- Red Hat Enterprise Linux v4 (AS) EM64t - U2
- Red Hat Enterprise Linux v4 WS 32 位 - U2

- Red Hat Enterprise Linux v4 WS EM64t - U2
- SUSE* Linux Server 9 ES 32 位 SP2
- SUSE Linux Server 9 EM64t SP2
- SUSE Linux Server 10 ES 32 位
- SUSE Linux Server 10 EM64t
- SUSE Linux Professional 9.3
- SUSE Linux Professional 9.3 EM64t
- HP-UX 11.1
- Unix AIX

## 浏览器

- Microsoft Internet Explorer 6.x（已安装 SP1）
- Mozilla 1.7 及更新的版本
- Firefox 1.5 及更新的版本

## 数据库

- MSDE（已安装 SP4）

## Microsoft 数据访问组件

- MDAC 2.8 或更新的版本

如果您希望让多个 LANDesk 管理产品使用同一数据库，则必须在同一“核心”计算机上安装这两个产品。相应地，如果您希望将多个产品安装在同一“核心”计算机上，则必须使用同一数据库。如果两个产品使用同一数据库，那么这两个产品的版本也必须是 8.70。

## 端口使用

## 简介

在装有防火墙（或过滤通信量的路由器）的环境中使用此产品时，可能需要调整防火墙或路由器配置，以保证产品正常运行。本节描述了各个产品组件使用的端口。此处着重讨论了配置路由器和防火墙时所需的信息，暂不考虑仅在本地使用的端口（在单个子网内）。

## 防火墙规则的背景信息

此信息用于设置防火墙规则。如果您不熟悉该主题,则本节提供了一些有关主要概念的一般背景信息。

## 防火墙规则

“打开一个端口”不是一个精确的术语。您不能直接打开防火墙软件然后“打开端口 x”。“打开一个端口”是设置一个防火墙规则的一种简写。防火墙规则描述了允许或不允许何种通信量通过防火墙。防火墙规则并非仅按端口号过滤通信量。可以根据协议、源端口号和目标端口号、方向（入网/出网）、源 IP 地址和目标 IP 地址以及其他方面来设置规则。

典型的防火墙规则如下所示：“允许 TCP 端口 9535 上有入网通信量”。为使用本产品，需要该规则来支持远程控制。该规则基于三个元素：

1. 协议（TCP 或 UDP）
- 端口号
- 方向（入网或出网）

这三个元素是设置防火墙规则所必需的。

## 源端口和目标端口、动态端口

TCP 或 UDP 通信中始终包含两个端口。任何 TCP 或 UDP 程序包都是从源端口发送到目标端口。防火墙规则是基于源端口、目标端口或根据这两个端口设置的。文档中列出的端口（如该端口）始终是目标端口。

熟知的端口（如 5007，由清单服务使用）指通信的一端。通信的另一端使用动态端口。动态端口由操作系统在 1024-5000 的范围内自动分配。

## 防火墙和 UDP 通信量

要允许 TCP 通信量通过防火墙，只设置一个规则即可，例如允许入网 TCP 连接到端口 5007。一旦建立了 TCP 连接，数据便可通过连接双向流通。

因为 UDP 通信量是无连接的，因此有所不同。例如，默认情况下，核心服务器在开始任务之前会在 UDP 端口 38293“ping”接设备。允许将 UDP 数据包发出到端口 38293 的防火墙规则也会允许从核心服务器向防火墙以外的设备发送数据包，但不允许发送设备的响应数据包。

允许将数据包同时发出和接收到端口 38293 的规则在单独发出和接收数据包时无效，因为只有通信一端在监听熟知的端口。另一端正在使用动态端口。因为核心服务器的外发数据包是从动态端口发送到端口 38293，设备的响应数据包是从端口 38293 发送到相同的动态端口而非端口 38293。要允许进行双向通信，则需要允许 UDP 数据包的源端口或目标端口 = 38293 的规则。通常在企业内部网中才能接受此类规则，但在外部防火墙上则不接受（因为这会允许向所有 UDP 端口发送入网数据包）。

因此，通常认为 UDP 通信量是“不适用于防火墙”的。现在回到示例中，有一个 UDP 端口 38293 的备用端口：TCP 端口 9595。当通过防火墙管理设备时，您可能希望对产品进行配置以使用 TCP 端口。

# 使用的端口

| 端口 | 方向 | 协议 | 服务 |
|---|---|---|---|
| 31770 | 控制台到设备，设备到核心服务器 | TCP | 控制台和设备之间的通信 |
| 9595, 9594 | 控制台到设备 | TCP | 服务器配置 |
| 9595 | 控制台到设备 | UDP | 搜寻 |
| 623 | 控制台到设备 | UDP | ASF、IPMI 搜寻 |
| 5007 | 控制台到设备 | TCP | 清单 |
| 9535 | 控制台到设备 | TCP | 远程控制 |
| 139, 145 | 控制台到设备 | TCP | 文件和打印机共享 |
| 137, 138 | 控制台到设备 | UDP | 文件和打印机共享 |

此产品需要在管理节点之前通过安装的标准管理代理搜寻到这些节点。UDP 端口 9595 用于搜寻。您也可以手动将单个设备添加到控制台，但仍需要设备对 UDP 端口 9595 的“ping”接进行响应。在控制台和设备之间的通信使用的是 TCP 端口 31770 和 6787。此后端口上的通信量都是基于 HTTP 的。UDP 端口 623 用于 ASF（alert standard forum，警报标准论坛）搜寻。另外，此产品使用 TCP 端口 9535 进行远程控制。IPMI 搜寻是一个与 ASF 链接的搜寻并使用相同的端口(udp/623)。

# 附录 B：激活核心服务器

在使用控制台前，必须先使用“核心服务器激活”实用程序激活核心服务器。通常该操作只需执行一次，但如果您购买了其他的许可证，则可能需要重复激活。使用核心服务器激活实用程序：

- 第一次激活新的服务器。
  更新现有的核心服务器或升级到 Management Suite 或 Server Manager。
  激活具有 45 天试用许可证的新服务器。

通过单击**开始|所有程序|LANDesk|核心服务器名称激活**启动该实用程序。如果您的核心服务器没有 Internet 连接，请参阅本节后面的“手动激活核心或验证节点数数据”。

每个核心服务器必须有一个唯一的授权证书。多台核心服务器不能共享同一授权证书，尽管它们可以向同一 LANDesk 帐户验证节点数。安装 System Manager 后，此实用程序会在第一次重新启动时自行运行。

核心服务器会定期在“\Program Files\LANDesk\Authorization Files\LANDesk.usage”文件中生成节点数验证信息。并将此文件定期发送到 LANDesk Software 授权服务器上。此文件是 XML 格式的，并被数字签名和加密。任何对此文件进行的手动更改都将使其内容和下一次向 LANDesk Software 授权服务器发送的使用情况报告无效。

核心服务器通过 HTTP 与 LANDesk Software 授权服务器通信。如果您使用代理服务器，请单击该实用程序的**代理**选项卡并输入您的代理信息。如果您的核心服务器有 Internet 连接，则与授权服务器之间的通信是自动的，不需要任何手动操作。如果未连接核心，请在重新启动时单击**关闭**，并通过电子邮件将授权文件发送到 licensing@landesk.com。

“核心服务器激活”实用程序将不会自动启动拨号 Internet 连接，但是如果您手动启动了拨号连接并运行激活实用程序，该实用程序可以使用拨号连接报告使用情况数据。

如果您的核心服务器没有 Internet 连接，您可以如本节中后面所述，手动验证和发送节点数。

## 使用 LANDesk Software 帐户激活服务器

可以使用完全使用许可激活新的服务器之前，您必须在 LANDesk Software 设置一个帐户，授权您使用所购买的 LANDesk Software 产品和节点数。要激活您的服务器，您将需要帐户信息（联系名称和密码）。如果您没有此信息，请联系您的 LANDesk Software 销售代表。

在从安装产品到激活核心服务器的这段时间内不要更改核心服务器的日期或时间。否则激活操作将失败。您将必须卸载并重新安装产品。

**激活服务器**

1. 单击**开始|所有程序|LANDesk|核心服务器激活**。
- 单击**激活**。

## 使用试用许可证激活服务器

45 天试用许可证使用 LANDesk Software 授权服务器激活您的服务器。一旦 45 天评估期过去，您将无法登录到核心服务器，并且它将停止接受清单扫描，但是您不会丢失软件或数据库中所有现有的数据。在 45 天试用许可期间或之后，您可以重新运行核心服务器激活实用程序并转换为使用 LANDesk Software 帐户的完全激活。如果试用许可证过期，转换为完全使用许可证将重新激活核心。

**激活 45 天评估**

1. 单击**开始|所有程序|LANDesk|核心服务器激活**。
2. 单击**激活此核心以进行 45 天评估**。
3. 单击**评估**。

## 更新现有帐户

更新选项将使用情况信息发送到 LANDesk Software 授权服务器。如果您有 Internet 连接，使用情况数据会自动发送，所以您通常不需要使用此选项发送节点计数验证。还可以使用此选项更改与 LANDesk Software 帐户关联的核心服务器。此选项也可将一个核心服务器从试用许可证转换为完全使用许可证。

**更新现有帐户**

1. 单击**开始|所有程序|LANDesk|核心服务器激活**。
2. 单击**使用您的 LANDesk 联系名称和密码更新此核心服务器**。
3. 输入您想要核心使用的**联系名称**和**密码**。如果您输入了与原来激活核心的用户名密码不同的用户名密码，这会将该核心转换到新的帐户。
4. 单击**激活**。

## 手动激活核心或验证节点数数据

如果核心服务器没有 Internet 连接，核心服务器激活实用程序将无法发送节点计数数据。您将看到一条消息，提示您通过电子邮件手动发送激活和节点计数验证数据。电子邮件激活是一个便捷的过程。当您在核心上看到手动激活消息时，或如果您使用核心服务器激活实用程序并看到手动激活消息，请执行以下步骤。

**手动激活核心或验证节点数数据**

1. 核心提示您手动验证节点数数据时，会在 \Program Files\LANDesk\Authorization Files 文件夹中创建一个名为 ACTIVATE.TXT 的数据文件。将此文件作为电子邮件消息的附件，发送至 licensing@landesk.com。邮件的主题和正文并不十分重要。
2. LANDesk Software 将处理该邮件附件并回复到您发送该邮件的邮件地址。LANDesk Software 消息会提供说明和新附加的授权文件。

3. 将附加的授权文件保存到 \Program Files\LANDesk\Authorization Files 文件夹。核心服务器会立即处理该文件并更新其激活状态。

如果手动激活失败或核心不能处理附加的激活文件，则您复制的授权文件会使用 .rejected 扩展名重命名，并且该实用程序会在 Windows 事件查看器的应用程序日志中记录一个具有更多详细信息的事件。

# 附录 C：配置服务

您可以使用“配置服务”小应用程序为任何核心服务器和数据库配置下列服务：



要启动“配置服务”小应用程序，请在核心服务器上单击**开始|程序文件| LANDesk | LANDesk 配置服务**。

两个按钮显示在选项卡之外：

- **凭证：**打开“服务器凭证”对话框，可以在此对话框中添加可充当首选服务器的设备。要添加设备，请单击**添加**。此操作将打开**用户名和密码**对话框（在下文中描述）。
2. **OSD 验证：**为了创建基于 Windows PE 或 DOS 的预启动环境，您必须能够访问 Windows PE 2005 和 Windows NT 4 安装光盘。在两种镜像环境下，都单击**立即验证**，输入相应光盘的路径，然后单击**确定**。

## 用户名和密码对话框

使用**用户名和密码**对话框提供有关您希望添加的首选服务器的信息。

**输入首选服务器信息**

1. 在“配置服务”小应用程序中，单击**凭证**。
- 在“服务器凭证”对话框中，单击**添加**。
- 输入说明、身份验证信息和 IP 地址范围。
- 单击**测试凭证**以验证信息的有效性。
- 单击**确定**将首选服务器添加到“服务器凭证”对话框。
- **服务器名：**首选服务器的名称。

**用户名：**用于向服务器验证身份的用户名。它必须是一个完全合格的域名（例如，Mydomain\user name）。

**说明：**首选服务器的说明。

**密码：**首选服务器的密码。

**起始 IP 地址：**输入某个地址范围的起始 IP 地址，将首选服务器的使用限制到该地址范围内。起始 IP 地址不能大于结束 IP 地址。起始和结束 IP 地址的前三个八位字节必须匹配，如 10.100.10.1 和 10.100.10.255。

**结束 IP 地址：**输入您要扫描的地址范围的结束 IP 地址。

**添加：**在对话框底部的工作队列中添加 IP 地址范围。
**删除：**从工作队列中删除所选的 IP 地址范围。

# 配置服务选项卡

在配置服务之前，请使用**常规**选项卡指定准备配置此项服务的核心服务器和数据库。

**注意：**必须重新启动核心服务器上的服务，才能使该核心服务器和数据库的任何服务配置更改生效。

## 选择核心服务器和数据库

使用**常规**选项卡，您可以选择核心服务器和数据库，并提供身份验证凭证，从而为该核心服务器配置各项服务。

### 关于“配置服务”对话框：“常规”选项卡

使用此对话框可选择要配置特定服务的核心服务器和数据库。接下来，选择服务选项卡，并为该服务指定设置。

- **服务器名：**显示当前连接的核心服务器的名称。
2. **服务器：**用于输入其他核心服务器的名称及其数据库目录。
3. **数据库：**用于输入核心数据库的名称。
4. **用户名：**用访问核心数据库的身份验证凭证标识用户（在安装期间指定）
5. **密码：**标识用户访问核心数据库所需的密码（在安装期间指定）。
6. **这是 Oracle 数据库：**指明上面指定的核心数据库是 Oracle 数据库。（不适用于 System Manager。）
7. **刷新设置。**恢复过去打开“服务配置”对话框时显示的设置。

## 配置清单服务

使用**清单**选项卡可为使用“常规”选项卡选择的核心服务器和数据库配置清单服务。

### 关于“配置服务”对话框：“清单”选项卡

使用此选项卡可指定下列清单选项：

- **服务器名：**显示当前连接的核心服务器的名称。
- **日志统计信息：**保持核心数据库操作和统计信息的日志。
- **加密数据传输：**使清单扫描器可以通过 SSL 将设备清单数据（来自已扫描的设备）作为加密数据发送回核心服务器。

- **扫描服务器的时间**：指定扫描核心服务器的时间。
- **执行维护的时间**：指定执行标准核心服务器维护的时间。
- **清单扫描结果的保留天数**：设置删除清单扫描记录之前的天数。
- **主所有者登录次数**：设置清单扫描器为确定设备的主所有者而跟踪登录的次数。主所有者是在指定登录次数内登录次数最多的用户。默认值为 5，最大值和最小值分别为 1 和 16。如果所有登录都是唯一的，那么最后登录的用户就是主所有者。一个设备一次只能有一个主所有者。主用户登录数据包括用户的全限定名称以及上次登录的日期，用户名称的格式为 ADS、NDS、域名或本地名称（按此顺序）。
- **高级设置**：打开**高级设置**对话框，在其中可以设置与清单扫描器相关的多种不同的高级设置。要更改设置，请单击该设置，更改**值**文本框中的设置，然后单击**设置**。要查看某个设置的说明，请单击该设置，然后在**说明**框中查看详细信息。
- **软件**：打开**软件扫描设置**对话框，在其中可以配置服务器软件扫描时间和历史记录设置。
- **属性**：打开“选择要保存的属性”对话框，在其中可以选择数据库中存储的清单扫描属性。
- **管理重复项：设备**：打开 配置重复设备名称的处理方式对话框，在其中可以选择选项以删除带重复设备名称、MAC 地址（或两者兼备）的设备（请参阅下面的**重复设备**）。
- **管理重复项：设备 ID**：打开**重复设备 ID**对话框，在其中可以选择唯一标识设备的属性。使用此选项可避免将重复的设备 ID 扫描到核心数据库中（请参阅下面的 配置重复设备 ID 的处理方式）。
- **清单服务状态**：指明该服务在核心服务器上是处于启动状态，还是处于停止状态。
- **启动**：在核心服务器上启动服务。
- **停止**：在核心服务器上停止服务。

## 关于“软件扫描设置”对话框

使用此对话框可配置软件扫描的频率。尽管每次在设备上运行清单扫描器时，都扫描设备的硬件，却只按照此处指定的时间间隔来扫描设备的软件。

- **每次登录时**：每次用户登录时都扫描设备上安装的所有软件。
- **间隔的天数**：只按照指定的时间间隔（以天数计）自动扫描设备的软件。
- **历史记录保存的天数**：指定保存设备清单历史记录的时间。

## 配置重复设备名称的处理方式

使用“重复设备”对话框删除数据库中的重复设备。

1. 在“清单”选项卡中，单击**设备**。
- 在“重复设备”对话框中，单击删除重复设备时要使用的选项，然后单击**确定**。

**删除重复设备的时间：**

- **设备名称匹配**：当数据库中有两个或两个以上设备名称匹配时，删除其中的旧记录。

**MAC 地址匹配**：当数据库中有两个或两个以上 MAC 地址匹配时，删除其中的旧记录。

**设备名称与 MAC 地址全部匹配**：仅当有两个或两个以上设备名称和 MAC 地址（同一记录）全部匹配时，删除其中的旧记录。

## 配置重复设备 ID 的处理方式

由于经常使用映像来配置网络中的设备，因此，在设备中出现重复设备 ID 的可能性也就加大了。通过指定其他设备属性，再将这些属性与设备 ID 结合使用，可以避免这个问题，为设备创建唯一的标识符。例如，设备名、域名、BIOS、总线、协处理器等等都属于这些属性。

利用重复 ID 功能，可以选择用来唯一标识服务器的设备属性。可以指定具体的属性，以及必须缺少其中的多少属性才能指定该设备与其他设备重复。如果清单扫描器检测到重复设备，便会在应用程序事件日志中写入一个事件，以指明重复设备的设备 ID。重复设备 ID 对话框包含以下选项：

- **属性列表：**列出可用来唯一标识设备的所有属性。
2. **标识属性：**显示选定用来唯一地标识某设备的属性。
3. **重复设备 ID 触发器：**
    - **标识属性：**指明只有当设备与多少个属性不相符时，才能认定该设备与另一个设备重复。

    **硬件属性：**指明只有当设备与多少个硬件属性不相符时，才能认定该设备与另一个设备重复。
4. **拒绝重复标识：**令清单扫描器记录重复设备的设备 ID，而且拒绝后来的任何扫描设备 ID 的尝试，并生成新的设备 ID。

**配置重复 ID 的处理方式**

1. 在“配置服务”对话框中，单击**清单**选项卡，然后单击**设备 ID**。
- 从**属性列表**中选择要用来唯一标识某设备的属性，然后单击右箭头按钮，将该属性添加到**标识属性**列表中。您可以添加任意数量的属性。
- 选择只有当某设备与多少个标识属性（和硬件属性）不相符时，才能认定该设备与另一个设备重复。
- 如果希望清单扫描器拒绝重复设备 ID，请选中**拒绝重复标识**选项。

# 配置调度程序服务

使用**调度程序**选项卡可为使用**常规**选项卡选择的核心服务器和数据库配置调度程序服务。您必须拥有执行这些任务的适当权限，包括在受管设备上拥有完全的管理员权限，以允许它们接收 System Manager 分发的程序包。您可以通过单击**更改登录**指定在设备上使用的多个登录凭证。

## 关于“配置服务”对话框：“调度程序”选项卡

使用此选项卡，可查看核心服务器的名称以及先前选择的数据库，并指定下列计划任务选项：

- **用户名：**运行计划任务服务时所使用的用户名。通过单击**更改登录**按钮，即可更改用户名。

    **重试间隔的秒数：**配置了计划任务的重试次数后，此设置将控制计划任务在重试任务之前等待的秒数。

**尝试唤醒的秒数**：为使用 Wake On LAN 而配置计划任务后，此设置将控制计划任务服务等待设备唤醒的秒数。

**查询评估的时间间隔**：指明查询评估之间的时间间隔量，以及计量单位（如分钟、小时、天、周）。

**Wake on LAN 设置**：为了唤醒设备，由计划任务设置、供 Wake On LAN 数据包使用的 **IP 端口**。

**计划服务状态**：指明该服务在核心服务器上是处于启动状态，还是处于停止状态。

**启动**：在核心服务器上启动服务。

**停止**：在核心服务器上停止服务。

**重新启动**：在核心服务器上重新启动服务。

**高级**：打开**高级调度程序设置**对话框，在其中可以修改控制调度程序操作方式的设置。要更改设置，请单击该设置，再单击**编辑**，更改该设置，然后单击**确定**。

## 关于“配置服务”对话框：“更改登录”对话框

使用**更改登录**对话框（单击**调度程序**选项卡中的**更改登录**）来更改默认调度程序登录。您还可以指定当调度程序服务需要在不受管的设备上执行任务时应尝试使用的备用凭证。

要在不受管的设备上安装 System Manager 代理，调度程序服务需要能够使用管理帐户连接至设备。调度程序服务使用的默认帐户是 LocalSystem。LocalSystem 凭证一般用于域外设备。如果设备在域中，必须指定域管理员帐户。

如果您想要更改调度程序服务登录凭证，您可以指定在设备上使用的不同的域级管理帐户。如果您在管理跨多个域的设备，您可以添加调度程序服务可以尝试使用的更多凭证。如果您想要对调度程序服务使用不是 LocalSystem 的帐户，或如果您想要提供备用凭证，您必须指定一个具有核心服务器管理权限的主调度程序服务登录。备用凭证不需要核心服务器管理权限，但它们必须具有对设备的管理权限。

调度程序服务将尝试默认的凭证，然后使用您在**备用凭证**列表中指定的每个凭证，直到成功或尝试完所有凭证。您指定的凭证都被安全加密和存储在核心服务器的注册表中。

您可以对默认调度程序凭证设置以下选项：

- **用户名**：输入默认域\用户名或您想要调度程序使用的用户名。
2. **密码**：输入您指定的凭证的密码。
3. **确认密码**：重新输入密码以确认。

您可以对其他调度程序凭证设置以下选项：

- **添加**：单击将您指定的用户名和密码添加到“备用凭证”列表。
- **删除**：单击以从列表中删除选定的凭证。
- **修改**：单击以更改选定的凭证。

当添加备用凭证时，请指定以下属性：

- **用户名**：输入调度程序所要使用的用户名。

- **域：**输入您指定的用户名的域。
- **密码：**输入您指定的凭证的密码。
- **确认密码：**重新输入密码以确认。

## 配置自定义作业服务

使用**自定义作业**选项卡，可为在“常规”选项卡中选择的核心服务器和数据库配置自定义作业服务。自定义作业的示例包括清单扫描或软件分发。

默认情况下，一旦禁止将 TCP 远程执行作为远程执行协议，自定义作业就会使用标准管理代理协议，而不管它是否被标记为禁用。另外，如果同时启用了 TCP 远程执行和标准管理代理，自定义作业将首先尝试使用 TCP 远程执行，如果没有同时启用这两项，则使用标准产品远程执行。

**自定义作业**选项卡还可以让您选择服务器搜寻的选项。在自定义作业服务可以处理作业之前，它需要搜寻每台服务器的当前 IP 地址。此选项卡使您可以配置服务联系服务器的方式。

## 关于“配置服务”对话框：“自定义作业”选项卡

使用此选项卡可设置下列自定义作业选项：

**远程执行选项：**

- **禁用 TCP 执行：**禁止将 TCP 作为远程执行协议，因此，默认使用 CBA 协议。
- **禁用 CBA 执行/文件传输：**禁止将标准管理代理作为远程执行协议。如果禁用了标准管理代理，而且在设备上又找不到 TCP 远程执行协议，远程执行将失败。
- **启用远程执行超时：**启用远程执行超时，并指定超时之前的秒数。当设备发送检测信号后，触发远程执行超时，但是设备上的作业将处于挂起或循环状态。此设置适用于这两种协议（TCP 或标准管理代理）。该值可介于 300 秒（5 分钟）到 86400 秒（1 天）之间。
- **启用客户端超时：**启用设备超时，并指定超时之前的秒数。默认情况下，TCP 远程执行以 45 秒的时间间隔从设备向设备发送检测信号，直到远程执行完成或超时。当设备不向设备发送检测信号时，便会触发客户端超时。
- **远程执行端口（默认值是 12174）：**TCP 远程执行所使用的端口。如果更改了此端口，也必须在客户端配置中对其进行更改。

**分发选项：**

- **同时分发的目标服务器数 <nn>：**将自定义作业同时分发到的设备的最大数目。

**搜寻选项：**

- **UDP：**选择 UDP 将通过 UDP 使用标准管理代理 ping。大多数 System Manager 组件依赖标准管理代理，所以您的受管设备应安装标准管理代理。这是最快的搜寻方法和默认方法。使用 UDP，您还可以选择 UDP ping **重试次数**和**超时**。

- **TCP**：选择 TCP 会在端口 9595 上使用 HTTP 连接至服务器。此搜寻方法的好处是如果您打开端口 9595，就能够通过防火墙工作，但如果设备不存在，则它将受到 HTTP 连接超时的限制。这些超时值可以为 20 秒或更多。如果大量目标设备不响应 TCP 连接，您的作业在开始之前将需要一段时间。
- **两者**：选择“两者”先使服务尝试使用 UDP 搜寻，然后使用 TCP 搜寻，最后使用 DNS/WINS 搜寻（如果选定）。
- **禁用子网广播**：当选定时，禁用通过子网广播搜寻。
- **禁用 DNS/WINS 查找**：当选定时，如果选定的 TCP/UDP 搜寻方法失败，禁用对每个设备进行名称服务查找。

## 配置多播服务

使用**多播**选项卡，可为在**常规**选项卡中选择的核心服务器和数据库配置多播域代表搜寻选项。

## 关于“配置服务”对话框：“多播”选项卡

使用此选项卡可设置下列多播选项：

- **使用多播域代表**：使用网络视图的**配置 > 多播域代表**组中存储的多播域代表列表。
- **使用高速缓存的文件**：查询每个多播域，以确定谁可能已高速缓存此文件。然后可以使用高速缓存的文件，而无需将文件下载到代表。
- **使用首选域代表之前的高速缓存文件**：更改搜寻顺序，使**使用高速缓存的文件**成为第一个尝试的选项。
- **使用广播**：发送一个子网定向的广播，以查找该子网中可以成为多播域代表的任何设备。
- **日志删除期限（天）：指定**日志中的条目在删除之前将保留的天数。

## 配置 BMC 密码

使用 **BMC 密码**选项卡创建 IPMI 底板管理控制器 (BMC) 的密码。

- 在 **BMC 密码**选项卡的**密码**文本框中输入密码，并在**确认密码**文本框中重新输入密码，然后单击**确定**。

  密码不得长于 15 个字符，每个字符必须是数字 0-9 或大小写字母 a-z。

## 配置 Intel AMT 选项

使用 **Intel AMT 配置**选项卡创建或更改已启用 Intel 活动管理技术的设备上的密码，并查看搜寻 AMT 设备的说明。

## 配置 Intel AMT 密码

1. 输入当前用户名和密码。这些内容必须与 Intel AMT 配置屏幕（可在计算机 BIOS 设置中访问）中配置的用户名和密码相符。
- 要更改用户名和密码，请完成**新 Intel AMT 密码**部分。
- 单击“确定”。此更改将在运行客户端配置时生效。

**注意：**新密码必须是强密码，即该密码

- 长度至少为七个字符
  包含字母、数字和符号
  在第二到第六个字符的位置至少包含一个符号
  与以前的密码明显不同
  不包含姓名或用户名
  不是常用的单词或名称

## 搜寻和部署 Intel AMT 设备

要搜寻 AMT 设备，请在 AMT BIOS 的“Provisioning Server”字段中输入核心服务器的 IP 地址，并使用 9982 端口。有关详细信息，请按**配置服务**中的**帮助**。当搜寻到 Intel AMT 设备并将其移动到**我的设备**列表时，它将使用 TLS 模式自动部署。

# 附录 D：代理安全证书和可信证书

每个核心服务器都有一个唯一的证书和私钥，它是安装程序在您第一次在设备上安装核心服务器时创建的。设备只有在具备与核心服务器匹配的可信证书文件的情况下，才能与这些服务器进行通信。

已安装的私钥和证书文件包括：

- **<keyname>.key：** .KEY 文件是核心服务器的私钥，该文件只驻留在核心服务器上。一旦此密钥泄密，就无法保障核心服务器与服务器之间的通信安全。请保护好此密钥。例如，不要使用电子邮件来传递密钥信息。
2. **<keyname>.crt:**.CRT 文件包含核心服务器的公钥。.CRT 文件是以用户友好的方式显示的公钥内容，您可以从中查看有关该密钥的详细信息。
3. **<hash>.0：**.0 文件是可信证书文件，其内容与 .CRT 文件相同。不过，该文件的命名方式使得计算机能够在包含许多不同证书的目录中迅速找到该证书文件。其名称是证书主题信息的哈希值（校验和）。要确定特定证书的哈希文件名，请查看 <keyname>.CRT 文件。该文件中包含一个 .INI 文件部分 [LDMS]。hash=value 对指示 <hash> 值。

所有密钥都存储在核心服务器上的 \Program Files\LANDesk\Shared Files\Keys 目录中。<hash>.0 公钥也存在于 LDLOGON 目录中，该目录为它的指定默认目录。<Keyname> 是您在安装核心服务器时提供的证书名称。在安装时最好提供描述性的密钥名称，如使用核心服务器的名称（甚至使用其全限定名称）作为密钥名（例如：ldcore 或 ldcore.org.com）。这样，在多核心服务器的环境中更易于识别证书/私钥文件。

## 在核心服务器之间备份和恢复证书/私钥文件

安装核心服务器时，安装程序会创建一个新的证书。如果你重新安装现有的核心服务器，安装程序也会创建一个新的证书。如果使用与新的核心服务器证书不匹配的证书安装设备，该核心服务器将无法与这些设备通讯。需要重新安装核心服务器时，您有两个选择：

1. 使用您在新的核心服务器上创建的配置来手工重新安装代理。由于核心服务器和设备之间没有匹配的证书和密钥，您不能使用软件分发来更新代理。
- 重新安装核心服务器之前，请将现有证书和关键文件备份到安全的地方。重新安装后，将原有密钥复制到新的核心服务器安装中。新的和原有的密钥可同时存在。核心服务器将自动使用适当的密钥。

核心服务器可包含多个证书/私钥文件。只要客户端能够使用密钥之一通过核心服务器上的身份验证，就可以与该核心服务器通信。

此产品中包含实用程序，可执行上述所列第二个选项。核心数据迁移实用程序 (CoreDataMigration.exe) 安装在 \ProgramFiles\LANDesk\ManagementSuite 文件夹中。它可处理数据备份和复制，例如安装新核心时的私钥和证书。

### 保存和恢复证书/私钥集

1. 在源核心服务器上，转到 \Program Files\LANDesk\Shared Files\Keys 文件夹。
2. 将源服务器的 <keyname>.key、<keyname>.crt 和 <hash>.0 文件复制到软盘或其他安全的地方。
3. 在目标核心服务器上，将源核心服务器上的这些文件复制到同一文件夹 (\Program Files\LANDesk\Shared Files\Keys) 中。密钥会立即生效。

**警告：保证私钥文件的安全**

确保私钥 <keyname>.key 不会泄密。不要使用不安全的方式传送私钥，如电子邮件或公共文件共享等。核心服务器使用此文件验证设备身份，而拥有相应 <keyname>.key 文件的任何核心服务器都能够对其管理的设备执行远程操作及进行文件传送。

# 故障排除技巧

以下故障排除技巧适用于最常见的控制台问题。

**无法激活核心服务器。**
如果您安装了一台核心服务器，然后更改了设备时间，则无法激活该服务器。要激活此核心服务器，您必须重新安装此产品。

**尝试激活核心服务器时出现错误消息，提示无法读取核心服务器数据库。**
请检查以确保核心服务器物理连接到网络并具有有效的因特网连接。如果线缆已拔出或核心服务器的因特网连接无效，则无法完成激活过程。

**不知道指向控制台页面的 URL。**
请联系安装核心服务器的人员，通常是您所在站点的网络管理员。但 Server Manager 和 System Manager 的 URL 通常是 http://*核心服务器机器名*/ldsm。Management Suite 的 URL 是 http://*核心服务器机器名*/remote。

**以什么身份登录？**
查看**连接为**部分中名称 LANDeskSystem Manager 下方的条形图上方的内容。

**登录哪台机器？**
查看**已连接到**部分中名称 LANDeskSystem Manager 下方的条形图上方的内容。

**启动 System Manager 后立即收到“会话超时”消息。**
如果从“收藏夹”或“书签”菜单打开 URL 结尾处带 "/frameset.aspx" 扩展名的 System Manager，则无法正确启动。要解决此问题，编辑您的“书签”或“收藏夹”链接删除此扩展名，或直接将 URL（不含扩展名）粘贴到浏览器窗口中。

**看不到左侧导航窗格的某些链接。**
这是因为您的网络管理员正在使用 LANDeskSystem Manager 的基于角色的管理或功能级安全选项，从而使您无法执行原本有权执行的一些任务。

**扫描器无法与设备连接。**
如果扫描器无法与设备连接，请核对 Web 应用程序目录的配置是否正确。如果您正在使用 HTTPS，则必须拥有有效的证书。请验证您的证书有效。

**尝试访问控制台时，出现“权限被拒绝”的错误。**
要在 Windows 2000 和 2003 中使用功能级安全选项，必须禁用匿名验证。检验 Web 站点和 Web 站点下 ..\LANDesk\ldsm 文件夹中的验证设置。

1. 在托管 Web 控制台的服务器上，单击**开始|管理工具| Internet 信息服务 (IIS) 管理器**。
2. 在**默认 Web 站点**快捷菜单中，单击**属性**。
3. 在**目录安全性**选项卡的**匿名访问和验证控制**区域中单击**编辑**。清除**启用匿名访问**选项并选中**集成的 Windows 验证**选项。
4. 单击**确定**，退出对话框。
5. 在默认 Web 站点的 .\LANDesk\ldsm 子文件夹中，单击**属性**。重复步骤 3、4。

**查看控制台时出现无效的会话。**
可能该浏览器会话已超时。单击浏览器的**刷新**按钮启动新的会话。

**尝试启动 Web 控制台时，出现 ASP.NET 错误。**
如果在尝试登录到 Web 控制台时显示了 ASP.NET 错误消息，则可能是因为 ASP 和 ASP 目录权限配置不正确。请运行以下命令，重新配置 ASP.NET。

```
ASPNET_REGIIS.EXE -i
```

**每个页面中的条目数与指定的数目不同。**
指定每个页面显示的条目数时，该设置被存储在 Web 浏览器的 cookie 目录中，并在控制台会话超时的时候到期。

**控制台超时过于频繁。**
可以更改控制台 Web 页的默认会话超时时间。IIS 的默认设置是只要无操作状态持续 20 分钟，登录就会失效。更改 IIS 会话超时时间：

1. 在 Web 服务器上，打开“IIS Internet 服务管理器”。
2. 展开默认的网站。
3. 右键单击 **LDSM** 文件夹，然后单击**属性**。
4. 在**虚拟目录**选项卡上，单击**配置**。
5. 单击**应用程序选项**选项卡，然后将会话超时更改为所需的值。

**注意：**LANDeskSystem Manager8.70 是基于会话的产品。不要禁用会话状态。

**无法在 Web 控制台中查看“远程控制”页面。**
要查看**远程控制**页面，必须启用 ActiveX 控件。有些浏览器会默认设置为禁用 ActiveX 控件。如果无法正确加载**远程控制**页面，请通过更改安全设置启用浏览器的 ActiveX 控件。

**完成了软件分发向导的各个步骤，但控制台却没有创建程序包。**
控制台在控制台服务器上使用 IUSR 和 IWAM 帐户。这些帐户最初是根据计算机名创建的。如果您曾经更改过计算机名，要成功的创建软件分发程序包，则须完成下列步骤。

1. 如果安装了 .Net Framework，请将其卸载。
2. 卸载 IIS。
3. 重新安装 IIS。
4. 如果已卸载了 .Net Framework，请将其重新安装。

**计划好的软件分发作业没有运行。**
如果计划了一项软件分发作业，但其没有启动，请核实设备上已运行了“Intel 调度程序服务”。

同时，请考虑到作业的计划过程是以核心服务器的时间为根据的。如果在属于另一时区的控制台上计划作业，该作业将根据核心服务器的时间启动，而这个时间可能与您的预计时间不同。

**报告图表显示不正确。**
必须安装 Macromedia Flash Player* 方可查看多数报表中显示的交互式条形图和饼形图。请核实已安装了 Flash，然后重新运行该报表。

**Web 控制台无法向数据库验证身份的错误。**
如果您使用的是 Oracle 9.2.0.1，则会有一个 Oracle 安装错误：不能为已通过身份验证的用户设置适当的权限（IIS 要用）。如果发现 Web 控制台发生无法向数据库验证身份的错误，请按以下步骤进行修复。

1. 以具有管理员权限的用户身份登录到 Windows。
2. 从**开始**菜单启动 Windows Explorer 并定位到 ORACLE_HOME 文件夹。它通常是 Oracle 文件夹下的 Ora92 文件夹（如 D:\Oracle\Ora92）。
3. 从 ORACLE_HOME 文件夹的快捷菜单中，单击**属性**。
4. 单击**安全**选项卡。
5. 在**名称**列表中，单击**已验证用户**。在 Windows XP 中，“名称”列表称为**组或用户名**。
6. 在**允许**列下的**权限**列表中，清除**读和执行**选项。在 Windows XP 中，**权限**列表称为**已验证用户的权限**。
7. 重新选中**允许**列下的**读和执行**选项（刚才取消选中的选项）。
8. 单击**高级**，在**权限条目**列表中，确保其中所列的**已验证用户**的“权限”为“读和执行”，并且“应用于”为“此文件夹、子文件夹和文件”。如果看不到上述内容，请编辑该行并确保**应用于**框设置为**此文件夹、子文件夹和文件**。此属性应该已正确设置，但您应务必对其进行核对。
9. 单击**确定**，直到关闭所有安全属性窗口。
10. 重新启动服务器以确保这些更改生效。

**安装时 Oracle 出现错误。**
安装过程中，您可能会看到以下消息：

没有在本地机器上注册 OraOLEDB.Oracle.1 提供程序。

如果出现这种情况，很可能是因为权限问题导致的。您很可能是使用 9i 客户端连接到 Oracle 数据库，这是一个已知的 Oracle 问题。如果您确定已经安装了 OraOLEDB 驱动程序，则请尝试以下步骤：

1. 在 Windows“资源管理器”中，转到 OraHome92 目录（默认情况下，该目录是 C:\oracle\ora92），右击此文件夹并选择**属性**、**安全性**、选择**已验证用户**，取消选择“读和执行”权限的**允许**框后重新选中此框，然后单击**应用**。
2. 单击**高级**按钮，选中**允许将父级对象的可继承权限传播到此对象**和**重置所有子级对象的权限并启用可继承权限的传播**复选框。单击**应用**并在出现提示时选择**是**。完成此过程后，您将会发现已选中**允许将父级对象的可继承权限传播到此对象**复选框。
3. 在“命令提示”窗口中，键入 ″iisreset″。

此时，您应当能够向数据库验证身份并使用控制台。 **为什么数据库中的同一设备出现两个实例？**
是否从核心数据库中删除了设备并使用 UninstallWinClient.exe 重新安装了该设备？

UninstallWinClient.exe 位于 LDMain 共享目录中，该目录是 ManagementSuite 的主程序文件夹。仅有管理员可以访问该共享目录。该程序将卸载所有运行该程序的设备上的 LANDesk 代理。您可以将其移至所需的任何文件夹或将其添加到登录脚本。它是 Windows 应用程序，可在不显示界面的情况下无提示运行。您可以在刚刚删除的数据库中看到该设备的两个实例。其中一个实例仅包含历史数据，另一个实例包含正在处理的数据。有关 UninstallWinClient.exe 的详细信息，请参阅*部署指南*。

**在重新安装的 Management Suite/Server Manager8.70 中使用来自 Server Manager8.70 或 Management Suite 8.X 的以前数据库。**
如果卸载以前安装的 LDMS 8.X 或 LDSM 8.70，且它们以前在同一台机器上使用 MSDE 数据库，将不卸载 MSDE 数据库和创建的实例，也就是说如果您想在该机器上重新安装 LDSM/LDMS 8.70，则还可以使用这些数据库和实例。重新安装过程中，可通过查看注册表获取连接该数据库所需的连接信息：

注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\Core\Connections\Local

以下字符串值对应需在“用户提供的数据库配置”页面中填写的内容：

服务器 <主机名\ldms 数据>
用户 <sa>
数据库 <lddb>
密码（可以是编码，这取决于“PWD 加密”）

**尝试搜寻 IPMI 设备时，该设备未列在不受管设备页面的 IPMI 文件夹中。**
IPMI 设备必须具有 BMC（底板管理控制器），其配置将设备搜寻为 IPMI 设备，并可使用完全 IPMI 功能。如果没有配置 BMC，设备则搜寻为计算机。然后可将设备添加到受管设备列表，并运行“配置服务”实用程序以配置 BMC 密码。本产品随后便可识别设备的 IPMI 功能。

**选择 PXE 启动菜单后无法获得核心服务器地址**
尝试在目标机器上运行 PXE 代表部署，重新启动设备，按下 F8 键并选择 PXE 启动菜单，您将获得消息“HTGET：无法获取<核心服务器>地址。错误：无法将名称：<核心服务器>解析为地址。ParseCoreAddressInof 失败

原因是客户端试图使用 HTTP 从核心服务器下载文件。客户端将使用 WINS 将核心服务器名称解析为 IP 地址。如果无法从核心服务器下载文件，则会返回 HTGET 错误。

要解决此问题，请参阅文章
http://kb.landesk.com/al/12/4/article.asp?aid=2558&n=7&tab=search&bt=4&r=0.1898264&s=1

**向服务器添加了 S.M.A.R.T. 驱动器，但在该服务器的清单列表中看不到 S.M.A.R.T. 驱动器监视。**
硬件监视有赖于安装在设备上的硬件功能，还有赖于硬件的正确配置。如果在设备上安装了具有

S.M.A.R.T. 监视功能的硬盘驱动器，但 S.M.A.R.T. 检测未在设备的 BIOS 设置中启用，或者该设备的 BIOS 不支持 S.M.A.R.T. 驱动器，则无法进行数据监视并会导致警报无法生成。

**在基于 PXE 的 OSD DOS 脚本中，逗号后的部分将被截断。**
在脚本行中，逗号之后的所有字符都会被删截，因此逗号之后的任何命令都不会执行。要避免发生此情况，请给整个命令加上引号，如下：

```
REMEXEC1=%QUOTE%echo "hi,good morning"%QUOTE%
```

正常引号将在 .INI 文件读取过程中剥离，因此不会起作用。

**尝试从不同子网中的 Web 控制台安装“远程控制”时，无法安装 RC 查看器。**
如果连接到由不同域中核心服务器托管的 Web 控制台，且在**我的设备**列表中右击计算机并选择**远程控制**，则会出现错误，提示 RC 查看器尚未正确安装。

要解决此问题，可通过从 web.config 中读取名为 "CabUrl" 的标记来获取 CAB 的 URL。标记 CabUrl 必须包含核心服务器的完全规范域名，而不仅仅是机器名。您需要打开 web.config 并将完全规范域名置于 CabUrl 标记中。

**在运行清单扫描之前，“清单”列表中不会列出 USB 磁盘设备。**
当磁盘设备通过 USB 电缆与受管设备相连时，该磁盘设备不会立即列出于设备清单的硬盘驱动器之下。连接到设备后，磁盘设备会在逻辑驱动器下列出。但是，清单扫描在设备上运行之前，它不会显示在硬盘驱动器之下。

在受管的 Linux 设备上，必须安装 USB 磁盘设备才能在清单中将其列出。如果已安装了 USB 磁盘设备，但尚未运行清单扫描，则 USB 磁盘设备会在逻辑驱动器下显示；清单扫描后，同时在硬盘驱动器下列出。设备断开连接时，应将其从系统中卸载。在某些运行旧版内核的 Linux 系统中，设备在断开连接且卸载后仍可能在清单列表中保留。在这种情况下，需要重新启动受管设备才能将其从清单列表中删除。

**当我查看 Web 控制台帮助索引时，它是黑色的。**
Web 控制台的 HTML 联机帮助具有全文搜索功能，它依赖于 Windows 索引服务。在正常情况下，该功能是默认启用的。如果需要在 Web 服务器上启用索引功能，请执行以下操作：

1. 单击**开始|程序|管理工具|服务**。
2. 双击**索引服务**，然后单击**启动**。
3. 单击**确定**，退出该对话框。

可能需要等待一会儿（最长达数小时），以便索引服务为服务器建立索引。