LANDesk® System Manager 8.7

安装和部署指南

LANDesk®

封页

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。

内容

概述

本指南阐述了 LANDesk® System Manager 的安装和部署过程。此产品可简化计算机的管理和常见计算机问题的解决，因此有助于降低总拥有成本。

在本指南中，您将了解到以下内容：

该版本的新增功能

随着计算机产业的不断发展，计算机系统变得日益复杂和难以管理。对于使用数年的计算机而言，维护和修复所花费的时间增加了总拥有成本 (TCO)，而这远远超出原先的购买价格。LANDesk® System Manager 简化了计算机的管理和常见计算机问题的解决，因此有助于降低 TCO。

- **查看系统清单：**System Manager 提供了大量计算机硬件和软件配置方面的信息。
- **监视计算机的健全性：**当计算机处于警告或严重健全性状况时，System Manager 会对诸如温度、电压、可用内存和磁盘空间等项目作出报告。
- **接收系统事件警报：**System Manager 能使用多种警报方式来通知问题。
- **监视实时或历史性能：**System Manager 可用于监视多种系统对象的性能，例如驱动器、处理器、内存和服务的性能。您可以对警报操作进行设置：指定当计数器超过阈值上限或下限的次数达到预先确定的次数时触发通知。
- **监视当前进程和服务：**System Manager 允许您查看当前服务及其状态，或设置警报操作来通知服务状态的更改。
- **远程关闭、打开和重启计算机：**对于支持远程电源管理的系统，System Manager 可从管理员控制台启用远程电源管理。
- **计划任务视图：**从一个位置查看或重新计划所有代理部署、搜寻、
- **增强的操作系统支持：**从单个控制台管理异质环境中的所有设备。支持 Windows 2000、2003 和 XP Professional、Red Hat Linux、SUSE Linux、HP-UX 和 AIX。有关详细信息，请参阅第 1 阶段：系统要求。
- **Intel* AMT 和智能型平台管理界面 (IPMI) 支持：**System Manager 支持基于硬件的管理组件，这些管理组件能够通过带外 (OOB) 通信远程管理处于任何状态的网络设备。只要设备连接到公司网络并且具有独立电源，您就可以访问清单、查看远程诊断信息、远程重新启动系统。
- **刀片服务器支持：**对刀片服务器和刀片机箱管理模块 (CMM) 的支持包括管理功能和清单功能。
- **脚本编写工具：**您可以安排和执行针对设备的自定义任务

- **任务调度程序：**通过数据完整性和可伸缩性都得到改进的单一数据库架构，您可以访问与受管设备有关的一组丰富信息（包括与 Management Suite 的完全集成）。这个单一架构的一部分就是任务调度程序。您现在可以在一个公共窗口中查看所有任务（搜寻、代理配置、。在该窗口中，您可以重新计划、修改计划或使计划重复执行。
- **基于角色的管理：**基于用户在组织中的管理角色配置用户对工具和网络设备的访问权限。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。
- **不受管的设备搜寻：**使用多种方式搜寻网络中的设备。该产品标识运行 Windows 或 Linux 的服务器、刀片服务器和刀片机箱、启用 IPMI 的服务器、启用 Intel AMT 的服务器以及其他网络设备。安排设备搜寻的时间，以便始终能掌握新设备。还可生成关于网络中未受管设备的报告。
- **增强的安全性：**采用基于证书的安全模型，使设备只与经授权的核心服务器和控制台进行通信。
- **软件分发：**使软件应用程序的安装过程或向设备分发文件的过程实现自动化。
- **报告：**预定义的服务报告可用于计划和策略分析。
- **计划任务支持：**提供多种登录，作为调度程序服务在没有代理的设备上运行任务时的验证方法。这对于管理多个 Windows 域的设备特别有用。

产品基础

System Manager 可以管理运行几种不同操作系统的设备，包括 Windows 2000 Pro SP4、Windows XP Pro SP1、Windows* 2000/2003 服务器、Red Hat Enterprise Linux v3 服务器、SUSE Linux 9 服务器、HP-UX 和 AIX 服务器，同时它还提供了通用界面来管理运行这些网络操作系统的设备。它还可以与其他 LANDesk 产品共存，如 LANDesk® Management Suite 和 LANDesk® Server Manager。

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：网络中安排产品代理的**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。

产品如何适应网络？

该产品使用现有网络的基础结构来建立与它所管理的设备之间的连接。无论是管理小型网络环境还是大型企业的网络环境，都可以大大简化现有设备的管理工作。

将 System Manager 与 Management Suite 或 Server Manager 配合使用

如果已经安装 System Manager 并且希望将它与 Management Suite 或 Server Manager 配合使用，则必须使用“核心服务器激活”实用程序提供要与 System Manager 配合使用的产品的有效用户名和密码。System Manager / Management Suite 安装可提供三种可用的控制台：Management Suite Windows 32 和 Web 控制台以及 System Manager Web 控制台。Server Manager 控制台包括三个导航项（警报、监视和日志），其中含有在 Management Suite 两个控制台上找不到的功能。

如果部署 Management Suite，则 Management Suite 安装会删除受管设备上的 System Manager 代理，反之亦然。在 System Manager 中运行 Management Suite 时，Management Suite 配置功能包括监视选项。

在已经安装 Management Suite 或 Server Manager 的情况下安装 System Manager

如果已经在核心服务器上安装了 Management Suite 或 Server Manager，希望添加 System Manager，则使用与原始 Management Suite 或 Server Manager 安装相同的安装。

1. 打开 autorun.exe。
2. 单击**立即安装**。
3. 选择一种语言，然后单击**确定**。
4. 此时将显示“欢迎使用”屏幕。单击**下一步**。
5. 选择**修改**（如果需要），然后单击**下一步**。
6. 单击 LANDesk® Server Manager，然后再单击**下一步**。
7. 按照向导的屏幕说明执行。

核心服务器的系统要求

在您考虑将哪个服务器设置为核心服务器之际，请参阅下列系统要求，并确认所需的服务器达到或超过“第 1 阶段：系统要求”中列出的要求。前提条件检查程序会自动执行此过程。

强烈建议您使用专用的核心服务器
由于通信量经由核心服务器才能对域进行管理，因此，强烈建议每台核心服务器均专门用于托管产品。

如果您在同一台服务器上安装了其他产品，则在长期或短期内可能会受到资源问题困扰。

不要在主域控制器、备用域控制器或 Active Directory 控制器上安装核心服务器组件。

安装和部署战略

当使用产品介质上的 Autorun 安装时，安装程序将自动验证核心服务器是否符合上述要求，然后再进行安装。要在异构网络中安装和部署系统级应用程序，在运行安装程序*之前* 需要慎重考虑安装和部署的方法并进行周密的计划。本指南提供了产品的安装策略。在部署产品之前，需要简明地列出您的管理需求。

部署策略注意事项

部署是将管理功能扩展到域要包含的服务器的过程。在本指南中，将按“阶段”来讨论部署。

分阶段部署策略为您提供了一个结构化的方法来启用对设备的管理。该方法基于以下两个简单原则：

- 首先，部署对现有网络影响最小的产品组件，然后依次进行，最后部署影响最大的组件。
- 第二，根据周密的计划分阶段部署产品，而不是一次部署完所有服务，因为这样有可能会使任何必要的故障排除过程复杂化。

本指南按部署阶段进行组织，可帮助您部署产品。请从本指南后面的第一章“第 1 阶段：设计管理域”开始。随后，应依次完成各个阶段。

安装和部署概述

本指南将安装和部署任务分为以下几个阶段。每个阶段在本指南中都能找到对应的章节，指导您完成相应的安装过程。一章通过配置服务、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等部分，帮助您快速入门使用产品。该章假设您将参考本书的其余部分了解详细信息，因此内容编排非常简明。本指南中的某些步骤在“入门”一章中重复提及。

第 1 阶段概述

安装的第 1 阶段，设计管理域，具体任务如下：

- 收集网络信息
- 确认网络符合系统要求

有关详细信息，请参阅本指南后面的“第 1 阶段：设计管理域”。

第 2 阶段概述

在第 2 阶段，安装产品，具体任务如下：

- 安装核心服务器

有关详细信息，请参阅本指南后面的“第 2 阶段：安装核心服务器和控制台”。

第 3 阶段概述

在安装的第 3 阶段，搜寻网络上的设备并部署产品代理。您可以从控制台“推”出代理，也可以从服务器共享“拉”出代理。

有关详细信息，请参阅本指南后面的第 3 阶段：将代理部署到设备。

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

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。将会填写用户名和密码。
2. 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。

第 1 阶段：设计管理域

在第 1 阶段中，您需要收集有关网络基础设施的信息，并做出有助于自定义管理域的决策。

在这一阶段您将了解以下内容：

收集网络信息

确定并收集与您的网络有关的信息中涉及到 System Manager 的所有重要信息。具体来说，您必须完成以下工作：

- 确定设备配置
- 选择核心服务器

选择核心服务器

核心服务器是一个管理域的中心。的所有重要文件和服务都包含在核心服务器中。从物理上讲，它可以是新服务器，也可以是重定目标的服务器。

您可以通过远程工作站上的浏览器运行管理员控制台，在控制台中，您可以执行多项管理活动，如管理警报、查询核心数据库或者创建自定义脚本。

请确保为核心服务器选择的服务器符合系统要求。请参阅本阶段后面的“系统要求”部分。

计划程序文件的安装位置

安装时可以指定程序文件的安装位置。除非您有令人信服的理由不使用默认的目录，否则请接受默认目录。如果您选择修改目标目录，则目标目录路径不能包含双字节字符。

核心服务器文件的默认目标目录是：

```
C:\Program Files\LANDesk\ManagementSuite
```

核心数据库

System Manager 在核心服务器上安装 MSDE 数据库。每个 MSDE 数据库的大小都不超过 2 GB。该数据库所支持的服务器数量取决于网络的清单扫描文件的大小。

如果对 MSDE 数据库同时进行五项以上的操作，就可能会遇到性能问题。例如，如果有五个 System Manager 管理员同时访问该数据库。

核心服务器/客户端安全性

此产品采用了基于证书的身份验证系统。在安装核心服务器时，安装程序会为核心服务器创建一个证书。客户端在与核心服务器通信时会查找该证书，如果客户端没有相应的证书，将无法与核心服务器通信。

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，才能与核心服务器进行通信。每台核心服务器都有自己的证书和私钥。默认情况下，您在每台核心服务器上部署的客户端代理只会与从中部署相应软件的核心服务器进行通信。

计划范围

基于角色的管理是功能安全管理的强大特性。在左窗格中单击“用户”可访问控制台中基于角色的管理工具。您必须以管理权限登录。

基于角色的管理提供了高级设备管理功能，允许在系统中添加用户以及为这些用户分配权限和范围。权限决定了用户可以看到并使用的工具和功能（请参阅《Server Manager 用户指南》中的“了解权限”）。范围决定用户可以看到和管理的设备范围（请参阅《Server Manager 用户指南》中的“创建范围”）。

您可以根据用户的责任、希望他们执行的管理任务以及希望他们看到、访问并管理的设备为他们创建角色。可以限制只能由某一地理位置的用户访问设备。该地理位置可以是国家/地区、地区、州（省/自治区）、城市，或使设备访问只限于特定组或特定类型的服务器。

要在网络中实施这种基于角色的管理，只需对当前用户进行设置，或者可以创建新用户并将其添加为产品用户，然后为其分配必要的权限和范围以访问产品功能和受管设备。

核心服务器利用范围来限定控制台用户可以看到的设备。可以为一个用户分配多个范围，多个用户也可以使用一个范围。您可以通过以下方法之一来确定范围：

- （默认）**所有机器范围：**用户可以查看所有设备。
- **基于查询：**用户可以看到符合特定查询（由管理员分配给用户）条件的设备。
- **基于组：**用户可以看到满足组条件的设备。

有关范围的详细信息，请参阅 Server Manager *《用户指南》*。

系统要求

在安装之前，请确保满足以下系统要求。前提条件检查程序会执行此过程。

核心服务器和数据库服务器

确保所有核心服务器和数据库服务器都符合概述中的下列要求：

- 装有 SP 4 的 Windows 2000 Server 或 Advanced Server、Windows Server 2003 Standard 或 Enterprise Edition x86 SP1 或者 Windows 2003 R2
- Microsoft Data Access Components (MDAC) 2.8 或更高版本
- Microsoft .NET Framework 1.1
- Internet Information Services (IIS)
- 用于 ASP.NET v1.1 脚本编写的 IIS 支持
- Internet Explorer 6.0 SP1 或更高版本
- Microsoft NT 文件系统 (NTFS)
- 用于核心服务器的 Windows 服务器必须作为独立的服务器来安装，而不应将其作为主域控制器 (PDC)、备用域控制器 (BDC) 或 Active Directory 控制器来安装。
- 必须安装 SNMP，并且必须启动 SNMP 和 SNMP 陷阱服务
- 系统驱动器上需有 200 MB 可用空间，并且至少一个驱动器上有 900 MB 可用空间
- 管理员权限
- LANDesk 客户端是正确版本或者未安装。

核心服务器的要求
Windows 页面文件的大小应至少为 12 + *N*（其中 *N* 表示核心服务器上的 RAM 容量，按 MB 计）。否则，产品应用程序可能会产生内存错误。

如果准备在同一核心服务器上安装 Management Suite 和 Server Manager 产品，建议核心计算机上具有 1 GB 内存。

由一台服务器托管所有产品服务

对于较小的管理域，您可以在一台服务器上安装核心服务器和核心数据库。对于此类网络，您最好使用默认的 Microsoft MSDE 数据库，该数据库通常更易于维护。 这是 System Manager 的数据库唯一选项。

要考虑的限制因素

在安装核心和数据库之前，您的服务器应至少满足以下系统要求：

- Pentium 4 处理器
- 4 GB 可用磁盘空间，硬盘驱动器速度不小于 10K RPM
- 768 MB 以上的 RAM

受管服务器计算机

该产品支持以下服务器操作系统（并非支持所有的操作系统）：

- 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 R2
- 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

Linux 受管服务器计算机

下面列出了启用 Linux 设备进行管理的防火墙和 RPM 前提条件。

防火墙

为了首次安装管理代理并配置 Linux 服务器，以便与核心服务器通信（使用“推”方法），必须允许 SSH 连接通过 Linux 服务器的本地防火墙：

22 - 仅 TCP

要使代理能够与核心服务器进行通信（以使用“清单扫描”、“软件分发”、“漏洞更新”等功能），Linux 服务器的本地防火墙必须配置为允许使用以下端口进行通信：

9593 - 仅 TCP

9594 - 仅 TCP

9595 - TCP 和 UDP

要与管理代理进行通信，Linux 服务器的本地防火墙必须被配置为允许使用以下端口进行通信：

6780 - 仅 TCP

所需要的 RPM（版本号或更高版本）

建议您在 ...\ManagementSuite\ldlogon\RPMS 目录中存储所有产品 RPM。您可以通过 http://core name/RPMS 浏览到此目录。

REDHAT_ENTERPRISE

python

RPM 版本：2.2.3-5 (RH3)

2.3.4-14 (RH4)

Binary 版本：2.2.3

pygtk2 RPM 版本：1.99.16-8 (RH3)

2.4.0-1 (RH4)

Binary 版本：

sudo

RPM 版本：1.6.7p5-1

Binary 版本：1.6.7.p5

bash RPM 版本：2.05b-29 (RH3)

3.0-19.2 (RH4)

Binary 版本：2.05b.0(1)-发行版

xinetd RPM 版本：2.3.12-2.3E (RH3)

2.3.13-4 (RH4)

Binary 版本：2.3.12

mozilla RPM 版本：1.7.3-18.EL4 (RH4)

Binary 版本：1.5

openssl RPM 版本：0.9.7a-22.1 (RH3)

0.9.7a-43.1 (RH4)

Binary 版本：0.9.7a

sysstat RPM 版本：4.0.7-4

Binary 版本：4.0.7

lm_sensors

RPM 版本：2.6（要显示较新 ASIC 计算机上的传感器，此版本可能太低。有关详细信息，请参阅 lm_sensors 文档或访问网站 (http://www2.lm-sensors.nu/~lm78)。

SUSE LINUX

(SUSE 64)

bash

RPM 版本：2.05b-305.6

mozilla

RPM 版本： 1.6-74.14

net-snmp

RPM 版本： 5.1-80.9

openssl

RPM 版本：0.9.7d-15.13

python-gtk

RPM 版本：2.0.0-215.1 [注：程序包名称更改]

python

RPM 版本： 2.3.3-88.1

sudo

RPM 版本：1.6.7p5-117.1

sysstat

RPM 版本： 5.0.1-35.1

xinetd

RPM 版本： 2.3.13-39.3

lm_sensors

RPM 版本：无（注：此版本已合并到 2.6 版本的内核）

产品端口使用情况

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，请参阅本节提供的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）
2. 端口号

3. 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
6787	控制台到设备	TCP	控制台和设备之间的通信

端口	方向	协议	服务
9595	控制台到设备	UDP	搜寻
9595	控制台到设备	TCP	代理配置
623	控制台到设备	UDP	ASF、IPMI 搜寻
9535	控制台到设备	TCP	远程控制

此产品需要在管理节点之前通过安装的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)。

第 2 阶段：安装核心服务器

此阶段的主要工作是安装核心服务器。

在这一阶段您将了解以下内容：

- 安装核心服务器
- 激活核心服务器
- 部署到 Windows 设备
- 部署到 Linux 设备

安装本阶段中所需要的组件大约需要 30-60 分钟。

安装核心服务器

安装核心服务器

1. 开始安装前，建议您关闭其他应用程序并保存所有打开的文件。在选定作为核心服务器的 Windows 2000/2003 服务器上： 将产品介质插入驱动器中，或从安装映像运行 AUTORUN.EXE。此时将显示“自动运行”屏幕。
2. 单击**检查先决条件并安装**。
3. 此时将运行系统要求检查程序，验证服务器是否满足最低系统要求。确保所有系统需求得到满足。 如果有任何系统需求未得到满足，对于与安装失败的要求相关的链接或信息，请在失败要求的链接上单击**失败**。
4. 单击**立即安装**，运行安装程序。
5. 选择希望安装程序安装的语言。单击“确定”。
6. 此时将显示“欢迎使用”屏幕。单击**下一步**继续操作。
7. 在“许可证协议”屏幕上，如果同意的话，单击**我接受许可证协议中的条款**继续。单击**下一步**。
8. 接受默认的目标文件夹，或指定一个自定义的目标文件夹，然后单击**下一步**。目标文件夹路径不能包含双字节字符。如果更改了该文件夹，请记住用路径替换您在产品文档中看到的路径。
9. 输入 MSDE 数据库密码。请记住或记录此密码。单击**下一步**继续操作。
10. 输入核心服务器的安全证书的组织和证书名称。该信息有助于命名和描述该证书。单击**下一步**。
11. 在“准备安装”页面上，单击**安装**。产品开始安装。
12. 完成安装后出现**安装向导完成**对话框。
13. 单击**完成**。
14. 安装程序会提示您重新启动服务器。必须单击**是**才能完成“安装”。服务器重新启动时，您将注意到，在登录后，安装程序还要运行数分钟，才能完成本安装进程。在第一次重新启动时，安装程序不会提示您输入任何信息。

在 Windows 2003 Server 上安装 MSDE 核心数据库时，Windows 可能会中断安装程序，并询问是否确定要打开 Setup.exe。如果看到该提示，请单击“打开”，否则产品将无法正确安装。如果要安装 Intel Platform Extensions for LANDesk Software，请按照安装 Server Manager 之后打开的向导执行。

激活核心服务器

必须激活核心服务器，才能在该服务器上使用 System Manager 产品。您可以通过 Internet 自动激活核心服务器，或通过电子邮件手动激活核心服务器。如果您对一个核心服务器的硬件配置进行了较大更改，可能需要重新激活该核心服务器。

核心服务器上的激活组件将定期生成以下相关数据：

- 您使用的设备的精确数量
- 非个人加密硬件配置
- 您正在使用的具体 LANDesk Software 程序（总称“服务器计数数据”）

激活组件不收集或生成任何其它数据。硬件密钥代码是使用非个人硬件配置因素在核心服务器上生成的，例如硬盘驱动器的大小、计算机的处理速度等。硬件密钥代码以加密格式发送到 LANDesk，该加密的私钥仅驻留在核心服务器上。然后，硬件密钥代码由 LANDesk Software 用于创建授权证书的一部分。

安装核心服务器之后，“核心服务器激活”实用程序（**开始|所有程序| LANDesk |核心服务器激活**）在第一次启动时运行，以便使用 OEM 提供的用户名和密码。

您可以使用核心激活实用程序从 System Manager 升级到 Server Manager 或 Management Suite。请参阅“将 System Manager 与 Management Suite 或 Server Manager 配合使用”。

在激活核心服务器之后，可使用控制台的**首选项|许可证**对话框查看产品授权信息。使用 Intel OEM 许可，您将有权在每个 Intel 品牌的服务器或主板上运行产品代理。

关于核心服务器激活实用程序

第一次激活新服务器时可使用“核心服务器激活”实用程序。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服务器计数数据”。

每个核心服务器必须有一个唯一的授权证书。

核心服务器会通过定期生成“\Program Files\LANDesk\Authorization Files\LANDesk.usage”文件来验证授权。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。对此文件进行的任何手动更改都会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。

请注意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该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，您可以按本节中后面所述，手动验证和发送服务器计数。

激活核心服务器

激活服务器

1. 单击**开始|所有程序|LANDesk|核心服务器激活**。
2. 使用您的 LANDesk 联系人姓名和密码，单击**激活此核心服务器**。

将会自动填写联系名称和密码。

手动激活核心或验证服务器计数数据

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服务器计数数据。然后，您将看到一条消息，提示您通过电子邮件手动发送激活和服务器计数验证数据。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服务器计数数据

1. 当核心服务器提示您手动验证服务器计数数据时，它会在“\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。

登录到控制台

在完成安装程序、已重新启动核心服务器并且激活核心之后，便可启动控制台，方法是打开一个浏览器，以下列格式输入服务器的地址：http://servername/ldsm。（在核心服务器上，单击“开始|所有程序|LANDesk|System Manager”）一旦启动控制台，您就会看到控制台登录窗口。控制台将提示您输入登录使用的帐户凭证（LDSM 是以该帐户身份安装的）。只有核心服务器 LANDesk Management Suite 组中的成员才可以登录。默认情况下，安装程序会将您先前安装核心服务器时登录所使用的用户名添加到 LANDesk Management Suite 组中。如果希望其他用户也可访问控制台，请将他们添加到此组中。

第一次在浏览器中启动控制台时，可能需要长达 90 秒的时间才能显示。这种延迟现象产生的原因是服务器必须对某些代码进行一次编译。启用过一次后，控制台的开启速度就快得多了。

部署到 Windows 设备

本产品支持已计划的、基于推的配置方法，允许远程部署代理。

要对尚未运行标准管理代理的 Windows 2000/2003 服务器启用基于“推”的配置，必须提供如下的正确登录凭证：

1. 在核心服务器上，单击**开始|所有程序| LANDesk** | LANDesk **配置服务**，然后再单击**调度程序**选项卡。
2. 单击**更改登录**。
3. 在**用户名和密码**字段中，指定域管理员帐户（采用“域\用户名”格式）。
4. 停止并重新启动调度程序服务。
5. 从 Web 控制台，以所需设备为目标，然后单击**代理配置 > 计划任务**以部署配置。

当配置与核心服务器同属一个域的 Windows 2000/2003 成员时，可以指定域管理员。要在其他域中配置 Windows 2000/2003 服务器，则必须设置信任关系。请记住，在前面第 3 步中确定的帐户也是调度程序服务在核心服务器上运行时所使用的帐户。请确保该帐户具有**以服务身份登录**的权限。

如果“推”配置失败，并显示“找不到代理”消息，请尝试执行以下步骤来找出问题所在。这些步骤与调度程序在“推”配置过程中的操作相仿。

1. 查找运行调度程序服务时所使用的用户名。
2. 在核心服务器上，使用第 1 步中找到的用户名登录。
3. 将驱动器映射到 \\服务器名称\C$。（这一步是最有可能失败的步骤。其失败的原因有二。很可能是，您对该服务器没有管理权限。如果此用户名无管理员权限，则可能是禁用了该服务器的管理共享 (C$)。）
4. 创建目录 \\服务器名称\C$\$ldtemp$ 并将文件复制到该目录中。
5. 使用 Windows 服务管理器并尝试在服务器上启动和停止服务。

1. 如果设备已启用 IPMI，则必须提供 BMC 密码。使用**配置服务**的 **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。

如果设备已启用 Intel* AMT，则必须提供 Intel AMT 密码。使用**配置服务**的 **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。

配置 Intel AMT 密码

1. 在 **Intel AMT 配置**选项卡中，键入当前的用户名和密码。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。
2. 要更改用户名和密码，请完成**新 Intel AMT 密码**部分。
3. 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

部署到 Linux 设备

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)。

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。

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。使用搜寻设备搜寻您的 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，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 服务器版本”，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. 单击**保存更改**。

要部署您的代理配置，在“代理配置”中选择您的代理配置，并单击**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 机器的任何健全性信息。 **拉 Linux 代理配置**

1. 在您的 Linux 机器上创建临时目录（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 (<configuration name>.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 <configuration name>.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“FILExx”。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\<any text>.ruleset.xml 应该被重命名为 internal.ruleset.xml
        - monitorrules\<any text>.ruleset.monitor.xml 应该被重命名为 masterconfig.ruleset.monitor.xml
2. 如果是 IPMI/BMC 计算机（安装中包括监视程序），则在命令行中键入下列内容：

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

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：请注意，如果您将某代理推或拉至一台 Linux 机器，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机器上留下的唯一文件。

-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。

第 3 阶段：分阶段部署

在第 3 阶段您将了解分阶段部署。*部署*是将管理功能扩展到您的管理域要包含的设备的过程。

通过将产品代理和服务加载到设备上来部署此产品。这样，您便可以从一个位置对它们进行集中管理。

在这一阶段您将了解以下内容：

- 阶段性部署策略
- 关于设备配置任务的核查清单
- 部署到 Windows 设备
- 了解设备配置的体系结构

阶段性部署策略

阶段性部署需要遵循三个原则：

1. 首先将组件部署到不太使用或对现有网络影响最小的设备上，然后依次进行，最后部署到使用最多或影响最大的设备上。
2. 在部署更多代理之前，请确保每个受管设备都能稳定运行。
3. 根据合理规划分阶段逐步部署产品，不要将代理同时部署到所有类型的设备上，否则可能会使所有必要的故障排除工作复杂化。

完成了前两个阶段的任务之后，就可以开始最后这个阶段的部署工作了，也就是将产品部署到设备上。

关于设备配置任务的核查清单

要配置设备，可以从 Web 控制台远程部署代理或从受管设备安装代理。为了进行基于“推”的配置，必须配置任何 IPMI 或 Intel* AMT 计算机的服务。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**。使用“BMC 密码”或“Intel AMT 配置”选项卡。

- **基于“推”的配置**：使用代理配置定义设备配置。通过“配置服务”（请参见*《用户指南》*中的“配置服务”部分）为 Intel AMT 或 IPMI 计算机提供必要的凭证。以所需的设备为目标，然后安排任务将配置推向设备。请参见*《用户指南》*中的“配置代理”部分。
- **手动配置**：在受管设备上，将某个驱动器映射到核心服务器的 LDLogon 共享目录，然后运行服务器配置程序 SERVERCONFIG.EXE。必须交互选择部署到设备的组件。

显然，在大型环境中，安装到设备和配置设备时手动配置的方法并不可取。多数情况下，您会将代理“推”向受管设备。请注意：产品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，然后自动重新启动核心服务器。

无论使用何种方法配置设备，都要确保已使用控制台中的代理配置创建了要部署的设备配置。

Windows XP Professional SP2 或 2003 SP1 系统需要手动配置防火墙，才能获得全部产品功能。为设备指定以下设置：　　**受管服务器：**

文件和打印机共享 - TCP 139、445；UDP 137、138（无此设置，代理“推”无法进行）

软件分发 - TCP 9594, 9595（无此设置，代理“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设备。）

核心服务器：

清单 - 5007

要指定这些设置，请在受管设备上单击**开始|控制面板|安全**。　　该产品随附了默认代理配置，包括标准管理代理、软件更新和监视代理。

您可以创建仅含有要安装组件的新配置，也可（仅限 OEM 版本）将 Intel Active System Console 添加到默认代理配置。请注意，部署代理的过程不可累积：任何部署都会卸载所有现有代理。要向配置部署新的代理，必须将其和先前所有需要的代理一起包括在配置中。　　**创建设备配置**

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，例如 DBServer 或 Executive Office Server。这可以是现有的配置名称，也可以是一个新名称。

4. 选择 **Linux 服务器版本**、**Microsoft Windows 服务器版本** 或 HP-UX。
5. 在未安装产品软件代理的情况下，要管理启用 IPMI 的服务器，如果**仅 IPMI BMC 配置**适用于 IPMI 兼容服务器，请选中该配置，然后单击**确定**。
6. 选择刚创建的配置并单击**编辑**。

在选项卡中，某些选项变暗，因为这些选项不适用于您选择的配置。例如，如果选择“仅 IPMI BMC Windows”配置，则没有可配置的选项。

7. 在**代理**选项卡中选择要部署的代理。
   - **所有：**在选定的设备上安装所有代理。
   - **软件更新：**安装软件更新代理。安装此代理后，可以配置如何运行扫描器检测可用更新。
   - **监控：**在选定的设备上安装监视代理。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、Intel Active System Console、Intel AMT 和 CIM。
8. **配置**仅用于显示信息。
9. 选择重新启动选项。

手动重新启动表示：即使选定的代理需要重新启动，设备也不会重新启动。您必须手动重新启动该设备。如果设备需要重新启动，则在其重新启动前，已安装的代理将无法正常工作。“必要时重新启动服务器”选项只在选定的代理需要重新启动时才会重新启动设备。

注意： 只有要更新现有 8.5 代理的设备需要重新启动。

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。

如果您选择清单扫描器的**指定时段**选项，您可以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。

- **始终在启动时运行：**每次设备启动时清单扫描器都将运行。

11. 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。
12. 单击**保存更改**以保存代理配置。

有关部署到设备的详细信息，请参阅本章结尾处的“了解代理配置的体系结构”。

部署到 Windows 设备

本产品支持已计划的、基于推的配置方法，允许远程部署代理。

要对尚未运行标准管理代理的 Windows 2000/2003 服务器启用基于“推”的配置，必须提供如下的正确登录凭证：

1. 在核心服务器上，单击**开始|所有程序|** LANDesk | LANDesk **配置服务**，然后再单击**调度程序**选项卡。
2. 单击**更改登录**。
3. 在**用户名和密码**字段中，指定域管理员帐户（采用“域\用户名”格式）。
4. 停止并重新启动调度程序服务。
5. 从 Web 控制台，以所需设备为目标，然后单击**代理配置 > 计划任务**以部署配置。

当配置与核心服务器同属一个域的 Windows 2000/2003 成员时，可以指定域管理员。要在其他域中配置 Windows 2000/2003 服务器，则必须设置信任关系。请记住，在前面第 3 步中确定的帐户也是调度程序服务在核心服务器上运行时所使用的帐户。请确保该帐户具有**以服务身份登录**的权限。

如果“推”配置失败，并显示“找不到代理”消息，请尝试执行以下步骤来找出问题所在。这些步骤与调度程序在“推”配置过程中的操作相仿。

1. 查找运行调度程序服务时所使用的用户名。
2. 在核心服务器上，使用第 1 步中找到的用户名登录。
3. 将驱动器映射到 \\服务器名称\C$。（这一步是最有可能失败的步骤。其失败的原因有二。很可能是，您对该服务器没有管理权限。如果此用户名无管理员权限，则可能是禁用了该服务器的管理共享 (C$)。）
4. 创建目录 \\服务器名称\C$\$ldtemp$ 并将文件复制到该目录中。
5. 使用 Windows 服务管理器并尝试在服务器上启动和停止服务。

1. 如果设备已启用 IPMI，则必须提供 BMC 密码。使用配置服务的 **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。

如果设备已启用 Intel* AMT，则必须提供 Intel AMT 密码。使用配置服务的 **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。

配置 Intel AMT 密码

1. 在 **Intel AMT 配置**选项卡中，键入当前的用户名和密码。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。
2. 要更改用户名和密码，请完成**新 Intel AMT 密码**部分。
3. 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

验证代理已部署成功

要验证管理代理是否已成功地部署到了设备，需要确保在控制台上可以执行以下任务。如果需要完成这些任务的附加信息，请参阅 *System Manager《用户指南》*中分别与这些功能相对应的章节。

清单

- 在**我的设备**列表中，双击设备，然后查看已安装代理的列表。
- 执行清单查询。
- 选择设备，然后单击**清单**查看该设备的数据。

- 修改 Windows 设备的 WIN.INI 文件，重新扫描设备，然后核对这些修改是否已记入了 CHANGES.LOG 中。

从命令行部署设备

可对 SERVERCONFIG.EXE 使用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。它位于核心服务器的（系统驱动器）\Program Files\LANDesk\ManagementSuite\LDLogon 中。SERVERCONFIG.EXE 还可在 \\coreservername\LDLogon 共享目录找到，这使得任何 Windows 2000/2003 服务器都可以读取该程序。

了解代理配置的体系结构

了解 SERVERCONFIG.EXE

SERVERCONFIG.EXE 是该产品的设备配置实用程序。它通过三个步骤来配置 Windows 服务器以进行管理：

1. 使用 SERVERCONFIG 确定计算机先前是否已由其它 LANDesk 产品配置。如果是，SERVERCONFIG 将删除旧文件并撤消任何其他更改。
2. 然后，SERVERCONFIG 会查找名为 CCDRIVER.TXT 的隐藏文件，以确定该服务器是否需要（重新）配置。（下面介绍了 SERVERCONFIG 的决策过程。）如果不需要（重新）配置设备，SERVERCONFIG 将退出。
3. 如果确实需要（重新）配置设备，SERVERCONFIG 将加载相应的初始化文件 (SERVERCONFIG.INI)，然后执行其中包含的指令。

如果您第二次运行 SERVERCONFIG.EXE 并选择了与第一次运行不同的代理，第一次执行时所用的代理将被删除。每次选择一个代理都要重新运行一次 SERVERCONFIG.EXE，尽管您之前曾安装了这些代理。

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）： "Common Base Agent" "Inventory Scanner" "Alerting" "Vulnerability scanner" "Server Monitor" "Active System Console" 可在同一命令行上组合这些组件。例如，

	示例：SERVERCONFIG.EXE /I="Mirror Driver" /I="Vulnerability scanner"
/IP	使用 IP 配置
/L 或 /Log=	CFG_YES 和 CFG_NO 日志文件的路径，这两种日志文件记录已配置和未配置的设备
/LOGON	执行带 [LOGON] 前缀的命令
/N 或 /NOUI	不显示用户界面
/NOREBOOT	完成后不重新启动设备
/P	请求用户执行权限
/REBOOT	运行后强制重新启动
/TCPIP	与 IP 参数相同（如上所述）
/X=	要排除的组件 示例：SERVERCONFIG.EXE /X=SD
/CONFIG=	/CONFIG]= 指定一个要使用的设备配置文件，取代默认的 SERVERCONFIG.INI 文件。 例如，如果已创建名为 NTTEST.INI 的配置文件，请使用以下语法： SERVERCONFIG.EXE /CONFIG=TEST.INI 自定义的 .INI 文件应和 SERVERCONFIG.EXE 位于同一目录下，请注意，/config 参数使用不带 95 前缀的文件名。
/? 或 /H	显示帮助菜单

部署标准管理代理

标准管理代理是必需的代理，是产品的基础协议。

部署漏洞扫描器

漏洞扫描器代理执行扫描和修复操作。使用**计划安全任务**按钮可创建一个任务，该任务将启动不带参数的 vulscan.exe。当 vulscan 不带参数启动时，它将查找其核心服务器的位置，方法是访问注册表项“hklm\software\intel\landesk\LDWM”的注册表值“CoreServer”。随后它将请求要扫描的最新漏洞信息列表，执行漏洞扫描，将结果提交给核心服务器。结果放在“检测到的更新”列表中。检测到的更新必须下载到核心服务器。通过修补过程也可以修补更新。如果修补过程成功安装了一个或多个修补程序，它将重新扫描并将新的结果提交到核心服务器。这种情况适用于 LANDesk 更新和 OEM 更新。

部署清单扫描器

使用清单扫描器向核心数据库添加设备，并收集设备的硬件和软件数据。第一次配置设备后，清单扫描器将自动运行。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。

部署监视代理

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、Intel AMT 和 CIM。

部署 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。此代理仅安装在带有 Intel 主板的设备上；如果在向非 Intel 主板的部署中包含此代理，它将不会进行安装。

卸载核心服务器

正如在部署不同的组件时应遵循各自的策略，在卸载各组件时也要遵循相应的策略。

以下内容介绍如何正确地卸载各个组件。必须按以下顺序卸载这些组件：

1. 从设备卸载产品代理。
2. 卸载核心服务器。

从设备卸载产品代理

从网络中卸载产品软件的第 1 步是，从设备上卸载该软件的代理。

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 ManagementSuite 共享文件夹下。
3. 打开命令提示窗口，转至 ManagementSuite 文件夹的驱动器盘符，输入以下命令：

```
uninstallwinclient.exe
```

4. 卸载程序将无提示运行，并移除所有代理。

也可以选择开始、运行，然后键入 *core name*\LANDesk\ManagementSuite\uninstallwinclient.exe。**从 Linux 服务器彻底删除 Linux 代理**

1. 在 ManagementSuite 共享文件夹中，找到 linuxuninstall.tar.gz 文件并将其复制到 Linux 框。
2. 使用 x、z 和 f 选项，执行该文件。命令行应为

```
tar xzf linuxuninstall.tar.gz
```

3. 执行该文件后，从命令行运行 ./linuxuninstall.sh。

要获得此文件的帮助，运行时加上 -h 选项。 注意：请注意，如果您将某代理推或拉至一台 Linux 机器，然后运行

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

将其清除之后再次推或拉，则会为具有相同名称和 IP 的同一机器创建重复的数据库条目，因为机器的 GUID 已删除。

-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。

卸载后仅剩下 /etc/ldiscnux.conf 文件。留下该文件可便于防止重复设备使数据库混乱。如果您不打算将此设备放回数据库，您可以安全地删除此文件。 UninstallWinClient.exe 在 ManagementSuite 共享文件夹中。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产品代理。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服务器的两个实例。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。

注意：默认情况下，卸载代理后，Uninstallwinclient.exe 将重新启动设备。如果不想重新启动，就在命令行添加 /noreboot 开关。

卸载核心服务器

从网络中卸载产品的最后一步是从核心服务器上卸载该软件。在此之前，确保已从服务器卸载了产品软件代理。

卸载核心服务器

1. 转到核心服务器。
2. 单击**开始|设置|控制面板**，然后双击**添加/删除程序**。
3. 如果尚未安装，请选择 Intel Platform Extensions for LANDesk software，然后单击添加/删除。
4. 要卸载产品软件，请选择 LANDesksoftware。
5. 单击**添加/删除**。

卸载核心数据库
您需要手动卸载核心数据库。

卸载核心数据库

默认情况下，卸载 LANDesk® System Manager 时不会卸载核心数据库。重要说明：如果您稍后将在计算机上重新安装 LANDesk® System Manager，则请不要卸载核心数据库。

卸载核心数据库

1. 转到核心服务器。
2. 单击**开始|设置|控制面板**，然后双击**添加/删除程序**。
3. 要卸载核心数据库，请选择 Microsoft SQL Server Desktop Engine (LDMSDATA)。
4. 单击**添加/删除**。

数据库文件
删除 Microsoft SQL Server Desktop Engine 将不会删除 LANDesk® System Manager 使用的数据库文件。除了占用磁盘空间外，在计算机上保留数据库文件不会有任何危害。如果要手动删除这些数据库文件，可删除 \ProgramFiles\Microsoft SQL Server\MSSQL$LDMSDATA\Data 文件夹中的内容。

支持

您可访问 LANDesk Software 在 Web 上提供的在线支持服务（仅限英语）。支持服务中包含有关 LANDesk Software 产品的最新信息。您还可找到安装说明、故障排除技巧、软件更新以及客户支持信息。请访问下面的网站，然后访问产品网页：

http://www.landesk.com/support/index.php

您还可以下载最新版本的发行说明和文档，其中包含的信息可能在产品出售时尚未发布。如果您是从 OEM 制造商收到 System Manager，请联系相应的支持服务。

如果本指南或 LANDesk Software 的 Web 支持站点无法帮助您解决所遇到的问题，LANDesk Software 还提供了一系列的有偿支持、咨询和合作伙伴服务。有关详细信息，请访问以下客户支持网页：

http://www.landesk.com/wheretobuy/

在致电客户支持部门寻求帮助之前，请准备好以下信息或资料：

- 您的姓名、公司名称和所使用的产品的版本。
- 您所使用的网络操作系统（名称及版本）。
- 您已安装的所有修补程序或 Service Pack。
- 重现问题的详细步骤。
- 针对该问题已采取的措施。
- 您的系统所独有、但可能有助于客户支持部门的工程师了解问题起因的任何信息。例如，您使用的是哪种数据库应用程序，安装的是哪个品牌的显卡，所使用的计算机的厂家和型号等。