LANDesk® System Manager 8.7

Installationsund- Verteilungshandbuch

LANDesk®

v8.5

Dieses Dokument stellt weder als Ganzes noch in Teilen eine ausdrückliche oder konkludente Garantie, Gewährleistung oder Lizenz dar. LANDesk übernimmt keinerlei Haftung für jegliche Garantien, Gewährleistungen und Lizenzen, einschließlich der Folgenden, ohne darauf beschränkt zu sein: Eignung zu einem bestimmten Zweck, Handelsüblichkeit, Nichtverletzung von Rechten am geistigen Eigentum oder anderer Rechte Dritter oder von LANDesk, Entschädigung und alles Übrige. Produkte von LANDesk sind nicht für den Einsatz in medizinischen, lebensrettenden oder lebenserhaltenden Apparaturen bestimmt. Der Leser wird darauf hingewiesen, dass Dritte Rechte am geistigen Eigentum besitzen können, die für dieses Dokument und die darin erläuterten Technologien relevant sein können, und dass er sich in rechtlichen Fragen an eine qualifizierte Rechtsberatung wenden soll, ohne dass LANDesk hierfür Verpflichtungen übernimmt.

LANDesk behält sich das Recht vor, dieses Dokument oder damit in Verbindung stehende Produktspezifikationen und -beschreibungen jederzeit ohne vorherige Ankündigung zu ändern. LANDesk gewährt keine Garantie für die Verwendung dieses Dokuments und übernimmt keine Haftung für Fehler, die möglicherweise in diesem Dokument enthalten sind. LANDesk verpflichtet sich auch nicht, die in diesem Dokument enthaltenen Informationen zu aktualisieren.

Inhalt

Übersicht

Dieses Handbuch unterstützt Sie bei der Durchführung der Schritte zur Installation und Bereitstellung von LANDesk® System Manager. Das Produkt vereinfacht die Computerverwaltung und Behebung gängiger Computerprobleme und hilft Ihnen, die Gesamtbesitzkosten (Total Cost of Owernship) zu reduzieren.

Diese Übersicht enthält Informationen zu den folgenden Themen:

- Funktionen in diesem Release
- Einführung in das Produkt (einschließlich Grundbegriffe)
- Installations- und Bereitstellungsstrategien
- Übersicht über Installation und Bereitstellung

Funktionen in diesem Release

Mit der zunehmenden Bedeutung der Computerindustrie sind auch Computersysteme heute komplexer und schwerer zu verwalten. Der mit der Wartung und Reparatur eines Computers verbundene Zeitaufwand kann während der vielen Jahre seiner Nutzung die Gesamtbesitzkosten weit über den ursprünglichen Anschaffungspreis hinaus ansteigen lassen. LANDesk® System Manager vereinfacht die Verwaltung und Behebung gängiger Computerprobleme und hilft auf diese Weise, die Gesamtbesitzkosten zu reduzieren.

- **Anzeigen des Systeminventars:** System Manager bietet eine umfassende Übersicht über die Hardware- und Softwarekonfiguration des Computers.
- **Überwachen des Systemzustands:** System Manager meldet, wenn der Computer einen bedenklichen oder kritischen Zustand erreicht; die Berichterstattung bezieht sich auf Leistungsdaten wie Temperatur, Spannung, freier Speicher und Datenträgerkapazität.
- **Alarmierung bei Systemereignissen:** System Manager kann Sie mithilfe mehrerer Alarmmethoden beim Auftreten von Problemen benachrichtigen.
- **Echtzeit- oder Vergangenheitsdaten:** System Manager gibt Ihnen die Möglichkeit, die Leistung mehrerer Systemobjekte wie Laufwerke, Prozessoren, Speicher und Dienste zu überwachen. Sie können Alarmaktionen festlegen, die eine Benachrichtigung auslösen, wenn der obere oder untere Grenzwert eines angegebenen Zählers häufiger als zulässig überschritten wird.
- **Überwachen aktueller Prozesse und Dienste:** Sie können mit System Manager aktuelle Dienste und deren Status anzeigen oder Alarmaktionen konfigurieren, die Sie darauf hinweisen, wenn sich der Status eines Dienstes ändert.
- **Herunterfahren, Hochfahren und Neustart über eine Remote-Verbindung:** Mit System Manager können Sie von der Administratorkonsole aus Remote-Power-Management-Befehle für Systeme erteilen, die diese Funktionalität unterstützen.
- **Ansicht "Geplanter Task":** Zentrale Konsole zum Anzeigen oder Ändern aller Tasks zur Agentenbereitstellungen sowie aller Erkennungs- und
- **Erweiterte Betriebssystemunterstützung:** Verwalten Sie alle Geräte in Ihrer heterogenen Umgebung über eine zentrale Konsole. Unterstützt Windows 2000, 2003 und XP Professional, Red Hat Linux, SUSE Linux, HP-UX und AIX. Weitere Informationen finden Sie in Stufe 1: Systemanforderungen.

- **Support für Intel* AMT und Intelligent Platform Management Interface (IPMI):** System Manager unterstützt Hardware-basierte Verwaltungskomponenten, mit denen vernetzte Geräte an einem entfernten Standort in jedem Systemzustand über Out-of-Band (OOB)-Kommunikation verwaltet werden können. Solange das Gerät mit einem Unternehmensnetzwerk verbunden ist und über Standby-Strom verfügt, können Sie auf das Inventar zugreifen, Remote-Diagnosedaten anzeigen und das System remote neu starten.
- **Unterstützung für Blade-Server:** Unterstützung für Blade-Server und Blade-Gehäuse-Verwaltungsmodule (CMMs, Chassis Management Modules), einschließlich Verwaltungs- und Inventarfunktionen.
- **Tool für die Skripterstellung:** Sie können benutzerdefinierte Tasks planen und ausführen
- **Taskplaner:** Ein zentrales Datenbankschema mit verbesserter Datenintegrität und Skalierbarkeit ermöglicht Ihnen den Zugriff auf umfassende Informationen zu verwalteten Geräten (einschließlich vollständiger Integration mit Management Suite). Teil dieses zentralen Schemas ist der Taskplaner. Alle Tasks (Agentenkonfiguration, können in einem gemeinsamen Fenster angezeigt werden. Von diesem Fenster aus können Sie Termine verlegen, den Zeitplan ändern oder periodisch wiederkehrend konfigurieren.
- **Rollenbasierte Administration:** Konfigurieren Sie den Benutzerzugriff auf Tools und Netzwerkgeräte basierend auf der administrativen Rolle eines Benutzers in Ihrem Unternehmen. In der rollenbasierten Administration entscheiden Sie mithilfe von Bereichen, welche Geräte bestimmte Benutzer anzeigen und verwalten können; darüber hinaus legen Sie durch die Erteilung von Nutzungsrechten fest, welche Tasks die Benutzer ausführen können.
- **Erkennung nicht verwalteter Geräte:** Erkennen Sie Geräte in Ihrem Netzwerk mit zahlreichen unterschiedlichen Methoden. Das Produkt erkennt Windows- oder Linux-Server, Blade-Server und Blade-Gehäuse, IPMI- sowie Intel AMT-kompatible Server sowie andere Netzwerkgeräte. Erstellen Sie einen Zeitplan für die fortlaufende Geräteerkennung, damit Sie stets über neue Geräte informiert werden. Außerdem können Sie Berichte zu den nicht verwalteten Geräten in Ihrem Netzwerk erstellen lassen.
- **Optimierte Sicherheit:** Ein zertifikatsbasiertes Sicherheitsmodell lässt Geräte nur mit autorisierten Core Servern und Konsolen kommunizieren.
- **Softwareverteilung:** Automatisieren Sie die Installation von Softwareanwendungen oder die Verteilung von Dateien an Geräte.
- **Berichte:** Vordefinierte Serviceberichte sind für die Planung und strategische Analyse verfügbar.
- **Unterstützung geplanter Tasks:** Stellen Sie mehrere für den Scheduler-Dienst zu authentifizierende Anmeldungen zur Verfügung, wenn Tasks auf Geräten ausgeführt werden, auf denen keine Agenten installiert sind. Dies ist besonders für die Verwaltung von Geräten in mehreren Windows-Domänen von Nutzen.

Einführung in das Produkt

System Manager verwaltet Geräte, auf denen mehrere unterschiedliche Betriebssysteme laufen, einschließlich Windows 2000 Pro SP4, Windows XP Pro SP1, Server unter Windows* 2000/2003, Server unter Red Hat Enterprise Linux v3, Server unter SUSE Linux 9 sowie Server unter HP-UX und AIX. Darüber hinaus stellt das Produkt eine gemeinsame Oberfläche für die Verwaltung der Geräte unter diesen Netzwerkbetriebssystemen bereit. Es ist darüber hinaus mit anderen LANDesk® Management Suite-Produkten kompatibel, z. B. LANDesk und LANDesk® Management Suite.

Bedeutung wichtiger Produktbegriffe

- **Core Server:** Der Mittelpunkt einer Verwaltungsdomäne. Alle Schlüsseldateien und Dienste des Produkts befinden sich auf dem Core Server. Eine Verwaltungsdomäne besitzt nur einen Core Server. Ein Core Server kann ein neuer Server sein oder Server, der einem anderen Zweck zugeführt wurde.
- **Konsole:** Die Browser-basierte Konsole ist die zentrale Benutzeroberfläche des Produkts.
- Core-Datenbank:Das Produkt erstellt eine MSDE-Datenbank auf dem Core Server, um Verwaltungsdaten zu speichern.
- **Verwaltete Geräte:** Geräte in Ihrem Netzwerk, auf denen Produktagenten installiert sind. Der Begriff Geräte umfasst Desktops, Server, Laptops/mobile Computer, Blade-Gehäuse usw. Core Server können mehrere Tausend Geräte verwalten.
- **Öffentlich:** Elemente, die für alle Benutzer sichtbar sind (z. B. Gruppen, Verteilungspakete oder Tasks). Wenn ein Benutzer ein öffentliches Element ändert, bleibt die Änderung öffentlich. Öffentliche Gruppen werden von einem Benutzer mit Administratorrechten erstellt.
- **Privat oder Benutzer:** Elemente, die vom derzeit angemeldeten Benutzer erstellt werden. Diese Gruppen sind für andere Benutzer nicht sichtbar. Private Elemente werden unter den Strukturansichten **Eigene Verteilungsmethoden**, **Eigene Pakete** und **Eigene Tasks** angezeigt. Benutzer mit Administratorrechten sehen private Gruppen sowie Benutzerpakete und -tasks.
- **Global:** Ein für andere Benutzer sichtbares Element. Wenn ein Benutzer Eigentümer eines globalen Elements wird (indem er es bearbeitet), wird das Element in zwei Elemente geteilt: Das globale Elemente bleibt bestehen und ein Benutzerelement wird im Ordner "Benutzer" gespeichert. Die Benutzerinstanz des Elements ist nicht mehr für andere Benutzer sichtbar. Ein Benutzer kann jeden für ihn sichtbaren Task als globalen Task kennzeichnen, um ihn auf diese Weise mit anderen Benutzern gemeinsam zu verwenden. Sobald ein Benutzer die Option "Global" in den Eigenschaften des Elements aktiviert, wird der Task nur noch in der Gruppe "Benutzertasks" des betreffenden Benutzers angezeigt.

Wie passt das Produkt in mein Netzwerk?

Dieses Produkt nutzt die Infrastruktur Ihres bestehenden Netzwerks, um Verbindungen mit den Geräten herzustellen, die vom Produkt verwaltet werden. Die Verwaltung Ihrer vorhandenen Geräte wird spürbar vereinfacht, ganz gleich, ob Sie ein kleines Netzwerk oder eine große Unternehmensumgebung zu betreuen haben.

Zur Verwendung von System Manager mit Management Suite oder Server Manager

Wenn Sie Management Suite installiert haben und zusammen mit Server Manager oder System Manager verwenden möchten, müssen Sie mithilfe des Core Server-Aktivierungsprogramms einen gültigen Benutzernamen und ein Kennwort für das Produkt bereitstellen, das Sie mit System Manager verwenden möchten. Mit einer System Manager/Management Suite-Installation werden Ihnen drei Arbeitskonsolen zur Verfügung gestellt. Die Management Suite Windows 32- und Webkonsolen sowie die System Manager-Webkonsole. Die Management Suite-Konsole enthält drei Navigationselemente (Alarmierung, Überwachung und Protokolle). Diese Elemente enthalten Funktionen, die in den beiden Server Manager-Konsolen nicht bereitgestellt werden.

Wenn Sie Management Suite bereitstellen, entfernt die Management Suite-Installation den System Manager-Agenten auf verwalteten Geräten und umgekehrt. Wenn Management Suite mit System Manager ausgeführt wird, beinhaltet die Management Suite-Konfigurationsfunktion Verwaltungsoptionen.

Installieren von System Manager mit bereits installiertem Management Suite oder Server Manager

Wenn Sie bereits Server Manager oder Management Suite auf Ihrem Core Server installiert haben und jetzt noch Server Manager hinzufügen möchten, sollten Sie dieselbe Installation verwenden, die Sie für die ursprüngliche System Manager- oder Management Suite-Installation verwendet haben.

1. Öffnen Sie autorun.exe.
2. Klicken Sie auf **Jetzt installieren**.
3. Wählen Sie eine Sprache aus und klicken Sie auf **OK**.
4. Der Begrüßungsbildschirm wird eingeblendet. Klicken Sie auf **Weiter**.
5. Wählen Sie **Ändern** aus (falls erforderlich) und klicken Sie auf **Weiter**.
6. Klicken Sie auf LANDesk® Server Manager und dann auf **Weiter**.
7. Folgen Sie den Bildschirmanweisungen des Assistenten.

Systemanforderungen für Core Server

Bei der Auswahl eines Servers als Core Server müssen Sie sicherstellen, dass der ausgewählte Server die in "Stufe 1: Systemanforderungen" aufgeführten Systemanforderungen erfüllt oder übertrifft. Der Checker für Systemanforderungen übernimmt diese Aufgabe automatisch für Sie.

Ein fest zugeordneter Server wird dringend empfohlen
Aufgrund des Datenaufkommens, das der Core Server für die Verwaltung Ihrer Domäne verarbeiten muss, wird dringend empfohlen, jeden Core Server als fest zugeordneten Hostserver für das Produkt einzurichten.

Wenn Sie andere Produkte auf demselben Server installieren, können kurz- oder langfristig Ressourcenprobleme auftreten.

Installieren Sie die Core Server-Komponenten nicht auf einem primären Domänencontroller oder Active Directory-Controller.

Installations- und Bereitstellungsstrategien

Beim Installieren unter Verwendung des Autorun-Befehls vom Datenträger des Produkts aus stellt das Installationsprogramm automatisch sicher, dass Ihr Core Server diese Anforderungen erfüllt. Die Installation und Bereitstellung einer systemweiten Anwendung in einem heterogenen Netzwerk setzt im *Vorfeld* der eigentlichen Installation des Produkts das Ausarbeiten einer durchdachten Strategie und umfassendes Planen voraus. In diesem Handbuch werden Strategien zum Einrichten des Produkts beschrieben. Bevor Sie es bereitstellen, müssen Sie zunächst Ihren Verwaltungsbedarf bestimmen.

Überlegungen zur Bereitstellungsstrategie

Mit Bereitstellung ist der Prozess gemeint, bei dem Verwaltungsfunktionen auf Server übertragen werden, die in die Domäne aufgenommen werden sollen. In diesem Handbuch wird die Bereitstellung als ein mehrere Stufen umfassender Vorgang beschrieben.

Der Ansatz der stufenweisen Bereitstellung ermöglicht ein systematisches Vorgehen beim Aktivieren der Verwaltung auf Geräten. Der Ansatz beruht auf zwei einfachen Grundsätzen:

- Erstens: Stellen Sie zuerst die Produktkomponenten bereit, die Ihr bestehendes Netzwerk am wenigsten beeinträchtigen, und zuletzt die Komponenten, die die größten Auswirkungen haben.
- Zweitens: Stellen Sie das Produkt in sorgfältig geplanten Stufen bereit, anstatt alle Dienste auf einmal bereitzustellen, was eine eventuell erforderliche Fehlerbehebung erschweren würde.

Dieses Handbuch ist sequentiell aufgebaut, um auf diese Weise die Bereitstellung des Produkts für Sie zu vereinfachen. Beginnen Sie mit dem ersten Kapitel Stufe 1: Entwerfen einer Verwaltungsdomäne weiter unten in diesem Handbuch. Anschließend sollten Sie jede Stufe nacheinander ausführen.

Übersicht über Installation und Bereitstellung

In diesem Handbuch sind die Installations- und Bereitstellungsaufgaben in die im Folgenden beschriebenen Stufen eingeteilt. Für jede Stufe gibt es einen entsprechenden Abschnitt in diesem Handbuch, der Sie durch diesen Teil der Installation führt. Das Kapitel zielt darauf ab, Sie so schnell wie möglich mit dem Produkt vertraut zu machen, indem Sie Dienste konfigurieren, die Konsole ausführen, Geräte erkennen, die Geräte in die Liste "Eigene Geräte" verschieben und die verwalteten Geräte für die Durchführung von Aktionen konfigurieren. Es ist als kompakte Einstiegshilfe gedacht und geht von der Annahme aus, dass Sie bei Detailfragen die übrigen Kapitel des Buches als Referenz verwenden. Einige der Verfahren, die in diesem Handbuch beschrieben werden, werden im Kapitel "Erste Schritte" wiederholt.

Übersicht über Stufe 1

In Stufe 1 der Installation erstellen Sie die Verwaltungsdomäne, indem Sie folgende Aufgaben ausführen:

- Sammeln von Netzwerkinformationen
- Sicherstellen, dass das Netzwerk den Systemanforderungen entspricht

Einzelheiten finden Sie unter Stufe 1: Entwerfen einer Verwaltungsdomäne weiter unten in diesem Handbuch.

Übersicht über Stufe 2

In Stufe 2 installieren Sie das Produkt, indem Sie folgende Aufgaben ausführen:

- Installieren des Core Servers

Einzelheiten finden Sie unter Stufe2: Installieren von Core und Konsole weiter unten in diesem Handbuch.

Übersicht über Stufe 3

In Stufe 3 der Installation verwenden Sie die Geräteerkennung in Ihrem Netzwerk und stellen die Produktagenten bereit. Sie können die Agenten von der Konsole aus als Pull-Task verteilen oder aus der Serverfreigabe mit einem Pull-Vorgang abrufen.

Einzelheiten finden Sie unter Stufe3: Bereitstellen der Agenten auf Geräten weiter unten in diesem Handbuch.

Erste Schritte

Übersicht

Willkommen bei LANDesk® System Manager! Diese Standalone-Anwendung für die Geräteverwaltung unterstützt Sie gezielt und effizient bei der Verwaltung Ihrer Geräteumgebung und hilft Ihnen, Ihre wertvolle Zeit optimal zu nutzen. Diese Vorteile machen sich für Ihr Unternehmen in einer deutlicheren Reduzierung des Zeit- und Kostenaufwands bezahlt. Mit System Manager können Sie Geräte zentral verwalten und für die Durchführung von Aktionen wie Power Cycling, Anfälligkeitsanalysen oder das Konfigurieren von Alarmen zu Gruppen zusammenfassen. Darüber hinaus können Sie mit System Manager Probleme an entfernten Standorten lösen, Ihr Netzwerk schützen und die Geräte mithilfe aktueller Patches auf dem neuesten Stand halten.

Dieses Handbuch zielt darauf ab, Sie so schnell wie möglich mit System Manager vertraut zu machen, indem Sie Dienste konfigurieren, die Konsole ausführen, Geräte erkennen, Geräte in die Liste Eigene Geräte verschieben und verwaltete Geräte für auf ihnen auszuführende Aktionen konfigurieren.

System Manager ist eine Webanwendung, auf die Sie mit Ihrem Browser zugreifen und auf diese Weise Ihre Server von einer Remote-Arbeitsstation aus verwalten können. Sie verhält sich wie viele der Webanwendungen, mit denen Sie ggf. bereits vertraut sind, jedoch verfügt sie über mehrere erweiterte Windows-ähnliche Steuerelemente, die die Anwendung benutzerfreundlicher machen. Zeigen Sie beispielsweise mit dem Mauszeiger auf ein Steuerelement und doppelklicken Sie dann auf dieses Element oder klicken Sie mit der rechten Maustaste darauf (so wie in einer Windows-Anwendung). Beispiel: Sie können in der Liste Eigene Geräte auf einen Gerätenamen doppelklicken, um auf die spezifischen Informationen zu diesem Gerät zuzugreifen, oder Sie können mit der rechten Maustaste klicken, um verfügbare Aktionen anzuzeigen.

In den folgenden Schritten wird beschrieben, wie Sie System Manager in Betrieb nehmen, Geräte in Ihrem Netzwerk erkennen lassen, die in die Liste Eigene Geräte zu verschiebenden Server auswählen, Agenten bereitstellen und die Geräte dann als Ziel für die Bearbeitung mit unterschiedlichen Tasks auswählen.

Ausführen des Installationsprogramms

Wählen Sie während der Installation auf der Autorun-Seite LANDesk® System Manager aus. Genaue Anweisungen finden Sie unter Stufe 2 des Installations- und Bereitstellungshandbuchs.

Sobald Sie System Manager installiert haben, steht der Verwendung des Produkts nichts mehr im Wege. In den nachstehenden Abschnitten machen wir Sie mit mehreren obligatorischen Schritten vertraut: Ausführen des Core-Aktivierungsprogramms, Konfigurieren von Diensten, Erkennen von Computern, Isolieren der aktiv zu verwaltenden Geräte durch Verschieben der Geräte in die Liste Eigene Geräte, Gruppieren von Geräten, Hinzufügen von Benutzern und Bereitstellen von Agenten. Sobald diese Aufgaben abgeschlossen sind, sind Sie bereit, die leistungsstarken und zuverlässigen Funktionen von System Manager kennenzulernen und zur Verwaltung Ihrer Geräte einzusetzen.

Aktivieren des Core Servers

Sie können das Produkt erst ausführen, nachdem Sie den Core Server aktiviert haben.

Verwenden Sie das Core Server-Aktivierungsprogramm für folgende Aufgaben:

- Erstmalige Aktivierung eines neuen System Manager Core Servers.
- Aktualisieren eines vorhandenen System Manager Core Servers

Jeder Core Server benötigt ein eindeutiges Autorisierungszertifikat.

Dieses Dienstprogramm wird beim ersten Neustart automatisch ausgeführt.

Verbinden Sie den Core Server mit dem Internet und führen Sie folgende Schritte aus:

1. Klicken **Sie auf Start | Alle Programme | Core Server-Aktivierung**. Der Benutzername und das Kennwort werden ausgefüllt.
2. Klicken Sie auf **Aktivieren**.

Der Core kommuniziert mit dem Software-Lizenzserver über HTTP. Wenn Sie einen Proxy-Server verwenden, klicken Sie auf die Registerkarte Proxy und geben die erforderlichen Proxy-Informationen ein. Wenn Ihr Core mit dem Internet verbunden ist, wird die Kommunikationsverbindung mit dem Lizenzserver automatisch, d.h. ohne Ihr Eingreifen, hergestellt. Wenn keine Verbindung mit dem Core besteht, klicken Sie beim Neustart auf Schließen und senden die Autorisierungsdatei an licensing@landesk.com.

Der Core Server hinterlegt in regelmäßigen Abständen Verifizierungsdaten zur Knotenzahl in der Datei "\Program Files\LANDesk\Authorization Files\LANDesk.usage". Diese Datei wird in regelmäßigen Abständen an den LANDesk Software-Lizenzserver gesendet. Die Datei wird im XML-Format erstellt und digital signiert und verschlüsselt. Jegliche Änderungen, die manuell an dieser Datei vorgenommen werden, machen ihren Inhalt und den nächsten Nutzungsbericht an den Software-Lizenzserver ungültig.

- Das Core Server-Aktivierungsprogramm startet keine DFÜ-Verbindung automatisch. Wenn Sie die DFÜ-Verbindung jedoch manuell starten und dann das Aktivierungsprogramm ausführen, kann das Programm die Daten zur Nutzung auch über eine DFÜ-Verbindung weiterleiten.

- Sie können den Core Server auch per E-Mail aktivieren. Senden Sie die Datei mit der Erweiterung .TXT, die Sie unter Programme\LANDesk\Authorization finden, an licensing@landesk.com. Der Kundensupport von LANDesk beantwortet die E-Mail mit einer Datei und mit Anweisungen zum Kopieren der Datei auf den Core Server. Dieser Vorgang bildet den Abschluss des Aktivierungsprozesses.

Hinzufügen von Benutzern

System Manager Benutzer sind Benutzer, die sich an der Konsole anmelden und bestimmte Aufgaben für bestimmte Geräte im Netzwerk ausführen können. Sie werden mithilfe der rollenbasierten Administrationsfunktion verwaltet. Mithilfe der rollenbasierten Administration können Sie Benutzern des Produkts, abhängig von ihren Rechten und ihrem Bereich, administrative Rollen zuweisen. Die Rechte legen fest, welche Produkt-Tools und -Funktionen der Benutzer sehen und verwenden kann. Der Bereich bestimmt, welche Geräte der Benutzer sehen und verwalten kann. Sie können eine Vielzahl von unterschiedlichen Benutzern erstellen und deren Rechte und Bereiche an Ihre Verwaltungsanforderungen anpassen. Sie können beispielsweise einen Benutzer erstellen, der die Help Desk-Aufgabe wahrnimmt, indem Sie diesem Benutzer die für diese Rolle erforderlichen Rechte erteilen. Zu diesem Thema finden Sie ausführliche Informationen im Kapitel "Rollenbasierte Administration" desSystem Manager Benutzerhandbuchs.

Beim Installieren des Produkts werden automatisch zwei Benutzerkonten erstellt (siehe unten). Sie können nach Bedarf weitere Benutzer manuell hinzufügen. Benutzer werden nicht in der Konsole erstellt. Sie werden stattdessen in der Gruppe "Benutzer" angezeigt (im linken Navigationsfenster auf Benutzer klicken), nachdem sie der LANDesk Management Suite-Gruppe in der Windows NT-Benutzerumgebung auf dem Core Server hinzugefügt wurden. Die Gruppe "Benutzer" zeigt alle Benutzer an, die gegenwärtig in der LANDesk Management Suite-Gruppe auf dem Core Server vorhanden sind.

Die Gruppe "Benutzer" umfasst zwei Standardbenutzer. Einer dieser beiden Benutzer ist der Standard-Administrator. Dies ist der Administrator, der während der Installation des Produkts am Server angemeldet war.

Der andere Benutzer ist der Standardvorlagenbenutzer.Dieser Benutzer verfügt über eine Vorlage mit Benutzereigenschaften (Rechte und Bereich), die zum Konfigurieren neuer Benutzer verwendet wird, wenn diese der Management Suite-Gruppe hinzugefügt werden. Wenn Sie also dieser Gruppe in der Windows NT-Umgebung einen Benutzer hinzufügen, erbt der Benutzer die Rechte und Bereiche, die aktuell in den Eigenschaften "Standardvorlagenbenutzer" definiert sind. Wenn Sie für den Standardvorlagenbenutzer alle Rechte und den "Standardbereich: Alle Rechner" ausgewählt haben, wird jeder neue Benutzer der LANDesk Management Suite-Gruppe der Gruppe "Benutzer" hinzugefügt (mit Rechten für alle Produkttools und mit Zugriff auf alle Geräte).

Sie können die Eigenschaftseinstellungen für den "Standardvorlagenbenutzer" ändern, indem Sie ihn auswählen und auf Bearbeiten klicken. Wenn Sie z.B. eine große Anzahl von Benutzern gleichzeitig hinzufügen möchten, von denen jedoch nicht alle Zugriff auf alle Tools oder Geräte haben sollen, ändern Sie zuerst die Einstellungen für den "Standardvorlagenbenutzer" und fügen dann die Benutzer zur LANDesk Management Suite-Gruppe hinzu (siehe unten beschriebene Schritte). Der "Standardvorlagenbenutzer" kann nicht entfernt werden.

Wenn Sie einen Benutzer zur LANDesk Management Suite-Gruppe in Windows NT hinzufügen, wird der Benutzer automatisch in die Gruppe "Benutzer" im Fenster Benutzer eingelesen und übernimmt dieselben Rechte und denselben Bereich wie der aktuelle "Standardvorlagenbenutzer". Es werden der Name, der Bereich und die Rechte des Benutzers angezeigt. Zusätzlich werden neue (nach der eindeutigen Anmelde-ID des Benutzers) benannte Benutzeruntergruppen in den Gruppen "Benutzergeräte", "Benutzerabfragen", "Benutzerberichte" und "Benutzerskripte" erstellt (beachten Sie, dass NUR ein Administrator Benutzergruppen anzeigen kann).

Umgekehrt wird ein Benutzer, den Sie aus der LANDesk Management Suite-Gruppe entfernen, nicht mehr in der Liste Benutzer angezeigt. Das Konto des Benutzers existiert weiterhin auf dem Core Server und kann jederzeit wieder der LANDesk Management Suite-Gruppe hinzugefügt werden. Außerdem bleiben die Benutzeruntergruppen unter "Benutzergeräte", "Benutzerabfragen", "Benutzerberichte" und "Benutzerskripte" erhalten, sodass Sie den Benutzer, ohne dessen Daten zu verlieren, wiederherstellen und Daten in andere Benutzer kopieren können.

Aktualisieren Sie den Frame Benutzerin der System Manager-Konsole, indem Sie die F5-Taste drücken. Um zu erfahren, wie Sie der LANDesk Management Suite-Gruppe einen Benutzer oder eine Domänengruppe hinzufügen oder ein neues Benutzerkonto erstellen, lesen Sie die Ausführungen unter "Hinzufügen von Produktbenutzern" die Ausführungen unter "Rollenbasierte Administration" im System Manager *Benutzerhandbuch*.

So fügen Sie einen Benutzer oder eine Domänengruppe der LANDesk Management Suite-Gruppe hinzu

1. Navigieren Sie zum Dienstprogramm **Verwaltung | Computerverwaltung | Lokale Benutzer und Gruppen | Gruppen** des Servers.
2. Klicken Sie mit der rechten Maustaste auf die **LANDesk Management Suite-Gruppe** und klicken Sie dann auf **Zur Gruppe hinzufügen**.
3. Klicken Sie auf **Hinzufügen**, geben Sie dann mindestens einen Benutzer ein bzw. wählen Sie mindestens einen Benutzer aus der Liste aus.
4. Klicken Sie auf **Hinzufügen** und dann auf **OK**.

Hinweis: Sie können der LANDesk Management Suite-Gruppe auch einen Benutzer hinzufügen, indem Sie mit der rechten Maustaste auf das Benutzerkonto in der Liste **Benutzer** klicken und dann auf **Eigenschaften | Mitglied von** sowie anschließend auf **Hinzufügen** klicken, um die Gruppe auszuwählen und den Benutzer hinzuzufügen.

Wenn noch keine Benutzerkonten auf dem Server existieren, müssen Sie sie erst erstellen.

So erstellen Sie ein neues Benutzerkonto

1. Navigieren Sie zum Dienstprogramm **Verwaltung | Computerverwaltung | Lokale Benutzer und Gruppe | Benutzer** des Servers.
2. Klicken Sie mit der rechten Maustaste auf **Benutzer** und klicken Sie dann auf **Neue Benutzer**.
3. Geben Sie im Dialogfeld **Neuer Benutzer** einen Namen und ein Kennwort ein.
4. Legen Sie die Kennworteinstellungen fest.
5. Klicken Sie auf **Erstellen**. Das Dialogfeld **Neuer Benutzer** bleibt geöffnet, sodass Sie zusätzliche Benutzer erstellen können.
6. Klicken Sie auf **Schließen**, um das Dialogfeld zu schließen.

Fügen Sie den Benutzer zur LANDesk Management Suite-Gruppe hinzu, damit er in der Gruppe "Benutzer" in der Konsole angezeigt wird.

Konfigurieren von Diensten und Berechtigungsnachweisen

Bevor Sie Geräte in Ihrem Netzwerk verwalten können, müssen Sie System Manager die erforderlichen Anmeldeinformationen zur Verfügung stellen. Geben Sie mithilfe des Dienstprogramms "Dienste konfigurieren" auf dem Core (SVCCFG.EXE) die erforderlichen Betriebssystem-, Intel* AMT- und IPMI BMC-Anmeldeinformationen an. Sie können außerdem zusätzliche Einstellungen angeben, beispielsweise Inventarstandards, PXE-Warteschlangeneinstellungen und LANDesk-Datenbankeinstellungen.

Verwenden Sie "Dienste konfigurieren", um Folgendes zu konfigurieren:

- Datenbankname, Benutzername und Kennwort. (Während der Installation festgelegt.)
- Anmeldeinformationen für das Planen von Jobs für verwaltete Geräte. (Sie können mehr als einen Satz Administratorberechtigungsnachweise eingeben.)
- Anmeldeinformationen zum Konfigurieren von IPMI BMCs. (Sie können nur einen Satz BMC-Berechtigungsnachweise eingeben.)
- Anmeldeinformationen zum Konfigurieren Intel AMT-kompatibler Geräte. (Sie können nur einen Satz Intel AMT-Anmeldeinformationen eingeben.)
- Scanintervall der Serversoftware, Wartung, Tage, die Inventarscans gespeichert bleiben, und Länge des Anmeldeprotokolls.
- Handhabung doppelt vorhandener Gerätekennungen.
- Scheduler-Konfiguration, einschließlich des Intervalls zwischen geplanten Aufträgen und Abfrageevaluierungen
- Benutzerdefinierte Auftragskonfiguration, einschließlich Timeout für die Remote-Ausführung.

1. Klicken Sie auf dem Core Server auf **Start | Alle Programme | LANDesk | LANDesk - Dienste konfigurieren**.
2. Klicken Sie auf die Registerkarte Scheduler.
3. Klicken **Sie auf Anmeldung ändern**.
4. Geben Sie die Anmeldeinformationen ein, die der Dienst auf den verwalteten Geräten verwenden soll, für gewöhnlich ein Domänenadministratorkonto.
5. Klicken **Sie auf Hinzufüge**n. Fügen Sie nach Bedarf weitere Anmeldeinformationen hinzu, wenn nicht auf allen verwalteten Geräten dieselben Administrator-Benutzernamenkonten aktiviert sind.
6. Klicken **Sie auf Übernehmen**.
7. Wenn es in Ihrer Umgebung IPMI-kompatible Server gibt, klicken Sie auf die Registerkarte BMC-Kennwort. Geben Sie ein Kennwort in das Textfeld Kennwort ein, geben Sie das Kennwort in das Textfeld Kennwort bestätigen erneut ein und klicken Sie dann auf OK. (Alle verwalteten IPMI-Server müssen denselben BMC-Benutzernamen und dasselbe BMC-Kennwort verwenden.)
8. Klicken **Sie bei Intel AMT**-aktivierten Geräten auf die Registerkarte Intel AMT-Konfiguration. Geben Sie den gegenwärtig konfigurierten Intel AMT-Benutzernamen in das Textfeld Benutzername und das aktuell konfigurierte Kennwort in das Textfeld Kennwort ein. Geben Sie das Kennwort erneut in der Textfeld Kennwort bestätigen ein und klicken Sie auf OK.

9. Definieren Sie nach Bedarf weitere Einstellungen, beispielsweise das Softwarescan-Intervall.
10. Klicken **Sie auf OK**, um die Änderungen zu speichern.

Klicken Sie auf **Hilfe** auf der jeweiligen Registerkarte "Dienste konfigurieren", um weitere Informationen zu erhalten.

Ausführen der Konsole

Mit dem umfassenden Tool-Angebot von System Manager können Sie die in Ihrem Netzwerk installierten Geräte anzeigen, konfigurieren, verwalten und schützen. Die Konsole ist der Zugriffspunkt für die Verwendung dieser Tools.

Im oberen Fensterausschnitt der Konsole sehen Sie den Server, bei dem Sie angemeldet sind, und den Benutzer, unter dem Sie sich angemeldet haben. Die Liste Eigene Geräte ist das Hauptfenster der Konsole und der Ausgangspunkt für die meisten Funktionen. Im linken Fensterausschnitt sind die verfügbaren Tools zu sehen. Im rechten Bereich der Konsole werden Dialogfelder und Bildschirme angezeigt, die zur Durchführung von Verwaltungsaufgaben dienen.

Der Vorteil der Konsole liegt darin, dass Sie ihre gesamten Funktionen aus der Ferne - beispielsweise von Ihrer Arbeitsstation aus - ausführen können; das heißt, Sie sparen sich zusätzliche Wege zum Serverraum oder müssen nicht mehr jedem einzelnen Gerät einen Besuch abstatten, um routinemäßige Wartungsaufgaben auszuführen oder Probleme zu beheben.

Es gibt drei Möglichkeiten, die Konsole zu starten:

- Klicken Sie auf dem Core **Server auf Start | Alle Programme | LANDesk |** System Manager.
- Geben Sie in einem Browser an einer Remote-Arbeitsstation die URL http://coreserver/LDSM ein.

Erkennen von Geräten

Verwenden Sie die Registerkarte **Erkennungskonfigurationen**, um neue Erkennungskonfigurationen zu erstellen, vorhandene Konfigurationen zu bearbeiten und zu löschen und eine Konfiguration für einen Erkennungsvorgang zu planen. Jede Erkennungskonfiguration besteht aus einem beschreibenden Namen, den zu scannenden IP-Bereichen und dem Erkennungstyp.

Nachdem Sie eine Konfiguration erstellt haben, können Sie mit dem Dialogfeld **Erkennung planen** festlegen, wann sie ausgeführt werden soll.

1. Klicken Sie im linken Navigationsfenster auf **Geräteerkennung**.
2. Klicken Sie auf der Registerkarte **Erkennungskonfigurationen** auf die Schaltfläche **Neu**.
3. Füllen Sie die unten beschriebenen Felder aus. Klicken Sie, nachdem Sie alle Daten eingegeben haben, auf die Schaltfläche **Hinzufügen** und dann auf **OK**.

Im Folgenden werden die einzelnen Abschnitte des Dialogfelds **Erkennungskonfiguration** beschrieben.

- **Konfigurationsname:** Geben Sie einen Namen für die Konfiguration ein. Geben Sie der Konfiguration einen einprägsamen Namen, den Sie sich leicht merken können. Die Konfiguration kann bis zu 255 Zeichen umfassen; folgende Zeichen sind unzulässig: **"**, **+**, **#**, **&** oder **%**. Der Konfigurationsname wird nach Verwendung eines dieser Zeichen nicht mehr angezeigt.
- **Standard-Netzwerkscan:** Diese Option sucht nach Geräten, indem sie ICMP-Pakete an die IP-Adressen in dem von Ihnen angegebenen Bereich sendet. Diese Suche ist am gründlichsten, verursacht jedoch auch den größten Zeitaufwand. Diese Option verwendet standardmäßig NetBIOS, um Informationen zum Gerät zu sammeln.

  Die Scanoption des Netzwerks verfügt über einen **IP-Fingerabdruck**, mit dem die Geräteerkennung versucht, den Betriebssystemtyp über TCP-Paketantworten ausfindig zu machen. Der IP-Fingerabdruck verlangsamt die Erkennung geringfügig.

  Die Scanoption des Netzwerks verfügt darüber hinaus über die Option **SNMP verwenden** , mit der Sie den Scan für die Verwendung von SNMP konfigurieren können. Klicken Sie auf **Konfigurieren**, um Informationen zu Ihrer SNMP-Konfiguration einzugeben.
- **LANDesk CBA-Erkennung:** Sucht nach dem Standard Management Agent (der frühere Common Base Agent [CBA] in Management Suite) auf Geräten. Mit dem Standard Management Agent kann der Core Server nach Clients im Netzwerk suchen und mit ihnen kommunizieren. Diese Option erkennt Geräte, auf denen Produktagenten installiert sind. Router blockieren durch den Standard Management Agent und PDS2 bedingten Datenverkehr. Um eine Standard-CBA-Erkennung über mehrere Subnetze hinweg durchzuführen, muss der Router so konfiguriert sein, dass an mehrere Subnetze gerichtete Broadcasts unterstützt werden.

  Die CBA-Erkennungsoption verfügt zudem über eine **LANDesk PDS2-Erkennungsoption**, mit der die Geräteerkennung nach dem LANDesk Ping Discovery Service (PDS2) auf Geräten sucht. LANDesk Softwareprodukte wie LANDesk® System Manager, Server Manager und LANDesk Client Manager verwenden den PDS2-Agenten. Wählen Sie diese Option aus, wenn es in Ihrem Netzwerk Geräte gibt, auf denen diese Produkte installiert sind. CBA-Erkennung wird für Linux-Rechner nicht unterstützt. Wenn Sie jedoch PDS2 auswählen, können Linux-Rechner, auf denen ein Agent installiert ist, erkannt werden.
- **IPMI:** Sucht nach IPMI-fähigen Servern. IPMI ist eine von Intel, ***** H-P,* NEC,* und Dell* entwickelte Norm, die die Nachrichten- und Systemschnittstelle für verwaltbare Hardwarebestandteile definiert. IPMI bietet Überwachungs- und Wiederherstellungsfunktionen, mit denen Sie auf diese Funktionen zugreifen können, ganz gleich, ob das Gerät eingeschaltet ist oder nicht, und in welchem Zustand das Betriebssystem sich befindet. Denken Sie daran, dass das Gerät nicht auf ASF-Pings reagiert, wenn der Baseboard Management Controller nicht konfiguriert ist. Das Produkt verwendet ASF-Pings zum Erkennen von IPMI. Das heißt, dass Sie das Produkt als normalen Computer erkennen lassen müssen. Beim Push-Bereitstellen des Clients durchsucht ServerConfig das System, erkennt das Gerät als IPMI und konfiguriert den BMC.
- **Servergehäuse:** Sucht nach Blade-Server Chassis Management Modules (CMMs). Die Blades in den Servern werden als normale Server erkannt.
- **Intel* AMT:** Sucht nach Geräten mit Intel Active Management Technology-Unterstützung.
- **Erste IP-Adresse:** Geben Sie die Start-IP-Adresse für den Adressbereich ein, den Sie überprüfen möchten.

- **Letzte IP-Adresse:** Geben Sie die Abschluss-IP-Adresse für den Adressbereich ein, den Sie überprüfen möchten.
- **Subnetzmaske:** Geben Sie die Subnetzmaske für den IP-Adressbereich ein, den Sie überprüfen möchten.
- **Hinzufügen:** Fügt den IP-Adressbereich in die Warteschlange im unteren Abschnitt des Dialogfelds ein.
- **Löschen:** Löscht den Inhalt der IP-Adressbereich-Felder.
- **Bearbeiten:** Wählen Sie einen IP-Adressbereich in der Arbeitswarteschlange aus und klicken Sie auf **Bearbeiten**. Der Bereich wird in den Textfelder oberhalb der Arbeitswarteschlange angezeigt. Sie können den Bereich dort bearbeiten und den neuen Bereich zur Arbeitswarteschlange hinzufügen.
- **Entfernen:** Entfernt den ausgewählten IP-Adressbereich aus der Arbeitswarteschlange.
- **Alle entfernen:** Entfernt alle IP-Adressbereiche aus der Warteschlange.

Nachdem Sie einen Erkennungstask konfiguriert haben, können Sie nun damit beginnen, die mit Ihrem Netzwerk verbundenen Geräte ausfindig zu machen, indem Sie festlegen, wann der Erkennungstask ausgeführt werden soll.

Planen und Ausführen des Erkennungstasks

Klicken Sie auf die Schaltfläche Zeitplan auf der Registerkarte Geräte erkennen, um das Dialogfeld Erkennung planen zu öffnen. Planen Sie mithilfe dieses Dialogfelds, wann eine Erkennung ausgeführt wird. Sie können festlegen, dass ein Erkennungstask sofort, zu einem späteren Zeitpunkt oder anhand eines Zeitplans (als regelmäßig wiederkehrender Vorgang) ausgeführt wird. Sie können die Option jedoch auch so konfigurieren, dass die Erkennung nur einmal ausgeführt wird, d.h., ohne eine etwaige Wiederholung zu einem späteren Zeitpunkt.

Nachdem Sie einen Erkennungstask geplant haben, können Sie sich auf der Registerkarte Erkennungstasks über den Status der Erkennung informieren. Die Planung eines wiederholt ausführenden Erkennungstasks ist hilfreich, da ein solcher Task Geräte, die im Netzwerk neu hinzukommen, automatisch erkennt.

Das Dialogfeld Erkennung planen beinhaltet folgende Optionen.

- **Ungeplant lassen:** Verknüpft den Task nicht mit einem Plan, belässt ihn jedoch in der Liste Erkennungsfunktionen, damit er nach Bedarf zu einem späteren Zeitpunkt zur Verfügung steht.
- **Jetzt starten:** Führt den Task so bald wie möglich aus. Es kann bis zu einer Minute dauern, bevor der Task gestartet wird.
- **Zum geplanten Zeitpunkt starten:** Startet den Task zu der von Ihnen angegebenen Uhrzeit. Wenn Sie auf diese Option klicken, müssen Sie Folgendes eingeben:
    - **Uhrzeit:** Die Uhrzeit für den Taskbeginn.
    - **Datum:** Das Datum für den Beginn des Tasks. Je nach lokalem Standard ist die Datumsreihenfolge entweder Tag-Monat-Jahr oder Monat-Tag-Jahr.
    - **Wiederholen alle:** Wenn der Task wiederholt werden soll, wählen Sie Täglich, Wöchentlich oder Monatlich aus. Wenn Sie "Monatlich" wählen und das Datum nicht in allen Monaten existiert (beispielsweise der 31.), wird der Task nur in den Monaten ausgeführt, in denen das Datum existiert.

So planen Sie einen Erkennungstask

1. Klicken **Sie im linken Navigationsfenster auf Erkannte Geräte**.
2. Wählen Sie auf der Registerkarte Erkennungskonfigurationen die gewünschte Konfiguration aus und klicken Sie auf Planen. Konfigurieren Sie den Erkennungsplan und klicken Sie auf Speichern.
3. Überwachen Sie den Fortschritt der Erkennung auf der Registerkarte Erkennungstasks. Klicken Sie auf Aktualisieren, um den Status zu aktualisieren.
4. Klicken Sie nach Abschluss des Erkennungsvorgangs auf Nicht verwaltet, um alle erkannten Geräte oben unter Erkannte Geräte einzublenden (der Fensterausschnitt aktualisiert sich nicht automatisch).

Anzeigen erkannter Geräte

Erkannte Geräte werden im Fensterausschnitt Erkannte Geräte nach Gerätetyp sortiert. Der Ordner Computer wird standardmäßig angezeigt. Klicken Sie auf die Ordner im linken Fensterausschnitt, um Geräte in unterschiedlichen Kategorien anzuzeigen. Klicken Sie auf Nicht verwaltet, um alle Geräte anzuzeigen, die von der Erkennung zurückgegeben werden.

- Blade-Server-Gehäuse werden im Ordner **Gehäuse** angezeigt.
- Standard-Enterprise-Geräte werden im Ordner **Computer** angezeigt.
- Router und andere Geräte werden im Ordner **Infrastruktur** angezeigt.
- Intel AMT-kompatible Geräte werden im Ordner **Intel AMT** angezeigt.
- IPMI-fähige Server werden im Ordner **IPMI** angezeigt.
- Geräte, die keiner Kategorie angehören, werden im Ordner **Andere** angezeigt.
- Drucker werden im Ordner **Drucker** angezeigt.

Hinweis: Für bestimmte Linux-Server wird ein allgemeines "Unix" als Betriebssystemname (oder manchmal sogar "Andere") angezeigt. Beim Bereitstellen des Standard Management Agent aktualisieren diese Server ihren Eintrag für den Betriebssystemnamen in der Liste **Eigene Geräte** und zeigen ein vollständiges Inventar an. So zeigen Sie erkannte Server an

1. Klicken Sie im linken Fensterausschnitt der Seite Geräteerkennung auf Computer oder einen anderen Gerätetyp, den Sie anzeigen möchten. Die Ergebnisse werden im rechten Fensterausschnitt angezeigt.
2. Klicken Sie zum Filtern der Ergebnisse auf das Filtersymbol, geben Sie mindestens einen Suchteil ein und klicken Sie auf Suchen.

Zuweisen von Namen

Bei einer Netzwerkscan-Erkennung geben manche Server einen leeren Knotennamen (oder Host-Namen) zurück. Dies passiert am häufigsten bei Servern, die Linux ausführen. Sie müssen dem Gerät einen Namen zuweisen, damit Sie es mit Verwalten in die Liste Eigene Geräte verschieben können.

1. Klicken Sie auf der Seite Geräteerkennung auf das Gerät, dessen Name leer ist. (Sie müssen auf den leeren Bereich in der Spalte mit den Knotennamen klicken.)
2. Klicken Sie auf Name zuweisen in der Symbolleiste.
3. Geben Sie den Namen ein und klicken Sie auf OK.

Wenn Sie einen Produktagenten auf einem Gerät installieren, scannt er automatisch den Hostnamen und aktualisiert die Core-Datenbank mit den korrekten Informationen.

Verschieben von Geräten in die Liste "Eigene Geräte"

Nach dem Erkennen von Geräten müssen Sie manuell die Zielgeräte auswählen, die Sie verwalten möchten und sie in die Liste Eigene Geräte verschieben. Durch das Verschieben der Geräts wird keine Software auf dem Gerät installiert. Die Geräte werden lediglich zum Abfragen, Gruppieren und Sortieren in der Liste Eigene Geräte zur Verfügung gestellt. Sie wählen bestimmte Geräte als "Ziel" für eine bestimmte Aktion aus; dieses Modell lässt sich mit dem "Einkaufswagenmodell" zahlreicher Webanwendungen vergleichen.

1. Klicken Sie in der Ansicht Erkannte Geräte auf das Gerät, das Sie in die Liste Eigene Geräte verschieben möchten. Mit UMSCHALT+Mausklick oder STRG+Mausklicken können Sie mehrere Geräte auswählen.
2. Klicken Sie auf die Schaltfläche Ziel. Falls diese Schaltfläche nicht zu sehen ist, klicken Sie in der Symbolleiste auf <<. Die Schaltfläche befindet sich ganz rechts. Oder klicken Sie mit der rechten Maustaste auf die ausgewählten Server und klicken Sie dann auf Ziel.
3. Klicken Sie im unteren Fensterbereich auf die Registerkarte Verwalten.
4. Wählen Sie die Option zum Verschieben ausgewählter Geräte in die Verwaltungsdatenbank oder zum Verschieben von Zielgeräten.
5. Klicken Sie auf Verschieben.

Durch Klicken auf Verschieben werden die Geräte in die Liste Eigene Geräte verschoben und die Gerätedaten in die Datenbank geschrieben. Sobald sich die Informationen in der Datenbank befinden, können Sie gefilterte Abfragen und Berichte erstellen (nach Gerätename, IP-Adresse oder Betriebssystem).

Gruppieren von Geräten für Aktionen

Es ist sinnvoll, Geräte zu Gruppen zusammenzufassen, beispielsweise nach Standort oder Funktion, damit Sie auf diesen Geräten Aktionen schneller ausführen können. Beispiel: Sie möchten die Prozessorgeschwindigkeit von Geräten eines bestimmten Standorts anzeigen.

1. Klicken Sie in der Liste Eigene Geräteauf Private Gruppenoder Öffentliche Gruppen und klicken Sie dann auf Gruppe hinzufügen.
2. Geben Sie einen Namen für die Gruppe in das Feld Gruppenname ein.
3. Klicken Sie auf den Gruppentyp, den Sie erstellen möchten.
    - **Statisch:** Geräte, die der Gruppe hinzugefügt wurden. Sie bleiben in der Gruppe, bis sie entfernt oder nicht mehr von Ihnen verwaltet werden.
    - **Dynamisch:** Geräte, die ein oder mehrere Kriterien erfüllen, die von einer Abfrage definiert wurden. Beispiel: Eine Gruppe kann alle Server beinhalten, die sich gegenwärtig in einem Warnzustand befinden. Sie bleiben in der Gruppe, solange sie die für die Gruppe definierten Kriterien erfüllen. Geräte werden automatisch dynamischen Gruppen hinzugefügt, wenn sie die Abfragekriterien der Gruppe erfüllen.
4. Klicken Sie abschließend auf **OK**.
5. Um Geräte einer statischen Gruppe hinzuzufügen, klicken Sie auf die Geräte im rechten Fensterausschnitt der Liste Eigene Geräte, klicken Sie auf Verschieben/Kopieren, wählen Sie die Gruppe aus und klicken Sie auf OK.

Konfigurieren von Geräten zum Verwalten mithilfe der Konsole

Das Erkennen der Geräte allein bedeutet noch nicht, dass diese Geräte einem zentralen Verwaltungsauftrag zugeordnet sind. Damit Sie Geräte vollständig mit der Konsole verwalten und Alarmmeldungen zum Zustand empfangen können, müssen Sie auf den betreffenden Servern Verwaltungsagenten installieren. Sie können die Standard-Agentenkonfiguration installieren (installiert alle Verwaltungsagenten) oder Sie können Ihre eigenen Agentenkonfigurationen anpassen, um sie auf Ihren Geräten zu installieren. (Die Agentenkonfiguration muss den Überwachungsagenten einschließen, um Warnmeldungen empfangen zu können.)

Verwaltungsagenten können mit einem der folgenden Verfahren installiert werden:

- Wählen Sie in der Liste Eigene Geräte Zielgeräte aus und planen Sie dann einen Konfigurationstask für Agenten, um Agenten über eine Fernsteuerungsverbindung auf den Geräten zu installieren. (siehe Schritte weiter unten)
- Erstellen Sie eine Zuordnung zur LDlogon-Freigabe des Cores (//coreserver/ldlogon) und führen Sie SERVERCONFIG.EXE aus. (Eine Beschreibung der hierfür erforderlichen Schritte finden Sie unter "Abrufen der Agenten mit einer Pull-Prozedur" im Kapitel "Installation und Konfiguration von Geräteagenten" des System Manager Benutzerhandbuchs)
- Erstellen Sie ein selbstextrahierendes Paket für die Geräteinstallation. Führen Sie dieses Paket lokal auf dem Gerät aus, um die Agenten zu installieren. Während dieses Vorgangs müssen Sie mit Administratorrechten angemeldet sein. (Eine Beschreibung der hierfür erforderlichen Schritte finden Sie unter "Installieren von Agenten mit einem Installationspaket" im Kapitel "Installation und Konfiguration von Geräteagenten" des System Manager Benutzerhandbuchs)

So stellen Sie den Agenten mit einer Push-Prozedur bereit

1. Wählen Sie Zielgeräte in der Liste Eigene Liste aus (wie oben unter "Verschieben von Geräten in die Liste "Eigene Geräte"" beschrieben)
2. Klicken Sie im linken Navigationsfenster auf Agentenkonfiguration, klicken Sie mit der rechten Maustaste auf die Konfiguration, die Sie mit einer Push-Prozedur bereitstellen möchten, und klicken Sie auf Task planen.
3. Klicken Sie im linken Fensterausschnitt auf Zielgeräte und klicken Sie dann auf die Schaltfläche Zielliste hinzufügen.
4. Klicken Sie auf Task planen, klicken Sie auf Jetzt starten, um den Task sofort zu starten, oder klicken Sie auf Später starten (und legen Sie Datum und Uhrzeit für den Start der Taskausführung fest) und klicken Sie auf Speichern.

Sie können den Taskstatus auf der Registerkarte Konfigurationstasks überprüfen.

Installieren von Linux-Serveragenten

Sie können Linux-Agenten und RPMs von einem Remote-Standort aus auf Linux-Servern bereitstellen und installieren. Ihr Linux-Server muss für diese Aufgabe richtig konfiguriert sein, da sie sich andernfalls nicht ausführen lässt. Hinweise zum ordnungsgemäßen Konfigurieren eines

Linux-Servers finden Sie unter "Installieren von Serveragenten" im Kapitel "Installation und Konfiguration von Geräteagenten" des *System Manager Benutzerhandbuchs.*

Einrichten von Alarmen

Wenn Probleme oder andere Ereignisse auf einem Gerät auftreten (z. B. eine Verknappung der Speicherressourcen des Geräts) kann System Manager einen Alarm senden. Sie können diese Alarme an Ihre Anforderungen anpassen, indem Sie den Schweregrad oder Grenzwert, der den Alarm auslösen wird, auswählen. Alarmmeldungen werden an die Konsole gesendet und lassen sich für die Ausführung spezifischer Aktionen konfigurieren. Sie können Alarme für zahlreiche unterschiedliche Ereignisse oder potenzielle Probleme definieren. Das Produkt umfasst einen Standard-Alarmregelsatz, der beim Installieren der Überwachungskomponenten auf dem verwalteten Gerät installiert wird. Dieser Alarm-Regelsatz leitet Feedback zum Systemzustand an das Konsole weiter. Dieser Standardregelsatz schließt u.a. folgende Alarme ein:

- Datenträger hinzugefügt oder entfernt
- Laufwerksspeicher
- Speichernutzung
- Temperatur, Lüfter und Spannung
- Leistungsüberwachung
- IPMI-Ereignisse (auf relevanter Hardware)

Weitere Informationen zur Alarmierung finden Sie im Kapitel "Alarmkonfiguration" des System Manager Benutzerhandbuchs.

Einrichten von Alarmen

Wenn Probleme oder andere Ereignisse auf einem Gerät auftreten (z.B. eine Verknappung der Speicherressourcen des Geräts) kann System Manager einen Alarm senden. Sie können diese Alarme an Ihre Anforderungen anpassen, indem Sie den Schweregrad oder Grenzwert, der den Alarm auslösen wird, auswählen. Alarmmeldungen werden an die Konsole gesendet und lassen sich für die Ausführung spezifischer Aktionen konfigurieren. Sie können Alarme für zahlreiche unterschiedliche Ereignisse oder potenzielle Probleme definieren. Das Produkt umfasst einen Standard-Alarmregelsatz, der beim Installieren der Überwachungskomponenten auf dem verwalteten Gerät installiert wird. Dieser Alarm-Regelsatz leitet Feedback zum Systemzustand an das Konsole weiter. Dieser Satz Standardregeln schließt u.a. folgende Alarme ein:

- Datenträger hinzugefügt oder entfernt
- Laufwerksspeicher
- Speichernutzung
- Temperatur, Lüfter und Spannung
- Leistungsüberwachung

Weitere Informationen zur Alarmierung finden Sie im Kapitel "Alarmkonfiguration" des System Manager *Benutzerhandbuchs*.

Wie geht´s weiter?

Sie haben Server Manager für den reibungslosen Betrieb konfiguriert. Dabei haben Sie nur einen Bruchteil der Funktionen kennengelernt, die in Server Manager zur Verfügung stehen (z. B. die

Geräteerkennung und Agentenkonfiguration). In den Begleithandbüchern (*Installations- und Bereitstellungshandbuch* und *Benutzerhandbuch*) können Sie sich ausführlich über alle Funktionen des Produkts informieren. Zu diesen Funktionen gehören:

Software-Updates: Sorgen Sie für fortlaufende Patchsicherheit auf allen verwalteten Geräten in Ihrem Netzwerk. Sie können mit diesem Tool die folgenden sich wiederholenden Prozesse automatisieren: Verwaltung aktueller Anfälligkeitsinformationen, Analyse der Anfälligkeit der verschiedenen Betriebssysteme, die auf den verwalteten Geräten ausgeführt werden, Herunterladen der relevanten ausführbaren Patchdateien, Reparieren von Anfälligkeiten durch die Verteilung und Installation notwendiger Patches auf Geräten und die Überprüfung des Patch-Installationserfolges.

Alarmierung: Stellen Sie sicher, dass Sie benachrichtigt werden, wenn ein Gerät einen bestimmten Grenzwert erreicht. In Zusammenarbeit mit dem Überwachungsfunktion kann die Alarmierung mit unterschiedlichen Verfahren benachrichtigen. Wenn Sie beispielsweise informiert werden möchten, wenn der Speicher auf Ihren Geräten eine Kapazitätsauslastung von 95% erreicht hat, können Sie auswählen, wie Sie über das Eintreten dieses Zustands informiert werden (der Agent kann eine E-Mail- oder Pager-Nachricht senden, ein Gerät neu starten oder herunterfahren oder Informationen in das Alarmprotokoll schreiben).

Abfragen: Verwalten Sie Ihr Netzwerk, indem Sie anhand bestimmter System- oder Benutzerkriterien nach Geräten in der Core-Datenbank suchen und sie entsprechend organisieren. Sie können eine Abfrage an die Liste der verwalteten Geräte richten, um die Geräte zu extrahieren zu machen, die den von Ihnen angegebenen Kriterien entsprechen (beispielsweise alle Geräte der Hauptniederlassung oder alle mit einer Arbeitsspeicherkapazität von 256 KB RAMI); anschließend können Sie diese Geräte zu Gruppen zusammenfassen und Aktionen ausführen. Diese Gruppen können statisch (die Mitglieder der Gruppe können nur manuell verwaltet werden) oder dynamisch sein (die Mitgliederzusammensetzung ändert sich, wenn Geräte bestimmte Kriterien erfüllen oder nicht erfüllen).

Softwareverteilung: Erstellen Sie Tasks zur Verteilung von Softwarepaketen (eine oder mehrere MSI-Dateien, eine Programmdatei, eine Batchdatei, RPM-Dateien (Linux) oder ein mit LANDesk Package Builder erstelltes Paket) auf Zielgeräten.

Überwachung: Überwachen Sie den Systemzustand eines Geräts mithilfe der unterstützten Überwachungsverfahren (direkte ASIC-Überwachung, In-Band IPMI, Out-of-Band IPMI, CIM usw.). Mithilfe der Überwachungsfunktion können Sie zahlreiche unterschiedliche Datenkategorien überwachen, beispielsweise die Anwendungsnutzung, Betriebssystemereignisse, Prozesse und Dienste, Vergangenheitsdaten und Hardwaresensoren (Lüfter, Spannung, Temperatur etc.). Die Alarmierung ist eine verwandte Funktion, die den Überwachungsagenten zur Initiierung von Alarmaktionen verwendet.

Berichte: Generieren Sie ein breites Spektrum an Spezialberichten, in denen kritische Informationen zu den verwalteten Geräten in Ihrem Netzwerk aufgezeichnet werden. Server Manager fügt mithilfe eines Inventarscanners Geräte (sowie erfasste Hardware- und Softwaredaten zu diesen Geräten) zur Core-Datenbank hinzu. Sie können diese Inventardaten von der Inventaransicht eines Geräts aus einsehen und drucken. Außerdem können Sie die Daten verwenden, um Abfragen zu definieren und Geräte zu Gruppen zusammenzufassen. Das Bericht-Tool nutzt diese gescannten Inventardaten zusätzlich, indem es die erfassten Daten in nützlichen Berichtformaten zusammenträgt und ordnet. Das kann sich beim Erfassen und Formatieren von Berichten zur vorschriftsmäßigen Nutzung als hilfreich erweisen.

Erkennung nicht verwalteter Geräte: Hiermit können Sie nach Geräten suchen, die nicht von der Konsole verwaltet werden. Das Identifizieren nicht verwalteter Geräte ist der erste Schritt für die Eingliederung neuer Geräte in ein verwaltetes System. Sie können einen Erkennungstask konfigurieren, der jeden Monat automatisch einen Scan zur Erkennung neuer Geräte ausführt.

Softwarelizenzüberwachung: Nachverfolgung der Lizenz-Compliance. Der Softwarelizenz-Überwachungsagent zeichnet Daten auf (beispielsweise die insgesamte Nutzung von Anwendung in Minuten, die Anzahl der Ausführungen und das Datum der letzten Ausführung für alle auf einem Gerät installierten Anwendungen) und speichert diese Daten in der Registrierung des Geräts. Diese Daten können von Ihnen für die Überwachung der Produktnutzung und Verdeutlichung von Verweigerungstrends genutzt werden. Der Agent überwacht passiv die Produktverwendung auf Geräten und belegt hierbei minimale Netzwerkbandbreite. Der Agent überwacht auch die Verwendung von Produkten auf mobilen Geräten, die nicht mit dem Netzwerk verbunden sind.

Betriebsystembereitstellung: Stellen Sie mithilfe des PXE-basierten Bereitstellungstools Betriebssystemabbilder auf den Geräten in Ihrem Netzwerk bereit. Mit dieser Funktionalität können Sie Abbilder von Geräten mit leeren Festplatten oder nicht funktionsfähigen Betriebssystemen erstellen. Dank der kompakten PXE-Repräsentanten benötigen Sie nicht mehr in jedem Subnetz einen fest zugeordneten PXE-Server. Die Betriebssystembereitstellung optimiert die Bereitstellung neuer Geräte, ohne dass während des Vorgangs zusätzliche Eingabeaufforderungen an den Endanwender oder IT-Abfragen eingeblendet werden.

Stufe 1: Entwerfen einer Verwaltungsdomäne

In Stufe 1 sammeln Sie Informationen zur Netzwerkinfrastruktur und treffen Entscheidungen, die Ihnen helfen, die Verwaltungsdomäne im Hinblick auf Ihre Anforderungen zu optimieren.

In dieser Stufe erhalten Sie Informationen zu den folgenden Themen:

Sammeln von Netzwerkinformationen

Identifizieren und sammeln Sie alle Netzwerkinformationen, die für System Manager relevant sind. Hierbei sind folgende Schritte besonders wichtig:

- Bestimmen der Gerätekonfigurationen
- Auswählen des Core Servers

Auswählen des Core Servers

Der Core Server ist der Mittelpunkt der Verwaltungsdomäne. Alle Schlüsseldatein und -dienste befinden sich auf dem Core Server. Es kann sich dabei um einen neuen Server handeln oder um einen Server, der einem neuen Zweck zugeführt wird.

Sie können die Administratorkonsole über einen Browser auf einer Remote-Arbeitsstation ausführen, auf der Sie Vorgänge ausführen wie das Verwalten von Alarmen, Ausführen von Abfragen für die Core-Datenbank oder Erstellen von benutzerdefinierten Skripten.

Stellen Sie sicher, dass der Server, den Sie als Core Server auswählen, die Systemanforderungen erfüllt. Weitere Informationen finden Sie unter "Systemanforderungen" weiter unten in dieser Stufe.

Planen der Platzierung von Programmdateien

Beim Installieren können Sie angeben, wo die Programmdateien installiert werden sollen. Übernehmen Sie die Standard-Zielverzeichnisse, sofern es keinen triftigen Grund gibt, sie zu ändern. Wenn Sie das Zielverzeichnis ändern, müssen Sie berücksichtigen, dass der Zielverzeichnispfad keine Doppelbyte-Zeichen enthalten darf.

Das Standardverzeichnis für Core Server-Dateien lautet:

```
C:\Programme\LANDesk\ManagementSuite
```

Die Core-Datenbank

System Manager installiert eine MSDE-Datenbank auf dem Core Server. Für jede MSDE-Datenbank gilt eine Größenbeschränkung von 2 GB. Wie viele Server von dieser Datenbank unterstützt werden, hängt von der Größe der Inventarscan-Datei Ihres Netzwerks ab.

Leistungsprobleme im Zusammenhang mit MSDE treten mit hoher Wahrscheinlichkeit auf, wenn die Datenbank mehr als fünf Aufgaben parallel ausführen muss. Wenn beispielsweise fünf System Manager-Administratoren zum exakt gleichen Zeitpunkt auf die Datenbank zugreifen.

Core-/Client-Sicherheit

Dieses Produkt arbeitet mit einem zertifkatsbasierten Authentifizierungssystem. Beim Installieren des Core Servers erstellt das Setup ein Zertifikat für diesen Core Server. Wenn Clients mit dem Core Server kommunizieren, suchen sie nach diesem Zertifikat. Wenn Clients für einen Core Server kein Zertifikat besitzen, können sie nicht mit ihm kommunizieren.

Geräte kommunizieren nur mit Core Servern, für die sie eine entsprechende vertrauenswürdige Zertifikatsdatei besitzen. Jeder Core Server besitzt ein eigenes Zertifikat und eigene private Schlüssel. Standardmäßig kommunizieren die Clientagenten, die Sie von den verschiedenen Core Servern verteilen, nur mit dem Core Server, von dem aus die Software verteilt wird.

Planen eines Bereichs

Die rollenbasierte Administration ist eine leistungsstarke Funktion für die Sicherheitsverwaltung. Öffnen Sie die Tools der rollenbasierten Administration in der Konsole, indem Sie im linken Fensterausschnitt auf "Benutzer" klicken. Sie müssen mit Administratorrechten angemeldet sein.

Die rollenbasierte Administration stellt komplexe Geräteverwaltungsfunktionen zur Verfügung, indem sie zulässt, dass Sie Benutzer zu Ihrem System hinzufügen und ihnen Rechte und Bereiche zuweisen können. Mit den Rechten wird festgelegt, welche Tools und Funktionen ein Benutzer sehen und verwenden kann (siehe "Erläuterungen zu Rechten" im Server Manager-Benutzerhandbuch). Der Bereich entscheidet, welchen Gerätebereich ein Benutzer sehen und verwalten kann (siehe "Erstellen von Bereichen" im Server Manager-Benutzerhandbuch).

Sie können Rollen erstellen, die auf dem Verantwortungsbereich der Benutzer basieren, auf den Verwaltungsaufgaben, die die Benutzer ausführen sollen, oder den Geräten, auf die die Benutzer zugreifen und die sie sehen und verwalten sollen. Der Zugriff auf Geräte kann auf einen geografischen Standort, z. B. ein Land, eine Region, eine Stadt oder einen spezifischen Benutzer oder Servertyp, beschränkt sein.

Um diese Art der rollenbasierten Administration netzwerkweit zu implementieren und zu erzwingen, richten Sie einfach aktuelle Benutzer ein; alternativ können Sie auch neue Benutzer als Produktbenutzer erstellen und hinzufügen und ihnen dann die erforderlichen Rechte (für Produktfunktionen) und Bereiche (für verwaltete Server) zuweisen.

Der Core Server legt mithilfe von Bereichen fest, welche Geräte für die Konsolenbenutzer sichtbar sind. Einem Benutzer können mehrere Bereiche zugewiesen und ein Bereich kann von mehreren Benutzern verwendet werden. Es gibt verschiedene Möglichkeiten, die Bereiche einzuschränken:

- (Standard) **Standardbereich: Alle Geräte:** Die Benutzer sehen alle Geräte.
- **Auf einer Abfrage basierend:** Benutzer können die Geräte sehen, die den ausgewählten Kriterien einer bestimmten, ihnen vom Administrator zugewiesenen Abfrage entsprechen.
- **Auf einer Gruppe basierend:** Die Benutzer sehen die Geräte, die die Gruppenkriterien erfüllen.

Weitere Informationen zu Bereichen finden Sie im Server Manager*Benutzerhandbuch*.

Systemanforderungen

Stellen Sie vor dem Ausführen des Installationsvorgangs sicher, dass folgende Systemanforderungen erfüllt sind. Der Checker für Systemanforderungen übernimmt diese Aufgabe für Sie.

Core- und Datenbankserver

Stellen Sie sicher, dass alle Core Server und Datenbankserver die in der Übersicht beschriebenen Anforderungen erfüllen.

- Windows 2000 Server oder Advanced Server mit SP 4 oder Windows Server 2003 Standard oder Enterprise Edition x86 SP1 oder Windows 2003 R2
- Microsoft Data Access Components (MDAC) 2.8 oder höher
- Microsoft .NET Framework 1.1
- Internet Information Services (IIS)
- IIS-Unterstützung für ASP.NET v1.1 Skripterstellung
- Internet Explorer 6.0 SP1 oder höher
- Microsoft NT File System (NTFS)
- Der als Core Server verwendete Windows-Server muss als eigenständiger Server und nicht als Primary Domain Controller (PDC), Backup Domain Controller (BDC) oder Active Directory-Controller installiert sein.
- SNMP muss installiert sein und SNMP- und SNMP-Trap-Dienste müssen gestartet werden.
- Sie müssen über 200 MB Speicher auf dem Systemlaufwerk und 900 MB Speicher auf mindestens einem Laufwerk verfügen.
- Administratorrechte
- LANDesk-Client ist entweder die korrekte Version oder nicht installiert

Core Server-Anforderungen
Die Windows-Auslagerungsdatei sollte mindestens 12 + *N* groß sein (*N* entspricht der verfügbaren RAM Megabyte auf dem Core Server). Andernfalls können Produktanwendungen Speicherfehler generieren.

Es wird empfohlen, auf dem Core-Rechner 1 Gigabyte Speicher bereitzustellen, falls Sie sowohl Server Manager- als auch Management Suite-Produkte auf demselben Core Server installieren möchten.

Alle auf einem Server gehosteten Produktdienste.

Für kleinere Verwaltungsdomänen können Sie den Core Server und die Core-Datenbank auf einem Server installieren. Bei diesen Netzwerken empfiehlt es sich, die Microsoft MSDE-Standarddatenbank zu verwenden, die in der Regel einfacher zu verwalten ist. Dies ist die einzige Datenbankoption für System Manager.

Einschränkungen

Stellen Sie vor dem Installieren von Core und Datenbank sicher, dass Ihr Server die folgenden Systemanforderungen erfüllt:

- Pentium 4-Prozessor
- 4 GB freier Speicherplatz auf Festplatten mit mindestens 10.000 RPM
- Mindestens 768 MB RAM

Verwaltete Server

Dieses Produkt unterstützt die folgenden Serverbetriebssysteme (nicht alle Betriebssysteme werden gleichermaßen unterstützt):

- Microsoft Windows 2000 Server (mit SP4)
- Microsoft Windows 2000 Advanced Server (mit SP4)
- Microsoft Windows 2000 Professional (mit SP4)
- Microsoft Windows 2003 Server R2
- Microsoft Windows 2003 Server R2 Standard Edition x86
- Microsoft Windows 2003 Server R2 Standard x64 Edition
- Microsoft Windows 2003 Server R2 Enterprise Edition x86
- Microsoft Windows 2003 Server R2 Enterprise x64 Edition
- Microsoft Windows XP Professional (mit SP2)
- Microsoft Windows XP Professional x64 (mit SP2)
- Windows Small Business Server 2000 (mit SP4)
- Windows Small Business Server 2003 (mit SP1)
- Red Hat Enterprise Linux v3 (ES) 32-Bit - U6
- Red Hat Enterprise Linux v3 (ES) EM64t - U6
- Red Hat Enterprise Linux v3 WS 32-Bit - U6
- Red Hat Enterprise Linux v3 WS EM64t - U6
- Red Hat Enterprise Linux v3 (AS) 32-bit - U6
- Red Hat Enterprise Linux v3 (AS) EM64t - U6
- Red Hat Enterprise Linux v4 (ES) 32-Bit – U3
- Red Hat Enterprise Linux v4 (ES) EM64t – U3
- Red Hat Enterprise Linux v4 (AS) 32-Bit – U3
- Red Hat Enterprise Linux v4 (AS) EM64t – U3
- Red Hat Enterprise Linux v4 WS 32-Bit – U3
- Red Hat Enterprise Linux v4 WS EM64t – U3
- SUSE* Linux Server 9 ES 32-Bit SP2
- SUSE Linux Server 9 EM64t SP2
- SUSE Linux Server 10 ES 32-bit

- SUSE Linux Server 10 EM64t
- SUSE Linux Professional 9.3
- SUSE Linux Professional 9.3 EM64t
- HP-UX 11.1
- Unix AIX

Verwaltete Linux-Server

In der folgenden Liste sind die Firewall- und RPM-Anforderungen aufgeführt, die erfüllt sein müssen, um Linux-Geräte verwaltungskonform zu machen.

Firewall

Um zunächst den Management Agent zu installieren und einen Linux-Server für die Kommunikation mit dem Core zu konfigurieren (mithilfe der "Push"-Methode), muss sichergestellt werden, dass SSH-Verbindungen die lokale Firewall des Linux-Servers passieren dürfen:

22 - nur TCP

Damit die Agenten mit dem/den Core Server(n) kommunizieren können (für Inventarscans, Softwareverteilung, Anfälligkeitsaktualisierungen usw.), muss die lokale Firewall des Linux-Server so konfiguriert werden, dass folgende Anschlüsse für die Kommunikation geöffnet sind:

9593 - nur TCP

9594 - nur TCP

9595 - TCP und UDP

Um mit dem Management Agent kommunizieren zu können, muss die lokale Firewall des Linux-Servers folgende Anschlüsse für die Kommunikation öffnen:

6780 - nur TCP

Erforderliche RPMs (ab Version #)

Es wird empfohlen, alle Produkt-RPMs im Verzeichnis "...\ManagementSuite\ldlogon\RPMS" zu installieren. Sie können in dieses Verzeichnis über http://core name/RPMS wechseln.

REDHAT_ENTERPRISE

python

RPM Version:2.2.3-5 (RH3)

2.3.4-14 (RH4)

Binärversion:2.2.3

pygtk2

RPM Version:1.99.16-8 (RH3)

2.4.0-1 (RH4)

Binärversion:

sudo

RPM-Version:1.6.7p5-1

Binärversion:1.6.7.p5

bash RPM Version:2.05b-29 (RH3)

3.0-19.2 (RH4)

Binärversion:2.05b.0(1)-release

xinetd RPM Version:2.3.12-2.3E (RH3)

2.3.13-4 (RH4)

Binärversion:2.3.12

mozilla RPM-Version: 1.7.3-18.EL4 (RH4)

Binärversion:1.5

openssl RPM-Version:0.9.7a-22.1 (RH3)

0.9.7a-43.1 (RH4)

Binärversion:0.9.7a

sysstat RPM-Version:4.0.7-4

Binärversion:4.0.7

lm_sensors

RPM-Version: 2.6 (diese Version ist u.U. nicht leistungsstark genug, um Sensoren auf neueren ASIC-Rechner anzuzeigen. Bitte lesen Sie die Informationen in der Dokumentation zu "lm_sensors" oder informieren Sie sich ausführlich auf der Website (http://www2.lm-sensors.nu/~lm78).

SUSE LINUX

(SUSE 64)

bash

RPM-Version: 2.05b-305.6

mozilla

RPM-Version: 1.6-74.14

net-snmp

RPM-Version: 5.1-80.9

openssl

RPM-Version: 0.9.7d-15.13

python-gtk

RPM-Version: 2.0.0-215.1 [Hinweis: Geänderter Paketname]

python

RPM-Version: 2.3.3-88.1

sudo

RPM-Version: 1.6.7p5-117.1

sysstat

RPM-Version: 5.0.1-35.1

xinetd

RPM-Version: 2.3.13-39.3

lm_sensors

RPM-Version: NA (Hinweis: wurde in den Kernel für die 2.6-Version eingearbeitet)

Vom Produkt verwendete Anschlüsse

Einführung

Wenn Sie dieses Produkt in einer Umgebung verwenden, die Firewalls einschließt (oder Router, die den Datenverkehr filtern), müssen Sie möglicherweise Firewall- oder Router-Konfigurationen anpassen, um die Funktionsfähigkeit des Produkts zu gewährleisten. Dieser Abschnitt beschreibt die von den einzelnen Produktkomponenten verwendeten Anschlüsse. Die hier angegebenen Informationen beziehen sich vor allem auf die Konfiguration von Routern und Firewalls. Nur lokal (in den einzelnen Subnetzen) verwendete Anschlüsse werden nicht besprochen.

Hintergrundinformationen zu Firewall-Regeln

Diese Informationen gelten für das Einrichten von Firewall-Regeln. Falls Sie sich mit diesem Thema noch nicht auskennen, finden Sie in diesem Abschnitt allgemeine Hintergrundinformationen zu den wichtigsten Konzepten.

Firewall-Regeln

Einen "Anschluss öffnen" ist nicht so einfach wie es klingt. Sie können nicht einfach zu einer Firewall gehen und "Anschluss x öffnen". Einen Anschluss zu öffnen bedeutet eigentlich, eine Firewall-Regel zu erstellen. Firewall-Regeln beschreiben, welche Netzwerkdaten die Firewall passieren dürfen und welche nicht. Die Firewall-Regel filtert den Netzwerkverkehr nicht nur nach der Anschlussnummer. Regeln können auf Protokollen, Quell- und Zielanschlussnummern, Richtung (ankommend/abgehend), Quell- und Ziel-IP-Adressen usw. basieren.

Eine typische Firewall-Regel sieht so aus: "ankommenden Verkehr an TCP Anschluss 9535 zulassen". Für dieses Produkt wird diese Regel als Unterstützung für die Fernsteuerung benötigt. Die Regel basiert auf drei Elementen:

1. Dem Protokoll (TCP oder UDP)
2. Der Anschlussnummer
3. Der Richtung (ankommend oder abgehend)

Diese drei Elemente werden zum Einrichten von Firewall-Regeln benötigt.

Quell- und Zielanschlüsse, dynamische Anschlüsse

An der TCP- oder UDP-Kommunikation sind immer zwei Anschlüsse beteiligt. Alle TCP- oder UDP-Pakete gehen von einem Quellanschluss an einen Zielanschluss. Firewall-Regeln können auf dem Quellanschluss, dem Zielanschluss oder beiden basieren. Die in Dokumenten wie dem vorliegenden angegebenen Anschlüsse sind immer Zielanschlüsse.

Bekannte Anschlüsse wie 5007 (vom Inventardienst verwendet) beziehen sich nur auf eine Seite der Kommunikation. Für die andere Seite der Kommunikation wird ein dynamischer Anschluss verwendet. Dynamische Anschlüsse werden automatisch vom Betriebssystem im Bereich 1024 bis 5000 zugeordnet.

Firewalls und UDP-Verkehr

Um TCP-Verkehr durch eine Firewall (z. B. ankommende TCP-Verbindungen an Anschluss 5007) passieren zu lassen, genügt eine einzelne Regel. Sobald die TCP-Verbindung hergestellt ist, können Daten über diese Verbindung in beide Richtungen fließen.

Bei UDP-Verkehr ist das anders, da hier keine Verbindung besteht. Der Core Server unterzieht z. B. standardmäßig Geräte am UDP-Anschluss 38293 einem Ping-Test, bevor er einen Task startet. Eine Firewall-Regel, die abgehende UDP-Pakete an Anschluss 38293 zulässt, erlaubt ebenfalls Pakete vom Core Server an Geräte außerhalb der Firewall, jedoch nicht die Antwortpakete des jeweiligen Pakets.

Eine Regel, die sowohl abgehende als auch ankommende Pakete an Anschluss 38293 erlaubt, funktioniert ebenfalls nicht, da eine Seite der Kommunikation am bekannten Anschluss mithört. Die andere Seite verwendet einen dynamischen Anschluss. Da die vom Core Server abgehenden Pakete von einem dynamischen Anschluss an Anschluss 38293 gesendet werden, gehen die Antwortpakete des Geräts von Anschluss 38293 an den gleichen dynamischen Anschluss, nicht an Anschluss 38293. Um eine Kommunkation in beide Richtungen zu ermöglichen, ist eine Regel nötig, die UDP-Pakete mit Anschluss 38293 als Quell- oder Zielanschluss zulässt. Eine solche Regel ist normalerweise akzeptabel für ein Intranet, nicht jedoch für eine externe Firewall (da sie ankommende Pakete an allen UDP-Anschlüssen erlauben würde).

Aus diesem Grund gilt UDP-Verkehr in der Regel nicht als Firewall-freundlich. Zurück zu unserem Beispiel: Es gibt eine Alternative zu UDP-Anschluss 38293, nämlich TCP-Anschluss 9595. Bei der Verwaltung firewallgeschützter Geräte ist es daher vorzuziehen, das Produkt zur Verwendung des TCP-Anschluss zu konfigurieren.

Verwendete Anschlüsse

Anschluss	Richtung	Protokoll	Dienst
31770	Konsole nach Geräten, Gerät nach Core	TCP	Kommunikation zwischen Konsole und Gerät
6787	Konsole nach Gerät	TCP	Kommunikation zwischen Konsole und Gerät
9595	Konsole nach Gerät	UDP	Erkennung
9595	Konsole nach Gerät	TCP	Agentenkonfiguration
623	Konsole nach Gerät	UDP	ASF, IPMI-Erkennung
9535	Konsole nach Gerät	TCP	Fernsteuerung

Dieses Produkt muss Knoten erkennen, auf denen der Management Agent installiert ist, damit er die Geräte verwalten kann. UDP Anschluss 9595 wird zur Erkennung verwendet. Sie können einzelne Geräte auch manuell der Konsole hinzufügen; dies setzt jedoch dennoch voraus, dass das Gerät einen "Ping" am UDP-Anschluss 9595 beantwortet. Die Kommunikation zwischen der Konsole und dem Gerät verwendet die TCP-Anschlüsse 31770 und 6787. Auf dem letzteren dieser beiden Anschlüsse ist der Verkehr HTTP-basiert. UDP-Anschluss 623 wird zur Erkennung von ASF (Alert Standard Forum) verwendet. Zusätzlich verwendet dieses Produkt TCP-

Anschluss 9535 für die Fernsteuerung. Die IPMI-Erkennung ist mit der ASF-Erkennung verknüpft und verwendet den gleichen Anschluss (udp/623).

Stufe 2: Installieren des Core Servers

Diese Stufe befasst sich in erster Linie mit der Installation des Core Servers.

In dieser Stufe erhalten Sie Informationen zu den folgenden Themen:

Die in dieser Stufe beschriebene Installation der Komponenten nimmt ca. 30 bis 60 Minuten in Anspruch.

Installieren des Core Servers

So installieren Sie den Core Server

Es wird empfohlen, vor dem Start der Installation alle anderen Anwendungen zu schließen und etwaige geöffnete Dateien zu speichern. Führen Sie auf dem Windows 2000/2003-Server, den Sie als Ihren Core Server ausgewählt haben, die folgenden Schritte aus:

1. Legen Sie den Datenträger des Produkts in das Laufwerk ein oder führen Sie AUTORUN.EXE von Ihrem Installationsabbild aus. Der Autorun-Bildschirm wird eingeblendet.
2. Klicken Sie auf **Anforderungen überprüfen und Installieren**.
3. Der Prüfer für die Systemanforderungen wird ausgeführt, um sicherzustellen, dass der Server die Mindestanforderungen erfüllt. Vergewissern Sie sich, dass alle Anforderungen erfüllt sind. Wenn eine Anforderung die Prüfung nicht besteht, klicken Sie auf der Verknüpfung der nicht erfüllten Anforderung auf **Fehlgeschlagen**, um weiterführende Verknüpfungen oder Informationen bzgl. der Installation der nicht erfüllten Anforderung zu erhalten.
4. Klicken Sie auf **Jetzt installieren**, um das Setup-Programm auszuführen.
5. Wählen Sie die Sprache aus, die das Setup installieren soll. Klicken Sie auf **OK**.
6. Der Begrüßungsbildschirm wird angezeigt. Klicken Sie auf **Weiter**, um fortzufahren.
7. Klicken Sie im Lizenzvereinbarungsbildschirm auf **Ich akzeptiere die Bedingungen dieser Lizenzvereinbarung**, wenn Sie die Lizenzvereinbarung akzeptieren und mit dem nächsten Schritt fortfahren möchten. Klicken Sie auf **Weiter**.
8. Akzeptieren Sie den Standardzielordner oder geben Sie einen benutzerdefinierten Zielordner ein und klicken Sie dann auf **Weiter**. Der Pfad des Zielordners darf keine Doppelbyte-Zeichen enthalten. Wenn Sie diesen Ordner ändern, sollten Sie daran denken, Ihren Pfad durch etwaige Pfade zu ersetzen, die in der Produktdokumentation angegeben sind.
9. Geben Sie ein Kennwort für die MSDE-Datenbank ein. Merken Sie sich dieses Kennwort oder schreiben Sie es auf. Klicken Sie auf **Weiter**, um fortzufahren.
10. Geben Sie eine Organisation und einen Zertifikatsnamen für das Sicherheitszertifikat des Core Servers ein. Diese Informationen finden beim Benennen und Beschreiben des Zertifikats Verwendung. Klicken Sie auf **Weiter**.

11. Klicken Sie auf der Seite "Installationsbereit" auf **Installieren**. Das Produkt beginnt mit der Installation.
12. Das Dialogfeld **Installationsassistent abgeschlossen** wird angezeigt, nachdem das Setup vollständig ausgeführt wurde.
13. Klicken Sie auf **Fertig stellen**.
14. Das Setup fordert Sie auf, den Server neu zu starten. Sie müssen auf **Ja** klicken, um das Setup zu beenden. Wenn der Server neu gestartet wird, werden Sie nach Ihrer Anmeldung feststellen, dass das Setup noch einige Minuten weiter ausgeführt wird, während die Installation fertig gestellt wird. Das Setup fordert Sie nicht zur Eingabe von weiteren Informationen während des ersten Neustarts auf.

Beim Installieren einer MSDE Core-Datenbank auf einem Windows 2003 Server unterbricht Windows möglicherweise die Ausführung des Setups und fragt Sie, ob Sie damit einverstanden sind, SETUP.EXE zu öffnen. Klicken Sie auf "Öffnen", wenn diese Eingabeaufforderung angezeigt wird, da das Produkt andernfalls nicht ordnungsgemäß installiert wird.
Wenn Sie "Intel Platform Extensions für LANDesk Software" installieren möchten, folgen Sie den Anweisungen des Assistenten, der nach der Installation von Server Manager geöffnet wird.

Aktivieren des Core Servers

Sie müssen den Core Server aktivieren, um System Manager-Produkte auf dem betreffenden Server verwenden zu können. Sie können den Core Server entweder automatisch über das Internet oder manuell per E-Mail aktivieren. Falls Sie die Hardwarekonfiguration des Core Servers erheblich ändern, müssen Sie den Core Server u. U. reaktivieren.

Die Aktivierungskomponente des Core Servers generiert in regelmäßigen Abständen Daten in Bezug auf:

- Die genaue Anzahl von Geräten, mit denen Sie arbeiten.
- Die nicht persönliche verschlüsselte Hardwarekonfiguration
- Die genauen LANDesk-Softwareprogramme, die Sie verwenden ("Serverzahldaten")

Dies sind die einzigen Daten, die von der Aktivierung erfasst oder generiert werden. Der Code für den Hardwareschlüssel wird auf dem Core Server unter Verwendung nicht persönlicher Faktoren für die Hardwarekonfiguration (beispielsweise die Größe der Festplatte, die Verarbeitungsgeschwindigkeit des Computers etc.) generiert. Der Code für den Hardwareschlüssel wird verschlüsselt an LANDesk gesendet, während sich der für die Verschlüsselung verwendete private Schlüssel nur auf dem Core Server befindet. Der Code für den Hardwareschlüssel wird dann von LANDesk Software zur Erstellung eines Teils des autorisierten Zertifikats verwendet.

Nachdem ein Core Server installiert wurde, wird beim ersten Start das Core Server-Aktivierungsprogramm ausgeführt (**Start | Alle Programme | LANDesk | Core Server-Aktivierung**), um den Core mit dem vom OEM bereitgestellten Benutzernamen und Kennwort auszuführen.

Sie können das Core-Aktivierungsprogramm verwenden, um von System Manager auf Server Manager oder Management Suite zu aktualisieren. Weitere Informationen finden Sie unter "Zur Verwendung von System Manager mit Management Suite oder Server Manager".

Nachdem Sie einen Core Server aktiviert haben, können Sie mit dem Dialogfeld **Einstellungen | Lizenz** Lizenzinformationen zum Produkt anzeigen. Die Intel OEM-Lizenz berechtigt Sie zur Ausführung eines Produktagenten auf jedem Intel-Server oder jeder Intel-Hauptplatine.

Informationen zum Core Server-Aktivierungsprogramm

Verwenden Sie das Core Server-Aktivierungsprogramm zum erstmaligen Aktivieren eines neuen Servers. Starten Sie das Programm, indem Sie auf **Start | Programme | LANDesk | Core Server-Aktivierung** klicken. Wenn Ihr Core Server nicht mit dem Internet verbunden ist, lesen Sie die Informationen unter Manuelles Aktivieren eines Core oder Überprüfen der Serverzahldaten weiter unten in diesem Abschnitt.

Jeder Core Server benötigt ein eindeutiges Autorisierungszertifikat.

Der Core Server verifiziert in regelmäßigen Abständen die Lizenzierung, indem er die Datei "\Programme\LANDesk\Authorization Files\LANDesk.usage" generiert. Diese Datei wird in regelmäßigen Abständen an den LANDesk Software-Lizenzserver gesendet. Die Datei wird im XML-Format erstellt und digital signiert und verschlüsselt. Jegliche Änderungen, die manuell an dieser Datei vorgenommen werden, machen ihren Inhalt und den nächsten Nutzungsbericht an den LANDesk-Softwarelizenzserver ungültig.

Der Core kommuniziert mit dem LANDesk Software-Lizenzserver über HTTP. Wenn Sie einen Proxy-Server verwenden, klicken Sie auf die Registerkarte **Proxy** und geben die erforderlichen Proxy-Informationen ein. Wenn Ihr Core mit dem Internet verbunden ist, wird die Kommunikationsverbindung mit dem Lizenzserver automatisch, d.h. ohne Ihr Eingreifen, hergestellt.

Beachten Sie, dass das Core Server-Aktivierungsprogramm keine DFÜ-Verbindungen automatisch startet. Wenn Sie eine DFÜ-Verbindung jedoch manuell starten und dann das Aktivierungsprogramm ausführen, kann das Programm die Daten zur Nutzung auch über eine DFÜ-Verbindung weiterleiten.

Wenn Ihr Core Server nicht mit dem Internet verbunden ist, können Sie die Serverzahldaten auch manuell überprüfen und weiterleiten. Lesen Sie hierzu die Ausführungen weiter unten in diesem Abschnitt.

Aktivieren des Core Servers

So aktivieren Sie einen Server

1. Klicken Sie auf **Start | Programme | LANDesk | Core Server-Aktivierung**.
2. Klicken Sie auf **Aktivieren Sie diesen Core Server** mit Ihrem Kontaktnamen und Kennwort für LANDesk.

Der Kontaktname und das Kennwort werden automatisch ausgefüllt.

Manuelles Aktivieren eines Core oder Überprüfen der Serverzahldaten

Wenn der Core Server nicht an das Internet angeschlossen ist, kann das Core Server-Aktivierungsprogramm keine Informationen bzgl. der Serverzahl senden. In diesem Fall erhalten Sie eine Meldung, in der Sie aufgefordert werden, Verifizierungsdaten zur Aktivierung und zur Serverzahl manuell per E-Mail zu senden. Die E-Mail-Aktivierung ist ein unkompliziertes und schnelles Verfahren. Wenn die Aufforderung zur manuellen Aktivierung auf dem Core angezeigt wird, oder wenn Sie das Core Server-Aktivierungsprogramm verwenden und die manuelle Aktivierungsmeldung angezeigt wird, führen Sie folgende Schritte aus:

So aktivieren Sie einen Core manuell oder veranlassen Sie eine manuelle Verifizierung der Serverzahldaten

1. Wenn der Core Sie auffordert, die Serverzahldaten manuell zu verifizieren, erstellt er eine Datendatei mit dem Namen ACTIVATE.TXT im Ordner "\Programme\LANDesk\Authorization Files". Fügen Sie diese Datei einer E-Mail-Nachricht bei und senden Sie sie an licensing@landesk.com. Betreff und Nachrichtentext können frei gewählt werden.
2. LANDesk Software verarbeitet die beigefügte Datei und schickt eine Antwort an die E-Mail-Adresse, von der aus Sie die Nachricht gesendet hatten. Die LANDesk Software-Nachricht enthält Instruktionen und eine neue Autorisierungsdatei.
3. Öffnen Sie die beigefügte Autorisierungsdatei im Ordner "\Programme\LANDesk\Authorization Files". Die Datei wird daraufhin sofort vom Core Server verarbeitet und ihr Aktivierungsstatus aktualisiert.

Wenn die manuelle Aktivierung misslingt oder der Core die beigefügte Aktivierungsdatei nicht verarbeiten kann, wird die von Ihnen kopierte Autorisierungsdatei unter Verwendung der Erweiterung ".rejected" umbenannt. Zusätzlich hierzu protokolliert das Aktivierungsprogramm unter Angabe weiterer Details ein Ereignis im Anwendungsprotokoll der Windows-Ereignisanzeige.

Anmelden bei der Konsole

Nachdem das Setup ausgeführt wurde, Sie den Core Server neu gestartet haben und der Core aktiviert wurde, starten Sie die Konsole, indem Sie einen Browser öffnen und die Adresse des Servers in folgendem Format eingeben: http://servername/ldsm. (Klicken Sie auf dem Core Server auf Start | Alle Programme | System Manager | LANDesk). Nach dem Start der Konsole wird das Anmeldefenster der Konsole angezeigt. Zur Anmeldung werden Sie möglicherweise aufgefordert, den Berechtigungsnachweis des Kontos einzugeben, mit dem LDSM installiert wurde. Nur Mitglieder der LANDesk Management Suite-Gruppe auf dem Core Server können sich anmelden. Standardmäßig fügt das Setup den Benutzer hinzu, der bei der Installation des Core bei der LANDesk Management Suite-Gruppe angemeldet war. Wenn Sie anderen Benutzern den Zugriff auf die Konsole ermöglichen möchten, fügen Sie die betreffenden Benutzer dieser Gruppe hinzu.

Wenn Sie die Konsole erstmalig in einem Browser starten, kann es bis zu 90 Sekunden dauern, bis sie angezeigt wird. Der Grund für die Verzögerung liegt darin, dass der Server einmalig Abschnitte des Codes kompilieren muss. Die Konsole wird nach dem erstmaligen Aufruf bedeutend schneller gestartet.

Bereitstellung auf Windows-Geräten

Dieses Produkt unterstützte eine zeitplangesteuerte, Push-basierte Konfigurationsmethode, mit der Agenten über eine Remote-Verbindung bereitgestellt werden können.

Zum Aktivieren einer Push-basierten Konfiguration von Windows 2000/2003-Servern, auf denen der Standard Management Agent noch nicht ausgeführt wird, müssen Sie die erforderlichen Anmeldeinformationen wie folgt bereitstellen:

1. Klicken Sie auf dem Core Server auf **Start | Alle Programme | LANDesk |** LANDesk**Dienste konfigurieren** und klicken Sie dann auf die Registerkarte **Scheduler**.
2. Klicken Sie auf **Anmeldung ändern**.
3. Geben Sie in den Feldern **Benutzername und Kennwort** ein Domänenadministratorkonto an (im Format Domäne\Benutzername).
4. Stoppen Sie den Scheduler-Dienst und starten Sie ihn neu.
5. Wählen Sie von der Webkonsole aus die gewünschten Geräte als Ziel aus und klicken Sie dann auf **Agentenkonfiguration > Geplanter Task**, um die Konfigurationen bereitzustellen.

Sie können den Domänenadministrator festlegen, wenn Windows 2000/2003-Mitglieder konfiguriert werden, die derselben Domäne wie der Core Server angehören. Um Windows 2000/2003-Server in anderen Domänen zu konfigurieren, müssen Sie vertrauenswürdige Beziehungen einrichten. Denken Sie daran, dass unter dem in Schritt 3 angegebenen Konto auch der Scheduler-Dienst auf dem Core Server ausgeführt wird. Stellen Sie sicher, dass das Konto über das Recht **Anmelden als Dienst** verfügt.

Wenn eine Push-Konfiguration misslingt und die Meldung "Agent kann nicht gefunden werden" angezeigt wird, versuchen Sie, das Problem mit den nachstehend beschriebenen Schritten zu isolieren. Diese Schritte ahmen die Aktionen des Schedulers während einer Push-Konfiguration nach.

1. Suchen Sie nach dem Benutzernamen, unter dem der Scheduler-Dienst ausgeführt wird.
2. Melden Sie sich am Core Server mit dem Benutzernamen an, den Sie unter Schritt 1 gefunden haben.
3. Ordnen Sie \\server name\C$ ein Laufwerk zu. (Vermutlich tritt der Fehler bei diesem Schritt auf. Dies kann zwei Ursachen haben. Am wahrscheinlichsten ist, dass Sie nicht über Administratorrechte für den Server verfügen. Wenn dieser Benutzername keine Administratorrechte besitzt, ist möglicherweise die Administrationsfreigabe (C$) deaktiviert.)
4. Erstellen Sie ein Verzeichnis \\server name\C$\$ldtemp$ und kopieren Sie in dieses Verzeichnis eine Datei.
5. Verwenden Sie den Windows-Dienst-Manager und versuchen Sie, Dienste auf dem Server zu starten oder anzuhalten.

Wenn das Gerät IPMI-kompatibel ist, müssen Sie das BMC-Kennwort bereitstellen. Verwenden Sie die Registerkarte **BMC-Kennwort** des Applets **Dienste konfigurieren**, um ein Kennwort für den IPMI Baseboard Management Controller (BMC) zu erstellen.

1. Geben Sie auf der Registerkarte **BMC-Kennwort** ein Kennwort in das Feld **Kennwort** ein, bestätigen Sie das Kennwort, indem Sie es erneut in das Feld **Kennwort bestätigen** eingeben, und klicken Sie auf **OK**.

Das Kennwort darf maximal 15 Zeichen beinhalten; jedes Zeichen muss eine Zahl zwischen 0-9 sein oder die Groß-/Kleinbuchstaben a-z beinhalten.

Wenn das Gerät Intel* AMT-kompatibel ist, müssen Sie das Intel AMT-Kennwort bereitstellen. Verwenden Sie die Registerkarte **Intel AMT Konfiguration** unter **Dienste konfigurieren**, um das Kennwort auf Intel* Active Management Technology-tauglichen Geräten zu erstellen oder zu ändern.

So konfigurieren Sie ein Intel AMT-Kennwort

1. Geben Sie auf der Registerkarte **Intel AMT-Konfiguration** den aktuellen Benutzernamen und das aktuelle Kennwort ein. Diese müssen mit dem Benutzernamen und dem Kennwort übereinstimmen, die auf dem Intel AMT-Konfigurationsbildschirm konfiguriert wurden (auf diesen Bildschirm wird über die BIOS-Einstellungen des Computers zugegriffen).
2. Um den Benutzernamen und das Kennwort zu ändern, füllen Sie den Abschnitt **Neues Intel AMT-Kennwort** aus.
3. Klicken Sie auf **OK**. Diese Änderung wird vorgenommen, wenn die Clientkonfiguration ausgeführt wird.

Hinweis: Das neue Kennwort muss ein starkes Kennwort sein, damit ist Folgendes gemeint:

- Es muss mindestens sieben Zeichen beinhalten
- Es muss Buchstaben, Zahlen und Symbole beinhalten
- Es besitzt mindestens ein Symbolzeichen in der zweiten bis zur sechsten Position
- Es unterscheidet sich deutlich von früheren Kennwörtern
- Es enthält keine Namen oder Benutzernamen
- Es handelt sich nicht um ein Gebrauchswort oder einen Namen

Bereitstellung auf Linux-Geräten

Sie können Linux-Agenten und RPMs von einem Remote-Standort aus auf Linux-Servern bereitstellen und installieren. Ihr Linux-Server muss für diese Aufgabe richtig konfiguriert sein, da sie sich andernfalls nicht ausführen lässt. Um einen Agenten auf einem Linux-Server installieren zu können, benötigen Sie root-Privilegien.

Die Linux-Standardinstallation (Red Hat 3 und 4 und SUSE) beinhaltet die RPMs, die vom Linux-Standard Management Agent vorausgesetzt werden. Wenn Sie den Überwachungsagenten in der Agentenkonfiguration auswählen, benötigen Sie ein zusätzliches RPMs (sysstat).

Für die erste Linux-Agentenkonfiguration verwendet der Core Server eine SSH-Verbindung, um Linux-Server als Zielserver auswählen zu können. Sie müssen über eine aktive SSH-Verbindung mit Benutzer-/Kennwortauthentifizierung verfügen. Die Produkt unterstützt keine Authentifizierung mittels öffentlichem/privatem Schlüssel. Alle etwaigen Firewalls zwischen dem Core und den Linux-Servern müssen den SSH-Anschluss unterstützen. Testen Sie Ihre SSH-Verbindung auf dem Core Server mit der SSH-Anwendung eines Drittanbieters.

Das Installationspaket für einen Linux-Agenten besteht aus einem Shell-Script, Agenten-Tarball(s), .INI-Agentenkonfiguration und Authentifizierungszertifikaten für den Agenten. Diese Dateien werden in der LDLogon-Freigabe des Core Servers gespeichert. Das Shell-Skript extrahiert Dateien aus dem/den Tarball(s), installiert die RPMs und konfiguriert den Server für

das Laden der Agenten und die regelmäßige Ausführung des Inventarscanners in einem von Ihnen in der Agentenkonfiguration festgelegten Intervall. Dateien werden unter /usr/landesk gespeichert.

Sie müssen außerdem den Scheduler-Dienst auf dem Core konfigurieren, um die SSH-Authentifizierungsnachweise (Benutzername/Kennwort) auf Ihrem Linux-Server zu verwenden. Der Scheduler-Dienst verwendet diese Berechtigungsnachweise, um die Agenten auf Ihren Servern zu installieren. Verwenden Sie das Programm Dienste konfigurieren, um die SSH-Berechtigungsnachweise einzugeben, die der Scheduler-Dienst als alternative Berechtigungsnachweise verwenden soll. Sie werden aufgefordert, den Scheduler-Dienst neu zu starten. Falls diese Aufforderung nicht angezeigt wird, klicken Sie auf "Stopp" und dann auf "Start" auf der Registerkarte **Scheduler**, um den Dienst neu zu starten. Hiermit werden Ihre Änderungen aktiviert.

Nachdem Sie die Linux-Server konfiguriert und dem Core Server Linux-Anmeldeinformationen hinzugefügt haben, müssen Sie Server der Liste **Eigene Geräte** hinzufügen, damit Sie die Linux-Agenten bereitstellen können. Bevor Agenten auf einem Server bereitgestellt werden können, müssen Sie den Server zur Ansicht **Eigene Geräte** hinzufügen. Tun Sie dies, indem Sie Ihre Linux-Server mit der Funktion "Geräte erkennen" erkennen lassen.

So lassen Sie Ihre Linux-Server erkennen

1. Erstellen Sie in der Geräteerkennung einen Erkennungstask für jeden Linux-Server. Verwenden Sie einen Standard-Netzwerkscan und geben Sie die IP-Adresse des Linux-Servers als die Start- und Abschluss-IP-Bereiche ein. Wenn Sie mehrere Linux-Server besitzen, geben Sie einen mehrere IP-Adressen umfassenden Bereich ein. Klicken Sie auf OK, sobald Sie Ihre IP-Erkennungsbereiche hinzugefügt haben.
2. Erstellen Sie einen Zeitplan für den soeben erstellten Erkennungstask, indem Sie auf den Task und dann auf **Planen** klicken. Vergewissern Sie sich nach Abschluss des Vorgangs, dass der Erkennungsprozess die Linux-Server gefunden hat, die Sie verwalten möchten.
3. Wählen Sie in der Geräteerkennung die Server aus, die Sie verwalten möchten, und klicken Sie auf **Ziel** , um die ausgewählten Geräte der Liste "Ziel" hinzuzufügen. Klicken Sie auf die Registerkarte **Verwalten** in der unteren Fensterhälfte. Klicken Sie auf **Ausgewählte Geräte verschieben** und klicken Sie dann auf **Verschieben**. Damit werden Server zur Liste **Eigene Geräte** hinzugefügt und stehen als Ziel für Bereitstellungen zur Verfügung.

So erstellen Sie eine Linux-Agentenkonfiguration

1. Klicken Sie in der Agentenkonfiguration auf **Neu**.
2. Geben Sie einen Konfigurationsnamen ein, klicken Sie auf HP-UX oder Linux Server Edition und klicken Sie dann auf **OK**.
3. Wählen Sie die soeben erstellte Konfiguration aus und klicken Sie auf **Bearbeiten**.
4. Wählen Sie die gewünschten Agenten aus.
5. Wählen Sie auf der Registerkarte "Inventar" die Optionen und das gewünschte Scanner-Intervall aus. Das Installationsskript fügt einen Cron-Job hinzu, der den Scanner in dem von Ihnen festgelegten Intervall ausführt.
6. Klicken Sie auf **Änderungen speichern**.

Um Ihre Agentenkonfiguration bereitzustellen, wählen Sie sie in "Agentenkonfiguration" aus und klicken Sie auf **Task planen**. Konfigurieren Sie den Task und überwachen Sie die Taskausführung unter "Konfigurationstasks".

Hinweis: Sie erhalten erst dann Zustandsdaten auf einem Linux-Rechner, nachdem der Inventarscanner seinen ersten Scan nach der Installation ausgeführt hat. **So rufen Sie eine Linux-Agentenkonfiguration mit einer Pull-Prozedur ab**

1. Erstellen Sie ein temporäres Verzeichnis auf Ihrem Linux-Computer (z. B. /tmp/ldcfg) und kopieren Sie Folgendes in das Verzeichnis:
    1. Alle Dateien aus dem Verzeichnis "LDLOGON\unix\linux".
    2. Kopieren Sie das nach der Konfiguration benannte Shellskript (<configuration name>.sh) in das temporäre Verzeichnis.
    3. Kopieren Sie die nach der Konfiguration benannte *.0-Datei in das temporäre Verzeichnis. Das * entspricht 8 Zeichen (0-9, a-f).
    4. Kopieren Sie alle in der <configuration name>.ini-Datei aufgelisteten Dateien in das temporäre Verzeichnis. Um diese Dateien zu identifizieren, durchsuchen Sie die .INI-Datei nach "FILExx" (wobei xx für eine Zahl steht). Bei den meisten Einträgen, die Sie finden werden, wird es sich um Einträge handelt, die in Schritt 1 auf den Client kopiert wurden; aber Sie werden auch die .XML-Dateien sehen, die kopiert werden müssen. Die Dateinamen sollten nicht geändert werden, bis auf folgende Aufnahmen:
        - alertrules\<any text>.ruleset.xml sollte in internal.ruleset.xml umbenannt werden
        - monitorrules\<any text>.ruleset.monitor.xml sollte in masterconfig.ruleset.monitor.xml umbenannt werden
2. Wenn der Rechner ein IPMI/BMC-Rechner ist (mit in der Installation eingeschlossener Überwachung), geben Sie Folgendes an der Befehlszeile ein:

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

3. Führen Sie (in einer Ausführung als Root) das Shell-Skript für die Konfiguration aus. Wenn Sie das Skript beispielsweise "pull" genannt haben, verwenden Sie folgenden vollständigen Pfad:

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

4. Entfernen Sie das temporäre Verzeichnis und seinen gesamten Inhalt.

Hinweis: Bitte beachten Sie: Wenn Sie einen Agenten auf einem Linux-Computer mit dem Push- oder Pull-Verfahren bereitstellen, dann zum Reinigen des Computers

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

ausführen und dann erneut einen Push- oder Pull-Vorgang starten, ist die Datei mit dem GUID die einzige Datei, die nach Abschluss dieses Vorgangs noch auf dem Computer vorhanden ist.

Mit der Option "-f " werden Verzeichnisse gelöscht, deren Eigentümer dieses Produkt ist. Weitere Informationen erhalten Sie in der Linux-Deinstallationsdokumentation.

Stufe 3: Stufenweise Bereitstellung

In Stufe 3 wird die stufenweise Bereitstellung beschrieben: Mit *Bereitstellung* ist der Vorgang gemeint, mit dem Sie Ihre Verwaltungsfunktionen auf die Geräte übertragen, die Sie in Ihre Verwaltungsdomäne einschließen möchten.

Sie stellen dieses Produkt bereit, indem Sie Produktagenten und Dienste auf Geräte laden. Auf diese Weise lassen sich die Geräte von einem zentralen Standort aus verwalten.

In Stufe 3 erhalten Sie Informationen zu den folgenden Themen:

- Zur Strategie der stufenweisen Bereitstellung
- Checkliste für die Gerätekonfiguration
- Bereitstellung auf Windows-Geräten
- Erläuterungen zur Gerätekonfigurationsarchitektur

Zur Strategie der stufenweisen Bereitstellung

Für die stufenweise Bereitstellung gelten drei Grundsätze:

1. Stellen Sie die Komponenten zuerst auf Geräten bereit, die seltener benutzt werden oder sich am wenigsten auf Ihr bestehendes Netzwerk auswirken, und dann nach und nach auf den Geräten, die die nachhaltigsten Auswirkungen haben.
2. Vergewissern Sie sich, dass die Funktionalität eines jeden verwalteten Geräts stabil ist, bevor Sie weitere Agenten bereitstellen.
3. Stellen Sie das Produkt in sorgfältig durchdachten Stufen bereit, anstatt alle Agenten auf einmal auf allen Gerätetypen gleichzeitig bereitzustellen; auf diese Weise stellen Sie sicher, dass sich etwaige Probleme leichter beheben lassen.

Nachdem Sie die ersten zwei Stufen abgeschlossen haben, können Sie mit der letzten Stufe der Bereitstellung des Produkts auf Ihren Geräten beginnen.

Checkliste für die Gerätekonfiguration

Sie können Geräte konfigurieren, indem Sie Agenten remote über die Webkonsole bereitstellen oder indem Sie sie von dem verwalteten Gerät aus installieren. Für eine Push-basierte Konfiguration müssen Sie die Dienste von allen IPMI- oder Intel* AMT-Rechnern konfigurieren. Mit dem Applet "Configure Services" können Sie die im Folgenden beschriebenen Dienste für Ihre Core Server und Datenbanken konfigurieren. Um das Applet "Configure Services" auf dem Core Server zu starten, klicken Sie auf **Start | Programme | LANDesk | LANDesk Configure Services**. Verwenden Sie die Registerkarte "BMC-Kennwort" oder "Intel AMT-Konfiguratio".

- **Push-basierte Konfiguration:** Verwenden Sie die Agentenkonfiguration zum Definieren einer Gerätekonfiguration. Stellen Sie die erforderlichen Berechtigungsnachweise für Intel AMT- oder IPMI-Rechner über "Dienste konfigurieren" zur Verfügung (siehe "Dienste konfigurieren" im *Benutzerhandbuch*). Sprechen Sie die gewünschten Geräte als Ziel an und planen Sie dann einen Task, mit dem die Konfiguration auf den Geräten bereitgestellt wird. Siehe "Konfigurieren von Agenten" im *Benutzerhandbuch*.
- **Manuelle Konfiguration:** Ordnen Sie vom verwalteten Gerät aus der LDLogon-Freigabe des Core Servers ein Laufwerk zu und führen Sie das Serverkonfigurationsprogramm SERVERCONFIG.EXE aus. Die auf dem Gerät bereitzustellenden Komponenten müssen interaktiv ausgewählt werden.

Es liegt auf der Hand, dass sich die manuelle Konfiguration für große Umgebungen, in denen eine Vielzahl von Geräten installiert und konfiguriert werden muss, nicht eignet. In den meisten Fällen stellen Sie Agenten mit einer Push-Prozedur auf Geräten bereit. Bitte beachten Sie, dass bei der Installation des Produkts keine Agenten automatisch auf dem Core installiert werden; die Agenten müssen auch auf dem Core installiert und der Core muss dann manuell neu gestartet werden.

Vergewissern Sie sich unabhängig von Ihrer Wahl der Gerätekonfiguration, dass Sie die Agentenkonfiguration in der Konsole verwendet haben, um die Gerätekonfiguration zu erstellen, die Sie bereitstellen möchten.

Windows XP Professional SP2 oder 2003 SP1-Systeme setzen voraus, dass die Firewall manuell konfiguriert wird, um vollständige Produktfunktionalität zu gewährleisten: Legen Sie für diese Geräte folgende Einstellungen fest:

Verwaltete Server:

File and Printer Sharing - TCP 139, 445; UDP 137,138 (unabdingbare Voraussetzung für Push-Bereitstellung von Agenten)

Software distribution - TCP 9594, 9595 (unabdingbare Voraussetzung für Push-Bereitstellung von Agenten)

Advanced - ICMP - "Allow incoming echo request" (das Gerät wird nicht erkannt, wenn diese Einstellung nicht aktiviert ist.)

Core Server:

Inventory - 5007

Um diese Einstellungen anzugeben, klicken Sie auf dem verwalteten Gerät auf **Start | Systemsteuerung | Sicherheit**. Dieses Produkt wird mit einer Standardagentenkonfiguration geliefert, die folgende Agenten einschließt: Standard Management Agent sowie Softwareaktualisierungs- und Überwachungsagenten.

Sie können neue Konfigurationen erstellen, die nur die Komponenten einschließen, die Sie installieren möchten; oder (nur für die OEM-Version) fügen Sie die Intel Active System Console der Standardagentenkonfiguration hinzu. Bitte beachten Sie, dass der Bereitstellungsprozess für Agenten nicht kumulativ ist; d.h., bei jeder Bereitstellung werden alle vorhandenen Agenten deinstalliert. Um einen neuen Agenten in einer Konfiguration bereitzustellen, müssen Sie diesen Agenten in alle vorherigen Agenten einschließen, die in der Konfiguration enthalten sein sollen.

So erstellen Sie eine Gerätekonfiguration

1. Klicken Sie im linken Navigationsfenster auf **Agentenkonfiguration**.
2. Klicken Sie auf **Neu**.
3. Geben Sie einen Namen für die neue Konfiguration in das Feld "Konfigurationsname" ein.

Geben Sie einen Namen ein, der die Konfiguration beschreibt, an der Sie arbeiten, z. B. DBServer oder Executive Office Server. Dies kann ein bereits vorhandener oder ein neuer Konfigurationsname sein.

4. Wählen Sie **Linux Server Edition**, **Microsoft Windows Server Edition** oder HP-UX aus.
5. Um IPMI-kompatible Server zu verwalten, ohne Produkt-Softwareagenten zu installieren, aktivieren Sie das Kontrollkästchen **IPMI Nur BMC**, wenn die Konfiguration für IPMI-kompatible Server vorgesehen ist; klicken Sie anschließend auf **OK**.
6. Wählen Sie die soeben erstellte Konfiguration aus und klicken Sie auf **Bearbeiten**.

Auf den Registerkarten sind einige Optionen möglicherweise abgeblendet, da sie für die von Ihnen ausgewählte Konfiguration nicht gelten. Beispiel: Wenn Sie eine "IPMI Nur BMC"-Windows-Konfiguration auswählen, gibt es keine konfigurierbaren Optionen.

7. Wählen Sie auf der Registerkarte **Agent** die Agenten aus, die Sie verteilen möchten.
    - **Alle:** Installiert alle Agenten auf dem ausgewählten Gerät.
    - **Softwareaktualisierung:** Installiert den Softwareaktualisierungsagenten. Wenn dieser Agent installiert ist, können Sie festlegen, wie der Scanner verfügbare Aktualisierungen erkennt.
    - **Überwachung:** Installiert den Überwachungsagenten auf dem ausgewählten Gerät. Der Überwachungsagent unterstützt zahlreiche Überwachungsmethoden, einschließlich Direct ASIC-Überwachung, In-Band IPMI, Out-of-Band IPMI, Intel Active System Console, Intel AMT und CIM.
8. **Konfiguration** wird nur zu Informationszwecken angezeigt
9. Wählen Sie eine neue Neustartoption aus.

Manuell neu starten bedeutet, dass die Geräte nicht neu gestartet werden, selbst wenn die ausgewählten Agenten einen Neustart erforderlich machen. Sie müssen das Gerät manuell neu starten. Wenn das Gerät einen Neustart erforderlich macht, funktionieren installierte Agenten erst fehlerfrei, nachdem das Gerät neu gestartet wurde. Die Option "Server bei Bedarf neu starten" startet Geräte nur dann neu, wenn ein ausgewählter Agent einen Neustart erforderlich macht.

Hinweis: Nur Geräte, die vorhandene 8.5-Agenten aktualisieren, erfordern einen Neustart.

10. Definieren Sie auf der Registerkarte **Inventar** die Konfigurationseinstellungen für den Inventarscanner. Diese Optionen werden nachstehend erläutert.

- **Automatisch aktualisieren:** Die Remote-Geräte beziehen die Softwareliste während der Softwarescans vom Core Server. Wenn diese Option ausgewählt ist, muss jedes Gerät über ein Laufwerk verfügen, das dem Verzeichnis LDLOGON auf dem Core Server zugewiesen wurde, damit es auf die Softwareliste zugreifen kann. In der Softwareliste erfolgte Änderungen stehen den Geräten sofort zur Verfügung.
- **Manuelle Aktualisierung:** Die während der Softwarescans zum Ausschließen von Titeln verwendete Softwareliste wird in jedes Remote-Gerät geladen. Immer, wenn die Softwareliste von der Konsole aus geändert wird, müssen Sie sie manuell erneut an die Remote-Geräte weiterleiten.

- **Inventarscanner-Einstellungen:** Der Zeitpunkt, zu dem die Inventarisierung ausgeführt wird. Sie können die Häufigkeit auswählen und Sie können angeben, dass der Inventarscanner bei jedem Systemstart ausgeführt werden soll.

Wenn Sie die Inventarscanneroption **Zwischen Stunden** auswählen, können Sie eine Zeitspanne (in Stunden) angeben, in der der Scanner ausgeführt werden kann. Meldet sich ein Gerät während des angegebenen Zeitraums an, so wird automatisch der Inventarscanner ausgeführt. Wenn das Gerät bereits angemeldet ist, wird der Scan zur angegebenen Stunde automatisch gestartet. Diese Option ist nützlich, wenn Sie Inventarscans auf Geräten zeitlich versetzt ausführen möchten, um zu verhindern, dass alle Scans gleichzeitig gesendet werden.

- **Auszuführen bei der Anmeldung:**Der Inventarscanner wird ausgeführt, sooft Sie das Gerät starten.

11. Wählen Sie auf der Registerkarte **Regelsätze** einen Überwachungs- und/oder Alarmregelsatz aus, den Sie in die Konfiguration einfügen möchten. Diese Regelsätze werden im Ordner "ldlogon/alertrules" gespeichert. Neue Regelsätze können in der Funktion "Überwachung" oder "Alarmierung" erstellt werden. Damit neu erstellte Regelsätze in den Dropdown-Listen angezeigt werden, müssen Sie die XML für den benutzerdefinierten Regelsatz generieren.
12. Klicken Sie auf **Änderungen speichern**, um die Agentenkonfiguration zu speichern.

Weitere Informationen zur Bereitstellung auf Geräten finden Sie unter Erläuterungen zur Agentenkonfigurationsarchitektur am Ende dieses Kapitels.

Bereitstellung auf Windows-Geräten

Dieses Produkt unterstützte eine zeitplangesteuerte, Push-basierte Konfigurationssmethode, mit der Agenten über eine Remote-Verbindung bereitgestellt werden können.

Zum Aktivieren einer Push-basierten Konfiguration von Windows 2000/2003-Servern, auf denen der Standard Management Agent noch nicht ausgeführt wird, müssen Sie die erforderlichen Anmeldeinformationen wie folgt bereitstellen:

1. Klicken Sie auf dem Core Server auf **Start | Alle Programme |** LANDesk | LANDesk**Dienste konfigurieren** und klicken Sie dann auf die Registerkarte **Scheduler**.
2. Klicken Sie auf **Anmeldung ändern**.
3. Geben Sie in den Feldern **Benutzername und Kennwort** ein Domänenadministratorkonto an (im Format Domäne\Benutzername).
4. Stoppen Sie den Scheduler-Dienst und starten Sie ihn neu.
5. Wählen Sie von der Webkonsole aus die gewünschten Geräte als Ziel aus und klicken Sie dann auf **Agentenkonfiguration > Geplanter Task**, um die Konfiguratrionen bereitzustellen.

Sie können den Domänenadministrator festlegen, wenn Windows 2000/2003-Mitglieder konfiguriert werden, die derselben Domäne wie der Core Server angehören. Um Windows 2000/2003-Server in anderen Domänen zu konfigurieren, müssen Sie vertrauenswürdige Beziehungen einrichten. Denken Sie daran, dass unter dem in Schritt 3 angegebenen Konto auch der Scheduler-Dienst auf dem Core Server ausgeführt wird. Stellen Sie sicher, dass das Konto über das Recht **Anmelden als Dienst** verfügt.

Wenn eine Push-Konfiguration misslingt und die Meldung "Agent kann nicht gefunden werden" angezeigt wird, versuchen Sie, das Problem mit den nachstehend beschriebenen Schritten zu isolieren. Diese Schritte ahmen die Aktionen des Schedulers während einer Push-Konfiguration nach.

1. Suchen Sie nach dem Benutzernamen, unter dem der Scheduler-Dienst ausgeführt wird.
2. Melden Sie sich am Core Server mit dem Benutzernamen an, den Sie unter Schritt 1 gefunden haben.
3. Ordnen Sie \\server name\C$ ein Laufwerk zu. (Vermutlich tritt der Fehler bei diesem Schritt auf. Dies kann zwei Ursachen haben. Am wahrscheinlichsten ist, dass Sie nicht über Administratorrechte für den Server verfügen. Wenn dieser Benutzername keine Administratorrechte besitzt, ist möglicherweise die Administrationsfreigabe (C$) deaktiviert.)
4. Erstellen Sie ein Verzeichnis \\server name\C$\$ldtemp$ und kopieren Sie in dieses Verzeichnis eine Datei.
5. Verwenden Sie den Windows-Dienst-Manager und versuchen Sie, Dienste auf dem Server zu starten oder anzuhalten.

Wenn das Gerät IPMI-kompatibel ist, müssen Sie das BMC-Kennwort bereitstellen. Verwenden Sie die Registerkarte **BMC-Kennwort** des Applets "Dienste konfigurieren", um ein Kennwort für den IPMI Baseboard Management Controller (BMC) zu erstellen.

1. Geben Sie auf der Registerkarte **BMC-Kennwort** ein Kennwort in das Feld **Kennwort** ein, bestätigen Sie das Kennwort, indem Sie es erneut in das Feld **Kennwort bestätigen** eingeben, und klicken Sie auf **OK**.

Das Kennwort darf maximal 15 Zeichen beinhalten; jedes Zeichen muss eine Zahl zwischen 0-9 sein oder die Groß-/Kleinbuchstaben a-z beinhalten.

Wenn das Gerät Intel* AMT-kompatibel ist, müssen Sie das Intel AMT-Kennwort bereitstellen. Verwenden Sie die Registerkarte **Intel AMT-Konfiguration** von "Dienste konfigurieren", um auf Intel Active Management Technology-tauglichen Geräten das Kennwort zu erstellen oder zu ändern.

So konfigurieren Sie ein Intel AMT-Kennwort

1. Geben Sie auf der Registerkarte **Intel AMT-Konfiguration** den aktuellen Benutzernamen und das aktuelle Kennwort ein. Diese müssen mit dem Benutzernamen und dem Kennwort übereinstimmen, die auf dem **Intel AMT-Konfigurationsbildschirm** konfiguriert wurden (auf diesen Bildschirm wird über die BIOS-Einstellungen des Computers zugegriffen).
2. Um den Benutzernamen und das Kennwort zu ändern, füllen Sie den Abschnitt **Neues Intel AMT-Kennwort** aus.
3. Klicken Sie auf **OK**. Diese Änderung wird vorgenommen, wenn die Clientkonfiguration ausgeführt wird.

Hinweis: Das neue Kennwort muss ein starkes Kennwort sein; damit ist Folgendes gemeint:

- Es muss mindestens sieben Zeichen beinhalten
- Es muss Buchstaben, Zahlen und Symbole beinhalten
- Es besitzt mindestens ein Symbolzeichen in der zweiten bis zur sechsten Position
- Es unterscheidet sich deutlich von früheren Kennwörtern
- Es enthält keine Namen oder Benutzernamen
- Es handelt sich nicht um ein Gebrauchswort oder einen Namen

Erfolgreiche Durchführung einer Agentenbereitstellung verifizieren

Um sicherzustellen, dass Sie den Management Agent erfolgreich auf Geräten bereitgestellt haben, versuchen Sie, die folgenden Aufgaben von der Konsole aus durchzuführen. Wenn Sie zusätzliche Informationen benötigen, um diese Tasks auszuführen, finden Sie in den Kapiteln des *System ManagerBenutzerhandbuchs*, die sich mit den jeweiligen Funktionen befassen, weitere Informationen.

Inventar

- Doppelklicken Sie in der Liste **Eigene Geräte** auf ein Gerät und zeigen Sie dann die Liste mit den installierten Agenten an.
- Führen Sie eine Inventarabfrage durch.
- Wählen Sie ein Gerät aus und klicken Sie dann auf **Inventar**, um Daten für das Gerät anzuzeigen.
- Ändern Sie die Datei WIN.INI eines Windows-Geräts, scannen Sie das Gerät neu und überprüfen Sie, ob die Änderungen in der Datei CHANGES.LOG aufgezeichnet wurden.

Bereitstellen von Geräten von der Befehlszeile aus

Durch die Verwendung von SERVERCONFIG.EXE mit Befehlszeilenparametern können Sie steuern, welche Komponenten auf Geräten installiert werden.

Sie können SERVERCONFIG.EXE im Standalone-Modus starten. Die Datei befinden sich in (Systemlaufwerk)\Programme\LANDesk\ManagementSuite\LDLogon auf dem Core Server. SERVERCONFIG.EXE befindet sich auch in der Freigabe \\coreservername\LDLogon, die von jedem Windows 2000/2003-Server aus lesbar ist.

Erläuterungen zur Agentenkonfigurationsarchitektur

Erläuterungen zur SERVERCONFIG.EXE

SERVERCONFIG.EXE ist das Gerätekonfigurationsprogramm des Produkts. Um Windows-Server für die Verwaltung zu konfigurieren führt dieses Programm drei Schritte aus:

1. SERVERCONFIG bestimmt, ob der Computer zuvor schon einmal von einem anderen LANDesk-Produkt konfiguriert wurde. Wenn dies der Fall ist, entfernt SERVERCONFIG die älteren Dateien und setzt alle anderen Änderungen zurück.

2. SERVERCONFIG sucht nach einer verborgenen Datei mit dem Namen CCDRIVER.TXT, um zu bestimmen, ob der Server (neu) konfiguriert werden muss. (Der Entscheidungsprozess, den SERVERCONFIG durchläuft, wird nachfolgend beschrieben.) Wenn das Gerät nicht (neu) konfiguriert werden muss, wird SERVERCONFIG geschlossen.
3. Wenn das Gerät (neu) konfiguriert werden muss, lädt SERVERCONFIG die entsprechende Initialisierungsdatei (SERVERCONFIG.INI) und führt die darin enthaltenen Anweisungen aus.

Wenn Sie SERVERCONFIG.EXE ein zweites Mal ausführen und andere Agenten als bei der ersten Ausführung auswählen, werden die Agenten der ersten Ausführung gelöscht. Sie werden jeden Agent, den Sie benötigen, mit jeder neuen Ausfühung von SERVERCONFIG.EXE auswählen müssen, obwohl Sie die Agenten zuvor installiert hatten.

Für SERVERCONFIG.EXE stehen folgende Befehlszeilenparameter zur verfügung:

Parameter	**Beschreibung**
/I=	Einzuschließende Komponenten (Anführungszeichen eingeschlossen): "Common Base Agent" "Inventory Scanner" "Alerting" "Vulnerability scanner" "Server Monitor" "Active System Console" Sie können diese Komponenten auf derselben Befehlszeile miteinander kombinieren. Zum Beispiel, Beispiel: SERVERCONFIG.EXE /I="Mirror Driver" /I="Vulnerability scanner"
/IP	Konfiguration mithilfe von IP
/L oder /Log=	Pfad zu den CFG_YES- und CFG_NO-Protokolldateien, die aufzeichnen, welche Geräte konfiguriert wurden und welche nicht.
/LOGON	Ausführen [LOGON] von vordefinierten Befehlen
/N oder /NOUI	Keine Anzeige der Benutzeroberfläche
/NOREBOOT	Kein Neustart des Geräts bei Abschluss
/P	Fragen nach der Benutzerberechtigung zur Ausführung
/REBOOT	Erzwingen des Neustarts nach der Ausführung

/TCPIP	Entspricht IP (siehe oben)
/X=	Auszuschließende Komponenten Beispiel: SERVERCONFIG.EXE /X=SD
/CONFIG=	/CONFIG]= Gibt eine Gerätekonfigurationsdatei an, die anstelle der SERVERCONFIG.INI-Datei zu verwenden ist. Wenn Sie beispielsweise Konfigurationsdateien mit den Namen NTTEST.INI erstellt haben, verwenden Sie diese Syntax: SERVERCONFIG.EXE /CONFIG=TEST.INI Die benutzerdefinierten .INI-Dateien sollten sich im selben Verzeichnis wie SERVERCONFIG.EXE befinden. Beachten Sie auch, dass der Parameter /config den Dateinamen ohne das 95-Präfix verwendet.
/? oder /H	Anzeigen des Hilfemenüs

Bereitstellen des Standard Management Agent

Der Standard Management Agent ist ein erforderlicher Agent; er ist das Protokoll, das dem Produkt zugrunde liegt.

Bereitstellen des Anfälligkeitsscanners

Der Anfälligkeitsscanneragent führt Scan- und Reparaturvorgänge aus. Mit der Schaltfläche **Sicherheitstasks planen** kann ein Task erstellt werden, der vulscan.exe ohne Parameter startet. Beim Starten ohne Parameter erkennt vulscan, wo sich sein Core befindet, indem er auf den Registrierungsschlüssel "hklm\software\intel\landesk\LDWM", Wert “CoreServer” zugreift. Anschließend fordert er die Liste mit den neuesten Anfälligkeiten an, nach denen gescannt werden soll, führt den Scan aus und übermittelt die Ergebnisse an den Core. Die Ergebnisse werden in die Liste "Erkannte Aktualisierungen" geschrieben. Erkannte Aktualisierungen müssen in den Core heruntergeladen werden. Aktualisierungen können im Rahmen des Reparaturvorgangs mit Patches bearbeitet werden. Wenn während des Reparaturvorgangs ein oder mehrere Patches erfolgreich installiert werden, wird der Scan erneut ausgeführt und das neue Ergebnis an den Core gesendet. Dies gilt für LANDesk- und OEM-Aktualisierungen.

Bereitstellen des Inventarscanners

Sie können den Inventarscanner verwenden, um Geräte zur Core-Datenbank hinzuzufügen und Informationen zur Hardware und Software des Geräts zu sammeln. Der Inventarscanner wird beim erstmaligen Konfigurieren des Geräts automatisch ausgeführt. Der Scanner erfasst Hard- und Softwaredaten und fügt sie in die Core-Datenbank ein. Danach wird der Hardwarescan bei

jedem Gerätestart ausgeführt. Im Gegensatz dazu läuft der Softwarescan nur in einem von Ihnen festgelegten Intervall.

Bereitstellen des Überwachungsagenten

Der Überwachungsagent unterstützt zahlreiche Überwachungsmethoden, einschließlich direkte ASIC-Überwachung, In-Band-IPMI, Out-of-Band-IPMI, Intel AMT und CIM.

Bereitstellen der Active System Console

Installiert die Agenten, die den Zugriff auf die Active System Console von System Manager aus über die Schnittstelle oder über die Menüs ermöglichen. Dieser Agent wird nur auf Geräten mit Intel-Platinen installiert; wenn Sie diesen Agenten in eine Bereitstellung für eine Nicht-Intel-Platine einschließen, wird er nicht installiert.

Deinstallieren des Core Servers

Ebenso wie es eine bestimmte Strategie zum Bereitstellen der verschiedenen Komponenten gibt, gibt es auch eine entsprechende Strategie zum Deinstallieren der Komponenten.

In den folgenden Abschnitten wird gezeigt, wie Sie die einzelnen Komponenten ordnungsgemäß deinstallieren. Sie müssen die Komponenten in dieser Reihenfolge deinstallieren:

1. Deinstallieren der Produktagenten auf den Geräten.
2. Deinstallieren des Core Servers.

Deinstallieren der Produktagenten auf Geräten

Der erste Schritt beim Deinstallieren der Produktsoftware in einem Netzwerk besteht im Entfernen der Agenten auf den Geräten.

So deinstallieren Sie Agenten auf Servern

1. Melden Sie sich mit administrativen Rechten am Server an.
2. Ordnen Sie dem freigegebenen ManagementSuite-Ordner des Core Servers ein Laufwerk zu.
3. Öffnen Sie eine Befehlsaufforderung, wechseln Sie zum Laufwerksbuchstaben des ManagementSuite-Ordners und geben Sie Folgendes ein:

uninstallwinclient.exe

4. Die Deinstallation wird im Hintergrund ausgeführt und löscht alle Agenten.

Sie können auch Start, Ausführen auswählen und dann *core name*\LANDesk\ManagementSuite\uninstallwinclient.exe eingeben.**So entfernen Sie den Linux-Agenten auf einem Linux-Server**

1. Suchen Sie im freigegebenen ManagementSuite-Ordner die Datei "linuxuninstall.tar.gz" und kopieren Sie sie in das Linux-Feld.
2. Führen Sie diese Datei unter Verwendung der Optionen x, z und f aus. Die Befehlszeile sollte Folgendes enthalten:

tar xzf linuxuninstall.tar.gz

3. Führen Sie nach Ausführung der Datei ./linuxuninstall.sh von der Befehlszeile aus.

Weitere Informationen zu dieser Datei erhalten Sie, wenn Sie sie mit der Option -h ausführen. Hinweis: Wenn Sie einen Agenten auf einem Linux-Computer mit dem Push- oder Pull-Verfahren bereitstellen, dann zum Reinigen des Computers

./linuxuninstall.sh -f ALL

ausführen und anschließend erneut einen Push- oder Pull-Vorgang ausführen, werden doppelte Datenbankeinträge für denselben Computer mit demselben Namen und derselben IP erstellt, da die GUID des Computers gelöscht wird.

Mit der Option "-f " werden Verzeichnisse gelöscht, deren Eigentümer dieses Produkt ist. Weitere Informationen erhalten Sie in der Linux-Deinstallationsdokumentation.

Die einzige Datei, die nach der Deinstallation noch vorhanden ist, ist die "/etc/ldiscnux.conf". Diese Datei wurde zurückbehalten, um das Überhäufen der Datenbank mit doppelten Geräten zu verhindern. Wenn Sie dieses Gerät nicht wieder in die Datenbank zurückgeben, können Sie die Datei bedenkenlos löschen. UninstallWinClient.exe befindet sich im freigegebenen ManagementSuite-Ordner. Nur Administratoren haben Zugriff auf diese Freigabe. Dieses Programm deinstalliert Produktagenten auf jedem Gerät, auf dem es ausgeführt wird. Es handelt sich dabei um eine Windows-Anwendung, die im Hintergrund ausgeführt wird, ohne eine Benutzeroberfläche einzublenden. Sie sehen möglicherweise zwei Instanzen des Servers, den Sie gerade gelöscht haben, in der Datenbank. Eine dieser Instanzen enthält nur Protokolldaten, während die andere nach vorne gerichtete Daten enthält.

Hinweis: Standardmäßig startet "Uninstallwinclient.exe" das Gerät nach dem Deinstallieren der Agenten neu. Um diesen Neustart zu vermeiden, können Sie den Schalter "/noreboot" in die Befehlszeile schreiben.

Deinstallieren des Core Servers

Der letzte Schritt zur Deinstallation des Produkts in einem Netzwerk besteht im Deinstallieren der Sofware auf dem Core Server. Bevor Sie dies tun, müssen Sie sicherstellen, dass die Produktagenten der Software auf den Servern deinstalliert wurden.

So deinstallieren Sie den Core Server

1. Wechseln Sie zum Core Server.
2. Klicken Sie auf **Start** | **Einstellungen** | **Systemsteuerung** und doppelklicken Sie dann auf **Software**.
3. Sofern Intel Platform Extensions for LANDesk Software installiert ist, wählen Sie es aus und klicken Sie auf Software.
4. Um Produktsoftware zu deinstallieren, wählen Sie LANDeskSoftware aus.
5. Klicken Sie auf **Software**.

Deinstallieren der Core-Datenbank
Sie müssen die Core-Datenbank manuell deinstallieren.

Deinstallieren der Core-Datenbank

Standardmäßig wird die Core-Datenbank nicht deinstalliert, wenn Sie LANDesk® System Manager deinstallieren. Wichtig: Deinstallieren Sie nicht die Core-Datenbank, wenn Sie später LANDesk® System Manager auf dem Computer erneut installieren.

So deinstallieren Sie die Core-Datenbank

1. Wechseln Sie zum Core Server.
2. Klicken Sie auf **Start** | **Einstellungen** | **Systemsteuerung** und doppelklicken Sie dann auf **Software**.
3. Um die Core-Datenbank zu deinstallieren, wählen Sie Microsoft SQL Server Desktop Engine (LDMSDATA) aus.
4. Klicken Sie auf **Software**.

Datenbankdateien

Durch das Entfernen der "Microsoft SQL Server Desktop Engine" werden nicht die von LANDesk® System Manager verwendeten Datenbankdateien gelöscht. Bis auf die Tatsache, dass die Datenbankdateien Speicherplatz belegen, hat es keine negativen Auswirkungen, wenn diese Dateien auf Ihrem Computer verbleiben. Wenn Sie diese Datenbankdateien manuell entfernen möchten, löschen Sie den Inhalt des Ordners \Programme\Microsoft SQL Server\MSSQL$LDMSDATA\Data.

Support

Der Online-Support von LANDesk Software ist im Web erreichbar (nur in Englisch). Er stellt die neuesten Informationen zu den Softwareprodukten von LANDesk zur Verfügung. Darüber hinaus finden Sie dort Installationshinweise, Tipps zur Fehlerkorrektur, Softwareaktualisierungen und Kundensupport-Informationen zur Verfügung. Besuchen Sie die nachstehend genannte Website und öffnen Sie die Produktseite:

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

Sie können auch die neueste Version der Release-Hinweise und Dokumentation herunterladen, die unter Umständen Informationen enthält, die zum Zeitpunkt der Auslieferung des Produkts noch nicht verfügbar waren. Wenn Sie System Manager bei einem OEM-Hersteller erworben haben, wenden Sie sich bitte an den Supportdienst dieses Herstellers.

Wenn Sie ein Problem nicht mithilfe dieses Handbuchs oder der Support-Website von LANDesk lösen können, bietet LANDesk Software verschiedene Support-, Consulting- und Partnerdienste an. Nähere Informationen hierzu finden Sie auf der Website für den Kundensupport unter folgender Adresse:

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

Halten Sie bei der telefonischen Kontaktaufnahme mit dem Kundensupport folgende Angaben bereit:

- Ihren Namen, den Namen Ihrer Firma und die Produktversion, mit der Sie arbeiten.
- Das verwendete Netzwerkbetriebssystem (Name und Version).
- Installierte Patches und Service Packs.
- Detaillierte Aufzeichnung der Schritte, mit denen sich das Problem reproduzieren lässt.
- Schritte, die Sie bereits zur Lösung des Problems unternommen haben.
- Informationen zu Ihrem System, die für den Techniker des Kundensupports bei der Problemdiagnose von Interesse sein könnten, beispielsweise Angaben zum verwendeten Datenbankprogramm, zum installierten Grafikkartentyp oder zu Hersteller und Modell des verwendeten Computers.