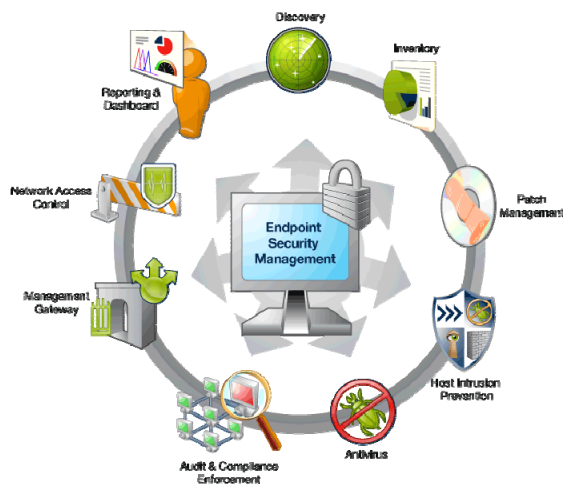


LANDesk Security Suite

Die LANDesk Security Suite stellt die Werkzeuge bereit, die Sie benötigen, um Geräte und kritische Daten in Ihrem heterogenen Unternehmensnetzwerk über eine zentrale Konsole zu verwalten und zu schützen. Die Security Suite unterstützt Windows NT-, Windows 2000/2003- Macintosh- und Linux-Netzwerke. Die breit gefächerte und mehrschichtige Security Suite-Sicherheitslösung basiert auf den zentralen LANDesk Management Suite-Funktionen, mit denen Sie Netzwerkgeräte konfigurieren und verwalten können. Zusätzlich erweitert und optimiert die Security Suite diese Funktionalitäten durch die Bereitstellung von Sicherheitswerkzeugen wie Security und Patch Manager, LANDesk Host Intrusion Prevention, Connection Control Manager, Agent-Wächter und vieles mehr.



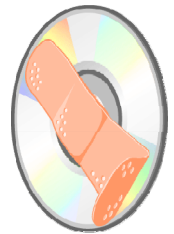
Mehrschichtige Sicherheitslösung

LANDesk Security Suite ist eine optimal ausgestattete Sicherheitsverwaltungslösung, mit der Sie Ihre Netzwerkinfrastruktur und Ressourcen proaktiv überwachen, schützen, reparieren und stärken können.

Das Basistool "Security und Patch Manager" ermöglicht es Ihnen, Sicherheitsrisiken, die eine fortlaufende Bedrohung für den Zustand und die Leistung Ihrer verwalteten Geräte darstellen, aufzuspüren und zu beseitigen. Zu diesen Risiken gehören: Bekannte Betriebssystem- und Anwendunganfälligkeiten, Spyware, Viren, Systemkonfigurationsfehler, unzulässige oder verbotene Anwendungen sowie andere potenzielle Sicherheitslücken. LANDesk® Host Intrusion Prevention geht weit über den Standard-Virenschutz hinaus – Es überwacht und beendet verdächtige Vorgänge, die auf eine böswillige Attacke auf Ihr System hinweisen. Auch wenn noch kein Antivirus-Update vorliegt, so können Sie mit LANDesk® Host Intrusion Prevention Ihr System sicher und zuverlässig überwachen und vor Angriffen schützen.

Security und Patch Manager Übersicht

Der Security und Patch Manager stellt Ihnen alle Tools zur Verfügung, die Sie für die Einrichtung einer systemweiten Sicherheit benötigen. Mit Security und Patch Manager lassen sich Routineprozesse im Zusammenhang mit der Verwaltung von Security- und Patch-Inhalten und dem Ordnen und Anzeigen dieser Inhalte automatisieren. Analysieren Sie verwaltete Geräte mithilfe von Sicherheitsscans-Tasks und Richtlinien auf bekannte plattformspezifische Anfälligkeiten. Sie können ausführbare Patch-Dateien herunterladen und verwalten. Schließlich können Sie erkannte Anfälligkeiten reparieren, indem Sie die vorgeschriebenen Patch-Dateien bereitstellen und installieren und sich von der gelungenen Durchführung eines Reparaturvorgangs überzeugen. Sie können zudem eigene benutzerdefinierte Anfälligkeitsdefinitionen erstellen, um verwaltete Geräte auf bestimmte Betriebssystem- und Anwendungsbedingungen hin zu überprüfen, die den Betrieb und die Sicherheit Ihres Systems beeinträchtigen können. Benutzerdefinierte Definitionen können entweder nur für Erkennungsaufgaben oder sowohl für Erkennungs- als auch Reparaturaufgaben konfiguriert werden.



Erstellen angepasster Definitionen und Erkennungsregeln

Zusätzlich zu bekannten Anfälligkeiten, die Sie über den LANDesk Security und Patch Manager-Dienst aktualisieren, können Sie auch eigene benutzerdefinierte Definitionen erstellen — einschließlich benutzerdefinierter Erkennungsregeln, verknüpfter Patch-Dateien und spezieller Zusatzbefehle, die eine erfolgreiche Reparatur gewährleisten. Anfälligkeitsdefinitionen bestehen aus einer eindeutigen Kennung, Titel, Datum der Veröffentlichung, Sprache, zusätzlichen Identifizierungsdaten und den Erkennungsregeln, die dem Sicherheitsscanner mitteilen, wonach er auf Zielgeräten suchen soll. Erkennungsregeln definieren die Plattform, Anwendung, Datei oder die Registrierungsbedingungen, nach denen der Sicherheitsscanner sucht, um eine Anfälligkeit auf gescannten Geräten ausfindig zu machen. Die Benutzerdefinierten Anfälligkeitsdefinitionen des Security und Patch Managers sind eine leistungsstarke, flexible Funktion, mit der Sie eine zusätzliche systembezogene Ebene der Patch-Sicherheit auf Ihrem LANDesk-System realisieren können. Zusätzlich zur Verbesserung der Patch-Sicherheit und anderen innovativen Tasks, die die Vorteile der Scanfunktionen des Anfälligkeitsscanners nutzen, können benutzerdefinierte Anfälligkeiten u.a. auch dazu verwendet werden, Systemkonfigurationen zu analysieren, nach bestimmten Datei- und Registrierungseinstellungen zu suchen und Anwendungsaktualisierungen zu verteilen.

Reparaturmethoden

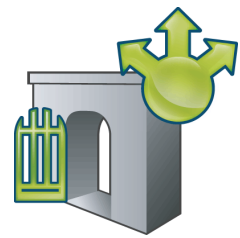
Der Security und Patch Manager stellt folgende Methoden für die Reparatur von der Konsole zur Verfügung:

- Geplanter Task
- Richtlinienbasiert
- Automatisches Korrigieren

Die Reparatur mittels geplanten Tasks lässt sich mit einer Push-Verteilung vergleichen, da das Patch vom Core Server via Push-Prozedur an Geräte übermittelt wird. Eine Richtlinie ist dagegen als Pull-Verteilung einzustufen, da der Richtlinienagent auf dem Gerät den Core Server auf zutreffende Richtlinien durchsucht und das Patch dann mittels Pull-Prozedur vom Core Server abrufen.

LANDesk Management Gateway

Seit der Version 8.7 bietet LANDesk die Möglichkeit bisher nicht zugängliche User über das Internet mittels Management Gateway zu verwalten. Dies ermöglicht einen sicheren Datenaustausch ohne Standleitung oder VPN. Durch die SSL-Verschlüsselung können Sie sicher sein, dass kein Unbefugter auf Ihre Daten Zugriff hat. Die Steuerung von externen Geräte ist aufgrund der Dynamischen Bandbreitendrosselung unabhängig vom Standort. LANDesk steuert automatisch die Bandbreitenauslastung und ermöglicht selbst bei einer 56K Anbindung optimale Leistung. Dabei ist das Management Gateway in der Lage bis zu 4000 gleichzeitigen Verbindungen aufzubauen und zu halten.



LANDesk Agent Wächter

Mit dem LANDesk-Agent-Wächter können Sie den Status ausgewählter LANDesk-Agentendienste und -Dateien proaktiv überwachen, damit Sie sich jederzeit von der Integrität dieser Dienste und Dateien überzeugen und sicherstellen können, dass wichtige LANDesk-Dienste auf verwalteten Geräten wie vorgesehen ausgeführt werden. Sie können den Agent-Wächter außerdem jederzeit aktualisieren, ohne eine vollständige Agentenkonfiguration durchführen zu müssen. Der Agent-Wächter überwacht nicht nur kritische LANDesk-Dienste und -Dateien, sondern übernimmt auch weitere Aufgaben für Sie, zum Beispiel das Reaktivieren beendeter Dienste, Zurücksetzen von Diensten auf automatisches Startup, Wiederherstellen von zu löschenden Dateien beim Neustart und Rückmeldung an den Core Server bei begründetem Verdacht auf Dateimanipulation.

Connection Control

Der Connection Control Manager überwacht und beschränkt den Zugriff auf I/O-Geräte und Netzwerkverbindungen. Sie sind in der Lage festzulegen, welche Geräte mit welchen Netzwerk-IP-Adressen Verbindungen herstellen können. Außerdem können Sie die Verwendung von Geräten beschränken, über die der Datenzugriff auf das Gerät ermöglicht wird (beispielsweise Anschlüsse, Modems, Treiber und drahtlose Verbindungen). Immer, wenn das Gerät eine Netzwerk-/Geräteverbindung aufbaut oder Änderungen an einer Netzwerk-/Geräteverbindung vornimmt, wendet der Connection Control Manager Konfigurationsregeln an. Zu diesen Regeln gehört das automatische Trennen unzulässiger Verbindungen und Alarmieren des Core Servers. Es bestehen zwei Möglichkeiten zum Konfigurieren von Netzwerkbeschränkungen. Entweder Sie geben an, welche Netzwerkadressen zulässig sind, oder Sie geben an, welche blockiert sind. Weiter besteht die Möglichkeit, entweder eine ganze USB-Gerätekategorie (z. B. Speichergeräte) oder nur bestimmte USB-Geräte zu blockieren. Sie



können mehrere Konfigurationen speichern und nach Bedarf auf mehrere Geräte übertragen. Um eine von Ihnen erstellte Konfiguration zu aktivieren, müssen Sie diese auf den Zielgeräten bereitstellen. Connection Control Manager unterstützt dabei Geräte, die Windows 2000, Windows Server 2003 und Windows XP ausführen.

LANDesk Host Intrusion Prevention System

LANDesk® Host Intrusion Prevention System ist Bestandteil der LANDesk® Security Suite. Zusammen mit der LANDesk® Security Suite und der LANDesk® Management Suite ergänzt LANDesk® Host Intrusion Prevention System Ihre Security Lösung und ermöglicht Ihnen die zentrale Kontrolle über die gesamte Netzwerkumgebung. LANDesk® Host Intrusion Prevention System hilft Ihnen, durch Anwendungskontrolle böswillige Attacken auf Ihr System zu verhindern.



Es ist maßgebend, das System mit den aktuellsten Antivirus-Updates zu schützen und sicherzustellen, dass bekannte Viren wichtige Daten nicht beschädigen oder den Arbeitsablauf beeinträchtigen. Aber durch die rapide wachsende Anzahl von Zero-Day Exploits wird es immer schwieriger, das System konstant zu schützen. An diesem Punkt kommt LANDesk® Host Intrusion Prevention System zum Einsatz. Es arbeitet zusammen mit der LANDesk® Security Suite und der LANDesk® Management Suite und bietet Ihnen ein zusätzliches Maß an Sicherheit – auch Vorbeugung genannt.

LANDesk® Host Intrusion Prevention geht weit über den Standard-Virenschutz hinaus – Es überwacht und beendet verdächtige Vorgänge, die auf eine böswillige Attacke auf Ihr System hinweisen. Auch wenn noch kein Antivirus-Update vorliegt, so können Sie mit LANDesk® Host Intrusion Prevention Ihr System sicher und zuverlässig überwachen und vor Angriffen schützen.

- zusätzliche Sicherheit für Ihr System und Schutz gegen Zero-Day Attacken, auch bevor ein Hotfix verfügbar ist.
- Gesteigerte Effizienz und reduzierte Trainings- und Wartungskosten durch eine Lösung für Ihr komplettes Security-System.
- Genaue Kontrolle, welche Anwendungen von bestimmten Usergruppen ausgeführt bzw. nicht ausgeführt werden dürfen.
- Automatisches Blocken & Logging von Fremdzugriffen auf Ihr System.
- Erkennt böartige Schreibvorgänge und Veränderungen der Registry automatisch und verhindert das Ausführen von Malware auf Ihrem System.
- Kompatibel zu Produkten wie Symantec Antivirus und McAfee Enterprise.

Rollenbasierte Administration

Die rollenbasierte Administration optimiert die LANDesk-Netzwerksicherheit, indem sie Ihnen die Möglichkeit bietet, den Zugriff von Benutzern auf verwaltete Geräte, Konsolenansichten und bestimmte Funktionen und Tools zu kontrollieren. Dabei können Sie festlegen, wer auf Geräte in Ihrem Netzwerk

Zugriff erhält und welche Tools oder Funktionen auf diesen Geräten verwendet werden dürfen. LANDesk Administratoren besitzen Vollrechte, mit denen sie auf alle Bereiche der Anwendung zugreifen und Benutzern gezielt Rechte zuweisen können. Die von Ihnen erstellten Rollen können auf den Verantwortungsbereichen der Benutzer basieren, den Verwaltungstasks, die Sie den Benutzern einräumen möchten, oder den Geräten, auf die die Benutzer zugreifen und die sie verwalten sollen. Der Gerätezugriff lässt sich auf einen Standort, beispielsweise ein Land, eine Region, ein Bundesland, eine Stadt oder sogar ein bestimmtes Büro oder eine Abteilung, einschränken. Der Zugriff kann auch auf eine bestimmte Geräteplattform, einen Prozessortyp oder andere Hard- und Softwareattribute der Geräte eingeschränkt werden. Bei der rollenbasierten Administration können Sie frei entscheiden, wie viele Rollen Sie erstellen möchten, welche Benutzer diese Rollen wahrnehmen können und wie groß oder klein ihr Bereich des Gerätezugriffs sein soll. Sie können z. B. einen oder mehreren Benutzern die Rolle des Managers für die Softwareverteilung zuordnen, einen anderen Benutzer für die Fernsteuerungsvorgänge verantwortlich machen, einen weiteren Benutzer mit der Berichterstellung beauftragen usw.

Dies sind nur Beispiele für administrative Rollen. Die rollenbasierte Administration besitzt die Flexibilität, Sie so viele benutzerdefinierte Rollen erstellen zu lassen, wie Sie möchten. Sie können dieselben Rechte auch verschiedenen Benutzern zuweisen, den Zugriff dieser Benutzer jedoch auf eine begrenzte Gruppe von Geräten limitieren. Sogar ein Administrator kann durch einen Bereich eingeschränkt werden, indem seine Administratortasks auf eine bestimmte geographische Region oder einen bestimmten Typ von verwalteten Geräten eingeschränkt wird. Wie Sie am besten von der rollenbasierten Administration profitieren, hängt von Ihren Netzwerk- und Personalressourcen und Ihrem individuellen Unternehmensbedarf ab.

Abfragen

Die LANDesk Security Suite bietet Ihnen die Möglichkeit Datenbankabfragen nach verwalteten Geräten zu starten.

Mithilfe von Abfragen können Sie auf der Basis bestimmter System- oder Benutzerkriterien nach in der Core-Datenbank gespeicherten Netzwerkgeräten suchen und diese entsprechend ordnen. Damit steht Ihnen ein praktisches Hilfsmittel für die Netzwerkverwaltung zur Verfügung. So können Sie beispielsweise eine Abfrage erstellen und ausführen, die nur Geräte mit einer Taktgeschwindigkeit von weniger als 166 MHz, weniger als 64 MB Arbeitsspeicher oder einer Festplatte mit weniger als 2 GB Speicherkapazität erfasst. Erstellen Sie eine oder mehrere Abfrageanweisungen für diese Bedingungen und verknüpfen Sie diese Anweisungen mithilfe von logischen Operatoren. Wenn die Abfragen ausgeführt wurden, können Sie die Ergebnisse drucken, auf die entsprechenden Geräte zugreifen und sie verwalten.

Außerdem bietet Ihnen die LANDesk Security Suite die Möglichkeit zur Abfrage mit dem Directory Manager über LDAP (Lightweight Directory Access Protocol) nach Geräten in

anderen Verzeichnissen zu suchen und auf diese Geräte zuzugreifen und sie zu verwalten.

Lightweight Directory Access Protocol (LDAP) ist ein dem Industriestandard entsprechendes Protokoll für den Zugriff auf und die Anzeige von Informationen über Benutzer und Geräte. LDAP ermöglicht Ihnen die Organisation und Speicherung dieser Informationen in einem Verzeichnis. Ein LDAP-Verzeichnis ist insofern dynamisch, als dass es ggf. aktualisiert werden kann. Es wird verteilt, wodurch ein Schutz vor einem zentralen Ausfall gegeben ist. Zu allgemeinen LDAP Verzeichnissen gehören Novell Directory Services (NDS) und Microsoft Active Directory Services (ADS).

Inventarverwaltung

LANDesk verwendet einen Inventarscanner, um Geräte zur Core-Datenbank hinzuzufügen und Informationen zur Hardware und Software des Geräts zu sammeln. Sie können Inventardaten anzeigen, drucken und exportieren. Mit dem Inventarscanner sind Sie zudem in der Lage Abfragen zu definieren, Server zu Gruppen zusammenfassen und benutzerdefinierte Berichte generieren.

Der Inventarscanner erfasst Hard- und Softwaredaten und fügt sie in die Core-Datenbank ein. Wenn Sie ein Gerät mit dem Tool "Agentenkonfiguration" konfigurieren, gehört der Inventarscanner zu den Komponenten des Standard-LANDesk-Agent, die auf dem Gerät installiert werden. Der Inventarscanner wird beim erstmaligen Konfigurieren des Geräts automatisch ausgeführt. Ein Gerät gilt als verwaltet, sobald es einen Inventarscan an die Core-Datenbank sendet. Der Scanner unterstützt Macintosh-, Linux- und Windows 95/98/NT/2000/2003/XP-Geräte.



Berichte

Das Bericht-Tool nutzt die Vorteile des leistungsstarken Inventarscanners, mit dem Hardware- und Softwaredaten erfasst werden, um nützliche, aussagekräftige und aktuelle Berichte zu erstellen. Sie können die vordefinierten Dienst- und Inventarstandardberichte verwenden oder eigene Berichte erstellen. Die vordefinierten Berichte werden standardmäßig mit der Anwendung zur Verfügung gestellt. Mithilfe der benutzerdefinierten Berichte können Sie eine spezifische

Informationssammlung definieren und als Basis für einen Bericht verwenden. Die vordefinierten oder benutzerdefinierten Parameter werden ausgeführt und es wird ein Bericht erstellt, der die relevanten Daten enthält. Der Bericht kann von der Konsole aus angezeigt werden. Darüber hinaus können Sie Berichte planen, die veröffentlicht und auf einem Datenträger oder in einer geschützten Dateifreigabe in Ihrem Netzwerk gespeichert werden. Dort können sie von jedem Benutzer, der über die entsprechenden Anmeldeinformationen verfügt, geöffnet und angezeigt werden. Mithilfe eines von Ihnen erstellten Zeitplans können die veröffentlichten Berichte per E-Mail an Empfänger gesendet werden, die über die erforderlichen Rechte und Bereiche verfügen



Skripte und Tasks



Die LANDesk Security Suite beinhaltet ein leistungsstarkes System für die Verwaltung geplanter Tasks. Sowohl der Core Server als auch die verwalteten Geräte verfügen über Dienste/Agenten, die geplante Tasks unterstützen. Die Management Suite-Konsolen und Webkonsolen können Tasks zum Scheduler hinzufügen. Ein Task besteht aus einem Verteilungspaket, einer Verteilungsmethode, Zielgeräten und einem Zeitplan für die Verteilung. Tasks, bei denen es sich nicht um Verteilungstasks handelt, beinhalten ein Skript, Zielgeräte und einen Zeitplan. Zu den anderen Tasks, die Sie planen können, gehören:

- Gerätekonfigurationen
- Verschiedene benutzerdefinierte Skripts
- Bereitstellen von benutzerdefinierten Datenformularen
- Erkennung nicht verwalteter Geräte
- Anfälligkeitsscans
- Softwareausführung auf verwalteten Geräten

Beim Durcharbeiten der Dialogfelder für die Skripterstellung wird für diese Tasks eine ASCII-Textdatei im Windows INI-Format mit einer .INI-Erweiterung angelegt. Softwareverteilungsskripte bilden eine Ausnahme. Sie erstellen keine INI-Datei und werden stattdessen in der Datenbank gespeichert. Die Skripte enthalten nur Informationen zu dem erstellten Task. Sie geben keine Auskunft darüber, auf welchen Geräten das Skript ausgeführt wird. Die Skripte verwenden eine benutzerdefinierte Scripting-Sprache, die nur von der LANDesk Security Suite verwendet wird.

Rollup-Core zum Planen globaler Tasks

Wenn in Ihrer LANDesk-Umgebung ein Rollup-Core installiert ist, können die auf diesem Rollup-Core erstellten Tasks global geplant werden. Darüber hinaus unterstützen diese Tasks Ziele von unterschiedlichen Child-Cores. Wenn Sie einen Task auf dem Rollup-Core erstellen und planen, überprüft der Rollup-Core in der Zielliste, welche Ziele zu welchem Child-Core Server gehören. Der Rollup-Core sendet dann den Task und den zugehörigen eindeutigen Abschnitt der Gesamt-Zielliste an die einzelnen Child-Core Server. Jeder Child-Core Server führt den Task im Hintergrund aus und gibt den Taskstatus an den Rollup-Core zurück. Wenn ein Child-Core zwar Ziele hat, aber über keine Rollup-Core-Zertifikate verfügt, führt der Rollup-Core den Task stattdessen auf diesen Zielen aus.

Softwareverteilung

Mithilfe der Softwareverteilung können Sie Software- und Dateipakete auf Geräten bereitstellen, auf denen folgende Betriebssysteme ausgeführt werden:

- Windows 95B/98SE
- Windows NT (4.0 SP6a und höher)

- Windows 2000/2003/2008/XP/Vista
- Mac OS 9.2.2, 10.2.8., 10.3.9, 10.4.11, 10.5.x
- Red Hat Linux Enterprise 3, 4 und 5 WS
- Red Hat Linux 7.3, 8.0 und 9.0
- Suse Linux 9.1 und 10
- Ubuntu
- Mandriva Linux 10.1

Folgende Funktionen sind für die Softwareverteilung verfügbar:

- LANDesk Targeted Multicasting-Funktionen, die bei der Massenverteilung großer Pakete den Bandbreitenverbrauch minimieren, ohne fest zugeordnete Hardware oder ein Neukonfigurieren der Router erforderlich zu machen.
- Einfacher Task-Scheduler arbeitet mit der Inventardatenbank zusammen, um die Auswahl der Ziele zu erleichtern
- Richtlinienbasierte Verteilungen, einschließlich Unterstützung zur Erstellung von richtliniengestützten Push-Tasks
- Unterstützung mobiler Geräte, einschließlich Bandbreitenerkennung, Checkpoint-Neustarts und die Fähigkeit zur Auftrags erledigung unter Verwendung einer Richtlinie
- Package Builder mit vollem Funktionsumfang
- Verteilung beliebiger Pakettypen, einschließlich MSI, setup.exe und anderer Installationsprogramme

Wenn Sie noch nicht über ein Paket verfügen, das Sie bereitstellen können, können Sie mithilfe der Pakettechnologie der Security Suite ein ausführbares Einzelprogramm für die erforderliche Softwareinstallation erstellen. Wenn Sie ein Paket erstellt haben, speichern Sie es auf einem Web- oder Netzwerkserver, dem so genannten "Delivery Server". Über die Konsole können Sie die Verteilung planen. Der Core Server übermittelt den Speicherort des Pakets (URL oder UNC-Pfad) an das Gerät. Das Gerät kopiert dann nur die Dateien oder die Teile der Dateien, die es benötigt, vom Delivery-Server. Wenn Sie beispielsweise ein Softwareprogramm neu installieren, weil einige Dateien beschädigt sind oder fehlen, werden vom System nur die beschädigten bzw. fehlenden Dateien kopiert, nicht das ganze Programm. Diese Technologie funktioniert auch über WAN-Verbindungen. Sie können das Paket auf mehreren Servern speichern und festlegen, dass die Geräte jeweils auf den Server zugreifen, der für ihre Anforderungen am besten geeignet ist. Die Softwareverteilung nimmt zudem unterbrochene Download-Vorgänge für Pakete wieder auf. Wenn beispielsweise ein mobiles Gerät gerade ein umfangreiches Paket heruntergeladen hat, als seine Netzwerkverbindung getrennt wurde, wird der Ladevorgang nach der Wiederherstellung der Verbindung genau an der Stelle fortgesetzt, an der er unterbrochen wurde.

Checkpoint-Neustarts auf Byte-Ebene und dynamische Bandbreitendrosselung

Die LANDesk Security Suite 8 und neuere Versionen unterstützen bei der Verteilung Checkpoint-Neustarts auf Byte-Ebene und dynamische Bandbreitendrosselung. Checkpoint-Neustarts werden von Verteilungsaufträgen unterstützt, die von SWD zuerst in den Cache-Ordner des Geräts kopiert werden. Wenn eine Bandbreitensteuerungsoption ausgewählt wird, werden die Dateien zuerst in den Cache des Geräts kopiert, mithilfe von "Checkpoint-Neustart" können dann unterbrochene Verteilungsvorgänge an der Stelle wieder aufgenommen werden, an der sie unterbrochen wurden.

Durch die Dynamische Bandbreitendrosselung wird festgelegt, dass der von einem Gerät erzeugte Netzwerkverkehr Vorrang vor dem durch die Verteilung bedingten Verkehr hat. Mit dieser Option wird zudem erzwungen, dass die gesamte Datei in den Cache des Geräts heruntergeladen wird. Damit wird gleichzeitig die Option für Checkpoint-Neustarts auf Byte-Ebene aktiviert. Das heißt, dass Download-Vorgänge im Fall einer Unterbrechung an der Stelle wieder aufgenommen werden, an der sie unterbrochen wurden. Wenn Sie diese Option auswählen und die Prozentangabe für Minimal verfügbare Bandbreite auf 0 belassen, wird die Verteilung auf etwa ein Paket pro Sekunde gedrosselt, sobald das Gerät Netzwerkverkehr initiiert, und bleibt auf diesem Niveau, bis der Netzwerkverkehr endet. Wenn Sie den Wert für die minimal verfügbare Bandbreite heraufsetzen, reserviert das System ungefähr die von Ihnen angegebene Menge an Gerätebandbreite für die Verteilung, sofern die Verteilung Netzwerkbandbreite benötigt und Anwendungen auf dem Gerät um Bandbreite konkurrieren.

Dynamische Bandbreitendrosselung ist nicht auf Windows 95-, Macintosh- oder DOS-Geräten verfügbar. Windows 98- und Windows NT-Geräte können die dynamische Bandbreitendrosselung verwenden, wenn auf ihnen Internet Explorer (ab Version 4) installiert ist.

Sie können eine "kollektive Bandbreitendrosselung" konfigurieren, sodass nur von einem Gerät aus der Multicast-Domäne Dateien aus der Remotequelle heruntergeladen werden. Sie können auch die beim Herunterladen aus der Quelle verwendete Bandbreitenmenge konfigurieren. Diese Funktion ist auf allen Versionen des Windows-Systems verfügbar. Kollektive Bandbreitendrosselung wird nicht auf Macintosh- oder DOS-Systemen unterstützt.

Softwareverteilung mit Targeted Multicast

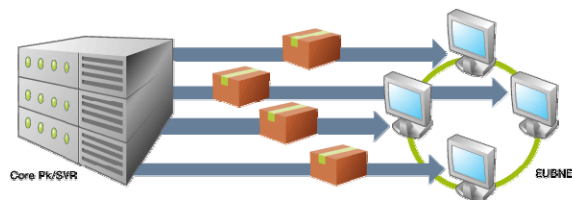
Mit der LANDesk Targeted Multicast-Technologie können Sie große Pakete als Massen-Rollout im Netzwerk verteilen und dabei die Netzwerkbelastung so gering wie möglich halten. Die Targeted Multicast-Funktionen benötigen zur Unterstützung von Multicast-Paketen weder eine zusätzliche Hardware- oder Software-Infrastruktur noch spezielle Router-Konfigurationen. Sie profitieren von den enormen Vorteilen der Multicast-Technologie ohne die sonst üblichen

Probleme. Targeted Multicast unterstützt Ihre vorhandenen Softwareverteilungspakete. Mit Targeted Multicast lassen sich Softwarepakete ganz einfach verteilen, selbst in WAN-Umgebungen mit mehreren Hops und niedriger Verbindungsgeschwindigkeit (56 KBit/s). Targeted Multicast verwendet HTTP für die Übermittlung von einer Website an einen Subnetzrepräsentanten. Der Security Suite-Inventarscanner stellt dem Targeted Multicast-Dienst alle Subnetzinformationen zur Verfügung.

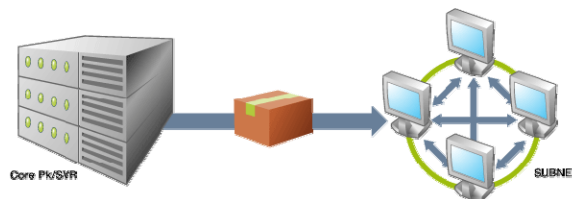
Targeted Multicast bietet zahlreiche Vorteile, die Standard-Multicast-Methoden nicht aufweisen. Mithilfe des inventarbasierten Targeting von Geräten können Sie ein Paket über ein Multicast an eine ausgewählte Gruppe von Computern senden, die bestimmte Kriterien erfüllen. Targeted Multicast ist auch deshalb unkompliziert, weil Router nicht extra für die Verarbeitung von übermittelten Paketen konfiguriert werden müssen. Verglichen mit konventionellen Softwareverteilungsmethoden wird bei der Übermittlung von Softwarepaketen mit Targeted Multicast deutlich weniger Zeit und Bandbreite benötigt. Statt für

jedes Gerät ein Paket über das Netzwerk zu senden, wird für jedes Subnetz nur eine Übertragung durchgeführt. Je höher die Anzahl der Gerät im jeweiligen Subnetz, umso mehr Bandbreite wird

wird in Push-, Push- und Liefermethoden (nur



eingespart. Multicast richtlinienbasierten Multicast-Cache) unterstützt.



Peer Download

Peer Download ist eine Targeted Multicast-Option, die Zielgeräte zwingt, ein Paket aus dem lokalen Cache des Geräts oder von einem Peer im gleichen Subnetz zu installieren. Diese Option reduziert zwar den Netzwerkverkehr, die Paketinstallation kann aber nur dann erfolgreich ausgeführt werden, wenn sich das Paket im lokalen Cache oder im Cache eines Peer befindet.

Verteilen von Softwareprodukten an Linux-Geräte

Sobald Sie die Linux-Agenten bereitgestellt haben, können Sie Softwareprodukte an Ihre Linux-Geräte verteilen. Die erstmalige Bereitstellung eines Linux-Agenten erfolgt über eine SSH-Verbindung. Nachdem die Agenten installiert sind, verwendet der Core Server den Standard LANDesk Agent, um mit dem Linux-Server zu kommunizieren und Dateien zu übertragen. Für die Verteilung von Software an ein Linux-Gerät benötigen Sie

Administratorrechte. Sie können nur RPMs an Linux-Geräte verteilen. Die Linux-Agenten installieren automatisch den von Ihnen verteilten RPM. Der eigentliche RPM wird nach der Installation nicht auf dem Server gespeichert. Sie können den von Ihnen angegebenen RPM mithilfe der Softwareverteilung installieren und deinstallieren. Für die Linux-Softwareverteilung werden nur Push-Verteilungsmethoden unterstützt. Die Einstellungen in der Push-Verteilungsmethode werden für die Linux-Softwareverteilung ignoriert, sodass es keine Rolle spielt, welche Push-Verteilungsmethode Sie auswählen oder wie die Einstellungen darin lauten.

Richtlinienbasierten Verwaltung

Die richtlinienbasierte Verwaltung wiederholt in regelmäßigen Abständen die Ausführung von Abfragen, die Sie als Teil der Richtlinie definiert haben. Auf diese Weise werden Ihre Richtlinien auf alle neu hinzukommenden verwalteten Geräte angewendet. Angenommen im LDAP-Verzeichnis gibt es einen Container "Abteilung", der Benutzerobjekte enthält. Alle Benutzer, deren Abteilungsobjekt "Marketing" ist, verwenden die Standardanwendungen. Nachdem Sie eine Richtlinie für die "Marketing"-Benutzer eingerichtet haben, werden auf den Computern der Benutzer, die dem Objekt "Marketing" neu hinzugefügt werden, automatisch die richtigen Anwendungen installiert.



Erkennung nicht verwalteter Geräte

Die Funktion "Erkennung nicht verwalteter Geräte" (UDD, Unmanaged Device Discovery) ist eine Neuerung der Version 8. UDD findet Clients in Ihrem Netzwerk, die keinen Inventarscan an die Core-Datenbank gesendet haben. UDD verwendet bei der Suche nach nicht verwalteten Geräten mehrere Methoden.

- Auf Computern wird nach dem LANDesk Agent gesucht. Mit dieser Option werden Computer gefunden, die über Management Suite, LANDesk Client Manager, LANDesk System Manager und so weiter verfügen.
- Mittels einer ICMP-Ping-Suche nach Computern. Diese Suche ist am gründlichsten, verursacht jedoch auch den größten Zeitaufwand. Sie können die Suche auf bestimmte IP- und Subnetzbereiche beschränken. Standardmäßig verwendet diese Option NetBIOS, um Informationen über das Gerät zu sammeln.
- UDD versucht, den Betriebssystemtyp über TCP-Paketantworten zu ermitteln. Der IP-Fingerabdruck verlangsamt den Erkennungsvorgang etwas.
- UDD verwendet SNMP zum Erkennen von Geräten.
- Es wird in einer von Ihnen angegebenen Domäne nach Geräten gesucht. Die Mitglieder werden unabhängig davon, ob der Computer an- oder ausgeschaltet ist, gefunden.
- Die Suche in einem von Ihnen angegebenen Verzeichnis nach Geräten. Die Mitglieder werden unabhängig davon, ob der Computer an- oder ausgeschaltet ist, gefunden.
- UDD unterstützt außerdem die folgenden zusätzlichen Erkennungsmethoden.

- IPMI: Sucht nach Servern mit aktiviertem Intelligent Platform Management Interface. Damit können Sie auf zahlreiche Funktionen zugreifen, unabhängig davon, ob der Server eingeschaltet ist oder in welchem Zustand sich das Betriebssystem befindet.
- Servergehäuse: Sucht nach Blade-Server Chassis Management Modules (CMMs). Die Blades in den Servern werden als normale Server erkannt.
- Intel AMT: Sucht nach Intel Active Management Technology-kompatiblen Geräten.

UDD unterstützt darüber hinaus die erweiterte Geräteerkennung, die mit einem Geräteagenten arbeitet, der das Netzwerk auf neue ARP-Broadcasts abhört. Anschließend überprüft der Agent der erweiterten Geräteerkennung dann ARP-erkannte Geräte auf das Vorhandensein des LANDesk-Agenten. Wenn der LANDesk-Agent nicht reagiert, zeigt die erweiterte Geräteerkennung das Gerät in der Liste Computer an. Die erweiterte Geräteerkennung leistet optimale Dienste in Situationen, in denen Firewalls Geräte daran hindern, auf die normalen pingbasierten UDD-Erkennungsmethoden zu antworten. Um die Suche nach nicht verwalteten Geräten zu automatisieren, können Sie regelmäßige Erkennungsvorgänge planen. Sie können beispielsweise Ihr Netzwerk in Drittel unterteilen und zeitplangesteuert für jedes Drittel eine Ping-Suche pro Nacht durchführen

Alert Management System (AMS)

Das LANDesk Alert Management System (AMS) automatisiert Aktionen, die als Reaktion auf Alarmmeldungen im Netzwerk ausgelöst werden. AMS überwacht LANDesk-Komponenten und -Geräte im Hinblick auf das Auftreten bestimmter Ereignisse. Wenn diese Ereignisse stattfinden, sendet die Komponente oder das Gerät eine Alarmmeldung an AMS. AMS kann Sie über den Alarm informieren, indem das Modul die von Ihnen konfigurierten Alarmaktionen durchführt. Beispielsweise können Sie die Konsole so konfigurieren, dass Sie benachrichtigt werden, sobald jemand eine Fernsteuerungssitzung einzurichten versucht. Wenn dieses Ereignis eintritt, erkennt AMS den Versuch und führt die konfigurierten Alarmaktionen aus, sendet z. B. eine Nachricht per Internet-Mail oder Pager.