LANDesk® System Manager 8.7

Manual de instalación e implementación

LANDesk®

v8.5

Ninguna parte de este documento constituye una garantía o licencia expresa o implícita. LANDesk no asume ningún tipo de responsabilidad por dichas garantías o licencias, incluidas pero sin limitarse a: Adecuación para un propósito determinado, comerciabilidad, infracción de patentes de propiedad intelectual u otros derechos de terceros o de LANDesk; indemnización y otros. Los productos LANDesk no se diseñaron para utilizarse en aplicaciones médicas, de emergencia o de mantenimiento de constantes vitales. Se le advierte al lector que terceros pueden tener derechos de propiedad intelectual pertinentes a este documento y las tecnologías descritas en él; por tanto, se le aconseja que solicite asesoramiento legal de representantes jurídicos competentes, sin que esto constituya una obligación de LANDesk.

LANDesk se reserva el derecho de modificar el presente documento o las especificaciones y descripciones de producto relacionadas en cualquier momento y sin previo aviso. LANDesk no garantiza el uso de este documento, ni asume responsabilidad alguna por los errores que puedan aparecer en él, ni se compromete a actualizar la información contenida en el mismo.

Contenido

Introducción

Esta guía le ayuda en el proceso de instalación e implementación de LANDesk® System Manager, un producto que ayuda a reducir el coste total de propiedad al simplificar la administración de los equipos y la solución de los problemas más comunes de los mismos.

En esta introducción se abordan los temas siguientes:

Características de esta versión

Con el crecimiento de la industria de la informática, los equipos de sistemas se volvieron más complejos y de difícil manejo. El tiempo que se dedica al mantenimiento y a la reparación de un equipo a través de sus años de operación puede aumentar su coste total de propiedad (TCO) mucho más allá del precio inicial de compra. LANDesk® System Manager puede ayudar a reducir el TCO al simplificar la administración de los equipos y la resolución de los problemas comunes en los mismos.

- **Ver inventario del sistema:** System Manager proporciona información completa sobre la configuración de hardware y software del equipo.
- **Supervisar la condición de un equipo:** System Manager informa cuando un equipo se encuentra en una condición crítica o que requiere precaución, e informa sobre elementos como temperatura, voltaje, memoria libre y espacio en el disco.
- **Recibir alertas de los sucesos del sistema:** System Manager puede utilizar varios métodos de alerta para notificarle problemas.
- **Supervisar el rendimiento histórico o en tiempo real:** System Manager permite supervisar el rendimiento de varios objetos de sistema como unidades, procesadores, memoria y servicios. Puede seleccionar acciones de alerta que envíen una notificación si un contador específico sobrepasa un umbral superior o inferior una cantidad determinada de veces.
- **Supervisar procesos y servicios actuales:** System Manager permite ver los servicios actuales y sus estados, o establecer acciones de alerta para notificarle los cambios en el estado del servicio.
- **Apagar, encender y reiniciar equipos de forma remota:** System Manager habilita la administración de energía remota desde la consola del administrador para los sistemas que lo admitan.
- **Vista de tarea programada:** Vea o vuelva a programar todas las tareas de implementación de agente, detección,
- **Compatibilidad mejorada de SO:** Administre todos los dispositivos en su entorno heterogéneo desde una sola consola. Es compatible con Windows 2000, 2003 y XP Profesional, Red Hat Linux, SUSE Linux, HP-UX y AIX. Consulte la Fase 1: Requisitos del sistema, si desea más información.

- **Compatibilidad con Intel* AMT e Intelligent Platform Management Interface (IPMI):** System Manager es compatible con componentes de administración basada en hardware que proporcionan capacidad para administrar de forma remota los dispositivos conectados a la red en cualquier estado del sistema a través de la comunicación fuera de banda (OOB). Siempre y cuando el dispositivo esté conectado a una red empresarial y tenga alimentación en espera, podrá tener acceso al inventario, ver información de diagnóstico remoto y reiniciar el sistema de forma remota.
- **Compatibilidad con servidores de hoja:** Se ofrece compatibilidad con los módulos de administración de chasis de hoja (CMM) y servidores de hoja, incluyendo las funciones de administración e inventario.
- **Herramienta de secuencia:** Permite programar y ejecutar tareas personalizadas en los dispositivos
- **Programador de tareas:** El esquema único de base de datos, con integridad y escalabilidad de datos mejoradas, permite el acceso a un gran conjunto de información sobre los dispositivos administrados (incluye la integración total con Management Suite). Parte de este esquema único es el programador de tareas. Ahora podrá ver todas las tareas (detección, configuración de agente, en una ventana común. En esta ventana puede cambiar la programación o hacer que la misma sea recurrente.
- **Administración basada en funciones:** Configura el acceso de los usuarios a los dispositivos y a las herramientas de red según la función administrativa de los usuarios en la organización. La administración basada en funciones permite asignar un ámbito para determinar los dispositivos que puede ver y administrar el usuario y los derechos para especificar las tareas que pueden realizar.
- **Detecciones de dispositivos no administrados:** Detecte dispositivos en la red mediante varios métodos. El producto identifica los servidores que ejecutan Windows o Linux, los servidores y chasis de hoja, los servidores habilitados para IPMI, los servidores habilitados para AMT, al igual que otros dispositivos de red. Detección programable de dispositivos para estar constantemente al tanto de los dispositivos nuevos. También se pueden generar informes de los dispositivos no administrados de la red.
- **Seguridad mejorada:** El modelo de seguridad basado en certificados permite que los dispositivos se comuniquen sólo con servidores y consolas centrales autorizados.
- **Distribución de software:** Automatice el proceso de instalación de aplicaciones de software o de distribución de archivos en dispositivos.
- **Informes:** Se incluyen informes de servicio predefinidos para la planificación y el análisis estratégico.
- **Compatibilidad con tareas programadas** proporciona varios inicios de sesión para el servicio programador con los cuales se puede realizar la autenticación cuando se ejecutan tareas en dispositivos que no tienen agentes. Esto resulta particularmente útil al administrar dispositivos en varios dominios de Windows.

Fundamentos del producto

System Manager administra los dispositivos que ejecutan varios sistemas operativos diferentes, incluyendo Windows 2000 Pro SP4, Windows XP Pro SP1, servidores Windows* 2000/2003, servidores Red Hat Enterprise Linux v3, servidores SUSE Linux 9, servidores HP-UX y servidores AIX. Además, ofrece una interfaz común para la administración de dispositivos de dichos sistemas operativos de red. También puede coexistir con otros productos de LANDesk, tales como LANDesk® Management Suite y LANDesk® Server Manager.

Términos del producto

- **Servidor central:** el centro de un dominio de administración. Todos los servicios y archivos clave del producto se incluyen en el servidor central. Cada dominio de administración tiene un solo servidor central. El servidor central puede ser un servidor nuevo o uno reacondicionado.
- **Consola:** Consola basada en explorador que constituye la interfaz principal del producto.
- Base de datos central:El producto crea una base de datos MSDE en el servidor central para almacenar los datos de administración.
- **Dispositivos administrados:** Dispositivos de la red que tienen instalados los agentes del producto. Los "dispositivos" incluyen equipos de escritorio, servidores, equipos portátiles, chasis de hoja, etc. Un servidor central puede administrar millares de dispositivos
- **Públicos:** Elementos (como grupos, paquetes de distribución o tareas) que son visibles a todos los usuarios. Si un usuario modifica un elemento público, la modificación permanece pública. Los grupos públicos son creados por un usuario con derechos de administrador.
- **Privado o de usuario:** Elementos creados por el usuario que ha iniciado la sesión. Los demás usuarios no pueden verlos. Los elementos privados o de usuario aparecen bajo los árboles **Mis métodos de entrega**, **Mis paquetes** o **Mis tareas**. Los usuarios con derechos de administrador pueden ver los grupos privados y los paquetes y las tareas de usuario.
- **Comunes:** Elementos que los demás usuarios pueden ver. Cuando un usuario asume la propiedad de un elemento común (mediante su modificación), el elemento se ramifica en dos elementos: el elemento común permanece y el elemento del usuario se guarda en la carpeta del usuario. La instancia del elemento correspondiente al usuario ya no es visible para los demás usuarios. Los usuarios pueden marcar cualquier tarea que sea visible para ellos como común, para poder compartirla con los demás usuarios. Una vez que el usuario desmarca la opción común de las propiedades del elemento, la tarea solamente está visible en su grupo de tareas de usuario.

¿Cómo se adapta el producto a mi red?

Este producto utiliza la infraestructura de la red existente para establecer las conexiones con los dispositivos que administra. Se ha simplificado considerablemente la tarea de administración de los dispositivos existentes, ya se trate de una red pequeña o de un entorno empresarial de gran tamaño.

Uso de System Manager con Management Suite o Server Manager

Si tiene System Manager y desea utilizarlo con Management Suite o Server Manager, debe utilizar la utilidad de activación del servidor central a fin de proporcionar un nombre de usuario y una contraseña válidos para el producto con el cual desea utilizar System Manager. La instalación de System Manager / Management Suite le proporciona tres consolas con las cuales trabajar con: las consolas de Windows 32 y Web de Management Suite y la consola Web de System Manager. La consola de Server Manager incluye tres elementos de navegación (Alerta, Monitoreo y Registros) que contienen la funcionalidad que no puede encontrarse en las dos consolas de Management Suite.

Si despliega Management Suite, la instalación de Management Suite elimina el agente de System Manager en los dispositivos administrados y viceversa. Al ejecutar Management Suite con System Manager, la función de configuración de Management Suite incluye opciones de monitoreo.

Instalación de System Manager con Management Suite o Server Manager ya instalados

Si está instalado Management Suite o Server Manager en el servidor central y desea agregar System Manager, utilice la misma instalación que utilizó en la instalación original de Management Suite o Server Manager.

1. Abra autorun.exe.
2. Haga clic en **Instalar ahora**.
3. Seleccione un idioma y haga clic en **Aceptar**.
4. Se muestra una pantalla de bienvenida. Haga clic en **Siguiente**.
5. Seleccione **Modificar** (en caso de ser necesario) y haga clic en **Siguiente**.
6. Haga clic en LANDesk® Server Manager y luego en **Siguiente**.
7. Siga las instrucciones de la pantalla del asistente.

Requisitos de sistema de un servidor central

Cuando considere cuál servidor debe configurar para que funcione como el servidor central, analice los requisitos de sistema a continuación y confirme que dicho servidor cumple o supera los requerimientos de la Fase 1: Requerimientos del sistema. El verificador de requisitos previos lo realiza de forma automática.

Se recomienda el uso de un servidor central dedicado
Debido al tráfico que soporta el servidor central para administrar el dominio, se recomienda que cada uno de los servidores centrales se dedique exclusivamente a alojar el producto.

Si se instalan otros productos en el mismo servidor, es posible que se produzcan diversos problemas a corto y largo plazo.

No instale los componentes del servidor central en un controlador de dominios primario, un controlador de dominios de respaldo o un controlador de Active Directory.

Estrategias de instalación e implementación

Si se realiza la instalación mediante la ejecución automática a partir del medio del producto, el programa de instalación verifica automáticamente que su servidor central cumpla estos requerimientos antes de la instalación. La instalación e implementación de una aplicación para todo el sistema en un entorno heterogéneo requiere una metodología concreta y una cierta planificación *antes* de ejecutar el programa de instalación. Este manual incluye estrategias para la configuración del producto. Antes de implementarlo, se deben catalogar brevemente sus necesidades de administración.

Consideraciones de la estrategia de implementación

La implementación es el proceso por el cual las funciones de administración se amplían a los servidores que se desean incluir en el dominio. En este manual, la implementación se analiza en "fases".

La estrategia de implementación en fases ofrece un enfoque estructurado que permite la administración de dispositivos. Dicho enfoque se basa en dos principios muy sencillos:

- En primer lugar, implementar los componentes del producto que conlleven el menor impacto en la red ya existente y, a continuación, los componentes de mayor repercusión.
- Y en segundo, implementar el producto en distintas fases perfectamente planificadas en lugar de implementar todos los servicios de una sola vez, lo cual puede complicar la resolución de posibles errores que se deba realizar.

Este manual está organizado en secuencia para ayudarle a implementar el producto. Comience con el primer capítulo, "Fase 1: Diseño del dominio de administración" incluida más adelante en esta guía. Después, debería seguir en orden cada una de las fases.

Introducción a la instalación e implementación

Este manual agrupa las tareas de instalación e implementación en las fases que se describen a continuación. Cada una de ellas tiene su sección correspondiente, la cual le guía a través de la fase de instalación de que se trate. El capítulo de está diseñado para ayudarle a empezar a utilizar rápidamente el producto mediante la configuración de servicios, la ejecución de la consola, la detección de dispositivos, la colocación de dispositivos en la lista de Mis dispositivos y la configuración de los dispositivos administrados para realizar acciones. Tiene un diseño conciso debido a que se supone que consultará el resto del libro con mayor detalle. Algunos de los procedimientos de este manual se repiten en el capítulo de Introducción.

Resumen de la fase 1

Durante esta fase de la instalación, se diseña el dominio de administración realizando las siguientes tareas:

- Recopilar información de la red
- Confirmar que la red cumple los requisitos del sistema

Para obtener detalles al respecto, consulte la "Fase 1: Diseño del dominio de administración" incluida más adelante en esta guía.

Resumen de la fase 2

Durante esta fase, se instala el producto mediante las siguientes tareas:

- Instalar el servidor central

Para obtener información detallada, consulte la "Fase 2: Instalación del servidor central y de la consola", más adelante en este manual.

Resumen de la fase 3

Durante esta fase de la instalación, se detectan los dispositivos de la red y se implementan las agentes del producto. Puede instalar los agentes de forma automática a partir de la consola o instalarlos a petición desde el recurso compartido del servidor.

Para obtener información detallada, consulte la "Fase 3: Implementación de los agentes en los dispositivos", más adelante en este manual.

Introducción

Introducción

Bienvenido a LANDesk® System Manager, una aplicación de administración de dispositivos independiente que maximiza su valioso tiempo al permitirle administrar sus dispositivos con rapidez y eficacia, lo cual le ahorra tiempo y dinero a usted y a su organización. System Manager le permite administrar sus dispositivos en una ubicación central, agruparlos para realizar acciones (como ciclos de encendido, evaluaciones de vulnerabilidades o configuración de alertas), solucionar problemas de forma remota, conservar la seguridad de la red y mantener los dispositivos al día con las revisiones más recientes.

El propósito de este manual es ayudarle a empezar a utilizar System Manager rápidamente mediante la configuración de servicios, la ejecución de la consola, la detección de dispositivos, la colocación de dispositivos en la lista de Mis dispositivos y la configuración de los dispositivos administrados para realizar acciones.

System Manager es una aplicación Web que permite su acceso a través del navegador para administrar los servidores desde una estación de trabajo remota. Se comporta como muchas aplicaciones Web a las que está acostumbrado, pero también contiene varios controles avanzados de tipo Windows que mejoran su facilidad de uso. Por ejemplo, puede colocar el puntero del ratón sobre un control y hacer doble clic o clic con el botón secundario en él (del mismo modo que en las aplicaciones Windows). Por ejemplo, en la lista Mis dispositivos, haga doble clic en el nombre de un dispositivo para el acceso a su información específica o haga clic con el botón secundario para ver las acciones disponibles.

Los pasos siguientes le guían a través de la puesta en servicio de System Manager, de forma específica la detección de dispositivos en la red, la selección de servidores que mover a la lista Mis dispositivos, la implementación de agentes y la definición de servidores de destino para diversas tareas.

Ejecución del programa de instalación

Durante la instalación, en la página de ejecución automática, seleccione LANDesk® System Manager. Las instrucciones de instalación específicas se encuentran en la fase 2 del Manual de instalación e implementación.

Tras la instalación de System Manager, podrá empezar a utilizarlo. Las secciones siguientes explican cómo completar varias tareas necesarias: la ejecución de la utilidad de activación del servidor central, la configuración de servicios, la detección de equipos, la especificación de los dispositivos que administrarán de forma activa mediante su traslado a la lista Mis dispositivos, la agrupación de dispositivos, la adición de usuarios y la implementación de agentes. Una vez que complete estas tareas, estará listo para empezar a explorar la forma en que el sólido conjunto de funciones de System Manager puede ayudarle en la administración de sus dispositivos.

Activación del servidor central

No podrá ejecutar el producto hasta que haya activado el servidor central.

Utilice la utilidad Activación del servidor central para:

- Activar un servidor central nuevo de System Manager por primera vez
- Actualizar un servidor central existente de System Manager

Cada servidor central debe tener un certificado de autorización único.

Esta utilidad se ejecuta de forma automática en el primer inicio.

Con el servidor central conectado a Internet,

1. Haga clic en **Inicio | Todos los programas | Activación del servidor central**. Se completan el nombre de usuario y la contraseña.
2. Haga clic en **Activar**.

El servidor central se comunica con el servidor de licencias de software a través de HTTP. Si utiliza un servidor proxy, haga clic en la ficha Proxy y escriba la información de proxy. Si el servidor central tiene conexión a Internet, la comunicación con el servidor de licencias es automática y no requiere su intervención. Si el servidor central no se encuentra conectado, haga clic en Cerrar durante el reinicio y envíe por correo electrónico el archivo de autorización a licensing@landesk.com.

De forma periódica, el servidor central genera información de verificación de cuenta de nodos en el archivo "\Archivos de programa\LANDesk\Authorization Files\LANDesk.usage". Este archivo se envía de forma periódica al servidor de licencias de LANDesk Software. Este archivo está en formato XML y se firma y codifica de forma digital. Si se cambia este archivo de forma manual, se anula su contenido y el informe de uso siguiente que se envía al servidor de licencias de software.

- La utilidad Activación del servidor central no inicia una conexión a Internet de acceso telefónico de forma automática, pero si usted la inicia manualmente y ejecuta la utilidad de activación, ésta puede utilizar la conexión para enviar los datos de uso.

- También puede activar el servidor central a través de un mensaje de correo electrónico. Envíe el archivo con la extensión .TXT que se encuentra en Archivos de programa\LANDesk\Authorization a licensing@landesk.com. La asistencia al cliente de LANDesk responderá al mensaje de correo electrónico con un archivo e instrucciones para copiar el archivo en el servidor central, a fin de completar el proceso de activación.

Adición de usuarios

Los usuarios de System Manager son los que pueden iniciar una sesión en la consola y realizar tareas concretas para determinados dispositivos de la red. Los usuarios se administran a través de la función de administración basada en funciones. La administración basada en funciones permite asignar funciones administrativas especiales a los usuarios del producto, según sus derechos y ámbito. Derechos determinan las herramientas y funciones del producto que el usuario puede ver y utilizar. Ámbito determina el conjunto de dispositivos que el usuario puede ver y administrar. Puede crear una variedad de usuarios y personalizar sus derechos y ámbitos con el fin de satisfacer sus requisitos de administración. Por ejemplo, para crear un usuario que se desempeñe la función de asistencia técnica, otórguele los derechos necesarios para dicha función. Encontrará más detalles en el capítulo Administración basada en funciones del Manual del usuario de System Manager.

Al instalar el producto se crean automáticamente dos cuentas de usuario (véase más adelante). Si desea agregar más usuarios, lo puede hacer de forma manual. Los usuarios no se crean en la consola. En su lugar, los usuarios aparecen en el grupo Usuarios (haga clic en Usuarios en el panel de navegación izquierdo) una vez que se hayan agregado al grupo de LANDesk Management Suite del entorno de usuarios de Windows NT del servidor central. El grupo Usuarios muestra todos los usuarios que actualmente residen en el grupo de LANDesk Management Suite del servidor central.

Hay dos usuarios predeterminados en el grupo Usuarios. Uno de los usuarios es el administrador predeterminado. Constituye el usuario administrativo que inició una sesión en el servidor al instalar el producto.

El otro usuario predeterminado es el usuario de plantillas predeterminado. Este usuario contiene una plantilla de propiedades del usuario (derechos y ámbito) utilizada para configurar nuevos usuarios cuando se agregan al grupo Management Suite. Es decir, al agregar un usuario a este grupo en el entorno de Windows NT, el usuario hereda los derechos y ámbito definidos actualmente en las propiedades del usuario de plantillas predeterminado. Si se han seleccionado para el usuario de plantillas predeterminado todos los derechos y el ámbito predeterminado de todos los equipos, los nuevos usuarios incluidos en el grupo de LANDesk Management Suite se agregarán al grupo Usuarios con los derechos de todas las herramientas del producto y el acceso a todos los dispositivos.

Para cambiar la configuración de propiedades para el usuario de plantillas predeterminado, selecciónelo y haga clic en Editar. Por ejemplo, si desea agregar un elevado número de usuarios a la vez, pero no desea que tengan acceso a todas las herramientas o los dispositivos, debe cambiar en primer lugar la configuración del usuario de plantillas predeterminado y agregar a continuación los usuarios al grupo de LANDesk Management Suite (consulte los pasos detallados a continuación). El usuario de plantillas predeterminado no se puede eliminar.

Al agregar un usuario al grupo de LANDesk Management Suite en Windows NT, dicho usuario se lee automáticamente en el grupo Usuarios de la ventana Usuarios y hereda los mismos derechos

y ámbito que el usuario de plantillas predeterminado. Se muestra el nombre, ámbito y derechos del usuario. Además, se crean subgrupos para el nuevo usuario, con el ID exclusivo de inicio de sesión del usuario, en los grupos Dispositivos de usuario, Consultas de usuarios, Informes de usuarios y Secuencias de usuario (tenga en cuenta que SÓLO el administrador puede ver los grupos de usuarios).

A la inversa, si elimina un usuario del grupo de LANDesk Management Suite, el usuario ya no aparecerá en el grupo Usuarios. La cuenta de usuario sigue existiendo en el servidor central y se puede volver a agregar al grupo de LANDesk Management Suite en cualquier momento. Asimismo, los subgrupos de usuario de Dispositivos de usuario, Consultas de usuarios, Informes de usuarios y Secuencias de usuario se conservan de modo que pueda restaurar el usuario sin perder los datos y copiar los datos a otros usuarios.

Para actualizar el marco Usuarios en la consola de System Manager, pulse la tecla F5. Para información sobre cómo agregar usuarios o grupos de dominios al grupo LANDesk Management Suite o sobre cómo crear cuentas de usuario nuevas, consulte "Adición de usuarios del producto" en el capítulo Administración basada en funciones del Manual del usuario de System Manager.

Para agregar un usuario o grupo de dominio al grupo de LANDesk Management Suite

1. En el servidor, desplácese hasta **Herramientas administrativas | Administración de equipos | Usuarios locales y grupos | Grupos**.
2. Haga clic con el botón secundario en el **grupo de LANDesk Management Suite** y, a continuación, seleccione **Agregar al grupo**.
3. Haga clic en **Agregar**, y escriba o seleccione un usuario (o usuarios) de la lista.
4. Haga clic en **Agregar** y luego en **Aceptar**.

Nota: Para agregar un usuario al grupo de LANDesk Management Suite, también puede hacer clic con el botón derecho en la cuenta de usuario de la lista **Usuarios**, hacer clic en **Propiedades | Miembro de** y, a continuación, hacer clic en **Agregar** para seleccionar el grupo y agregar el usuario.

Si no existen cuentas de usuario en el servidor, primero debe crearlas.

Para crear una cuenta de usuario nueva

1. En el servidor, desplácese hasta **Herramientas administrativas | Administración de equipos | Usuarios locales y grupos | Usuarios**.
2. Haga clic con el botón derecho en **Usuarios** y, a continuación, haga clic en **Nuevo usuario**.
3. En el cuadro de diálogo **Nuevo usuario**, escriba un nombre y una contraseña.
4. Especifique la configuración de la contraseña.
5. Haga clic en **Crear**. El cuadro de diálogo **Nuevo usuario** permanece abierto para que pueda crear usuarios adicionales.
6. Haga clic en **Cerrar** para salir del cuadro de diálogo.

Agregue el usuario al grupo de LANDesk Management Suite para que aparezca en el grupo Usuarios de la consola.

Configuración de servicios y credenciales

Antes de administrar dispositivos en la red debe proporcionar las credenciales de dispositivo necesarias a System Manager. Utilice la utilidad Configurar servicios en el servidor central (SVCCFG.EXE) para especificar el sistema operativo necesario, Intel* AMT y las credenciales IPMI BMC. También puede especificar configuraciones adicionales, tales como opciones predeterminadas de inventario, opciones de cola de espera de PXE y opciones de la base de datos de LANDesk.

Utilice Configurar servicios para configurar:

- El nombre de la base de datos, el nombre de usuario y la contraseña. (Éstos se definen al momento de la instalación.)
- Las credenciales para las tareas de programación en los dispositivos administrados. (Puede especificar más de un conjunto de credenciales de administrador.)
- Las credenciales para la configuración de IPMI BMC. (Solamente puede especificar un conjunto de credenciales BMC.)
- Las credenciales para la configuración de dispositivos habilitados para AMT. (Solamente puede especificar un conjunto de credenciales de Intel AMT.)
- El intervalo de exploración del software de servidor, el mantenimiento y los días para llevar a cabo exploraciones de inventario y la longitud del historial de inicio de sesión.
- La administración de Id. de dispositivo duplicado.
- La configuración del programador, que incluye los intervalos de tarea programada y de evaluación de consultas.
- La configuración de tareas personalizadas, incluido el período de espera en ejecución remota.

1. En el servidor central, haga clic en **Inicio | Todos los programas | LANDesk |Configuración de servicios de LANDesk** .
2. Haga clic en la ficha **Programador**.
3. Haga clic en el botón **Cambiar inicio de sesión**.
4. Escriba las credenciales que desee que utilice el servicio en los dispositivos administrados, normalmente una cuenta de administrador de dominio.
5. Haga clic en **Agregar.** Agregue credenciales adicionales como sea necesario, si los dispositivos administrados no tienen activadas las mismas cuentas de nombre de usuario administrador.
6. Haga clic en **Aplicar**.
7. Si existen servidores habilitados para IPMI en el entorno, haga clic en la ficha **Contraseña BMC**. Escriba la contraseña en el cuadro de texto Contraseña, vuelva a escribirla en el Confirmar contraseña, y luego haga clic en Aceptar. Todos los servidores IPMI administrados deben compartir el mismo nombre de usuario y la misma contraseña BMC.
8. Si tiene los dispositivos compatibles con Intel AMT instalados, haga clic en la ficha Configuración de Intel AMT. Ingrese el nombre de usuario de Intel AMT actualmente configurado en el cuadro de texto de Usuario y la contraseña actualmente configurada en el cuadro de texto de Contraseña. Vuelva a ingresar la contraseña en el cuadro de texto Confirmar contraseña y haga clic en Aceptar.
9. Configure las otras opciones como lo desee, tales como los intervalos de rastreo de software.
10. Haga clic en **Aceptar** para guardar los cambios.

Haga clic en **Ayuda** en cada una de las fichas Configurar servicios para obtener más información.

Ejecución de la consola

System Manager ofrece una gama completa de herramientas que le permiten ver, configurar, administrar y proteger los dispositivos de la red. La consola es el punto de entrada para el uso de estas herramientas.

El panel superior de la consola muestra el servidor en el que ha iniciado una sesión y el usuario que inició la sesión. La lista Mis dispositivos es la ventana principal de la consola y constituye el punto de inicio para la mayor parte de las funciones. El panel de la izquierda muestra las herramientas disponibles. El panel derecho de la consola muestra los cuadros de diálogo y las pantallas que permiten completar las tareas de administración.

La ventaja de la consola radica en que se pueden llevar a cabo todas las funciones desde una ubicación remota, tal como una estación de trabajo, a fin de evitar la necesidad de desplazarse hasta el servidor o de ir a cada dispositivo administrado individual para realizar el mantenimiento rutinario o solucionar problemas.

La consola se inicia de tres modos:

- En el servidor central, haga clic en Inicio | Todos los programas | LANDesk | System Manager.
- En un explorador de una estación de trabajo remota, escriba la URL http://servidorcentral/LDSM.

Detección de dispositivos

Utilice la ficha **Configuraciones de detección** para crear nuevas configuraciones de detección, editar y eliminar las existentes, y programar una configuración de detección. Cada configuración de detección consiste de un nombre descriptivo, los intervalos IP que rastrea y el tipo de detección.

Una vez que cree una configuración, utilice el cuadro de diálogo **Programar detección** para configurar cuándo se ejecutará.

1. En el panel de exploración izquierdo, haga clic en **Detección de dispositivos**.
2. En la ficha **Configuraciones de detección**, haga clic en el botón **Nueva**.
3. Complete los campos descritos a continuación. Al finalizar, haga clic en **Agregar** y en **Aceptar**.

El texto siguiente describe las partes del cuadro de diálogo **Configuración de detección**.

- **Nombre de configuración:** Escriba un nombre para la configuración. Elija un nombre significativo para la configuración, uno que pueda recordar con facilidad. La configuración puede tener una extensión de hasta 255 caracteres y no debe incluir ninguno de los caracteres siguientes: **"**, **+**, **#**, **&** o **%**. El nombre de la configuración no se mostrará después del uso con algunos de estos caracteres.

- **Rastreo de red estándar:** Busca dispositivos mediante el envío de paquetes ICMP a las direcciones IP que se encuentran en el intervalo especificado. Se trata de la búsqueda más minuciosa, aunque también es la más lenta. De forma predeterminada, esta opción utiliza NetBIOS para recopilar información sobre el dispositivo.

  La opción de rastreo de red contiene la opción **Huella digital de IP** en la cual la detección de dispositivos intenta detectar el tipo de sistema operativo a través de respuestas de paquetes TCP. La opción de huella digital de IP reduce un poco la velocidad de la detección.

  La opción de rastreo de red también contiene la opción **Utilizar SNMP**, donde puede configurar el uso de SNMP en el rastreo. Haga clic en **Configurar** para especificar la información sobre la configuración de SNMP.
- **Detección LANDesk CBA:** Busca el agente de administración estándar (anteriormente conocido como agente de base común, [CBA] en Management Suite) en los dispositivos. El agente de administración estándar permite que el servidor central detecte los clientes de la red y se comunique con ellos. Esta opción detecta los dispositivos que tienen agentes del producto en ellos. Los enrutadores bloquean el tráfico PDS2 y el agente de administración estándar. Para ejecutar una detección CBA estándar a través de varias subredes, debe configurarse el enrutador para permitir la difusión dirigida a través de varias subredes.

  La opción de detección CBA también contiene la opción **Detección LANDesk PDS2**, donde la detección busca LANDesk Ping Discovery Service (PDS2) en los dispositivos. Los productos de LANDesk Software como LANDesk® System Manager, Server Manager y LANDesk Client Manager utilizan el agente PDS2. Seleccione esta opción si existen dispositivos en la red que tengan instalados estos productos. Los equipos Linux no admiten la detección CBA, pero si elije PDS2, pueden detectarse los equipos Linux con un agente instalado.
- **IPMI:** Busca los servidores habilitados para IPMI. IPMI es una especificación desarrollada por Intel,***** H-P,* NEC,* y Dell* con el fin de definir la interfaz de mensaje y sistema del hardware activado para la administración. IPMI contiene funciones de monitoreo y recuperación que le permite acceder a estas funciones sin importar si el dispositivo se encuentra o no activado, o en que estado se encuentre el SO. Recuerde que el Baseboard Management Controller no se encuentra configurado, por lo qeu no responderá a los pings de ASF que el producto utiliza para detectar IPMI. Esto significa que tendrá que detectarlo como un equipo normal. Cuando instala automáticamente el cliente, ServerConfig rastreará el sistema y detectará si se trata de IPMI y configurará el BMC.
- **Chasis del servidor:** busca módulos de administración de chasis de hoja (CMM). Las hojas en el chasis del servidor se detectan como servidores individuales.
- **Intel* AMT:** busca dispositivos compatibles con la tecnología Intel Active Management.
- **IP inicial:** introduzca la dirección IP de inicio para el intervalo de direcciones que desee explorar.
- **IP de finalización:** introduzca la dirección IP de finalización para el intervalo de direcciones que desee explorar.
- **Máscara de subred:** introduzca la máscara de subred para el intervalo de dirección IP que desee explorar.
- **Agregar:** agrega intervalos de dirección IP a la cola de trabajo en la parte inferior del cuadro de diálogo.
- **Borrar:** Elimina los intervalos de las direcciones IP.

- **Editar:** Seleccione un intervalo de direcciones IP en la cola de trabajo y haga clic en **Editar**. El intervalo figura en los cuadros de texto encima de la cola de trabajo, donde puede editar el intervalo y agregar un intervalo nuevo a la cola de trabajo.
- **Quitar:** Elimina el intervalo de direcciones IP seleccionado de la cola de trabajo.
- **Quitar todos:** Elimina todos los intervalos de direcciones IP seleccionados de la cola de trabajo.

Ahora que ha configurado una tarea de detección, puede detectar los dispositivos conectados a la red mediante la programación de la ejecución de la tarea.

Programación y ejecución de tareas de detección

Utilice el botón Programar de la ficha Detectar dispositivos para abrir el cuadro de diálogo Programar detección. Utilice este cuadro de diálogo para programar cuándo ejecutar una detección. Puede programar la detección para que se ejecute inmediatamente, en algún momento posterior, hacer que sea recurrente o bien, ejecutarla una sola vez.

Una vez que programe una tarea de detección, consulte la ficha Tareas de detección para ver el estado de la detección. La programación de una tarea de detección recurrente le ayuda a detectar automáticamente los nuevos dispositivos que se agregan a la red.

El cuadro de diálogo Programar detección tiene las opciones siguientes.

- **Dejar sin Programar:** Deja la tarea sin programar pero la conserva en la lista Configuraciones de detección para su uso en el futuro.
- **Iniciar ahora:** ejecuta la tarea lo más pronto posible. La tarea podría tomar hasta un minuto en iniciarse.
- **Iniciar a la hora programada:** inicia la tarea a la hora especificada. Si hace clic en esta opción, debe definir lo siguiente:
    - **Hora:** hora en que desea iniciar la tarea
    - **Fecha:** fecha en que desea iniciar la tarea Según la configuración regional, el orden de la fecha será día-mes-año o mes-día-año.
    - **Repetir cada:** Si desea repetir la tarea, seleccione si desea repetirla Diariamente, Semanalmente o Mensualmente. Si elige Mensualmente y la fecha no existe en todos los meses (por ejemplo, 31), la tarea se ejecutará en los meses en que exista la fecha.

Para programar una tarea de detección

1. En el panel de exploración izquierdo, haga clic en **Dispositivos detectados**.
2. En la ficha Configuraciones de detección, seleccione la configuración que desee y haga clic en Programar. Configure la programación de detección y haga clic en Guardar.
3. Observe el progreso de la detección en la ficha Tareas de detección. Haga clic en **Actualizar** para actualizar el estado.
4. Al finalizar la detección, haga clic en No administrado para ver todos los dispositivos detectados en el panel superior Dispositivos detectados (el panel no se actualiza automáticamente).

Visualización de dispositivos detectados

Los dispositivos detectados se clasifican según el tipo de dispositivo en el panel Dispositivos detectados. La carpeta Equipos se visualiza de forma predeterminada. Haga clic en las carpetas del panel izquierdo para ver los dispositivos en las distintas categorías. Haga clic en No administrados para ver todos los dispositivos devueltos por la detección.

- Los servidores de chasis de hoja figuran en la carpeta Chasis.
- Los dispositivos empresariales estándar figuran en la carpeta Equipos.
- Los enrutadores y otros dispositivos figuran en la carpeta Infraestructura.
- Los dispositivos habilitados para Intel AMT figuran en la carpeta Intel AMT.
- Los servidores habilitados para IPMI figuran en la carpeta IPMI.
- Los dispositivos no clasificados figuran en la carpeta Otros.
- Las impresoras figuran en la carpeta Impresoras.

Nota: algunos servidores Linux figuran con el nombre genérico "Unix" como el nombre del sistema operativo (o algunas veces figuran como Otros). Cuando se implementa el agente de !CompanyName! estándar, estos servidores actualizan la entrada del nombre del SO en la lista Mis dispositivos y muestran un inventario completo. Para ver servidores detectados

1. En la página Detección de dispositivos del panel izquierdo, haga clic en Equipos o en otro tipo de dispositivo que desee ver. Los resultados se muestran en el panel derecho.
2. Para filtrar los resultados, haga clic en el icono Filtro, escriba una porción de lo que busca y haga clic en Buscar.

Asignación de nombres

Al realizar una detección de rastreo de red, algunos servidores devuelven un nombre de nodo (o de host) en blanco. Esto sucede con frecuencia con los servidores que ejecutan Linux. Debe asignar un nombre al dispositivo antes de utilizar Administrar para moverlo a la lista Mis dispositivos.

1. En la página Detectación de dispositivos, haga clic en el dispositivo con el nombre en blanco. (Debe hacer clic en el área en blanco en la columna con el nombre del nodo.)
2. Haga clic en Asignar nombre en la barra de herramientas.
3. Escriba el nombre y haga clic en Aceptar.

Al instalar un agente de producto en un dispositivo, el agente rastrea de forma automática el nombre del host y actualiza la base de datos central con la información correcta.

Traslado de dispositivos a la lista Mis dispositivos

Una vez que se han detectado, debe especificar los dispositivos de destino que desee administrar y moverlos a la lista Mis dispositivos, de forma manual. Al mover un dispositivo no se instala ningún software en él. Solamente hace que el dispositivo esté disponible para la consulta, agrupación y clasificación en la lista Mis dispositivos. Los dispositivos específicos se definen como "destinos" de una acción particular, lo cual es un modelo similar a la "cesta de compras" de muchas aplicaciones de Internet.

1. En la vista Dispositivos detectados, haga clic en el dispositivo que desee mover a la lista Mis dispositivos. Para seleccionar varios dispositivos, pulse **MAYÚSCULAS+clic** o **CTRL+clic**.
2. Haga clic en el botón **Destino**. Si no esta visible, haga clic en << en la barra de herramientas. El botón se encuentra en el extremo derecho. O bien, haga clic con el botón secundario en los servidores seleccionados y haga clic en **Destino**.
3. En el panel inferior, haga clic en la ficha Administrar.
4. Seleccione los dispositivos para moverlos a la base de datos de administración o para mover los dispositivos de destino.
5. Haga clic en **Mover**.

Al hacer clic en Mover, se mueven los dispositivos a la lista Mis dispositivos y se coloca la información de los mismos en la base de datos. Una vez que la información se encuentre en la base de datos, podrá ejecutar consultas e informes (por ejemplo, según el nombre del dispositivo, la dirección IP o el SO).

Agrupación de dispositivos para las distintas acciones

Es probable que desee organizar los dispositivos en grupos, según la ubicación geográfica o la función, para realizar acciones en ellos de forma más rápida. Por ejemplo, podría consultar las velocidades de los procesadores de todos los dispositivos en una ubicación determinada.

1. En la lista Mis dispositivos, haga clic en Grupos privados o en Grupos públicos, y haga clic en **Agregar grupo**.
2. Escriba un nombre para el grupo en el cuadro Nombre de grupo.
3. Haga clic en el tipo de grupo que desee crear.
    - **Estático:** dispositivos que se han agregado al grupo. Permanecen en el grupo hasta que se eliminan o hasta que ya no los administra.
    - **Dinámico:** dispositivos que cumplen con uno o más criterios definidos en una consulta. Por ejemplo, un grupo podría contener todos los servidores que se encuentran en un estado de advertencia. Permanecen en el grupo siempre que cumplan el criterio definido para el grupo. Los dispositivos se agregan automáticamente a los grupos dinámicos si satisfacen el criterio de consulta de grupo.
4. Una vez que haya finalizado, haga clic en **Aceptar**.
5. Para agregar dispositivos al grupo estático, haga clic en los dispositivos en el panel derecho de la lista Mis dispositivos, haga clic en Mover/Copiar, seleccione el grupo y haga clic en Aceptar.

Configuración de dispositivos para la administración

La detección de dispositivos por sí mismas no los coloca bajo la sombrilla de administración. Para administrar los dispositivos de forma total con la consola y recibir alertas de estado, debe instalar los agentes de administración en ellos. Puede elegir la instalación de la configuración de agente predeterminada (la cual instala todos los agentes de administración) o personalizar su propia configuración de agente para instalarla en los dispositivos. La configuración de agente debe incluir el agente monitor para recibir alertas de integración.

Para instalar los agentes de administración se utiliza uno de los modos siguientes:

- Defina los dispositivos de destino en la lista Mis dispositivos y programe una tarea de configuración para instalar los agentes de forma remota en los dispositivos. (los pasos se encuentran a continuación)
- Asigne una unidad al recurso compartido LDlogon del servidor central (//servidorcentral/ldlogon) y ejecute SERVERCONFIG.EXE. (los pasos se encuentran en la sección "Instalación de agentes a petición" del capítulo Instalación y configuración de un agente de dispositivo del Manual del usuario de System Manager)
- Cree un paquete de instalación de dispositivo de extracción automática. Ejecute el paquete de forma local en el dispositivo para instalar los agentes. Esto debe realizarse tras iniciar una sesión con privilegios administrativos. (los pasos se encuentran en la sección " Instalación de agentes con un paquete de instalación." del capítulo Instalación y configuración de un agente de dispositivo del Manual del usuario de System Manager

Para instalar el agente automáticamente:

1. Defina los dispositivos de destino en la lista Mis dispositivos (tal como se explica anteriormente en Traslado de dispositivos a la lista Mis dispositivos).
2. En el panel de navegación izquierdo, haga clic en Configuración del Agente, haga clic con el botón secundario en la configuración que desee instalar automáticamente y haga clic en Programar tarea.
3. En el panel izquierdo, haga clic en Dispositivos de destino y haga clic en el botón Agregar la Lista de destino.
4. Haga clic en Programar tarea y luego en Iniciar ahora para iniciar la tarea inmediatamente o en Iniciar más tarde y especifique la fecha y hora de inicio y a continuación, haga clic en Guardar.

El estado de la tarea se muestra en la ficha Tareas de configuración.

Instalación de agentes de servidores Linux

Puede implementar e instalar agentes Linux y RPM en servidores Linux de forma remota. El servidor Linux debe configurarse de forma debida para que esto funcione. La instrucciones para la configuración debida de un servidor Linux se encuentran en la sección "Instalación de agentes de servidor" del capítulo Instalación y configuración de un agente de dispositivo del Manual del usuario de *System Manager.*

Definición de alertas

Cuando se presenta un problema u otro evento en un dispositivo (por ejemplo, hay poco espacio de disco en el dispositivo), System Manager puede enviar una alerta. Para personalizar las alertas, elija el nivel de gravedad o el umbral que activará la alerta. Las alertas se envían a la consola y se pueden configurar para que realicen acciones específicas y para diversos eventos o problemas posibles. El producto incluye un reglamento de alertas predeterminado, el cual se instala en los dispositivos administrados cuando se instala el componente de supervisión. Este reglamento de alertas proporciona información del estado de la integridad a la consola. Este reglamento predeterminado incluye alertas como:

- Adición o eliminación de disco
- Espacio de disco

- Uso de la memoria
- Temperatura, ventiladores y voltajes
- Supervisión del desempeño
- Eventos IPMI (en hardware correspondiente)

Para obtener más información sobre las alertas, consulte el capítulo Configuración de alertas del Manual del usuario de System Manager.

Definición de alertas

Cuando se presenta un problema u otro evento en un dispositivo (por ejemplo, hay poco espacio de disco en el dispositivo), System Manager puede enviar una alerta. Para personalizar las alertas, elija el nivel de gravedad o el umbral que activará la alerta. Las alertas se envían a la consola y se pueden configurar para que realicen acciones específicas y para diversos eventos o problemas posibles. El producto incluye un reglamento de alertas predeterminado, el cual se instala en los dispositivos administrados cuando se instala el componente de supervisión. Este reglamento de alertas proporciona información del estado de la integridad a la consola. Este reglamento predeterminado incluye alertas como:

- Adición o eliminación de disco
- Espacio de disco
- Uso de la memoria
- Temperatura, ventiladores y voltajes
- Supervisión del desempeño

Para obtener más información sobre las alertas, consulte el capítulo Configuración de alertas del Manual del usuario de System Manager.

¿Cuál es el siguiente paso?

Ahora Server Manager se encuentra en marcha. Solamente ha utilizado una fracción de las funciones disponibles en Server Manager y sólo una porción de las funciones utilizadas (como la detección de dispositivos y la configuración de agentes). Los manuales proporcionados (el *Manual de instalación e implementación* y el *Manual del usuario*) contienen información más detallada sobre todas las funciones del producto. Algunas de estas funciones son:

Actualizaciones de software: establezca seguridad continua a nivel de revisión en los dispositivos administrados en toda la red. Puede automatizar los repetitivos procesos de mantenimiento de la información de vulnerabilidad actual, de evaluación de las vulnerabilidades de los distintos sistemas operativos que se ejecutan en los dispositivos administrados, de descarga de archivos de revisión ejecutables adecuados, de reparación de vulnerabilidades mediante la implementación e instalación de las revisiones necesarias en los dispositivos afectados y de verificación de la instalación satisfactoria de las revisiones.

Alertas: asegúrese de que reciba alertas si cualquiera de los dispositivos alcanza un umbral particular. La función de alertas está relacionada con la función de supervisión y puede notificarles de diversos modos. Por ejemplo, si necesita saber en qué momento el almacenamiento de los dispositivos ha llegado a un 95% de su capacidad, puede elegir que se le envíe una alerta (el agente envía mensajes de correo electrónico o de localizador, reinicia o apaga el dispositivo o agrega información al registro de alertas).

Consultas: administre la red mediante la búsqueda y organización de dispositivos en la base de datos central en base a un criterio de sistema o usuario específico. Puede consultar la lista de dispositivos administrados en busca de los que cumplan con un criterio que especifique (por ejemplo, todos los que se encuentran en la oficina matriz o todos los que tienen 256K de RAM) y agruparlos para realizar acciones. Estos grupos pueden ser estáticos (los miembros del grupo solamente se pueden cambiar manualmente) o dinámicos (los miembros pueden cambiar cuando los dispositivos satisfagan o no un criterio especificado).

Distribución de software: cree tareas o distribuya paquetes de software (uno o más archivos MSI, un ejecutable, un archivo de proceso por lotes, archivos RPM (Linux) o un paquete creado con el generador de paquetes de LANDesk) en los dispositivos de destino.

Supervisión: supervise el estado de integridad de un dispositivo mediante uno de los tipos de supervisión (supervisión ASIC directa, IPMI en banda, IPMI fuera de banda, CIM, etc.). La supervisión permite llevar un seguimiento de diversos datos de los dispositivos, tales como niveles de uso, eventos, procesos y servicios de sistema operativo, desempeño histórico y sensores de hardware (ventiladores, voltajes, temperaturas, etc.). Las alertas constituyen una función relacionada que utiliza el agente de supervisión para iniciar acciones de alerta.

Elaboración de informes: genere una variedad de informes especializados que ofrecen información crítica sobre los dispositivos administrados en la red. Server Manager utiliza una utilidad de rastreo de inventario para agregar dispositivos (y datos de hardware y software recopilados en los dispositivos) a la base de datos central. Esta herramienta permite ver e imprimir los datos de inventario en una vista de inventario del dispositivo, al igual que definir consultas y agrupar dispositivos. La herramienta de informe aprovecha los datos de inventario rastreados mediante la recopilación y organización de dichos datos en formatos de informe útiles, lo cual ayuda al recopilar y formatear datos para informes reglamentarios.

Detecciones de dispositivos no administrados: busque dispositivos que no estén siendo administrados por la consola. La detección es el primer paso para agregar nuevos equipos a la administración con rapidez. Puede configurar una tarea de detección que rastree en busca de equipos nuevos cada mes.

Monitoreo de licencias de software: lleve un seguimiento del cumplimiento de licencias. El agente de supervisión de licencias de software recopila datos (como los minutos totales de uso, la cantidad de ejecuciones y la fecha de la última ejecución de todas las aplicaciones instaladas en un dispositivo) y almacena estos datos en el registro del dispositivo. Puede utilizar los datos para supervisar el uso de los productos y las tendencias de denegación. El agente supervisa de forma pasiva el uso del producto en los dispositivos, utilizando un ancho de banda de red mínimo. El agente también supervisa el uso de los dispositivos móviles desconectados de la red.

Despliegue de SO: implemente imágenes de sistema operativo en los dispositivos de la red mediante la herramienta de implementación basada en PXE. Permite crear una imagen de los dispositivos con discos duros en blanco o con sistemas operativos inutilizables. Los representantes de PXE ligeros eliminan la necesidad de contar con un servidor PXE dedicado en cada subred. El despliegue de SO facilita la incorporación de nuevos dispositivos sin que sea necesaria la actuación de ningún otro usuario final o tecnología de la información una vez se haya iniciado el proceso.

Fase 1: Diseño de dominios de administración

En la fase 1, se recopila información sobre la infraestructura de red y se toman decisiones que contribuyen a personalizar el dominio de administración.

En esta fase se abordan los temas siguientes:

- Recopilación de información de la red
- Selección del servidor central
- Base de datos central
- Planificación del modelo organizativo y de seguridad
- Requisitos del sistema

Recopilación de información de la red

Identifique y recopile información importante sobre la red en relación con System Manager. Más concretamente, deberá:

- Determine las configuraciones de los dispositivos
- Seleccionar el servidor central

Selección del servidor central

El servidor central es el centro de un dominio de administración. Todos los servicios y archivos clave se incluyen en el servidor central. Desde el punto de vista físico, puede ser un servidor nuevo o uno reacondicionado.

Puede ejecutar la consola del administrador a partir de un explorador en una estación de trabajo remota, donde realiza las actividades de administración como la gestión de alertas, las consultas a la base de datos o la creación de secuencias de comandos personalizadas.

Asegúrese de que los servidores seleccionados para el servidor central cumplan los requisitos de sistema. Consulte la sección Requisitos del sistema más adelante es esta fase.

Planificación de la ubicación de los archivos de programa

Durante la instalación, se puede especificar dónde se desean instalar los archivos de programa. Se recomienda utilizar los directorios de destino predeterminados, siempre que no haya ninguna razón de peso para modificarlos. Si elige modificar el directorio de destino, la ruta del mismo no puede contener caracteres de doble byte.

El directorio de destino predeterminado para los archivos del servidor central es:

```
C:\Archivos de programa\LANDesk\ManagementSuite
```

Base de datos central

System Manager instala una base de datos MSDE en el servidor central. Cada base de datos MSDE tiene un tamaño límite de 2 GB para la base de datos. El número de servidores que admite esta base de datos depende del tamaño del archivo de rastreo de inventario de la red.

Es posible que detecte problemas de rendimiento con MSDE cuando la base de datos tenga más de cinco tareas que hacer simultáneamente. Por ejemplo, cuando cinco System Manageradministradores tienenacceso simultáneo a la base de datos.

Seguridad de cliente y servidor central

Este producto utiliza un sistema de autenticación basado en certificado. Durante la instalación del servidor central, el programa de configuración crea un certificado para el mismo. Los clientes buscan dicho certificado al comunicarse con el servidor central y no se pueden comunicar con ningún servidor central para el que no tengan un certificado.

Los dispositivos solamente se comunican con servidores centrales para los cuales tienen un archivo de certificado de confianza coincidente. Cada servidor central tiene su propio certificado y claves privadas, y de forma predeterminada, los agentes de cliente que se implementen desde ellos sólo se comunicarán con aquél desde el que se implementó el software.

Planificación de un ámbito

La administración basada en funciones es una potente función de la administración de seguridad. Para obtener acceso a las herramientas de administración basada en funciones de la consola, haga clic en Usuarios en el panel izquierdo. Debe haber iniciado la sesión con derechos administrativos.

La administración basada en funciones proporciona una capacidad de administración de dispositivos avanzada, ya que permite agregar usuarios al sistema y asignarles derechos y ámbitos. Los derechos determinan las herramientas y funciones que un usuario puede ver y utilizar (consulte la sección "Descripción de los derechos", en el Manual del usuario de Server Manager). El ámbito determina la gama de dispositivos que un usuario puede ver y administrar (consulte la sección "Creación de ámbitos", en el Manual del usuario de Server Manager).

Puede crear funciones basándose en las responsabilidades de los usuarios, las tareas de administración que desea que realicen y los dispositivos que desea que puedan ver, acceder y administrar. El acceso a los dispositivos se puede restringir a una ubicación geográfica, como por ejemplo, un país, una región, un estado, una ciudad, o a un grupo o tipo de servidor.

Para implementar y forzar este tipo de administración basada en funciones en toda la red, tan solo tiene que configurar los usuarios actuales o bien, crear y agregar usuarios nuevos como usuarios del producto y después asignarles los derechos necesarios (a las funciones del producto) y el ámbito (a los dispositivos administrados).

El servidor central utiliza ámbitos para limitar los dispositivos que pueden ver los usuarios de la consola. Se pueden asignar varios ámbitos a un usuario y un ámbito puede ser utilizado por varios usuarios. Los ámbitos se pueden basar en uno de los métodos siguientes:

- (Predeterminado) **Ámbito de todos los equipos:** Los usuarios pueden ver todos los dispositivos.
- **Basado en la consulta:** Los usuarios pueden ver los dispositivos que se adaptan a los criterios seleccionados de una consulta específica que les ha sido asignada por el administrador.
- **Basado en un grupo:** Los usuarios solamente pueden ver los dispositivos que satisfacen el criterio del grupo.

Si desea obtener más información sobre los ámbitos, consulte el Server Manager*Manual del usuario*.

Requisitos del sistema

Asegúrese de que se cumplen los siguientes requisitos del sistema antes de la instalación. El verificador de requisitos previos lo lleva a cabo.

Servidores de base de datos y centrales

Asegúrese de que todos los servidores de base de datos y centrales cumplen los requisitos explicados en la introducción.

- Windows 2000 Server o Advanced Server con SP 4, Windows Server 2003 Standard o Enterprise Edition x86 SP1, o Windows 2003 R2
- Microsoft Data Access Components (MDAC) 2.8 o posterior
- Microsoft .NET Framework 1.1
- Internet Information Services (IIS)
- Compatibilidad de IIS con secuencias ASP.NET v1.1
- Internet Explorer 6.0 SP1 o superior
- Microsoft NT File System (NTFS)
- El servidor Windows que utiliza como el servidor central debe estar instalado como un servidor independiente, no como un controlador de dominio principal (PDC), un controlador de dominio de respaldo (BDC) o un controlador de Active Directory.
- SNMP debe estar instalado y deben iniciarse los servicios de SNMP y de captura SNMP
- 200 MB de espacio disponible en la unidad del sistema y 900 MB de espacio disponible en al menos una unidad
- Privilegios de administrador
- El cliente de LANDesk tiene la versión correcta o no se ha instalado

Requisitos del servidor central
El archivo de paginación de Windows debe tener al menos 12 + *N* (donde *N* representa el número de megabytes de RAM del servidor central). Caso contrario, las aplicaciones del producto pueden provocar errores de memoria.

Se recomienda 1 gigabyte de memoria en el equipo central si desea instalar ambos productos Management Suite y Server Manager en el mismo servidor central.

Todos los servicios del producto deben estar alojados en un servidor

Para los dominios de administración más pequeño, se puede instalar el servidor central y la base de datos central en un servidor. Para estas redes, se recomienda utilizar la base de datos predeterminada Microsoft MSDE, que resulta mucho más fácil de mantener. Es la única opción de base de datos para System Manager.

Limitaciones

El servidor debe cumplir al menos estos requisitos del sistema antes de instalar el servidor central y la base de datos:

- Procesador Pentium 4
- 4 GB de espacio libre en disco en unidades de 10.000 RPM o más
- 768 MB de RAM como mínimo

Equipos de servidor administrados

Este producto admite los siguientes sistemas operativos de servidor (no todos los sistemas operativos se admiten en la misma medida):

- Microsoft Windows 2000 Server (con SP4)
- Microsoft Windows 2000 Advanced Server (con SP4)
- Microsoft Windows 2000 Professional (con SP4)
- Microsoft Windows 2003 Server R2
- Microsoft Windows 2003 Server Standard Edition x86 (con SP1)
- Microsoft Windows 2003 Server Standard x64 Edition (con SP1)
- Microsoft Windows 2003 Server Enterprise Edition x86 (con SP1)
- Microsoft Windows 2003 Server Enterprise x64 Edition (con SP1)
- Microsoft Windows XP Professional (con SP2)
- Microsoft Windows XP Professional x64 (con SP2)
- Windows Small Business Server 2000 (con SP4)
- Windows Small Business Server 2003 (con 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

Equipos de servidor administrados por Linux

La lista siguiente contiene los requisitos previos de servidores de seguridad y RPM para la habilitación de dispositivos Linux para la administración.

Servidor de seguridad

A fin de instalar el agente de administración al principio y configurar un servidor Linux para la comunicación con el servidor central (mediante el método de "instalación automática"), debe permitirse que pasen las conexiones SSH a través del servidor de seguridad local del servidor Linux:

22 - sólo TCP

A fin de que los agentes puedan comunicarse con los servidores centrales (para los rastreos de inventario, la distribución de software, las actualizaciones de vulnerabilidades, etc.), el servidor de seguridad local del servidor de Linux debe configurarse de modo que permita la comunicación en los puertos siguientes:

9593 - sólo TCP

9594 - sólo TCP

9595 - ambos TCP y UDP

A fin de establecer comunicación con el agente de administración, el servidor de seguridad local del servidor Linux debe configurarse de modo que permita la comunicación en los puertos siguientes:

6780 - sólo TCP

RPM requeridos (versión # o posterior)

Es recomendable que almacene todos los RPM del producto en el directorio ...\ManagementSuite\ldlogon\RPMS. Puede ir hasta el directorio a través de http://nombre del servidor central/RPMS.

REDHAT_ENTERPRISE

python

Versión de RPM:2.2.3-5 (RH3)

2.3.4-14 (RH4)

Versión binaria:2.2.3

pygtk2 Versión de RPM:1.99.16-8 (RH3)

2.4.0-1 (RH4)

Versión binaria:

sudo

Versión de RPM:1.6.7p5-1

Versión binaria:1.6.7.p5

bash Versión de RPM:2.05b-29 (RH3)

3.0-19.2 (RH4)

Versión binaria:revisión 2.05b.0(1)

xinetd Versión de RPM:2.3.12-2.3E (RH3)

2.3.13-4 (RH4)

Versión binaria:2.3.12

mozilla Versión de RPM: 1.7.3-18.EL4 (RH4)

Versión binaria:1.5

openssl Versión de RPM:0.9.7a-22.1 (RH3)

0.9.7a-43.1 (RH4)

Versión binaria:0.9.7a

sysstat Versión de RPM:4.0.7-4

Versión binaria:4.0.7

lm_sensors

Versión de RPM: 2.6 (esta versión puede resultar insuficiente para mostrar los sensores en los equipos ASIC más nuevos. Consulte la documentación de lm_sensors o el sitio Web (http://www2.lm-sensors.nu/~lm78) para obtener información más detallada.

SUSE LINUX

(SUSE 64)

bash

Versión de RPM: 2.05b-305.6

mozilla

Versión de RPM: 1.6-74.14

net-snmp

Versión de RPM: 5.1-80.9

openssl

Versión de RPM: 0.9.7d-15.13

python-gtk

Versión de RPM: 2.0.0-215.1 [nota: se cambió el nombre del paquete]

python

Versión de RPM: 2.3.3-88.1

sudo

Versión de RPM: 1.6.7p5-117.1

sysstat

Versión de RPM: 5.0.1-35.1

xinetd

Versión de RPM: 2.3.13-39.3

lm_sensors

Versión de RPM: NA (nota: se ha incorporado en el kernel para la versión 2.6)

Uso de puertos del producto

Introducción

Al utilizar este producto en un entorno que incluya servidores de seguridad (o enrutadores que filtran el tráfico), se necesita ajustar la configuración del servidor de seguridad o enrutador para que funcione el producto. Esta sección describe los puertos utilizados por los diversos componentes del producto. La información se enfoca en lo que se necesita saber para configurar los enrutadores y los servidores de seguridad, excluyendo los puertos que solamente se usan localmente (dentro de las subredes individuales).

Información básica sobre las reglas de servidor de seguridad

Esta información se aplica a la configuración de reglas de servidor de seguridad. Si no está familiarizado con este tema, esta sección brinda información básica sobre los conceptos más importantes.

Reglas del servidor de seguridad

La "apertura de un puerto" no es un término preciso. No se puede ir al servidor central y "abrir el puerto x". La apertura de un puerto es una abreviación para la configuración de una regla del servidor de seguridad. Las reglas de servidor de seguridad describen el tráfico que se permite y que no se permite a través del servidor de seguridad. Las reglas del servidor de seguridad no filtran el tráfico solamente en base al número de puerto. Las reglas pueden basarse en los protocolos, los números de puerto de origen y destino, la dirección (entrante o saliente), las direcciones IP de origen y destino, y otros factores.

Una regla común de servidor de seguridad podría ser: "permitir tráfico entrante en el puerto TCP 9535". A fin de utilizar este producto, esta regla es necesaria para admitir el control remoto. La regla está basada en tres elementos:

1. El protocolo (TCP o UDP)
2. El número de puerto
3. La dirección (entrante o saliente)

Los tres elementos son necesarios para la configuración de reglas de servidor de seguridad.

Puertos de origen y destino, puertos dinámicos

Siempre se involucran dos puertos en la comunicación TCP o UDP. Cualquier paquete TCP o UDP proviene de un puerto de origen y se dirige a uno de destino. Las reglas de servidor de seguridad se pueden basar en el puerto de origen, en el puerto de destino o en ambos. Los puertos que se mencionan en documentos como éste, son siempre puertos de destino.

Los puertos más conocidos, como 5007 (utilizado por el servicio de inventario), se refieren solamente a un extremo de la comunicación. El otro extremo de la comunicación utiliza un puerto

dinámico. Los puertos dinámicos son asignados automáticamente por el sistema operativo en el intervalo 1024-5000.

Servidores de seguridad y tráfico UDP

Para permitir el tráfico TCP a través de un servidor de seguridad, es suficiente una sola regla, por ejemplo, para permitir todas las conexiones entrantes en el puerto 5007. Una vez que se establece la conexión TCP, los datos pueden viajar en ambas direcciones a través de la conexión.

El tráfico UDP es distinto debido a que no utiliza conexiones. Por ejemplo, el servidor central realiza de forma predeterminada un "ping" de los dispositivos en el puerto UDP 38293 antes de iniciar una tarea. La regla de servidor de seguridad que permite paquetes UDP salientes en el puerto 38293, también permite paquetes del servidor central en un dispositivo externo al servidor de seguridad, pero no permite los paquetes de respuesta del dispositivo.

Una regla que permite tanto los paquetes entrantes como salientes en el puerto 38293 no funcionará debido a que solamente un extremo de la comunicación está escuchando en el puerto conocido. El otro extremo está utilizando un puerto dinámico. Debido a que los paquetes salientes del servidor central provienen de un puerto dinámico y se dirigen al puerto 38293, los paquetes de respuesta del dispositivo provienen del puerto 38293 y se dirigen al mismo puerto dinámico, y no al puerto 38293. Para permitir la comunicación en dos direcciones, se necesita una regla que permita paquetes UDP con el puerto 38293 como origen o destino. Dicha regla es por lo general aceptable en la Intranet, pero no en un servidor de seguridad externo (debido a que permitiría paquetes entrantes de todos los puertos UDP).

Por esta razón, el tráfico UDP por lo general no se considera como "favorable para los servidores de seguridad". En el ejemplo utilizado, existe una alternativa para el puerto UDP 38293: el puerto TCP 9595. Al administrar dispositivos a través de un servidor de seguridad, podría ser recomendable que configure el producto para que utilice el puerto TCP.

Puertos utilizados

Puerto	Dirección	Protocolo	Servicio
31770	de consola a dispositivo, de dispositivo a servidor central	TCP	comunicación entre la consola y el dispositivo
6787	de consola a dispositivo	TCP	comunicación entre la consola y el dispositivo
9595	de consola a dispositivo	UDP	detección

Puerto	Dirección	Protocolo	Servicio
9595	de consola a dispositivo	TCP	configuración de agentes
623	de consola a dispositivo	UDP	ASF, detección IPMI
9535	de consola a dispositivo	TCP	control remoto

Este producto necesita detectar los nodos con el agente de administración instalado antes de que pueda administrarlos. El puerto UDP 9595 se utiliza para la detección. Puede agregar de forma manual dispositivos individuales a la consola. Sin embargo, esto aún requiere que el dispositivo responda a un "ping" en el puerto UDP 9595. La comunicación entre la consola y el dispositivo utiliza los puertos TCP 31770 y 6787. El tráfico en este último puerto se basa en HTTP. El puerto UDP 623 se utiliza para la detección ASF (foro estándar de alertas). Además, este producto utiliza el puerto TCP 9535 para el control remoto. La detección IPMI está vinculada a la detección ASF y utiliza el mismo puerto (udp/623).

Fase 2: Instalación del servidor central

Esta fase se enfoca en la instalación del servidor central.

En esta fase se abordan los temas siguientes:

- Instalación del servidor central
- Activación del servidor central
- Implementación en dispositivos Windows
- Implementación en dispositivos Linux

La instalación de los componentes de esta fase requiere entre 30 y 60 minutos.

Instalación del servidor central

Para instalar el servidor central

Antes de iniciar la instalación, es recomendable que cierre las demás aplicaciones y guarde los archivos abiertos. En el servidor Windows 2000/2003 seleccionado para que sea el servidor central:

1. Inserte el medio del producto en la unidad o ejecute AUTORUN.EXE a partir de la imagen de instalación. Se abre una pantalla de ejecución automática.
2. Haga clic en **Verificar requisitos previos e instalar**.
3. El verificador de requisitos del sistema se ejecuta para verificar que el sistema cumpla con los requisitos mínimos. Asegúrese de que se cumplen todos los requisitos. Si no se cumplen, haga clic en **No aceptable** en el vínculo del requisito no aceptable para los vínculos o información relacionada con la instalación del requerimiento no aceptable.
4. Haga clic en **Instalar ahora** para ejecutar el programa de instalación.
5. Seleccione el idioma que desee instalar. Haga clic en **Aceptar**.
6. Se abre una pantalla de bienvenida. Haga clic en **Siguiente** para continuar.
7. En la pantalla Contrato de licencia, si está de acuerdo, haga clic en **Acepto los términos del contrato de licencia** para continuar. Haga clic en **Siguiente**.
8. Acepte la carpeta de destino predeterminada o especifique una personalizada y haga clic en **Siguiente**. La ruta de acceso a la carpeta de destino no puede contener caracteres de doble byte. Si cambia esta carpeta, recuerde sustituir la ruta con las rutas que aparecen en la documentación del producto.
9. Ingrese una contraseña para la base de datos de MSDE. Memorice o anote esta contraseña, Haga clic en **Siguiente** para continuar.
10. Introduzca los nombres de una organización y de un certificado para el certificado de seguridad del servidor central. Esta información sirve para asignar un nombre y describir el certificado mismo. Haga clic en **Siguiente**.
11. En la página Listo para instalar, haga clic en **Instalar**. El producto iniciará la instalación.
12. Cuando termina la Instalación, aparece el diálogo **El Asistente de la instalación ha finalizado**.
13. Haga clic en **Finalizar**.

14. El programa de Instalación le indicará que vuelva a iniciar el servidor. Debe hacer clic en **Sí** para finalizar la instalación. Cuando se reinicia el servidor, descubrirá después de iniciar una sesión que la Instalación se ejecutará durante unos cuantos minutos más mientras finaliza el proceso de instalación. El programa de configuración no solicita ningún otro dato durante el primer reinicio.

Durante la instalación de una base de datos central MSDE en un Windows 2003 Server, es posible que Windows interrumpa la instalación y pregunte si está bien abrir SETUP.EXE. Si se le presenta este aviso, haga clic en Abrir o el producto no se instalará correctamente.
Si desea instalar las extensiones de plataforma Intel para el software de LANDesk, siga al asistente que se abre después de la instalación de Server Manager.

Activación del servidor central

Debe activar el servidor central antes de utilizar los productos de System Manager en dicho servidor. Puede activar el servidor central ya sea automáticamente a través de Internet o manualmente a través de correo electrónico. Si se cambia considerablemente la configuración de hardware de un servidor central, es probable que sea necesaria la reactivación.

De forma periódica, el componente de activación del servidor central genera datos pertinentes a:

- La cantidad precisa de dispositivos que se utilizan
- La configuración de hardware codificada no personal
- Los programas de LANDesk Software específicos que se utilizan (de forma colectiva, los "datos de cuenta de servidor").

La activación no recopila ni genera ningún otro tipo de datos. El código de clave de hardware se genera en el servidor central haciendo uso de factores de configuración de hardware no personales, tales como el tamaño de la unidad de disco duro, la velocidad de procesamiento del equipo, etc. El código de clave de hardware se envía a LANDesk en formato codificado y la clave privada de la codificación reside solamente en el servidor central. LANDesk Software utiliza el código de clave de hardware para crear una porción del certificado autorizado.

Tras la instalación de un servidor central, la utilidad Activación del servidor central (**Inicio | Todos los programas | LANDesk | Activación del servidor central**) se ejecuta durante el primer inicio para activar el servidor central con el nombre de usuario y la contraseña de usuario proporcionados por el OEM.

Puede realizar la actualización de System Manager a Server Manager o Management Suite mediante la utilidad de activación del servidor central. Consulte Uso de System Manager con Management Suite o Server Manager.

Una vez activado el servidor central, puede utilizar el cuadro de diálogo **Preferencias | Licencia** de la consola para ver la información de licencia del producto. Con la licencia OEM de Intel tiene autorización para ejecutar un agente del producto en todos los servidores y la placas base de marca Intel.

Sobre la utilidad Activación del servidor central

Utilice la utilidad de Activación del servidor central para activar un nuevo servidor por primera vez. Para iniciar la utilidad, haga clic en **Inicio | Todos los programas | LANDesk | Activación del servidor central**. Si el servidor central no tiene una conexión a Internet, consulte "Activación de un servidor central o verificación de los datos de cuenta de servidores de forma manual", más adelante en esta sección.

Cada servidor central debe tener un certificado autorizado único.

De forma periódica, el servidor central verifica las licencias mediante la generación del archivo "\Archivos de programa\LANDesk\Authorization Files\LANDesk.usage". Este archivo se envía de forma periódica al servidor de licencias de LANDesk Software. Este archivo está en formato XML y se firma y codifica de forma digital. Si se cambia este archivo de forma manual, se anula su contenido y el informe de uso siguiente que se envía al servidor de licencias de LANDesk Software.

El servidor central se comunica con el servidor de licencias de LANDesk Software a través de HTTP. Si utiliza un servidor proxy, haga clic en la ficha **Proxy** y escriba la información de proxy. Si el servidor central tiene conexión a Internet, la comunicación con el servidor de licencias es automática y no requiere su intervención.

Tenga en cuenta que la utilidad Activación del servidor central no inicia una conexión a Internet de acceso telefónico de forma automática, pero si usted la inicia manualmente y ejecuta la utilidad de activación, ésta puede utilizar la conexión para enviar los datos de uso.

Si el servidor central no tiene conexión a Internet, verifique y envíe la cuenta de servidores manualmente, tal como se describe más adelante en esta sección.

Activación del servidor central

Para activar un servidor

1. Haga clic en **Inicio | Todos los programas | LANDesk | Activación del servidor central**.
2. Haga clic en **Activar el servidor central** haciendo uso de su nombre de contacto y contraseña de LANDesk.

El nombre y la contraseña se completan de forma automática.

Activación de un servidor central o verificación de los datos de cuenta de servidores de forma manual

Si el servidor central no tiene conexión a Internet, la utilidad Activación del servidor central no podrá enviar los datos de cuenta de servidores. Se muestra un mensaje, el cual le indica que envíe los datos de activación y de verificación de cuenta de servidores de forma manual a través de correo electrónico. La activación por correo electrónico es un proceso sencillo y rápido. Si aparece el mensaje de activación manual en el servidor central o si utiliza la utilidad Activación del servidor central y aparece el mensaje, siga estas pasos.

Para activar un servidor central o verificar los datos de cuenta de servidores de forma manual

1. Cuando el servidor central le indica que verifique los datos de cuenta de servidores de forma manual, crea un archivo de datos llamado activate.txt en la carpeta "\Archivos de programa\LANDesk\Authorization Files". Adjunte este archivo a un mensaje de correo electrónico y envíelo a licensing@landesk.com. Puede utilizar cualquier asunto o cuerpo en el mensaje.
2. LANDesk Software procesa el adjunto del mensaje y responde a la dirección de correo electrónico desde la cual se envió. El mensaje de LANDesk Software brinda instrucciones y un nuevo archivo de autorización.
3. Guarde el archivo de autorización adjunto en la carpeta "\Archivos de programa\LANDesk\Authorization Files". El servidor central procesa inmediatamente el archivo y actualiza el estado de activación.

Si la activación manual falla o el servidor central no puede procesar el archivo de activación adjunto, se cambia el nombre del mismo con la extensión .rejected y la utilidad registra el suceso con más detalles en el registro de aplicaciones del visor de sucesos de Windows.

Iniciar la sesión en la consola

Tras finalizar la instalación, reiniciar el servidor central y activar el servidor central, inicie la consola. Para ello, abra un explorador y escriba la dirección del servidor en el formato siguiente: http://nombredeservidor/ldsm. (En el servidor central haga clic en Inicio | Todos los programas | LANDesk | System Manager) Cuando se inicie la consola verá la ventana de inicio de sesión de la consola. Es probable que se le pida la credencial de la cuenta que instaló LDSM a fin de iniciar la sesión. Solamente los miembros del grupo LANDesk Management Suite del servidor central pueden iniciar una sesión. De forma predeterminada, el programa de configuración agregó el usuario con el que inició la sesión al instalar el servidor central en el grupo LANDesk Management Suite. Para que otros usuarios puedan acceder a la consola, agréguelos a este grupo.

La primera vez que inicie la consola en un explorador puede demorar hasta 90 segundos para que se visualice. Este retraso sucede debido a que el servidor tiene que realizar la compilación de cierto código, lo cual se efectúa una sola vez. La consola se ejecutará con mayor rapidez después de la primera vez.

Implementación en dispositivos Windows

Este producto admite el método de configuración automática, lo que permite implementar los agentes de forma manual.

Para activar la configuración de instalación automática de servidores Windows 2000/2003 que aún no contienen el agente de administración estándar, debe suministrar las credenciales correspondientes de inicio de sesión, del modo siguiente:

1. En el servidor central, haga clic en **Inicio | Todos los programas | LANDesk |** LANDesk**Configuración de servicios** y luego haga clic en la ficha **Programador**.
2. Haga clic en **Cambiar inicio de sesión**.

3. En los campos **Nombre de usuario y Contraseña**, especifique una cuenta de administrador de dominio (en el formato dominio\nombreusuario).
4. Detenga y reinicie el servicio programador.
5. En la consola Web, seleccione los dispositivos deseados y haga clic en **Configuración del agente > Tarea programada** para implementar las configuraciones.

Puede especificar el administrador de dominios al configurar los miembros Windows 2000/2003 que pertenecen al mismo dominio que el servidor central. Para configurar los servidores Windows 2000/2003 en otros dominios, se deben configurar relaciones de confianza. Es necesario recordar que la cuenta identificada en el paso 3 es la cuenta en la que se ejecutará el servicio programador en el servidor central. Asegúrese de que la cuenta dispone del derecho **Iniciar una sesión como un servicio**.

Si no se realiza correctamente la configuración de instalación automática y aparece el mensaje "No se encuentra el agente", siga los pasos que se muestran a continuación para identificar el problema. Estos pasos simulan las acciones del programador durante una configuración de instalación automática.

1. Busque el nombre de usuario bajo el que se ejecuta el servicio de programación.
2. En el servidor central, inicie la sesión con el nombre de usuario del paso 1.
3. Asigne una unidad a \\nombre de servidor\C$. (Éste es el paso que con mayor probabilidad puede dar error. Esto se puede deber a dos razones. Lo más probable es que no se disponga de derechos administrativos para el servidor. En caso de que este nombre de usuario no disponga de dichos derechos, es probable que la carpeta administrativa compartida del servidor (C$) esté inhabilitada).
4. Cree el directorio \\nombre de servidor\C$\$ldtemp$ y copie un archivo en él.
5. Utilice el Administrador de servicios de Windows e intente iniciar y detener los servicios en el servidor.

Si el dispositivo se encuentra habilitado para IPMI, debe proporcionar la contraseña BMC. Use la ficha **Contraseña BMC** de **Configuración de servicios** para crear una contraseña para el IPMI Baseboard Management Controller (BMC).

1. En la ficha **Contraseña BMC** , ingrese una nueva contraseña en el cuadro de texto **Contraseña**, vuelva a ingresarla en el cuadro de texto **Confirmar contraseña**, y luego haga clic en **Aceptar**.

La contraseña no debe tener más de 15 caracteres y los mismos deben ser números (0-9) o letras mayúsculas o minúsculas (a-z).

Si el dispositivo está habilitado para Intel* AMT, debe proporcionar la contraseña de Intel AMT. Utilice la ficha **Configuración de Intel AMT**de **Configuración de servicios** para crear o cambiar la contraseña en los dispositivos habilitados para la tecnología de Intel* Active Management.

Para configurar la contraseña de Intel AMT

1. En la ficha **Configuración de Intel AMT**, escriba el nombre de usuario y la contraseña actuales. Estos deben coincidir el nombre de usuario y contraseña como se configuró en la Pantalla de configuración de Intel AMT (que se accede en la configuración de la BIOS del equipo).
2. Para cambiar el nombre de usuario y la contraseña, complete la sección **Nueva contraseña de Intel AMT**.

3. Haga clic en **Aceptar**. Este cambio se llevará a cabo cuando se ejecute la configuración del cliente.

Nota: La contraseña nueva debe ser robusta, lo cual quiere decir que

- Tiene al menos siete caracteres de longitud
- Contiene letras, números y símbolos
- Tiene al menos un carácter de símbolo entre la segunda y la sexta posición
- Es muy distinta a las contraseñas anteriores
- No contiene nombres o nombres de usuario
- No es una palabra o nombre común

Implementación en dispositivos Linux

Puede implementar e instalar agentes Linux y RPM en servidores Linux de forma remota. El servidor Linux debe configurarse de forma debida para que esto funcione. Para instalar un agente en un servidor Linux, debe contar con privilegios de raíz.

La instalación predeterminada de Linux (Red Hat 3 y 4 y SUSE) incluye los RPM que requiere el agente de administración estándar para Linux. Si selecciona un agente de supervisión en Configuración de agentes, necesita un RPM adicional: sysstat.

Durante la configuración inicial del agente Linux, el servidor central utiliza una conexión SSH con los servidores Linux de destino. Debe contar con una conexión SSH activa que utilice la autenticación mediante nombre de usuario y contraseña. Este producto no es compatible con la autenticación mediante clave pública o privada. Los servidores de seguridad que se encuentren entre el servidor central y los servidores Linux deben permitir el puerto SSH. Pruebe la conexión SSH del servidor central por medio de una aplicación SSH de terceros.

El paquete de instalación del agente Linux consiste de una secuencia de comandos de shell, los archivos tar de agente, la configuración de agente .INI y los certificados de autenticación de agente. Estos archivos se almacenan en el recurso compartido LDLogon del servidor central. La secuencia de comandos de shell extrae los archivos de los archivos tar, instala los RPM y configura el servidor para cargar los agentes y ejecutar el rastreador de inventario de forma periódica según el intervalo especificado en la configuración del agente. Los archivos se colocan en /usr/landesk.

También debe configurar el servicio programador en el servidor central para utilizar las credenciales de autenticación SSH (nombre de usuario/contraseña) en el servidor Linux. El servicio programador utiliza las credenciales para instalar los agentes en los servidores. Utilice la utilidad de configuración de servicios para especificar las credenciales SSH que desee que el servicio programador utilice como credenciales alternas. Recibirá un indicador para que reinicie el servicio programador. Si no lo recibe, haga clic en Detener y luego en Iniciar en la ficha **Programador** para reiniciar el servicio. Esto activa los cambios.

Tras configurar los servidores Linux y agregar las credenciales Linux al servidor central, debe agregar los servidores a la lista **Mis dispositivos** para implementar los agentes Linux. Antes de la implementación a un servidor, debe agregar éste a la lista **Mis dispositivos**. Para ello, detecte el servidor Linux con Detectar dispositivos.

Para detectar los servidores Linux

1. En Detección de Dispositivos, cree una tarea de detección para cada servidor Linux. Utilice un rastreo de red estándar y especifique la dirección IP del servidor Linux de los intervalos IP iniciales y finales. Si tiene varios servidores Linux, especifique una rango de direcciones IP. Haga clic en Aceptar tras agregar los intervalos IP de detección.
2. Para programar la tarea de detección creada, haga clic en ella y luego en **Programar**. Al finalizar la tarea, verifique que el proceso de detección de dispositivos encontró los servidores Linux que desee administrar.
3. En Detección de dispositivos, seleccione los servidores que desee administrar y haga clic en **Destino** para agregar los dispositivos seleccionados a la lista Destino. Haga clic en la ficha **Administrar** en la parte inferior de la ventana. Haga clic en **Mover dispositivos seleccionados** y en **Mover**. Al hacerlo, se agregan los servidores a la lista **Mis dispositivos**, para especificarlos como destinos de la implementación.

Para crear una configuración de agente Linux

1. En Configuración de agentes, haga clic en **Nuevo**.
2. Escriba el nombre de la configuración, haga clic en HP-UX o en Linux Server Edition y haga clic en **Aceptar**.
3. Seleccione la configuración que ha creado y haga clic en **Editar**.
4. Seleccione los agentes que desee.
5. En la ficha Inventario, seleccione las opciones y el intervalo de frecuencia del rastreador que desee. La secuencia de comandos de instalación agrega una tarea cron que ejecute el rastreador según el intervalo seleccionado.
6. Haga clic en **Guardar cambios**.

Para implementar la configuración de agente, selecciónelo en Configuración de agentes y haga clic en **Programar tarea**. Configure la tarea y supervise el progreso de la misma en Tareas de configuración.

Nota: No recibirá información de la integridad del equipo Linux hasta que el rastreador de inventario haya completado el primer rastreo después de la instalación. **Para obtener una configuración de agente Linux**

1. Cree un directorio temporal en el equipo Linux (por ejemplo, /tmp/ldcfg), y copie lo siguiente en el directorio:
    1. Todos los archivos del directorio LDLOGON\unix\linux.
    2. Copie la secuencia de shell que tiene el nombre de la configuración (<nombre de configuración>.sh) en el directorio temporal.
    3. Copie el archivo *.0 con el nombre de la configuración en el directorio temporal. El asterisco (*) representa ocho caracteres (0-9, a-f).
    4. Copie todos los archivos enumerados en el archivo <nombre de configuración>.ini en el directorio temporal. Para identificar estos archivos, busque "FILExx" en el archivo .INI, donde xx es el número. La mayoría de las entradas que encontrará ya habrán sido copiadas en el cliente durante el paso 1, pero encontrará archivos .XML que deben ser copiados. Los nombres de los archivos deben dejarse intactos, con las excepciones siguientes:
        - Debe cambiarse el nombre de alertrules\<cualquier texto>.ruleset.xml a internal.ruleset.xml
        - Debe cambiarse el nombre de monitorrules\<cualquier texto>.ruleset.monitor.xml a masterconfig.ruleset.monitor.xml

2. Si el equipo es un equipo IPMI/BMC (con el monitoreo incluido en la instalación), escriba la línea de comandos siguiente:

export BMCPW="(contraseña bmc)"

3. Con ejecución de raíz, ejecute la secuencia de comandos de shell de la configuración. Por ejemplo, si la secuencia de comandos tiene el nombre "solicitar", utilice la ruta completa siguiente:

/tmp/ldcfg/solicitar.sh

4. Elimine el directorio temporal y todo su contenido.

Nota: Recuerde que si instala el agente automáticamente o a petición a partir de un equipo Linux y luego ejecuta

./linuxuninstall.sh -f ALL

para limpiarlo y a continuación, realiza una instalación automática o a petición, el archivo con el GUID es el único que se queda en el equipo tras completar esta operación.

La opción -f elimina todos los directorios que el producto posee. Consulte la documentación de desinstalación de Linux para obtener información adicional.

Fase 3: Implementación en fases

En la fase 3 se aborda la implementación en fases: La *Implementación* es el proceso por el cual las funciones de administración se amplían a los dispositivos que desee incluir en el dominio de administración.

La implementación de este producto se realiza mediante la carga de agentes y servicios del producto en los dispositivos. De este modo, podrá administrarlos desde una única ubicación central.

En esta fase se abordan los temas siguientes:

- La estrategia de implementación en fases
- Lista de comprobación para la configuración de los dispositivos
- Implementación en dispositivos Windows
- Comprensión de la arquitectura de configuración de dispositivos

La estrategia de implementación en fases

La implementación en fases se basa en tres principios:

1. Implemente los componentes en los dispositivos menos utilizados o que tengan menos impacto en la red ya existente y, a continuación, pase a los dispositivos más utilizados o de mayor repercusión.
2. Confirme que la funcionalidad de cada dispositivo administrado sea estable antes de implementar más agentes.
3. Continúe con la implementación del producto en fases perfectamente planificadas en lugar de desplegar agentes a todos los tipos de dispositivos de una sola vez, lo cual puede complicar la resolución de cualquier problema que se presente.

Una vez completadas las des primeras fases, podrá proceder con esta última fase del proceso de implementación del producto en los dispositivos.

Lista de comprobación para la configuración de los dispositivos

Para configurar dispositivos puede desplegar agentes de forma remota desde la consola Web o instalarlos desde el dispositivo administrado. Para configurar automáticamente debe configurar los servicios de los equipos de IPMI o Intel* AMT. Puede utilizar el subprograma Configuración de servicios para configurar los siguientes servicios en cualquiera de sus servidores y bases de datos. Para iniciar el subprograma Configuración de servicios en el servidor central, haga clic en **Inicio | Archivos de programa | LANDesk | LANDesk Configuración de servicios**. Utilice las fichas Contraseña BMC o Configuración de Intel AMT.

- **Configuración de instalación automática:** Utilice la configuración del agente para definir la configuración del dispositivo. Proporcione las credenciales necesarias para los equipos de Intel AMT o IPMI mediante la Configuración de servicios (consulte "Configuración de servicios" en el *Manual del usuario*). Defina los dispositivos que desee y programe una tarea para enviar la configuración a los dispositivos. Consulte "Configuración de agentes" en el *Manual del usuario*.
- **Configuración manual:** Desde un dispositivo administrado, asigne una unidad a la carpeta compartida LDLogon del servidor central y ejecute SERVERCONFIG.EXE, el cual es el programa de configuración de servidores. Los componentes implementados en el dispositivo se deben seleccionar de forma interactiva.

Obviamente, la configuración manual no resulta adecuada en entornos cuando se encuentre instalando en dispositivos y configurándolos. En la mayoría de los casos, se enviarán agentes a sus dispositivos administrados. Observe que la instalación de productos no instala agentes en el servidor central automáticamente; también debe instalar los agentes en el servidor central y luego reiniciar éste de forma manual.

Independientemente del modo en que se configuren los dispositivos, es preciso asegurarse de utilizar la ficha que se encuentra en la consola Configuración del agente para crear la configuración de dispositivo que se desea implementar.

Los sistemas de Windows XP Professional SP2 o 2003 SP1 requieren la configuración manual del servidor de seguridad para que el producto funcione de forma completa. Especifique la siguiente configuración para estos dispositivos: **Servidores administrados:**

Uso compartido de archivos e impresoras - TCP 139, 445; UDP 137,138 (sin esto, la instalación automática del agente no funcionará)

Distribución de software - TCP 9594, 9595 (sin esto, la instalación automática del agente no funcionará)

Opciones avanzadas - ICMP - "Permitir las solicitudes de eco entrantes" (si esta opción no se encuentra habilitada, el dispositivo no puede detectarse).

Servidor:

Inventario - 5007

Para especificar esta configuración, haga clic en **Inicio | Panel de control | Seguridad**, en el dispositivo administrado. Este producto incluye una configuración de agente predeterminada con lo siguiente: el agente de administración estándar, la actualización de software y los agentes de monitoreo.

Puede crear nuevas configuraciones que incluyan sólo los componentes que desee instalar o bien, (sólo para la versión OEM) agregar la consola de Intel Active System a la configuración predeterminada del agente. Observe que el proceso de implementación de agentes no es acumulativo, ya que las implementaciones desinstalan todos los agentes existentes. Para implementar un nuevo agente en la configuración debe incluirlo con todos los agentes previos que desee que formen parte de la configuración. **Para crear una configuración de dispositivo**

1. En el panel de exploración izquierdo, haga clic en **Configuración del Agente**.
2. Haga clic en **Nuevo**.

3. Escriba el nombre de la configuración nueva en el cuadro Nombre de la configuración.

Ingrese un nombre que describa la configuración sobre la que se encuentre trabajando, como DBServer o Executive Office Server. Puede ser un nombre de configuración existente o uno nuevo.

4. Seleccione **Linux Server Edition**, **Microsoft Windows Server Edition** o **HP-UX**.
5. Para administrar los servidores compatibles con IPMI sin instalar los agentes de software del producto, marque la **Configuración sólo para IPMI BMC** si la configuración es para los servidores compatibles con IPMI, y haga clic en **Aceptar**.
6. Seleccione la configuración que ha creado y haga clic en **Editar**.

Algunas opciones de las fichas podrían atenuarse debido a que no se aplican a la configuración elegida. Por ejemplo, si selecciona una configuración de Windows sólo para IPMI BMC, no se puede configurar ninguna opción.

7. En la ficha **Agente**, seleccione los agentes que desee implementar.
    - **Todos:** Instala todos los agentes en el dispositivo seleccionado.
    - **Actualización de software:** Instala el agente de actualización de software. Con este agente instalado, puede configurar la forma en que se ejecuta el rastreador para detectar las actualizaciones disponibles.
    - **Monitoreo: I**nstala todos los agentes de monitoreo en el dispositivo seleccionado. El agente de monitoreo permite diversos tipos de monitoreo, tales como el monitoreo ASIC directo, IPMI en banda, IPMI fuera de banda, la consola de Intel Active System, Intel AMT y CIM.
8. La **Configuración** se muestra solamente con fines informativos
9. Seleccione una opción de reinicio.

El reinicio manual significa que los dispositivos no se reiniciarán aunque los agentes seleccionados requieran el reinicio. Debe reiniciar el dispositivo de forma manual. Si el dispositivo requiere el reinicio, los agentes instalados funcionarán debidamente hasta que se reinicie el dispositivo. El reinicio del dispositivo es necesario solamente si el agente seleccionado requiere el reinicio.

Nota: solamente los dispositivos que actualizan los agentes 8.5 existentes requieren el reinicio.

10. En la ficha **Inventario**, especifique la configuración del rastreador de inventario. La opciones de configuración se explican a continuación.

- **Actualización automática**: Los dispositivos remotos leen la lista de software en el servidor central durante las exploraciones de software. Si se establece esta opción, cada dispositivo debe disponer de una unidad asignada en el directorio LDLOGON del servidor central de modo que puedan tener acceso a la lista. Los cambios de la lista están disponibles de inmediato en los dispositivos.
- **Actualización manual:** La lista de software utilizada para excluir títulos durante las exploraciones de software se carga en los dispositivos remotos. Cada vez que la lista se modifica en la consola, es necesario volver a enviarla manualmente a los dispositivos remotos.
- **Valores del rastreador de inventario:** Hora en que se ejecutará el inventario. Puede seleccionar la frecuencia y puede especificar que se ejecute siempre al inicio.

Si selecciona la opción **Entre las horas de** del rastreador de inventario, puede especificar un lapso de tiempo en el cual se ejecutará el rastreador. Si un dispositivo inicia una sesión durante

el rango de hora, el rastreo de inventario se ejecuta automáticamente. Si el dispositivo ya ha iniciado una sesión, el rastreo de inventario se inicia automáticamente una vez que se llega a la hora inicial. Esta opción resulta útil si desea que los rastreos de inventario se ejecuten por etapas en los dispositivos a fin de que no envíen los rastreos al mismo tiempo.

- **Siempre ejecutar al inicio:** El rastreador de inventario se ejecuta cada vez que se inicia el dispositivo.

11. En la ficha **Reglamentos**, seleccione algunos reglamentos de alertas y/o monitoreo que desee incluir en la configuración. Estos reglamentos se almacenan en la carpeta ldlogon/alertrules. Se pueden crear nuevos reglamentos de alertas en Monitoreo o Alertas. Para que los reglamentos recientemente creados se muestren en las listas desplegables, debe generar el XML para el reglamento personalizado.
12. Haga clic en **Guardar cambios** para guardar la configuración del agente.

Para obtener más información sobre la implementación en dispositivos, consulte "Descripción de la arquitectura de configuración de agentes", al final de este capítulo.

Implementación en dispositivos Windows

Este producto admite el método de configuración automática, lo que permite implementar los agentes de forma manual.

Para activar la configuración de instalación automática de servidores Windows 2000/2003 que aún no contienen el agente de administración estándar, debe suministrar las correspondientes credenciales de inicio de sesión, del modo siguiente:

1. En el servidor central, haga clic en **Inicio | Todos los programas |** LANDesk | LANDesk**Configuración de servicios** y luego haga clic en la ficha **Programador**.
2. Haga clic en **Cambiar inicio de sesión**.
3. En los campos **Nombre de usuario y Contraseña**, especifique una cuenta de administrador de dominio (en el formato dominio\nombreusuario).
4. Detenga y reinicie el servicio programador.
5. En la consola Web, seleccione los dispositivos deseados y haga clic en **Configuración del agente > Tarea programada** para implementar las configuraciones.

Puede especificar el administrador de dominios al configurar los miembros Windows 2000/2003 que pertenecen al mismo dominio que el servidor central. Para configurar los servidores Windows 2000/2003 en otros dominios, se deben configurar relaciones de confianza. Es necesario recordar que la cuenta identificada en el paso 3 es la cuenta en la que se ejecutará el servicio programador en el servidor central. Asegúrese de que la cuenta dispone del derecho **Iniciar una sesión como un servicio**.

Si no se realiza correctamente la configuración de instalación automática y aparece el mensaje "No se encuentra el agente", siga los pasos que se muestran a continuación para identificar el problema. Estos pasos simulan las acciones del programador durante una configuración de instalación automática.

1. Busque el nombre de usuario bajo el que se ejecuta el servicio de programación.
2. En el servidor central, inicie la sesión con el nombre de usuario del paso 1.

3. Asigne una unidad a \\nombre de servidor\C$. (Éste es el paso que con mayor probabilidad puede dar error. Esto se puede deber a dos razones. Lo más probable es que no se disponga de derechos administrativos para el servidor. En caso de que este nombre de usuario no disponga de dichos derechos, es probable que la carpeta administrativa compartida del servidor (C$) esté inhabilitada).
4. Cree el directorio \\nombre de servidor\C$\$ldtemp$ y copie un archivo en él.
5. Utilice el Administrador de servicios de Windows e intente iniciar y detener los servicios en el servidor.

Si el dispositivo se encuentra habilitado para IPMI, debe proporcionar la contraseña BMC. Use la ficha **Contraseña BMC** de Configuración de servicios para crear una contraseña para el IPMI Baseboard Management Controller (BMC).

1. En la ficha **Contraseña BMC** , ingrese una nueva contraseña en el cuadro de texto **Contraseña**, vuelva a ingresarla en el cuadro de texto **Confirmar contraseña**, y luego haga clic en **Aceptar**.

La contraseña no debe tener más de 15 caracteres y los mismos deben ser números (0-9) o letras mayúsculas o minúsculas (a-z).

Si el dispositivo está habilitado para Intel* AMT, debe proporcionar la contraseña de Intel AMT. Utilice la ficha **Configuración de Intel AMT** de Configuración de servicios para crear o cambiar la contraseña en los dispositivos habilitados para la tecnología de Intel Active Management.

Para configurar la contraseña de Intel AMT

1. En la ficha **Configuración de Intel AMT**, escriba el nombre de usuario y la contraseña actuales. Estos deben coincidir el nombre de usuario y contraseña como se configuró en la pantalla **Configuración de Intel AMT** (que está disponible en la configuración del BIOS del equipo).
2. Para cambiar el nombre de usuario y la contraseña, complete la sección **Nueva contraseña de Intel AMT**.
3. Haga clic en **Aceptar**. Este cambio se llevará a cabo cuando se ejecute la configuración del cliente.

Nota: La contraseña nueva debe ser robusta, lo cual quiere decir que

- Tiene al menos siete caracteres de longitud
- Contiene letras, números y símbolos
- Tiene al menos un carácter de símbolo entre la segunda y la sexta posición
- Es muy distinta a las contraseñas anteriores
- No contiene nombres o nombres de usuario
- No es una palabra o nombre común

Comprobación de la finalización correcta de la implementación de agente

Para comprobar la implementación correcta del agente de administración en los dispositivos, confirme que puede realizar las tareas siguientes desde la consola. Si necesita información adicional para realizar estas tareas, consulte los capítulos del *System ManagerManual del usuario* correspondientes a las características en cuestión.

Inventario

- En la lista **Mis dispositivos**, haga doble clic en un dispositivo y vea la lista de los agentes instalados.
- Realice una consulta de inventario.
- Seleccione un dispositivo y haga clic en **Inventario** para ver la información para dicho dispositivo.
- Modifique el archivo WIN.INI de un dispositivo Windows, vuelva a explorar dicho dispositivo y, a continuación, compruebe que los cambios realizados se han registrado en CHANGES.LOG.

Implementación de dispositivos desde la línea de comandos

Es posible controlar los componentes que se instalan en los dispositivos mediante los parámetros de línea de comandos con SERVERCONFIG.EXE.

Puede ejecutar el archivo SERVERCONFIG.EXE en modo independiente. Se encuentra en (unidad de sistema)\Archivos de programa\LANDesk\ManagementSuite\LDLogon en el servidor central. SERVERCONFIG.EXE también se puede encontrar en el recurso compartido \\servidorcentral\LDLogon, el cual se puede leer en cualquier servidor Windows 2000/2003.

Descripción de la arquitectura de configuración de agentes

Introducción a SERVERCONFIG.EXE

SERVERCONFIG.EXE es la utilidad de configuración de dispositivos del producto. la cual configura los servidores Windows para su administración en tres pasos.

1. SERVERCONFIG determina si otro producto de LANDesk ha configurado el equipo con anterioridad. Si es así, SERVERCONFIG quita los archivos anteriores e invierte los cambios realizados.
2. SERVERCONFIG busca el archivo oculto CCDRIVER.TXT para determinar si es necesaria la reconfiguración del servidor. El proceso de decisión de SERVERCONFIG se desarrolla más adelante. Si el dispositivo no necesita volver a configurarse, se cierra SERVERCONFIG.
3. Si el dispositivo no precisa volver a configurarse, el SERVERCONFIG carga el archivo de inicialización correcto (SERVERCONFIG.INI) y ejecuta las instrucciones contenidas en él.

Si se ejecuta SERVERCONFIG.EXE por segunda vez y se seleccionan agentes distintos a los de la primera ejecución, se eliminarán los agentes de la primera ejecución. Se deberán seleccionar todos los agentes que se necesiten con cada nueva ejecución de SERVERCONFIG.EXE, aunque anteriormente se hayan instalado los agentes.

Los siguientes parámetros de línea de comandos están disponibles para SERVERCONFIG.EXE:

Parámetro	Descripción
/I=	Componentes que se incluirán (deben incluirse las comillas): "Common Base Agent" "Inventory Scanner" "Alerting" "Vulnerability scanner" "Server Monitor" "Active System Console" Puede combinarlos en la misma línea de comandos. Ejemplo: SERVERCONFIG.EXE /I="Mirror Driver" /I="Vulnerability scanner"
/IP	Configura utilizando IP
/L o /Log=	Va a los archivos de registro CFG_YES y CFG_NO en los que se registran cuál dispositivo se ha configurado y cual no.
/LOGON	Ejecuta comandos con el prefijo [LOGON]
/N o /NOUI	No muestra la interfaz de usuario
/NOREBOOT	No reiniciar el dispositivo una vez que ha finalizado
/P	Solicita al usuario permiso para realizar la ejecución
/REBOOT	Reinicia tras la ejecución
/TCPIP	Igual que IP (vea más arriba)
/X=	Componentes que se van a excluir Ejemplo: SERVERCONFIG.EXE /X=SD
/CONFIG=	/CONFIG]= Especifica un archivo de configuración de dispositivo que debe utilizarse en lugar del archivo SERVERCONFIG.INI predeterminado. Por ejemplo, si ha creado archivos de configuración denominados NTTEST.INI, utilice la sintaxis: SERVERCONFIG.EXE /CONFIG=TEST.INI

	Los archivos .INI deben encontrarse en el mismo directorio que SERVERCONFIG.EXE. Observe que el parámetro /config utiliza el nombre de archivo sin el prefijo 95.
/? o /H	Muestra el menú de ayuda

Implementación del agente de administración estándar

El agente de administración estándar es un agente requerido y es el protocolo subyacente del producto.

Implementación del rastreador de vulnerabilidades

El agente del rastreador de vulnerabilidades lleva a cabo las operaciones de rastreo y reparación. El botón **Programar tareas de seguridad** crea una tarea que ejecuta vulscan.exe sin parámetros. Si se ejecuta sin parámetros, vulscan determina la ubicación del servidor central mediante el acceso de la clave de registro "hklm\software\intel\landesk\LDWM", valor "CoreServer". A continuación solicita la lista de información de vulnerabilidad más actualizada, lleva a cabo una exploración y presenta los resultados en el servidor central. Los resultados se colocan en la lista de Actualizaciones detectadas. Las actualizaciones detectadas pueden descargarse al servidor central. Las actualizaciones se pueden revisar en el proceso de reparación. Si el proceso de reparación instala de forma correcta una o más revisiones, volverá a rastrear y presentará nuevos resultados al servidor central. Esto se aplica a actualizaciones de LANDesk y OEM.

Implementación del rastreador de inventario

Puede emplear el rastreo de inventario para agregar dispositivos a la base de datos central y recopilar datos del hardware y software de dispositivos. El rastreador de inventario se ejecuta automáticamente cuando el dispositivo se configura por primera vez. También recopila datos del hardware y software y lo introduce en la base de datos central. A continuación, se producirá el rastreo del hardware cada vez que se inicie el dispositivo, mientras que el del software sucederá en el intervalo que se especifique.

Implementación del agente de monitoreo

El agente de monitoreo permite diversos tipos de monitoreo, tales como el monitoreo ASIC directo, IPMI en banda, IPMI fuera de banda, Intel AMT y CIM.

Implementación de la consola de Active System

Instala el agente que permite el acceso a la consola de Intel Active System desde System Manager por medio de la interfaz o los menús. Este agente se instala solamente en los dispositivos con placas Intel. Si incluye el agente en una implementación en una placa que no sea Intel, no se instalará.

Desinstalación del servidor central

Al igual que se debe seguir una estrategia determinada para implementar los distintos componentes, se dispone de la estrategia correspondiente para la desinstalación de los mismos.

En las secciones siguientes se muestra el modo de desinstalar correctamente cada uno de los componentes. Desinstale los componentes en el orden siguiente:

1. Desinstale los agentes del producto de los dispositivos.
2. Desinstale el servidor central.

Desinstalación de los agentes del producto de los dispositivos

El primer paso del proceso de desinstalación del software del producto de la red es desinstalar los agentes de los dispositivos.

Para desinstalar agentes de los servidores

1. Inicie una sesión en el servidor con derechos administrativos.
2. Asigne una unidad a la carpeta compartida ManagementSuite del servidor central.
3. Abra una interfaz de comandos, vaya a la letra de unidad de la carpeta ManagementSuite e introduzca lo siguiente:

uninstallwinclient.exe

4. La desinstalación se ejecuta el segundo plano y desinstala todos los agentes.

También puede seleccionar Inicio, Ejecutar y luego escribir *nombre de servidor central*\LANDesk\ManagementSuite\uninstallwinclient.exe.**Para eliminar un agente Linux de forma definitiva de un servidor Linux**

1. En la carpeta compartida ManagementSuite, busque el archivo linuxuninstall.tar.gz y cópielo al cuadro de Linux.
2. Ejecute este archivo, utilizando las opciones x, z y f. La línea de comandos debería decir

tar xzf linuxuninstall.tar.gz

3. una vez ejecutado el archivo, ejecute ./linuxuninstall.sh desde la línea de comandos.

Si necesita ayuda con este archivo, ejecútelo con la opción -h. Nota: Recuerde que si instala el agente automáticamente o a petición a partir de un equipo Linux y luego ejecuta

./linuxuninstall.sh -f ALL

para limpiarlo y entonces lo vuelve instalar automáticamente o a petición, este proceso crea entradas duplicadas de base de datos para el mismo equipo con el mismo nombre y dirección IP debido a que se elimina el GUID del equipo.

La opción -f elimina todos los directorios que el producto posee. Consulte la documentación de desinstalación de Linux para obtener información adicional.

El único archivo que queda luego de la desinstalación es el archivo /etc/ldiscnux.conf. Este archivo quedó allí para evitar que la base de datos se llene de dispositivos duplicados. Si no va a colocar de nuevo este dispositivo en la base de datos, puede eliminar el archivo de forma segura. UninstallWinClient.exe se encuentra en la carpeta compartida ManagementSuite. Solamente los administradores tienen acceso a dicho recurso compartido. Este programa desinstala los agentes del producto en todos los dispositivos en los que se ejecuta. Es una aplicación de Windows que se ejecuta en segundo plano sin mostrar una interfaz. Quizá se muestren dos instancias del servidor en la base de datos que se ha eliminado recientemente. Una de las instancias contiene solamente datos históricos y la otra contiene datos futuros.

Nota: De forma predeterminada, Uninstallwinclient.exe reinicia el dispositivo después de desinstalar los agentes. Para evitar el reinicio, puede agregar el intercambiador /noreboot en la línea de comandos.

Desinstalación del servidor central

El último paso del proceso de desinstalación del producto de la red es desinstalar el software del servidor central. Antes de hacerlo, asegúrese de haber desinstalado los agentes de software del producto de los servidores.

Para desinstalar el servidor central

1. Vaya al servidor central.
2. Haga clic en **Inicio** | **Configuración** | **Panel de control** y, a continuación, haga doble clic en **Agregar o quitar programas**.
3. Si se encuentra instalado seleccione Extensiones de plataformas Intel para software de LANDesk y haga clic en Agregar/Eliminar.
4. Para desinstalar un producto de software seleccione software deLANDesk.
5. Haga clic en **Agregar o quitar**.

Desinstalación de la base de datos central
Se debe desinstalar la base de datos central de forma manual.

Desinstalación de la base de datos central

De forma predeterminada, la base de datos central no se encuentra desinstalada cuando desinstala LANDesk® System Manager. Importante: No desinstale la base de datos central si más adelante reinstalará LANDesk® System Manager en el equipo.

Para desinstalar la base de datos central

1. Vaya al servidor central.
2. Haga clic en **Inicio** | **Configuración** | **Panel de control** y, a continuación, haga doble clic en **Agregar o quitar programas**.

3. Para desinstalar la base de datos central, seleccione el Motor de escritorio de Microsoft SQL Server (LDMSDATA).
4. Haga clic en **Agregar o quitar**.

Archivos de la base de datos

Al eliminar el Motor de escritorio de Microsoft SQL Server no se eliminan los archivos de la base de datos que se utilizan en LANDesk® System Manager. Además de ocupar espacio en el disco, no hay peligro de dejar los archivos de la base de datos en su equipo. Si desea eliminar estos archivos de forma manual, elimine el contenido de la carpeta \Archivos de programa\Microsoft SQL Server\MSSQL$LDMSDATA\Data.

Asistencia

En Internet encontrará servicios de atención al cliente en línea de LANDesk Software (sólo disponibles en inglés). En estos servicios encontrará la información más actualizada sobre los productos de LANDesk Software. Asimismo, encontrará notas de instalación, sugerencias para la solución de problemas, actualizaciones de software e información de atención al cliente. Vaya al sitio Web que se indica a continuación y visite la página del producto:

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

Asimismo, puede descargar las últimas versiones de las notas de versión y la documentación, en las que puede encontrar información que no estaba disponible cuando adquirió el producto. Si recibió System Manager de un fabricante OEM, póngase en contacto con su servicio técnico.

Si no puede resolver el problema con este manual o tras consultar el sitio Web de atención al cliente de LANDesk Software, ponemos a su disposición varios servicios de pago de atención al cliente, asesoría y asociación. Para obtener más información, consulte la página de atención al cliente:

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

Antes de llamar al servicio de atención al cliente, asegúrese de que dispone de la información siguiente:

- Su nombre, nombre de la empresa y versión del producto.
- Sistema operativo de red (nombre y versión).
- Actualizaciones y Service Pack instalados.
- Pasos detallados para reproducir el problema.
- Pasos que ha dado para solucionar el problema.
- Información exclusiva del sistema que pueda ayudar al ingeniero de atención al cliente a comprender el problema, como el tipo de aplicación de base de datos, marca de la tarjeta de vídeo instalada, o el fabricante y modelo del equipo.