LANDesk® System Manager 8.7

Manual del Usuario

LANDesk®

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

Acerca de LANDesk® System Manager

Bienvenido a LANDesk® System Manager 8.70 que es una aplicación de administración independiente que permite preservar la disponibilidad de servidores, incluso aquellos que ejecutan Windows, Linux, HP-UX y AIX. También puede instalarse y utilizarse de forma simultánea con LANDeskManagement Suite, mediante la misma base de datos central que Management Suite para facilitar los informes de TI en toda la empresa.

Diseñado con énfasis en un bajo impacto en los recursos, este producto tiene varios agentes y servicios "a petición" que se ejecutan solamente cuando son necesarios, lo cual libera la memoria y los ciclos de CPU para otras tareas. LANDesk reconoce que la disponibilidad de los dispositivos es crucial para su empresa, de modo que el producto se ha diseñado para que ofrezca estabilidad al ejecutarse en entornos de 24 horas al día y 7 días a la semana. Le permite tener control sobre el software que se ejecuta en los dispositivos. Puede instalar el agente completo, seleccionar componentes específicos o mover los dispositivos a la lista de dispositivos sin instalar ningún agente.

Para que los cuadros de diálogo y las ventanas se muestren apropiadamente, el sitio Web de System Manager debe agregarse a la lista de bloqueo de ventanas emergentes del explorador.

Novedades de la versión 8.70

Las funciones siguientes se han agregado o mejorado a partir de la versión anterior de System Manager:

Administración de dispositivos sin agentes: Administre dispositivos en la vista **Mis dispositivos** sin instalar un agente de administración en ellos, cuando estén habilitados con una tecnología de administración fuera de banda, tales como Intel* AMT, IPMI o DRAC.

Grupos personalizados en Tareas programadas: Puede agrupar las tareas en los grupos personalizados para la ejecución.

Modo de principiante: Puede visualizar etiquetas en los botones de las barras de herramientas, lo cual facilita que los usuarios nuevos vean lo que hacen los botones. Del mismo modo, puede elegir que no se visualicen las etiquetas (la información de herramientas todavía se visualiza al colocar el cursor del ratón).

Configuración de hardware: Esta nueva herramienta permite configurar opciones para los dispositivos con capacidad para Intel* AMT. Puede generar identificadores para la incorporación de dispositivos Intel AMT, ver los identificadores generados y cambiar las opciones de configuración para la incorporación de los dispositivos Intel AMT. También puede definir políticas de interrupción de circuito, las cuales detectan y bloquean las actividades de red sospechosas en los dispositivos.

Compatibilidad mejorada con Active Management Technology: Este producto ahora es compatible con Intel* Active Management Technology 2 (además de la versión 1). La versión 2 de AMT también es compatible con la administración sin agentes y la detección automática de los dispositivos Intel* AMT 2.

Funciones del producto

System Manager le permite elegir el nivel de cobertura de la administración, desde la recopilación sencilla de la información hasta el análisis extendido del rendimiento y el control de la configuración. System Manager incluye lo siguiente:

Consola Web de fácil uso: Ejecute el producto en cualquier momento y en cualquier lugar con una consola basada en Web y diseñada para la entrega de datos suntuosos en una interfaz de fácil uso. Puede ejecutarla a partir de la estación de trabajo principal o de una estación de trabajo de la sala de servidores sin necesidad de instalación. Simplemente vaya a la dirección URL del producto, http://*servidorcentral*/LDSM. A fin de especificar los dispositivos como "destino" para acciones como la distribución de software, selecciónelos para colocarlos en la lista **Dispositivos de destino**, del mismo modo que en el modelo de "cesta de compras" de muchas aplicaciones Web.

Compatibilidad con una mayor cantidad de sistemas operativos: Administre varios entornos de red desde una consola integrada. Además de administrar servidores de Windows 2000 y 2003, System Manager proporciona compatibilidad con diferentes variedades de Linux y Unix:

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

Vista de tarea programada: Vea todas las tareas programadas o completadas de implementación de agentes, detección, actualización de software y secuencias de comandos personalizadas desde una ubicación. Puede volver a programar la tarea, modificarla o convertirla en un suceso recurrente.

Compatibilidad con **Intel* AMT:** Se ofrece compatibilidad con Intel* Active Management Technology versiones 1 y 2. Intel AMT permite administrar de forma remota los dispositivos administrados en cualquier estado del sistema mediante la comunicación OOB (fuera de banda), aun cuando el SO no obtenga respuesta o cuando el dispositivo se encuentre apagado. Los únicos requerimientos por parte del dispositivo es que se encuentren conectados con una red de empresa y que tengan alimentación independiente.

Compatibilidad con IPMI: El producto ofrece compatibilidad con servidores habilitados para Intelligent Platform Management Interface (IPMI) (versiones 1.5 o 2.0), para permitir la recuperación remota y fuera de banda de servidores fuera de servicio, al igual que la consulta de datos de administración autónomos aunque el SO o el procesador no estén en ejecución.

Herramienta de secuencia: Puede ejecutar tareas en los dispositivos mediante la creación de secuencias de comandos del programador local.

Supervisión del desempeño: Puede supervisar el rendimiento en tiempo real de los servidores empresariales o de hoja administrados, mediante una amplia variedad de atributos. Lleve un seguimiento de los atributos y consulte los datos históricos del rendimiento informados a través de varios días. Supervise los dispositivos que tengan instalado el agente de supervisión, al igual que los servidores habilitados para IPMI fuera de banda que no tengan el agente.

Compatibilidad con servidores de hoja: Se admiten chasis de hoja y servidores de hoja IBM, y se incluyen capacidades de detección, detección de chasis, inventario, y administración de revisiones. Las herramientas del producto permiten agrupar los servidores de hoja según la función, el chasis, el bastidor o cualquier otro criterio para una recopilación de datos más eficaz.

Elaboración de informes: Ejecute informes en cualquier dispositivo de la base de datos, los cuales incluyen estadísticas de uso, asignación de recursos y muchas otras medidas. Este producto incluye varios informes base (previamente formulados). Estos informes se ejecutan con rapidez mediante el acceso directo de la base de datos para recopilar información y presentar los datos en gráficos de barras o circulares de dos o tres dimensiones. Cree informes adicionales mediante la creación de consultas personalizadas.

Monitoreo de condición / Alertas: El monitoreo de la condición general de un dispositivo es una tarea sencilla. Puede definir umbrales para medidas como el espacio de disco o el uso de la CPU, y configurar la forma en que desee recibir las alertas en caso de que se exceda un umbral. Podrá observar los factores de estado del dispositivo seleccionado e iniciar una acción que resuelva el problema antes de que los usuarios tengan una mala experiencia o se produzca la inactividad de los sistemas.

Actualizaciones de software: Ppuede recibir las actualizaciones de software de System Manager y del hardware de Intel*. Además, puede desplegar de forma manual las actualizaciones seleccionadas utilizando las capacidades de distribución de software.

Administración basada en funciones: Agregar usuarios y configurar su acceso a las herramientas y otros dispositivos en su función administrativa. La administración basada en funciones permite asignar un ámbito para determinar los dispositivos que puede ver y administrar el usuario y los derechos que especifiquen las tareas que pueden realizar, tales como usuarios que solamente pueden ejecutar informes.

Inventario: Mediante la herramienta de rastreo, el producto compila una gran cantidad de información de hardware y software en la base de datos central. Entonces podrá visualizar, imprimir y exportar datos dichos datos.

Detección de dispositivos: Sepa lo que existe en su red. La detección de dispositivos recopila información básica de todos los dispositivos y de otros dispositivos del entorno, para permitir un mayor control y acelerar la implementación de agentes en los dispositivos de destino.

Compatibilidad con la consola de Active System: Se ofrece compatibilidad con la consola de Active System, la cual ofrece un panorama rápido de la integridad del sistema cuando se instala el agente de la consola de Active System en un dispositivo. Puede ver a simple vista si los elementos de hardware seleccionados funcionan correctamente y si existen problemas potenciales que puedan necesitar tratarse. También puede ver métricas detalladas de rendimiento del sistema y ver una lista de componentes del sistema, incluyendo hardware, software, registros e información sobre Intel* AMT e IPMI (si el dispositivo se encuentra habilitado con alguno de los dos).

Tablero ejecutivo: Grupo de herramientas (gráficos informativos, diagramas, cuadrantes y medidores) que permiten que los ejecutivos supervisen la integridad o el estado de sus empresas.

Ayuda: Este producto incluye un Manual de introducción, al igual que temas de ayuda contextuales.

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 la información 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.
- **Público:** Elementos (como grupos, paquetes de distribución o tareas) que todos los usuarios pueden ver. Cuando un usuario modifica un elemento público, la modificación permanece pública. Los grupos públicos son creados por un usuario con derechos de administrador.
- **Privado** o **Usuario:** Elementos creados por el usuario que ha iniciado la sesión en curso. Los demás usuarios no pueden verlos. Los elementos privados o de usuario figuran bajo los árboles **Mis métodos de entrega**, **Mis paquetes** y **Mis tareas**. Los usuarios con derechos de administrador pueden ver los grupos privados y los paquetes y las tareas de usuario.
- **Común:** Elemento que los demás usuarios pueden ver. Cuando el usuario asume la propiedad de un elemento común (mediante su modificación), el elemento se ramifica en dos elementos: el elemento común permanece y se guarda un elemento de usuario en la carpeta Usuarios. Los demás usuarios ya no pueden ver la instancia de usuario del elemento. Un usuario puede marcar cualquier tarea que sea visible como común, para poder compartirla con los demás usuarios. Una vez que el usuario desmarca la opción Común en las propiedades del elemento, la tarea solamente se puede ver en el grupo de tareas de usuario del usuario.

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 realizar la actualización a Management Suite o 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.
2. Escriba el nombre de usuario y la contraseña proporcionados al comprar las licencias.
3. 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 enAceptar.
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 System Manager se encuentra en marcha. Solamente ha utilizado una fracción de las funciones disponibles en System 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.

Licencias

El proceso de licencia ayuda a que la organización cumpla con los contratos de nodos con licencia a través de la ejecución de un proceso de autorización continuo. Este método también permite el uso de varios servidores centrales bajo una cuenta de usuario definida. El proceso de licencia utiliza una base de datos de segundo plano para crear y administrar las cuentas de los usuarios. El proceso de licencia consta de una solicitud y respuesta sencilla del servidor central al proceso de segundo plano, lo cual permite que el servidor central actualice su actividad durante otro periodo.

Cuando ejecuta el producto (o cualquier complemento) tras una instalación, podrá activar una licencia de evaluación para iniciar un periodo de evaluación o especificar un nombre de usuario y una contraseña para activar una licencia adquirida a través del canal de ventas de LANDesk. Se utiliza un solo nombre de usuario y contraseña para activar todos los servidores centrales de una cuenta existente.

El proceso de activación es, en esencia, el mismo para los productos de evaluación y los comprados. Si el dispositivo está conectado a Internet, el proceso consta de un sencillo intercambio de información. Si el dispositivo no está conectado, debe seguirse un proceso manual de envío de un archivo por correo electrónico a LANDesk para luego guardar el archivo devuelto en el servidor central. El proceso de activación funciona de este modo:

1. El usuario ejecuta la utilidad de activación del servidor central
2. Se crea un archivo que contiene la información de servidor y de uso. El mismo se firma con la clave privada del servidor central y se cifra con la clave pública de LANDesk.
3. Si está disponible una conexión a Internet, el servidor central y los servidores de LANDesk se comunican y el servidor central carga el archivo de activación. Se procesa la información en segundo plano y se envía la información de activación, la cual se escribe directamente en la base de datos.
4. Si no está disponible una conexión a Internet, envíe el archivo que se encuentra en la carpeta \Archivos de programa\LANDesk\Authorization Files a licensing@landesk.com.

Adición de licencias

La funcionalidad disponible mediante la consola varía en función de una clave de licencia. Puede agregar una clave de licencia nueva para acceder a funcionalidad adicional o para actualizar la cantidad de usuarios. Durante la instalación, se genera una licencia de prueba por 45 días. Cuando agrega una licencia válida utilizando la consola, la licencia temporal se borra.

Para agregar una clave de licencia

1. En el panel de exploración izquierdo, haga clic en **Preferencias**.
2. Haga clic en la ficha **Licencia**.
3. En la parte inferior de la pantalla, haga clic en el vínculo http:/www.landesk.com/contactus/.

Si no funciona el vínculo anterior, es probable que el nivel de seguridad del explorador se haya especificado en Medio. Cambie el nivel de seguridad de Internet predeterminado a Medio en

Internet Explorer (**Herramientas > Opciones de Internet > Seguridad > Internet > Nivel predeterminado**).

La consola

Inicio de la consola

Para iniciar la consola

1. En el servidor central, haga clic en **Inicio | Todos los programas | LANDesk | LANDesk System Manager**.

   O bien

   En una estación de trabajo remota, abra un explorador y escriba la dirección de la consola. Esto tiene el formato http://*servidorcentral*/ldsm.

2. Escriba un nombre de usuario y una contraseña válidos.

   Si se va conectar a un servidor central remoto, siga las reglas habituales de Windows para el inicio de sesión remoto (por ejemplo, si el usuario es local para el servidor central, escriba únicamente el nombre de usuario; si se trata de un usuario de dominio, escriba el nombre de dominio o de usuario).
3. Haga clic en **Aceptar**.

Si la lista de dispositivos y los botones no aparecen al iniciar la consola, es posible que sea necesario activar el servidor central.

Acerca del cuadro de diálogo Inicio de sesión de System Manager

Utilice este cuadro de diálogo para ejecutar la consola y conectarse a un servidor central.

- **Nombre de usuario:** Identifica a un usuario. Puede ser un usuario administrador u otro tipo de usuario del producto con acceso restringido (si desea obtener más información, consulte Administración basada en funciones). El usuario debe ser miembro del grupo de LANDesk Management Suite en el servidor central. Si se conecta a un servidor central remoto, escriba el nombre de dominio o de usuario.
- **Contraseña:** La contraseña de usuario.

Uso de la consola

Puede utilizar las herramientas para ver, configurar, administrar y proteger los dispositivos en su red, todo desde una sola consola. Puede actualizar el software o las opciones de configuración, diagnosticar problemas de hardware y software, y utilizar la administración basada en funciones para controlar el acceso de los usuarios a las funciones y a los dispositivos Además, si también se encuentra utilizando otros productos de LANDesk, puede conectarlos de forma directa desde la consola.

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 incluye cuadros de diálogo y pantallas que permiten administrar los dispositivos y usuarios, ver informes, ejecutar detecciones, crear y modificar consultas, etc. Puede cambiar el tamaño de las paneles y columnas de la lista **Mis dispositivos**. Si no se han instalado agentes en un dispositivo, el nombre y la dirección IP son las únicas columnas que contienen información. En algunos casos, también se muestra el sistema operativo.

System Manager proporciona ciertas funcionalidades similares a las aplicaciones de Windows con la conveniencia y accesibilidad de un explorador Web.

- Haga clic con el botón secundario en un dispositivo de la lista **Mis dispositivos** a fin de ver las opciones disponibles para el dispositivo, tales como Ping y Destino.
- Para seleccionar varias entradas consecutivas en una lista, haga clic en el primer elemento, mantenga presionada la tecla **Mayús** y haga clic en el último elemento.
- Para seleccionar varias entradas no consecutivas en una lista, mantenga presionada la tecla **Ctrl** y haga clic en cada uno de los elementos.

Para que los cuadros de diálogo y las ventanas se muestren apropiadamente, el sitio Web de System Manager debe agregarse a la lista de bloqueo de ventanas emergentes del explorador.

Administración basada en funciones
Como usuario, los dispositivos que puede visualizar y administrar en la lista **Mis dispositivos** y las herramientas que puede utilizar dependerán de los derechos de acceso y del ámbito de los dispositivos que le haya asignado el administrador. Para obtener más información, consulte "Administración basada en funciones".

Esta sección brinda información sobre:

- Lista Mis dispositivos
- Iconos de dispositivos
- Uso de los menús contextuales
- Uso de las herramientas
- Visualización de las propiedades del dispositivo

Lista Mis dispositivos

La lista **Mis dispositivos** incluye los siguientes grupos y subgrupos: Además, según sus derechos de acceso y ámbitos de dispositivos, podrá crear sus propios grupos para simplificar la administración de los dispositivos.

Todos los dispositivos

La lista **Todos los dispositivos** muestra un listado no jerárquico (sin subgrupos) de todos los dispositivos, el cual corresponde al usuario que actualmente ha iniciado sesión, en función del ámbito de dicho usuario. Cuando se encuentra conectado a un servidor central específico, el administrador puede ver todos los dispositivos administrados por ese servidor central. Los usuarios del producto, por otra parte, tienen restricciones y únicamente pueden ver los

dispositivos que residen dentro del ámbito que tengan asignado (un ámbito está definido por una consulta de base de datos o por una ubicación de directorio).

Los dispositivos que ejecutan agentes del producto (agente de administración estándar e inventario) aparecen automáticamente en la lista **Todos los dispositivos** cuando el rastreador de inventario los rastrea en la base de datos central. Generalmente, este rastreo se realiza por primera vez durante la configuración inicial de dispositivo. Una vez que se ha rastreado un dispositivo en la base de datos central, se considera como dispositivo administrado y puede ser administrado por el servidor central. Si desea obtener más información acerca de la configuración de los dispositivos, consulte "Configuración de agentes de clientes".

Como el grupo **Todos los dispositivos** se rellena automáticamente mediante un rastreo de inventario, es probable que nunca necesite detectar a los dispositivos manualmente. No obstante, con el fin de detectar dispositivos que no se encuentren en la base de datos central (o mover servidores no administrados al grupo de dispositivos), utilice la herramienta de detección de dispositivos para rastrear los dispositivos de la red. Para obtener más información, consulte "Uso de la detección".

El grupo **Todos los dispositivos** brinda la información siguiente de cada dispositivo. Haga doble clic en **Todos los dispositivos** para abrir la lista.

- **Nombre:** Nombre de host del dispositivo, tal como el nombre de equipo Windows*.
- **Dirección IP:** La dirección IP del dispositivo.
- **Condición:** Estado de salud y disponibilidad del dispositivo. Podría ser Normal, Advertencia o Crítico.
- **Agente:** Agente que se ejecuta en el dispositivo.
- **Tipo de dispositivo:** Muestra el tipo de hardware en el equipo (Intel AMT, IPMI, ASIC o IPMI avanzado).
- **Sistema operativo:** Ttipo de sistema operativo que se ejecuta en el dispositivo.
- **Activo desde:** Hora y fecha desde las cuales el equipo ha estado en funcionamiento sin interrupción (en el huso horario de la base de datos).

Al seleccionar un dispositivo, las propiedades de éste se muestran en el panel **Propiedades** debajo de la lista de dispositivos. El panel **Propiedades** muestra varios atributos de dispositivo importantes:

- **Id.:** Número de identificación del dispositivo. El número lo determina la secuencia en la cual se agregó el dispositivo a la lista
- **Todos los dispositivos**.**Dirección IP:** La dirección IP del dispositivo.
- **Fabricante:** Fabricante del dispositivo.
- **Modelo:** Modelo del dispositivo.
- **Velocidad del procesador:** Velocidad de la CPU del dispositivo.
- **Tipo de procesador:** Tipo de la CPU del dispositivo.

En la consola puede ver un inventario detallado, y especificar una acción en el dispositivo, tal como la ejecución de un informe.

Al hacer doble clic en un dispositivo de la lista **Todos los dispositivos** se abre la Consola de información del servidor, la cual contiene la información de resumen, la configuración, las opciones de control remoto y la información de reglamento de alertas del dispositivo.

Grupos Públicos

La lista **Grupos públicos** muestra los grupos de dispositivos que han sido creados por usuarios con derechos administrativos. Los demás usuarios pueden verlos.

Esta lista también muestra los grupos de chasis de hoja que se crean automáticamente al agregar un módulo de administración de chasis (CMM) a la lista de dispositivos administrados. El grupo incluye el CMM y cada servidor de hoja asociado que administre. No se puede editar un grupo de chasis del mismo modo que se edita un grupo que usted haya creado.

Los grupos pueden ser estáticos o dinámicos. Los grupos dinámicos contienen dispositivos que satisfacen criterios de filtro predefinidos, tales como la velocidad del procesador, el SO del dispositivo o un atributo personalizado como el tipo de dispositivo. Los grupos estáticos incluyen una lista definida de dispositivos u otros grupos estáticos o dinámicos.

Grupos Privados

Los **Grupos privados** muestran grupos de dispositivos creados por el usuario que ha iniciado la sesión. Los demás usuarios no pueden ver ni utilizar los grupos privados.

Iconos de dispositivos

Los iconos de dispositivo que se muestran en la lista **Todos los dispositivos** indican el estado actual de cada dispositivo. Para actualizar el estado de los dispositivos uno a la vez, a medida que los selecciona en la lista **Mis dispositivos**, haga clic en el botón **Actualizar** de la barra de herramientas.

En la tabla siguiente se muestra un listado de los iconos de dispositivos y de estados posibles así como de sus significados:

Icono	Descripción
	Dispositivo con estado normal
	Dispositivo con estado de advertencia
	Dispositivo con estado crítico
	Dispositivo con estado desconocido

Uso de los menús contextuales

Los menús contextuales están disponibles para todos los elementos de la consola, incluidos grupos, dispositivos, consultas, tareas programadas, secuencias de comandos, etc. Los menús contextuales proporcionan un acceso rápido a las tareas comunes e información esencial de un elemento.

Para ver el menú contextual de un elemento y haga clic con el botón derecho en el elemento. Por ejemplo, si hace clic con el botón derecho en un dispositivo administrado en la lista **Mis dispositivos**, el menú contextual mostrará por lo general las siguientes opciones:

- **Quitar del grupo:** Quita el elemento del grupo definido por el usuario.
- **Destino:** Mueve el dispositivo seleccionado a la lista Dispositivos de destino. **Nota:** Si no hay dispositivos de destino en la lista **Destino**, haga clic en **Actualizar** en la ficha **Dispositivos de destino**.
- **Ping de dispositivo:** Verifica que el dispositivo esté activo.
- **Rastrear dispositivo:** Envía un comando de seguimiento de ruta para ver un paquete de red que se está enviando y recibiendo y la cantidad de saltos necesarios para que el paquete llegue al destino.

La ayuda no abarca los menús contextuales de todos los elementos de la consola. Es recomendable que haga clic con el botón derecho en cualquier elemento para ver las opciones disponibles.

Uso de las herramientas

Las herramientas están disponibles en el panel izquierdo. Utilice las flechas del teclado en la parte superior del panel para ver todas las herramientas.

El administrador ve todas las herramientas en el panel de exploración izquierdo. El resto de los usuarios verán únicamente las herramientas (funciones) que les estén permitidas en función de los derechos que tengan asignados. Por ejemplo, si un usuario no tiene el derecho Informes, la herramienta Informes no aparece en el panel de exploración izquierdo.

A continuación se muestra una lista completa de las herramientas:

- **Actualizaciones de software:** Descargue los paquetes de actualización correspondientes.
- **Secuencias:** Cree y administre secuencias de comandos.
- **Tareas programadas:** Vea todas las tareas (originadas en Configuración de agentes, Vulnerabilidades, Detección de dispositivos, o Secuencias de comandos) en el Programador.
- **Monitoreo:** Monitorea el rendimiento en tiempo real de los dispositivos mediante una amplia variedad de atributos.
- **Alertas:** Configure alertas y defina los umbrales y las respuestas que utilizará el producto si se excede un umbral.
- **Configuración de agentes:** Cree una configuración de agente IPMI (Baseboard Management Controller), Linux o Windows.
- **Detección de dispositivos:** Busque dispositivos en la red que no se rastrean en la base de datos central.

- **Registros:** Muestra el registro de alertas, que muestra las alertas marcadas como las que desea ver en los dispositivos administrados.
- **Informes:** Administre informes de servicio predefinidos.
- **Consultas:** Cree y modifique consultas de la base de datos para aislar dispositivos que satisfagan cierto criterio.
- **Usuarios:** Controle el acceso de los usuarios a los dispositivos y herramientas en función de los derechos y el ámbito del usuario.
- **Preferencias:** Cree atributos de inventario personalizados y vea la información de licencia.
- **Configuración de hardware:** Abra una ventana aparte con las opciones de configuración de los dispositivos Intel* AMT.

Si hace clic en el nombre de una herramienta, se abre la ventana de dicha herramienta en el panel derecho.

Visualización de las propiedades del dispositivo

En **Mis dispositivos** de !ServerName!, podrá ver información sobre el dispositivo con rapidez. Para ello, haga clic en el dispositivo en la lista y seleccione **Propiedades** en el panel inferior.

Información más detallada acerca del dispositivo se encuentra disponible en los datos de inventario de éste. Para ver datos de inventario en la vista **Todos los dispositivos**, haga clic en el dispositivo y seleccione la ficha **Ver inventario** en el panel inferior, con lo cual se abre la ventana **Inventario**.

Dispositivos de destino

La lista **Dispositivos de destino** ayuda a completar tareas en los dispositivos seleccionados, tales como la implementación de agentes de servidor o la exploración de actualizaciones de software en un grupo selecto de dispositivos.

El número recomendado de dispositivos que debe agregar a la lista es de 250 o menos. Los dispositivos permanecen en la lista hasta que se agote el tiempo de sesión de la consola (tras 20 minutos de inactividad).

Para agregar dispositivos a la lista **Dispositivos de destino**, selecciónelos en cualquier lista de dispositivos. Si no encuentra los dispositivos que desee, utilice el botón **Buscar** en la barra de herramientas. Puede buscar un dispositivo determinado o varios de ellos. Para ello, utilice los caracteres comodín % o *. Haga clic en el botón de la barra de herramientas **Destino** para agregar el dispositivo a la lista **Dispositivos de destino**. Si el botón no está visible, haga clic en el botón **<<**.

Si se encuentran varios dispositivos, seleccione los que desee agregar a la lista y haga clic en **Destino**. Si la lista de dispositivos devuelta genera varias páginas, deberá hacer clic en **Destino** en cada una de las páginas. No podrá seleccionar los dispositivos en varias páginas y hacer clic en los botones una sola vez para todas las páginas. Puede hacer clic en la flecha hacia abajo que se encuentra bajo la barra de herramientas a la derecha para establecer la cantidad de dispositivos que desee mostrar por página. Puede mostrar hasta 500 dispositivos por página. Para cambiar la cantidad de dispositivos que se muestran en una lista, vea Configuración de página bajo **Preferencias**.

Con uno o más dispositivos en la lista **Dispositivos de destino**, puede completar tareas, tal como la implementación de una configuración de agente en cada uno de los dispositivos de destino o la colocación de dispositivos no administrados en la lista **Mis dispositivos**.

Para definir dispositivos de destino

1. En la lista **Mis dispositivos** o en la vista **Dispositivos detectados**, haga clic en el dispositivo que desee seleccionar para una acción. Para seleccionar varios dispositivos, utilice los métodos normales de selección múltiple (MAYÚS+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.

Los dispositivos seleccionados se muestran en el panel inferior, bajo la ficha **Dispositivos de destino**. Una vez que figuren bajo esta ficha, puede abrir una herramienta (tal como Implementación de agentes) y programar una tarea que se pueda aplicar a los dispositivos de destino. Si ha seleccionado dispositivos no administrados como destino, haga clic en la ficha **Administrar** y colóquelos en la lista **Mis dispositivos**.

Filtro de la lista de visualización

La lista **Mis dispositivos** tiene un icono de filtro que puede utilizar para determinar los dispositivos que aparecerán en la lista. Puede filtrar según uno de los criterios (nombre de dispositivo o dirección IP) o puede combinar los criterios para enfocarse en un subconjunto de equipos.

Para filtrar la lista de visualización

1. En la lista **Misdispositivos** haga doble clic en **Todos los dispositivos** o navegue hasta un grupo.
2. Haga clic en **Filtro**  en la barra de herramientas.
3. En la lista desplegable, seleccione **Nombre de dispositivo** o **Dirección IP**.
4. Para definir los parámetros del criterio especificado, escríbalos en el cuadro de texto. En el cuadro **Buscar** no se admiten los caracteres ampliados siguientes: < , > , " , ' , !.

   Si filtró por nombre de dispositivo, escriba el nombre de host o el intervalo de nombres de equipos. Puede utilizar caracteres de comodín para buscar ciertos nombres de equipos (como *srv).

5. Haga clic en **Buscar**.

Uso de los grupos

Puede agrupar los dispositivos para facilitar la administración. Puede crear grupos para organizar los dispositivos según la función, la ubicación geográfica, el departamento, los atributos de dispositivo o cualquier otra categoría que satisfaga sus necesidades. Puede crear, por ejemplo, un grupo de servidores Web para todos los servidores que estén configurados como servidores Web, o crear un grupo que incluya todos los dispositivos que ejecutan un SO concreto. Haga clic

con el botón derecho en un grupo para abrirlo, borrarlo o indicar como destino a todos los dispositivos que contengan acciones como la , el reglamento de alertas y la implementación de agentes.

La visualización principal **Mis dispositivos** contiene los siguientes grupos:

- **Todos los dispositivos:** Se muestra un listado no jerárquico (sin subgrupos) de todos los dispositivos que puede ver el usuario que actualmente ha iniciado sesión en función del ámbito de dicho usuario. Para el administrador, **Todos los dispositivos** incluye la totalidad de los dispositivos administrados que se han rastreado o movido de la base de datos central. Los dispositivos configurados con los agentes de administración estándar aparecen automáticamente en el grupo o la carpeta **Todos los dispositivos** cuando el rastreador de inventario los rastrea en la base de datos central. Los usuarios, incluyendo los administradores, no pueden crear grupos en **Todos los dispositivos**.
- **Grupos públicos:** Se muestra una lista de los dispositivos o grupos que un administrador ha agregado desde el grupo **Todos los dispositivos**, así como grupos de chasis de hoja. El administrador (un usuario con derechos de administrador) puede ver todos los dispositivos de este grupo, mientras que el resto de los usuarios sólo pueden ver los dispositivos que permite su ámbito. Sólo los administradores pueden crear grupos en **Grupos públicos**.
- **Grupos Privados:** Muestra una lista de los grupos o dispositivos del usuario que ha iniciado sesión en función del ámbito de dicho usuario. El usuario puede crear subgrupos de dispositivos únicamente en **Grupos Privados**. Para agregar dispositivos al grupo **Grupos privados** o a uno de sus subgrupos, el usuario debe copiarlos o moverlos de **Grupos públicos** y **Todos los dispositivos**. Los usuarios pueden crear grupos en **Grupos Privados**.

Para obtener más información sobre qué dispositivos se pueden visualizar y administrar en la vista del dispositivo, y qué herramientas administrativas se pueden utilizar, consulte "Administración basada en funciones".

Tipos de grupo:

Puede crear y administrar dos tipos de grupos:

- **Grupos estáticos**. Un *grupo estático* se compone de dispositivos que se agregaron al grupo de forma manual. Los grupos estáticos solo pueden modificarse al agregar o quitar dispositivos de forma manual.
- **Grupos dinámicos**. Un *grupo dinámico* está compuesto por equipos que cumplen con definiciones de filtro o consultas. Cada vez que el grupo se expande, la consulta se resuelve y se muestran los resultados. Por ejemplo, un grupo dinámico podría contener todos los dispositivos en estado de Advertencia. Las máquinas pueden agregar o quitar grupos a medida que cambian los estados.

Para crear un grupo estático

1. En la vista de red del dispositivo, haga doble clic sobre el grupo principal (como por ejemplo **Grupos privados**) y, a continuación en **Agregar grupo**.
2. Escriba un nombre para el nuevo grupo.
3. Seleccione **Estático** y haga clic en **Aceptar**.

Luego de crear un grupo estático, puede mover o copiar los dispositivos al grupo. Para ello, selecciónelos en la lista y haga clic en **Mover/Copiar** en la barra de tareas. También puede copiar dispositivos de la lista **Todos los dispositivos** al grupo o bien, moverlos o copiarlos a partir de otros grupos.

Para crear un grupo dinámico

1. En la vista de red del dispositivo, haga doble clic sobre el grupo principal (como por ejemplo **Grupos privados**) y, a continuación en **Agregar grupo**.
2. Escriba un nombre para el nuevo grupo.
3. Seleccione **Dinámico** y haga clic en **Aceptar**.

Una vez creado el grupo dinámico, se debe crear un filtro para determinar qué equipos aparecerán en ese grupo. Se puede especificar un nuevo filtro o se lo puede basar en una consulta existente.

Para crear un nuevo filtro

1. Seleccione el grupo dinámico que se creó (al hacer esto, se muestran las **Propiedades de grupo** en el panel inferior).
2. Desde **Propiedades de grupo**, seleccione **Crear un filtro nuevo**, y luego **Nuevo filtro**.
3. Seleccione el criterio de filtro que desea usar y haga clic en **Aceptar**.

Para Crear un filtro basado en una consulta existente.

1. Seleccione el grupo dinámico que se creó (al hacer esto, se muestran las **Propiedades de grupo** en el panel inferior).
2. Desde las **Propiedades de grupo**, haga clic en **Crear un filtro basado en una consulta existente**.
3. Seleccione la consulta existente que se desee utilizar para filtrar el grupo y haga clic en **Nuevo filtro**.
4. Seleccione cualquier otro criterio de filtro que desee utilizar y haga clic en **Aceptar**.

Si basa un filtro en una consulta existente, y cualquier usuario posteriormente la modifica, el filtro basado en esa consulta no cambiará de forma dinámica para coincidir con la consulta modificada.

Uso de la ficha Acciones

Utilice la ficha **Acciones** para ejecutar operaciones en dispositivos determinados y seleccionados. Se pueden eliminar dispositivos de la lista de dispositivos administrados, encenderlos, apagarlos y reiniciarlos y supervisar conexiones con dispositivos administrados.

- Eliminar dispositivos
- Opciones de alimentación
- Monitor de dispositivos

Eliminar dispositivos

La opción **Eliminar dispositivos** permite borrar dispositivos determinados y seleccionados de la lista de equipos administrados. La función eliminar puede borrar uno o varios dispositivos de cualquier grupo de System Manager (ya sea un grupo predeterminado o un grupo creado por un usuario). Una vez eliminado el dispositivo del grupo, se elimina por completo de la lista de todas las listas de dispositivos administrados o inventariados, incluyendo el grupo predeterminado **Todos los dispositivos**.

Si se encuentra eliminando una gran cantidad de dispositivos, la operación puede agotar le tiempo de espera. Si la operación agota el tiempo de espera, intente separar la operación en porciones de operaciones menores.

Opciones de apagado y encendido

Las **Opciones de apagado y encendido** permiten apagar, reiniciar, y en el caso de equipos IPMI administrados, encender dispositivos remotos. Para los servidores que no son IPMI, el dispositivo debe tener el agente de LANDesk implementado a fin de ejecutar las funciones de reinicio y apagado. En los equipos IPMI, se deben tener las credenciales IPMI debidas para ejecutar funciones de encendido, apagado y reinicio. Si una caja IPMI tiene implementado el agente de LANDesk, podrá ejecutar las funciones de apagado y reinicio sin las credenciales IPMI. Utilice la utilidad Configuración de servicios para establecer la contraseña IPMI BMC, a fin de utilizar en la administración de servidores IPMI.

Para utilizar las opciones de alimentación

1. En la lista **Mis dispositivos**, haga clic en un dispositivo o seleccione una lista de dispositivos.
2. En el panel inferior, haga clic en la ficha **Acciones**.
3. Haga clic en **Opciones de alimentación**.
4. Seleccione si se realizarán las acciones en los dispositivos de la Dispositivos de destino o solamente en los dispositivos seleccionados.
5. Se encuentran disponibles las opciones siguientes:
    - Reinicio
    - Desactivar
    - Activar (funciona en los dispositivos habilitados para IPMI y para Wake on LAN)

6. Haga clic en **Mostrar la ventana de redireccionamiento de la consola** para abrir un contenedor sumamente ligero con un ejecutor (es más fácil recompilar el ejecutor en EM64T que en el control TTY).

   Al activar o reiniciar un servidor IPMI administrado, puede abrir una ventana de redireccionamiento de la consola que muestra la información de inicio del servidor. Esto puede resultar útil si desea comprobar que el servidor se está reiniciando. También puede utilizar la ventana de la consola para pausar el proceso de inicio y cambiar la configuración del BIOS en el servidor administrado.

   Para ver la ventana de redireccionamiento de la consola, el servidor debe tener habilitado el redireccionamiento de la consola a través de un puerto serie en la configuración del BIOS. La información de la consola se envía al puerto de serie. Si existe un cable serie que conecta el servidor con la consola del administrador, el redireccionamiento de la consola se lleva a cabo por el cable. De no ser así, System Manager inicia un puerto serie mediante una conexión de LAN (SOL) para redireccionar la información del puerto serie a la conexión LAN. La conexión SOL se mantiene abierta mientras que la ventana de la consola esté abierta. Una vez que se hayan terminado de visualizar los datos de la consola, debe cerrar la ventana.

   Cuando se abre la ventana, también se abre una segunda ventana de mensaje. Puede cerrar la ventana de mensajes. Una vez que se abre la ventana de redireccionamiento de la consola, pero antes de que la consola muestre la secuencia de inicio, podría ver caracteres aleatorios en la ventana. Aparecen debido a que el BMC del servidor envía mensajes de transacción de control, los cuales se transmiten en la conexión a la consola del administrador. No se muestran los caracteres mientras la consola muestra la pantalla de inicio, pero podrían volver a aparecer una vez completado el proceso de inicio

Monitor de dispositivos

Utilice el Monitor de dispositivos para comprobar la conectividad de los dispositivos seleccionados. Si un dispositivo pierde su conectividad, no puede enviar la alerta al servidor central. El monitor de dispositivos verifica que todos los dispositivos puedan comunicarse en la red.

1. En la lista **Todos los dispositivos**, haga clic en un dispositivo o seleccione una lista de dispositivos.
2. En el panel inferior, haga clic en la ficha **Acciones** y luego en **Monitor de dispositivos**.
3. Para ver una lista de los dispositivos que se están monitoreando, haga clic en **Mostrar Dispositivos monitoreados**.
4. Ingrese los números de los minutos entre los barridos de ping y la cantidad de veces que el producto intentará comunicarse con el dispositivo.
5. Seleccione si se realizarán las acciones en los dispositivos de la lista de Dispositivos de destino o en todos los dispositivos del grupo **Todos los dispositivos**.
6. Para detener la supervisión en todos los dispositivos, seleccione **Nunca realizar ping en los dispositivos**.
7. Haga clic en **Aplicar**.

Únicamente se supervisa el último grupo de dispositivos de destino. Por ejemplo, si seleccionan los dispositivos de destino A y B, y se les aplica la supervisión de dispositivos, el servidor central solo enviará un ping a los dispositivos A y B. Si luego se selecciona el dispositivo C y el D, y se

aplica la supervisión de dispositivos en aquellos dispositivos, sólo se supervisarán los dispositivos C y D, y los A y B dejarán de ser supervisados.

Columnas personalizadas

Utilice **Columnas personalizadas** para modificar nombres y campos de columna. El nombre es el nombre de la columna y el campo contiene los atributos que aparecen en la columna (si el atributo está presente). Los demás usuarios no podrán ver los cambios de columna que usted realice. Los cambios de columnas personalizadas se ven en la vista **Mis dispositivos**.

Este producto incluye un conjunto de columnas predeterminado con siete columnas. No puede editar el conjunto predeterminado, pero puede definir un conjunto de columnas personalizado y utilizarlo como predeterminado propio.

No es aconsejable crear columnas personalizadas en las que pudiese haber varios nombres de campo. Por ejemplo, si crea el campo Computer.Software.Package.Name y se han instalado varios paquetes en el dispositivo, System Manager solamente incluye el nombre de un paquete en cada línea, aunque los distintos nombres de paquetes estén en el mismo dispositivo, lo cual hace que la lista **Todos los dispositivos** tenga varias entradas para el mismo dispositivo.

Para crear un conjunto de columnas personalizado

1. En el panel de exploración izquierdo, haga clic en **Preferencias**.
2. Haga clic en la ficha **Columnas personalizadas**.
3. Haga clic en **Nuevo**.
4. Escriba el nombre del conjunto de columnas.
5. En el cuadro superior, seleccione cada uno de los encabezados de columna que desee en el conjunto de columnas y haga clic en **Agregar**.

   El cuadro muestra una lista que representa todos los datos de inventario que se encuentran en la base de datos. Desplácese por la lista para seleccionar el atributo que desea mostrar en la lista de resultados de consulta. No olvide seleccionar los atributos que le ayudarán a identificar los equipos cliente devueltos en la consulta. Si no encuentra los atributos que desea visualizar, agréguelos en el cuadro de diálogo Atributos personalizados. No obstante, estos atributos deben asignarse a los equipos antes de que aparezcan en el cuadro de diálogo Consulta.

   Nota: Si selecciona un atributo en la base de datos, el cual tenga una relación 1:*, obtendrá entradas duplicadas para el dispositivo. Si selecciona atributos con una relación 1:1 (sólo un atributo posible, como la etiqueta Computer.System.Asset), no recibirá entradas duplicadas.

6. Para cambiar el orden de las columnas, seleccione el encabezado de la columna y haga clic en **Subir** o **Bajar**.
7. Para eliminar una columna, selecciónela en el cuadro inferior y haga clic en **Quitar**.
8. Para cambiar el encabezado visualizado en una columna, selecciónelo en el cuadro inferior, haga clic en **Editar**, modifíquelo y pulse **Intro**. No se admiten los caracteres ampliados siguientes: < , > , ' , " , !.
9. Haga clic en **Aceptar** para guardar el conjunto de columnas.

10. Para utilizar el conjunto de columnas personalizado cuando visualice la lista **Todos los dispositivos**, selecciónelo y haga clic en **Definir como conjunto de columnas actual** en la barra de herramientas.

Para editar un conjunto de columnas personalizado

1. En el panel de exploración izquierdo, haga clic en **Preferencias**.
2. Haga clic en la ficha **Columnas personalizadas**.
3. Seleccione el conjunto de columnas personalizado y haga clic en **Editar**.
4. En el cuadro superior, seleccione un encabezado de columna y haga clic en **Agregar** para agregar la columna (vea las notas bajo el paso 5 más arriba).
5. Para eliminar una columna, selecciónela en el cuadro inferior y haga clic en **Quitar**.

6. Para cambiar el encabezado visualizado en una columna, selecciónelo en el cuadro inferior, haga clic en **Editar**, modifíquelo y pulse **Intro**. No se admiten los caracteres ampliados siguientes: < , > , ' , " , !.
7. Para cambiar el orden de las columnas, seleccione el encabezado de la columna y haga clic en **Subir** o **Bajar**.
8. Haga clic en **Aceptar** para guardar los cambios.

Atributos personalizados

Los atributos son características o propiedades que pertenecen a un dispositivo. Entre más atributos un dispositivo tenga en una base de datos, más fácil será identificar el dispositivo de forma exclusiva. Puede crear atributos personalizados solamente si utiliza LANDesk® Server Manager con el derecho de Administrador. Si se han creado y agregado los atributos personalizados a la base de datos central, puede asignar valores a dichos atributos para un dispositivo administrado. Si no se han agregado atributos personalizados a la base de datos central, la opción **Asignar atributos** no figura en la ficha **Acciones**.

Para asignar atributos personalizados a los dispositivos

1. En la lista **Todos los dispositivos**, seleccione uno o más dispositivos.
2. En el panel inferior, haga clic en la ficha **Acciones**.
3. Seleccione **Asignar atributos** en el panel izquierdo.
4. Cada nombre de atributo tiene una lista desplegable de valores. Seleccione un valor para el nombre del atributo en la lista desplegable y repita este paso como sea necesario. Haga clic en **Dispositivos seleccionados**.
5. Haga clic en **Asignar** y en **Aceptar**.

También puede asignar atributos personalizados en varios dispositivos que haya definido como destinos. Si existen dispositivos en la lista Destino, haga clic en **Dispositivos de destino** en el paso 4 anterior.

Configuración de páginas

Utilice **Configuración de páginas** para definir las preferencias de las páginas con listad de dispositivos o con gráficos.

1. En el panel de exploración izquierdo, haga clic en **Preferencias**.
2. Seleccione la ficha **Configuración de páginas**.
3. En la lista desplegable **Tipo de gráfico**, seleccione el tipo de gráfico que desee incluir en los **Informes**.
4. En el cuadro **Elementos por página**, escriba la cantidad máxima de elementos que desee mostrar en cada página que utilice paginación. El valor debe ser de 500 elementos o menos.

Modo de principiante

Puede mostrar texto junto a los botones de las barras de herramientas para ayudar a los usuarios nuevos con la identificación de funciones. Si no se selecciona esta opción, solamente se muestran iconos en la barra de herramientas. Los iconos muestran texto cuando se coloca el cursor del ratón encima de ellos.

1. Para mostrar texto junto a los botones de las barras de herramientas, haga clic en la casilla **Mostrar texto en barra de herramientas**.
2. Haga clic en **Actualizar**.

Visualización de la consola de información del servidor

Utilice la consola de información del servidor para ver información resumida de alto nivel sobre el dispositivo, ver información como la del CPU o del ventilador, supervisar el estado y los umbrales de los componentes clave del dispositivo, administrar vulnerabilidades y encender, apagar o reiniciar el dispositivo. La consola de información del servidor tiene las secciones siguientes bajo el panel de exploración izquierdo.

- Información del sistema
- Actualizaciones de software
- Supervisión
- Reglamentos
- Opciones de alimentación
- Configuración de hardware

Para ver la consola de información del servidor de un dispositivo, primero debe implementar el agente de administración estándar en el dispositivo (consulte Configuración de agentes). Además, debe reiniciar el dispositivo tras la instalación del agente para que la consola de información funcione de forma debida. Se requiere el reinicio cuando instala el agente en el servidor central, al igual que en los dispositivos administrados.

Para ver la consola de información del servidor

1. En la vista **Mis dispositivos**, haga doble clic en el nombre del dispositivo.

   La consola se abre en una nueva ventana de exploración y muestra la página **Resumen de condición** de forma predeterminada.

2. Haga clic en los botones del panel de navegación izquierdo para ver la información del servidor y utilizar las herramientas disponibles.

Información del sistema

La página **Información del sistema** contiene datos resumidos sobre la integridad del dispositivo, al igual que información sobre el hardware y software, registros del sistema y otros datos como información sobre activos y la red.

Resumen de condición

La página **Resumen de condición** ofrece un panorama rápido de la integridad del sistema del dispositivo. Puede ver a simple vista si los elementos de hardware seleccionados funcionan correctamente y si existen problemas potenciales que puedan necesitar tratarse.

Si uno de los elementos de integridad se encuentra en un estado de advertencia o crítico, el botón correspondiente contiene un icono amarillo (advertencia) o rojo (crítico) que indica que hay un problema. Haga clic en el botón para ver una descripción del evento que ha causado la alerta de advertencia o crítica.

Resumen del sistema

Utilice la página **Resumen del sistema** para ver información importante sobre el dispositivo seleccionado. La información contenida en la página podría incluir lo siguiente, en función del tipo de hardware y software configurado en el dispositivo.

- **Condición:** Integridad general del dispositivo, tal como lo definen las condiciones y parámetros establecidos.
- **Tipo:** Tipo de dispositivo, tales como el de impresión, de aplicación o de base de datos.
- **Fabricante:** Fabricante del dispositivo.
- **Modelo:** Modelo del dispositivo.
- **Versión de BIOS:** Versión del BIOS del dispositivo.
- **Sistema operativo:** Sistema operativo del dispositivo.
- **Versión del SO:** El número de versión del sistema operativo.
- **CPU:** Fabricante, modelo y velocidad del procesador del dispositivo.
- **Rastreador de vulnerabilidades:** La versión del rastreador de vulnerabilidad.
- **Control remoto:** Versión del agente de control remoto.
- **Distribución de software:** Versión del agente de distribución de software.
- **Rastreador de inventario:** Versión del rastreador de inventario.
- **Tipo de IPMI, Versión de IPMI:** Tipo y número de versión de IPMI que utiliza el dispositivo.

- **Versión de SDR:** Versión del registro de datos de sensor del BMC del dispositivo.
- **Versión de BMC:** Versión del controlador de administración de placa base del dispositivo.
- **Kernel:** En los dispositivos Linux, es el número de versión del kernel instalado.
- **Supervisión:** Número de versión del agente de monitoreo que se encuentra en el dispositivo.
- **Uso de la CPU:** El porcentaje del procesador actualmente en uso.
- **Memoria física utilizada*:** Porcentaje de la memoria física total utilizada en el dispositivo.
- **Memoria Virtual utilizada*:** Porcentaje de la memoria virtual total utilizada en el dispositivo.
- **Último reinicio*:** Fecha y hora del último reinicio del dispositivo (en el huso horario de la base de datos).
- **Unidad:** Unidades del dispositivo con el tamaño total de la unidad y el porcentaje de espacio utilizado.

Esta información se obtiene del registro de Windows o de los archivos de configuración de Linux.

* Esta información aparece cuando se ha instalado un agente en el dispositivo.

Hardware

Utilice la página **Hardware** para ver detalles sobre la configuración de hardware del dispositivo. Los elementos de la lista **Hardware** se agrupan en las categorías siguientes. Observe que no todas las categorías están presentes para todos los dispositivos. Por ejemplo, si el dispositivo no tiene sensores de ventilador y temperatura, la categoría **Enfriamiento** no figura en la lista.

- **CPU:** Procesadores y memoria caché
- **Almacenamiento:** Unidades lógicas, unidades físicas, medios extraíbles y adaptadores de almacenamiento
- **Memoria:** Información de uso y módulos de memoria
- **Chasis:** Chasis del servidor, indica si la caja está abierta o cerrada.
- **Dispositivos de entrada:** Teclado, ratón y otros dispositivos
- **Motherboard:** Motherboard, ranuras de expansión y BIOS
- **Enfriamiento:** Sensores de ventilador y temperatura
- **Alimentación:** Fuentes de alimentación y voltaje

Definición de umbrales de alerta para elementos de hardware

Algunos elementos de la lista **Hardware** representan datos de los sensores del dispositivo, tales como los sensores de temperatura. Si un dispositivo administrado contiene componentes con sensores compatibles, puede cambiar las lecturas de los sensores que ocasionan una alerta. Por ejemplo, un sensor de temperatura de CPU podría tener lecturas de temperatura mínima y máxima que ocasionan alertas de advertencia y críticas. Por lo general, los umbrales se basan en los valores recomendados por el fabricante, pero puede cambiar los valores superiores e inferiores en el cuadro de diálogo **Umbrales**.

1. En la consola de información de servidor, haga clic en **Información del sistema**.
2. Amplíe la carpeta **Hardware** y aumente el nivel de detalle para encontrar el elemento de hardware que desee (por ejemplo, **Enfriamiento | Temperaturas**).

3. En la lista de sensores, haga doble clic en el sensor en el cual desee definir los umbrales.
4. Escriba los valores en los cuadros de texto de umbral inferior o superior, o mueva los deslizadores en la barra de seguimiento hacia la izquierda o la derecha para cambiar los valores.
5. Haga clic en **Actualizar** para guardar los cambios.
6. Para volver a utilizar los valores originales de los umbrales, haga clic en **Restaurar valores predeterminados**.

Registros

La página Registros muestra los registros del sistema local, el registro de eventos del sistema (SEL) de los dispositivos IPMI y un registro de alertas.

Los registros locales, tales como los registros de aplicación, seguridad y sistema, no tienen ningún botón para borrar el registro de la consola, pero puede ver y borrar los registros mediante la Administración de equipos de Windows.

Si el dispositivo de la BIOS tiene la capacidad para borrar el registro de SMBIOS, haga clic en el botón **Borrar registro** para eliminar todas las entradas de registro. Este botón no está disponible si el BIOS no es compatible con esta acción.

Software

La página **Software** muestra información de resumen sobre los procesos, servicios y paquetes del dispositivo, al igual que una lista de las variables de entorno actuales.

- **Procesos:** Muestra los procesos que están en ejecución. Seleccione un proceso y haga clic en **Terminar proceso** para terminarlo
- **Servicios:** Muestra los servicios disponibles en el dispositivo y su estado. Para efectuar cambios, seleccione un servicio y haga clic en **Detener**, **Iniciar** o **Reiniciar**
- **Paquetes:** Muestra los paquetes instalados con los números de versión y el nombre del proveedor
- **Entorno:** Muestra las variables de entorno que se han definido en el dispositivo

Otros

La página **Otros** muestra información sobre los activos y un resumen del hardware y las conexiones de red.

- **Información de activos:** Vea y edite la información de administración de activos, tales como la ubicación y el número de etiqueta de activo. También puede ver la información del sistema, como el número de serie, el fabricante y el tipo de chasis.
- **Información de la red:** Vea una lista del hardware de red instalado, las estadísticas de la actividad de red, un resumen de la configuración (incluso la dirección IP, la dirección de puerta de enlace predeterminada, y la información de servidor WINS, DHCP y DNS), al igual que una lista de las conexiones de red actuales (unidades asignadas)

Actualizaciones de software

Utilice la página **Actualizaciones de software** para rastrear las vulnerabilidades detectadas en el dispositivo seleccionado.

Para buscar vulnerabilidades detectadas

1. En la vista **Mis dispositivos**, haga doble clic en el dispositivo que desee configurar. La consola de información del servidor se abre en una ventana nueva del explorador.

2. Desde el panel de exploración izquierdo, haga clic en **Actualizaciones de software**.

Descriptores de columnas

- **Id:** Identifica la vulnerabilidad con un código alfanumérico único y definido por el proveedor.
- **Severidad:** Indica el nivel de gravedad de la vulnerabilidad. Los niveles de gravedad posibles incluyen: Service Pack, Crítica, Alta, Media, Baja, No aplica y Desconocida.
- **Título:** Describe la naturaleza o el destino de la vulnerabilidad en una breve cadena de texto.
- **Idioma:** Indica el idioma del sistema operativo afectado por la vulnerabilidad.
- **Fecha de publicación:** Indica la fecha en la que el proveedor publicó la vulnerabilidad.
- **Instalación en segundo plano:** Indica si el archivo de revisión asociado a la vulnerabilidad se instala en segundo plano (sin la intervención del usuario). Algunas vulnerabilidades tienen más de una revisión. Si alguna de las revisiones de la vulnerabilidad no se instalan en segundo plano, el atributo **Instalación en segundo plano** de la vulnerabilidad indica **No**.
- **Reparable:** Indica si la vulnerabilidad se puede reparar mediante el despliegue o instalación de un archivo de revisión. Los valores posibles son: Sí, No, Algunas (para una vulnerabilidad que incluye varias reglas de detección y no se pueden reparar todas las vulnerabilidades detectadas).

Supervisión

Utilice la página **Supervisión** para ver los contadores y gráficos de rendimiento, y definir los umbrales de los componentes del dispositivo. Si desea más información sobre esta función, consulte la sección Monitoreo de dispositivos.

Para seleccionar un contador de rendimiento que se supervisará

1. En la vista **Mis dispositivos**, haga doble clic en el dispositivo que desee configurar. La consola de información del servidor se abre en una ventana nueva del explorador.

2. En el panel de exploración izquierdo, haga clic en **Supervisión**.
3. Haga clic en la ficha **Configuración del contador de rendimiento**.
4. En la columna **Objetos**, seleccione el objeto que desee supervisar.
5. En la columna **Instancias**, seleccione la instancia del objeto que desee supervisar, si corresponde.
6. En la columna **Contadores**, seleccione el contador específico que desee supervisar.

7. Especifique la frecuencia de sondeo y la cantidad de días que se conservará el historial de conteo.
8. En el cuadro de texto **Alertar si el contador se sale del intervalo**, especifique la cantidad de veces que el contador podrá sobrepasar los umbrales antes de generar una alerta.
9. Especifique los umbrales superiores e inferiores.
10. Haga clic en **Aplicar**.

Para visualizar un gráfico de rendimiento de un contador supervisado

1. Haga clic en la ficha **Contadores activos de rendimiento**.
2. Seleccione un contador de la lista.
3. En la lista **Contadores**, seleccione el contador para el cual desee ver el gráfico de rendimiento.
4. Seleccione **Ver datos en tiempo real** para visualizar un gráfico del rendimiento actual o bien, seleccione **Ver datos históricos** para visualizar un gráfico que muestre el rendimiento a través de un lapso de tiempo especificado (Llevar historial) al seleccionar el contador.

En el gráfico de rendimiento el eje horizontal representa el tiempo que ha pasado. El eje vertical representa las unidades que se miden, tales como bytes por segundo (por ejemplo, al supervisar transferencias de archivos), porcentaje (al supervisar el porcentaje de la CPU que se utiliza) o bytes disponibles (al supervisar el espacio en la unidad de disco duro).

Reglamentos

Utilice la página **Reglamentos** para ver una lista de reglamentos de alertas y monitoreos asignados al dispositivo seleccionado y ver los detalles de cada alerta.

Para ver los reglamentos de alertas

1. En la vista **Mis dispositivos**, haga doble clic en el dispositivo que desee configurar. La consola se abre en una ventana nueva del explorador.
2. En el panel de exploración izquierdo, haga clic en **Reglamentos**.
3. Haga clic en la ficha **Reglamentos de alertas**.

El texto siguiente describe los detalles proporcionados sobre cada alerta. Si desea más información sobre la modificación de los detalles, consulte Uso de las alertas.

- **Cuando el estado es:** Si el estado de la alerta alcanza el estado mostrado, se genera una alerta.
- **Afecta la condición:** Si el estado de alerta llega al umbral especificado, el estado afecta la integridad general del dispositivo. La selección de una alerta que afecta la integridad se determina en el diálogo Reglamentos de alertas.
- **Nombre del Reglamento:** Nombre del reglamento de alertas especificado, tal como se ha definido en el cuadro de diálogo Reglamentos de alertas.
- **Tipo de alerta:** Tipo de alerta que se generará, tales como un mensaje de correo electrónico, una captura SNMP o la ejecución de un programa.
- **Configuración de acciones:** Acción que se realiza si se genera la alerta, tal como se ha definido en el cuadro de diálogo Reglamentos de acción.

- **Controlador de alertas:** Controlador asociado a la alerta, tal como el controlador de correo electrónico.
- **Instancia:** Indica el origen específico de la alerta.

Para ver los reglamentos de monitoreo

1. En la vista **Mis dispositivos**, haga doble clic en el dispositivo que desee configurar. La consola de información del servidor se abre en una ventana nueva del explorador.
2. En el panel de exploración izquierdo, haga clic en **Reglamentos**.
3. Haga clic en la ficha **Reglamentos de monitoreo**.

El texto siguiente describe los detalles proporcionados sobre cada uno de los reglamentos de monitoreo. Si desea más información sobre la modificación de los detalles, consulte Acerca del monitoreo.

- **Nombre:** Nombre de la configuración de reglamento, tal como se ha definido en el cuadro de diálogo Monitoreo.
- **Nombre del Reglamento:** Si el reglamento es un reglamento predeterminado o no.
- **Habilitado:** Si el reglamento ha sido habilitado o no para ejecutarse en el dispositivo.
- **Umbral de Advertencias:** Umbral que al excederse, el dispositivo enviará un mensaje de precaución al servidor central.
- **Umbral crítico:** El umbral que al excederse el dispositivo enviará un mensaje crítico al servidor central.
- **Revisar cada:** La frecuencia a la que se monitoreará el elemento.

Opciones de apagado y encendido

Las **Opciones de apagado y encendido** permiten apagar, reiniciar, y en el caso de dispositivos IPMI e Intel AMT administrados, encender dispositivos remotos. Para los servidores que no son IPMI, el servidor debe tener el agente de LANDesk implementado a fin de ejecutar las funciones de reinicio y apagado.

En los equipos IPMI e Intel AMT, se deben tener las credenciales configuradas debidas para ejecutar funciones de encendido, apagado y reinicio. Si los dispositivos IPMI o Intel AMT tienen implementado el agente de LANDesk, podrá ejecutar las funciones de apagado y reinicio sin las credenciales IPMI o Intel AMT. Para configurar las credenciales BMC para los dispositivos IPMI o las credenciales de dispositivos Intel AMT, utilice la utilidad de configuración de servicios (consulte Configuración de servicios y credenciales).

Para utilizar las opciones de apagado y encendido en el dispositivo seleccionado

1. En la vista **Mis dispositivos**, haga doble clic en el dispositivo que desee configurar. La consola se abre en una ventana nueva del explorador.
2. En el panel de exploración izquierdo, haga clic en **Opciones de alimentación**.
3. Se encuentran disponibles las opciones siguientes:

   -  Reiniciar
   -  Desactivar

-  Activar

Configuración de hardware

La herramienta **Configuración de hardware** permite configurar opciones para los dispositivos con capacidad para IPMI o Intel* AMT. Esta herramienta y las opciones se visualizan solamente en los dispositivos que tienen el hardware correspondiente (por ejemplo, las opciones de IPMI sólo se visualizan si el dispositivo se reconoce como dispositivo IPMI).

Puede generar identificadores para la incorporación de dispositivos Intel AMT, ver los identificadores generados y cambiar las opciones de configuración para la incorporación de los dispositivos Intel AMT. También puede definir políticas de interrupción de circuito, las cuales detectan y bloquean actividades de red sospechosas en los dispositivos, y puede activar el monitoreo de Agent Presence para asegurarse de que los agentes de administración de los dispositivos se ejecuten de forma continua. Si desea más información, consulte Compatibilidad con Intel AMT.

En los dispositivos IPMI puede personalizar las opciones de configuración, tales como el temporizador de vigilancia, las opciones de alimentación y la configuración de usuarios de BMC. También puede configurar el uso de un canal LAN o de serie a través de LAN para mantener la comunicación fuera de banda con un dispositivo IPMI. Si desea más información, consulte Configuración de IPMI BMC".

En los dispositivos que tienen un Dell* DRAC (controlador de acceso remoto), puede ver los registros Dell DRAC y editar los nombres de usuario para el acceso a OpenManage Server Administrator. Si desea más información, consulte Administración de dispositivos Dell DRAC.

Administración de dispositivos Intel* AMT

Tras detectar un dispositivo Intel* AMT y agregarlo a la base de datos central para su administración, se puede administrar el mismo de maneras limitadas, aunque el dispositivo no tenga instalado el agente de LANDesk. (Consulte Detección de dispositivos Intel* AMT si desea información sobre la detección de dispositivos y el traslado de éstos a la base de datos central).

La tabla siguiente contiene las opciones de administración disponibles para un dispositivo que solamente tiene instalado Intel AMT en comparación a un dispositivo que tiene instalado Intel AMT y un agente de administración de System Manager.

	Sólo Intel AMT	**Intel AMT y el agente**	**Sólo agente**
Inventario	resumen	X	X
Registro de sucesos	X	X	X
Administración de inicio remoto	X	X	

	Sólo Intel AMT	Intel AMT y el agente	Sólo agente
Desactivar la red de SO		X	
Habilitar la red de SO		X	
Forzar Vulscan al iniciar		X	
Histórico de inventario		X	X
Control remoto		X	X
Conversación		X	X
Transferencia de archivos		X	X
Ejecución remota		X	X
Reactivar		X	X
Apagar		X	X
Reinicio		X	X
Rastreo de inventario		X	X
Tareas programadas y políticas	limitado	X	X
Opciones de grupo		X	X
Ejecutar consultas de informes		X	X
Alertas de Intel AMT		X	X

Para ver el resumen de inventario Intel AMT para un dispositivo

1. Haga doble clic en el dispositivo en la lista **Todos los dispositivos**.
2. En la consola de información del servidor, haga clic en **Opciones de Intel AMT**.
3. Haga clic en **Resumen de inventario**.

El resumen muestra el GUID del dispositivo, el producto, el fabricante, el número de serie y BIOS, el procesador, los resúmenes de memoria y el número de versión de Intel AMT. Si falta alguna información, puede actualizar la información haciendo clic en **Actualizar inventario**.

Acceso de dispositivos incorporados con el modo empresarial

Al incorporar un dispositivo Intel AMT en el modo empresarial, el servidor central instala un certificado en el dispositivo a fin de garantizar la comunicación segura. Si el dispositivo se administrará en otro servidor central, debe anularse la incorporación y volver a incorporarse mediante el nuevo servidor central. De no ser así, el acceso al dispositivo de Intel AMT no responderá debido a que el nuevo servidor central no tiene un certificado coincidente. De forma similar, si otro equipo intenta acceder a la funcionalidad de Intel AMT del dispositivo, no tendrá éxito debido a que no tiene un certificado coincidente. Consulte Compatibilidad con Intel* AMT si desea información sobre los modos de incorporación.

Registro de sucesos Intel AMT

System Manager proporciona una vista del registro de sucesos que genera los dispositivos Intel AMT. La configuración determina qué sucesos se capturan en este registro. Puede ver la fecha/hora del evento, el origen del suceso (Columna de entidad), una descripción y la importancia establecida por la configuración de Intel AMT (Crítico o No crítico). También puede exportar la información de registro en el formato de valores separados por comas (CSV).

Para ver el registro de sucesos de Intel AMT

1. Haga doble clic en el dispositivo en la lista **Todos los dispositivos**.
2. En la consola de información de servidor, haga clic en **Información del sistema**.
3. Amplíe **Registros** y haga clic en **Registro de Intel AMT**.
4. Para exportar el registro a un archivo de formato CSV, haga clic en el botón **Exportar** de la barra de tareas y especifique una ubicación donde guardar el archivo.
5. Para limpiar toda la información en el registro, haga clic en el botón **Purgar registro** en la barra de tareas.
6. Para actualizar las entradas de registro, haga clic en el botón **Actualizar registro** de la barra de herramientas.

Opciones de energía de Intel AMT

System Manager contiene opciones para encender y apagar los dispositivos Intel AMT. Estas opciones pueden utilizarse aún cuando el sistema operativo del dispositivo no responda, siempre que el dispositivo se encuentre conectado a la red y tenga alimentación en espera.

Cuando System Manager inicia los comandos de opciones de alimentación, en algunos casos no es posible verificar que los comandos sean compatibles con el hardware que recibe el comando. Algunos dispositivos con Intel AMT pueden no ser compatibles con todas las funciones de las opciones de alimentación (por ejemplo, un dispositivo puede ser compatible con el reinicio IDE-R desde el CD, pero no desde un disquete). Consulte la documentación del proveedor de hardware si le parece que una opción de alimentación no se encuentra funcionando en un dispositivo en particular. También puede revisar si hay actualizaciones BIOS o firmware desde Intel para el dispositivo si las opciones de energía no funcionan como se espera.

Pude simplemente encender o apagar la alimentación del dispositivo o puede reiniciar y especificar cómo se reiniciará el dispositivo. A continuación se presenta una tabla donde se describen las opciones.

Desactivar	Apaga la alimentación del dispositivo
Activar	Apaga la alimentación del dispositivo
Reinicio	Enciende y apaga cíclicamente el dispositivo
Inicio normal	Inicia el dispositivo utilizando cualquier secuencia de inicio que esté establecida como predeterminado en el dispositivo
Inicio desde un disco duro local	Fuerza un inicio desde el disco duro del dispositivo sin importar el modo de inicio predeterminado en el dispositivo
Inicio desde un unidad local de CD/DVD	Fuerza un inicio desde la unidad de CD o DVD del dispositivo sin importar el modo de inicio predeterminado en el dispositivo
Inicio de PXE	cuando se reinicia, el dispositivo compatible con PXE busca un servidor PXE en la red; si se encuentra, se inicia una sesión de PXE en el dispositivo
Inicio IDE-R	Reinicia el dispositivo utilizando la opción de redirección IDE seleccionada (ver a continuación)
Ingrese a la configuración de BIOS	Cuando se reinicia un dispositivo, le permite al usuario ingresar a la configuración del BIOS

Mostrar Ventana de la Consola de redireccionamiento	Cuando se inicia un dispositivo, se inicia en serie en el modo LAN para que se muestre en la ventana de la consola de redirección
Redirección IDE: reinicio desde disquete	Cuando se inicia un dispositivo, comienza desde la unidad de disquete o desde la imagen que se especificó (los archivos de imagen de disquete debe tener el formato .img; ver la nota a continuación)
Redirección IDE: reiniciar desde CD/DVD	Cuando se inicia un dispositivo, comienza desde la unidad de CD o desde la imagen que se especificó (los archivos de imagen de CD debe tener el formato .iso; ver la nota a continuación)
Redirección IDE: reiniciar desde una imagen específica	Cuando se inicia un dispositivo, se inicia desde el archivo de imagen que se especifique (ver nota a continuación)

Para utilizar las opciones de alimentación de Intel AMT

1. Haga doble clic en el dispositivo en la lista **Todos los dispositivos**.
2. En la consola de información de servidor, haga clic en **Opciones de alimentación**.
3. Seleccione un comando de alimentación. Si selecciona **Reiniciar**, seleccione una opción de inicio.
4. Haga clic en **Enviar** para iniciar el comando.

Notas sobre el uso de las opciones de redirección IDE

Para utilizar las opciones de redirección IDE, debe especificarse tanto el archivo de imagen del disquete y del disquete de inicio, como el de un CD/DVD de inicio o el archivo de imagen de un CD/DVD. Los archivos de imágenes de disquetes deben tener el formato .img y los archivos de imagen de CD deben tener el formato .iso. Algunos BIOS pueden requerir que la imagen de CD se encuentre en el disco duro.

Intel AMT generalmente recuerda la última configuración IDE-R, pero System Manager elimina la configuración después de 45 segundos, para que los inicios siguientes no se lleven a cabo con la función IDE-R. La sesión IDE-R del dispositivo Intel AMT dura 6 horas o hasta que se apaga la consola de System Manager. Cualquier operación IDE-R que sigue en progreso después de 6 horas se finalizará.

Imposición de un rastreo de vulnerabilidad y desactivación del acceso a la red en los equipos Intel AMT

Cuando se ha instalado el agente de LANDesk en un dispositivo configurado para AMT, el agente incluye funcionalidad que puede ayudar a resolver problemas con software malévolo u otros problemas que evitan el acceso al dispositivo.

El servicio amtmon.exe se instala con el agente de LANDesk. Cuando este servicio se ejecuta en un dispositivo, puede forzar un rastreo de vulnerabilidad en el siguiente reinicio para intentar identificar cualquier software malintencionado del dispositivo. Si falla la comunicación con el dispositivo, puede deshabilitar la conexión a la red del dispositivo aún cuando el SO no es funcional, como cuando el software malintencionado deshabilita el SO al consumir todos los ciclos de la CPU. Puede deshabilitar la conexión de red para prevenir que el dispositivo envíe a toda la red paquetes no solicitados.

Cuando el agente de LANDesk se encuentra instalado en un dispositivo Intel AMT, las siguientes opciones se encuentran disponibles en la página **Opciones de Intel AMT**:

- **Conexión de red del sistema operativo:** Haga clic en **Deshabilitar** para deshabilitar la pila de red del SO para detener el acceso a la red; haga clic en **Habilitar** para habilitar el acceso a la red del SO, si se deshabilitó.
- **Después de reiniciar, rastrear por vulnerabilidades** fuerza la ejecución del rastreador de vulnerabilidad la próxima vez que se inicia el dispositivo.

Cuando un dispositivo no responde o puede tener software malintencionado en ejecución, el caso de uso recomendado es ejecutar primero el rastreo de vulnerabilidades en el siguiente reinicio para intentar identificar el problema. Si el problema continúa y el equipo se encuentra infectando o atacando la red o si no puede acceder al dispositivo, tiene la opción de deshabilitar el SO NIC.

Forzar un rastreo de vulnerabilidad después de reiniciar

1. Haga doble clic en el dispositivo en la lista **Todos los dispositivos**.
2. En la ventana de la consola del dispositivo, haga clic en **Opciones de Intel AMT**.
3. Haga clic en **Opciones de configuración** y luego en **Rastrear**. Aparece un mensaje en el dispositivo que indica que se ejecutará un rastreo la siguiente vez que se reinicie.
4. Para apagar o reiniciar el dispositivo, utilice las funciones del administrador de inicio remoto de Intel AMT que se mencionan más arriba.

Habilitar o inhabilitar una conexión de red en un equipo que no responde

1. Haga doble clic en el dispositivo en la lista **Todos los dispositivos**.
2. En la ventana de la consola del dispositivo, haga clic en **Opciones de Intel AMT**.
3. Para deshabilitar la tarjeta de red del dispositivo para detener la comunicación con otros dispositivos en la red, haga clic en **Deshabilitar**. cuando se deshabilita la conexión de red, aparece un mensaje en el dispositivo que dice que la tarjeta de red se deshabilitó.

4. Si el dispositivo es seguro para conectarse nuevamente con la red, haga clic en **Habilitar**. Cuando se restablece la conexión, aparece un mensaje en el dispositivo que dice que la tarjeta de red se habilitó nuevamente.

Abrir la pantalla de configuración de Intel AMT

System Manager incluye un vínculo que permite abrir la Pantalla de configuración de Intel AMT. Es una interfaz provista por Intel para ver el estado del dispositivo, la información de hardware, el registro de eventos de Intel AMT, la configuración de inicio remoto y la configuración de red. También le permite agregar y editar las cuentas de usuarios de Intel AMT para el dispositivo. La ventana que muestra esta pantalla está separada de la consola de System Manager y cualquier duda que pueda tener sobre el uso de esta interfaz debe consultarse con el soporte técnico del fabricante del producto.

Abrir la pantalla de configuración de Intel AMT

1. Haga doble clic en el dispositivo en la lista **Todos los dispositivos**.
2. En la ventana de la consola del dispositivo, haga clic en **Opciones de Intel AMT**.
3. Haga clic en la **Consola de Intel AMT** y en **Iniciar la consola web de Intel AMT**.

Administración basada en funciones

Acerca de la administración basada en funciones

Utilice la administración basada en funciones para configurar el acceso de los usuarios a las herramientas y a otros dispositivos según la función administrativa que poseen en el sistema. 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.

Los administradores (usuarios con el derecho de administrador) tienen acceso a las herramientas de administración basada en funciones al hacer clic en **Usuarios** en el panel de exploración izquierdo.

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 funciones para los usuarios según sus responsabilidades, las tareas de administración que desea que realicen y los dispositivos a los que desea que tengan acceso, vean y administren. El acceso a los dispositivos se puede limitar a una ubicación geográfica como un país, región, estado, ciudad o incluso una sola oficina o departamento. El acceso también se puede limitar a una plataforma determinada, tipo de procesador o cualquier otro atributo de hardware o software del dispositivo. Con la administración basada en funciones, puede elegir el número de funciones que desea crear, qué usuarios pueden actuar en dichas funciones y la dimensión del ámbito de acceso al dispositivo.

Ejemplo de funciones administrativas

En la siguiente tabla se incluyen algunas de las funciones administrativas posibles que desee implementar, la tareas comunes que el usuario puede realizar y los derechos que el usuario necesita para desempeñar con eficacia una función.

Función	Tareas	Derechos requeridos
Administrador	Configurar servidores centrales, administrar usuarios, configurar alertas, integrar productos de otras empresas, etc. (Los administradores con derechos completos pueden realizar cualquier tarea de administración.)	Administrador (todos los derechos implícitos)
Asset Manager	Detectar dispositivos, configurar dispositivos, ejecutar el rastreo de inventario, activar el	Detección de dispositivos, distribución de software y

Función	Tareas	Derechos requeridos
	seguimiento del historial de inventario, etc.	administración de consultas públicas
Administrador de informes	Ejecutar informes predefinidos, impresos, etc.	Informes (requerido para todos los informes)

Los anteriores sólo son ejemplos de funciones. La administración basada en funciones es lo suficientemente flexible para permitirle crear tantas funciones personalizadas como sea necesario. Puede asignar los mismos derechos a varios usuarios, aunque deberá restringir el acceso a una serie limitada de dispositivos con un ámbito reducido. Se puede limitar incluso el ámbito de un administrador, sobre todo si pasa a ser administrador de un área geográfica o un tipo de dispositivo administrado específicos. El modo en que aproveche las ventajas de la administración basada en funciones depende tanto de los recursos de red y personal como de sus necesidades concretas.

Para implementar y hacer efectiva la administración basada en funciones, sólo tiene que designar a los usuarios locales actuales de Windows o crear y agregar nuevos usuarios de Windows, como los usuarios del producto, agregar los usuarios al grupo de usuarios de Management Suite y a continuación asignarles los derechos (para las funciones del producto) y ámbitos (para los dispositivos administrados) necesarios. Siga estos procedimientos:

Conocimiento de los derechos

Los derechos proporcionan acceso a las herramientas y funciones. Los usuarios deben tener el derecho (o derechos) necesarios para realizar las tareas correspondientes. Por ejemplo, para controlar los dispositivos de forma remota en su ámbito, el usuario debe tener el derecho de control remoto. Si ha instalado varios productos de LANDesk Management, los derechos se pueden asignar a los usuarios desde cualquier consola y tendrán efecto en todas las consolas.

Si no se ha asignado un derecho a un usuario, las herramientas asociadas con dicho derecho no están visibles para el usuario en la consola del producto. Por ejemplo, si un usuario no recibe el derecho de informes, el elemento informes no aparece en el panel de exploración izquierdo. La tabla siguiente contiene los derechos necesarios para que el usuario visualice la herramienta.

Herramienta	Derechos necesarios para la visualización en el panel de exploración izquierdo
Mis dispositivos	Consola Web básica
Configuración de agentes	Administrador
Alertas	Alertas y monitoreo
Detección de dispositivos	Detección de dispositivos

Herramienta	Derechos necesarios para la visualización en el panel de exploración izquierdo
Supervisión	Alertas y monitoreo
Consultas	Consola Web básica, administración de consultas públicas, informes
Informes	Informes, Administración de revisiones
Tareas programadas	Detección de dispositivos
Secuencias de comandos	Administración de revisiones
Usuarios	Administrador
Actualizaciones de software	Administración de revisiones
Preferencias	Consola Web básica
Configuración de hardware	Administrador

Consulte las descripciones que se incluyen a continuación si desea obtener más información sobre los derechos de producto y el modo en que se pueden utilizar estos derechos para crear funciones administrativas.

El ámbito controla el acceso a los dispositivos
Al utilizar las funciones permitidas por estos derechos, los usuarios siempre estarán limitados por su ámbito (los dispositivos que pueden ver y manipular).

Administrador

El derecho de administrador proporciona un acceso completo a todas las herramientas del producto (no obstante, el uso de estas herramientas sigue limitado a los dispositivos incluidos en el ámbito del administrador).

Es el derecho predeterminado de un usuario recién agregado, a menos que haya modificado la configuración del usuario de plantillas predeterminado.

El derecho de administrador confiere a los usuarios capacidad para:

- Ver y tener acceso a la herramienta **Usuarios** en el panel de exploración izquierdo
- Ver las licencias de producto en **Preferencias** del panel de exploración izquierdo.
- Realizar todas la tareas del producto permitidas por el resto de los derechos que se especifican a continuación.

No se recomienda la eliminación del usuario Administrador. Si usted es el último administrador que inicia una sesión en una consola LDSM particular y utiliza la Administración de equipos de Windows para eliminar el usuario Administrador del grupo Management Suite, se podrían producir problemas cuando vuelva a entrar a la consola. La sesión de Administrador continuará vigente durante los siguientes 20 minutos (el cual es el tiempo de espera predeterminado de la sesión), pero cuando inicie cualquier acción o actualice el explorador (tecla F5) en el cual ha iniciado la sesión como Administrador, ya no estarán disponibles los derechos que pertenezcan solamente al Administrador. No es recomendable que elimine el último usuario Administrador bajo ninguna circunstancia.

Nota sobre los derechos y herramientas
El derecho de administrador se asocia exclusivamente con la herramienta **Usuarios**. Si un usuario no tiene el derecho de administrador, esta herramienta no aparece en la consola.

Todas las herramientas de la consola del producto están asociadas con un derecho correspondiente (como se describe abajo).

Detección de dispositivos

El derecho de detección de dispositivos confiere a los usuarios capacidad para:

- Encontrar dispositivos de la red que no han enviado un rastreo de inventario a la base de datos central del producto de diferentes maneras, como el rastreo de inventario, la detección de agentes de administración estándar y la detección IPMI.
- Programar detecciones periódicas
- Mover dispositivos desde Detectados a Administrados

Administración de consultas públicas

El derecho de administración de Consultas públicas confiere a los usuarios capacidad para:

- Crear consultas disponibles para todos los usuarios
- Capacidad para crear o eliminar consultas públicas
- Capacidad para modificar/editar consultas públicas

Informes

El derecho de informes confiere a los usuarios capacidad para:

- Ver y tener acceso a la herramienta **Informes** en el panel de exploración izquierdo
- Ejecutar informes predefinidos

Administración de revisiones

El derecho de Administración de revisiones es específico a la función de rastreo de vulnerabilidades. Para obtener más información, consulte "Uso de las herramientas de administración de software".

Consola Web básica

El derecho de consola Web básica confiere a los usuarios capacidad para utilizar las funciones asociadas con el derecho. A continuación se enumeran dichas funciones, junto con las excepciones correspondientes a cada función.

- **Mis dispositivos** (el derecho no permite la actualización de grupos públicos ni la eliminación de dispositivos bajo la ficha **Acciones**)
- Cambiar preferencias (pero no los atributos personalizados)

Alertas y monitoreo

El derecho de alertas y monitoreo confiere a los usuarios capacidad para:

- Monitorear el desempeño de varios sistemas y componentes de SO, tales como unidades, procesadores, memoria, procesos, bytes/sec transferidos por el servidor Web del sistema, etc.
- Controlar la condición exacta de todos los dispositivos administrados
- Personalizar alertas que se envían según el nivel de gravedad (crítico, advertencia, informativo, normal, desconocido) o el umbral (por ejemplo, si la utilización del disco duro excede el 90% de su capacidad)
- Elija la acción a realizarse si la alerta excede un umbral (agregar información al histórico, enviar un aviso por correo electrónico, ejecutar un programa en el servidor central o en un dispositivo individual, o enviar una trampa SNMP a una consola de administración SNMP de la red)

Adición de usuarios del producto

Los usuarios del producto son aquellos que pueden iniciar una sesión en la consola del producto y realizar tareas concretas para determinados dispositivos de la red.

Los usuarios del producto no se crean en la consola. Los usuarios aparecen en la ficha **Usuarios** (en el panel de navegación izquierdo, haga clic en **Usuarios**) una vez que se han agregado al grupo de LANDesk Management Suite del entorno de usuarios de Windows del servidor central. El grupo **Usuarios** muestra todos los usuarios que actualmente residen en el grupo LANDesk Management Suite del servidor central.

Existen dos usuarios predeterminados en el grupo **Usuarios**:

- **Usuario de plantillas predeterminado:** Este usuario consiste fundamentalmente en una plantilla de propiedades del usuario (derechos y ámbito) utilizada para configurar nuevos usuarios cuando se agregan al grupo de LANDesk Management Suite. Es decir, al agregar un usuario a este grupo en el entorno de Windows, el usuario hereda los derechos y ámbito definidos actualmente en las propiedades del usuario de plantillas predeterminado. Si el usuario de plantillas predeterminado tiene seleccionados todos los derechos y el ámbito predeterminado de todos los equipos, cualquier usuario que se coloque en el grupo LANDesk Management Suite se agregará al grupo **Usuarios** con derechos en todos las herramientas del producto y acceso a todos los dispositivos.

  Para cambiar las opciones de propiedad del usuario de plantillas predeterminado, haga clic con el botón secundario en él y haga clic en **Modificar derechos**. Por ejemplo, si desea agregar un número elevado 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).

  No se puede eliminar el usuario de plantillas predeterminado.

- **Administrador predeterminado:** Es el usuario administrativo que inició una sesión en el servidor al instalar el servidor central del producto.

Al agregar un usuario al grupo de LANDesk Management Suite en Windows, dicho usuario se lee automáticamente en el grupo **Todos los usuarios** de la ventana **Usuarios** y hereda los mismos derechos y ámbitos que el usuario de plantillas predeterminado. Se muestra el nombre, ámbito y derechos del usuario.

Si elimina un usuario del grupo LANDesk Management Suite en el entorno de usuarios de Windows, el usuario ya no será un usuario activo y podrá eliminarlo del grupo **Usuarios**. La cuenta de usuario sigue existiendo en el servidor 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 la lista **Usuarios** y mostrar los usuarios recién añadidos, haga clic en **Usuarios** y en **Actualizar** en el explorador.

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 más) de la lista.
4. Haga clic en **Agregar** y, a continuación, 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 de usuarios, hacer clic en **Propiedades | Miembro de** y, a continuación, hacer clic en **Agregar** para seleccionar el grupo y agregar el usuario.

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

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

Ahora puede asignar los derechos y ámbito de usuario del producto.

Creación de ámbitos

El ámbito define los dispositivos que puede visualizar y administrar el usuario del producto. Si ha instalado varios productos de LANDesk Management, los ámbitos se pueden asignar a los usuarios desde cualquier consola y tendrán efecto en todas las consolas.

El ámbito puede tener una dimensión tan amplia o reducida como desee y abarcar así todos los dispositivos administrados que se rastrean en la base de datos central, al igual que un solo dispositivo o ninguno. Esta flexibilidad, combinada con el acceso a las herramientas modulares, es lo que hace que la administración basada en funciones sea una función de administración tan versátil.

Ámbitos predeterminados

La administración basada en funciones incluye dos ámbitos predeterminados. Estos dos ámbitos predefinidos pueden resultar útiles al configurar las propiedades del usuario de plantillas predeterminado.

- **Ámbito Ningún equipo (predeterminado):** Excluye todos los dispositivos de la base de datos.
- **Ámbito Todos los equipos (predeterminado):** Incluye todos los dispositivos de la base de datos.

Los ámbitos predeterminados no se pueden editar ni quitar.

Ámbitos personalizados

Puede crear los tipos siguientes de ámbitos personalizados y asignarlos a los usuarios:

- **Basado en la consulta:** Controla el acceso tan sólo a aquellos dispositivos que coinciden con una búsqueda de consultas personalizadas. Puede seleccionar una consulta existente o crear consultas nuevas en el cuadro de diálogo **Consulta**, para definir un ámbito. Si desea obtener más información sobre la creación de consultas, consulte "Creación de consultas de base de datos".
- **Basado en el grupo:** Permite el acceso solamente a los dispositivos ubicados en el grupo seleccionado. Para definir un ámbito, seleccione los grupos en el cuadro de diálogo **Propiedades de ámbito de grupo**.

Puede asignar más de un ámbito a cualquiera de los usuarios. Si se asignan ámbitos múltiples a un usuario, el ámbito acumulado efectivo (es decir, la gama completa de los dispositivos que se pueden acceder y administrar como resultado de la combinación de los ámbitos asignados) es un compuesto sencillo.

Puede personalizar el ámbito efectivo de un usuario mediante la adición y eliminación de ámbitos en cualquier momento. Se pueden utilizar todos los tipos de ámbitos juntos.

Para crear un ámbito

1. En el panel de exploración izquierdo, haga clic en **Usuarios.**
2. En la ficha **Ámbito**, haga clic en el botón **Nuevo ámbito de consulta** o **Nuevo ámbito de grupo** de la barra de herramientas.
3. Escriba un nombre para el ámbito nuevo.
4. Si ha seleccionado Basado en la consulta, elija una consulta existente o haga clic en **Definir** para crear una consulta nueva. Haga clic en **Aceptar**.
5. Si ha seleccionado Basado en grupo, elija un grupo y haga clic en **Aceptar**.
6. Haga clic en **Aceptar** para guardar el ámbito y cierre el cuadro de diálogo.

Asignación de derechos y ámbitos a los usuarios

- Acerca del cuadro de diálogo Derechos o ámbito de usuario
- Acerca del cuadro de diálogo Configuración de control remoto

Una vez que haya agregado los usuarios del producto, obtenido información sobre los derechos y el modo en que controlan el acceso a las funciones y herramientas y creado ámbitos para permitir o limitar el acceso a los dispositivos administrados, el siguiente paso para establecer la administración basada en funciones es asignar los derechos y ámbito adecuados para cada usuario.

Puede modificar los derechos y el ámbito de un usuario en cualquier momento.

Si modifica los derechos o ámbito de un usuario, dichos cambios surtirán efecto la próxima vez que el usuario inicie una sesión en la consola.

Para asignar derechos y ámbito a un usuario

1. En el panel de exploración izquierdo, haga clic en **Usuarios.**

2. Expanda la lista de usuarios para ver los usuarios que son miembros del grupo LANDesk Management Suite en el entorno Windows NT del servidor central.

   Esta lista muestra los nombres de usuario y los derechos asignados (el carácter de verificación indica que el derecho se ha activado).

3. Haga clic con el botón secundario en un usuario y haga clic en **Editar**.
4. En el cuadro de diálogo **Derechos y ámbitos de usuario**, marque o desmarque los derechos como sea necesario.
5. Haga clic en **Ámbito** y seleccione un ámbito en la lista **Ámbitos asignados.**
6. Haga clic en **Aplicar**.

Los nuevos derechos se muestran junto al nombre del usuario en la lista y surten efecto la próxima vez que el usuario se conecta al servidor central.

Para eliminar un ámbito

1. En el panel de exploración izquierdo, haga clic en **Usuarios**.
2. En la ficha **Ámbito**, haga clic en el ámbito que desee eliminar y luego en **Eliminar**. Haga clic en **Aceptar**.

Tenga cuidado al eliminar ámbitos. Los usuarios asignados a ellos tendrán acceso a derechos que se prohibían con el ámbito.

Acerca del cuadro de diálogo Derechos de usuario / Ámbitos de usuario

Utilice este cuadro de diálogo para visualizar y modificar los derechos asignados y el ámbito de un usuario. Para abrir el cuadro de diálogo, seleccione un usuario y haga clic en **Editar**.

Ficha Derechos: muestra los derechos asignados al usuario.

- **Administrador**
- **Detección de dispositivos**
- **Administración de consultas públicas**
- **Informes**
- **Administración de revisiones**
- **Consola Web básica**
- **Alertas y monitoreo**

Ficha Ámbito: muestra los ámbitos asignados al usuario.

- **Ámbitos asignados:** Identifica los ámbitos actuales del usuario.
- **Agregar:** Abre el cuadro de diálogo **Agregar ámbito**, el cual permite seleccionar el ámbito que agregar al usuario.
- **Quitar:** Elimina el ámbito seleccionado.
- **Cancelar:** Cierra el cuadro de diálogo sin guardar los cambios.

Detección de dispositivos

Uso de la detección de dispositivos

La detección de dispositivos busca dispositivos de la red que no tienen instalados los agentes del servidor central que realiza la detección y que no han enviado un rastreo de inventario a la misma base de datos central. La detección de dispositivos dispone de varias formas de localizar dispositivos.

- **Rastreo de red:** Busca equipos realizando un barrido de ping ICMP. Se trata de la búsqueda más profunda, pero podría tomar más tiempo (si se utiliza la huella digital de IP). La búsqueda se puede limitar a ciertos intervalos IP y de subred. De forma predeterminada, esta opción utiliza NetBIOS para recopilar información sobre el dispositivo. También se pueden seleccionar las Huellas IP, que también otorgan el tipo de SO (en la mayoría de los casos). La opción de rastreo de red también incluye la opción **Utilizar SNMP**, que configura el rastreo que se utiliza con SNMP para los dispositivos SNMP, tales como las impresoras.
- **Detección de CBA:** Busca el agente de administración estándar (anteriormente conocido como agente de base común, [CBA] en Management Suite) en los equipos. Esta opción detecta equipos que han sido administrados por Server Manager, System Manager, etc. Puede seleccionar la opción PDS2 para detectar dispositivos con el agente PDS2 de LANDesk anterior. Los equipos Linux no admiten la detección CBA, pero si elije PDS2, pueden detectarse los equipos Linux con un agente instalado.
- **IPMI:** Busca servidores habilitados para la Interfaz de administración de plataforma inteligente (IPMI), que permite el acceso al controlador de administración de placa base (BMC), sin importar que el servidor esté encendido o no, o en qué estado se encuentre el SO.
- **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 que tienen Intel Active Management Technology (version 1), lo que permite funciones de administración limitadas sin importar que el servidor esté encendido o no, o en qué estado se encuentre el SO.

La detección de dispositivos intenta detectar la información básica sobre cada dispositivo. No toda la información siguiente está disponible para cada dispositivo.

- **Nombre de nodo:** Nombre del dispositivo detectado, si está disponible.
- **Dirección IP:** Dirección IP detectada.
- **Máscara de subred:** Máscara detectada.
- **Categoría:** Grupo de detección de dispositivos al que pertenece el dispositivo.
- **Nombre de SO:** Descripción del sistema operativo detectado, si está disponible.

Cuando la detección de dispositivos encuentra un dispositivo por primera vez, consulta la base de datos central para ver si la dirección de IP del dispositivo y el nombre ya están en la base de datos, en la lista **Mis dispositivos**. Los dispositivos de la lista **No administrados** se vuelven a detectar y posiblemente arrojan más datos. Si hay una coincidencia, la detección de dispositivos hace caso omiso del dispositivo. Si no hay ninguna coincidencia, la detección de dispositivos agrega el dispositivo a la tabla de dispositivos **No administrados**. Los dispositivos de esta tabla

no utilizan ninguna licencia de System Manager. Un dispositivo se considera administrado una vez que envía un rastreo de inventario a la base de datos central. Una vez que el dispositivo se mueve al grupo **Todos los dispositivos**, ya no aparece en la lista **Dispositivos detectados**.

Los dispositivos IPMI deben tener un BMC (controlador de administración de placa base) que se configura para poder detectarse como dispositivos IPMI y utilizar la funcionalidad completa de IPMI. Si no se configura BMC, el dispositivo puede detectarse como un equipo. Entonces puede agregar el dispositivo a la lista de dispositivos administrados y ejecutar la función de configuración de hardware para configurar la contraseña BMC. Entonces, este producto reconocerá la funcionalidad del dispositivo IPMI se reconocerá. Observe que la dirección IP del BMC no es necesariamente la misma que la dirección IP del sistema operativo, y por lo tanto, quizá no sea posible que se realice una instalación automática de agente directamente en la dirección IP del BMC. Es probable que sea necesaria una nueva detección de direcciones IP estándares para realizar la instalación automática de un agente en la dirección IP del BMC. La dirección IP del BMC debe ser capaz de recibir una instalación automática de agente de IP.

Los dispositivos habilitados para Intel* AMT (versión 1) deben configurarse con un nombre de usuario y una contraseña de Intel AMT para que sean reconocidos y detectados como dispositivos Intel AMT. Tras la detección, ejecute la función de configuración de hardware para configurar las opciones de Intel AMT e incorporar el dispositivo en el modo Pequeños negocios o en el modo Empresa, el cual es más seguro.

Para automatizar la detección de dispositivos, puede programar las detecciones para que se produzcan periódicamente. Por ejemplo, la red se puede dividir por subredes y se puede programar un barrido de ping para una subred diferente cada noche. El servidor central lleva a cabo todas las detecciones.

Para detectar y administrar dispositivos en su red, debe completar las tareas siguientes:

- Crear configuraciones de detección
- Programar y ejecutar las detecciones
- Ver los dispositivos detectados
- Trasladar los dispositivos detectados a la lista **Mis dispositivos**

Uso de la detección de dispositivos no administrados con dispositivos que utilizan servidores de seguridad

Tenga en cuenta que la detección de dispositivos no administrados por lo general no funciona con dispositivos que utilizan un servidor de seguridad, tal como el Servidor de seguridad de Windows, a menos que el servidor de seguridad se configure de forma manual. Debe abrir lo siguientes puertos. Para cambiar estas opciones, vaya al servidor de seguridad de Windows a través del Panel de control de Windows.

Servidores administrados:

- Archivos e impresoras compartidas: TCP 139, 445; UDP 137,138 (sin esto, la instalación automática no funcionará)
- Distribución de software: TCP 9595 (sin esto, el envío no funcionará)
- Opciones avanzadas - ICMP: "Permitir las solicitudes de eco entrantes" (si esto no se encuentra habilitado, no puede detectarse).

Servidor central:

- Inventario: 5007
- Control remoto: 9535

Creación de configuraciones de detección

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. Si desea más información, consulte Configuración de rastreos 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. Para obtener una descripción de IPMI, consulte Compatibilidad con IPMI.
- **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.

Para editar o eliminar una configuración

- En la ficha **Configuraciones de detección**, haga clic en la configuración que desee y en **Editar** o **Eliminar**.

Configuración de rastreos de SNMP

Las detecciones de rastreo de red pueden utilizar SNMP. Según la configuración de SNMP de la red, es probable que deba especificar información adicional sobre SNMP en la configuración de detección. Haga clic en **Configurar** junto a la opción **SNMP** para abrir el cuadro de diálogo **Configuración de SNMP**, el cual contiene tres opciones:

- **Reintentos:** Cantidad de veces que la detección de dispositivos reintenta la conexión SNMP.
- **Espera de respuesta en segundos:** Lapso de tiempo que la detección de dispositivos debe esperar una respuesta SNMP.
- **Port:** Puerto al que la detección de dispositivos debe enviar las consultas de SNMP.
- **Nombre de comunidad:** Nombre de la comunidad SNMP que la detección de dispositivos debe utilizar.
- **Configurar SNMP V3:** La detección de dispositivos también admite SNMP V3. Haga clic en este botón para configurar las opciones de SNMP V3 en el cuadro de diálogo **Configuración de SNMP V3**.

El cuadro de diálogo **Configuración de SNMP V3** contiene estas opciones:

- **Nombre de usuario:** El nombre de usuario que la detección de dispositivos debe utilizar para la autenticación con el servicio SNMP remoto.
- **Contraseña:** Contraseña del servicio SNMP remoto.
- **Tipo de autenticación:** Tipo de autenticación que SNMP utiliza. Puede ser **MD5**, **SHA** o **Ninguna**.
- **Tipo de privacidad:** Método de codificación que utiliza el servicio SNMP. Puede ser **DES**, **AES128** o **Ninguna**.
- **Contraseña de privacidad:** Contraseña que se utiliza con el tipo de privacidad especificado. No está disponible si selecciona el tipo de privacidad **Ninguna**.

Programación y ejecución de detecciones

Utilice el botón **Programar** de la ficha **Configuración de la detección** para abrir el cuadro de diálogo **Tarea programada**. Utilice este cuadro de diálogo para programar cuándo ejecutar las configuraciones de detección. Puede programar una configuración de detección o de servidor para que se ejecute inmediatamente, en algún momento del futuro, de forma recurrente o una sola vez.

Las tareas de detección pueden reprogramarse o eliminarse de la ficha **Tareas de detección**. Una vez que programe una tarea de detección, consulte la ficha **Tareas de detección** para ver el estado de la detección. También se puede tener acceso al estado de las tareas de detección en la herramienta **Tareas programadas**. Tras completar las tareas de detección, los nuevos dispositivos que aún no se encuentran en la base de datos central se agregan a las categorías de dispositivos detectados.

El cuadro de diálogo **Tareas programadas** contiene las opciones siguientes.

- **Mostrar en Tareas comunes:** Permite que otros usuarios vean la tarea. Cuando otro usuario edita o ejecuta la tarea, el usuario se convierte en el propietario de una instancia de la tarea.

- **Propietario:** Propietario de la tarea.
- **Dejar sin programar:** (opción predeterminada) Deja la tarea en la lista de tareas para su programación futura.
- **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:
    - **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.
    - **Hora:** Hora en que desea iniciar la tarea.
    - **Repetir cada:** Si desea repetir la tarea, seleccione la frecuencia (cada Día, Semana o Mes). Si elige Mes 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 detección

1. En el panel de navegación izquierdo, haga clic en **Detección de dispositivos**.
2. En la ficha **Configuraciones de detección**, seleccione la configuración que desee y haga clic en **Programar**. Configure la programación de detección. Una vez que haya finalizado, haga clic en **Guardar**.
3. Observe el progreso de la detección en la ficha **Tareas de detección**.
4. Al finalizar la detección, los resultados se visualizan en el panel superior **Dispositivos detectados**. Si hace doble clic en la tarea de detección, la cantidad y el porcentaje de dispositivos es de cero debido a que estas cifras se asocian a los dispositivos de destino y las tareas de detección no tienen destinos.

La ficha **Tareas de detección** muestra el estado de las tareas de detección. El estado incluye lo siguiente:

- El nombre de la configuración de detección.
- El estado de la tarea, el cual puede ser En curso, Todas completadas, Ninguna completada o Fallida.
- La última ejecución de la tarea.
- El tipo de tarea ejecutada.

Para eliminar o volver a programar una detección

Si desea eliminar una tarea de la lista, ya sea que se haya ejecutado o no, haga clic en la tarea y en **Eliminar**. Si la tarea aún no se ha ejecutado o es una tarea recurrente, su eliminación evita que se ejecute en el futuro.

También puede volver a programar una tarea de detección de la lista o ejecutarla de nuevo en otro momento. Para ello, haga clic en la tarea, luego en **Editar**, elija **Programar** y restablezca la programación. Para volver a ejecutar la tarea de inmediato, selecciónela y haga clic en **Iniciar ahora**.

Para ver el estado de las tareas de detección

1. En el panel de exploración izquierdo, haga clic en **Dispositivos detectados**.

2. Haga clic en la ficha **Tareas de detección** o en **Actualizar** en la barra de herramientas de dicho panel.

Visualización de dispositivos detectados

Todos los dispositivos detectados aparecen en el panel superior **Detección de dispositivos**. Este panel muestra los resultados de todas las detecciones que ha ejecutado. Al ejecutar una detección nueva, los dispositivos encontrados se agregan a la lista.

Cuando la Detección de dispositivos encuentra un dispositivo, intenta especificar el tipo de dispositivo de modo que pueda agregarlo a una de las siguientes categorías:

- **Chasis:** Contiene un módulo de administración de chasis de hoja (CMM).
- **Equipos:** Incluye equipos. Los sistemas Linux podrían clasificarse como sistemas Unix en la columna **Nombre de SO**.
- **Infraestructura:** Iincluye enrutadores a otro hardware de red.
- **Intel AMT:** Contiene dispositivos compatibles con Intel* Active Management Technology.
- **IPMI:** Contiene dispositivos compatibles con IPMI.
- **Otros:** Contiene dispositivos no identificados.
- **Impresoras:** Incluye impresoras.

Estas categorías ayudan a mantener organizada la lista **Detección de dispositivos**, por lo que resulta más sencillo localizar los dispositivos de interés. Las listas de dispositivos se pueden organizar por cualquier encabezado de columna al hacer clic en uno de ellos. Puede que la Detección de dispositivos no clasifique los dispositivos correctamente en todas las ocasiones. Para mover con facilidad los dispositivos no identificados al grupo debido, haga clic con el botón secundario en el dispositivo que desee mover, haga clic en **Mover**, seleccione la categoría correspondiente y haga clic en **Aceptar**.

Algunas veces, el servidor central figura dos veces. Esto sucede debido a que el mismo equipo es encontrado por medio de distintos mecanismos de detección (por ejemplo, CBA, IPMI, CMM, PDS1 y PDS2) y a que la información del equipo se agrega a la base de datos mediante dicho mecanismo.

Una vez que se implementan los agentes en un dispositivo detectado y el dispositivo envía un rastreo de inventario al servidor central, el dispositivo detectado se eliminará de la lista de dispositivos detectados.

Filtro de la lista de dispositivos

Para encontrar dispositivos que coincidan con un criterio de búsqueda determinado, utilice el campo **Filtrar por** de la barra de herramientas. Puede filtrar según el nombre del nodo, la dirección IP, la máscara de subred, la categoría o el nombre de SO. Al utilizar un filtro, los dispositivos se ordenan alfabéticamente según el atributo utilizado en el filtro.

Para filtrar la lista de dispositivos

1. En el panel de exploración izquierdo, haga clic en **Detección de dispositivos**.
2. En el árbol **No administrados**, haga clic en el grupo que desee filtrar.

3. En **Filtrar por**, haga clic en el atributo que filtrar. Si el botón **Filtrar por** no está visible, haga clic en **>>** para ampliarlo.
4. En el cuadro junto al atributo, escriba el texto que filtrar.
5. Haga clic en **Buscar**.

Adición de categorías

Se pueden crear categorías de dispositivos para agrupar los dispositivos no administrados. Si mueve un dispositivo a otra categoría, aparecerá en dicho grupo de nuevo si la detección de dispositivos detecta el dispositivo más adelante. Al mover los dispositivos que sabe que no administrará con la consola a otros grupos, podrá ver con más facilidad los dispositivos nuevos del grupo **Equipos**.

Si elimina un grupo que incluye dispositivos, la detección de dispositivos los mueve al grupo **Otros**.

Para agregar una categoría de dispositivo

1. En la vista **Detección de dispositivos**, haga clic en **Agregar categoría**.
2. Escriba un nombre para el grupo en el cuadro **Nombre de categoría** y haga clic en **Aceptar**.
3. Para eliminar una categoría que ha agregado, seleccione la categoría, haga clic en **Eliminar categoría** y luego en **Aceptar** para confirmar la eliminación.

Traslado de dispositivos detectados a la lista Mis dispositivos

Tras la detección de dispositivos, puede moverlos a la lista **Mis dispositivos**. Al mover los dispositivos, su información se agrega a la base de datos. Una vez que la información se encuentre en la base de datos, podrá implementar la configuración del agente, ejecutar consultas e informes con dicha información y realizar muchas otras tareas administrativas.

Para los dispositivos que pueden administrarse fuera de banda (los que tienen funcionalidad de IPMI, Intel AMT o DRAC) también tiene la opción de administrar los dispositivos sin implementar un agente. Al hacerlo, la información del dispositivo se guarda en la base de datos y se configura el BMC del dispositivo para que pueda utilizar las funciones de administración permitidas por el hardware de administración fuera de banda del dispositivo.

Para trasladar los dispositivos detectados a la lista Mis dispositivos

1. En la vista **Detección de dispositivos**, haga clic en el dispositivo que desee mover a la lista **Mis dispositivos**. Para seleccionar varios dispositivos, pulse MAYÚS+clic o CTRL+clic.
2. Haga clic en el botón **Destino**. Los dispositivos seleccionados se muestran en la ficha **Lista de destino**.
3. Haga clic en la ficha **Administrar**.
4. Seleccione **Mover dispositivos de destino**.

5. Si los dispositivos se pueden administrar fuera de banda y no desea implementar un agente de administración en ellos, seleccione **Administrar dispositivos sin agente que están fuera de banda**.
6. Haga clic en **Mover**.

Se eliminan los dispositivos de la lista de dispositivos no administrados y figuran en la lista **Mis dispositivos**.

Si ha seleccionado la opción de administración fuera de banda, puede ver el estado del proceso de traslado al hacer clic en la ficha **Estado del traslado** en el panel inferior. Cualquier error que se produzca en la configuración se indica aquí. Para mover un dispositivo habilitado para IPMI a la lista **Mis dispositivos**, debe haber proporcionado las credenciales de BMC debidas en la utilidad Configuración de servicios para permitir que el servidor central se autentique de forma satisfactoria en el dispositivo.

Cuando se mueve un módulo de administración de chasis (CMM) a la lista **Mis dispositivos**, se muestra en la lista **Todos los dispositivos** y también como grupo en la lista **Grupos públicos**. Los detalles del grupo muestran el CMM y una lista de compartimientos disponibles en el chasis con los nombres de los servidores de hoja en los compartimientos. Los servidores de hoja también se detectan y administran como servidores individuales.

Detección de dispositivos Intel* AMT

System Manager incluye una opción para detectar dispositivos configurados con la tecnología Intel* Active Management (Intel* AMT) versión 1. Los dispositivos se pueden detectar como dispositivos Intel AMT solamente después que ha ido a la pantalla de configuración de Intel AMT en el dispositivo y ha cambiado la contraseña predeterminada del fabricante a una contraseña segura. (Consulte la documentación del fabricante para la información sobre el acceso a la Pantalla de configuración de Intel AMT). Si aún no hecho esto, se detectarán los dispositivos pero no se identificarán los dispositivos Intel AMT y no se podrá ver la misma información de inventario, como se podría en otra situación.

Los dispositivos con Intel AMT versión 2 no se detectan con este proceso. Después de escribir las identificaciones de incorporación en la pantalla de configuración de Intel AMT con la dirección IP del servidor central, el dispositivo se detecta automáticamente. Consulte Configuración de dispositivos Intel AMT para obtener detalles sobre el funcionamiento con la versión 2.

Detectar dispositivos Intel AMT

1. En el panel de exploración izquierdo, haga clic en **Detección de dispositivos**.
2. Haga clic en **Nuevo** para crear una nueva configuración e ingrese un nombre para la configuración. O haga clic en una configuración existente y en **Editar** para modificarla.
3. Compruebe la opción **Detectar dispositivos Intel AMT**.
4. Ingrese las direcciones IP de inicio y fin para rastrear un intervalo de direcciones e ingrese una máscara de subred.
5. Haga clic en **Agregar** y luego en **Aceptar**.
6. Seleccione una configuración y haga clic en **Programar**. Compruebe las opciones de programación o haga clic en **Iniciar ahora** y en **Guardar**.
7. Para ver el progreso del rastreo, haga clic en la ficha **Tareas de detección**.

Los dispositivos configurados para Intel AMT se muestran en una carpeta etiquetada como **Intel AMT**. Desde esta carpeta puede seleccionar el dispositivo y moverlo a la lista de dispositivos administrados.

Para agregar el dispositivo a la base de datos central de inventario a fin de administrarlo, el nombre de usuario y la contraseña del dispositivo deben coincidir con el nombre de usuario y la contraseña almacenados en la utilidad Configuración de servicios, lo que permite que System Manager realice la autenticación en el dispositivo. Cuando guarda la configuración de la contraseña en la utilidad Configuración de servicios, ésta almacena la información en la base de datos central para que System Manager realice la autenticación en los dispositivos Intel AMT.

Si tiene dispositivos Intel AMT con diferentes credenciales, necesitará comprobar que las credenciales para cada dispositivo coincidan con la utilidad Configuración de servicios antes de administrarlos.

Cuando el dispositivo Intel AMT se detecta y se mueve a la lista **Mis dispositivos**, se incorpora de forma automática utilizando el modo que seleccionó mediante la utilidad Configuración de servicios. El modo Pequeños negocios proporciona una administración básica sin los servicios de infraestructura de red y no es seguro, mientras que el modo Empresa está diseñado para grandes empresas y proporciona seguridad de acuerdo con los servicios de red, tales como DHCP, DNS y un servicio de autoridad de certificación TLS.

Si el servidor central está utilizando el servidor proxy, éste debe ser compatible con Digest Access Authentication para poder detectar los dispositivos Intel AMT.

Para configurar la contraseña de Intel AMT

1. Haga clic en **Inicio | Todos los programas | LANDesk | Configuración de servicios**. Haga clic en la ficha **Configuración de Intel AMT**.
2. Escriba el nombre de usuario actual y la contraseña. Los mismos deben coincidir el nombre de usuario y contraseña configurados en la pantalla de configuración de Intel AMT (disponible en la utilidad de configuración de BIOS del equipo) a fin de administrar los dispositivos Intel AMT.
3. Para cambiar el nombre de usuario y contraseña, complete la sección **Nueva contraseña Intel ATM**.
4. Seleccione el modo (**Pequeños negocios** o **Empresa**) que desee utilizar para incorporar dispositivos cuando los agrega a la base de datos central a fin de administrarlos.
5. Haga clic en **Aceptar**. Este cambio se llevará a cabo cuando se ejecute la configuración del cliente.

Para mover dispositivos AMT detectados en la lista de dispositivos administrados

1. Haga clic en uno o más nombres de dispositivo en la lista de dispositivos no administrados.
2. Haga clic en el botón **Destino** de la barra de herramientas.
3. Haga clic en el botón **Administrar** en el panel inferior, seleccione **Mover dispositivos de destino** y haga clic en **Mover**.

   Si todos los dispositivos que desea administrar están visibles en la lista, puede seleccionarlos. Para ello, haga clic en el botón **Administrar** en el panel inferior, seleccione **Mover dispositivos seleccionados** y haga clic en **Mover**.

El dispositivo se elimina de la lista de dispositivos no administrados y aparece en la lista de **Todos los dispositivos**. Observe que cuando mueve los dispositivos a la lista **Mis dispositivos**, la incorporación de Intel AMT se ejecuta en un proceso de segundo plano independiente. Mientras esto ocurre, puede continuar con otras tareas administrativas y de detección.

Para obtener más información sobre la administración de dispositivos Intel AMT, consulte Administración de dispositivos Intel* AMT y Compatibilidad con Intel* AMT.

Instalación y configuración de un agente de dispositivo

Introducción a la instalación y configuración del agente

Para administrar totalmente los dispositivos con la consola, debe instalar los agentes de administración en ellos. Puede elegir la instalación de la configuración de agente predeterminada (la cual instala todos los agentes del producto) o personalizar su propia configuración de agente para instalarla en los dispositivos. La instalación de System Manager no instala agentes en el servidor central automáticamente; también debe instalar los agentes en el servidor central y luego reiniciar éste de forma manual. La configuración de agente debe incluir el agente monitor para recibir alertas de integridad.

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

- Implementación de agentes. 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.
- Instalación de agentes con un paquete de instalación. 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.
- Instalación del agente a petición. Asigne una unidad al recurso compartido ldlogon del servidor central (//*nombre de servidor*/ldlogon) y ejecute SERVERCONFIG.EXE.
- De forma manual en un dispositivo con una unidad USB portátil (consulte Instalación de agentes con un paquete de instalación)

Otro recurso de instalación y configuración de agentes se encuentra en el capítulo Detección de dispositivos en el *Manual del usuario*.

Nota: Para definir una configuración de dispositivo como predeterminada, selecciónela en la página **Configuración del agente** y haga clic en **Establecer como predeterminada**. Las configuraciones de IPMI BMC solamente, no pueden ser la configuración predeterminada. Las configuraciones predeterminadas no pueden eliminarse.

En los sistemas Windows, las opciones de puerto siguientes requieren la configuración manual del servidor de seguridad para que el producto funcione a plenitud. Para cambiar estas opciones, vaya al servidor de seguridad de Windows a través del Panel de control de Windows.

Servidores administrados:

- Archivos e impresoras compartidas: TCP 139, 445; UDP 137,138 (sin esto, el envío no funcionará)
- Distribución de software: TCP 9595 (sin esto, el envío no funcionará)
- Avanzada: ICMP - "Permitir las solicitudes de eco entrantes" (si esto no se encuentra habilitado, no puede detectarse).

Servidor:

- Inventario: 5007
- Control remoto: 9535

Para conseguirlo, haga clic en **Inicio** | **Panel de control** | **Seguridad**.

Actualización de agentes existentes

Se pueden instalar configuraciones de agente de forma automática en los dispositivos, aunque todavía no estén presentes los agentes de administración estándar o de control remoto. Consulte Configuración de servicios y credenciales en el *Manual del usuario* para obtener información sobre la configuración de credenciales.

Una vez que ha instalado un paquete de agente, se elimina la instalación anterior y se instala una nueva. No puede desinstalar un agente al crear un nuevo paquete que no incluya el agente que desea eliminar.

Desinstalación de agentes

Si necesita desinstalar agentes de servidores, siga este procedimiento.

Advertencia: De forma predeterminada, Uninstallwinclient.exe reinicia el dispositivo tras la desinstalación de los agentes, a menos que utilice el conmutador **/noreboot** en la línea de comandos. Es necesario reiniciar el sistema para que se complete la desinstalación. Si se realiza el reinicio, el servidor se reinicia sin previo aviso y se fuerza el cierre de todas las demás aplicaciones. El conmutador /noreboot permite que el servidor continúe sin el reinicio.

Para desinstalar agentes de un servidor

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

   ```
   uninstallwinclient.exe /noreboot
   ```

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

También puede seleccionar **Inicio** > **Ejecutar** >***nombre de servidor central*\ldmain\uninstallwinclient.exe /noreboot**.

Para desinstalar agentes de un servidor Linux

1. Copie el archivo linuxuninstall.tar.gz a un directorio temporal del dispositivo Linux. Lo puede encontrar en la carpeta compartida ManagementSuite del servidor central.

   Es probable que no se haya instalado o configurado Samba en el dispositivo Linux, de modo que no podrá copiarlo directamente; puede obtenerlo mediante una operación pscp en el servidor central y copiarlo en la carpeta ldlogon o en un medio extraíble.
2. Desde el símbolo de sistema del shell (en el equipo Linux), descomprima este archivo utilizando tar y las opciones x, z y f.

   ```
   tar -xzf linuxuninstall.tar.gz
   ```
3. Un vez que haya descomprimido el archivo, desde el símbolo de sistema del shell, ejecute la secuencia de comandos de linuxuninstall desde el directorio actual:

   ```
   ./linuxuninstall.sh
   ```

Configuración de agentes

Para administrar totalmente los dispositivos con la consola, debe instalar los agentes de administración en ellos. La instalación de System Manager no instala agentes en el servidor central automáticamente; también debe instalar los agentes en el servidor central y luego reiniciar éste de forma manual. Ya sea que utilice una de las configuraciones predeterminadas de agentes o que cree una configuración de agente en la consola, podrá instalarla en los dispositivos Windows o Linux de uno de los tres modos siguientes:

- Cree una configuración de agente, 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.
- Cree un paquete de instalación 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. Si desea más información, consulte "Instalación de agentes con un paquete de instalación".
- En un dispositivo Windows, asigne una unidad al recurso compartido ldlogon del servidor central (*miservidor*\ldlogon) y ejecute SERVERCONFIG.EXE.

Para crear una configuración de agente

1. En el panel de exploración izquierdo, haga clic en **Configuración del Agente**.
2. Haga clic en **Nuevo**.
3. Escriba un nombre para la configuración nueva en el cuadro **Nombre de la configuración**.

   Especifique un nombre que describa la configuración en la cual está trabajando. Puede ser un nombre de configuración existente o uno nuevo.

4. Seleccione la plataforma de la configuración.

5. Seleccione el tipo de instalación de la configuración (seleccionada por el usuario o IPMI BMC solamente). Seleccione **IPMI BMC solamente** bajo **Configuración** para configurar el controlador de administración de placa base (BMC) en dispositivos habilitados para IPMI (véase la nota del paso 9 más abajo).

   La configuración IPMI BMC solamente configura el BMC para el acceso fuera de banda, realiza un rastreo de inventario completo y se elimina a sí mismo. Las configuraciones de IPMI BMC solamente, no pueden ser la configuración predeterminada. Al crear una configuración IPMI BMC solamente, observe que no están disponibles la mayoría de las opciones de edición descritas en los pasos siguientes.

6. Seleccione la configuración que ha creado y haga clic en **Editar**.

   En las fichas, algunas opciones están atenuadas debido a que no se pueden configurar en la configuración que ha elegido.
7. En la ficha **Agente**, seleccione los agentes que desee implementar.

   - **Todos:** instala todos los agentes en el dispositivo seleccionado.
   - **Agente de administración estándar:** forma la base de la comunicación entre los dispositivos y el servidor central. Este agente es requerido (excepto en las configuraciones BMC solamente). La mayoría de los procesos de este agente son a petición.
   - **Actualizaciones de software:** instala el rastreador de actualizaciones de software. Tras instalar este agente podrá configurar la forma en que se ejecuta el rastreador. Éste no es un agente a petición.
   - **Monitoreo:** instala el agente de monitoreo en el servidor seleccionado. El agente de monitoreo permite diversos tipos de monitoreo, tales como el monitoreo ASIC directo, IPMI en banda, IPMI fuera de banda y CIM. Éste no es un agente a petición.
   - **Consola de Active System:** instala el agente que permite el acceso a la consola de Active System desde System Manager a través de la interfaz o de los menús. Este agente solamente se admite en los dispositivos con motherboards Intel.

8. En los cuadros **Tipo de sistema de configuración**, seleccione el tipo. Si se encuentra atenuada esta opción, quiere decir que ya ha seleccionado el tipo.

9. Seleccione la opción **Reiniciar**.

   El reinicio manual significa que los dispositivos no se reinician tras la instalación. No es necesario el reinicio del dispositivo tras la configuración del agente. Debe reiniciar el dispositivo de forma manual.

   El reinicio, cuando es necesario, causa el reinicio para las actualizaciones de software si los archivos actualizados se encuentran bloqueados.

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 los rastreos 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 los rastreos 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. Puede ejecutar el rastreador de forma manual desde el servidor administrado, para ello ejecútelo en Inicio | Programas | LANDesk Management | Rastreo de inventario. En Linux, deberá haber iniciado sesión como raíz y ejecutar lo siguiente desde la línea de comando: `/usr/LANDesk/ldms/ldiscan -ntt`

    - **Ejecutar siempre al iniciar:** ejecuta el rastreador de inventario al iniciar el dispositivo. Si está creando una configuración HP-UX, este botón estará atenuado debido a que el rastreador de HP-UX se ha definido para ejecutarse como tarea cron, la cual se ejecutará ya sea cada día, cada semana o cada mes. Esto no puede modificarse.
    - **Hora de inicio:** especifique un intervalo de tiempo en el cual se puede ejecutar 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.
    - **Repetir cada:** escriba un número que represente el incremento (como 1, 2 ó 3), y la medida (minutos, horas o días).
    - **Restricciones:** limita los días y las horas disponibles en los cuales se puede ejecutar el rastreador de inventario. Haga clic en **Hora**, **Día de la semana** o **Día del mes** y escriba parámetros inclusivos. Por ejemplo, escriba 10 en **Día del mes** y 1:00 AM y 3:00 AM en **Hora** para permitir que el rastreador de inventario se ejecute el día 10 de cada mes entre las horas de 1:00 AM y 3:00 AM.

11. En la ficha **Actualizaciones de software**, defina los días y las horas en que desea ejecutar el rastreador de actualizaciones de software. El rastreador se ejecuta automáticamente, sin necesidad de una tarea programada.
    - **Ejecutar siempre al iniciar:** ejecuta el rastreador de actualizaciones de software al iniciar el dispositivo.
    - **Hora de inicio:** especifique un intervalo de tiempo en el cual se puede ejecutar el rastreador. Si un dispositivo inicia una sesión durante el rango de hora, el rastreo de actualizaciones de software se ejecuta automáticamente. Si el dispositivo ya ha iniciado una sesión, el rastreo de actualizaciones de software se inicia automáticamente una vez que se llega a la hora inicial. Esta opción resulta útil si desea que los rastreos se ejecuten por etapas en los dispositivos a fin de que no envíen los rastreos al mismo tiempo.
    - **Repetir cada:** escriba un número que represente el incremento (como 1, 2 ó 3), y la medida (minutos, horas o días).

- **Restricciones:** limita los días y las horas disponibles en los cuales se puede ejecutar el rastreador de actualizaciones de software. Haga clic en **Hora**, **Día de la semana** o **Día del mes** y escriba parámetros inclusivos. Por ejemplo, escriba 10 en **Día del mes** y 1:00 AM y 3:00 AM en **Hora** para permitir que el rastreador de inventario se ejecute el día 10 de cada mes entre las horas de 1:00 AM y 3:00 AM.

12. 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.
13. Haga clic en **Guardar cambios** para guardar la información en la base de datos. Haga clic en **Guardar como archivo** para guardar la configuración como paquete de distribución.

Nota: Para definir una configuración de agente como predeterminada, selecciónela en la página **Configuraciones del Agente** y haga clic en **Establecer como predeterminada**. Las configuraciones predeterminadas no pueden eliminarse.

Para programar una tarea de configuración de agente

1. En el panel de exploración izquierdo, haga clic en **Configuración del Agente**.
2. Haga clic en la configuración de agente y luego en **Programar tarea**.
3. Edite la lista de dispositivos de destino y la programación de la tarea.
4. Haga clic en **Guardar**.

Cuando hace clic en **Programar tarea**, se crea una tarea (no tiene dispositivos de destino y no se encuentra programada). Si cancela esta tarea de configuración de agente sin guardarla, tenga en cuenta que ya se ha creado y que figurará en la lista **Tarea** con un estado de No programada. Puede eliminarla de la lista **Mis tareas**.

Después que se completa la tarea de configuración de agente, debe reiniciar el dispositivo para ver los detalles sobre el dispositivo en la consola (consulte Visualización de la consola de información del servidor). Se requiere el reinicio cuando instala el agente en el servidor central, al igual que en los dispositivos administrados. El proceso de configuración del agente permite elegir en qué momento se realiza el reinicio para que no interfiera con el uso del servidor.

Implementación de agentes en dispositivos administrados

Una vez detectados los dispositivos, se pueden implementar los agentes en ellos. Sólo se pueden implementar agentes en dispositivos compatibles con Windows, Linux y HP-UX. Debe tener derechos de administrador para desplegar agentes en los dispositivos de Windows y el privilegio de raíz para configurar los servicios de Linux y HP-UX.

Los agentes se pueden implementar en dispositivos no administrados del siguiente modo:

- Implementaciones basadas en instalación forzada utilizando las tareas de detección y una cuenta administrativa de dominio configurada para el servicio programador, que procesa tareas de detección. La cuenta administrativa de dominio le otorga a los servicios de programación los derechos que necesita para instalar los agentes de servidor. Esto funciona con la familia de servidores Windows NT.
- Implementaciones automáticas usando el agente de administración estándar. Si los servidores tienen el agente de administración estándar, el cual se utiliza en varios productos de LANDesk Software, puede implementarlos sin necesidad de una cuenta de administración de dominio.

Cuando se hace implementación de dispositivos detectados, utilice la opción **Filtrado por** del árbol **No administrado**. Puede filtrar por dirección IP para dispositivos aislados.

En los sistemas Windows, las opciones de puerto siguientes requieren la configuración manual del servidor de seguridad para que el producto funcione a plenitud. Para cambiar estas opciones, vaya al servidor de seguridad de Windows a través del Panel de control de Windows.

Servidores administrados:

- Archivos e impresoras compartidas: TCP 139, 445; UDP 137,138 (sin esto, la instalación automática no funcionará)
- Distribución de software: TCP 9594, 9595 (sin esto, la instalación automática no funcionará)
- Opciones avanzadas - ICMP: "Permitir las solicitudes de eco entrantes" (si esto no se encuentra habilitado, no puede detectarse).

Servidor:

- Inventario: 5007
- Control remoto: 9535

Configuración de credenciales de autenticación de dispositivo

Los dispositivos no administrados que tienen instalados el agente de administración estándar no necesitan credenciales de autenticación para la implementación de los agentes. Para instalar los agentes en los servidores con SO Windows que no tienen el agente de administración estándar, deberá especificar las credenciales que utilizará el servicio programador del dispositivo de consola para obtener los derechos requeridos.

Para instalar agentes de dispositivo en dispositivos no administrados, el servicio programador debe tener la capacidad de establecer conexión con dispositivos mediante una cuenta administrativa. La cuenta predeterminada que utiliza el servicio programador es LocalSystem. Por lo general, las credenciales de LocalSystem funcionan en dispositivos que no se encuentran en un dominio.

Si los dispositivos están en un dominio, especifique una cuenta de administrador de dominio. Si se está configurando dispositivos no administrados en dominios múltiples, se los debe configurar en un sólo dominio a la vez, debido a que el servicio programador autentica con un conjunto de credenciales, y cada dominio requerirá una cuenta de administrador de dominio diferente.

El servidor central incluye una utilidad de configuración de servicios, que puede utilizar para personalizar las opciones de inventario. Esta utilidad sólo puede ejecutarse en el servidor central.

Para configurar las credenciales de inicio de sesión del servicio programador

1. Iniciar la utilidad de configuración de servicios, en el servidor central al hacer clic en **Inicio | Archivos de programa | LANDesk | Configurar servicios**.
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 clientes, normalmente una cuenta de administrador de dominio.

Instalación de agentes

Una vez que haya creado una configuración de agente en la consola, necesita instalarla en los dispositivos. La instalación de System Manager no instala agentes en el servidor central automáticamente; también debe instalar los agentes en el servidor central y luego reiniciar éste de forma manual.

Los paquetes de agentes de clientes son un solo archivo ejecutable de extracción automática. De forma predeterminada, se almacenan en la carpeta \Archivos de programa\LANDesk\ManagementSuite\ldlogon del servidor central. La ejecución del ejecutable instala los agentes de clientes silenciosamente, sin necesidad de ninguna interacción del usuario. No se requiere un navegador para la instalación satisfactoria de agentes en los dispositivos de destino.

Instalación de agentes

Para actualizar los agentes, cree una configuración de cliente nueva y distribúyala a partir de la consola, o bien, instale los agentes directamente en los dispositivos no administrados.

Una vez que ha instalado un paquete de agentes de cliente, al instalar otros paquetes de agentes de cliente se eliminan todos los agentes y se instalan los que se han seleccionado de forma específica. No puede desinstalar un agente al crear un nuevo paquete de cliente que no incluya el agente que desea eliminar.

Desinstalación de agentes

Si necesita desinstalar agentes de los dispositivos, consulte "Introducción a la instalación y configuración del agente".

Instalación de agentes con un paquete de instalación

Uno de los métodos de instalación de agentes es a través de un paquete de agentes de dispositivo de extracción automática. Esto permite que copie el archivo en una unidad de CD o

USB para instalar los agentes de forma manual. Para crear los paquetes, haga clic en **Guardar como archivo** en la parte inferior del cuadro de diálogo **Configuración**.

1. Haga clic en **Configuración de agentes** y haga doble clic en el nombre de una configuración.
2. En el cuadro de diálogo **Configuración de agentes**, haga clic en **Guardar como archivo** y luego en **Cerrar**.

Al hacer clic en **Guardar como archivo** se crea un paquete ejecutable de extracción automática con un nombre de archivo que coincide con el nombre especificado de la configuración. Podría tomar unos minutos para que el paquete esté disponible en la carpeta \Archivos de programa\LANDesk\ManagementSuite\ldlogon\ConfigPackages del servidor central.

La ejecución del ejecutable instala los agentes, sin necesidad de ninguna interacción del usuario. Debe iniciar una sesión con privilegios administrativos.

Si sus usuarios no se pueden registrar con los privilegios administrativos para instalar el paquete, puede implementar los paquetes usando correo electrónico, descargas desde la Web, secuencias de comando de inicio de sesión, o desde un recurso compartido.

Instalación de agentes a petición

Esta sección incluye los detalles de implementación de agentes a partir de una línea de comandos. Es posible controlar los componentes que se instalan en los dispositivos mediante los parámetros de línea de comandos SERVERCONFIG.EXE. Puede ejecutar el archivo SERVERCONFIG.EXE en modo independiente. Se encuentra en el recurso compartido *http:**servidorcentral**LDLogon*, el cual se puede leer en cualquier servidor Windows.

SERVERCONFIG.EXE utiliza SERVERCONFIG.INI para configurar dispositivos.

Introducción a SERVERCONFIG.EXE

SERVERCONFIG.EXE configura los servidores de la familia Windows NT para su administración mediante el proceso siguiente:

1. SERVERCONFIG determina si el equipo se ha configurado con un agente de administración con anterioridad . Si es así, SERVERCONFIG elimina todos los componentes y reinstala los componentes seleccionados.
2. SERVERCONFIG carga el archivo de inicialización correcto (SERVERCONFIG.INI) y ejecuta las instrucciones contenidas en él.

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

Parámetro	Descripción
/I	Componentes que incluir (deben incluirse las comillas): "Common Base Agent"

Parámetro	Descripción
	"Inventory Scanner" "Alerting" "Vulnerability Scanner" "Server Monitor" Todas ellas se pueden combinar en la misma línea de comandos. Por ejemplo: `SERVERCONFIG.EXE /I="Alerting" /I="Vulnerability Scanner"`
/L o /Log=	Ruta a los archivos de registro CFG_YES y CFG_NO en los que se registran los servidores configurados y no configurados
/LOGON	Ejecuta comandos con el prefijo [LOGON]
/N o /NOUI	No muestra la interfaz de usuario
/NOREBOOT	No reinicia el servidor una vez que ha finalizado (opción predeterminada)
/REBOOT	Reinicia tras la ejecución
/X=	Componentes que desea excluir. Por ejemplo: `SERVERCONFIG.EXE /X=SD`
/CONFIG= /[CONFIG]=	Especifica un archivo de configuración de servidor 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 NT.
/? o /H	Muestra el menú de ayuda

Creación de una configuración de agente

Utilice la **Configuración de agente** para crear y actualizar las configuraciones de agentes de servidor (como cuáles agentes se instalan o administran). Se pueden crear diferentes configuraciones para las necesidades específicas de los grupos. Por ejemplo, se puede crear una configuración para servidores Web y otra para los servidores de aplicación.

Para instalar automáticamente una configuración en un servidor, debe realizar lo siguiente:

- **Crear una configuración de agente**: Establecer las configuraciones específicas para los servidores.
- **Programar la configuración de agente**: Instale automáticamente la configuración en los servidores o, desde el servidor, ejecute SERVERCONFIG.EXE desde el recurso compartido LDLogon del servidor central.

Para crear una configuración de agente

1. En la consola, haga clic en **Configuración del Agente**.
2. Haga clic en el botón **Nuevo** de la barra de herramientas.
3. Ingrese un **Nombre de configuración** y seleccione el sistema operativo, luego haga clic en **Aceptar**.
4. Haga clic en el nuevo nombre de la configuración y luego en **Editar**.
5. Seleccione los agentes que desea implementar.
6. Utilice las fichas en la parte superior del cuadro de diálogo para navegar a las opciones relacionadas con los componentes seleccionados. Personalice las opciones que ha seleccionado, como sea necesario.
7. Haga clic en **Guardar cambios** para cerrar el cuadro de diálogo.
8. Si desea que la configuración sea la predeterminada, haga clic en **Establecer como predeterminada**.

Obtención de una configuración de agente Linux

Para obtener una configuración de agente Linux

1. Cree un directorio temporal en el dispositivo Linux (por ejemplo, /tmp/ldcfg) y copie lo siguiente en dicho directorio:
    1. Todos los archivos del directorio LDLOGON\unix\linux.
    2. Copie la secuencia de comandos 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 mencionados en el archivo <*nombre de configuración*>.ini en el directorio temporal. Para identificar estos archivos, el archivo .INI busque "FILE*xx*", donde *xx* es un número. La mayoría de las entradas que se encuentran ya se habrán copiado en el cliente durante el paso 1, pero encontrará archivos .XML que deben copiarse. Los nombres de archivo 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.xml a masterconfig.ruleset.monitor.xml

2. Si el dispositivo tiene IPMI y un 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: Tenga en cuenta que si instala un agente automáticamente o a petición en un dispositivo Linux, debe ejecutar

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

para limpiarlo y luego volver a realizar la instalación automática o a petición, el archivo con el GUID es el único que queda en el dispositivo 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.

Creación de un paquete independiente de configuración de agente

Generalmente la utilidad de configuración del agente, SERVERCONFIG.EXE, se encarga de la configuración de los agentes de los dispositivos administrados. Si desea, puede hacer que una ventana **Configuración de agentes** cree un archivo de ejecución automática que instale la configuración de agente en el servidor donde se ejecuta. Esto resulta útil cuando se desea instalar agentes desde una unidad de CD o de USB portátil.

Instalación automática de configuraciones de agentes en los dispositivos

Para instalar automáticamente una configuración de agente

1. En la consola, seleccione los dispositivos en los que desea implementar el agente, y haga clic en **Destino**.
2. En el panel de exploración izquierdo, haga clic en **Configuración del Agente**.
3. Haga clic en el botón derecho sobre la configuración de agente que desee instalar automáticamente y, acto seguido, haga clic en **Programar tarea.**
4. Haga clic en **Dispositivos de destino** en el cuadro de diálogo **Programar propiedades de tareas**, luego haga clic en **Agregar la Lista de Destino**.
5. Haga clic en **Programar tarea**:
6. Especifique la hora de implementación del agente, y luego haga clic en **Guardar**.

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. 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 **Configurar agentes**, necesita un RPM adicional: sysstat. Si desea una lista completa de los RPM requeridos por el producto, consulte el *Manual de instalación e implementación de System Manager*

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.

Implementación de agentes Linux

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 **Detección de 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 haya encontrado los servidores Linux que desea 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 de 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 del Agente**, haga clic en **Nuevo**.
2. Escriba el nombre de la configuración, haga clic en **HP-UX** o en **Linux Server Edition**, seleccione el tipo de instalación (servidor o escritorio) 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. 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.
7. Haga clic en **Guardar cambios**.

Para implementar la configuración de agente, selecciónelo en **Configuraciones del agente** y haga clic en **Programar tarea**. Configure la tarea y siga el progreso de la tarea en **Tareas de configuración**.

Nota: No recibirá información de estado del dispositivo 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 dispositivo Linux (por ejemplo, /tmp/ldcfg) y copie lo siguiente en dicho directorio:
    - Todos los archivos del directorio LDLOGON\unix\linux.
    - La secuencia de comandos de shell que tiene el nombre de la configuración (<*nombre de configuración*>.sh).
    - El archivo *.0 que tiene el nombre de la configuración. El asterisco (*) representa ocho caracteres (0-9, a-f).
    - Todos los archivos mencionados en el archivo <*nombre de configuración*>.ini. Para identificar estos archivos, busque el archivo .INI de "FILE*xx*", donde *xx* es un número. La mayoría de las entradas que se encuentran ya se habrán copiado en el cliente durante el paso 1, pero encontrará archivos .XML que deben copiarse. Los nombres de archivo 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.xml a masterconfig.ruleset.monitor.xml

2. Si el dispositivo tiene IPMI y un BMC (con el monitoreo incluido en la instalación), escriba la línea de comandos siguiente:

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

3. En calidad de raíz, ejecute la secuencia de comandos de shell de la configuración con la ruta completa siguiente:

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

4. Elimine el directorio temporal y todo su contenido.

Nota: Tenga en cuenta que si instala un agente automáticamente o a petición en un dispositivo Linux, debe ejecutar

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

para limpiarlo y luego volver a realizar la instalación automática o a petición, el archivo con el GUID es el único que queda en el dispositivo 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.

Parámetros de la línea de comandos del rastreador de inventario

El rastreador de inventario, ldiscan, presenta varios parámetros de línea de comandos que especifican su modo de ejecución. Consulte "ldiscan -h" o "man ldiscan" para obtener una descripción detallada de cada uno de ellos. Cada opción puede estar precedida de '-' o '/'.

Parámetro	Descripción
-d=Dir	Inicia el rastreo del software en el directorio Dir en lugar de la raíz. De forma predeterminada, la exploración comienza en el directorio raíz.
-f	Fuerza un rastreo de software. Si no especifica -f, el rastreador realiza la exploración de software en el intervalo de días (de forma predeterminada, todos los días) especificado en la consola en **Configurar | Servicios | Inventario | Configuración del rastreador**.
-f-	Inhabilita la exploración de software.
-i=nombredeconfiguración	Especifica el nombre de archivo de configuración. De forma

Parámetro	Descripción
	predeterminada es /etc/ldappl.conf.
-ntt=dirección:puerto	Nombre de host o dirección IP del servidor central. El puerto es opcional.
-o=archivo	Escribe la información de inventario en el archivo de salida especificado.
-s=servidor	Especifica el servidor central. Este comando es opcional y solamente existe para la compatibilidad con versiones anteriores.
-stdout	Escribe la información de inventario en la salida estándar.
-v	Habilita los mensajes de estado detallados durante la exploración.
-h o -?	Muestra la pantalla de ayuda.

Ejemplos

Para que la salida de datos sea en forma de archivo de texto, escriba:

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

Para enviar datos al servidor central, escriba:

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

Archivos del rastreador de inventario de Linux

Archivo	Descripción
ldiscan	Archivo ejecutable que se ejecuta con parámetros de línea de comandos para indicar la acción que se desea realizar. Para ejecutar el rastreador, los usuarios deben disponer de los derechos necesarios para ejecutar el archivo. Existe una versión diferente de este archivo para cada una de las plataformas anteriores admitidas.
/etc/ldiscan.conf	Este archivo se encuentra siempre en /etc y contiene la información siguiente:

Archivo	Descripción
	• Id. único de inventario asignado • Última exploración de hardware • Última exploración de software Para ejecutar el rastreador, los usuarios deben disponer de atributos de lectura y escritura para este archivo. El Id. único en /etc/ldiscan.conf es un número único asignado a un equipo la primera vez que se ejecuta el rastreador de inventario. Este número se utiliza para identificar el equipo. Si este número se modifica, el servidor central lo tratará como un equipo diferente, lo que pueda dar lugar a una entrada duplicada en la base de datos. **Advertencia:** No modifique el número de Id. único ni quite el archivo ldiscan.conf una vez se haya creado.
/etc/ldappl.conf	Es en este archivo donde se personaliza la lista de ejecutables que el rastreador de inventario informará al realizar una exploración de software. El archivo incluye algunos ejemplos y tendrá que agregar entradas para los paquetes de software que utiliza. El criterio de búsqueda se basa en el nombre de archivo y en el tamaño de éste. Aunque este archivo se ubica normalmente en /etc, el rastreador puede utilizar un archivo alternativo haciendo uso del parámetro de línea de comandos -i=.
ldiscan.8	Página Man para ldiscan.

Integración de la consola

Una vez que un equipo Linux se ha explorado en la base de datos central, podrá:

- Realizar consultas sobre los atributos devueltos por el rastreo de inventario en Linux de la base de datos central.
- Utilizar las funciones de informe para generar informes que incluyan información recopilada por el rastreador de Linux. Por ejemplo, Linux aparecerá como un tipo de SO en el informe de resumen de sistemas operativos.
- Ver la información de inventario para los equipos Linux.

Las consultas del "Tiempo activo del sistema" se muestran en orden alfabético con resultados inesperados

Si desea realizar una consulta para determinar la cantidad de servidores que han estado en ejecución durante cierto número de días (por ejemplo, 10 días), realice una consulta del "Inicio del sistema" en lugar del "Tiempo activo del sistema". Las consultas sobre la actualización del sistema pueden dar lugar a resultados no esperados, ya que el tiempo de actividad del sistema no es más que una cadena con formato "x" días, "y" horas, "z" minutos y "j" segundos. La clasificación tiene lugar alfabéticamente y no en intervalos de tiempo.

La ruta a los archivos de configuración mencionados en ldappl.conf no aparece en la consola Las entradas ConfFile de ldappl.conf deben incluir una ruta.

Monitoreo de dispositivos

Acerca de la supervisión

System Manager ofrece varios métodos para la supervisión de la integridad de los dispositivos. Las funciones de supervisión recopilan datos de diversas fuentes con el fin de ayudar a llevar un seguimiento de los distintos datos contenidos en los dispostivos, tales como:

- Niveles de uso
- Eventos de SO
- Procesos y servicios
- Desempeño histórico
- Sensores de hardware (ventiladores, voltajes, temperaturas, etc.)

Este capítulo incluye información sobre las distintas características que supervisan los dispositivos administrados:

- Instalación de un agente monitor en dispositivos y creación de reglamentos de monitoreo que se pueden implementar en los dispositivos
- Definición de contadores de desempeño en dispositivo y monitoreo de datos de desempeño
- Monitoreo de cambios de configuración con alertas cuando se producen los cambios
- Envío de ping a dispositivos para monitorear su conectividad, mediante la función **Monitor de dispositivos**

La función de alertas, que está relacionada, utiliza el agente monitor para iniciar las acciones de alerta, tales como el envío de mensajes de correo electrónico o de buscapersonas, el reinicio o apagado de un dispositivo o la adición de información al registro de alertas. Puede generar alertas a partir de cualquiera de los eventos de dispositivo que se supervisan. Si desea más información, consulte "Uso de las alertas".

Notas

- La comunicación al agente monitor se realiza mediante HTTP a través de TCP/IP en forma de solicitudes GET, POST o XML. Las respuestas a las solicitudes se incluyen en documentos de tabla XML o HTML.
- Para ejecutar y almacenar una consulta sobre el estado de la integridad de los dispositivos (Computer.Health.State), debe tener en cuenta que el estado se representa con un número en la base de datos. Los números corresponden a los estados siguientes: 4=Crítico, 3=Advertencia, 2=Normal, 1=Informativo, nulo o 0=desconocido.
- El monitoreo de hardware depende de las capacidades del hardware instalado en un dispositivo, así como en la configuración correcta del hardware. Por ejemplo, si un disco duro con capacidades de monitoreo S.M.A.R.T. se instala en un dispositivo, pero S.M.A.R.T.no se encuentra habilitado en la configuración del BIOS del dispositivo, o si el BIOS del dispositivo no es compatible con S.M.A.R.T., la información de monitoreo no se encontrará disponible.

- Si los informes de un equipo específico parecen haberse detenido, puede utilizar restartmon.exe en la carpeta LDCLIENT para reiniciar el compilador y todos los proveedores de monitoreo. Esta utilidad es para los equipos en los que se instaló la opción de informes y donde éstos se detuvieron. Utilice esta utilidad para reiniciar el compilador sin reiniciar el dispositivo.

Implementación del agente monitor en los dispositivos

System Manager ofrece un resumen inmediato de la integridad del dispositivo cuando se instala el agente monitor en el mismo. El agente monitor es uno de los seis agentes que se pueden instalar en los dispositivos administrados. Verifica el hardware y la configuración del dispositivo de forma regular y periódica, y refleja los cambios realizados en la integridad del sistema. Esto se muestra en el icono de estado de la lista **Mis dispositivos** y los detalles se muestran en las entradas del registro (en el resumen **Características** del dispositivo) y en los gráficos (en la página de resumen **Monitoreo** del dispositivo).

Por ejemplo, un dispositivo supervisado con una unidad de disco que se está llenando podría mostrar un icono de estado de advertencia si el disco se llena a un 90% de su capacidad y cambiar a un icono de estado crítico si se llena a un 95%. También puede recibir alertas para el mismo estado de unidad de disco si el dispositivo tiene un reglamento de alertas que incluya reglas para una alerta de espacio de disco.

Puede implementar el reglamento de monitoreo predeterminado en los dispositivos. O si lo prefiere, puede crear un reglamento personalizado que incluya solamente los elementos de integridad que le interesen.

Creación de un reglamento de supervisión

Puede elegir lo que se supervisa en un dispositivo mediante la creación de un reglamento de monitoreo, que define lo que el agente monitor verifica en el dispositivo. Puede implementar el reglamento a un dispositivo o a un grupo de dispositivos de destino. Por ejemplo, podría definir un reglamento para los servidores dedicados al almacenamiento y utilizar otro reglamento para los servidores Web.

El reglamento de monitoreo predeterminado incluye 16 elementos. Al crear un reglamento, puede activar o desactivar cualquiera de estos elementos, especificar la frecuencia con que se verifican y, para algunos elementos, definir umbrales de desempeño. También puede seleccionar los servicios que se ejecutan en los dispositivos que desee supervisar.

El proceso general para crear e implementar un reglamento de alertas es el siguiente:

1. Seleccione los dispositivos a los que desee implementar el reglamento y haga clic en **Destino** para agregarlos a la lista de **Dispositivos de destino**.
2. Cree o edite un reglamento de monitoreo. Tenga en cuenta que debe seleccionar la casilla de verificación para encender el monitoreo para cada suceso que desee que se monitoree en el reglamento. De forma predeterminada, no se monitorearán todos. Algunos sucesos como los servicios también requieren que seleccione cada servicio que desee monitorear. (Consulte los pasos detallados a continuación).

3. Implemente los reglamentos en los dispositivos destino. Si lo necesita, puede seleccionar como destino otros dispositivos antes de implementar el reglamento. (Consulte los pasos detallados a continuación).

Para crear un reglamento de monitoreo

1. En el panel de exploración izquierdo, haga clic en **Supervisión**.
2. Haga clic en **Nueva**, escriba un nombre en el campo y una descripción para la configuración y haga clic en **Aceptar**.
3. Seleccione la configuración en la columna izquierda.
4. En la lista de elementos, haga clic en el elemento que desee cambiar y haga clic en **Editar**.
5. Para desactivar el monitoreo del elemento, desmarque la casilla de verificación y haga clic en **Actualizar**.
6. Para cambiar la frecuencia con la cual se supervisa el elemento, seleccione **Segundos** o **Minutos** y especifique un número en el cuadro de texto.
7. Si corresponde, defina los porcentajes de umbral de los estados de advertencia y crítico.
8. Para los **Servicios** que se supervisan, seleccione el SO en la lista desplegable. Seleccione uno o más servicios que supervisar (utilice CTRL + clic para seleccionar más de uno) y haga clic en **>>** para agregar los servicios a la lista de la derecha.
9. Por cada elemento que modifique, haga clic en **Actualizar** para aplicar los cambios a la configuración. Si modifica un elemento y luego decide no cambiarlo, haga clic en **Revertir** para restaurar la configuración original.

Cuando edite los servicios en una configuración de monitoreo desde el servidor central, la lista **Servicios disponibles** muestra los servicios conocidos desde la base de datos de inventario. No se muestran servicios en el cuadro de la lista **Servicios disponibles** hasta que un agente de LANDesk se haya implementado en uno o más de los dispositivos y se haya recuperado un rastreo de inventario en el servidor central. Por ejemplo, para seleccionar cualquier servicio Linux de la lista, debe haber implementado un agente en un dispositivo Linux.

Para implementar un reglamento de monitoreo

1. En el panel de navegación izquierdo, haga clic en **Mis dispositivos** y luego en el grupo **Todos los dispositivos**.
2. Seleccione los dispositivos para los cuales desea implementar el reglamento de alerta y haga clic en **Destino** para colocar los dispositivos en la lista **Dispositivos de destino**.
3. En el panel de navegación izquierdo, haga clic en **Monitoreo** y luego en la ficha **Implementar reglamento**.
4. En el cuadro **Reglamentos de monitoreo**, seleccione el reglamento que desee implementar.
5. Haga clic en el vínculo para ver la lista de **Dispositivos de destino**. Para eliminar un dispositivo de la lista, haga clic con el botón secundario en él y haga clic en **Eliminar**. Para agregar dispositivos, debe agregarlos a la lista de destinos, tal como se describe en el paso 2.
6. Haga clic en **Implementar** para implementar el reglamento seleccionado en los dispositivos de destino.

Como parte del proceso de implementación, se crea una página XML con una lista de los reglamentos implementados y de los dispositivos en los que se implementaron. Este informe se guarda en el directorio LDLOGON del servidor central y se le asigna un nombre con un número

de secuencia asignado por la base de datos. Si desea consultar dicha página XML de forma aparte a la implementación del reglamento, haga clic en el botón **Generar XML** y luego en el vínculo para ver el archivo XML. La generación de un reglamento en XML también permite que se visualice el mismo en la lista de reglamentos disponibles de la **Configuración de agente**.

Apagado del servicio ModemView

El servicio ModemView es el servicio o controlador que supervisa las llamadas de módem (tanto entrantes como salientes) y que genera una alerta si se detecta uno. Este servicio utiliza alrededor de 10 Mb de memoria debido a que utiliza MFC. Es probable que no desee que esté en ejecución, particularmente si no existe un módem en el dispositivo.

Para apagar el servicio ModemView

1. En el dispositivo (ya sea de forma directa o a través del control remoto), haga clic en **Inicio** > **Panel de control** > **Herramientas administrativas** > **Servicios**.
2. Haga doble clic en **Servicio controlador de mensajes de LANDesk**.
3. En **Tipo de inicio**, seleccione **Manual** y haga clic en **Aceptar**.

También puede hacer clic en **Detener** en **Estado del servicio**.

Configuración de los Contadores de desempeño

System Manager permite seleccionar los elementos de rendimiento (contadores) que desee supervisar en un dispositivo administrado. Puede supervisar distintos tipos de elementos tales como componentes de hardware (tales como unidades, procesadores y memoria), componentes del SO (tales como procesos) o componentes de aplicaciones (tales como bytes por segundo transferidos por el servidor Web del sistema). Al seleccionar un contador de rendimiento también especifica la frecuencia de sondeo del elemento, al igual que los umbrales de rendimiento y la cantidad de infracciones que se permiten antes de generar una alerta.

Si se ha seleccionado un contador de rendimiento, podrá supervisar el rendimiento en la página **Monitoreo** mediante un gráfico con datos de tiempo real o de historial. Para obtener más información, consulte "Supervisión de rendimiento".

Para seleccionar un contador de rendimiento que se supervisará

1. En la vista **Mis dispositivos**, haga doble clic en el dispositivo que desee configurar. La consola de información del servidor se abre en otra ventana del explorador.
2. En el panel de exploración izquierdo, haga clic en **Supervisión**.
3. Haga clic en la ficha **Configuración del contador de rendimiento**.
4. En la columna **Objetos**, seleccione el objeto que desee supervisar.
5. En la columna **Instancias**, seleccione la instancia del objeto que desee supervisar, si corresponde.

6. En la columna **Contadores**, seleccione el contador específico que desee supervisar.

   Si el contador no figura en la lista, haga clic en **Volver a cargar contadores** para actualizar la lista con los nuevos objetos, instancias o contadores.

7. Especifique la frecuencia de sondeo (**Revisar cada** *n* **segundos**) y la cantidad de días que debe llevarse el historial de conteo.
8. En el cuadro de texto **Alertar si el contador se sale del intervalo**, especifique la cantidad de veces que el contador podrá sobrepasar los umbrales antes de generar una alerta.
9. Especifique los umbrales máximos y mínimos.
10. Haga clic en **Aplicar**.

Notas

- Los archivos de registro de rendimiento aumentan de tamaño con rapidez; el sondeo de un solo contador cada dos segundos agrega 2,5 MB de información al registro de rendimiento cada día.
- Se genera una alerta de precaución cuando un contador de rendimiento se encuentra por debajo de un umbral mínimo en un dispositivo de Windows o Linux. Cuando un contador supera el umbral máximo en un dispositivo Linux, se genera una alerta de precaución. Cuando un contador supera el umbral máximo en un dispositivo Windows, se genera una alerta crítica.
- Cuando se establecen los umbrales, tenga en cuenta que las alertas se generan sin importar si se cruza el umbral mínimo o máximo. En el caso de un factor como el espacio en el disco, podría desear que se alerte sólo si el dispositivo se encuentra ejecutándose muy bajo. En este caso, podría establecer el umbral máximo en un número lo suficientemente alto como para que no se le alerte si queda mucho espacio libre en el disco.
- La cifra seleccionada en **Alertar si el contador se sale del intervalo**, permite el enfoque en un aspecto si éste se convierte en un problema persistente o si se trata de un evento aislado. Por ejemplo, si supervisa los bytes enviados por un servidor Web, System Manager puede enviar una notificación si la cantidad de bytes por segundo es demasiado alta de forma constante. O bien, puede especificar una cifra baja como 1 ó 2 para recibir una alerta cada vez que las conexiones de FTP anónimas exceden una cierta cantidad de usuarios.

Supervisión de rendimiento

La página **Monitoreo** permite supervisar el rendimiento de varios objetos del sistema. Puede supervisar componentes de hardware específicos, tales como unidades, procesadores y memoria, o bien, componentes del SO, tales como procesos o los bytes por segundo transferidos por el servidor Web. La página **Monitoreo** incluye un gráfico que muestra datos de contadores en tiempo real o históricos.

A fin de supervisar un contador de rendimiento, primero debe seleccionar el contador, lo cual lo agrega a la lista de contadores supervisados. También se debe especificar la frecuencia de sondeo del elemento y definir los umbrales de rendimiento y la cantidad de infracciones que se permiten antes de que se genere una alerta. Consulte "Configuración de contadores de rendimiento" para obtener detalles sobre la selección de contadores.

Para visualizar un gráfico de rendimiento de un contador supervisado

1. En la vista **Mis dispositivos**, haga doble clic en el dispositivo que desee configurar. La consola de información del servidor se abre en otra ventana del explorador.
2. En el panel de exploración izquierdo, haga clic en **Monitoreo**
3. Haga clic en la ficha**Contadores de rendimiento activos**, si es necesario.
4. En la lista desplegable **Contadores**, seleccione el contador para el cual desea ver el gráfico de rendimiento.
5. Seleccione **Ver datos en tiempo real** para visualizar un gráfico del rendimiento en tiempo real.

   o bien

   Seleccione **Ver datos históricos** para visualizar un gráfico que muestre el rendimiento a través de un lapso de tiempo especificado (Llevar historial) al seleccionar el contador.

En el gráfico de rendimiento el eje horizontal representa el tiempo que ha pasado. El eje vertical representa las unidades que se miden, tales como bytes por segundo (por ejemplo, al supervisar transferencias de archivos), porcentaje (al supervisar el porcentaje de la CPU que se utiliza) o bytes disponibles (al supervisar el espacio en la unidad de disco duro). La altura de la línea no es una unidad fija. Ésta cambia de forma relativa a los extremos de los datos; para un contador, el eje vertical podría representar de 1 a 100 unidades y para otro podría representar de 1 a 500.000 unidades. Si los datos varían a través de un extremo amplio, los cambios mínimos podrían figurar como una línea plana.

Notas

- Al seleccionar otro contador se actualiza el gráfico y se restablecen las unidades de medida.
- Haga clic en **Actualizar**  para borrar y reiniciar el gráfico.
- Si recibe una alerta generada por un contador de la lista, haga clic con el botón secundario en el contador y haga clic en **Confirmación** para borrar la alerta.

Para detener la supervisión de un contador de rendimiento

1. En la vista **Mis dispositivos**, haga doble clic en el dispositivo que desee configurar. La consola de información del servidor se abre en otra ventana del explorador.
2. En el panel de exploración izquierdo, haga clic en **Supervisión**.
3. Haga clic en la ficha **Contadores de rendimiento activos**, si es necesario.
4. En **Contadores de rendimiento administrados**, haga clic con el botón secundario en el contador y haga clic en **Eliminar**.

Supervisión de los cambios de configuración

Este producto puede generar alertas si cambia la configuración del hardware o software de un dispositivo y el agente de monitoreo se encuentra instalado en el dispositivo. Los cambios podrían afectar el desempeño y la estabilidad del dispositivo o causar problemas en una

instalación estándar. Al supervisar las piezas vitales del dispositivo, este producto puede reducir el coste total de propiedad (TCO).

Los cambios de configuración de dispositivo que generan alertas son:

- **Instalación o desinstalación de aplicaciones:** Se pueden ver qué usuarios instalaron o eliminaron aplicaciones. Esto resulta útil al hacer un seguimiento de las licencias o de la productividad de los empleados. Se supervisan las aplicaciones que se han registrado en el área de Agregar o quitar programas del Panel de control de Windows. Se hace caso omiso a las demás aplicaciones. El nombre de la aplicación que se utiliza en Agregar o quitar programas de Windows es el nombre que aparece en el registro de notificaciones o en la ventana emergente de alerta.
- **Memoria agregada o quitada:** Este producto detecta y supervisa la cantidad y el tipo de memoria instalada. Si la configuración cambia, se genera una alerta.
- **Unidades de disco duro agregadas o quitadas:** Este producto detecta y monitorea la cantidad y el tamaño de las unidades instaladas en los dispositivos. Si la configuración cambia, se genera una alerta.
- **Procesadores agregados, quitados o modificados:** Este producto detecta y monitorea la cantidad, el tipo y la velocidad de los procesadores. Si la configuración cambia, se genera una alerta.
- **Tarjetas de red agregadas o quitadas:** Este producto detecta y monitorea la cantidad y el tipo de tarjetas de interfaz de red de los dispositivos y genera alertas si se cambia la configuración.

Para ver un registro de las alertas debidas a cambios de configuración, consulte el registro de alertas en la consola de información del servidor. Consulte "Visualización del registro de alertas", para obtener detalles.

Supervisión de la conectividad

En la mayoría de los casos, los dispositivos emiten una alerta ante situaciones críticas, como en el caso de un disco duro esté llegando a su límite de almacenamiento, o cuando se detiene el ventilador. Sin embargo, en determinadas situaciones, el dispositivo puede desconectarse antes de enviar la alerta. Por ejemplo, un interruptor o enrutador puede afectar el tráfico de la red, o el dispositivo puede sufrir una falla en el suministro eléctrico.

Para cubrir estas situaciones, este producto verificar los dispositivos en forma periódica para determinar si se encuentran disponibles en la red. Si el dispositivo no responde al ping, el estado de su integridad cambiará a crítico la próxima vez que actualice la lista **Mis dispositivos**.

Se debe configurar el monitor de dispositivos para que envíe un ping a los dispositivos de destino o a todos los que se encuentran en el grupo **Todos los dispositivos**.

Para configurar el monitor de dispositivos

1. En la lista **Mis dispositivos** se seleccionan los dispositivos que se desean supervisar. Se los puede seleccionar desde **Todos los dispositivos** o desde un grupo público o privado.
2. Haga clic en **Destino**.
3. En el panel inferior, haga clic en **Acciones** y luego en **Monitor de dispositivos**.

4. Para ver una lista de los dispositivos que se están monitoreando, haga clic en **Mostrar Dispositivos monitoreados**.
5. Ingrese los números de los minutos entre los barridos de ping y la cantidad de veces que el producto intentará comunicarse con el dispositivo.
6. Seleccione si se realizarán las acciones en los dispositivos de la lista de Dispositivos de destino o en todos los dispositivos del grupo **Todos los dispositivos**.
7. Para detener la supervisión en todos los dispositivos, seleccione **Nunca realizar ping en los dispositivos**.
8. Haga clic en **Aplicar**.

Únicamente se supervisa el último grupo de dispositivos de destino. Por ejemplo, si seleccionan los dispositivos de destino A y B, y se les aplica la supervisión de dispositivos, el servidor central solo enviará un ping a los dispositivos A y B. Si luego se selecciona el dispositivo C y el D, y se aplica la supervisión de dispositivos en aquellos dispositivos, sólo se supervisarán los dispositivos C y D, y los A y B dejarán de ser supervisados.

Configuración de alertas

Uso de las 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 realizar acciones específicas. Este capítulo explica el funcionamiento de las alertas.

¿Cómo se ven las alertas?

Este producto le notifica sobre problemas u otros eventos en los equipos mediante:

- La adición de información al registro
- El envío de un aviso por correo electrónico o de un mensaje a un buscapersonas
- La ejecución de un programa en el servidor central o en un dispositivo individual
- El envío de una captura SNMP a una consola de administración SNMP de la red
- El reinicio o apagado de un dispositivo

Tenga en cuenta que ciertas alertas asignadas a grupos de equipos pueden generar una gran cantidad de respuestas de forma simultánea. Por ejemplo, puede definir la alerta "Cambio de configuración de equipo" y asociarla con una acción de correo electrónico. Si se aplica una revisión de distribución de software a los equipos con esta configuración de alerta, se genera una cantidad de mensajes de correo electrónico a partir del servidor central, la cual equivale a la cantidad de equipos en los que se aplicó la revisión, lo cual podría "atascar" el servidor de correo electrónico. En ese caso, podría optarse por definir esta alerta para que simplemente se escriba en el registro del servidor central en lugar de enviar un mensaje de correo electrónico.

¿Qué tipos de problemas de dispositivo generan alertas?

Este producto incluye una lista exhaustiva de los eventos que pueden generar alertas. Algunos son problemas que ameritan atención inmediata, otros son cambios de configuración que podrían ser un problema o no pero que proporcionan información útil al administrador de sistemas. Consulte "Supervisión de cambios de configuración", si desea información pertinente. Las alertas solamente se generan si los dispositivos están equipados con el hardware debido. Por ejemplos, las alertas generadas a partir de lecturas de sensor sólo se aplican a los dispositivos equipados con los sensores correspondientes.

Los tipos de eventos que pueden supervisarse incluyen los siguientes:

- **Cambio de hardware:** se ha agregado o extraído un componente, como un procesador, una memoria, una unidad o una tarjeta.
- **Aplicaciones agregadas o quitadas:** se ha instalado o desinstalado una aplicación en un dispositivo.
- **Evento de servicio:** se ha iniciado o detenido un servicio en el dispositivo.
- **Desempeño:** se ha sobrepasado un umbral de desempeño, como la capacidad de una unidad, la memoria disponible, etc.
- **Evento IPMI:** se ha producido un evento que puede detectarse en los dispositivos IPMI, lo cual incluye cambios en los controladores, los sensores, los históricos, etc.
- **Uso del módem:** se ha utilizado el módem del sistema o bien, se ha agregado o quitado un módem.
- **Seguridad física:** se ha detectado la intrusión del chasis, un ciclo de energía u otro cambio físico.
- **Instalación de paquete**: se ha instalado un paquete en el equipo de destino.
- **Actividad de control remoto:** se ha producido actividad de control remoto, lo cual incluye el inicio, la detención o los errores.

El monitoreo de hardware que genera alertas depende de las capacidades del hardware instalado en un dispositivo, así como en la configuración correcta del hardware. Por ejemplo, si un disco duro con capacidades de monitoreo S.M.A.R.T. se instala en un dispositivo, pero S.M.A.R.T.no se encuentra habilitado en la configuración del BIOS del dispositivo, o si el BIOS del dispositivo no es compatible con S.M.A.R.T., las alertas no se generarán a partir del monitoreo de unidades S.M.A.R.T.

Configuración de niveles de gravedad para eventos

Los problemas o eventos de dispositivo pueden asociarse con algunos o con todos los niveles de gravedad mencionados a continuación.

- **Informativo:** admite los cambios de configuración o los eventos que los fabricantes podrían incluir en sus sistemas. Este nivel de gravedad no afecta la condición del dispositivo.
- **Aceptar:** indica que el estado se encuentra en un nivel aceptable.
- **Advertencia:**brinda advertencia anticipada sobre un problema antes de que alcance un punto crítico.
- **Crítica:** indica que el problema requiere atención inmediata.
- **Desconocido:** el estado de alerta no se puede determinar o el agente de supervisión no se ha instalado en el dispositivo.

Según la naturaleza del evento o problema del servidor, algunos niveles de gravedad no se aplican o no se incluyen. Por ejemplo, con el evento de detección de la intrusión, el chasis del dispositivo está ya sea abierto o cerrado. Si está abierto, se podría activar una acción de alerta con una gravedad de advertencia. Otros eventos, tales como el espacio de disco y la memoria virtual, incluyen tres niveles de gravedad (normal, advertencia y crítico).

Puede elegir el nivel de gravedad o umbral que activarán algunas alertas. Por ejemplo, puede seleccionar distintas acciones como resultado de un estado de advertencia o crítico de una alerta. El estado desconocido no se puede seleccionar como desencadenante de alertas. No obstante, indica que no se puede determinar el estado.

Proceso de configuración para los reglamentos de alerta personalizados

Puede configurar un reglamento de alerta para implementarlas en un dispositivo individual o en un grupo de dispositivos de destino. Cada uno de los dispositivos administrados debe tener instalado el componente de supervisión del producto para enviar alertas al servidor central. Consulte "Configuración de agentes", si desea más información.

Al instalar el componente de supervisión en un dispositivo administrado, se incluye un reglamento de alertas predeterminado que brindan información de estado 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)

Además del reglamento predeterminado, puede configurar e implementar reglamentos de alerta personalizados. Puede incluir acciones de alerta personalizadas que responda a eventos particulares. Por ejemplo, si se detiene un ventilador, se podría activar una alerta y enviar un mensaje de correo electrónico al grupo de asistencia de hardware.

El proceso general para crear e implementar un reglamento de alertas es el siguiente:

1. Seleccione los dispositivos a los que desee implementar el reglamento y haga clic en **Destino** para agregarlos a la lista de **Dispositivos de destino**.
2. Cree los reglamentos de acción de alerta que utilizará. Estos reglamentos de acción de alerta definen los tipos de acciones que pueden iniciar las alertas. Si desea más información, consulte "Configuración de las acciones de alerta".
3. Cree el reglamento de alertas personalizado. Cuando hace esto puede seleccionar las acciones que definió con anterioridad. Si desea más información, consulte "Configuración del reglamento de alertas".
4. Implemente los reglamentos en los dispositivos destino. Puede seleccionar como destino otros dispositivos antes de implementar el reglamento. Si desea obtener más información, consulte "Implementación de reglamentos".

El siguiente es un ejemplo sencillo de este proceso.

Ejemplo: Configuración de un reglamento de alertas para un problema de espacio de disco

1. En el panel de navegación izquierdo, haga clic en **Mis dispositivos** y haga doble clic en el grupo **Todos los dispositivos**.
2. Seleccione los dispositivos para los cuales desea definir la alerta y haga clic en **Destino** para colocar los dispositivos en la lista **Dispositivos de destino**.
3. Haga clic en **Alertas** y luego en la ficha **Reglamentos de acción**.

4. En la lista desplegable **Acciones**, seleccione la acción que desee configurar (como **Enviar correo electrónico/página**). Haga clic en **Nuevo**, escriba un nombre en el campo **Nombre** y haga clic en **Aceptar**.
5. De regreso en la página **Reglamentos de acciones**, seleccione el reglamento al que ha asignado un nombre y haga clic en **Editar acciones**. Especifique la información a medida que se necesite en los cuadros de texto. Una vez que haya finalizado, haga clic en **Guardar**.
6. Haga clic en la ficha **Reglamentos de alertas**.
7. Haga clic en **Nuevo**, escriba un texto similar a "Problema de espacio de disco" en el campo **Nombre**, escriba una descripción en el campo **Descripción** y haga clic en **Aceptar**.
8. Haga clic en la alerta que acaba de crear y haga clic en **Editar reglamentos**.
9. Haga clic en el botón **Nuevo**.
10. En la lista desplegable **Tipo de alerta**, haga clic en **Espacio de disco**.
11. Marque el estado para el que desee recibir alertas: **Normal**, **Advertencia** o **Crítico**. Si desea la misma acción en varios estados, seleccione más de uno. Si desea una acción diferente en cada estado, cree una configuración distinta para cada estado a fin de desencadenar diversas acciones en los distintos niveles de estado.
12. En la lista desplegable **Acción** seleccione la acción que desee que se realice si se cumplen las condiciones especificadas en los pasos 6 y 7. Si desea una acción que no esté en la lista, deberá crear una en la página **Reglamentos de acción**. (Si no ha creado un reglamento de alertas, no figurará en la lista).
13. En la lista desplegable **Acción de alerta**, seleccione la configuración que desee.
14. Marque la opción **Afecta la condición del dispositivo**, si desea que la alerta se aplique al estado del servidor cuando se visualiza en la lista **Todos los servidores**. Si el nivel de gravedad de la alerta es solamente **Informativo**, la alerta no afecta el estado del dispositivo.
15. Haga clic en **Agregar**.
16. Repita los pasos del 6 al 12 si desea agregar alertas adicionales al reglamento.
17. Una vez que haya finalizado, haga clic en **Cerrar**.
18. Si desea cambiar cualquier tipo de alerta en el reglamento, seleccione el tipo de alerta y haga clic en **Editar**, haga los cambios, haga clic en **Actualizar** y luego en **Cerrar**.
19. Cuando se define un reglamento de alertas, aplique el reglamento a los dispositivos de destino: haga clic en **Implementar reglamento**, seleccione el reglamento y haga clic en **Implementar**.

Configuración de las acciones de alerta

Utilice la página **Reglamentos de acciones** para especificar información adicional sobre la forma en que deben comportarse las acciones al seleccionarlas. Si se sobrepasa un umbral, se genera una alerta. La alerta puede tener una acción asociada a ella, tal como el envío de un mensaje de correo electrónico. Cada acción tiene su propia configuración y debe definirse de forma individual.

Para crear un reglamento de acciones

1. En el panel de navegación izquierdo, haga clic en **Alertas** y luego en la ficha **Reglamentos de acciones**.
2. En la lista desplegable **Acciones**, seleccione la acción que desee configurar. Cada acción tiene su propia lista de configuraciones únicas.

3. Haga clic en **Nuevo**, escriba un nombre en el campo **Nombre** y haga clic en **Aceptar**.
4. De regreso en la página **Reglamentos de acciones**, seleccione el reglamento al que ha asignado un nombre y haga clic en **Editar acciones**.
5. Si ha seleccionado **Ejecutar programa en servidor central** o **Ejecutar programa en cliente**, escriba o pegue la ruta al programa que desee ejecutar con la alerta, y haga clic en **Guardar**. Cuando selecciona la acción **Ejecutar programa**, observe que los programas pueden no mostrarse de la forma esperada en el escritorio. Al ejecutar el programa, se inicia como servicio en Windows de modo que no se visualiza al igual que una aplicación normal. Los programas que se ejecutan de este modo no deben contener interfaz de usuario que requiera interacción. Para determinar de forma definitiva si se ejecutó el programa, compruebe el proceso en el Administrador de tareas de Windows.

   Si ha seleccionado **Enviar correo electrónico o aviso**, escriba la dirección de correo electrónico completa de la persona que recibirá el mensaje de correo electrónico en el campo **A**; escriba una dirección de correo electrónico válida en el campo **De**; escriba el asunto en el campo **Asunto**; escriba un mensaje en el campo **Cuerpo**; seleccione el día y la hora en que debe enviarse el mensaje; y escriba la ubicación del servidor SMTP en el campo **Servidor SMTP**. Haga clic en el cuadro **Ayuda** para obtener información sobre el envío de mensajes a varios destinatarios y el uso de variables en los mensajes. Una vez que haya finalizado, haga clic en **Guardar**.

   Si ha seleccionado **Enviar captura SNMP**, escriba el nombre del host, seleccione una versión, escriba la cadena de comunidad en el campo **Cadena de comunidad** y haga clic en **Guardar**.

Notas

- Ciertas alertas asignadas a grupos de equipos pueden generar una gran cantidad de respuestas de forma simultánea. Por ejemplo, puede definir la alerta "Cambio de configuración de equipo" y asociarla con una acción de correo electrónico. Si se aplica una revisión de distribución de software a los equipos con esta configuración de alerta, se genera una cantidad de mensajes de correo electrónico a partir del servidor central, la cual equivale a la cantidad de equipos en los que se aplicó la revisión, lo cual podría "atascar" el servidor de correo electrónico. En ese caso, podría optarse por definir esta alerta para que simplemente se escriba en el registro del servidor central en lugar de enviar un mensaje de correo electrónico.
- Algunas acciones de alerta no afectan el estado del dispositivo. Dichas acciones incluyen la ejecución de un programa en el cliente, el apagado o reinicio y cualquier alerta que sea solamente informativa. No obstante, si cualquiera de estas acciones se combina con otras acciones de alerta que sí afectan la condición del dispositivo, las alertas generadas afectarán la condición del dispositivo y aparecerán en el histórico de alertas.
- El campo **De** de un mensaje de correo electrónico debe contener una dirección de correo electrónico válida para que funcionen las alertas SMTP.
- Se procesan las capturas SNMP identificadas como de versión 1, mientras que las de versión 3 solamente se envían.
- Para las capturas SNMP, los niveles de gravedad se informan en el campo Tipo específico de captura de la captura. Los valores son: 1 = desconocido, 2 = información, 3 = normal, 4 = advertencia, 5 = crítico.

Configurar un reglamento de alertas

Utilice la página **Reglamentos de alertas** para crear un reglamento de alerta nuevo. Antes de configurar las alertas, se deben configurar las acciones. Si desea más información, consulte "Configuración de las acciones de alerta".

Existen dos reglamentos de alertas que aparecen de forma predeterminada en la página de **Reglamentos de alertas**:

- **Reglamento de alertas centrales**: este reglamento asegura que las alertas se envían al servidor central cuando la función **Monitor de dispositivos** se encuentra habilitado (consulte Monitoreo de conectividad). Este reglamento contiene un grupo predefinido de tipos de alertas, incluso los tipos Monitor de dispositivos, Interruptor de circuito AMT y Sesión serie a través de LAN. Puede editar la configuración de estado, acción, acción de alerta e integridad para los tipos de alerta centrales, pero si intenta realizar otros cambios, se hará caso omiso de éstos.
- **Reglamento predeterminado**: este reglamento está implementado en todos los dispositivos administrados y contiene una cantidad de tipos de alertas que son usuales para la mayoría de los administradores. Puede editar este reglamento para agregar otros tipos de alertas y cambiar la configuración de los tipos de alerta predeterminados. Cuando edite este reglamento, los cambios se implementan en todos los dispositivos administrados aunque no vuelva a implementar el reglamento de forma explícita.

Además de estos reglamentos, puede crear reglamentos personalizados para aplicar los grupos de destino de los dispositivos administrados. Estos reglamentos deben generarse en formato XML para que se muestre en la **configuración del agente**.

Si crea un reglamento personalizado para un dispositivo, tenga en cuenta que si ya se ha implementado dicho reglamento en el dispositivo, podrían existir reglas superpuestas o conflictivas. Si implementa el reglamento predeterminado cuando configura el dispositivo administrado y luego implementa otro reglamento personalizado, se ejecutarán ambos reglamentos en el dispositivo. Por ejemplo, si ambos reglamentos generan alertas para el mismo tipo de alerta pero efectúan acciones distintas, podrían realizarse acciones duplicadas o impredecibles como resultado. Aunque no puede eliminar el reglamento predeterminado una vez que se ha implementado, puede editarlo si desea cambiar parte de él.

Para crear un reglamento de alertas

1. En el panel de exploración izquierdo, haga clic en **Alertas** y, a continuación, en la ficha **Reglamentos de Alertas** (de ser necesario).
2. Haga clic en **Nueva**, escriba un nombre en el campo **Nombre**, escriba una descripción de la alerta en el campo
   Descripción y haga clic en **Aceptar**.
3. Haga clic en el reglamento al cual ha asignado un nombre y haga clic en **Editar reglamento**.
4. Haga clic en **Nuevo**.
5. En la lista desplegable **Tipo de alerta**, seleccione el componente, la acción o el tipo de evento para el cual desee recibir alertas.

6. Marque cada uno de los estados para los que desee recibir alertas: **Informativo**, **Normal**, **Advertencia** o **Crítico**. Por ejemplo, para recibir una alerta si el tipo seleccionado en el paso 5 sobrepasa un umbral crítico, seleccione **Crítico**.
7. En la lista desplegable **Acción** seleccione la acción que desee que se realice si se cumplen las condiciones especificadas en los pasos 5 y 6. Estas acciones se definen con anticipación. Si desea una acción que no esté en la lista, deberá crear una en la página **Reglamentos de acciones**.

   Nota: Ciertas alertas asignadas a grupos de equipos pueden generar una gran cantidad de respuestas de forma simultánea. Por ejemplo, puede definir la alerta "Cambio de configuración de equipo" y asociarla con una acción de correo electrónico. Si se aplica una revisión de distribución de software a los equipos con esta configuración de alerta, se genera una cantidad de mensajes de correo electrónico a partir del servidor central, la cual equivale a la cantidad de equipos en los que se aplicó la revisión, lo cual podría "atascar" el servidor de correo electrónico. En ese caso, podría optarse por definir esta alerta para que simplemente se escriba en el registro del servidor central en lugar de enviar un mensaje de correo electrónico.

8. En la lista desplegable **Acción de alerta**, seleccione una configuración. Podría existir solamente una configuración disponible (el contenido de la lista cambia según lo seleccionado en el paso 7).
9. Marque la opción **Afecta la condición del dispositivo**, si desea que la alerta se aplique al estado del servidor cuando se visualiza en la lista **Todos los servidores**. Si el nivel de gravedad de la alerta es solamente **Informativo**, la alerta no afecta el estado del dispositivo.
10. Haga clic en **Agregar**.
11. Repita los pasos del 5 al 10 para agregar alertas adicionales al reglamento
12. Una vez que haya finalizado, haga clic en **Cerrar**.

Para editar un reglamento de alerta, seleccione el reglamento (paso 3) y haga clic en **Editar reglamento**, luego continúe con los pasos anteriores.

Unos minutos después de que cree o edite un reglamento, el servicio de implementación de reglamentos intenta actualizar de forma automática todos los equipos en los cuales se haya implementado anteriormente el reglamento. O, si desea implementar el reglamento de inmediato, haga clic en la ficha **Configuración de reglamentos** y luego en **Implementar**.

Implementación de reglamentos

Utilice la página **Implementar reglamentos** para mover la alerta seleccionada a los dispositivos de destino.

Para implementar un reglamento en un dispositivo administrado, primero debe instalar un agente de administración en el dispositivo. Cuando se implementa el agente de administración estándar, también se implementa el reglamento predeterminado. Tras completar la configuración del agente, puede actualizar o implementar reglamentos nuevos. Para empezar, debe definir los dispositivos de destino en los cuales desee implementar el reglamento.

Para implementar un reglamento de alertas

1. En el panel de navegación izquierdo, haga clic en **Mis dispositivos** y luego en el grupo **Todos los dispositivos**.
2. Seleccione los dispositivos para los cuales desea implementar el reglamento de alertas y haga clic en **Destino** para colocar los dispositivos en la lista **Dispositivos de destino**.
3. En el panel de navegación izquierdo, haga clic en **Alertas** y luego en la ficha **Implementar reglamento**.
4. En el cuadro **Reglamentos de alertas**, seleccione el reglamento que desee implementar.
5. Haga clic en el vínculo para ver la lista de dispositivos de destino. Para eliminar un dispositivo de la lista, haga clic con el botón secundario en él y haga clic en **Eliminar**. Para eliminar todos los dispositivos, haga clic con el botón secundario en cualquier nombre de dispositivo y haga clic en **Restablecer**. Para agregar dispositivos, debe agregarlos a la lista de destinos (pasos 1 y 2 anteriores).
6. Cierre la ventana **Lista de destinos** y haga clic en **Implementar** para implementar la configuración seleccionada en los dispositivos de destino.

Como parte del proceso de implementación, se crea una página XML con una lista de los reglamentos implementados y de los dispositivos en los que se implementaron. Este informe se guarda en el directorio \ldlogon\alertrules del servidor central y se le asigna un nombre con un número de secuencia asignado por la base de datos. Si desea consultar dicha página XML de forma aparte a la implementación del reglamento, haga clic en el botón **Generar XML** y luego en el vínculo para ver el archivo XML.

Observe que solamente un reglamento personalizado puede tener vigencia en un dispositivo administrado a la vez. Si ha implementado un reglamento personalizado y luego implementa un segundo reglamento personalizado en el mismo dispositivo, el primer reglamento personalizado se sobrescribe y el segundo tiene vigencia.

Visualización de los reglamentos de alertas para un dispositivo

Utilice la página **Reglamentos de alertas** para ver una lista de los reglamentos de alertas asignados al dispositivo seleccionado y ver los detalles de cada alerta.

Para ver los reglamentos de alertas

1. En la vista **Mis dispositivos**, haga doble clic en el dispositivo que desee configurar. La consola de información del servidor se abre en otra ventana del explorador.
2. En el panel de exploración izquierdo, haga clic en **Reglamentos**.
3. Haga clic en la ficha **Reglamentos de alertas**.

A continuación se brindan detalles sobre cada reglamento. Si desea más información sobre la modificación de los detalles, consulte Uso de las alertas.

- **Cuando el estado es:** Si el estado de la alerta alcanza el estado mostrado, se genera una alerta.
- **Afecta la integridad:** Indica si desea que el estado de la alerta se aplique al estado de integridad del servidor cuando se visualiza en la lista **Todos los dispositivos**.

- **Nombre del Reglamento:** Nombre del reglamento de alertas especificado, tal como se ha definido en el cuadro de diálogo Reglamentos de alertas.
- **Tipo de alerta:** Descripción del origen de la alerta (hardware, software, evento, etc.).
- **Configuración de acciones:** Acción que se realiza si se genera la alerta, tal como se ha definido en el cuadro de diálogo Configuraciones de acciones.
- **Controlador de alertas:** Tipo de alerta que se generará, tales como un mensaje de correo electrónico, una captura SNMP o la ejecución de un programa.
- **Instancia:** Indica el origen específico de la alerta.

También puede hacer clic en el botón de **Registro de alertas** para dirigirse al registro de alertas del dispositivo y ver los detalles sobre las alertas. (Consulte Visualización del registro de alertas para obtener detalles).

Visualización del registro de alertas

Utilice la página **Registro de alertas** para ver las alertas enviadas al servidor central (registro global de alertas) o a los dispositivos administrados. El registro se ordena según la hora (GMT), con las alertas más recientes en la parte superior del registro.

El registro de alertas contiene las columnas siguientes:

- **Nombre de la alerta:** nombre asociado con la alerta, tal como se ha definido en la página **Configuraciones de alertas**.
- **Hora:** fecha y hora de generación de la alerta (GMT).
- **Estado:** estado de la alerta, el cual es uno de los siguientes:
  - **Desconocido:** no puede determinarse el estado.
  - **Informativo:** admite los cambios de configuración o los eventos que los fabricantes podrían incluir en sus sistemas.
  - **Aceptar:** indica que el estado se encuentra en un nivel aceptable.
  - **Advertencia:** brinda advertencia anticipada sobre un problema antes de que alcance un punto crítico.
  - **Crítica:** indica que el problema requiere atención inmediata.
- **Instancia:** indica el origen específico de la alerta.
- **Nombre de dispositivo:** nombre del dispositivo en el que se generó la alerta. Debe ser un nombre completamente aceptable. (Sólo registro de alertas globales).
- **Dirección IP:** dirección IP del dispositivo en el que se generó la alerta. (Sólo registro de alertas globales).

Si el nombre del dispositivo no aparece el nombre completo del dominio, debido a que este producto no puede resolver el nombre completo de dominio para el dispositivo.

Para ver el registro global de alertas

1. En el panel de exploración izquierdo, haga clic en **Registros**.
2. Para ordenar las entradas por hora, nombre, estado o instancia, haga clic en el encabezado de la columna.
3. Para ver una descripción más detallada de la alerta, haga doble clic en la entrada en la columna **Nombre de alerta**.

4. Para obtener una lista de las entradas de registro por nombre, estado o instancia, seleccione el criterio de filtro en la lista desplegable Filtro. Por ejemplo, seleccione **Nombre de alerta** y escriba un nombre completo (tal como Desempeño) o uno parcial con el comodín * (tal como Remoto*). Para buscar por fecha, seleccione **Habilitar filtro de fecha**, escriba un intervalo con una fecha inicial y una final, y haga clic en **Buscar**.
5. Para borrar el estado de integridad de una alerta, haga clic en el número de la columna **Nombre de alerta** para seleccionar la alerta, haga clic en **Borrar alerta** y haga clic en **Aceptar**. Para eliminar una entrada de registro, seleccione la alerta y haga clic en **Eliminar entrada**.
6. Para eliminar todas las entradas del registro, haga clic en **Purgar registro**.

Para ver el registro de alertas de un dispositivo específico

1. Haga doble clic en el dispositivo en la lista **Mis dispositivos**.
2. En el panel de exploración izquierdo, haga clic en **Información de sistema**.
3. Haga clic en **Registros** y haga doble clic en **Registro de alertas**.
4. Para ordenar las entradas por hora, nombre, estado o instancia, haga clic en el encabezado de la columna.
5. Para ver una descripción más detallada de la alerta, haga clic en la entrada en la columna **Nombre de alerta**.
6. Para ordenar las capturas del registro por nombre, estado o instancia, haga clic en el botón **Filtro** en la barra de herramientas y seleccione el criterio de filtro. Por ejemplo, seleccione **Nombre de alerta** y escriba un nombre completo (tal como Desempeño) o uno parcial con el comodín * (tal como Remoto*). A continuación, haga clic en Buscar en la barra de herramientas para ver las alertas asociadas con las opciones de filtro que ha elegido.
7. Para ver las capturas del registro en un intervalo de fechas, desmarque la casilla **Mostrar eventos para todas las fechas** y seleccione un intervalo de fechas. Haga clic en **Actualizar** para ver las entradas correspondientes a dicho intervalo de fechas.

Actualizaciones de software

System Manager incluye una herramienta de actualización de software que permite buscar actualizaciones de software de administración, de software de sistemas operativos y de controladores de dispositivos. Puede descargar dichas actualizaciones y reparar dispositivos afectados mediante la implementación e instalación de las actualizaciones correspondientes (también conocidas como revisiones).

Lea este capítulo para obtener información sobre:

Introducción a las actualizaciones de software

La herramienta de actualización de software ayuda a mantener el software al día en los dispositivos administrados en toda la red. Puede automatizar los procesos repetitivos de mantenimiento de software actualizado, de descarga de los archivos de actualización debidos y de implementación e instalación de las actualizaciones necesarias en los dispositivos afectados.

Este producto utiliza la administración estándar basada en funciones para permitir el acceso de usuarios a la herramienta de actualización de software. La administración basada en funciones del producto constituye el modelo de acceso y seguridad que permite que los administradores restrinjan el acceso a herramientas y dispositivos. Cada usuario recibe derechos y ámbitos específicos que determinan las características que puede utilizar y los dispositivos que puede administrar. El administrador asigna dichos derechos a otros usuarios (consulte Administración basada en funciones si desea más información). Para utilizar la herramienta de actualización de software, el usuario debe iniciar una sesión con los derechos de administración de revisiones, consola Web básica e informes.

Plataformas de servidor compatibles

Las actualizaciones de software admiten la mayoría de las plataformas de servidor y permiten el rastreo de actualizaciones y la implementación de las mismas en los servidores administrados que ejecuten los siguientes sistemas operativos:

- Windows 2000 Server SP4
- Windows 2000 Advanced Server SP4

- Windows 2000 Professional SP4
- Windows 2003 Standard Edition SP1
- Windows 2003 Enterprise Edition SP1
- Windows XP Pro SP2
- RedHat Enterprise Linux ES/AS 3
- SUSE Linux Server 9 (Professional, Enterprise y Advanced)

Acerca de la ventana Actualizaciones de software

Los usuarios con el derecho de administración de revisiones verán la herramienta **Actualizaciones de software** en el panel de exploración izquierdo de la consola. Si hace clic en **Actualizaciones de software**, verá una barra de herramientas con dos paneles en la parte derecha de la ventana. El panel izquierdo muestra una vista de árbol jerárquico con los grupos de actualización de software. Haga clic en un grupo para ver su contenido en el panel derecho. El panel derecho muestra los detalles de la definición de actualización de software en una columna. En la parte superior, contiene un botón **Buscar** que permite la búsqueda rápida del criterio especificado. En el cuadro **Buscar** no se admiten los caracteres ampliados siguientes: <, >, ', ", !.

Botones de la barra de herramientas

- **Actualizar:** Abre el cuadro de diálogo **Actualizar configuración de vulnerabilidades** donde podrá especificar las plataformas y los idiomas cuya información de actualización de software desee actualizar. También puede configurar si desea colocar las actualizaciones en el grupo **Rastrear**, si desea descargar revisiones asociadas al mismo tiempo, la ubicación donde se descargan las revisiones y la configuración del servidor proxy.
- **Programar descarga:** Abre la tarea de descarga en el cuadro de diálogo **Tarea programada**, donde podrá configurar las opciones de la tarea. Si hace clic en **Guardar**, la tarea de descarga se coloca en la ventana **Tareas programadas** de la ficha **Tareas de vulnerabilidad**.
- **Programar tareas de revisión:** Abre el cuadro de diálogo **Programar rastreo de vulnerabilidades**, donde podrá especificar un nombre y configurar las opciones de rastreo.
- **Actualizar:** Actualiza la lista en el panel derecho con la información de actualización descargada más recientemente.
- **Purgar:** Abre el cuadro de diálogo **Purgar las definiciones de seguridad y de revisiones** donde puede especificar las plataformas y los idiomas cuya información de vulnerabilidad desee eliminar de la base de datos central.

Panel izquierdo (vista de árbol)

El panel izquierdo de la ventana muestra los grupos siguientes:

- **Rastrear:** Enumera todas las actualizaciones que se buscan cuando la herramienta de actualización de software se ejecuta en los dispositivos administrados. En otras palabras, si se incluye una actualización en este grupo, formará parte de la próxima operación de rastreo; caso contrario, no se incluirá en el rastreo.

  Rastrear puede considerarse como uno de los tres estados de vulnerabilidad, junto con No rastrear y No asignadas. Como tal, una actualización de software sólo puede residir en uno de esos tres grupos a la vez. Las actualizaciones se identifican con un icono exclusivo para cada estado (icono de signo de interrogación (?) para No asignada, icono de X roja para No rastrear y el icono de vulnerabilidad normal para Rastrear). Al mover una actualización de un grupo a otro se cambia su estado automáticamente.

  Para mover una actualización de software de un grupo a otro, haga clic con el botón secundario en la actualización y seleccione el grupo al cual se moverá la misma.

  Al mover actualizaciones al grupo Rastrear, podrá controlar la naturaleza y el tamaño específico del próximo rastreo de actualizaciones de software.

  También se pueden agregar automáticamente nuevas actualizaciones al grupo Rastrear durante una actualización, mediante la selección de la opción **Colocar nuevas definiciones en el grupo Rastrear** del cuadro de diálogo **Actualizar configuración de vulnerabilidades**.

  Precaución al desplazar actualizaciones desde el grupo Rastrear
  Cuando se mueven actualizaciones de software desde el grupo Rastrear al grupo No rastrear, la información actual de la base de datos central sobre los dispositivos rastreados que detectaron dichas actualizaciones se elimina de la base de datos y ya no está disponible en los cuadros de dialogo Propiedades de actualización de software e Información de servidor rastreado. Para restaurar la información de evaluación, debe volver a mover las actualizaciones de software al grupo Rastrear y ejecutar de nuevo el rastreo.

- **No rastrear:** Enumera todas las actualizaciones de software que no se buscan la próxima vez que el rastreador se ejecuta en los dispositivos. Tal y como se indicó anteriormente, si hay una actualización en este grupo, no puede estar también en el grupo Rastrear o No asignadas. Puede mover actualizaciones a este grupo para eliminarlas de un rastreo de actualizaciones de software.

- **Detectada:** Enumera todas las actualizaciones de software detectadas en el rastreo anterior, para todos los dispositivos de destino incluidos en la tarea de rastreo. El contenido de este grupo siempre es determinado por el último rastreo de actualizaciones de software, ya sea que se haya rastreado un dispositivo o varios.

  La lista Detectadas está compuesta de todas las actualizaciones de software detectadas que se han encontrado en el rastreo más reciente. Las columnas Rastreadas y Detectadas son útiles a la hora de mostrar cuántos dispositivos se rastrearon y en cuántos de esos dispositivos se detectó la actualización de software. Para ver específicamente qué servidores presentan una actualización detectada, haga clic con el botón secundario en la definición y seleccione **Ver equipos afectados**. Observe que también puede ver la información de actualización de un servidor específico en el cuadro de diálogo Consola de información del servidor del servidor.

  Sólo puede mover actualizaciones de software desde el grupo Detectadas a los grupos No asignadas o No Rastrear.

- **No asignadas:** Enumera todas las actualizaciones de software que no pertenecen a los grupos Rastrear o No rastrear. El grupo No asignadas es esencialmente un área de espera para actualizaciones recopiladas hasta que decida si desea rastrearlas o no.

  De forma predeterminada, las actualizaciones de software recopiladas se agregan al grupo Rastrear durante una actualización.

  Puede mover las actualizaciones de software desde el grupo No asignadas a los grupos Rastrear o No rastrear.

- **Mostrar según SO:** Enumera todas las actualizaciones de software descargadas organizadas en subgrupos de sistemas operativos de dispositivo específicos. Estos subgrupos le ayudan a identificar las actualizaciones de software por categoría de SO. Puede utilizar estos subgrupos de SO a fin de copiar un conjunto de actualizaciones de software en el grupo Rastrear para el rastreo de un SO específico.

  Las actualizaciones de software se pueden copiar de un grupo de SO al grupo Rastrear, No rastrear o No asignadas. Las actualizaciones pueden residir en más de una plataforma o grupo de productos de forma simultánea.

- **Ver por producto:** enumera todas las actualizaciones de software descargadas organizadas en subgrupos de productos específicos. Estos subgrupos le ayudan a identificar las actualizaciones de software por categoría de producto. Puede utilizar estos subgrupos de productos para copiar las actualizaciones de software en el grupo Rastrear para el rastreo específico al producto.

Panel derecho (vista de lista)

El panel derecho de la ventana muestra los siguientes detalles de actualización de software, en columnas que pueden ordenarse.

- **Id:** Identifica la actualización con un código alfanumérico único y definido por el proveedor.
- **Severidad:** Indica el nivel de gravedad de la actualización. Los niveles de gravedad posibles incluyen: Service Pack, Crítica, Alta, Media, Baja, No aplica y Desconocida.

- **Título:** Describe la naturaleza o el destino de la actualización en una breve cadena de texto.
- **Idioma:** indica el idioma del sistema operativo afectado por la actualización.
- **Fecha de publicación:** Indica la fecha en la que el proveedor publicó la actualización.
- **Instalación en segundo plano:** Indica si el archivo de revisión asociado a la actualización se instala en segundo plano (sin la intervención del usuario). Algunas actualizaciones tienen más de una revisión. Si alguna de las revisiones de una actualización no se instalan en segundo plano, el atributo Instalación en segundo plano de la actualización indica No.
- **Reparable:** Indica si la actualización se puede reparar mediante el despliegue o la instalación de un archivo de revisión. Los valores posibles son: Sí, No, Algunas (para una actualización que incluye varias reglas de detección y no se pueden reparar todas las actualizaciones detectadas).

Haga doble clic en el Id. de actualización para ver más información detallada en el diálogo de propiedades correspondiente. En el cuadro de diálogo de propiedades de actualización de software podrá ver las reglas de detección de la actualización, descargar los archivos de revisión asociados y hacer clic en la regla para ver el cuadro de diálogo de propiedades detalladas correspondiente.

Configuración de dispositivos para el rastreo de actualizaciones de software

Antes de que se puedan explorar los dispositivos administrados para encontrar vulnerabilidades y recibir implementaciones de revisiones, estos deben tener instalado el agente de actualizaciones de software.

El modo más sencillo de implementar el agente de actualizaciones de software en varios dispositivos administrados es mediante la creación de una nueva configuración de agente, con el agente rastreador de actualizaciones de software seleccionado (opción predeterminada) y la programación de la configuración en los dispositivos de destino deseados en **Tareas programadas**.

Cuando se configura un dispositivo para que admita el rastreo de actualizaciones de software, los archivos necesarios para el rastreo y la reparación de actualizaciones de software (por ejemplo, implementación e instalación de revisiones) se instalan en el dispositivo de destino.

Actualización de definiciones de actualización de software

La red presenta una vulnerabilidad continua ante aspectos de mantenimiento como actualizaciones de software y correcciones de defectos. La herramienta de actualización de software lleva a cabo de forma rápida y sencilla el proceso de recopilación de la información más reciente sobre revisiones, para permitir la actualización de software a través de una base de datos alojada en LANDesk. Este servicio consolida las actualizaciones conocidas provenientes de fuentes de confianza del sector o de los proveedores.

Al establecer y mantener al día la información de las revisiones, podrá entender mejor la naturaleza y el ámbito de las actualizaciones de software necesarias para cada uno de los

sistemas operativos que utiliza. El primer paso consiste en mantenerse al corriente de la información de actualización más reciente.

Se pueden configurar y realizar actualizaciones de software al mismo tiempo o bien, crear una tarea de actualización programada para que se lleve cabo en un momento establecido o como tarea recurrente.

Para actualizar la información de actualización de software

1. Desde el panel de exploración izquierdo, haga clic en **Actualizaciones de software**. Para obtener una descripción del cuadro de diálogo, consulte Acerca de la ventana Actualizaciones de software.
2. Haga clic en el botón **Actualizar** de la barra de herramientas.
3. Seleccione el sito de descarga de la actualización en la lista de servidores de contenido disponibles.
4. Seleccione las plataformas cuya información de actualización de software desee actualizar. Puede seleccionar una o varias plataformas de la lista. Cuantas más plataformas seleccione, más durará el proceso de actualización.
5. Seleccione los idiomas cuya información de actualización de software desee actualizar en las plataformas especificadas. Puede seleccionar uno o varios idiomas de la lista. Cuantos más idiomas seleccione, más durará el proceso de actualización.
6. Si desea que las nuevas definiciones de actualización de software (es decir, las que no existen en la base de datos) se coloquen de forma automática en el grupo No asignadas en lugar de la ubicación predeterminada, la cual es el grupo Rastrear, desmarque la casilla **Colocar nuevas definiciones en el grupo Rastrear**.
7. Si desea descargar automáticamente los archivos ejecutables de la revisión, active la casilla de verificación **Descargar revisiones para las definiciones seleccionadas anteriormente** y a continuación, haga clic en una de las opciones de descarga.

    - **Sólo para definiciones detectadas:** Descarga únicamente las revisiones asociadas con actualizaciones de software detectadas por el último rastreo de actualizaciones de software (p. ej., actualizaciones que residen actualmente en el grupo Detectadas).
    - **Para todas las definiciones con referencia:** Descarga TODAS las revisiones asociadas con las actualizaciones de software que residen actualmente en el grupo Rastrear. Esto toma mucho tiempo.

Las revisiones se pueden descargar en la ubicación especificada en la sección Configuración de revisiones del cuadro de diálogo (consulte el siguiente procedimiento).

8. Si tiene un servidor proxy en la red que se utiliza para las transmisiones de Internet externas (necesarias para actualizar la información de actualizaciones de software y descargar revisiones) haga clic en **Configuración del proxy** y marque la casilla **Usar servidor proxy**. Especifique la dirección del servidor, el número de puerto y las credenciales de autenticación si se requiere el inicio de sesión para el acceso al servidor proxy.
9. Haga clic en **Aplicar** en cualquier momento para guardar la configuración.
10. Haga clic en **Actualizar ahora** para ejecutar la actualización de software. En el cuadro de diálogo **Actualizar definiciones de seguridad y revisiones** se muestra el estado y la operación actual.

11. Una vez completada la actualización, haga clic en **Cerrar**. Tenga en cuenta que si hace clic en **Cancelar** antes de que finalice la actualización, solamente se descargará en la base de datos central la información de actualización de software que se ha procesado hasta ese momento. Tendrá que ejecutar la actualización de nuevo a fin de obtener el resto de la información.

Nota: No cierre la consola mientras se ejecute un proceso de actualización o hasta que el mismo haya finalizado. Esto no se aplica a la tarea de descarga programada.

Si System Manager y LANDesk® Management Suite están instalados en el mismo servidor central, ambos productos utilizan el mismo archivo de configuración para determinar los tipos de vulnerabilidades que se actualizarán. En algunos casos podría ver actualizaciones en System Manager que sólo se pueden configurar desde Management Suite cuando se ejecuta la actualización. Por ejemplo, si seleccionó las amenazas de seguridad como una opción de actualización en Management Suite y selecciona la actualización de las actualizaciones de software en System Manager, cuando ejecute la actualización en System Manager verá las actualizaciones de software y las amenazas de seguridad en los elementos actualizados.

Para configurar la ubicación de descarga de revisiones

1. En el cuadro de diálogo **Actualizar configuración de vulnerabilidades**, haga clic en la ficha **Configuración de revisiones**.
2. Indique una ruta UNC donde desee que se copien los archivos de revisión. La ubicación predeterminada es el directorio \LDLogon\Patch del servidor central.
3. Si la ruta UNC especificada señala una ubicación que no sea el servidor central, escriba un nombre de usuario y una contraseña válidos para la autenticación en dicha ubicación.

   La carpeta debe tener activado el uso compartido de archivos y de Internet, y debe activarse el acceso anónimo.

4. Indique una dirección URL del Web donde los servidores puedan tener acceso a las revisiones descargadas para la implementación. La dirección debe coincidir con la ruta UNC indicada anteriormente.
5. Puede hacer clic en **Comprobar configuración** para comprobar si se puede realizar una conexión a la dirección Web especificada con anterioridad.
6. Si desea restaurar la ruta UNC y la dirección URL del Web en sus ubicaciones predeterminadas, haga clic en **Restablecer la Configuración de la Revisión**. La ubicación predeterminada es el directorio \LDLogon\Patch del servidor central.

Programación de descargas de actualización de software

También puede configurar actualizaciones de software como tarea programada para que se produzca de forma automática en un momento establecido en un futuro o como tarea recurrente. Para ello, haga clic en el botón **Programar descarga** de la barra de herramientas, para abrir el cuadro de diálogo **Propiedades de tarea programada**, donde podrá asignar un nombre a la tarea y configurar sus opciones. Al hacer clic en **Guardar**, la tarea aparece en la ventana Tareas programadas.

Todas las tareas de actualización de software programadas utilizan las opciones definidas en el diálogo **Actualizar configuración de vulnerabilidades**. Por lo tanto, si desea cambiar el sitio de origen, las plataformas, los idiomas el sitio de descarga de revisiones o el servidor proxy de una tarea de actualización particular, en primer lugar debe modificar esta configuración en el cuadro de diálogo **Actualizar configuración de vulnerabilidades**, antes de programar la tarea para su ejecución.

Para configurar una tarea de programación de tarea

1. Desde el panel de exploración izquierdo, haga clic en **Actualizaciones de software**.
2. Haga clic en **Programar descarga**.
3. En la página **Tarea programada**, configure la programación.
4. Haga clic en **Guardar**.

Cuando hace clic en **Programar descarga**, se crea una tarea (no tiene dispositivos de destino y no se encuentra programada). Si cancela este procedimiento de **Tareas programadas**, tenga en cuenta que ya se creó y que figura en la lista **Mis tareas**.

Visualización de la información de actualización de software y de reglas de detección

Después que se han actualizado las actualizaciones de software con la información más reciente del servicio de seguridad LANDesk, podrá ver las listas de actualizaciones de software en la consola, verlas según la plataforma y el producto, y mover las actualizaciones de software a distintos grupos de estado. Si desea información sobre los distintos grupos de la ventana y su utilización, consulte Acerca de la ventana Actualizaciones de software, anteriormente en este capítulo.

Para ver los detalles de las actualizaciones de software, haga doble clic en un Id. de actualizaciones de software, lo cual abre el cuadro de diálogo de propiedades respectivo. En este diálogo también puede tener acceso a los detalles de la regla de detección. Para ello, haga doble clic en el nombre de un archivo de revisión en la lista **Reglas de detección** para abrir el cuadro de diálogo de propiedades de la revisión (consulte Cuadro de diálogo Propiedades de la revisión).

Esta información puede ayudarle a determinar qué actualizaciones son relevantes para las plataformas de servidor admitidas de la red, el modo en que las reglas de detección de actualizaciones verifican la presencia de vulnerabilidades, qué revisiones se encuentran disponibles y cómo se desea configurar y realizar la reparación de los dispositivos afectados.

También puede ver la información de definición de actualización de software y de regla de detección específica a los dispositivos rastreados directamente en la consola. Para ello, acceda a la consola de información de servidor a partir de **Mis dispositivos** y haga clic en **Actualizaciones de software** en el panel de exploración izquierdo.

Purga de la información de actualización de software

La información de actualización de software se puede purgar desde la ventana de actualizaciones de software (y posteriormente de la base de datos central) si se determina que no es relevante en el entorno.

Al purgar la información de actualización de software, la información de la regla de detección asociada también se borra de la base de datos. No obstante, con este proceso no se eliminan los archivos ejecutables de la revisión real. Los archivos de revisión se deben eliminar manualmente en el depósito local que suele encontrarse en el servidor central.

Para purgar la información de actualización de software

1. Haga clic en el botón **Purgar** de la barra de herramientas. Para obtener una descripción del diálogo, consulte Acerca del cuadro de diálogo Purgar las definiciones de seguridad y de revisiones.
2. Seleccione las plataformas cuya información de actualización de software desee eliminar. Puede seleccionar una o varias plataformas de la lista.

   Si una actualización está asociada con más de una plataforma, debe seleccionar todas sus plataformas asociadas a fin de que se elimine la información de la actualización.

3. Seleccione los idiomas cuya información de actualización desee eliminar (asociada con la plataforma especificada anteriormente).

   Si selecciona una plataforma de Windows, debe especificar los idiomas cuya información de actualización desee eliminar. Si elige una plataforma UNIX, es necesario especificar la opción Idioma neutral para poder eliminar la información de actualización en distintos idiomas.

4. Haga clic en **Eliminar**.

Rastreo de actualizaciones de software en dispositivos

La evaluación de actualizaciones de software implica la comprobación de las versiones instaladas actualmente de los archivos específicos del sistema operativo, así como las claves de registro en un dispositivo en relación a las actualizaciones de software detectadas más recientes con el fin de poder identificar las necesidades de actualización en los servidores. Tras revisar la información de actualización de software conocida (actualizada a partir de fuentes del sector) y decidir qué actualizaciones se desean rastrear, puede realizar una evaluación personalizada en los dispositivos administrados que dispongan del agente de actualizaciones de software instalado. Si desea información sobre la configuración de dispositivos para el rastreo y la implementación de revisiones, consulte "Configuración de dispositivos para el rastreo de actualizaciones de software", anteriormente en este capítulo).

Al ejecutar el rastreador de actualizaciones de software, éste siempre lee el contenido del grupo Rastrear y se exploran actualizaciones específicas. Antes de rastrear los servidores en busca de actualizaciones, siempre debe asegurarse de que se incluyan en ese grupo solamente las actualizaciones de software que desee rastrear. Puede mover las actualizaciones de software dentro y fuera del grupo Rastrear para personalizar el tamaño y la naturaleza del rastreo.

Ejecución del rastreador de actualizaciones de software

El rastreador de actualizaciones de software se puede instalar automáticamente en los dispositivos en calidad de tarea de rastreo desde la consola.

Para crear una tarea de rastreo de actualizaciones de software

1. Desde el panel de exploración izquierdo, haga clic en **Actualizaciones de software**.
2. Compruebe que las definiciones de actualización de software se hayan actualizado recientemente.
3. Asegúrese de que el grupo Rastrear contenga únicamente las actualizaciones de software que se deseen rastrear.
4. Haga clic en el botón **Programar tarea de revisión** de la barra de herramientas. Para obtener una descripción del diálogo, consulte "Cuadro de diálogo Programar rastreo de vulnerabilidades".
5. Escriba un nombre único para el rastreo. Si ya existe la secuencia de comandos de la tarea, puede seleccionar si se debe anular la secuencia de comandos existente.
6. Especifique si desea que el rastreador de actualizaciones de software muestre un cuadro de diálogo de progreso en el dispositivo de destino. También se puede especificar que aparezca el botón Cancelar en el cuadro de diálogo de rastreo, para que el usuario tenga la opción de cancelar el rastreo.
7. Especifique la forma en que se debe cerrar el cuadro de diálogo del rastreador de actualizaciones de software una vez que finaliza su ejecución en los dispositivos de destino. Puede elegir entre solicitar información del usuario final o que el cuadro de diálogo se cierre tras un lapso de tiempo de espera especificado.
8. Haga clic en **Aceptar**.
9. Seleccione la tarea en el panel inferior (bajo **Tareas de vulnerabilidad**) y haga clic en **Editar**. Defina los parámetros de destino y programación, y haga clic en **Guardar**.

Visualización de actualizaciones detectadas

Si el rastreador de actualizaciones de software detecta alguna de las actualizaciones de software habilitadas en los dispositivos de destino, esta información se transmitirá al servidor central y se agregará a la lista **Detectadas**.

Puede utilizar alguno de los siguientes métodos para ver las actualizaciones detectadas tras la ejecución del rastreo de actualizaciones de software:

Según el grupo Detectadas

Seleccione el grupo **Detectadas** en la ventana de actualizaciones de software para ver una lista completa de todas las actualizaciones detectadas con el rastreo más reciente.

Según un dispositivo individual

Haga doble clic en un nombre de dispositivo en **Mis dispositivos** y luego haga clic en **Actualizaciones de software**, para ver la información detallada sobre la evaluación de actualizaciones de software correspondiente al dispositivo.

Descarga de revisiones

Para poder implementar las revisiones en los dispositivos con actualizaciones de software detectadas, en primer lugar el archivo ejecutable de la revisión se debe descargar en un depósito de revisiones local de la red. La ubicación predeterminada para las descargas es el directorio

/LDLogon del servidor central. Puede cambiar esta ubicación en la ficha **Configuración de revisiones** del cuadro de diálogo **Actualizar configuración de vulnerabilidades**.

Ubicación de la descarga de revisiones y configuración del servidor proxy
Las descargas de revisiones siempre emplean la configuración de ubicación de descarga localizada actualmente en la ficha **Configuración de revisiones** del cuadro de diálogo **Actualizar configuración de vulnerabilidades**. Observe también que si la red utiliza un servidor proxy para el acceso a Internet, en primer lugar debe establecer la configuración del servidor en la ficha **Configuración de proxy** del cuadro de diálogo **Actualizar configuración de vulnerabilidades** antes de que pueda descargar los archivos de revisión.

El producto primero intenta descargar un archivo de revisión desde la dirección URL mostrada en el cuadro de diálogo Propiedades de la revisión. Si no se puede realizar ninguna conexión, o bien, si la revisión no está disponible por algún motivo, el producto descarga la revisión del servicio de seguridad de LANDesk, el cual consiste de una base de datos alojada por la empresa que contiene revisiones de fuentes del sector de confianza.

Se puede descargar una sola revisión, o bien, un conjunto de revisiones al mismo tiempo.

Para realizar la descarga de revisiones simples

1. Haga doble clic en el nombre de una actualización de software para abrir el cuadro de diálogo **Propiedades**.
2. En la sección **Reglas de detección**, seleccione los archivos de revisión de regla de detección que desee descargar y haga clic en **Descargar revisiones seleccionadas**.
3. El estado y la operación de descarga se muestran en el cuadro de diálogo **Descarga de revisiones**. Puede hacer clic en **Cancelar** en cualquier momento para detener todo el proceso de descarga.
4. Una vez finalizada la descarga, haga clic en el botón **Cerrar**.

Para realizar la descarga de revisiones múltiples

Todas las tareas de actualización de software programadas utilizan las opciones definidas en el diálogo **Actualizar configuración de vulnerabilidades**. Por lo tanto, si desea cambiar el sitio de origen, las plataformas, los idiomas el sitio de descarga de revisiones o el servidor proxy de una tarea de actualización particular, en primer lugar debe modificar esta configuración en el cuadro de diálogo **Actualizar configuración de vulnerabilidades**, antes de programar la tarea para su ejecución.

1. Desde el panel de exploración izquierdo, haga clic en **Actualizaciones de software**.
2. Haga clic en **Programar descarga**.
3. En la página **Tarea programada**, programe la tarea.
4. Haga clic en **Guardar**.

Eliminación de archivos de revisión

Para eliminar los archivos de revisión, debe borrarlos manualmente del depósito de revisiones que suele situarse en el directorio LDLogon del servidor central.

Reparación de actualizaciones de software

Una vez que se han actualizado las definiciones de actualización de software, se han colocado las actualizaciones que se desean rastrear en el grupo Rastrear, se ha ejecutado un rastreo en los dispositivos administrados, se han determinado las actualizaciones de software que precisan atención y se han descargado las revisiones necesarias, el paso siguiente consiste en la reparación de actualizaciones de software mediante la implementación e instalación de las revisiones necesarias en los dispositivos afectados.

La reparación de cada actualización de software se realiza de forma individual. En otras palabras, debe crear una tarea de reparación para una actualización de software específica, la cual implementa e instala los archivos de revisión necesarios.

Observe que la reparación, al igual que sucede con el rastreo de actualizaciones, sólo funciona en dispositivos configurados con el agente de actualización de software. Si desea obtener más información, consulte Configuración de dispositivos para el rastreo de actualizaciones de software, anteriormente en este capítulo.

Se admite la reparación de Linux. Puede utilizar la herramienta de actualización de software para detectar vulnerabilidades en dispositivos Linux y luego decidir si desea reparar las actualizaciones. Si desea hacerlo, utilice una suscripción de asistencia del proveedor de Linux para descargar los RPM necesarios y luego implemente los RPM en los dispositivos.

Advertencia: muchas revisiones reinician el dispositivo de forma automática al finalizar.

Para crear una secuencia de comandos de reparación personalizada

1. Desde el panel de exploración izquierdo, haga clic en **Actualizaciones de software**.
2. Seleccione el grupo **Detectadas** para ver las actualizaciones de software en el rastreo más reciente. No es necesario seleccionar este grupo. Si desea crear una secuencia de comandos de reparación personalizada que busque actualizaciones de software que aún no se han rastreado o detectado, haga clic en cualquiera de los otros grupos de vulnerabilidades para ver su contenido y seleccionar una vulnerabilidad determinada.
3. Haga clic con el botón secundario en la definición y seleccione **Ver dispositivos afectados** para ver los dispositivos que son afectados por dicha actualización de software.
4. Haga clic con el botón secundario en la definición y seleccione **Crear tarea de reparación**.
5. (Opcional) Modifique el nombre en el cuadro de texto **Nombre de la tarea**.
6. Seleccione las opciones disponibles y haga clic en **Aceptar**.
    - **Copiar afectó a los equipos en la cesta de destino:** Copia los equipos afectados por la actualización de software a la cesta de destino para la reparación.
    - **Mostrar progreso durante la ejecución:** Habilita que el rastreador muestre información en los dispositivos de usuario final mientras se ejecuta. Haga clic en esta opción si desea mostrar la actividad del rastreador, y si desea configurar otras opciones de muestra e interacción en este cuadro de diálogo. Si no hace clic en esta opción, ninguna de las otras opciones en este diálogo estarán disponibles para la configuración, y el rastreador se ejecuta de forma transparente en los dispositivos.

- **Requerir la entrada del usuario antes de cerrar el diálogo Rastreo de vulnerabilidad**: Haga clic en esta opción si desea que el rastreador solicite la interacción del usuario antes de cerrar el cuadro de diálogo en el dispositivo. Si seleccionó esta opción, y el usuario final no responde, el diálogo permanece abierto, lo que puede causar que se agote el tiempo de espera de otras tareas programadas.
- **Cerrar el cuadro de diálogo automáticamente al vencer el tiempo de espera:** Haga clic en esta opción si desea que el cuadro de diálogo se cierre tras el intervalo especificado.

Secuencias de comandos

Administración de las secuencias de comandos

Este producto utiliza secuencias de comandos para ejecutar tareas personalizadas en los dispositivos. Al completar los diálogos de creación de secuencias de comandos se genera un archivo de texto ASCII en el formato de Windows INI, con extensión .INI. Las secuencias de comandos se almacenan en el servidor central en la carpeta \Archivos de programa\LANDesk\ManagementSuite\Scripts. El nombre del archivo de la secuencia de comandos se convierte en el nombre de la secuencia de comandos en la consola. Puede crear secuencias de comandos del programador local para dispositivos Windows mediante la ventana **Secuencias de comandos** (haga clic en **Secuencias de comandos** en el panel de exploración izquierdo) o escriba sus propias secuencias de comandos y guárdelas en la carpeta Scripts.

La ventana **Secuencias de comandos** divide las secuencias en las categorías siguientes:

- **Mis secuencias de comandos:** Son las secuencias de comandos que asocia con este grupo.
- **Todas las demás secuencias:** Todas las secuencias de comandos que se encuentran en el servidor central.
- **Secuencias de comandos de usuarios** (solo visibles para los administradores): Secuencias de comandos creadas por todos los usuarios del producto. Se ordenan por nombre de quien las creó.

Puede crear grupos en el elemento **Mis secuencias de comandos** para categorizar aún más las secuencias de comandos. Para crear una nueva secuencia de comandos del programador local, haga clic en el botón **Local**.

Una vez creada la secuencia de comandos, puede hacer clic en **Programar** en el menú contextual de la misma. En la ventana **Mis dispositivos**, puede especificar los dispositivos en los cuales se ejecutará la tarea y puede programar en qué momento se ejecutará la tarea en la ventana **Tareas programadas**. Para obtener más información sobre la programación de tareas, consulte la sección Programación de tareas.

Cambios de la propiedad de las tareas y secuencias de comandos para los usuarios de versiones anteriores de Management Suite

En las versiones de Management Suite anteriores a 8.70, todas las secuencias de comandos eran globales y todos los usuarios podían verlas. Ahora las secuencias de comando sólo son visibles al usuario que las creó y a los administradores.

La ventana **Secuencias de comandos** tiene la columna Estado. Dicha columna indica Público si todos los usuarios pueden ver la secuencia de comandos, o Privado si sólo el usuario que la creó o los administradores pueden verla. Los usuarios pueden hacer clic en el botón derecho en las

secuencias de comandos que hayan creado y hacer clic en Privado o Público para cambiar el estado de la secuencia de comandos. Los administradores pueden cambiar el estado de cualquier secuencia de comandos.

El valor predeterminado es DOS PE. Si selecciona otro PE, no podrá crear una secuencia de comandos. En los PE de Windows y Linux, solamente se puede generar una secuencia de comandos de captura o de implementación.

Si elige el PE de Linux, solamente tiene las opciones de herramientas de creación de imágenes LANDesk y Otro. Si elige el PE de Windows, tiene las opciones LANDesk, Otro y Microsoft* XImage.

Creación de una secuencia de comandos del programador local

El programador local es un servicio que se ejecuta en los dispositivos. Se instala cuando se implementa una configuración de agente como parte del agente de administración estándar. Normalmente, el programador local realiza las tareas del producto, tal como la ejecución del rastreador de inventario de forma periódica. Las otras tareas programadasson realizadas por el servidor central en lugar del programador local. Puede utilizar el programador local para programar la ejecución periódica de sus propias tareas en los dispositivos. Una vez que crea una secuencia de comandos del programador local, la puede implementar en los dispositivos administrados al igual que cualquier otra secuencia de comandos.

El programador local asigna un número de identificación a cada tarea. Los archivos de comandos del programador local tienen un intervalo de identificadores que difiere de los archivos de comandos del programador local que utiliza el producto. Solamente puede haber un archivo activo de comandos del programador personalizado en cada dispositivo. Si crea un archivo de comandos nuevo y lo despliega en los dispositivos, se reemplaza el archivo de comandos anterior (cualquier archivo de comandos en el intervalo de identificadores del programador local personalizado) sin afectar los archivos de comandos del programador local, tal como la programación de rastreo de inventario local.

Al seleccionar opciones de programación de la secuencia de comandos, recuerde las características restrictivas de las diversas opciones. Por ejemplo, si selecciona el lunes como el día de la semana y el 17 como el día del mes, la tarea solamente se ejecutará en un lunes que también sea el día 17, lo cual sucede con poca frecuencia.

Puede crear una secuencia de comandos para iniciar restartmon.exe en un equipo local, inmediatamente o en cualquier momento que prefiera. Si los informes de un equipo específico parecen haberse detenido, puede utilizar restartmon.exe en la carpeta LDClient para reiniciar el compilador y todos los proveedores de monitoreo. Esta utilidad es para los equipos en los que se instaló la opción de informes y donde éstos se detuvieron. Utilice esta utilidad para reiniciar el compilador sin reiniciar el dispositivo.

1. En el panel de exploración izquierdo, haga clic en **Secuencias de comandos**.
2. Haga clic en **Local**.
3. Introduzca un nombre de secuencia.
4. Haga clic en **Agregar** para definir las opciones del archivo de comandos.
5. Configure las opciones del programador local, tal y como se describió anteriormente. Una vez que haya finalizado, haga clic en **Guardar**.

6. Haga clic en **Guardar** para guardar el archivo de comandos.
7. Seleccione la secuencia de comandos en el grupo **Mis secuencias**, luego haga clic en **Programar** para ejecutar la secuencia de comandos que ha creado en los dispositivos.

Opciones de ancho de banda

Al configurar los comandos del programador local, puede especificar el criterio de ancho de banda que necesita el dispositivo administrado para que se ejecute la tarea. Cuando llega el momento de ejecutar la tarea, cada dispositivo que ejecuta la tarea del programador local envía una pequeña cantidad de tráfico de red ICMP al equipo especificado y evalúa el rendimiento de la transferencia. Si el equipo de destino de prueba no está disponible, la tarea no se ejecuta.

Las opciones de ancho de banda son:

- **RAS:** La tarea se ejecuta si la conexión de red del dispositivo al equipo de destino tiene al menos una velocidad RAS o de acceso telefónico. Normalmente, la selección de esta opción significa que la tarea siempre se va a ejecutar si el dispositivo tiene una conexión de red de algún tipo.
- **WAN:** La tarea se ejecuta si la conexión del dispositivo al equipo de destino es al menos una velocidad WAN. La velocidad WAN se define como una conexión no RAS que es más lenta que el umbral LAN.
- **LAN:** La tarea se ejecuta cuando la conexión del dispositivo al equipo de destino excede la configuración de velocidad LAN. La velocidad de la red local se define en 262,144 bps de forma predeterminada.

Programación de tareas de secuencias de comandos

La ventana **Tareas programadas** muestra el estado de la tarea programada mientras se ejecuta la tarea y cuando se completa. El Servicio programador puede comunicarse con los dispositivos de dos maneras distintas:

- A través del agente de administración estándar (debe estar ya instalado en los dispositivos).
- A través de una cuenta del sistema a nivel de dominio. La cuenta que elija debe tener el inicio de sesión como un privilegio del servicio y deben existir credenciales especificadas en la utilidad Configuración de servicios. Para obtener más información sobre la configuración de la cuenta Programador, consulte "Configuración del servicio de programación".

LANDesk instala varias secuencias de comandos estándares que se pueden programar para que realicen tareas de mantenimiento de rutina; por ejemplo, ejecución de rastreos de inventario en los dispositivos seleccionados. Haga clic en **Secuencias de comandos** en el panel de navegación izquierdo y haga clic en **Todas las demás secuencias** para ver y programar las secuencias de comandos.

Para programar una tarea

1. En el panel de exploración izquierdo, haga clic en **Secuencias de comandos**.
2. Haga clic para navegar al grupo de secuencias de comandos.
3. Haga clic en una secuencia de comandos y luego en **Programar**.

4. Escriba un nombre para la tarea y haga clic en **Aceptar**.
5. En la ficha **Tareas de secuencias de comandos personalizadas**, haga clic en **Todas las tareas**, en la tarea a la que asignó un nombre en el paso 3 y en **Editar**.
6. Complete las páginas de la tarea de secuencia de comandos personalizada. Haga clic en el botón Ayuda para obtener ayuda en cualquier página o consulte la ayuda del Programador de tareas.

Cuando hace clic en **Programar**, se crea una tarea (no tiene dispositivos de destino y no se encuentra programada). Si cancela este procedimiento de tarea programada, tenga en cuenta que la tarea ya se creó y que figurará en la lista de tareas.

Uso de las secuencias predeterminadas de comandos

Este producto incluye dos secuencias de comandos predeterminadas. Puede utilizarlas para realizar algunas tareas habituales. Estas tareas están disponibles bajo el árbol **Todas las demás secuencias** de la ventana **Secuencias de comandos** (en el panel de navegación izquierdo **| Secuencias de comandos**) .

- **Rastreador de inventario:** Ejecuta el rastreador de inventario en los dispositivos seleccionados. Esta secuencia de comandos contiene documentación que describe la forma en que se escribe un archivo de secuencia de comandos; lea o imprima este archivo para obtener más información sobre el uso correcto de los comandos y parámetros.
- **Restaurar registros de cliente:** Ejecuta un rastreo de inventario en los dispositivos seleccionados y el rastreador informa al servidor central en el que se configuró el dispositivo. Si es necesario restablecer la base de datos, esta tarea permite agregar dispositivos de nuevo a la base de datos central correspondiente en un entorno con varios servidores centrales.

Programación de tareas

La herramienta **Tareas personalizadas** es común a la configuración de agente, las actualizaciones de software, las secuencias de comandos y la detección de dispositivos. Las tareas se filtran en el panel inferior de las páginas de la función específica para mostrar solamente las tareas relacionadas. Por ejemplo, si abre la herramienta **Detección de dispositivos**, las tareas de detección se visualizan en la ficha **Tareas de detección** en el panel inferior. Todas las tareas aún están visibles a través de la herramienta **Tareas programadas**. Aquí puede programar la ejecución de configuraciones ya sea de inmediato, en el futuro, de forma recurrente o solamente una vez.

El panel izquierdo de la página **Tareas programadas** muestra los grupos de tareas:

- **Mis tareas:** Tareas que se han programado. Solamente la persona que las programó y los usuarios administrativos pueden ver estas tareas.
- **Todas las tareas:** Sus tareas y las marcadas como públicas.
- **Tareas comunes:** Tareas que los usuarios han marcado como comunes. Cualquier usuario que edite o programe una tarea de este grupo se convertirá en el propietario de esa tarea. La tarea permanece en el grupo Tareas comunes y también figura en el grupo Tareas de usuario de ese usuario.
- **Tareas de usuario** (sólo usuarios administrativos): Tareas que han creado los usuarios.

Si hace clic en **Mis tareas**, **Tareas comunes** o **Todas las tareas**, el panel derecho muestra esta información:

- **Tarea:** Nombres de las tareas.
- **Iniciar el:** Momento en que está programada la ejecución de la tarea. Haga clic en el nombre de una tarea y luego en **Editar** para editar la hora de inicio o volver a programarla.
- **Status:** Estado general de la tarea. Consulte la columna Estado del panel derecho, para más detalles. El panel derecho muestra el estado de la tarea, el cual puede ser En curso, Todas completadas, Ninguna completada o Fallida.
- **Paquetes de distribución:** Nombre del paquete de las tareas de distribución. Este campo se aplica a la distribución de software.
- **Métodos de entrega:** El método de entrega que utiliza la tarea. Este campo se aplica a la distribución de software.
- **Propietario:** Nombre del usuario que creó la secuencia de comandos que utiliza esta tarea.

Si hace doble clic en una tarea programada, el panel derecho muestra la siguiente información a manera de resumen:

- **Nombre:** Nombre del estado de la tarea.
- **Cantidad:** Cantidad de dispositivos en cada estado de la tarea.

- **Porcentaje:** Porcentaje de dispositivos en cada estado de la tarea.

Antes de programar tareas para un dispositivo, éste debe contener el agente debido y encontrarse en la base de datos de inventario. Las configuraciones del servidor constituyen una excepción. Pueden seleccionar un dispositivo que no tenga el agente de administración estándar. Las tareas pueden reprogramarse (editarse) o eliminarse de la ficha Tareas. Una vez que programe una tarea, consulte la ficha Tareas para ver el estado de la tarea.

Para editar una tarea, seleccione la tarea que desee editar y haga clic en **Editar**. La tarea se abre con las opciones de edición correspondientes a la tarea.

Grupos de tareas personalizados

Puede crear grupos personalizados para los tipos de tareas **Mis tareas**, **Todas las tareas** y **Tareas comunes**. Con los grupos personalizados, puede agrupar las tareas relacionadas, tales como el rastreo de vulnerabilidades y la ejecución de una secuencia de comandos. Los grupos y subgrupos pueden tener 20 niveles de profundidad.

Para crear un grupo de tareas personalizado

1. En el panel de exploración izquierdo, haga clic en **Tareas programadas**.
2. En el panel izquierdo, haga clic en el tipo de tarea en el cual desee crear el grupo.
3. Haga clic en **Nuevo grupo** en la barra de herramientas.
4. Escriba un nombre en el cuadro de texto **Nombre de grupo** y haga clic en **Aceptar**.

Luego de crear un grupo personalizado, puede mover o copiar las tareas u otros grupos al grupo. Para ello, selecciónelos en la lista y haga clic en **Mover** en la barra de herramientas.

Página Dispositivos de destino

Utilice esta página para agregar destinos de dispositivos a la tarea que está configurando. En esta ficha también puede ver los dispositivos de destino, las consultas y los grupos de dispositivos de la tarea. Si ha instalado varios productos de LANDesk Management, los grupos de dispositivos creados en la consola de un producto se pueden ver en todas las consolas. No se necesita esta página para las tareas de detección de dispositivos.

- **Agregar la Lista de Destino:** Agrega los dispositivos previamente colocados en la lista de destino a partir de **Mis dispositivos**.
- **Agregar consulta:** Especifica el destino de los resultados de una consulta que haya creado anteriormente.
- **Quitar:** Elimina los destinos seleccionados.

Aunque esta página visualiza los grupos de dispositivos de destino, observe que los grupos se visualizan solamente si se ha instalado LANDesk Management Suite en el servidor central. Si está ejecutando Server Manager, System Manager o la consola Web en Management Suite, los grupos de dispositivos no se definen como destinos en calidad de grupos. Más bien, si selecciona un grupo y lo define como destino, los dispositivos individuales del grupo se agregan a la lista de dispositivos de destino y se visualizan bajo **Dispositivos de destino** en lugar de bajo **Grupos de destino**.

Página Tarea programada

El Programador contiene la ficha **Tarea programada - propiedades**, la cual incluye estas opciones.

- **Dejar sin Programar**: (opción predeterminada) Deja la tarea en la lista de tareas para su programación futura.
- **Iniciar ahora**: Ejecuta la tarea lo más pronto posible. La tarea podría tomar hasta un minuto en iniciarse, según la configuración.
- **Iniciar a la hora programada**: Inicia la tarea a la hora especificada. Si hace clic en esta opción, debe definir lo siguiente:
  - **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.
  - **Hora**: Hora en que desea iniciar la tarea.
  - **Repetir cada**: Si desea repetir la tarea, seleccione si desea repetirla cada **Hora**, **Día**, **Semana** o **Mes**. Si elige **Mes** y la fecha no existe en todos los meses (por ejemplo, 31), la tarea se ejecutará en los meses en que exista la fecha.
- **Programar estos dispositivos:** La primera vez que se ejecuta una tarea, es recomendable que utilice la opción predeterminada Esperando o en ejecución. En las ejecuciones subsiguientes, elija entre Todos, Dispositivos que no ejecutaron la tarea o Dispositivos que no intentaron ejecutar la tarea. Estas opciones se explican en detalle a continuación.
  - **Dispositivos no satisfactorios:** Seleccione esta opción si se desea que la tarea solamente se ejecute en todos los dispositivos que no la completaron la primera vez. Esta opción excluye los dispositivos que tienen el estado Satisfactorio. La tarea se ejecutará en los dispositivos con todos los demás estados, incluso Esperando o Activo. Considere esta opción si necesita ejecutar la tarea en la mayor cantidad posible de dispositivos que no la ejecutaron, y solamente necesita ejecutarla una vez en cada dispositivo.
  - **Esperando o en ejecución:** Seleccione esta opción si desea que la tarea se ejecute en los dispositivos que están esperando ser procesados o que se están procesando.
  - **Todos:** Seleccione esta opción si desea que la tarea se ejecute en todos los dispositivos, independientemente del estado. Considere esta opción si tiene una tarea, particularmente una repetitiva, que necesite ejecutarse en la mayor cantidad de dispositivos posible.
  - **Dispositivos que no intentaron ejecutar la tarea:** Seleccione esta opción si desea que la tarea solamente se ejecute en los dispositivos que no la ejecutaron pero que tampoco fallaron. Esto excluye los dispositivos con el estado Apagado, Ocupado, Fallido o Cancelado. Considere esta opción si varios dispositivos de destino fallaron y no tienen importancia como destino.

Página Secuencias de comandos personalizadas

- **Secuencia personalizadas de comandos seleccionada:** Seleccione la secuencia de comandos de resumen que desea programar.

Informes

Acerca de los informes

System Manager incluye una herramienta de informe, la cual se utiliza para generar una gran variedad de informes especializados que brindan información crítica sobre los dispositivos administrados de la red.

System Manager emplea una utilidad de rastreo de inventario para agregar dispositivos (y los datos de hardware y software recopilados de dichos 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 informes aprovecha aún más los datos de inventario rastreados mediante la recopilación y organización de los datos en formatos de informe útiles.

Puede utilizar los informes de servicio y de activos de inventario predefinidos. Tras la ejecución de un informe, éste se puede ver en la consola.

Si Server Manager y Management Suite están instalados juntos, los informes que ejecute en Server Manager sólo incluirán los servidores. Si ejecuta una consulta, obtendrá tanto los servicios como los demás dispositivos, a menos que la consulta haya estado configurada para excluir los demás dispositivos.

Si los informes de un equipo específico parecen haberse detenido, puede utilizar restartmon.exe en la carpeta LDCLIENT para reiniciar el compilador y todos los proveedores de monitoreo. Esta utilidad es para los equipos en los que se instaló la opción de informes y donde éstos se detuvieron. Utilice esta utilidad para reiniciar el compilador sin reiniciar el dispositivo.

Grupos de informes e informes predefinidos

Los informes se organizan en grupos en la ventana **Informes** (en el panel de exploración izquierdo, **| Informes**). Los administradores pueden ver el contenido de todos los grupos de informes. System Manager incluye una función específica, llamada Informes, la cual permite que otros usuarios vean los informes sin brindarles acceso a otras funcionalidades de administración. (Para obtener más información, consulte "Administración basada en funciones"). Los usuarios con derecho de Informes también pueden ver y ejecutar informes, pero sólo en los dispositivos incluidos en su ámbito.

La ventana **Informes** tiene los grupos de informes siguientes:

- Hardware
- Software

Visualización de informes

En la ventana **Informes** se puede proceder a la ejecución de cualquiera de ellos.

En la ventana **Informes**, haga clic en un grupo de informes y luego en el informe que desee ejecutar. Los datos del informe aparecen en **Vista de informes**.

Acerca de la ventana Vista de informes

Los informes le ofrecen acceso rápido a una representación gráfica de los activos en los equipos cliente. Los informes se crean a partir de datos que almacena el rastreador en la base de datos. Podrá visualizar o imprimir los informes a través del explorador.

Para ver un informe

1. En el panel de exploración izquierdo, haga clic en **Informes**. Las categorías de informe aparecen en el panel derecho. Para ver la lista de informes, haga clic en un encabezado de categoría. El icono junto a cada informe indica el tipo de informe.

    Un informe con un icono gráfico a su lado se presenta como un gráfico circular o de barras (bi o tridimensional). En un gráfico, puede hacer clic en cualquier sección de círculo o barra coloreada y se desplazará a un resumen.

    Un informe con un icono de documento a su lado se presenta como texto.

2. Haga clic en el nombre del informe para visualizarlo.
3. Para los resúmenes de fechas de exploraciones de hardware o software, haga clic en las fechas de inicio y fin para establecer el período de tiempo, acto seguido haga clic en **Ejecutar**.

El informe Resumen del espacio en disco contiene datos que solamente se aplican a los dispositivos basados en Windows.

Para imprimir un informe, haga clic con el botón secundario del ratón en la página y haga clic en **Imprimir**. En el diálogo Imprimir, haga clic en **Imprimir**. Si un informe ocupa varias páginas, es necesario hacer clic con el botón derecho en cada página para imprimirlas.

Para distribuir un informe

- Para enviar un informe por correo electrónico, el método recomendado es imprimir el informe en un archivo con el formato .PDF e incluirlo al mensaje electrónico.

La consola presenta los gráficos de informes como gráficos circulares y de barras. Para definir el tipo de gráfico, haga clic en la lista desplegable del gráfico de informe y cambie el tipo de gráfico.

Para visualizar los gráficos de barras y circulares interactivos en varios informes, es necesario que Macromedia Flash Player* 7 esté instalado.

Consultas

Uso de las consultas

Las consultas son búsquedas personalizadas de las bases de datos centrales. Este producto ofrece herramientas que permiten crear consultas de base de datos de dispositivos que se encuentran en la base de datos central. Las consultas de la base de datos central se crean en la vista **Consulta**. Las consultas públicas de System Manager son visibles en LANDesk® Management Suite y viceversa, si se utilizan ambos.

Consulte esta sección para obtener información sobre:

Introducción a las consultas

Las consultas facilitan la administración de la red, ya que permiten buscar y organizar dispositivos en la base de datos central, en función del sistema operativo y los criterios de búsqueda especificados por el usuario.

Por ejemplo, puede crear y ejecutar una consulta que capture sólo los dispositivos con una velocidad de reloj de procesador inferior a 166 MHz, con menos de 64 MB de RAM o un disco duro inferior a 2 GB. Cree una o varias instrucciones de consulta que representen dichas condiciones y relacione las instrucciones entre sí utilizando operadores lógicos estándar. Al ejecutar las consultas, puede imprimir los resultados de la consulta y acceder y administrar los dispositivos que coincidan.

Grupos de consultas

Las consultas se pueden asociar a grupos en la vista **Mis dispositivos**. A éstos se le llaman grupos dinámicos, y el contenido de un grupo dinámico es el resultado de una consulta asociada con dicho grupo dinámico. Por ejemplo, un grupo que consta de todos los dispositivos de un área geográfica puede asociarse con una consulta en la memoria, el tamaño en el disco duro, etc.

Para obtener más información sobre cómo se muestran las consultas y grupos de consultas en la vista **Todos los dispositivos** y sobre qué puede hacer con ellos, consulte "Agrupación de dispositivos para ejecutar acciones".

Creación de consultas de base de datos

Utilice el cuadro de diálogo **Nueva consulta** para crear una consulta seleccionando atributos, operadores relacionales y valores de atributo. Cree una instrucción de consulta seleccionando un atributo de inventario y relacionándolo a un valor aceptable. Relacione de forma lógica las

instrucciones de consulta entre sí para garantizar que se evalúan como grupo antes de relacionarlas a otras instrucciones o grupos.

Para crear una consulta de base de datos

1. En la vista **Consultas** de la consola, haga clic en un **Nueva**.
2. Seleccione un **componente** de la lista de atributos del inventario.
3. Bajo **Paso 1: Condiciones de búsqueda**, haga clic en **Editar**.
    1. Desplácese por la lista para seleccionar los atributos de la condición de búsqueda. Por ejemplo, para localizar los equipos cliente que ejecutan un tipo concreto de software, seleccione Computer.Software.Package.Name.
    2. Tras seleccionar los atributos deseados, aparecerán una serie de campos en el lado derecho de la ventana. En estos campos, seleccione un operador y un valor para completar la condición de búsqueda. Por ejemplo, para localizar todos los equipos cliente que ejecutan Internet Explorer 5.0, los atributos serían "Computer.Software.Package.Name", el operador "=" y el valor "Internet Explorer 5".
    3. En la parte inferior de la ventana, haga clic en **Agregar** para rellenar el campo vacío con la condición de búsqueda creada.
    4. Para ajustar la consulta, cree otra condición de búsqueda y, a continuación, agréguela a la primera con un operador booleano (Y u O). Asimismo, utilice los botones adecuados para agregar, eliminar, sustituir, agrupar o desagrupar las condiciones de búsqueda creadas.
    5. Una vez que haya finalizado, haga clic en **Aceptar**.
4. Bajo **Paso 2: Atributos que se van a mostrar**, haga clic en **Editar**.
    1. Desplácese por la lista para seleccionar el atributo que desea mostrar en la lista de resultados de consulta. No olvide seleccionar los atributos que le ayudarán a identificar los equipos cliente devueltos en la consulta. Si no encuentra los atributos que desea visualizar, agréguelos en el cuadro de diálogo Atributos personalizados. No obstante, estos atributos deben asignarse a los equipos antes de que aparezcan en el cuadro de diálogo Consulta.

    2. Tras seleccionar un atributo, haga clic en **Agregar** para moverlo a un campo vacío en la parte inferior de la ventana. Para enumerar la lista de resultados de la consulta, haga clic en **Incluir recuento**.
    3. Repita el proceso si desea agregar más atributos. Utilice el botón **Eliminar** para eliminar atributos y haga clic en **Subir/Bajar** para cambiar el orden de los atributos.
    4. Haga clic en **Convertir resultados en destinos** para permitir que los resultados de la consulta puedan ser el destino de cualquier acción especificada.
    5. Una vez que haya finalizado, haga clic en **Aceptar**.
5. (opcional) Bajo **Paso 3: Ordenar resultados por atributo**, haga clic en **Editar** para personalizar el orden de los resultados de la consulta.
6. Si desea ejecutar la consulta más de una vez, haga clic en **Guardar consulta** u escriba un nombre único para la consulta. Si ejecuta la consulta antes de guardarla, se pierden los parámetros de la consulta y debe volver a crearse la misma para ejecutarla de nuevo.
7. Bajo **Paso 4: Ejecutar consulta**, haga clic en **Ejecutar consulta**.

Las instrucciones se ejecutan en el orden mostrado
Si no se realizan agrupaciones, las instrucciones de consulta enumeradas en el cuadro de diálogo se ejecutan en su totalidad. Asegúrese de agrupar los elementos de consulta

relacionados para que se evalúen como grupo; de lo contrario, los resultados de la consulta pueden ser diferentes a los esperados.

Ejecución de consultas

Para ejecutar una consulta

1. En el panel de exploración izquierdo, haga clic en **Consultas**.
2. Seleccione la consulta y haga clic en **Ejecutar**.

   o bien

   Para realizar cambios en la consulta antes de ejecutarla, haga doble clic en la consulta, haga clic en **Editar**, modifique los pasos del 1 al 3 y luego haga clic en **Ejecutar consulta**.

   Nota: Si ha modificado la consulta y desea guardar los cambios, haga clic en **Guardar consulta** para guardar los cambios o en **Guardar consulta como** para dar un nombre nuevo a la consulta modificada. Haga esto antes de ejecutar la consulta. Si no guarda los cambios antes de ejecutar la consulta, los mismos no se guardarán en la consulta.

3. Los resultados (dispositivos coincidentes) se muestran en el panel derecho de la vista **Todos los dispositivos**.

Importación y exportación de consultas

Puede utilizar la importación y exportación para transferir consultas de una base de datos central a otra. Las consultas exportadas se guardan como archivos XML.

Para importar una consulta

1. Haga clic con el botón secundario del ratón en el grupo de consultas en el que desea situar la consulta importada.
2. Seleccione **Importar** en el menú contextual.
3. Vaya a la consulta que desea importar y selecciónela.
4. Haga clic en **Abrir** para agregar la consulta al grupo seleccionado en la vista **Todos los dispositivos**.

Para exportar una consulta

1. Haga clic con el botón secundario del ratón en la consulta que desea exportar.
2. Seleccione **Exportar** en el menú contextual.
3. Vaya a la ubicación en la que desea guardar la consulta (como archivo .XML).
4. Escriba un nombre para la consulta.
5. Haga clic en **Guardar** para exportar la consulta.

Consultas personalizadas

Las consultas personalizadas resultan de gran utilidad cuando se desean obtener detalles de inventario sobre el hardware y el software instalado en los dispositivos. Una consulta personalizada permite generar una lista de equipos con inventarios similares. Las consultas personalizadas también se utilizan para definir grupos y ámbitos.

La página **Consultas personalizadas** (haga clic en **Consultas** en el panel de navegación) muestra una lista de las consultas guardadas. Para ejecutar una consulta guardada, seleccione la consulta y luego **Ejecutar**.

Si la lista de consultas abarca varias páginas, utilice las flechas de la parte superior de la página para navegar entre las páginas. Escriba la cantidad de elementos que se visualizarán en cada página y haga clic en **Establecer**.

Creación de consultas personalizadas

Las consultas personalizadas resultan de gran utilidad cuando se desean obtener detalles de inventario sobre el hardware y el software instalado en los dispositivos. Una consulta personalizada permite generar una lista de dispositivos con inventarios similares. Por ejemplo, si desea actualizar todos los dispositivos a un procesador de al menos 750 MHz, se pueden consultar en la base de datos los dispositivos con velocidades de procesador inferiores a 750 MHz. Las consultas personalizadas también se utilizan para definir grupos y ámbitos.

Se pueden realizar consultas sobre cualquiera de los elementos del inventario (conocidos como "atributos") que el rastreador de inventario almacena en la base de datos, así como cualquier atributo personalizado.

Administración de consultas

Administre las consultas en la vista **Consultas**. Esta página permite crear, editar y eliminar consultas:

- Para ejecutar una consulta existente, selecciónela y haga clic en **Ejecutar**.
- Para crear una consulta, haga clic en **Nueva**. Una vez haya creado y guardado la consulta, el nombre de ésta se mostrará en la lista de esta página.
- Para editar una consulta de la lista, haga doble clic en la misma. Se abre la página **Modificar consulta** con los parámetros de consulta que puede modificar.
- Para editar la consulta más reciente, haga clic en **Modificar consulta actual**.
- Para eliminar una consulta, selecciónela y haga clic en **Eliminar**.

Se requieren cuatro pasos para crear una consulta:

1. **Crear una condición de búsqueda:** Especifique un conjunto de atributos de inventario que servirá como base para la consulta.
2. **Seleccionar los atributos que se mostrarán:** Limite o "filtre" la consulta de modo que los resultados muestren los atributos más útiles como, por ejemplo, las direcciones IP o los nombres de dispositivos de los equipos.

3. **Ordenar los resultados por atributos (opcional):** Especifique cómo desea ordenar los resultados de la consulta. (Sólo se aplica si, en el paso 2, se seleccionó la visualización de más de un tipo de atributos en los resultados de la consulta.)
4. **Ejecutar la consulta:** Ejecute la consulta que se acaba de crear. También se puede guardar para utilizarla posteriormente, o borrar toda la información que incluya para comenzar de nuevo.

Paso 1: Creación de una condición de búsqueda (requerido)

Una condición de búsqueda es un conjunto de atributos de inventario y valores asociados sobre los que se realiza una consulta. La consulta puede estar formada por una sola condición de búsqueda o varias de ellas.

Los siguientes pasos corresponden a la página **Editar consulta**. En la vista **Ejecutar consultas**, haga clic en **Nueva** o bien, seleccione una consulta existente y haga clic en **Editar**.

Para crear una condición de búsqueda

1. En el **paso 1**, haga clic en **Editar**. Aparecerá una ventana en la que se muestra una lista que representa todos los datos de inventario que se encuentran actualmente en la base de datos.
2. Desplácese por la lista para seleccionar los atributos de la condición de búsqueda. Por ejemplo, para localizar los equipos cliente que ejecutan un tipo concreto de software, seleccione Computer.Software.Package.Name.
3. Tras seleccionar los atributos deseados, aparecerán una serie de campos en el lado derecho de la ventana. En estos campos, seleccione un operador y un valor para completar la condición de búsqueda. Por ejemplo, para localizar todos los equipos cliente que ejecutan Internet Explorer 5.0, los atributos serían "Computer.Software.Package.Name", el operador "=" y el valor "Internet Explorer 5".
4. En la parte inferior de la ventana, haga clic en **Agregar** para rellenar el campo vacío con la condición de búsqueda creada.
5. Para ajustar la consulta, cree otra condición de búsqueda y, a continuación, agréguela a la primera con un operador booleano (Y u O). Asimismo, utilice los botones adecuados para agregar, eliminar, sustituir, agrupar o desagrupar las condiciones de búsqueda creadas.
6. Una vez que haya finalizado, haga clic en **Aceptar**.

Para ejecutar y almacenar una consulta sobre el estado de la integridad de los servidores (Computer.Health.State), debe tener en cuenta que el estado se representa con un número en la base de datos. Utilice la tabla siguiente para crear condiciones de búsqueda. Por ejemplo, para crear una condición de búsqueda para equipos con una integridad "Desconocida", utilice el operador "NOT EXIST".

Condición de integridad	Operador
Desconocida	NOT EXIST

Condición de integridad	Operador
Normal	2
Advertencia	3
Crítica	4

Paso 2: Selección de los atributos que se van a mostrar (requerido)

En el paso 2, seleccione los atributos que resultarán más útiles para identificar los equipos devueltos en los resultados de la consulta. Por ejemplo, para obtener resultados que faciliten la localización física de los equipos que coincidan con los criterios de búsqueda definidos en el paso 1, se pueden especificar atributos como el nombre de visualización del equipo o la dirección IP.

Los siguientes pasos corresponden a la página **Editar consulta**.

Para seleccionar los atributos que se van a mostrar

1. En el **paso 2**, haga clic en **Editar**. Aparecerá una ventana en la que se muestra una lista que representa todos los datos de inventario que se encuentran actualmente en la base de datos.
2. Desplácese por la lista para seleccionar el atributo que desea mostrar en la lista de resultados de consulta. No olvide seleccionar los atributos que le ayudarán a identificar los equipos cliente devueltos en la consulta. Si no encuentra los atributos que desea visualizar, agréguelos en el cuadro de diálogo Atributos personalizados. No obstante, estos atributos deben asignarse a los equipos antes de que aparezcan en el cuadro de diálogo Consulta.

   Nota: Si utiliza una base de datos de Oracle, asegúrese de seleccionar, al menos, un atributo definido de forma nativa por el rastreador de inventario (por ejemplo, Computer.Display Name, Computer.Device Name, Computer.Device ID, Computer.Login Name, etc.).

3. Tras seleccionar un atributo, haga clic en **>>** para moverlo a un campo vacío en el lado derecho de la ventana. Para enumerar la lista de resultados de la consulta, haga clic en **Incluir recuento**.
4. Repita el proceso si desea agregar más atributos. Utilice los botones de flecha para agregar o eliminar atributos y haga clic en **Subir/Bajar** para cambiar el orden de los atributos.
5. Haga clic en **Convertir resultados en destinos** para permitir que los resultados de la consulta puedan ser el destino de cualquier acción especificada.
6. Una vez que haya finalizado, haga clic en **Aceptar**.

Asimismo, puede agregar encabezados de columna a la lista de resultados de consulta.

Para cambiar encabezados de columna (opcional)

1. En el **paso 2**, haga clic en **Editar**.
2. En el cuadro inferior, haga clic en un encabezado de columna y luego en **Editar**. Edite el encabezado y pulse **Intro**. Repita este paso las veces que sea necesario.
3. Haga clic en **Aceptar**.

Llegados a este punto, es adecuado que guarde la consulta; el procedimiento siguiente en el proceso de creación de consultas es opcional y se aplica sólo a los resultados de consultas que contienen dos o más columnas. Para guardar la consulta, haga clic en la opción **Guardar consulta** en la parte superior de la página. Se abre una ventana en la que se le solicita que escriba un nombre para la consulta. Escriba un nombre y, a continuación, haga clic en **Guardar** en la esquina superior derecha de la ventana.

Paso 3: Ordenar los resultados por atributos (opcional)

Este procedimiento es necesario sólo si se define más de un atributo y encabezado de columna en el paso 2 y se desea ordenar los resultados alfabética o numéricamente dentro de una de esas columnas.

Por ejemplo, digamos que especifica visualizar dos atributos diferentes en los resultados de consulta: la dirección IP y el tipo de procesador de cada equipo devuelto. En el paso 3, se puede ordenar los resultados alfabéticamente por tipo de procesador.

Si se salta este paso, la consulta se ordenará automáticamente por el primer atributo seleccionado en el paso 2.

Para ordenar los resultados por atributo

1. En el **paso 3**, haga clic en **Editar**. Aparecerá una ventana en la que se muestran los atributos seleccionados en el **Paso 2**.
2. Seleccione el atributo por el que desea realizar la ordenación y haga clic en **>>** para desplazarlo al cuadro de texto vacío.
3. Haga clic en **Aceptar**.

Paso 4: Ejecución de la consulta

Después de crear la consulta, es posible ejecutarla, guardarla o borrarla para comenzar de nuevo.

Para guardar la consulta con la finalidad de usarla en un futuro, haga clic en el botón **Guardar** de la barra de herramientas. La consulta se muestra en la lista de la página **Consultas personalizadas**. Si la consulta es una versión modificada de otra, haga clic en el botón **Guardar como** de la barra de herramientas para asignarle un nombre nuevo.

De forma predeterminada, sólo podrá visualizar las consultas guardadas por la persona que las guardó. Si activa **Consultas públicas** antes de guardarla, la consulta guardada estará disponible para todos los usuarios. Únicamente los administradores con derechos de administración de consultas públicas pueden hacer una consulta pública.

Si ha instalado varios productos de la familia de productos, las consultas se comparten entre ellos. Si guarda una consulta en la consola de un producto, la misma estará visible en las consolas de los otros productos.

Para ver los resultados de esta consulta, haga clic en el botón **Ejecutar** de la barra de herramientas.

Para borrar los parámetros de consulta de la página **Modificar consulta**, haga clic en el botón **Borrar** de la barra de herramientas. Si ya se ha guardado la consulta, se borrará de la página pero permanecerá en la lista **Consultas personalizadas**.

Visualización de resultados de consulta

Los resultados de la consulta coinciden con los criterios de búsqueda especificados en el proceso de generación de consultas. Si no se obtienen los resultados esperados, regrese a la página **Modificar consulta** y modifique los datos introducidos.

Para recibir más información sobre uno de los dispositivos en la lista de resultados de la consulta, haga doble clic en los datos de la consulta o en **Ver equipo** en el menú resultante.

En la página **Resultados de la consulta**, haga clic en el botón **Guardar como CSV** de la barra de herramientas para exportar los resultados en un formato compatible con hojas de cálculo u otras aplicaciones.

Para imprimir los resultados de la consulta, haga clic en **Vista preliminar** en la página de resultados de consulta.

Visualización de resultados de consulta detallados

Los resultados de la consulta coinciden con los criterios de búsqueda especificados en el proceso de generación de consultas. Si no se obtienen los resultados esperados, regrese a la página **Modificar consulta** y modifique los datos introducidos.

Para recibir más información sobre uno de los dispositivos en la lista de resultados de la consulta, haga doble clic en los datos de la consulta o en **Ver equipo** en el menú resultante.

Exportación de los resultados de la búsqueda a archivos CSV

Para ver los resultados de consulta en una aplicación de hoja de cálculo, exporte los datos como un archivo CSV (Valores separados por comas). En la página **Resultados de la consulta**, haga clic en el icono **Guardar como CSV** de la barra de herramientas para guardar la información como un archivo CSV. Puede utilizar una aplicación como Microsoft Excel* para importar y trabajar con el archivo CSV.

Cambio de encabezados de columnas de consulta

1. Abrir una consulta existente o crear una nueva consulta.
2. En el cuadro inferior, haga clic en un encabezado de columna y luego en **Editar**. Edite el encabezado y pulse **Intro**. Repita este paso las veces que sea necesario.
3. Haga clic en **Aceptar**.

Exportación e importación de consultas

Puede exportar e importar las consultas que ha creado. Todas las consultas se exportan como archivos XML. Si se exporta el mismo nombre de archivo de consulta más de una vez, se sobrescribirá el archivo existente. Para evitar esto, copie el archivo en otra ubicación tras exportarlo.

Las características de exportación e importación resultan útiles en dos escenarios:

- Si necesita reinstalar una base de datos, utilice las características de exportación e importación a fin de guardar las consultas existentes para su uso en una base de datos nueva.

  Por ejemplo, puede exportar las consultas y, a continuación, moverlas a un directorio que no se vea afectado por una reinstalación de la base de datos. Tras reinstalar la base de datos, puede volver a mover las consultas al directorio de consultas del servidor Web e importarlas a la base de datos nueva.
- Puede utilizar las funciones de exportación e importación para copiar consultas en otras bases de datos.

  Por ejemplo, puede exportar una consulta en un directorio de consultas del servidor Web y luego enviarlas a alguien por correo electrónico o a través de FTP. La persona que las reciba puede posteriormente situarlas en el directorio de consultas de otro servidor Web e importarlas a una base de datos diferente. Asimismo, se puede asignar una unidad y copiar las consultas directamente en el directorio de otro servidor Web.

Para exportar una consulta

Complete estos pasos mientras se encuentra conectado a una base de datos que tenga una consulta que desee exportar.

1. En el panel de exploración izquierdo, haga clic en **Consultas**.
2. En la página **Consultas personalizadas**, haga clic en el nombre de la consulta que desea exportar. Haga clic en **Editar**.
3. En la página **Modificar consulta**, haga clic en el botón **Exportar** de la barra de herramientas, para exportar la consulta a disco.
4. En la página **Consulta exportada**, haga clic con el botón secundario del ratón en la consulta para descargarla como un archivo XML en el directorio seleccionado. La consulta pasa a ser el archivo XML.

Observe que si se exporta el mismo nombre de archivo de consulta más de una vez, se sobrescribirá el archivo existente. Para evitar esto, copie el archivo en otra ubicación tras exportarlo.

Si más adelante desea volver a importar la consulta a una base de datos, deberá moverla al directorio de consultas reconocido por el servidor Web, de forma predeterminada, c:\inetpub\wwwroot\LANDesk\LDSM\queries.

Para importar una consulta

Complete estos pasos mientras se encuentra conectado a una base de datos a la que desea importar una consulta.

1. En el panel de exploración izquierdo, haga clic en **Consultas**.
2. En la página **Consultas personalizadas**, haga clic en **Nueva**.
3. En la página **Modificar consulta**, haga clic en el botón **Importar** de la barra de herramientas.
4. Seleccione la consulta que desea importar. Para comprobar los parámetros de esta consulta antes de importarla, haga clic en **Ver**.
5. Haga clic en **Importar** para cargar la consulta en la página **Modificar consulta**.
6. Una vez se haya cargado la consulta, desplácese hacia abajo y haga clic en **Guardar consulta** para guardarla en esta base de datos.

Administración del inventario

Puede emplear la utilidad de rastreo de inventario para agregar dispositivos a la base de datos central y recopilar datos del hardware y software de dispositivos. Puede visualizar, imprimir y exportar datos de inventario. Se puede además utilizar para definir consultas, agrupar dispositivos y generar informes especializados.

Consulte esta sección para obtener información sobre:

- Introducción al rastreo de inventario
- Visualización de datos del inventario

Introducción al rastreo de inventario

Al configurar un dispositivo con la función de configuración de dispositivos, el rastreador de inventario es uno de los componentes que se instala en el dispositivo. Durante la creación de la configuración del cliente, podrá especificar cuándo se ejecuta el rastreo de inventario en el dispositivo.

El rastreador de inventario se ejecuta automáticamente cuando el dispositivo se configura por primera vez. El archivo ejecutable del rastreador se denomina LDISCAN32.EXE en Windows y LDISCAN en Linux. 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. Para configurar la configuración de rastreo de software, en el servidor central, haga clic en **Inicio | Archivos de programa | LANDesk | Servicios de configuración de LANDesk**.

Para obtener más información sobre la configuración del servicio de inventario, consulte "Configuración del servicio de inventario", en el Apéndice C.

Tras el rastreo inicial, el rastreador de inventario se puede ejecutar desde la consola como tarea programada. El agente de administración estándar debe encontrarse en ejecución en los dispositivos remotos, a fin de programar un rastreo de inventario a los mismos.

Nota: Un dispositivo agregado a la base de datos central mediante la función de detección aún no ha rastreado los datos de su inventario en dicha base de datos. Deberá ejecutar un rastreo de inventario en cada dispositivo para que aparezcan todos los datos de dicho dispositivo.

Puede ver los datos de inventario y utilizarlos para:

- Personalizar las columnas de la lista **Todos los dispositivos** para mostrar atributos específicos del inventario
- Consultar la base de datos central en cuanto a los servidores con atributos específicos del inventario
- Agrupar dispositivos para acelerar tareas de administración
- Generar informes especializados según los atributos del inventario

- Realizar un seguimiento de los cambios de hardware y software en los dispositivos, así como para generar alertas o entradas en el archivo de registro cuando dichos cambios se produzcan.

Lea las secciones siguientes para obtener más datos sobre el funcionamiento del rastreador de inventario.

Rastreo delta

Tras el rastreo completo inicial en un dispositivo, la ejecución siguiente del rastreador de inventario sólo captura los cambios delta y los envía a la base de datos central. Utilice la opción del rastreador /RSS para recopilar información de software del registro de Windows.

Rastreo completo obligatorio

Si desea forzar un rastreo completo de los datos de hardware o software de un dispositivo, elimine el archivo de rastreo delta existente y cambie una opción en el subprograma **Configuración de servicios de LANDesk Software**.

1. Elimine el archivo **invdelta.dat** del servidor. El sistema almacenará de forma local una copia del último rastreo de inventario en el archivo oculto denominado invdelta.dat en la raíz del disco duro. (La variable de entorno LDMS_LOCAL_DIR define la ubicación de dicho archivo.)
2. Agregue la opción **/sync** a la línea de comandos de la utilidad de rastreo de inventario. Para editar la línea de comandos, haga clic en **Inicio | Todos los programas | LANDesk Management**, haga clic con el botón secundario del ratón en el icono de acceso directo **Rastreo de inventario** y seleccione **Propiedades | Acceso directo** y, a continuación, edite la ruta **Destino**.
3. En el servidor central, haga clic en **Inicio | Todos los programas | LANDesk |Configuración de servicios de LANDesk** .
4. Haga clic en la ficha **Inventario** y luego en **Configuración avanzada**.
5. Haga clic en la opción **Crear delta**. En el cuadro **Valor** escriba **0**.
6. Haga clic en **Aceptar** dos veces y haga clic en **Sí** cuando se presente el indicador a fin de reiniciar el servicio.

Compresión del rastreo

De forma predeterminada, los rastreos de inventario realizados por el rastreador de inventario de Windows (LDISCAN32.EXE) se comprimen. El rastreador comprime los rastreos completos y delta, utilizando una tasa de compresión de 8:1. En primer lugar, los rastreos se generan completamente en memoria; a continuación, se comprimen y se envían al servidor central utilizando un tamaño de paquete mayor, por lo que requiere un menor número de paquetes y se reduce el uso del ancho de banda.

Cifrado del rastreo

Los rastreos de inventario se cifran (sólo los rastreos de TCP/IP). Para desactivar el cifrado del rastreo de inventario, cambie una opción en el subprograma Configuración de servicios de LANDesk.

1. En el servidor central, haga clic en **Inicio | Todos los programas | LANDesk |Configuración de servicios de LANDesk** .
2. Haga clic en la ficha **Inventario** y luego en **Configuración avanzada**.
3. Haga clic en la opción **Deshabilitar cifrado**. En el cuadro **Valor** escriba **1**.
4. Haga clic en **Establecer** y luego en **Aceptar**.
5. Haga clic en **Aceptar** y haga clic en **Sí** cuando se presente el indicador a fin de reiniciar el servicio.

Visualización de datos del inventario

Una vez que se haya rastreado un dispositivo mediante el rastreador de inventario, puede visualizar la información del sistema en la consola.

Los inventarios del dispositivo se almacenan en la base de datos central; incluyen hardware, controladores de dispositivos, software, memoria e información del entorno. Puede utilizar el inventario para ayudar en la administración y configuración de dispositivos, así como para identificar rápidamente problemas del sistema.

Puede visualizar datos de inventario de las formas siguientes:

- Inventario resumen
- Inventario completo
- Visualización de las propiedades de atributos
- Información del sistema

Puede además visualizar datos de inventario en los informes que genere. Para obtener más información, consulte "Introducción a los informes".

Visualización del inventario de resumen en la consola de información del servidor

El inventario de resumen se encuentra en la página **Resumen** de la consola de información de servidor y proporciona una descripción breve sobre la información básica de la configuración del SO y del sistema correspondiente al dispositivo.

Nota: Si ha agregado un dispositivo a la base de datos central utilizando la herramienta de detección, los datos de su inventario aún no se han rastreado en la base de datos central. Debe ejecutar un rastreo de inventario en el servidor para que la función Inventario resumen finalice correctamente.

Para ver el inventario resumen:

1. En la vista **Todos los dispositivos** de la consola, haga doble clic en un dispositivo.
2. En el panel de exploración izquierdo, haga clic en **Información de sistema** y luego en **Resumen de sistema**.

Datos de resumen de servidor con Windows 2000/2003

Esta información aparecerá cuando visualice el inventario resumen en un servidor con Windows 2000/2003.

- **Condición:** Estado actual del servidor.
- **Tipo:** Tipo de servidor, tal como de aplicaciones, archivos, correo electrónico, etc.
- **Fabricante:** Fabricante del servidor.
- **Modelo:** Ttipo de modelo del servidor.
- **Versión de BIOS:** La versión del ROM BIOS.
- **Sistema operativo:** SO Windows o Linux que se ejecuta en el servidor: 2000, 2003 o Red Hat.
- **Versión de SO:** Número de versión del sistema operativo Windows 2000/2003 o Linux que se ejecuta en el dispositivo.
- **CPU:** Tipo de procesador o procesadores que se ejecutan en el servidor.
- **Rastreador de vulnerabilidades:** Versión del agente instalado.
- **Rastreador de inventario:** Versión del agente instalado.
- **Monitoreo:** Versión del rastreador de monitoreo instalado.
- **Último reinicio:** Ultima vez que se reinició el servidor.
- **Uso de la CPU:** Porcentaje del procesador actualmente en uso.
- **Memoria física utilizada:** Cantidad de memoria RAM disponible en el servidor.
- **Memoria Virtual utilizada:** Cantidad de memoria disponible en el servidor, incluida la RAM y la del archivo de intercambio.
- **Espacio de disco** El porcentaje del espacio en disco actualmente en uso. Si tiene más de una unidad de disco duro, se muestra cada una de ellas.

Los servidores habilitados para IPMI muestran datos adicionales específicos a IPMI. Los servidores Linux también muestran información adicional en la vista **Resumen**.

Visualización de un inventario completo

Un inventario completo proporciona una lista entera de los componentes detallados de hardware y software de un dispositivo. Dicha lista contiene objetos y atributos de objeto.

Para ver un inventario completo:

1. En la vista **Todos los dispositivos** de la consola, haga doble clic en un dispositivo.
2. En la ficha **Propiedades**, haga clic en **Ver inventario**.

Visualización de las propiedades de atributos

En la lista de inventario, puede ver las propiedades de los atributos de los objetos de inventario de un dispositivo. Estas propiedades le informarán de las características y valores de un objeto de inventario. Puede además crear atributos personalizados y editar otros definidos por el usuario.

Para ver las propiedades de un atributo, haga clic en el atributo en el panel izquierdo.

Para imprimir esta información en Internet Explorer, haga clic con el botón secundario en el marco y haga clic en **Imprimir**. Para imprimir en Mozilla, haga doble clic en el marco, haga clic en **Este marco | Guardar marco como** (This Frame > Save Frame As), luego haga clic en **Guardar** (Save), abra el archivo en una aplicación y haga clic en **Imprimir** (Print).

Información del sistema

En la consola de información del servidor podrá ver y modificar la información de sistema del dispositivo. La información que se incluye en **Hardware**, **Software**, **Registros** y **Otras categorías**, son ya sea datos almacenados o de tiempo real. Si hace clic en un enlace de información, podrá ver información detallada sobre el componente seleccionado y en los casos correspondientes, definir umbrales y especificar información.

1. En la vista **Todos los dispositivos** de la consola, haga doble clic en un dispositivo.
2. En el panel de exploración izquierdo de la consola de información del sistema, haga clic en **Información de sistema**.
3. Expanda el grupo y haga clic en el vínculo de información que desee ver.

Personalización de las opciones de inventario

La consola incluye la utilidad Configuración de servicios, la cual puede utilizar para personalizar las opciones de inventario. Los valores predeterminados de la mayoría de las opciones deben funcionar bien, pero si necesita cambiarlos puede utilizar esta utilidad. Para iniciar el subprograma Configuración de servicios en el servidor central, haga clic en **Inicio | Archivos de programa | LANDesk | LANDesk Configuración de servicios**. El nombre de archivo de la utilidad es svccfg.exe.

Utilice la utilidad Configuración de servicios para configurar:

- El nombre de la base de datos, el nombre de usuario y la contraseña
- El intervalo de la exploración del software de dispositivo, el mantenimiento y los días para llevar a cabo exploraciones de inventario y la longitud del historial del inicio de sesión en el cliente
- La administración de Id. de dispositivo duplicado
- La configuración del programador, incluidos la tarea programada y los intervalos de evaluación de consultas
- La configuración de tareas personalizadas, incluido el período de espera en ejecución remota

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

Edición del archivo LDAPPL3.TEMPLATE

La información relacionada específicamente con los parámetros de inventario del escáner está contenida en el archivo LDAPPL3.TEMPLATE. Este archivo de plantilla, junto con LDAPPL3.INI, identifica el inventario de software de un dispositivo. Este archivo se ubica en los dispositivos Windows administrados como parte de la configuración del agente. Sus parámetros se establecen en la ficha de Inventario de la Configuración del agente.

En los dispositivos Linux, un archivo de configuración similar (/etc/ldappl.conf) contiene información sobre los parámetros del rastreador. Puede editar este archivo para cambiar la forma en que funciona el rastreador. El archivo contiene instrucciones para la modificación del funcionamiento del rastreador en Linux.

Puede editar la sección [Inventario LANDesk] del archivo de plantilla para configurar los parámetros que determinan el modo en que el escáner identifica el inventario de software. De forma predeterminada, LDAPPL3.TEMPLATE se encuentra entre los archivos compartidos de LDLogon del servidor central.

Utilice esta tabla como guía de ayuda en la edición de la sección [LANDesk Inventory] en un editor de texto.

Opción	Descripción
Mode	Determina el modo en que el escáner explora el software en los dispositivos. El valor predeterminado es Listed. Los distintos valores son: • **Listed (En lista):** Registra los archivos contenidos en LDAPPL3. • **Unlisted (No en lista):** Registra los nombres y las fechas de todos los archivos con las extensiones que aparecen en la línea ScanExtensions pero que no están definidos en LDAPPL3. Este modo facilita la localización de software no autorizado en la red. • **Todos:** Detecta tanto los archivos que están en lista como los que no.
Duplicate	Registra varias instancias de los archivos. Defina el valor en OFF para registrar sólo la primera instancia, o en ON para registrar todas las instancias detectadas. El valor predeterminado es ON.
ScanExtensions	Define las extensiones de archivo (.EXE, .COM, .CFG, etc.) que se van a explorar. Utilice un espacio para separar las extensiones de archivo. De forma predeterminada, sólo se exploran los archivos .EXE.

Opción	Descripción
Versión	El número de versión del archivo LDAPPL3.
Revision	El número de revisión del archivo LDAPPL3; ayuda a garantizar la compatibilidad futura.
CfgFiles 1-4	Registra la fecha, hora, tamaño y contenido de los archivos especificados. No es necesario incluir la letra de la unidad (por ejemplo, C:) si se va a buscar en todas las unidades locales. Puede especificar más de un archivo en cada una de las cuatro líneas, pero la longitud de la línea se limita a 80 caracteres. Separe con un espacio los nombres de ruta que aparezcan en la misma línea. El rastreador compara la fecha y el tamaño del archivo actual con los del rastreo anterior. Si no coinciden, el rastreo registrará el contenido del archivo como una revisión nueva.
ExcludeDir 1-3	Excluye directorios específicos de una exploración. No es necesario incluir la letra de la unidad (por ejemplo, C:) si se van a excluir todas las unidades locales. La enumeración debe ser continua y comenzar por 1. Cada línea debe finalizar con "\".
MifPath	Especifica la ubicación de almacenamiento de los archivos MIF en una unidad local del equipo. La ubicación predeterminada es c:\DMI\DOS\MIFS.
UseDefaultVersion	Si se define en TRUE, el escáner informa de una coincidencia cuando el archivo coincide con una entrada de nombre y tamaño exactos en LDAPPL3 sólo en el nombre de archivo (la versión se informará como EXISTS). Esto puede ocasionar varios positivos falsos para aplicaciones que comparten un nombre de archivo común con una aplicación desconocida. En el archivo LDAPPL3.TEMPLATE (tal y como se proporciona), este parámetro está definido en FALSE; por tanto, sólo agregue una entrada si la coincidencia es exacta. Si falta el parámetro, el valor predeterminado será TRUE.
SendExtraFileData	Si se define en TRUE, envía datos de archivo adicionales al servidor central. El valor predeterminado es FALSE. Esto conlleva que, de forma predeterminada, sólo la ruta, el nombre y la versión se introducen en la base de datos central.

Para editar el archivo LDAPPL3.TEMPLATE

1. En el servidor central, vaya al directorio \Archivos de programa\LANDesk\ManagementSuite\LDLogon y abra LDAPPL3.TEMPLATE en el Bloc de notas o en otro editor de texto.
2. Desplácese hasta el parámetro que desea actualizar y realice los cambios correspondientes.
3. Guarde el archivo.

Actualización de la lista de aplicaciones

Los datos de la lista de aplicaciones, DEFAULTS.XML, se almacenan en la base de datos central. Debido a que los nombres y los números de versión de las aplicaciones de software de uso común cambian con frecuencia, LANDesk publica un nuevo archivo DEFAULTS.XML varias veces al año (en las versiones del software de LANDesk anteriores, este archivo era LDAPPL.INI).

Para actualizar la lista de aplicaciones

1. Descargue un nuevo archivo DEFAULTS.XML o LDAPPL3.TEMPLATE en http://www.landesk.com/support/downloads. Seleccione un producto y haga clic en **Actualización de software** para descargar el archivo.
2. Guarde el archivo en el directorio LDLOGON.
3. Siga las instrucciones incluidas en "Publicación de la lista de aplicaciones" para publicar un nuevo archivo LDAPPL3.INI.

Publicación de la lista de aplicaciones

La publicación de la lista de aplicaciones incluye la importación de la lista de aplicaciones más reciente de DEFAULTS.XML en la base de datos, y la posterior combinación de la lista de aplicaciones con el contenido de LDAPPL3.TEMPLATE para generar un archivo LDAPPL3.INI actualizado. La utilidad independiente COREDBUTIL.EXE que se encuentra en el directorio \Archivos de programa\LANDesk\ManagementSuite, se utiliza para realizar ambos pasos de forma automática.

Para publicar la lista de aplicaciones

1. Ejecute CoreDBUtil.exe
2. Haga clic en el botón **Publicar lista de aplicaciones**.

Publique la lista de aplicaciones tras modificar o descargar una versión actualizada de LDAPPL3.TEMPLATE o DEFAULTS.XML.

Configuración de hardware

Compatibilidad con Intel* AMT

System Manager es compatible con dispositivos que utilizan la tecnología Intel* Active Management (Intel* AMT), la cual es una funcionalidad de hardware y firmware que habilita la administración remota de dispositivos. Intel AMT utiliza una comunicación fuera de banda (OOB) para acceder a los dispositivos sin importar el estado del sistema operativo o la alimentación del dispositivo.

La compatibilidad con Intel AMT de este producto incluye las versiones 1 y 2. El proceso de incorporación de dispositivos Intel AMT 2 abarca algunas funciones nuevas que no se encuentran en la versión 1. Consulte Configuración de dispositivos Intel AMT para obtener detalles sobre la incorporación con la versión 2. La información de esta sección se aplica a ambas versiones, excepto cuando se indica lo contrario.

La herramienta de configuración de hardware incluye las funciones siguientes para la administración de dispositivos Intel AMT:

- Generación automática de identificaciones de incorporación (PID y PPS) (versión 2)
- Cambio del nombre de usuario y de la contraseña de los dispositivos administrados
- Configuración y habilitación de políticas de System Defense (versión 2)
- Configuración y habilitación de monitoreo de Agent Presence (versión 2)

Administración de dispositivos con o sin agentes de administración

Cuando los dispositivos se configuran con Intel AMT, está disponible una cantidad limitada de funciones de administración aunque no se haya instalado el agente de LANDesk en el dispositivo. Mientras los dispositivos se encuentren conectados a la red y tengan alimentación en espera, pueden detectarse y agregarse al inventario para que otros dispositivos en la red los administren.

Si un dispositivo tiene instalado Intel AMT, pero no el agente de administración, puede detectarse con una búsqueda de dispositivos no administrados y moverse a la base de datos de inventario para luego verlo en la lista **Mis dispositivos**. No obstante, muchas opciones de administración de System Manager no están disponibles. Estas opciones sólo están disponibles cuando el agente de LANDesk se encuentra instalado. Las funciones de administración que se encuentran disponibles para los dispositivos configurados para Intel AMT incluyen:

- **Resumen del inventario:** Un subconjunto de información de inventario normal puede consultarse y verse en tiempo real para el dispositivo, aún cuando el dispositivo se encuentre apagado.
- **Registro de sucesos:** Se puede ver en tiempo real un registro de sucesos específicos de Intel AMT, el cual muestra la gravedad y la descripción de los sucesos.

- **Administración de inicio remoto:** Se pueden realizar varios inicios y ciclos de alimentación desde la consola de alimentación remota, sin importar el estado de la alimentación o SO del dispositivo. Las opciones disponibles se basan en la compatibilidad de las opciones en el dispositivo. Algunos dispositivos pueden no ser compatibles con todas las opciones de inicio.
- **Forzar el rastreo de vulnerabilidades y deshabilitar la red de SO:** Si un dispositivo parece tener en ejecución algún software malintencionado, se puede ejecutar un rastreo de vulnerabilidades durante el siguiente reinicio; si fuera necesario, el acceso a la red a nivel de SO del dispositivo puede deshabilitarse para prevenir que se distribuyan en la red paquetes no deseados.

Si desea más información sobre las opciones de administración, consulte Administración de dispositivos Intel AMT.

Requisitos de incorporación de Intel AMT versión 1

Los dispositivos pueden detectarse como dispositivos Intel AMT sólo después de que se haya accedido a la Pantalla de configuración de Intel AMT en el dispositivo y se haya cambiado la contraseña predeterminada del fabricante a una contraseña segura. (Consulte la documentación del fabricante para la información sobre el acceso a la Pantalla de configuración de Intel AMT). Si aún no lo ha llevado a cabo, se detectarán los dispositivos pero no se identificarán los dispositivos de Intel AMT y no se podrá ver la misma información de inventario, como se podría en otra situación.

Para que el servidor central pueda autenticarse con los dispositivos de Intel AMT, las credenciales de nombre de usuario y contraseña deben coincidir con las credenciales que configure mediante la utilidad Configuración de servicios. Puede cambiar las credenciales utilizando la Pantalla de configuración de AMT.

Cuando el dispositivo Intel AMT se agrega a la base de datos central que se administrará, System Manager lo incorpora de forma automática en el modo seleccionado en la utilidad Configuración de servicios, sin importar si ya se incorporó. El modo Pequeños negocios proporciona una administración básica sin los servicios de infraestructura de red y no es seguro, mientras que el modo Empresa está diseñado para grandes empresas y utiliza DHCP, DNS y un servicio de autoridad de certificación TLS para garantizar la comunicación segura entre el dispositivo administrado y el servidor central.

Al incorporar un dispositivo Intel AMT en el modo empresarial, el servidor central instala un certificado en el dispositivo a fin de garantizar la comunicación segura. Si el dispositivo se administrará en otro servidor central, debe anularse la incorporación y volver a incorporarse mediante el nuevo servidor central. De no ser así, el acceso al dispositivo de Intel AMT no responderá debido a que el nuevo servidor central no tiene un certificado coincidente. De forma similar, si otro equipo intenta acceder a la funcionalidad de Intel AMT del dispositivo, no tendrá éxito debido a que no tiene un certificado coincidente.

Configuración de dispositivos Intel* AMT

Los dispositivos equipados con la funcionalidad de Intel AMT deben configurarse durante su instalación y encendido iniciales. El proceso de incorporación incluye varias medidas de seguridad que aseguran que solamente los usuarios autorizados tengan acceso a las funciones de administración de Intel AMT.

Los dispositivos Intel AMT se comunican con un servidor de incorporación de la red. El servidor de incorporación escucha los mensajes de los dispositivos Intel AMT de la red y permite que el personal de TI administre los servidores a través de la comunicación fuera de banda, independientemente del estado en que se encuentre el SO del dispositivo. !ProductName! actúa en calidad de servidor de incorporación para los dispositivos Intel AMT e incluye funciones que ayudan a incorporar los dispositivos cuando se configuran. A continuación, puede administrar los dispositivos con o sin agentes de administración de !ProductName! adicionales.

Esta sección describe el proceso recomendado para la configuración de nuevos dispositivos Intel AMT (versión 2). Durante este proceso, utilizará System Manager para generar un conjunto de identificadores de incorporación (PID y PPS). Cuando se escriben estos identificadores en la pantalla de configuración de Intel AMT del dispositivo, aseguran la conexión con el servidor de incorporación que está al tanto de los identificadores, de modo que el dispositivo Intel AMT pueda completar su proceso de incorporación inicial.

Los dispositivos con Intel AMT versión 1 utilizan un proceso similar pero no utilizan las claves PID y PPS. Consulte las notas que se encuentran al final de esta sección para obtener detalles.

Incorporación de dispositivos Intel AMT 2

Cuando se recibe un dispositivo Intel AMT 2, el técnico de TI ensambla el equipo y lo enciende. Tras encender el dispositivo, el técnico inicia una sesión en la pantalla de configuración de Intel ME (equipo de administración) basado en BIOS y cambia la contraseña predeterminada (admin) a una contraseña robusta. Esto permite el acceso a la pantalla de configuración de Intel AMT.

En la pantalla de configuración de Intel AMT, se escribe la siguiente información previa a la incorporación:

- Un identificador de incorporación (PID)
- Una clave de contraseña previa a la incorporación (PPS), también conocida como clave precompartida (PSK)
- La dirección IP del servidor de incorporación
- El puerto 9982 en calidad de puerto de comunicación del servidor de incorporación
- Debe seleccionarse el modo Empresa
- El nombre de host del dispositivo Intel AMT

La PPS debe ser conocida por el servidor de incorporación y por el dispositivo administrador, pero no puede transmitirse en la red por razones de seguridad. Debe escribirse de forma manual en el dispositivo (en la pantalla de configuración de Intel AMT) y almacenarse en el servidor de incorporación, el cual en este caso es también el servidor central de System Manager. Los pares PID/PPS son generados por System Manager y almacenados en la base de datos. Puede imprimir una lista de pares de identificadores generados para utilizarlos en la incorporación.

El técnico de TI debe escribir la dirección IP del servidor central de System Manager como servidor de incorporación y especificar el puerto 9982. Caso contrario, de forma predeterminada el dispositivo Intel AMT envía una transmisión general que puede recibirse si el servidor de configuración está escuchando en el puerto 9971.

El nombre de usuario y la contraseña predeterminados para el acceso a la pantalla de configuración de Intel AMT son "admin" y "admin". Durante el proceso de incorporación se cambian sus valores. El nombre de usuario puede quedar igual pero debe cambiarse la

contraseña por una robusta. La nueva combinación de nombre de usuario y contraseña se escribe en la utilidad Configuración de servicios que se incluye con System Manager, tal como se describe en los pasos de procedimiento más adelante. Después de configurar cada uno de los dispositivos, puede cambiar el nombre de usuario y la contraseña de forma individual para cada dispositivo, pero para fines de incorporación, se utiliza el nombre de usuario y la contraseña que se encuentran en Configuración de servicios.

Después de introducir la información anterior en la pantalla de configuración de Intel AMT, el dispositivo envía mensajes de "saludo" cuando se conecta a la red por primera vez, en un intento por comunicarse con el servidor de incorporación. Si el servidor de incorporación recibe el mensaje, se inicia el proceso de incorporación una vez que el servidor establece conexión con el dispositivo administrado.

Cuando el servidor central recibe el mensaje de saludo y verifica las claves PID/PPS, incorpora el dispositivo Intel AMT en el modo TLS. El modo TLS (seguridad de nivel de transporte) establece un canal seguro de comunicación entre el servidor central y el dispositivo administrado mientras se completa la incorporación. Este proceso incluye la creación de un registro en la base de datos con el UUID y las credenciales cifradas del dispositivo. Una vez que los datos del dispositivo se encuentran en la base de datos, el dispositivo figura en la lista de dispositivos no administrados.

Una vez que el servidor central ha incorporado un dispositivo Intel AMT, éste puede administrarse solamente a través de la funcionalidad de Intel AMT. Puede seleccionarlo en la lista de dispositivos no administrados y agregarlo a los dispositivos administrados. También puede implementar los agentes de administración de System Manager en el dispositivo para utilizar un conjunto mayor de funciones de administración.

El proceso recomendado para el uso de System Manager en la incorporación de dispositivos Intel AMT 2 es el siguiente. Las instrucciones específicas para los elementos 1 y 2 se proporcionan en los pasos de procedimiento siguientes.

1. Ejecute la utilidad Configuración de servicios a fin de especificar una contraseña nueva y robusta para la incorporación de dispositivos Intel AMT. (Consulte los pasos detallados a continuación).
2. Utilice System Manager para generar un lote de identificadores de incorporación de Intel AMT (PID y PPS) e imprimir la lista de claves. (Consulte los pasos detallados a continuación).
3. Inicie una sesión en la pantalla de configuración de Intel ME del dispositivo desde el BIOS y cambie la contraseña predeterminada a una contraseña robusta.
4. Inicie una sesión en la pantalla de configuración de Intel AMT. Escriba el par de claves PID/PPS de la lista de identificadores de incorporación que imprimió. Escriba la dirección IP del servidor central (servidor de incorporación) y especifique el puerto 9982. Asegúrese de que esté seleccionado el modo Empresa para la incorporación. Escriba el nombre de host del dispositivo Intel AMT.
5. Después de que cierra la pantalla del BIOS, el dispositivo empieza a enviar mensajes de "saludo".
6. El servidor central recibe un mensaje de "saludo" y verifica la PID/PPS con la lista de claves generadas, y si la clave coincide, incorpora el dispositivo en el modo TLS.
7. El dispositivo se agrega a la lista de detección de dispositivos no administrados.
8. Seleccione el dispositivo y agréguelo a la lista de dispositivos administrados. De forma predeterminada, se administrará como dispositivo sin agentes y podrá implementar agentes de administración en él.

Para definir el nombre de usuario y la contraseña de Intel AMT en Configuración de servicios

1. En el servidor central, haga clic en **Inicio |** LANDesk **| Configuración de servicios**.
2. Haga clic en la ficha **Configuración de Intel AMT**.
3. Escriba **admin** como el nombre de usuario y la contraseña bajo **Credenciales actuales de Intel AMT**.
4. Escriba un nombre de usuario nuevo (opcional) y una contraseña robusta bajo **Configurar con las nuevas credenciales de Intel AMT**.
5. Haga clic en **Aceptar**.

Los campos de nombre de usuario y contraseña deben completarse aquí para que pueda generar un lote de identificadores de incorporación.

Para generar un lote de identificadores de incorporación de Intel AMT

1. En el servidor central, haga clic en **Configuración de hardware** en el panel de navegación izquierdo.
2. Amplíe **AMT** y aumente el detalle hasta llegar a **Proveyendo** y **Generar IDs de AMT**.
3. Escriba la cantidad de identificadores que generar (por lo general, es la cantidad de dispositivos que planea incorporar).
4. Si desea utilizar un prefijo diferente para las PID, escríbalo en el cuadro de texto **Prefijo de PID**. Este prefijo solamente puede contener caracteres alfabéticos en mayúsculas y números del conjunto de caracteres ASCII. Puede escribir un máximo de 7 caracteres en el prefijo.
5. Escriba el nombre del lote para identificar el grupo de identificadores generados.
6. Marque la opción **Mostrar los IDs de AMT generados** para mostrar los identificadores generados en la lista. Si no marca esta opción, los identificadores se generan y se guardan en la base de datos pero no se visualizan ahí.
7. Haga clic en **Generar IDs**.
8. Tras generar los identificadores, haga clic en **Imprimir lista de ID** para abrir una ventana nueva con la lista de identificadores. Solamente los identificadores que figuran en la lista se muestran en la ventana nueva. Utilice la función de impresión del explorador para imprimir la lista.
9. Para ver todos los identificadores que se han generado con anterioridad, deje el cuadro **Nombre de lote** en blanco y haga clic en **Ver IDs de lotes**.
10. Para ver un lote de identificadores generados, escriba el nombre del lote en el cuadro de texto **Nombre de lote** y haga clic en **Ver IDs de lotes**

Puede generar cualquier cantidad de claves de incorporación a la vez. Las claves se almacenan en la base de datos para referencia futura al incorporar nuevos dispositivos de Intel AMT. A medida que incorpora los dispositivos y se consumen las claves de incorporación, la página **Generar IDs de AMT** sombrea los identificadores que se han consumido para que pueda controlar los identificadores que se han utilizado.

Se agrega un prefijo de PID para facilitar la identificación de ID y PID, pero el uso del prefijo no es requerido. Es recomendable que se utilicen de 0 a 4 caracteres en el prefijo, con un máximo de 7 caracteres.

Para identificar los lotes de claves de incorporación, especifique un nombre de lote. Debe ser un nombre descriptivo que indique los dispositivos a los cuales se aplican los identificadores. Por

ejemplo, puede generar lotes para cada organización de la empresa y nombrar los lotes Desarrollo, Mercadeo, Finanzas, etc. Si más adelante desea ver los identificadores generados, escriba el nombre del lote y haga clic en **Ver IDs de lotes** para ver una lista que contenga solamente esos identificadores.

Contraseñas robustas

Intel AMT requiere el uso de una contraseña robusta para la habilitación de una comunicación segura. Las contraseñas deben satisfacer estos requisitos:

- Contar con al menos 8 caracteres
- Al menos un carácter numérico (0-9)
- Al menos un carácter ASCII que no sea alfanumérico (tal como !, &, %)
- Deben incluirse caracteres latinos en mayúsculas y minúsculas o caracteres que no sean ASCII (UTF+00800 y superior)

Errores en el proceso de incorporación

Si escribe una PID y una PPS que no forman un par correctamente (por ejemplo, la PPS debe formar un par con otra PID), recibirá un mensaje de error en el registro de alertas y no continuará la incorporación de dicho dispositivo. Debe reiniciar el dispositivo y volver a escribir el par PID/PPS correcto en la pantalla de configuración de Intel AMT.

Si al escribir una PID, la pantalla de configuración de Intel AMT muestra un mensaje de error, quiere decir que no ha escrito bien la PID. Se realiza una suma de comprobación para asegurarse de que la PID sea correcta.

Detección de dispositivos Intel AMT 1.0

Al ejecutar un rastreo de detección de dispositivos, los dispositivos Intel AMT versión 1 se detectan y se agregan a la carpeta Intel AMT de la lista de dispositivos **No administrados**. Los dispositivos se reconocen como dispositivos Intel AMT si se han configurado con un nombre de usuario y una contraseña que son seguros, para reemplazar los definidos por el fabricante.

Cuando agrega un nombre de usuario y una contraseña seguros a la pantalla de configuración de Intel AMT, también puede escribir la dirección IP del servidor de incorporación y especificar el puerto 9982, tal como se hace con los dispositivos Intel AMT 2. No obstante, no se utilizan pares PID/PPS en la incorporación de dispositivos Intel AMT 1. Si especifica una dirección IP de un servidor de incorporación, el servidor central funciona como servidor de incorporación y puede administrar el dispositivo en calidad de dispositivo sin agentes.

Observe que Intel AMT versión 1 no utiliza el mismo nivel de seguridad que la versión 2. Intel recomienda que los dispositivos de la versión 1 se configuren en una red aislada y segura. Tras completar la configuración, pueden trasladarse a una red menos segura para su administración.

Cambio del nombre de usuario y la contraseña de los dispositivos Intel* AMT

Se requiere un nombre de usuario y una contraseña para incorporar nuevos dispositivos Intel AMT (versión 1). Para los dispositivos que administrará con System Manager, el nombre de usuario y la contraseña que escribe en la pantalla de configuración de Intel AMT deben coincidir con los escritos en la utilidad Configuración de servicios de System Manager. El nombre de usuario y la contraseña de la utilidad Configuración de servicios se guardan en la base de datos y se aplican en forma global en la incorporación de dispositivos Intel AMT.

Intel AMT requiere el uso de una contraseña robusta para la habilitación de una comunicación segura. Las contraseñas deben satisfacer estos requisitos:

- Al menos 8 caracteres de longitud
- Al menos un carácter de número (0-9)
- Al menos un carácter ASCII que no sea alfanumérico (tal como !, &, %)
- Deben incluirse caracteres latinos en mayúsculas y minúsculas o caracteres que no sean ASCII (UTF+00800 y superior)

Tras la incorporación, debe cambiar los nombres de usuario y las contraseñas con regularidad como parte del mantenimiento de TI. Puede utilizar una combinación distinta de nombre de usuario y contraseña para cada dispositivo Intel AMT o aplicar una sola combinación de nombre de usuario y contraseña en varios dispositivos. Las combinaciones nuevas de nombre de usuario y contraseña que escribe en la página de configuración de hardware se almacenan en la base de datos y son utilizadas por System Manager para comunicarse de forma segura con los dispositivos Intel AMT administrados.

Para cambiar el nombre de usuario y la contraseña de los dispositivos Intel AMT

1. En el servidor central, haga clic en **Configuración de hardware** en el panel de navegación izquierdo.
2. Amplíe **AMT** y aumente el detalle hasta llegar a **Configuración**.
3. En la lista **Todos los dispositivos**, seleccione uno o más dispositivos en los cuales desee cambiar el nombre de usuario y la contraseña. Haga clic en **Destino** en la barra de herramientas.
4. En el panel inferior, escriba el nuevo nombre de usuario, y escriba y confirme la nueva contraseña.
5. Haga clic en **Dispositivos de destino** y luego en **Aplicar**.

   Para un solo dispositivo o para varios dispositivos de la misma lista, seleccione los dispositivos y haga clic en **Dispositivos seleccionados** y luego haga clic en **Aplicar**.

Configuración de políticas de System Defense

Intel AMT* 2.0 incluye una función de System Defense, la cual impone las políticas de seguridad de red en los dispositivos con la funcionalidad Intel AMT 2.0. Puede seleccionar y aplicar las políticas de System Defense en los dispositivos administrados mediante la herramienta **Configuración de hardware**.

Si se aplica una política de System Defense a un dispositivo Intel AMT, el dispositivo filtra los paquetes de red entrantes y salientes según las políticas definidas. Cuando el tráfico de red coincide con las condiciones de alerta definidas en un filtro, se genera una alerta y se bloquea el acceso a la red. A continuación, se aísla el dispositivo de la red hasta que se realicen los pasos de reparación de la política.

System Manager contiene políticas de System Defense predefinidas que puede aplicar a los dispositivos Intel AMT. Cada una de las políticas contiene un conjunto de filtros que definen el tipo de tráfico de red que no se permite y las acciones resultantes cuando el tráfico cumple el criterio del filtro. El proceso de selección y aplicación de políticas es el siguiente:

1. Defina uno o más dispositivos de destino
2. Seleccione la directiva de System Defense que desee aplicar y edítela de ser necesario.
3. Aplique la política a los dispositivos de destino

Cuando una política de System Defense se encuentra activa en un dispositivo administrado, el dispositivo supervisa todo el tráfico de red entrante y saliente. Si se detectan las condiciones de un filtro, se realizan las acciones siguientes:

1. El dispositivo administrado envía una alerta ASF al servidor central y se agrega una entrada al registro de alertas
2. El servidor central determina la política que se ha violado y desactiva el acceso a la red en el dispositivo administrado
3. El dispositivo figura en la cola de reparación de System Defense (en la herramienta **Configuración de hardware**)
4. Para restaurar el acceso a la red en el dispositivo, el administrador realiza los pasos de reparación debidos y elimina el dispositivo de la cola de reparación; de este modo se restaura la política de System Defense original en el dispositivo.

Este proceso se describe con mayor detalle en las secciones siguientes.

Selección y aplicación de políticas de System Defense

System Manager contiene las políticas de System Defense predefinidas siguientes, las cuales pueden aplicarse a los dispositivos Intel AMT 2.0. Las políticas se definen con parámetros como el número de puerto, el tipo de paquete y la cantidad de paquetes durante un lapso de tiempo específico. Cuando se activa una política, ésta se registra con Intel AMT en los dispositivos que ha seleccionado. Las políticas se guardan como archivos XML en la carpeta CircuitBreakerConfig del dispositivo administrado.

- **BlockFTPSrvr:** Esta política impide el tráfico a través de un puerto FTP. Cuando se envían o reciben paquetes en el puerto FTP 21, se descartan los paquetes y se suspende el acceso a la red.
- **LDCBKillNics:** Esta política bloquea el tráfico en todos los puertos de red con excepción de los puertos de administración siguientes:

Descripción del puerto	Intervalo de números	Dirección del tráfico	Protocolo

Descripción del puerto	Intervalo de números	Dirección del tráfico	Protocolo
Administración de LANDesk	9593-9595	Envío y recepción	TCP, UDP
Administración de Intel AMT	16992-16993	Envío y recepción	Sólo TCP
DNS	53	Envío y recepción	Sólo UDP
DHCP	67-68	Envío y recepción	Sólo UDP

Cuando el servidor central desactiva el acceso a la red en un dispositivo administrado, en realidad aplica esta política al dispositivo. A continuación, cuando el dispositivo se elimina de la cola de reparación, la política original se vuelve a aplicar al dispositivo.

- **LDCBSYNFlood:** Esta política detecta un ataque de denegación de servicio de desborde SYN: no permite más de 10.000 paquetes TCP con el indicador SYN activado, en un minuto. Si se excede esta cantidad, se suspende el acceso a la red.
- **UDPFloodPolicy:** Esta política detecta un ataque de denegación de servicio de desborde UDP: no permite más de 20.000 paquetes UDP por minuto en los puertos numerados del 0 al 1023. Si se excede esta cantidad, se suspende el acceso a la red.

Para seleccionar una política de System Defense

1. Haga clic en **Configuración de hardware** en el panel de navegación izquierdo.
2. Haga clic en **AMT** y aumente el detalle en el árbol hasta llegar a **Directivas**.
3. En la lista de dispositivos, seleccione los dispositivos en los cuales desee aplicar la política (utilice Ctrl+clic o Mayús+clic para seleccionar varios dispositivos).
4. Haga clic en el botón **Destino** de la barra de herramientas para agregar el dispositivo a la lista **Dispositivos de destino**.
5. En el panel inferior, seleccione una política en la lista desplegable.
6. Haga clic en **Dispositivos de destino** y luego en **Aplicar**.

Restauración del acceso a la red en los dispositivos que figuran en la cola de reparación

Si se suspende el acceso a la red de un dispositivo debido a una politica de System Defense, el dispositivo figura en la cola de reparación. Permanece ahí hasta que lo elimina de la lista, lo cual restablece la política activa en el dispositivo. Antes de hacerlo, debe resolver el problema que colocó al dispositivo en la cola. Por ejemplo, si se detectó tráfico FTP, debe verificar que se tomen las medidas debidas para impedir que haya más tráfico FTP en el dispositivo.

Para eliminar un dispositivo de la cola de reparación

1. Haga clic en **Configuración de hardware** en el panel de navegación izquierdo.
2. Haga clic en **AMT** y aumente el detalle en el árbol hasta llegar a **Reparación**.

3. Seleccione los dispositivos cuya política de System Defense puede restaurarse y haga clic en **Eliminar**.

Configuración de Agent Presence de Intel* AMT

Intel* AMT 2.0 incluye la herramienta de seguridad Agent Presence que supervisa la presencia de los agentes de software en los dispositivos administrados. Puede habilitar la supervisión de Agent Presence para asegurarse de que los agentes de administración que se encuentran en los dispositivos se ejecuten de forma continua, y para recibir alertas cuando un agente se detenga aunque otros agentes basados en software no puedan detectar el problema.

System Manager utiliza Agent Presence de Intel AMT para supervisar dos agentes: el agente de administración estándar y el servicio de supervisión. Resulta útil en situaciones en las cuales no está disponible la comunicación de supervisión normal. Por ejemplo, el nivel de comunicación de un dispositivo podría dejar de funcionar o el agente de supervisión mismo podría haber detenido su ejecución. De forma predeterminada, Agent Presence también supervisa su propio proceso de supervisión de modo que se envían alertas si detiene su ejecución.

La supervisión de Agent Presence se realiza mediante la configuración de un temporizador que escucha los mensajes de "transacción de control" provenientes de los agentes de administración en el dispositivo, para verificar que los agentes estén en ejecución. Si un temporizador caduca debido a que no ha recibido un mensaje de transacción de control, Intel AMT envía una alerta al servidor central.

Al configurar Agent Presence, el agente del dispositivo se registra con Intel AMT para enviar las transacciones de control directamente a Intel AMT; si las transacciones de control se detienen, Intel AMT puede enviar alertas al servidor central a través de la comunicación fuera de banda para indicar que el agente no responde. Intel AMT envía una alerta de captura de evento de plataforma (PET) al servidor central con una descripción del estado modificado. De forma predeterminada, esta alerta se registra con la integridad del dispositivo. Puede configurar otras acciones de alerta para que se inicien cuando se recibe la alerta (si desea información sobre la configuración de acciones de alerta, consulte Configuración de acciones de alerta).

Al configurar la supervisión de Agent Presence, puede activar o desactivar la supervisión de dos agentes y definir los valores siguientes:

- **Transacción de control:** cantidad máxima de tiempo (en segundos) que puede transcurrir entre las señales de transacción de control. Si se excede este límite de tiempo sin que se reciba una nueva transacción de control, se considera que el agente no está respondiendo. El valor predeterminado es de 120 segundos para el agente de administración estándar y de 180 segundos para el servicio de supervisión; el valor mínimo para ambos es de 30 segundos.
- **Tiempo de inicio:** cantidad máxima de tiempo (en segundos) que puede transcurrir después del inicio del sistema operativo antes de que se reciba una transacción de control del agente. Si se excede este tiempo límite, se considera que el agente no está respondiendo. Agent Presence se configura en Intel AMT durante la instalación del agente, de modo que debe permitirse tiempo suficiente para que el agente empiece a ejecutarse y envíe la primera transacción de control. El valor predeterminado es de 360 segundos y el valor mínimo es de 30 segundos.

Para editar la configuración de Agent Presence de Intel AMT

1. Haga clic en **Configuración de hardware** en el panel de navegación izquierdo.
2. Amplíe **AMT** y aumente el detalle en el árbol hasta llegar a **Configuración de AP**.
3. Para desactivar la supervisión de Agent Presence en Intel AMT 2.0, desmarque la casilla **Activar la supervisión de Agent Presence**.
4. Para desactivar la supervisión de un agente específico, desmarque la casilla situada junto al nombre del agente. Aunque se desmarquen ambas casillas, Agent Presence continuará supervisando su propio proceso de supervisión siempre que esté activado.
5. Escriba un valor nuevo en el cuadro de texto **Transacción de control** para cambiar el tiempo máximo permitido entre las transacciones de control (mínimo de 30 segundos).
6. Escriba un valor nuevo en el cuadro de texto **Tiempo de inicio** para cambiar el tiempo máximo que se permite para que el agente envíe la primera transacción de control después del inicio del sistema operativo en el dispositivo (el mínimo es de 30 segundos y se recomiendan 120 segundos).

Compatibilidad con IPMI

System Manager incluye compatibilidad con Intelligent Platform Management Interface (IPMI) 1.5 y 2.0. 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 supervisión y recuperación que permiten el acceso a varias funciones independientemente de si el equipo está encendido o no, o del estado del SO. Si desea más detalles sobre IPMI, visite el sitio Web de Intel.

La supervisión IPMI es manejada por el BMC (controlador de administración de placa base). BMC funciona con alimentación en espera y consulta el estado del sistema de forma autónoma. Si BMC detecta que existen elementos fuera del rango, puede configurar las acciones IPMI resultantes, tal como el registro del evento, la generación de alertas o la realización de acciones de recuperación automática, tales como el encendido o el restablecimiento del sistema.

SMBIOS 2.3.1 o superior debe estar instalado a fin de que se pueda detectar BMC en el sistema. Si no se detecta BMC, podría omitirse cierta información de IPMI en los informes, las exportaciones, etc.

IPMI define interfaces comunes en el hardware utilizado para supervisar las características de integridad física, tales como la temperatura, el voltaje, los ventiladores, las fuentes de alimentación y la intrusión del chasis. Además de la supervisión de la integridad, IPMI incluye otras capacidades de administración del sistema, que incluyen las alertas automáticas, el apagado y reinicio automático del sistema, las capacidades de reinicio y control de energía remotos, y el seguimiento de activos.

Las opciones de menú de System Manager varían ligeramente en dispositivos habilitados para IPMI, según el estado del sistema operativo.

Funciones de administración en dispositivos habilitados para IPMI

La supervisión de las capacidades depende de lo que se encuentre instalado en el dispositivo que se supervisa, al igual que del estado del dispositivo. Cualquier dispositivo habilitado para IPMI con un BMC (Baseboard Management Controller) se puede supervisar con la consola del administrador de forma limitada sin agentes de administración adicionales tras la configuración del BMC. Esto incluye la administración fuera de banda cuando el dispositivo está apagado o el SO no está funcionando. La administración con todas las funciones está disponible si se instala el agente de administración, BMC está presente, el dispositivo está encendido y el SO está funcionando. La tabla siguiente compara la funcionalidad disponible con estas configuraciones.

	Sólo BMC*	**BMC + agente**	**Agente (no IPMI)**
Administración fuera de banda activada	X	X	
Administración en banda activada		X	X
Se puede detectar el dispositivo**	X	X	X
Lectura de detectores de entorno	X	X	Depende del hardware
Apagado y encendido remoto	X	X	X
Lectura y borrado del registro de eventos	X	X	
Configuración de alertas	X	X	X
Lectura de información de SO		X	X
Apagado normal		X	X
Lectura de información de SMBIOS (procesador, ranuras, memoria)		X	X

	Sólo BMC*	BMC + agente	Agente (no IPMI)
Sincronización IP (SO a BMC)		X	
Temporizador de vigilancia		X	
BMC se comunica con el servidor central	X	X	
Los componentes locales de System Manager se comunican con el servidor central		X	X
Gama completa de funciones de administración de System Manager		X	

*BMC estándar. Mini BMC es una versión reducida de BMC. Tiene la funcionalidad mencionada con las limitaciones siguientes:

- No es compatible con el redireccionamiento serie a través de LAN (SOL)
- Solamente tiene un nombre de usuario para la administración de BMC
- Utiliza solamente un canal para la comunicación con BMC
- Tiene un depósito para el registro de eventos del sistema (SEL)

**Si el BMC no está configurado, no responderá a los pings ASF que el producto utiliza para detectar IPMI. Esto significa que tendrá que detectarlo como un equipo normal. Cuando implementa automáticamente un agente de administración, la configuración del servidor rastrea el sistema, detecta si se trata de IPMI y configura el BMC.

Conflictos con otros controladores IPMI

Si ha instalado otro software de administración que incluye los controladores IPMI en los dispositivos que desea administrar con System Manager, debe desinstalar dichos productos para que pueda implementar los agentes de Management Suite con las funciones de administración de IPMI.

Por ejemplo, Microsoft* Windows* Server 2003 incluye compatibilidad con IPMI a través de la instalación de Windows Remote Management (WinRM), que incluye un proveedor de Windows Management Instrumentation (WMI) y un controlador IPMI. No obstante, System Manager no admite la instalación de dicho controlador de IPMI e instala su propio controlador IPMI. Si se ha instalado WinRM en un dispositivo que desee administrar con System Manager, primero debe desinstalar WinRM a través de la función Agregar o quitar programas de Windows (**Inicio | Panel de control | Agregar o quitar programas | Agregar o quitar componentes de Windows |**

Herramientas de administración y supervisión | desmarque la casilla **Administración de hardware** y haga clic en **Aceptar**).

Configuración de IPMI BMC

Utilice la página **Configuración de IPMI BMC** para personalizar las opciones de comunicación con los dispositivos habilitados para IPMI. Las funciones descritas a continuación están disponibles para dispositivos en banda; si un dispositivo está fuera de banda, solamente está disponible la configuración de alimentación del usuario BMC.

PRECAUCIÓN: Se recomienda enfáticamente que no cambie la configuración de IPMI a menos que esté familiarizado con la especificación IPMI y entienda las tecnologías pertinentes a estas opciones. El uso indebido de estas opciones de configuración podría evitar que System Manager se comunique satisfactoriamente con los dispositivos habilitados para IPMI.

Están disponibles las siguientes opciones de configuración:

- Temporizador de vigilancia
- Configuración de alimentación
- Configuración de usuario
- Contraseña BMC
- Configuración de LAN
- Configuración de SOL
- Configuración de IMM

Cambio de la configuración del temporizador de vigilancia

IPMI provee una interfaz para el temporizador de vigilancia BMC. Se puede definir el temporizador para que se agote de forma periódica e inicie ciertas acciones al agotarse (tal como un ciclo de energía). Se ha configurado System Manager para que restablezca el temporizador de forma periódica de modo que no se agote; si el dispositivo deja de estar disponible (por ejemplo se apaga o se bloquea), el temporizador no se restablece y se agota, lo cual inicia la acción.

Puede especificar el lapso de tiempo que debe transcurrir para que se agote el temporizador y seleccionar una acción a realizar si se agota. Puede elegir entre no realizar ninguna acción, realizar un restablecimiento de hardware (apagado y reinicio) en el dispositivo, apagar el dispositivo normalmente o ejecutar un ciclo de energía (apagado normal seguido del reinicio).

También puede definir el BMC para que detenga la transmisión de mensajes de ARP (protocolo de resolución de direcciones) mientras el temporizador de vigilancia esté activado, lo cual puede reducir la cantidad de tráfico de red que se genera. Si se suspenden los ARP, se reanudarán éstos de forma automática si se agota el temporizador de vigilancia.

Para cambiar la configuración del temporizador de vigilancia

1. En la vista **Mis dispositivos**, haga doble clic en el dispositivo que desee configurar.

2. En el panel de exploración izquierdo de la consola de información del sistema, haga clic en **Configuración de hardware**.
3. Amplíe **Configuración de IPMI BMC** y haga clic en **Temporizador de vigilancia**.
4. Marque la opción **Activar el temporizador de vigilancia** para activar el temporizador.
5. Especifique la frecuencia de verificación del temporizador (cantidad de minutos o segundos).
6. Seleccione una acción que iniciar cuando el temporizador de vigilancia se agota.
7. Si desea que BMC deje de transmitir mensajes de ARP mientras esté activado el temporizador de vigilancia, marque la opción **Suspender ARP de BMC**.
8. Haga clic en **Aplicar**.
9. Si ha cambiado la configuración del temporizador de vigilancia, puede restablecer la configuración predeterminada. Para ello, haga clic en **Restaurar valores predeterminados**.

Opciones de configuración de cambio en la alimentación

Cuando se pierde la alimentación en un equipo habilitado para IPMI, puede especificar la acción a llevar a cabo cuando se restablece el mismo. Se recomienda que restablezca el equipo a cualquier estado que se haya encontrado en el momento que se perdió la energía, pero puede elegir mantenerlo apagado o siempre encender el equipo.

Para cambiar las opciones de configuración de cambio en la alimentación

1. En la vista **Mis dispositivos**, haga doble clic en el dispositivo que desee configurar.
2. En el panel de exploración izquierdo de la consola de información del sistema, haga clic en **Configuración de hardware**.
3. Amplíe **Configuración de IPMI BMC** y haga clic en **Configuración de alimentación**.
4. Seleccione una opción para cuando se restablezca la alimentación.
5. Haga clic en **Aplicar**.
6. Si ha cambiado la configuración de alimentación, puede restablecer la configuración predeterminada. Para ello, haga clic en **Restaurar valores predeterminados**.

Cambio de la configuración de usuario BMC

System Manager realiza la autenticación a un BMC con una combinación de nombre de usuario y contraseña que es única para el BMC (distinta de cualquier otro nombre de usuario de System Manager). System Manager reserva el primer nombre de usuario de modo que siempre se pueda comunicar con el BMC. Si BMC permite que se definan otros nombres de usuario, puede definir nombres de usuarios con contraseñas para la autenticación BMC.

También puede especificar los niveles de privilegio de cada usuario. Para los IMM avanzados, puede especificar los niveles de privilegio (telnet, http y https) de cada canal.

PRECAUCIÓN: Tenga mucho cuidado al realizar cambios en estas configuraciones. Si la configuración contiene errores, puede deshabilitar la comunicación BMC del dispositivo con este producto.

Para cambiar la configuración de usuario BMC

1. En la vista **Mis dispositivos**, haga doble clic en el dispositivo que desee configurar.
2. En el panel de exploración izquierdo de la consola de información del sistema, haga clic en **Configuración de hardware**.
3. Amplíe **Configuración de IPMI BMC** y haga clic en **Configuración de usuario**.
4. Para borrar los datos de un nombre de usuario, haga clic en el número de índice y en **Borrar**.
5. Para agregar o cambiar un nombre de usuario, haga clic en el número de índice y en **Editar**.
6. Escriba un nombre de usuario.
7. Para definir una contraseña, marque la casilla **Definir contraseña** y a continuación, escriba y confirme la contraseña.
8. Seleccione los niveles de privilegio del acceso LAN y serie.
9. Haga clic en **Guardar cambios**.

Cambio de la contraseña BMC

System Manager se autentica en el BMC de un dispositivo mediante un nombre de usuario predeterminado (usuario 1) y una contraseña. No puede cambiar el nombre de usuario, pero sí puede cambiar la contraseña. Si cambia el valor de la contraseña, el cambio se guarda en la base de datos y en el BMC.

Para cambiar la contraseña BMC predeterminada

1. En la vista **Mis dispositivos**, haga doble clic en el dispositivo que desee configurar.
2. En el panel de exploración izquierdo de la consola de información del sistema, haga clic en **Configuración de hardware**.
3. Amplíe **Configuración de IPMI BMC** y haga clic en **Contraseña**.
4. Escriba la contraseña nueva y confírmela.
5. Haga clic en **Aplicar**.

Cambio de configuraciones de LAN

Los mensajes de IPMI se pueden conducir directamente a partir del BMC a través de la interfaz de LAN, además de la interfaz de sistema del dispositivo. Al activar la comunicación a través de LAN se permite que el servidor reciba alertas específicas a IPMI, aunque el dispositivo se encuentre apagado. El servidor central mantiene esta comunicación siempre y cuando el dispositivo tenga una conexión de red física con una dirección de red válida, siempre y cuando permanezca conectada la alimentación principal del dispositivo.

PRECAUCIÓN: Si elije establecer la configuración personalizada para la comunicación LAN o serie con el BMC, sea extremadamente precavido al realizar los cambios en la configuración. Si la configuración contiene errores, puede deshabilitar la comunicación BMC del dispositivo con este producto.

Si ha definido un canal LAN, puede utilizar la configuración predeterminada del BMC del dispositivo o bien, cambiar la configuración de dirección IP y de puerta de enlace. Utilice esas opciones para configurar los destinos de las capturas SNMP que envía el BMC para cada captura de evento de plataforma (PET).

También puede cambiar la configuración de la cadena de comunidad SNMP para el envío de alertas a través de LAN. Al configurar esas opciones, debe especificar la cadena de comunidad SNMP utilizada en la autenticación de SNMP. Para cada configuración, puede editar la información de destino de captura para especificar dónde y cómo se envían las capturas, y si se se confirma su recepción.

Para definir propiedades de la configuración de canal LAN

1. En la vista **Mis dispositivos**, haga doble clic en el dispositivo que desee configurar.
2. En el panel de exploración izquierdo de la consola de información del sistema, haga clic en **Configuración de hardware**.
3. Amplíe **Configuración de IPMI BMC** y haga clic en **Configuración de LAN**.
4. Seleccione **Siempre disponible** en la lista desplegable de comunicación de LAN para mantener abierto el acceso al BMC. Si selecciona **Deshabilitado** no tendrá acceso LAN al BMC cuando el dispositivo esté fuera de banda.
5. Seleccione el nivel de privilegio de usuario del canal: El **nivel de administrador** tiene acceso a todos los comandos, mientras que el **Nivel de usuario** está limitado a un acceso de sólo lectura (tendrá un conjunto restringido de funciones si selecciona el nivel de usuario).
6. Marque la opción **Desactivar permanentemente los BMC ARP** para desactivar los mensajes del protocolo de resolución de direcciones) del BMC. De este modo se reduce el tráfico de red pero se podría evitar la comunicación con el BMC cuando el dispositivo está fuera de banda.
7. Marque la opción **Desactivar respuestas de ARP** para impedir que el BMC envíe respuestas de mensajes ARP cuando el SO no está disponible. Si activa esta opción podría evitar la comunicación con el BMC cuando el dispositivo está fuera de banda.
8. La configuración de IP del canal LAN se define automáticamente si el BMC está sincronizado con el canal de SO. Caso contrario, la casilla bajo la ficha **Configuración de IP** se activa. Puede dejar marcada la casilla para utilizar la configuración de DHCP que se proporciona automáticamente o bien, desmarcar la casilla y editar los campos de texto con los valores estáticos. Por lo general, es preferible utilizar los valores automáticos.
9. Haga clic en la ficha **Enviar alertas a través de LAN** para configurar la cadena de comunidad SNMP (vea los detalles más abajo).
10. Haga clic en **Aplicar** para guardar los cambios.

Para cambiar las propiedades del envío de alertas a través de LAN

1. Abra la página **Configuración de LAN** (pasos del 1 al 3 más arriba).
2. Haga clic en la ficha **Enviar alertas a través de LAN**.
3. Marque la casilla **Habilitado** para activar el envío de alertas SNMP.
4. Especifique la **Cadena de comunidad SNMP** que se utilizará para la autenticación SNMP.
5. Para configurar los destinos de las capturas, haga doble clic en el número de índice y abra el cuadro de diálogo **Propiedades**.
6. Especifique la dirección IP a la cual BMC enviará las alertas, al igual que la dirección MAC correspondiente.
7. Especifique la cantidad de reintentos, la frecuencia de los reintentos y la puerta de enlace preferida que debe utilizarse.
8. Si desea que se confirme la recepción de las alertas (lo cual aumenta la cantidad de tráfico de red que se genera), marque la casilla **Confirmar recepción de alertas**.
9. Haga clic en **Aceptar**.

10. En la página Configuración de LAN, haga clic en **Aplicar** una vez que haya completado toda la configuración.

Cambio de las configuraciones de serie a través de LAN (SOL)

Utilice las opciones de configuración de SOL (serie a través de LAN) para personalizar la configuración del módem serie para usos específicos, como la redirección de mensajes BIOS POST al puerto serie. Si se requiere que BMC marque una conexión de módem, deben especificarse configuraciones de módem específicas como cadenas de inicialización y marcado.

Para la operación de módem de serie, es probable que tenga que configurar el BIOS y los puentes de la placa del dispositivo. Consulte la documentación del dispositivo particular si necesita detalles.

PRECAUCIÓN: Si elije establecer la configuración personalizada para la comunicación LAN o serie con el BMC, sea extremadamente precavido al realizar los cambios en la configuración. Si la configuración contiene errores, puede deshabilitar la comunicación BMC del dispositivo con este producto.

Para cambiar la configuración de SOL

1. En la vista **Mis dispositivos**, haga doble clic en el dispositivo que desee configurar.
2. En el panel de exploración izquierdo de la consola de información del sistema, haga clic en **Configuración de hardware**.
3. Amplíe **Configuración de IPMI BMC** y haga clic en **Configuración de SOL**.
4. Marque la opción **Activar la comunicación de serie a través de LAN** para activar SOL.
5. Seleccione el valor mínimo de **Nivel de usuario necesario para activar SOL**.
6. Seleccione la **Velocidad en baudios de las sesiones SOL** que sea adecuada para la configuración de hardware del dispositivo.
7. Haga clic en **Aplicar**.

Cambio de las configuraciones de IMM

La página **Configuración de IMM** se muestra solamente para los dispositivos IPMI que están equipados con una tarjeta de complemento IMM avanzada. Las opciones de esta página permiten activar o desactivar protocolos y funciones para su uso en el dispositivo habilitado para IMM. Consulte la documentación del fabricante para IMM antes de realizar cambios en estas opciones.

Para cambiar las opciones de configuración de IMM

1. En la vista **Mis dispositivos**, haga doble clic en el dispositivo que desee configurar.
2. En el panel de exploración izquierdo de la consola de información del sistema, haga clic en **Configuración de hardware**.
3. Amplíe **Configuración de IPMI BMC** y haga clic en **Configuración de IMM**.
4. Marque las casillas de los protocolos y funciones que desee activar y agregue cualquier opción que sea necesaria. Las opciones disponibles se incluyen:
    - KVM

- SNMP
- telnet
- Alertas SMTP
- HTTP
- HTTPS

5. Haga clic en **Aplicar**.

Administración de dispositivos Dell* DRAC

Este producto incluye la integración de la administración con dispositivos que tienen Dell* DRAC (controlador de acceso remoto). El DRAC es un controlador de hardware remoto que brinda una interfaz con el hardware de administración del servidor compatible con IPMI en el dispositivo Dell. El DRAC tiene una dirección IP asignada, la cual se utiliza para identificar el dispositivo DRAC en la detección del dispositivo y en la administración del mismo.

Los dispositivos que contienen un Dell DRAC se pueden administrar con la misma funcionalidad que los demás dispositivos compatibles con IPMI. Cuando el dispositivo se ha detectado y agregado a la lista de dispositivos administrados, se administra como cualquier otro dispositivo IPMI. Además, System Manager también tiene funciones exclusivas para Dell DRAC.

OpenManage Server Administrator es una consola basada en Web proporcionada por Dell para la administración de dispositivos Dell DRAC. Normalmente, para obtener acceso a ella se escribe la dirección IP del DRAC en un explorador y se inicia una sesión con un nombre de usuario y una contraseña. Si un dispositivo Dell DRAC se administra con System Manager, también se puede abrir esta utilidad directamente desde la interfaz de System Manager.

Además, System Manager permite administrar nombres de usuarios y contraseñas para el acceso a OpenManager Server Administrator, y visualiza tres registros de esta utilidad en la consola de información del servidor.

Para abrir OpenManage Server Administrator para un dispositivo Dell DRAC

1. Haga doble clic en el dispositivo en la lista **Todos los dispositivos**.
2. En la consola de información del servidor, amplíe **Hardware** y haga clic en **Dell DRAC**. Se visualiza la dirección IP del dispositivo y otra información de identificación.
3. Haga clic en **Ejecutar la utilidad Dell DRAC** para abrir la instancia de OpenManage Server Administrator del dispositivo en una ventana nueva.

Los registros de Dell DRAC están disponibles en System Manager

Se visualizan tres registros de la utilidad OpenManage Server Administrator en la consola de información del servidor de System Manager.

- **Registro de Dell DRAC**: Lleva un seguimiento de todos los eventos registrados por Server Administrator, tales como las actividades de inicios de sesión, los estados de las sesiones, los estados de las actualizaciones de firmware y la interacción entre el DRAC y los demás componentes del dispositivo. La información visualizada en System Manager incluye gravedad de eventos, descripciones y acciones correctivas sugeridas para los errores.
- **Registro de comandos de Dell DRAC**: Lleva un seguimiento de todos los comandos emitidos para Server Administrator. Muestra los comandos realizados, quién los emitió y cuándo se emitieron, e incluso los intentos de inicio y cierre de sesión y los errores de acceso.
- **Registro de seguimiento de Dell DRAC**: Es útil para el seguimiento de detalles sobre los eventos de comunicación de red, como alertas, búsqueda de personas o conexiones de red realizados por el DRAC.

Para ver los registros de un dispositivo Dell DRAC

1. Haga doble clic en el dispositivo en la lista **Todos los dispositivos**.
2. En la consola de información de servidor, amplíe **Registros**.
3. Haga clic en **Registro de Dell DRAC**, **Registro de comandos de Dell DRAC** o **Registro de seguimiento de Dell DRAC**.

Administración de nombres de usuario de dispositivos habilitados para Dell DRAC

Para el acceso a la interfaz de OpenManage Server Administrator, inicie una sesión con el nombre de usuario y la contraseña definidos para el dispositivo. El usuario **raíz** predeterminado es el primer usuario de la lista y no puede eliminarse, pero sí se puede cambiar su contraseña. Se pueden agregar hasta 15 usuarios adicionales. Aunque los nombres de usuario de DRAC pueden tener distintos niveles de acceso, System Manager solamente define los nombres de usuario con nivel de administrador.

Para agregar o editar nombres de usuarios y contraseñas de un dispostivo habilitado para DRAC

1. Haga doble clic en el dispositivo en la lista **Todos los dispositivos**.
2. En la consola de información de servidor, haga clic en **Configuración de hardware**.
3. En la consola de configuración de hardware, amplíe **Configuración de Dell DRAC** y haga clic en **Usuarios de Dell DRAC**. Se visualiza la lista de usuarios definidos.
4. Para cambiar la contraseña de un usuario, haga clic en el número de usuario y en **Cambiar contraseña**. Escriba y confirme la contraseña nueva, y haga clic en **Aplicar**. Para asignar la misma contraseña a varios usuarios, selecciónelos con Ctrl+clic o Mayús+clic.

5. Para agregar un usuario, haga clic en **Agregar usuario**. Escriba un nombre de usuario, escriba y confirme la contraseña, y haga clic en **Aplicar**. Se agrega el usuario a la lista.

   Nota: Si escribe un nombre de usuario que ya está en la lista, la contraseña nueva que especifica sobrescribe la contraseña existente del nombre de usuario y no se agrega un segundo usuario con ese nombre en la lista.

6. Para eliminar un usuario, haga clic en el número del usuario, en **Eliminar usuario** y en **Aceptar**. Para eliminar varios usuarios, selecciónelos con Ctrl+clic o Mayús+clic.

Todos los usuarios de la lista tienen acceso de nivel de administrador en OpenManage Server Administrator.

Mantenimiento e instalación de la base de datos central

Instalación de la base de datos central

La instalación predeterminada de este producto instala una base de datos MSDE de Microsoft en el servidor central. Esta opción de base de datos es la única diponible para System Manager y solamente se puede instalar una base de datos central. La base de datos debe instalarse solamente en un servidor independiente.

El esquema de la base de datos es compatible con Microsoft SQL Server 2000 con SP4. Es necesario que todos los servidores de base de datos incluyan MDAC 2.8.

La base de datos instalada en su servidor central debe ser una base completamente nueva. Si está instalando System Manager en un servidor que anteriormente tenía una instalación de LANDesk® Management Suite o de Server Manager, no puede utilizar la estructura de base de datos existente para la instalación de System Manager.

La utilidad LANDeskConfiguración de servicios incluye una interfaz para configurar varios servicios. La ficha General de esta utilidad muestra el nombre actual del servidor, el nombre de la base de datos y el nombre de usuario y la contraseña requeridos para acceder a la base de datos central. Todos los servicios utilizan estas credenciales para acceder a la base de datos. Debido a que System Manager puede utilizar sólo una base de datos, no necesita cambiar el nombre del servidor ni el de la base de datos. Si lo desea, puede cambiar las credenciales. Para obtener más información, consulte Apéndice C: Configuración de servicios.

Apéndice A: Requerimientos del sistema y uso del puerto

El servidor central debe tener una dirección IP estática.

Administración central

El servidor central administrativo admite los sistemas operativos siguientes:

- Microsoft Windows 2000 Server (con SP4)
- Microsoft Windows 2000 Advanced Server (con SP4)
- Microsoft Windows 2003 Server Standard Edition (con SP1)
- Microsoft Windows 2003 Server Enterprise Edition (con SP1)

Compatibilidad del servidor (agentes)

- Microsoft Windows 2000 Server (con SP4)
- Microsoft Windows 2000 Advanced Server (con SP4)
- Microsoft Windows 2000 Professional (con SP4)
- 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

Exploradores

- Microsoft Internet Explorer 6.x (con SP1)
- Mozilla 1.7 y posterior
- Firefox 1.5 y posterior

Bases de datos

- MSDE (con SP4)

Microsoft Data Access Components

- MDAC 2.8 o posterior

Si desea que más de un producto de administración de LANDesk utilice la misma base de datos, debe instalar ambos productos en el mismo equipo "central". Del mismo modo, si desea instalar varios productos en el mismo equipo "central", debe utilizar la misma base de datos. Si ambos productos utilizan la misma base de datos, también deben ser de la versión 8.70.

Uso de los puertos

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
9595, 9594	de consola a dispositivo	TCP	Configuración para el servidor
9595	de consola a dispositivo	UDP	detección
623	de consola a dispositivo	UDP	ASF, detección IPMI
5007	de consola a dispositivo	TCP	Inventario
9535	de consola a dispositivo	TCP	control remoto
139, 145	de consola a dispositivo	TCP	archivos e impresoras compartidas
137, 138	de consola a dispositivo	UDP	archivos e impresoras compartidas

Este producto necesita detectar los nodos con el agente de administración estándar 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).

Apéndice B: Activación del servidor central

Antes de utilizar la consola, primero debe activar el servidor central mediante la utilidad Activación del servidor central. Por lo general se trata de un procedimiento único que solamente debe repetirse si adquiere licencias adicionales. Utilice la utilidad Activación del servidor central para:

- Activar un servidor nuevo por primera vez.
- Actualizar un servidor central existente o realizar la actualización a Management Suite o Server Manager.
- Activar un servidor nuevo con una licencia de evaluación de 45 días.

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 nodos de forma manual", más adelante en esta sección.

Cada servidor central debe tener un certificado autorizado único. Varios servidores centrales no pueden compartir el mismo certificado de autorización, aunque pueden verificar las cuentas de nodos de la misma cuenta de LANDesk. Esta utilidad se ejecuta de forma automática en el primer reinicio tras la instalación de System Manager.

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 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 que realice ninguna acción manual. 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.

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 de acceso telefónico para enviar los datos de uso.

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

Activación de un servidor con la cuenta de LANDesk Software

Antes de activar un servidor nuevo con una licencia completa, debe configurar una cuenta en LANDesk Software, la cual le otorga licencia para los productos de LANDesk Software y la cantidad de nodos que haya adquirido. Necesita la información de la cuenta (nombre de contacto y contraseña) a fin de activar el servidor. Si no tiene dicha información, comuníquese con el representante de ventas de LANDesk Software.

No cambie la fecha u hora del servidor central entre la instalación del producto y la activación del servidor central. La activación tendrá errores. Tendrá que desinstalar y volver a instalar el producto.

Para activar un servidor

1. Haga clic en **Inicio | Todos los programas | LANDesk | Activación del servidor central**.
2. Haga clic en **Activar**.

Activación de un servidor con una licencia de evaluación

La licencia de evaluación de 45 días activa el servidor con el servidor de licencias de LANDesk Software. Una vez que caduca el período de evaluación de 45 días, no podrá iniciar una sesión en el servidor central y éste dejará de aceptar rastreos de inventario. No obstante, no se perderán los datos existentes en el software y la base de datos. Mientras utiliza la licencia de evaluación de 45 días o después que ésta expire, puede volver a ejecutar la utilidad Activación del servidor central y cambiar a la activación completa que utiliza una cuenta de LANDesk Software. Si ha caducado la licencia de evaluación, al cambiar a la licencia completa se reactiva el servidor central.

Para activar la evaluación de 45 días

1. Haga clic en **Inicio | Todos los programas | LANDesk | Activación del servidor central**.
2. Haga clic en **Activar este servidor central para la evaluación de 45 días**.
3. Haga clic en **Evaluar**.

Actualización de una cuenta existente

La opción de actualización envía la información de uso al servidor de licencias de LANDesk Software. Los datos de uso se envían automáticamente si tiene conexión a Internet, de modo que no necesitará utilizar esta opción para enviar la verificación de la cuenta de nodos. También puede utilizar esta opción para cambiar el servidor central asociado con la cuenta de LANDesk Software. Esta opción también puede cambiar un servidor central de una licencia de evaluación a una licencia completa.

Para actualizar una cuenta existente

1. Haga clic en **Inicio | Todos los programas | LANDesk | Activación del servidor central**.
2. Haga clic en **Actualizar el servidor central que está utilizando su nombre de contacto y contraseña de LANDesk**.
3. Escriba el **Nombre de contacto** y la **Contraseña** que desea para el servidor central. Si escribe un nombre y una contraseña distintos a los utilizados originalmente para activar el servidor central, el servidor cambia a la nueva cuenta.
4. Haga clic en **Activar**.

Activación de un servidor central o verificación de los datos de cuenta de nodos 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 nodos. Se muestra un mensaje, el cual le indica que envíe los datos de activación y de verificación de cuenta de nodos 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 nodos de forma manual

1. Cuando el servidor central le indica que verifique los datos de cuenta de nodos 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.

Apéndice C: Configuración de servicios

Puede utilizar el subprograma Configuración de servicios para configurar los siguientes servicios en cualquiera de sus servidores y bases de datos centrales:

- Selección de un servidor y una base de datos centrales
- Configuración del servicio Inventario
- Configuración del control de los nombres de dispositivos duplicados
- Configuración del control de los ID de dispositivos duplicados
- Configuración del servicio programador
- Configuración del servicio de tareas personalizadas
- Configuración del servicio de multidifusión
- Configuración de la contraseña BMC
- Configuración de la contraseña de Intel AMT

Para iniciar el subprograma Configuración de servicios en el servidor central, haga clic en **Inicio | Archivos de programa | LANDesk | LANDesk Configuración de servicios**.

Se visualizan dos botones afuera de las fichas:

- **Credenciales:** Abre el cuadro de diálogo Credenciales del servidor, en el cual puede agregar dispositivos que funcionen como servidores preferidos. Para agregar un dispositivo, haga clic en **Agregar**. Se abre el cuadro de diálogo **Nombre de usuario y contraseña** (que se describe a continuación).
- **Validación de OSD:** Para crear entornos previos al inicio basados en Windows PE o en DOS, debe proporcionar acceso a los CD de instalación de Windows PE 2005 y Windows NT 4. Haga clic en **Validar ahora** en ambos entornos de creación de imágenes, escriba la ruta al CD correspondiente y haga clic en **Aceptar**.

Cuadro de diálogo Nombre de usuario y contraseña

Utilice el cuadro de diálogo **Nombre de usuario y contraseña** para proporcionar información sobre el servidor preferido que desee agregar.

Para escribir información del servidor preferido

1. En el subprograma Configurar servicios, haga clic en **Credenciales**.
2. En el cuadro de diálogo Credenciales del servidor, haga clic en **Agregar**.
3. Escriba una descripción, la información de autenticación y los intervalos de dirección IP.
4. Haga clic en **Credenciales de prueba** para verificar la validez de la información.
5. Haga clic en **Aceptar** para agregar el servidor preferido al cuadro de diálogo Credenciales del servidor.

- **Nombre del servidor:** Nombre del servidor preferido.
- **Nombre de usuario:** Nombre de usuario utilizado para la autenticación en el servidor. Debe ser un nombre de dominio completo (por ejemplo, mi dominio\nombre de usuario).
- **Descripción:** Descripción del servidor preferido.
- **Contraseña:** Contraseña del servidor preferido.

- **Dirección IP inicial:** Introduzca la dirección IP inicial del intervalo de direcciones que el servidor preferido debe limitarse a utilizar. La dirección IP inicial no debe ser mayor que la dirección IP final. Los primeros tres octetos de las direcciones IP inicial y final deben coincidir, por ejemplo, 10.100.10.1 y 10.100.10.255.
- **Dirección IP final:** Introduzca la dirección IP de finalización para el intervalo de direcciones que desee explorar.
- **Agregar:** Agrega intervalos de dirección IP a la cola de trabajo en la parte inferior del cuadro de diálogo.
- **Eliminar:** Elimina el intervalo de direcciones IP seleccionado de la cola de trabajo.

Fichas de configuración de servicios

Antes de configurar un servicio, utilice la ficha **General** para especificar el servidor y la base de datos centrales para los que desea configurar el servicio.

Nota: Todos los cambios en la configuración de un servicio que realice para un servidor y una base de datos centrales no tendrán efecto hasta que reinicie el servicio en el servidor central.

Selección de un servidor y una base de datos centrales

La ficha **General** le permite seleccionar un servidor y una base de datos centrales y proporcionar credenciales de autenticación de modo que pueda configurar los servicios para ese servidor central.

Acerca del cuadro de diálogo Configuración de servicios: Ficha General

Utilice este cuadro de diálogo para seleccionar el servidor y la base de datos centrales para los que desea configurar un servicio específico. A continuación, seleccione la ficha de servicios y especifique la configuración para ese servicio.

- **Nombre del servidor:** Muestra el nombre del servidor central al que está actualmente conectado.
- **Servidor:** Permite escribir el nombre de un servidor central diferente y el directorio de la base de datos del mismo.
- **Base de datos:** Permite escribir el nombre de la base de datos central.
- **Nombre de usuario:** identifica un usuario con credenciales de autenticación a la base de datos central (especificada durante la configuración).
- **Contraseña:** Identifica la contraseña de usuario necesaria para tener acceso a la base de datos central (especificada durante la configuración).
- **Base de datos Oracle:** Indica que la base de datos central especificada anteriormente es de Oracle. (No se aplica a System Manager).
- **Actualizar configuración:** Restaura la configuración que existía al abrir el cuadro de diálogo Configuración del servicio.

Configuración del servicio Inventario

Utilice la ficha **Inventario** para configurar el servicio de Inventario para el servidor y la base de datos centrales que se seleccionaron mediante la ficha General.

Acerca del cuadro de diálogo Configurar servicios: Ficha Inventario

Utilice esta ficha para especificar las opciones de inventario siguientes:

- **Nombre del servidor**: muestra el nombre del servidor central al que está conectado.
- **Registrar estadísticas**: mantiene un registro de las acciones y estadísticas de la base de datos central.
- **Transporte de datos cifrados:** Activa el rastreador de inventario para enviar los datos de inventario de dispositivo del dispositivo rastreado de regreso al servidor central en calidad de datos cifrados a través de SSL.
- **Rastrear el servidor en**: Especifica la hora en que se rastreará el servidor central.
- **Realizar el mantenimiento en**: Especifica la hora en que se realizará el mantenimiento estándar de la base de datos central.
- **Días que conservar los rastreos de inventario**: Define el número de días anteriores a la eliminación del registro de rastreo de inventario.
- **Inicios de sesión del propietario primario**: Define el número de veces que el rastreador de inventario realiza un seguimiento de los inicios de sesión para determinar el propietario primario de un dispositivo. El propietario primario es el usuario que ha iniciado sesión la mayoría de las veces dentro de este número especificado de inicios de sesión. El valor predeterminado es 5 y los valores mínimo y máximo son 1 y 16 respectivamente. Si todos los inicios de sesión son exclusivos, el último usuario que ha iniciado una sesión se considera el propietario primario. Un dispositivo sólo puede tener un propietario primario asociado cada vez. Los datos de inicio de sesión del usuario primario incluyen el nombre completo del usuario como ADS, NDS, nombre de dominio o formato de nombre local (en este orden) además de la fecha del último inicio de sesión.
- **Configuración avanzada:** Abre el cuadro de diálogo **Configuración avanzada**, donde puede definir diversas opciones avanzadas pertinentes al rastreador de inventario. Para cambiar un valor, haga clic en él, cámbielo en el cuadro de texto **Valor** y haga clic en **Establecer**. Para ver una descripción de un valor, haga clic en él y vea los detalles en el cuadro **Descripción**.
- **Software:** Abre el cuadro de diálogo **Configuración del rastreo de software** desde donde puede configurar el tiempo de rastreo del software de cliente y la configuración de historial.
- **Atributos:** Abre el cuadro de diálogo Seleccionar atributos para guardar, donde puede seleccionar los atributos de rastreo de inventario que se almacenan en la base de datos.
- **Administrar duplicados: Dispositivos**: Abre el cuadro de diálogo Configuración del manejo de nombres de dispositivos duplicados, donde puede elegir una opción para eliminar dispositivos con nombres duplicados, direcciones MAC o ambos (consulte **Dispositivos duplicados** más adelante).

- **Administrar duplicados: ID de dispositivos:** Abre el cuadro de diálogo **Identificador de dispositivos duplicados**, donde pueden seleccionar atributos que identifiquen los dispositivos de modo exclusivo. Puede utilizar esta opción para evitar rastrear Id. de dispositivos duplicados en la base de datos central (consulte Configuración del control de los ID de dispositivos duplicados a continuación).
- **Estado del servicio de inventario**: Indica si el servicio se ha iniciado o detenido en la base de datos central.
- **Iniciar**: Inicia el servicio en el servidor central.
- **Detener**: Detiene el servicio en el servidor central.

Cuadro de diálogo Rastreo de software

Utilice este cuadro de diálogo para configurar la frecuencia de los rastreos de software. El hardware de un dispositivo se rastrea cada vez que el rastreador de inventario se ejecuta en el dispositivo, sin embargo el software del dispositivo se rastrea únicamente en el intervalo de tiempo que se especifique aquí.

- **Cada inicio de sesión:** Rastrea todo el software instalado en el dispositivo cada vez que el usuario inicia sesión.
- **Una vez cada (días):** Rastrea el software del dispositivo únicamente en el intervalo diario especificado, como un rastreo automático.
- **Histórico (en días):** Especifica el periodo de tiempo durante el que se guarda el historial de inventario del dispositivo.

Configuración del control de los nombres de dispositivos duplicados

Utiliza el diálogo Dispositivos duplicados para eliminar dispositivos duplicados de la base de datos.

1. En la ficha Inventario, haga clic en **Dispositivos**.
2. En el cuadro de diálogo Dispositivos duplicados, haga clic en la opción que desee utilizar al eliminar dispositivos duplicados, y luego haga clic en **Aceptar**.

   Quitar duplicados cuando:
   - **Los nombres de dispositivo coinciden:** Elimina el registro más antiguo cuando dos o más nombres de dispositivos coinciden en la base de datos.
   - **Las direcciones MAC coinciden:** Elimina el registro más antiguo cuando dos o más direcciones MAC coinciden en la base de datos.
   - **Los nombres de dispositivo y las direcciones MAC coinciden:** Elimina el registro más antiguo SOLAMENTE si dos o más nombres de dispositivo y direcciones MAC (en el mismo registro) coinciden.

Configuración del control de los ID de dispositivos duplicados

Como la creación de imágenes se utiliza con frecuencia para configurar los dispositivos en una red, la probabilidad de que existan ID de dispositivos duplicados en los dispositivos se

incrementa. Puede evitar este problema si especifica otros atributos de dispositivo que, junto con el ID de dispositivo, proporcionen un identificador único para los dispositivos. Ejemplos de éstos y otros atributos son el nombre del dispositivo, nombre de dominio, BIOS, bus, coprocesador, etc.

La función de ID duplicado le permite seleccionar los atributos de dispositivo que se pueden utilizar para identificar al servidor de modo exclusivo. Especifique los atributos y la cantidad de atributos que deben faltar para que el dispositivo se designe como duplicado de otro. Si el rastreador de inventario detecta un dispositivo duplicado, escribe un evento en el registro de eventos de la aplicación para indicar el ID del dispositivo duplicado. El cuadro de diálogo Id. de dispositivo duplicado contiene las opciones siguientes:

- **Lista de atributos:** Muestra una lista de atributos que puede elegir para identificar de modo exclusivo a un dispositivo.
- **Atributos de identidad:** Muestra los atributos que ha seleccionado para identificar exclusivamente a un dispositivo.
- **Desencadenantes de ID de dispositivo duplicado:**
  - **Atributos de identidad:** Identifica el número de atributos que deben ser distintos en un dispositivo para que éste se considere un duplicado de otro.
  - **Atributos de hardware:** Identifica el número de atributos de hardware que deben ser distintos en un dispositivo para que éste se considere un duplicado de otro.
- **Rechazar identidades duplicadas:** Hace que el rastreador de inventario registre el ID de dispositivo duplicado y rechaza todos los intentos posteriores de rastrear el ID de ese dispositivo. A continuación, el rastreador de inventario genera un nuevo ID de dispositivo.

Para configurar el control de ID duplicados

1. En el cuadro de diálogo Configuración de servicios, haga clic en la ficha **Inventario**, y luego en **ID de dispositivos**.
2. Seleccione los atributos de la **Lista de atributos** que desee utilizar para identificar un dispositivo de modo exclusivo y a continuación, haga clic en el botón de flecha hacia abajo para agregar el atributo a la lista de **Atributos de identidad**. Podrá introducir tantos atributos como desee.
3. Seleccione el número de atributos de identidad (y de hardware) que deben no coincidir en un dispositivo para que éste se considere un duplicado de otro dispositivo.
4. Si desea que el rastreador de inventario rechace los ID de dispositivos duplicados, active la opción **Rechazar identidades duplicadas**.

Configuración del servicio programador

Utilice la ficha **Programador** para configurar el servicio programador del servidor central y de la base de datos que ha seleccionado en la ficha **General**. Debe contar con los derechos correspondientes para realizar estas tareas, incluso privilegios plenos de administrador en los dispositivos administrados que les permita recibir distribuciones de paquetes de System Manager. Para especificar varias credenciales de inicio de sesión que puedan utilizarse en los dispositivos, haga clic en **Cambiar inicio de sesión**.

Acerca del cuadro de diálogo Configurar servicios: Ficha Programador

Utilice esta ficha para ver el nombre del servidor y la base de datos centrales que se seleccionaron previamente así como para especificar las opciones de tareas programadas siguientes:

- **Nombre de usuario**: Nombre de usuario con el que se ejecutará el servicio de tareas programadas. Éste se puede cambiar haciendo clic en el botón **Cambiar inicio de sesión**.
- **Número de segundos entre reintentos**: Cuando una tarea programada se configura con varios reintentos, esta configuración controla el número de segundos que el servicio de Tareas programadas esperará antes de reintentar la tarea.
- **Número de segundos para intentar la activación**: Cuando se configura una tarea programada para que utilice Wake On LAN, esta configuración controla el número de segundos que el servicio de tareas programadas esperará para que se active un dispositivo.
- **Intervalo entre las evaluaciones de las consultas**: Número que indica el periodo de tiempo entre las evaluaciones de las consultas, y la unidad de medida para el número (de minutos, horas, días o semanas).
- **Configuración de activación Wake On LAN**: Puerto IP que utilizará el paquete Wake On LAN configurado por las tareas programadas para activar los dispositivos.
- **Estado del servicio programador**: Indica si el servicio se ha iniciado o detenido en la base de datos central.
- **Iniciar**: Inicia el servicio en el servidor central.
- **Detener**: Detiene el servicio en el servidor central.
- **Reiniciar:** Reinicia el servicio en el servidor central.
- **Avanzada:** Abre el cuadro de diálogo **Configuración avanzada del programador**, en el cual puede modificar las opciones que controlan la forma en que funciona el programador. Para cambiar un valor, haga clic en él, haga clic en **Editar**, cambie el valor y haga clic en **Aceptar**.

Acerca del cuadro de diálogo Configuración de servicios: Cuadro de diálogo Cambiar inicio de sesión

Utilice el diálogo **Cambiar inicio de sesión** (haga clic en **Cambiar inicio de sesión** en la ficha **Programador**) para cambiar el inicio de sesión predeterminado del programador. También puede especificar credenciales alternas que el servicio programador puede intentar cuando necesite ejecutar una tarea en dispositivos no administrados.

Para instalar agentes de System Manager en dispositivos no administrados, el servicio programador debe tener la capacidad de establecer conexión con dispositivos mediante una cuenta administrativa. La cuenta predeterminada que utiliza el servicio programador es LocalSystem. Por lo general, las credenciales de LocalSystem funcionan en dispositivos que no se encuentran en un dominio. Si los dispositivos están en un dominio, especifique una cuenta de administrador de dominio.

Si desea cambiar las credenciales de inicio de sesión del servicio programador, puede especificar otra cuenta administrativa a nivel de dominio que utilizar en los dispositivos. Si

administra dispositivos a través de varios dominios, puede agregar credenciales adicionales para el programador. Si desea utilizar una cuenta diferente a LocalSystem para el servicio programador, o si desea proporcionar credenciales alternas, debe especificar un servicio de inicio de sesión primario para el programador que posea derechos de administrador en el servidor central. Las credenciales alternas no requieren derechos administrativos en el servidor central, pero sí en los dispositivos.

El servicio programador intenta las credenciales predeterminadas y utiliza cada credencial especificada en la lista **Credenciales alternas** hasta que tiene éxito o se terminan las credenciales. Las credenciales especificadas se codifican y almacenan de forma segura en el registro del servidor central.

Defina las opciones siguientes para las credenciales predeterminada del programador:

- **Nombre de usuario:** Escriba el dominio\nombre de usuario o el nombre de usuario predeterminado que el programador va a utilizar.
- **Contraseña:** Escriba la contraseña para las credenciales especificadas.
- **Confirmar contraseña:** Vuelva a escribir la contraseña para confirmarla.

Defina las opciones siguientes para las credenciales adicionales del programador:

- **Agregar:** Haga clic para agregar el nombre de usuario y la contraseña especificados a la lista Credenciales alternas.
- **Quitar:** Haga clic para quitar las credenciales seleccionadas de la lista.
- **Modificar:** Haga clic para cambiar las credenciales seleccionadas.

Al agregar credenciales alternas, especifique lo siguiente:

- **Nombre de usuario:** Escriba el nombre de usuario que el programador va a utilizar.
- **Dominio:** Escriba el dominio para el nombre de usuario especificado.
- **Contraseña:** Escriba la contraseña para las credenciales especificadas.
- **Confirmar contraseña:** Vuelva a escribir la contraseña para confirmarla.

Configuración del servicio de tareas personalizadas

Utilice la ficha **Tareas personalizadas** a fin de configurar el servicio de tareas personalizadas para el servidor y la base de datos centrales que se seleccionaron mediante la ficha General. Algunos ejemplos de tareas personalizadas son los rastreos de inventarios y las distribuciones de software.

Cuando deshabilita TCP como protocolo de ejecución remota, los trabajos personalizados utilizan el protocolo del agente de administración estándar de forma predeterminada, ya sea que esté marcado como inhabilitado o no. Asimismo, si están habilitadas la ejecución remota TCP y el agente de administración estándar, los trabajos personalizados primero intentan utilizar la ejecución remota TCP y, si no está presente, utilizan la ejecución remota estándar del producto.

La ficha **Tareas personalizadas** también permite elegir las opciones de la detección de servidores. Para que un servicio de tareas personalizadas pueda procesar una tarea, debe detectar cada dirección IP actual de los servidores. Esta ficha permite configurar el modo en que el servicio se comunicará con los servidores.

Acerca del cuadro de diálogo Configurar servicios: Ficha trabajos personalizados

Utilice esta ficha para configurar las opciones siguientes de tareas personalizadas:

Opciones de ejecución remota:

- **Deshabilitar ejecución de TCP**: Deshabilita TCP como protocolo de ejecución remota y utiliza el protocolo CBA de forma predeterminada.
- **Inhabilitar ejecución/transferencia de archivos por CBA**: Deshabilita el agente de administración estándar como protocolo de ejecución remota. Si el agente de administración estándar está deshabilitado y el protocolo TCP no se encuentra en el dispositivo, la ejecución remota fallará.
- **Habilitar tiempo de espera de ejecución remota**: Habilita un tiempo de espera de ejecución remota y especifica el número de segundos que deben transcurrir hasta que finalice el tiempo de espera. Los tiempos de espera de ejecución remota se activan cuando el dispositivo envía transacciones de control, pero el trabajo en el dispositivo está bloqueado o en un bucle. Esta configuración se aplica a los dos protocolos (TCP o agente de administración estándar). El valor se puede establecer entre 300 segundos (5 minutos) y 86.400 segundos (1 día).
- **Habilitar tiempo de espera del cliente**: Habilita un tiempo de espera del dispositivo y especifica el número de segundos que deben transcurrir hasta que finalice el tiempo de espera. De forma predeterminada, la ejecución remota por TCP envía una transacción de control de un dispositivo a otro a intervalos de 45 segundos hasta que la ejecución remota se completa o finaliza el tiempo de espera. Los tiempos de espera del cliente se activan cuando el dispositivo no envía una transacción de control al dispositivo.
- **Puerto de ejecución remota (el predeterminado es el 12174)**: Puerto a través del cual tiene lugar la ejecución remota de TCP. Si se cambia este puerto, se deberá cambiar asimismo en la configuración del cliente.

Opciones de distribución:

- **Distribuir a <nn> servidores simultáneamente**: Número máximo de dispositivos a los que se distribuirá el trabajo personalizado simultáneamente.

Opciones de detección:

- **UDP:** Al seleccionar UDP se utiliza un ping de agente de administración estándar a través de UDP. La mayoría de los componentes de System Manager dependen del agente de administración estándar, de modo que los dispositivos administrados deben tener dicho agente. Constituye el método de detección predeterminado y el más rápido. Con UDP, también puede seleccionar **Reintentos** y **Tiempo de espera** del ping de UDP.
- **TCP:** Al seleccionar TCP se utiliza una conexión HTTP al servidor en el puerto 9595. Este método de detección tiene la ventaja de que es capaz de funcionar a través de un servidor de seguridad si se abre el puerto 9595. No obstante, está sujeto a los tiempos de espera de conexión HTTP si no se encuentran los dispositivos. Dichos tiempos de espera pueden tomar 20 segundos o más. Si muchos de los dispositivos de destino no responden a la conexión TCP, la tarea tomará mucho tiempo para iniciarse.
- **Ambos:** Al seleccionar Ambos el servicio intenta la detección primero con UDP, luego con TCP y finalmente con DNS/WINS, si está seleccionado.

- **Deshabilitar difusión de subred:** Si se selecciona, se inhabilita la detección a través de una difusión de subred.
- **Deshabilitar búsqueda de DNS/WINS:** Si se selecciona, inhabilita la búsqueda del servicio de nombre para cada dispositivo, si falla el método de detección TCP/UDP seleccionado.

Configuración del servicio de multidifusión

Utilice la ficha **Multidifusión** para configurar las opciones del representante de dominio de multidifusión para el servidor y la base de datos centrales que haya seleccionado mediante la ficha **General**.

Acerca del cuadro de diálogo Configurar servicios: Ficha Multidifusión

Utilice esta ficha para establecer las opciones de multidifusión siguientes:

- **Utilizar representante de dominio de multidifusión:** Utiliza la lista de representantes de dominio de multidifusión almacenados en el grupo **Configuración > Dominio de multidifusión**, en la vista de red.
- **Usar archivo guardado en caché:** consulta cada una de las multidifusiones para averiguar cuál de ellas podría haber colocado el archivo en la memoria caché. El archivo guardado en la memoria caché se utiliza en lugar de descargar el archivo en un representante.
- **Usar archivo de caché antesdel representante de dominio preferido:** Cambia el orden de detección para hacer que primero se intente la opción **Usar archivo guardado en caché**.
- **Usar difusión:** Envía una difusión dirigida por subred para encontrar los dispositivos de esa subred que podrían ser representantes de dominio de multidifusión.
- **Registrar período de descarte (días):** Especifica el número de días que las entradas del registro se conservarán antes de eliminarse.

Configuración de la contraseña BMC

Use la ficha **Contraseña BMC** para crear una contraseña para el IPMI BMC (controlador de administración de placa base).

- En la ficha **Contraseña para BMC**, escriba una contraseña en el cuadro de texto **Contraseña**, vuelva a escribir la contraseña en el cuadro de texto **Confirmar contraseña** y haga clic en **Aceptar**.

  La contraseña no debe tener más de 15 caracteres, cada uno de los cuales debe ser un número (0-9) o una letra mayúscula o minúscula (a-z).

Configuración de opciones de Intel AMT

Utilice la ficha **Configuración de Intel AMT** para crear o cambiar la contraseña en un dispositivo habilitado para la tecnología Intel Active Management y para ver las instrucciones sobre la detección de dispositivos AMT.

Para configurar la contraseña de Intel AMT

1. Escriba el nombre de usuario actual y la contraseña. 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

Detección e incorporación de dispositivos Intel AMT

Para detectar los dispositivos AMT, escriba la dirección IP del servidor central en el campo Servidor de incorporación del AMT BIOS y utilice el puerto 9982. Pulse **Ayuda** en **Configurar servicios** para obtener más información. Cuando se detecta un dispositivo Intel AMT y se mueve a la lista **Mis dispositivos**, se incorpora de forma automática utilizando el modo TLS.

Apéndice D: Seguridad de agente y certificados de confianza

Todos los servidores centrales tienen un certificado único y una clave privada que el programa de Instalación crea durante la primera instalación del servidor central en un dispositivo. Los dispositivos sólo se comunicarán con los servidores centrales para los que tienen un archivo de certificado de confianza que coincide.

Las claves privadas y los archivos de certificado que se instalan son:

- **<nombredeclave>.key:** El archivo .KEY es la clave privada para el servidor central y sólo reside en dicho servidor. Si esta clave no es confidencial, la comunicación entre el servidor y el servidor central no será segura. No dé a conocer esta clave. Por ejemplo, no la incluya en ningún correo electrónico.
- **<nombredeclave>.crt:** El archivo .CRT contiene la clave pública para el servidor central. Este archivo es una versión de la clave pública fácil para el visualizador que se puede consultar para ver más información sobre la clave.
- **<hash>.0:** Eel archivo .0 es un archivo de certificado de confianza y su contenido es idéntico al del archivo .CRT. Sin embargo, se le ha dado un nombre que permite al equipo encontrar rápidamente el archivo de certificado que se está buscando en un directorio que contiene varios. El nombre es un valor hash (suma comprobación) de la información del asunto del certificado. A fin de determinar el nombre de archivo hash de un certificado específico, abra el archivo <nombredeclave>.CRT. Hay una sección de archivo .INI [LDMS] en el archivo. El par hash=valor indica el valor <hash>.

Todas las claves se almacenan en el servidor central en \Archivos de programa\LANDesk\Shared Files\Keys. La clave pública <hash>.0 también se incluye en el directorio LDLOGON y es necesario que permanezca allí de forma predeterminada. <nombredeclave> es el nombre del certificado que suministró durante la instalación del servidor central. En dicho proceso, resulta útil ofrecer un nombre de clave descriptivo, como el nombre del servidor central (o incluso su nombre completo) y el de la clave (ejemplo: ldcore o ldcore.org.com). De este modo, se facilitará la identificación de los archivos de certificado/clave privada en un entorno de varios servidores.

Copia de seguridad y restauración de archivos de las claves certificadas y privadas entre servidores centrales

Cuando se instala un servidor central, el programa de Instalación crea un certificado nuevo. Aún si está volviendo a instalar en presencia de un servidor central existente, el programa de Instalación todavía crea un certificado nuevo. Si instala dispositivos con un certificado que no coincide con el certificado del servidor central nuevo, el servidor central no podrá comunicarse con ellos. Si necesita volver a instalar el servidor central, tiene dos opciones:

1. Reinstale los agentes manualmente con una versión de configuración en el servidor central nuevo. No podrá utilizar la distribución de software para actualizar los agentes, debido a que el servidor central y los dispositivos no tendrán un certificado y clave que coincidan.

2. Antes de volver a instalar un servidor central, cree una copia de seguridad de los archivos del certificado y claves existentes en un lugar seguro. Tras la reinstalación, copie las claves previas a la instalación central nueva. Las claves nuevas y previas pueden coexistir. El servidor central utilizará la clave apropiada de forma automática.

Estos servidores pueden contener varios archivos de certificado/clave privada. Siempre que un cliente pueda autenticarse con una de las claves en un servidor central, podrá comunicarse con dicho servidor.

Se incluye una utilidad en este producto que lleva acabo la segunda opción enumerada anteriormente. La utilidad de migración de datos del servidor central (CoreDataMigration.exe) se encuentra instalada en la carpeta \ProgramFiles\LANDesk\ManagementSuite. Maneja las copias de seguridad y copia la información de dicha información como claves y certificados cuando instala un nuevo servidor.

Para guardar y restaurar un conjunto de claves de certificados y privadas

1. En el servidor central de origen, diríjase a la carpeta \Archivos de programa\LANDesk\Shared Files\Keys.
2. Copie los archivos <nombredeclave>.key, <nombredeclave>.crt y <hash>.0 del servidor de origen en un disquete o en otro lugar que sea seguro.
3. En el servidor central de destino, copie los archivos desde el servidor central de origen a la misma carpeta (\Archivos de programa\LANDesk\Shared Files\Keys). Las claves surtirán efecto de inmediato.

Advertencia: Proteja el archivo de la clave privada
Cerciórese de que la seguridad de la clave privada <nombredeclave>.key no se comprometa. No la transfiera mediante un método sin seguridad, tal como correo electrónico o un compartimiento para archivos públicos. El servidor central utiliza este archivo para autenticar dispositivos y cualquier servidor central con el archivo <nombredeclave>.key apropiado que puede realizar ejecuciones remotas y una transferencia de archivos a un dispositivo administrado.

Sugerencias de solución de problemas

Las siguientes sugerencias de solución de problemas van destinadas a los problemas más frecuentes con la consola Web.

No puedo activar el servidor central
Si se ha instalado un servidor central, y luego se ha cambiado la hora del dispositivo, la activación no será exitosa. Se debe reinstalar el producto para activar el servidor central.

Al intentar activar el servidor central, recibo un mensaje de error que indica que no se pudo leer la base de datos del servidor central.
Verifique que el servidor central esté conectado de forma física a la red y que cuente con una conexión válida a Internet. Si uno de los cables está desconectado o si la conexión a Internet del servidor central no es válida, no se podrá completar el proceso de activación.

Si no conoce la URL de las páginas de la consola.
Póngase en contacto con la persona que instaló el servidor central, quien con toda probabilidad, es el administrador de red del sitio. No obstante, la URL típica de Server Manager y System Manager es http://*nombre del equipo del servidor central*/ldsm. La URL de Management Suite es http://*nombre del equipo del servidor central*/remote.

¿Con qué nombre de usuario se inició mi sesión?
Vea encima de la barra que se encuentra debajo del nombre LANDeskSystem Manager, en la sección **Conectado como**.

¿En qué equipo inicié una sesión?
Vea encima de la barra que se encuentra debajo del nombre LANDeskSystem Manager, en la sección **Conectado a**.

Al ejecutar System Manager, inmediatamente recibo un mensaje de "Tiempo de sesión agotado".
Si abre System Manager desde el menú Favoritos o Marcadores, con la extensión "/frameset.aspx" al final de la URL, no se ejecutará correctamente. Para solucionar este problema, edite sus enlaces de Marcadores o Favoritos para quitar esta extensión, o pegue la URL (sin la extensión) directamente en la ventana del explorador.

No están visibles algunos de los vínculos del panel de navegación izquierdo.
Esto sucede debido a que el administrador de red está utilizando la opción de administración basada en funciones o de seguridad a nivel de funciones de LANDeskSystem Manager, que limita la ejecución de ciertas tareas para las que se dispone de los derechos necesarios.

El rastreador no puede conectase al dispositivo.
Si el rastreador no puede conectarse al dispositivo, compruebe que el directorio de la aplicación Web haya sido configurado correctamente. Si utiliza https, debe contar con un certificado válido. Compruebe tener un certificado válido.

Recibo un error de "permiso denegado" cuando intento acceder a la consola.
Para poder hacer uso de la seguridad a nivel de funciones en Windows 2000 y 2003, es necesario deshabilitar la autenticación anónima. Verifique la configuración de autenticación en el sitio Web y la carpeta ..\LANDesk\ldsm dentro de dicho sitio.

1. En el servidor que contiene la consola Web, haga clic en **Inicio | Herramientas administrativas | Administrador de Servicios de Internet Information Server (IIS)**.
2. En el menú contextual **Sitio Web predefinido**, haga clic en **Propiedades**.
3. En la ficha **Seguridad del directorio**, dentro del área **Acceso anónimo y control de autenticación**, haga clic en **Editar**. Borre la opción **Habilitar acceso anónimo** y seleccione **Autenticación integrada de Windows**.
4. Haga clic en **Aceptar** para salir de los cuadros de diálogo.
5. En la subcarpeta .\LANDesk\ldsm del sitio Web predeterminado, haga clic en **Propiedades**. Repita los pasos 3 y 4.

Recibo un mensaje de una sesión no válida cuando abro la consola.
Es posible que el tiempo de espera de la sesión del explorador se haya agotado. Haga clic en el botón **Actualizar** del explorador para iniciar una sesión nueva.

Recibo un error de ASP.NET cuando intento iniciar la consola Web.
Si recibe un mensaje de error de ASP.NET al intentar el inicio de sesión en la consola Web, es probable que no se hayan configurado de forma debida los permisos de ASP y de directorio ASP. Reinicie la configuración ASP.NET ejecutando el siguiente comando:

```
ASPNET_REGIIS.EXE -i
```

El número de elementos por página difiere del número que especifiqué.
Al especificar la cantidad de elementos que desea mostrar por cada página, la configuración se guarda en el directorio de cookies del explorador Web, y caduca cuando se agota el tiempo de sesión.

El tiempo de espera de la consola Web se agota muy frecuentemente.
Se puede modificar el tiempo de espera de sesión predeterminada de las páginas Web de la consola. El valor para IIS es de 20 minutos de inactividad antes de que caduque la sesión. Para cambiar el tiempo de espera de sesión de IIS predeterminado:

1. En el servidor Web, abra el Administrador de servicios de Internet IIS.
2. Expanda el sitio Web predeterminado.
3. Haga clic con el botón derecho sobre la carpeta **LDSM** y, a continuación, haga clic en **Propiedades**.
4. En la ficha **Directorio virtual**, haga clic en **Configuración**.
5. Haga clic en la ficha **Opciones de aplicación** y, a continuación, establezca el valor que desee para el tiempo de espera de sesión.

Nota:LANDeskSystem Manager8.70 es un producto basado en sesiones. No desactive el estado de la sesión.

Los gráficos de informe no se muestran correctamente.
Para visualizar la barra interactiva y los gráficos circulares que aparecen en muchos informes, es necesario tener instalado Macromedia Flash Player*. Confirme que Flash esté instalado, acto seguido vuelva a ejecutar el informe.

¿Porqué veo dos instancias del mismo dispositivo en mi base de datos?
¿Ha eliminado un dispositivo de la base de datos central y lo ha reinstalado utilizando UninstallWinClient.exe?

UninstallWinClient.exe se encuentra en el recurso compartido LDMain, el cual constituye la carpeta principal del programa ManagementSuite. Solamente los administradores tienen acceso a dicho recurso compartido. Este programa desinstala los agentes de LANDesk en todos los dispositivos en los que se ejecuta. Puede moverlo a cualquier carpeta que desee o agregarlo a la secuencia de comandos de inicio de sesión. Es una aplicación de Windows que se ejecuta en segundo plano sin mostrar una interfaz. Quizá se muestren dos instancias del dispositivo en la base de datos que se ha eliminado recientemente. Una de las instancias contiene solamente datos históricos y la otra contiene datos futuros. Para más información, consulte el *Manual de implementación* en UninstallWinClient.exe.

Cuando intento detectar un dispositivo IPMI, no se enumera en la carpeta IPMI de la página de dispositivos No administrados.
Los dispositivos IPMI deben tener un BMC (controlador de administración de placa base) que se configura para poder detectarse como dispositivos IPMI y utilizar la funcionalidad completa de IPMI. Si no se configura BMC, el dispositivo puede detectarse como un equipo. Entonces puede agregar el dispositivo a la lista de dispositivos administrados y ejecutar la utilidad de Servicios de configuración para configurar la contraseña BMC. Entonces, este producto reconocerá la funcionalidad del dispositivo IPMI se reconocerá.

Agregué una unidad S.M.A.R.T. a un servidor, pero no veo el monitoreo de unidad S.M.A.R.T. en la lista de inventario del servidor.
El monitoreo de hardware depende de las capacidades del hardware instalado en un dispositivo, así como en la configuración correcta del hardware. Si un disco duro con capacidades de monitoreo S.M.A.R.T. se instala en un dispositivo, pero S.M.A.R.T. no se encuentra habilitado en la configuración del BIOS del dispositivo, o si el BIOS del dispositivo no es compatible con S.M.A.R.T., la información de monitoreo no se encontrará disponible, y no se generarán alertas resultantes.

El dispositivo de disco USB se incluye en la lista hasta que se haya ejecutado el rastreo de inventario.
Cuando un dispositivo de disco se conecta con un cable USB al dispositivo administrado, no se enumera de forma inmediata en los discos duros del inventario del dispositivo. Se enumera en Unidades lógicas una vez conectado al dispositivo. Sin embargo, aparecerá en las unidades de disco duro hasta que se haya ejecutado un rastreo de inventario en el dispositivo.

En los dispositivos administrados por Linux, el dispositivo de disco USB debe montarse para que se incluya en el inventario. Si se montó pero no se ejecutó un rastreo de inventario, aparecerá en las Unidades lógicas; luego de que el rastreo de inventario se enumere en los Discos duros. Cuando se desconecta un dispositivo, debe desmontarse del sistema. En algunos sistemas Linux que se ejecutan utilizando un kernel anterior, el dispositivo también debe estar en la lista de inventario una vez desconectado y desmontado. En este caso, el dispositivo administrado debe reiniciarse antes de que el dispositivo se elimine de la lista de inventario.

El índice de la ayuda de la consola Web está en blanco.
La ayuda en línea HTML de la consola Web contiene una función de búsqueda de texto que depende del servicio de indexación de Windows. Esta función suele estar habilitada de forma predeterminada. Si necesita habilitar la elaboración de índices en el servidor Web, siga el procedimiento siguiente:

1. Haga clic en **Inicio | Programas | Herramientas administrativas | Servicios**.
2. Haga doble clic en **Servicio de Index Server** y, a continuación, haga clic en **Iniciar**.

3. Haga clic en **Aceptar** para salir de los cuadros de diálogo.

Quizá tome un poco de tiempo (hasta varias horas) para que el servicio de indexación indexe el servidor.