LANDesk® System Manager 8.7

Guia de instalação e implantação

Capa

Nada neste documento constitui uma garantia ou licença, expressa ou implícita. A LANDesk isenta-se de todas as obrigações por tais garantias e licenças, inclusive, mas não limitada a: Adequação a um propósito específico, comercialização, não violação de propriedade intelectual ou outros direitos de terceiros ou da LANDesk, indenização e todos os outros. Os produtos LANDesk não se destinam ao uso em aplicações médicas, para o salvamento ou sustentação à vida. O leitor é advertido de que terceiros podem ter direitos de propriedade intelectual relevantes a este documento e sobre as tecnologias nele discutidas e é aconselhado a procurar orientação de um conselheiro legal competente, sem compromisso com a LANDesk.

A LANDesk reserva o direito de fazer modificações neste documento ou em especificações e descrições dos produtos relacionados, a qualquer momento, sem aviso prévio. A LANDesk não oferece nenhuma garantia de uso deste documento e não assume nenhuma responsabilidade por quaisquer erros que possam aparecer no documento nem se compromete a atualizar as informações nele contidas.

LANDesk, Autobahn, NewRoad, Peer Download e Targeted Multicast são marcas registradas ou marcas comerciais da LANDesk Software, Ltd. ou das subsidiárias por ela controladas nos Estados Unidos e/ou outros países.

*Outras marcas e nomes são propriedades de seus respectivos proprietários.

Conteúdo

Visão geral

Este guia o orienta no processo de instalação e distribuição do LANDesk® System Manager, o qual é um produto que ajuda a reduzir o custo total de propriedade tornando mais fácil gerenciar computadores e resolver problemas comuns de computadores.

A seguir estão as informações desta visão geral:

- O que esta versão contém
- Conceitos básicos do produto (incluindo termos)
- Estratégias de instalação e distribuição
- Visão geral da instalação e distribuição

O que esta versão contém

Com o crescimento da indústria de computadores, o gerenciamento de sistemas de computadores tornou-se mais complexo e difícil. O tempo gasto na manutenção e reparo de um computador durante seus anos de funcionamento pode aumentar o custo total de propriedade (TCO) para muito além do preço inicial da compra. O LANDesk® System Manager auxilia na redução do TCO, facilitando o gerenciamento do computador e também a solução de problemas comuns.

- **Ver o inventário do sistema:** O System Manager fornece extensas informações sobre a configuração de hardware e software do computador.
- **Monitoração do funcionamento do computador:** O System Manager reporta o funcionamento do computador quando há um estado de advertência ou um estado crítico, incluindo aspectos como temperatura, voltagem, memória disponível e espaço em disco.
- **Recebimento de alertas nos eventos do sistema:** O System Manager pode usar vários métodos de alerta para notificá-lo dos problemas encontrados.
- **Monitoração do desempenho em tempo real ou histórico (anterior):** O System Manager permite a monitoração do desempenho de vários objetos do sistema como, por exemplo, unidades, processadores, memória e serviços. É possível configurar ações de alerta para disparar notificações quando um contador específico cruzar um limite mais alto ou mais baixo, um número predeterminado de vezes.
- **Monitoração de processos e serviços atuais:** O System Manager permite ver os serviços atuais e os respectivos status ou permite ainda a configuração de ações de alerta para notificá-lo de mudanças no status de serviço.
- **Ligar, desligar e reinicializar computadores remotamente:** O System Manager permite o gerenciamento de energia remota a partir do console do administrador para os sistemas que o suportam.
- **Tela da tarefa agendada:** Veja ou reagende toda a distribuição de agente, descoberta,
- **Suporte melhorado ao SO:** Gerencie todos os dispositivos no seu ambiente heterogêneo de um único console. Suporta Windows 2000, 2003 e XP Professional, Red Hat Linux, SUSE Linux, HP-UX e AIX. Consulte a Etapa 1: Requisitos de sistema, para ver mais informações.

- **O Intel* AMT e o IPMI (Intelligent Platform Management Interface) oferecem suporte ao seguinte:** O System Manager suporta componentes de gerenciamento com base em hardware que fornecem a habilidade de gerenciar remotamente dispositivos gerenciados em rede em qualquer estado de sistema através da comunicação fora de banda (OOB). Desde que o dispositivo esteja conectado a uma rede corporativa e tenha alimentação de espera, você pode acessar inventário, ver informações de diagnóstico remoto, e reinicializar remotamente o sistema.
- **Suporte a servidores blade:** Suporte para servidores blade e CMMs (módulos de gerenciamento) do chassi blade, inclusive funções de gerenciamento e inventário.
- **Ferramenta de scripts:** você pode agendar e executar tarefas personalizadas nos dispositivos
- **Agendador de tarefas:** Um esquema único de banco de dados com integridade e escalonabilidade de dados melhorada que permite acessar um robusto conjunto de informações sobre dispositivos gerenciados (inclusive integração completa com Management Suite). O agendador de tarefas é parte deste esquema único. Agora você pode ver todas as tarefas (descoberta, configuração de agentes, em uma janela comum. Nessa janela, você pode reagendar, modificar o agendamento ou tornar o agendamento reocorrente.
- **Administração com base em função:** configura o acesso dos usuários a ferramentas e dispositivos de rede de acordo com a função administrativa do usuário na organização. Com a administração baseada em funções você atribui um escopo para determinar os dispositivos que um usuário pode ver e gerenciar, e os direitos para determinar as tarefas que ele pode realizar.
- **Descoberta de dispositivos não gerenciados:** Descobre dispositivos na rede através de uma variedade de métodos. O produto identifica servidores Windows ou Linux, servidores blade e gabinetes blade, servidores habilitados com IPMI, servidores Intel habilitados para AMT assim como outros dispositivos de rede. A descoberta de dispositivos pode ser agendada para torná-lo constantemente alerta para a existência de novos dispositivos. É possível também gerar relatórios sobre os dispositivos não gerenciados na sua rede.
- **Segurança avançada:** um modelo baseado em certificado que permite aos dispositivos apenas se comunicarem com os servidores núcleo e consoles autorizados.
- **Distribuição de software:** Automatiza o processo de instalação dos aplicativos de software ou de distribuição de arquivos aos dispositivos.
- **Relatórios:** relatórios predefinidos de serviço que estão disponíveis para o planejamento e análise estratégica.
- **Suporte a tarefa agendada:** Fornece múltiplos logins para o serviço do planejador utilizar para autenticação, quando estiver executando tarefas em dispositivos que não têm agentes. Isto é especialmente útil no gerenciamento de dispositivos em vários domínios do Windows.

Conceitos básicos do produto

O System Manager gerencia dispositivos executando vários sistemas operacionais diferentes, inclusive Windows 98 Second Edition*, Windows 2000 Pro SP4, Windows XP Pro SP1, servidores Windows* 2000/2003, servidores Red Hat Enterprise Linux v3, SUSE Linux 9 servers, servidores HP-UX e AIX e fornece uma interface comum para o gerenciamento de dispositivos desses sistemas operacionais de rede. Ele também pode coexistir com os produtos LANDesk como, por exemplo, o LANDesk® Management Suite e LANDesk® Server Manager.

Termos do produto

- **Servidor núcleo:** o centro de um domínio de gerenciamento. Todos os arquivos e serviços essenciais do produto estão contidos no servidor núcleo. Um domínio de gerenciamento tem apenas um servidor núcleo. Um servidor núcleo pode ser um servidor novo ou um que foi redirecionado para o fim específico.
- **Console:** O console baseado em browser que é a interface principal do produto.
- Banco de dados núcleo:O produto cria um banco de dados MSDE no servidor núcleo para armazenar dados de gerenciamento.
- **Dispositivos gerenciados:** Dispositivos na rede, que têm agentes do produto instalados. "Dispositivos" são computadores de desktop, servidores, computadores laptop/móveis, chassis blade, etc. Um servidor núcleo pode gerenciar milhares de dispositivos.
- **Público:** Itens visíveis a todos os usuários (por exemplo, grupos, pacotes de distribuição ou tarefas). Quando um usuário modifica um item Público, a modificação permanece pública. Grupos públicos são criados por um usuário com direitos administrativos.
- **Privado ou Usuário:** Itens criados pelo usuário conectado no momento. Eles não são visíveis aos outros usuários. Os itens privados ou usuário aparecem sob as árvores **Meus métodos de entrega**, **Meus pacotes** e **Minhas tarefas**. Os usuários com direitos administrativos podem ver os grupos Privado e pacotes e tarefas do Usuário.
- **Comum:** Um item visível a outros usuários. Quando um usuário adquire propriedade de um item Comum (modificando-o), o item se divide em dois: o item Comum permanece e o item Usuário é salvo na pasta Usuários. A instância Usuário do item não é mais visível aos outros usuários. Um usuário pode marcar qualquer tarefa visível como Comum, assim compartilhando-a com outros usuários. Após o usuário desmarcar a opção Comum da propriedade do item, a tarefa só é visível no grupo de tarefas Usuário.

Como o produto se adequa à minha rede?

Este produto usa a infra-estrutura da rede existente para estabelecer conexões com os dispositivos que ele gerencia. A tarefa de gerenciar os dispositivos existentes é bem simplificada, esteja você gerenciando uma rede pequena ou um grande ambiente empresarial.

Uso do System Manager com Management Suite ou Server Manager

Se tiver o System Manager e quiser usá-lo com o Management Suite ou Server Manager, é necessário usar o utilitário de ativação do servidor núcleo para fornecer um nome de usuário e uma senha válidos para o produto com o qual quiser utilizar System Manager. Uma instalação System Manager / Management Suite lhe proporciona três consoles para trabalhar: os consoles Management Suite Windows 32 e Web e o console Web System Manager. O console do Server Manager contém três elementos de navegação (Alerta, Monitoração e Logs) que têm funcionalidade não encontrada nos dois consoles do Management Suite.

Se você distribuir o Management Suite, a instalação Management Suite remove o agente System Manager nos dispositivos gerenciados e vice-versa. Ao executar o Management Suite com o System Manager, o recurso de configuração Management Suite inclui as opções de monitoração.

Instalação do System Manager com o Management Suiteou Server Manager já instalados

Se já tiver o Management Suite ou o Server Manager instalados no servidor núcleo e quiser acrescentar o System Manager, use a mesma instalação original do Management Suite ou Server Manager.

1. Abra o autorun.exe.
2. Clique em **Instalar agora**.
3. Selecione um idioma e clique em **OK**.
4. Aparece a tela de boas-vindas. Clique em **Avançar**.
5. Selecione **Modificar** (se necessário) e clique em **Avançar**.
6. Clique em LANDesk® Server Manager, em seguida clique em **Avançar**.
7. Siga as instruções na tela do assistente.

Requisitos de sistema para o servidor núcleo

Enquanto você avalia qual servidor será configurado como o servidor núcleo, verifique os requisitos de sistema e confirme se o servidor atende ou excede os requisitos indicados na Etapa 1: Requisitos de sistema. O verificador de pré-requisitos faz isso automaticamente.

Recomenda-se enfaticamente um servidor núcleo dedicado
Devido ao tráfego que passa pelo servidor núcleo para gerenciar o domínio, recomendamos enfaticamente que cada servidor núcleo seja dedicado à hospedagem do produto.

Se outros produtos forem instalados no mesmo servidor, poderão ocorrer problemas de recursos a curto e a longo prazo.

Não instale os componentes do servidor núcleo em um controlador de domínio primário, em um controlador de domínio de backup ou em um controlador do Active Directory.

Estratégias de instalação e distribuição

Ao instalar através do Autorun da mídia do produto, o programa de instalação verifica automaticamente se o seu núcleo satisfaz esses requisitos. A instalação e distribuição de um aplicativo de sistema inteiro para uma rede heterogênea, requer uma metodologia deliberada e um planejamento significativo *antes* da execução do programa de configuração. Este guia contém estratégias de configuração do produto. Antes de fazer a distribuição dele, é necessário caracterizar brevemente suas necessidades de gerenciamento.

Considerações sobre as estratégias de distribuição

A distribuição é o processo de expansão dos recursos de gerenciamento para servidores que você deseja incluir no domínio. Neste guia, a distribuição é discutida em "etapas".

A estratégia de distribuição em etapas oferece uma abordagem estruturada para a habilitação do gerenciamento nos dispositivos. Essa abordagem baseia-se em dois princípios simples:

- Primeiro, a distribuição dos componentes do produto que causam o menor impacto na rede existente, avançando para os componentes que causam maior impacto.
- Segundo, distribuição do produto em estágios bem planejados, em vez de distribuir todos os serviços de uma vez, processo que pode dificultar qualquer solução de problemas necessária.

Este guia é organizado seqüencialmente para ajudá-lo a distribuir o produto. Comece com o primeiro capítulo, "Etapa 1: Desenvolvimento do domínio de gerenciamento" posteriormente neste guia. É necessário continuar na ordem seqüencial em cada fase.

Visão geral da instalação e distribuição

Este guia agrupa tarefas de instalação e distribuição nas etapas apresentadas abaixo. Cada etapa tem uma seção correspondente neste guia que o orientará no processo de instalação. O capítulo é destinado a auxiliá-lo a iniciar o uso do produto rapidamente através da configuração de serviços, execução do console, descoberta de dispositivos, transferência de dispositivos para a lista Meus dispositivos e a configuração de dispositivos gerenciados para executar ações. Ele é projetado para ser sucinto, pressupondo-se que o resto do manual será consultado para ver os detalhes. Alguns procedimentos neste guia são repetidos no capítulo Guia de introdução.

Resumo da etapa 1

Durante a etapa 1 de instalação, você cria o domínio de gerenciamento através das seguintes tarefas:

- Coleta de informações da rede.
- Verificação da conformidade da rede aos requisitos do sistema.

Para obter mais detalhes, consulte a "Etapa 1: Desenvolvimento do domínio de gerenciamento" posteriormente neste guia.

Resumo da etapa 2

Durante a etapa 2, o produto é instalado através da execução das seguintes tarefas:

- Instalação do servidor núcleo

Para ver mais detalhes, consulte a "Etapa 2: Instalação do núcleo e do console", adiante neste guia.

Resumo da etapa 3

Durante a etapa 3 da instalação, você descobre dispositivos na rede e faz a distribuição dos agentes do produto. Os agentes podem ser instalados por envio (push), do console ou por recepção (pull), do compartilhamento do servidor.

Para ver mais detalhes, consulte a "Etapa 3: Distribuição de agentes para dispositivos", adiante neste guia.

Introdução

Visão geral

Bem-vindo ao LANDesk® System Manager, um aplicativo de gerenciamento de dispositivos independente que maximiza o seu tempo valioso ao permitir a gestão rápida e eficiente dos seus dispositivos, economizando tempo e dinheiro para a sua organização. O System Manager permite gerenciar seus dispositivos em um local central, agrupá-los para ações (como, ciclagem de alimentação, avaliação de vulnerabilidade ou configuração de alerta), resolver problemas remotamente, manter a rede segura e os dispositivos atualizados com os patchs mais recentes.

Este guia é destinado a auxiliá-lo a iniciar o uso do System Manager de forma rápida através da configuração de serviços, execução do console, descoberta de dispositivos, transferência de dispositivos para a lista Meus dispositivos e a configuração de dispositivos gerenciados para executar ações.

O System Manager é um aplicativo da web que permite o acesso através do seu navegador de forma a permitir-lhe gerenciar seus servidores de uma workstation remota. Ele se comporta como muitos dos aplicativos da web, com os quais você já deve estar acostumado, mas também contém vários controles do tipo Windows avançados para melhorar a usabilidade. Por exemplo, passe o ponteiro do mouse sobre um controle e clique duas vezes ou clique com o botão direito no mesmo (da mesma forma como faria em um aplicativo Windows). Por exemplo, na lista Meus dispositivos, clique duas vezes em um nome de dispositivo para acessar informações específicas ou clique com o botão direito para ver as ações disponíveis.

As etapas abaixo o orientam na utilização do System Manager, na descoberta de dispositivos na sua rede, na seleção de servidores para mudar para a lista Meus dispositivos, na distribuição de agentes e na seleção desses dispositivos para várias tarefas.

Execução do programa de instalação

Durante a instalação, na página de instalação Execução automática (Autorun), selecione LANDesk® System Manager. As instruções específicas de instalação podem ser encontradas na Fase 2 do Guia de distribuição e instalação.

Após instalar o System Manager, você já está pronto para começar a usá-lo. As seções abaixo lhe mostrarão como realizar várias tarefas requeridas: execução do utilitário de ativação do núcleo, configuração de serviços, descoberta de computadores, especificação de quais dispositivos gerenciar ativamente mudando os servidores para a lista Meus dispositivos, agrupamento de dispositivo, adição de usuários e distribuição de agentes. Quando essas tarefas são concluídas, você está pronto para começar a explorar o conjunto de recursos robustos do System Manager e ver como eles podem ajudá-lo a gerenciar seus dispositivos.

Ativar o servidor núcleo

Para executar o produto será necessário ativar o servidor núcleo.

Use o utilitário de Ativação do servidor núcleo para:

- Ativar um novo servidor núcleo System Manager pela primeira vez
- Atualizar um servidor núcleo System Manager

Cada servidor núcleo deve ter um certificado de autorização exclusivo.

Este utilitário é executado automaticamente na primeira reinicialização.

Com o seu servidor núcleo conectado na Internet,

1. Clique em Iniciar | Todos os programas | Ativação do servidor núcleo. O nome de usuário e a senha já estão preenchidos.
2. Clique em Ativar.

O núcleo se comunica com o servidor de licenciamento de software via HTTP. Se você usa um servidor proxy, clique na guia Proxy do utilitário e digite as informações do seu proxy. Se seu núcleo tem uma conexão com a internet, a comunicação com o servidor de licenciamento é automática, não exigindo nenhuma intervenção de sua parte. Se o núcleo não estiver conectado, clique em Fechar na reinicialização e envie o arquivo de autorização por email para licensing@landesk.com.

Periodicamente, o servidor núcleo gera informações de verificação de contagem de nós no arquivo "\Arquivos de programa\LANDesk\Authorization Files\LANDesk.usage". Esse arquivo é enviado periodicamente para o servidor de licenciamento da LANDesk Software. Esse arquivo está em formato XML, é assinado digitalmente e criptografado. Todas as mudanças feitas manualmente neste arquivo invalidam seu conteúdo e também o próximo relatório de utilização para o servidor de licenciamento.

- O utilitário de Ativação do servidor núcleo não inicia automaticamente uma conexão dial-up à internet, mas se você iniciar a conexão dial-up manualmente e executar o utilitário de ativação, o utilitário poderá utilizar a conexão dial-up para enviar os dados do relatório de utilização.
- O servidor núcleo pode também ser ativado por email. Envie o arquivo com a extensão .TXT localizado em Arquivos de programa\LANDesk\Authorization para licensing@landesk.com. O suporte ao cliente da LANDesk responderá ao email com um arquivo e as instruções sobre como copiá-lo no servidor núcleo para completar o processo de ativação.

Adição de usuários

Os usuários do System Manager podem fazer logon no console do produto e realizar determinadas tarefas em dispositivos específicos da rede. Você gerencia seus usuários através do recurso de administração baseado em funções. A administração baseada em funções lhe permite atribuir a usuários do produto funções administrativas especiais com base em seus direitos e escopos. Direitos determinam as ferramentas e os recursos do produto que um usuário pode ver e utilizar. Escopo determina a gama de dispositivos que um usuário pode ver e gerenciar. Você pode criar uma variedade de usuários e personalizar seus direitos e escopos para se adequarem aos requisitos da gestão. Por exemplo, você pode criar um usuário que assuma o papel de Help Desk dando a ele os direitos necessários para essa função. Há mais detalhes disponíveis no capítulo Administração baseada em funções doSystem Manager Guia do usuário.

Quando você instala o produto, automaticamente são criadas duas contas de usuário (veja a seguir). Se desejar adicionar mais usuários, você pode fazer isso manualmente. Na verdade, os usuários não são criados no console. Em vez disso, os usuários aparecem no grupo Todos os usuários (clique em Usuários no painel esquerdo de navegação) após a sua inclusão no grupo LANDesk Management Suite do ambiente de usuários do Windows NT no servidor núcleo. O grupo Usuários mostra todos os usuários que integram o grupo LANDesk Management Suite no servidor núcleo.

Existem dois usuários padrão no grupo Usuários. Um dos usuários é o Administrador padrão. Esse é o usuário administrativo que estava conectado ao servidor quando o produto foi instalado.

O outro usuário padrão é o Usuário modelo padrão.Esse usuário contém um modelo de propriedades de usuário (direitos e escopo) usado para configurar novos usuários quando estes são incluídos no grupo Managemente Suite. Em outras palavras, quando um usuário é adicionado a esse grupo no ambiente Windows NT, ele herda os direitos e o escopo definidos atualmente nas propriedades do Usuário modelo padrão. Se o Usuário modelo padrão tiver todos os direitos selecionados e o Escopo de todas as máquinas padrão selecionado, todos os novos usuários inseridos no grupo LANDesk Management serão adicionados ao grupo Usuários com direitos a todas as ferramentas do produto e acesso a todos os dispositivos.

Você pode mudar as configurações de propriedades do Usuário modelo padrão, selecionando-o e clicando em Editar. Por exemplo, se você deseja adicionar um grande número de usuários de uma só vez, mas não quer que eles tenham acesso a todas as ferramentas ou todos os dispositivos, altere, primeiramente, as configurações do Modelo padrão de usuário e, em seguida, adicione os usuários ao grupo LANDesk Management Suite (veja os passos a seguir). O Usuário modelo padrão não pode ser removido.

Quando você adiciona um usuário ao grupo LANDesk Management Suite no Windows NT, ele é automaticamente lido no grupo Usuários da janela Usuários, herdando os mesmos direitos e o escopo do Usuário modelo padrão atual. São mostrados o nome, o escopo e os direitos do usuário. Além disso, novos subgrupos de usuários, que recebem nome do ID exclusivo de login do usuário, são criados nos grupos Dispositivos de usuários, Consultas de usuários, Relatórios de usuários e Scripts de usuários (observe que APENAS o Administrador pode ver os grupos de Usuários).

Por outro lado, se você remover um usuário do grupo LANDesk Management Suite, ele não aparecerá mais na lista Usuários. A conta do usuário permanece no servidor núcleo, podendo

ser adicionada novamente ao grupo LANDesk Management Suite a qualquer momento. Além disso, os subgrupos do usuário em Dispositivos de usuários, Consultas de usuários, Relatórios de usuários e Scripts de usuários são preservados para que seja possível restaurar o usuário sem perder seus dados, e de maneira que esses dados possam ser copiados para outros usuários.

Atualize o frame Usuários no console do System Manager pressionando F5. Para aprender a adicionar um grupo de usuário ou de domínio ao grupo LANDesk Management Suite ou a criar uma nova conta de usuário, consulte "Adição de usuários do produto" no capítulo Administração com base em funções do System Manager *Guia do usuário*.

Para adicionar um usuário ou grupo de domínio ao grupo LANDesk Management Suite:

1. Navegue até o utilitário do servidor **Ferramentas administrativas | Gerenciamento de computadores | Usuários e Grupos locais | Grupos**.
2. Clique com o botão direito no grupo **LANDesk Management Suite** e, em seguida, clique em **Adicionar ao grupo**.
3. Clique em **Adicionar**, em seguida, digite ou selecione um usuário (ou usuários) na lista.
4. Clique em **Adicionar** e, a seguir, clique em **OK**.

Nota: Também é possível adicionar um usuário ao grupo LANDesk Management Suite clicando com o botão direito na conta do usuário na lista **Usuários**, clicando em **Propriedades | Membro de** e, em seguida, em **Adicionar** para selecionar o grupo e adicionar o usuário.

Se as contas de usuário já não existirem no servidor, é preciso, antes, criá-las no servidor.

Para criar uma nova conta de usuário

1. Navegue até o utilitário do servidor **Ferramentas administrativas | Gerenciamento de computadores | Usuários e grupo locais | Usuários**.
2. Clique com o botão direito do mouse em **Usuários** e, em seguida, clique em **Novo usuário**.
3. No diálogo **Novo usuário**, digite um nome e uma senha.
4. Especifique as configurações de senha.
5. Clique em **Criar**. A caixa de diálogo **Novo usuário** permanece aberta para que você possa criar outros usuários.
6. Clique em **Fechar** para sair da caixa de diálogo.

Adicione os usuários ao grupo LANDesk Management Suite para que eles apareçam no grupo Usuários no console.

Configuração de serviços e credenciais

Antes de poder gerenciar dispositivos na rede, é preciso fornecer as credenciais necessárias ao System Manager. Use o utilitário Configurar serviços (Configure Services) no núcleo (SVCCFG.EXE) para especificar as credenciais requeridas do sistema operacional, Intel* AMT e IPMI BMC. Especifique também configurações adicionais como padrões de inventário, configurações de fila de espera PXE e as configurações de banco de dados LANDesk.

Use Configurar serviços para configurar:

- o nome da base de dados, o nome do usuário e a senha. (Definidos durante a instalação.)
- Credenciais para agendamento de trabalhos para os dispositivos gerenciados. (Você pode inserir mais de um conjunto de credenciais de administrador.)
- Credenciais para configuração de BMCs de IPMI. (Você pode inserir apenas um conjunto de credenciais de BMC.)
- Credenciais para a configuração de dispositivos habilitados para Intel AMT. (Você pode inserir apenas um conjunto de credenciais da Intel AMT.)
- O intervalo de varredura do software do servidor, a manutenção, os dias para realizar varreduras do inventário e o histórico da duração do login.
- Como lidar com IDs de dispositivos duplicados.
- Configuração do agendador, incluindo trabalhos agendados e intervalos de avaliação de consultas.
- Configuração de tarefas personalizadas, incluindo o tempo limite de execução remota.

1. No servidor núcleo, clique em Iniciar | Todos os programas | LANDesk | Configurar serviços LANDesk
2. Clique na guia Planejador.
3. Clique no botão Alterar login.
4. Insira as credenciais que quer que o serviço use nos dispositivos gerenciados, em geral, uma conta de administrador de domínio.
5. Clique em Adicionar. Adicione credenciais conforme necessário, se nem todos os dispositivos gerenciados tiverem as mesmas contas de nome de usuário administrador habilitadas.
6. Clique em Aplicar.
7. Se tiver servidores habilitados com IPMI no seu ambiente, clique na guia Senha de BMC. Digite a senha na caixa de texto Senha, redigite a senha na caixa de texto Confirmar senha, em seguida, clique em OK. (Todos os servidores IPMI gerenciados devem compartilhar o mesmo nome e senha de BMC.)
8. Se você tiver dispositivos habilitados com o Intel AMT, clique na guia Configuração do Intel AMT. Digite o nome do usuário atual configurado Intel AMT no quadro de texto Nome do usuário e senha configurada atual no quadro de texto Senha. Redigite a senha no quadro a de texto Confirmar senha, em seguida cliue em OK.
9. Defina outras configurações que desejar como, por exemplo, intervalos de análise de software.
10. Clique em OK para salvar as mudanças.

Clique em **Ajuda** em cada guia do Configurar serviços (Configure Services) para ver mais informações.

Execução do console

O System Manager inclui um pacote completo de ferramentas que permitem exibir, configurar, gerenciar e proteger os dispositivos na rede. O console é o ponto de entrada pelo qual você pode usar estas ferramentas.

O painel superior no console mostra o servidor ao qual você está conectado, e o nome do usuário como está conectado. A lista Meus dispositivos é a janela principal do console e o ponto de partida para a maioria das funções. O painel esquerdo mostra as ferramentas disponíveis. O painel da direita no console mostra os diálogos e as telas que permitem realizar tarefas de gerenciamento.

A praticidade do console é que ele permite realizar todas as funções de um local remoto como a sua estação de trabalho, liberando-o da necessidade de ir a cada servidor ou de ir a cada

dispositivo gerenciado individualmente para fazer manutenção de rotina ou solução de problemas.

O console pode ser iniciado de três maneiras:

- No servidor núcleo, clique em Iniciar | Todos os programas | LANDesk System Manager.
- Em um navegador na workstation remota, digite o URL http://coreserver/LDSM.

Como descobrir dispositivos

Use a guia **Configurações de descoberta** para criar novas configurações de descoberta, editar e excluir configurações existentes, e agendar uma configuração para descoberta. Cada configuração de descoberta consiste em um nome descritivo, nos intervalos de endereços IP a serem analisados e no tipo de descoberta.

Após criar a configuração, use o diálogo **Agendar descoberta** para configurar o horário de execução.

1. No painel de navegação esquerdo, clique em **Descoberta de dispositivos**.
2. Na guia **Configurações de descoberta**, clique no botão **Nova**.
3. Preencha os campos descritos abaixo. Quando terminar, clique no botão **Adicionar** e clique em **OK**.

O texto abaixo descreve as partes da caixa de diálogo da **Configuração da descoberta**.

- **Nome de configuração:** Digite um nome para essa configuração. Dê à configuração um nome significativo que lhe permita lembrar a configuração facilmente. O nome não pode ter mais de 255 caracteres, e não deve conter os seguintes caracteres: **"**, **+**, **#**, **&** ou **%**. O nome da configuração não será mostrado após o uso de um desses caracteres.
- **Varredura de rede padrão:** Procura dispositivos enviando pacotes ICMP para endereços IP na faixa que você especificar. Essa é a pesquisa mais completa, porém a mais lenta. Como padrão, esta opção utiliza o NetBIOS para coletar informações sobre o dispositivo.

  A opção de análise de rede tem uma opção de **Impressão digital IP** onde a descoberta de dispositivo tenta descobrir o tipo de SO através de respostas de pacotes TCP. A opção Impressão digital IP atrasa um pouco a descoberta.

  A opção de análise de rede também tem uma opção **Usar SNMP**, onde você pode configurar a análise para usar. Clique em **Configurar** para digitar informações sobre a sua configuração to SNMP.

- **Descoberta LANDesk CBA:** Procura o agente padrão de gerenciamento (antes denominado agente de base comum, [CBA] no Management Suite) nos dispositivos. O agente padrão de gerenciamento permite que o servidor núcleo descubra e comunique-se com outros clientes na rede. Esta opção descobre os dispositivos que têm os agentes do produto. Roteadores normalmente bloqueiam o agente padrão de gerenciamento e o tráfego PDS2. Para executar uma descoberta padrão de CBA em várias subredes, o roteador deve ser configurado para permitir difusões diretas em múltiplas subredes.

  A opção de descoberta CBA também tem uma opção **Descoberta LANDesk PDS2**, onde a descoberta de dispositivo procura o Serviço de descoberta de ping LANDesk (PDS2) nos dispositivos. LANDesk Produtos de software como LANDesk® System Manager, Server Manager e LANDesk Client Manager usam o agente PDS2. Selecione esta opção se houver dispositivos na sua rede com esses produtos instalados. A descoberta CBA não é suportada pelos computadores Linux, mas se você escolher PDS2, os computadores Linux com um agente instalado podem ser descobertos.
- **IPMI:** Procura servidores habilitados com IPMI. IPMI é uma especificação desenvolvida pela Intel,***** H-P,* NEC,* e Dell* para definir a interface de mensagens e do sistema para hardwares habilitados para gerenciamento. O IPMI contém recursos de monitoração e recuperação que lhe permitem acessar esses recursos independentemente do dispositivo estar ligado ou desligado, ou do estado no qual o SO se encontrar. Lembre-se que se o BMC (Baseboard Management Controller) não estiver configurado, ele não responderá aos pings ASF, usados pelo produto, para descobrir o IPMI. Isso significa que você terá que descobrí-lo como um computador normal. Quando enviar o cliente, o ServerConfig analisará o sistema e detectará que é IPMI e configurará o BMC.
- **Chassi de servidor:** Procura módulos de gerenciamento (CMMs) de chassis de servidores blade. Os blades no chassi de servidores são detectados como servidores normais.
- **Intel* AMT:** Procura dispositivos com suporte para a Tecnologia Intel Active Management.
- **IP inicial:** Digite o endereço IP inicial do intervalo de endereços a ser analisado.
- **IP final:** Digite o endereço IP final do intervalo de endereços a ser analisado.
- **Máscara da sub-rede:** Digite a máscara da sub-rede do intervalo de endereços IP que você está analisando.
- **Adicionar:** Adiciona os intervalos de endereços IP à fila de trabalho, na parte inferior do diálogo.
- **Limpar:** Limpa os campos dos intervalos de endereços IP.
- **Editar:** Selecione um endereço de IP na fila de trabalhos e clique em **Editar**. O intervalo aparece nas caixas de texto acima da fila onde você pode editar o intervalo e adicionar o novo intervalo para a fila de trabalhos.
- **Remover:** Remove o intervalo de endereços IP selecionado da fila de trabalho.
- **Remover todos:** Remove todos os intervalos de endereços IP selecionados da fila de trabalho.

Agora que você configurou uma tarefa de descoberta, está preparado para descobrir os dispositivos conectados à rede agendando a execução da tarefa de descoberta.

Agendamento e execução da tarefa de descoberta

Use o botão Agendar na guia Descobrir dispositivos para abrir a caixa de diálogo Agendar descoberta. Use este diálogo para agendar a execução de uma descoberta. Você pode agendar uma tarefa de descoberta para executar imediatamente, em algum ponto no futuro, criar uma agenda que se repete ou executá-la apenas uma vez e nunca mais se preocupar com ela.

Após agendar uma tarefa de descoberta, consulte a guia Tarefas de descoberta para ver o status da descoberta. O agendamento de uma tarefa de descoberta que se repete o assiste através da descoberta automática de novos dispositivos que entram na rede.

A caixa de diálogo Agendar descoberta contém as seguintes opções.

- **Deixar sem agendar:** Deixa a tarefa sem agendar, mas a mantém na lista Configurações de descoberta para uso futuro.
- **Iniciar agora:** Executa a tarefa assim que possível. Pode levar até um minuto para a tarefa iniciar.
- Iniciar na hora agendada: Inicia a tarefa na hora em que você especificar. Se você clicar nessa opção, precisará digitar o seguinte:
    - **Hora:** A hora em que você deseja que a tarefa inicie.
    - **Data:** O dia em que você deseja que a tarefa inicie. Dependendo do local, a ordem da data será dia-mês-ano ou mês-dia-ano.
    - **Repetir a cada:** Se quiser que a tarefa seja repetida, selecione o tipo de repetição Diária, Semanal ou Mensal. Se escolher Mensal e a data não existir em todos os meses (por exemplo, 31), a tarefa só será executada nos meses que tiverem esse dia.

Para agendar uma tarefa de descoberta

1. No painel de navegação à esquerda, clique em Dispositivos descobertos.
2. Na guia Configurações da descoberta, selecione a configuração que desejar e clique em Agendar. Configure a agenda da descoberta e clique em Salvar.
3. Monitore o andamento da descoberta na guia Tarefas de descoberta. Clique em Atualizar para atualizar o status.
4. Quando o processo de descoberta terminar, clique em Não gerenciadopara ver todos os dispositivos descobertos no painel superior de Dispositivos descobertos (o painel não se atualiza automaticamente).

Como ver os dispositivos descobertos

Os servidores e dispositivos descobertos são categorizados por tipo de dispositivo no painel Dispositivos descobertos. A pasta Computadores aparece como padrão. Clique nas pastas no painel esquerdo para ver os dispositivos em categorias diferentes. Clique em Não gerenciado para ver todos os dispositivos retornados pela descoberta.

- Os chassis de servidores blade aparecem na pasta **Chassi**.
- Os servidores padrão de empresa aparecem na pasta **Computadores**.
- Os roteadores e outros dispositivos aparecem na pasta **Infra-estrutura**.
- Os dispositivos habilitados com IPMI aparecem na pasta **Intel AMT**.
- Os servidores habilitados com IPMI aparecem na pasta **IPMI**.
- Os dispositivos não caracterizados aparecem na pasta **Outro**.
- A impressoras aparecem na pasta **Impressoras**.

Nota: Alguns servidores Linux aparecem com "Unix" genérico como nome do sistema operacional (ou, algumas vezes, como Outro). Quando o agente padrão de gerenciamento é distribuído, esses servidores atualizam suas entradas de nome de SO na lista Meus dispositivos e mostram um inventário completo. Para ver os servidores descobertos

1. Na página Descoberta de dispositivos, no painel esquerdo, clique em Computadores ou outro tipo de dispositivo que você desejar ver. Os resultados são mostrados no painel direito.
2. Para filtrar os resultados, clique no ícone Filtro e digite pelo menos uma parte do que está procurando e clique em **Localizar**.

Atribuição de nomes

Ao fazer uma descoberta de análise de rede, alguns servidores retornam com o nome do nó vazio (ou nome de host). Isso acontece mais freqüentemente com os servidores Linux. É necessário atribuir um nome ao dispositivo antes de poder Gerenciar para mudá-lo para a lista Meus dispositivos.

1. Na página Descoberta de dispositivos, clique no dispositivo com o nome em branco. (É necessário clicar na área em branco na coluna do nome do nó.)
2. Clique em Atribuir nome na barra de ferramentas.
3. Digite o nome e clique em **OK**.

Quando você instala um agente de produto em dispositivo, ele analisa automaticamente o nome do host e atualiza o banco de dados núcleo com as informações corretas.

Como mover dispositivos para a lista Meus dispositivos

Depois da descoberta, é necessário selecionar manualmente os dispositivos que quiser gerenciar e mudar para a lista Meus dispositivos. A mudança do dispositivo não instala nenhum software nele. Ela apenas torna o dispositivo disponível para consulta, agrupamento e ordenação na lista Meus dispositivos. Dispositivos específicos são selecionados como "alvo" para ações específicas, um modelo semelhante ao de um "carrinho de compras" em muitos aplicativos da web.

1. Na tela Dispositivos descobertos, clique no dispositivo que desejar mover para a lista Meus dispositivos. Selecione múltiplos dispositivos utilizando as combinações **SHIFT+clique** ou **CTRL+ clique**.
2. Clique no botão **Alvo**. Se ele não estiver visível, clique em **<<**, na barra de ferramentas. O botão se encontra na extremidade direita. Ou, clique com o botão direito nos servidores selecionados e clique em **Alvo**.
3. No painel inferior, clique na guia **Gerenciar**.
4. Selecione **Mover** os dispositivos selecionados para o banco de dados de gerenciamento ou selecione Mover os dispositivos alvo.
5. Clique em **Mover**.

Clique em **Mover** para mudar os dispositivos para a lista Meus dispositivos e colocar as informações do dispositivo no banco de dados. Quando as informações estiverem no banco de dados, você pode executar consultas e relatórios limitados nele (por exemplo, por nome de dispositivo, endereço IP ou SO).

Como agrupar dispositivos para ações

É uma boa idéia organizar os dispositivos em grupos, isto é, por região ou por função para poder executar ações neles de maneira mais rápida. Por exemplo, você pode verificar as velocidades dos processadores de todos os dispositivos em um local específico.

1. Na lista Meus dispositivos, clique em Grupos privados ou Grupos públicos, e clique em Adicionar grupo.
2. Digite o nome do grupo na caixa Nome do grupo.
3. Clique no tipo de grupo que deseja criar.
    - **Estática:**Dispositivos que foram adicionados ao grupo. Eles permanecem no grupo até serem removidos ou até você não os gerenciar mais.
    - **Dinâmica:**Dispositivos que satisfazem um ou mais critérios definidos por uma consulta. Por exemplo, um grupo pode conter todos os servidores que estão em estado de Advertência no momento. Eles permanecem no grupo enquanto corresponderem aos critérios definidos para o grupo. Dispositivos são adicionados automaticamente a grupos dinâmicos quando satisfazem os critérios de consulta do grupo.
4. Ao terminar, clique em **OK**.
5. Para adicionar dispositivos a um grupo estático, clique em dispositivos no painel direito da lista Meus dispositivos, clique em Mover/Copiar, selecione o grupo e clique em **OK**.

Configuração de dispositivos para gerenciamento

A descoberta de dispositivos por si só não os coloca sob o guarda-chuva do gerenciamento. Antes de poder gerenciar os dispositivos totalmente com o console e receber alertas de condições, é necessário instalar neles os agentes de gerenciamento. Você pode decidir instalar a configuração de agente padrão (a qual instala todos os agentes de gerenciamento) ou personalizar a sua própria configuração de agente para instalá-la em seus dispositivos. (A configuração de agente deve incluir o agente de monitoração para receber alertas de estado de funcionamento.)

Você pode instalar os agentes de gerenciamento de qualquer das seguintes maneiras:

- Selecione os dispositivos alvo na lista Meus dispositivos, em seguida agende uma tarefa de configuração de agentes para instalar os agentes remotamente nos dispositivos. (etapas abaixo)
- Faça um mapeamento para o compartilhamento LDlogon do núcleo (//coreserver/ldlogon) e execute SERVERCONFIG.EXE. (as etapas estão em "Instalação dos agentes por recepção" no capítulo Instalação e configuração do agente de dispositivo do System Manager Guia do usuário)
- Crie um pacote de instalação de dispositivo auto-extraível. Execute esse pacote localmente no dispositivo para instalar os agentes. Isso deve ser feito conectado com privilégios administrativos. (as etapas estão em "Instalação do agente com um Pacote de instalação" no capítuo Instalação e configuração do agente de dispositivo do System Manager Guia do usuário)

Para instalar o agente por envio:

1. Selecione dispositivos alvo na lista Meus dispositivos (conforme explicado acima em Mudar dispositivos para a lista Meus dispositivos)
2. No painel de navegação esquerdo, clique em Configuração do agente, clique com o botão direito na configuração que quer enviar e clique em Agendar tarefa.
3. No painel esquerdo, clique em Selecionar dispositivos (Dispositivos alvo) e clique no botão Adicionar lista de alvos.
4. Clique em Agendar tarefa, clique em Iniciar agora para iniciar a tarefa imediatamente ou em Iniciar depois e defina a data e a hora do início da tarefa, e clique em Salvar.

Você pode ver o status da tarefa de rollup na guia Tarefas de configuração..

Instalação de agentes de servidores Linux

É possível distribuir e instalar remotamente agentes Linux e RPMs em servidores Linux. Seu servidor Linux deve estar configurado corretamente para isto funcionar. As instruções para a configuração correta de um servidor Linux encontram-se em "Instalação de agentes de servidor" no capítulo Instalação e configuração de agente de dispositivo no *System Manager Guia do usuário.*

Configuração de alertas

Quando ocorre um problema ou outro evento em um dispositivo (por exemplo, o dispositivo está com pouco espaço no disco) o O System Manager pode enviar um alerta. Você pode personalizar esses alertas ao escolher o nível de severidade ou o limite que acionará o alerta. Os alertas são enviados para o console e podem ser configurados para executar ações específicas. Você pode definir alertas para muitos eventos ou problemas em potencial. O produto vem com um conjunto de regras de alerta o qual é instalado em um dispositivo gerenciado quando o componente de monitoração é instalado. Esse conjunto de regras de alertas fornece feedback de status de funcionamento para o console. O conjunto padrão de regras contém alertas do tipo:

- disco adicionado ou removido
- espaço na unidade
- uso da memória
- temperatura, ventiladores e voltagens
- monitoração do desempenho
- eventos de IPMI (em hardwares aplicáveis)

Para saber mais sobre alertas, consulte o capítulo Configuração de alerta no System Manager Guia do usuário.

Configuração de alertas

Quando ocorre um problema ou outro evento em um dispositivo (por exemplo, o dispositivo está com pouco espaço no disco) o O System Manager pode enviar alertas. Você pode personalizar esses alertas ao escolher o nível de severidade ou o limite que acionará o alerta. Os alertas são enviados para o console e podem ser configurados para executar ações específicas. Você pode definir alertas para muitos eventos ou problemas em potencial. O produto vem com um conjunto

de regras de alerta padrão o qual é instalado em um dispositivo gerenciado quando o componente de monitoração é instalado. Esse conjunto de regras de alertas fornece feedback de status de funcionamento para o console. O conjunto padrão de regras contém alertas do tipo:

- disco adicionado ou removido
- espaço na unidade
- uso da memória
- temperatura, ventiladores e voltagens
- monitoração do desempenho

Para saber mais sobre alertas, consulte o capítulo Configuração de alerta no System Manager *Guia do usuário*.

O que vem a seguir?

O Server Manager está configurado e pronto para usar. Você usou apenas uma fração dos recursos disponíveis no Server Manager e usou apenas uma parte dos recursos configurados (como, descoberta de dispositivo e configuração de agente). Os guias de acompanhamento (o *Guia de instalação e distribuição* e o *Guia de usuário*) podem fornecer informações mais detalhadas sobre os recursos do produto. Alguns desses recursos são:

Atualizações de software: Estabelece uma segurança contínua de nível de patch nos dispositivos gerenciados na rede inteira. Com o Server Manager, você pode automatizar os processos repetitivos de manutenção das informações de vulnerabilidades atuais, avaliar as vulnerabilidades de vários sistemas operacionais de dispositivos gerenciados, fazer o download dos arquivos executáveis de patchs apropriados, corrigir vulnerabilidades através da distribuição e instalação dos patchs necessários nos dispositivos afetados, e verificar se as instalações dos patchs foram bem-sucedidas.

Alertas: Assegura que você seja alertado se qualquer um dos dispositivos atingir um limite específico. Este recurso é relacionado ao recurso de Monitoração e pode notificá-lo de muitas maneiras diferentes. Por exemplo, se precisar saber quando o armazenamento nos dispositivos atingir 95% da capacidade, você pode escolher a maneira de ser alertado para isso (o agente pode enviar mensagens de email ou de pager, reinicializar ou desligar o dispositivo ou ainda adicionar informações aos logs de alerta).

Consultas: Gerencie a sua rede procurando e organizando os dispositivos no banco de dados núcleo com base num sistema específico ou nos critérios do usuário. Você pode consultar a lista de dispositivos gerenciados para aqueles que correspondem aos critérios que você especificar (como, por exemplo, todos localizados na sede ou todos com 256K de RAM) e agrupá-los para ações. Esses grupos podem ser estáticos (os membros do grupo só podem ser mudados manualmente) ou dinâmicos (os membros mudam quando os dispositivos satisfazem ou não satisfazem critérios especificados).

Distribuição de software: Cria tarefas para distribuir pacotes de software (um ou mais arquivos MSI, um executável, um arquivo de lote, arquivos RPM (Linux) ou um pacote criado com o Package Builder da LANDesk) para dispositivos alvo.

Monitoração: Monitora o status de funcionamento de um dispositivo usando um dos tipos suportados de monitoração (monitoração ASIC direta, IPMI em banda, IPMI fora de banda, CIM e assim por diante). A monitoração permite manter controle de muitos conjuntos de dados nos

dispositivos, como níveis de uso, eventos do SO, processos e serviços, desempenho histórico e sensores de hardware (ventiladores, voltagens, temperaturas, etc.). O recurso Alertas é um recurso relacionado que usa agente de monitoração para iniciar as ações de alerta.

Relatórios: Geram um ampla variedade de relatórios especializados que fornecem informações críticas sobre os dispositivos gerenciados na rede. O Server Manager utiliza um utilitário de inventário para adicionar dispositivos (e dados de hardware e software coletados sobre esses dispositivos) para o banco de dados núcleo. Você pode ver e imprimir esses dados de inventário da tela de inventário de um dispositivo, e também usá-los para definir consultas e grupos. A ferramenta de relatório aproveita as vantagens totais desses dados analisados de inventário, coletando e organizando esses dados em formatos úteis de relatório, que podem ser de ajuda na coleta e formatação de dados para os relatórios normativos.

Descoberta de dispositivos não gerenciados: Encontra dispositivos que não estão sendo gerenciados pelo console. Descoberta é o primeiro passo para incluir rapidamente novos computadores no gerenciamento. Você pode configurar uma tarefa de descoberta para analisar novos computadores todo mês.

Monitoração de licenças de software: Controla a conformidade geral de licenças. O agente de monitoração de licenças de software coleta dados (como, por exemplo, o total de minutos de uso, os números de execuções e a data da última execução de todos os aplicativos instalados em um dispositivo) e armazena-os no registro do dispositivo. Você pode usar os dados para monitorar o uso de produto e as tendências de recusa. O agente monitora passivamente o uso do produto em dispositivos, ocupando o mínimo de largura de banda. O agente continua a monitorar o uso para dispositivos móveis que estão desconectados da rede.

Distribuição de SO: Distribui imagens de SO para dispositivos na rede usando a ferramenta de distribuição baseada em PXE. Isso permite criar a imagem de dispositivos com discos rígidos vazios ou sistemas operativos não utilizáveis. Os representantes PXE leves eliminam a necessidade de um servidor PXE dedicado em cada sub-rede. A distribuição do SO facilita a provisão de novos dispositivos sem exigir a interação do usuário final ou da TI, após o início do processo.

Etapa 1: Criação do domínio de gerenciamento

Na etapa 1, são coletadas informações sobre a infra-estrutura da rede e são tomadas decisões para ajudá-lo a personalizar o domínio de gerenciamento.

Nesta etapa, você encontrará informações sobre o seguinte:

Coleta de informações da rede

Identifique e colete todas as informações críticas sobre a rede em relação a System Manager. É necessário, especificamente:

- determinar as configurações do dispositivo
- selecionar o servidor núcleo

Seleção do servidor núcleo

O servidor núcleo é o centro de um domínio de gerenciamento. Todos os arquivos e serviços essenciais estão contidos no servidor núcleo. Fisicamente, pode ser um servidor novo ou um servidor redirecionado.

Você pode executar o console de administrador do browser em uma estação de trabalho remota, onde são realizadas as atividades de gerenciamento como, por exemplo, gerenciar alertas, consultar o banco de dados núcleo ou criar scripts personalizados.

Verifique se o servidor selecionado para o servidor núcleo satisfaz os requisitos de sistema. Consulte Requisitos de sistema, adiante nesta fase.

Planejamento da disposição dos arquivos de programa

Durante a instalação, será possível especificar em que local os arquivos de programa serão instalados. Aceite os diretórios de destino padrão, a menos que tenha bons motivos para mudá-los. Se você decidir modificar o diretório de destino, o caminho desse diretório não pode conter caracteres de dois bytes.

O diretório de destino padrão dos arquivos do servidor núcleo é o seguinte:

```
C:\Arquivos de programas\LANDesk\ManagementSuite
```

O banco de dados núcleo

O System Manager instala um banco de dados MSDE no servidor núcleo.O tamanho limite de cada banco de dados MSDE é 2 GB. O número de servidores para os quais esse banco de dados fornece suporte depende do tamanho do arquivo de varredura de inventário da rede.

É provável que ocorram problemas de desempenho com o MSDE quando o banco de dados tiver mais de cinco tarefas simultâneas a serem realizadas. Por exemplo, se cinco admnistradores do System Manager são acessam o banco de dados ao mesmo tempo.

Segurança do núcleo/cliente:

Este produto usa um sistema de autenticação baseado em certificados. Durante a instalação do núcleo, o programa de instalação cria um certificado para o respectivo núcleo. Os Clientes procuram esse certificado quando se comunicam com o núcleo; e não podem se comunicar com um núcleo para o qual não tenham um certificado.

Os dispositivos só se comunicam com os servidores núcleo para os quais eles têm um arquivo de certificado confiável correspondente. Cada servidor núcleo possui o seu próprio certificado e as suas próprias chaves privadas e, por padrão, os agentes do cliente distribuídos a partir de cada servidor núcleo se comunicarão apenas com o servidor núcleo a partir do qual o software é distribuído.

Planejamento de um escopo

A administração com base em função é um recurso potente para o gerenciamento de segurança. Acesse as ferramentas de administração com base em função, no console, clicando em Usuários no painel esquerdo. Você deve estar conectado com direitos administrativos.

A administração com base em funções oferece recursos avançados de gerenciamento de dispositivo, permitindo adicionar usuários ao seu sistema !ServerName! e atribuir direitos e escopos a esses usuários. Os direitos determinam as ferramentas e os recursos que um usuário pode ver e usar (consulte "Compreensão de direitos" no Guia do Usuário do Server Manager). O escopo determina a gama de dispositivos que um usuário pode ver e gerenciar (consulte "Criação de escopos" no Guia do Usuário do Server Manager).

As funções podem ser criadas com base nas responsabilidades dos usuários, nas tarefas administrativas que você deseja que eles realizem e nos dispositivos que deseja que eles vejam, acessem e gerenciem. O acesso aos dispositivos pode ser restrito a uma localização geográfica, como um país, uma região, um Estado, uma cidade ou a um grupo ou tipo específico de servidor.

Para implementar e executar esse tipo de administração com base em funções por toda a rede, basta configurar os usuários atuais ou criar e adicionar novos usuários como usuários do produto e, em seguida, atribuir os direitos necessários (aos recursos do produto) e o escopo (para os dispositivos gerenciados).

O servidor núcleo utiliza escopos para limitar os dispositivos que os usuários do console podem ver. Podem ser atribuídos múltiplos escopos a um usuário, e um escopo pode ser usado por vários usuários. É possível criar os escopos de acordo com um dos métodos a seguir:

- (Padrão) **Escopo de todos os computadores:** Os usuários podem ver todos os dispositivos.
- **Baseado em uma consulta:** os usuários podem ver os dispositivos que atendem aos critérios selecionados de uma consulta específica atribuída a eles pelo administrador.
- **Baseado em um grupo:** Os usuários podem ver os dispositivos que satisfazem os critérios do grupo.

Para ver mais informações sobre escopos, consulte o Server Manager*Guia do usuário*.

Requisitos de sistema

Verifique se os seguintes requisitos de sistema são satisfeitos antes de instalar. O verificador de pré-requisitos faz isso automaticamente.

Servidores núcleo e de banco de dados

Verifique se todos os servidores núcleo e de banco de dados satisfazem os requisitos indicados na visão geral.

- Windows 2000 Server ou Advanced Server com SP 4, Windows Server 2003 Standard ou Enterprise edition x86 SP1 ou Windows 2003 R2
- Microsoft Data Access Components (MDAC) 2.8 ou superior
- Microsoft .NET Framework 1.1
- IIS (Internet Information Services)
- Suporte de IIS para scripts de ASP.NET v1.1
- Internet Explorer 6.0 SP1 ou mais recente
- Sistema de arquivos do Microsoft NT (NTFS)
- O servidor Windows usado no servidor núcleo precisa ser instalado como um servidor independente e não como um controlador de domínio primário (PDC), um controlador de domínio de backup (BDC) ou um controlador do Diretório Ativo.
- O SNMP deve estar instalado e o SNMP e os serviços de interceptação de SNMP devem ser iniciados
- 200 MB de espaço disponível na unidade do sistema e 900 MB de espaço disponível em pelo menos uma unidade de disco
- Privilégios de administrador
- O cliente LANDesk é a versão correta ou não está instalado

Requisitos do servidor núcleo
O arquivo da página do Windows deve ter pelo menos 12 + *N* (onde *N* é o número de megabytes de RAM do servidor núcleo). Caso contrário, os aplicativos do produto poderão gerar erros de memória.

É recomendado que haja 1 gigabyte de memória no computador núcleo se planejar instalar os produtos Management Suite e Server Manager no mesmo servidor núcleo.

Todos os serviços do produto hospedados em um servidor

No caso de domínios de gerenciamento menores, você pode instalar o servidor núcleo e o banco de dados núcleo em um servidor. Para essas redes, você pode considerar o uso do banco de dados padrão Microsoft MSDE que, geralmente, é mais fácil de manter. Essa é a única opção de bancos de dados para o System Manager.

Considerações quanto ao limite

Os servidores devem atender aos seguintes requisitos de sistema para instalar o núcleo e o banco de dados:

- Processador Pentium 4
- 4 GB de espaço livre em unidades de disco de 10.000 RPM ou mais velozes
- 768 MB + de RAM

Computadores de servidor gerenciado

O Management Suite dá suporte aos sistemas operacionais do cliente (nem todos os sistemas operacionais são suportados da mesma forma):

- Microsoft Windows 2000 Server (com SP4)
- Microsoft Windows 2000 Advanced Server (com SP4)
- Microsoft Windows 2000 Professional (com SP4)
- Microsoft Windows 2003 Server R2
- Microsoft Windows 2003 Server Standard Edition x86 (com SP1)
- Microsoft Windows 2003 Server Standard x64 Edition (com SP1)
- Microsoft Windows 2003 Server Enterprise Edition x86 (com SP1)
- Microsoft Windows 2003 Server Enterprise x64 Edition (com SP1)
- Microsoft Windows XP Professional (com SP2)
- Microsoft Windows XP Professional x64 (com SP2)
- Windows Small Business Server 2000 (com SP4)
- Windows Small Business Server 2003 (com SP1)
- Red Hat Enterprise Linux v3 (ES) 32 bits - U6
- Red Hat Enterprise Linux v3 (ES) EM64t - U6
- Red Hat Enterprise Linux v3 WS 32 bits - U6
- Red Hat Enterprise Linux v3 WS EM64t - U6
- Red Hat Enterprise Linux v3 (ES) 32 bits - U6
- Red Hat Enterprise Linux v3 (ES) EM64t - U6
- Red Hat Enterprise Linux v4 (ES) 32 bits - U2
- Red Hat Enterprise Linux v4 (ES) EM64t - U2
- Red Hat Enterprise Linux v4 (ES) 32 bits - U2
- Red Hat Enterprise Linux v4 (ES) EM64t - U2
- Red Hat Enterprise Linux v4 (WS) 32 bits - U2
- Red Hat Enterprise Linux v4 (WS) EM64t - U2
- SUSE* Linux Server 9 ES 32 bits SP2
- SUSE Linux Server 9 EM64t SP2
- SUSE Linux Server 10 ES 32 bits

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

Computadores com servidor gerenciado Linux

Abaixo está uma lista dos prerequisitos de firewall e RPM para a habilitação dos dispositivos Linux para gerenciamento.

Firewall

Para instalar inicialmente o agente de gerenciamento e configurar um servidor Linux para comunicar-se com o núcleo (usando o método "Por envio"), as conexões SSH devem ter permissão de passar através da firewall local do servidor Linux:

22 - TCP somente

Para os agentes poderem comunicar-se com o(s) Servidor(es) núcleo (para varreduras de inventário, distribuição de software, atualizações de vulnerabilidades, etc.), a firewall local do servidor Linux deve ser configurada para permitir a comunicação com as seguintes portas:

9593 - TCP somente

9594 - TCP somente

9595 - ambos TCP e UDP

Para se comunicar com o agente de gerenciamento, a firewall local do servidor Linux deve ser configurada para permitir a comunicação nas seguintes portas:

6780 - TCP somente

RPMs necessário (nº da versão ou mais recente)

É recomendado armazenar todos os produtos RPMs no diretório ...\ManagementSuite\ldlogon\RPMS. Você pode navegar até este diretório através de http://core name/RPMS.

REDHAT_ENTERPRISE

python

Versão do RPM:2.2.3-5 (RH3)

2.3.4-14 (RH4)

Versão binária:2.2.3

pygtk2 Versão do RPM:1.99.16-8 (RH3)

2.4.0-1 (RH4)

Versão binária:

sudo

Versão do RPM:1.6.7p5-1

Versão binária:1.6.7.p5

bash Versão do RPM:2.05b-29 (RH3)

3.0-19.2 (RH4)

Versão binária:2.05b.0(1)-release

xinetd Versão do RPM:2.3.12-2.3E (RH3)

2.3.13-4 (RH4)

Versão binária:2.3.12

mozilla Versão do RPM: 1.7.3-18.EL4 (RH4)

Versão binária:1,5

openssl Versão do RPM:0.9.7a-22.1 (RH3)

0.9.7a-43.1 (RH4)

Versão binária:0.9.7a

sysstat Versão do RPM:4.0.7-4

Versão binária:4.0.7

lm_sensors

Versão do RPM: 2.6 (esta versão pode não ser suficiente para mostrar sensores em novos computadores ASIC. Consulte a documentação dos lm_sensors ou o site (http://www2.lm-sensors.nu/~lm78) para ver informações mais detalhadas.

SUSE LINUX

ment(SuSE 64)

bash

Versão do RPM: 2.05b-305.6

mozilla

Versão do RPM: 1.6-74.14

net-snmp

Versão do RPM: 5.1-80.9

openssl

Versão do RPM: 0.9.7d-15.13

python-gtk

Versão do RPM: 2.0.0-215.1 [nota: mudança do nome do pacote]

python

Versão do RPM: 2.3.3-88.1

sudo

Versão do RPM: 1.6.7p5-117.1

sysstat

Versão do RPM: 5.0.1-35.1

xinetd

Versão do RPM: 2.3.13-39.3

lm_sensors

Versão do RPM: NA (nota: foi incorporado no kernel da versão 2.6)

Uso de porta do produto

Introdução

Ao usar este produto em um ambiente que inclua firewalls (ou roteadores que filtram tráfego), pode ser necessário ajustar as configurações de firewall ou de roteador para permitir a operação do produto. Esta seção descreve as portas utilizadas por vários componentes do produto. As informações aqui encontradas concentram-se no que é necessário para configurar roteadores e firewalls, deixando de fora as portas que só são usadas localmente (dentro das subredes individuais).

Informações de background sobre as regras do firewall

Essas informações aplicam-se à configuração das regras de firewall. Se não estiver familiarizado com este assunto, esta seção fornece algumas informações gerais de background sobre os conceitos principais.

Regras de firewall

"Abrir uma porta" não é um termo preciso. Não é possível simplesmente ir a uma firewall e "abrir a porta x". Abrir uma porta é a representação do processo de configurar uma regra de firewall. As regras de firewall descrevem que tráfego será ou não permitido passar por ela. As regras de firewall não filtram tráfego apenas no número da porta. Regras podem ser baseadas nos protocolos, números de origem e destino da porta, sentido (entrando / saindo), origem e destino de endereços IP e outras coisas.

Uma regra típica de firewall é semelhante à seguinte: "permitir tráfego que entra na porta 9535 de TCP". Para utilizar este produto, esta regra é necessária para suporte a controle remoto. A regra é baseada em três elementos:

1. Protocolo (TCP ou UDP)
2. Número da porta
3. Sentido (entrando ou saindo)

Esses três elementos são requeridos para a definição das regras de firewall.

Portas de origem e destino, portas dinâmicas

Há sempre duas portas para a comunicação de TCP ou UDP. Os pacotes TCP ou UDP são de uma porta de origem para uma porta de destino. As regras de firewall podem ser baseadas na porta de origem, na porta de destino ou em ambas. As portas citadas em documentos como este são sempre portas de destino.

As portas conhecidas como 5007 (usadas pelo serviço de inventário) referem-se a apenas um lado da comunicação. O outro lado da comunicação usa a porta dinâmica. As portas dinâmicas são designadas automaticamente pelo sistema operacional dentro da faixa 1024 a 5000.

Firewalls e tráfego de UDP

Para permitir tráfego de TCP pelo firewall, uma única regra é suficiente, por exemplo, para permitir conexões entrantes de TCP para a porta 5007. Quando a conexão TCP é estabelecida, os dados podem fluir em ambos os sentidos na conexão.

O tráfego UDP é diferente porque é sem conexão. Por exemplo, como padrão, o servidor núcleo faz "ping" para dispositivos na porta UDP 38293 antes de iniciar uma tarefa. Uma regra de firewall que permite pacotes UDP de saída para a porta 38293 deixa passar pacotes do servidor núcleo para um dispositivo fora do firewall, mas não os pacotes de resposta do dispositivo.

A regra que permite pacotes entrando e saindo na porta 38293 também não funciona por que só um lado da comunicação está ouvindo na porta conhecida. O outro lado usa uma porta dinâmica. Os pacotes de saída do servidor núcleo são de uma porta dinâmica para a porta 38293, por isso os pacotes de resposta do dispositivo são da porta 38293 para a mesma porta dinâmica e não para a porta 38293. Para permitir comunicação de duas vias, é necessária uma regra que permita aos pacotes UDP com porta de origem ou de destino = 38293. Essa regra, em geral, é aceitável na intranet, mas não em uma firewall externa (por que ela permitiria pacotes de entrada nas portas UDP).

Por esse motivo o tráfego UDP, em geral, não é considerado "aceitável para firewall". Para usar o exemplo considerado, há uma alternativa à porta UDP 38293: a porta TCP 9595. Ao gerenciar dispositivos através de um firewall, pode ser melhor configurar o produto a usar a porta TCP.

Portas utilizadas

Porta	Direção	Protocolos	Service
31770	console para dispositivo, dispositivo para núcleo	TCP	comunicação entre console e dispositivo
6787	console para dispositivo	TCP	comunicação entre console e dispositivo
9595	console para dispositivo	UDP	descoberta
9595	console para dispositivo	TCP	configuração de agentes
623	console para dispositivo	UDP	descoberta de ASF, IPMI
9535	console para dispositivo	TCP	controle remoto

Este produto precisa descobrir nós com o agente de gerenciamento instalado antes de poder gerenciá-lo. A porta UDP 9595 é usada para descoberta. Você pode também adicionar dispositivos individuais manualmente ao console, mas isso ainda exige que o dispositivo responda a um "ping" na porta UDP 9595. As comunicações entre o console e o dispositivo usam as portas TCP 31770 e 6787. O tráfego nesta última é baseado em HTTP. A porta UDP 623 é usada para descoberta de ASF (fórum padrão de alerta). Além disso, este produto utiliza a porta TCP 9535 para controle remoto. A descoberta IPMI está vinculada à descoberta ASF e utiliza a mesma porta (udp/623).

Etapa 2: Instalação do servidor núcleo

Esta etapa é focalizada na instalação do servidor núcleo.

Nesta etapa, você verá informações sobre o seguinte:

- Instalação do servidor núcleo
- Ativação do servidor núcleo
- Distribuição para dispositivos Windows
- Distribuição para dispositivos Linux

A instalação dos componentes descritos nesta etapa leva de 30 a 60 minutos.

Instalação do servidor núcleo

Para instalar o servidor núcleo

Antes de iniciar a instalação, é recomendado fechar os outros aplicativos e salvar os arquivos abertos. No Windows 2000/2003 Server que você selecionou para ser o servidor núcleo:

1. insira a mídia do produto na unidade ou execute o AUTORUN.EXE da sua imagem de instalação. Aparece a tela de execução automática (Autorun).
2. Clique em **Verificar prerequisitos e instalar**.
3. O verificador de requisitos de sistema é executado para verificar se o servidor satisfaz os requisitos mínimos do sistema. Verifique se todos os requisitos estão corretos. Se algum dos requisitos não for satisfeito, clique em **Falha**na linha de requisitos falhos para links ou informações referentes à instalação do requisito não atendido.
4. Clique em **Instalar agora** para executar o programa de configuração.
5. Selecione o idioma a ser instalado pelo programa de instalação. Clique em **OK**.
6. Aparece a tela de boas-vindas. Clique em **Avançar** para continuar.
7. Na tela do Contrato de licença, se concordar, clique em **Eu aceito os termos do contrato de licença** para continuar. Clique em **Avançar**.
8. Aceite a pasta de destino padrão ou especifique uma pasta de destino personalizada e clique em **Avançar**. A pasta de destino não pode conter caracteres de dois bytes. Se você mudar esta pasta, lembre-se de substituir o caminho dela por qualquer um dos caminhos encontrados na documentação do produto.
9. Digite uma senha de banco de dados MSDE. Anote ou decore essa senha. Clique em **Avançar** para continuar.
10. Digite o nome de uma organização e de um certificado para o certificado de segurança do servidor núcleo. Essas informações ajudam a nomear e descrever o certificado. Clique em **Avançar**.
11. Na página Pronto para instalar, clique em **Instalar**. O produto inicia a instalação.
12. O diálogo **Conclusão do assistente de instalação** será mostrado quando a configuração for concluída.
13. Clique em **Concluir**.

14. A configuração solicitará a reinicialização do servidor. Você deve clicar em **Sim** para concluir a instalação. Você perceberá, após a reinicialização e o início da sessão, que o programa de instalação será executado por mais alguns minutos enquanto finaliza a instalação. O programa de instalação não solicitará mais informações durante a primeira reinicialização.

Durante a instalação de um banco de dados núcleo MSDE em um servidor Windows 2003, o Windows poderá interromper a configuração e pedir permissão para abrir o SETUP.EXE. Se aparecer esse prompt, clique em Abrir ou o produto não será instalado corretamente.
Se quiser instalar as extensões Intel Platform Extensions para LANDesk Software, siga o assistente que se abre após a instalação do Server Manager.

Ativar o servidor núcleo

É necessário ativar o servidor núcleo antes de poder usar os produtos System Manager no servidor. Você pode ativar o servidor núcleo automaticamente pela Internet ou manualmente por email. Você pode reativar um servidor núcleo no caso de modificar significativamente a configuração do seu hardware.

Periodicamente, o componente de ativação no servidor núcleo gerará dados relativos a:

- número preciso de dispositivos que você está utilizando
- configuração do hardware criptografada, que não é de caráter pessoal
- Os programas de software específicos da LANDesk que você estiver usando (coletivamente, "dados de contagem de servidor")

Nenhum outro dado é coletado ou gerado pela ativação. O código chave de hardware é gerado no servidor núcleo com o uso de fatores de configuração de hardware não pessoais como, o tamanho do disco rígido, velocidade de processamento do computador, etc. O código chave de hardware é enviado para a LANDesk no formato criptografado e a chave privada para a criptografia reside apenas no servidor núcleo. O código chave de hardware é, então, usado pela LANDesk Software para criar uma parte do certificado autorizado.

Após a instalação do servidor núcleo, o utilitário de Ativação do servidor núcleo (**Iniciar | Todos os programas | LANDesk | Ativação do servidor núcleo**) é executado na primeira inicialização para atitvar o núcleo com o nome de usuário e senha fornecidos pelo OEM.

É possível fazer o upgrade a partir do System Manager ao Server Manager ou Management Suite ao usar o utilitário de ativação do núcleo. Consulte Uso do System Manager com o Management Suite ou o Server Manager.

Após ter ativado o servidor núcleo, utilize o diálogo **Preferências | Licença** para ver as informações de licenciamento do produto. Com a licença de OEM Intel, você está autorizado a executar o agente do produto em todo servidor ou placa principal Intel.

Sobre o utilitário de Ativação do servidor núcleo

Use o utilitário Ativação do servidor núcleo para ativar um novo servidor pela primeira vez. Inicie o utilitário clicando em **Iniciar | Todos os programas | LANDesk | Ativação do servidor**

núcleo. Se o seu servidor núcleo não tiver conexão para a Internet, consulte "Ativar um núcleo ou verificar os dados de contagem de servidores manualmente", adiante nesta seção.

Cada servidor núcleo deve ter um certificado autorizado exclusivo.

Periodicamente, o servidor núcleo verifica as licenças gerando o arquivo "\Arquivos de programas\LANDesk\Authorization Files\LANDesk.usage". Esse arquivo é enviado periodicamente para o servidor de licenciamento da LANDesk Software. Esse arquivo está em formato XML, é assinado digitalmente e criptografado. Quaisquer mudanças manuais feitas neste arquivo invalidam seu conteúdo e também o próximo relatório de utilização para o servidor de licenciamento da LANDesk Software.

O núcleo se comunica com o servidor de licenciamento de software da LANDesk via HTTP. Se você usa um servidor proxy, clique na guia **Proxy** do utilitário e digite as informações do seu proxy. Se seu núcleo tem uma conexão com a internet, a comunicação com o servidor de licenciamento é automática, não exigindo nenhuma intervenção de sua parte.

Observe que o utilitário de Ativação do servidor núcleo não inicia automaticamente uma conexão dial-up à internet, mas se você iniciar a conexão dial-up manualmente e executar o utilitário de ativação, o utilitário poderá utilizar a conexão dial-up para enviar os dados do relatório de utilização.

Se seu servidor núcleo não dispor de uma conexão com a internet, você pode verificar e enviar a contagem de servidores manualmente, do modo descrito mais adiante nesta seção.

Ativação do servidor núcleo

Para ativar um servidor

1. Clique em **Iniciar | Todos os programas | LANDesk | Ativação do servidor núcleo**.
2. Clique em **Ativar este servidor núcleo** usando o nome do contato e a senha da LANDesk.

O nome de contato e a senha são preenchidos automaticamente.

Ativação manual de um núcleo ou verificação manual dos dados de contagem de servidor

Se o servidor núcleo não dispor de uma conexão de Internet, o utilitário de Ativação do servidor núcleo não poderá enviar os dados da contagem de servidor. Nesse caso, aparecerá uma mensagem pedindo-lhe para enviar os dados de verificação de contagem de servidor e de ativação manualmente através de um email. A ativação por email é um processo simples e rápido. Quando você vir a mensagem de ativação manual no núcleo, ou se usar o utilitário de Ativação do servidor núcleo e vir a mensagem de ativação manual, siga os passos a seguir.

Para ativar manualmente um núcleo ou verificar manualmente os dados de contagem de servidores

1. Quando o núcleo lhe pedir para verificar manualmente os dados da contagem de servidor, ele criará um arquivo de dados chamado activate.txt na pasta "\Arquivos de programas\LANDesk\Authorization Files". Anexe este arquivo a uma mensagem de email e envie-a para licensing@landesk.com. O assunto e o corpo da mensagem não são importantes.
2. LANDesk Software processará o anexo da mensagem e enviará uma resposta ao endereço de email do qual a mensagem foi enviada. A mensagem da LANDesk Software lhe fornecerá instruções e incluirá um novo arquivo de autorização com anexo.
3. Grave o arquivo de autorização anexado na pasta "\Program Files\LANDesk\Authorization Files". O servidor núcleo processará o arquivo imediatamente e atualizará o status da ativação.

Se a ativação manual falhar ou o núcleo não conseguir processar o arquivo de ativação anexado, o arquivo de autorização que você copiou será renomeado com a extensão .rejected, e o utilitário irá registrar um evento com mais detalhes no log do aplicativo do Visualizador de eventos do Windows.

Conexão ao console

Após a configuração terminar, você ter reinicializado o servidor núcleo e a configuração ter sido completada e o núcleo ter sido ativado, inicie o console abrindo um browser e digitando o endereço do servidor no seguinte formato: http://servername/ldsm. (No servidor núcleo, clique em Iniciar | Todos os programas | LANDesk | System Manager) Ao iniciar o console, a janela de login do console aparecerá. Você pode ser solicitado a digitar a credencial da conta que instalou o LDSM a fim de conectar. Somente os membros do grupo LANDesk Management Suite no servidor núcleo podem conectar. Por padrão, o programa de instalação inclui o usuário ao qual você estava conectado no momento da instalação do núcleo no grupo LANDesk Management Suite. Se você quiser que outros usuários possam acessar o console, adicione-os a este grupo.

A primeira vez que o console é iniciado em um navegador, ele pode levar até 90 segundos para aparecer na tela. Essa demora ocorre porque o servidor precisa fazer uma compilação inicial de determinados códigos. Nas vezes subseqüentes o console iniciará muito mais rápido.

Distribuição para dispositivos Windows

Este produto também oferece suporte a um método de configuração agendado e baseado na instalação por envio, permitindo a distribuição remota dos agentes.

Para ativar a configuração baseada na instalação por envio de dispositivos Windows 2000/2003 que ainda não executam o agente de gerenciamento, é necessário fornecer as credenciais corretas de login, da seguinte forma:

1. No servidor núcleo, clique em **Iniciar | Todos os Programas | LANDesk |** LANDesk**Configurar serviços**, em seguida clique na guia **Agendador**.
2. Clique em **Alterar login**.
3. Nos campos **Nome de usuário e senha**, determine uma conta de administrador de domínio (no formato domínio\nome de usuário).

4. Pare e reinicie o serviço do planejador.
5. No Web console, defina os dispositivos alvos desejados, em seguida clique em **Configuração do agente > Tarefa agendada** para distribuir as configurações.

Você pode especificar o administrador de domínio durante a configuração dos membros Windows 2000/2003 que pertencem ao mesmo domínio do servidor núcleo. Para configurar servidores Windows 2000/2003 em outros domínios, é necessário configurar relações confiáveis. Lembre-se de que a conta identificada na etapa 3 também será a conta na qual o serviço do agendador será executado no servidor núcleo. Verifique se ela tem o direito de **Logon como um serviço**.

Se uma configuração de instalação por envio falhar e uma mensagem que diz "Não é possível localizar agente" for exibida, tente executar as etapas relacionadas a seguir para identificar o problema. Elas imitam as ações do agendador durante uma configuração de instalação por envio.

1. Localize o nome de usuário no qual o serviço do agendador é executado.
2. No servidor núcleo, inicie a sessão com o nome de usuário localizado na etapa 1.
3. Mapeie uma unidade para \\nome do servidor\C$. (Essa etapa provavelmente não será bem-sucedida. Ela poderá falhar por dois motivos. É muito provável que você não tenha direitos administrativos para o servidor. Se este nome de usuário não tiver direitos administrativos, é possível que o compartilhamento administrativo do servidor (C$) esteja desativado.)
4. Crie um diretório \\nome do servidor\C$\$ldtemp$ e copie um arquivo nele.
5. Use o Gerenciador de serviço do Windows e tente iniciar e parar serviços no servidor.

Se o dispositivo for habilitado com IPMI, é necessário fornecer a senha de BMC. Use a guia **Senha BMC** de **Configurar serviços** para criar uma senha para o BMC (Baseboard Management Controller) IPMI.

1. Na guia **Senha BMC**, digite uma senha no quadro de texto **Senha**, redigite a senha no quadro de texto **Confirmar senha**, em seguida clique em **OK**.

A senha não pode ser maior que 15 caracteres, cada um dos quais deve ser os números de 0 a 9 ou as letras de a a z maiúsculas ou minúsculas.

Se o dispositivo for habilitado com Intel* AMT, é necessário fornecer a senha do Intel AMT. Use a guia **Configuração de Intel AMT** dos **Serviços de configuração** para criar ou mudar a senha em um dispositivo habilitado com a tecnologia Intel* Active Management.

Para configurar a senha da tecnologia Intel AMT

1. Na guia **Configuração do Intel AMT**, digite nome do usuário e a senha atuais. Essas informações devem corresponder ao nome do usuário e à senha configurados na tela de configuração da Intel AMT (que é acessada nas configurações de BIOS do computador).
2. Para mudar o nome de usuário e a senha, preencha a seção **Nova senha Intel AMT**.
3. Clique em **OK**. Essa mudança será feita quando a configuração do cliente for executada.

Nota:A nova senha deve ser forte, o que significa que ela deve:

- ter pelo menos sete caracteres
- conter letras, números e símbolos

- ter pelo menos um caracter símbolo localizado numa posição entre o segundo e o sexto caracter
- ser significativamente diferente das senhas anteriores
- não conter nomes ou nomes de usuários
- não ser uma palavra ou nome comum

Distribuição para dispositivos Linux

É possível distribuir e instalar remotamente agentes Linux e RPMs em servidores Linux. Seu servidor Linux deve estar configurado corretamente para isto funcionar. Para instalar um agente em um servidor Linux, é necessário ter privilégios de raiz.

A instalação padrão Linux (Red Hat 3 e 4 e SUSE) inclui os RPMs requeridos pelo agente de gerenciamento padrão Linux. Se selecionar o agente de monitoração na Configuração de agentes, você precisará de um RPM adicional, o sysstat.

Para a configuração inicial dos agentes Linux, o servidor núcleo utiliza uma conexão SSH para identificar os servidores Linux alvo. É necessária uma conexão SSH funcional e com autenticação de nome de usuário/senha. Este produto não oferece suporte à autenticação de chaves públicas/chaves privadas. Qualquer firewall entre o núcleo e os servidores Linux deve abrir a porta SSH. Considere a execução de um teste da sua conexão SSH do servidor núcleo com um aplicativo SSH de terceiros.

O pacote de instalação de agentes Linux consiste em um script de shell, tarball(s) de agentes, configuração .INI dos agentes e certificados de autenticação dos agentes. Esses arquivos são armazenados no compartilhamento LDLogon do servidor núcleo. O script do shell extrai os arquivos da(s) tarball(s), instala os RPMs e configura o servidor para carregar os agentes e executar a análise de inventário periodicamente no intervalo especificado no agente de configuração. Os arquivos são colocados em /usr/landesk.

Você também deve configurar o serviço do planejador no núcleo para usar as credenciais de autenticação SSH (nome do usuário/senha) no servidor Linux . O serviço do planejador utiliza essas credenciais para instalar os agentes nos servidores. Use o Utilitário de configuração de serviços para digitar as credenciais SSH que você deseja que o serviço do planejador utilize como credenciais alternativas. Deve lhe ser pedido para reiniciar o serviço do planejador. Se isto não acontecer, clique em Parar e, em seguida, em Iniciar na guia do **Agendador**, para reiniciar o serviço. Isto ativará as alterações.

Após ter configurado seus servidores Linux e adicionado as credenciais Linux ao servidor núcleo, é necessário adicionar servidores à lista **Meus dispositivos** para que você possa distribuir os agentes Linux. Antes de poder distribuir para um servidor, ele deve ser adicionado à lista **Meus dispositivos**. Faça isso através da descoberta de seus servidores Linux com a Descoberta de dispositivos.

Para descobrir seus servidores Linux

1. Na Descoberta de dispositivos, crie uma tarefa de descoberta para cada servidor Linux. Use uma análise de rede padrão e digite o endereço IP do servidor Linux como o endereço IP inicial e final da faixa de endereços IP. Se houver muitos servidores Linux, digite uma faixa de endereços IP. Clique em OK após ter adicionado as faixas de endereços IP da descoberta.
2. Agende a tarefa de descoberta que você acabou de criar. Para fazer isto, clique na tarefa e clique em **Agendar**. Quando a tarefa for concluída, verifique se o processo de descoberta encontrou os servidores Linux que você deseja gerenciar.
3. Na Descoberta de dispositivos, selecione os servidores que quiser gerenciar, clique em **Alvo** para acrescentar os dispositivos selecionados à lista Alvo. Clique na guia **Gerenciar** na parte inferior da janela. Clique em **Mover dispositivos selecionados** e em **Mover**. Isto adiciona os servidores à lista **Meus dispositivos**, para que você possa defini-los como alvo da distribuição.

Para criar uma configuração de agentes Linux

1. Na Configuração de agentes, clique em **Nova**.
2. Digite um nova para a configuração, clique em HP-UX ou Linux Server Edition e clique em **OK**.
3. Selecione a configuração que acabou de criar e clique em **Editar**.
4. Selecione os agentes desejados.
5. Na guia Inventário, selecione as opções e o intervalo da freqüência do analisador que desejar. O script de instalação irá adicionar uma tarefa cron que executa o analisador nos intervalos selecionados.
6. Clique em **Salvar as alterações**.

Para distribuir a sua configuração de agentes, selecione-a em Configuração de agentes e clique em **Agendar a tarefa**. Configure a tarefa e monitore o progresso da tarefa em Configuração de tarefas.

Nota: Não aparecerá nenhuma informação de funcionamento em um computador Linux até o analisador de inventário terminar a primeira análise após a instalação. **Para instalar por pull uma configuração de agentes Linux**

1. Crie um diretório temporário no computador Linux (por exemplo, /tmp/ldcfg), e copie o seguinte no diretório:
    1. Todos os arquivos do diretório LDLOGON\unix\linux.
    2. Copie o script shell que tem o nome da configuração (<nome da configuração>.sh) no diretório temporário.
    3. Copie o arquivo *.0 que tem o nome da configuração no diretório temporário. O * (asterisco) representa oito caracteres (0-9, a-f).
    4. Copie todos os arquivos listados no arquivo <nome da configuração>.ini no diretório temporário. Para identificar esses arquivos, faça uma busca do arquivo .INI para "FILExx", onde xx é um número. A maioria das entradas que encontrar terão sido copiadas ao cliente na etapa 1, mas você encontrará arquivos .XML que devem ser copiados. Os nomes de arquivos devem permanecer sem mudanças, com as seguintes exceções:
        - alertrules\<qualquer_texto>.ruleset.xml deve ser renomeado para internal.ruleset.xml

- monitorrules\<qualquer_texto>.ruleset.monitor.xml deve ser renomeado para masterconfig.ruleset.monitor.xml

2. Se o computador for um IPMI/BMC (com a Monitoração inclusa na instalação), digite o seguinte na linha de comando:

export BMCPW="(bmc password)"

3. Como raiz, execute o script shell para a configuração. Por exemplo, se você nomeou o script "pull", use o caminho completo usado a seguir:

/tmp/ldcfg/pull.sh

4. Remova o diretório temporário e todo o seu conteúdo.

Nota: Se você instalar um agente por envio ou por recepção num computador Linux, em seguida executar

./linuxuninstall.sh -f ALL

para limpá-lo e depois enviar ou enviar novamente, o arquivo com GUID é o único arquivo que permaneceu no computador após esta operação ser completada.

A opção -f apaga todos os diretórios que pertencem ao produto. Consulte a documentação de desinstação Linux para informações adicionais.

Etapa 3: Distribuição em etapas

Na etapa 3, você verá informações sobre a distribuição em etapas. *Distribuição* é o processo de expansão de recursos de gerenciamento nos dispositivos que você deseja incluir no domínio de gerenciamento.

Você distribui este produto ao carregar os agentes e serviços do produto nos dispositivos. Isso permite gerenciá-los de um único local central.

Na fase 3, você obterá informações sobre os seguintes tópicos:

- A estratégia de distribuição em etapas
- Lista de verificação para configuração de dispositivos
- Distribuição para dispositivos Windows
- Compreensão da arquitetura de configuração do dispositivo

A estratégia de distribuição em etapas

A distribuição em etapas baseia-se em três princípios:

1. Distribuir os componentes para dispositivos menos utilizados ou de menor impacto em sua rede existente primeiro e, em seguida, prosseguir com os dispositivos que causam o maior impacto.
2. Confirmar que a funcionalidade de cada dispositivo gerenciado esteja estável antes da distribuição de mais agentes.
3. Prosseguir com a distribuição do produto em etapas bem planejadas, em vez de distribuir agentes para todos os tipos de dispositivo de uma só vez, o que poderia dificultar uma solução de problemas necessária.

Se as duas primeiras etapas forem concluídas, você estará pronto para iniciar a etapa final de distribuição do produto em seus dispositivos.

Lista de verificação para configuração de dispositivos

Para configurar dispositivos, você pode distribuir agentes remotamente do Web console ou instalá-los de um dispositivo gerenciado. Para fazer uma configuração por envio é necessário configurar os serviços de computadores IPMI ou Intel* AMT. Você pode usar o miniaplicativo Configurar serviços do !ServerName! para configurar os seguintes serviços para qualquer dos seus servidores núcleo e banco de dados. Para abrir o miniaplicativo Configurar serviços, no servidor núcleo, clique em **Iniciar | Arquivos do programa | LANDesk | LANDesk Configurar serviços**. Use a Senha BMC ou as guias Configuração Intel AMT.

- **Configuração por envio:**Use a configuração de agente para definir uma configuração de dispositivo. Dê as credenciais necessárias para os computadores AMT ou IPMI através de Configurar serviços (consulte "Configurar serviços" no *Guia de usuários*). Faça o alvo dos dispositivos desejados, em seguida agende uma tarefa por envio da configuração aos dispositivos. Consulte "Agentes de configuração" no *Guia do usuário*.
- **Configuração manual:** No dispositivo gerenciado, mapeie uma unidade para o compartilhamento LDLogon do servidor núcleo e execute SERVERCONFIG.EXE, o programa de configuração do servidor. Os componentes distribuídos para o cliente devem ser selecionados de forma interativa.

Obviamente, a configuração manual não é prática em um ambiente grande onde devem ser instalados e configurados dispositivos. Na maioria dos casos, você enviará os agentes ao seus dispositivos gerenciados. Observe que a instalação de produtos não instala agentes no núcleo automaticamente; é também necessário instalar agentes no núcleo, e depois reinicializar o núcleo manualmente.

Independente do modo de configuração dos dispositivos, utilize a Configuração do agente no console para criar a configuração do dispositivo a ser distribuída.

Os sistemas com o Windows XP Professional SP2 ou 2003 SP1 exigem configuração manual da firewall para obter uma funcionalidade completa do produto. Especifique os seguintes parâmetros para esses dispositivos: **Servidores gerenciados:**

Compartilhamento de arquivos e impressoras - TCP 139, 445; UDP 137,138 (O agente por envio não funciona sem isso)

Distribuição de software - TCP 9594, 9595 (Agente por envio não funciona sem isso)

Avançado - ICMP - “Permitir requisição de eco de entrada” (o dispositivo não pode ser descoberto se este não estiver habilitado.)

Servidor núcleo:

Inventário - 5007

Para especificar esses parâmetros, no dispositivo gerenciado, clique em **Iniciar | Painel de controle | Segurança**. Este produto vem com uma configuração de agente que contém: o agente padrão de gerenciamento, a atualização de software e os agentes de monitoração.

Você pode criar novas configurações que incluam somente os componentes que desejar instalar ou (apenas para a versão OEM) adicionar o Intel Active System Console à configuração padrão de agente . Observe que o processo de distribuir agentes não é cumulativo; qualquer distribuição desinstala todos os agente existentes. Para distribuir um novo agente para uma configuração, é necessário adicioná-lo aos agentes que quiser incluir na configuração. **Para criar uma configuração**

1. No painel de navegação esquerdo, clique em **Configuração do agente**.
2. Clique em **Novo**.
3. Digite um nome para a nova configuração na caixa Nome da configuração.

Digite um nome que descreva a configuração que você está criando, por exemplo, DBServer ou Executive Office Server. O nome pode ser o nome de uma configuração existente ou um novo nome.

4. Selecione **Linux server edition**, **Microsoft Windows server edition** ou HP-UX.
5. Para gerenciar servidores habilitados com o IPMI sem instalar os agentes de software do produto, cheque a configuração **somente IPMI BMC** se a configuração for para servidores compatíveis com IPMI, em seguida clique em **OK**.
6. Selecione a configuração que acabou de criar e clique em **Editar**.

Nas guias, algumas opções podem aparecer desativadas, pois elas não são aplicáveis à configuração escolhida. Por exemplo, se você selecionar uma configuração Windows de IPMI de apenas BMC, não haverá opções configuráveis.

7. Na guia **Agente**, selecione os agentes que desejar distribuir.
    - **Todos:**Instala todos os agentes no dispositivo selecionado.
    - **Atualização de software:** Instala o agente de atualização. Com este agente instalado, você pode configurar a forma como o analisador é executado para detectar atualizações disponíveis.
    - **Monitoração:**Instala o agente de monitoração no dispositivo selecionado. O agente de monitoração permite muitos tipos de monitoração, inclusive a monitoração direta ASIC, IPMI em banda, IPMI fora de banda, Intel Active System Console, Intel AMT e CIM.
8. A **Configuration** é mostrada somente para informação
9. Selecione uma opção de reinicialização.

A reinicialização manual significa que os dispositivos não reinicializarão mesmo se os agentes selecionados precisarem de reinicialização. Você deve reinicializar o dispositivo manualmente. Se o dispositivo precisar de uma reinicialização, os agentes instalados não funcionarão corretamente até o dispositivo reinicializar. A reinicialização de servidores, se necessária, reinicializa somente dispositivos e se um agente selecionado requerer a reinicialização.

Nota: Somente os dispositivos que atualizarem agentes 8.5 existentes requerem uma reinicialização.

10. Na guia **Inventário**, defina as configurações do Analisador de inventário. Elas são explicadas abaixo.

- **Atualização automática:** Os dispositivos remotos lêem a lista de softwares do servidor núcleo durante as análises de software. Caso essa opção esteja selecionada, cada dispositivo deverá ter uma unidade mapeada para o diretório LDLOGON no servidor núcleo, de modo que possam acessar a lista de softwares. Alterações na lista de softwares são imediatamente disponibilizadas para os dispositivos.
- **Atualização manual:**A lista de softwares usada para excluir títulos durante as análises de software é carregada em cada dispositivo remoto. Sempre que a lista de softwares for alterada no console, ela deverá ser reenviada manualmente para os dispositivos remotos.
- **Configurações do analisador de inventário:**Quando o inventário for executado. É possível selecionar a freqüência e especificar que seja executada sempre na inicialização.

Se selecionar a opção **Entre as horas de** do analisador de inventário, você pode especificar um intervalo de horas no qual a varredura pode ser executada. Se um dispositivo conectar durante o intervalo de horas que você especificar, a varredura de inventário será executada automaticamente. Se o dispositivo já estiver conectado, quando o momento chegar, a varredura de inventário iniciará automaticamente. Essa opção é útil se você quiser intercalar disparos de varreduras de inventários nos dispositivos de forma que eles não enviem varreduras de um só vez.

- **Sempre executar no início:**A varredura de inventário é executada sempre que o dispositivo é iniciado.

11. Na guia **Conjuntos de regras**, selecione qualquer conjunto de regras de monitoração e/ou de alerta que quiser incluir na configuração. Esses conjuntos de regras são armazenados na pasta ldlogon/alertrules. Novos conjuntos de regras podem ser criados na Monitoração ou no Alerta. Para que os conjuntos de regras recém-criados sejam exibidos nas listas suspensas, é necessário gerar o XML para o conjunto de regras personalizado.
12. Clique em **Salvar mudanças** para salvar a configuração do agente.

Para ver mais informações sobre a distribuição para dispositivos, consulte "Compreensão da arquitetura de configuração do agente" no final deste capítulo.

Distribuição para dispositivos Windows

Este produto também oferece suporte a um método de configuração agendado e baseado na instalação por envio, permitindo a distribuição remota dos agentes.

Para ativar a configuração baseada na instalação por envio de dispositivos Windows 2000/2003 que ainda não executam o agente de gerenciamento, é necessário fornecer as credenciais corretas de login, da seguinte forma:

1. No servidor núcleo, clique em **Iniciar | Todos os programas |** LANDesk | LANDesk**Configurar serviços**, em seguida clique na guia **Agendador**.
2. Clique em **Alterar login**.
3. Nos campos **Nome de usuário e senha**, determine uma conta de administrador de domínio (no formato domínio\nome de usuário).
4. Pare e reinicie o serviço do planejador.
5. No Web console, defina os dispositivos alvos desejados, em seguida clique em **Configuração do agente > Tarefa agendada** para distribuir as configurações.

Você pode especificar o administrador de domínio durante a configuração dos membros Windows 2000/2003 que pertencem ao mesmo domínio do servidor núcleo. Para configurar servidores Windows 2000/2003 em outros domínios, é necessário configurar relações confiáveis. Lembre-se de que a conta identificada na etapa 3 também será a conta na qual o serviço do agendador será executado no servidor núcleo. Verifique se ela tem o direito de **Logon como um serviço**.

Se uma configuração de instalação por envio falhar e uma mensagem que diz "Não é possível localizar agente" for exibida, tente executar as etapas relacionadas a seguir para identificar o problema. Elas imitam as ações do agendador durante uma configuração de instalação por envio.

1. Localize o nome de usuário no qual o serviço do agendador é executado.
2. No servidor núcleo, inicie a sessão com o nome de usuário localizado na etapa 1.
3. Mapeie uma unidade para \\nome do servidor\C$. (Essa etapa provavelmente não será bem-sucedida. Ela poderá falhar por dois motivos. É muito provável que você não tenha direitos administrativos para o servidor. Se este nome de usuário não tiver direitos administrativos, é possível que o compartilhamento administrativo do servidor (C$) esteja desativado.)
4. Crie um diretório \\nome do servidor\C$\$ldtemp$ e copie um arquivo nele.

5. Use o Gerenciador de serviço do Windows e tente iniciar e parar serviços no servidor.

Se o dispositivo for habilitado com IPMI, é necessário fornecer a senha de BMC. Use a guia **Senha BMC** de Configurar serviços para criar uma senha para o BMC (Baseboard Management Controller) IPMI.

1. Na guia **Senha BMC**, digite uma senha no quadro de texto **Senha**, redigite a senha no quadro de texto **Confirmar senha**, em seguida clique em **OK**.

A senha não pode ser maior que 15 caracteres, cada um dos quais deve ser os números de 0 a 9 ou as letras de a a z maiúsculas ou minúsculas.

Se o dispositivo for habilitado com Intel* AMT, é necessário fornecer a senha do Intel AMT. Use a guia **Configuração de Intel AMT** dos Serviços de configuração para criar ou mudar a senha em um dispositivo habilitado com a tecnologia Intel Active Management.

Para configurar a senha da tecnologia Intel AMT

1. Na guia **Configuração do Intel AMT**, digite nome do usuário e a senha atuais. Essas informações devem corresponder ao nome do usuário e à senha configurados na tela de **Configuração da Intel AMT** (que é acessada nas configurações de BIOS do computador).
2. Para mudar o nome de usuário e a senha, preencha a seção **Nova senha Intel AMT**.
3. Clique em **OK**. Essa mudança será feita quando a configuração do cliente for executada.

Nota: A nova senha deve ser forte, o que significa que ela deve:

- ter pelo menos sete caracteres
- conter letras, números e símbolos
- ter pelo menos um caracter símbolo localizado numa posição entre o segundo e o sexto caracter
- ser significativamente diferente das senhas anteriores
- não conter nomes ou nomes de usuários
- não ser uma palavra ou nome comum

Verificação da distribuição bem sucedida de agente

Para verificar se a distribuição do agente de gerenciamento nos dispositivos foi bem-sucedida, veja se consegue executar as seguintes tarefas dentro do console. Para obter informações adicionais sobre a conclusão destas tarefas, consulte os capítulos no *System ManagerGuia do usuário* que correspondem aos respectivos recursos.

Inventário

- Na lista **Meus dispositivos**, clique duas vezes em um dispositivo, em seguida veja a lista dos agentes instalados.
- Execute uma consulta de inventário.
- Selecione um dispositivo, em seguida clique em **Inventário** para ver os dados para aquele dispositivo.
- Modifique um arquivo WIN.INI do dispositivo Windows, analise novamente o dispositivo e verifique se as alterações foram registradas no CHANGES.LOG.

Distribuição de dispositivos na linha de comando

Você pode controlar que componentes são instalados nos dispositivos usando os parâmetros da linha de comandos com o SERVERCONFIG.EXE.

É possível iniciar o SERVERCONFIG.EXE no modo standalone. Ele está localizado em (unidade de sistema)\Arquivos de programas\LANDesk\ManagementSuite\LDLogon no servidor núcleo. O SERVERCONFIG.EXE pode ser encontrado também no compartilhamento \\coreservername\LDLogon, que é legível em qualquer servidor Windows 2000/2003.

Arquitetura de configuração do agente

O SERVERCONFIG.EXE

SERVERCONFIG.EXE é o utilitário de configuração do dispositivo para o produto. Ele configura os servidores Windows para gerenciamento em três etapas:

1. Ele determina se o computador já foi configurado anteriormente por outro produto LANDesk. Nesse caso, o SERVERCONFIG remove os arquivos antigos e reverte qualquer mudança.
2. O SERVERCONFIG procura um arquivo oculto denominado CCDRIVER.TXT para determinar se o servidor precisa ser (re)configurado. (O processo de decisão do SERVERCONFIG é descrito abaixo.) Se o dispositivo não precisar ser (re)configurado, o SERVERCONFIG será fechado.
3. Se o dispositivo não precisar ser (re)configurado, o SERVERCONFIG carrega o arquivo de inicialização apropriado (SERVERCONFIG.INI) e executa as instruções nele contidas.

Se você executar o SERVERCONFIG.EXE outra vez e selecionar agentes diferentes da primeira execução, os agentes desta execução serão eliminados. É necessário selecionar cada agente que você precisa em cada nova execução do SERVERCONFIG.EXE, mesmo se tiver instalado os agentes anteriormente.

Os seguintes parâmetros da linha de comandos estão disponíveis para o SERVERCONFIG.EXE:

Parâmetro	Descrição
/I=	Componentes a incluir (incluindo as aspas): "Common Base Agent" "Inventory Scanner" "Alerting" "Vulnerability scanner" "Server Monitor" "Active System Console" Você pode combinar todos esses na mesma linha. Por exemplo, Exemplo: SERVERCONFIG.EXE /I="Mirror Driver" /I="Vulnerability scanner"

/IP	Configura utilizando IP.
/L ou /Log=	Caminho para arquivos de log CFG_YES e CFG_NO que registram quais dispositivos foram ou não configurados.
/LOGON	Executa comandos [LOGON] com prefixos.
/N ou /NOUI	Não exibe a interface do usuário.
/NOREBOOT	Não reinicializa dispositivo quando concluído.
/P	Solicita permissão de execução ao usuário
/REBOOT	Força a reinicialização após execução
/TCPIP	Mesmo que IP (veja acima)
/X=	Componentes a serem excluídos Exemplo: SERVERCONFIG.EXE /X=SD
/CONFIG=	/CONFIG]= Especifique um arquivo de configuração de dispositivo para usar no lugar do arquivo padrão SERVERCONFIG.INI. Por exemplo, se você tiver criado um arquivo de configuração chamado NTTEST.INI, use esta sintaxe: SERVERCONFIG.EXE /CONFIG=TEST.INI Os arquivos .INI personalizados devem estar no mesmo diretório do SERVERCONFIG.EXE e observe que o parâmetro /config utiliza o nome de arquivo sem o prefixo 95.
/? ou /H	Exibir menu de ajuda

Distribuição do agente de gerenciamento padrão

O agente de gerenciamento padrão é um agente necessário e está no protocolo subjacente do produto.

Distribuição da Análise de inventário

O agente do analisador de inventário executa a análise e as operações de reparo. O botão **Agendar tarefas de segurança** cria uma tarefa que inicia o vulscan.exe sem parâmetros. Quando iniciado sem parâmetros, o vulscan descobre onde está seu núcleo acessando a chave de registro “hklm\software\intel\landesk\LDWM”, valor “CoreServer”. Ele, então, solicita as informações da lista mais recente de vulnerabilidades para analisar, executa a análise e submete os resultados para o núcleo. Os resultados são colocados na lista Atualizações detectadas. As atualizações detectadas devem ser descarregadas no núcleo. As atualizações podem receber patch através do processo de correção. Se o processo de correção instalar um ou mais patches com êxito, ele reanalisa e envia os novos resultados ao núcleo. Este é para as atualizações LANDesk e atualizações OEM.

Distribuição do analisador de inventário

Você pode usar o analisador de inventário para adicionar dispositivos ao banco de dados núcleo e para coletar dados de hardware e software dos dispositivos. A varredura de inventário é automaticamente executada quando o dispositivo é inicialmente configurado. O analisador coleta os dados de hardware e software e os insere no banco de dados núcleo. Depois disso, a análise de hardware é executada sempre que o dispositivo é inicializado, mas a análise de software é executada apenas em um intervalo especificado.

Distribuição de agentes de monitoração

O agente de monitoração permite muitos tipos de monitoração, inclusive a monitoração direta ASIC, IPMI em banda, IPMI fora de banda e CIM.

Distribuição do Active System Console

Instala o agente que permite ao Intel Active System Console ser acessado do System Manager através da interface ou através dos menus. Esse agente é instalado somente em dispositivos com placas Intel; se você incluir esse agente em uma distribuição para placa não-Intel, ele não será instalado.

Desinstalação do servidor núcleo

Assim como há uma estratégia específica que deve ser seguida para distribuir os diferentes componentes, há uma estratégia correspondente para desinstalá-los.

As seções a seguir mostram como desinstalar corretamente cada componente. É necessário desinstalar os componentes na ordem a seguir:

1. Desinstalação dos agentes do produto dos dispositivos.
2. Desinstalar o servidor núcleo.

Desinstalação dos agentes de produto dos dispositivos

A primeira etapa para desinstalar o software da rede é desinstalar seus agentes de produto dos seus dispositivos.

Para desinstalar agentes de servidores

1. Faça logon em um servidor com direitos administrativos.
2. Mapeie uma unidade à pasta do compartilhamento ManagementSuite do servidor núcleo.
3. Abra uma tela de comando, mude para a letra da unidade da pasta ManagementSuite e digite o seguinte:

uninstallwinclient.exe

4. A desinstalação será executada silenciosamente e removerá todos os agentes.

Você também pode selecionar Iniciar,Executar, em seguida digitar *core name*\LANDesk\ManagementSuite\uninstallwinclient.exe.**Para remover completamente o agente Linux de um servidor Linux**

1. Na pasta de compartilhamento ManagementSuite, procure o arquivo linuxuninstall.tar.gz e copie-o na caixa Linux.
2. Execute esse arquivo, usando as opções x, z e f. A linha de comando deve mostrar

tar xzf linuxuninstall.tar.gz

3. Após o arquivo ter sido executado, rode ./linuxuninstall.sh da linha de comando.

Para obter ajuda neste arquivo, execute-o com a opção -h. Nota: Se você instalar um agente por envio ou por recepção num computador Linux, em seguida executar

./linuxuninstall.sh -f ALL

para limpá-lo e depois fizer novamente o envio ou recepção, este processo criará entradas duplicadas do banco de dados para o mesmo computador com o mesmo nome e IP porque o GUID do computador é apagado.

A opção -f apaga todos os diretórios que pertencem ao produto. Consulte a documentação de desinstação Linux para informações adicionais.

O arquivo /etc/ldiscnux.conf é o único que permanece após a desinstalação. Este arquivo foi lá deixado para evitar que o banco de dados tenha vários dispositivos duplicados. Se não for colocar este dispositivo de volta no banco de dados, você pode excluir o arquivo com segurança. O arquivo UninstallWinClient.exe está na pasta de compartilhamento ManagementSuite. Apenas os administradores têm acesso a esse compartilhamento. Este programa desinstala os agentes do produto em qualquer dispositivo em que é executado. É um aplicativo Windows que é executado silenciosamente sem exibir nenhuma interface. Você pode ver duas instâncias do servidor no banco de dados que acabou de excluir. Uma dessa instâncias contém somente dados históricos,e a outra contém os dados de agora para o futuro.

Nota: Por padrão, o Uninstallwinclient.exe reinicializa o dispositivo após desinstalar os agentes. Para evitar a reinicializacão, adicione a chave /noreboot à linha de comando.

Desinstalação do servidor núcleo

A etapa final de desinstalação do produto da rede é desinstalar o software do servidor núcleo. Antes disso, verifique se os agentes de software do produto foram desinstalados dos servidores.

Para desinstalar o servidor núcleo:

1. Vá para o servidor núcleo.
2. Clique em **Iniciar** | **Configurações** | **Painel de controle** e clique duas vezes em **Adicionar/Remover programas**.
3. Se tiver instalado, selecione Intel Platform Extensions para LANDesk software e clique em Adicionar/Remover.
4. Para desinstalar o software, selecione LANDesksoftware.
5. Clique em **Adicionar/Remover**.

Desinstalação do banco de dados núcleo
É necessário desinstalar manualmente o banco de dados núcleo.

Desinstalação do banco de dados núcleo

Como padrão, o banco de dados núcleo não é desinstalado quando você desinstala o LANDesk® System Manager. Importante: Não desinstale o banco de dados núcleo se for reinstalar, mais tarde, o LANDesk® System Manager no computador.

Para desinstalar o banco de dados núcleo.

1. Vá para o servidor núcleo.
2. Clique em **Iniciar** | **Configurações** | **Painel de controle** e clique duas vezes em **Adicionar/Remover programas**.
3. Para desinstalar o banco de dados núcleo, selecione Microsoft SQL Server Desktop Engine (LDMSDATA).

4. Clique em **Adicionar/Remover**.

Arquivos do banco de dados

A remoção do Microsoft SQL Server Desktop Engine não apaga os arquivos do banco de dados usados pelo LANDesk® System Manager. Além de ocupar espaço no disco, não nenhum problema em deixar os arquivos do banco de dados no seu computador. Se quiser remover manualmente esses arquivos de banco de dados, apague o conteúdo da pasta \Arquivos de programas\Microsoft SQL Server\MSSQL$LDMSDATA\Data.

Suporte

São oferecidos serviços de suporte on-line pela LANDesk Software na web (disponível apenas em inglês). Os serviços contêm as informações mais atualizadas de produtos da LANDesk Software. Também é possível localizar notas de instalação, dicas para solução de problemas, atualizações de software e informações de atendimento ao cliente. Visite o site a seguir e acesse a página do produto:

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

Também é possível o download das versões mais recentes das Notas de versão e da documentação, que podem conter informações não disponíveis no momento de lançamento do produto. Se tiver recebido o System Manager de um fabricante OEM, contate o respectivo serviço de suporte.

Caso não consiga resolver um problema por meio deste guia ou por meio da consulta ao site de suporte da LANDesk Software, a LANDesk Software oferece vários serviços pagos de suporte, consultoria e parceria. Para ver mais informações, consulte a página de atendimento ao cliente em:

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

Antes de entrar em contato com o atendimento ao cliente, tenha as seguintes informações disponíveis:

- Seu nome, o nome da empresa e a versão do produto que está usando.
- Sistema operacional de rede usado (nome e versão).
- O patch ou pacote de serviços instalado.
- Etapas detalhadas para reproduzir o problema.
- Etapas já realizadas para solucionar o problema.
- Qualquer informação importante sobre o sistema que possa ajudar o engenheiro do Atendimento ao cliente a entender o problema como, o tipo de aplicativo de banco de dados usado, a marca da placa de vídeo instalada ou o fabricante ou o modelo do computador usado.